WIRELESS AIRSPACE MANAGEMENT FOR MAXIMUM SPEED AND RELIABILITY

Ensuring Reliable, Uncontaminated RF Signals Is Key to Delivering Predictable Mobility Services and Nonstop Wireless Connectivity

Challenge

The RF spectrum is becoming crowded as more and more 802.11 and non-802.11 devices compete for precious airtime. Left unchecked, reduced airtime availability and degraded air quality result in user dissatisfaction.

Solution

From advanced three-dimensional planning capabilities that optimize the design for maximum coverage and capacity, to location-aware spectrum analysis across all frequencies, Juniper enables network managers to effortlessly detect, classify, and isolate performance degrading interference sources, and maximize the user experience.

Benefits

- Continuous connectivity with a predictable user experience
- Best possible coverage and capacity for all users at all times
- Consistent signal strength tuned for optimal voice services
- Enterprise-wide visibility of RF Spectrum health

The number of users with Wi-Fi-enabled devices now competing for airtime continues to grow at an astonishing rate. Not only is the user base growing, so too is the number of devices, as more and more people whip out their dual mode smartphones for some tasks, while using a laptop or tablet for others. But that is not all. The average airtime demands from each user are also growing, as the mix of content shifts ever more toward high bandwidth multimedia.

On enterprise wireless LANs, airtime is a scarce resource that is easily squandered either by careless planning or inadequate tools for detecting, isolating, and avoiding rogues, or adjacent 802.11 networks. Ignorance about the growing number of non-802.11 interference sources which also occupy the unlicensed spectrum is another contributing factor. For these reasons, airtime and air quality must be carefully managed, in order to maximize signal strength and maintain optimal transmission rates.

In keeping with its strategy to deliver the most reliable end-to-end mobility and a simply connected experience for users, Juniper Networks delivers a comprehensive solution for maximizing air quality and signal strength, even when faced with non Wi-Fi interference sources. Beginning with advanced radio frequency (RF) planning tools for designing the best possible physical layout of a wireless network, Juniper's wireless access points, controllers, and management software work together to eliminate most potential sources of signal degradation while minimizing the level of hands-on involvement required from a network manager.

The Challenge

Security issues aside, the most important and yet most vulnerable part of a wireless network is the "over-the-air" signal transmission. Without an adequate signal, there is no wireless service. Too strong a signal from one access point causes co-channel and adjacent channel interference with other access points, while too weak a signal causes coverage holes and dropped sessions. Further, a variety of potential interference sources can degrade signal quality so much that a wireless footprint that appears to have no coverage gaps may actually behave more like one that does. Either way, suboptimal RF performance ultimately wastes capacity and in extreme cases results in user frustration and complaints that the network is unreliable.

One of the problems, of course, is the fact that RF is as mysterious as it is invisible. There is a tendency for the old adage "out of sight, out of mind" to prevail until a serious problem surfaces. IT managers generally don't understand how RF works, nor do they want to, and frankly nor should they need to. Nevertheless, what you can't see, can hurt you! Turning a blind eye to RF signal integrity can mean that users suffer degraded performance while IT, oblivious to the problem, assumes that everything is OK. On the other hand, over obsession about every momentary RF glitch is also counterproductive. It is simply not worth the effort to investigate half of the interference incidents, because they are beyond ITs control. In other words, once you've planned around them, you should only care if their severity or frequency worsens.

Therefore, to successfully maximize RF signal quality, enterprise network managers should begin with careful planning and then monitor the network with the necessary tools for detecting, classifying, and mitigating RF problems. The goal should be to maximize transmission quality with the minimum effort—without needing to become RF experts, and also without unnecessary fire drills for every minor fluctuation in signal quality that cannot be prevented anyhow.

The Juniper Networks Coordinated Spectrum Management Solution

Juniper's approach to RF signal quality management does away with the need for time-consuming site surveys using third-party handheld spectrum analyzers. Instead, it provides in-band spectrum analysis and airtime management capabilities that tackle the three main problem areas:

1. **Planning and Establishing a Robust Channel and Power Plan**—This is basic RF management that all vendors address with varying degrees of effectiveness. Assuming you have planned your wireless network correctly, it should provide ubiquitous coverage with no gaps when everything is working right. But if an access point should fail for any one of a number of reasons, it leaves a coverage hole. When this coverage hole is detected, the adjacent access points can each turn up their transmit power to fill in a part of the hole, and collectively it is possible to restore coverage until the failed access point is repaired or replaced.

   As part of the RF planning process, Juniper's 3D predictive planning application calculates the right power and channel settings in advance for every possible access point failure scenario. Aware of the settings of all nearby access points on the floors above and below as well as the floor being planned, Juniper Networks RingMaster® planning is able simulate failure of each access point in turn by temporarily removing it from the plan. In this way, having anticipated what a failure scenario looks like, it can determine the optimal mounting position, channel, and settings for every access point in order to best accommodate full operation and failure conditions alike.

   This offline planning approach is ideal for optimizing the coverage and capacity of your deployment in large enterprise environments where the air space is exclusively under your control. These include university or college campuses, hospitals, and warehouses. However, in more crowded locations such as inner city schools and multi-tenant buildings where your network is surrounded by neighbors with wireless of their own, it is prudent to augment planning with auto-tuning at deployment time. Auto-tune lets access points negotiate their channel and power based on what they see in the RF signals around them. So for example, if a neighboring network is found, your nearby access points can automatically select different channels than those being used by the neighbor to create co-channel separation. Once an optimal plan is determined, it can be locked in.

   On detecting an access point failure, RingMaster issues appropriate alarms and reports. Channel and transmit power changes must be carefully coordinated to avoid abrupt changes to signal strength for active sessions, especially during active voice calls. Voice sessions are particularly susceptible because wireless VoIP handsets prefer the signal strength to fluctuate only within a narrow range.

   No amount of auto-configuration can displace good planning; the combination of RingMaster and Auto-tune lets you avoid placing access points in "RF toxic" areas where they will never be content with the channel. This also prevents the network instability that is caused if you allow ripples of channel changes to thrash back and forth across your network. By using both RingMaster and Auto-tune, you can arrive at an optimal design to meet your capacity requirements with the least number of access points, settling on a reliable channel plan that avoids neighbors and interference.

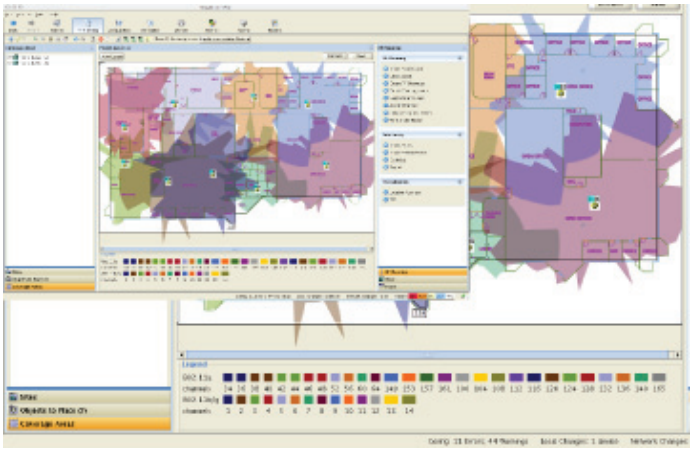

Figure1: Ringmaster planning—screenshot of a completed RF channel plan.

2. **Detecting, Classifying, and Mitigating 802.11 Rogues and Attacks**—Rogue access points are a fact of life, but it is a mistake to assume that they are all malicious. Oftentimes it is simply naive users doing things they don't even realize are a bad idea, such as turning a smartphone or other 3G/4G mobile device into a Wi-Fi hot spot with 3G backhaul to the Internet. Another common problem (not strictly a "rogue") is the result of neighboring businesses adding wireless access or altering their existing configuration. These are easily detected and mitigated using standard mechanisms that almost every vendor supports. On the other hand, malicious attacks such as distributed denial of service (DDOS) are more worrisome, and these require more sophisticated wireless intrusion prevention and detection system (WIPS/WIDS) capabilities.

   Like most other vendors' products, Juniper Networks RingMaster wireless LAN management application coordinates the wireless local area network (WLAN) controllers and access points to exploit standard features provided by wireless chipsets, and it tackles approximately 40 of the most common types of RF abuses and security attacks. But it does not end there. In addition, real-time location tracking capabilities that

are deeply embedded in Juniper's wireless solution also make it possible to block wireless access from devices outside a designated perimeter—for example, the perimeter of a building. Together, all of these measures serve to protect and preserve wireless airtime for legitimate users.

Numerous compliance initiatives such as Payment Card Industry (PCI) for retail, Health Insurance Portability and Accountability Act (HIPAA) for healthcare, and Sarbanes-Oxley Act (SOX) for financial services require regular reports to monitor compliance to these standards. To address these requirements and enable advanced detection and mitigation of nearly 200 more complex attack types, RingMaster may be tightly integrated with advanced third-party WIPS/WIDS solutions using industry standard APIs. For example, the integration with AirTight SpectraGuard provides a rich customizable reporting architecture with predefined reports for compliance initiatives such as PCI, HIPAA, SOX, Gramm-Leach-Bliley Act (GLBA), and Department of Defense (DoD) Directive.

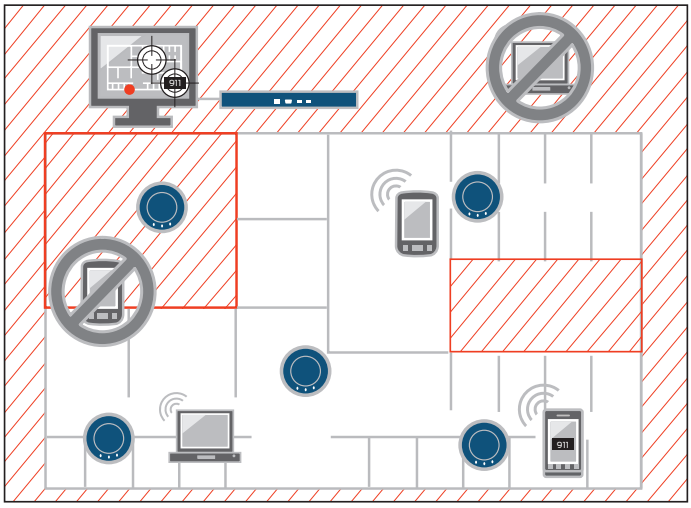

Figure 2: Using real-time location awareness to enforce Geo-fencing.

3. **Detecting and Identifying non-802.11 Interference Sources**—The third form of signal degradation comes from non Wi-Fi devices such as microwaves, radar, frequency hopping spread spectrum (FHSS) phones, and a large number of devices supporting other wireless transmission protocols such as Zigbee, WiMAX, and Bluetooth that overlap Wi-Fi in either the 2.4 or 5.0 GHz frequency ranges. The interference these devices generate results in higher retransmissions from 802.11 clients, which in turn causes affected clients to progressively step down to lower connection rates than they are actually capable of.

   This form of interference is particularly annoying because the originating devices, unlike a rogue access point, cannot be controlled in any way since they are not Wi-Fi compliant. While this class of interference is not new, it is of growing importance for several reasons. First, increasing user demand makes every byte of capacity all the more precious. And second, the number of potential interfering devices is growing at a rapid pace. While changing the transmission channel an access point uses is often the best strategy to avoid these interferers, from a session continuity point of view, on-the-fly channel changes should be considered a last resort. That is because a channel change requires the client to disconnect and reconnect, which results in active voice calls being dropped. Hence, Juniper believes that prevention rather than a cure is the best approach. In addition, since static devices likely represent 80% of incidents, dealing with them in advance eliminates the worst offenders before they can become a problem. For these reasons, the Juniper approach focuses first on informed avoidance before moving to real-time mitigation.

   During the planning stage, all known potential interferers can be added as predefined objects to the 3D RF plan. With each addition, the plan inherits the RF footprint and energy signature exhibited by that type of device. Drag and drop a microwave oven here, a wireless movement sensor there, and so on. Now, the bad effects of these static interferers can be simulated to derive the optimal channel and power settings which take into account the presence of the static interferers in addition to the RF attenuation of the building materials. The result is an RF plan that offers predictable signal strength under all prevailing conditions, and has the least exposure to interference from known static devices.

   With such an optimized RF plan, when interference from these known sources occurs, there is no cause for alarm, because the network was designed around them and the interference impact has already been reduced as much as possible. Nothing is to be gained by changing channels and suffering dropped sessions, only to do the reverse moments later once the interference stops (much like lane changing during peak rush hour, which rarely gets you there any faster). Further, by tackling non-802.11 interferers up front during the planning stage, IT has a unique opportunity to educate facilities colleagues so that they can work together to find more favorable places to put equipment such as microwaves, cordless phones and the like, before these become troublesome. Rather than dealing with interference after the fact, a joint awareness of the issues will pay dividends forever after, as more and more facilities controlled equipment, including heating controls, surveillance cameras, etc, becomes wireless-enabled over time.

   Juniper Networks spectrum intelligence provides unprecedented flexibility. First, the full spectrum scanning may be implemented either in a dedicated sensor mode, or simultaneously together with client access on the same access point. Second, since the spectrum scanning functionality is enabled through software licenses and not tied to the access point itself as is the case with some other solutions, it is possible to move the sensor function from one access point to another as needed. This enables a much higher concentration of sensors than the 1 in 4 ratio recommended for normal on-demand network conditions to assist with troubleshooting. In addition to CapEx savings, this solution also provides the flexibility for multiple access points in the same locale to be instantly converted to sensor mode, in order to assist in the classification and avoidance of unexpected new interference sources. And this can be done entirely remotely from

a management console. Then, when local scanning is no longer needed, those licenses may be redistributed around the campus, to return to the former state of passively scanning the airwaves in a ratio of one sensor access point to four client access points.

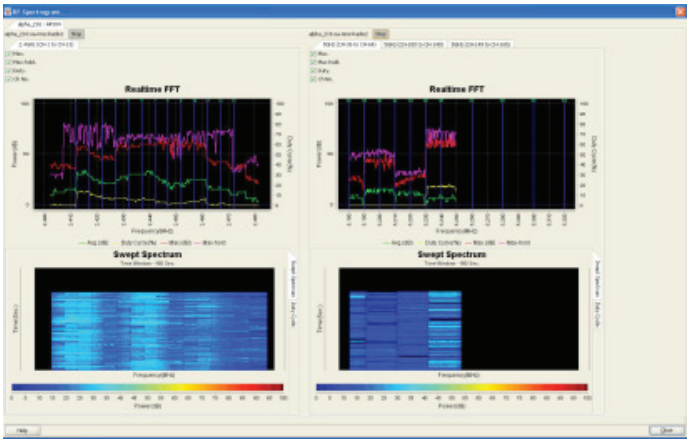

Figure 3: Screenshot of real-time spectrograms in RingMaster.

Juniper 802.11n access points can examine the energy signature of nearby non-802.11 interference sources and classify them. And since RingMaster knows where those access points are physically located, RingMaster can generate appropriate alerts and visualize the interferers in the floor view of the management console. If it is a known device and the severity is as expected, there is no cause for alarm. But if it is a new source, or a known source that has been moved, higher priority alarms can be raised. Once the new interference source has been evaluated, the network manager can add it to the plan, recalibrate the settings for the affected nearby access points, and push a new configuration out to the controller and access points—all with a few mouse clicks, and virtually zero RF know-how.

Features and Benefits

Table 2. Features and Benefits of Juniper's Nonstop Wireless Solution

FEATURE	BENEFIT
RingMaster planning	• Enables 3D planning of the RF environment for maximum coverage, capacity, and reliability with the least number of access points.
Auto-tune	• Negotiates among all access points to ensure that the optimal channel plan and transmit powers on discovering neighboring access points and channel conflicts.
WIDS/WIPS	• Able to detect and locate rogue access points and their users and many other common threat types, including denial of service (DoS) and probe attacks. • RingMaster can also be integrated with advanced wireless intrusion detection systems (WIDS) and wireless intrusion prevention systems (WIPS) from third parties, allowing alarms to be correlated with other service information for faster threat mitigation.
Spectrum analysis	• Support for both dedicated sensor and simultaneous sensor/client access modes of operation enables flexible deployment options. • Includes the ability to detect and classify non Wi-Fi interference sources and report their existence in real time to RingMaster.

Solution Components

Juniper Networks WLC Series Wireless LAN Controllers—WLC Series controllers provide users with a seamless, secure, and exceptionally reliable roaming experience wherever they are and no matter what device they are using. Meeting the needs of any size network, from small branch offices or retail outlets to large enterprises and university campuses, identity-based networking policies enable users to have a common experience with consistent services across wide geographies.

Juniper Networks WLA Series Wireless LAN Access Points—WLA Series WLAN access points provide indoor and outdoor client access as well as active scanning of the air waves. The WLA Series delivers reduced latency, massive scalability, and high performance for wireless VoIP, video, and location services.

Juniper Networks WLM Series Wireless LAN Management Appliances—In addition to RF planning, the WLM Series Wireless LAN Management suite unifies infrastructure, security, and services management, enabling network administrators to plan, configure, deploy, monitor, and optimize wireless networks of any size and geography, all from one console.

Summary—Keeping Users Simply Connected

Juniper's approach to over-the-air reliability tackles the three primary threats to signal integrity, and does so a way that reduces IT management operational overhead, while maximizing signal quality from the moment the wireless LAN is first planned and put into operation. First, signal loss resulting from access point or radio downtime is corrected through coordinated channel and power adjustments on adjacent access points to fill in coverage holes,

without compromising the continuity of existing sessions. Second, through early detection of rogues and neighboring access points, as well as the most common malicious attack types, Juniper's WLAN system can isolate rogues, avoid the airspace occupied by neighbors, and prevent security threats, all of which, if left unchecked, erode available airtime. And third, by identifying the position of static non Wi-Fi transmitters such as microwaves during the planning stage, their potential contaminating effects can also be avoided or minimized by transmitting on different channels.

One of the secrets of success with wireless deployments is to maximize performance and reliability, while minimizing the resources required to design, install, and operate the wireless network. By combining the powerful 3D planning and management features of RingMaster with advanced spectrum analysis capabilities in the access points, Juniper Networks makes it easy for users to be simply connected and to enjoy a more predictable and nonstop wireless experience.

Next Steps

To learn more about Juniper's wireless LAN solution, please go to **www.juniper.net/us/en/products-services/wireless** or contact your Juniper account representative.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

3510407-001-EN June 2011 Printed on recycled paper