TAC: Top 10 Tech Tips
Objectives: Help our customers understand some of the recent issues around the Region
Aruba’s **Customer First** Commitment

**24 x 7 Commitment**
- 24x7x365 live telephone support
- IP Networking and WLAN expertise
- Onsite critical care

**Global Delivery**
- 13 Technical Assistance Centers on 4 continents.
- Global partner network
- Same-day & Next-day RMA parts delivery on a global basis.
Before you open a ticket...

Check online resources such as

- Aruba Networks Product User and Reference Guides
- Aruba Networks Knowledge Base (support.arubanetworks.com)
- Aruba Networks validated reference designs (VRDs)
- Software Release Notes
- Airheads Social (community.arubanetworks.com)
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 omitted
clear definition of start of the problem, correlation to other IT changes
Less is “less”

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

Top 10 Problem Areas
Top 10 Problem Areas

#1    AP Problem Determination
#2    Client Authentication
#3    Client Connectivity
#4    Client Performance
#5    Captive Portal – External
#6    Captive Portal – OCSP
#7    Upgrading ArubaOS
#8    ArubaOS Configuration
#9    Broadcast/Multicast Mitigation
#10   Spectrum
#11   Your Input ????
#1 AP Problem Determination
#1 – AP Problem Determination

• Isolate to a single defective AP

  • Multiple APs affected
  • View the AP as a small PC – does it function properly alone?
  • Connection to controller?
  • Controller logs?
  • AP console?
#1 – AP Problem Determination

- An AP in essence is a small computer

- **Hardware Blocks**
  - Power – External/PoE ?
  - CPU/Memory ?
  - I/O – Ethernet, WLAN, console port ?

- **Symptoms**
  - Constant ?
  - Intermittent ? How Frequently ? Duration of the symptoms ?
  - Triggerable ?
#1 – AP Problem Determination

### Access Point > System Status

**IP Address:** 192.168.50.151

**Reboot Information**

AP rebooted Fri Dec 31 16:03:27 PST 1999; SADP: Reboot after successful image upgrade

**Rebootstrap Information**

Date/Time Reason (Latest 10)
- 1999-12-31 16:01:12 Changing to LMS #0 (192.168.17.249)

**Rebootstrap LMS**

1999-12-31 16:01:12 Changing to LMS #0 (192.168.17.249)

**Crash Information**

(none found)

**Heartbeat Stats**

<table>
<thead>
<tr>
<th>Heartbeats Sent</th>
<th>Heartbeats Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>4856</td>
<td>4847</td>
</tr>
</tbody>
</table>

**Descriptor Usage**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Queue</th>
<th>Alloc</th>
<th>Free</th>
<th>In-use</th>
<th>Max</th>
<th>Failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>wIf0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>wIf0</td>
<td>1</td>
<td>6435</td>
<td>6435</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>wIf0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>wIf0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>wIf0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>wIf0</td>
<td>5</td>
<td>116</td>
<td>116</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>wIf0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>wIf0</td>
<td>7(UAPSD)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>wIf0</td>
<td>8(CAB)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>wIf1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>wIf1</td>
<td>1</td>
<td>7464</td>
<td>7464</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>wIf1</td>
<td>2</td>
<td>13681</td>
<td>13681</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
#1 – AP Problem Determination

- When Filing an RMA Request, Help us help you
  - Note Full Shipping Address
  - Advanced Replacement/Return To Factory?
  - Full Symptom description – this helps us correlate potential series defects more rapidly
#2,3,4 Client Connectivity/Performance
#2 - Client Connectivity/Performance

- 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
#2 - 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
  - Observe how this output looks for successful/regular auth
  - Compare it when problems arise (can often spot certificate issues with this command)
#2 - Client Connectivity/Perf Issues
A Major Airport:
Had their old wireless replaced with Aruba APs

Problem:
some Bag Scanning devices start to fail at specific locations causing flight delays

Received Complain:
Signal instability in one Area, causing Flight Delays

Many days spent of site visits, working on spectrum analysis and RF adjustments
Actual Problem:

Client was configured with regulatory constrain to connect only when it receives specific Country Code

- Do not ignore Clients, they are Half of the connection
An Exhibition Center: Installation was done and wireless performance was tested with good results.

Complain: Clients Unable to Use Wireless During ‘big Events with thousands of clients around.

Problem: Using incorrect types of AP & Antennas resulting in large Cells, with too many clients air becomes too Busy for clients and APs to use.

Validated Reference Designs (VRD)
http://www.arubanetworks.com/technology/reference-design-guides/
Validated reference Designs is very helpful in putting best design with optimum configuration to your setup.
#4 - Client Connectivity/Perf Issues

- RF Health and Common problems
- Which Band do I have Problem With ?
- Do I have Proper Coverage ?
- Do I connect to the nearest AP ?
- Check Noise / Interference Levels
- How Busy is the Air ?

- Aruba Dashboard provides a very helpful instant view on all the above details, helps have a quick overview on the environment overall Health, and help troubleshoot specific problems
#5 Captive Portal
#5 – Captive Portal

- Many Captive Portal Issues are Network Issues
  - Ensure basic VLAN/IP/Routing configuration is correct, then add the Captive portal ACL
  - DNS related Issues/Configuration.
  - Certificate related Issues/Configuration
  - Remember the sequence necessary to arrive at the login/landing page
#5 – Captive Portal

Steps 3, 4,5
Client POST
To Controller
#5 – Captive Portal

### Clients

<table>
<thead>
<tr>
<th>Association State</th>
<th>Authentication State</th>
<th>Mobility State</th>
<th>Firewall State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client MAC Address</td>
<td>AP Name</td>
<td>VLAN</td>
<td>ESSID</td>
</tr>
<tr>
<td>00:0b:66:60:0c:ba</td>
<td>1</td>
<td>0</td>
<td>Wired</td>
</tr>
</tbody>
</table>

### Authentication State

<table>
<thead>
<tr>
<th>General</th>
<th>Idlo Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>Total Number</td>
</tr>
<tr>
<td>Username</td>
<td>ICMP Requests Sent</td>
</tr>
<tr>
<td>User Role</td>
<td>ICMP Replies Received</td>
</tr>
<tr>
<td>Age</td>
<td>0</td>
</tr>
<tr>
<td>Authenticated</td>
<td>No</td>
</tr>
<tr>
<td>Authentication Status</td>
<td>not started</td>
</tr>
</tbody>
</table>

### Mobility State

#### Host Information

None found.

#### Trail Information

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Controller IP</th>
<th>Current VLAN</th>
<th>Roaming Status</th>
<th>Start Date</th>
<th>ESSID</th>
<th>BSSID</th>
<th>Radio Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.17.30</td>
<td>53</td>
<td>192.168.17.218</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.17.210</td>
<td>42185</td>
<td>192.168.17.30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.17.30</td>
<td>53</td>
<td>192.168.17.218</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.17.30</td>
<td>53</td>
<td>192.168.17.218</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.17.218</td>
<td>44245</td>
<td>192.168.17.30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.17.30</td>
<td>53</td>
<td>192.168.17.218</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### User Firewall State

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.17.30</td>
<td>53</td>
<td>192.168.17.218</td>
<td>54220</td>
<td>UDP</td>
<td>Allow</td>
</tr>
<tr>
<td>192.168.17.210</td>
<td>42185</td>
<td>192.168.17.30</td>
<td>53</td>
<td>UDP</td>
<td>Allow</td>
</tr>
<tr>
<td>192.168.17.30</td>
<td>53</td>
<td>192.168.17.218</td>
<td>37483</td>
<td>UDP</td>
<td>Allow</td>
</tr>
<tr>
<td>192.168.17.30</td>
<td>53</td>
<td>192.168.17.218</td>
<td>37066</td>
<td>UDP</td>
<td>Allow</td>
</tr>
<tr>
<td>192.168.17.218</td>
<td>44245</td>
<td>192.168.17.30</td>
<td>53</td>
<td>UDP</td>
<td>Allow</td>
</tr>
<tr>
<td>192.168.17.30</td>
<td>53</td>
<td>192.168.17.218</td>
<td>54902</td>
<td>UDP</td>
<td>Allow</td>
</tr>
</tbody>
</table>
#5 – Captive Portal

### Controller > Firewall Hits

<table>
<thead>
<tr>
<th>Role</th>
<th>Policy</th>
<th>Src</th>
<th>Dst</th>
<th>Service</th>
<th>Action</th>
<th>Dest/Opcode</th>
<th>New Hits</th>
<th>Total Hits</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>logon</td>
<td>logon-control</td>
<td>any</td>
<td>any</td>
<td>svc-tlmp</td>
<td>permit</td>
<td></td>
<td>15</td>
<td>15</td>
<td>8620</td>
</tr>
<tr>
<td>logon</td>
<td>logon-control</td>
<td>any</td>
<td>any</td>
<td>svc-dns</td>
<td>permit</td>
<td></td>
<td>121</td>
<td>121</td>
<td>8621</td>
</tr>
<tr>
<td>logon</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>0</td>
<td>deny</td>
<td></td>
<td>34</td>
<td>34</td>
<td>8636</td>
</tr>
<tr>
<td>sys-ap-role</td>
<td>sys-control</td>
<td>any</td>
<td>any</td>
<td>sys-svc-sec-papi</td>
<td>permit</td>
<td></td>
<td>20</td>
<td>20</td>
<td>8653</td>
</tr>
<tr>
<td>sys-ap-role</td>
<td>sys-ap-acl</td>
<td>any</td>
<td>any</td>
<td>sys-svc-gre</td>
<td>permit</td>
<td></td>
<td>1</td>
<td>1</td>
<td>8579</td>
</tr>
<tr>
<td>sys-ap-role</td>
<td>sys-ap-acl</td>
<td>any</td>
<td>any</td>
<td>sys-ap-syslog</td>
<td>permit</td>
<td></td>
<td>7</td>
<td>7</td>
<td>8580</td>
</tr>
<tr>
<td>sys-ap-role</td>
<td>sys-ap-acl</td>
<td>user</td>
<td>controller</td>
<td>sys-svc-ftp</td>
<td>permit</td>
<td></td>
<td>1</td>
<td>1</td>
<td>8587</td>
</tr>
<tr>
<td>sys-ap-role</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>0</td>
<td>deny</td>
<td></td>
<td>1</td>
<td>1</td>
<td>8589</td>
</tr>
</tbody>
</table>

### Port Based Session ACL Hits

<table>
<thead>
<tr>
<th>Policy</th>
<th>Src</th>
<th>Dst</th>
<th>Service</th>
<th>Action</th>
<th>Dest/Opcode</th>
<th>New Hits</th>
<th>Total Hits</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>validuser</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>permit</td>
<td></td>
<td>1</td>
<td>1</td>
<td>7983</td>
</tr>
</tbody>
</table>

### Port ACL Hits

<table>
<thead>
<tr>
<th>ACL</th>
<th>ACE</th>
<th>New Hits</th>
<th>Total Hits</th>
<th>Index</th>
</tr>
</thead>
</table>
#6 Captive Portal - OCSP
Captive portal server sends it’s certificate to the client. Client attempts to validate if this certificate belongs to the ‘URI’ that sent.

- Client attempts to validate sender ‘URI’ against the CN field in the certificate.

- Depending on browser/configuration – the client may also use OCSP to validate the certificate against the sending IP.

http://www.ietf.org/rfc/rfc2560.txt
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](http://ocsp.usertrust.com):

- Netdestination ocsp.usertrust.com
  - Name ocsp.usertrust.com
- aaa authentication captive-portal default
  - white-list ocsp.usertrust.com
#6 Captive Portal - OCSP

## Captive Portal Authentication Profile

<table>
<thead>
<tr>
<th>Default Role</th>
<th>local_ACME_role</th>
<th>Default Guest Role</th>
<th>guest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect Pause</td>
<td>3 sec</td>
<td>User Login</td>
<td></td>
</tr>
<tr>
<td>Guest Login</td>
<td>Logout popup window</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use HTTP for authentication</td>
<td>Logon wait minimum wait</td>
<td>5 sec</td>
<td></td>
</tr>
<tr>
<td>Logon wait maximum wait</td>
<td>10 sec</td>
<td>Logon wait CPU utilization threshold</td>
<td>60 %</td>
</tr>
<tr>
<td>Max Authentication failures</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use CHAP (non-standard)</td>
<td>Show FQDN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Welcome page</td>
<td>/auth/welcome.html</td>
<td>Login page</td>
<td>/auth/index.html</td>
</tr>
<tr>
<td>Add switch IP address in the redirection URL</td>
<td>Show Welcome Page</td>
<td>Allow only one active user session</td>
<td></td>
</tr>
</tbody>
</table>

**White List**

| ocsu.usertrust.com | Delete |

**Black List**

| Delete | Add |

**Show the acceptable use policy page**

---

CONFIDENTIAL © Copyright 2012. Aruba Networks, Inc. All rights reserved

#airheadsconf
#6 Captive Portal - OCSP

- Check client routing table, ARP cache, DHCP status
- Packet capture, firebug or other method to see the entire URL at the client is helpful.
- Using the default certificate is not recommended for production deployment
- If using self-signed certificates, ensure the certificate hostname/IP addresses match.
- If necessary, ensure the internal PKI is reachable to answer OCSP requests.

#7 Upgrading to ArubaOS 6.1
#7 - 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.
Provisioning image versus running image

– RAP5 or RAP2 has 2 s/w images on it
– the provisioning image that runs the rapconsole
– 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.
#7 - 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
#8 ArubaOS Configuration
#8 – ArubaOS Configuration

- **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
#8 – ArubaOS Configuration

- **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
• **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,
#9 Broadcast/Multicast Mitigation
#9 – Broadcast/Multicast Mitigation

Why?
#9 – Broadcast/Multicast Mitigation

Duty Cycle / Channel Busy 100%
#9 – Broadcast/Multicast Mitigation

**Global Knob**

**Drop-broadcast arp** (Global firewall knob)

This knob will enable ARP conversion on all VLANs. If this knob is enabled, all the broadcast ARPs destined to wireless clients that are part of the station or user table are converted to unicast ARP requests.

**Virtual AP Profile Knobs**

**Drop-broadcast all**: This knob will drop all broadcasts and multicasts except DHCP on that VAP. In addition, broadcast DHCP frames destined to clients i.e. broadcast DHCP offers/ACKs to unicast DHCP frames over the air. In ArubaOS 6.1.3.2 and later, the function that converts broadcast DHCP offers/ACKs to unicast DHCP frames over the air will be part of the “Drop-broadcast arp” knob.

**Drop-broadcast arp**: This knob will enable ARP conversion on a per VAP basis. If enabled on a VAP, broadcast ARP requests are converted to unicast ARP requests if the target IP/Mac address are part of user table and station table.
#9 – Broadcast/Multicast Mitigation

**Wired AP Knob**

**Broadcast**: This knob will flood broadcast traffic to the tunnel on which it is enabled. This knob works only for wired ports in tunnel mode. (More clarification requested w.r.t any difference in behavior in trusted tunnel vs. untrusted tunnel)

**VLAN Knobs**

**BC-MC Optimization**: This will drop all the broadcast and multicast frames on a VLAN (both wired and wireless interfaces) except for ARP, DHCP and VRRP traffic.

**Local-proxy-ARP**: If this is enabled on a VLAN, the controllers will proxy-ARP with target’s MAC address when we receive an ARP request on an L2 VLAN. However, if the target IP is a known user on an L3 VLAN, the controller will respond with its MAC address instead. (A known user is considered as someone that the controller is aware of either through route cache or user table)

**Suppress-ARP**: This knob will drop gratuitous ARPs on wireless tunnels and all unknown ARP flooding on untrusted interfaces
#9 – Broadcast/Multicast Mitigation

<table>
<thead>
<tr>
<th><strong>Virtual AP &gt; campus_cp</strong></th>
<th><strong>Virtual AP enable</strong></th>
<th><strong>Allowed band</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>all</strong></td>
</tr>
</tbody>
</table>

| **VLAN**                  | 2                     | **--**          |

| **Deny time range**       | **--NONE--**          | **Mobile IP**   |

<table>
<thead>
<tr>
<th><strong>HA Discovery on-association</strong></th>
<th><strong>DoS Prevention</strong></th>
</tr>
</thead>
</table>

| **Station Blacklisting**      | **Blacklist Time**  | **3600**        |

| **Dynamic Multicast Optimization (DMO)** | **Dynamic Multicast Optimization (DMO) Threshold** | **6** |

<table>
<thead>
<tr>
<th><strong>Authentication Failure Blacklist Time</strong></th>
<th><strong>Multi Association</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Strict Compliance</strong></th>
<th><strong>VLAN Mobility</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Preserve Client VLAN</strong></th>
<th><strong>Remote-AP Operation</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Drop Broadcast and Multicast</strong></th>
<th><strong>Convert Broadcast ARP requests to unicast</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Band Steering</strong></th>
<th><strong>Steering Mode</strong></th>
</tr>
</thead>
</table>
#9 – Broadcast/Multicast Mitigation

**Configuration > AP Group > Edit "campus"**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Transmit Attempts</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>2333</td>
<td>bytes</td>
</tr>
<tr>
<td>Short Preamble</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Multimedia</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WMM TSPEC Min Inactivity Interval</td>
<td>0</td>
<td>msc</td>
</tr>
<tr>
<td>Override DSCP mappings for WMM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSCP mapping for WMM voice AC</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>DSCP mapping for WMM best-effort AC</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>Hide SSID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Probe Request Threshold</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Battery Boost</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WEP Key 1</td>
<td></td>
<td>Retype:</td>
</tr>
<tr>
<td>WEP Key 2</td>
<td></td>
<td>Retype:</td>
</tr>
<tr>
<td>WEP Key 3</td>
<td></td>
<td>Retype:</td>
</tr>
<tr>
<td>WEP Key 4</td>
<td></td>
<td>Retype:</td>
</tr>
<tr>
<td>WPA Hexkey</td>
<td></td>
<td>WPA Transmit Key Index: 1</td>
</tr>
<tr>
<td>Maximum Transmit Failures</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>BC/MC Rate Optimization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strict Spectralink Voice Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BSSID 802.11g Beacon Rate</td>
<td></td>
<td>default</td>
</tr>
<tr>
<td>802.11a Beacon Rate</td>
<td></td>
<td>advertise QBSL Load IE</td>
</tr>
</tbody>
</table>
#9 – Broadcast/Multicast Mitigation

Network > IP > IP Interface > Edit VLAN (18)

<table>
<thead>
<tr>
<th>DHCP Helper Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.17.30</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**IGMP**

- Enable IGMP
- Snooping
- Proxy

**NAT**

- Enable source NAT for this VLAN

**Inter-VLAN Routing**

- Enable Inter-VLAN Routing

**MLD**

- Enable MLD
- Snooping

**BCMC (Broadcast-Multicast) Optimization**

- Enable BCMC Optimization

**OSPF**

- Enable OSPF
- Area Network (e.g., 192.168.1.1)
- Authentication
  - Message-digest
- Message-digest Key
  - Key [1-255]
- Cost [1-65535]
- Dead Interval [1-65535]
- Hello Interval [1-65535]
- Priority [0-255]
- Retransmit Interval [1-65535]
#10 Spectrum
#10 – Spectrum

Spectrum interferers quick example
#11 Your Input ???
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 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)
–Coming very soon Partners/customers will be able to open and monitor their own RFE’s

Outdoor planner tool
–https://outdoorplanner.arubanetworks.com/
THANK YOU
JOIN US AT CASINO ROYALE
BUSES LEAVE AT 19.00 HR
MAIN RECEPTION
LICENCE TO WIN

JOIN: community.arubanetworks.com
FOLLOW: @arubanetworks
DISCUSS: #airheadsconf