Arista WIPS and the Marker Packet™

Introduction

There are a number of wireless threat vectors that network managers need to defend against. One of the more common types of threats to WLANs is from rogue APs. An analysis of Wireless Intrusion Prevention Systems (WIPS) that are available today reveals that many require a high level of administration and often provide less-than-trustworthy rogue AP detection. Organizations that depend on these less capable systems often have a false sense of security as their networks are in fact vulnerable to breaches via rogue APs. Less capable WIPS are also prone to raising false alarms, which can lead administrators to ignore alerts or turn notifications off altogether, leaving their organizations unprotected. In contrast to competing WIPS offerings, the industry leading solution from Arista Networks requires a minimal amount of management overhead while providing reliable rogue AP detection and prevention. This paper shows how Arista WIPS with its patented Marker Packet™ auto-classification technology compares to rogue AP detection techniques used by competitors.

Rogue APs can be defined as any unauthorized AP that is connected to an authorized network. Rogue APs are a serious threat to enterprise networks as they allow unauthorized wireless access to the private network and data, as shown in the diagram below. Rogue APs can appear on the enterprise network either due to naïve acts of employees or due to malicious attempts by insiders. A naïve way to detect rogue APs in the LAN is to declare every AP seen in the air that does not belong to the list of authorized APs as rogue. In fact, many WIPS available in the market will actually follow this approach, by default. Such an approach has the following disadvantages:

- False alarms: A security alert would be raised even if the non-authorized AP seen in the air but not actually connected to the monitored wired network and as such it does not pose any security threat
- Manual intervention: The system administrator has to manually examine the non-authorized APs visible in the air to decide which of them are actual rogue APs and which of them are external APs (i.e. neighbor APs).

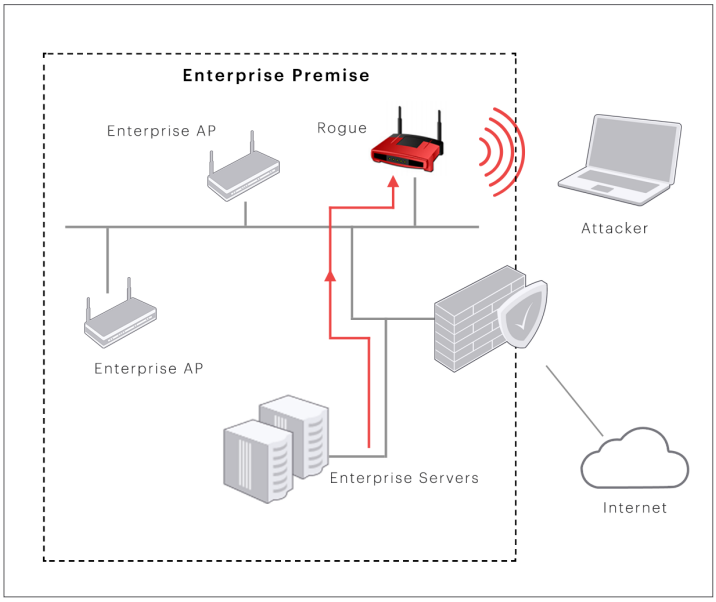


Figure 1: Intrusion into the enterprise network through rogue AP

- No automatic instantaneous prevention: Since it is highly undesirable to block neighbors' APs accidentally or indiscriminately, instantaneous and automatic blocking of rogue APs is not possible with such an approach.

AP Auto-Classification

AP auto-classification is the positive segregation of visible APs into three categories:

- Authorized – Managed APs in the enterprise wired network, which the administrator knows about.
- External – Unmanaged APs in the wireless neighborhood, which are not connected to the monitored enterprise wired network
- Rogue – Unauthorized APs installed in the enterprise wired network without administrator knowledge.

Arista WIPS enables automatic classification as described above, which in turn facilitates automatic enforcement of the Wi-Fi security policy.

Challenges of traditional techniques

Many WIPS attempt to classify APs based on user-configured classification signatures. A myriad of AP properties such as SSID, vendor, power level, encryption settings, channels are used to define classification signatures. Network connectivity of the AP to the enterprise network may or may not even be a factor in classification rules. This approach has several disadvantages:

- Overhead of configuring and maintaining signatures: Significant configuration overhead is involved in defining classification signatures. On top of that, the signatures need to be regularly updated, e.g., what happens when known friendly neighborhood WLAN configurations are changed to use a different SSID?
- Ongoing manual intervention: Wireless configurations of newly-detected APs may not exactly match the defined signatures, in which case, manual intervention is required to classify the newly detected APs.
- Missed threats: This approach often misses genuine threats. For example, a classification signature such as: if "SSID = attwifi AND signal strength = Low; then classify as known neighbor AP"; will be evaded by a rogue AP with low transmit power whose SSID is configured to be attwifi.

Is there a more efficient and reliable way to classify APs?

The most natural and elegant way to classify APs is via network connectivity detection. This type of autoclassification does not require unreliable or unmanageable classification signatures based on SSID, vendor, power level, encryption setting or channel; all it needs is

reliable network connectivity and access to the desired VLANs. Accurate, dependable AP autoclassification is a key to a "usable" Wireless Intrusion Prevention System! Arista Networks is the ONLY vendor that provides built-in AP network connectivity based auto-classification. This is made possible by Arista's unique Marker Packet technology, which accurately detects network connectivity of all types of APs. Arista is the inventor and pioneer of the Marker Packet™, and Arista holds several patents on these techniques.

Finding Rogue APs

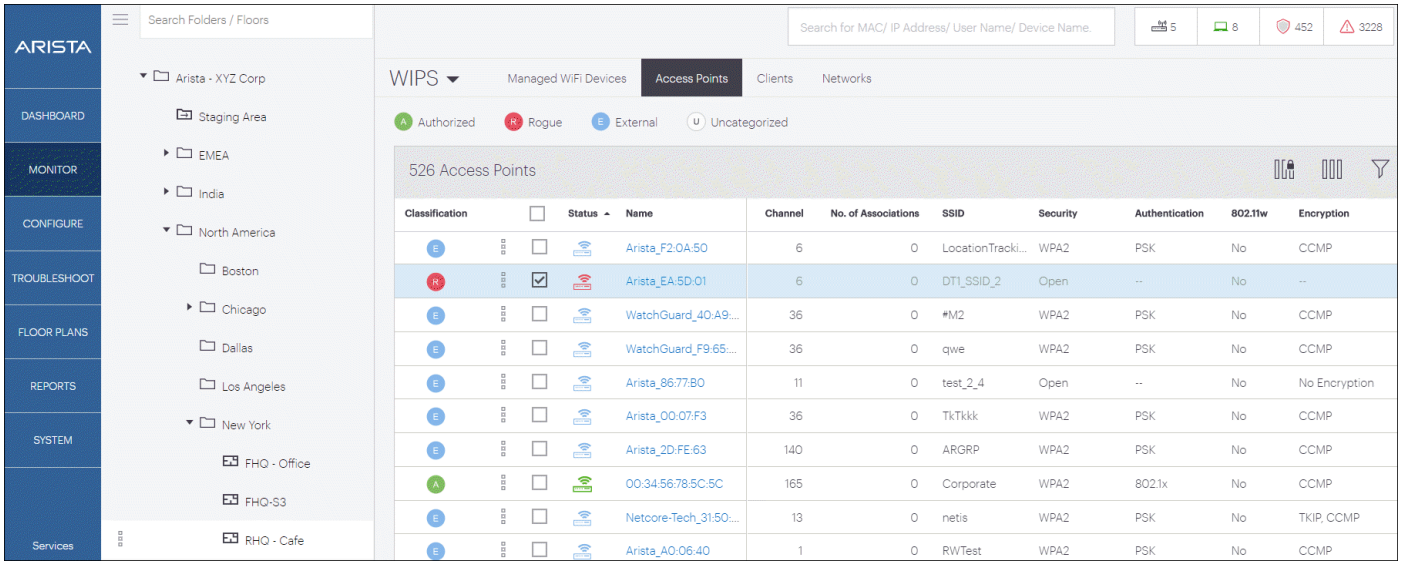
All WIPS available in the market provide some level of AP network connectivity detection. It can be just a "best effort" parameter that is used in user-configured classification signatures, or it can be a built-in foundational technique that delivers reliable AP auto-classification.

Threat Type #1: Rogue Bridging APs

These types of rogue APs relay all packets that arrive on their wired interface to the wireless network at layer-2 and vice versa.

CAM Table Lookup: This technique compares MAC addresses of wireless devices visible in the air with MAC addresses registered at the ports of managed switches in the wired network. If a common MAC address is found between the wireless and the wired sides, it is determined that the device with that MAC address is connected to the monitored wired network. In case of Bridging APs, detection must wait until a client connects to the AP. After the client connects, its MAC address gets registered in the switch port where the AP is connected. Collection of MAC addresses registered at the ports of managed switches in the network is performed by polling the CAM tables of each switch over SNMP. This suffers from several disadvantages:

- This technique is intrusive on enterprise switching infrastructure. It requires maintenance of switch credentials in the WIPS so that it can poll CAM tables of the switches. It also suffers from interoperability problems with switches from different vendors.
- CAM table polling of all managed switches in the network is a resource intensive and time consuming task, especially in large enterprise networks with hundreds of switches. Thus, in large networks, network connectivity detection with this approach can only happen infrequently.
- There is a "luck" factor involved in detection. A client's MAC entry disappears from the CAM table after the client becomes inactive, so when CAM table polling occurs (this is typically scheduled at periodic intervals) the technique is only successful while the client is actually connected to the rogue AP.



Passive MAC Correlation

This method attempts to overcome CAM table lookup disadvantages. In this technique, the WIPS AP passively listens on its wire-side interface for MAC addresses that are active on the subnet. MAC addresses discovered by this technique are used for wired/wireless MAC address correlation. However, even this approach suffers from an issue wherein APs not connected to the monitored network, such as neighbor APs, can appear connected to the monitored wired network. This occurs when clients flip between these APs.

Arista's Approach: Wire-side Packet Injection

This technique involves injecting Marker Packets™ into the wired network from the wired side of a WIPS AP. These packets are relayed to the wireless side by APs that are connected to the monitored wired network, which are then detectedover the air by the wireless side of the WIPS AP. The AP may be placed in a subnet or on a trunk port of a managed switch for multiple subnets.

Advantages of this technique are:

- It does not require intrusive interaction with the switches in the network
- It does not require any initial or ongoing configuration to be operational
- This technique quickly detects the APs' connectivity irrespective of the size of the network, since it operates on each local subnet simultaneously
- The volume of traffic generated due to packet injection is negligible (less than 0.1% of the LAN port capacity).
- This technique is free from false alarms in that it never marks rogue APs as external APs; nor does it mark external APs as rogues.

Threat Type #2: Rogue NAT APs These types of rogue APs are layer-3 routing APs that behave like a NAT device on the wireless side.

Wireless-side Tracing In this technique, after a WIPS AP detects an AP in the air, it will try to actively connect to the AP on the wireless side. The WIPS AP then either pings something on the wired network through the potential rogue AP or sends a packet to a known host on the wireside of the network, to try to detect if the AP is connected to the enterprise wired network.

This approach of actively connecting to the AP has limitations, in that it takes a fair amount of time for the AP to connect to the AP by completing a L2 and L3 connection (for

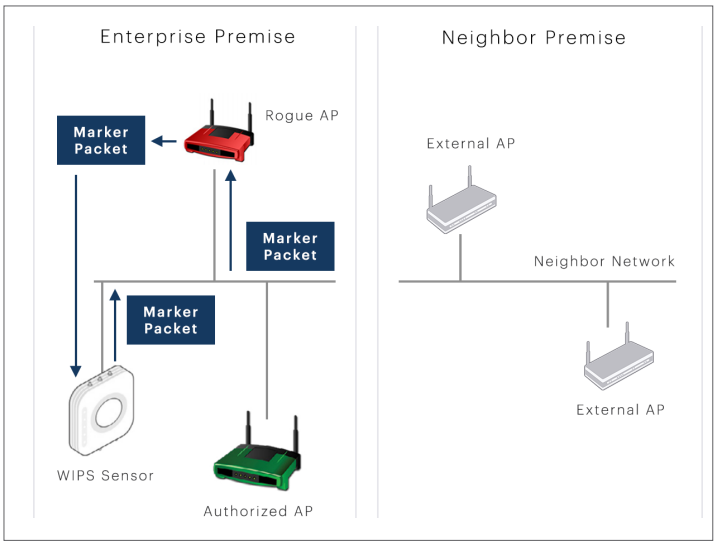


Figure 2: Arista's wire-side Marker Packets determining rogue AP network connectivity

example, up to 5 seconds). During this time, the WIPS AP needs to be locked on the AP's channel and cannot perform its scanning function. Thus, in the presence of large number of potential rogue APs visible to the WIPS AP, this technique can only be executed infrequently, thereby causing large latency in the detection of AP connectivity.

Moreover, this technique fails to detect rogue APs which may have special settings, such as an authorized client MAC address list on the wireless interface, which can prevent the WIPS AP from actively associating to the potential rogue AP.

Arista's Approach: Wireless-side Packet Injection

Once the WIPS AP sees a client associated with an AP, it sends packets with unique identifier (Marker Packets™) from the wireless side of the potential rogue AP directed towards the IP addresses of a known wire-side host. These packets are piggy backed on the client's link with the potential rogue AP. If any of these packets are received at the target host, the AP is confirmed to be connected to the monitored wired network

High Maintenance and Unreliable vs. Automatic and Trustworthy

This paper has compared different approaches to WIPS. As was discussed, all WIPS are not equally capable of distinguishing where APs reside. The Arista WIPS approach -- powered by Marker Packet™ -- offers the highest level of security with the minimal amount of maintenance. Accurate rogue AP detection is just one step to ensure network security, but a WIPS will need to get this part right before prevention measurescan be taken. Arista's WIPS includes a full complement of detection and prevention techniques. Arista's WIPS can reliably and automatically detect and prevent treats that could expose your organization's data and reputation.

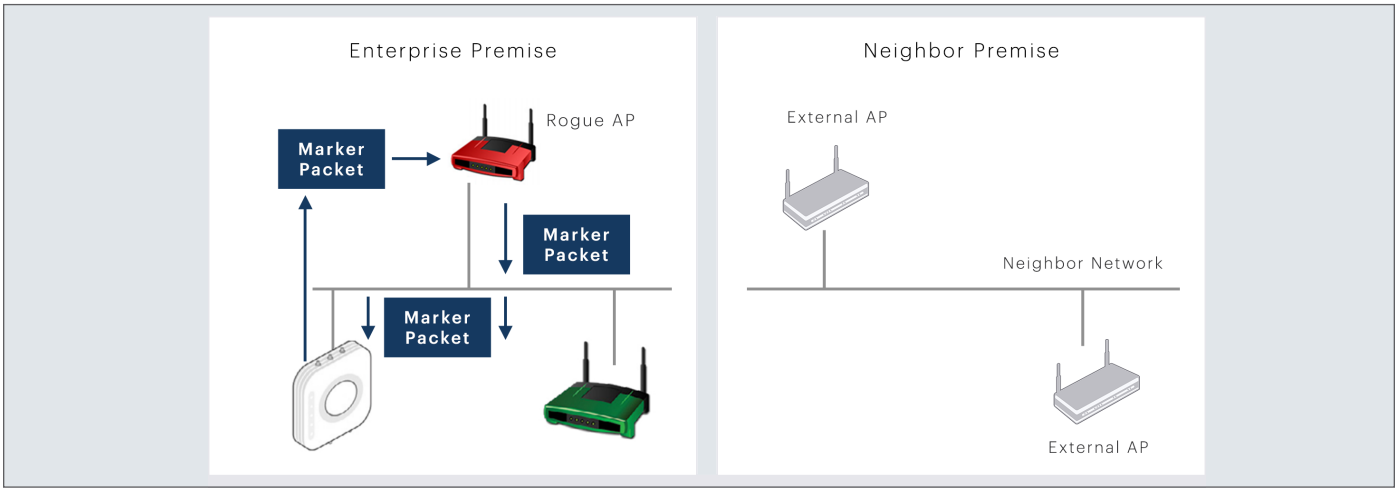


Figure 3: Arista's wireless-side Marker Packets determining rogue AP network connectivity

	Marker Packet	Signature Based	CAM Table Lookup	Passive MAC	Wire-side Tracking
Speed	Fast	Slow	Slow	Slow	Slow
Reliability	High	Low	Low	Low	Low
Scalability	High	Low	Low	Low	Low
Management Overhead	Low	High	High	High	Low

Table 1: Comparison of Rogue AP Detection Techniques

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062