SAVER TechNote
Technical Information for the Emergency Responder March 2005

802.11 Technology

Introduction to Usability

802.11 is a rule set for wireless communications that now reaches virtually every location on earth. Wireless networks liberate mobile users from dependence on hard-wired networks.

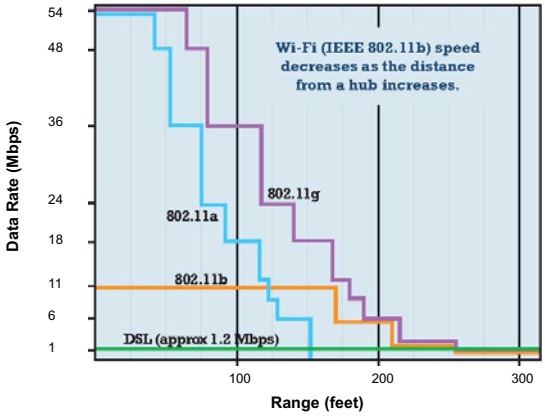
802.11 Fundamentals

- The Institute of Electrical and Electronics Engineers (IEEE) developed 802.11 in 1997.
- The 802.11 standard is designed for wireless local area networks (WLANs).
- Enhancements to the standard are designated by a letter following the 802.11 name, such as 802.11a, 802.11b, or 802.11g.
- Several other standards (802.11c - 802.11n) are in place or in development.
- Each enhancement increases data rates and functionality.
- Commercial wireless vendors have united to form the Wi-Fi Alliance.
- The Wi-Fi Alliance certifies cross vendor interoperability and compatibility of wireless networking products and promotes the standards.

What is a Wireless LAN?

A wireless local area network (WLAN) is a data transmission system designed to provide network access between computing devices, such as a laptop computer, mobile phone, or personal digital assistants (PDA), by using radio waves rather than a cable infrastructure. Untethered from conventional network connections, network users can move about without restriction and access LANs from anywhere within reach of a wireless access point. More than 95 percent of current WLAN infrastructure includes 802.11b products.

Various Data Rate Falloffs



802.11 Up Close

Standard	Frequency (GHz)	Maximum Data Rate	Major Advantage	Major Disadvantage
802.11	2.4	2 Mbps	• Higher range	• Lowest data rate
802.11a	5	54 Mbps	• Higher data rate in less crowded frequency	• Shortest signal range of 802.11 standards
802.11b	2.4	11 Mbps	• Most widely deployed	• Data rate low for emerging applications and products
802.11g	2.4	54 Mbps	• Higher data rate in 2.4 GHz frequency	• Limited collocated WLANs with range higher than 802.11a

SAVER is sponsored by the U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness.

For further information regarding this 802.11 technology overview please contact David A. DeRieux, Head, Communications Systems Naval Research Laboratory (NRL), Code 8144, (202) 767-0002, derieux@kingcrab.nrl.navy.mil.

Interference in WLANs

- 802.11b and 802.11g equipment operate in the same frequencies as microwave ovens and cordless phones, which may interfere with their operation.
- Wi-Fi equipment using 802.11a is less subject to interference because it uses a less populated frequency.
- When a Wi-Fi system encounters interference, it does not turn off. Instead it slows down and reduces range.
- Options for handling interference: separate the devices, change the Wi-Fi network's operating channel (11 to pick from), or use Wi-Fi equipment that uses other protocols.

Branding

The WiFi-Alliance has developed a group of tests that define how member products are certified for compatibility with other Wi-Fi CERTIFIED products.

Sources of Interference

- Other Wireless LANs
- Tall buildings (canyon effect)
- UHF TV broadcast antennas
- Wireless phones
- High-end cordless phones
- Microwave ovens
- Children's monitors

Practical Uses of 802.11

- Information Technology Laboratory (ITL) established a distrubuted testbed for first responders, May - June 2003.
  ITL's Advanced Network Technologies Division (ANTD) built a wireless ad hoc network (WANET) consisting of Compaq iPAQ Personal Digital Assistants (PDAs) with IEEE 802.11b WLAN cards to demonstrate how first responders could communicate with each other on scene as well as those outside the WANET. The network allows for voice, video, text, and sensor data communications. The WANET can also determine locations of all assets of interest, such as the first responders themselves and any civilians trapped at the disaster site.
- Arlington County Fire Department (ACFD), Arlington, VA, September 2004.
  ACFD tested Sensatex SmartShirt to monitor fire fighters. A wireless network was set up to pass vitals from SmartShirt to ERV utilizing Rajant BreadCrumb® from a:
  - Multi-level closed cement parking deck
  - Multi-floor building
  - Smoke House (three stories)
- Wireless Integrated Network (WIN) project at the U.S. Naval Research Laboratory (NRL), September 2004.
  The NRL WIN project integrates and transmits output of multiple types of wireless monitoring equipment from an incident site to the Incident Commond Post (ICP). The NRL WIN Project is developing a prototype equipment suite in which all selected sensors, regardless of wireless interface capabilites, are connected via a mesh network so that sensor data is brought back to the ICP.

802.11 Resources

- IEEE 802.11 Wireless LAN Working Group - http://grouper.ieee.org/groups/802/11/index.html
  Contains working group documents plus discussion archives.
- Wi-Fi Alliance -http://www.weca.net/OpenSection/index.asp
  Industry group discussing certified products and standards.
- Rajant Corporation -http://www.rajant.net/demos_arlington.htm
  Press releases describing Rajant's BreadCrumb demos.
- Advanced Network Technologies Division - http://w3.antd.nist.gov./first_responders_news.shtml
  Description of testbed demonstration with first responders.

Making 802.11 Secure

- WPA (Wi-Fi Protected Access) is a powerful, standards-based, interoperable security technology for Wi-Fi networks. It provides strong data protection by using encryption as well as strong access controls and user authentication.
- WPA2 (Wi-Fi Protected Access 2) provides network administrators with a high level of assurance that only authorized users can access the network.
- WPA2 provides government-grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm.
- Wi-Fi access points may be programmed to accept only certain MAC addresses and filter out all others. The MAC control table thus created works like "call blocking" on a telephone.