

Arista Wireless: Q&A

What is Wi-Fi 6?

Wi-Fi 6 is the latest wireless LAN standard. It is also known as 802.11ax.

What are the key benefits of Wi-Fi 6?

The key benefits are:

- More deterministic uplink and downlink performance.
- Higher data rates with peak Gbps speeds
- Increased network efficiency (by up to 4 times)
- Improved performance in high client density environments
- Improved power efficiency and longer battery life on client devices

Do I have to change all my clients to connect to Wi-Fi 6 network?

No. Wi-Fi 6 is backward compatible and will support all current wireless clients.

Will Wi-Fi 6 APs need 803.bt power?

Yes, for full functionality, Wi-Fi 6 APs will require 802.3bt power. However, most APs will function on 802.3at power as well, with some services reduced. The AP data sheet will specify this in detail.

How far does a Wireless signal travel?

In an open area with no obstructions, a wireless signal transmitted by a typical WiFi AP can travel approx 300ft before it becomes unusable.

Note that the further away a device moves from the AP, the slower its connection becomes. If there are obstructions like walls, buildings, trees and other sources of RF interference (example: bluetooth and other wireless devices) in the vicinity of the signal - the deterioration of signal quality occurs much closer to the AP. A site-survey is always recommended to establish the usable coverage area of an AP.

How many clients can connect to a single AP?

The number of client associations is typically set to be 512 per radio on an Arista AP. However, this is never the recommended design. The number of APs to client ratio is decided based on the throughput needs of the end devices, as well as the RF environment of that location.

How is the management plane tunnel between AP and cloud secured? Can Arista anonymize the connection and the data at the AP?

Arista provides authentication and privacy of data sent from AP to the cloud. TLS 1.2 128-bit encryption is used between the AP and the CV-CUE management platform (cloud or on-prem device).

What kind of actions can be taken from the cloud for a local Wi-Fi failure?

A multitude of tests and troubleshooting data is available from the CV-CUE interface including :

- Client debug logs
- Client event logs
- Wired and Wireless packet traces.

Additionally, APs that include the 3rd radio can:

- Take a wireless sniffer trace on any channel (2.4 and 5GHz bands),
- Perform client connection tests (includes Wi-Fi, wired, Application, VoIP, and data performance)
- Perform spectrum analysis
- Can radio-trace client connections
- Take a packet capture

Which tunneling protocols do the APs support?

APs currently support EoGRE on a per-SSID basis. They also support VxLAN encapsulation which can be de-encapsulated by any Arista 720XP campus switch.

Do I need to change the AP placement when migrating to Arista Wi-Fi?

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

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

Do I need to change the underlying network design or VLAN architecture when migrating to the Arista solution?

If you are replacing an existing controller-less or cloud-based WLAN system to Arista's CV-CUE, then replicating the SSID-to-VLAN mapping is straightforward and should not require any changes to your underlying network design.

Most controller-based Wi-Fi deployments use tunnel mode. Each AP tunnels the traffic from its Wi-Fi 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 to Arista switches using standards based tunneling methods such as VxLAN. So, you can integrate CV-CUE into your existing network architecture with no required changes to the underlying network design or VLAN architecture.

Can I gradually migrate to Arista's Wi-Fi and have my current WLAN and the Arista Wi-Fi coexist?

Yes, you can have your existing WLAN and Arista WLAN coexist. Arista's architecture allows the Arista WLAN to co-exist alongside your current controller-based WLAN and can help you gradually transition your Wi-Fi deployment to Cognitive Wi-Fi 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.

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 Wi-Fi 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 Wi-Fi APs and Arista APs, the Wi-Fi clients on that SSID should experience no difference.

Roaming:

Wi-Fi 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 Wi-Fi 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 Wi-Fi 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 Wi-Fi 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 Wi-Fi 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.

How do Arista APs communicate to the Cloud?

Arista APs only require Internet connectivity to automatically discover and connect to Arista CV-CUE management. 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 Wi-Fi 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.

What type of traffic is exchanged between CV-CUE and the APs and what is the typical WAN bandwidth requirement?

The communication between Arista APs and the cloud is limited to management traffic—networking monitoring APs do not send any data traffic to the cloud. Typical WAN bandwidth requirement per AP is about 3 APs. a

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. Wi-Fi 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 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.

Can CV-CUE 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.

Is Arista Wireless GDPR compliant?

Yes, the Arista wireless cloud is GDPR compliant. For further information click on the link below:

<https://support.wifi.arista.com/support/solutions/folders/9000184874>

What kind of APIs are supported by Arista Wireless?

REST APIs are supported both in CV-CUE and from APs. Along with push and pull of data, periodic and real-time integration with third-party systems is supported. The APIs can be used to manage many parameters including users, location and layouts, devices, events, reports, templates, association and analytics, logs of user actions along with local policies and even troubleshooting.

What kind of APIs are supported by Arista Wireless?

A comprehensive set of REST APIs are supported by all Wi-Fi services to configure and monitor network parameters as well as build custom applications. CV-CUE, Arista's WLAN manager, is built entirely on APIs. For more information click on the link below:

<http://apidocs.mojonetworks.com/>