

Broadband Wireless for Rural Areas --

WiFiRe: Medium Access Control (MAC) and Physical Layer (PHY) Specifications

Release 2006

(This document is - Aug 2006 draft)

Center of Excellence in Wireless Technology (CEWiT)



About CEWiT

The Centre of Excellence in Wireless Technology (CEWiT), India, has been set up under a public-private initiative with the mission of making India a leader in the research, development and deployment of wireless technology. It is an autonomous institution temporarily headquartered at IIT Madras.

Broadband wireless technology has great potential in the coming years. Emerging standards can be leveraged to build a system that specifically meets India's broadband access needs. CEWiT will play a pro-active role in engaging with academic and industry research groups in India to focus research on areas with strong potential. CEWiT will also foster collaboration with similar efforts worldwide. CEWiT seeks to actively participate in International standards bodies, and to assist government and public institutions in policy-making, spectrum management and regulation.

CEWiT Std, WiFiRe, 2006 Edition

CEWiT standards are developed within the Technical Committees of CEWiT. Members of the committees serve voluntarily and without any compensation. The standards developed within CEWiT represent a consensus of the broad expertise of the subject. The existence of a CEWiT standard does not imply that there are no other ways to provide services related to the scope of the standard. Furthermore, a standard is subject to change brought about through developments in the state of the art and comments received from the users of the standard. Users should check that they have the latest edition of any CEWiT standard. These may be obtained from <http://www.cewit.org.in/>

Comments on standards and requests for interpretations relating to specific applications should be addressed to:
Secretary, Center of Excellence in Wireless Technology
CSD152 (ESB)
Indian Institute of Technology Madras
Chennai – 600 036, INDIA
email: feedback@cewit.org.in

The distribution and usage of this Standard are as per the Creative Commons license – Attribution-Share Alike. See <http://creativecommons.org/licenses/by-sa/2.5/> for details. A brief excerpt from the license is given below.

You are free:

- to copy, distribute, display, and perform the work
- to make derivative works
- to make commercial use of the work

Under the following conditions:



Attribution. You must attribute the work in the manner specified by the author or licensor.



Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under a license identical to this one.

- Any of these conditions can be waived if you get permission from the copyright holder.

CEWiT Std, WiFiRe, 2006 Edition

Abstract:

WiFiRe stands for **WiFi – Rural extension**. It seeks to leverage the license free nature of the WiFi spectrum (IEEE 802.11b, 2.4 GHz Band) and the easy availability of WiFi RF chipsets, in order to provide long-range communications (15-20 Kms) for rural areas. The key idea in WiFiRe is to replace the 802.11b MAC mechanisms (DCF/PCF), with something more suitable for long-range communication, while continuing to use the 802.11b PHY support. WiFiRe is meant for a star topology - a Base Station (BS) at the fiber Point of Presence (PoP) and Subscriber Terminals (ST) in the surrounding villages – with sectorized antennas at the BS and a directional antenna at each ST. The WiFiRe MAC is time-division duplex (TDD) over a single 802.11b channel along with a multi-sector TDM mechanism.

This document specifies the details of WiFiRe, including services provided to the higher layers, the message formats and sequences, the protocol description and various timings involved. WiFiRe capacity analysis, scheduler design and simulation analysis are also provided as annexure.

Authors:

Sridhar Iyer (IIT Bombay), **Krishna Paul** (IIT Bombay)¹, **Anurag Kumar** (IISc Bangalore) and **Bhaskar Ramamurthi** (IIT Madras).

Contributors:

Person	Contribution
Ashok Jhunjhunwala, IIT Madras	Conceptualization
Bhaskaran Raman, IIT Kanpur	Management sub-procedures
Anirudha Sahoo, IIT Bombay	Data transport sub-procedures
Om Damani, IIT Bombay	Security sub-procedures
Anitha Varghese, IISc Bangalore	Capacity analysis and scheduler design
Anirudha Bodhankar, IIT Bombay	Simulation model and analysis
Alok Madhukar, IIT Bombay	Data flow and state transition diagrams
Anand Kannan, CEWiT ²	Initial concept document

¹ Krishna Paul was with IIT Bombay when this work was initiated. She joined Intel, Bangalore, towards the end of this work.

² Anand Kannan is now with Valued Epistemics (Pvt) Ltd., Chennai

Reviewers:

The following is a tentative list of reviewers for the draft version of this release:

(The final list of reviewers will include all those who return detailed comments)

Uday Desai, IIT Bombay	Pravin Bhagwat, AirTight Networks
Abhay Karandikar, IIT Bombay	Rajeev Shorey, GM R&D
Vishal Sharma, IIT Bombay	Rajiv Rastogi, Bell Labs
Ashwin Gumaste, IIT Bombay	Vijay Raisinghani, TCS
Varsha Apte, IIT Bombay	
S. Krishna, IIT Bombay	David Koilpillai, IIT Madras
Srinath Perur, IIT Bombay	Rajesh Sundaresan, IISc Bangalore
Raghuraman Rangarajan, IIT Bombay	Kameshwari Chebrolu, IIT Kanpur

Acknowledgements:

The following persons contributed to the discussions and/or other supporting activities:

Pavan Kumar, IIT Kanpur	Pratik Sinha, Zazu Networks
Narasimha Puli Reddy, IIT Kanpur	
Klutto Milleth, CEWiT	K. Giridhar, IIT Madras

Contents

1	OVERVIEW	7
1.1	BACKGROUND	7
1.2	DEPLOYMENT SCENARIO	8
1.3	TECHNOLOGY ALTERNATIVES	8
1.4	WiFiRE APPROACH	10
1.5	SCOPE	12
2	GENERAL DESCRIPTION	14
2.1	DEFINITIONS AND ABBREVIATIONS	14
2.2	DESIGN DRIVERS AND ASSUMPTIONS	14
2.3	WiFiRE SYSTEM ARCHITECTURE	15
2.4	NETWORK INITIALIZATION	17
2.5	IMPACT OF SECTORIZATION	18
2.6	MAC PROTOCOL OVERVIEW	20
2.7	MAC SERVICES	21
2.8	MAC SERVICE INTERFACES	23
2.9	TYPICAL FRAME AND SLOT TIMINGS	23
2.10	RANGING AND POWER CONTROL	26
2.11	PDU FORMATS	27
2.12	BS SCHEDULER FUNCTIONS	28
2.13	SUPPORT FOR MULTIPLE OPERATORS	28
2.14	SUMMARY OF PROTOCOL STEPS	29
3	MAC SERVICE DEFINITION	31
3.1	SERVICE SPECIFIC SUB-LAYER (SSS)	31
3.2	LINK SPECIFIC SUB-LAYER (LCS)	35
3.3	DETAILED DESCRIPTION OF SERVICE PRIMITIVES	39
4	MAC DETAILED DESCRIPTION	47
4.1	ADDRESSING AND CONNECTION IDENTIFICATION	47
4.2	BANDWIDTH REQUEST GRANT SERVICE	48
4.3	MAC PDU FORMAT	50
4.4	MAC HEADER FORMAT	50
4.5	MAC MANAGEMENT PDU(S)	52

- 4.6 MAC DATA PDU(S) 53
- 4.7 NETWORK INITIALIZATION SUB-PROCEDURES 54
- 4.8 CONNECTION MANAGEMENT SUB-PROCEDURES 61
- 4.9 DATA TRANSPORT SUB-PROCEDURES 64
- 4.10 PROTOCOL SUMMARY: STATE-TRANSITION DIAGRAMS 64
- 5 AUTHENTICATION AND PRIVACY 70**
- 6 MAC MANAGEMENT 70**
- 7 PHY SERVICE SPECIFICATION AND MANAGEMENT 70**
- 8 GLOSSARY OF TERMS 71**
 - 8.1 ABBREVIATIONS AND ACRONYMS 71
 - 8.2 DEFINITIONS 73
- A. ANNEX A: DESIGN DRIVERS 75**
- B. ANNEX B: CAPACITY ANALYSIS 82**
- C. ANNEX C: SCHEDULER DESIGN 91**
- D. ANNEX D: SIMULATION ANALYSIS 100**
- E. BIBLIOGRAPHY 110**

WiFiRe: Medium Access Control (MAC) and Physical Layer (PHY) Specifications

1 OVERVIEW

1.1 Background

About 70% of India's population, or 750 million, live in its 600,000 villages, and around 85% of these villages are in the plains. The average village has 250-300 households, and occupies an area of 5 sq. km. Most of this is farmland, and typically the houses are in one or two clusters. Villages are thus spaced 2-3 km apart, and spread out in all directions from the market centers. The market centers are typically spaced 30-40 km apart. Each such center serves around 250-300 villages, in a radius of about 20 km [1], as shown in Figure 1.

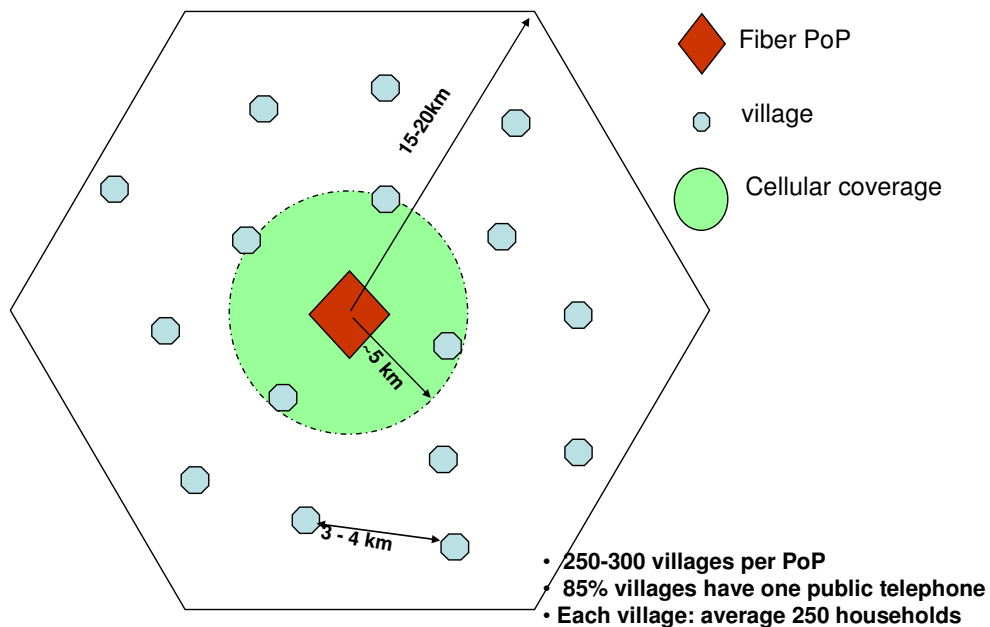


Figure 1: Background

The telecommunication backbone network, passing through all these centers, is new and of high quality optical fiber. The base stations of the mobile (cellular) operations are also networked using optical fiber.

However, the solid telecom backbone ends abruptly at the towns and larger villages. Beyond that, cellular coverage extends mobile telephone connectivity only up to a radius of 5 km, and then telecommunications services peter out. Fixed wireless telephones have been provided in tens of thousands of villages, but the telecommunications challenge in rural India remains the “last ten miles”. This is particularly true if the scope includes broadband Internet access.

The Telecom Regulatory Authority of India has defined broadband services as those provided with a minimum data rate of 256 kbps [2]. Assuming a single kiosk (end-point) in each village, generating sustained 256 kbps flows, 300 kiosks will generate traffic of the order of 75 Mbps. This is a non-trivial amount of traffic to be carried over the air, per base station, even with a spectrum allocation of 20 MHz.

1.2 Deployment Scenario

Given the need to cover a radius of 15-20 km from the fiber point-of-presence (PoP), a broadband wireless system will require a system gain of at least 150 dB. The *system gain* is a measure of the link budget available for overcoming propagation and penetration (through foliage and buildings) losses while still guaranteeing system performance. This may be achieved using Base Station towers of 40 m height, at the PoP, and a roof-top antenna of 10 m height at each Subscriber end (kiosk), with line-of-sight deployment. A subscriber kiosk may also be installed in a vehicle, which may be stationed at different villages over a period of time.

A more detailed discussion on the background and deployment considerations is given in Annex A.

1.3 Technology Alternatives

Technical reviews of current wireless broadband technologies and their evaluations are given in [1,3]. A summary is as follows:

- Present day mobile cellular technologies (such as GSM [4], GPRS [5], CDMA [6]) may meet the cost targets but are unlikely to be able to provide broadband services as defined above.
- Proprietary broadband technologies (such as iBurst [7], Flash-OFDM [8]) meet many of the performance requirements, but typically have low volumes and high costs. The indigenously-developed Broadband corDECT technology [9] of Midas Communication Technologies, Chennai is a fixed-access wireless broadband system that meets the performance and cost requirements.
- WiMAX-d (IEEE 802.16d) [10], is a new standards-based technology for fixed wireless-access that meets the performance requirements, but not the cost targets, because of low adoption rate and volume. WiMAX-e (IEEE 802.16e) [10] is a mobile evolution of the standard, which may see

sufficient adoption beginning 2008 to generate high volume and drive down the cost. If this happens, it is likely to be a technology that meets performance and cost requirements. However, it will take some years for the costs to drop to levels viable for rural deployment.

- WiFi (IEEE 802.11b) [11], is an inexpensive local-area broadband technology. It can provide 256 kbps or more to tens of subscribers simultaneously, but can normally do so only over short distances (less than 50 m indoors). One attraction of WiFi technology is the de-licensing of its spectrum in many countries, including India. Another is the availability of low-cost WiFi chipsets. In rural areas, where the spectrum is hardly used, WiFi is an attractive option, provided its limitations when used over a wide-area are overcome. Various experiments with off-the-shelf equipment have demonstrated the feasibility of using WiFi for long-distance rural point-to-point links [12]. The main issue is that WiFi typically uses a Carrier Sense Multiple Access (CSMA) protocol, which is suited only for a LAN deployment. Further, the Distributed Coordination Function (DCF) mechanism does not provide any delay guarantees, while the Point Coordination Function (PCF) mechanism becomes inefficient with increase in number of stations [13]. When off-the-shelf WiFi equipment is used to set up a wide-area network, medium access (MAC) efficiency becomes very poor, and spectrum cannot be re-used efficiently even in opposite sectors, of a base station. One solution for this problem is to replace the MAC protocol with one more suited to wide-area deployment. This will have to be crafted carefully such that a low-cost WiFi chipset can still be used, while bypassing the in-built WiFi MAC. The alternative MAC can be implemented on a separate general-purpose processor with only a modest increase in cost.

WiFiRe, as defined herewith, is one such alternative MAC designed to leverage the low cost of WiFi technology for providing fixed wireless access. It is a Time Division Duplex (TDD) communication protocol over a single WiFi channel, along with a multi-sector Time Division Multiplex (TDM) mechanism. This is explained in the next section.

There are existing commercial products which support long-distance WiFi links [14,15,16,17]. Some of these products are for point-to-point links and others are for point-to-multipoint links. While the protocol used by such products is proprietary, they are likely to be based on some kind of Time Division Multiple Access (TDMA) mechanism. This is supported by the fact that some of these products allow a network operator to flexibly split the available bandwidth among various clients in a point-to-multipoint setting.

WiFiRe has the following advantages over such products:

- WiFiRe is an *open standard*, whereas the above products involve proprietary protocols which are non-interoperable. The non-interoperability also implies that the *cost* of such products is likely to be higher than standards based products.
- Related to the above, the performance of WiFiRe is more predictable and understandable than that

of the proprietary commercial products. This is especially important for large scale deployments.

- All of the commercial products above consider only a single sector operation (single point-to-multipoint link). WiFiRe is designed for higher spectral reuse through multiple carefully planned sectors of operation. Such reuse is estimated to achieve 3-4 times higher throughput performance. With WiFiRe, it is estimated that one can support about 25 Mbps (uplink + downlink) per cell, using a single WiFi carrier at 11 Mbps service. This would be sufficient for about 100 villages in a 15 km radius.

1.4 WiFiRe Approach

WiFiRe stands for **WiFi – Rural extension**. The main design goal of WiFiRe is to enable the development of low-cost hardware and network operations for outdoor communications in a rural scenario. This has two implications: (i) a WiFiRe system avoids frequency licensing costs by operating in the unlicensed 2.4 GHz frequency band, and (ii) WiFiRe uses the WiFi (IEEE 802.11b) physical layer (PHY), due to the low cost and easy availability of WiFi chipsets.

WiFiRe requires a 40 m tower at the base station (BS) near the fiber PoP (point-of-presence) and 10-12 m poles at the subscriber terminals (ST), in order to maintain the desired system gain of about 150 dB. The network configuration is a star topology, as shown in Figure 2.

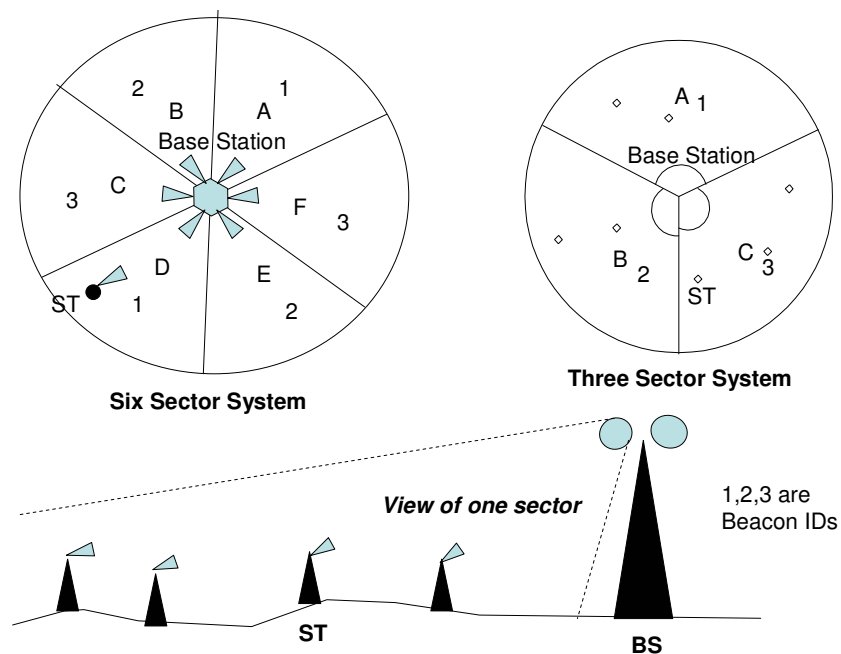


Figure 2: WiFiRe Network Configuration

One base station (BS), using a single IEEE 802.11b channel, will serve a cell with about 100-120 villages spread over a 15 Km radius. The cell will be sectorized, with each sector containing a sectorized BS antenna. Two example configurations: (i) six sectors of 60 degrees each and (ii) three sectors of 120 degrees each, are shown in Figure 2. There will be one fixed subscriber terminal (ST) in each village, which could be connected to voice and data terminals in the village by a local area network. All ST(s) in a sector will associate with the BS antenna serving that sector. The ST antennas will be directional. While permitting reliable communication with the serving BS, this limits interference to/from other co-located BSs, and more importantly, to/from BSs belonging to adjacent cells.

However, because of antenna side-lobes, transmitters in each sector may interfere with receivers in other sectors. Thus, depending on the attenuation levels, a scheduled transmission in one sector may exclude the simultaneous scheduling of certain transmitter-receiver pairs in other sectors. Further, simultaneous transmissions will interfere, necessitating a limit on the number of simultaneous transmissions possible. This is explained further in section 2.5.

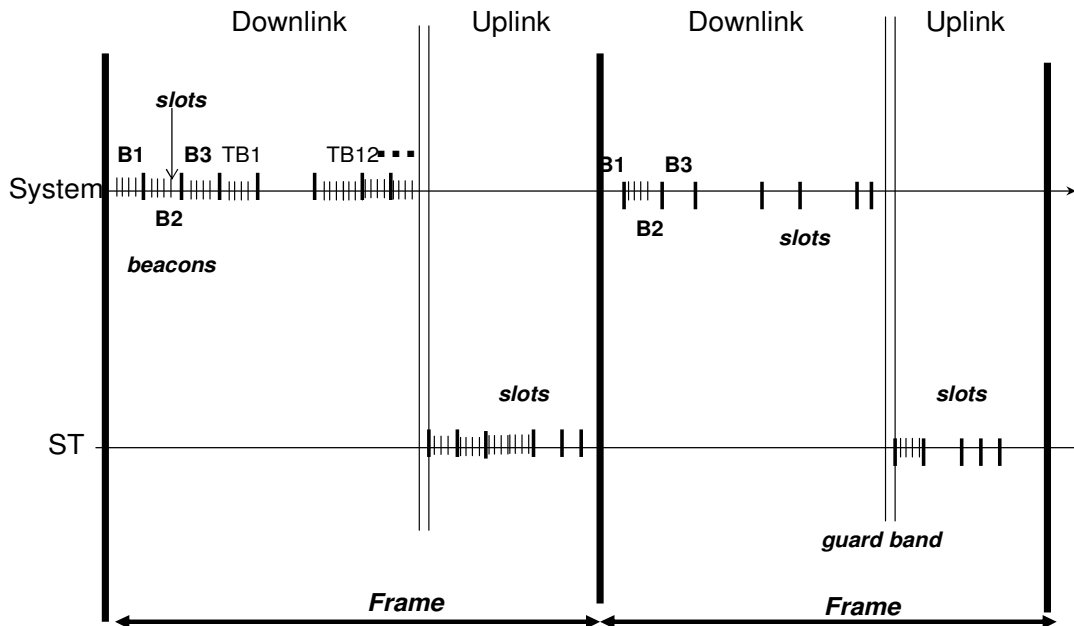
As a result, WiFiRe has one medium access (MAC) controller for all the sectors in a BS, to co-ordinate the medium access among them. The multiple access mechanism is time division duplexed, multi-sector TDM (TDD-MSTDM) scheduling of slots. As shown in Figure 3, time is divided into frames. Each frame is further partitioned into a downlink (DL) and an uplink (UL) segment, which need not be of equal durations. Within each segment there are multiple slots, of equal duration each. In each DL slot, one or zero transmissions can take place in each sector. Multiple BS antennas (for different sectors) may simultaneously transmit a packet to their respective ST(s), provided they do so in a non-interfering manner. Similarly, in each UL slot, multiple ST(s) (from different sectors) may simultaneously transmit a packet to the BS, provided they do so in a non-interfering manner.

Beacons are transmitted at the start of each DL segment. The beacon for each sector contains information for time synchronization of the ST(s) in that sector, information regarding the DL and UL slot allocations (DL-MAP, UL-MAP) for that frame, and other control information. Due to site and installation dependent path loss patterns, and time varying traffic requirements, the MAP(s) need to be computed on-line.

In order to ensure that the beacons get through to the ST(s) even under poor channel conditions, the beacons are transmitted at a lower rate (2 Mbps) than the data packets. In case of a three-sector system, the beacon for each sector is transmitted one after another, to ensure that they do not interfere. In case of a six-sector system, opposite sectors may transmit their beacons simultaneously. The order of transmission of the beacons is indicated by the numbers in Figure 2.

Note that having a 3-sector separation between beacons that are transmitted simultaneously is a conservative action. However, this is recommended since the front-to-back attenuation ratio of antenna

lobes is more reliable than that of side-lobes. For subsequent data transmission, alternate sectors may transmit simultaneously, based on the interference matrix. This is explained in detail, along with a capacity analysis, in Annex B. A further general description of WiFiRe is given in section 2.



B1, B2, B3 – Beacons; contain MAP(s) on DL and UL allocation.
 TB - Transmit Block; can be of unequal durations. Slots are of equal duration.

Figure 3: WiFiRe Multiple Access Mechanism

1.5 Scope

The scope of this standard is to develop a medium access control (MAC) and Physical layer (PHY) specification for WiFiRe broadband wireless connectivity for fixed stations within a rural area. In this context, a rural area is characterized by the presence of optical-fiber point-of-presence (PoP) within 15-20 km of most villages and fairly homogenous distribution of about 100-120 villages around each PoP, in the plains. The network configuration is a star topology with sectorized Base Station (BS) antennas on a tower at the PoP and a directional Subscriber Terminal (ST) antenna at each village kiosk.

Specifically, this standard

- Describes functions and services required for a WiFiRe compliant device to operate in the network.
- Defines the MAC procedures and protocols to support the data delivery services.
- Specifies the various aspects of the WiFi PHY being used.

The reference model for the layers and sub-layers of this standard are shown in Figure 4.

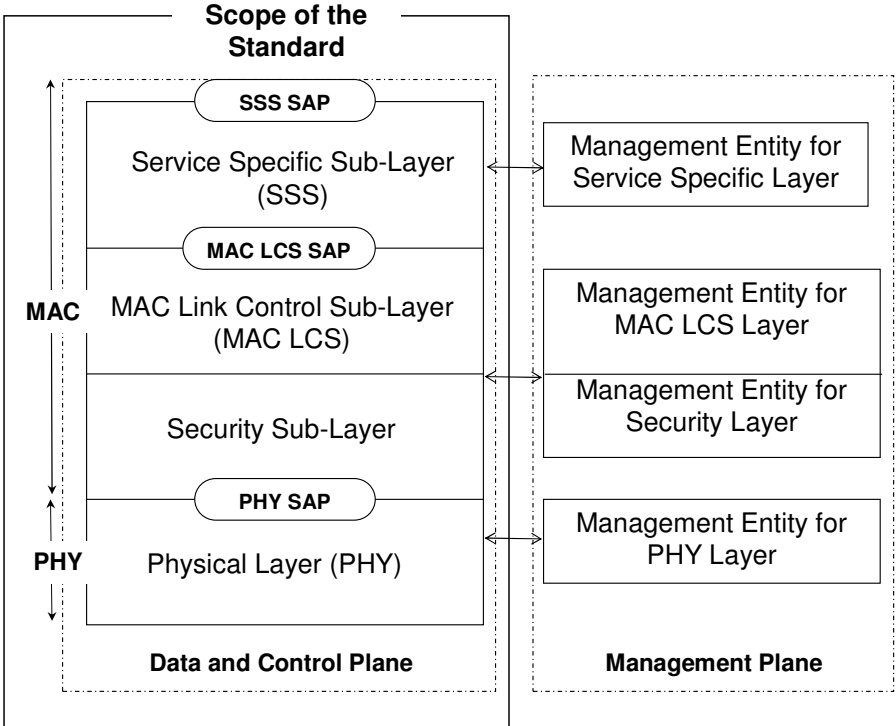


Figure 4: WiFiRe Reference Model showing the service interfaces and the scope of the standard

2 GENERAL DESCRIPTION

A WiFiRe system is one approach to design a *long-range and low-cost* fixed wireless communication network. The WiFiRe physical layer (PHY) directly employs the low-cost WiFi PHY (IEEE 802.11b, Direct Sequence Spread Spectrum). The WiFi PHY is for operation in the 2.4 GHz band and designed for a wireless local area network (LAN) with 1 Mbps, 2 Mbps and 11 Mbps data payload communication capability. It has a processing gain of at least 10 dB and uses different base-band modulations to provide the various data rates, with a typical reach of about 100 meters. WiFiRe extends the transmission range of the WiFi PHY to 15-20 Kilometers, by using a deployment strategy based on sectorized and directional antennas and line-of-sight communication.

The WiFiRe medium access control layer (MAC) replaces the WiFi MAC (IEEE 802.11b, Distributed Coordination Function) with a mechanism more suited to wide-area deployment, in terms of providing efficient access and service guarantees. The MAC is time division duplexed, multi-sector TDM (TDD-MSTDM), as described subsequently. The WiFiRe MAC is conceptually similar to the WiMax MAC (IEEE 802.16) in some respects.

2.1 Definitions and abbreviations

The various terms and abbreviations in this document are defined at the first point of their use. They are also provided collectively in the form of a glossary in section 8, for quick reference.

2.2 Design drivers and assumptions

The key design drivers for WiFiRe are as follows:

- The existence of a fiber point of presence (PoP) every 25 km or so in rural India, for backbone connectivity.
- The availability of unlicensed or free spectrum in the 2.4 GHz band.
- The low cost of WiFi chipsets. Most WiFi chipsets are designed so that the PHY and MAC layers are separate. Thus it is possible to change the MAC, or in the least, bypass it, while retaining the same PHY.
- The link margins for WiFi PHY being quite adequate for line-of-sight outdoor communication in flat terrain for 15-20 Km range.
- It being possible to have high efficiency outdoor systems, providing application service guarantees, without significantly changing radio costs. This is done by retaining the same PHY but changing the MAC, sectorization and antenna design choices and tower/site planning.

- Base Station towers of 40 m height and fixed Subscriber Terminal antennas of 10-12 m height being sufficient to cover a radius of 15-20 km from the fiber PoP for 85% of the area in rural India. This configuration can provide the required system gain with line-of-sight deployment.

The key assumptions in WiFiRe are as follows:

- The wireless links in the system are fixed, single hop, with a star topology. *Handling of mobile nodes, multi-hop wireless links and other topologies are deferred to a later release.*
- There is a fixed carrier frequency f_c and the WiFi radios are operating at 11 Mbps, except for PHY synchronization and certain control packets which may be sent at 2 Mbps.
- About 20 MHz (1 carrier) of conditionally licensed spectrum is available for niche/rural areas. The spectrum mask, power level and carrier location exactly match those for WiFi (IEEE 802.11b).
- All nodes in the system are operated by a single operator who also owns the conditional license.
- Multiple operators will use different carriers and will synchronize out-of-band, to avoid interference.
- The PHY overhead is 192 microseconds for 1 Mbps and 96 microseconds for 2 Mbps and 11 Mbps.
- No meaningful higher layer information can be sent using the PHY overhead.
- There are no multi-path issues due to the deployment topology and the line-of-sight design.
- All the transmissions in a cell (set of co-located BS) are controlled by a single scheduler.
- All systems in adjacent cells belonging to the same operator use the same frequency, and do not interfere significantly with each other. This is made possible by the use of directional antennas at the Subscriber Terminals.
- The various components in the system have unique IP addresses.
- A single voice over IP (VoIP) packet is approximately 40 bytes. For active connections, VoIP packets are generated periodically, once in 20 milliseconds. This implies the use of a codec such as G.729, having a sampling rate of 8 Kbps. A codec such as G.711 has a sampling rate of 64 Kbps as it includes provisions for modems etc. This is not required in WiFiRe.

A more detailed discussion of the design drivers and assumptions is given in Annex A.

2.3 WiFiRe system architecture

The WiFiRe system architecture consists of several components that interact to provide a wireless wide area network (WAN) connectivity. In order to operate outdoors with a reach of 15-20 Kilometers, using the Direct Sequence Spread Spectrum (DSSS) based 802.11b PHY, WiFiRe adopts a star network topology using directional antennas with (i) appropriate transmission power and (ii) adequate height of transmitter and receiver, for Line of Sight (LoS) connectivity.

As shown in Figure 2, a WiFiRe system consist of a set of sectorized antennas at the base station (BS), mounted on a transmission tower with a height of 40 meters and directional antennas at the subscribers terminals (ST), mounted on poles with height of around 10 meters. Typically a system is designed to cover an approximately circular area with radius of 15-20 Kms, around the tower. This area is called as a *Cell*. WiFiRe supports a link layer providing long-haul reliable connection, with service guarantees to real time and non real time data applications.

As shown in Figure 5, the key components of the WiFiRe architecture are:

- **System** (S) is a set of co-located BS (typically, six) each with a sectorized antenna, mounted atop a tower with elevation of around 40 meters, providing coverage to a cell of radius around 15-20 Km. All the transmissions in a System are coordinated by a single scheduler.
- **Base Station** (BS) of a system 'S' is radio transceiver having the electronics for WiFi (IEEE 802.11b) physical layer. A WiFiRe BS uses a sectorized antenna, with a triangular coverage area; the exact shape of the coverage area depends on the design of the antenna and transmission power. The impact of sectorization is discussed in section 2.5.
- **Subscriber Terminal** (ST) is the user premise network equipment. An ST has a directional antenna, and it is pointed towards a System 'S'. The system S is determined at the time of deployment and fixed thereafter. Appropriate initialization, ranging and registration are required to ensure that a ST can communicate with one and only one BS of system S. This is discussed in section 2.6.
- **User Equipment** (UE) is a user devices that connect to ST. UE(s) are source and sink of user data. WiFiRe does not specify the nature of the network media between ST and UE. They may be wired or wireless links. The service interfaces at ST provide a list services to UE(s). This is discussed in section 2.7.

The BS is connected to the external world (Internet) through the fiber PoP, while the ST is connected to voice and data terminals, through a local area network.

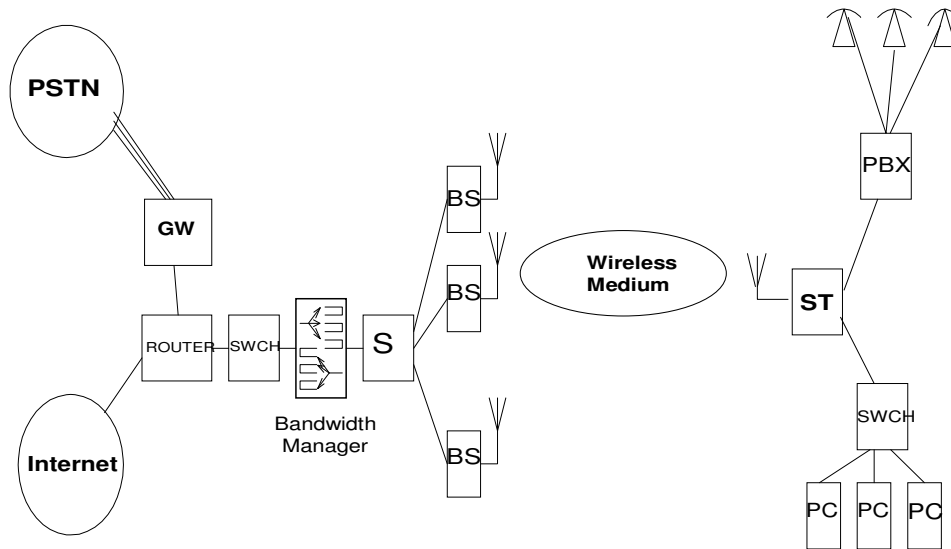


Figure 5: WiFiRe system architecture

2.4 Network initialization

The association between a ST and a System S is static. This is determined by configuration at the ST, during deployment. It is possible that a ST may hear more than one system or more than one BS of a system, depending on spatial planning of the system deployment. Appropriate topological planning and orientation of the ST directional antenna is required to ensure that a ST communicates with one and only one system S.

The association of a ST with a BS in a system S, is dynamic and can change during each ‘power-on’ scenario of the ST. Appropriate initialization, ranging and registration are required to ensure that a ST communicates with one and only one BS of system S. This association depends on antenna gain and other selection factors. Once this association is performed, it is fixed as long as the ST remains in ‘power-on’ mode. This is described in more detail in section 4.7.

The impact of inter-cell interference caused by neighborhood system at a ST (a common issue in cellular systems) is considered minimal since the ST directional antenna is locked onto one system and BS at the time of deployment and initialization, respectively.

2.5 Impact of sectorization

All BS in a system, use the same WiFi channel (single carrier) for communication with their respective STs. This is unlike typical sectorized deployments, in which co-located sectors use separate frequency channels. In WiFiRe all the sectors in a multiple antenna configuration continue to use the same frequency channel. As a result, transmission by one BS may interfere with adjacent sectors. An ST may hear transmission from more than one BS of a system S. An ST may or may not be able receive the transmission from its BS, depending on interference caused by the neighboring sector BS. Also, transmitters in one sector may interfere significantly with receivers in other sectors, because of BS antenna side-lobes. Hence, the MAC layer design at S includes a functionality that coordinates and manages the transmission of different BS.

A situation in which the system coverage area is partitioned into six sectors of 60 degrees each is shown in Figure 6. All ST(s) in a sector will associate with the BS antenna serving that sector. Each antenna's radiation pattern covers an additional 20 degrees on either side. Thus, depending on the attenuation levels, a scheduled transmission in one sector may exclude the simultaneous scheduling of certain transmitter-receiver pairs in other sectors. A detailed discussion on the radiation pattern for a typical BS antenna, the regions of interference and system capacity bounds is given in Annex B.

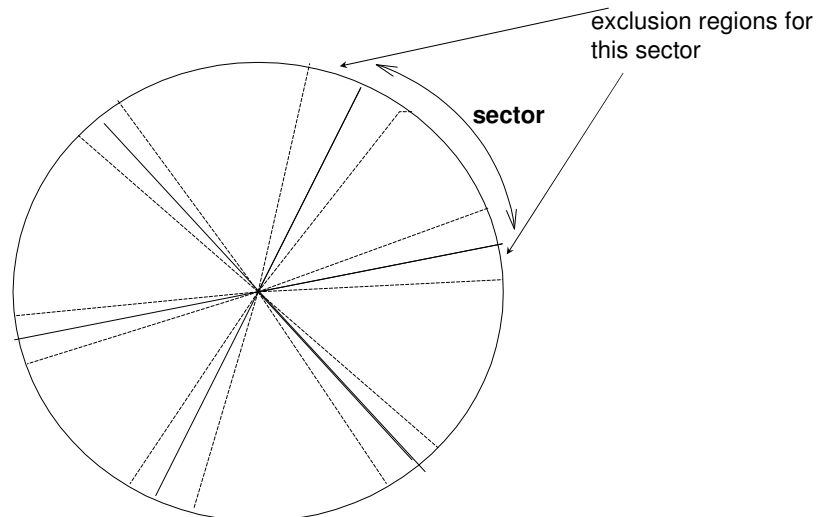


Figure 6: A simple antenna coverage and interference for six sectors

This aspect of sectorization of the coverage area while using the same frequency channel for all the sector antennas, is a key feature in WiFiRe. It not only impacts the design of the MAC protocol between

transmitters and receivers, but also the scheduling policies and the system performance. During downlink transmission, a significant amount of power from the transmitting BS reaches the adjacent BS antennas, the distance separating them being very small. Hence, when a downlink transmission is scheduled in any one of the sectors, the other BS(s) cannot be in receiving mode. Hence downlink (DL) and uplink (UL) transmissions must alternate. As a result, the MAC layer avoids conflict between interfering BS antennas by using time division duplex (TDD) between the DL and UL directions (See Figure 3). The MAC scheduler at S further needs to ensure that the adjacent/interfering BS do not transmit simultaneously. Only non-interfering BS(s) may transmit simultaneously and that too in a synchronized manner. This is explained further in section 2.9.

Each BS antenna is controlled by an IEEE 802.11b PHY. The MAC layer at S is on top of all of these PHY(s), as shown in Figure 7. From the perspective of the MAC, each PHY (hence each BS antenna) is addressable and identifiable. Thus a single MAC controls more than one PHY and is responsible for scheduling MAC packets appropriately in one more PHY(s), while resolving possible transmission conflicts from the perspective of the receivers. The MAC at S can individually address each PHY and can schedule packets for transmission through any of the PHY(s), either sequentially or in parallel.

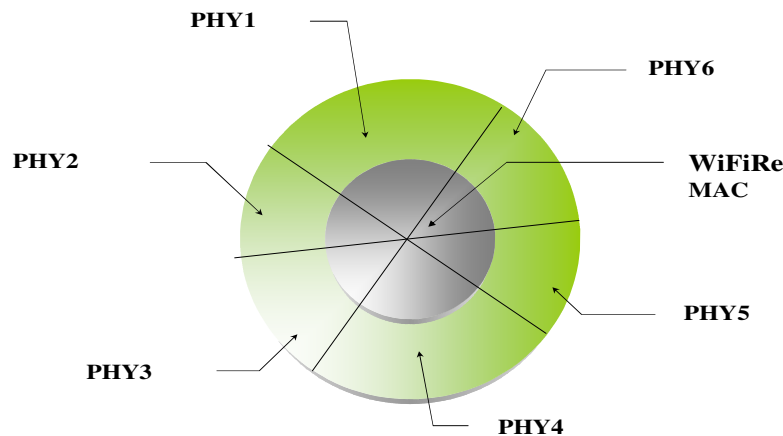


Figure 7: Single WiFiRe MAC controlling six WiFi PHY(s).

The system S broadcasts a downlink map (DL-MAP) and uplink map (UL-MAP) in specific slots (Beacons) of the downlink. These MAP(s) contain the slot allocations for the various transmissions and convey the link schedule information to the ST(s). Adjacent sectors (for example, sector 1, 2, 6 in Figure 7), resolve interference issues by employing time-division multiplexing (TDM) within each DL and UL period. The DL and UL are non-overlapping in time. Opposite sectors (for example, sector 1 and 4 in Figure 7), are not expected to interfere with each other in a typical installation and may transmit simultaneously during DL.

Opposite sectors may also receive simultaneously during UL. This leads to better resource utilization, as shown in Figure 8.

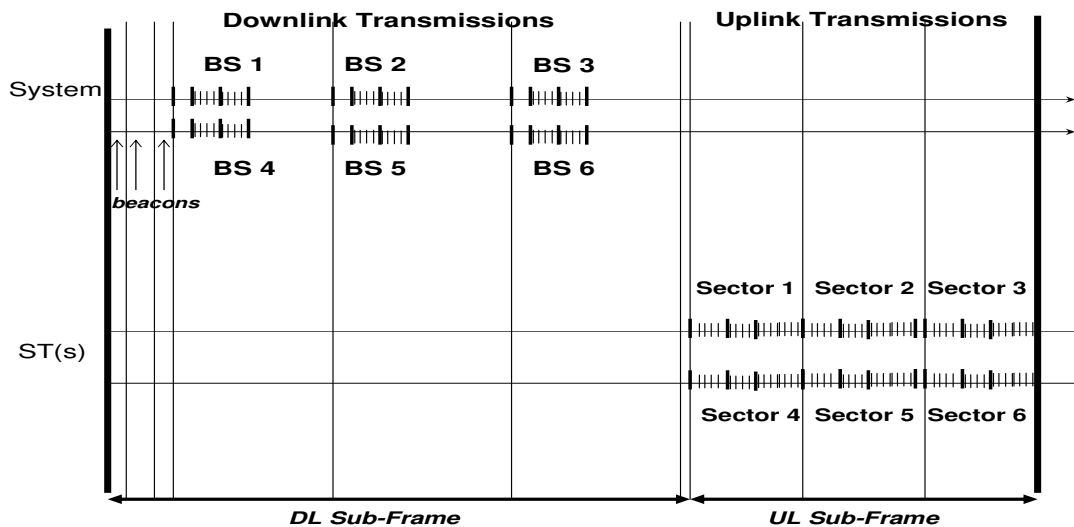


Figure 8: Parallel transmissions in a six sector system (conservative case)

The scheduler may further exploit such a situation to increase throughput by increasing the parallelism to include other non-interfering transmissions also. For example, in a particular deployment of ST(s), it may be possible to schedule parallel transmission of alternate BS(s), such as BS 1, 3 and 5. This depends upon the interference matrix determined by the ST locations and antenna radiation patterns. A discussion on scheduler design is given in Annex C.

2.6 MAC protocol overview

The MAC mechanism is a time division duplexed, multi-sector TDM (TDD-MSTDM) scheduling of slots. Time is divided into frames (See Figure 8). Each frame is further partitioned into a downlink (DL) and an uplink (UL) segment, which need not be of equal durations. The downlink - from the system S to the ST(s) - operates on a point-to-multipoint basis. The uplink - from a ST to system S - operates on a point-to-point basis. Within each segment there are multiple slots, of equal duration each. The slot duration and various timings are discussed in section 2.9.

The DL segment begins with each BS in the system transmitting a Beacon packet, in a non-interfering manner. For example, in the six sector system shown in Figure 7, the BS(s) for sectors PHY 1 and PHY 4 may transmit their beacons (say B1 and B4) simultaneously, followed by the BS(s) for PHY 2 and PHY 5, followed by PHY 3 and PHY 6. All BS(s) are synchronized with each other; hence transmission of beacon

B2 by PHY 2 starts only after completion of transmission of beacon B1 from PHY 1. Note that even though two beacons may get transmitted simultaneously (such as B1 and B4), their contents are not identical.

The beacon for each sector contains information for time synchronization of the ST(s) in that sector, information regarding the DL slot allocations (DL-MAP) and UL slot allocations (UL-MAP) for that frame, and other control information. Informally, a beacon contains <Operator ID, System ID, BS ID, All registered ST(s) scheduled for that frame and their corresponding slot assignments>. The BS ID identifies the BS (or the PHY) through which this beacon is transmitted. The structure of a beacon is given in section 4.5.

The rest of the DL transmissions follow the DL-MAP in the Beacon. In each DL slot, one or zero transmissions can take place in each sector. The DL-MAP may allow multiple non-interfering BS to simultaneously transmit a packet to the ST(s) in their respective sectors, in each slot. The DL segment ends when all the transmissions as given in the DL-MAP have been completed.

To account for propagation delays, there is a guard time of a few slots between the end of the DL segment and the start of UL segment (see section 2.9). In each UL slot, one or zero transmissions can take place in each sector, as governed by the UL-MAP. The UL-MAP is constructed in such a way that multiple ST(s) from different sectors, may transmit in the same UL slot, provided these transmissions are non-interfering at the BS. Because of path loss patterns and time varying traffic requirements, the DL-MAP and UL-MAP need to be computed on-line. A discussion on scheduler design is given in Annex C.

The link protocol includes mechanisms that allow a ST to transmit resource (slot) reservation requests to S, for the UL and DL segments. This enables a ST to request for specific delay and bandwidth guarantees. On receipt of such resource reservation requests, the MAC layer at S executes a scheduling functionality that tries to meet the demands of the ST(s), for the next time frame. This link schedule information is captured as the DL-MAP and the UL-MAP and transmitted with the corresponding beacon. An ST listens to all the beacons from its associated BS. From the DL-MAP, the ST determines the DL slots to be monitored for its downlink data packets. From the UL-MAP, the ST determines the UL slots in which to send its data (or control) packets to the BS. Depending on the class of service, a ST may have regular slot(s) allocated in each time frame, or may be granted slot(s) by the S, after explicit resource requests. The protocol details, including the request-grant mechanism, packing, data transmission etc. are given in section 4.8 onwards.

2.7 MAC services

The WiFiRe MAC is connection-oriented. A connection defines both the mapping between peer data link processes that utilize the MAC and a service flow category. The service flow category defines the quality of

service (QoS) parameters for the PDU(s) (protocol data units) that are exchanged on the connection. Each connection has a unique identifier (CID). Service flow categories provide a mechanism for uplink and downlink QoS management. Each ST adheres to a transmission protocol that controls contention and enables the service to be tailored to the delay and bandwidth requirements of each user application. This is accomplished through different types of uplink scheduling mechanisms. An ST requests uplink bandwidth (slots) on a per connection basis (implicitly identifying the service flow category).

A system *S* may grant bandwidth to a ST in one or more of the following ways: (i) Unsolicited bandwidth grants, (ii) Polling, and (iii) Contention Procedures. For example, real-time applications like voice and video require service on a more uniform basis and would fall in the Unsolicited bandwidth grant category, data applications that are delay-tolerant may be serviced by using the Polling mechanism and the Contention mechanism may be used when an ST has been inactive for a long period of time. These are described in more detail in section 4.8.

A default set of service flows may be provisioned when a ST is initialized. Subsequently, connections may be associated with these service flows, to provide a reference against which to request bandwidth. New connections may also be established when required. Connections once established may require active maintenance, depending on the type of service. For example, VoIP services are fixed demand and would require virtually no connection maintenance. On the other hand, Internet access services may require a substantial amount of ongoing maintenance due to their bursty nature and due to the high possibility of fragmentation. Finally, connections may be terminated. All connection management functions are supported through the use of static configuration and dynamic addition, modification, deletion of connections.

Also, within a scheduling interval, bandwidth may be granted by *S* on a per connection basis (Grant Per Connection) or as an aggregate of grants for each service flow category (Grant Per Service Flow) or as an aggregate of all grants for a ST (Grant Per Subscriber Terminal). The grant per connection would be typically used for VoIP, while the grant per service flow would be used for TCP traffic. These are described in more detail in section 4.2.

Mechanisms are defined to allow vendors to optimize system performance using different combinations of these bandwidth allocation techniques while maintaining consistent inter-operability definitions.

2.8 MAC service interfaces

The service interfaces include the Service Specific Sub-layer (SSS), MAC Link Control Sub-layer (LCS) and the MAC Security Sub-layer. The reference model for service access points (SAP) is shown in Figure 4. A brief mention of the main services is given below. The detailed service specification is given in section 3.

The SSS should provide protocol-specific services to UE(s) for protocols such as IP, ATM, Ethernet, etc. The MAC being connection-oriented provides for higher layer peer-to-peer connection(s) between a ST and BS, with associated QoS parameters for data transport. The SSS should provide connection management and packet classification services, for mapping higher layer PDU(s) (protocol data units) to connections provided by the MAC LCS sub-layer. These functions should be as follows:

- *Connection Management*: The SSS should provide SAP(s) to higher layers to create and maintain higher layer peer-to-peer connection(s) between a ST and BS, with associated QoS parameters.
- *Packet Classification*: The SSS should provides SAP(s) to carry out the task of classifying higher layer PDU(s) into appropriate connections (based on some policy database), and mapping the higher layer PDU(s) to MAC PDU(s).

The SSS in turn uses the following LCS services to communicate with the peer SSS:

- *Connection Provisioning*: This includes primitives for creating and terminating MAC connections. Each connection has a unique identifier (CID).
- *Data Transport*: This includes primitives for delivery of the MAC SDU(s) (service data units) to the peer MAC entity, in accordance with the QoS associated with a connection's service flow characteristics.
- *Security*: This includes primitives for the security sub-layer, for authentication of the end-points, and for secure transmission of the connection's PDU(s).

2.9 Typical Frame and Slot Timings

The MAC assumes that a single voice over IP (VoIP) packet, approximately 40 bytes long, will fit into one time slot of the frame. Since a single voice call may be the only traffic to/from an ST in several instances, it is important to design the MAC so that system capacity utilization is as efficient as possible even with a large number of STs with single VoIP calls. Also, VoIP packets are generated periodically, once in 20 or 30 milliseconds, for active connections. As a result, the duration of a frame is chosen as 10 milliseconds and a slot is defined as 32 microseconds. At 11Mbps, one slot corresponds to 44 bytes; at 2 Mbps, this is 8 bytes. The PHY overhead at 1 Mbps is 6 slots (192 microseconds) and 3 slots at 2 Mbps and 11Mbps (96 microseconds). In case the VoIP packet is longer, the slot duration will need to be increased and the

number of slots per frame correspondingly reduced. The Beacon carries system information using which the ST(s) can appropriately interpret the frames.

A frame corresponds to $10 * 1000 / (32) = 312.5$ slots. This is partitioned between the downlink (DL) and uplink (UL). The DL to UL ratio is to be fixed at the time of system initialization. A roughly 2:1 ratio is the default value. Hence there are 208 slots for the DL and 100 slots for UL, including overheads. As shown in Figure 9, 4.5 slots are used as guard time between the DL and UL, to account for propagation delays and to provide for transmitter-receiver turn-around at the BS radio. This gives a maximum possible range of about 24 Kms. Varying the DL to UL ratio dynamically, on a periodic or per frame basis, is optional. In this case, care needs to be taken to ensure synchronization of the BS antennas, to prevent UL, DL interference.

Beacons

Beacons are sent consecutively (for 3 adjacent sectors) at the beginning of each frame. These beacons are broadcast from the system, each by a different BS. The beacons are several slots long. Opposite sectors may transmit beacons simultaneously, when number of sectors is greater than 3.

A beacon is sent at 2 Mbps. Thus a beacon is 3 slots (PHY Overhead) + 1 slot (Control Overhead) + 1 slot (DL-MAP) + 1 slot (UL-MAP). The control overhead includes the beacon header, operator ID, etc.

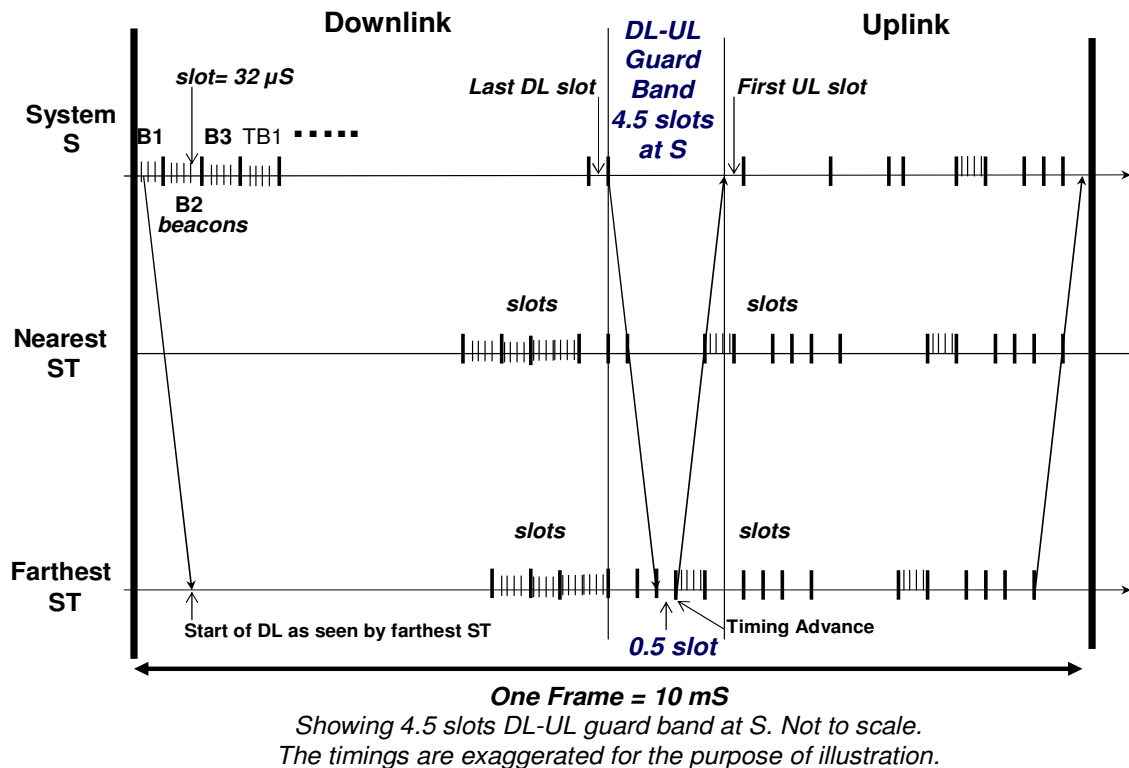


Figure 9: WiFiRe Timing Diagram

Downlink Transport Block

All downlinks, excluding the beacon, are at 11 Mbps. A DL slot is at least 4 slots (3 PHY overhead + 1). Since DL is point-to-multipoint within each sector, (i) multiple MAC PDU(s) can be combined and (ii) MAC PDU(s) for different ST can be combined, and transmitted using a single PHY overhead. This is termed as a *Downlink Transport Block* (DL-TB). The DL-TB should always begin at slot boundary and may be of variable size. However, it should fit in an integral number of slots (minimum 4) and should not exceed the maximum payload size defined by the chosen WiFi PHY; $aMPDUMaxLength = 2312$ bytes, for DSSS as specified in IEEE 802.11b [11]. The DL-MAP specifies the <ST-ID> of the ST(s) for which there are packets in the current DL sub-frame. The MAC header specifies how one or more ST(s) extract one or more IP packets (including VoIP) from the DL-TB payload.

Uplink Transport Block

All uplinks are at 11Mbps. A UL slot is at least 4 slots (3 PHY overhead + 1). Since UL is point-to-point within each sector, multiple MAC PDU(s) at a given ST can be combined and transmitted using a single PHY overhead. This is termed as a *Uplink Transport Block* (UL-TB). The UL-TB should always begin at slot boundary and may be of variable size. However, it should fit in an integral number of slots (minimum 4) and should not exceed the maximum payload size defined by the WiFi PHY. The UL-MAP specifies the <ST-ID, Slot No> mapping for which ST is to transmit in which slot. The MAC header specifies how the BS extracts one or more IP packets from the UL-TB payload. The key difference between UL-TB and DL-TB is that the UL-TB is always for one ST whereas DL-TB can be for multiple ST(s) in the same sector.

There should be a few microseconds of silence after every UL-TB to accommodate for estimation errors in ranging. This is ensured during slot allocation, depending on the fraction of last slot that is actually occupied by an ST's transmission. The MAC headers for the UL-TB and DL-TB are similar. The MAC header includes information for concatenating fractional IP packets split between the last TB of one frame's DL/UL and the first TB of the next frame's DL/UL. This is described in more detail in section 4.9.

Note that a maximum of $100 / 4 = 25$ simultaneous users can be supported on UL, when there is no spectrum reuse among the sectors. This means a payload of $25 * 2$ bytes <ST-ID, Starting slot>, for the UL-MAP (and DL-MAP). If there are no allocations for an ST in DL-MAP (and UL-MAP), the ST may go into power-save mode.

The start of the UL may have ranging blocks. Each ranging block is of size 8.5 slots (3 PHY overhead + 1 slot + 4.5 slots guard time). An ST-ID of all 1's in the UL-MAP indicates that the corresponding slot is a

ranging block. These slots are used to transmit ranging request messages. The guard time is required to account for the propagation delay(s) between the BS and the ST and for computing the timing advance by the BS (See Figure 11).

The end of the UL may have contention slots. Each contention slot is of size 4 slots (3 PHY overhead + 1 slot). An ST-ID of all 0's in the UL-MAP indicates that the corresponding slot is a contention slot. Contention slots are used to transmit registration request messages, resource reservation messages and data for best-effort connections. There should be at least one contention slot per frame. Also, *polling slots*, specifically for transmission of resource reservation requests by an ST, may occur optionally in each frame. A polling slot should occur at least once every 50 frames. The sequence of slots for one BS is shown in Figure 10.

Beacon (BS ID DL-MAP UL-MAP)	DL-TB(s) 1...M (Min 4 slots each)	DL-UL Guard time (4.5 slots)	Ranging Block(s) (8.5 slots) (optional)	UL-TB Polling Slot(s) (optional)	UL-TB(s) 1...N (Min 4 slots each)	Contention Block(s) (Min 4 slots)
---	--	---	--	---	--	--

Figure 10: Frame structure as seen by one BS

2.10 Ranging and power control

New and un-synchronized ST(s) are allowed to Range and Register. During power-on initialization, a ST gets attached to a BS of the system S, depending on the beacons it is able to hear from the system S. On powering up a ST listens for one or more beacons from the Operator and System ID it is programmed for. There are specific time slots defined in the uplink segment for ranging. These are called ranging blocks and ranging request packets are transmitted in them. Informally, ranging request has the following information: <System ID, ST ID, BS IDs that are audible to the ST, Signal strengths of beacons from the various BS>. Based on this, the system S associates the ST with one of the BS. Then S informs the ST about the timing synchronization and BS ID that will service the ST. This is done through a ranging response packet. Upon receipt of a ranging response from a BS, the ST is live and ready to receive from and transmit data to that BS. The ranging process is shown in Figure 11 and is described in more detail in section 4.7.

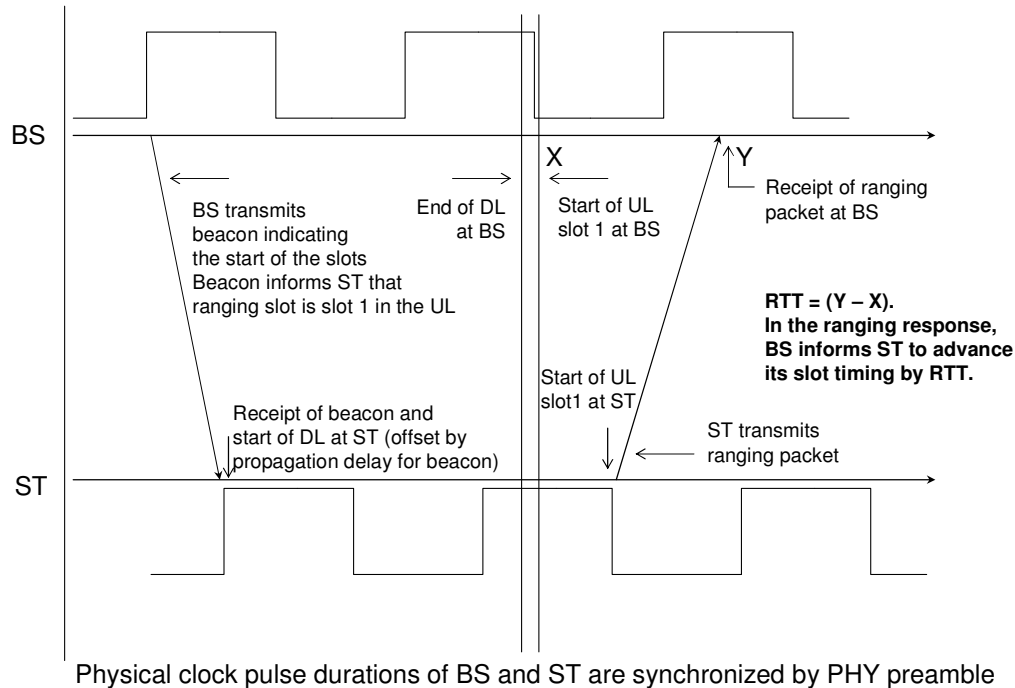


Figure 11: Ranging and Timing Advance Mechanism

The ranging response may optionally recommend the transmitter power level to be used by the ST. This may facilitate power control and better re-use across sectors. It may also contain information to enable the ST to switch to sleep modes to conserve power when needed. *The specification of protocol actions and PDU formats for power control are deferred to a later release.*

2.11 PDU formats

The details of the formats for the various protocol data units (PDU(s)) are given in section 4.3 onwards. A brief description of some of the important PDU(s) is as follows:

- *Beacon*: This contains <Operator ID; System ID; BS ID; DL-MAP; UL-MAP>. It also specifies whether a ranging block is present in the UL sub-frame.
- *Ranging Request*: This contains the <Operator ID; System ID; ST ID> of the ST sending the request. It also contains the <BS ID, Signal Strength> information for each beacon heard by the ST.
- *Ranging Response*: This contains the <BS ID, Basic CID, Primary CID, Timing Advance>. It assigns two connection identifiers - a Basic CID to the ST for periodic ranging and a Primary CID for further exchange of management messages. It also conveys the Timing Advance information to the ST to synchronize the ST transmissions with the BS slot timings.

- *Registration Request and Response*: The ST exchanges capabilities with the BS and gets assigned an IP address using these messages.
- *Dynamic Service Addition Request and Response*: The ST requests for and gets assigned a data CID using these messages. The service flow parameters are sent as Type-Length-Value tuples.
- *Dynamic Service Change Request and Response*: The ST uses these messages to either change the properties of a connection or to send a resource reservation request to the BS.
- *Data*: This contains the higher-layer data (MSDU) to be transferred from ST to BS or vice versa.

2.12 BS Scheduler functions

As mentioned earlier, a single MAC at S controls more than one PHY and is responsible for scheduling. The MAC at S can individually address each PHY and can schedule packets for transmission through any of the PHY(s) either sequentially or in parallel. The scheduler should optimally do the following:

- Simultaneously schedule multiple pairs of transmissions to/from BS(s) from/to ST(s), in a non-interfering manner.
- Appropriately combine traffic to one or more ST(s) in a sector into one DL-TB, without affecting the scheduling of other sectors.
- Assign uplink capacity keeping QoS requirements in consideration, especially the periodic nature of VoIP packets and TCP ACK(s).
- Adapt to new additions or dropout of ST(s) in the system, within a frame.

The specification of the scheduler is beyond the scope of this document. However, a detailed discussion on scheduler design is given in Annex C.

2.13 Support for multiple operators

The WiFiRe channel model requires about 20 MHz (1 WiFi Carrier) spectrum in order to provide VoIP and broadband Internet services to the users in a cell. In order to support multiple operators in an outdoor environment, a WiFiRe system operator may require conditional licensing of one channel (frequency band of 20 MHz) within the unlicensed 2.4 GHz band. The charges/fees for this channel licensing are expected to be negligible. A single operator is expected to own the conditional license and operate the site towers, in any given area. All the components (transmitters, receivers and directional antennas) belonging to an operator should use the same channel, while another operator should use a different channel. In case multiple operators are to be permitted in the same area, each operator would need to conditionally license one channel, in a non-overlapping manner. Receivers located in a coverage area of multiple antenna(s) should point towards a designated antenna during deployment time and remain locked to this tower.

2.14 Summary of protocol steps

The main steps involved in the protocol are as follows:

1. ST powers On and determines the Operator ID and System ID from its configuration.
2. ST listens for beacon messages – format is defined in section 4.5.
3. For each beacon received, ST notes the BS ID, the signal strength of the beacon and the ranging blocks as allocated in the UL-MAP.
4. ST constructs a ranging request message – format is defined in section 4.7.
5. ST determines the BS to transmit ranging request to – beacon received with highest signal strength.
6. ST waits for start of ranging block in the corresponding UL sub-frame.
7. ST transmits the ranging request message in the ranging block.
8. ST waits for ranging response – monitors DL-MAP in all beacons of the subsequent frames.
9. If no response is received within a timeout period, ST waits for a random backoff time and repeats the actions from step 6.
10. S receives the ranging request message and selects an appropriate BS and determines the timing advance to be used by the ST for being in slot synchronization with the BS.
11. S constructs a ranging response message – format is defined in section 4.7
12. S puts the ranging response in transmit queue of the corresponding BS and invokes the scheduler.
13. Scheduler (asynchronously) constructs the DL-MAP for the next frame. Transmission of the ranging response may get scheduled in the next or some other subsequent frame.
14. Scheduler may (optionally) provide a UL slot allocation (in the UL-MAP) for the registration request transmission by the ST.
15. S transmits the DL-MAP and UL-MAP in the next beacon.
16. S transmits the ranging response in appropriate DL slot.
17. ST finds its id in DL-MAP and receives the ranging response message in the corresponding slot. ST determines the basic CID and primary CID to be used for further exchanges.
18. ST constructs a registration request message.
19. ST transmits registration request in the allocated UL slot (if any) or in one of the UL contention slots and waits for a registration response. If no response is received within a timeout period, ST waits for a random backoff time and retransmits the registration request.
20. S receives the registration request and assigns an IP address to the ST, after authentication.
21. S constructs a registration response message and transmits it in the appropriate DL slot.
22. Registration is complete when the ST receives and is able to process the registration response. Now the ST has an IP address and is ready to setup data connections.
23. When the higher layer at ST has a data packet to send, it sends a dynamic service addition request message to S, in one of the polling slots or contention slots. If no response is received within a

timeout period, ST waits for a random backoff time and retransmits the request.

24. Upon receipt of the message, S assigns a data CID and responds with a dynamic service response message. The service flow and QoS parameters associated with the CID are now known to both.
25. If it is a UGS flow, the scheduler at S assigns periodic bandwidth grant in the UL sub-frame to ST.
26. If it is a rtPS or nrtPS flow, the ST requests bandwidth whenever required by sending an appropriate dynamic service change request message. Subsequently it transmits the data in the assigned slots.
27. Finally, it transmits a dynamic service deletion message to terminate the connection.

3 MAC SERVICE DEFINITION

The MAC provides a connection-oriented wireless link with provisioning to meet the QoS requirements of higher layer data streams. The information flow across the boundaries between the layers can be defined in terms of primitives that represent different items of information and cause actions to take place. These are called service access point (SAP) primitives (See Figure 4). These primitives describe the information that must necessarily be exchanged between the MAC and the higher layer to enable correct functioning of each. These primitives do not appear on the air interface but serve to define the relations of the different layers. The semantics are expressed in the parameters that are conveyed with the primitives.

The WiFiRe MAC being connection-oriented provides for higher layer peer-to-peer connection(s) between a ST and BS, with associated QoS parameters for data transport. This section defines the services provided by the MAC sub-layer(s). It does not impose message formats or state machines for these primitives.

3.1 Service Specific Sub-Layer (SSS)

The Service Specific Sub-layer (SSS) resides on top of the MAC Link Control Sub-layer (LCS). It utilizes the services provided by the LCS and in turn provides services to external higher layers. The SSS provides protocol-specific services to UE(s). It provides connection management and packet classification services for mapping higher layer PDU(s) to connections provided by the MAC LCS sub-layer.

The packet SSS is used for transport for all packet-based protocols such as Internet protocol (IP), point-to-point protocol (PPP), and IEEE 802.3 (Ethernet). The packet SSS should perform the following functions:

1. providing SAP(s) to higher layers for creating and maintaining higher layer peer-to-peer connection(s) between a ST and BS, along with associated QoS parameters.
2. accepting higher-layer PDU(s) from the higher layer protocol.
3. classification of the higher-layer PDU(s) into the appropriate MAC layer connection(s).
4. processing (if required) the higher-layer PDU(s) based on the classification.
5. mapping the higher layer PDU(s) to MAC SDU(s) (service data units).
6. delivering the MSDU(s) to the appropriate LCS SAP.
7. accepting the MSDU(s) from the peer LCS entity.
8. mapping the MSDU(s) received from peer entity into appropriate higher layer PDU(s) and delivering them to the higher layer.

For each MSDU, the sending SSS is responsible for delivering the MSDU to the LCS SAP. The LCS is responsible for delivery of the MSDU to peer LCS SAP. This is done in accordance with the QoS, fragmentation, concatenation and other functions associated with a particular connection's service flow characteristics. The LCS uses appropriate MAC management PDU(s) to get the resources (slots) required for sending the MSDU to its peer LCS. The MSDU maps to the payload part in a MAC data PDU. Finally, the receiving SSS is responsible for accepting the MSDU from the peer LCS SAP and delivering it to a higher-layer entity.

3.1.1 Classification

Classification is used to map MSDU(s) to a particular connection for transmission to its MAC peer. Different classifiers are to be used, depending on the upper layer protocol.

A classifier is a set of matching criteria applied to each packet entering the WiFiRe MAC. It consists of protocol-specific matching criteria, a classifier priority and a reference to a CID. When a packet matches a criteria, then the packet is associated with the corresponding CID and is delivered to the corresponding SAP. The service flow characteristics associated with the CID decides the QoS offered to the packet. Classifier priority is provided because overlapping matching criteria may be used by multiple classifiers. Hence priority is used to determine the order in which the classifiers will be applied to a packet.

IP classifier: IP classifiers can be based on one or more of the following fields

- ToS/DSCP bits
- Source address
- Destination address
- Protocol id
- Source port
- Destination port

Ethernet classifier: This classifier may consists of one or more of

- Source MAC address
- Destination MAC address
- Ether type

The packet classification may be done implicitly by the SSS, by examining the higher layer headers. For example, TCP ACK(s) may be identified by parsing the higher layer headers and are assigned a separate data CID. Similarly VoIP packets are identified by their size (VoIP payload is about 20 bytes; VoIP header + tolerance for power amplifier and estimation errors is less than 20 bytes). The packet classification may also be done explicitly. The explicit classification rules follow the TLV encoding, similar to IEEE 802.16.

Further detailed specifications of the SSS primitives are deferred to a later release.

3.1.2 Concatenation

Multiple MPDU(s) may be concatenated as a single PHY PDU. Maximum size of MPDU can be 2312 bytes, as defined in IEEE 802.11 (when DSSS PHY is used). When individual MPDU(s) are smaller than maximum MPDU size, they should be concatenated as shown in Figure 12.

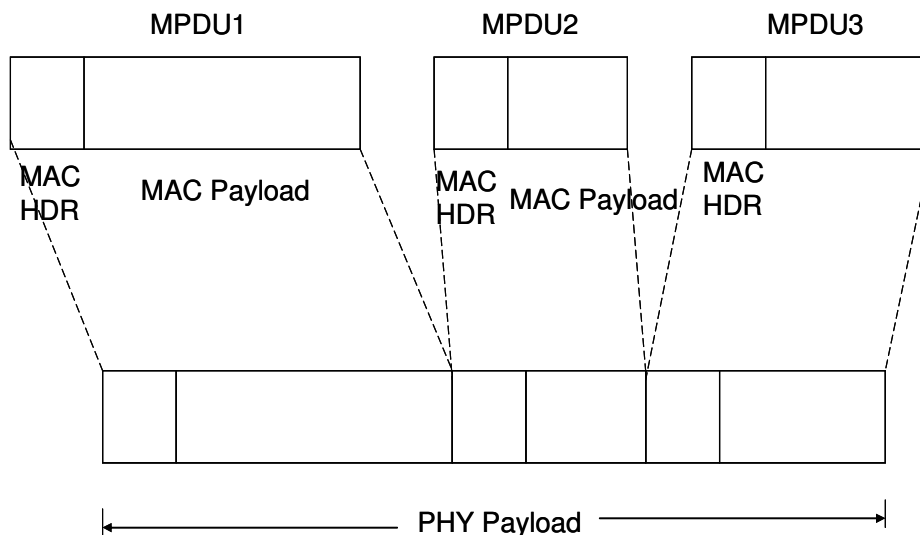


Figure 12: Concatenation of Multiple MPDU(s)

To keep the design simple, WiFiRe does not recommend *packing* (as defined in IEEE 802.16). Instead, multiple MSDU(s) can be concatenated in a similar manner as shown above. MPDU(s) should be constructed out of each individual MSDU and concatenation operation may be performed on the MPDU(s).

When ARQ is enabled, each MPDU will carry fragmentation sub-header which will have FC value set to “unfragmented” and will carry appropriate FSN value, as described in the next sub-section

3.1.3 Fragmentation

Fragmentation is the process by which a MAC SDU may be divided into multiple MAC PDU(s). The constituent fragments are then reassembled at the receiver to construct the original MAC SDU. Capabilities of fragmentation and reassembly are mandatory.

The IP layer will have a MTU of 2312 bytes. For a given MPDU, if the MAC scheduler can assign enough slots, then the MPDU can be transmitted without fragmentation. But, when the scheduler assigns less number of slots, then the MPDU has to be fragmented. Each fragment will carry a *fragmentation sub-*

header which will carry information required for reassembly at the receiver. The fragmentation sub-header is shown below in Figure 13 and the fragmentation of an IP packet is shown in Figure 14.

FC (Fragment Control) 2 bits	FSN (Fragment Sequence Number) 11 bits	Reserved 3 bits
---------------------------------	---	--------------------

Fragment	Fragment Control (FC) value
Unfragmented	00
First Fragment	01
Continue Fragment	10
Last Fragment	11

Figure 13: Fragmentation Sub-Header

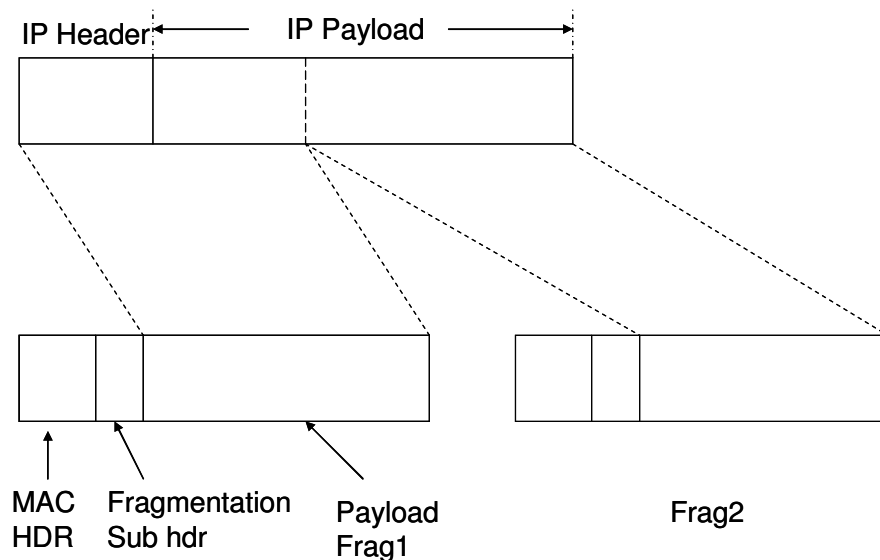


Figure 14: Fragmentation of an IP packet

3.1.4 Fragmentation and ARQ

ARQ is an optional mechanism defined under the MAC to provide link layer reliability. When an MPDU is not fragmented, but the connection has ARQ enabled, ARQ is applied as though the entire MPDU is a single fragment. The MPDU should carry fragmentation sub header with FC field set to “unfragmented” and the FSN should be set to current FSN.

For fragmented MPDU(s), ARQ is applied on each fragment. FSN is increased sequentially for the fragments. The worst case of fragmentation happens when a max size frame (2312 bytes) is allocated only one slot (40bytes) at a time. Hence the number of fragments is $2312/40 = 57.8$. Hence FSN should be at least 6 bits long.

Fragments in ARQ enabled connections are handled according to a standard ARQ process. If a fragment is not received, then the sender retransmits the fragment as per the ARQ functionality. Note that when ARQ is enabled, each fragment acts as an ARQ block. FSN across MPDU(s) of a connection increases sequentially according to ARQ rules. The ARQ rules and parameters are similar that used in IEEE 802.16.

For non-ARQ connections, fragments are sent only once and in the increasing order of FSN. If all the fragments were received correctly by the receiver, then the receiver should build the original MPDU from the fragments. FSN assigned to each fragment enables the receiver in constructing the original MPDU. If there was any loss in fragment, then the receiver should discard all the fragments of the MPDU, including the ones received subsequently until it finds a new first fragment or an fragmented MPDU.

3.2 Link Specific Sub-Layer (LCS)

The MAC-LCS services are used by Service Specific Sub-layer (SSS) to access the connection-oriented wireless link for data packet transport. The LCS layer provides the following categories of services:

1. Connection provision services, including creation, termination and change.
2. Data delivery services, from/to the higher layer SSS to/from the peer LCS entity.
3. Security services, including authentication and privacy.
4. Management services, for configuration of various default and power-on values.

The initial request for service from the LCS is provided by the “request” primitive. When this request is made by the initiating SSS, the initiating-side LCS constructs the appropriate Dynamic Service Request message (addition, change, or deletion; see section 3.2.1) and sends it across the wireless link to the peer (receiver-side) LCS. This peer LCS generates an “indicate” primitive to inform its SSS of the request. The peer (receiver-side) SSS entity responds with a “response” primitive to its LCS. This causes the receiver-side LCS to send an appropriate Dynamic Service Response message to its peer (initiating-side) LCS. This LCS generates a “confirm” primitive to the original requesting SSS entity. The LCS may also send a Dynamic Service Acknowledge message to its peer, if appropriate. At any point along the way, the request may be rejected (such as due to lack of resources), terminating the protocol.

In some cases, for example when the MAC LCS on the initiating-side itself rejects the request, it is not necessary to send information to the peer entity and the “reject” primitive is issued directly by the LCS.

3.2.1 Connection Provision Services

The use of these services is to provide peer communication between System S and a ST for the purpose of creating a connection with QoS parameters. The traversal of connection request and response messages is as shown in Figure 15.

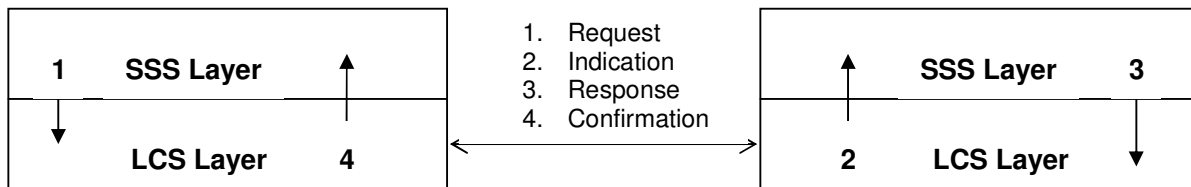


Figure 15: Primitives to request service of MAC sub-layer and generate response

The following primitives are supported:

1. **MAC_CREATE_CONNECTION.request:** This primitive is issued by a SSS entity in a system S or at a ST, to request S to dynamically set up (add) a connection. If the primitive is generated on the ST side, the receipt of this primitive causes the corresponding LCS to pass the request (in the form of a Dynamic Service Addition Request message) to its peer LCS entity in the S. The originating LCS at the ST maintains the correlation between sequence number and the requesting SSS entity.
2. **MAC_CREATE_CONNECTION.indication:** This primitive is issued by the receiver-side LCS entity to its SSS, to request the dynamic addition of a connection, (typically in response to the receipt of a Dynamic Service Addition Request message). If the LCS entity is at S, a CID is generated and the request is authenticated.
3. **MAC_CREATE_CONNECTION.response:** This primitive is issued by a receiver-side SSS entity to its LCS in response to the request for creation of a new connection. The LCS then passes on the response to its peer (initiating-side) LCS entity, in the form of a Dynamic Service Addition Response message.
4. **MAC_CREATE_CONNECTION.confirmation:** This primitive is issued by initiating-side LCS entity to its SSS entity, upon receipt of a Dynamic Service Addition Response message from its peer LCS. This informs the SSS of the status of its request and provides a CID, if the request was successful.
5. **MAC_CHANGE_CONNECTION.request:** This primitive is issued by a SSS entity in a system S or at a ST, to request S to dynamically change a connection's characteristics. For example, this may be to reflect changing bandwidth requirements. If the primitive is generated on the ST side, the receipt of this primitive causes the LCS to pass the request (in the form of a Dynamic Service Change Request message) to the LCS entity in the S.

6. **MAC_CHANGE_CONNECTION.indication:** This primitive is issued by the receiver-side LCS entity to its SSS, to request the dynamic change of a connection.
7. **MAC_CHANGE_CONNECTION.response:** This primitive is issued by a receiver-side SSS entity to its LCS, in response to the request for changing a connection. The LCS then passes on the response to its peer (initiating-side) LCS entity, in the form of a Dynamic Service Change Response message.
8. **MAC_CHANGE_CONNECTION.confirmation:** This primitive is issued by initiating-side LCS entity to its SSS, upon receipt of a Dynamic Service Change Response message from its peer LCS. This informs the SSS of the status of its connection change request.
9. **MAC_TERMINATE_CONNECTION.request:** This primitive is issued by a SSS entity in S or ST to request the termination of a connection. If the primitive is generated on the ST side, it causes the LCS to pass the request (in the form of a Dynamic Service Deletion Request message) to the LCS entity in the S.
10. **MAC_TERMINATE_CONNECTION.indication:** This primitive is issued by the receiver-side LCS entity to request the termination of a connection, in response to the receipt of a Dynamic Service Deletion Request message from its peer LCS.
11. **MAC_TERMINATE_CONNECTION.response:** This primitive is issued by the receiver-side SSS entity to its LCS, in response to a request for the termination of a connection. The LCS then passes it on to its peer (initiating-side) LCS entity in the form of a Dynamic Service Deletion Response message.
12. **MAC_TERMINATE_CONNECTION.confirmation:** This primitive confirms to an initiating SSS entity that a requested connection has been terminated.

While processing these Connection Provisioning messages, MAC LCS at S and ST also verify the QoS constraints requirement (indicated with the request). The resultant MAC connection then provides QoS guaranteed data transport service to the originator. More detail about the primitives is given in section 3.3.

3.2.2 Data Delivery Services

These services provide peer LCS entities with the ability to exchange MAC service data units (MSDU(s)). At S, the LCS determines the destination SAP, sector and associated BS antenna for a given MSDU, by looking up a connection table; the specification of the table fields are left open for implementation choices. The LCS then uses the underlying Security sub-layer (if required) and PHY-level services to transport an MSDU to a peer LCS entity. Such asynchronous MSDU transport is performed on a QoS constrained and/or best-effort basis. An acknowledgement procedure ensures reliable delivery of MSDU.

The overview of primitives falling in this class of service by MAC LCS is as follows:

1. **MAC_DATA.request:** This primitive is issued by a SSS entity to transfer data to its LCS SAP. This causes the LCS entity to transfer the data to its peer LCS entity, in the appropriate downlink or uplink slot(s), as governed by the DL-MAP/UL-MAP and the MAC protocol.
2. **MAC_DATA.indication:** This primitive is issued by a LCS entity to transfer data from the MAC to the SSS. The specific SSS to receive the indicate message is implicit in the Connection Identifier (CID) information in the MAC header.

More detail about the primitives is given in section 3.3.

3.2.3 Security services

No SAP needs to be provided for security services. Authentication and encryption are part of only LCS. Using the Management Service primitives given in section 6, the administrator configures the security services for the BS/ST. The LCS then provides the security services without any intervention from the SSS. These services include mechanisms for:

1. Mutual authentication between BS and a ST. An appropriate authentication protocol may be used. In the simplest case, the BS may be configured to know the MAC addresses of all the ST(s) in the system. An ST sends its MAC address to the BS along with the Registration Request. The BS verifies its authenticity and then proceeds with the next steps in registration. Similarly each ST may be configured with the MAC address of the BS, which is verified by the ST upon receipt of the Registration Response.
2. Encryption of the MPDU(s) by the LCS before they are transmitted over the air and decryption by the peer LCS. Appropriate key-exchange and encryption protocols may be used.

The detailed specifications of appropriate security sub-layer primitives are deferred to a later release.

3.2.4 Management services

These services provide mechanisms for configuring various default and power-on values, including:

1. Operator ID, System ID, Time.
2. MAC address of peer entity (if required, for authentication).
3. Various keys (if required, for encryption/decryption).
4. TDD frame duration, DL to UL ratio, slot duration, no of slots for ranging, guard time, max TB size, and other values may also be made into configurable parameters. In this case, the operator must ensure that all the active entities in a cell (system S and its ST(s)) are configured to have the same value for any given parameter. *As a result, these system parameter values need to be transmitted along with the Beacon, periodically.* Care needs to be taken to ensure one mis-configured device does not lead to inappropriate or incorrect functioning of the entire network.

The detailed specifications of appropriate management service primitives are deferred to a later release.

3.3 Detailed description of service primitives

3.3.1 *MAC_CREATE_CONNECTION.request*

3.3.1.1 *Function*

This primitive is issued by a SSS entity in a *S* or *ST* unit to request the dynamic addition of a connection.

3.3.1.2 *Semantics of the service primitive*

The parameters of the primitive are as follows:

MAC_CREATE_CONNECTION.request

```
(
scheduling service type,
service flow parameters,
payload header suppression indicator,
length indicator,
encryption indicator,
Packing on/off indicator,
Fixed-length or variable-length SDU indicator,
SDU length (only needed for fixed-length SDU connections),
CRC request,
ARQ parameters,
sequence number
)
```

The scheduling service type (see section 2.7) is one of the following: Unsolicited bandwidth grant (UGS), Polling (PS), and Contention or best effort (BE) service. The service flow parameters include details such as peak and average rate. These parameters are the same as those in the Dynamic Service Change Request message. The payload header suppression indicator specifies whether the SDUs on the service flow are to have their headers suppressed. The packing on/off indicator specifies whether packing may be applied to the MAC SDUs on this connection. The indicator being ON means that packing is allowed for the connection. The fixed-length or variable-length SDU indicator specifies whether the SDUs on the service flow are fixed-length or variable-length. The SDU length specifies the length of the SDU for a fixed-length SDU service flow. The encryption indicator specifies that the data sent over this connection is to be encrypted, if ON. No encryption is used, if OFF. Cyclic redundancy check (CRC) request, if ON, requests that the MAC SDUs delivered over this connection are transported in MAC PDUs with a CRC added to them. The automatic repeat request (ARQ) parameters are: whether or not ARQ is used for the connection and the maximum retransmission limit. As specified in section 2.6, selective-ARQ is to be used. The sequence number is used to correlate this primitive with its response from the *S* via the MAC.

3.3.1.3 *When Generated*

This primitive is generated by a SSS of an *S* or *ST* unit to request the *S* to set up a new connection.

3.3.1.4 *Effect of Receipt*

If the primitive is generated on the *ST* side, the receipt of this primitive causes the MAC to pass the request (in the form of a Dynamic Service Addition Request message) to the MAC entity in the BS. The *ST* MAC remembers the correlation between sequence number and the requesting SSS entity. If the primitive is generated on the *S* side, the *S* checks the validity of the request and, if valid, chooses a CID and includes it in the Dynamic Service Addition Request message sent to the *ST*. This CID shall be returned to the requesting SSS via the CONFIRM primitive. If the primitive originated at the *ST*, the actions of generating a CID and authenticating the request are deferred to the INDICATION/RESPONSE portion of the protocol.

3.3.2 **MAC_CREATE_CONNECTION.Indication**

3.3.2.1 *Function*

This primitive is sent by the receiver-side (non-initiating) MAC entity to the SSS, to request the dynamic addition of a connection in response to the MAC sublayer receiving a Dynamic Service Addition Request message. If the non-initiating MAC entity is at *S*, a CID is generated and the request is authenticated.

3.3.2.2 *Semantics of the service primitive*

The parameters of the primitive are as follows:

MAC_CREATE_CONNECTION.indication

```
(
service type,
service flow parameters,
sequence number
)
```

Parameters: See MAC_CREATE_CONNECTION.request.

The encryption and CRC flags are not delivered with the indication primitive since the lower layers would have already acted on it to decrypt the data or to check a CRC, before the MAC SDU is passed up to the SSS.

3.3.2.3 *When Generated*

This primitive is generated by the MAC sublayer of the non-initiating side of the protocol when it receives a Dynamic Service Addition Request message from the initiating side of the connection.

3.3.2.4 *Effect of Receipt*

When the SSS receives this primitive, it checks the validity of the request from the point of view of its own resources. It accepts or rejects the request via the `MAC_CREATE_CONNECTION.response` primitive. If the connection request has originated on the *ST* side, the *S* sends the CID to the *ST* side in this `RESPONSE` primitive. Otherwise, if the origin was *S* itself, the `RESPONSE` contains the CID in the DSA header bearing the indication.

3.3.3 ***MAC_CREATE_CONNECTION.response***

3.3.3.1 *Function*

This primitive is issued by a non-initiating MAC entity in response to a `MAC_CREATE_CONNECTION.indication` requesting the creation of a new connection.

3.3.3.2 *Semantics of the service primitive*

The parameters of the primitive are as follows:

`MAC_CREATE_CONNECTION.response`

```
(
Connection ID,
response code,
response message,
sequence number,
ARQ parameters
)
```

The Connection ID is returned to the requester for use with the traffic specified in the request. If the request is rejected, then this value shall be ignored. The response code indicates success or the reason for rejecting the request. The response message provides additional information to the requester, in type-length-value (TLV) format. The sequence number is returned to the requesting entity to correlate this response with the original request.

The ARQ parameters are: whether or not ARQ is used for the connection, maximum retransmission limit and acknowledgment window size.

3.3.3.3 *When Generated*

This primitive is generated by the non-initiating SSS entity when it has received a `MAC_CREATE_CONNECTION.indication`.

3.3.3.4 *Effect of Receipt*

The receipt of this primitive causes the MAC sublayer to send the Dynamic Service Addition Response

message to the requesting MAC entity. Once the Dynamic Service Addition Acknowledgement is received, the MAC is prepared to pass data for this connection on to the air link.

3.3.4 *MAC_CREATE_CONNECTION.confirmation*

3.3.4.1 Function

This primitive confirms to a convergence entity that a requested connection has been provided. It informs the *ST* or *S* of the status of its request and provides a CID for the success case.

3.3.4.2 Semantics of the service primitive

The parameters of the primitive are as follows:

MAC_CREATE_CONNECTION.confirmation

(
 Connection ID,
 response code,
 response message,
 sequence number
)

Parameters: see MAC_CREATE_CONNECTION.response.

3.3.4.3 When Generated

This primitive is generated by the initiating side MAC entity when it has received a Dynamic Service Addition Response message.

3.3.4.4 Effect of Receipt

The receipt of this primitive informs the convergence entity that the requested connection is available for transmission requests.

3.3.5 *MAC_Terminate_CONNECTION.request*

3.3.5.1 Function

This primitive is issued by a *SSS* entity in a *S* or *ST* unit to request the termination of a connection.

3.3.5.2 Semantics of the service primitive

MAC_TERMINATE_CONNECTION.request

(
 Connection ID
 Sequence number
) The Connection ID parameter specifies which connection is to be terminated.

3.3.5.3 *When Generated*

This primitive is generated by a SSS of a *S* or *ST* unit to request the termination of an existing connection.

3.3.5.4 *Effect of Receipt*

If the primitive is generated on the *ST* side, the receipt of this primitive causes the MAC to pass the request to the MAC entity in the *S* via the Dynamic Service Deletion Request message. The *S* checks the validity of the request, and if it is valid it terminates the connection. If the primitive is generated at *S*, it has already been validated and the MAC at *S* informs the *ST* by issuing a Dynamic Service Deletion Request message.

3.3.6 ***MAC_Terminate_CONNECTION.indication***

3.3.6.1 *Function*

This primitive is issued by the MAC entity on the non-initiating side to request the termination of a connection in response to the receipt of a Dynamic Service Deletion—Request message.

3.3.6.2 *Semantics of the service primitive*

The parameters of the primitive are as follows:

MAC_TERMINATE_CONNECTION.indication

```
(
Connection ID
)
```

The Connection ID parameter specifies which connection is to be terminated.

3.3.6.3 *When Generated*

This primitive is generated by the MAC sublayer when it receives a Dynamic Service Deletion—Request message to terminate a connection, or when it finds it necessary for any reason to terminate a connection.

3.3.6.4 *Effect of Receipt*

If the protocol was initiated at the *ST*, when it receives this primitive, the *S* checks the validity of the request. In any case, the receiving SSS returns the MAC_TERMINATE_CONNECTION.response primitive and deletes the CID from the appropriate polling and scheduling lists.

3.3.7 ***MAC_Terminate_CONNECTION.response***

3.3.7.1 *Function*

This primitive is issued by a SSS entity in response to a request for the termination of a connection.

3.3.7.2 *Semantics of the service primitive*

The parameters of the primitive are as follows:

MAC_TERMINATE_CONNECTION.response

(
 Connection ID,
 response code,
 response message
 sequence number
)

The Connection ID is returned to the requesting entity. The response code indicates success or the reason for rejecting the request. The response message provides additional information to the requester, in TLV format.

3.3.7.3 *When Generated*

This primitive is generated by the SSS entity when it has received a MAC_TERMINATE_CONNECTION.indication from its MAC sublayer.

3.3.7.4 *Effect of Receipt*

The receipt of this primitive causes the MAC sublayer to pass the message to the initiating side via the Dynamic Service Deletion—Response message. The initiating MAC in turn passes the CONFIRM primitive to the requesting convergence entity. The convergence entity shall no longer use this CID for data transmission

3.3.8 **MAC_Terminate_CONNECTION.confirmation**

3.3.8.1 *Function*

This primitive confirms to a convergence entity that a requested connection has been terminated.

3.3.8.2 *Semantics of the service primitive*

The parameters of the primitive are as follows:

MAC_TERMINATE_CONNECTION.confirmation

(
 Connection ID,
 response code,
 response message
 sequence number

) Parameters: see MAC_TERMINATE_CONNECTION.response.

3.3.8.3 *When Generated*

This primitive is generated by the MAC entity when it has received a Dynamic Service Deletion—Response message.

3.3.8.4 *Effect of Receipt*

The receipt of this primitive informs the convergence entity that a connection has been terminated. The convergence entity shall no longer use this CID for data transmission.

3.3.9 ***Changing a Connection***

The following primitives are used:

MAC_CHANGE_CONNECTION.request

MAC_CHANGE_CONNECTION.indication

MAC_CHANGE_CONNECTION.response

MAC_CHANGE_CONNECTION.confirmation

The semantics and effect of receipt of these primitives are the same as for the corresponding CREATE primitives, except that a new CID is not generated.

3.3.10 ***MAC_Data.request***

3.3.10.1 *Function*

This primitive defines the transfer of data to the MAC entity from a SSS SAP.

3.3.10.2 *Semantics of the service primitive*

The parameters of the primitive are as follows:

MAC_DATA.request

```
(
Connection ID,
length,
data,
discard-eligible flag,
encryption flag
)
```

The Connection ID parameter specifies the connection over which the data is to be sent; the service class is implicit in the Connection ID. The length parameter specifies the length of the MAC SDU in bytes. The data parameter specifies the MAC SDU as received by the local MAC entity. The discard-eligible flag specifies whether the MAC SDU is to be preferentially discarded in the event of link congestion and consequent buffer overflow. The encryption flag specifies that the data sent over this connection is to be

encrypted, if ON. No encryption is used, if OFF.

3.3.10.3 *When Generated*

This primitive is generated by a SSS whenever a MAC SDU is to be transferred to a peer entity or entities.

3.3.10.4 *Effect of Receipt*

The receipt of this primitive causes the MAC entity to process the MAC SDU through the MAC sublayer and pass the appropriately formatted PDUs to the PHY transmission SSS for transfer to peer MAC sublayer entities, using the CID specified.

3.3.11 **MAC_Data.indication**

3.3.11.1 *Function*

This primitive defines the transfer of data from the MAC to the SSS. The specific SSS to receive the indicate message is implicit in the CID.

3.3.11.2 *Semantics of the service primitive*

The parameters of the primitive are as follows:

MAC_DATA.indication

```
(
Connection ID,
length,
data,
reception status,
encryption flag
)
```

The Connection ID parameter specifies the connection over which the data was sent. The length parameter specifies the length of the data unit in bytes. The data parameter specifies the MAC SDU as received by the local MAC entity. The reception status parameter indicates transmission success or failure for those PDUs received via the MAC_DATA.indication.

3.3.11.3 *When Generated*

This primitive is generated whenever an MAC SDU is to be transferred to a peer convergence entity or entities.

3.3.11.4 *Effect of Receipt*

The effect of receipt of this primitive by a convergence entity is dependent on the validity and content of the MAC SDU. The choice of SSS is determined using the CID over which the MAC SDU was sent.

4 MAC DETAILED DESCRIPTION

The addressing, protocol actions at the ST and BS, and PDU formats (Protocol Data Units) are specified in this subsection. During the interaction between a ST and a BS, the MAC PDU(s) exchanged between them fall under three categories: (i) Network Initialization, (ii) Connection Management and (iii) Data Transport. All stations shall be able to properly construct PDU(s) for transmission and decode PDU(s) upon reception.

4.1 Addressing and connection identification

Each ST shall have a 48-bit universal MAC address. This address uniquely defines the ST from within the set of all possible vendors and equipment types. It is used during the registration process to establish the appropriate connections for an ST. It is also used as part of the authentication process by which the BS and ST each verify the identity of each other.

Connections are identified by a 16-bit Connection Identifier (CID). The use of a 16-bit CID permits a total of 64K connections within each downlink and uplink channel. The CID serves as a pointer to context and destination information. It is assigned even for nominally connectionless traffic like IP. The type of service may be implicitly specified in the CID itself. In order to avoid the overhead in creating and deleting the context for a CID, many higher-layer sessions may use the same CID over a period of time, sequentially one after another.

At ST initialization, two management connections in each direction (uplink and downlink) shall be established between the ST and the BS. These CID(s) shall be assigned in the Ranging Response messages and reflect the fact that there are inherently two different types of management traffic between an ST and the BS. One of them is the *basic CID*, used by the BS MAC and ST MAC to exchange short, time-urgent MAC management messages, such as ranging. The other is the *primary CID*, used by the BS MAC and ST MAC to exchange longer, more delay tolerant MAC management messages, such as creation of data connections. When the higher layer at BS or ST requests for a data connection as per one of the supported service flow types, a *data CID* is assigned by S to that connection. Since the MAC is connection-oriented, there are as many *data CID(s)* as there are active data connections, at any given point of time. The reason for having different types of CID(s) is mainly to facilitate the QoS scheduler. A scheduler could give different levels of importance to the messages in the queue(s) depending on the connection CID(s).

The format of the CID is shown in Figure 16. The first two bits implicitly identify the type of the CID: (00) implies it is a *basic CID*; (01) implies *primary CID*; both (10) and (11) imply *data CID*. In case of data CID,

the next two bits implicitly identify the type of the associated service flow: (00) for UGS, (01) for rtPS, (10) for nrtPS and (11) for BE. (The exact semantics of these types are defined in section 4.2).

Type of CID	Type of associated	Identifier
-------------	--------------------	------------

Figure 16: CID format

4.2 Bandwidth Request Grant Service

The following specifies how the uplink is scheduled for bandwidth requests from ST(s) and how bandwidth grants are provided to ST(s).

4.2.1 Types of services

WiFiRe provides following types of bandwidth request services:

- Unsolicited Grant Service:* The Unsolicited Grant Service (UGS) is designed to support real-time flows that generate fixed size data packets on a periodic basis, such as T1/E1 and Voice over IP without silence suppression. When a data CID is associated with UGS service flow type, the ST does not have to send periodic bandwidth request to the BS for that connection (data CID). The UGS service offers fixed size grants on a real-time periodic basis, which eliminate the overhead and latency of ST requests and assure that grants are available to meet the flow's real-time needs. The BS shall provide fixed size data grant slots at periodic intervals to the service flow. The UGS shall be specified using the following parameters: the Unsolicited Grant Size, the Nominal Grant Interval, the Tolerated Grant Jitter, and the Request/Transmission Policy.
- Real-time Polling Service:* The Real-Time Polling Service (rtPS) is designed to support real-time flows that generate variable size data packets on a periodic basis, such as MPEG video. The service offers real-time, periodic, unicast request opportunities, which meet the flow's real-time needs and allow the ST to specify the size of the desired grant. This service requires more request overhead than UGS, but supports variable grant sizes for optimum data transport efficiency. The BS shall provide periodic unicast request opportunities, by assigning appropriate *polling slots* in the uplink. The key service information elements are the Nominal Polling Interval, the Tolerated Poll Jitter, and the Request/Transmission Policy.
- Non real time Polling Service:* The Non-Real-Time Polling Service (nrtPS) is designed to support non real-time flows that require variable size data grant slots on a regular basis, such as high bandwidth FTP. The service offers unicast polls on a regular basis, which assures that the flow receives request opportunities even during network congestion. The BS typically polls nrtPS CIDs

on an interval (periodic or non-periodic). The BS shall provide timely unicast request opportunities by assigning appropriate *polling slots* in the uplink. The key service elements are Nominal Polling Interval, Minimum Reserved Traffic Rate, Maximum Sustained Traffic Rate, Request/Transmission Policy, and Traffic Priority.

- *Best Effort Service*: The intent of the Best Effort (BE) service is to provide efficient service to best effort traffic. Request/Transmission Policy setting should be such that the ST is allowed to use contention request opportunities. The key service elements are the Minimum Reserved Traffic Rate, the Maximum Sustained Traffic Rate, and the Traffic Priority.

4.2.2 Types of Grants

Regarding the grant of the bandwidth requested, there are three modes of operation:

- *Grant per Connection mode (GPC)*: In GPC, the BS grants bandwidth explicitly to each connection.
- *Grant per Subscriber Terminal mode (GPST)*: In GPST, the bandwidth is granted collectively to all the connections belonging to an ST. This allows for smaller UL-MAP(s) and provides freedom to ST to make real-time scheduling decisions and perhaps utilize the bandwidth differently than it was originally granted by the BS.
- *Grant per Service Flow type (GPSF)*: GPST is an intermediate between GPC and GPST. In GPST, the bandwidth is granted collectively to all the connections *of a particular flow type* belonging to an ST. This avoids the need for transmitting a detailed UL-MAP as in GPC. It also avoids the need for a complex scheduler at ST as in GPST.

The BS and ST exchange capabilities and agree upon the type of grant mechanism during registration. Also, in case of GPC or GPSF, the BS uses the ST-id field in the UL-MAP to inform the ST about the CID or flow type for which it has allocated slots in the uplink.

4.2.3 Polling process

Polling is the process by which the BS allocates bandwidth to the ST(s), specifically for the purpose of making bandwidth requests. These allocations may be to an individual connection at an ST, a group of connections at an individual ST or to a group of ST(s). These are indicated as Polling Slots in the UL-MAP.

When a connection is polled individually, no explicit message is transmitted for polling it. Instead, the ST is allocated (in the UL-MAP), sufficient bandwidth in order to transmit a bandwidth request for that connection. If the ST does not need bandwidth for that connection, it returns stuff bytes (0xFF).

When a ST is polled individually, no explicit message is transmitted for polling it. Instead, the ST is allocated (in the UL-MAP), sufficient bandwidth in order to transmit a bandwidth request for some of its connections. ST decides the choice of connections based on the service flow type associated with them. If

the ST does not need bandwidth for any of its data connections, it returns stuff bytes (0xFF). ST(s) operating in GPST mode that have an active UGS connection of sufficient bandwidth shall not be polled individually unless they set the Poll Me (PM) bit in the header of a packet on the UGS connection. This saves bandwidth over polling all ST(s) individually. Similarly, a More Data (MD) bit is set in the header of an active uplink transmission whenever the ST wants to be polled for rtPS and nrtPS connections.

When the allocation is to a group of ST(s), it actually defines the bandwidth request polling slot(s) among that group. The BS may schedule one or more of the polling slot(s) in uplink to be shared by many ST(s) to transmit bandwidth requests. An ST may randomly choose one of these slots to transmit its request. In case the ST does not receive the bandwidth grant correspond to this request within a timeout, it assumes that there was a bandwidth request collision. In this case, a standard backoff algorithm is used. This backoff algorithm is similar to that defined for timed-out ranging and registration requests.

4.3 MAC PDU format

MAC PDU(s) are of the form illustrated in Figure 17. Each PDU shall begin with a fixed-length Generic MAC Header. The header may be followed by the Payload of the MAC PDU. If present, the Payload shall consist of zero or more sub-headers and zero or more MAC SDU(s) (Service Data Units). The payload information may vary in length, so that a MAC PDU may represent a variable number of bytes. A MAC PDU may contain a CRC (Cyclic Redundancy Check). The maximum size of a single MAC PDU is bounded by the maximum size payload accepted by the WiFi PHY. Larger MPDU(s) may be fragmented and transmitted.

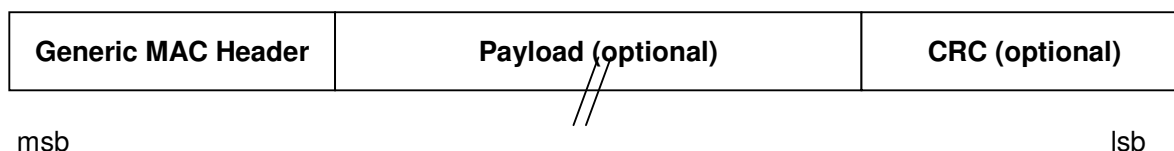


Figure 17: MAC PDU format

4.4 MAC header format

Two MAC header formats are defined – Generic MAC Header and Beacon Header. The Generic MAC Header is used for Management and Data PDU(s). The Beacon Header used to transmit a beacon message. The single-bit Header Type (HT) field distinguishes the Generic and Beacon Header formats. The HT field shall be set to zero for the Generic Header and to one for a Beacon Header. Additionally, there may be sub-Header(s) defined for packing multiple MAC SDU(s) into a single MAC PDU.

4.4.1 Generic MAC header

The fields of the Generic MAC header are as shown in Figure 18.

HT	Len	Type	CID	Reserved
-----------	------------	-------------	------------	-----------------

Figure 18: Generic MAC Header

Generic MAC header:

HT is 1 bit header type and is set to 0 for Generic MAC header.

Len is 7 bits and represents length of the MAC PDU including header length.

CID is 2 bytes and represents Connection to which the MPDU belongs to.

Reserved is 1 byte and is reserved for future use. It may carry information regarding presence or absence of CRC in the MPDU, authentication, encryption etc.

Type is 1 byte and has the following Values:

0x00 – no sub headers present

0x01 – sub header present

0x03- Management PDU of type Initial Ranging Request

0x04- Management PDU of type Initial Ranging Request Response

0x05- Management PDU of type Registration Request

0x06- Management PDU of type Registration Response

0x07- Management PDU of type Dynamic Service Addition Request

0x08- Management PDU of type Dynamic Service Addition Response

0x09- Management PDU of type Dynamic Service Change Request

0x10- Management PDU of type Dynamic Service Change Response

0x11- Management PDU of type Dynamic Service Deletion Request

0x12- Management PDU of type Dynamic Service Deletion Response

0x14 – MAC PDU with data Payload

4.4.2 Beacon header

The fields of the Beacon header are as shown in Figure 19.

HT	Len	Reserved
-----------	------------	-----------------

Figure 19: Beacon Header

Beacon Header

HT is 1 bit and the value is set to 1.

Len is 7 bits and represents length of the Beacon including header length.

Reserved is 1 byte and reserved for future use.

4.5 MAC Management PDU(s)

MAC Management messages are carried in the Payload of the MAC PDU. The type of MAC Management Message is specified in Type field of generic MAC header. MAC management messages on the Basic, Broadcast, and Initial Ranging connections shall neither be fragmented nor packed. MAC management messages on the Primary Management connection may be packed. MAC management messages shall not be carried on the data transport connections.

As mentioned earlier, the MAC procedures can be categorized mainly under: (i) Network Initialization, (ii) Connection Management and (iii) Data Transport. Each of these phases involves management messages to be exchanged between ST and S. The control plane includes (i) and (ii) while the Data plane includes (iii). These messages exchanged in these phases are described below. The detailed description of MAC procedures in ST and in S is provided in the subsequent sections.

4.5.1 Beacon Message

The format of the Beacon Message is as shown in Figure 20.

Header	Opr ID	Sys ID	BS ID	Rng Slot	DL MAP	UL MAP
---------------	---------------	---------------	--------------	-----------------	---------------	---------------

Figure 20: Beacon Message

Beacon

Header is the 2 bytes defined earlier.

Opr ID is a 1 byte value identifying the Operator of the network.

Sys ID is a 1 byte a value identifying the System (S).

BS ID is a 7 bits value identifying the BS in the System that is transmitting this Beacon.

DL-MAP is 50 bytes. It is a 50 element vector of <ST ID = (1 byte)>. ST ID = 0x11 value implies that the message in the corresponding DL slot is a broadcast message for all ST(s).

UL-MAP is 50 bytes. It is a 25 element vector of <ST ID = (1 byte), Slot id= (1 byte)>.

Rng Slot is a 1 bit indicating if there are any ranging blocks allocated in the UL-MAP. The value is set to 1 if any ranging block is present in the UL sub-frame, 0 otherwise. Ranging block information is transmitted in the first few entries of the DL-MAP. These entries are identified by a specific value in the ST ID field of the DL-MAP vector. Ranging block(s) (if present) are always the starting slot(s) of the UL. An ST-ID of all 1s is used to denote a ranging block, while an ST-ID of all 0's is used to denote a contention slot.

4.5.2 Network Initialization Messages

In addition to the Beacon, the management messages used in this phase are:

- 1) Initial Ranging Request
- 2) Initial Ranging Response
- 3) Initial Authentication Request
- 4) Initial Authentication Response
- 5) Registration Request
- 6) Registration Response

The PDU Formats for these messages are given along with the network initialization procedure in section 4.7.

4.5.3 Connection Management Messages

The management messages used in this phase are:

- 1) Dynamic Service Addition Request
- 2) Dynamic Service Addition Response
- 3) Dynamic Service Change Request
- 4) Dynamic Service Change Response
- 5) Dynamic Service Deletion Request
- 6) Dynamic Service Deletion Response

The PDU Formats for these messages are given along with the connection management procedure in section 4.8.

4.6 MAC Data PDU(s)

The format of the MAC Data PDU is as shown in Figure 21.

Gen. Header (5 bytes)	Sub Header (Optional)	Payload (MAC SDU(s)) (Maximum 2312 bytes)	CRC (optional)
---------------------------------	---------------------------------	---	--------------------------

Figure 21: MAC Data PDU

MAC Data PDU

Header is the 5 bytes Generic MAC header defined earlier.

Payload is the MSDU(s). On the uplink, multiple MSDU(s) of one or more data connections in a ST, may be packed into one MAC Data PDU. On the downlink, multiple MSDU(s) of one or more data connections to the *same or different ST(s)*, may be packed into one MAC Data PDU. The maximum size of a MSDU is 2312 bytes.

CRC is the (optional) cyclic redundancy check. The reserved bits in the Header are used to indicate the presence or absence of CRC.

4.7 Network Initialization sub-procedures

Network Initialization consists of Ranging, Authentication, and Registration sub-procedures. These are described below.

4.7.1 Ranging

Upon completion of power-up sequence and self-initialization, the ST enters the process of 'Ranging' in order to synchronize clock and other physical layer parameters with system S. This is important since the links can be over several Kilometers (RF propagation latency can be in the order of 50-100 micro-seconds). Ranging is also performed periodically so that the ST is kept in-sync with S.

The System S periodically transmits a *beacon*, having the structure described in section 4.5.1. An ST first listens for a beacon and then sends a *ranging request*. The System S then sends a *ranging response*. In the ranging response, the System S assigns the ST two connection-IDs (CIDs) called the *primary CID* and the *basic CID*. The primary CID is used for further exchange of management messages, while the basic CID is used for further periodic ranging exchanges. The detailed steps involved in ranging are as follows:

1. An ST in the Ranging phase detects the beacons from the System and Operator ID it is configured for. From the UL-MAP in the beacon, it determines the location of ranging block(s) in the UL sub-frame. Ranging block information is transmitted in the first few entries of the DL-MAP. Ranging block(s) if present, are always the starting slot(s) of the UL. These are identified by a specific value in the ST ID field of the UL-MAP vector. There should be at least one Ranging block per TMax seconds. Slotted ALOHA is to be used as the multiple access mechanism. A standard backoff mechanism is to be used in case of collision.
2. The ST constructs an Initial Ranging Request (IRR) PDU having the structure given below:

Initial Ranging Request:

MAC generic Header: with type field = 0x04

Operator ID : 1 byte

System ID: 1 byte

ST ID: 4 byte (MAC address)

BS ID 1: 1 byte

SignalStrength1 = 2 bytes

BS ID 2: 1 byte

SignalStrength2 = 2 bytes

BS ID 3: 1 byte

SignalStrength3 = 2 bytes

CID = 2 bytes

Bkoff = 1 byte

Field Description:

Operator ID is a configured value at ST indicating which operator the ST should associate with.

System ID is a configured value at ST indicating which System the ST should associate with.

ST ID is the MAC address of ST.

BS id 1/2/3 are the BS ID(s) which are audible from ST.

Signal Strength 1/2/3 are the signal strengths received by the ST from each BS.

CID is basic connection ID set to a fixed value for PDU(s) used for re-ranging. This is left as blank for first ranging request for an ST.

Bkoff contains the backoff time of the ST, in case the ST does not transmit immediately at the start of the ranging block.

3. After construction of the Initial Ranging Request PDU (IRR), the ST waits for the ranging contention slot. It transmits the IRR MAC PDU in the appropriate slot during the UL sub-frame. One or more ST(s) may transmit a 'Ranging Request' message in a ranging block.
4. Upon receiving the IRR PDU, the system S extracts the ST ID and signal strength measurements from the IRR PDU. It determines the best BS that the ST should be associated with and forms the Initial Ranging Request Response (IRRe) PDU. The structure of the IRRe PDU is given below:

Initial Ranging Response

MAC Header: with type field = 0x05

BS ID: 1 byte

Basic CID: 2 bytes; Primary CID: 2 bytes

Time Advance (T_{adv}) = 4 bytes

Field Description:

BS ID is the id of BS to which the ST should associate (register).

Basic CID is a connection id used for subsequent periodic ranging.

Primary CID is a connection id used for exchanging management messages.

T_{adv} is the time by which the ST is required to advance its slot timing. This is calculated as shown in Figure 11.

5. This IRRe PDU is transmitted in DL sub-frame in the ranging response slot (size = 1 slot). The BS first indicates the ranging response slot in DL-MAP entry \langle ST ID, Slot ID \rangle , where ST ID is the ID of the ST for which the response is being sent. The BS then waits for the appropriate DL-slot and transmits the IRRe PDU.
6. On the client side, the ST continues to scan DL sub-frame and read beacons. In order to find the IRRe PDU, it processes the DL-MAP in all the beacons it receives to determine if there is a targeted IRRe PDU for it. If it finds its ST ID in any of the DL-MAP, it identifies the corresponding ranging response slot and waits to receive the IRRe PDU in that DL-slot.
7. In case it does not find such a DL-MAP within a specific timeout period (T_{max-Rg}), it waits for a random amount of time (C_w) and transmits a IRR PDU once again. Since multiple ST(s) may perform ranging simultaneously, it is possible that the IRR PDU(s) collide. Hence the value for C_w is chosen from a window of C_w -Min and C_w -Max using a standard backoff algorithm. A flag is set in the IRR PDU to indicate that it is a retransmitted or duplicate request.
8. Ranging is complete when the ST is able to complete processing the IRRe PDU to determine the BS it should associate with, the timing advance value and record the primary and basic Connection ID. The primary CID is used for further exchange of management messages, while the basic CID is used for further periodic ranging exchanges.

Note: The ranging block(s) occur at the same time in the synchronized frames for all BS(s) of system S. All ST(s) will transmit their respective IRR packets using a contention resolution protocol. The IRR packet should contain the IDs of the BS beacons the ST is able to receive in decreasing order of signal strength. One or more BS will successfully receive the IRR packet transmitted by an ST. The BS then transmits the IRRe packet to the ST in the ranging response slot of the downlink sub-frame. The ST will continue to

transmit the IRR packet till such time as the BS whose beacon is the strongest received by the ST sends an IRRe packet, or till a specified timer expires.

Each time a BS receives the IRR packet from an ST, it measures the time delay from the start of the ranging block as determined by the System's slot clock to the arrival of the IRR packet. This requires the PHY to provide information about the time of arrival of a received packet. This could be a specific signal provided by the PHY, or it could be a measurement inferred from some other signal (e.g. the start of transfer of received data by the PHY) provided by the PHY. This measurement will have associated with it a margin of error $\pm m$ bits (@11 Mbps)

After the System receives the IRR, the System determines which BS to associate the ST with. This will normally be the strongest BS which successfully received the IRR, though this is not a must. The System will then register the ST to the BS it selects for the SS. Using the IRRe, the System will inform the ST about the timing advance (in number of bit periods at 11 Mbps) it must employ for uplink transmissions. Every ST will advance its uplink sub-frame by the number of bits specified in its timing advance.

The guard time between uplink transmissions from different ST(s) must be at least $2m$. This is best provided by ensuring that the last slot of an ST's transmission has at least $2m$ bits of silence at the end. Every ST can then start its transmission at the slot boundary, (after advancing the uplink sub-frame by the timing advance specified for it).

4.7.2 Authentication and Security

After Ranging, the ST authenticates itself to the S. The authentication process is required prior to registration. The process involves a authentication request from the ST, followed by multiple message exchange between the BS and ST depending on the authentication scheme chosen. The 802.1x authentication and security mechanisms shall be used. The primary CID will be used for any such exchange. Encryption and other privacy mechanisms may be required for the transfer of various PDU(s).

Mechanisms are provided for:

1. Mutual authentication between BS and a ST.
2. Encryption of the MSDU(s) and/or MPDU(s) by the LCS before they are transmitted over the air and decryption by the peer LCS. All the security services are performed in LCS and no SAP needs to be exported to SSS.

There are three possible security schemes:

- a) MAC based authentication and no encryption.

- b) Globally Shared key based WPA authentication and encryption.
- c) Pairwise Shared key base TKIP authentication and encryption.

While in option b) and c) both BS and ST authenticate each-other by way of a shared secret, we recommend that in option a) only the ST needs to authenticate itself to BS and the BS does not have to authenticate itself. This is because in our deployment scenario, a ST cannot communicate with multiple BS due to interference. Hence a ST will either get service or it will not. The reward for spoofing a BS is not high. Hence a ST may transact with any BS that is willing to provide it service.

The options b) and c) also provide for appropriate encryption schemes. The authentication process results in the initialization of the appropriate seed values, if any, for the chosen security scheme. In the initial stages of deployment, privacy concerns are not important in general and hence no encryption needs to be used. Any privacy concerns can be taken care of at application layer.

The steps involved in authentication are as follows:

1. ST constructs an Authentication Request PDU. The PDU has the following structure:

MAC Header: with type field set to Authentication Request (chosen in 4.3.1) and

CID = Primary CID for that ST.

MAC Address = 6 bytes - MAC address of the sender

Authentication Algorithm Identification = 1 byte.

Authentication Transaction Sequence No = 1 byte.

Len = 1 byte.

2. The Authentication PDU can be sent in the contention slot(s) allocated in UL sub-frame. These slots are indicated in the Beacon's UL-MAP, by the ST ID value 0x0. Since Authentication typically follows immediately after Initial Ranging, the scheduler may optionally allocate UL-slot(s) specifically to the ST, in the next frame(s). This is again indicated in the UL-MAP.

3. The MAC sub-layer of S receives the Authentication Request PDU and depending on the Authentication Algorithm, performs the authentication. This process may involve multiple message exchange with the ST. The structure of these messages is same as that described in step 1 above. The Authentication Transaction Sequence No is incremented at every step by both sides.

4. These Authentication Response PDUs are transmitted on the DL, in a manner similar to the Ranging Response (IRRe).

5. The ST processes the DL-MAP, identifies the corresponding authentication message slot and waits to receive the Authentication Response PDU in that DL-slot.
6. In case the ST does not receive the Authentication Response PDU within a specific timeout period, it performs a backoff in a manner similar to that defined for Ranging and retransmits the Authentication PDU with the duplicate flag set to 1. When the S receives an Authentication PDU with the duplicate flag set to 1, it simply processes the PDU again.
7. After successful authentication S associates the related authentication information with the primary CID. When new connections are created using this CID, they inherit the security parameters of the primary CID.
8. Authentication is complete when the ST receives a message from S with Authentication Result set to 'successful'.
9. In case of authentication failure, primary CID can be released and a warning logged.

Further detailed specifications of appropriate security sub-procedures are deferred to a later release.

4.7.3 Registration

Registration of and ST to S happens after ST is authenticated with S. Through this procedure, the ST informs the System S that it is entering the set of ST serviced by S. The link between S and ST is connection-oriented: one or more connections can be established for data exchange. The registration process is required prior to any data connection formation. The process involves a *registration request* from the ST, followed by a *registration response* from S. During this process, ST and S exchanges operational parameters and capabilities. This process enables the ST to communicate packet protocol specification such as IP version and acquire IP address from S for set up of provisioned connections. The detailed steps involved in registration are as follows:

1. ST constructs Registration Request (RegR) PDU to S. The PDU has the following structure:

Registration Request

MAC Header: with type field = 0x06 and CID = Primary CID for that ST.

IP version = 1 byte.

ParamSet = 38 bytes (44 bytes (one slot) – 5 bytes Header – 1 byte IP version).

Field Description:

The value of CID is set to the primary CID as received in the Ranging Response (IRRe).

IP Version is the IP version supported by ST.

Paramset is a Type-Length-Value parameter which can be used for representing operational parameters of ST. The data is byte-stream serialized and represented as type-value pairs.

2. The RegR PDU can be sent in the contention slot(s) allocated in UL sub-frame. These slots are indicated in the Beacon's UL-MAP, by the ST ID value 0x1. Since Registration typically follows immediately after Initial Ranging, the scheduler may optionally allocate UL-slot(s) specifically to the ST, in the next frame(s). This is again indicated in the UL-MAP.
3. The MAC sub-layer of S receives the RegR PDU and a) checks for appropriate version, b) Generates IP address and c) installs resource for provisioned connection. Thereafter it constructs the Registration Response (RegRe) PDU with following structure:

Registration Response

MAC Header: with type field = 0x07

IP Version: 1 byte; IP Address: 4/ 6 bytes

ParamSet: (44 – above) bytes

Field Description:

IP Version is required for ST to interpret the IP address correctly.

Paramset is a Type-Length-Value parameter which can be used for representing operational parameters of S. The byte stream is serialized data, represented as type value pair. The result (success or failure) of connection provisioning is given in the byte stream. In case of success, the duration of registration validity may be provided here.

4. This RegRe PDU is transmitted on the DL, in a manner similar to the Ranging Response (IRRe).
5. The ST processes the DL-MAP identifies the corresponding registration response slot and waits to receive the RegRe PDU in that DL-slot.
6. In case it does not receive the RegRe PDU within a specific timeout period, it performs a backoff in a manner similar to that defined for Ranging and retransmits the RegR PDU with the duplicate flag set to 1. When the BS receives a RegR PDU with the duplicate flag set to 1, it checks if it had received any valid RegR from the same ST. If yes, it simply retransmits the corresponding RegRe. Otherwise the same ST may get multiple IP addresses.
7. Registration is complete when the ST is able to process the RegRe PDU, determine its IP address

and the secondary CID assigned to it.

After completion of the registration process, a ST has an IP address, provisioned connections, active operation parameters and access to the network for future data communication. Now the ST may enter the connection request phase depending on connection demand from higher layers.

4.8 Connection Management sub-procedures

After registration, the ST can request for any number of further connections. A *connection request* from ST to S elicits a *connection response* from S to the ST. The number of connections may be restricted by S in an implementation specific fashion. The MAC is connection-oriented and data flow between BS and ST occurs as per the service flow type associated with that particular data flow. For example, a real-time VoIP data flow may be associated with one type of service flow while a best-effort TCP data flow may be associated with another type of service flow. The various types of service flows supported are described in section 4.2.

An active service flow is identified uniquely by a connection identifier (CID). There are two ways to create and change service flow with intended QoS parameters: a) create the connection with the desired QoS, using a Dynamic Service Addition message or b) create a generic connection (by specifying only the type of Bandwidth request service) and then use the CID to send Dynamic Service Change message to add specified QoS parameters to the connection. Thus, Connection Management consists of Service Addition, Change and Deletion sub-procedures.

4.8.1 Service Addition

This may also be termed as the Connection Creation phase. In this phase, the entity (BS or ST) wishing to create a data connection exchanges a management message which installs a CID at BS and informs the destination about the nature of bandwidth request service to be used with the connection. The destination responds with a either acceptance or rejection of the request. The detailed steps involved in service addition are as follows:

1. A ST wishing to create a data connection sends a Dynamic Service Addition Request (DSA-Req) PDU to the BS. The DSA-Req PDU has the following structure:

Dynamic Service Addition Request

MAC Header: with type field = 0x08 and CID as the primary CID for that ST.

CID: 2 bytes

QosParamSet = (44 – above) bytes

Field Description:

CID is Primary Connection ID for that ST.

QosParamSet is a Type-Length-Value parameter which can be used for representing QoS parameters for the requested connection.

- The BS processes the DSA-Req PDU, assigns a data CID and responds with a Dynamic Service Addition Response (DSA-Resp) PDU. The DSA-Resp PDU has the following structure:

Dynamic Service Addition Response

MAC Header: with type field = 0x09 and CID as primary CID for that ST.

CID: 2 bytes

Accpetd QosParamSet = (44 – above) bytes

Field Description:

CID is Data CID for admitted connection requested by ST.

Accpetd QosParamSet is a Type-Length-Value parameter which represents the allotted QOS parameters for the requested connection.

- If the BS is initiating a connection creation then it generates a data CID and sends a DSA-Req PDU containing this CID in the CID field and the QoS parameter description. The ST responds to this message with a DSA-Resp PDU containing same CID and acceptance of QoS parameters.

After this process, a data CID has been created for data transmission. Also, the BS knows the service flow type of the connection. Hence it can appropriately schedule slots in uplink for ST to send data as well as resource (slot) request messages for that connection.

Note that in case of flows such as TCP, the higher layer may request for a separate data connection ID in order to send the ACK(s). Otherwise the ACK(s) may be sent in the contention slots, leading to reduced TCP throughput.

4.8.2 Service Change

This may also be termed as the QoS Management phase. It is applicable to a new connection having a CID but not having any specified/allocated bandwidth resource. It is also applicable to an existing connection having some allocated resources but wanting a change in the allocation. The detailed steps involved in service change are as follows:

- The ST sends a Dynamic Service Change Request (DSC-Req) PDU to the BS. The DSC-Req PDU has the following structure:

Dynamic Service Change Request

MAC Header: with type field = 0x10

CID : 2 bytes

QosParamSet = 36 (44- 8) bytes

Field Description:

CID is Data Connection ID of the active connection.

QosParamSet is a Type-Length-Value parameter which represents the change required in QoS parameters for the connection.

2. The BS may admit or reject the request, depending upon the admission control scheduler. It then responds with a Dynamic Service Change Response (DSC-Resp) PDU. The DSC-Resp PDU has the following structure:

Dynamic Service Change Response

MAC Header: with type field = 0x11

CID : 2 bytes

AccpetdQosParamSet = 36 (44- 8) bytes

Field Description:

CID is Data Connection ID of the active connection.

QosParamSet is a Type-Length-Value parameter which represents change accepted in QoS parameters for the connection.

4.8.3 Service Deletion

This may also be termed as the Connection Termination phase. In this phase, the entity (BS or ST) wishing to terminate a data connection exchanges a management message to inform the peer entity. The steps involved in service deletion are as follows:

1. A ST wishing to terminate a data connection sends a Dynamic Service Deletion Request (DSD-Req) PDU to the BS. The DSD-Req PDU has the following structure:

Dynamic Service Deletion Request

MAC Header: with type field = 0x

CID : 2 bytes

ParamSet = 36 (44 – 8) bytes

Field Description:

CID is data Connection ID for the connection that is being terminated.

ParamSet may contain authentication information to guard against bogus deletion requests.

- The BS processes the DSD-Req PDU, releases the resources assigned to that data connection ID and responds with a Dynamic Service Deletion Response (DSD-Resp) PDU. The DSD-Resp PDU has the following structure:

Dynamic Service Deletion Response

MAC Header: with type field = 0x

CID : 2 bytes

Status = 36 (44 – 8) bytes

Field Description:

CID is Data Connection ID for connection being terminated.

Status is a Type-Length-Value parameter which represents the success or error flag as a result of the deletion.

- The BS may unilaterally decide to terminate a connection. In this case it simply sends a DSD-Req PDU to the ST. The ST responds to this message with a DSD-Resp PDU containing the status.

4.9 Data Transport sub-procedures

These include procedures for concatenation, fragmentation, ARQ and reassembly of data. They have been described in brief in sections 3.1.2 and 3.1.3 respectively.

Further detailed description of these sub-procedures is deferred to the next release.

4.10 Protocol Summary: State-Transition Diagrams

A high-level summary of the actions performed at the BS and ST is shown in Figure 22. A more detailed view of the ranging and registration process is shown in Figure 23.

Figure 24 represents the state transition diagram for the subscriber terminal (ST). Since ST may have limited battery power, it may go to power-saving mode. Hence, the initial state of ST is either ST_PowerOn, when the ST wakes up or the initial state is Idle, when ST is already 'on' and is waiting for some action to happen.

While in Idle state, ST can receive a notification that network layer has an IP packet to transmit. ST goes to ST_NetworkLayerHasPacketToSend state. It appends MAC header to the packet, does concatenation or fragmentation as required and adds the packet to the uplink traffic queue. ST transmits data and request while it is in ST_TransmitDataAndRequest state.

For the downlink sub-frame duration, ST PHY continuously listens to downlink channel to discover if there are any downlink packets intended for it. A message is sent by physical layer to notify the MAC for receiving a packet sent by the BS and the ST goes to ST_ReceivePacketFromPhy state. Downlink packets addressed to the ST are received and processed based on their type. Downlink and uplink control messages sent by BS on downlink channel are used for determining various control parameters for uplink and downlink channels. Downlink control message is decoded to determine start time of the frame, frame duration, etc. ST determines its uplink transmission time and duration of transmission in the current frame by decoding uplink control message. Downlink data packets are handed over to higher layer after removing MAC header.

Figure 25 represents the state transition diagram for the Base Station (BS). The initial state for BS is the Idle state. Periodically, BS transmits beacon by going to the BS_TransmitBeacons state.

When the PHY layer receives a packet from any ST, it notifies the MAC layer. BS goes to the BS_ReceivePacketFromPhy state. The packet is processed based on whether it is a data packet or a request packet. Uplink data packets handed to BS MAC layer are sent to higher layer after removing MAC header. Uplink bandwidth request packets are classified and placed in uplink grant queues.

On receiving a message from network layer for sending an IP packet, BS goes to the BS_NetworkLayerHasPacketToSend state and BS adds it to one of the downlink traffic queues. BS invokes the multi-sector scheduling algorithm by going to the BS_PerformMultiSectorScheduling state and constructs DL MAP and UL MAP that are sent in the next beacon. The data is transmitted in the appropriate DL slot. BS generates periodic request grants by going to the BS_GeneratePeriodicGrant state.



Figure 22: Summary of Actions

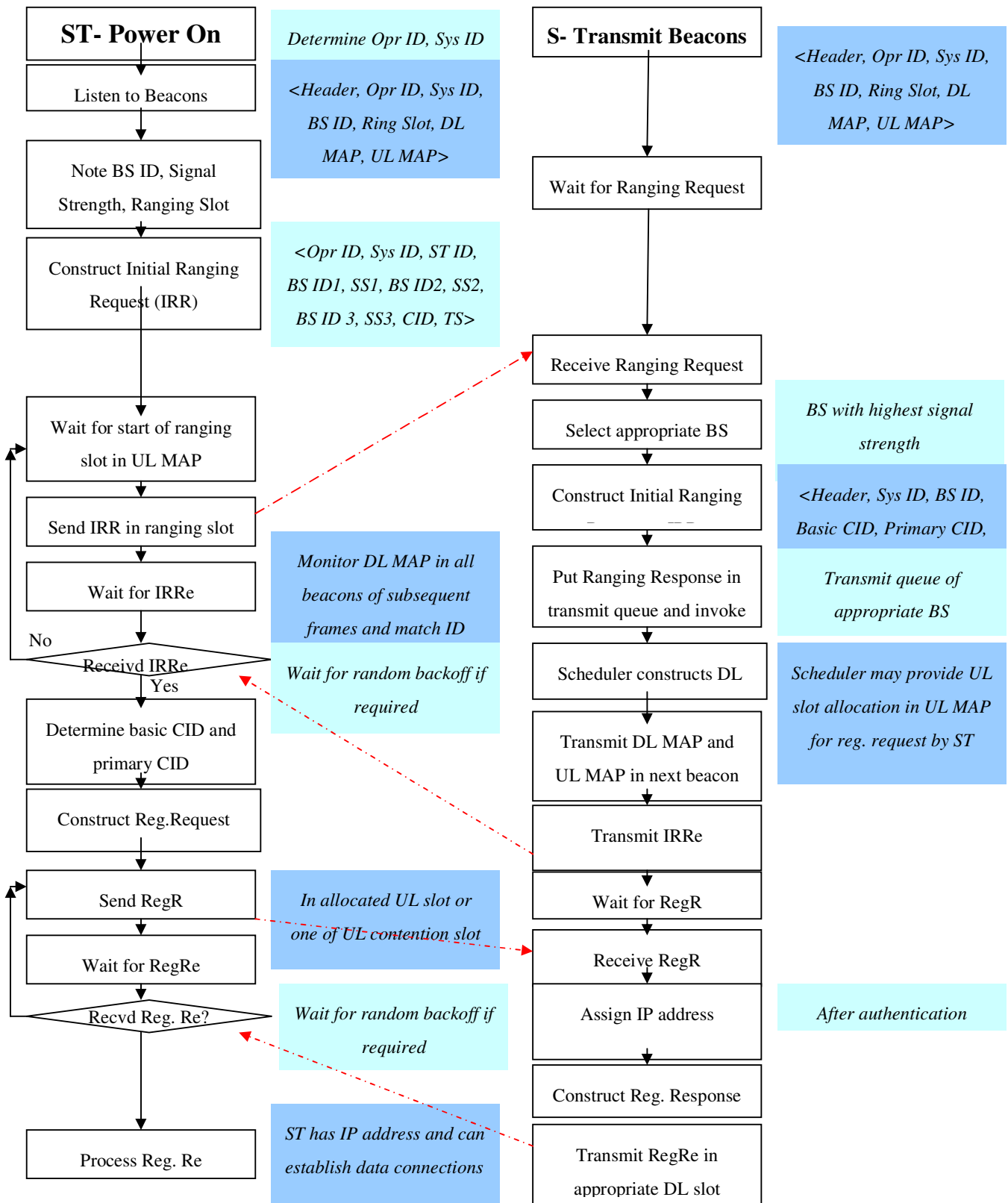


Figure 23: Ranging and Registration

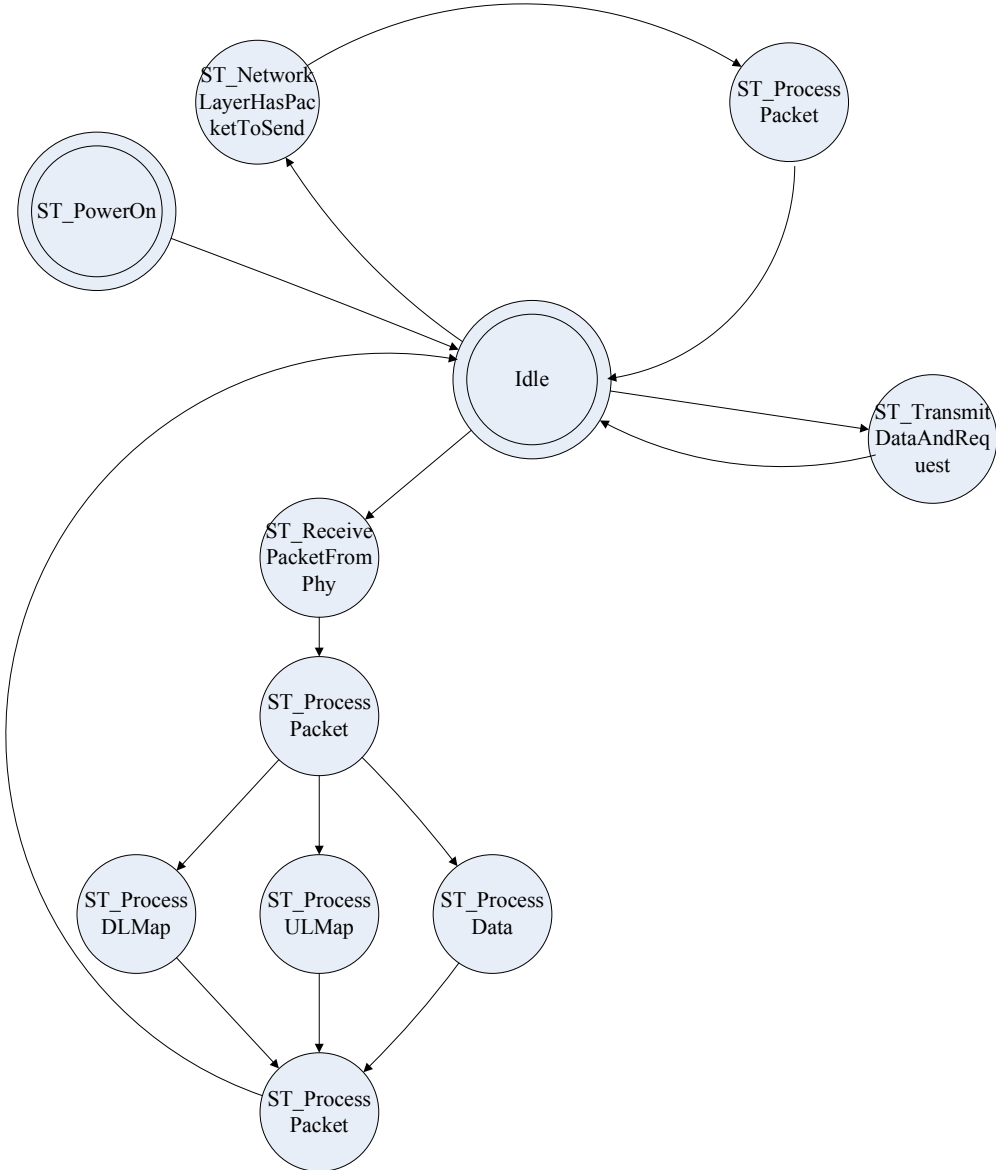


Figure 24: ST State-Transition Diagram

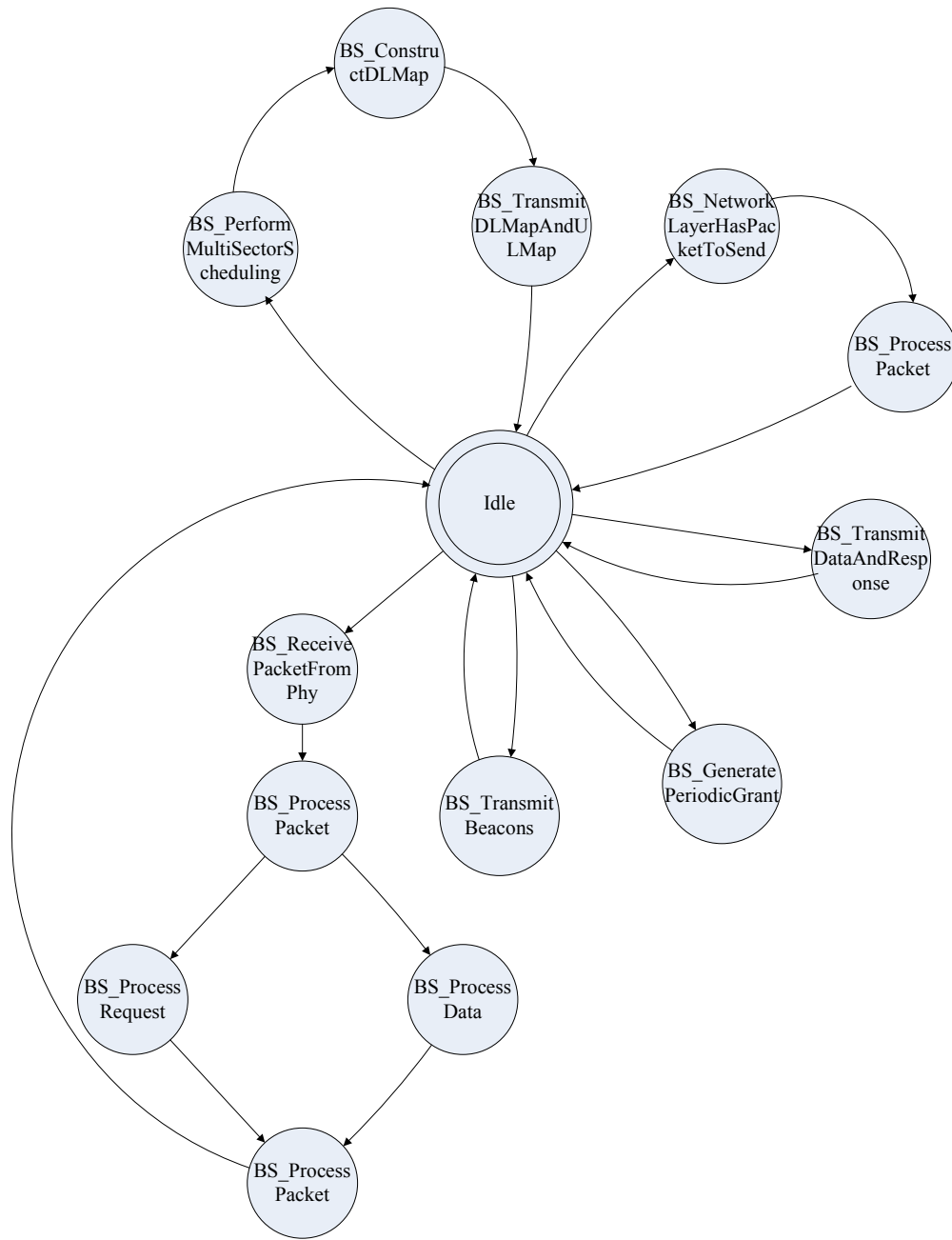


Figure 25: BS State-Transition Diagram

5 AUTHENTICATION AND PRIVACY

These mechanisms have been described in brief in section 4.7.2. Further detailed specification of the authentication and privacy mechanism is deferred to the next release.

6 MAC MANAGEMENT

This section describes the API(s) to be provided for configuring and management of a WiFiRe compliant device. This includes API(s) for setting the operator ID, system ID, WiFi channel, slot duration, frame duration, authentication parameters, encryption keys etc.

The detailed specification of the MAC management API(s) is deferred to the next release.

7 PHY SERVICE SPECIFICATION AND MANAGEMENT

The PHY is identical to the IEEE 802.11b Direct Sequence Spread Spectrum (DSSS). The PHY services used by the WiFiRe MAC are:

1. **PHY-DATA.request:** Issued by MAC to transfer data from the MAC sublayer to the local PHY entity.
2. **PHY-DATA.confirm:** Issued by PHY to confirm transfer data from the MAC sublayer to the local PHY entity.
3. **PHY-DATA.indication:** Issued by PHY to transfer data from the PHY sublayer to the local MAC entity.
4. **PHY-TXSTART.request:** Issued by MAC sublayer to local PHY entity to start the transmission of an MPDU.
5. **PHY-TXSTART.confirm:** Issued by PHY to confirm the start of transmission of an MPDU.
6. **PHY-TXEND.request:** Issued by MAC sublayer to local PHY entity to complete the transmission of the current MPDU.
7. **PHY-TXEND.confirm:** Issued by PHY to confirm completion of transmission of the current MPDU.
8. **PHY-RXSTART.indication:** Issued by PHY sublayer to local MAC entity to indicate receipt of a valid start frame delimiter.
9. **PHY-RXEND.indication:** Issued by PHY sublayer to local MAC entity to indicate that the MPDU currently being received is complete.

8 GLOSSARY OF TERMS

8.1 Abbreviations and Acronyms

ACK	acknowledgment
ARQ	automatic repeat request
BE	best effort
BR	bandwidth request
BS	base station
BSID	base station identification
BWA	broadband wireless access
C/I	carrier-to-interference ratio
C/N	carrier-to-noise ratio
CRC	cyclic redundancy code
CS	carrier sense
CSMA	carrier sense multiple access
DA	destination address
DCF	distributed co-ordination function
DL	downlink
DL-MAP	downlink slot allocation map
DL-TB	downlink transport block
DLL	data link layer
DSSS	direct sequence spread spectrum
ETSI	European Telecommunications Standards Institute
GPC	grant per connection
GPSF	grant per service flow type
GPST	grant per subscriber terminal
ID	identifier
IETF	Internet engineering task force
IFS	Inter frame space
IP	Internet protocol
LAN	local area network
LLC	logical link control
LoS	line of sight
MAC	medium access control layer
MAN	metropolitan area network

nrtPS	non-real-time polling service
PBR	piggyback request
PCF	point co-ordination function
PDU	protocol data unit
PHY	physical layer
PoP	point of presence
PS	physical slot
PSH	packing subheader
QoS	quality of service
RF	radio frequency
RSSI	received signal strength indication
rtPS	real-time polling service
Rx	reception
SAP	service access point
SDU	service data unit
SF	service flow
ST	subscriber terminal
TCP	transmission control protocol
TDD	time division duplex
TDM	time division multiplex
TDMA	time division multiple access
Tx	transmission
UDP	user datagram protocol
UE	user equipment
UGS	unsolicited grant service
UL	uplink
UL-MAP	uplink slot allocation map
UL-TB	uplink transport block
VoIP	voice over IP
WAN	wide area network
WDM	wireless distribution media
WDS	wireless distribution system
WiFi	wireless fidelity
WiMax	wireless microwave access

8.2 Definitions

1. **access control:** The mechanisms to prevent unauthorized usage of resources.
2. **authentication:** The service used to establish the identity of a subscriber terminal (ST) to the base station (BS) and vice versa.
3. **base station (BS):** The equipment used for providing wireless connectivity, management, and control of the subscriber terminals. It typically has a sectorized antenna.
4. **beacon:** A control packet transmitted by the BS at the start of every time frame.
5. **broadband:** Having bandwidth greater than 1 MHz and supporting data rates more than 256 Kbit/s.
6. **broadcast address:** A unique multicast address that specifies all ST(s).
7. **cell:** A set of co-located BS that provide wireless service to a given geographical area.
8. **channel:** An instance of medium use for the purpose of passing protocol data units (PDUs).
9. **concatenation:** The act of combining multiple medium access control (MAC) PDU(s) into a single time division multiplex (TDM) burst.
10. **connection:** A unidirectional mapping between BS and ST MAC layer peers for the purpose of transporting a service flow's traffic. All traffic is carried on a connection, even for service flows that implement connectionless protocols, such as internet protocol (IP). Connections are identified by a connection identifier (CID).
11. **connection identifier (CID):** Identifies a connection uniquely. It maps to a *service flow identifier* (SFID), which defines the quality of service (QoS) parameters of the service flow associated with that connection.
12. **deauthentication:** The service that voids an existing authentication relationship.
13. **downlink:** The direction from the base station (BS) to the subscriber terminal (ST).
14. **downlink map (DL-MAP):** Defines the mapping between ST identifier and slot start times for traffic sent on the downlink.
15. **dynamic service:** The set of messages and protocols that allow the base station and subscriber terminal to add, modify, or delete the characteristics of a service flow.
16. **frame:** A periodic, fixed duration, structured data transmission sequence. A frame contains both an uplink subframe and a downlink subframe.
17. **grant per connection (GPC):** A bandwidth allocation method in which grants are allocated to a specific connection within a ST. Note that bandwidth requests are always made for a connection.
18. **grant per service flow (GPSF):** A bandwidth allocation method in which grants are aggregated for all connections of the same service flow type, within a subscriber terminal.
19. **grant per subscriber terminal (GPST):** A bandwidth allocation method in which grants are

aggregated for all connections within a subscriber terminal and are allocated to the subscriber terminal as that aggregate.

- 20. MAC protocol data unit (MPDU):** The unit of data exchanged between two peer MAC entities using the services of the physical layer (PHY).
- 21. MAC service data unit (MSDU):** Information that is delivered as a unit between MAC service access points (SAPs).
- 22. multicast:** A medium access control (MAC) address that has the group bit set.
- 23. packing:** The act of combining multiple service data units (SDUs) from a higher layer into a single medium access control protocol data unit (PDU).
- 24. privacy:** The service used to prevent the content of messages from being read by other than the intended recipients.
- 25. ranging:** The service used by a subscriber terminal (ST) to notify the base station (BS) of its presence in the network.
- 26. registration:** The service used to establish mapping between ST and BS and enable ST to invoke the system services.
- 27. rural area:** An area about 15-20 Km radius, having a low density population.
- 28. service access point (SAP):** The point in a protocol stack where the services of a lower layer are available to its next higher layer.
- 29. slot:** A unit of time for allocating bandwidth.
- 30. station (ST):** Any device that contains a WiFiRe conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM). It typically has a directional antenna.
- 31. time division duplex (TDD):** A duplex scheme where uplink and downlink transmissions occur at different times but may share the same frequency.
- 32. time division multiplex (TDM):** A scheme where the total number of available time slots are shared between multiple transmitters and receivers.
- 33. unicast:** A PDU that is addressed to a single recipient, not a broadcast or multicast.
- 34. uplink:** The direction from a subscriber terminal to the base station.
- 35. uplink map (UL-MAP):** Defines the mapping between ST identifier and slot start times for traffic on the uplink, for a scheduling interval.
- 36. wireless medium (WM):** The medium used to implement the transfer of protocol data units (PDUs) between peer physical layer (PHY) entities.