When to stop supporting WPA3/OWE transition modes?

Wi-Fi 6E mandates the use of WPA3 to ensure better security on the wireless link. However, one can expect to see a significant number of WPA2 client devices until the client ecosystem matures to 100% adoption of WPA3. For serving client devices that do not yet support WPA3, an enterprise network can operate in WPA3-Enterprise transition mode where WPA2 and WPA3 are both supported. In this mode, Management Frame Protection (MFP) is optional. Legacy clients can connect using WPA2 without MFP, while WPA3 capable clients can connect using WPA3 with MFP enabled. The use of MFP is mandatory for WPA3 clients, even though the AP advertises it as optional.

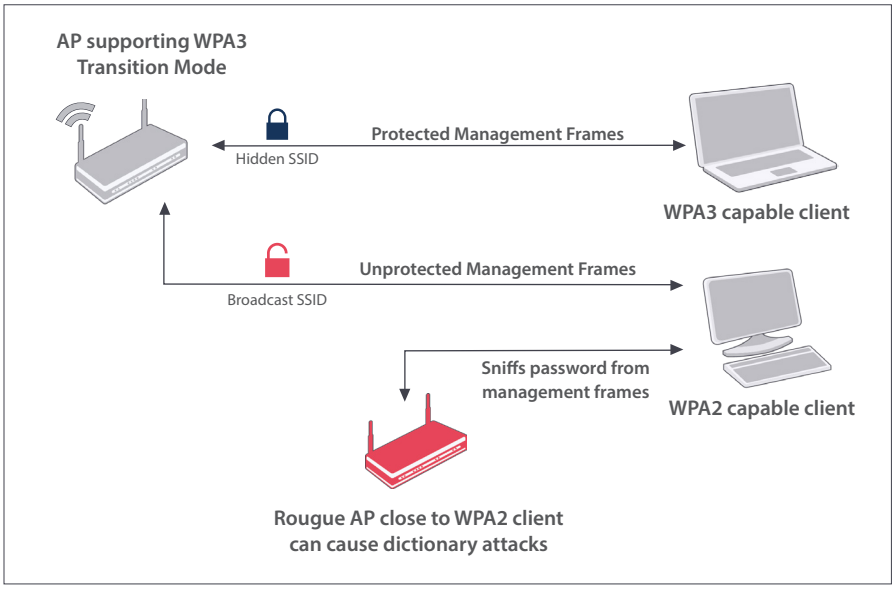
A parallel to the WPA3-Enterprise in public Wi-Fi networks is the Opportunistic Wireless Encryption (OWE). OWE encrypts the AP-client communication with Diffie-Hellman key, exchanged in a 4-way handshake. OWE also supports a transition mode where legacy clients are allowed to connect to the network without any encryption.

Both WPA3 and OWE transition modes require that the AP activate two BSSIDs – a BSSID with broadcast SSID in legacy mode and a BSSID with a hidden SSID using WPA3/OWE. Legacy clients that do not support WPA3/OWE associate with the AP on the broadcast BSSID whereas WPA3/OWE capable clients associate on the hidden BSSID. However, depending upon the client driver implementation, some clients capable of WPA3/OWE may continue to use the legacy security mechanisms just because they are available, and do not associate with the WPA3/OWE BSSID.

Vulnerabilities in Transition Modes

Any network is only as secure as its weakest link. A network operating in the WPA3 transition mode is vulnerable because the same password is used for both WPA2 and WPA3, leaving the network at risk of dictionary and spoofing attacks. This scenario is depicted in the figure below. The fact that WP3 clients stay protected using MFP doesn't help, as the legacy clients and hence the network, are still at risk.

Another disadvantage of supporting transition mode is that the AP must maintain two SSIDs. The broadcast SSID introduces management overhead, which can lead to more contention in the network.



WPA2 clients at the risk of dictionary attacks in WPA3 Transition Mode

When to stop supporting WPA3-Enterprise/OWE Transition Modes?

The transition mode should be supported only as long as required for the clients in the enterprise to be upgraded to the newer security protocols. The benefits of better security mechanisms can be realized to their full potential only when all the devices in the network are WPA3/OWE capable.

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