TELECOM INFRA PROJECT

TIP OpenWiFi Lab Test Plan

Wi-Fi Solution Group

Date January 2021

Document version: v1.0

Confidentiality Level: GREEN [Public Access]

TIP Document License

By using and/or copying this document, or the TIP document from which this statement is linked, you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions:

Permission to copy, display and distribute the contents of this document, or the TIP document from which this statement is linked, in any medium for any purpose and without fee or royalty is hereby granted under the copyrights of TIP and its Contributors, provided that you include the following on ALL copies of the document, or portions thereof, that you use:

1. A link or URL to the original TIP document.

2. The pre-existing copyright notice of the original author, or if it doesn't exist, a notice (hypertext is preferred, but a textual representation is permitted) of the form: "Copyright © <<year>>, TIP and its Contributors. All rights Reserved"

3. When space permits, inclusion of the full text of this License should be provided. We request that authorship attribution be provided in any software, documents, or other items or products that you create pursuant to the implementation of the contents of this document, or any portion thereof.

No right to create modifications or derivatives of TIP documents is granted pursuant to this License. except as follows: To facilitate implementation of software or specifications that may be the subject of this document, anyone may prepare and distribute derivative works and portions of this document in such implementations, in supporting materials accompanying the implementations, PROVIDED that all such materials include the copyright notice above and this License. HOWEVER, the publication of derivative works of this document for any other purpose is expressly prohibited.

For the avoidance of doubt, Software and Specifications, as those terms are defined in TIP's Organizational Documents (which may be accessed at https://telecominfraproject.com/organizational-documents/), and components thereof incorporated into the Document are licensed in accordance with the applicable Organizational Document(s).

Disclaimers

THIS DOCUMENT IS PROVIDED "AS IS," AND TIP MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE; THAT THE CONTENTS OF THE DOCUMENT ARE SUITABLE FOR ANY PURPOSE; NOR THAT THE IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

TIP WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE DOCUMENT OR THE PERFORMANCE OR IMPLEMENTATION OF THE CONTENTS THEREOF.

The name or trademarks of TIP may NOT be used in advertising or publicity pertaining to this document or its contents without specific, written prior permission. Title to copyright in this document will at all times remain with TIP and its Contributors.
This TIP Document License is based, with permission from the W3C, on the W3C Document License which may be found at https://www.w3.org/Consortium/Legal/2015/doc-license.html.

Table of Contents

Introduction

This document is a test **template** document. It's purpose is to help Wi-Fi service providers (MNOs, MSOs, ISPs, SIs or MSPs) setup and test a TIP Open Wi-Fi solution, using the test cases described here as a helpful reference. The document is intended to provide structure and to help providers get started with testing typical Enterprise grade functionality. We encourage Wi-Fi providers to adapt and customize this document to suit their individual testing requirements.

Given the open source nature of the effort, and the options for vendors to customize their WLAN (Wi-Fi) offerings, a TIP open Wi-Fi vendor may offer more or less functionality than may be described here in this document. Further, the actual testing steps (such as configuration commands, event descriptions etc.) may vary from vendor to vendor and are not detailed here.

Note: The term Wi-Fi is used in all places in lieu of WLAN for convenience. Note that TIP supports Wi-Fi certification as established by the Wi-Fi Alliance and encourages all TIP Wi-Fi Solution Project Group members to obtain necessary Wi-Fi certification.

Testing Assumptions

Access Point capabilities:

- Support for 802.11 a/b/g/n/ac wv2
  - The following Wi-Fi5 Access Points are available from TIP certified AP manufacturers
    - Proware (TP-Link) EC420: Wi-Fi5 indoor AP, 2x2 2.4 GHz, 4x4 5GHz
    - Edge-Core ECW5211-L: Wi-Fi5 Indoor AP, 2x2 2.4 GHz, 2x2 5GHz
    - Edge-Core ECW5410-L: Wi-Fi5 Indoor AP, 4x4 2.4 GHz, 4x4 5GHz
    - Edge-Core OAP100: Wi-Fi5 Outdoor AP, 2x2 2.4 GHz, 2x2 5GHz
    - CIG WF-610D: Wi-Fi5 Outdoor AP, 2x2 2.4 GHz, 2x2 5GHz
- Support for 802.11ax (Roadmap)
  - WI-Fi6 APs are under software development and QA testing for release early 2021
- Dual band 2.4 GHz, 5 GHz support
- DFS enabled

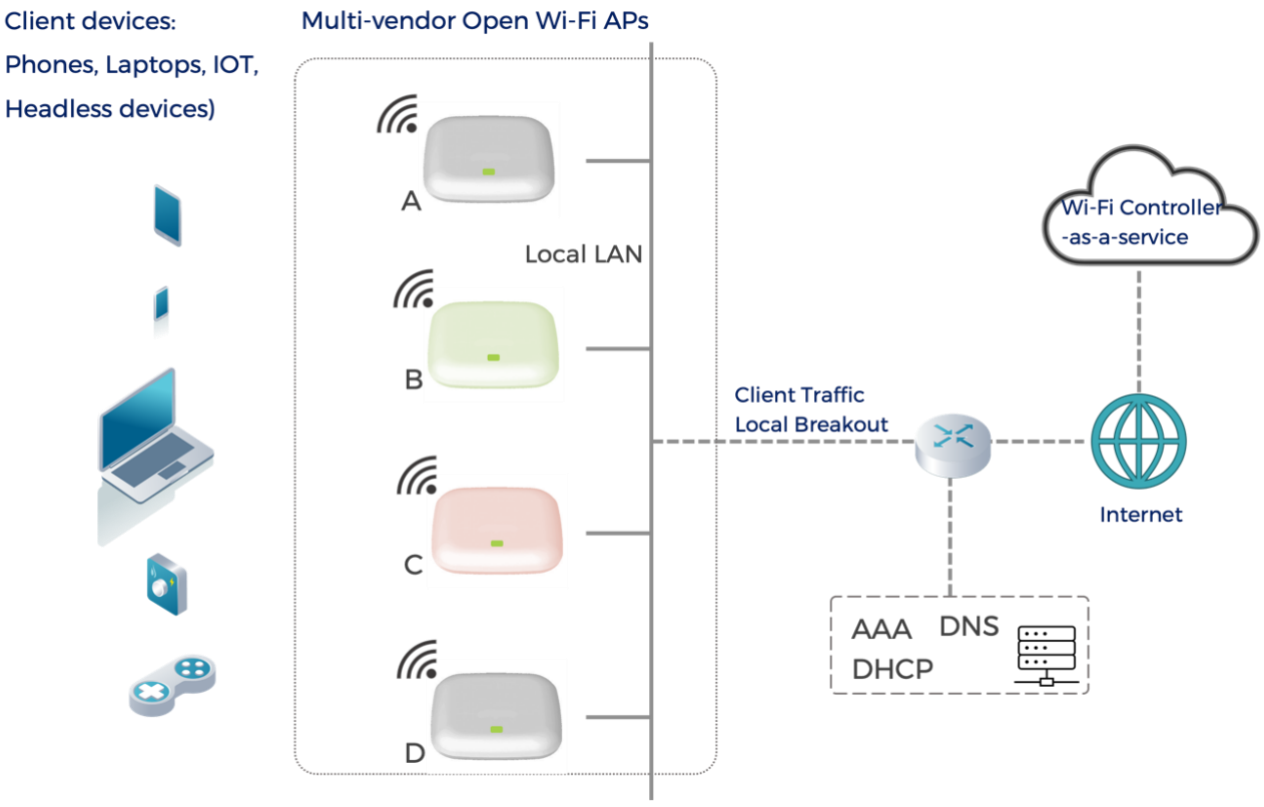
Client capabilities

- Support for 802.11 a/b/g/n/ac wv2. 802.11ax preferred.
- Support for 802.11ax
- Dual band 2.4 GHz, 5 GHz support
- Preferred: Ability to turn off MAC address randomization
- This test plan doc. Will be updated for Wi-Fi 6 AP in subsequent revisions

Test setup

- Deploy 4 or more TIP OPEN Wi-Fi compliant APs (hereafter called simply as APs) in this document) with at least 2 of the APs, coming from different hardware device manufacturers. It recommended that APs be separated by at least 10m and ceiling mounted for optimal coverage
- Create an account on one or more TIP OPEN Wi-Fi compliant Cloud controller (Controller as a service) or alternatively deploy the TIP OPEN Wi-Fi compliant controller(s) in the test lab in a private bare metal or cloud environment on Kubernetes. See TIP Wi-Fi Confluence for details.
- If the TIP Open Wi-Fi controller is deployment on a private data center, X509 certificates need to be generated for the specific deployment. Furthermore, the AP Controller redirector address must be set to reach the specific data center IP address. In the first release for the product, this process is manual but will be automated in the subsequent releases.
- Ensure APs and the controller are able to communicate; check relevant firewalls in the organization allow for this.
- DHCP server and switches are assumed to exist as required in a Wi-Fi network to setup the APs and to switch traffic from the APs when used in bridge mode. Per SSID NAT is also available.

- A RADIUS server is required to test for AAA authentication methods such as WPAx-Enterprise, Passpoint or Specific Captive Portal authentication methods.
- VLAN: Default: Unique VLAN per SSID or native VLAN can be validated
- Test are assumed to be run by an admin/super-user role on the controller, unless otherwise specified
- Manual radio settings
    - Tx Power: Set to Default
    - Channel BW:Default Set to 20 MHz for 2.4 GHz radios and 40 MHz for 5GHz radios
    - Channel selection: Channels must be set with a good optimal coloring scheme
- Automated Radio Resource Management
    - The TIP CloudSDK does not support full operation of automatic Radio Management features. The TIP CloudSDK application layer is responsible for those features.
    - Automated RRM features offered by Application Layer Commercial Vendors such as NetExperience, including auto channel planning, auto radio cell size planning and intelligent Client steering.



The tests are grouped by typical lifecycle stages seen in any communication network

1. Provisioning a new Wi-Fi network

2. Access point (edge) functionality
3. Client devices handling and Management
4. Daily Network Operations and Maintenance – Fault Isolation, Swap out, Group Upgrades
5. Network refresh and expansion
6. Scale and system Performance tests

Wi-Fi Network provisioning

This section tests the configuration, provisioning, and initialization of a TIP Open Wi-Fi network when TIP Open Wi-Fi APs are deployed for the first time

AP binding to the TIP controller

Objective: Test that APs can be either manually or automatically bound to a specific TIP Compliant Controller.

It should be noted that in the first release of the TIP controller, some specific factory pre-setup is required to reach a specific TIP Compliant controller. The manual steps will be eliminated in a upcoming release with the introduction of a central TIP security certificate service.

Setup: The AP(s) have proper security certificates and redirector addresses to point the controller.

Steps:

1. Test pre-provisioned AP binding (expected standard practice for SPs)
    1. Pre-provision the AP inventory number in the Controller UI
    2. Pre-bind the AP to a customer account and location
    3. Power-up the AP
    4. The AP will be automatically added to the specific customer account location
2. Test adding the AP with no account
    1. Add the AP QR code to the Controller
    2. Power up the AP
    3. The AP will auto-join the Cloud
    4. On the Controller GUI, query the AP QR code or inventory number to ensure the AP has been added to the Controller inventory but not assigned to an account
3. Test customer binding from controller Inventory
    1. Using the Controller UI, assign a specific AP inventory number to a specific account and specific Account location
    2. Ensure AP is displayed and in service in the respective account location
4. Test Certificate mismatch
    1. Pre-provision the AP with wrong X.509 certificates (using SSH private commands)
    2. Ensure the AP has the right redirector IP address
    3. Power-up the AP
    4. The AP should not be able to join the TIP compatible controller

Anticipated result: On the controller:

1. Ensure the specific AP is present at the expected customer account and locations and/or the controller inventory database
2. Ensure only authorized APs are allowed to join the controller

Summary:

What does this test prove?	Business Impact
Unauthorized APs cannot connect to a TIP OPEN Wi-Fi network	Security. Integrity of network operations

Test TCP IP Port security

Objective: Test that APs have all their communication ports disabled

Setup: Single AP connected to the Controller

Steps:

1. Ensure AP is Inservice at the Controller
2. On the local AP management subnet, ensure the AP management IP can be reached with ICMP Pings
3. Using Telnet or SSH, ensure access is not possible on the local subnet to the IP management IP

Anticipated result: On the AP:
No ports other than the AP to Controller port should be opened

Summary:

What does this test prove?	Business Impact
Unauthorized applications cannot connect to a TIP OPEN Wi-Fi AP using TCP or UDP ports	Security. Integrity of network operations

Multi-vendor AP Zero Touch provisioning (MVZTP)

Objective: Test that it is possible to configure and operationalize a network of APs without the APs having to be setup manually (staged) ahead of time

Test Setup: Ensure there are two or more TIP compliant APs setup as part of the test from two or more AP vendors

Test setup:

1. Ensure APs have the proper certificates and redirector addresses to reach the controller
2. The APs should be set to default to ensure no prior profiles are stored
3. Ensure the APs run a factory default APNOS load
4. Setup the AP Profile (and RF profile) and the SSID profile on the GUI
5. Setup the Baseline AP Software rev for the account to the wanted baseline release
6. AP profile may include attributes that are particular to the AP hardware such as location, SW version that the AP should be running (sync'd to cloud or permitted to be different from the cloud version), Regulatory Tx power by country/region, NTP settings, AP names etc. member of AP group etc.
7. SSID profile includes service layer attributes such as the SSID name, type of Authentication/Encryption, AAA details etc.
8. Setup 2 SSID profiles – SSID A and SSID B
    1. For SSID A, setup, WPA2, passphrase, and other profile information
    2. For SSID A, setup, open (no authentication)

Steps:

1. Power on the AP and ensure APs can connect to the controller GUI
2. Ensure AP appears on the correct account and location tags
3. The AP should automatically be upgraded to the baseline release and auto-activate the baseline software load.
4. Once the AP is back in service after the software upgrade, ensure the software revision reported on the Controller GUI is as expected
5. Using client device, A (Mobile, laptop), ensure the client can connect to SSID-A using the proper PSK
6. Conduct traffic test on SSID-A to ensure end-to-end provisioning integrity
7. Using client device B (Mobile, laptop), ensure the client can connect to SSID-B with no password / PSK
8. Conduct traffic test on SSID-B to ensure end-to-end provisioning integrity
9. On the Controller GIU, ensure both Clients are present on the Network Inventory tables with the proper related metrics (RSSI, Data rate, etc)

Anticipated result: The controller accepts the configuration as above with no error. When the APs with the factory default configuration "call home" to the controller, the APs have downloaded the right version of the software and the config from the controller.

1. The AP is registered on the controller.
2. The AP shows as "online" or "connected" status on the controller
3. The latest software as specified on the controller (upgrade from Factory default SW)
4. The latest configuration as specified on the controller is downloaded to the AP

Anticipated Result:

What does this test prove?	Business Impact

The TIP OPEN Wi-Fi solution supports Zero touch provisioning feature	Cost & time savings: Eliminates traditional need to "stage" the APs before being shipped to the customer site. Supply chain efficiency: Enables direct shipping of APs to the customer site from warehouse/factory
It is possible to virtually provision a network (aka pre-provisioning) prior to AP shipment	Reduced fixed costs and cost of operations Fewer admins need to be specialist trained for setup. Installation can be outsourced to field personnel with no training to stage APs Project management flexibility: Delink setup activity from install activity timelines
TIP OPEN Wi-Fi compliant solutions can support APs from multiple vendors	TIP OPEN Wi-Fi solutions offer greater procurement choice for Wi-Fi providers, reducing vendor-lock in, and greater competition in choice of APs with more competitive pricing TIP OPEN Wi-Fi solutions also offer a choice of controllers as well (This is covered in another section)

One-Time Local provisioning

Objective: Test that AP IP configuration can be locally provisioned at staging time with no controller, if required

Setup: Single AP

Steps:

1. Use a factory default AP running a compliant APNOS load
2. Power-up the AP and ensure to connection to the controller is possible (physically or routing wise)
3. The AP should be broadcasting an Open SSID "Maverick"
4. Connect to the Open SSID
5. Using a laptop browser, ensure the simple provisioning GUI is available from the AP. The GUI should allow for setting only the IP attributes
6. Setup a static IP management address
7. Ensure the selected address has a route to the controller subnet
8. Connect the AP to the Cloud
9. The AP should delete the Maverick SSID immediately and get auto-provisioned for service
10. The local IP configuration GUI is not accessible anymore

Anticipated result: On the AP:
AP Management IP attributes can be locally provisioned if required without controller connectivity once after factory default

Summary:

What does this test prove?	Business Impact
A method exists to use APs in a static IP environment even if the APs can't reach the Controller from the default DHCP setup.	Flexibility of network operations

Mass (Bulk) upgrade at initial join time

Objective: Test that when APs join a controller for the first time all the APs (up to 50 APs) are upgraded in parallel and are sync'd up to the right configuration.

Steps:

1. Use at least one AP per model available for testing
2. Provision a specific baseline AP software level per AP model type on the controller GUI
3. Ensure the APs all have a default factory APNOS load
4. Connect the APs to the Cloud
5. APs should be auto upgraded to the provisioned baseline revision for all vendor and model types

Anticipated result: The APs are upgraded and brought up to the latest configuration in parallel and the operation is not serialized
Note that some controllers may limit the number of APs that can be upgraded in parallel.

Bulk upgrade for new AP software

Objective: In addition to the initial bulk upgrade test, validate that groups of APs can be upgraded in bulk

Steps:

1. Use at least one AP per model available for testing
2. Ensure the APs are connected to the controller and in service with no alarms
3. Using the upgrade manager panel of the controller, provision a new target AP software revision per model type for a specific account location tag
4. Set the upgrade method to parallel
5. Start the upgrade job
6. Ensure all APs are upgraded simultaneously on the target location
7. APs should be auto upgraded to the provisioned revision for all vendor and model types and all services should be available
8. Using the upgrade manager panel of the controller, provision a new target AP software revision per model type for a specific account location tag

9. Set the upgrade method to staggered. This method takes longer but ensures minimal disruption to users
10. Start the upgrade job
11. Ensure all APs are upgraded in sequence on the target location
12. APs should be auto upgraded to the provisioned revision for all vendor and model types and all services should be available

Anticipated result: The APs are upgraded and brought up to the latest configuration either in parallel or staggered per the provisioning settings. Note that some controllers may limit the number of APs that can be upgraded in parallel.

AP ownership

Objective: Test that an AP once registered or admitted to a Service Provider (SP) account on the controller cannot be automatically "claimed" by another SP account on the same controller

Setup:
Create a separate SP account on the controller (Account #2). Login to Account #2.

Steps:
1. Manually or otherwise enter the details to claim the AP previously registered (with Account #1). This may include AP's serial number/Mac address etc. Attempt to register the AP to account #2
2. Record result

Anticipated result: The registration with Account #2 should fail.
The Controller should provide an indication that the AP has ALREADY registered elsewhere and should also provide a means to redress the situation if the account holder believes the AP is theirs.

Summary:

What does this test prove?	**Business Impact**
An AP can only be owned by one entity (SP) on the controller.	Eliminates ability to register an AP falsely (for e.g. "Stolen AP") Security. Integrity of network operations

Transferring AP ownership:

Test that a means exists for a TIP Open Wi-Fi compliant AP that has been admitted to a SP's account on a given controller can be transferred to another SP account by the root user

Setup:
Create a separate SP account on the controller (Account #2).

Steps:
1. Using the Controller Root account, unbind the AP from the SP Account #1
2. Manually or otherwise enter the details to claim the AP previously registered (with SP Account #1). This may include AP's serial number/Mac address etc. Attempt to register the AP to account #2
3. Record result
4. Note that this procedure can be repeated for boot Root/SP/Customer hierarchies or SP/Customer Hierarchies

Anticipated result: The registration with SP Account #2 should succeed.

Client datapath networking

The TIP Compliant controller and AP supports both local breakout and tunneled datapath setup.

Setup:
1. One AP connected to the controller
2. One tunnel end point appliance with a reachable IP route from the AP

Steps:
1. Provision SSID-A in bridge Mode using VLAN-A
2. Provision SSID-B in NAT mode
3. Provision SSID-C in bridge mode using VLAN-C
4. Provision an L2GRE tunnel in the AP profile to map to VLAN-C
5. Connect client devices to SSID-A, B, C
6. Ensure end user traffic integrity on the 3 SSIDs
7. Using the Tunnel End Point Appliance management panels, ensure performance counters indicate traffic from VLAN-C

Anticipated result: Client device traffic shall be supported in local breakout mode and L2GRE tunneled mode.

Summary:

What does this test prove?	Business Impact

Architecture is flexible to meet different scenarios, including brownfield scenarios and can replace existing Wi-Fi infrastructure	Enables operators to minimize disruption to existing network architecture and easily slot in TIP Open Wi-Fi architecture as they upgrade their networks Enables multiple verticals, including Enterprise IT (where local offload may be more dominant) to operator run networks (where tunneled architecture may be more dominant)

Wi-Fi AP

AP dual partition test

Objective: This test for the ability to manage the redundant software banks of the APs

Test setup:
One AP connected to the Controller running a valid APNOS software

Test steps:
1. Ensure the AP is connected to the controller and in-service
2. Using the Upgrade manager or the AP detailed panel, record the software revision of both AP banks
3. Load a new version on the inactive bank without activation and ensure service is not impaired
4. Verify the new load has successfully been transferred to the redundant bank
5. Activate the new software. The related software bank should become active and the previous bank standby.

Anticipated result: Software can be loaded on the AP without service interruption and activation can be performed at a later time during a maintenance window.

Summary:

What does this test prove?	Business Impact
Implementation helps increase the Wi-Fi network availability (one of the supporting features that can contribute to a high availability architecture)	Increases network availability, by reducing the probability of the equipment being down (reduced MTBF window) thereby increasing customer satisfaction and reduced impact to revenue or service requirements.

Manage Wi-Fi network Channel allocation

Objective: This test for the ability of the Controller to automatically manage AP channels in a Wi-fi network.

Test setup:
1. Setup the 3 access points in an office space (ensure at least 10m separation)
2. Initially turn OFF dynamic channel selection / RRM for both bands
3. Manually select the channels for 2.4 GHz and 5 GHz. Set at least 2 of the APs to the same channel on 5GHz.

4. Attach one or more STAs to the APs. Browse to Internet (or *ping* a server to validate access)

Test steps:

1. Record the manually set channels per AP
2. Turn ON dynamic channel selection and trigger an immediate location channel rebalance
3. Wait for 10 to 30 minutes (based on vendor implementation)
4. Record the channel settings

Anticipated result: The APs have selected non-overlapping 5 GHz and 2.4 GHz channels. Both primary and secondary channels are updated.

What does this test prove?	**Business Impact**
Dynamic channel selection works on both bands	Wi-Fi RF environments are dynamic and can vary by the hour. is a foundation feature or for making Wi-Fi APs as resilient and adaptable to RF change

Note: This test may be conducted by actively introducing interference on a given channel to raise its occupancy level and checking to see if dynamic channel selection picks a proper channel plan at the controller scheduled time.

Manage Transmit Power management

Objective: This test the ability of the Controller to automatically manage AP Tx power dynamically and associated Radio Physical layer key parameters

Test setup:

1. Setup 4 access points in an office space at 10m separation
2. Ensure auto Radio cell size management is enabled

Test steps:

1. Wait 45 mins for the Controller algorithm to establish proper cell size for each radio (TX Power and other related radio parameters)
2. Record all radio cell size parameters
3. Power down one AP
4. Wait 10-15 mins for the Controller algorithm to establish proper cell size for each radio
5. Record all radio cell size parameters

Anticipated result: The Controller should have pushed new cell size to the APs in the location to compensate for the coverage hole

What does this test prove?	Business Impact
Auto Tx power can dynamically adjust power levels to reduce co-channel interference	Reduces/eliminates the need for manual planning of Tx power levels. Can reduce setup costs and OpEx costs.

DFS support

The TIP APs and Controller fully support the regulatory procedures associated with DFS. Using automated RRM Controller algorithms, the channel plan will include a secondary channel for each radio in case of DFS triggered switching.

Validation of the DFS operation requires specialized equipment to generate the required radar interference pulses.

More details can be obtained from the related RF Regulatory standards per country.

What does this test prove?	Business Impact
Increases the number of channels in 5GHz bands that could be used for user communication on Wi-Fi Mandatory requirements are satisfied for certification in many countries.	Higher probability to offer high bandwidth channels to end users (resulting in higher throughputs), while ensuring regulatory compliance

Client testing

Client: Layer 2 Roaming with PSK

Objective: Test for the ability of the clients to roam "seamlessly" or automatically across APs on the same L2 network

Test setup:

1. Connect at least 2 APs on the same L2 network, spaced 20m apart with overlapping areas of coverage
2. Setup the SSID-B with WPA2 encryption and map it all the AUTs here.
3. Attach one or more clients to a one of the AP by locating the client very close to the AP (or power off the other APs and ensuring that the client only attaches to SSID-B: AP-1, for example)
4. Record the AP and client mapping

Test steps:

1. Walk from AP-1 to AP-2, while streaming video and observing the attach status (Wi-Fi icon) on the client.
2. When close enough to AP-2 and far away from AP-1, the phone should have roamed from AP-1 to AP-2, without requesting the user to re-authenticate (Seamless roaming)
3. Record events on the controller indicating the phone has roamed (vendor specific)
4. Record any glitches (temporary pause or delays) in the video streaming experience
5. Repeat steps 1-4 with an RTP based UCC session such as Zoom.

Anticipated result: one or more clients have roamed seamlessly from one AP to another in the Wi-Fi network, with minimal disruption

What does this test prove?	**Business Impact**
Support for Wi-Fi roaming	Seamless roaming is a proven customer delight factor Higher usage of Wi-Fi network

Client: Layer 2 Roaming with RADIUS

Objective: Test for the ability of the clients to roam "seamlessly" or automatically across APs on the same L2 network when authenticated using WPA2-Enterprise

Test setup:

1. Connect at least 2 APs on the same L2 network, spaced 20m apart with overlapping areas of coverage
2. Setup the SSID-B with WPA2-Enterprise encryption and map it all the AUTs here.
3. Configure a Radius profile associated with the SSID
4. Attach one or more clients to a one of the AP by locating the client very close to the AP (or power off the other APs and ensuring that the client only attaches to SSID-B: AP-1, for example)
5. Record the AP and client mapping

Test steps:

1. Ensure 802.11r is enabled on the controller
2. Walk from AP-1 to AP-2, while streaming video and observing the attach status (Wi-Fi icon) on the client.
3. When close enough to AP-2 and far away from AP-1, the phone should have roamed from AP-1 to AP-2, without requesting the user to re-authenticate (Seamless roaming)
4. Record events on the controller indicating the phone has roamed (vendor specific)
5. Record any glitches (temporary pause or delays) in the video streaming experience
6. Repeat steps 1-4 with an RTP based UCC session such as Zoom.

Anticipated result: one or more clients have roamed seamlessly from one AP to another in the Wi-Fi network, with minimal disruption

What does this test prove?	**Business Impact**
Support for Wi-Fi roaming for AAA enterprise authentication	Seamless roaming is a proven customer delight factor Higher usage of Wi-Fi network

Captive Portal Client Authentication: Local AP Splash page with T&Cs

Objective: Tests for ability to redirect users to a splash page using a local AP web service and associated Captive Portal Redirect function using T&Cs

Test setup:

1. Connect one AP to the Controller
2. Setup the SSID-A with WPA2-PSK and Captive Portal authentication
3. Configure a Captive Portal profile associated with the SSID with T&C authentication and allowed pre-auth URLs

4. In the Captive Portal profile, input the T&C text and the Splash Page content i.e. logo, background color, etc.

Test steps:

1. Connect one client using PSK to SSID-A
2. Ensure the splash page shows up on the client device
3. Accept T&Cs
4. Ensure the client can reach the internet for any web sites
5. Attach another client device to the same SSID with PSK
6. Do not accept T&C
7. Ensure URLs on the Allowed list can be reached

Anticipated result: Clients can connect after accepting T&Cs. Allowed URLs can be reached without Captive Portal authentication.

What does this test prove?	**Business Impact**
Ability to adapt the architecture to different customer requirements	Helps monetization of Wi-Fi networks Enables brownfield migration from legacy Wi-Fi to TIP Open Wi-Fi

Captive Portal Client Authentication: Local AP Splash page with allowed users

Objective: Tests for ability to redirect users to a splash page using a local AP web service and associated Captive Portal Redirect function using an “allowed user” list

Test setup:

1. Connect one AP to the Controller
2. Setup the SSID-A with WPA2-PSK and Captive Portal authentication
3. Configure a Captive Portal profile associated with the SSID with User List authentication and allowed pre-auth URLs
4. In the Captive Portal profile, input the T&C text and the Splash Page content i.e. logo, background color, etc.
5. In the same Captive Portal profile, input a list of username and password

Test steps:

1. Connect one client using PSK to SSID-A
2. Ensure the splash page shows up on the client device
3. Enter a proper username and password
4. Ensure the client can reach the internet for any web sites
5. Attach another client device to the same SSID with PSK
6. Use an invalid username and password

7. Ensure the client does not get access to the internet

Anticipated result: Clients can connect after inputting successful credentials.

What does this test prove?	Business Impact

Client authentication with Hotspot 2.0

The TIP Compliant Controller and APNOS Software support the Hotspot 2.0 feature set associated with WFA Passpoint Release 1 and 2.

The testing of the feature set requires a full Hotspot 2.0 compliant backend server setup comprised of:

- Radius Authentication Servers
- Radius Accounting Servers
- 3GPP Authentication emulation
- OSU Servers
- Web Servers

The Hotspot 2.0 features requires configuration of the following Controller Profiles :

- HS2.0 Profile
- Operator Profile
- Identity Provider Profile
- OSU Profile
- Venue Profile
- Radius Authentication Profile
- Radius Accounting Profile
- OSU and Access SSID Profiles

A detailed specific test plan for Hotspot 2.0 / Passpoint is available from TIP and/or the TIP Compliance controller vendor. Link to Hotspot 2.0 test)

Client Rate limiting

Test Objective: Test for ability to offer differentiated services to users/clients, such as capping speeds

Test setup

1. Connect one AP to the Controller
2. Setup SSID-A profile with WPA2-PSK with passphrase-A
3. Setup SSID-B profile with WPA2-PSK with passphrase-B
4. Setup SSID-A with no rate limiting

5. Setup SSID-B with 5 Mbps rate limit

Test steps:

1. Connect client-A to SSID-A
2. On the client, run a "speed test" to a server in the Internet (e.g. Ookla speed test)
3. Record speed test results
4. Repeat steps 2-3 to get a reliable average speed test result.
5. Connect client-B to SSID-B
6. On the client, run a "speed test" to a server in the Internet (e.g. Ookla speed test)
7. Ensure the client maximum rate matches the rate limiting value (5 Mbps for example)

Anticipated result: Rate limiting per client is applied per SSID

What does this test prove?	**Business Impact**
That the TIP Open Wi-Fi network can enforce rate limit per SSID	Allows providers to offer differentiated service to consumers based on billing status, customer prioritization Enables ability to set rate limits down for some SSIDs while enabling higher throughput on other SSIDs that may be setup for public safety or emergency services (in the event of emergency)

L2 Client Access Control

ACLs (Access control lists) are rules by which to enable/disable certain aspects of a client device's behavior. This can be enforced via Layer 2 Mac address block /permit lists, Layer 3 IP address based or L4 (TCP/UDP) or L7 (https). In the first release of the TIP Compliant Controller, layer-2 MAC address blocking is supported

Test Objective: Test for ability to block client access using a layer-2 ACL

Test setup

1. Connect one AP to the Controller
2. Setup SSID-A profile with WPA2-PSK with passphrase-A

Test steps:

1. Connect client-A to SSID-A
2. Using the Controller client inventory table, record the Client Mac address
3. Disconnect the Client devices by "forgetting the SSID" in the client Wi-Fi setup
4. Enter the Client MAC address in the ACL list
5. Attempt connecting the client back to SSID-A

Anticipated result: The client device should not be able to connect to the AP

What does this test prove?	Business Impact
Wi-Fi Controller Policy Enforcement feature exists	Permits use cases that deny access to clients based on certain business rules. For example, an MDU tenant who is behind on rent may be denied internet access or an employee device is barred from the internet in line with company policy.

Daily Network Operations

AP Inventory/Status display

Test Objective: Verifies the ability of the controller to provide a summary high level information for verifying overall status of APs in the network

Setup:
AP state: APs A & B are booted up, registered on the network and are online (Up). APs C & D are “offline” (down). APs C & D are powered off.

Steps

1. Verify that the controller shows the correct statuses of APs: A, B, C and D APs per setup above. Verify APs, A & B are online. APs C & D are offline
2. Power up AP C and bring to a “service providing” state
3. Verify that the controller shows the correct statuses of APs: A, B, and C – Online while D is offline.
4. Power up AP D and bring to a “service providing” state
5. Verify that the controller shows the correct statuses of APs: A, B, and C and D – Online
6. Power off AP C and bring to a “offline” state
7. Verify that the controller shows the correct statuses of APs: A, B, and D – Online while AUT C is offline.

Anticipated result:

1. Verify that at all times, the controller reflects the correct status for the AUTs.
2. Verify that the configuration profile on the Controller for the APs, matches with the status of the AP as shown on the controller
3. Verify that the APs are running the S/W version as expected by the controller
4. This proves that the APs and controllers are in-sync at all times

Summary:

What does this test prove?	Business Impact
The controller reflects the status of the APs at all times (to the extent the AP communicates with the controller)	Table stakes feature: Avoids field visit to obtain status of the APs

Client Inventory/Status display

Test Objective: Verifies the ability of the controller to provide a summary high level information for verifying overall status of attached client devices in the network

Setup:
- Multiple APs
- Multiple SSIDs
- Client devices from different vendors attached to the various SSIDs

Steps
1. Ensure client devices are connected to the various SSIDs
2. Enable traffic tests on some of the clients

Anticipated result:
The client inventory tables should display all connected clients with their associated attributes such as: MAC address, IP address, SSID, AP, RSSI

Summary:

What does this test prove?	Business Impact
The controller reflects the status of the attached clients at all times	Table stakes feature: Avoids field visit to obtain status of the Client devices

Event and alarm Management

Repeat the setup as described in the test: AP Inventory/Status display

Anticipated result: Timestamped Events and alarms corresponding to APs going offline and online are displayed in near real time on the controller. If the TIP Controller supports alarm notification services, ensure alarms are sent via email to the right provisioned destination.

Summary: The test proves that TIP Open Wi-Fi publishes time stamped events that can be subscribed to by a 3rd party ecosystem player and used for such things as friendly GUI output etc. The TIP Compliant controller vendor may support a full extended set of alarms and events for AP and client status and events.

AP in Controller offline mode

Objective: Verify the ability for TIP OPEN Wi-Fi APs to continue to handle data from attached clients is unaffected, if the controller were to go “offline” from the perspective of the TIP Open Wi-Fi AP.

Setup:

1. The APs are up and running and connected to the controller
2. The APs are in a service providing state and at least one secure SSID exists
3. Client is attached successfully to the secure SSID
4. The client is able to browse access the Internet for the client.

Test Steps:

1. Record the state of the AUT (SW version, the SSID over which the STA(s) is providing service etc.), and for all STAs connected to the AP, observe the traffic already being serviced by the AP
2. Attach one or more clients to the AUT.
3. Now Via modifications to DNS entries or otherwise, ensure that the controller is "not reachable" from the AP. Ensure the AP is able to connect to the Internet.
4. Observe the AP status on the controller and the Client status on the controller. AP status is offline
5. Introduce a new client (client) to the network. This client will not be able to attach to the secure SSID
6. Verify that any previously connected client continues to access the Internet undisturbed

Anticipated result:

1. An AP in controller-offline mode can continue providing service to already existing clients
2. The AP state is reflected as offline on the controller
3. New client connections requiring authentication do not succeed

Summary:

What does this test prove?	Business Impact
Controller is essential for continued network optimization and troubleshooting. However basic WLAN services should be maintained with AP connections to the Controller.	Resiliency and uptime for existing attached clients provide some level of uptime in the presence of faults

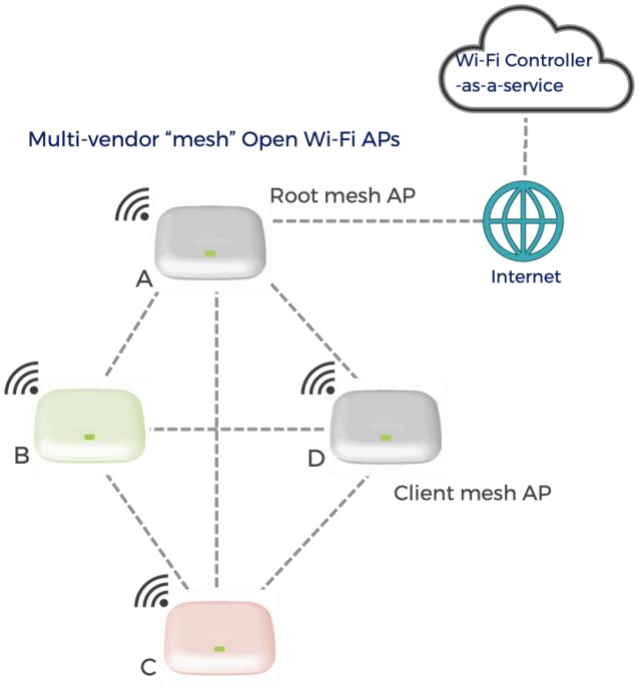
Client roaming across APs in controller offline mode

Client roaming attached to either WPA2-PSK or WPA2-Enterprise can roam across TIP Open Wi-Fi APs when the controller is offline (from the perspective of the APs)
Repeat the test steps described in Event & Alarm Management

Perform client roaming tests to ensure no loss of connectivity

Mesh topology

Background:



Expand Wi-Fi network with a meshed Wi-Fi AP

Objective: Test for TIP Open Wi-Fi compliant Wi-Fi network to be able to expand via wireless Wi-Fi mesh network

Test setup:

1. Set up an operational Wi-Fi network with at least 1 APs (A), with wired WAN connection to the Internet
2. On the controller virtually setup AP B, such that it too has the same relevant AP and SSID profiles as of AP A. Setup a secure SSID.
3. Setup a client to attach to the secure SSID.
4. Introduce a new AP, B, from another TIP Open Wi-Fi vendor.
5. Factory reset AP B
6. Ensure AP B has no wired connection to the Internet
7. Point AP B to the same controller as AP A (via DHCP or otherwise)

Test steps:

1. Record observation on the controller indicating AP A is the only operational AP on the network. And AP B is in an “unregistered” state.
2. Boot up AP B
3. After some time, Observe AP B has registered with the controller
4. AP B has the same secure SSID as AP A
5. Record observations on the controller, indicating AP B is “meshed” to AP A
6. Attach a client to AP B’s SSID. The client should attach seamlessly
7. Test the client for connectivity to the Internet

Anticipated Result:
The AP B connects to the controller, registers and upgrades to the latest software and configuration as specified on the controller and activates the Secure SSID. The AP B is connected to the Internet via AP A. The client attaches without further manual intervention to the secure SSID on the meshed AP B and is able to browse the Internet

What does this test prove?	Business Impact
A new TIP OpenWiFi AP can mesh into a TIP compliant Wi-Fi network	Industry unique feature - avoids AP-Controller lock in. Greater choice (and likely competitive prices) for Wi-Fi providers when procuring APs and Controllers. Wi-Fi mesh feature ensure rapid deployment of APs without the need for wired WAN link and can extend an existing Wi-Fi network Clients are agnostic to the nature of the AP (root AP or meshed AP) and get seamless service

Multi-hop Mesh network

Objective: Test for TIP Open Wi-Fi compliant Wi-Fi network to be able to expand via a multi-hop wireless Wi-Fi mesh network

Test setup:
1. An operational Wi-Fi network exists with APs A and B with AP B meshed to AP A (as per test: Expand Wi-Fi network with a meshed Wi-Fi AP, 5.2).
2. Introduce a new AP, C.
3. Provision AP C on the controller
4. Factory reset AP C
5. Ensure AP C has no wired connection to the Internet
6. Point AP C to the same controller as AP A (via DHCP or otherwise)

Test steps:
1. Power off AP A (the root AP)
2. Ensure AP C connects to AP B

3. Power on AP A
4. Record observation on controller indicating a multi-hop network in existence with AP A as the root AP and APs B and C as meshed AP.
5. Attach a client to the SSID for AP C
6. Browse to the Internet on the client, indicating AP C is providing service
7. Turn of power to AP B
8. Observer on the controller that AP C is in an “controller offline mode” with no ability to reach the controller
9. The client is unable to browse to the Internet

Anticipated Result:

1. In a mesh network it is possible to connect to a designated AP. AP C connects wirelessly to AP B.
2. The network was expanded via a multi-hop (2 hops). Clients were able to get Wi-Fi service without the AP C connected via a wired port or connected directly to a root AP.
3. Clients are dependent on state of intermediate APs to access the Internet.

What does this test prove?	**Business Impact**
A new TIP Open Wi-Fi AP can mesh into a TIP compliant Wi-Fi network, connecting to another mesh AP in the process	Multi-hop Wi-Fi mesh feature ensure rapid Wi-Fi network expansion, without having to connect to a wired WAN AP directly Large scale Wi-Fi mesh networks can offer flexibility and savings on the switch port side, as not all APs will need to be directly connected to a switch port.

Full mesh mode resiliency

Test Objective: Create a 4x4 mesh AP to demonstrate the inherent resiliency of mesh networks

Test setup:

1. Setup a 4 APs with at least 3 of the APs in full Wi-Fi mesh mode, with at least 2 of the APs belonging to two different TIP Open Wi-Fi compliant AP vendors. One of the APs (A) functioning as a mesh root AP.
2. Ensure one of the 4 APs is a “root AP” with a wired WAN link.
3. Setup at least one SSID profile enabling a client to attach and browse to the Internet
4. Setup a client that can connect to the said SSID and browse to the Internet
5. Ensure all APs are “in-service” (a service providing state)

Test steps:

1. Record observation on controller indicating a 4x4 mesh network as shown in picture
2. Note that the Wi-Fi mesh network is self-forming with the APs connected to multiple APs via a wireless mesh backhaul network (Self forming feature)
3. Attach a client to AP C and test that the client can successfully access the InternetThere are at least three paths for the client to access the Internet: via APs B and A or APs D and A and APs, B, D and A
4. Via controller logs and/or events or GUI (Vendor specific) or sniffer tools, record the path taken by client attached to AP C, when accessing the Internet (observations 1)
5. Assume the traffic from C goes via B.
6. Turn off power to AP B
7. record the path taken by client attached to AP C, when accessing the Internet (observation 2). The client traffic goes via APs C to D to A to the Internet and back.
8. The client is able to continue accessing the Internet. Note: Depending on the vendor implementation, the client may notice a temporary disruption to the service that this then restored upon the client path switchover

Anticipated Result:
Per Observations 1 and 2, the self-healing nature of the multi-vendor Wi-Fi mesh is demonstrated when one of the APs is removed (goes down).

What does this test prove?	Business Impact
A full mesh network can provide resiliency. The test demonstrates the ability to rapidly expand Wi-Fi networks via mesh with the benefits of flexibility, self-forming and self-healing.	Wi-Fi mesh has inherent fault tolerance, ensuring higher system availability or Wi-Fi network uptime and minimal disruption to clients ensuring lower revenue disruption, and higher customer satisfaction

Future variation of this tests (may be dependent on vendor specific implementations)

1. Test for optimal path or least-cost path
2. Test for ability to specify a path ranking such that the Wi-Fi network fails over to the alternate path in a preferred order

Scale and Performance test

These tests may require a simulator to simulate client connection and performance loading

Maximum SSIDs

Test objective: Test for ability to configure the maximum number of SSIDs as specified by the manufacturer of the AP. It must be possible to provision a minimum of 8SSIDs per AP.

Test setup:

1. Setup the maximum number of profiles on the controller.
2. Map the maximum SSIDs per AP to each of the APs in the Wi-Fi network
3. Record observations shown on the controller (Events, GUI data etc.)

Anticipated Result:
The TIP Open Wi-Fi solutions allow multiple SSIDs (up to the max per AP) to be successfully configured on the APs up to the maximum limit per AP as specified by the vendor.

Max Clients per AP

Test Objective: Tests for the ability to attach maximum number of clients to the AP as specified by the AP manufacturer

Test setup:

1. Connect one AP to the controller
2. Configure SSID-A with WPA2-PSK
3. Configure SSID-B with WPA2-PSK with a maximum capacity of 25 client devices

Test Steps:

1. Gradually connect real or simulated client devices to SSID-A to the limit documented by the TIP controller vendor
2. Ensure the clients are present on the controller client inventory panel
3. Ensure all clients can run traffic
4. Gradually connect real or simulated client devices to SSID-B to the client limit provisioned (a.k.a 25)
5. Ensure the clients are present on the controller client inventory panel
6. Ensure all clients can run traffic

Anticipated Result:
The maximum controller documented number of clients can be attached. Client limit provisioning is functional.

What does this test prove?	Business Impact
AP can support what the data sheet claims	Helps in network planning

Appendix

Cloud controller Features

- Northbound API (see Swagger)
- Basic UI (NBI)
- Southbound Adapters (MQTT Telemetry, OVSDB + OpenSync, gRPC)
- Zero Touch Provisioning using X.509 Certificates
- Device Identity (Model, MAC, Serial Number)
- AP Software Upgrade
- Profile Provisioning Templates
- Multiple SSID Configuration
- Bandwidth Rate Control per SSID
- Multi-Radio 2.4/5GHz control
- AP Network Mode Control (Bridge/NAT mode)
- Basic Captive Portal (Local Splash Page admin from Controller)
- Security (WPA-Personal/WPA & WPA2 Personal Mixed/WPA & WPA2 Enterprise Mixed/WPA2 Personal/WPA2 Enterprise/WEP)
- VLAN per SSID
- IEEE802.11r Fast BSS Transition per Radio Control
- IEEE802.11k RRM Radio Information per Radio Control
- IEEE802.11v Network Assisted Roaming per Radio Control
- RRM Location AP Channel Table Provisioning
- RRM Location AP Cell Size Table Provisioning
- RRM Location Client Steering Threshold Table Provisioning
- NTP Enable/Disable
- Syslog Enable/Disable
- Management VLAN
- RADIUS Profile Management
- AP Alarm Aggregation and Device Status
- WLAN Service Usage Metrics (NBI & Bulk Retrieval)
- User Account Management
- Containerized Services – Cloud native & Agnostic Platform

AP NOS features

- IEEE 802.11b/g/n/ac (wave2)
- Wi-Fi 5, Wi-Fi 6 (2021)
- Dual Bank Bootloader
- Multi-SSID (8) per Radio
- SSID Authentication (WPA/WPA2/WPA3 Mixed, Personal, Enterprise)
- Un-Authorized Device List
- VLAN per SSID
- SSID Bridge Mode (IEEE802.1d domain per SSID)
- Dynamic & Static IP subnets per SSID
- SSID NAT Mode (with LAN mobility)
- Management VLAN
- NTP Client
- Background Scan Neighbor Discovery
- IEEE 802.11e WMM Upstream/Downstream Queues & L3 DSCP
- IEEE 802.11e Over The Air QoS EDCH Procedures
- IEEE 802.11e WMM-PS (Power Save)
- IEEE 802.11e UAPSD (Unscheduled Power Save) Procedures
- IEEE 802.11r Fast BSS Transition
- IEEE 802.11v Network Assisted Roaming
- IEEEE 802.11k Client Radio Resource Management - Directed Steering
- IEEE 802.11w Management Frame Encryption
- IEEE 802.11h Channel Switch Announcement (CSA)
- IEEE 802.11h Dynamic Frequency Selection & Transmit Power Control (DFS/TPC)
- Embedded Captive Portal (Local Splash non-auth)
- Link Layer Discovery Protocol (LLDP)
- Airtime Fairness
- Wireline & Wireless Tracing (PCAP Cloud Remote Troubleshooting)
- Synthetic Client (Cloud Remote Troubleshooting)
- Flight Recorder (Stack Remote Collection)
- Local Provisioning over SSID (when Cloud or WAN down)
- Multimedia Heuristics (Detection of Unified Communication Sessions)

- SSID Rate Limiting
- Inter-AP Communication (Client - Session Signaling)
- Client / AP / Network Metric Telemetry (MQTT)
- Provisioning profiles

Glossary

Example	Example
STA	Per IEEE, S**tation** (abbreviated as **STA**) is a device that has the capability to use the **802.11** protocol. E.g. Laptop, Smart phones, etc.
SUT	Station under test
Client	A user device that uses Wi-Fi for connectivity. Used in this document in most places in lieu of STA
AP	Access point. In this document this refers to a TIP Open Wi-Fi compliant Access point
Unregistered AP	The AP has not been previously provisioned (virtually) at the controller.
ZTP	Zero touch Provisioning. The ability to provision an AP out of the box, with little to none manual intervention
Root mesh AP	Also known as “root AP”. It is as defined by 802.11s. The root AP is typically connected by a wired WAN port. Mesh APs connect to a root AP
DFS	Dynamic Frequency Selection. If the AP detects that a radar is using a particular DFS channel, then it will exclude that channel from the list of available channels. This state will last for 30 minutes, after which the AP will check again if the channel can be used for WiFi transmissions