AIRHEADS meetup

aruba
a Hewlett Packard Enterprise company

#ArubaAirheads

AIRHEADS meetup

aruba
a Hewlett Packard Enterprise company

MobileFirst Dynamic Segmentation

Dik van Oeveren – Aruba Consulting System Engineer

November 14, 2018

#ArubaAirheads

Agenda

- Introduction to colorless ports
- Port Based Tunneling
- User Based Tunneling
- How does it work
- Speeds and Feeds
- Demonstration

Introduction to colorless ports

Optional subtitle

Understanding Connectivity Options

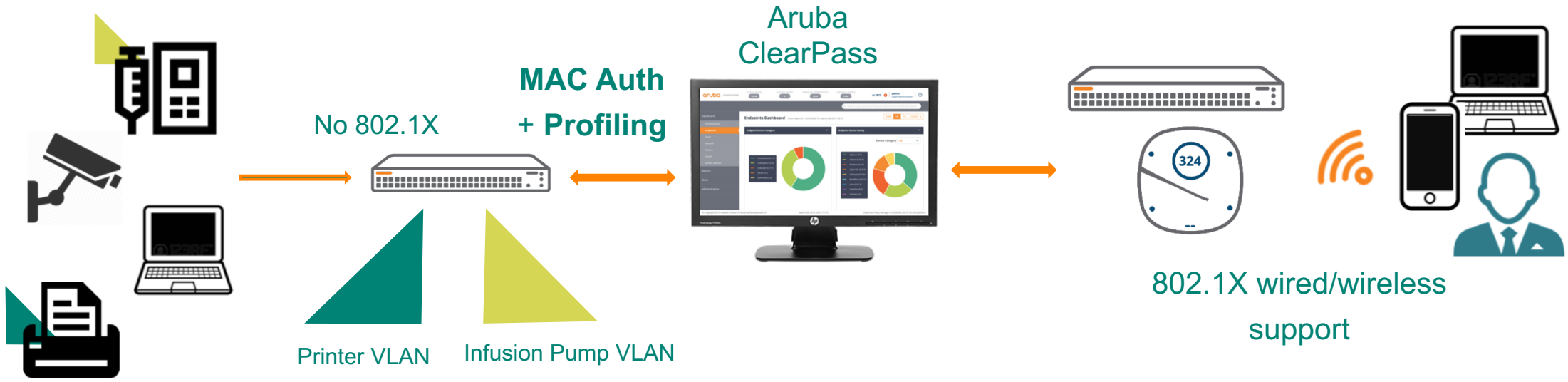
Customers want to **manage** what devices connect

Only some support .1X supplicants

50% of IoT may be wired

- ClearPass supports any customer Infrastructure and need

802.1X + MAC Auth + Profiling => Colorless ports



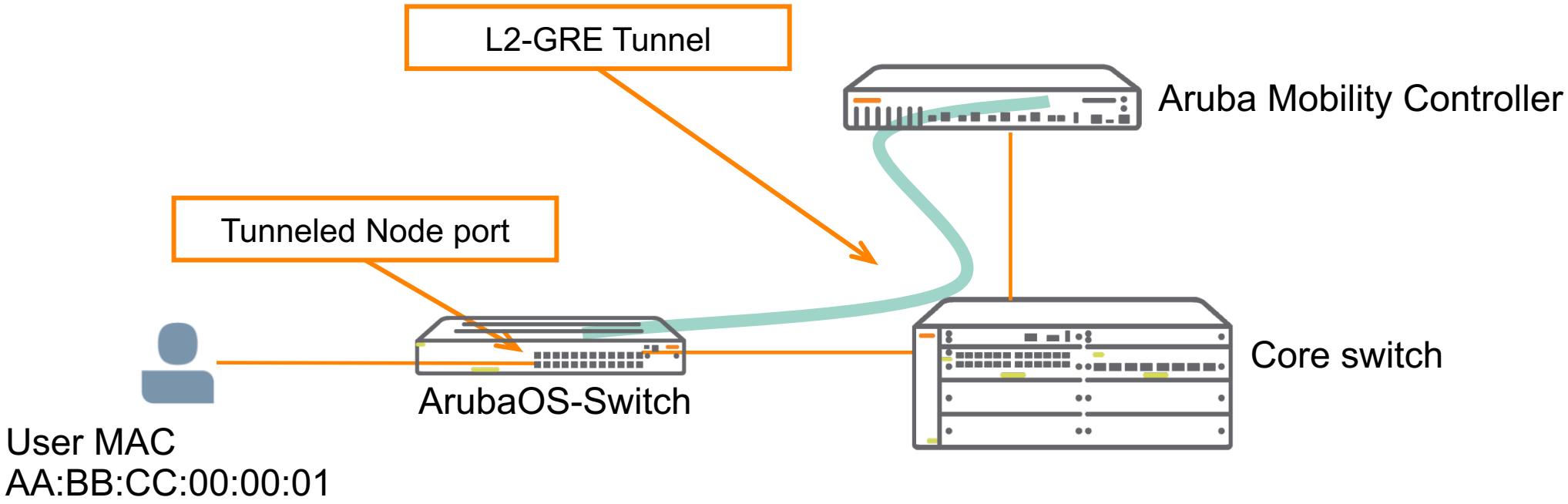
- Use 802.1X whenever possible
- Fallback to MAC authentication for non 802.1X capable devices
- Leverages ClearPass profiling for wired/wireless - IoT, laptops, mobile phones.

Port Based Tunneling

Optional subtitle

Port Based Tunnel: What is it?

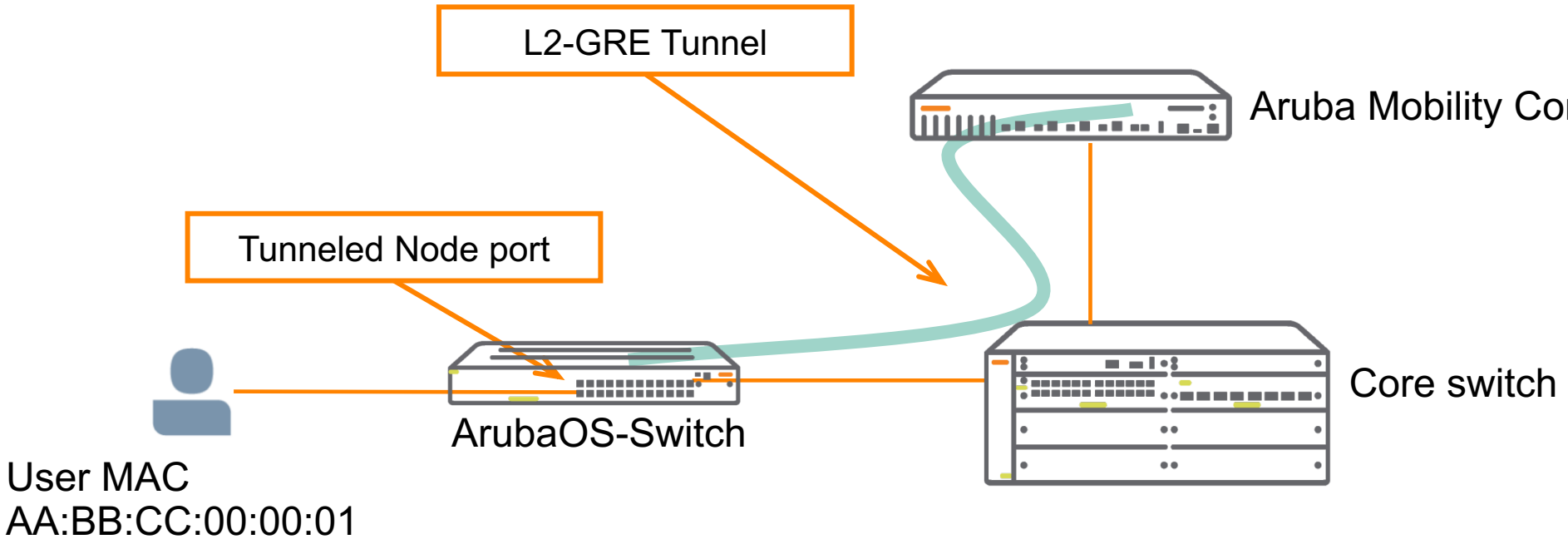
- Traffic on wired switch port is handled by central Aruba Mobility Controller
- It's a tunnel, therefore MAC address table size relief on the intermediate devices



Port Based Tunnel: Advantages

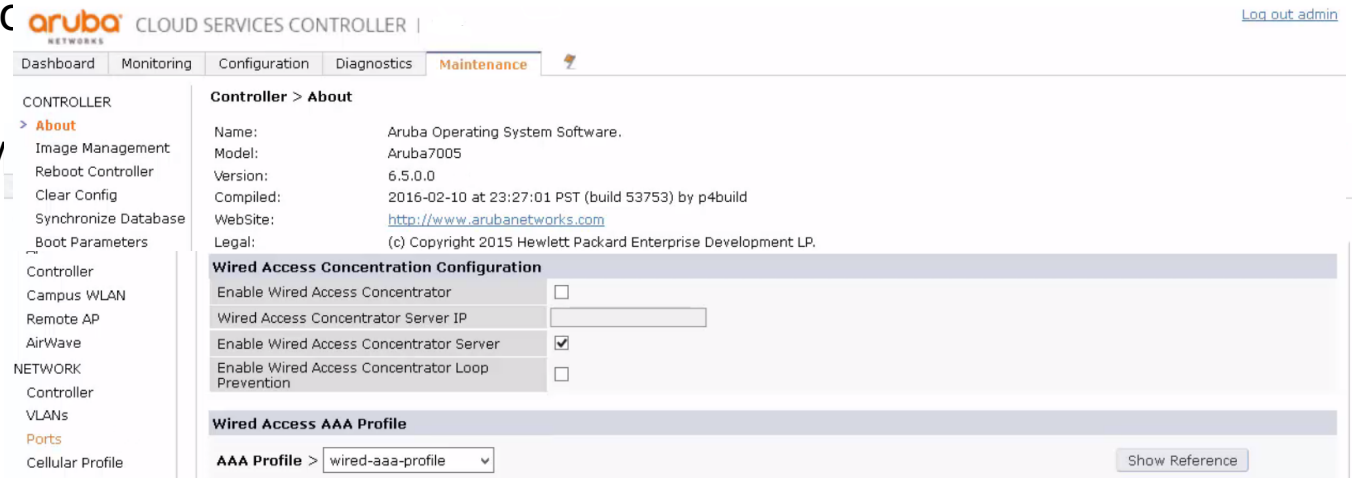
- Advanced Aruba controller features available for wired access
  - Device authentication (Captive portal, 802.1X, MAC authentication)
  - Device fingerprinting
  - Firewall
  - Deep packet inspection

Wired and wireless centralized Control

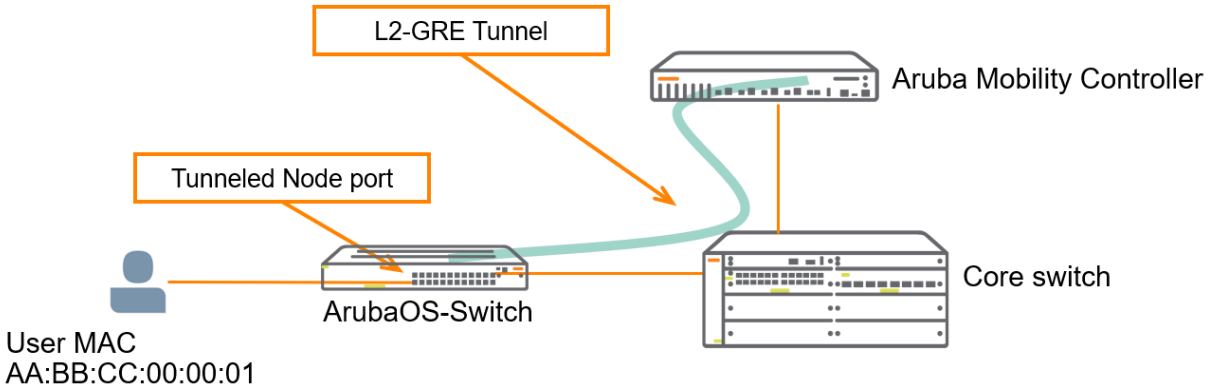


Port Based Tunnel: How does it work?

- On the mobility controller:
  - Ensure that the MC runs version AOS 6.5 or later
  - Enable Wired Access Concentrator server (c
  - Set the appropriate AAA profile
  - Ensure that the switch VLAN exists on the M
  - Switch port that is connected to the MC has
- On the switch:
  - Configure the tunnel node server, this is the
  - Enable tunneled-node on the access port




```
tunnel(config)# interface controller-ip 1.2.3.4
access(eth-2)# tunneled-node-server
```



Port Based Tunnel: Considerations

- Avoid plugging access points into wired tunneled-node ports
  - This creates a “tunnel within a tunnel”, which can impact performance
  - Instead, set aside physical ports to use solely for access points and wired tunneled node ports (i.e. one block of ports for AP’s, one for wired tunneled node ports)
  - New option in 16.05 allows device profiles to have a “`no allow-tunneled-node`” setting that prevents this
- Ensure that the wireless controller can handle the necessary bandwidth and number of tunnels
- Ensure that the Tunneled-Node VLAN is present and enabled on both the controller and switch
- The VLAN on the access switch must not have an IP address (Layer 2 only)
- Required licenses on the Mobility Controller: AP (one per tunnel)
- Optional Licenses on the Mobility Controller: Policy Enforcement Firewall (one per tunnel)

User Based Tunneling

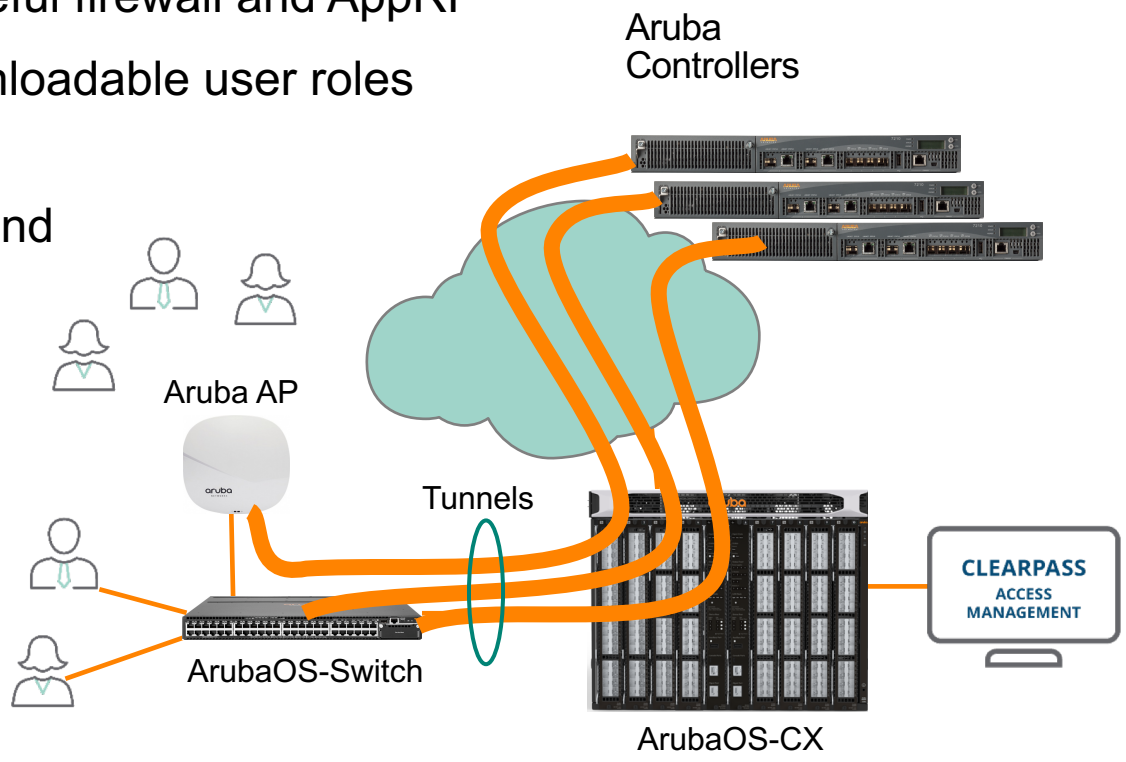
Optional subtitle

User Based Tunnel: What is it?

- UBT uses the concept of a colorless access port
- It doesn't matter what you connect to the port
  - Roles and policies are assigned per device
- Authentication takes place at the access port level
  - Successful authentication enforces VLAN and ACL assignments
  - Successful authentication creates a per user tunnel to the Mobility Controller
  - Mobility Controller can enforce additional security

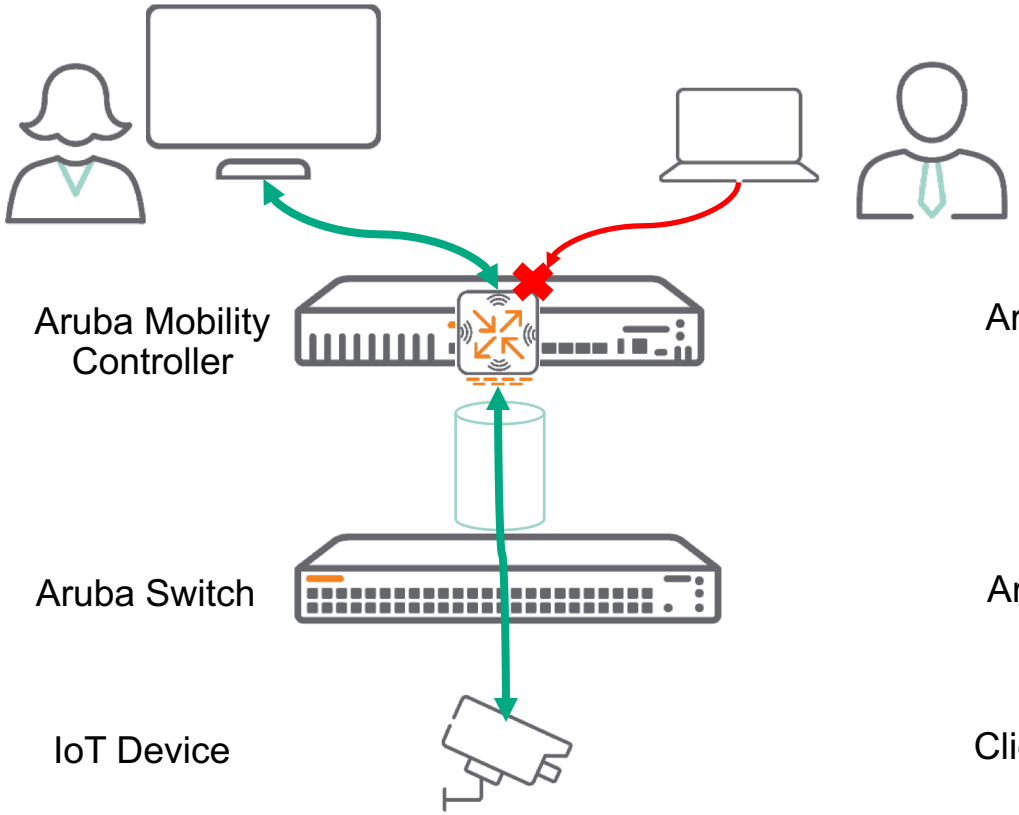
User Based Tunnel

- Secured and flexible control of access layer
  - With ClearPass or switch configuration, only traffic from a specific user/device role is sent to the Mobility Controller
  - Policies (e.g., QoS, ACL, rate-limit) can be enforced at Tunneled Node ports or at the controller
- Access to Controller's applications
  - Users can access Controller's applications such as stateful firewall and AppRF
- Policy enforcement is achieved by local user roles or downloadable user roles
  - Local user roles are configured on the switch
  - Downloadable user roles are configured on ClearPass and pushed to the switch
- High availability and scalability
  - Load balance to multiple controllers for high scalability
  - Stateful failover to standby mobility controller
- Supported on 5400R/v3, 3810M, and 2930F/M
- Requires AOS 8.1 or later on the Mobility Controllers

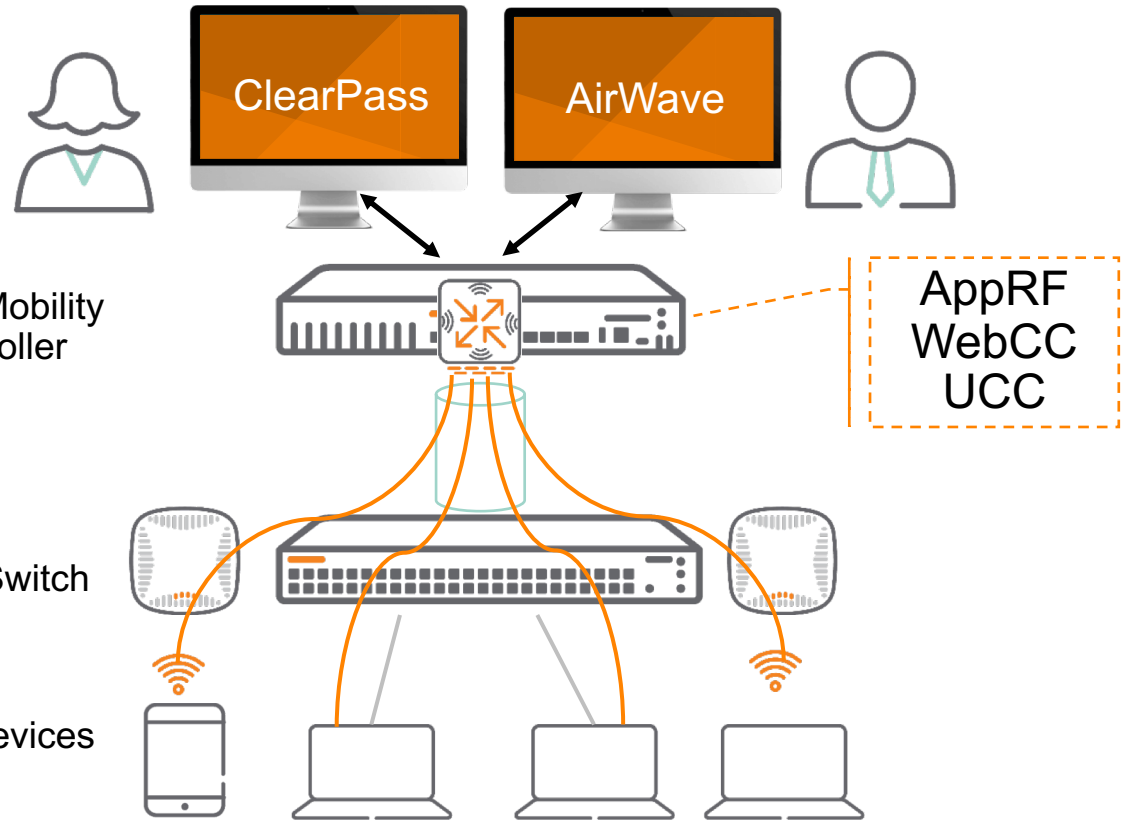


User Based Tunnel use cases

Critical client protection

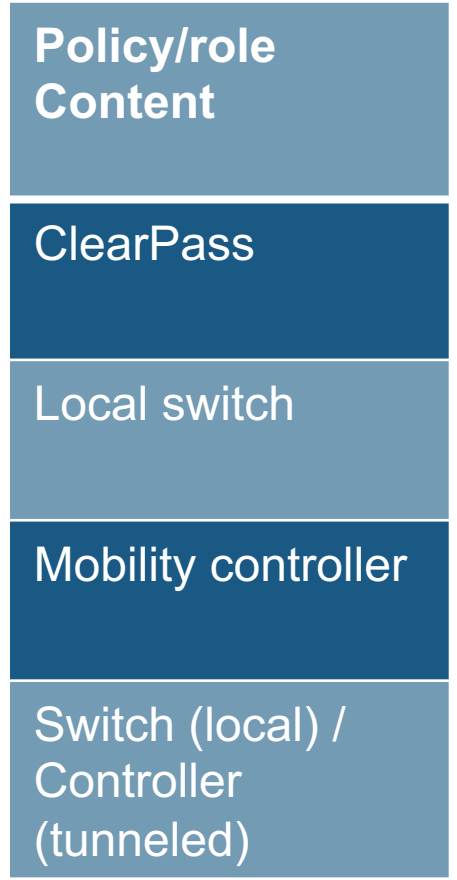


Unified policy and visibility



Downloadable roles (ArubaOS 16.05)

- Starting ArubaOS 16.05, Downloadable user roles are supported with ClearPass 6.7.0+
- This feature allow you to define the role content in ClearPass instead of locally on the switch
- ArubaOS for wireless supports Downloadable roles for a while already
- Pro's for central defined roles (ClearPass):
  No need to go in each switch/controller if roles need to be defined, or changed.
- Pro's for local defined roles:
  Easier to make role content location specific (example: floor VLAN, location VLANs)
  Less moving parts
- You have both options available in your toolkit



User Based Tunnel: Terminology

- Tunneled Node Switch: The switch on which the tunnel profile is configured
- Tunneled Node Profile: Set of parameters required to be set (controller IP, backup controller IP, etc)
- Tunneled Node Interface: Interface on which the tunnel is configured.
- Client Device: Edge device connected to a tunneled port which is authenticated by credentials like Username/Password or mac authentication.
- Primary controller: Aruba Mobility Controller working as a tunnel server
- Back-up controller: Aruba back-up Mobility Controller working as backup tunnel server
- Radius server: ClearPass
- User Anchor Controller: Mobility Controller that functions as tunnel server for the clients
- Switch Anchor Controller: Mobility Controller that is used to provide services information to the switch

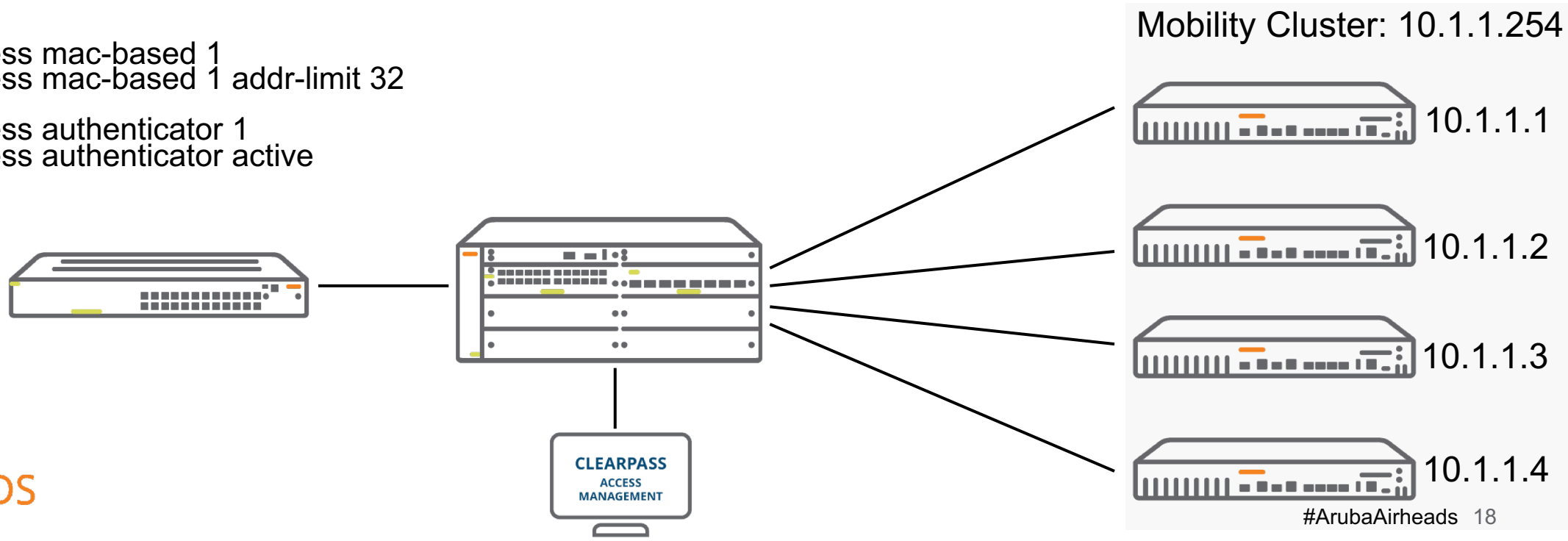
Confused?

User Based Tunnel: How does it work with local user roles

- Switch Configuration:

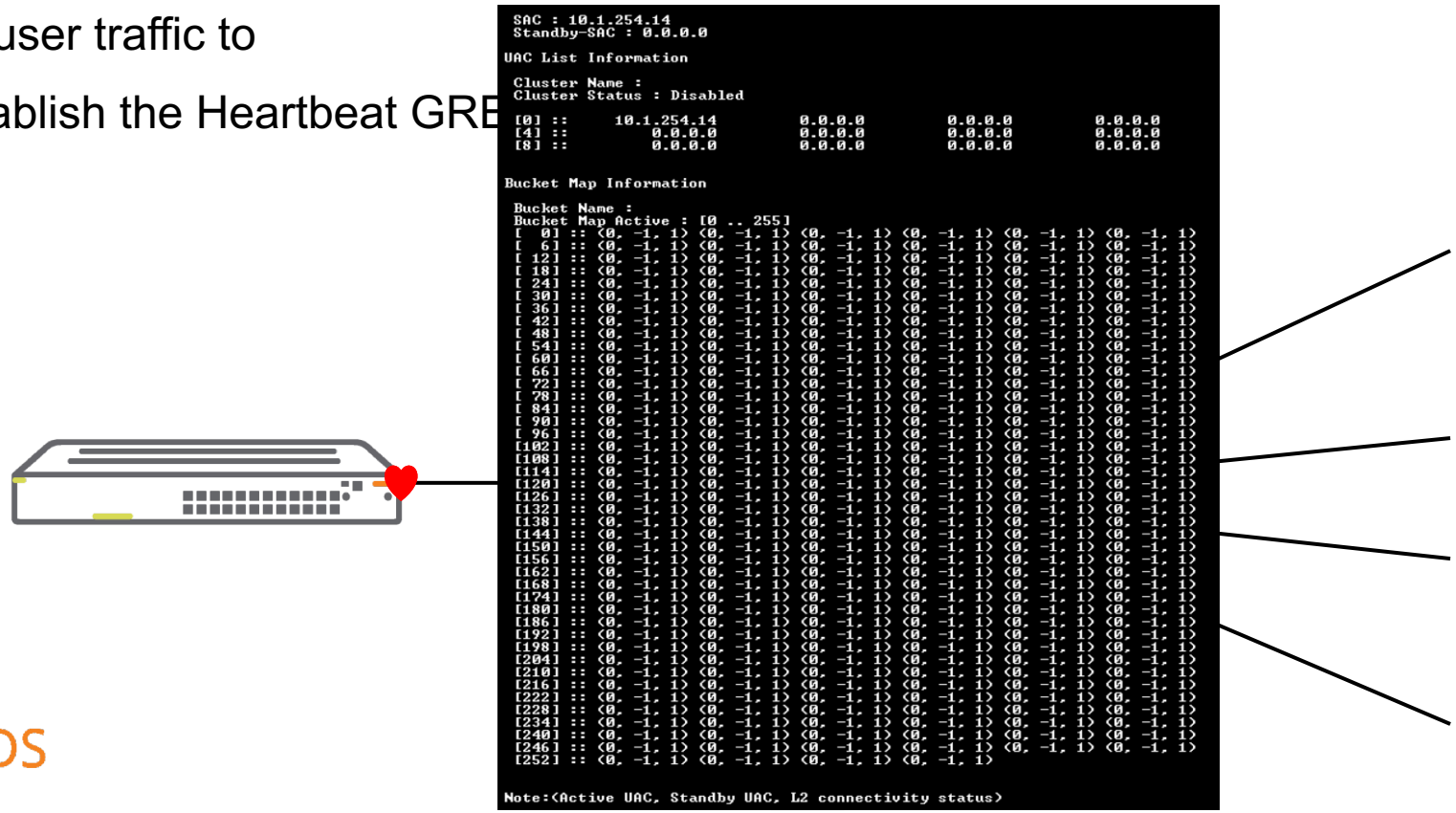
Tunneled node server config:
tunneled-node-server
  controller-ip 10.1.1.254
  mode role-based
VLAN and secondary-role config:
aaa authorization user-role enable
aaa authorization user-role name “employee-role"
  vlan-id 30
  tunneled-node-server-redirect secondary-role “MC-role"
  exit
MAC Auth:
aaa port-access mac-based 1
aaa port-access mac-based 1 addr-limit 32
Dot1X:
aaa port-access authenticator 1
aaa port-access authenticator active

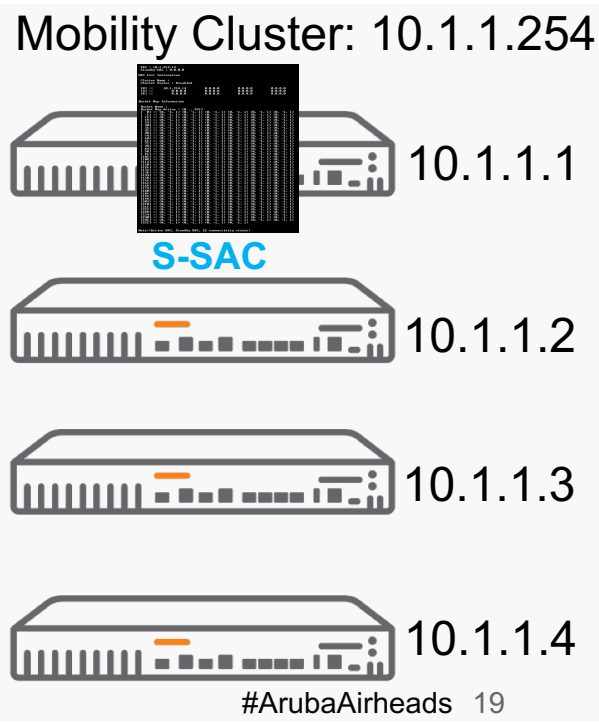
After successful authentication, this rule is sent to the Mobility Controller for enforcement on the Mobility Controller



User Based Tunnel: How does it work with local user roles

- Switch and Mobility Cluster (10.1.1.254) negotiate feature support (per user or per port)
- Switch establish the Heartbeat GRE tunnel with the Switch Anchor Controller (10.1.1.1) GRE tunnel
- 10.1.1.1 acknowledges the request with cluster information including Secondary-SAC (backup: 10.1.1.2), node list and bucket map. The bucket map is an array of 256 entries with each entry containing the active and standby User Anchor Controller to use. A user's mac address is hashed into this table to get the controller to tunnel the user traffic to
- Switch establish the Heartbeat GRE

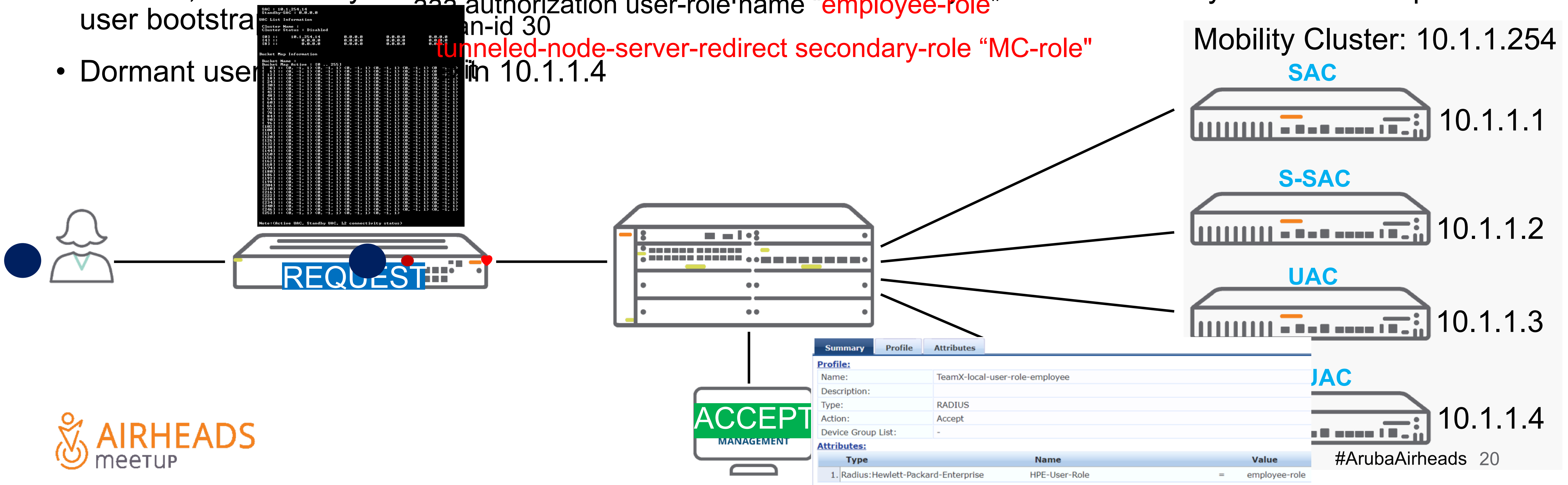




User Based Tunnel: How does it work with local user roles

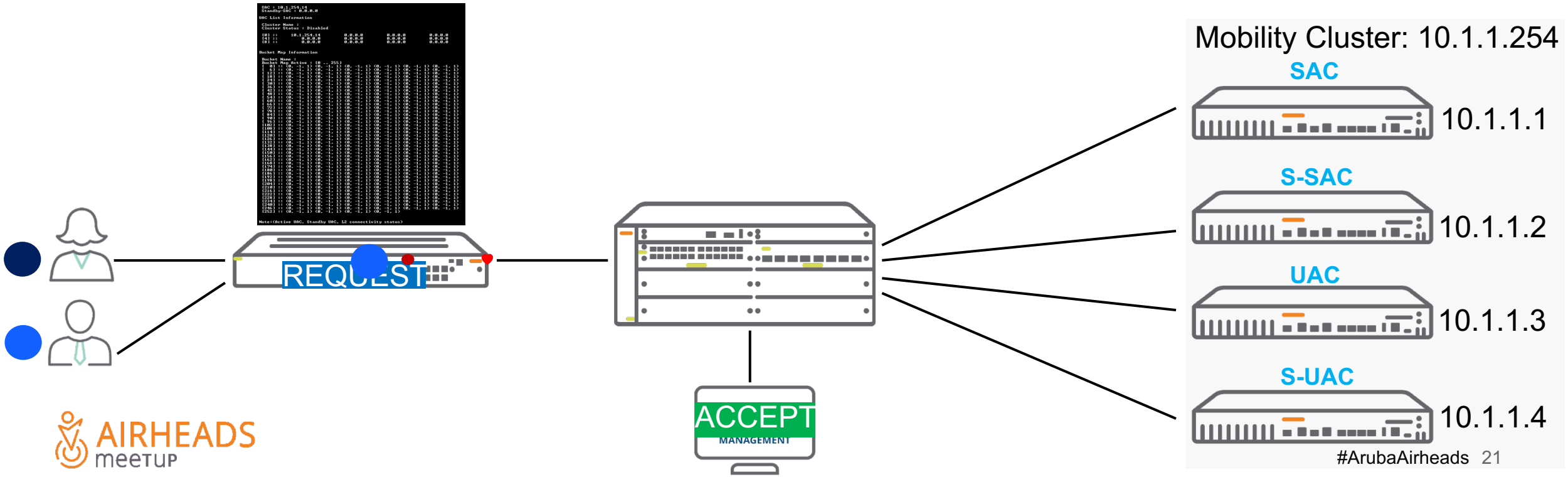
- Client connects to secure port 1
- Authentication takes place and ClearPass returns the local configured user role VSA
- Switch checks the bucket map to find the UAC information. Bucket map says that the UAC for the client is 10.1.1.3 and the Secondary UAC is 10.1.1.4
- Switch establishes a UAC GRE tunnel by sending the user bootstrap to 10.1.1.3, this is acknowledged by 10.1.1.3, a user entry is created in the bucket map. The secondary user role is sent by the switch as part of user bootstra
- Dormant user … in 10.1.1.4

aaa authorization user-role name "employee-role"
…an-id 30
tunneled-node-server-redirect secondary-role "MC-role"



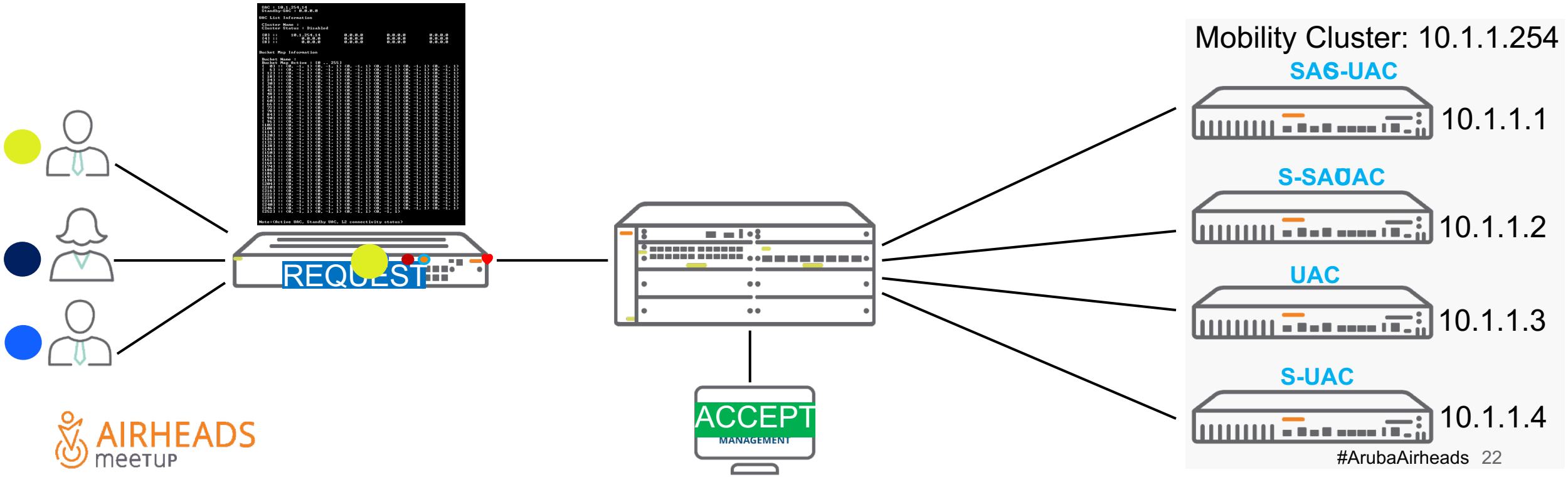
User Based Tunnel: How does it work with local user roles

- Another client connects to secure port 1, authenticated with ClearPass and same user-role is applied
- The bucket map is queried and switch establishes a GRE tunnel to 10.1.1.3 and the secondary user role is applied
- Dormant entry is added to 10.1.1.4
- The second client uses the same GRE tunnel as the first client because the tunnel is already present



User Based Tunnel: How does it work with local user roles

- Another client connects to secure port 2, authenticated with ClearPass and same user-role is applied
- The bucket map is queried (UAC can be a different controller) and switch establishes a GRE tunnel to 10.1.1.2 and the secondary user role is applied
- Dormant entry is added to 10.1.1.1 (S-UAC can be a different controller)
- The second client created a new GRE tunnel because the edge device termination is on a different port



User Based Tunnel: What about downloadable user roles

- The process is very much the same, instead of having the user role configured on the edge switch, it is configured on ClearPass and sent to the edge switch after successful authentication
- The method for sending the user role is through REST API using an SSL connection
- This means that a HTTPS certificate has to be installed on the edge switch
- In addition, a username/password has to be configured to authenticate the switch with ClearPass
- Let’s have a look how this is done

User Based Tunnel: What about downloadable user roles

- First, ensure that ClearPass has obtained a valid HTTPS certificate
- Export the root certificate that is located on ClearPass and install it on the switch
- On ClearPass, create a read only admin user that will be used by the switch for authentication
- On the switch, create the user entry for the read only user and enable downloadable user roles
- And configure the downloadable user roles profiles
- Assign the profiles to a policy and the policy to a service

Configuration » Enforcement » Profiles » Edit Enforcement Profile - TeamX-dur-employee

Enforcement Profiles - TeamX-dur-employee

Summary | Profile | Attributes

	Type	Name		Value
1.	Radius:Hewlett-Packard-Enterprise	HPE-CPPM-Role	=	class ipv4 "employee-class-dur" 10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 exit policy user "employee-policy-dur" 10 class ipv4 "employee-class-dur" action permit exit aaa authorization user-role name "employee-dur" policy "employee-policy-dur" vlan-id 10 tunneled-node-server-redirect secondary-role "authenticated" exit
2.	Click to add...			

User Based Tunnel: What about downloadable user roles

- Check out what is happening on the switch

```
0000:00:09:16.46 UMIB mdcaCtrl:added new dca client dc4a3e-d02939 for new client port 1.
0000:00:09:16.55 UMIB mdcaCtrl:Client MAC: dc4a3e-d02939, access mode session: 6, access method: PORT-ACCESS, User Name: user1, Calling-Station-Id: dc4a3e-d02939, NAS-Port-Id: 1, NAS-IP-Address: 10.1.254.101.
0000:00:09:16.75 TLOG mdcaCtrl:Sending User Tunnel Add request for the client dc4a3e-d02939 for port 1
0000:00:09:17.44 UMIB mdcaUserCtrl:Received downloadable user role vsa for client with request-id 6 and assigned user role is TeamX_dur_employee-3012-2
0000:00:09:17.82 UMIB mdcaUserCtrl:New user dc4a3e-d02939 added to the downloadable user role TeamX_dur_employee-3012-2
0000:00:09:17.99 UMIB mdcaUserCtrl: Client with request-id 6 is added to waiting queue for downloadable user role TeamX_dur_employee-3012-2 in INITIAL state
0000:00:09:17.96 UMIB mdcaUserCtrl:Download of userRole TeamX_dur_employee-3012-2is success
0000:00:09:18.04 UMIB mdcaUserCtrl: Sending message to authentication task for client with request-id 6
0000:00:09:18.13 1X m8021xCtrl:Port 1: Received Auth Success for client dc4a3e-d02939, User user1.
0000:00:09:18.24 UMIB mdcaUserCtrl:Created parent node for downloadable user role TeamX_dur_employee-3012-
0000:00:09:18.35 1X m8021xCtrl:Port 1: MAC dc4a3e-d02939 RADIUS Attributes, vid: 10.
0000:00:09:18.39 TLOG mdcaCtrl:Tunnel Status Up for dca client dc4a3e-d02939 for port 1.
```

```
0000:00:09:16.56 1X m8021xCtrl:Port 1: connection detected.
0000:00:09:16.33 RAD mRadiusCtrl:ACCESS REQUEST id: 28 to 10.1.254.12 8021x
0000:00:09:16.63 PSEC m8021xCtrl:Calling added new dc4a3e-d02939 to authorized addr list of port 1 for vlan 10.
0000:00:09:16.55 RAD tRadiusR:ACCESS ACCEPT id: 28 from 10.1.254.12 received.
0000:00:09:17.49 UNIT mtnodeUserCtrl:Bucket pm 192 initialized
0000:00:09:17.63 TNT mtnodeUserCtrl:Entering userTNodeTCAMDecapReserveResources
0000:00:09:17.79 UNIT mtnodeUserCtrl:Node is created for the
0000:00:09:17.79 UNIT mtnodeUserCtrl:UAC Bootstrap to node: 10.1.254.14
0000:00:09:17.87 TNT mtnodeUserCtrl:userTNodeSendUACBStrapReq: Packet Sent Successfully
0000:00:09:17.51 UNIT mupperTaskCtrl:User dc4a3e-d02939 bootstrapping
0000:00:09:18.02 RAD tRadiusR: ACCOUNTING RESPONSE id: 29 from 10.1.254.12 received.
0000:00:09:18.13 RAD tRadiusR:Removing RADIUS REQUEST id: 29 from queue.
0000:00:09:18.21 TNT mtnodeCtrl:Create a tunnel: port 1 uac: a0a010a ifindex: 0 count: 0
0000:00:09:18.31 TNT mtnodeUserCtrl:User dc4a3e-d02939 tunneling to 31876775
```

User Based Tunnel: What about downloadable user roles

- Check out what is happening on the switch (this is for an 802.1X authenticated user)

```
Port Access Client Status Detail

 Client Base Details :
   Port              : 1                       Authentication Type  : 802.1x
   Client Status     : authenticated           Session Time         : 262 seconds
   Client name       : user1                   Session Timeout      : 0 seconds
   MAC Address       : dc4a3e-d02939
   IP                : n/a
Downloaded user roles are preceded by *

 User Role Information

   Name                                 : *TeamX_dur_employee-3012-4
   Type                                 : downloaded
   Reauthentication Period (seconds)    : 0
   Untagged VLAN                        : 10
   Tagged VLANs                         :

   Captive Portal Profile               :
   Policy                               : emp-policy-dur_TeamX_dur_employee-3012-4

Statements for policy "emp-policy-dur_TeamX_dur_employee-3012-4"
policy user "emp-policy-dur_TeamX_dur_employee-3012-4"
     10 class ipv4 "emp-class-dur_TeamX_dur_employee-3012-4" action rate-limit
 kbps 1000 action priority 2 action permit
   exit


Statements for class IPv4 "emp-class-dur_TeamX_dur_employee-3012-4"
class ipv4 "emp-class-dur_TeamX_dur_employee-3012-4"
     10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
     20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
   exit

   Tunnelednode Server Redirect         : Enabled
   Secondary Role Name                  : authenticated
```

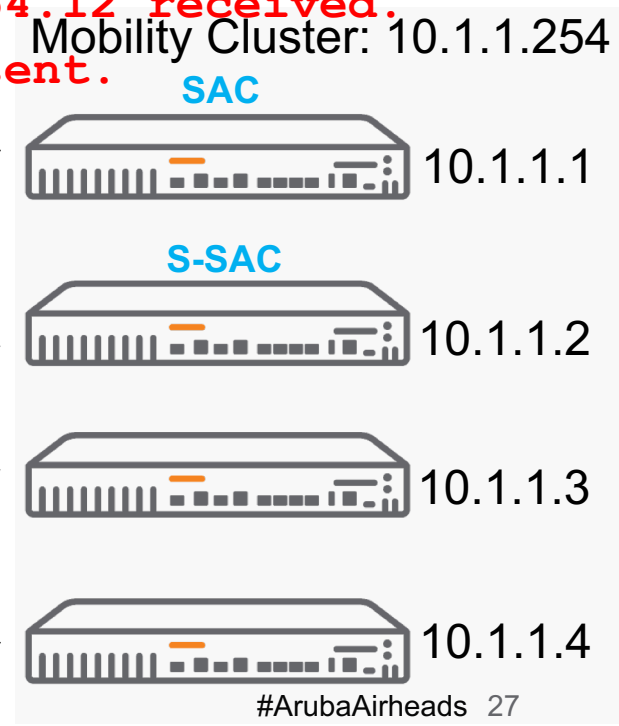
User Based Tunnel: Captive Portal

- Captive Portal is also supported. ClearPass captive portal configuration process is the same as regular captive portal. In the MAC Auth profile and Web Auth profile a Downloadable User Role has to be configured
- The authentication process consists of three steps:
- MAC Authentication (Allow All MAC), can be a tunnel, but can also be locally switched
- Web Authentication (if succes the access port)
- Second MAC Authentication

```
0000:00:06:59.25 RAD  t                                    10.1.254.12 received.
0000:00:06:59.33 RAD  t                                    54.12 sent.
```

```
Port Access Client Status Detail

 Client Base Details :
  Port             : 1                    Authentication Type : mac-based
  Client Status    : authenticated        Session Time        : 402 seconds
  Client Name      : dc4a3ed02939         Session Timeout     : 0 seconds
  MAC Address      : dc4a3e-d02939
  IP               : n/a
Downloaded user roles are preceded by *
```

```
Port Access Client Status Detail

 Client Base Details :
  Port             : 1                    Authentication Type : mac-based
  Client Status    : authenticated        Session Time        : -3128 seconds
  Client Name      : dc4a3ed02939         Session Timeout     : 0 seconds
  MAC Address      : dc4a3e-d02939
  IP               : n/a
Downloaded user roles are preceded by *

User Role Information

  Name                              : *TeamX_dur_MacAuth-3015-5
  Type                              : downloaded
  Reauthentication Period (seconds) : 0
  Untagged VLAN                     : 11
  Tagged VLANs                      :

  Captive Portal Profile            :
0000:00:14:38.20 1X   m8021xCtrl:Port 1: sent ReqId #7 to 0180c2-000003.
  Policy                            : guest-policy-dur_TeamX_dur_MacAuth-3015-5

Statements for policy "guest-policy-dur_TeamX_dur_MacAuth-3015-5"
policy user "guest-policy-dur_TeamX_dur_MacAuth-3015-5"
    10 class ipv4 "guest-class-dur_TeamX_dur_MacAuth-3015-5" action rate-limit
kbps 1000 action priority 2 action permit
  exit

Statements for class IPv4 "guest-class-dur_TeamX_dur_MacAuth-3015-5"
class ipv4 "guest-class-dur_TeamX_dur_MacAuth-3015-5"
    10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
    20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
  exit

  Tunnelednode Server Redirect      : Enabled
  Secondary Role Name               : authenticated
  Secondary Role Name               :
```



AIRHEADS meetup

Speeds and Feeds

Optional subtitle

User Based Tunnel: Speeds and feeds

Controller	Maximum supported tunnels
7280	34816
7240 /7240XM	34816
7220	17408
7210	8704
7205	4352
7030	1088
7024	544
7010	544
7008	272
7005	272

Switch or stack	Maximum Supported User Tunnels per Switch or Stack	Maximum Supported User Tunnels per port
5400R	1024	32
3810M	1024	32
2930M	1024	32
2930F	1024	32

User Based Tunnel: Speeds and feeds

- Mutually exclusive with User Based Tunneling:
  - Port Based Tunnel
  - Meshing
  - QinQ
- Not configurable on a tunneled user port:
  - ARP Protect, DHCP Relay, DHCP Server, DHCP Snooping, IGMP, MLD, mDNS, OpenFlow, Portal commands, sFlow, RA Guard
- VLAN's that are used for User Based Tunneling have to be configured on the switch
  - No dynamic VLAN creation when pushing the user role
  - These VLAN's don't have IP addresses assigned
- Jumbo frames preferred to be enabled on the switches forming the path to the controller
  - GRE adds 46 byte header, which makes maximum payload size 1454 bytes

Demonstration

Optional subtitle

aruba
a Hewlett Packard Enterprise company

AIRHEADS meetup

Thank You