Tech Brief |

Enterprise

Dedicated Air Monitors? You Decide.

ARUBA® networks

Introduction

Aruba customers commonly ask:

"Do I need dedicated air monitors in an Aruba deployment, or can I get by with just access points?"

The answer is:

Aruba access points double perfectly well as air monitors, but dedicated air monitors provide extra performance and protection.

An Aruba access point can be configured as a thin access point (AP) that provides 802.11a/b/g wireless access to users, as an air monitor (AM) that constantly scans the RF spectrum, or as a device that provides both AP and AM functions simultaneously (a scanning AP).

Any Aruba AP can be dynamically configured into AM mode. Dual-radio APs such as the Aruba 70 can operate one radio in AP mode (servicing clients) and the other in AM mode. As an AM, a radio goes into "listen-only" mode and continuously scans all channels in its band.

An AP automatically provides monitoring on its configured channel. For example, an AP servicing clients on channel 1 provides full monitoring on channel 1. If set to perform off-channel scanning, the AP spends brief time intervals scanning other channels in the band. The shorter the scan interval, the less the impact on client performance.

Some performance impact is unavoidable with off-channel scanning. Multi-vendor lab testing recently found that when using scanning APs for both client service and off-channel monitoring, a throughput drop of up to 16% was possible when APs were required to spend significant time off-channel.

Are dedicated air monitors necessary? Although Aruba leaves this choice up to the customer, we highly recommend their use. The following sections detail some of the benefits of monitoring with dedicated devices.

Security

Dedicated AMs provide a number of security-related enhancements over scanning APs with multiple responsibilities.

Rogue Access Points

A rogue access point is an AP not sanctioned or authorized by network administrators. Typically, rogue APs are connected to a network by well-intentioned employees unaware of the security risks they cause. Enhanced security monitoring enables faster response to these security breaches by performing the following functions:

Detection

A dedicated AM will recognize a rogue AP within seconds, while a scanning AP may take minutes to find a rogue operating on a different channel – or it may never discover the rogue at all. This is because a lightly-used rogue AP may not generate traffic during the brief period an AP is monitoring that channel.

Classification

Rogue classification is the ability determine whether a rogue AP is connected to the wired network, and, if so, where it is connected. Aruba invented this concept, which uses network-wide data sampling along with Aruba's patent-pending automatic classification algorithms. The longer the AP or AM can spend on a channel sampling data, the more accurate the classification algorithm will be - and in turn the accuracy and timeliness of the results. Scanning APs that are servicing clients can also classify rogue APs, but they are much slower because they must dedicate time to the clients.

Containment

Once a rogue AP has been detected and classified, Aruba can automatically disable it using a low-bandwidth wired and wireless denial of service (DoS) attack. For the wireless DoS attack, the transmitting device must be on the same channel as the rogue AP and must stay on that channel to continue the containment action. While a scanning AP can go off-channel to perform rogue AP containment, throughput can be severely impacted if the rogue is on a different channel than the local. Dedicated air monitors provide a more effective way to perform rogue AP containment without negatively impacting the performance of the wireless network.

Ad-hoc Network Detection and Containment

The issues related to ad-hoc network detection and containment are the same as those relating to rogue AP detection and containment. Aruba was the first vendor to automatically detect, classify, and disable ad-hoc networks. The challenge, however, is that ad-hoc networks typically generate much less traffic than rogue APs. For this reason, there is a low probability that a scanning AP will find an ad-hoc network during its brief scan interval. With dedicated AMs, ad-hoc networks are quickly detected and disabled.

"Honeypot" AP Protection

In a "honeypot" attack, an intruder sets up an AP within range of a wireless network (often outside a building) and begins advertising the enterprise network's ESSID. Unsuspecting client devices associate to the intruder's AP, believing they are roaming to a valid AP. The attacker then gets direct L2 access to the client devices, enabling a number of additional attacks such as man-in-the-middle, ARP poisoning, DHCP/DNS hijacking, and injection of network worms and viruses.

To avoid detection, honeypot APs often use non-standard channels, such as channel 2 in an 802.11b/g network. Dedicated AMs immediately detect these devices, recognize that they are using a reserved enterprise ESSID, and disable the devices with an over-the-air DoS attack. The AMs remain on-channel with the intruding AP to ensure that no stations can associate to it. A scanning AP that is servicing clients can perform this action, but often experiences two critical problems: 1) delays in discovering the honeypot, and 2) degraded network performance as a result of the time spent off-channel.

Wireless Bridge Detection

Typically used to interconnect buildings, wireless bridges are a favorite tool of corporate spies. Placed under a conference room table or in a lobby, a bridge can be used to quietly connect into the corporate network. Because of their directed signal and their lack of beacons, they are difficult to detect. Scanning APs monitoring a channel for a short

interval may not discover the bridge, while a dedicated AM will find it immediately. Once a bridge is located, the IT staff can easily remove it.

Spatial Diversity of Reporting Points

More sources of data yield greater coverage and accuracy. An attacking device could be located in such a way that infrastructure APs couldn't hear it, but client devices could. The best way to solve this problem is with dense deployments of APs, as detailed in Aruba's Wireless Grid design, and a small number of AMs with high-gain antennas.

RF Management and Troubleshooting

Remote Packet Capture

Packet capture, or "sniffing," enables network managers to troubleshoot the network. An AP can perform packet capture on its configured channel, but performing this function on another channel affects client throughput. A dedicated AM solves this problem because it can capture traffic on any channel.

In addition, an AP can capture received data, but cannot listen to itself while transmitting. If the transmit circuitry in an AP were to partially fail, packet capture data from the AP itself could be misleading. Dedicated AMs provide an "independent 3rd-party" view of network traffic and a client-perspective view of a conversation rather than the AP's view.

Statistics Monitoring

Statistics monitoring is another valuable troubleshooting tool. Aruba devices collect a wealth of statistical information about the RF environment such as interference levels, number of devices, top talkers, frame retry rates, RSSI, devices out of range, and frame type/size distribution. APs provide this functionality for their own channels and offer a limited view of what is happening on other channels. Dedicated AMs scan channels with a much longer dwell time and provide a more accurate picture of what is happening on each channel.

Spatial Diversity of Reporting Points

Like security monitoring, more sources of data provide greater accuracy. A source of interference could be located such that infrastructure APs couldn't hear it, but client devices could. Denser deployment of monitoring devices provides greater odds of finding the problem.

High Availability

Fault Tolerance

Dedicated AMs increase reliability of the network by acting as redundant APs. In the event of an AP failure, an AM can be set to notice the failure, automatically convert itself into an AP, and alert the network manager without noticeable downtime.

Future Capacity

Dedicated AMs provide extra capacity for:

- *On-demand overflow coverage. AMs, sensing high traffic in the network, can be set up to notice the traffic and convert themselves into APs for on-demand overflow coverage during high demand situations like a large company meeting.*
- *On-demand outdoor wireless access. AMs placed to protect the perimeter of a building can be converted into APs to provide temporary outdoor coverage.*
- *Temporary growth coverage. AMs can be automatically converted into APs to provide cushion during growth.*

About Aruba Networks, Inc.

Aruba securely delivers the enterprise network to users, wherever they work or roam, with user-centric networks that significantly expand the reach of traditional port-centric networks. User-centric 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 follow-me 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.

TB_AMS_US_071217

1322 Crossman Ave. Sunnyvale, CA 94089-1113
Tel. +1.408.227.4500 | Fax. +1.408.227.4550 | info@arubanetworks.com
http://www.arubanetworks.com