OCP – CBW
Campus, Branch, Wi-Fi

Rajat Ghai
Lead OCP-CBW
Disaggregation of H/W & S/W at the edge
Campus, Branch, Wi-Fi
OCP-CBW 2017

H/W (Wi-Fi)
- 5 open source Wi-Fi H/W choices available
  - 3 Broadcom based designs (802.11 AC Wave 1, MIMO)
  - 2 Qualcomm based designs (802.11 AC WAVE 2, MU-MIMO)

H/W (Branch Switch)
- 2 open source 1Gb PoE Branch Switches

S/W (NOS)
- ONIE support
- Commercial NOS (Mojo Networks)
- Open Source NOS (Network Operating System)
  - CBW Linux (OpenWRT fork)

http://www.opencompute.org/wiki/Networking/SpecsAndDesigns

- OCP Accepted™
- Available @ OCP Marketplace
  - http://www.opencompute.org/products/
DevOPs for Wi-Fi
Walk The Talk: OCP WiFi at US Summit 2018

Sudhan Kayarkar
Mojo Networks
Cloud Managed Enterprise WiFi with 400,000+ APs shipped

2500+ customers

Award-winning Cognitive WiFi™ solution

kate spade NEW YORK
COMCAST BUSINESS
Time Warner Cable
AMC Theatres
Outcomes Health
LG
Yum!
Jio
Gartner’s Magic Quadrant
RED HERRING 100 WINNER
MOBILE BREAKTHROUGH AWARD 2017
STARTUP AWARD 2017
Cloud Disruptor: Enterprise
Cloud Computing 2017
TEXTRON
Costco Wholesale
CareFirst
COSTICIO
OCP WiFi at US Summit 2018

- The Case for Hardware-Software Disaggregation in WiFi
- OCP Accepted™ WiFi deployed at US Summit 2018
- “Open AP” adoption in WiFi industry
- Mojo Networks’ efforts to open up the WiFi industry
The case for HW/SW Disaggregation in WiFi

Same OCP principles that have driven growth for Open Ethernet Switches apply to WiFi Access Points (APs)

• Vendor “Lock In”
  • High deployment cost of APs
  • “Rip-and-Replace” of APs difficult and unfeasible

• High AP HW margins
  • Expensive to buy, implement and operate
  • Value creation primarily in silicon and NOS

• Pace of innovation not meeting market needs

Mojo Networks is committed to leading this Open Standards driven disruption in the WiFi industry
OCP Accepted™ WiFi at Summit 2018

- 24 APs in Main Expo Hall
- 12 EdgeCore OCP APs
- 12 Mojo APs
- Demonstrating OCP AP and vendor AP interoperability
- Serving ~3000 attendees @ OCP Summit
- SSID: OCP18 or z2.4-OCP18
  
  Password: SUMMIT2018

Thank you: EdgeCore Networks, FnTech, OCP Summit Org. Committee, NW & CBW groups
"We do massive WiFi deployments every week at large scale events and we were pleased with how well this Open WiFi network performed" - Networking Team, FnTech
OCP Accepted™ WiFi Access Point @ Summit 2018

Hardware
- Qualcomm 802.11ac WAVE-2 4x4 Dual Band Dual Radio
- Submitted to OCP in Mar 2017
- Available @ OCP Marketplace
  [http://www.opencompute.org/products](http://www.opencompute.org/products)

Software
- U-Boot : Version 2012.07
- ONIE partition : ONIE version 2017.02-rc1
- NOS partition : Mojo NOS Ver. 8.6.1; Linux kernel 3.14.77 based on Qualcomm SDK SPF 5.0.2
Learn more about how we did it

• Coming soon: whitepaper detailing the Open WiFi deployment at OCP Summit
  – Planning for interoperable WiFi
  – Technical challenges
  – Testing and validation
  – Lessons learned from the live event
  – Where can the wireless industry go from here?

• Whitepaper will be available at OCP CBW Wiki
  http://www.opencompute.org/wiki/Networking/CBW Campus2c Branch2CAndWireless
ONIE Overview

• Open Network Install Environment (ONIE) defines a dual partition boot mechanism allowing end users to install their Network OS (NOS) of choice

• ONIE Repository and Build system consists of:
  • Platform independent functionality for NOS installer discovery, ONIE update etc.
  • Well defined hooks and mechanisms to add support for a particular platform i.e. Bootloader, Kernel, Ethernet drivers etc.

• Primary adoption has been for ethernet switches within x86 UEFI ecosystem
### “Open AP” Adoption in WiFi Industry

<table>
<thead>
<tr>
<th></th>
<th>Switches</th>
<th>Access Points</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Architecture (ONIE)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>Mostly x86 &amp; ARM-64</td>
<td>Mostly ARM-32; some MIPS, PowerPC</td>
</tr>
<tr>
<td>Bootloader</td>
<td>Unified Extensible Firmware Interface (UEFI)</td>
<td>U-boot or proprietary</td>
</tr>
</tbody>
</table>
| **Security (ONIE)** | Current ONIE Secure Boot Proposal based on x86 UEFI ecosystem | ・ CPU specific secure boot mechanisms. eg. ARM TrustZone™  
              |                                              | ・ Trust Platform Module (TPM) HW may or may not be present  
              |                                              | ・ NOS vendor key management                       |
| Wireless Certifications | Not applicable                               | Cannot ship without necessary regulatory wireless certifications |
ONIE on WiFi Access Points: Architecture

Approach A

Add ONIE build option to chipset SDK

ONIE Repository + New Access Point Platform support = ONIE AP SW image

Working with chipset vendors to open source patches and components of licensed chipset SDK
ONIE on WiFi Access Points: Architecture

**Approach B**

**Add ONIE build option to chipset SDK**

**Normal SDK build**

- Chipset SDK
- Platform BSP Patches

= Vanilla AP SW image

**Modified SDK with ONIE build option**

- Chipset SDK
- Platform BSP Patches
- ONIE
  - Discovery Scripts
  - Compliant Env Vars
  - Dual Boot Support

= ONIE AP SW image

- No licensing issues related to chipset SDK
- Scalable. ONIE build available immediately for every chipset reference platform
- Lowers adoption barrier for HW vendors; leverages familiarity with chipset SDK
- Enables ONIE and chipset SDK development to happen in parallel
ONIE on WiFi Access Points: Architecture

Summary

• Approach A: Adding Access Point platform support to ONIE
  • Enable HW vendors to submit patches for their Open APs to ONIE repository

• Approach B: Add ONIE build option to chipset SDK
  • Enable HW vendors to generate ONIE builds from Chipset SDKs for their Open APs

Both options could co-exist

<table>
<thead>
<tr>
<th>mlib</th>
<th>bootconfig</th>
<th>sbl</th>
<th>…..</th>
<th>ddr</th>
<th>ssd</th>
<th>rpm</th>
<th>tz</th>
<th>Boot Loader</th>
<th>U-boot Env Vars</th>
<th>RF Cal Data</th>
<th>ONIE Partition Kernel + Initram FS</th>
<th>NOS Partition</th>
</tr>
</thead>
</table>

Logical Flash Partition Layout on a Qualcomm ARM AP platform
ONIE Secure Boot for x86 platforms

- Utilizes UEFI mechanisms
- Establish “root of trust” in HW and Boot Firmware; extend “chain of trust” along boot path
- Components
  - UEFI and databases
  - Shimx64.efi
    - Thin EFI application, typically signed by Microsoft, contains shim owner’s embedded public certificate
  - MokManager.efi
    - Machine Owner Key (MOK) database
    - Allows Enrolment / Removal of NOS Installer / Image keys

Source: ONIE UEFI Secure Boot proposal, Curt Brune
ONIE on WiFi Access Points: Security

• Today, AP vendors implement some sort of verification of signed images to restrict flashing of arbitrary images on their APs.

• U-boot supports “verified boot” starting version 2013.07

• Vendor’s certificate public key is stored in an OTP partition

• Leverage mechanisms like ARM TrustZone™

• Maintaining NOS vendor key databases within the AP SW/HW ecosystem is the main challenge
ONIE on WiFi Access Points: Security

NOS Vendor Key Management Possibilities

• PKI system involving HW and NOS vendors
  • HW vendor generates root CA and programs certificate hash in OTP ROM.
  • NOS vendors get derived CAs from HW vendor’s root CA to sign their NOS images

• Port UEFI to AP HW/SW subsystem and follow the ONIE Secure Boot model
  • UEFI support in u-boot
    • Work in progress (SUSE Linux)
    • EFI variables required for key database management; unclear if supported
  • UEFI on ARM
    • Targeted for Server market to bring uniformity between x86 and ARM
    • May be too disruptive to existing WiFi AP SW ecosystem
“Open AP” Adoption in WiFi Industry: Certifications

• Access Points cannot ship without necessary regulatory wireless certifications
• Possible solution
  • OCP Acceptance to include regulatory certification
  • Approved regulatory domain power tables published for an Access Point must be adopted by NOS vendors
  • Need a model to distribute certification NRE costs that is fair to all
  • Should ONIE for Access Points include WiFi subsystem ?

• FCC does not currently support a certification model that recognizes HW / SW disaggregation

• “RF Calibration Data” partition (unique to an Access Point) must be maintained intact throughout operational lifetime
Bringing Disaggregation benefits to Mojo customers

Open Standards are a core belief at Mojo Networks
They are also a fundamental piece of our business strategy

1. Make APs available at “factory costs” with no margin for Mojo
   – Complete, April 2016

2. Get zero margin hardware out of our financials
   – Complete, December 2016

3. Collaborate with OCP.
   Leverage ONIE to enable end users to install NOS of choice on their APs
   – Continuing to make progress
Leading the Cognitive WiFi revolution

www.mojonetworks.com