ACCESS POINT OPTIMIZATION

SUMMARY OF FEATURES

AIRTIME FAIRNESS

BAND STEERING

OPTIMAL CLIENT FILTERING

MULTICAST TO UNICAST CONVERSION

WI-FI MULTIMEDIA (WMM)

PROXY ARP

WI-FI PROTECTED ACCESS II (WPA2)

STATION ISOLATION

DHCP SNOOPING

LAYER 2 FIREWALL

ENTERPRISE VS. CONSUMER AP

"Why should I pay an extra five to ten times the cost for an enterprise-grade AP (access point), when I can buy a much cheaper wireless router from Amazon or the electronics shop down the block?" This is one of the most commonly asked questions in all segments of the enterprise Wi-Fi market, including hospitality, education, large enterprises, and SMBs. To answer this question, we must first look at the fundamental difference between the consumer and enterprise Wi-Fi markets – more specifically, how access points are deployed and used. For example, Power over Ethernet (PoE) is a hardware specification that is ubiquitous on all enterprise-grade APs, due to the presence of PoE switches that lie at the core of every enterprise's network infrastructure as well as the expensive cost of physical cabling.

In this feature guide we will highlight the performance and security features of 4ipnet access points, and in the process clearly illustrate the differences between 4ipnet APs and regular consumer-grade APs.

AIRTIME FAIRNESS

As networks migrate between wireless standards – previously from 11g to 11n, and now from 11n to 11ac – network operators are increasingly struggling with the tradeoffs between legacy client support and wireless performance. For example, when both 11g and 11n clients are connected to the same AP, an 11g client will take much longer (use more airtime) to complete the transfer of the same amount of data as an 11n client. To understand why this matters, we must first briefly explain how data is transmitted over Wi-Fi.

The fundamental concept behind wireless transmission is that two devices cannot transmit at exactly the same time in the same frequency, otherwise collisions occur and the transmission will be unsuccessful. Wi-Fi deals with this issue by utilizing CSMA/CA (carrier sense multiple access with collision avoidance), which incorporates a random back-off period for each transmitting device when detecting that the medium is busy. Therefore, the longer a single device takes to transmit, the higher the probability that other devices trigger their respective wait periods.

Back to the legacy client example, this means that all other clients have to wait for the legacy client to finish transmission, which results in decreased overall network throughput. However, if legacy standards such as 11g are not allowed, operators will surely receive a lot of complaints from users who have older devices that only support legacy standards. Herein lies a dilemma: do operators allow legacy clients to connect at the expense of overall network throughput, or do they block all legacy clients and maximize performance?

Luckily, on 4ipnet APs there is a middle ground. **AIRTIME FAIRNESS** is a feature that allows networks to mitigate the decrease in performance incurred by supporting legacy clients. Depending on the needs and preferences of each deployment, the following two options can be selected:

1. All clients, regardless of standards supported, obtain roughly the same amount of airtime. If a client occupies the wireless medium for a longer period of time in one transmission, then subsequent transmissions are placed on a lower priority, ensuring that overall airtime distribution is balanced.
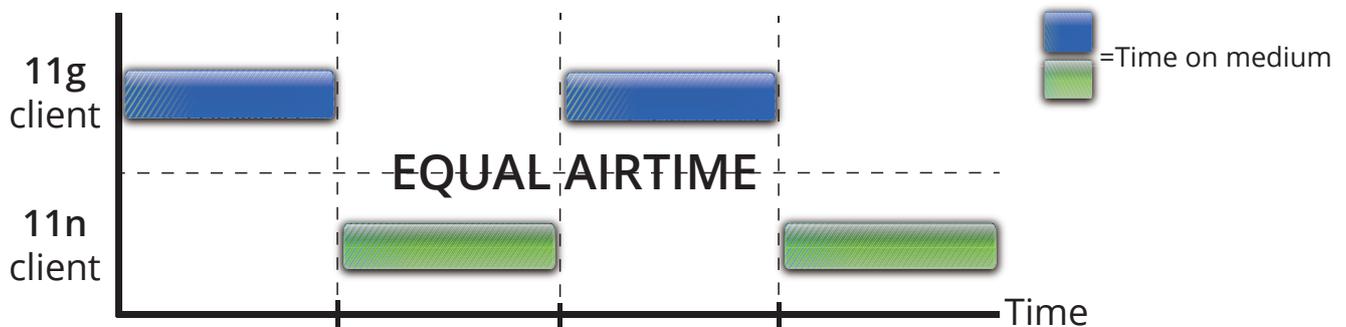

Figure 1: All clients are allocated equal airtime to prevent starvation due to slower/legacy clients

2. 11n clients are given a slight preference. Legacy clients are not blocked from the network, but they will be allocated less airtime. This option is ideal for organizations that wish to optimize network performance while still supporting older clients. Organizations can also use this feature as a method to slightly "nudge" older clients to migrate from 11b/g to 11n.

With either option, administrators are able to increase overall network throughput without sacrificing the support of legacy clients. Further details on how priority is managed by the AP will be described in the section on WMM.

BAND STEERING

In today's wireless environment the unlicensed 2.4 GHz frequency band is becoming increasingly congested due to the explosion of mobile devices. As a result, many consumer device manufacturers, whether it be of laptop computers or smartphones, have incorporated 5 GHz-capable Wi-Fi chipsets in their devices. Furthermore, 802.11ac ready consumer devices are already making their way into the hands of everyday users. This begs the question: When a Wi-Fi environment offers connectivity in both 2.4 GHz and 5 GHz, and clients have both 2.4 GHz and 5 GHz capability, how do network operators balance the load

Figure 2: Clients capable of 5 GHz are "steered" towards 5 GHz networks

between the two frequency bands? One method is to simply to add the frequency band to the SSID name. For example, instead of "Hotel", "Hotel-2.4GHz" and "Hotel-5GHz" can be used instead. But what if organizations don't want to advertise the frequency band in the SSID?
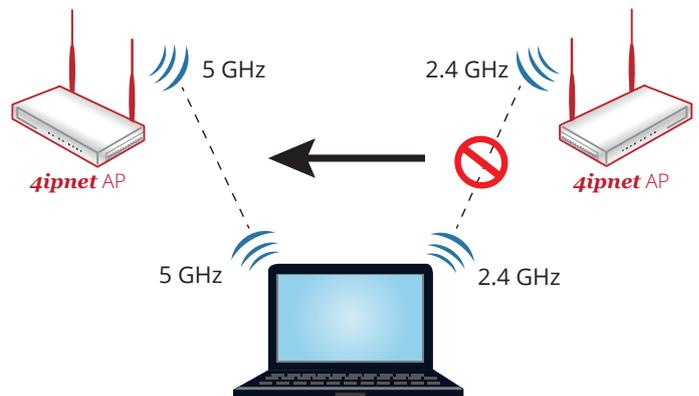
BAND STEERING is a function that addresses this exact issue. When enabled on a 4ipnet access point, the AP will use one of two methods to "steer" clients that are capable of operating in the 5 GHz band away from 2.4 GHz networks and towards 5 GHz networks.

1. The AP does not respond to 2.4 GHz probe requests of the client, tricking the client into believing that it does not exist. For the user, this means that the SSID cannot be seen. However, if the user happens to know the SSID, he/she can still manually connect. This is a more passive method of Band Steering, as users will not completely be prohibited from using 2.4 GHz if their device supports 5 GHz.

2. The AP rejects 2.4 GHz connections from the client, even if the client were to know the SSID and manually connect. This is the more aggressive method of Band Steering, and in essence forces all 5 GHz clients to only connect to 5 GHz networks.

Band Steering is a feature that can be enabled or disabled individually for each AP, but it does not make much sense if the setting is not consistent between neighboring APs. For example, if the purpose is to reduce congestion in the 2.4 GHz frequency band, then network administrators should enable Band Steering for all APs to redirect as many connections to 5 GHz as possible. If only a few of the APs have the function enabled, then 5 GHz clients will still be able to connect to other 2.4 GHz SSIDs, meaning that actual spectrum usage and medium access in 2.4 GHz is still the same. Although at times Band Steering can be viewed as a feature to load balance clients between different APs, ultimately its end goal to lower 2.4 GHz medium access contention.

OPTIMAL CLIENT FILTERING

Earlier in this feature guide we described Wi-Fi as a form of a wireless communication that utilizes CSMA/CA to avoid collisions during data transmission. As mentioned, one caveat of this protocol is that anyone who wishes to use the medium to transmit must wait until the medium is free (unused). Therefore, if a device or client takes a long time to transmit a small amount of data, overall network throughput is decreased. Now let us consider the case where a network consists of only 802.11n (or 802.11ac) clients. Theoretically, everyone can get in and out of the medium in a short amount of time, since under 802.11n/ac standards data can be transmitted at relatively fast rates. In this case, is network performance optimized?

Legacy clients are not the only issue in a wireless environment – even though all clients may utilize the most up-to-date standard, some clients will inevitably have poorer transmission rates than others due to interference, physical obstructions, or large distances between themselves and the AP. As a result, these clients have to stay on the medium longer to complete data transmissions, which creates the exact same phenomenon as legacy clients. If you've ever wondered why the network feels very slow even when you have "full bars" of connection in the taskbar, it may be because others using the same network have less than ideal connectivity.

For a wireless network to perform optimally, not only should clients comply with the newest standards, they should also connect to APs that offer them best connection. However, this is a best-case scenario that cannot always be guaranteed, since all Wi-Fi users usually think about is getting "connected". Should everyone be allowed to connect to the network even when under conditions of poor connectivity (which drags down the entire network's throughput)? Or do you prevent these devices from connecting to let others enjoy higher throughput? This is a question that many network administrators struggle with as Wi-Fi becomes more pervasive and common in our daily lives.

OPTIMAL CLIENT FILTERING is a method that helps 4ipnet APs filter out clients that will negatively impact the AP's overall throughput. Through a set of thresholds, such as Dropped Packet Threshold, Transmission Rate Threshold, and Receiving RSSI Threshold, the AP is able to remove (kick) clients that have poor connectivity. This ensures that all clients connected to an AP have an acceptable connection quality, minimizing the number of packet retries and increasing airtime efficiency.

Figure 3: Client connections are filtered based on pre-defined connectivity thresholds

How does this translate to real-life deployments? Some environments such as hospitals may be very strict on

connectivity and performance issues (where delays may be the difference between life and death), while other environments may be more tolerant towards devices with slow connectivity. With 4ipnet's Optimal Client Filtering, network administrators can fine-tune each threshold value depending on the needs of each deployment to ensure optimal wireless performance.

MULTICAST TO UNICAST CONVERSION

In Wi-Fi networks, multicast packets are typically sent at slower rates to ensure that devices at the edge of an AP's cell are able to receive the packets without error. This may be useful in environments where most clients are a certain distance (further away) from the AP. However, if the cell size is very small and most clients are densely packed around the AP, this would be an inefficient use of airtime. Why send at 11M when you can send at 300M?

MULTICAST TO UNICAST CONVERSION is a method that 4ipnet APs employ to convert multicast transmissions to unicast so that they can be sent at unicast rates. When clients are close to an AP, high transmission rates can be more easily sustained, and thus unicast is more efficient. On the other hand, attempting to use the same rate with clients far away from the AP will lead to a high number of retransmissions, which lowers efficiency. As a result, Multicast to Unicast Conversion is not a universally beneficial feature – it merely allows network administrators to optimize performance based on how clients are spatially distributed around APs.
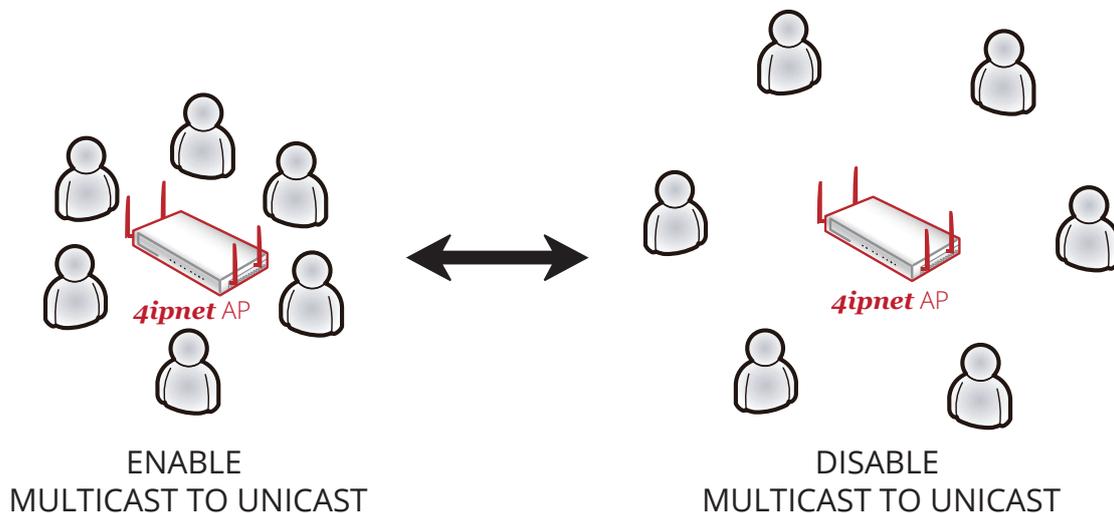

ENABLE
MULTICAST TO UNICAST

DISABLE
MULTICAST TO UNICAST

Figure 4: Multicast to Unicast Conversion is ideal in environments where the majority of clients are densely packed around APs

WI-FI MULTIMEDIA (WMM)

If you've ever observed VoIP over Wi-Fi working flawlessly even when there were tons of other applications simultaneously using the network, then you've seen **WMM (WI-FI MULTIMEDIA)** in action. WMM provides fundamental QoS (Quality of Service) functionality to wireless networks by increasing the performance of differentiated wireless traffic, such as audio, video, and traditional application data. Based on the needs of each type of data, they are placed in one of four different queues, BE (Best Effort), BK (Background), VI (Video), and VO (Voice).

Recall the earlier description of Wi-Fi medium access using CSMA/CA – clients must wait for a random amount of time before retrying transmission if a busy medium is detected. WMM assigns shorter or longer average back-off periods to each of the four queues, which in essence gives each queue a different priority. The queue with the shorter average random back-off period (e.g. Voice) will forward traffic faster and more easily (with higher priority) than queues with longer average random back-off periods (e.g. Best Effort).

On 4ipnet access points, traffic is automatically prioritized and placed into one of the four queues based on its 802.1p priority tag or DiffServ Code Point (DSCP) value. Along with the traffic remarking function on 4ipnet wireless

LAN controllers, network administrators have a complete arsenal of tools at their disposal to guarantee reliable, latency-free operation of mission-critical applications.

It is important to note that WMM and Airtime Fairness both utilize priority assignment but with very different purposes. WMM performs prioritization based on the type of traffic, while Airtime Fairness performs prioritization based on the type of client.

PROXY ARP

ARP (Address Resolution Protocol) is an essential protocol in networking (both wired and wireless) that resolves IP addresses to MAC addresses when data needs to be sent between two hosts. Whenever a host wishes to obtain the physical address (MAC) of another, it will broadcast an ARP request onto the network. On wireless networks this may sometimes be additional and unnecessary traffic that decreases overall network performance.

4ipnet access points address this issue by employing **PROXY ARP** to reduce the amount of ARP packets in the wireless medium, handling ARP requests itself instead of forwarding them onto the wireless medium when possible. As long as the AP's own ARP table has a record of the address requested, it can respond on behalf of the actual host. As a result, the amount of ARP packets in the air diminishes and hosts learn MAC addresses much more quickly, increasing overall network throughput.

WI-FI PROTECTED ACCESS II (WPA2)

In enterprise-grade deployments security is one of the most commonly emphasized features and requirements. The first line of defense is usually at the point of access to the network, which back in the old days was composed primarily of network switches, but is now shifting rapidly towards wireless access points. Similar to the port-based authentication features on Ethernet switches, wireless access points also have methods to authenticate devices. Furthermore, the evolution of Wi-Fi in recent years has begun to invalidate the notion that data transmission over wireless is insecure – with authentication and encryption protocols such as **WPA2-ENTERPRISE**, organizations can rest assured that confidential information will remain confidential.

WPA2-Enterprise provides 802.1X authentication with the access point acting as the authenticator, blocking access until successful authentication. For deployments where security is not as stringent, network administrators can use WPA2-Personal and simply perform passphrase verification in order to gain access to the network. Both methods utilize AES data encryption, which would theoretically take longer than the age of the universe to be cracked via brute-force by even by the most powerful supercomputers today.

STATION ISOLATION

In many Wi-Fi environments, it is not uncommon to see upwards of twenty or thirty devices connected to a single access point. Allowing direct communication between these clients would be a security concern for network operators, as malicious traffic from one client could potentially affect another. The **STATION (CLIENT) ISOLATION** feature on 4ipnet APs allows network operators to prevent devices connected to the same AP from communicating with one another, essentially creating a virtual network per client.

Imagine that you have a bunch of strangers connected to the same access point in a coffee shop, all of whom are assigned IP addresses by the same DHCP server, which usually means that they are on the same network (subnet). If a user were to have file sharing turned on
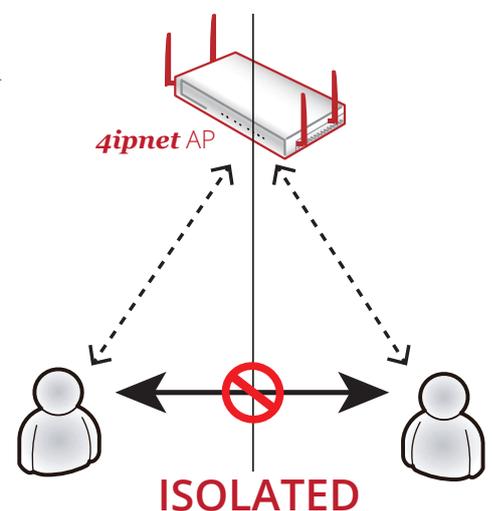

4ipnet AP

ISOLATED

Figure 5: Station Isolation prevents direct communication between clients on the same AP

(e.g. Windows-based system), then all of the other users on the network would be able to browse the files of the exposed system. So while the user may have only wanted to get coffee and browse the Internet, he/she actually ended up sharing all of his/her personal documents to every other coffee-goer. This illustrates why Station Isolation is a crucial security feature, and why it is imperative for network administrators to enable the feature, especially when providing public Wi-Fi service.

DHCP SNOOPING

In order for a device to begin using network services after connecting to an access point, it must first obtain an IP address from the network's DHCP server. This is a point of vulnerability, as attackers can install their own DHCP server and assign clients arbitrary IP addresses and default gateways. In the worst case, a rogue DHCP server controlled by a hacker could potentially cause network administrators to lose control of their entire network, which is a major security flaw.

The **DHCP SNOOPING** feature on 4ipnet APs prevents this type of network failure by allowing network administrators to specify the IP and MAC addresses of trusted DHCP servers. As a result, the APs will filter out DHCP messages from unrecognized servers, preventing them from ever reaching client devices. Although DHCP attacks are typically not as big of a concern for small-sized networks, enterprise and government networks requiring the tightest of security measures will find DHCP snooping to be a beneficial added-layer of security.

LAYER 2 FIREWALL

For security purposes, network administrators may sometimes want to block specific types of traffic directly at the access point, preventing them from ever reaching associated wireless devices, such as applications running on specific ports, or traffic originating from specific IP addresses. For example, if a school discovers that students are using the school's network to play online games during class time, the school may want to block the port(s) that are used by the game to serve content. To address requirements such as these, 4ipnet access points are equipped with a **LAYER 2 FIREWALL** feature that help network administrators enforce usage policies.

Another usage of the Layer 2 Firewall feature is to improve wireless performance by preventing unnecessary traffic from being sent out by the AP. Throughout this feature guide we constantly reiterated how a wireless network's throughput is affected by the number of hosts contending for medium access – even network maintenance packets such as STP (spanning tree protocol), which do not necessarily need to be sent to edge nodes (e.g. wireless devices), can negatively impact a network's performance. By blocking these packets, the airtime that would have been required to send them is freed for transmissions other devices.
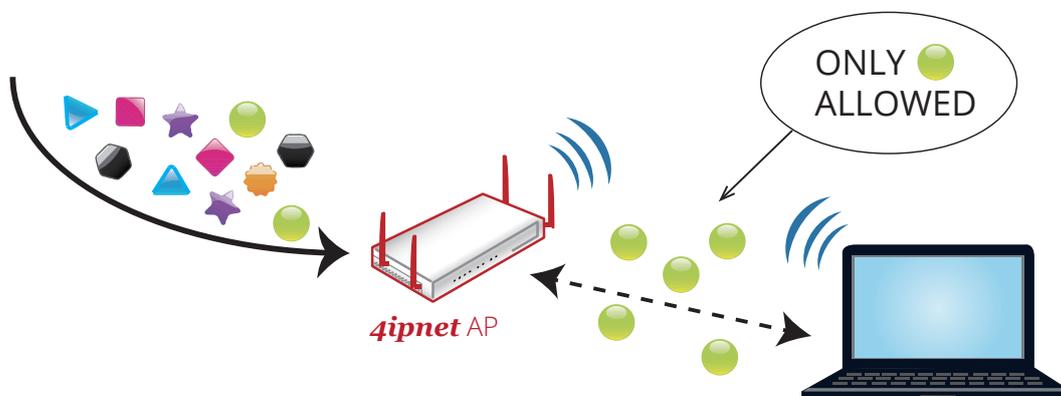

Figure 6: Layer 2 Firewall can be configured to prevent unnecessary traffic from entering the wireless medium, improving overall performance

Although firewall features are also available on 4ipnet wireless LAN controllers, there are a few major reasons for blocking packets directly at the network edge (at the access points):

1. Specific types of packets from the wired end of the access point will not be flooded out onto the

wireless medium, decreasing interference and increasing overall wireless throughput.
2. Malicious traffic from wireless clients can be blocked before ever entering the network, limiting the amount of potential damage.

CONCLUSION

By introducing the various performance and security features on 4ipnet access points, the difference between consumer and enterprise-grade APs should now be much clearer – many of these features deal with applications and usage scenarios only found in large-scale deployments. In today's smartphone and tablet environment, it is not uncommon to see an average of five to ten Wi-Fi enabled devices in traditional households. However, public Wi-Fi hotspots such as coffee shops, hotels, or office buildings may have ten times that amount or even more. The need for enterprise-grade APs is real. Enterprises and organizations have to address the ever increasing number of mobile devices and the seemingly insatiable desire for bandwidth. 4ipnet's wireless LAN solution is well-aligned to help organizations of all types and scales face this rapidly evolving Wi-Fi landscape.