Migrating Your Controller-based WLAN to Arista Cognitive WiFi™

Introduction

Wireless LAN (WLAN) controllers have been prevalent in large enterprise and campus WiFi deployments for over a decade. But controller-based architectures have not changed much since inception. In today's world, where the density and quantity of WiFi networks has exploded, WiFi has moved from being a convenience to the exclusive way of accessing the network. As the diversity of clients and applications running on WiFi has simultaneously increased, controller-based architectures present serious shortcomings: complex management, high maintenance overhead, proprietary hardware, single point of failure, limited scalability and high cost.

The first generation of controller-less and cloud-based WiFi solutions served small-to-medium and distributed enterprises but they did not meet the needs of larger enterprise and campus deployments. Their poor performance, unreliability, limited scalability, lack of features, and the requirement of fundamental changes to the underlying network design kept large enterprises and higher education institutes from adopting controller-less and cloud WiFi solutions.

Cognitive WiFi — Designed For Large Enterprise and Campus Deployments

Arista Networks, with its innovative cloud architecture, meets the needs of high-performance, high-density and secure WiFi networks in large enterprises and campuses by providing Cognitive WiFi™, a scalable, reliable, secure, extensible, and feature-rich WiFi solution.

Now that you have decided to take advantage of cloud, the challenge is how to migrate from a controller-based WLAN to the cloud. This white paper discusses the key considerations for migrating from a controller-based WLAN to Arista Cognitive WiFi.

Key Considerations for Migrating to Arista Cognitive WiFi

1. Do I need to change the AP placement?
Unless the WLAN network requirements have changed, AP replacement can occur one-for-one during migration. Some of the factors that may change the WLAN requirements are:

- Need for better RF coverage
- Higher WiFi client density
- More diverse types of WiFi client devices
- Application QoS requirements
- Application bandwidth requirements
- Changes in the physical environment
- Need for better reliability as WiFi become the exclusive way to access the network

These factors should be considered regardless of WLAN architecture: controller-based, controller-less or cloud.

2. Do I need to change the underlying network design or VLAN architecture?
If you are replacing an existing controller-less or cloud-based WLAN system with Cognitive WiFi, then replicating the SSID-to-VLAN mapping is straightforward and should not require any changes to your underlying network design.
Most controller-based WiFi deployments use tunnel mode. Each AP tunnels the traffic from its WiFi clients back to the controller that in turn switches the packets to the VLANs. In many cases, a flat network design with a single VLAN is used.

The Arista architecture supports tunneling with a virtual server that can run on an x86 platform and dynamically terminate GRE tunnels from Arista APs. So you can integrate Cognitive WiFi into your existing network architecture with no required changes to the underlying network design or VLAN architecture.

3. Can I gradually migrate to Cognitive WiFi and have my current WLAN and Arista WiFi coexist?
Yes, you can have your existing WLAN and Arista WLAN coexist. Arista's architecture allows the Arista WLAN to coexist alongside your current controller-based WLAN and can help you gradually transition your WiFi deployment to Cognitive WiFi without any downtime. A recommended approach to minimize any impact is to first migrate locations that have separate RF and network boundaries, e.g., a building in a large campus, or a remote branch site. This will help validate the Arista WLAN operation at an independent site and help create a blueprint for migrating the rest of the network.

4. How does authentication and roaming work with Arista in a multi-vendor WLAN environment?

802.1x
Both the existing WLAN and Arista WLAN should be mapped to the same RADIUS server. This ensures that the same EAP types and authentication databases are used and that the RADIUS server behaves consistently with WiFi clients regardless of which vendor's APs they are associated with. Unlike a controller, RADIUS requests come directly from the Arista APs.

Pre-Shared Key (PSK)
As long as the same PSK is configured on an SSID running on your current WiFi APs and Arista APs, the WiFi clients on that SSID should experience no difference.

Roaming
WiFi clients can roam between your existing WLAN and the Arista WLAN if the ESSID and VLAN configuration is identical. As long as the configuration is the same, the client ends up on the same VLAN being served by the same ESSID regardless of which vendor's AP is handling the WiFi client's communication.

One caveat for 802.1x authentication is the lack of fast roaming support—using Opportunistic Key Caching (OKC) or 802.11r—while roaming between your current WLAN and Arista WLAN. In fact, the user experience will be no different than a WiFi client roaming between two controllers of the same vendor because most vendors do not support key caching across controllers. In absence of fast roaming, when a WiFi client roams across a WLAN boundary (from one vendor's WLAN to another or from one controller to another of the same vendor), a full 802.1x authentication transaction occurs. This is mostly seamless to WiFi clients on a single VLAN and is unlikely to cause any perceptible issue beyond a momentary glitch for real-time interactive applications such as VoIP.

5. How do Arista APs communicate to the Cloud?
Arista APs only require Internet connectivity to automatically discover and connect to the Arista Cognitive WiFi. When an Arista AP is deployed, it first connects to Arista's redirector, which maps the AP's serial number to the customer and points (redirects) the AP to the customer's Arista WiFi instance.

Arista APs use UDP port 3851 for cloud communications and require the firewall at the customer site to be configured for allowing outbound traffic on that port. All communication between Arista APs and the cloud is AES-encrypted and FIPS 140-2 certified. If APs cannot reach the cloud on port 3851, they fall back to port 443.

The following table summarizes the port numbers used by Arista APs to communicate with Arista WiFi.

Port	Source	Destination	Function
UDP 3851	AP management network	Redirector and Cloud server URL	AP to Cloud communication – encrypted management traffic
TCP 443	AP management network	Redirector and Cloud server URL	Backup for AP to Cloud communication if UDP port 3851 is blocked – encrypted management traffic
TCP 80	AP management network	Cloud server URL	AP firmware upgrade – encrypted bundle
UDP 3852	AP management network	Cloud server URL	Optional – for integration with on-prem IT systems such as NMS, SIEM, and WLAN controllers.

6. What type of traffic is exchanged between Cognitive WiFi and APs and what is the typical WAN bandwidth requirement?
The communication between Arista APs and the cloud is limited to management traffic—networking monitoring updates are sent from the APs to the cloud and configuration changes are sent from the cloud to the APs. Arista APs do not send any data traffic to the cloud. Typical WAN bandwidth requirement per AP is about 1.5 Kbps.

7. Can Cognitive WiFi integrate with other IT systems that the controllers integrate with?
A key requirement of an enterprise WLAN is the ability to integrate with Network Management System (NMS) and Security Information and Event Management (SIEM) systems. Information is gathered by the following means:

- Polling: NMS periodically poll WLAN controllers for status, events, and other information.
- SNMP Traps: Trap notifications are sent from the WLAN to NMS and other systems such as IT helpdesk ticketing for automated action.
- Syslog: SIEM systems often use Syslog to gain a rich, real-time view of the network.

Traditional cloud-based WLAN solutions have two weaknesses:

1. The remote cloud management system does not have visibility into the local network at a customer site.

2. Cloud-managed and controller less WLAN APs talk directly to local NMS systems via SNMP or Syslog. This drastically increases the number of manageable elements on the NMS dashboard but doesn't provide a system-wide, correlated view of events.

Arista Cognitive WiFi overcomes these challenges by communicating directly to the customer NMS and SIEM systems using a dynamically created VPN tunnel on UDP port 3852.
The tunnel is terminated at an Arista AP operating in a special Cloud Integration Point (CIP) mode and residing on the customer network. The CIP forwards Syslog messages to

NMS and SIEM, and polls co-existing WLAN controllers, e.g., Aruba and Cisco, for WIPS integration.

8. Will my WLAN go down if Arista APs lose connectivity to the cloud?
Arista APs communicate with the cloud only for management purposes, e.g., for sending network monitoring information and to receive configuration changes, and do not rely on the cloud for handling data traffic or for any control plane operations, e.g., RF optimization. If the connectivity between Arista APs and the cloud goes down, the Arista APs continue to operate in a stand-alone mode without loss of functionality. WiFi clients see no difference and are able to associate, communicate and roam across Arista APs as they would normally do. The Arista APs also continue to enforce the wireless security policies. Once the cloud connectivity is restored, the Arista APs send cached network monitoring updates to the cloud and receive configuration changes, if any.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062