Per Port Tunneled Node

Contents

Purpose

The purpose of this document is to provide configuration and troubleshooting information on Per Port Tunneled Node (sic). There are a number of very good references but they tend to include more complex interactions with AAA integration and policy enforcement through Clearpass. This document focuses on the most basic configuration on the switch and controller. Hopefully this provides clarity on the underlying technology and how to troubleshoot it.

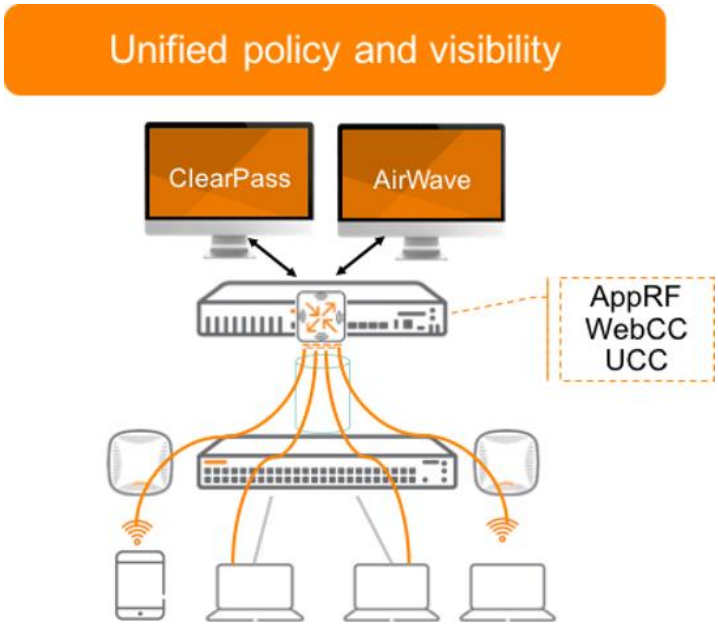

Figure 1: PPTN can provide centralised policy enforcement and Visibility

What is Per Port Tunneled Node (PPTN) ?

Per Port Tunneled node feature encapsulates incoming packets from end-hosts in GRE and forwards them to a Mobility Controller for additional processing. The Mobility Controller strips the GRE header and processes the packet for authentication and stateful firewall, which enables centralized security policy, authentication, and access control. The tunneled node feature is enabled on a per-port basis. Any traffic coming from non tunneled node interfaces is forwarded without being tunneled to a Mobility Controller. BPDUs and LLDP traffic is terminated at the switch and not tunneled.

Note: Ensure that the Tunneled-Node VLAN is present and enabled on both the controller and switch.

Note: The switch will establish a single GRE tunnel between it and a Mobility Controller for Tunneled Node operation. However from the perspective of the Mobility Controller, each Tunneled Node port will appear as an individual port.

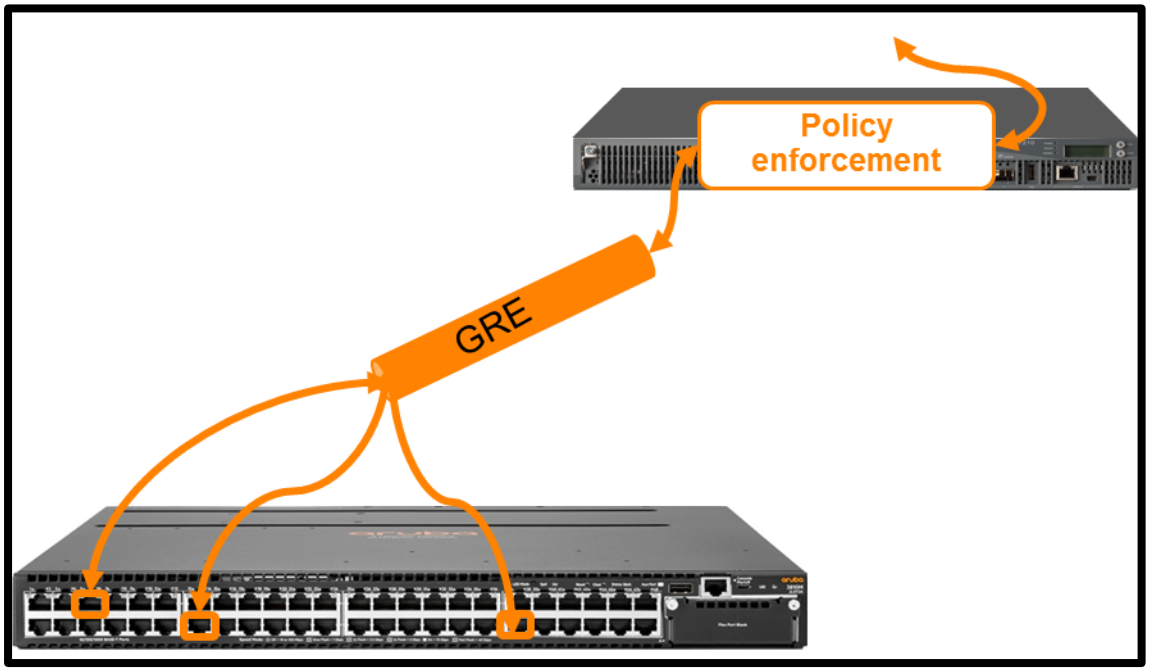

Figure 2: Per Port Tunneled Node

- When a port is configured for tunneled-node, ingress packets are encapsulated in an IP GRE frame which is then forwarded to the controller
- A unique GRE Key is needed – 1 to 1 Mapping:
    1. For the controller to uniquely identify GRE packet source port
    2. For the switch to send de-capsulated packet to particular port

As the traffic is encapsulated in a GRE tunnel so Jumbo frames should be enabled through the network and on the transport vlan.

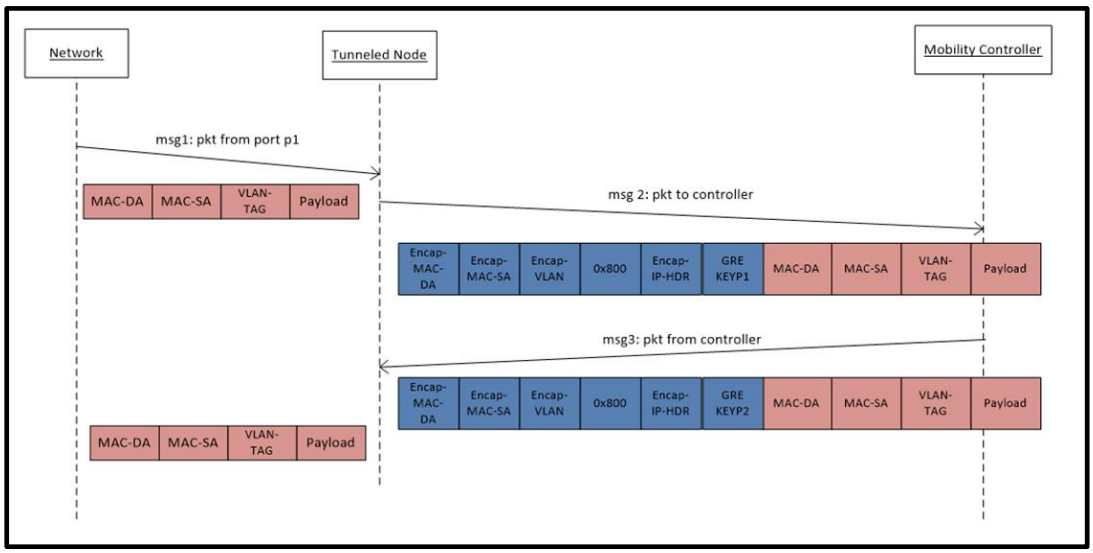

Figure 3:GRE encapsulation

What is it used for?

Per-Port Tunneled-Node allows using the same enforcement options for wired and wireless clients. This includes stateful session processing, deep packet inspection, URL filtering and bandwidth contracts

- Tunneled-node provides traffic separation across a layer 3 network. This could be used to present user traffic to a specific zone on the firewall. For example CCTV or POS traffic could carried across a layer 3 campus core. This is much simpler alternative to VRF or MPLS
- Alternative to vlan creation for branch Does not require any interaction or co-ordination with Telco provider to segment office networks with all traffic terminated on a branch Controller acting as branch router and security Gateway.
- Provides a simple overlay for new use case like CCTV deployment
- With Clearpass integration can provide ”colorless” (sic) ports for public spaces
- Can provide an aggregation layer for basic layer 2 switches to provide advanced traffic control and centralised policy driven Network Access

Switch support

PPTN is supported on:

- 5400R switch series with v2 and v3 modules

- 3810 switch series
- 2920 switch series
- 2930 switch series

- 3800 switch series

PPTN Feature limitations in 16.04.008

Global:

- Mesh
- QinQ
- Distributed Trunking

The following feature **are** supported on V3 platforms (2930,3810 and 5400R in V3 only mode).

- ıp multicast-routing
- Openflow
- VXLAN
- Service insertion
- IGMP lookup mode IP

Per port restrictions:

- ISC port
- Port is member of LAG
- Port security
- AAA (This would happen at the controller)
- Ipv4 address on vlan
- Ipv6 address on vlan
- Dipld
- Filter – multicast and protocol (Happens at controller)
- Virus throttling

The following features **are** supported on V3 platforms (2930,3810 and 5400R in V3 only mode).

- MLD on VLAN with PPTN ports
- IGMP on with PPTN ports

Best Practices

Ensure that the wireless controller can handle the necessary bandwidth and number of tunnels (Max physical ports that can be used as tunnels is listed below).

Max number of tunneled node ports

- 5400R [non-stacked] = 288
- 5400R [stacked] = 576
- 3810 [stacked] = 520
- 2930F [4mbr] = 208
- 2920[stacked] = 208

- 3800[stacked] = 520
- 2930M[10 mbr stack] = 520

- Ensure that the Tunneled-Node VLAN is present and enabled on both the controller and switch.
- Ensure that enough licenses are on the controller to handle the tunneled-node ports within the network (1 switch with Tunneled-Node ports enabled = 1 license on controller). Will need PEFNG license if using firewall functionality on controller

Test network

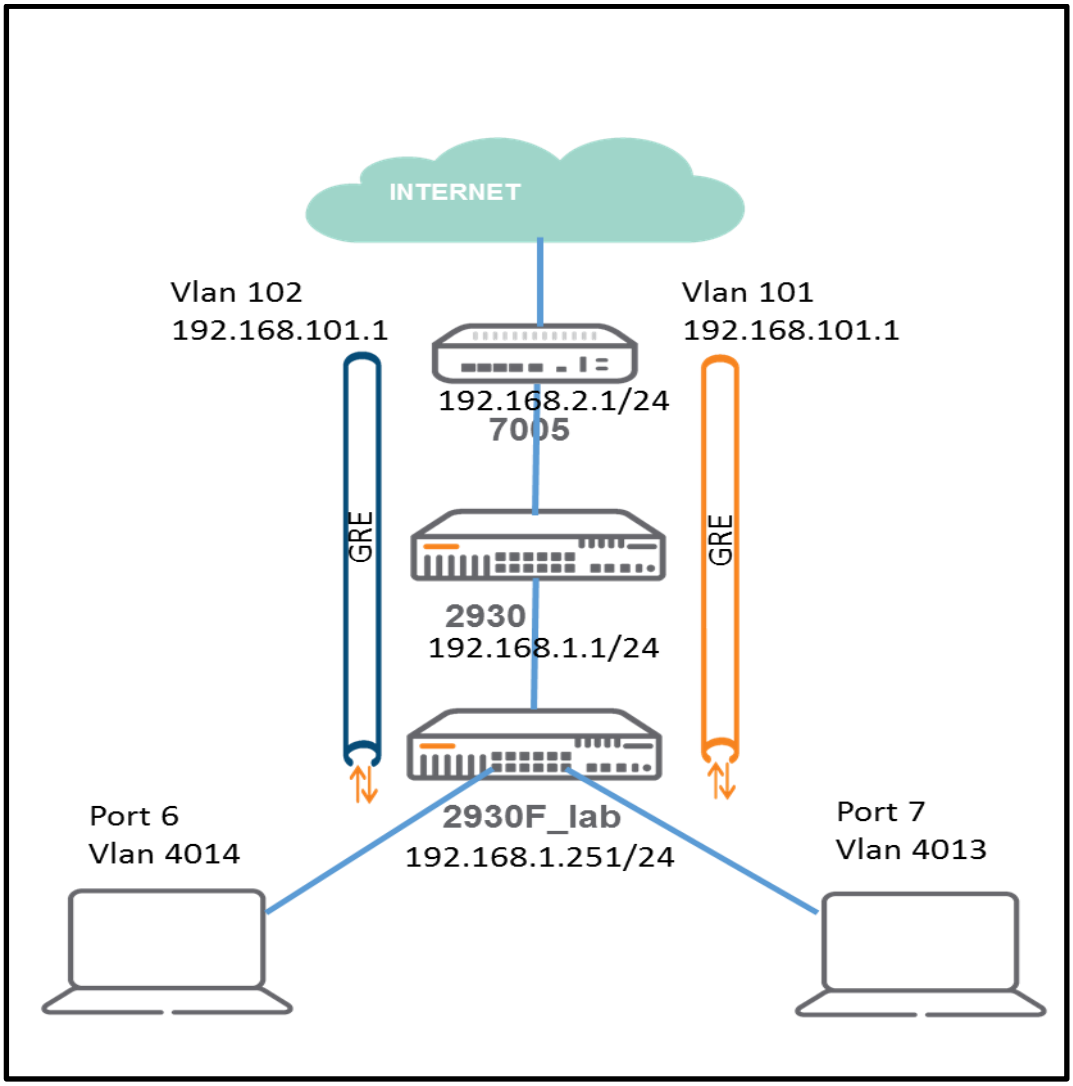

Figure 4: Test network

Test Scenario

In the above test scenario there are two PPTN transit vlans created to provide traffic separation between the Blue network and the Orange network. The laptop in port 6 (blue) is isolated from the laptop in port 7 (Orange) and they are carried across the layer 3 core to the central controller where DPI and Policy enforcement is performed. The Blue Laptop ends up in Vlan 102 and the Orange laptop in vlan 101. These vlans are only configured on the

controller, they do not exist in the access network. The PPTN transit vlans 4013 and 4014 are local to the lab switch and the 7005 controller and again they are not configured on the core 2930 switch. They just provide an encapsulation ID

Although this simplified test scenario only delivers Layer 2 transport to separate VLANs it is possible to provide advanced traffic filtering on the user traffic. The show commands in this document indicate what controls and traffic visibility is available

.

Software versions

Controller

```
(rbhome7005) *[mynode] #show version

Aruba Operating System Software.
ArubaOS (MODEL: Aruba7005), Version 8.2.0.0-beta
Website: http://www.arubanetworks.com
(c) Copyright 2017 Hewlett Packard Enterprise Development LP.
Compiled on 2017-08-24 at 09:09:20 UTC (build 61118) by p4build

ROM: System Bootstrap, Version CPBoot 1.0.2.0 (build 46859)
Built: 2014-10-31 10:10:57
Built by: p4build@re_client_46859


Switch uptime is 8 hours 52 minutes 22 seconds
Reboot Cause: User reboot (Intent:cause:register 78:86:0:2c)
Supervisor Card
Processor (XLP208 Rev B0 (Secure Boot) , 500 MHz) with 3797M bytes of memory.
32K bytes of non-volatile configuration memory.
1920M bytes of Supervisor Card system flash.
(rbhome7005) *[mynode] #
```

Switch

```
2930_lab(vlan-4014)# show version

Image stamp:
 /ws/swbuildm/rel_ukiah_qaoff/code/build/lvm(swbuildm_rel_ukiah_qaoff_rel_ukiah)
            Jul 21 2017 14:09:42
            WC.16.04.0008
            423
Boot Image:     Primary

Boot ROM Version:    WC.16.01.0003
Active Boot ROM:     Primary

2930_lab(vlan-4014)#
```

Controller Configuration

```
interface vlan 101
   ip address 192.168.101.1 255.255.255.0
```

```
!
ip dhcp excluded-address 192.168.1.20 192.168.101.1
ip dhcp pool wiredpptn
   dns-server 103.237.40.66 103.237.40.66
   default-router 192.168.101.1
   network 192.168.101.0 255.255.255.0
!
vlan 4013
   wired aaa-profile 2930PPTN
!
aaa profile "2930PPTN"
   initial-role "2930pptnuser"
!
aaa authentication wired
   profile "2930PPTN"

user-role 2930pptnuser
 vlan 101
   access-list session global-sacl
   access-list session apprf-2930pptnuser-sacl
   access-list session ra-guard
   access-list session allowall
   access-list session v6-allowall
```

Controller show commands

Verify the profile information

Show AAA profile

```
 (rbhome7005) *[mynode] #show aaa profile

AAA Profile List
----------------
Name                 References  Profile Status
----                 ----------  --------------
2930PPTN             2
default              1
default-dot1x        0           Predefined (changed)
default-dot1x-psk    0           Predefined (changed)
default-mac-auth     0           Predefined (changed)
default-open         0           Predefined (changed)
default-tunneled-user  0         Predefined (changed)
default-xml-api      0           Predefined (changed)
labtest              1
NoAuthAAAProfile     1           Predefined (changed)

Total:10
```

Show AAA profile

```
(rbhome7005) *[mynode] #show aaa profile 2930PPTN

AAA Profile "2930PPTN"
----------------------
Parameter                    Value
---------                    -----
Initial role                 2930pptnuser
MAC Authentication Profile   N/A
```

```
MAC Authentication Default Role     guest
MAC Authentication Server Group     default
802.1X Authentication Profile       N/A
802.1X Authentication Default Role  guest
802.1X Authentication Server Group  N/A
Download Role from CPPM             Disabled
Set username from dhcp option 12    Disabled
L2 Authentication Fail Through      Disabled
Multiple Server Accounting          Disabled
User idle timeout                   N/A
Max IPv4 for wireless user          2
RADIUS Accounting Server Group      N/A
RADIUS Roaming Accounting           Disabled
RADIUS Interim Accounting           Disabled
XML API server                      N/A
RFC 3576 server                     N/A
User derivation rules               N/A
Wired to Wireless Roaming           Enabled
Device Type Classification          Enabled
Enforce DHCP                        Disabled
PAN Firewall Integration            Disabled
Open SSID radius accounting         Disabled
(rbhome7005) *[mynode] #
```

Show VLAN

```
(rbhome7005) *[mynode] #show vlan
 (rbhome7005) *[mynode] #
VLAN CONFIGURATION
------------------
VLAN   Description  Ports           AAA Profile  Option-82
----   -----------  -----           -----------  ---------
1      Default      GE0/0/1 Pc0-7     N/A          Disabled
2      VLAN0002     GE0/0/0 GE0/0/2   N/A          Disabled
10     WAN          GE0/0/3           N/A          Disabled
100    VLAN0100                       N/A          Disabled
101    VLAN0101                       N/A          Disabled
4013   VLAN4013                       2930PPTN     Disabled
(rbhome7005) *[mynode] #
```

Show user role

```
(rbhome7005) *[mynode] #show user role 2930pptnuser
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
---------     -------------      ------    ----          ----------  ----  --------  -------   -------  ---------------                 -------
------------  ----  ---------  ---------
 192.168.101.2  98:4b:e1:eb:8e:08          2930pptnuser  00:00:13                tunnel 9  Wired
192.168.1.251:7/b0:5a:da:98:c4:c0  2930PPTN  tunnel                    WIRED
```

The laptop has been assigned an address in VLAN101 DHCP Pool 192.168.101.2
We can see the link back to the AAA Profile 2930PPTN

Show rights

We can look at the detail of the 2930pptnuser with the show rights command

```
(rbhome7005) *[mynode] #show rights

RoleTable
---------
Name                ACL  Bandwidth               ACL List
Type
----              ---  ---------              --------
----
2930pptnuser         87   Up: No Limit,Dn: No Limit  global-sacl/,apprf-2930pptnuser-sacl/,ra-
guard/,allowall/,v6-allowall/
User

User Entries: 1/1
 Curr/Cum Alloc:5/36 Free:0/31 Dyn:5 AllocErr:0 FreeErr:0
(rbhome7005) *[mynode] #
```

Further detail can be obtained by including the role name

```
(rbhome7005) *[mynode] #show rights 2930pptnuser

Valid = 'Yes'
CleanedUp = 'No'
Derived Role = '2930pptnuser'
 Up BW:No Limit   Down BW:No Limit
 L2TP Pool = default-l2tp-pool
 PPTP Pool = default-pptp-pool
 Number of users referencing it = 2
 Assigned VLAN = 101
 Periodic reauthentication: Disabled
 DPI Classification: Enabled
 Youtube education: Disabled
 Web Content Classification: Enabled
 IP-Classification Enforcement: Enabled
 ACL Number = 87/0
 Openflow: Enabled
 Max Sessions = 65535

 Check CP Profile for Accounting = TRUE

Application Exception List
--------------------------
Name  Type
----  ----

Application BW-Contract List
----------------------------
Name  Type  BW Contract  Id  Direction
----  ----  -----------  --  ---------

access-list List
----------------
Position  Name                 Type     Location
--------  ----               ----     --------
1         global-sacl            session
2         apprf-2930pptnuser-sacl  session
3         ra-guard               session
```

```
4       allowall              session
5       v6-allowall           session

global-sacl
-----------
Priority Source Destination Service Application Action TimeRange Log Expired Queue TOS 8021P
Blacklist Mirror DisScan IPv4/6 Contract
-------- ------ ----------- ------- ----------- ------ --------- --- ------- ----- --- ----- --------- ------ ------- ------ --
------
apprf-2930pptnuser-sacl
----------------------
Priority Source Destination Service Application Action TimeRange Log Expired Queue TOS 8021P
Blacklist Mirror DisScan IPv4/6 Contract
-------- ------ ----------- ------- ----------- ------ --------- --- ------- ----- --- ----- --------- ------ ------- ------ --
------
ra-guard
--------
Priority Source Destination Service       Application Action TimeRange Log Expired Queue TOS 8021P
Blacklist Mirror DisScan IPv4/6 Contract
-------- ------ ----------- -------       ----------- ------ --------- --- ------- ----- --- ----- --------- ------ ------- ---
--- --------
1       user    any         icmpv6 rtr-adv            deny                    Low                             6
allowall
--------
Priority Source Destination Service Application Action TimeRange Log Expired Queue TOS 8021P
Blacklist Mirror DisScan IPv4/6 Contract
-------- ------ ----------- ------- ----------- ------ --------- --- ------- ----- --- ----- --------- ------ ------- ------ --
------
1       any     any         any               permit                  Low                             4
2       any     any         any-v6            permit                  Low                             6
v6-allowall
-----------
Priority Source Destination Service Application Action TimeRange Log Expired Queue TOS 8021P
Blacklist Mirror DisScan IPv4/6 Contract
-------- ------ ----------- ------- ----------- ------ --------- --- ------- ----- --- ----- --------- ------ ------- ------ --
------
1       any     any         any-v6            permit                  Low                             6

Expired Policies (due to time constraints) = 0
(rbhome7005) *[mynode] #
```

Tunneled node show commands

192.168.1.251 is the IP address of the 2930 switch

show tunneled-node config

```
(rbhome7005) *[mynode] #show tunneled-node config

Tunneled node Server:Enabled
Tunnel Loop Prevention:Disabled


(rbhome7005) *[mynode] #show tunneled-node database

Tunneled node database
----------------------
IP          #Tunnels
```

```
--              --------
192.168.1.251  1
```

show tunneled-node state

```
(rbhome7005) *[mynode] #show tunneled-node state

Tunneled Node State
-------------------
IP              MAC               port  state     vlan  tunnel  inactive-time
--              ---               ----  -----     ----  ------  -------------
192.168.1.251  b0:5a:da:98:c4:c0  7     complete  4013  9       0
(rbhome7005) *[mynode] #
```

Switch config

```
tunneled-node-server
   controller-ip 192.168.2.1
   exit
interface 6
   tunneled-node-server
   exit
interface 7
   tunneled-node-server
   exit
interface 8
   tunneled-node-server
   exit
vlan 4013
   name "TN-TRANSPORT"
   untagged 6-8
   no ip address
   jumbo
   exit
```

Switch Show commands

Laptop is plugged into port 7 of my switch. The port state should come up as complete when all of the configuration is in place and the laptop is plugged in. If the port shows “in progress” there is an issue with configuration or ip reachability between the Switch and controller.

```
2930_lab(config)# show tunneled-node-server state

 Tunneled Node Port State

 Active Controller IP Address  : 192.168.2.1

 Port   State
 ------ -------------------------
 6      Port down
 7      Complete
 8      Port down

2930_lab(config)#
```

Note that laptop is plugged into port 7 of the switch

```
2930_lab(config)# show tunneled-node-server statistics

 Tunneled Node Statistics

  Port : 6
  Port : 7

   Control Plane Statistics

    Bootstrap packets sent      : 8
    Bootstrap packets received  : 8
    Bootstrap packets invalid   : 0

   Tunnel Statistics

    Rx Packets                          : 2554
    Tx Packets                          : 1827
    Rx 5 Minute Weighted Average Rate (Pkts/sec)  : 0
    Tx 5 Minute Weighted Average Rate (Pkts/sec)  : 0

  Port : 8

 Aggregate Statistics

  Heartbeat packets sent          : 2153
  Heartbeat packets received      : 2149
  Heartbeat packets invalid       : 0
  Fragmented Packets Dropped (Rx)  : 0
  Packets to Non-Existent Tunnel   : 0
  MTU Violation Drop              : 0

2930_lab(config)#
```

Appendix

Controller screenshots

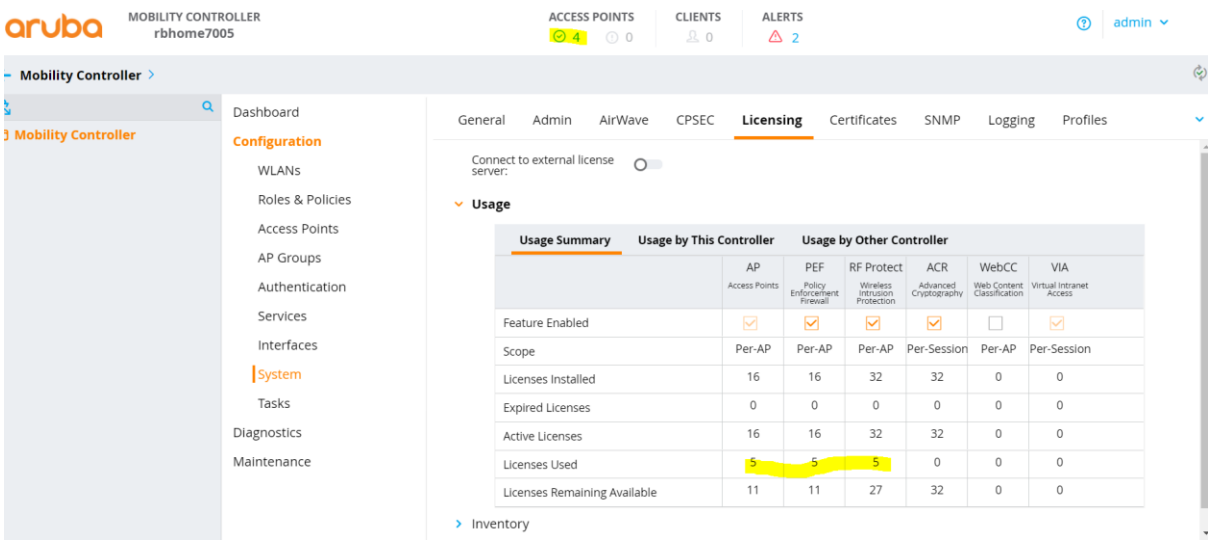

Figure 5: PPTN switch uses another license

As we can see from above there are 4 APs but 5 licenses used. Each PPTN switch consumes AP licenses. 4 licenses used by APs and 1 by PPTN switch

Another Cli example

On the access switch we want to use port 6 for a printer. Port 7 + 8 are allocated for laptops

We want printers to be placed in vlan 102. This can be done by adding the following config on the controller and switch.

Configuration commands to the controller.

```
ip access-list session apprf-tnprint-sacl
!
user-role tnprint
   access-list session allowall
   access-list session v6-allowall
   vlan 102
!
user-role 2930pptnuser
   access-list session apprf-authenticated-sacl
!
vlan 102
   description TNPRINT
!
vlan 4014
   wired aaa-profile 2930tnprint
!
interface vlan 102
   ip address 192.168.102.1 255.255.255.0
!
ip dhcp excluded-address 192.168.102.1 192.168.102.20
ip dhcp pool printpptn
   dns-server 103.237.40.66 103.237.40.66
   default-router 192.168.102.1
   network 192.168.102.0 255.255.255.0
!
aaa profile "2930tnprint"
   initial-role "tnprint"
!
aaa authentication wired
   profile "2930tnprint"
!
```

```
(rbhome7005) *[mynode] #show tunneled-node state

Tunneled Node State
-------------------
IP            MAC               port  state     vlan  tunnel  inactive-time
--            ---               ----  -----     ----  ------  -------------
```

```
192.168.1.251  b0:5a:da:98:c4:c0  6     complete  4014  31      1
192.168.1.251  b0:5a:da:98:c4:c0  7     complete  4013  14      1
(rbhome7005) *[mynode] #show tunneled-node database

Tunneled node database
----------------------
IP            #Tunnels
--            --------
192.168.1.251  2
(rbhome7005) *[mynode] #
```

Controller show commands

```
(rbhome7005) *[mynode] #show user role 2930pptnuser
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
----------     ------------      ------    ----         ----------  ----  --------  -------    -------  ---------------                 -------
------------  ----  ---------  ---------
192.168.101.3  b8:27:eb:7b:87:b9           2930pptnuser  00:00:08                  tunnel 14  Wired
192.168.1.251:7/b0:5a:da:98:c4:c0  2930PPTN  tunnel                     WIRED

User Entries: 1/1
 Curr/Cum Alloc:6/38 Free:0/32 Dyn:6 AllocErr:0 FreeErr:0
(rbhome7005) *[mynode] #show user role tnprint
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
----------     ------------      ------    ----      ----------  ----  --------  -------    -------  ---------------                 -------
------------  ----   ---------  ---------
192.168.102.21  98:4b:e1:eb:8e:08           tnprint   00:00:14                  tunnel 31  Wired
192.168.1.251:6/b0:5a:da:98:c4:c0  2930tnprint  tunnel        Win 7            WIRED

User Entries: 1/1
 Curr/Cum Alloc:6/38 Free:0/32 Dyn:6 AllocErr:0 FreeErr:0
(rbhome7005) *[mynode] #
```

Additional configuration commands to the switch

Tunneled node is already configured so we simple add the PPTN Vlan and bind it to the port

```
vlan 4014
   name "TNPRINT"
   untagged 6
   no ip address
   jumbo
   exit
interface 6 untagged vlan 4014
```

AppRF data for tunneled node

One of the major benefits of tunneled node is Deep Packet Inspection (DPI) capabilities that are available on the controller. Here is a screenshot showing the laptop traffic connected to the tnprint vlan 102.

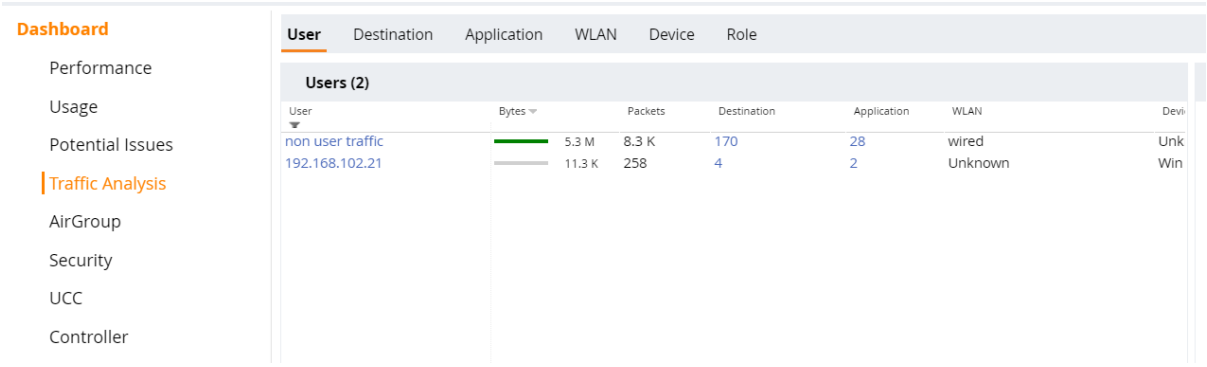

Figure 6: AppRF users

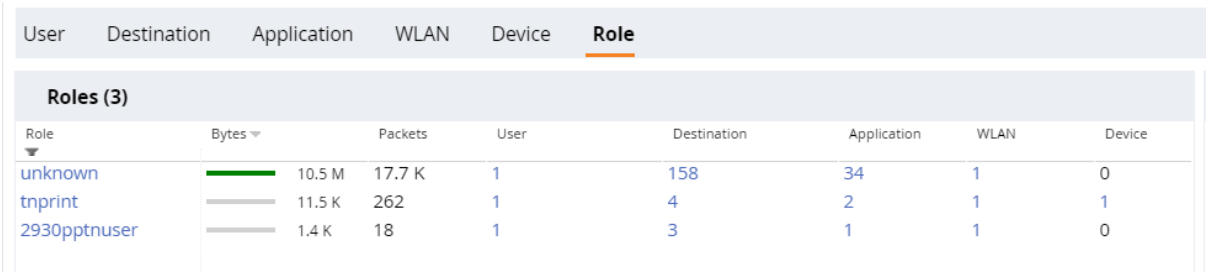

Figure 7: AppRF breakdown by role