

# **ARUBA S3500**

# TUNNELED NODE DEMO GUIDE

JUNE 2011

VERSION 1.0

1344 Crossman Ave. Sunnyvale, CA 94089 | p: 408.227.4500 | f: 408.227.4550 | www.arubanetworks.com



# TABLE OF CONTENTS

Aruba S3500	1	
Table of Cont	ents	2
Who is the au	Idience for this demo guide?	3
What exactly	is the tunneled node?	3
What does th	is demo cover?	3
What do I nee	ed for the demo?	3
Overview of a	configuration	4
Topology	5	
Configuration	steps	6
<ol> <li>Config</li> <li>Config</li> </ol>	uration on S3500: uration on 3400 controller:	
Demo steps	16	
Appendix	24	
Reference	25	
S3500 configu 3400 Mobility	uration v controller configuration	



# WHO IS THE AUDIENCE FOR THIS DEMO GUIDE?

This demo guide is intended for System Engineers to demonstrate the tunneled node capability of S3500 series in conjunction with Aruba Mobility Controller to customers.

# WHAT EXACTLY IS THE TUNNELED NODE?

The tunneled node is the one of the *key differentiators* of S3500 in the Enterprise access switch market. Previously known as *Mux* in earlier Aruba platforms and releases, the feature had been re-named as tunneled node. The tunneled node encapsulates incoming packets from end-host in GRE packets and forwards them to the Mobility Controller to be processed further. The controller, upon receiving the GRE packets, strips the GRE header and further processes the packet for additional purposes such as authentication, stateful firewall, and so on. This is how the tunneled node feature enables centralized security policy, authentication, and access control.

To allow additional flexibility, the tunneled node feature is enabled per-port basis. Any traffic coming from nontunneled node interface will be forwarded "normally" without being tunneled to the controller.

# WHAT DOES THIS DEMO COVER?

This demo covers a deployment scenario where a group of ports on the S3500 is enabled with tunneled node and differentiated role to the connected client/supplicant is assigned without any change necessary from the network administrator. A more application-centric way to describe this demo would be a *conference room* scenario. Think of a conference room in customer's network where both employees (customers) and guests/contractors need wired connectivity. A typical solution would be something similar to the following: blue-colored wall jacks are for employees (thus direct connectivity to internal network) while red-colored wall jacks are for the guests/contractors (for Internet access only). This solution obviously would lead to potential security issues as well as additional overhead for every employee to remember which port is set up for whom. The S3500 with tunneled node with Aruba Mobility Controller can authenticate end-hosts and still provide necessary level of security without requiring end-hosts to be connected to specific ports (blue or red). This will demonstrate how the controller can provide different authentication method (802.1X and Captive portal) depending on supplicant/client capability and assign appropriate role such as employee and guest.

# WHAT DO I NEED FOR THE DEMO?

As this demo is designed to be quick-and-concise in a stand-alone format, efforts have been made to reduce the number of required devices to *absolute minimal* with concise configuration with *minimal amount of optional features*. This helps the discussion during the demo to stay focused on intended topics rather than moving the focus to other unrelated topics.

The following list can be referenced in terms of preparation:

- Aruba S3500 Mobility Access switch running the recommended software image. Current recommended image is 7.0.0.0 build 28198, which is the FCS release. The image name is ArubaOS\_S3500\_7.0.0.0\_28198.
- Aruba Mobility Controller this can be either 6000 chassis with M3 module, 3x00 series controller, or 6xx series controller running recommended software image for tunneled node server functionality (651 controller in the Demo kit for SEs can be used here). Current recommended image is 6.1.1.0 build 28288. The image name is ArubaOS\_MMC\_6.1.1.0\_28288 or ArubaOS\_6xx\_6.1.1.0\_28288 for 6xx series controller. If 6xx series controller is to be used, then scalability needs to be kept in mind in case this demo set-up is left on-site as an evaluation test-bed for customers. Refer to the appendix for scalability numbers.



- For this demo, AP license is required for the Mobility controller as each S3500 will consume one AP license. S3500 itself does not require any license for tunneled node feature. In addition, if there are any additional requirements, additional licenses such as PEF and WIP would be required.
- Laptop with 802.1X capability and a web browser for captive portal functionality. Ideally, two laptops could be used (one with 802.1X and the other without), but in order to reduce the number of required equipment, one laptop can be used by turning on/off the 802.1X supplicant functionality.

# **OVERVIEW OF CONFIGURATION**

In terms of configuration, 802.1X and captive portal will be configured and enabled on the controller. The controller will have two roles defined for end-host: employee (authenticated) and guest (guest). Depending on the authentication method supported by the end-host, either method will be utilized to allow the user to get on the network with appropriate role:

Role	Authentication method
Employee (authenticated)	802.1X
Guest (guest)	Captive portal (Web)

<u>Key Point</u> The S3500 needs to be configured for tunneled node only. All authentication process/configuration takes place on the controller. The S3500 is only providing the tunnel (GRE) functionality.

For testing the set-up, a laptop can be connected to the interface with tunneled node configured.

In terms of 802.1X, termination mode will be used on the controller to streamline the demo without requiring additional piece of equipment (i.e. external RADIUS server). If usage of external authentication server is desired, then non-termination mode can be used with external authentication server.

DHCP pool will also be configured on the controller for the end-host. To show differentiated roles, each role will be using a different DHPC pool (subnets).

Lastly, the configuration provided in this document can be modified to accommodate any necessary changes per customer requirements such as IP addressing, physical interface, etc. For additional information on the configuration, please refer to the ArubaOS 7.0 S3500 Mobility Access Switch User Guide.



# **TOPOLOGY**





# **CONFIGURATION STEPS**

## 1. Configuration on S3500:

## Step 0 (optional): Clearing the configuration on the S3500

This configuration assumes that the S3500 does not have any existing configuration (i.e. write erase had been performed). If this has not been done already, configuration can be erased by using write erase command, then rebooting the unit. Once the S3500 reboots, quick-setup can be skipped.

If write erase and reboot was performed, admin password needs to be changed in order to save the configuration. The admin password can be changed using the following password:

```
(ArubaS3500) (config) #mgmt-user admin root
```

Password: <password>

```
Re-Type password:<password>
```

## Step 1: Basic configuration including IP address and VLAN

Start by configuring the IP address of VLAN for connectivity and the guest VLAN (999). We will use VLAN 1 for sole purpose to make the demo as simple as possible. Default gateway configuration is included as a reference and not required for this demo.

```
(ArubaS3500) (config) #interface vlan 1
(ArubaS3500) (vlan "1") #ip address 172.16.0.100 netmask 255.255.255.0
(ArubaS3500) (vlan "1") #exit
(ArubaS3500) (config) #ip-profile
(ArubaS3500) (ip-profile) #default-gateway 172.16.0.254
(ArubaS3500) (ip-profile) #exit
(ArubaS3500) (config) #vlan 999
(ArubaS3500) (VLAN "999") #description CONTROLLER_VLAN_999
(ArubaS3500) (VLAN "999") #exit
```

VLANs

VLANS		
ID	Description	
1	VLAN0001	*
999	CONTROLLER_VLAN_999	E
4086	MUX Internal VLAN	
4087	MUX Internal VLAN	-



Optional: By default, all interfaces belong to VLAN 1. Following configuration is being provided as reference only:

```
(ArubaS3500) (config) #interface-profile switching-profile VLAN1
(ArubaS3500) (switching profile "VLAN1") #access-vlan 1
(ArubaS3500) (switching profile "VLAN1") #exit
(ArubaS3500) (config) #interface gigabitethernet 0/0/0
(ArubaS3500) (gigabitethernet "0/0/0") #switching-profile VLAN1
(ArubaS3500) (gigabitethernet "0/0/0") #exit
```

Step 2: Configuring the interface profiles for switching and tunneled node to be applied to the tunneled node interfaces

```
(ArubaS3500) (config) #interface-profile switching-profile
CONTROLLER_VLAN_999
(ArubaS3500) (switching profile "CONTROLLER_VLAN_999") #access-vlan 999
(ArubaS3500) (switching profile "CONTROLLER_VLAN_999") #exit
(ArubaS3500) (config) #interface-profile tunneled-node-profile TUNNELED_NODE
(ArubaS3500) (tunneled Node Server profile "TUNNELED_NODE") #controller-ip
172.16.0.254
(ArubaS3500) (Tunneled Node Server profile "TUNNELED NODE") #exit
```

**Basic Info** 

Name:	ArubaS3500							
Password for user "Admin":	•••••			6-32	cha	rac	ters	
Retype:	•••••							
Password for Enable Mode:	•••••			6-15	i cha	rac	ters	
Retype:	•••••							
Tunneled Server IP Address :	172.16.0.254	1						
Date & Time:	<ul><li>C Get time</li><li>Get time</li></ul>	from N manua	TP S	erver				
	Date :	May	•	25	•		2011	
	Time :	01	• :	15	•	:	31	•
	Timezone:	GMT ·	-08:0	0 +		PST	r]	



## Step 3: Applying the configured switching and tunneled node profiles

Define the interface group to include interfaces from 0/0/1 - 0/0/9 where end-host(s) will be connected during the actual demo, then apply the configured interface profiles.

```
(ArubaS3500) (config) #interface-group gigabitethernet TUNNELED_NODE_DEMO
(ArubaS3500) (gigabitethernet "TUNNELED_NODE_DEMO") #apply-to 0/0/1-0/0/9
(ArubaS3500) (gigabitethernet "TUNNELED_NODE_DEMO") #tunneled-node-profile
TUNNELED_NODE
(ArubaS3500) (gigabitethernet "TUNNELED_NODE_DEMO") #switching-profile
CONTROLLER VLAN 999
```

#### Ports

Switching	QoS	Ethernet	PoE	Port Channel								
Profiles												
Name		Switch mode	e	Access VLAN	Native VL	AN	Allowed VLAN	A	Association			
CONTROLLE	R_V	access	-	999	<b>v</b> 1	-	1-4094	*				
default		access		1	1		1-4094		All Ports:		Selected:	_
VLAN1		access		1	1		1-4094		GE-0/0/0 GE-0/0/10 GE-0/0/11 GE-0/0/12	< >	GE-0/0/1 GE-0/0/2 GE-0/0/3 GE-0/0/4	
New	Delete								GE-0/0/13 GE-0/0/14 GE-0/0/15 GE-0/0/16 GE-0/0/17 GE-0/0/18	« »	GE-0/0/5 GE-0/0/6 GE-0/0/7 GE-0/0/8 GE-0/0/9	
Port	Descr	iption	Admi	in Forwarding Mod	le Trusted	PoE	Speed/Duplex	Na			2	
GE-0/0/43			Up	bridged	Enabled	Enabled	auto/auto	1			Ok Car	ncel
GE-0/0/44			Up	bridged	Enabled	Enabled	auto/auto	1	no		1-4094	
			Up	bridged	Enabled	Enabled	auto/auto	1	no		1-4094	
GE-0/0/45					V-2-10-20-20-20-20-20-20-20-20-20-20-20-20-20		and a fairba		444.900			
GE-0/0/45 GE-0/0/46	227		Up	bridged	Enabled	Enabled	auto/auto	-	по		1-4094	(#)

Step 4 (optional): Verify the configuration is completed using show run and show tunneled-node config command

```
(ArubaS3500) #show tunneled-node config
Tunneled Node Client: Enabled
Tunneled Node Server: 172.16.0.254
Tunneled Node Loop Prevention: Disabled
```

## Step 5: Save the configuration

```
(ArubaS3500) #write memory
Saving Configuration...
Configuration Saved.
```



## 2. Configuration on 3400 controller:

## Step 0 (optional):

Similar to the S3500, the controller should have clean configuration with write erase performed. Since the initial set-up cannot be skipped on the controller, accept the default values given during the set-up such as the IP address (172.16.0.254) and the subnet mask.

## Step 1: Basic configuration including IP address and VLAN

Create VLAN 400 for Employees and VLAN 999 for Guests. For this demo, the IP address of VLAN 1 is set to 172.16.0.254, which set by default by initial controller set-up (step 0).

```
(Aruba3400) (config) #vlan 400
(Aruba3400) (config) #interface vlan 400
(Aruba3400) (config-subif)#ip address 192.168.0.1 255.255.255.0
(Aruba3400) (config-subif)#exit
(Aruba3400) (config) #vlan 999
(Aruba3400) (config) #interface vlan 999
(Aruba3400) (config-subif)#ip address 192.168.99.1 255.255.255.0
(Aruba3400) (config-subif)#ip address 192.168.99.1 255.255.255.0
```

#### Network > VLAN ID

VLAN ID	IPv4 Address	IPv4 Net Mask	IPv6 Address	<b>Associated Ports</b>	AAA Profile	Admin State	<b>Operation State</b>	Mode		Actions	
1	172.16.0.254	255.255.255.0	fe80::b:8600 -	GE1/0-3,Pc0-7	N/A	Enabled	Up	Regular	Disable	Edit	Delete
400	192.168.0.1	255.255.255.0	fe80::b:8601 -		N/A	Enabled	Up	Regular	Disable	Edit	Delete
999	192.168.99.1	255.255.255.0	fe80::b:8603 -		ARUBA_DEMO	Enabled	Up	Regular	Disable	Edit	Delete
Add a V	LAN Add/E	dit Bulk VLANs	Delete Bulk V	LANs							

#### Step 2: DHCP pools for employee and guest roles

DHCP pools need to be created so that the IP address can to be given out to the end-host (laptop). The IP addressing (through DHCP) on the laptop can be used for verification purpose in case of employee laptop. For guest laptop, IP address is required in order to successfully start the captive portal authentication. The IP Address of the controller will be used for DNS server since this is a stand-alone demo.

```
(Aruba3400) (config) #ip dhcp pool EMPLOYEE_POOL
(Aruba3400) (config-dhcp)#default-router 192.168.0.1
(Aruba3400) (config-dhcp)#network 192.168.0.0 255.255.255.0
(Aruba3400) (config-dhcp)#dns-server 192.168.0.1
(Aruba3400) (config-dhcp)#exit
(Aruba3400) (config) #ip dhcp pool GUEST_POOL
(Aruba3400) (config-dhcp)#default-router 192.168.99.1
```



Aruba3400)	(config-dhcp)#network 192.168.99.0 255.255.255.0
Aruba3400)	(config-dhcp)#dns-server 192.168.99.1
Aruba3400)	(config-dhcp) #exit

## (Aruba3400) (config) **#service dhcp**

#### Network > IP > DHCP Server

IP Interfaces IP Routes IPv6 Neighbors GRE Tunnels NAT Pools DHCP Server OSPF Mulitcast Routing

Enable DHCP Server			<b>v</b>	
Pool Configuration				
Name	Default Router	Network	Range	Action
EMPLOYEE_POOL	192.168.0.1	192.168.0.0	192.168.0.2-192.168.0.254	Edit Delete
GUEST_POOL Add	192.168.99.1	192.168.99.0	192.168.99.2-192.168.99.254	Edit Delete
Excluded Address Ran	je			
Excluded Address				Delete
				Apply
Commands				View Commany

# Step 3: Populating the Internal server database

Two entries need to be configured: one for employee and the other for guest. This is a part of the effort to reduce the number of necessary equipment for the demo (i.e. external RADIUS server).

(Aruba3400)	<pre>#local-userdb</pre>	add	username	employee	1 passwor	d employee1	
(Aruba3400)	#local-userdb	add	username	guest1 p	assword g	uest1	

(Optional) Use show local-userdb to verify the entries just created.

rvers	AAA Profiles	L2 Authentication	L3 Auth	entication	User Rul	es Adv	anced					
Serv	er Group	Inte	ernal DB M	laintenance								
	default	Ма	ximum Expi	iration					min			
	internal		Guest User	r Page E	xport I	mport	Delete All Us	ers	Repair Database			
	Internal_Server	Use	ers									
+ RAD	IUS Server	Us	ser Name	Password	Role	E-mail	Enabled	Expiry	IP-Address		Action	
in total		emp	oloyee1	*****	guest		Yes		0.0.0	Disable	Delete	Modify
+ LDA	P Server	gue	st1	*****	guest		Yes		0.0.0	Disable	Delete	Modify
+ Inter	mal DB		Add User			1   1-2	of 2					
+ Taca	cs Accounting Server				-		51 2					
• TAC	ACS Server											
XML	API Server											
• RFC	3576 Server											
+ Wind	dows Server											

## Step 4: Authentication for employee



802.1X for employee role: we will use "authenticated role" that is already defined with addition of VLAN 400 for authenticated employees. Termination mode will be used with internal server so this demo can function as in stand-alone format. Since the demo will be utilizing a Windows-based laptop, EAP-type parameters are also configured to EAP-PEAP with MSChapV2.

Some line(s) of configuration shown here are actually parts of the default configuration so it is not necessary to be configured. However, it has been included to help understanding of the demo configuration.

```
(Aruba3400) (config) #user-role authenticated
(Aruba3400) (config-role) #vlan 400
(Aruba3400) (config-role) #exit
(Aruba3400) (config) #aaa server-group INTERNAL SERVER
(Aruba3400) (Server Group "Internal Server") #auth-server Internal
(Aruba3400) (Server Group "Internal Server") #exit
(Aruba3400) (config) #aaa authentication dot1x EMPLOYEE DOT1X
(Aruba3400) (802.1X Authentication Profile "EMPLOYEE DOT1X") #termination
enable
(Aruba3400) (802.1X Authentication Profile "EMPLOYEE DOT1X") #termination
eap-type eap-peap
(Aruba3400) (802.1X Authentication Profile "EMPLOYEE DOT1X") #termination
inner-eap-type eap-mschapv2
(Aruba3400) (802.1X Authentication Profile "EMPLOYEE DOT1X") #exit
(Aruba3400) (config) #aaa profile ARUBA DEMO
(Aruba3400) (AAA Profile "ARUBA DEMO") #initial-role logon
(Aruba3400) (AAA Profile "ARUBA DEMO") #authentication-dot1x EMPLOYEE DOT1X
(Aruba3400) (AAA Profile "ARUBA DEMO") #dot1x-default-role authenticated
(Aruba3400) (AAA Profile "ARUBA DEMO") #dot1x-server-group INTERNAL SERVER
(Aruba3400) (AAA Profile "ARUBA DEMO") #exit
```



#### Security > User Roles > Edit Role(authenticated)

	System Roles	Policies	Time Ranges (	Guest Access			
							« Bi
irewall P	olicies						
1	Name		Rule Count		Location	Action	
allowall		2				Edit Delete 🔺 🔻	
v6-allowa	all	1				Edit Delete 🔺 🔻	
Add							
te-authen	tication Interval		() II	-			
Re-authen Disabled	tication Interval			Change (0 disa	ables re-authentication. A positive valu	re enables authentication 0 - 4096 )	
<b>Re-authen</b> Disabled <b>Role VLAN</b> 400	itication Interval		400	Change (0 disa	bles re-authentication. A positive valu	e enables authentication 0 - 4096 )	
Re-authen Disabled Role VLAN 400 Bandwidth	itication Interval I ID 1 Contract		400	Change (0 disa	ibles re-authentication. A positive valu ge	ue enables authentication 0 - 4096 )	
Re-authen Disabled Role VLAN 400 Bandwidth Jpstream: 1	tication Interval I ID n Contract Not Enforced		400	Change (0 disa	obles re-authentication. A positive valu ge ge Per User	ue enables authentication 0 - 4096 )	
Re-authen Disabled Role VLAN 400 Bandwidth Upstream: 1 Downstrean	I ID I Contract Not Enforced n: Not Enforced		400	Change (0 disi	ubles re-authentication. A positive valu ge ge ge Per User ge Per User	e enables authentication 0 - 4096 )	
Re-authen Disabled Role VLAN 400 Bandwidth Jpstream: I Downstream	I ID I Contract Not Enforced n: Not Enforced r		400	Change (0 disi Chan Chan Chan Chan	ubles re-authentication. A positive valu ge ge	ie enables authentication 0 - 4096 )	

#### Security > Authentication > Servers

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

Server Group	Server Group > INTE	RNAL_SERVER		Show Refere	nce Save As Reset
default					
internal	Fail Through				
INTERNAL SERVER	Servers				
1	Name	Server-Type	trim-FQDN	Match-Rule	Actions
RADIUS Server	Internal	Internal	No		Edit Delete 🔺 🔻
	New				
LDAP Server	Server Rules				
Internal DB	Priority Attril	oute Operation Ope	erand Type	Action Value	Validated Actions
Tacacs Accounting Server	New				
TACACS Server					
TACACS Server					
TACACS Server XML API Server RFC 3576 Server					



#### Security > Authentication > L2 Authentication

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

MAC Authentication Profile	802.1X Authentication Profile > EMPLOYEE_DOT1X	Show Reference Save As Reset				
802.1X Authentication Profile	Basic Advanced					
default	Max authentication failures	0				
DOT1X	Enforce Machine Authentication					
EMPLOYEE_DOT1X	Machine Authentication: Default Machine Role	guest 🔹				
	Machine Authentication: Default User Role	guest 👻				
Stateful 802.1X Authentication Profile	Reauthentication					
	Termination	N				
	Termination EAP-Type	🗆 eap-tis 🔽 eap-peap				
	Termination Inner EAP-Type					
	Enforce Suite-B 128 bit or more security level Authentication					
	Enforce Suite-B 192 bit security level Authentication					

#### Security > Authentication > Profiles

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

AAA Profile	AAA Profile > ARUBA_DEMO		Show F	eference Save As Reset
ARUBA_DEMO     MAC Authentication	Initial role	logon 👻	MAC Authentication Default Role	guest 👻
Profile MAC Authentication	802.1X Authentication Default Role	authenticated 🗸	L2 Authentication Fail Throu	ah 🗖
Server Group	RADIUS Interim Accounting		User derivation rules	NONE 🔻
802.1X Authentication	Wired to Wireless Roaming		SIP authentication role	NONE +
Profile EMPLOYEE_DOT1X	Device Type Classification	V	Enforce DHCP	Г
RADIUS Accounting Server Group				
RADIUS Accounting Server Group XML API server RFC 3576 server default default default-dottx default-dottx-psk default-dottx-psk default-dottx-psk default-open				

### Step 5: Authentication for guest

Captive portal for guest: logon role will be used for captive portal. Again, some line(s) of configuration shown here are actually parts of the default configuration so they do not need to be configured.

```
(Aruba3400) (config) #aaa authentication captive-portal CAPTIVE_PORTAL
(Aruba3400) (Captive Portal Authentication Profile "CAPTIVE_PORTAL") #server-
group INTERNAL_SERVER
(Aruba3400) (Captive Portal Authentication Profile "CAPTIVE_PORTAL") #user-
logon
(Aruba3400) (Captive Portal Authentication Profile "CAPTIVE_PORTAL")
#default-role guest
```



(Aruba3400) <b>popup-windov</b>	(Captive Port	al Authentication	Profile	"CAPTIVE_PORTAL")	#logout-
(Aruba3400)	(Captive Port	al Authentication	Profile	"CAPTIVE_PORTAL")	#exit
(Aruba3400)	(config) # <b>use</b>	er-role logon			
(Aruba3400)	(config-role)	#captive-portal	CAPTIVE_P	PORTAL	
(Aruba3400)	(config-role)	#exit			

#### Security > Authentication > L3 Authentication

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

Captive Portal Authentication     Profile	Captive Portal Authentic	ation Profile > CAPTIVE_PORTAL	Shc	w Reference Save As Reset
CAPTIVE_PORTAL	Default Role	guest 👻	Default Guest Role	guest 👻
Server Group INTERNAL_SERVER	Redirect Pause	10 sec	User Login	
💿 default	Guest Login	Γ	Logout popup window	
WISPr Authentication Profile	Use HTTP for authentication	Г	Logon wait minimum wait	5 sec
VPN Authentication Profile	Logon wait maximum wait	10 sec	logon wait CPU utilization threshold	60 %
Stateful NTLM Authentication     Drofile	Max Authentication failures	0	Show FQDN	
Profile	Use CHAP (non-standard)		Login page	/auth/index.html
VIA Authentication Profile	Welcome page	/auth/welcome.html	Show Welcome Page	
VIA Connection Profile	Add switch IP address in the redirection URL		Allow only one active user session	
VIA Web Authentication	White List	Delete Add	Black List	Delete Add
	Show the acceptable use policy page			(Arr - Arr -

Re-authentication Interval	
Disabled	Change (0 disables re-authentication. A positive value enables authentication 0 - 4096 )
Role VLAN ID	
Not Assigned	Not Assigned 👻 Change
Bandwidth Contract	
Upstream: Not Enforced	✓ Change □ Per User
Downstream: Not Enforced	✓ Change □ Per User
VPN Dialer	
Not Assigned	Not Assigned 👻 Change
L2TP Pool	
default-l2tp-pool	Not Assigned 👻 Change
PPTP Pool	
default-pptp-pool	Not Assigned 👻 Change
Captive Portal Profile	
CAPTIVE_PORTAL	Not Assigned 👻 Change

# Step 6: Apply the configured profile on the VLAN (999)

The configured AAA profile needs to be applied to the VLAN (999) so it will take effect.



(Aruba3400) (config) **#vlan 999 wired aaa-profile ARUBA\_DEMO** 

#### Network > VLAN > Edit VLAN (999)

Associated with © Port © Port-Channel Wired AAA Profile ARUBA\_DEMO Port-Channel ID 0 

Commands

« Back

Apply

View Commands

# Step 7: Save the configuration

(Aruba3400) **#write memory** 

Saving Configuration...

Configuration Saved.



# **DEMO STEPS**

Once the configuration is completed, demo steps can take place.

# Step 1: Verify Connectivity

From the S3500, ping the controller IP address to ensure connectivity. Or ping the S3500 IP address from the controller if more convenient.

```
(ArubaS3500) #ping 172.16.0.254
Press 'q' to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1.799/1.823/1.839
ms
(ArubaS3500) #
```

# Step 2: Connect the laptop with 802.1X (as employee) capability

If you don't know how to enable 802.1X on a Windows laptop, follow the steps listed on this link:

http://windows.microsoft.com/en-US/windows-vista/Enable-802-1X-authentication

Once 802.1X functionality has been enabled, use the following figures as reference for settings. In particular, ensure that "Validate server certificate" and automatic use of Windows logon options have been unchecked, and *user authentication* is chosen for authentication mode:



laturadain -	
erworking	Authentication Sharing
Select this Ethe	his option to provide authenticated network access for emet adapter.
📝 E <u>n</u> ab	ole IEEE 802.1X authentication
~	
Choose	a network authentication method:
Microso	oft: Protected EAP (PEAP)
Rem	nember my credentials for this connection each
time	I'm logged on
Eallb	ack to unauthorized network access
Ad <u>d</u> iti	ional Settings
	OK
/anced se	ettings 📃
02.1X set	tings
Spe	cify authentication mode
Spe	crify authentication mode
Spe	er authentication mode
Us	cify authentication mode er authentication
Us Us	cify authentication mode er authentication  Cave gredentials  Delete credentials for all users  ble single sign on for this petwork
Spe	cify authentication mode  er authentication  Delete credentials for all users  ble single sign on for this network  Berform immediately before user laces
Spe	cify authentication mode  ser authentication  Cave gredentials  Delete credentials for all users  ble gingle sign on for this network  Perform immediately before user logon  Perform immediately after user logon
Spe Us Ena Ma:	cify authentication mode  cer authentication  Cave gredentials  Delete credentials for all users  ble single sign on for this network  Perform immediately before user logon  Perform immediately after user logon  ximum delay (seconds):  10
Spe Us Ena @ Mar	cify authentication mode  ser authentication  Delete credentials for all users  ble gingle sign on for this network  Perform immediately before user logon Perform immediately after user logon ximum delay (seconds):  10  Allow additional gialogs to be displayed during single
Spe Us Ena Ma:	er authentication mode         er authentication         Delete credentials for all users         ble gingle sign on for this network         Perform immediately before user logon         Perform immediately after user logon         ximum delay (seconds):         10         Xilow additional gialogs to be displayed during single sign on
Spe Us Ena @ Ma <sup>2</sup>	er authentication mode         er authentication         Delete credentials for all users         ble gingle sign on for this network         Perform immediately before user logon         Perform immediately after user logon         ximum delay (seconds):         10         Allow additional gialogs to be displayed during single sign on         This network uses separate virtual LANs for machine and user authentication
Ena Ma:	cify authentication mode   ser authentication   Delete credentials for all users   Belete credentials for all users   ble gingle sign on for this network   Perform immediately before user logon   Perform immediately after user logon   Perform immediately after user logon   Ximum delay (seconds):   10   Allow additional dialogs to be displayed during single sign on   This network uses separate virtual LANs for machine and user authentication
Spe Us Ena Mai	cify authentication mode   eer authentication   Delete credentials for all users   ble single sign on for this network Perform immediately before user logon Perform immediately after user logon ximum delay (seconds): Allow additional gialogs to be displayed during single sign on This network uses separate virtual LANs for machine and user authentication
Spe Us Ena @ Ma <sup>2</sup>	cify authentication mode     eer authentication     Delete credentials for all users     ble gingle sign on for this network   Perform immediately before user logon Perform immediately after user logon ximum delay (seconds):   10   Allow additional dialogs to be displayed during single sign on This network uses separate virtual LANs for machine and user authentication
Ena Ma:	ecify authentication mode Save gredentials Delete credentials for all users Delete credentials for
Spe Us Ena Ma: V	cdfy authentication mode     eer authentication     Delete credentials for all users     ble gingle sign on for this network   Perform immediately before user logon   Perform immediately after user logon   ximum delay (seconds):     10   Allow additional gialogs to be displayed during single sign on   This network uses separate virtual LANs for machine and user authentication
Spe Us Ena @ Ma:	cify authentication mode   ser authentication   Delete credentials for all users     ble gingle sign on for this network   Perform immediately before user logon   Perform immediately after user logon   Ximum delay (seconds):   Allow additional gialogs to be displayed during single sign on   This network uses separate virtual LANs for machine and user authentication
Spe Us Ena @ Ma:	ecify authentication mode  er authentication  Delete credentials for all users  ble gingle sign on for this network  Perform immediately before user logon Perform immediately after user logon ximum delay (seconds):  Allow additional gialogs to be displayed during single sign on  This network uses separate virtual LANs for machine and user authentication
Spe Us Ena Ma:	ecify authentication mode  er authentication  Delete credentials for all users  ble gingle sign on for this network  Perform immediately before user logon  Perform immediately after user logon  Allow additional gialogs to be displayed during single sign on  This network uses separate virtual LANs for machine and user authentication  CK  Cancel



hen connecting:		
Validate server cer	tificate	
Connect to these	servers:	
Trusted Root Certifica	ation Authorities:	
AAA Certificate S	ervices	
AddTrust Externa	al CA Root	
administrator		
America Online R	oot Certification Authority 1	
aruba-server		
Class 1 Dublic Drin	noru Cortification Authority	12
	mary certification Additionty	17.
Do not prompt use	er to authorize new servers or trusted	
Do not grompt use certification autho	er to authorize new servers or trusted rities.	
Do not prompt use certification author elect Authentication Me secured password (EAR	er to authorize new servers or trusted rities. ethod: P-MSCHAP v2)	nfigure
Do not prompt use certification author elect Authentication Me Gecured password (EAF Enable East Reconne Enforce Network Acc Disconnect if server Enable Identity Priva	er to authorize new servers or trusted rities. ethod: <u>P-MSCHAP v2</u> ect ect ect does not present cryptobinding TLV acy	nfigure



# Step 3: Complete the authentication process by clicking the balloon message, then proving the username/password





Network A	Authentication
Please enter u	user credentials
	employee1

Step 4: Verify that appropriate IP address (in 192.168.0.0/24 subnet) has been received from DHCP server



## Step 5 (optional): Verify the tunneled node state on either S3500 or controller

(ArubaS3500)	#show tunneled-node	state				
Tunneled Node	State					
ТР	MAC	Port	state	vlan	tunnel	
inactive-time	1110	1010	blace	vian	cunner	
172.16.0.254	00:0b:86:6a:31:c0	GE0/0/1	complete	0999	4094	0000
172.16.0.254	00:0b:86:6a:31:c0	GE0/0/2	not-started	0999	4093	0000
172.16.0.254	00:0b:86:6a:31:c0	GE0/0/3	not-started	0999	4092	0000
172.16.0.254	00:0b:86:6a:31:c0	GE0/0/4	not-started	0999	4091	0000
172.16.0.254	00:0b:86:6a:31:c0	GE0/0/5	not-started	0999	4090	0000



172.16.0.25400:0b:86:6a:31:c0GE0/0/6not-started099940890000172.16.0.25400:0b:86:6a:31:c0GE0/0/7not-started099940880000172.16.0.25400:0b:86:6a:31:c0GE0/0/8not-started099940870000172.16.0.25400:0b:86:6a:31:c0GE0/0/9not-started099940860000

```
(Aruba3400) #show user-table
Users
____
             MAC
                    Name Role Age(d:h:m) Auth
  ΤP
VPN link AP name Roaming Essid/Bssid/Phy
Profile Forward mode Type
          _____
                                           _____ ___
_____
                        _____
                                ____
_____ ____
192.168.0.254 2c:27:d7:be:6d:37 employee1 authenticated 00:00:00
802.1x-Wired tunnel 9 Wired
172.16.0.100:gigabitethernet0/0/1/00:0b:86:6a:31:c0 ARUBA DEMO tunnel
Win 7
User Entries: 1/1
(Aruba3400) #show tunneled-node state
Tunneled Node State
_____
                               state vlan tunnel
IP MAC
                 s/p
inactive-time
                        ___
                                        ____
_____
172.16.0.100 00:0b:86:6a:31:c0 gigabitethernet0/0/1 complete 999
                                                    9
0
```

## Step 6: Disconnect the laptop

# Step 7: Turn off the 802.1X functionality on the laptop then reconnect (this time as guest)

The laptop should obtain an IP address in 192.168.99.0/24 subnet

- - X



# Command Prompt

C:\Users>ipconfig	-
Windows IP Configuration	
Ethernet adapter Local Area Connection:	
Connection-specific DNS Suffix . : IPv4 Address : 192.168.99.254 Subnet Mask : 255.255.255.0 Default Gateway : 192.168.99.1	
Tunnel adapter isatap.{837FAE52-0C3A-49D4-8C08-DC11B228097C}:	
Media State Media disconnected Connection-specific DNS Suffix . :	
Tunnel adapter Teredo Tunneling Pseudo-Interface:	
Media State Media disconnected Connection-specific DNS Suffix . :	
C:\Users>	-

# Step 8: Authenticate via web browser using http://1.1.1.1 as destination IP address



Note that for this demo to work, *IP address needs to be used* due to a bug in the controller software image used for this demo. Do not use domain name such as <u>http://arubanetworks.com</u>.

Step 9: Verify that authentication is successful as guest





## Step 10 (optional): Verify the tunneled node state on either S3500 or controller

(ArubaS3500)	#show tunneled-node	state				
Tunneled Node	State					
IP inactive-time	MAC	Port	state	vlan	tunnel	
172.16.0.254	00:0b:86:6a:31:c0	GE0/0/1	complete	0999	4094	0000
172.16.0.254	00:0b:86:6a:31:c0	GE0/0/2	not-started	0999	4093	0000
172.16.0.254	00:0b:86:6a:31:c0	GE0/0/3	not-started	0999	4092	0000
172.16.0.254	00:0b:86:6a:31:c0	GE0/0/4	not-started	0999	4091	0000
172.16.0.254	00:0b:86:6a:31:c0	GE0/0/5	not-started	0999	4090	0000
172.16.0.254	00:0b:86:6a:31:c0	GE0/0/6	not-started	0999	4089	0000
172.16.0.254	00:0b:86:6a:31:c0	GE0/0/7	not-started	0999	4088	0000
172.16.0.254	00:0b:86:6a:31:c0	GE0/0/8	not-started	0999	4087	0000
172.16.0.254	00:0b:86:6a:31:c0	GE0/0/9	not-started	0999	4086	0000

(Aruba3400) **#show user-table** 



Users \_\_\_\_\_ IP MAC Name Role Age(d:h:m) Auth VPN link AP name Roaming Essid/Bssid/Phy Profile Forward mode Type \_\_\_\_\_ \_\_\_\_\_ ----- ----\_\_\_\_\_ \_\_\_\_ ---- ----------- -----192.168.99.254 2c:27:d7:be:6d:37 guest1 guest 00:00:01 Web tunnel 9 Wired 172.16.0.100:gigabitethernet0/0/1/00:0b:86:6a:31:c0 ARUBA DEMO tunnel Win 7 User Entries: 1/1 (Aruba3400) #show tunneled-node state Tunneled Node State \_\_\_\_\_ IP MAC s/p state vlan tunnel inactive-time \_\_\_ \_\_\_\_ ---\_\_\_\_ \_\_\_\_ \_\_\_\_ \_\_\_\_\_ 172.16.0.100 00:0b:86:6a:31:c0 gigabitethernet0/0/1 complete 999 9 0

You have successfully completed the S3500 tunneled node demo.



# **APPENDIX**

Controller scalability numbers for tunneled node:

		6000 Chassis	M3 Module	3600	3400	3200	650/651	620
	Device Capacity	4096	1024	512	256	128	64	32
$\Rightarrow$	# of Wired APs	512	128	32	16	8	2	1
	# of Campus APs (WLAN)	2048	512	128	64	32	16/17	8
	# of Remote APs	4096	1024	512	256	128	64	32
$\Rightarrow$	# of Tunnels	16384	4096	1024	512	256	96	48
	Concurrent Users	32768	8192	81 <b>92</b>	4096	2048	512	256



# **REFERENCE**

## S3500 configuration

```
version 7.0
enable secret "*****"
hostname "ArubaS3500"
clock timezone PST -8
location "Building1.floor1"
controller config 1
ip cp-redirect-address disable
ip access-list eth validuserethacl
 permit any
1
netservice svc-https tcp 443
netservice svc-dhcp udp 67 68
netservice svc-telnet tcp 23
netservice svc-sip-tcp tcp 5060
netservice svc-kerberos udp 88
netservice svc-tftp udp 69
netservice svc-dns udp 53
netservice svc-h323-udp udp 1718 1719
netservice svc-h323-tcp tcp 1720
netservice svc-vocera udp 5002
netservice svc-http tcp 80
netservice svc-sip-udp udp 5060
netservice svc-natt udp 4500
netservice svc-ftp tcp 21
netservice svc-smtp tcp 25
netservice svc-sips tcp 5061
netservice svc-ntp udp 123
netservice svc-icmp 1
netservice svc-ssh tcp 22
ip access-list stateless dhcp-acl-stateless
 any any svc-dhcp permit
1
ip access-list stateless validuser
  network 169.254.0.0 255.255.0.0 any any deny
  any any any permit
1
ip access-list stateless https-acl-stateless
 any any svc-https permit
1
ip access-list stateless dns-acl-stateless
  any any svc-dns permit
1
ip access-list stateless logon-control-stateless
 user any udp 68 deny
 any any svc-icmp permit
  any any svc-dns permit
 any any svc-dhcp permit
  any any svc-natt permit
!
```



```
ip access-list stateless icmp-acl-stateless
  any any svc-icmp permit
!
ip access-list stateless allowall-stateless
  any any any permit
1
ip access-list stateless http-acl-stateless
 any any svc-http permit
!
user-role ap-role
!
user-role denyall
1
user-role guest-logon
1
user-role quest
access-list stateless http-acl-stateless
access-list stateless https-acl-stateless
access-list stateless dhcp-acl-stateless
access-list stateless icmp-acl-stateless
access-list stateless dns-acl-stateless
1
user-role stateful-dot1x
!
user-role authenticated
access-list stateless allowall-stateless
!
user-role logon
access-list stateless logon-control-stateless
!
!
ip dhcp default-pool private
ssh mgmt-auth username/password
mgmt-user admin root e141f5db014bfad8e6d2fcaf9e02c947df64dcfebfa2c08ba6
ip igmp
!
no firewall attack-rate cp 1024
!
firewall cp
!
firewall cp
packet-capture-defaults tcp disable udp disable sysmsg disable other disable
!
ip domain lookup
!
```



```
country US
aaa authentication mac "default"
aaa authentication dot1x "default"
1
aaa server-group "default"
auth-server Internal
set role condition role value-of
1
aaa profile "default"
1
aaa authentication mgmt
1
aaa authentication wired
1
web-server
1
aaa password-policy mgmt
1
traceoptions
1
gos-profile "default"
!
policer-profile "default"
!
ip-profile
  default-gateway 172.16.0.254
1
lcd-menu
1
interface-profile switching-profile "CONTROLLER_VLAN_999"
   access-vlan 999
1
interface-profile switching-profile "default"
1
interface-profile switching-profile "VLAN1"
1
interface-profile tunneled-node-profile "TUNNELED NODE"
   controller-ip 172.16.0.254
I.
interface-profile poe-profile "default"
!
interface-profile poe-profile "poe-factory-initial"
   enable
!
interface-profile enet-link-profile "default"
!
interface-profile lldp-profile "default"
1
interface-profile lldp-profile "lldp-factory-initial"
  lldp transmit
  lldp receive
  med enable
```



```
!
interface-profile mstp-profile "default"
!
mstp
   enable
1
lacp
!
igmp-snooping-profile "default"
!
igmp-snooping-profile "igmp-snooping-factory-initial"
!
poemanagement member-id "0"
!
vlan "1"
   igmp-snooping-profile "igmp-snooping-factory-initial"
1
vlan "999"
   description "CONTROLLER_VLAN_999"
!
interface gigabitethernet "0/0/0"
  switching-profile "VLAN1"
!
interface vlan "1"
   ip address 172.16.0.100 netmask 255.255.255.0
1
interface mgmt
!
interface-group gigabitethernet "default"
  apply-to ALL
  lldp-profile "lldp-factory-initial"
   poe-profile "poe-factory-initial"
1
interface-group gigabitethernet "TUNNELED NODE DEMO"
   apply-to 0/0/1-0/0/9
   tunneled-node-profile "TUNNELED NODE"
   switching-profile "CONTROLLER_VLAN_999"
!
snmp-server enable trap
end
```



## 3400 Mobility controller configuration

```
version 6.1
enable secret "*****"
hostname "Aruba3400"
clock timezone PST -8
location "Building1.floor1"
controller config 2
ip NAT pool dynamic-srcnat 0.0.0.0 0.0.0.0
ip access-list eth validuserethacl
 permit any
!
netservice svc-netbios-dgm udp 138
netservice svc-snmp-trap udp 162
netservice svc-syslog udp 514
netservice svc-l2tp udp 1701
netservice svc-ike udp 500
netservice svc-https tcp 443
netservice svc-smb-tcp tcp 445
netservice svc-dhcp udp 67 68
netservice svc-pptp tcp 1723
netservice svc-sec-papi udp 8209
netservice svc-sccp tcp 2000
netservice svc-telnet tcp 23
netservice svc-lpd tcp 515
netservice svc-netbios-ssn tcp 139
netservice svc-sip-tcp tcp 5060
netservice svc-kerberos udp 88
netservice svc-tftp udp 69
netservice svc-http-proxy3 tcp 8888
netservice svc-noe udp 32512
netservice svc-cfgm-tcp tcp 8211
netservice svc-adp udp 8200
netservice svc-pop3 tcp 110
netservice svc-rtsp tcp 554
netservice svc-msrpc-tcp tcp 135 139
netservice svc-dns udp 53
netservice svc-h323-udp udp 1718 1719
netservice svc-h323-tcp tcp 1720
netservice svc-vocera udp 5002
netservice svc-http tcp 80
netservice svc-http-proxy2 tcp 8080
netservice svc-sip-udp udp 5060
netservice svc-nterm tcp 1026 1028
netservice svc-noe-oxo udp 5000 alg noe
netservice svc-papi udp 8211
netservice svc-natt udp 4500
netservice svc-ftp tcp 21
netservice svc-microsoft-ds tcp 445
netservice svc-svp 119
netservice svc-smtp tcp 25
netservice svc-gre 47
netservice svc-netbios-ns udp 137
netservice svc-sips tcp 5061
netservice svc-smb-udp udp 445
netservice svc-ipp-tcp tcp 631
netservice svc-esp 50
netservice svc-v6-dhcp udp 546 547
netservice svc-snmp udp 161
netservice svc-bootp udp 67 69
netservice svc-msrpc-udp udp 135 139
netservice svc-ntp udp 123
netservice svc-icmp 1
netservice svc-ipp-udp udp 631
netservice svc-ssh tcp 22
netservice svc-v6-icmp 58
netservice svc-http-proxy1 tcp 3128
netexthdr default
ip access-list session v6-icmp-acl
```



```
ipv6 any any svc-v6-icmp permit
1
ip access-list session control
  user any udp 68 deny
  any any svc-icmp permit
 any any svc-dns permit
  any any svc-papi permit
  any any svc-sec-papi permit
  any any svc-cfgm-tcp permit
  any any svc-adp permit
  any any svc-tftp permit
 any any svc-dhcp permit
 any any svc-natt permit
I
ip access-list session allow-diskservices
 any any svc-netbios-dgm permit
  any any svc-netbios-ssn permit
 any any svc-microsoft-ds permit
 any any svc-netbios-ns permit
ip access-list session validuser
  network 169.254.0.0 255.255.0.0 any any deny
 any any any permit
 ipv6 any any any permit
Т
ip access-list session v6-https-acl
  ipv6 any any svc-https permit
1
ip access-list session vocera-acl
 any any svc-vocera permit queue high
I.
ip access-list session icmp-acl
 any any svc-icmp permit
ip access-list session v6-dhcp-acl
 ipv6 any any svc-v6-dhcp permit
ip access-list session captiveportal
 user alias controller svc-https dst-nat 8081
 user any svc-http dst-nat 8080
 user any svc-https dst-nat 8081
 user any svc-http-proxyl dst-nat 8088
 user any svc-http-proxy2 dst-nat 8088
user any svc-http-proxy3 dst-nat 8088
I
ip access-list session v6-dns-acl
  ipv6 any any svc-dns permit
ip access-list session allowall
 any any any permit
  ipv6 any any any permit
ip access-list session https-acl
  any any svc-https permit
ip access-list session sip-acl
 any any svc-sip-udp permit queue high any any svc-sip-tcp permit queue high
I.
ip access-list session ra-guard
  ipv6 user any icmpv6 rtr-adv deny
ip access-list session dns-acl
 any any svc-dns permit
I.
ip access-list session v6-allowall
 ipv6 any any any permit
L
ip access-list session tftp-acl
  any any svc-tftp permit
1
```



```
ip access-list session skinny-acl
 any any svc-sccp permit queue high
I
ip access-list session srcnat
 user any any src-nat
ip access-list session vpnlogon
 user any svc-ike permit
 user any svc-esp permit
 any any svc-l2tp permit
 any any svc-pptp permit
 any any svc-gre permit
I.
ip access-list session logon-control
  user any udp 68 deny
  any any svc-icmp permit
  any any svc-dns permit
 any any svc-dhcp permit
 any any svc-natt permit
ip access-list session allow-printservices
  any any svc-lpd permit
 any any svc-ipp-tcp permit
 any any svc-ipp-udp permit
1
ip access-list session cplogout
       alias controller svc-https dst-nat 8081
 user
1
ip access-list session v6-http-acl
 ipv6 any any svc-http permit
I.
ip access-list session http-acl
 any any svc-http permit
ip access-list session dhcp-acl
 any any svc-dhcp permit
I.
ip access-list session captiveportal6
  ipv6 user alias controller6 svc-https captive
  ipv6 user any svc-http captive
  ipv6 user any svc-https captive
  ipv6 user any svc-http-proxy1 captive
  ipv6 user any svc-http-proxy2 captive
  ipv6 user any svc-http-proxy3 captive
ip access-list session ap-uplink-acl
  any any udp 68 permit
  any any svc-icmp permit
 any host 224.0.0.251 udp 5353 permit
ip access-list session noe-acl
 any any svc-noe permit queue high
Т
ip access-list session svp-acl
 any any svc-svp permit queue high
 user host 224.0.1.116 any permit
ip access-list session ap-acl
 any any svc-gre permit
  any any svc-syslog permit
 any user svc-snmp permit
 user any svc-snmp-trap permit
 user any svc-ntp permit
 user alias controller svc-ftp permit
ip access-list session v6-logon-control
 ipv6 user any udp 68 deny
  ipv6 any any svc-v6-icmp permit
 ipv6 any any svc-v6-dhcp permit
  ipv6 any any svc-dns permit
!
```



```
ip access-list session h323-acl
  any any svc-h323-tcp permit queue high
  any any svc-h323-udp permit queue high
1
vpn-dialer default-dialer
  ike authentication PRE-SHARE ******
1
user-role ap-role
access-list session control
 access-list session ap-acl
1
user-role default-vpn-role
access-list session allowall
access-list session v6-allowall
!
user-role voice
access-list session sip-acl
 access-list session noe-acl
access-list session svp-acl
 access-list session vocera-acl
 access-list session skinny-acl
 access-list session h323-acl
 access-list session dhcp-acl
 access-list session tftp-acl
 access-list session dns-acl
access-list session icmp-acl
1
user-role default-via-role
access-list session allowall
1
user-role guest-logon
captive-portal "default"
 access-list session logon-control
access-list session captiveportal
 access-list session v6-logon-control
access-list session captiveportal6
!
user-role guest
access-list session http-acl
 access-list session https-acl
access-list session dhcp-acl
 access-list session icmp-acl
 access-list session dns-acl
access-list session v6-http-acl
 access-list session v6-https-acl
 access-list session v6-dhcp-acl
access-list session v6-icmp-acl
access-list session v6-dns-acl
Т
user-role stateful-dot1x
user-role authenticated
vlan 400
 access-list session allowall
access-list session v6-allowall
Т
user-role logon
captive-portal "CAPTIVE PORTAL"
access-list session logon-control
 access-list session captiveportal
 access-list session vpnlogon
 access-list session v6-logon-control
 access-list session captiveportal6
!
1
interface mgmt
        shutdown
dialer group evdo us
```



```
init-string ATQ0V1E0
 dial-string ATDT#777
1
dialer group gsm us
 init-string AT+CGDCONT=1,"IP","ISP.CINGULAR"
 dial-string ATD*99#
!
dialer group gsm_asia
 init-string AT+CGDCONT=1,"IP","internet"
 dial-string ATD*99***1#
!
dialer group vivo br
 init-string AT+CGDCONT=1,"IP","zap.vivo.com.br"
  dial-string ATD*99#
1
vlan 400
vlan 999 wired aaa-profile "ARUBA DEMO"
interface gigabitethernet 1/0
       description "GE1/0"
        trusted
        trusted vlan 1-4094
ļ
interface gigabitethernet 1/1
       description "GE1/1"
       trusted
       trusted vlan 1-4094
!
interface gigabitethernet 1/2
       description "GE1/2"
        trusted
       trusted vlan 1-4094
1
interface gigabitethernet 1/3
       description "GE1/3"
       trusted
        trusted vlan 1-4094
Т
interface vlan 1
       ip address 172.16.0.254 255.255.255.0
!
interface vlan 400
       ip address 192.168.0.1 255.255.255.0
T
interface vlan 999
       ip address 192.168.99.1 255.255.255.0
I.
uplink disable
ap mesh-recovery-profile cluster Recovery3wcwFj9k+t3SQl8+ wpa-hexkey
e84864632f5f91b031905a687a9230c8bbb4fc65f7c838fc0aa695bcd64e4acaa3b2233b49ccd90b33bfc22fba8741
ab16518b16fdb070a4a9f3772dec4d30b7c5017eb468006e82c72f11d6be810cf1
wms
general poll-interval 60000
general poll-retries 3
general ap-ageout-interval 30
general adhoc-ap-ageout-interval 5
```



```
general sta-ageout-interval 30
general learn-ap disable
general persistent-neighbor enable
general propagate-wired-macs enable
general stat-update enable
general collect-stats disable
general learn-system-wired-macs disable
!
wms-local system max-system-wm 1000
wms-local system system-wm-update-interval 8
crypto isakmp policy 20
 encryption aes256
!
crypto ipsec transform-set default-boc-bm-transform esp-3des esp-sha-hmac
crypto ipsec transform-set default-rap-transform esp-aes256 esp-sha-hmac
crypto ipsec transform-set default-aes esp-aes256 esp-sha-hmac
crypto dynamic-map default-dynamicmap 10000
 set transform-set "default-transform" "default-aes"
!
crypto isakmp eap-passthrough eap-tls
crypto isakmp eap-passthrough eap-peap
crypto isakmp eap-passthrough eap-mschapv2
vpdn group 12tp
ip dhcp pool EMPLOYEE POOL
default-router 192.168.0.1
dns-server 192.168.0.1
network 192.168.0.0 255.255.255.0
authoritative
!
ip dhcp pool GUEST POOL
default-router 192.168.99.1
dns-server 192.168.99.1
network 192.168.99.0 255.255.255.0
authoritative
!
service dhcp
!
vpdn group pptp
tunneled-node-address 0.0.0.0
adp discovery enable
adp igmp-join enable
adp igmp-vlan 0
voice rtcp-inactivity disable
voice sip-midcall-req-timeout disable
ssh mgmt-auth username/password
mgmt-user admin root 4613065e012eb7932a6d94ac1c2cf37b78fcb8e7b722ebf94b
no database synchronize
database synchronize rf-plan-data
ip mobile domain default
!
ip igmp
1
```



```
ipv6 mld
!
no firewall attack-rate cp 1024
Т
firewall cp
1
firewall cp
packet-capture-defaults tcp disable udp disable sysmsg disable other disable
ip domain lookup
!
country US
aaa authentication mac "default"
1
aaa authentication dot1x "default"
1
aaa authentication dot1x "EMPLOYEE DOT1X"
  termination enable
   termination eap-type eap-peap
  termination inner-eap-type eap-mschapv2
1
aaa server-group "default"
auth-server Internal
set role condition role value-of
!
aaa server-group "INTERNAL SERVER"
auth-server Internal
!
aaa authentication via connection-profile "default"
1
aaa authentication via web-auth "default"
aaa authentication via global-config
1
aaa profile "ARUBA DEMO"
  authentication-dot1x "EMPLOYEE DOT1X"
   dot1x-default-role "authenticated"
  dot1x-server-group "INTERNAL SERVER"
!
aaa profile "default"
1
aaa authentication captive-portal "CAPTIVE PORTAL"
  server-group "INTERNAL SERVER"
aaa authentication captive-portal "default"
aaa authentication wispr "default"
aaa authentication vpn "default"
aaa authentication vpn "default-rap"
1
aaa authentication mgmt
aaa authentication stateful-ntlm "default"
aaa authentication stateful-kerberos "default"
1
aaa authentication stateful-dot1x
1
aaa authentication via auth-profile "default"
aaa authentication wired
web-server
papi-security
```



```
I
guest-access-email
voice logging
voice dialplan-profile "default"
voice real-time-config
voice sip
1
aaa password-policy mgmt
1
control-plane-security
ids management-profile
ids ap-rule-matching
valid-network-oui-profile
1
ap system-profile "default"
1
ap regulatory-domain-profile "default"
  country-code US
   valid-11g-channel 1
  valid-11g-channel 6
  valid-11g-channel 11
   valid-11a-channel 36
   valid-11a-channel 40
   valid-11a-channel 44
   valid-11a-channel 48
   valid-11a-channel 149
   valid-11a-channel 153
   valid-11a-channel 157
   valid-11a-channel 161
   valid-11a-channel 165
   valid-11g-40mhz-channel-pair 1-5
   valid-11g-40mhz-channel-pair 7-11
   valid-11a-40mhz-channel-pair 36-40
   valid-11a-40mhz-channel-pair 44-48
   valid-11a-40mhz-channel-pair 149-153
   valid-11a-40mhz-channel-pair 157-161
1
ap wired-ap-profile "default"
1
ap enet-link-profile "default"
1
ap mesh-ht-ssid-profile "default"
1
ap mesh-cluster-profile "default"
ap wired-port-profile "default"
ap mesh-radio-profile "default"
ids general-profile "default"
ids rate-thresholds-profile "default"
ids signature-profile "default"
ids impersonation-profile "default"
ids unauthorized-device-profile "default"
ids signature-matching-profile "default"
   signature "Deauth-Broadcast"
   signature "Disassoc-Broadcast"
ids dos-profile "default"
```



```
Т
ids profile "default"
1
rf arm-profile "arm-maintain"
   assignment maintain
  no scanning
1
rf arm-profile "arm-scan"
rf arm-profile "default"
rf optimization-profile "default"
1
rf event-thresholds-profile "default"
rf am-scan-profile "default"
rf dotlla-radio-profile "default"
rf dotlla-radio-profile "rp-maintain-a"
   arm-profile "arm-maintain"
1
rf dotlla-radio-profile "rp-monitor-a"
  mode am-mode
1
rf dotlla-radio-profile "rp-scan-a"
   arm-profile "arm-scan"
1
rf dot11g-radio-profile "default"
1
rf dot11g-radio-profile "rp-maintain-g"
   arm-profile "arm-maintain"
1
rf dot11g-radio-profile "rp-monitor-g"
  mode am-mode
!
rf dot11g-radio-profile "rp-scan-g"
   arm-profile "arm-scan"
1
wlan dot11k-profile "default"
1
wlan voip-cac-profile "default"
wlan ht-ssid-profile "default"
wlan edca-parameters-profile station "default"
wlan edca-parameters-profile ap "default"
wlan ssid-profile "default"
wlan virtual-ap "default"
1
ap provisioning-profile "default"
ap spectrum local-override
1
ap-group "default"
logging level warnings security subcat ids
logging level warnings security subcat ids-ap
snmp-server enable trap
process monitor log
end
```