prplMesh: Open-source Implementation of the spec underlying Wi-Fi CERTIFIED EasyMesh™
Overview

- Multiple access points problem
- Wi-Fi CERTIFIED EasyMesh™
- prplMesh architecture
- Security
- Missing features
Multiple access points in house

Insufficient coverage
Multiple access points in house

Insufficient coverage → add access point
Multiple access points in house

Insufficient coverage → add access point → setup complexity
Multiple access points in house

More access points → more complexity
Multiple access points in house

More access points → more complexity → interference
Multiple access points in house

More access points → more complexity → interference → suboptimal use
Wi-Fi CERTIFIED EasyMesh™:
Smart, extended coverage home Wi-Fi®

Wi-Fi Alliance Multi-AP specification underlies Wi-Fi CERTIFIED EasyMesh
Wi-Fi Alliance Multi-AP specification

- Based on IEEE 1905.1
  - ethertype 0x893A
  - fixed multicast address
  - device “AL MAC” address

<table>
<thead>
<tr>
<th>version</th>
<th>0</th>
<th>CMDU type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message ID</td>
<td>frag ID</td>
<td>flags</td>
</tr>
<tr>
<td>type</td>
<td>length</td>
<td>value</td>
</tr>
<tr>
<td>value</td>
<td>type</td>
<td>length</td>
</tr>
<tr>
<td>length</td>
<td>value</td>
<td>type</td>
</tr>
<tr>
<td>length</td>
<td>value</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
Wi-Fi Alliance Multi-AP specification

- Based on IEEE 1905.1
  - Topology discovery
  - Onboarding (push-button)
Wi-Fi Alliance Multi-AP specification

- Based on IEEE 1905.1
- New CMDUs and additional TLVs
- Extended onboarding procedure
- Capability / metric collection
- Configuration, channel selection, steering
- Controller and Agent roles
WFA Multi-AP architecture
WFA Multi-AP Discovery
WFA Multi-AP Steering
WFA Multi-AP Onboarding
WFA Multi-AP Onboarding

Controller
Agent

Agent

WSC

Agent

Agent

Gateway

WAN

mind

prpl

THE LINUX FOUNDATION
WFA Multi-AP WPS
Implementation stakeholders

- Chip vendors start implementing Multi-AP
- OEMs want to use different chips without changing their software
- Carriers want interoperability and manageability
prpl Foundation

• An open-source, community-driven, collaborative, non-profit foundation

• Working on standards, APIs and software for IoT, embedded devices and the smart society of the future

• International membership of 30+ member organizations, and 200+ active engineers
prpl combines standardisation & open source

- **High-level API**
  A single API for on-device software

- **Low-level API**
  A single API for chipsets and SoCs
prplMesh Multi-AP implementation

- Open source reference implementation for Linux
- *Agent* ready for Wi-Fi CERTIFIED EasyMesh™
- *Controller* as differentiator
- Match with prpl APIs, add carrier manageability
- Contracted Essensium/Mind for implementation
• Delivers IEEE 1905.1a stack
  https://github.com/BroadbandForum/1905.1a
• Define architecture and interface for carrier management
  – QoS
  – metrics acquisition for diagnostics
  – ...
• Define additional test plans
prplMesh architecture

Control -> Data model

Data model <-> 1905.1 Multi-AP

Data model -> Platform integration

Data model -> Drivers

Drivers

Platform integration
prplMesh Data Model

local device

radio
phy0

radio
phy1

remote
device

radios

AP
SSID1

AP
SSID1

Backhaul
SSID2

BSSes
prplMesh Data Model

local device

radio
phy0

addAP()
→ cfg80211
+ hostapd

remote device

radio
phy1

addAP()
→ vendor driver
+ forked hostapd

radios

addAP()
→ Multi-AP CMDUs
OpenWRT platform integration

- **access**: prpl API
- **persist**: hostapd API
- **AP creation**: UCI, rpcd
- **metrics/control**: netifd, nl80211

**/etc/config**
Stretch goal: unified AP interface

access

prpl API

hostapd API

persist

UCI

rpcd

AP creation/metrics/control

socket

hostapd

nl80211

cfg80211

/etc/config
Multi-AP messaging is protected against out-of-network eavesdropping through utilization of encryption feature(s) of its underlying network connectivity.

A Multi-AP interface is considered authenticated when the underlying networking technology encryption mode has been successfully configured.
Missing features

- Specification of NAT/firewall/VLAN rules
- Separate networks (guest, fon)
- Quality of Service
- End-to-end authentication / encryption
- Controller election
Router with multiple bridges

- **lan**: wired LAN ports, PSK Wi-Fi
- **wan**: NATed from other bridges
- **guest**: open Wi-Fi, isolated
- **dmz**: PSK Wi-Fi, firewalled