Aerohive NETWORKS

White Paper

BYOD and Beyond:

How To Turn BYOD into Productivity

HOWARD | TECHNOLOGY
www.howardcomputers.com | (888) 912-3151

Mobility, Productivity, and BYOD

The mobility phenomenon is truly one of the drivers of technology today. A few short years ago, wireless was simply a convenience feature to provide connectivity in conference rooms and on campuses for students who wanted to sit outside while writing a term paper. Now with the advent of all these wireless devices, the requirement for mobility and wireless in motion, and the lack of physical Ethernet ports on these devices, wireless has moved from being just a convenience into being the true primary access layer for network connectivity. Gone are the days when a network administrator could sit down and plan "3 Ethernet ports per cube" and be ready to go for switch, access, and capacity planning. Now users aren't connecting just their corporate-provided computers, but a bevy of personal and corporate-provided devices that are truly changing work from a place you go to a thing you do – any time, anywhere, and from any device. In fact, over 80% of workers surveyed are bringing their personal devices to work – and 87% of those users are using them for work-related activities (not just Facebook!). [1]

In 2011, IDC research reported that for the first time ever, more devices shipped without an Ethernet port than with one[2]. As we prepare for this onslaught of wireless mobility in the workplace, IT administrators are faced with more challenges than ever before – how much bandwidth is enough? What types of devices might show up? Today we hear 72% of personal devices are Apple devices[3] – but what about next year? How can an IT administrator prepare for an unknown set of devices, with unknown bandwidth and connectivity requirements, with the same number of resources, and still rest assured that he can confidently say his network is secure, high performance, and ready for the next wave of new technology – especially gigabit Wi-Fi?

This is the BYOD predicament. Efforts to allow users to bring their own devices to work to improve productivity and mobility are countered by the worry that devices may not be secure, that workers may be distracted by applications rather than using the device for work activities, and above all, place an overwhelming burden on the limited IT staff for supporting and troubleshooting these unmanaged devices.

One of the most overlooked aspects of the BYOD phenomenon isn't just connecting the users to the network, but how to manage them once they're there. Getting mobile and BYO devices onto the network is now table stakes. Having a way to securely connect and monitor managed and unmanaged devices should be one of the very first requirements for a network administrator evaluating a networking vendor solution. However – once you get them onto the network, what do you do with them? What features/functionality should you look for in order to ensure that once you allow users to connect their devices, that you can still ensure security, privacy, and productivity? The real drain on IT resources was never getting devices onto the network – it's what to do with them once they're there. Reporting on security compliance, ensuring the devices can use available services and assets and are restricted from those which they should not access, and making sure the devices don't overwhelm available network resources are the real game changers for a successful BYOD implementation.

This whitepaper will take you through the necessary connectivity and productivity requirements in order to ensure your network is truly ready for the mobility explosion, including an overview of necessary access, authentication, and security options as well as focusing on the equally essential features required to ensure your network is prepared to make all devices attached to it productive and compliant.

---

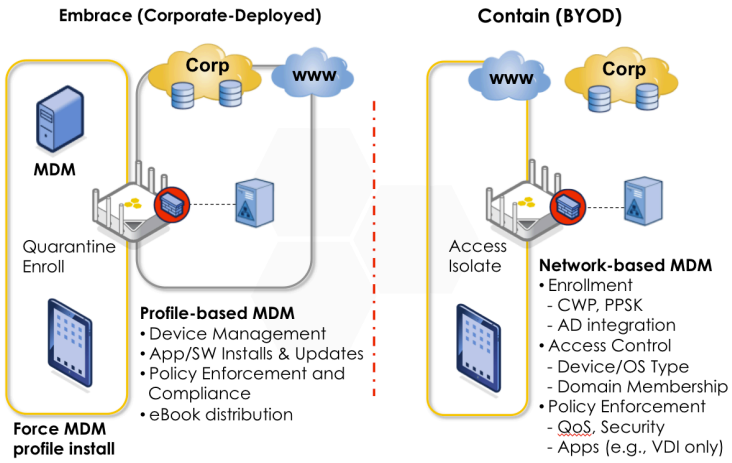
[1] Dimensional Research, "Consumerization of IT: A Survey of IT Professionals", Dell KACE 2011

[2] IDC, "Market Analysis Perspective (MAP) Enterprise Communications Infrastructure Market" 2010

[3] Dimensional Research, "Consumerization of IT: A Survey of IT Professionals" 2011

Connecting Users to the Network

One of the first challenges facing administrators looking at implementing a BYOD solution is defining exactly which devices "BYOD" is referring to. Often "BYOD" is misused to refer to any consumer-grade device connected to the corporate network. The reality is, "BYOD" refers to devices brought in by end users to connect to the network instead of being distributed by the IT department. There is also a parallel initiative facing network administrators planning for mobility, where IT may consider using consumer-grade devices, such as tablets, to lower hardware costs and increase productivity for dedicated applications like retail kiosks or Electronic Medical Records (EMR). This "Consumerization of IT" also requires network intelligence to embrace the inherent cost savings and flexibility built into such devices while controlling exactly what and how the devices are used on the network. A truly comprehensive mobile device solution will need to address both Consumerization of IT as well as BYOD in order to support, contain, and embrace both types of devices.



There are really two major camps when it comes to ensuring mobile devices are accessing the network securely. On one side, there are many companies who are very successful in deploying agent-based Mobile Device Management solutions to ensure connected devices have the right software, permissions, and security settings before allowing them to connect to the network. These agent-based solutions are very popular with larger companies and education facilities, especially those embracing the Consumerization of IT and manage large numbers of corporate or school-issued mobile devices. On the other side of the MDM spectrum is what is called Network-based MDM, where there is no agent to install on the client device, and the network devices are intelligent enough to make classification decisions based on user identity, device type, location, and time. In order to provide a truly comprehensive BYOD and mobile device-friendly infrastructure, you must be able to support both agent-based MDM as well as network-based MDM. This allows companies to leverage and control consumer devices in the enterprise, while also supporting users who will not accept the inherent risk to their personal data that comes along with installing an agent-based solution. This means that the network devices must be even more intelligent to provide administrators the ability to enforce MDM agent installation or utilize user and device-level classification and access control to ensure secure and productive BYOD use on the network.

Aerohive has focused particularly closely on intelligent infrastructure built for the mobile device explosion, and has many features to ensure devices are connected properly to the network. Features like MDM agent enrollment quarantine and enforcement, Network-based MDM, built-in stateful firewalls in every access point, and GRE tunneling are an integral part of HiveOS, the network operating system that powers all Aerohive devices, which together help ensure success in implementing a BYOD strategy.

At its core, HiveOS is built to be inherently redundant, resilient, and future-proof by using edge-based intelligence and Cooperative Control to ensure connectivity for clients. A single Aerohive access point

can make all the forwarding decisions, security enforcement, and advanced feature functions that you read about below, but when joined together as a hive of devices, the power of the Aerohive system becomes truly remarkable. Using Aerohive Cooperative Control to provide MDM services on top of secure wired/wireless access ensures that BYO devices are connected to the right resources based on all associated context – identity, device type, location, etc – making BYOD truly a productivity enhancement rather than a resource drain.

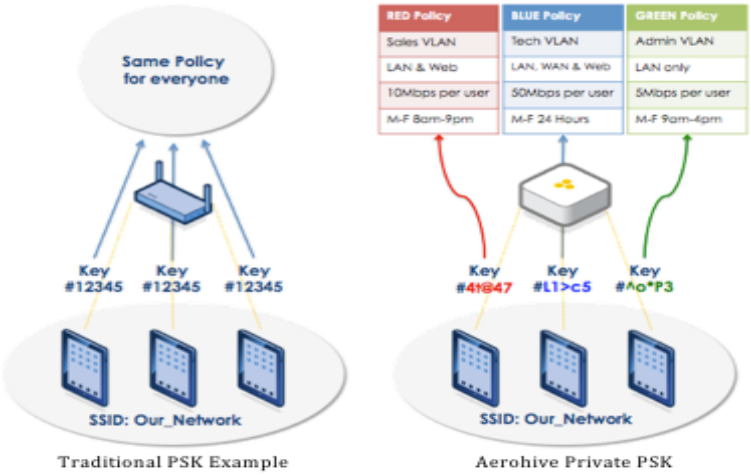
Authentication and Access

With BYOD, one of the major challenges to ensuring secure access is that these devices are developed to make it easy to connect them to any type of network – even one requiring certificates. However, it is equally important to support older BYO devices that only support legacy networks like 802.11g and don't support certificate-based authentication. The Aerohive solution provides an administrator with many options to aid getting users onto the network securely.

One of the most common secure network types is to configure WPA2-Enterprise (802.1X) on your corporate SSID, which requires at least a username/password combination and acceptance of a server certificate in order to authenticate. However, unless an administrator takes an extreme stance and requires that every single device connected to this network also has a certificate installed on it (not only a huge administrative burden but sometimes impossible based on the device support), the modern mobile devices have made it as easy as checking the "Accept" button and entering network credentials to connect a BYO device to this type secure network. Now the administrator may have a secure authentication method, but who knows what these devices are doing on the network? Read on to the security and enforcement section below for a way to control this behavior.

Even before the devices get onto the network, however, there are several additional options Aerohive has available in order to short circuit some of the trickier aspects of connecting users securely. Beyond just the basic open Guest SSID with a terms and conditions splash page, Aerohive will allow you to authenticate users connected to any type of SSID (open or secured with a key) against a Captive Web Portal which can be tied back to Active Directory (or other directory server). You could even enforce MAC authentication to ensure only certain devices or types of devices connect to the network.

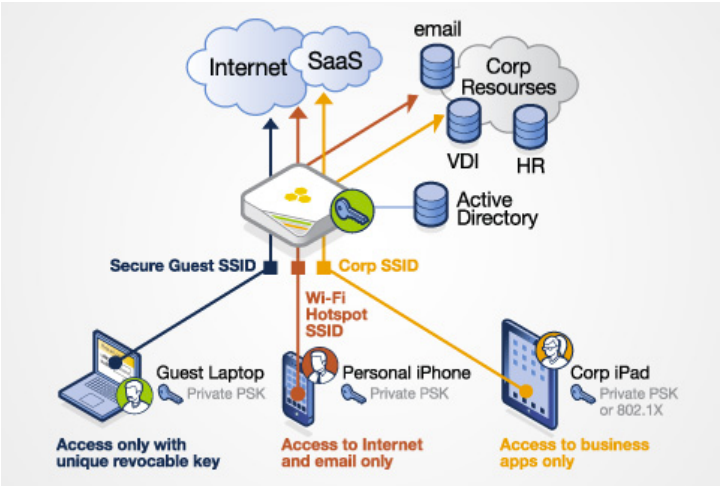
An additional option unique to Aerohive is our patent-pending Private Pre-Shared Key feature. This feature is remarkable because it allows an administrator to enforce per-user and per-device permissions and security, but doesn't require any certificate or username/password credentials for the connecting users. An administrator can specify a particular key or group of keys to have defined network permissions, such as assigned VLAN, firewall policy, and tunneling permissions, and then he can even tie that key to the first device connected using it to ensure that no additional BYO devices can be connected with the same key. This simple solution provides all the per-device encryption and security normally associated with the more complex 802.1X solutions, but works on all devices that support PSK and requires no certificates.



Security and Enforcement

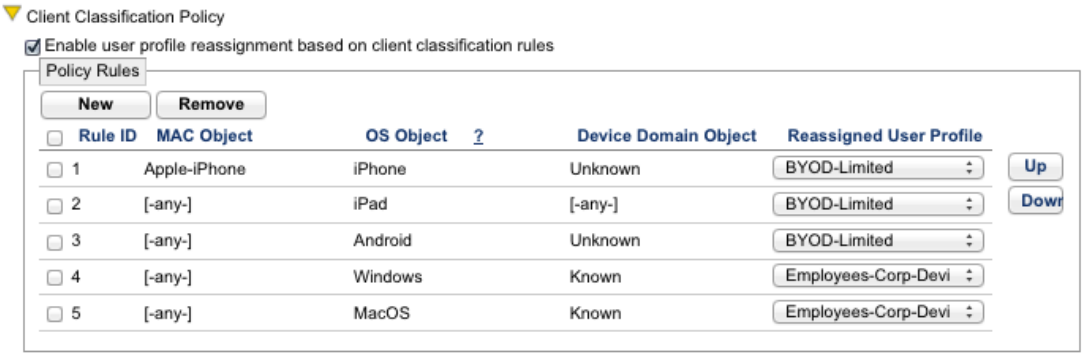
Once the administrator decides on an authentication and access method, the next step is ensuring the connected devices follow the guidelines for the network – based on context such as identity, device, location, and time.

At the heart of Aerohive policy enforcement is assignment of a User Profile to a connected device. An Aerohive user profile defines permissions to the network, such as what VLAN the user should be assigned to, the firewall, tunnel, and QoS policies for that user or group of users, client enforcement features such as SLA and client classification settings, and various other settings that can be applied on a per-user basis. Defining how the user profiles are applied is dependent on the type of authentication defined and the client classification rules configured.



Client classification allows administrators to implement full network-based mobile device management with a few simple clicks. Network-based MDM (NMDM) means the devices providing access to the network, such as access points, switches, or routers, are the ones doing the enforcement rather than requiring an agent installed on the client. This provides complete flexibility in what clients are supported and how many clients a single user can connect to the network, without any worry of installation/compatibility issues or licensing heartache. It does not extend to controlling device-level permissions like requiring a passcode, enforcing app or software installation and updates, or distributing eBooks or other on-device content; all of that requires a software MDM (SMDM) profile or agent on the device itself.

With the Aerohive client classification feature, administrators get several layers of network-based mobile device enforcement, starting with the initial user authentication. This is important because it means identity of the user remains the first variable when further defining permissions based on context such as device type, location, and domain membership. For example – it means you can differentiate between BYO devices, such as iPads, owned by your executive staff versus your sales team, and enforce different policies for users not only based on device context but also by identity, rather than just making a blanket policy for all attached iPads.



Once the new profile is assigned based on contextual identity, permissions to the network change based on the firewall, tunnel, and schedule policies configured in the new profile. One of the most commonly used features to ensure segregation of specific devices on the network is using the built-in stateful firewall in every Aerohive device. Even if all users and devices are connected to the same VLAN, an administrator can still enforce policies between users and network resources. This allows the enforcement to happen right at the edge, where the traffic first enters the network, instead of having to traverse the entire infrastructure before eventually being restricted by a core security appliance. For instance, an administrator may wish to keep Employee BYO devices on the same network as corporate-issued trusted clients, but the BYO devices only can access the Internet and not any restricted corporate resources.

Another common way to enforce segregation of traffic is by using layer 3 tunneling features. This feature is often used to connect different virtual LANs throughout a campus to enable seamless roaming between subnetworks, but can also be used to force a roam to a specific access point based on identity and device type. Rather than configuring a guest VLAN throughout the network to support BYO devices, an administrator might prefer to define a policy where any detected BYO device is automatically tunneled to an access point located in a DMZ. This simplifies the network configuration, but still ensures that BYO devices are completely segregated from the corporate network.

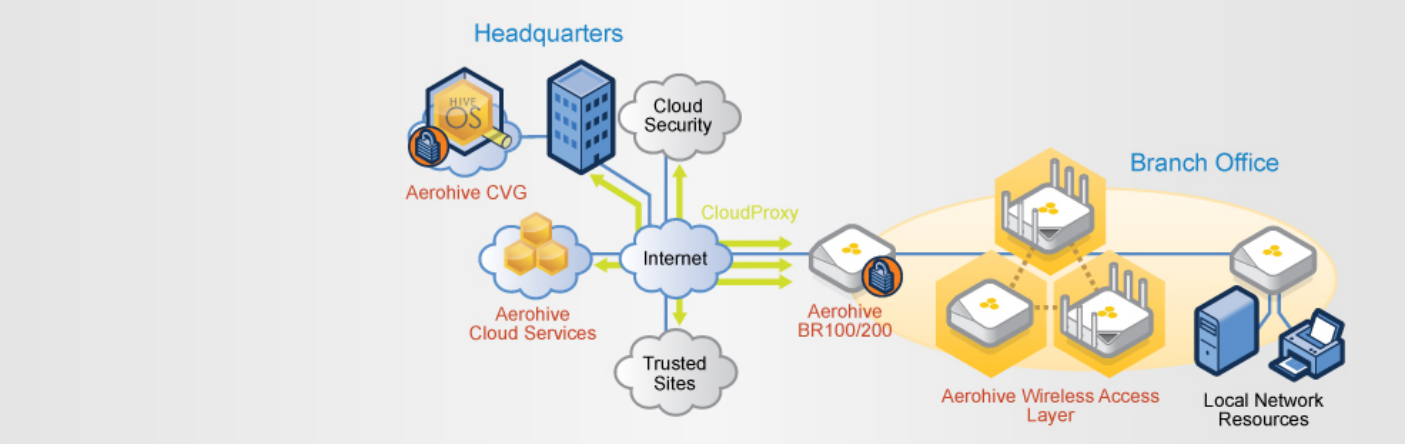
Connecting Remote Users

The last piece of the BYOD connectivity puzzle is ensuring that employees remain productive and connected to essential resources, regardless of where that employee may be – at the corporate office, at a branch location, or even at home. Once the administrator has defined the network access policy, configured the available SSIDs and VLANs, and created policies to assign permissions based on identity and device type, that same policy should apply to any device accessing the corporate network from wherever that device and user are located. Aerohive seamlessly enables remote access for connected users by using IPsec VPN. Two different IPsec options are available for administrators to use for connecting users, based on whether they wish to deploy full remote networking capabilities at the remote locations or just extend existing corporate networks to a remote branch.

Aerohive Layer 2 IPsec VPN allows an administrator to connect two Aerohive access points and seamlessly extend the existing network to a remote location. The remote access point will bridge traffic from the remote location back to the access point located at the corporate office, and any policies

the administrator has configured for access on that network will apply to users connected from behind that remote access point. This solution is especially useful for devices or applications that require broadcast support on the same virtual LAN to function properly, but does run into scalability challenges if many devices in multiple remote locations are all trying to use the same layer 2 network concurrently.

Another alternative for enabling remote connectivity for users and devices is the Aerohive Branch on Demand solution. The Aerohive branch routers support full layer 3 IPsec VPN as well as edge-based networking, including wired and wireless support for employee and BYOD access. Branch on Demand was designed from the ground up to provide headquarters-like connectivity from any size location, whether it be a retail store, long-term healthcare facility, enterprise branch, or telecommuter.



Besides extending the corporate network to remotely connected users and devices, Aerohive branch routers support full enterprise-class enforcement for BYOD, including client classification and full stateful firewall.

NOW WHAT? Ensuring productivity for connected Users

Now that the administrator has defined the access and authentication permissions and feels reasonably confident that the myriad of devices brought onto the corporate network will be appropriately authenticated and secured, the next and biggest challenge presents itself.

Getting the devices onto the network really isn't breaking news anymore. As you read above, there are many different options to ensure devices are permitted onto the network and integrated or segregated according to the security posture set by the administrator. All networking vendors must have at least one or several solutions for getting BYO devices onto the network securely and easily. Planning and building a network prepared for the onslaught of additional devices is just part of the process now - this is simply table stakes when evaluating a potential networking solution.

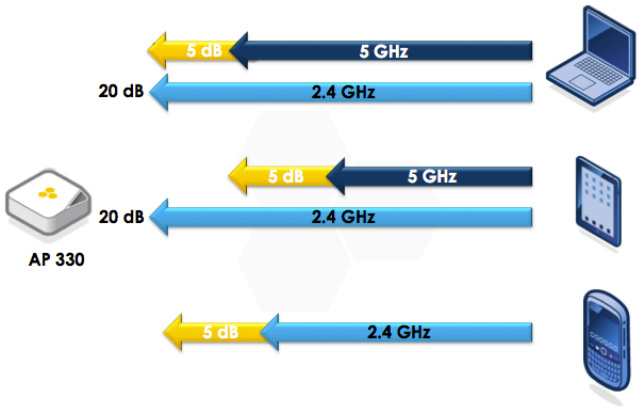
The real drain on IT resources and potentially on the network is what these devices do once they're on the network. If a CIO planned his IT resources to support a single corporate-issued laptop/desktop per user plus a phone and a printer or few per building, and all of a sudden the IT department is slammed with calls about the 3-5 devices per person each user is carrying around, the system becomes overwhelming almost immediately. The desire to allow BYOD and even consumerization of IT – where the IT department distributes consumer-grade devices because of their ease of use and lower cost – quickly becomes outweighed by the potential drain on the available resources. Dealing with the devices once they're on the network is the true test of a robust, scalable, and simpli-fied enterprise networking solution.

Enhanced Connectivity

Getting the devices connected securely to the network is only the first step in a comprehensive solution for mobile devices in the enterprise. Another important aspect is keeping them connected and providing a seamless and productive working experience while they're on the network. Since many of these devices are especially designed for consumer use on a home-network, they are often optimized for enhanced battery life and user experience, rather than the best Wi-Fi transmission/receive capability. Aerohive access points and routers are custom-designed to enhance Wi-Fi experience for consumer grade radios in mobile devices.

One of the most misunderstood aspects of building a Wi-Fi network is focusing purely on access point power to transmit farther and louder. Even if government agencies didn't impose limits on the power a wi-fi radio can transmit, simply increasing the transmit power would only solve half the problem anyway. Even though a client device may hear the AP's high-power transmission, the client device likely can not respond at the same transmission power level, rendering the AP unable to hear the client responses. It is a bit like yelling through a megaphone to someone standing on the other end of a football field – just because the person can hear the sound amplified through the megaphone does not help him shout back loudly enough to be heard also.

Modern access points and routers should be designed to enhance Wi-Fi experience for low transmit-power, consumer-grade devices. Aerohive has custom-designed antenna for our access points that specifically enhance receive sensitivity, which allows Aerohive APs to hear transmissions from lower-power devices, such smart phones and tablets. Enhanced receive sensitivity – as much as 5dBM per band – allows Aerohive devices to receive more quality radio transmissions with many fewer errors, which increases the overall speed of the transmission and lowers the errors and retransmissions.



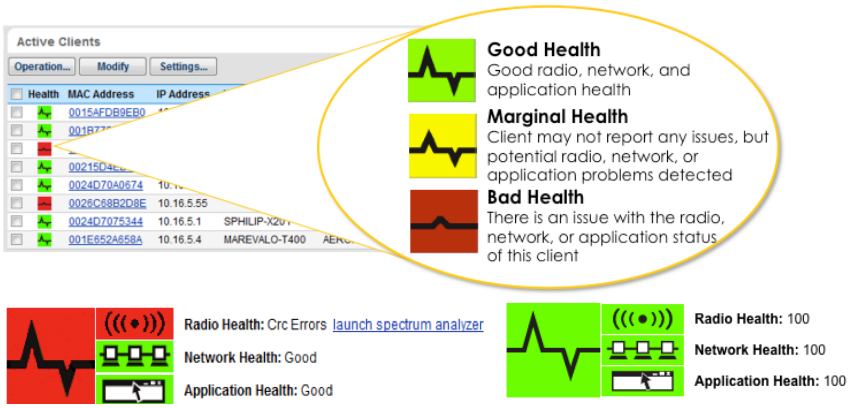
Enhanced receive sensitivity also has the added benefit of making 5Ghz coverage much broader and available to more clients who support the 5Ghz band, which helps to free up the over-used and crowded 2.4Ghz spectrum and allows higher speed radio communication on both spectrums. All in all, more intelligent access points combined with cloud-managed, cooperative control software enhance the Wi-Fi experience on any type of device, consumer-focused or not.

Efficient Management of BYOD

Another common issue that administrators face with all these additional devices on the network is how to manage and monitor them. If the devices have trouble accessing resources, the IT administrator often gets a call where the user is complaining about the network – because it could never be the device's fault, right? Aerohive has several features built into the access points and routers that make this onslaught of devices easier to manage, monitor, and troubleshoot.

Clearly the first step in identifying any problem with attached clients is knowing if there is a problem in the first place. However, while many IT professionals are networking experts, they may not all be radio experts. Translating retransmissions, CRC errors, and selected radio rates may look like Greek to the

average IT administrator. The Aerohive Client Health feature was custom-designed to take the guesswork out of monitoring attached clients. It will determine the best possible transmission speed for an individual client, and then track the statistics and potential issues with that client before displaying a simple green, yellow, or red icon to represent the health of that client. This works for both wireless and wired clients, and also includes information on whether the client radio health or wired connection is satisfactory, but the client is unable to acquire a network address via DHCP or is unable to meet the SLA defined for that particular user. All of this equals an extremely simple and visible way to track any clients – including BYOD.



Just being able to the view what's going on with the clients is certainly useful, but since the real drain on IT will be dealing with any and all issues that do arise with clients on the network, Aerohive has also integrated automatic remediation and mitigation into its products. This allows an administrator to set up a policy for attached clients, with separate policies defined for corporate-issued clients versus BYO/guest devices, and then if client health drops below marginal status, the Aerohive devices can automatically provide additional resources to the ailing client. This includes features such as band steering the client to another supported radio, load balancing the client to another AP, and even boosting the airtime for slow transmissions and avoided retransmissions for that associated client if for some reason it is unable to hit the configured SLA performance target. This allows an administrator to focus on the rest of the problems in the world instead of worrying about all the potential issues with attached clients.

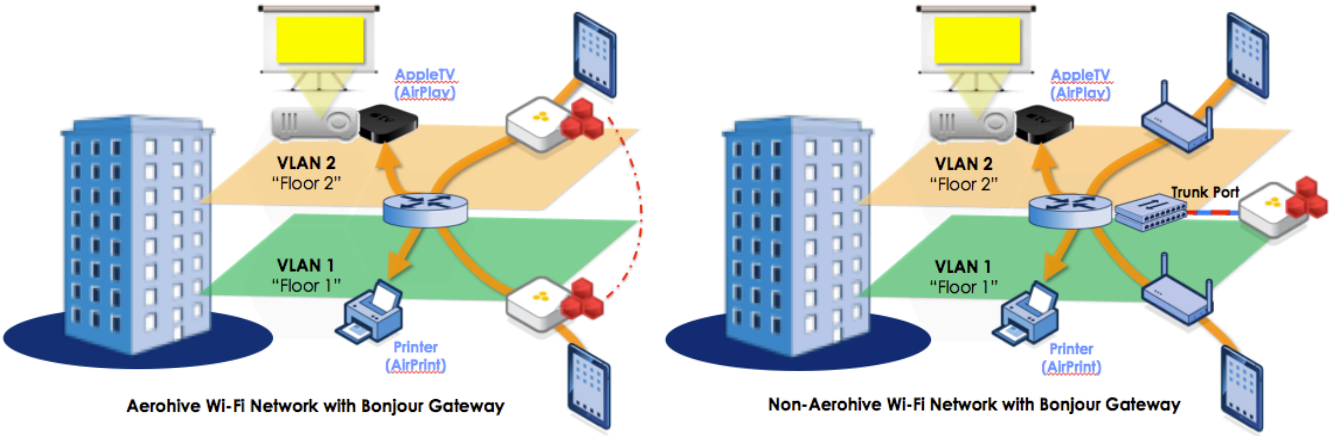
Making BYOD a Productivity Tool

Let's assume for a minute a perfect world where all the attached clients are perfectly connected, the network is working like a dream at full performance, and every single user is perfectly happy with his or her ability to connect any device to the network and get the proper permissions defined by the administrator. Even so, enabling BYOD and especially company-issued consumer devices means users will want to actually use their device to connect and interact with network resources and services. Printing and projecting are two common requests that come up almost immediately, which means another necessary feature for making a BYOD policy successful is a truly service-aware network solution, where the network aids clients in finding necessary resources without requiring IT intervention.

As we look at BYOD in general, one of the statistics that bubbles to the surface almost immediately is that 72% of the devices that users are bringing to the office and expecting to attach to the corporate network are Apple devices.[4] Apple products, and iOS in particular, rely on Bonjour "Zero Configuration" networking in order to find available resources on the network such as printers or Apple TVs attached to projectors. Bonjour is a protocol that relies on multicast DNS (mDNS) to operate, and more details about

[4] Dimensional Research, "Consumerization of IT: A Survey of IT Professionals" 2011

how the protocol works are available in the Bonjour Gateway solution brief[5]. One of the issues with mDNS is that it is limited to a single broadcast domain (virtual LAN). If an administrator has defined a BYOD policy that separates client devices from the corporate network using VLANs, this immediately becomes a hurdle to productive network use. Aerohive has developed the Bonjour Gateway to enable users on any VLAN to see and use Bonjour-enabled resources available on the network, regardless of where those resources reside on the network. Bonjour Gateway can be configured to allow all services through, or limit the advertisement and discovery of Bonjour resources based on identity, location, and device type using the built-in filtering capability.



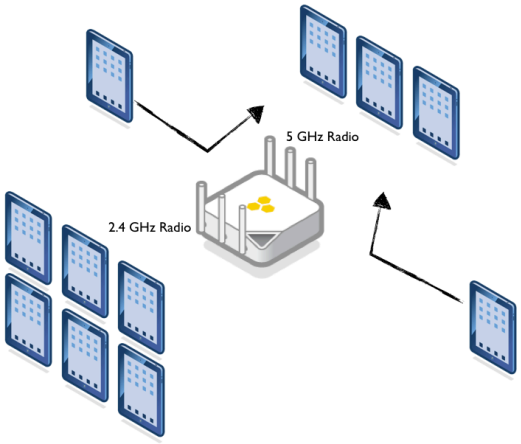
Aerohive's leadership in service-aware networking ensures all devices are productive on the network. In addition, administrators can use built-in DHCP proxies and RADIUS features to continue enabling BYO and corporate-issued devices to attach and use network resources throughout the corporation.

Ensuring the Network is Prepared for BYOD Density

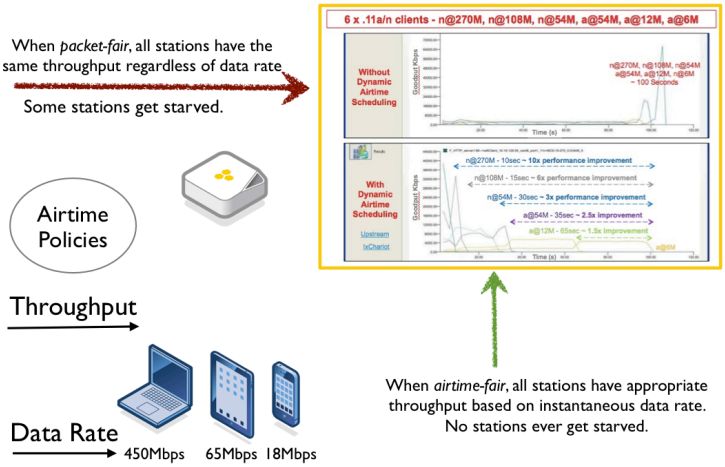
Now that the devices are on the network and functioning as productive clients, the ongoing maintenance of the network comes to mind. Many consumer devices used for BYOD, especially mobile phones, are limited to supporting the 2.4GHz Wi-Fi spectrum. This could wreak havoc in a network that was designed to support fewer clients or is already running at high capacity. Thankfully, Aerohive has developed a bunch of features to help both with high density deployments as well as troubleshooting issues that might arise from an environment where the majority of the devices are competing for airtime.

It's clear from the recent 802.11ac announcements that the 2.4GHz radio spectrum has officially reached its peak. Limited by channel capacity and general over-use by a myriad of Wi-Fi and non-802.11 devices alike, the 2.4GHz will not be joining its 5GHz brother in moving towards gigabit Wi-Fi. However, since many of the devices on the market still support only this band, it's important that Wi-Fi vendors provide adequate functionality to deal with the ever-expanding load on this struggling spectrum. Aerohive has integrated many high density features into HiveOS, including the ability to steer clients who can support 5GHz off the overloaded 2.4GHz spectrum. An important detail about Aerohive, however, is that in the rare case where 2.4 is out-performing 5GHz for whatever reason – interference, overuse, etc – Aerohive is also intelligent enough to steer clients to whichever radio is less burdened. HiveOS can also efficiently load balance client devices across access points in the same Hive, or group of Cooperative Control access points. Even if all your users connect their BYO devices to the network and sit down in auditorium, HiveOS will easily and efficiently balance the clients across the available access points and ensure no one access point is completely overloaded with attached clients.

[5] http://www.aerohive.com/pdfs/Aerohive-Solution_Brief-Bonjour_Gateway.pdf



Another problem often encountered with a high volume of BYO devices is that in order to fairly implement a policy allowing the devices on the network, an administrator can't really limit which devices users might bring to it. It certainly wouldn't be fair if only the people who can afford a new iPad that supports high-speed 802.11n are allowed to attach their devices, so the administrator and network are forced to accept some users may still want to bring in their 802.11b netbook and connect to the wireless network. This means the network must be able to compensate for much slower and less efficient legacy devices. Aerohive's Dynamic Airtime Scheduling automatically detects the maximum speed supported by each associated client based on the client type and distance from the attached access point, and then will balance the airtime between the clients. Gone are the days when one slow client would make the entire wireless network sluggish – HiveOS is constantly monitoring the maximum potential of every associated client and ensures that the network operates at maximum performance and speed. Of course, if any client falls below a defined SLA, HiveOS can also automatically remediate and assign more airtime in order to boost that client performance back into compliance.



Raising the Stakes

All of these features together mean that Aerohive really has changed the game when it comes to enterprise networking. Gone are the days of designing a network purely for enterprise-grade corporate-deployed devices, and Aerohive has made it simple to not only connect consumer grade clients and BYOD, but also actually changed how administrators manage and users operate on the networks these devices are attached to. As more and more devices are added to the network, it is critical that your network solution be able to scale efficiently, secure effectively, and deliver enterprise-class access to all devices, even consumer grade. This will become more and more apparent as mobile devices continue to increase in speed and efficiency, and user expectations of what can be delivered to them anywhere and anytime reach all-time highs.