Aerohive NETWORKS

White Paper

Leveraging Mobility:

How government agencies can boost productivity with bring your own device (BYOD)

Mobility, Productivity, and BYOD

As the popularity of mobile devices shows no sign of waning, an increasing number of government organizations are taking steps to accommodate employees' demands for anytime, anywhere access to wireless networks. The benefits are clear: by embracing today's mobility phenomenon, government agencies can equip employees with the tools they need to work more efficiently, better address the challenges of work-life balance, and enhance job satisfaction.

Many government employees are already reaping the rewards. According to a February 2012 CDW-G Federal Mobility Report, 99 percent of federal IT professionals report they have deployed mobile devices to their agency's workforce. Nearly 90 percent of federal employees who use mobile devices for work report that the technology allows them to be more productive, especially while traveling on agency business and working remotely. And 69 percent believe that increasing mobility will enhance service to citizens.[1]

State and local agencies are also embracing mobility in the workplace. More than 60 percent of state and local IT professionals say their agency has or is developing policies that allow employees to use personally owned devices for work purposes, according to a *Government Technology* survey.[2]

No wonder then that many government agencies are fast embracing wireless as the primary access layer for network connectivity. Take, for example, the U.S. Army, which is moving toward allowing some of its soldiers and Army civilian employees to use their own personal mobile devices at work.[3] And the state of Delaware has launched a BYOD program which could save an estimated $2.5 million in reduced wireless costs.[4]

However, managing mobile devices without an Ethernet port in the workplace presents its fair share of risks. Government employees, contractors, and constituents alike are connecting to networks with a hodgepodge of personal and government-issued devices. Whether owned by the government entity or by the employee, these devices give rise to serious concerns. Public sector IT administrators must now determine things like how much bandwidth is enough? What types of devices might show up? 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 his network is secure, performing highly, and ready for the next wave of new technology, especially gigabit Wi-Fi?

This is the BYOD predicament for government agencies. Efforts to allow employees 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 devices for work activities, and that IT administrators will be overwhelmed by supporting unmanaged devices. And then there are the policy, technical, and legal challenges that, if not addressed properly, could erode the trust of taxpayers, business partners, and fellow government agencies.

This white paper will take government agencies through the necessary connectivity and productivity requirements and explain how Aerohive can help ensure the network is truly ready for the mobility explosion. This will include an overview of the necessary access, authentication, and security options, as well as a focus on how to properly manage devices once they are on the network — one of the most overlooked aspects of a BYOD implementation. Networks should be prepared to make all devices attached to it productive and compliant for a successful BYOD implementation.

Connecting Devices to the Network: Gaining Control of Consumer Devices in the Workplace

Wireless connectivity allows government employees to have mobile access to resources, but it also allows employees to bypass a government organization's secure Trusted Internet Connections (TICs) and connect directly to the Internet. To minimize increased exposure to security and data breaches in a wireless work environment, government organizations need to ensure that connecting public servants to a network remains consistent with NSTIC and Federal Identity Credential and Access Management (ICAM) requirements.

There are really two major camps when it comes to ensuring mobile devices are accessing the network securely. On one side, deploying agent-based Mobile Device Management solutions ensures connected devices have the

right software, permissions, and security settings before being connected to the network. 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 government agencies to leverage and control consumer devices in the workplace, 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 focuses 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.

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.). That's an enormous help to today's time-strapped, resource-limited government agencies. Rather than serve as a resource drain, Aerohive Cooperative Control transforms BYOD into a productivity enhancement tool for faster decision-making and seamless management. Following are advanced feature functions that help ensure government agencies are securely and efficiently connecting devices to the network.

Authentication and Access

Before BYO devices get onto a network, there are several 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 the patent-pending Private Pre-Shared Key feature. This feature 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 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 (WPA-Enterprise) solutions, but works on all devices that support PSK and requires no certificates.

But it's not enough for a government agency to simply secure devices. IT administrators must also ensure that a network is only accessed by authorized employees and that employees authenticate their identity before gaining access. That's because government agencies house all types of sensitive and confidential data, from employee records to citizens' personally identifiable information. Keeping these data sources secure means carefully managing access while still ensuring transparency to authorized users.

One of the most common secure network types is to configure WPA2-Enterprise (802.1X) on a government SSID, which requires at least a username/password combination and acceptance of a server certificate in order to authenticate. Unless an administrator takes an extreme stance and requires that every single device connected to

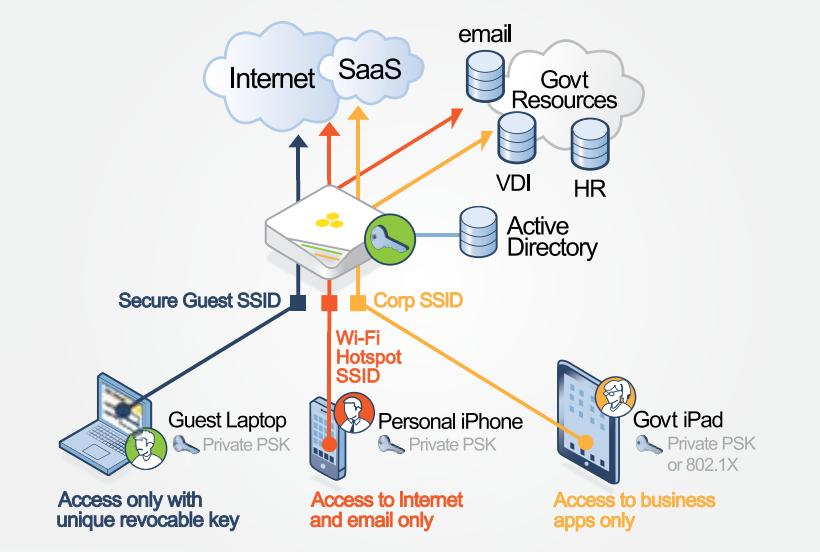
this network also has a certificate installed on it (not only a huge administrative burden but sometimes impossible based on the device support), modern mobile devices have made it as easy as checking the "accept" button and entering network credentials to connect a BYO device to this type of secure network. Aerohive devices inherently support WPA2-Enterprise and can even perform the authentication server function as well.

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. By failing to enforce these guidelines, government agencies risk exposing sensitive data such as email, employee records, citizens' personally identifiable information, and any other applications employees access via mobile devices.

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.

AEROHIVE POLICY ENFORCEMENT: ASSIGNING A USER PROFILE TO A CONNECTED DEVICE



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. In fact, 68 percent of federal IT professionals who have implemented MDM cite improved security as the top benefit, according to the CDW-G Federal Mobility Report.[5]

NMDM 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, and enforce different policies for users based on device context and identity, rather than just making a blanket policy for all attached iPads.

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. As a result, administrators can ensure security the moment traffic first enters a network rather than watch it traverse the entire infrastructure before finally being restricted.

Another common way to enforce segregation of traffic is by using layer 3 tunneling features. By connecting different virtual LANs throughout a campus, a government agency can enable seamless roaming, as well as force a roam based on identity and device type. For example, rather than take the time configuring a guest VLAN, an administrator can define a policy so that BYO devices are automatically tunneled to a particular access point. This simplifies the network configuration, but still ensures that BYO devices are completely segregated from the network.

Managing Devices on the Network:
Ensuring Connected Users Make Significant Productivity Gains

Now that the administrator has defined the access and authentication permissions and feels reasonably confident that devices brought onto the government agency network will be appropriately authenticated and secured, the next and biggest challenge presents itself — managing devices once they are on the network.

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. But the real drain on IT resources and potentially on the network is what these devices do once they're on the network. For example, IT resources configured to support a single government-issued laptop per employee will easily become overwhelmed once personal handheld devices are added to the mix. 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 simplified networking solution, and Aerohive helps ensure this transition is seamless.

Enhancing Connectivity

Getting the devices connected securely to the network is only the first step in a comprehensive solution for mobile devices in the public sector. Another important aspect is keeping them connected and providing a seamless and productive working experience while they're on the network. Since many devices are 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 (APs) and routers are custom-designed to enhance the 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.

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. Modern APs and routers should be designed to enhance the Wi-Fi experience for low transmit power, consumer-grade devices. Aerohive has custom-designed antennas for the APs that specifically enhance receive sensitivity, which allows Aerohive APs to hear

CONNECTING REMOTE USERS

With its promises of cost savings and improved performance, telework is an increasingly popular strategy for government. In fact, a study by the Telework Research Network claims that potential savings for the federal government could reach nearly $3.8 billion as a result of reduced real estate costs, electricity savings, reduced absenteeism, and reduced employee turnover.[6] That's all the more reason for government agencies to ensure that employees can remain connected to essential resources, regardless of where they are.

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:

Aerohive Layer 2 IPsec VPN:
This option allows an administrator to connect two Aerohive access points and seamlessly extend the existing network to a remote location. 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.

Aerohive Branch on Demand:
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 federal department or municipal office.

transmissions from lower power devices, such as smartphones and tablets. Enhanced receive sensitivity — as much as 5dBM per band — allows Aerohive devices to receive more quality radio transmissions with fewer errors, which increases the overall speed of the transmission. More intelligent APs combined with cloud-managed, cooperative control software enhance the Wi-Fi experience on any type of device, consumer-focused or not.

Improving Management Efficiency

Another common issue that government agencies face with additional devices on the network is how to manage and monitor them. The more consumer devices connected to a government agency's network, the greater the need for enhanced monitoring, management, and security.

Fortunately, Aerohive has several features built into the access points and routers that make this onslaught of devices easier to manage, monitor, and troubleshoot. 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 a foreign language 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 client's health. This works for both wireless and wired clients, and also includes information on whether the client radio health or wired connection is satisfactory, if the client is unable to acquire a network address via DHCP, or is unable to meet the SLA defined for that particular user. This is an extremely simple and visible way to track any client.

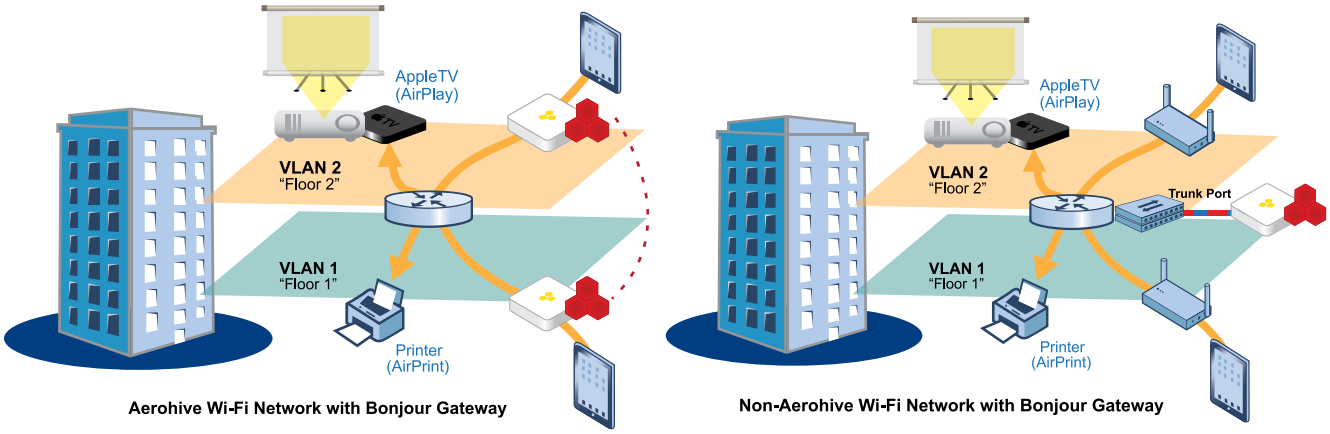
Aerohive has also integrated automatic remediation and mitigation into its products. This allows an administrator to set up a policy for attached clients, with separate policies defined for government-issued clients versus BYO/guest devices so that administrators can better prioritize which devices receive the necessary resources. 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 higher-level tasks instead of worrying about all the potential issues with attached clients.

Increasing Productivity

By enabling BYOD, a government agency can enhance employee satisfaction, foster loyalty among workers, facilitate faster communication and better accommodate remote access — all important drivers of increased productivity.

Embracing BYOD, however, requires supporting some of today's most popular devices which in the past has challenged productivity. Many devices that government employees expect to attach to the network are Apple devices. 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. 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 government 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.



Preparing the Network for Density

Now that the devices are on the network and functioning as productive clients, the ongoing maintenance of the network becomes important. 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. Fortunately, Aerohive has developed features to help 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.

To address the ever-expanding load on today's struggling 2.4GHz 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. In the rare case where 2.4 is outperforming 5GHz — because of 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 employees connect their BYO devices to the network, 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.

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. Moreover, HiveOS is constantly monitoring the maximum potential of every associated client and ensures that the network operates at maximum performance and speed.

The Future of BYOD in Government

BYOD demand in government is only just beginning. For agencies that are prepared, this high-tech trend promises to deliver enormous productivity gains as employees and constituents alike turn to consumer devices for faster communication, remote access, and increased efficiencies.

Fortunately, Aerohive has made it simple to not only connect consumer grade clients and BYOD, but has also changed how administrators manage and employees operate on the networks these devices are attached to. As more devices are added to the network, it is critical that the network solution be able to scale efficiently and deliver secure and reliable access to all devices, even consumer grade. This will become more apparent as mobile devices continue to increase in speed and efficiency, and workers' expectations of what can be delivered to them anywhere and anytime

reach all-time highs. Being able to meet these expectations with the right authentication, access, security, and network solutions is the only way to allow employees to bring their own devices to work to improve productivity without sacrificing security.

Aerohive's Cooperative Control architecture allows an administrator to build a network designed for today's devices as well as tomorrow's, making your investment truly future-proof and ready for the next wave of highly mobile users and devices. Our custom-designed, service-aware network infrastructure will ensure high-performance networking whether you're connecting a decade-old scanner or the latest 802.11ac gigabit Wi-Fi client. Aerohive cloud-enabled networks with distributed intelligence provide inherent network-based mobile device management, corral the BYOD explosion, and simplify the very complex government network problem of how to deal with high-speed smart mobile devices.

Take a minute to learn about Aerohive's Cooperative Control architecture and market-leading features for enabling productive Wi-Fi use by visiting us at www.aerohive.com. Also learn more about BYOD and the consumerization of IT and its impact on government networking. Sign up for a demo and build your own plan to redesign your network for the next step in enabling the smart device explosion. Hive On!

Endnotes

1. http://webobjects.cdw.com/webobjects/media/pdf/CDWG-Federal-Mobility-Report-020712.pdf
2. www.govtech.com/policy-management/BYOD-Policies-Expand-State-Local-Agencies.html
3. www.informationweek.com/government/mobile/us-army-plots-bring-your-own-device-stra/232601375
4. http://fcw.com/articles/2012/08/23/steven-vanroekel-digital-gov-milestones.aspx
5. http://webobjects.cdw.com/webobjects/media/pdf/CDWG-Federal-Mobility-Report-020712.pdf
6. www.federalnewsradio.com/163/2412827/A-Conversation-on-Implementing-Telework

About Aerohive

Aerohive Networks reduces the cost and complexity of today's networks with cloud-enabled, distributed Wi-Fi and routing solutions for enterprises and medium sized companies including branch offices and teleworkers. Aerohive's award-winning cooperative control Wi-Fi architecture, public or private cloud-enabled network management, routing and VPN solutions eliminate costly controllers and single points of failure. This gives its customers mission critical reliability with granular security and policy enforcement and the ability to start small and expand without limitations. Aerohive was founded in 2006 and is headquartered in Sunnyvale, Calif. The company's investors include Kleiner Perkins Caufield & Byers, Lightspeed Venture Partners, Northern Light Venture Capital and New Enterprise Associates, Inc. (NEA).

Aerohive™ NETWORKS