TECHNICAL WHITEPAPER

Zero-Touch Provisioning for AOS-Switch

Version 16.08

aruba
a Hewlett Packard Enterprise company

CONTENTS

OVERVIEW

The ArubaOS-Switch software platform provides three primary methods to automatically provision Aruba switches with predefined configuration and software images — TFTP automatic download, AirWave, and Central. This document provides setup instructions, best practices, and troubleshooting guidelines for utilizing zero-touch provisioning on ArubaOS-Switches.

Zero touch provisioning (ZTP) is a switch feature that allow the devices to be provisioned and configured automatically, eliminating most of the manual labor involved with adding them to a network. ZTP allows the hardware to be installed directly into the environment and for that act to be the last hands-on moment. When it is powered on, and gains network connectivity, the switch will send out a request through DHCP (Dynamic Host Configuration Protocol) or TFTP (Trivial File Transfer Protocol) to get the location of its centrally stored image and configuration, which it downloads and installs.

The objectives of this document is to demonstrate Aruba's various ZTP solutions that enables the auto-configuration of Aruba switches (from a factory default configuration) without requiring any administrator's intervention at the switch level. The switches can use DHCP server options to provide the relevant info for successful provisioning via a TFTP server or Aruba's AirWave management platform. A third option, Aruba Central, a cloud-based management platform, allows switches to reach out to the Aruba Central servers when in a factory default state, subsequently managed by Central.

Aruba Zero Touch Provisioning Compatibility

Platform	Standalone	Backplane Stacking	Virtual Switching Framework
AirWave			
Aruba 5400R	Yes	N/A	Yes
Aruba 3810M	Yes	Yes	N/A
Aruba 2930M	Yes	Yes	N/A
Aruba 2930F	Yes	N/A	Yes
Aruba 2540	Yes	N/A	N/A
Aruba 2530	Yes	N/A	N/A
Central			
Aruba 5400R	Yes	N/A	Yes
Aruba 3810M	Yes	Yes	No
Aruba 2930M	Yes	Yes	No
Aruba 2930F	Yes	N/A	Yes
Aruba 2540	Yes	No	No
Aruba 2530	Yes	No	No
TFTP via DHCP			
Aruba 5400R	Yes	Yes	Yes
Aruba 3810M	Yes	Yes	Yes

Platform	Standalone	Backplane Stacking	Virtual Switching Framework
TFTP via DHCP			
Aruba 2930M	Yes	Yes	Yes
Aruba 2930F	Yes	Yes	Yes
Aruba 2540	Yes	Yes	Yes
Aruba 2530	Yes	Yes	Yes

ZTP VIA ARUBA AIRWAVE

The main goal of ZTP is that when a switch, in its initial configuration, boots up, it will perform a DHCP request on its default VLAN (VLAN-1) and then uses DHCP response to discover AirWave. The switch then contacts AirWave and gets its configuration.

The AirWave details received from the DHCP options are stored in the switch configuration. This assures that the configuration is retained even after the switch is rebooted. This section discusses the various configuration and steps required in setting up ZTP in details.

DHCP server configuration

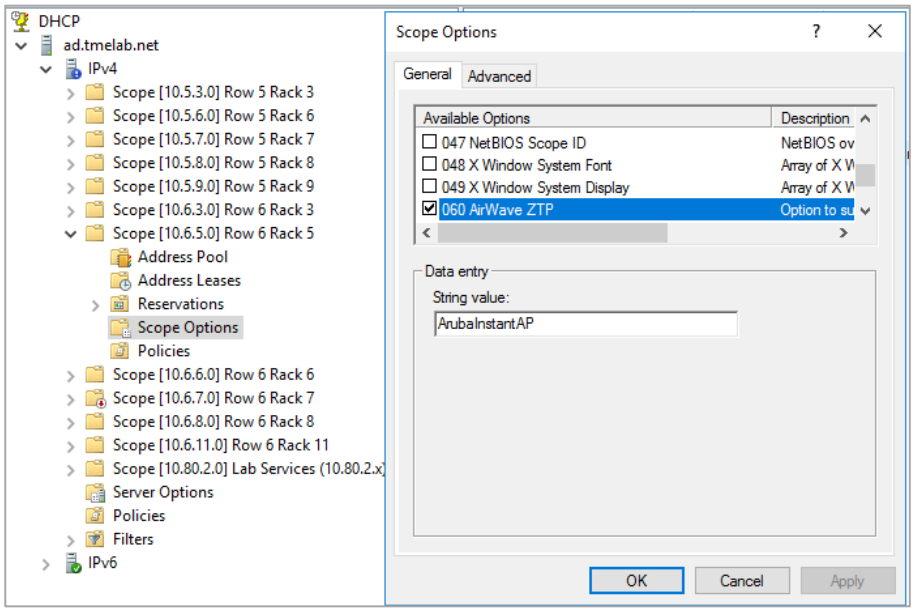
The switch will receive AirWave information via DHCP options 43 and 60. Option 43 can provide AirWave details in two ways:

- Provide AirWave details in Sub option 146 - For Traditional DHCP ZTP Deployments
- Provide AirWave details directly in option 43 in conjunction with option 60 (with Value " ArubaInstantAP") - For deployments where Aruba APs are involved

The presence of option 60 with the value "ArubaInstantAP" helps the Aruba switch to decide how to read Option 43. If Option 60 is not provided, or sent with a different value, the switch will try to look for sub option146 with AirWave details. If AirWave details are not found, the switch will try to reach out to Aruba Activate. Option 60 is included in the initial DHCP discover message that a DHCP client broadcasts in search of an IP address. Option 60 is used by DHCP clients in order to identify itself to the DHCP server.

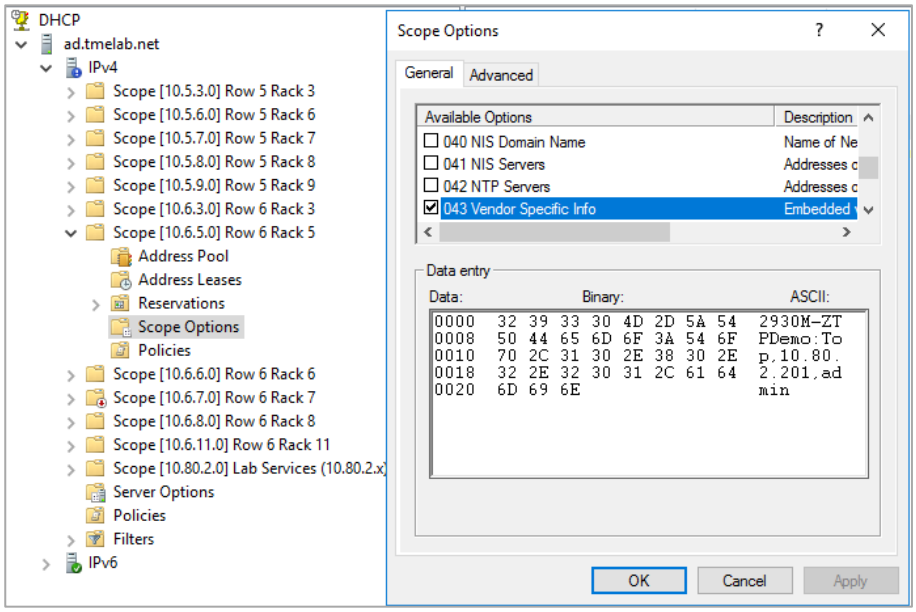
In the following example, the DHCP server needs to be configured to provide the correct information back to new Aruba switches. The following is the procedure to configure:

- First, the DHCP Option 60 string needs to be defined in the scope options of the DHCP server, for this example, Windows Server 2016 is being used.



- Then, DHCP option 43, needs to be configured, which points to the AirWave server in the following format:

```
<Group>:<Topfolder>,<AMP IP>,<shared secret>
LAN switches:Branch1,192.168.1.15,aruba123
```



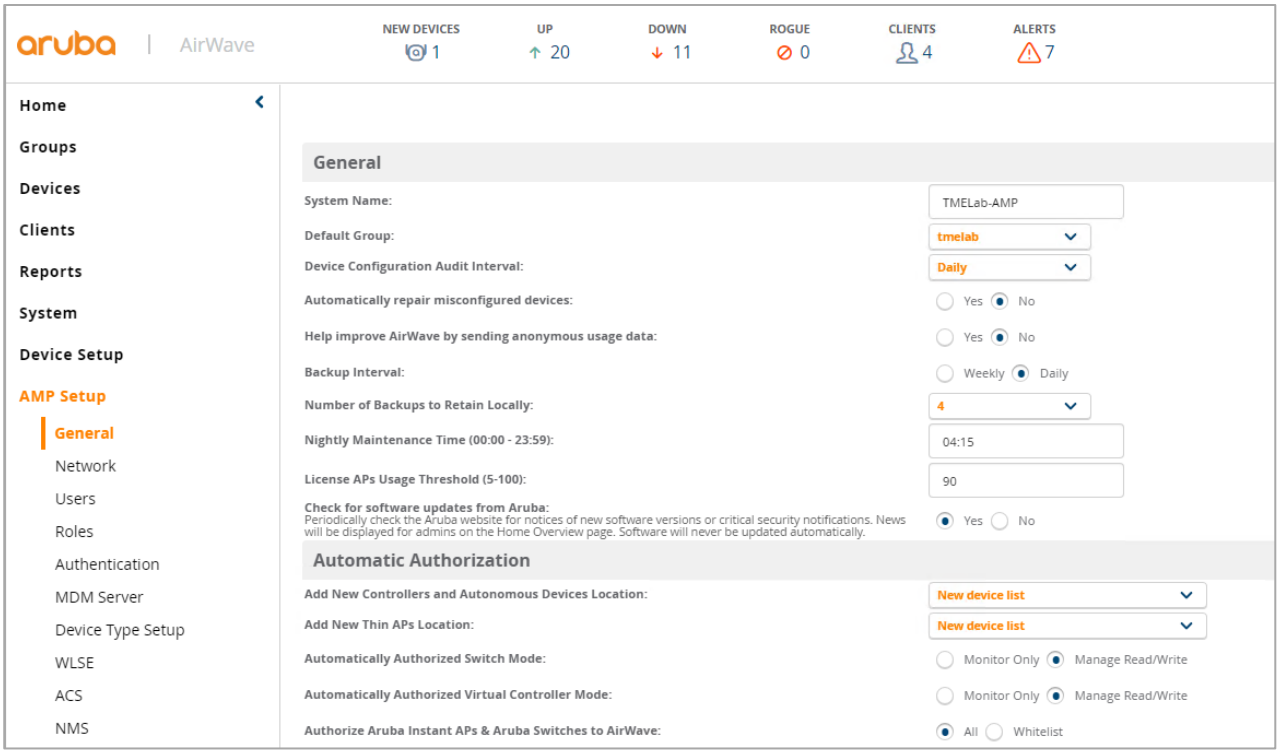
Workflow

The provisioning workflow is as follows:

- The switch boots up with a factory default configuration.
- The switch sends out a DHCP discovery from the primary VLAN interface.
- The switch will expect DHCP option 60 with the configured string value “ArubaInstantAP” along with DHCP option 43 to parse AirWave details.
- After the AirWave details are verified and configured, the switch initiates the HTTPS connection to the AirWave server.
- After a successful registration, AirWave can then monitor, configure, and troubleshoot the switches.

If the DHCP options are not configured for AirWave, the switch is left in its default state for manual configuration.

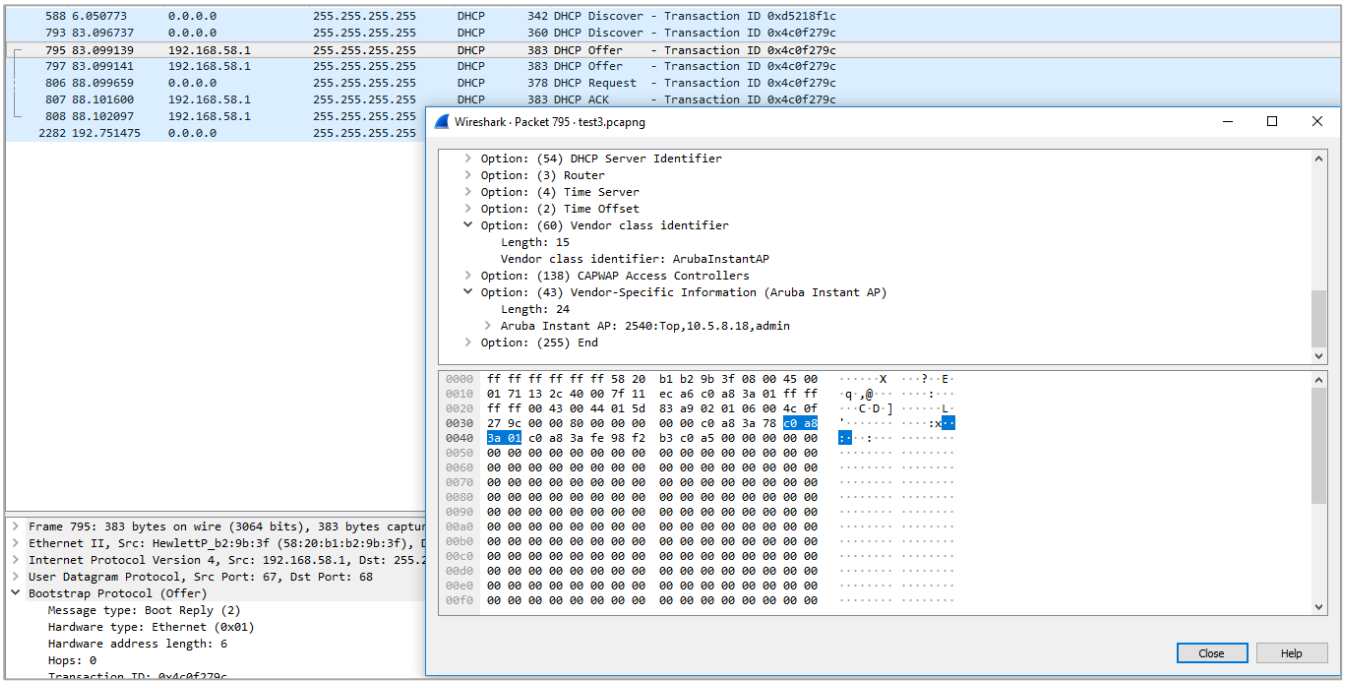
In AirWave, select **AMP Setup > General > Automatic Authorization**, automatically authorized switch mode should be set to “*Managed Read/Write*” and switch whitelisting should be set to “*All*”. This is the default setting for AirWave.



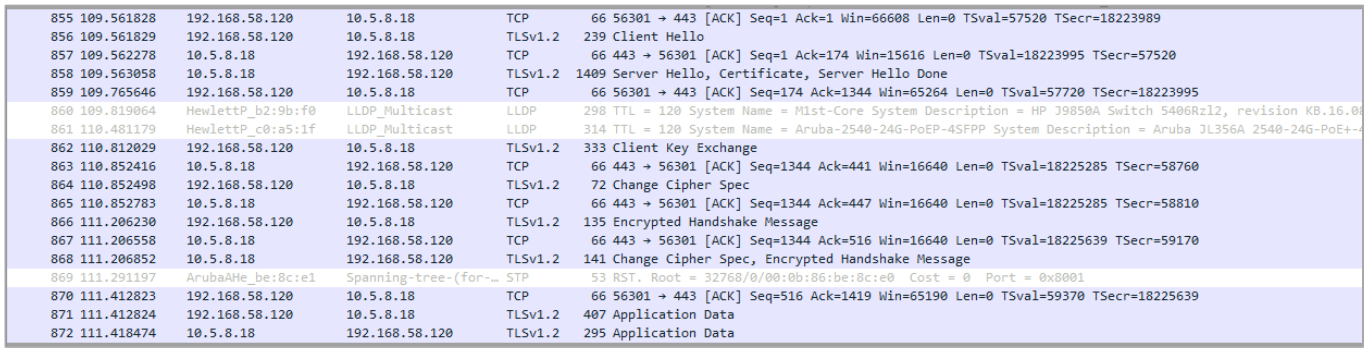
Once the switch connects to the network, it should receive a DHCP address if proper connectivity to the DHCP server is configured. Executing the command "*show ip*" should validate whether the switch has received an IP address or not.

```
switch# show ip

 Internet (IP) Service

  IP Routing : Disabled

  Default Gateway : 192.168.58.254
  Default TTL     : 64
  Arp Age         : 20
  Domain Suffix   :
  DNS server      :

                        |                                                 Proxy ARP
  VLAN                  | IP Config  IP Address      Subnet Mask     Std  Local
  --------------------- + ---------- --------------- --------------- ---------- -----
  DEFAULT_VLAN          | DHCP/Bootp 192.168.58.120  255.255.255.0    No     No
```

By performing a packet capture and examining the DHCP options sent to the switch, the previous DHCP option configuration can be observed.



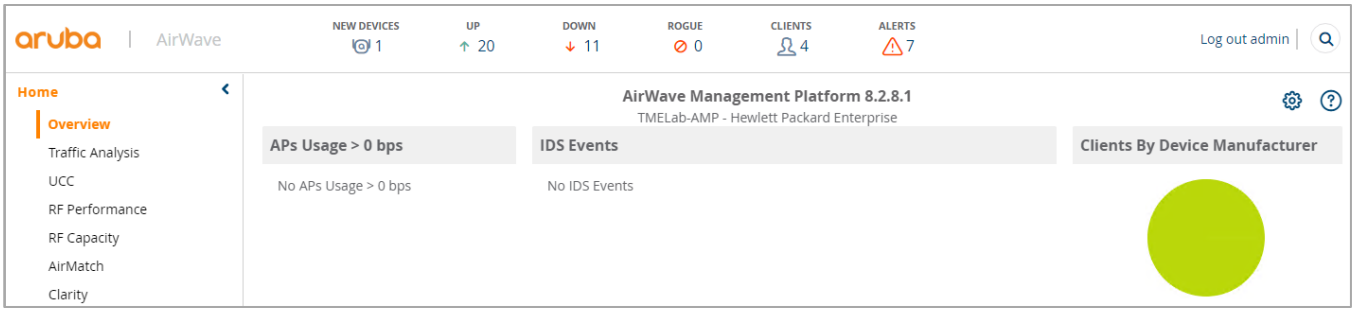
After the switch registers with AirWave, the switch-initiated TLS connection can then be viewed.



855	109.561828	192.168.58.120	10.5.8.18	TCP	66 56301 → 443 [ACK] Seq=1 Ack=1 Win=66608 Len=0 TSval=57520 TSecr=18223989
856	109.561829	192.168.58.120	10.5.8.18	TLSv1.2	239 Client Hello
857	109.562278	10.5.8.18	192.168.58.120	TCP	66 443 → 56301 [ACK] Seq=1 Ack=174 Win=15616 Len=0 TSval=18223995 TSecr=57520
858	109.563058	10.5.8.18	192.168.58.120	TLSv1.2	1409 Server Hello, Certificate, Server Hello Done
859	109.765646	192.168.58.120	10.5.8.18	TCP	66 56301 → 443 [ACK] Seq=174 Ack=1344 Win=65264 Len=0 TSval=57720 TSecr=18223995
860	109.819064	HewlettP_b2:9b:f0	LLDP_Multicast	LLDP	298 TTL = 120 System Name = M1st-Core System Description = HP J9850A Switch 5406Rzl2, revision KB.16.0
861	110.481179	HewlettP_c0:a5:1f	LLDP_Multicast	LLDP	314 TTL = 120 System Name = Aruba-2540-24G-PoEP-4SFPP System Description = Aruba JL356A 2540-24G-PoE+-
862	110.812029	192.168.58.120	10.5.8.18	TLSv1.2	333 Client Key Exchange
863	110.852416	10.5.8.18	192.168.58.120	TCP	66 443 → 56301 [ACK] Seq=1344 Ack=441 Win=16640 Len=0 TSval=18225285 TSecr=58760
864	110.852498	192.168.58.120	10.5.8.18	TLSv1.2	72 Change Cipher Spec
865	110.852783	10.5.8.18	192.168.58.120	TCP	66 443 → 56301 [ACK] Seq=1344 Ack=447 Win=16640 Len=0 TSval=18225285 TSecr=58810
866	111.206230	192.168.58.120	10.5.8.18	TLSv1.2	135 Encrypted Handshake Message
867	111.206558	10.5.8.18	192.168.58.120	TCP	66 443 → 56301 [ACK] Seq=1344 Ack=516 Win=16640 Len=0 TSval=18225639 TSecr=59170
868	111.206852	10.5.8.18	192.168.58.120	TLSv1.2	141 Change Cipher Spec, Encrypted Handshake Message
869	111.291197	ArubaAHe_be:8c:e1	Spanning-tree-(for-…	STP	53 RST. Root = 32768/0/00:0b:86:be:8c:e0 Cost = 0 Port = 0x8001
870	111.412823	192.168.58.120	10.5.8.18	TCP	66 56301 → 443 [ACK] Seq=516 Ack=1419 Win=65190 Len=0 TSval=59370 TSecr=18225639
871	111.412824	192.168.58.120	10.5.8.18	TLSv1.2	407 Application Data
872	111.418474	10.5.8.18	192.168.58.120	TLSv1.2	295 Application Data

It should be noted that if the ZTP device is the first discovered device in the newly created group and folder. Then it will show under the new devices list, which we need to move into the desired group/ folder.

From the second ZTP device onwards for the same group and folder as the first device, it will automatically move into the corresponding group and folder.



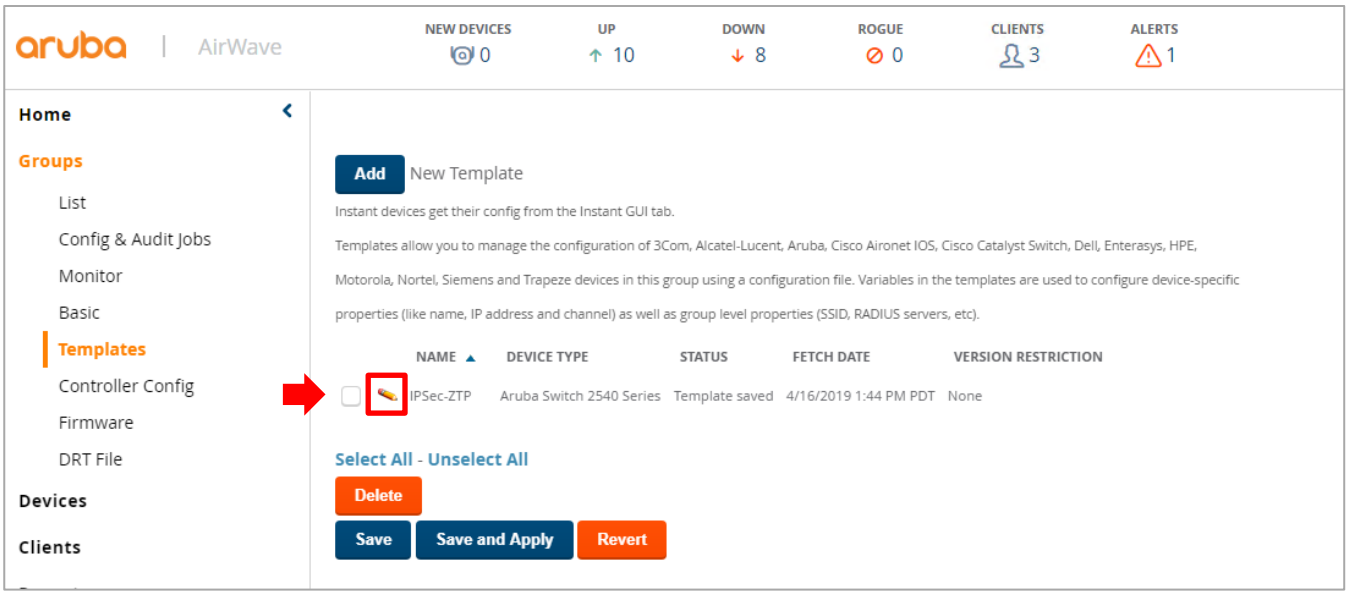
Templates

Once the switch is registered with AirWave and moved to a group, a template needs to be created. This can be done in two ways:

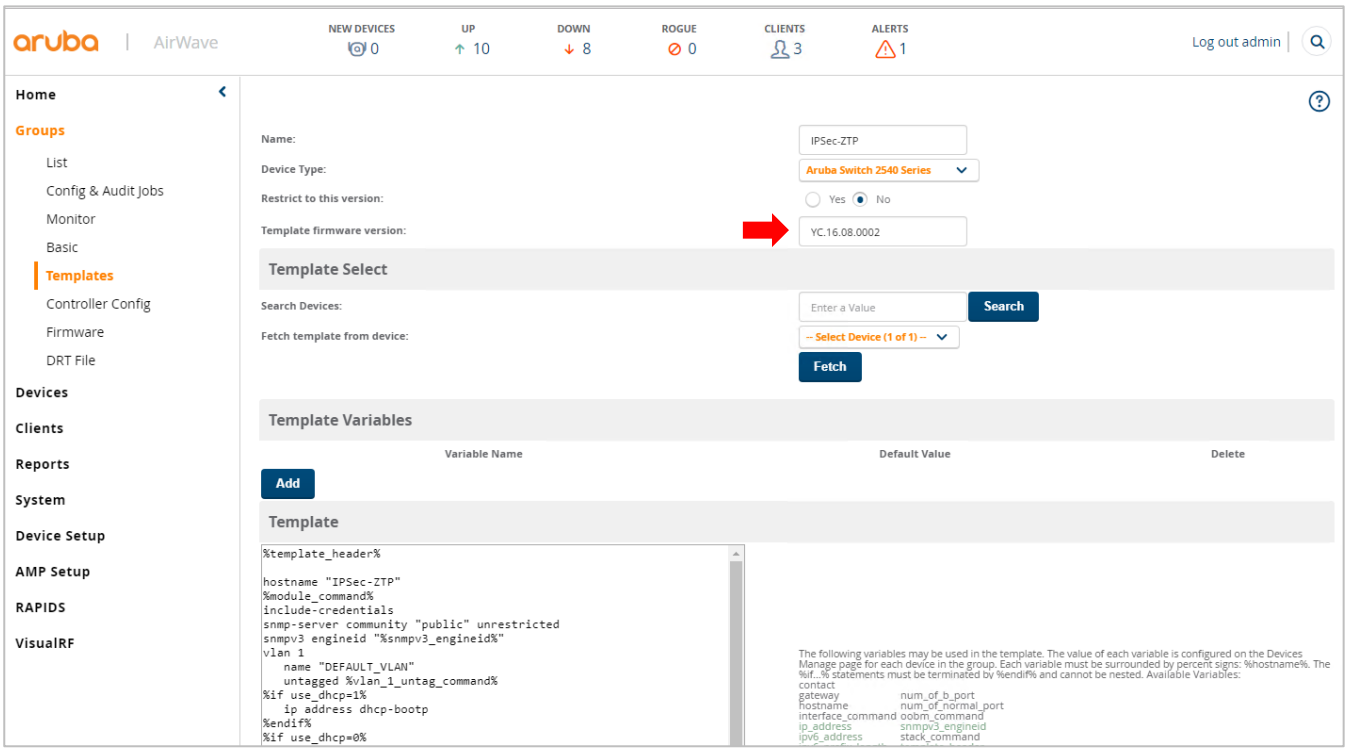
1. A template can be manually created
2. Fetched from the switch after it is manually configured with a “golden configuration”.

To navigate to templates in AirWave, select the “*Groups*” menu on the left, then select the desired group from the list and then click “*Templates*”.

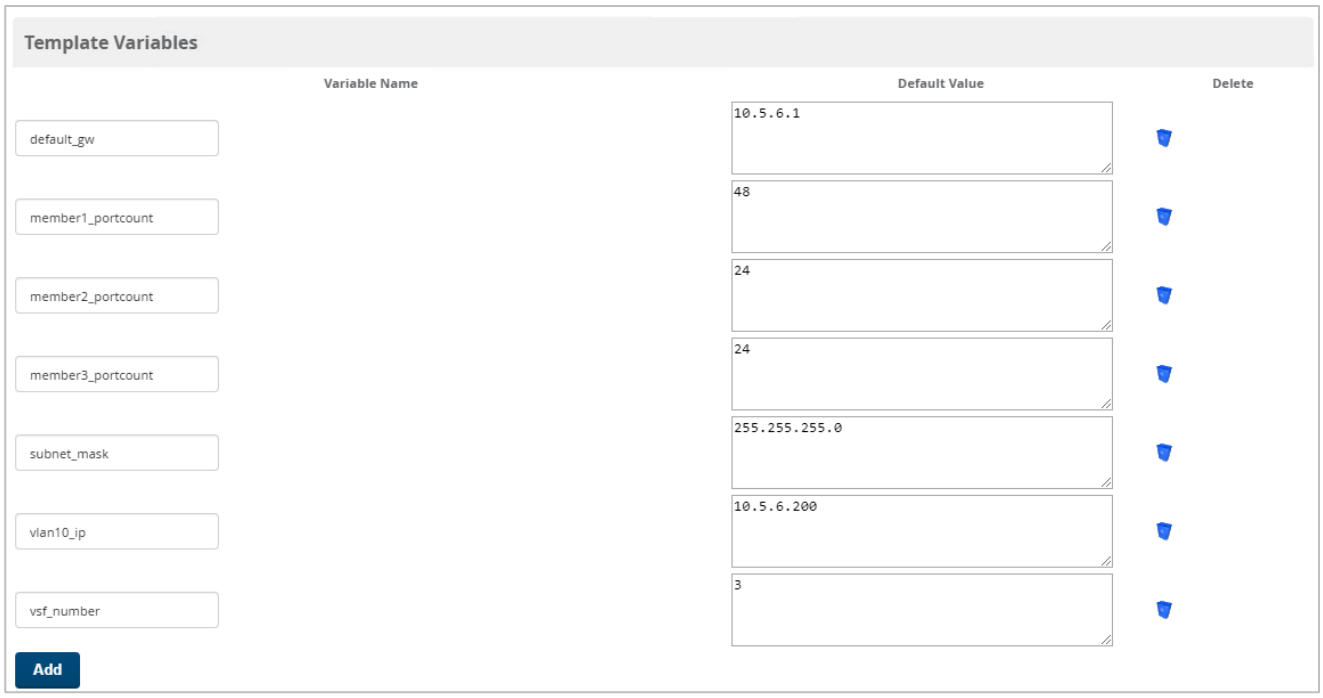
Once in the template window, select the “*pencil icon*” to edit the template as shown in the figure below.



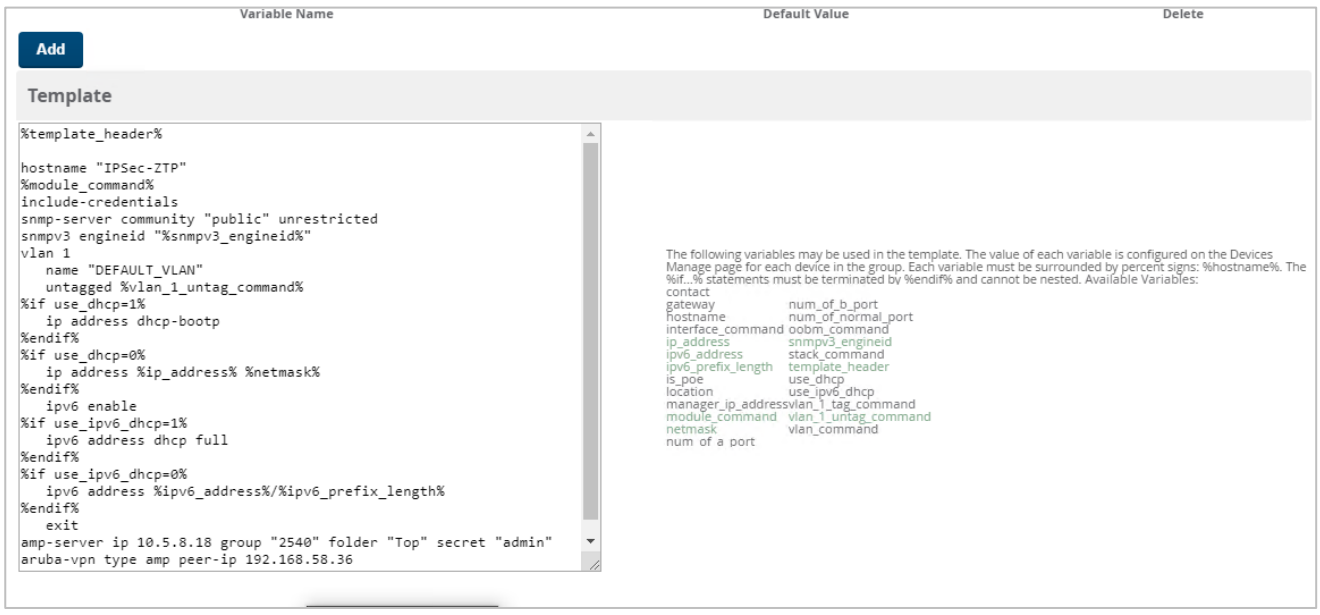
From here, the desired switch can be selected from the "*Search devices*" field and the template fetched from the switch.



The other method is to manually enter the template into the template window. Variables can be used for settings that may change across a suite of switches. Template examples for stacking are in Appendices A and B. Variables can be entered in the template window as shown below:



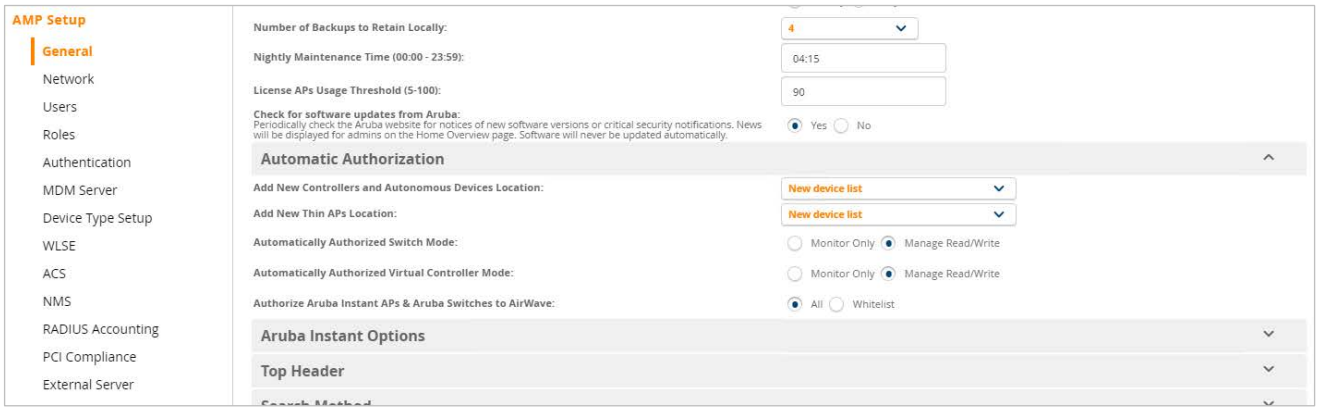
An additional way to add variables into the template is to use a Bulk CSV file. This allows a CSV file containing pertinent switch information to be imported into AirWave, using variables to assign the values from the CSV spreadsheet. This is helpful when provisioning stacks or switches that could contain many different variables.



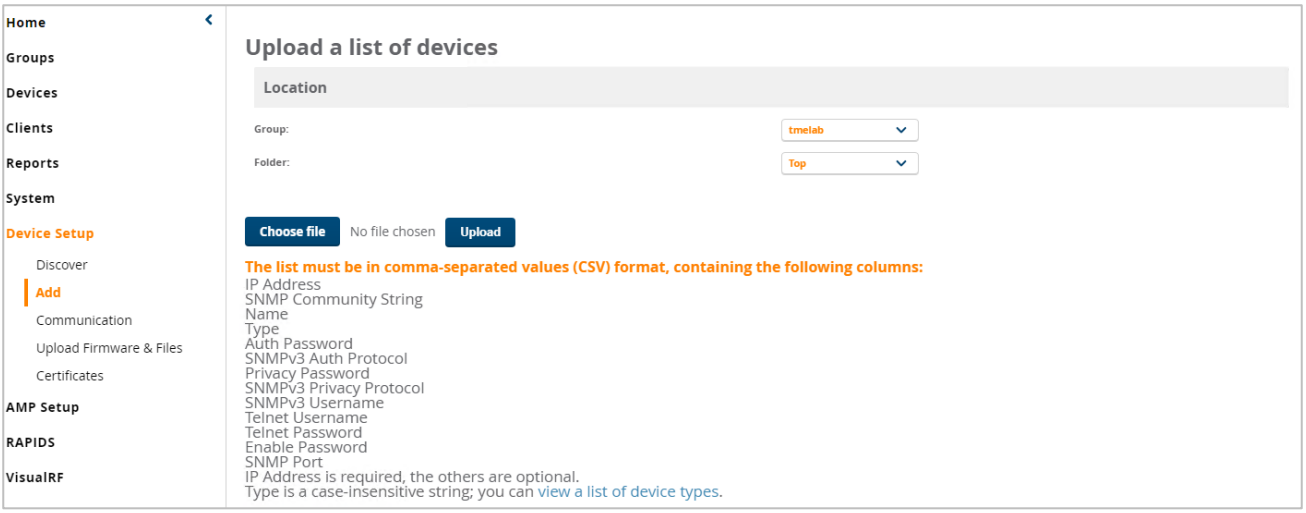
A sample variable file is embedded below:

VSF-Test-whitelist.csv

To enable uploading the CSV file, Whitelisting must be selected from Automatic Authorization in AMP **Setup > General**.



This CSV file can then be uploaded in the new device section:



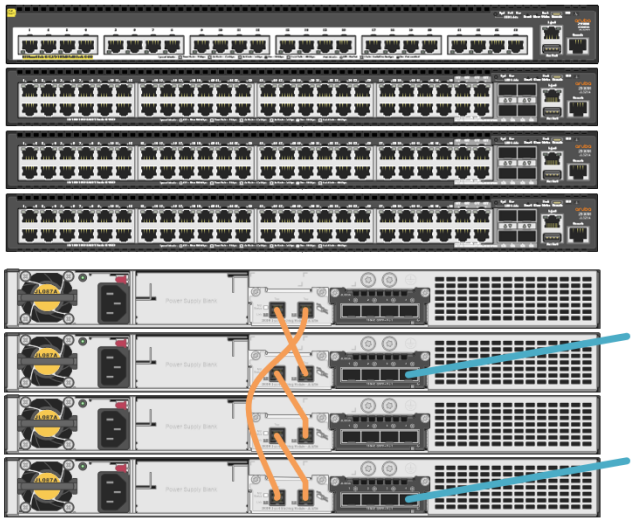
Another key consideration with templates and stacking is the way port counts are handled. As switches are provisioned to the stack, different models can have different port counts. Within the template, variables and if/else statements can be used to assign the necessary port counts as the switches are added to the stacks. An example of how to handle this is below, as well as full sample templates in the Appendices of this document.

```
%if member1_portcount=48%
interface 1/3-1/48 rate-limit bcast in percent 80
interface 1/3-1/48 rate-limit mcast in percent 80
```

```
interface 1/3-1/48 rate-limit unknown-unicast in percent 80
interface 1/3-1/48 untagged vlan 10
aaa port-access authenticator 1/1-1/48
aaa port-access authenticator 1/1-1/48 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 1/1-1/48
aaa port-access mac-based 1/1-1/48 addr-limit 32
aaa port-access lldp-bypass 1/1-1/48
spanning-tree 1/1-1/48 bpdu-protection
%else%
interface 1/3-1/24 rate-limit bcast in percent 80
interface 1/3-1/24 rate-limit mcast in percent 80
interface 1/3-1/24 rate-limit unknown-unicast in percent 80
interface 1/3-1/24 untagged vlan 10
aaa port-access authenticator 1/3-1/23
aaa port-access authenticator 1/3-1/23 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 1/3-1/23
aaa port-access mac-based 1/3-1/23 addr-limit 32
%endif%
```

Backplane Stacking Templates with AirWave

In a typical Aruba switch stack deployment, 4 member stacks are a common sight. The below image shows what a typical 4 member Aruba 2930M Switch Series backplane-connected stack would appear.



Stacks are handled much more delicately than a standalone switch with AirWave. It is recommended when provisioning a stack within AirWave, to first cable up all the stack members with the desired stacking topology and uplinks. The figure above shows an example of a ring topology.

Steps to Deploy – Estimated time to completion = 16 minutes with a 4-member stack

1. After completing all the physical connections, with the stacked switches powered off, create the group and template within AirWave to be used for the stack, an example of a template with commonly configured switch features is in Appendix A.

   Note: If the devices are not "brand new" out of the box, the command "*erase all*" should be executed on each switch and then immediately powered off upon reboot. This will put the switch back into a factory default state, clearing any old stacking information.

   In the default configuration, stacking is enabled on these switches. However, if a 3810M switch is powered on and it does not have a Stacking Module installed, stacking is disabled. If a Stacking Module is subsequently installed in the switch, stacking must be enabled from the switch CLI (in the configuration context) by entering the following command:

   ```
   switch(config)# stacking enable
   ```

   a. It is important to note the need for the stacking information to be present in the template. If/Else statements can be created using variables to provision multiple stack members and satisfy multiple stack topologies by editing the statements for greater or fewer stack members.

   ```
   stacking
   member 1 type %member1_sku%
   member 1 priority 255
   %if stack_number>1%
   member 2 type %member2_sku%
   member 2 flexible-module A type JL083A
   %endif%
   %if stack_number>2%
   member 3 type %member3_sku%
   member 3 priority 200
   %endif%
   %if stack_number>3%
   member 4 type %member4_sku%
   member 4 flexible-module A type JL083A
   %endif%
   Exit
   ```

   The template should already be configured at this stage and ready to deploy to the stack.

   ***Note**: It is recommended to not have the member 1 MAC address or MAC Address variable in the template. The Commander's MAC address is the LAN MAC address from the variable CSV file.*

2. Power on the first stack member, which should be the stack commander.

   Note: If the stack will have redundant uplinks on the same stack member, it is recommended to remove one of the links to avoid a network loop. If the redundant uplink is on another stack member, proceed using the following steps and the uplink will be enabled when the appropriate stack member is rebooted.

3. Wait until the commander boots up, receives the DHCP IP address and AirWave information via DHCP options. Once the template is pushed, it will reboot, this process takes approximately 8 minutes.
4. After the Commander is booted and template pushed, power up the remaining stack members one by one. If stack priorities are set, the entire stack will need to be rebooted for the priorities to take effect. From start to completion, this should take approximately 16 minutes for the entire stack to be provisioned, depending on how fast members are powered on.

Virtual Switching Framework (VSF) Templates with AirWave

Virtual Switching Framework or VSF is Aruba's front plane stacking feature on its edge switches. Zero Touch Provisioning (ZTP) with VSF handles differently than with a backplane stack. Each time VSF is enabled on a switch, the switch will reboot into the VSF configuration. Because of this, it takes a big longer to bring a stack up, 20 minutes or more with a 4 VSF members. The key is to wait for each member to reboot into "VSF mode" before booting the next member. The steps to provisioning a VSF stack are as follows:

1. After completing all the physical connections, with the stacked switches powered off, create the group and template within AirWave to be used for the stack, an example of a template with commonly configured switch features is in *Appendix A*.

   Note: If the devices are not "brand new" out of the box, the command "erase all" should be executed on each switch and then immediately powered off upon reboot. This will put the switch back into a factory default state, clearing any old stacking information. Cable up and configure the switches powered off, a 2930F VSF stack should look like the following:

   The **orange links** being either fiber optic cables or DAC cables, the **green cables** being the typical uplinks for a stack.

1. Configure the template in AirWave, a sample VSF stack template is located in *Appendix B* of this document. The configuration would look similar as the backplane stack except for the VSF configuration will have to be "strictly provisioned".

```
vsf
   enable domain 1000
   member 1
      type "JL256A"
      priority 255
      link 1 1/49
      link 1 name "I-Link1_1"
      link 2 1/50
```

```
   link 2 name "I-Link1_2"
   exit
member 2
   type "JL255A" mac-address e0071b-c26520
   priority 128
   link 1 2/25
   link 1 name "I-Link2_1"
   link 2 2/26
   link 2 name "I-Link2_2"
   exit
member 3
   type "JL255A" mac-address e0071b-c20500
   priority 200
   link 1 3/25
   link 1 name "I-Link3_1"
   link 2 3/26
   link 2 name "I-Link3_2"
   exit
member 4
   type "JL255A" mac-address e0071b-c2a520
   priority 128
   link 1 3/25
   link 1 name "I-Link3_1"
   link 2 3/26
   link 2 name "I-Link3_2"
   exit
port-speed 10g
exit
```

2. Power on the first switch, which will become the VSF Commander. After it reboots and receives the template, it will need to be placed into VSF mode, which causes the switch to reboot. This process takes approximately 8-9 minutes.

3. After the template has been applied to the commander, the subsequent members can be rebooted one at a time. Power up each member, running the "*show vsf*" command on the commander to verify when the next member is rebooted. From start to finish for a 4 member VSF stack, the approximate time is 20 minutes for the process to complete.

Secure ZTP with an Aruba Controller

This solution provides a secure communication method between Aruba Switches and the Aruba Controller (acting as a VPN concentrator) for network management traffic to AirWave.

Internet Protocol Security (IPSec) is a secure network protocol suite that authenticates and encrypts the packets of data sent over an internet protocol network. IPSecincludes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session. IPSec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPSec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPSecsupports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection.

The IPSecis an open standard as a part of the IPv4 suite. IPSecuses the following protocols to perform various functions:

- Authentication Headers (AH) provides connectionless data integrity and data origin authentication for IP datagrams and provides protection against replay attacks.
- Encapsulating Security Payloads (ESP) provides confidentiality, connectionless integrity, data-origin authentication, an anti-replay service (a form of partial sequence integrity), and limited traffic-flow confidentiality.
- Security Associations (SA) provides the bundle of algorithms and data that provide the parameters necessary for AH and/or ESP operations. The Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for authentication and key exchange, with actual authenticated keying material provided either by manual configuration with pre-shared keys, Internet Key Exchange (IKE and IKEv2).

The process works as follows:

- An IPSec tunnel for AirWave is auto-configured. The switch decides to create IPSec tunnel only when an Aruba Controller IP is present in the device before establishing the connection to AirWave.
- If the Controller IP is not provided and only AirWave details are provided, the switch will try to establish a direct HTTPS connection to AirWave.
- If AirWave details are missing from DHCP, the ZTP process will try to connect to Activate to receive AirWave details
- If the Controller IP is present, the ArubaOS-Switch auto configures and initiates an IPSec tunnel interface. Once the tunnel is established, the Aruba controller provides an inner IP which the switch will then use as source IP to send any AirWave bound traffic. The switch then creates a static route to AirWave with the IPSec tunnel interface as the gateway.

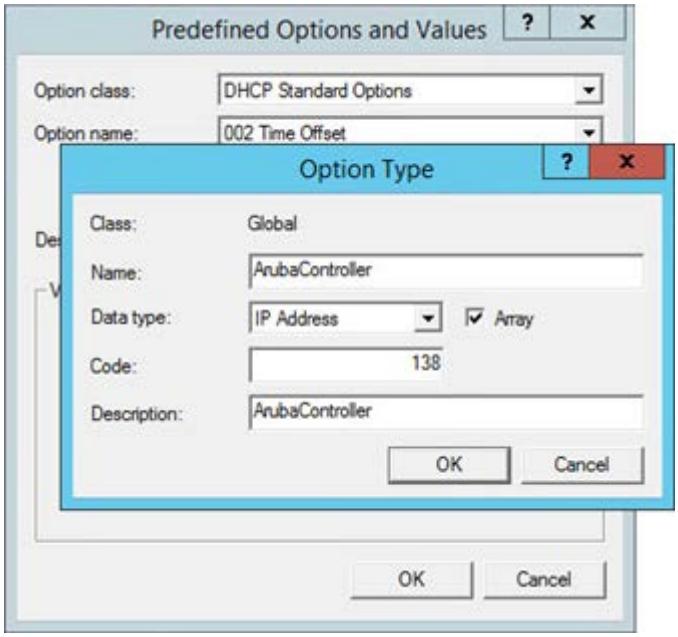
  Note: It is vital that AirWave can reach the inner switch IP address via the IPSec tunnel for the solution to work.

  This method uses the DHCP server to provide the IP address of the controller, it is recommended to have a valid NTP server so that the time can be synchronized between the switch and controller.

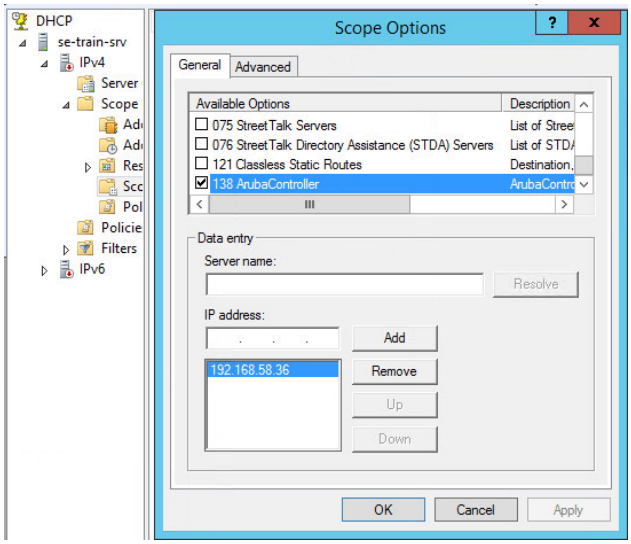
DHCP Server Configuration

Historically, option 138 was used for CAPWAP, in this case, it will be used to pass the Controller IP address to the new switch. To be able to add DHCP option 138, the DHCP server scope options will need to be edited, in the following examples, Windows Server 2016 is used. Option 138 is used in conjunction with Options 43 and 60.

From the DHCP scope, right click on IPv4 and "*set Predefined Options*". Click on "**Add**" and enter the relevant controller information as shown below.



After clicking "**OK**", enter the controller's IP address and select "**OK**"



Aruba Controller Configuration

Before configuring the controller, the MAC address of the switch to be provisioned needs to be captured. This can be done by executing the command "*show system*" at the switch:

```
switch# show system

 Status and Counters - General System Information

  System Name         : Switch
  System Contact      :
  System Location     :

  MAC Age Time (sec) : 300

  Time Zone           : 0
  Daylight Time Rule : None

  Software revision  : YC.16.08.0002        Base MAC Addr      : 98f2b3-c0a500
  ROM Version        : YC.16.01.0002        Serial Number      : CN77JYK05S

  Up Time            : 21 hours             Memory    - Total  : 360,047,104
  CPU Util (%)       : 0                              Free     : 257,178,964

  IP Mgmt   - Pkts Rx : 613,583             Packet    - Total  : 6600
              Pkts Tx : 618,296             Buffers     Free   : 4859
                                                        Lowest : 4829
                                                        Missed : 0
```

The MAC address above will then be added to the Controller's whitelist after disabling control-plane-security on the Controller.

```
(Controller) [mynode] (config) #no control-plane-security
control-plane-security
    no cpsec-enable
!
(Controller) #whitelist-db rap add mac-address 98:f2:b3:c0:a5:00 ap-group default
(Controller) #local-userdb add username 98:f2:b3:c0:a5:00 password 98:f2:b3:c0:a5:00
(Controller) #configure t
ip local pool "ARUBA-IPSEC" 10.88.88.10 10.88.88.50
!

ip access-list session aruba-acl any any tcp 22 permit
any any tcp 443 permit
!

user-role ap-role
access-list session aruba-acl
```

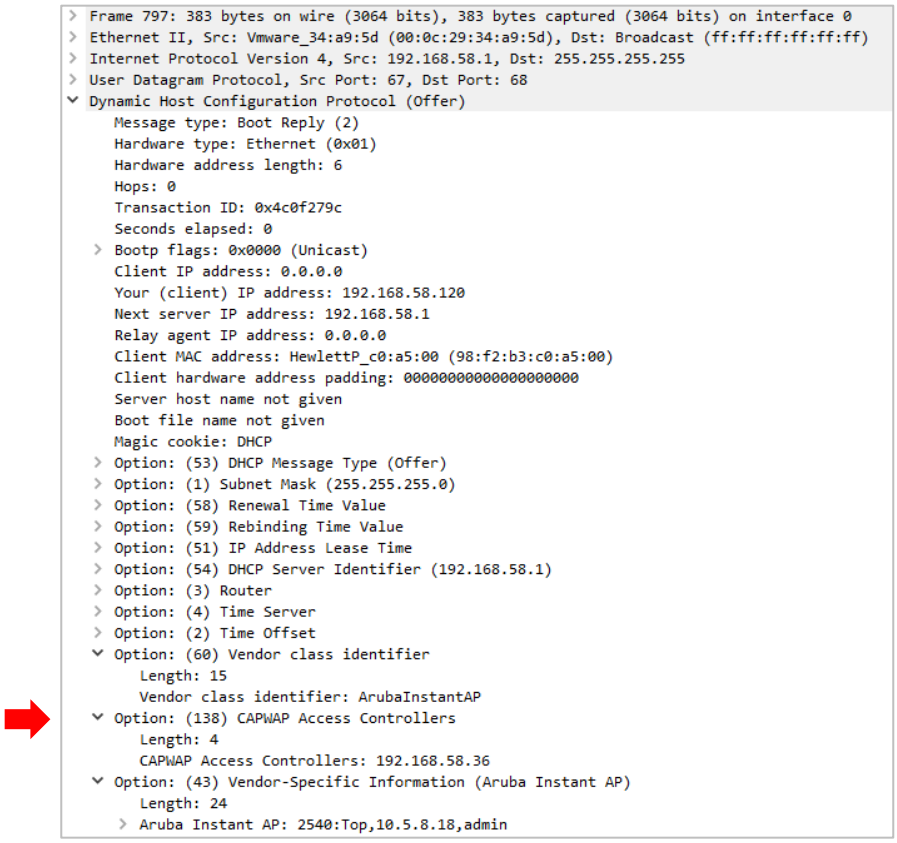
Since user role ap-role is already defined, the "*aruba-acl*" gets added as the last ACL.

***Note**: For production deployments, ClearPass should be used as the central point for all the whitelist entries.*

When a factory defaulted switch is connected to the network, it will get its IP from the DHCP server and then try to establish an IPSec tunnel with the controller.

```
824 107.159830   192.168.58.120   192.168.58.36    ISAKMP   542 IKE_SA_INIT MID=00 Initiator Request
825 107.162832   192.168.58.36    192.168.58.120   ISAKMP    98 IKE_SA_INIT MID=00 Responder Response
826 107.163444   192.168.58.120   192.168.58.36    ISAKMP   570 IKE_SA_INIT MID=00 Initiator Request
827 107.176281   192.168.58.36    192.168.58.120   ISAKMP   563 IKE_SA_INIT MID=00 Responder Response
828 107.290620   ArubaAHe_be:8c:e1 Spanning-tree-(for-… STP    53 RST. Root = 32768/0/00:0b:86:be:8c:e0  Cost = 0  Port = 0x8001
829 109.276853   192.168.58.120   192.168.58.36    ISAKMP   590 IKE_AUTH MID=01 Initiator Request (Message fragment 1)
830 109.276854   192.168.58.120   192.168.58.36    ISAKMP   590 IKE_AUTH MID=01 Initiator Request (Message fragment 2)
831 109.276855   192.168.58.120   192.168.58.36    ISAKMP   590 IKE_AUTH MID=01 Initiator Request (Message fragment 3)
832 109.276856   192.168.58.120   192.168.58.36    ISAKMP   590 IKE_AUTH MID=01 Initiator Request (Message fragment 4)
833 109.276860   192.168.58.120   192.168.58.36    ISAKMP   590 IKE_AUTH MID=01 Initiator Request (Message fragment 5)
834 109.276861   192.168.58.120   192.168.58.36    ISAKMP   590 IKE_AUTH MID=01 Initiator Request (Message fragment 6)
835 109.276862   192.168.58.120   192.168.58.36    ISAKMP   590 IKE_AUTH MID=01 Initiator Request (Message fragment 7)
836 109.276864   192.168.58.120   192.168.58.36    ISAKMP   590 IKE_AUTH MID=01 Initiator Request (Message fragment 8)
837 109.276865   192.168.58.120   192.168.58.36    ISAKMP   590 IKE_AUTH MID=01 Initiator Request (Message fragment 9)
838 109.276865   192.168.58.120   192.168.58.36    ISAKMP   590 IKE_AUTH MID=01 Initiator Request (Message fragment 10)
839 109.276866   192.168.58.120   192.168.58.36    ISAKMP   590 IKE_AUTH MID=01 Initiator Request (Message fragment 11)
840 109.276867   192.168.58.120   192.168.58.36    ISAKMP   270  (Reassembled + Message fragment 12 - last)
```

From the DHCP Offer packet, the DHCP options can been seen, note Option 138 contains the Controller IP address.



To validate the IPSec tunnel is up, here are some useful commands:

```
switch# show amp-server

 AMP Server Configuration details

  AMP Server IP            : 10.5.8.18
  AMP Server Group         : 2540
  AMP Server Folder        : Top
  AMP Server Secret        : admin
  AMP Server Config Status : Configured


switch# show aruba-vpn type amp

 Aruba VPN details

  Aruba VPN Type           : amp
  Aruba VPN Peer IP        : 192.168.58.36
  Aruba VPN Backup Peer IP :
  Aruba VPN Config Status  : Configured
```

```
  Aruba VPN tos            : Value from IPv4 header
  Aruba VPN ttl            : 64
```

```
switch# show interfaces tunnel brief

 Status - Tunnel Information Brief


  Tunnel                   : tunnel-129
  Mode                     : IPSecIPv4
  Source Address           : 192.168.58.120
  Destination Address      : 192.168.58.36
  Configured Tunnel Status : Enabled
  Current Tunnel State     : Up
```

```
switch# show interfaces tunnel aruba-vpn


 Tunnel Configuration :

  Tunnel               : tunnel-129
  Tunnel Name          : aruba-vpn-tunnel
  Tunnel Status        : Enabled
  Source Address       : 192.168.58.120
  Destination Address  : 192.168.58.36
  Mode                 : IPSecIPv4
  TOS                  : Value from IPv4 header
  TTL                  : 64
  IPv6                 : Disabled
  MTU                  : 1280


 Current Tunnel Status :

  Tunnel State               : Up
  Destination Address Route  : 192.168.58.0/24
  Next Hop IP                : 192.168.58.36
  Next Hop Interface         : vlan-1
  Next Hop IP Link Status    : Up
  Source Address             : Configured on vlan-1
  IP Datagrams Received      : 0
  IP Datagrams Transmitted   : 0
```

Useful Controller Commands:

```
(Controller) [mynode] #show local-userdb


User Summary
------------
Name               Password  Role   E-Mail  Enabled  Expiry  Status  Sponsor-Name  Remote-IP  Grantor-Name
----               --------  ----   ------  -------  ------  ------  ------------  ---------  ------------
98:f2:b3:c0:a5:00  ********  guest          Yes              Active                0.0.0.0    admin

User Entries: 1



(Controller) [mynode] #show crypto ipsec


IPSECSA (V2) Active Session Information
-----------------------------------
Initiator IP                              Responder IP                              SPI(IN/OUT)        Flags Start Time
Inner IP
------------                              ------------                              ----------------   ----- ---------------   ---
-----
192.168.58.120                            192.168.58.36                             c9d60c00/1ead187d  T2    Apr 18 15:22:23
192.168.58.195

Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap
       L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2
       l = uplink load-balance

Total IPSECSAs: 1



(Controller) [mynode] #show crypto isakmp sa

ISAKMP SA Active Session Information
-----------------------------------
Initiator IP                           Responder IP                           Flags     Start Time        Private IP
Peer ID
------------                           ------------                           -----     ----------        ----------
-------------
192.168.58.120                         192.168.58.36                          r-v2-c    Apr 18 15:23:43   192.168.58.196

Flags: i = Initiator; r = Responder
       m = Main Mode; a = Agressive Mode; v2 = IKEv2
       p = Pre-shared key; c = Certificate/RSA Signature; e =  ECDSA Signature
       x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled
       3 = 3rd party AP; C = Campus AP; R = RAP;  Ru = Custom Certificate RAP; I = IAP
       V = VIA; S = VIA over TCP; l = uplink load-balance

Total ISAKMP SAs: 1
```

Sample Debug Outputs

Example Log Messages

```
I 01/01/90 00:12:44 00076 ports: port 1 is now on-line
I 01/01/90 00:12:44 00828 lldp: PVID mismatch on port 1(VID 1) with peer device port 7(VID 30)(1)
I 01/01/90 00:12:56 00083 dhcp: updating IP address and subnet mask
I 01/01/90 00:12:56 05177 ip: Setting IP address 10.10.30.1 as default gateway.
I 01/01/90 00:12:56 00025 ip: DEFAULT_VLAN: ip address 10.10.30.100/24 configured on vlan 1
I 01/01/90 00:12:56 03783 dhcp: DHCP server did not offer all the DNS parameters on Primary VLAN
I 01/25/18 00:24:09 00413 SNTP: Updated time by 885687073 seconds from server at 192.168.1.250. Previous time
was Mon Jan 1 00:12:56 1990. Current time is Thu Jan 25 00:24:09 2018.
I 01/25/18 00:24:09 03125 mgr: Startup configuration changed by SNMP. New seq. number 2
I 01/25/18 00:24:09 05101 amp-server: AMP server details configured.
I 01/25/18 00:24:09 05101 amp-server: AMP server configuration is disabled due to first configuration.
I 01/25/18 00:24:09 05301 ztpIpsec: L3 IPv4 Tunnel Interface: Tunnel ID 129(4874) created.
I 01/25/18 00:24:09 05102 amp-server: AMP server registration started through Primary VLAN.
I 01/25/18 00:24:13 04611 job: Job Scheduler enabled
I 01/25/18 00:24:19 05304 ztpIpsec: IKE session initialization with peers 10.10.30.100 and 192.168.1.253 was
successful.
I 01/25/18 00:24:19 05306 ztpIpsec: IKE Security Association (SA) negotiation with peers 10.10.30.100 and
192.168.1.253 was successful.
I 01/25/18 00:24:19 00025 ip: aruba-vpn-tunnel: ip address 10.88.88.10/32 configured on tunnel 129
I 01/25/18 00:24:19 05310 ztpIpsec: 10.88.88.10 configured on IPSec VPN tunnel interface: Tunnel ID 129.
I 01/25/18 00:24:19 05308 ztpIpsec: IPSec VPN Tunnel ID 129 successfully established with peers 10.10.30.100 and
192.168.1.253.
D 01/25/18 00:24:19 05319 ztpIpsec: IKE_SA Created
D 01/25/18 00:24:19 05325 ztpIpsec: IPSEC_SA Created
I 01/25/18 00:24:19 05102 amp-server: AMP server registration started through Primary VLAN.
I 01/25/18 00:24:19 05311 ztpIpsec: IPv4 route to Airwave Controller 10.99.99.15 via IPSec VPN tunnel interface:
Tunnel ID 129 created.
I 01/25/18 00:24:19 05102 amp-server: Device registration to AMP server successful.
I 01/25/18 00:24:19 05102 amp-server: AMP server registration success.
```

Example ZTP Debug Output

```
switch# debug ztp
switch# debug destination session
0000:00:01:00.64 ZTP mairwaveCtrl:Received message 0x2200060
0000:00:01:06.21 ZTP mDHCPClint:Received option - OPTION_CAPWAP_AC_V4
0000:00:01:06.29 ZTP mDHCPClint:Access Controller IP address = 0xC0A801FD
0000:00:01:11.21 ZTP mDHCPClint:Received option - OPTION_CAPWAP_AC_V4
0000:00:01:11.29 ZTP mDHCPClint:Access Controller IP address = 0xC0A801FD
0000:00:01:11.76 ZTP mDHCPClint:Configuring AMP and VPN(if present) parameters.
0000:00:01:11.85 ZTP mairwaveCtrl:Received message 0x910012
0000:00:01:11.91 ZTP mSnmpCtrl:IPSEC ZTP: Establish New Session
0000:00:01:12.04 ZTP tSntpTask:Updated switch time
0000:00:01:12.87 ZTP mairwaveCtrl:Configured VPN details
0000:00:01:12.93 ZTP mSnmpCtrl:AMP server details configured- 10.99.99.15, LAN switches, Branch1 aruba123
0000:00:01:14.09 ZTP mairwaveCtrl:Configured AMP details
0000:00:01:14.19 ZTP mairwaveCtrl:ZTP is disabled
0000:00:01:14.24 ZTP mairwaveCtrl:Received message 0x91000F
0000:00:01:14.31 ZTP mairwaveCtrl:Received message 0x910004
0000:00:01:14.37 ZTP mairwaveCtrl:ZTP IPSEC: valid vlan found
0000:00:01:14.44 ZTP mairwaveCtrl:ZTP IPSEC: src ip selected: 10.10.30.100
0000:00:01:14.51 ZTP mairwaveCtrl:Configure IP Sec Tunnel, gw lport (1), gw vlan (1), retry(0)
0000:00:01:14.62 ZTP mairwaveCtrl:Scheduling retry in 60 seconds
0000:00:01:14.69 ZTP mairwaveCtrl:Received message 0x910001
0000:00:01:14.75 ZTP mairwaveCtrl:Default, Primary or Management VLAN is configured with IP or DHCP
0000:00:01:14.86 ZTP mairwaveCtrl:AMP server registration started through Primary VLAN.
0000:00:01:14.96 ZTP mairwaveCtrl:IPSEC ZTP: tunnel can not be established
0000:00:01:15.04 ZTP mairwaveCtrl:Can not start Airwave Check-in, tunnel not ready
0000:00:01:15.13 ZTP mairwaveCtrl:Received message 0x910005
0000:00:01:15.19 ZTP mairwaveCtrl:Received message 0x910008
0000:00:01:15.26 ZTP mairwaveCtrl:IPSEC ZTP: IKE session with controller is in progress.
0000:00:01:15.35 ZTP mairwaveCtrl:IPSEC ZTP: Waiting for Inner Src IP.
0000:00:01:15.43 ZTP mairwaveCtrl:Received message 0x91000A
0000:00:01:15.49 ZTP mairwaveCtrl:IPSEC ZTP: Inner Src IP received from Controller.
0000:00:01:15.58 ZTP mairwaveCtrl:IPSEC ZTP: Configure new Inner IP.
```

```
0000:00:01:15.66 ZTP mairwaveCtrl:Received message 0x910010
0000:00:01:15.72 ZTP mairwaveCtrl:Received message 0x910011
0000:00:01:15.78 ZTP mairwaveCtrl:Received message 0x910001
0000:00:01:15.85 ZTP mairwaveCtrl:Default, Primary or Management VLAN is configured with IP or DHCP
0000:00:01:15.96 ZTP mairwaveCtrl:AMP server registration started through Primary VLAN.
0000:00:01:16.05 ZTP mairwaveCtrl:IPSEC ZTP: Airwave IP is discovered.
0000:00:01:16.13 ZTP mairwaveCtrl:sending request to https://10.99.99.15/switch_https
0000:00:01:16.22 ZTP mairwaveCtrl:Added X-Type: Device-Reg
0000:00:01:16.29 ZTP mairwaveCtrl:Added X-OEM: HP
0000:00:01:16.34 ZTP mairwaveCtrl:Added X-Mode: SWITCH
0000:00:01:16.40 ZTP mairwaveCtrl:Added X-Current-Version: WC.16.04.0009_271
0000:00:01:16.48 ZTP mairwaveCtrl:Added X-Device-Info: CN6BHKZ1RQ, B0:5A:DA:98:9A:00, 2930F-8G-PoE+-2SFP+ Switch
0000:00:01:16.60 ZTP mairwaveCtrl:Added X-Group: LAN switches
0000:00:01:16.67 ZTP mairwaveCtrl:Added X-Folder: Branch1
0000:00:01:16.73 ZTP mairwaveCtrl:Added X-Shared-Secret: aruba123
0000:00:01:16.80 ZTP mairwaveCtrl:Added X-Device-State: Factory
0000:00:02:29.23 ZTP mairwaveCtrl:Switch registration failed 7 -
0000:00:02:29.30 ZTP mairwaveCtrl:Error string: Couldn't connect to server
0000:00:02:29.38 ZTP mairwaveCtrl:Registration with AMP server failed. Scheduling retry in 60 seconds
0000:00:02:29.49 ZTP mairwaveCtrl:Received message 0x91000B
0000:00:02:29.56 ZTP mairwaveCtrl:IPSEC ZTP: In Health-Check timer
0000:00:02:29.63 ZTP mairwaveCtrl:IPSEC ZTP: Switch sends HB
0000:00:02:49.23 ZTP mairwaveCtrl:Received message 0x91000B
0000:00:02:49.30 ZTP mairwaveCtrl:IPSEC ZTP: In Health-Check timer
0000:00:02:49.37 ZTP mairwaveCtrl:IPSEC ZTP: Switch sends HB
0000:00:03:09.23 ZTP mairwaveCtrl:Received message 0x91000B
0000:00:03:09.30 ZTP mairwaveCtrl:IPSEC ZTP: In Health-Check timer
0000:00:03:09.37 ZTP mairwaveCtrl:IPSEC ZTP: Switch sends HB
0000:00:03:29.24 ZTP mairwaveCtrl:Received message 0x91000B
0000:00:03:29.31 ZTP mairwaveCtrl:IPSEC ZTP: In Health-Check timer
0000:00:03:29.38 ZTP mairwaveCtrl:IPSEC ZTP: Switch sends HB
0000:00:03:29.44 ZTP mairwaveCtrl:Received message 0x910002
0000:00:03:29.51 ZTP mairwaveCtrl:Default, Primary or Management VLAN is configured with DHCP
0000:00:03:29.64 ZTP mairwaveCtrl:AMP server registration started through Primary VLAN.
0000:00:03:29.74 ZTP mairwaveCtrl:IPSEC ZTP: Check-in to Airwave through IPSec
0000:00:03:29.82 ZTP mairwaveCtrl:sending request to https://10.99.99.15/switch_https
0000:00:03:29.92 ZTP mairwaveCtrl:Added X-Type: Device-Reg
0000:00:03:29.98 ZTP mairwaveCtrl:Added X-OEM: HP
0000:00:03:30.03 ZTP mairwaveCtrl:Added X-Mode: SWITCH
0000:00:03:30.12 ZTP mairwaveCtrl:Added X-Current-Version: WC.16.04.0009_271
0000:00:03:30.20 ZTP mairwaveCtrl:Added X-Device-Info: CN6BHKZ1RQ, B0:5A:DA:98:9A:00, 2930F-8G-PoE+-2SFP+ Switch
0000:00:03:30.33 ZTP mairwaveCtrl:Added X-Group: LAN switches
0000:00:03:30.39 ZTP mairwaveCtrl:Added X-Folder: Branch1
0000:00:03:30.45 ZTP mairwaveCtrl:Added X-Shared-Secret: aruba123
0000:00:03:30.52 ZTP mairwaveCtrl:Added X-Device-State: Factory
0000:00:03:30.60 ZTP mairwaveCtrl:Switch registered Sucessfully 0 - HTTP/1.1 200 OK Server: nginx Dat
0000:00:03:30.74 ZTP mairwaveCtrl:Registration with AMP server successful. Scheduling periodic checking for 3600
seconds
```

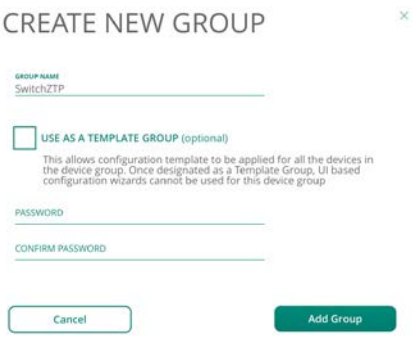
PROVISIONING WITH ARUBA CENTRAL

Group Creation and Device Assignment

In order to provision devices using Aruba Central, they must first be assigned to a configuration group. There are two types of configuration groups: the default group type utilizes UI-based settings and offers a subset of ArubaOS-Switch features, while *template groups* provide full access to the switch feature set via configuration templates, which can be adapted to apply to various device types and use variables to apply different values to a group of devices from the same base template.

To create a configuration group in the Central UI, open **Global Settings**, then select **Manage Groups**. Click or tap the **New Group** button in the bottom left corner, under the group list.

In the *Create New Group* dialog, give the new group a name. If the new group will use UI-based settings, enter a group password as prompted. If this will be a new template group, check the *USE AS A TEMPLATE GROUP* box. Select **Add Group** to create the new group.



You can also create a new UI-based configuration group by importing the existing configuration from a device in the list. Select the switch you wish to use as the configuration source, then click or tap **Import Configuration to New Group**. Enter a group name and assign a password, then select **Import Configuration**.

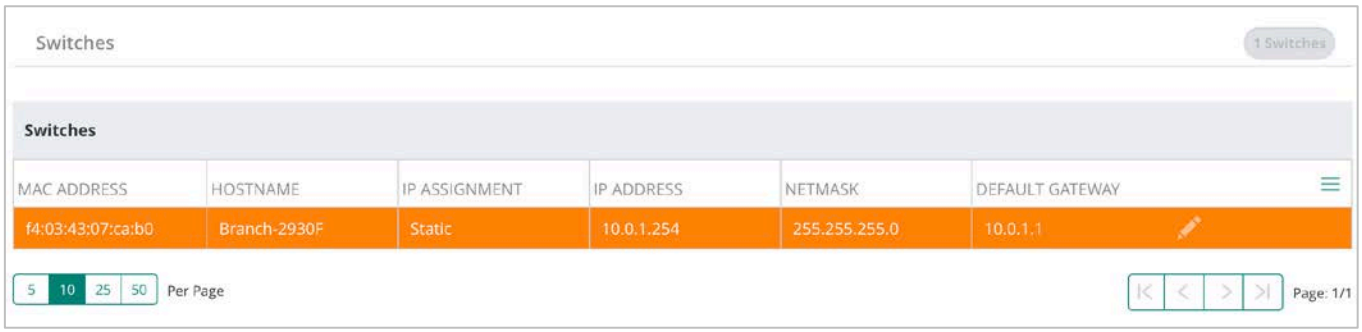
Once the group has been created, select one or more devices from the list on the right (hold Control on Windows or Command on macOS to select multiple devices at once) and drag them to the target group in the list to the left to assign them to that group. You will be presented with the dialog pictured to the right; select **Yes** to confirm the move, or **No** to cancel.

UI-based Group and Device Configuration

Use the **CURRENT APP** navigation menu to open **Wired Management**. Switches can be managed by group or by individual device; use the filter menu at the top of the page to select either the group you created or an individual switch. Note that, when configuring at the group level, the switch port configuration page displays 52 ports as a group may contain 8-port, 24-port, or 48-port switches (some with 2 or 4 dedicated uplink ports each, for a total of 10, 28, or 52 ports, respectively).

When any setting on a page has been changed, you will need to commit those changes using the **Save Settings** button in the bottom-right corner before leaving the page. If you attempt to leave the page without saving, a warning prompt will be displayed; choose **Continue** to remain on the current page (keeping changes intact), or **Discard** to revert your changes and navigate to the new page.

Basic switch settings can be changed by highlighting a switch in the list, and clicking the pencil-shaped edit button in the rightmost column.



Settings that can be changed here are the hostname and IP address assignment (DHCP or static).

Navigate through each configuration section to configure interfaces, VLANs, ACLs, and other settings. Once the group-level configuration is complete, provision devices in that group by powering them up and connecting them to a network that provides internet connectivity, either directly or via a proxy server (configurable via DHCP option).

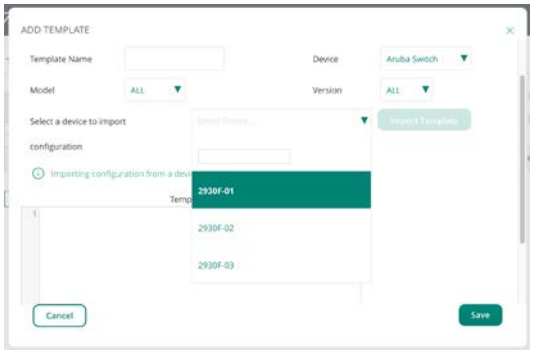
Template-based Group Configuration

After creating a template-based configuration group and adding at least one device to it, navigate to **CURRENT APP ➔ Wired Management**. From the filter bar at the top of the page, select the group you just created from the list under **GROUPS**; it will have the letters TG just to the left of the group name.

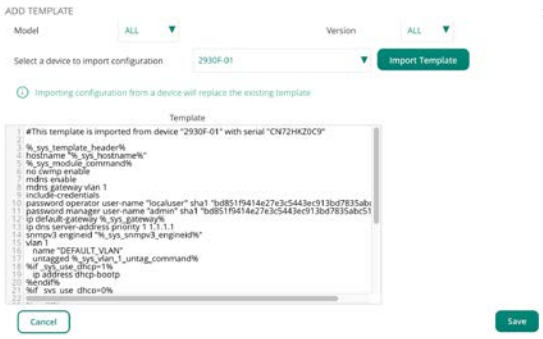
To create a new template, open the **Templates** page and click the + link near the bottom left of the template list.

Give the template a unique name, and for **Device**, select **Aruba Switch**. The Model and Version fields can either be left at **ALL** or set to a specific switch series and major software release (16.03 through 16.08). If a specific switch model or software version are selected, the template will be applied only to switches in the group that match those criteria.

To import a baseline configuration to build the template from, select a device from the list presented, then click or tap **Import Template**.



The resulting template can be modified to suit the desired configuration for the group, using variables (either Central-defined or custom) for device-specific values. For more information on template and variable management, refer to the Central documentation.



Once you have finished editing the template and are ready to apply it to switches in the group, select **Save** in the bottom-right corner of the template editor.

If any applicable switches in the group are currently online and being managed by Central, the new or updated template should be pushed to them within 1-2 minutes.

Provisioning sequence with Activate and Central

Once the switch boots from a factory default state and acquires a DHCP address with DNS server information, the following events will occur in order:

- The switch will attempt to resolve the Activate server URL to an IP address, and if successful, will attempt to reach the Activate service for initial provisioning. (If a proxy server is configured via DHCP, the switch will use the proxy server to establish connections to Activate and Central.)
- Once connected to Activate, the switch will attempt to synchronize its clock using NTP, then HTTP Time Protocol with the Activate time server (even if time is already synchronized from a local time server configured via DHCP; in this case, the local time synchronization should prevail).
- Activate then pushes a Trust Anchor certificate to the switch to secure communications.
- Activate will determine which management platform the switch needs to register with (Central or AirWave). If the switch has been added to Central, added to a license subscription, and assigned to a group, the URL for the provisioned Central instance will be pushed to the switch.
- The switch connects to the configured Central instance and loads the Central SSL certificate.
- Central begins polling and pushes the applicable configuration (UI-based or template) to the switch.

To view the status of Activate provisioning, use the following command:

```
switch# show activate provision

 Configuration and Status - Activate Provision Service

  Activate Provision Service   : Enabled
  Activate Server Address      : device.arubanetworks.com
  Activation Key               : XXXXXXXX
  Time Sync Status             : Time sync from HTTP Time Protocol
  Activate DNS Lookup          : Success
  Proxy Server DNS Lookup      : Success
  Activate Connection Status   : Success
  Error Reason                 : Time sync has failed from NTP pool
```

For the status of the Central connection, use this command:

```
switch# show aruba-central

 Configuration and Status - Aruba Central

  Server URL              : https://portal.central.arubanetworks.com/ws
  Connected               : Yes
  Mode                    : Monitor
  Last Disconnect Time    : Thu Apr 18 14:43:19 2019
  Server DNS Lookup       : Success
  Proxy Server DNS Lookup : Success
  Error Reason            : NA
```

Stacking and Central

Stacking works much the same way as with AirWave, namely the template format and process is like the same process with AirWave. The recommended way to bring up a stack is to cable everything up, leaving the switches powered off. For examples of how to cable the switches, refer to pages 13 and 15 for diagrams on how a cabled VSF or backplane stack should appear. The template and variable process is the same as described on page 25.

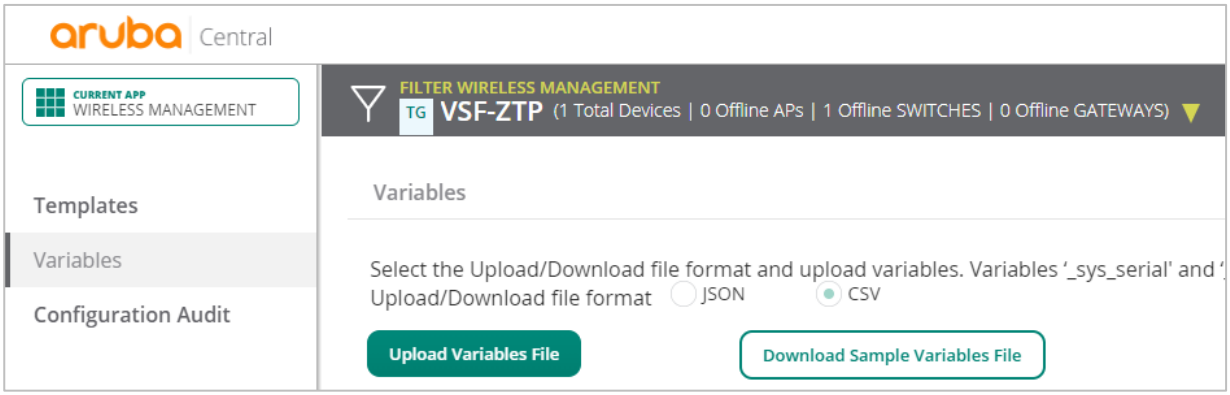
1. First, boot the commander up, wait for the template to apply, the switch may reboot for VSF or stacking configuration.
2. Boot/power up each member sequentially to ensure that the switch connects to the stacking commander correctly
3. Central will automatically “take-over” the switch configuration where it can then be monitored by Central.

Note: Sample templates for both VSF and Backplane stacking are in the Appendix. The templates work much the same way as AirWave, for example, a port count variable can be used to control the port settings across different members of a stack. An IF/ELSE statement can be used to set interface settings for both a 48 port or 24 port switch depending on what will be connected to the stack. Variables are entered in the same way that is shown on page

An Example is below:

```
%if vsf_number>1%
%if member2_portcount=48%
interface 2/1-2/46 rate-limit bcast in percent 80
interface 2/1-2/46 rate-limit mcast in percent 80
interface 2/1-2/46 rate-limit unknown-unicast in percent 80
interface 2/1-2/46 untagged vlan 2525
aaa port-access authenticator 2/1-2/46
aaa port-access authenticator 2/1-2/46 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 2/1-2/46
aaa port-access mac-based 2/1-2/46 addr-limit 32
aaa port-access lldp-bypass 2/1-2/46
spanning-tree 2/1-2/46 bpdu-protection
%else%
interface 2/1-2/24 rate-limit bcast in percent 80
interface 2/1-2/24 rate-limit mcast in percent 80
interface 2/1-2/24 rate-limit unknown-unicast in percent 80
interface 2/1-2/24 untagged vlan 2525
aaa port-access authenticator 2/1-2/24
aaa port-access authenticator 2/1-2/24 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 2/1-2/24
aaa port-access mac-based 2/1-2/24 addr-limit 32
aaa port-access lldp-bypass 2/1-2/24
spanning-tree 2/1-2/24 bpdu-protection
%endif%
%endif%
```

Variables can be entered in from the variable menu in the template config:



A sample variable file can be downloaded directly from Central where the desired variables can be entered in.

A 4-member backplane stack (2930M) takes approximately 13-14 minutes to bring up from start to finish. A 4 member VSF stack (2930F) takes approximately 20 minutes from start to finish

ENCRYPTED CREDENTIALS FOR DOWNLOADABLE USER ROLES IN DYNAMIC SEGMENTATION

To ensure that downloadable user roles can be used in the ZTP process for both AirWave and Central, the current way to ensure that the downloadable role ClearPass credentials are saved into the config and avoid having to manually enter the credentials, the following process is needed:

Preparation

- AirWave or Central is setup with a template (See Appendix)
- CSV whitelist has been uploaded to AirWave or Central (See previous provisioning sections
- Ensure the first switch is running AOS-S 16.08.0003
- Setup the first switch (stack commander) as the golden config to generate the template.
    - Key things are noted below;
        - Use the encrypt-credentials command and set up a PSK
        - Enable the encrypt-credentials
        - Enable include-credentials
        - Copy the line below from the switch config to your template;
            - ; encrypt-cred rkFUqUNIgep7pvhEKydLmtnV/CrkTLlwSgC8puxGg+FYSZBFZ+w9eIBOaQk+3Z+E
    - Define your config which requires passwords
        - User's
        - ClearPass/Radius
        - Etc.

Configuration

1. Create the Group in AirWave
2. Create the template and link it to the appropriate switch model
3. Upload the firmware for the appropriate switch model
4. Under group set the firmware to desired firmware (Ex: WC.16.08.0003)
5. Upload the CSV file under new devices
6. Connect the commander switch to the network (Ex: port 1/a1)
7. Power on commander
    a. Commander will connect to AMP
    b. Download code if not later
    c. Will download template (and should reboot when the config is downloaded correctly – this is due to the config being pushed to the startup-configuration)
    d. Wait for commander to move from new devices to group based on CSV file (Ex: ZTP-BPS)
    e. Wait for commander to get "Good" config state in AirWave;

8. Power up remaining stack members

ZERO TOUCH PROVISIONING WITH DHCP AND TFTP

This method utilizes DHCP vendor classes and options to point the switch at a TFTP server to acquire firmware images and configuration files. This requires switches using this method to be provisioned on a network from which the TFTP server is reachable, and the server must host software images and configuration files compatible with each model of switch to be provisioned.

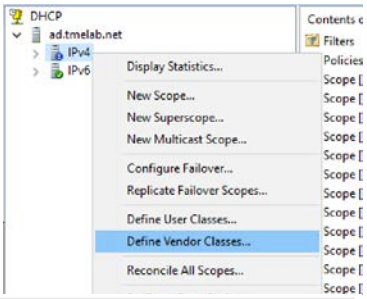
Create vendor class on DHCP server

First, obtain the vendor class string from each switch model to be provisioned. This can be done using the following command:

```
switch# show dhcp client vendor-specific

Vendor Class Id = Aruba JL258A 2930F-8G-PoE+-2SFP+ Switch
Processing of Vendor Specific Configuration is enabled
```

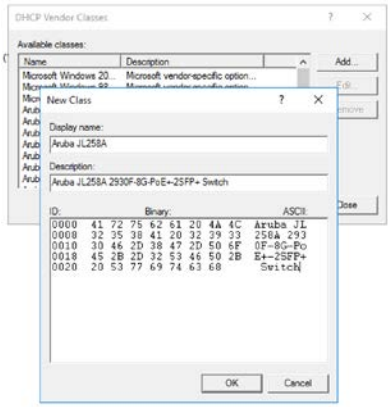
The section in **bold** must be copied in its entirety and used to create a vendor class on the DHCP server; for the examples that follow, the Windows Server 2016 DHCP Server was used. For other DHCP server implementations, refer to the appropriate platform documentation.

From the DHCP management window, expand the tree in the left-hand navigation pane, right-click the **IPv4** list item, and select **Define Vendor Classes...**



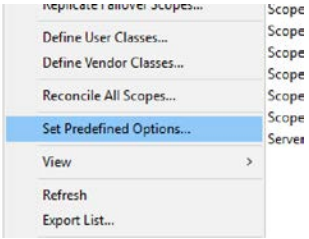
In the window that opens, select **Add...**, then give the new vendor class a unique name and description (either or both may include the part number and/or model name for quick reference).

In the **ASCII** field, type in the full vendor class string obtained from the switch (copying and pasting may not function in this field). Once this is done, select **OK** to save the new class, and **Close** to return to the main DHCP management window.

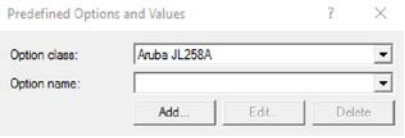


Set Predefined Options

Right-click the **IPv4** item again, and select **Set Predefined Options...**

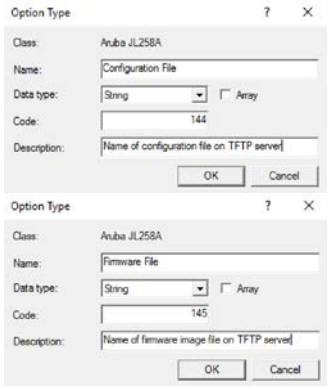


In the **Predefined Options and Values** window, select the newly-created vendor class from the **Option class** dropdown list, and then click or tap **Add...**

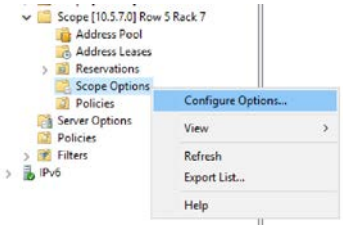


Name the new option "Configuration File"; set the **Data type** to **String**, assign the **Code** a value of **144**, and give the option an appropriate description (see example pictured). Click **OK** to save.

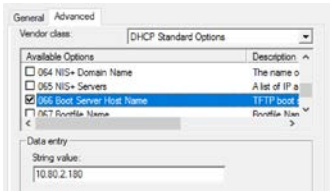
Repeat this process, naming the second new option "Firmware File"; set **Data type** to **String** and **Code** to 145, and add a description. Click **OK**, then click **OK** again to dismiss the **Predefined Options and Values** window.



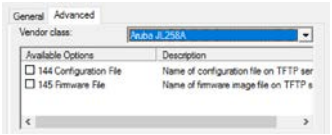
In the main DHCP management window, browse to an IPv4 scope and expand it in the list. Right-click the **Scope Options** list item and select **Configure Options...**



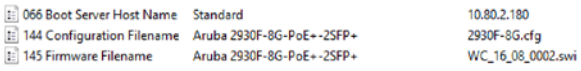
Select the **Advanced** tab. Under the **DHCP Standard Options** vendor class, locate option **066 Boot Server Host Name** and check the box. In the **String value** field, enter the IP address of the TFTP server hosting the configuration and/or firmware files.



Now, select the vendor class created earlier from the dropdown list. You should see the two just created predefined options in the list. Check the box next to one or both of them, and set their string values to the configuration and firmware filenames, as stored on the TFTP server. Click **OK** to apply the selected options to the DHCP scope.



In the DHCP Scope Options view, you should now see the three new options and their configured values.



When a switch is connected to the network and acquires a DHCP IP address in this scope, it will attempt to connect to the TFTP server specified by option 66 and first download the firmware image in suboption 145, if configured. If the download is successful, the firmware image will be verified and copied to the primary flash. Regardless of the result, the switch will then attempt to download the configuration file from suboption 144; if successful, the configuration will be validated for compatibility. If the configuration is determined to be valid for the switch model and firmware version, it will replace the default startup configuration and the switch will reboot. This process may take up to 2-3 minutes from initial boot.

To prevent the switch from repeating the ZTP process on subsequent reboot cycles, it is recommended that the configuration file on the TFTP server contain the following commands:

```
no dhcp config-file-update
no dhcp image-file-update
```

This will result in the switch ignoring DHCP suboptions 144 and 145 when acquiring a DHCP IP address on the configured scope.

Backplane Stacking

With using a TFTP server to push a config to a stack, this works differently than Central or AirWave, which uses templates. In this case, the exact config for the stack (Backplane or VSF) will need to be pushed to the device(s). The switch OS can only parse the exact config that is sent to the switch, with AirWave or Central, it will send an exact config. An example for this is in the Appendix, this process takes approximately 16 minutes from start to finish to complete the stack. It is expected you will have all members new out of the box and cabled up like the AirWave and Central methods, or use the erase all method as mentioned on page

The procedure is as follows:

1. First, boot up the commander and wait for it to get the DHCP address and options, it will then download the config file from the TFTP server. Once it downloads and parses it successfully, it will then reboot to enable the provisioned stacking members.
2. After the commander has been rebooted, boot the next stack member up which should become the standby.
3. Once the commander and standby are up, boot every other member one at a time until it is shown as “booting” in the show stack output.

VSF

VSF works similar in this method as with backplane stacking, the major difference being that each switch will reboot after being powered on and detecting the VSF packets. In total, the entire process takes approximately 18 minutes for a 4-member stack. This process is the same as with backplane stacking:

1. First, boot up the commander and wait for it to get the DHCP address and options, it will then download the config file from the TFTP server. Once it downloads and parses it successfully, it will then reboot to enable VSF and have the other stack members provisioned
2. After the commander has been rebooted, boot the next stack member up which should become the standby.
3. Once the commander and standby are up, boot every other member one at a time until it is shown as “booting” in the show vsf output.

APPENDIX

Sample Backplane Stack AirWave Template

```
%template_header%
; encrypt-cred Sc5WXEUCc2Q7tqfFk3FIakDPdqgVf0fwR4clm8s3QWqnQ6mhcrr3YJqXmRqe4lyH
stacking
   member 1 type %member1_sku%
   member 1 priority 255
   %if stack_number>1%
   member 2 type %member2_sku%
   member 2 flexible-module A type JL083A
   %endif%
   %if stack_number>2%
   member 3 type %member3_sku%
   member 3 priority 200
   %endif%
   %if stack_number>3%
   member 4 type %member4_sku%
   member 4 flexible-module A type JL083A
   %endif%
   exit
hostname "%hostname%"
encrypt-credentials
no cdp run
dhcp-snooping
no dhcp-snooping option 82
dhcp-snooping vlan 75 100 176 2525 2530-2531 3001

banner motd " "
no banner last-login
no telnet-server

igmp filter-unknown-mcast
```

```
radius-server host 10.5.8.12 key admin
radius-server host 10.5.8.12 dyn-authorization
radius-server host 10.5.8.12 time-window plus-or-minus-time-window
radius-server host 10.5.8.12 time-window 30
radius-server cppm identity "durtest" key aruba123

timesync ntp
ntp unicast
ntp server 10.80.2.219 iburst
ntp enable

time daylight-time-rule continental-us-and-canada
time timezone -360
no web-management

ip dns domain-name tmelab.net
ip dns server-address priority 1 10.80.2.219

ip source-interface tacacs vlan 1055
ip source-interface radius vlan 1055
ip source-interface syslog vlan 1055
ip source-interface telnet vlan 1055
ip source-interface tftp vlan 1055
ip source-interface sntp vlan 1055
ip source-interface sflow vlan 1055
ip source-interface tunneled-node-server vlan 1055
ip client-tracker

tunneled-node-server
   controller-ip 10.5.8.6
   mode role-based reserved-vlan 1000
```

```
   exit

%if stack_number=1%
trunk 1/1,1/2 trk1 lacp
interface 1/1,1/2 name "Uplink"
%endif%

%if stack_number>1%
trunk 2/A4,4/A4 trk1 lacp
interface 2/A4,4/A4 name "Uplink"
interface 2/A1-2/A3,4/A1-4/A3 disable
%endif%

interface Trk1 dhcp-snooping trust

%if member1_portcount=48%
interface 1/3-1/48 rate-limit bcast in percent 80
interface 1/3-1/48 rate-limit mcast in percent 80
interface 1/3-1/48 rate-limit unknown-unicast in percent 80
interface 1/3-1/48 untagged vlan 10
aaa port-access authenticator 1/1-1/48
aaa port-access authenticator 1/1-1/48 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 1/1-1/48
aaa port-access mac-based 1/1-1/48 addr-limit 32
aaa port-access lldp-bypass 1/1-1/48
spanning-tree 1/1-1/48 bpdu-protection
%else%
interface 1/3-1/24 rate-limit bcast in percent 80
interface 1/3-1/24 rate-limit mcast in percent 80
interface 1/3-1/24 rate-limit unknown-unicast in percent 80
interface 1/3-1/24 untagged vlan 10
```

```
aaa port-access authenticator 1/3-1/23
aaa port-access authenticator 1/3-1/23 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 1/3-1/23
aaa port-access mac-based 1/3-1/23 addr-limit 32
%endif%

%if stack_number>1%
%if member2_portcount=48%
interface 2/1-2/48 rate-limit bcast in percent 80
interface 2/1-2/48 rate-limit mcast in percent 80
interface 2/1-2/48 rate-limit unknown-unicast in percent 80
interface 2/1-2/48 untagged vlan 2525
aaa port-access authenticator 2/1-2/48
aaa port-access authenticator 2/1-2/48 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 2/1-2/48
aaa port-access mac-based 2/1-2/48 addr-limit 32
aaa port-access lldp-bypass 2/1-2/48
spanning-tree 2/1-2/48 bpdu-protection
%else%
interface 2/1-2/24 rate-limit bcast in percent 80
interface 2/1-2/24 rate-limit mcast in percent 80
interface 2/1-2/24 rate-limit unknown-unicast in percent 80
interface 2/1-2/24 untagged vlan 2525
aaa port-access authenticator 2/1-2/24
aaa port-access authenticator 2/1-2/24 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 2/1-2/24
aaa port-access mac-based 2/1-2/24 addr-limit 32
aaa port-access lldp-bypass 2/1-2/24
spanning-tree 2/1-2/24 bpdu-protection
```

```
%endif%
%endif%

%if stack_number>2%
%if member3_portcount=48%
interface 3/1-3/48 rate-limit bcast in percent 80
interface 3/1-3/48 rate-limit mcast in percent 80
interface 3/1-3/48 rate-limit unknown-unicast in percent 80
interface 3/1-3/48 untagged vlan 2525
aaa port-access authenticator 3/1-3/48
aaa port-access authenticator 3/1-3/48 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 3/1-3/48
aaa port-access mac-based 3/1-3/48 addr-limit 32
aaa port-access lldp-bypass 3/1-3/48
spanning-tree 3/1-3/48 bpdu-protection
%else%
interface 3/1-3/24 rate-limit bcast in percent 80
interface 3/1-3/24 rate-limit mcast in percent 80
interface 3/1-3/24 rate-limit unknown-unicast in percent 80
interface 3/1-3/24 untagged vlan 2525
aaa port-access authenticator 3/1-3/24
aaa port-access authenticator 3/1-3/24 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 3/1-3/24
aaa port-access mac-based 3/1-3/24 addr-limit 32
aaa port-access lldp-bypass 3/1-3/24
spanning-tree 3/1-3/24 bpdu-protection
%endif%
%endif%

%if stack_number>3%
```

```
%if member4_portcount=48%
interface 4/1-4/48 rate-limit bcast in percent 80
interface 4/1-4/48 rate-limit mcast in percent 80
interface 4/1-4/48 rate-limit unknown-unicast in percent 80
interface 4/1-4/48 untagged vlan 2525
aaa port-access authenticator 4/1-4/48
aaa port-access authenticator 4/1-4/48 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 4/1-4/48
aaa port-access mac-based 4/1-4/48 addr-limit 32
aaa port-access lldp-bypass 4/1-4/48
spanning-tree 4/1-4/48 bpdu-protection
%else%
interface 4/1-4/24 rate-limit bcast in percent 80
interface 4/1-4/24 rate-limit mcast in percent 80
interface 4/1-4/24 rate-limit unknown-unicast in percent 80
interface 4/1-4/24 untagged vlan 2525
aaa port-access authenticator 4/1-4/24
aaa port-access authenticator 4/1-4/24 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 4/1-4/24
aaa port-access mac-based 4/1-4/24 addr-limit 32
aaa port-access lldp-bypass 4/1-4/24
spanning-tree 4/1-4/24 bpdu-protection
%endif%
%endif%

snmp-server community public unrestricted
snmpv3 engineid "%snmpv3_engineid%"

aaa server-group radius "CPPM" host 10.5.8.12
aaa authorization user-role enable download
```

```
vlan 1
   name "DEFAULT_VLAN"
   no ip address
   ip igmp
   jumbo
   exit
vlan 10
   name "Management"
   untagged Trk1
   ip address %vlan10_ip% %subnet_mask%
   ip igmp
   jumbo
   exit
vlan 513
   name "GUEST"
   no ip address
   ip igmp
   jumbo
   exit
vlan 1000
   name "TUNNELED_NODE_SERVER_RESERVED"
   no ip address
   exit
vlan 2525
   tagged Trk1
   no ip address
   ip igmp
   ipv6 mld enable
   jumbo
   exit
vlan 2530
```

```
   tagged Trk1
   ip igmp
   jumbo
   exit
vlan 2531
   tagged Trk1
   ip igmp
   jumbo
   exit

spanning-tree
spanning-tree bpdu-protection-timeout 90

mac-delimiter colon

no tftp server
no autorun
no dhcp config-file-update
no dhcp image-file-update

trunk-load-balance L4-based

device-profile name "ARUBA-AP"
   untagged-vlan 10
   allow-jumbo-frames
   no allow-tunneled-node
   exit
device-profile type "aruba-ap"
   associate "ARUBA-AP"
   enable
   exit
```

```
ip default-gateway %default_gw%

primary-vlan 10
amp-server ip 10.80.2.201 group "2930M-ZTPDemo" folder "Top" secret "admin"
activate provision disable
allow-unsupported-transceiver
```

Sample VSF Stack AirWave Template

```
; hpStack_WC Configuration Editor; Created on release #WC.16.08.0003
; Ver #14:27.6f.f8.1d.9b.3f.bf.bb.ef.7c.59.fc.6b.fb.9f.fc.ff.ff.37.ef:04
; encrypt-cred B+Zd5Wj3/rhBq1UsyDDqAfFjvGxFlGEltuL0/yggZSY3UlfcpVemhWgF0TCT5Djy
hostname "%hostname%"
vsf
   enable domain 1000
   member 1
      type "JL256A"
      priority 255
      link 1 1/49
      link 1 name "I-Link1_1"
      link 2 1/50
      link 2 name "I-Link1_2"
      exit
   member 2
      type "JL255A" mac-address e0071b-c26520
      priority 128
      link 1 2/25
      link 1 name "I-Link2_1"
      link 2 2/26
      link 2 name "I-Link2_2"
      exit
   member 3
      type "JL255A" mac-address e0071b-c20500
      priority 200
      link 1 3/25
      link 1 name "I-Link3_1"
      link 2 3/26
      link 2 name "I-Link3_2"
      exit
   member 4
```

```
      type "JL255A" mac-address e0071b-c2a520
      priority 128
      link 1 3/25
      link 1 name "I-Link3_1"
      link 2 3/26
      link 2 name "I-Link3_2"
      exit
   port-speed 10g
   exit
encrypt-credentials
include-credentials
no cdp run
dhcp-snooping
no dhcp-snooping option 82
dhcp-snooping vlan 75 100 176 2525 2530-2531 3001

banner motd " "
no banner last-login
no telnet-server

igmp filter-unknown-mcast

radius-server host 10.5.8.12 key admin
radius-server host 10.5.8.12 dyn-authorization
radius-server host 10.5.8.12 time-window plus-or-minus-time-window
radius-server host 10.5.8.12 time-window 30
radius-server cppm identity "durtest" key aruba123

timesync ntp
ntp unicast
ntp server 10.80.2.219 iburst
ntp enable
```

```
time daylight-time-rule continental-us-and-canada
time timezone -360
no web-management

ip dns domain-name tmelab.net
ip dns server-address priority 1 10.80.2.219

ip source-interface tacacs vlan 1055
ip source-interface radius vlan 1055
ip source-interface syslog vlan 1055
ip source-interface telnet vlan 1055
ip source-interface tftp vlan 1055
ip source-interface sntp vlan 1055
ip source-interface sflow vlan 1055
ip source-interface tunneled-node-server vlan 1055
ip client-tracker

tunneled-node-server
   controller-ip 10.5.8.6
   mode role-based reserved-vlan 1000
   exit
%if vsf_number=1%
trunk 1/3,1/4 trk1 lacp
interface 1/3,1/4 name "Uplink"
%endif%

%if vsf_number>1%
trunk 1/52,3/28 trk1 lacp
interface 1/52,3/28 name "Uplink"
%endif%
```

```
interface Trk1 dhcp-snooping trust

%if member1_portcount=48%
interface 1/1-1/48 rate-limit bcast in percent 80
interface 1/1-1/48 rate-limit mcast in percent 80
interface 1/1-1/48 rate-limit unknown-unicast in percent 80
interface 1/1-1/48 untagged vlan 10
aaa port-access authenticator 1/2-1/48
aaa port-access authenticator 1/2-1/48 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 1/2-1/48
aaa port-access mac-based 1/2-1/48 addr-limit 32
aaa port-access lldp-bypass 1/1-1/48
%else%
interface 1/1-1/24 rate-limit bcast in percent 80
interface 1/1-1/24 rate-limit mcast in percent 80
interface 1/1-1/24 rate-limit unknown-unicast in percent 80
interface 1/1-1/24 untagged vlan 10
aaa port-access authenticator 1/2-1/24
aaa port-access authenticator 1/2-1/24 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 1/2-1/24
aaa port-access mac-based 1/2-1/24 addr-limit 32
aaa port-access lldp-bypass 1/1-1/24
%endif%

%if vsf_number>1%
%if member2_portcount=48%
interface 2/1-2/48 rate-limit bcast in percent 80
interface 2/1-2/48 rate-limit mcast in percent 80
interface 2/1-2/48 rate-limit unknown-unicast in percent 80
interface 2/1-2/48 untagged vlan 2525
```

```
aaa port-access authenticator 2/1-2/48
aaa port-access authenticator 2/1-2/48 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 2/1-2/48
aaa port-access mac-based 2/1-2/48 addr-limit 32
aaa port-access lldp-bypass 2/1-2/48
spanning-tree 2/1-2/48 bpdu-protection
%else%
interface 2/1-2/24 rate-limit bcast in percent 80
interface 2/1-2/24 rate-limit mcast in percent 80
interface 2/1-2/24 rate-limit unknown-unicast in percent 80
interface 2/1-2/24 untagged vlan 2525
aaa port-access authenticator 2/1-2/24
aaa port-access authenticator 2/1-2/24 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 2/1-2/24
aaa port-access mac-based 2/1-2/24 addr-limit 32
aaa port-access lldp-bypass 2/1-2/24
spanning-tree 2/1-2/24 bpdu-protection
%endif%
%endif%

%if vsf_number>2%
%if member3_portcount=48%
interface 3/1-3/48 rate-limit bcast in percent 80
interface 3/1-3/48 rate-limit mcast in percent 80
interface 3/1-3/48 rate-limit unknown-unicast in percent 80
interface 3/1-3/48 untagged vlan 2525
aaa port-access authenticator 3/1-3/48
aaa port-access authenticator 3/1-3/48 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 3/1-3/48
```

```
aaa port-access mac-based 3/1-3/48 addr-limit 32
aaa port-access lldp-bypass 3/1-3/48
spanning-tree 3/1-3/48 bpdu-protection
%else%
interface 3/1-3/24 rate-limit bcast in percent 80
interface 3/1-3/24 rate-limit mcast in percent 80
interface 3/1-3/24 rate-limit unknown-unicast in percent 80
interface 3/1-3/24 untagged vlan 2525
aaa port-access authenticator 3/1-3/24
aaa port-access authenticator 3/1-3/24 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 3/1-3/24
aaa port-access mac-based 3/1-3/24 addr-limit 32
aaa port-access lldp-bypass 3/1-3/24
spanning-tree 3/1-3/24 bpdu-protection
%endif%
%endif%

snmp-server community "public" unrestricted
snmpv3 engineid "%snmpv3_engineid%"

aaa server-group radius "CPPM" host 10.5.8.12
aaa authorization user-role enable download

vlan 1
   name "DEFAULT_VLAN"
%if use_dhcp=1%
   ip address dhcp-bootp
%endif%
%if use_dhcp=0%
   ip address %ip_address% %netmask%
%endif%
```

```
   ipv6 enable
%if use_ipv6_dhcp=1%
   ipv6 address dhcp full
%endif%
%if use_ipv6_dhcp=0%
   ipv6 address %ipv6_address%/%ipv6_prefix_length%
%endif%
   exit
vlan 10
   name "Management"
   untagged Trk1
   ip address %vlan10_ip% %subnet_mask%
   ip igmp
   jumbo
   exit
vlan 513
   name "GUEST"
   no ip address
   ip igmp
   jumbo
   exit
vlan 1000
   name "TUNNELED_NODE_SERVER_RESERVED"
   no ip address
   exit
vlan 2525
   tagged Trk1
   no ip address
   ip igmp
   ipv6 mld enable
   jumbo
   exit
```

```
vlan 2530
   tagged Trk1
   ip igmp
   jumbo
   exit
vlan 2531
   tagged Trk1
   ip igmp
   jumbo
   exit

spanning-tree
spanning-tree bpdu-protection-timeout 90

mac-delimiter colon

no tftp server
no autorun
no dhcp config-file-update
no dhcp image-file-update

trunk-load-balance L4-based

device-profile name "ARUBA-AP"
   untagged-vlan 10
   allow-jumbo-frames
   no allow-tunneled-node
   exit
device-profile type "aruba-ap"
   associate "ARUBA-AP"
   enable
   exit
```

```
ip default-gateway %default_gw%

primary-vlan 10
amp-server ip 10.80.2.201 group "2930M-ZTPDemo" folder "Top" secret "admin"
activate provision disable
allow-unsupported-transceiver
```

Sample Backplane Stack Central Template

```
%ver_info%
; encrypt-cred B+Zd5Wj3/rhBq1UsyDDqAfFjvGxFlGEltuL0/yggZSY3UlfcpVemhWgF0TCT5Djy

hostname "%hostname%"
stacking
   member 1 type %member1_sku%
   member 1 priority 255
   %if stack_number>1%
   member 2 type %member2_sku%
   member 2 flexible-module A type JL083A
   %endif%
   %if stack_number>2%
   member 3 type %member3_sku%
   member 3 priority 200
   %endif%
   %if stack_number>3%
   member 4 type %member4_sku%
   member 4 flexible-module A type JL083A
   %endif%
   exit
Encrypt-credentials
include-credentials
no cdp run
dhcp-snooping
no dhcp-snooping option 82
dhcp-snooping vlan 75 100 176 2525 2530-2531 3001

banner motd " "
no banner last-login
no telnet-server

igmp filter-unknown-mcast

radius-server host 10.5.8.12 key admin
radius-server host 10.5.8.12 dyn-authorization
radius-server host 10.5.8.12 time-window plus-or-minus-time-window
radius-server host 10.5.8.12 time-window 30
radius-server cppm identity "durtest" key aruba123

timesync ntp
ntp unicast
ntp server 10.80.2.219 iburst
ntp enable

time daylight-time-rule continental-us-and-canada
time timezone -360
no web-management

ip dns domain-name tmelab.net
ip dns server-address priority 1 10.80.2.219
```

```
ip source-interface tacacs vlan 1055
ip source-interface radius vlan 1055
ip source-interface syslog vlan 1055
ip source-interface telnet vlan 1055
ip source-interface tftp vlan 1055
ip source-interface sntp vlan 1055
ip source-interface sflow vlan 1055
ip source-interface tunneled-node-server vlan 1055
ip client-tracker

tunneled-node-server
   controller-ip 10.5.8.6
   mode role-based reserved-vlan 1000
   exit
%if stack_number=1%
trunk 1/3,1/4 trk1 lacp
interface 1/3,1/4 name "Uplink"
%endif%

%if stack_number>1%
trunk 1/24,2/48 trk1 lacp
interface 1/24,2/48 name "Uplink"
%endif%

interface Trk1 dhcp-snooping trust

%if member1_portcount=48%
interface 1/1-1/48 rate-limit bcast in percent 80
interface 1/1-1/48 rate-limit mcast in percent 80
interface 1/1-1/48 rate-limit unknown-unicast in percent 80
interface 1/1-1/48 untagged vlan 10
aaa port-access lldp-bypass 1/1-1/48
%else%
interface 1/1-1/22 rate-limit bcast in percent 80
interface 1/1-1/22 rate-limit mcast in percent 80
interface 1/1-1/22 rate-limit unknown-unicast in percent 80
interface 1/1-1/22 untagged vlan 10
%endif%

%if stack_number>1%
%if member2_portcount=48%
interface 2/1-2/46 rate-limit bcast in percent 80
interface 2/1-2/46 rate-limit mcast in percent 80
interface 2/1-2/46 rate-limit unknown-unicast in percent 80
interface 2/1-2/46 untagged vlan 2525
aaa port-access authenticator 2/1-2/46
aaa port-access authenticator 2/1-2/46 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 2/1-2/46
aaa port-access mac-based 2/1-2/46 addr-limit 32
aaa port-access lldp-bypass 2/1-2/46
spanning-tree 2/1-2/46 bpdu-protection
```

```
%else%
interface 2/1-2/24 rate-limit bcast in percent 80
interface 2/1-2/24 rate-limit mcast in percent 80
interface 2/1-2/24 rate-limit unknown-unicast in percent 80
interface 2/1-2/24 untagged vlan 2525
aaa port-access authenticator 2/1-2/24
aaa port-access authenticator 2/1-2/24 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 2/1-2/24
aaa port-access mac-based 2/1-2/24 addr-limit 32
aaa port-access lldp-bypass 2/1-2/24
spanning-tree 2/1-2/24 bpdu-protection
%endif%
%endif%

snmp-server community "public" unrestricted

aaa server-group radius "CPPM" host 10.5.8.12
aaa authorization user-role enable download

vlan 1
   name "DEFAULT_VLAN"
%if use_dhcp=1%
   ip address dhcp-bootp
%endif%
%if use_dhcp=0%
   ip address %ip_address% %netmask%
%endif%
   ipv6 enable
%if use_ipv6_dhcp=1%
   ipv6 address dhcp full
%endif%
%if use_ipv6_dhcp=0%
   ipv6 address %ipv6_address%/%ipv6_prefix_length%
%endif%
   exit
vlan 10
   name "Management"
   untagged Trk1
   ip address %vlan10_ip% %subnet_mask%
   ip igmp
   jumbo
   exit
vlan 513
   name "GUEST"
   no ip address
   ip igmp
   jumbo
   exit
vlan 1000
   name "TUNNELED_NODE_SERVER_RESERVED"
   no ip address
```

```
   exit
vlan 2525
   tagged Trk1
   no ip address
   ip igmp
   ipv6 mld enable
   jumbo
   exit
vlan 2530
   tagged Trk1
   ip igmp
   jumbo
   exit
vlan 2531
   tagged Trk1
   ip igmp
   jumbo
   exit

spanning-tree
spanning-tree bpdu-protection-timeout 90

mac-delimiter colon

no tftp server
no autorun
no dhcp config-file-update
no dhcp image-file-update

trunk-load-balance L4-based

device-profile name "ARUBA-AP"
   untagged-vlan 10
   allow-jumbo-frames
   no allow-tunneled-node
   exit
device-profile type "aruba-ap"
   associate "ARUBA-AP"
   enable
   exit

ip default-gateway %default_gw%

primary-vlan 10
activate provision disable
allow-unsupported-transceiver
proxy server http://10.80.2.217:8080
```

Sample VSF Stack Central Template

```
%ver_info%
; encrypt-cred B+Zd5Wj3/rhBq1UsyDDqAfFjvGxFlGEltuL0/yggZSY3UlfcpVemhWgF0TCT5Djy

hostname "%hostname%"
vsf
   enable domain 1000
   member 1
      type "JL256A"
      priority 255
      link 1 1/49
      link 1 name "I-Link1_1"
      link 2 1/50
      link 2 name "I-Link1_2"
      exit
   member 2
      type "JL255A" mac-address e0071b-c26520
      priority 128
      link 1 2/25
      link 1 name "I-Link2_1"
      link 2 2/26
      link 2 name "I-Link2_2"
      exit
   member 3
      type "JL255A" mac-address e0071b-c20500
      priority 200
      link 1 3/25
      link 1 name "I-Link3_1"
      link 2 3/26
      link 2 name "I-Link3_2"
      exit
   member 4
      type "JL255A" mac-address e0071b-c2a520
      priority 128
      link 1 3/25
      link 1 name "I-Link3_1"
      link 2 3/26
      link 2 name "I-Link3_2"
      exit
   port-speed 10g
   exit
encrypt-credentials
include-credentials
no cdp run
dhcp-snooping
no dhcp-snooping option 82
dhcp-snooping vlan 75 100 176 2525 2530-2531 3001

banner motd " "
no banner last-login
no telnet-server
```

```
igmp filter-unknown-mcast

radius-server host 10.5.8.12 key admin
radius-server host 10.5.8.12 dyn-authorization
radius-server host 10.5.8.12 time-window plus-or-minus-time-window
radius-server host 10.5.8.12 time-window 30
radius-server cppm identity "durtest" key aruba123

timesync ntp
ntp unicast
ntp server 10.80.2.219 iburst
ntp enable

time daylight-time-rule continental-us-and-canada
time timezone -360
no web-management

ip dns domain-name tmelab.net
ip dns server-address priority 1 10.80.2.219

ip source-interface tacacs vlan 1055
ip source-interface radius vlan 1055
ip source-interface syslog vlan 1055
ip source-interface telnet vlan 1055
ip source-interface tftp vlan 1055
ip source-interface sntp vlan 1055
ip source-interface sflow vlan 1055
ip source-interface tunneled-node-server vlan 1055
ip client-tracker

tunneled-node-server
   controller-ip 10.5.8.6
   mode role-based reserved-vlan 1000
   exit
%if vsf_number=1%
trunk 1/3,1/4 trk1 lacp
interface 1/3,1/4 name "Uplink"
%endif%

%if vsf_number>1%
trunk 1/27,2/51 trk1 lacp
interface 1/27,2/51 name "Uplink"
%endif%

interface Trk1 dhcp-snooping trust

%if member1_portcount=48%
interface 1/1-1/48 rate-limit bcast in percent 80
interface 1/1-1/48 rate-limit mcast in percent 80
interface 1/1-1/48 rate-limit unknown-unicast in percent 80
interface 1/1-1/48 untagged vlan 10
aaa port-access lldp-bypass 1/1-1/48
```

```
%else%
interface 1/1-1/22 rate-limit bcast in percent 80
interface 1/1-1/22 rate-limit mcast in percent 80
interface 1/1-1/22 rate-limit unknown-unicast in percent 80
interface 1/1-1/22 untagged vlan 10
%endif%

%if vsf_number>1%
%if member2_portcount=48%
interface 2/1-2/46 rate-limit bcast in percent 80
interface 2/1-2/46 rate-limit mcast in percent 80
interface 2/1-2/46 rate-limit unknown-unicast in percent 80
interface 2/1-2/46 untagged vlan 2525
aaa port-access authenticator 2/1-2/46
aaa port-access authenticator 2/1-2/46 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 2/1-2/46
aaa port-access mac-based 2/1-2/46 addr-limit 32
aaa port-access lldp-bypass 2/1-2/46
spanning-tree 2/1-2/46 bpdu-protection
%else%
interface 2/1-2/24 rate-limit bcast in percent 80
interface 2/1-2/24 rate-limit mcast in percent 80
interface 2/1-2/24 rate-limit unknown-unicast in percent 80
interface 2/1-2/24 untagged vlan 2525
aaa port-access authenticator 2/1-2/24
aaa port-access authenticator 2/1-2/24 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 2/1-2/24
aaa port-access mac-based 2/1-2/24 addr-limit 32
aaa port-access lldp-bypass 2/1-2/24
spanning-tree 2/1-2/24 bpdu-protection
%endif%
%endif%

snmp-server community "public" unrestricted

aaa server-group radius "CPPM" host 10.5.8.12
aaa authorization user-role enable download

vlan 1
   name "DEFAULT_VLAN"
%if use_dhcp=1%
   ip address dhcp-bootp
%endif%
%if use_dhcp=0%
   ip address %ip_address% %netmask%
%endif%
   ipv6 enable
%if use_ipv6_dhcp=1%
   ipv6 address dhcp full
%endif%
```

```
%if use_ipv6_dhcp=0%
   ipv6 address %ipv6_address%/%ipv6_prefix_length%
%endif%
   exit
vlan 10
   name "Management"
   untagged Trk1
   ip address %vlan10_ip% %subnet_mask%
   ip igmp
   jumbo
   exit
vlan 513
   name "GUEST"
   no ip address
   ip igmp
   jumbo
   exit
vlan 1000
   name "TUNNELED_NODE_SERVER_RESERVED"
   no ip address
   exit
vlan 2525
   tagged Trk1
   no ip address
   ip igmp
   ipv6 mld enable
   jumbo
   exit
vlan 2530
   tagged Trk1
   ip igmp
   jumbo
   exit
vlan 2531
   tagged Trk1
   ip igmp
   jumbo
   exit

spanning-tree
spanning-tree bpdu-protection-timeout 90

mac-delimiter colon

no tftp server
no autorun
no dhcp config-file-update
no dhcp image-file-update

trunk-load-balance L4-based

device-profile name "ARUBA-AP"
```

```
   untagged-vlan 10
   allow-jumbo-frames
   no allow-tunneled-node
   exit
device-profile type "aruba-ap"
   associate "ARUBA-AP"
   enable
   exit

ip default-gateway %default_gw%

primary-vlan 10
activate provision disable
allow-unsupported-transceiver
```

Sample Backplane Stack TFTP Config

```
; hpStack_WC Configuration Editor; Created on release #WC.16.08.0003
; Ver #14:27.6f.f8.1d.9b.3f.bf.bb.ef.7c.59.fc.6b.fb.9f.fc.ff.ff.37.ef:04

stacking
   member 1 type "JL324A" mac-address 9c:dc:71:fc:17:c0
   member 1 priority 255
   member 2 type "JL320A" mac-address f4:03:43:d2:34:00
   member 2 flexible-module A type JL083A
   member 3 type "R0M68A" mac-address b8:83:03:de:38:c0
   member 3 priority 200
   member 4 type "R0M67A" mac-address b8:83:03:de:8c:00
   member 4 flexible-module A type JL083A
   exit
hostname "2930M-Stack"
no cdp run
dhcp-snooping
no dhcp-snooping option 82
dhcp-snooping vlan 75 100 176 2525 2530-2531 3001
trunk 2/A4,4/A4 trk1 lacp
banner motd " "
no banner last-login
igmp filter-unknown-mcast
radius-server host 10.5.8.12 key admin123
radius-server host 10.5.8.12 dyn-authorization
radius-server host 10.5.8.12 time-window plus-or-minus-time-window
radius-server host 10.5.8.12 time-window 30
radius-server cppm identity "durtest" key admin123
timesync ntp
ntp unicast
ntp server 10.80.2.219 iburst
ntp enable
no telnet-server
time daylight-time-rule continental-us-and-canada
time timezone -360
no web-management
ip default-gateway 10.6.5.1
ip dns domain-name "tmelab.net"
ip dns server-address priority 1 10.80.2.219
ip source-interface tacacs vlan 1055
ip source-interface radius vlan 1055
ip source-interface syslog vlan 1055
ip source-interface telnet vlan 1055
ip source-interface tftp vlan 1055
ip source-interface sntp vlan 1055
ip source-interface sflow vlan 1055
ip source-interface tunneled-node-server vlan 1055
ip client-tracker
tunneled-node-server
   controller-ip 10.5.8.6
```

```
   mode role-based reserved-vlan 1000
   exit
interface 1/3
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/4
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/5
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/6
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/7
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/8
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/9
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/10
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/11
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/12
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
```

```
interface 1/13
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/14
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/15
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/16
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/17
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/18
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/19
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/20
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/21
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/22
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/23
   rate-limit bcast in percent 80
```

```
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/24
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/1
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/2
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/3
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/4
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/5
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/6
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/7
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/8
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/9
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
```

```
   exit
interface 2/10
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/11
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/12
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/13
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/14
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/15
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/16
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/17
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/18
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/19
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/20
```

```
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/21
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/22
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/23
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/24
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/A1
   disable
   exit
interface 2/A2
   disable
   exit
interface 2/A3
   disable
   exit
interface 2/A4
   name "Uplink"
   exit
interface 3/1
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/2
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/3
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/4
```

```
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/5
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/6
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/7
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/8
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/9
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/10
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/11
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/12
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/13
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/14
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
```

```
   rate-limit unknown-unicast in percent 80
   exit
interface 3/15
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/16
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/17
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/18
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/19
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/20
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/21
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/22
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/23
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/24
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
```

```
interface 4/1
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/2
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/3
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/4
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/5
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/6
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/7
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/8
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/9
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/10
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/11
   rate-limit bcast in percent 80
```

```
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/12
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/13
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/14
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/15
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/16
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/17
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/18
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/19
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/20
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/21
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
```

```
   exit
interface 4/22
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/23
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/24
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/25
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/26
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/27
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/28
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/29
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/30
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/31
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/32
```

```
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/33
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/34
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/35
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/36
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/37
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/38
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/39
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/40
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/41
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/42
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
```

```
   rate-limit unknown-unicast in percent 80
   exit
interface 4/43
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/44
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/45
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/46
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/47
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/48
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 4/A1
   disable
   exit
interface 4/A2
   disable
   exit
interface 4/A3
   disable
   exit
interface 4/A4
   name "Uplink"
   exit
interface Trk1
   dhcp-snooping trust
   exit
snmp-server community "public" unrestricted
aaa server-group radius "CPPM" host 10.5.8.12
aaa authorization user-role enable download
aaa port-access authenticator 1/3-1/23,2/1-2/24,3/1-3/24,4/1-4/48
aaa port-access authenticator 1/3 client-limit 32
```

```
aaa port-access authenticator 1/4 client-limit 32
aaa port-access authenticator 1/5 client-limit 32
aaa port-access authenticator 1/6 client-limit 32
aaa port-access authenticator 1/7 client-limit 32
aaa port-access authenticator 1/8 client-limit 32
aaa port-access authenticator 1/9 client-limit 32
aaa port-access authenticator 1/10 client-limit 32
aaa port-access authenticator 1/11 client-limit 32
aaa port-access authenticator 1/12 client-limit 32
aaa port-access authenticator 1/13 client-limit 32
aaa port-access authenticator 1/14 client-limit 32
aaa port-access authenticator 1/15 client-limit 32
aaa port-access authenticator 1/16 client-limit 32
aaa port-access authenticator 1/17 client-limit 32
aaa port-access authenticator 1/18 client-limit 32
aaa port-access authenticator 1/19 client-limit 32
aaa port-access authenticator 1/20 client-limit 32
aaa port-access authenticator 1/21 client-limit 32
aaa port-access authenticator 1/22 client-limit 32
aaa port-access authenticator 1/23 client-limit 32
aaa port-access authenticator 2/1 client-limit 32
aaa port-access authenticator 2/2 client-limit 32
aaa port-access authenticator 2/3 client-limit 32
aaa port-access authenticator 2/4 client-limit 32
aaa port-access authenticator 2/5 client-limit 32
aaa port-access authenticator 2/6 client-limit 32
aaa port-access authenticator 2/7 client-limit 32
aaa port-access authenticator 2/8 client-limit 32
aaa port-access authenticator 2/9 client-limit 32
aaa port-access authenticator 2/10 client-limit 32
aaa port-access authenticator 2/11 client-limit 32
aaa port-access authenticator 2/12 client-limit 32
aaa port-access authenticator 2/13 client-limit 32
aaa port-access authenticator 2/14 client-limit 32
aaa port-access authenticator 2/15 client-limit 32
aaa port-access authenticator 2/16 client-limit 32
aaa port-access authenticator 2/17 client-limit 32
aaa port-access authenticator 2/18 client-limit 32
aaa port-access authenticator 2/19 client-limit 32
aaa port-access authenticator 2/20 client-limit 32
aaa port-access authenticator 2/21 client-limit 32
aaa port-access authenticator 2/22 client-limit 32
aaa port-access authenticator 2/23 client-limit 32
aaa port-access authenticator 2/24 client-limit 32
aaa port-access authenticator 3/1 client-limit 32
aaa port-access authenticator 3/2 client-limit 32
aaa port-access authenticator 3/3 client-limit 32
aaa port-access authenticator 3/4 client-limit 32
aaa port-access authenticator 3/5 client-limit 32
aaa port-access authenticator 3/6 client-limit 32
aaa port-access authenticator 3/7 client-limit 32
aaa port-access authenticator 3/8 client-limit 32
```

```
aaa port-access authenticator 3/9 client-limit 32
aaa port-access authenticator 3/10 client-limit 32
aaa port-access authenticator 3/11 client-limit 32
aaa port-access authenticator 3/12 client-limit 32
aaa port-access authenticator 3/13 client-limit 32
aaa port-access authenticator 3/14 client-limit 32
aaa port-access authenticator 3/15 client-limit 32
aaa port-access authenticator 3/16 client-limit 32
aaa port-access authenticator 3/17 client-limit 32
aaa port-access authenticator 3/18 client-limit 32
aaa port-access authenticator 3/19 client-limit 32
aaa port-access authenticator 3/20 client-limit 32
aaa port-access authenticator 3/21 client-limit 32
aaa port-access authenticator 3/22 client-limit 32
aaa port-access authenticator 3/23 client-limit 32
aaa port-access authenticator 3/24 client-limit 32
aaa port-access authenticator 4/1 client-limit 32
aaa port-access authenticator 4/2 client-limit 32
aaa port-access authenticator 4/3 client-limit 32
aaa port-access authenticator 4/4 client-limit 32
aaa port-access authenticator 4/5 client-limit 32
aaa port-access authenticator 4/6 client-limit 32
aaa port-access authenticator 4/7 client-limit 32
aaa port-access authenticator 4/8 client-limit 32
aaa port-access authenticator 4/9 client-limit 32
aaa port-access authenticator 4/10 client-limit 32
aaa port-access authenticator 4/11 client-limit 32
aaa port-access authenticator 4/12 client-limit 32
aaa port-access authenticator 4/13 client-limit 32
aaa port-access authenticator 4/14 client-limit 32
aaa port-access authenticator 4/15 client-limit 32
aaa port-access authenticator 4/16 client-limit 32
aaa port-access authenticator 4/17 client-limit 32
aaa port-access authenticator 4/18 client-limit 32
aaa port-access authenticator 4/19 client-limit 32
aaa port-access authenticator 4/20 client-limit 32
aaa port-access authenticator 4/21 client-limit 32
aaa port-access authenticator 4/22 client-limit 32
aaa port-access authenticator 4/23 client-limit 32
aaa port-access authenticator 4/24 client-limit 32
aaa port-access authenticator 4/25 client-limit 32
aaa port-access authenticator 4/26 client-limit 32
aaa port-access authenticator 4/27 client-limit 32
aaa port-access authenticator 4/28 client-limit 32
aaa port-access authenticator 4/29 client-limit 32
aaa port-access authenticator 4/30 client-limit 32
aaa port-access authenticator 4/31 client-limit 32
aaa port-access authenticator 4/32 client-limit 32
aaa port-access authenticator 4/33 client-limit 32
aaa port-access authenticator 4/34 client-limit 32
aaa port-access authenticator 4/35 client-limit 32
aaa port-access authenticator 4/36 client-limit 32
```

```
aaa port-access authenticator 4/37 client-limit 32
aaa port-access authenticator 4/38 client-limit 32
aaa port-access authenticator 4/39 client-limit 32
aaa port-access authenticator 4/40 client-limit 32
aaa port-access authenticator 4/41 client-limit 32
aaa port-access authenticator 4/42 client-limit 32
aaa port-access authenticator 4/43 client-limit 32
aaa port-access authenticator 4/44 client-limit 32
aaa port-access authenticator 4/45 client-limit 32
aaa port-access authenticator 4/46 client-limit 32
aaa port-access authenticator 4/47 client-limit 32
aaa port-access authenticator 4/48 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 1/3-1/23,2/1-2/24,3/1-3/24,4/1-4/48
aaa port-access mac-based 1/3 addr-limit 32
aaa port-access mac-based 1/4 addr-limit 32
aaa port-access mac-based 1/5 addr-limit 32
aaa port-access mac-based 1/6 addr-limit 32
aaa port-access mac-based 1/7 addr-limit 32
aaa port-access mac-based 1/8 addr-limit 32
aaa port-access mac-based 1/9 addr-limit 32
aaa port-access mac-based 1/10 addr-limit 32
aaa port-access mac-based 1/11 addr-limit 32
aaa port-access mac-based 1/12 addr-limit 32
aaa port-access mac-based 1/13 addr-limit 32
aaa port-access mac-based 1/14 addr-limit 32
aaa port-access mac-based 1/15 addr-limit 32
aaa port-access mac-based 1/16 addr-limit 32
aaa port-access mac-based 1/17 addr-limit 32
aaa port-access mac-based 1/18 addr-limit 32
aaa port-access mac-based 1/19 addr-limit 32
aaa port-access mac-based 1/20 addr-limit 32
aaa port-access mac-based 1/21 addr-limit 32
aaa port-access mac-based 1/22 addr-limit 32
aaa port-access mac-based 1/23 addr-limit 32
aaa port-access mac-based 2/1 addr-limit 32
aaa port-access mac-based 2/2 addr-limit 32
aaa port-access mac-based 2/3 addr-limit 32
aaa port-access mac-based 2/4 addr-limit 32
aaa port-access mac-based 2/5 addr-limit 32
aaa port-access mac-based 2/6 addr-limit 32
aaa port-access mac-based 2/7 addr-limit 32
aaa port-access mac-based 2/8 addr-limit 32
aaa port-access mac-based 2/9 addr-limit 32
aaa port-access mac-based 2/10 addr-limit 32
aaa port-access mac-based 2/11 addr-limit 32
aaa port-access mac-based 2/12 addr-limit 32
aaa port-access mac-based 2/13 addr-limit 32
aaa port-access mac-based 2/14 addr-limit 32
aaa port-access mac-based 2/15 addr-limit 32
aaa port-access mac-based 2/16 addr-limit 32
aaa port-access mac-based 2/17 addr-limit 32
```

```
aaa port-access mac-based 2/18 addr-limit 32
aaa port-access mac-based 2/19 addr-limit 32
aaa port-access mac-based 2/20 addr-limit 32
aaa port-access mac-based 2/21 addr-limit 32
aaa port-access mac-based 2/22 addr-limit 32
aaa port-access mac-based 2/23 addr-limit 32
aaa port-access mac-based 2/24 addr-limit 32
aaa port-access mac-based 3/1 addr-limit 32
aaa port-access mac-based 3/2 addr-limit 32
aaa port-access mac-based 3/3 addr-limit 32
aaa port-access mac-based 3/4 addr-limit 32
aaa port-access mac-based 3/5 addr-limit 32
aaa port-access mac-based 3/6 addr-limit 32
aaa port-access mac-based 3/7 addr-limit 32
aaa port-access mac-based 3/8 addr-limit 32
aaa port-access mac-based 3/9 addr-limit 32
aaa port-access mac-based 3/10 addr-limit 32
aaa port-access mac-based 3/11 addr-limit 32
aaa port-access mac-based 3/12 addr-limit 32
aaa port-access mac-based 3/13 addr-limit 32
aaa port-access mac-based 3/14 addr-limit 32
aaa port-access mac-based 3/15 addr-limit 32
aaa port-access mac-based 3/16 addr-limit 32
aaa port-access mac-based 3/17 addr-limit 32
aaa port-access mac-based 3/18 addr-limit 32
aaa port-access mac-based 3/19 addr-limit 32
aaa port-access mac-based 3/20 addr-limit 32
aaa port-access mac-based 3/21 addr-limit 32
aaa port-access mac-based 3/22 addr-limit 32
aaa port-access mac-based 3/23 addr-limit 32
aaa port-access mac-based 3/24 addr-limit 32
aaa port-access mac-based 4/1 addr-limit 32
aaa port-access mac-based 4/2 addr-limit 32
aaa port-access mac-based 4/3 addr-limit 32
aaa port-access mac-based 4/4 addr-limit 32
aaa port-access mac-based 4/5 addr-limit 32
aaa port-access mac-based 4/6 addr-limit 32
aaa port-access mac-based 4/7 addr-limit 32
aaa port-access mac-based 4/8 addr-limit 32
aaa port-access mac-based 4/9 addr-limit 32
aaa port-access mac-based 4/10 addr-limit 32
aaa port-access mac-based 4/11 addr-limit 32
aaa port-access mac-based 4/12 addr-limit 32
aaa port-access mac-based 4/13 addr-limit 32
aaa port-access mac-based 4/14 addr-limit 32
aaa port-access mac-based 4/15 addr-limit 32
aaa port-access mac-based 4/16 addr-limit 32
aaa port-access mac-based 4/17 addr-limit 32
aaa port-access mac-based 4/18 addr-limit 32
aaa port-access mac-based 4/19 addr-limit 32
aaa port-access mac-based 4/20 addr-limit 32
aaa port-access mac-based 4/21 addr-limit 32
```

```
aaa port-access mac-based 4/22 addr-limit 32
aaa port-access mac-based 4/23 addr-limit 32
aaa port-access mac-based 4/24 addr-limit 32
aaa port-access mac-based 4/25 addr-limit 32
aaa port-access mac-based 4/26 addr-limit 32
aaa port-access mac-based 4/27 addr-limit 32
aaa port-access mac-based 4/28 addr-limit 32
aaa port-access mac-based 4/29 addr-limit 32
aaa port-access mac-based 4/30 addr-limit 32
aaa port-access mac-based 4/31 addr-limit 32
aaa port-access mac-based 4/32 addr-limit 32
aaa port-access mac-based 4/33 addr-limit 32
aaa port-access mac-based 4/34 addr-limit 32
aaa port-access mac-based 4/35 addr-limit 32
aaa port-access mac-based 4/36 addr-limit 32
aaa port-access mac-based 4/37 addr-limit 32
aaa port-access mac-based 4/38 addr-limit 32
aaa port-access mac-based 4/39 addr-limit 32
aaa port-access mac-based 4/40 addr-limit 32
aaa port-access mac-based 4/41 addr-limit 32
aaa port-access mac-based 4/42 addr-limit 32
aaa port-access mac-based 4/43 addr-limit 32
aaa port-access mac-based 4/44 addr-limit 32
aaa port-access mac-based 4/45 addr-limit 32
aaa port-access mac-based 4/46 addr-limit 32
aaa port-access mac-based 4/47 addr-limit 32
aaa port-access mac-based 4/48 addr-limit 32
aaa port-access lldp-bypass 2/1-2/24,3/1-3/24,4/1-4/48
oobm
   ip address dhcp-bootp
   member 1
      ip address dhcp-bootp
      exit
   member 2
      ip address dhcp-bootp
      exit
   member 3
      ip address dhcp-bootp
      exit
   member 4
      ip address dhcp-bootp
      exit
   exit
vlan 1
   name "DEFAULT_VLAN"
   no untagged 1/3-1/24,2/1-2/24,3/1-3/24,4/1-4/48,Trk1
   untagged 1/1-1/2,2/A1-2/A3,4/A1-4/A3
   no ip address
   ip igmp
   jumbo
   exit
vlan 10
```

```
   name "Management"
   untagged 1/3-1/24,Trk1
   ip address 10.6.5.25 255.255.255.0
   ip igmp
   jumbo
   exit
vlan 513
   name "GUEST"
   no ip address
   ip igmp
   jumbo
   exit
vlan 1000
   name "TUNNELED_NODE_SERVER_RESERVED"
   no ip address
   exit
vlan 2525
   name "VLAN2525"
   untagged 2/1-2/24,3/1-3/24,4/1-4/48
   tagged Trk1
   no ip address
   ip igmp
   ipv6 mld enable
   jumbo
   exit
vlan 2530
   name "VLAN2530"
   tagged Trk1
   no ip address
   ip igmp
   jumbo
   exit
vlan 2531
   name "VLAN2531"
   tagged Trk1
   no ip address
   ip igmp
   jumbo
   exit
primary-vlan 10
spanning-tree
spanning-tree 2/1 bpdu-protection
spanning-tree 2/2 bpdu-protection
spanning-tree 2/3 bpdu-protection
spanning-tree 2/4 bpdu-protection
spanning-tree 2/5 bpdu-protection
spanning-tree 2/6 bpdu-protection
spanning-tree 2/7 bpdu-protection
spanning-tree 2/8 bpdu-protection
spanning-tree 2/9 bpdu-protection
spanning-tree 2/10 bpdu-protection
spanning-tree 2/11 bpdu-protection
```

```
spanning-tree 2/12 bpdu-protection
spanning-tree 2/13 bpdu-protection
spanning-tree 2/14 bpdu-protection
spanning-tree 2/15 bpdu-protection
spanning-tree 2/16 bpdu-protection
spanning-tree 2/17 bpdu-protection
spanning-tree 2/18 bpdu-protection
spanning-tree 2/19 bpdu-protection
spanning-tree 2/20 bpdu-protection
spanning-tree 2/21 bpdu-protection
spanning-tree 2/22 bpdu-protection
spanning-tree 2/23 bpdu-protection
spanning-tree 2/24 bpdu-protection
spanning-tree 3/1 bpdu-protection
spanning-tree 3/2 bpdu-protection
spanning-tree 3/3 bpdu-protection
spanning-tree 3/4 bpdu-protection
spanning-tree 3/5 bpdu-protection
spanning-tree 3/6 bpdu-protection
spanning-tree 3/7 bpdu-protection
spanning-tree 3/8 bpdu-protection
spanning-tree 3/9 bpdu-protection
spanning-tree 3/10 bpdu-protection
spanning-tree 3/11 bpdu-protection
spanning-tree 3/12 bpdu-protection
spanning-tree 3/13 bpdu-protection
spanning-tree 3/14 bpdu-protection
spanning-tree 3/15 bpdu-protection
spanning-tree 3/16 bpdu-protection
spanning-tree 3/17 bpdu-protection
spanning-tree 3/18 bpdu-protection
spanning-tree 3/19 bpdu-protection
spanning-tree 3/20 bpdu-protection
spanning-tree 3/21 bpdu-protection
spanning-tree 3/22 bpdu-protection
spanning-tree 3/23 bpdu-protection
spanning-tree 3/24 bpdu-protection
spanning-tree 4/1 bpdu-protection
spanning-tree 4/2 bpdu-protection
spanning-tree 4/3 bpdu-protection
spanning-tree 4/4 bpdu-protection
spanning-tree 4/5 bpdu-protection
spanning-tree 4/6 bpdu-protection
spanning-tree 4/7 bpdu-protection
spanning-tree 4/8 bpdu-protection
spanning-tree 4/9 bpdu-protection
spanning-tree 4/10 bpdu-protection
spanning-tree 4/11 bpdu-protection
spanning-tree 4/12 bpdu-protection
spanning-tree 4/13 bpdu-protection
spanning-tree 4/14 bpdu-protection
spanning-tree 4/15 bpdu-protection
```

```
spanning-tree 4/16 bpdu-protection
spanning-tree 4/17 bpdu-protection
spanning-tree 4/18 bpdu-protection
spanning-tree 4/19 bpdu-protection
spanning-tree 4/20 bpdu-protection
spanning-tree 4/21 bpdu-protection
spanning-tree 4/22 bpdu-protection
spanning-tree 4/23 bpdu-protection
spanning-tree 4/24 bpdu-protection
spanning-tree 4/25 bpdu-protection
spanning-tree 4/26 bpdu-protection
spanning-tree 4/27 bpdu-protection
spanning-tree 4/28 bpdu-protection
spanning-tree 4/29 bpdu-protection
spanning-tree 4/30 bpdu-protection
spanning-tree 4/31 bpdu-protection
spanning-tree 4/32 bpdu-protection
spanning-tree 4/33 bpdu-protection
spanning-tree 4/34 bpdu-protection
spanning-tree 4/35 bpdu-protection
spanning-tree 4/36 bpdu-protection
spanning-tree 4/37 bpdu-protection
spanning-tree 4/38 bpdu-protection
spanning-tree 4/39 bpdu-protection
spanning-tree 4/40 bpdu-protection
spanning-tree 4/41 bpdu-protection
spanning-tree 4/42 bpdu-protection
spanning-tree 4/43 bpdu-protection
spanning-tree 4/44 bpdu-protection
spanning-tree 4/45 bpdu-protection
spanning-tree 4/46 bpdu-protection
spanning-tree 4/47 bpdu-protection
spanning-tree 4/48 bpdu-protection
spanning-tree Trk1 priority 4
spanning-tree bpdu-protection-timeout 90
allow-unsupported-transceiver
no tftp server
no autorun
no dhcp config-file-update
no dhcp image-file-update
trunk-load-balance L4-based
device-profile name "ARUBA-AP"
   untagged-vlan 10
   allow-jumbo-frames
   no allow-tunneled-node
   exit
device-profile type "aruba-ap"
   associate "ARUBA-AP"
   enable
   exit
activate provision disable
mac-delimiter colon
```

Sample VSF TFTP Config

```
; hpStack_WC Configuration Editor; Created on release #WC.16.08.0003
; Ver #14:27.6f.f8.1d.9b.3f.bf.bb.ef.7c.59.fc.6b.fb.9f.fc.ff.ff.37.ef:04
; encrypt-cred pYHWt1OD++qupvpLqM780tJzwww14b6SuUlFTtyDA+5KBdUchg/ZZy0MFxbdhNDg
hostname "Aruba-VSF-2930F"
vsf
   enable domain 1000
   member 1
      type "JL256A" mac-address f4:03:43:f6:c8:00
      priority 255
      link 1 1/49
      link 1 name "I-Link1_1"
      link 2 1/50
      link 2 name "I-Link1_2"
      exit
   member 2
      type "JL255A" mac-address e0:07:1b:c2:65:20
      priority 128
      link 1 2/25
      link 1 name "I-Link2_1"
      link 2 2/26
      link 2 name "I-Link2_2"
      exit
   member 3
      type "JL255A" mac-address e0:07:1b:c2:05:00
      priority 200
      link 1 3/25
      link 1 name "I-Link3_1"
      link 2 3/26
      link 2 name "I-Link3_2"
      exit
   member 4
      type "JL255A" mac-address e0:07:1b:c2:a5:20
      priority 128
      link 1 4/25
      link 1 name "I-Link4_1"
      link 2 4/26
      link 2 name "I-Link4_2"
      exit
   port-speed 10g
   exit
encrypt-credentials
no cdp run
dhcp-snooping
no dhcp-snooping option 82
dhcp-snooping vlan 75 100 176 2525 2530-2531 3001
trunk 1/52,3/28 trk1 lacp
banner motd " "
no banner last-login
igmp filter-unknown-mcast
include-credentials
```

```
radius-server host 10.5.8.12 encrypted-key "lBVPrvdSyf0Q2rZ1vtV3YmhGiDTZWAbVPRT3dk21KOU="
radius-server host 10.5.8.12 dyn-authorization
radius-server host 10.5.8.12 time-window plus-or-minus-time-window
radius-server host 10.5.8.12 time-window 30
radius-server cppm identity "durtest" encrypted-key
"RhBwjrAcpkmsVQr8hcjtX4b3riAaUogyW3MS+8tO1lY="
timesync ntp
ntp unicast
ntp server 10.80.2.219 iburst
ntp enable
no telnet-server
time daylight-time-rule continental-us-and-canada
time timezone -360
no web-management
ip default-gateway 10.5.6.1
ip dns domain-name "tmelab.net"
ip dns server-address priority 1 10.80.2.219
ip source-interface tacacs vlan 1055
ip source-interface radius vlan 1055
ip source-interface syslog vlan 1055
ip source-interface telnet vlan 1055
ip source-interface tftp vlan 1055
ip source-interface sntp vlan 1055
ip source-interface sflow vlan 1055
ip source-interface tunneled-node-server vlan 1055
ip client-tracker
tunneled-node-server
   controller-ip 10.5.8.6
   mode role-based reserved-vlan 1000
   exit
interface 1/1
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/2
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/3
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/4
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/5
   rate-limit bcast in percent 80
```

```
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/6
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/7
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/8
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/9
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/10
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/11
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/12
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/13
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/14
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/15
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
```

```
   exit
interface 1/16
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/17
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/18
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/19
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/20
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/21
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/22
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/23
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/24
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/25
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/26
```

```
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/27
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/28
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/29
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/30
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/31
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/32
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/33
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/34
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/35
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/36
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
```

```
   rate-limit unknown-unicast in percent 80
   exit
interface 1/37
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/38
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/39
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/40
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/41
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/42
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/43
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/44
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/45
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/46
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
```

```
interface 1/47
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/48
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 1/52
   name "Uplink"
   exit
interface 2/1
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/2
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/3
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/4
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/5
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/6
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/7
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/8
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
```

```
   exit
interface 2/9
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/10
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/11
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/12
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/13
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/14
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/15
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/16
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/17
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/18
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/19
```

```
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/20
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/21
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/22
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/23
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 2/24
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/1
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/2
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/3
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/4
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/5
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
```

```
   rate-limit unknown-unicast in percent 80
   exit
interface 3/6
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/7
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/8
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/9
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/10
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/11
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/12
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/13
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/14
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/15
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
```

```
interface 3/16
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/17
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/18
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/19
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/20
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/21
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/22
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/23
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/24
   rate-limit bcast in percent 80
   rate-limit mcast in percent 80
   rate-limit unknown-unicast in percent 80
   exit
interface 3/28
   name "Uplink"
   exit
interface Trk1
   dhcp-snooping trust
   exit
snmp-server community "public" unrestricted
```

```
snmpv3 engineid "00:00:00:0b:00:00:f4:03:43:f6:c8:0a"
aaa server-group radius "CPPM" host 10.5.8.12
aaa authorization user-role enable download
aaa port-access authenticator 1/2-1/48,2/1-2/24,3/1-3/24
aaa port-access authenticator 1/2 client-limit 32
aaa port-access authenticator 1/3 client-limit 32
aaa port-access authenticator 1/4 client-limit 32
aaa port-access authenticator 1/5 client-limit 32
aaa port-access authenticator 1/6 client-limit 32
aaa port-access authenticator 1/7 client-limit 32
aaa port-access authenticator 1/8 client-limit 32
aaa port-access authenticator 1/9 client-limit 32
aaa port-access authenticator 1/10 client-limit 32
aaa port-access authenticator 1/11 client-limit 32
aaa port-access authenticator 1/12 client-limit 32
aaa port-access authenticator 1/13 client-limit 32
aaa port-access authenticator 1/14 client-limit 32
aaa port-access authenticator 1/15 client-limit 32
aaa port-access authenticator 1/16 client-limit 32
aaa port-access authenticator 1/17 client-limit 32
aaa port-access authenticator 1/18 client-limit 32
aaa port-access authenticator 1/19 client-limit 32
aaa port-access authenticator 1/20 client-limit 32
aaa port-access authenticator 1/21 client-limit 32
aaa port-access authenticator 1/22 client-limit 32
aaa port-access authenticator 1/23 client-limit 32
aaa port-access authenticator 1/24 client-limit 32
aaa port-access authenticator 1/25 client-limit 32
aaa port-access authenticator 1/26 client-limit 32
aaa port-access authenticator 1/27 client-limit 32
aaa port-access authenticator 1/28 client-limit 32
aaa port-access authenticator 1/29 client-limit 32
aaa port-access authenticator 1/30 client-limit 32
aaa port-access authenticator 1/31 client-limit 32
aaa port-access authenticator 1/32 client-limit 32
aaa port-access authenticator 1/33 client-limit 32
aaa port-access authenticator 1/34 client-limit 32
aaa port-access authenticator 1/35 client-limit 32
aaa port-access authenticator 1/36 client-limit 32
aaa port-access authenticator 1/37 client-limit 32
aaa port-access authenticator 1/38 client-limit 32
aaa port-access authenticator 1/39 client-limit 32
aaa port-access authenticator 1/40 client-limit 32
aaa port-access authenticator 1/41 client-limit 32
aaa port-access authenticator 1/42 client-limit 32
aaa port-access authenticator 1/43 client-limit 32
aaa port-access authenticator 1/44 client-limit 32
aaa port-access authenticator 1/45 client-limit 32
aaa port-access authenticator 1/46 client-limit 32
aaa port-access authenticator 1/47 client-limit 32
aaa port-access authenticator 1/48 client-limit 32
aaa port-access authenticator 2/1 client-limit 32
```

```
aaa port-access authenticator 2/2 client-limit 32
aaa port-access authenticator 2/3 client-limit 32
aaa port-access authenticator 2/4 client-limit 32
aaa port-access authenticator 2/5 client-limit 32
aaa port-access authenticator 2/6 client-limit 32
aaa port-access authenticator 2/7 client-limit 32
aaa port-access authenticator 2/8 client-limit 32
aaa port-access authenticator 2/9 client-limit 32
aaa port-access authenticator 2/10 client-limit 32
aaa port-access authenticator 2/11 client-limit 32
aaa port-access authenticator 2/12 client-limit 32
aaa port-access authenticator 2/13 client-limit 32
aaa port-access authenticator 2/14 client-limit 32
aaa port-access authenticator 2/15 client-limit 32
aaa port-access authenticator 2/16 client-limit 32
aaa port-access authenticator 2/17 client-limit 32
aaa port-access authenticator 2/18 client-limit 32
aaa port-access authenticator 2/19 client-limit 32
aaa port-access authenticator 2/20 client-limit 32
aaa port-access authenticator 2/21 client-limit 32
aaa port-access authenticator 2/22 client-limit 32
aaa port-access authenticator 2/23 client-limit 32
aaa port-access authenticator 2/24 client-limit 32
aaa port-access authenticator 3/1 client-limit 32
aaa port-access authenticator 3/2 client-limit 32
aaa port-access authenticator 3/3 client-limit 32
aaa port-access authenticator 3/4 client-limit 32
aaa port-access authenticator 3/5 client-limit 32
aaa port-access authenticator 3/6 client-limit 32
aaa port-access authenticator 3/7 client-limit 32
aaa port-access authenticator 3/8 client-limit 32
aaa port-access authenticator 3/9 client-limit 32
aaa port-access authenticator 3/10 client-limit 32
aaa port-access authenticator 3/11 client-limit 32
aaa port-access authenticator 3/12 client-limit 32
aaa port-access authenticator 3/13 client-limit 32
aaa port-access authenticator 3/14 client-limit 32
aaa port-access authenticator 3/15 client-limit 32
aaa port-access authenticator 3/16 client-limit 32
aaa port-access authenticator 3/17 client-limit 32
aaa port-access authenticator 3/18 client-limit 32
aaa port-access authenticator 3/19 client-limit 32
aaa port-access authenticator 3/20 client-limit 32
aaa port-access authenticator 3/21 client-limit 32
aaa port-access authenticator 3/22 client-limit 32
aaa port-access authenticator 3/23 client-limit 32
aaa port-access authenticator 3/24 client-limit 32
aaa port-access authenticator active
aaa port-access mac-based 1/2-1/48,2/1-2/24,3/1-3/24
aaa port-access mac-based 1/2 addr-limit 32
aaa port-access mac-based 1/3 addr-limit 32
aaa port-access mac-based 1/4 addr-limit 32
```

```
aaa port-access mac-based 1/5 addr-limit 32
aaa port-access mac-based 1/6 addr-limit 32
aaa port-access mac-based 1/7 addr-limit 32
aaa port-access mac-based 1/8 addr-limit 32
aaa port-access mac-based 1/9 addr-limit 32
aaa port-access mac-based 1/10 addr-limit 32
aaa port-access mac-based 1/11 addr-limit 32
aaa port-access mac-based 1/12 addr-limit 32
aaa port-access mac-based 1/13 addr-limit 32
aaa port-access mac-based 1/14 addr-limit 32
aaa port-access mac-based 1/15 addr-limit 32
aaa port-access mac-based 1/16 addr-limit 32
aaa port-access mac-based 1/17 addr-limit 32
aaa port-access mac-based 1/18 addr-limit 32
aaa port-access mac-based 1/19 addr-limit 32
aaa port-access mac-based 1/20 addr-limit 32
aaa port-access mac-based 1/21 addr-limit 32
aaa port-access mac-based 1/22 addr-limit 32
aaa port-access mac-based 1/23 addr-limit 32
aaa port-access mac-based 1/24 addr-limit 32
aaa port-access mac-based 1/25 addr-limit 32
aaa port-access mac-based 1/26 addr-limit 32
aaa port-access mac-based 1/27 addr-limit 32
aaa port-access mac-based 1/28 addr-limit 32
aaa port-access mac-based 1/29 addr-limit 32
aaa port-access mac-based 1/30 addr-limit 32
aaa port-access mac-based 1/31 addr-limit 32
aaa port-access mac-based 1/32 addr-limit 32
aaa port-access mac-based 1/33 addr-limit 32
aaa port-access mac-based 1/34 addr-limit 32
aaa port-access mac-based 1/35 addr-limit 32
aaa port-access mac-based 1/36 addr-limit 32
aaa port-access mac-based 1/37 addr-limit 32
aaa port-access mac-based 1/38 addr-limit 32
aaa port-access mac-based 1/39 addr-limit 32
aaa port-access mac-based 1/40 addr-limit 32
aaa port-access mac-based 1/41 addr-limit 32
aaa port-access mac-based 1/42 addr-limit 32
aaa port-access mac-based 1/43 addr-limit 32
aaa port-access mac-based 1/44 addr-limit 32
aaa port-access mac-based 1/45 addr-limit 32
aaa port-access mac-based 1/46 addr-limit 32
aaa port-access mac-based 1/47 addr-limit 32
aaa port-access mac-based 1/48 addr-limit 32
aaa port-access mac-based 2/1 addr-limit 32
aaa port-access mac-based 2/2 addr-limit 32
aaa port-access mac-based 2/3 addr-limit 32
aaa port-access mac-based 2/4 addr-limit 32
aaa port-access mac-based 2/5 addr-limit 32
aaa port-access mac-based 2/6 addr-limit 32
aaa port-access mac-based 2/7 addr-limit 32
aaa port-access mac-based 2/8 addr-limit 32
```

```
aaa port-access mac-based 2/9 addr-limit 32
aaa port-access mac-based 2/10 addr-limit 32
aaa port-access mac-based 2/11 addr-limit 32
aaa port-access mac-based 2/12 addr-limit 32
aaa port-access mac-based 2/13 addr-limit 32
aaa port-access mac-based 2/14 addr-limit 32
aaa port-access mac-based 2/15 addr-limit 32
aaa port-access mac-based 2/16 addr-limit 32
aaa port-access mac-based 2/17 addr-limit 32
aaa port-access mac-based 2/18 addr-limit 32
aaa port-access mac-based 2/19 addr-limit 32
aaa port-access mac-based 2/20 addr-limit 32
aaa port-access mac-based 2/21 addr-limit 32
aaa port-access mac-based 2/22 addr-limit 32
aaa port-access mac-based 2/23 addr-limit 32
aaa port-access mac-based 2/24 addr-limit 32
aaa port-access mac-based 3/1 addr-limit 32
aaa port-access mac-based 3/2 addr-limit 32
aaa port-access mac-based 3/3 addr-limit 32
aaa port-access mac-based 3/4 addr-limit 32
aaa port-access mac-based 3/5 addr-limit 32
aaa port-access mac-based 3/6 addr-limit 32
aaa port-access mac-based 3/7 addr-limit 32
aaa port-access mac-based 3/8 addr-limit 32
aaa port-access mac-based 3/9 addr-limit 32
aaa port-access mac-based 3/10 addr-limit 32
aaa port-access mac-based 3/11 addr-limit 32
aaa port-access mac-based 3/12 addr-limit 32
aaa port-access mac-based 3/13 addr-limit 32
aaa port-access mac-based 3/14 addr-limit 32
aaa port-access mac-based 3/15 addr-limit 32
aaa port-access mac-based 3/16 addr-limit 32
aaa port-access mac-based 3/17 addr-limit 32
aaa port-access mac-based 3/18 addr-limit 32
aaa port-access mac-based 3/19 addr-limit 32
aaa port-access mac-based 3/20 addr-limit 32
aaa port-access mac-based 3/21 addr-limit 32
aaa port-access mac-based 3/22 addr-limit 32
aaa port-access mac-based 3/23 addr-limit 32
aaa port-access mac-based 3/24 addr-limit 32
aaa port-access lldp-bypass 1/1-1/48,2/1-2/24,3/1-3/24
vlan 1
   name "DEFAULT_VLAN"
   no untagged 1/1-1/48,2/1-2/24,3/1-3/24,Trk1
   untagged 1/51,2/27-2/28,3/27,4/1-4/24,4/27-4/28
   ip address dhcp-bootp
   ipv6 enable
   ipv6 address dhcp full
   exit
vlan 10
   name "Management"
   untagged 1/1-1/48,Trk1
```

```
   ip address 10.5.6.200 255.255.255.0
   ip igmp
   jumbo
   exit
vlan 513
   name "GUEST"
   no ip address
   ip igmp
   jumbo
   exit
vlan 1000
   name "TUNNELED_NODE_SERVER_RESERVED"
   no ip address
   exit
vlan 2525
   name "VLAN2525"
   untagged 2/1-2/24,3/1-3/24
   tagged Trk1
   no ip address
   ip igmp
   ipv6 mld enable
   jumbo
   exit
vlan 2530
   name "VLAN2530"
   tagged Trk1
   no ip address
   ip igmp
   jumbo
   exit
vlan 2531
   name "VLAN2531"
   tagged Trk1
   no ip address
   ip igmp
   jumbo
   exit
primary-vlan 10
spanning-tree
spanning-tree 2/1 bpdu-protection
spanning-tree 2/2 bpdu-protection
spanning-tree 2/3 bpdu-protection
spanning-tree 2/4 bpdu-protection
spanning-tree 2/5 bpdu-protection
spanning-tree 2/6 bpdu-protection
spanning-tree 2/7 bpdu-protection
spanning-tree 2/8 bpdu-protection
spanning-tree 2/9 bpdu-protection
spanning-tree 2/10 bpdu-protection
spanning-tree 2/11 bpdu-protection
spanning-tree 2/12 bpdu-protection
spanning-tree 2/13 bpdu-protection
```

```
spanning-tree 2/14 bpdu-protection
spanning-tree 2/15 bpdu-protection
spanning-tree 2/16 bpdu-protection
spanning-tree 2/17 bpdu-protection
spanning-tree 2/18 bpdu-protection
spanning-tree 2/19 bpdu-protection
spanning-tree 2/20 bpdu-protection
spanning-tree 2/21 bpdu-protection
spanning-tree 2/22 bpdu-protection
spanning-tree 2/23 bpdu-protection
spanning-tree 2/24 bpdu-protection
spanning-tree 3/1 bpdu-protection
spanning-tree 3/2 bpdu-protection
spanning-tree 3/3 bpdu-protection
spanning-tree 3/4 bpdu-protection
spanning-tree 3/5 bpdu-protection
spanning-tree 3/6 bpdu-protection
spanning-tree 3/7 bpdu-protection
spanning-tree 3/8 bpdu-protection
spanning-tree 3/9 bpdu-protection
spanning-tree 3/10 bpdu-protection
spanning-tree 3/11 bpdu-protection
spanning-tree 3/12 bpdu-protection
spanning-tree 3/13 bpdu-protection
spanning-tree 3/14 bpdu-protection
spanning-tree 3/15 bpdu-protection
spanning-tree 3/16 bpdu-protection
spanning-tree 3/17 bpdu-protection
spanning-tree 3/18 bpdu-protection
spanning-tree 3/19 bpdu-protection
spanning-tree 3/20 bpdu-protection
spanning-tree 3/21 bpdu-protection
spanning-tree 3/22 bpdu-protection
spanning-tree 3/23 bpdu-protection
spanning-tree 3/24 bpdu-protection
spanning-tree Trk1 priority 4
spanning-tree bpdu-protection-timeout 90
allow-unsupported-transceiver
no tftp server
no autorun
no dhcp config-file-update
no dhcp image-file-update
trunk-load-balance L4-based
device-profile name "ARUBA-AP"
   untagged-vlan 10
   allow-jumbo-frames
   no allow-tunneled-node
   exit
device-profile type "aruba-ap"
   associate "ARUBA-AP"
   enable
   exit
```

```
amp-server ip 10.80.2.201 group "2930M-ZTPDemo" folder "Top" secret "admin"
activate provision disable
mac-delimiter colon
```

a Hewlett Packard Enterprise company

www.arubanetworks.com

3333 Scott Blvd. | Santa Clara, CA 95054

1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | info@arubanetworks.com