

# Considerations for Planning and Deploying a Wireless LAN



Wireless LANs continue to grow in capability and availability. If your organization is expanding the use of wireless LANs and/or implementing functionality such as Voice over Wi-Fi calling, this document will assist you through a review of several areas of consideration.





# Table of Contents

## Contents

<b>Introduction</b>	<b>3</b>
In this document	3
<b>Section 1: Considerations for deploying a WLAN</b>	<b>4</b>
What applications do users need?	4
Overview	4
Data applications	5
Voice applications	5
Mixed voice and data applications	5
Quality of service	6
Coverage	7
Coverage versus capacity	8
WLAN standards	9
IEEE 802.11	9
Differences between IEEE 802.11a, 802.11b, 802.11g, and 802.11n	10
Dual-band radios and dual-radio APs	11
Additional functions and certifications	11
Voice considerations	11
Standalone and centrally coordinated wireless networks	12
Site survey	13
Obstacles to signal strength	13
Security	14
VPN	16
RF Monitoring, intrusion detection, and quarantine	16
Secured access using unsecured WLANs	17
Home WLAN guidelines	17
Hotspot WLAN guidelines	18
Putting it all together for voice and data over a WLAN	18
<b>Section 2: Questions to ask WLAN Vendors</b>	<b>19</b>
Architecture	19
Standards and certifications	19
APs	20
WLAN end-user devices	20
Management	21
Security	21
<b>Glossary</b>	<b>22</b>
<b>Legal Notice</b>	<b>25</b>

## Introduction

Wireless Local Area Networks (WLANs) continue to grow in capability and availability, particularly in enterprise networks. Your organization might be considering deploying a new WLAN or expanding an existing WLAN infrastructure, to leverage the advantages of this technology, such as:

- Reducing the amount of cabling to mobilize the workplace.
- Mobile, ubiquitous access to enterprise IT systems throughout the global enterprise.
- A more productive and efficient workforce, with employee access to resources without being tethered to a traditionally wired network connection.

Equally important within an enterprise is the ability to leverage the WLAN for PBX-based mobile voice communication. Using the BlackBerry® Enterprise Server solution in combination with BlackBerry® Mobile Voice System 5.0, BlackBerry® smartphone users can now have access to the enterprise data applications and also take advantage of VoWLAN for PBX voice communication.

WLANs can allow workers to access and contribute information far more quickly than before, boosting the productivity of all workers who depend on that critical information and increasing the overall agility of the organization.

## In this document

**Section 1: Considerations for deploying a WLAN:** Identifies areas that might be considered in the planning and requirements definition of deploying a WLAN, including use for voice, to assist organizations that are beginning to plan for a WLAN deployment or upgrade.

**Section 2: Questions to ask WLAN Vendors:** Builds on the consideration areas and provides questions you should ask a WLAN equipment and services vendor.

## Section 1: Considerations for deploying a WLAN

### Overview

One of the most important questions to ask is what you're looking for in your WLAN solution that you can't get from your wired LAN. The feature that makes most people take the wireless plunge is mobility: the ability to connect to the network through the air from anywhere near a wireless AP. But enabling mobility for your organization using WLAN technology leads to other questions, such as:

- What does mobility mean to you and your organization?
- Does it mean you want to be able to have network connectivity throughout your offices?
- Do you want your remote offices to be connected, too?
- If you have a campus, do you want to be able to connect to the network both inside and outside?
- Do you want to talk on your VoWLAN phone from one end of the building to the other without dropping your connection, or use your mobile device anywhere from the lobby to the most remote area in the facility?

These types of questions and others regarding security, management, and so on, all need to be explored and identified as part of the design process to effectively plan and deploy a successful WLAN. This section addresses these important initial considerations.

### What applications do users need?

#### Overview

Wireless capacity is a finite, scarce and shared resource. Engineering with little planning, or not understanding the true nature of applications, as is often found for wired LANs, is not an option for wireless LANs.

A good understanding of the applications and the load they will generate is essential to avoid overestimating the cost of the WLAN or underestimating the coverage and capacity you need, and will result in a more effective and usable experience for all WLAN users.

Because of the shared nature of the wireless medium, deploying too many APs might contribute to polluting the air waves without any tangible increase in usability.

Key application parameters to consider when planning a WLAN deployment include the:

- application mix
- relative proportion of voice and data traffic
- expected traffic demands
- application performance requirements

These application requirements eventually translate into constraints for the WLAN deployment such as the minimum rate and maximum cell coverage.

The performance metrics and performance targets used to assess the users' quality of experience depend on the type of application being assessed. The quality of experience is the overall performance of a system from the point of view of its end users. It is a measure of how the system lets users do what they need to do, when they need to do it.

## Data applications

For data applications, the time elapsed between the moment the user issues a command and the time when the output of the command is displayed at the user's device is a key measure of the perceived quality of the system. Different applications have varying response time requirements.

Interactive applications in which users issue commands and expect "immediate" results typically require end-to-end, round-trip delays of less than 400ms. This may seem like a lot but it includes not only the network propagation, serialization and queuing delays, but also the TCP timeouts and retransmissions, and the processing delays in the end systems. The wireless data throughput rate has only a limited effect on the response time when small amounts of data are transmitted. The wireless connection performance in terms of delay and quality characteristics are the most important factor in providing a good experience for applications that use small data transactions.

For applications in which larger amounts of data are transferred, such as email and browser-based applications, users are usually prepared to tolerate delays of a few seconds. Because of the larger amount of data that must be transferred, the actual data throughput rate of the connection is more important in this case. But the connection quality, measured by the number of packets delivered, also remains essential since TCP, the transport protocol used by a majority of data applications, interprets packet losses as an indication that it should slow down its transmission rate. Even if the nominal data throughput rate is high, the actual TCP throughput will not be very high unless the packet loss rate remains low.

## Voice applications

There are many areas within a WLAN design and deployment that can affect the performance of the voice capability on a WLAN. The WLAN architecture, roaming, QoS, and RF planning all place demands on the connection quality, coverage, and user experience when using VoWLAN. Voice applications are very sensitive to latency or delay, jitter, and packet loss. Conversational voice has much more stringent delay requirements than any other application.

For excellent conversational voice quality of experience, the end-to-end one-way delay should be less than 150 milliseconds. Beyond this point some users may notice the delay.

A number of factors contribute to the one-way delay of VoIP connections and, therefore, the WLAN can only use a small portion of the total 150 millisecond delay budget. Significant contributors to the delay include the packetization, propagation, de-jitter, and playout delays. Other delay contributors include processing delays in the end systems and queuing delays in the network routers and switches. In a typical Enterprise network, approximately 50 milliseconds of the total 150 millisecond end-to-end delay budget is available to WLAN networking. The communications delay between a WLAN phone and the AP must be less than 50 milliseconds, and the phone must be able to roam from one AP to another within 50 milliseconds.

## Mixed voice and data applications

The traffic streams generated by voice and data applications have very different characteristics and it is even more challenging to meet the requirements of both types of traffic with one network. Voice traffic is made up of short packets that are fairly evenly distributed in time. As long as they do not exhaust the medium capacity, several voice streams can coexist on the WLAN without any noticeable impact on voice quality.

Data applications, on the other hand, tend to generate bursts of rather large packets. These bursts often involve several kilobytes of data. Bursty streams can coexist on the same LAN without any significant degradation of data application performance. But in a wireless network, if no precautions are taken, even a single bursty data stream can temporarily saturate the medium capacity and cause delays and losses impacting voice quality on an otherwise lightly loaded WLAN.

A mixed voice and data environment deployed with the current IEEE® 802.11® standards without any QoS mechanism is unlikely to result in a satisfactory experience, especially for the voice users. In the absence of any QoS mechanisms, an alternative workaround involves separating voice and data traffic users by frequency bands, for example, using IEEE® 802.11b/g for data-only users and IEEE® 802.11a/n for voice and data users (the differences between frequency bands are described in [WLAN standards](#)).

This approach is relatively easy to implement with multi-mode APs, but consider the following:

- It requires two channels per cell: one in the 2.4 GHz band for IEEE® 802.11 b/g clients, and one in the 5 GHz band for the IEEE® 802.11 a/n clients.
- The number of channels available in the 2.4 GHz band for planning each of the voice and data WLANs is smaller and the co-channel interference problems are more serious in a large deployment.

## Quality of service

QoS mechanisms are necessary to ensure that there is an acceptable voice experience over the WLAN. There are many alternatives in deploying QoS for the WLAN with the best solution (or mixture of alternatives) depending on your environment.

The following are some of the most widely deployed and effective QoS methods for WLAN environments:

- VLANs: Use VLANs to separate data and voice traffic. VLANs serve many functions, including security and scalability, but for QoS, VLANs serve the purpose of isolating higher-priority voice traffic so that it can be dealt with using maximum resources.

This requires a minimum of two VLANs, one for voice and one for data, with an assigned SSID on the WLAN for each VLAN. Using separate data and voice VLANs allows for specifying QoS settings on all traffic on the voice VLAN to give it a higher QoS profile.

- WMM: To improve the reliability of voice transmissions in the unpredictable wireless environment, APs and VoWLAN devices should support the industry-standard Wi-Fi® Alliance's "WMM certified". WMM is based on the IEEE 802.11e EDCA (enhanced distributed channel access) mechanism. WMM enables differentiated services for voice, video, best-effort data, and other traffic.
- CAC: Various WLAN infrastructure vendors support IEEE 802.11e CAC to limit the call capacity on a "per-access-point" basis. WLAN-capable devices must have support of the vendor's particular implementation to take advantage of CAC.

CAC works by assigning a voice flow by the WLAN system and allocating bandwidth to client devices on a first-come, first-served basis. The WLAN system maintains a small reserve so the mobile voice clients can roam onto a neighboring AP. Once the limit for voice bandwidth is reached on an AP, the next call is prevented from using the original AP to initiate the call and is automatically load-balanced to a neighboring AP and the call is completed without affecting the quality of the existing calls on the channel.

## Coverage

Mobility is a major reason that companies go wireless. Yet many discover that the wireless coverage is insufficient, hampered by “dead-spots” or has inadequately sized overlap of coverage between APs, resulting in dropped connections. A detailed site survey, described in [Site survey](#), can help minimize and even prevent these coverage issues.

However, the restriction of mobility is always a possibility with wireless networks. Where multiple addressing subnets on the Wireless network exist, many IT personnel are unaware of the limitations posed when roaming workers cross over subnets. For example, VoWLAN applications require the device to remain on the same subnet in order to maintain the IP address while roaming from one AP to another, preventing long roaming latencies and dropped calls. Additionally, depending on how the WLAN security solution is implemented, it might not permit users to cross over subnets or even to leave a specific coverage area.

Consequently, both standards-based and vendor-specific roaming capabilities must be closely examined. In larger campus settings, IP addressing and user mobility across various network segments will become increasingly important. Standards-based roaming capabilities include mapping a VLAN to an IP subnet, thus limiting broadcast traffic to the subnet and eliminating roaming across subnets. To address roaming and other manageability issues, vendor-specific solutions build on top of VLAN mapping and use their specific technologies to increase the scalability and manageability of the whole WLAN infrastructure.

The shape of an area is another consideration. A narrow, elongated area, for example, may require more APs than its surface area would seem to indicate. This is because some of the roughly circular coverage of the APs will fall outside the area of interest. Generally, irregular areas will require more APs, and/or external antennae with specific radio propagation patterns, than regular ones.

For example, semi-directional antennae could be used to provide coverage from the side of an atrium and highly directional antennae would be useful down hallways. Conversely, if the coverage area includes multiple adjacent floors, depending on the type of floor building materials, it may be possible to take advantage of the fact that radio signals penetrate through ceilings to provide coverage between floors. For example, coverage of a three-storey building might be achieved by deploying APs only on the first and third floors.

VoWLAN devices impose strict requirements on roaming between APs because of the traffic characteristics for voice and the sensitivity to jitter and delay. VoWLAN requires more overlapping coverage and denser deployment of APs. In this case, RF planning and analysis tools are crucial to maintain high service levels.

There are professional service organizations that will perform WLAN site surveys. This is important for all applications but becomes critical when VoWLAN is introduced. There are also a number of software tools that can be used to collect and report site survey results. All WLAN-enabled BlackBerry® smartphones include a site survey tool that should be used to collect site data. This data provides results that will be based on the BlackBerry smartphone’s actual WLAN characteristics versus other end-points, such as a laptop.

## Coverage versus capacity

Simple site surveys, while guaranteeing coverage, do not guarantee that your organization's capacity or performance targets will be met. Because of the nature of the shared medium, and the dependence of effective throughput on packet sizes, the WLAN traffic characteristics also need to be taken into account to ensure satisfactory performance for all users and applications.

In larger deployments where channels are reused, the WLAN performance can be degraded by co-channel interference, and a simple site survey, while verifying a specific data rate with no interfering traffic, may not take into account the data rate reduction due to the increase in noise from additional channels.

Due to the interactions and interferences that are only present in a full deployment, further analysis is required to guarantee both coverage and capacity. Automated real-time planning tools can help refine the number, placement and configuration of APs.

The WLAN user population, usage patterns, physical layout, and application mix will probably change over time, especially during the early phases of the WLAN deployment.

Detailed activity reports and intelligent management systems are required to monitor the health of the WLAN. For example, you may need to adjust the power levels to minimize interferences and maximize capacity and performance, and to automatically identify problem areas before they impact the users' quality of experience.

Later in this section there is a more in-depth discussion of the requirements and expected outputs of a [Site survey](#).

## WLAN standards

### IEEE 802.11

IEEE® 802.11™ - otherwise known as the Wi-Fi® standard - denotes a set of standards for WLANs. The original IEEE 802.11 standard, released in 1997, defines a common media MAC layer that supports the operation of all 802.11 based WLANs by performing core functions such as managing communications between radio network cards and APs.

Subsequent amendments to IEEE 802.11 define specific physical layers that enabled three faster radio layers: 802.11a and 802.11b in 1999, and 802.11g in 2003. Work on a new high-speed physical layer (802.11n) started in late 2003 and was ratified in October 2009. The physical layer defines the data transmission for the WLAN, using various modulation schemes.

The IEEE 802.11a physical layer which was originally defined for the 5 GHz band supports up to 54 Mbps data rates using OFDM technology.

The IEEE 802.11b physical layer is a backward-compatible extension of the original DSSS radio physical layer in the 2.4 GHz band that supports up to 11 Mbps data rates.

The IEEE 802.11g amendment extended the use of OFDM to the 2.4 GHz band with some modifications required for backwards compatibility with the 802.11b devices operating in this band.

The IEEE 802.11h amendment allows devices operating in the 5 GHz band to meet the regulatory requirements stipulated by some countries. It provides a mechanism to identify and adjust WLAN transmissions that interfere with radar systems by implementing DFS and TPC. DFS ensure that the access points avoid channels that contain radar and TPC allows the access point to mandate a maximum power output to its connected devices. DFS and TPC implementation and the subsequent impacts should be discussed with your WLAN vendor to ensure that all WLAN devices can conform and work properly within the WLAN. The WLAN device must ensure that there is no radar operating on a DFS channel prior to transmitting on that channel. As a result, access point handover is less efficient when access points are deployed on channels in the DFS bands. It might be necessary to avoid deploying access points with DFS channels so that WLAN devices can properly connect and roam between access points.

The IEEE 802.11n amendment added the following:

- MIMO, a technology that uses multiple antennas to coherently resolve more information than possible using a single antenna.
- 40 MHz channels double the channel width from 20 MHz in previous 802.11b/g/a physical layer standards to transmit and receive data. This allows for a doubling of the physical layer data rate over a single 20 MHz channel.
- Frame aggregation, which allows devices to combine several packets into one, reducing the wasted overhead between frames.

Coupling MIMO architecture with wider bandwidth channels offers increased physical transfer rate over 802.11a (5 GHz) and 802.11g (2.4 GHz) with a theoretical maximum data rate of 450 Mbps using the different optional features of 802.11n.

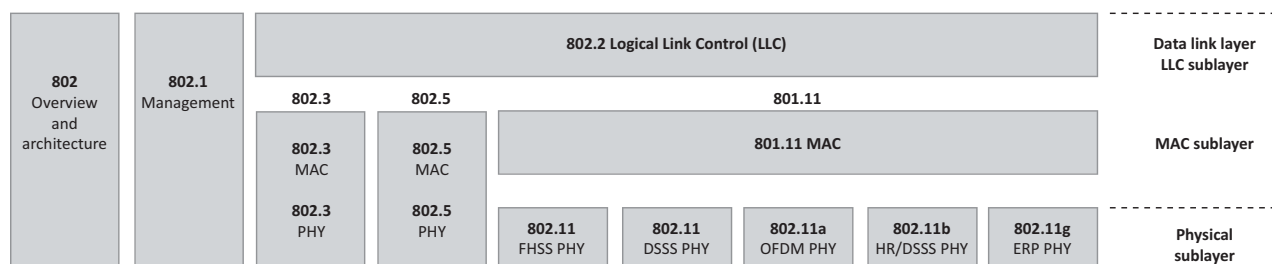


Figure 1. 802.11 data link and physical layers

(Source: *802.11 Wireless Networks*, O'Reilly)

## Differences between IEEE 802.11a, 802.11b, 802.11g, and 802.11n

Some early IEEE® 802.11a devices had notoriously bad performance and there is still some confusion in the industry about the range and capacity of WLANs in the 2.4 and 5 GHz bands. Although some specific building materials exhibit different absorption and reflection characteristics at 2.4 and 5 GHz, differences in the average indoor propagation models at 2.4 and 5 GHz are small and, therefore, it should be possible to achieve roughly equivalent range performance anywhere in the 2.4 to 5 GHz band.

Tests conducted with current generation equipment show that the maximum ranges for IEEE 802.11a, 802.11b and 802.11g are essentially the same. However, the simpler but less efficient DSSS modulation used by 802.11b puts it at a significant speed disadvantage which has led the industry to manufacture WLAN devices predominantly operating in the 2.4 GHz band using OFDM modulation (that is, 802.11g).

When IEEE 802.11b and 802.11g devices operate simultaneously on a WLAN, the 802.11g devices must protect their OFDM signals from interfering with the 802.11b devices. Because 802.11b devices cannot decode OFDM signals, the 802.11g devices are permanently hidden to them. To avoid interference from 802.11b devices, the 802.11g devices must reveal their presence by entering protection mode, prefacing their OFDM transmissions with a Clear to Send-to-Self or a Request to Send/Clear to Send exchange that is transmitted using DSSS modulation. The overhead associated with this extra transmission can be substantial and considerably reduces the effective maximum data throughput of a cell operating in 802.11b protection mode. To alleviate reduced throughput from intermingling of 802.11b and 802.11g client devices the AP and 802.11g devices will go into protection mode. With 802.11g devices only, the WLAN has the highest available throughput, but when the 802.11b client is introduced, protection mode begins and all 802.11g connected clients experience an impact on performance. The impact varies, but in general the throughput is seriously reduced. If feasible, an organization should consider removing or disabling all 802.11b clients. This also allows you to disable the lower 802.11b data rates, which lets end-user devices roam more readily to a better AP when throughput becomes degraded.

The number of non-overlapping channels is another major difference between IEEE 802.11b/g and 802.11a/n. The 802.11 b/g standard defines a total of 14 frequency channels. The FCC allows channels 1 through 11 within the U.S. (and also in Canada). Most of Europe can use channels 1 through 13. Therefore, IEEE 802.11b/g is limited to 3 non-overlapping channels.

In North America IEEE 802.11a/n using the 5 GHz frequency has 12 indoor channels with no overlap. Outside of North America, availability of the 5 GHz 802.11a/n non-overlapping channels varies by region. When deploying a new or expanding an existing WLAN, the channels available to increase coverage and/or capacity need to be accounted for at each step. The available channels are a major factor in determining which frequency band to use in designing a WLAN with limited co-channel interference while maximizing coverage and capacity.

## Dual-band radios and dual-radio APs

IEEE® 802.11a/b/g/n dual-band APs with two radios can simultaneously support both 2.4 GHz and 5 GHz RF bands. They offer backward compatibility (to preserve existing investments), a larger number of channels, and increased throughput. A WLAN device with a dual-band radio can scan both the 2.4 and 5 GHz bands and choosing the best AP on either band.

Dual-band APs are well-suited to a wide range of network topologies. In addition to the benefits of increased bandwidth, it is fairly common to find deployments that use dual-band APs to segregate data types onto the different RF bands. The AP's 5 GHz radio can service wireless traffic from time-sensitive voice/data clients (VoWLAN devices), while the 2.4 GHz radio supports data traffic from laptops. This can reduce data and voice traffic contention by creating two separate RF networks. Since 802.11a/n are able to both use a different frequency band, it is not affected by interference from the possible pervasive 802.11b/g WLANs, and is better insulated from overhead activity (for example, probes/responses from clients) generated by internal and external 802.11b/g WLANs.

## Additional functions and certifications

Careful capacity planning is important because the number of wireless devices and users may increase significantly with the advent of new mobile applications or the implementation of dual-mode technology. Some companies ensure adequate capacity by using dual-band APs (5 GHz and 2.4 GHz standards combined) to separate voice and data onto different spectrums. Engineering a WLAN network for VoWLAN often involves installing more APs and backing off the transmit power to minimize co-channel interference with APs on the same channel. Another option is to use advanced management tools that provide site survey analysis and real-time capacity planning and RF management. Such tools can provide visibility into network usage per AP or per facility, and can determine when additional APs are required. Real-time RF management tools tune the WLAN's RF parameters to provide a better user experience.

## Voice considerations

If your organization is considering voice capabilities over the WLAN, you need to consider additional standards in the planning and design. The WLAN clients and APs should support the following features:

- Operation in the 5 GHz bands to take advantage of higher density AP deployment, better overlapping coverage, and reduced interference from other technologies (microwave ovens, cordless phones, Bluetooth® devices).
- QoS to prioritize delay/jitter-sensitive voice traffic through protocols such as IEEE® 802.11e or the WMM specification. Another application that benefits from QoS is prioritized traffic management, which allows the IT administrator to assign different priority levels to different users. For example, network administrators may want to assign a lower priority to visitors sharing the network, or to provide more resources to employees working on critical tasks, or to applications like video streaming or teleconferencing.
- A major challenge to integrating WLAN and mobile devices is impact on battery life of the mobile devices. To address this aspect, the IEEE 802.11e standard defines a method of improving battery life and power-saving mechanisms. The Wi-Fi® Alliance has created a certification for this standard called WMM-Power Save. WMM-Power Save offers advanced power management mechanisms that are optimized for mobile devices. It was introduced in answer to demand from manufacturers, application developers and service providers who want to take advantage of the opportunity that WLAN mobile devices offer for new capabilities and services.

## Standalone and centrally coordinated wireless networks

In planning your wireless network, you'll need to determine which WLAN architecture to adopt in your environment. The architectures available - standalone and centrally coordinated - have benefits that are well-suited to different environments.

A wireless network based on standalone APs relies on the integrated functionality of each AP to enable wireless services, authentication and security. A standalone WLAN can be characterized as follows:

- All APs in the network operate independently of each other.
- Encryption and decryption is done at the AP.
- Each AP has its own configuration file.
- The network configuration is static and does not respond to changing network conditions such as interfering rogue APs or failures of neighboring APs.

In a centralized or coordinated wireless network, an access controller communicates with the APs to provide scalable centralized control, management, and policy enforcement across the wireless network. A centralized WLAN can be characterized as follows:

- AP activity is coordinated by a wireless centralized controller.
- To maintain the health of the network, the controller can monitor and control the wireless network to automatically reconfigure AP parameters as needed to maintain high service levels.
- The WLAN network can be expanded or reduced easily by simply plugging in or removing APs, after which the controller will reconfigure the network based on the changes in RF footprint.
- The WLAN controller performs tasks such as client authentication, policy enforcement, configuration control, fault tolerance and network expansion.
- Redundancy can be provided through redundant controllers in separate locations, which can assume control in the event of a switch or controller failure.

Both the standalone and centrally coordinated architectures have advantages and disadvantages, depending on the age of the wired infrastructure, deployment area, building architecture, and types of applications that you want to support. Regardless which approach you choose, it is essential that your architecture provide you with a way to manage your network efficiently and effectively.

However, the operational overhead to manage and maintain a WLAN increases with the size of the WLAN deployment. WLAN management tools help simplify configuration and monitoring of the WLAN, but the inherent "independence" of standalone APs presents a challenge in addressing security, configuration control, bandwidth predictability, and reliability, as users and applications become dependent on a reliable WLAN connection.

Centralized AP deployments are most appropriate in larger organizations with a wireless overlay throughout the facility, campus-wide. This kind of deployment allows a facility to address operational concerns, simplify network management, and assure availability and resiliency - with more users, it's essential to minimize help desk calls and trouble tickets. A centralized AP deployment should seriously be considered as the sole alternative when the main user applications require fast client roaming and coordinated QoS for traffic-sensitive applications such as VoWLAN.

## Site survey

One of the key factors in ensuring the success of a WLAN deployment is a site survey. Before deploying your WLAN, you need to understand the needs of users in the current environment. By performing a site survey, you can identify the:

- appropriate technologies to apply
- obstacles to avoid, eliminate, or work around
- ideal coverage patterns
- amount of capacity needed

The site survey should yield a network design document that describes the location of each AP, its coverage area, and the 802.11a/b/g/n channel selections for the AP.

A great deal of information can be obtained from a site survey, but even more important is how that information is analyzed to support cell planning; cell boundary threshold; range and throughput; interference/delay spread; bandwidth management for applications like VoWLAN; AP density and load balancing.

Surveying for the “weakest link” is another important activity. This requires a consideration of the different radio characteristics of the devices to be used on the WLAN, as well as the devices themselves and how they interact within the environment. For example: due to the differences in power capabilities and radio antenna characteristics, surveying with a laptop with an exposed radio will not accurately illustrate the same coverage that a BlackBerry® smartphone will experience.

With limited channel availability, channel usage and selection are paramount. It isn't simply a question of installing more APs to provide more performance or greater coverage. The limited channel capacity of 802.11 based WLANs does not allow for an infinite number of APs and overlapping coverage within a given area. To optimize the WLAN, work with providers that have an intimate understanding of the behavior of radio frequency and wireless standards. This becomes even more important when deploying dual-radio APs.

## Obstacles to signal strength

In general, objects absorb or reflect signal strength and degrade or block the signal. Identify any potential obstacles or impediments in the area to be served. For example:

- Walls, especially if the wall is composed of heavier construction materials such as concrete. Also note any firewalls in the area.
- Ceiling tiles, particularly if they are made of material such as metal.
- Furniture, especially pieces that are largely made of metal.
- Natural elements such as water, trees, and bushes (outdoors, and also in lobbies, courtyards or other interior spaces).
- Coated glass. Transparent glass generally does not greatly degrade signal strength, but it can if it is coated with a metallic film or has a wire mesh embedded in it.
- People or objects. Wireless propagation will change depending on whether there are people or objects moving around the area. Site surveys should be done at the same time(s) as when the service is expected to be used.

## Security

Security is paramount and must be a major consideration for any WLAN deployment. The open nature of wireless, compared to wired, access creates significant security concerns, especially regarding user authentication and data encryption. Broadcast signals often travel into public areas that can be accessed by eavesdropping individuals who have not passed through any type of authentication process to validate their presence at the site. The site survey should identify the security status of all locations considered for wireless access.

When deploying a WLAN, IT security and network managers must decide how to secure WLAN communication with multiple forms of authentication and encryption. When selecting networking equipment, they must choose APs that provide a comprehensive range of industry-proven security capabilities which integrate easily into any network design.

Larger enterprises that are deploying complex WLANs with hundreds of stations and dozens of APs require more sophisticated access control using RADIUS servers. For smaller networks without a centralized RADIUS server for user authentication, some APs offer built-in RADIUS authentication. Your APs should integrate seamlessly with existing authentication systems. Your networking equipment should provide standards based authentication and encryption methods that satisfactorily address security concerns such as data privacy, authentication, and access control.

Standards and certification bodies have released various security standards to secure WLANs. This section briefly describes some of these standards.

**WEP:** The initial attempt at providing wireless networks with a level of security comparable to that of wired networks that only involves data encryption. In this regard, the standard has proven to be a failure due to an abundance of widely publicized vulnerabilities. These weaknesses include static keys, keys that can be broken and that WEP is highly susceptible to a variety of "man-in-the-middle" attacks and session hijacks.

**IEEE® 802.11i™ and IEEE® 802.1X™:** When the weaknesses of WEP were identified, industry professionals were forced to look for other solutions. IEEE 802.11i specified authentication mechanisms based on IEEE 802.1X, an encryption key management protocol, and stronger data encryption mechanisms. IEEE 802.1X leverages EAP to provide strong mutual authentication between the client and the network. The client must authenticate itself to the RADIUS server, and the AP must authenticate itself to the client before the client is granted access to the larger network. IEEE 802.1X in its native state provides mutual authentication and encryption key derivation.

**EAP:** To deliver both authentication and key management, the IEEE 802.1X protocol requires EAP. EAP is responsible for establishing how the authentication process should be carried out. EAP establishes the rules so that both client and AP know the rules and appropriate responses for a successful authentication. The most popular EAP types are LEAP, PEAP, TLS, TTLS and Cisco's FAST. Each of these methods has their own unique strengths and considerations, and choosing the correct method for your network can be one of the most important steps of the security design process.

The following table identifies the differences between the most widely available EAP methods.

EAP Type	Client Certificate	Server Certificate	Mutual Authentication	Credential Security
MD5	No	No	No	Weak
LEAP	No	No	Yes	Moderate
TLS	Yes	Yes	Yes	Strong
PEAP	No	Yes	Yes	Strong
TTLS	No	Yes	Yes	Strong
FAST	No	No	Yes	Strong

- **MD5:** The weakest of the possible EAP methods, MD5 typically should not be employed in a WLAN as it provides negligible benefits over WEP.
- **LEAP:** Provides an easy way to get 2-way authentication without using certificates. The weakness is that it is susceptible to dictionary attacks.
- **TLS:** Provides a very secure solution, but requires the use of certificates on the client devices.
- **PEAP:** Very secure solution. Uses TLS to create a secure tunnel where a second authentication mechanism can be used. PEAP does not require a certificate on the client, but will use a server-side certificate.
- **TTLS:** Very secure solution. It is very similar to PEAP using TLS to create a tunnel to avoid using certificates on the client.
- **FAST:** Very secure. Creates a secure tunnel, then uses a RADIUS server to authenticate the server and client.

**WPA™ and WPA2™:** WPA and WPA2 are the Wi-Fi® Alliance's certification program related to specifications based on the IEEE® 802.11i™ standards. WPA or WPA2 are not the security mechanisms themselves, but are a name for a collection of specific security protocols. Both standards rely on IEEE® 802.1X™ to provide strong authentication. Both standards then apply strong encryption mechanisms to serve as a complete replacement for WEP. WPA and WPA2 leverage IEEE 802.1X for authentication and key management; and TKIP or AES cipher suites for encryption.

WPA is the specification delivered by the Wi-Fi Alliance as a solution that could be used in advance of the ratification of the 802.11i standard. The key difference between the two specifications revolves around the encryption mechanism used in each. WPA replaces the WEP encryption with a mechanism called TKIP. TKIP, like WEP, uses the RC4 cipher but counters the methods that were used to attack WEP-enabled WLANs. WPA2 is virtually identical to WPA, except it specifies the use of CCMP for encryption instead of TKIP. CCMP makes use of the AES cipher and is typically considered the most robust encryption strategy available. The trade-off is that AES requires additional processing power and may not be supported by older hardware. Most hardware today supports both AES and TKIP ciphers. It should also be noted that the AES cipher suite may be used with WPA.

The Wi-Fi alliance has defined two flavors of WPA and WPA2: personal and enterprise. WPA and WPA2-Enterprise specifies how IEEE 802.11i should be used in an enterprise environment where there is authentication infrastructure (for example, RADIUS servers) available. WPA/WPA2-Personal specifies how IEEE 802.11i should be used in a small office or home office environment using a pre-shared key.

The Wi-Fi Alliance also developed a method to simplify security configuration for small office or home office users, allowing them to take advantage of the security WPA and WPA2 called Wi-Fi Protected Setup™. This method provides an automated mechanism to configure WPA Personal on both the AP and client device for easy configuration.

For more information on which WLAN security authentication and encryption methods are supported in WLAN capable BlackBerry® smartphones, refer to the [BlackBerry Wi-Fi Implementation Supplement](#).

## VPN

For existing legacy WEP-based WLAN deployments, or for deployments that have difficulty deploying IEEE® 802.11i™ based link layer encryption, a robust VPN can be used. IPSec VPNs have been and remain a standard security practice for providing secure access from an unsecure or non-trusted connection. In this regard, IPSec VPNs can make sense for use in unsecure WLANs and may even be deemed a requirement for use at an external home or hotspot WLANs.

The main advantage of the VPN approach is that it leverages technology and skills that many IT managers already have, and is neutral in terms of APs. It is also worth noting that a VPN solution only begins working at Layer 3, but the other WLAN security methods discussed above work at Layer 2.

The drawback is that it may require management effort on each wireless client, which can quickly become unmanageable if WLAN is to be rolled out to all employees and network users. To address this, the IPSec VPN client available on all WLAN enabled BlackBerry® smartphones was designed to provide a straightforward solution in implementing IPSec VPN. The client is built into every WLAN-enabled BlackBerry smartphone, and the management and configuration can be managed from the BlackBerry® Enterprise Server.

For more information on which VPN clients are supported and how they can be managed on WLAN-capable BlackBerry smartphones, refer to the [BlackBerry Wi-Fi Implementation Supplement](#).

## RF Monitoring, intrusion detection, and quarantine

To secure today's campus network, enterprises must implement security policies and mechanisms that keep outsiders out and insiders honest.

Fully protecting the WLAN means:

- Preventing external hackers from getting access to the network
- Allowing only authorized users into the network
- Preventing those inside the network from executing deliberate or inadvertent attacks
- Monitoring of the WLAN to:
  - Identify rogue APs
  - Detect intruders
  - Detect impending threats
  - Enforce WLAN security policies

There are a number of products on the market today that integrate intrusion detection, virus checking, rogue AP detection, and quarantine both on the wireless and wired network. Use of these tools can also help to identify and display the location of a device on the campus.

To be truly effective, the security policy must accomplish these goals in a way that is transparent to the users, easy to administer, and that does not disrupt business.

## Secured access using unsecured WLANs

Providing access to the secured enterprise network for remote and mobile workers allows workers to be more productive and reachable when not within the enterprise campus.

If remote workers are allowed to use home or hotspot based WLANs for remote enterprise access, additional considerations in the areas of security and implementation are required. Additionally, the types of applications and intended use enabled for remote workers will also drive the considerations. Most important is that the security mechanisms employed ensure that the data in transit is secured and not accessible and also ensure that the enterprise network is not compromised.

Layer 3 IPSec-based VPN solutions, as described earlier, have been used for many years to secure Internet-based connections into the enterprise, allowing access to the end-point as if it was connected directly to the enterprise network. The IPSec VPN solution can also be extended to mobile end-points that use unsecured WLANs for Internet connectivity. By extending the VPN to the mobile end-point, the mobile device can connect to any Internet-capable WLAN and use the same applications as if they were on the enterprise WLAN. For home workers, for example, this would allow the user to use PBX-based VoWLAN while connected to their home WLAN.

Enabling VPN for remote access does require other considerations that must be planned for, regardless of the solutions implemented. Home and hotspot WLANs are inherently an unmanaged, unsecured, and best effort service since the Internet is the transit route between the home/hotspot and the enterprise network. QoS, congestion, throughput and latency, among other network factors, are effectively uncontrollable, and VoWLAN is the application that is most impacted by these factors.

Security of the WLAN may not be controllable, especially at a public hotspot. For home use, there could be security guidelines produced and provided for home WLANs, but if those users are purchasing and using unmanaged, non-enterprise retail-based WLAN routers, there is no guarantee that any security is implemented, reinforcing the key reason a VPN solution is required.

Setting users expectations of the experience at the home or hotspot WLAN is a key necessity, which is that WLAN use in these environments will not be the same as in the enterprise.

## Home WLAN guidelines

There are steps that you can take to reduce the impact of some of the issues described above, resulting in a better user experience. Consider the following areas, and then document and communicate the guidelines you establish to home WLAN users:

- Identify the type of applications that are allowed on remote WLANs and include expectations for home use around those applications. For example, if VoWLAN will be allowed, because of the particular network requirements of VoWLAN, you should include the following guidelines:
- Specify an expected minimum download and upload speed for home Internet connectivity.
- If there is simultaneous use of many different applications while using VoWLAN (that is, video streaming, gaming, file transfers, and so on), turn on QoS on the home WLAN router to ensure the VoWLAN devices have precedence over other endpoints.
- To reduce the variables from interoperability or WLAN router configuration settings, consider creating a short list of WLAN router vendors or minimal version(s) of routers that have been tested against the enterprise-approved WLAN devices.
- Identify the minimal expected level of authentication and encryption configured on the home WLAN router (for example, PSK with WPA2).

## Hotspot WLAN guidelines

Consider the following areas and then document and communicate the guidelines you establish to hotspot WLAN users:

- A hotspot WLAN is an unmanaged, shared resource that can impact any application using the WLAN. There is a possibility that congestion, high latency, absent QoS, and restricted bandwidth are all present at the hotspot.
- VoWLAN on a hotspot WLAN might not be possible due to several possible network factors and should not be relied on as a reliable method to make or take VoWLAN calls. If a VoWLAN call on hotspot WLAN does connect, the voice quality is not guaranteed and a conversation may even be unintelligible.
- Data applications running over the hotspot WLAN are better able to adjust and tolerate a poor WLAN environment, but there still could be an adverse impact on data applications.
- Security on hotspot WLAN is non-existent or should be expected to be compromised, requiring the use of VPN and/or other additional security mechanisms, such as the VPN available in the BlackBerry® solution security model.

## Putting it all together for voice and data over a WLAN

By understanding the different user profiles and use cases for a WLAN, and considering the information in this document, if your enterprise is deploying a WLAN that will support data and voice applications, you should ensure the following key capabilities are present in the infrastructure and the clients:

- QoS priority maintained end-to-end throughout the network infrastructure on both the wireless and wired network.
- The ability to differentiate, optimize, and control the flow of voice traffic to increase transmission reliability.
- Highly secure authentication and encryption that doesn't compromise voice quality.
- Seamless, low-latency mobility across Layer 2 and Layer 3 boundaries without compromising security.
- Proper WLAN instrumentation to proactively identify performance issues and isolate them during the diagnosis of WLAN problems.
- Centralized management of the RF environment to ensure pervasive coverage, network capacity and availability.
- Support for extending BlackBerry® smartphone, or other device, battery life.

## Section 2: Questions to ask WLAN Vendors

How do you begin to identify what is required in a WLAN and ensure that the WLAN vendors know exactly what you're looking for? You can ask questions on the functions and capabilities of the different WLAN solutions, which provides a foundation to clearly outline the technical requirements to the vendor.

Below are some WLAN functional areas with examples of questions that can help you define your technical requirements. It is essential that you work closely with your WLAN vendor so they clearly understand your requirements and determine how the answers to the questions will drive their recommendations on design, implementation, and administration of the WLAN.

This following list of questions is not intended to be exhaustive, but provides a solid foundation for starting the evaluation process.

### Architecture

- Does the vendor's solution consist of a centralized controller supporting APs or is the solution built with stand-alone intelligent APs only?
- What functions does the controller perform for the wireless network?
- Does the controller support seamless roaming across IP subnets?
- What is the tunneling protocol running between the controller and the APs? Is that protocol, AP agnostic? Is the protocol proprietary or standards-based?
- How many APs can a single controller support?
- How many user sessions can a controller support?
- What interfaces are supported on the controller?
- Can the controller be upgraded to support more APs?
- Does the system support redundant controllers?
- Do the APs fail over to a secondary controller if the primary controller goes down?
- When failing over from one controller to another, does the mobile user's session stay active? Does the IP address change?

### Standards and certifications

- Which 802.11 standards does the solution support?
- Does the solution support 802.1X?
- What EAP methods are supported?
- Does the solution support WPA™ or WPA2™?
- Does the solution support WMM?
- Is the solution Wi-Fi® Alliance certified?
- What other WLAN certifications does the solution have?

## APs

- Which radio frequencies are supported on the APs?
- Do the APs have dual radios (2.4 GHz and 5 GHz)?
- Can the administrator control which 802.11 services are available (a,b,g, or n)?
- Are the power levels configurable on the APs?
- What is the maximum power level available?
- Is the RF management software provided able to automatically support channel selection, power levels, load-balancing, and failover?
- Are the RF management functionality calculations performed on the AP or on the controller?
- Is the Power-over-Ethernet standard 802.3af supported?
- Are third-party antennae supported?
- Is there any user information stored on the AP?
- How many SSIDs can each radio support?
- When roaming between APs, what is the typical latency?
- Is QoS supported?
- Do the APs support CAC?
- Can a voice call roam between APs without being dropped?
- Can a voice call roam between APs that are on different subnets without being dropped?

## WLAN end-user devices

- Do the devices have multiple radios (802.11a/b/g/n)?
- What are the supported WLAN security methods for the devices?
- What are the supported EAP methods for the devices?
- Is there VPN client support for the devices? Is the VPN client separate software or is it built-in?
- Do the devices support QoS?
- Do the devices support CAC? Which vendor's CAC is supported?
- What are the supported capabilities for extending battery life on the devices?
- What is the expected battery life on both standby, data only, and if applicable, data and voice usage?
- Can the devices scan for available networks?
- Do the devices support connectivity to hotspot and public WLANs using a captive portal?
- Do the devices support EAP-SIM for carrier's hotspots?
- What are the policies available to manage and control access, features, and functionality of the devices?
- What are the processes and capabilities for provisioning the devices? Can provisioning be done remotely?
- Can provisioning be updated after issuing the device without recovery to a central point?

## Management

- Does the controller support a Command Line Interface?
- Does the solution support GUI-based centralized management?
- Can software be upgraded on all APs at once? Is it automatic?
- Does the solution support RF management?
- Is the RF management algorithm processing done by the AP or the controller?
- Does the RF management include correcting for failed APs, channel interference, and unbalanced loads?

## Security

- Is there a RADIUS authentication server available?
- If a RADIUS server is available, which EAP protocols are supported?
- Does the hardware support AES encryption?
- Does the solution detect rogue APs?
- Can rogue AP scans be scheduled?
- Can rogue AP scans be scheduled by individual AP, by radio, and by channel?
- Can detected rogue APs be classified into groups?
- Can the rogue AP scans parameters be configured?
- Does the solution support WPA/WPA2 in both enterprise and pre-shared key modes?

## Glossary

### A

**AP** Access Point. A layer-2 networking device that serves as an interface between a wireless network and a wired network and can control medium access. Access points combined with a distribution system (for example, Ethernet) support the creation of multiple radio cells that enable roaming throughout a facility.

**AES** Advanced Encryption Standard. The standard cryptographic algorithm for use by US government organizations to protect sensitive (unclassified) information.

**Attenuation** Decrease in the amplitude of an RF signal due to resistance of cables, connectors, splitters, or obstacles encountering the signal path.

**Authentication** The process a station uses to announce its identity to another station.

### C

**CAC** Call Admission Control. The set of actions taken by the network during the call set-up phase (or during call re-negotiation phase) in order to determine whether a connection request can be accepted or should be rejected, or whether a request for re-allocation can be accommodated.

**CCMP** Counter-Mode Cipher Block Chaining Message Authentication Code Protocol. Wireless encryption protocol based on the AES and defined in the IEEE 802.11i specification.

### D

**Delay** The transfer delay is defined as the amount of time elapsed from the time a frame exits the source to the time it reaches the destination.

**DFS** Dynamic frequency selection.

**DSSS** Direct Sequence Spread Spectrum. Combines a data signal at the sending station with a higher data rate bit sequence, which many refer to as a chip sequence (also known as processing gain). A high processing gain increases the signal's resistance to interference.

### E

**EAP** Extensible Authentication Protocol. A general protocol for authentication that supports multiple authentication mechanisms. EAP does not select a specific authentication mechanism at link control phase, but rather postpones this until the authentication phase. This allows the authenticator to request more information before determining the specific authentication mechanism. This permits the use of a "back-end" server, which implements the various mechanisms while the PPP authenticator passes through the authentication exchange.

**EAP-SIM** Extensible Authentication Protocol Method for GSM Subscriber Identity Module. An EAP mechanism for authentication and session key distribution using the Global System for Mobile Communications (GSM) SIM card.

**EAP-TLS** Extensible Authentication Protocol-Transport Layer Security. A protocol used for layer 2 access security through mutual authentication and the use of client-side certificates.

**EAP-TTLS** Extensible Authentication Protocol-Tunneled Transport Layer Security. Similar to PEAP in authenticating to a WLAN. EAP-TTLS does not require a client-side certificate.

**Encryption** The process of coding data so that a specific code or key is required to restore the original data, used to make transmissions secure from unauthorized reception.

**Ethernet** A 10 Mbps LAN medium-access method that uses CSMA to allow the sharing of a bus-type network. IEEE 802.3 is a standard that specifies Ethernet.

### F

**FAST** A two-phase WLAN authentication protocol developed by Cisco. Phase 0, provision client with a credential called PAC (Protected Access Credentials). Phase 1, uses the PAC to establish a tunnel with the server and authenticate the username and password.

**FCC** Federal Communications Commission. An independent United States government agency, directly responsible to Congress. The FCC was established by the Communications Act of 1934 and is charged with regulating interstate and international communications by radio, television, wire, satellite and cable. The FCC's jurisdiction covers the 50 states, the District of Columbia, and U.S. possessions.

### G

**Gigahertz (GHz)** One billion hertz.

### I

**IEEE®** Institute of Electrical and Electronic Engineers. A United States-based standards organization participating in the development of standards for data transmission systems. IEEE has made significant progress in the establishment of standards for LANs, namely the IEEE® 802® series of standards.

**IEEE® 802.1x™** An IEEE standard for port-based network access control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails.

**IEEE® 802.3af** An IEEE standard that describes a mechanism for Power over Ethernet. The standard provides the capability to deliver both power and data over standard Ethernet cabling.

**IEEE® 802.11a** A revision to the IEEE standard that operates in the unlicensed 5 GHz band. 802.11a products have data rates up to 54 Mbps and must support 6, 12, & 24 Mbps.

**IEEE® 802.11b** A wireless networking standard offering transmission speeds of up to 11 megabits per second (Mbps); it operates on three non-overlapping channels in the unlicensed 2.4 GHz radio frequency (RF) range.

**IEEE® 802.11e** A standard that defines a set of Quality of Service enhancements for LAN applications, in particular the 802.11 standard. The standard is considered of critical importance for delay-sensitive applications, such as Voice over Wireless IP. The protocol enhances the IEEE 802.11 MAC layer.

**IEEE® 802.11g** A wireless networking standard offering transmission speeds of up to 54 Mbps; it operates on three non-overlapping channels at the 2.4 GHz RF range, and is backward compatible with 802.11b.

**IEEE® 802.11i™** An amendment to the 802.11 standard specifying increased security mechanisms for wireless networks.

**IEEE® 802.11n** An amendment to the 802.11 standard for wireless local-area networks. The data throughput is estimated to reach a theoretical 540 Mbit/s (which may require an even higher raw data rate at the physical layer), and should be up to 50 times faster than 802.11b, and well over 10 times faster than 802.11a or 802.11g.

**IP Internet Protocol.** A protocol that specifies the format of packets and how they are sent; it is often used in combination with TCP.

#### **IPSec Internet Protocol Security.**

A protocol used to secure IP-based communication by authenticating and encrypting each IP packet.

**IP telephony** Transmission of voice calls over data networks that use IP.

**ISM bands** Industrial, Scientific, and Medical bands. Radio frequency bands that the FCC authorized for wireless LANs. The ISM bands are located at 915+/- 13 MHz, 2450+/- 50 MHz, and 5800+/- 75 MHz.

## J

**Jitter** A measure of the variability over time of the delay across a network. A very low amount of jitter is important for real-time applications using voice and video.

## L

**LAN** Local Area Network. A data network that connects computers, peripherals, terminals, and other devices in a single building or other geographically limited area.

**Layer 2 access security** Security provided by encryption on the 802.11 network through one or more encryption protocols used on the access point(s).

**Layer 3 access security** Security provided at the application level within a data network. (for example, a VPN connection).

**LEAP** Lightweight Extensible Authentication Protocol. A protocol used for layer 2 access security through mutual authentication and the use of dynamic WEP keys; it is also called EAP-LEAP.

## M

**ms** Millisecond. One thousandth of a second.

**MAC layer** Medium Access Control layer. Provides medium access services for IEEE 802 LANs.

**MITM** Man-in-the-middle. An attack in which an attacker can read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.

**MHz** Megahertz. One million cycles per second.

## O

**OFDM** Orthogonal Frequency Division Multiplexing. A method of digital modulation in which a signal is split into several narrow band channels at different frequencies.

## P

**Packet loss** The loss of data in a packet based network, usually due to congestion and consequent buffer overflow.

**PBX** Private Branch Exchange. Telephone system within an enterprise organization.

**PEAP** Protected EAP. A method to securely transmit authentication information, including passwords, over wired or wireless networks. PEAP uses only server-side public key certificates to authenticate clients by creating an encrypted tunnel between the client and the authentication server, protecting the exchange of authentication information.

**PSK** Pre-shared Key. A shared secret key used for layer 2 access security.

## Q

**QoS** Quality of Service. The concept of applying and ensuring specific, quantifiable performance levels on a shared network. The methods by which network traffic is prioritized, and on how the network is managed.

## R

**RADIUS** Remote Authentication Dial In User Service. A protocol used for single point authentication of dialup systems, wireless LANs, and applications roaming within a wireless LAN, moving from one AP coverage area to another.

**RC4** A widely deployed symmetric key stream cipher.

**RF** Radio Frequency. A generic term for radio-based technology.

**Roaming** The process of moving from one access point to another without having to re-authenticate to the wireless network.

**Rogue AP** Rogue access point. An AP that is being used to gain wireless access within an enterprise, but is not part of a sanctioned WLAN.

**RTS/CTS** Request-to-Send/Clear-to-Send.

An extension to CSMA/CA, in which clients enter into a 4-way handshake with an access point to send data. (1) Client sends RTS packet to request use of the medium, (2) if the medium is free, access point sends the CTS packet to the client, (3) client sends the DATA to the receiving client, (4) receiving client sends the ACK packet to acknowledge receipt of the DATA. 4-way handshake = RTS-CTS-DATA-ACK.

## S

**Site survey** The act of surveying an area to determine the contours of RF coverage in order to ensure proper wireless LAN operation through appropriate wireless LAN hardware placement.

**SSID** Service Set Identifier. A sequence of up to 32 letters or numbers that is the name of a wireless local area network.

**Subnet** An interconnected, but independent segment of a network that is identified by its Internet Protocol (IP) address.

## T

**TCP/IP** Transmission Control Protocol/Internet Protocol. A combination communication protocols used to connect hosts and transmit data on data networks.

**TKIP** Temporal Key Integrity Protocol. A protocol used by EAP to improve data encryption.

**TPC** Transmission Power Control.

## U

**U-APSD** Unscheduled Automatic Power Save Delivery. A feature that provides a dramatic improvement in talk time for battery-powered handsets.

## V

**VLAN** Virtual LAN. A method of differentiating traffic on a LAN by tagging the Ethernet frames. It provides the ability to associate different LAN-attached workstations as being part of the same LAN independent of where the workstation is physically attached to the LAN. The term VLAN was specified by IEEE 802.1Q

**VoIP** Voice over IP. Voice calls over an IP network, also referred as IP telephony

**VoWLAN** Voice over WLAN. VoIP calls over a wireless LAN

**VPN** Virtual Private Network. A network that uses access security to prevent unauthorized users from accessing the network and intercepting data.

## W

**WEP** Wired Equivalent Privacy. A security protocol designed to provide the same level of security as that of a wired LAN.

**Wi-Fi™** Wireless Fidelity. A set of product compatibility standards for wireless local area networks (WLAN) based on the IEEE 802.11 specifications. Trademarked by the Wi-Fi™ Alliance.

**Wi-Fi™ Alliance** Founded in 1999, this organization's charter is to certify interoperability of IEEE 802.11a/b/g products and to promote Wi-Fi™ as the global wireless LAN standard across all market segments.

**WME/WMM** Wireless Multimedia Extensions also known as Wi-Fi Multimedia. A Wi-Fi Alliance certification, based on the IEEE 802.11e draft standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to 4 AC (Access Categories), however it does not provide guaranteed throughput.

**WLAN** Wireless LAN. One in which a mobile user can connect to a LAN through a wireless (radio) connection. A standard, IEEE 802.11, specifies the technologies for wireless LANs.

**WPA™** Wi-Fi Protected Access™. The Wi-Fi Alliance's certification that uses the TKIP encryption method and EAP or PSK authentication.

**WPA2™** Wi-Fi Protected Access™ 2. The Wi-Fi Alliance's certification that uses the CCMP encryption method and EAP or PSK authentication.

## Legal Notice

©2010 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™ and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S and countries around the world.

Bluetooth is a trademark of Bluetooth SIG. IEEE, IEEE 802, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1X IEEE 802.11 IEEE 802.11i are trademarks of the Institute of Electrical and Electronics Engineers, Inc. Wi-Fi, Wi-Fi Protected Access, Wi-Fi Protected Setup, WPA, and WPA2 are trademarks of the Wi-Fi Alliance. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available at <http://www.blackberry.com> is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party web sites (collectively the "Third Party Products and Services"). RIM does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by RIM of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABILITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL RIM BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF RIM OR ANY AFFILIATES OF RIM HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with RIM's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with RIM's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by RIM and RIM assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with RIM.

Certain features outlined in this documentation require a minimum version of BlackBerry® Enterprise Server, BlackBerry® Desktop Software, and/or BlackBerry® Device Software.

The terms of use of any RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

#### Research In Motion Limited

295 Phillip Street  
Waterloo, ON N2L 3W8  
Canada

#### Research In Motion UK Limited

Centrum House  
36 Station Road  
Egham, Surrey TW20 9L7  
United Kingdom  
Published in Canada

For More Information | [www.blackberry.com](http://www.blackberry.com)

---

