TOP 10 TIPS FROM ARUBA TAC
Foreword
Before you open a ticket...

• Check online resources such as
  – Airheads forum
  – Aruba Knowledge Base
  – 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
  – 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 optimisations that might be clouding the issue, or, put up a default virtual AP for testing (if possible)
    - Sometimes config is over optimised/tweaked
The Countdown
The Top 10 Countdown

- Airwave
- Amigopod
- RMA Alphabet Soup (RMA, LLW, RTF, NBD)
- Upgrading to Release 6.1.x
- Upgrading RAPs to Release 6.1.x
- Controller under stress
- Mesh
- Client connectivity and performance issues
- Common misconfiguration
- Best practice optimisations/tweaks
#10 – Airwave

- Software now on Aruba site in Downloads area
- Support via support@arubanetworks.com
  - support@airwave.com deprecated
- Evaluation licenses now self administered via licensing.arubanetworks.com
  - 3 x 30 day eval licenses
  - log a support ticket if any issues
- Airwave TAC escalation time-zone
  - slightly outside of APAC time-zones (especially NZ + East coast AUS in GMT+10 or higher)
#10 – Airwave

- **Airwave software release is rapid - need to stay current**
  - shell based upgrade if Airwave connected to internet
  - local file upgrade if not.

- **Supportability**
  - There is a double license count issue for the virtual controller AP when using Aruba Instant APs
    - contact support to get “extra" licenses, to be fixed in Airwave 7.5
  - Airwave syslog should be used for small to medium size networks only
  - Airwave support often ask for remote access to troubleshoot, be ready for that
  - Ensure that Airwave AMON feature is not enabled on ArubaOS lower than 6.x (`conf t no mgmt-server type amp`)
#9 – Amigopod

- **Support is handled via the Airwave team**
  - Previous comments about time-zone, support etc. apply.
- **MDPS require solid understanding of certificates**
- **Webpage customisation requires solid understanding of HTML, javascript, CSS etc.**
  - Most successful customisations are done by web programmers (not WiFi engineers and SEs)
  - Having a support contract doesn’t replace having a suitable programmer for heavy customisations!
- **Amigopod also releases software frequently**
  - always make a backup before just accepting new plugins on a production system
#9 – Amigopod

- **Supportability**
  - must be connected to the internet to download plugins
  - changes to license limits are not updated until the Amigopod can contact the license server on internet
  - never install multiple user lic’s (i.e. AMG-100 + AMG-1500)
  - Always use latest version when testing latest features (MDPS, EAP-termination etc.)
  - Watch out for 3.3 -> 3.5+ upgrade procedure
  - Always read the release notes for upgrade procedures
#9 – Amigopod

**Supportability**

- In a multivendor design, support may not have access to the hardware that you are using. We need your help to solve these kinds of issues.
- Be aware of how captive portal auth works
  - Refer to Amigopod Deployment Guide on Aruba support site
  - Wireshark capture at the client device is the best place to get a good idea of what is happening when there are issues
- Some interop issue between iOS5 / Android 2.3 that causes some captive portal pages to slowly load
  - Disable RFC 1323 timestamps on Amigopod
  - **Administrator->System Control->System Config** and paste in “net.ipv4.tcp_timestamps = 0”
#9 – Amigopod

- **Apple Captive Network assistant on i-devices.**
  - Scrolls up sometimes after connection or when open Safari, which hides the captive portal and advertising if present.
  - Cancelling this screen causes strange connectivity issues
    - Multiple ways to workaround
      - Named (or ip) acl in initial role to bypass captiveportal ACL to allow [www.apple.com](http://www.apple.com)
      - Captive portal whitelist entry for apple.com
    - Refer to Amigopod technote
#8 – RMA Alphabet soup

- Acronyms everywhere...
  - RMA – return materials authorisation
  - LLW – limited lifetime warranty (qualifying h/w only, never for s/w)
  - NBD – next business day
  - RTF – return to factory
  - Bestway – within 3-5 business days

- RMA policies are all on the [www.arubanetworks.com](http://www.arubanetworks.com) website

- Lifetime Warranty (LLW) is covered by RTF (Return to Factory)
  - Customer must return the defective part first
  - It usually takes up to 10 business days after the part is received before replacement is sent back to RMA requestor

- TAC can only RMA “apples to apples”
  - Anything else should be escalated to Aruba Order Entry (orderentry@arubanetworks.com) including miss order, shipping issues or credit returns.
Top causes for RMA delay

- Incorrect or lack of info in the RMA request
  - No matter the support coverage, you can always contact support to help diagnose an RMA
  - Try to pre-empt the questions to avoid delays (e.g. AP RMAs always ask the same info)
- Lack of console output
  - Not always possible, but pinpoints many issues quickly
- Missing or incorrect serial numbers
- Assumptions about phone numbers or addresses
  - The person processing the RMA may not know country specific abbreviations for states.
- Support contract dispute
  - Aruba is not innocent on this either 😞
  - If you believe you have a valid Arubacare contract and it’s not acknowledged, escalate to your local Aruba staff
- Submitting RMA after NBD cutoff time
  - 1pm Singapore time is the deadline for APAC.
#7 - 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
#7 - 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 utilised 3200 controller may need to be rebooted to ensure there is enough free memory for the upgrade
  - Same applies to 6x0 controllers, but there is no XM kit for those.
#6 - 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.
#6 - 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 d/l 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.
#6 – 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
#6 - 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**

- Easiest way to upgrade is with 2\textsuperscript{nd} controller running 5.0.4.x
  - your network is already on 6.1.x 🙁
  - the 50 RAPs just received from distributor are all 5.0.0.2 based provisioning image 😞
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
#6 - 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) #
#5 – 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)
#5 – 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
#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 behaviour**
  - 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 below data and contact support for assistance**
#4 – Controller under stress

- **Multiple places to check**
  - show datapath utilization
  - show datapath bwm
  - show datapath bridge counters
  - show cpuload current
  - show processes sort-by cpu
  - show memory
#3 - Client Connectivity/Perf Issues

- **A common support topic!**

- **Frequent causes**
  - RF issues
  - Client driver issues (versions, power save, roaming quirks)
  - Client certificate/captive portal issues (OCSP, latest Lion)
  - Config on controller (ARM, A-MSDU, rates etc)
  - Important L3 hosts stuck in user table
  - Controller datapath under stress (covered in #4)
#3 - Client Connectivity/Perf Issues

- **RF Issues**
  - Make use of spectrum analyser 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 behaviours
    - 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
    - SOE/locked down devices may not be able to do this
    - 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 wifi cards are regionalised 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

- **Client certificate issues**
  - Recent Mac OS Lion issue in 10.7.2 [https://discussions.apple.com/thread/3428078](https://discussions.apple.com/thread/3428078)
  - If using HTTPS on captive portal – watch out for OCSP
    - Most public CA certs use OCSP now
    - Symptom is often captive portal page loads on IE, some Mac’s but not Firefox, or takes “minutes” to load. The certificate revocation check from the browser is getting caught by the captive portal
  - **Workarounds**
    - Disable OCSP on client browser
    - Use HTTP
    - Add whitelist (AOS 6.x) in CP profile or named ACL in CP role if 5.x

```bash
conf t
netdestination ocsp.comodoca.com
  name ocsp.comodoca.com
!
aaa authentication captive-portal profile <cp-profile-name>
  white-list ocsp.comodoca.com
!```

[Certificate Viewer]
#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-response-threshold`
    • Need to find a balance
#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"
• **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
```
• **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)
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>MAC Address</th>
<th>SSID</th>
<th>Result</th>
<th>VLAN</th>
<th>username</th>
<th>server</th>
<th>EAP ID</th>
<th>length</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov 3 11:08:02</td>
<td>station-up</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>wpa2 aes</td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>station-data-ready</td>
<td>00:21:6a:8b:0a:dc 00:00:00:00:00:00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>authenticated</td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>m-auth resp</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>authenticated</td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>wpa2-key1</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>117</td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>eap-start</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>eap-id-req</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>eap-id-resp</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>44</td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>m-auth</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td>authenticated</td>
<td></td>
<td>host/pc1.lab.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>wpa2-key2</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>119</td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>wpa2-key3</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>151</td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>wpa2-key4</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>95</td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>eap-start</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>eap-id-req</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>eap-id-resp</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>44</td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>m-auth</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td>authenticated</td>
<td></td>
<td>host/pc1.lab.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>wpa2-key2</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>119</td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>wpa2-key3</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>151</td>
</tr>
<tr>
<td>Nov 3 11:08:02</td>
<td>wpa2-key4</td>
<td>00:21:6a:8b:0a:dc 00:1a:1e:66:f7:30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>95</td>
</tr>
</tbody>
</table>
Recently seen authentication issues

- Cannot connect dot1x wireless on XP via RDP
  - 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](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 **not** 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 misconfig 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 mcast traffic, often voice networks will use mcast for callhold music etc

- VLAN interface equivalent of the above for wired ports, again beware existing traffic that uses this to work (bpdus, mcast etc.)
  - `interface vlan X bcmc-optimisation`
#1 - Best practice tweaks

- **IPv6**
  - Disable IPv6 if not using it
  - Avoid dual stack issues when using radius accounting
  - "no ipv6 enable"

- **Voice Clients**
  - Voice is always hard to do on 2.4GHz
  - Always follow manufacturers recommendations for DTIM period in SSID profile. Same for max-retries, typical to see values more like 2-4 rather than default 8
  - Need to find a balance of high power (-65dBm or better) without hitting co-channel interference issues
  - Local-probe-response threshold to stop clients jumping to distant APs
#1 - Best practice tweaks

- **RF optimisations**
  - 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 optimisations
- SSID profile “mcast-rate-opt”
  - Send broadcast and multicast frames at the rate of the worst client, up to 24Mbps. Improves WLAN air time utilisation
- 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 optimisations
- 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 PKM ID” in dot1x profile to prevent any state mismatches with half baked OKC clients
#1 - Best practice tweaks

- **Load balancing optimisations**
  - Always use a wlan traffic mgmt profile when doing high density testing
    - “fair-access” when all clients are same time
    - “preferred-access” if a mix of legacy/11n clients
  - 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**

**Validated Reference Designs (VRD)**

**Airheads Forum**
- [http://community.arubanetworks.com/](http://community.arubanetworks.com/)

**Aruba Knowledge Base**
- [https://kb.arubanetworks.com/](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/](https://outdoorplanner.arubanetworks.com/)

**Demo kit support (Partners)**
- dl-demokit-support@arubanetworks.com

#airheadsconf
#11 – RAP connectivity

- **Common connectivity challenges**
  - Requires 4500/UDP NAT-T
    - Interop issues with some NAT-T aware VPN firewalls
  - Loss or intermittent issues on RAP to controller link will cause rebootstraps and config push delays
    - May require port mirror to really know where the loss is occurring
  - 3G can be challenging
    - Biggest challenges are getting the modem to mode-switch and in some cases determining the correct deviceID
    - Linux user community is usually a good place to start via your favorite search engine, i.e. “huawei E1969 + linux + ttyUSB”
    - ArubaOS supports usb-modeswitch in all recent versions which means most modems will work (eventually)
#11 – RAP connectivity

- **Quick way to find 3G actual device ID (windows)**
  - Insert modem, install s/w, **connect** it to internet and open up Device Manager

![Device Manager window showing Hardware IDs and ID = 0x12d11003](image)