Brief Tutorial on IEEE 802.11 Wireless LANs

Application Note February 1999 AN9829

Authors: Jim Zyren and Al Petrick

Introduction

Final approval of the IEEE 802.11 standard for wireless local area networking (WLAN) last year and rapid progress made toward higher data rates have positioned this technology to fulfill the promise of truly mobile computing. While wired LANs have been a mainstream technology for at least fifteen years, WLANs are uncharted territory for most networking professionals. There are some important differences worth explaining.

When considering wireless networking, some obvious questions come to mind:

How can WLANs be integrated with wired infrastructure?

What is the underlying radio technology

How is multiple access handled?

What about network security?

These are just a few of the issues addressed by the standard. IEEE 802.11 is limited in scope to the PHY layer and MAC sublayer. The following overview touches on some of the salient differences between wired and wireless LANs and should answer some of the questions facing MIS professionals evaluating WLAN technology.

Network Topology

The basic topology of an 802.11 network is shown in Figure 1. A Basic Service Set in its simplest form consists of two or more wireless nodes, or stations (STAs), which have recognized each other and have established communications. This situation has a special designation, namely the Independent BSS (IBSS). Within an IBSS, STAs communicate directly with each other on a peer-to-peer level. This type of network is often formed on a temporary basis, and is commonly referred to as an ad hoc network.

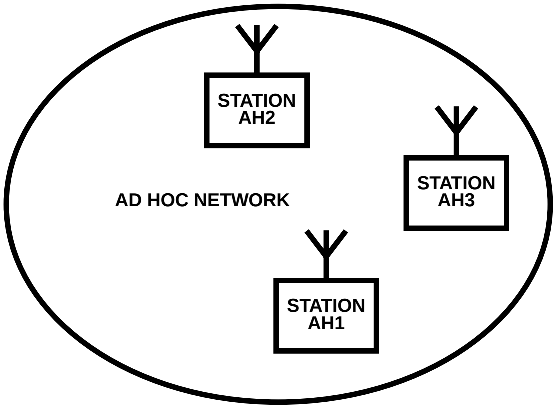

FIGURE 1. PEER-TO-PEER COMMUNICATIONS IN AD HOC NETWORK

A more common and far more and flexible configuration is that of a BSS which contains an Access Point (AP). The main function of an AP is to form a bridge between wireless and wired LANs. When an AP is present within a BSS, STAs do not communicate on a peer-to-peer basis. Instead, all communications between STAs or between an STA and a wired network client go through the AP. APs are not mobile, and form part of the wired network infrastructure. A BSS in this configuration is said to be operating in the infrastructure mode.

The Extended Service Set (ESS) shown in Figure 2 consists of a series of BSSs (each containing an AP) connected together by means of a Distribution System (DS). Although the DS could be any type of network (including a wireless network), it is almost invariably an Ethernet LAN. Within an ESS, STAs can roam from one BSS to another and communicate with any mobile or fixed client in a manner which is completely transparent in the protocol stack above the MAC sublayer. The ESS enables coverage to extend well beyond the range of a WLAN radio. By using an ESS, seamless campus-wide coverage is possible.

Radio Technology

The IEEE 802.11 standard actually provides for three variations of the PHY. These include Direct Sequence Spread Spectrum (DSSS), Frequency Hopped Spread Spectrum (FHSS), and Infrared (IR). In practice, only the first two, DSSS and FHSS, have any significant presence in the market. The DSSS and FHSS PHY options were designed specifically to conform to FCC regulations (FCC 15.247) for operation in the 2.4GHz ISM band. The 2.4GHz ISM band is particularly attractive because it enjoys worldwide allocations for unlicensed operation, as summarized in Table 1.

TABLE 1. GLOBAL SPECTRUM ALLOCATION AT 2.4GHz

REGION	ALLOCATED SPECTRUM
US	2.4000 – 2.4835GHz
Europe	2.4000 – 2.4835GHz
Japan	2.471 - 2.497GHz
France	2.4465 - 2.4835GHz
Spain	2.445 - 2.475GHz

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. It therefore stipulated the use of either DSSS or FHSS modulation when radiating in excess of roughly 0dBm (1mW). Both FHSS and DSSS PHYs currently support 1Mbps and 2Mbps. However, 802.11 recently adopted a proposal for a waveform which will enable the DSSS PHY to provide data rates up to 11Mbps. Final approval of the high rate extension to the DSSS PHY is expected by mid 1999. Point-to-point network bridges supporting 11Mbps are already available.

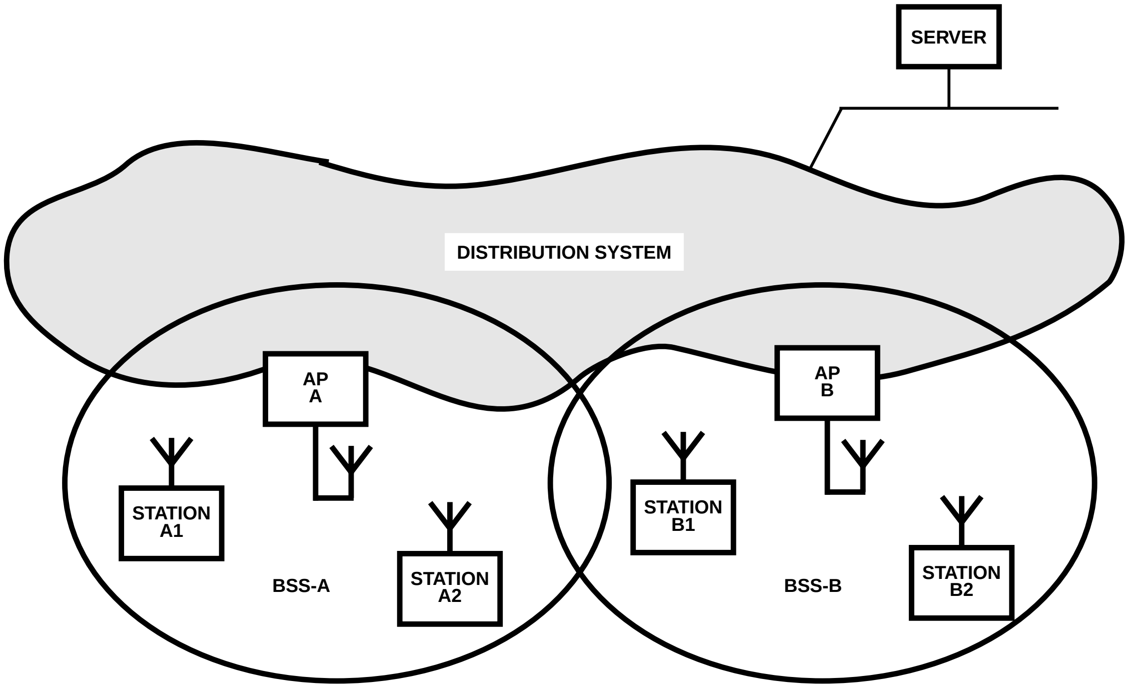

FIGURE 2. ESS PROVIDES CAMPUS-WIDE COVERAGE

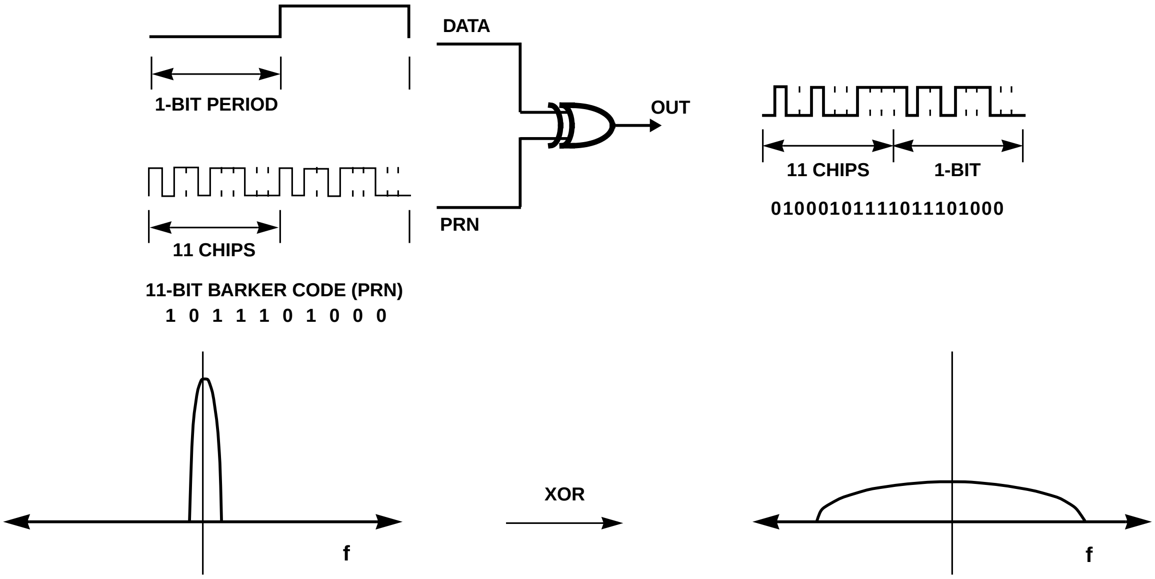

FIGURE 3. DSSS DATA AND BARKER SEQUENCE ARE COMBINED VIA XOR FUNCTION

DSSS is the same technology used in GPS satellite navigation systems and in CDMA cellular telephones, though IEEE 802.11 does not employ Code Diversity Multiple Access, as will be explained in more detail. In a nutshell, the data stream is combined is via an XOR function with a high-speed pseudo-random numerical sequence (PRN) as shown in Figure 3. The PRN specified by 802.11 is an 11 chip Barker Code. The term “chip” is used instead of “bit” to denote the fact that the Barker Code does not carry any binary information by and of itself. The result is an 11Mbps digital stream which is then modulated onto a carrier frequency using Differential Binary Phase Shift Keying (DBPSK).

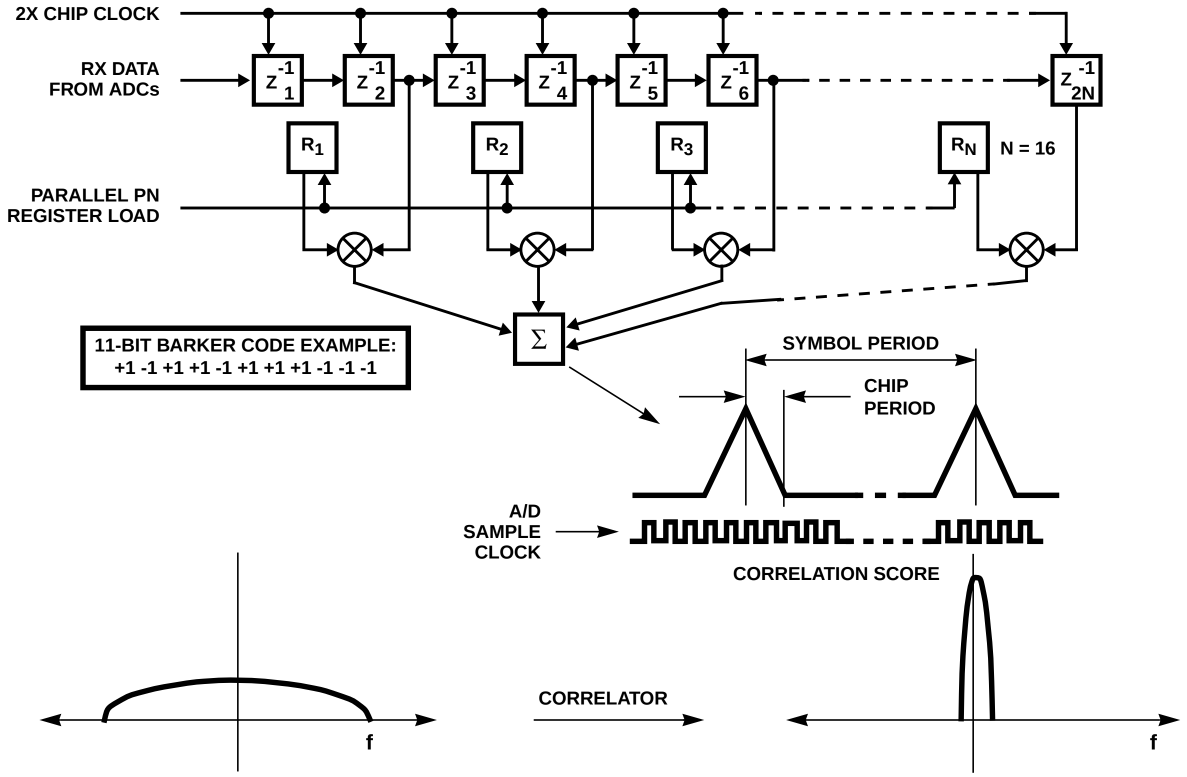

FIGURE 4. RX SIGNAL IS CORRELATED WITH PRN TO RECOVER DATA AND REJECT INTERFERENCE

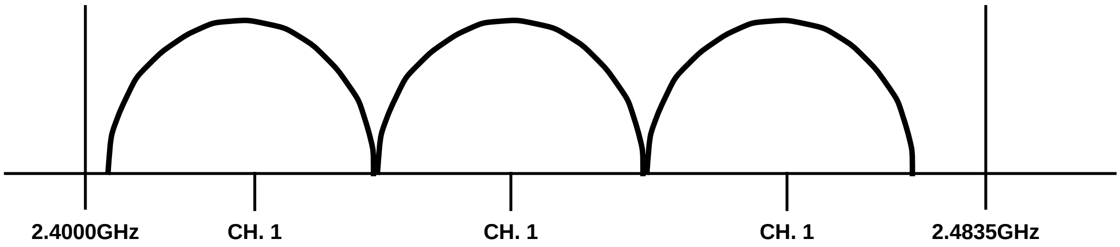

FIGURE 5. THREE NON-OVERLAPPING DSSS CHANNELS IN THE ISM BAND

As shown in Figure 3, the effect of the Barker sequence is to spread the transmitted bandwidth of the resulting signal by a ratio of 11:1 (thus the term, “spread spectrum”). At the same time, the peak power of the signal is reduced by an identical ratio. Note however, that the total power is unchanged. Upon reception, the signal is demodulated and the 11Mcps binary stream is recovered. Bit decisions are made by correlating this binary stream with the same 11 chip Barker code. During this process, the original bandwidth and peak power are restored. The correlation process has a significant benefit, it reduces the level of narrow band interference which falls in band by the same 11:1 ratio. This effect is known as processing gain.

DSSS radios use DBPSK at 1Mbps and Differential Quadrature Phase Shift Keying (DQPSK) at 2Mbps. The channel bandwidth is about 20MHz in either case. Although there are 11 channels identified for DSSS systems in the US and Europe, there is a lot of overlap. When multiple APs are located in close proximity, it is recommended to use frequency separations of at least 25MHz. Therefore, the ISM band will accommodate three non-overlapping channels.

FHSS relies on a completely different approach. In this method, the carrier frequency hops from channel to channel in a prearranged pseudo-random manner. The receivers are programmed to hop in sequence with the transmitter. If one channel is jammed, the data is simply retransmitted when the system hops to a clear channel.

Information is modulated using either 2-level Frequency Shift Keying (2FSK) at 1Mbps, or 4 level FSK (4FSK) at 2Mbps. The occupied channel width of an FHSS radio is restricted to 1MHz. IEEE 802.11 specifies 79 channels (US and Europe) over which the FHSS radios hop in a predetermined manner. There are 78 different hop sequences, so several AP's can be located in close proximity to each other with a fairly low probability of collision on any given channel. IEEE 802.11 does not specify a hop rate. That parameter is left up to local regulations. In the US, FCC regulations stipulate a rate of 2.5 hops/s, or a channel dwell period of 400s.

There has been a raging debate within the WLAN community regarding the relative merits of the two PHY options. A thorough discussion of this matter is well beyond the scope of this article. It is safe to say that with the advent of 11Mbps for the DSSS PHY, there is more clear distinction between the competing technologies, and the market will begin to segment accordingly. Even with the clear advantage in speed going to DSSS, FHSS radios will continue to find applications and will remain significant in the overall WLAN picture.

Multiple Access

The basic access method for 802.11 is the Distributed Coordination Function (DCF) which uses Carrier Sense Multiple Access / Collision Avoidance (CSMA / CA). STAs sense the medium to determine if it is idle. If so the STA may transmit. However if it is busy, each STA waits until transmission stops, and then enters into a random back off procedure. This prevents multiple STAs from seizing the medium immediately after completion of the preceding transmission.

Packet reception in DCF requires acknowledgment as shown in Figure 7. The period between completion of packet transmission and start of the ACK frame is one Short Inter Frame Space (SIFS). Fast acknowledgment is one of the salient features of the 802.11 standard, because it requires ACKs to be handled at the MAC sublayer.

Transmissions other than ACKs must wait at least a DCF inter frame space (DIFS) before transmitting data. If a transmitter senses a busy medium, it determines a random back-off period by setting an internal timer. After medium becomes idle, STAs wishing to transmit wait a DIFS plus an integer number of Slot Times depending on the timer setting (0 to 7 on first attempt). Upon expiration of a DIFS, the timer begins to decrement. If the timer reaches zero, the STA may begin transmission. However, if the channel is seized by another STA before the timer reaches zero, the timer setting is retained at the decremented value for subsequent transmission.

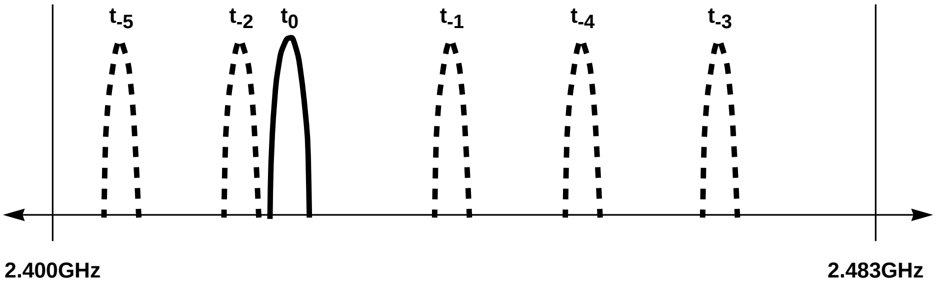

FIGURE 6. FHSS RADIOS HOP CHANNELS IN A PSUEDO RANDOM SEQUENCE

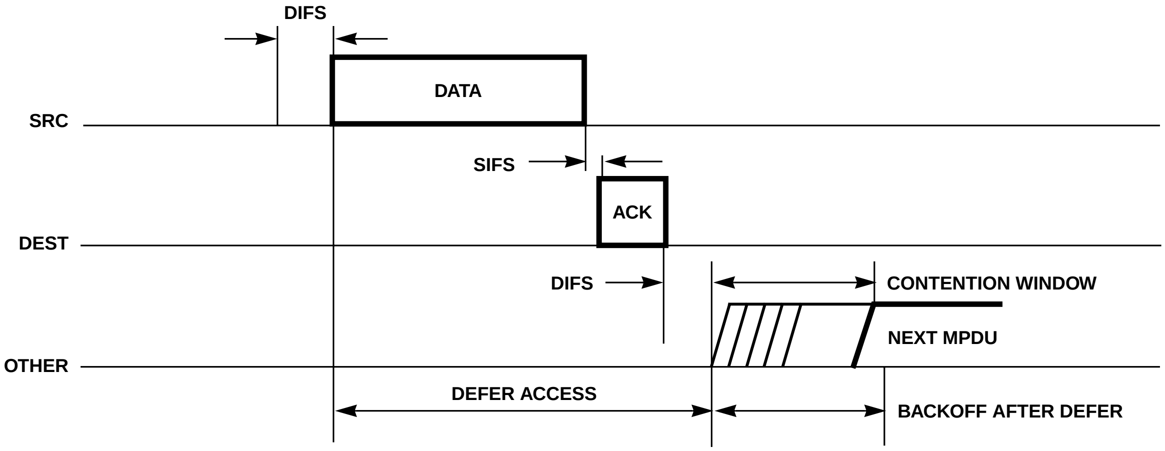

FIGURE 7. CSMA/CD BACK-OFF ALGORITHM

If a transmission is not acknowledged, the packet may not have been received due to a collision. On a second attempt, the random back-off window is increased to 15 Slot Times. The window is doubled on each successive attempt up to a maximum value of 256 Slot Times. Unacknowledged packets may be due to a failure in reception of the packet, or in failure to receive an ACK. Either case is indistinguishable to the sending STA and the same retransmission procedure is followed.

The method described above relies on the ability of each STA to sense signals from all other STAs within the BSS. This approach is referred to as Physical Carrier Sense. The underlying assumption that every STA can “hear” all other STAs is not always valid. Referring to Figure ABC, the AP is within range of the STA-A, but STA-B is out of range. STA-B would not be able to detect transmissions from STA-A, and the probability of collision is greatly increased. This known as the Hidden Node.

In order to combat this problem, a second carrier sense mechanism, Virtual Carrier Sense, is described in the standard. Virtual Carrier Sense is implemented by reserving the medium for a specified period of time for an impending transmission. This is most commonly achieved by use of RTS/CTS frames. Referring to Fig ABC, STA-A sends an RTS frame to the AP. The RTS will not be heard by STA-B. The RTS frame contains a duration/ID field which specifies a period of time for which the medium is reserved for a subsequent transmission. The reservation information is stored in the Network Allocation Vector (NAV) of all STAs detecting the RTS frame.

Upon receipt of the RTS, the AP responds with a CTS frame, which also contains a duration/ID field specifying the period of time for which the medium is reserved. While STA-B did not detect the RTS, it will detect the CTS and update its NAV accordingly. Thus, collision is avoided even though some nodes are hidden from other STAs. The RTS/CTS procedure is invoked according to a user specified parameter. It can be used always, never, or for packets which exceed an arbitrarily defined length.

As mentioned above, DCF is the basic media access control method for 802.11 and it is mandatory for all STAs. An optional extension to DCF is the Point Coordination Function (PCF). PCF works in conjunction with DCF as shown in Figure DEF. PCF was included specifically to accommodate time bounded connection-oriented services such as cordless telephony.

It is interesting to compare CSMA/CA to Carrier Sense Multiple Access / Collision Detection (CSMA/CD), which is commonly used in wired LANs, including Ethernet. Collision detection is impractical because WLAN radios are half duplex and cannot receive while transmitting. Therefore, a collision cannot be detected by a radio while transmission is in progress. Code diversity is not a suitable multiple access scheme either. CDMA would require more processing gain (and therefore more bandwidth) and active transmitter amplifier control to overcome the near-far problem. Neither was deemed practical for WLAN applications.

Logical Addressing

The authors of the 802.11 standard allowed for the possibility that the wireless media, distribution system, and wired LAN infrastructure would all use different address spaces. IEEE 802.11 only specifies addressing for over the wireless medium, though it was intended specifically to facilitate integration with IEEE 802.3 wired Ethernet LANs. IEEE 802 48-bit addressing scheme was therefore adopted for 802.11, thereby maintaining address compatibility with the entire family of IEEE 802 standards. In the vast majority of installations, the distribution system is an IEEE 802 wired LAN and all three logical addressing spaces are identical.

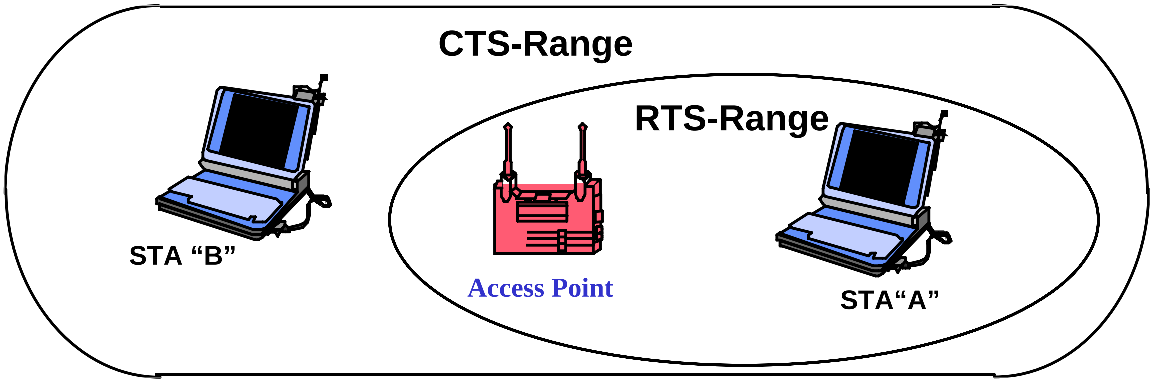

FIGURE 8. RTS/CTS PROCEDURE ELIMINATES THE “HIDDEN NODE” PROBLEM

Security

Special precautions must be taken to maintain security in a wireless network. IEEE 802.11 provides for security via two methods: authentication and encryption. Authentication is the means by which one STA is verified to have authorization to communicate with a second STA. In the infrastructure mode, authentication is established between an AP and each STA. Authentication is a prerequisite for association. Association is the establishment of communication services between the STA and the AP, and mapping the STA to the AP to provide the mobile node with access to the wired LAN.

Authentication can be either Open System or Shared Key. In an Open System, any requesting STA may be granted authentication. However, success is not guaranteed. The STA receiving the request may still deny authentication. In a Shared Key system, only stations which possess a secret key can be authenticated.   Obviously transmission of the Shared Key could lead to its interception by unauthorized users. It is therefore encrypted prior to encryption. Shared Key authentication is available to systems having the optional encryption capability.

Encryption is intended to provide a level of security comparable to that of a wired LAN. The encryption algorithm is designated as Wired Equivalent Privacy (WEP). WEP uses the RC4 PRNG algorithm from RSA Data Security, Inc. The WEP algorithm was selected to meet the following criteria:

- Reasonably Strong
- Self-Synchronizing
- Computationally Efficient
- Exportable
- Optional

Timing and Power Management

Synchronization of all STA clocks within a BSS is maintained by periodic transmission of beacons containing time stamp information. In the infrastructure mode, the AP serves as the timing master and generates all timing beacons. Synchronization is maintained to within 4 microseconds plus propagation delay.

Timing beacons also play an important role in power management. There are two power saving modes defined: awake and doze. In the awake mode, STAs are fully powered and can receive packets at any time. While in the doze mode, it is unable to transmit or receive data and consumes very little power. A STA must inform the AP that it is entering the doze mode. The AP does not sent packets to STAs in the doze mode, but instead buffers them for transmission at a designated time.

When an AP has packets queued for STAs in doze, a traffic indication map (TIM) is broadcast as part of the timing beacon described above. STAs in the doze mode power up receivers to listen for beacons. If identified by the TIM, they return to the *awake* mode and transmit a PS-Poll message to alert the AP that they are ready to receive data.

In addition directed packets, there could be buffered broadcast/multicast packets queued in the AP. For this reason, a delivery traffic indication message (DTIM) is broadcast periodically to awaken all STAs and alert them to a forthcoming broadcast/multicast message. The queued message is then transmitted by the AP without the requirement of a PS-Poll message.

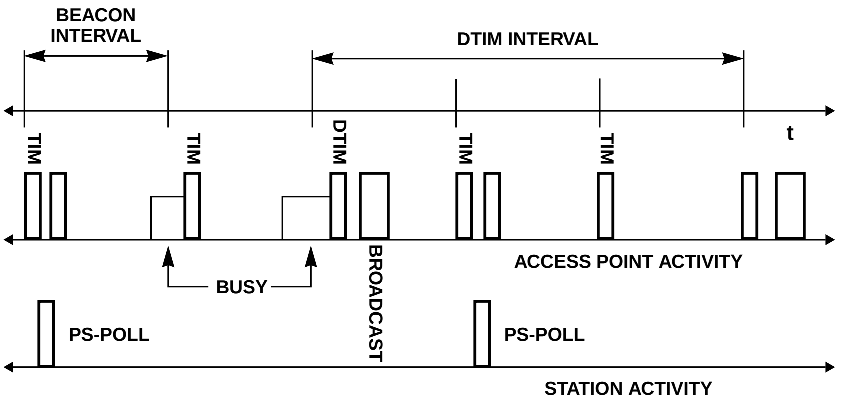

FIGURE 9. TIMING BEACONS FACILITATE POWER SAVING MODE

Roaming

Roaming is perhaps the least defined feature among those discussed in this article. The standard does identify the basic message formats to support roaming, but everything else is left up to the network vendor. In order to fill the void, the Inter-Access Point Protocol (IAPP) was jointly developed by Aironet, Lucent Technologies, and Digital Ocean. Among other things, IAPP extends multi-vendor interoperability to the roaming function. It addresses roaming within a single ESS and between two or more ESSs.

Latest Developments

Approval of the hi-rate extension for the DSSS PHY at 2.4GHz is expected by mid-1999. The Complimentary Code Keying (CCK) waveform renders speeds of 5.5Mbps and 11Mbps in the same occupied bandwidth as current generation 1Mbps and 2Mbps DSSS radios and will be fully backward compatible.

In addition to the developments at 2.4GHz, a waveform supporting 20Mbps to 30Mbps in the 5GHz band is also under development. A separate task group is now drafting a standard based on Orthogonal frequency Division Multiplexing. The draft should be ready for approval in late 1999. While global spectrum allocation in the 5GHz band is not yet in place, a liaison has been established with ETSI to try to maximize commonality between the IEEE standard and ETSI's HIPERLAN2.

Now that a standard is firmly in place and quantum increases in performance are on the horizon, WLANs will become a part of the enterprise networking landscape. With cross vendor interoperability assured and prices falling rapidly, WLANs are finally beginning to fulfill the promise of campus-wide high speed mobile computing.

Sales Office Headquarters

NORTH AMERICA
Intersil Corporation
P. O. Box 883, Mail Stop 53-204
Melbourne, FL 32902
TEL: (321) 724-7000
FAX: (321) 724-7240

EUROPE
Intersil SA
Mercure Center
100, Rue de la Fusee
1130 Brussels, Belgium
TEL: (32) 2.724.2111
FAX: (32) 2.724.22.05

ASIA
Intersil (Taiwan) Ltd.
7F-6, No. 101 Fu Hsing North Road
Taipei, Taiwan
Republic of China
TEL: (886) 2 2716 9310
FAX: (886) 2 2715 3029