Roaming Behavior and Client Troubleshooting

Presented by
Herman Robers
Systems Engineer Aruba Networks
hrobers@arubanetworks.com
About me

• Herman Robers
• Systems Engineer for Netherlands
• Almost 4 years at Aruba Networks
• Security background (and ClearPass experience)
• Past: worked 13 years as security engineer / consultant
• Ham radio license (PA3FYW)
• herman@robers.org hrobers@arubanetworks.com
Agenda

This session will be focused on what you need to do your jobs on a daily basis as a wireless network designer, engineer and/or administrator

- **Design for roaming:**
  - Channel planning for roaming
  - Access Point Planning and Placement
  - Adaptive Radio Management (ARM)

- **Client Roaming**

- **Client Troubleshooting**
Shameless plug: Airheads community

http://community.arubanetworks.com/t5/Validated-Reference-Design/tkb-p/Aruba-VRDs
802.11 Wireless Communications Refresher
Wireless Networks allow one device to communicate at a time per channel

Each Wi-Fi channel is in effect a hub that is in the air

- In the analogy below, only the person with the ball can talk.
- All the others within earshot can hear him speak, including potentially others outside of the meeting area depending on how loud the person is speaking.
- The volume that the speaker speaks with is equivalent to the wireless transmit power.
- Access points can transmit at a much higher power than clients can.
- A significant imbalance between the power that the access point communicates at and a client transmits at is the equivalent to having a conversation where one person shouts while the other person whispers.
The same channel being re-used in close proximity negates the benefit of the additional access point (same contention domain/co-channel interference)

- In the analogy below, the two tables/meetings are clients associated to two different access points on the same channel and can hear each other
- This causes things to be repeated, or in the wireless world re-transmitted
- Another bad thing is that meeting 2 can’t hear what exactly is being said in meeting 1 so it can’t pick a good time to interrupt
- The louder the speaker’s voice (transmit power) the worse this problem can be
- In other words, too many wireless access points can be as bad as too few access points

![Diagram of two meetings on the same channel](image-url)
The solution is to use another channel so that the communications don’t overlap each other

- In the analogy below, the two tables/meetings are clients associated to two different access points but now are on different channels
- Now each can communicate within each meeting without having to worry about hearing things from the other meeting and being interrupted with noise
- Once again, only one speaker can speak at a time in each meeting but you only have to worry about competing with others in your respective meeting for “talk time”, or in the wireless world, “Airtime”
• **Wireless is 3 Dimensional – goes through floors**
  – Common sense but easy to forget
  – The louder the meetings are (transmit power), the worse this gets

---

**Channel 1**

**Blah, Blah, Blah, Blah**

**Channel 11**

**Blah, Blah, Blah, Blah**

**Meeting 1**

Interference

**Meeting 3**

Interference

**Meeting 2**

**Blah, Blah, Blah, Blah**

**Meeting 4**

Will you keep it down???
• **There are a finite amount of available channels to communicate on (US regulatory Domain)**
  - **2.4 GHz – “B/G Band” – 3 Channels**
    - Only 3 non-overlapping channels (1,6,11) that can be used
    - Discussion if 4 channel plan (1,5,9,13) in EU/ETSI is useful in high-density seems a religious one
    - Older technology
    - Limited number of channels means more channel overlap and potential same channel interference when in close proximity. This is known as Co-Channel Interference and is another reason that too much access point power is a bad idea
    - Travels further than 5 GHz – A because of longer frequency
    - Adjacent channel Interference
Basic 802.11 Wireless Communications
Fundamentals

- There are a finite number of available channels to communicate on (US regulatory Domain)
- 5 GHz Channel Bonding
  Bonding channels means higher throughput but less available channels and thus more co-channel Interference because of channel overlap
  - 20 MHz Channels
    - 9 - Non-DFS FCC / 4 Non-DFS ETSI
    - 13 - DFS FCC / 15 DFS ETSI
  - 40 MHz Channels (80.11n)
    - 4 - Non-DFS / 2 Non-DFS
    - 6 – DFS / 7 DFS in ETSI
  - 80 MHz Channels (802.11ac)
    - 4 - Non-DFS / 2 Non-DFS
    - 6 – DFS / 7 DFS in ETSI
  - 160 MHz Channels (802.11ac)
    - 1 - Non-DFS
    - 1 – DFS

Remember that the 80/160MHz Channel usage is dynamic as opposed to 40MHz channels which are static

(Chart showing channel usage and interference)

NOT IN EU (ETSI)
Basic 802.11 Wireless Communications
Fundamentals

- **There are a finite amount of available channels to communicate on (US regulatory Domain)**
  - **5 GHz Channels – Things you should know**
    - Higher frequency so it only travels about 60% of the distance that 2.4 GHz does equating to approximately a 6dB power difference
    - Channel 144 was added as part of the 802.11ac amendment and is not supported by some clients and should not be used yet
    - US FCC: Channels 120-128 were used by weather radar. We have these channels back from the FCC but they are not currently supported yet.
    - Not all devices will send probe request on DFS channels and rely on beacons to build their roaming tables
In HD: VHT20 Beats VHT40 & VHT80 – 2SS Clients
In HD: VHT20 Beats VHT40 & VHT80 – 2SS Clients
In HD: VHT20 Beats VHT40 & VHT80 – 2SS Clients

![Graph showing performance of VHT20, VHT40, and VHT80 in high-density scenarios. The graph compares data rates at various client densities.]
• **Should I use DFS Channels?**
  
  – Are they really needed?
    – What are the expectations of throughput?
    – **Are you planning on using 80MHz channels? Do you really need to?**
    – If the environment is very dense access point wise, can you just use 20 or 40MHz channels?
    – How much attenuation do you have between your APs?
  
  
  – Is the 2.4 GHz spectrum clean enough to support 2.4 GHz fallback for clients that don’t?
  
  – Or do we have enough non-DFS 5GHz coverage for fallback?
  
  – Are you using VoIP and is seamless voice handover as clients roam important?
  
  – What is your tolerance for user complaints and troubleshooting?
  
  – Are you close to an airport, seaport, weather station?
    – Depending on the age of the radar you may get radar detections
      – AP must change channel on radar detect!
      – If no channel is available then go completely silent on 802.11a in APM mode (monitor)
      – B/G will continue to operate normally
What channel width should I be using?

- If you are **NOT** using DFS channels
  - 80 MHz
    - 2 channels (FCC) / 1 channel (ETSI)
    - In a 2 AP deployment which really means never
    - Too much CCI if there are more than 2 APs (FCC) or 1 AP (ETSI)
  - 40 MHz
    - 4 channels / 2 (ETSI)
    - Close office space or cubicles with outer offices ringing
    - No more than 4 (2 in ETSI) AP’s with line of sight between each other
  - 20 MHz
    - 9 channels (some older devices don’t see channel 165) / 4 in ETSI
    - Wide open office space with dense AP deployment
    - More than 4 AP’s that have line of sight to each other
    - Dense cubicles
    - Device density with each user having at least 2 devices (laptop, smartphone, tablet, VoIP phone)
• **What channel width should I be using?**
  
  – If you **ARE using DFS channels**
    
    • 80 MHz
      
      • 5 channels but some of your devices may not support 3 of them (4 in ETSI)
      • Less than 25-30 users per channel
      • High AP density to support SNR’s higher than 35 (support the highest 802.11ac data rates)
      • Requires close monitoring of your user community for the first month to identify potential issues
      • Be prepared to drop back to 40 MHz channels
    
    • 40 MHz
      
      • 10 channels / 9 in ETSI
      • Any deployment where 80MHz channels are problematic because of more than 4 AP’s with line of sight to each other or because of client side support issues
    
    • 20 MHz
      
      • 22 channels / 19 in ETSI
      • Large Public Venues
  
  • **In EU / ETSI you probably will need to use the DFS channels**
Basic 802.11 Wireless Communications
Power, Signal to Noise Ratio and Data Rates

• **Transmit Power**
  • Using high transmit power on access points doesn’t create significantly increased usable coverage because of the two way nature of communications
    – Laptop Clients can only typically transmit at 30 milliwatts versus access points that can transmit at up to 200 milliwatts
    – You typically want to keep the AP to user power at no more than a 2 to 1 ratio to your highest powered client
    – Most laptops transmit around 30 milliwatts so you typically don’t want your AP power higher than 60 milliwatts
    – Yes access points have better receive sensitivity but the CCI/ACI introduced by higher power negate the benefit of it
Signal to Noise Ratio

- Relative measurement of the signal to the “noise floor” of the environment
- The “noise floor” is the environmental or ambient noise in the 2.5GHz or 5GHz frequency
  - Analogies:
    - Library – you can whisper since there is no noise at all
    - Office – you have to speak in a normal voice to be heard over the background noise
    - Concert – you have to shout to be heard
  - Remember that the 2.4 GHz and 5 GHz are unlicensed so any device can use them, adding to the noise floor and/or causing interference
- This noise floor is usually between -85 and -100 dB with 5GHz almost always having a lower noise floor
- The higher the noise floor, the stronger your signal needs to be and the more APs you need
- So if you have a -65 dBm signal at your device and the noise floor is -95dBm then you have a 30 signal to noise ratio which is excellent
- A minimum SNR of 25 will support the highest data rates between a 802.11n client and AP
- A minimum SNR of 35 will support the highest data rates between a 802.11ac client and AP
- Any SNR below that and the client or access point will slowly start to down rate to a lower megabits per second data rate
  - This happens rapidly and signal to noise ratios below 20 are practically unusable
Signal to Noise Ratio

- The lower the signal to noise ratio, the more the device is susceptible to interference
- Remember the two way nature of communications
  - AP’s usually transmit at a higher power level than the client(s)
  - AP’s are better listeners than clients (what we call receive sensitivity)
    - Think of the AP as a dog and a client device as a human
    - Some devices have better antennas (ears) than others so they can hear better
  - The client may be transmitting at 30 mW and the AP at 60 mW so the signal to noise ratios will be different downstream versus upstream
    - The worse this power imbalance the worse the upstream signal to noise ratio, the lower the upstream data rate and the more susceptible the upstream is to interference
    - Therefore, the client signal to noise ratio (from client to AP) that the access point sees is almost always the limiting factor as it relates to performance
  - Signal to noise ratios below 20 are practically un-useable because of client performance expectations and this is about the point you want your devices to roam to a better AP
Remember that wireless devices are like using two way radios
- There is the signal from the AP to the device
- There is the signal from the device to the AP
- The smaller the device, typically the lower the transmit power and the weaker the signal is to the AP
  - Laptop – 30 mW
  - Old IPad – 12 mW
  - Newer IPad – 50 mW
  - Android device 10-13 mW
  - Vocera B3000 – 39 mW
  - Motorola Handhelds – 12 to 30 mW
- AP’s can transmit at very high power relative to the clients
  - Up to 200 mW(and up for outdoor)

Power Levels
- Usually an absolute measurement
- Anything higher than -65dBm is considered an excellent signal
- Anything higher than -50 to -55dBm would be consider too much signal which can issues by being too “loud” and causing issues with co-channel and adjacent channel interference
- Analogy: It’s best to have both parties speaking in a normal voice versus screaming or whispering
Transmit Power – Rule of 10’s and 3’s

- For every 10dB of gain multiply the power by 10
- For every 10dB of loss divide the power by 10
- For every 3dB of gain multiply the power by 2
- For every 3dB of loss divide the power by 2

<table>
<thead>
<tr>
<th>Power Level</th>
<th>Equivalent Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>3dBm</td>
<td>2mW</td>
</tr>
<tr>
<td>6dBm</td>
<td>4mW</td>
</tr>
<tr>
<td>9dBm</td>
<td>8mW</td>
</tr>
<tr>
<td>12dBm</td>
<td>16mW</td>
</tr>
<tr>
<td>15dBm</td>
<td>31mW</td>
</tr>
<tr>
<td>18dBm</td>
<td>63mW</td>
</tr>
<tr>
<td>21dBm</td>
<td>125mW</td>
</tr>
<tr>
<td>22dBm</td>
<td>158mW</td>
</tr>
<tr>
<td>22.5dBm</td>
<td>177mW</td>
</tr>
<tr>
<td>23dBm</td>
<td>200mW</td>
</tr>
</tbody>
</table>
• **Down-rating**
  
  - If the client or access point can’t successfully transmit to the other party they “down rate” and try using a slower mbps data rate. This can go down as low as 1, 2 or 5 Mbps which really means that the signal is all but unusable and will cause major customer satisfaction issues with the network.
  - Once again, bringing the power levels more in balance with each other will sustain higher data rates and make happier users.
Basic 802.11 Wireless Communications
Power, Signal to Noise Ratio and Data Rates

- **Down Rating Affects Faster Users on that Channel**
- Each channel is hub
  - Also, remember that each channel is in effect, a hub, and thus a very finite resource so having clients connected at lower data rates slows everyone down on that AP since they have to wait for those slow clients to get on and off the channel
  - So the further away a client is from an AP, the lower his signal to noise ratio and thus the client’s data rate
  - Walls/Floors exacerbate this issue if AP’s are not put in correct positions

![Image of traffic congestion](image-url)
Trimming Data Rates

Why Trim the Lower Rates?
- If the client can’t down rate any further, it must roam
- Has a similar effect to lowering the power in that it effectively shrinks the effective range of each AP at which clients can connect. It does not shrink the RF range, so for CCI normal rules apply.
- Get the slower users off the AP to let the faster users better utilize the channel/AP
- Once the user down rates to a value lower 11 or so the connection is almost unusable so it makes sense, especially in typical office environments
- The denser the AP deployment, the more trimming the rates helps
- There are certain older devices that must see the lower data rates in order to connect
- If the customer is using newer devices then it makes sense

What devices need to see the low data rates for connectivity?
- Older gaming systems
- Older handheld scanners but this is fine since low data rates really don’t affect these devices negatively since they mostly use terminal applications.
- Old VoIP Phones
- Certain medical devices/monitors
Trimming Data Rates

- **How much should I trim?**
  - Typically up to 11 Mbps and 12 Mbps respectively but can go as high as 18 or 24 with some experimentation, depending on the client devices.
  - Certain Android devices need to see the 11 Mbps data rate
    
    wlan ssid-profile "Test-GUEST-ssid_prof"
    
    a-basic-rates 12 18 24
    a-tx-rates 12 18 24 36 48 54
    g-basic-rates 11
    g-tx-rates 11 12 18 24 36 48 54
    g-beacon-rate 18
    a-beacon-rate 18

- **Why set the beacon rate**
  - If you don’t then the beacons are sprayed out at the lowest data rate even if trimmed, following the 802.11 specifications.
  - This means that devices can passively scan and then try and roam to an AP that they can’t connect to.
  - Set the beacon rate to one value higher than your lowest supported and basic rates.
  - Example – If the lowest supported data/basic rate is set to 12 Mbps then set the beacon rate to 18.

Don’t trim data rates in University, Medical Environments or any other connectivity critical environments without careful testing and monitoring.
Access Point Planning and Placement
AP Placement is the single most important predictor of user satisfaction

- ARM is very effective but it can't defy the laws of physics and make up for poor AP placements
- Cabling is a very large expense when deploying network devices.
- Make poor AP placement decisions and you are going to live with them for a long time.
- Too many AP's for the building/users and you are going to be locked into 20 MHz channels if you can't use the DFS channels
- Too Few AP's and you are going to create bad coverage areas
  - ARM is going to want to put the AP power too high creating near/far issues
  - Client match will help with the near/far issues but it takes time to steer clients (typically about 60 seconds once stationary)
- Badly placed AP's are almost as bad as putting too many AP's and to few AP's
  - Avoid AP's having Line of Sight to each other if you can avoid It
    - In dense deployments you can't avoid this most of the time but the fewer AP's that have LOS to each other, the better.
    - Think about the number of channels in each band and how much overlap you have in dense areas
- A few feet can make a big difference in signal quality and the way that ARM reacts
- Don't stack AP's on top of each other floor to floor
• **Stacking AP’s Floor to Floor Usually Causes Major Issues**
  
  Remember if the client sees AP power within 10-12dB of each other it will randomly select an AP to connect to and it might be the AP on the floor above or below.

Since the AP’s are stacked on top of each other there isn’t enough signal strength differentiation so that the client knows which AP to connect to. Sometimes they connect to the AP directly above them and other times they connect to the AP below them. When the client connects to the AP below them the upstream SNR is not that good and they get a lot of re-transmissions and a lower upstream data rate from the client.
• **Having a too many AP’s with line of sight to each may cause issues as well**
  - Remember if the client sees AP power within 10-12dB of each other is will randomly select an AP to connect to.

  ![Diagram showing AP planning and placement](image)

  *This client can hear 4 AP’s all within a small margin of signal strength so it just randomly selects one.
  In addition, the AP can hear 4 other AP’s on the same floor. Remember that there are only 3 available b/g channels so you will have 2 overlapping channels between these 5 AP’s, effectively hobbling the effectiveness of those channels unless you can lower the power of the AP’s to make them “speak at a lower volume”.*
• **You can’t lower power too much if you only have AP’s in hallways**
  - Lower the power too much and it will not be enough to reach users in rooms where the signal has to go through walls
  - Raise the power enough to penetrate the walls and you have out of control co-channel interference

Now the client can only hear two AP’s and both are equally okay to connect, providing a good user experience.

However, the client in the room can hear an AP but the signal is not high enough to provide a good signal to noise ratio. In addition, because of the client’s position in the room it must penetrate two walls further deteriorating the signal.
• AP’s with line of sight and stacked on top of each other leads to an extremely poor client experience (aka, the perfect storm)

Stack the AP’s floor to floor and now you’ve just compounded your issues by a factor of X with the power where it needs to be to reach the users in the rooms. The client will randomly select one of the APs to connect to because the power levels are all very similar. If they pick the wrong one, they going to get a very poor user experience. Now the retries may be so high that the client decides it needs to move to a different AP but it may again pick another one that is far away or through the floor.
• With a proper design you can lower the AP power to a point where the clients are encouraged to connect to the correct AP
  – Now the client only will see AP’s that it should connect to at strong signal levels
AP Density

- How many AP’s does it take to cover typical areas without taking user density into account?
  - The higher the down-tilt AP is mounted (Aruba AP 205, 215, 225) the larger the cone of coverage
  - If mounting a true omni (no down-tilt) don’t mount too high

  **Warehouse (terminal applications and no VoIP)**
  - 1 AP every 7500 to 10,000 sq feet / 750-1000m² with 50% overlap so an AP every 85 to 100 feet / 30-35m

  **Retail (open floors, eg. Grocery Store)**
  - 1 AP every 5000 to 7500 sq feet / 500-750m² with 50% overlap so an AP every 70-85 feet / 25-30m

  **Open Office Space (open floor/cubes with offices around periphery)**
  - 1 AP every 2500 to 3600 sq 250-350m² feet with 50% overlap so an AP 50-60 feet / 15-20m

  **Closed Office Space**
  - Needs to be walked, depends on construction materials

- Why is more AP density needed
  - User Density
  - Device Density/Devices per use
  - All Wireless Offices
**AP Density**

- What is a dense deployment?
  - The most dense deployments are an AP every 1500-1600 sq feet /150m² so the AP’s are anywhere between 35-40 feet / 12-15m apart
  - This is extreme and you must use 20 MHz channels in the A band to avoid too much CCI if you can’t use the DFS channels
  - If you are deploying 802.11ac and you want to use 40 MHz or 80MHz channels you MUST use the DFS channels in dense deployments
Adaptive Radio Management

• **An Aruba Feature That Automatically Adjusts AP Channels and Power Levels**

  The Aruba ARM technology uses a distributed channel reuse management algorithm where each AP makes decisions independently by sensing its environment and optimizing its local situation. The algorithm is designed so that this iterative process converges quickly on the optimum channel.

  - ARM uses a distributed channel reuse management algorithm where each AP makes decisions independently by sensing its environment and optimizing its local situation. The algorithm is designed so that this iterative process converges quickly on the optimum channel (client aware is enabled by default).
  - So…if the AP doesn’t see any other AP’s on channel 40 it will use channel 40 and set it’s power to the highest value allowed by the ARM profile assigned (within regulatory domain).
  - Remember that high default power can be as high as 200mW creating poor client roaming behavior and as a consequence near/far issues.
  - Using our channel 40 example, If it sees other AP’s on channel 40 that it’s selected because it deems it to be the least interfering channel, it will balance it power with the other AP on that channel BUT you may end up with one AP at a very high power and the other at a very low power. This is especially true if the neighboring AP sees another AP on channel 40 but the AP that is coming up can’t hear the 3rd AP.
  - Bottom line, ARM is a great tool but bases it decisions on what each AP sees as neighbors, its not perfect!

  ........But, you can make it operate better!

*What happens to the channels when you first start up a new system or assign a new ARM profile?*
Adaptive Radio Management

• **Getting ARM to Settle Quicker**
  – Arm will not change channels when a client is connected to an AP (*client aware*, enabled by default)
  – When initially deploying an Aruba wireless network it’s a good idea to adjust ARM so that it will settle quicker, otherwise it may take 24 to 48 hours to fully settle, depending on client density
  – Using these ARM settings will get it to settle within 2 hours
    • Aggressive Settings
      ```
      rf arm-profile "default"
      scan-interval 1
      no client-aware
      ideal-coverage-index 5
      acceptable-coverage-index 2
      backoff-time 120
      min-scan-time 2
      ```
    • Default Settings (don’t forget to revert back to defaults after 2 hours)
      ```
      rf arm-profile "default"
      scan-interval 10
      client-aware
      ideal-coverage-index 10
      acceptable-coverage-index 4
      backoff-time 240
      min-scan-time 8
      ```
Tuning ARM Profiles

- It’s important to remember that there is ONE default ARM profile that is used in both the A and B/G radio profiles.
- You need to create one for the A band one for the B/G band so that you can use different settings in each.
- Recommendations on ARM Power Level Starting Points Prior to Testing/Tuning
  - **B/G – 2.4 GHz**
    - AP’s 50-55 feet apart/open air - 12dBm to 15dBm
    - AP’s closer than 50 feet apart/open air - 9dBm/12dBm
    - AP’s closer than 43 feet apart/open air - 6dBm/9dBm
    - Chances are that most are going to be at 9dBm (fewer channels/more APs on an individual channel)
    - If most of the AP’s go to minimum power after they settle then you might want to lower the values each by 3dBm, especially in denser environments.
  - **A – 5 GHz**
    - AP’s 50-55 feet apart/open air - 18dBm to 18dBm
    - AP’s closer than 50 feet apart/open air 12dBm/15dBm
    - AP’s closer than 43 feet apart/open air 9dBm/12dBm
    - You want the 5 GHz power at least 6dB higher than 2.4 GHz to make it more attractive for clients to initially connect to.
Client Roaming
Client Roaming

- **Clients are the ultimate decision maker of the best access point to initially connect to, as well as move to, when in motion**
  - Clients make connection decisions primarily based on power
  - … and/or 802.11k channel and neighbor reports (if supported)
  - Clients don’t always make the right decision especially if the access points are not placed properly and/or access point power is too high (with the latter typically being a symptom of the former)
  - When moving, a client bases its roaming decisions on probe responses or beacons if they don’t support probe requests on DFS channels
Client Roaming – Properly Designed and Tuned Network

Signal Strength

A

Good signal!

Time / distance
Client Roaming – Properly Designed and Tuned Network

Signal Strength

Time / distance

Good signal!

Device starts to move
Client Roaming – Properly Designed and Tuned Network

Device starts to move

Signal Strength

Good signal!

Probe Threshold Reached
Device Sends out Probe Requests

Time / distance
Client Roaming – Properly Designed and Tuned Network

Good signal!

Device starts to move

Probe Threshold Reached
Device Sends out Probe Requests

All AP’s that hear >-85dBm respond (dynamic based on NF)
Client Roaming – Properly Designed and Tuned Network

Signal Strength

A

B

C

D

E

F

G

H

I

Device starts to move

Good signal!

Probe Threshold Reached
Device Sends out Probe Requests

All AP’s that hear >-85dBm respond

Roaming threshold reached and device picks an AP in the table built from the probe responses based on signal strength received and/or 802.1k information (if supported)
Client Roaming – AP Power Too High

Signal Strength

B

C

D

Time / distance

Client picks far away AP versus the proper one since the received signal strengths of the probe response were within -10dB of each other. The down stream connection (green line) is okay but the upstream from the client (red line) is garbage leading to down-rating, retransmissions, errors and slowing other users down on that channel for any AP on the same channel within earshot.
Client picks far away AP versus the proper one since the received signal strengths of the probe response were within -10dB of each other. The downstream connection (green line) is okay but the upstream from the client (red line) is garbage leading to down-rating, retransmissions, errors and slowing other users down on that channel for any AP on the same channel within earshot.

Device reaches an error threshold and starts looks for another AP to go to by probing and once again may go to a far away AP.
Client picks far away AP versus the proper one since the received signal strengths of the probe response were within -10dB of each other. The down stream connection (green line) is okay but the upstream from the client (red line) is garbage leading to down-rating, retransmissions, errors and slowing other users down on that channel for any AP on the same channel within earshot.

Device reaches an error threshold and starts looks for another AP to go to by probing and once again may go to a far away AP.
802.11k, v if enabled and if client supports (802.11v iOS 8+ and SG5 today)

11k Neighbor report
Information about other APs to help with handover candidate discovery

11k Beacon Report
Client reports how it hears (RSSI) the beacons of other APs

11k Channel Report
AP informs client of channels used by the WLAN

11v BSS Transition Management
AP instructs client to move to another AP

<table>
<thead>
<tr>
<th>AP</th>
<th>chan</th>
<th>secy</th>
<th>key</th>
<th>beacon scope</th>
<th>offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>6</td>
<td>WPA2</td>
<td>0</td>
<td>45</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>52</td>
<td>WPA2</td>
<td>0</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>161</td>
<td>WPA2</td>
<td>0</td>
<td>74</td>
<td></td>
</tr>
</tbody>
</table>

BSSID RSSI
- AP B: -65
- AP D: -72
- AP E: -65

Overlaps with neighbor report
Client Match
Client Match

• **What is it?**
  – Client Match is a tool to get users to the best AP based on the client Signal to Noise ratio versus simply relying on clients to decide which AP to connect to
  – This is measured by signal strength/SNR of the client probe requests as they are heard at the AP’s
  – Enhancements were added to also use the following frames to measure client signal strength which is a big step forward
    • Block ACK
    • Management frames
    • Probe Request
    • NULL data frame
    • Data frame with rate no higher than 36Mbps
  – The controller takes the client signals/SNR information and builds a “Virtual Beacon Report”
  – **Client match is NOT a roaming tool….it takes time to build the VBR and apply actions**
What does it do with the “Virtual Beacon Report”?!

- The controller takes this information and takes one of three actions provided that certain thresholds are met
  - Band Steer
  - Sticky
  - Load Balance

- Steer through 802.11v
- Sticky clients using too much airtime de-auth as an emergency measure
• **Client Match Events – BandSteer**

Pushing the client to 5 GHz from 2.4 GHz

- **Do not start logic flow if only 2.4 GHz probe requests seen**
- **ID Clients that are dual band capable by looking at probe req**
- **Stop if 2.4 GHz client signal is stronger than -45dBm**

- **Stop**
- **No**
  - 5 GHz client signal is >75dBm
  - **No**
  - Associated on 2.4 GHz
  - **2.4GHz signal is weaker than -45dBm AND Client SNR >18**
  - **Yes**
  - **Stop**
- **Yes**
  - **Stop**
- **Yes**
  - Total number of clients >15 on BOTH radios
  - **No**
  - MOVE CLIENT
  - Send 802.11v BSS Transition Message (if supported) 5 BTM messages and then timeout OR DeAuth and Blacklist for 10 Seconds
Client Match

- **Client Match Events – Sticky**
  
  Client is associated to an AP that is not receiving the client’s signal above an SNR threshold

```
Stop Logic  No  Y > -65 dBm  Y = Neighbor AP  No  X >= 18 SNR  X = Current AP  Yes  Stop and apply bandsteering flow

Start Sticky Algorithm

AP Monitors its Attached Clients SNR

Stop Logic  No  Y > 10 dB SNR Versus X SNR  Yes  MOVE CLIENT  Send 802.11v BSS Transition Message (if supported) OR DeAuth and Blacklist for 10 Seconds
```
Client Match

- **Client Match Events – Load Balancing**
  Steering Clients to Under-loaded Radios

  - Radio has more than 30 Clients on radio
    - No → Do Nothing
    - Yes → Actual Channel Load
      - Number of clients per channel
      - Compare
    - Target Channel Load
      - # clients/# Channels
      - Determine the under-loaded and overloaded radios by comparing the actual per channel and target per channel
      - On the overloaded radios, determine the target clients that can be moved >30 SNR on target radio and no worse than 5 dB of the existing AP
      - Yes → MOVE CLIENT
      - No → Visit next radio to see if >30SNR and no worse than 5 dB of the existing AP
      - Yes → MOVE CLIENT
      - No → Visit next radio to see if >30SNR and no worse than 5 dB of the existing AP
      - Yes → MOVE CLIENT
**Default Thresholds**

- **Client Match**
  - Client Match report interval (sec)
  - Allows Client Match to automatically clear unsteerable clients after ageout
  - Client Match Unsteerable Client Ageout (min)
  - Client Match Band Steer G Band Max Signal (-dBm)
  - Client Match Band Steer A Band Min Signal (-dBm)
  - Client Match Sticky Client Ageout (sec)
  - Client Match Static client check SNR (dB)
  - Client Match SNR threshold(dB)
  - Client Match Sticky Min Signal
  - Client Match Load Balancing threshold (%)
  - Client Match Restriction timeout (sec)
  - Client Match Load Balancing client threshold
  - Client Match Load Balancing SNR threshold (dB)
  - Client Match Load Balancing signal delta bound (dB)
  - Client Match 11v BSS Transition Management clients

---

**Enabled** ➔ **Enabled by default starting in 6.3, please DO NOT DISABLE**

<table>
<thead>
<tr>
<th>Default Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>How often the AP’s send their VBR</td>
</tr>
<tr>
<td>2 Days 0 Hours</td>
<td>Clients are deemed Unsteerable after 2 unsuccessful attempts</td>
</tr>
<tr>
<td>45</td>
<td>Signal level above which clients on B/G band will not be bandsteered</td>
</tr>
<tr>
<td>75</td>
<td>Signal level above which clients on A band will not be bandsteered</td>
</tr>
<tr>
<td>3</td>
<td>Frequency with which the AP runs the sticky algorithm</td>
</tr>
<tr>
<td>18</td>
<td>Minimum SNR under which a client will declared sticky</td>
</tr>
<tr>
<td>10</td>
<td>Delta value between current AP and new AP SNR</td>
</tr>
<tr>
<td>65</td>
<td>Minimum signal level in RSSI over which a client will be declared sticky</td>
</tr>
<tr>
<td>10</td>
<td>Blacklist timeout for sticky move</td>
</tr>
<tr>
<td>20</td>
<td>Threshold value for client distribution across channels</td>
</tr>
<tr>
<td>300</td>
<td>Bandsteer backoff interval for IOS devices for failed bandsteer</td>
</tr>
<tr>
<td>120</td>
<td>How often stale VBR entries are aged out</td>
</tr>
<tr>
<td>2</td>
<td>How many steer fails will trigger a client being classified as unsteerable</td>
</tr>
<tr>
<td>30</td>
<td>Number of clients on an AP before the load balancing algorithm kicks in</td>
</tr>
<tr>
<td>30</td>
<td>Minimum SNR value of AP that is under loaded before a load balancing event</td>
</tr>
<tr>
<td>5</td>
<td>Target AP should not have weaker signal strength than source AP by this</td>
</tr>
</tbody>
</table>

---

**Client Match 11v BSS Transition Management**

Enabled ➔ **802.11v mechanisms will be tried first before using de-auth’s to steer**
Client Match

- Client Match – Tuning
  - Client Match forces users to other AP’s typically after they are connected
    - In software versions >6.4.2.3 802.11v BSS transition messages are used if the client is 802.11v capable
    - Prior to 6.4.2.3 or if the client doesn’t support 802.11v, the mechanism used is a 802.11 de-auth message
    - De-auth’s force the user off an AP and can result is a less than desirable user experience in certain circumstances
    - Client Match is voice aware and will not issue a de-auth if a client is on a voice call
  - Based on this it desirable to have the client connect to the best AP on their own and avoid having Client Match having to guide them to a better AP if possible
  - The following default setting should be adjusted to make sure that clients are always bandsteered to the A band if possible

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Match Band Steer G Band Max Signal (dBm)</td>
<td>10</td>
<td>Signal level above which clients on B/G band will not be bandsteered. We always want the client to be bandsteered to the A band if possible so this should be set to 10 to effectively disable. Default is 45.</td>
</tr>
<tr>
<td>Client Match Restriction timeout (sec)</td>
<td>3</td>
<td>When a device is de-auth’ed, all the AP’s except for the AP that we want them to go to temporarily blacklist the client. If a client is very stubborn and won’t go were we want them to we don’t want them disconnected for more than a few seconds. Default is 10.</td>
</tr>
<tr>
<td>Client Match Sticky client check SNR (dB)</td>
<td>18-25</td>
<td>Minimum SNR under which a client will declared sticky. Default is 18. The higher the AP density the higher value this should be.</td>
</tr>
</tbody>
</table>
• **Un-Steerable Clients**
  
  Non - IOS
  
  – Controller keeps track of successive steer failures for the respective steer reason to the desired destination radio
  – Upon 2 consecutive failed steer attempts the controller notifies the associated AP to mark the client as unsteerable (with reason)
  – AP will not attempt to band steer that client for that specific reason (SLB and Sticky are still in play)
  – To view unsupported clients “show ap arm client-match unsupported”
  – Default Unsteerable client ageout 2 days

  IOS Clients
  
  – IOS clients can get into a state where they will NOT try to reconnect after multiple de-authentications sent by the controller
  – To work around this we have implemented a backoff timer for IOS devices that is defaulted to 300 seconds/5 Minutes after an unsuccessful client steer
  – You will see an “I” flag with a “T” (temporary) if the 2 threshold has not been hit yet
• To view the VBR on the controller
• Show ap virtual-beacon-report client-mac/ap-name/ip-addr/ip6-addr

```
(Mejnar-7200) #show ap virtual-beacon-report client-mac 24:77:03:f8:5e:78

Client MAC :24:77:03:f8:5e:78
Current association :Primary-220 (9c:1c:12:88:63:d1)
Steer attempts/Success :1/9
Consecutive Failures (HTM Reg/HTM Timeout) :0/0/0
Sndsteer window (Steers/Start time/Expiry time) :2/Jan 21 05:17:50/Jan 21 05:47:50
Client Device Type :Win 7
Current state :Steerable
Client Supported Channels :{36,4},{32,4},{100,11},{149,4},{165,1}
Current Time :Jan 21 11:37:24 2013

STA Beacon Report
AP IP address Radio ESSID Signal (dBm) Last update Add time Channel/EIRP/Clients Flag
Primary-220 192.168.1.1 9c:1c:12:88:63:d0 H-Peripherals -51 Jan 21 11:17:12 Jan 21 05:17:30 101/1/1
Primary-220 192.168.1.1 9c:1c:12:88:63:d0 H-Peripherals -55 Jan 21 11:17:12 Jan 21 05:17:30 101/1/1

VBR Flags "-Associated S-State U-Unsupported Channel"

- Primary-220
  - The client’s signal strength is -51dBm on B/G and -55dBm on A
  - The client’s upstream SNR is 89-51 = 38 B/G and 97-55 = 42 on A
- Secondary-220
  - The client’s signal strength is -65dBm on B/G and -70dBm on A
  - The client’s upstream SNR is 96-65 = 31 B/G and 93-70 = 23 on A
## Client Match

Looking the client match history for a client

### Show ap arm client-match history/advanced/client-mac<mac>
Client Troubleshooting
Client Troubleshooting

- Association
- Authentication
- Network Connectivity
Client Troubleshooting

- **Association**
  - Is the user associated
  - What AP is the user connected to?
    - Remember that the user is going to connect on their own to begin with before Client Match steers them anywhere
    - Does it makes sense where they are connected to?
      - Through walls, floors?
      - Farther AP via line of sight?
    - The user should connect to the closest unobstructed AP
  - Is it the correct/expected AP?
    - If not, why not?
  - Is Client Match pushing the user to the correct AP after 2-4 minutes?
    - If not, why not?
**Association**

*show ap association client-mac <mac address>*

- shows a lot of detailed information for a specific user including:
  - AP Name the user is connected to
  - BSSID the user is connected to
  - MAC address
  - ESSID
  - VLAN-ID – The vlan that the user traffic is being sent on once it hits the distribution system (aka., wired network)
  - Tunnel-id - Identification number of the AP’s tunnel.
  - Assoc. time - Amount of time the client has associated with the AP, in the format hours:minutes:seconds.
  - Band steer moves (T/S) – Tries and Success
  - Channel – Channel number
  - Channel Frame Retry Rate – A high number indicates a busy channel  ≤ is the channel super busy >50%, why?
  - Channel Frame Error Rate – What percentage of traffic is errors  ≤ High # needs to be looked at
  - Channel Bandwidth Rate(kbps) - at this point in time
  - Channel Noise – Noise Floor  ≤ Is the noise floor high? > 85 for B/G or >90 for A
  - Client Frame Retry Rate – How many frames need to be transmitting as a percentage of all frames
  - Client Tx Packets
  - Client Rx Packets
  - Client Tx Bytes
  - Client Rx Bytes
  - **Client SNR – Noise floor minus the RSSI of the client**
    - By far the most important piece of information besides the AP the client is connected to
    - 25 is bare minimum, 30 is a good target
    - Below 25 and the client or AP will down rate the connection 802.11n
    - > 33-35 is best for AC rates
Client Troubleshooting

• Association

show ap association client-mac <mac address>

– Other information that is not important in most circumstances –
  • Association and Authentication State (802.11) – Remember that there are two types of 802.11 authentication, Open System and Shared Key (aka., WEP). So, this should not be confused with network authentication like 802.1X (which uses 802.11 Open System authentication).
  • AID – Association Identifier. A client receives a unique 802.11 association ID when it associates to an AP
  • I-int – Number of beacons in the 802.11 listen interval. There are ten beacons sent per second, so a ten-beacon listen interval indicates a listen interval time of 1 second.
  • Num assoc – how many users are associated to this BSSID, including the user you are current viewing
  • Channel Frame Fragmentation Rate – 802.11 Fragmentation – only an issue is extremely high
  • Channel Frame Low Speed Rate - what percentage of traffic is sent at the lowest supported data rate
  • Channel Frame Non Unicast Rate – percentage of multicast/broadcast traffic. Note that this may be zero if using multicast optimization and broadcast filter arp/broadcast filter all.

– This command is really useful for doing roaming test and keeping an eye on the SNR for the client and when user roams (based on the AP name changing) in real time. Note that the information contained in the association table (top) of the output (AP Name, bssid, client mac, auth/assoc, assoc. time, flag, etc. is updated real time. However, the information in the lower part of the output labeled as “stats” where you have the two columns, “parameter” and “value” is updated every 60 seconds.
Client Troubleshooting

- **Association**

  `show ap association client-mac <mac address>` shows association information only
### Client Troubleshooting

- **Is the client 802.11v capable (steerable)**

  **show ap association**

<table>
<thead>
<tr>
<th>Name</th>
<th>bssid</th>
<th>mac</th>
<th>auth</th>
<th>assoc</th>
<th>a1-int</th>
<th>essid</th>
<th>vlan-id</th>
<th>tunnel-id</th>
<th>phy</th>
<th>assoc. time</th>
<th>num assoc</th>
<th>Flags</th>
<th>DataReady</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAP205H-00:04</td>
<td>04:bd:88:75:00:0f2</td>
<td>d:1f:5:bc:fd:23:d9</td>
<td>y</td>
<td>y</td>
<td>1</td>
<td>wlan_spllt</td>
<td>1234</td>
<td>0x0</td>
<td>a-vht-205g1-1ss</td>
<td>2h:37m:7s</td>
<td>1</td>
<td>W</td>
<td>Yes (Implicit)</td>
</tr>
<tr>
<td>IAP205H-00:04</td>
<td>04:bd:88:75:00:0f1</td>
<td>5e:0:0:0:0:3e:19</td>
<td>y</td>
<td>y</td>
<td>1</td>
<td>wlan_br</td>
<td>3333</td>
<td>0x0</td>
<td>a-vht-205g1-1ss</td>
<td>2m:45s</td>
<td>1</td>
<td>W</td>
<td>Yes (Implicit)</td>
</tr>
<tr>
<td>IAP205H-00:04</td>
<td>04:bd:88:75:00:0f2</td>
<td>d:50:66:7d:01:00</td>
<td>y</td>
<td>y</td>
<td>1</td>
<td>wlan_spllt</td>
<td>1234</td>
<td>0x0</td>
<td>a-vht-205g1-1ss</td>
<td>42m:59s</td>
<td>1</td>
<td>W</td>
<td>Yes (Implicit)</td>
</tr>
</tbody>
</table>

**Num Clients:** 3

The phy column shows the client's operational capabilities for the current association.

Flags: A: Active, B: Band Steerable, H: Hotspot (802.11u) client, K: 802.11k client, R: 802.11r client, W: WMM client, V: 802.11v client

**VHT**: High throughput; 20: 20MHz; 40: 40MHz; t: turbo-rates (256-QAM)

**<n>ss**: <n> spatial streams

---

**CONFIDENTIAL © Copyright 2015. Aruba Networks, an HP company. All rights reserved.**
Client Troubleshooting

- Association – Windows
  
  `netsh wlan show interfaces`  (or all which shows everything)

  ![Netsh wlan show interfaces output]
  
  Don't trust these numbers, The controller shows much more accurate information
Client Troubleshooting

- **Association – Mac**
  
  
  `airport -s` and `airport -l`

```
-MacBook-Air-2:~$ airport -s
SSID BSSID RSSI CHANNEL HT CC SECURITY (auth/unicast/group)
  -1X9c:1c:1d:8b:9fa0 -72 1 Y US WPA2(PSK/AES/AES)
  -1X9c:1c:1d:8b:9fb0 -39 149,1 Y US WPA2(PSK/AES/AES)
```

```
-MacBook-Air-2:~$ airport -l
agrcIdeRSSI: -62
agrcExtRSSI: 0
agrcIdeNoise: -91
agrcExtNoise: 0
  state: running
  op mode: station
  lastTxRate: 405
  maxRate: 450
  lastAssocStatus: 0
  802.11 auth: open
  link s
    BSSID: 9c:1c:1d:8b:9fb0
    SSID: Griffth-1X
    MCS: 23
    channel: 149,1
```
Client Troubleshooting

• Association

  *show ap debug client-table ap-name Primary-220*

  This is a critical command for viewing the upstream data rates from the client to the AP and vice versa

Remember that data rates are dynamic and will fluctuate
Client Troubleshooting

- Roaming – Where has the client been did the controller do something to force a roam?

```
show ap client trail-info <mac>
```
• **Authentication**
  - 802.1X used as part of WPA2/AES is the source of most authentication issues in wireless networks, especially with client roaming
    - Remember that are a LOT of radius transactions that occur during initial connectivity and/or roaming between access points unless PMK caching or OKC is utilized by the client and AP.
  - Server issues
    - Where is the radius authentication server? What is the latency to that server?
    - Does this radius server have to do a backend authentication requests to another AA repository like Active Directory? What is the latency between the radius front end and backend AA database?
    - Are there any timeouts occurring
  - Client driver issues
    - Key exchanges not happening properly as seen in the “show auth-tracebuf”?
    - Other client transactions not happening properly as seen in the “show auth-tracebuf”? 

Client Troubleshooting
Authentication - 802.1X

- 802.1X authentication happens when
  - The user initially connects
  - The user roams between access points
    - Pairwise Master Key (PMK) Caching
      - Enabled by default and cannot disable but you can disable validation of the PMKID BUT DON’T!!
      - Enables 4 way key exchange versus going through a full authentication
      - Is done when a user roams back to an access point that the user has been to in the last 8 hours (timer is configurable)
      - Doesn’t always work, key can be invalidated by either party

From IEEE 802.11i section 8.4.1.2.1 - A STA (AP) can retain PMKs for APs (STAs) in the ESS to which it has previously performed a full IEEE 802.1X authentication. If a STA wishes to roam to an AP for which it has cached one or more PMKSAs, it can include one or more PMKIDs in the RSN information element of its (Re)Association Request frame. An AP whose Authenticator has retained the PMK for one or more of the PMKIDs can skip the 802.1X authentication and proceed with the 4-Way Handshake. The AP shall include the PMKID of the selected PMK in Message 1 of the 4-Way Handshake. If none of the PMKIDs of the cached PMKSAs matches any of the supplied PMKIDs, then the Authenticator shall perform another IEEE 802.1X authentication. Similarly, if the STA fails to send a PMKID, the STA and AP must perform a full IEEE 802.1X authentication."

- Opportunistic Key Caching (OKC)
  - Enabled by default
  - Enables 4 way key exchange versus going through a full authentication
  - Not all clients support

- Based on all this the radius server MUST be local or available over a very low latency link
  - Remember that there are 20+ radius transactions per user authentication if no PMK caching or OKC

Client Troubleshooting
### Authentication – Troubleshooting 802.1X Auth Issues

**Radius Authentication Server**

- Common issue when radius servers are not local (or even when they are because of overutilization)
- To view radius server timeouts and look for a high percentage of timeouts relative to the overall number of requests
  - `show aaa authentication-server radius statistics`
    (sort of hidden command since if you type `show aaa authentication-server radius statistics`? It won’t show up)

---

**Average response times should be below 100ms and the timeouts should not be incrementing**
• **Authentication – Troubleshooting 802.1X Auth Issues**
  If the radius server statistics look good but the user is not authenticating properly or having trouble roaming do the following….
  – Enable debugging for their mac address
    • `logging level debugging user-debug <mac address>`
  – Have them try to authenticate or roam to re-create the issue
  – Look at the auth-tracebuf on the controller to see what the issue is
    • `Show auth-tracebuf | inc <mac address>`
    • Note that this is a rolling buffer that is FIFO so don’t wait too long to view
    • Also, when you are done troubleshooting make sure you disable the debug logging on the controller
      • `Config t no logging level debugging user-debug <mac address>`
### Authentication – Troubleshooting 802.1X Auth Issues

**Viewing the auth-tracebuf – Almost Normal Full 802.1X Authentication**

(XYZ Company) #show auth-tracebuf | include 38:aa:3c:12:dd:32

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Type</th>
<th>MAC Address</th>
<th>Result</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 29 20:16:47</td>
<td>station-down</td>
<td>38:aa:3c:12:dd:32 db:c7:c8:96:70:bc</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>May 29 20:16:50</td>
<td>rad-req</td>
<td>38:aa:3c:12:dd:32 db:c7:c8:96:70:bc</td>
<td>2 400</td>
<td></td>
</tr>
</tbody>
</table>

CONFIDENTIAL © Copyright 2015. Aruba Networks, an HP company. All rights reserved.
Client Troubleshooting

- **Authentication – Troubleshooting 802.1X Auth Issues**

Viewing the auth-tracebuf – Almost Normal Full 802.1X Authentication Continued

```plaintext
user supplicant timed out here and server had to make another EAP-ID request
May 29 20:16:53  station-data-ready * 38:aa:3c:12:dd:32 00:00:00:00:00:00  851 -
May 29 20:16:53  wpa2-key1 ← 38:aa:3c:12:dd:32 d8:c7:c8:96:70:bc - 117
May 29 20:16:53  wpa2-key4 → 38:aa:3c:12:dd:32 d8:c7:c8:96:70:bc - 95
```
Client Troubleshooting

- Authentication – Troubleshooting 802.1X Auth Issues

Viewing the auth-tracebuf – Normal Full 802.1X Authentication After Roam

## Authentication – Troubleshooting 802.1X Auth Issues

### Viewing the auth-tracebuf – Normal Full 802.1X Authentication After Roam

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Source MAC Address</th>
<th>Destination MAC Address</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 29 20:17:28</td>
<td>station-data-ready</td>
<td>38:aa:3c:12:dd:32</td>
<td>00:00:00:00:00:00</td>
<td>851 444</td>
</tr>
<tr>
<td>May 29 20:17:28</td>
<td>wp2-key1</td>
<td>38:aa:3c:12:dd:32</td>
<td>d8:c7:c8:96:4b:b8</td>
<td>- 117</td>
</tr>
<tr>
<td>May 29 20:17:28</td>
<td>wp2-key4</td>
<td>38:aa:3c:12:dd:32</td>
<td>d8:c7:c8:96:4b:b8</td>
<td>- 95</td>
</tr>
</tbody>
</table>

All good with this exchange and user roam
Client Troubleshooting

• Authentication – Troubleshooting 802.1X Auth Issues
  Viewing the auth-tracebuf – PMK Caching After Roaming Back to Original BSSID

May 29 20:18:04 station-down          * 38:aa:3c:12:dd:32  d8:c7:c8:96:4b:b8          - -
May 29 20:18:04 station-up            * 38:aa:3c:12:dd:32  d8:c7:c8:96:70:bc          - - wpa2 aes
May 29 20:18:04 station-data-ready    * 38:aa:3c:12:dd:32  00:00:00:00:00:00          851 -
May 29 20:18:04 wpa2-key1            <- 38:aa:3c:12:dd:32  d8:c7:c8:96:70:bc          - 117 -
May 29 20:18:04 wpa2-key2            -> 38:aa:3c:12:dd:32  d8:c7:c8:96:70:bc          - 135 -
May 29 20:18:04 wpa2-key3            <- 38:aa:3c:12:dd:32  d8:c7:c8:96:70:bc          - 151 -
May 29 20:18:04 wpa2-key4            -> 38:aa:3c:12:dd:32  d8:c7:c8:96:70:bc          -  95 -

Note the abbreviated authentication since PMK caching has kicked in here
Authentication – Troubleshooting 802.1X Auth Issues

Viewing the auth-tracebuf – User Supplicant Not Responding to EAP-ID Request

- User roams here
- Appears that the AP no longer has the PMK cached so a full re-auth is started
- Houston we have a problem…the client is not responding to the eap requests, see the next 3 requests and the timestamps. Our timeout (which is configurable) is 5 seconds by default which is more than enough time.
- Remember that these EAP messages are between the client and the server so the server decides to timeout and force the client to try again.
- The station didn’t respond to the last message so it’s timed out and the process starts over
- On the next try the user responds to the second EAP ID request and then things proceed normally.

Note that this ended up to be a client driver/supplicant issue that was reported to the appropriate manufacturer
Client Troubleshooting

- **Authentication – Troubleshooting 802.1X Auth Issues**
  
  Viewing the auth-tracebuf – Bad Client Driver

(7200-xyz) #show auth-tracebuf | include 3c:a9:43:32:da:bc
Jan 29 07:04:36 station-down   * 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 - -
Jan 29 07:14:55 station-up     * 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 - - wpa2 aes
Jan 29 07:14:57 eap-start    -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 - -
Jan 29 07:15:00 eap-id-resp -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 1 11 nmdq87
Jan 29 07:15:00 eap-resp    -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 45 227
Jan 29 07:15:00 rad-resp   <- 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 Radius-2 65516 1089
Jan 29 07:15:00 eap-req     <- 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 46 1012
Jan 29 07:15:00 eap-resp    -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 46 6
Jan 29 07:15:00 rad-req    <- 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 Radius-2 65517 237
Jan 29 07:15:00 rad-resp  -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 65517 1085
Jan 29 07:15:00 eap-req     <- 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 47 1008
Jan 29 07:15:00 eap-resp    -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 47 6
Jan 29 07:15:00 rad-req    <- 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 Radius-2 65518 237
Jan 29 07:15:00 rad-resp  -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 65518 1085
Jan 29 07:15:00 eap-req     <- 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 48 1008
Jan 29 07:15:00 eap-resp    -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 48 6
Jan 29 07:15:00 rad-req    <- 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 Radius-2 65519 237
Jan 29 07:15:00 rad-resp  -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 65519 1085
Jan 29 07:15:00 eap-req     <- 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 49 1008
Jan 29 07:15:00 eap-resp    -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 49 6
Jan 29 07:15:00 rad-req    <- 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 Radius-2 65520 237
Jan 29 07:15:00 rad-resp  -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 65520 1085
Jan 29 07:15:00 eap-req     <- 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 50 195
Jan 29 07:15:00 eap-resp    -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 50 1310
Jan 29 07:15:00 rad-req    <- 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 Radius-2 65521 1551
Jan 29 07:15:00 rad-resp  -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 65521 77
Jan 29 07:15:00 eap-req     <- 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 51 6
Jan 29 07:15:00 eap-resp    -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 51 895
Jan 29 07:15:00 eap-req     <- 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 52 195
Jan 29 07:15:00 eap-resp    -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 52 1310
Jan 29 07:15:00 rad-req    <- 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 Radius-2 65522 1551
Jan 29 07:15:00 rad-resp  -> 3c:a9:43:32:da:bc 9c:1c:12:8a:75:00 65522 77
• Authentication – Troubleshooting 802.1X Auth Issues
Viewing the auth-tracebuf – Bad Client Driver
Client Troubleshooting

- Authentication – Troubleshooting 802.1X Auth Issues
  Viewing the auth-tracebuf – Bad Client Driver

Jan 29 07:23:57 wpa2-key1 <- 3c:a9:14:32:da:bc 9c:1c:12:8a:75:c0 88 17
Jan 29 07:23:57 wpa2-key4 -> 3c:a9:14:32:da:bc 9c:1c:12:8a:75:c0 - 95

CONFIDENTIAL © Copyright 2015. Aruba Networks, an HP company. All rights reserved.
Client Troubleshooting

- **Authentication – Troubleshooting 802.1X Auth Issues**

  **Viewing the auth-tracebuf – Bad Client Driver**

  Ubuntu Linux Driver Issue with Intel 6300
  Resolution was to disable 40 MHz channels on the client
Client Troubleshooting

- **Network Connectivity**
  - DHCP
    - Is the server getting overloaded?
      - DHCP NACKs happen during roams (client checking to make sure it can still use the address)
    - Is the controller the DHCP server?
      - If greater than X number of clients then an external DHCP needs to be used
    - Use debug logging on the controller for DHCP
      - `conf t logging level debugging network subcat dhcp`
  - User VLAN
    - Is the user vlan being switched/routed properly
### Network Connectivity – DHCP Normal Release/Renew

- Viewing DHCP requests in the controller after enabling debug logging

```
show log network 100 (| inc dhcp)
```

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Length</th>
<th>Message Type</th>
<th>Option Code</th>
<th>Message</th>
<th>Option Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>00:11:00:00:00:00</td>
<td>68</td>
<td>Discover</td>
<td>100</td>
<td>DHCP</td>
<td>128</td>
</tr>
<tr>
<td>192.168.1.1</td>
<td>00:12:00:00:00:00</td>
<td>68</td>
<td>Offer</td>
<td>100</td>
<td>DHCP</td>
<td>128</td>
</tr>
<tr>
<td>192.168.1.1</td>
<td>00:13:00:00:00:00</td>
<td>68</td>
<td>Request</td>
<td>100</td>
<td>DHCP</td>
<td>128</td>
</tr>
<tr>
<td>192.168.1.1</td>
<td>00:14:00:00:00:00</td>
<td>68</td>
<td>Inform</td>
<td>100</td>
<td>DHCP</td>
<td>128</td>
</tr>
<tr>
<td>192.168.1.1</td>
<td>00:15:00:00:00:00</td>
<td>68</td>
<td>Ack</td>
<td>100</td>
<td>DHCP</td>
<td>128</td>
</tr>
</tbody>
</table>

**DHCP - Dynamic Host Configuration Protocol**
- **Message Type**: 1 - Discover (284)
Network Connectivity – DHCP Normal Roam

- Viewing DHCP requests in the controller after enabling debug logging

```
show log network 100 (| inc dhcp)
```
**User Role(s)**
- What user roles are assigned to the user both pre-authentication (captive portal) and post authentication? Do the respective roles have the correct ACLs?

```
show user mac <mac>
```

```
Name: IP: 192.168.1.9, MAC: 24:77:03:ff:5e:78, Role: authenticated, ACL: 64/0, Age: 00:01:25
Authentication: N-A, status not started, method: protocol, server:
Role Derivation: AAS profile default role
VLAN Derivation: Default VLAN
TTL timeout (global): 3600 seconds, Age: 00:01:00
Mobility state: Wireless, HA: Yes, Proxy ARP: No, Roaming: No Tunnel ID: 0 (L3 Mobs: 0)
Flags: internal=0, trusted=x=0, lauth=0, aban=0, vpnFlag=0, auth��ageout=1
Flags: inner=0, outer=0, vpn_inner_indio, download=1, wisp=0
IP User timeouts: 0
Phy type: a-MT-40, l3 reauth: 0, BW Contract: up=0 down=0, user-how: 14
Vlan default: 1, Assigned: 1, Current: 1 vlan-how: 1 BP assigned vlan: 0
Mobility Messages: L2-0, Move-0, INT-0, INR-0, Flags=0x0
SlotPort=0x2126, Port=0x10012 (Tunnel 18)
Role assignment: L3 assigned role n/a, VPN role n/a, Dot1x cached role n/a
Current Role name: authenticated, role-when: 10, L3-role: authenticated, L3-role: authenticated
BurpAccess sessionID/1
BurpAccess Traffic 6336/182799 Out 7675/405785 (0:6336/0:0:0:342,0:1675/0:0:65:44925)
info flags ud=0 mac=0 dot1x 4 AUTHINTERM accounting 0
IP Runtime 1432008306 (Wed Feb 4 15:03:26 2015)
Core User-Born: 1432008305 (Wed Feb 4 15:03:25 2015)
Upstream AP ID: 5, Downstream AP ID: 9
User Agent String: N900/21.8.0.32 MTD/H:6gEx-k8L3fPYBYgC01Dyo ALuron/6.1;SP1.0;X64;ENU
HTTP based device-id info - Index: 40, Devices Windows
Overall device-id info - Index: 27, Device: Windows
L3 Auth Session Timeout From Radius: 0
Mac Auth Session Timeout Value from Radius: 0
Dot1x Session Timeout Value from Radius: 0
C8A Session Timeout Value from Radius: 0
Dot1x Session Term-Action Value from Radius: Default
Reauth-interval from radius: 0
Number of reauthentications attempted: mac reauth 0, dot1x reauth 0
Mac auth server: N/A, Dot1x auth server: N/A
Address 15 from EAP: yes
Per-user-log pointer: 0x7f2a03c (Id 224), num logs 23
```
Client Troubleshooting

- User Role(s) – What ACLS are applied?
- Show rights <role name>
Client Troubleshooting

- **User Role(s)** – Is the user hitting the ACL
- **Show datapath session | inc <user ip address>**
- or
- **Show datapath session | include "Source IP,Flags,no syn,set ToS,mirror,Real-Time,Deep inspect,Media Deep,Application Firewall,<user ip>"** to show column headers and flag definitions

![Datapath Session Table](image-url)
What we covered

• **Design for roaming:**
  • Channel planning for roaming
  • Access Point Planning and Placement
  • Adaptive Radio Management (ARM)

• **Client Roaming**

• **Client Troubleshooting**
THANK YOU