

INSTANT AP – APP RF AND MIXED IAP CLUSTER DEPLOYMENTS

Technical Climb Webinar

10:00 GMT | 11:00 CET | 13:00 GST
Aug 9th, 2016

Presenter: Barath Srinivasan

barath.srinivasan@hpe.com

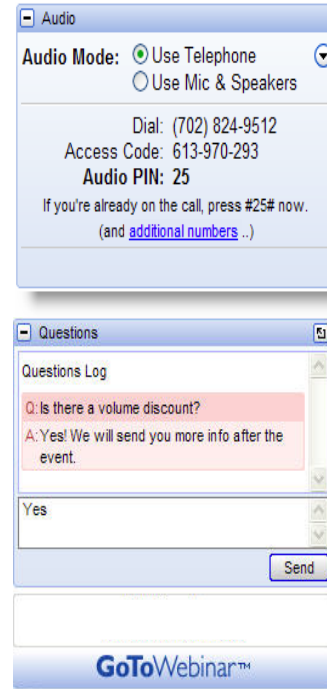


Welcome to the Technical Climb Webinar

Listen to this webinar using the **computer audio broadcasting** or dial in by phone.

The dial in number can be found in the audio panel, click **additional numbers** to view local dial in numbers.

If you experience any difficulties accessing the webinar contact us using the **questions panel**.



Housekeeping



This webinar will be recorded



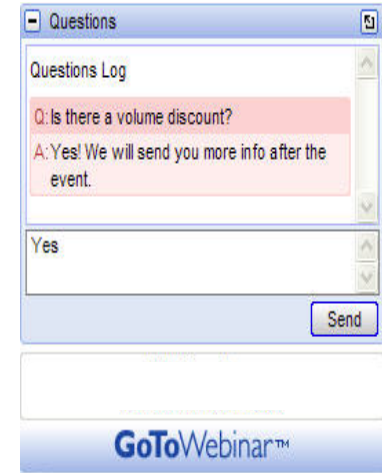
All lines will be muted during the webinar



How can you ask questions?
Use the question panel on your screen



The recorded presentation will be posted on Arubapedia for Partners (<https://arubapedia.arubanetworks.com/afp/>)



INTRODUCTION TO IAP CLUSTERS

What is clustering?

IAP's in the same VLAN will automatically find each other to form a single functioning network managed by a virtual controller. This is the basic form of the concept called clustering in Instant AP. Moving an IAP from one cluster to another requires a factory reset of the IAP.

Master

One IAP among the cluster is elected as the cluster master.

This access point is responsible for managing the respective cluster's configuration

As well as WLAN functionality.

Slave

The non-master AP's which are being a part of the cluster are called slave-IAP's.

They rely on the master IAP for obtaining the functional configuration, Regulatory domain, etc.

Things you need to know about clustering

Vital points which are considered necessary to be known while implementing cluster

Adding new AP's into an existing cluster:

When a new IAP is added into an existing cluster, it can join the cluster only if the existing cluster is running at least the minimum required version of that AP. If the existing cluster is running a version below the minimum required version of the new AP, new AP will not come up and may reboot with the reason Image sync fail. To recover from this condition, upgrade the existing cluster to at least the minimum required version of the new AP first, and add the new AP.

Things you need to know about clustering

IAP Platform	Minimum Instant Version
RAP-3WN/3WNP	6.1.3.1-3.0.0.0 or later
IAP-104	6.1.3.1-3.0.0.0 or later
IAP-175AC/175P	6.1.3.1-3.0.0.0 or later
IAP-134/135	6.1.2.3-2.0.0.0 or later
IAP-105	5.0.3.0-1.0.0.0 or later
IAP-92/93	5.0.3.0-1.0.0.0 to 6.4.2.0-4.1.1.0

Things you need to know about clustering

Handling large clusters:

It is recommend that – Networks with more than 128 APs be designed as multiple, smaller virtual-controller networks with Layer-3 mobility enabled between these networks.

Support for new hardware:

Instant 6.4.3.1-4.2.0.0 release introduces support for few new IAP devices. These new devices do not interoperate with Instant versions lower than 6.4.3.1-4.2.0.0. If these IAPs are placed into a cluster running older Instant versions such as 6.4.x.x-4.1.x.x, the devices will reboot with the Image Sync Fail reason. To resolve this issue, upgrade the existing cluster to minimum Instant 6.4.3.1-4.2.0.0 release, and then add the new IAP devices.

Things you need to know about clustering

AP Platform	Description
IAP-205H	<p>The IAP-205H is a high-performance, dual-radio wireless and wired access point for small business, hospitality, and branch deployments. This device combines high-performance wireless mobility with Gigabit wired local access to deliver secure network access to dormitories, hotel rooms, classrooms, medical clinics, and multi-tenant environments.</p> <p>The IAP-205H can be attached to a wall box using the bracket provided, or converted into a desk-mounted remote access point for branch office deployments using the AP-205H-MNTR desk mount kit. The IAP-205H is equipped with a total of four active Ethernet ports (E0-E3) and USB port .</p> <p>Multiple-Input, Multiple-Output (MIMO) technology enables the IAP-205H to provide wireless 2.4 GHz 802.11n and 5 GHz 802.11n/ac functionality, while simultaneously supporting existing 802.11a/b/g wireless services.</p>
IAP-228	<p>The IAP-228 is a fully temperature-hardened, water-resistant, indoor-rated, dual-radio IEEE 802.11ac wireless access point. This access point uses MIMO technology and other high-throughput mode techniques to deliver high-performance and 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while simultaneously supporting existing 802.11a/b/g/n wireless services.</p>
IAP-277	<p>The IAP-277 is an environmentally-hardened, outdoor-rated, dual-radio IEEE 802.11ac wireless access point. This access point uses MIMO technology and other highthroughput mode techniques to deliver high-performance and 802.11n 2.4 GHz and 802.11ac 5 GHz functionality, while simultaneously supporting existing 802.11a/b/g/n wireless services.</p>

Things you need to know about clustering

Legacy AP support in latest code:

Starting with 6.4.3.1-4.2.0.0 release, **Instant does not support IAP-92/93** devices.

Do not upgrade an IAP cluster running IAP-92/93 devices to 6.4.3.1-4.2.0.0 or later release version. In case of an accidental upgrade, the IAPs will be automatically downgraded. You can manually downgrade IAPs to an Instant 4.0 or 4.1 release, without losing the existing configuration.

Country code handling:

The Country Code window is displayed for the IAP-RW variants when you log in to the IAP UI for the first time. The *Please Specify the Country Code* drop-down list displays only the supported country codes. If the IAP cluster consists of multiple AP platforms, the country codes supported by the master IAP is displayed for all other APs in the cluster. Not applicable for US, Israel or Japan IAP's.

How does config push occur in Instant AP

Configuration change propagation across a given IAP cluster

Each command processed by the Virtual Controller is applied on all the slaves in a cluster. The changes configured in a CLI session are saved in the CLI context. The CLI does not support the configuration data exceeding the 4K buffer size in a CLI session. Therefore, Aruba recommends that you configure fewer changes at a time and apply the changes at regular intervals.

To apply and save the configuration changes at regular intervals, use the following command in the privileged mode:

```
(Instant AP)# commit apply
```

To apply the configuration changes to the cluster without saving the configuration, use the following command in the privileged mode:

```
(Instant AP)# commit apply no-save
```

To view the changes that are yet to be applied, use the following command in the privileged mode:

```
(Instant AP)# show uncommitted-config
```

To revert to the earlier configuration, use the following command in the privileged mode.

```
(Instant AP)# commit revert
```

Zone settings on an IAP

Configuring IAP Zones

All APs in a cluster use the same SSID configuration including master and slave IAPs. However, if you want to assign an SSID to a specific IAP, you can configure zone settings for an IAP.

Points to remember:

- An IAP can belong to only one zone and only one zone can be configured on an SSID.
- If an SSID belongs to a zone, all IAPs in this zone can broadcast this SSID. If no IAP belongs to the zone configured on the SSID, the SSID is not broadcast.
- If an SSID does not belong to any zone, all IAPs can broadcast this SSID.

In the Instant UI:

- On the *Access Points* tab, click the IAP for which you want to set the zone. The *edit* link is displayed.
- Click the *edit* link. The edit window for modifying IAP details is displayed.
- Specify the AP zone in *Zone*.
- Click *OK*.

AppRF - Deep packet inspection

What is DPI? Why is this significant?

AppRF is Aruba's custom built Layer 7 firewall capability. It consists of an on-board deep packet inspection and a cloud-based Web Policy Enforcement service that allows creating firewall policies based on types of application.

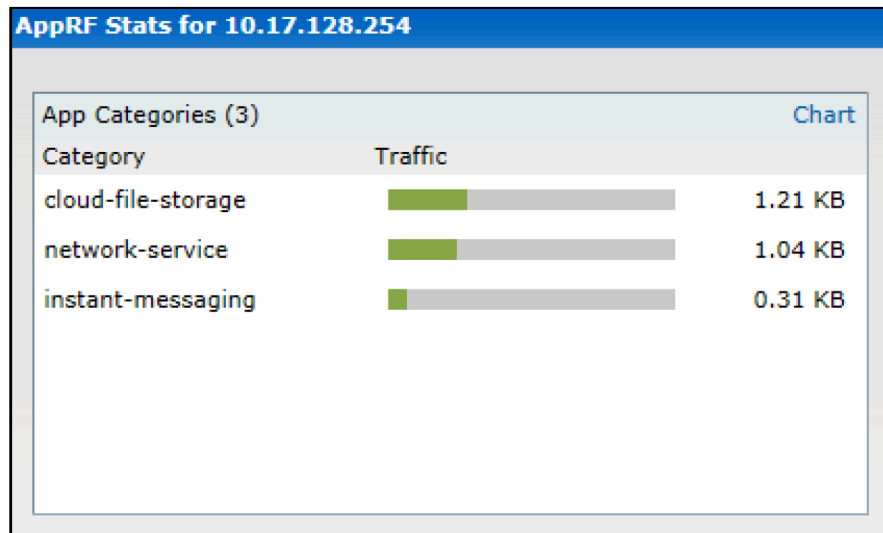
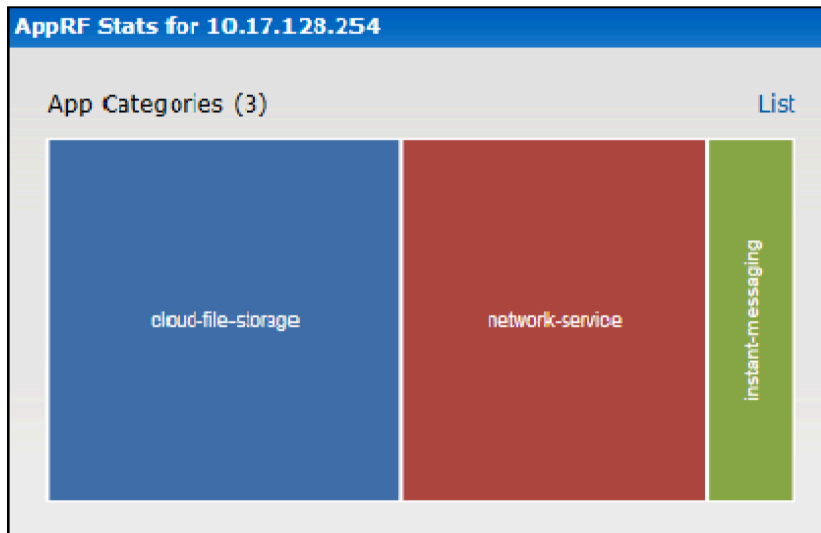
IAPs with DPI capability analyze data packets to identify applications in use and allow you to create access rules to determine client access to applications, application categories, web categories and website URLs based on security ratings. You can also define traffic shaping policies such as bandwidth control and QoS per application for client roles. For example, you can block bandwidth monopolizing applications on a guest role within an enterprise.

In the Instant UI:

- Navigate to *System >General*
- Select Enabled from the *AppRF visibility* drop-down
- Click *OK*

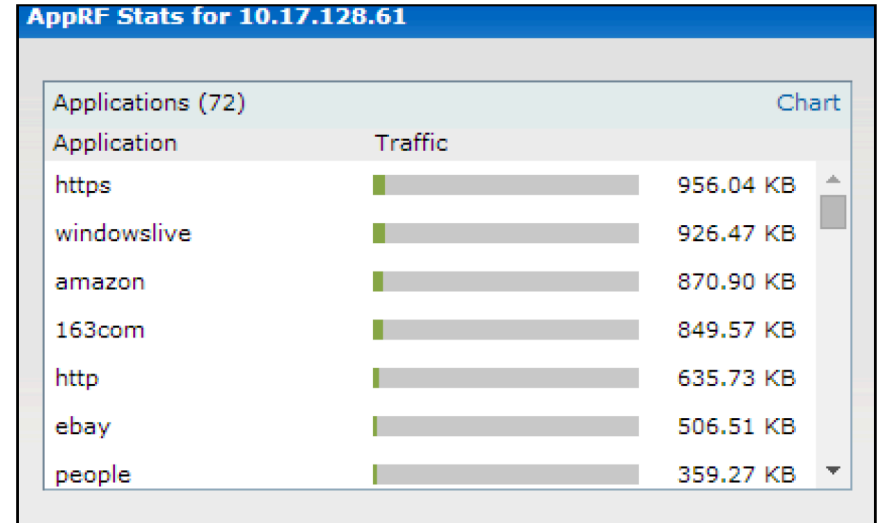
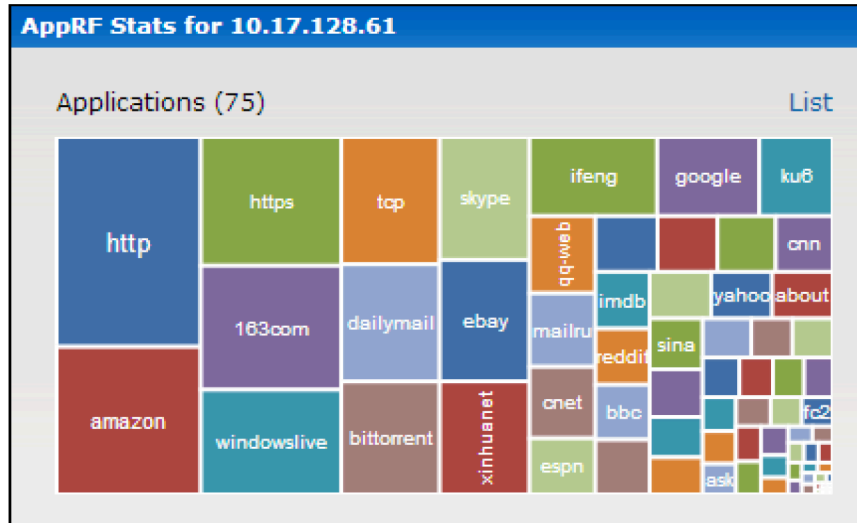
AppRF – Application Categories

The application category chart displays details on the client traffic towards the application categories. On clicking in the rectangle area, you can view the relevant graphs and toggle between the chart and list views.



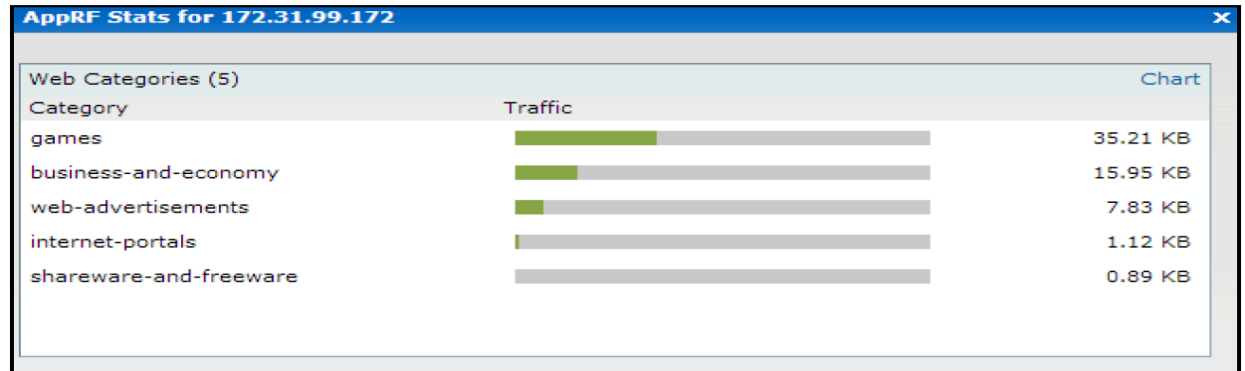
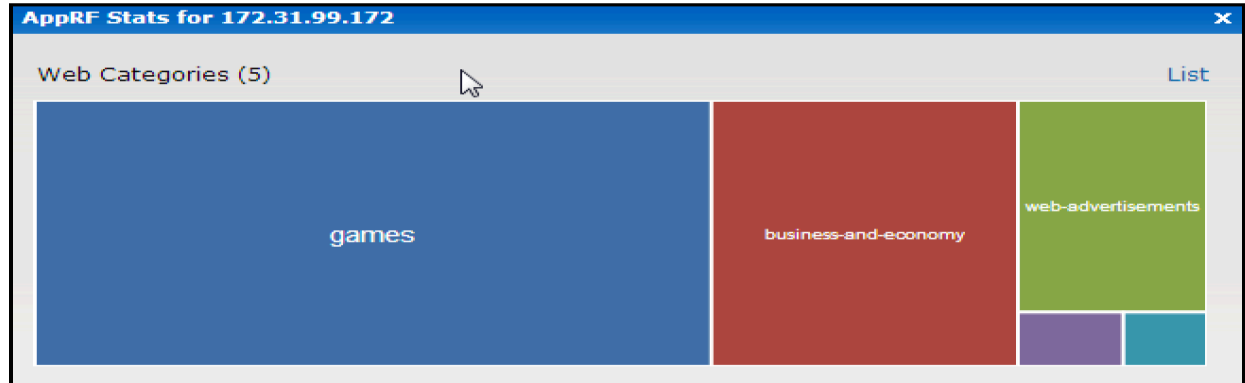
AppRF – Application charts (Client)

The application chart displays details on the client traffic towards the applications.



AppRF – Web Categories

The web categories chart displays details about the client traffic to the web categories.



Mixed IAP Clustering + AppRF

Things to note:

- If you mix an IAP-9x in with any other model the cluster will be limited to the lowest common denominator which is the IAP-9x such that the cluster size max is 16
- AppRF is not fully supported on earlier models of IAPs including the IAP-105 but is fully supported on the newer models like the IAP-225
- While performing mixed clustering, ensure that the Low capacity AP as well as the high capacity AP are using the same firmware and the hardware supports the said firmware as well.

Mixed IAP Clustering + AppRF

In IAP FW v4.1 - AppRF will be the only feature in 4.1 that imposes limits on the older IAP models. All other features will work across all models. AppRF is composed of two functions: native Deep Packet Inspection (DPI) and web-classification / categorization.

For mixed-class deployments (web-filtering-only-supported-aps with full-AppRF-supported-aps) works as follows:

1. Each ap visualizes and enforces the traffic per capability.
 - Implies, if app-classification rules are configured on a ap-105, it will be considered a NO-OP. as if that rule does NOT exist
 - But, at the same time, the same app-classification rules will be enforced in the ap-225.
2. For visualization, it is per-ap. You have to click on a AP or client to see the app-rf charts.
 - So, in ap-105, the AppRF will ONLY have 2 graphs – the web-category and web-reputation
 - In ap-225, all the 4 charts will be shown.

QUESTIONS

Any Questions?

THANK YOU!

Bonus! – Best practices

Try these tips and tricks if you're facing any issues in your IAP cluster:

- Keep Wired and Wireless(clients) on separated vlans. Do not mix wired clients and wired clients in the same vlans.
- Enable Broadcast filter if you are able to, one of the biggest issues on the wireless network is the broadcast.
- Enable Broadcast Filter ARP
- Enable Dynamic Multicast Optimization
- Enable AirGroup (for environments where there are many iOS devices)
- Protect wired port of IAP using firewall rules to prevent someone from assigning DHCP IPs to clients by connecting a rogue DHCP server into the wired port.
- Set any ACLs to classify Lync/Facetime or any other high priority traffic and disable scanning for the same.
- Try not using UNII-I band
- If you can pick an IAP-135 to take advantage of the higher CPU capability
- use a dedicated IAP mgmt vlan for the VC
- Alter the user limit in the ssid to 64
- Set the local probe request threshold to 20dBm
- Enable fair access
- Use VLAN pooling

THANK YOU FOR ATTENDING THE SESSION!

(Really this time, no kidding!)