



Regulatory Domain Unification For Cisco Wireless LAN Access Points

Table of Contents

1.1	Requirements	2
1.2	Scope.....	2
2	Functional Overview.....	2
2.1	Feature List (Software/Firmware).....	2
2.1.1	Universal AP Boot Sequence Cycle	2
2.1.2	Domain Identification Engine	4
2.1.2.1	Manual Identification	4
2.1.2.2	Automatic Identification.....	8
2.1.3	External Interfaces (Software/Firmware).....	11
2.1.3.1	SmartPhone Application	11
2.1.4	Security Considerations.....	17
2.1.4.1	Infrastructure Security	17
2.1.4.2	Client Security	17
2.2	Platform Requirements	18
2.2.1	Access Points	18
2.2.2	SmartPhone Applications.....	19
3	Glossary	19
4	Questionnaires from Previous Correspondence.....	20

1.1 Requirements

The purpose of the Universal Access Point (AP) is to address worldwide regulatory compliance requirements based on geo-location of Cisco Wireless Access Points.

Key elements of the requirements are:

- Domain and thus channel/power plan shall be determined based on the geographical location of an AP prior to operation.
- The End User shouldn't be allowed to change the Regulatory Domain and Country configuration on APs.
- Any mechanism shall minimize user interaction to configure the correct regulatory domain .
- The provision process shall work with all Cisco APs.

1.2 Scope

In order to meet the above requirements, the solution relies on information from trusted RF neighbors along with a smartphone based audit scheme in order to convert Universal APs into appropriate regulatory configurations post installation.

2 Functional Overview

2.1 Feature List (Software/Firmware)

2.1.1 Universal AP Boot Sequence Cycle

In order to honor compliance regulations for all countries, one of the key requirements for the Universal AP, will be to initially only operate on frequencies that are allowed in all countries across the world. Currently there are no available frequencies in the 5GHz spectrum that are valid in all countries, therefore during the Universal AP initial startup cycle, only 2.4GHZ transmissions will be allowed. 5GHz transmissions will not occur until the regulatory domain conversion is completed.

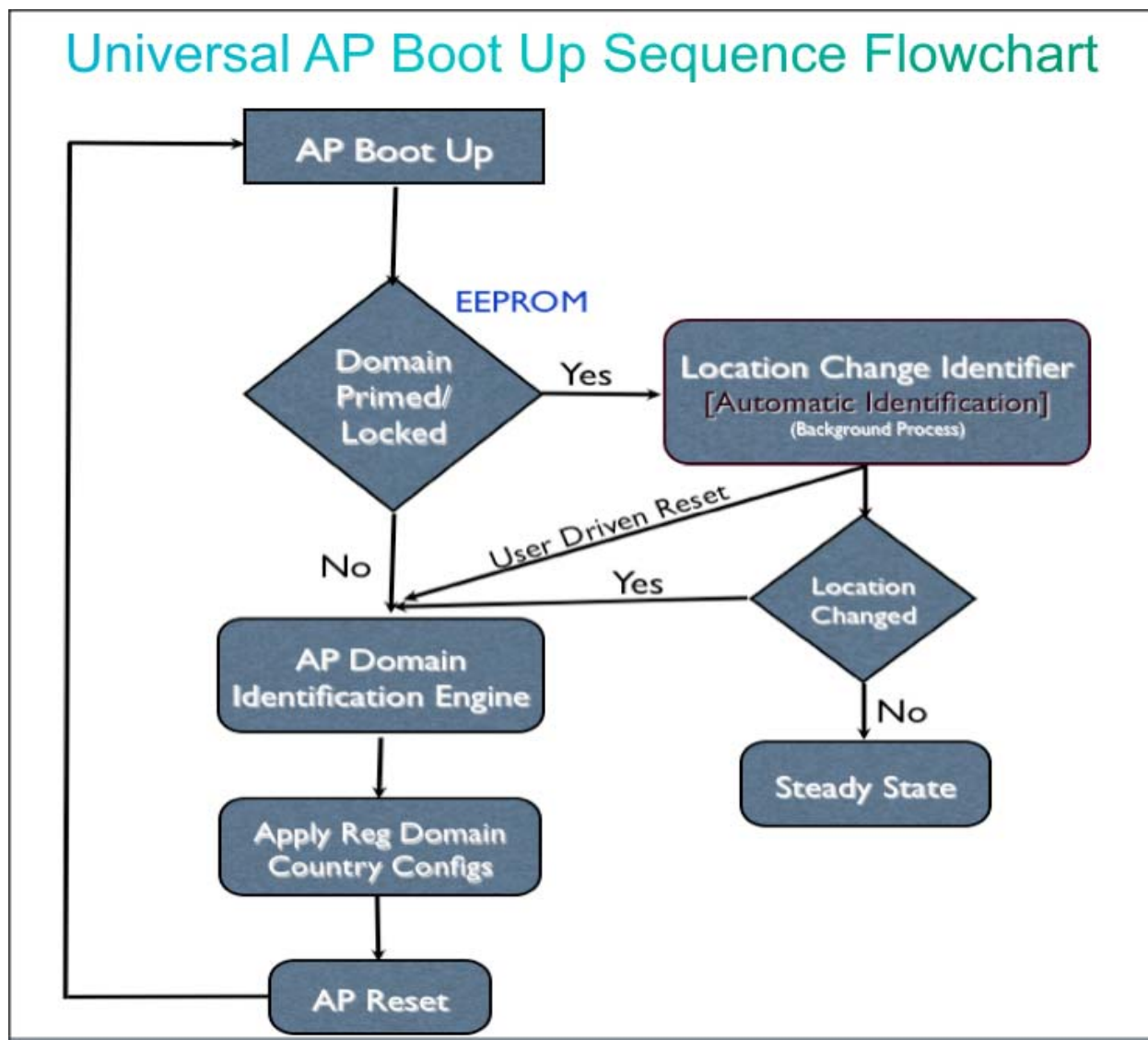


Image 1.1 Universal AP Boot Up Sequence Flowchart

The above flowchart shows the boot sequence diagram of Universal AP's bring up cycle. When a fresh out-of-box AP gets installed at a customer site, after the boot loader initialization the host will read regulatory domain configurations from the cookie that is burned in the EEPROM of the device. For a non-configured APs, both Regulatory Domain and Country Code will be set to Universal Attribute "UX".

For out-of-box APs, the Domain Identification Engine (DiE) will trigger regulatory domain migration. DiE will convert UX AP into correct domain using two phases of identification methods explained in section 2.2.2. After successful migration, AP will reset and come up with new regulatory domain and country configurations and operate similar to our existing pre-configured APs.

One key difference between a converted Universal AP and existing Cisco Aps (Non-Universal) is that the DiE engine's Location Change Identifier (LCi) will run in the background during the Universal AP's boot up cycle. LCi will ensure the Universal AP is installed with the correct regulatory domain in case APs are physically moved after priming. If the LCi reports no location change, AP will enable TX on 5GHz radios. Prior to the migration into correct SKU, only 2.4 GHz radios will be operational.

2.1.2 Domain Identification Engine

Overall SW architectural changes to migrate Universal AP into correct regulatory configs can be categorized into 2 major functional phases.

- 1. Manual Identification:**

Manual identification encompasses a technique using a smartphone application that migrates Universal SKU AP into the correct regulatory domain.

- 2. Automatic Identification:**

Automatic Identification leverages Cisco proprietary Neighbor Discovery Protocol (NDP) to propagate regulatory domain configurations across the AP's localized RF neighborhoods.

2.1.2.1 Manual Identification

This method encompasses a Smartphone application that runs on different flavors of mobile OSs. Upon successful authentication smartphone will communicate with Universal AP on a secure 2.4 GHz channel. Smartphone then will request AP configurations to differentiate Universal SKU AP from other access points. When associated Access Point is identified as Universal AP, smartphone will push regulatory configurations to the AP.

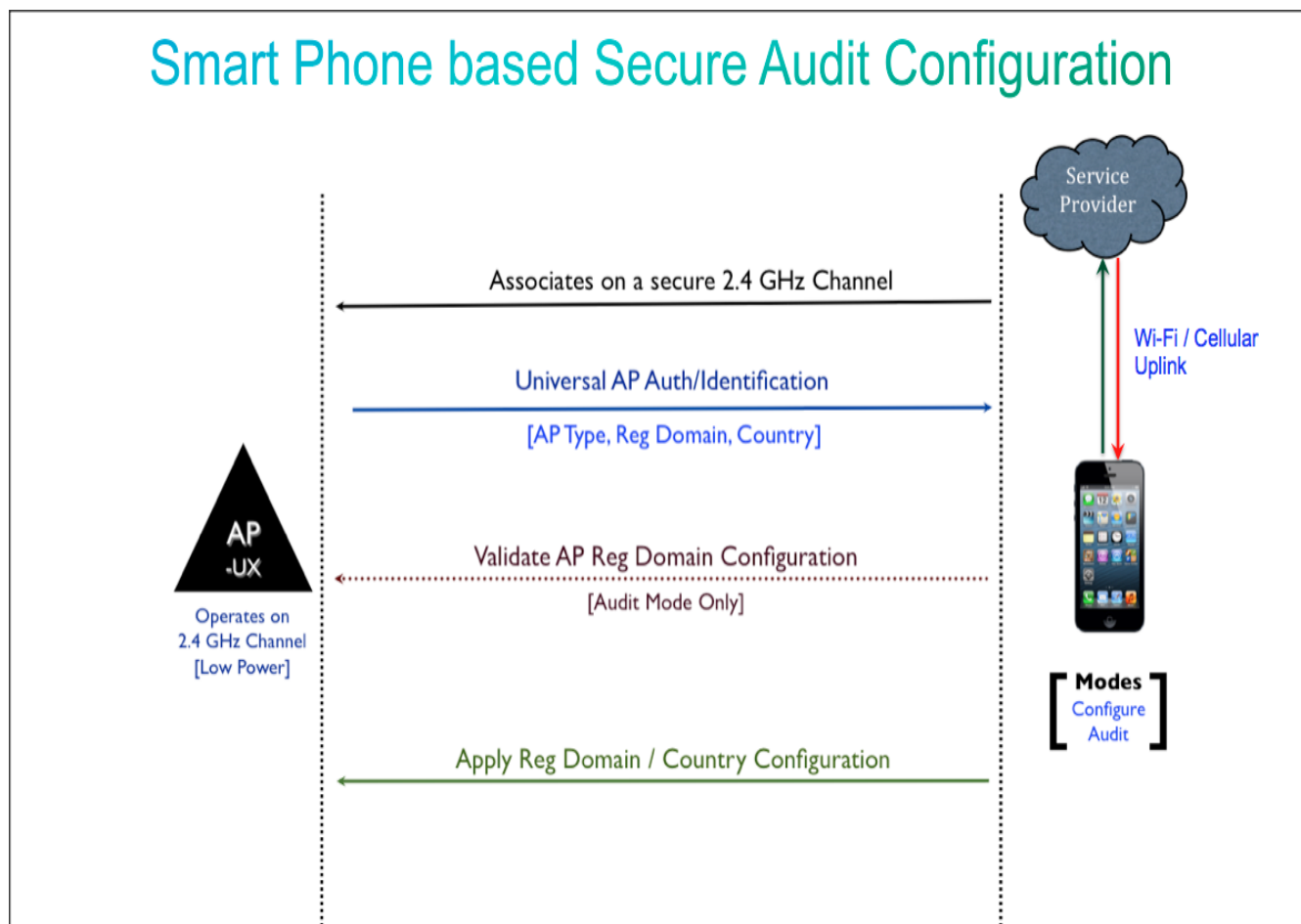


Image 1.2 Highlights configuration exchanges between Smartphone App and the Universal AP

When user wants to prime a Universal AP, he/she must authenticate with CCO credentials. Without proper authentication, Smartphone will be disabled and not able to configure the AP. After successful authentication, Smartphone will associate to Universal AP over a secure 2.4 GHz channel as a client. Prior to the association with AP, smartphone app will also gather its location information from inbuilt GPS and cell tower that advertise country information by extracting Mobile Country Code (MCC) Identifier from the Public LAN Mobile Network (PLMN). Once associated, Universal AP then will send information about its AP type and Regulatory Domain and Country configurations in order to distinguish from existing Cisco APs and whether it has been primed already. For an unprimed/out-of-box Universal AP, smartphone will configure the AP with the correct regulatory domain derived based on the AP information and country code details via GPS and MCC ID. Smartphone App will maintain a database that maps country configurations to regulatory domain for a specific AP model. This information will

be sent to the Universal AP to migrate it into the correct Regulatory Domain and country configurations.

Smartphone App will support following 2 modes of operations

- 1) **Configure Mode:** This will be the default mode of operation for Smartphone App to configure Universal SKU AP, fresh out of box Aps will get configured via configure knob when associated AP is configured with Universal Attributes (*Reg. Domain: -UX, Country: UX*)
- 2) **Audit Mode:** This special mode will handle wrongly primed Universal Aps, when Universal Aps are shipped via tier-2 distributors or were misconfigured due to change in location, in such cases reg. domain configurations will be corrected via Smartphone App in audit mode. Audit mode can overwrite reg. domain configurations of an already primed Universal AP. During the Universal AP boot up process when LCI notifies host about the potential change in location, such Aps can be only reconfigured via Smartphone App in audit mode.

When Universal AP gets re-primed by Smartphone App in audit mode, a special flag will be enabled in NDP frame to propagate corrected regulatory domain settings to rest of the RF neighborhood. It will speedup overall network convergence time when majority of the Aps installed in the network are misconfigured.

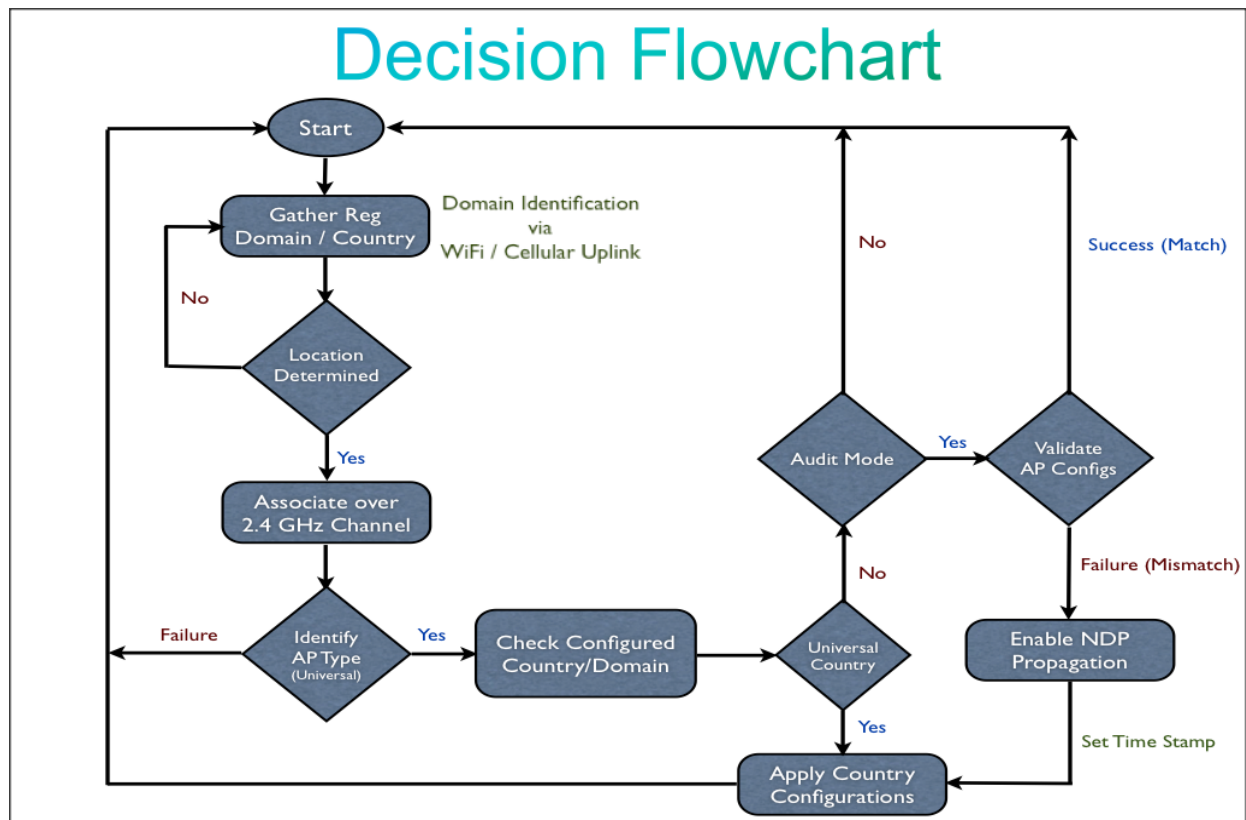


Image 1.3 Decision Flowchart of Smartphone App with modes of operations

Above decision flowchart explains the basic communication flow between the smartphone application and the Universal AP. Upon successful authentication with the required credentials, Smartphone will gather its location information from the GPS and Cell ID, once the location is determined it will associate to Universal AP over a secure 2.4GHz channel. After successful authentication, smartphone app will establish communication with the AP to gather AP information and regulatory details. If associated AP is identified as Universal AP, smartphone will configure regulatory settings into AP's cookie under EEPROM to prime correct Regulatory Domain ID and Country configurations.

For misconfigured Universal APs, Smartphone App will operate in Audit mode that can correct regulatory domain configurations when user physically moves Universal APs into a new location or when Universal APs were primed in a different country. In such case, NDP Propagation Override flag will be enabled to automatically correct Reg. Domain information to rest of the RF neighborhood and with minimal user intervention.

2.1.2.2 Automatic Identification

Automatic Identification method solely relies on Cisco's RF intelligence in order to propagate the new Regulatory Domain and Country configurations to the local RF neighborhood. Cisco proprietary Neighbor Discovery Protocol (NDP) frames will be leveraged to discover secure Cisco Universal APs in the network and propagate reg. domain attributes to the localized RF neighborhood. Sub mode of Automatic Identification process will run in the background during Universal AP's boot up cycle (under Location Change Identifier) to determine change in AP's location once it is primed.

Automatic Identification method will be the default method used by Cisco Universal APs. While manual identification helps migrate Universal APs into the correct regulatory domain, automatic method will propagate regulatory domain configuration to the localized RF neighborhood quickly and efficiently. This method is dependent on the presence of existing Cisco Universal Aps in the network, therefore user needs to prime at least one Universal AP in the network. Automatic Identification also helps to autocorrect already primed Universal AP; this will be addressed by special notification via NDP that can override other Universal AP's configurations.

Cisco Proprietary Neighbor Discovery Frame needs information about the AP type, Regulatory Domain and Country Configurations to efficiently propagate to localized RF neighborhood. New NDP message for Universal Aps will be differentiated based on the versioning of the NDP frames.

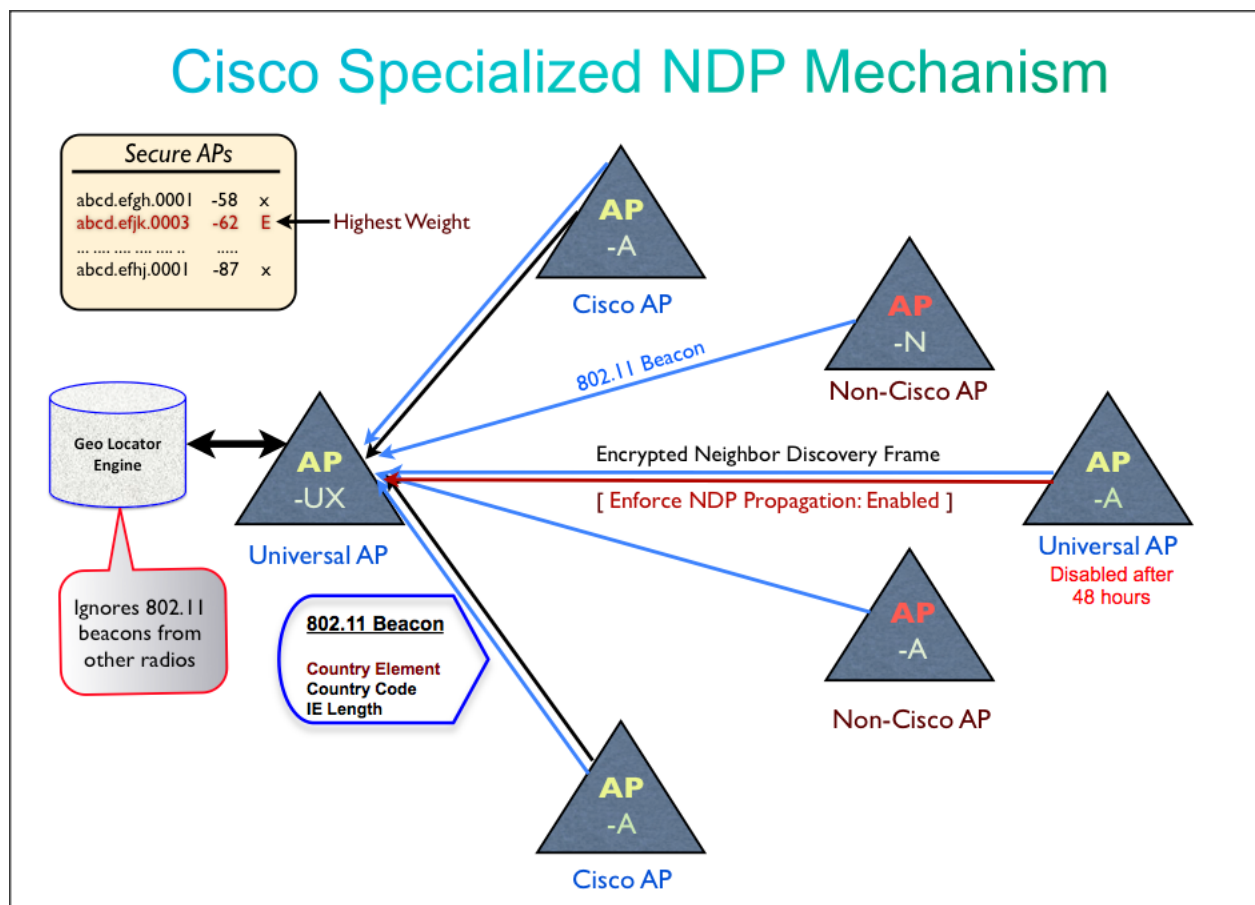


Image 1.4 Automatic Identification Method Leveraging NDP For Domain Propagation

Above explains Universal AP's communication with other Universal, existing Cisco and third party APs. AP maintains Geo-locator engine that is responsible to maintain database of the adjacent neighbors in the RF neighborhood, compute their approximate distance from the Universal AP, identify Cisco Universal AP, and filter out other third party or malicious rogue APs. Once secure AP list is established, Universal AP will process 802.11 beacons from such APs to learn regulatory configurations. The 802.11 beacon carries a country element includes country code details. All beacons from non-secure Cisco and third party APs will be ignored.

When Smartphone configures Universal AP with regulatory configurations, an NDP propagation flag will be enabled to propagate the configuration out to the AP's localized RF neighborhood.

Special provisions are added to create safety net when a Universal AP is installed in a location where the rest of the colocated APs are configured with the incorrect regulatory domain. This would be a rare scenario, however in such occurrences when Universal AP detects mismatch with its RF neighbors, it will shutdown its transmissions on 5GHz radios.

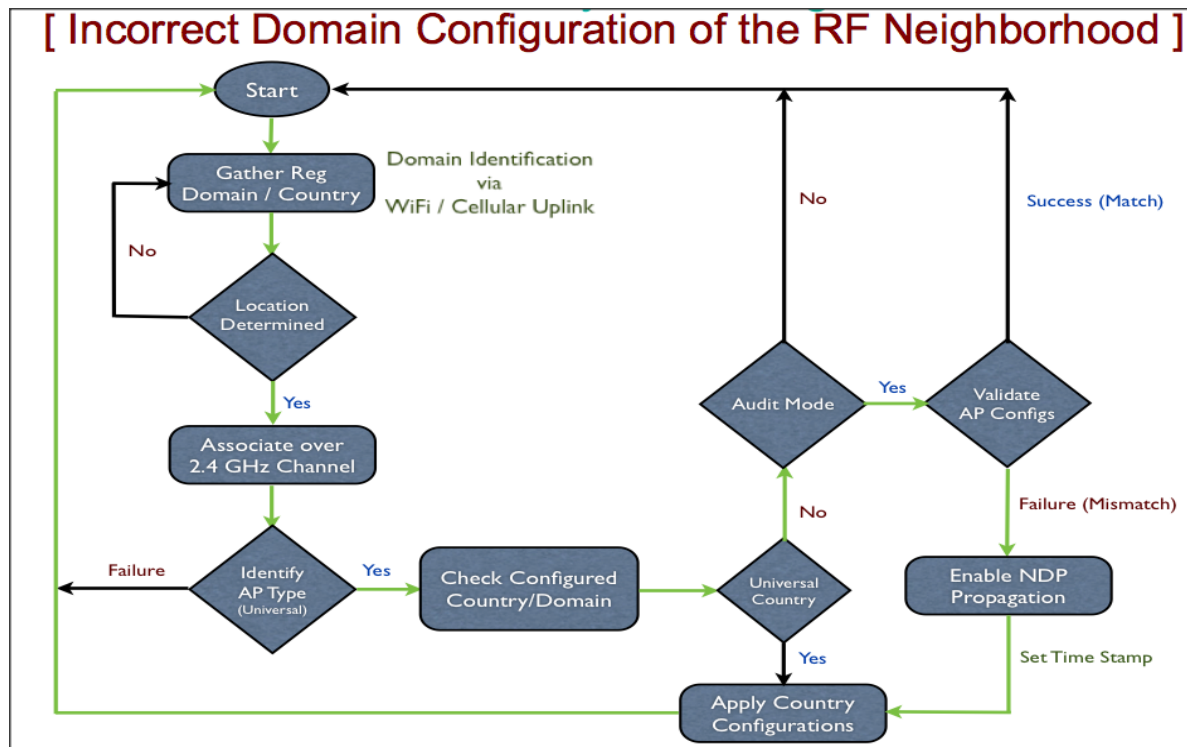


Image 1.5 Migrating Universal AP from Incorrect Regulatory Configurations

Additionally, such Universal APs will also provide visual feedback with flashing RED LEDs to notify user about potential misconfigurations. User then needs to reconfigure Universal AP with SmartPhone (Audit mode) to validate its configurations. Any config corrections via audit mode will enable NDP propagation override flag, which will override the rest of the Universal APs configurations. Universal APs with propagation override will ignore domain configurations from other APs. Propagation override will automatically get disabled after 48 hours.

2.1.3 External Interfaces (Software/Firmware)

2.1.3.1 SmartPhone Application

Primary means of communication with Universal APs will be established by Smartphone application to migrate AP into correct regulatory domain.



Launch Screen:





CCO Authentication:

The image shows a login interface for 'Universal AP Connect'. It features a blue gradient background with a Cisco logo at the bottom. The login form consists of two input fields: 'User Name' and 'Password', followed by a 'Log In' button. Below the button is a link for 'Forgot Password?'. The Cisco logo is prominently displayed at the bottom center.

User will be required to authenticate into Smartphone app using CCO credentials. Explicit user registration process will be required to create CCO credentials.

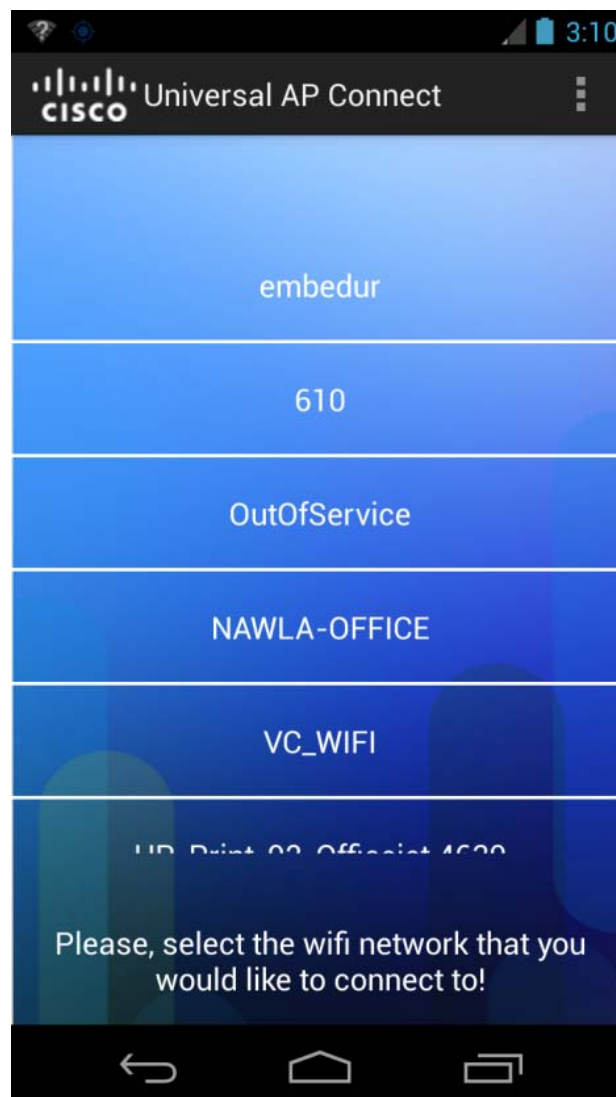
WiFi Connection:

If capability is available on the corresponding phone (Android only), a list of available SSIDs will be displayed.

iOS and Windows Phone 8 – User will be prompted to go the settings menu and connect to the Admin SSID for the AP.

Android – SSIDs list can be retrieved and application can programmatically connect/ disconnect to/from an SSID. Only SSIDs configured on the 2.4 GHz radios will be listed.

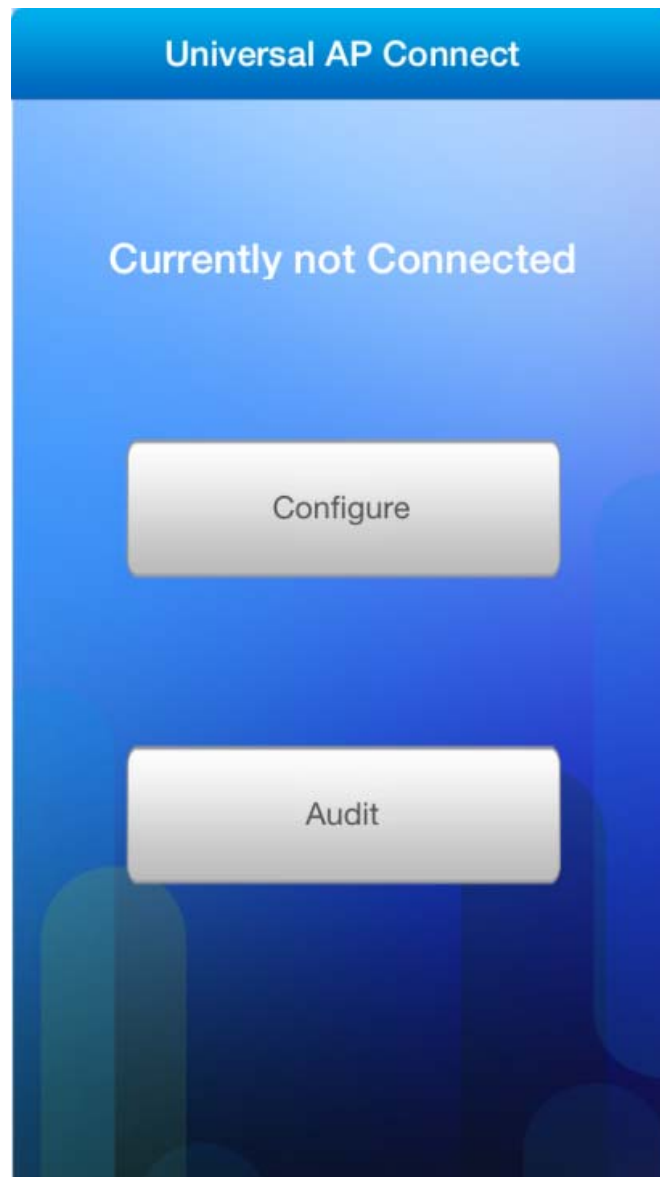
User should proceed to connect to the selected SSID with the specific interface available on the application or the phones settings menu.





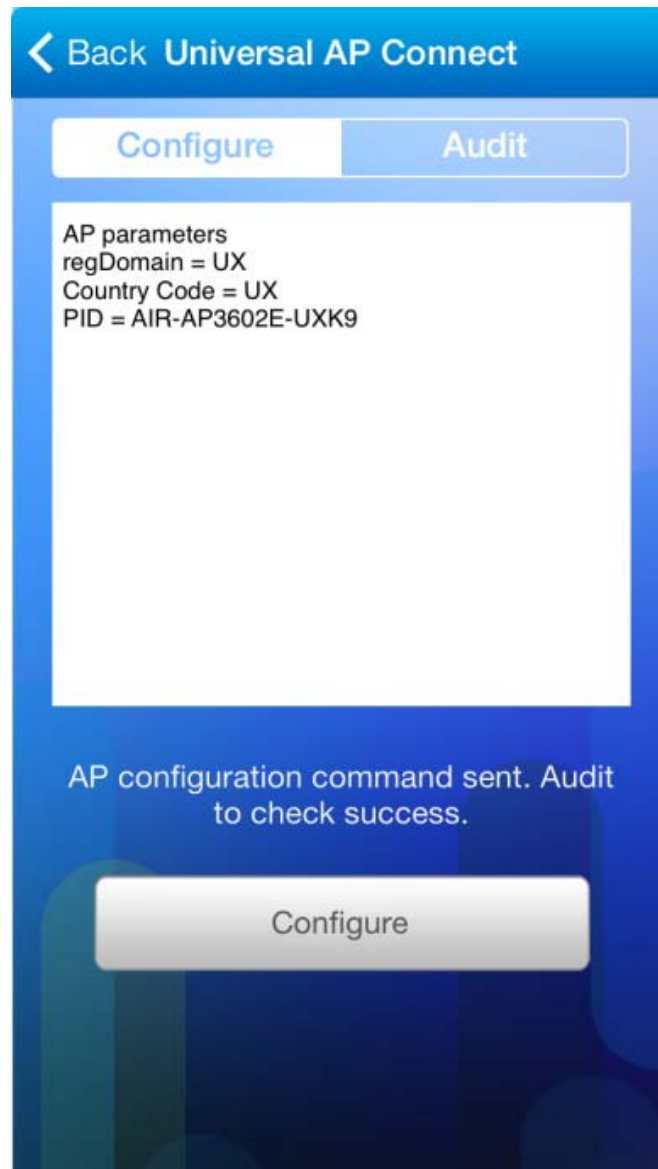
Home Page

Home page will display mainly configure and audit buttons. User then can move to appropriate settings to configure either out of box or an already primed Universal AP.





Configure Mode:

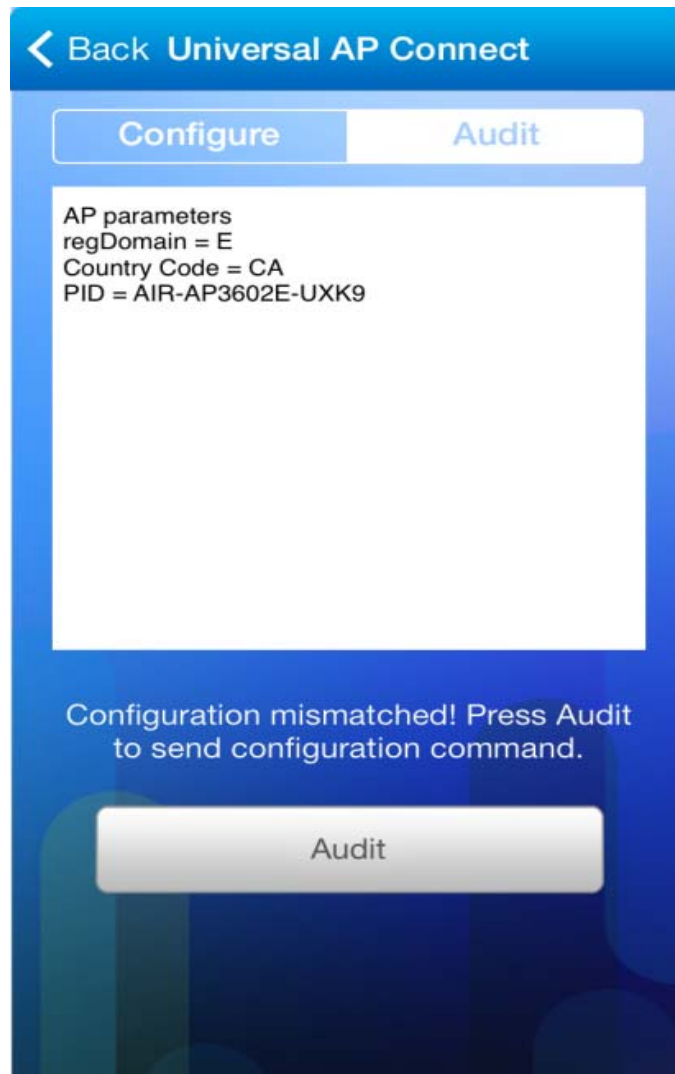


After successful authentication, in order to configure out-of-box Universal APs, network admin will be able to configure units with a correct regulatory domain. Universal APs that are already primed with a specific domain cannot get configured with config knob.

Note: Network admin will not have ability to specify Reg. Domain configurations. Location determination and country/domain configurations will solely made based on the SmartPhone App's location



Audit Mode:



Universal APs that are already configured via either a SmartPhone App config mode or NDP can be reconfigured via SmartPhone Audit mode. Audit mode is specifically designed to automatically correct misconfigured Universal APs. Audit mode can be also used to validate the prior Reg. Domain configurations as well. Like config mode, user will not have any ability to influence the decision of Reg. Domain and Country configurations. When associated with Universal APs, they will be able to learn the current Reg. Domain settings and autocorrect it if required.

2.1.4 Security Considerations

As part of the solution has dependencies on the third party devices (SmartPhone), it is critical to ensure that all vulnerabilities are addressed. Therefore, following security measures were added to prevent unauthorized access of the SmartPhone Application to end-user.

2.1.4.1 Infrastructure Security

Prior to SmartPhone App usage, user needs to explicitly authenticate via CCO (Cisco Connections Online) server. Any customer who has a valid purchase order from Cisco needs to have a valid CCO Account. CCO Account will be primary way any user can communicate with Cisco TAC or provide feedback about the Cisco products. While authenticating to CCO server, a user who is a customer, partner or Cisco employee can login into the application after he/she is successfully authenticated to CCO server. SmartPhone Application will not function unless CCO authentication is successful.

Once authenticated, when user is trying to provision Cisco Universal AP; SmartPhone client needs to be associated to a Wireless LAN that has universal-admin configurations enabled. Only network admins who has complete access to the WLAN Controller and Access Points can enable Universal-Admin configurations. When enabled, WLAN Controller will enforce minimum of WPA2-AES 802.1X security configurations prior to WLAN's operation. Therefore all communications over WiFi channel between the Access Point and the SmartPhone client will be encrypted via secure AES tunnel.

2.1.4.2 Client Security

In order to prevent any device centric spoofing, SmartPhone Application does have various security measures added along with additional safety nets.

SmartPhone will not function unless minimum criteria for OS compatibility is matched *[Please refer to section 2.3.3 for supported OS list]* In case when the device legitimacy is compromised by installation of OS that does not have valid certificates or when the device itself is jail broken or rooted, SmartPhone Application will completely shutdown its operation. Additionally, Cisco Air Provision will only accept location inputs from base cell towers (via PLMN ID) and the installed GPS device. It will not accept location coordinates from any other device; simulator or third party app that can potentially send spoofed coordinates.

Once the location is determined, SmartPhone App will solely determine correct regulatory domain and country configurations and provision Universal AP. This would be completely system driven decision and any user will not be able to determine or influence these configurations in any manner.

2.2 Platform Requirements

Universal AP will be initially supported on following Cisco Wireless Access Point Models

2.2.1 Access Points

HW Models

-  AIR-AP702-UXK9
-  AIR-AP1602-UXK9
-  AIR-AP2602-UXK9
-  AIR-AP2702-UXK9
-  AIR-AP3602-UXK9
-  AIR-AP3702-UXK9
-  AIR-AP1532-UXK9
-  AIR-AP1572-UXK9

2.2.2 SmartPhone Applications

SmartPhone Application to migrate Universal AP into correct regulatory domain will be supported on following versions of SmartPhone Operating Systems

-  Android Jelly Bean 4.0 or higher
-  Apple iOS 7.0 or higher
-  Windows Mobile OS 8.0

SmartPhone Apps will be made available to registered customers via Google Play, Windows Mobile Store and Apple Store.

3 Glossary

The following list describes acronyms and definitions for terms used throughout this document:

- **AP:** Access Point
- **DiE:** Domain Identification Engine
- **LCi:** Location Change Identifier
- **NDP:** Neighbor Discovery Protocol
- **PLMN:** Public LAN Mobile Network
- **MCC:** Mobile Country Code

4 Questionnaires from Previous Correspondence

- Discovery Mode: after any Power up/Reset, (transition step) and operating ☐ on default channels, and propagation mode disabled.☐
 - If CC = UX (EEPROM = UX Default Universal Mode) ☐ • Find successful neighbor(s) go to operate mode, ☐ • or go to Audit manual mode.☐

Cisco Systems Inc >>[Clarification] When Universal AP is not primed (fresh out of box) it will either try to get domain information from nearby Universal APs (that are already provisioned) or if it is an initial seed AP in the network, it needs to be provisioned via SmartPhone Application (Cisco AirProvision) via secure Wi-Fi uplink

- CC=XY (EEPROM = XY (country determined)) ☐ • Find successful neighbor(s) go to operate mode, ☐ • or go to Audit manual mode.

Cisco Systems Inc >>[Clarification] when domain is already configured via aforesaid methods, Universal does not need to find neighbors or Smartphone application for domain updates. However, it enables active scan to learn any new updates in the local RF neighborhood prior to any successful transmissions.

- Audit manual mode, operating on default channels and propagation mode ☐ disabled), enable use of smart phone.

Cisco Systems Inc >>[Clarification] There are mainly two propagation modes leveraging Cisco's Neighbor Discovery Protocol

1) Normal Propagation: After domain configurations are done via SmartPhone, such universal AP will propagate regulatory domain and country configurations to nearby Aps in the local neighborhood.

2) Override Propagation: SmartPhone audit mode provides audit functionality to address misconfigured Universal Access Point. Domain is overwritten for an already primed access point, override propagation is enabled to expedite domain correction across RF neighborhood

- Operate Mode.(after successful discovery mode) operating on country
 - discovered channels, propagation mode enabled and monitor for mismatch.
- Mismatch go to Audit manual mode

I. Questions

1. The write up indicates that at first power up the unit sets the CC = UX □Default. Is this done at the factory or is there a UAP condition - never □powered up.

Cisco Systems Inc >> Manufacturing does this before unit goes out for shipping

Confirm that during discover mode all transmissions are only over 2.4 default □channels independent of EEPROM set to UX (default mode) or CC (country □determined) .

Cisco Systems Inc >> That is correct, during this phase all transmissions are only sent on 2.4GHz channel 1 to 11 with lowest power allowed across regulatory domains

2. Discovery Mode means: default transmission mode and propagation mode □disabled.

Cisco Systems Inc >> Correct, no propagation will be done until unit is primed and goes through full scan cycle

3. Discovery Mode and Audit manual mode includes: default mode, propagation ☐ mode disabled and AP light blinking (or NMS) with ability to connect to a ☐ manual configuration via Cisco App in Smart phone.

Cisco Systems Inc >> Not sure, if I completely understood this comment but there can be two cases when Universal AP boots up

- 1) Out of Box AP: For out of box Universal AP's first boot up cycle, AP's LED will continue to cycle between RED, GREEN and OFF. During this phase, Universal AP will only allow radio operations on 2.4GHz common channels with lowest powered allowed across regulatory domains in the world. Such Aps can be either primed automatically via NDP or manually with SmartPhone application. We do not provide any knobs or manual configuration access to users that can either influence or change regulatory domain configurations on Universal AP.
- 2) Already Primed Universal AP: When already primed universal AP boots up, it will perform active scan to identify any changes into local RF neighborhood prior to its operation. During this phase, AP LED will continue to cycle between RED, BLUE and OFF. After successful scan, it will allow transmissions on both (2.4 / 5GHz) radios. In order to avoid any anomalies Universal AP does also conduct passive scan to efficiently measure any changes in the local RF neighborhood

4. Discovery mode clarification:

- a. Discovery Protocol (NDP) finds that all universal APs (or UAP) in the operating mode have the same CC set to XY (country determined), or finds just one operating mode UAP's that has a CC set to XY (country determined). Then that Universal UAP sets the CC to the discovered CC (or confirms that the current EPROM CC is valid) and then will switch to the operate mode.

Cisco Systems Inc >> For non-primed Universal AP it will go through full NDP scan cycle to find all nearby Aps before it provisions itself with corresponding CC. When AP is already primed during its active scan it will match neighbor's CC with its own and if there is any conflict it will go back to default mode (LEDs chirping RED)

- b. No other UAP is discovered in operating mode (–none may be discovered or all may be in discovery mode), then that Universal AP goes into audit manual mode (for both EEPROM Set to CC or UX). This means that a standalone AP will always go into audit mode on power up. Will end-users accept that?

Cisco Systems Inc >> Standalone AP out of box AP will go into manual mode where SmartPhone based provisioning is required in order to allow Tx operations of the radios. Once AP is already primed, it doesn't have to go through audit mode unless reg. domain anomalies are detected.

Follow Up Question:

Clarify that an Access point in Japan in a standalone environment, once the country code is set by a smart phone and then brought to The US and powered up in a stand-alone environment (no anomalies are detected), the AP will remain configured for Japan.

Cisco Systems Inc >> When AP is physically moved even within country we mandate user to configurations via factory default settings [WLC CLI or by pressing hardware reset button on the AP]. This will reset Universal AP's settings back to UX domain. Let's say, a user has deliberately chosen to ignore Cisco's mandatory requirement for config reset, such AP when moved to US controller will not be able to associate and therefore its mode of operation will be disabled [both radios down] until it gets config reset.

Further Follow Up Question:

DAVE /Vishal we are unclear what "not able to associate means".

Let's say, a user has deliberately chosen to ignore Cisco's mandatory requirement for config reset, such AP when moved to US

controller will not be able to associate and therefore its mode of operation will be disabled [both radios down] until it gets configured.

Does this mean that a stand-alone AP after a power cycle must be reconfigured, or only if it is not associated with clients?

Cisco Systems Inc >> Let me try to clarify few items here. Cisco primarily manufactures two modes of Access Points. Unified (Cisco Wireless LAN Controller managed) and Standalone (Autonomous). Cisco Universal SKU AP is supported on both modes of these Aps. Following would be the behavior both Aps when they are physically moved from one country to another without going through Cisco's "config reset" requirement.

- 1) Unified (Controller Managed): When Unified AP is moved physically from one country (ex: Japan) to another (ex: United States), in lieu of config reset it will preserve its configurations across reboots. However, when such AP joins US Controller, such AP will be rejected (CAPWAP) by the controller and hence it won't be operational. Only way to recover such AP would be via explicit configuration reset via AP CLI or Hardware button on the device.
- 2) StandAlone (Autonomous): Standalone APs do not require WLAN Controller in order to operate, as long as they have valid network connection. For Standalone case, location change will be determined by NTP (Network Time Protocol). When StandAlone AP is physically moved to another country without explicit config reset, when it is plugged into US network, NTP will flag mismatch in AP's regulatory configurations. Such AP will be automatically reverted back to factory defaults (Both Radios in UX Domain) and needs to be re-provisioned via SmartPhone Application.

- c. The power up AP has the EEPROM set to XY (country determined), which is a mismatch with all other operating

discovered visible APs. Then that UAP is set to the country code discovered from all the others.

Cisco Systems Inc >> Good question. Correct answer is, it depends!! Although in almost all certain cases, UAP will inherit new CC from rest of the local RF neighborhood, our design also has an additional safety net for an extremely rare case when rest of the RF neighborhood is wrong primed (extremely low probability). In such case, when an UAP is primed via SmartPhone (Audit) mode with its Domain and CC overwritten, it will enable Propagation override (via NDP) to automatically correct rest of the RF neighborhood.

- d. In operating mode, what happens if a mismatch is discovered, □do all UAP(s) go into discovery mode and require Audit manual mode for manual re-configuration. This would be the same situation if a power up UAP in discovery mode found a mismatch set of other APs. All UAP(s) are put into Discovery mode.

Cisco Systems Inc >> Let's say we have two sets of UAPs primed in two different regulatory domains. If we somehow bring them together to form single RF neighborhood, upon bootup yes the UAP that discover domain mismatch will go back to discover mode. While multiple UAPs are in discover mode, user does have to prime only one UAP via SmartPhone audit mode and leveraging NDP propagation override they will automatically get newer domain configured

- e. Five universal APs power up in an area where number 5 only detects AP #6 in operating mode and sets #5 to CC of #6 and #4 , now sees # 5 in operating mode and sets # 4 CC, etc. All 5 access points work in default mode until discovery chain is completed.

Cisco Systems Inc >> They don't need to wait until all AP's discovery process is completed. For sparse deployment and when APs can only hear one other UAP (ex: linear topology), they will get primed in sequence.

- f. Can all APs be in operational mode and EEPROM CC set to UX, or is UX only a Discovery mode parameter.

Cisco Systems Inc >> Even for primed Universal AP (where CC is not equal to UX) they will still conduct discovery mode.

6. Is MCC only for LTE (MCC)?

Cisco Systems Inc >> Mobile Country Code (MCC) is encompassed within PLMN-ID, a mandatory code for all cellular operators world wide irrespective of the cellular technology (GSM / CDMA)

7. To obtain both MCC and GPS must these functions be operational or can this a recently stored value?

Cisco Systems Inc >> Our location determination doesn't rely on A-GPS or recently stored value. They need to be retrieved at the same time during the UAP provision.

8. We need more detail on the Manual Identification Method (phone).

- a. Users are notified by blinking light (Net management system) that AP is in default mode and manual identification is required.

Cisco Systems Inc >> Correct, via AP console message and cycling RED, GREEN and OFF LED sequence.

- b. If all universal APs are in default mode because of a mismatch and nobody does anything, what happens after 48 Hours?

Cisco Systems Inc >> They will continue to operate in default mode until any user action is performed

- c. The Security Considerations explains the authentication and security between CCO and the phone client. However, Security between the client and the AP is only through Admin privileges. How secure is the link between the client and the AP from being HAC or spoofed.

Cisco Systems Inc >> All communication between SmartPhone client and Access Points will be only available via secure http uplink. Wireless link between SmartPhone client and the UAP will be encrypted with minimum WLAN security policy of WPA2-AES/PSK. Additionally, in order to provision UAP WLAN under which the client associated needs to have uap-admin (special configuration that network admin can enable). All client associations under WLANs that do not have uap-admin configurations will be rejected even if they pass security checks. After client goes through aforementioned security checks, it needs to authenticate to AP's via admin configure username / password which will be unique per network.

Follow Up Question:

Clarify the Security of the Cisco application on the smart phone.. As described in your response, the only authentication appears to be the AP's admin configure username / password. Not sure of the aforementioned security checks are:

- How easy is it for a third party to provide the app or spoof the protocol?
- Need clarification on CCO credentials. How does it prevent third party Spoofing?
- Must Phone's APP authenticate with Cisco operations center to activate

Cisco Systems Inc >> In order to prevent SmartPhone Application vulnerability, we enforce security mechanisms from infra (network) and client side.

From network side, we enforce CCO Registration, WLAN UAP-Admin Configurations and AP authentication

1) CCO Registration: Prior to SmartPhone App (Cisco AirProvision) it requires explicit authorization and registration with CCO (Cisco Connections Online) centralized server. We validate SmartPhone application user against approved CCO Policies (Employee, Authorized Partner or Customer (with valid PO#),

anyone that doesn't fall into aforementioned privileges will not be able to use AirProvision Application.

2) WLAN UAP-Admin Configurations: We also provide explicit control to network admin so that no unauthorized user can tweak Cisco Universal AP configurations. This is done via UAP-Admin configurations under WLAN settings. When enabled, such WLAN must have minimum of WPA2-AES PSK security configurations, which results in Wi-Fi link encryption between SmartPhone and the Access Point. Any user trying to access Universal AP with a WLAN that doesn't have UAP-Admin configuration will get access denied.

3) AP Authentication: Once user is able to authenticate with correct CCO privileges and authenticates via uap-admin enabled secure WLAN, needs to further authenticate to AP with AP's management username / password. Authentication is completely handled in AP, so no user should be able to sniff packets from the wired port.

Additionally, we also have client centric logic on the SmartPhone App to disallow location spoofing or prevent hacking into the phone. Cisco AirProvision includes built-in device legitimacy check via OS signature validation and disallowing Cisco AirProvision to get downloaded on jail broken devices which will address any location spoofing or third party Apps trying to reverse engineer our secure application. Cisco AirProvision also doesn't accept any external or internal inputs from other Applications, and only relies on built in GPS and PLMN codes from the service providers for location determination.

Combination of aforesaid network (infra) and client centric security mechanisms make it impossible to hack into Cisco AirProvision.

Follow Up Question:

The question is when the AP is taken out of the box what is the "AP's management username/password"? Is that unique to each AP or can someone spoof an application and communicate with AP on default username and password? There is no information I saw about the default username and password description. If they say that each AP that is shipped has unique default information that is downloaded in their CCO privileges, I

think that is fine then there will not be an issue. Also, it means that someone buying a refurbished unit will have to go through a Cisco reset process.

Cisco Systems Inc >> At present fresh out of box Cisco APs have default username / password that is common across all radios in the network. It is not possible to regenerate unique username/password per AP, or tie it up with CCO at the manufacturing site because a customer can buy thousands of APs and same CCO ID can be used by the same customer to buy multiple orders. Therefore, for out of box AP any person who is able to get hold of the SmartPhone App and login with CCO credential will still get denied AP access with management credentials unless that AP has a WLAN which explicitly have UAP-Admin configurations enabled by the network admin. Also any client that is going to provision Universal AP needs to get authenticated with WPA2-AES PSK or 802.1x security configurations. When network admin installs Cisco Aps, upon controller configurations AP's default username and password can be changed to unique (per AP or per whole network) credentials, which is a typical practice done by all of our existing customers even today in order to avoid any proprietary config exposure to un-authorized users.