# Review of Detection, Classification, and Prevention Techniques in WIPS

Synopsis

This paper provides information on multiple common security threats to the enterprise network from WiFi and various threat detection, classification, and prevention techniques used by the Wireless Intrusion Detection/Prevention Systems (WIPS). This paper focuses on threats related to Rogue access points (APs), client misassociations and Honeypot APs, Rogue clients, unapproved personal smartphones and tablets, ad-hoc connections, denial of service (DoS) attacks, reconnaissance, cracking, and spoofing.

ROGUE APs

Unauthorized access points (APs) connected to the enterprise wired network are considered Rogue APs. Rogue APs are a serious threat to the enterprise network as they allow unauthorized wireless access to the private wired network. Rogue APs can appear on the enterprise network either due to naïve acts of employees or due to malicious attempts of 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 WIDS/WIPS available in the market will actually follow this approach, by default. Such an approach has the following disadvantages:

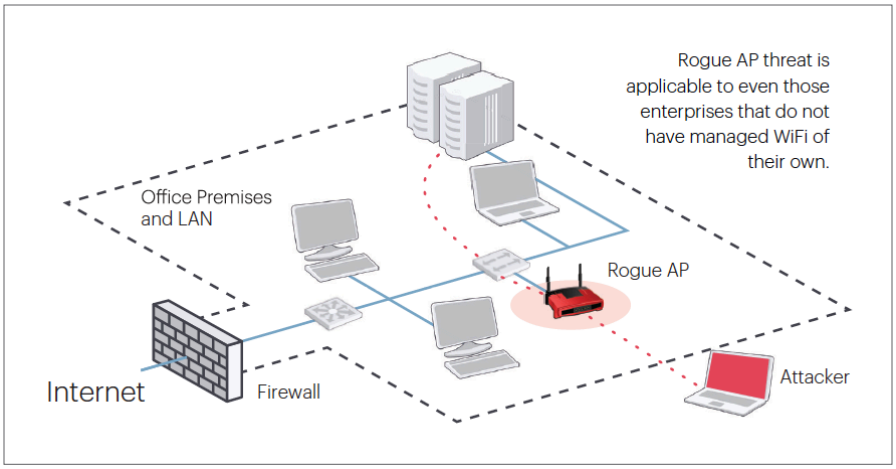



Figure 1: Intrusion into the Enterprise Wired Network through Rogue AP

1. False alarms: A security alert would be raised even if the non-Authorized AP seen in the air is not connected to the monitored wired network and does not pose any security threat.

2. Manual intervention: The system administrator has to manually examine the non-Authorized APs visible in the air to decide which of them are genuine Rogue APs and which of them are External APs.

3. No automatic instantaneous prevention: Since it is undesirable to block neighbors' APs accidentally or indiscriminately, instantaneous and automatic blocking of Rogue APs is not possible in such an approach. A solution to the above stated problems is AP auto-classification.

What is AP Auto-Classification?

Positively segregating the APs visible in the air 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 (neighborhood APs).

• ROGUE: Unmanaged APs installed in the enterprise wired network without administrator knowledge. If the APs can be automatically classified as above, it facilitates automatic enforcement of the WiFi security policy as shown below. Reviewed below are the techniques for AP auto-classification that are prevalent in different WIPS available in the market today.

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

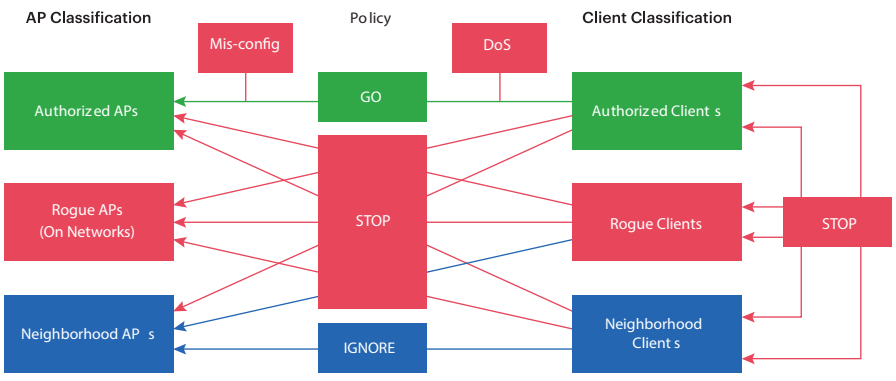



Figure 2: WiFi Security Policy Enforcement in WIPS

1. Overhead of configuring and maintaining auto-classification signatures: Significant configuration overhead is involved in defining auto-classification signatures. On top of that, the signatures need to be regularly updated, e.g., what happens when a known friendly neighborhood WLAN configuration is changed to use a different SSID?
2. 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.
3. Missed threats: This approach often misses genuine threats. For example, the autoclassification signature such as "SSID = GoogleWiFi AND signal strength = Low, then classify as Known Neighbor AP"; will be evaded by a miniature Rogue AP (with low transmit power) whose SSID is configured to be GoogleWiFi.

B. AP network connectivity detection based auto-classification:
The most natural and fundamental way to auto-classify APs is via their network connectivity detection. The network connectivity detection based auto-classification does not require flaky auto-classification signatures based on SSID, vendor, power level, encryption setting, channel etc. It however requires robust network connectivity detectors in the WIPS.

AP Network Connectivity Detection Techniques:
All WIPS available in the market provide some level of AP network connectivity detection. It can either be just a "best effort" parameter to be used in user-configured auto-classification signatures, or it can be a built-in core parameter for the AP auto-classification. Reviewed below are different AP network connectivity detection methods available in different WIPS products.

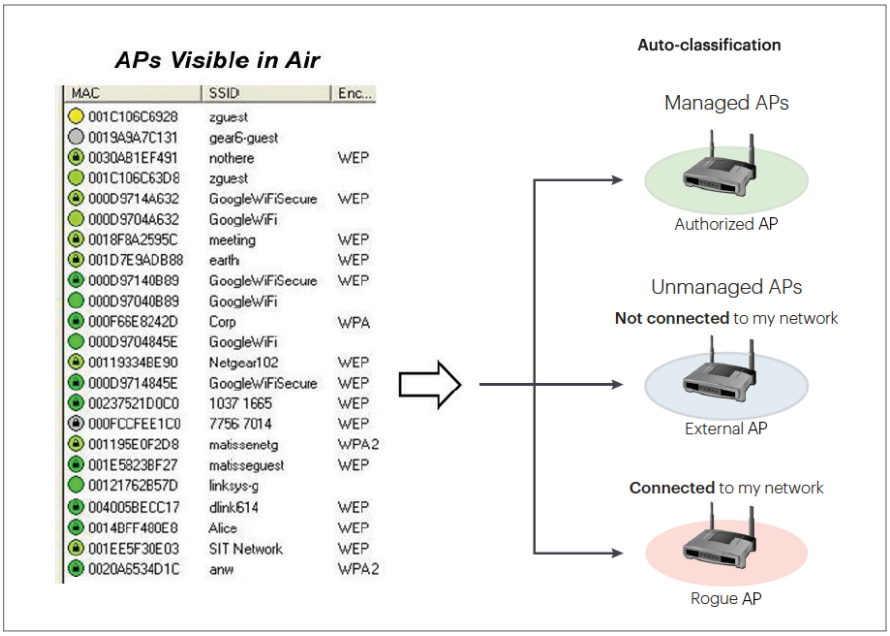



Figure 3: AP Network Connectivity based Auto-classification

1. Bridging APs: These APs relay all packets that arrive on their wired interface to the wireless network at layer-2 and vice versa.

a. Wire-side Packet Injection: Arista's Sleek Technique
This technique involves injecting packets with a unique identifier (Marker Packets™) into the wired network from the wired side of a WIPS sensor. These packets are relayed to the wireless side by the APs that are connected to the monitored wired network, which can then be detected over the air by the wireless side of the WIPS sensor. The sensor may be placed in a subnet or on a trunk port of a managed switch for multiple subnet injection (upto 100 subnets from single sensor).

This technique works on both nonencrypting and encrypting Bridging APs. Advantages of this technique are:

- It does not require intrusive interaction with the switches in the network (such as polling CAM tables of switches as required in other approaches).
- It does not require any initial or ongoing configuration to be operational (in contrast to CAM table lookup based approach, which requires configuration and maintenance of switch credentials in the WIPS).
- This technique quickly detects the APs' connectivity irrespective of the size of the network, since it operates on each subnet locally. This is in contrast to other techniques, notably CAM table lookup, whose performance degrades as the number of switches to be polled grows.
- The volume of traffic generated due to packet injection is negligible (less than 0.1% of the LAN port capacity).
- This technique is completely free from false alarms, i.e., on both sides. It never marks Rogue AP as External nor marks External AP as Rogue.

b. CAM Table Lookup: Conventional Inefficient Technique

This technique involves comparing MAC addresses of the wireless devices visible in the air with the MAC addresses registered at the ports of the managed switches in the wired network. If a common MAC address is found between the wireless and the wired sides, inference is drawn that the device with that MAC address is connected to the monitored wired network. In case of Bridging APs, the detection has to wait until some client connects to the AP. After the client connects to the AP, its MAC address gets registered in the switch port where the AP is connected. Collection of the MAC addresses registered at the ports of the managed switches in the network is performed by polling the CAM tables of the switches over SNMP. This is an old technique, which suffers from several disadvantages as follows:

- This technique is intrusive into the enterprise switching infrastructure. It also requires maintenance of switch credentials in the WIPS so that the WIPS can poll the CAM tables of the switches. It also suffers from interoperability problems with the switches from different vendors.
- The CAM table polling of all the managed switches in the network is an expensive task, especially in large enterprise networks with 100's of switches. Thus, in large networks, network connectivity detection with this approach can only happen infrequently.
- There is also a "luck" factor involved in detection. This is because a client's MAC entry disappears from the CAM table after the client becomes inactive. So, if the CAM table polling of the switch happens (this is typically scheduled at periodic intervals) while the client is actually connected to the Rogue AP, only then the AP's network connectivity detection will succeed in this approach.

b. Passive MAC Correlation: Weak Attempt to Overcome CAM Table Lookup Disadvantages

In this technique, instead of the WIPS server polling the switch CAM tables for wire-side MAC addresses, the WIPS sensor passively listens on its wire-side interface for the MAC addresses, which are active on the subnet. The MAC addresses so discovered are used for wired/ wireless MAC address correlation. Many practical implementations of this approach suffer from the problem that the network unconnected AP (neighbor AP) shows up as connected to the monitored wired network. This is a statistical phenomenon, which manifests when clients flap association between the network connected AP and the network unconnected AP.

2. NAT APs (wireless routers) with Encryption OFF

These are layer-3 routing APs with encryption turned off that behave like a NAT device on the wireless side.

a. Wireless-side Packet Injection: Arista's Sleek Technique

Once the WIPS sensor sees a client associated to an AP, it sends packets with unique identifier (Marker Packets™) from the wireless side of the sensor directed towards the IP addresses of the known wire-side host. These packets are piggy backed on the client's link with the AP. If any of these packets is received at the target host, the AP is confirmed to be connected to the monitored wired network. In addition to this, Arista system also performs MAC adjacency test on such APs for speedy classification (see next section for the description of the MAC adjacency test).

However, MAC adjacency testing alone is not sufficient since it does not cover NAT APs, which do not exhibit relation between their wired and wireless MAC addresses, such as WiFi routers with cloned WAN addresses, USB APs on employee laptops etc.

b. Wireless-side Tracing: Inefficient Approach of Actively Connecting to APs from Wireless Side

In this technique, after a WIPS sensor detects an AP in the air, it will try to actively connect to the AP on the wireless side (in contrast to Arista's piggy backing approach). The sensor then either pings something on the wired network through the AP or sends a packet to a known host on the wire-side 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 the limitation that it takes a fair amount of time for the sensor to connect to the AP by completing L2 and L3 connection (for example, upto 5 seconds).

During this time, the sensor needs to be locked on the AP's channel and cannot do the scanning function. Thus in the presence of large number of APs visible to the sensor, this technique has to be executed only infrequently, thereby causing large latency in the detection of connectivity.

Moreover, this technique fails to detect Rogue APs, which may have special settings on the wireless interface, which prevent the sensor from actively associating to the AP.

3. NAT APs (wireless routers) with Encryption ON
These APs with encryption turned on behave like a NAT device on the wireless side. In some cases, they also have a 4 or 8-port switch in addition to the wired and wireless interfaces behind the NAT.

a. MAC Address Adjacency Test: Arista Technique with Proper Workflow
This technique looks for a MAC address on the wired network that is in numerical vicinity of any of the detected wireless MAC addresses. If such an address is found, the corresponding AP is declared to be connected to the network. This technique relies on the fact that, in many NAT APs, the BSSID and the wire-side (WAN-side) MAC addresses are within +/- 1 of each other.

Though many NAT APs will satisfy this MAC address adjacency criteria, there are many which do not. In addition, all NAT APs provide a configuration setting to clone their wired (WAN) MAC address to any MAC address that the user chooses. This option is provided so that users can change APs at their homes without having to register the new MAC address with the ISP. In this case, this technique will not detect such APs as connected to the network when indeed they are connected.

MAC adjacency testing requires a proper workflow. Without proper workflow, it can be deceptive. Suppose there are 100 APs detected in the air and 45 of these are Authorized APs. Suppose there are 3 NAT APs with Encryption ON among the remaining 55 as follows.

- AP1: Rogue without cloned wire-side MAC address (passes MAC adjacency test)
- AP2: Rogue with cloned wire-side MAC address (fails MAC adjacency test)
- AP3: Neighbor's AP.

Improper Workflow:
Tag 45 AP's as Authorized. Tag AP1 as Rogue and remaining 54 as External. Note there is one actual Rogue among those 54, which is missed. Indeed many WIPS follow this workflow.

Proper Arista Workflow:
Tag 45 AP's as Authorized. Tag AP1 as Rogue, AP2 as Indeterminate and remaining 53 as External. In this case, the administrator has to manually examine only one AP that is tagged indeterminate – a huge saving of manual effort and no security lapse!

Rogue AP Prevention Techniques:
When a Rogue AP is detected, communication of wireless clients with the enterprise network through the Rogue AP must be blocked to avoid security breaches through it.

1. Over the Air Prevention: The WIPS sensor sends spoofed "deauthentication" packets over the wireless medium, which prevents any clients from associating to the Rogue AP. Both broadcast and unicast "deauthentication" packets are transmitted by the sensor. These prevention packets take up negligible wireless bandwidth (few Kbps).

2. Wire-side Prevention: Communication of the Rogue APs with the network can also be blocked from the wire-side of the network. The wire-side blocking helps contain Rogue APs operating on illegal channels (where sensors do not transmit being legal devices) and Rogue APs which use deauthentication resistant protocols such as 802.11w.

a. Wire-side ARP Poisoning: Arista's Overlay Technique
The WIPS sensor transmits selective ARP poisoning packets from its wire-side interface, to ensure that wireless clients cannot connect to the wired enterprise network via the Rogue AP. These packets do not disturb any legitimate communication on the subnet.

b. Switch Port Blocking: Network Intrusive and Risky Technique
This technique attempts to trace a switch port where the Rogue AP is connected and then turns that port off using SNMP SET. This technique is usually found in the systems which also use CAM table lookup for Rogue AP connectivity detection.

This technique has several disadvantages as follows:

- Switch port blocking is intrusive into the switching infrastructure. WIPS needs to be given WRITE access to the switches for this technique to work. This technique also entails overhead of maintaining credentials of switches in the WIPS. It also suffers from interoperability problems with the switches from different vendors.
- Practical implementations of the switch port blocking cannot always pinpoint the leaf port in the switch hierarchy This stands the risk of turning off a port in the upstream switch, thus causing disruption to the enterprise infrastructure.
- It is unscalable for large networks with 100's of switches.
- This technique is not self recovering. That is, switch port needs to be manually enabled after the Rogue AP is disconnected from the network.

AUTHORIZED CLIENT MISASSOCIATIONS AND HONEYPOT APs

Misassociation of the Authorized clients on the enterprise premises to neighborhood APs is a very common problem in most networks. It typically occurs due to the following reasons:

1. Misassociation can happen inadvertently if the client's wireless network profile contains commonly found SSIDs such as default SSID, hotspot SSIDs etc. These SSIDs get into the wireless profile on the client when the client connects to them. Once in the profile, the client continues to search for these SSIDs when the WiFi radio is turned on and will automatically connect to one if found.
2. Misassociation can also happen when the employees deliberately connect to the neighborhood APs. This could be to bypass the Internet usage controls (IM, webmail, objectionable content etc.) on the corporate firewall.
3. Malicious hackers are known to set up Honeypot APs (Evil Twin APs) with default SSIDs, hotspot SSIDs, and even corporate SSIDs outside of the buildings and watch a large number of clients automatically lured to them. These APs can then inflict a variety of attacks on the client such as port scanning to explore and exploit client vulnerabilities, password stealing by throwing the login page to the client over the misassociated wireless connection, and man-in-the-middle attack (Wi-Phishing). Client misassociations must be detected and effectively prevented!

Client Classification:

In order to prevent misassociations without disrupting friendly neighborhood communications, or in general, in order to enforce the WiFi security policy as shown in Figure 2, it is necessary to properly classify the clients as follows:

- AUTHORIZED – Managed clients in the monitored enterprise network. These are allowed to access the managed APs, but not allowed to access neighborhood APs.
- EXTERNAL – Unmanaged clients in the wireless neighborhood. These are not allowed to access the managed APs in the monitored enterprise network, but are allowed to access their own APs. For example, clients in the neighborhood premises accessing the APs in the neighborhood premises are External clients.
- ROGUE – Any clients intruding or providing path for intrusion into the monitored enterprise wired network.

One way to classify clients is to input the list of MAC addresses of Authorized clients in the WIPS. All clients outside of this list are then automatically classified as External, unless the client is found intruding into the enterprise wired network. If a client outside of the Authorized clients list is found intruding or providing path for intrusion into the enterprise wired network, it is classified as a Rogue client. Typical examples of Rogue clients are clients which bridge their wired interface connected to the enterprise wired network with the wireless interface, or clients which attempt connection to Rogue APs etc.

Not all network administrators necessarily have the list of Authorized clients' MAC addresses readily available with them. To address this scenario, Arista also provides client autoclassification, which can automatically identify Authorized clients using one or more of the following techniques:

i) analysis of client's wireless behavior, ii) wired/wireless client MAC correlation, and iii) presence of WiFi connection management agent (SpectraGuard SAFE) on the client.

Clients Misassociation and Honeypot AP Prevention Techniques:
As soon as an attempt of an Authorized client to connect to the neighborhood AP or the Honeypot AP is detected, the client must be blocked from getting into that connection. Such a technique has to work over the air. The sensor sends spoofed deauthentication packets over the wireless medium, which prevents the misbehaving client from getting into the undesirable connection. Unicast deauthentication packets are sent by the sensor in both directions (client to AP and AP to client) to break the undesirable connection. This way, other clients (External clients) connecting to those APs are not disturbed.

Multiple simultaneous prevention on multiple channels:
Each Arista sensor can prevent multiple undesirable connections on multiple channels, simultaneously. On any given channel, practically unlimited number of undesirable connections can be blocked. The uniqueness of Arista's over the air prevention comes from its ability to perform effective and simultaneous blocking of connections on multiple channels. This is made possible by Arista's optimized channel rotation technique, which prevents even the most aggressive misbehaving clients from getting in the undesirable connections.

Scanning with prevention: Arista sensor continues to scan for new threats while performing over the air prevention.

Prevention of association hopping clients (Multipots): In some cases, misbehaving client switches association between multiple APs so fast that the de-authenticaction technique is unable to chase the client in order to contain it. This typically happens if there are multiple neighborhood APs with identical SSIDs which attract the client. Some Honeypot AP tools (called Multipots) can also deliberately induce fast association switching in order to evade deauthentication based prevention. For such cases, Arista uses its patented over the air ARP poisoning prevention technique to block client misbehavior.

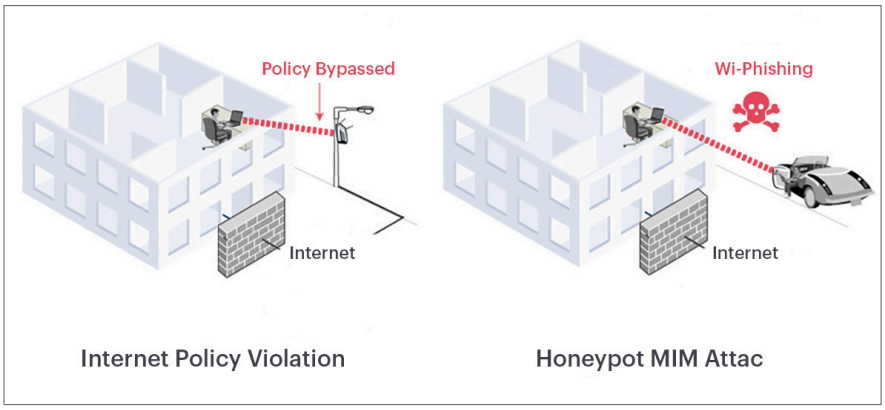



Figure 4: Client Misassociation Scenarios

PERSONAL SMARTPHONES AND TABLETS
With unprecedented proliferation of WiFi enabled smartphones and tablets, IT departments are under pressure to allow employee-owned devices onto their enterprise networks. This growing bring your own device (BYOD) trend is causing new security concerns for enterprise network and data security.

Using their personal smartphones and tablets, authorized users (e.g., employees, contractors) can now access the enterprise network over WiFi without the knowledge of security administrators. As shown in the example, to connect to a WPA2, 802.1x secured enterprise WiFi network, authorized users only need to use their enterprise login credentials (which will successfully authenticate them to the AAA server using PEAP). As a result, they can choose to ignore the step of configuring a certificate on their personal device and in turn, avoid any intervention from the network security staff.

Security threats from such uncontrolled access to enterprise networks can lead to inadvertent or malicious backdoors to the enterprise network, leakage of sensitive data, and exposure of IT infrastructure to malware.

Classification of Smart Devices and BYOD Policy Enforcement
To allow enterprises to address the challenge of BYOD and regain control of their network security, Arista has extended its Client Auto-Classification engine with a unique workflow (patent pending) to automatically detect smartphones and tablets; identify the make and type of smart devices, e.g., iPhone, iPad, Blackberry, and Android; and automatically block their access to enterprise network unless approved by the network security manager.

To minimize false alarms, Arista WIPS uses a combination of packet analysis techniques for fingerprinting smart devices, including use of different types of packets (e.g., DHCP, mDNS) observed over the air and on the wire. In addition to monitoring the smart devices that are trying to gain access to the enterprise network, organizations can also use Arista WIPS to enforce their BYOD policy, whether it is to automatically block or quarantine unapproved personal devices from connecting to the enterprise WiFi network or to restrict their access to a separate VLAN, for instance, via Guest WiFi.

SOFT APs

WiFi client devices (e.g., laptops, smartphones, tablets) that are converted into a WiFi AP by running a software utility or by adding a peripheral device such as a USB drive or modem are commonly termed as "Soft APs." Soft APs can pose both outside-in (Rogue APs) and inside-out (Mobile Hotspots) threats to enterprise networks.

Soft Rogue APs

Soft Rogue APs are client devices that are attached to the enterprise LAN and share the enterprise network access with other devices over WiFi. They create a WiFi backdoor into the enterprise network allowing intrusion by unauthorized devices. Common examples of Soft Rogue APs are:

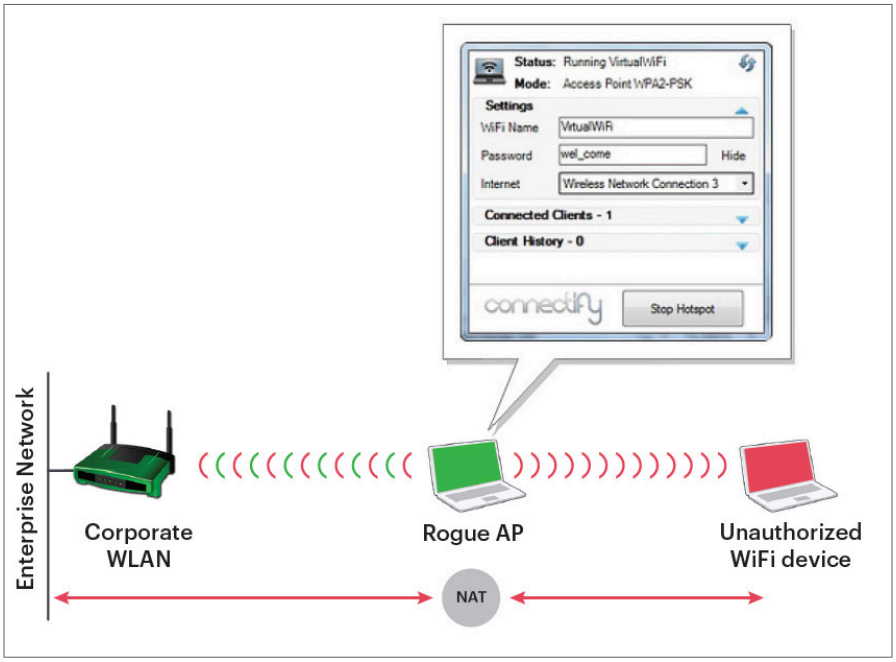
1. A laptop attached to the wired enterprise LAN and sharing the network access over WiFi by bridging its Ethernet and WiFi interfaces; or
2. A laptop that is associated with the corporate WLAN and sharing the network access via its virtual WiFi interface.

Soft Rogue AP Detection and Prevention

Soft Rogue APs cannot be detected by any wired side security solution such as a wired IDS/IPS or NAC because the Soft AP usually runs on an authorized client and they cannot differentiate between packets originating from that client versus those that the client (acting as an AP) is routing for other unauthorized WiFi clients. WIDS/ WIPS solutions that employ passive techniques such as CAM table lookups also fail to detect Soft Rogue APs attached to the wired LAN. Using patented Marker Packet techniques, Arista WIPS can accurately and instantly detect presence of Soft Rogue APs on the enterprise LAN. By using over-the-air and wire-side prevention techniques, Arista WIPS can completely block access to Soft Rogue APs.

Mobile WiFi Hotspots

Mobile WiFi Hotspots are client devices, usually smartphones, tablets or MiFi devices, that tether or bridge their 3G and WiFi




interfaces to share their 3G Internet access with other devices over WiFi. Tethering is readily available as a feature on most mobile operating systems making this a very common phenomenon. Mobile WiFi Hotspots can open a wireless backdoor through which corporate devices can bypass conventional enterprise security measures such as firewalls, to access prohibited content on the Internet. Hackers can also use Mobile WiFi Hotspots to create honeypots and launch a Wi-Phishing attack on corporate WiFi users.

Mobile Hotspot Detection and Prevention

With its techniques for fingerprinting smart devices, Arista WIPS can accurately detect when a Mobile WiFi Hotspot is present, and block authorized clients from misassociating to such Mobile WiFi Hotspots using over-the-air prevention methods.

Ad-hoc Connections

A peer-to-peer wireless client network is called an ad-hoc connection. Ad-hoc connections are undesirable for the following reasons:

- If Authorized clients form ad-hoc connections among themselves, proper security policies cannot be ensured for such connections due to lack of centralized security control on them. Wireless communication over such connections is vulnerable to eavesdropping and man-in-the-middle attacks.
- Malicious unauthorized devices in the neighborhood can lure Authorized clients into ad-hoc connection. Ad-hoc connection provides direct layer-2 access to the victim.

Ad-hoc Connection Prevention Techniques:

1. ARP Poisoning – Arista's Patented Technique: Many ad-hoc connections, most notably ad-hoc connections between Centrino Clients, do not respond to deauthentication prevention. Arista utilizes its patented ARP poisoning based prevention technique to block ad-hoc connections, which works even on Centrino clients.

2. Cell Splitting – Arista's Patent Pending Technique: ARP poisoning cannot be used

if the ad-hoc connection is encrypted. For encrypted ad-hoc connections, Arista uses cell splitting technique. In this technique, the sensor advertises a changed BSSID to introduce itself as man-in-the-middle of ad-hoc connections. In other words, it splits the ad-hoc cell into two cells anchored at the sensor. Once inserted, the sensor blocks packet transfer between the two cells thereby disrupting the ad-hoc connection.

3. Deauthentication – Conventional Technique Ineffective on Centrino Clients: Some vendors continue to use deauthentication technique on ad-hoc connections even if it does not work on Centrino ad-hoc connections. Centrino clients simply ignore deauthentication messages in ad-hoc mode.

4. Tarpitting – Inefficient Variant of Cell Splitting: Tarpitting is an inefficient variant of cell splitting, which requires the WIPS sensor to block on the channel where ad-hoc connection is prevented.

DoS ATTACKS

Shared nature of wireless medium, unlicensed frequency of operation, and fundamental characteristics of 802.11 protocol make DoS attacks inevitable for WiFI networks. The 802.11w standard and its precursor Cisco MFP address only few specific DoS attacks, and there are a number of DoS attacks which are not within their purview. As a result, for any WiFI network that needs to operate reliably, a wireless security system that provides good DoS management workflow will always be required. The common DoS attacks that need to be addressed are different types of connection floods, different types of forced disconnections, MAC layer jamming, and RF jamming.

Arista's Unique DoS Management Workflow:

1. DoS Attack Detection

Good DoS management workflow starts with accurate detection of DoS attacks while avoiding false alarms during normal wireless activity.

2. DoS Impact Reduction

Avoiding impact of DoS attacks altogether is not possible. The wireless security system should implement steps to reduce the impact of DoS attacks on legitimate communication whenever possible.

3. DoS Attacker Location Tracking

Physical remediation is necessary for DoS attacks. For this, the administrator needs to know the physical location of the DoS attacker device so that it can be removed from the wireless network. DoS attacker location tracking needs to work differently from location tracking of APs and clients. This is because many of the DoS attacks are launched by spoofing authorized devices' MAC addresses. Many others are launched using random MAC addresses. This makes it challenging to precisely measure RSSI of DoS attacker, without confusing it with authorized devices' RSSI or without getting lost in random MAC addresses.

RECONNAISSANCE, CRACKING, MAC SPOOFING

Reconnaissance:

Reconnaissance refers to activity (wardriving) in the wireless neighborhood targeted to discover weaknesses in the wireless security posture. Typical weaknesses that wardriver seeks to find are open managed APs, Rogue APs, clients seeking connections to default/hotspot SSIDs, clients seeking to connect to ad-hoc connections, so that penetration is possible through them. While some wardriving tools actively probe to find out these security weaknesses, others can operate completely passively. As a result, the best defense against wardriving is to ensure that the weaknesses in the network security posture are discovered and instantly blocked by the security monitoring system – which is the foundation of intrusion prevention. Arista WIPS provides full feature set to ensure this by monitoring and blocking managed AP misconfigurations, Rogue APs on network, client misassociations, Honeypot APs, ad-hoc connections as described above, and more as exhibited in the actual product. Nonetheless, for information purposes, Arista WIPS detects and reports use of active wardriving tools in the neighborhood which have distinct signatures.

Cracking:
Cracking refers to breaking the wireless encryption to recover keys, inject/modify data in transit etc. Arista WIPS provides detection of cracking activity as follows:

1. LEAP Crack: You need to detect LEAP cracking only if you use LEAP on your managed APs. LEAP is an antiquated (WEP contemporary) Cisco proprietary WiFI security protocol. Practically no authorized WLANs use LEAP today. Moreover, effective LEAP cracking can be done completely passively, which is fundamentally impossible to detect for any monitoring system. Hence, Arista does not support LEAP cracking detection.

2. WEP Crack: WEP cracking is relevant only for those deployments that use WEP on the managed APs. Detection is supported in Arista WIPS for active WEP cracking. Also, early warnings are given for vulnerabilities, which can be exploited by the passive WEP cracking (e.g., weak IVs).

3. WPA (TKIP) Crack: This is not a key recovery exploit. It is relevant only for those deployments, which use WPA (TKIP) on the managed APs. Arista WIPS detects the TKIP exploit. Overall, the best way to prevent cracking is to make a policy to use the strongest available encryption on managed APs, which today is WPA2/802.11i; and then have the WIPS continuously monitor that the managed APs indeed stick to this policy.

MAC Spoofing:
MAC spoofing refers to masquerading the legitimate device's wireless MAC address by an unscrupulous device. This is typically done, when the unscrupulous device wants its wireless activity to go unnoticed. To protect against the threat of MAC spoofing, Arista WIPS detects spoofing of the MAC address of authorized AP/client. The MAC spoofing detection is performed using combination of detection of time-based anomalies, protocol-based anomalies, and protocol implementation-based anomalies.

**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