

Tech Brief |



**Effective Network Access Control
in a Wireless World**

March 2009

Jon Green, CISSP | Aruba Networks



Contents

Executive Summary.....	1
Overview.....	2
<i>Ubiquitous Access</i>	
<i>Mobility</i>	
Ensuring Integrity with NAC	2
Why Do You Need NAC?	2
Building Scaleable, Secure Wireless Infrastructure.....	2
Aruba Endpoint Compliance System	3
Endpoint Compliance.....	4
Identity Management	5
Authentication	6
Location-based Management	7
Best Practices for Phasing In Wireless NAC	7
Customer Example.....	8
About Aruba Networks.....	9

Executive Summary

Enterprise wireless LANs have grown exponentially over the last several years. Having such ubiquitous access across the organization 24X7 dramatically changes the way we live, work and play - leaving us wanting more. Securing such a wireless infrastructure is no easy task, however, given the mobility and diversity of needs its users demand. Many challenges must be overcome to provide the availability, performance, reliability and integrity required for ubiquitous wireless service. Deploying an open, public wireless infrastructure means developing, managing and executing a scalable wireless security policy with appropriate resources. This includes managing user credentials and associating policies based on their levels of authorization. In addition, the wireless infrastructure itself must be protected from attack and intrusion.

Network Access Control, or NAC, provides the mechanism for ensuring the integrity of connected users, their devices, the network infrastructure and its attached resources. NAC provides detailed information about users and devices on your network: who, what, when, where, and how. More specifically, who are the users and what are the devices connecting to your network? When are they connecting? Where are they connecting? How are they connecting (wired LAN, wireless LAN, VPN)? The answers to all these questions are important for determining the appropriate level of network access allowed.

NAC is most effective and scales best when deployed out-of-band, letting the distributed wireless LAN controller collect and report, in real time, the information required for policy determination, then execute the policy using an integrated stateful firewall. When an out-of-band NAC system such as Aruba's ECS appliance is fully integrated with the stateful policy engine of a controller, a more effective balance of NAC intelligence is achieved, becoming more scalable and available while enabling a more cost effective use of resources than would be possible without such integration.

Recognizing the need for a secure wireless infrastructure that scales to the performance of the enterprise and meets its challenges more effectively, Aruba Networks and Bradford Networks, a leader in Network Access Control (NAC), have collaborated on an integrated product that delivers a cost-effective, ubiquitous, secure and scalable enterprise wireless infrastructure.

Overview

Enterprise wireless LANs have grown exponentially over the last several years and with good reason. Coupling ubiquitous access with wireless mobility puts the Internet plus all of your favorite IT resources at your fingertips anywhere at any time. Having such ubiquitous access across the organization 24X7 dramatically changes the way we live, work and play—leaving us wanting more. Securing such a wireless infrastructure is no easy task however, given the mobility and diversity of needs its users demand. Many challenges must be overcome to provide the availability, performance, reliability and integrity required for ubiquitous wireless service.

Ubiquitous Access

Wireless is a public medium, available to all within its reach. That is its main attraction but this very openness has become its major weakness for those charged with deploying and operating it. Given such openness, protecting access to the network and its attached resources is paramount. IT teams must allow access only to those authorized with appropriate credentials. IT must also assure that the network infrastructure and its resources are available yet protected from attacks such as Denial of Service that block access to or compromise the availability of provisioned bandwidth.

For a network to be truly ubiquitous its reach must match the mobility of its clients. Often times that reach is quite large covering varying geographies and different population densities with diverse performance requirements. Building ubiquitous wireless is all about scaling. Ultimately, how the network scales in its availability, performance, security and integrity will determine how ubiquitous and effective it will become.

Mobility

Mobility is a big part of the lure of wireless but makes the challenges described above exponentially more complex. Tracking down a problem caused by a moving target can be difficult or impossible especially if that target is intentionally malicious and deceptive. Mechanisms must be found to identify and track users with their associated mobile devices in real time. They must also be able to enable or deny network access based on a pre-defined policy regardless of their location.

Ensuring Integrity with NAC

Deploying an open, public wireless infrastructure means developing, managing and executing a scalable wireless security policy with appropriate resources. This includes managing user credentials and associating policies based on their levels of authorization. In addition, the wireless infrastructure itself must be protected from attack and intrusion.

Network Access Control, or NAC, provides the mechanism for ensuring the integrity of connected users, their devices, the network infrastructure and its attached resources. NAC provides detailed information about users and devices on your network: who, what, when, where, and how. More specifically, who are the users and what are the devices connecting to your network? When are they connecting? Where are they connecting? How are they connecting (via wired LAN, wireless LAN, VPN)? The answers to all these questions are important for determining the appropriate level of network access allowed.

NAC also involves checking devices to determine if they are safe to connect to your network. This part of NAC is referred to as endpoint compliance or endpoint security posture assessment. It effectively answers the question – do devices on your network meet your security policy requirements?

Finally, and most importantly, NAC enforces security policies on your network so that only authorized and safe users and devices are allowed access – and they are allowed access only to network resources that are appropriate.

Why Do You Need NAC?

NAC provides a number of benefits from both business and technology standpoints, including:

- | | |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security | <ul style="list-style-type: none">• Allow only known and authorized users and devices onto your organization's network• Ensure all devices on your network meet your security policies and are considered 'safe' |
| Visibility | <ul style="list-style-type: none">• Know who and what is on your organization's network at all times |
| Control | <ul style="list-style-type: none">• Control access to specific network resources based on identity of users and/or devices<ul style="list-style-type: none">- Allow "Employee" users access to appropriate resources based on their job or role- Allow "Guest" users access only to the Internet, not to internal network resources- Deny or limit access to users or devices that do not satisfy your security policies |
| Operational Efficiency | <ul style="list-style-type: none">• Automate IT functions that otherwise are very manual and labor-intensive• Off-load tasks from IT and Help Desk resources to increase their productivity |
| Regulatory Compliance | <ul style="list-style-type: none">• Be able to track and report on all users and devices accessing your network resources• Provide detailed "audit trails" in the event of compliance audits |
| Return on Investment (ROI) | <ul style="list-style-type: none">• Leverage your existing network infrastructure to enforce your organizations policies• Get more value out of your existing investments (in addition to other benefits of NAC) |

Building Scalable, Secure Wireless Infrastructure

Building an effective and ubiquitous wireless infrastructure requires deployment of two major, fully integrated components. The first is an intelligent, controller-based, Wi-Fi Access Point (AP) system. This system regionalizes APs and consolidates their intelligence within that region, allowing you to scale access and performance effectively. The regionalized intelligence lets you balance the client load across deployed APs to utilize their bandwidth fully and effectively. Regionalizing intelligence also creates a centralized mechanism that enables and scales security mechanisms more effectively than would be possible in just an AP. This makes high-performance, complex and expensive resources for encryption, VPN and other functions available to all APs without burdening their cost.

While the Wi-Fi controller centralizes AP intelligence, its ability to manage and deliver global network security policy across all controllers in the infrastructure doesn't scale for the same reasons that APs don't scale across a global wireless infrastructure without regional control. There needs to be a global NAC intelligence that can manage security policy, credentials and intrusions across the wireless infrastructure while delivering a security control plane that can work in concert with Wi-Fi controllers to enforce that policy.

NAC is most effective and scales best when deployed out-of-band, letting the distributed, Wi-Fi controllers collect and report in real time, the information required for policy determination then execute the policy delivered to them. Fully integrating NAC with that controller means better access to real-time, decision-quality data for dynamically managing policy and building a more reliable inventory of clients (whether authenticated or rogue), intrusions and their location. This balances intelligence more effectively and allows you to use resources in a more scalable, cost-effective way than would be possible without such integration.

Aruba Controllers

The heart of Aruba's secure mobility solution is the controller, which is designed to provide policy management and stateful firewall-based policy enforcement in even the most active networks. Aruba's controller architecture is unique in terms of providing an integrated ICSA certified stateful firewall. Through the use of this technology, Aruba provides the highest level of security for user traffic and protects WLAN operations from L3-L7 malicious activity & attacks

The controller handles the performance needs of high-speed 802.11n with 32-core, multi-threaded network processors, dedicated cryptographic processor cores and high performance hardware acceleration, A single Aruba 6000 controller offers 80Gbps of throughput, supporting over 32,000 users. These controllers can be configured in a hierarchical fashion for redundancy or to support mobility and security in even the largest multi-national deployments.

Policy Management

With the Aruba controller, every client is associated with a user role which determines the client's network privileges, how often it must re-authenticate, which bandwidth contracts are applicable for which applications, etc. A policy is a set of rules that applies to traffic that passes through the Aruba controller, with one or more policies applying to a user role. A role can be assigned to a client before or after they authenticate to the system.

Policies maintained by the controller are:

- Stateful: recognizing flows in a network and keeping track of the state of sessions
- Bi-directional: Keeping track of data connections traveling into or out of the network
- Dynamic: Address information in the policy rules can change as the policies are applied to user

Application Awareness

In addition to enabling granular user separation, the policy enforcement firewall empowers Aruba controllers with the intelligence to separate "applications" per user. Within Aruba controllers, IT administrators define which applications a particular user can have access to, and sessions are logged for troubleshooting or security monitoring. They can mirror session flows (for troubleshooting), redirect flows (for HTTPS proxy, 3rd party Anti-Virus / IDS scanning, etc.), assign custom quality of service markings (ToS & CoS) per application for increased visibility and management of WLAN client activities.

Policy Enforcement

The controller provides strong enforcement of policy over both wireless and wired connections. Enforcement is provided by role-based policies tied to a stateful firewall engine rather than VLAN-based ACLs, allowing VLANs to remain focused on broadcast control, not security enforcement. A firewall policy identifies specific characteristics about a data packet passing through the Aruba controller and takes some action based on that information. In an Aruba controller, that action can be a firewall-type action such as permitting or denying the packet, an administrative action such as logging the packet, a quality of service (QoS) action, etc. There is the granularity to apply firewall policies to user roles to give differential treatment to different users on the same network, or to physical ports to apply the same policy to all traffic through the port.

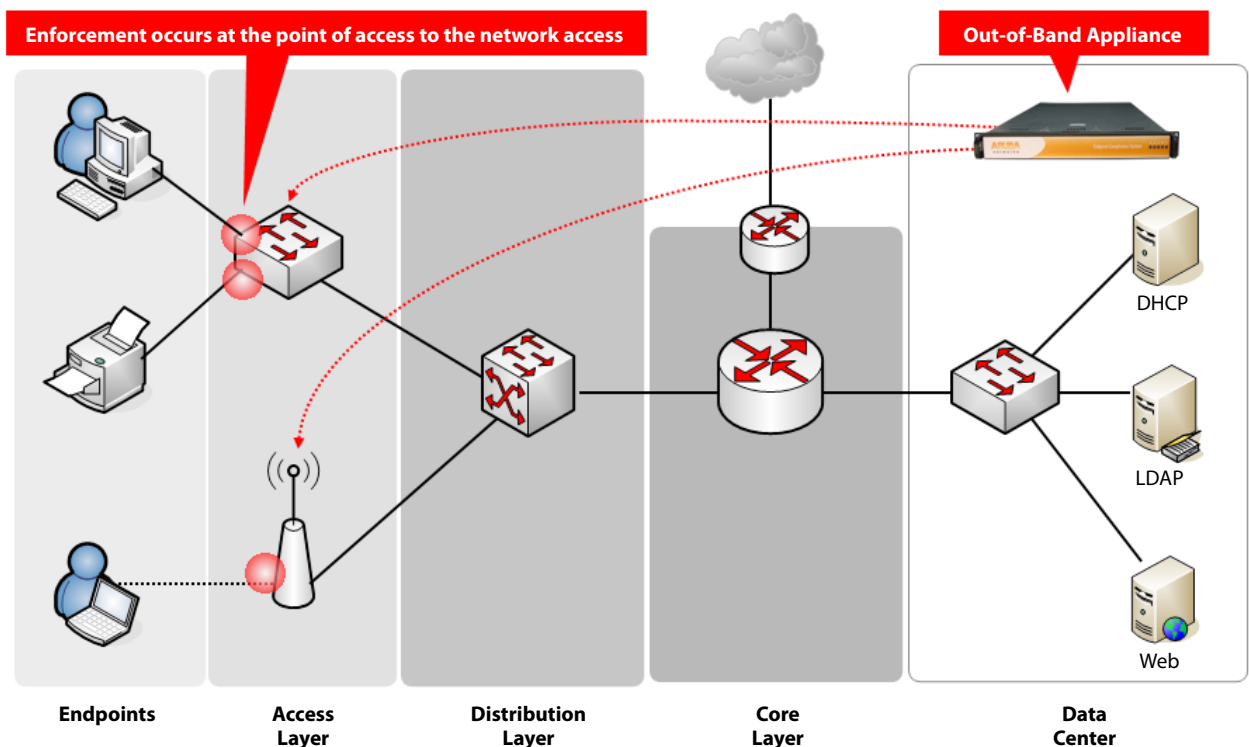
Fully integrating an out of band appliance with the controller offers a complete, high performance NAC solution with better access to real-time, decision-quality data for dynamically managing policy and building a more reliable inventory of clients (whether authenticated or rogue), intrusions and their location. This balances intelligence more effectively and allows you to use resources in a more scalable, cost-effective way than would be possible without such integration.

Aruba Endpoint Compliance System

Recognizing the need for a secure wireless infrastructure that scales to the performance of the enterprise and meets its challenges more effectively, Aruba Networks and Bradford Networks, a leader in Network Access Control (NAC), have collaborated on an integrated product that helps enable a cost-effective, ubiquitous, secure and scalable enterprise wireless infrastructure.

That product is ECS, Aruba's Endpoint Compliance System. ECS integrates with and leverages components of the Aruba controller, providing it with distributed security intelligence. ECS manages policy and oversight for the global wired and wireless infrastructure leveraging the policy intelligence and the in-line, hardware-accelerated components of the Aruba controller. The Aruba controller leverages the policy delivered by ECS as an input to help determine a firewall role that will be applied to that authenticated user or device. ECS is capable of delivering a policy that directly maps to roles that are contained on the controller's policy server. ECS can also deliver this policy to non-Aruba wired network devices which have varying capabilities in enforcing that policy. ECS also works with host-based agents to extend policy and oversight all the way to the network end points. This division of labor brings the kind of scale necessary to build and operate a ubiquitous network infrastructure.

Out-of-Band with Edge Enforcement



ECS is based on an "out-of-band architecture," which gives it great flexibility and scale to manage both wireless and wired clients. This type of architecture treats network components as objects, collecting information from them. As new components are added, it simply establishes new lines of communication with those components. This means new network components both within and outside the Aruba family may be easily integrated without disrupting network operations or requiring "forklift" upgrades.

Because it is out of band, ECS is not burdened with the expense of processing the real-time stream of traffic. That job is left to the wireless controller and other network components whose main function necessitate in-band processing for routing and filtering the traffic. ECS places little burden on those components to provide the information it requires to do its job. This achieves the balance of intelligence required to scale the infrastructure.

The ECS architecture is comprised of three major components: Endpoint Compliance, Identity Management and Authentication. The features of each will be examined in turn.

Endpoint Compliance

The ECS architecture can leverage the presence of an agent on each client (host) it is tasked with managing. The agent can be either persistent or dissolvable, meaning that it lives permanently on the client or is downloaded to the client as needed, then discarded or “dissolved” after use. ECS supports both types of agents, as different environments demand different solutions.

For example, compliance for temporary users (contractors, visitors, etc.) needing limited, short-term access to the network and its resources may require simple validation upon entry. In this case, downloading a dissolvable agent to the user eliminates overhead of installing and maintaining a more sophisticated agent while affording the necessary protections required for temporary users.

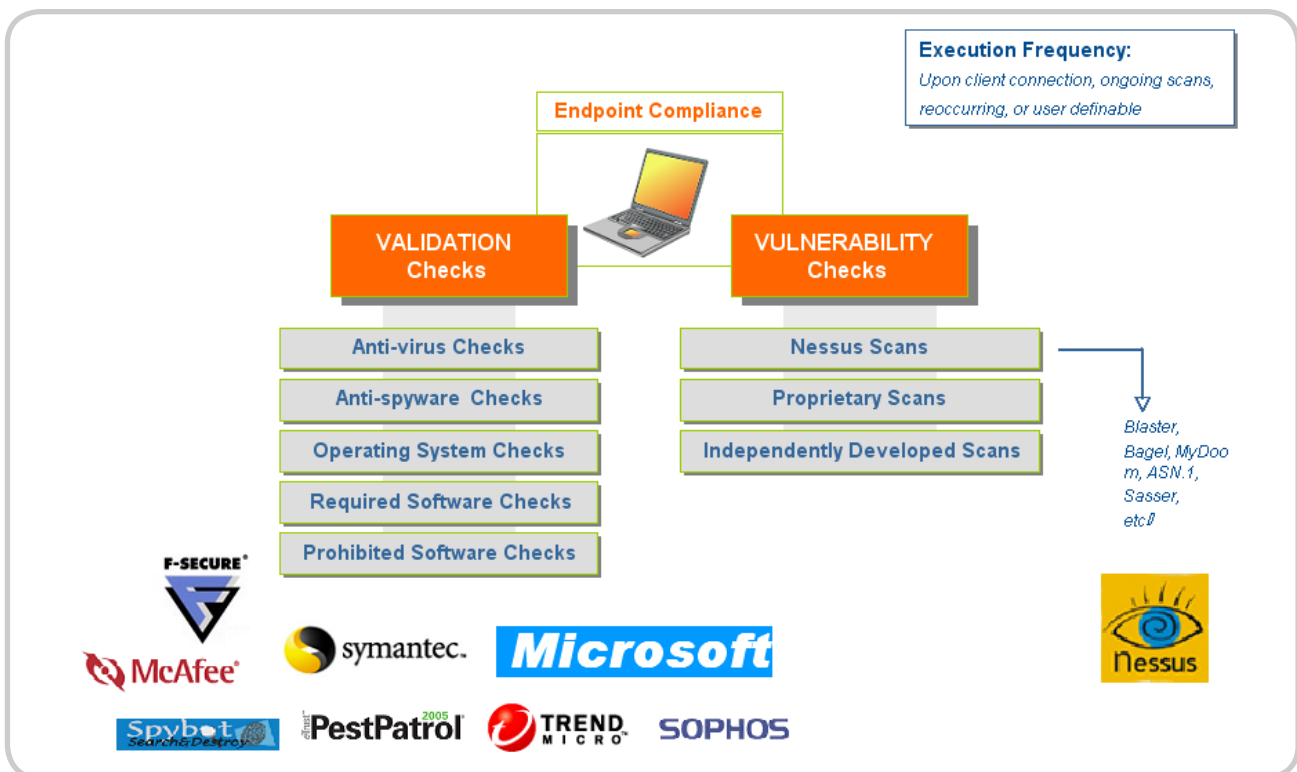
On the other hand, more permanent or sophisticated users (employees, students, etc.) may benefit from the advantage of a resident or “persistent” agent. This approach allows for constant analysis of and communication with the client that may be beneficial when managing more than simple access validation. Persistent agents find great advantage in their ability to inventory and analyze client applications, security and resources. Persistence affords a more integrated experience, providing improved analysis and control.

A good example of how this integration has been leveraged is the use of the persistent agent’s messaging capability. Many college campuses and enterprises have requirements for deploying an emergency notification system capable of delivering emergency messages instantly to everyone. Using the persistent agent to “pop-up” a display of an emergency message to network users accomplishes that task without requiring the deployment, operation and maintenance of an additional messaging system. The persistent agent is strictly controlled by network operations staff, as opposed to the user. Its messages and availability can be guaranteed, therefore, which is a key requirement of such an application.

The choice of whether to use a persistent or dissolvable agent depends heavily on the environment in which it’s deployed and the depth and type of analysis/functionality required. In either case, these agents provide ECS with information allowing it to perform an effective compliance analysis of the client:

- Client Inventory – scanning the host’s applications, developing an inventory then determining if they’re acceptable or should be prohibited
- Checking for required OS or application validity
- Checking for required anti-virus and anti-spyware software

Agents also assist with effecting remediation, working in tandem with ECS which in turn works with the wireless infrastructure components to isolate clients until the required changes can be made. Lastly, agents allow ECS to perform Identity Management and Authentication as described below.



Identity Management

The Aruba controllers and ECS work together to maintain a complete picture of user and device identity.

ECS Identity Management operates at several levels. At the first level, ECS establishes a registration policy. This discovers and creates an inventory of all wireless clients, then collects and categorizes them. The canonical registration identity is the wireless device's MAC address. Bound with this is information about the device's owner and/or who's accountable for the device. The device's name, IP address and port are also logged.

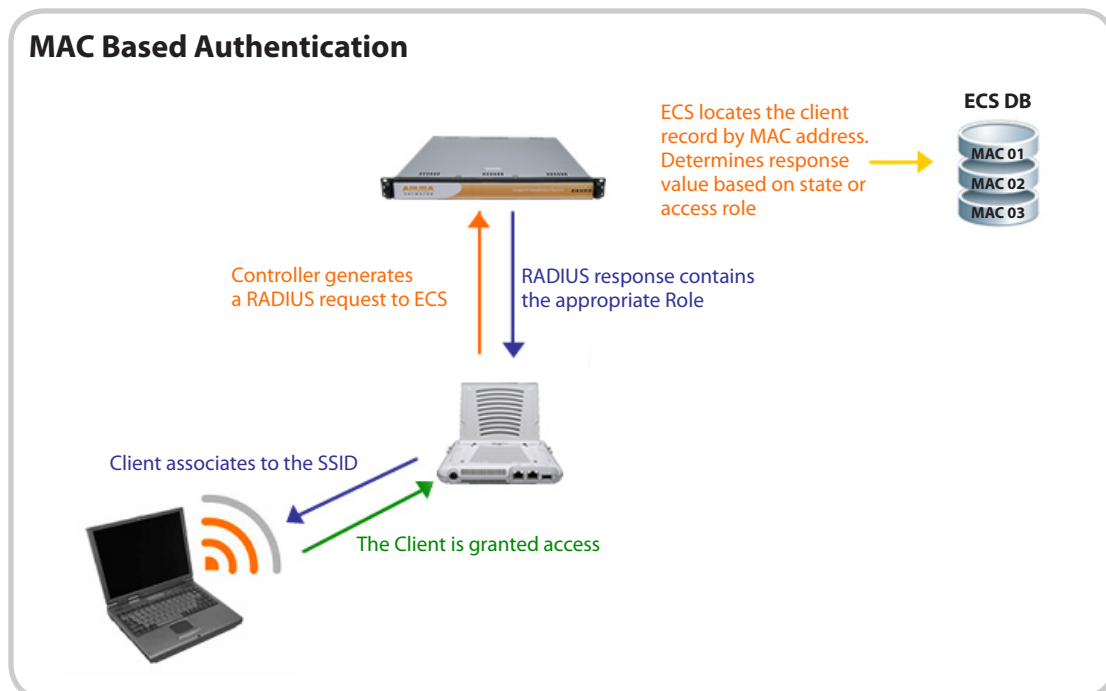
ECS then establishes an authentication policy which effectively acts as a proxy between a directory system that manages credentials and the Aruba controller, which acts as the authenticator.

ECS' integration with the Aruba controller allows it to effect Role-based access management. Clients can be associated with different Aruba controller roles as ECS determines their credentials and levels of access. These roles may or may not be associated with unique VLANs.

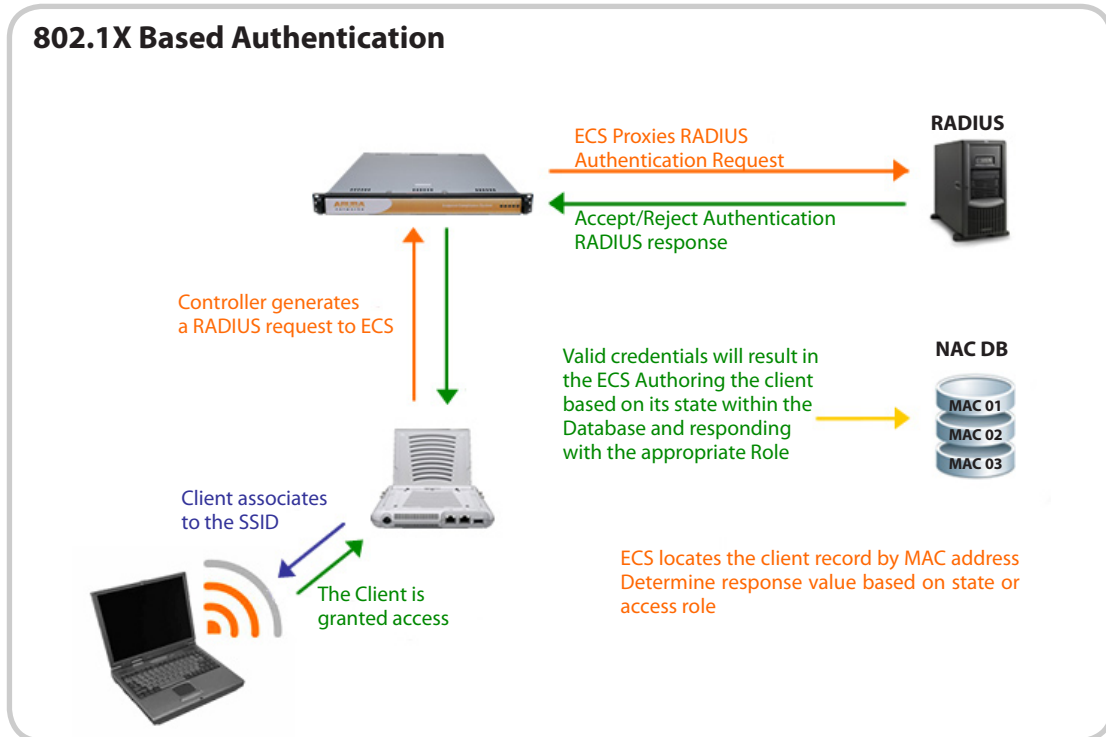
Authentication

Different methods of authentication are possible through the Aruba system. The first is MAC address based. Recall that one of the challenges with scaling a ubiquitous wireless infrastructure is being able to deal with both simple and intelligent devices. Many Wi-Fi appliances and sensors have no credentials other than their MAC address. Binding this with owner/operator information as part of the Identity Management registration process delivers a base level of security.

The process for MAC-level authentication starts with the device associating with the AP and its controller. While MAC based authentication can be handled directly on the controller, the device registration process implemented by ECS can provide a simplified approach to administering this type of authentication. The controller would issue a RADIUS request to ECS. ECS locates the client record from its canonical registration identity (MAC address) then determines the appropriate response value based on state or role. ECS issues a RADIUS response to the AP's controller that contains the appropriate Aruba controller Role.



The process for 802.1x authentication, used in WPA wireless security, starts with the device associating with the AP and its controller. The controller then issues an EAP-based RADIUS request to ECS. ECS proxies a RADIUS authentication request receiving either a Reject or Accept response from the RADIUS server. If ECS has valid credentials for the client, it issues an authorization based on the client's state within the ECS database and responds with the appropriate Role. The controller considers the role delivered by ECS against other attributes of the user, device, environment and traffic flow that are known by the controller to make a final policy decision.



Location-based Management

Included in the decision tree for authentication is the ability for ECS to work with the controller to determine the client's current location. This solves the problem of replacing the wired paradigm previously discussed for using location as a parameter for authorizing network access within a given venue. This function will be enhanced over time as the controller gains the ability to triangulate specific geographies within the infrastructure. The controller's ability to both manipulate AP power and control many overlapping AP's within a given geography makes location-based authentication surprisingly effective.

Best Practices for Phasing-In Wireless NAC

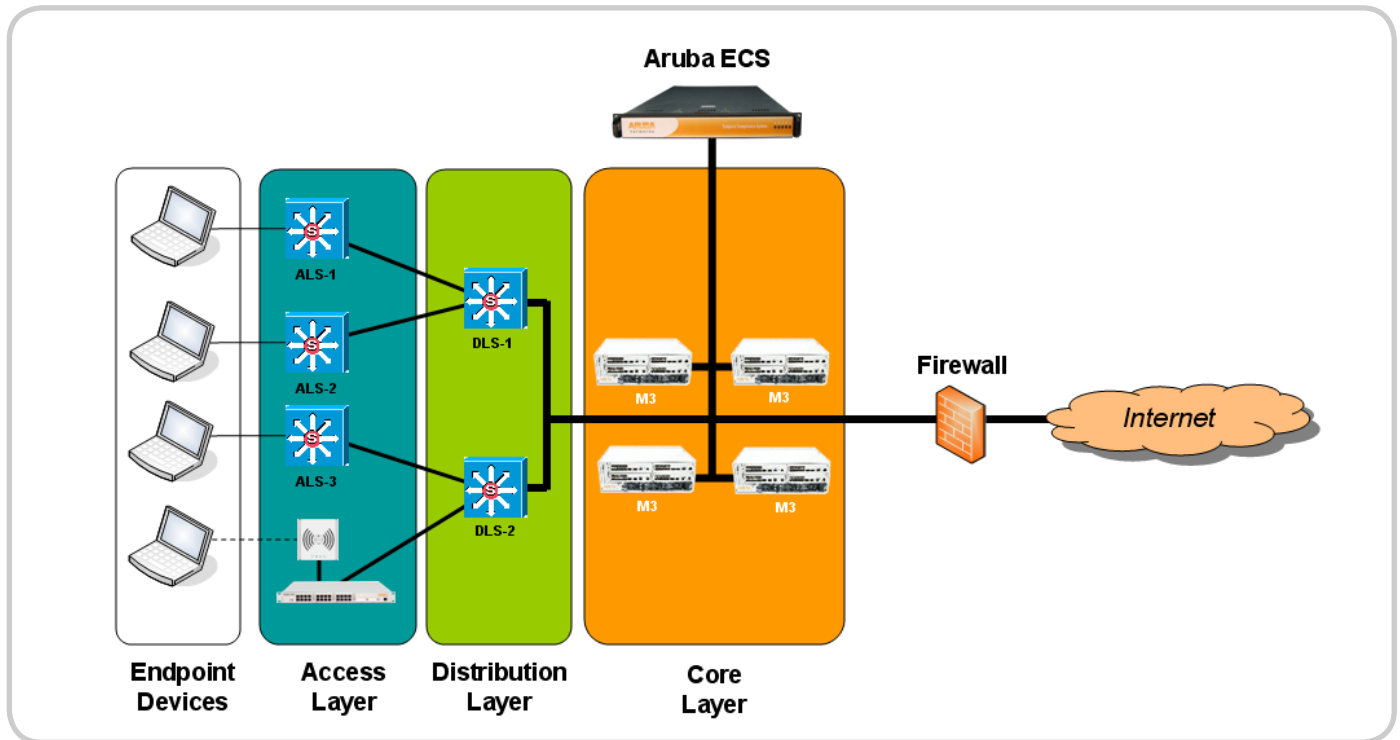
When rolling out such a powerful, integrated NAC solution, a phased approach is the best practice. NAC can have a major social impact on wireless users while performing its intended purpose. It is recommended that the following sequence be followed:

- Strong Authentication** Implement 802.1x
- Identify** Let ECS discover and register clients so you have a complete inventory. Use information on rogue clients to pursue and resolve these unknown sources.
- Monitor & Record** Use the Aruba system (ECS, Controllers and APs and AirWave management) to monitor and record client activities to observe current behaviors and determine current level of compliance with policy. This provides the baseline for discussion with clients of ECS' future role.
- Notify** Allow ECS to inform clients that they are out of compliance with defined policies, if this is the case, but grant them access regardless.
- Enforce** Enable the Aruba Controller and ECS to execute policy as defined.

This phased approach not only allows users time to understand ECS' role in securing the network, but also provides administrators with greater visibility to the devices and users connecting to the network to refine policy prior to activation of any enforcement controls.

Customer Example - Public College in New York City, NY USA

The challenge at this New York City public college was to add a ubiquitous wireless overlay to their existing wired network while maintaining consistent security policies for both infrastructures and their users. Maintaining a common user interface was equally important to avoid confusion and frustration as users flowed back and forth between wired and wireless. Finally, the deployed solution had to integrate well with the existing wired infrastructure to avoid a forklift upgrade of that infrastructure.



The college chose to use the Aruba 6000 and ECS to provide a unified NAC solution for both the wired and wireless network. The Aruba 6000 Multi-Service Controllers are actually used as the default routers for the entire wired network, taking advantage of the 10Gbps Ethernet connections and the 80Gbps high-speed firewall. So users entering the network, either wired or wireless, will be directed by the Aruba controller to ECS for registration, authentication and posture assessment.

ECS was a great match for this assignment providing a common place for creating, maintaining and delivering user and network policies. Its integral web portal provided the same, consistent user experience regardless of the infrastructure used. By providing a logical, single point of user entry, ECS delivered an easy and very effective way to inventory, analyze and remediate users before allowing them to enter either infrastructure. This was a huge benefit to the college. Not only did they achieve a common point of entry for both infrastructures but they were able to qualify and maintain users more effectively than ever before. Of particular value was their ability to track both users and equipment separately while identifying their relationship. Having access to at least MAC-level identification allowed them to manage simple appliances and sensors that were not traceable before.

ECS proved especially valuable in its ability to direct the controller's firewall to trigger role changes, rather than VLAN changes. VLAN changes are disruptive to users, requiring a new IP address and an interruption in connectivity, while firewall and role changes do not. ECS effectively leveraged the in-line, hardware-assisted packet processing of the Aruba controller to obtain the information needed for policy analysis, then executed the policy delivered.

ECS was equally effective in integrating with the legacy wired infrastructure. By placing extra controller capacity in-band to the wired access layer, the college was able to avoid the added expense and complexity of configuring additional VLANs to manage user authentication, validation, remediation and access. This also allowed a single point through which to manage both wired and wireless users, greatly simplifying their management operations.

In summary, the combination of the Aruba mobility controller and Aruba's ECS gave the college the most scalable, cost-effective solution for creating and delivering security policy for their environment. Its distributed architecture provided the scale required. Its ability to be infrastructure agnostic allowed the common user experience that the college was seeking while greatly reducing their cost of operating multiple infrastructures.

About Aruba Networks

People move. Networks must follow. Aruba securely delivers networks to users, wherever they work or roam. Our mobility solutions enable the Follow-Me Enterprise that moves in lock-step with users:

- Adaptive 802.11 a/b/g/n Wi-Fi networks optimize themselves to ensure that users are always within reach of mission-critical information;
- Identity-based security assigns access policies to users, enforcing those policies whenever and wherever a network is accessed;
- Remote networking solutions ensure uninterrupted access to applications as users move;
- Multi-vendor network management provides a single point of control while managing both legacy and new wireless networks from Aruba and its competitors.

The cost, convenience, and security benefits of our secure mobility solutions are fundamentally changing how and where we work. Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at <http://www.arubanetworks.com>.



1344 Crossman Ave. Sunnyvale, CA 94089
Tel. 408.227.4500 | Fax. 408.227.4550 | info@arubanetworks.com
<http://www.arubanetworks.com>