Brief of Access Point's Operation Theorem

Introduction:

The IEEE 802.11 specification is a wireless LAN standard developed by IEEE (Institute of Electrical and Electronic Engineering) committee in order to specify an "over the air" interface between a wireless client and a base station or Access Point, as well as among wireless clients. Two network topologies are defined:

-Infrastructure is a kind of network architecture for providing communication between wireless clients and wired network resources via an Access Point (AP). AP is a device that coexists IEEE 802.3 (Ethernet) and IEEE 802.11 (wireless LAN) architectures. The coverage area of an infrastructure wireless LAN is defined by its AP and associated wireless clients, and together all the devices from a Basic Service Set (BSS). When an AP is present within a BSS, all transmissions only between clients and AP. Clients communicate with AP directly and AP then determines where to send these frames: to another clients in the BSS or to wired network terminals. In other words, all beacons are used for synchronization are transmitted by AP in an infrastructure wireless LAN.

-Ad-Hoc network is an architecture that is used to support mutual communication among wireless clients without access point and independents from other LANs.

In order to compatible with different upper layers, the IEEE 802.11 specification is like the IEEE 802.3 Ethernet and 802.5 Token Ring standards addresses both the Physical (PHY) and Media Access Control (MAC) layers.

Physical Layer (PHY):

An AP that is a bridge between a wireless LAN and the wired network has two physical layers: IEEE 802.3 (Ethernet) PHY and IEEE 802.11 (wireless LAN) PHY. Ethernet that is a popular and used widely network standard almost follows IEEE 802.3 standard. We will not mention to 802.3 PHY detail. On the other hand, IEEE 802.11 standard provides three physical characteristics for wireless local area networks: Infrared (IR), Direct Sequence Spread Spectrum (DSSS), and Frequency Hopping Spread Spectrum (FHSS). Actually, only DSSS and FHSS have any significant presence in the market. The DSSS and FHSS PHY options operate in the 2.4 GHz ISM band, a global band primarily set aside for industrial, scientific and medical use, but can be used for operating wireless LAN devices without the need for end-user licenses. The FCC established the operating rules specifically to facilitate

shared use of the band for the transmission of data and voice by multiple users in an unlicensed environment. Where DSSS was designed specifically to conform to FCC regulations (FCC 15.247) and it uses DBPSK (1 Mbps) DQPSK (2 Mbps). The draft text of high-speed extension of the IEEE802.11 Standard specifies Complementary Code Keying (CCK) as the modulation scheme for 5.5 and 11Mbps data rates in the 2.4GHz band. FHSS uses 2GFSK and 4GFSK as the modulation scheme for 1 and 2 Mbps individually.

Media Access Control Layer (MAC):

AP combines 802.3 MAC and 802.11 MAC and provides the service of transformation between different standards' frame formats. As the description in PHY section, we will not mention to 802.3 MAC detail and only brief the interaction between 802.3 and 802.11 MACs. The IEEE 802.11 MAC layer, supported by an underlying PHY layers, is concerned primarily with rules for accessing the wireless medium. The primarily services provided by the MAC layer of AP are as follow:

-Association
When a client enters the range of a wireless LAN initially, this service enables the establishment of wireless links between wireless clients and APs in Infrastructure Networks.

-Reassociation
This takes place in addition to association when a wireless client moves from one Basic Service Set (BSS) to another. Two adjoining Basic Service Sets form an Extended Service Set (ESS) if they are defined by a common ESSID. If a common ESSID is defined, a wireless client can roam from one BSS to another. Although reassociation is specified in 802.11, the mechanism that allows AP-to-AP coordination to handle roaming is not specified.

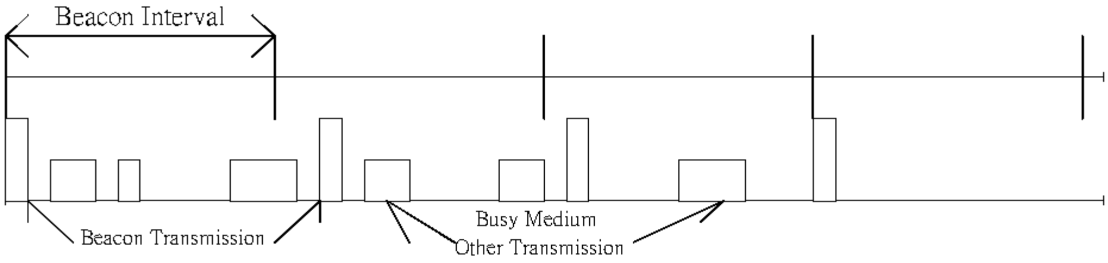
-Authentication
Authentication is the process of proving a client identity, and in IEEE 802.11 this process takes place prior to a wireless client associating with an AP. By default, IEEE 802.11 devices operate in an Open System, where essentially any wireless client can associate with an AP without the checking of credentials. True authentication is possible with the use of the IEEE 802.11 option known as Wired Equivalent Privacy

or WEP, where a Shared Key is configured into the AP and its wireless clients. Only those devices with a valid Shared Key will be allowed to be associated to the AP.

-Data transfer
Wireless clients use Distributed Coordination Function (DCF) mode for asynchronous data service and optional Point Coordination Function (PCF) mode for time bounded services**.** Under DCF mode, each client should follow a Collision Sense Multiple Access with Collision Avoidance (CSMA/CA) algorithm as the media access scheme. AP also has to follow this method under DCF mode. Optional RTS / CTS pair of control frames exchange between transmitter and receiver will reserve the medium for subsequent data access and reduce "Hidden Node" problem. In an infrastructure wireless LAN, AP should deals with two kinds of frame formats (one is 802.3 frame, the other is 802.11 frame) and may transform them. All clients only communicate with AP directly and frames only sent between clients and AP. According to the information of frame header, AP then relays frames to another client in the BSS or wired terminal. AP also relays frames from Ethernet to wireless LAN clients. A frame that is relayed between Ethernet and wireless LAN must be separated into header and Data Frame Body first. According to the information of header, AP's MAC then transfers one header type to the other header type secondly. AP's MAC puts Data Frame Body into the new header as a new frame finally, then the new frame will be sent into proper network.

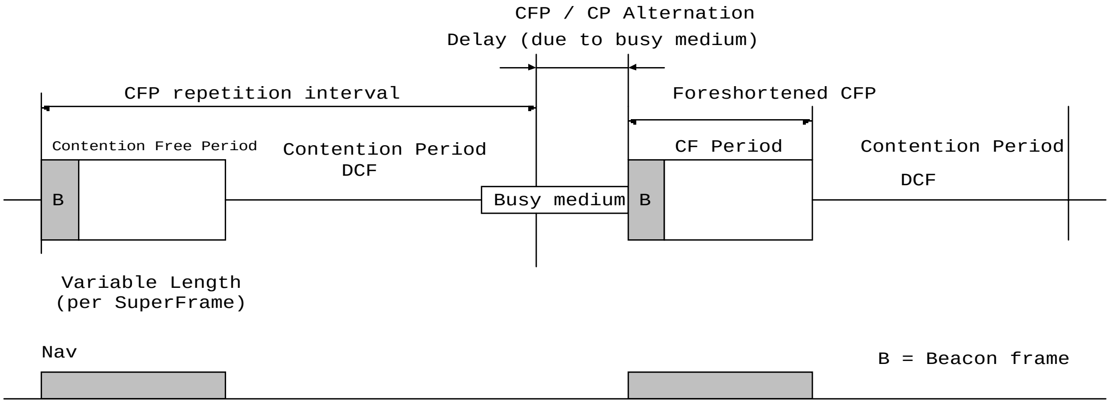
-Beacon

The AP shall define the timing for the entire BSS by transmitting beacons according to the aBeaconPeriod attribute within a AP. A beacon includes the information of Timestamp, Beacon interval, SSID, Supported rates, traffic indication map (TIM) and so on. Though the transmission of a beacon may be delayed because of CSMA deferrals, subsequent beacons shall be scheduled at the nominal beacon interval.

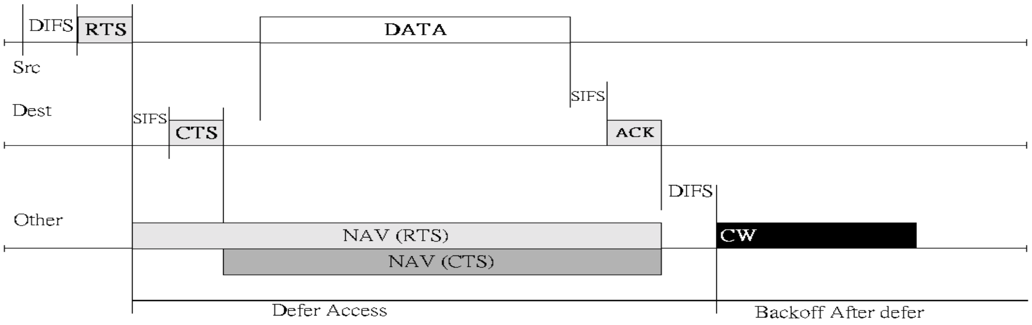


-Operation Scheme

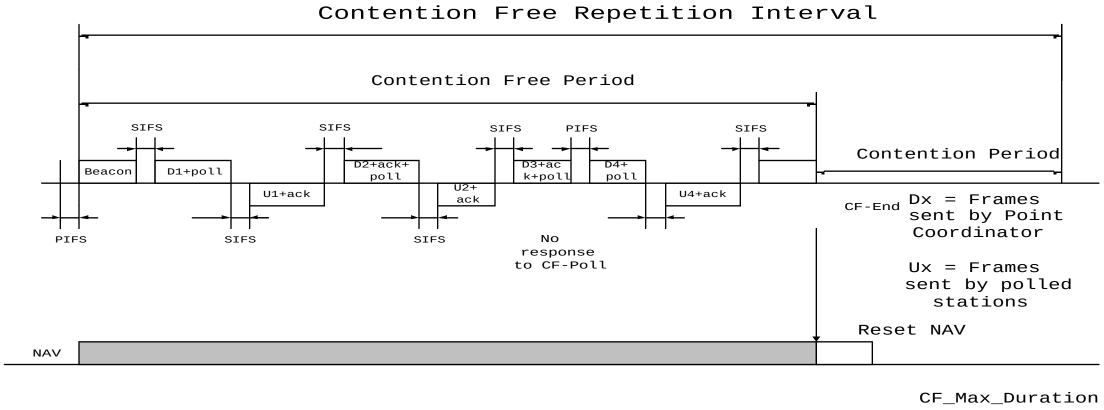
Contention Free Period (CFP) repetition interval consists of DCF and PCF durations and begins at PCF duration if PCF mode was used. The beacon that polls all clients enters PCF mode will be delayed due to the busy medium of last DCF duration.



In a wireless LAN under DCF mode, a client that wins the medium and uses RTS/CTS mechanism, the LAN has the time schedule as follow. Except Src and Dest, all the other clients stay at idle state in Network Allocation Vector (NAV) duration.

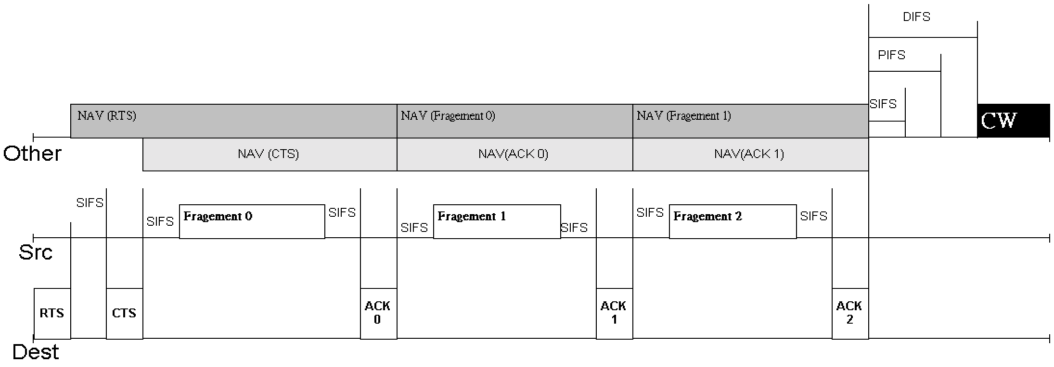


In PCF mode, PC (AP) sends polls to pollable clients according to polling scheme. Some of the poll frames include data inside and a pollable client then transmits a data frame include acknowledge. If PC sends a poll but and doesn't get a ACK frame, it will sends next poll while medium is free over a PIFS duration.



-MSDU fragmentation and reassembly

A data stream that is from LLC layer and serviced by MAC layer is called MAC Service Data Unit (MSDU). If the data frame is too long, it will be fragmented into several smaller frames. Then these smaller frames will be ordering and packaged into many MAC package data units (MPDUs) individually. MSDU is assembled by these ordering MPDUs. According to the order of MPDUs, the MAC layer of destination can reassemble the MSDU. It provides LLC to exchange MAC Service Data Units.



-Security Services by WEP

By default, data is transferred “in the clear” ; any 802.11-compliant device can potentially eavesdrop like-PHY 802.11 traffic that is within range. The WEP option encryption algorithm known as RC4 . The same Shared Key used in authentication is used to encrypt or decrypt the data; thus only wireless clients with the exact Shared Key can correctly decipher the data.