

 BlackBerry®



Deploying a Wireless LAN

Considerations and Questions in Planning a Wireless LAN

Deploying a Wireless LAN

Table of Contents

Executive Summary	1
Section One – Areas to consider in deploying a WLAN	1
What are the applications that the user needs	1
Coverage	4
WLAN Standards	6
Standalone and Centrally Coordinated Wireless Networks	9
Site Survey	10
Security	11
Putting It All Together for Voice and Data over WLAN	14
Section Two – Questions to pose to WLAN Vendors	15
Architecture	15
Standards	15
Access Points	15
WLAN End-user Devices	16
Management	16
Security	16
Glossary	17

Executive Summary

As wireless LANs (WLANs) continue to grow in popularity, particularly in enterprise networks, your enterprise might be considering deploying a WLAN to leverage the different advantages that come with this type of technology. The ability to do away with massive amounts of cabling to mobile workplace is a very obvious advantage. There are many more. Mobile, ubiquitous access to enterprise IT systems throughout the global enterprise yields a more productive and efficient workforce, allowing employees to access resources without being tethered to a traditionally static wired network connection. WLANs 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, hence, increasing the overall agility of the organization.

For those organizations that are beginning to plan for a WLAN deployment, this paper identifies areas that should to be considered and helps the planning and requirement definition of deploying a WLAN. Section two of this paper builds upon the considerations areas and provides a starting point for posing questions to any WLAN equipment and services vendor.

Section One – Areas to consider in deploying a WLAN

One of the most important questions to ask yourself, is what is it 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. What does mobility mean to you and your organization? Does it mean you want to be able to have network connectivity throughout your offices? Or does it mean you want your remote offices connected, too? If you have a campus, do you want to be able to connect to the network both inside and outside? If you're a doctor – do you want to be able to access your patients' records at the point of care? 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 on security, management, etc, all need to be explored and identified up front to effectively plan and deploy a successful WLAN. This first section goes over these considerations that need to be finalized up front.

What are the applications that the user needs

Wireless capacity is a finite, somewhat scarce resource and, therefore, engineering with little planning or not understanding the true nature of applications, as is often found for wired LANs, is usually not an option for WLANs. A good handle on the applications and the load they will generate is essential to avoid overestimating the cost of the WLAN (or underestimating the coverage and capacity) and will result in a more effective and usable experience for all users. Furthermore, because of the shared nature of the wireless medium, deploying too many access points might simply 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, or the relative proportion of voice and data traffic, the expected traffic demands and the application performance requirements.

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

Quality of experience

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 enables the users to do what they need to do when they need to do it. The performance metrics and performance targets used to assess the users' quality of experience depend upon the type of application.

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 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 link rate has only a limited effect on the response time when small amounts of data are transmitted. The delay and quality of the connection are the most important factor in providing good quality of experience for applications that use small transactions.

For applications in which larger amounts of data are transferred (i.e., a few kilobytes) such as email and browser-based applications, users are usually prepared to tolerate longer delays of the order of a few seconds. Because of the larger amount of data that must be transferred, the rate of the connection is more important in this case. Link quality 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 link rate is high, the TCP throughput will not be very high unless the packet loss rate remains low.

Voice

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 excessive 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 milliseconds delay budget. Significant contributors to the delay include the packetization delay, the propagation delay, and de-jitter and playout delay. 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 millisecond, 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 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 and cause voice quality impacting delays and losses on an otherwise lightly loaded WLAN.

A mixed voice and data environment deployed with the current 802.11 standard without any Quality of Service (QoS) mechanism is unlikely to result in 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 instance, using 802.11b/g for data-only users and 802.11a for voice and data users (the differences between frequency bands are described further down). This approach is relatively easy to implement with multi-mode APs but requires two channels per cell, one in the 2.4-GHz band and another one in the 5-GHz band. More important, the number of frequencies available for planning each of the voice and data WLANs is smaller and the co-channel interference problems are therefore 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 environment. The following are some of the most widely deployed and effective QoS for WLAN environments.

- VLANs – Utilize VLANs to separate data and voice traffic. VLANs serve many functions, including security and scalability, but with regards to QoS, VLANs serve the purpose of isolating of higher-priority voice traffic so that it can be dealt with using maximum resources. This requires a minimum of two VLANs, and an assigned SSID on the WLAN for each VLAN. Using separate data and voice VLANs enables specific QoS settings on all traffic on the voice VLAN to give it a higher QoS profile.
- Wi-Fi® Multimedia - To improve the reliability of voice transmissions in the nondeterministic environment, access points and VoWLAN devices should support the industry-standard Wi-Fi Multimedia (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.
- Call Admission Control - Various WLAN infrastructure vendors support IEEE 802.11e Call Admission Control (CAC) to limit the call capacity on a "per-access-point" basis. WLAN end devices must have support of the vendor's implementation to take advantage of CAC. CAC works by assigning a voice flow by the WLAN system and allocate 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 into a neighboring access point. Once the limit for voice bandwidth is reached on an access point, the next call is prevented from using the original access point to initiate the call and is automatically load-balanced to a neighboring access point and the call completed without affecting the quality of the existing calls on the channel.

Coverage

Mobility is why companies go wireless. And yet many discover that the wireless coverage is inadequate or hampered by "dead-spots". A site survey, a concept explored later in this paper, can help minimize and even prevent this. However, the restriction of mobility is always a possibility with wireless networks. Where multiple subnets on the Wireless network are in play, many IT personnel are unaware of the limitations posed when roaming workers cross over subnets. For instance, VoWLAN applications require the device to remain on the same subnet while roaming from one AP to another to prevent long roaming latencies and dropped calls. Some of today's security solutions do 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 type 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 domains and eliminating roaming across subnets. To address roaming and other manageability issues, vendor specific solutions build on top of VLAN mapping and utilize their specific technologies to increase the scalability and manageability of the whole WLAN infrastructure.

The size of an area fails to take into consideration its shape. A narrow, elongated area such as, for instance, a hospital wing may require more access points than its surface area would indicate. This is simply because some of the roughly circular coverage of the access points will necessarily fall outside the area of interest. Generally, irregular areas will require more access points than regular ones or external antennae with specific radio propagation patterns. 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 access points only on the first and third floors.

VoWLAN devices impose strict requirements on AP-AP roaming because of the traffic characteristics for voice and the sensitivity to jitter and delay. VoWLAN requires more overlapping coverage and denser deployment of AP's. 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 Voice over WLAN is introduced. There are also a number of software tools that can be used to collect and report site survey results.

Coverage vs. capacity

Simple site surveys, while guaranteeing coverage do not by themselves guarantee capacity or performance targets will be met. Because of the very 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 in order to guarantee a 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 in order to guarantee both coverage and capacity. This is where automated virtual planning tools can help refine the number, placement and configuration of access points.

The WLAN user population, the usage patterns, physical layout, and the 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, adjusting the power levels to minimize interferences and maximize capacity and performance, and automatically identify problem areas before they impact the users' quality of experience.

Later in this section there will be 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 access control (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 access points.

Subsequent amendments to 802.11 define specific physical (PHY) 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 continues today. The physical layer defines the data transmission for the WLAN, using various modulation schemes.

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

The 802.11a physical layer which was originally defined for the 5-GHz band supports up to 54-Mbps data rates using Orthogonal Frequency Division Multiplexing (OFDM) technology. The 802.11g amendment extended the use of OFDM to the 2.4-GHz band with some minor modifications required for backwards compatibility with the 802.11b devices operating in this band.

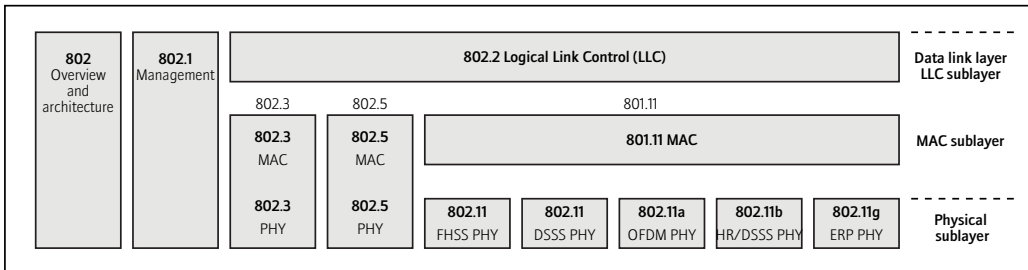


Figure 1: 802.11 data link and physical layers

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

Differences between 11a, 11b and 11g

Some early 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 11a, 11b and 11g are essentially the same. However, the simpler but less efficient DSSS modulation used by 11b puts it at a significant speed disadvantage which has led the industry to manufacture recent WLAN devices predominantly operating in the 2.4-GHz band will predominantly use OFDM modulation i.e., 802.11g.

When 11b and 11g devices operate simultaneously in a WLAN cell, the 11g devices must protect their OFDM signals from interfering with the 11b devices. Because 11b devices are incapable of decoding OFDM signals, the 11g devices are permanently hidden to them. To avoid interferences from 11b devices, the 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 (RTS/CTS) exchange that is transmitted using DSSS modulation. The overhead associated with this extra transmission is can be substantial and reduces considerably the effective maximum data throughput of a cell operating in 11b protection mode. To alleviate reduced throughput from intermingling of 11b and 11g client devices the Access Point and 11g devices will go into protection mode. This ensures that a network with 11g devices has the highest available throughput, both when only 11g devices are connected and when an 11b client is introduced. However, once the 11b client is introduced, all 11g connected clients will have a performance impact. This impact varies but in general the throughput is reduced from 25 Mb/s.

The number of non-overlapping channels is another major difference between 802.11b/g and 802.11a. 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 adopted by Canada); whereas, most of Europe can use channels 1 through 13. 802.11b/g has been limited to 3 non-overlapping channels. In North America 802.11a has 23 channels with no overlap. Outside of North America, availability of 802.11a 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 channels available is 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 access points

802.11a/b/g dual-band access points with two radios can simultaneously support both 2.4 GHz (802.11b/g) and 5 GHz (802.11a) RF bands. They offer backward compatibility (to preserve existing investments) along with a larger number of channels and consequently increased throughput. A wireless station with a dual-band radio is capable of scanning both the 2.4 and 5 GHz bands and choosing the best AP on either band.

Dual-band access points 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 access points to segregate data types onto the different RF bands. The access point's 802.11a radio can service wireless traffic from time-sensitive voice/data clients (VoWLAN handsets), while the 802.11b/g radio supports data traffic from laptops, this can reduce data and voice traffic contention by creating two separate RF networks. Since 802.11a is in 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 (e.g., clients probes/responses) generated by internal and external 802.11b/g WLANs.

Additional Functions and certifications

Capacity planning: 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 emergence of dual-mode technology. Some companies ensure adequate capacity by using dual-band access points (802.11a and 802.11g standards combined) to separate voice and data onto different spectrums. Engineering a WLAN network for VoWLAN often involves installing more Access Points and backing off the transmit power to minimize co-channel interference with AP's on the same channel. Another option is to use advanced management tools that provide site survey analysis and capacity planning and RF management. Such tools can provide visibility into network usage per access point or per facility, and determine when additional access points are required. Virtual RF management tools tune the WLAN's RF parameters to provide a better user experience.

If an enterprise is considering voice capabilities over their WLAN, additional standards need to be accounted for in the planning and design. The WLAN clients and access points should support the following features:

- Supports 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).
- Quality of service (QoS) for prioritization of delay/jitter-sensitive voice traffic through protocols such as IEEE 802.11e or the WiFi Alliance's Wireless Multimedia (WMM) specification. If an enterprise is considering voice applications over the WLAN, QoS is imperative and needs to be included in any planning and design of the WLAN. Another application that benefits from QoS is prioritized traffic management, which allows the IT administrator to assign different priority levels to different users. For instance, network administrators may wish 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 those 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 Wireless Multimedia -Power Save (WMM-PS). WMM-PS addresses the challenge by offering 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 access points and centrally coordinated – have benefits that are well suited to different environments.

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

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

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

- Access point 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 reconfigure access point parameters as needed to maintain high service levels.
- The WLAN network can be expanded or reduced easily by simply plugging in or removing Access Points after which the controller will reconfigure the network based on the new 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 that 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 these access points presents a challenge in addressing security, configuration control, bandwidth predictability, and reliability, as users and applications become dependent on an always available and reliable WLAN connection.

Coordinated 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 voice over WLAN.

Site Survey

One of the key factors in determining 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; coverage patterns to adopt; and amount of capacity needed. Your site survey should yield a network design document that describes the location of each access point, its coverage area, and the 802.11 a, or b/g channel selections for the access point.

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 search threshold; range and throughput; interference/delay spread; bandwidth management for applications like voice over WLAN; access point density and load balancing.

Surveying for the “weakest link” is another important activity. This requires a consideration of different radio cards, as well as the devices themselves and how they interact within the environment. For example: surveying with a laptop with an exposed radio will not accurately illustrate the coverage that a mobile handheld terminal will experience.

With the limited channel availability, channel usage and selection are paramount. It isn't simply a question of installing more access points to provide more performance or greater coverage. The limited channel capacity of 802.11 based WLANs does not allow for an infinite number of access points 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 access points.

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 – not only outdoors, but also in many lobbies, courtyards or other interior public spaces.
- Coated glass – transparent glass generally does not greatly degrade signal strength. But it may do so 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 times when the service is expected.

Security

Security needs to be paramount and a major consideration for any WLAN deployment. The inherently open nature of wireless access – compared to the wired world – creates significant security concerns, especially 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.

One of the obstacle's in deploying WLANs is that IT security and network managers face the difficult decision in choosing how to secure WLAN communication with multiple forms of authentication and encryption. In selecting networking equipment, it is essential to choose access points 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 access points require more sophisticated access control through incorporating remote authentication dial-in service (RADIUS) servers. For smaller networks that function without a centralized RADIUS server for user authentication, some access points offer built-in RADIUS authentication. Your access points 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. In regards to security options, standards and certification bodies have released various security standards to secure WLANs.

Wired Equivalent Protection - WEP represents the initial attempt at providing wireless networks with a level of security comparable to that of wired networks that involves only one-way authentication. 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 WEP highly susceptible to a variety of Man-in-the-middle attacks and session hijacks.

802.11i and 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 the EAP (extensible authentication protocol) protocol to provide strong mutual authentication between the user and the network. In such a scenario, the client must authenticate itself to the RADIUS server, and the AP must authenticate itself to the client before either granted access to the larger network. 802.1X in its native state provides only authentication not encryption. To deliver encryption capabilities, 802.1X should be used in conjunction with an encryption method.

EAP - To deliver both authentication and key management, the 802.1X protocol requires EAP (Extensible Authentication Protocol). 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, 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. Below is a table that identifies the differences between the most widely available EAP methods.

Deploying a Wireless LAN

Considerations and Questions in Planning a Wireless LAN

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 – This is the weakest of the possible EAP methods and 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.

PEAP – Very secure solution. Uses TLS to create a secure tunnel where a second authentication mechanism can be used. Does not require a cert on the client, but will use a cert on the server.

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 RADIUS server to authenticate the server and client.

WiFi Protected Access (WPA)/WPA2 - WPA and WPA2 are related specifications based on the IEEE 802.11i standards. WPA or WPA2 are not the security mechanisms themselves, but simply a name for a collection of specific security protocols. Both standards rely on 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 AES or TKIP 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 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 versions of WPA and WPA2: personal and enterprise. WPA (2)-Enterprise specifies how IEEE 802.11i should be used in an enterprise environment where there is authentication infrastructure (i.e. RADIUS servers) available. WPA (2)-Personal specifies how IEEE 802.11i should be used in a SOHO environment using a pre-shared key.

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

VPN

For either existing legacy WEP-based WLAN deployments, or for new deployments that have difficulty deploying 802.1X end-to-end and therefore are not suitable for 802.11i-based link layer encryption, robust Virtual Private Network (VPN) should be utilized. VPNs have been and remain a standard security practice for providing secure access from an insecure or non-trusted location. In this regard, VPNs make a good deal of sense for use in WLANs, and many network managers have taken this approach. The main advantage of the VPN approach is that it leverages technology and skills that many IT managers already possess and is vendor neutral in terms of access points. The drawback is that it requires management effort on each wireless client, which can quickly become unmanageable if WLAN is to be rolled out to all employees and network users. Additionally, VPNs come with significant processing requirements that could negatively impact the overall performance and scalability of the network. It is also worth noting that a VPN solution only begins working at Layer 3, whereas the other security methods discussed above work at Layer 2.

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 network to identify rogue WLANs, detect intruders and impending threats, and 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. Some of these tools will actually 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 does not disrupt business.

Putting It All Together for Voice and Data over WLAN

Given the above considerations, 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 voice end point battery life.

Section Two – Questions to pose to WLAN Vendors

How do you begin to define a WLAN to ensure that vendors will know exactly what you're looking for? Well, it means asking enough of the related questions on how you plan to use your wireless network so you can clearly outline your requirements. Below are some of the areas with specific questions that may help you define those requirements. This following list of questions is not intended to be exhaustive, but provides a solid foundation for a starting the evaluation process.

Architecture

- Does the solution consist of a centralized controller supporting access points or is it built with stand-alone intelligent access points only?
- What functions does the controller perform for the wireless network?
- Does the controller support seamless roaming across IP subnets?
- What is the tunnelling protocol running between the controller and the access points? Is that protocol access point agnostic? Is it proprietary or standards based?
- How many access points 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 access points?
- Does the system support redundant controllers?
- Do the access points failover to a secondary server if the primary goes down?
- When failing over from one controller to another, does the mobile user's session stay active? Does the IP address change?

Standards

- Which 802.11 standards does the solution support?
- Does the system support 802.1X?
- What EAP methods are supported?
- Is there support for WPA or WPA2?
- Does it support WMM, U-APSD?
- Is the system Wi-Fi certified?
- What other WLAN certifications?

Access Points

- Which radio frequencies are supported?
- Can the administrator control which 802.11 services are available (a,b, and/or g)?
- Are the power levels configurable?
- What is the maximum power level?
- Is RF Management software available to automatically support channel selection, power levels, load-balancing and failover?
- Are the RF Management functionality calculations performed on the access point or on the access point or on the controller?
- Is Power-over-Ethernet standard 802.3af supported?
- Are third party antennas supported?
- Is the access point accessible via Ethernet?
- Is any user information stored on the access point?
- How many SSIDs can each radio support?
- Is the name and description of the access point configurable via the controller?
- When roaming between access points is the latency under 20ms?
- Is QoS supported?
- Do the access points support Call Admission Control (CAC)?
- Can a voice call roam from access point to access point without being dropped?
- Can a voice call roam between access points that are on different subnets on the wired side without being dropped?

WLAN End-user Devices

- Do the end devices have multiple radios (802.11a/b/g radios)?
- Do the devices have the ability to support a wide range of WLAN security methods?

WEP, WPA, WPA2

- Do the devices have the ability to support a wide range of EAP methods?

LEAP, PEAP, EAP-TTLS, EAP-TLS, EAP-FAST

- VPN client support for end-device? Separate software or built-in?
- Does the end-device have QoS?
- Does the end-device support Call Admission Control? Which vendors CAC is supported?
- What are the supported capabilities of extending battery life?
- What is the expected battery life on both standby, data only, and if applicable, data and voice usage?
- Can device scan for available networks?
- Device supports connectivity to hotspot and public WLAN using captive portals? EAP-SIM for carriers' hotspots?
- Policies available to manage and control access, features, functionality of end device?
- Process and capabilities of provisioning end device? Can provisioning be done remotely?
- Can it 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 access points at once? Automatically? In groups?
- Does the solution support RF management?
- Are the RF Management algorithm processing done by the access point or the controller?
- Does RF management include correcting for failed access points, channel interference, and unbalanced loads?

Security

- Does the solution support 802.1X? Is there a RADIUS authentication server available?
- If a RADIUS server is available, which EAP protocols are supported?
- Does the solution support WEP?
- Does the solution support 802.11i? WPA or WPA2?
- What encryption methods are supported? Does the hardware support AES encryption?
- Is rogue AP detection supported?
- Can rogue AP scans be scheduled?
- Can rogue AP scans be scheduled by AP, by radio and by channel?
- Can detected rogue AP's be classified into groups?
- Can rogue AP scan parameters be configured?
- Does the solution support WPA in both enterprise and pre-shared key modes?
- Is WEP with static and dynamic keys supported?

Glossary

802.1x - IEEE 802.1X is 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.

802.3af - The IEEE standard 802.3af describes a mechanism for Power over Ethernet (PoE). The standard provides the capability to deliver both power and data over standard Ethernet cabling.

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.

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.

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 Media Access Control (MAC) layer.

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.

802.11i - Is an amendment to the 802.11 standard specifying increased security mechanisms for wireless networks.

802.11n - In January 2004 IEEE announced that it had formed a new 802.11 Task Group to develop a new 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.

A

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

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

Attenuation - A term used to describe decreasing 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

Call Admission Control (CAC) - 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).
Counter-Mode Cipher Block Chaining Message Authentication

Code Protocol (CCMP) - Wireless encryption protocol based on the Advanced Encryption Standard (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.

Direct Sequence Spread Spectrum (DSSS) - 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

Extensible Authentication Protocol (EAP) - The Extensible Authentication Protocol is 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 also permits the use of a "back-end" server, which actually implements the various mechanisms while the PPP authenticator merely passes through the authentication exchange.

Extensible Authentication Protocol Method for GSM

Subscriber Identity Module (EAP-SIM) - Is an EAP mechanism for authentication and session key distribution using the Global System for Mobile Communications (GSM) SIM card.

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

Extensible Authentication Protocol-Tunnelled Transport

Layer Security (EAP-TTLS) - 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 - is 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.

Federal Communications Commission (FCC) - The Federal Communications Commission (FCC) is 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

Institute of Electrical and Electronic Engineers (IEEE) - 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.

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

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

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

J

Jitter - Jitter is 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

Local Area Network (LAN) - 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). Lightweight Extensible Authentication Protocol (LEAP) - 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 is one thousandth of a second.

Man-in-the-middle (MITM) - A man in the middle is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.

Medium Access Control layer (MAC Layer) - Provides medium access services for IEEE 802 LANs.

Megahertz (MHz) - One million cycles per second.

O

Orthogonal Frequency Division Multiplexing (OFDM) - A method of digital modulation in which a signal is split into several narrowband channels at different frequencies.

P

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

Protected EAP (PEAP) - Is 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

Quality of Service (QoS) - 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

Remote Authentication Dial In User Service (RADIUS) - 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.

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

Request-to-Send/Clear-to-Send (RTS/CTS) - 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.

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

Rogue access point - A rogue AP refers to an Access Point that is being used to gain wireless access within an enterprise, but is not part of a sanctioned WLAN.

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.

Service Set Identifier (SSID) - 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 are combined communication protocols used to connect hosts and transmit data on data networks.

Temporal Key Integrity Protocol (TKIP) - A protocol used by EAP to improve data encryption.

U

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

V

VLAN - The term VLAN was specified by IEEE 802.1Q; it defines 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.

Voice over IP (VoIP) - Voice calls over an IP network, also called IP telephony

Voice over WLAN (VoWLAN) - VoIP calls over a wireless LAN

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

W

Wi-Fi™ - short for "Wireless Fidelity", is 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.

Deploying a Wireless LAN

Considerations and Questions in Planning a Wireless LAN

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

WLAN - A wireless LAN is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. A standard, IEEE 802.11, specifies the technologies for wireless LANs.

Wired Equivalent Privacy (WEP) - A security protocol designed to provide the same level of security as that of a wired LAN. WPA - Wi-Fi™ Protected Access is the Wi-Fi Alliance's certification that uses the TKIP encryption method and EAP or PSK authentication.

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

Deploying a Wireless LAN

Considerations and Questions in Planning a Wireless LAN

*Check with service provider for availability, roaming arrangements and service plans. Certain features outlined in this document require a minimum version of BlackBerry Enterprise Server software, BlackBerry Desktop Software, and/or BlackBerry Device Software. May require additional application development. Prior to subscribing to or implementing any third party products or services, it is your responsibility to ensure that the airtime service provider you are working with has agreed to support all of the features of the third party products and services. Installation and use of third party products and services with RIM's products and services may require one or more patent, trademark or copyright licenses in order to avoid infringement of the intellectual property rights of others. You are solely responsible for determining whether such third party licenses are required and are responsible for acquiring any such licenses. To the extent that such intellectual property licenses may be required, RIM expressly recommends that you do not install or use these products and services until all such applicable licenses have been acquired by you or on your behalf. Your use of third party software shall be governed by and subject to you agreeing to the terms of separate software licenses, if any, for those products or services. Any third party products or services that are provided with RIM's products and services are provided "as is". RIM makes no representation, warranty or guarantee whatsoever in relation to the third party products and services and RIM assumes no liability whatsoever in relation to the third party products and services even if RIM has been advised of the possibility of such damages or can anticipate such damages.

© 2007 Research In Motion Limited. All rights reserved. Research In Motion, the RIM logo, BlackBerry, and the BlackBerry logo, are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries. These marks, images and symbols are owned by Research In Motion Limited. All other brands, product names, company names, and trademarks are the properties of their respective owners. The specifications and features contained in this document are subject to change without notice. MKT-15757-001

All other brands, product names, company names and trademarks are the properties of their respective owners.

The handheld and/or associated software are protected by copyright, international treaties and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D,445,428; D,433,460; D,416,256. Other patents are registered or pending in various countries around the world. Please visit www.rim.net/patents.shtml for a current listing of applicable patents.

This document is provided "as is" and Research In Motion Limited (RIM) assumes no responsibility for any typographical, technical or other inaccuracies in this document. RIM reserves the right to periodically change information that is contained in this document; however, RIM makes no commitment to provide any such changes, updates, enhancements or other additions to this document to you in a timely manner or at all. RIM MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR COVENANTS, EITHER EXPRESS OR IMPLIED (INCLUDING WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, MERCHANTABILITY, DURABILITY, TITLE, OR RELATED TO THE PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE REFERENCED HEREIN OR PERFORMANCE OF ANY SERVICES REFERENCED HEREIN). IN CONNECTION WITH YOUR USE OF THIS DOCUMENTATION, NEITHER RIM NOR ITS AFFILIATED COMPANIES AND THEIR RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES OR CONSULTANTS SHALL BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER BE THEY DIRECT, ECONOMIC, COMMERCIAL, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY OR INDIRECT DAMAGES, EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF BUSINESS REVENUE OR EARNINGS, LOST DATA, DAMAGES CAUSED BY DELAYS, LOST PROFITS, OR A FAILURE TO REALIZE EXPECTED SAVINGS.

This document might contain references to third party sources of information and/or third party web sites ("Third-Party Information"). RIM does not control, and is not responsible for, any Third-Party Information, including, without limitation the content, accuracy, copyright compliance, legality, decency, links, or any other aspect of Third-Party Information. The inclusion of Third-Party Information in this document does not imply endorsement by RIM of the third party in any way. Any dealings with third parties, including, without limitation, compliance with applicable licenses and terms and conditions, are solely between you and the third party. RIM shall not be responsible or liable for any part of such dealings.



© 2007 Research In Motion Limited. All rights reserved. Research In Motion, the RIM logo, BlackBerry, and the BlackBerry logo, are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries. These marks, images and symbols are owned by Research In Motion Limited. All other brands, product names, company names, and trademarks are the properties of their respective owners. The specifications and features contained in this document are subject to change without notice. MKT-15421-001.