AIRHEADS meetup

aruba
a Hewlett Packard Enterprise company

ClearPass Wired Lessons Learned

14 November 2018

Frank van Breugel

#ArubaAirheads

Wie ben ik?

Frank van Breugel

1. Wie heeft ClearPass Wired al eens uitgerold?
2. Wie heeft ClearPass Wired al vaker dan 5 keer uitgerold?
3. Wie heeft ClearPass Wired uitgerold op andere merken switches dan Aruba?


Multiple VLAN's
Controlled-direction
User-based
Port-based
MAC-pinning
DUR
Dynamic
Segmentation


ROME
ROME
ROME
ROME

Firmware upgrade?

Waarom zou je de laatste switch firmware installeren?

- Omdat TAC/support dit adviseert?
- Laatste features?
- Bugfixes?

Firmware upgrade?

switch-lab# sh radius

Status and Counters - General RADIUS Information

Deadtime(min) : 0
Timeout(secs) : 5
Retransmit Attempts : 3
Global Encryption Key :
Dynamic Authorization UDP Port : 3799

Server IP Addr	Auth Port	Acct Port	DM/ CoA	Time Window	Encryption Key
11.2.168.192	1812	1813	Yes	30	Aruba123!

Firmware upgrade?

Filter: Request ID ▾ contains ▾ [+] Go Clear Filter

#	Server	Username	Service	Login Status	Request Timestamp ▾
1.	192.168.2.11	4448c1c6aa96	MAC	ACCEPT	2018/11/10 21:18:04
2.	192.168.2.11	4448c1c6aa96	802.1x	REJECT	2018/11/10 21:13:53

Radius:IETF:NAS-Port	1
Radius:IETF:NAS-Port-Id	1
Radius:IETF:NAS-Port-Type	15
Radius:IETF:Service-Type	10
Radius:IETF:User-Name	4448c1c6aa96

Radius:IETF:NAS-Port	1
Radius:IETF:NAS-Port-Id	1
Radius:IETF:NAS-Port-Type	15
Radius:IETF:Service-Type	2
Radius:IETF:User-Name	4448c1c6aa96

Multiple VLANs per port

Welke use-cases?

- Instant AP
- Hospitality AP
- ?

Ondanks use-case wil je uiteraard wel een colorless port.

Aruba vs de rest

Provision OS/ASIC ken geen access of trunk port!

Multiple VLANs per port

Voorbeeld (tagged 88, untagged 1)
VLAN 88 -> HEX 58
0x31 tagged / 0x32 untagged
0x31000058 -> DEC 822083672 (tagged vlan 88)

VLAN 1 -> HEX 1
0x32000001 -> DEC 838860801 (untagged vlan 1)

Summary | Input | **Output** | Accounting

Enforcement Profiles:	TRUNK PORT IAP
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Hewlett-Packard-Enterprise:HPE-Egress-VLAN-ID	822083672
Radius:Hewlett-Packard-Enterprise:HPE-Egress-VLAN-ID	822083772
Radius:Hewlett-Packard-Enterprise:HPE-Egress-VLAN-ID	822083784
Radius:Hewlett-Packard-Enterprise:HPE-Egress-VLAN-ID	838860801
Radius:IETF:Session-Timeout	10800

```
2930F# sh vlan ports 1 detail

 Status and Counters - VLAN Information - for ports 1

  VLAN ID Name                | Status     Voice Jumbo Mode
  ------- ------------------- + ---------- ----- ----- --------
  1       DEFAULT_VLAN        | Port-based No    Yes   Untagged
  88      LAB88               | Port-based No    No    Tagged
  188     LAB188              | Port-based No    No    Tagged
  200     Guest               | Port-based No    No    Tagged
```

Port-based/user-based

Wat is het verschil?

Welke use-cases?

- Instant AP
- Hospitality AP
- End-user met VM’s
- Specifieke apparaten met meerdere mac-adressen (ademlucht pomp met Siemens PLC)

Port-based/user-based

```
2930F# sh port-access  sum

 Port Access Status Summary

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No
  Use LLDP data to authenticate [No] : No

  Note: * indicates values dynamically overridden by RADIUS.

       |   Authenticator     |   Web Auth    |      MAC Auth
  Port | Enable Mode  Limit | Enable Limit | Enable Mode  Limit
  ---- + ------ ----- ----- + ------ ----- + ------ ----- -----
  1    | Yes    User  10    | No     1     | Yes    User  10
```

```
2930F(config)# sh port-access  sum

 Port Access Status Summary

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No
  Use LLDP data to authenticate [No] : No

  Note: * indicates values dynamically overridden by RADIUS.

       |   Authenticator     |   Web Auth    |      MAC Auth       | Local MAC
  Port | Enable Mode  Limit | Enable Limit | Enable Mode  Limit | Enable Limit
  ---- + ------ ----- ----- + ------ ----- + ------ ----- ----- + ------ -----
  1    | Yes    User  10    | No     1     | Yes    Port* 10    | No     1
```

Enforcement Profiles:	TRUNK PORT IAP, Port-mode MAC
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Hewlett-Packard-Enterprise:HPE-Egress-VLAN-ID	822083672
Radius:Hewlett-Packard-Enterprise:HPE-Egress-VLAN-ID	822083772
Radius:Hewlett-Packard-Enterprise:HPE-Egress-VLAN-ID	822083784
Radius:Hewlett-Packard-Enterprise:HPE-Egress-VLAN-ID	838860801
Radius:Hewlett-Packard-Enterprise:HPE-Port-Dot1x-Client-Limit	0
Radius:Hewlett-Packard-Enterprise:HPE-Port-MA-Port-Mode	1
Radius:IETF:Session-Timeout	10800

‘Sleepy’ devices

Wat is een ‘sleepy’ device?

Welke ‘hulpmiddelen’ zijn er?

- controlled-direction in
- mac-pin
- ip client-tracker (trusted/untrusted)
- Monitoring tool

AIRHEADS COMMUNITY

AIRHEADS meetup

aruba
a Hewlett Packard Enterprise company

AIRHEADS
meetup

Thank You

frank@deltics.nl
mrtwentytwo @AIRHEADS

Caution

1. Chassis switches per module uitrollen
2. DACL op oudere non Provision ASIC switches (2610/2530/etc)