Aruba Networks Position Statement on CAPWAP

The CAPWAP (Control and Provisioning of Wireless Access Points) protocol, currently published in the IETF as RFC5415, has the potential to someday allow access points and wireless LAN controllers from different vendors to interoperate with each other. This Technical Brief will explain what CAPWAP is as well as what it is not and will present Aruba’s position on CAPWAP.

Overview of CAPWAP
The CAPWAP protocol defines a management and control protocol between centralized wireless LAN controllers and thin access points. Work on CAPWAP was begun in 2003 with the original publication of an Internet draft called LWAPP (Lightweight Access Point Protocol) written principally by Airespace, a company later acquired by Cisco. After the IETF approved a working group to standardize an AP control protocol, LWAPP was chosen as the basis for the CAPWAP protocol. LWAPP, however, was shown to have numerous security flaws, so while some of the messaging framework of LWAPP was preserved, an entirely new security scheme was required. The CAPWAP protocol of today thus bears little resemblance to LWAPP circa 2003.

Current Limitations of CAPWAP
There are significant limitations with CAPWAP today. Most notably, any vendor moving to CAPWAP for its current offering would find significantly less functionality available. This is because CAPWAP defines a “least common denominator” approach to AP control, and does not (some would argue “cannot”) allow for all the different architectures and features provided by all vendors in the enterprise WLAN space. Given the current state of the Wi-Fi market, many argue that a closed and proprietary system is required to support the pace of new development. As one example, since the time that CAPWAP development began, the IEEE has progressed on 802.11n, 802.11k, 802.11r, and 802.11y. CAPWAP takes none of these developments into account, and given the pace of standards development and ratification, it may be several years before CAPWAP catches up.

CAPWAP also suffers from intellectual property rights (IPR) encumbrances related to claims made by Cisco. As of March 2009, Cisco has not disclosed exactly which portions of CAPWAP are subject to its IPR claims. Thus, any vendor implementing CAPWAP may find itself subject to royalty claims by Cisco, without the ability to develop a non-infringing alternative compatible solution because of lack of disclosure. Cisco’s statement may be found at http://www.ietf.org/ietf/IPR/cisco-ipr-draft-ietf-capwap-protocol-specification.txt. The position taken by Cisco makes it difficult for competing vendors to adopt CAPWAP.

Aruba’s Position on CAPWAP
Aruba is fully supportive of standards and interoperability, and CAPWAP is no exception. Aruba representatives fully participated in the development of CAPWAP and an Aruba representative is listed as an editor of RFC5415. However, Aruba’s position today is that CAPWAP represents a “least common denominator” approach to wireless AP management. CAPWAP needs to evolve significantly before it can approach the capabilities of today’s vendor-specific systems.

From a market demand standpoint, Aruba has not seen and does not anticipate significant demand for APs and controllers from different vendors interoperating. Aruba has conducted extensive surveys amongst its customer base of over 6,000 enterprises, and overwhelmingly these customers expressed a preference for buying APs and controllers from the same vendor. Where Aruba anticipates CAPWAP becoming useful in the future is for special-purpose APs that Aruba may not offer itself – for example, specialized industrial APs with ratings for heavy vibration or explosive environments. CAPWAP would allow specialized vendors to build such access points without customers needing to integrate multiple systems.
Aruba customers who today have wireless LAN equipment from multiple vendors are able to integrate these networks using the AirWave Wireless Management Suite, a multi-vendor management platform that integrates monitoring, control, configuration, and visualization. This solution is already well-proven in the field.

**Frequently Asked Questions**

**Q:** Which vendors have implemented CAPWAP?

**A:** It is the opinion of Aruba Networks that at the time of this writing in March 2009, no wireless LAN vendor has implemented CAPWAP as defined in RFC5415. Any vendor who claims to support CAPWAP is using proprietary extensions to the protocol that make it non-interoperable with any other vendor claiming to support CAPWAP. It is also Aruba’s opinion that any vendor who did support RFC5415 and only RFC5415 as its control and management protocol would not be competitive in the market due to lack of functionality.

**Q:** Will Aruba implement CAPWAP someday? When?

**A:** Providing the IPR claims made by Cisco become more clear, it is likely that Aruba will provide support for CAPWAP in the controller software at some point in the future. As of this writing, a prediction of when that may happen cannot be made.

**Q:** Will Aruba replace its own AP control and management protocol with CAPWAP?

**A:** It is very unlikely that the current protocol, known as PAPI, will be replaced by CAPWAP. This would be a very disruptive change to Aruba’s customers with no obvious benefits.

**Q:** Is Aruba’s equipment capable of supporting CAPWAP?

**A:** Yes. An implementation of CAPWAP is simply the protocol specification written into software. There are no hardware dependencies that would make Aruba equipment incompatible with the CAPWAP protocol.

**Q:** How is the AirWave Wireless Management System involved with CAPWAP?

**A:** AWMS can monitor, control, and configure Cisco wireless LAN equipment from multiple architectures, including standalone, SWAN, LWAPP, and CAPWAP.