TELECOM INFRA PROJECT

TIP OpenWiFi Technical Requirements

Wi-Fi Solution Project 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.

Authors

Company (Alphabetic order)	**Contributors**	**Title**
Deutsche Telekom	Joachim-Fritz Westphal	Senior Architect, DTAG Strategy& Technology Innovation (CTO team) Co-chair, Wi-Fi Project group, The Telecom Infra Project
	Sascha Dech	Product Manager Seamless Connectivity, Telekom Connectivity Co-lead, Solutions & Applications Wi-Fi Project group, The Telecom Infra Project
Facebook Inc	Chetan Hebbalae	Connectivity Technologies & Ecosystem manager, Facebook Connectivity (FBC) Co-chair, Wi-Fi Project group, The Telecom Infra Project
Liberty Latin America	Amilkar Torres	Senior Director of Product Development
	Jose Quintero	Senior Director, Innovation Labs
	Paulo Simoes	Senior Manager Product Development
MTN	Leanne Da Cerca	Group Senior Manager: enterprise Connectivity
	Zaheer Sarang	Group Manager: enterprise connectivity
Vodacom	Khetan Gajjar	Executive head Fixed & Mobile, Technical & Commercial lead
	Dean Manefeldt	Principle Specialist: Radio Network Architecture Enterprise Network Services

Change Tracking

Date	Revision	Author(s)	Comment
11/15/2020	v0.1	Joachim-Fritz Westphal, Sascha Dech, Amilkar Torres, Jose Quintero, Paulo Simoes Leanne Da Cerca, Zaheer Sarang, Khetan Gajjar, Dean Manefeldt, Chetan Hebbalae	Draft version

Table of Contents

Requirements Terminology

This Requirement document follows the terminology recommended per IETF RFC 2119

The table below provides key excerpts on the usage of key words

Date	Revision
MUST	MUST or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the Requirement.
MOST NOT	This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the Requirement
SHOULD	There may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item.

Introduction

This document describes the technical requirements for a TIP OpenWiFi based WLAN network (referred to here as The TIP OpenWiFi network) across multiple verticals.

Audience scope: intended audience

The intended audience of this document primarily include:

1. Demand side CTO teams: Wi-Fi communication service providers (CSPs) such as MNOs, MSOs, ISPs, WISPs, SIs, MSPs etc.
2. Supply side: Wi-Fi solution providers or Wi-Fi vendors also called Original Equipment Manufacturers (OEMs) and independent software vendors or ISVs (to use a terminology made popular by the Microsoft ecosystem)

This document may also be useful to general IT, industry bodies or others looking for requirements around deploying Wi-Fi in different verticals

Wi-Fi solution providers or Wi-Fi CSPs:

Unlike cellular networks, unlicensed Wi-Fi network solutions are deployed by a wide array of CSPs including:

Licensed Internet Service Providers (ISPs) or Wireless ISPs (WISPs)	Mobile Network Operators (MNOs)	Managed services providers (MSPs)	System integrators (SIs)

For simplicity, in this document, the above categories are referred to as Wi-Fi Communication Service Providers or simply CSPs. Where a distinction needs to be made, this document will call out the specific role or specific nature of the service provider for clarity.

Note: That Enterprise IT or corporate IT also, in many cases, deploy Wi-Fi networks. However, they are not directly addressed in this revision. This document assumes that corporate IT is a customer of the above categories of CSPs (unless called out explicitly)

Wi-Fi vendors or OEMs (Other Equipment manufacturers):
This may include vendors who offer controllers and/or Access points. Suppliers include

- **Wi-Fi controller only vendors**: a relatively new category of Wi-Fi suppliers enabled by the use of standardized interfaces like OpenSync™, who may supply controllers as a software only solution available on-premises or in the cloud (software-as-a-service, SaaS)
- Access point hardware vendors or Original Design Manufacturing (ODMs) who supply designed and white label ready hardware to OEMs or to CSPs

A. **ISVs:** These are vendors who offer predominantly software driven solutions leveraging or interacting with the Wi-Fi network

Note: The technical requirements document will address the technical requirements that map to the Business requirements as laid out in the business requirements document

The TIP OpenWiFi Business Requirements can be found here.

Why TIP OpenWiFi platform?

The TIP Wi-Fi solution project group, under the umbrella of the wider TIP (The Telecom Infra Project) organization have come together to address industry gaps that have thus far, not been addressed by solutions available in the market. Our goal is to re-think various aspects of the Wi-Fi network and its use cases and unlock value. The TIP OpenWiFi offers:

1) a new class of Wi-Fi solution vendors who may specialize in either controller functionality or access point only functionality or both, while still retaining the ability to participate in large scale Wi-Fi deployments

2) an increase in the competitive choices and richness of Wi-Fi solutions available to CSPs - which we believe will naturally lower the total cost of operations (TCO)

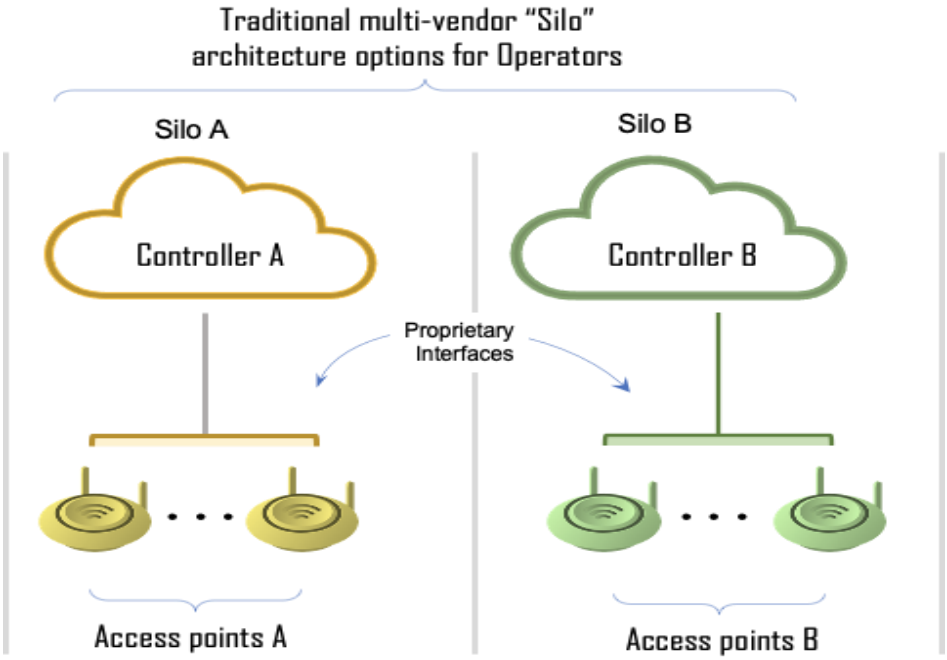
3) reduced the time and cost involved for new vendors to offer innovative solutions to the market by offering validated solutions that undergo automated testing in TIP's labs

4) Increasing the options for CSPs to get involved in requirements definition in the early stage, in order to drive their unique service differentiation, while still leveraging generally available solutions in the market

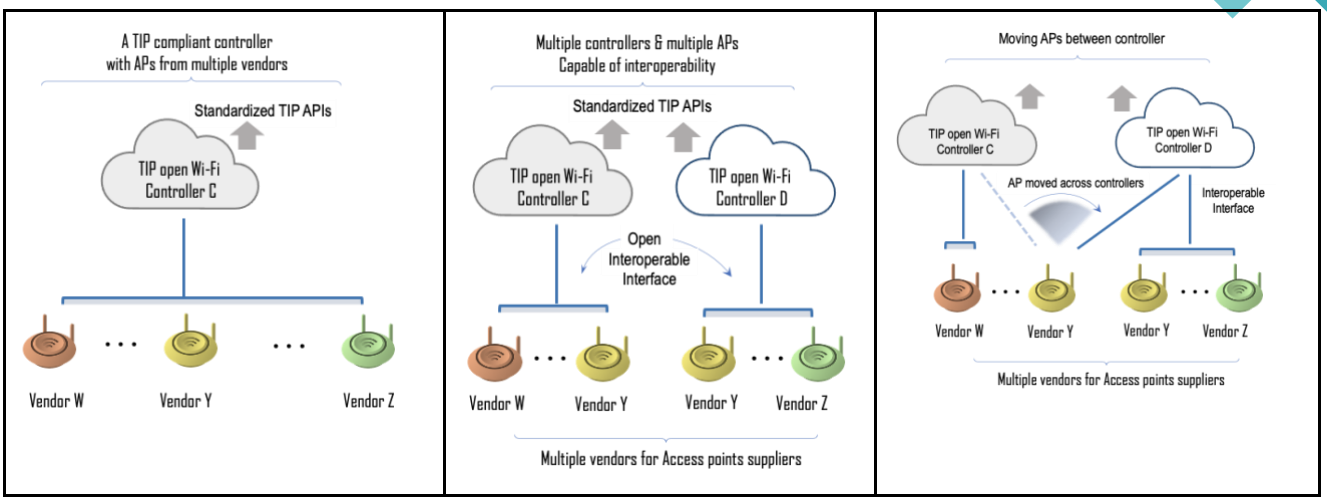
   Example: A CSP may choose to use a base open-source solution while ensuring that algorithms related to Radio resource management (RRM) are custom built to drive differentiation to their customer.

The TIP Open Architecture - Key Differentiation

Typical enterprise Wi-Fi network architectures use a controller and access points model with a proprietary interface between the controller and the access points, requiring that the set of controllers and access points be procured from the same vendor, limiting competitive choice and resulting in complex architectures requiring siloed deployments that can't cross manage APs across vendors.



The key differentiation via a TIP OpenWiFi architecture is the ability to mix and match a TIP compliant controller with TIP compliant access point(s), enabling CSPs to deploy controllers from one TIP OpenWiFi compliant vendor with access points from another TIP OpenWiFi compliant vendor(s)



A more detailed summary of TIP OpenWiFi Architecture is included in the appendix.

TIP OpenWiFi compliance definitions

- **TIP OpenWiFi compliant controller**: A controller that can successfully manage two or more TIP OpenWiFi compliant Access points, from different vendors, “out of the box” satisfying the set of use cases defined for compliance in this document is deemed a TIP OpenWiFi compliant controller

- **TIP OpenWiFi compliant access point**: A Wi-Fi access point that implements the baseline OpenSync Requirements and that can be managed from a TIP OpenWiFi compliant controller “out of the box”, satisfying the set of use cases defined for compliance in this document is deemed a TIP OpenWiFi compliant controller

- **TIP compliant solution**: A vendor solution that comprises a TIP compliant controller and a set of TIP compliant APs (preferably from two or more vendors) is defined as a TIP compliant solution

    - **Note-1:** It is possible to use the open-source TIP OpenWiFi compliant software to develop a “closed system” of controllers managing the vendor’s own APs only. Such a system while still utilizing TIP OpenWiFi open-source software would **not** be considered a TIP OpenWiFi compliant solution (Access points and controller)

    - **Note-2**: A controller from company A may manage access points from the same company A that are *NOT* TIP OpenWiFi compliant (potentially utilizing a proprietary protocol to manage interactions between the controller and the access point). In addition, company A controller may also incorporate support for TIP OpenWiFi Access Points. Such a controller would be considered a TIP OpenWiFi compliant controller, even though it is additionally managing other of their APs via a proprietary protocol.

Mandatory Use Cases Compliance Matrix

The minimum set of use cases required to earn the entry level TIP Validated Product (Silver) Badge and be considered TIP compliant are listed below. The actual use cases are defined in subsequent sections

The mandatory use case descriptions listed further in the document are marked with an asterisk (*)

Number	Use Case Title	Notes
1	Multivendor virtual provisioning	
2	Redirect to an Operator specified controller	
3	Multivendor Zero touch provisioning	
4	AP ownership transfer to another authorized TIP compliant controller	
5	TIP OpenWiFi Meshing use cases	
6	Network upgrade use cases	

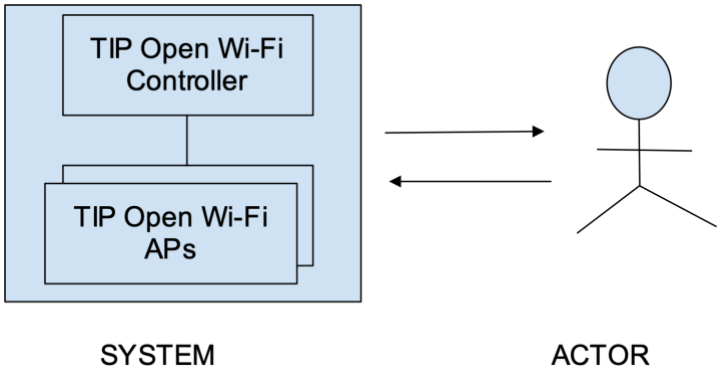
More information can TIP Test & Validation Badges and Ribbons can be found here.

System Use cases: Enterprise Wi-Fi for MDUs & SMBs

In most of the use cases below the Wi-Fi network comprised of the TIP Wi-Fi controller and APs is treated as the "System" with the operators with their admin role acting as the actor

System: The Wi-Fi controller + TIP Wi-Fi APs

Actor: The role-based operator(s) of the Wi-Fi network



System state definitions

This section defines the terms and inherent states mentioned in the use case below

1. AP connection states
   1.1. AP-admitted or unregistered: AP has made contact and been joined/mapped to the users account
   1.2. AP-Registered/unregistered/deregistered - The admitted AP has successfully been incorporated into the network
   1.3. A registered AP has successfully been removed from the Wi-Fi network
2. AP Operational states on the controller:
   2.1. Online In-service (INS) (maybe simplify this state to "Active")?
   2.2. Online out-of-service (SSID off for example, but AP responsive)
   2.3. Offline-N/A – Controller has lost contact with the AP. AP actual State unknown
   2.4. Others?
3. Alarm states: Critical, Major, Minor, Warning

Multivendor virtual provisioning*

Virtual provisioning (popularly called pre-provisioning)

Use case: The operator is able to log in to the controller and "virtually" specify the Wi-Fi network's required attributes, such as the AP hardware configuration, radio parameters, SSID names and attributes, the client authentication parameters (AAA), policy attributes and other required attributes, prior to any of the access point(s) physically being setup and operational in the network.

Redirect to an Operator specified controller*

Use case: The operator is able to specify a local controller or a controller in the operator's cloud of choice (private data center), redirecting the a TIP OpenWiFi away from it's default public cloud controller.

TBD: This operation may require access to the default public cloud controller at least once.

Multivendor Zero touch provisioning*

Scenario: APs from different vendors are successfully brought to a service providing state for the first time

Pre-condition:

1. TIP compliant APs are registered with the system
2. A TIP OpenWiFi controller is virtually provisioned with AP admit rules for provisioning of TIP compliant APs when the connect with the controller
3. The APs are assumed to be "out of the box" with factory installed software and appropriate certificates

Use case:

1. TIP OpenWiFi APs, preferably from two or more different vendors, are shipped to the field, in vendor supplied boxes
2. The APs are unboxed and installed correctly in the field by an authorized installer
   The installer should require no specialized knowledge for bringing the APs to operational state
3. The installer validates that the APs are installed as per requirements (location, connected to an approved prior source) and the APs powerup successfully (Green led light visible for example)
4. Upon powerup the APs contact the controller successfully
5. The TIP OpenWiFi controller "admits" the APs to the system, using the rules specified by the operator, configures the APs to the admin designated

software version and the right configuration parameters, per virtual provisioning rules and operationalizes the TIP OpenWiFi APs, bringing the APs to a "service providing state"

Successful Post-condition: The operator is able to bring up a network of APs from multiple vendors to an In-service (service providing state) without having to necessarily stage the APs in a lab prior to shipping to site and installing the APs. The operator can avoid training installers on the details of AP configuration, providing the option of outsourcing installation activity to lightly trained personnel.

Alternate scenario (for future consideration)

1. APs connect but do not match controller's rules for provisioning
2. APs do not connect with the controller successfully
3. The APs connect to the controller but are not recognized to be pre-configured in the system
4. An AP that has previously registered with an operator (i.e., admin account A) attempts a connection attempt to another admin account (admin account B)
5. The APs are flagged as "missing" (APs reported as lost by one operator show up on another operator's network)
   Note: A main use case to report an AP as "missing" is required.

AP ownership transfer to another authorized TIP compliant controller*

This use case is a unique TIP OpenWiFi differentiation (as compared to proprietary Wi-Fi solutions today). A TIP OpenWiFi system permits (a) APs from different vendors to connect to a controller from another vendor and (b) the operator to transfer AP ownership between controllers belonging to the same or different operator.

Pre-condition:

1. A TIP OpenWiFi compliant solution "A" exists with multi-vendor APs in an In-service operational state
2. A TIP OpenWiFi compliant controller or alternative solution "B" exists with TIP OpenWiFi controller in an In-service state

Use case:

1. Operator initiates a command on TIP OpenWiFi compliant controller A to "Transfer ownership" of one or more APs, indicating the address of controller B for the APs to connect to
2. The system confirms, acts on the command and responds with a successful response indicating the de-registered APs
3. The APs disconnect from controller A and connect with controller B
   Note: The APs may undergo a reboot in the process. Implementation behavior
4. States, Events and Alarms on the system indicate the AP state, the events and alarms capture the admin credentials, the new indicated owner and the de-registered state of the APs

Post-condition: APs from different vendors transfer over from one controller to another controller, either within the same operator network or between operators.

- Permits operators to flexibly manage APs from two or more controller vendors. Enables operators to avoid vendor lock-in
- Permits operators to introduce a new controller to an existing network, balancing between different controllers or transferring ownership from one controller to another controller

AP upgrade and restart

For APs supporting store and switch features for software (e.g. implemented via dual partitions at bootup time), the operator is able to initiate an upgrade on the APs, without impacting the current operational state of the APs. The operator is able to have the upgrade take effect at a later point in time, for TIP OpenWiFi APs supporting the ability to download software and switch to the new software at a later point in time.

Use case:

1. The controller indicates the APs that support the ability to download software and restart at a later time on the new software (upgrade complete)
2. The Operator selects and initiates upgrade on a set of APs
3. Effecting the upgrade: For the APs that support the ability to download software and upgrade later, the operator is able to specific the time when the upgrade should take effect (Immediate, or alter point in time)
4. The controller downloads the new software to the selected APs and for those A in-line with the operator's command upgrade the APs to the new software immediately or at the time indicated by the operator
5. The controller provides a status indication of the success/failure of the upgrade action to the operator

Post condition: All the APs are successfully upgraded

Alternate scenarios:

1. Download fails for some/all of the APs (upgrade failure)
2. At the time specified, some/all of the APs fail to reboot to the new software (upgrade failure)

AP continually attempts to get to an operational state

Unless otherwise specified, TIP OpenWiFi APs will, in good faith without any operator intervention, attempt to get to an operational In-service state. To do so, the APs may utilize active and backup software partitions, where the AP architecture supports such a capability, in an attempt to get operationally In-service (active).

Example: An AP powered up in the field will try to boot up successfully to an "operational state of In-service" and connect to a controller via methods provided to discover and connect to controllers

RRM and Transmit power

The operator is not required to manually set the Wi-Fi networks' channels and power settings relying on the network smarts to determine the legal and right power and channel settings

Use case:

1. The operator selects the operating country and/or the regulatory region.
2. The controller will present the operator with a default option of letting the controller determine the power and channel settings for the AP(s), based on the country/regulatory region settings
3. The system will dynamically use the appropriate frequency channels without operator manual intervention, optimizing the Wi-Fi network, in accordance with the local RF environment
4. Events and displays will indicate to the operator the choice of channels and AP transmission power

Override default RRM and Tx Power behavior with manual settings

Use case:

1. The operator selects the operating country and/or the regulatory region.
2. The controller will present the operator with a default option of letting the controller determine the power and channel settings for the AP(s), based on the country/regulatory region settings
3. The operator overrides the default settings and manually sets the operating channels and/or the transmit power of the AP.
4. Events and displays will indicate the operator choice of channels and AP transmission power

TIP OpenWiFi Meshing*

Use case:

1. The operator is able to create a mesh Wi-Fi system with the APs meshing with each other with one or more of the APs acting as a "root AP" (with WAN ingress/egress).
2. The operator is able to able to add additional APs to the mesh system up to at least 10 APs in total creating a full 10x10 AP mesh system with the APs meshing with each other

Note: In practice, such a system may be inefficient due to the nature of how Wi-Fi protocols work over a shared medium.

3. The operator is able to suspend some of the mesh routes (or links) ensuring that mesh link is NOT used for routing client traffic or any type of broadcast traffic over those links
4. the operator is able to create at least a **two** hop Point-to-point links of TIP OpenWiFi compliant APs
5. In an environment where multiple TIP OpenWiFi compliant mesh APs exist, A TIP OpenWiFi system must mesh with only the APs under the same admin ownership. i.e., the APs only mesh to the APs under the same ownership, even though other TIP compliant APs may be in the neighborhood belonging to other owners

6. **Optional advanced requirement:** At the discretion of two operators, it should be possible for APs belonging to two different operators to mesh with each other

MDU use case

A catch all use case for setting up and operating in a multi-dwelling unit (MDUs)

Use case: The Wi-Fi network operator is able to offer building wide Wi-Fi service providing the different stakeholders like tenants with comprehensive Wi-Fi service across the individual apartments, in common indoor areas like corridors, gym rooms, club centers, and any office spaces as well outdoor areas like parks, and by swimming pools.
The operator can setup the Wi-Fi network such that

1. Multiple APs in the network all host the same secure WPA2 or WPA3 SSID; one service SSID hosted across multiple indoor/outdoor APs
2. The tenants can all login to the one secure service SSID with unique passwords per set of devices owned by a given tenant
3. A tenant using a Hotspot 2.0 protocol device can connect to the Wi-Fi network
4. The Wi-Fi network can offer guest access portal pages for guests and visitors
5. The Wi-Fi network can interface to an ID provider as part of the OpenRoaming™ consortium, permitting utilization of the Wi-Fi network by visitors or tenants, just as if they were connected to their local Wi-Fi network
6. At the discretion of the operator, visitors belonging to certain other operators or emergency personnel, can attach and utilize the Wi-Fi network, seamlessly without requiring any manual interaction
7. The traffic across the tenants and others are isolated from each other Implementation: separate VLANs
8. On a per SSID basis, the traffic can be tunneled to a central gateway of the operator's choice; WAG or a TWAG or locally offloaded at the building depending on the SSID

9. It should be possible to securely tunnel traffic from an SSID to an element in the operator's network. E.g: IPSec tunnels
10. The devices belonging to a tenant can communicate with each other even when they are geographically dispersed throughout the building, just as if they were located in the same apartment
11. Some of the APs can mesh with other APs in the network, as defined by the system configuration
12. Multiple operator personnel have access to the system based on their roles, with varying levels of access controls per role. These roles include
    1) Admin: ability to set any configuration parameter with global control over the entire Wi-Fi network
    2) Monitor: Ability to monitor any part of the Wi-Fi network with no ability to set any configuration parameter
    3) Monitor+: This is a monitor mode with the added ability to set a few key attributes like SSID password
    4) A monitor mode that allows monitoring of the network limited to specific buildings, for use by building manager(s).
13. The building IOT system (such as heating and cooling systems) can be connected to the Wi-Fi network and their traffic is isolated from the main traffic
14. A blocklist (blacklist) and a permit list (whitelist) can be established determining what URLs can be accessed or not

Post condition: The Wi-Fi network has been setup in the MDU

Technical Requirements

Initial network bring-up*

	Requirement headline	Requirement
1.	Multi-vendor Zero Touch provisioning (MV-ZTP)	The TIP OpenWiFi controller must be able to admit, configure and operationalize one or more TIP OpenWiFi APs, preferably from two or more different vendors, “out-of-the-box” out-of-the-box: The TIP OpenWiFi APs do not have to be setup (staged) prior to attempting to be managed by a TIP OpenWiFi compliant controller
2.	Unregistered AP	A TIP OpenWiFi Access point that does not satisfy rules of auto-admittance and provisioning on the TIP OpenWiFi controller must be rejected from joining the network and going operational and must be placed in a “quarantine” state awaiting manual resolution (reject/accept)
3.	Auto provisioning	When a TIP OpenWiFi AP is successfully admitted to the controller, unless explicitly authorized otherwise by the network admin, it must be automatically provisioned (with no manual intervention at run time) to have the right software and configuration parameters as required by the admin, before it can transition to a service providing state
4.	AP Ownership	An AP once admitted to a user’s account on the controller cannot be automatically “claimed” by another admin account on the same or different TIP OpenWiFi controller
5.	Transferring AP ownership	It must be possible for a TIP OpenWiFi compliant AP that has been admitted to a user’s account on a given controller, to be transferred to another admin account on the same or a different TIP OpenWiFi controller

Access points

	Requirement headline	Requirement
1.	Dual partition failover	An AP that is unable to boot up successfully to a service providing state, should fallback to backup software on-board the AP and attempt to move to a service providing state
2.	Automatic channel assignment	TIP compliant APs must support the ability to automatically set channels for a given frequency band per assignments per or per regulatory region (e.g. ETSI)
3.	Automatic transmit power per country or regulatory region requirements	TIP compliant APs must support the ability to automatically set AP transmit power for a given frequency band per country or regulatory region requirements
4.	Dynamic channel assignment	TIP compliant APs should support an option for APs to automatically select the operating channel at run time
5.	AP support for DHCP-1	TIP compliant APs must support DHCP option 43 enabling CSPs to direct TIP compliant APs to a controller of the CSP's choice
6.	AP support for DHCP-2	TIP compliant APs should support DHCP option 82
7.	DFS	A TIP compliant AP operating in the DFS bands must per the country/region DFS regulatory requirements
8.	SSIDs per AP	A TIP compliant AP must support at least 2 SSIDs per AP
9.	Hidden SSID(s)	A TIP compliant AP must support the ability to host hidden SSIDs
10.	VLAN to SSID mapping	A TIP compliant AP must support ability to map all traffic to/from an SSID to a designated VLAN
11.	Hotspot 2.0	TIP compliant APs should support Hotspot 2.0/Passpoint release 1.0 air interface Requirements
12.	Multiple PSKs per SSID	A TIP compliant solution should support the ability to map multiple passphrases or keys to a given SSID, in order to enable users to join the same SSID with different passwords Note: Typically seen in MDU scenarios or schools where users all use the same SSID, but join using different passwords

Authentication methods, Authorization & Accounting

	Requirement headline	Requirement
1.	WPA2-PSK	A TIP compliant solution must support WPA2-PSK authentication requirements
2.	WPA3	A TIP compliant solution must support WPA3 based authentication requirements
3.	WPA-2 Enterprise (802.1x)	A TIP compliant solution must support WPA-2 Enterprise (802.1x) authentication requirements including EAP based authentication methods
4.	Hotspot 2.0	A TIP compliant AP should support Hotspot2.0 air interface Requirements

5.	Guest Access	A TIP compliant AP should support the ability for guest access SSID with redirection to a built-in portal on the controller or to a 3rd party portal hosted independently
6.	OpenRoaming™	A TIP compliant solution should support the ability to authenticate a user via the OpenRoaming™ protocol
7.	RADIUS Accounting	A TIP compliant solution must support the ability to account for client data usage via RADIUS protocol Account Start|Stop support Accounting update when roaming rather that Accounting stop/ start
8.	RADIUS CoA	A TIP compliant solution must support the ability to enforce “change of authorization” directives from an authorized RADIUS server

Client device behavior

9.	**Requirement headline**	**Requirement Requirement**
10.	Client seamless roaming – L2	A TIP compliant solution must support the ability for client fast roaming across APs on the same L2 network Support for 802.11k, v, and r
11.	Client seamless roaming – L3	Roadmap: A TIP compliant solution must support the ability for client fast roaming across APs on different IP subnets
12.	Sticky client handling	A TIP compliant solution should offer an option to automatically dissociate a client from a given access point, if the Wi-Fi network determines that the client can be serviced better by another AP in the network For example: Apple devices maintain the Basic Service Set Identifier (BSSID)'s connection until the Received Signal Strength Indicator (RSSI) exceeds -70 dBm.
13.	Airtime fairness (ATF)	The TIP OpenWiFi solution should support Airtime fairness features

Client Data records

	Requirement headline	Requirement Requirement
1.	Client device identity and RF data - basic	The TIP OpenWiFi solution must provide the following information on client devices attached to the network 1) Client device mac address 2) Client device IP address 3) Client host name 4) Attached AP name and optionally IP address 5) Time of last attach 6) RSSI
2.	Client device fingerprinting - advanced	<to be filled>
3.	Client record (aka call data record)	A TIP OpenWiFi compliant solution must provide a means to obtain historic client device activity data including: 1) Client identity – MAC address and IP address of client 1) AP identity and timestamp – the AP to which the client had attached initially and timestamp 2) Other APs – the list of APs to which the client may have roamed and timestamp 3) List of URL requests generated by the client while on the network The requirement may be satisfied by having this data streamed to an offline server or stored on the controller

Infrastructure Operations & management

1.	**Requirement headline**	**Requirement**
2.	NTP	Time: The TIP Wi-Fi solution shall support NTP
3.	AP config attributes	A TIP compliant solution shall support the provisioning of the following attributes for an AP: 1) AP vendor name 2) user friendly name 3) AP lat/long 4) SSID profiles mapped to an AP 5) AP hierarchical group the AP belongs to 6) AP IP address 7) AP Venue Friendly name (used in Option-82 for personalized landing pages/ journeys) Note: Per vendor implementation, certain attributes may be populated automatically or overridden by manual provisioning
4.	AP inventory status data	A TIP compliant solution must provide the following information pertaining to AP inventory status: 1) AP mac address 2) AP logical/friendly name provided by the admin 3) AP IP address 4) AP running SW version 5) AP vendor name 6) AP SSID profiles mapped 7) AP hierarchical group
5.	Events	A TIP compliant solution must notify the admin of important “events” or status of interest that may occur in a Wi-Fi network
6.	Alarms	A TIP compliant solution must support “alarm indications” classifying an alarm into at least one of the 4 categories – Critical, major, minor, warning (Adopt standards from ITU X.733)
7.	Active software version	A TIP compliant solution must provide information on the active software version(s) running on the controller and the APs
8.	Backup software version	A TIP compliant solution should provide a view to the software version available on the controller and the APs
9.	Key statistics streaming interval	A TIP compliant solution must provide updates on key statistics at at-least a 15-minute interval
10.	Key Stats (metrics)	A TIP compliant solution must provide the admin with information on the following key stats (minimal set) 1) <to be filled> Stats across: APs, Client devices, traffic, RF and controller
11.	Role based administration	A TIP compliant controller and APs must at least offer the ability to set the admin role to either (a) full control or (b) monitor only mode full control: This provides the admin with ability to set configuration, upgrade and monitor the entire Wi-Fi network (default mode) monitor only mode: This is a view only mode enabling the

		ability to view the network without modifying any configuration attributes Note – Vendors may offer additional roles not listed above

Security & Policy Management – Infra & Clients

	Requirement headline	Requirement
1.	**Infrastructure**	
2.	Rogue AP detection	A TIP compliant solution must be able to detect and report the presence of a "rogue AP" (unauthorized AP) Definition: A rogue access point is a device not sanctioned by an administrator but operating as part of the Wi-Fi network. This could be an AP that is broadcasting the same SSID as the authorized AP but may or may not be on the network. Other definitions include APs attached to the L2 network, but not broadcasting the authorized SSID as well. Rogue AP detection and reporting are important for PCI compliance
3.	Rogue AP management	Future: Roadmap
4.	OpenRoaming policy	Future: Question: Can policy enforcement guidance be communicated to the WLAN infrastructure by the IDP?
5.	SSID Rate limiting	A TIP compliant solution should support the ability to rate limit the throughput of all clients for a given SSID
6.		
7.	**Security & Policy Management – Clients**	
8.	Client rate limit	A TIP compliant solution should support the ability to rate limit the throughput of specified clients attached to the Wi-Fi network The client rate limiting may occur via a policy enforcement directed by an external AAA or via a setting on the controller (implementation dependent)
9.	Client device block list	A TIP compliant solution must support the ability to block a set of devices to attach to the Wi-Fi network mapped per SSID or per AP Note: The implementation of the block list may use an external AAA (via RADIUS) and/or onboard capabilities
10.	Client device whitelist	A TIP compliant solution must support the ability to permit a set of devices to freely attach to the Wi-Fi network, mapped per SSID or per AP
11.	Access control – L2	A TIP compliant solution must support the ability to block or permit specific clients based on client MAC address
12.	Access control – L3	A TIP compliant solution must support the ability to block or permit destination or source IP address of traffic
13.	Access control – L4	A TIP compliant solution should support the ability to block or permit specific ports or protocols used by clients to access the Internet
14.	Access control – L7	A TIP compliant solution should offer the ability to block access to specified URLs

Mesh*

	Requirement headline	Requirement
1.	Multi-vendor mesh	A TIP OpenWiFi system must have the ability to mesh across TIP compliant APs from different vendors for up to at least 10 APs, with one of the APs acting as the “root AP”
2.	Multiple root APs	A TIP OpenWiFi system must have the ability to designate multiple APs as “root APs”
3.	Multi-hop mesh	A TIP OpenWiFi system must support the ability for at least 2 mesh hops
4.	NxN mesh	A TIP OpenWiFi system must support the ability for at least 10 APs to form a a full NxN (10x10) mesh system with one or more root APs
5.	Mesh to owners network only	In an environment where multiple TIP OpenWiFi compliant mesh APs exist, A TIP OpenWiFi system must mesh with only the APs under the same admin ownership
6.	Mesh ESSID/Passphrase	The operator must be able to create a controlled mesh passphrase, ensuring only the APs belonging to the operator can mesh with each other (even though the APs otherwise may be TIP compliant APs)

Network upgrade*

	Requirement headline	Requirement
1.	Bulk upgrade	A TIP OpenWiFi solution must support the ability to at least upgrade 10 APs at the same time
2.	Upgrade exception	It must be possible for the admin to have the Open Wi-Fi controller skip certain APs marked explicitly as exempt from software upgrade and configuration sync
3.	Controller upgrade	A TIP OpenWiFi solution must support the ability to upgrade the controller only without forcing an upgrade of the access points

Optional upgrade requirement:

4.	Scheduled upgrade	It should be possible to upgrade a TIP compliant AP such that the AP can store the new software version without interfering with current operations and at a later time as specified by the operator, actually make the upgrade operation happen. For example: The operator upgrades the APs during normal business hours. The APs however do not reboot and boot up on the new software until 3 a.m. the following morning when impact to most users, of an outage is considered likely low, by the operator.

	Scheduled upgrade	Future: Roadmap

LED cadence and Indications

	Requirement headline	Requirement
1.	To be defined in future requirements revision	

Appendix

Overview

The TIP architecture takes a “cloud first” approach to the architecture, implementing the controller solution in the cloud. This approach has the benefit of enabling controller-as-a-service (CaaS), eliminating the need for capital spend in deploying an on-site controller appliance. The architecture however still allows for deploying the controller as a software on a local server or an appliance, where on-site controllers are a requirement.

The Cloud controller utilizing an open source defined protocol, OpenSync, can communicate, manage and interact with TIP compliant access points (APs), provided by multiple AP manufacturers.

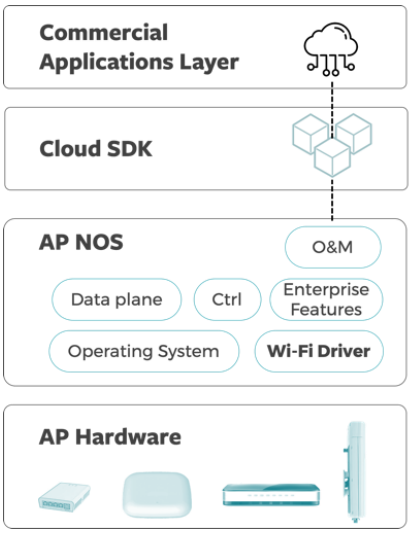
The main layers of the TIP OpenWiFi architecture are as shown in Figure 1: The TIP OpenWiFi solution architecture

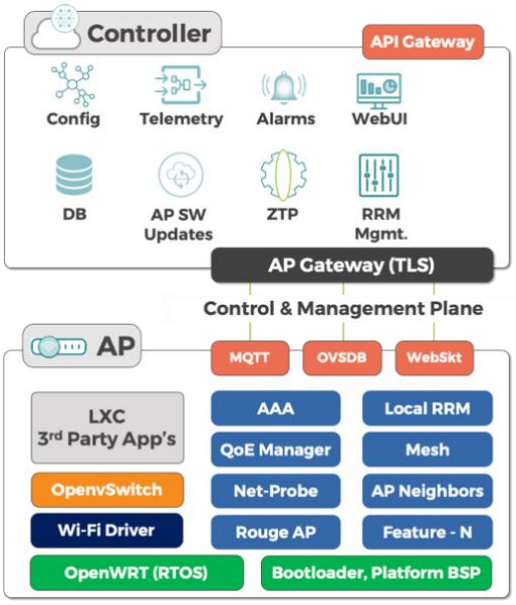
The edge layer – Access Points

The edge layer - Access points (APs): The AP Network Operating System (NOS) is an open-source driven AP Enterprise software designed to work with a TIP compliant cloud controller. It can, however, still function in a stand-alone mode, when communications with the controller are interrupted (with resulting loss in feature scope due to loss of controller implemented functionality).
The overall architecture approach ensures all APs are treated uniformly. And lower-level details such as whether it is a 2x2, 4x4, Indoor or outdoor access point, or wall plate access point are abstracted out.

TIP OpenWiFi AP provides a number of key features to enable abstraction of operation with multiple AP hardware platforms, radio configurations, network configurations, telemetry and zero touch provisioning. All AP functions are managed using the TIP OpenWiFi Controller.

For the latest hardware reference: The hardware PRD for TIP captures the requirements for TIP OpenWiFi Hardware and is updated as we progress through the development process.





The controller

A Wi-Fi controller for commercial availability is expected to include a base cloud SDK layer (described below) and a vendor implemented commercial layer that wraps the cloud SDK layer and offers value added vendor controller functionality.
The cloud SDK layer, as the name suggests, is implemented in the cloud. The Cloud SDK provides an abstract representation of a physical Access Point, acting as an intermediary layer that hides the details of access point architecture, and driver details from the north side “application layer”. A common data model is presented with OpenSync 2.x contribution southbound from Cloud SDK to TIP APs. Existing WLAN Cloud vendors may integrate with Cloud SDK’s Northbound APIs for simplified access to all TIP compliant Wi-Fi Access points.

In general, the Controller normalizes all data into a set of stream processors. The Community can access this data directly, extend the MVP UI environment via API, or build a unique product utilizing the Controller APIs and stream processors directly.

A Snapshot of features available in the MVP functionality stage includes:

- IEEE 802.11b/g/n/ac (wave2)
- Wi-Fi 5 Open-Source Driver
- Dual Bank Bootloader
- Multi-SSID (8) per Radio
- SSID Authentication (WPA/WPA2/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)
- OpenSync 2.0 Provisioning

The software delivery model:

The TIP project team has adopted a CI/CD model - continuous integration, continuous delivery, and continuous deployment, model. This approach introduces automated builds, testing and integration through the software development and delivery phase.

TIP members ensure daily builds and daily regression tests. Members have the ability to consume these daily builds or wait to consume a more substantial collection of features and builds which are then made available as major software releases out of TIP.

To enable the daily tests, TIP runs a number of test beds with test chambers containing physical APs, on which automated tests are run.

How TIP addresses today's Wi-Fi solution limitations?

For CSPs deploying Enterprise Wi-Fi solutions, the choices provided by vendors include stand-alone Wi-Fi access points that can be managed by SNMP, at one end of the spectrum, to tightly coupled architectures where the vendor supplies both access points (the hardware) and the controller with a deeply coupled proprietary protocol between the two.

Limitation faced by CSPs today	TIP solution to limitation	Benefits
Enterprise Wi-Fi networks choices are limited to controller and access point from the same vendor	TIP OpenWiFi architecture enables interoperability between the controller and the access point	Unlock value - CSPs can deploy best-in-class controllers and access points from different vendors, ensuring more choice of available solutions, to get to the desired best-in-class Wi-Fi network as a whole This added choice and competition is expected to offer competitive prices while offering Enterprise grade functionality
Lack of Enterprise grade Open Source solutions	OpenWrt provides a good foundation but is missing Enterprise grade features. TIP OpenWiFi builds on the OpenWrt foundation adding Enterprise “muscle”	Open-Source solutions implemented by the community, provide a faster route to market, with lower R&D costs, with options for vendors and manufacturers to pass on the savings to the CSPs