Commercializing heterogeneous networks with CAPWAP

The introduction of 11ac marks an important inflection point, where several vendors are now realizing the importance of RFC-compliant CAPWAP, in order to support multi-vendor wireless networks in future.

TECHNOLOGY BRIEF

The maturity of wireless deployment worldwide in Enterprise and Service Provider networks is driving wireless equipment vendors and chip vendors to add RFC-compliant Control And Provisioning of Wireless Access Points (CAPWAP) to their roadmaps and products. Whether one sees this shift as a threat or an opportunity, rather depends on where in the wireless eco-sphere each vendor stands.

Europe and North America

In Europe and North America which account for ~75% of the $4B annual WLAN equipment market, the opportunities for green-field deployment are few and far between in almost every vertical market. Many Enterprises, especially the early adopters, are in their second or third refresh, with over 90% of APs purchased in 2012 supporting 11n.

To oust an incumbent competitor in these mature markets, savvy vendors recognize they must co-exist with legacy gear from other vendors, as it becomes due for replacement. Doing this requires interoperability at the management level, in one way or another. This is what CAPWAP is intended for. However, until now it has failed to fulfill this purpose, because almost no-one is using an RFC-compliant CAPWAP stack. Long term however, vendors must embrace interoperability if they want to compete for a piece of the action in heterogeneous wireless networks. Hence, some vendors are beginning to take CAPWAP more seriously.

Emerging markets and ODMs

In the emerging markets of Asia/Pacific and Latin America the situation is reversed. Most deployments are green-field opportunities. However the sales dynamics are different. The Enterprise WLAN equipment market in China alone is worth about $600M in 2013. But many of these new markets are characterized by massive rollouts of *Wireless Cities* by a small few Service Providers, accounting for 30-40% of total Enterprise sales.

The changing dynamics combined with the introduction of 11ac mark an important inflection point. Since 11ac offers so much bandwidth, an average reference design AP offers more than enough capacity and functionality for the majority of use cases. Service Providers simply don't need all the high-end Enterprise features offered by WLAN vendors.

Competitive vendor strategies

A few Enterprise WLAN vendors have already targeted competitor interoperability as a short term, account penetration strategy. By changing their WLAN network management software (NMS) to be able to manage their own network gear as well as some equipment from other vendors.

This is done by reverse engineering management protocols and exploiting SNMP. But it is a strategy that cannot scale. It requires continuous regression testing, and is subject to the whims of the other vendors who continuously change and extend those protocols to enable new features and capabilities with next generation AP products.

This capacity abundance moves buyer focus away from functionality and toward price, further accelerating the commoditization of the WLAN Access Point market. It opens the door for chip vendors and ODMs to flood the market with different flavors of high-performance Access Points at competitive price points that software-burdened WLAN vendors have difficulty matching.

For Service Provider Wi-Fi networks, the sheer volume of CPE devices needed has always made deployment cost the overriding concern in determining the financial viability of large-scale Wi-Fi rollouts. Low cost AP hardware from the growing number of ODMs, is not just an attractive path, it may be the only economically sane option for many managed services applications.

For example, for a managed Wi-Fi service offering to SMBs with 10 or less employees, 11ac is overkill, and many of the Enterprise features in high-end 11ac APs are simply not required. Therefore, paying a premium for high-end APs from WLAN vendors, hugely impacts time to ROI and puts the service offering at risk of being over-priced and uncompetitive. Why pay for fancy software features you cannot monetize, when you can get the minimum you need from ODM hardware at a fraction of the price.

CAPWAP the missing ingredient

Of course, this all hinges on Service Providers and Enterprises having the tools to configure and manage unbranded, heterogeneous networks and provision a consistent set of essential services at any access point. This is where CAPWAP comes in. Service Providers understand that interoperability gives them even more price leverage, so whether the vendors produce interoperable CAPWAP stacks, they are motivated in their own right to have a reliable stack they can implement on any vendors' hardware.

The intent of the CAPWAP protocol is to facilitate configuration, management and provisioning of WLAN Access Points specifying the 802.11 services, functions and resources enabled, in order to allow full interoperability between WLAN Controller and Access Point devices in a heterogeneous deployment.

Properly implemented, CAPWAP should enable any WLAN Controller to perform the following functions with Access Points from any number of different vendors:

- AP discovery
- Authentication
- Association
- Firmware distribution
- Management traffic
- Configuration

CAPWAP reality check

All Enterprise WLAN equipment vendors need and implement some form of communication protocol between controllers and APs and among controllers in order to perform the necessary configuration, management and provisioning functions. Indeed, they all have the CAPWAP protocol or something very similar. But they are not interoperable.

All vendors' implementations are proprietary, and permit only devices from the same vendor to interoperate. This because they have deviated far from the RFC and layered on top of the basic functions, all the advanced features that make them different. In most cases, the deviations are so far-reaching, it is almost impossible for vendors to separate out the minimum feature-set for interoperability. They are not entirely to blame for this.

In fact, one of the shortcomings of the CAPWAP proposed standard is it simply does not properly define all of the necessary requirements for even basic features. And more advanced features for new 802.11 capabilities

CAPWAP Working Group

It was the job of the CAPWAP working group (within the IETF) to bring to fruition a WLAN architecture taxonomy document and a CAPWAP protocol standard to provide interoperability among WLAN backend architectures.

The CAPWAP working group began work on defining the protocol in early 2004. During that time, they received various proposals from different vendors, including Chantry (CTP), Cisco (LWAPP), and Trapeze and Aruba (SLAPP). Since March 2009 the CAPWAP specification has been defined in the form of two standards-track RFCs: CAPWAP (RFC 5415) and CAPWAP Protocol Binding for IEEE 802.11 (RFC5416). Both have an IETF status of Proposed Standard. An additional proposal (RFC5417) specifies CAPWAP AC DHCPv4 or CAPWAP AC DHCPv6, which are two DHCP options for Access Controller discovery. The CAPWAP WG was concluded in May 2010.

are not being added to the spec as time goes on. The spec has been dormant since 2009, while 802.11 has evolved greatly.

Deployment in practice

In practice, to build a heterogeneous wireless network using RFC-based CAPWAP, you need to be willing to ignore advanced features from any one vendor, and replace AP software with a simplified RFC-based CAPWAP stack. Whether Enterprise WLAN vendors are willing to provide such a stack for their AP hardware remains to be seen. ODMs are more motivated to do so. And Service Providers even more so, as they have the most to gain from being able to build heterogeneous wireless networks.

For this reason, Service Providers have approached embedUR to develop stacks for them. We have the know-how to deliver a stack that will run on whichever APs they want to use.

OpenSource CAPWAP

Several efforts have been made to develop and distribute open source CAPWAP stacks based on IETF RFC5415 and RFC5416. The most notable of these is/was a stack dubbed OpenCAPWAP, developed by a group of distinguished computer scientists and software engineers associated with the University Campus Bio-Medico di Roma, Italy. It was based on pre-RFC specifications. As such it is not compliant with the official RFC. Nevertheless, for companies that want to do-it-themselves, this is a starting point. www.opencapwap.org unfortunately no longer exists, but the source code can be found on open-source libraries, such as: https://bitbucket.org/dex0827/capwap/src

The big question to ask about going it alone with an open-source CAPWAP stack is, did its developers have the experience, motivation and infrastructure, to conduct large-scale interoperability testing, and how recently was it done? Followed by the next big question, are there enough people using it, for there to be an experienced support network you can tap into.

Deployment experience is everything, that's where all the scalability bugs get uncovered and worked out. If you don't have the resources to undertake the integration and interoperability testing, this is a poor starting point. The software may be free, but your time and resources are not.

embedUR CAPWAP architecture

Our objective was to develop RFC-compliant CAPWAP stacks for Access Controllers (AC) Wireless Terminations Points (WTP) A.K.A. WLAN Controllers and APs, which were optimized for easy integration into Service Provider networks.

We wanted the stacks to be lean, and designed for maximum portability across operating systems and multi-core processors. We also needed to ensure our solution could scale to meet the needs of large Service Provider deployments.

After evaluating open source stacks, we decided to build our stack from the ground up, and to fully implement the specifications defined in RFC5415 and RFC5416. We felt this was the best way to meet our goals and avoid a common pitfall with open source code - the software bloat that comes from taking a monolithic IP/routing stack and adding CAPWAP on top.

Our ground up approach, has allowed us to separate CAPWAP functionality from the OS, while completely eliminating anything that we do not need. The result is a memory footprint 50-75% smaller than most other CAPWAP stacks. This translates into faster image management and booting of APs, and it also permits a lower cost AP hardware design.

Another benefit of our approach is that it allowed us to focus on one of our core competencies. Namely optimizing control plane and data

plane performance. The data-path and control-path are completely separate. This means that the data-path can be moved to a separate processor or thread to boost performance if needed. Data plane forwarding is all performed without copying buffers, so throughput is excellent even when a standard PC is used as the controller. We estimate throughput performance to be 15-30% higher than most competing CAPWAP stacks.

In general, the architecture is designed for rapid portability. It is not necessary to optimize for each target platform. Instead it is designed to take advantage of the inherent advantages of the target hardware for offload and fast path integration. The stacks are also well designed for easy integration with the end customer's control and provisioning systems making it easier to manage the solution as well as to scale the deployment. For example, features specific to a radio chipset can be added easily to the configuration/management subsystem and added to AC/WTP TLV/messaging.

embedUR CAPWAP experience

Of course, having CAPWAP stacks with proven interoperability is only one third of the solution. The second part is having the resources to help you integrate those stacks on the platform(s) of choice, so you can get to market quickly, and avoid tying up valuable resources deciphering complex protocols. And the third is having access and exposure to the real-world scalability issues that occur on large wireless deployments. embedUR scores well on all counts.

With over 75 wireless LAN engineering projects under our belt, embedUR is the most experienced embedded software engineering firm serving the Wireless LAN industry. We have the core competencies and in-house intellectual property, to rapidly deploy CAPWAP on any multi-core processor system, using any AP reference design or Wi-Fi chipset.

embedUR has a complete understanding of the carrier market and the Enterprise market and has a team of highly experienced engineers who can port embedUR CAPWAP stacks to a customer's platform of choice based on the processor, wireless chipset and the peripherals chosen.

To-date, we have successfully implemented and licensed these stacks in a variety of use cases, including large-scale Service Provider deployments. More information is available under non-disclosure.

Whether you are a Service Provider, chip vendor, Wireless ODM or WLAN equipment vendor, we can help you develop, integrate and test CAPWAP multi-vendor interoperability, in order to achieve fast market entry, and maximize your revenue opportunities in the world of heterogeneous wireless LANs.

embedUR CAPWAP features

- Ultra-compact memory footprint
- Fully RFC5415 and RFC5416 compliant
- AC runs on off the shelf standard Linux PC
- WTP runs on embedded Linux systems
- Automatic AC discovery and association
- Automatic WTP configuration download
- WTP image management features
- Encrypted control traffic with DTLS tunnels
- Local MAC and Split MAC support
- Optimized data plane performance
- All CAPWAP message types supported
- SNMP MIBs are RFC standard compliant
- Full SMNP v1,v2,v3 management
- Integrated diagnostic and debug options