Beyond 802.11 Standards:
A Wi-Fi Lexicon for the Rest of Us

June 2009

Joanie Wexler, Joanie M. Wexler & Associates
Devin Akin, CWNP
Paul DeBeasi, Burton Group

Every industry has its own vernacular, and the Wi-Fi environment is no different. Many Wi-Fi terms are easily researchable because they have a common meaning from vendor to vendor, context to context. Definitions for these terms often can be found in the formal IEEE 802.11 series of standards as well as in detailed reference guides such as *The Official CWNP Dictionary of Wireless Terms and Acronyms*.

Beyond the standards, however, most vendors attempt to differentiate themselves with complementary features and products. Some of these enhancements have become common enough that de facto names for them have cropped up in everyday language. In addition to having generic names, these functions might also have any number of brand names assigned to them by Wi-Fi vendor marketing departments.

• THE VOCABULARY PROBLEM: Having inconsistent terms for the same functions can be confusing and can make it difficult to conduct apples-to-apples vendor and product comparisons.

• THE SOLUTION: A lexicon of terms that starts on the next page is an attempt to ease this confusion by documenting and defining some common Wi-Fi functions that may be important to you but are not necessarily required by 802.11 technical standards. Different vendors might refer to them by different brand names.

• THE CAVEAT: We have elected to omit vendor-specific brand names, because many do not have a one-for-one mapping and thus might generate outbursts of protest from vendor marketing departments. For example, some vendors combine a number of RF management and performance optimization tools under an umbrella name and don't create separate names for each individual feature. Others give separate monikers to every feature, making their features list appear longer. Still other vendors claim that certain features are not needed because their system designs inherently solve the problem at hand.

Hopefully, the lexicon that follows—written in as simple English as possible—will ease the task of accurately comparing capabilities across the disparate vendors and systems in the Wi-Fi market. If the capabilities listed are important to you, ask your vendors whether they support them and if so, what brand name (if any) they use to describe them.

NOTE: This is intended to be a living document, edited from time to time as new terminology emerges and older terminology fades away. As such, all contributions are welcome and will be considered. Please submit suggestions to joanie@jwexler.com.

Lexicon begins on the next page.

A Lexicon of Common Wi-Fi Terms

Term	Basic Definition
access point (AP)	A Wi-Fi network infrastructure device with varying degrees of software intelligence that combines one or more radio and antenna pairs within a common housing. Its function is to bridge Wi-Fi clients to other APs or to wired networks.
AP, thick; *also, fat AP, autonomous AP, standalone AP, independent AP*	APs that locally contain all 802.11 media-access control (MAC) functions. Historically, these APs operated without a controller and were provisioned and managed individually, which became time-consuming and impractical when scaling beyond a handful of them. So some now are provisioned and managed by a centralized wireless network management system.
AP, thin; *also lightweight AP, dependent AP, controller-based AP*	APs with a minimum of intelligence and few, if any, standalone functions. Thin APs are often completely dependent on a centralized WLAN controller for data transmission, management, control and other functions. In this way, 802.11 media-access control (MAC) functions are sometimes, but not always, “split” between AP and controller. Which MAC functions reside on the AP and which reside on the controller is vendor-specific.
air time fairness (ATF)	A mechanism that prevents the slowest client on the Wi-Fi network from gating overall network performance. ATF allows each client to transmit at the speed that it would if there were no slower-speed clients on the network holding it back. Once ATF has been accomplished, administrators can set priorities or weights for certain transmissions based on protocol, application, user, or other criteria. To do this, they use a separate but related capability often called *policy-based QoS* or *wireless QoS*.
architecture	How a WLAN system is designed to operate, both from a data transmission and RF management perspective. Architectures can involve some or all elements being centralized, distributed, or a little of both. A given vendor’s Wi-Fi architecture also dictates how channels are reused.
automatic channel assignment	A tool within WLAN system software that alternately selects and assigns APs to non-interfering channels throughout an installation, precluding network administrators from having to hard code each AP to a channel. Used primarily in multi-channel/micro-cell architectures (MCA).

band steering	Automatically forcing a dual-band-capable client to associate with an AP using the preferred band. In practice, this usually involves moving clients away from the crowded 2.4GHz band and onto the 5GHz band, but can be applied either way.
beamforming	Using special transmission techniques to improve signal reception. The goal is to achieve improved throughput and greater connection reliability and predictability. There are four primary categories of beamforming (see below).
	1) Static Using semi- or highly directional antennas or arrays of antennas to concentrate and aim RF energy in the appropriate direction to improve signal reception for the benefits described above.
	2) *Transmit beamforming (TxBF), 802.11n Draft standard* Improving signal reception in 802.11n networks by using over-the-air feedback continually generated by the client station. Feedback is either *explicitly* generated for the beamforming process or constitutes *implicit* feedback, which is information generated inherently for other purposes but also used for beamforming. APs continually gather information about the client environment and make dynamic best-path transmission decisions. This function requires the same multiple input, multiple output (MIMO) TxBF signal-processing capabilities in the client as in the AP.
	3) *Transmit beamforming (TxBF), proprietary* Improving signal reception in 802.11n networks by using implicit client feedback generated by the client device upon initial client-to-AP association. This feedback is not explicitly generated for the beamforming application; rather, it typically consists of 802.11 control frames.
	4) Dynamic beamforming, proprietary Improving signal reception in 802.11n networks by using continual, implicit feedback from the client station as it moves. Such beamforming leverages 802.11's built-in acknowledgement (ACK) mechanisms to continually determine the quality and performance of a physical RF link and thus does not require the same beamforming signal processing capabilities in the client as in the AP. APs use this information to continually make dynamic transmission decisions on a per-frame basis. See also, *smart antenna technology*.
channel layering	Tuning a set of access points to a single radio channel to avoid co-channel interference. When more capacity is required, a second set of access points is tuned to another channel, then a third set is tuned to a third, and so forth. See also, *single-channel architecture.*
controller	See *WLAN controller*.

Draft N; *also, Draft 2.0*	An informal reference to the technology currently specified by the IEEE's 802.11 Task Group N for a next-generation wireless LAN that supports several hundred megabit-per-second connect rates. The term "Draft" is used, because the formal standard is not ratified as of this writing. However, early products that support the mandatory capabilities of the current draft spec, Draft 2.0, are on the market, and the Wi-Fi Alliance industry consortium has taken to certifying Draft 2.0-compliant products for interoperability so that some benefits of 802.11n technology can be realized ahead of formal standards ratification.
Dynamic Frequency Selection (DFS-2); regulatory	An international agreement requiring that WLAN systems operating in certain 5GHz frequencies in the U.S., Canada, and Europe avoid interfering with incumbent military and weather radar systems. They do so by continually scanning the frequencies for radar interference and, upon detection, move an AP and its clients off the occupied channel and onto an available one. Products must be certified and tested by each country's communications regulatory agency for this capability to operate within the regulated frequencies. If not certified, vendors must configure their products to block the use of these frequencies, which currently are 5.25-5.35GHz and 5.47-5.725GHz.
dynamic frequency selection; generic	Working in a manner similar to the above, a general RF management technique in some Wi-Fi systems that adaptively moves an AP and its clients off of one channel and onto an available one to avoid interference and/or improve performance, regardless of spectrum band in use or regulatory requirements.
load balancing	Dynamically allocating wireless traffic among access points to avoid congestion on any one AP and to ensure sustained client-to-AP connectivity. Can also apply, in the case of at least one vendor, to load balancing at the back end among virtualized controllers.
multiple channel architecture (MCA); *also, multi-cell architecture, micro-cell architecture*	A network of Wi-Fi access points in a traditional configuration that tunes adjacent APs to alternating, non-overlapping channels to avoid co-channel interference. In addition to also being called a *multi-cell architecture* and a *micro-cell architecture*, this configuration is often referred to as a "channel reuse," "tiling" or "checkerboard" pattern. Clients determine which AP they will associate with based on local RF conditions. Contrast with *single-channel architecture (SCA).*
per-station pre-shared key (PSK)	A security mechanism that delivers greater security than the low-end 802.11i security standard option, called WPA2-Personal by the Wi-Fi Alliance. WPA2-Personal requires all users to share a single authentication key, making the network vulnerable to eavesdropping and requiring that the key be changed as users leave the company. Per-station PSK, instead, assigns a private key to each user to boost security but allows enterprises to avoid the deployment complexity of the higher-end 802.11i 802.1x security standard recommended for corporate use, called WPA2-Enterprise by the Wi-Fi Alliance.

policy-based QoS; *also, wireless QoS*	Giving preferential transmission treatment to clients or applications operating across a shared Wi-Fi access medium.
predictive modeling	See *site survey, predictive.*
radio resource management; *also,* *RF management,* *spectrum management*	1) A collection of automated infrastructure-based tools built into a Wi-Fi transmission system or provided by a third party to mitigate the effects of interference, optimize channel assignments, counter the effects of a failed AP or otherwise help improve over-the-air performance. Often an umbrella term for a set of features within a WLAN vendor's system that contribute to optimal performance in various ways. 2) The name of an amendment to the 802.11 standard, also called 802.11k, which defines and exposes radio and network information to facilitate the management and maintenance of a mobile wireless LAN.
real-time location system or service (RTLS)	The use of one or more methods to wirelessly locate, to within a few feet, a piece of equipment, object, person or animal that contains a mounted or embedded Wi-Fi tag or connection. Location methods include triangulation, trilateration, RF fingerprinting and time difference of arrival (TDOA).
roaming	The transitioning of a Wi-Fi client association with one access point to another access point over the air as a user moves. Depending on the vendor architecture and system implementation, this may or may not require the user's security credentials to be reauthenticated.
sensor (security)	A device that monitors wireless channels to detect unauthorized or suspicious activity. It usually operates in conjunction with an appliance or server software for data collection and correlation. See also, *wireless intrusion detection and prevention system/software (WIDS or WIPS).*
single-channel architecture	Tuning all access points to a single radio channel and using a controller to coordinate data transmissions. The primary goal is to avoid co-channel interference and to reduce or eliminate AP-to-AP handoff delay as clients roam. The network, rather than the clients, determines the APs to which clients should associate for the good of the network as a whole, rather than each client making a local decision. In this architecture, all APs share a single MAC address. Contrast with *multiple-channel architecture.*

site survey, manual	Using mobile software tools to check connectivity and throughput to locally determine the placement, channel assignments and output power of local wireless access points. Sometimes performed as the only site survey and often used as a follow-on check to predictive site surveys (see below) to achieve the desired wireless coverage, data rates, network capacity, roaming capability and quality of service (QoS). An *active* manual site survey uses the survey utility software to the test AP to make specific measurements. A *passive* manual site survey involves listening to the test AP's beacons and the traffic around the test AP to measure the RF environment.
site survey, predictive; ***also, virtual site survey, predictive modeling***	Using imported floor plans and centralized software tools to remotely determine the placement, channel assignments, antenna types and output power of wireless access points that will deliver the desired wireless coverage, data rates, network capacity, roaming capability and quality of service (QoS).
smart antenna technology	Special firmware in access points that creates "smart" antennas, which continually gather information about the client environment and adjust transmissions to keep them optimally focused at all times. The firmware maintains thousands of possible beam patterns to clients and dynamically selects, on a per-frame basis, the best pattern. See also, *beamforming (4): dynamic with implicit feedback.*
spectrum analysis	Detecting and identifying wireless devices (Wi-Fi or other) in the air space and determining what effect they are having on a Wi-Fi network's performance.
spectrum management	Using one or more intelligent RF features or tools – either embedded in the Wi-Fi system or provided by a third party – to make optimum use of the available spectrum. See also, *radio resource management (RRM); RF management.*
transmit power control (TPC)	A type of RF management involving the intelligent and often dynamic selection and adjustment of AP transmit power to improve Wi-Fi performance.
Wi-Fi	A trademark of the Wi-Fi Alliance industry consortium, an organization that conducts basic interoperability testing among different vendors' 802.11-based products. An abbreviation for "wireless fidelity," "Wi-Fi" has become a de facto, casual term for any network based on 802.11 technology, regardless of whether it is an 802.11a, b, g, or n network.
wireless firewall	Stateful inspection of Layer 1-7 traffic (depending on vendor) at the juncture where the wireless LAN meets the wired LAN so as to block any unwanted traffic per corporate policy.

wireless intrusion detection and prevention system/software (WIDS or WIPS)	A network system, usually involving an appliance and a distributed set of part-time or full-time sensors, that monitors the radio spectrum for the presence of unauthorized devices (intrusion detection) and can automatically take measures to prevent an unwanted network connection to thwart attacks (intrusion prevention).
wireless security	Catch-all term for a number of security functions that address any or all of the following: • User access control, including authentication, authorization and encryption inherent in the IEEE 802.11i amendment • User policy enforcement • Endpoint compliance • Encryption of over-the-air data • Scanning for network intruders and preventing them from connecting to the corporate wireless or wired network *(see WIDS/WIPS, above)* • Ensuring that an authorized client doesn't associate with an unauthorized access point • Remote wiping of data on a lost or stolen device • Antivirus/ anti-malware intrusion detection • URL/content filtering • Secure guest access
WLAN controller; *also, WLAN switch*	A standalone appliance or special module in an enterprise-class Ethernet switch or router that allows for the centralized management of two or more APs. Controllers were created to help scale the provisioning, management and security of large numbers of enterprise-class APs. Older "thick" APs were generally deployed in small numbers for niche applications and each had to be touched separately to be configured and updated. Also known as a "WLAN switch."
WLAN switch	See *WLAN controller*.
WPA	Wi-Fi Protected Access, a term created by the Wi-Fi Alliance industry consortium to describe an early version of the 802.11i security amendment that supports RC4 encryption. Can operate in two modes, "Personal" and "Enterprise."
WPA2	Wi-Fi Protected Access 2, a term created by the Wi-Fi Alliance industry consortium to describe a stronger implementation of the 802.11i security amendment than WPA. WPA2 supports a form of AES encryption. Can operate in two modes, "Personal" and "Enterprise."