Arista Wi-Fi 6 and 6E: Q&A

What is WiFi 6E?

WiFi 6E is the industry name that identifies Wi-Fi devices that operate in the 6GHz frequency range. It offers the features of Wi-Fi 6 extended into the 6 GHz band.

What are the key benefits of WiFi 6E?

The key benefits that Wi-Fi 6E adds to Wi-Fi 6 are :

- Additional 1200 MHz spectrum capacity through contiguous spectrum blocks.
- 14 new 80 MHz channels or 7 additional 160 Mhz wide channels.
- Less congested band
- No backward compatibility for Wi-Fi clients
- WPA3 is required for Wi-Fi Alliance certification

Do I have to change all my clients to connect to WiFi 6E radio?

Yes. existing clients do not support the new 6 GHz band. That also guarantees that only fast clients use the channel resulting in the best performance.

Is the new 6 GHz frequency band available worldwide?

No. Currently (August 2021) 6 Ghz band is available as an unlicensed band in the FCC domain and several different countries around the world. You can check the availability for your region/country here.

Will WiFi 6E APs need 803.bt power?

Yes, for full functionality, WiFi 6E APs will require 802.3bt power. However, most APs will function on 802.3at power as well, with some services reduced. The AP datasheet will specify this in detail.

Will we need more access points to get the best coverage for the new 6 GHz band?

There is slightly higher attenuation for the 6 GHz band than it is for the 5 GHz band and the difference is small enough that we do not expect the need for a higher AP density.

How many clients can connect to a Wi-Fi 6E radio?

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 do I protect investment into the new Wi-Fi 6E access point before more 6 GHz client devices become available?

Arista's new C-360 Wi-Fi 6E access point features a multiband 5 GHz/ 6 GHz radio which allows you to use the AP as a dual 5 GHz until the number of 6 GHz clients justifies switching the radio to 6 GHz.

Are they any new security threats with the 6 GHz band?

Arista is committed to security and the APs are designed with security in mind. Arista’s new C-360 access point includes the 4th radio to:

- Take a wireless sniffer trace on any channel (2.4 GHz, 5GHz and 6 GHz bands),
- Perform client connection tests (includes WiFi, wired, Application, VoIP, and data performance)
- Perform spectrum analysis
- Can radio-trace client connections
- Take a packet capture
- Act as a Wireless Intrusion Prevention System (WIPS)

Are there any other security considerations for the 6 GHz band?

Wi-Fi Alliance makes WPA3 and Enhanced Open security mandatory for Wi-Fi 6 and Wi-Fi 6E. However, there is no WPA2 backwards compatibility for the 6 GHz band. Practically that means that PSK protected and Open SSIDs cannot exist in the 6 GHz band and 6 GHz SSIDs will have to be separate SSIDs on your wireless network.

Do I need to change the AP placement when migrating to Arista WiFi?

AP placement should always consider the following requirements:

- RF coverage
- WiFi client density
- Diverse types of WiFi client devices
- Application QoS requirements
- Application bandwidth requirements
- Physical environment
- Need for reliability as WiFi becomes the exclusive way to access the network

These factors will dictate the number of access points and their placement and may result in one-for-one replacement or in the need for more access points.

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 Cloudvision 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 to Arista switches using standards based tunneling methods such as VxLAN. So, you can integrate Cloudvision WiFi into your existing network architecture with no required changes to the underlying network design or VLAN architecture.

Can I gradually migrate to Arista's WiFi and have my current WLAN and the Arista WiFi 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 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.

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.

How do Arista APs communicate to the Cloud?

Arista APs only require Internet connectivity to automatically discover and connect to Arista Cloudvision WiFi 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 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.

What type of traffic is exchanged between Cloudvision WiFi 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 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 3 - 4 Kbps.

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.

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?

A comprehensive set of REST APIs are supported by all WiFi services to configure and monitor network parameters as well as build custom applications. CloudVision WiFi, Arista's WLAN manager, is built entirely on APIs. For more information click on the link here.