

1 Table of Contents

Table of Contents

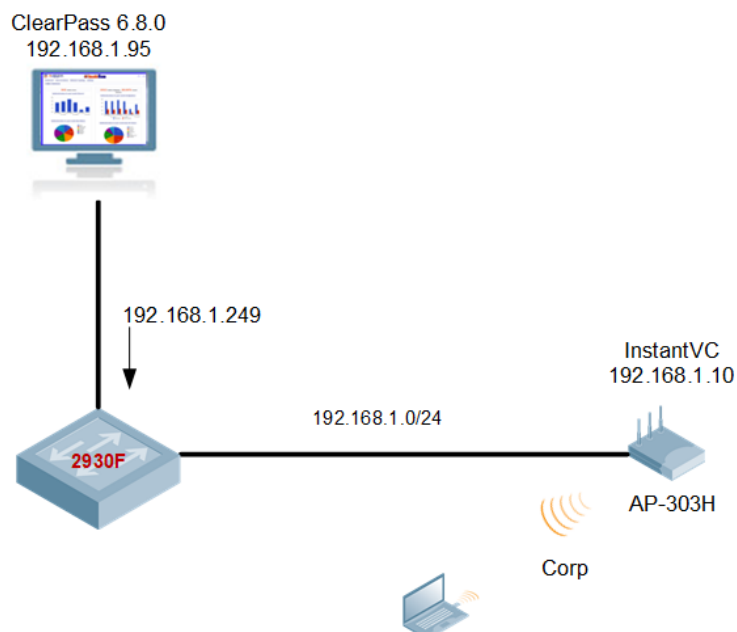
1	Table of Contents	1
1.1	Revision History	1
2	Time Based Services	2
2.1	Things you need	2
3	Instant AP Configuration.....	3
3.1	Network Time Protocol Configuration	3
3.2	Time Base Service Configuration	3
3.3	Assigning Time range Profiles to User Roles.....	4
3.4	Assigning Time range Profiles to SSIDs.....	6
3.5	Testing Time Range Profile for SSIDs.....	6
3.6	Testing Time Range Profile for User roles	8

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
08 May 2019	0.1	Ariya Parsamanesh	Initial creation

2 Time Based Services

Instant APs back in 6.4.x days supported enabling or disabling a SSID for clients at a particular time of the day. With the 8.4.x version you can now use a time range profile which can be particularly useful to restrict user access during a specific time period and gives much more flexibility.



2.1 Things you need

- Aruba Instant version 8.4.0.0 or later
- NTP source
- Aruba ClearPass or any authentication server
- A Layer three switch and some WiFi clients

3 Instant AP Configuration

Instant APs support the configuration of both absolute and periodic time range profiles. You can configure an absolute time range profile to execute during a specific timeframe or create a periodic profile to execute at regular intervals based on the periodicity specified in the configuration.

3.1 Network Time Protocol Configuration

The Time based services are dependent on Network Time Protocol (NTP), so first we need to configure it.

aruba

VIRTUAL
CONTROLLER

InstantVC

Dashboard

Configuration

Networks

Access Points

System

RF

Security

IDS

Routing

Tunneling

Services

DHCP Server

Maintenance

Support

General

Name

InstantVC

System location

Virtual Controller IP

192.168.1.10

Allow IPv6 Management

Virtual Controller IPv6

::

Dynamic RADIUS Proxy

Dynamic TACACS Proxy

MAS integration

NTP server

216.239.35.4

Timezone

Melbourne UTC+10

Daylight Saving Time

Preferred band

5 GHz

AppRF visibility

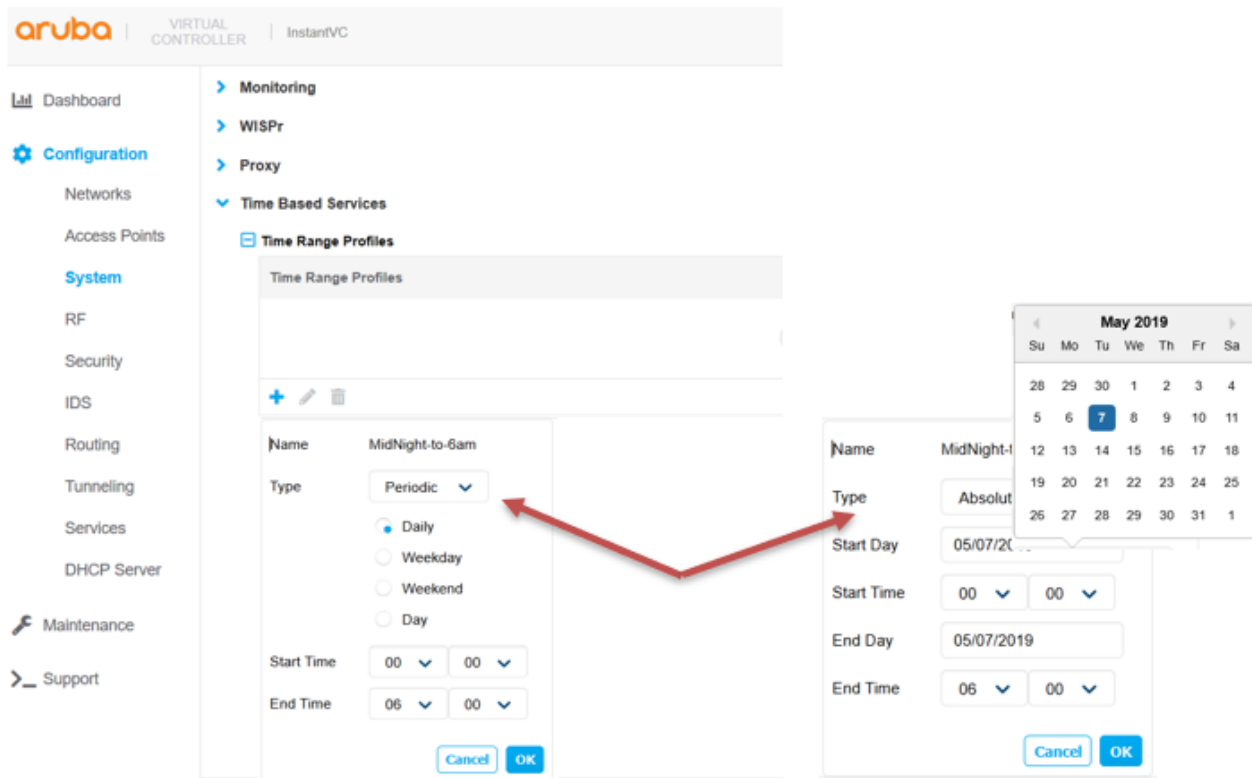
All

URL visibility

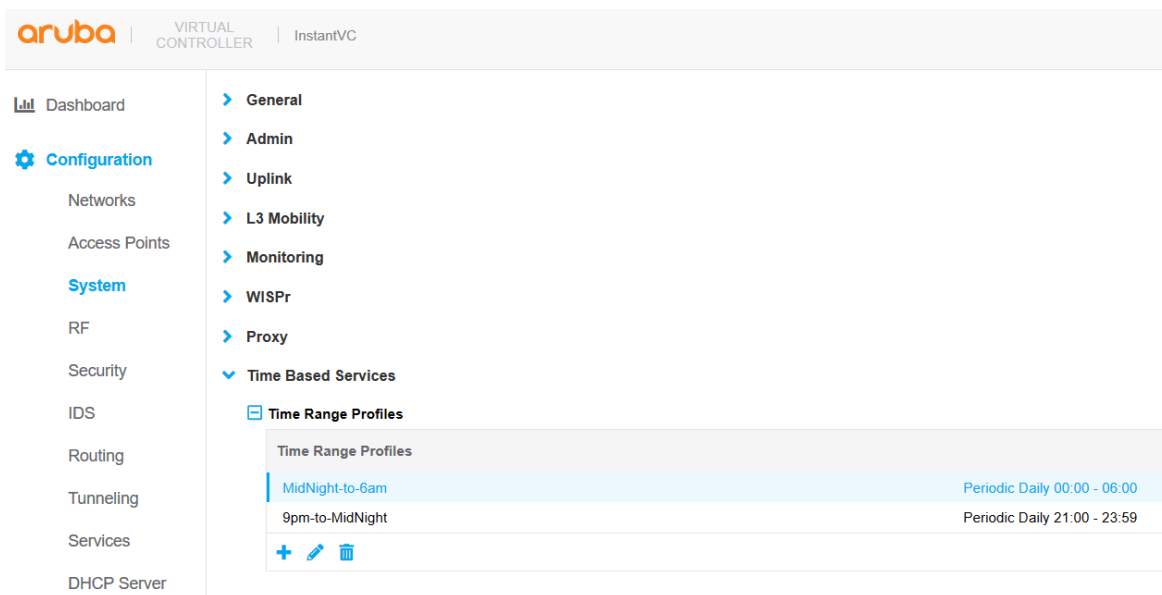
Cluster security

3.2 Time Base Service Configuration

First we need to create a few Time Range profiles that we can reference in the user roles. We'll start with a specific time range that we want to deny access.



Here you can use Period or absolute type. Now we have created two time range profiles to deny access during after hours periods as shown below.



Once you have saved it you can assign it to

1. various user roles. Here we'll add it to "students" use role
2. or a number of SSIDs

3.3 Assigning Time range Profiles to User Roles

Here we'll add it to "students" use role

aruba | VIRTUAL CONTROLLER | InstantVC

Dashboard

Configuration

Networks

Access Points

System

RF

Security

IDS

Routing

Tunneling

Services

DHCP Server

Authentication Servers

Users

Roles

Roles

Wired-VLAN20

dot1x

BYOD-Provision

Exec

CaptivePortalPreAuth

EpsonPrinter

CapeSensor

SG9

ArubaMPSK

Students

S5-Remote

Access Rules for Students

No data to display

Here we are editing the first rule denying DHCP services from 9pm to mid night.

Edit rule

Rule type: Access control

Service: Network

bootp

Action: Deny

Destination: to all destinations

Options

Log

DSCP Tag

Time Range: 9pm-to-MidNight

Blacklist

Disable scanning

802.1p priority

Cancel OK

The final configuration looks as shown below.

aruba | VIRTUAL CONTROLLER | InstantVC

Dashboard

Overview

Networks

Access Points

Clients

Configuration

Networks

Access Points

System

RF

Security

IDS

Authentication Servers

Users

Roles

Roles

Wired-VLAN20

dot1x

BYOD-Provision

Exec

CaptivePortalPreAuth

EpsonPrinter

CapeSensor

SG9

ArubaMPSK

Students

S5-Remote

Access Rules for Students

Deny bootp to all destinations + time range 9pm-to-MidNight

Deny any to all destinations + time range 9pm-to-MidNight

Deny bootp to all destinations + time range MidNight-to-6am

Deny any to all destinations + time range MidNight-to-6am

Allow any to all destinations

But for our testing which will be after 9pm, we'll change it so that the the client is permitted to get an IP address but will deny all traffic to 8.8.8.8 and log it.

Roles

Roles

Wired-VLAN20

dot1x

BYOD-Provision

Exec

CaptivePortalPreAuth

EpsonPrinter

CapeSensor

SG9

ArubaMPSK

Students

S5-Remote

+

🗑️

Access Rules for Students

• Deny bootp to all destinations + log + time range 9pm-to-MidNight

• Deny any on server 8.8.8.8 + log + time range 9pm-to-MidNight

• Deny bootp to all destinations + time range MidNight-to-6am

• Deny any to all destinations + time range MidNight-to-6am

• Allow any to all destinations

+

✎

🗑️

↑

↓

3.4 Assigning Time range Profiles to SSIDs

We are going to assign the time range profiles to Corp SSID.

aruba

VIRTUAL CONTROLLER

InstantVC

Dashboard

Overview

Networks

Access Points

Clients

Configuration

Networks

Access Points

System

RF

Security

IDS

Routing

Tunneling

Services

DHCP Server

Maintenance

Transmit Rates

802.11

Zone

Time Range

Time Range Profiles

Bandwidth Limits

WMM

Miscellaneous

Content filtering

Inactivity timeout

Deauth inactive clients

SSID

Out of service (OOS)

OOS time (global)

Max clients threshold

SSID encoding

ESSID

Deny inter user bridging

Openflow

1000

VPN down

30 sec.

64

Default

Corp

Content filtering

Inactivity timeout

Deauth inactive clients

SSID

Out of service (OOS)

OOS time (global)

Max clients threshold

SSID encoding

ESSID

Deny inter user bridging

Openflow

Content filtering

Inactivity timeout

Deauth inactive clients

SSID

Out of service (OOS)

OOS time (global)

Max clients threshold

SSID encoding

ESSID

Deny inter user bridging

Openflow

Time Range Profiles

Name

Status

MidNight-to-6am

Not Applied

3pm-to-9pm

Not Applied

9pm-to-MidNight

Disabled

Cancel

OK

You should note that, for the “Disabled” action, if the current time is greater than the start time and lesser than the end time, the SSID will not be broadcast by the AP in the list of available networks. If an ACL rule is linked to the time profile, it is re-programmed and the rule which is time-based is not applied. All the user sessions having this role assigned will be deleted.

3.5 Testing Time Range Profile for SSIDs

This is the current BSS table. Note that Corp ESSID is enabled and broadcasting.

```
BLDG-A-ATV1# sh clock

Current Time      :2019-05-07 16:46:54
BLDG-A-ATV1#
BLDG-A-ATV1# sh ap bss-table

Aruba AP BSS Table
-----
bss          ess          port  ip          phy    type  ch/EIRP/max-EIRP  cur-cl  ap name
in-t(s)  tot-t    flags                --      ---   ----  -----
-----  -----  -----
24:f2:7f:d5:fa:d0  SG1      ?/?    192.168.1.121  a-VHT  ap    36E/23.0/23.0     6       BLDG-A-
ATV1  0      28m:42s
24:f2:7f:d5:fa:d1  Corp     ?/?    192.168.1.121  a-VHT  ap    36E/23.0/23.0     0       BLDG-A-
ATV1  0      28m:41s
24:f2:7f:d5:fa:d2  SG9      ?/?    192.168.1.121  a-VHT  ap    36E/23.0/23.0     0       BLDG-A-
ATV1  0      28m:24s  W3M
24:f2:7f:d5:fa:d3  ArubaMPSK ?/?    192.168.1.121  a-VHT  ap    36E/23.0/23.0     0       BLDG-A-
ATV1  0      28m:24s
24:f2:7f:d5:fa:c0  SG1      ?/?    192.168.1.121  g-HT   ap    11/9.0/23.0       1       BLDG-A-
ATV1  0      28m:41s
24:f2:7f:d5:fa:c1  Corp     ?/?    192.168.1.121  g-HT   ap    11/9.0/23.0       0       BLDG-A-
ATV1  0      28m:33s
24:f2:7f:d5:fa:c2  SG9      ?/?    192.168.1.121  g-HT   ap    11/9.0/23.0       0       BLDG-A-
ATV1  0      28m:24s  W3M
24:f2:7f:d5:fa:c3  ArubaMPSK ?/?    192.168.1.121  g-HT   ap    11/9.0/23.0       0       BLDG-A-
ATV1  0      28m:23s

Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:8
Num Associations:7

Flags:      K = 802.11K Enabled; W = 802.11W Enabled; 3 = WPA3 BSS; O = OWE Transition mode OWE
BSS; o = OWE Transition mode Open BSS; M = WPA3-SAE mixed mode BSS
BLDG-A-ATV1#
```

Now after 9:00pm we don't see the Corp ESSID.

```
BLDG-A-ATV1# sh clock

Current Time      :2019-05-07 21:07:50
BLDG-A-ATV1# sh ap bss-table

Aruba AP BSS Table
-----
bss          ess          port  ip          phy    type  ch/EIRP/max-EIRP  cur-cl  ap name
in-t(s)  tot-t    flags                --      ---   ----  -----
-----  -----  -----
24:f2:7f:d5:fa:d0  SG1      ?/?    192.168.1.121  a-VHT  ap    36E/23.0/23.0     4       BLDG-A-
ATV1  0      4h:52m:16s
24:f2:7f:d5:fa:d2  SG9      ?/?    192.168.1.121  a-VHT  ap    36E/23.0/23.0     0       BLDG-A-
ATV1  0      4h:51m:58s  W3M
24:f2:7f:d5:fa:d3  ArubaMPSK ?/?    192.168.1.121  a-VHT  ap    36E/23.0/23.0     0       BLDG-A-
ATV1  0      4h:51m:58s
24:f2:7f:d5:fa:c0  SG1      ?/?    192.168.1.121  g-HT   ap    11/9.0/23.0       1       BLDG-A-
ATV1  0      4h:52m:15s
```

```

24:f2:7f:d5:fa:c2 SG9      ???  192.168.1.121 g-HT  ap  11/9.0/23.0  0  BLDG-A-
ATV1 0      4h:51m:58s W3M
24:f2:7f:d5:fa:c3 ArubaMPSK ???  192.168.1.121 g-HT  ap  11/9.0/23.0  0  BLDG-A-
ATV1 0      4h:51m:57s

Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:6
Num Associations:5

Flags:      K = 802.11K Enabled; W = 802.11W Enabled; 3 = WPA3 BSS; O = OWE Transition mode OWE
BSS; o = OWE Transition mode Open BSS; M = WPA3-SAE mixed mode BSS
BLDG-A-ATV1#

```

3.6 Testing Time Range Profile for User roles

First we need to check if our time ranges are correct and valid. Note that even though we the “valid” column is set to “No”, that does not necessarily means that the configuration will not work. It simply stating that the time ranges are not valid since it is 3:43 pm.

```

BLDG-A-ATV1# sh clock

Current Time      :2019-05-07 15:43:42
BLDG-A-ATV1#
BLDG-A-ATV1# sh time-range

Current Time      :2019-05-07 15:43:55
Time Range Summary
-----
Profile Name      Type      Start Day  Start Time  End Day  End Time  Valid
-----
MidNight-to-6am   Periodic  daily     00:00      -        06:00     No
9pm-to-MidNight   Periodic  daily     21:00      -        23:59     No
BLDG-A-ATV1#

```

Now lets add another time range called 3pm-to-9pm

Time Based Services

Time Range Profiles

Time Range Profiles	
MidNight-to-6am	Periodic Daily 00:00 - 06:00
3pm-to-9pm	Periodic Daily 15:00 - 21:00
9pm-to-MidNight	Periodic Daily 21:00 - 23:59
  	

Now we should get a valid time range profile.

```

BLDG-A-ATV1# sh time-range

Current Time      :2019-05-07 15:45:02
Time Range Summary
-----
Profile Name      Type      Start Day  Start Time  End Day  End Time  Valid
-----

```

MidNight-to-6am	Periodic	daily	00:00	-	06:00	No
3pm-to-9pm	Periodic	daily	15:00	-	21:00	Yes
9pm-to-MidNight	Periodic	daily	21:00	-	23:59	No
BLDG-A-ATV1#						

We can also check which time profile is added to a user role or SSID profile. Note that the SSID profile is dot1x and the ESSID is “Corp”

```
BLDG-A-ATV1# sh time-profile
```

Time Range	SSID Profile	
-----	-----	-----
Time Profile Name	SSID profile Name	Enable/Disable
-----	-----	-----
9pm-to-MidNight	dot1x	Disable

```
Time Range ACL Profile
```

Time Profile Name	Access Role Name	Rule
-----	-----	----
MidNight-to-6am	Students	any any match udp 67 69 deny time-range MidNight-to-6am
MidNight-to-6am	Students	any any match any any any deny time-range MidNight-to-6am
9pm-to-MidNight	Students	8.8.8.8 255.255.255.255 match any any any deny time-range
9pm-to-MidNight		

```
BLDG-A-ATV1#
```

We will get a client to connect the “Corp” SSID before 9pm and the user connects fine.

VIRTUAL CONTROLLER
InstantVC

Dashboard
Overview
Networks
Access Points
Clients
Configuration
Networks
Access Points
System
RF
Security
IDS

Wireless (4) Wired (0)

Name	IP Address	MAC address	OS	ESSID	Access Point	Channel	Type	Role	IPv6 Address
--	192.168.1.122	f8:d0:27:34:e9:12	--	SG1	BLDG-A-ATV1	6	GN	EpsonPrinter	fe80::fad0:27ff:fe34:...
--	192.168.1.128	84:38:38:46:a9:39	Android	SG1	BLDG-A-ATV1	36E	AC	S5-Remote	fd14:5f94:8156:260...
Galaxy-S8	192.168.1.136	30:07:4d:4a:e5:66	Android	SG1	BLDG-A-ATV1	36E	AC	SG1	fd14:5f94:8156:260...
student1	192.168.1.120	a4:d1:d2:5f:32:52	Apple	Corp	BLDG-A-ATV1	36	AN	Students	fd14:5f94:8156:260...

Overview

Client Match

AppRF

Info

Name	student1
IPv6 Address	fd14:5f94:8156:2600:8e1:313a:3231:2cf5
IP Address	192.168.1.120
MAC address	a4:d1:d2:5f:32:52
OS	Apple
ESSID	Corp
Access Point	BLDG-A-ATV1
Channel	36
Type	AN
Role	Students

RF Dashboard

Client	Signal
student1	
Access Point	Utilization
BLDG-A-ATV1	
	Noise

And now from the client we'll ping 8.8.8.8, as you can see, the traffic will get through.

```
BLDG-A-ATV1# sh datapath session | incl 192.168.1.120
```

17.252.252.42	192.168.1.120	6	5223	55983	0	0	0	1	dev8	2d	1	34	FCA
17.252.252.85	192.168.1.120	6	5223	56003	0	0	0	1	dev26	2f	b	107c	
1.1.1.1	192.168.1.120	17	53	59929	0	0	0	1	dev26	46	0	0	FIA
192.168.1.120	192.168.1.1	17	54640	53	0	0	48	1	dev26	47	0	0	FCIA
192.168.1.120	8.8.8.8	1	1	2048	0	0	0	1	dev26	1e	0	0	FYCI
192.168.1.120	8.8.8.8	1	0	2048	0	0	0	1	dev26	23	0	0	FYCI
192.168.1.120	8.8.8.8	1	3	2048	0	0	0	0	dev26	14	0	0	FYCI
192.168.1.120	8.8.8.8	1	2	2048	0	0	0	0	dev26	19	0	0	FYCI
192.168.1.120	8.8.8.8	1	5	2048	0	0	0	0	dev26	a	0	0	FYCI
192.168.1.120	8.8.8.8	1	4	2048	0	0	0	0	dev26	f	0	0	FYCI

1.1.1.1	192.168.1.120	17	53	52141	0	0	0	1	dev26	4b	0	0	FIA
192.168.1.120	1.1.1.1	17	55048	53	0	0	48	1	dev26	50	0	0	FCIA
1.1.1.1	192.168.1.120	17	53	51508	0	0	0	1	dev26	4b	0	0	FIA
8.8.8.8	192.168.1.120	1	1	0	0	0	0	1	dev26	1e	1	54	FI
8.8.8.8	192.168.1.120	1	0	0	0	0	0	1	dev26	23	1	54	FI
8.8.8.8	192.168.1.120	1	3	0	0	0	0	1	dev26	14	1	54	FI
8.8.8.8	192.168.1.120	1	2	0	0	0	0	1	dev26	19	1	54	FI
8.8.8.8	192.168.1.120	1	5	0	0	0	0	0	dev26	a	1	54	FI
8.8.8.8	192.168.1.120	1	4	0	0	0	0	1	dev26	f	1	54	FI

BLDG-A-ATV1#

Now after 9:00pm the client is still connected and had a valid IP address. Remember that in the time based ACL we also denied dhcp service. Now the client tries to ping 8.8.8.8, the ping is unsuccessful.

BLDG-A-ATV1# sh client

Client List

Name	IP Address	MAC Address	OS	ESSID	Access Point	Channel	Type	Role	IPv6
Address		Signal	Speed (mbps)						
----	-----	-----	--	-----	-----	-----	----	----	-----

```
student1 192.168.1.120 a4:d1:d2:5f:32:52 Apple Corp BLDG-A-ATV1 36 AN Students
fd14:5f94:8156:2600:8e1:313a:3231:2cf5 44 (good) 58 (good)
```

Number of Clients :1

Info timestamp :2744

BLDG-A-ATV1#

BLDG-A-ATV1# sh datapath sess | incl 192.168.1.120

Flags: F - fast age, S - src NAT, N - dest NAT

D - deny, R - redirect, Y - no syn

H - high prio, P - set prio, T - set ToS

C - client, M - mirror, V - VOIP

I - Deep inspect, U - Locally destined

s - media signal, m - media mon, a - rtp analysis

E - Media Deep Inspect, G - media signal

A - Application Firewall Inspect

L - ALG session

O - Session is programmed through SDN/Openflow controller

p - Session is marked as permanent

RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to master, t - time based

Source IP	Destination IP	Prot	SPort	Dport	Cntr	Prio	ToS	Age	Destination	TAge	Packets	Bytes	Flags
-----	-----	---	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
192.168.1.120	192.168.1.1	17	54349	53	0	0	48	0	dev26	3f	0	0	FDCA
192.168.1.120	8.8.8.8	1	9	2048	0	0	0	0	dev26	25	0	0	FDYCA
192.168.1.120	8.8.8.8	1	8	2048	0	0	0	0	dev26	2a	0	0	FDYCA
192.168.1.120	8.8.8.8	1	11	2048	0	0	0	0	dev26	1b	0	0	FDYCA
192.168.1.120	8.8.8.8	1	10	2048	0	0	0	0	dev26	20	0	0	FDYCA
192.168.1.120	8.8.8.8	1	13	2048	0	0	0	0	dev26	11	0	0	FDYCA
192.168.1.120	1.1.1.1	17	54349	53	0	0	48	0	dev26	30	0	0	FDCA
192.168.1.120	1.1.1.1	17	54640	53	0	0	48	0	dev26	36	0	0	FDCA
192.168.1.120	1.1.1.1	17	59353	53	0	0	0	0	dev26	9	0	0	FDYCA
192.168.1.120	1.1.1.1	17	61636	53	0	0	0	0	dev26	9	0	0	FDYCA

BLDG-A-ATV1#

Here is the logs that we had configured.

BLDG-A-ATV1# sh log sec 10

```
May 9 21:19:31 stm[6213]: <124006> <WARN> |AP BLDG-A-ATV1@192.168.1.121 stm| UDP srcip=192.168.1.120
srcport=63892 dstip=1.1.1.1 dstport=53, action=deny
May 9 21:19:32 stm[6213]: <124006> <WARN> |AP BLDG-A-ATV1@192.168.1.121 stm| UDP srcip=192.168.1.120
srcport=59353 dstip=1.1.1.1 dstport=53, action=deny
May 9 21:19:32 stm[6213]: <124006> <WARN> |AP BLDG-A-ATV1@192.168.1.121 stm| UDP srcip=192.168.1.120
srcport=54640 dstip=1.1.1.1 dstport=53, action=deny
May 9 21:19:32 stm[6213]: <124006> <WARN> |AP BLDG-A-ATV1@192.168.1.121 stm| UDP srcip=192.168.1.120
srcport=64869 dstip=1.1.1.1 dstport=53, action=deny
May 9 21:19:32 stm[6213]: <124006> <WARN> |AP BLDG-A-ATV1@192.168.1.121 stm| UDP srcip=192.168.1.120
srcport=64011 dstip=1.1.1.1 dstport=53, action=deny
```

```
May 9 21:19:32 stm[6213]: <124006> <WARN> |AP BLDG-A-ATV1@192.168.1.121 stm| UDP srcip=192.168.1.120  
srcport=64011 dstip=1.1.1.1 dstport=53, action=deny
```

```
BLDG-A-ATV1#
```

Now we get the client to release and renew its IP address and it will never gets a valid IP address since the time based ACL denies this traffic.

```
BLDG-A-ATV1# sh log sec 10
```

```
May 9 21:37:03 stm[6213]: <124006> <WARN> |AP BLDG-A-ATV1@192.168.1.121 stm| UDP srcip=0.0.0.0 srcport=68  
dstip=255.255.255.255 dstport=67, dhcp msgtype=1(discover) clientip=0.0.0.0 clientmac=a4:d1:d2:5f:32:52,  
action=deny  
May 9 21:37:03 stm[6213]: <124006> <WARN> |AP BLDG-A-ATV1@192.168.1.121 stm| ICMPv6  
srcip=fe80::1016:5191:c8f2:7703 dstip=ff02::2, type=133, code=0, action=deny  
May 9 21:37:05 stm[6213]: <124006> <WARN> |AP BLDG-A-ATV1@192.168.1.121 stm| UDP srcip=0.0.0.0 srcport=68  
dstip=255.255.255.255 dstport=67, dhcp msgtype=1(discover) clientip=0.0.0.0 clientmac=a4:d1:d2:5f:32:52,  
action=deny  
May 9 21:37:07 stm[6213]: <124006> <WARN> |AP BLDG-A-ATV1@192.168.1.121 stm| ICMPv6  
srcip=fe80::1016:5191:c8f2:7703 dstip=ff02::2, type=133, code=0, action=deny  
May 9 21:37:12 stm[6213]: <124006> <WARN> |AP BLDG-A-ATV1@192.168.1.121 stm| UDP srcip=0.0.0.0 srcport=68  
dstip=255.255.255.255 dstport=67, dhcp msgtype=1(discover) clientip=0.0.0.0 clientmac=a4:d1:d2:5f:32:52,  
action=deny  
May 9 21:37:23 stm[6213]: <124006> <WARN> |AP BLDG-A-ATV1@192.168.1.121 stm| proto = igmp  
srcip=169.254.156.14 dstip=224.0.0.22, action=deny  
May 9 21:37:29 stm[6213]: <124006> <WARN> |AP BLDG-A-ATV1@192.168.1.121 stm| UDP srcip=0.0.0.0 srcport=68  
dstip=255.255.255.255 dstport=67, dhcp msgtype=1(discover) clientip=0.0.0.0 clientmac=a4:d1:d2:5f:32:52,  
action=deny  
BLDG-A-ATV1#
```

Here is another show command that can be helpful that shows the rules for a given rule name along with the hits.

```
BLDG-A-ATV1# show datapath acl-rule Students  
Datapath SSID: Students ACL Entries
```

```
-----  
Flags: P - permit, L - log, E - established, M/e - MAC/etype filter  
       S - SNAT, D - DNAT, R - redirect, r - reverse redirect m - Mirror  
       I - Invert SA, i - Invert DA, H - high prio, O - set prio, C - Classify Media  
       A - Disable Scanning, B - black list, T - set TOS, t - time based, o - tunnel only  
       K - App Throttle, s - Domain SA, d - Domain DA, 4 - IPv4, 6 - IPv6  
-----
```

```
ACL Name {Students 0} Number {195}  
1: any any 17 0-65535 8209-8211 P4  
2: any any 17 0-65535 4434-4434 P4  
3: any any 17 0-65535 67-69 Lt6  
4: any any 17 0-65535 67-69 Lt4 hits 37  
5: any 8.8.8.8 255.255.255.255 any Lt4 hits 15  
6: any any any Lt6 hits 8  
7: any any any Lt4 hits 8  
8: any any any P6  
9: any any any P4  
10: any any any Pe4 hits 14  
-----
```

```
ACL Name {Students 1} Number {196}  
1: any any 17 0-65535 8209-8211 P4  
2: any any 17 0-65535 4434-4434 P4  
3: any any 17 0-65535 67-69 LTt6  
4: any any 17 0-65535 67-69 LTt4  
5: any 8.8.8.8 255.255.255.255 any LTt4  
6: any any any LTt6  
7: any any any LTt4  
8: any any any PT6  
9: any any any PT4  
10: any any any Pe4  
-----
```

```
BLDG-A-ATV1#
```