AIRHEADS

LAS VEGAS 2012

▶ JOIN: community.arubanetworks.com

▶ FOLLOW: @arubanetworks

▶ DISCUSS: #airheadsconf

Ken Peredia
Aruba Networks
March 2012

TOP 10 TIPS FROM ARUBA TAC

AIRHEADS

#airheadsconf

Objectives: Help our customers understand some of the recent issues around the Region

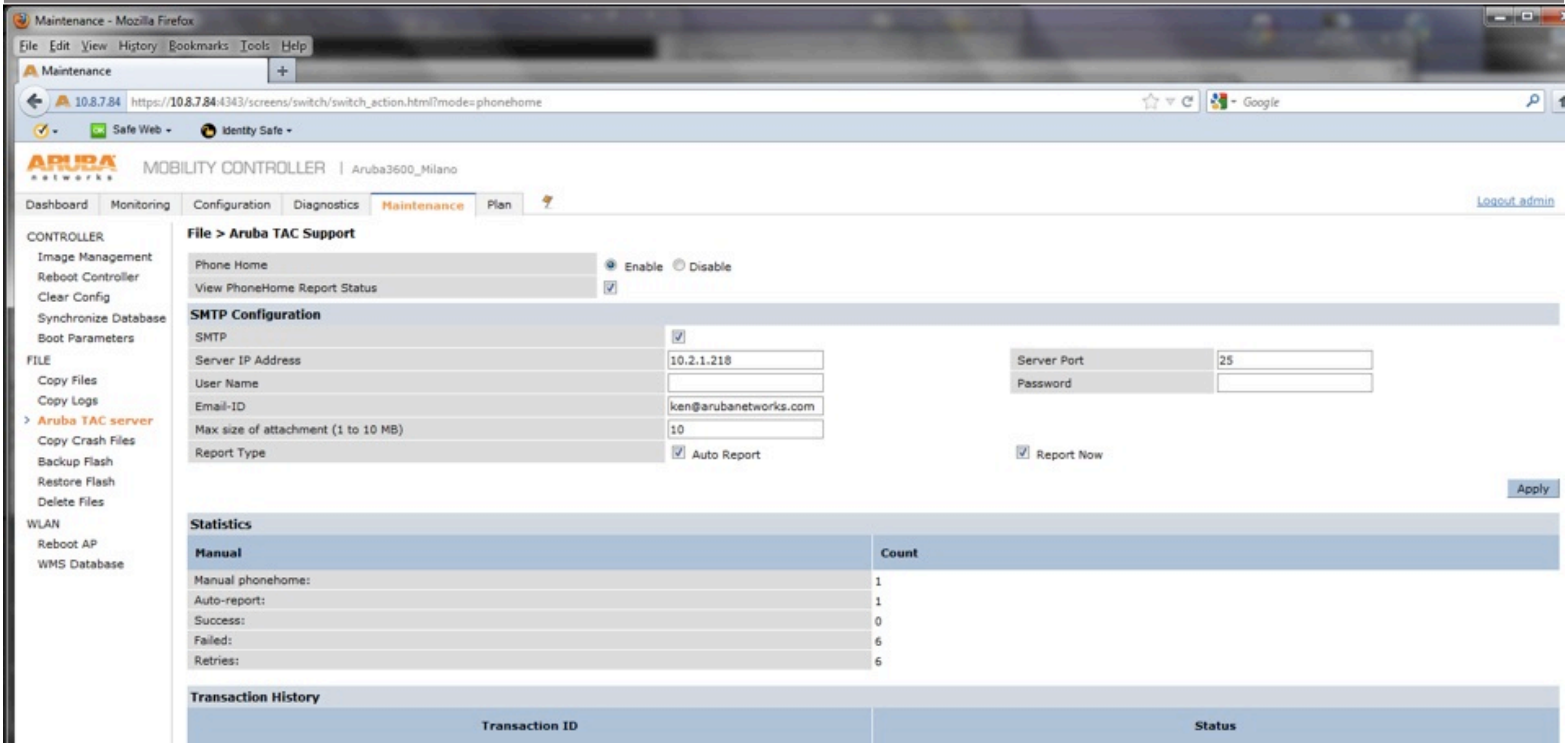
Foreword

Before you open a ticket...

- **Check online resources such as**
  - Airheads Social (community.arubanetworks.com)
  - Aruba Knowledge Base (support.arubanetworks.com)
  - Aruba validated reference designs (VRDs)
  - Software Release Notes

- **Enable PhoneHome on all controllers**
  - phonehome enable
  - phonehome auto-report
  - phonehome smtp <mail server ip address> <email address>

Before you open a ticket…



File > Aruba TAC Support

Phone Home	● Enable ○ Disable
View PhoneHome Report Status	☑

SMTP Configuration

SMTP	☑		
Server IP Address	10.2.1.218	Server Port	25
User Name		Password	
Email-ID	ken@arubanetworks.com		
Max size of attachment (1 to 10 MB)	10		
Report Type	☑ Auto Report	☑ Report Now	

Statistics

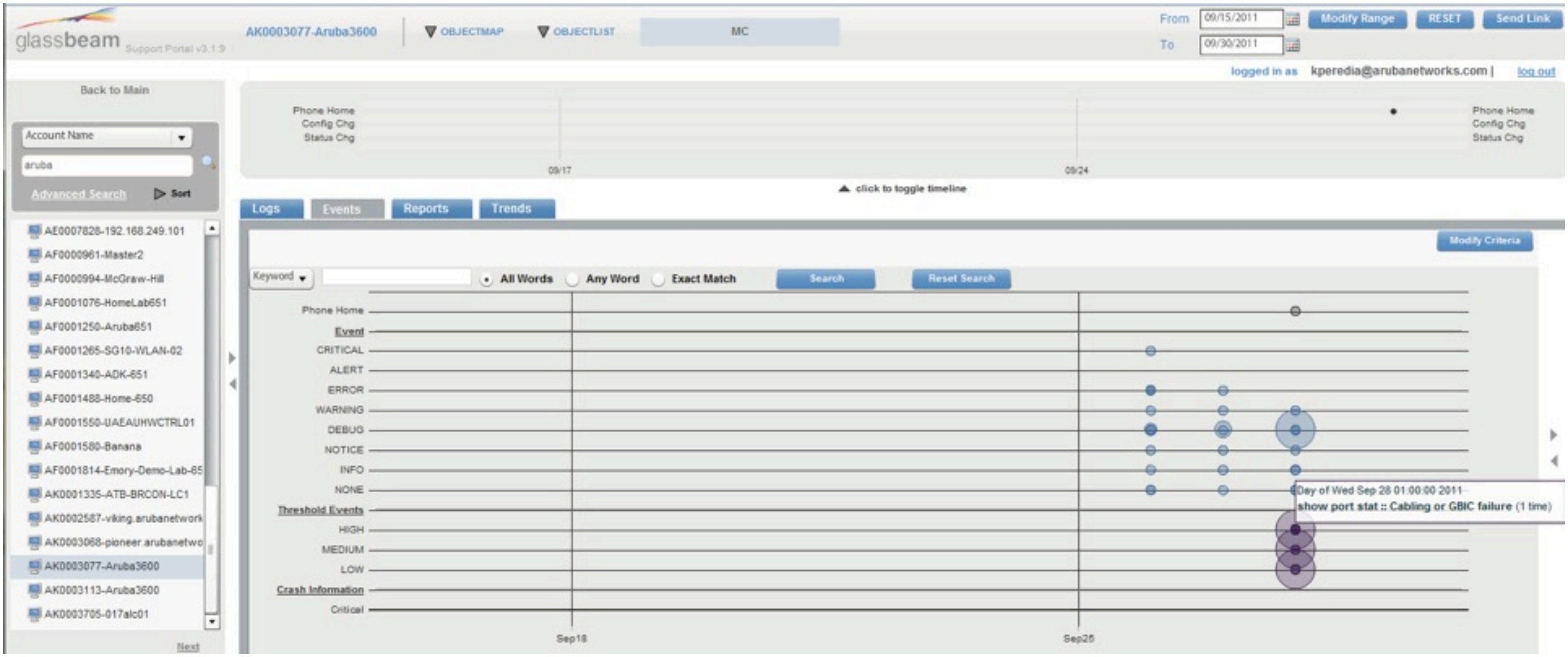
Manual	Count
Manual phonehome:	1
Auto-report:	1
Success:	0
Failed:	6
Retries:	6

Transaction History

Transaction ID	Status

CONFIDENTIAL

Before you open a ticket…



From 09/15/2011

To 09/30/2011

logged in as kperedia@arubanetworks.com | log out

Account Name ▾

aruba

- AE0007828-192.168.249.101
- AF0000961-Master2
- AF0000994-McGraw-Hill
- AF0001076-HomeLab651
- AF0001250-Aruba651
- AF0001265-SG10-WLAN-02
- AF0001340-ADK-651
- AF0001488-Home-650
- AF0001550-UAEAUHWCTRL01
- AF0001580-Banana
- AF0001814-Emory-Demo-Lab-65
- AK0001335-ATB-BRCON-LC1
- AK0002587-viking.arubanetwork
- AK0003068-pioneer.arubanetwo
- AK0003077-Aruba3600
- AK0003113-Aruba3600
- AK0003705-017alc01

Keyword ▾ ● All Words ○ Any Word ○ Exact Match

Day of Wed Sep 28 01:00:00 2011
show port stat :: Cabling or GBIC failure (1 time)

CONFIDENTIAL

#airheadsconf

Before you open a ticket...

- **Check online resources such as**
  - Airheads Social (community.arubanetworks.com)
  - Aruba Knowledge Base (support.arubanetworks.com)
  - Aruba validated reference designs (VRDs)
  - Software Release Notes

- **Pre-empt the support info requests**
  - Be ready to supply “tar logs tech-support”
  - Best to attach it to the ticket, or, send it once ticket is assigned to engineer
    - Don’t attach to original support request email if it is larger than 5MB
  - Console output for RMAs (or a reason why there is none)

Before you open a ticket...

- **Delays to case resolution**
  - Lack of controller logs or logs taken too long after the issue
    - Controller can only store fixed amount of logs, the higher the logging verbosity, the shorter that time is
  - Logs from other points, such as IAS/NPS or client
  - “did it work before” or “new config” ?

- **Try to simplify the issue**
  - Does the simple case work ?
  - Remove any tweaks and optimizations that might be clouding the issue, or, put up a default virtual AP for testing (if possible)
    - Sometimes config is over optimized/tweaked

The Countdown

#10 - Upgrading to 6.1.x

- **Double upgrades are required for most older ArubaOS versions**
  - Latest s/w in most older streams “knows” how to upgrade to release 6.1.x
  - Due to changes in the flash layout on the controller to accommodate larger ArubaOS image
  - This is further complicated for RAPs (to be covered next)
- **Please read the release notes “Upgrade Procedures” section !**
  - 3.3.x (or 3.4.x) → latest 3.4.4.x → 6.1
  - 5.0.x → latest 5.0.4.x → 6.1
  - 6.0.x → latest 6.0.1.x or 6.0.2.x → 6.1

#10 - Upgrading to 6.1.x

- **Aruba 3200**
  - The 3200 is getting low on free memory due to ever expanding feature set of ArubaOS.
  - Aruba has released an “XM” (extra memory) version of the 3200 also a field kit (3200-MEM-UG) where you can upgrade the memory yourself
    - No you can’t use your own memory from local PC shop !
  - A long running or heavily utilized 3200 controller may need to be rebooted to ensure there is enough free memory for the upgrade
  - Non upgraded 3200 will not be supported for ArubaOS 6.2

#9 - Upgrading RAPs to 6.1.x

- **The problem**
  - ArubaOS has a check to ensure that an image that is downloaded during self upgrade is not of unexpected size
  - Prior to 6.x, that maximum was 4MB
  - ArubaOS 5.0.3.x and higher knows that 6.x is > 4MB and has a new maximum size check

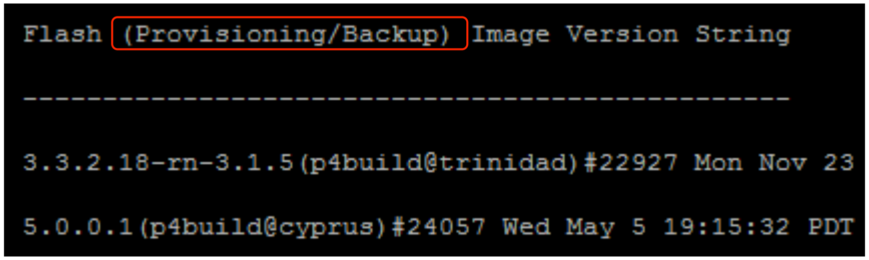
- **Two common issues for RAP2/RAP5**
  - RAP is running 6.1.x due to correct upgrade sequence but has old provisioning image (pre 5.0.3.x)
    - if it is reset to default it will not be able to re-connect/re-upgrade as it reverts to the provisioning image
  - "Brand new out of the box" RAP won't connect to controller
    - It is running older provisioning image.

#9 - Upgrading RAPs to 6.1.x

- **Provisioning image versus running image**
  - RAP5 or RAP2 has 2 s/w images on it
    1. the provisioning image that runs the rapconsole
    2. the production image that is downloaded after first connect to controller
  - The provisioning image can be upgraded via CLI in all releases **except 6.x**
    - CLI command removed in 6.1.x
    - CLI command exists in 6.0.x but fails (6.x cannot be saved)
  - provisioning image is **never** automatically upgraded.
    - Old in-service RAPs may still have 5.0.0.x or 3.3.2 RN code in it.

#9 – Upgrading RAPs to 6.1.x

- **History of RAP factory images**
  - 3.3.2.18-RN (2009~2010)
  - 5.0.0.2 (2010~2011)
  - 5.0.4.0 (**15 Oct 2011** ~ present)
- **What is on my RAP ?**
  - “***show ap image version***”
  - also visible on RAP console

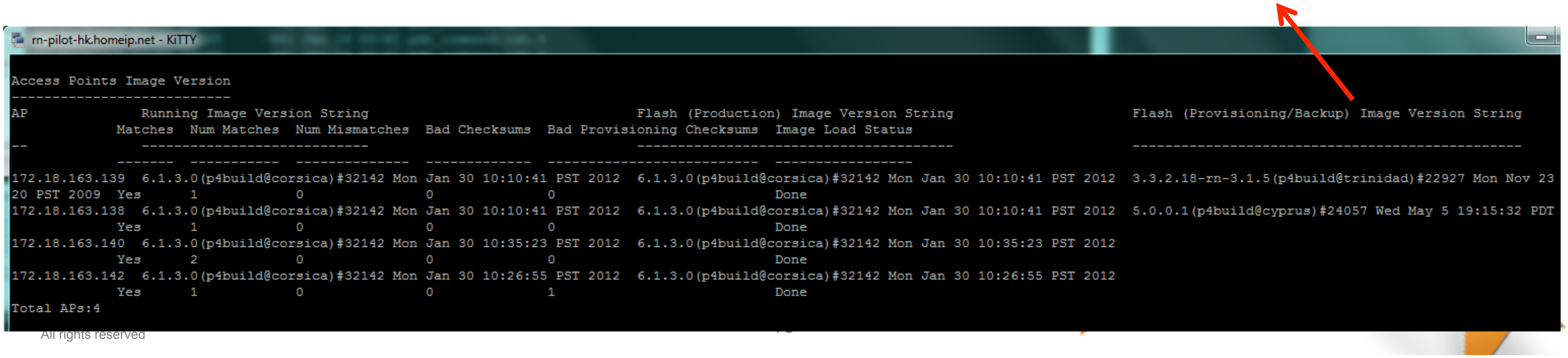


```
Flash (Provisioning/Backup) Image Version String

------------------------------------------------

3.3.2.18-rn-3.1.5(p4build@trinidad)#22927 Mon Nov 23

5.0.0.1(p4build@cyprus)#24057 Wed May 5 19:15:32 PDT
```



```
Access Points Image Version
---------------------------
AP              Running Image Version String                                 Flash (Production) Image Version String                      Flash (Provisioning/Backup) Image Version String
             Matches  Num Matches  Num Mismatches  Bad Checksums  Bad Provisioning Checksums  Image Load Status
--              ----------------------------                                 ---------------------------------------                      ------------------------------------------------
             -------  -----------  --------------  -------------  --------------------------  -----------------
172.18.163.139  6.1.3.0(p4build@corsica)#32142 Mon Jan 30 10:10:41 PST 2012  6.1.3.0(p4build@corsica)#32142 Mon Jan 30 10:10:41 PST 2012  3.3.2.18-rn-3.1.5(p4build@trinidad)#22927 Mon Nov 23
20 PST 2009  Yes      1            0               0              0                           Done
172.18.163.138  6.1.3.0(p4build@corsica)#32142 Mon Jan 30 10:10:41 PST 2012  6.1.3.0(p4build@corsica)#32142 Mon Jan 30 10:10:41 PST 2012  5.0.0.1(p4build@cyprus)#24057 Wed May 5 19:15:32 PDT
             Yes      1            0               0              0                           Done
172.18.163.140  6.1.3.0(p4build@corsica)#32142 Mon Jan 30 10:35:23 PST 2012  6.1.3.0(p4build@corsica)#32142 Mon Jan 30 10:35:23 PST 2012
             Yes      2            0               0              0                           Done
172.18.163.142  6.1.3.0(p4build@corsica)#32142 Mon Jan 30 10:26:55 PST 2012  6.1.3.0(p4build@corsica)#32142 Mon Jan 30 10:26:55 PST 2012
             Yes      1            0               0              1                           Done
Total APs:4
```

#9 - Upgrading RAPs to 6.1.x

- **6.1 Upgrade challenge**
  - The ArubaOS 6.x image is too big to be a provisioning image
  - RAP just hangs after it is provisioned from RAP console
  - Must upgrade provisioning image to 5.0.4.x before trying to upgrade to 6.1.x
    1. Ensure RAP is UP (***show ap active***)
    2. From CLI "apflash ap-name ***someRAP*** backup-partition"

  - **apflash command will cause RAP to reboot** ❗

#9 - Upgrading RAPs to 6.1.x

- **A final comment about RAP upgrades**
  - During 3.x code timeframe, the ap-role did not allow svc-ftp, but it was added as a default in 5.x/6.x
  - Despite the fact a RAP communicates with IPSEC, there are generic protocols running inside the tunnel, ftp being one of them
    - FTP is used to upgrade the s/w on the RAP
    - By default RAP will try FTP a number of times before reverting to tftp, overall this can take 15 minutes or so to time out, delaying the upgrade.
  - Before upgrading a RAP network, please ensure that svc-ftp is permitted in one of the ACLs within the ap-role
    - "***show rights ap-role***" and look for entry allowing "user" to "controller" for svc-ftp

#9 - Upgrading RAPs to 6.1.x

```
(c620) #show rights ap-role

access-list List
----------------
Position  Name      Location
--------  ----      --------
1         control
2         ap-acl

control
-------
Priority  Source  Destination  Service      Action  TimeRange  Log  Expired  Queue  TOS  8021P  Blacklist  Mirror
--------  ------  -----------  -------      ------  ---------  ---  -------  -----  ---  -----  ---------  ------  -------  -------------  ------
1         user    any          udp 68       deny                               Low                                  4
2         any     any          svc-icmp     permit                             Low                                  4
3         any     any          svc-dns      permit                             Low                                  4
4         any     any          svc-papi     permit                             Low                                  4

ap-acl
------
Priority  Source  Destination  Service       Action  TimeRange  Log  Expired  Queue  TOS  8021P  Blacklist  Mirror
--------  ------  -----------  -------       ------  ---------  ---  -------  -----  ---  -----  ---------  ------  -------  -------------  ------
1         any     any          svc-gre       permit                             Low                                 4
2         any     any          svc-syslog    permit                             Low                                 4
3         any     user         svc-snmp      permit                             Low                                 4
4         user    any          svc-http      permit                             Low                                 4
5         user    any          svc-http-accl permit                             Low                                 4
6         user    any          svc-ntp       permit                             Low                                 4
7         user    controller   svc-ftp       permit                             Low                                 4

(c620) #
```

CONFIDENTIAL

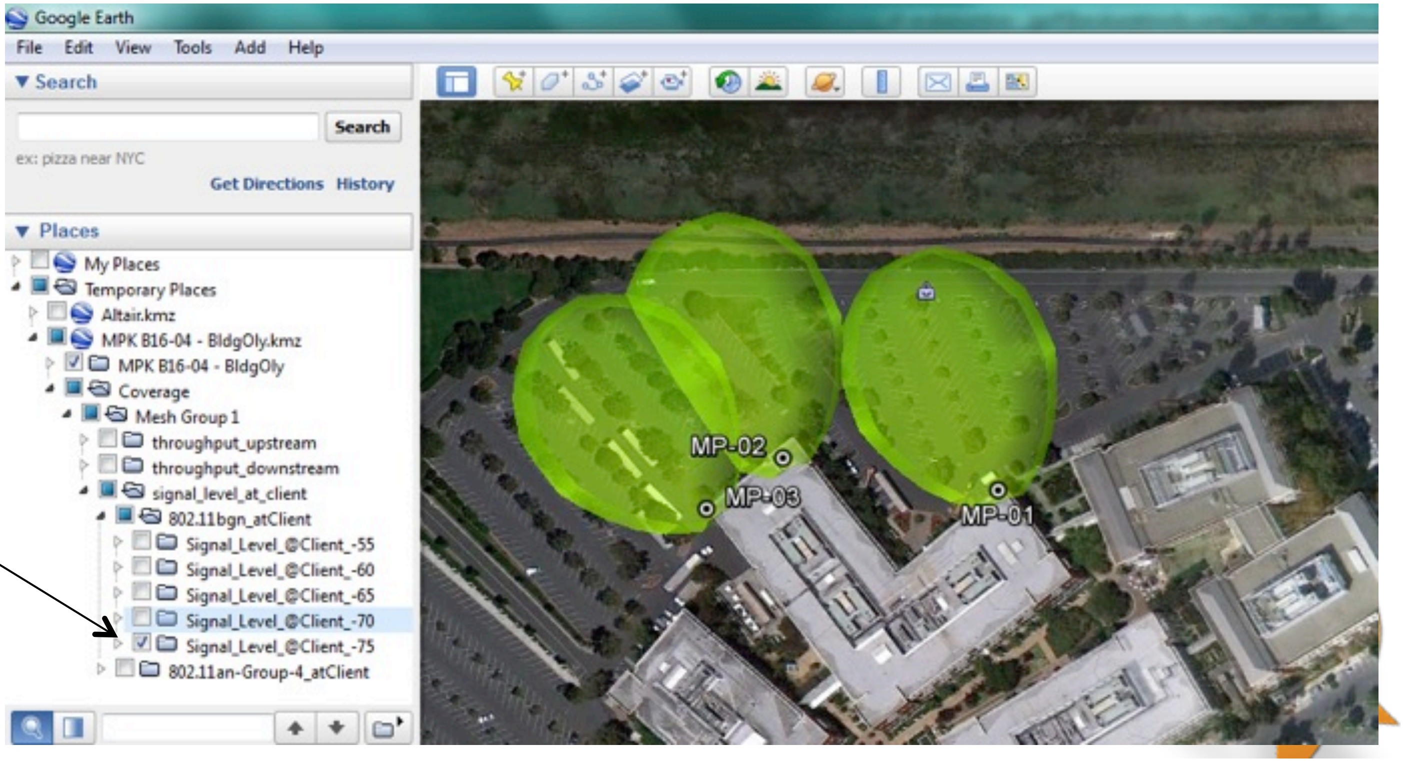
#airheadsconf

#8 – Mesh networks

- **RF RF RF RF !!**
  - Most issues with mesh all come back to RF !
- **Common issues**
  - Insufficient RSSI to achieve the desired rate
    - Use the outdoor planner to predict
  - High gain antenna misalignment
    - Not always good enough to just “aim by eye”
  - Vertical height mismatch on omni antennas
    - Most important over short distance and high gain omnis
  - Hidden nodes
    - All mesh points must hear each other, not just the portal
    - Can mitigate with RTS threshold (to an extent)

#8 – Mesh networks

- **Outdoor planner helps predict performance**
  - Great for understanding the effect of antenna choice and height of antenna
  - Planner knows the regulatory constraints (max EIRP etc.)



-75dBm predicted coverage

#7 – OCSP

- **Online Certificate Status Protocol (OCSP)**
  - Is an IETF standard used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 2560 and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI). Messages communicated via OCSP are encoded in ASN.1 and are usually communicated over HTTP. The "request/response" nature of these messages leads to OCSP servers being termed OCSP responders.

#7 – OCSP

- **You could be running into an issue where web browsers attempt to contact an OCSP server, to see if the captive portal certificate is valid and has not been revoked.**
  - The following browsers (or OS) enables OCSP validation by default:
    - Firefox 3 (on all platforms) enables OCSP checking by default.
    - Safari and Google Chrome in Mac OS X follow system-wide setting in Keychain Access. It was disabled by default prior to Mac OS X Lion (10.7). As of 10.7 (Lion), the default setting is 'Best Attempt'. That means the browser will attempt to perform OCSP validation (or CRL validation) if the information is available in the cert.

#7 – OCSP

- **Since it is not efficient to disable OCSP checking on all your clients, you can open up traffic to the OCSP server in your logon role**
  - For AOS 6.0 and below:

```
netdestination OCSP
  host <ip addresses from the DNS name in the OSCP portion of the certificate>
!
ip access-list session Permit_OCSP
  user   alias OCSP svc-http permit
  user   alias OCSP svc-https permit
!
user-role guest-logon
 captive-portal "guest-cp_prof"
 session-acl logon-control
 session-acl Permit_OCSP
 session-acl captiveportal
!
```

#7 – OCSP

- Using AOS 6.1 and later, the whitelist feature can accomplish the same thing using DNS names. The following example assumes that the OCSP URL embedded in the certificate is http://ocsp.usertrust.com:
  - Netdestination ocsp.usertrust.com
    - Name ocsp.usertrust.com
  - !
  - aaa authentication captive-portal default
    - white-list ocsp.usertrust.com

#6 – Broadcast/Multicast Mitigation

- **Currently, the following knobs mitigate flood traffic in customer networks:**
  - Global Knob
    - firewall broadcast-filter arp
      - This knob would enable broadcast ARP conversion on all vlans and convert all the broadcast ARP req to unicast ARP requests for the target wireless clients (that are part of the station table/user table).
  - Virtual AP profile knobs
    - broadcast-filter arp
      - This knob would convert the mcast ARP request to unicast ARP request (on that VAP) if the target IP/mac is part of user table and station table. And datapath would send the unicast ARP request to the target station.
    - broadcast-filter all
      - This would drop everything else except DHCP today on that VAP. And for the dhcp frames destined to clients, datapath would convert the dhcp broadcast offers/acks to unicast dhcp frames.

#6 – Broadcast/Multicast Mitigation

- Vlan knobs
  - bcmc-optimization
    - This would drop all the bcast/mcast frames on the vlan with exceptions for ARP, DHCP, VRRP. This would mean datapath dropping all other broadcasts/multicast frames on wired interfaces on the vlan also.
  - ip local-proxy-arp
    - This will enable the local proxyARP functionality on the vlan.
    - Controller datapath would proxyARP with target's mac when we receive an ARP request on an L2 vlan if the targetip is a known user thru route cache/user table.
    - On an L3 vlan, datapath would respond with controller mac instead.
  - suppress-arp
    - In addition to enforcing proxyARP functionality, datapath would drop grat ARPs on WiFi tunnels and all ARP flooding on un-trusted interfaces.

#5 – Voice

- **TIPs for deploying Voice over Wi-Fi**
  - Follow the manufacturer's deployment guide
  - Review the "Optimizing Aruba WLANs for Roaming Devices" VRD to see if your voice device has best practice config.
  - Clip the lower data rates.
  - Make sure voip-aware-scan is enabled
  - In 11n deployments make sure the WMM/DSCP markings match the wired QoS settings
    - Also make sure "single-chain-legacy" is enabled in the rf ht radio profile
  - If the voice device supports 5GHz be mindful of what channels it supports. Some phones do not support channel 165 for example.
  - Enable local-probe-req-thresh 25 as a start
  - Do not have more than 2 steps of tx-power diff between APs.

#3 - Client Connectivity/Perf Issues

- **A common support topic!**

- **Frequent causes**
  - RF issues
  - Client driver issues (versions, power save, roaming quirks)
  - Config on controller (ARM, A-MSDU, rates etc.)
  - Important L3 hosts stuck in user table
  - Controller datapath under stress (covered in #4)

CONFIDENTIAL

#4 – Controller under stress

- **Controller can be impacted by network floods or loops resulting in high CPU on datapath**
  - Datapath is where packets are mostly handled
  - Symptoms may be high latency for all clients, slow response of webUI on controller, ping loss to controller interfaces.
- **High CPU can also come from unexpected process behavior**
  - Httpd running high due to high bit HTTPS certs
  - WMS too busy doing IDS type work
- **If you suspect a high CPU condition, collect the following data and contact support for assistance**

#4 – Controller under stress

- **Multiple places to check**
  - show cpuload current
  - show datapath bwm
  - show datapath bridge counters
  - show datapath crypto
  - show datapath frame
  - show datapath maintenance
  - show datapath message-queue
  - show datapath utilization
  - show memory
  - show netstat
  - show processes sort-by cpu

#3 - Client Connectivity/Perf Issues

- **RF Issues**
  - Make use of spectrum analyzer function, or, check the radio stats (covered in the RF presentation)
  - Causes may be 802.11 or non 802.11 related
  - Some s/w options exist, including s/w retry, interference immunity
  - Sometimes 2.4GHz just cannot cope
    - Public events and stadiums are a good example

#3 - Client Connectivity/Perf Issues

- **Client driver issues**
  - Many clients have their own strange behaviors
    - Vendor algorithms for roaming are often secret, some clients are notoriously sticky
    - Same for selection of 11gn vs. 11an for dual band clients
    - Can try a dedicated test SSID profile for a problem client on a single AP
  - Where possible, always try to update drivers
    - Try to work out “everyone affected or just that client”

#3 - Client Connectivity/Perf Issues

- **Client driver issues**
  - Driver settings can influence connectivity
    - Power save and battery/AC status can impact “ping tests”
    - To much “roaming aggressiveness” can cause thrashing
  - Be careful of dual band clients that don’t support the same channel set as the APs
    - Many client chipsets don’t support UNII-2/UNII-2e channels
    - Some Wi-Fi cards are regionalized and may not support your regulatory domain
    - Band-steering may be trying to steer you to a channel the client doesn’t support (i.e. Galaxy Tab doesn’t use UNII-3)

#3 - Client Connectivity/Perf Issues

- **Config on controller**
  - In noisy 2.4GHz environment, default ARM settings may be too aggressive for noise/error threshold channel changes
    - Review ARM history "***show ap arm history ap-name <ap>***"
    - Increase 2.4GHz ARM profile "noise-wait-time" and/or "error-wait-time" to be more tolerant of noisy/congested 2.4GHz
  - Aggressive config tuning for 2.4GHz (especially for voice) can often cause reduced coverage
    - Often results in low speed rates removed from SSID profiles
    - ***wlan ssid-profile <profile> local-probe-req-thresh***
    - Need to find a balance of the right snr

#3 - Client Connectivity/Perf Issues

- **Config on controller**
  - Apple 10.6.x iMAC devices with 3x3 Atheros chipsets sold in 2011 had A-MSDU enabled by default, Aruba had it disabled until recently due to a bug.
    - "***firewall amsdu***"
    - Apple disabled AMSDU by default on 10.7.x
  - Older non-802.11n devices may have interoperability issues with 802.11n APs
    - Commonly seen with handheld/industrial devices
    - Often enabling single chain legacy can help
      - Transmits legacy non 11n frames on single radio chain
      - "***rf ht-radio-profile <profile> single-chain-legacy***"

#3 - Client Connectivity/Perf Issues

- **Important L3 host stuck in user table**
  - If a packet with a source IP of (for example) the default gateway arrives via an IP, the controller will create a user entry for it.
  - This can cause intermittent connectivity issues due to firewall policy or session limit exceeded
  - Often triggered by Windows bridging between wired and wireless. Could also be caused by a host with static IP.
  - Use validuser ACL to prevent users being created for important IP addresses.

```
ip access-list session validuser
  any any svc-sec-papi  permit
  network 169.254.0.0 255.255.0.0 any any  deny
  alias protected_hosts any any deny
  any any any  permit
  ipv6  any any any  permit
!
```

```
netdestination protected_hosts
    host 192.168.1.253
    host 192.168.1.254
    network 10.0.0.0  255.255.255.0
```

#3 - Client Connectivity/Perf Issues

- **Authentication issues**
  - Incorrect time settings on clients can cause certificate validation issues, often silently
  - For windows clients, use MSFT tracing "***netsh ras set tracing * enabled***" to debug issues on Windows side
  - Use ArubaOS command "***show auth-tracebuf***" for all auth issues
    - This is a magical command !
    - Observe how this output looks for successful/regular auth
    - Compare it when problems arise (can often spot certificate issues with this command)

#3 - Client Connectivity/Perf Issues

```
Nov  3 11:08:02  station-up           *  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                   -   -    wpa2 aes
Nov  3 11:08:02  station-data-ready    *  00:21:6a:8b:0a:dc  00:00:00:00:00:00                      180  -
Nov  3 11:08:02  m-auth resp          *  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                     -   -    authenticated
Nov  3 11:08:02  wpa2-key1           <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                      -   117
Nov  3 11:08:02  eap-start           ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                   -   -
Nov  3 11:08:02  eap-id-req          <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                    2   5
Nov  3 11:08:02  eap-id-resp         ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                    2  44    host/pc1.lab.com
Nov  3 11:08:02  rad-req             ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                   11   259
Nov  3 11:08:02  rad-resp            <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30/radpolicy1            11   129
Nov  3 11:08:02  eap-req             <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                   144  6
Nov  3 11:08:02  eap-resp            ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                    144  180
Nov  3 11:08:02  rad-req             ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30/radpolicy1           12   478
Nov  3 11:08:02  rad-resp            <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30/radpolicy1            12   1141
Nov  3 11:08:02  eap-req             <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                   145  1012
Nov  3 11:08:02  eap-resp            ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                    145  6
Nov  3 11:08:02  rad-req             ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30/radpolicy1           13   304
Nov  3 11:08:02  rad-resp            <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30/radpolicy1            13   1137
Nov  3 11:08:02  eap-req             <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                   146  1008
Nov  3 11:08:02  eap-resp            ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                    146  6
Nov  3 11:08:02  rad-req             ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30/radpolicy1           14   304
Nov  3 11:08:02  rad-resp            <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30/radpolicy1            14   1137
Nov  3 11:08:02  eap-req             <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                   147  1008
Nov  3 11:08:02  eap-resp            ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                    147  6
Nov  3 11:08:02  rad-req             ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30/rradpolicy1            15   304
Nov  3 11:08:02  rad-req             ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30/radpolicy1           19   1436
Nov  3 11:08:02  rad-resp            <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30/radpolicy1            19   188
Nov  3 11:08:02  eap-req             <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                   152  65
Nov  3 11:08:02  eap-resp            ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                    152  6
Nov  3 11:08:02  rad-req             ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30/ise-policy1           20   304
Nov  3 11:08:02  rad-accept           <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30/ise-policy1            20   276
Nov  3 11:08:02  eap-success          <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                    152  4
Nov  3 11:08:02  station-data-ready    *  00:21:6a:8b:0a:dc  00:00:00:00:00:00                      180  -
Nov  3 11:08:02  m-auth resp          *  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                     -   -    authenticated
Nov  3 11:08:02  wpa2-key1           <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                      -   117
Nov  3 11:08:02  wpa2-key2           ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                      -   119
Nov  3 11:08:02  wpa2-key3           <-  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                      -   151
Nov  3 11:08:02  wpa2-key4           ->  00:21:6a:8b:0a:dc  00:1a:1e:66:f7:30                      -   95
```

VLAN

username

server

Radius ID
EAP ID

length

result

#3 - Client Connectivity/Perf Issues

- **Recently seen authentication issues**
  - Cannot connect dot1x wireless on XP via RDP
    - Refer **http://technet.microsoft.com/en-us/network/dd727529.aspx#EWKAC**
    - Use VNC instead, resolved vista/NPS2008
  - IAS can “discard” messages, which triggers the ArubaOS “server out of service” as no response is seen
    - Hotfix exists for unknown domain, for other cases always send reject not “discard”
  - XP SP3 clients have PEAP auth issues with NPS 2008
    - http://support.microsoft.com/kb/969111

#2 – Common misconfiguration

- **Spanning Tree**
  - Beware changes to STP type between ArubaOS versions
    - 3.x → 3.4.x RSTP became default
    - 6.x → PVST+ added (not used by default)
  - If controller connectivity is impacted after an upgrade, it may be STP related.
  - Test thoroughly any STP interop between controller and your switches.
    - Example: our RSTP does not always play nice with MSTP which is the default on many switches.
- **Controller DHCP scalability**
  - Internal DHCP server is <u>**not**</u> recommended to be used for more than 2 x /24 scopes

#2 – Common misconfiguration

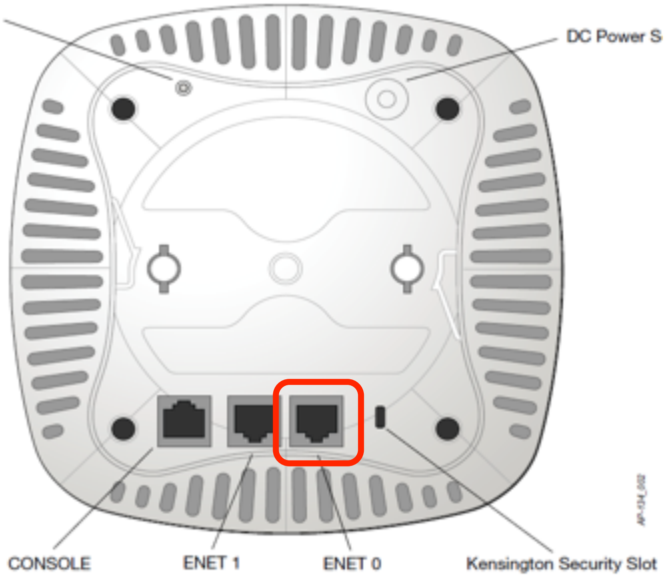
- **Too fast periodic DB sync**
  - Master to redundant master periodic DB sync requires the controller to dump various databases and transfer them across.
  - While the databases are being dumped, client processing is not occurring.
  - In most cases, periodic DB sync should not be required more than once per 24 hours.
- **Misconfigured multi-association on Virtual AP**
  - Also known as "fast-roaming"
  - Multi-association should not be configured. Having it enabled can cause the APs to hit max-client count very quickly.
  - Planned to be removed in rel 6.2

#2 – Common misconfiguration

- **Captive portal web max clients too low**
  - If you are using the controller captive portal for many users, you must adjust the default setting for "Maximum supported concurrent clients" to be higher, i.e.
    - "***web-server web-max-clients 300***"
  - Default value is 25 to protect HTTPd from abuse

#2 – Common misconfiguration

- **Insufficient power for 2nd enet port on AP 13x**
  - Not a controller misconfiguration per-se
  - AP13x hardware must have 802.3at power to run both ethernet ports
  - If only presented with 802.3af power, can still run 3x3 but only with enet0
    - After bootup, s/w will disable enet1
  - Ensure to always connect enet0 if just using a single cable to avoid any issues with AP power management



#1 - Best practice tweaks

- **Layer 2 broadcast filtering**
  - Virtual AP broadcast filter “arp”
  - Virtual AP broadcast filter “all”
  - Use these on tunnel mode VAPs to reduce the amount of broadcast and multicast traffic that may leak from the layer2 network onto the air
    - i.e. filters out CDP, STP BDPUs etc. from leaking to WLAN
    - Make sure that the VAP **is not required to support multicast traffic**, often voice networks will use multicast for call hold music etc

#1 - Best practice tweaks

- **RF optimizations**
  - band-steering
    - Multiple modes available – “force”, “prefer”, “balance”
  - s/w retry (new in 6.1.2.6+)
    - A different retry mechanism for 11n clients
    - Shows benefit with i-devices, especially in presence of interference
    - “***wlan ht-ssid-profile <profile> sw-retry***”
  - High density 5GHz should use 20MHz channels not 40MHz
    - Also watch out for this with outdoor mesh – most countries only have 2 non overlapped 40MHz outdoor channels

#1 - Best practice tweaks

- **Rate optimizations**
  - SSID profile “mcast-rate-opt”
    - Send broadcast and multicast frames at the rate of the worst client, up to 24Mbps. Improves WLAN air time utilization
  - SSID profile “eapol-rate-opt” (new in 6.1.2.7+)
    - Use lowest tx rates for EAPOL frames to improve roaming reliability for dot1x enabled devices
- **Auth optimizations**
  - Decrease default EAPOL ID request period from 30 to 3 seconds, for faster state recovery
    - ***aaa authentication dot1x <profile> timer idrequest_period 3***
  - Enable “validate-pmkid” in dot1x profile to prevent any state mismatches with half baked OKC clients

#1 - Best practice tweaks

- **Load balancing optimizations**
  - Always use a wlan traffic mgmt profile when doing high density testing
    - “fair-access” is the best practice configuration for all client types
    - “preferred-access” if non-11n clients do not have an application performance requirement
  - SSID local probe response threshold
    - “wlan ssid-profile <profile> local-probe-req-thresh X” is a useful way to stop APs from responding to probes from distant clients.
    - Use “show ap debug client-table ap-name <ap>” to determine signal from nearby clients
    - Typical values of X might be in the range 20~30,

In conclusion

- support@arubanetworks.com
  - One email address for all products
- **Timezone/shift-work nature of support front line**
  - You can always request your ticket to be moved to another time-zone
  - Avoid unicasting emails/attachments to support staff
    - Using reply to all will get more eyes on your issue
- **Always call support for urgent issues**
- **Please exercise caution when making changes**
  - Always keep off-box backups
  - When tweaking, incrementally add changes
    - ArubaOS has a number of ways to contain changes

Takeaways

TAC Quick Reference Guide

- https://support.arubanetworks.com/DOCUMENTATION/tabid/77/DMXModule/512/Command/Core_Download/Default.aspx?EntryId=1371

Validated Reference Designs (VRD)

- http://www.arubanetworks.com/technology/reference-design-guides/

Airheads Social

- http://community.arubanetworks.com/

Aruba Knowledge Base

- https://kb.arubanetworks.com/

Raise a ticket for any product, RMA, anything !

- support@arubanetworks.com

Requests for Enhancements (RFE)

- Please discuss with your SE/Sales team

Outdoor planner tool

- https://outdoorplanner.arubanetworks.com/

Questions?

AIRHEADS
LAS VEGAS 2012

Coming Up:
Tech Playground 12pm – 1:30pm