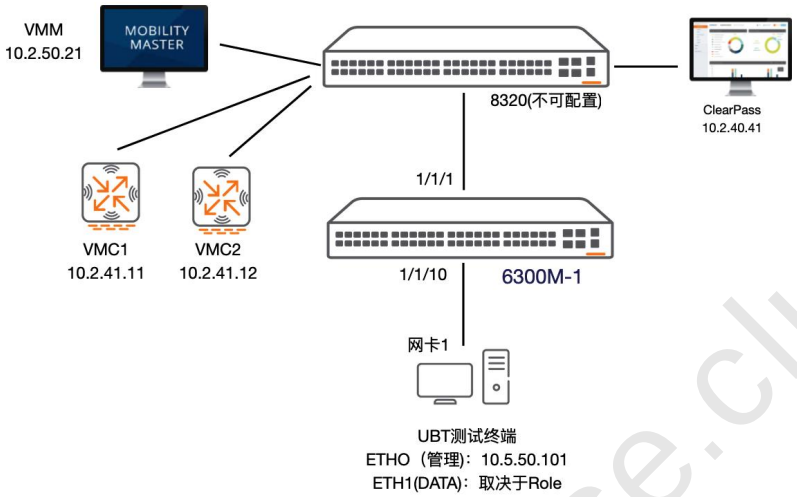
1 实验拓扑



注意事项：

1、本实验内容采用 6300M 物理交换机，非虚机。6300 和 VSF 共用同一套设备，可能有其他配置，注意辨别。

2、点击 6300 图标即可访问设备。

3、6300 采用 Console 连接，可以做初始化操作。

4、此实验不需要自行添加 NODE 设备，添加任何设备不会和 6300 互联互通。

5、6300 只是借用 EVE 平台显示拓扑和链接设备，不要随意删除拓扑内容。

6、6300 不能正常点击访问或者误删设备请点击上方菜单栏“重置 EVE”。

7、需要断电重启设备请联系管理员。

如果设备链接出现 

这个界面，需要先点击上方菜单“EVE PC”，打开 PC 远程桌面，浏览器会缓存登录信息 cookie，然后再点击其他设备就正常出现命令行界面。

2 UBT 配置

2.1 用户需求

要求交换机支持动态隧道技术，根据用户认证的身份信息确定其业务流量是本地转发还是通过隧道到数据中心进行转发。

2.2 实现思路

Aruba CX 6300和6400交换机支持Dynamic Segmentation技术，支持基于用户的动态隧道（User-Based Tunneling）。

UBT可以实现基于用户认证返回的用户角色（LUR），将用户流量通过隧道转发到Aruba无线控制器，由Aruba无线控制器统一实施防火墙策略，也可以跟ClearPass配合实现可下载的用户角色（DUR），由ClearPass统一下发用户角色，无需在交换机本地配置用户角色。

UBT支持两种类型的控制器部署模式：

- ✓ Standalone单台控制器部署方式
- ✓ Cluster多台控制器集群部署方式

支持的交换机型号：

- ✓ 6300F/M
- ✓ 6400

版本要求：

- ✓ 交换机：AOS-CX 10.4或更新
- ✓ 无线控制器：AOS 8.4或更新

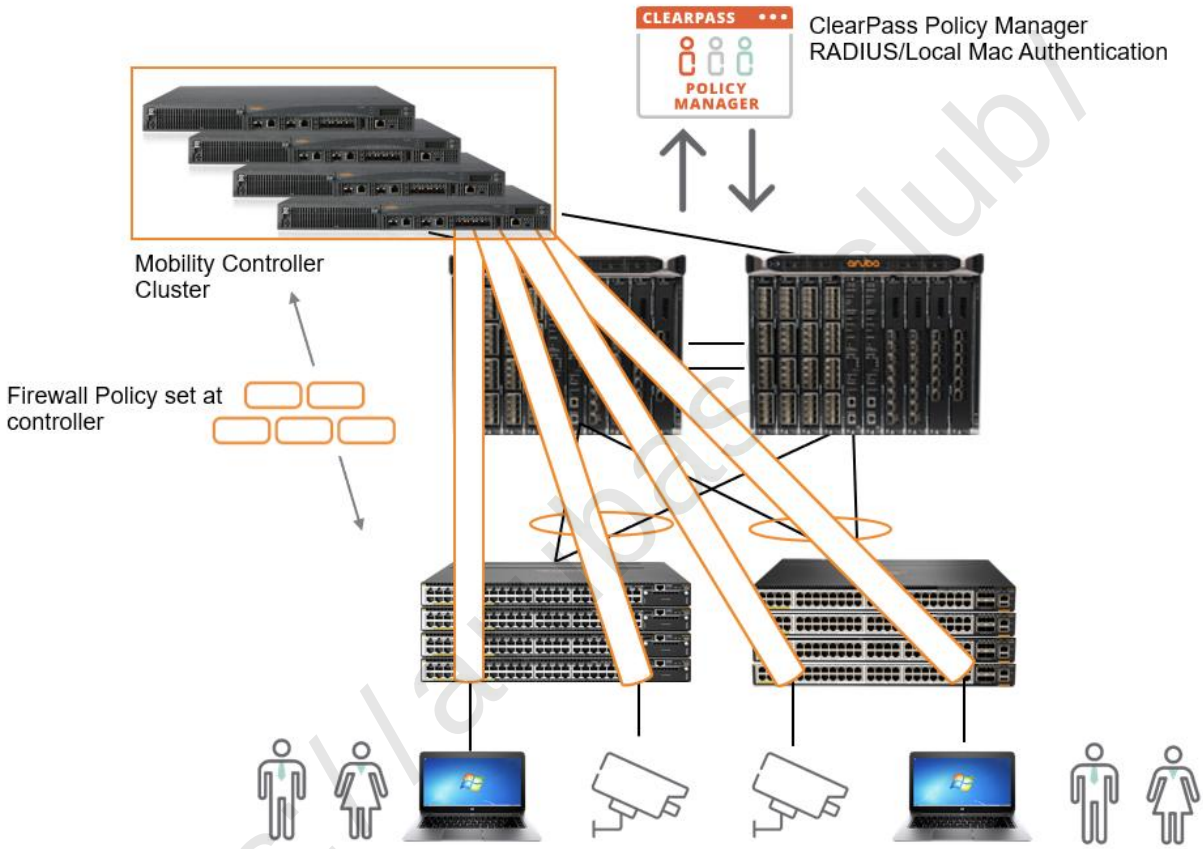
License要求：

- ✓ 只需要在 MM /Standalone Controller 上安装许可
- ✓ 一台/一个堆叠交换机消耗与一个AP相同的License（AP、PEF）

UBT主要由两部分组成：

- ✓ 用户角色：
  - ➢ 交换机User-Role：用户通过交换机端口设置的MAC认证、Dot1X认证等进行身份验证，获取到交换机User-Role（LUR或者DUR）
  - ➢ 移动控制器User-Role（Gateway Role）：交换机本地User-Role下设置的Gateway Role或者通过ClearPass下发的交换机User-Role下带有的Gateway Role
- ✓ 隧道：

- 交换机与移动控制器之间建立GRE隧道
- 用户通过身份认证获取到交换机User-Role，根据此User-Role下是否设置了Gateway Role决定用户流量是否通过隧道转发到移动控制器，未设置Gateway Role用户流量将通过交换机本地转发，设置了Gateway Role用户流量将通过GRE隧道转发到移动控制器，并在移动控制器上给用户发配此Gateway Role，由移动控制器实施基于此Role的状态防火墙策略和AppRF等策略，并在移动控制器上提供此用户的可视化管理。



需要配置的内容如下：

- ✓ LabX-CX-CPPM上配置强制执行策略，给交换机下发LUR和DUR（带gateway role），并创建测试账号：

用户名	密码	说明
wired-user6	123456	dot1x 认证，实现 LUR 下的 ubt
wired-user7	123456	dot1x 认证，实现 DUR 下的 ubt

- ✓ labX-6300-1上配置ubt-client-vlan、ubt zone、LUR（带gateway role）
- ✓ 通过LabX-CX-MM在vmc1/2上的user-role authentication（gateway role）下配置vlan

2.3 达成目标

熟悉基于LUR的UBT配置，以及ClearPass如何给交换机下发LUR；

熟悉基于DUR的UBT配置，以及ClearPass如何给交换机下发DUR。

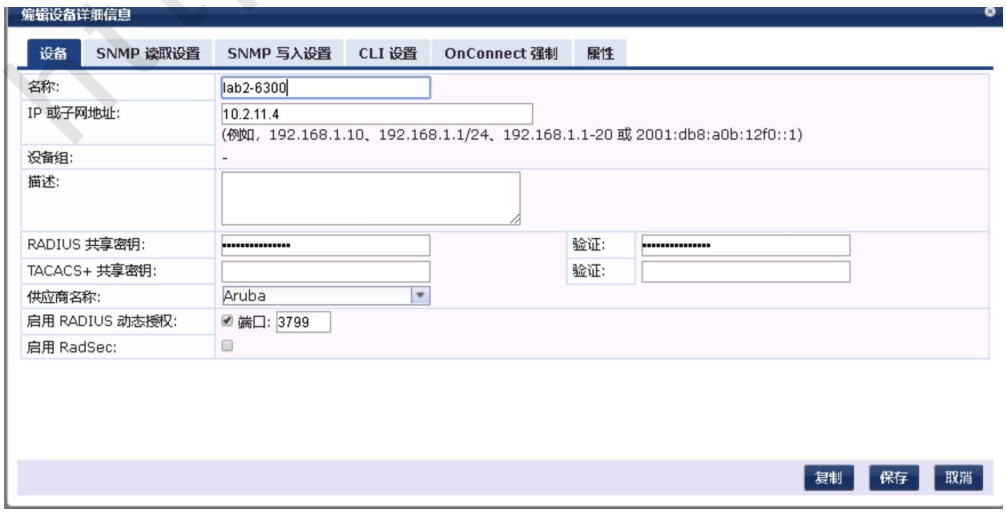
2.4 基于 LUR 的 UBT 配置

2.4.1 ClearPass 配置（GUI）

通过 EVE PC 访问 ClearPass GUI 界面。https://10.x.40.41/

第 1 步:添加网络设备。打开 配置 -> 网络 -> 设备 ，点右上角的 添加设备 链接，创建一个新的网络设备，配置如下：

- 名称：labX-6300
- IP 或子网地址：10.X.11.Y(自行在 6300 设备确认 IP 地址)
- RADIUS 恭喜密钥：aruba123 认证：aruba123
- TACACS+共享密钥：aruba123 认证：aruba123
- 供应商名称：Aruba
- 启用 RADIUS CoA：勾选 RADIUS CoA 端口：3799



第 1 步:打开 配置 -> 身份 -> 本地用户，点右上角的 添加用户 链接，新增一个用户

用户名	密码	说明
wired-user6	123456	dot1x 认证，实现 LUR 下的 ubt

第 2 步:打开 配置 -> 强制执行-> 配置文件，点右上角的 添加强制执行配置文件 链接，创建一个新的强制执行配置文件（为 ubt 用户下发 role）

- 模板：Aruba RADIUS 强制执行
- 名称：send-tunnel-mc-role

点 Next 按钮进入属性配置页面

1. Radius:Aruba Aruba-User-Role = tunnel-mc

第 3 步:打开 配置 -> 强制执行 -> 策略，新增 wired-dot1x-enf，在强制执行策略窗口中点 规则 选项卡，点 “Add Rule”按钮添加一条策略

- 条件：(Tips:Role EQUALS [User Authenticated])

  AND (Authentication:Username CONTAINS user6)

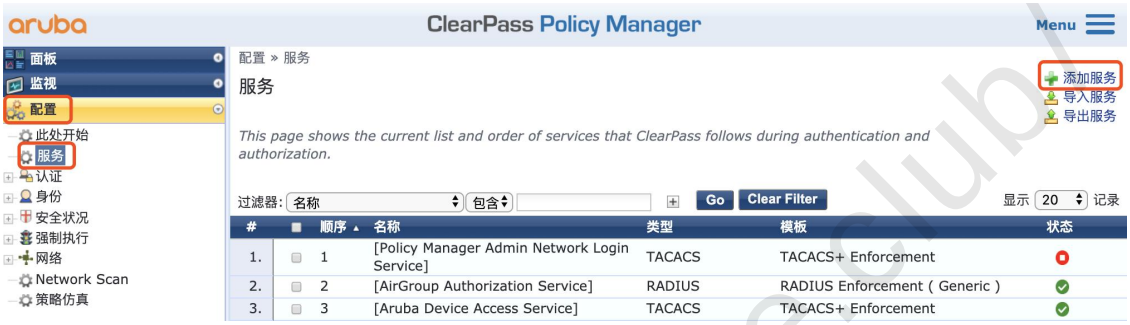
- 配置文件名：send-tunnel-mc-role

点“保存”按钮，再点“保存”按钮保存配置

第 4 步:打开 配置 -> 服务，点右上角的 添加服务 链接，创建一个新的服务

- 类型：802.1X 有线
- 名称：wired-dot1x-auth
- 匹配项：以下所有条件
- 匹配规则：

1. Radius:IETF NAS-Port-Type EQUALS Ethernet (15)
2. Radius:IETF Service-Type BELONGS_TO Login-User (1), Framed-User (2), Authenticate-Only (8)
3. Radius:IETF NAS-IP-AddressEQUALS 10.X.11.4



第 5 步:设置认证方法和认证源

- 认证方法: [EAP PEAP]
  [EAP MSCHAPv2]
- 认证源: [Local User Repository]

第 6 步:角色中的角色映射策略保持默认，即未设置角色映射规则

第 7 步:在强制策略选择之前创建的 wired-dot1x-enf，然后保存

2.4.2 交换机配置（CLI）

第 1 步:在 labX-6300-1 上配置 vlan X11，X 74，X 75，上行接口 1/1/1 放行这些 vlan。接着配置静态路由 ip route 10.X.0.0/16 10.X.11.250，并测试到 LabX-CX-CPPM（10.X.40.41）是否路由可达。交换默认情况下会获取到 Vlan 1（对应 native vlan211）IP 地址：10.X.11.YY。

登录到 labX-6300-1 上:

```
labX-6300-1# configure terminal
LabX-6300-1(config)# interface 1/1/1
LabX-6300-1(config-if)# vlan trunk allowed all
LabX-6300-1(config-if)# exitlabX-6300-1(config)# ip route 10.X.0.0/16 10.X.14.11.250
labX-6300-1(config)# exit
labX-6300-1# ping 10.X.43.41 vrf default
PING 10.X.40.41 (10.X.43.41) 100(128) bytes of data.
108 bytes from 10.X.43.41: icmp_seq=1 ttl=63 time=0.614 ms
```

第 2 步:配置 Radius 服务器

NOTE 可以通过 radius-server host 10.X.43.41 key plaintext aruba123 **vrf <vrf-name>** 指定通过哪个 vrf 发送 radius 请求，未指定时默认表示 vrf default

---

登录到 labX-6300-1 上:

```
labX-6300-1# configure terminal
labX-6300-1(config)# radius-server host 10.X.43.41 key plaintext aruba123
labX-6300-1(config)#ip source-interface radius 10.X.11.4    <-可选配置，先前步骤中应该有设置，如果没有的话，请再次设置好源接口 IP，当设置了 source-interface，交换机将始终使用此 IP 或者接口发起 radius 情况；未设置 source-interface 时，如果 radius server ip 是直连路由，将选择直连接口 ip 作为 source ip 发起 radius 请求，如果非直连路由，交换机将根据路由表选择与下一跳 ip 直连的接口 ip 作为 surce ip 发起 radius 请求
```

第 3 步:配置 Radius Tracking（可选配置）。此功能用于检测 Radius 服务器是否可用，只有 Radius 服务器可用时才向此服务器发起认证。

NOTE

Radius 测试完毕后，请通过 radius-server host 10.X.40.41 tracking disable 命令关闭 tracking，以免 ClearPass 访问跟踪器中全是此用户的 Radius 认证记录。

登录到 labX-6300-1 上:

```
labX-6300-1# configure terminal
labX-6300-1(config)# radius-server tracking interval 300        <-tracking 的时间间隔，60-86400 秒，默认 300 秒
labX-6300-1(config)# radius-server tracking user-name cxadmin password plaintext cxadmin        <-交换机使
labX-6300-1(config)# radius-server host 10.X.40.41 tracking enable
```

第 4 步:配置 Radius 服务器组

NOTE

可以通过 server 10.X.43.41 **vrf <vrf-name>**指定通过哪个 VRF 发送 radius 请求，未指定时表示 VRF default

登录到 labX-6300-1 上:

```
labX-6300-1# configure terminal
labX-6300-1(config)# aaa group server radius clearpass
labX-6300-1(config-sg)# server 10.X.43.41
labX-6300-1(config-sg)# exit
```

第 5 步:配置 Radius fail-through。

NOTE

只有开启了 aaa authentication allow-fail-through 功能，当第一个 Radius 服务器认证失败后才会到第二个 Radius 服务器进行认证，否则认证失败将直接无法接入，默认配置下未开启该功能。

登录到 labX-6300-1 上:

```
labX-6300-1# configure terminal
labX-6300-1(config)# aaa authentication allow-fail-through
```

第 6 步:全局配置下开启 radius 动态授权功能，并配置 radius 动态授权客户端。

NOTE 只有开启了 dyn-authorization 才可以通过 radius 下发用户角色。

只有开启了 dyn-authorization 并配置了 dyn-authorization client 才可以通过 radius 下发 CoA。

登录到 labX-6300-1 上:

```
labX-6300-1# configure terminal
labX-6300-1(config)# radius dyn-authorization enable
labX-6300-1(config)# radius dyn-authorization client 10.X.43.41 secret-key plaintext aruba123
```

第 7 步:开启 Radius Accounting，设置每 10 分钟发送一次 Accounting Interim（计费更新）报文。

登录到 labX-6300-1 上:

```
labX-6300-1# configure terminal
labX-6300-1(config)# aaa accounting port-access start-stop interim 10 group clearpass
```

第 8 步:交换机上配置 ubt-client-vlan，即 tunnel 用户保留 vlan。

登录到 labX-6300-1 上:

```
labX-6300-1# configure terminal
labX-6300-1(config)# vlan 1000
labX-6300-1(config-vlan-1000)# exit
```

```
labX-6300-1(config)# ubt-client-vlan 1000
labX-6300-1(config)# ip source-interface ubt 10.X.11.YY
```

第 9 步:交换机上配置 ubt zone。

在 ubt 实验中，所有 lab 组使用各自的 2 台 VMC（Cluster），vmc1：10.X.41.11，vmc2：10.X.41.12。

NOTE primary-controller ip 和 backup-controller ip 必须为 MD 的物理接口 IP，不能指定 VRRP IP

MD Cluster 情况下，交换机通过 primary-controller ip 即可获取 cluster 信息，这里指定 backup-controller 是为了避免 vmc1 宕机后，新上线的交换机因无法访问 vmc1，而无法获取 cluster 信息

登录到 labX-6300-1 上：

```
labX-6300-1# configure terminal
labX-6300-1(config)# ubt zone test vrf default
labX-6300-1(config-ubt-test)# primary-controller ip 10.X.41.11          <-必须指定物理接口 IP
labX-6300-1(config-ubt-test)# backup-controller ip 10.X.41.12           <-设置 backup-controller ip 可以避免 vmc1 宕机后，新上线的交换机因无法访问 vmc1，而无法获取 cluster 信息
labX-6300-1(config-ubt-test)# enable
labX-6300-1(config-ubt-test)# exit
```

第 10 步:　交换机上配置 LUR（Local User Role），名称为 tunnel-mc。

登录到 labX-6300-1 上：

```
labX-6300-1# configure terminal
labX-6300-1(config)# port-access role tunnel-mc
labX-6300-1(config-pa-role)# gateway-zone zone test gateway-role authenticated
```

```
labX-6300-1(config-pa-role)# exit
```

第 11 步:　通过 Lab Management 页面登录 labX-6300-1 的 SSH 界面。

全局配置下开启 Dot1X 认证，并指定 Dot1X 认证的服务器组。

登录到 labX-6300-1 上:

```
labX-6300-1# configure terminal
labX-6300-1(config)# aaa authentication port-access dot1x authenticator radius server-group clearpass
labX-6300-1(config)# aaa authentication port-access dot1x authenticator enable
```

第 12 步:　交换机 1/1/10 接口开启 Dot1X 认证。

登录到 labX-6300-1 上:

```
labX-6300-1# configure terminal
labX-6300-1(config)# interface 1/1/10
labX-6300-1(config-if)# aaa authentication port-access dot1x authenticator enable
```

2.4.3 控制器配置（CLI）

第 1 步: 针对控制器的配置，在 ubt 配置的 gateway-role（这里为 authenticated）下配置 VLAN　X30，用户通过 tunnel 到 VMC 拿到此 role 会通过此 VLAN 获取 IP。本实验所有 lab 组的 VMC-1 和 VMC-2，学员可以登录到 VMM 上进行管理和查看 VMC 的配置。

登录到 labX-CX-MM 上:

(LabX-CX-MM) [mynode] #show switches （查看下当前 mm 管理域下的控制器状态）

All Switches

IP Address IPv6 Address Name Location Type Model Version Status Configuration State Config Sync Time (sec) Config ID

10.X.50.21 None LabX-CX-MM Building1.floor1 master ArubaMM-VA 8.6.0.2_73853 up UPDATE SUCCESSFUL 0 12

10.X.41.11 None LabX-CX-VMC-1 Building1.floor1 MD ArubaMC-VA 8.6.0.2_73853 up UPDATE SUCCESSFUL 6 12

10.X.41.12 None LabX-CX-VMC-2 Building1.floor1 MD ArubaMC-VA 8.6.0.2_73853 up UPDATE SUCCESSFUL 8 12

Total Switches:3

(LabX-CX-MM) [mynode] #show configuration node-hierarchy （查看下当前无线控制器的配置路径）

Default-node is not configured. Autopark is disabled.

Configuration node hierarchy

Config Node Type Name

/ System

/md System

/md/ubt Group

/md/ubt/00:50:56:ac:60:e1 Device LabX-CX-VMC-2

/md/ubt/00:50:56:ac:bc:49 Device LabX-CX-VMC-1

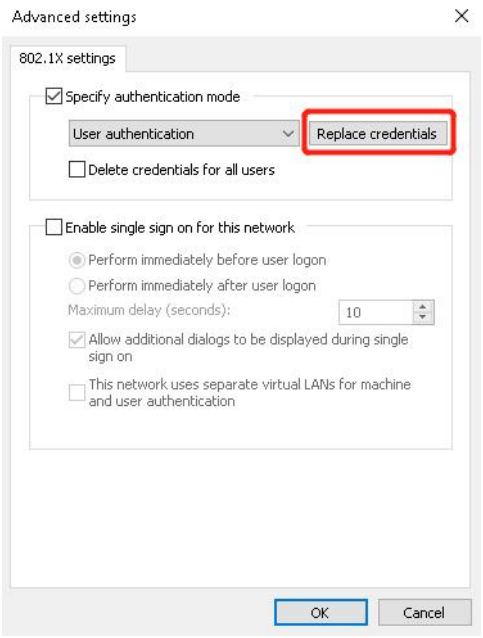
/mm System

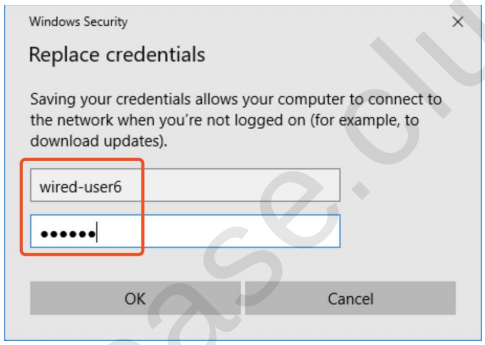
/mm/mynode System

```
(LabX-CX-MM) [mynode] #cd /md/ubt (更改配置路径到 /md/ubt)
(LabX-CX-MM) [ubt] #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(LabX-CX-MM) [ubt] (config) #vlan X30 (创建 UBT 用户 VLAN)
(LabX-CX-MM) ^ [ubt] (config-submode)#!
(LabX-CX-MM) ^ [ubt] (config) #write memory
(LabX-CX-MM) [ubt] (config) #user-role authenticated
(LabX-CX-MM) [ubt] (config-submode)#vlan X30
(LabX-CX-MM) ^[ubt] (config-submode)#!
(LabX-CX-MM) ^[ubt] (config) #write memory

(LabX-CX-VMC-1) [MDC] #show rights authenticated
Valid = 'Yes'
CleanedUp = 'No'
Derived Role = 'authenticated'
 Up BW:No Limit  Down BW:No Limit
 L2TP Pool = default-l2tp-pool
 PPTP Pool = default-pptp-pool
 Number of users referencing it = 0
 Assigned VLAN = X30
 Periodic reauthentication: Disabled
 DPI Classification: Enabled
 Youtube education: Disabled
 Web Content Classification: Enabled
 IP-Classification Enforcement: Enabled
 ACL Number = 85/0
 Openflow: Enabled
 Max Sessions = 65535
```

2.4.4 验证结果

第 1 步:有线测试终端修改 Dot1X 认证用户名密码，wired-user6/123456





第 2 步:关闭并再次开启 1/1/10 接口，以触发有线终端 Dot1X 认证

由于虚机问题，可能关闭接口不能触发，可以禁用网卡再启用。如果提示管理员用户名密码，可以用 lab-admin/aruba123

登录到 labX-6300-1 上:

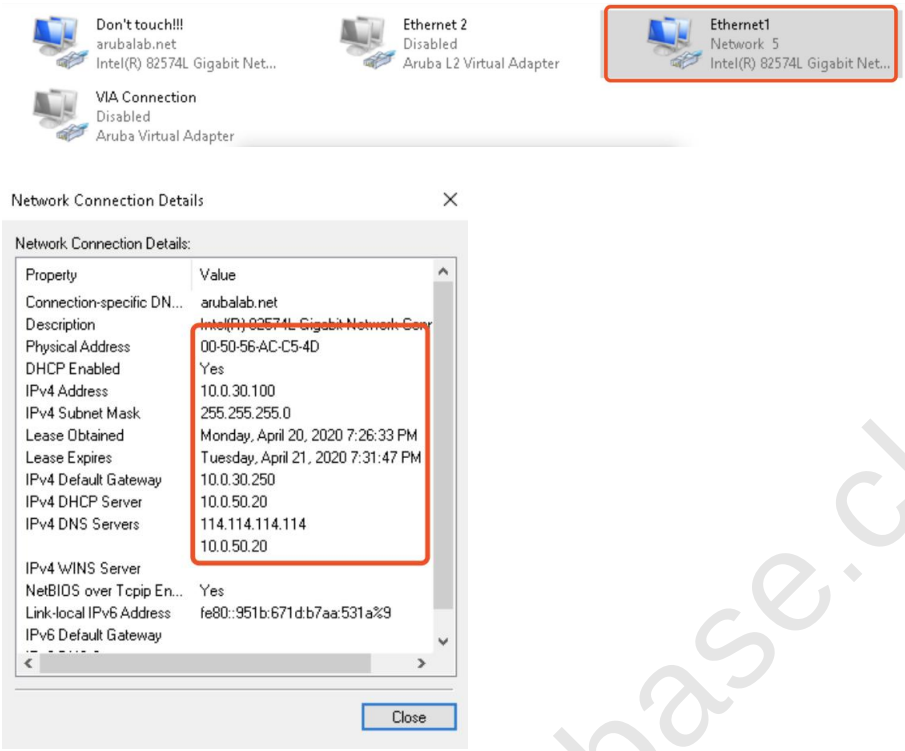
```
labX-6300-1# configure terminal
labX-6300-1(config)# interface 1/1/10
labX-6300-1(config-if)# shutdown
labX-6300-1(config-if)# no shutdown
```

第 3 步:查看有线终端 Ethernet1 网口是否正常获取 IP，可以看到终端获取到 10.X.30.0/24 段的 IP

NOTE 终端通过 tunnel 到 vmc，在 vmc 上获取到 authenticated 角色，该角色下配置了 vlan

---

X30，终端是通过此 vlan 获取的 ip 地址，网关位于核心交换机。



无线控制器上的命令：

第 1 步:学员可以通过各自 lab 环境中的 LabX-CX-MM，查看 ubt 用户状态，由于各 lab 组都采用的 **wired-user6** 以及获取到 10.X.30.0/24 段的 IP，请检查本组 lab 终端获取的 ip，通过此 ip 查询用户，记录该用户当前所处的控制器，vmc1：10.X.41.11，vmc2：10.X.41.12

```
(LabX-CX-MM) [mynode] #show global-user-table list ip 10.X.30.100
Global Users
------------
    IP              MAC               Name          Current switch   Role            Auth
          AP name      Roaming   Essid       Bssid                Phy      Profile
    Type   User Type
```

```
----------  ------------  ------  --------------  ----  ----
     -------  -------  -----  -----  ---  -------  ----  -
--------

10.X.30.100  00:50:56:ac:c5:4d  wired-user6  10.X.41.11  authenticated  Tunneled-User
-802.1X  10.X.14.2  Wired  tunnel 10  88:3a:30:a4:0f:00  1/1/10  default-tunneled-user
N/A  TUNNELED USER
```

第 2 步:通过 mdconnect 进入用户所处的 vmc(这里为 vmc-1),通过 show tunneled-node-mgr tunneled-nodes 命令查看交换机建立 ubt 隧道的 SAC(主用)和 S-SAC(备用)

```
(LabX-CX-MM) [mynode] #cd labx-cx-vmc-1

(LabX-CX-MM) [00:50:56:ac:3d:ca] #mdconnect

(LabX-CX-VMC-1) [MDC] #show tunneled-node-mgr tunneled-nodes


Tunneled Node Table Entries

---------------------------


Flags: A - Active Switch Anchor Controller(A-SAC),
       S - Standby Switch Anchor Controller(S-SAC),
       U - Active User Anchor Controller(A-UAC),
       X - Standby User Anchor Controller(S-UAC),
       C - Convert BC & MC into Unicast,

Name  Tunneled Node Mac  IP Address  Age(d:h:m)  Key  Tunnel Index  SAC IP
Address  S-SAC IP Address  A-Users  S-Users  Flags

----  ----------------  ----------  ----------  ---  ------------  --------------  -
---------------  -------  -------  -----

labX-6300-1  88:3a:30:a4:0f:00  10.X.14.2  00:02:14  deed  tunnel 11  10.X.41.11
    10.X.41.12  1  0  AUC
```

第 3 步:show tunneled-node-mgr tunneled-users 命令查看 tunnel 用户信息，注意核对用户 mac，可以看到用户 vlan 显示为 1000（X30），其中 1000 为 tunnel 用户保留 vlan（前面配置的 ubt-client-vlan），X30 为用户 vlan，即用户获取到 gateway-role（这里为 authenticated）下配置的 vlan，可以看到用户是通过 tunnel 10 转发到控制器，可以通过 show datapath tunnel tunnel-id 10 查看该 tunnel 详细信息

```
(LabX-CX-VMC-1) [MDC] #show tunneled-node-mgr tunneled-users

Tunneled User Table Entries

---------------------------


Flags: U - User Anchor Controller(UAC),

       S - Standby User Anchor Controller(S-UAC),

       T - Tagged VLAN,

       A - Authenticated on Tunneled Node,

       C - Convert BC & MC into Unicast,


User          Tunneled User Mac  Tunneled Node Mac  Vlan      UAC IP Address  Key  T
unnel Index  Flags

----          -----------------  -----------------  ----      --------------  ---  -----------
-  -----

wired-user6  00:50:56:ac:c5:4d  88:3a:30:a4:0f:00  1000(X30)  10.X.41.11       a     tunnel
10      UAC


(LabX-CX-VMC-1) [MDC] #show datapath tunnel tunnel-id 10


Datapath Tunnel Table Entries

----------------------------
```

```
Flags: E - Ether encap,  I - Wi-Fi encap,  R - Wired tunnel,  F - IP fragment OK
       W - WEP,  K - TKIP,  A - AESCCM,  G - AESGCM,  M - no mcast src filtering
       S - Single encrypt,  U - Untagged,  X - Tunneled node,  1(cert-id) - 802.1X Term-PEAP
       2(cert-id) - 802.1X Term-TLS,  T - Trusted,  L - No looping, d - Drop Bcast/Unknown Mcast,
       D - Decrypt tunnel,  a - Reduce ARP packets in the air, e - EAPOL only
       C - Prohibit new calls, P - Permanent, m - Convert multicast, B - Bgw peer uplink tunnel
       n - Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled), s - Split tunnel
       V - enforce user vlan(open clients only), x - Striping IP, z - Datazone
       H - Standby (HA-Lite), u - Cluster UAC tunnel, b - Active AAC tunnel, t - Cluster s-AAC tunnel
       c - IP Compression, g - PAN GlobalProtect Tunnel, w - Tunneled Node Heartbeat
       B - Cluster A-SAC Mcast, G - Cluster S-SAC Mcast, l - Tunneled Node user tunnel
       f - Static GRE Tunnels, k- keepalive enabled, Y - Convert BC/MC to Unicast


Tunnel's: Session Index, Session route/cache Version Number[TSIDX SRTRCV]


 #            Source         Destination     Prt  Type  MTU   VLAN         Acls
    BSSID            Decaps      Encaps       RxBytes        TxBytes     Heartbeats TSIDX
 SRTRCV    ActvAACIP       StripIP          Flags

------  -------------- --------------  ---  ----  ----  ---- ----------------------  ------
----------  ---------- ---------- ------------ ------------ ---------- -------- -------- ---
----------- -------------- ---------------

10       10.X.41.11       10.X.14.2        47    a      1500  0     0    0     0     0     0
88:3a:30:a4:0f:00        6132        6923        3886963        2742102          0 21
  14        0.0.0.0          0.0.0.0          EUPRIY
```

第 4 步:控制器上常用的 debug 命令:show station-table、show user、show tunneled-node-mgr trace-buf count 10

```
(LabX-CX-VMC-1) [MDC] #show station-table

Station Entry
-------------
      MAC               Name          Role             Age(d:h:m)   Auth   AP name     Essid   Ph
y      Remote   Profile                  User Type
------------       ------       ----           ----------  ----  -------    -----  ---     --
----  -------                 ---------
00:50:56:ac:c5:4d  wired-user6  authenticated  00:00:25    Yes   10.X.14.2  -      1/1/10
  No       default-tunneled-user  TUNNELED USER


Station Entries: 1


(LabX-CX-VMC-1) [MDC] #show user
This operation can take a while depending on number of users. Please be patient ....


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.X.30.100  00:50:56:ac:c5:4d  wired-user6  authenticated  00:00:25    Tunneled-User-80
2.1X         10.X.14.2  Tunneled  tunnel  10/88:3a:30:a4:0f:00/1/1/10  default-tunneled-
user  tunnel                          TUNNELED USER


User Entries: 1/1
 Curr/Cum Alloc:1/1 Free:0/0 Dyn:1 AllocErr:0 FreeErr:0


(LabX-CX-VMC-1) [MDC] #show tunneled-node-mgr trace-buf count 10


TNM Trace Buffer
```

```
----------------

Apr 20 17:43:40  sos  SW hb tun created     10.X.14.2  tunnel 11.

Apr 20 17:43:40   *   SW BS Ack not sent    10.X.14.2  bucket map absent.

Apr 20 17:43:40  gsm  Nodelist not sent     10.X.14.2  SW bootstrap ack not yet sent.

Apr 20 17:43:40   *   SW BS Ack not sent    10.X.14.2  bucket map absent.

Apr 20 17:43:40  gsm  Bucketmap not sent    10.X.14.2  SW bootstrap ack not yet sent.

Apr 20 17:43:40  <--  SW Bootstrap Ack      10.X.14.2  SBY=10.X.41.12

Apr 20 19:24:16  -->  User bootstrap req    10.X.14.2  00:50:56:ac:c5:4d rsvd-vid=1 vlan=1
000 key=10 role=authenticated flags=6 mtu=1500 server=0.0.0.0.

Apr 20 19:24:16  sos  User tunnel created  10.X.14.2  00:50:56:ac:c5:4d dormant=0 tunnel
 10.

Apr 20 19:24:16  gsm  Publish tun user      10.X.14.2  00:50:56:ac:c5:4d.

Apr 20 19:24:16  <--  User bootstrap ack    10.X.14.2  00:50:56:ac:c5:4d assigned vlan=X3
0   L2=1  S-UAC=10.X.41.12   idx=36  status=1:Success.
```

第 5 步:检查控制器上 license 的消耗：show license-usage ap

```
(LabX-CX-VMC-1) [MDC] # show license-usage ap

AP Licenses

-----------

Type                        Number

----                        ------

AP Licenses                  10

RF Protect Licenses          10

PEF Licenses                 10

MM Licenses                  10

MC-VA Licenses               10

MC-VA country                cn

Controller License           True

Overall AP License Limit   10
```

```
AP Usage

--------

Type                Count

----                -----

Active CAPs         0

Active RAPs         0

Remote-node APs     0

Active MUX          0

Active PUTN         1

Total APs           1


Remaining AP Capacity

---------------------

Type    Number

----    ------

CAPs    9

RAPs    9
```

交换机上的命令：

第 1 步:在 labX-6300-1 上通过 show aaa authentication port-access interface all client-status 查看终端认证状态及用户 role，通过 show port-access role 查看该 role 的参数

```
登录到 labX-6300-1 上：

labX-6300-1# show aaa authentication port-access interface all client-status

Port Access Client Status Details
```

```
Client 00:50:56:ac:c5:4d, wired-user6
============================
  Session Details
  ---------------
    Port         : 1/1/10
    Session Time : 1500s

  Authentication Details
  ----------------------
    Status             : dot1x Authenticated
    Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted

  Authorization Details
  ---------------------
    Role   : tunnel-mc
    Status : Applied

labX-6300-1# show port-access role
Role Information:

Name   : tunnel-mc
Type   : local
-------------------------------------------
    Reauthentication Period              :
    Authentication Mode                  :
    Session Timeout                      :
    Client Inactivity Timeout            :
    Description                          :
    Gateway Zone                         : test
```

```
UBT Gateway Role                    : authenticated
Access VLAN                         :
Native VLAN                         :
Allowed Trunk VLANs                 :
MTU                                 :
QOS Trust Mode                      :
PoE Priority                        :
Captive Portal Profile              :
Policy                              :
```

第 2 步:交换机上常用的 debug 命令: show ubt、show ubt state、show ubt statistics、show ubt information、show ubt users all、show ubt users count

```
登录到 labX-6300-1 上:
labX-6300-1# show ubt
Zone Name               : test
Primary Controller      : 10.X.41.11
Backup Controller       : 10.X.41.12
SAC HeartBeat Interval : 1
UAC KeepAlive Interval : 60
VLAN Identifier         : 1000
VRF Name                : default
Admin State             : Enabled
PAPI Security Key       : Disabled

labX-6300-1# show ubt state
Local Master Server (LMS) State:
LMS Type        IP Address      State
--------------------------------------------------
```

```
Primary        : 10.X.41.11 ready_for_bootstrap

Secondary    : 10.X.41.12 ready_for_bootstrap


Switch Anchor Controller (SAC) State:


                IP Address       MAC Address            State

-------------------------------------------------------------------

Active         : 10.X.41.11       00:50:56:ac:3d:ca     Registered

Standby      : 10.X.41.12       00:0c:29:a3:e0:b6     Registered


User Anchor Controller(UAC): 10.X.41.11


User                 Port     State                              Bucket ID   Gre Key

-------------------------------------------------------------------------------

00:50:56:ac:c5:4d    1/1/10 registered                  36          10


labX-6300-1# show ubt statistics

UBT Statistics

Control Plane Statistics


  Active    : 10.X.41.11

    Bootstrap Tx     : 1                  Bootstrap Ack Rx    : 1

    Nodelist Rx      : 0                   Nodelist Ack Tx     : 0

    Bucketmap Rx     : 0                 Bucketmap Ack Tx    : 0

    Failover Tx      : 0                    Failover Ack Rx     : 0

    Unbootstrap Tx   : 0                Unbootstrap Ack Rx : 0

    Heartbeat Tx     : 10720           Heartbeat Ack Rx    : 10720


  Standby   : 10.X.41.12

    Bootstrap Tx     : 1                  Bootstrap Ack Rx    : 1
```

```
    Nodelist Rx       : 0                 Nodelist Ack Tx     : 0
    Bucketmap Rx      : 0                 Bucketmap Ack Tx    : 0
    Failover Tx       : 0                 Failover Ack Rx     : 0
    Unbootstrap Tx    : 0                 Unbootstrap Ack Rx : 0
    Heartbeat Tx      : 10720             Heartbeat Ack Rx    : 10720

  UAC    : 10.X.41.11
    Bootstrap Tx      : 2                 Bootstrap Ack Rx    : 2
    Unbootstrap Tx    : 1                 Unbootstrap Ack Rx : 1
    Keepalive Tx      : 0                 Keepalive Ack Rx    : 0

  UAC    : 10.X.41.12
    Bootstrap Tx      : 0                 Bootstrap Ack Rx    : 0
    Unbootstrap Tx    : 0                 Unbootstrap Ack Rx : 0
    Keepalive Tx      : 0                 Keepalive Ack Rx    : 0

  Data Plane Statistics
  UAC              Packets Tx    Packets Rx
  ------------------------------------

 10.0.50.67      :    0                    0

 10.X.41.11      :    1256                 1500

 10.X.41.12      :    0                    0

labX-6300-1# show ubt information
SAC Information :
  Active              : 10.X.41.11
  Standby             : 10.X.41.12
```

```
Node List Information :

  Cluster Name    : selab-ubt


  Node List       :

  ---------------

    10.X.41.11

    10.X.41.12


Bucket Map Information :


Bucket Map Active    : [0...255]


Bucket ID   A-UAC              S-UAC                  Connectivity

-----------------------------------------------------------

0              10.X.41.11        10.X.41.12           L2

......

255          10.X.41.12        10.X.41.11           L2


labX-6300-1# show ubt users all

Displaying All UBT Users for Zone: test

Downloaded user roles are preceded by *

Port         Mac-Address          Tunnel Status       Secondary-UserRole    Failure Reason

-------------------------------------------------------------------------------------------

1/1/10       00:50:56:ac:c5:4d   activated            authenticated             ---/---


labX-6300-1# show ubt users count

Total Number of Users using ubt Zone : test is 1
```

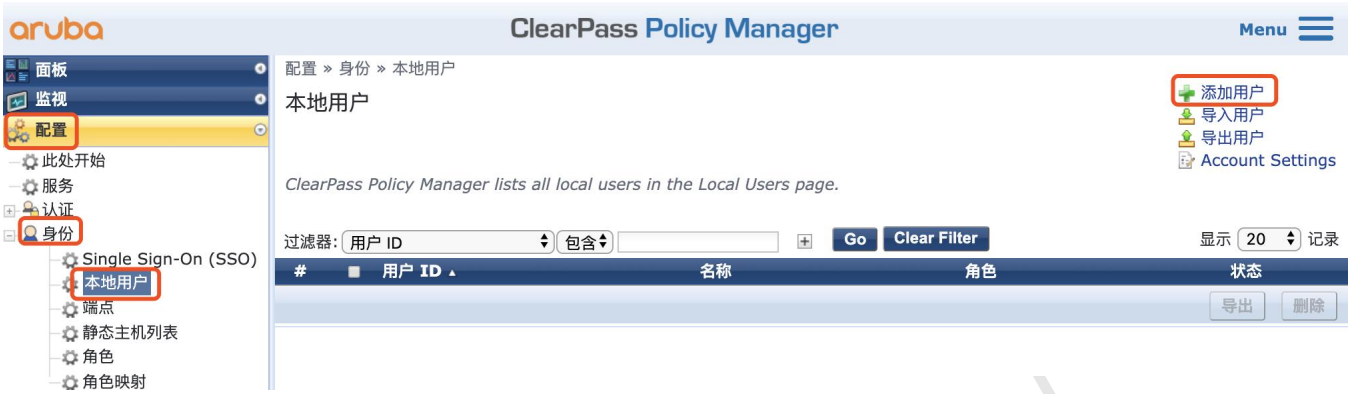
第 3 步:在 LabX-CX-CPPM 上查看访问跟踪器，可以查看到终端 dot1x 认证成功的记录，Login Status 为 ACCEPT，点击该认证记录进入请求详细信息界面，打开输出选项卡，强制执行配置文件为 send-tunnel-mc-role，下发了 Aruba-User-Role 属性。

2.5 基于 DUR 的 UBT 配置

2.5.1 ClearPass 配置(GUI)

第 1 步:打开 配置 -> 身份 -> 本地用户，点右上角的 添加用户 链接，新增一个用户

用户名	密码	说明
wired-user7	123456	dot1x 认证，实现 DUR 下的 ubt



#	用户 ID	名称	角色	状态
1.	wired-user1	wired-user1	[Other]	Enabled
2.	wired-user2	wired-user2	[Other]	Enabled
3.	wired-user3	wired-user3	[Other]	Enabled
4.	wired-user4	wired-user4	[Other]	Enabled
5.	wired-user5	wired-user5	[Other]	Enabled
6.	wired-user6	wired-user6	[Other]	Enabled
7.	wired-user7	wired-user7	[Other]	Enabled

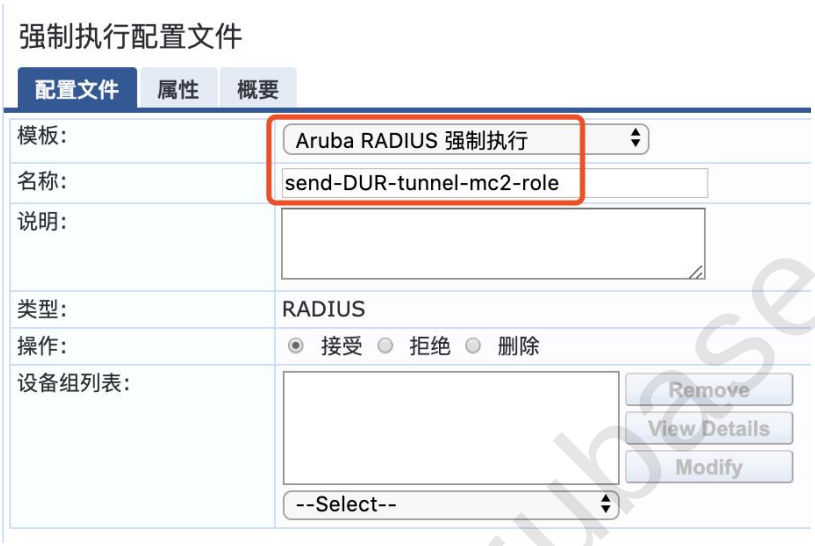
第 2 步:打开 配置 -> 强制执行-> 配置文件，点右上角的 添加强制执行配置文件 链接，创建一个新的强制执行配置文件（为 ubt 用户下发 DUR）

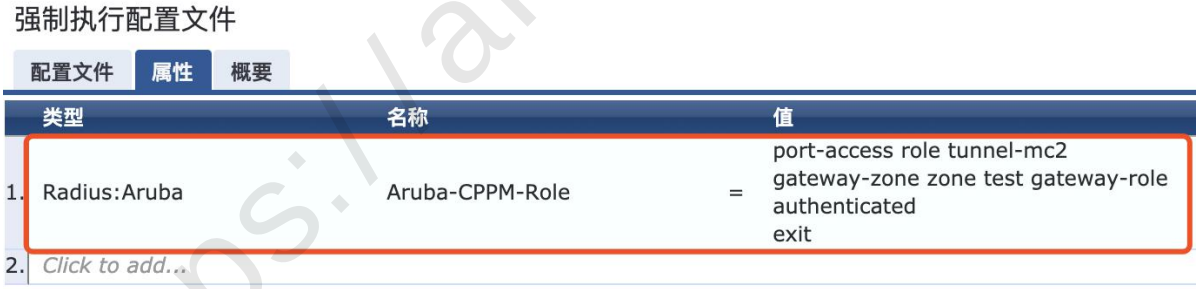
- 模板：Aruba RADIUS 强制执行
- 名称：send-DUR-tunnel-mc2-role

点 Next 按钮进入属性配置页面

1. Radius:Aruba Aruba-CPPM-Role = <下面命令>

```
port-access role tunnel-mc2
gateway-zone zone test gateway-role authenticated
exit
```





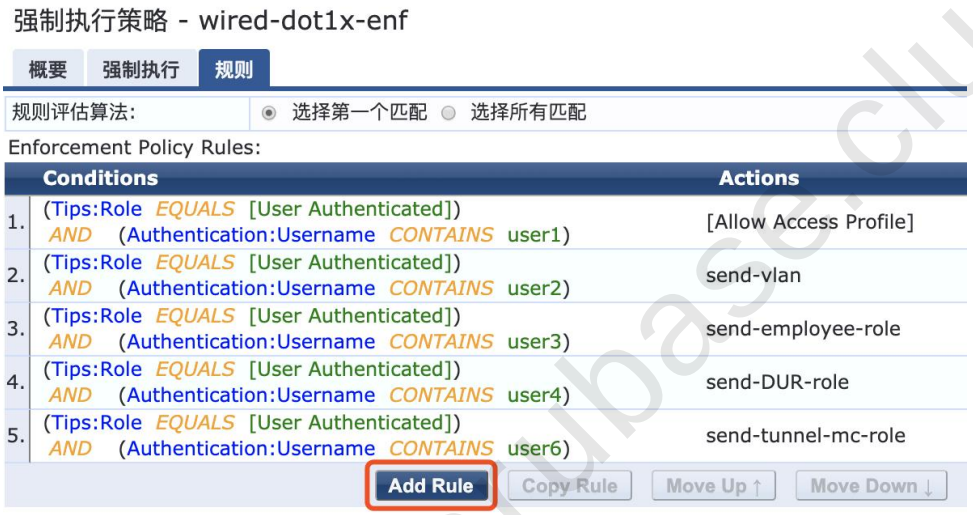
第 3 步:打开 配置 -> 强制执行 -> 策略，在右边的窗口中点击 wired-dot1x-enf,在强制执行策略窗口中点 规则 选项卡,点“Add Rule”按钮添加一条策略

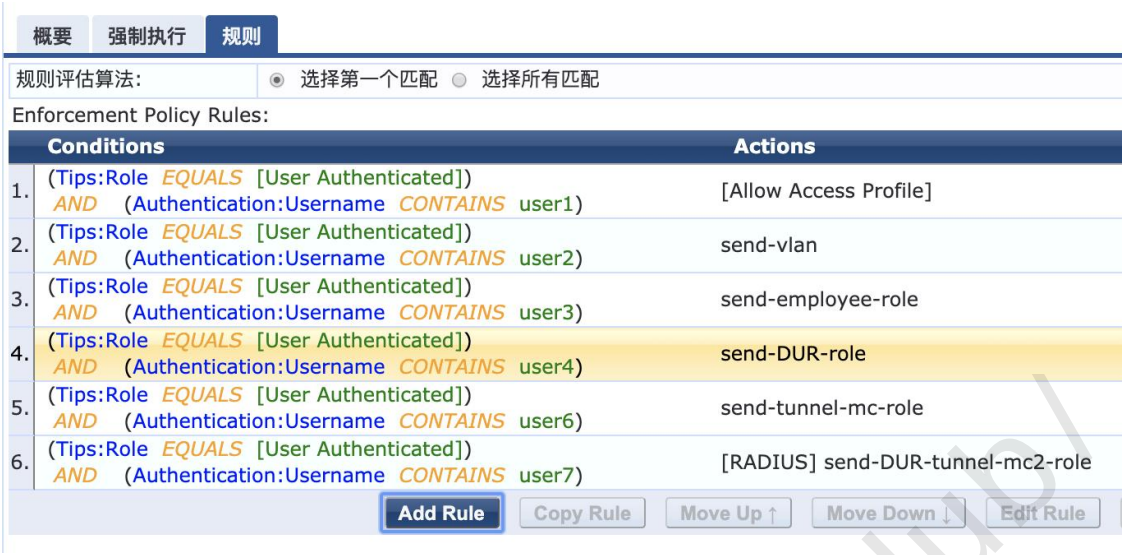
- 条件：(Tips:Role EQUALS [User Authenticated])

  AND (Authentication:Username CONTAINS user7)

- 配置文件名：send-DUR-tunnel-mc2-role

点“保存”按钮，再点“保存”按钮保存配置





2.5.2 交换机配置（CLI）

本章节规划用户采用 wired-user7/123456 完成 Dot1X 认证后，ClearPass 下发 DUR（tunnel-mc2）到交换机，并下发此 role 的 gateway-role 为 authenticated。

基于 DUR 的 UBT，交换机上不需要配置本地的 role（即 port-access role tunnel-mc2），由 ClearPass 下发此 role 及 role 下的配置。

NOTE

要实现 DUR，交换机上需要安装 ClearPass HTTPS 服务器证书的根证书（Root CA），ClearPass 上需要创建具有下载 user role 权限的账户，这部分的内容在上一章的“通过 Dot1X 认证实现 DUR”中已完成，这里不再介绍。

第 1 步：交换机上配置 ubt-client-vlan，即 tunnel 用户保留 vlan 1000，这部分配置在“基于 LUR 的 UBT 配置”章节中已完成，此处不需要再配置。

登录到 labX-6300-1 上：

```
labX-6300-1# configure terminal
labX-6300-1(config)# vlan 1000
```

```
labX-6300-1(config-vlan-1000)# exit
labX-6300-1(config)# ubt-client-vlan 1000
labX-6300-1(config)# ip source-interface ubt 10.X.11.4
```

第 2 步:交换机上配置 ubt zone，这部分配置在“基于 LUR 的 UBT 配置”章节中已完成，此处不需要再配置。

```
登录到 labX-6300-1 上:
labX-6300-1# configure terminal
labX-6300-1(config)# ubt zone test vrf default
labX-6300-1(config-ubt-test)# primary-controller ip 10.X.41.11
labX-6300-1(config-ubt-test)# backup-controller ip 10.X.41.12
labX-6300-1(config-ubt-test)# enable
labX-6300-1(config-ubt-test)# exit
```

第 3 步:交换机 1/1/10 接口开启 Dot1X 认证，这部分配置在“基于 LUR 的 UBT 配置”章节中已完成，此处不需要再配置。

```
登录到 labX-6300-1 上:
labX-6300-1# configure terminal
labX-6300-1(config)# interface 1/1/10
labX-6300-1(config-if)# aaa authentication port-access dot1x authenticator enable
```

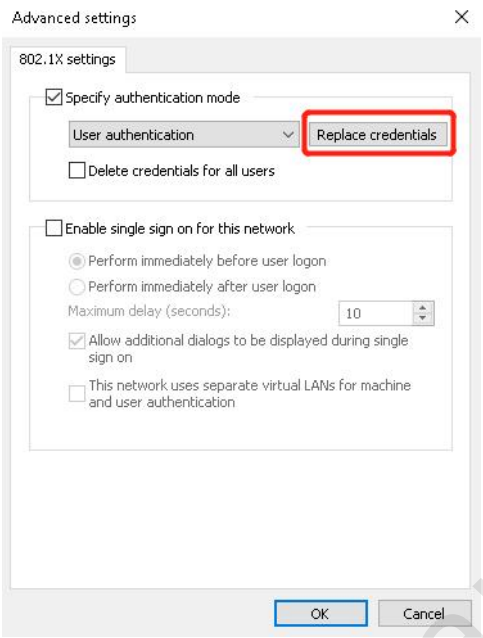

2.5.3 控制器配置（CLI）

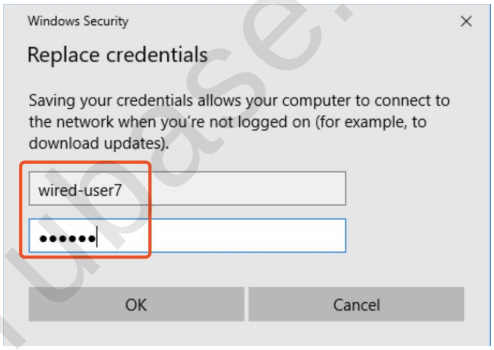
第 1 步:针对控制器的配置，在 ubt 配置的 gateway-role（这里为 authenticated）下配置 VLAN　X30，用户通过 tunnel 到 VMC 拿到此 role 会通过此 VLAN 获取 IP。本实验所有 lab 组的 VMC-1 和 VMC-2，

学员可以登录到 VMM 上进行管理和查看 VMC 的配置。（该部分的配置已经在 5.4.3 章节中介绍）

2.5.4 验证结果

第 1 步:有线测试终端修改 Dot1X 认证用户名密码，wired-user7/123456





第 2 步:关闭并再次开启 1/1/10 接口，以触发有线终端 Dot1X 认证

登录到 labX-6300-1 上:

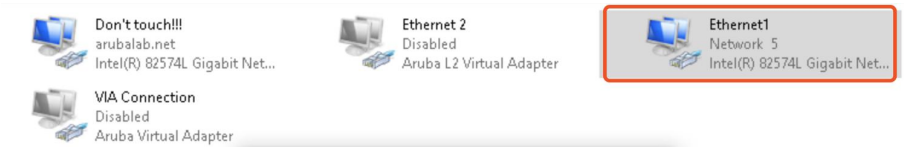
```
labX-6300-1# configure terminal
labX-6300-1(config)# interface 1/1/10
labX-6300-1(config-if)# shutdown
labX-6300-1(config-if)# no shutdown
```

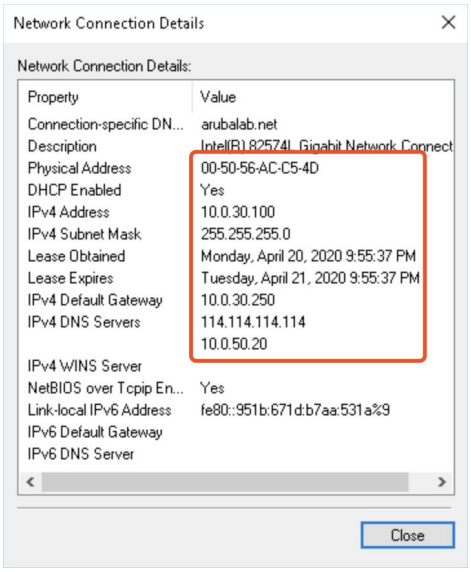
第 3 步:查看有线终端 Ethernet1 网口是否正常获取 IP，可以看到终端获取到 10.X.30.0/24 段的 IP

NOTE 终端通过 tunnel 到 vmc，在 vmc 上获取到 authenticated 角色，该角色下配置了 vlan

---

X30，终端是通过此 vlan 获取的 ip 地址，网关位于核心交换机。





无线控制器上的命令：

第 1 步:学员可以通过各自 lab 环境中的 LabX-CX-MM，查看 ubt 用户状态，由于各 lab 组都采用的 **wired-user7** 以及获取到 10.0.30.0/24 段的 IP，请检查本组 labX 终端获取的 IP，通过此 IP 查询用户，记录该用户当前所处的控制器，VMC-1：10.X.41.11，VMC-2：10.X.41.12

```
(LabX-CX-MM) [mynode] #show global-user-table list ip 10.X.30.100

Global Users

------------

    IP              MAC               Name          Current switch   Role              Auth
            AP name      Roaming   Essid       Bssid                Phy      Profile
    Type   User Type
```

```
----------  ------------  ------  --------------  ----  ----
     -------  -------  -----  -----  ---  -------  ----  -
--------

10.X.30.100  00:50:56:ac:c5:4d  wired-user7  10.X.41.11  authenticated  Tunneled-User
-802.1X  10.X.14.2  Wired  tunnel 10  88:3a:30:a4:0f:00  1/1/10  default-tunneled-user
N/A  TUNNELED USER
```

第 2 步:通过 mdconnect 进入用户所处的 VMC(这里为 VMC-1),通过 show tunneled-node-mgr tunneled-nodes 命令查看交换机建立 ubt 隧道的 SAC（主用）和 S-SAC（备用）

```
(LabX-CX-MM) [mynode] # cd labx-cx-vmc-1

(LabX-CX-MM) [00:50:56:ac:3d:ca] #mdconnect

(LabX-CX-VMC-1) [MDC] #show tunneled-node-mgr tunneled-nodes


Tunneled Node Table Entries

---------------------------


Flags: A - Active Switch Anchor Controller(A-SAC),
       S - Standby Switch Anchor Controller(S-SAC),
       U - Active User Anchor Controller(A-UAC),
       X - Standby User Anchor Controller(S-UAC),
       C - Convert BC & MC into Unicast,

Name  Tunneled Node Mac  IP Address  Age(d:h:m)  Key  Tunnel Index  SAC IP
Address  S-SAC IP Address  A-Users  S-Users  Flags

----  ----------------  ----------  ----------  ---  ------------  --------------  -
---------------  -------  -------  -----

labX-6300-1  88:3a:30:a4:0f:00  10.X.14.2  00:04:13  deed  tunnel 11  10.X.41.11
    10.X.41.12  1  0  AUC
```

第 3 步:show tunneled-node-mgr tunneled-users 命令查看 tunnel 用户信息，注意核对用户 mac，可以看到用户 vlan 显示为 1000（X30），其中 1000 为 tunnel 用户保留 vlan（前面配置的 ubt-client-vlan），X30 为用户 vlan，即用户获取到 gateway-role（这里为 authenticated）下配置的 vlan，可以看到用户是通过 tunnel 10 转发到控制器，可以通过 show datapath tunnel tunnel-id 10 查看该 tunnel 详细信息

```
(LabX-CX-VMC-1) [MDC] #show tunneled-node-mgr tunneled-users

Tunneled User Table Entries

---------------------------

Flags: U - User Anchor Controller(UAC),

       S - Standby User Anchor Controller(S-UAC),

       T - Tagged VLAN,

       A - Authenticated on Tunneled Node,

       C - Convert BC & MC into Unicast,



User          Tunneled User Mac  Tunneled Node Mac  Vlan      UAC IP Address  Key  T
unnel Index  Flags

----          -----------------  -----------------  ----      --------------  ---  -----------
-  -----

wired-user7  00:50:56:ac:c5:4d  88:3a:30:a4:0f:00  1000(X30)  10.X.41.11       a     tunnel
10      UAC


(LabX-CX-VMC-1) [MDC] #show datapath tunnel tunnel-id 10


Datapath Tunnel Table Entries

----------------------------

Flags: E - Ether encap,  I - Wi-Fi encap,  R - Wired tunnel,  F - IP fragment OK
```

```
        W - WEP,  K - TKIP,  A - AESCCM,  G - AESGCM,  M - no mcast src filtering

        S - Single encrypt,  U - Untagged,  X - Tunneled node,  1(cert-id) - 802.1X Term-
PEAP

        2(cert-id) - 802.1X Term-TLS,  T - Trusted,  L - No looping, d - Drop Bcast/Unkno
wn Mcast,

        D - Decrypt tunnel,  a - Reduce ARP packets in the air, e - EAPOL only

        C - Prohibit new calls, P - Permanent, m - Convert multicast, B - Bgw peer uplink t
unnel

        n - Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled), s - Split tunnel

        V - enforce user vlan(open clients only), x - Striping IP, z - Datazone

        H - Standby (HA-Lite), u - Cluster UAC tunnel, b - Active AAC tunnel, t - Cluster s-
AAC tunnel

        c - IP Compression, g - PAN GlobalProtect Tunnel, w - Tunneled Node Heartbeat

        B - Cluster A-SAC Mcast, G - Cluster S-SAC Mcast, l - Tunneled Node user tunnel

        f - Static GRE Tunnels, k- keepalive enabled, Y - Convert BC/MC to Unicast


Tunnel's: Session Index, Session route/cache Version Number[TSIDX SRTRCV]


 #            Source         Destination    Prt  Type   MTU    VLAN         Acls
    BSSID             Decaps      Encaps       RxBytes        TxBytes     Heartbeats TSIDX
 SRTRCV    ActvAACIP        StripIP          Flags

------  --------------  --------------  ---  ----  ----  ---- ----------------------  ------
----------- ---------- ---------- ------------ ------------ ---------- -------- -------- ---
------------ --------------- ---------------

10       10.X.41.11       10.X.14.2        47    a      1500   0     0    0     0     0     0
88:3a:30:a4:0f:00          32          81          5055          7119          0 21
14       0.0.0.0          0.0.0.0          EUPRIY
```

第 4 步:控制器上常用的 debug 命令:show station-table、show user、show tunneled-node-mgr trace-buf count 10

```
(LabX-CX-VMC-1) [MDC] #show station-table

Station Entry
```

```
-------------

      MAC               Name          Role              Age(d:h:m)   Auth   AP name     Essid   Ph
y      Remote   Profile                  User Type

------------       ------       ----           ----------  ----  -------    -----  ---     --
----  -------                 ---------

00:50:56:ac:c5:4d  wired-user7  authenticated  00:00:04    Yes   10.X.14.2  -      1/1/10
  No        default-tunneled-user   TUNNELED USER

Station Entries: 1


(LabX-CX-VMC-1) [MDC] #show user

This operation can take a while depending on number of users. Please be patient ....


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.X.30.100   00:50:56:ac:c5:4d  wired-user7  authenticated  00:00:05    Tunneled-User-80
2.1X              10.X.14.2   Tunneled   tunnel 10/88:3a:30:a4:0f:00/1/1/10   default-tunneled-
user   tunnel                        TUNNELED USER


User Entries: 1/1

 Curr/Cum Alloc:1/1  Free:0/0  Dyn:1  AllocErr:0 FreeErr:0


(LabX-CX-VMC-1) [MDC] #show tunneled-node-mgr trace-buf count 10


TNM Trace Buffer

---------------

Apr 20 21:52:19   gsm   Publish tun user       10.X.14.2   00:50:56:ac:c5:4d.
```

```
Apr 20 21:52:19 <-- User bootstrap ack 10.X.14.2 00:50:56:ac:c5:4d assignedvlan=30
 L2=1 S-UAC=10.X.41.12 idx=36 status=1:Success.

Apr 20 21:54:46 --> User Unbootstrap Req 10.X.14.2 00:50:56:ac:c5:4d reason=5, key=
10.

Apr 20 21:54:46 sos User tunnel removed 10.X.14.2 00:50:56:ac:c5:4d tunnel 10.

Apr 20 21:54:46 gsm Delete tun user 10.X.14.2 00:50:56:ac:c5:4d.

Apr 20 21:54:46 <-- User Unbootstrap Ack 10.X.14.2 00:50:56:ac:c5:4d key=10 status=
1:Success.

Apr 20 21:54:52 --> User bootstrap req 10.X.14.2 00:50:56:ac:c5:4d rsvd-vid=1 vlan=
1000 key=10 role=authenticated flags=6 mtu=1500 server=0.0.0.0.

Apr 20 21:54:52 sos User tunnel created 10.X.14.2 00:50:56:ac:c5:4d dormant=0 tunn
el 10.

Apr 20 21:54:52 gsm Publish tun user 10.X.14.2 00:50:56:ac:c5:4d.

Apr 20 21:54:52 <-- User bootstrap ack 10.X.14.2 00:50:56:ac:c5:4d assignedvlan=30
 L2=1 S-UAC=10.X.41.12 idx=36 status=1:Success.
```

第 5 步:检查控制器上 license 的消耗：show license-usage ap

```
(LabX-CX-VMC-1) [MDC] # show license-usage ap

AP Licenses

-----------

Type                        Number

----                        ------

AP Licenses                  10

RF Protect Licenses          10

PEF Licenses                 10

MM Licenses                  10

MC-VA Licenses               10

MC-VA country                cn

Controller License           True

Overall AP License Limit   10
```

```
AP Usage

--------

Type                Count

----                -----

Active CAPs         0

Active RAPs         0

Remote-node APs     0

Active MUX          0

Active PUTN         1

Total APs           1


Remaining AP Capacity

---------------------

Type    Number

----    ------

CAPs    9

RAPs    9
```

交换机上的命令：

第 1 步:在 labX-6300-1 上通过 show aaa authentication port-access interface all client-status 查看终端认证状态及用户 role，通过 show port-access role 查看该 role 的参数

```
登录到 labX-6300-1 上:

labX-6300-1# show aaa authentication port-access interface all client-status

Port Access Client Status Details

Client 00:50:56:ac:c5:4d, wired-user7

============================

  Session Details
```

```
---------------

  Port           : 1/1/10

  Session Time : 105s


Authentication Details

----------------------

  Status             : dot1x Authenticated

  Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted


Authorization Details

----------------------

  Role    : send_DUR_tunnel_mc2_role-3012-1

  Status : Applied


labX-6300-1# show port-access role

Role Information:


Name   : send_DUR_tunnel_mc2_role-3012-1

Type   : clearpass

Status: Completed

-------------------------------------------

  Reauthentication Period              :

  Authentication Mode                  :

  Session Timeout                      :

  Client Inactivity Timeout            :

  Description                          :

  Gateway Zone                         : test

  UBT Gateway Role                     : authenticated

  Access VLAN                          :

  Native VLAN                          :
```

```
Allowed Trunk VLANs                    :
MTU                                    :
QOS Trust Mode                         :
PoE Priority                           :
Captive Portal Profile                 :
Policy                                 :
```

第 2 步:交换机上常用的 debug 命令: show ubt、show ubt state、show ubt statistics、show ubt information、show ubt users all、show ubt users count

登录到 labX-6300-1 上:

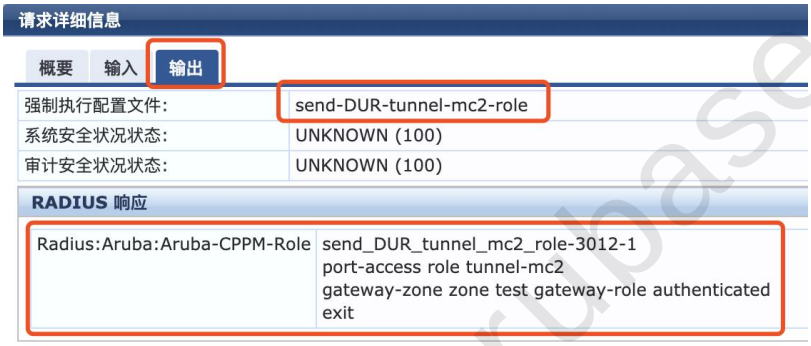
```
labX-6300-1# show ubt
Zone Name                  : test
Primary Controller         : 10.X.41.11
Backup Controller          : 10.X.41.12
SAC HeartBeat Interval : 1
UAC KeepAlive Interval : 60
VLAN Identifier            : 1000
VRF Name                   : default
Admin State                : Enabled
PAPI Security Key          : Disabled

labX-6300-1# show ubt state
Local Master Server (LMS) State:
LMS Type        IP Address      State
--------------------------------------------------
Primary      : 10.X.41.11       ready_for_bootstrap
Secondary    : 10.X.41.12       ready_for_bootstrap
```

```
Switch Anchor Controller (SAC) State:

                IP Address        MAC Address            State
-----------------------------------------------------------------------
Active        : 10.X.41.11        00:50:56:ac:3d:ca      Registered
Standby       : 10.X.41.12        00:0c:29:a3:e0:b6      Registered

User Anchor Controller(UAC): 10.X.41.11

User                 Port     State                          Bucket ID   Gre Key
-------------------------------------------------------------------------------
00:50:56:ac:c5:4d    1/1/10 registered                       36          10

labX-6300-1# show ubt statistics
UBT Statistics
Control Plane Statistics

  Active    : 10.X.41.11
    Bootstrap Tx     : 1                 Bootstrap Ack Rx    : 1
    Nodelist Rx      : 0                 Nodelist Ack Tx     : 0
    Bucketmap Rx     : 0                   Bucketmap Ack Tx    : 0
    Failover Tx      : 0                 Failover Ack Rx     : 0
    Unbootstrap Tx   : 0                   Unbootstrap Ack Rx : 0
    Heartbeat Tx     : 15655               Heartbeat Ack Rx    : 15655

  Standby   : 10.X.41.12
    Bootstrap Tx     : 1                 Bootstrap Ack Rx    : 1
    Nodelist Rx      : 0                 Nodelist Ack Tx     : 0
    Bucketmap Rx     : 0                   Bucketmap Ack Tx    : 0
    Failover Tx      : 0                 Failover Ack Rx     : 0
```

```
    Unbootstrap Tx  : 0                  Unbootstrap Ack Rx : 0
    Heartbeat Tx    : 15655              Heartbeat Ack Rx   : 15655


  UAC   : 10.X.41.11
    Bootstrap Tx    : 7                  Bootstrap Ack Rx   : 7
    Unbootstrap Tx  : 6                  Unbootstrap Ack Rx : 6
    Keepalive Tx    : 0                  Keepalive Ack Rx   : 0

  UAC   : 10.X.41.12
    Bootstrap Tx    : 0                  Bootstrap Ack Rx   : 0
    Unbootstrap Tx  : 0                  Unbootstrap Ack Rx : 0
    Keepalive Tx    : 0                  Keepalive Ack Rx   : 0

  Data Plane Statistics
  UAC              Packets Tx    Packets Rx
  ------------------------------------

 10.0.50.67       :   0                 0

 10.X.41.11       :   0                 0

 10.X.41.12       :   0                 0

labX-6300-1# show ubt information

SAC Information :

  Active          : 10.X.41.11
  Standby         : 10.X.41.12
```

```
Node List Information :

  Cluster Name    : selab-ubt

  Node List       :
  ---------------
    10.X.41.11
    10.X.41.12

Bucket Map Information :

Bucket Map Active    : [0...255]

Bucket ID   A-UAC              S-UAC              Connectivity
-----------------------------------------------------------
0           10.X.41.11         10.X.41.12         L2
......
255         10.X.41.12         10.X.41.11         L2

labX-6300-1# show ubt users all
Displaying All UBT Users for Zone: test
Downloaded user roles are preceded by *
Port        Mac-Address          Tunnel Status       Secondary-UserRole    Failure Reason
-------------------------------------------------------------------------------------------
1/1/10      00:50:56:ac:c5:4d  activated           authenticated           ---/---


labX-6300-1# show ubt users count
Total Number of Users using ubt Zone : test is 1
```

第 3 步:在 LabX-CX-CPPM 上查看访问跟踪器，可以查看到终端 dot1x 认证成功的记录，Login Status 为 ACCEPT，点击该认证记录进入请求详细信息界面，打开输出选项卡，强制执行配置文件为 send-DUR-tunnel-mc2-role，下发了 Aruba-CPPM-Role 属性。



2.6 配置备份

登录到 labX-6300-1 上:

```
labX-6300-1# write memory

Configuration changes will take time to process, please be patient.

labX-6300-1# copy running-config checkpoint task3-done-labX          (配置保存到交换机本地 flash 上)

Configuration changes will take time to process, please be patient.


labX-6300-1# show checkpoint list

CPC20200408031408
```

```
CPC20200408032505

task2-done-labX

task3-done-labX

startup-config

CPC20200408035054

AUTO20200408035118

CPC20200408100133

ZERO-labX
```

依次针对其他交换机（labX-8400-1、labX-8400-2 和 labX-8400-core）设备重复上面的配置备份操作。