

Enterprise



Interoperability Considerations for Today's Wi-Fi Networks

Kevin Lin

Introduction

As Wireless LANs (WLANs) have expanded rapidly over the recent years, the adoption rate for the IEEE 802.11 technology has seen a tremendous growth. Such market demand for unwiring enterprise networks have created business opportunities for companies to introduce wireless access equipment and client devices to meet such demand.

Today, end users often have to choose between some popular brands such as Intel, Netgear, Cisco/Linksys and Dell when it comes to everyday purchases to satisfy their wireless needs. What the users might not realize is how their decisions could affect how their wireless infrastructure should be deployed in order to gain maximum performance due to their unique characteristics.

This paper addresses some of the deployment issues users might face with Wi-Fi deployments and methods to avoid these issues.

Where the 802.11 Specification Leaves Off

It is first important to identify areas that the 802.11 specifications leaves open and consider how manufacturers may interpret the intentions of the specification. Differences in interpretation can easily lead to interoperability or even security issues.

For example, until very recently, Microsoft XP SP2 wireless configuration service (WZCSVC) attempted to “park the NIC” by sending a random ESSID to the driver with no security options (plain text). Many drivers will see this as a request made by the supplicant, and sends probe request for association. This is a legitimate implementation and does not violate any 802.11 specifications, but it placed Windows clients at risk for any unscrupulous person to sniff the ESSID in the air and provide an AP for the client to associate to. This is a very common and undesirable security flaw, and Microsoft may not be the only supplicant manufacturer to have this flaw. Any device used within the trusted corporate machines should be tested. All it takes is one single device in the entire network to compromise security.

Such vulnerabilities can be seen within the 802.11 specification itself. On page 376 of the 802.11-1999 specification, it allows an authentication response to contain a different source address rather than its own BSSID, thereby creating a “BSSID redirection”. At this point, it is up to the client’s discretion whether to associate to the new BSSID or to ignore such redirection. Once again, this is a security flaw only if manufacturers realize such holes in the specification during the implementation. Neither implementation is out of specification and is therefore fully 802.11 compliant.

It is well accepted that not all clients are designed to strictly comply with specification. This is where interoperability issues arise and manufacturers hold interoperability events to ensure intra-vendor compatibility. Thus, it is important to check with the WLAN infrastructure vendor for a list of approved devices and software before heavily investing in various wireless devices and software.

Legacy devices

The early adaptations of 802.11 did not have the options of 802.11g nor 802.11a, as it was a time when 802.11b was *the* wireless LAN solution in the market. Since 802.11g has made a conscience effort to be backwards compatible with 802.11b, there are still many of these legacy devices in the field today. This is especially true for the more expensive barcode scanners which are costly to replace, and they do not need the higher speed offered by 802.11a/g.

Knowing that these legacy devices are out there, special care needs to be taken to ensure interoperability with more modern architecture. 802.11b and 802.11g both operate in the same 2.4GHz spectrum, but the primary difference is speed (11Mbps for 802.11b and 54Mbps for 802.11g). The difference in speed is mainly due to transmission method. 802.11b uses Direct Sequence Spread Spectrum (DSSS) while 802.11g and 802.11a uses Orthogonal Frequency Division Multiplex (OFDM). This results in the new basic and supported rates for 802.11g and 802.11a.

To ensure 802.11b is supported, make sure to enable basic and supported rates of 1, 2, 5.5 and 11Mbps on the 2.4GHz radio of the AP. The 1Mbps and 2Mbps rates are essential for transmission and receipt of management packets in some devices.

Also note that some legacy devices may not have the ability to support short preamble. As a result, this option could be turned off if there are connectivity issues even though short preamble supports the normal preamble length. The tradeoff is 9 bytes difference in the Physical Layer Convergence Protocol (PLCP), increasing performance throughput for devices that supports the shorter preamble.

Proprietary solutions

In an effort to tackle some of the challenges observed by wireless LAN users, some companies have developed proprietary solutions in hopes of solving these challenges and use these as selling points for their products. While these solutions may sound promising, they are not WiFi certified – implying that they are not part of the 802.11 standard and will likely not be supported by most other vendors.

In an effort to understand the interoperability implications of these proprietary solutions, a few examples will be discussed in this section. The important question is whether the benefits of proprietary technology are superior to those of industry standards, if there is an existing or pending industry standard to satisfy the same need. Often, this is not the case, as propriety solutions imply higher costs for both the infrastructure and client, with very little flexibility to support alternative vendors.

Cisco Compatible Extensions (CCX)

CCX is a specification for 802.11 wireless LAN vendors for ensuing compliance with Cisco's proprietary wireless LAN protocols. There are four (4) versions of the Cisco Compatible specification at the time this paper is written: Version 1 (V1), Version 2 (V2), Version 3 (V3) and Version 4 (V4), with each version building upon its predecessors.

The CCX specification includes proprietary encryption methods and protocols such as the Cisco TKIP (also known as CKIP), Lightweight Extensible Authentication Protocol (LEAP) and Cisco Centralized Key Management (CCKM).

- CKIP is a pre-standard implementation which offers a hashing algorithm and Message Integrity Check (MIC), which is also present in the common implementation of TKIP. CCX V2 and beyond adds support for TKIP, which has been mandatory for WiFi certification.
- LEAP is a WEP-based authentication type that has proven vulnerable to brute-force attacks. EAP-FAST was later developed as an alternative to LEAP. In security, it is not safe to assume that a proprietary encryption or authentication type is secure. The more public scrutiny given to an encryption type, the more secure it is likely to become.
- CCKM enables fast 802.1x reauthentication – where a client does not have to be reauthenticated by an authentication server if it was previously authenticated. This protocol helps with a smoother transition for clients to roam between APs. In response to the need for an industrial protocol standard for fast roaming in today's WiFi deployments, the IEEE 802.11r task group is completing a standard for all WiFi certified devices to participate in fast roaming technology without the use of CCKM.

Prior to deploying a proprietary CCX network cost must be considered. Make sure that the CCX solution is justification for higher infrastructure and end-user costs. Keep in mind that the 802.11 task groups are constantly working on standardized improvements for common wireless needs.

Chipset Specific Enhancements (Atheros Super, Turbo and XR capability)

Atheros chipsets supports proprietary technologies (i.e. Super, Turbo and XR) to enhance wireless performance. However, some misconceptions are often associated with cards that support these chipsets. What may not be immediately apparent is that these are proprietary protocols and are not compliant with standard WiFi infrastructure. For most enterprises or large scale implementations, this is simply not acceptable. In these environments, it makes more sense to rely on standards such as the IEEE 802.11n specification to provide a standardized solution for tackling performance, throughout and range enhancements in WiFi networks.

Application Specific Devices (ASD)

Application specific devices cover a wide range of WiFi products that are manufactured to perform a certain set of tasks. Examples of ASDs include cellular phones, PDAs, scanners, printers, projectors and cameras. Not only do these devices often come with special chipsets and drivers, they are also designed to be very power efficient.

Power-Save Compatibility

802.11 devices save power by allowing the chip to power down in time intervals defined by the DTIM. It is essential for APs to recognize the power-save state of the devices, so that packets will be buffered properly during sleep, and sent once the client is awake. It may be possible for a client to sleep for a long time if it was not designed to transmit or receive a high volume of traffic.

To reduce potential interoperability issues due to power-save mechanism, it is advisable to look for a WLAN solution with extra power-save intelligence built-in. Modern WLAN solutions often have the ability to change channels dynamically based on the changing RF environment, and can, therefore, optimize background scanning. Giving APs the intelligence to be power-save aware will make the AP more conservative with its background scanning algorithm and avoid channel changes when there are clients in a power-save state. Having such intelligence will improve connectivity or performance issues compared to a basic product.

Roaming Compatibility

Because ASDs are typically based on mobile applications, they tend to move around frequently. This is where roaming capabilities of the supporting infrastructure are relevant. Ideally, devices should experience seamless handoffs while moving between APs within the network. Voice over IP (VoIP) clients tend to be the least tolerant of a poor mobility architecture resulting in reduced voice quality or even dropped calls. Similar to power-save clients, it is equally important for APs to recognize VoIP clients and adjust to the RF requirements dynamically.

Especially in cases where VoIP is a critical network application of the intended WLAN deployment, it will be crucial to select an infrastructure that handles voice-centric devices with maximum power save, while still providing complete mobility.

Interoperability in the Enterprise

Modern WLAN deployments in enterprises are architected and deployed in a pico cell layout. Unlike open spaces, indoor enterprise buildings typically provide challenges such as multi-path, blind spots, interference, and high user density. To counter most of these challenges, a common approach is to deploy several thin APs on a single floor and manage them via a controller or a WLAN management system using a RF planning tool or application. In an enterprise environment, the deployment of these APs opens up a new set of considerations related to interoperability that may affect user experience.

The advantages of thin AP over fat AP deployments not only include the ease of management, but also RF technologies to change power and channel settings adaptively based on the changing environment. Having pico cell deployments with these capabilities will also force clients to perform a lot of roaming and channel shifting, so it is very important that the infrastructure is designed for mobility.

Here are some of the simple actions that could help address enterprise interoperability issues:

-
- Take a survey of popular devices in use, and plan based on the characteristics of these devices. For example, if all the clients will be 802.11b/g only, then the APs should be set for the same mode. This will likely be the case in environments where only handheld devices are used, since most of these devices only support 802.11b/g at the present time.
 - Make sure RF planning is done for both 802.11b/g and 802.11a coverage. A well planned 5GHz RF coverage for 802.11a devices does not imply that 802.11b/g clients will get the same coverage and vice versa. If there is known interference in one of the spectrums, most of the clients can be configured to operate in 802.11b, 802.11g or 802.11a mode only. This way client do not waste time scanning for channels without network connectivity.
 - Adjust roaming aggressiveness on clients. Depending on how closely APs are placed together, and on several environmental factors, it may be advisable to change roaming properties in the client's driver settings. For instance, if a client tends to "hop between APs" too frequently, the roaming aggressiveness should be lowered. Some WLAN solutions have an AP assisted handoff feature which helps reduce the client "stickiness" problem.
 - Make proper adjustments to the power save parameter. Clients should be configured to a constant "awake" mode if they are typically plugged into a power source, since battery life is not a factor in this case. Do not set DTIM too high if the application demands high data throughput, but try to stick to the manufacturer's recommended settings and experiment and tweak power-save values before deployment.
 - Adjust AP settings as necessary. Some clients have a tendency to attempt authentication or to send data at high rates even though packet loss may be high at such rates. Try providing a cleaner RF environment by adjusting channels and power levels on nearby APs, or change the supported rates if necessary. For APs that support automated RF management capabilities, parameters can be fine tuned so that power and channel settings are adjusted to optimal levels automatically.
 - Select the correct antennae type and placement. Try using directional antennas if Omni directional antennas are not well suited for deployments such as ceilings or rooftops. Make sure the antenna selected matches the impedance recommended by the AP manufacturer, and that the antenna is designed to work in the frequency range intended. More often than not, antennae selection are the main culprits of interoperability issues.

Conclusion

Interoperability is the underpinning of any successful wireless deployment. Having the most current and advanced clients is only useful if the wireless infrastructure is configured to work well with these devices. When deploying a WLAN network, the most important considerations should go into usability, security and mobility. Try to consult WLAN infrastructure vendor documentation for supported wireless network interfaces cards and software. If the clients are already in place, make sure the new infrastructure will provide flexible support to tweak its operating environment while providing a secured and smooth mobile experience. WLAN infrastructure advancements now help ease interoperability considerations considerably. Advancements include:

- RF Automation techniques
- AP radio flexibility
- Advanced roaming capabilities (load balancing, assisted handoff, etc)
- Application aware infrastructure that can help optimize network performance based on device type and usage
- Diversity of AP and Antennae options

A network should be carefully chosen to accommodate both current and anticipated interoperability considerations. Making this a planning requirement instead of an afterthought will help to smoothly transition the enterprise into wireless mobility.

About Aruba Networks

Aruba securely delivers the enterprise network to users, wherever they work or roam, with usercentric networks that significantly expand the reach of traditional port-centric networks. Usercentric networks integrate adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system that can be easily deployed as an overlay on top of existing network infrastructure. Adaptive WLANs deliver high-performance, follow-me connectivity so users are always within reach of mission-critical information. Identity-based security associates access policies with users, not ports, to enable follow-me security that is enforced regardless of access method or location. Application continuity services enable followme applications that can be seamlessly accessed across WLAN and cellular networks. The cost, convenience, and security benefits of user-centric networks are fundamentally changing how and where we work. Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at <http://www.arubanetworks.com>.

© 2007 Aruba Networks, Inc. All rights reserved. Aruba Networks, BlueScanner and RFprotect are trademarks of Aruba Networks, Inc. All other trademarks or registered trademarks are the property of their respective holders. All rights reserved. Specifications are subject to change without notice.

WP_INT_US_071217

