The Wireless LAN "Catch-22"

Every network administrator seeking to deploy a wireless LAN is faced with a Catch-22. The dilemma has little to do with security, management, or cost, but it has everything to do with the technology embedded in the access points (APs) available on the market today. The Catch-22 is AP placement – if the APs are placed too close to each other, they cause interference, and if they are placed too far apart, they cause coverage holes.

Unfortunately, this is an issue that network administrators have had to deal with ever since the adoption of 802.11 as an industry specification. This problem exists because the specification simply doesn't address issues regarding multiple APs – it only considers an AP as a single entity. This is fundamentally why 802.11 has enjoyed so much success in single-AP environments such as the home, small office/home office (SOHO), and hotspot markets, and this is also the reason why 802.11 has not had much success in multi-APs environment such as the enterprise market.

There are countless tales of leading-edge enterprise network administrators who have **tolerated** these issues only to see their deployments go awry. These brave souls have had to tolerate extensive (and expensive) site surveys, strategically placing their APs to mitigate the problem of RF interference while manually configuring and managing the RF channels on their APs. And, after all of this, many WLAN deployments reach a point at which the project is simply halted because it has become completely unmanageable.

The Catch-22 is well known throughout the industry, and today, many vendors focus their efforts on **automating** the process of site surveys to provide a best guess on AP placement and RF channel management. In addition, several vendors are debating the question of whether "fat" APs or "thin" APs are better. These approaches, however, simply do not address the technical issues of RF interference, which is the underlying issue stalling the deployment of most wireless LANs. The real question is: why should anyone automate a broken, unmanageable process instead of solving the root cause of the problem? The answer is that solving the fundamental issue of RF interference, while still maintaining compliance with 802.11, is quite challenging.

AirFlow Networks, however, has overcome these technical challenges with patent-pending technology that fundamentally solves this Catch-22. AirFlow's solution **completely eliminates** the need for site surveys, overcomes the AP proximity issue, and eliminates the necessity of RF channel management. In addition, AirFlow's solutions provide a centralized security and management platform that addresses the needs of network administrators looking to deploy wireless networks. The solution is simple, installs in minutes, and is scalable to over 1,000 wireless users with almost no operational costs involved – a secure WLAN that's as easy as Ethernet.

Solving the Catch-22: A Single, Scalable Access Point

The claims made above may seem bold, but AirFlow is able to deliver this low-risk solution due to a simple yet innovative way of looking at wireless networks. Instead of considering a wireless LAN as a collection of individual access points, AirFlow has developed a solution that treats the entire WLAN as a single, scalable AP. That's right, a SINGLE, scalable AP.

Although the underlying technology is quite complicated (with 10 patents filed for protection), the concept is quite simple. AirFlow has designed an access point, called an AirServer, whose Packet Antennas™ can be spread throughout a network over Ethernet cabling. AirFlow's Packet Antennas operate in the same way that the two antennas do on most access points – they do not interfere with each other; instead, they complement each other by providing diversity. Therefore, each Packet Antenna can be placed in close proximity to another to allow uniform wireless coverage at maximum throughput. In addition, Packet Antennas are simple devices that are managed completely by the AirServer, enabling complete plug-and-play wireless networking that's as easy to install as Ethernet.

With this single AP architecture, the Catch-22 with multi-AP deployments evaporates. The issues with RF interference disappear completely, and that opens up a whole new world for wireless networks. Gone are the days of site surveys. Gone are the days of struggling with access point placement and deciding which RF channels to use. And in their place are entirely new possibilities. Imagine a high-performance network with complete uniform coverage, no re-association or re-authentication requirements for mobility, consistent end-user performance, and scalability that can be deployed at any time and without any expertise.

In essence, imagine a world in which secure wireless networking is as easy as Ethernet.

Network Administrator Benefits

The most obvious benefit to network administrators is that they don't have to become RF experts before deploying and managing a wireless network. Since the limitations and complexities of WLANs have been completely eliminated, network administrators can build WLANs as easily as Ethernet networks while still maintaining security and scalability throughout their deployment. The overall result is a drastically lower cost of ownership as well as piece of mind, knowing that there are no wireless "gotchas" lurking somewhere in the network.

No Pre-Installation Site Surveys Required

Most network administrators looking to build a wireless network were forced to hire expensive outside contractors to provide an "RF site survey" of their facility before installing the first piece of wireless equipment. With AirFlow's solution, the whole notion of an RF site survey becomes obsolete since there are no interference issues and therefore no placement issues. Wireless coverage is achieved by placing Packet Antennas where coverage is required instead of being limited by first-generation technology.

Easy Installation

The installation of a Packet Antenna is as simple as installing an Ethernet hub. Like an Ethernet hub, the Packet Antenna is an unmanaged device: no IP address to configure, no serial interface to connect to, no access lists to manage, no security keys to implement. Like an Ethernet hub, the Packet Antenna concentrates traffic back to the network. Unlike an Ethernet hub, though, the Packet Antenna can be powered over the Ethernet link, providing wireless coverage that can be done with only a single connection.

The Packet Antennas can be placed wherever wireless coverage is required. They can be mounted on a wall or placed on a desk. An additional benefit of the Packet Antenna is its pass-through Ethernet port. This allows the Packet Antenna to be connected in-line with an existing Ethernet connection, allowing re-use of cabling. For instance, if a printer is already connected to the Ethernet wall jack, the Packet Antenna can be plugged in between the wall jack and the printer, allowing both devices to share the same Ethernet link.

The installation of an AirServer is as easy as any managed appliance. The AirServer is a rack-mounted device that only requires 1 rack unit of space. This can be installed in the wiring closet or in the data center. After the AirServer is configured with it's IP address, all configuration and management can be accomplished over an IP network.

Centralized Wireless LAN Configuration and Management

The AirServer is where all of the configuration, management, and security reside for the entire wireless network, meaning the network administrator only deals with one device, not each and every AP. The Packet Antennas are completely unmanaged devices, so there is no additional configuration or management required as these Packet Antennas are deployed. There is no need to worry about synchronization between the AirServer and Packet Antenna since there is no configuration stored on the Packet Antenna. As mentioned, all configurations are provided within the AirServer itself.

Centralized Wireless Security

Not only does the AirServer provide centralized configuration and management, but it also provides centralized security for the entire wireless network. Since all wireless traffic is brought back through the AirServer, it is able to monitor the airwaves and determine who is authenticated, who is a guest, and who is a hacker.

The AirServer has integrated support for 802.11 security standards, including 802.1x, WEP, WPA, and future support for 802.1i. In addition, it also has support for IPSec to enable clients to provide encrypted tunneling between the wireless client and the AirServer.

In addition, since the AirServer is the centralized wireless management device, installing additional Packet Antennas do not pose a security risk. The Packet Antennas immediately inherit the security policy as set in the AirServer as opposed to standard APs, which usually ship with security turned off and pose a security hole when installed. Even then, widely publicized surveys have shown that AP security configuration is often so complicated that many enterprise users never activate it properly, leaving serious security holes in their networks.

Guest Access via a “Private Hotspot”

The AirServer has an interesting feature that allows administrators to provide guests with wireless Internet access without connecting that guest to the enterprise network – in essence, a “private hotspot”. The wireless guest is automatically redirected to the web server within the AirServer over an SSL link, and the guest provides a 4-digit key given out by the receptionist. This allows the guest with access to the Internet, but not to the internal corporate network since the guest’s traffic is shunted out the AirServer’s “public port” and directly onto the Internet. Therefore, the guest gets Internet access without having to open a port on the corporate firewall and without jeopardizing the internal network. The 4-digit key is time-based and expires to provide extended security. As expected, any unauthorized user without a key will be immediately rejected.

Scalable Coverage

Since the Packet Antennas can be placed in close proximity to each other, network administrators can scale their wireless coverage. With each Packet Antenna providing it’s own 11Mbps coverage area, and without any concerns for interference, overlapping 11Mbps coverage areas can be created to provide maximum available throughput for clients. Since 802.11 is a shared media, Packet Antennas can overcome the performance issues of traditional shared media by installing these overlapping Packet Antennas.

This feature also has a side benefit. The further a client is from a standard AP, the worse their performance. In a shared media like 802.11, a slow client connection ends up hogging more than their share of the network. For instance, a 10MB file transfer would take about 8 seconds at 11Mbps and 100 seconds at 1Mbps. Since wireless is a shared medium, each user will occupy the network until their task is finished. Traditional AP networks have to deal with this issue since APs cannot be placed in proximity to each other, which tends to aggravate the issue. A uniform 11Mbps AirFlow network can keep all clients at maximum performance and eliminate this issue.

Scalable Throughput

As mentioned above, the Packet Antennas can provide a unique way to provide scalable coverage. One of the benefits is that this entire coverage map is on a single channel and looks like a single AP, providing seamless mobility and consistent throughput. However, what happens when the density of wireless clients increases and divides the 802.11 shared media even further? AirFlow has a unique solution that allows network administrators to overlay multiple coverage areas on top of each other. Imagine a complete 11Mbps coverage map on channel 1. On top of that, there is another completely separate 11Mbps coverage map on channel 6. On top of that, there is a third completely separate 11Mbps coverage map on channel 11. The AirServer manages all of these coverage maps and can assist with load balancing clients across these channels to provide the best overall throughput for the network. In this manner, network administrators can scale the throughput of their wireless network to provide performance enhancements for an increased density of wireless clients.

Dynamic Wireless Coverage Load Balancing

However, a separate issue arises in the instance of a large meeting, where many users congregate in a single area. If they all have wireless client devices, they have traditionally been limited to the single AP in their coverage area. However, with the AirFlow solution, multiple 802.11 channels can be overlaid to provide scalable throughput. In this instance, the AirServer will know the density of wireless devices and load-balance nearby Packet Antennas to use alternative channels (i.e. 1, 6, and 11) to simultaneously provide three separate 11Mbps coverage networks, scaling the performance in the meeting to 33Mbps. After the meeting adjourns, the AirServer will re-load balance back to a uniform 11Mbps coverage map. (This same example can be duplicated with 802.11g and 802.11a as well.)

Wireless Diversity

A further benefit of this coverage density is to provide packet diversity for wireless traffic. Just as a standard AP has two antennas, a few inches apart, for RF diversity, so the wider array of Packet Antennas provides packet diversity through the enterprise. At any given point in the network, a wireless client will be covered by more than one coverage cell. All packet traffic from that client is received at the AirServer from as many Packet Antennas as are in range. Whenever it detects duplicate packets, the switch selects the highest quality signals and discards the duplicates, ensuring the highest possible data transfer performance. This diversity not only providing the highest throughput, but it also provides redundancy in case of a failure.

High-Availability: Fault Tolerance and Redundancy

The AirFlow solutions have been carefully designed to provide complete fault tolerance and redundancy. The AirServer can be multi-homed to multiple switches in the backbone to provide redundancy against an upstream switch or link failure. Multiple AirServeres themselves can be placed in redundant configuration in case of any failure on the device itself. And Packet Antennas can be multi-homed as well to provide redundancy in case of upstream switch or link failure.

Another fault tolerant benefit that is enabled through AirFlow's unique RF solution is redundancy of wireless coverage areas. Since today's standard access points can't be placed in close proximity to each other, an AP failure leads to lost coverage area. With AirFlow's Packet Antennas, though, Packet Antennas can be placed near each other, and if a Packet Antenna fails, then the surrounding Packet Antennas can fill in the gap without sacrificing coverage.

Investment Protection: Support for Next-Generation Protocols

Scenario #1: Imagine that a new security protocol is developed and you determine that you need to implement this throughout your wireless network. Fortunately, all that is required to provide this new security is a software patch. With the AirFlow solution, all that is required is loading new software on the AirServer and your job is done. With traditional APs, the software would have to be installed on each and every AP in order to provide the new security.

Scenario #2: Imagine the above scenario, except this time it requires a hardware change. With AirFlow, you deploy a new AirServer that has the hardware support for this security protocol, but you do not need to worry about the Packet Antennas. With traditional APs, you would need to locate and rip-and-replace each and every AP throughout the network, and then go through the process of reconfiguring each one individually after they are installed.

Future-Proofing: Support for Next-Generation Applications

Although many network administrators may not be planning for applications such as Voice over Wi-Fi, these applications are being developed to take advantage of the wireless LAN. In order to support these real-time applications, the wireless network will need to avoid the re-associating and re-authenticating process that occurs with standard APs when roaming with a handset that supports Voice over Wi-Fi. The AirFlow solution completely avoids the re-association and re-authentication process and therefore provides an infrastructure that can provide support for these next-generation applications.

End-User Benefits

With this unique wireless network, the end-users won't notice any differences. That is the intention – as they roam throughout the network, they won't notice a difference in throughput, they won't notice a difference in connectivity, and they won't notice a difference in configuration. Their performance will be consistent instead of variable, their IP addresses will remain constant, and their IPSec tunnels will remain constant since there are no re-association and no re-authentication issues. As they roam throughout the extensive wireless network, they won't notice any differences because they are associated with the single AP: the AirServer.

Uniform Coverage for Consistent Performance

In any wireless network, a client's performance depends on its proximity to an AP. The closer they are, the better. In an 802.11b network, the performance decreases from 11Mbps to 5.5Mbps to 2Mbps to 1Mbps as the client moves away from the AP. Eventually, their performance decreases below a certain threshold, at which time they de-associate with their AP and re-associate with a new AP.

Since traditional APs don't allow the APs to be placed near each other, this performance degradation and variability is aggravated for roaming clients. With AirFlow, the entire wireless LAN looks like a single AP with uniform coverage provide through overlapping coverage areas. The AirServer monitors the roaming client and can hand off the client to a different Packet Antenna with greater signal strength without forcing the client to deal with a drop in performance to minimum threshold levels. This minimizes the variable throughput most wireless clients deal with today. The AirFlow solution provides more consistent throughput as well as eliminating the side effect of re-association and re-authentication required when moving between APs in traditional wireless networks.

Seamless Mobility

In a standard AP network, wireless devices must disconnect from the network each time they leave one coverage zone and reconnect when they enter a new one. In the AirFlow architecture, by contrast, clients authenticate and connect once, and then can roam seamlessly from one antenna's coverage cell to another with no reconnection.

The AirServer tracks the clients' connection and hands it from one Packet Antenna to another based on signal strength and quality as well as available bandwidth. The effect, for the user, resembles the way cell phone base stations manage subscriber mobility, transferring live calls from one station to another in a completely transparent handover. This allows AirFlow's architecture to handle VoIP/VoWLAN traffic in a seamless way that is not possible with standard APs.

Conclusion

AirFlow’s innovative single AP architecture accomplishes two tasks that once seemed mutually exclusive: solving the 802.11 Catch-22 while still complying with the 802.11 standard. This innovative solution fundamentally eliminates the issues with RF interference and enables a breadth of benefits to network administrators and end-users alike. In the end, AirFlow has enabled a simple, scalable, and secure wireless network that is as easy to deploy as Ethernet.