Dynamic Segmentation 2.0
Simplificación y automatización de la red cableada

Antonio Sáez – antonio.saez@hpe.com
Dynamic Segmentation?

Traditional Campus Network

- Centralized WLAN
- Distributed LAN?

East-West vs North-South?
Traffic flows?

- WLAN – Overlay mode
- LAN – “Native” mode
easy to deploy new services?
security?

- WLAN – Statefull Firewall, L7 application aware, Content filtering, …
  (µSegmentation)
- LAN – ACLs, L4 ports,…
more features?
more control?

![Diagram of Aruba Network Components](image-url)
What is Dynamic Segmentation?

ClearPass role-based policy provides the “Dynamic”

“Segmentation” refers to the separation of traffic

Users and Devices
- Corp
- BYOD
- IOT
- Guest

Applications and Destinations
- Office 365
- Academic Records
- ndtware.biz
- AirGroup

Access Switch
Access Point
Campus Controller Cluster
ClearPass

What is Dynamic Segmentation?

Campus Controller Cluster
ClearPass role-based policy provides the “Dynamic”

“Segmentation” refers to the separation of traffic

Users and Devices
- Corp
- BYOD
- IOT
- Guest

Applications and Destinations
- Office 365
- Academic Records
- ndtware.biz
- AirGroup

Access Switch
Access Point
Campus Controller Cluster
ClearPass
Dynamic Segmentation Orchestration of services

Where does Dynamic Segmentation play today?

**Enterprise Campus (Large Site)**
Traditional controller-based architecture with APs and switches

**SD-Branch (Distributed Sites)**
Central-managed Branch Gateways with APs and switches (SD-LAN)
Dynamic Segmentation: Key Value Propositions
Use role-based access and profiling that follows the user for better segmentation

Automated Policy
Save time and reduce errors by eliminating manual configuration

Segmented Policy
Separate traffic to enhance network security posture

Centralized Policy
Define rules that leverage user, device, app, location data in one place

Dynamic Segmentation Deep Dive
Downloadable User Roles vs Local User Roles

**Downloadable User Roles (DUR)**
- Single point of policy management
  - Dynamically assigned by ClearPass at the time of authentication

**Local User Roles (LUR)**
- Multiple point of policy management
  - Defined in every switch on the network

---

Port Based Tunneling (legacy PPTN)

- All traffic on wired switch port is tunneled to the Mobility Controller
- Authentication takes place on Mobility Controller
  - Traffic is handled by central Aruba Mobility Controller
- It’s a tunnel, therefore MAC address table size relief on the intermediate devices
User Based Tunneling (legacy PUTN)

- 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 – Secondary Role

User Based Tunneling 2.0 enhancements

No more user VLAN requirement on the Mobility Controller and Access Switches
- The user VLAN is configured on the Mobility Controller in the role configuration
- Switch is not aware of the user VLAN anymore, this is enforced on the Mobility Controller
- Only requires a reserved VLAN for establishing the SAC tunnel (automatically created)

The root certificate for downloadable user roles is downloaded automatically
- Allows for zero touch deployment

Multicast traffic optimization

License enforcement on the Mobility Controllers for User Based Tunneling
- Per Switch IP address: Access Point (AP), Policy Enforcement Firewall (PEF) and RFProtect (RFP) license
- Mobility Controller limits are also enforced
- If a MC supports 32 AP’s, number of switches AND AP’s cannot exceed 32
- License enforcement is with UBT 1.0 and 2.0. Enforcement is done by the Mobility Controller running software release 8.4
User Based Tunneling (UBT)

UBT to a Cluster

Switch gets Switch Anchor Controller

Tunneled-node-server
controller-ip 172.30.229.211
backup-controller-ip 172.30.229.212
node role-based vlan 4000
exit

Vlan 4000 does NOT need to exist on the switch
User Based Tunneling (UBT)
UBT to a Cluster

1. Switch sets up Heartbeat/Multicast GRE tunnel with configured cluster node (MC2)

2. MC2 responds with S-SAC, Node list and Bucket map
User Based Tunneling (UBT)

**UBT to a Cluster**

1. **Switch sets up Heartbeat/Multicast GRE tunnel with configured cluster node (MC3)**
2. **MC3 responds with S-SAC, Node list and Bucket map**
3. **Switch sets up Heartbeat/Multicast GRE tunnel with S-SAC cluster node (MC1)**
4. **When client connects to switch, user authentication (dot1x/mac) takes place**
User Based Tunneling (UBT)

UBT to a Cluster

5. If derived role has redirect attribute and opt. secondary role, Switch checks bucket map to find UAC=MC1 and S-UAC=MC2

6. Switch sets up a UAC GRE tunnel with MC1, and sends the user role

Switch Config

```
aaa authorization user-role name "VideoCamera_DURUBT_USB"
tunneled-node-server-redirect secondary-role "_IOT_VideoCamera"
exit
```
User Based Tunneling (UBT)

UBT to a Cluster

5. If derived role has redirect attribute and opt. secondary role, Switch checks bucket map to find UAC=MC1 and S-UAC=MC2

6. Switch sets up a UAC GRE tunnel with MC1, and sends the user vlan and role

7. UAC creates the user entry with the secondary role sent by the switch

8. Dormant user entry is added to S-UAC
User Based Tunneling (UBT)

PCAP capture

**SAC GRE Tunnel**

- Frame 30: 184 bytes on wire (144 bits), 184 bytes captured (144 bits) on interface 0
- Ethernet II, Src: Hewlett-Packard 00:20:00:44:15:00, Dist: Aruba_AgoraTech19 00:64:00:10:51:00
- Internet Protocol Version 4, Src: 172.30.229.235, Dist: 00:18:00:00:00:00
  - Generic Routing Encapsulation (Transparent Ethernet bridging)
  - Flags and Version: 0x3000
  - Protocol Type: Transparent Ethernet bridging (0x6550)
    - Key: 0x6550
    - Sequence Number: 19013

- Ethernet II, Src: Hewlett-Packard 00:20:00:44:15:00, Dist: VMware_08:08:03:46 (00:50:56:00:40:00)
  - Destination: VMware_08:08:03:46 (00:50:56:00:40:00)
  - Source: Hewlett-Packard 00:20:00:44:15:00
  - Type: IEEE 802.3 22 Extended Ethertype (0x8886)

**UAC GRE Tunnel**

- Frame 178: 1840 bytes on wire (1472 bits), 1840 bytes captured (1472 bits) on interface 0
- Ethernet II, Src: Aruba-AgoraTech19 00:60:00:10:51:00, Dist: Hewlett-Packard 00:20:00:44:15:00
- Internet Protocol Version 4, Src: 172.30.229.235, Dist: 00:18:00:00:00:00
  - Generic Routing Encapsulation (Transparent Ethernet bridging)
  - Flags and Version: 0x2000
  - Protocol Type: Transparent Ethernet bridging (0x6550)
    - Key: 0x6550
    - Sequence Number: 1851

- Ethernet II, Src: Raspberry_06:27:eb:ab:55:14, Dist: Aruba-AgoraTech19 00:60:00:10:51:00
  - Destination: Aruba-AgoraTech19 00:60:00:10:51:00
  - Type: IPv4 (0x0800)

  - Internet Control Message Protocol
Access Control

Authentication 802.1x

Authentication MAC

Authentication

CoA

Device Profiled

Device Profiled

CLEARPASS

Role IT_Manager

Role Profiling

Role IOT_RaspPi

Role IOT_VideoCamera

Role IOT_VoIP Phone

Vlan Scope

Device to VLAN mapping does not mean Policy!!

<table>
<thead>
<tr>
<th>Vlan 101 Profiling</th>
<th>Vlan 102 IP_Telephony</th>
<th>Vlan 103 IOT</th>
<th>Vlan 104 Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITManager</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Telephone</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>IOT - RaspBerry</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>VideoCamera</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Vlan Scope

Vlan 101 – Profiling
Vlan 103 - IOT
Vlan 104 - Users

Access Layer
2930F-1# show vlans
Status and Counters - VLAN Information
Maximum VLANs to support : 256
Primary VLAN : Gestion
Management VLAN :

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Name</th>
<th>VLAN ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Gestion</td>
<td>102</td>
<td>IP_Telephony</td>
</tr>
<tr>
<td>4000</td>
<td>TUNNELED_NODE_SERVER_RESERVED</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Setting up Anchor Controllers

Debug
debug destination session
dump event
dump userns

Access Layer
tunneled-node-server
controller-ip 10.150.2.111
node role-based reserved-vlan 4000
exit

Shows Access Layer
show tunneled-node-server statistics
show tunneled-node-server state

Shows Mobility Controller
show tunneled-node-mgr state
show tunneled-node-mgr tunneled-nodes
show datapath tunnel
### Setting up Authentication Server

#### Access Layer

```plaintext
radius-server host 10.150.0.60 key "qwerty"
radius-server cppm identity "duruser" key XXXXXXX
radius-server host 10.150.0.60 clearpass
download timesync ntp
```

#### Downloable User Roles – Vlan segmentation

```plaintext
Profile: Allusers_VLAN_100_VLANPhone
Name: Allusers_VLAN_100_VLANPhone
Description: All users Phone
Type: RADIUS
Action: Accept
Device Group List: :-
Product: ArubaOS-Switch

Attributes:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>class ldap &quot;Any&quot;</td>
<td>25.25.25.254/24</td>
<td>exit</td>
</tr>
<tr>
<td>policy user tel_vlan_DUR_UA</td>
<td>102</td>
<td>exit</td>
</tr>
<tr>
<td>device-peer Pharmacy</td>
<td>'true'</td>
<td>exit</td>
</tr>
<tr>
<td>device-peer-identity</td>
<td>'true'</td>
<td>exit</td>
</tr>
<tr>
<td>device-peer-privilege</td>
<td>'true'</td>
<td>exit</td>
</tr>
<tr>
<td>device-peer-privilege</td>
<td>'true'</td>
<td>exit</td>
</tr>
<tr>
<td>device-peer-privilege</td>
<td>'true'</td>
<td>exit</td>
</tr>
<tr>
<td>device-peer-privilege</td>
<td>'true'</td>
<td>exit</td>
</tr>
<tr>
<td>device-peer-privilege</td>
<td>'true'</td>
<td>exit</td>
</tr>
<tr>
<td>device-peer-privilege</td>
<td>'true'</td>
<td>exit</td>
</tr>
<tr>
<td>device-peer-privilege</td>
<td>'true'</td>
<td>exit</td>
</tr>
</tbody>
</table>
```
Downloable User Roles - UBT

<table>
<thead>
<tr>
<th>Profile</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: ASwitch_DUR_UBT_ITManager</td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td></td>
</tr>
<tr>
<td>Type: RADIUS</td>
<td></td>
</tr>
<tr>
<td>Action: Accept</td>
<td></td>
</tr>
<tr>
<td>Device Group List:</td>
<td>-</td>
</tr>
<tr>
<td>Product: ArubaOS-Switch</td>
<td></td>
</tr>
</tbody>
</table>

Attributes:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Radius: Hewlett-Packard-Enterprise</td>
<td>RADIUS-Role = aaa authorization user-name &quot;ITManager-DUR_UBT&quot; tuned-mode-server-realm secondary-role &quot;ITManager&quot; exit</td>
</tr>
</tbody>
</table>

Secondary Role - µSegmentation

IP Telephone

VideoCamera

ITManager

IOT - RaspBerry

Mobility Controller

ip access-list session _permit_networkservices
user any svc-dhcp permit
user any svc-dns permit
alias _internalnetworks user any permit

ip access-list session _permit_telephonynetworks
user alias _telephonynetworks any permit

ip access-list session _allow-user-to-iot_videocamera
user userrole _IOT_VideoCamera any permit

ip access-list session _allow-user-to-iot_rasppi
user userrole _IOT_RaspPi any permit

user-role _ITManager
access-list session _permit_networkservices
access-list session _permit_telephonynetworks
access-list session _allow-user-to-iot_videocamera
access-list session _allow-user-to-iot_rasppi
access-list session _permit_internet
vlan Vlan104_Users

user-role _IOT_RaspPi
access-list session _permit_networkservices
access-list session _permit_telephonynetworks
access-list session _allow-user-to-iot_videocamera
vlan Vlan103_IOT

#ArubaAgoraTech19
Secondary Role - μSegmentation

ITManager

VideoCamera

SDT - Raspberry

IP Telephone

Secondary Role - μSegmentation

ITManager

VideoCamera

SDT - Raspberry

IP Telephone
Some Information

### Scalability

<table>
<thead>
<tr>
<th>Controller</th>
<th>Maximum supported tunnels</th>
</tr>
</thead>
<tbody>
<tr>
<td>7280</td>
<td>34816</td>
</tr>
<tr>
<td>7240 / 7240XM</td>
<td>34816</td>
</tr>
<tr>
<td>7220</td>
<td>17408</td>
</tr>
<tr>
<td>7210</td>
<td>8704</td>
</tr>
<tr>
<td>7205</td>
<td>4352</td>
</tr>
<tr>
<td>7030</td>
<td>1088</td>
</tr>
<tr>
<td>7024</td>
<td>544</td>
</tr>
<tr>
<td>7010</td>
<td>544</td>
</tr>
<tr>
<td>7008</td>
<td>272</td>
</tr>
<tr>
<td>7005</td>
<td>272</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Switch or stack</th>
<th>Maximum Supported User Tunnels per Switch or Stack</th>
<th>Maximum Supported User Tunnels per port</th>
</tr>
</thead>
<tbody>
<tr>
<td>5400R</td>
<td>1024</td>
<td>32</td>
</tr>
<tr>
<td>3810M</td>
<td>1024</td>
<td>32</td>
</tr>
<tr>
<td>2930M</td>
<td>1024</td>
<td>32</td>
</tr>
<tr>
<td>2930F</td>
<td>1024</td>
<td>32</td>
</tr>
</tbody>
</table>
Functionality

- ArubaOS 8.4 controller supports both UBT 1.0 and 2.0 deployment
- UBT 2.0 is supported on switch release 16.08.xx
- UBT 1.0 release is supported with the following switch releases
  - 16.04.xx to 16.08.xx
- It is mandatory to upgrade VMC Cluster controllers to 8.4 version if switch is upgraded to 16.08.xx
- Standalone/MC/Cluster deployments are supported for both UBT 1.0/2.0
- UBT 1.0 supports both tagged/untagged UBT users
- UBT 2.0 supports only untagged UBT users
- ClearPass Downloadable User Role (DUR) feature is supported for UBT 1.0/2.0
- Role Based VLAN derivation is not supported for UBT 1.0

License requirements

- User Based tunneling 1.0 does not require any additional licenses
- User Based tunneling 2.0 requires the same licenses as Access Points (AP’s)
  - Access Point (AP), Policy Enforcement Firewall (PEF), RFProtect (RFP)
- Mobility Controller (MC) limits are also enforced with UBT 2.0
  - If an MC supports 32 Access Points then that MC will support a total of 32 AP’s and/or Switches, the total number of switches and AP’s cannot exceed the MC supported AP limit in this example 32.
    - 1 AP = 1 AP License
    - 10 AP’s = 10 AP Licenses
    - 1 Switch = 1 AP License
    - 10 Switches = 10 AP Licenses
- 8.4 will require and enforce license requirements regardless if the switch is 1.0 or 2.0
Gracias