4ipnet®

SIMPLIFIED AP MANAGEMENT

FEATURE GUIDE

SUMMARY OF FEATURES

- CENTRALIZED DISCOVERY
- REMOTE AP MANAGEMENT
- AUTOMATIC PROVISIONING
- FIRMWARE MANAGEMENT
- ROGUE AP DETECTION
- LOAD BALANCING
- THIRD PARTY AP MANGEMENT
- REAL-TIME STATUS CHANGE NOTIFICATION
- DETAILED STATUS MONITORING

INTRODUCTION

As smartphones, tablets, and other mobile devices become increasingly ubiquitous, we find ourselves in a new digital age where real-time information is readily accessible and people are more connected than ever. With the data deluge, simply providing wireless connectivity for these devices is no longer enough. Enterprises and organizations have to address a plethora of concerns from network performance to security and reliability, all of which can impact productivity and affect revenues. However, the bigger question is often how to deploy, maintain, and manage a network that can meet these requirements without creating sky-high expenses.

An essential component of every wireless network, wireless access points (AP) are devices that sit at the network edge and allow devices to connect to the network via wireless connections (i.e. Wi-Fi). Imagine when you use Wi-Fi at home or at a coffee shop – usually you are connecting to a network that only has one or two APs. On the other hand, when you connect to Wi-Fi at a public venue, a university, or a hotel, you are most likely connecting to a much larger network that has hundreds or even thousands of APs. The complexity and difficulty of network management for these two types of networks are on completely different levels, with the latter requiring additional tools and interfaces to keep deployment and maintenance efforts from spiraling out of control.

In this feature guide we will describe the synergy between 4ipnet access points and wireless LAN controllers, and how 4ipnet's AP management functions can help simplify the tasks and reduce the costs associated with WLAN deployment and maintenance.

CENTRALIZED DISCOVERY

When deploying a wireless network consisting of hundreds of access points, it would be very inefficient if network administrators had to individually add each AP to the wireless controller. Although the time required to access a single AP's interface and specify the controller's IP address is not too long, it becomes much more significant when multiplied by the total number of APs being deployed. If also taking into account the increased probability of error when performing a task repetitively, network administrators suddenly find themselves staring at a daunting task.

To ease network deployment, 4ipnet wireless LAN controllers have the capability of performing **CENTRALIZED DISCOVERY** of APs in the same Layer 2 subnet in their out of box default state. Upon successful discovery, administrators can then assign unique IP address and device names from the controller's interface. Even if the APs have already been individually pre-configured with unique IP addresses, the controller can still discover all of them by simply scanning a user-defined IP address range. This discovery mechanism greatly reduces initial configuration effort while providing a flexibility that caters to the different habits of each network administrator.

For larger networks, the subnet on which APs are located may be very large, resulting in long discovery scan times. By allowing background discovery, network administrators can perform other configuration changes and settings while the discovery process is running, minimizing thumb twiddling time and increasing efficiency.

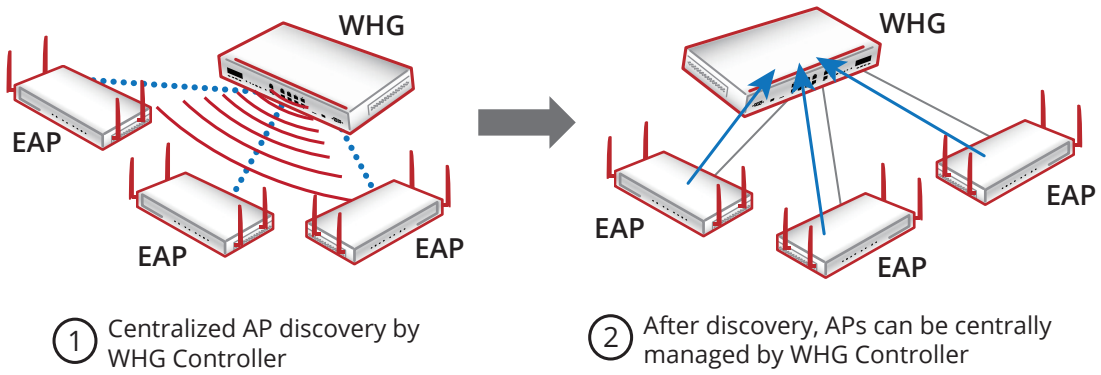

Figure 1: Centralized AP Discovery by WHG controller reduces initial deployment time and effort

REMOTE AP MANAGEMENT

For many enterprises and organizations, it is not uncommon to deploy access points on different subnets than the central controller due to security concerns or simply geographic location. For example, APs at an enterprise's headquarters and its branch or remote offices reside on completely different physical networks. In order to enforce unified network access policies for devices and users in these two separate locations, wireless LANs must offer a method to manage remote APs and tunnel their traffic back to the controller. Immediately, you will realize that this architecture presents a tradeoff between security and performance. From the security standpoint, having traffic go through the controller offers network administrators a method to directly examine and shape traffic, providing central visibility and management for incident response. However, tunneling traffic back to the controller also limits the maximum attainable network throughput when compared to a more distributed architecture.

4ipnet's **REMOTE AP MANAGEMENT** utilizes a centralized controller architecture and CAPWAP-based tunnels to provide enforcement of network access policies across different subnets (or through the Internet) without compromising overall network security. As there is no effective method for the controller to automatically

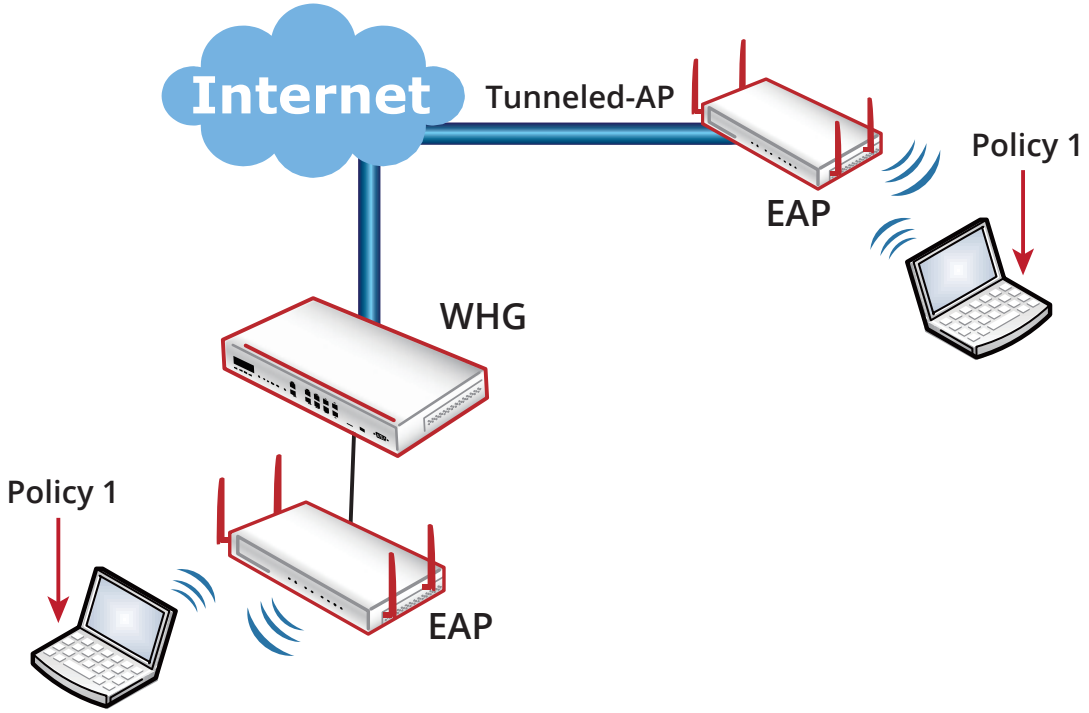

Figure 2: Tunneled management of remote APs allows organizations to apply the same user policies at headquarters and branch offices

discover a set of remote APs all residing on different subnets, 4ipnet's remote AP management allows each access point to individually specify the controller's network location to simplify the deployment process. Furthermore, multiple controllers can be specified, such that when the connection is disrupted access point(s) will automatically switch to one of the other listed controllers for failover purposes. Finally, administrators can define certificates as another security measure to ensure that APs attempting to connect to the controller are authorized.

Thus, while network elements (e.g. access points and controllers) may physically reside in separate and potentially very distant locations, 4ipnet overcomes the physical barrier by connecting them virtually, allowing network administrators to easily manage both the network and its users.

AUTOMATIC PROVISIONING

During large scale wireless network infrastructure deployments, it would be too time-consuming and impractical if each AP had to be configured individually. Furthermore, it would make even less sense when taking into account the fact that most APs in a deployment end up with essentially the same configuration, differing only in a few basic parameters such as operating frequency (channel), VLAN ID, or device name. This phenomena naturally begs the question: is there a way where we can just perform the configuration once for all APs?

Extending the notion that AP deployment and management must be straightforward and easy in order to increase efficiency and decrease total cost of ownership, 4ipnet wireless LAN controllers enable **AUTOMATIC PROVISIONING** with template-based AP configuration. By configuring an AP template, which includes basic AP system settings as well as fine-grained VAP (virtual access point) settings such as ESSID name and WPA/WPA2 security, network administrators can quickly complete the deployment of hundreds of access points. For settings that typically vary between each AP (e.g. operating channel, VLAN ID, etc.), the controller provides the flexibility to customize each one individually during the initial discovery process, eliminating redundant or unnecessary tasks.

During regular network operation, administrators may sometimes also need to change settings for security purposes, such as the WPA passphrase. Once again, this can be an extremely cumbersome task in deployments with large quantities of access points. However, with 4ipnet's solution administrators can simply modify the associated template and apply the changes directly to the associated APs. Therefore, the AP templates effectively reduce the difficulty of both initial deployment as well as in-operation configuration changes.

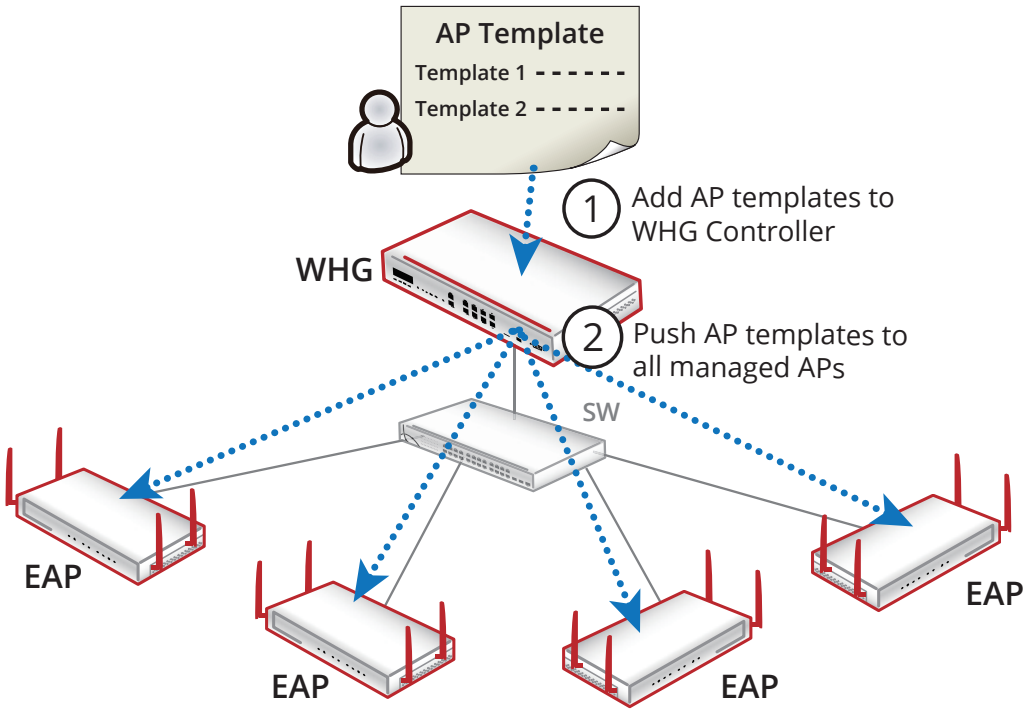

Figure 3: Automatic provisioning of managed APs via templates minimizes redundant configuration tasks

FIRMWARE MANAGEMENT

So far in this feature guide we have presented features that make deployment more intuitive and less time-consuming for an organization's IT staff. However, unlike the Wi-Fi that you use at home, operating a complex enterprise-grade wireless network does not simply end after deployment. Due to the more widespread Wi-Fi coverage required and the larger number of simultaneous users, network administrators continually face a variety of challenges, ranging from connectivity issues to performance complaints. Therefore, an effective WLAN solution not only decreases deployment efforts, but also streamlines the network's in-operation management, monitoring, and maintenance.

For any device that has a software system, whether it be a smartphone or laptop, there are almost always periodic software releases to address reported issues or provide new features. Wireless access points are no different, but installing updates for APs are much more difficult than updating your iPhone, especially when there are hundreds of them. Organizations need to be able to perform software updates without causing a major headache for IT personnel and inducing too much network downtime.

The centralized **FIRMWARE MANAGEMENT** on the 4ipnet wireless LAN controllers provide network administrators with an interface to directly perform firmware upgrade to all managed APs at the click of a button. Rather than having to individually upgrade each AP or issue a command/action per AP, the firmware can be stored directly on the controller and pushed down to multiple APs in batch. When the process is completed, the APs automatically resume operation to serve Wi-Fi clients, ensuring that network downtime is kept at a minimum.

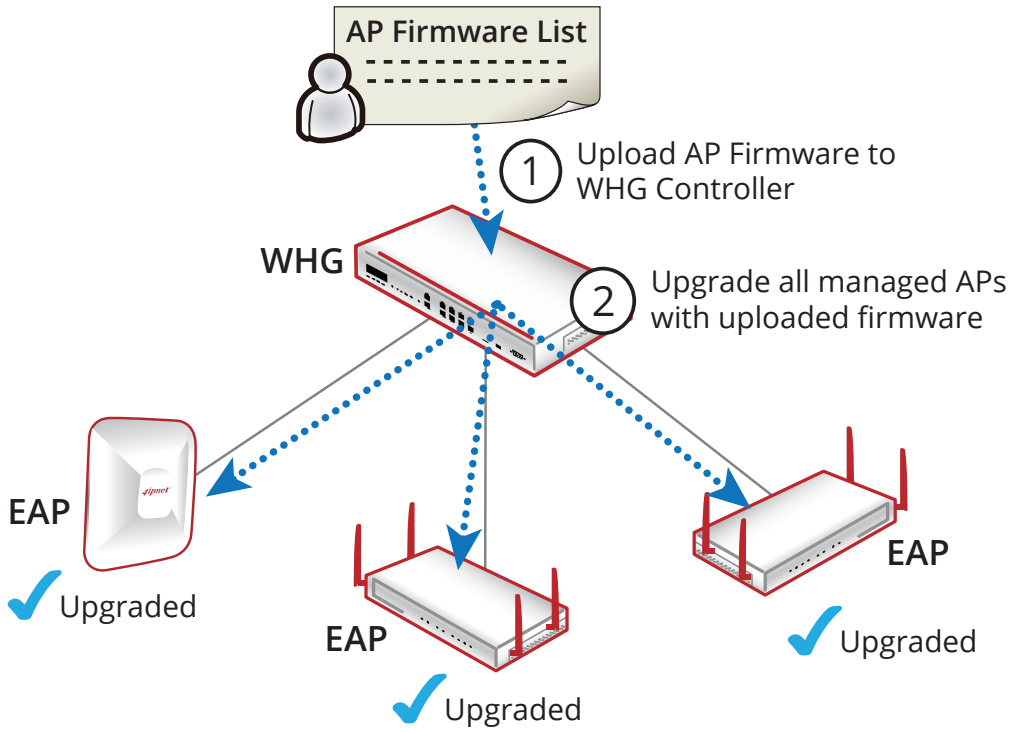

Figure 4: Managed APs can be upgraded in bulk during new software releases, eliminating the need to manually upgrade each AP

ROGUE AP DETECTION

The feature guide on Access Point Optimization emphasizes that one of the primary benefits of a managed wireless network is the ability to control the usage of each user in order to maintain network reliability and performance. However, one of the reasons why this is sometimes difficult is because users like to plug in their own access point to the network and gain unfettered Wi-Fi access. Even with tightened security measures for wired ports, network savvy users can still find alternative methods to install their own APs. For security-minded establishments such as enterprises and government organizations, this is a potential security risk that cannot be afforded. Furthermore, access points may interfere with the operation of mission-critical network applications and

ultimately result in lost productivity.

The **ROGUE AP DETECTION** feature on 4ipnet wireless LAN controllers allow network administrators to scan the surrounding wireless medium for rogue access points – access points that have not been authorized for use in the network. The flexibility in the design offers a configurable scanning interval for sensor APs (APs performing the scanning), while APs under management are automatically filtered from the scan results. Furthermore, the scan results by different sensor APs are collocated onto a single pane view, along with detailed information such as operating channel, wireless encryption method, and RSSI. Finally, on selected 4ipnet access point models, scanning can be performed real-time without interfering with regular Wi-Fi usage, eliminating the need for specific sensor APs and enabling channel optimization applications.

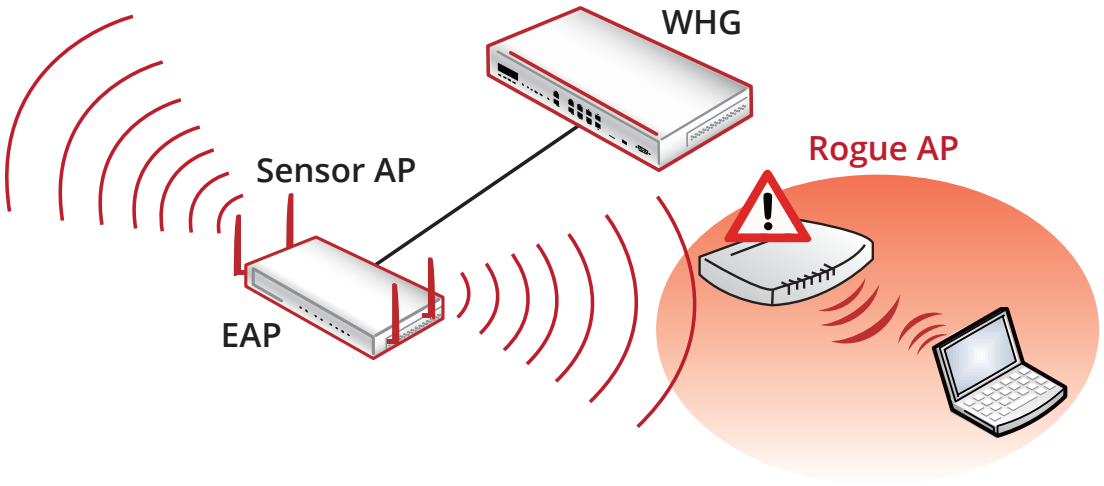

Figure 5: Rogue AP detection allows organizations to quickly detect and respond to unauthorized access points

With these capabilities, organizations can easily monitor their networks for unauthorized access points and take appropriate responsive actions, ensuring that the network environment is both secure and reliable.

LOAD BALANCING

In university lecture halls and other high density environments, network administrators may often find that some APs are overloaded with clients, while other APs have disproportionately very few clients. This situation may occur due to a variety of reasons, such as the "sticky" nature of client devices or simply because most devices have identified a single AP as the one with the strongest signal strength. However, strongest signal strength does not always correspond to highest performance, as signal strength does not take into account the effects of medium access contention.

When an AP is overloaded, connected devices experience reduced performance due to both medium access contention (all the clients are transmitting on the same channel) and competition for the AP's processing resources. Given that it is inefficient for network administrators to continually monitor AP loading status around the clock, an effective algorithm is needed to automatically maintain the distribution of clients across APs. This ensures that overall network throughput will not be severely affected by fluctuations in connection behavior or user density around specific APs.

When deploying the combination of 4ipnet wireless LAN controllers and 4ipnet APs, the APs can be configured to perform load balancing between administrator-defined load balancing groups. APs within the same group will automatically coordinate and make adjustments depending on the current connected client status. For example, if the number of connected clients on an AP exceeds a pre-defined threshold, the AP will lower its perceived signal strength (received by client devices) such that a neighboring AP will seem more "desirable" to connect to. In other words, the load balancing function leverages user behavior (users usually connect to the SSID with the strongest signal strength) to nudge users towards other APs. Instead of strictly enforcing a balanced distribution of clients across APs, which would potentially require kicking the clients and interrupting their currently in-use network

applications, 4ipnet APs employ a more passive yet still effective method to maintain an equal device distribution. Another application made possible by the load balancing function is coverage hole detection, where the wireless

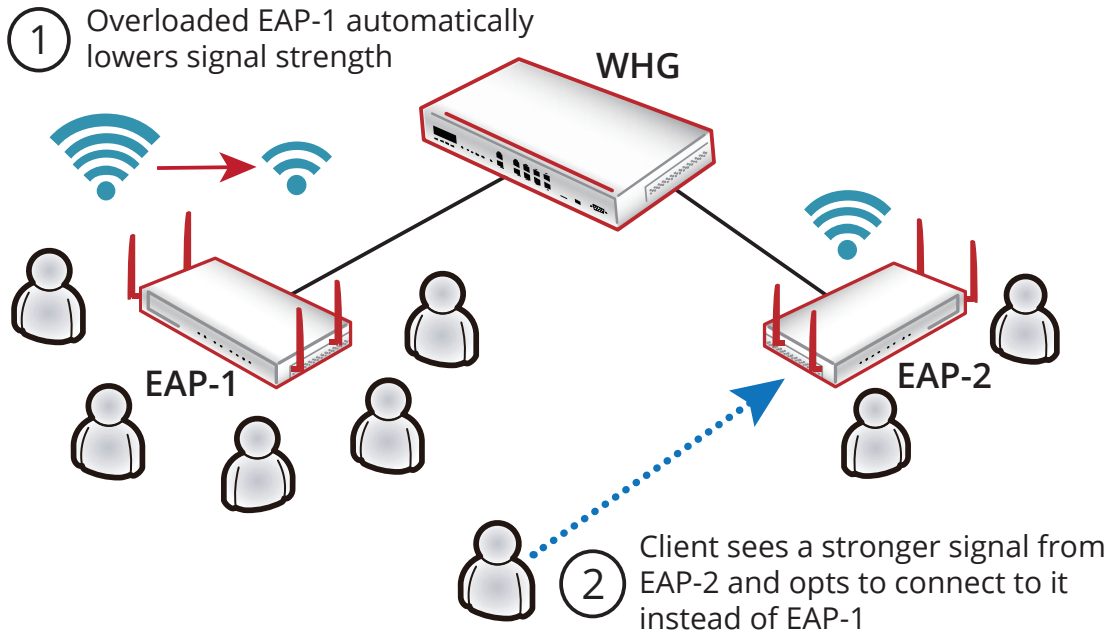

Figure 6: Load Balancing nudges clients to connect to APs that have less clients, distributing clients across APs and optimizing overall network throughput

LAN automatically detects when certain APs have failed and increase the transmit power of neighboring APs to fill the gap in Wi-Fi signal coverage. This is especially important for organizations that cannot afford network downtime, and with the prevalence of mobile devices in today's environment, having areas without wireless connectivity is increasingly becoming unacceptable.

THIRD PARTY AP MANAGEMENT

One of the most unique features of 4ipnet's WLAN solution is the ability for 4ipnet wireless LAN controllers to "manage" access points from other vendors (i.e. third-party access points). Although management capabilities are limited when compared to management of 4ipnet access points, many of the basic applications can still be met. For example, one of the most important features in an enterprise-grade wireless solution is user policy assignment. Without managing the access and usage of users, both network performance and reliability cannot be guaranteed. For most solution offerings in the enterprise WLAN space, these user policies (and many other functions) cannot be enforced when devices from other vendors are used, due to proprietary communication protocols or design limitations.

4ipnet offers a vendor agnostic architecture that allows organizations to perform fine-grained user traffic management such as traffic shaping, applying specific firewall rules, or enforcing QoS priorities without overhauling the entire wireless network. This is especially beneficial for organizations that may have already placed substantial investment in existing network infrastructure, but wish to partially upgrade or switch to equipment from other vendors. However, 4ipnet's solution is not "completely" vendor agnostic – functions such as automatic AP discovery and provisioning are still limited to 4ipnet access points only. In summary, the user management plane (e.g. role-based policies, online user status, etc.) is vendor agnostic, while the AP management plane (e.g. AP traffic status, performance statistics, etc.) is vendor specific.

As the enterprise Wi-Fi market continues to expand and vendors become more diversified, 4ipnet provides a flexibility to unify different platforms. Nevertheless, the most streamlined network deployment and management experience is still realized through the synergy between 4ipnet's own wireless LAN controllers and APs.

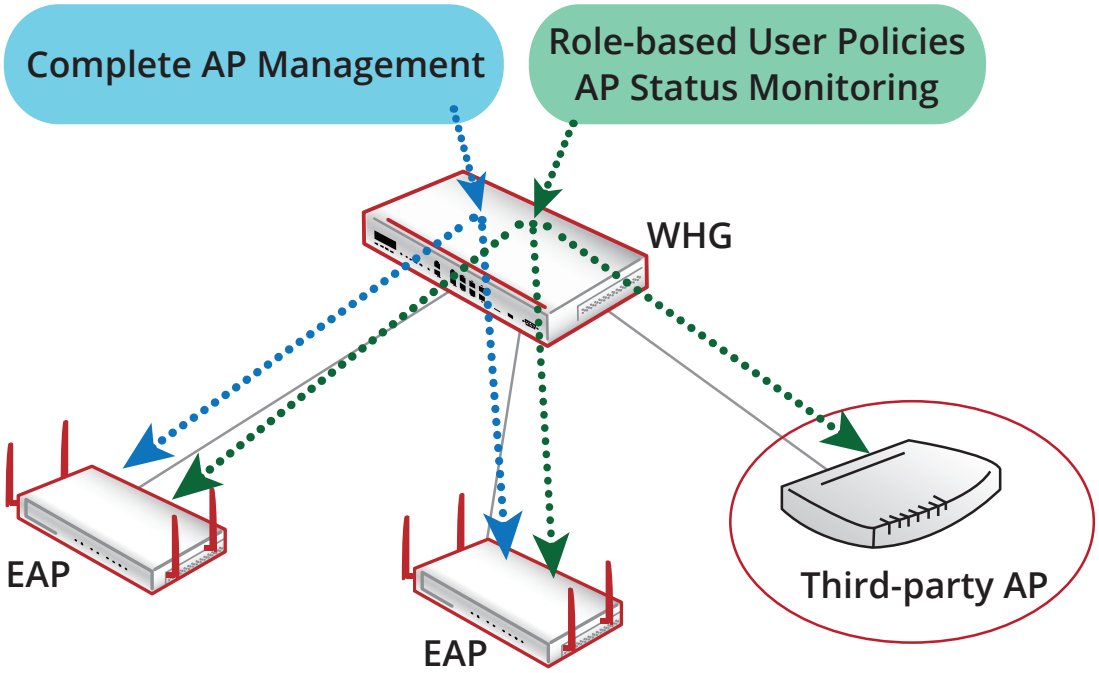

Figure 7: Third party APs have limited management capabilities when compared to 4ipnet APs, but fine-grained role-based user policies can still be enforced

REAL-TIME STATUS CHANGE NOTIFICATION

One of the main reasons why AP status monitoring is an extremely crucial task is because whenever an AP stops functioning network connectivity is interrupted, leading to lost productivity and revenue. However, having a network administrator sit in front of a console and continually watch the statuses of over a hundred access points is also implausible. So how can the IT staff be immediately alerted to network issues while not creating too much maintenance overhead?

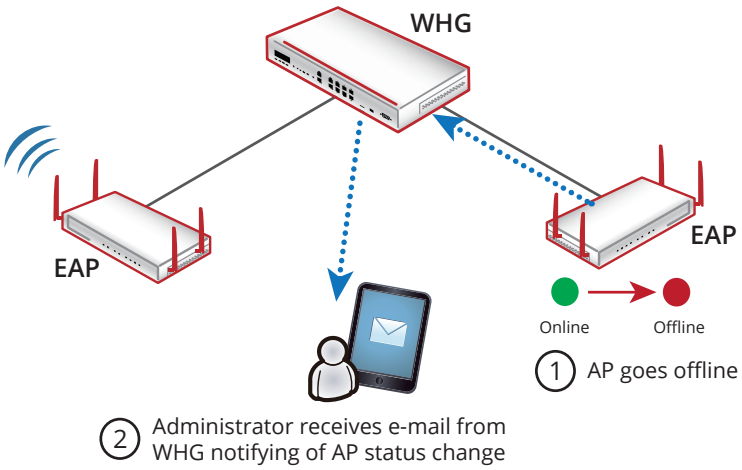

Figure 8: Administrators receive prompt e-mail notifications of AP status changes

With the widespread penetration of smartphones in the consumer mobile phone market, checking e-mails anytime and anywhere is now a common occurrence. 4ipnet wireless LAN controllers take advantage of this trend to make network monitoring easier and more real-time through e-mail notifications of AP status changes. If an AP goes offline (i.e. loses connectivity with the controller), the administrator will receive an e-mail notifying him/her of the incident. He/she can then take the appropriate measures to ensure that network service resumes in a timely manner, minimizing downtime. The added benefit is that the APs do not have to be monitored non-stop – network administrators can go on with their daily lives without worrying about missing critical events.

DETAILED STATUS MONITORING

When network issues are reported, administrators need to have enough tools and information at their disposal to aid in troubleshooting. For example, slow performance can be due to too many clients associated to the same AP, irregular memory or processing unit behavior, or an increased number of packet collisions in the air resulting in high retransmission count. Without the appropriate network traffic and system performance statistics, it is difficult for the IT staff to determine the real cause of connectivity and performance issues.

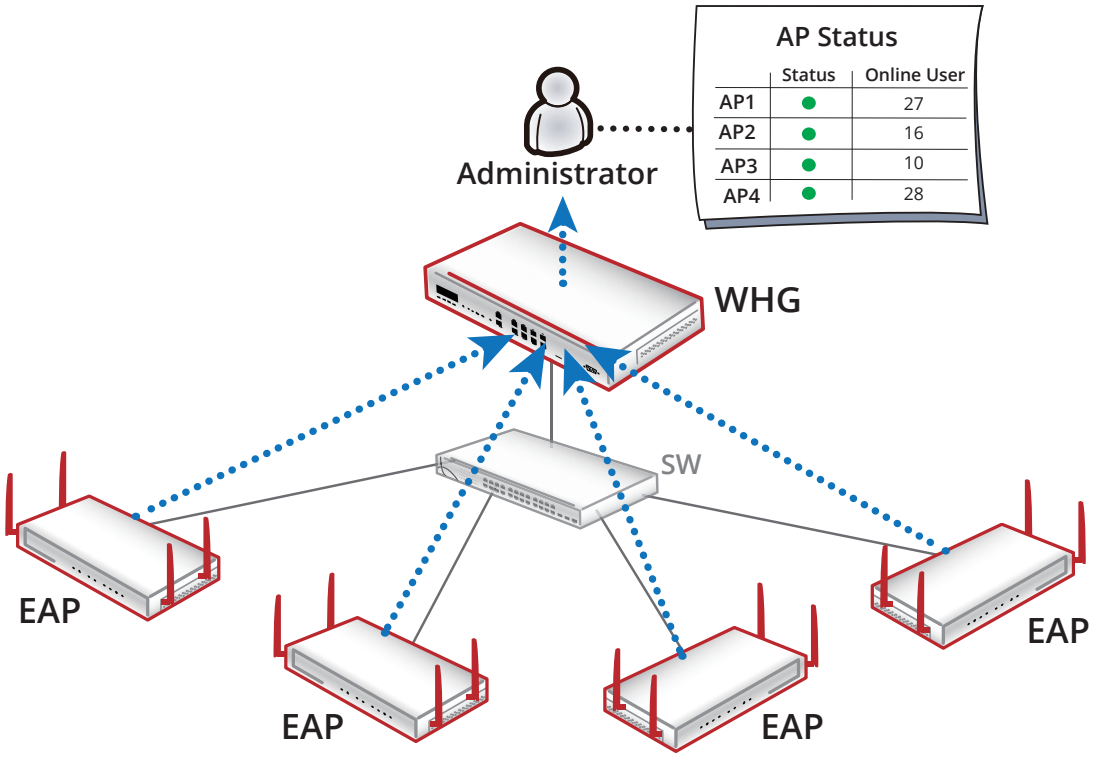

Figure 9: Detailed AP status monitoring enables network administrators to quickly troubleshoot connectivity or performance issues

Administrators have access to all of this information through the centralized interface on 4ipnet wireless LAN controllers, including but not limited to transmitted and received packets/bytes, memory usage, and number of associated devices. Furthermore, all of the basic system settings and detailed per VAP traffic statistics are presented on the same page for simple and complete visibility of the entire AP's status. If the administrator does not wish to access the controller's interface frequently to view these statistics, the controller can automatically send out complete reports of managed APs on a daily, weekly, or monthly basis. In summary, 4ipnet's wireless LAN controllers track and record detailed information regarding each managed AP, reducing network maintenance and troubleshooting complexities.

CONCLUSION

Enterprise-grade wireless LAN deployments are often difficult and time-consuming to deploy due to complex environments (e.g. physical obstructions, high user density, etc.) that must be accounted for. Even after completing initial deployment, there is no guarantee that the network will operate and perform as planned, given the unpredictable nature of user behavior. Therefore, it is critical for network administrators to have methods to efficiently deploy, manage, monitor, and troubleshoot network issues.

4ipnet wireless LAN controllers help organizations reduce total cost of ownership by offering a simple yet powerful AP management interface. Furthermore, features such as rogue AP detection and AP load balancing help guarantee the security and performance of the network. By deploying 4ipnet's access points alongside its wireless LAN controllers, organizations can ensure that their wireless networks are reliable, cost-effective, and highly flexible.