AIRHEADS meetup

aruba
a Hewlett Packard Enterprise company

DUR & UBT

“Automation” via ClearPass

14 November 2018

#ArubaAirheads

Who Am I

René Jorissen

4IP solutions — Co-owner / Solution Specialist

aruba MOBILE FIRST EXPERT — AMFX #26

PARTNER AMBASSADOR

AIRHEADS COMMUNITY — Guest-Blogger

AIRHEADS meetup

Back in the Days

Statische Config

```
interface 1/1
   name “workstation”
   untagged vlan 50
   speed-duplex 100-full
   spanning-tree admin-edge-port
   spanning-tree root-guard bpdu-protection
   loop-protect
exit
```

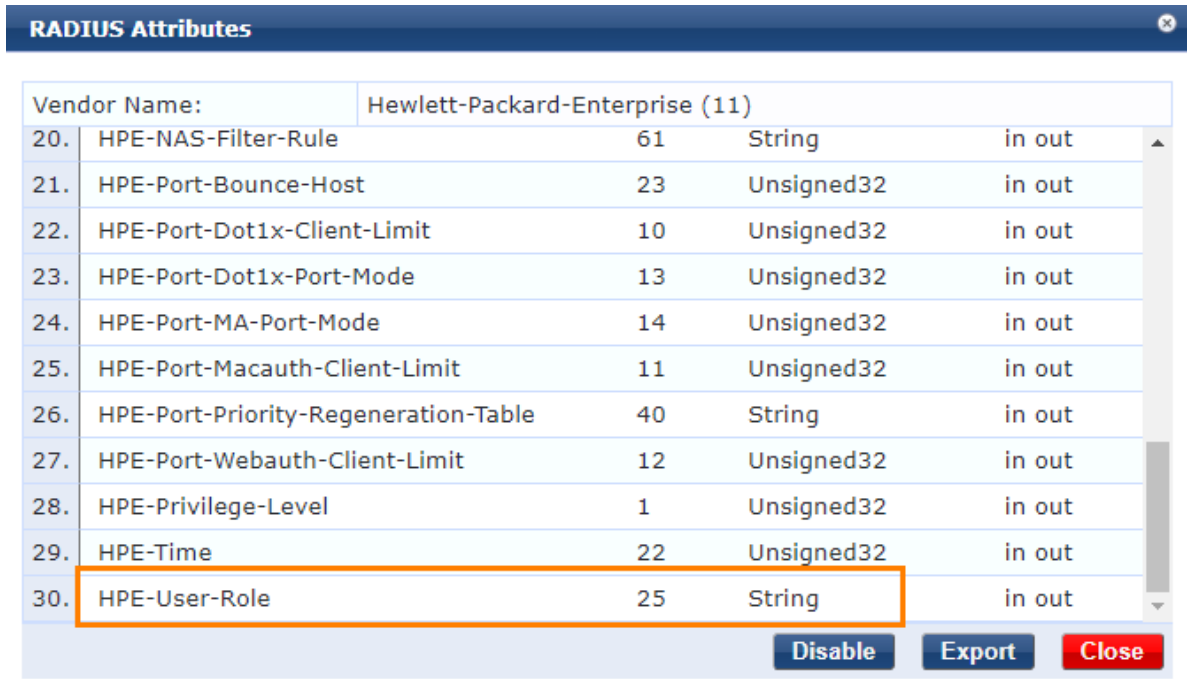
Wired Auth - *the beginning*

- MAC Auth
- 802.1x
  - aaa port-access mac-based 35 reauth-period 3600
  - aaa port-access mac-based 35 auth-vid 4
  - aaa port-access mac-based 35 unauth-vid 505
- Dynamic VLAN
  - Tunnel-Medium-Type
  - Tunnel-Pvt-Group-ID
  - Tunnel-Type

User Roles

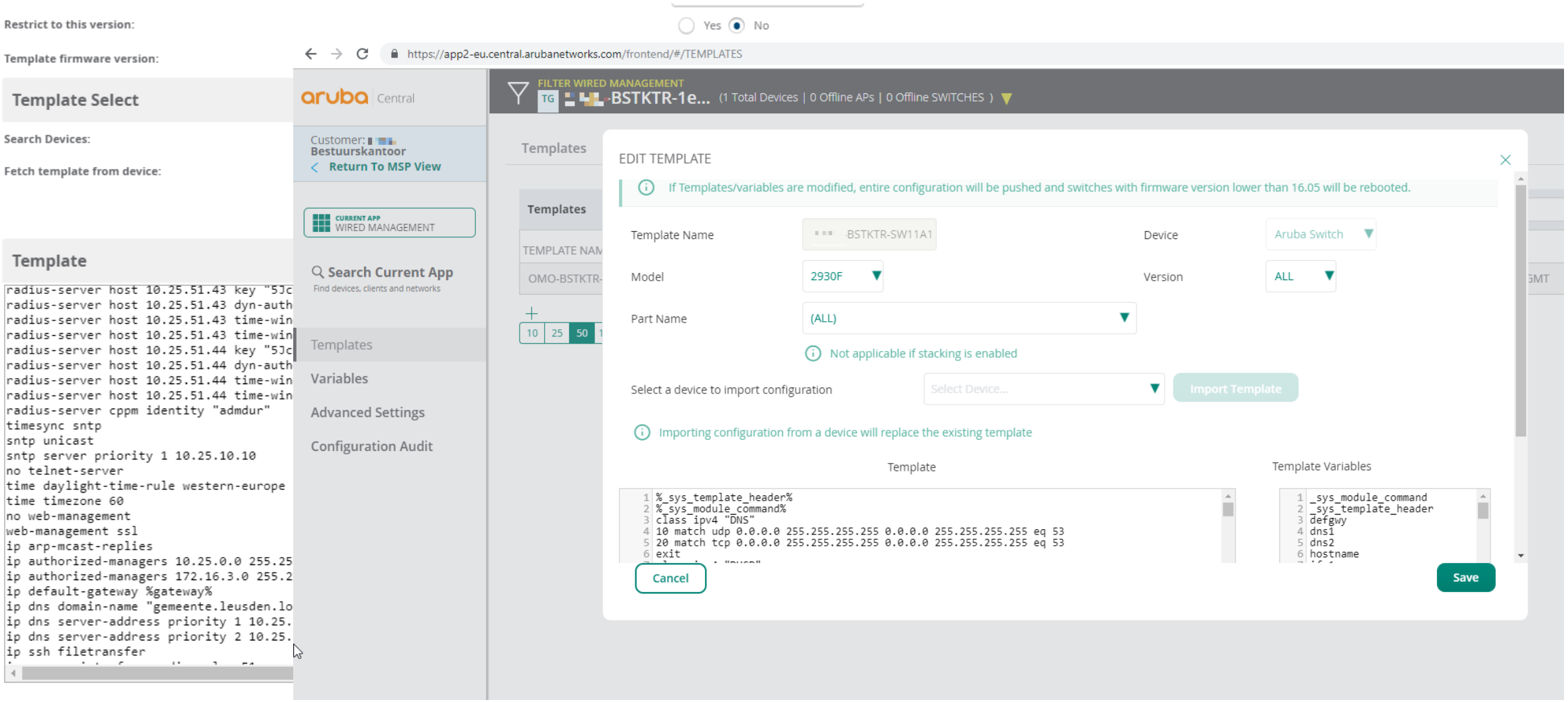
User-Role

```
class ipv4 "DNS"
     10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53
   exit
policy user "DENY-INTERNAL"
     10 class ipv4 "DNS" action permit
     20 class ipv4 "DHCP" action permit
     30 class ipv4 "INTERNAL" action deny
     40 class ipv4 "IP-ANY-ANY" action permit
   exit
 aaa authorization user-role name “SECURE”
  policy “DENY-INTERNAL"
  reauth-period 28800
  vlan-name “SECURE_EDGE"
exit
```



Multiple Changes…..

AirWave & Central



Real Python

Downloadable User Roles

Enforcement Profiles

Profile | Role Configuration | Summary

Template:	Aruba Download
Name:	
Description:	
Type:	R
Action:	
Device Group List:	
Role Configuration Mode:	
Product:	A

Profile

Captive Porta
Policy:
Secondary R
Controller St
VLAN:
VLAN Name:
VLAN Tagged
Re-Authentic
Class Config
User Role Co

Profile | Role Configuration | Summary

Profile:

Template:	Aruba Downloadable Role Enforcement
Name:	
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Role Configuration:

Captive Portal Profile:	-
Policy:	PERMIT-ALL
Controller Static Role :	secure-wired
VLAN Name:	SECURE-EDGE
VLAN ID Tagged <1-4094>:	0
VLAN Name Tagged:	
Re-Authentication Period <0-999999999>:	28800 Seconds
User Role Configuration:	class ipv4 "IP-ANY" 10 match ip any any exit policy user "PERMIT-ALL" 10 class ipv4 "IP-ANY" action permit exit aaa authorization user-role name "cppmrole_7f71e0f2a00f4a9" policy "PERMIT-ALL" vlan-name SECURE-EDGE tunneled-node-server-redirect secondary-role "secure-wired" reauth-period 28800 exit

AIRHEADS meetup

Enforcement Profiles

Profile | Attributes | Summary

Profile | Attributes | Summary

Profile:

Template:	Aruba Downloadable Role Enforcement
Name:	
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Hewlett-Packard-Enterprise	HPE-CPPM-Role	=	class ipv4 "IP-ANY" 10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 exit policy user "PERMIT-ALL" 10 class ipv4 "IP-ANY" action permit exit aaa authorization user-role name "SECURE" policy "PERMIT-ALL" reauth-period 28800 vlan-name "SECURE_EDGE" tunneled-node-server-redirect secondary-role secure-wired exit

Switch Output (1)

```
A-SW-SER0# show port-ac clients 3/9 detail

 Port Access Client Status Detail

  Client Base Details :
   Port            : 3/9                  Authentication Type : mac-based
   Client Status   : authenticated        Session Time        : 29488 seconds
   Client Name     : 442b03a2e511         Session Timeout     : 86400 seconds
   MAC Address     : 442b03-a2e511
   IP              : 10.25.91.121
Downloaded user roles are preceded by *

 User Role Information

   Name                              : *_DUR___VoIP_Client_-3033-3
   Type                              : downloaded
   Reauthentication Period (seconds) : 86400
   Logoff Period (seconds)           : 86400
   Untagged VLAN                     :
   Tagged VLANs                      : 91
   Captive Portal Profile            :
   Policy                            : VOIP-CLIENTS__DUR___VoIP_Client_-3033-3
```

Switch Output (2)

```
Statements for policy "VOIP-CLIENTS__DUR___VoIP_Client_-3033-3"
policy user "VOIP-CLIENTS__DUR___VoIP_Client_-3033-3"
     10 class ipv4 "IP_ANY_ANY__DUR___VoIP_Client_-3033-3" action permit
   exit


Statements for class IPv4 "IP_ANY_ANY__DUR___VoIP_Client_-3033-3"
class ipv4 "IP_ANY_ANY__DUR___VoIP_Client_-3033-3"
     10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
   exit

   Tunnelednode Server Redirect      : Disabled
   Secondary Role Name               :
```

User Based Tunnel

User Based Tunneling - MC

```
(A-Aruba-MC-02) #show user-table role printer

Users
-----
    IP              MAC               Name     Role      Age(d:h:m)  Auth  VPN link  AP name
Roaming  Essid/Bssid/Phy                          Profile                Forward mode
Type  Host Name  User Type
----------   ------------       ------    ----      ----------  ----  --------  -------
10.25.80.13  00:20:6b:83:a4:ec             printer   00:12:51                    tunnel
9    Wired    TUNNELED_NODE_ESSID/04:09:73:9c:8c:a2/-  default-tunneled-user  tunnel
TUNNELED USER
10.25.80.15  00:20:6b:83:a5:2d             printer   00:00:05                    tunnel
243  Wired    TUNNELED_NODE_ESSID/b8:83:03:e1:be:c0/-  default-tunneled-user  tunnel
TUNNELED USER

User Entries: 2/2
 Curr/Cum Alloc:160/38619 Free:77/38459 Dyn:237 AllocErr:0 FreeErr:0
```

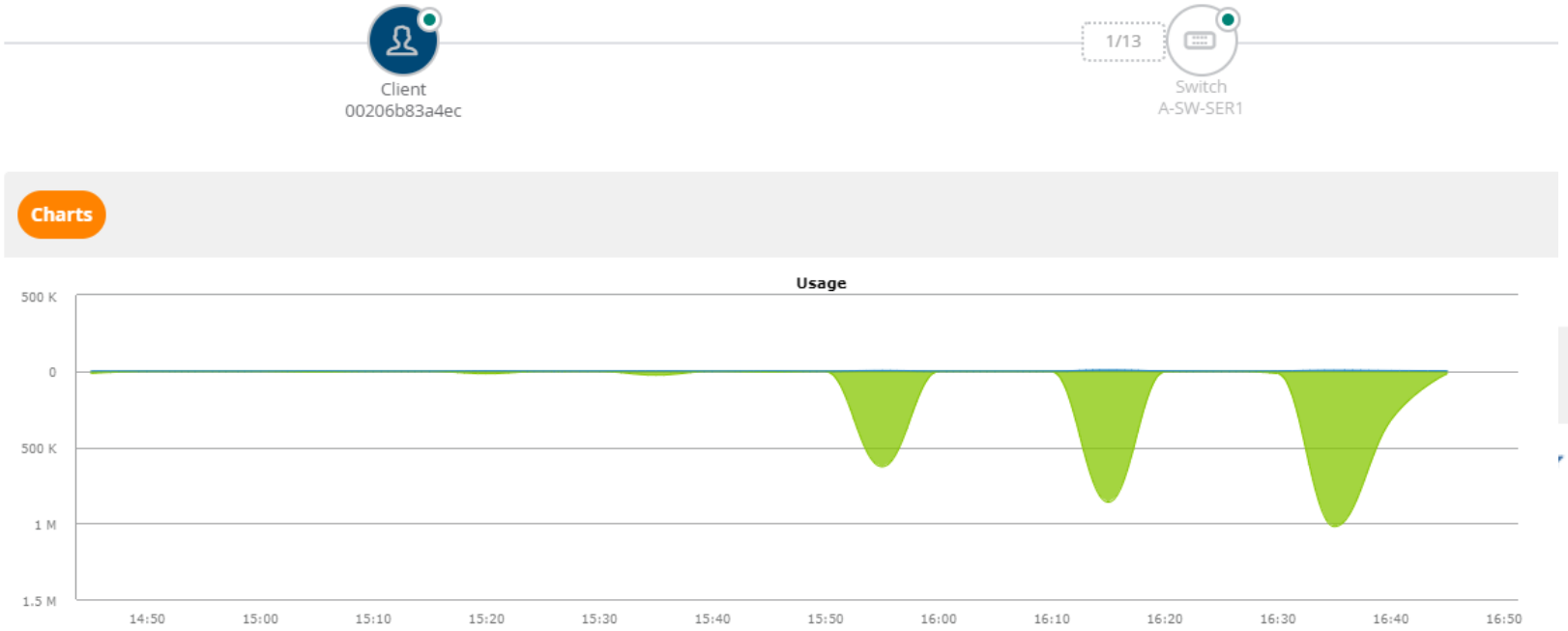
User Based Tunneling - MM

CONTROLLERS	ACCESS POINTS	CLIENTS	ALERTS
2 0	48 0	204 10	0

Wireless (202) **Wired (10)** Default Columns

Client	IP Address	Device Type	Role	Connected to	Rx Bytes
10.25.108.205	10.25.108.205	-	thin-client	tunnel 371	18.50 M
10.25.109.14	10.25.109.14	-	thin-client	tunnel 147	27.65 M
10.35.10.201	10.35.10.201	-	lariks	tunnel 254	43.49 M
10.25.80.13	10.25.80.13	-	printer	tunnel 9	5.56 M
10.25.102.144	10.25.102.144	-	wired-specials	tunnel 155	30.00 M
10.25.108.191	10.25.108.191	-	thin-client	tunnel 227	8.77 M
10.25.108.212	10.25.108.212	-	thin-client	tunnel 91	78.69 M
10.45.10.11	10.45.10.11	-	voila	tunnel 297	297.72 M
10.25.130.22	10.25.130.22	-	kiosk	tunnel 163	1.92 M
10.25.130.23	10.25.130.23	-	kiosk	tunnel 62	2.63 G

User Based Tunneling - AMP



Device Info	
Username:	00206b83a4ec
Device Name:	
Device Type:	KONICA MINOLTA HOLDINGS, INC.
MAC Address:	00:20:6B:83:A4:EC
Role:	_DUR___TN___Printer_-3045-9_7Z4q
Notes:	

Current Association	
Connection Mode:	Wired
Duration:	4 days 3 hours 15 minutes
IP Address:	10.25.80.13
Hostname:	
Usage:	16.8 Kbps
Security Mode:	

The Future?


GIVES YOU WINGS
GIVES YOU WINGS
Red Bull
ASTON MARTIN
Mobil 1

Aandachtspunten

HTTP GET

Importeren CPPM Intermediate HTTPS Certificate

VLAN DATABASE (Per User Tunneled Node)

Configureren VLAN op switch en Mobility Controller

TRAFFIC

Broadcast & multicast

METHODE

User-Roles vs “traditioneel”

Some legacy secure client access functionality is not supported when user roles are enabled.

aruba
a Hewlett Packard Enterprise company

AIRHEADS meetup

Thank You

@rene_booches

rene@4ip.nl