An ALTEN Group Company

Whitepaper

802.11s Wireless Mesh Solution

Contents P.no

1.0. Abstract

Wireless Mesh Networking standards and technologies have been undergoing lot of developments in last 5+ years. After lot of deliberations and proposals, wireless mesh networking is yet to be leveraged by wireless service providers but certainly finding its use in various enterprise wireless scenarios as well as niche wireless deployment areas.

In 2011, the IEEE published the 802.11 amendment for mesh networking, named as 802.11s. This amendment primarily focused on mesh networks, resolving key issues such as WPA/WPA2 pre-shared key authentication attacks or frame collisions etc.

This whitepaper describes mesh networks, 802.11s amendment, and Calsoft lab's Wireless Mesh solution, applications and benefits.

2.0. Wireless Mesh Introduction

In 2003, the 802.11 working group defined the concept of a Wireless Distribution System (WDS) as a mechanism for wireless communication using a four address frame format (802.11 def 3.170) between access points. It was a simple definition, and indicated that the standard describe[d] such a frame format, but [did] not describe how such a mechanism or frame format would be used (802.11 def 3.170). With all the growth of wireless network usage today, the benefits of replacing an Ethernet cable with a wireless link certainly brings several benefits such as increased flexibility of a wireless link over a wired link. With wireless links, you may need a first access point to connect to a switch and the wired network, but then many other APs can connect through this first access point, even if they are miles away from the switch, and even if they are on moving objects (trains, cranes, etc.). Another benefit is in the path(s) taken by the wireless link. With an Ethernet cable, there is only one possible path from the AP to the switch. With a wireless link, any AP may be in range of one or several APs, and it can choose the best radio path. This ability of any AP to connect to one or several other APs, and the possibility for a redundant connection, is the very definition of a wireless mesh network. The multiple inter-mesh AP links form what is called the backhaul, as multiple users' data is backhauled through the mesh cloud to the main distribution points to the wired network.

2.1. Basic Features of Wireless Mesh Network

2.1.1 Flexibility

One of the key benefit and feature of wireless mesh network is increased flexibility of a wireless link over wired link. Since all the APs in the wireless mesh are connected to each other via multiple paths, the wireless mesh network provides great flexibility of deployment of the access points, locations and changes without disturbing wireless network availability for the stations. It also provided flexibility to chose best possible path from AP to the switch.

2.1.2 Backhaul

The wireless mesh network also support inter-mesh AP links providing what is called the backhaul, as multiple users' data is backhauled across the mesh.

2.1.3 Self-forming

Another key feature of wireless mesh network is self-forming. Usually an algorithm is embedded into a mesh AP's to detect best path to the wired network, building or expanding wireless mesh network may be as simple as adding new access points and making sure they are in the range of other access points. Rest all is taken care by embedded mesh applications running on the Mesh APs.

2.1.4 Self-healing

Wireless mesh network offers great redundancy for path to the wired network/switch via multiple wireless paths available within the mesh. This is self-healing feature of the wireless mesh network. If an access point has several possible paths to the wired network, and if the AP is able to automatically choose the best path, removing one access point in the mesh cloud simply forces the other access points to find the new best path to the wired network, without the need for a wireless engineer to be deployed to replace the missing access point.

2.1.5 Security

One of the key requirements for having intern connected wireless Mesh APs is security. As peering between two Mesh APs is a flexible process, the risk exists that a rogue mesh stations would peer with a valid mesh station, thus hijacking a legitimate bandwidth or offering rogue connections to fake resources or the wired network. Wireless Mesh usually supports secure protocols such as Authenticated Mesh Peering Exchange (AMPE) where the Mesh APs leverage either 802.1x or Simultaneous Authentication or Equals (SAE) methods for authentication.

2.2. Basic Features of Wireless Mesh Network

2.2.1. Benefits of Wireless Mesh Networking

- **Ease of planning and deployment:** Intelligent nodes mean less site surveying; indoor and outdoor nodes can coexist.
- **Reduced backhaul requirements:** Several nodes are able to use one wireless/wireline dedicated point-to-point or point-to-multipoint link.
- **Resilience:** Data packets have multiple paths and can be dynamically rerouted around failed nodes or interference transparent to the user.
- **Expandability:** New nodes can easily be added to self-adjusting networks.

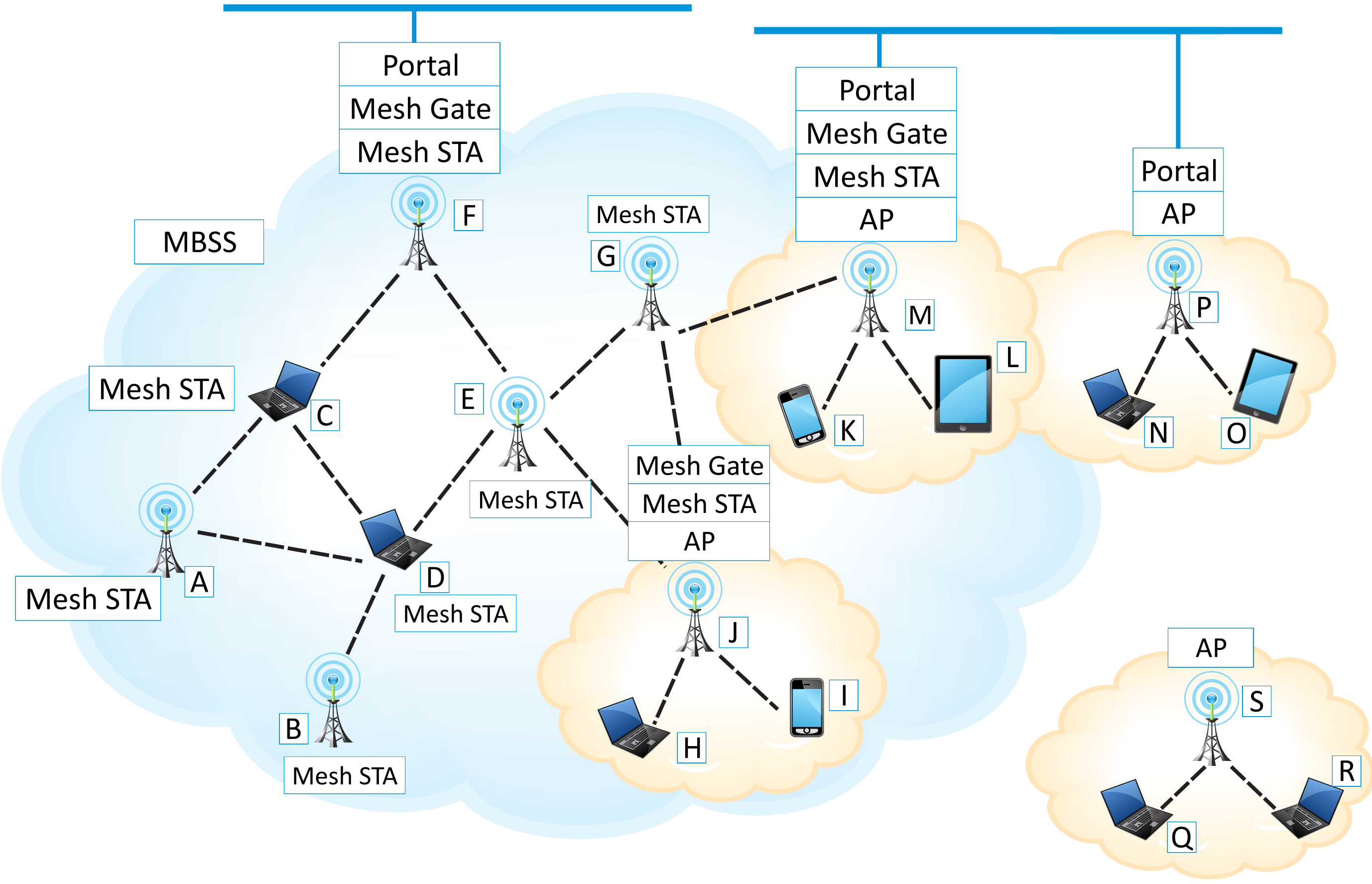
2.2.2. Issues with Wireless Mesh Networking

- **Latency:** The more nodes there are in the network, the more hops to route traffic, meaning increased latency.
- **Security:** Point-to-point communications are more predictable. Routing from multiple different nodes means greater vulnerability and exposure to unauthorized access if adequate controls are not established. Rogue access points can be easily set up within the mesh.
- **Non-incremental network deployment :** Meshes don't lend themselves to incremental approaches; they have to be almost completely built out within a coverage area to be useful.
- **Scalability:** Single mesh networks are generally not scalable because system capacity is reduced as more mesh APs are added. Dual- or multi-radio mesh where access and back haul radios operate on different frequencies increase scalability.

3.0. 802.11s Wireless Mesh Solution

3.1. Architecture Overview

Amendments for Wireless Mesh, 802.11s define various functions for wireless network elements including stations, access points and gateways. Following diagram depicts the architecture followed by definition/function/role of various network elements and protocols.



- **AP:** Wireless Access Point. (Nodes J, M, P & S in the above diagram)
- **Mesh STA:** Wireless Station (STA) that implements the mesh facility. (All Nodes except H, I, K, L, N, O, Q and R which are 802.11 clients or Non-AP STAs)
- **Mesh Gate:** Any entity that has mesh station (STA) functionality and provides access to one or more distribution systems, via the wireless medium (WM) for the mesh basic service set (MBSS). (Nodes F, J, M)
- **Mesh BSS (MBSS):** A basic service set (BSS) that forms a self-contained network of mesh stations (STAs). An MBSS contains zero or more mesh gates. (All nodes having the mesh Point or Mesh STA functionality run a MBSS)
- **Portal:** The logical point at which the integration service is provided. This is the node that bridges between 802.11 and non 802.11 networks. In the above diagram, Nodes F, M and P are portals bridging the wireless (802.11) and wired networks.
- **MCF (Mesh coordination function):** A coordination function that combines aspects of the contention-based and scheduled access methods. The MCF includes the functionality provided by both enhanced distributed channel access (EDCA) and MCF controlled channel access (MCCA).
- **MCCA (MCF controlled channel access):** A coordination function for the mesh basic service set (MBSS).
- **Precursor:** A neighbor peer mesh STA on the mesh path to the destination mesh STA, that identifies the mesh STA as the next-hop mesh STA.
- **Source:** A mesh STA from which a MAC service data unit (MSDU) enters the mesh basic service set (MBSS). A source mesh STA may be a mesh STA that is the source of an MSDU or a proxy mesh gate that receives an MSDU from a STA outside of the MBSS and forwards the MSDU on a mesh path.

Description:

The above architecture diagram gives sight of the different components of MESH networking, All the components might not be mesh capable device. In the above figure the End stations 'H' and 'I' are simple 802.11 clients associated with an AP functionality device. Nodes J for example, have both Mesh AP and Mesh point functionalities collocated on the same device. It associates with other MPs in the mesh when it becomes part of the mesh. Similarly, Nodes S , M and P have the functionality of the Mesh Point and AP co-located and they bridge the 802.11 data frames received from the clients to the Wireless DS links on the upstream MBSS. The nodes M, P depicts Portal functionality which serves the conversion of frame from Wireless to Wired interface. The node J depicts pure Mesh Gate functionality which serves the conversion of frame form MBSS(802.11s) to BSS (802.11). From the perspective of any mesh station in the MBSS, a next hop mesh station on the path to the destination mesh station is called a precursor mesh station. E is a precursor mesh station for J or D, their next hop on the path to mesh STA F.

3.2. Forming the Wireless Mesh

As mentioned earlier, the key feature of wireless mesh network is self-forming. As a mesh station boots up, it takes following steps to become part of a wireless mesh network.

1. Discovery
2. Peering
3. Security

3.2.1. Discovery

The station first need to discover mesh network and associated stations/access points. The discovery process uses the standard active and passive scanning mechanisms. Mesh stations participating in an MBSS sends

Mesh stations participating in an MBSS send beacons and answer to probe requests with probe responses. The major difference with standard 802.11 frames is that mesh stations' broadcasts and probes (requests and responses) contain several new elements. These elements form what is called the mesh profile. This mesh profile is a set of parameters that specifies the attributes of a mesh BSS; these attributes consist of a Mesh ID and multiple parameters advertised in the Mesh configuration Element. In a mesh BSS all mesh STAs use the same mesh profile. Mesh profiles are considered the same if all parameters in the mesh profiles match. A mesh station cannot establish a peering with another mesh station if their mesh profiles are different. A mesh profile consists of the following:

- **Mesh ID element** that uniquely identifies the MBSS.
- **Mesh Configuration element** that contains several subfields to describe the mesh capabilities of the local mesh station.
- **Path selection protocol identifier**, identifying which protocol is being used to determine the best path to the wired network or any destination in the mesh.
- **Path selection metric identifier,** identifying the metric used to calculate the best path.
- **Congestion control mode identifier**, identifying which protocol is used to manage congestion in the MBSS.
- **Synchronization method identifier**, identifying the synchronization method among mesh stations
- **Authentication protocol identifier**, identifying authentication method and protocol.
- **Mesh Formation Info element**, that specifies how many peers the local station has, and if the station is connected to the wired network or to a mesh gate
- **Mesh capability element**, specifying among other parameters if the station accepts new peerings.

3.2.2. Peering

After mesh discovery, two neighbor mesh STAs (STAs within direct wireless communication with one another) need to agree to establish a mesh peering to each other. After successfully establishing the mesh peering, they become peer mesh stations and can communicate directly with one another. A mesh station can establish a mesh peering with multiple neighbor mesh stations, and can also establish multiple peering sessions with a given neighbor, if necessary.

A key characteristic of the peering mechanism is to be a distributed, non-hierarchical, and non-exclusive agreement to communicate. Each mesh station manages its peerings with other mesh stations. When peering occurs, each side offers and agrees to parameters that define the conditions of the peering and the subsequent communications. Two peering modes are defined: a secured peering mode, through the Authenticated Mesh Peering Exchange (AMPE), and an unsecured peering mode through standard Mesh Peering Management (MPM).

Peering uses Mesh Peering Open frames, Mesh Peering Confirm frames, and Mesh Peering Close frames to establish, manage, and tear down a mesh peering. All these are also considered mesh management frames. Neighbour agrees to the peering if it has matching mesh profile and is set to accept peerings. Notice that the peering process has to occur both ways: each side has to offer attributes, and each side has to confirm the peering.

3.2.3. Security

The AMPE (Authenticated mesh peering exchange) uses Mesh Peering Management frames. Parameters are exchanged via the RSN element, the Authenticated Mesh Peering Exchange element, and the MIC element. The major functions provided by AMPE are security capabilities selection, key confirmation, and key management. During the AMPE handshake, the mesh STAs generate nonces and transmit them via Mesh Peering Management frames. The mesh STA shall generate a random value for its localNonce. The candidate peer mesh STA is expected to generate a random value for the peerNonce, which the mesh STA receives from the candidate peer mesh STA in Confirm and Close Action frames. Mesh Peering Management frames used in the AMPE are protected using the deterministic authenticated encryption mode of AES-SIV

3.3. Mesh Path Selection

Mesh networking involves selecting and maintaining the best path to the network. Usually vendor proprietary methods can be employed for path discovery and selection. However 802.11s requires a default path selection protocol to be supporeted by mesh station and that is Hybrid Wireless Mesh Protocol (HWMP).

3.3.1. HWNP

HWMP provides both proactive path selection and reactive path selection. A mesh station that needs to transmit a frame to an unknown destination can dynamically discover the best path to this destination. Mesh stations can also proactively discover the MBSS and determine best paths to any point of the mesh cloud before needing to send any data frame.

- **On-demand mode (Reactive):** The functionality of this mode is always available, independent of whether a root mesh STA is configured in the MBSS or not. It allows mesh STAs to communicate using peer-to peer paths.
- **Proactive tree building mode:** In this mode, additional proactive tree building functionality is added to the on-demand mode. This can be performed by configuring a mesh STA as root mesh STA using either the proactive PREQ or RANN (Root Announcement) mechanism. The proactive PREQ mechanism creates paths from the mesh STAs to the root, using only group-addressed communication. The RANN mechanism creates paths between the root and each mesh STA using acknowledged communication.

3.3.2. Path Selection Algorithm and Link Metric

Path discovery relies on Path Requests (PREQ) and Path Replies (PREP). Suppose that mesh station A needs to discover the path to mesh station D. Station A sends PREQ frames to all mesh stations in range. A station receiving an HWMP Mesh Path Selection frame containing a PREQ may reject it in some cases (the main case being when the receiving station has no information about the destination MAC address that is to be discovered). The station that has no path to the intended destination replies with a Path Error (PERR) message, that identifies the target address, the HWMP sequence number, and provides a reason for a rejection. When a station has a path to the target destination, the station accepts the frame and replies with a frame containing a Path Reply (PREP) element. Key subfields in the PREP element are as below.

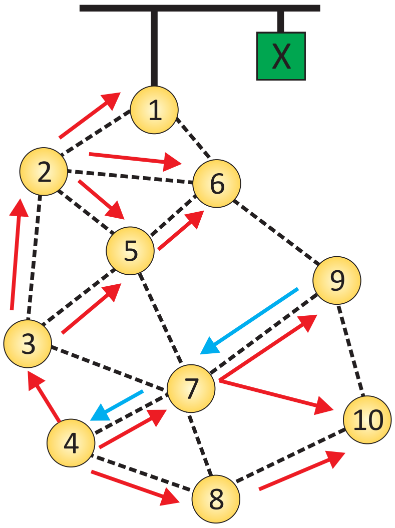
- **The target MAC address,** and the associated target HWMP sequence number as a PREQ may be used to discover several target MAC addresses.
- **The hop count to the target:** this critical element will allow the originator to know how far the target is, from the responding station standpoint.
- **The metric to the target:** this information will be combined with the hop count by the originator to determine a best path to the target.
- **Time To Live (TTL) field and a Life Time field,** used for loop prevention, just like for the PREQ process. This field is set by the responding station, and changed by the stations on the path back to the originator.

3.3.3. Path Selection Modes

The Path selection can be classified as four general cases to take as follows.

3.3.3.1 Reactive Mode

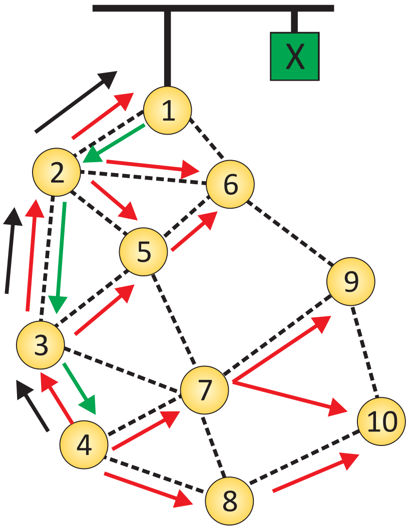
Scenario 1- Destination is Inside the Mesh: In figure below Mesh Node 9 wants to communicate to Mesh Node 9 which is in the MBSS.



Sequence of steps:

- MP 4 first checks its local forwarding table for an active forwarding entry to MP 9
- If no active path exists, MP 4 sends a broadcast PREQ to discover the best path to MP 9
- MP 9 replies to the RREQ with a unicast RREP to establish a bi-directional path for data forwarding
- MP 4 begins data communication with MP 9

Scenario 2- Destination is Outside the Mesh: In figure below Mesh Node 9 wants to communicate to Mesh Node 9 which is in the MBSS.

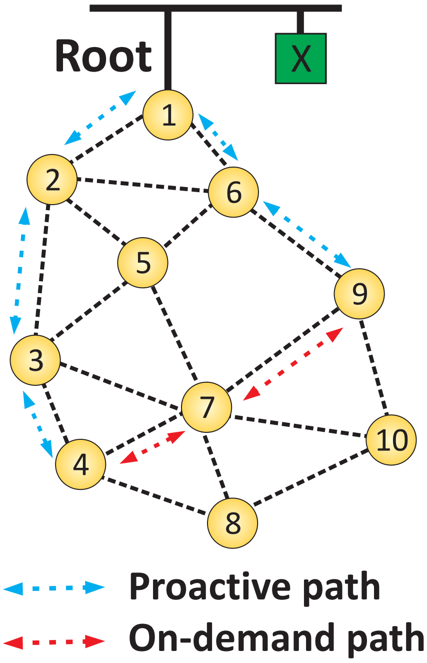


Sequence of steps:

- MP 4 first checks its local forwarding table for an active forwarding entry to X.
- If no active path exists, MP 4 sends a broadcast PREQ to discover the best path to X
- When no PREP received, MP 4 assumes X is outside the mesh and sends messages destined to X to Mesh Portal(s) for interworking Frame Format and Address Scheme.
- Mesh Portal MP 1 ` LAN segments according to locally implemented interworking.

3.3.3.2 Proactive Mode

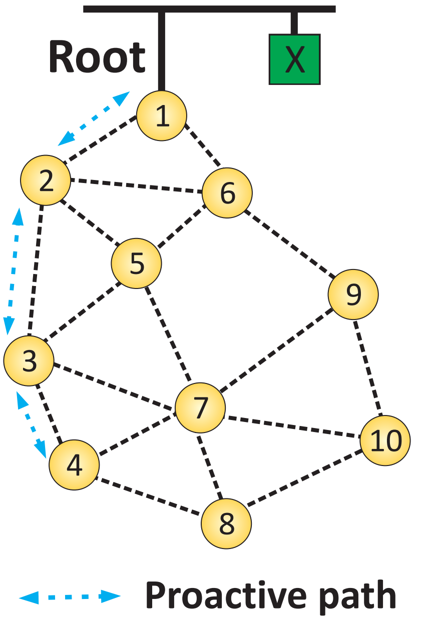
Scenario 1- Destination is Inside the Mesh: In figure below Mesh Node 9 wants to communicate to Mesh Node 9 which is in the MBSS.



Sequence of steps:

- MPs learns Root MP 1 through Root Announcement messages
- MP 4 first checks its local forwarding table for an active forwarding entry to MP 9
- If no active path exists, MP 4 may immediately forward the message on the proactive path toward the Root MP 1
- When MP 1 receives the message, it flags the message as "intra-mesh" and forwards on the proactive path to MP 9
- MP 9, receiving the message, may issue a PREQ back to MP 4 to establish a path that is more efficient than the path via Root MP 1

Scenario 2- Destination is Outside the Mesh: In figure below Mesh Node 9 wants to communicate to Mesh Node 9 which is in the MBSS.



Sequence of steps:

- MPs learns Root MP 1 through Root Announcement messages
- If MP 4 has no entry for X in its local forwarding table, MP 4 may immediately forward the message on the proactive path toward the Root MP 1.
- When MP 1 receives the message, if it does not have an active forwarding entry to X it may assume the destination is outside the mesh.
- Mesh Portal MP 1 forwards messages to other LAN segments according to locally implemented interworking.

3.3.4. Frame Format and Address Scheme

802.11s adds a mesh control field to the 802.11 frame as shown in figure below. The mesh control field starts after the normal 802.11 header and is interpreted as payload by a normal 802.11 STA. The 2 bit Address Extension Flag (AE) indicates which of the three addresses pairs are present in the mesh control field. The Mesh Address Extension is required in MBSS as three different source destination pairs can exist. These pairs can be: (1) One Hop away transmitter [ADD2] and receiver [ADD1], (2) Mesh Path source [ADD4] and Destination [ADD3], and (3) End to End source [ADD6] and destination [ADD5].

Frame Cntrl	Duration	ADD1	ADD2	ADD3	Seq Cntrl	ADD4	QoS Cntrl	Mesh Cntrl	Payload	FCS
2	2	6	6	6	2	6	2		0 - 7955	4

Octets

1				1	4	0.6.12 or 18		
Mesh Flags				Mesh TTL	Mesh Sequence Number	Mesh Address Extension		
AE	PS Level	RSPI	Reserved			ADD4	ADD5	ADD6

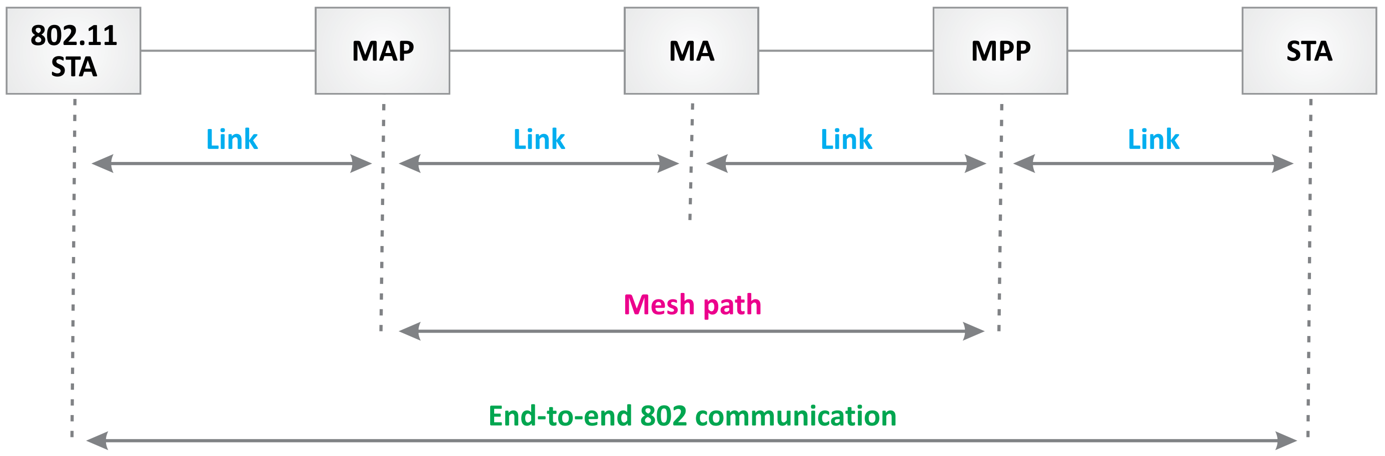
The ordering of the addresses should be from the innermost to the outermost "connections"

– Address 1 & 2 for endpoints of a link between RX and TX

– Address 3 & 4 for endpoints of a mesh path between a destination and a source MP Including MPPs and MAPs

– Address 5 & 6 for endpoints of an (end-to-end) 802 communication

- A series of mesh paths connected at MPPs (e.g., TBR in HWMP) or
- An 802 path between legacy STAs (including nodes outside the mesh) or
- Any mixture of them (e.g., an MP to an STA or vice versa).



4.0. Calsoft Labs Mesh Solution & Expertise

4.1. TECHNOLOGY EXPERTISE

Calsoft labs team has got a strong technical knowledge and knowhow on wireless protocol stack, 802.11s mesh protocol implementation as well as wireless mesh based custom solution. Calsfot labs wireless team has been closely following wireless industry trends and understanding implementation issues associated. Calsoft has 45 man years of Development experience and 40 man years of Product Verification (QA) experience on leading wireless and networking products development.

Calsoft team's expertise include various standards and technologies as below.

- **WiFi Standards**
  - 802.11a, b, g
  - 802.11e / WMM & WMM-SA
  - 802.11s
  - Security suites: (802.11i / WPA / WPA2)
  - 802.11h DFS, TPC & Measurements
  - 802.11d & 11j regulatory domains
  - Triple mode 2.4 GHz / 5 GHz bands
- **Wireless Products**
  - Access Point Development & Porting on Variety of Host Processors & WiFi Chipsets
  - Stations development
  - IBSS
  - MBSS
  - Standalone/Managed APs, Wireless Internet Gateways, Wireless Controllers, Wireless switches.
- **Wireless networking**
  - MAC filtering
  - Mesh Networking
  - L2 & L3 : Bridging, Forwarding, IPv4/V6 Routing
  - QoS & Differentiated Services (DiffServ), 802.1p, 802.11e : EDCA / WMM, HCCA / WMM-SA
  - Virtual AP / Multi SSID
  - CMOS based RF IP with Digital Interface to Baseband
  - NAT, Firewall , 802.1x Authentication, DHCP, PPP, Radius, Diameter
  - WDS Wireless Distribution System
  - WiFi chipset Drivers
  - Platforms : RTOS VxWorks, Embedded Linux,
  - Processors: Arm, MIPS, X86, Freescale, PowerPC
  - Drivers: Atheros Fusion SDK, MadWifi, mac80211 etc.

Calsoft team has delivered product engineering services for development and testing of various wireless products using latest, popular, third party or open source wireless technologies.

4.2 CALSOFT LABS OPEN 802.11S BASED SOLUTION

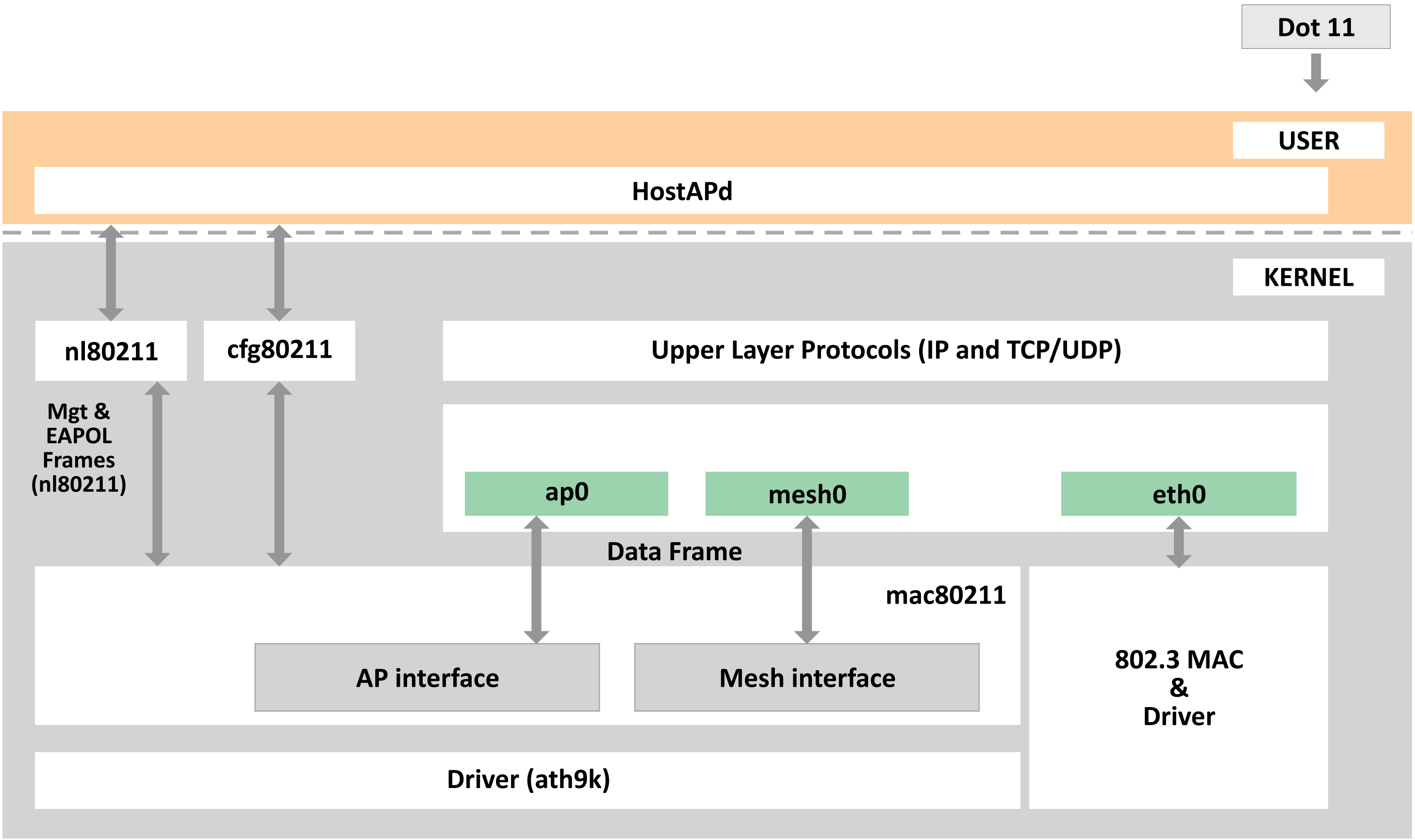
4.2.1. Open802.11s Porting

As part of Calsoft's Wireless stack development efforts and Calsoft's IP development strategy, Calsoft labs has ported 802.11s based wireless mesh solution and integrated with its wireless stack solution.

- Ported OpenWRT Attitude Adjustment Version on Atheros AR7100 with radio AR5416.
- Mesh Solution supports Dual radio and Dual band (2.4GHz, 5GHz).
- Security supported is AuthSAE(Simultaneous Authentication of Equals).
- Supports HT mode.
- Supports 2X3 MIMO.
- Supports HWMP Reactive and Proactive Mode routing.

4.2.2. Software Architecture for a Mesh AP Node

Typical architecture of a mesh AP is shown in following diagram, followed by brief description of each software element.



- mac80211 is a framework which driver developers can use to write drivers for SOFTMAC wireless devices.
- nl80211 is the new 802.11 netlink interface public header.
- cfg80211 is the new Linux wireless configuration API(Callback). cfg80211 replaces Wireless-Extensions.
- All the user applications make use of nl80211 to pass the respective configuration to the radio.
- In the above figure hostapd makes use of nl80211 to set the radio device in Master mode(AP Mode).
- Ath9k, ath5k are specific low level drivers for Atheros Chipsets.
- All the Mesh configuration will pass through nl80211, mac80211 in order to set a Mesh node on physical radio device using iw user space utility.
- Calsoft specific application DoT11 will be integrated in the AP to talk to the WLAN Controller to receive the respective mesh configuration and to send back the status , statistics to the WLAN Controller. The Dot11 app will make use of the nl80211.
- The WLAN Controller and AP will use CAPWAP protocol to communicate in between them.

4.2.3. Features Supported by Open802.11s

Following key features are supported by Open802.11s Implementation.

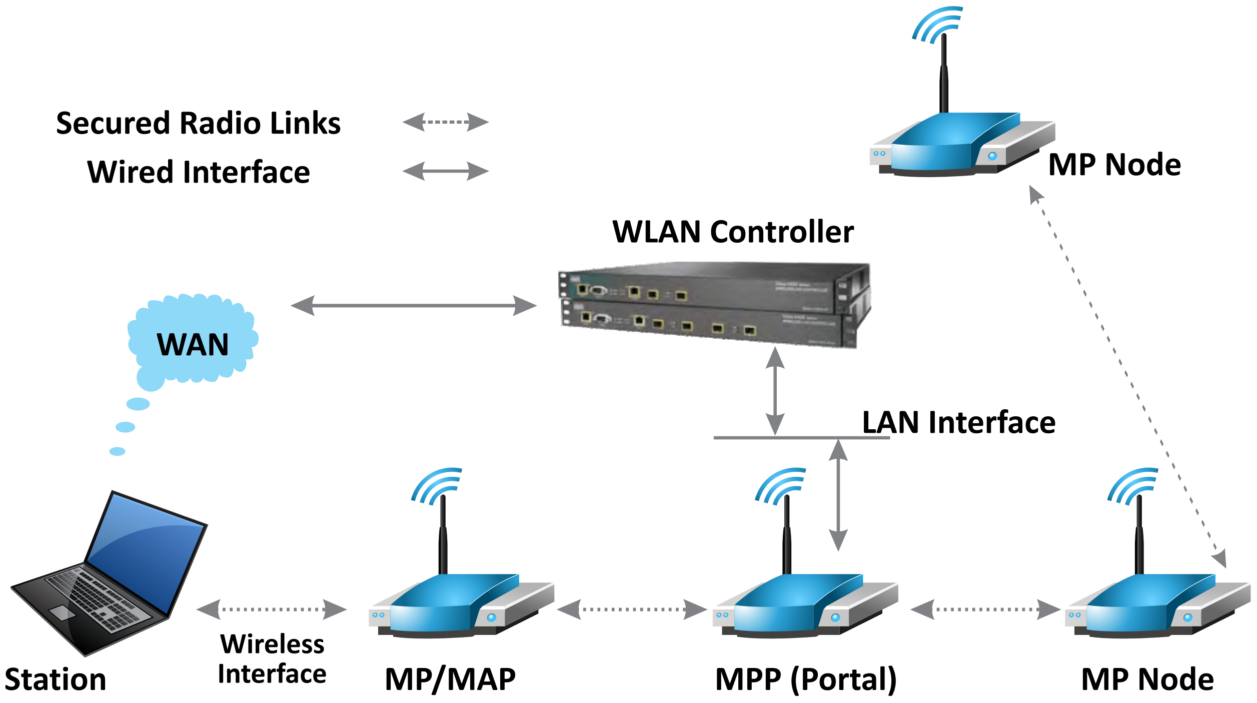
- Multicast/broacast frame forwarding with controlled flooding.
- On-Demand HWMP (based on hopcount, not airtime link metric) .
- Per-neighbor rate adaptation.
- Airtime link metric support for HWMP.
- Support for scanning mesh networks.
- support for authenticated mesh networks (using SAE) by extending nl80211, mac80211, wpa_supplicant.
- Mesh nodes that have access to external networks can now advertise themselves to other mesh nodes .
- Include QoS header on all mesh frames
- Experimental HT support

4.3. Integrated WLAN Controller Solution for MESH Networks

Wireless LAN Controllers are responsible for system wide wireless LAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility. They work in conjunction with Access Points to support business-critical wireless applications. Wireless LAN Controllers provide the control, scalability, security, and reliability that network managers need to build secure, enterprise-scale wireless networks-from branch offices to main campuses.

Wireless LAN Controllers smoothly integrate into existing enterprise networks. They communicate with Controller-based Access Points over any Layer 2 (Ethernet) or Layer 3 (IP) infrastructure using the CAPWAP protocol. These devices support automation of numerous WLAN configuration and management functions across all enterprise locations.

Following figure depicts the WLAN based MESH solution for various applications.



Configuring Mesh Node using WLAN Controller

The WLAN Controller functions as below -

- WLAN Controller identifies the MPP(Root AP) and does the necessary mesh configuration and initiates the Mesh scanning for other Mesh Nodes.
- MPP scans the neighboring MP nodes and gives the info to the WLAN controller.
- Mp-to-MP links are formed without the Controller's involvement. Bus as soon as an MPs mesh link is established with a peer MP, it tries to reach out to the Controller.
- As the new MPs discover the controller, and get activated at the WLAN Controller, the Controller further does the on demand configuration of the necessary MP nodes.
- All the information is now centralized by the controller device.
- Stations connect to MAP and talk to the non 802.11 stations.
- Each MP Node is directly managed by WLAN Controller.
- All configuration related to control are taken care by controller relieving AP for only Data forwarding. Less burden on AP.
- Dynamic and Automated MP Node load balancing to optimize overall WLAN system performance.

Benefits of WLAN Controller Based Mesh Solutions:

- **Quick Deployment Less Time for on the go operation:** Controller Based solution automates configuration, reducing Ethernet cabling and eliminating extensive RF planning, enabling Smart Mesh Networking WLANs to be deployed and operational in half the time of conventional WLANs. No extensive RF site surveys, cable runs, configuration, or optimization adjustments are required.

- **High reliability:** WLAN Controller directs the AP to pick the best signal path for traffic at any given time and automatically steers signals around interference to ensure high availability of mesh links.

- **Highly Secure:** All mesh back haul links between nodes are encrypted and hidden to ensure safe and secure operation.

4.4. Calsoft Product Engineering Services

Calsoft Labs provides specialized concept to market Product Engineering and embedded design and engineering services both established and early stage product and technology companies in select market segments which includes wireless technology products, access points, WLAN controller, wireless security products etc.

Calsoft WLAN product development expertise: With our extensive knowledge and experience with various WLAN products and chipsets, we can help you reach your productization goal quicker. We offer development and QA services for WLAN product development which could be a new product to be developed from the scratch or an existing product needing sustenance support and customizations based on your customer's requirements. In case of a new product – we can guide and help you through the product life cycle - right from helping you choose the right hardware to defining functionalities, to designing a solution best suited to your needs, implementing and testing it.

Calsoft Labs helps accelerate the development of products and reduce time to market through its expertise/ know-how, proven processes, methodologies, and tools. Calsoft's full lifecycle services include product development, testing and QA, sustenance, wireless and embedded engineering services, and embedded systems design. Calsoft's experienced engineers with strong expertise in leading edge WiFi technologies and evolving converged wireless networking technology landscape, help improve the quality and reliability of the products. Calsoft has helped several Fortune 500 and early stage companies ship some of the most widely used wireless networking appliances & software products in the world, on time and within budget.

About Calsoft Labs

Calsoft Labs provides specialized concept to market Product Engineering services to product and technology companies in select market segments. Our target markets include Automotive, Consumer Electronics, Media, Networking, Storage and Independent Software Vendors (ISVs). Calsoft Labs delivers unmatched business value to its customers through a combination of process excellence, reusable frameworks and technology innovation.

Calsoft Labs is a wholly owned subsidiary of ALTEN. Set up in 1988, ALTEN is a European leader in Engineering and Technology Consulting (ETC) with 15,950 employees in over 16 countries worldwide.

USA
2953 Bunker Hill Lane, Suite 203, Santa Clara, CA 95054
Phone : +1 408 755 3000 - Fax : +1 925 249 3031

INDIA
196, Bannerghatta Road, Arekere Circle Bangalore - 560076
Phone : +91 80 4034 3000 - Fax : +91 80 4034 3111

FRANCE
40 avenue André Morizet, 92514 Boulogne-Billancourt, France
Phone : +33 (0)1 46 08 70 00 - Fax : +33 (0)1 46 08 70 10