Today’s enterprise is changing dramatically in the face of a series of inescapable global trends, including the Bring Your Own Device (BYOD) mobility explosion, the emergence of “mobile first” access preference for every device, and the efficiencies of cloud services. These initiatives, combined with the decentralisation of the corporate office to include remote offices, branch offices, and teleworkers performing critical functions are forcing enterprises to re-evaluate IT strategies.

Aerohive is a cloud networking company that provides comprehensive access solutions for the mobile first enterprise. Built from the ground up for today’s challenges, Aerohive sets new standards for how to address these global trends that are impacting every organisation with a unique and powerful combination of distributed networking intelligence, known as Aerohive Cooperative Control architecture, and an industry leading cloud services infrastructure. This allows Aerohive to deliver secure, enterprise-class access to every site—from a large campus or headquarters to remote branches and even single teleworker offices – with consistent, predictable service and maximum security.

Enabling secure mobility regardless of the user’s location or device and optimising the user experience with mobile applications allows the enterprise to enjoy greater productivity, improved employee morale, and better customer service, while at the same time reducing cost and complexity. With Aerohive, work becomes what you do, not a place you go.
Approach

Legacy WLANs were designed in an era when wireless was an add-on network that needed to be isolated and managed. The central controller is a direct result of the fact that there was insufficient processing power at that time to distribute intelligence to the APs at the edge, which is the model used in other networking infrastructure like routers or firewalls. Controllers were invented to “deal with the problem” of Wi-Fi in the enterprise, using the technology that was available ten years ago.

At Aerohive, on the other hand, they designed their systems using today’s advanced processing power, to create an access network with intelligence at the edge, the ability to dynamically route around problems, and no single point of failure. The design was based upon the fundamental premise that mobile device use would expand dramatically in the enterprise, that Wi-Fi would become the primary form of access, and that user identity is far more important than connection type. Aerohive’s solution distributes all control functions, policy enforcement, and data forwarding to edge devices while maintaining a centralised management system for monitoring and configuration—similar to how routing and firewall systems function.

To further increase the power and flexibility of the access layer and “simpli-fi” the deployment and operation of access solutions in a distributed environment, Aerohive pioneered cloud-enabled networking. This new solution leverages a cloud services platform to remove the cost and complexity of deploying and managing network services in a distributed environment, while delivering enterprise-class performance and security.

The Aerohive Cloud Services Platform is a globally distributed cloud-based infrastructure that leverages Aerohive’s patent-pending Cloud-Proxy technology and HiveManager Online SaaS offering. The combination is seamlessly integrated with a set of partner Software- and Infrastructure-as-a-Service applications and with your corporate network architecture.

With Aerohive, network survivability is built-in, and interruptions to cloud connectivity do not impact ongoing network operation. This is because data does not go to the cloud to enable control or policy enforcement functions, such as authentication, roaming, or QoS. These functions are all handled at the edge with Aerohive Cooperative Control architecture.
Access Points

802.11ac Access Points

**AP130 Dual Radio**

The AP130 Enterprise access points provide a seamless transition to 802.11ac. With more users, more devices, more things, more applications, and strained infrastructure and budget, the AP130 is a powerful option to meet those challenges. Aerohive has built an AP for pervasive Wi-Fi prepared for ultra-high density environments, powerful enough to provide all the services needed for an enterprise network, and inexpensive enough to deploy for ultra-high capacity networks. The AP130 combines 2x2, 2-stream, 802.11ac Wi-Fi technology and advanced security and device lifecycle management together into a cost-optimised solution that allows you to deploy high speed Wi-Fi into every office or classroom.

[www.aerohive.com/products/access-points/ap130](http://www.aerohive.com/products/access-points/ap130)

**AP230**

By combining the latest in 3x3, 3-stream 802.11ac Gigabit Wi-Fi technology and advanced security and mobility management together into an economical package, the AP230 allows you to deploy 802.11ac into every part of the network infrastructure – from Corp HQ to remote branches and outlets to every campus and classroom. It provides high-performance aggregate data rates up to 1300 Mbps in 5-GHz band. It supports dual concurrent 2.4Ghz 802.11n/g/b with Turbo-QAM™ and 5Ghz 802.11ac/n/a radios that can support legacy 802.11a, b, g and n clients and interoperate with the rest of the Aerohive Cooperative Control devices to provide a seamless enterprise-class experience for all connected users.


**AP370/AP390**

The AP370 and AP390 access points provide high-performance aggregate data rates up to 1750 Mbps with dual concurrent 2.4Ghz 802.11n/g/b and 5Ghz 802.11ac/n/a radios which can support legacy 802.11a, b, g and n clients and interoperate with the rest of the Aerohive Cooperative Control devices to provide a seamless enterprise-class experience for all connected users. The AP370 and AP390 are enterprise-grade, high performance two radio (3x3) three stream MIMO 802.11ac/n Access Points. The AP370 is targeted at high capacity enterprise environments. The AP390 is targeted at high capacity best range enterprise environments with external antenna and extended temperature option.

[www.aerohive.com/products/access-points/ap370](http://www.aerohive.com/products/access-points/ap370)
[www.aerohive.com/products/access-points/ap390](http://www.aerohive.com/products/access-points/ap390)
802.11n Access Points

**AP121/AP141**

The AP121 and AP141 access points provide 2x2:2 802.11n as well as optimised RF performance and enhanced receive sensitivity to provide a groundbreaking user experience for networks supporting multiple types of clients, including consumer-grade and bring-your-own devices (BYOD). The AP121 and AP141 are cost-effective, enterprise-grade 2x2 MIMO solutions, which are ideal for education, healthcare, and distributed environments. AP121 and AP141 are two radios, concurrent 2.4Ghz and 5Ghz access, and security scanning across both bands provide top performance and security at an entry-level price point.

Unlike the AP121, the AP141 has an external antenna option.

www.aerohive.com/products/access-points/ap121

www.aerohive.com/products/access-points/ap141

**AP1130 802.11ac Outdoor Access Point**

The Aerohive AP1130 is an enterprise-grade, high performance product, designed for high bandwidth outdoor wireless environments. With extended temperature range and a watertight chassis, the AP1130 can be deployed in almost any outdoor environment on earth. With two antennas on each radio and the ability to provide service concurrently on both 2.4Ghz and 5Ghz bands, the AP1130 provides support for 802.11ac as well as legacy 802.11a, b, g and n clients, through Aerohive’s industry unique and resilient controller-less architecture.

www.aerohive.com/products/access-points/ap1130

**AP330**

The AP330 access point is a high performance 802.11n access point with cloud-enabled management, on-demand provisioning, and integrated tools like spectrum analysis and application visibility and control. It provides high-performance dual concurrent (2.4Ghz and 5Ghz) radio 802.11n access and is designed for high bandwidth wireless enterprise environments. With multiple radios running 3x3 three spatial stream MIMO, the AP330 can provide an aggregate data rate up to 450Mbps. In addition, the AP330 can support legacy 802.11a, b, and g clients and interoperate with the rest of the Aerohive Cooperative Control devices.

www.aerohive.com/products/access-points/ap330

**AP350**

The AP350 access point is a rugged, high performance 802.11n access point with cloud-enabled management, on-demand provisioning, and integrated tools like spectrum analysis and application visibility and control. It provides high-performance dual concurrent (2.4Ghz and 5Ghz) radio 802.11n access and is designed for rugged, high bandwidth wireless enterprise environments. With multiple radios running 3x3 three spatial stream MIMO, the AP350 can provide an aggregate data rate up to 450Mbps. In addition, the AP350 can support legacy 802.11a, b, and g clients.
HiveManager NG Virtual Appliance

Next Generation Management System

HiveManager NG is Aerohive’s next generation enterprise-class network management solution. It sets a new standard for simplicity and flexibility in unified networking by combining streamlined configuration workflows, real-time client and event monitoring, simplified troubleshooting, versatile RF planner tools and API integrations. HiveManager NG truly provides a platform for enabling a next-generation network focused on mobility.

HiveManager NG Virtual Appliance is a new deployment option for HiveManager NG. Instead of using Aerohive’s Cloud Services Platform, customers have the flexibility to deploy the HiveManager NG Virtual Appliance on-premises as a single virtual machine.

Features & Benefits

The HiveManager Virtual Appliance is a standalone version of NG running in the customer’s private network. It has the same essential network management system function as that of the on-cloud version. The difference lies in the installation and administration features specific for a virtual appliance, on-premises deployment. The key benefits include:

**Simplified Deployment** - Simplified deployment workflow and seamless transition from demo to production.

**Centralised Configurations** - Granular and streamlined device and network configuration.

**Centralised Policy management** - Context-aware user policies with granular and flexible control enable IT to deliver an optimised end-user experience.

**Dashboard** - Dashboard with contextual filters and time range slider enables monitoring of network from assets, health status, data usage and security standpoints.

**Monitor** - Real-time and historical view of devices, clients, alarms and events. Ability to take informed action on devices immediately from the monitor interface.

**Troubleshooting** - Help-desk optimised interface to triage historical and real-time client problems with actionable data for resolution. Reduce escalation and provide better end-user experience.
Dashboards

Powerful dashboard with contextual filters and time range slider provides current and historical view, insights into applications, trend of client count, device data usage, and ability to drilldown to 360 degree views of network policy, single device, application, client and user.

Streamlined Configuration

Streamlined device and network configuration with task-based policy workflows enable configuration of a mobility network from sign-up to deployment within 15 minutes.
Centralised Management
Centralised network management with unified policy and monitoring for access points and switches with context-aware user policies.

Historical and Real-Time Troubleshooting
Help-desk optimised troubleshooting interface enables historical and real-time troubleshooting, provides problem summary and suggested remedy, reduces problem escalation, and provides better service experience to end users.
ID Manager

Several trends have recently emerged to ignite the requirement for enterprise guest management. One is BYOD, which makes guests virtually certain to have an internet-enabled device that they will want to use while visiting the enterprise. As Wi-Fi becomes the dominant access method of choice, guests have increasingly come to expect wireless access anywhere and from any device. It is becoming more important than ever to provide differentiated access to individual guests, since their profiles can range from unknown one-time visitor to long-standing contractor to board member. When on the network, guests may exchange sensitive company information and even passwords, making an open guest network a significant risk.

In the past, provisioning secure, identity-based enterprise guest management has required the attention of an already overstretched IT staff and front desk personnel to administer credentials. Today’s enterprises need a solution that is simple to administer and even simpler to deploy. In addition, guest management should not require additional dedicated infrastructure, available only to a few individuals with complete training and only in a few locations (typically those with a local guest management server device). The solution should be simple enough for anyone in the enterprise to use, including lobby ambassadors, receptionists and employees. Secure guest accounts must also be easy to take down, to ensure that connections don’t remain open longer than necessary. Finally, in today’s increasingly mobile and BYOD world, the solution needs to be deployed anywhere and at any time to securely support enterprise guests.

Aerohive has revolutionised network access by leveraging the cloud to provide simple, secure, and scalable connectivity and management. Aerohive’s unique, cloud-based HiveManager Online network management system enables enterprises to bring up WLANs and branch office networks with unprecedented ease, while eliminating the cost and complexity of additional centralised datacenter infrastructure. Because the Aerohive system is truly distributed with only centralised network management, a WAN outage has no effect on network services. Now Aerohive brings this same model to enterprise guest management with ID Manager.

Aerohive’s ID Manager is the first system to leverage the cloud to simplify and automate the deployment and maintenance of enterprise guest management. ID Manager combines authentication integration with the deployment-tested Aerohive Cloud Services platform to eliminate the need for any additional hardware or software. ID Manager delivers a scalable, easy-to-use enterprise guest management solution that streamlines the on-boarding of visitors of all types. Whether required at a single site or over a globally distributed, multi-lingual network, ID Manager’s cloud-enabled flexibility provides a complete solution for every site. No hardware, no software, no hassles.

How it works

One of the most difficult concepts in provisioning a fully functional guest management system is the fact that all guests are not the same. Some visitors only need Internet access, while long-term contractors or VIP guests, such as board members, may need extensive access to corporate applications or resources. A simple “one size fits all” guest network does not provide the granularity that is needed to deliver this differentiated access. The missing element is authentication integration, which is usually a costly and complex procedure requiring significant expertise in working with AAA infrastructure and often leads to additional hardware, software, and licensing expenses beyond the existing network infrastructure.

All Aerohive devices run HiveOS, Aerohive’s network operating system and already provides authentication services and integration with existing directory services. ID Manager leverages this capability, already built in to Aerohive existing devices, and uses RadSec to create an authentication-specific private connection between the Aerohive devices and the Aerohive Cloud Services Platform. This allows you to globally set security policies for any guest, and allows employees to instantly authorize enterprise visitors, which are then policed by corporate use policy, anywhere in the world. Multiple secure guest profiles can be established and automatically applied to the visitor – from casual guests to fully secure temporary employees – ensuring that every guest has precisely the access you intended without requiring intervention from IT or helpdesk staff. By leveraging the cloud, ID Manager can be deployed to any office, anywhere in the world - instantly. There is no additional hardware or software to buy; the cloud vastly simplifies the deployment and maintenance of guest management for anything from a single site to a global rollout. ID Manager handles secure, profile-based access for thousands of concurrent users and integrates with existing RADIUS systems to streamline deployments and meet compliance mandates such as PCI DSS or HIPAA.
Guest access profiles are fully configurable, allowing IT to determine not only what resources the guest can access, but when and for how long. Aerohive’s innovative Private Pre-Shared Key, or PPSK, can also protect all communications. Traditional PSKs, where all users have the same network password, are simply not secure enough for use outside the home. Aerohive’s Private PSKs are unique pre-shared keys that are created for individual users on the same SSID. They allow users to be individually identified and authenticated, similar to the experience with 802.1X or RADIUS authentication, but without the overhead to IT. PPSK ensures that each device has its own secret password with configurable expiration time. Of course, traditional username/password authentication is also supported for use with 802.1X (WPA2-Enterprise) or Captive Web Portals.

Guests on the network can vary wildly in needs and sometimes you may not know who the guest actually is, but you’ve provided Internet access anyhow. Just because they’re unknown doesn’t mean that finer, granular controls and services cannot be applied. ID Manager provides these controls by a new feature called Anonymous Access. This feature allows the operator of the network to configure data limits, time usage or time of day caps for guest users - whether they’re known or not. These usage caps can be created for guest users, based on time or data usage, and apply to all users on an SSID. For example, it’s now possible to restrict a guest user to an hour of access to the Internet, or, alternatively, restrict a guest to use a 200 MB data quota. Once that quota is met, the guest is then disconnected from the network.

Use Cases

Let’s take a look at three common use cases that an enterprise guest management system could deal with everyday. They include:

- Guest Self-Registration (via kiosk in lobby or personal mobile device)
- Employee Sponsorship for Guest Account
- Bulk Guest Account Creation

Guest Self-Registration

ID Manager allows for a self-service portal to be created and served via a simple web browser in a kiosk, in the case where there is no lobby staff. In this case, guests simply login to the web portal in the kiosk, enter their name, and specify how they would like to have their credentials immediately forwarded to them. Methods include SMS, email, directly on the screen, or Twitter direct message. To enable self-registration, IT administrators just provision web-enabled computers or tablets in the lobby and set the guest policy through their HiveManager interface. IT administrators can also enable guests to self-register through a captive web portal on guests’ own mobile devices. Admins can specify encryption, time until expiration, and device profiles for registrations. The Aerohive Cloud Services Platform even includes automatic localisation into nearly a dozen languages.

Employee Sponsorship for Guest Account

In some instances, employees may want to sign up a guest that they know is coming into the office. ID Manager makes it easy and doesn’t require the help of IT staff or helpdesk personnel. An intuitive web-based interface allows an employee to sponsor a guest or group of guests from any internet-connected device. This feature allows any authorised employee to provision their visitors with secure access while enforcing corporate use policy and providing IT with an audit trail on which employee authorised which visitor.

Bulk Guest Account Creation

Still another feature of ID Manager is bulk guest account creation. This feature, which can also be used by employee sponsors, allows the simultaneous creation of many guest accounts. ID Manager can use SMS to send credentials to a valid phone number, adding a layer of verification to the user’s identity. Credentials can also be sent by e-mail or shown on a web page. Once enabled, the network will automatically administer the appropriate access to resources based on the security policy assigned.
Client Management

BYOD and the Consumerisation of IT have redefined how administrators manage their networks. These trends have also extended IT responsibilities to include both personally-owned and corporate-issued mobile devices and the cloud-based applications such devices typically utilise. In 2014, we expect nearly 3 billion new devices to show up on enterprise networks, wielded by many different user types and accompanied by thousands of new applications. This means the lines between corporate-issued and end-user-owned devices are blurring. The “mobile first” transition has created a borderless network in which the network “edge” is the non-location-based point where BYO and devices transition from being consumer devices to business devices.

Aerohive cloud-enabled networking with distributed intelligence streamlines and automates connectivity, management, and monitoring of client devices to help corral the “iEverything” explosion and transform your network into a platform for mobility.

How Aerohive Solves the Problem

The Aerohive Client Management application gives administrators the power to easily provision, configure, and monitor end user devices as simply as HiveManager manages Aerohive access points.

This functionality allows an administrator to clearly differentiate between corporate-issued devices (CID) and BYOD, giving them the additional layer of context necessary to create granular policies controls over connected devices. The Client Management application includes:

- **Client Auto-Provisioning:** Client Management simplifies onboarding of corporate-issued and BYO devices by supporting a single-SSID solution to automatically create and install a unique credential as well as install a secure profile on iOS, OS X, Android, and Chrome OS. When clients join the SSID, they are automatically redirected to the enrollment page and provisioned with wired and wireless connection info, device certificates and/or Aerohive’s unique Private Pre-Shared Key functionality, and even advanced settings like VPN and LDAP configurations.

- **Customisable Enrollment Portal:** Users will see a completely customised, self-service enrollment portal that can display their company logo and corporate-defined details about enrolling their issued and BYO devices. This reduces Helpdesk costs by communicating terms of use and policies directly and in a familiar way.

- **Integrated Certificate Authority:** Aerohive’s certificate management system automates the entire certificate generation, distribution, validation, and revocation process. Aerohive Client Management leverages the certificate authority to publish unique credentials that include certificate information as well as user and device data. This means the IT administrator doesn’t have to worry about implementing a certificate authority, and can instead focus on advancing their BYOD and CID initiatives.

The combination of these features provides a unified workflow and process for organisations to deal with the iEverything explosion. While many mobile device management solutions have the ability to install a certificate onto a device that downloads the enrollment profile, Aerohive has designed a method to generate that certificate on the fly, based on the identity of the user, the device type, and the state of device ownership.

10  |  © 2015 Maintel  |  maintel.co.uk
Device certificates have long been the answer to distinguishing similar devices with like users and context from one another, but the creation and management of a Public Key Infrastructure (PKI) can be a challenge even for the most seasoned IT professional. The most daunting issue of implementing PKI, however, is the “the chicken and the egg” problem of certificate installation: users need a certificate to get their device onto the network, but they need to be on the network to get the certificate onto the device. This can lead to a multiple SSID configuration, where users have to connect to an enrollment SSID to get the profile and certificate, and then connect to the secure SSID once enrollment completes.

Once an administrator has decided to implement device certificates to solve network access challenges, BYOD and the Consumerisation of IT present another hurdle. These devices are specifically designed to be user-centric, with the user in charge of everything that is installed and running on them, including certificates and device profiles. In fact, Apple in particular designed their interface and devices this way intentionally to provide exceptional user experience, not to be hardened business devices. IT now faces the challenge of incenting the user to accept the user profile and certificate on their device and keep it there.

Aerohive has once again paved the way to Simpli-Fi by providing a way to generate and install a unique device certificate and profile using a single SSID. The user connects a device to the SSID using standard 802.1X/PEAP credentials. The administrator can configure a list of expected MAC addresses for corporate issued devices, and any device not matching that list will be treated as BYOD. Once connected with their username and password, the user will have their device provisioning status confirmed. If the device has not been provisioned or has the profile uninstalled, the user will be redirected to the self-service portal and assigned a unique certificate that reflects their identity as well as the device type and ownership. The certificate is then pushed to the device and the device is automatically reconnected to the same SSID – no user or IT intervention required!

Aerohive even has a solution for situations where directory credentials are hard to administer. In the event that a network is not configured to use WPA2-Enterprise or 802.1X authentication for the secure SSID, for example at a school where many of the devices are brought in by students, Aerohive can provide a unique credential on every device using Aerohive’s patent-pending Private Pre-Shared Key (PPSK) feature. Instead of a unique device certificate, Client Management provisions each connecting device with a PPSK that reflects identity, device type, and device ownership context to yield the same result as the 802.1X/PEAP solution above. The PPSK is automatically installed on the device and completely hidden from the user, making it impossible to re-use that key for any other device.

The ability to easily create and distribute secure profiles offers value far past login. If an administrator wants to implement device controls, such as passcode restrictions, application permissions (for example, disallowing cloud file sharing), or email, VPN or calendar configurations on the connected devices, a secure profile can be assigned to the device based on the identity of the user, device type, and ownership of the device. These secure profiles provide real-time configuration and monitoring capabilities for the provisioned devices, and allow an administrator to get even more granular control over the network and optimise for mobility.
Even if the administrator does not want to implement device-level configuration and controls on the device using the profile, the unique device certificate or PPSK created by Client Management adds the additional level of context (device ownership) to further refine the Aerohive user profile assigned to a particular device, which applies network permissions such as VLAN assignment, firewall, QoS, and tunnelling policies.

This combination of network control and device control highlights one of the unique benefits of the Aerohive solution. The tight integration between the HiveOS user profile and Client Management device profile allows for an extremely personalised mobile experience for the connecting users. An administrator can configure the Client Management device profile attribute to match the user profile assigned in HiveOS, and as the user profile in HiveOS changes, either because of a change in location, authentication status, or re-auth, the device profile can also dynamically be updated and change device restrictions or configuration. For example, an administrator may have the same SSID across an entire deployment of APs, but in the corporate office the HiveOS user profile may be Employees-Corp. The Employees-Corp user profile can match the attribute in a Client Management device profile that simply requires a passcode when connected at the corporate office. When the device connects at a remote location, even to the same SSID with the same credentials, the user profile may be Employees-Remote and therefore trigger a dynamic update to the device profile, which now disables the camera and cloud file sharing. The ability to personalise the network experience based on all of the available context and tie it to how the device is interacting with the network opens up many exciting opportunities for the administrator to increase visibility and control over what users can do in the mobile-first enterprise.
Private Preshared Key (PPSK)

Wireless networking has gone through several evolutionary steps to equal – and in some cases, exceed – the security found in wired networks. The first step in this evolution was the development of preshared keys, or PSK. Each device in a network uses a preshared key to encrypt traffic, thus providing additional security. The disadvantages of classic PSK include the fact that it is impossible to revoke the network-wide key should an individual leave the organisation, as well as the fact that it is relatively easy to crack. Today, the clear choice in authentication for enterprises that are deploying or upgrading wireless networks is 802.1X. However, moving from PSK to 802.1X can prove to be challenging, as some devices do not support 802.1X or are cumbersome to set up. This can lead to the choice between the purchase of new equipment or a compromise in security. 802.1X also faces challenges when used to secure devices not owned by the enterprise, such as those of guests, students, subcontractors or the like. Because 802.1X requires the installation of a software client, it is difficult or impossible to use on such unmanaged devices.

Aerohive’s patent-pending Private PSK provides the ease of PSK with many of the advantages of 802.1X solutions. The IT manager can provide unique passphrases to each user on a single SSID, which creates a one-to-one relationship between the key and user instead of the one-to-many paradigm of classic PSK, thus providing the ability to truly authenticate each individual. This enables 802.1X-like capabilities even though it appears like only a PSK is required on the laptop or Wi-Fi device. While classic PSK does not allow the revocation of a single user’s credentials since all users share the same passphrase, Private PSK offers a unique PSK per individual and therefore enables the administrator to revoke a single set of credentials. Furthermore, since Private PSK, like 802.1X, allows a means to identify individual, users on a single SSID, each can be granted different user profiles. This allows all users to connect to the same network, but get unique levels of service based on their roles.

Benefits

- Simple key creation, distribution and revocation saves administrator time and reduces the cost and complexity of using single PSK or trying to get hard-to-configure devices online using 802.1X
- Guests can be given unique keys, thereby eliminating the risk of one guest eavesdropping on another. In addition, entering a PSK is often simpler than loading up a captive web-portal and entering a username and password
- If a person leaves the company, classic PSK requires that the key be reset for all users, which can be an IT support burden. With Private PSK, just that one user’s key can be revoked
- Many clients do not support 802.1X or the latest WPA2 standard with opportunistic key caching required for fast roaming between APs. With Private PSK, those clients can see significant performance increases with roaming
- Many legacy clients don’t support 802.1X but most will support WPA-PSK. Those clients can be made secure without a costly client and application upgrade

Aerohive Key Differentiators

- Cooperative Control – Controller-less Wi-Fi architecture eliminates WLAN controllers and reduces costs
- Public or private cloud management – Moves Capex to Opex and lets you start small and grow your network gradually
- Zero-touch provisioning – Ship devices to each site, plug them in, and they will automatically find the cloud system for its configuration
- Application reporting & visibility – View all applications on the network and control the quality and access to them from the cloud
- Cloud-enabled mobility management – Simplifies and automates onboarding, management, and troubleshooting of connected mobile devices