IEEE 802.11 Tutorial

by Jim Zyren and Al Petrick

Approval of the IEEE 802.11 standard for wireless local area networking (WLAN) and rapid progress made toward higher data rates have put the promise of truly mobile computing within reach. While wired LANs have been a mainstream technology for at least fifteen years, WLANs are uncharted territory for most networking professionals. Some obvious questions come to mind when considering wireless networking:

- How can WLANs be integrated with wired network infrastructure?
- What is the underlying radio technology?
- How is multiple access handled?
- What about network security?

IEEE 802.11 is limited in scope to the Physical (PHY) layer and Medium Access Control (MAC) sublayer, with MAC origins to IEEE802.3 Ethernet standard. The following overview explains major differences between wired and wireless LANs and should answer some of the questions facing MIS professionals evaluating WLAN technology.

Network Topology

WLANs can be used either to replace wired LANs, or as an extension of the wired LAN infrastructure. The basic topology of an 802.11 network is shown in Figure 1. A Basic Service Set (BSS) consists of two or more wireless nodes, or stations (STAs), which have recognized each other and have established communications. In the most basic form, stations communicate directly with each other on a peer-to-peer level sharing a given cell coverage area. This type of network is often formed on a temporary basis, and is commonly referred to as an *ad hoc* network, or Independent Basic Service Set (IBSS).

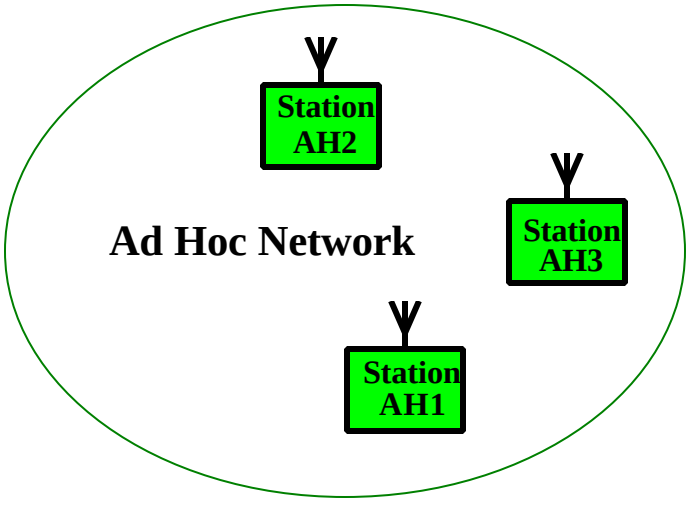

Figure 1 Peer-to-Peer Communications in Ad Hoc Network

In most instances, the BSS contains an Access Point (AP). The main function of an AP is to form a bridge between wireless and wired LANs. The AP is analogous to a basestation used in cellular phone networks. When an AP is present, stations do not communicate on a peer-to-peer

basis. All communications between stations or between a station and a wired network client go through the AP. AP's 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*.

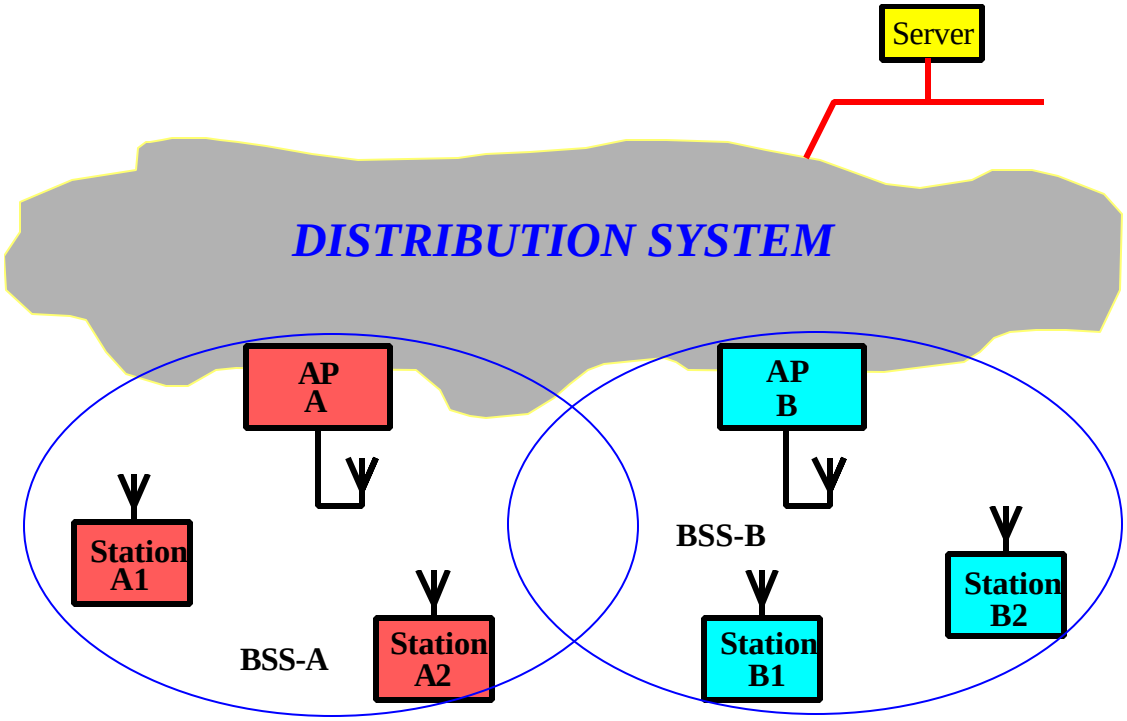

Figure 2 ESS Provides Campus-Wide Coverage

The Extended Service Set (ESS) shown in Figure 2 consists of a series of overlapping BSSs (each containing an AP) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between APs and seamless campus-wide coverage is possible.

Radio Technology

IEEE 802.11 provides for two variations of the PHY. These include two (2) RF technologies namely Direct Sequence Spread Spectrum (DSSS), and Frequency Hopped Spread Spectrum (FHSS). The DSSS and FHSS PHY options were designed specifically to conform to FCC regulations (FCC 15.247) for operation in the 2.4 GHz ISM band, which has worldwide allocation for unlicensed operation.

Region	Allocated Spectrum
US	2.4000 – 2.4835 GHz
Europe	2.4000 – 2.4835 GHz
Japan	2.471 - 2.497 GHz
France	2.4465 - 2.4835 GHz
Spain	2.445 - 2.475 GHz

Table 1 Global Spectrum Allocation at 2.4 GHz

Both FHSS and DSSS PHYs currently support 1 and 2 Mbps. However, all 11 Mbps radios are DSSS. Operating principles of DSSS radios are described in the following paragraphs.

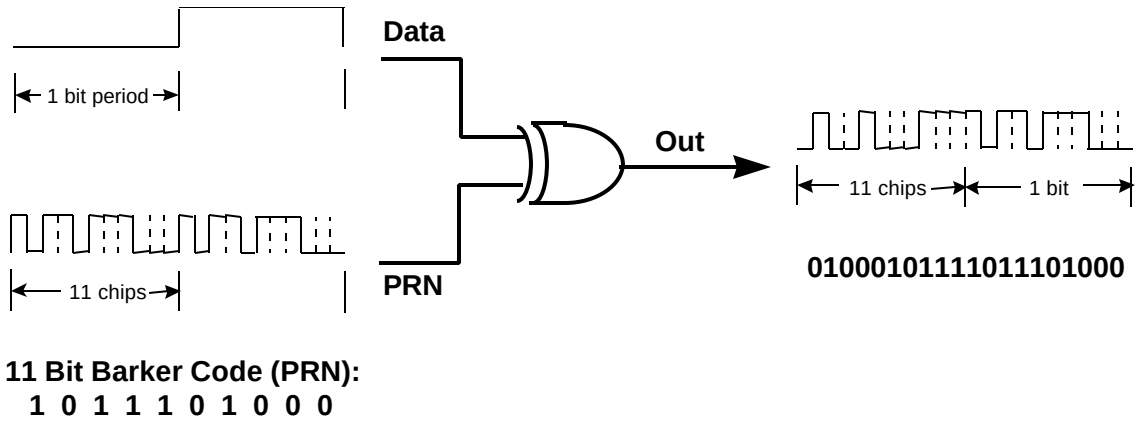

Figure 3 Digital Modulation of Data with PRN Sequence

DSSS systems use technology similar to GPS satellites and some types of cell phones. Each information bit is combined via an XOR function with a longer Pseudo-random Numerical (PN) sequence as shown in Figure 3. The result is a high speed digital stream which is then modulated onto a carrier frequency using Differential Phase Shift Keying (DPSK).

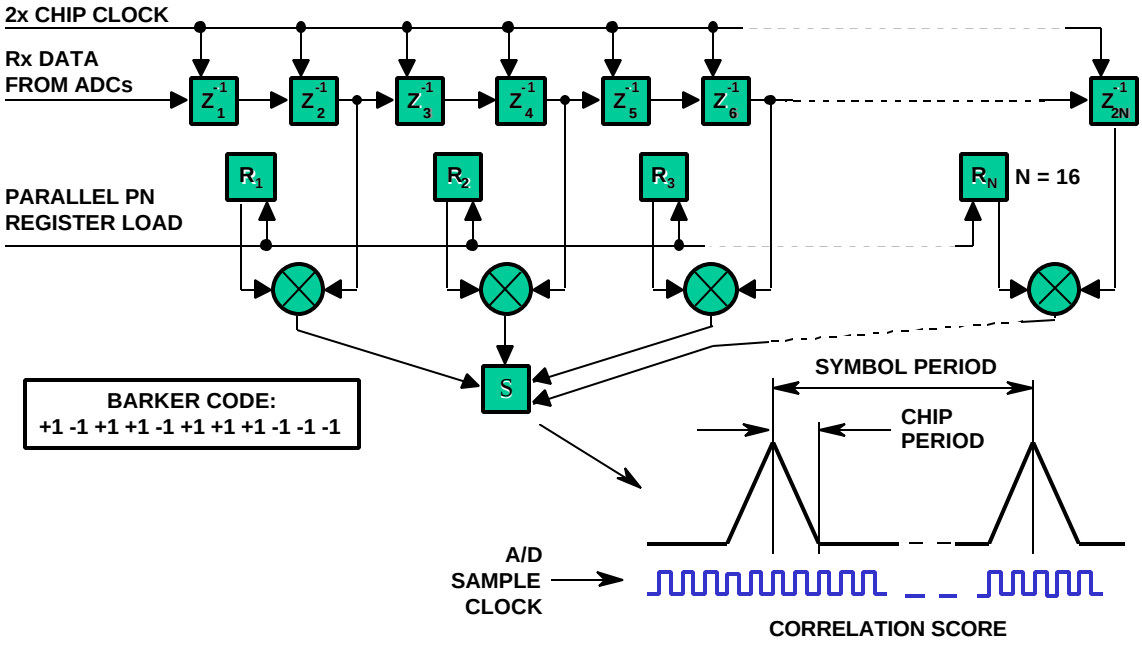

Figure 4 Matched Filter Correlator Used for Reception of DSSS Signal

When receiving the DSSS signal, a matched filter correlator is used as shown in Figure 4. The correlator removes the PN sequence and recovers the original data stream. Tat the higher data rates of 5.5 and 11 Mbps, DSSS receivers employ different PN codes and a bank of correlators to recover the transmitted data stream. The high rate modulation method is called *Complimentary*

Code Keying (CCK). The effects of using PN codes to generate the spread spectrum signal are shown in Figure 5.

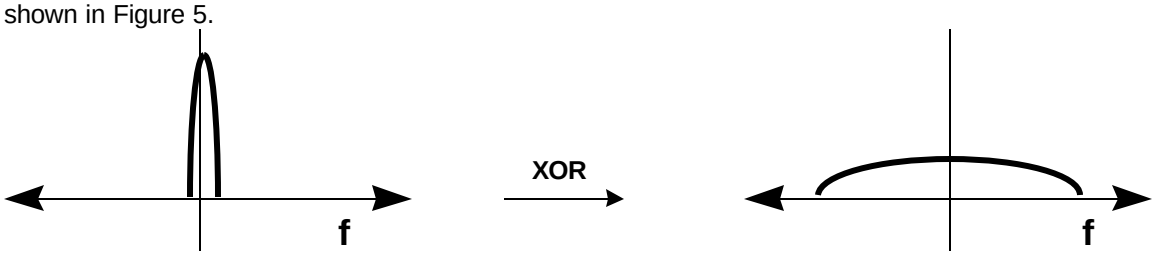

Figure 5a Effect of PN Sequence on Transmit Spectrum

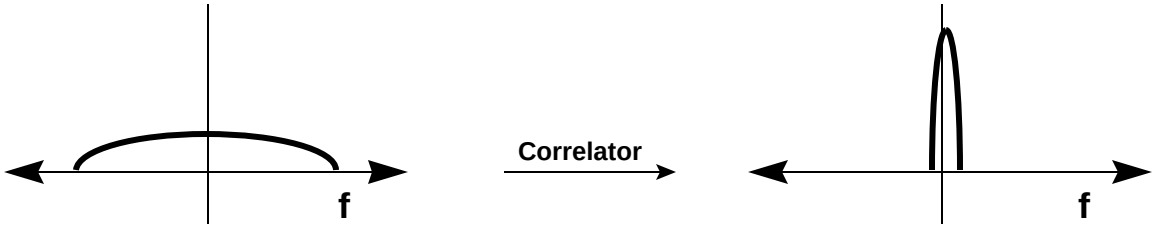

Figure 5b Received Signal is Correlated with PN to Recover Data and Reject Interference

As shown in Figure 5a, the PN sequence spreads the transmitted bandwidth of the resulting signal (thus the term, "spread spectrum") and reduces *peak* power. Note however, that *total* power is unchanged. Upon reception, the signal is correlated with the same PN sequence to reject narrow band interference and recover the original binary data (Fig. 5b). Regardless of whether the data rate is 1, 2, 5.5, or 11 Mbps, the channel bandwidth is about 20 MHz for DSSS systems. Therefore, the ISM band will accommodate up to three non-overlapping channels

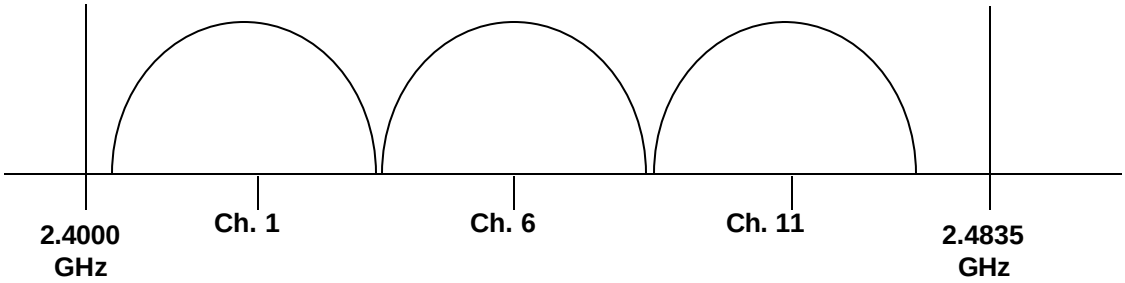

Figure 6 Three Non-Overlapping DSSS Channels in the ISM Band

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). This requires each station to listen for other users. If the channel is idle, the station may transmit. However if it is busy, each station waits until transmission stops, and then enters into a random back off

procedure. This prevents multiple stations from seizing the medium immediately after completion of the preceding transmission.

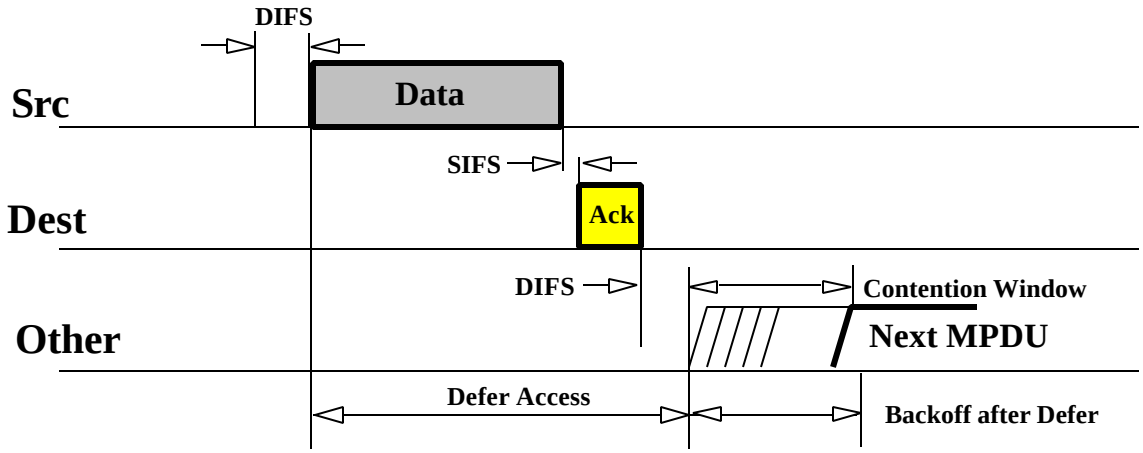

Figure 7 CSMA/CD Back-off Algorithm

Packet reception in DCF requires acknowledgement 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). ACK frames have a higher priority than other traffic. Fast acknowledgement 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 one 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 to an integer number of slot times. Upon expiration of a DIFS, the timer begins to decrement. If the timer reaches zero, the station may begin transmission. However, if the channel is seized by another station before the timer reaches zero, the timer setting is retained at the decremented value for subsequent transmission.

The method described above relies on the *Physical Carrier Sense*. The underlying assumption is that every station can "hear" all other stations. This is not always the case. Referring to Figure 8, 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 is known as the *Hidden Node*.

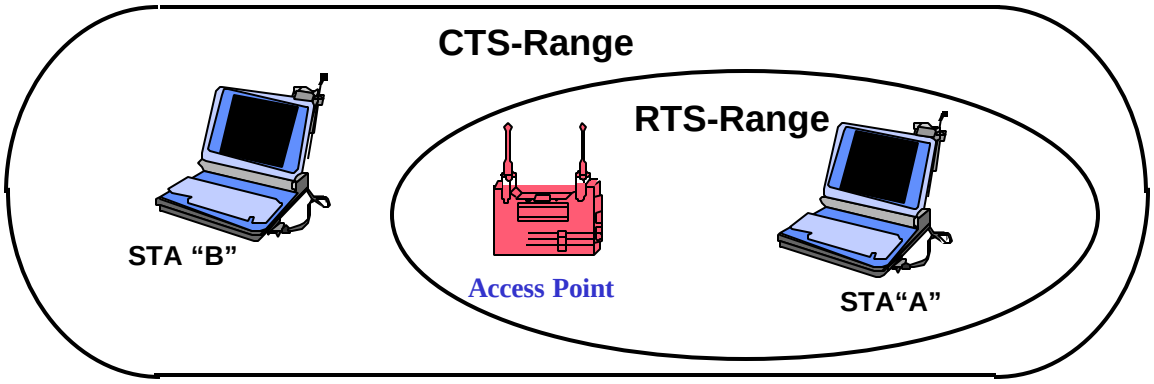

Figure 8 RTS/CTS Procedure Eliminates the "Hidden Node" Problem

To combat this problem, a second carrier sense mechanism is available. *Virtual Carrier Sense* enables a station to reserve the medium for a specified period of time through the use of RTS/CTS frames. In the case described above, 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 the 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 stations 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 stations. 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 stations. The Point Coordination Function (PCF) is an optional extension to DCF. PCF provides a time division duplexing capability to accommodate time bounded, connection-oriented services such as cordless telephony.

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. IEEE802 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.

Security

IEEE 802.11 provides for security via two methods: *authentication* and *encryption*. Authentication is the means by which one station is verified to have authorization to communicate with a second station in a given coverage area. In the infrastructure mode, authentication is established between an AP and each station.

Authentication can be either *Open System* or *Shared Key*. In an Open System, any STA may request authentication. The STA receiving the request may grant authentication to any request, or only those from stations on a user-defined list. In a Shared Key system, only stations which possess a secret encrypted key can be authenticated. Shared Key authentication is available only to systems having the optional encryption capability.

Encryption is intended to provide a level of security comparable to that of a wired LAN. The Wired Equivalent Privacy (WEP) feature 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

All station clocks within a BSS are synchronized by periodic transmission of time stamped beacons. 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, stations are fully powered and can receive packets at any time. Nodes must inform the AP before entering doze. In this mode, nodes must "wake up" periodically to listen for beacons which indicate that AP has queued messages.

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 network vendors. 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.

The Wireless Ethernet Compatibility Alliance

The recently adopted Complimentary Code Keying (CCK) waveform delivers speeds of 5.5 and 11 Mbps in the same occupied bandwidth as current generation 1 and 2 Mbps DSSS radios and will be fully backward compatible. Now that a standard is firmly in place, WLANs will become a part of the enterprise networking landscape within the next twelve months.

The mission of the Wireless Ethernet Compatibility Alliance is to provide certification of compliance with the IEEE 802.11 Standard and to ensure that products from multiple vendor meet strict requirements for interoperability. With cross vendor interoperability assured, WLANs are now able to fulfill the promise of high speed mobile computing.