Wireless LANs

Considerations and Configurations

TP.WL.5000.2014.02

Copyright

Vocollect®, Talkman®, Vocollect Adaptive Speech Recognition™, Vocollect Voice®, VoiceConsole®, and the Vocollect logo are registered trademarks of Vocollect.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

Published by Vocollect
703 Rodi Road
Pittsburgh, PA 15235
(412) 829-8145
fax (412) 829-0972
http://www.vocollect.com

Vocollect has carefully checked the information in this document and believes it to be accurate. However, Vocollect assumes no responsibility for any inaccuracies that this document may contain. In no event will Vocollect be liable for direct, indirect, special, exemplary, incidental, or consequential damages resulting from any defect or omission in this document, even if advised of the possibility of such damages.

Any alterations or inconsistent replications of this document cannot be considered accurate and are void. Vocollect may not be able to support issues related to altered documents that are not approved by subject matter experts.

In the interest of product development, Vocollect reserves the right to make improvements to the information in this document and the products that it describes at any time, without notice or obligation.

Table of Contents

1 The WLAN Environment

Vocollect Talkman® devices are specifically designed to provide reliable and forgiving voice operation under a wide variety of operating conditions. All wireless local area network (WLAN) devices, including the Talkman device, rely upon the underlying wireless communications infrastructure to deliver data in a reliable and timely fashion. A properly installed and operating wireless network is critical to successful deployment and use of the Talkman device. Based on Vocollect's experience in integrating products into thousands of wireless environments, this document discusses key considerations in WLAN planning and deployment as well as best practices for problem-free implementation.

Knowing the demands of the applications relying on wireless access, the mobility patterns of the wireless clients (users), and the security requirements of your network are integral to making proper WLAN deployment decisions.

Application performance depends heavily on WLAN deployment. The WLAN networks provide access to the wireless medium according to a contention-based protocol. The logical result of contention is induced latency in the network. As a result, effective per-client throughput and packet delays may be adversely affected as each new user is added to the network. Application types and demands also may significantly impact throughput and delay performance based on their different traffic characteristics. For example, a streaming application type has very different characteristics from a bursty application type.


The applications that run on Talkman devices can be classified as low-bandwidth but latency-sensitive with seamless roaming requirements.

Basic WLAN Requirements

Standards-Based WLAN

- IEEE 802.11b
- IEEE 802.11b/g
- IEEE 802.11a
- IEEE 802.11a/b/g
- IEEE 802.11b/g/n
- IEEE 802.11a/b/g/n

The choice of standard depends on requirements including data communications speed and range, the level of security, noise and interference concerns, compatibility issues and cost.

Table 3.1: Supported IEEE 802.11 Standards Supported

A700	802.11a/b/g/n
A500 (TT-800)	802.11a/b/g
A500 (TT-801)	802.11b/g
T5 series (RoHS)	802.11b/g
T2x series (RoHS)	802.11b/g
T1	802.11b/g

Certified for WiFi Interoperability

WiFi certification can be verified at the WiFi web site at http://certifications.wi-fi.org/wbcs_certified_products.php or request a copy of the WiFi certificate from the WLAN manufacturer.

WLAN Hardware

Due to the popularity of wireless networks and the subsequent economies of scale, the cost of WLAN components such as Access Points (APs), switches, and controllers have decreased dramatically in recent years. Before shopping based on price alone, be aware that there are two classes of WLAN hardware: consumer and enterprise.

Consumer class APs are designed for small office/home office environments and are the least expensive. Since home/small offices rarely require more than one AP and have very few users, consumer APs place little emphasis on factors like roaming or user capacity. In contrast, enterprise class APs, switches, and controllers are designed for high speed roaming, large numbers of users, and add other important features such as remote management, power management, antenna diversity, Power over Ethernet, network security, etc. Recommended examples of manufacturers of enterprise grade APs that are WiFi certified include Cisco, Motorola, Aruba, and Hewlett-Packard.

Summary:

The wireless network is the foundation of the entire warehouse network; install a WLAN network that is enterprise grade and WiFi certified.

2 WLAN Configurations

When you create a device profile in VoiceConsole, you can configure your network settings in the user interface as shown in Figure 1.1

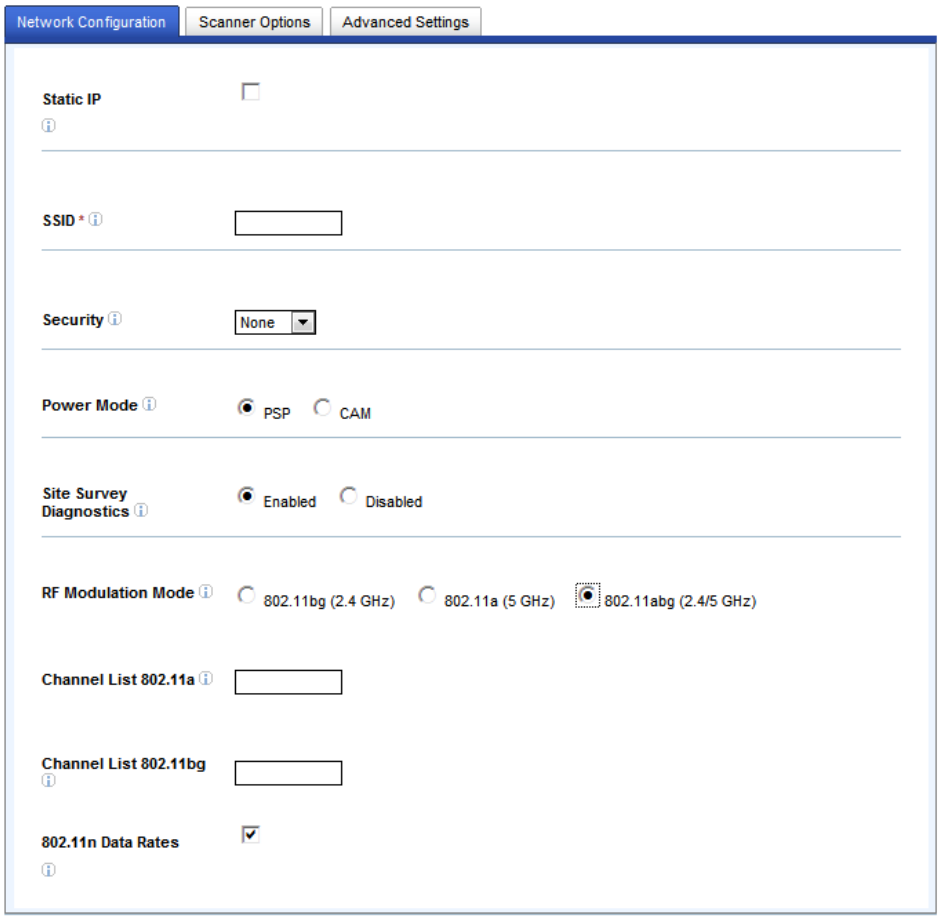

Figure 1.1: Network Configuration Settings in VoiceConsole

Field Name	Field Value	Description	Available when you select
IP Address Assignment	DHCP	Dynamic Host Configuration Protocol: With dynamic addressing, a device can have a different IP address every time it connects to the network. This means that a new computer can be added to a network without manually assigning it a unique IP address.	Always Available
	Static IP	A constant assigned IP address for the device.	Always Available
Subnet Mask		Mask (which is a filter that selectively includes or excludes certain values) used to determine to which subnet (a portion of a network that shares a common address component) an IP address belongs	Static IP for IP Address Assignment
Gateway		IP address of the default router	Static IP for IP Address Assignment
DNS Server		Domain Name Server: an Internet service that translates domain names into IP addresses.	Static IP for IP Address Assignment
WINS		Windows Internet Naming Service, a system that determines the IP address associated with a particular network computer.	Static IP for IP Address Assignment
Service Set Identifier (SSID)		Name that identifies a wireless network. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID.	Always Available

Field Name	Field Value	Description	Available when you select
Security	None	No security	Always Available
	WEP	Wireless Equivalent Privacy	Always Available
	WPA	Wi-Fi Protected Access	Always Available
	WPA-2	Wi-Fi Protected Access 2	Always Available
WEP Key		WEP key	WEP for Security
WEP Index	1, 2, 3, 4	Select 1, 2, 3, or 4	WEP for Security
Dynamic WEP Keys	Yes, No	Keys for confidentiality over a wireless network.	WEP *and* the site is configured to use LEAP.
Authentication	PSK	Pre-shared Key	WPA or WPA-2 for Security
	EAP	Extensible Authentication Protocol	WPA or WPA-2 for Security This option is only available if EAP is configured for the site you are viewing.
PSK Key		Key for PSK authentication.	PSK for Authentication
EAP Settings		You can view the EAP settings that have been set up by your site administrator.	EAP for Authentication
Optional Advanced Settings	Use Mixed Mode	Activate this check box if you have some access points configured to use WPA and others configured to use WPA-2. In a mixed WPA/WPA-2 network, the device will accept *group messages* from the	WPA-2 for Security

Field Name	Field Value	Description	Available when you select
		access point using WPA/TKIP encryption and messages that are only *between the access point and the device* using WPA-2/AES encryption. **Warning:** Do not activate this check box if the access points are configured to use only one or the other. Some devices will fail to connect to the network.	

3 WLAN Planning and Deployment Considerations

Decisions made during the planning and deployment of a wireless network are crucial for optimal WLAN performance. Discussed below are key considerations.

About Coverage and Capacity

The two fundamental considerations in optimizing the performance of a WLAN are coverage and capacity (assuming a specified cost constraint). The performance perception of the WLAN is that of the users – where they have wireless access and how well their applications run.

To get the required coverage from the WLAN it is necessary to understand the fundamentals of radio frequency (RF) wave propagation. The inherent nature of radio propagation poses challenges to network performance. Path loss, multipath propagation, signal fading and interference are all typical attributes of RF propagation that affect received signal quality, and thereby performance.

As an RF signal propagates, it disperses energy and is also absorbed by obstacles in its path. Thus, there is a loss in signal power, known as path loss. RF signals can propagate between the transmitting antenna and the receiving antenna by means of a direct path (referred to as line of sight or LOS), reflection, refraction, diffraction and scattering. This results in multiple copies of the transmitted signal arriving at the receiving antenna by different paths, each with a different delay and path loss. This is known as multipath propagation.

Multipath propagation can result in signal fading, which is a time-varying change in received signal level due to the movement of objects in the environment, including the transmitter and receiver themselves. Under LOS conditions (between a wireless transmitter and receiver), path loss is proportional to the square of the distance between the transmitter and receiver, and multipath propagation has less of an impact.

Typical indoor WLAN environments are NLOS (non-line of sight) and are cluttered with walls, furniture, people and other objects that can increase path loss and multipath induced fading. Interference from other signals occupying the same frequency can also corrupt the quality of the received signal. Outdoor applications offer a different challenge and LOS is more important since the amount of objects available for reflections are greatly reduced. Any object in the LOS path will completely obstruct the RF signal.

To provide WLAN coverage to a specified area several factors need to be considered.

Building Construction and Clutter

Different types of material affect RF in different ways. RF signals are attenuated by metal, brick, concrete and tinted or coated glass. The more clutter in an environment, the more blockage for RF waves, and hence the range of an AP will be reduced.

There may also be other challenges posed by the physical environment, such as operation under extremes of temperature and humidity. In such a case, it may be necessary to place

the AP inside an enclosure to ensure that the operating conditions meet the manufacturer's specifications.

Noise and Interference Considerations

Wireless devices operating in the 2.4 GHz Industrial, Scientific and Medical (ISM) band in which 802.11b/g/n WLANs operate can interfere with an access point or client device trying to send or receive data. Certain devices can cause severe interference such as cordless phones, Class 1 Bluetooth devices in discovery mode, frequency hoppers (802.11 and otherwise), microwave ovens etc. If there is interference from such devices, you must consider ways to mitigate the interference as performance of the WLAN will otherwise be degraded. The 5 GHz band, although less cluttered, may still have interference. Wireless backhauls (the use of wireless communications systems to get data from an end user to a node) require clean RF on both the client side and backhaul side. If using a wireless backhaul in your network, the client or access side of the network should operate on a different frequency band than the backhaul side to reduce self- interference.

Antenna Considerations

The type of coverage required also has implications on the choice of antennas. Omni-directional antennas provide a sphere of coverage with the antenna at the center. Directional antennas provide a beam or cone of coverage with the antenna at the apex by focusing their radiation in a specific direction and thereby offer greater range than omni-directional antennas in the areas to which they are directed. For areas that will never be obstructed, Vocollect recommends smaller or more directional coverage areas that put the RF energy right where it is needed. Directional antennas allow the amount of energy that bleeds into other areas when the shelves are empty to be minimized and to fill in coverage where needed. Figure 1.2 depicts an example of a deployment using directional antennas to provide coverage down aisles and omni-directional antennas to provide coverage in more open areas.

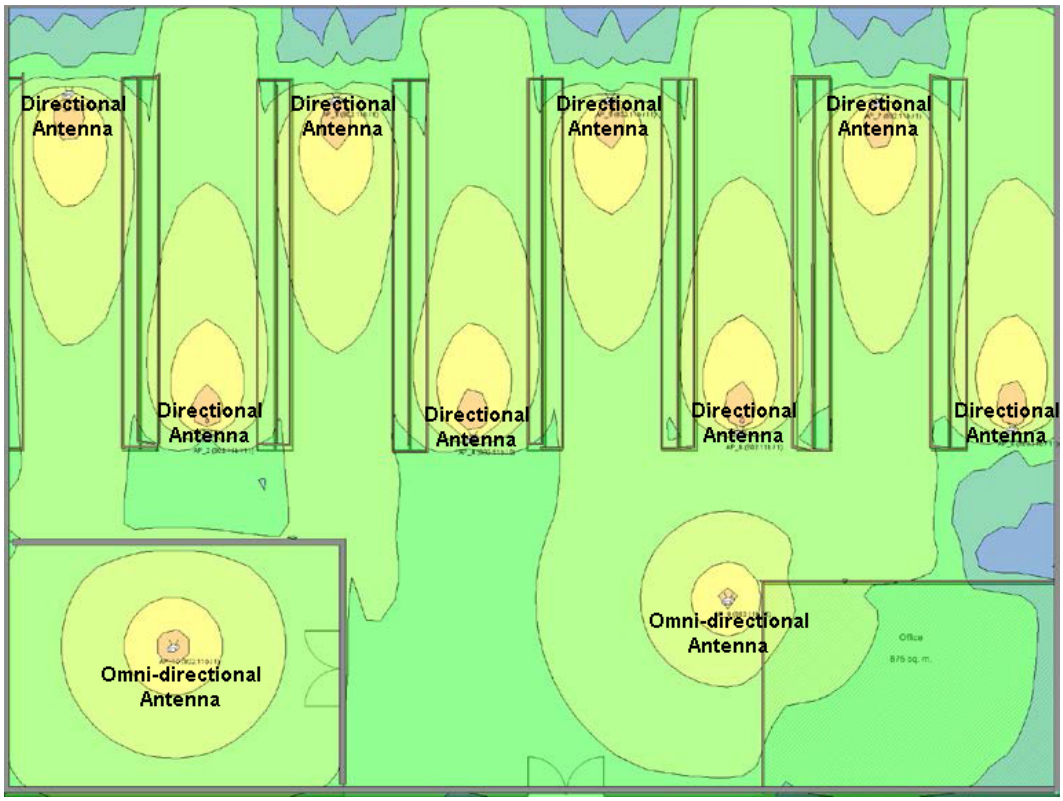

Figure 1.2: Example WLAN coverage using directional and Omni-directional antennas

Rates, Range and Robustness

The transmission range of an 802.11b/g radio decreases with increasing data rate, for a given transmit power level. The range at 1 Mbps is much greater than the range at 54 Mbps. This is because the receive sensitivity of 802.11 WLAN receivers decreases with increasing data rates. To be able to receive signals at a higher data rate the radio needs to receive signals at a higher power level than that required for a lower data rate. Note that a network capable of supporting a 54 Mbps data rate throughout its coverage area will require many more APs than a network that simply provides some wireless access everywhere.

The transmit power level does have a bearing on the range of a radio. Increasing the power level of a transmitted signal enables it to travel farther. Regulatory agencies that have jurisdiction over the use of WLAN radios specify the transmit power levels that can be used. These vary from region to region. For example, in the US a peak level of +36 dBm or 4W EIRP (Effective Isotropic Radiated Power) may be utilized, while in Europe the maximum is +20 dBm or 100mW EIRP. The effective isotropic radiated power (EIRP) is the sum of the radio transmitter power (in dBm) and the antenna gain (in dBi).

$$EIRP(dBm) = TxPwr(dBm) + Ant.Gain(dBi)$$

Important: Under no circumstances should the local regulatory limits be violated.

Figure 1.3 illustrates the approximate power-range relationship for various data rates. The plot is based on theoretical calculations of path loss in an indoor environment, taking into account receive sensitivity values typical of 802.11b/g radios. The calculations did not consider the effect of multipath fading, which would decrease the range further.

Vocollect Talkman terminals have a typical EIRP of about +20 dBm or 100 mWatts.

In order for two-way communications to function properly, the range of the AP should approximate the range of the mobile device. This ensures that each can "hear" each other without drowning out coexisting RF devices within the transmission range. As a rule of thumb, the range for 802.11a or 5 GHz will be reduced by one third compared to 2.4 GHz.

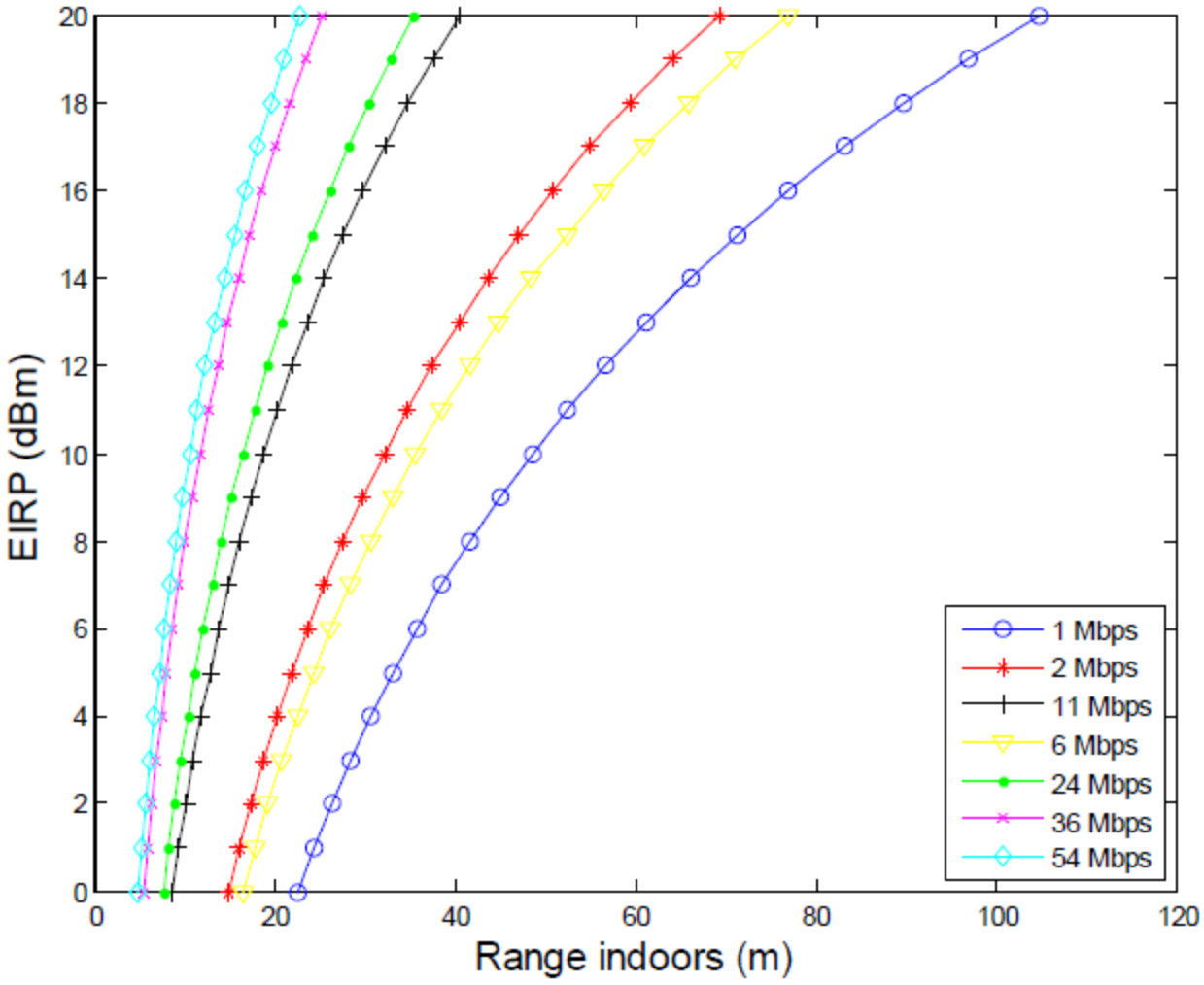

Figure 1.3: EIRP vs. Range for 802.11 b/g data rates

When a mobile device is communicating with an AP that has a strong signal, the highest supported data rate is used. If the mobile device moves away from the AP and the radio signal diminishes, a lower data rate is used to minimize data errors. This lowering of data rate

continues until a reliable signal cannot be maintained at the lowest supported data rate. A similar adaptation of data rate is also done as the received radio signal strengthens. This adaptive data rate mechanism adds to the robustness of a radio under varying channel conditions.

Mobility

The coverage area of a WLAN can be easily extended by installing additional APs with the same Service Set Identifier (SSID) and security settings, allowing uninterrupted handoff between them. The 802.11 WLAN standards support a break-before-make handoff mechanism at Layer 2 (the data link layer) that allows for mobile devices to roam between access points within the roaming domain. APs that are in the same broadcast domain (same subnet or VLAN) and configured with the same SSID are within the natively supported 802.11 roaming domain. Scaling the roaming domain beyond a single subnet or VLAN requires upper-layer solutions that add to the complexity of the roaming process and can impact application sessions during roaming. The application types that use the WLAN play a critical role in determining roaming requirements.

Although Talkman applications have minimal bandwidth requirements, they require coverage that allows for seamless roaming throughout the network.

Roaming in 802.11 WLANs is initiated and controlled by the mobile device and, therefore, the roaming algorithms are implemented in the client radios. It is important that the network is set up such that it facilitates the roaming process and makes it efficient. A key consideration is to lay out adjacent APs on unique channels, preferably non-overlapping channels (for example, channels 1, 6, 11 in the US; 1, 7, 13 in Europe). This allows for AP coverage areas to overlap, as shown in Figure 1.4 below. Such overlapping of coverage areas enables seamless roaming with minimal mutual interference.

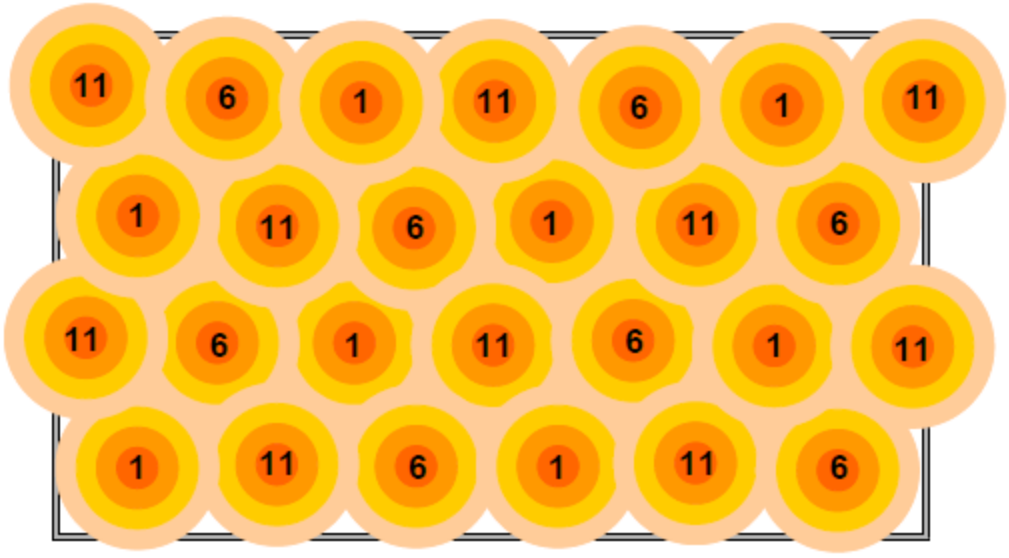

Figure 1.4: Extending coverage through non-overlapping channel layout

While an area may be covered by a WLAN network it is also important for that coverage to have the capacity needed to carry the demands of the attached wireless devices. Coverage and capacity should both be uniform to assure a seamless experience for all WLAN users.

This can be understood in simple terms as the number of users typically associated with a given AP and the type of applications they run. The density of APs within the coverage area plays an important role in application support. If there is a high concentration of users or bandwidth-intensive applications running on the WLAN, a high-capacity topology is preferred. In such a capacity-oriented setup, APs are placed closer together and their range adjusted accordingly, so that the load on the APs is reduced, allowing for more bandwidth per user. Networks designed for coverage only and based purely on a sparse AP layout to keep costs low may need to move to a higher-capacity deployment to accommodate additional demands on the network from the types of applications being run or an increase in the number of users.

Site Survey

A site survey is the only definite way to get an accurate representation of RF propagation in a targeted WLAN environment. RF site surveys facilitate verification and optimization of WLAN coverage and ensure that the WLAN environment is clear of any unintentional or outside interference. In recent years the cost of WLAN APs has fallen dramatically. This has precipitated a tendency to skip the site survey process entirely and simply install APs at regular intervals within a building. This method is not recommended. APs spaced too closely can cause them to interfere with each other. APs spaced too far apart will result in coverage gaps.

Engagement of a reputable network integrator with WLAN expertise is highly recommended. The integrator should be able to provide a spectrum analysis of your site to identify any potential sources of interference, be able to design your wireless network, recommend antenna options, guarantee needed RF coverage, perform a physical site survey, and provide comprehensive documentation once the WLAN installation is complete.

Site survey related recommendations:

- Assuming a spherical coverage area, the coverage of one AP should ideally overlap an adjacent AP's coverage area by 25% or less unless non-interfering channels usage can be guaranteed. Since antennas radiate in three dimensions, radiation patterns that extend above and below onto adjacent floors must be considered.
- The site survey should approximate mobile device performance as closely as possible by using a similar device, or by adjusting power as appropriate.

  Typically, the received signal level for optimal operation of Vocollect Talkman devices is - 70 dBm or better.

- Ideally, site surveys should be performed with the installation environment as close to its final configuration as possible. For example, when installing in an environment where inventory is stored, the inventory should be in place in the storage

locations prior to performing the RF survey. This ensures that radio signals will not be blocked by the final state of the environment.

- Identify sources of noise and interference from RF devices coexisting in the 2.4 or 5 GHz ISM band and other 802.11 WLAN networks. Investigate ways of reducing interference from these sources. Signal to noise ratio (SNR) is a good metric to determine the quality of the received signal relative to the noise level.

  An SNR of 25 or better is important for good performance.

- Mesh networks and outdoor networks require a different skill set when performing a site survey. LOS (Line of Sight) is critical in determining coverage for an outdoor network. Increased latency may occur in a mesh network depending on the number of hops. Using different RF frequency bands for the access side and backhaul side of the network is highly recommended to reduce RF interference.
- The IXIA IXChariot endpoint is installed on all Vocollect devices so network testing may be done using this endpoint. The endpoint is always available for use, no configuration is needed on the device. You may just put in the IP address of the Vocollect device as one of the endpoints and begin testing.

Security Considerations

No recommendation would be complete without some discussion on wireless LAN security. A comprehensive discussion is beyond the scope of this document. The right amount of security for your network will be a balance between the burden that your data security implementation imposes in terms of expense and administration, the value of the data being protected, and the likelihood of an incursion.

Wireless LAN security is designed to control access to the network through authentication and encryption mechanisms. Security implementations in WLANs are based on one of three models, each of which is described below.

Site-based

Security credentials are system- or site-wide. There is no capability to de-authorize only a single user. It assumes that anyone who has the credentials is authorized for use.

Device-based

Each device is uniquely authorized and can be de-authorized or expired independently. Authorization in the form of digital certificates and access control. Digital certificates can be administered transparently to the user.

Operator-based

Each user is authorized and de-authorized individually and independently of a particular device. Each operator is required to provide a valid login/password combination for access. This can be used in conjunction with a digital certificate, but user login is still required.

Table 4.1 summarizes the standards-based security protocols available for 802.11 WLANs.

Table 4.1: Security Standards Support

Standard	Encryption	Authentication	External Requirements
WEP	WEP	None	None
WPA-PSK	TKIP	Pre-Shared Key	None
WPA-Enterprise	TKIP	• EAP-TLS • EAP-TTLS/MSCHAPv2 • PEAPv0/EAP-MSCHAPv2 • PEAPv1/EAP-GTC • LEAP	RADIUS, LDAP*
WPA2-PSK	AES	Pre-Shared Key	None
WPA2-Enterprise	AES	• EAP-TLS • EAP-TTLS/MSCHAPv2 • PEAPv0/EAP-MSCHAPv2 • PEAPv1/EAP-GTC • LEAP	RADIUS, LDAP*
* LDAP is required for operator-based EAP implementations, and strongly recommended for site- and device-based implementations.			

WEP

The original encryption method used in 802.11 networks. WEP was later found to be vulnerable to cracking by exploiting weak keys. Most modern wireless infrastructure vendors have eliminated the use of weak keys. Check with your vendor to be certain. Even though WEP encryption can be cracked, it is only vulnerable when enough data is passed while on a single AP (roughly 500,000 uniquely keyed packets). Most mobile terminal applications do not pass enough data while not roaming and under the coverage of a single AP to allow cracking. The very mobile nature of the terminal is a substantial barrier against WEP cracking. Security can also be improved by enabling MAC address filtering.

WPA-PSK

Wireless Protected Access Pre-Shared Key (WPA-PSK) replaces WEP with a strong new encryption technology called Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC). WPA-PSK is a subset of the IEEE 802.11i specification. Deployment of

WPA/PSK is strongly recommended, as it overcomes the vulnerability of WEP but does not require a security server and the associated overhead costs.

WPA-Enterprise

WPA-Enterprise adds authentication via the Extensible Authentication Protocol (EAP) in combination with the IEEE 802.1x access protocol. Each client device must present its credentials to prove access privileges prior to connecting to the wireless network. The access privileges are verified against a RADIUS database. The type of credential and its presentation method is determined by the type of EAP authentication implemented. Supported EAP types are shown in the table above. WPA-Enterprise is a subset of the IEEE 802.11i specification and uses TKIP encryption.

WPA2-PSK

WPA2 Pre-Shared Key is the upgraded version of WPA-PSK. It uses a new advanced encryption mechanism using the Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES). AES satisfies U.S. government security requirements and has been adopted as an official government standard by the U.S. Department of Commerce and the National Institutes of Standards and Technology (NIST). Organizations that require the AES encryption available in WPA2 should be aware that upgrading to it may require new hardware.

WPA2-Enterprise

WPA2-Enterprise is the certified interoperable version of the full IEEE 802.11i specification which was ratified in June 2004. Like WPA, WPA2 supports IEEE 802.1X/EAP authentication, or PSK technology. It also includes the Advanced Encryption Standard (AES) as its encryption method.

Vocollect is committed to supporting the best 802.11i standards-based wireless security methods.

Table 4.2 shows the security standards supported by Talkman terminal models.

Table 4.2: Security Standards Support

Standard	Model			
	Legacy Platforms			Current Platforms
	T2	T2xT5 (non-RoHS*)	T2x (RoHS) T5 (RoHS) T5m T1	A500 A700
WPA-PSK	✓	✓	✓	✓
WPA-Enterprise	✓	✓	✓	✓
WPA2-PSK	•	✓	✓	✓
WPA2-Enterprise	•	•	✓	✓
*RoHS terminals began shipment in 2006 to meet European Union Restriction on Hazardous Substances regulations. All current shipping units are RoHS compliant.				

4 AP Configuration Recommendations

There are many options when configuring an Access Point and there are many manufacturer specific parameters, so this section does not attempt to cover them all. The following table summarizes Vocollect's recommendations for specific configuration settings. Note that none of these settings are absolutely required, but are recommended, based on experience. Details about the settings are provided following the table.

Table 5.1: Configuration Recommendations

Data Rates	Restriction of basic rates to 1 and 2Mbps (6 and 9 Mbps for 802.11a or 802.11g-only networks)
Antenna Diversity	Dual antenna diversity enabled
Output Power	30mW – 50mW (15dBm – 17dBm)
Traffic Filtering	Filter out extraneous broadcast traffic, same IP subnet and VLAN
Security	WEP at minimum, WPA2-Enterprise recommended
DTIM	Set to 2 beacon intervals (assumes beacon interval of 100 msec)
Broadcast SSID	Recommended for interoperability. Required if using 802.11a DFS channels.
WPA Handshake Timeout	Set to 1000 msec to allow time for EAPoL handshake packets to be transmitted—especially when using PSP (Power Save Polling) mode.

Data Rates

APs are designed to operate at varying data rates. An 802.11b AP uses data rates of 11, 5.5, 2, and 1 Mbps while an 802.11g AP can operate at rates up to 54 Mbps. APs can be configured to either operate at all of the available data rates or be restricted to only specific data rates. The basic rates setting defines the data rates at which all devices on the network should be capable of operating. Supported rates are rates at which the AP is capable of operating. All control and management packets are sent out at the basic rate. It is recommended that the basic rates be set to 1 and 2 Mbps only for b and b/g networks, and to 6 and 9 Mbps for g-only network. Also, for mixed b/g networks it should be ensured that protected mode (CTS-to-self) is activated.

Antenna Diversity

Enterprise class access points generally support antenna diversity. The purpose of antenna diversity is to allow for two separate receive paths so that a signal null is unlikely at both antennas simultaneously. This is especially important in mobile environments or where metal structures exist in the AP coverage area. In order for antenna diversity to work, the AP software configuration must be set to use two antennas.

Output Power

You may be tempted to set the output power at maximum for a large RF coverage area. However, this can result in mutual interference between APs. Mutual interference can be minimized by careful placement of the AP when installed. In general, APs should be installed so that the RF coverage area of one AP has no or minimal overlap into the coverage area of a neighboring AP on the same channel. Lower power settings can make overlap more manageable. In general, an output power setting in the range of 30mW-50mW (about +15 to +17 dBm) on the AP better approximates the range of a mobile device and limits mutual interference. This parameter specifies the transmitter output power only. To obtain an EIRP value, you can just take the transmitter power (in dBm), add the gain of the antenna (in dBi) and subtract the losses of the cable or other inserted devices (in dB). The WLAN installer can recommend the optimum power setting for two- way communications through a site survey.

Broadcast Traffic

When deploying WLANs, it is especially important to eliminate extraneous broadcast traffic from being passed from the wired LAN. Broadcasts are widely used by Microsoft, Novell, and other enterprise network operating systems. By design, broadcast packets require all receiving devices to process the data they contain, even if the data is not applicable to the receiving device. This unnecessary packet processing on battery powered mobile devices results in poor user response and decreases battery runtime. Broadcast traffic can be filtered by using settings in the AP, or through the design of the wired LAN (e.g., VLANs). Consult with your WLAN vendor to determine the best method for your architecture.

Security

At the very minimum, WEP (Wired Equivalent Privacy) security should be enabled. Better security is always more desirable. Other more advanced security methods are available and may be more desirable for your organization. The more advanced the security, more the overhead that is required for additional equipment and administration. As the security method will have a direct impact on the performance of the WLAN, it is important to fully understand the implications of its choice. The chosen security method must be supported by all client devices on the network.

5 WLAN Frequently Asked Questions

Should I upgrade to the latest access point or wireless controller firmware?

Yes. Most wireless vendors make frequent updates to their firmware in order to improve performance and address issues.

Do you support 802.11d? What is its purpose?

A700 devices support the 802.11d standard, which enables the Talkman device to automatically detect and correctly configure the correct regulatory parameters for the country in which it is operating. This causes the device to use the correct radio power levels and frequencies for the country.

What does 802.11n support on A700 devices mean to my network?

All RF information in this document regarding site layout, signal strength and channel selection also applies to 802.11n. A700 devices will operate in a non-802.11n environment with no issues. The 802.11n radio in A700 devices operates as a single spatial stream (not multiple input/output, or MIMO), 20 MHz wide channel signal with a short guard interval and is capable of a maximum throughput of 72 Mbps. It supports MCS 0-7 data rates. 802.11n operates on either the 2.4 GHz (802.11bg) or the 5 GHz (802.11a) RF band.

Will the way that the Talkman device is worn or placed have any effect on its radio performance?

The WLAN antenna in Talkman devices is designed to work optimally when worn as recommended. The antenna orientation is designed to match typical warehouse antennas that are in a vertical position. If the device is not worn on the belt or shoulder holster, it should be placed in a Vocollect-approved holder or in a secure location away from any objects that may shield the RF antenna, and in a similar position to that it would have if it were being worn. Typically, this is horizontally—where the long edge of the device is parallel to the floor. Vocollect does not recommend vertically mounting the Talkman with its long edge perpendicular to the floor.

Why does Vocollect recommend an RSSI of -70 dBm or better throughout the site?

Ideal performance is maintained when the Vocollect device is operating at the highest data rate available based on the receive sensitivity of the radio. Signal strength must be strong enough to operate at the higher 802.11 data rates and ensure the radio is not continuously scanning for a new AP.

Can other devices operating in the 2.4 GHz frequency range cause issues with my WLAN or Vocollect devices?

Any interference due to non-WLAN traffic (microwaves, cell phones, Bluetooth devices) may cause packets to be lost in the air due to collisions. A failed packet will initiate MAC retries and TCP back-offs, which introduces more WLAN traffic and latency in the WLAN packet.

Rather than worry about under-coverage or dead spots, should I just blanket my site with access points and provide over-coverage?

Over-coverage is worse than under-coverage. WLAN channels used should be non- over-lapping and the cell size controlled by the TX power of the access point not by limiting data rates. (For example, not using 1 and 2 Mbps is not a recommended way of shrinking a cell).

Is it necessary to have a line-of-sight (LOS) from the Talkman device to the access point for adequate coverage?

If the work area is covered by only one AP (with no other AP to roam to) and there are no reflective surfaces (metal shelving, ceiling), then the RF may have only one path to the device so a LOS connection is critical.

My Talkman device is being frequently "deauthenticated". What is causing this?

If "deauthentication" is due to the client or the AP not receiving packets, this is typically a symptom of RF interference. All Vocollect terminals have a radio RX sensitivity of -92 to -96 dBm at 1 Mbps.

Some APs now deauthenticate the client at a specified interval and/or require the client to renegotiate the groupwise key due to "broadcast key rotation" being specified.

How does the Talkman device determine if it should be roaming to a new access point?

Vocollect terminals are configured to begin scanning for a new AP at -75 dBm RSSI (Received Signal Strength Indicator). To scan for a new AP, the terminal must leave the current RF operating channel and scan on all available channels. The terminal will then roam to an AP that is at least 5 dB higher in RF power. Frequent scanning and roaming when using more advanced security may cause a slight delay if occurring during a LUT or ODR transfer.

My EAPoL handshake is failing. How can I fix this?

If the WPA handshake time is set to less than 1000 msec., the client radio may not have enough time to respond, which results in failures to authenticate. Vocollect recommends that the WPA handshake timeout be set to 1000 msec. or greater.

What is the optimal level of DTIM (Delivery Traffic Indicator Messages) when using Power Save mode?

To reduce latency to an acceptable level for voice applications, the DTIM setting must be set to no greater than 2 based on a 100 msec beacon interval. With a setting of 2, latency will not

exceed 200 msec. Setting to greater than 2 will cause a perceptible delay in the voice application.

The network throughput seems to be low. What should I do?

If available on the network, configure the Talkman for 802.11g rates.

Do Cisco Compatible Extensions (CCX) need to be disabled?

Although Vocollect clients are not CCX certified, all clients will operate in a CCX network and include CCX features after they are approved 802.11 standards.

6 Additional Information

There are a number of excellent resources for additional information. Below are some links to articles and books:

http://www.oreillynet.com/pub/a/wireless/2005/05/02/80211myths.html http://www.wi-fiplanet.com/tutorials/article.php/1116311

802.11 Wireless Networks: The Definitive Guide, 2nd Ed. by Matthew S. Gast, ISBN 0-596-10052-3

802.11 Wireless LAN Fundamentals: A Practical Guide to Understanding, Designing and Operating 802.11 WLANs, by Pejman Roshan and Jonathan Leary, ISBN 1-58705-077-3

Ensuring Wireless Security In Your Distribution Center Voice Operations, Vocollect

Appendix A: EAP Recommendations and Requirements

This appendix describes recommendations and requirements for implementing Extensible Authentication Protocol (EAP) as used in Vocollect VoiceConsole®. EAP is part of the next generation of a wireless security protocol that supports a variety of authentication types. For more information on these concepts, see the document EAP Wireless Security: A White Paper.

This document provides different recommendations for the three credential association types that can be set up in VoiceConsole: site-based, device-based and operator-based. These are described in greater detail below.

General Concepts

Credential Distribution

VoiceConsole will be distributing credentials to devices in the configuration (.cci) file. Once these credentials are on the devices, the devices will use them to connect to the wireless network. Credentials only need to be entered once per site, operator or device until the credentials need to be changed. When necessary, VoiceConsole will manage the distribution of the new credentials.

Site-wide Configuration

Although we are offer three credential association types in VoiceConsole, each of these must be configured on a site-wide basis. That is, even if the client selects to have device-, site- or operator-based security, all devices and operators at a particular site must use the same type of security. This is reinforced by the user interface, which requires that you select one and only one EAP type per site.

Restricted User

With each type of security, we are requiring a restricted user. The restricted user lets the device connect to the network with a restricted set of credentials, identifying itself as a Vocollect device. It can only connect to VoiceConsole, from where it can load the proper credentials. You can further restrict this user's access by assigning it to a different SSID that only has access to a portion of the network. This different SSID may be on an open network. In this case, you would not need credentials for the restricted user.

Without the restricted user solution, we would require that the credentials be loaded onto each device through the serial port if the credentials expire or become obsolete when the password is changed. The restricted user has the following roles:

- When the device is in the charger, the restricted user is used to log onto the network.

- Credentials are distributed through the restricted user through the Talkman® T5 Combination Charger, TouchConfig, or over the network.
- The restricted user can load tasks and operators.

PINs

PINs are not part of standard security, but are used by Vocollect to provide an additional level of security. PINs are numeric Personal Identification Numbers of up to eight characters in length that the operator will select on the Talkman and are used to uniquely identify a user logging onto the network. If you choose to use PINs, there are a variety of circumstances under which the operator will be forced to enter the PIN.

When **Use PINs?** is set to Yes and:

- a device is shut down and restarted
- the **Device Behavior: Log off of the network when it goes into the charger** check box is selected and a device is removed from the charger and the operator turns it on
- an operator load occurred and the operator turns on the device afterward
- the actual (not the restricted) user information changed such that PINs are now required and it is the next time after the change the operator is turning on the device.

Device Behavior

There is a check box available in the EAP configuration that lets you force the device to log off when it is in the charger. When it logs in, it will be as the restricted user. This option is selected by default when you select the operator-based configuration.

Note: If the restricted user credentials expire, you will be required to load the credentials by the serial port. We recommend that you either set the restricted user credentials to not expire or you change the credentials in advance of their expiration.

LDAP

VoiceConsole can use an existing Lightweight Directory Access Protocol (LDAP) server to:

- Verify that entered credentials are correct
- Change the credentials on the server when they are changed in VoiceConsole

Note: You must configure LDAP settings when setting up an operator-based configuration. The initial login of an operator must be confirmed by an external source as VoiceConsole does not yet have this information.

Note: Credential changes only happen through a secure connection.

What You Will Need

The VoiceConsole EAP Security options will either be configured by or with significant input from an IT professional. It is this person who will make the decision as to which type of configuration will be used at this site and will have the needed information described in the table below.

These concepts will be described in greater detail in the configuration sections below as they are relevant to each association.

Field	Description
EAP Type	Which EAP method the device will use to authenticate to the client's network. These are described in detail later in the document.
Association	Which of the three credential association options the client would like to select (site-based, device-based or operator-based)
Type	Which type of credentials the client wants the device to use to authenticate to the network
Use PINS?	Whether the user will need to enter a PIN to get onto the network
Device Behavior	Whether the device will log off when it goes into the charger
Restricted User	The username and password/certificate of the restricted user that the device will use when it is on the charger in order to communicate to VoiceConsole.
Site-wide PIN	The PIN that the user will have to enter to log onto the network

LDAP settings are optional for site- and device-based association types. They are required for the operator-based association type.

Field	Description
LDAP Host	The hostname of the machine on which the LDAP server is running
LDAP Port	The port that the LDAP server is listening on.
LDAP Search Distinguished Name	The username that VoiceConsole will use when attempting to find the distinguished name of an operator in the Directory Service
LDAP Search User Password	The password that VoiceConsole will use when attempting to find the distinguished name of an operator in the Directory Service
LDAP Search Base	The search base that VoiceConsole will use when trying to find a particular user in the Directory Service
LDAP Searchable Attribute	The attribute that VoiceConsole will search on when trying to find a particular user in the Directory Service
LDAP Password Attribute	The attribute that VoiceConsole will modify when changing the password of a user in the Directory Service

Default Active Directory Settings

The examples shown here are a guide for formatting; the actual settings may be different at your site.

AD login name/username: sAMAccountName

Port:

636 is default for SSL

389 is default for non-SSL

AD SearchUserName assuming vanilla AD:

dn=cn=<users DISPLAY name>,cn=Users,dc=<domain>,dc=<Top Level Domain>

AD Default SearchBase (for testing large AD installs, this could cause delays):

Dc=<domain>,DC=<Top Level Domain e.g., com, int, net, org, ...>

Alternately, reduce the scope to just users:

cn=User,dc=<domain>,dc=<Top Level Domain>

AD Password Attribute: unicodePWD

Operator Login

The operator-based configuration differs from the site- and device-based in that it requires the operators to interact with the VoiceConsole user interface. Operators will set up their network usernames and passwords through VoiceConsole. If the client requires that the passwords adhere to a corporate policy—for example, they must contain at least one number and one special character—the validation for this must be done through the directory server.

Changing Credentials

If network credentials need to be changed, we recommend that you do not change the restricted user's credentials at the same time as the actual credentials, or there is a possibility that the operators will be unable to log onto the network.

Likewise, do not delete old credentials until all devices have downloaded the current credentials.

EAP Types and Descriptions

The table below describes each of the supported EAP methods.

Type	Stands for	Definition
EAP-TLS	EAP-Transport Layer Security	A newer version of the SSL protocol, It supports more cryptographic algorithms than SSL. TLS is designed to authenticate and encrypt data communications, preventing eavesdropping, message forgery and interference.
EAP-TTLS/ MSCHAPv2	EAP-Tunneled Transport Layer Security/Microsoft Challenge Authentication Handshake Protocol version 2	Securely tunnels clients authentication within TLS records
PEAPv0/ EAP-MSCHAPv2	Protected Extensible Authentication Protocol version 0/Microsoft Challenge Authentication Handshake Protocol version 2	A proprietary, extended-function version of EAP that Microsoft, Cisco and RSA Security developed
PEAPv1/EAP-GTC	Protected Extensible Authentication Protocol version 1/Generic Token Card	A protocol developed jointly by Microsoft, RSA Security and Cisco for transmitting authentication data, including passwords, over 802.11 wireless networks. PEAP authenticates wireless LAN clients using only server-side digital certificates by creating an encrypted SSL/TLS tunnel between the client and the authentication
LEAP	Lightweight Extensible Authentication Protocol	A proprietary Cisco protocol used for 802.1X authentication

Appendix B: Glossary

A

Access Point

A hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN. APs are important for providing heightened wireless security and for extending the physical range of service.

D

Delivery Traffic Indication Message

A kind of traffic indication map (TIM) that informs the clients about the presence of buffered multicast/broadcast data on the access point.

E

Effective Isotropic Radiated Power

In antenna measurements, the measured radiated power in a single direction.

I

Industrial Scientific and Medical

Radio bands (portions of the radio spectrum) reserved internationally for the use of radio frequency (RF) energy for industrial, scientific and medical purposes other than telecommunications. Iin recent years the fastest-growing uses of these bands have been for short-range, low power communications systems. Cordless phones, Bluetooth devices, near field communication (NFC) devices, and wireless computer networks all use frequencies allocated to low power communications as well as ISM.

L

Line of Sight

Radio frequency technologies use the term LOS to describe an unobstructed path between the location of the signal transmitter and the location of the signal receiver. Obstacles that can cause an obstruction in the line of sight include trees, buildings, mountains, hills and other natural or manmade structures or objects.

N

Near Line of Sight

Radio frequency technologies use the term NLOS to describe a partially obstructed path between the location of the signal transmitter and the location of the signal receiver. Obstacles that can cause an obstruction in the line of sight include trees, buildings, mountains, hills and other natural or manmade structures or objects.

R

Radio Frequency

Any frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. Many wireless technologies are based on RF field propagation.

S

Service Set Identifier

A case sensitive, 32 alphanumeric character unique identifier attached to the header of packets sent over a wireless local-area network (WLAN) that acts as a password when a mobile device tries to connect to the basic service set (BSS) -- a component of the IEEE 802.11 WLAN architecture.

Signal to Noise Ratio

A measure that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power, often expressed in decibels.

Index