ALTEN CALSOFTLABS
AN ALTEN GROUP COMPANY

Innovate, Integrate, Transform

# WIRELESS 802.11S MESH NETWORKS, A TECHNO COMMERCIAL

# ABSTRACT

The constant search for longer range and increased scalability has stretched traditional wireless networks to the point where they cannot handle new requirements posed on the system. To compete with wired communication alternatives, wireless LAN has been evolving for a decade. To address large deployment schemes over a large dispersed geographical area, a paradigm shift in the technology was needed. Wireless Mesh networks have emerged the answer to such challenging problems for people who stretch the limits of technology in a constant endeavor to come up with game changing solutions. Although Wireless mesh networks have been around for some time, it is only recently that they have moved from the periphery to occupy center stage. In last couple of years, we have seen rapid deployment of Wireless Mesh networks in a variety of areas, including large multi-story building and even whole cities.

The economics of a Wireless Mesh network can be summarized by the simple fact that while traditional wireless LAN can only cover an area of up to hundreds of meters, 802.11s Wireless Mesh network can cover tens of kilometers practically, and up to hundreds of kilometers theoretically.

Given its greater mobility and scalability, Wireless Mesh networks are set to grow multifold in the market. According to ABI research, the Wireless Mesh market will achieve revenues in excess of $1.2 billion in 2010 alone. The same research claims that more than one million Wireless Mesh routers will be shipped in 2010. Industry estimates put the number of Wi-Fi chipsets in the market close to 500 million. These large numbers of chipsets that are already deployed can support wireless mesh without any hardware modification.

Considering these factors, Wireless Mesh network appears to be the sole evolution path and is here to stay. This is further validated by industry acceptance and support.


# INTRODUCTION

## *Potential for 802.11s Mesh Networks*

The driving force behind the wireless network arises from the user's desire for increased mobility. Traditional wireless networks have been in the market for a decade now and they have seen transformations in several areas, especially in terms of the width they offer, to the extent that they are now easily competing with their wired counterparts.

Having solved the problem of the inherent insecurity of the link that carries data through air with the advent of WPA/WPA2, wireless networking recently received a shot in the arm with the formal ratification of 802.11n standard that takes bandwidth to the new heights - up to 300 mbps more than a traditional 10/100 LAN. But the buck is not stopping here. Wireless LAN has been an important segment of the market that has been getting billions of investment in technologies, before they were standardized, simply because there has been a constant pull from the market. 802.11n has been witnessing the same phenomenal growth; almost every major vendor in this segment had an enterprise class product offering this extended bandwidth of 802.11n, long before it was formally ratified in the last quarter of 2009.

As the wireless network grows, it puts an increased demand on the infrastructure because infrastructure is wired and it cannot grow beyond a certain point. 802.11s Wireless Mesh network is a concrete step that addresses this paradox; to make infrastructure itself wireless. Consider a scenario where a small locality with an area of around 10 kilometers offers wireless network services with minimum wiring, and multimedia class bandwidth. Yes, this is now possible with the advent of 802.11s mesh networks. There are examples of complete cities covered by a Wireless Mesh network providing residential and business internet services, video surveillance for municipality office and numerous public safety applications.

802.11s Wireless Mesh is experiencing the same growth trajectory that 802.11n experienced. Even though no formal standard has been ratified, there are many heavy weights as well as smaller fish already competing in the market with their solutions, largely based on draft 802.11s.

Going by the current trend in the industry, the time is not far when every single wireless chip will be used to provide mesh services. That will be most natural culmination of all the efforts to provide mobility at the backbone. Eventually, as a natural evolution to wireless technology, 802.11s Wireless Mesh networks have the potential to create a huge market.

## WHY MESH

The natural question that crops up at this point is what is so good about mesh that it is becoming an inevitable technology proposition with the answer lies in the motivation of wireless LAN. Since Access points themselves are wired and they need a wired connection, either to a centralized controller or with the wired gateway, they cannot provide a coverage range greater than the range of a single radio. This range is typically in hundreds of meters. If we try to unwire the Access point and somehow make them wireless, so that they are able to talk to other similar creatures and create a data forwarding path consisting of multiple such nodes - in a manner similar to how the internet was built - we can then extend the range of such wireless coverage hundred fold, in the range of tens of kilometers. So range extension becomes an important driving factor behind the growth of Mesh networks.

On a similar note, Wireless Mesh networks remove the constraint of wired infrastructure. This means a mesh can be deployed with ease in hard-to-wire areas, in difficult terrains, in areas where environmental concerns prohibits wiring and in monuments. In such cases a mesh network is the only solution. The capability of a mesh network to create optimal forwarding links between themselves creates enough redundancy in the system to make it less prone to failure. Its inbuilt capacity for congestion control ensures uniform coverage in the mesh.

An added benefit of the mesh network is the ability of mesh devices to create a network among themselves, eliminating the need for a centralized device. This capability opens Pandora's Box. Consider a case of home networking where various household devices like a computer, a TV and an oven communicating with themselves, creating a self-sufficient wireless network. So with shorter hops in the forwarding path, high bandwidth will be achieved, not to mention reduced battery power consumption with the help of enhanced power saving mechanism.

## TYPICAL USE CASES

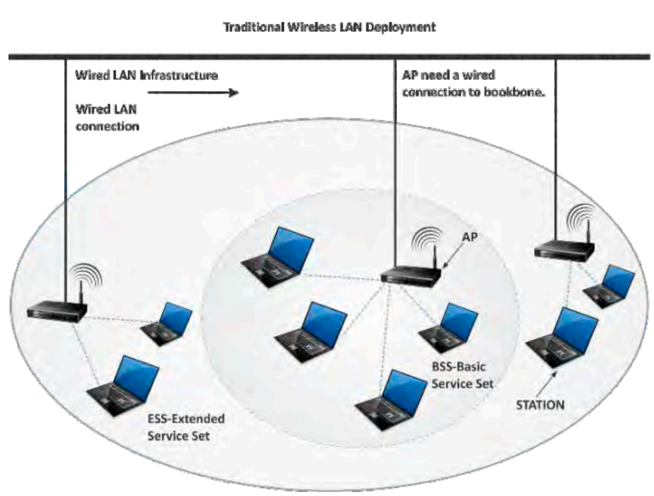
A mesh network can be deployed in a variety of situations with ease, at little cost and with little administrative overhead. Here are some of the major use cases for a mesh network that have been taken from actual deployments.

- Residential : In a typical residential use case, various devices in the home are connected via a Wireless Mesh network. This requires a low cost, easy to deploy and easy to manage, high bandwidth network system that also provides uniform coverage and eliminates the dead spot.
- Office : In an office deployment, the primary incentive to use a mesh network is increased mobility for devices and greater coverage. Capital cost on Ethernet cable installation can be reduced. Also network will be up and running in a minimal time, much faster than a wired or semi wireless counterpart. The mesh network also effectively addresses the two most important criteria for offices - reliability and fault tolerance.
- Campus, community, public access : The benefit of using mesh networks are realized the most in case of a campus or a community installation where covering a large area is the chief criteria. The main goal in this case is to provide seamless internet connectivity over a geographically diverse area in minimum time. The wireless backhaul lowers the cost and increases the bandwidth in comparison to wired media; this is especially true if there are many hard-to-wire areas that will escalate installation costs if a wired alternative is chosen. This also helps providing location based services for various administrative purposes.
- Public Safety : Public safety is an important area that has been mentioned in mesh drafts repeatedly. This is basically formalizing an ad-hoc network and connecting it to infrastructure networks. This can provide network access to all municipal workers handling routine or emergency calls in various city locations. This helps them connect to a central office for any kind of assistance or emergency response.
- Military : Military is another area that can exploit the full potential of a wireless mesh network. This can be gauged by the keen interest of major military hardware manufacturers in the standardization committee of 802.11s Wireless Mesh. For example, various units in a small geographical area can communicate with each other through a Wireless Mesh network that can be deployed rapidly and easily, and can also be removed with equal ease as units move forward.

## IMPLEMENTATION OF MESH NETWORKS

### *How Mesh Networks Work*

In traditional Wireless LAN, Access Points (APs) create a radio coverage area around themselves called a BSS. Several such BSS, when logically connected, create an Extended Service Set (ESS). This BSS is responsible for providing services to stations, to get associated to an AP and use LAN services. A representation of this is shown in the diagram below. The dark, solid black lines are wires of the LAN. The thin, dotted, black lines represent the wireless link between a station and an AP. The inner circle represents the radio coverage area of a single AP or the BSS. The outer oval shape represents the ESS - the logical coverage area of many such APs.

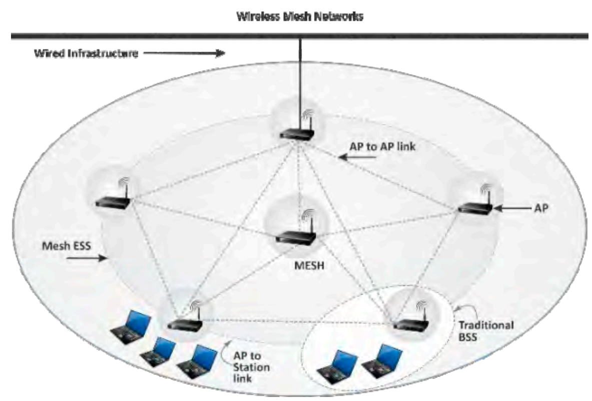


As can be seen from this diagram, the architecture requires that APs have a wired connection. This wired connection, that takes the data from a station to the outside world and vice -versa, is called a distribution system (DS). So the point here is that this architecture requires a wired Distribution System. Since DS is wired, the capacity of the deployment to offer greater range is limited because at some place in the path, it needs a wire. The effective coverage area is therefore restricted to the range that a single radio (AP) can offer.

The Wireless Mesh network offers a fundamentally different concept - Wireless Distribution System (WDS). The Distribution System that was wired in the traditional wireless LAN has been replaced with a Wireless Distribution system. This means that all the APs do not require a wired connection. They can act as a wireless forwarding node.

Refer the figure below. This is almost the same wireless network that has been described in the first paragraph, but it looks a little messy. That's what a Mesh network looks like. Here the 3 APs circled in green do not have a wired connection. They are merely talking to other APs and creating wireless links, depicted as thin, green, dotted lines. The inner oval shape represents the mesh ESS. These green links can carry the data from a station to its ultimate destination by using AIR as media, by forwarding the data to the next AP wirelessly which in turn takes the data to next AP and so on. This is the same hop-by-hop forwarding concept that powers the operation of internet.

This kind of self-organizing and self-configuring mesh is the fundamental concept ofmesh networks. True, that at least one AP require a wired connection if data has to travel to the outside world. But notice that the range of the wireless network has been significantly expanded and does not depend on the coverage area of a single AP. Even stations that are far away from the wired connection can access the network as green circled APs are acting on behalf of network to create a data forwarding path for the station. This is the basic working principle of 802.11s ESS Mesh networks.



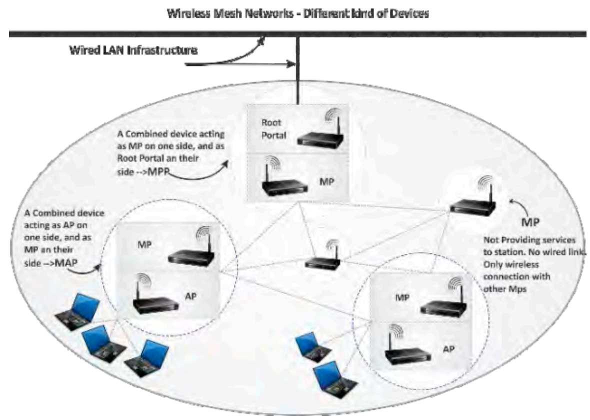

## TOPOLOGY AND DISCOVERY

Before we delve further into mesh networks, a brief about the various classes of devices in mesh is in order.

- Mesh Point : A mesh point is a device that communicates with its peer to make a forwarding path. It is only used for one hop communication to create peer link.
- Mesh Access Point : A Mesh Point that additionally supports station access or non-mesh nodes is called MAP. So an AP collocated with an MP that provides BSS coverage for a station is a MAP. In the figure below these are the devices circled in blue.
- Mesh Portal : A Mesh portal is an MP that acts as an exit and entry point for data that needs to travel outside the mesh or vice versa. It must have a non 802.11 connection to the internet. In the figure this is device circled in Grey.

These devices overlap each other in terms of the functionality they provide. Broadly categorizing an MP can act an MAP when it has the additional capacity to act as an AP or an MP can act as a Mesh portal when it has the additional capacity to act as a root forwarding agent having a wired connection.

Mesh points intending to join the mesh, first need to perform member discovery. Path selection is an important criterion if a mesh is to be viable. The following important questions must be kept in mind while designing a solution.




- How will MPs discover a candidate neighbor? In networking, "frames" are used to encapsulate data with the address of the receiver and other control information. Information Elements (IE), in 802.11 frames are used to communicate with other devices. New IEs have been introduced in Beacon frame, a frame which devices use to advertise their services, and in probe response frame, a frame devices use to answer queries from other devices. These are WLAN mesh capability element and an ESS Mesh name.
- How will mesh services be supported? Action Frames are a special class of frames that are used to initiate certain actions even after initial communication between devices. To support mesh services, new IEs are exchanged between MPs in Action frames.
- How will membership be determined? Secure peer-to-peer links has to be established. MPs authenticate each other before creating a link between them.
- How will different mesh running different protocols interoperate? There has to be one mandatory protocol running on a single mesh. MPs will have this information in the WLAN Mesh Capability IE. A mesh that is running a protocol other than the mandatory protocol is not required to change its protocol when a new MP joins.

## MESH SECURITY

Wireless communication is inherently unreliable as it travels through the air. In the current architecture, the communication between an AP and the Station has been made secure by extensive use of crypto graphically secure algorithms and extensible security protocols. Since a security chain is only as strong as its weakest link, the same kind of security paradigm is called for when MPs communicate with each other instead of stations. The approach adopted by a mesh network is the reuse of existing, widely deployed 80.11i infrastructure, a security specification for 802.11 wireless networks. Following are major points pertaining to mesh security:

- Mps don't have wired connections with each other as in traditional WLAN networks. A mesh network places no topology constraint on an MP so there is no node hierarchy. In this context, MPs need to maintain secure links with several other MPs.
- Mesh should not allow unauthorized devices from directly forwarding their data using mesh services. This should enable a mechanism for parties to exchange a Pairwise Master Key (PMK), a cryptographic key. This PMK will be treated as an authorization token in a mesh.
- For authentication, both parties should agree on the role that they are going to perform. An initial negotiation lets them understand if they are acting as supplicant -providing credentials or as an authenticator -verifying credentials.

## ROUTING

802.11s is basically meant to extend the concept of the traditional, less used, ad-hoc network. One important difference is that data packets may now travel to their ultimate destination through intermediate MPs. 802.11s gives a distribution system to ad-hoc networks. This brings an important question to the fore, how is an optimum and minimal path selected for packets to travel to their destination. This question brings the concept of Layer 3 routing to the domain of Layer 2. Ultimately both have to address same question, hop-by-hop traveling of packets.

Here are the requirements placed on routing in a mesh networks:

- Routing should be able to optimize unicast frame delivery between MPs and Stations and Between MPs to Mps.
- Devices that are part of a mesh should be able to calculate the best path to reach a particular device. In typical mesh networks, with added mobility, link state may keep changing. Devices should be able to factor this in their calculation and should converge quickly when link state changes.
- Additionally routing can also support broadcast and multicast frame delivery.

In 802.11s there is one mandatory protocol that has to be implemented. The standard also defines an optional protocol.

The important routing protocols are:

- Hybrid Wireless Mesh Protocol (HWMP): This is the default protocol for interoperability. This is a combination of two different protocols.
- Radio Metric - Ad-hoc on demand distance vector (RM-AODV): RMAODV uses the basic mandatory features of RFC 3561. Its appeal lies in the fact that destination in the mesh can be discovered when demand arises. It does not require devices to maintain routes to nodes that are no longer active. This way, mobile nodes obtain new routes quickly. This addresses the problem of Route maintenance and loop avoidance clearly.

- Proactive tree based routing: This exploits a logical tree like structure in a mesh deployment to provide routing functions. Its main function is topology creation and topology maintenance. If a route portal is present in the mesh, its first function is to create a distance vector routing tree and then maintain it. This is most efficient for hierarchical networks or a network that can be represented in a hierarchical form. It avoids unnecessary route discover flooding. All in all, this protocol effectively merges the flexibility offered by RM-AODV and the efficiency offered by tree-based routing. This combination makes it suitable for deployment in a large number of use cases. Apart from the mandatory metric of Air time, it also allows any other path selection metric.
- Radio Aware Optimized link state routing protocol (RA-OLSR): This is an optional path selection protocol in mesh networks based on RFC -3626. The primary appeal of this scheme is that it proactively maintains link state and any change in the link state is communicated to the neighboring MPs. It uses Radio aware metric in path selection.

## MAC EXTENSION

Mesh requirements like Mobility awareness and dynamic radio environment puts a tremendous strain on basic 802.11 Medium Access Control (MAC), a low level fundamental data communication protocol. To solve the various problems pertaining to mesh, support has to be provided at the MAC level. Following are the functions that a 802.11s MAC is supposed to perform.

- Enhanced Distributed Channel Access ( EDCA) : Background EDCA mechanism is a QOS enhancement function introduced by 802.11e. It facilitates service differentiation in 802.11 networks by using four different channel Access functions executing four different back off counters. These four different back off counters, to large extent, ensure that the medium is shared based on the priority of the content thereby ensuring Quality of Service.
- Mesh Deterministic Access ( MDA) : The MAC enhancement MDA is a deterministic mechanism based on reservation. It facilitates Quality of Service (QoS) support in large scale mesh networks. It employs distributed scheduling to reduce the contention period for channel access. By operating in a synchronized manner it reduces collision.
- Power Management : The traditional approach of power saving relies on beacon frames and on PS-Poll frames, a special class of frame to fetch data for sleeping station, to achieve power saving objectives. Though advanced PS options are being standardized, mesh reuses the same mechanism defined in BSS networks with some enhancements. Some new rules have been introduced and APSD (Automatic Power Save Delivery) is used.
- Congestion Control : A typical characteristic of a mesh is heterogeneous link capacities along the forwarding path as no restriction has been imposed on the link capacity.

  Traffic from many nodes may travel through same path, resulting in traffic aggregation. This introduces the problem of flow control in the network. As hop count increases, and if there is no congestion control mechanism, MPs that are located at the outer edge of the mesh will experience performance degradation and lower throughput. Congestion monitoring is the principle employed to handle this situation. MPs continuously monitor links and if they find a congestion they inform their neighbors. This way information about congestion is spread throughout the mesh. Nodes will control the data generation rate, if this data has to travel through a congested path.

## TECHNICAL CHALLENGES FOR WIRELESS MESH NETWORKS

The key challenges in mesh networks arise from the fact that the concept of L3 routing has been introduced and Access points will start playing the additional role of a station in the link security context. Heterogeneous link capacities in a mesh pose the problem of congestion control. In addition, a mesh network has to provide a host of services to ensure the smooth operation of a mesh.

Apart from these, major challenges pertaining to the design of a mesh can be summarized as:

- Bandwidth : Traditional wireless communication is half-duplex. That means that the device can either transmit or receive at a given time. This is an inherent property of radio communication because transmission goes through air. If it is sending and receiving at the same time, data will collide in air as the entire transmission happens over single channel, the frequency of the communication. In a Wireless Mesh network this poses great challenges. If node A is forwarding data to node B on a channel, node B cannot transmit to node C on same channel because the medium will be sensed as busy by both nodes C and B. Also node C cannot communicate to node D on same channel. This can potentially reduce the available bandwidth to half at every forwarding node. If a path consists of just 5 forwarding nodes, the bandwidth will become 1/32 of actual bandwidth.

  Some mechanisms can be employed to address this issue. One solution is to let multiple channels work in a mesh where all devices have a single radio. This adds overhead on MAC, how to select appropriate channel between node-pair to maximize bandwidth. In the example cited above, node A and Node B can communicate on channel no. 6 while at the same time node C and node D can communicate on channel no. 11. This requires that the all devices in a mesh agree with their neighbors on what channel they will be operating on. One other solution where multiple radios can be present in a single device will increase the cost of mesh devices. Also multi-radio device may not conform to the 802.11 framework and may not be interoperable with other implementations. Overall a mesh will experience some bandwidth degradation at every hop and the challenge lies in keeping this number to a minimum by efficient utilization of radio resources.

- Mobility and Roaming : By definition, mesh devices can be mobile. If a mesh device situated in a data forwarding path, tries to move beyond the range of its neighbors, the link carrying the data through that path will be broken. This requires some kind of roaming support for MPs. If an MP moves beyond the range of a wireless forwarding path, other MPs should be able to sustain data flow. This requires a mesh device to inform its neighbors about its movement so they can start talking to each other or to some other device, which they can bring in the forwarding path to fill the gap caused by the moving device. The moving device may have some frames stored, that it was unable to forward. In this case, a mechanism is needed to forward these frames to its destination via a new forwarding path where the device has now moved to or through some default forwarding path.

- Quality of Service (QoS): In tradition wireless LAN, QoS comes into the picture between a station and an AP. So an AP has to reserve certain resources to guarantee QoS. When a station wants a certain quality such as voice, it informs the AP ahead of the actual data. If the AP can honor the request, it makes a reservation. In mesh, every forwarding node will halve the bandwidth because of half duplex communication. So QoS has to be maintained, not only between stations and an MAP but between MP and MP as well. This will require MPs to communicate with each other about the quality needs of the content before it arrives. If not properly designed, MPs can act as delay point that will destroy the concept of QoS.

- Fairness and uniform coverage : Devices that are lying at the outer edge of a mesh or that are located far away from a Mesh Portal can potentially be in a disadvantageous position. As every single hop reduces the bandwidth, outer devices will take longer to reach the network and will experience performance degradation as there is no differentiation between traffic fromdifferent nodes. To ensure uniform coverage in the mesh, some kind of fairness method is required. One possible approach is to compute the share of each device in the mesh capacity and then enforce it. If not properly designed, such outer devices may starve for network resources.
- Network Management : Network management also poses a challenge because of the mobile nature of mesh devices. Device failure can potentially go undetected because of the self-healing and self-organizing nature of the network. Mesh health has to be continuously monitored for efficient management. Another problem is to find rogue or intruder devices that can initiate Denial-of-Service (DOS) attacks making the mesh dysfunctional. These devices have to be identified in time and relevant measures have to be taken to prevent such attacks.

To address these challenges, the product team requires significant cross domain expertise, apart from superior engineering skills in architecting, developing and testing the products. Expertise in the following domains is essential:

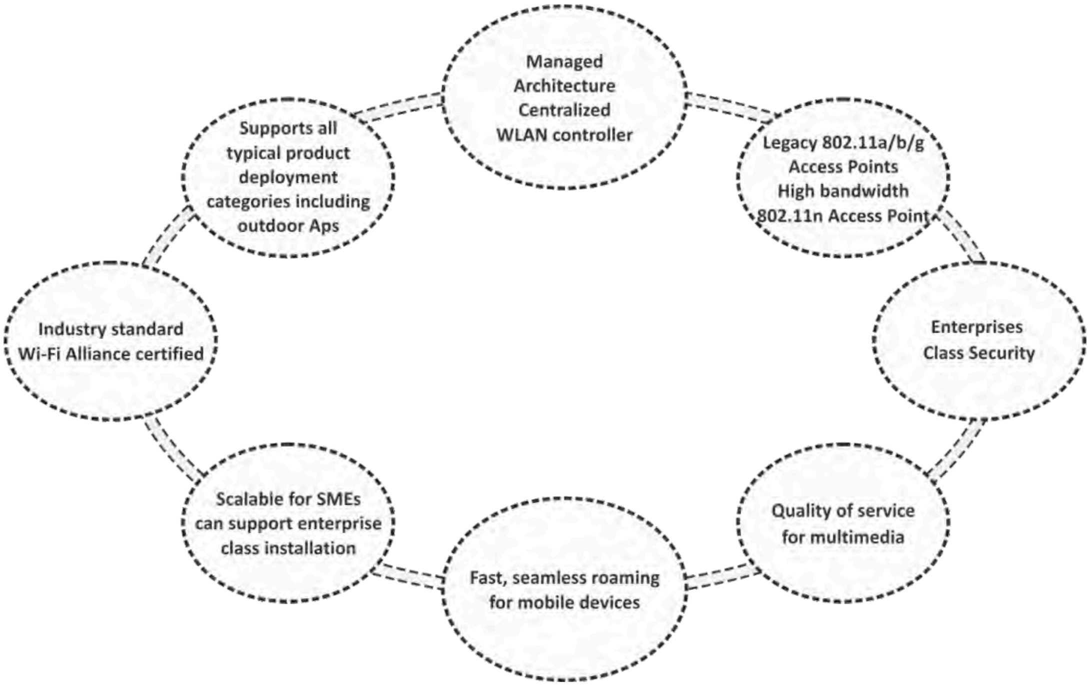
- Wireless LAN ( Wi-Fi) : In-depth knowledge of 802.11 standards, general and complete picture of networking stack and their integration process. In-depth understanding of various 802.11 standard like 802.11 a,802.11b, 802.11g, 802.11n, 802.11h, MAC implementation and issues for these protocols.
- Security : Knowledge and working of various security protocols, frameworks and algorithms like WEP, WPA, 802.1x, WPA2-PSK and WPA-2 with External server.
- Routing and forwarding : In depth knowledge of networking and various layers, Layer 3 routing and implementations, Knowledge of networking devices like router, repeater, bridge, 802.1D etc,
- Innovative Solutions to Complex Engineering Problems : Expertise in proposing and implementing various components of the architecture that are not part of the standard but significantly enhance the working of the solution, like Access point load balancing, Preferred Channel selection algorithms and auto transmit power control. Expertise in off standard security paradigms like Rogue AP concept and ESS isolation. MAC and proposed enhancements.

Overall, a technology like Wireless Mesh demands significant resources and poses significant challenges on the part of development to deliver a cost effective, scalable, secure and reliable product that can cater to the needs of the market.

## ALTEN CALSOFT LABS ' EXPERTISE

### *Technology Expertise*

ALTEN Calsoft Labs’ has extensive experience with in designing and implementing Wireless LAN solutions. It has a working, field deployed, SMB class product and it can also address other service requirements in any area of Wireless technology. ALTEN Calsoft Labs’ expertise in various protocols such 802.11a/b/g/n, 802.11e, 802.1d, APSD, WPA, WPA-2 etc. together with the proven hardware design capabilities of its subsidiary, Aspire Communications, offers a unique capability to execute and deliver state-of-the-art Wireless projects. The expertise includes hardware and software design, implementation, interoperability testing, performance testing, product certification testing etc.




## PRODUCT ENGINEERING SERVICES

Together with the relevant expertise, ALTEN Calsoft Labs' offers various engagement models that allow customers to leverage ALTEN Calsoft Labs' capabilities to stay competitive and cost effective in a very dynamic marketplace.

The models include

- Short term consultation by subject matter experts in time and material mode.
- Complete NRE price based product or subsystem development.
- Long term strategic Offshore Development Center, providing great value for investment over time.

ALTEN Calsoft Labs' WLAN lab and other networking lab infrastructure are fully equipped with various product development and test equipment. In the past, customers have entrusted the ALTEN Calsoft Labs' team with complete analysis, design, implementation and testing of WLAN solutions, while many have leveraged ALTEN Calsoft Labs' expertise to fill gaps by entrusting them to enhance their product or perform various product testing.

Example Product & Case Studies:

- A centralized WLAN controller
- 802.11 a/b/g and 802.11 n Access Points

### ABOUT ALTEN CALSOFT LABS

ALTEN Calsoft Labs is a next gen digital transformation, enterprise IT and product engineering services provider. The company enables clients innovate, integrate, and transform their business by leveraging disruptive technologies like mobility, big data, analytics, cloud, IoT and software-defined networking (SDN/NFV). ALTEN Calsoft Labs provides concept to market offerings for industry verticals like education, healthcare, networking & telecom, hi- tech, ISV and retail. Headquartered in Bangalore, India, the company has offices in US, Europe and Singapore. ALTEN Calsoft Labs is a part of ALTEN group, a leader in technology consulting and engineering services.

www.altencalsoftlabs.com

business@altencalsoftlabs.com