aruba
a Hewlett Packard Enterprise company

ARUBA OS – UNDERSTANDING CONTROL PLANE SECURITY FEATURE

Technical Climb Webinar

10:00 GMT | 11:00 CET | 13:00 GST
Sep 27th, 2016

Presenter: Barath Srinivasan

barath.srinivasan@hpe.com

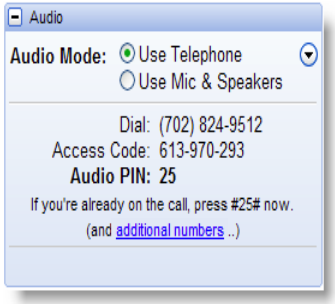
AIRHEADS COMMUNITY

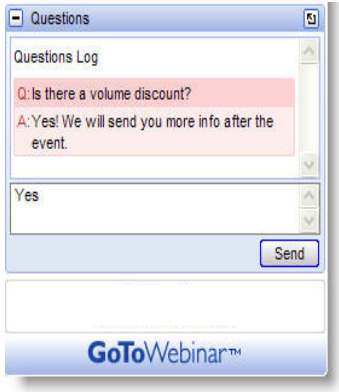
Welcome to the Technical Climb Webinar

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.



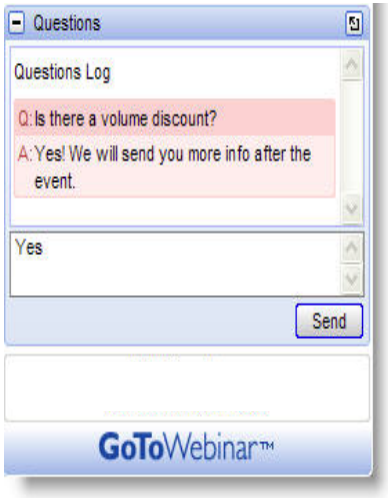


Housekeeping

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 CONTROL PLANE SECURITY (CPSEC)

aruba
a Hewlett Packard Enterprise company

What is cpsec?

Aruba OS supports a secure form (IPsec) of communication between the mobility controller and AP in order to protect the control plane communications. This is performed by means of using public-key self-signed certificates created by each master controller.

Role of Master:

If the master controller hosts any local controllers, it sends the certificate to the local controllers or any AP's which are terminating directly on the master controller.

Role of Local:

Using the certificate obtained from the Master, the local controller will be able to certify the AP's terminating on the corresponding controller. In the event, that a local controller is unable to communicate with the Master controller (and if control plane security is enabled), it will be unable to certify the AP's, until the master-local communication is restored.

Things you need to know about cpsec

Vital points which are considered necessary to be known prior to implementing cpsec

- It is ideal to enable cpsec while performing the initial controller setup
- The ArubaOS initial setup wizard enables cpsec by default
- Ensure that there is proper communication between master-local controllers prior to provisioning AP
- AP models from AP-105 & AP-12x and above have factory-installed digital certificates from Aruba Networks Inc. and do not need a certificate downloaded from the master controller
- Once a campus AP is certified, it can failover among any local and remain connected to the secure network, as the trust anchor is the master controller
- The campus AP whitelist contains a list of all AP's connected to the network
- The whitelist can be used to add new AP's to the network or revoke any AP suspected as Rogue or unauthorized AP within the campus network.

Things you need to know about cpsec

Vital points which are considered necessary to be known prior to implementing cpsec

- When the controller sends the AP a certificate, the AP will need to reboot, before it can begin secure channel communications with the controller

- If you are running a campus network with a large number of controllers and AP's – it is pivotal to note that the network will experience several minutes of interrupted connectivity while the AP's obtain the digital certificate and reboot

- Control plane security feature has been designed to support campus AP's **only**, It is not intended for use with Remote AP's. Please do not attempt to use cpsec with any RAP devices.

CPSEC – An Overview

- Controller will send certificate only to those AP's that you have identified as Valid AP's on the network
- The valid AP list can be generated on the controller automatically or manually by means of adding AP's to the campus-ap-whitelist
- The initial setup wizard can be used to configure automatic certificate provisioning or the certificate can be sent to all AP's within a specific range of IP Addresses
- The default option that comes up during the setup is to manually enter the campus AP details into the whitelist for certification
- This can be changed to automatic, where every AP that contacts the controller will be automatically provided a certificate from the master controller, Go for this option only if you are sure that there is no unauthorised AP's on the network
- The certificates can also be issued to AP's within an IP range – However, even if a valid campus AP exists outside the IP range, it will not be provided a certificate from the controller.

Control Plane Security - Configuration

Initial setup

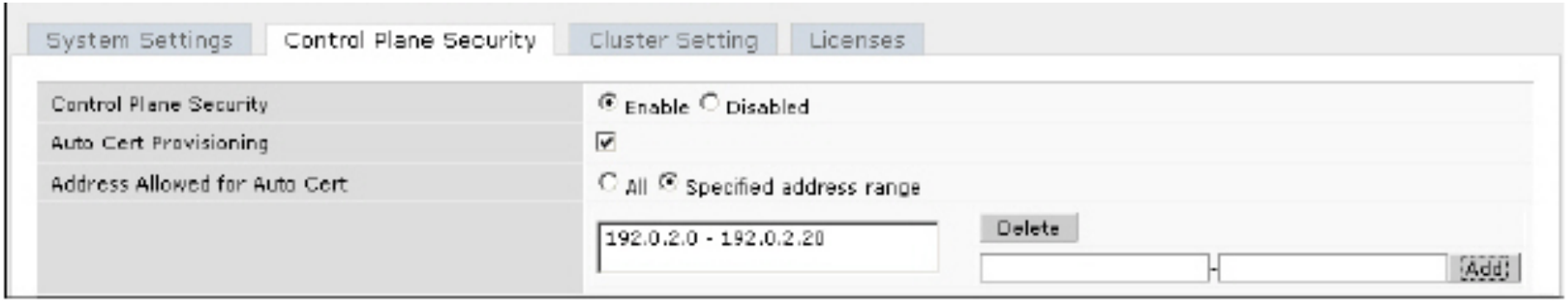
While deploying a controller running ArubaOS 6.0 or later, using the initial setup wizard, cpsec configurations are recommended to be performed. These settings can be changed in an existing network as well, via the WebUI or CLI.

In the WebUI:

- Access the webUI and goto **Configuration > Controller**
- Select the **Control Plane Security** tab
- Configure these parameters –

  - Control Plane Security – Select **Enable**
  - Auto Cert Provisioning – If you prefer for the controller to automatically issue certificates to the campus connected AP's, **Enable** this option (if not, the AP whitelist needs to be populated manually).
  - Auto Cert Allow All – If you have enabled cpsec & Auto cert provisioning, **Enable** this option to provide certificate to ALL of the existing campus connected AP's.
  - Addresses Allowed for Auto Cert – If you choose to allow only a range of AP's IP to be provided controller cert, instead of allowing ALL campus connected AP's, then **Enable** this option and **Add** IP range.

Control Plane Security - Configuration



NOTE:

Once all campus connected AP's have obtained a certificate and have started operations, remember to disable the "Auto Cert Provisioning" configuration – in order to prevent any Rogue AP's from being able to access the secure network at a later stage.

How to Manage Campus AP Whitelist

After the campus AP's connect to the controller once it is provisioned via automatic certificate provisioning, the AP's connect to the controller using the secure tunnel. Any AP's that are not approved or certified on the network will be included in the campus AP whitelist along with the valid AP's and these uncertified AP's will appear in an **unapproved** state.

To Manually add AP's to the campus AP whitelist:

- Access the WebUI and goto **Configuration > AP Installation**
- Click **Campus AP Whitelist** tab
- To add a new AP to the whitelist, click **New**
- Define these parameters for each campus AP you want to add to the campus AP whitelist

    - AP MAC Address – Enter the MAC address of the AP which is to be added to the secure network
    - Description – Write a brief description about the AP (such as BLDG1-FL2-AP4)
    - Click **Add** to add the AP to the Campus AP Whitelist and **Apply** the changes

How to Manage Campus AP Whitelist

Once an entry is added to the whitelist, that entry will be updated by the controller with additional information as the status of the AP changes. In order to view the latest status of the AP whitelist, use the following steps:

- Access the WebUI, goto **Configuration > AP Installation**
- Click the **Campus AP Whitelist** tab an you will be presented with the information below,

AP MAC Address – MAC address of the campus AP

Cert Type – Type of certificate used by the AP (switch-cert or Factory-cert)

State – Current state of the AP as it goes thru the process of getting getting certified by the controller

Description – Used to identify the specific AP

Revoked – Mentions whether an AP's secure status has been revoked or not

Revoked Text – Reason for why the AP's status has been revoked

How to Manage Campus AP Whitelist

Campus AP Whitelist state conditions and their meaning:

unapproved-no-cert:
AP has no certificate and is not approved.

unapproved-factory-cert:
AP has a preinstalled certificate that was not approved.

approved-ready-for-cert:
The AP has been approved as a valid campus AP and is ready to receive a certificate.

certified-factory-cert:
The AP is already has a factory certificate. If an AP has the f**actory-cert** certificate type and is in the **certified-factory-cert** state, then that campus AP will not be re-issued a new certificate if automatic certificate provisioning is enabled.

How to Manage Campus AP Whitelist

certified-switch-cert:
AP has an approved certificate from the controller.

certified-hold-factory-cert:
An AP is put in this state when the controller thinks the AP has been certified with a factory certificate yet the AP requests to be certified again. Since this is not a normal condition, the AP will not be approved as a secure AP until a network administrator manually changes the status of the AP to verify that it is not compromised.

Certified-hold-switch-cert:
An AP is put in this state when the controller thinks the AP has been certified with a controller certificate yet the AP requests to be certified again. Since this is not a normal condition, the AP will not be approved as a secure AP until a network administrator manually changes the status of the AP to verify that it is not compromised.

Modifying an AP in the Campus AP Whitelist

Use these steps to modify a whitelist entry parameter which was mentioned in the previous slides:

- Access the master controller UI and goto **Configuration > AP Installation**
- Click the **Campus AP Whitelist** tab
- Select the checkbox by the entry for the AP you want to edit, then click **Modify**

  Cert-type:
  Type of certificate used by the AP, whether switch-cert or Factory-cert

  State:
  Can be changed between approved-ready-for-cert or certified-factory-cert

  Revoke:
  Toggling this check box will allow you to revoke an AP and mention a brief comment as reason

  Once done, Click **Update** to update the whitelist with the new settings

Note: A campus AP whitelist entry can also be deleted by selecting the corresponding whitelist entry and clicking the **Delete** button.

Modifying an AP in the Campus AP Whitelist

Purging the Campus AP Whitelist:

Before adding any local controller to the campus connected network it is best practice to purge the Campus AP Whitelist on it. If not, any residue entry for Campus AP Whitelist on this controller will be merged with the other valid entries which exists on the master controller which is part of the active cluster.

To Purge the Campus AP Whitelist:

Access the master controller WebUI and navigate to **Configuration > AP Installation**

Click the **Campus AP Whitelist** tab

Click **Purge**

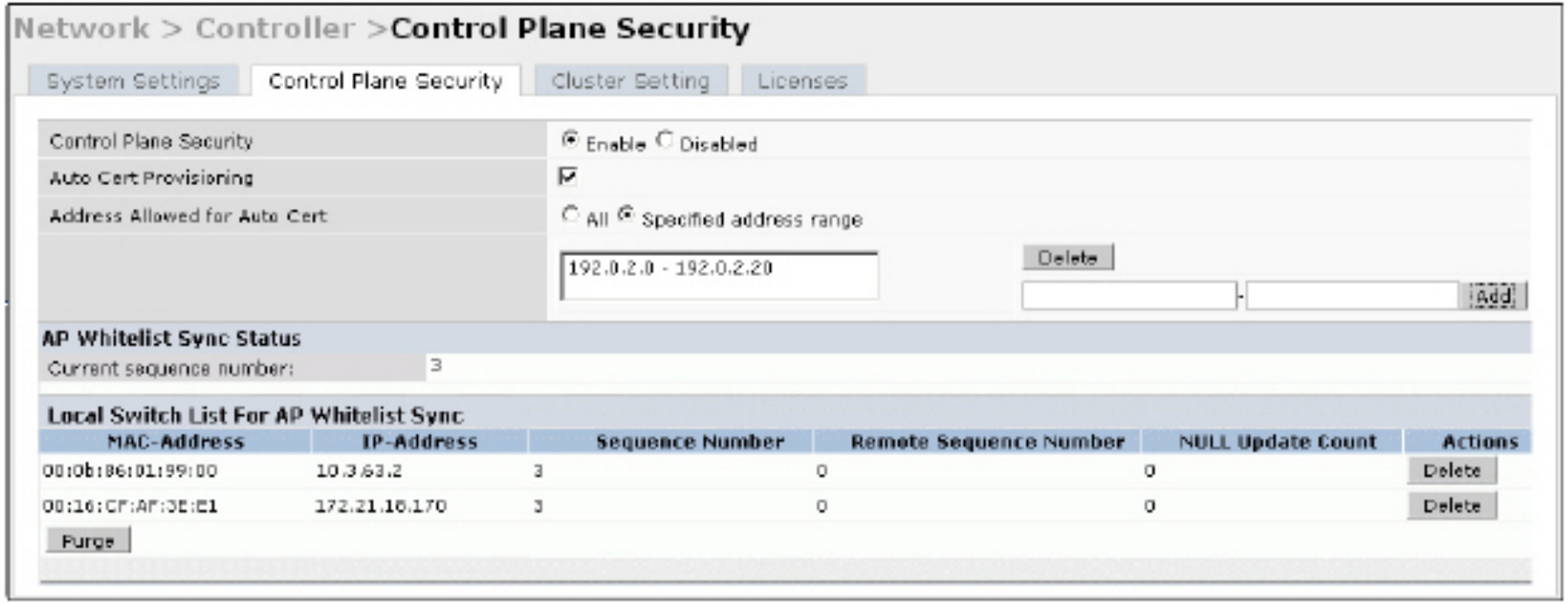
Campus AP Whitelist Synchronization

Every controller using cpsec feature maintains a Campus AP Whitelist, a local switch whitelist and a master switch whitelist.

The contents of these whitelists vary, depending upon the role of the controller.

Controller Role	Campus AP Whitelist	Master Switch Whitelist	Local Switch Whitelist
On a (standalone) master controllerwith no local controllers:	The campus AP whitelist contains entries for the secure campus APs associated with that controller.	The master switch whitelist is empty, and does not appear in the WebUI.	The local switch whitelist is empty, and does not appear in the WebUI.
On a master controllerwith local controllers:	The campus AP whitelist contains an entry for every secure campus AP on the network, regardless of the controllerto which it is connected.	The master switch whitelist is empty, and does not appear in the WebUI.	The local switch whitelist contains an entry for each associated local controller.
On a Local controller:	The campus AP whitelist contains an entry for every secure campus AP on the network, regardless of the controllerto which it is connected.	The master switch whitelist contains the MAC and IP address of the master controller.	The local switch whitelist is empty, and does not appear in the WebUI.

Campus AP Whitelist Synchronization

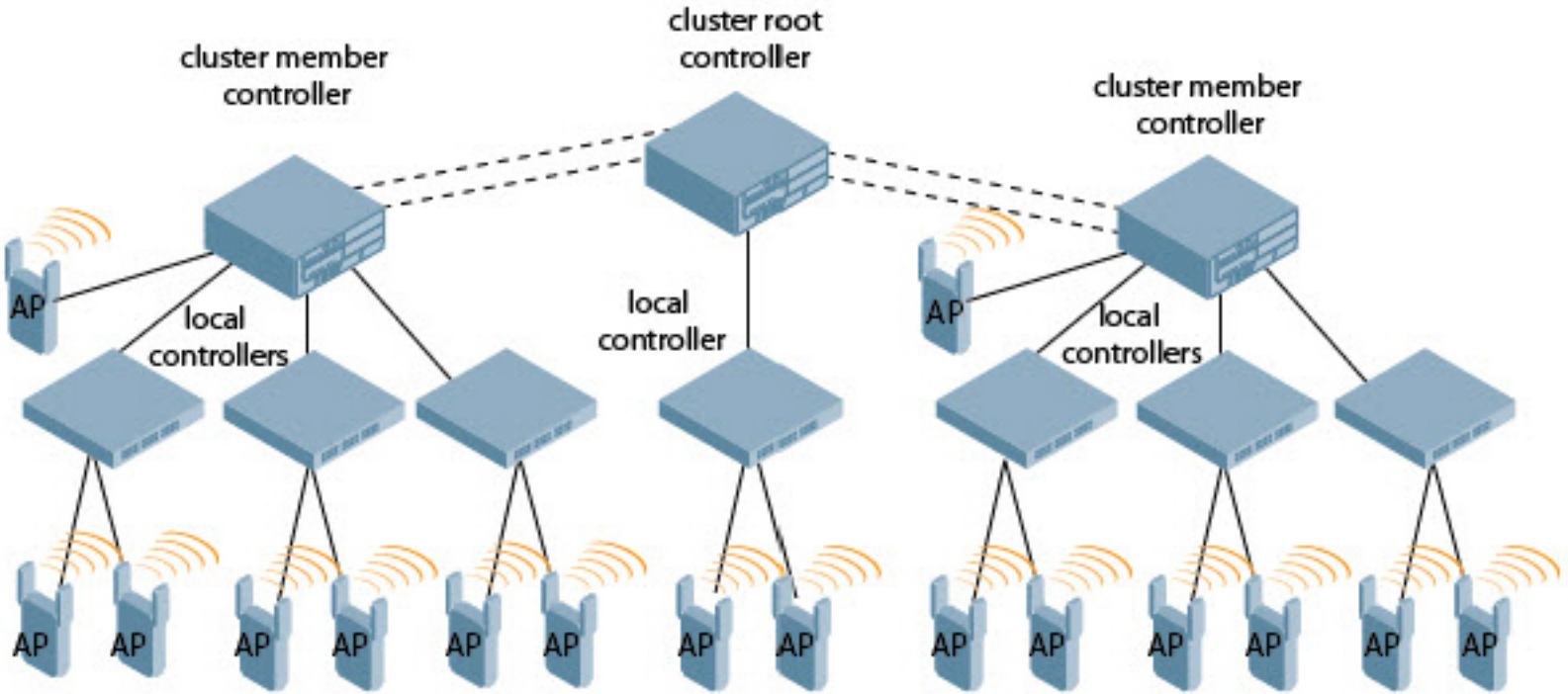


Campus AP Whitelist Synchronization

Synchronization: Points to Remember

- The current sequence number shows the number of changes made to the campus AP whitelist on that controller
- By default, each controller compares its whitelist against whitelist on other controller every 2 minutes
- If a controller detects changes, it will send the changes to the corresponding controller.
- If there is a difference in sequence number, it signals that the controller may b sending/awaiting whitelist change
- Null Update Count shows the number of times the controller checked its campus AP whitelist and found nothing to synchronize. If a null update count reaches 5, the controller will send an “empty sync” heartbeat to the remote controller to ensure that the sequence numbers on both controllers are the same and reset the null update count to zero

Environments with Multiple Master Controllers



Environments with Multiple Master Controllers

If the network includes multiple master controller with their own hierarchy of AP's and controllers,
You can allow AP's from one hierarchy to failover to any other hierarchy by defining a cluster of master controllers.

Each cluster will have a cluster root and all other master controller as cluster members. The cluster root will create a self-signed certificate and propagate it to its own local's and AP's as well as send it across to the cluster members.

Since AP's across all masters are certified using the same trust anchor, the AP's can switch to any other controller within the cluster and remain securely connected to the network.

Note: How to create controller cluster is beyond the scope of this CPSEC session. A link with the complete step-by-step configuration detail (techdoc) is provided in the slide notes below, you can use it for further learning/reference.

TROUBLESHOOTING

aruba
a Hewlett Packard
Enterprise company

Certificate Problems

If an AP has a problem with its certificate, check the state of the AP in the campus AP whitelist. If the AP is in either the **certified-hold-factory-cert** or **certified-hold-switch-cert** states, you may need to manually change the status of that AP before it can be certified.

An AP is put in this state when the controller thinks that the AP has been certified, yet the AP requests to be certified again. As this is abnormal activity, the AP will not be approved as a secure AP until a network administrator manually changes the status of the AP to verify that this is not a compromised AP.

If the network is experiencing connectivity issues, then the AP will recover out of this state as soon as the connectivity is restored.

Verifying Certificates

If you are unable to configure the control plane security feature on Aruba M3, 600 or 3000 series controllers, verify that its Trusted Platform Module (TPM) and factory-installed certificates are present and valid by accessing the controller's CLI interface and issuing the command "show tpm cert-info". If the controller has a valid certificate, the output of the command should appear as below,

```
(host) # show tpm cert-info
subject= /CN=AC1234567::00:0b:86:11:22:33
issuer= /DC=com/DC=companyname/DC=ca3/CN=DEVICE-CA3
serial=5147D5BC00000000000C
notBefore=Aug 29 22:16:12 2009 GMT
notAfter=Aug 18 22:16:12 2029 GMT
```

Verifying Certificates

If the certificate is corrupted or missing TPM and factory certificates, Contact Aruba Technical Support

```
(host) # show tpm cert-info
Cannot get TPM and Factory Certificate Info.
TPM and/or Factory Certificates might be missing.
```

Disabling Control Plane Security

- If you disable cpsec on a standalone or local controller, all AP's connected to that controller will then reboot and then reconnect to the controller over clear channel
- If you disable cpsec on a master controller, AP's directly connected to the master will reboot and then reconnect to the master controller over clear channel.
- AP's connected to its local controller will continue to communicate over a secure channel until the configuration is saved on the master controller. Once this is done, the AP's on local will also reboot and reconnect to the local controllers over a clear channel.

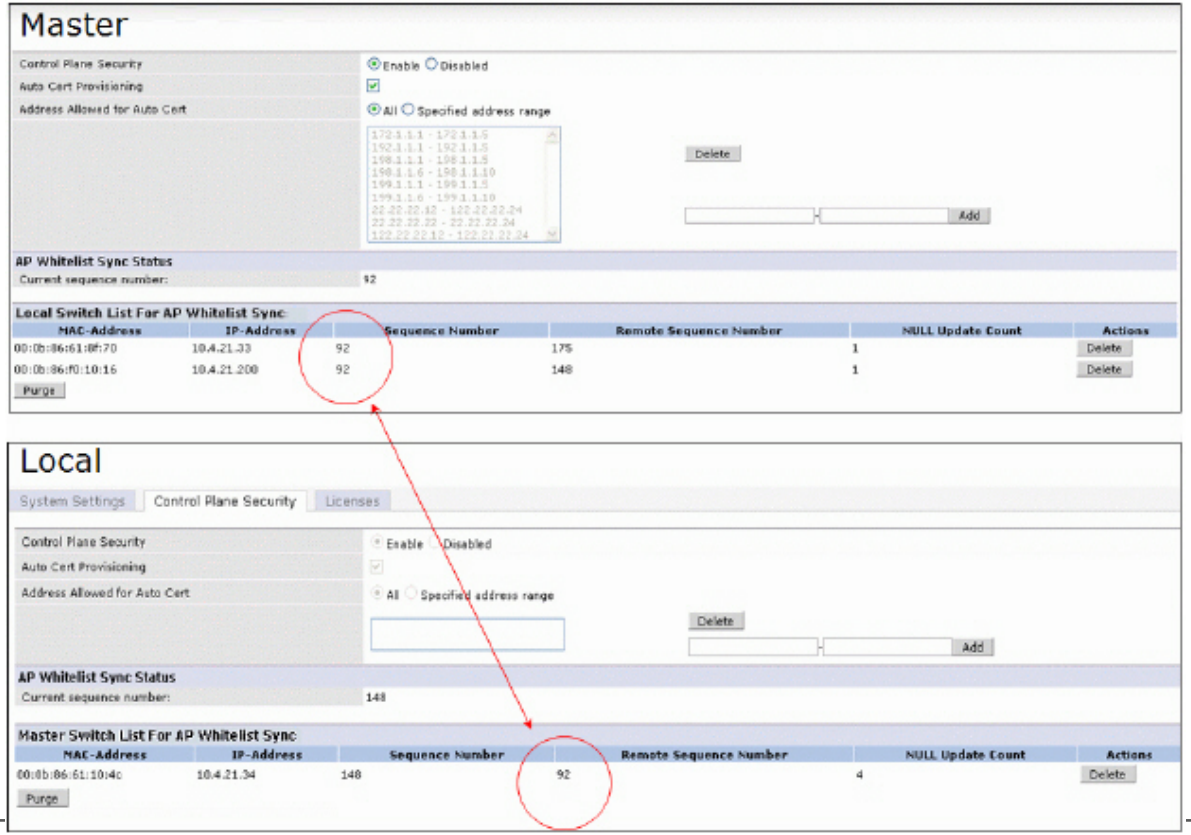
Verify Whitelist Synchronization

To verify that a network of master and local controllers are correctly sharing their campus AP whitelists, check the sequence numbers on the master and local switch whitelists

- The sequence number value on a master controller should be the same as the remote sequence number of the local controller
- The sequence number on a local controller should be same as the remote sequence number on the master

NOTE: whitelist table sync occurs once every two minutes, so the sync might not happen immediately.

Verify Whitelist Synchronization



QUESTIONS

Any Questions?

aruba
a Hewlett Packard
Enterprise company

THANK YOU!

aruba
a Hewlett Packard
Enterprise company