



Design Considerations for Cisco PanGo Asset Tracking

This document is intended for network professionals and others participating in the design and deployment of enterprise location-aware wireless LANs. Specifically, this information targets those individuals who plan to integrate the following asset tracking product offerings into a Cisco Unified Wireless Network (Cisco UWN):

- PanGo Networks PanOS location management platform
- PanGo Networks PanGo Locator asset tracking applications

Contents

Introduction	3
Fundamental Concepts	4
Location-Based Services in the Cisco Unified Wireless Network	4
Location Clients and the SOAP/XML API	6
Active RFID Tags	8
PanGo PanOS Server and PanGo Locator	9
PanGo PanOS Server	9
PanGo Locator Web Applications	11
PanGo Locator and Cisco WCS	14
PanGo Active RFID LAN Tags v2	16
Overview	17
Assembly	17
Tag Operation	19
Tag Initialization	20
Theory of Operation	20
RSSI Mode	22



Chirp Mode	23
Tag Serial Interface	27
Upgrading Tag Firmware	29
Design and Deployment Best Practices	31
PanGo Software Installation	31
Firewall Port Considerations	34
Cisco UWN Location-Based Services Best Practices	34
Planning for Tag Initialization	35
Planning for PanGo Version 2 Tag Deployment	42
Tag Security Considerations	42
WLAN Controller Tag Considerations	43
Location Appliance Tag Considerations	45
WCS Tag Considerations	46
PanGo Locator Tag Considerations	48
Other Tag Considerations	51
PanGo PanOS Server and PanGo Locator Considerations	53
Defining Users and Groups	54
Secure HTTP	54
Accessing Locator Applications	55
PanOS Server Location Appliance Polling	56
Monitoring Assets	56
Unassigned Devices	58
Tag MAC Address Identification	59
Defining Maps	61
Defining Physical Locations	67
Use of Multiple Location Appliances	70
Notifications	70
Caveats	72
Known Caveats	72
Additional Caveats	72
Chirp Mode Tags Using OTA Update May Not Be Detected By All APs	72
AP1210/1220/123x Access Points May Not Reliably Detect Chirp Mode Tags	73
Chirp Mode Tags Using OTA Update May Vary Transmit Power With DTPC	73
Chirp Mode Multicast Frames May Vary In Transmitted Signal Strength	73
Tags May Appear As Two Tracked Devices in Location Appliance	74
Appendix A—RSSI Mode Tag Operation	74
Appendix B—Stand-alone Access Point Initialization Configuration	77
Appendix C—Manual Chirp Mode Configuration	79
Appendix D—Suspending Over-The-Air Configuration Updates	80

[Appendix E—Multiple Location Appliance Properties Files](#) 80

[Appendix F—Basic PanGo v2 Tag CLI Commands](#) 82

Introduction

This document is not intended to serve as a step-by-step configuration guide. Several quality documents available from both Cisco Systems and PanGo Networks (<http://www.pango.com>) provide such guidance. References are made from such documents within this guide as necessary.

Rather, the intent is to educate the technical reader with regard to the following:

- Basic architecture, benefits, and operational characteristics of the Cisco Technology Development Partner (CTDP) solution known as PanGo Locator and the PanGo PanOS Platform
- How the CTDP solution interfaces to the Cisco UWN
- Relevant design aspects of both the CTDP solution and the Cisco location-enabled wireless network directed towards achieving a successful installation

It is assumed that the reader is familiar with 802.11 wireless LAN technology as well as the basic architecture, components, and design best practices associated with the location-aware Cisco UWN.



Note

To review background material pertaining to design best practices associated with the Cisco UWN, see the following URLs:

<http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/emob30dg-Book.html> and <http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html>

This document contains the following sections:

- Fundamental Concepts—Overall architecture and operation of the location-enabled Cisco UWN and the mechanisms through which third-party partner solutions interface with it
- PanGo PanOS Server and PanGo Locator—Roles and functions of the PanGo location client
- PanGo Locator and Cisco WCS—Relationship between PanGo Locator and Cisco Wireless Control System (WCS), highlighting the fundamental differences in the feature set and target audience each is intended to address
- PanGo Active RFID LAN Tags v2—Details of the PanGo v2 LAN Tag along with its various initialization and operation modes
- Design and Deployment Best Practices—Best practice considerations for the design and deployment of an integrated Cisco/PanGo Asset tracking solution
- Appendices—Additional technical information regarding the initialization of PanGo PanOS, Locator, and v2 tags

This document is based on the following software and hardware:

- Cisco UWN software release 4.0, including the following:
 - Cisco WCS
 - Cisco Wireless LAN Controller 4400
 - Cisco 2700 Series Wireless Location Appliance (release 2.1)
- PanGo PanOS Server and Locator version 4.5
- PanGo v2 LAN Tag with MIPS firmware 2.1.5 and microcode 87.68.

Fundamental Concepts

Location-Based Services in the Cisco Unified Wireless Network

Figure 1 shows the overall architecture of the location-aware Cisco Unified Wireless Network.

Figure 1 *Location-Aware Cisco UWN Architecture*

Optional Third Party
Location Client



Access points (APs) forward information to WLAN controllers (WLCs) regarding the detected signal strength of any Wi-Fi clients, 802.11 active RFID tags, rogue APs, or rogue clients. APs collect signal strength information on their primary channel of operation, periodically going off-channel and scanning the other channels in the assigned regulatory channel set. The collected information is forwarded to the WLAN controller to which the AP is currently registered. Each controller manages and aggregates all such signal strength information, awaiting polling from the location appliance.

The location appliance uses Simple Network Management Protocol (SNMP) to poll each controller for the latest signal strength information pertaining to each enabled tracked device category. The location appliance can also issue notifications to external systems using Simple Object Access Protocol/Extensible Markup Language (SOAP/XML), SNMP, Syslog, or Simple Mail Transfer Protocol (SMTP) protocols.

Some location clients, such as PanGo Locator, can issue notifications to external systems independently of the location appliance.

**Note**

For more information regarding the various modes of localization possible using Cisco WCS and the Cisco Location Appliance, see the “Cisco Unified Wireless Control System” chapter in the *Enterprise Mobility 3.0 Design Guide* at the following URL:
<http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/emob30dg-Book.html>.

Figure 2 shows a step-by-step flow diagram of the process where the flow of signal strength and tag payload information is shown for active RFID asset tags that communicate via the use of Layer 2 multicasts. As is discussed in more detail in later sections, the PanGo LAN Tag v2 configured for *chirp mode* operates in this fashion.

Figure 2 Asset Tag RSSI Information Flow

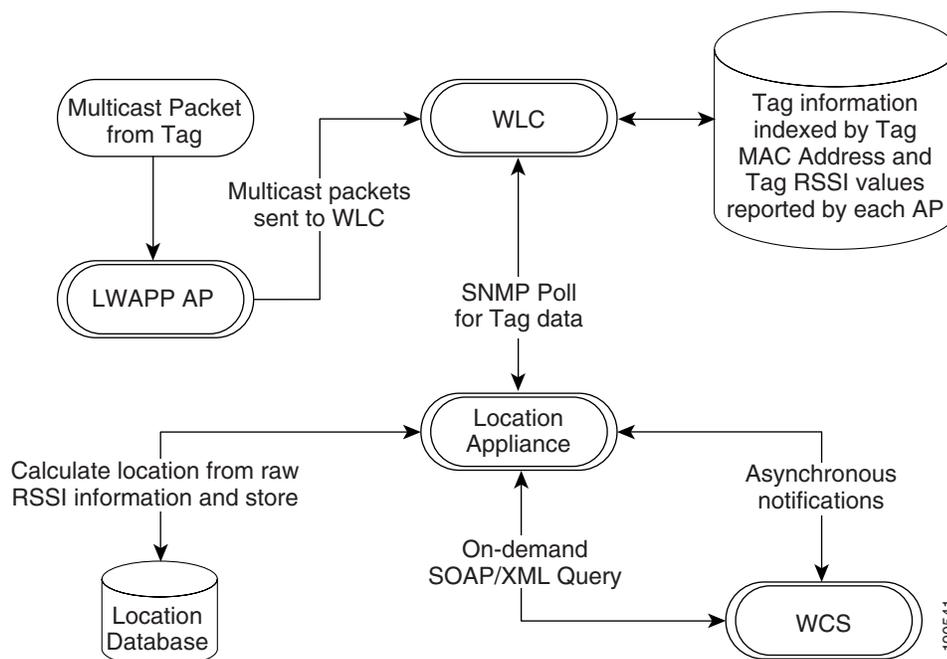


Figure 2 provides a pictorial representation of the following:

- At each beacon interval, the asset tag transmits a Layer 2 multicast on its configured channels.
- Access points detect the asset tag transmission, which is forwarded to the WLC to which the detecting access points are registered.
- The WLC stores the battery status information associated with the asset tag in an internal table indexed by the asset tag MAC address.
- For each tag detected in the network by an access point registered to this WLC, the WLC places the following asset tag information in an internal table:
 - Tag MAC address
 - AP MAC address
 - AP interface
 - Received-signal-strength-indication (RSSI) measurement

- The location appliance periodically polls the WLC for the contents of both asset tag tables using SNMP.
- The location appliance calculates the location of the asset tag using the RSSI information and stores the location information in its database.
- The location server dispatches any asynchronous notification events based on the updated asset tag location to configured notification recipients.
- Location end users make use of WCS (or third-party location clients such as PanGo Locator) to request location information based on floor maps or search criteria. A request for location information is made from the location client to the location server via a SOAP/XML online query.

WCS and the location appliance exchange information such as maps and network designs during a process known as *synchronization*. During a *network design synchronization* between WCS and the location appliance, design and calibration information is exchanged and updated.

Location clients such as the PanGo PanOS Server also synchronize with the location appliance. In this case, the location appliance updates location clients with the latest information regarding network designs and map images.

Location Clients and the SOAP/XML API

To facilitate the deployment of location-enabled applications in the enterprise, the Cisco Wireless Location Appliance is equipped with a SOAP/XML applications programming interface (API). Applications can make use of the location information contained within the location appliance by importing components via the API such as building and floor maps, access point locations, coverage areas, and device lists. Rich and actionable data such as recent or historical location and device statistics can also be imported. Location-based alarms and notifications can be triggered in applications through area boundary definitions, allowed areas, and distances.

These capabilities allow the SOAP/XML API to be used for integration with external location-aware software applications such as E-911 applications, asset management, enterprise-resource-planning (ERP) tools, and workflow automation systems.

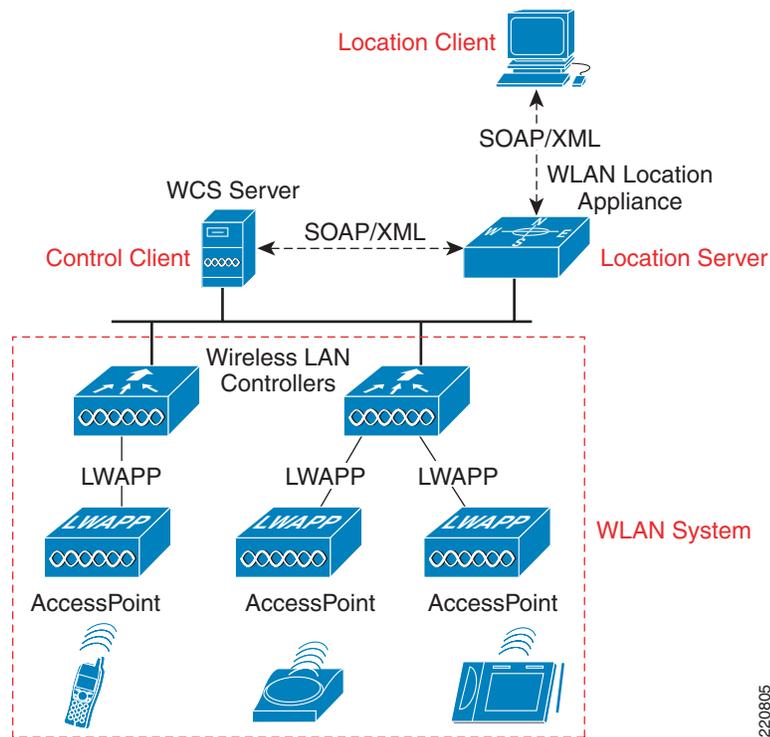


Note

Cisco makes the location appliance API available to the Cisco development community along with the tools to facilitate solution development. Integration support is available via the Cisco Developer Services Program. For complete details, see the following URL: <http://www.cisco.com/go/developersupport>.

The use of this SOAP/XML API to interface a CTDP location client to a location-enabled Cisco UWN can be seen in [Figure 3](#).

Figure 3 Cisco UWN with CTD Location Client



The overall solution consists of the following four basic components.

- **Location client**—The primary role of the location client is to serve as the interface to the location and asset information contained on the location server. Location clients may receive information on a request basis (“pull” mode), or they may assume a listening role awaiting regular transmissions of location data from the location server based on pre-defined criteria (“push” mode). This information may include device location coordinates, updated network designs, and maps from the location server.

In some cases, WCS can serve as the primary location client, which is typically seen in IT-centric deployments.

- **Control client**—The control client is capable of administering the location server as well as reading/writing location data to the location server databases. In the Cisco location-aware UWN, the role of control client is undertaken by the Cisco WCS. The primary role of the control client is to populate the server with information about the physical environment (network designs, floors maps, calibration models, access point locations, and so on) and the network elements that should be monitored. The control client may also have management capabilities over one or more of the location servers deployed in the network. In some implementations, the control and location clients may be combined in a single physical or logical entity.
- **Location server**—The location server provides general location services for the Cisco UWN and is responsible for running the algorithms that predict device location. Multiple location servers can be deployed within a single network mobility group. A location server can communicate with multiple location or control clients. In the Cisco LBS solution, the Cisco Wireless Location Appliance fulfills the role of the location server. The Cisco Location Appliance is also responsible for the archival of historical location records and is also capable of issuing notifications to external systems via e-mail (SMTP), syslog, SNMP traps, or the SOAP/XML protocol.
- **Wireless LAN System**—The wireless LAN system is comprised of the following:

- Embedded software contained within WLAN controllers that functions as an aggregation point for information regarding station/tag/rogue discovery, device tracking, and statistics
- All the mobile devices (tags, mobile stations, rogue clients, and rogue access points) that interact with the wireless network and whose location the location-aware Cisco UWN and its location servers monitor

Active RFID Tags

The most common type of RFID tag used with Real-Time Location Systems (RTLS) is the *active RFID tag*, which is a self-contained battery-powered long range signaling device. Active RFID tags typically transmit (or *beacon*) information about themselves to receivers on a timed basis or after the detection of a state change (such as the detection or cessation of motion or proximity, for example).

Active tags are typically used in real-time tracking of high-value assets in *closed-loop* systems (that is, systems in which the tags are not intended to permanently exit the control of the tag owner or originator). The relatively higher cost of assets tracked with active RFID tags usually justifies the higher cost of the active tag itself and presents strong motivation for tag re-use. Medical equipment, electronic test gear, computer equipment, re-usable containers, and assembly line materials-in-process are all excellent examples of applications for active tag technology. Active RFID tags can provide tracking in terms of *presence* (positive or negative indication of whether an asset is present in a particular area) or *real-time location* within large areas.

Active RFID tags are typically found operating in a wide variety of radio frequencies with read ranges that range out to as far as 300 feet. A distinguishing feature of active RFID tag technology is a very high read reliability rate. This is primarily because of the higher transmitter output, optimized antenna, and reliable power source of the active RFID tag.

Of the various subcategories of active RFID tags that exist in the marketplace today, those of particular interest to the design described in this document are known as *802.11* or *Wi-Fi active RFID tags*. This document focuses on the PanGo v2 Wi-Fi 802.11 active RFID tag, as shown in [Figure 4](#). This type of active RFID tag reliably transmits information about itself at ranges that are similar to those of well-known 802.11 wireless clients such as laptops, PDAs, and handheld phones.

Figure 4 PanGo LAN Tag v2



802.11 (Wi-Fi) active RFID tags are designed to operate in the unlicensed bands allocated for 802.11 usage by the appropriate regulatory authorities. 802.11 Wi-Fi active RFID tags available at publication encompass the 2.4 GHz band only.

802.11 Wi-Fi active RFID tags exhibit the features of active RFID tags as discussed previously, but also comply with applicable IEEE 802.11 standards and protocols. This type of active RFID tag can readily communicate with standard Wi-Fi infrastructure hardware without any special hardware or firmware modifications, and can co-exist alongside other Wi-Fi devices such as laptop clients, PDAs, and handheld Wi-Fi voice clients.

Beaconing active RFID tags are used in many RTLS implementations and are typically relied on when the location of an asset needs to be dependably determined across a large area. With a beaconing active RFID tag, a short message payload known as a “beacon” is emitted at programmed intervals along with the unique identifier of the RFID tag. This interval is pre-programmed into the tag and can be set depending on the degree of criticality associated with providing tag location updates. For example, the beaconing interval could be set for as short as every minute or as long as twice a day or more. In practice, the price paid for increased beaconing frequency is a reduction in tag battery life along with an increase in RF network traffic.

A variation of the beaconing design may include *motion-sensitive triggering*, which causes the RFID tag to change its beacon rate depending on whether the tag senses it has entered a motion state. Thus, an active RFID tag in a stationary state may beacon at a very slow rate to extend its battery life, whereas that same tag when in motion may begin beaconing much more rapidly, providing more frequent updates of its location when moving.


Note

For more information regarding the Cisco location-aware UWN architecture and RFID technologies, see *Wi-Fi Location-Based Services 4.1 Design Guide* at the following URL:
<http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html>.

PanGo PanOS Server and PanGo Locator

The location client from PanGo Networks is commonly referred to as *PanGo Locator*, but it actually is comprised of two important and distinct components: the *PanGo PanOS Server* and a powerful collection of *web-enabled location applications*. These components interface to the location information contained within the Cisco UWN via the location appliance SOAP/XML API, as is illustrated in [Figure 8](#).

The remainder of this section briefly describes the roles and functions of each component of the PanGo location client.

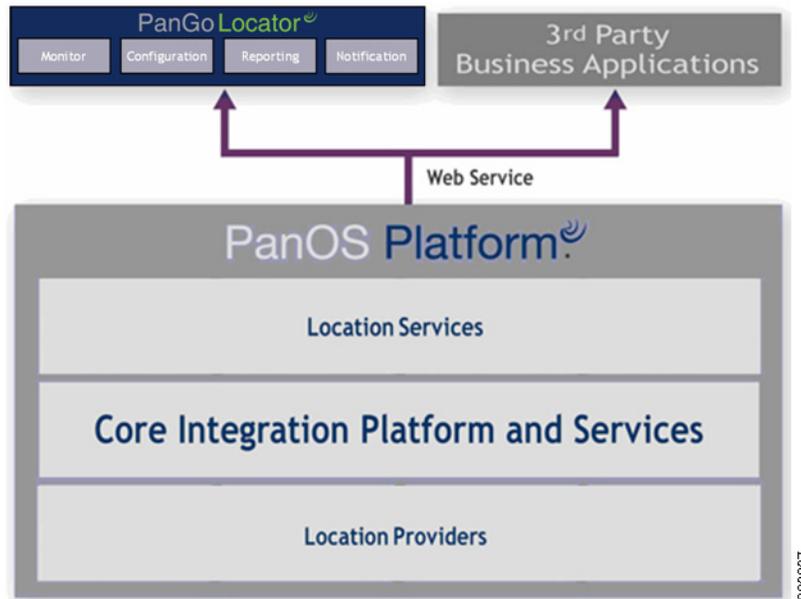
PanGo PanOS Server

PanGo PanOS Server version 4 is a location management platform for enabling, managing, and integrating location and related device mobility information. Designed and built around a service-oriented architecture (SOA), the PanGo PanOS Server consists of location source providers, a core integration platform, and a rich set of location services functions for building and deploying location-aware applications. PanGo PanOS Server is installed as a service on Microsoft Windows Server 2003 and adheres to a standards-based approach that is interoperable with common technology standards such as J2EE, Microsoft .NET, XML, and HTTP web services.

PanGo PanOS Server version 4.5 manages the identification and location of assets, and facilitates integration of that information into enterprise IT systems and applications. The PanGo PanOS Server provides important location-based intelligence such as where an asset is currently located, where it has been, how long it has been there, and what other assets are within its vicinity.

[Figure 5](#) illustrates the three key components of the PanGo PanOS Server and their relationship to PanGo Locator.

Figure 5 PanGo Locator and PanGo PanOS Server



Following is a description of these three components:

- *Location Providers*—This functionality within the PanOS server allows the PanGo location client to accept location data from a wide variety of sources, including the Cisco 2710 Wireless Location Appliance via its SOAP/XML API.

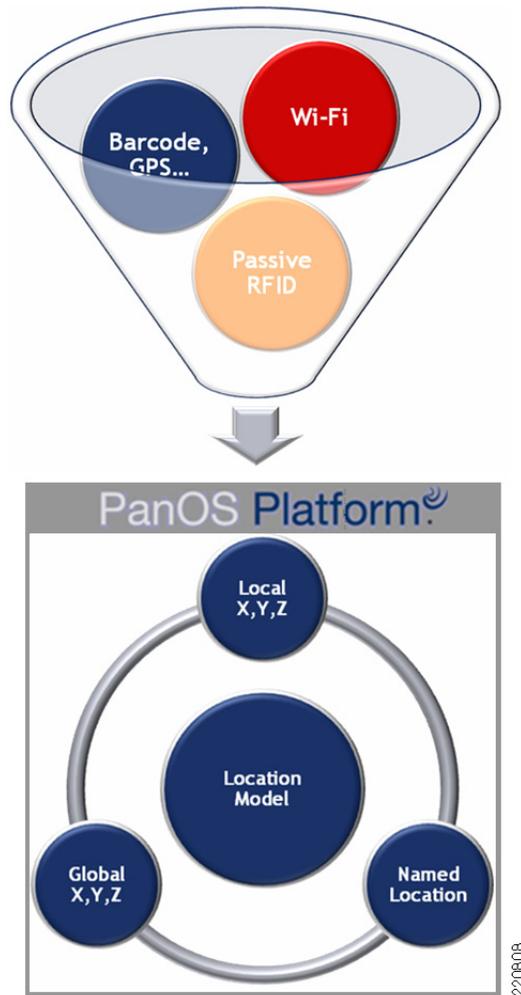
Although the focus of this paper is on the interaction of PanOS with the Wi-Fi localization capabilities provided by the Cisco location appliance, PanOS can also provide asset location services based on passive RFID, barcode, and GPS location providers. PanOS can process location input from other providers in a complementary fashion to the location information received from the Cisco Location Appliance (as shown in [Figure 6](#)).



Note

A discussion of the location client capabilities available from PanGo Networks using non-Wi-Fi-based technologies is outside the scope of this document. For more information about these capabilities, contact your PanGo representative.

Figure 6 PanOS Multiple Location Provider Input

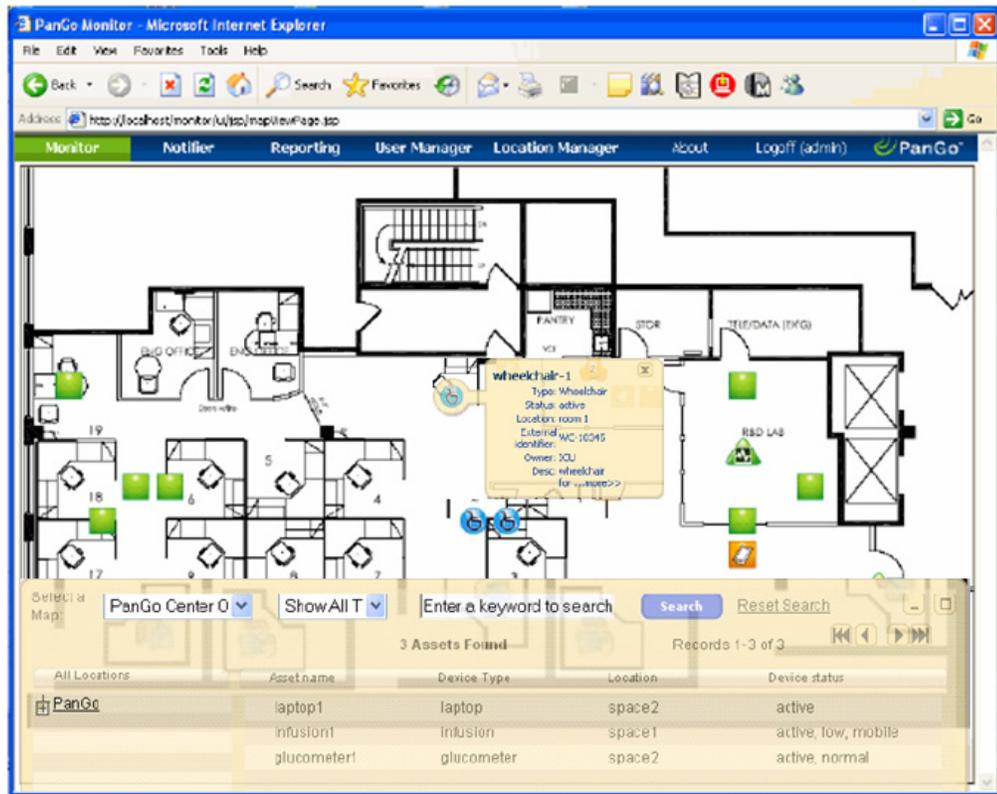


- *Core Integration and Services Platform*—Enables enterprise scalability and provides an open, standards-based integration environment. Web service-based design ensures interoperability with standard servers, operating systems, and underlying protocols.
- *Location Services Functions*—Examples include space and zone management, tag/device management, location information access, and rule-based notifications that facilitate the integration of end-user and third-party developed applications such as those from McKesson, Emergin, Four Rivers Software Systems, and Tele-Tracking Technologies.

PanGo Locator Web Applications

The PanGo Locator suite of web-based applications provides the user interface to information contained within the Cisco Location Appliance and made accessible via the PanGo PanOS Server, as shown in [Figure 7](#).

Figure 7 PanGo Locator 4.5



PanGo Locator applications are accessed via industry-standard web browsers (see the *PanGo Locator User's Guide* for a current listing of supported web browsers).

Among many other functions, PanGo Locator makes possible the display of location coordinates and other metadata received from the location appliance. PanGo Locator and the PanOS Server operate as a closely knit entity, harnessing the power of the Cisco location appliance and its SOAP/XML API to accurately track assets in the enterprise environment.

PanGo Locator contains the following five modular web-based application components (shown in Figure 7):

- PanGo Locator Monitor—Provides asset location tracking and motion detection, including the following:
 - Detailed floor and zone level “zoom-to-fit” view of asset location
 - Asset search and filtering based on asset class, location, and other criteria
 - Detailed asset data (including time in location)
- PanGo Locator Reporting—Generates reports on asset location, movement, and tag condition, including detailed asset reports such as the following:
 - Filtered asset and location reports using customizable criteria (asset class, type, location, and so on)
 - Asset state reporting (location, motion, low battery and other states).
- PanGo Locator Notifier—Generates automatic e-mail notifications regarding system events, such as context-sensitive, rules-based notifications triggered by the following:
 - Tag status warnings—Low battery, device motion, tag shutdown

- Asset location—Entering a prohibited area, exiting a containment zone
- Location duration—In location beyond a permitted time interval
- PanGo Locator User Manager—Allows management of Locator access via the creation of users and groups, with the assignment of various privileges to each
- PanGo Locator Location Manager—Manages the physical location hierarchy used by the other Locator applications

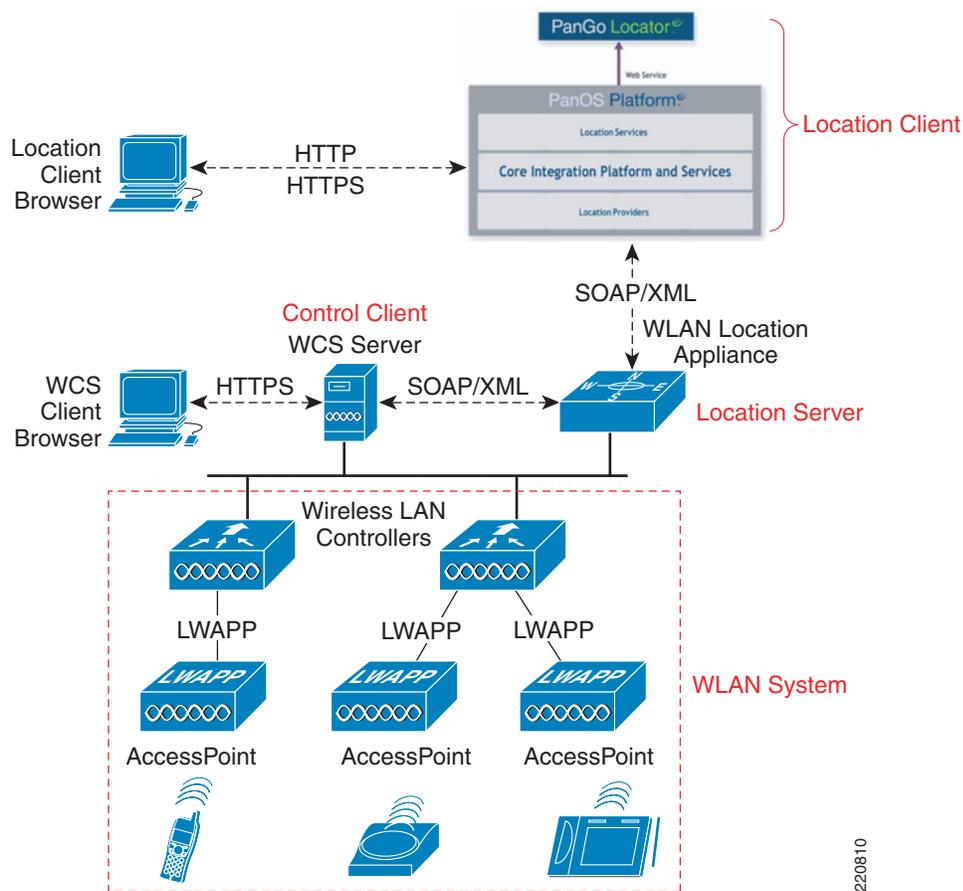
PanGo Locator also includes the PanGo Locator Configuration utility, a Java-based client application that is installed on a workstation and used to configure the assets and tags used with the system.

Some of the functionality provided by PanGo Locator Configuration includes the following:

- Defining assets, asset type categories, and asset owners
- Associating tags with assets and recording descriptive data (serial numbers and so on)
- Defining asset tag configuration profiles (channels, beacon rates, server IP addresses, and so on)

The user interface presented by PanGo Locator is primarily designed for business asset owners and users whose main goal is to locate the assets they need quickly and efficiently. Figure 8 shows the integration of PanGo PanOS Server and Locator into the Cisco Unified Wireless Network.

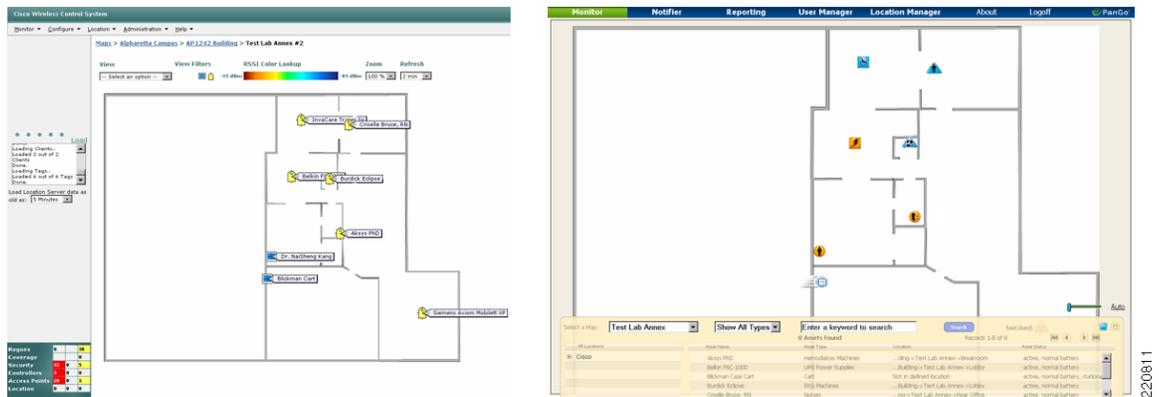
Figure 8 Integrated Cisco/PanGo Solution



PanGo Locator and Cisco WCS

As has just been described, both the Cisco WCS as well as PanGo Locator make use of the SOAP/XML API when interfacing to the location appliance. PanGo Locator and Cisco WCS co-exist in the integrated Cisco/PanGo solution, with WCS having the capability to act as both a location as well as a control client to the Cisco Wireless Location Appliance, as indicated in [Figure 8](#). Cisco WCS is a standard part of most enterprise deployments and is required to define network designs and manage the Cisco Wireless Location Appliance. Although both products have location client capabilities, there are distinct differences in the user interfaces and presentation approaches that serve to better align each product with different audiences. This can be seen in [Figure 9](#), which shows two different views of the same set of tracked assets on the same floor from both the Monitor Maps panel of Cisco WCS and the Monitor web application of PanGo Locator.

Figure 9 Cisco WCS and PanGo Locator Floor Map Views



For example, in [Figure 9](#) you see that WCS displays tracked assets on floor maps by using one of two icons. WCS uses the blue rectangle icon  for tracked assets that probe or associate to the WLAN infrastructure, and the yellow tag icon  for tracked assets that communicate via Layer 2 multicasts only.

In contrast, PanGo Locator uses over 30 categories of asset icons, each of which is available in three shapes (circular, rectangular, and triangular) and three colors (blue, green, and orange) for a total of over 270 asset icons. PanGo Locator also provides another suite of icons that are used when PanGo LAN tags in RSSI mode are in motion, thereby increasing the overall number of icons available to 540.

WCS is closely aligned with the needs of the IT network professional concerned with the management of the individual components that comprise the network, their current state of operation, network access security, and the capability of the network to meet the current and future needs of the business. These individuals desire to be made aware not only of the presence of authorized WLAN clients, access points, and asset tags but of unauthorized entities as well (that is, rogue clients or rogue access points). WCS provides such users with an excellent “top-down” view of the wireless network and allows the various networks to be easily managed. As a location client, WCS provides the IT user with display and reporting capabilities that allow for the identification of authorized as well as rogue wireless devices in the network. WCS reporting criteria allow for tags and clients to be found in the location databases based on device MAC address or asset name, category, group name, controller, location appliance, or floor map.

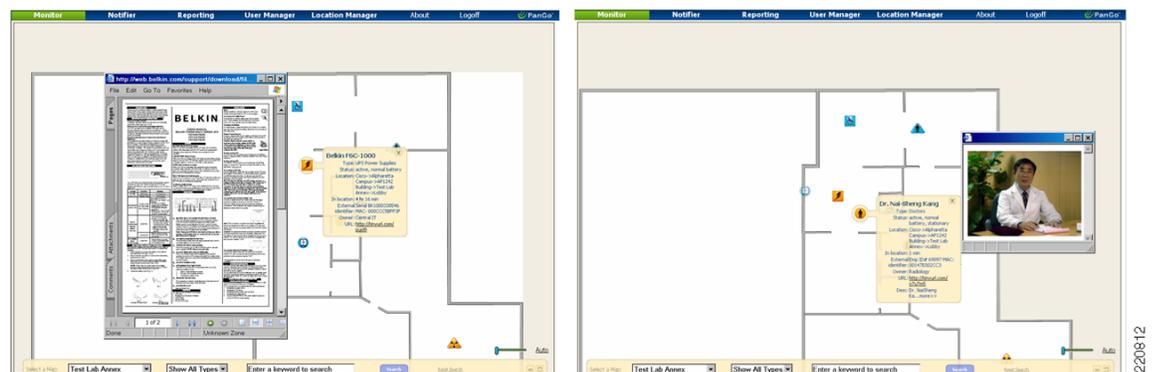
Conversely, asset users and business operations professionals tend to be much more concerned with using tools such as asset tracking to operate their business more effectively, and much less about the behind-the-scenes technical details. For example, in contrast to the IT network professional, a medical

technician at a hospital radiology unit might be much more concerned about knowing the location of a particular X-ray machine (and its manufacturer, model, and perhaps its serial number to verify its service and maintenance record), and not concerned about the type of RFID asset tag attached to it or its MAC address. In most cases, asset owners and users want a system that makes it simple to quickly locate the assets they need and to match those assets with the people that need them, leaving other tasks such as the tracking of rogue clients, access points, or location tracking system configuration to their IT support personnel or network security team.

PanGo Locator was primarily designed to address the needs of business users desiring to manage assets, not asset tags. PanGo Locator is designed to be an asset management tool, so much so that an asset tag in PanGo Locator that is not assigned to an asset is not able to be tracked in the application. Some of the differentiating features provided by PanGo Locator specifically intended to provide enhanced asset visibility include the following:

- The display of asset location via a floor plan or table view (shown in [Figure 7](#)). This includes the capability to define real-world spaces comprised of multiple individual space elements. An example of this is an intensive care unit (ICU) consisting of six separately defined sub-areas.
- Industry-specific asset icons (healthcare, warehousing, and so on) representing both stationary and movement states.
- Very flexible and detailed reporting capabilities that include the ability to create reusable historical and current reports that include location-based or status-based events.
- Sophisticated asset search capabilities including a web service interface to allow tags to be easily linked with assets and then interfaced to external asset information sources. This interface can be used to link each asset to their entry in an asset maintenance management system (that is, to track the calibration status of a critical piece of measurement equipment), or to simply refer the user to a source of more in-depth information regarding the asset, as shown in [Figure 10](#).

Figure 10 External Web Application Linking



The use of PanGo Locator in combination with Cisco WCS in the location-aware Cisco UWN allows enterprise users with differing needs to use the same common bank of location data via presentation portals that best fit their requirements. Users requiring the integration of location data with the supporting details of their managed assets can find these capabilities and much more available when augmenting the control client and management capabilities of Cisco WCS with the PanGo location client.

PanGo Active RFID LAN Tags v2

**Note**

For the latest datasheet on the PanGo version 2 Locator LAN asset tag, see http://www.pangonetworks.com/documents/Active_RFID_Tag_DataSheet.pdf or contact PanGo Networks directly.

Overview

PanGo v2 LAN Tags are intelligent 802.11-based active RFID devices that can communicate with the Cisco UWN using either Layer 2 or Layer 3 protocols. These active RFID asset tags have a footprint of 2.6" x 1.7" x 0.9" and weigh 2.5 ounces, allowing them to be affixed to a wide variety of asset types, including medical devices, manufacturing equipment, IT equipment, containers, vehicles, and carts. These motion-sensitive asset tags are powered by a set of three 1.5 volt disposable lithium batteries encased in thermoplastic wrap.

**Note**

As this document went to publication, PanGo Networks announced the availability of their third generation of PanGo LAN Tags, known as the PanGo v3 LAN Tag. Significant improvements in the v3 asset tag are reported to include dramatically improved battery life, smaller size (2.5" x 1.7" x 0.7"), external alert button and asset detachment detection.

Assembly

The PanGo v2 asset tag is broken down into the following six physical components (shown in [Figure 11](#)):

- Printed circuit board (PCB)
- Battery pack
- Tag enclosure
- Neoprene gasketed end cap
- Neoprene gasketed machine screws (2)

Figure 11 PanGo LAN Tag Assemblies

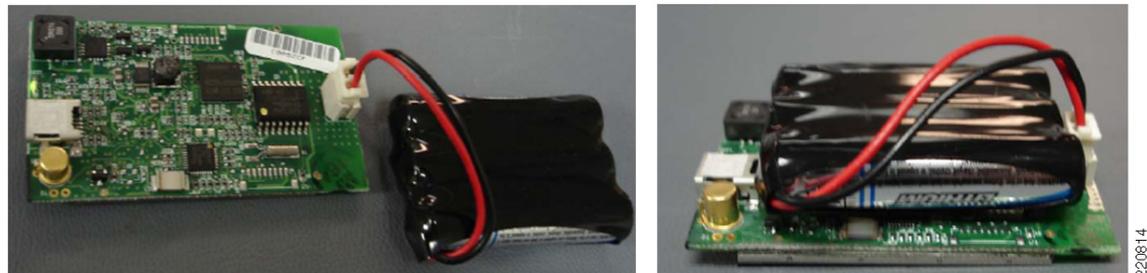


Note

When disassembling PanGo tags, take particular care to keep tag PCBs and tag enclosures together. The MAC address programmed into the tag is marked on the sealed end of the enclosure but not on the PCB. Inadvertent confusion of tag PCBs and enclosures can result in assembled tags with incorrectly labeled MAC addresses.

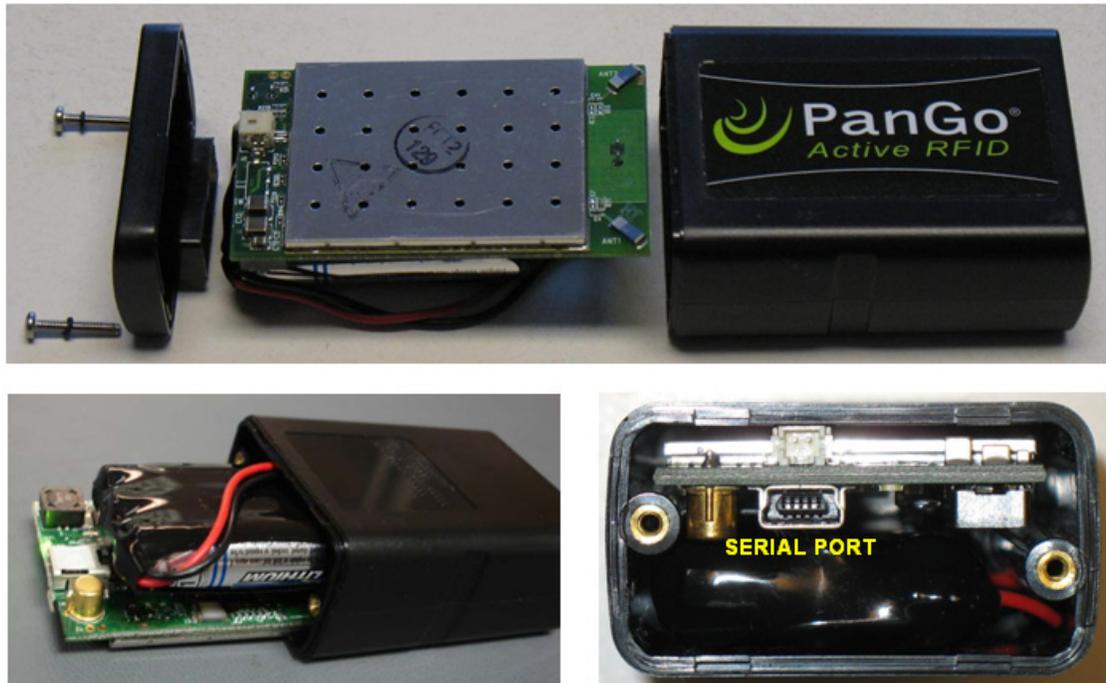
The white polarized connector on the battery power cable should be connected to its mating receptacle on the PCB, as shown in [Figure 12](#). The PCB and the battery pack should then be properly oriented and placed into the tag enclosure to avoid undue stress on the power connector. Note that the enclosure is compartmentalized into two sections by an interior molded divider.

Figure 12 Proper Tag/Battery Orientation



The PCB should be inserted into the smaller of the two enclosure compartments, power connector first, as shown in [Figure 13](#).

Figure 13 Proper Orientation of PCB and Battery Pack



When the PCB is oriented in this manner, the shielded RF enclosure and the diversity antennas of the tag are placed directly underneath the “PanGo Active RFID” tag casing label (as shown in [Figure 13](#)). As seen in this figure, when the PCB is properly oriented, the serial port is accessible from the open end of the tag case.

The PCB protrudes from the tag case by approximately 1/4”, as shown in [Figure 14](#). This is a normal condition; do not attempt to force the PCB deeper into the case. Note the proper orientation of the end cap prior to assembly.

Figure 14 Assembled Tag, Battery, and Case Side View



Note

Further information regarding the correct assembly of the PanGo asset tag v2 can be found in the document entitled *PanGo Version 2 Tag Battery Installation Guide*, available on request from your PanGo representative.

Tag Operation

PanGo v2 asset tags use a single chip 802.11bg radio capable of delivering up to +19 dBm of transmitter output power. The tag uses miniature board-mounted diversity antennas that are located in the corners of the tag PCB adjacent to the shielded RF enclosure, directly below the white power connector, as shown by the red circles in [Figure 15](#).

Figure 15 PanGo v2 Asset Tag Internal PCB (Top and Bottom)



The detection of motion allows the PanGo v2 asset tag to change its transmission behavior as it transitions from the stationary state to the mobile state. As the asset and the attached tag come to rest, the tag modifies its behavior once again as it transitions from the mobile state back to the stationary state. Transmission behavior is controlled via individual reporting interval properties that are specified in the tag configuration profiles in the PanGo Locator Configuration utility.

PanGo asset tags are capable of sending a full complement of alert messages regarding their internal condition, such as battery status. These alerts are recognized and displayed by PanGo Locator on maps, reports, and in e-mail notifications. PanGo v2 asset tags are configured via the PanGo Locator Configuration software utility or the tag serial port. As of the publication of this document, PanGo v2 asset tags support either open or secured communication using 64- or 128-bit static WEP keys only. Other authentication and encryption methods (such as 802.1x authentication and Wi-Fi Protected Access (WPA or WPA2)) are not supported by the v2 asset tag.

Tag Initialization

Before newly acquired PanGo tags can join the Cisco UWN, they must be configured with basic parameters such as SSID, WEP keys, and other settings. Tags are capable of receiving such information over-the-air (OTA) from an initialization server using an LWAPP initialization WLAN or a temporary stand-alone (formerly referred to as autonomous) access point configured to match the factory default settings of the tag. After asset tags are initially configured, further use of this factory-default configured LWAPP WLAN or stand-alone access point is not required. Initialized tags periodically receive updates from the PanGo PanOS Server via their normal communication channels.

A detailed description of the steps necessary to initialize newly acquired or factory-defaulted tags can be found in Chapter 4 of the *PanGo Administration Guide*. This document is included on the PanGo Locator Installation CD and is available from your PanGo representative. Best practice recommendations regarding the use of the initialization WLAN can be found in [Planning for Tag Initialization, page 35](#). The remainder of this section discusses operational details intended to provide a thorough understanding of what occurs during the two-stage tag initialization process.

Theory of Operation

In the first stage of the tag initialization process, newly acquired PanGo asset tags initially associate to an LWAPP WLAN or a temporary stand-alone access point that has been configured with the PanGo factory-default SSID of “PanG0pgtp” and 104-bit WEP key of *0x503935396372666D614D425253* or ASCII “P959crfmaMBRS”. When the tag associates, it obtains its IP information via DHCP and immediately begins listening for a special UDP broadcast emanating from the PanGo Tracking Protocol (PGTP) Broadcaster utility.

The PGTP Broadcaster (shown in [Figure 16](#)) is a command line utility that transmits a 194-byte frame containing a UDP broadcast to port 1177 (default) approximately every 5 seconds. As described in Chapter 4 of the *PanGo Administration Guide*, the PGTP Broadcaster can be run on the production PanGo PanOS Server or a standalone “beaconing” PanGo PanOS Server. For further information, see [Planning for Tag Initialization](#), page 35.

Figure 16 PanGo PGTP Broadcaster

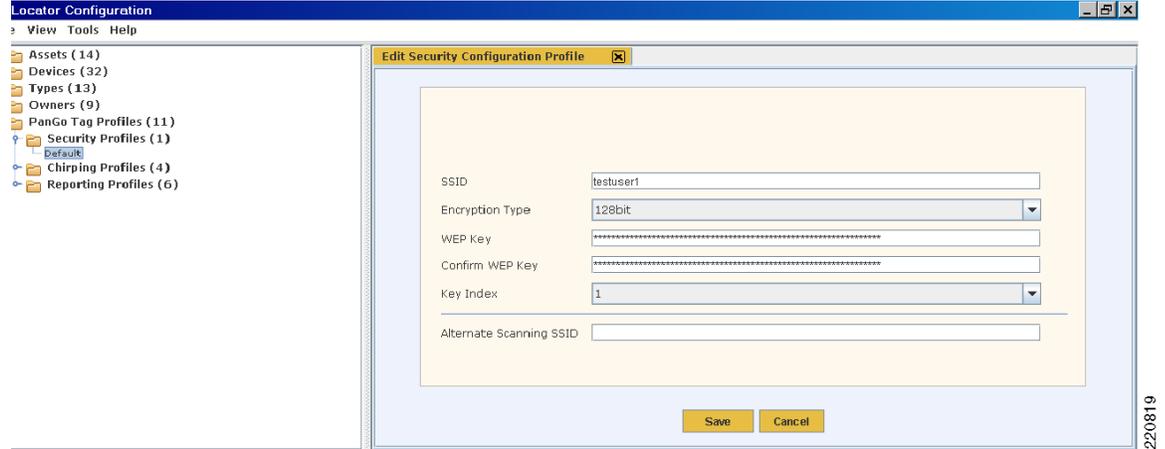
```

c:\ PGTP Broadcaster
Beacon version: 2
Broadcaster configuration source: Reporting profile = Default, Security Profile
= Default
Beacon interval (seconds): 5
Beacon address: 10.1.59.255
Beacon port: 1177
Broadcast server address: 10.1.56.33
Broadcast server port: 1177
Attempting to detect another broadcaster...
No broadcaster detected.
Process running, press CTRL-C to terminate.
2:20:18
  
```

The UDP broadcast frames sent by the PGTP Broadcaster contain basic information from the default security and reporting profiles. Site-specific SSID and WEP key information contained in the UDP payload is encrypted using the TwoFish block cipher.

In the second stage of tag initialization, asset tags use the information acquired in the first stage to establish a new association using the SSID defined in the default security profile (as seen in [Figure 17](#); note that SSID here is *not* “PanG0pgtp”). After associating using this SSID for the first time, the asset tags contact the PanGo PanOS Server and receive the complete default reporting profile.

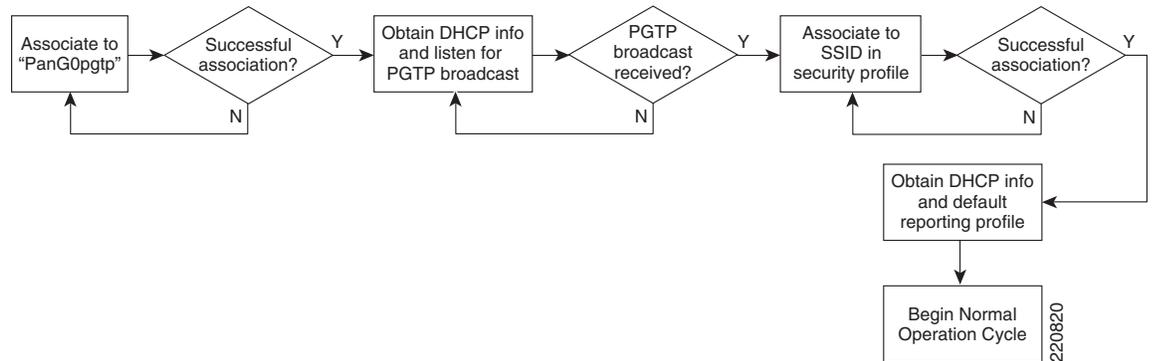
Figure 17 Default Security Profile Definition



After all asset tags have received their configuration information, the PGTP Broadcaster utility and the LWAPP WLAN (or the temporary stand-alone access point) used for initialization are no longer necessary. To help ensure overall security, the broadcaster utility should be closed and the LWAPP WLAN or stand-alone access point should be disabled or removed.

The initialization process is summarized by the flowchart shown in [Figure 18](#).

Figure 18 PanGo Tag Initialization Process



A frame analysis that includes both stages of initialization can be seen in [Figure 19](#). Stage one is shown within the red rectangle and stage two within the blue rectangle.

Figure 19 PanGo Tag Initialization Frame Analysis

Packet	Source	Destination	Protocol	Size	Summary
1	00:14:7E:00:2C:2C	Ethernet Broadcast	802.11 Probe Req	52	FC=.....,SM= 0, FN= 0,SSID=PanG0pgtp
2	00:14:1B:59:3F:41	00:14:7E:00:2C:2C	802.11 Probe Rsp	111	FC=.....,SM=3347, FN= 0,BI=100,SSID=PanG0pgtp,DS=11
3	00:14:7E:00:2C:2C	00:14:1B:59:3F:41	802.11 Probe Req	52	FC=.....,SM= 0, FN= 0,SSID=PanG0pgtp
4	00:14:1B:59:3F:41	00:14:7E:00:2C:2C	802.11 Probe Rsp	111	FC=.....,SM=3350, FN= 0,BI=100,SSID=PanG0pgtp,DS=11
5	00:14:7E:00:2C:2C	00:14:1B:59:3F:41	802.11 Auth	34	FC=.....,SM= 1, FN= 0,Algorith=0 (Open System),ATSN=1,S...
6	00:14:1B:59:3F:41	00:14:7E:00:2C:2C	802.11 Auth	34	FC=.....,SM=3351, FN= 0,Algorith=0 (Open System),ATSN=2,S...
7	00:14:7E:00:2C:2C	00:14:1B:59:3F:41	802.11 Assoc Req	56	FC=.....,SM= 2, FN= 0, Listen=0,SSID=PanG0pgtp
8	00:14:1B:59:3F:41	00:14:7E:00:2C:2C	802.11 Assoc Rsp	50	FC=.....,SM=3352, FN= 0, Status=0,AID=1
9	IP-0.0.0.0	IP Broadcast	DHCP	316	C DISCOVER
10	IP-1.1.1.1	IP-10.1.59.248	DHCP	368	R OFFER 10.1.59.248
11	00:14:7E:00:2C:2C	Ethernet Broadcast	ARP Request	64	10.1.59.248 = ?
12	IP-0.0.0.0	IP Broadcast	DHCP	328	C REQUEST 10.1.59.248
13	IP-1.1.1.1	IP-10.1.59.248	DHCP	368	R ACK
14	00:14:7E:00:2C:2C	Ethernet Broadcast	ARP Request	64	10.1.59.248 = ?
15	IP-10.1.56.33	IP-10.1.59.255	UDP	194	Src= 1660,Dst= 1177, L= 130
16	00:14:7E:00:2C:2C	Ethernet Broadcast	802.11 Probe Req	52	FC=.....,SM= 0, FN= 0,SSID=testuser1
17	00:14:1B:59:3F:42	00:14:7E:00:2C:2C	802.11 Probe Rsp	143	FC=.....,SM= 210, FN= 0,BI=100,SSID=testuser1,DS=11
18	00:14:7E:00:2C:2C	00:14:1B:59:3F:42	802.11 Probe Req	52	FC=.....,SM= 0, FN= 0,SSID=testuser1
19	00:14:1B:59:3F:42	00:14:7E:00:2C:2C	802.11 Probe Rsp	143	FC=.....,SM= 212, FN= 0,BI=100,SSID=testuser1,DS=11
20	00:14:7E:00:2C:2C	00:14:1B:59:3F:42	802.11 Auth	34	FC=.....,SM= 1, FN= 0,Algorith=0 (Open System),ATSN=1,S...
21	00:14:1B:59:3F:42	00:14:7E:00:2C:2C	802.11 Auth	34	FC=.....,SM= 213, FN= 0,Algorith=0 (Open System),ATSN=2,S...
22	00:14:7E:00:2C:2C	00:14:1B:59:3F:42	802.11 Assoc Req	56	FC=.....,SM= 2, FN= 0, Listen=0,SSID=testuser1
23	00:14:1B:59:3F:42	00:14:7E:00:2C:2C	802.11 Assoc Rsp	50	FC=.....,SM= 215, FN= 0, Status=0,AID=1
24	IP-0.0.0.0	IP Broadcast	DHCP	316	C DISCOVER
25	IP-1.1.1.1	IP-10.1.59.248	DHCP	368	R OFFER 10.1.59.248
26	00:14:7E:00:2C:2C	Ethernet Broadcast	ARP Request	64	10.1.59.248 = ?
27	IP-0.0.0.0	IP Broadcast	DHCP	328	C REQUEST 10.1.59.248
28	IP-1.1.1.1	IP-10.1.59.248	DHCP	368	R ACK
29	00:14:7E:00:2C:2C	Ethernet Broadcast	ARP Request	64	10.1.59.248 = ?
30	00:14:7E:00:2C:2C	Ethernet Broadcast	ARP Request	64	10.1.56.33 = ?
31	IP-10.1.59.248	IP-10.1.56.33	TCP	96	Src= 1024,Dst= 1177,....S.
32	IP-10.1.56.33	IP-10.1.59.248	TCP	96	Src= 1177,Dst= 1024,.A.S.
33	IP-10.1.59.248	IP-10.1.56.33	TCP	106	Src= 1024,Dst= 1177,.AP...
34	IP-10.1.56.33	IP-10.1.59.248	TCP	267	Src= 1177,Dst= 1024,.AP...
35	IP-10.1.59.248	IP-10.1.56.33	TCP	88	Src= 1024,Dst= 1177,.A....
36	IP-10.1.59.248	IP-10.1.56.33	TCP	108	Src= 1024,Dst= 1177,.AP...
37	IP-10.1.56.33	IP-10.1.59.248	TCP	215	Src= 1177,Dst= 1024,.AP...
38	IP-10.1.59.248	IP-10.1.56.33	TCP	108	Src= 1024,Dst= 1177,.AP...
39	IP-10.1.59.248	IP-10.1.56.33	TCP	88	Src= 1024,Dst= 1177,.A....
40	IP-10.1.56.33	IP-10.1.59.248	TCP	88	Src= 1177,Dst= 1024,.A....
41	IP-10.1.56.33	IP-10.1.59.248	TCP	88	Src= 1177,Dst= 1024,.A....
42	IP-10.1.59.248	IP-10.1.56.33	TCP	88	Src= 1024,Dst= 1177,.A....
43	IP-10.1.59.248	IP-10.1.56.33	TCP	76	Src= 1024,Dst= 1177,.A.R..
44	IP-10.1.59.248	IP-10.1.56.33	TCP	96	Src= 1025,Dst= 1177,....S.
45	IP-10.1.56.33	IP-10.1.59.248	TCP	96	Src= 1177,Dst= 1025,.A.S.
46	IP-10.1.59.248	IP-10.1.56.33	TCP	88	Src= 1025,Dst= 1177,.A....
47	IP-10.1.56.33	IP-10.1.59.248	TCP	76	Src= 1177,Dst= 1025,.A.R..

220821

In frames 1 through 8 of the first initialization stage, a tag with MAC address 00:14:7E:00:14:16 can be seen probing and associating using the factory default SSID of “PanG0pgtp”. This is followed by the DHCP assignment of an IP address in frame 9 and the reception of a UDP broadcast frame from the PGTP Broadcaster in frame 15. This UDP frame contains the TwoFish-encrypted SSID and WEP key that is used by the second stage of initialization.

Stage two of initialization consists of the remainder of the frames shown from 16 through 47. In frames 16 through 23, tag 00:14:7E:00:14:16 is once again seen probing and associating, but this time it is using the SSID that was acquired via the encrypted payload found in the UDP broadcast in frame 15. In packet 30, the tag uses the Address Resolution Protocol (ARP) to determine the Ethernet address of the PanOS server, seen here as 10.1.56.33. This value was defined in the connectivity panel of the default reporting profile when the system was originally configured. Frames 31 through 47 represent a successful TCP session between the tag and the PanGo PanOS Server. At this point, both stages of initialization have concluded and the tag begins operation as either an RSSI or chirp mode tag, as per the parameters specified in its assigned profile.

RSSI Mode

When PanGo v2 asset tags are configured to operate as Layer 3 wireless client devices (otherwise known as *RSSI mode*, *device mode*, or *reporting mode*), they communicate their location to the Cisco UWN via the use of probe requests. At each and every beacon interval, a V2 tag in RSSI mode authenticates, associates, and obtains an IP address using DHCP in an analogous fashion to other wireless LAN client devices such as PDAs and laptops.

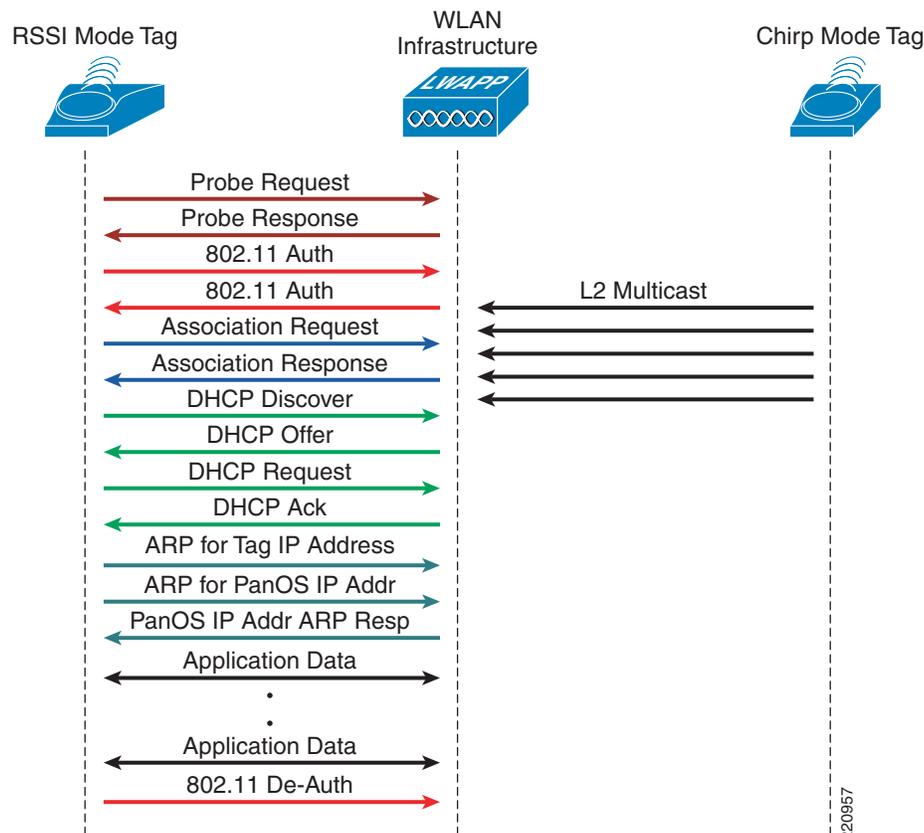
The overwhelming majority of Cisco/PanGo deployments involve *chirp mode* tags and not RSSI mode tags. However, because there are several existing Cisco UWN deployments with PanGo v2 LAN Tags configured in RSSI mode, RSSI mode is described in detail in [Appendix A—RSSI Mode Tag Operation, page 74](#).

Chirp Mode

Layer 2 (*chirp mode*) operation was first supported by PanGo in the v2 asset tag and is used in the majority of recent Cisco/PanGo asset tracking deployments. In contrast to Layer 3 RSSI mode, tags configured for chirp mode do not rely on probe requests for localization and do not associate to the Cisco UWN (except if configured to perform periodic over-the-air configuration updates). Instead, chirp mode tags transmit 34-byte Layer 2 multicast frames to uni-directionally communicate to the Cisco UWN at 1 Mbps.

A visual frame flow comparison of RSSI mode versus chirp mode operation can be seen in [Figure 20](#), which contrasts the flow of frames seen from an RSSI mode tag to a WLAN controller (shown on the left) to the flow of frames from a chirp mode tag to the same WLAN controller on the right. A more detailed comparison can be seen by examining [Figure 23](#) and [Figure 62](#). Chirp mode multicast transmissions are sent on each of the channels specified in the *chirping profiles* that were assigned to the tag using the PanGo Locator Configuration utility. Note that chirp mode tags by default send five repetitions of the multicast frame on each configured channel.

Figure 20 RSSI Mode vs. Chirp Mode Frame Flow (Single Channel)



220957

Upon expiration of the over-the-air configuration request interval set in the chirping profile (which defaults to twenty-four hours), the chirp mode tag probes the network, associates, obtains an IP address, and attempts to contact the PanGo PanOS Server to check for any configuration and firmware updates that have been queued for it. Initially, this communication with the PanOS Server is performed using the information contained in the default security reporting profiles. After the chirp mode tag associates and contacts the PanGo PanOS Server, it receives any configuration, firmware, or microcode updates including any changes made to the default security profile.

The scope of these updates can be quite extensive and can include a total re-configuration of the tag from chirp mode to RSSI mode. If a PanGo v2 asset tag in chirp mode successfully associates and obtains an IP address via DHCP, but cannot contact the PanOS Server, it remains in chirp mode and continues using its existing chirp mode configuration. It does this until the next configuration request interval, at which time it tries once again to associate and contact the PanGo PanOS Server.

A key difference to keep in mind when comparing chirp mode operation to RSSI mode operation is that RSSI mode tags always probe, authenticate, and associate to the production WLAN (shown in [Figure 20](#)) at each and every beacon interval. Chirp mode tags send only multicast frames at each beacon interval, and attempt to probe, authenticate, and associate to the production WLAN only for over-the-air updates (if enabled). Therefore, the production static WEP WLAN must always be available for RSSI mode tags to function properly. In contrast, once initialized, chirp mode tags require the static WEP production WLAN to be available only for OTA updates.

In some cases, it may be desirable or even necessary to suspend the OTA update capabilities of chirp mode tags. [Appendix D—Suspending Over-The-Air Configuration Updates, page 80](#) discusses the mechanics behind this, and [Design and Deployment Best Practices, page 31](#) describes some circumstances where this may be necessary.

The parameter that dictates how often the tag sends L2 multicasts is the “blink rate”, otherwise more commonly referred to as the beacon interval. Blink rates are entered in the reporting panel of the chirping profile, as shown in [Figure 21](#). If motion detection is enabled, different blink rates can be entered for the stationary as well as the in-motion state.

Figure 21 Chirp Mode Profile

The figure displays three screenshots of the Chirp Mode Profile configuration interface, showing the Reporting tab settings.

Top Left Screenshot: Reporting Tab (Server Information)

	Primary	Secondary
Server IP	10 . 1 . 56 . 33	10 . 1 . 56 . 33
Subnet Mask	255 . 255 . 252 . 0	255 . 255 . 252 . 0
Listening Port	1177	1177
Beacon Port	1177	1177

Top Right Screenshot: Reporting Tab (Channels)

Channels: 01 02 03 04 05 06 07 08 09 10 11

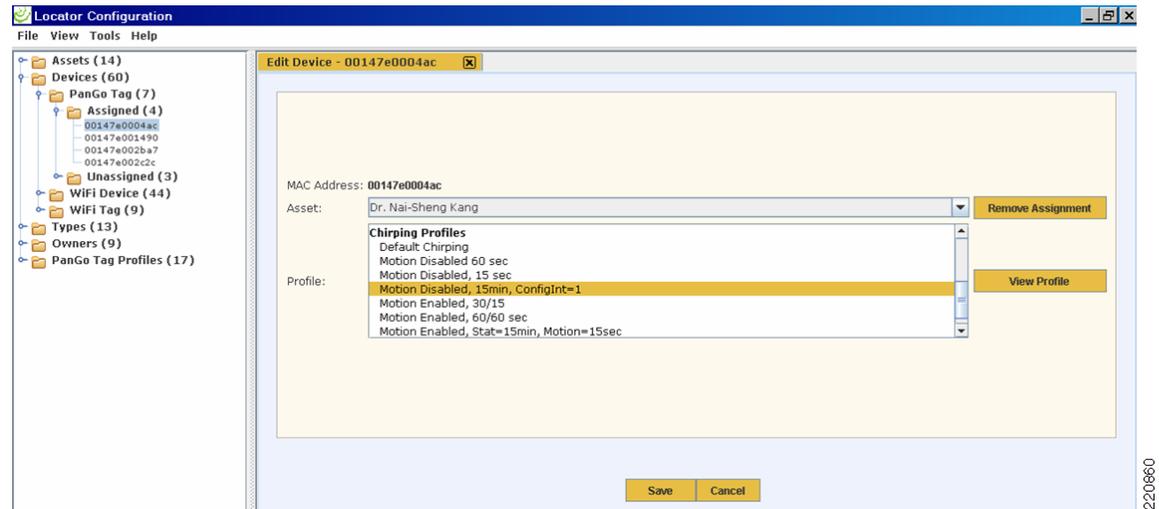
Bottom Screenshot: Reporting Tab (Blink Rates and Intervals)

Stationary Blink Rate (sec)	3600	(00:01:00:00)
Motion Enabled	<input checked="" type="checkbox"/>	
Motion Blink Rate (sec)	60	(00:00:01:00)
Motion Sensitivity	15	
Motion Detection Interval (sec)	3	(00:00:00:03)
Rest Sensitivity	15	
Rest Detection Interval (sec)	4	(00:00:00:04)
Configuration Request Interval (hrs)	1	(00:01:00:00)

220822

PanGo v2 asset tags by default are configured for RSSI mode. They are placed into chirping mode by the assignment of a chirping mode profile. This profile assignment is performed using the PanGo Locator Configuration utility. To do so, select the tag MAC address from the Devices > PanGo Tag > Assigned tree branch on the left side of the screen and place the brown screen bar across the chirping profile that you wish to assign (as shown in [Figure 22](#)).

Figure 22 Assignment of Chirping Profile using Locator Configuration



Keep in mind the following differences between chirp mode and RSSI mode when working with the PanGo Locator Configuration utility:

- Tag events—Except for battery status, PanGo v2 tags configured in chirp mode do not transmit status and event information.
- Scan count specifications (scanning panel)—Scan counts determine the number of times probe requests are generated. Asset tags in chirp mode do not rely on probe requests for localization. Therefore scan counts are notably absent from the scanning panel in chirp mode configuration profiles (only channels may be selected).
- Transmission rates (scanning panel)—Asset tags in chirp mode always transmit their multicast frames at 1 Mbps regardless of the basic or extended rates specified in access point beacons and probe responses.
- Transition state reporting (reporting panel)—Asset tags configured for chirp mode do not modify their blink rate to represent the transition period (the time at which a moving asset first stops) between the stationary and motion states.

By default, the PanGo asset tag transmits a sequence of five multicast frames on each configured channel, as shown in [Figure 23](#).

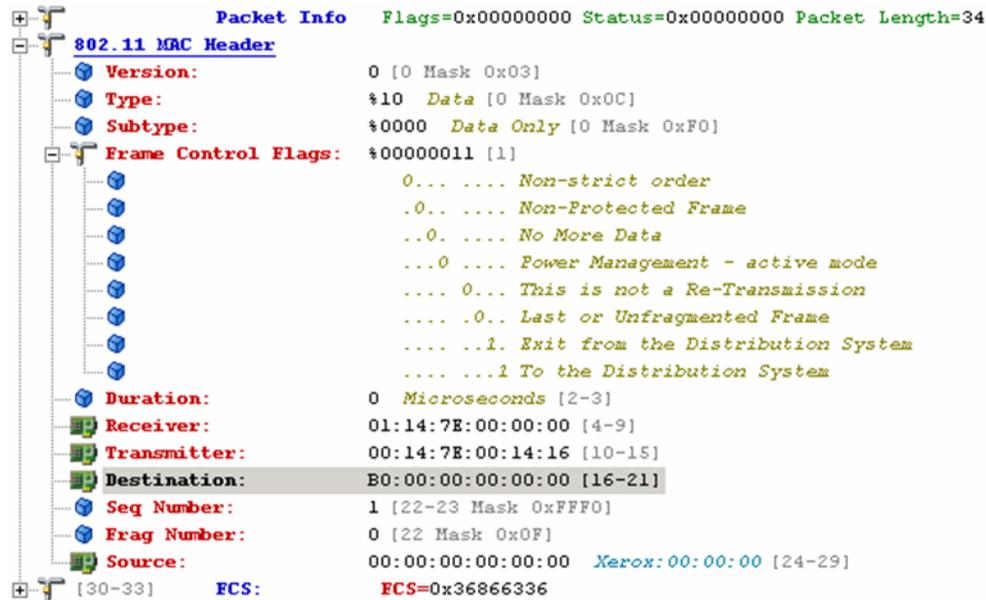
Figure 23 Chirp Mode Frames

Relative Time	Packet	Transmitter	Receiver	Protocol	Dat...	Size	Summary
0.000000	1	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	1.0	34	FC=TF.....,SN= 0,FM= 0
0.016583	2	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	1.0	34	FC=TF.....,SN= 1,FM= 0
0.033248	3	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	1.0	34	FC=TF.....,SN= 2,FM= 0
0.049902	4	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	1.0	34	FC=TF.....,SN= 3,FM= 0
0.067605	5	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	1.0	34	FC=TF.....,SN= 4,FM= 0

These multicast frames are sent using the Wireless Distribution System (WDS) four address frame format, with the To Distribution System (ToDS) and FromDS bits in the 802.11 MAC header, both set to “1”. Other fields are set as follows and shown in [Figure 24](#):

- Receiver address—Fixed multicast destination address of 01:14:7E:00:00:00.
- Transmitter address—MAC address of the asset tag.
- Destination address—Information field used for control and miscellaneous data. The first nibble of this field indicates the channel that the multicast was transmitted on (0xB=11, for example).
- Source address—Used for additional data.

Figure 24 Chirp Mode Frame Analysis (802.11)



All PanGo v2 tags configured for chirp mode use the same multicast address of 01:14:7E:00:00:00 (seen in the receiver address field). Each access point performs an LWAPP encapsulation of the frame, includes the detected RSSI/SNR, and passes this information to the registered WLAN controller via the wired infrastructure (shown in [Figure 25](#)).



Note

The LWAPP decode used by the protocol analyzer in [Figure 25](#) does not correctly interpret the signed 8-bit integers used to represent RSSI (0xCE) and SNR (0x2F). The correct decoded values in this example should be RSSI = -50dBm and SNR = 47dB.

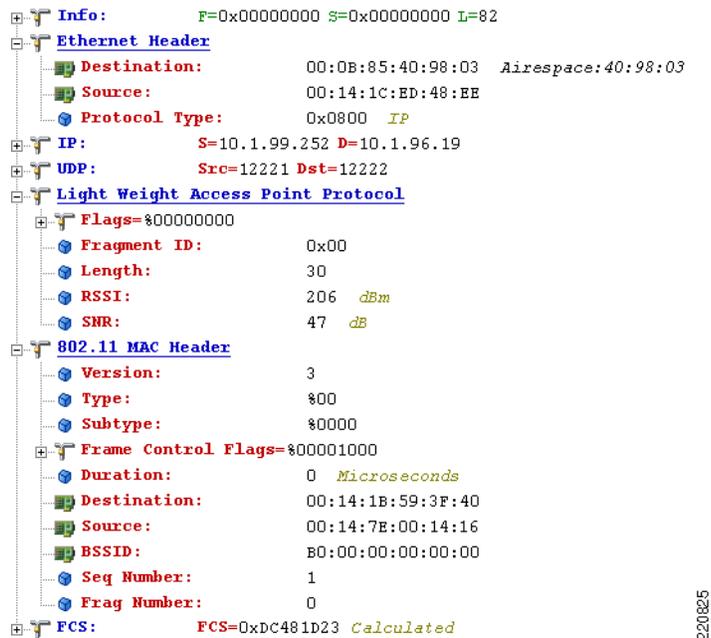
Figure 25 Chirp Mode Frame Analysis (802.3)

Figure 25 shows that the frame received from tag MAC address 00:14:7E:00:14:16 is transmitted via the wired infrastructure from the access point (00:14:1C:ED:48:EE or 10.1.99.252) to the WLAN controller (00:0B:85:40:98:03 or 10.1.96.19). The frame length at this point is 82 bytes because of the encapsulations. Note that the multicast address has been removed. The destination address in the 802.11 MAC header is now shown as the access point radio MAC address and the source address is the MAC address of the tag itself.

The content of these packets is parsed and forwarded, along with the signal strength information, from the controller to the location appliance when the location appliance polls the controller. The location appliance enters this information into its local database and uses the signal strength information in its algorithms to calculate device location. The location appliance in turn also makes available the information received in the tag frames (such as battery status) to location clients via the SOAP/XML API.

Note that the information contained in the tag multicasts is available only to location clients via the location appliance API. Applications that wish to make use of this data must be capable of interfacing to the location appliance and requesting this information using API calls (in a similar fashion to Cisco WCS and the PanGo Location Client). The WLAN controller does not forward tag multicast frames to other devices or applications.

A detailed description of the steps necessary to configure chirping profiles can be found in Chapter 4 of the *PanGo Administration Guide*, which is available on your PanGo Locator installation CD or from your PanGo representative. PanGo also has available upon request a *PanGo Version 2 Tag Quick Start Guide: Chirping Profile* document that provides the rudiments necessary to get chirping mode tags working in a Cisco environment.

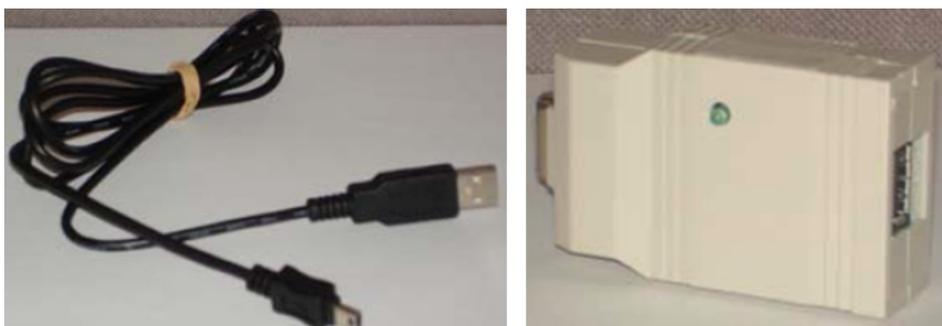
Tag Serial Interface

As mentioned earlier, configuring the PanGo v2 asset tag for use on the Cisco UWN does not mandate a physical connection to the tag. However, circumstances where a physical connection is preferred and/or required include the following:

- Performing tag diagnostics and troubleshooting
- Verifying tag configuration; useful especially for new PanGo users with limited experience
- Configuring tag parameters not addressed by profile definition panels
- Upgrading firmware or microcode in situations where OTA firmware upgrade is not possible

The physical connection for the serial interface on the PanGo v2 asset tag is a female mini-USB female 5-pin jack. To connect the tag to a personal computer, a cable equipped with USB 2.0 “A” and mini-USB “B” plugs must be used along with the serial-to-USB converter, shown in [Figure 26](#). These are available from your PanGo representative.

Figure 26 *Cable and Serial Converter*



Caution

Do not connect the PanGo v2 asset tag directly to the USB port of any device other than the serial-to-USB converter obtained from PanGo Networks. Connecting the v2 asset tag to any other device may result in permanent damage to the tag.

The serial communication parameters used to communicate to the asset tag are as follows:

- Speed—115200
- Bits—8
- Parity—None
- Stop Bits—1
- Flow Control—None

Use a terminal emulation program such as Hyperterm or TeraTerm, configured with the communication parameters shown above, to communicate to the asset tag after the cable and serial-to-USB adapter have been installed.



Note

The serial cable should not be left attached to the tag when the serial port is not actively being used for tag CLI commands. When the cable is left connected for an extended period, premature exhaustion of the tag battery can occur. Use of the serial port should be concluded in as expeditious a manner as possible and the cable promptly removed from the tag.

Some typical scenarios where serial access to the asset tag can be of benefit include the following:

- Tags that have been used previously with other non-factory-default settings—Previously used asset tags can receive new settings over-the-air only if they are able to associate to a WLAN that matches the settings already programmed in the tags. If this is inconvenient or impossible (for example, if

the tag WEP key settings are not known), it may be simpler to reset the tags to factory defaults and to initiate both stages of tag initialization by issuing the **AT&F** CLI command followed by **reset**. After the **AT&F** command, the tag should reboot with factory defaults and begin listening for broadcast beacons from the PGTP Broadcaster using the default WEP key and “PanG0pgtp” SSID (stage one of the initialization process). After the **reset** command, the tag should reboot once again but retain the settings it learned in stage one initialization. At this point, the tag attempts to associate using the default security profile SSID and WEP key.

- Troubleshooting tag association during stage one initialization—After the **AT&F** CLI command has been issued, the **config tag** CLI command should display “0x1 11”. If the **config** command instead displays “0x0 00”, retry initialization after checking that the PGTP Broadcaster is operating properly and that the initialization WLAN or temporary stand-alone access point is configured correctly.
- Troubleshooting tag association during stage two initialization—After the **reset** command has been issued, the **config tag** CLI command should display “0x2 22”. If it displays “0x1 11” instead, issue the **reset** command again after checking the status of the network and the settings in the default profiles. There should be an active WLAN available to the tag using the SSID and WEP key defined in the default security profile. After verifying that the PanGo PanOS Server is running and available and that its IP address and mask match those specified in the default reporting profile, retry initialization.
- Validating tag battery status using the **batt** command—Tag voltage is displayed in millivolts (mv).
- Checking IP information obtained from DHCP—The **dhcpip** and **lvmask** CLI commands are used to verify IP address and mask information obtained from DHCP servers.
- Checking IP connectivity—This can be performed using the **ping** CLI command when a tag is associated. The tag sends eight pings by default.

These are just a few examples of the functionality available using tag CLI commands via the serial interface. Additional commands you may find useful can be found in [Appendix F—Basic PanGo v2 Tag CLI Commands, page 82](#).

For a comprehensive list of CLI commands for the PanGo v2 LAN Tag, contact your PanGo representative.

Upgrading Tag Firmware



Note

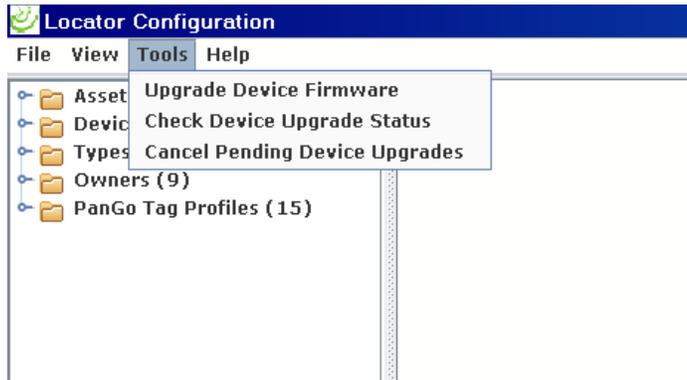
Tag firmware and microcode update should be performed only upon the recommendation of PanGo technical representatives. Perform upgrades only on tags with “Normal” battery levels. Improper upgrade procedures may result in non-functioning tags.

The firmware and microcode in PanGo v2 tags can be upgraded either over-the-air from the PanGo Locator Configuration utility or via the tag serial interface. Over-the-air firmware upgrade can be performed for tags in either chirping or RSSI modes after they have been initialized and fully configured. Chirping mode tags can receive over-the-air firmware upgrades only if they are configured to periodically check for configuration updates.

Schedule an over-the-air update of tag firmware and microcode by performing the following steps.

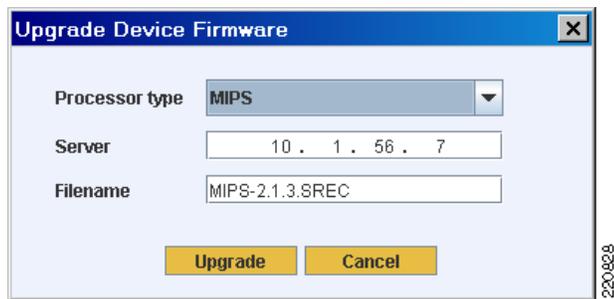
- Step 1** Select Tools > Upgrade Device Firmware option in the Locator Configuration utility, as shown in [Figure 27](#).

Figure 27 *Initiating Over-The-Air Tag Upgrade*



Step 2 Select the type of upgrade you wish to perform (either an upgrade of the MIPS processor or the tag microprocessor), and enter the address of a TFTP server and the name of the file containing updated the firmware (see [Figure 28](#)).

Figure 28 *Specify Update Parameters*



Caution

Do not attempt to upgrade both MIPS firmware and tag microcode simultaneously. If it is necessary to upgrade both firmware and microcode, *always upgrade the MIPS firmware first*, then proceed to upgrade the tag microcode as a separate operation.

Step 3 When connectivity is verified, the update you have selected is scheduled for all defined tags. The status of tag updates can be viewed via Tools > Check Device Upgrade Status ([Figure 29](#)). Pending updates may be cancelled using Tools > Cancel Pending Device Upgrades.

Figure 29 *Display Upgrade Status*

Device	Processor	Signal	Status	Time stamp
00147e002cc3	MIPS	10.1.56.7 MIPS-2...	COMPLETED	2007-01-24 19:4...
00147e002c2c	MIPS	10.1.56.7 MIPS-2...	PENDING	2007-01-24 19:2...
00147e001416	MIPS	10.1.56.7 MIPS-2...	PENDING	2007-01-24 19:2...

Keep the following points in mind when performing an over-the-air tag upgrade:

- The over-the-air upgrade process is non-selective. When initiated, over-the-air upgrade queues all known tags (including those not assigned to any assets) for the selected firmware upgrade. Similarly, pending tag updates are cancelled for the entire group of tags, not just individual tags. To perform selective upgrades of individual tags, use the serial CLI method of upgrading tag firmware.
- After the firmware update parameters have been entered and submitted, the tag upgrade process begins immediately after the tags associate to the production WLAN and contact the PanOS Server. For chirp mode tags, note that the upgrade process begins only upon the expiration of the configuration update interval timer. For both reporting and chirp mode tags, the tag upgrade status is not updated until the next time the tag associates after it completes the upgrade process.
- When a tag begins the upgrade process, the green LED remains solidly lit for approximately 1.5 minutes. During this period, the tags downloads its firmware and then updates its internal FLASH memory. *Do not remove power from the tag during this process.* Doing so risks internal corruption of the tag and may result in the tag becoming non-functional.
- Because this portion of the upgrade relies on a continuous source of tag battery power, before upgrading tag firmware or microcode, Cisco recommends that tag battery status be at the “Normal” level.
- Ensure that firewall and ACL definitions in your network and on WLAN controllers permit tag access to your designated TFTP server. For security, Cisco recommends that this TFTP server permit read-only access to its files and that it be disabled when not in use for actual tag upgrades.

Firmware and microcode upgrade of individual tags can also be performed using a serial cable and the tag CLI. For further information about this procedure, see the *PanGo Version 2 Tag Firmware Upgrade Quick Start Guide*, which is available upon request from your PanGo Networks representative.

Design and Deployment Best Practices

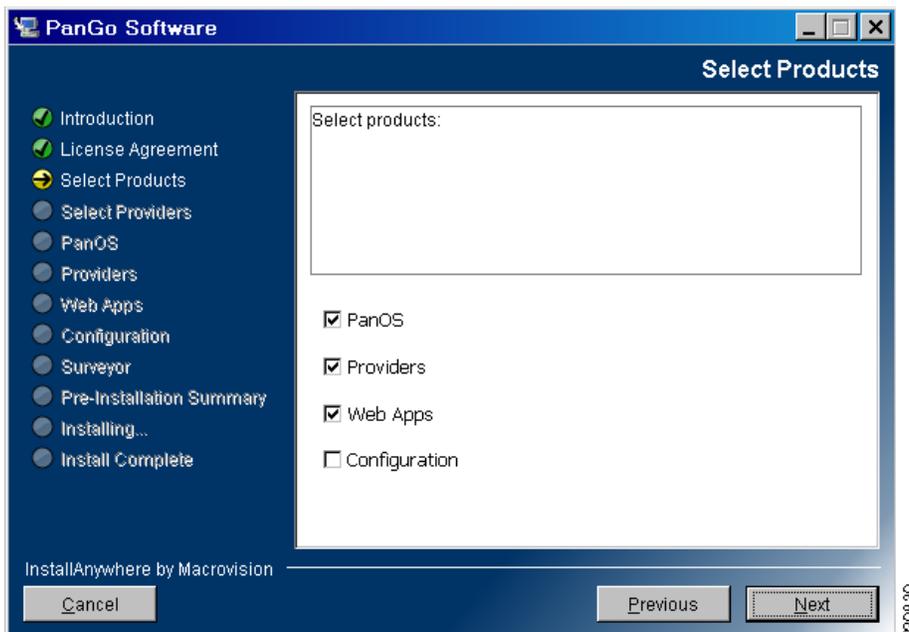
PanGo Software Installation

Installation instructions for all PanGo Networks software components can be found in the document entitled *PanGo Installation Guide for Version 4*, available on your installation CD or from your PanGo representative.

Beginning with version 4.1, PanGo uses a unified software installer (see [Figure 30](#)) that installs or upgrades all PanGo software components, including the following:

- PanGo PanOS Server
- PanGo Application Provider for the Cisco Location Appliance
- PanGo Notifier
- PanGo Locator web-based client applications
- PanGo Locator Configuration Utility

Figure 30 PanGo Unified Software Installer



Complete information regarding software and hardware pre-requisites as well as installation procedures can be found in the document entitled *PanGo Installation Guide for Version 4*, available on the PanGo 4.x installation CD or from your PanGo representative.

Keep in mind the following points when installing PanGo software:

- Cisco WCS is designed, tested, and supported assuming that its own set of hardware and software requirements are satisfied, and not in contention with other applications. Therefore, Cisco recommends that Cisco WCS be installed on an independent hardware platform and not co-reside with other applications, including the PanGo PanOS Platform.
- The user and password credentials specified for the Cisco location appliance during PanOS installation are those that are used for HTTP/HTTPS access to the appliance. These credentials should not be confused with that of the root user used to access the location appliance via its CLI.
- As a security best practice, it is always recommended that the default location appliance password be changed to a strong password. It is also not necessary to provide the PanGo location client with write privileges to the databases of the location appliance. To function properly, PanOS requires only read access to the databases of the location appliance. Therefore, Cisco recommends that WCS be used to create a separate read-only userid and password assigned exclusively to location clients such as PanGo Locator. This is performed in WCS using Location > Location Servers > Accounts > Users and selecting “Add User”, as shown in [Figure 31](#).

Figure 31 Defining User Credentials

- The installation of the PanGo Location client proceeds more expeditiously if the Cisco location appliance is already configured and online when installing the PanGo PanOS Server. If not, installation pauses while attempting to communicate with the location appliance. If the location appliance is not available, the user is alerted after a timeout and prompted as to whether installation should continue regardless.
- If you choose to configure PanGo Notifier during installation, the SMTP server and port you specify must be available and online during installation.
- If you are upgrading from a previous software installation, be sure to follow the instructions outlined in *PanGo Installation Guide for Version 4* relating to upgrading the PanGo PanOS Server. If you wish to retain your current PanOS configuration, *do not uninstall* your current version of PanGo PanOS Server before exporting your configuration data.
- Checking the **Configuration** check box in [Figure 30](#) schedules the installation of the PanGo Locator Configuration client utility, which should not be confused with the client browser-based web applications such as PanGo Location Monitor or PanGo Location Manager. The PanGo Location Configuration utility is a java-based application that must be installed on each client PC for which configuration access is denied. Unless you plan to use your PanGo PanOS Server as a client to manage your Locator configuration, you will probably want to install the configuration utility on a computer other than the PanOS server itself. To do this, insert the CD and start the installation routine on a client computer that meets the system pre-requisites stated in the *PanGo Installation Guide for Version 4*. Do not enable any checkboxes other than the Configuration checkbox when presented with the screen shown in [Figure 30](#).
- Keep in mind that the Locator Configuration utility is installed on a client workstation and does not provide for userid and password access control. For this reason, access to the Locator Configuration utility should be tightly controlled and installed only on secured systems.

- Cisco recommends that PanGo Locator be installed “with security”. This allows the PanGo Locator User Manager application to be used post-installation to configure multiple users and groups, assigning each an appropriate level of security for the task at hand. PanGo Locator can also be installed using Active Directory; however, this feature was not examined in this document revision.
- During the installation of PanGo PanOS Server, you are prompted to specify the geodetic coordinates (latitude, longitude, and altitude) of both the PanGo PanOS Server and the Cisco location appliance.



Note The geodetic coordinates entered for the location appliance and the PanOS Server should represent the (0,0) origin of the high level campus map used by the location appliance, *not the coordinates of where the location appliance itself is installed*. For further information, see [Defining Maps, page 61](#).

The *PanGo Installation Guide for Version 4* explains how geodetic coordinates for locations worldwide can be easily be acquired from publicly available sources such as Google Maps.

Firewall Port Considerations

The following considerations regarding required open ports should be kept in mind when deploying the PanOS server and PanGo Locator:

- By default, PanOS platform must be able to bi-directionally communicate with the Cisco location appliance using TCP ports 8001 and 8002 on the location appliance.
- The PanGo Locator Configuration program must be able to bi-directionally communicate with the PanOS server using TCP ports 3050 and 3066 on the PanOS server.
- HTTP or HTTPS is used between client browsers and the PanOS server when any of the PanGo Locator web applications are executed. By default, only HTTP is enabled using TCP port 80 on the PanOS server. This can be changed, or HTTPS can be enabled via the `http.properties` file (see [Secure HTTP, page 54](#)).
- If the PanGo Notifier notification system is used, ensure that TCP port 25 is not blocked such that the PanOS platform can successfully transmit SMTP messages to an SMTP server. PanGo Notifier allows for test messages to be sent to validate proper operation.

If any of these ports are changed from the defaults, Cisco recommends that the appropriate adjustments be made to any intermediary firewall devices to ensure continued proper function.

Cisco UWN Location-Based Services Best Practices

General best practices in deploying a location-aware Cisco Unified Wireless Network can be found in *Wi-Fi Location Based Services: Design and Deployment Considerations* at the following URL: <http://www.cisco.com/univercd/cc/td/doc/solution/wifidesi.pdf>

However, you should be aware of additional considerations specific to a Cisco/PanGo Asset Tracking solution. The following sections detail these considerations and offer best practice recommendations wherever possible. In addition, important caveats and potential workarounds are mentioned in [Caveats, page 72](#).

Planning for Tag Initialization

As described in [Tag Initialization, page 19](#), PanGo v2 LAN Tags can be initialized over-the-air or manually via individual CLI commands using the tag serial interface. If replacing a defective asset tag or deploying only a few new asset tags, using the serial interface to perform a manual configuration may be the best route. However, if you are deploying a large number of new tags or simply prefer to avoid manual configuration, the over-the-air initialization capability can be used quite effectively provided that security precautions are carefully observed.

As with the case of any WLAN using static WEP keys, there is always the risk of an attacker discovering the WEP key through a variety of well-published attacks. Although it does apply a very basic level of security, WEP is generally viewed as insufficient for securing business communications because the original 802.11 standard did not address the issue of how to manage encryption keys. The encryption mechanism itself was also found to be flawed, in that a WEP key can be derived simply by monitoring client traffic.

It is typically a recommended best practice to avoid the use of static WEP entirely if possible. In some cases, however, client devices critical to the overall business mission may require the support of static WEP simply because other security alternatives (such as 802.1x, WPA, WPA2, and so on) may not be supported by the device. Unless there are alternate devices available that can satisfy the business need while avoiding the use of static WEP, steps must be taken to assure that the static WEP WLAN is properly configured such that clients accessing the system via this WLAN are not permitted to access resources outside those that are absolutely essential to their function. Note that such practices do not make static WEP secure, but rather they attempt to mitigate obvious security holes (such as shared authentication) and limit the scope of network resources that may be directly at risk.

To conduct over-the-air tag initialization, PanGo v2 tags use a factory-default SSID and WEP key that is separate and distinct from the SSID used for normal tag operations. When configuring this initialization WLAN, keep in mind that the SSID and WEP key used are published both in vendor documentation as well as in the default tag configuration itself. Because of this well-published nature, it is reasonable to assume that any party within range of access points on the initialization WLAN could potentially be able to gain access at any time with little difficulty.

Chapter 4 of the *PanGo Administration Guide* describes how over-the-air tag initialization is performed using the PGTP Broadcaster utility application, which was shown in [Figure 16](#). To support OTA initialization, an initialization WLAN on a WLAN controller should be configured as shown in [Figure 32](#).

Figure 32 Initialization WLAN Configuration

```

WLAN Identifier..... 2
Network Name (SSID)..... PanG0pgtp
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Disabled
AAA Policy Override..... Disabled
Number of Active Clients..... 1
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Interface..... vlan60
DHCP Server..... Default
DHCP Address Assignment Required..... Enabled
Quality of Service..... Silver (best effort)
WMM..... Disabled
CCX - AironetIe Support..... Disabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Radio Policy..... 802.11B and 802.11G only
Security
  802.11 Authentication:..... Open System
  Static WEP Keys..... Enabled
  Key Index:..... 1
  Encryption:..... 104-bit WEP
  802.1X..... Disabled
  Wi-Fi Protected Access (WPA/WPA2)..... Disabled
  CKIP ..... Disabled
  IP Security..... Disabled
  IP Security Passthru..... Disabled
  L2TP..... Disabled
  Web Based Authentication..... Disabled
  Web-Passthrough..... Disabled
  Auto Anchor..... Disabled
  Cranite Passthru..... Disabled
  Fortress Passthru..... Disabled
  H-REAP Local Switching..... Disabled
  Management Frame Protection..... Enabled (Global MFP Disabled)
    
```

220832

Keep in mind the following:

- The over-the-air initialization procedure depends on the availability of a static WEP WLAN configured with an SSID of “PanG0pgtp” and a 104-bit static WEP key of 0x503935396372666D614D425253 (ASCII “P959crfmaMBRS”).
- Newly delivered tags (or tags that have been reset to factory defaults using the **AT&F CLI** command) by default probe for access points using this SSID and WEP key. Tags associate to the initialization WLAN and receive information regarding the production server IP address, SSID, and WEP key encrypted in the UDP broadcast frame emanating from the PGTP Broadcaster.
- Tags must receive an IP address to receive UDP directed broadcasts and successfully complete initialization. Cisco recommends that a DHCP server be used to assign tag IP addresses.
- After initialization, the PanGo tag disconnects from the initialization WLAN and attempts to contact the production PanGo PanOS Server on the production WLAN for the remainder of its configuration information. If the production WLAN is not available, the tag continues attempting to contact it.

Cisco WLAN LAN Controllers by default do not send any broadcast or multicast traffic received on the VLAN from first hop routers to wireless devices that have successfully associated to access points. To pass the UDP broadcast frames from the Ethernet PGTP Broadcaster to PanGo tags associated to the initialization WLAN, the WLC used for tag initialization must be configured to perform broadcast forwarding.

Enabling broadcast forwarding and selecting a forwarding method are global parameters that can impact all the WLANs configured on a controller. Before enabling these parameters on production controllers or other mission-critical networks, be certain that you understand the nature and composition of both the PanGo-related as well as the non-PanGo-related broadcast traffic present on your wired network.

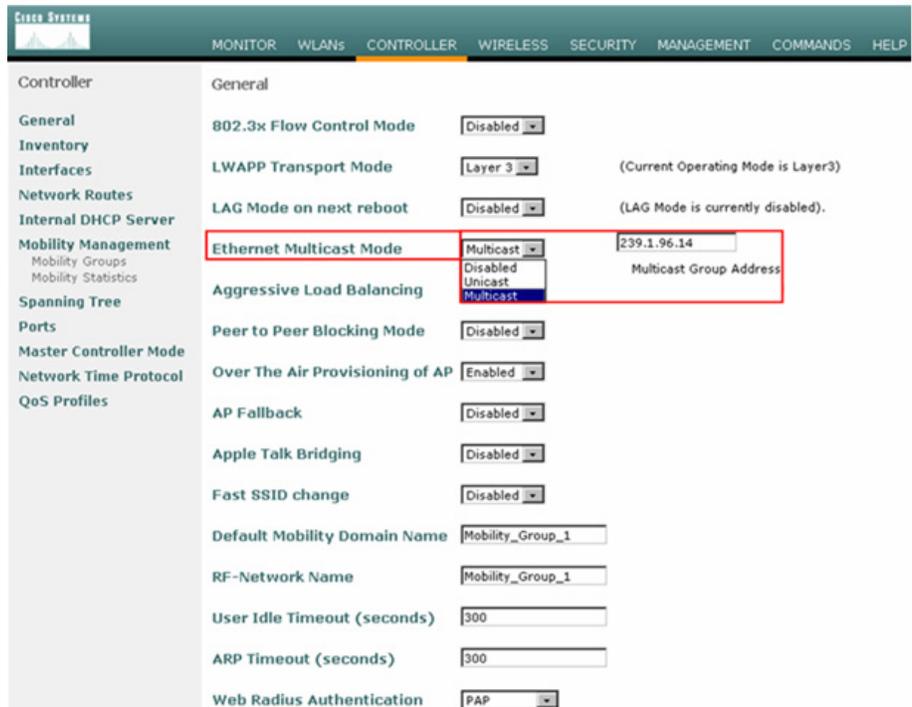
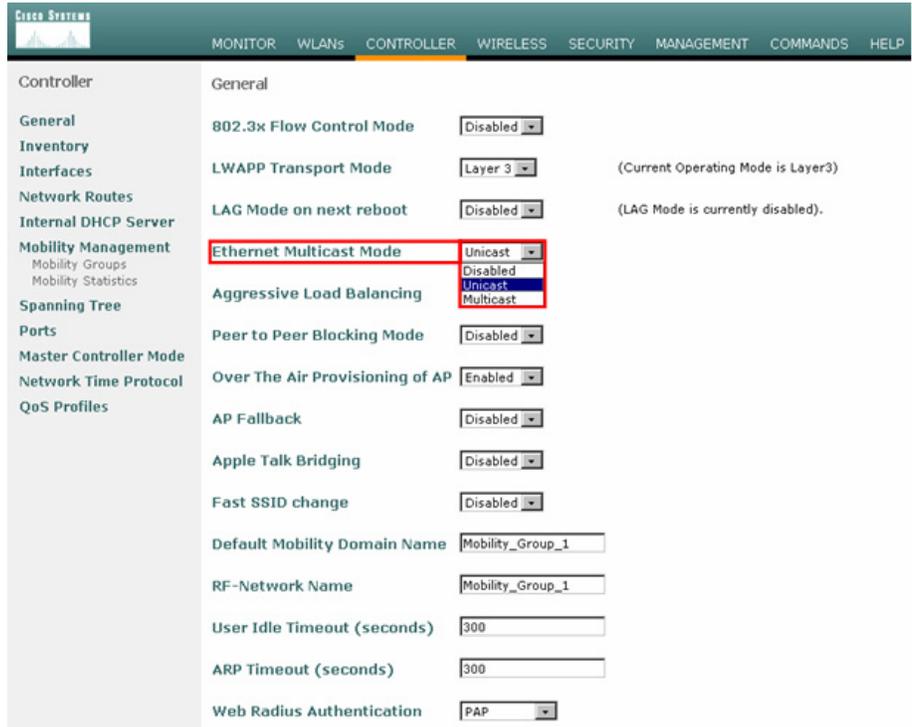
A comprehensive discussion of broadcast and multicast forwarding on wireless networks is beyond the scope of this document. For an excellent review of this topic, see the following:

- “Cisco Unified Wireless Multicast Design Guide” chapter in the *Enterprise Mobility 3.0 Design Guide*:
<http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/emob30dg-Book.htm>.
- “Multicast with WLAN Controllers and LWAPP Access Points”:
http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00807cc10d.shtml

In networks with a routing infrastructure capable of multicast delivery, a multicast forwarding method can be configured on the controller for efficient delivery of broadcasts to end clients via the registered access points of the controller.

Broadcast forwarding is configured differently depending on the specific release of WLAN controller software in use. For 4.0 WLAN controller releases up to and including 4.0.179.11, broadcast forwarding is enabled by default whenever multicast forwarding is enabled. [Figure 33](#) shows how this can be done using the controller GUI with either a unicast or multicast forwarding method. Note that when specifying a multicast forwarding method, a multicast forwarding address must also be specified.

Figure 33 Enabling Broadcast/Multicast Forwarding in Release 4.0.179.11



2208033

Regardless of whether a unicast or multicast forwarding method is selected, *both* broadcasts and multicasts are forwarded, because the use of broadcast and multicast forwarding is coupled in 4.0 WLAN controller releases up to and including 4.0.179.11.

Starting with release 4.0.206.0, the enabling of global broadcast forwarding and global multicast forwarding has been decoupled when using the controller CLI. Because of this, Cisco recommends that the controller or WCS CLI be used when configuring broadcast or multicast forwarding modes. Note that the default states for both broadcast and multicast forwarding have not changed; they are still both disabled.

The following CLI commands allow for a common forwarding mode as well as broadcast forwarding state to be quickly and efficiently specified in WLAN 4.0 controller software releases 4.0.206.0 and later:

- To specify a common mode for both broadcast and multicast forwarding:

```
config network multicast mode {unicast | multicast ipaddr}
```

- To enable broadcast forwarding independently of multicast forwarding:

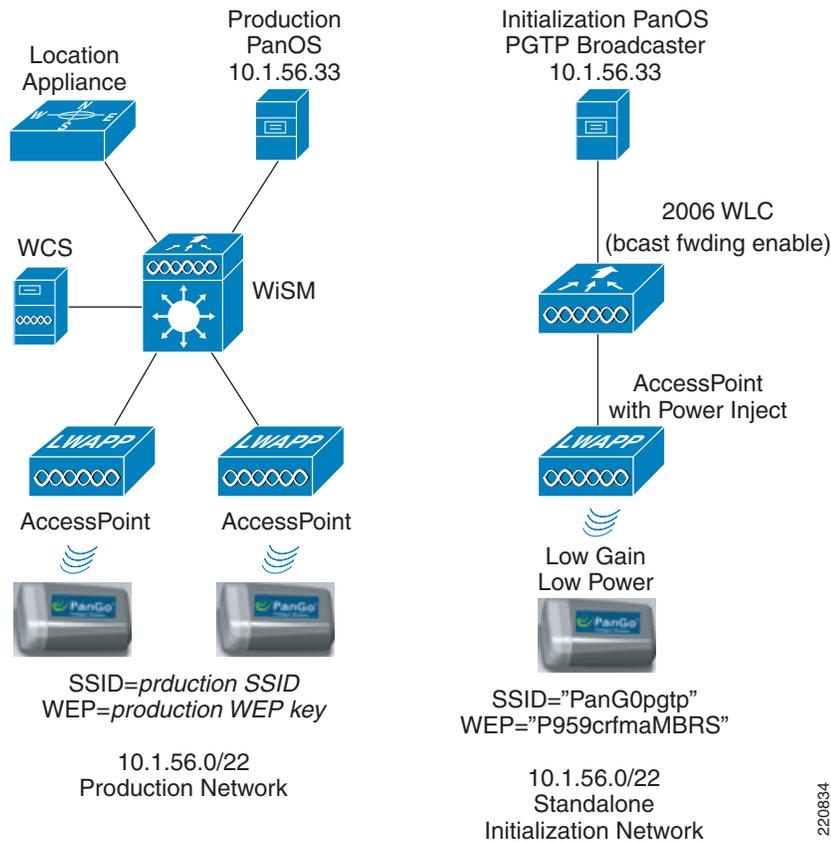
```
config network broadcast enable
```

Note that the specification of a common forwarding mode in the first command above does not implicitly enable multicast forwarding. Multicast forwarding can be enabled using the CLI command **config network multicast global enable**. It is not necessary to enable multicast forwarding for PanGo initialization purposes when using controller software release 4.0.206.0 or later.

The *PanGo Administration Guide* describes two approaches to configuring and using a PGTP broadcast server to initialize asset tags. The first is to activate the PGTP Broadcaster on the production PanOS Server. An alternative approach is to install a separate PanOS Server on a completely independent network. Although both approaches can be used to successfully initialize PanGo tags, the use of the alternative approach (shown in [Figure 34](#)) offers the following advantages and is recommended:

- **Security**—The possibility of unauthorized wireless clients accessing resources on the production network by associating to the well-known “PanG0pgtp” initialization WLAN is significantly reduced. The initialization network is now a separate physical entity with no connection to the production network.
- **Scalability**—This approach lends itself nicely to use in centralized staging facilities. One or more staging facilities can be configured to initialize tags centrally for shipment to production sites worldwide. Staging facilities can easily be configured to support sites with different SSIDs and WEP credentials.
- **No production WLC broadcast forwarding**—Use of a separate initialization network averts the requirement to enable broadcast forwarding on your production controller for tag initialization purposes. This avoids having to construct ACLs to prevent unwanted broadcast traffic from being sent on the air interface, because all broadcasts received by the WLC on the VLANs from the first hop router would otherwise be transferred to mapped WLANs. Using a simple standalone network to perform tag initialization eliminates having to make these changes on production networks, especially in the case of “one-time” tag initializations.

Figure 34 Tag Initialization Using Independent Network



220834

When using the method shown in [Figure 34](#), the default reporting and security profiles should be configured identically to that of the production PanGo PanOS Server. Follow the configuration guidelines outlined in Chapter 4 of the *PanGo Administration Guide* closely to ensure that the initialization PanGo PanOS Server mirrors the credentials of the production server. This is important because the destination address of the UDP broadcast is based on the subnet of the server IP address contained in the connectivity panel of the default reporting profile contained on the initialization PanGo PanOS Server.

Hardware requirements for the independent initialization network are modest. A server hardware and operating system platform meeting PanGo requirements is necessary, as detailed in the *PanGo Installation Guide for Version 4*. Keep in mind that the function of this server is basically only to run the PGTP Broadcaster utility and not to participate in actual tag tracking, so the minimum PanGo recommended hardware is typically sufficient. A single LWAPP access point is capable of providing more than sufficient coverage to initialize tags gathered into a group (for example, in a single room), even at the lowest power settings. A small-scale WLAN controller (configured for broadcast forwarding) such as the Cisco 2006 with its integrated four-port switch and DHCP server works well in this application.



Note

Although the Cisco 2006 is suggested here, other WLAN controllers can be used as well. When using the Cisco 2006, a power injector, power supply, or third-party power over Ethernet (PoE) solution is required to supply power to access points.

Alternatively, if a Cisco Aironet stand-alone access point is available, it can be used in place of the WLAN controller and LWAPP access point (a DHCP server is required as well as an Ethernet switch or crossover cable). A sample configuration for a Cisco Aironet 1200 series stand-alone access point used for tag initialization is provided in [Appendix A—RSSI Mode Tag Operation, page 74](#). Note that the UDP broadcasts required for tag initialization are forwarded by default.

Regardless of whether tag initialization is performed using an independent system or the production WLAN, the following best practice recommendations should be followed to reduce the potential security exposure when using a static WEP-based initialization WLAN:

- Install or enable the “PanG0pgtp” initialization SSID on only a single access point if possible.
- To limit the range of the initialization access point, configure it for the lowest supported transmit power that is found to acceptably cover the area within which the tags are to be initialized. On access points with external antenna capability, use the lowest gain external antenna available (Cisco AIR-ANT4941 is recommended). Gather the tags requiring initialization into a group that is in range of this single, low transmit power access point.
- Keep the initialization WLAN active for only as long as required to initialize all tags. After tag initialization has been completed, power down the initialization network or deactivate the initialization WLAN and remove any temporary initialization infrastructure.
- The use of “shared key authentication” on static WEP WLANs is not recommended because this practice increases vulnerability by facilitating WEP key discovery.
- Conduct all tag initialization operations indoors, toward the center of buildings or in other areas where the potential for RF propagation of the initialization WLAN outside the building is poor or non-existent. A good example is a below-ground basement facility. Avoid conducting tag initialization in an outdoor environment, especially when using the production PanGo PanOS Server as a PGTP broadcaster.
- If using the production network for tag initialization (not recommended), use a firewall between the VLAN associated with the initialization WLAN and any other resources, including the PanGo PanOS Server.
- Limit traffic on the initialization WLAN to the outbound flow of UDP broadcast packets from the PGTP Broadcaster to addresses on the initialization WLAN at destination port 1177. Depending on the configuration of your network, additional services may need to be permitted as well (such as DHCP). Because the conveyance of UDP broadcasts from the PGTP Broadcaster outbound via the WLC to associated tags is the sole purpose of the initialization WLAN, all other unrelated IP traffic inbound and outbound should be denied.
- Clients on the initialization WLAN should be prevented from attempting to manage the associated WLAN controller. This can be accomplished by disabling the “Management Via Wireless” controller configuration option. Note that disabling “Management Via Wireless” still allows wireless clients on this WLAN to ping the management interface of the controller. To prevent this, a more restrictive ACL can be defined on the controller and assigned inbound to the controller CPU using the CLI.

Planning for PanGo Version 2 Tag Deployment

Tag Security Considerations

Chirp Mode

As described in [Chirp Mode, page 23](#), PanGo v2 tags in chirp mode use Layer 2 multicasts to uni-directionally communicate their presence and battery status information via the transmission of 34-byte unencrypted 802.11 data frames at 1 Mbps. Unless engaged in performing an OTA update of configuration or firmware, chirp mode tags do not associate to the wireless infrastructure, do not require access to any network resources such as hosts or databases, and do not require the presence of any static WEP WLANs.

Chirp mode tags attempt to associate to the network infrastructure once every 24 hours using the information contained in the default security profile (otherwise known as the over-the-air update process) unless this behavior is disabled (see [Appendix D—Suspending Over-The-Air Configuration Updates, page 80](#)).

For the OTA update mechanism to function properly, there must be a static WEP WLAN available configured with the production SSID and production WEP key contained in the default security profile. Because of the potential vulnerabilities associated with the use of static WEP, appropriate measures limiting the realm of resources available to clients associating to this WLAN should be in place whenever the static WEP WLAN is in use. This should include the following:

- Avoiding the use of “shared key authentication” on static WEP WLANs because this practice increases the vulnerability of static WEP by facilitating key discovery.
- Restricting traffic on the production static WEP WLAN to and from destination TCP port 1177 on the PanGo PanOS Server. Use of a firewall is recommended. Depending on the configuration of your network, you may need to expand these restrictions to include other network services such as the following:
 - DHCP.
 - TFTP, which is only necessary if you desire to perform over-the-air tag firmware updates. Tags were observed to use UDP port 1024 for UDP file transfer when performing firmware upgrades during lab testing. As a matter of good policy, this TFTP server should be disabled when not needed for tag firmware updates.
- Clients associating to this WLAN should be prevented from attempting to manage the associated controller by disabling the “Management Via Wireless” controller configuration option. Note that disabling “Management Via Wireless” still allows wireless clients on this WLAN to ping the management interface of the controller. To prevent this, a more restrictive ACL can be defined on the controller and assigned inbound to the controller CPU using the CLI.

An important consideration to keep in mind is that the static WEP WLAN used by the v2 tag in chirp mode is required only when it is necessary to deliver tag configuration and firmware updates. If it is known beforehand that there are no updates to be delivered, Cisco recommends that the static WEP WLAN be administratively disabled. This does not affect the general “chirping” operation of the tags. Regardless of the status of the static WEP WLAN, tags still attempt to probe using the production SSID at the expiration of each configuration request interval. If the static WEP WLAN is disabled, tags continue with their normal routine of transmitting L2 multicasts after detecting the lack of probe responses from the infrastructure. This behavior can be seen in [Figure 35](#).

Figure 35 Chirping Tag with Static WEP SSID Administratively Disabled

Packet	Transmitter	Receiver	Protocol	Size	Dat...	Summary
1	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 0,FN= 0
2	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 1,FN= 0
3	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 2,FN= 0
4	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 3,FN= 0
5	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 4,FN= 0
6	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 0,FN= 0
7	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 1,FN= 0
8	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 2,FN= 0
9	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 3,FN= 0
10	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 4,FN= 0
11	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 0,FN= 0
12	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 1,FN= 0
13	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 2,FN= 0
14	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 3,FN= 0
15	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 4,FN= 0
16	00:14:7E:00:14:16	Ethernet Broadcast	802.11 Probe Req	51	1.0	FC=.....,SN= 0,FN= 0,SSID=testuser
17	00:14:7E:00:14:16	Ethernet Broadcast	802.11 Probe Req	51	1.0	FC=.....,SN= 0,FN= 0,SSID=testuser
18	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 0,FN= 0
19	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 1,FN= 0
20	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 2,FN= 0
21	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 3,FN= 0
22	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 4,FN= 0
23	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 0,FN= 0
24	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 1,FN= 0
25	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 2,FN= 0
26	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 3,FN= 0
27	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 4,FN= 0
28	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 0,FN= 0
29	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 1,FN= 0
30	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 2,FN= 0
31	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 3,FN= 0
32	00:14:7E:00:14:16	01:14:7E:00:00:00	802.11 Data	34	1.0	FC=TF.....,SN= 4,FN= 0

220855

RSSI Mode

As described in [RSSI Mode, page 22](#), PanGo v2 tags in RSSI mode associate to the production static WEP WLAN to bi-directionally communicate with the PanGo PanOS Server. During this process, PanGo v2 tags probe and associate in a similar manner to other wireless clients. Packets flow between the tag and TCP destination port 1177 on the PanGo PanOS Server, updating the server with the latest tag and event status as well as checking for configuration or firmware updates on the server.

PanGo v2 tags in RSSI mode rely on the constant availability of a static WEP WLAN configured with the production SSID and production WEP key. Because static WEP vulnerabilities are common to both RSSI mode as well as chirp mode usage (only if the OTA update capability is used in chirp mode), all the precautions mentioned in [Chirp Mode, page 43](#) should be applied to RSSI mode tags as well except for disabling the static WEP WLAN.

WLAN Controller Tag Considerations

Chirp Mode

The tracking of Layer 2 multicasting RFID tags is disabled by default in the WLAN controller for software releases up to and including 4.0.x.x.

Therefore, perform the following before attempting to track RFID tags:

- Connect to the controller via Telnet, SSH, or the console port and issue the following commands:

```
(Cisco Controller) >show rfid config
RFID Tag data Collection..... Disabled
RFID Tag Auto-Timeout..... Disabled
RFID Client data Collection..... Disabled
RFID data timeout..... 1200 seconds
```

- Note “RFID Tag data collection” is disabled by default. To enable it issue the following:

```
(Cisco Controller) >config rfid status enable
(Cisco Controller) >show rfid config
RFID Tag data Collection..... Enabled
RFID Tag Auto-Timeout..... Disabled
RFID Client data Collection..... Disabled
RFID data timeout..... 1200 seconds
```

Cisco WLAN controllers also contain a parameter known as the *rfid timeout* that specifies how much time is allowed to elapse before a Layer 2 multicasting tag is removed from the internal tables of a controller whose access points are no longer detecting the tag.

For chirp mode tags, this value should be set to a minimum of three times (and a maximum of eight times) the longest tag blink (beacon) rate found in the tag population (inclusive of stationary as well as motion blink rates). These rates are specified in the reporting panel of the assigned chirping profile (see [Figure 21](#)). The default value for the rfid timeout is 1200 seconds, with the maximum allowable setting being 7200 seconds.

For example, for a tag population of 500 tags where the longest stationary tag blink rate is 600 seconds and the longest motion blink rate is 60 seconds, the rfid timeout should be set to a minimum of $3 * \max(600,60) = 3 * (600) = 1800$ seconds.

The rfid timeout is configured as follows:

```
(Cisco Controller) >config rfid timeout 1800
(Cisco Controller) >show rfid config
RFID Tag data Collection..... Enabled
RFID Tag Auto-Timeout..... Disabled
RFID Client data Collection..... Disabled
RFID data timeout..... 1800 seconds
```



Note

Subject to the rfid timeout, Cisco WLAN controllers accumulate RSSI information for up to 500 L2 multicasting tags in software releases up to and including 4.0206.0. RSSI for detected tags exceeding this limit are not recorded by the controller and are not passed to the location appliance. This state continues until the expiration of one or more tag rfid timeouts causes the current number of detected tags to drop below 500 for the controller.

RSSI Mode

Cisco WLAN controllers are configured by default to aggregate and report RSSI of detected WLAN clients, including PanGo v2 tags that are configured for RSSI mode. Therefore, it is not necessary to explicitly enable tag data collection on the controller when using PanGo v2 tags in RSSI mode.

Cisco WLAN controllers accumulate client RSSI up to the following limits in software releases up to and including 4.0.206.0:

- 2006 controllers—Up to 256 clients.
- WLCM module—Up to 256 clients.
- 4402 controllers—Up to 2,500 clients.
- 4404 controllers—Up to 5,000 clients.
- WiSM module—Up to 10,000 clients.

RSSI for detected clients exceeding these limits are not recorded by the controller and are not passed to the location appliance.

AP 1210/1220/1230 Access Points

Note that a caveat exists with regard to the use of Cisco Aironet AP 1210, 1220, and 1230 Series LWAPP access points and PanGo v2 asset tags configured for chirp mode.

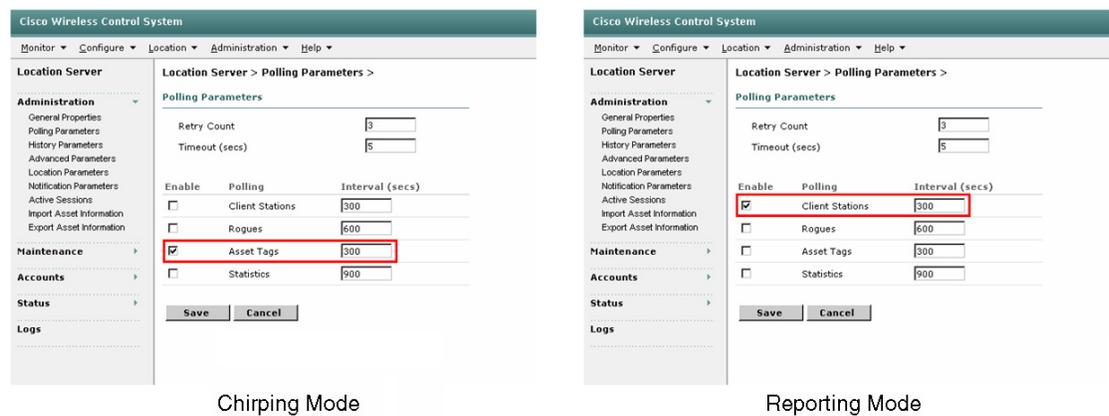
For further details, see [AP1210/1220/123x Access Points May Not Reliably Detect Chirp Mode Tags](#), page 72.

Location Appliance Tag Considerations

Polling of WLAN controllers for aggregated RSSI information is not enabled in the default location appliance configuration. This includes any aggregated RSSI from PanGo v2 tags in either RSSI or chirp modes. To enable RSSI collection, polling must be explicitly enabled on the location appliance using the Cisco WCS. This is a good example of WCS acting in its role as a *control client* for the location appliance.

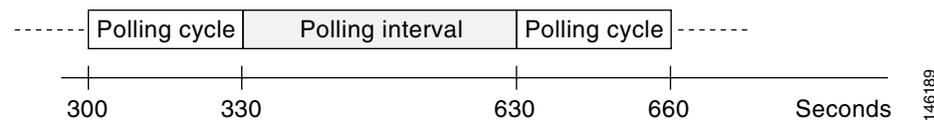
Figure 36 shows the use of the WCS Locate > Location Server > Polling Parameters menu panel to accomplish this.

Figure 36 Enabling Tag Data Collection in the Location Appliance



The polling interval values shown represent the time period between the start of subsequent polling cycles. For example, if a polling cycle requires 30 seconds to complete and the polling interval is 300 seconds, polling cycles would start every 330 seconds. This is shown in Figure 37.

Figure 37 Polling Interval

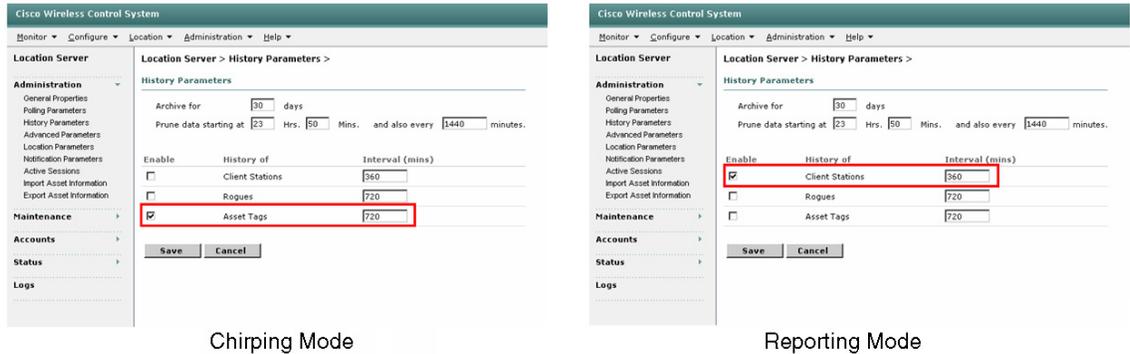


Bear in mind that when setting the client station polling for RSSI mode tags, this polling value also determines how frequently RSSI information is collected for other non-PanGo WLAN clients such as laptops, PDAs, wireless VoIP phones, handheld barcode computers, and so on.

Cisco WCS also provides the ability to playback asset tag location history records that are archived by the location appliance. The archival of asset tag location history is disabled by default in the location appliance. However, if location trending and the analysis of asset tag location history is desired using

WCS, enable location history recording in the location appliance via Location > History Parameters, as shown in Figure 38. Enable the appropriate line item, keeping in mind that enabling location history archival enables it for other WLAN clients as well as RSSI mode tags.

Figure 38 Enabling Location History Archival



220837

Tracked Device Capacity

As described in [Chirp Mode, page 23](#), chirp mode tags can periodically associate to WLAN infrastructure to verify whether there are any configuration updates present on the PanGo PanOS Server.

Because of this unique tag behavior, PanGo v2 asset tags in chirp mode can be conceptualized as possessing a “dual personality”. The personality of the chirp mode tag is dependent on whether the tag is engaged in sending Layer 2 multicasts or associating to the WLAN to check for updates. Technically, this means that the MAC address of a single chirp mode tag may be conceived as potentially representing two different device classes: an L2 multicasting active RFID tag and a 802.11 WLAN client.

Currently, a caveat exists when using chirp mode tags with the OTA configuration update feature enabled (see [Tags May Appear As Two Tracked Devices in Location Appliance, page 73](#)). Depending on the number of chirp mode tags in your environment as well as the total number of devices being tracked by your location appliance, periodic spikes can occur in the total tracked device count.

This caveat also has implications regarding what is displayed on WCS floor maps. When the PanGo v2 chirp mode tag is seen as two different categories of tracked device, the MAC address of the tag is associated with more than one icon on floor maps (both a yellow tag icon as well as a blue WLAN client are shown). PanGo Locator, however, displays the v2 tag in chirp mode as only a single icon, regardless of its dual personality.

WCS Tag Considerations

As was discussed in section [PanGo Locator and Cisco WCS, page 14](#), both products have location client capabilities, with each being optimized to address the needs of different audiences. To enable WCS to display the location of chirp mode tags on floor maps, it is necessary to ensure that this capability is enabled via Monitor > Maps > Campus > Building > Floor, as shown in [Figure 39](#).

Figure 39 Enabling WCS Display of Chirp Mode Tag Location



Ensure that **Show 802.11 Tags** is selected from the drop-down menu. When properly enabled, a yellow tag icon is shown under View Filters at the top of the map display. This configuration change can be saved as a default by choosing **Set as My Default** from the drop-down option menu.

By performing a mouse-over or clicking on any yellow tag icon on any WCS floor map, additional information can be displayed regarding the asset tag. This includes the tag MAC address, the time it was last located, any location notifications generated, and the latest battery status.

In a similar fashion, the display of RSSI mode tags on WCS floor maps must also be enabled by using WCS Monitor > Maps > Campus > Building > Floor. However, for RSSI mode tags you should ensure that **Show Clients** is selected from the drop-down menu. When properly enabled to display RSSI mode tag location, a blue rectangular icon is shown under View Filters at the top of the map display. This configuration setting can be saved as a default by choosing **Set as My Default** from the drop-down option menu.

Bear in mind that when enabling the display of PanGo v2 tags in RSSI mode, other WLAN clients will also be displayed as well. To limit the scope of the display, assign a group or category name to the PanGo RSSI mode tags in WCS. You can then use the available display filters to limit the display to only those WLAN client devices assigned to a matching group or category.

PanGo Locator Tag Considerations

Security Profiles

PanGo Locator offers great flexibility in allowing for the definition of multiple profiles to best match tag behavior to the anticipated behavior of assets. Although multiple reporting and chirping profiles can be defined, each with a different set of tag parameters, note that only one security profile (the default security profile) can currently be defined in the PanOS Server. The default security profile must be initialized with the correct values for SSID and WEP key for PanGo v2 tags to initialize properly.

Note that the use of the Alternate Scanning SSID parameter is not applicable when using PanGo Locator as a location client in the Cisco Unified Wireless Network.

RSSI Mode Reporting Profiles

When defining profiles for PanGo v2 tags that operate in RSSI mode, note the following:

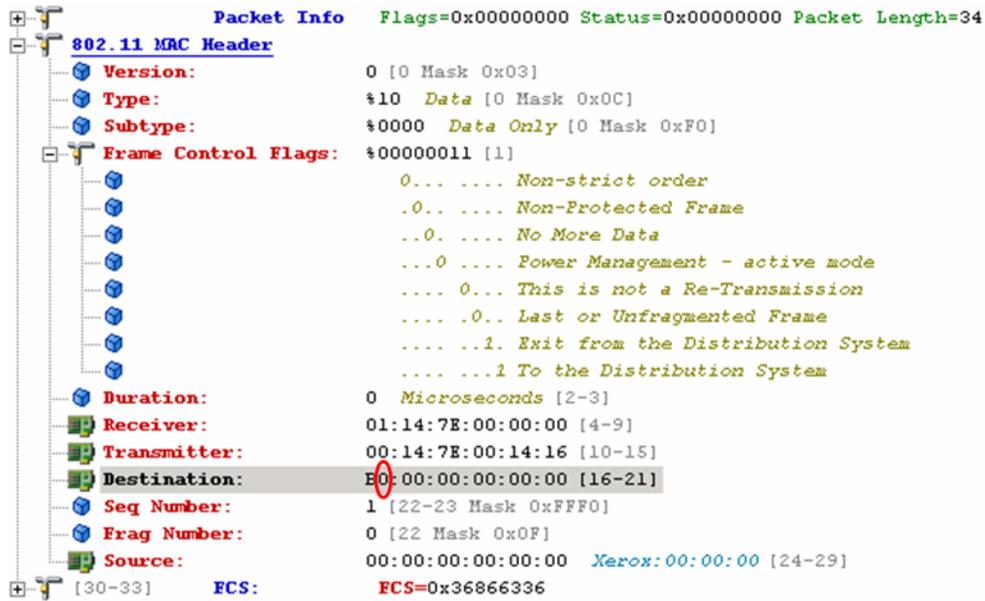
- **Transmission rates**—PanGo v2 tags support communication at rates of 1, 2, 5.5, 6, 9, 11, 12, 18, and 24 Mbps. Tags pass data frames at the highest supported rate of the access point in all cases. Lab testing indicates that the transmission rate values specified in the reporting profiles of PanGo PanOS v4.5 do not appear to influence the set of basic and extended rates communicated by the v2 tag in its probe and association requests.
- **Max Access Points**—This parameter represents the maximum number of access points that an RSSI mode tag uses to obtain access point RSSI information from the infrastructure. This parameter should be set to “1” because localization is not performed in this manner in the Cisco UWN.
- **Stationary, Transition, and Mobile Scan Counts**—These parameters represent the number of probe requests issued on each configured channel by tags operating in RSSI mode when in various stages of movement. These probe requests are issued upon the expiration of the stationary, transition, or mobile reporting intervals. The default value is ten probe requests for stationary and transition scan counts, and five for the mobile scan count. Lab testing indicates that the stationary and transition scan counts can be reduced somewhat to increase the battery life of the v2 PanGo tag in RSSI mode. A suggested reduced value for these two parameters is 5. Values below this may reduce the reliability of tag detection in very busy wireless environments. In environments where there is much airtime contention or interference, it may be desirable to leave all scan count settings at their defaults.

RSSI Mode Tag State Events

PanGo v2 tags configured for RSSI mode support a variety of tag events that are intended to alert the user to important state changes. These events are not communicated to PanGo Locator via the location appliance but instead are transmitted via the higher-level session established between the tag and the PanGo PanOS Server. Tag events are configured in the events panel of the reporting profile assigned to the tag, as follows:

- **Motion State**—When enabled, PanGo v2 tags configured for RSSI mode notify the PanGo PanOS Server of changes in their motion state (for example, from the stationary state to the “in-motion” state). PanGo Locator indicates this state change by assigning a special icon variant to the asset, graphically indicating that the asset has entered a motion state (shown in [Figure 40](#)). Note that the icon associated with a moving asset bearing an RSSI mode tag undergoes an appearance change but does not continuously move on the map. This is done to avoid clutter and confusion on complex and busy maps with many assets in motion.

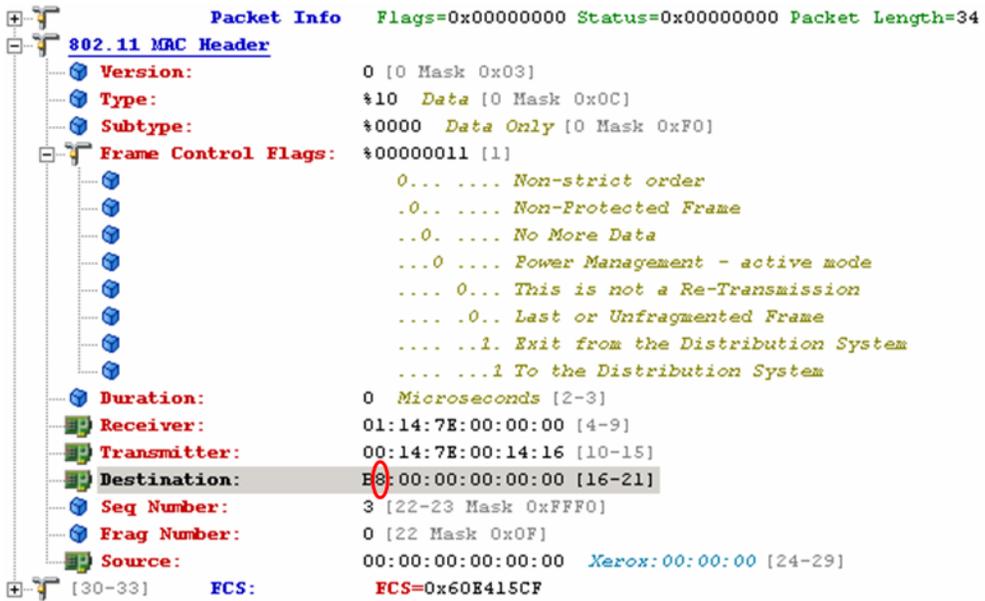
Figure 42 Battery State Bit Pattern = "00" Binary



220840

- Bit pattern = "10", representing a battery voltage that is typically less than ~3.80 volts (shown in Figure 43). WCS interprets this as the "low battery" state, whereas PanGo Locator interprets it as the "very low battery" state.

Figure 43 Battery State Bit Pattern = "10" Binary



220841

These states are reflected in the second nibble of the destination address, with the normal state having a value of 0x0 and the very low state having a value of 0x8.

If the PanGo Notifier module (discussed in [Notifications, page 70](#)) is enabled to generate e-mail notifications based on tag battery state, the Very Low Battery state (or bit pattern of binary “10”) results in the generation of the Low Power Shutdown e-mail notification.

It is highly recommended that tag batteries be replaced *without delay* when indication of an imminent tag Low Power Shutdown (or very low battery state) is received. No further warning will be received between that battery state and the point at which tag operation becomes unreliable.

If tag firmware or microcode updates are to be performed, it is highly recommended that tag batteries be replaced if the battery status is other than “Normal”.

Other Tag Considerations

Battery Life

The battery life of the v2 asset tag can be heavily impacted by choices made for profile and internal CLI parameters with regard to the modes in which the tag transmits, how often it transmits, and for what duration of time. For example, all the following can have a significant impact on overall tag battery life:

- Number of channels selected—PanGo v2 tags repeat their transmission payloads on all the channels enabled in the configuration profiles. Therefore, the number of channels selected should reflect only the channels used in your environment. Avoid having the tag transmit unnecessarily on channels that have not been assigned to access points in your environment. Exceptions to this recommendation are cases where tags may be required to migrate between environments that do not have the same channels allocated (because of interference issues, for example).
- Number of “scans” performed (probe requests) or “chirps” (L2 multicasts)—For chirp mode tags, the default number of “chirps” transmitted is five chirps per configured channel upon the expiration of the stationary or motion blink intervals. For the majority of environments, this setting ensures that the tag is detected despite any random packet loss. In noisy environments, the number of chirp packets transmitted can be increased via the **chirpcount** tag CLI command. This parameter is not accessible via the GUI.

Note that a caveat has been identified regarding signal strength consistency across the frames comprising a chirp mode burst. For further information, see [Chirp Mode Multicast Frames May Vary In Transmitted Signal Strength, page 73](#).

For RSSI mode tags, the default number of “scans” or probe requests transmitted is controlled by the stationary, transition, and mobile scan counts. The stationary and transition scan counts default to 10 and the mobile scan count default is 5 per selected channel. To improve battery life, it is suggested that all three scan counts be set to 5. The exception would be very noisy or very RF-busy environments, where higher scan counts (an increased number of probe requests) can improve detection under adverse conditions.

- Interval between association attempts or tag “blinks” (beacons)—Known as the reporting interval or “blink rate”, this parameter specifies how often a tag attempts to either associate to the infrastructure and communicate directly with the PanOS server (RSSI mode), or issue L2 multicasts (chirp mode). Customized intervals can be set for the stationary or motion states (as well as the transition state for RSSI mode tags).

Reporting interval can have a major impact on overall battery life. This can be seen from the chart shown in [Table 1](#), pertaining to a v2 tag in chirp mode with three active channels, motion detection disabled, and default values for chirp count and configuration request interval.

Table 1 Battery Life Projection for Chirp Mode v2 Tag

Blink Rate (minutes)	Estimated Battery Lifetime (days)
120	1500
60	750
30	375
15	188
12	150
5	63
2	25
1	12.5

When selecting reporting intervals or blink rates, keep in mind the need to balance optimum battery life against sufficiently frequent location updates, so as not to impair system usability. For example, from [Figure 16](#) you can see that a 30-minute blink rate may yield a battery life exceeding one year. However, for an asset in motion, a 30-minute blink rate may seriously detract from the ability of the system to accurately reflect the current location of the asset, because assets can change location quite frequently in a 30-minute time period. Enabling motion detection can assist in this situation, although at the cost of increased battery consumption.

- Motion detection—When enabled, the tag is triggered to report more frequently when in motion. More frequent transmission negatively impacts battery life, the degree to which is dependent on the motion blink rate chosen, the degree of motion sensitivity, how often the attached asset moves, and other motion-related variables contained in the reporting and chirp mode profiles. As mentioned previously, enabling motion detection has the potential to increase the timeliness of reported device location for devices that move frequently, especially in chirp mode. However, a compromise must typically be reached between the desire for more frequent localization of current asset position versus optimal battery life. Caution is advised against setting too short a motion blink rate for an asset that moves frequently, because this results in the tag beacons almost constantly at the motion blink rate. As can be seen from [Figure 16](#), this can result in reduced battery lifetimes.

Channel Assignment

Unlike standard 802.11 clients, RFID tags in general require the desired channels of operation to be pre-configured. Pre-configuring one or more channels of operation allows the tag to repeat its payload on each channel (probes for RSSI mode tags and L2 multicasts for chirp mode tags). This ensures that the tag is readily detected by access points whose main channel of operation matches one of the channels configured in the tag. Channel configuration is performed in the connectivity panel of the chirping or reporting profile assigned to the tag.

In most deployments, access points are typically installed using the non-overlapping channels in the 2.4 GHz band (FCC channels 1, 6, 11; ETSI channels 1, 7, 13; MKK channels 1, 5, 10, 14). In the large majority of installations, configuring tags in this way provides for commonality between sites. In some cases, however, interference conditions may exist, making certain channels less desirable or ruling them out entirely. Therefore, to ensure best results, PanGo v2 tags should be configured to match the deployed set of channels in your particular site.

Tag Transmit Power and DTPC

Dynamic Transmit Power Control (DTPC) consists of beacon and probe information elements that allow access points to broadcast their configured transmit power to clients. Clients can use this information to automatically configure themselves to the advertised power level of an access point while associated with it. In this manner, both devices are configured to use approximately the same transmitter output power, avoiding “one-way” exchanges between a high-powered access point and a low-powered client. DTPC is enabled by default on Cisco WLAN controllers.

PanGo v2 tags configured for RSSI mode interpret and respond to DTPC information elements. RSSI mode tags adjust their current transmit output power when transmitting data frames in accordance with the power level advertised by the access point to which it has associated. In tests where the transmit power of AP1242 access points was manually varied with DTPC enabled on the controller, the current transmit output power setting observed via the tag CLI is shown in [Table 2](#).

Table 2 *RSSI Mode Tag DTPC Behavior (using AP1242)*

AP Transmit Level	Current Transmit Output Power (dBm)
1 (+20 dBm)	+19
2 (+17 dBm)	+17
3 (+14 dBm)	+14
4 (+11 dBm)	+11
5 (+8 dBm)	+8.0
6 (+5 dBm)	+5.0
7 (+2 dBm)	+2.0
8 (-1 dBm)	Prior setting unchanged

The current transmit output power of the tag can be displayed via the `lvdump` tag CLI command.

Testing indicates that the transmit power used for probe requests issued by the v2 tag is not affected by the DTPC information transmitted by access points. Probe requests are transmitted at the internal transmit power setting of the tag, which defaults to +19 dBm. Note that the location-aware Cisco UWN uses the detected signal strength of probe requests (not data frames) when determining the location of WLAN clients and RSSI mode tags.

PanGo v2 tags configured for chirp mode generally do not use DTPC information when sending L2 multicasts. In most cases, chirp mode tags transmit their L2 multicast payload at the internal transmit power level setting of the tag. However, an exception to this was noticed during lab testing and is listed as a caveat (see [Chirp Mode Tags Using OTA Update May Vary Transmit Power With DTPC, page 73](#)).

PanGo PanOS Server and PanGo Locator Considerations

Complete documentation regarding PanGo PanOS Server and the various PanGo Locator applications can be found in the following documents available on your PanGo installation CD or from your PanGo representative:

- *PanGo Locator User’s Guide*
- *PanGo Locator Administrator’s Guide*

This section discusses important information to keep in mind when configuring and using PanGo PanOS Server and the PanGo Locator applications in a Cisco location-enabled Unified Wireless Network.

Defining Users and Groups

The PanGo Locator User Manager is used after installation to define user credentials and user access rights for the PanGo Locator web applications. Keep in mind that by default, newly created users are not assigned to any groups, and that newly created groups are not assigned any access permissions. Assignment of group or user access privileges must be explicitly performed or users will have insufficient access right to log into any of the Locator applications.

“View-only” groups should be created in Locator Manager and users not requiring the ability to modify application configurations should be assigned to these groups. An example of this can be seen in [Figure 44](#).

Figure 44 “View-Only” User Access Groups



Full modify access should be granted only to administrators and those users requiring it. Users not granted view or modify privileges to applications will not see entries for those applications appearing on the blue menu bar at the top of the screen.

Secure HTTP

The default protocol used between PanGo Locator web applications and the PanGo PanOS Server is HTTP. During login, HTTP allows user and password credentials to be passed in clear text between the client browser and the PanGo PanOS Server. For increased security, Cisco recommends that HTTP be used with Secure Sockets Layer (SSL) cryptography (HTTPS). The use of HTTPS prevents user credentials from being disclosed in clear text when using protocol analyzers or other tools to monitor session traffic between browsers and the PanOS server.

To enable the use of HTTPS, it is necessary to manually configure the PanGo PanOS Server to take advantage of it. A key store containing an appropriate SSL certificate must be created. The following procedure illustrates how to configure one-way SSL for the PanGo PanOS Server using a self-signed certificate.

-
- Step 1** Open Settings > Control Panel > Administrative Tools > Services on the PanGo PanOS Server and stop the PanOS Service.

- Step 2** Open a command prompt window on the PanGo PanOS Server and create a directory to be used to contain a new key store (for this example, a new directory is created called “SSL” below the “C:\” root directory). Make this newly created directory your current directory.
- Step 3** Create a key store that contains a self-signed certificate:
- ```
keytool -genkey -alias server -keyalg RSA -keystore server.keystore
```
- Step 4** After executing the above command, a series of questions will be posed to properly create the self-signed certificate. You should put the hostname of the server machine as both the first and last name for hostname validation to work properly. Use the same password each time you are prompted.
- When completed, the file “server.keystore” is generated in the directory where the **keytool** command was executed. This file now contains a self-signed certificate that can be used to authenticate incoming requests to the server.
- Step 5** Modify the “http.properties” file in “C:\Program Files\PanGo PanOS Server\Conf” such that the following attributes are set:
- https.enabled = true
  - https.keystoreFile = C:/ssl/server.keystore
  - https.keystorePasswordKey = keystore.key
  - https.keystoreType = JKS
- The HTTPS port is defined as 8443 by default. This can be changed if desired by setting the https.port property.
- Be sure to remove any leading # characters from these lines. Otherwise, they remain as comments and will not take effect. Notice that within the properties file backslashes are not used. All slashes in this file are represented as forward slashes (/) instead.
- Step 6** The keystore password that you chose in [Step 4](#) must now be stored in the PanOS password store. Use the pwstore.bat utility in “C:\Program Files\PanOS Platform\bin” to add the password using the “key keystore.key”:
- ```
C:\Program Files\PanGo PanOS Server\bin>pwstore.bat -add -key keystore.key
```
- Ensure that you specify the same password you used in [Step 4](#).
- Step 7** Restart the PanOS service that was stopped in [Step 1](#).
- Step 8** Verify that HTTPS is configured correctly and is now available by accessing “https://hostname:port”.

Accessing Locator Applications

Each of the web applications that comprise PanGo Locator can be accessed from one another. When logged into PanGo Monitor, for example, access to PanGo Notifier is available from the menu bar to users with appropriate privileges. There is no need to logout and login again.

Direct access using HTTPS to any of the Locator web applications is available from the client browser using URLs of the form shown in [Table 3](#).

Table 3 Direct Access URLs for PanGo Locator

Application	Web Browser URL
Monitor	https://PanOS-System/monitor/
Notifier	https://PanOS-System/notifier/

Table 3 Direct Access URLs for PanGo Locator

Reporting Application	https://PanOS-System/reporting/
User Manager Application	https://PanOS-System/usermanager/
Location Manager	https://PanOS-System/LocationManager/

Replace *PanOS-System* with the IP address or fully qualified domain name of the PanOS server. These URLs facilitate the use of multiple browser windows when using more than a single PanGo Locator web application simultaneously.

PanOS Server Location Appliance Polling

When the PanOS service is started on the PanOS server, it obtains the following information from the location appliance via the SOAP/XML API:

- All client stations and asset tags the location appliance is tracking
- All network designs contained in the location appliance
- All floor maps contained in the location appliance

By default, PanOS queries the location appliance via the SOAP/XML API every 60 seconds. During this query, PanOS queries the location appliance for newly-added or modified:

- Client station location coordinates
- Asset tag location coordinates
- Network designs and floor maps

For information pertaining to the deletion of location appliance network designs and maps, see [Location Appliance Network Design and Map Deletions, page 68](#).

The default 60-second polling interval can be changed if desired. To do so, modify the `poll.interval` parameter contained in the `.\PanGo\PanGo PanOS Server\provider-cisco-1.properties` file. You must stop and restart the PanOS server for this parameter change to take effect.

If a critical additions or modifications have been made to location appliance network designs and maps, re-synchronization of the PanOS databases can be forced by stopping and re-starting the PanOS server. While this is seldom required with the default polling interval, this technique can prove useful if the polling interval has been extended.

Monitoring Assets

PanGo Locator Monitor displays PanGo tags, non-PanGo Wi-Fi tags, and Wi-Fi WLAN clients using a wide variety of assigned icons. When the PanOS service is started on the server, it requests the location of all devices of which the location appliance is currently aware. By default, it polls the location appliance for any changes that have occurred every 60 seconds. These updated device locations are shown in PanGo Locator Monitor in both a graphical and tabular format as seen at the beginning of this document in [Figure 7](#).

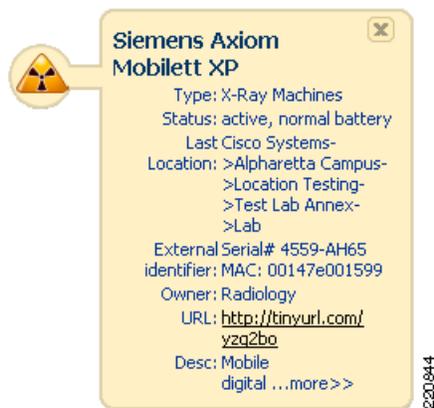
If the Cisco location appliance no longer provides location information for a device to PanOS server, the following occurs:

- PanOS server applies a “grace period” of 20 minutes, during which time the device icon continues to remain displayed “In Location”, as shown in [Figure 45](#).

Figure 45 Device “In Location”

- If the location appliance resumes providing location information for the device to PanOS Server before the expiration of the grace period, the device continues to be displayed “In Location”. If the device location has changed, the “In Location” time is reset and the device is located at the new map coordinates.

If the location appliance does not resume providing location information for the device and the grace period expires, the status information for the device is updated to indicate that the location indicated on the map is the “Last Location” known for the device, as shown in [Figure 46](#).

Figure 46 Device “Last Location”

Subsequently, the icon representing the device is removed from the monitor display according to an expiration timer as follows:

1. For PanGo RSSI mode tags, the timer defaults to 720 minutes.
2. For PanGo chirp mode tags that have successfully completed stage two of initialization or otherwise have established a TCP session to the PanOS server at least once, the timer defaults to 720 minutes.
3. For PanGo chirp mode tags that have never established a TCP session with the PanOS server (for example, tags that have been manually configured via the CLI for chirp mode immediately after delivery), the timer defaults to 120 minutes.
4. For non-PanGo Layer 2 multicasting Wi-Fi asset tags, this timer value defaults to 120 minutes.
5. For all Wi-Fi WLAN clients, this timer value defaults to 120 minutes.

In some cases, it may be desirable to modify the expiration timer values. This can be done as follows:

- For cases involving PanGo tags as shown in items 1. and 2. above, modify the following parameter value accordingly in the `devicetype-pango-tag.properties` file located in the `/PanGo/PanOS Platform/conf/typeloader` directory on the PanOS server:

```
expiration.time.minutes = 720
```

- For the case involving PanGo tags shown above in item 3., or the case involving non-PanGo Wi-Fi tags shown in item 4., modify the following parameter value accordingly in the `devicetype-wifi-tag.properties` file located in the `/PanGo/PanOS Platform/conf/typeloader` directory on the PanOS server:

```
expiration.time.minutes = 120
```

- For cases involving Wi-Fi WLAN clients as shown in item 5. above, modify the following parameter value accordingly in the `devicetype-wifi-stations.properties` file located in the `/PanGo/PanOS Platform/conf/typeloader` directory on the PanOS server:

```
expiration.time.minutes = 120
```

After saving your changes to these files, the PanOS Platform service on the PanOS server must be stopped and restarted for the changes to take effect.

Note that once detected, PanGo Locator does not allow *any* type of asset tag or Wi-Fi client device to be manually deleted.

Unassigned Devices

As described in [PanGo PanOS Server and PanGo Locator, page 9](#) and [PanGo Locator and Cisco WCS, page 14](#), PanGo Locator is designed to facilitate the tracking of assets (not necessarily asset tags) by the users and owners of those assets. Keeping that in mind, be aware that PanGo Locator does not display the location of tags or WLAN clients whose MAC addresses have not been assigned to actual assets via the Locator Configuration utility. Rather, these and any other devices are found in the “Unassigned” subfolder of their respective device folders in Locator Configuration. An example of unassigned PanGo asset tags can be seen in the red rectangle in [Figure 47](#).

Figure 47 Example of Unassigned PanGo Tags

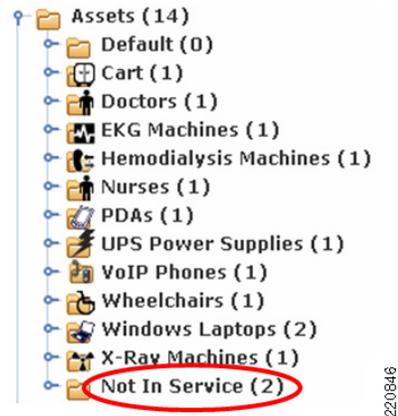


Assigning these devices to assets removes them from the “Unassigned” subfolder and places them into the “Assigned” subfolder for that device category. PanGo Locator then begins displaying the location of the asset to which the device MAC address has been assigned.

PanGo Locator does not allow for assets, once defined to the system, to be deleted. The asset can be edited or moved amongst asset categories, but it cannot be deleted from the system altogether.

At times, the retention of asset definitions that are no longer in service may prove to be a bit cumbersome. To better manage this, it is recommended that a separate asset type be created for assets no longer in active service (that is, “Not In Service”) and that all such unused assets be assigned to this category, as shown in [Figure 48](#).

Figure 48 “Not In Service” Category for Unused Assets



Tag MAC Address Identification

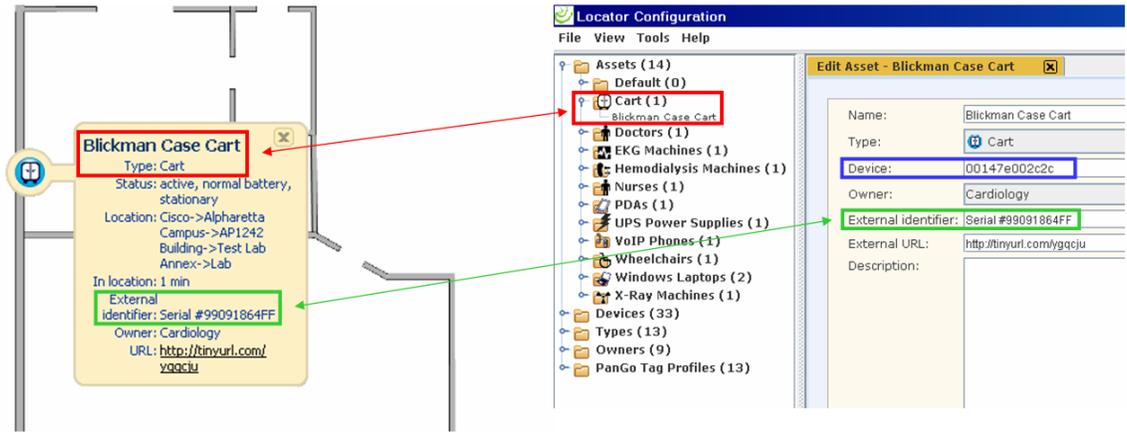
PanGo Locator Monitor typically allows assets to be identified by asset characteristics such as asset name, type, owner, and external identifier information such as its serial number. Locator Monitor makes it possible to search for active assets based on its name, description, external identifier, or any part of these fields. Because Locator is designed to manage assets and not necessarily asset tags, tag hardware identification (MAC address) is not included in Locator Monitor when viewing asset detail.

For most users of PanGo Locator, the fact that the assigned tag MAC address is not included as a search field does not prove to be a handicap, because their primary interest is the management of assets, and not asset tags per se. Thus, they identify the assets they are searching for by the asset type, name, or serial number for example.

However, administrators of the asset tracking system (or IT professionals involved with optimizing or debugging) may prefer having the ability to correlate assets with the tags attached to them. In some cases, the assigned tag MAC address may be the only piece of reliable and unique information known about a particular asset.

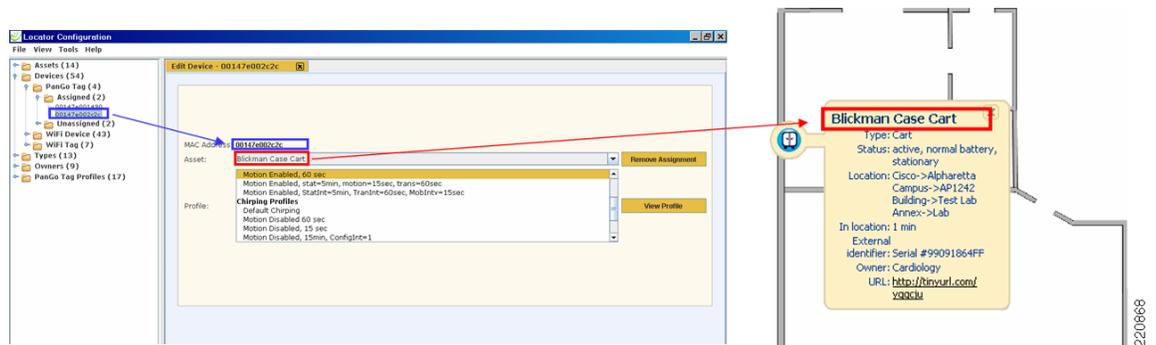
For administrators with access to the PanGo Locator Configuration utility, the correlation of an asset name in PanGo Locator Monitor to the MAC address of the attached asset tag in the PanGo Locator Configuration utility can easily be made in just a few steps. With both applications open on the desktop, the asset shown in Locator Monitor can be manually identified in the Locator Configuration utility, as shown by the red and green rectangles in [Figure 49](#). Once identified, the assigned asset tag MAC address can be seen as the assigned device (the blue rectangle in [Figure 49](#)).

Figure 49 Matching an Asset with an Asset Tag MAC Address



However, at times it may be necessary to search for the asset to which a particular tag MAC address has been assigned. The Locator Configuration utility allows for all tag MAC addresses to be displayed as a list and the desired tag MAC address can then be located on the list. Double-clicking the MAC address of interest brings up its edit panel, where the asset name that has been assigned to this MAC address can be found, as shown in Figure 50. This asset name can then be used to search for the asset in PanGo Locator Monitor.

Figure 50 Matching a Tag MAC Address with an Asset Name



The process of correlating asset names with assigned tag MAC addresses (and vice versa) can be significantly simplified if a few extra steps are taken during the initial asset definition and assignment process. These steps significantly enhance the information contained in the pop-up bubble on Locator Monitor such that it includes the assigned tag MAC address. To do this, when assigning a tag MAC address to an asset using the Locator Configuration utility, copy and paste the MAC address of the assigned tag from the device field to the external identifier field of the asset definition.

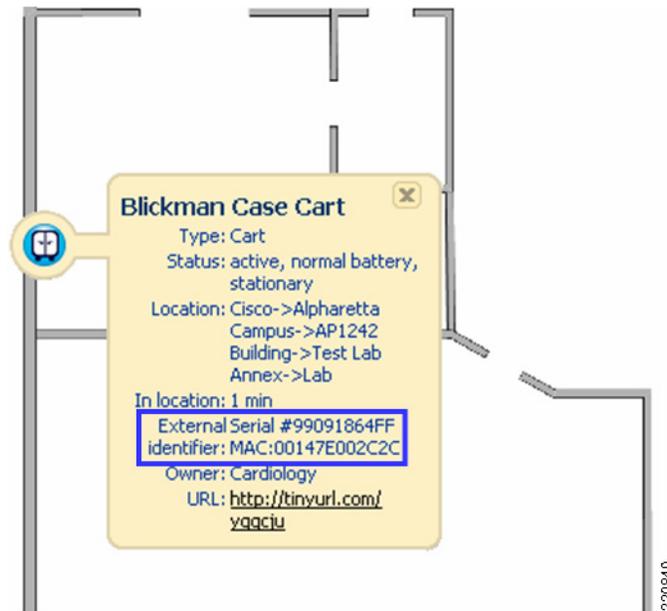


Note

The Locator Configuration utility does not provide the ability to paste via right-click or the standard Windows Edit drop-down menu. Use CTRL+V to paste when using the Locator Configuration utility.

The benefit of adding the MAC address to the external identifier field can be clearly seen in Figure 51. Note that adding the MAC address to the external identifier field does not preclude using the field to contain other information, such as the asset serial number.

Figure 51 Results of Including Tag MAC Address in External Identifier



This approach affords all users, not just those with access to the Locator Configuration utility (which should not be made available to the general user population) with the ability to easily cross-reference an asset by its assigned tag MAC address. In addition, including the tag MAC address in the external identifier field in this manner allows the user to search for active assets in PanGo Locator Monitor using any portion of the tag MAC address.

PanGo Locator does not currently provide a mechanism to dynamically link the external identifier field to the tag MAC address. Therefore, if the asset is reassigned to a different asset tag, the MAC address that was pasted into the external identifier field must be manually updated.

Defining Maps

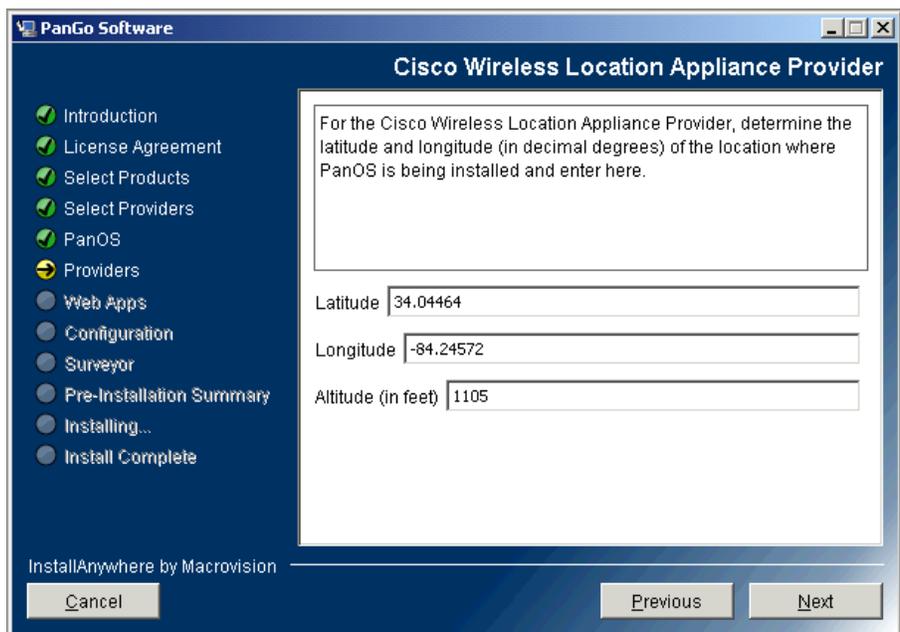
As shown in [Figure 6](#), the PanGo PanOS Server can display asset locations received from one of several different location providers, with the focus in this paper being the Cisco location appliance. Different location providers may represent asset location using a variety of means; for example, local Cartesian coordinates, global coordinates, or named locations. Because of this, PanGo PanOS internally converts the reported location from its location providers to a worldwide geodetic system using longitude, latitude, and altitude global coordinates.

PanOS uses the World Geodetic System (WGS-84) to define a fixed global reference frame for all points on earth. WGS-84 was defined in 1984 and last revised in 2004. To uniquely identify any point on any map, global coordinates are calculated using a combination of WGS-84 map anchor coordinates and local Cartesian offsets.

This approach considers the upper left corner of any map as the *map origin* or the (0,0) local coordinate point of that map. By associating a latitude, longitude, and altitude with the map origin, the map becomes anchored to a precise location in the real world. By combining the local Cartesian offset of any point on a map with the geodetic coordinates of the map origin, PanOS is capable of representing any location uniquely in the world geodetic system.

During the installation of the PanGo PanOS Server, the installation wizard prompts for the latitude, longitude, and altitude coordinates of the Cisco location appliance, as shown in [Figure 52](#).

Figure 52 Specifying Location Appliance Origin Coordinates



In the integrated Cisco-PanGo solution, the location appliance coordinates specified during installation shown in [Figure 52](#) serve as the provider origin for this location appliance. In a location appliance that contains a single campus design (one campus map), the provider origin is assigned as the map origin of the campus map (the top level map) transferred from the location appliance to the PanOS server. The origins of all lower level elements (buildings, floors, and outdoor areas) are then calculated using offsets specified by the location appliance relative to the top-level map origin.

Because of this inter-relationship, the provider origin specified for the location appliance should always represent the map origin of the campus map. A common mistake is to specify instead the global coordinates of where the location appliance hardware happens to be physically situated for the provider origin. This is incorrect, unless of course the two happen to coincide.

If the incorrect coordinates for the location appliance are specified during installation, they can be corrected as follows:

1. Open the file named `provider-cisco-offsets.properties` located in the PanOS installation directory (typically found under the `\PanGo PanOS Server\conf` directory).
2. Enter the correct unit of measure for `provider.origin.units`.
3. Enter the correct values for `provider.origin.latitude`, `provider.origin.longitude`, and `provider.origin.altitude`.
4. Save the file, then stop and restart the PanOS service or reboot the PanOS server.

Single Campus Designs

The single campus design is probably the most common enterprise model, and typically consists of a single top-level campus map with one or more buildings that have been placed on the campus using WCS Map Editor. Each building has one or more floor maps defined to it.

In this design, the geodetic coordinates specified for the provider origin using the installation screen in [Figure 52](#) should always be the latitude, longitude, and altitude associated with the map origin of the campus. In the example shown in [Figure 53](#), the origin of the campus map is the location at the extreme topmost left hand corner, illustrated by the red crosshair.

**Note**

Crosshairs appear here for illustrative purposes only and are not displayed when using the actual WCS Map Editor.

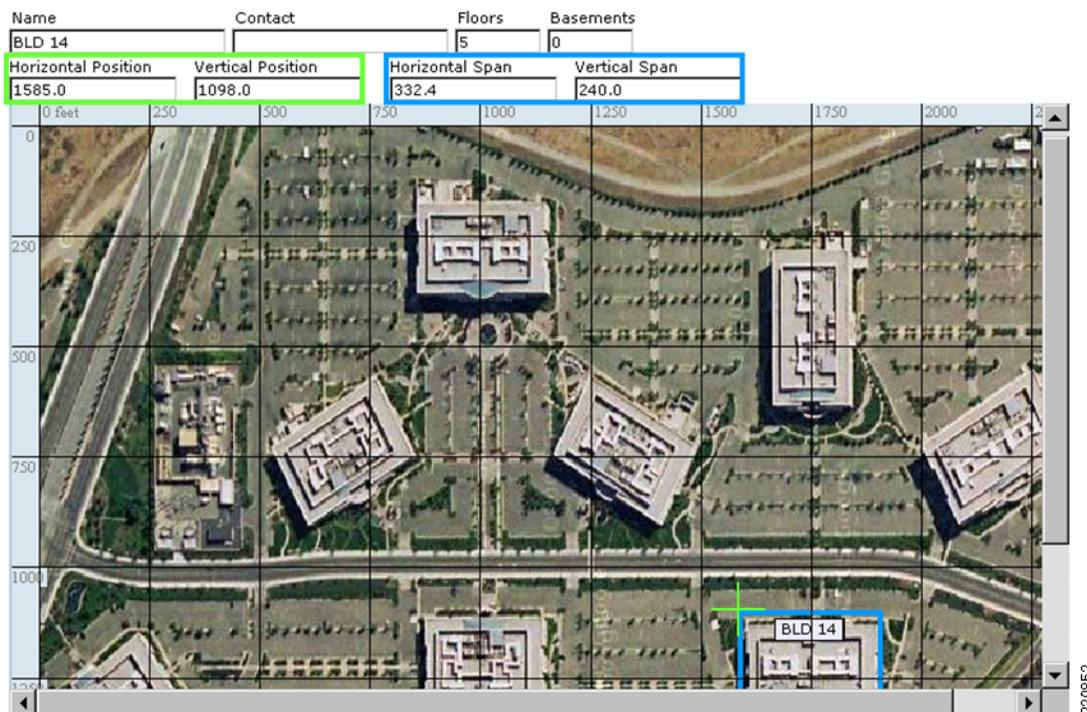
Figure 53 *Campus and Building Map Origins*



Buildings on the campus are located in the real world geodetic system by combining the global coordinates for the campus map origin with the local Cartesian offset of the building map origin (building map origin for Building 14 is shown in [Figure 53](#) and [Figure 54](#) by the green crosshair).

The local (x,y) offset of each building map origin is automatically calculated by WCS when the building is placed on the campus map. This is shown in [Figure 54](#), where the calculated value of the building map origin offset can be seen in the green rectangle.

Figure 54 Local Cartesian Building Offsets



Note Crosshairs and color-coded rectangles appear here for illustrative purposes only and are not displayed when using the actual WCS Map Editor.

Note that WCS does not allow for the specification of building altitude. Therefore, all buildings placed on the campus map are assumed to be at the same altitude as the campus map origin.

The horizontal and vertical position values shown in Figure 54 correspond to the location indicated by the green crosshair. These local offsets are passed to the PanGo PanOS Server during periodic network design synchronization between the server and the location appliance.

To assure that buildings are assigned the proper global coordinates by PanOS, Cisco recommends that buildings be accurately placed using the WCS Map Editor. When this is done, the WCS Map Editor calculates the correct offset values for each building based on where the building is located on the map. This procedure ensures that the horizontal and vertical span of each building is accounted for and that each building is uniquely identified on the campus map.

Floor maps are anchored in PanOS in much the same fashion. The origin for a floor is assumed to have the same global coordinates as the origin of the building it is contained within plus any local Cartesian offsets that may apply to the floor.

By using the drag-and-drop method of locating the floor within WCS Map Editor (illustrated in Figure 55), the floor span as well as any applicable offsets (x,y,z) are automatically computed. PanOS calculates the z offset (altitude) of each floor map using the floor height (red rectangle in Figure 55), number of floors in the building, and the following formulae:

- For ground level and above floors ($\text{Floor}_{\text{NUM}} > 0$)

$$\text{Altitude}_{\text{FLOOR}} = \text{Altitude}_{\text{MAPORIGIN}} + ((\text{Floor}_{\text{NUM}} - 1) * \text{Height}_{\text{FLOOR}})$$
- For basements ($\text{Floor}_{\text{NUM}} < 0$)

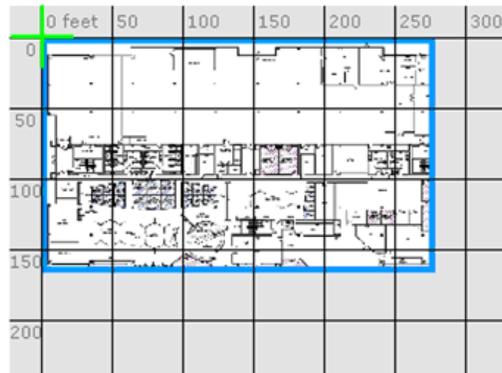
$$\text{Altitude}_{\text{FLOOR}} = \text{Altitude}_{\text{MAPORIGIN}} + (\text{Floor}_{\text{NUM}} * \text{Height}_{\text{FLOOR}})$$

Figure 55 Local Cartesian Floor Coordinates

BLD 14 > Edit Floor Area '1st floor'

Floor Area Name	<input type="text" value="1st floor"/>
Contact	<input type="text"/>
Floor	<input type="text" value="1"/>
Floor Height (feet)	<input type="text" value="10.0"/>
Floor Type(RF Model)	<input type="text" value="Cubes And Walled Offices"/>
Existing	
Image File	domain_0_1128643014546.gif
Import New	
FPE File	<input type="checkbox"/>
Image File	<input checked="" type="checkbox"/> <input type="text"/>
	<input type="checkbox"/> Maintain Aspect Ratio
Dimensions (feet)	
Horizontal Span	<input type="text" value="278.9"/>
Vertical Span	<input type="text" value="166.5"/>
Coordinates of top left corner (feet)	
Horizontal Position	<input type="text" value="0"/>
Vertical Position	<input type="text" value="0"/>

Total Floor Area Size (sq. feet) :46221.5



2200953

For example, assume the case where the altitude specified for the location appliance is 1500 feet above sea level (ASL) and a building possesses a uniform floor height of ten feet. In this case, the first floor of the building has an indicated altitude in PanGo Location Manager of 1500 feet ASL, whereas the second floor has an altitude of 1510 feet ASL. The basement of the same building has an indicated altitude of 1490 feet ASL.

Note that the floor offsets in [Figure 55](#) are zero, indicating that the floor offset is the same as the building offset, with structural wall and framework thicknesses representing numerically negligible quantities. Although this is common, it is not always the case, because some floors may occupy only a portion of the available building footprint. Therefore, accurate representation of the floor location is recommended for proper geodetic placement.

Multiple Campuses

Some enterprise environments may contain two or more independent campuses where the total count of Wi-Fi clients and asset tags is easily accommodated by the device tracking capacity of a single location appliance. In such cases, network designs for each of the campuses may co-reside in a single location appliance.

When using a Cisco location appliance containing multiple campus-level network designs, additional steps are necessary to offset the map origins of campuses apart from each other. This is necessary to ensure that the campuses do not overlap when they are placed in the world geodetic system.

To accomplish this, the map origin of one of the campuses is chosen as the provider origin for the location appliance. This can be entered during installation via the menu panel shown in [Figure 52](#), or can be entered manually using the procedure described in the previous section. All other campuses must then be offset from the provider origin.

For example, assume two campus network designs (assigned names Campus1 and Campus2 in WCS) are defined in the location appliance, with the origin of Campus2 being physically located two miles east and one mile north of the origin of Campus1. When the PanOS Server is installed, the provider origin specified corresponds to the origin of Campus1. For PanOS to properly anchor the location of Campus2, it is necessary to provide the distance offset information (in the units of measure used by the location appliance) between the provider origin and the origin of Campus2.

This offset information is provided in the PanGo PanOS Server via the use of the `provider-cisco-offsets.properties` file that is located in the PanOS installation directory under `\PanGo PanOS Server\conf`. To offset Campus2 from the provider origin, add the name of the campus (taken from WCS) requiring the offset to the properties file, followed by its x,y offset from the provider origin.

Because the provider origin is the same as the origin of Campus1, an offset need only be specified for the map origin of Campus2. The correct entry in the `cisco-offsets.properties` file would appear as follows:

```
Campus2 = 10560, 5280
```

Note that offsets must be specified in the units of measure configured in the location appliance. In the case of our example, the offset information must be entered in feet. When entering campus offset information for campuses that are directly adjacent or otherwise very near to each other, ensure that the physical size and span of each campus is accounted for, and there is no accidental overlap.

In some cases, the campuses managed by a single location appliance may be geographically distant and the correct distance offsets may not be obvious or easily determined from simple map measurements. In such cases, the following conversion can be used to find the approximate distance between two points when the correct latitude and longitude is known in decimal degrees.

Assume:

- LAT_A = Latitude of campus A map origin in decimal degrees
- LON_A = Longitude of campus A map origin in decimal degrees
- LAT_B = Latitude of campus B map origin in decimal degrees
- LON_B = Longitude of campus B map origin in decimal degrees

Then:

$$\Delta\text{Lat-Dist}_{\text{meters}} = (LAT_B - LAT_A) * 111,300$$

$$\Delta\text{Lon-Dist}_{\text{meters}} = (LON_B - LON_A) * 85,300$$

$$\Delta\text{Lat-Dist}_{\text{feet}} = (LAT_B - LAT_A) * 365,153$$

$$\Delta\text{Lon-Dist}_{\text{feet}} = (LON_B - LON_A) * 279,853$$

The assumption is made that the Earth is spherical but that the distances between points of concern are small enough that the route traversed can be considered flat. The (x,y) offset of campus B from campus A can then be thought of as (Δ Lon-Dist, Δ Lat-Dist).

When entering campus names and offset information into the provider-cisco-offsets.properties file, any special characters (such as a space, ‘:’ or ‘=’) in the names of the campuses must be encapsulated by escape characters. For further details, refer to the comments contained at the beginning of the cisco-offset.properties files themselves.

Standalone Building Designs

When using WCS to create network designs for the integrated Cisco/PanGo asset tracking solution, it is recommended that buildings *always* be placed on campuses and not created as standalone entities.

The rationale behind this recommendation is straightforward. A building placed on a campus automatically has Cartesian offsets calculated, whereas “standalone buildings” (buildings not placed on a campus) do not. All standalone building designs will have the same map origin (which is equal to the provider origin) and overlap in the PanOS server. Therefore, if more than one standalone building is resident in the location appliance, manual offsetting of the standalone buildings (as described in the previous section for multiple campuses) is required.

Defining Physical Locations

In the integrated Cisco/PanGo asset tracking solution, the PanGo PanOS Server considers itself to be the “locator of origin” for the devices it tracks via its location providers. Because of this, the following tasks must be performed using PanGo Location Manager before being able to display asset location:

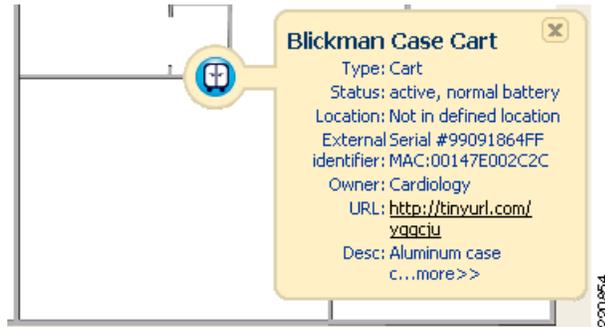
- A physical location hierarchy must be defined within PanOS.
- Maps (supplied by the location appliance) must be applied to the appropriate levels of the physical location hierarchy.
- Discrete areas on maps (known as *spaces*) representing the lowest level in the physical location hierarchy must be defined. These areas are used by PanOS and Locator to display tracked assets.

These three tasks *must* be performed using the PanGo Location Manager regardless of whether similar tasks have already been performed using WCS and the location appliance, such as the following:

- Definition of campuses, buildings, or floors
- Application of maps to their respective floors
- Definition of coverage areas using the WCS Map Editor

In some cases, defined spaces may not encompass all areas on a floor map. If the system calculates asset location as being in an area not currently assigned to a defined space, the asset is indicated as “not in defined location”. This situation is shown in [Figure 56](#), where the system has located a tagged asset in a doorway that was accidentally not included in either of the rooms adjacent to it.

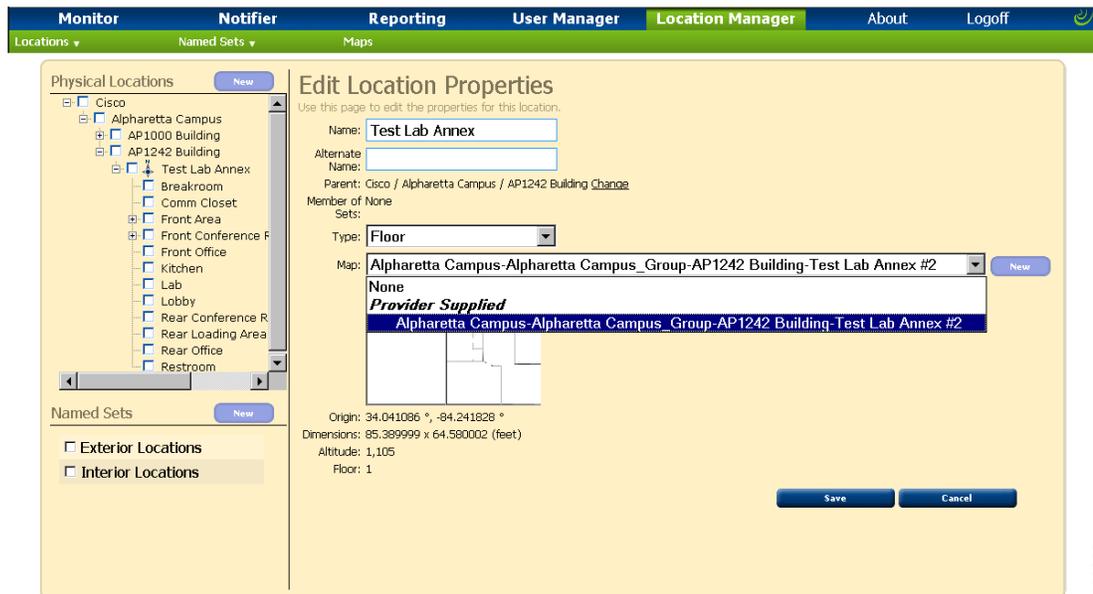
Figure 56 *Asset Not in Defined Location*



Chapter 3 of the *PanGo Locator Administrator's Guide* fully describes how to set up physical location hierarchies, define maps, and specify spaces. Keep in mind that there is no need to create new maps in PanGo Location Manager. Rather, maps that have been acquired from the location appliance during periodic synchronizations (see [PanOS Server Location Appliance Polling, page 56](#)) can now be selected and applied.

[Figure 57](#) shows how the application of a map received from the location appliance is applied to the PanGo physical location hierarchy at the floor level.

Figure 57 *Applying Provider-Supplied Floor Maps to the Location Hierarchy*



Location Appliance Network Design and Map Deletions

The addition or modification of location appliance network designs and maps are automatically reflected in the PanGo physical location hierarchy. However, deletions of any location appliance map, campus, building, or floor will require manual application using PanGo Location Manager. This is because when the PanOS server periodically synchronizes to the location appliance (as described in [PanOS Server](#)

Location Appliance Polling, page 56), only newly-added (or modified existing) location appliance maps and network designs are transferred. PanOS does not automatically synchronize its databases with network design and map deletions that have been made to the location appliance.

Map deletion in the PanOS Server can be performed by selecting **Maps** from the Location Manager taskbar and then clicking the “X” in the “Delete” column on the right side of the screen for the appropriate map to be deleted, as shown in Figure 58.

Figure 58 Location Manager Map Listing

Name	Source	Location	Origin (lat, long)	Altitude	Floor Delete
Alpharetta Campus-Alpharetta Campus-Group-AP1000 Building-Test Lab Annex	Provider	Test Lab	34.04158, -84.241948	1,105.00	1 X
Alpharetta Campus-Alpharetta Campus-Group-AP1242 Building-Test Lab Annex #2	Provider	Test Lab Annex	34.041086, -84.241828	1,105.00	1 X
Alpharetta Campus-Alpharetta Campus-Group-Experimental Building-Basement	Provider	Basement	34.041282, -84.241584	1,095.00	-1 X
Alpharetta Campus-Alpharetta Campus-Group-Experimental Building-Floor 1	Provider	Floor 1	34.041282, -84.241584	1,105.00	1 X
Alpharetta Campus-Alpharetta Campus-Group-Experimental Building-Floor 2	Provider	Floor 2	34.041282, -84.241584	1,115.00	2 X
Alpharetta Campus-Alpharetta Campus-Group-Experimental Building-Floor 3	Provider	Floor 3	34.041282, -84.241584	1,125.00	3 X
Alpharetta Campus-Alpharetta Campus-Group-Experimental Building-Sub-Basement	Provider	Sub-Basement	34.041282, -84.241584	1,085.00	-2 X

Manual deletions of building, campuses, or floors is accomplished in Location Manager by first selecting the level of the physical location hierarchy you wish to delete from the tree listing. Then, choose Locations > Delete Selected, as shown by the red arrow in Figure 59.

Figure 59 Deleting a Physical Location

The screenshot shows the 'Edit Location Properties' dialog box with the following fields:

- Name: AP1000 Building
- Alternate Name: (empty)
- Parent: Cisco Systems / Alpharetta Campus Change
- Member of Sets: None
- Type: Building

A red arrow points to the 'Delete Selected' option in the 'Locations' dropdown menu.

Use of Multiple Location Appliances

In some large enterprise environments, the number of tracked assets may exceed the tracked device capacity of the Cisco location appliance. The potential for this to occur is increased if the location appliance is used to track rogue access points and rogue clients.

The maximum supported asset tracking capacity of PanGo Locator v4.5 is reported by PanGo Networks as being 5000 tracked assets (WLAN clients and assets equipped with asset tags only).

If the following is assumed:

$LOC_{NETMAXASSET}$ = Location appliance maximum asset tracking capacity (tags and clients)

$LOC_{MAXTRACKED}$ = Location appliance maximum tracked device capacity

$AP_{MAXROGUE}$ = Maximum anticipated rogue APs tracked

$Clients_{MAXROGUE}$ = Maximum anticipated rogue clients tracked

Then the anticipated maximum net asset tracking capacity of the Cisco location appliance can be stated as the following:

$$LOC_{NETMAXASSET} = LOC_{MAXTRACKED} - (AP_{MAXROGUE} + Clients_{MAXROGUE})$$

In the case where location tracking of rogue access points and clients is disabled, $AP_{MAXROGUE} = Clients_{MAXROGUE} = 0$, which simplifies the equation to the following:

$$LOC_{NETMAXASSET} = LOC_{MAXTRACKED} = 2500$$

In the case where location tracking of rogues is enabled, $LOC_{NETMAXASSET}$ is likely to be less than 2500.

From this, you can reasonably draw the conclusion that each paired instance of PanGo Locator and the PanOS Server is capable of accepting location information and tracking the devices contained in two Cisco location appliances. Although from a purely technical standpoint this relationship is based on the $LOC_{NETMAXASSET}$ of each location appliance, for planning and design purposes it is recommended that this 2:1 relationship between the number of location appliance and PanOS/Locator always be observed. Doing so ensures that the capabilities of the PanGo Location client are not exceeded by the combined tracked device capacity of its Cisco location providers.

In cases where it is necessary to track more than 5000 assets, multiple PanOS servers can be installed, each with its own independent set of web-enabled applications (PanGo Locator). As described earlier, each of these PanOS servers can then be paired with two Cisco location appliances. In this fashion, large deployments can be segmented into smaller portions of 5000 assets or less.

PanGo PanOS views each Cisco location appliance defined to it as a separate location provider. Because of this, in a multiple appliance configuration, each location appliance must be configured separately via its own PanOS properties file and its own entry in the PanOS provider registry.

Note that the definition of multiple location appliances to a single PanGo location client is not recommended as a redundancy solution. The PanGo PanOS Server operates under the assumption that tracked devices are not reported by more than one Cisco location provider. In the event that the same tracked device is reported by more than one location appliance, the information from the location appliance with order precedence in the provider registry will dominate. In this event, the dominating location appliance may (or may not) be the location appliance actually having the most up-to-date location coordinates for the device.

Notifications

As mentioned in [PanGo Locator Web Applications, page 11](#), PanGo Locator possesses the capability to issue e-mail-based notifications to one or more recipients via its the PanGo Notifier component. The following categories of e-mail notifications can be generated:

- Tag state change events—A tag state change event notification is triggered when a tag indicates that there has been a change in state. The supported states vary depending on whether the tag is configured in RSSI or chirp mode.

Both chirp mode and RSSI mode tags support the following tag state events:

1. Failure to Report
2. Low Power Shutdown

Lab testing has validated that RSSI mode tags can generate the following tag state events:

3. Device Motion Started
4. Device Motion Stopped
5. Low Battery
6. Unqualified Shutdown
7. Device Error Shutdown

Note that events 3. through 7. are not currently supported in chirp mode.

- Location-based notifications—Location-based notifications are triggered when assets enter or exit specific spaces or groups of spaces that have been defined on maps by the PanGo Location Space Editor. Location-based notifications are functional with tags in either chirp or RSSI mode. When using location-based notifications, the application of a smoothing factor in the location appliance (Location > Location Servers > Administration > Location Parameters) helps minimize the amount of random “jitter” seen in the displayed device location. This in turn reduces the number of “false alarms” seen when using location entry and exit notifications. Smoothing factors are enabled by default in the location appliance, and the degree of smoothing can be modified to suit the particular deployment situation.
- Count-based notifications—Count-based notifications are triggered when the number of assets detected by the PanGo location client rises above or drops below pre-defined thresholds for a specific space or groups of spaces. Count-based notifications are functional with tags in either chirp or RSSI mode. Because count-based notifications use the same fundamental mechanisms as location-based notifications, the use of smoothing factors can be of value in minimizing the number of “false alarms” that occur because of random location jitter.

PanGo Notifier offers a multitude of flexible notification options including the following:

- Managing notifications and e-mail recipients independently
- Configuring valid notification times on both a daily and hourly basis
- Assigning notifications to assets based on asset name, owner, type, or external identifier
- Using runtime variables in the message subject and body fields of e-mail notifications to convey customized, per-asset meaning in each notification
- Tracking the history of the last ten notifications issued and a per-category count of notifications category issued since the last system start

Complete documentation regarding the configuration of PanGo Locator Notifier can be found in Chapter 4 of the *PanGo Locator User’s Guide*, available on the PanGo PanOS installation CD or from your PanGo representative.

In addition to the capabilities afforded by PanGo Locator Notifier, the Cisco location appliance also offers the ability to generate complementary location and event notifications, but with the option of using SOAP/XML, SNMP, or Syslog (in addition to SMTP) as a transport. This would be useful, for example, if it is necessary to send battery status or other location notifications pertaining to PanGo v2 tags to an enterprise management system such as CiscoWorks, Tivoli, or OpenView using SNMP, or to log this information to an enterprise syslog server.

Caveats

Known Caveats

The following documents should be consulted for known caveats that may affect your design and/or deployment efforts:

- Cisco 4400 Wireless LAN Controller (4.0.206.0) and Cisco Aironet AIR-LAP1242AG Access Points— <http://www.cisco.com/en/US/docs/wireless/controller/release/notes/cont402060rn.html>
- Cisco Wireless Control System software 4.0.96.0—
http://www.cisco.com/en/US/docs/wireless/wcs/release/notes/wcsrn_MR2.html

In addition, updated information regarding recent product bugs are available to registered Cisco Connection Online users via the Cisco Bug ToolKit, available at the following URL:
http://www.cisco.com/en/US/support/tsd_most_requested_tools.html.

The hardware and software described above in [Known Caveats, page 72](#) was used in conjunction with the following products from PanGo Networks:

- PanGo Locator and PanOS version 4.5
- PanGo LAN Tags version 2 (MIPS firmware 2.1.5, microcode 87.68)

Contact your PanGo technical representative for any known caveats with regard to these products.

Additional Caveats

In addition to the information available from the sources mentioned, the following behaviors were observed during laboratory validation of the information presented in this document, using the previously-mentioned Cisco hardware and software.

Chirp Mode Tags Using OTA Update May Not Be Detected By All APs

If a PanGo v2 tag in chirp mode uses periodic over-the-air update, after the update has concluded, Layer 2 multicasts may not be forwarded by the access point to which the tag had associated. This condition is temporary and has been seen to occur for a time period equal to the client timeout of the controller. During this time period, reduced location accuracy may result.

Workaround

Suspend use of the over-the-air configuration capability (see [Appendix D—Suspending Over-The-Air Configuration Updates, page 80](#)).

AP1210/1220/123x Access Points May Not Reliably Detect Chirp Mode Tags

If PanGo v2 tags in chirp mode are used with Cisco Aironet Access Point models AP1210, 1220, or 1230, a condition may arise in the access points where multicasts received from tags are no longer forwarded to the WLAN controller. This condition has been seen to occur (but is not limited to) situations where the access points in question are disconnected from the WLC and then subsequently reconnected and allow to reload and re-register.

Symptoms of this issue include but may not be limited to the following:

- Known functional chirp mode tags missing from the output of the **show rfid summary** controller CLI command.
- Known functional access points deployed at close-range to known functional chirp mode tags are seen as missing from the output of the **show rfid client detail <mac-address>** controller CLI command.

Workaround

None at this time. This caveat is targeted for resolution in an upcoming maintenance release. Consult your local Cisco technical representative or the Cisco Technical Assistance Center regarding the availability of a controller software upgrade to resolve this caveat (CSCsi15393).

Chirp Mode Tags Using OTA Update May Vary Transmit Power With DTPC

This caveat affects PanGo v2 tags in chirp mode that use periodic over-the-air update and either probe or associate to a static WEP WLAN on a controller with DTPC enabled. The first group of L2 multicast packets transmitted after the completion of the over-the-air configuration update may be sent at the current transmit output power level established by DTPC and not the configured tag transmit power. Subsequent L2 multicasts are sent at the configured tag transmit power level. Depending on the transmit power conveyed by DTPC at the time, a short-term shift in reported location may be noticed.

Workaround

Suspend use of the over-the-air configuration capability (see [Appendix D—Suspending Over-The-Air Configuration Updates, page 80](#)).

Chirp Mode Multicast Frames May Vary In Transmitted Signal Strength

It has been noticed in testing that the first one, two, or in some cases even three multicast frames transmitted per burst by a PanGo v2 chirp mode tag can vary significantly in signal strength as compared to subsequent frames. This behavior can degrade location accuracy depending on several factors, including the following:

- Number of frames per burst that are affected
- Magnitude of this variation as compared to other frames comprising the same burst
- Degree to which all frames per burst are reliably detected by nearby access points (thereby impacting average detected RSSI)

Workaround

The impact of this caveat can be reduced by increasing the number of frames transmitted per burst using the **chirpcount** CLI command from the default of 5 to a new value of 10 or more. However, be aware that increasing the number of frames per burst reduces the overall tag battery life.

Tags May Appear As Two Tracked Devices in Location Appliance

If a PanGo v2 tag in chirp mode uses periodic over-the-air update and either probes or associates to a static WEP WLAN defined to controllers polled by the location appliance, it is tallied as two tracked devices (RFID tag and WLAN client) toward the maximum tracked device capacity of the location

appliance. Depending on the number of chirp mode tags in your environment as well as the total number of devices being tracked by your location appliance, this may result in a reduction in the tracked device capacity of the location appliance for a period of 24 hours or longer.

Workaround

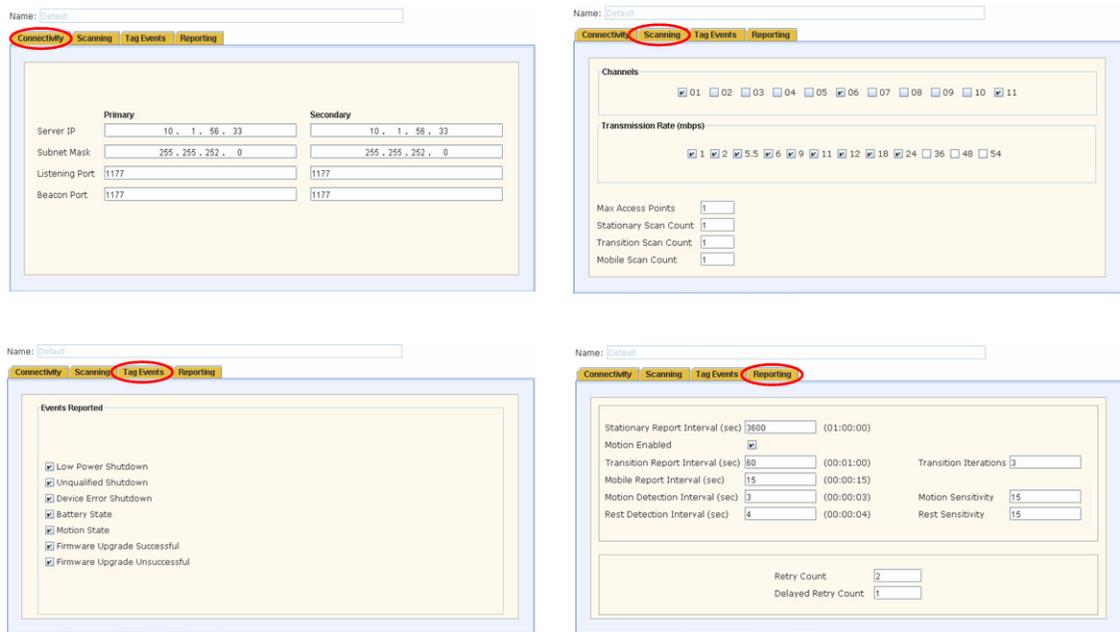
Suspend use of the over-the-air configuration capability (see [Appendix D—Suspending Over-The-Air Configuration Updates, page 80](#)). This caveat is targeted for resolution in an upcoming maintenance release. Consult your local Cisco technical representative or the Cisco Technical Assistance Center regarding the availability of a location appliance software upgrade to resolve this caveat (CSCsh47699).

Appendix A—RSSI Mode Tag Operation

PanGo v2 tags operating in RSSI mode are identified on the floor maps of Cisco WCS using the blue rectangular icon which is used to represent WLAN clients. From the perspective of the location appliance and the WLAN controller, PanGo LAN tags operating in RSSI mode are detected in a similar fashion to traditional WLAN clients such as laptops and PDAs.

When initialized, PanGo LAN Tags configured in RSSI mode use DHCP and establish IP connectivity with the PanGo PanOS Server and PanGo Locator on a regular basis as defined by their report intervals (either stationary, in transition, or in motion). The length of a report interval is specified in seconds via the reporting profile of the tag using the Locator Configuration utility (see [Figure 60](#)).

Figure 60 Reporting Profile Definition



After expiration of the report interval, the tag probes for access points and authenticates/associates using the SSID and WEP key it received in the default security profile during the initialization process. LWAPP access points in the Cisco UWN detect the probe requests and forward the detected RSSI of these probes to the controllers to which they are registered. These controller aggregate the collected RSSI for later collection by the Cisco wireless location appliance.

A detailed description of the steps necessary to configure reporting profiles for RSSI mode tags can be found in Chapter 4 of the *PanGo Administration Guide*, available on your PanGo Locator installation CD or from your PanGo representative. In addition, PanGo also makes available upon request the *PanGo Version 2 Tag Quick Start Guide: Reporting Profile* that provides the rudimentary information necessary to get RSSI mode tags working in a Cisco environment.

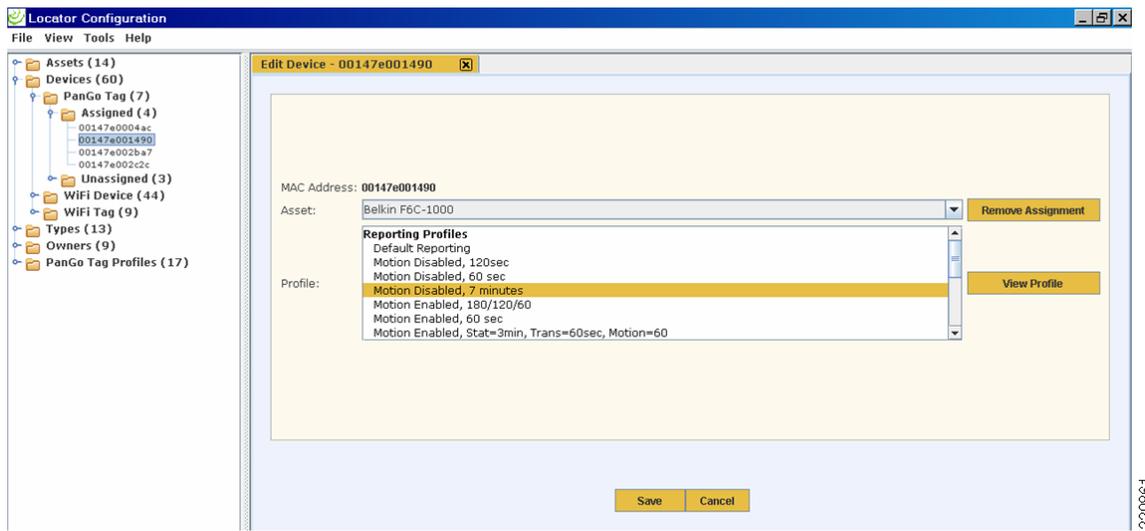
There are four parts of a RSSI mode reporting profile (see [Figure 60](#)) that specify the following:

- **Connectivity**—Primary and secondary IP address information associated with the PanGo PanOS Server.
- **Scanning**—Channels and data rates that the tag should use when probing and attempting to associate. Unless a channel is explicitly selected here, probe requests are not sent and association does not occur despite the presence of any access points advertising the SSID specified in the security profile. This panel also specifies the number of scan counts (probe requests) that are issued each time the tag attempts to locate an access point for association.
- **Tag Events**—Tag states that are reported to PanGo Locator via the session established between the tag and the PanGo PanOS Server. These tag states provide enhanced tag status information in the PanGo Locator Monitor, Notifier, and Reporting modules.
- **Reporting**—Various reporting intervals used when a tag is stationary, in motion, or in a transition state. These are fully explained in Chapter 4 of the *PanGo Administration Guide* under Reporting Profile Properties.

These panels can be used to create customized reporting profiles attuned to the movement characteristics of assets in your environment. For example, some assets such as wheelchairs and IV pump poles might be expected to change location very frequently. Other assets such as beds and equipment carts may remain in the same location for much longer periods of time. Customized reporting profiles can be defined such that assets that change location frequently associate and contact PanGo Locator more often than assets that remain stationary for longer periods of time. This helps prolong tag battery life and reduce tag maintenance.

PanGo v2 asset tags default to RSSI mode and are assigned the default reporting profile. This assignment can be changed using the PanGo Locator Configuration utility. Select the tag MAC address from the Devices > PanGo Tag > Assigned tree branch and place the brown screen bar across the profile that you wish to assign to the tag (as shown in [Figure 61](#)).

Figure 61 Assignment of RSSI Mode Reporting Profile



Click **Save** at the screen bottom to save the new reporting profile assignment of the tag. Note that the mode of operation of the tag can be changed from reporting mode to chirp mode by simply assigning the tag a chirping profile instead of a reporting profile via this same process.

Changes made to assigned reporting or security profiles are propagated to the tag the next time the tag successfully associates and contacts the PanOS server. Tags can be extensively reprogrammed over-the-air in this fashion, which can include not only configuration changes but firmware and microcode updates as well.

In the integrated Cisco/PanGo asset tracking solution, the determination of the physical location (localization) of the PanGo tag is performed by the Cisco Wireless Location Appliance, the PanGo PanOS Server, and the Cisco UWN. The asset tag provides the RF signal whose RSSI is detected by the infrastructure, but the asset tag itself does not participate in the actual calculation of its location. Tag location coordinates are communicated to the PanGo PanOS Server via the SOAP/XML API interface. PanGo Locator accepts this information and maps it to its physical location hierarchy, which is anchored in the real world using World Geodetic System (WGS) coordinates.

PanGo Locator interfaces to PanOS Server and displays the RSSI mode tag location to the user, both pictorially and in tabular format. However, because in RSSI mode the PanGo asset tag and PanGo Locator are able to communicate bi-directionally via a session established between the tag and the PanOS server, the PanGo location client is able to make use of several unique PanGo asset tag features.

An example of this can be seen when changes are made to the security or reporting profiles assigned to an asset tag in the PanGo Locator Configuration Utility. These changes are communicated to the asset tag the next time the tag associates and contacts the PanGo PanOS Server. Similarly, the tag routinely passes information to PanOS Server including its motion and battery status, the completion status of any firmware upgrades, and its shutdown state. This exchange of information can be seen in the packet analysis shown in [Figure 62](#).

Figure 62 RSSI Mode Frames

Relative Time	Packet	Source	Destination	Protocol	Size	Summary
0.000000	1	00:14:7E:00:2C:C3	00:14:1B:59:43:82	802.11 Probe Req	52	FC=.....,SM= 0,FM= 0,SSID=testuser1
0.000314	2	00:14:1B:59:43:82	00:14:7E:00:2C:C3	802.11 Ack	14	FC=.....
0.001672	3	00:14:1B:59:43:82	00:14:7E:00:2C:C3	802.11 Probe Rsp	143	FC=.....,SM=3059,FM= 0,BI=100,SSID=testuser1,DS=11
0.002604	4	00:14:7E:00:2C:C3	00:14:1B:59:43:82	802.11 Auth	34	FC=.....,SM= 1,FM= 0,Algorithm=0 (Open System),AT...
0.002915	5	00:14:1B:59:43:82	00:14:7E:00:2C:C3	802.11 Ack	14	FC=.....
0.005803	6	00:14:1B:59:43:82	00:14:7E:00:2C:C3	802.11 Auth	34	FC=.....,SM=3060,FM= 0,Algorithm=0 (Open System),AT...
0.007494	7	00:14:7E:00:2C:C3	00:14:1B:59:43:82	802.11 Assoc Req	56	FC=.....,SM= 2,FM= 0,Listen=0,SSID=testuser1
0.007809	8	00:14:1B:59:43:82	00:14:7E:00:2C:C3	802.11 Ack	14	FC=.....
0.016464	9	00:14:1B:59:43:82	00:14:7E:00:2C:C3	802.11 Assoc Rsp	50	FC=.....,SM=3061,FM= 0,Status=0,AID=1
0.034517	10	IP-0.0.0.0	IP Broadcast	DHCP	316	C DISCOVER
0.036396	11	IP-1.1.1.1	IP-10.1.59.250	DHCP	368	R OFFER 10.1.59.250
0.528810	12	IP-0.0.0.0	IP Broadcast	DHCP	328	C REQUEST 10.1.59.250
0.531314	13	IP-1.1.1.1	IP-10.1.59.250	DHCP	368	R ACK
0.532468	14	00:14:7E:00:2C:C3	Ethernet Broadcast	ARP Request	64	10.1.59.250 = ?
0.532704	15	00:14:7E:00:2C:C3	Ethernet Broadcast	ARP Request	64	10.1.59.250 = ?
1.035418	16	00:14:7E:00:2C:C3	Ethernet Broadcast	ARP Request	64	10.1.56.33 = ?
1.036391	17	VMWare:D7:F5:78	00:14:7E:00:2C:C3	ARP Response	64	VMWare:D7:F5:78 = 10.1.56.33
1.037099	18	IP-10.1.59.250	IP-10.1.56.33	TCP	96	Src= 1024,Dst= 1177,...S.,S=2078917053,L= 0,A= ...
1.037865	19	IP-10.1.56.33	IP-10.1.59.250	TCP	96	Src= 1177,Dst= 1024,.A..S.,S=2086282838,L= 0,A=2078...
1.038723	20	IP-10.1.59.250	IP-10.1.56.33	TCP	88	Src= 1024,Dst= 1177,.A....S.,S=2078917054,L= 0,A=2086...
1.097947	21	IP-10.1.59.250	IP-10.1.56.33	TCP	120	Src= 1024,Dst= 1177,.AP....S.,S=2078917054,L= 32,A=2086...
1.099626	22	IP-10.1.56.33	IP-10.1.59.250	TCP	100	Src= 1177,Dst= 1024,.AP....S.,S=2086282839,L= 12,A=2078...
1.100843	23	IP-10.1.59.250	IP-10.1.56.33	TCP	88	Src= 1024,Dst= 1177,.A...F,S=2078917086,L= 0,A=2086...
1.100887	24	00:14:1B:59:43:82	00:14:7E:00:2C:C3	802.11 Ack	14	FC=.....
1.101476	25	IP-10.1.56.33	IP-10.1.59.250	TCP	88	Src= 1177,Dst= 1024,.A....S.,S=2086282851,L= 0,A=2078...
1.102096	26	IP-10.1.56.33	IP-10.1.59.250	TCP	88	Src= 1177,Dst= 1024,.A...F,S=2086282851,L= 0,A=2078...
1.102911	27	IP-10.1.59.250	IP-10.1.56.33	TCP	88	Src= 1024,Dst= 1177,.A....S.,S=2078917087,L= 0,A=2086...
1.128598	28	IP-10.1.59.250	IP-10.1.56.33	TCP	76	Src= 1024,Dst= 1177,.A.R...S.,S=2078917087,L= 0,A=2086...
1.129516	29	00:14:7E:00:2C:C3	00:14:1B:59:43:82	802.11 Deauth	30	FC=.....,SM= 14,FM= 0,Reason=3
1.129827	30	00:14:1B:59:43:82	00:14:7E:00:2C:C3	802.11 Ack	14	FC=.....

220659

Appendix B—Stand-alone Access Point Initialization Configuration

A stand-alone access point may be used in place of a WLAN controller and LWAPP access point when configuring PanGo tags on a standalone initialization network. Note that a DHCP server is recommended for assigning IP addresses to tags.

This appendix provides a sample configuration for a stand-alone access point configured for such usage.

```

version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname PanGo_AP
enable secret 5
clock timezone GMT -5
clock summer-time R recurring
ip subnet-zero
ip domain name testlab.com
no aaa new-model
!
dot11 ssid PanG0pgtp
    authentication open
    guest-mode
!
crypto pki trustpoint TP-self-signed-2427845085
    enrollment selfsigned
    subject-name cn=IOS-Self-Signed-Certificate-2427845085
    revocation-check none
    rsakeypair TP-self-signed-2427845085
!
crypto ca certificate chain TP-self-signed-2427845085
    certificate self-signed 01

```

```

quit
username Cisco password 7 096F471A1A0A
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption key 1 size 128bit 7 3C78624FFE4F8608AE1B03567B6D transmit-key
encryption mode wep mandatory
!
ssid PanG0pgtp
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0
54.0
no power client local
power client 1
power local cck 1
power local ofdm 1
channel 2462
station-role root
beacon privacy guest-mode
no dot11 extension aironet
no cdp enable
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
hold-queue 160 in
!
interface BVI1
ip address 10.1.59.120 255.255.252.0
no ip route-cache
!
ip default-gateway 10.1.56.23
no ip http server
ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
access-list 111 permit tcp any any neq telnet
no cdp run
control-plane
bridge 1 route ip
!
line con 0
access-class 111 in
line vty 0 4
access-class 111 in
login local
line vty 5 15
access-class 111 in
login
end

```

Appendix C—Manual Chirp Mode Configuration

To manually place a previously initialized PanGo v2 tag into chirp mode via the serial interface CLI, follow these procedures:

Step 1 Connect tag to PC as per the recommendations discussed in [Tag Serial Interface, page 27](#).

Step 2 After the tag has been successfully connected, issue the following CLI commands to the tag:

- a. **AT&F**—Resets the tag to factory default configuration
- b. **reset**—Performs soft reset of the tag
- c. **config 1**—Sets tag device state as “not configured”
- d. **devicemode 1**—Sets tag operational mode to “RSSI mode”
- e. **rssiintstat xx**—Sets the stationary chirping blink rate in seconds
- f. **rssich 0x8420**—Configures tag for channels 1, 6, 11
- g. **motion x**—Set to 1 or 0 for motion enabled or disabled)
- h. **rssiintmov xx**—Sets the in-motion blink rate in seconds (if applicable)
- i. **chirpcount xx**—Sets number of frames sent per interval; default is 5
- j. **configint xxxxxxxx**—Sets the over-the-air update interval, in seconds. Default is 86400.



Note If you wish not to use the OTA update capability in chirp mode, see [Appendix D—Suspending Over-The-Air Configuration Updates, page 80](#).

- k. **devicemode 2**—Sets tag operational mode to “chirp mode”
- l. **config 2**—Sets tag device state as “configured”
- m. **reset**—Saves the tag configuration and performs a soft reset of the tag

Step 3 Disconnect the tag from the serial interface promptly to conserve battery life.

By following these instructions, the tag is configured by default to transmit five multicast packets on each of channels 1, 6, and 11. DHCP is enabled by default.

Step 4 If DHCP is not desired, the tag can be given a static IP address by using the following CLI commands:

- a. **lvip <ip addr>**—Assigns tag static IP address
- b. **lvmask <mask>**—Assigns static IP mask
- c. **lvgate <gateway ip addr>**—Assigns tag gateway address
- d. **reset**

Appendix D—Suspending Over-The-Air Configuration Updates

The default mode of operation for PanGo v2 tags in chirp mode is to periodically attempt to contact the PanOS server for updated configuration information and firmware updates every 24 hours.

In some cases, this may not be desirable. To suspend this capability, there are two options:

- Administratively disable the static WEP WLAN across all controllers using WCS. Without the presence of an active static WEP WLAN, v2 tags in chirp mode are not able to associate and continue currently configured chirp mode operation until the next configuration request interval. *This is the preferred method and is highly recommended* because it allows chirp mode OTA updating to be suspended via a simple change that can easily be reversed when it is desired to do so.
- Manually set the configuration request interval of each tag to a very high time period using the tag serial port CLI as follows:
 - Connect the tag to PC as per the recommendations discussed in [Tag Serial Interface, page 27](#).
 - When the tag has been successfully connected, issue the following CLI commands to the tag:
 - **config 1**—Sets tag device state as “unconfigured”
 - **devicemode 1**—Sets tag operational state to “RSSI mode”
 - **configint 15768000**—Sets configuration request interval to 15,768,000 seconds or six months. To effectively permanently disable OTA updates, you may set the configuration request interval to a maximum of 31.7 years (999999999 seconds).
 - **devicemode 2**—Sets tag operational state to “chirp mode”
 - **config 2**—Sets tag device state as “configured”
 - **reset**—Saves the configuration and performs a soft reset of the tag
 - Disconnect the tag from the serial interface promptly to conserve battery life.

After the chirp mode tag is reset at the end of this procedure, it does not attempt to associate or contact the PanOS server for a period of six months. A period of six months was chosen here as an example that allows for the resumption of over-the-air configuration updates in a reasonable time frame. Choose a time interval that you are most comfortable with, keeping in mind that should you wish to re-enable OTA configuration update before the end of that period, the configuration request interval must be individually reset via the tag CLI.

Appendix E—Multiple Location Appliance Properties Files

This section contains examples of the PanOS Cisco location provider properties files as well as the provider registry necessary to define multiple location appliances to the PanGo PanOS Server.

In this example, two Cisco location appliances (10.1.56.20 and 10.1.56.21) are defined to a single PanGo PanOS Server.

- `.\PanGo\PanGo PanOS Server\provider-cisco-1.properties`

```
# Cisco Location Server provider
poll.interval=60

# changes to the following require a server restart
classname=com.pangonetworks.provider.cisco.CiscoPollingProvider
identifier=ciscoProvider.1
```

```

provider.units=feet

# double, defaults to 0.0
provider.origin.latitude=34.041640
provider.origin.longitude=-84.242720

# double, defaults to 0.0, in provider.units
provider.origin.altitude=1105

# integer, in provider.units
provider.accuracy=30

# changes to connectivity info will be detected and applied
cisco.hostname=10.1.56.20
cisco.port=8001
#cisco.user=admin
cisco.user=pango
cisco.password.key=cisco.password
cisco.protocol=https

# changes to any of the following require a server restart
cisco.device.identifier.namespace=MAC_ADDRESS
cisco.station.device.type.key=WiFiStation
cisco.tag.device.type.key=WiFiTag

# no location event grace period (seconds)
cisco.no.location.timeout.seconds=1200

```

- `.\PanGo\PanGo PanOS Server\provider-cisco-2.properties`

```

# Cisco Location Server provider
poll.interval=60

# changes to the following require a server restart
classname=com.pangonetworks.provider.cisco.CiscoPollingProvider
identifier=ciscoProvider.2

provider.units=feet

# double, defaults to 0.0
provider.origin.latitude=34.901250
provider.origin.longitude=-84.104670

# double, defaults to 0.0, in provider.units
provider.origin.altitude=1500

# integer, in provider.units
provider.accuracy=30

# changes to connectivity info will be detected and applied
cisco.hostname=10.1.56.21
cisco.port=8001
cisco.user=pango
cisco.password.key=cisco.password
cisco.protocol=https

# changes to any of the following require a server restart
cisco.device.identifier.namespace=MAC_ADDRESS
cisco.station.device.type.key=WiFiStation
cisco.tag.device.type.key=WiFiTag

# no location event grace period (seconds)
cisco.no.location.timeout.seconds=1200

```

- .\PanGo\PanGo PanOS Server\provider-registry.properties


```
# comment off provider to deactivate it
provider.1 = provider-pango.properties
provider.2 = provider-cisco-1.properties
provider.3 = provider-cisco-2.properties
```

Appendix F—Basic PanGo v2 Tag CLI Commands

Figure 63 Basic CLI Commands

Command	Description	Input Range	Default	Read/Write
AT\$HWVERSION	Displays microcontroller firmware version	N/A	N/A	Read Only
AT&F	Restore tag factory defaults	N/A	N/A	Write Only
ATI2	Displays MIPS firmware version	N/A	N/A	Read Only
BATT	Current battery voltage in millivolts	N/A	N/A	Read Only
CHIRPCOUNT	Number of frames in a chirping burst cycle	1 - 255	5	Read/Write
CONFIG	Tag Configuration State	0 - 3	0	Read/Write
CONFIGINT	Chirp Mode OTA update configuration interval	1 - 999999999 secs	86400 secs	Read/Write
DHCP	IP address obtained via DHCP	any valid IP address format	0.0.0.0	Read Only
KEYINDEX	WEP Key Index	1, 2, 3, 4	1	Read/Write
LVAUTH1	WEP Key Length in WiFi Profile 1	0, 40, 104	104	Read/Write
LVDUMP	List tag WiFi Configuration Listing	N/A	N/A	Read Only
LVGATE	Gateway Address currently in use	any valid IP address format	0.0.0.0	Read/Write
LVLWEP1	104 bit WEP Key for Profile 1	13 char quoted string or 26 hex char (0 prefix)	P959crmaMBRS	Write Only
LVMASK	Subnet mask currently in use	any valid IP address format	255.255.255.0	Read/Write
LVSSID1	SSID used in WiFi Profile 1	"string"	"PanG0pgtp"	Read/Write
MACADDR	List Tag MAC Address	6 byte hex	factory programmed	Read/Write
MOTION	Enable/disable Tag Motion Reporting	0, 1	1	Read/Write
RESET	Save parameters and perform soft tag reset	N/A	N/A	Write Only
RSSICH	Channel bit mask, left to right ascending order	0x0000 - 0xFFFF	0x8420 (1, 6 11)	Read/Write
RSSIINTMOV	Motion Reporting Interval	0 - 65535 seconds	60 seconds	Read/Write
RSSIINTSTAT	Stationary Reporting Interval	0 - 65535 seconds	21600 seconds	Read/Write
SERVERIP1	PGTP Server IP Address	any valid IP address format	0.0.0.0	Read/Write

22/08/02