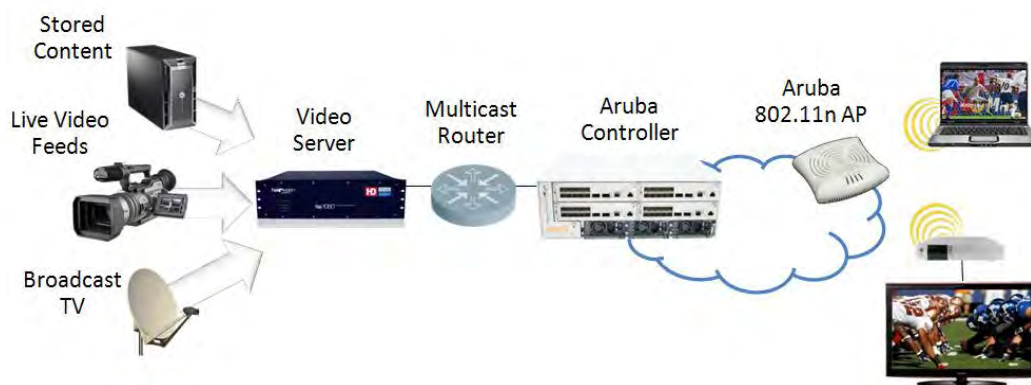


## Aruba Video Quick Reference & Design Guide

This document is aimed at creating a single location for successful video deployment best practices and methodologies using the Aruba Infrastructure. Distributing standard and high definition video has long been the promise of Wi-Fi, but the results have been less than satisfactory due to the limitations of slow 802.11 clients, inadequate multicast capabilities, and the lack of control over client behavior. Now you can enjoy high-fidelity, high-availability, multi-channel video using Aruba's application-aware 802.11n wireless LANs. Our high-speed 802.11n networks feature intelligent multicast services, and leverage infrastructure-based client and radio management techniques. The result is high quality, reliable video even in crowded environments with shared devices and applications.



To optimize video content from end-to-end, over-the-wire and over-the-air, there are considerations that need to be made in both environments. This quick reference guide makes recommendations for the Ethernet infrastructure and for the wireless LAN. The latter is specific to Aruba architecture and mentions software and hardware dependencies when relevant.

### Wired Infrastructure Optimization

There are four primary recommendations to consider in the wired network for supporting broadcast-quality video. Reference the User Guide provided by the appropriate wired infrastructure vendor to enable these settings:

#### 1. Utilize Gigabit Ethernet End-to-End

It is recommended to have Gigabit Ethernet connectivity from the between all components in the path of video delivery. This includes Gigabit to the Video Server, Aruba Controller, and Aruba 802.11n APs.

**2. Enable IGMP**

IGMP proxy or IGMP snooping should be used to facilitate video delivery only to those APs with subscribers. See below for recommendations regarding proxy vs. snooping.

**3. Configure Quality of Service Traffic Tagging and Prioritization**

Traffic tagging and prioritization should be enabled in the wired network to provide Quality of Service (QoS) to the video streams. It is important to enable Layer 3 Video Differentiated Services Code Point (DSCP) tagging and Layer 2 802.1p tagging on the application (server and clients if possible), the controller (see below), and prioritization/QoS on the wired infrastructure for end-to-end QoS guarantees.

**4. Adjust Video Frame Size**

It is recommended to set the frame size at the video server low enough to avoid fragmentation, or enable jumbo frames to the largest supported size if possible. It is important to ensure the MTU of the video server is not larger than the maximum frame size on any wired segment. Fragmentation can be verified by monitoring the frame counters on the switch or router interface(s) along the video data path. Fragment loss results in the entire video frame<sup>1</sup> being retransmitted, also increasing over the air bandwidth.

**Wireless LAN Optimization**

The table below is a summary of recommended configurations to optimize Aruba WLANs for high-quality video. These features require AOS 3.4.1 or later.

Feature	Setting	Where to find it?
Radio	2.4 GHz or the 5GHz based on the design, 5 GHz is recommended for most deployments. Ideally, segregate video into a separate HT 802.11n 5GHz SSID.	Configuration->AP conf->AP name->RF management>802.11a/g Radio profile settings
IGMP Proxy	Enabled on the ingress port (from the server towards the controller) of the appropriate VLAN. Recommended for most deployments, does not require a multicast router, and must be used when L3 mobility is required.	Configurations->IP->appropriate VLAN

<sup>1</sup> The term video frame here refers to an I, P, or B frame using the H.264 video codec, for example. Decoding can only start after reception of a 'key' frame which may only appear every few seconds, so it is most important that these are not lost in-transit.

## Aruba Video Quick Reference & Design Guide

<b>IGMP Snooping</b>	Disabled by default and not recommended for most deployments. If enabled, clients on different VLANs will require separate streams (video server to controller) for each VLAN. This will tend to increase traffic if VLAN pooling is used.	Configurations->IP->appropriate VLAN									
<table border="1"> <tr> <td data-bbox="175 474 548 720"><b>Access Control List</b></td> <td data-bbox="553 474 1024 720">Enable an ACL which tags all traffic with a destination address of „multicast group IP“ has to be tagged with a TOS of 40 and a dot1p tag of 5, and sent to the high priority queue. Note: if the multicast server and user are on the same VLAN, DSCP tags will not be used.</td> <td data-bbox="1029 474 1414 951" rowspan="3"> <table border="1"> <tr> <td data-bbox="1029 533 1289 730">Configuration-&gt;Access Control-&gt;Appropriate User role</td> </tr> <tr> <td data-bbox="1029 737 1289 869">Configuration-&gt;ports-&gt;appropriate port-&gt;firewall policy</td> </tr> </table> </td> </tr> <tr> <td data-bbox="175 726 548 846"><b>User based</b></td> <td data-bbox="553 726 1024 846">User based ACL – has to be applied to the appropriate user role and prioritized to the top</td> </tr> <tr> <td data-bbox="175 852 548 951"><b>Port based</b></td> <td data-bbox="553 852 1024 951">Port based ACL – has to be applied to the upstream port that carries the media traffic</td> </tr> </table>	<b>Access Control List</b>	Enable an ACL which tags all traffic with a destination address of „multicast group IP“ has to be tagged with a TOS of 40 and a dot1p tag of 5, and sent to the high priority queue. Note: if the multicast server and user are on the same VLAN, DSCP tags will not be used.	<table border="1"> <tr> <td data-bbox="1029 533 1289 730">Configuration-&gt;Access Control-&gt;Appropriate User role</td> </tr> <tr> <td data-bbox="1029 737 1289 869">Configuration-&gt;ports-&gt;appropriate port-&gt;firewall policy</td> </tr> </table>	Configuration->Access Control->Appropriate User role	Configuration->ports->appropriate port->firewall policy	<b>User based</b>	User based ACL – has to be applied to the appropriate user role and prioritized to the top	<b>Port based</b>	Port based ACL – has to be applied to the upstream port that carries the media traffic		
<b>Access Control List</b>	Enable an ACL which tags all traffic with a destination address of „multicast group IP“ has to be tagged with a TOS of 40 and a dot1p tag of 5, and sent to the high priority queue. Note: if the multicast server and user are on the same VLAN, DSCP tags will not be used.	<table border="1"> <tr> <td data-bbox="1029 533 1289 730">Configuration-&gt;Access Control-&gt;Appropriate User role</td> </tr> <tr> <td data-bbox="1029 737 1289 869">Configuration-&gt;ports-&gt;appropriate port-&gt;firewall policy</td> </tr> </table>		Configuration->Access Control->Appropriate User role	Configuration->ports->appropriate port->firewall policy						
Configuration->Access Control->Appropriate User role											
Configuration->ports->appropriate port->firewall policy											
<b>User based</b>	User based ACL – has to be applied to the appropriate user role and prioritized to the top										
<b>Port based</b>	Port based ACL – has to be applied to the upstream port that carries the media traffic										
<b>Band Steering</b>	Enable to steer clients to 5 GHz for video delivery.	Configuration->AP conf->AP name->Wireless LAN->VAP profile->profile name									
<b>Dynamic Multicast Optimization</b>	Enabled with threshold set to a high value depending on the client mix (see later section regarding DMO and scalability for recommended settings).	Configuration->AP conf->AP name->Wireless LAN->VAP profile->profile name									
<b>BC/MC rate optimization</b>	Enabled	Configuration->AP conf->AP name->Wireless LAN->SSID Profile->Profile name									
<b>WMM traffic management profile - Shaping</b>	Enabled with an appropriate share of bandwidth dedicated for the video traffic. This changes for various deployment scenarios and must be calculated based on video and data sizing requirements.	Configuration->AP conf->AP name->Wireless LAN->SSID Profile->WMM traffic management profile->profile name									
<b>Spectrum Load balancing</b>	Enable to distribute clients across channels.	Configuration->AP conf->AP name->RF management>802.11a/g Radio profile settings									
<b>Adaptive Radio Management (ARM) profile settings</b>		Configuration->AP conf->AP name->RF- management->802.11a/g Radio									

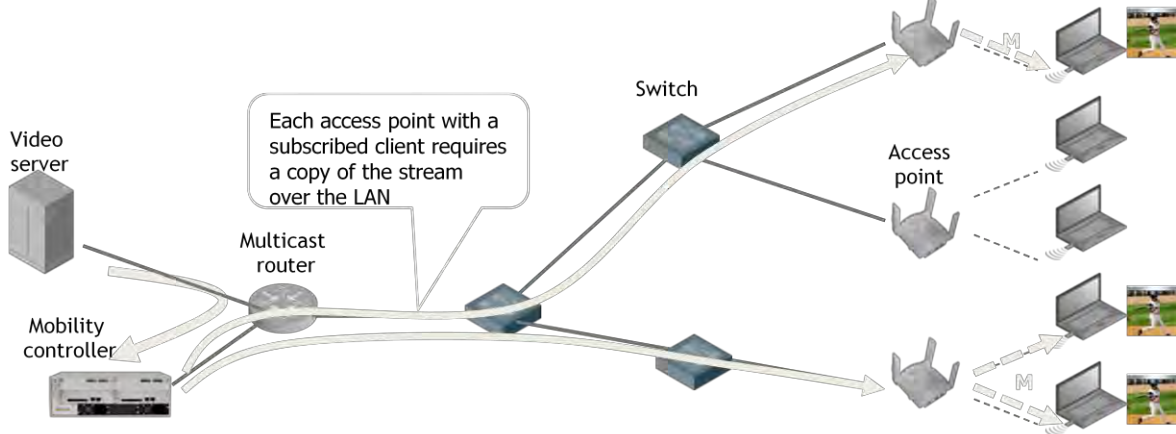
<b>Assignment</b>	Single-band or multi-band depending on whether AP is single or dual-radio.	profile settings->ARM profile	
<b>Client Aware</b>	Enabled		
<b>Scanning</b>	Enabled		
<b>Video aware scanning</b>	Enabled		
<b>Load aware scan threshold</b>	125000 Bps		
<b>Power save aware scan</b>	enabled		
<b>Traffic Management Profile</b>	Fair Access	Configuration->AP conf->AP name->QoS->802.11a/g Traffic Management Profile	

### Enable IGMP on the Controller

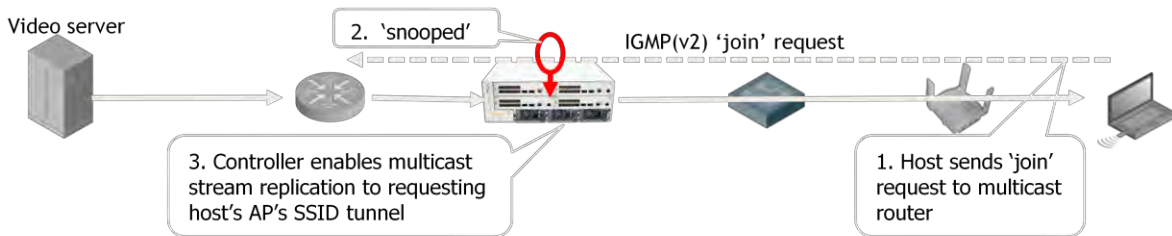
IGMP snooping<sup>2</sup> by the Aruba controller limits forwarding of multicast streams to access points serving multicast video subscribers. The result is improved efficiency and network performance for video. The controller reads IGMP messages from clients to multicast routers and keeps track of which APs have clients subscribing to multicast. This allows the controller to send multicast traffic to only those APs, thereby avoiding unnecessary replication to other APs.

<sup>2</sup> Note that with snooping, clients on different VLANs will require separate streams (video server to controller) for each VLAN. This will tend to increase traffic if VLAN pooling is used, as clients will be randomly allocated to VLANs, so it is quite possible for multiple clients with the same characteristics to end up on different VLANs.

IGMP Snooping and Multicast Streams in a Centralized-Traffic WLAN

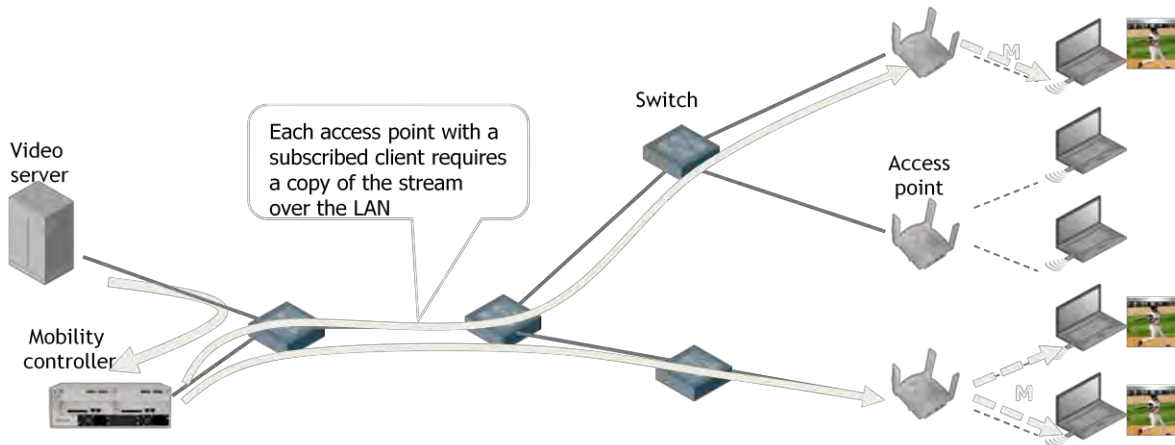


Control packets and media stream flow

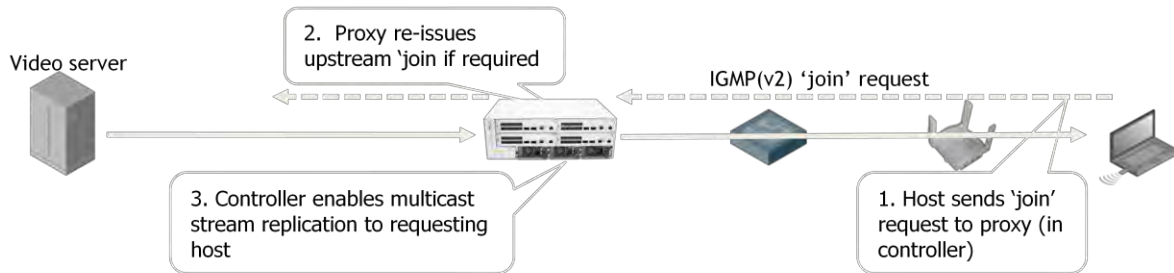


**Enable IGMP Proxy** – IGMP proxy implements multicast routing by re-originating IGMP joins and leaves from the source of the controller. As an alternative to IGMP snooping, which works on a per-SSID tunnel basis and requires an external multicast router to generate the IGMP membership reports, IGMP proxy works on a per-client basis and does not require an external multicast router.

IGMP Proxy and Multicast Streams in a Centralized-Traffic WLAN



Control packets and media stream flow



IGMP proxy should be enabled on the user VLAN IP interface, also stating the interface where the multicast frames are being transmitted into the controller. This will make sure that the IGMP client membership table is filled out properly. Without the IGMP client membership table properly filled out, dynamic multicast optimization will not take place, leading to video quality degradation. The screenshot below shows the settings that need to be configured in order to enable intelligent forwarding of multicast data in the Aruba controllers.

Go to **Configurations->IP->appropriate VLAN** and select **,Edit'**. Select the appropriate checkboxes as shown below.

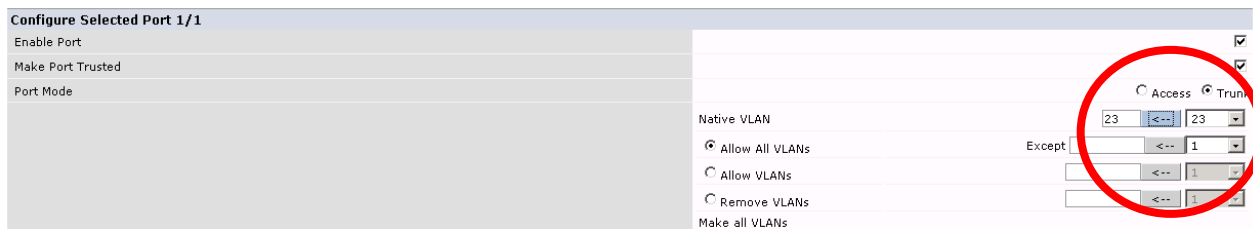


*Note - IGMP snooping and IGMP proxy should not be enabled concurrently on the same interface.*

IGMP proxy is recommended in most applications. If you require L3 IP Mobility for your multicast clients, you must use IGMP Proxy. Only Proxy synchronizes IGMP state across the Home Agent and Foreign Agent. If L3 IP Mobility is not required, either snooping or proxy may be used.

**Extend VLAN Upstream to Router.** This step must be taken for IGMP proxy to work. This enables the switch to respond to IGMP messages from the upstream router. The Aruba controller will send all IGMP reports to the upstream router on the interface configured since IGMP routing is done by the upstream router.

Go to **Configurations->Network->Ports** and select the appropriate port number. Select the appropriate VLAN for either access or trunking on this port as shown below.



### Set Traffic Tagging and Prioritization

1. **Enable DSCP on the Controller** - The Aruba controller translates DSCP tags over the wire to WMM tags over the air automatically. This allows end-to-end prioritization of video traffic. As stated earlier, it is also important to enable Video DSCP tagging on wired infrastructure for end-to-end QoS guarantees.

Go to **Configurations->AP configuration->AP name** and select **edit**. Expand **Wireless LAN->VAP profile->profile name->SSID profile**. Select the advanced tab. Ensure that WMM is enabled (see checkbox) and the corresponding DSCP mappings are present as shown in the screenshot. These are the default mappings for voice, video and the best effort data – adjust if necessary.

Wireless Multimedia (WMM)	<input checked="" type="checkbox"/>	Wireless Multimedia U-APSD (WMM-UAPSD) Powersave	<input checked="" type="checkbox"/>
WMM TSPEC Min Inactivity Interval	0 msec	DSCP mapping for WMM voice AC	56
DSCP mapping for WMM video AC	40	DSCP mapping for WMM best-effort AC	24
DSCP mapping for WMM background AC	8	902il Compatibility Mode	<input type="checkbox"/>

2. **Create Video ACL Rule** - If the network is already tagging video, you don't need an ACL rule to tag it, but it is still recommended best practice to have one. The ACL shown in the example below will tag all traffic destined to a multicast address with a TOS value and direct it towards the high priority queue in order to ensure end-to-end quality of service. The multicast address can be any<sup>3</sup> address in the private address space that is used by the media server to stream video.

Go to **Configuration->Access control** and select the **policies** tab. A new policy has to be created with a firewall rule (example name: mcast\_video\_port\_acl):

**source – any, destination- an alias that points to the right multicast address, action – permit, queue – high , TOS – 40, 802.1p – 5**

A second firewall rule **to allow all traffic** is also created as shown in the screenshot below.

Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Pause ARM Scanning	BlackList	TOS	802.1p	Priority	Action
any	mcast_subnet	any	permit			High		Yes		40	5		Delete ▲ ▼
any	any	any	permit			Low							Delete ▲ ▼

**Port based ACL** – It is recommended to apply the port ACL firewall policy upstream to the server on the ingress port that carries the media stream.

Go to **Configuration->ports** and select the **upstream** port. In the firewall policy drop down box select the appropriate policy and select apply.



<sup>3</sup> TOS values are configurable to match values in use on the wired network. Those shown are default values.

**User based ACL** – Optionally, a user based ACL can be employed to prioritize traffic after the traffic hits the controller. Every client in an Aruba user centric network is associated with a user role, which determines the client’s network privileges. You specify one or more policies for a user role. The multicast policy is applied either to the logon role for an open network or an authenticated role in a network with some level of security enabled. Firewall policies are executed in order, so be sure that the multicast policy is the first in the rule in the policy.

The screenshot below shows how the multicast policy is prioritized and tied to the authenticated role.

Name	Firewall Policies
authenticate4d	Not Configured
authenticated	mcast_video_acl/allowall/,v6-allowall/
authenticated_conf	authenticated_http_https_proxy_acl/,allowall/,v6-allowall/
default-vpn-role	allowall/,v6-allowall/
guest	http-acl/,https-acl/,dhcp-acl/,icmp-acl/,dns-acl/,v6-http-acl/,v6-https-acl/,v6-dhcp-acl/,v6-icmp-acl/,v6-dns-acl/
guest-logon	logon-control/,captiveportal/

*Note: The port based ACL must be different from the user based ACL in that the allowall statement does not immediately follow the multicast prioritization rule in the user based ACL. This is needed in the port based ACL so that the non-multicast traffic will still get through the ingress interface.*

### Adaptive Radio Management (ARM) settings

Aruba’s ARM is a distributed approach to enable self configuring, self healing wireless networks. In order to fully utilize the available spectrum, increase the system capacity, and the number of users supported, ARM dynamically learns about the RF medium and adapts accordingly. This is accomplished by AP’s that periodically scan other channels, analyzes the interference level seen on other channels and reports it back to the controller. The controller then computes the most optimized setting and instructs the AP to work accordingly. There is a small amount of time when the AP’s leave their channel to conduct scanning operations that are essential to ARM. Where there are real time applications such as video/voice running on the network, this periodic scan might result in latency, jitter and eventually degrade the quality of the signal. Because of the stateful firewall in the Aruba controller, ARM is application-aware, so that access points stop scanning other channels in the presence of time-sensitive applications such as voice and video. Aruba’s Video Aware Scan setting is required to be enabled for video deployments.

To modify the ARM settings go to **Configuration->AP configuration-> AP name**.

Select **RF management->802.11a radio profile->ARM radio profile->profile name**

**Adaptive Radio Management (ARM) Profile** > default Show Reference Save As Reset

Assignment	<span>single-band</span>	Allowed bands for 40MHz channels	<span>a-only</span>
Client Aware	<input checked="" type="checkbox"/>	Max Tx EIRP	<span>127</span>
Min Tx EIRP	<span>9</span>	Multi Band Scan	<input checked="" type="checkbox"/>
Rogue AP Aware	<input type="checkbox"/>	Scan Interval	<span>10</span> sec
Active Scan	<input type="checkbox"/>	Scanning	<input checked="" type="checkbox"/>
Scan Time	<span>110</span> msec	VoIP Aware Scan	<input type="checkbox"/>
Power Save Aware Scan	<input checked="" type="checkbox"/>	Video Aware Scan	<input checked="" type="checkbox"/>
Ideal Coverage Index	<span>10</span>	Acceptable Coverage Index	<span>4</span>
Free Channel Index	<span>25</span>	Backoff Time	<span>240</span> sec
Error Rate Threshold	<span>50</span> %	Error Rate Wait Time	<span>30</span> sec
Noise Threshold	<span>75</span> -dBm	Noise Wait Time	<span>120</span> sec
Minimum Scan Time	<span>8</span>	Load aware Scan Threshold	<span>1250000</span> Bps
Mode Aware Arm	<input type="checkbox"/>		

Assignment	Single-band or multi-band depending on whether AP is single or dual-radio.	Disables ARM calibration and reverts AP's back to default channel and power settings
Client Aware	Enabled	AP does not change channel if there is active client traffic
Scanning	Enabled	Enables AP scanning across other channels
Video Aware Scan	Enabled	AP does not change channel if there is active video traffic
Load Aware Scan Threshold	125000 Bps	The traffic threshold above which the AP stops scanning
Power Save Aware Scan	Enabled	AP stops scanning if one or more clients is in power save mode

### Deploy a separate HT 802.11n SSID

In most RF environments, the 2.4GHz band is more crowded than a 5 GHz band. For time sensitive applications such as video it is important to ensure that the infrastructure provides end-to-end QoS. Video QoS is typically better on the 5 GHz band as a result of the higher capacity and less congestion, so dedicating an SSID in 5 GHz is recommended whenever possible. Most voice clients cannot operate on 5 GHz band, so this facilitates separation of two distinct real-time applications on different bands of spectrum which may be desirable.

### Enable Band Steering

This feature enhances performance and user experience by automatically moving clients to the 5 GHz band when capable and reserving the 2.4 GHz band for single band clients. Use of band steering is recommended to divert video clients to the 5 GHz band if the SSID is available in both bands.

To enable Band steering

Go to **Configuration->AP Configuration-> AP name** and select **edit**

Select **WLAN profile->VAP Profile->Profile name**

Virtual AP enable	<input checked="" type="checkbox"/>	Allowed band	all
VLAN	23  <--	Forward mode	tunnel
<small>Named VLAN or list of VLAN IDs to use for this virtual AP.</small>			
Deny time range	--NONE--	Mobile IP	<input checked="" type="checkbox"/>
HA Discovery on-association	<input type="checkbox"/>	DoS Prevention	<input type="checkbox"/>
Station Blacklisting	<input checked="" type="checkbox"/>	Blacklist Time	3600 <input type="text"/> sec
Dynamic Multicast Optimization (DMO)	<input checked="" type="checkbox"/>	Dynamic Multicast Optimization (DMO) Threshold	40 <input type="text"/>
Authentication Failure Blacklist Time	3600 <input type="text"/> sec	Multi Association	<input type="checkbox"/>
Strict Compliance	<input type="checkbox"/>	VLAN Mobility	<input type="checkbox"/>
Remote-AP Operation	standard	Drop Broadcast and Multicast	<input type="checkbox"/>
Convert Broadcast ARP requests to unicast	<input type="checkbox"/>	Band Steering	<input checked="" type="checkbox"/>

### Enable Dynamic Multicast Optimization (DMO)

Over-the-air transmissions can benefit from unicast transmissions depending on the number of clients in use. If only a small number of clients are subscribed to a multicast group, it can be more efficient to convert over-the-wire multicast to over-the-air unicast due to the faster data rates and prioritization capabilities of unicast connections. As this number grows, multicast gains in efficiency over unicast. Aruba's Dynamic Multicast Optimization (DMO) technology dynamically selects the appropriate conversion based on real-time network and video usage information. The conversion takes place at the controller at the 802.11 layer, on a client-by-client basis, and is transparent to the higher-level client layers.

Benefits of DMO include:

- Ease of deployment: DMO is dynamic, providing automatic multicast-to-unicast traffic optimization in the controller without requiring ongoing monitoring and configuration. Multicast IP frames are transmitted over the air using 802.11 unicast headers dynamically based on a configurable threshold.
- QoS: Multicast video traffic utilizes the WMM video queue for prioritization.
- Higher capacity: Reliable multicast video over 802.11n at HT rates.

To enable Dynamic Multicast Optimization

Go to **Configuration->AP Configuration-> AP name** and select **edit**

Select **WLAN profile->VAP Profile->Profile name**

Virtual AP enable	<input checked="" type="checkbox"/>	Allowed band	all <input type="button" value="v"/>
VLAN	23 <input type="button" value="v"/> <-- 23 <input type="button" value="v"/>	Forward mode	tunnel <input type="button" value="v"/>
Deny time range	--NONE-- <input type="button" value="v"/>	Mobile IP	<input checked="" type="checkbox"/>
HA Discovery on-association	<input type="checkbox"/>	DoS Prevention	<input type="checkbox"/>
Station Blacklisting	<input checked="" type="checkbox"/>	Blacklist Time	3600 <input type="button" value="v"/> sec
Dynamic Multicast Optimization (DMO)	<input checked="" type="checkbox"/>	Dynamic Multicast Optimization (DMO) Threshold	40 <input type="button" value="v"/>
Authentication Failure Blacklist Time	3600 <input type="button" value="v"/> sec	Multi Association	<input type="checkbox"/>
Strict Compliance	<input type="checkbox"/>	VLAN Mobility	<input type="checkbox"/>
Remote-AP Operation	standard <input type="button" value="v"/>	Drop Broadcast and Multicast	<input type="checkbox"/>
Convert Broadcast ARP requests to unicast	<input type="checkbox"/>	Band Steering	<input checked="" type="checkbox"/>

## Aruba Video Quick Reference & Design Guide

The DMO threshold has a default value of 6 clients, but it may be set higher. The DMO threshold specifies the number of HT WLAN clients per Virtual AP, per VLAN for video delivery mode. Video is delivered as multicast when the number of HT clients exceeds the threshold, and video delivered as unicast when the number of HT clients is below the threshold. For this computation, 1 legacy client (802.11a/b/g) has a penalty factor equal to 3 HT clients (802.11n).

For example, if there are three 802.11n clients associated to a VAP and the threshold value is set to 4, DMO will take place. Once the fifth HT client associates to the same VAP, DMO will no longer take place. If two 802.11b clients are associated to the VAP and the threshold is set to 4, they will be treated as if they were 6 HT 802.11n clients and DMO will not take place. Consult the video scalability section below for recommendations regarding this setting.

### Enable Wireless Multi-Media (WMM) Shaping Policy

WMM traffic shaping provides bandwidth allocation among the four WMM access categories. For optimal performance it is strongly recommended to have a dedicated video SSID, and to set the video share to 80%. For shared video + data SSIDs, it is recommended to set the video share to between 40 and 70%, depending on the percentage of video traffic on the network and the requirement for data users.

In order to set the WMM shaping policy

Go to **Configuration -> AP configuration -> AP name** and select **edit**.

Select **Wireless LAN profile->SSID Profile->WMM traffic management profile**.

For example, in the screenshot below, 15% of the airtime is assigned to the Voice traffic, and 70% is reserved for video in the WMM traffic management profile, and data will maintain at least 10% of the airtime during congested conditions.

WMM Traffic Management Profile > video-priority Show Reference Save As Reset

Enable Shaping Policy	<input checked="" type="checkbox"/>	Voice Share	<input type="text" value="15"/>	%
Video Share	<input type="text" value="70"/>	Best-effort Share	<input type="text" value="10"/>	%
Background Share	<input type="text" value="5"/>			

### Enable Multicast Rate Optimization

In cases where Dynamic Multicast Optimization (DMO) determines that it is more efficient to send traffic over-the-air as multicast, Multicast Rate Optimization (MRO) supports higher data rate multicast frame transmissions increasing multicast traffic capacity in a given channel. The AP transmits multicast traffic at the lowest common rate sustainable for all associated subscribers instead of using the lowest common supported rate for all clients. This allows conservation of wireless bandwidth and higher video density. It

## Aruba Video Quick Reference & Design Guide

is recommended to enable this feature whenever deploying video, but note that DMO will always take precedence over MRO up to the configurable threshold value.

Go to **Configuration->AP configuration-> AP name** and select **edit**

Select **Wireless LAN Profile-> VAP Profile-> Profile name->SSID profile**

Go to the advanced tab and scroll down to find **BC/MC rate optimization** as shown in the screenshot below

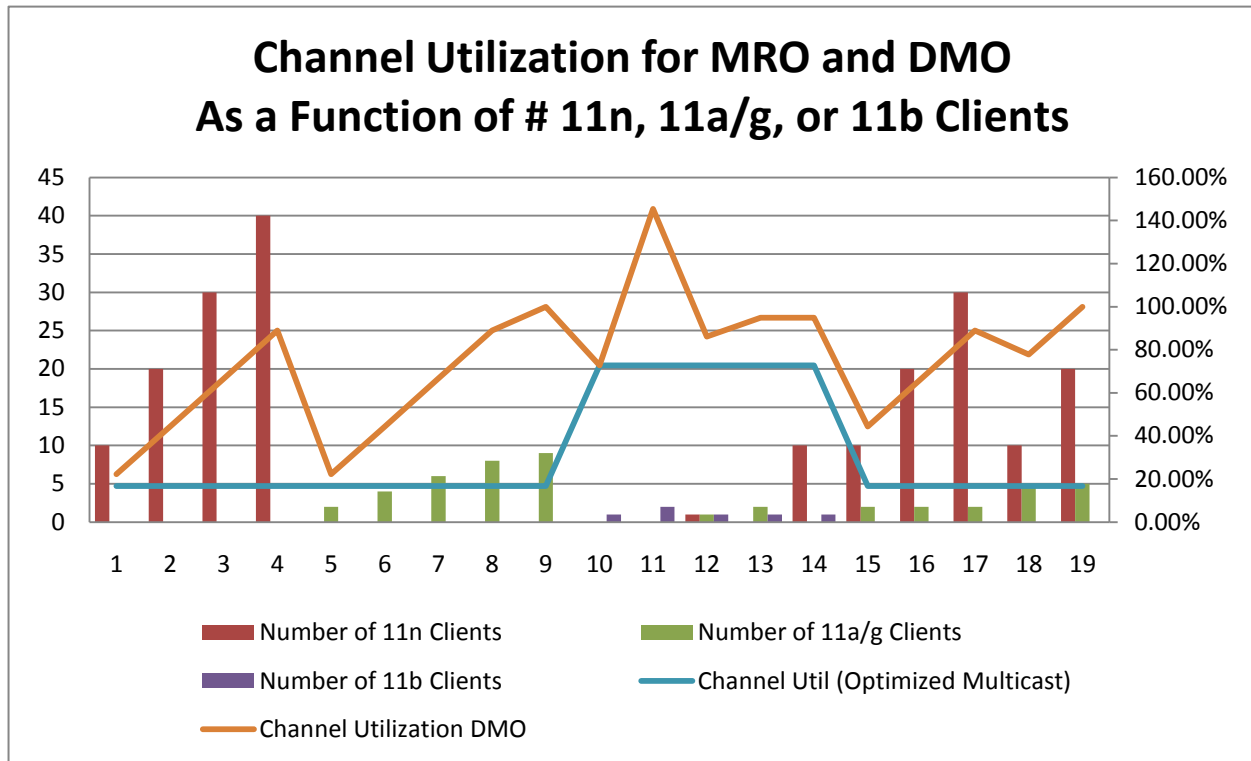
WPA Hexkey	<input type="text"/> Retype: <input type="text"/>	WPA Passphrase	<input type="text"/> Retype: <input type="text"/>
Maximum Transmit Failures	<input type="text" value="0"/>	BC/MC Rate Optimization	<input checked="" type="checkbox"/>
Strict Spectralink Voice Protocol (SVP)	<input type="checkbox"/>	802.11g Beacon Rate	default ▾
802.11a Beacon Rate	default ▾		

*Note - Since 802.11 multicast frames are not acknowledged by the receiving client, transmissions are capped at a maximum of 24 Mbps even for clients capable of higher data rate transmissions (such as 802.11n clients) to sustain reliability. This provides up to a maximum of ~9 Mbps of good quality video throughput per radio (for example 3 clients each running 3 Mbps video streams).*

### Video Scalability

The example below demonstrates the impact of DMO and MRO transport on video scalability as it relates to over-the-air channel utilization. Unicast transport is almost always optimal; however, there are use cases in which optimized multicast delivery will reduce channel utilization. This needs to be balanced against the need to assure reliable delivery and QoS. Thus unicast delivery is preferred and recommended to ensure reliable delivery and QoS for multicast video applications.

In the example below, channel utilization is estimated for MRO vs. DMO as a function of 802.11n, 802.11a/g, and 802.11b client counts. This model assumes a single 2 Mbps video stream and average rates of 180, 36, and 5.5 Mbps for 11n, 11a/g, and 11b clients respectively.



Note that in the figure above, 40 11n clients averaging 180 Mbps of PHY rate can sustain 2 Mbps video with good quality and still remain below the full channel utilization. Also, note that the channel utilization shown above is for illustration purposes only, and should never exceed 80% in practice.

To verify channel utilization, use the command “show ap debug radio-stats ap-name AP-125-2 radio 0 advanced | include Clear” and select enter. This will show the channel utilization and the resulting air time. High numbers represent high channel utilization and low numbers reflect more channel capacity is available for transmissions, with averages over the past 1, 4, and 64 seconds respectively.

```
(rfi-testbox-3600) #show ap debug radio-stats ap-name AP-125-2 radio 0 advanced | include lear
Rx Clear 1s          12
Rx Clear 4s          12
Rx Clear 64s         10
```

Aruba has tested the following configurations and recommends the following settings be used based on the size of the video streams that will be delivered:

- If the video stream bandwidth is around 500 Kbps, the threshold can be set as high as 12
- If the video stream bandwidth is > 2 Mbps then keep the threshold between 6 to 8
- For HD video (stream bandwidth > 10 Mbps) drop threshold to between 2 and 3

These values will clearly be dependent on the video stream size, the client mix, the number of unique video streams or channels, the AP density, and the reserved channel capacity (see earlier sections for instructions on reserving channel capacity for video).

### **Video Servers and Clients Tested**

The following video servers have been tested in Aruba's video solutions lab: Video Furnace, Windows Media Server with Media Encoder, and VLC. Additionally, the following client end points have been tested in this lab: Intel 5300agn, Intel 5100agn, Intel 4965agn, Intel 3945ag, Broadcom 802.11n, and Atheros 802.11n chipsets using different Windows and Mac-based operating systems.

### **Liberty University Case Study**

Liberty University has 46,000 local and distance-learning students, and more than 2,600 full time employees. The university's 802.11n network was designed anticipating the deployment of wireless IPTV, and today delivers 15 live TV channels over the wireless network. Popular channels include ABC, CBS, NBC, Fox CNN, ESPN, Liberty University Channel, and others, with 2 to 3 Mbps per channel/video stream.

Liberty University tested video performance up to 30 simultaneous users, viewing 30 different video channels on a single Access Point with good quality under favorable conditions. They deployed with a design incorporating 15 users per AP and 15 video channels, a pragmatic capacity planning decision based on their need for a mixed video and data environment.

The network includes more than 770 Aruba 802.11n AP-125s, 3 Aruba 6000 controllers with M3 blades, and 2 Aruba 3600 controllers. The controllers run Aruba's policy-enforcement firewall module for identity-based security, Quality of Service control, and traffic management. Liberty University selected HaiVision's Video Furnace system and InStream client player for secure multicast video distribution and instant access to live channels, channels delivered from disk, and video on demand.

## **A New Paradigm for Video Delivery**

As a result of 802.11n and Aruba advancements, it is now possible to enable reliable, multi-channel high definition (HD) video to fixed and mobile devices over the air. This new model not only reduces the cost structure of video delivery, but also improves accessibility to video content and interactive media.