國立交通大學

電信工程研究所

碩士論文

基於 IEEE 802.11s
標準之無線網狀網路之研究

A Study on Wireless Mesh Networks
based on the IEEE 802.11s Standard

研究生：哈 馬迪

指導教授：黃家齊 教授

中華民國九十九年九月

A Study on Wireless Mesh Networks based on the IEEE 802.11s Standard

研究 生：哈 馬迪　　　　Student: Laith Alsmadi

指導教授：黃家齊 教授　　　　Advisor: Prof. Chia-Chi Huang

國立交通大學

電信工程研究所

碩士論文

A Thesis

Submitted to Institute of Communication Engineering
College of Electrical and Computer Engineering
National Chiao Tung University
in Partial Fulfillment of the Requirements
for the Degree of

Master

in Communication Engineering

Sep 2010

Hsinchu, Taiwan, Republic of China

中　華　民　國　九十九　年　九　月

基於 IEEE 802.11s
標準之無線網狀網路之研究

研究 生：哈 馬迪　　　　　　　　指導教授：黃家齊 教授

國立交通大學

電信工程研究所

中文摘要

關於無線網狀網路在無線區域網路(WLAN)上的研究在最近幾年內已經被廣泛的探討。在近年內，為了改進無線區域網路上的無線網狀網路的效能，專家們制定了許多新的通訊協定。然而，這些解決的方案通常被各自的專利所保護，以至於在區域網路之間的連結上造成了困難。因此，一個共同的標準就變成一個必要的目標。為了滿足這個需求，一個IEEE的工作小組—802.11s正在為無線網狀網路制定一個共同的標準。儘管這個小組已經公佈了許多文件，但是仍然有許多的問題是懸而未決的。本篇論文的主要貢獻是：(1)了解在現存的802.11s架構及功能。(2)了解在802.11s標準中可以增加什麼功能來改善效能。(3)本論文對802.11s無線網狀網路做了一個細節性的介紹。

A Study on Wireless Mesh Networks based on the IEEE 802.11s Standard

Student: Laith Alsmadi Advisor: Prof. Chia-Chi Huang

Institute of Communication Engineering
National Chiao Tung University

Abstract

Wireless mesh networking based on 802.11 Wireless Local Area Network (WLAN) has been explored for a few years. To improve the performance of WLAN mesh networks, a few new communication protocols have been developed in recent years. However, these solutions are usually proprietary and prevent WLAN mesh networks from interworking with each other. Thus, a standard becomes indispensable for WLAN mesh networks. To meet this need, an IEEE 802.11 task group, i.e., 802.11s, is specifying a standard for WLAN mesh networks. Although several standard drafts have been released by 802.11s, many issues still remain to be resolved. In order to understand what functions can be expected from the existing framework of 802.11s standard and what additional functionalities shall be added to 802.11s standard to improve its performance, a detailed study on wireless mesh networks based on the existing 802.11s standard is given in this work.

Acknowledgments

To my parents who gave me love and support. Who encouraged me in every right step I took, I mention a step that leads me to make this project which is choosing to study communication engineering in this university.

I would like to express my gratitude and respect to my supervisor Prof. Chia-Chi Huang who advised and helped me through this project.

A deep appreciation to all friends and people especially Tamara who stood by me and support me all the time and who supplied me with the knowledge that helped me complete my thesis.

Contents

List of Tables

List of Figures

Chapter One

Wireless Mesh Networks

1.1 Introduction

As different wireless networks evolve into the next generation to provide better services, a key technology, wireless mesh networks (WMNs) has emerged recently.

In WMNs, nodes are comprised of mesh routers and mesh clients. Each node operates not only as a host but also as a router.

A WMN is dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves.

Conventional nodes, e.g., desktops, laptops, PDAs, PocketPCs, phones, equipped with wireless network interface cards (NICs) can be connected directly to wireless mesh routers.

Customers without wireless NICs can access WMNs by connecting to wireless mesh routers using Ethernet. Thus, WMNs will greatly help users to be always on- line anywhere anytime.

Moreover, the gateway functionalities in mesh routers enable the integration of WMNs with various existing wireless networks such as cellular systems, wireless sensor networks, wireless-fidelity (Wi-Fi) systems, worldwide inter-operability for microwave access (WiMAX), and WiMedia networks.

Wireless Mesh Networking is a promising wireless technology for numerous applications, e.g., broadband home networking, community and neighborhood networks, enterprise networking, building automation, etc. It is gaining significant attention as a possible way for cash-strapped Internet service providers (ISPs), carriers, and others to roll out robust and reliable wireless broadband service access in a way that needs minimal up-front investments.

Deploying a WMN is not too difficult, because all the required components are already available in the form of ad hoc routing protocols, IEEE 802.11 MAC protocol, wired equivalent privacy (WEP) security, etc. Several companies have already realized the potential of this technology and offer wireless mesh networking products. A few testbeds have been established in university research labs.

However, to make a WMN be all it can be, considerable research efforts are still needed. For example, the available MAC and routing protocols applied to WMNs do not have enough scalability; e.g., throughput drops significantly as the number of nodes or hops increases. Existing security schemes may be effective for certain types of attack, but they lack a comprehensive mechanism to prevent attacks from different protocol layers. Similar problems exist in other networking protocols. Thus, existing communication protocols, ranging from application layer to transport, routing, MAC, and physical layers, need to be revisited and enhanced. In some circumstances, new protocols need to be invented.

Researchers have started to revisit the protocol design of existing wireless networks, especially of IEEE 802.11 networks, ad hoc networks, and wireless sensor networks, from the perspective of WMNs. Industrial standards groups are also actively working on new specifications for mesh networking. For example, IEEE 802.11, IEEE 802.15, and IEEE 802.16 based wireless local area network (WLAN), wireless personal area network (WPAN), and wireless metropolitan area network (WMAN) technologies have established subworking-groups to focus on new standards for WMNs [1, 3, 9].

1.2 Network Architecture

WMNs include two types of nodes as shown in Figure 1.1 [1, 3, 5]:

- Mesh routers
- Mesh clients

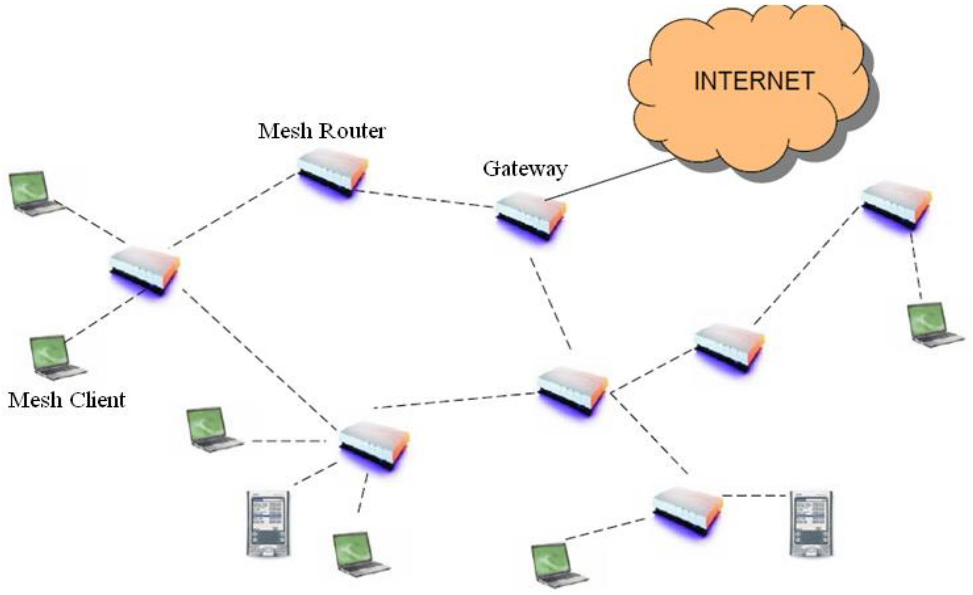


Figure 1.1 System Model of WMN

Mesh router can act as gateway that give it more functionalities to enable the integration of WMNs with other wireless networks such as cellular, wireless sensor, wireless-fidelity (Wi-Fi), worldwide inter-operability for microwave access (WiMAX) networks.

Comparing with conventional wireless router, a wireless mesh router contains additional routing functions to support mesh networking to improve the flexibility of mesh networking. And it can achieve the same coverage with much lower transmission power through multihop communications.

With these differences, mesh and conventional wireless routers built based on a similar hardware platform. As shown in Figure 1.2 some examples of mesh routers [1, 2].

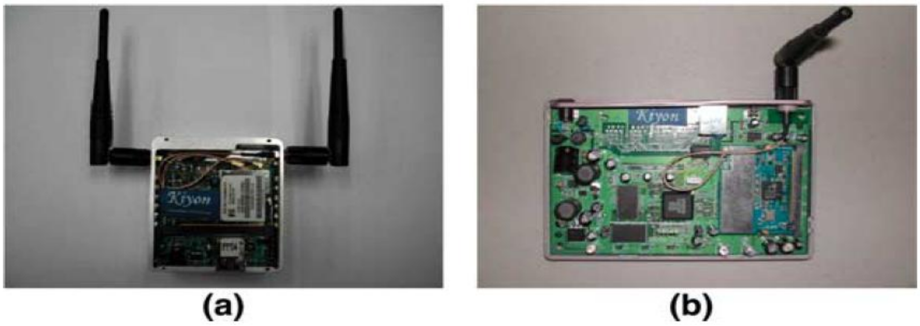


Figure 1.2 Examples of mesh routers based on different embedded systems: (a) PowerPC (b) Advanced Risc Machines (ARM)

Mesh clients have functions for mesh networking, and it can works as a router in WMN. But, gateway functions do not exist in these nodes. Although, the hardware platform and the software can be much simpler than those for mesh routers. Mesh clients have a larger diversity of devices compared to mesh routers. as shown in Figure 1.3 it can be a laptop/desktop PC, pocket PC, PDA, IP phone, RFID reader, and many other devices.

Figure 1.3 Examples of mesh clients: (a) Laptop, (b) PDA, (c) Wi-Fi IP Phone (d) Wi-Fi RFID Reader.

The architecture of WMNs classify into three groups based on the functionality of the nodes [1, 6, 23]:

- **Infrastructure/Backbone WMNs:**

  As shown in Figure 1.4, where dashed and solid lines represent wireless and wired links.

  Mesh routers figure an infrastructure for clients that connect to them and it form a mesh with a self-configuring, self healing links among themselves, with gateway functionality.

  According to infrastructure meshing that provides backbone for conventional clients and enables the combination of WMNs with existing wireless networks, via gateway functionalities in mesh routers.

  Ethernet interface connect the conventional clients to mesh routers through Ethernet links.

  The WMN can be build infrastructure/backbone by using different types of radio technology, so for conventional clients that use same radio technologies as mesh routers, they can directly communicate with mesh routers. But for different radio technologies, clients have to communicate with the base stations that have Ethernet connections to mesh routers.

  Infrastructure/Backbone WMNs are the most commonly used type. For example, community and neighborhood networks can be built using infrastructure meshing.

  The mesh routers are placed on the roofs of houses in a neighborhood, and these can serve as access points for users in homes and along the roads. Typically, two types of radio are used in the routers, i.e., for backbone communication and for user communication. The mesh backbone communication can be established using long range communication techniques including, for example, directional antennas.

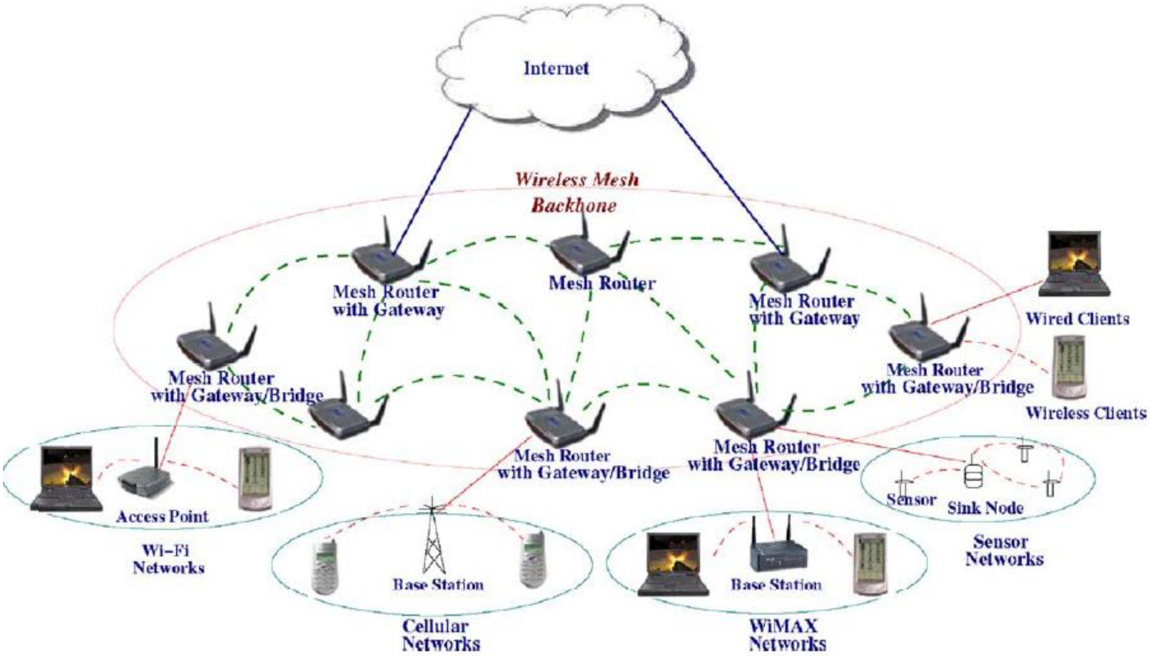


Figure 1.4 Infrastructure/backbone WMNs

- **Client WMNs:**

  Client nodes compose the actual network to execute routing and configuration functionalities with providing end-user applications to customers.

  As shown in Figure 1.5. A packet sends to a node in the network through multiple nodes to reach the destination.

  Furthermore, comparing with infrastructure meshing the requirements on end-user devices is increased, because in Client WMNs, the end users have to provide additional functions such as routing and self-configuration.

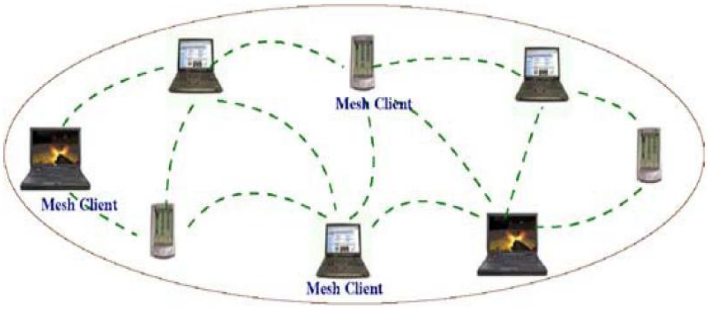


Figure 1.5 Client WMNs

- **Hybrid WMNs:**

  The architecture is mixture of infrastructure and client meshing as shown in Figure 1.6.

  The infrastructure gives connectivity to other networks such as the Internet, WiMAX, Wi-Fi, cellular, and sensor networks. While mesh clients can access the network through mesh routers.

  In the other hand, the routing capabilities of clients offer better connectivity and coverage inside the WMN.

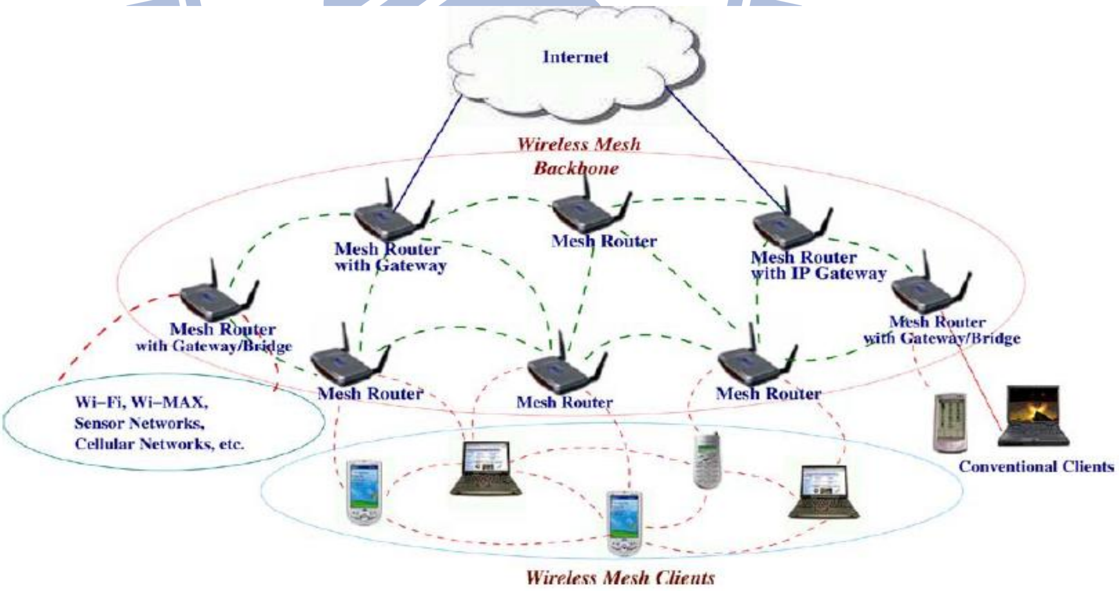

Internet
Wireless Mesh Backbone
Mesh Router with Gateway
Mesh Router
Mesh Router with IP Gateway
Mesh Router with Gateway/Bridge
Mesh Router with Gateway/Bridge
Mesh Router
Mesh Router
Mesh Router
Wi-Fi, Wi-MAX, Sensor Networks, Cellular Networks, etc.
Conventional Clients
Wireless Mesh Clients

Figure 1.6 Hybrid WMNs

1.3 Characteristics

Here is some characteristics of WMNs [1]:

- **Increased Reliability:**

  The wireless mesh routers provide redundant paths between the sender and the receiver of the wireless connection. That increase the communication reliability by eliminates single point failures and potential bottleneck links. The existence of multiple possible alternative routes can be ensured the network robustness against potential problems, e.g., node failures, and path failures due to radio frequency (RF) interferences or obstacles. So, the network can operate reliably over an extended period of time by utilizing WMN technology.

- **Low Installation Costs:**

  The main attempt to provide wireless connection to the end-users is through the deployment of 802.11 based Wi-Fi Access Points (APs). To assure almost full coverage in a metro scale area, it is required to deploy a large number of APs because of the limited transmission range of the APs. The drawback of this solution is highly expensive infrastructure costs, since an expensive cabled connection to the wired Internet backbone is necessary for each AP. On the other hand, constructing a wireless mesh network decreases the infrastructure costs, since the mesh network requires only a few points of connection to the wired network. Hence, WMNs can enable fast implementation and possible modifications of the network at a reasonable cost, which is extremely important in today's competitive market place.

- **Large Coverage Area:**

  At this time, the data rates of wireless local area networks (WLANs) have been increased, e.g., 54 Mbps for 802.11a and 802.11g, by utilizing spectrally efficient modulation schemes. Although the coverage and connectivity of WLANs decreases as the end-user becomes further from the access point. On the other hand, multi-hop and multi-channel communications among mesh routers and long transmission range of WiMAX towers deployed in WMNs can enable long distance communication without any significant performance degradation.

- **Automatic Network Connectivity:**

  Wireless mesh networks are dynamically self-organized and self-configured. In other words, the mesh clients and routers automatically establish and maintain network connectivity, which enables seamless multi-hop interconnection service. For example, when new nodes are added into the network, these nodes utilize their meshing functionalities to automatically discover all possible routers and determine the optimal paths to the wired Internet. Furthermore, the existing mesh routers reorganize the network considering the newly available routes and hence, the network can be easily expanded.

1.4 Advantages and Disadvantages of Use

Advantages of Use

Table 1.1 shows common advantages and disadvantages associated with the use of a wireless mesh network [2].

Table 1.1 Advantages and Disadvantages Associated with the Use of Mesh Networks

Advantages	*Disadvantages*
Reliability	Lack of standards
Self-configuration	Security
Self-healing	Overhead
Scalability	
Economics	

- **Reliability**

  In a WMN each node functions as a relay to move packets toward their destination. Because nodes can enter and leave the mesh, each node must be capable of dynamically changing its forwarding pattern based upon its neighborhood. Thus, the mesh topology improves reliability because the failure of one link due to RF interference, the movement of a node between source and destination, will result in packets being forwarded using an alternative link toward their destination.

- **Self-Configuration**

  Since nodes in a mesh network learn their neighbors and paths to other nodes, there is no need to configure each node. Thus, the self-configuration capability of nodes can significantly reduce the need for network administration.

- **Self-Healing**

  Since nodes in a WMN dynamically learn their neighbors as well as links to other nodes, there is automatic recompense for the failure or removal of a node. So, other nodes establish alternate paths when the event of transmission destruction that adversely affects the use of a link or the failure of a node. The establishment of alternative paths results in a self-healing capability.

- **Scalability**

  As mentioned above, nodes can enter and exit a mesh network. This means that you can extend the area of coverage of a WMN by simply placing new nodes at proper locations where they can communicate with existing network nodes. Thus, a WMN is scalable. Still, the number of nodes you may require and the upper limit concerning the total number of nodes you can have in a network will vary based upon your organization's physical and technical operating environment. Concerning the physical environment, the number of obstacles and the level of RF interference will govern the number of nodes required within a given area.

- **Economics**

  According with no requirement for centralized administration or manual configuration for the nodes that means these networks are less expensive to set up and operate than conventional networks. Also, the ability of WMNs to automatically resolve link and node outage problems via their self-healing capability eliminates the necessity for manual intervention when things go wrong.

Disadvantages of Use

- **Lack of Standards**

  There is several organizations in the process of developing wireless mesh networking standards. The key factor to note is the lack of interoperability between different vendors because there are no existing standards with which vendors can tailor their products to comply.

- **Security**

  Because nodes within a wireless mesh network function as routers relaying packets to other nodes, security is an important issue. Because the numbers of nodes in a WMN increases, there will be more locations where dangerous persons can view your data. This means that a method of authentication of nodes is required in addition to securing the flow of data through nodes.

- **Overhead**

  As nodes must learn their neighbors as well as paths to other nodes, they must create and maintain routing tables. Because network traffic and number of nodes in the network increases, the amount of processing devoted to routing packets is increasing also. Thus, the efficiency of routing software and the number of network nodes and level of network traffic results in processor overhead that can adversely affect the performance of the node to perform other tasks.

1.5 Comparison between Ad Hoc and WMN

Ad hoc networks can actually be considered as a subset of WMNs. To illustrate this point, the differences between WMNs and ad hoc networks are outlined below [3, 4]:

- **Wireless infrastructure/backbone:**

  As discussed before, WMNs consist of a wireless backbone with mesh routers. The wireless backbone provides wide coverage, connectivity, and robustness in the wireless domain. However, the connectivity of ad hoc networks depends on the individual contributions of end users which may not be reliable.

- **Integration:**

  WMNs support conventional clients that use the same radio technologies as a mesh router. This is accomplished through a host-routing function available in mesh routers. WMNs also enable integration of various existing networks such as Wi- Fi, the Internet, cellular and sensor networks through gateway/bridge functionalities in the mesh routers. Consequently, users in one network are provided with services in other networks, through the use of the wireless infrastructure. The integrated wireless networks through WMNs resemble the Internet backbone, since the physical location of network nodes becomes less important than the capacity and network topology.

- **Dedicated routing and configuration:**

  In ad hoc networks, end-user devices also perform routing and configuration functionalities for all other nodes in the networks. However, WMNs contain mesh routers for these functionalities. Hence, the load on end-user devices is significantly decreased, which provides a lower energy consumption and high-end application capabilities to possibly mobile and energy-constrained end-users. Moreover, the end-user requirements are limited which decreases the cost of devices that can be used in WMNs.

- **Multiple radios:**

  As discussed before, mesh routers can be equipped with multiple radios to perform routing and access functionalities. This enables separation of two main types of traffic in the wireless domain. While routing and configuration traffic is performed between mesh routers, access to the network from end users can be carried on a different radio. This significantly improves the capacity of the network. On the other hand, these functionalities are performed in the same channel in ad hoc networks constraining the performance.

- **Mobility:**

  Since ad hoc networks provide routing using the end-user devices, the network topology and connectivity depend on the movement of users.

  Since mesh routers provide the infrastructure in WMNs, the coverage of the WMN can be engineered easily. While providing continuous connectivity throughout the network, the mobility of end users is still supported, without compromising the performance of the network.

- **Compatibility:**

  WMNs contain many differences when compared to ad hoc networks.

  However, as discussed above, ad hoc networks can be considered as a subset of WMNs.

  More specifically, the existing techniques developed for ad hoc networks are already applicable to WMNs. As an example, through the use of mesh routers and routing capable end users, multiple ad hoc networks can be supported in WMNs, but with further integration of these networks.

1.6 Free-For-Use and Commercial WMN Examples

Early stage of research works of WMNs have been performed on actual test beds or free-to-use networks. The first free-to-use WMN is Roofnet, which is an 802.11b/g community-oriented WMN developed by the Massachusetts Institute of Technology (MIT) to provide broadband Internet access to the users in Cambridge, MA.

Some other free-to-use WMNs have Champaign-Urbana CommunityWireless Network (CUWiN), SeattleWireless, Broadband andWireless Network (BWN), and Southampton Open Wireless Network (SOWN), Technology For All (TFA). These WMNs are typically implemented with open source software and free of addition of new nodes.

These test beds fostered tremendous advances and consequently built up the confidence for commercial applications in the design of architectures, protocols, algorithms, services, and applications of WMNs. Some of the commercial WMN solutions include Motorola, Tropos, BelAir, Cisco, Nortel, Microsoft, Firetide, Sensoria Corporation, PacketHop, MeshDynamics, and Radiant Networks.We illustrate them by using the example of Cisco.

Cisco has commercial WMN solution by using its Aironet products to allow government, public safety, and transportation organization to build cost-effective outdoor WMNs for private or public use. The Aironet MR products are designed to provide secure, high-bandwidth, and scalable networks to enable access to fixed and mobile applications across metropolitan areas. The products use an 802.11 radio to provide network connectivity to the end users and a separate radio that is used for communication with the other MRs on the backbone. For instance, Aironet 1500 works as a MR that uses 802.11g/b for connecting the end users while using 802.11a radio to connect with neighboring MRs. The Aironet 1500 series support 16 broadcast identifiers to create multiple Wireless LANs so that the accessing network can be segmented to provide services to multiple user types. The IGW node is able to connect 32 other Cisco MRs (i.e., Aironet 1500).

A routing algorithm based on Adaptive Wireless Path Protocol (AWPP) allows remote MRs to dynamically select the multihop path toward the destination or the IGW. If new MRs are added to the network, each MR self-adjusts to ensure networking capability. The Cisco Aironet 1500 Series interacts with Cisco wireless LAN controllers and Cisco Wireless Control System (WCS) Software, having centralized key functions, scalable management, security, and mobility support. The security solution is compliant with 802.11i, Wi-Fi Protected Access (WPA2), and Wired Equivalent Privacy (WEP), which provide authentication for various WAP types and ensure data privacy with necessary encryption. The MR joins the network using X.509 digital certification and the wireless backbone uses the hardware-based Advanced Encryption Standard (AES) encryption. The Cisco solution based on the dual-radio approach raises the question of scalability and capacity in the infrastructure mesh, where all the MRs use 802.11a and the clients use 802.11b/g.

1.7 Application Scenarios

Research and development of WMNs is motivated by several applications which clearly demonstrate the promising market, but, at the same time, these applications cannot be supported directly by other wireless networks such as cellular systems, ad hoc networks, wireless sensor networks, standard IEEE 802.11, etc.

In this section, we discuss these applications [1, 9]:

- **Broadband home networking:**

  Currently broadband home networking is realized through IEEE 802.11WLANs. An obvious problem is the location of the access points.

Without a site survey, a home (even a small one) usually has many dead zones without service coverage. Solutions based on site survey are expensive and not practical for home networking, while installation of multiple access points is also expensive and not convenient because of Ethernet wiring from access points to backhaul network access modem or hub. Moreover, communications between end nodes under two different access points have to go all the way back to the access hub. This is obviously not an efficient solution, especially for broadband networking. Mesh networking, as shown in Figure 1.7, can resolve all these issues in home networking. The access points must be replaced by wireless mesh routers with mesh connectivity established among them.

Therefore, the communication between these nodes becomes much more flexible and more robust to network faults and link failures. Dead zones can be eliminated by adding mesh routers, changing locations of mesh routers, or automatically adjusting power levels of mesh routers. Communication within home networks can be realized through mesh networking without going back to the access hub all the time. Thus, network congestion due to backhaul access can be avoided. In this application, wireless mesh routers have no constraints on power consumptions and mobility. Thus, protocols proposed for mobile ad hoc networks and wireless sensor networks are too cumbersome to achieve satisfactory performance in this application. On the other hand, Wi-Fis are not capable of supporting ad hoc multihop networking. As a consequence, WMNs are well suited for broadband home networking.

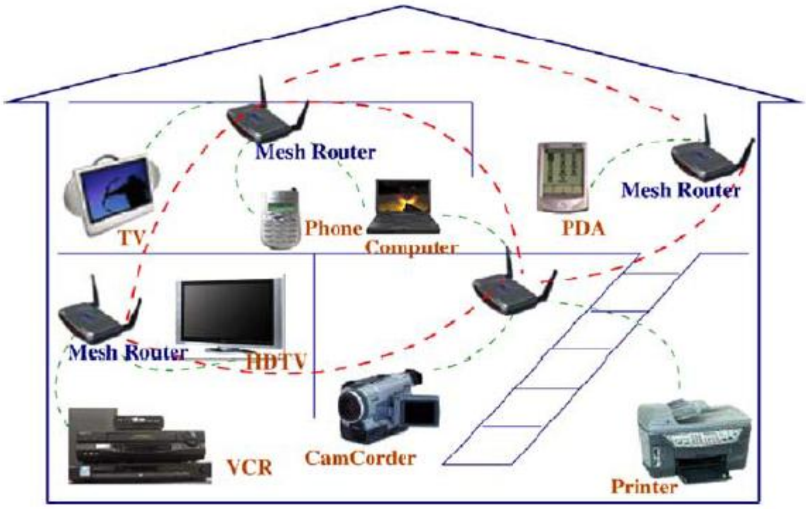


Figure 1.7 WMNs for broadband home networking

- **Community and neighborhood networking:**

  In a community, the common architecture for network access is based on cable or digital subscriber line (DSL) connected to the Internet, and the last hop is wireless by connecting a wireless router to a cable or DSL modem. This type of network access has several drawbacks.

  – Even if the information must be shared within a community or neighborhood, all traffic must flow through the Internet. This significantly reduces network resource utilization.

  – A large percentage of areas in between houses is not covered by wireless services.

  – An expensive but high-bandwidth gateway between multiple homes or neighborhoods may not be shared, and wireless services must be set up individually. As a result, network service costs may increase.

  – Only a single path may be available for one home to access the Internet or communicate with neighbors.

WMNs mitigate the above disadvantages through flexible mesh connectivities between homes, as shown in Figure 1.8. WMNs can also enable many applications such as distributed file storage, distributed file access, and video streaming.

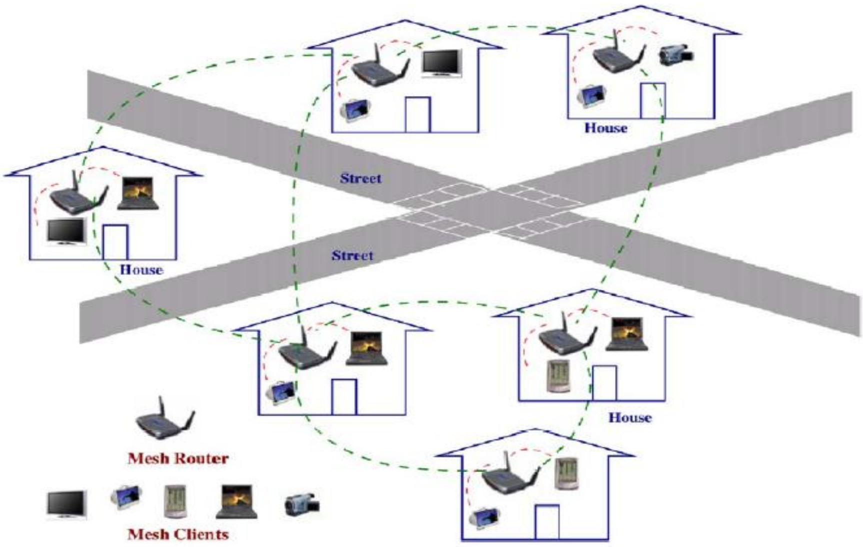


Figure 1.8 WMNs for community networking

- **Enterprise networking:**

  This can be a small network within an office or a medium-size network for all offices in an entire building, or a large-scale network among offices in multiple buildings. Currently standard IEEE 802.11 wireless networks are widely used in various offices. However, these wireless networks are still isolated islands.

  Connections among them have to be achieved through wired Ethernet connections, which is the key reason for the high cost of enterprise networks. In addition, adding more backhaul access modems only increases capacity locally, but it does not improve robustness to link failures, network congestion, and other problems of the entire enterprise network. If the access points are replaced by mesh routers, as shown in

Figure 1.9, Ethernet wires can be eliminated. Multiple backhaul access modems can be shared by all nodes in the entire network, and thus improve the robustness and resource utilization of enterprise networks. WMNs can grow easily as the size of enterprise expands.

WMNs for enterprise networking are much more complicated than at home because more nodes and more complicated network topologies are involved. The service model of enterprise networking can be applied to many other public and commercial service networking scenarios such as airports, hotels, shopping malls, convention centers, sport centers, etc.

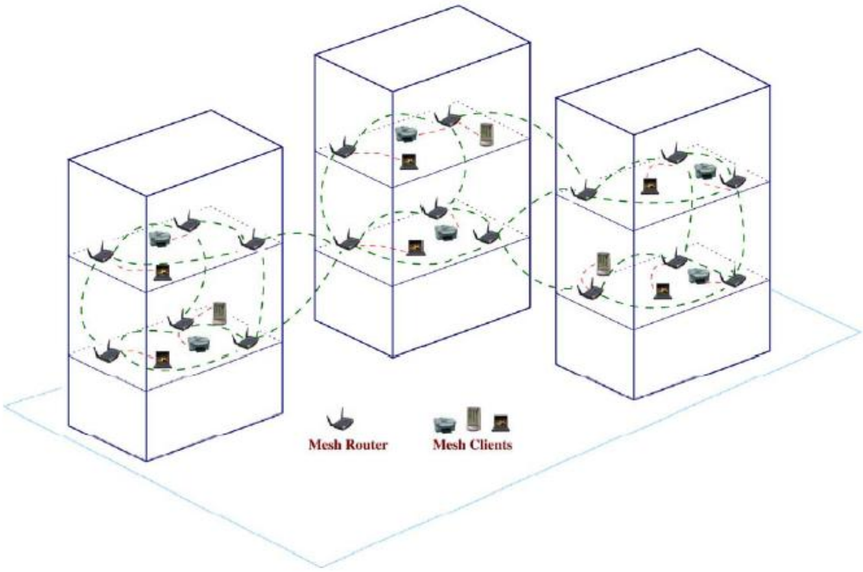


Figure 1.9 WMNs for enterprise networking

- **Metropolitan area networks (MAN):**

  WMNs in a metropolitan area have several advantages. The physical-layer transmission rate of a node in WMNs is much higher than that in any cellular systems. For example, an IEEE 802.11g node can transmit at a rate of 54 Mbps.Moreover, the communication between nodes inWMNs does not rely on a wired backbone. Compared to wired networks, e.g., cable or optical networks, wireless mesh MAN is an economic alternative to broadband networking, especially in underdeveloped regions. The wireless mesh MAN covers a potentially much larger area than home, enterprise, building, or community networks, as shown Figure 1.10.

Thus, the requirement on the network scalability by wireless mesh MANs is much higher than that by other applications.

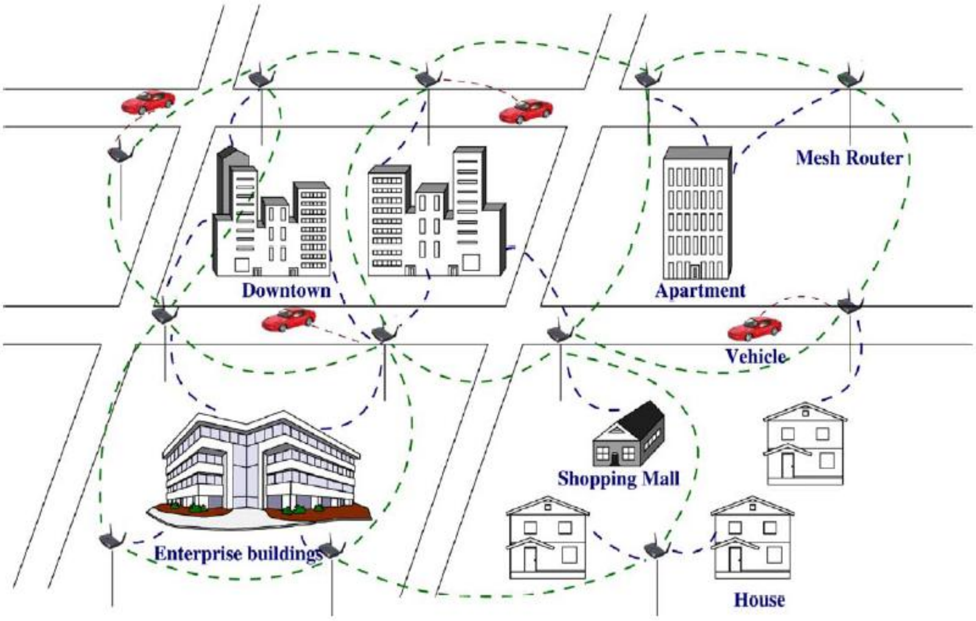


Figure 1.10 WMNs for metropolitan area networks

- **Transportation systems:**

  Instead of limiting IEEE 802.11 or 802.16 access to stations and stops, mesh networking technology can extend access into buses, ferries, and trains. Thus, convenient passenger information services, remote monitoring of invehicle security video, and driver communications can be supported. To enable such mesh networking for a transportation system, two key techniques are needed: the highspeed mobile backhaul from a vehicle (car, bus, or train) to the Internet, and mobile mesh networks within the vehicle, as shown in Figure 1.11.

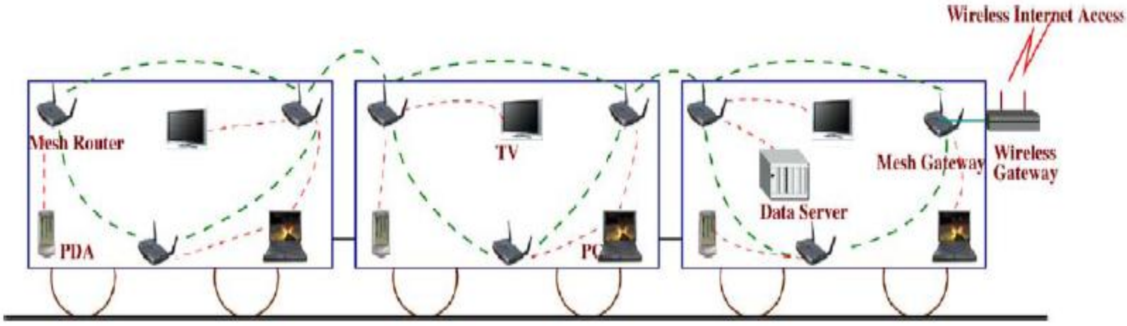


Figure 1.11 WMNs for transportation systems

- **Building automation:**

  In a building, various electrical devices including power, light, elevator, air conditioner, etc., need to be controlled and monitored. Currently, this task is accomplished through standard wired networks, which is very expensive due to the complexity in deployment and maintenance of a wired network. Recently, Wi-Fi-based networks have been adopted to reduce the cost of such networks.

  However, this effort has not achieved satisfactory performance yet, because the deployment of Wi-Fi for this application is still rather expensive due to the wiring of Ethernet. If BACnet (Building Automation and Control networks) access points are replaced by mesh routers, as shown in Figure 1.12, the deployment cost will be significantly reduced. The deployment process is also much simpler due to the mesh connectivity among wireless routers.

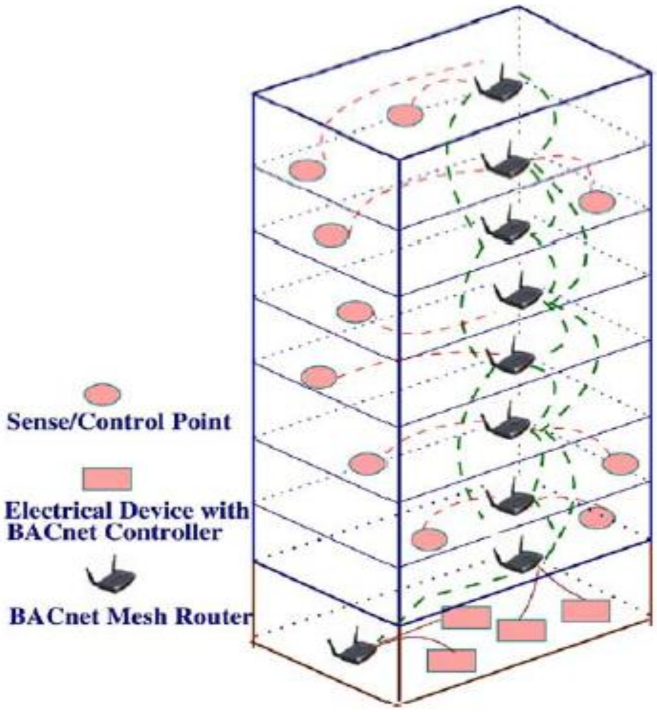


Figure 1.12 WMNs for building automation

- **Health and medical systems:**

  In a hospital or medical center, monitoring and diagnosis data need to be processed and transmitted from one room to another for various purposes. Data transmission is usually broadband, since high resolution medical images and various periodical monitoring information can easily produce a constant and large volume of data. Traditional wired networks can only provide limited network access to certain fixed medical devices. Wi-Fi-based networks must rely on the existence of Ethernet connections, which may cause high system cost and complexity but without the abilities to eliminate dead spots. However, these issues do not exist in WMNs.

- **Security surveillance systems:**

  As security is turning out to be a very high concern, security surveillance systems become a necessity for enterprise buildings, shopping malls, grocery stores, etc. In order to deploy such systems at locations as needed, WMNs are a much more viable solution than wired networks to connect all devices.

Since still images and videos are the major traffic flowing in the network, this application demands much higher network capacity than other applications.

In addition to the above applications, WMNs can also be applied to spontaneous (emergency/disaster) networking and P2P communications. For example, wireless networks for an emergency response team and firefighters do not have in-advance knowledge of where the network should be deployed. By simply placing wireless mesh routers in desired locations, a WMN can be quickly established. For a group of people holding devices with wireless networking capability, e.g., laptops and PDAs, P2P communication anytime anywhere is an efficient solution for information sharing. WMNs are able to meet this demand. These applications illustrate that WMNs are a superset of ad hoc networks, and thus, can accomplish all functions provided by ad hoc networking.

Chapter Two

Introduction to IEEE 802.11

2.1 Introduction

Definitely, the IEEE 802.11 protocols and transmission schemes are truly one of the most remarkable standardization achievements. An uncountable number of devices are today based on this standard.

It started with a wireless extension for local area networks in 1997, and since then has been gradually improved and extended towards a very flexible, well-understood technology. Because 802.11 was built for radio systems in unlicensed spectrum, there is virtually no limitation to the use of 802.11: unlicensed spectrum is often harmonized throughout the world, which means that such radio systems can be used at any location and time. Because of its inherent simplicity, 802.11 is the dominant standard for commercial wireless communication systems, and the research community often refers to this standard during experimentation, and when developing future wireless systems.

The IEEE published the original IEEE 802.11 standard in 1997 as a specification for the transmission scheme and medium access control protocol for Wireless Local Area Networks (WLANs). A revised version of improved accuracy followed in 1999. At the same time, 802.11a and 802.11b, which were the first sub standards to extend 802.11, were published in parallel in 1999. The *IEEE Wireless LAN Edition* is a compilation of 802.11, 802.11a and 802.11b (IEEE, 2003a). Today’s 802.11 is divided into many more sub standards each addressing particular extensions.

With this diverse set of incremental improvements, 802.11 continues to evolve into different directions that are demanded by commercial, scientific, medical, public safety, and military needs.

As a result, because of this flexibility, 802.11 emerge towards an ever-present technology.

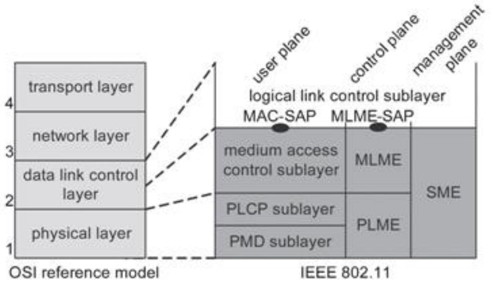
IEEE 802.11 is described and analyzed in detail in this chapter, where focus is given to the layer 2 protocols for spectrum management and Quality of Service (QoS) [6, 7, 8].

2.2 Scope of 802.11

Like IEEE 802.3 (Ethernet) and IEEE 802.5 (Token Ring), the 802.11 standard focuses on the two lower layers (1 and 2) of the Open System Interconnection (OSI) reference model. This is indicated in the reference model of 802.11 illustrated in Figure 2.1. This reference model divides the Data Link Control (DLC) layer (i.e., OSI layer 2) into Logical Link Control (LLC) and Medium Access Control (MAC) sublayers. 802.11 defines Physical layer (PHY) transmission schemes (OSI layer 1), and the MAC protocol, but no LLC functionality.

For LLC, the 802.11 system may rely on general protocols that are usable with all 802 standards.

This LLC layer is independently specified for all 802 LANs, wireless or wired. Whereas this LLC protocol can be applied for wired and wireless systems, the management and control functions to address the characteristic implications of wireless communication systems need to be specified by 802.11 in particular. To consider for example radio range aspects, 802.11 includes functions for the management and maintenance of the radio network, which exceed the usual MAC objectives [6].



Layer 1: PHY transmission scheme
Layer 2: MAC protocols, MAC Layer Management Entity (MLME)
Layer 1 & 2: Station Management Entity (SME)
Interface to higher layers: Service Access Points (SAPs)

Figure 2.1 The IEEE 802.11 reference model (right) and the OSI reference model (left).

2.2.1 Architecture

The 802.11 network architecture, illustrated in Figure 2.2, is hierarchical. Its basic element is the Basic Service Set (BSS), which is a group of stations controlled by the so-called Coordination Function (CF). The CF manages the access to the wireless medium. The Distributed Coordination Function (DCF) is used by all stations in the BSS, whereas the Point Coordination Function (PCF) is an optional extension for the support of QoS, described in older versions of the standard [6, 19].

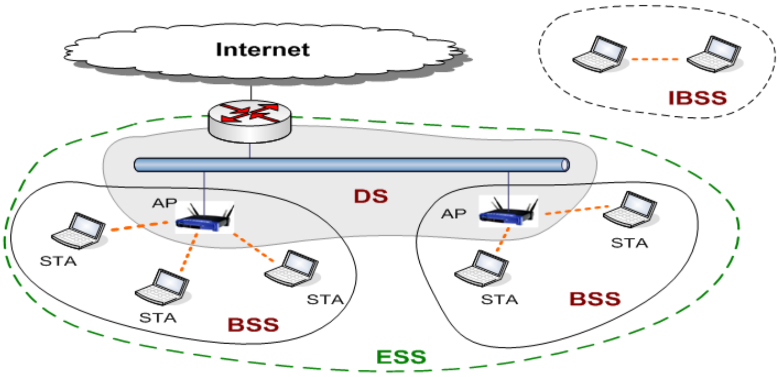


Figure 2.2 The IEEE 802.11 architecture with typical scenarios of the different service sets.

The DCF/PCF coordination functions are concepts for spectrum management and medium access. The PCF uses the DCF coordination function to support QoS.

An Independent Basic Service Set (IBSS) is the simplest 802.11 network type. It is a network consisting of a minimum of two stations, where each station operates with exactly the same protocol. No station has priority over another, the responsibility of coordinating the medium access is distributed among all stations.

An infrastructure-based BSS includes one station that has access to the wired network and is therefore referred to as an Access Point (AP). The abbreviation “BSS” in the following is used to refer to both types of service sets, if not stated otherwise. Stations, including the AP, are simply referred to as stations, which in the original standardization documents is abbreviated as STA.

A BSS may also be part of a larger network, the so-called Extended Service Set (ESS). This ESS consists of one or more BSSs connected over the Distribution System (DS). Originally, without the mesh network extension, BSS and DS operate independently on different media.

The BSS operates on wireless channels whereas the DS typically uses the Distribution System Medium (DSM). As the 802.11 architecture is specified independently of any specific media, the DSM may use different variants of IEEE 802 networks for its service, for example Ethernet.

2.2.2 Services

The DS provides the service to transport MAC Service Data Units (MSDUs) between stations that are not in direct communication.

An AP provides the Distribution System Services (DSS). The DSSs enable the MAC to transport MSDUs between stations that cannot communicate over a single instance of radio channel.

There are two categories of services in 802.11, the Station Services (SS) and the Distribution System Service (DSS). DSSs are not available in an IBSS. The main SS of a BSS is the MAC Service Data Unit (MSDU) delivery. Other SSs include (de-) authentication and privacy.

DSSs include (re-) association, (dis-) association, and integration. The integration service enables the delivery of MSDUs between non-802.11 LANs and the DS via the so-called portal. A portal is the logical point where a non-802.11 LAN is connected to the DS, for communication across the different types of LANs [6].

Chapter Three

IEEE 802.11s WMNs

3.1 Introduction

IEEE 802.11s started with a charter to extend WLAN for extended service set (ESS) mesh networking. Existing IEEE 802.11 standards specify WLAN access network operations between WLAN clients [stations (STAs)] and access points (APs).

In order to extend IEEE 802.11 standards for mesh, backhaul (infrastructure WLAN links) and gateway (infrastructure WLAN to wired-LAN links) operations must be amended to the existing standards (see Figure 3.1). These operations are in the areas of medium access control (MAC), power saving, routing and forwarding, interworking with 802 other networks, security, quality of service (QoS), management and configuration of a WLAN mesh network [16, 18, 22, 32].

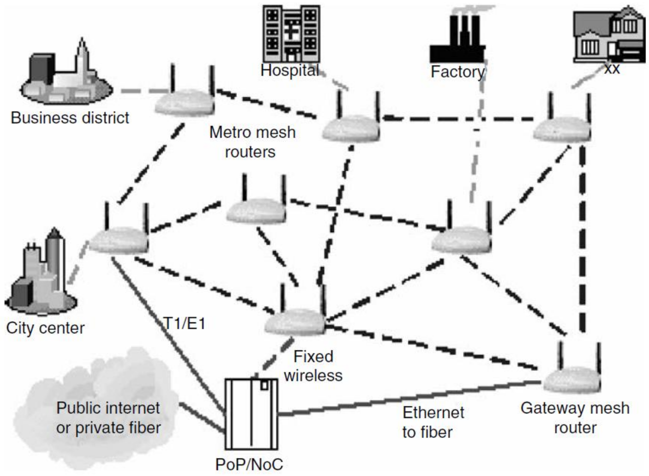


Figure 3.1: A WLAN mesh network.

3.2 History of IEEE 802.11s Standard

The IEEE 802.11s draft standard has gone through a lot of upgrades. It started as a study group of the IEEE 802.11 in September 2003. It became a task group in July 2004 [10]. A call for proposal's but mergers and elimination of these proposals reduced the number to two and these two the "See-Mesh" and the "Wi-Mesh" proposals were merged in January 2006 to form the initial Draft D1.0 [11]. That was failed to be approved in the first trial of a letter ballot in November 2008. Then Draft 2.0 [12] has been adopted and again failed in their 2nd letter ballot because many issues still remain in May 2008.

After that new drafts established as in March 2009 Draft 3.0 [13], December 2009 Draft 4.0 [14], March 2010 Draft 5.0 [15], June 2010 Draft 6.0 and all of them failed to approve and now days Draft 7.0 established.

3.3 Network Architecture of 802.11s

In order to understand the network architecture of 802.11s, we first need to explain 802.11 Extended Service Set (ESS) and its difference from IBSS.

An 802.11 ESS consists of multiple basic service set (BSS) connected through a distributed system (DS) and integrated with wired LANs. The DS service (DSS) is provided by the DS for transporting MAC service data units (MSDU) between APs, between APs and portals, and within the same BSS if MSDU is broadcast/multicast or intended to involve DSS.

The portal is the logical point for letting MSDUs from a non-802.11LAN enter the DS. An ESS appears as a single BSS to the logical link control layer at any station associated with one of the BSSs. The 802.11 standard has pointed out the difference between IBSS and ESS.

IBSS actually has one BSS and does not contain a portal or an integrated wired LAN since no physical DS is available. Thus, the ESS architecture can meet the needs of client support and Internet access, while IBSS cannot. As show in Figure 3.2 [16, 19]

However, IBSS has the advantage of self-configuration and ad hoc multihop networking.

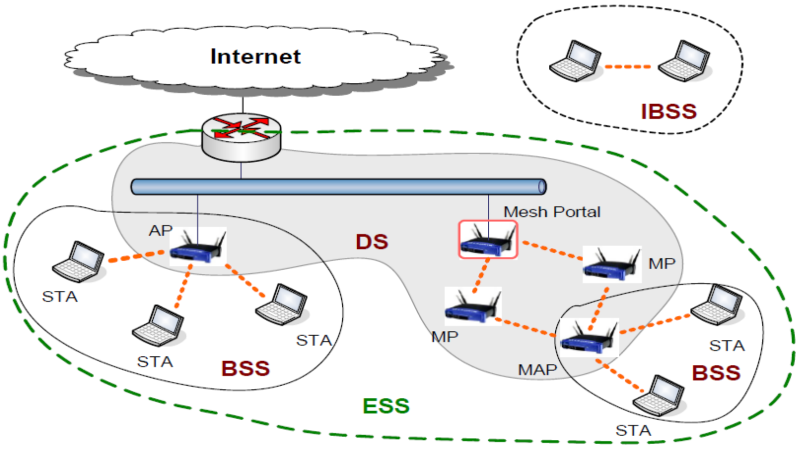


Figure 3.2: Architectural Model

In 802.11s, a meshed wireless LAN is formed via ESS mesh networking. In other words, BSSs in the DS do not need to be connected by wired LANs. Instead, they are connected via mesh networking, possibly with multiple hops in between. Portals are still needed to interconnect 802.11 wireless LANs and wired LANs.

Based on such a concept, the network architecture of 802.11s is formed as shown in Figure 3.3. There are three new nodes in this architecture. A mesh point (MP) is an 802.11 entity that can support wireless LAN mesh services. A mesh access point (MAP) is an MP that can also work as an access point. A mesh portal (MPP) is a logical point where MSDUs enter and exit the mesh network from and to other parts of the DS such as a traditional 802.11 LAN or from and to a non-802.11 network. Mesh portal includes the functionality of MP. It can be co-located with an 802.11 portal [23, 25, 31].

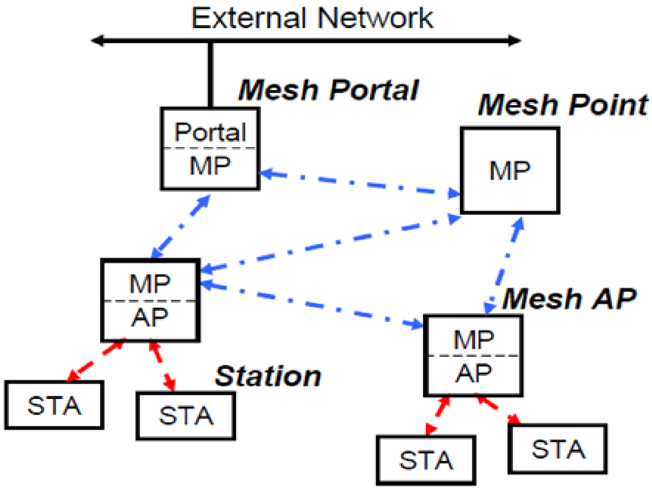


Figure 3.3: Network architecture of 802.11s meshed wireless LANs

3.4 System Architecture of 802.11s

Figure 3.4 shows system architecture for WLAN mesh network technology [22].

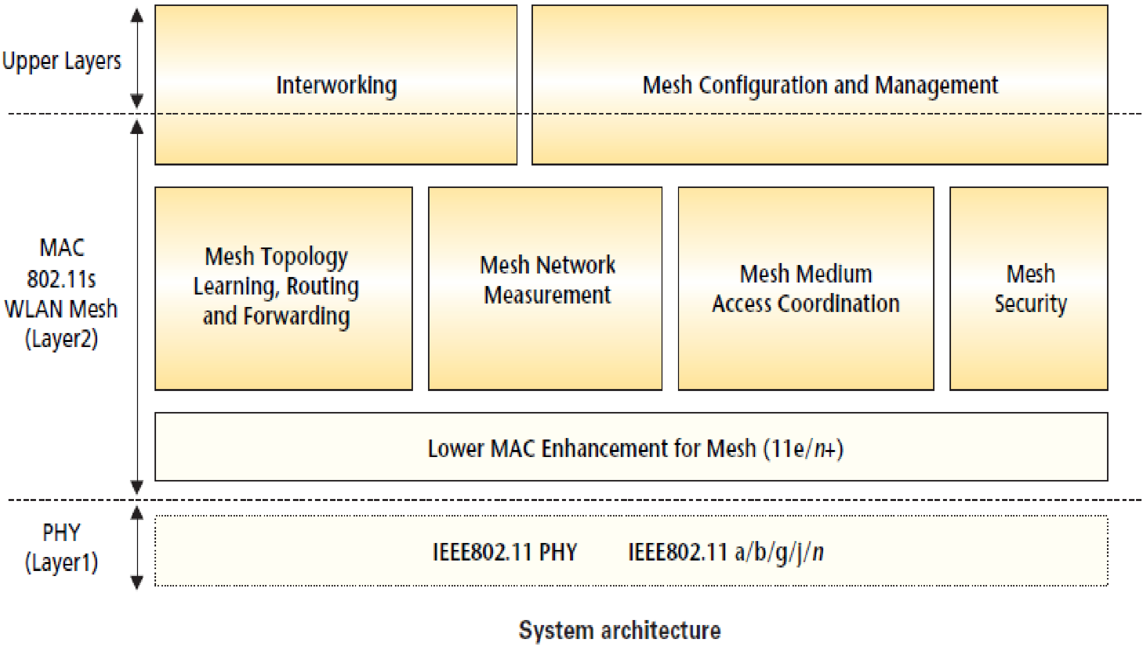


Figure 3.4: System Architecture of 802.11s

3.4.1 Mesh Topology Learning, Routing, and Forwarding

It is including [17, 22, 23]:

- A function for discovering neighboring nodes.
- A function for obtaining radio metrics that provides information on the quality of wireless links.
- Routing protocol for determining routes to transfer packet to their destinations using MAC addresses as identifiers.
- A packet forwarding function.

NETWORK DISCOVERY IN MESH

This is a mandatory feature of 802.11s draft standard. Mesh formation requires that the members of a mesh network have sufficient information about themselves and the available connections between them. This process requires detection of mesh members through beacons or active scanning using mesh probe requests, followed by the exchange of routing information, which may include link-state information.

Mesh formation is a continuous process that entails monitoring of neighbor nodes and their connectivity so as to detect and react to changes in mesh memberships and in connectivity between mesh members [10, 33].

The two sub elements of network discovery:

- Topology discovery
- Neighbor discovery

Topology Discovery

802.11s draft standard supports topology discovery using profiles [10, 25, 35].

A device must support at least one profile. A profile consists of:

- Mesh ID
- Path selection protocol identifier
- Path selection metric identifier

The path selection protocol and path selection metrics in use may be different for different profiles.

Neighbor Discovery

An MP performs passive or active scanning to discover neighboring MPs. In case of passive scanning, a device is considered a neighbor MP if and only if all of the following conditions are met (similar conditions must be met with probe responses in case of active scanning) [6, 10]:

1. A beacon is received from that device.

2. The received beacon contains a mesh ID that matches the mesh ID of at least one of the profiles on the MP.

3. The received beacon contains WLAN mesh capabilities: Version, MP-active indication, and path selection protocol identifier with a matching metric identifier.

Mesh Peer Link Establishment

Once a mesh node has joined a mesh network, and before it can start send packets, it needs to establish peer links with its neighbors.

In 802.11s, state machines and detailed procedures have been specified for setting up peer links. Once this step is completed, it is also necessary to establish a measure of link quality for each peer link. This requires a link quality measurement scheme and a procedure for populating such information among neighbors. When necessary, a procedure to ensure symmetrical link quality information has to be available. It should be noted that the link quality information of each peer link will also be one of the routing metrics for the routing protocol [25].

Channel Selection

This is a mandatory feature of 802.11s draft standard. A WLAN mesh network topology may include MPs with one or more radio interfaces and may utilize one or more channels for communication between MPs. When channel switching is not supported, each radio interface on an MP operates on one channel at a time. But the channel may change during the lifetime of the mesh network according to dynamic frequency selection (DFS) requirements.

The specific channel selection scheme used in a WLAN mesh network may vary with different topology and application requirements. A set of MP radio interfaces that are interconnected to each other by a common channel are referred to as a unified channel graph (UCG). The same device may belong to different UCGs.

An MP logical radio interface that is in simple unification mode selects a channel in a controlled way such that it enables the formation of a UCG that becomes merged and hence fully connected. The MP logical radio interface thus establishes links with neighbors that match the mesh ID and mesh profile and selects its channel based on the highest channel precedence value [10, 25, 27, 33].

As shown in Figure 3.5 an example UCGs in WLAN Mesh

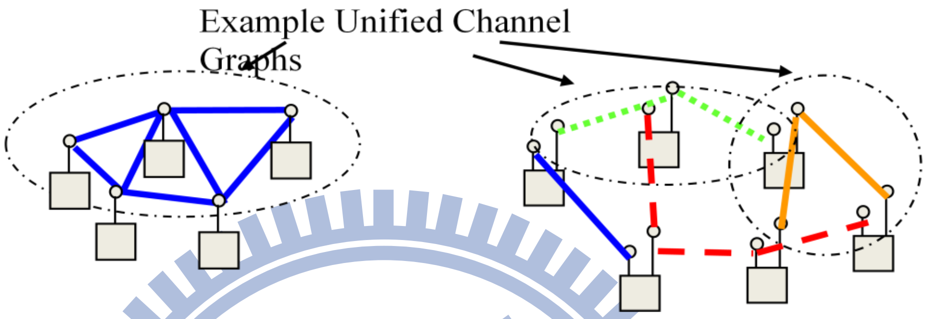


Figure 3.5: Example UCGs in WLAN Mesh

Simple Channel Unification Protocol

At boot time, an MP logical radio interface that is configured in simple channel unification mode performs passive or active scanning to discover neighboring MPs.

If an MP is unable to detect any neighboring MPs, it adopts a mesh ID from one of its profiles, and selects a channel for operation as well as an initial channel precedence value. The initial channel precedence value may be initialized to the number of microseconds since the boot time of the MP plus a random value.

In the event that an MP logical radio interface that is configured in simple channel unification mode discovers a disjoint mesh, i.e., the list of candidate peer MPs spans more than one channel, it selects the channel that is indicated by the candidate peer MP which has the numerically highest channel precedence indicator to be the unification channel.

3.4.2 Mesh Network Measurement

It is including [35]:

- Functions for calculation radio metrics used by routing protocol.
- Functions for measuring radio conditions within the WLAN mesh network for use in frequency channel selection.

3.4.3 Mesh Medium Access Coordination

It is including:

- Functions for preventing degraded performance due to hidden and exposed terminals.
- Functions for performing priority control, congestion control, and admission control.
- A function for achieving spatial frequency reuse.

3.4.4 Mesh Security

The security specification in 802.11s is dedicated to protection of transporting packets. The security in routing or forwarding functionality in a mesh network is not specified.

The 802.11s security inherits lots of work from 802.11i for initial authentication. In order to satisfy the peer-to-peer environment, a role negotiation protocol is added before starting the security protocol exchange [10, 21, 25].

3.4.5 Interworking

The interworking between mesh networks and other LAN segments is carried out through the bridging function in mesh point portals (MPPs) in a manner compatible with IEEE 802.1D [10, 21].

A transparent bridge (technology used for interconnecting LANs defined by IEEE 802.1D, it enables terminals belonging to different LANs to be seen by each other as if they were operating on the same LAN) function must be implemented in the MPP.

In order to tell MPs in the mesh networks of its presence, an MPP needs to send an MPP announcement. An MPP announcement protocol is specified in 802.11s [25, 33].

3.4.6 Mesh Configuration and Management

A WLAN interface used for automatic setting of each MPs Radio Frequency (RF) parameters (frequency channel selection, transmit power) for mesh network management.

WMNs were originally envisioned to be self-configuring, self-healing, and self-monitoring networks. The need for management and configuration is reduced to a very minimum set as by the 802.11s draft standard [21, 31].

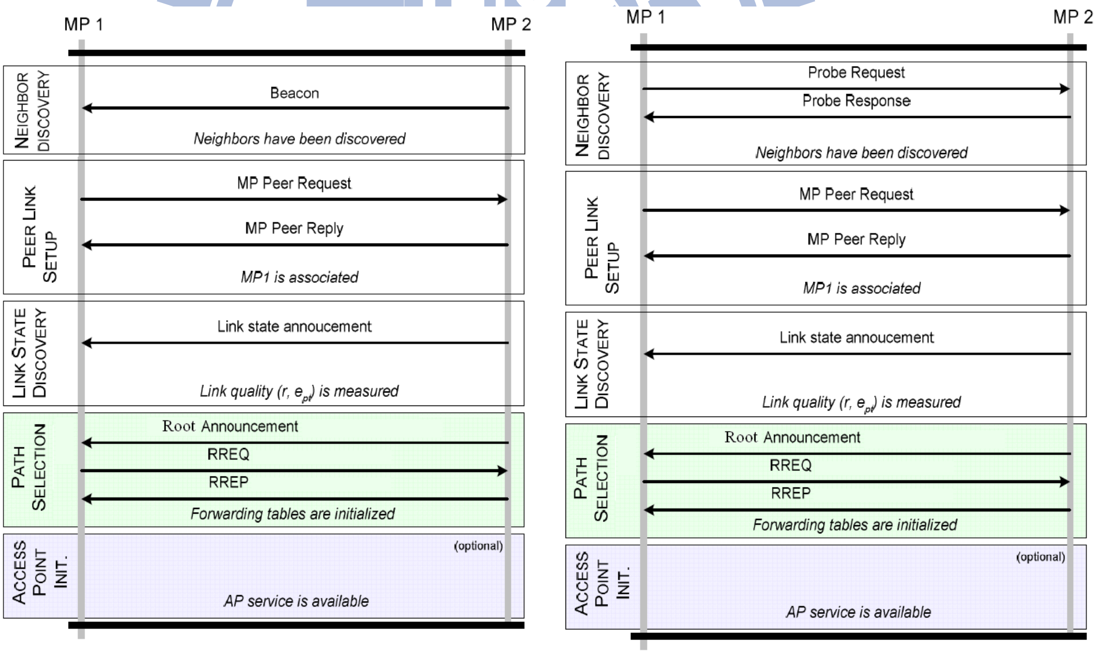
3.5 MP Boot Sequence

At power up, a configured MP shall perform the following sequence of operations [10]:

1. Passive or Active scanning to discover other MP
2. Channel selection
3. Begin mesh beaconing.
4. Neighbor MP link establishment
5. Local link state measurement
6. Routing initialization
7. AP initialization (optional – if MAP)

This sequence is illustrated in Figure 3.6.

Link establishment may be performed with a number of nodes but not all of the links will become active – that depends on the outcome of the link state measurements and on the routing initialization. The final (optional) step of the boot sequence is AP service initialization.



(a) Using Passive Scanning **(b) Using Active Scanning**

Figure 3.6: Mesh Point Boot Sequence

Chapter Four

IEEE 802.11s MAC

4.1 Introduction

WMNs require the coordination and collaboration of mesh APs over multiple hops. Therefore, new MAC features designed specifically for WMNs become necessary to improve the performance of such networks.

Recently, an IEEE 802.11 task group (TGs) was formed to draft a standard for wireless mesh networking. The first baseline draft of 802.11s supports the 802.11 distributed coordination function (DCF) protocol and the 802.11e enhanced distributed channel access (EDCA) protocol with several additional MAC features.

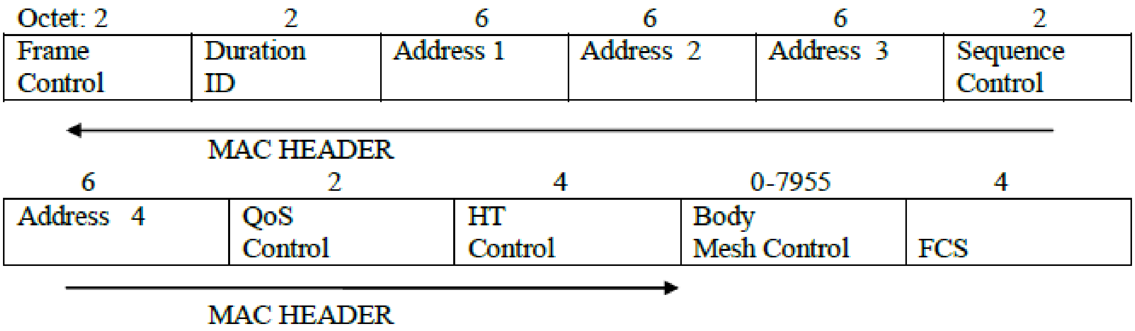
The Optional MAC Enhancements include:

- Multichannel MAC protocol, i.e., common channel framework (CCF)
- Mesh deterministic access (MDA) scheme that offers better QoS.
- An intra mesh congestion control scheme that seeks to relieve the congestion situations among wireless mesh nodes
- Power Management

4.2 The MAC frame format

Table 4.1 depicts in general the MAC frame format [10, 18, 32, 34].

Table 4.1: MAC Frame Format



Octet: 2	2	6	6	6	2
Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control

MAC HEADER

6	2	4	0-7955	4
Address 4	QoS Control	HT Control	Body Mesh Control	FCS

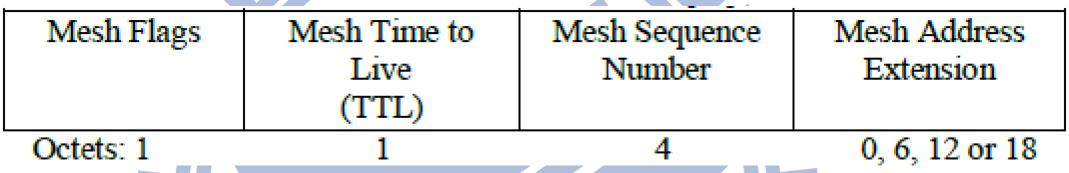
MAC HEADER

4.2.1 Mesh control field

The mesh control field is a 6 to 24 octet field shown in the Table 4.2 below. The control field helps to support all kinds of unicast, multicast and broadcast traffic. The control field includes:

- An 8-bit mesh flag field
- Mesh Time to Live
- Mesh Sequence Number
- Mesh Address Extension

Table 4.2: Mesh Control Field

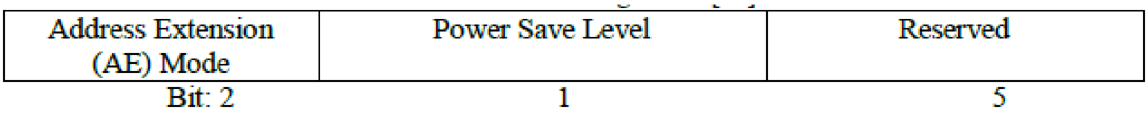


Mesh Flags	Mesh Time to Live (TTL)	Mesh Sequence Number	Mesh Address Extension
Octets: 1	1	4	0, 6, 12 or 18

4.2.2 Mesh flags field

The first octet contains an 8-bit mesh flags field which is used to control mesh specific header processing. As an example, the first two bits indicate the presence of Address Extension (AE). Another bit indicates the power save level while the rest of the bits are reserved for future use. Table 4.3 shows the Mesh flags Field.

Table 4.3: Mesh Flags Field



Address Extension (AE) Mode	Power Save Level	Reserved
Bit: 2	1	5

4.2.3 Mesh Time To Live

The second octet defines the mesh time to live (TTL). “The field is also 8 bits in length containing an unsigned integer that counts down depending on the number of times remaining that the frame can be forwarded.” It is used to mitigate the frame being forwarded in an infinite loop. Hence once the decremented integer in the frame goes to zero, the next hop device discards the frame.

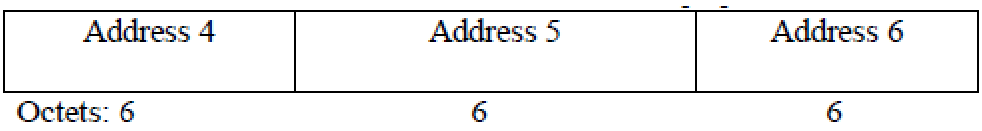
4.2.4 Mesh Sequence Number field

The third and fourth octet defines the mesh sequence number (SN) field. This sequence number is used by the receiving station to detect duplicate broadcast frames and avoid unnecessary retransmissions.

4.2.5 Mesh Address Extension field

The mesh address extension field works in tandem with the mesh flag field when the entry in the address extension (AE) mode is a non-zero entry value. It contains 6, 12 or 18 octets in length. Table 4.4 shows the mesh address extension field which contains three additional address fields for mesh address extensions.

Table 4.4: Mesh Address Extension Field



Address 4	Address 5	Address 6
Octets: 6	6	6

“The address 4 field is used in the mesh management frames of subtype multi-hop action to include a fourth address that is missing from the MAC header of management frames.

Address 5 and Address 6 are very useful in cases where the endpoints are non-mesh entities. Their source and destination addresses are transported in this address field”.

4.3 Background

4.3.1 CSMA and CSMA/CA

In Carrier sense multiple access (CSMA), a node first senses the channel to make sure that it is idle before transmitting. If the channel is busy, the node defers its transmission.

Using carrier sensing, a node can successfully avoid collisions with transmitting stations within its carrier sense range.

CSMA with collision avoidance (CSMA/CA) leverages the performance benefits of CSMA and extends CSMA to further reduce the likelihood of collisions.

In a wireless network, as radio signals attenuate over distance, simultaneous transmissions may lead to collisions at the receiver even though both senders have sensed an idle channel. This is called the hidden node problem. By utilizing two small control packets, i.e., request-to send (RTS) and clear-to-send (CTS), CSMA/CA can effectively mitigate the hidden node problem [1, 3, 31].

4.3.2 IEEE 802.11 DCF Protocol

The IEEE 802.11 standard specifies two medium access methods:

(1) Distributed coordination function (DCF) that builds on CSMA/CA

(2) Point coordination function (PCF) providing contention-free access.

Because PCF requires a central control entity, i.e., a point coordinator, it is rarely used in WMNs.

Additionally, because of its robustness and flexibility, many advanced MAC protocols are also based on the IEEE 802.11 DCF protocol.

The IEEE 802.11 DCF protocol is based on the CSMA/CA principle and it operates in a similar way. A node wishing to transmit first senses the channel. If the medium is sensed busy, it defers its transmission. If the medium is free for a specified period of time called distributed inter frame space (DIFS), the node is allowed to transmit. Upon correctly receiving the data packet, the receiver returns an ACK after a fixed period of time called short inter frame space (SIFS). Receipt of the ACK indicates the correct reception of the data packet.

If no ACK is received, the sender assumes a collision has occurred and doubles the size of its contention window. Then, the sender chooses a random back-off number between 0 and its contention window size. The sender is allowed to retransmit the packet when the channel is free for a DIFS period of time augmented by the random back-off time. The packet is dropped after a given number of failed retransmissions [3, 7, 31].

4.3.3 IEEE 802.11e MAC Protocol

The IEEE 802.11e standard draft defines a number of QoS enhancements to IEEE 802.11. Two main functional blocks are defined in IEEE 802.11e:

(1) The channel access functions

(2) The traffic specification (TSPEC) management.

The channel access function defines a new coordination function called the hybrid coordination function (HCF).

HCF has two modes of operation: a contention based protocol called enhanced distributed channel access (EDCA) and a polling mechanism called HCF controlled channel access (HCCA).

EDCA enhances the original DCF by providing prioritized medium access based on different traffic classes, also called access categories (ACs).

The IEEE 802.11e defines four ACs, each of which has its own queue and its own set of EDCA parameters. The differentiation in priority between ACs is realized by setting different values for the EDCA parameters.

The EDCA parameters include:

(1) Arbitration interframe space number (AIFSN)

(2) Minimum contention window (CWmin)

(3) Maximum contention window (CWmax)

(4) Transmission opportunity (TXOP) limit.

AIFS is the period of time the wireless medium is sensed idle before the start of a frame transmission.

Although, real-time traffic such as video and voice has more aggressive EDCA parameters, which is to ensure QoS traffic has a better chance to acquire the medium than the best-effort or background traffic. This basic idea of supporting prioritized traffic [1, 3, 7, 9].

4.4 Enhanced Distributed Channel Access

The EDCA is a distributed, contention based medium access mechanism. It is an extension of the DCF. EDCA is the default and mandatory MAC function for all mesh stations in the 802.11s draft standard. It provides MAC QoS enhancement introduced by 802.11e.
In EDCA, stations access the wireless Medium Using 8 different user priorities. This means that packets forwarded by the stations are assigned priority values before access into the MAC based on the information they carry.
These packets are then mapped into four different categories called Access categories (ACs) implemented in EDCA which include [6, 7]:

- Voice
- Background
- Best Effort
- Video

An AC has a specific parameter set that defines its probability to access the Wireless Medium (WM). Since EDCA was designed for single hop networks, it has inherent problems like in the case of high load, EDCA devices throttle themselves as unsuccessful transmission leading to increasing contention window sizes and making EDCA less efficient in high medium usage [18].

4.5 Common Channel Framework

An optional CCF is proposed to enable the operation of single-radio devices in a multichannel environment.

The CCF assumes that each node is equipped with a single half-duplex transceiver and nodes in the network or in the same cluster share a common control channel. To legacy devices (STAs and AP) and MPs that do not support the CCF, the common channel appears as any other 802.11 channel and their operation remains unaffected. Using the CCF, node pairs, select a different channel and switch to that channel for a short period of time, after which they return to the common channel. During this time, nodes exchange one or more DATA frames. The channel coordination itself is carried out on the common channel by exchanging control frames or management frames that carry information about the destination channel. In this way, simultaneous transmission on multiple channels is achieved which in turn results in increased aggregate throughput.

As shown in Figure 4.1, MPs communicate to each other and utilize the common control channel to select an available data channel [3, 10, 25].

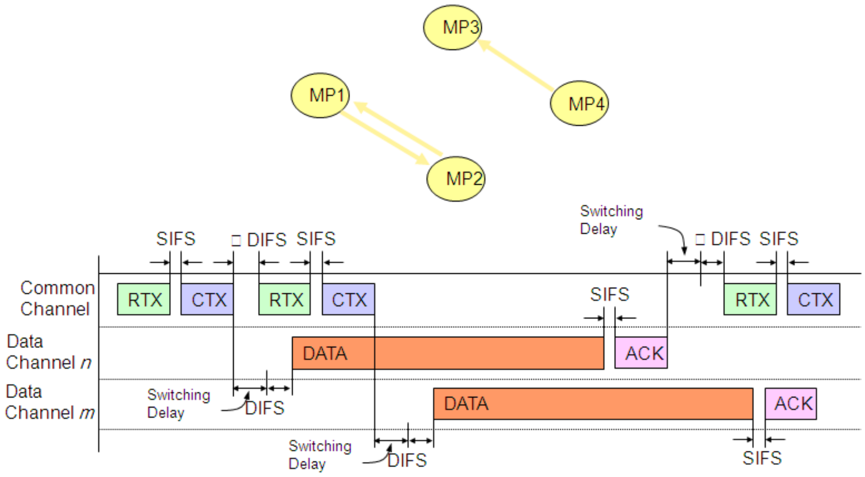


Figure 4.1: channel selection on the common control channel.

4.6 Mesh Deterministic Access

MDA allows MPs to access a certain period with lower contention than that in other periods without MDA. Such a period is called an MDA opportunity (MDAOP). Before using MDAOP to access the medium, the owner of this MDAOP, i.e., the transmitter, needs to set up the MDAOP with its receiver [3, 10, 19].

If this period is accessed by the transmitter, i.e., the owner of MDAOP, it attempts to use CSMA/CA but uses new backoff parameters, MDA maximum contention window (MDACWmax), MDA minimum contention window (MDACWmin), and MDA interframe space number (MDAIFSN), to set up an TXOP. However, for a nonowner of TXOP, it has to defer its access by setting its NAV to the end of the MDOAP or by using a carrier sensing scheme [20, 23, 25, 31].

4.7 Intra mesh Congestion Control

In an IEEE 802.11s network intra-Mesh congestion control is achieved by implementing the following three main mechanisms [33]:

- Local congestion monitoring
    - Each node actively monitors local channel utilization
    - If congestion detected, MP notifies previous-hop neighbors and/or the neighborhood
- Congestion control signaling
    - Congestion Control Request (unicast)
    - Congestion Control Response (unicast)
    - Neighborhood Congestion Announcement (broadcast)

- Local rate control
  - Each node that receives either a unicast or broadcast congestion notification message should adjust its traffic generation rate accordingly
  - Rate control (and signaling) on per-AC basis – e.g., data traffic rate may be adjusted without affecting voice traffic rate

Local congestion is defined as the condition when an intermediate MP receives more packets than it can transmit in a predefined time window. The result of local congestion is that the local buffer gets filled up quickly, and eventually the buffer may become full and packets will have to be dropped from the buffer.

The situation is exacerbated by the presence of hidden and exposed nodes on the same channel causing extensive back-off and retransmissions [3, 10].

Congestion control may not be as critical in a wired network as it is in a wireless network, because each individual hop in the wired network is isolated from other hops, also it does not work well across a multihop wireless network largely due to its susceptibility to high packet loss [22, 24, 25, 26].

4.8 Power Management

Many nodes in 802.11s mesh networks always work in an active state since they either need to be an AP or to forward traffic for other nodes. However, there are still other nodes that need to work in power-save mode [10, 24, 25].

All MPs have the capability to operate in power save mode. More specifically, two different power states are considered [33]:

- Awake: the MP is able to transmit or receive frames and is fully powered.
- Doze: the MP is not able to transmit or receive and consumes very low power.

The manner in which an MP switches between these two power states is determined by the Power Management mode of MP .

These include:

- Active mode: the MP shall be in the Awake state all the time.
- Power save mode: the MP alternates between Awake and Doze states, as determined by the frame transmission and reception rules.

Chapter Five

IEEE 802.11s Routing

5.1 Introduction

It is a widely accepted concept that it is beneficial to have layer-2 routing for WMNs.

Although, 802.11s is probably the first standards committee that actually specifies routing in the MAC layer. Among many other reasons, interoperability is the most obvious motivation to do so. Previously many proprietary 802.11 mesh networks were built using different routing protocols, which result in the difficulty of interoperation.

In 802.11s, the framework for routing is extensible, which means that different routing protocols can be supported by following this framework, but the mandatory protocol will be implemented in order to achieve interoperability.

The routing mechanism in 802.11s handles packet forwarding for MPs, MAPs, and associated STAs. Unicast, multicast, and broadcast frames are all supported in the same framework. Since routing is performed in the MAC layer, packet forwarding is carried out via MAC addresses [1, 3, 9].

In a routing protocol, nodes usually need to exchange routing messages for the purpose of finding link status, collecting neighbor information, requesting routing path, and so on.

In the current draft of 802.11s, one mandatory routing protocol and one optional routing protocol are specified [10]:

- The mandatory routing protocol is called hybrid wireless mesh protocol (HWMP), which is a hybrid routing protocol of reactive on - demand path selection routing and proactive tree building routing.

- The optional routing protocol is based on link state routing and is called radio aware optimized link state routing (RA-OLSR).

5.2 Background

5.2.1 Ad hoc On-Demand Distance Vector Routing Protocol

AODV is a reactive protocol i.e. route are created and maintained only when needed to forward data. It is developed for use in MANET and support both unicast and multicast communication.

The protocol information elements contain sequence number for detecting current routing information and outdated routing information to ensure a loop free network.

AODV uses a conventional routing table approach which allows one entry per destination, it permits nodes to react to link break and change in topology in a timely manner. Routes are only created when needed and maintained as long as it is active with data, routes that have no data traffic are not maintained making this approach to significantly reduce routing overhead in the network as compared to the proactive routing approach [6, 18].

AODV uses the following information elements to carry out route discovery, link monitoring and link breakage notification.

- Route Request (RREQ) Message: the message is used for triggering route discovery by node that needs a path to another node in the network.
- Route Reply (RREP) Message: this message is sent in reply to the message received by the destination node to the originator node of the RREQ.

- Route Error (RERR) Message: the message is generated and sent whenever a node detect a link break in the network to notify other nodes that have link with the affected destination.

5.2.2 Radio Metric - Ad hoc On-Demand Distance Vector Routing Protocol

RM-AODV is path selection protocol that uses basic features of the original AODV protocol.

To create a route the source node broadcasts a RREQ message flooded by all nodes and when a RREQ is received, the distinct node creates a reverse path to the source then the forward path is established when a RREP is received.

In contrast to AODV, intermediate nodes MUST NOT generate a RREP even if they have a route to the destination as shown in figure 5.1 [10].

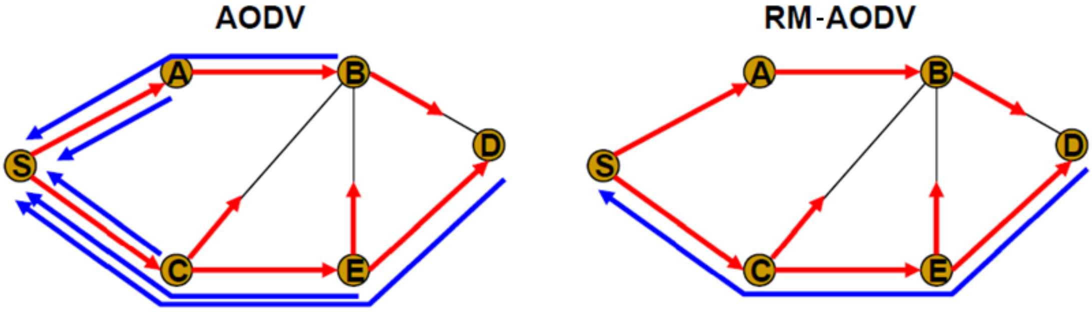


Figure 5.1 AODV and RM-AODV

5.2.3 Optimized Link State Routing

OLSR is a proactive protocol based on table driven techniques. The proactive nature of the protocol makes it to maintain routes to all nodes in the network by frequent exchange of topology information with other nodes in the network.

OLSR adopts the Multipoint Relay (MPR) mechanism to reduce the routing overhead caused by the flooding of control information in the network. Each node in the network selects a set of one-hop symmetric neighbor that can cover at least two-hop symmetric neighbor as MPR.

It is only the selected MPR that is permitted to forward a control message across the network, thereby limiting the number of nodes in the network to retransmit control message. This approach significantly reduces the routing overhead in the network.

The control message contains the list of link state information of the originating nodes, which the MPR declares periodically to all its MPR selectors.

There are fundamental message types that must be observed in the OLSR implementation and must maintain compatibility with old implementation if any additional message type is to be implemented in OLSR. The messages are listed below [10, 18]:

- Hello Message: It is used for conducting link sensing, neighbor detection and MPR signaling process.
- Topology Control (TC) Message: this is used for the topology declaration (advertisement of link state)
- Multiple Interface Declaration (MID) Message: It handles the declaration of the presence of multiple interfaces on a node

5.3 Hybrid Wireless Mesh Protocol

Hybrid Wireless Mesh Protocol is the default path selection protocol developed for use in IEEE802.11s standard. Every WLAN mesh network devices from various vendors shall use HWMP and airtime link metric to ensure interoperability [10, 18].

The protocol combines the strengths of both the proactive and reactive routing protocols due to its hybrid nature.

The operation of HWMP is divided into two modes, where each mode has it’s own strength and weakness [25, 32].

The two modes include:

- On demand mode: this is a reactive approach mode, it establishes peer to peer path for forwarding of data between MPs when there is no root MP configured.
- Tree building mode: The mode builds and maintains tree to link the configured root MP and other MPs in the network.

The information elements used in the HWMP follows closely the concept and principle of the AODV. The elements are:

- Path Request (PREQ)
- Path Reply (PREP)
- Path Error (PERR)
- Root Announcement (RANN)

HWMP includes Sequence Number (SN) in its information elements to detect a fresh path information and stale path information. This enhances loop free network [33, 34].

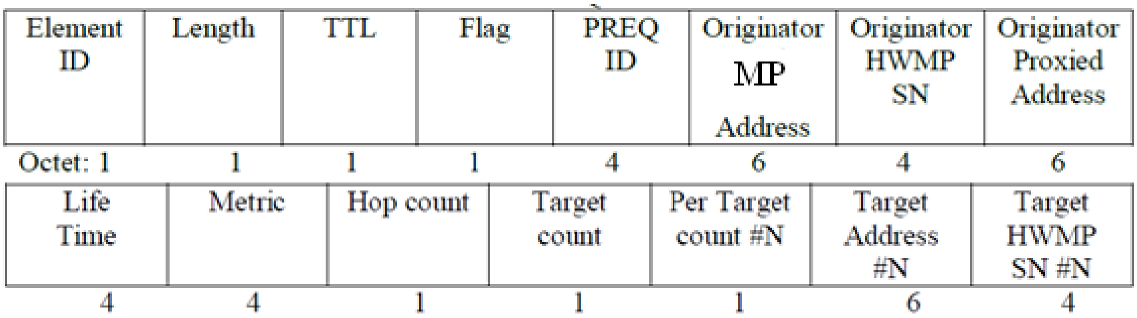
5.3.1 Reactive On- Demand Path Selection Mode

When a MP needs to communicate with a destination MP, it checks the path selection table for a valid path to the destination MP. If there is no exiting path, then the source MP triggers a path discovery using the on demand path selection protocol using the below information element:

PATH REQUEST (PREQ)

The source MP generates and broadcasts a PREQ element to the destination MP. Table 5.1 shows PREQ element format.

Table 5.1: PREQ element



Element ID	Length	TTL	Flag	PREQ ID	Originator MP Address	Originator HWMP SN	Originator Proxied Address
Octet: 1	1	1	1	4	6	4	6

Life Time	Metric	Hop count	Target count	Per Target count #N	Target Address #N	Target HWMP SN #N
4	4	1	1	1	6	4

The originator MP generates the PREQ as follows:

1. The originator address is set to the MAC address of the source MP

2. Originator HWMP SN and PREQ ID are incremented by 1,

3. Proxied address field included if only the Address Extension (AE) in the flag field is set to 1,

4. Metric field and the hop count field are initialized to 0,

5. Lifetime field is set to the time interval the receiving MP of PREQ consider the forwarding information valid,

6. Target count field is set to the number of destinations to be discovered and

7. Time to Live (TTL) field is set to the maximum number of hops allowed for PREQ information element.

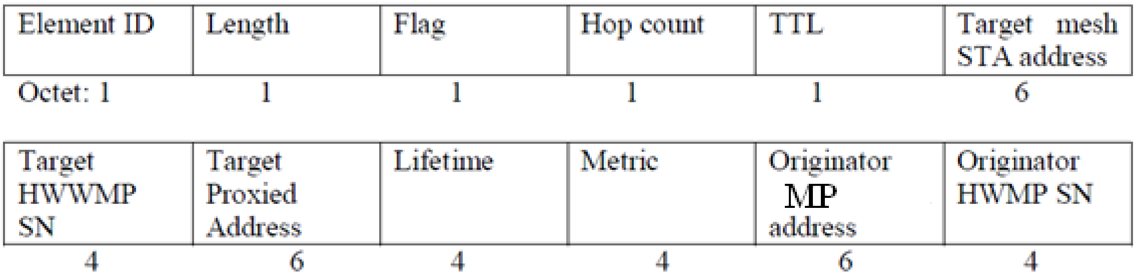
8. Target Address is set to the MAC address of the requested destination and target HWMP SN is set to the last known HWMP SN to the originator MP for the path to the target.

9. In the per target count field Bit 0 contains the Target Only (TO) flag and Bit 1 contains the Reply and Forward (RF) flag. If TO = 1, only the target MP can send an individually addressed PREP to the PREQ. If TO = 0, an intermediate MP that have valid forwarding information to the target MP can reply with an individually addressed PREP to the PREQ and forward the PREQ. This forward of PREQ is controlled by RF flag. When TO = 0 and RF = 0, the intermediate MP does not forward the PREQ, but when RF = 1, intermediate MP set TO flag to 1 before it forwards the PREQ so that other MPs along the path does not respond to the PREQ. The PREQ creates a reverse path from the target MP to the originator MP who triggered the path discovery.

PATH REPLY (PREP)

The PREP is generated by the target MP of the destination MAC address or an intermediate MP that has a valid path to the required destination. The PREP builds a forward path to the originator MP. PREP frame format is shown in table 5.2.

Table 5.2: PREP element



Element ID	Length	Flag	Hop count	TTL	Target mesh STA address	Target HWWMP SN	Target Proxied Address	Lifetime	Metric	Originator MP address	Originator HWMP SN
Octet: 1	1	1	1	1	6	4	6	4	4	6	4

The PREP is built as follows:

1. The Target Proxied address present only if the AE is set to1 in the flag field.

2. Hop count field and the metric field are set to 0.

3. TTL is set to the maximum number of hops allowed for PREP

4. Target MP address is set to MAC address of the target MP or target proxy MAC address.

5. Target HWMP SN is incremented by 1.

6. Originator MP address is set to MAC address of the originator MP, and Lifetime field depends on the PREQ that initiated the PREP.

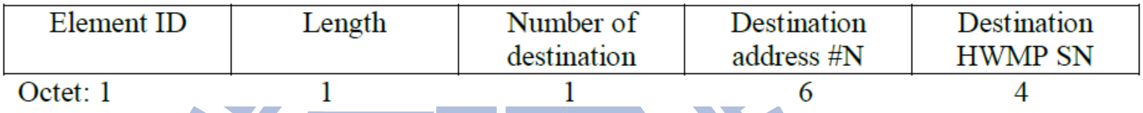
The receiving MP creates or updates valid forwarding information to the target MP. The update is done only when the received target HWMP SN in the PREP is greater than or equal to the existing target HWMP SN and the new path metric information is better than the existing path metric otherwise the information is discarded.

PATH ERROR (PERR)

The PERR element is used in HWMP for link breakage announcement in the WLAN mesh networking to all affected MPs that have an active path across the broken link.

MP triggers a link break detection when is unable to forward data to it next hop MP, it then generates and propagates PERR to inform all MPs that have valid path information with it through the affected MP. Table 5.3 shows the PERR element format as given in the standard.

Table 5.3: PERR element



Element ID	Length	Number of destination	Destination address #N	Destination HWMP SN
Octet: 1	1	1	6	4

The PERR is generated as follows:

1. The number of destination gives total number of unreachable destination.

2. The destination address is set to MAC address of detected unreachable destination.

3. The destination HWMP SN is set to HWMP SN of the detected unreachable MP.

5.3.2 Proactive tree building mode

The proactive tree building is used when a root MP is configured in the network, it is responsible for building a tree to connect MPs to the root MP. The mode provides MPs path information required for reaching the root MP.

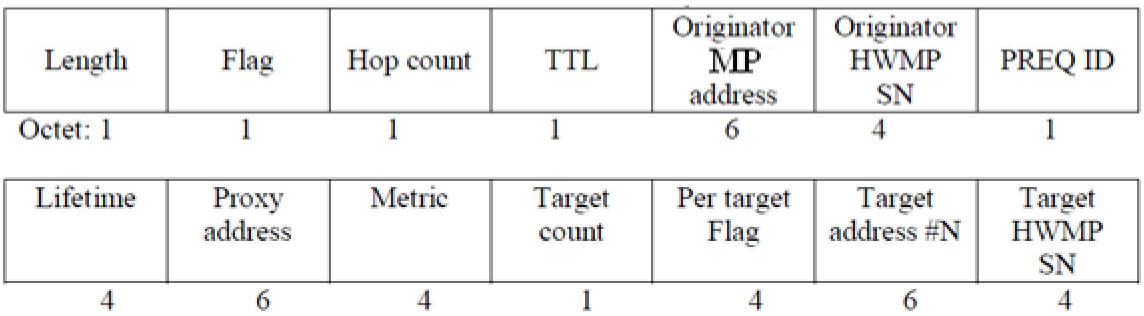
The draft standard defines two approaches designed for tree building mode in HWMP for propagating path information to the root MP. They include:

- Proactive PREQ
- Proactive Root Announcement (RANN)

Proactive PREQ

The root MP generates and broadcasts periodically proactive PREQ across the network in order to distribute path information to other MPs for reaching the root MP. Table 5.4 shows proactive PREQ format.

Table 5.4: proactive PREQ element



Length	Flag	Hop count	TTL	Originator MP address	Originator HWMP SN	PREQ ID
Octet: 1	1	1	1	6	4	1

Lifetime	Proxy address	Metric	Target count	Per target Flag	Target address #N	Target HWMP SN
4	6	4	1	4	6	4

The root MP builds the proactive PREQ as follows:

1. Hop count field and metric field are initialized to 0.

2. PREQ ID and the originator HWMP SN are incremented by 1.

3. Originator MP address is set to MAC address of the root MP.

4. Target count is set to 1,

5. Both TO and RF flag in the per target flag field are set to 1.

6. Target address is set to all 1´s (broadcast address).

7. Target HWMP SN is set to 0.

When MP receives this proactive PREQ, it create or updates forwarding information to root MP, it also updates the hop count and the metric of the proactive PREQ and records the HWMP SN, hop count and metric to the root MP. This updated proactive PREQ is broadcasted across the network to provide path information for reaching the root MP to MPs in the network.

The receiving MP updates its path information to the root MP if only the received Proactive PREQ HWMP SN is greater than or equal to the HWMP SN of the current path information and the received path metric is better than the current path metric. Depending on the Proactive Reply (bit 2) in the flag field of the Proactive PREQ, if set to 1 the receiving MP responds with Proactive PREP which enables path from the root MP to the MP. If Proactive Reply is set to 0, the receiving MP replies only if there is data to exchange with the root MP as shown in Figure 5.2 [35].

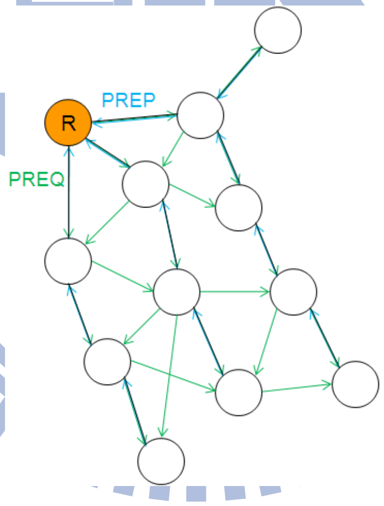
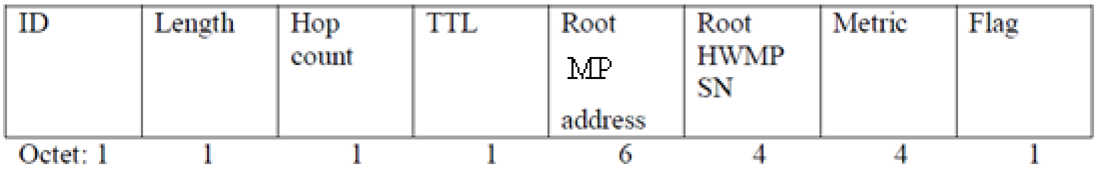


Figure 5.2 Proactive PREQ mechanism

Root Announcement (RANN)

The root announcement (RANN) is adopted to advertise the presence of the root MP in the network. Root MP generates and broadcasts periodically RANN across the network which includes path information other MPs will need for reaching the root MP. The draft standard defined RANN element format given in table 5.5

Table 5.5: RANN element



	ID	Length	Hop count	TTL	Root MP address	Root HWMP SN	Metric	Flag
Octet:	1	1	1	1	6	4	4	1

The RANN element is set as follows:

1. Hop count field and metric field are initialized to 0.

2. TTL set to the maximum number of hops allowed for RANN.

3. Root MP address set to MAC address of the root MP.

4. Root HWMP SN is incremented by 1.

MP receiving the RANN creates or updates forwarding information to the root MP with root MP address, metric, hop count and root MP HWMP SN, the update is carried out only if the received RANN HWMP SN is greater than or equal to the current root MP HWMP SN and the path metric is better than the current path metric.

“When the forwarding information to the root MP has been created or updated, MP triggers an individually addressed PREQ to the root MP through the next hop the RANN was received”.

MP decrements the TTL by 1 and increments the hop count by 1 before propagating the PREQ. The PREQ creates a reverse path from the root MP to the originator MP in relation to the on demand mode discussed earlier. Upon the reception of the PREQ by the root MP it replies with PREP which set up a forward path from the originator MP to the root MP as shown in Figure 5.3 [35].

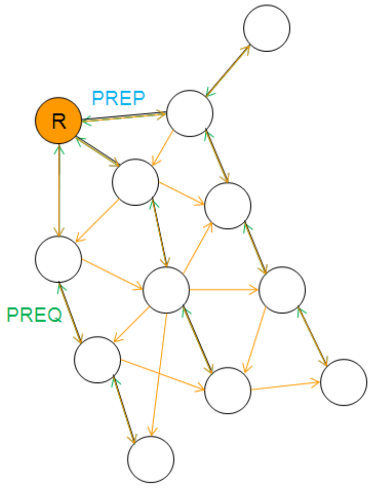


Figure 5.3 Proactive RANN mechanism

HWMP Examples [36]:

#1: No Root, Destination inside the Mesh (Figure 5.4)

MP 4 wants to communicate with MP 9

1. MP 4 first checks its local forwarding table for an active forwarding entry to MP 9

2. If no active path exists, MP 4 sends a broadcast PREQ to discover the best path to MP 9

3. MP 9 replies to the PREQ with a unicast PREP to establish a bi-directional path for data forwarding

4. MP 4 begins data communication with MP 9

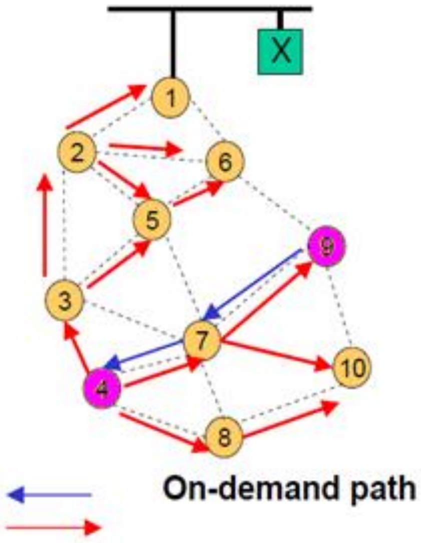


Figure 5.4 HWMP Example 1

#2: Non-Root Portal(s), Destination Outside the Mesh (Figure 5.5)

MP 4 wants to communicate with X

1. MP 4 first checks its local forwarding table for an active forwarding entry to X

2. If no active path exists, MP 4 sends a broadcast PREQ to discover the best path to X

3. When no PREP received, MP 4 assumes X is outside the mesh and sends messages destined to X to Mesh Portal(s) for interworking

– A Mesh Portal that knows X may respond with a unicast PREP

4. Mesh Portal MP 1 forwards messages to other LAN segments according to locally implemented interworking

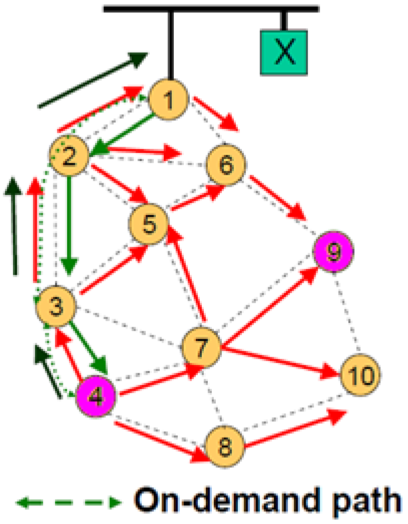


Figure 5.5 HWMP Example 2

#3: Root Portal, Destination Outside the Mesh (Figure 5.6)

MP 4 wants to communicate with X

1. MPs learns Root MP 1 through Root Announcement messages

2. 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

3. 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

4. Mesh Portal MP 1 forwards messages to other LAN segments according to locally implemented interworking

Note: No broadcast discovery required when destination is outside of the mesh

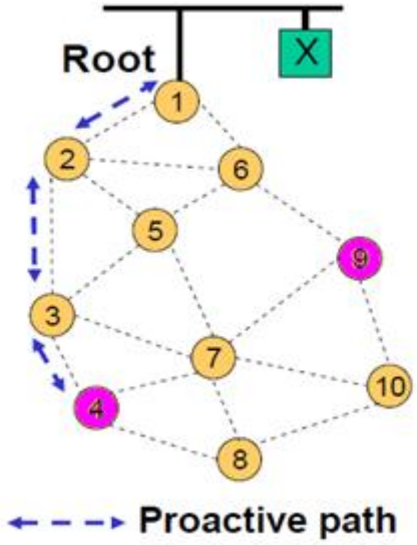


Figure 5.6 HWMP Example 3

#4: With Root, Destination Inside the Mesh (Figure 5.7)

MP 4 wants to communicate with MP 9

1. MPs learns Root MP 1 through Root Announcement messages

2. MP 4 first checks its local forwarding table for an active forwarding entry to MP 9

3. If no active path exists, MP 4 may immediately forward the message on the proactive path toward the Root MP 1

4. When MP 1 receives the message, it flags the message as “intra-mesh” and forwards on the proactive path to MP 9

5. 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

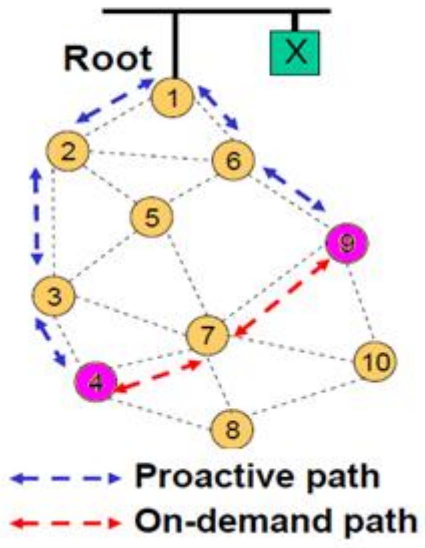


Figure 5.7 HWMP Example 4

5.4 Radio Aware – Optimized Link State Routing

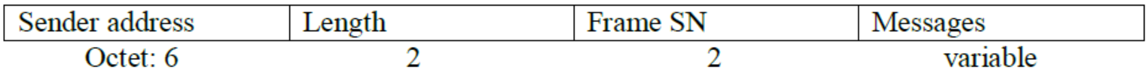
RA-OLSR is an optional path selection protocol proposed by the IEEE802.11s Task Group for WLAN mesh networking in the upcoming IEEE802.11s. It is proactive in nature and follows closely the concepts and principles of OLSR routing mechanism.

RA-OLSR is an adaptation of OLSR to operate on layer 2 using the MAC address and radio aware metric e.g. airtime link metric instead of IP address and hop count metric used for Layer 3 routing. This metric field is included in the control messages of the RA-OLSR to be able to disseminate metric information between MPs in the network [18, 25].

RA-OLSR adopts the MPR mechanism for the optimization of flooding of the control message in the network [32, 33].

RA-OLSR packet is employed in building the frame body of a mesh management frame which includes the messages. RA-OLSR packet format is shown in the table 5.6.

Table 5.6: RA-OLSR packet format

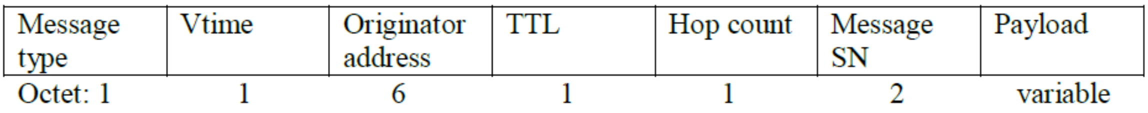


Sender address	Length	Frame SN	Messages
Octet: 6	2	2	variable

The sender address, length and the frame sequence number are referred to as message header.

The message format of RA-OLSR is given in table 5.7.

Table 5.7: RA-OLSR message format



Message type	Vtime	Originator address	TTL	Hop count	Message SN	Payload
Octet: 1	1	6	1	1	2	variable

The message format is built as follows:

1. The originator address is set to the MAC address of the source node that initiated the message

2. The message type is set as required.

3. TTL is set to the maximum number the message is to be retransmitted which must be decremented by 1 before retransmission.

4. Hop count determines the number of hops the message has gone which is incremented by 1 before retransmission.

5. The message sequence number is set to the originator node SN which enhances unique identification of each message in the network.

Multi Point Relay (MPR)

Proactive routing protocol is known for continuous maintenance of route to all participating MPs in the network by frequent flooding of topology information across the network.

MPR is one basic concept of the RA-OLSR for the optimization of the flooding of the topology information. This approach significantly reduces the flooding problem. Each MP selects 1-hop symmetric neighbor that can at least forward message to 2-hop symmetric neighbor. This reduces the number of MP to retransmit message in the network.

MPR mechanism reduces the routing overhead in the network, the smaller the MPR set the lower the overhead as shown in Figure 5.8.

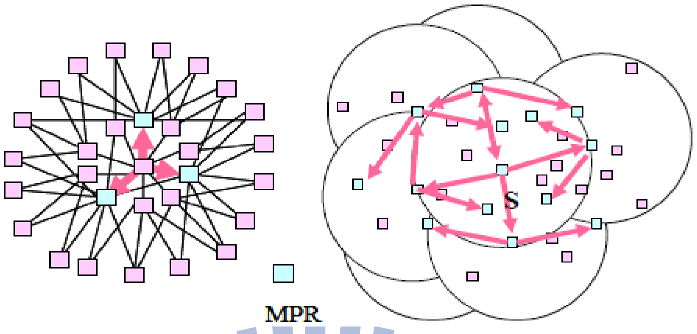


Figure 5.8 MPR

5.5 Routing Metric: Airtime Link Metric

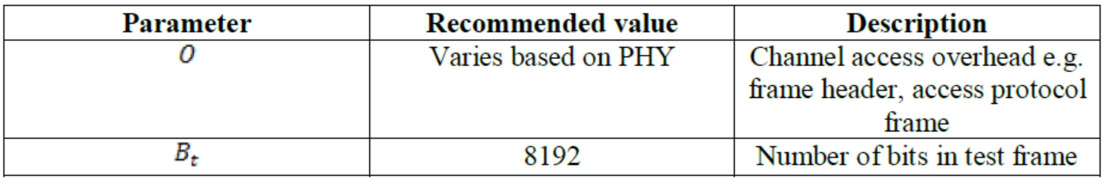
This is the default radio aware metric defined by the IEEE802.11s TG for interoperability of WLAN mesh network devices. It is used together with path selection protocol in building paths between MPs at the data link. The extensible mesh routing framework permits flexible implementation with different path selection metric as specified by the active profile on each MP beacon.

Airtime link metric gives the cost of the of channel resources consumed while transmitting frame over a particular wireless link. The airtime cost for each link can be evaluated as:

$$c_a = \left[O + \frac{B_t}{r} \right] \frac{1}{1-e_f}$$

Where channel access overhead O and the size of the test frame B_t, are constant based on 802.11 modulation type used. The rate r in Mb/s is the data rate at which MP would transmit frame of size B_t according to current conditions of the radio environment, and the frame error e_f is the probability that the transmitted frame of size B_t at the current transmission bit rate r is corrupted due to transmission error. the draft standard presented the airtime cost constant which is shown in Table 5.8.

Table 5.8: Airtime cost constant



Parameter	Recommended value	Description
O	Varies based on PHY	Channel access overhead e.g. frame header, access protocol frame
B_t	8192	Number of bits in test frame

Conclusions

- IEEE 802.11s is new standard to support WMNs to improve its performance.

- As we see there are many issues still not that clear on this standard and a lot of research going on these days to make this is official standard.

- There many things in this standard as optional strategies as in MAC or routing it make you asking why to have something like that.

- We focus on this study on MAC and routing protocol and we plan to continue our research by simulate everything and try to notice the performance, throughout, delay, traffic load and other issues.

References

[1] I. F. Akyildiz and X. Wang, "Wireless Mesh Networks", John Wiley & Sons Ltd, 2009.

[2] G. Held, "Wireless Mesh Networks", Taylor & Francis Group, 2005.

[3] Y. Zhang, J. Luo, and H. Hu, "WIRELESS MESH NETWORKING: Architectures, Protocols and Standards", Taylor & Francis Group, 2007.

[4] S. Misra, S. C. Misra, and I. Woungang, "Guide to Wireless Mesh Networks", Springer-Verlag London Limited, 2009.

[5] E. Hossain and K. Leung, "Wireless Mesh Networks: Architectures and Protocols", Springer Science+Business Media, 2008.

[6] B. H. Walke, S. Mangold, and L. Berlemann, "IEEE 802 Wireless Systems", John Wiley & Sons Ltd, 2006.

[7] A. R. Prasad and N. R. Prasad, "802.11 WLANs and IP Networking", Artech House, 2005.

[8] Y. Xiao and Y. Pan, "Emerging Wireless LANs, Wireless PANs, and Wireless MANs", John Wiley & Sons, Inc., Hoboken, New Jersey, 2009.

[9] I. F. Akyildiz and X. Wang, "A Survey on Wireless Mesh Networks", IEEE Communications Magazine, vol. 43, no. 9, pp. S23–S30, Sep. 2005.

[10] IEEE P802.11s/initial proposal, "Joint SEE-Mesh/Wi-Mesh Proposal to IEEE 802.11 TGs", Feb. 2006.

[11] IEEE P802.11s/D1.0, "Draft Amendment to Standard IEEE 802.11TM: ESS Mesh Networking", Nov. 2006.

[12] IEEE P802.11s/D2.0, "IEEE P802.11/D2.0, Draft Standard, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer

(PHY) specifications, Amendment 10: Mesh Networking", Sep. 2008.

[13] IEEE P802.11s/D3.0, "Draft Amendment to Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment 10: Mesh Networking", Mar. 2009.

[14] IEEE P802.11s/D4.0, "Draft Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 10: Mesh Networking", Dec. 2009.

[15] IEEE P802.11s/D5.0, "IEEE Draft Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications-Amendment 10: Mesh Networking", Jun. 2010.

[16] I. Alocci, S. Murphy, A. Nafaa, and J. Murphy, "Development of an IEEE 802.11s Simulation Model for QualNet", NAEC2008/ATSMA conference In Riva del Garda, Italy, 25th-28th of Sep. 2008.

[17] M. J. Lee, J. Zheng, Y. Ko, and D. M. Shrestha, "Emerging Standards for Wireless Mesh Technology", IEEE Wireless Communications, Apr. 2006.

[18] E. K. O. Nwup and I. A. Akande, "Evaluation of the pre IEEE 802.11s RFC", Blekinge Institute of Technology, Jun. 2009.

[19] G. R. Hiertz, S. Max, Y. Zang, T. Junge, and D. Denteneert, "IEEE 802.11 s MAC Fundamentals", IEEE conference, 2007.

[20] G.R. Hiertz, S. Max, T.Junge, D. Denteneert, and L. Berlemann, "IEEE802.11s-Mesh Deterministic Access" 14th European Wireless Conference, EW 2008, pp.1-8, 22-25 Jun. 2008.

[21] G. R. HIERTZ, S. MAX, R. TAORI, J. CARDONA, L. BERLEMANN, and B. WALKE, "IEEE 802.11S: THE WLAN MESH STANDARD", IEEE Wireless Communications, Feb. 2010.

[22] H Aoki, S Takeda, and K Yagyu, "IEEE 802.11s Wireless LAN Mesh Network Technology", NTT DoCoMo Technical, 2006.

[23] A. Daniilidis and K. Khalid, "IEEE 802.11s Wireless Mesh Networks", Department of Communication System, Lund University, Sweden.

[24] A. Sgora, D.D. Vergados, and P. Chatzimisios, "IEEE 802.11s Wireless Mesh Networks: Challenges and Perspectives", ICST Institute for Computer Sciences, Social-Informatics and Telecommunication Engineering, 2009.

[25] X. Wang and A. O. Lim, "IEEE 802.11s wireless mesh networks: Framework and challenges", Ad Hoc Networks, 2008.

[26] G. R. Hiertz, Y. Zang, S. Max, T. Junge, E. Weiss, and B. Wolz, "IEEE 802.11s: WLAN Mesh Standardization and High Performance Extensions", IEEE Network, May. 2008.

[27] R. Zhao, "Mesh Distributed Coordination Function for Efficient Wireless Mesh Networks Supporting QoS", Apr. 2007.

[28] R. G. Garroppo, S. Giordano, D. Iacono, and L. Tavanti, "Notes on implementing a IEEE 802.11s Mesh Point", 2008.

[29] R. G. Garroppo, S. Giordano, D. Iacono, and L. Tavanti, "On the development of a IEEE 802.11s Mesh Point prototype", Mar., 2008.

[30] G.R. Hiertz, S. Max, R. Zhao, D. Denteneert, L. Berlemann, "Principles of IEEE 802.11s" in proceedings of 16th International

Conference on Computer Communications and Networks, Honolulu Hawaii, pp.1002-1007, Aug. 2007.

[31] M. Bahr, “Proposed routing for IEEE 802.11s WLAN mesh networks” 2nd International Wireless Internet Conference (WiCON), Boston, MA, USA, Aug. 2006.

[32] J. D. Camp and E. W. Knightly, “The IEEE 802.11s Extended Service Set Mesh Networking Standard”, IEEE Communications Magazine, 2008.

[33] M. Bahr, “Update on the Hybrid Wireless Mesh Protocol of IEEE 802.11s”, IEEE Conference on Mobile Adhoc and Sensor, 2007.

[34] D. Cheung, “WLAN Mesh Architectures and IEEE 802.11s”, Annual review of communications, 2006.

[35] Y. Ko, “A Brief Overview on IEEE 802.11s”, Dept of Info & Computer Engineering, Ajou Univ. Korea.

[36] W. S. Conner, J. Kruys, K. Kim, and J. C. Zuniga, “IEEE 802.11s Tutorial”, IEEE 802 Plenary, Dallas, Nov. 2006.