RangeLAN*802.11*™

The IEEE 802.11 Wireless Standard

White Paper

What is IEEE 802.11?

Two widespread standards today underpin much of the commercial 2.4 GHz wireless LAN market. They are the IEEE 802.11 standard and the OpenAir 2.4 standard. This paper examines the IEEE 802.11 standard: its genesis, its current status, its strengths and shortcomings.

The IEEE 802.11 specification is a wireless LAN standard developed by the 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. First conceived back in 1990, the standard has evolved from various draft versions (Drafts 1 through 6), with approval of the final draft on June 26, 1997.

802.11 Physical Layer

Like the IEEE 802.3 Ethernet and 802.5 Token Ring standards, the IEEE 802.11 specification addresses both the Physical (PHY) and Media Access Control (MAC) layers. At the PHY layer, IEEE 802.11 defines three physical characteristics for wireless local area networks: diffused infrared, direct sequence spread spectrum (DSSS), and frequency hopping spread spectrum (FHSS).

While the infrared PHY operates at the baseband, the other two radio-based PHYs operate at the 2.4 GHz band. This latter frequency band is part of what is known to be the 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. In order for wireless devices to be interoperable they have to conform to the same PHY standard. All three PHYs specify support for 1 Mbps and 2 Mbps data rate.

802.11 Media Access Control Layer

The 802.11 MAC layer, supported by an underlying PHY layer, is concerned primarily with rules for accessing the Wireless medium. Two network architectures are defined: the Infrastructure Network and the Ad Hoc Network. An Infrastructure Network is a network architecture for providing communication between wireless clients and wired network resources. The transition of data from the wireless to the wired medium is via an Access Point. The coverage area is defined by an Access Point (AP) and its associated wireless clients, and together all the devices form a Basic Service Set.

An Ad Hoc network is an architecture that is used to support mutual communication among wireless clients. Typically created spontaneously, an ad hoc network does not support access to wired networks, and does not need an AP to be part of the network.

The primary services provided by the MAC layer are as follows:

Data transfer

Wireless clients use a Collision Sense Multiple Access with Collision Avoidance (CSMA/CA) algorithm as the media access scheme.

Association

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 to roam from one area to another. Although reassociation is specified in 802.11, the mechanism that allows AP-to-AP coordination to handle roaming is not specified.

proxim

Authentication

Authentication is the process of proving a client identity, and in IEEE 802.11this 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 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.

Privacy

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 encrypts data before it is sent wirelessly, using a 40-bit 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.

Power management

IEEE 802.11 defines two power modes, an Active Mode, where a wireless client is powered to transmit and receive, and Power Save mode, where a client is not able to transmit or receive, but consumes less power. Actual power consumption is not defined and is dependent upon the implementation.

Wireless device interoperability through IEEE 802.11

Standardization and interoperability among devices utilizing the same PHY is the intent of the IEEE 802.11 specification. (At the physical level, the three modulation schemes are incompatible with each other, so an infrared wireless client will not synchronize to a DSSS Access Point, for example). However, even among devices with the same PHY, a few key ingredients necessary to achieve multivendor interoperability are absent in the ratified standard.

1 AP-to-AP coordination for roaming

The standard does not specify the handoff mechanism to allow clients to roam from one AP to another.

2 Data frame mapping

The standard does not state how an Access Point addresses data framing between the wired and the wireless media.

3 Conformance test suite

There is no conformance test suite specified to verify that a device is compliant with the IEEE 802.11 specification. Vendor claims for compliance to the 802.11 standard will need to be ratified by a neutral third party.

The lack of specification of these items does not inhibit vendors from producing 802.11 products. Rather, each vendor will devise their own algorithm for AP-to-AP roaming and data framing. IEEE 802.11 did not set up a committee for addressing interoperability and interpretation issues, so determination of a common method for AP-to-AP roaming and data framing will need to be addressed in a group outside of that organization. At this writing, several vendors have retained the University of New Hampshire as an independent test facility to verify compliance to the 802.11 specification and perform multivendor interoperability testing. Results from UNH have not yet been published.

Finding out more about IEEE 802.11

With the ratification of 802.11 standard for IR, FHSS and DHSS at 2.4 GHz, the 802.11 committee has moved on to focus on higher speed PHYs beyond the 2 Mbps data rate. Further information about current IEEE 802.11 activities can be obtained through IEEE's web site at:

http://stdsbbs.ieee.org/groups/802/11/

Proxim, Inc
Corporate Headquarters
295 North Bernardo Avenue
Mountain View, CA 94043 USA
Phone: 650-960-1630 / 800-229-1630
Fax: 650-960-1984
sales@proxim.com
www.proxim.com

Europe
4, avenue Morane Saulnier
78140 Velizy, France
Phone: +33 01 30 70 61 18
Fax: +33 01 30 70 61 19
europe@proxim.com
www.proxim.com

© Copyright 1997 Proxim, Inc. Specifications are subject to change without notice. Proxim RangeLAN2 products covered by one or more of U.S. Patent Numbers 5,231,634, 5,412,687 and Des. 375,297. U.S. and international patents pending. RangeLAN2 and Proxim are trademarks of Proxim, Inc. All other names mentioned herein are trademarks or registered trademarks of their respective owners.

#7680-//// 12/97 CI/LC