



2018

ENTERPRISE WI-FI BUYER'S GUIDE

How to Deploy Adaptable, Scalable
and Cost-Effective Connectivity

CONTENTS

It's a Wireless-First World	3
Key Considerations	4
Planning - Setting Expectations	5
The Need for Speed	5
Architecture - Cloud, Controllers & Distributed Control	7
Management - From Deployment to Support	9
Security - Personalized Access	10
Applications and Insights	13
Summary	13

IT'S A WIRELESS- FIRST WORLD

You may have noticed one or two, or realistically speaking maybe several thousand more mobile devices within your environment in the last few years, and as you are all too aware, it's things like tablets and smartphones that account for this surge. Pick any typical office and it is reasonable to expect 2-3 devices per person, with an employee simultaneously hosting a web meeting on their corporate laptop, sending an email from their tablet, and sneakily watching a hot new YouTube video on their phone. As a result, we have now surpassed the tipping point where mobile devices outnumber human beings on the planet, and as the world becomes ever increasingly connected, there are no signs of slow down ahead.

Today, you are most likely dealing with laptops, smartphones, and tablets for corporate, guest, and BYOD access, but as IoT continues to grow to become more than a buzz word, organizations will find a rapidly increasing number of machine-based systems and sensors that require network connectivity as well. Just as top down pressure from executives caused the rise of consumer grade tablets in the workplace, it will be the facilities, logistics, and security departments that will request, or politely demand, network access for their shiny new systems including building controls, surveillance systems, HVAC, and lighting sensors and switches.

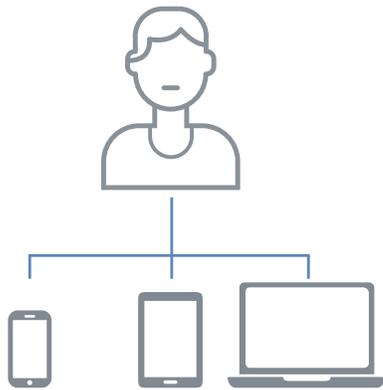
2018 OUTLOOK

Connectivity is an expectation today, and with the rise of Wi-Fi enabled devices entering our organizations, we need to ensure that we have sufficient bandwidth; can scale and adapt as required; have appropriate network security; and have a central point of visibility and management; all while keeping cost and complexity to a minimum. 2018 will offer solutions to all of these requirements as we see market shifts including increased 11ac Wave 2 adoption; a large transition from centralized to distributed control architectures; and the continued rise of Cloud Networking and software defined architectures.

This guide will provide you with the information and key questions to take to every vendor to ensure that you are getting a solution that is tailored to your own needs through 2018 and beyond.

KEY CONSIDERATIONS

Wi-Fi has unequivocally become the medium of choice for network access for most organizations today, and it is therefore crucial that any wireless-first workplace has the right infrastructure in place. Conversations with vendors will typically include coverage; capacity; security; management; scalability; and investment protection. Even if you only require basic connectivity today, it is important to determine what the complete vendor offering looks like, so that you can easily add new functionality as your business needs evolve. This section will highlight some of your key discussion points with your vendor to ensure maximum value is achieved.



ENSURING CAPACITY FOR THE GROWING NUMBER OF DEVICES

ENSURING CAPACITY FOR THE GROWING NUMBER OF DEVICES

With the network witnessing continually increasing demand for access by a wider range of devices, bandwidth is crucial. 802.11ac has unlocked theoretical speeds of Gigabit and beyond, but is that enough? As we explore the various implementations of WLAN architecture and performance optimization features, we will help you determine how to realize the true potential of your infrastructure, and protect future growth within a single site or across multiple geographic locations.

GUARANTEEING NETWORK UPTIME

9 out of 10 organizations consider the use of mobile devices to be either critical or very important to their business processes and productivity; therefore the supporting infrastructure must be rock solid, otherwise there is a significant impact to the business. How quickly can your infrastructure and organization recover from service outage or reduced productivity?

FLEXIBILITY VS. SECURITY

To cope with the influx of devices, IT departments are balancing flexibility against security in order to meet business needs. There is top down pressure to enable productivity and efficiency, and mobility is a key part of this, however for IT to get the job done, the highest levels of security that should be implemented are often neglected in favor of flexibility.

VISIBILITY OF USERS, DEVICES, AND APPLICATIONS

If your doors are open to BYOD, guest, and IoT devices, it may not always be clear who exactly is on the network, which devices they are connecting with, what applications are being accessed, and where they are located. Selecting an appropriate management platform is crucial to providing comprehensive visibility and control.

RETURN ON INVESTMENT

Wi-Fi offers a unique opportunity to better connect with people through their mobile device, and provide connectivity for network connected systems and sensors that enable intelligent buildings or security systems, all of which can leverage cloud-based analytics engines and applications to increase business intelligence. As organizations seek to increase engagement, productivity, and cost savings, these capabilities will become a key part of the WLAN selection criteria for organizations in 2018 and beyond.

PLANNING SETTING EXPECTATIONS

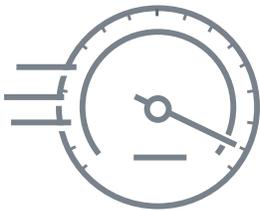
Whether 2018 holds upgrades or expansions for your organization, the number one rule for a successful deployment is to not skimp on the planning. The first step is defining your requirements and understanding the demand on the network. This has to be viewed from both a budgetary and technical perspective. It is crucial to advise your vendor on your exact requirements so that accurate access point locations and quantities can be determined. Do you need 100% wireless coverage? What devices are you supporting? Laptops, tablets, smart phones and other mobile devices? How about services and applications; do you intend to run voice, video, and other latency sensitive apps? And do you require your network to have guaranteed uptime and availability? Providing the answers to these questions will help shape a clear bill of materials for your organization.

It is predicted that there will be over 50 billion devices connected to networks by 2020, the vast majority using wireless. How are you planning for these devices in your network? Many Wi-Fi networks are not properly designed to deliver on the capacity requirement enterprises will face with the explosion of corporate, BYOD, guest, and IoT access requirements. To assist with your planning, there are various *predictive* planning tools available today that will reduce the amount of time and effort involved with WLAN design. Don't be fooled though, these tools are called predictive for a reason, and may only focus on coverage, rather than capacity, which is a far more important measure than your access point count.

Every environment is different, and nothing beats a good old-fashioned on-site survey to guarantee the success of your network. That said, in a very simplistic environment, an online survey will provide a highly accurate picture, however a validation survey should be performed in order to sample certain areas and confirm the predicted results.

During your site survey, ensure that your vendor is performing a spectrum analysis. Spectrum analysis checks your environment for non-RF interference, including microwaves, radar, cameras, and other devices that operate on either the 2.4GHz or 5GHz frequencies. Failure to identify potential sources of interference could be highly detrimental to the operation of your wireless network. WLAN solutions that support integrated spectrum analyzers can be highly beneficial to monitor any changes in your environment once deployed.

THE NEED FOR SPEED



With proper planning, you should have an accurate idea of the number and type of access points required for your environment. For the first half of 2018, 802.11ac Wave 2 will remain as the incumbent standard for speed gains, the latest option with theoretical bandwidth over 1 Gbps. However, towards the middle of 2018, a new standard – 802.11ax – will be released that focuses primarily on efficiency gains.

Buying the “latest and greatest” access points is certainly important to some, but you can go to your local PC store and pick up the newest access point for a low cost, so what's the difference between the SoHo and 'enterprise' WLAN solutions, if the advertised bandwidth is the same? The difference is how that bandwidth is managed and provisioned.

SO WHAT SHOULD I LOOK FOR?

Bandwidth management is achieved in various forms, but overall, you should be asking your vendor for the following:

SOFTWARE DEFINED RADIOS

The 2.4GHz frequency band has limited capacity and high interference with only 3 non-overlapping channels. The 5GHz frequency band has roughly 7x the bandwidth of the 2.4GHz band with less RF and Wi-Fi interference. Because of spectrum congestion on the 2.4GHz band, you will undoubtedly face interference in a high capacity deployment. To increase performance, in many cases it is actually recommended that you TURN OFF the 2.4GHz radio in 2/3 of your deployed access points. Recognizing these issues, but also

knowing that 2.4GHz must still be supported in a more limited capacity, some vendors have implemented dual 5GHz capable radios within their access points, with the ability to configure one of the radios between 2.4GHz and 5GHz. With a software selectable dual 5GHz band access point, you have the ability to switch the 2.4GHz radio into a second 5GHz radio. With this advancement, you can instantly deploy dual 5GHz access points in high capacity areas, or in the areas where you would otherwise disable the 2.4GHz radio, convert it to a 5GHz radio. This maximizes your investment both today and in the future, without needing to rip and replace devices; allowing for flexibility, better network efficiency, and optimal Wi-Fi design.

LOAD BALANCING & BAND STEERING

As an absolute minimum, WLAN solutions must be able to identify overcrowded access points or radios, and take action. Load balancing ensures that if an access point is carrying a high number of clients, and there is an underutilized access point nearby, the clients can be redistributed and balanced across the two access points. Band steering is a similar principle to load balancing, but it occurs within a single access point that has two radios. Commonly, mobile devices are equipped with both a 2.4GHz and 5GHz radio, and are programmed to favor one radio over the other. That could leave a situation where many devices are connecting to 'radio 1', and only a handful on 'radio 2'. In a situation such as this, band steering will take charge and ensure that your two radio access point is being fully balanced and utilized.

L2/L3 FAST SECURE ROAMING

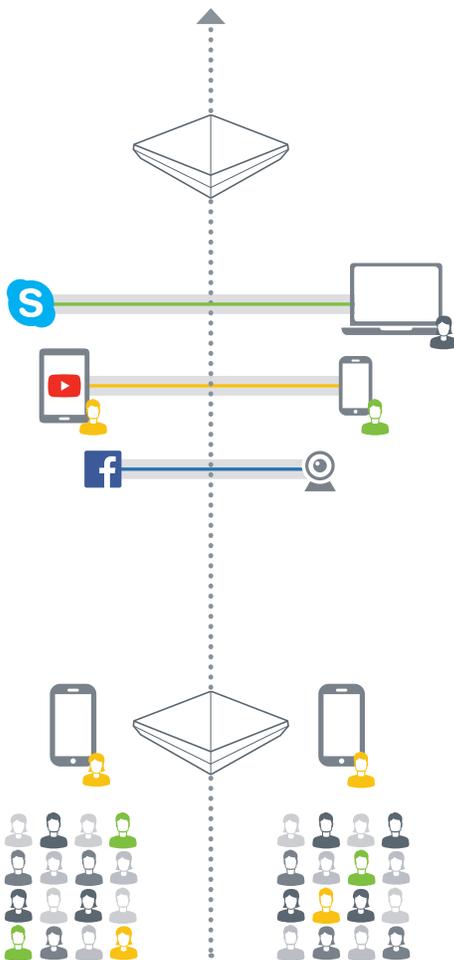
With more users and devices on the move, and many organizations enabling voice and video services over Wi-Fi, it is imperative that handoff between one access point to the next is seamless. Most WLAN solutions on the market support fast roaming handoff within layer 2 domains, however if your access points are spread across multiple VLANs, check how your vendor copes with (if at all) supporting a seamless handover between one VLAN to the next. Typically, this will require a GRE tunnel between controllers or access points in the different VLANs that allow a client to maintain their original IP address until they have finished transmitting data, then the tunnel will be torn down and the client will establish an IP address in the new VLAN. Without Layer 3 roaming capabilities, the client may lose its connection, which could be highly problematic in areas where clients are on the border between the two VLANs.

DYNAMIC AIRTIME SCHEDULING & SLA'S

In a mixed client environment, older clients may slow down the performance of newer devices. SLA's allow you to set a minimum targeted throughput level for certain device types, and if they are not met, a boost can be given through Dynamic Airtime Scheduling to push it up the priority queue. Dynamic Airtime Scheduling also looks at the overall client landscape and can intelligently re-order the data transmissions of clients to improve the performance of newer devices such as .11ac/n, without actually impacting the performance of legacy .11b/g/a devices.

CONTEXT-BASED QOS

While bandwidth optimization features such as band steering and load balancing maintain general order within your network, there are often user, device, or application groups that you want to prioritize, restrict, or even ban altogether. Context-based access, which we will talk about in the security section, enables the identification of your users, devices, and applications. Once identified, you can set different



CONTEXT-BASED QOS

levels of access and service quality for each. For performance, this means that you can assign more bandwidth to your staff over guests; staff-owned devices over BYOD; or voice and video apps over gaming apps; it also allows the throttling or banning of illegal or bandwidth intensive apps including software updates and torrents.

ARCHITECTURE CLOUD, CONTROLLERS & DISTRIBUTED CONTROL

As the WLAN standards evolve to support faster data rates, so too does the underpinning infrastructure. Back in the late 90's when Wi-Fi was in its infancy, access points operated independently of each other. Although they would share common settings such as SSID, in terms of fast roaming, load balancing, RF coordination etc., there was no communication or data sharing between access points. In the 2000's when Wi-Fi became mainstream, a control plane was required if Wi-Fi were to survive as an enterprise-grade technology. With chipset costs at a premium, the WLAN controller was created to centralize the control plane and provide a smarter, coordinated solution. Although WLAN controllers are still widely used today, there is a stronger emphasis on cloud-enabled solutions, and de-centralizing the control plane to the edge of the network. Let's look at the various options available today.

CONTROL PLANE SUMMARY

The control plane is the set of real-time operations within the infrastructure, such as controlling connections, disseminating connectivity information, and calculating optimal path. In Wi-Fi this can include RF management, roaming, load balancing, mesh, policy enforcement and many more critical operations. A shared control plane in any infrastructure system can be achieved in either of two ways: centralized or distributed. In both switching and routing, the control plane is distributed, operated by protocols (e.g. spanning tree, OSPF) between intelligent devices. In the past, the control plane in Wi-Fi technologies was centralized, but this has changed in the last few years with some of the major WLAN vendors offering a distributed control plane model.

ARCHITECTURE ADVANCEMENTS

"WLAN controllers were purely an economic decision at the time. To place greater processing power into the access points themselves was simply cost prohibitive." – Bob O'Hara, inventor of the WLAN Controller.

At the time of their creation, controllers eased the management and security headaches that non-pervasive networks comprised of autonomous access points would cause. Today however, with the increased reliance on Wi-Fi, expanding networks and increased performance requirements, the centralized model has severe architectural limitations, including data bottlenecks, scalability, reliance, and unnecessary cost.

Recognizing some of the shortfalls of the fully centralized controller model, vendors began to adapt their solutions through virtualization and portfolio integration. Virtualization provided increased scalability as the host's processor, memory, and network interfaces could be increased as required. This model also placed some of the intelligence back into the access points, along with the introduction of local data forwarding. Alternative offerings included the embedding of the controller within access layer switches, firewalls, and other networking solutions, which helped to reduce solution components. For smaller deployments, an access point within a cluster could also act as a controller for a group of local access points.

While these hybrid models offer increased deployment flexibility, there are some tradeoffs to be aware of. The reality is that most vendors were attempting to retrofit their controller architecture to deal with a more modern day network. With the controller still acting as the brain of the network, if local data forwarding was enabled, organizations would be sacrificing the usage of some important features, such as QoS and firewall policies, as they required user traffic to pass through the controller.

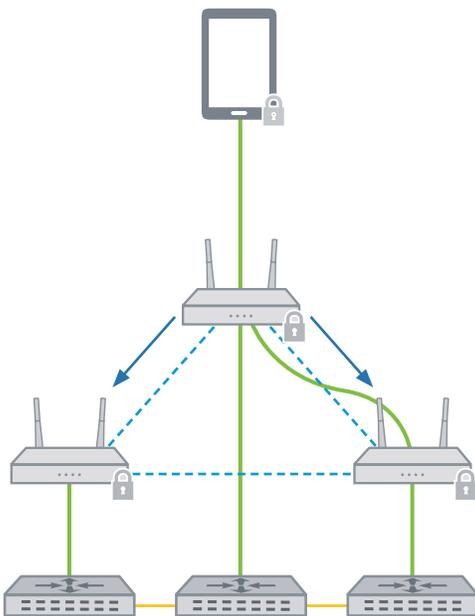


Figure 2: Distributed Controller Architecture

Solutions that integrated controller functionality into the access points would also struggle over a certain number of connected access points, given a single access point has nowhere near the processing power of a dedicated appliance (physical or virtual).

Hybrid solutions are still used by many vendors today as they are bound to their legacy architecture, having invested so heavily in the technology, however most are slowly moving away.

CLOUD CONTROLLERS

In recent years, the cloud has proved popular with organizations looking to centralize software services and reduce costs. With access points having less reliance on controllers for features and functions, some WLAN vendors provide hosted controller services as an annual payment plan, giving organizations more flexibility with their budgeting.

Commercially this model works for many, however technically there are still limitations. Ultimately the solution still utilizes a controller, and the access points still depend on the controller for certain functions, therefore if connectivity is lost between the two, organizations will face an impacted service, from user connectivity to security policies and enforcement. Additionally, although organizations purchase their hardware outright, if they forget to renew their controller license or support, then their wireless network will cease to operate, which is a major pain point for many organizations.

When evaluating solutions of this kind, it is imperative that organizations ascertain from the vendors what exactly will happen if-- 1. access points lose connectivity to the cloud and 2. what happens if the cloud controller license expires.

DISTRIBUTED CONTROL WITH CLOUD MANAGEMENT

Leveraging the increased processing power of today's chipsets, combined with a control plane protocol similar to OSPF and STP used in switching and routing, it has now become possible to create a fully distributed control plane, thus eliminating the need for a dedicated wireless LAN controller entirely, whether physical, virtual, or cloud-based, while maintaining a centralized management plane.

Fully distributing the control plane achieves three main benefits:

- **Operational Simplicity** - Using a distributed control plane is inherently resilient and allows the WLAN devices to self-organize and integrate directly into the access architecture, enforcing security policy before WLAN traffic ever traverses the wired LAN.
- **Scalability and Flexibility** - With every access point or networking device participating in the processing of data, much like a grid computer, the network can provide full functionality to any deployment regardless of size. Every device added to the network increases not only the coverage, but also the total compute capacity of the network.
- **Cost Savings** - By removing controller hardware, software, and licensing, dramatic cost savings can be realized without losing functionality.

Fully distributed control and data planes are essential for a mobile-first network, however the management plane plays a key role in the deployment and support of the wireless LAN and should remain centralized.

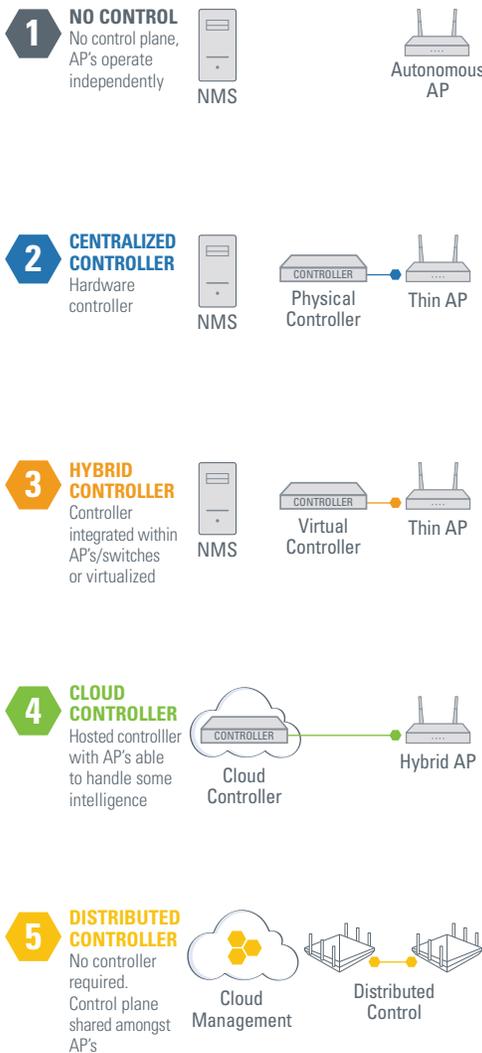


Figure 3: Five Generations of Wi-Fi Architecture

MANAGEMENT FROM DEPLOYMENT TO SUPPORT

Once you know which access points you will install, you must then consider how you will deploy and support them. As wireless networks increase in complexity, IT departments are searching for solutions that remove the need to become an RF guru to deploy and manage their Wi-Fi. There is little need for CLI with modern WLAN solutions, with most vendors offering a management platform to centralize the configuration and support of networks. If your vendor is proposing WLAN controllers, ensure that management is included within the proposal, as vendors may neglect to initially include management in an attempt to mask additional cost. The cloud is becoming a popular method for WLAN management as it offers additional flexibility, both technically and commercially while still offering a centralized management view.

Having a centralized management platform makes the deployment, visibility, and support of your network much simpler, especially if you have multiple locations. When investigating various solutions, determine if public and private cloud, and on-premises options are available to meet your needs, and challenge the vendor to demonstrate the following:

- **Planning** – How to import floor plans and perform a predictive survey, and use those plans for a live environment to report coverage, client locations, access point status etc.
- **Provisioning** – What is the process to connect an access point and configure features, both basic and advanced? What level of expertise is required to learn the interface; novice or 500-page manual with a week of training?
- **Unified Policies** – Does the platform support additional devices such as switches and routers, and how straightforward is it to configure consistent policies? Does the solution have the ability to manage 3rd party devices?
- **Visibility** – How granular is the visibility and reporting offered? Is historical data available? Is it possible to search within the system? Are customizable dashboards available? Can you anonymously and dynamically compare infrastructure and client metrics to similar-sized deployments and/or industries?
- **Support** – What happens if we have a problem? How would I go about troubleshooting a problematic client? What tools are included for troubleshooting?

Ah, the never ending fun of keeping your network secure. There is a delicate balance between security and maintaining usability to avoid making network access unnecessarily complex for your legitimate users. With a range of devices to support, IT departments are looking for a simple way to on-board and secure both staff-owned and personal devices, including BYOD, guest, and peripherals. However, simple and secure are not two words that are typically associated.

IT departments are also looking for context – understanding who is connected, what devices they can connect with, which apps they attempt to use, and where they are located. Mobility has changed the way we approach network security at the access layer, and context is key to a successful deployment.

PROVIDING ACCESS TO ONLY THOSE THAT SHOULD HAVE IT

When you think about Wi-Fi, one of the most important considerations is of course network security. Over the years, WLAN security has evolved far beyond basic authentication and encryption. As more devices go mobile, and different use cases arise, extra border controls must be put into place. In a simplistic view there are two main things that you want to achieve 1. Making sure that only the right people and devices have access and 2. Once they are in, making sure that they behave themselves. Let's start with number 1.

WHO'S ON THE GUEST LIST?

Before anything else, authentication comes first, and if it isn't done right, you can forget reading the rest of this section. Before we determine which authentication method to use, we first need to determine who you want to be able to access the network. In most organizations, there is a growing demand for corporate, guest, BYOD, and peripheral device connectivity.

- **Corporate Owned** – Usually centrally controlled and administered. The IT department has easier access to these devices and in many cases can push configurations and settings remotely.
- **BYOD** – For consumer devices owned by the employees, MDM (Mobile Device Management) can be implemented to maintain some order, however for personal BYOD, staff members want to be able to access the network, without having to jump through too many hoops.
- **Guest** – With a growing expectation from your visitors that they will receive Internet access, there are various methods that can be used to secure and administer guest connectivity. For the user, access must be very simple, but in the backend there must be controls in place to prevent guests from accessing certain areas of the network.
- **IoT** – An increase of network connected 'things' ranging from Apple TV's and printers, to light bulbs, surveillance, HVAC systems etc., means that IT departments face a new wave of security challenges.

In an ideal scenario, we would implement 802.1X (RADIUS based authentication) for every device, however, for some of the above use cases, this may not be possible. Corporate devices are straightforward, they are centrally managed, and using tools such as Group Policy or MDM, 802.1X settings can be configured remotely. However, for personal BYOD, guest, and IoT devices, the IT department may not have the access or rights to install certificates, or the devices may not actually support 802.1X in the first place.

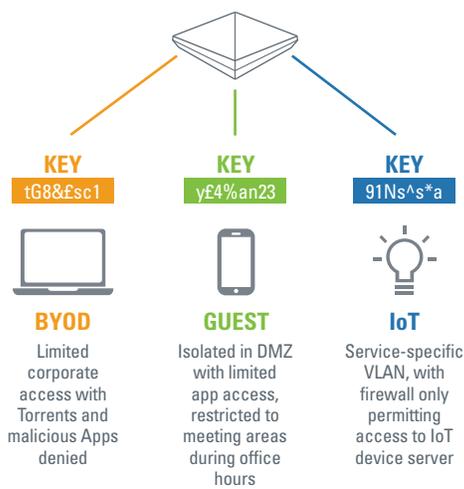


Figure 4: Example benefit of private pre-shared key

Typically, the only alternative would be to use a basic captive portal for guests, or PSK (Pre-Shared Key) for the devices that don't support 802.1X, neither of which are particularly compelling for the security conscious organization. While PSK still authenticates users, every device shares a common password, which prevents context-based access that we will discuss shortly, and if the key becomes compromised, you face an administrative headache. There is hope though; an authentication method that an increasing number of vendors are adopting is 'Private' Pre-Shared Key (PPSK). PPSK's are unique pre-shared keys created for individual users or devices on the same SSID. They offer the key uniqueness and policy flexibility that 802.1X provides, with the simplicity of pre-shared keys, without any of the inherent drawbacks. As the keys are still industry standard WPA2-AES keys, they are compatible with any device that supports PSK today, requiring no additional software to be installed on the client device. For the user, PPSK's are a simple method of accessing the network, and for the administrators, they have the confidence that every device has been uniquely identified.

THE IMPORTANCE OF CONTEXT-BASED ACCESS

We have already discussed the importance of authentication and its role in preventing access to unauthorized users and devices, however your first line of security is an enabler of a powerful second wave of defense: context-based access controls. Unbeknown to the user who simply clicks and connects to the network, there are powerful security services that can run in the background of your wireless infrastructure. Once a user has entered their 802.1X (Typically AD) or PPSK credentials, the WLAN infrastructure will analyze every detail of this user, and assign a user profile based on their role within the organization. A user profile typically controls the following:

- **Device Availability** – Although the user has been granted access, it is also important to validate the device that they are connecting with. If, for example, the user is using corporate credentials on their personal device, the access points can either restrict or block access.
- **VLAN Assignment** – To prevent the creation of multiple SSID's for each department, everyone can connect to a single SSID, and based on their identity, can be placed into separate VLAN's through the user profile.
- **Firewall & Application Access** – Limit the access a user or device has to applications and particular parts of the network, using integrated DPI Layer 2-7 firewalls within the access points.
- **Time of Day Access** – Limit the time of day certain groups of users or devices can access the network. This can be useful to prevent guest access outside of working hours for example.
- **Location Access** – In some cases, organizations may want to prevent mobile access for highly secure areas.
- **Bandwidth Allocation (QoS)** – Set minimum and maximum performance levels per user, device, or application, to prevent (for example) BYOD devices streaming cat videos and consuming your bandwidth.
- **Tunnel Policy** – VPN or GRE tunnel policies can be created to segregate the traffic of users to an isolated DMZ or other part of the network; this is a common practice for guest networks.
- **Device Enrollment** – As BYOD becomes more prevalent, the WLAN infrastructure can integrate with MDM servers and redirect unenrolled devices to a registration page where they can download the MDM profile. Until the profile is installed, the access points will quarantine the device.

Auth Type	PPSK	Social Login	ID Manager	Active Directory
Unique Identity	IoT device	Sarah - Guest	Emma - BYOD	Stephen - Corp Device
Time of Day Access	24 Hr	9-5	7-9	24 Hr
VLAN assignment	1	DMZ	2	3
Layer 7 DPI firewall	Specific server only	Limited Web	No Torrents	Corp Apps
Bandwidth	Low	Very Low	Medium	High

Figure 5: Context-Based Access Profiles Example

Context-based access policies ensure that the network is used as intended, and prevents abuse. Remember, without identity (obtained through the authentication phase), your policy granularity will be restricted. Each vendor provides different policy capabilities, so it is important to clarify both what is achievable and how granular the policies are. Secondly, and crucially, understand what functionality is included within the controller (if required as part of the solution) or access points natively, and which functionality requires additional licenses or additional hardware/software appliances. Covering these bases at the beginning will ensure that costs are clear today, and avoid nasty surprises in the future.

INCREASING VISIBILITY

If you implement WLAN solutions that can provide context-based network access as discussed, then you are already on the road to a properly secured network. One of the advantages of context-based access is that you have identified exactly who and what are on your network, and once you have this information, it not only allows you to set policies according to your requirements, but also increases visibility into how your network is actually being used.

Once connected to the network, your WLAN will identify and track every mobile user, device, and app. If a WLAN solution is deployed with a management platform, it then becomes very easy to monitor the activity of your network, filtering information based on SSID, location, network policy, group of access points, etc. This enables administrators to ensure that networks are not being abused, and if so, identify threats and adjust security policies accordingly.

In addition to monitoring your own network, select vendors have also introduced Comparative Analytics. This capability allows customers to anonymously and dynamically compare infrastructure and client metrics to similar-sized deployments and/or industries; helping you proactively determine if and where to focus corrective or optimization efforts. Comparative Analytics capabilities allow IT professionals to accurately compare key infrastructure and client metrics both dynamically and over time.

END-TO-END SECURITY

Having discussed some of the most important elements of your WLAN security, there are some other areas that should be addressed before selecting your WLAN solution.

- **RADIUS/AD Integration** – To achieve 802.1X authentication, it requires the use of a RADIUS server and certificate authority (CA). Many WLAN solutions provide on-board RADIUS servers, eliminating the need for additional server builds, and allowing for direct integration with AD, reducing the amount of disruption to network configurations.
- **Firewall** – To protect the network at the edge, enterprise WLAN solutions often implement fully stateful, app aware firewalls directly within their access points, however this is not a complete substitute for a dedicated firewall within your network.
- **VPN** – For organizations that have remote offices or teleworkers, access points that integrate VPN server/client functionality offer the ability to extend WLAN security policies to remote locations.
- **WIPS** – Ensuring that only authorized users connect to the network relies on both proper authentication methods along with active monitoring tools such as wireless intrusion prevention (WIPS). WIPS features monitor the network for potential internal and external threats and alert administrators to attacks, such as denial of service (DoS) attacks or rogue access points and clients. The administrator in turn can activate anti-threat protection methods manually or automatically to contain or eliminate the threat.

With the amount of protection mechanisms used to control the access to wireless networks in modern solutions, WLANs are in many cases more secure than the implementation of many wired networks today. Every feature discussed in this section ensures that you can confidently deploy a wireless network that supports your corporate, guest, BYOD, and IoT devices without fear of threat.

You now have all of your devices connected in a secure manner, at fast speeds, and you can easily view the activity of your network from any location using cloud based management solutions...if you have followed the guidelines outlined in this guide of course. As we discussed at the beginning of the guide, Wi-Fi is offering a unique opportunity, with a return on investment never before seen, through information, insight, and applications. The leading WLAN solutions are beginning to leverage their access layer solutions and cloud architectures to provide organizations with an increasing amount of value beyond connectivity. This is a new area to explore with your vendors, requiring a conversation outside of speeds and feeds, and likely a number of new stakeholders within your organization.

The smart office, powered by mobile devices, data, insight, analytics, and applications is very real, offering the opportunity for organizations to not only streamline their operations, but also open up new ways of engaging with their staff. When discussing WLAN solutions with your vendors, in addition to asking “how fast is it?” and “how easy is it to manage?”, you should include questions like “what value does it offer our organization?”.

Increasingly, WLAN solutions are utilizing their cloud backend to analyze data points collected from the mobile devices connected to your network. These data points, combined with a rich set of APIs and applications, allow your organization to tap into new business insights that can be used for a wide variety of use cases. Now, your Wi-Fi can be used to determine building space utilization through the tracking of devices, and identify possibilities to reduce your real estate. In-house applications can be created that leverage the Wi-Fi and iBeacons to communicate with your staff based on their location, creating relevant engagement and alternatives to traditional communication methods. How about reducing the burden on IT teams for guest administration, by integrating the guest access with outlook, so that when a meeting is created, it automatically generates a secure PPSK for the visitor that is only valid during the meeting times, and when the visitor arrives, their device can be automatically configured for them?

Wi-Fi is starting to offer far more value than basic connectivity, make sure that you see it in your vendor's offerings.

SUMMARY

Assessing your connectivity needs and finding a solution tailored to those requirements is vital to the success of your digital workplace. Ensure your vendors are delivering true value beyond connectivity, while reducing the cost and complexity of managing and supporting your mobile centric network.

In short, ask yourself if your solution today, or any WLAN proposed by your vendor, can deliver these 5 attributes:

- **Adaptability** - Continuously adjusts to client, application, and infrastructure changes
- **Flexibility** - Easily integrates with existing architecture and applications
- **Affordability** - Reduces the cost of acquisition and ongoing operation of the network
- **Continuity** – Self-optimizing, self-healing, and self-organizing operation
- **Scalability** – Starts small and grows – or shrinks – as requirements change

With the changing economics and opportunities posed by software-defined, distributed WLAN architectures and cloud networking technologies, buyers are set to have plenty of good options for a better connected experience in 2018.

Happy shopping.

ABOUT AEROHIVE

Aerohive (NYSE: HIVE) enables our customers to simply and confidently connect to the information, applications, and insights they need to thrive. Our simple, scalable, and secure platform delivers mobility without limitations. For our customers worldwide, every access point is a starting point. Aerohive was founded in 2006 and is headquartered in Milpitas, CA. For more information, please call us at 408.510.6100 or go to our company's website at www.aerohive.com.

CORPORATE HEADQUARTERS

Aerohive Networks, Inc.

1011 McCarthy Blvd
Milpitas, California 95035 USA
Phone: 408.510.6100
Toll Free: 1.866.918.9918
Fax: 408.510.6199
info@aerohive.com
www.aerohive.com

INTERNATIONAL HEADQUARTERS

Aerohive Networks Europe LTD

The Courtyard
16-18 West Street
Surrey, UK GU9 7DR
+44 (0)1252 736590
Fax: +44 (0) 1252711901