Dynamic Authorization Extensions to Radius in Comware

Background

Dynamic Authorization Extensions (DAE) is an extension to Radius. It is officially documented in RFC 3576 (circa 2003). The RFC 5176 (circa 2008) is an updated version of RFC 3576.

DAE is comprised of two additional Radius messages:

CoA Change of Authorization

This message is used to modify an already-authenticated session, hence the name “Change of Authorization”. It can be used to modify the attributes that were sent in the Access-Accept, or a CoA message can be built for any purpose, i.e. any combination of valid Radius attributes can be put into the CoA Request and the receiver can take any action it sees fit.

DM Disconnect Message

This message is used to disconnect an already-authenticated session.

Most often, DAE is referred to as “COA”.

References to “COA” will mean DAE for the remainder of this document.

Radius uses the following UDP ports (these are default values) :

- For Authentication 1812
- For Accounting 1813
- COA uses the following port: 3799

It is important to note that a Radius server (Aruba Clearpass Policy Manager aka CPPM, FreeRadius, Windows, etc.) listens for Radius Authentication/Accounting on those ports (1812, 1813) whereas a device that listens for COA requests (like a switch) will listen on port 3799. So the Comware switch is, in effect, a COA Server. The COA client can be anywhere.

Common examples of COA clients are Aruba Clearpass and Linux (radclient command), and even a FreeRadius server can be configured to act as a COA client.

Comware Support for COA

Comware 5 and Comware 7 have taken slightly different paths for support for COA.

Until recently, COA was not supported on Comware at all.

Comware 5 would accept COA messages, log them, but they would be discarded from that point on.

Comware 7 would silently discard any COA messages.

COA for Customer

Customer had a strong desire to have COA functionality for their 5130 (Comware 7) switches.

They wanted to have the ability to do disconnect authenticated sessions (mac-authentication and dot1x) with the ability to disable the port on which it was received. They also wanted multiple combinations of those two factors.

In summary:

1) Ability to disconnect one session, leave all other sessions, and leave the port in UP state.
2) Ability to disconnect all sessions on a port, and have the port go into ADM Down state and then back into UP state.
3) Ability to disconnect all sessions on a port, and have the port go into ADM Down state and stay there until some other stimulus changed it (e.g.: “undo shutdown” on the port)

Customer was provided with this functionality as follows:

1) Disconnect Message (standard DAE Disconnect Message)
2) “Bounce Port” custom COA message
3) “Disable Port” custom COA message

The “Bounce Port” and “Disable Port” messages are constructed with the following Radius attributes:

1)	IETF Attribute	User-Name
2)	IETF Attribute	Calling-Station-Id
3)	Cisco Vendor-Specific Attribute	Cisco-AVPair

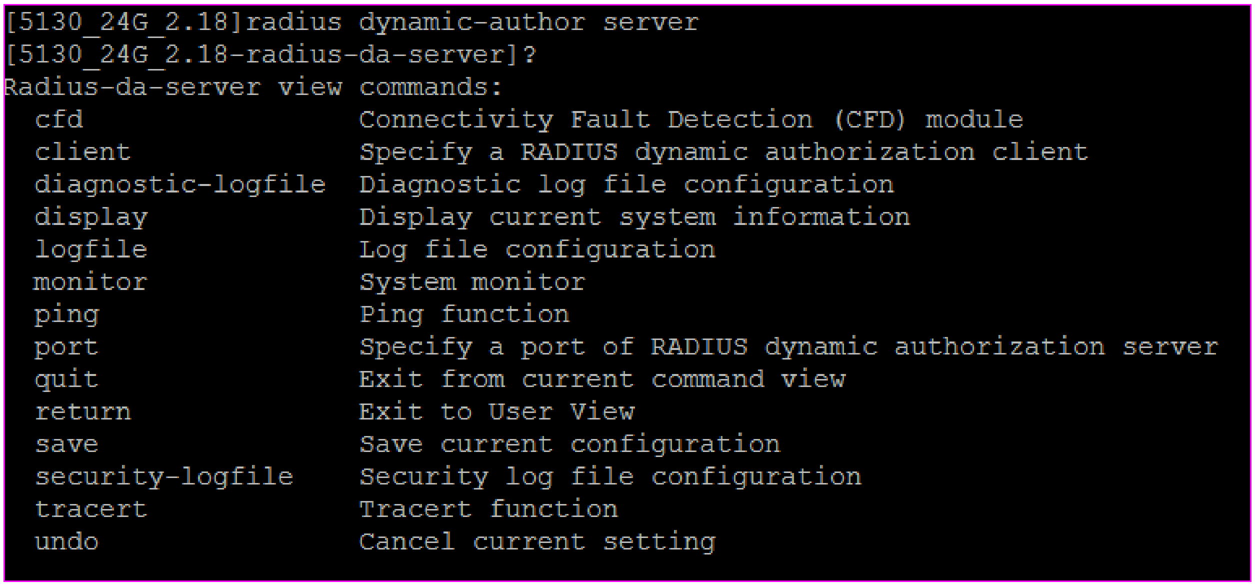
Both the User-Name and the Calling-Station-Id are the same that was sent in the Access-Request message.

For the Bounce, Cisco-AVPair has the value: “subscriber:command=bounce-host-port”

For the Disable, Cisco-AVPair has the value: “subscriber:command=disable-host-port”

COA Setup on Comware

Comware versions that support COA will have the following:



```
[5130_24G_2.18]radius dynamic-author server
[5130_24G_2.18-radius-da-server]?
Radius-da-server view commands:
  cfd                   Connectivity Fault Detection (CFD) module
  client                Specify a RADIUS dynamic authorization client
  diagnostic-logfile    Diagnostic log file configuration
  display               Display current system information
  logfile               Log file configuration
  monitor               System monitor
  ping                  Ping function
  port                  Specify a port of RADIUS dynamic authorization server
  quit                  Exit from current command view
  return                Exit to User View
  save                  Save current configuration
  security-logfile      Security log file configuration
  tracert               Tracert function
  undo                  Cancel current setting
```

Basic COA functionality is added with the following:

client ip <ip of device sending COA> key simple abc

where “abc” is the shared secret between the switch and the COA client

COA Setup on COA Clients

COA on Aruba Clearpass

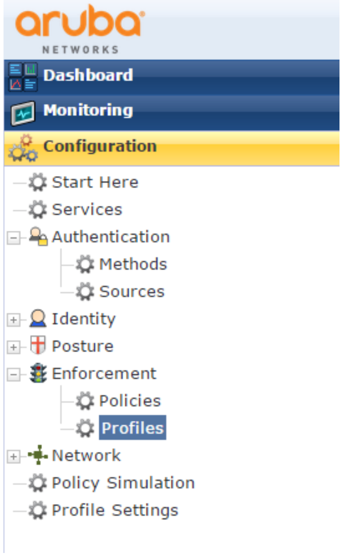
Customer is using Aruba Clearpass Policy Manager (CPPM).

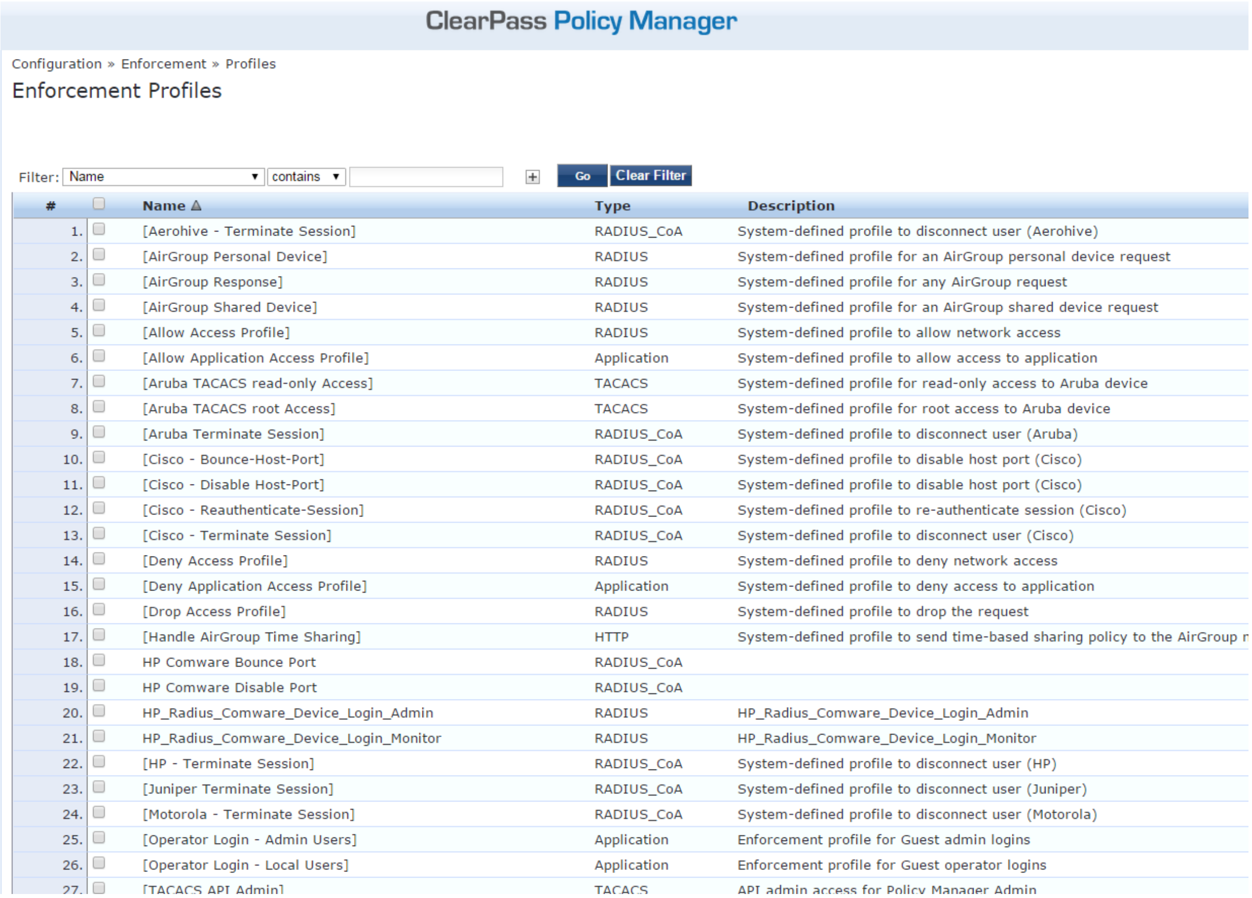
- CPPM can be obtained from Aruba as a virtual machine (OVF format) and can be instantiated on any hypervisor (Type 2 or Bare-Metal)
- It comes with a 90-day trial.
- CPPM is accessed with a secure browser session: https://<ip address of CPPM>

Using CCPM is beyond the scope of this document, but these examples will show how the Bounce and Disable are created and used.

Creating COA Actions in CPPM

CPPM has “Enforcement Profiles”





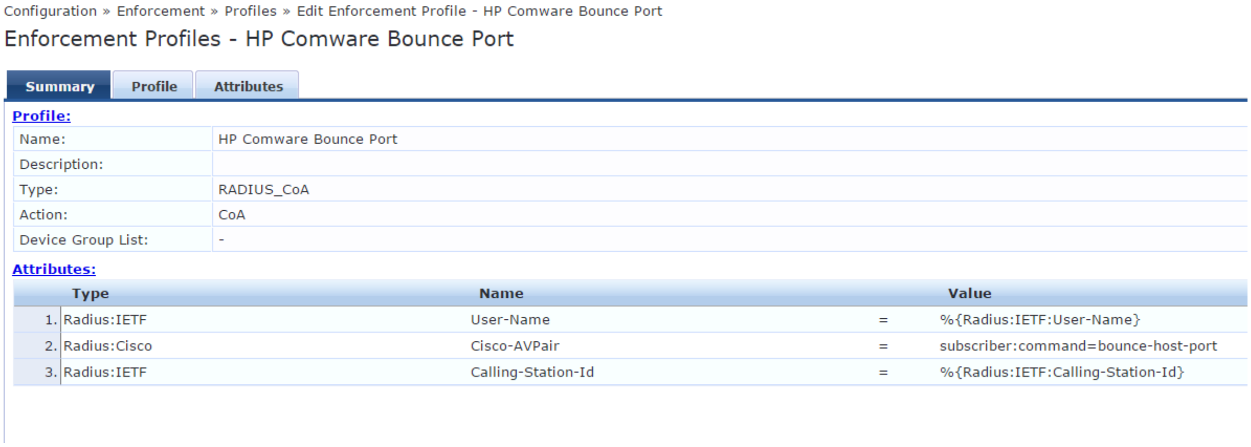
Configuration » Enforcement » Profiles

Enforcement Profiles

#	□	Name ▲	Type	Description
1.	□	[Aerohive - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aerohive)
2.	□	[AirGroup Personal Device]	RADIUS	System-defined profile for an AirGroup personal device request
3.	□	[AirGroup Response]	RADIUS	System-defined profile for any AirGroup request
4.	□	[AirGroup Shared Device]	RADIUS	System-defined profile for an AirGroup shared device request
5.	□	[Allow Access Profile]	RADIUS	System-defined profile to allow network access
6.	□	[Allow Application Access Profile]	Application	System-defined profile to allow access to application
7.	□	[Aruba TACACS read-only Access]	TACACS	System-defined profile for read-only access to Aruba device
8.	□	[Aruba TACACS root Access]	TACACS	System-defined profile for root access to Aruba device
9.	□	[Aruba Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aruba)
10.	□	[Cisco - Bounce-Host-Port]	RADIUS_CoA	System-defined profile to disable host port (Cisco)
11.	□	[Cisco - Disable Host-Port]	RADIUS_CoA	System-defined profile to disable host port (Cisco)
12.	□	[Cisco - Reauthenticate-Session]	RADIUS_CoA	System-defined profile to re-authenticate session (Cisco)
13.	□	[Cisco - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Cisco)
14.	□	[Deny Access Profile]	RADIUS	System-defined profile to deny network access
15.	□	[Deny Application Access Profile]	Application	System-defined profile to deny access to application
16.	□	[Drop Access Profile]	RADIUS	System-defined profile to drop the request
17.	□	[Handle AirGroup Time Sharing]	HTTP	System-defined profile to send time-based sharing policy to the AirGroup r
18.	□	HP Comware Bounce Port	RADIUS_CoA	
19.	□	HP Comware Disable Port	RADIUS_CoA	
20.	□	HP_Radius_Comware_Device_Login_Admin	RADIUS	HP_Radius_Comware_Device_Login_Admin
21.	□	HP_Radius_Comware_Device_Login_Monitor	RADIUS	HP_Radius_Comware_Device_Login_Monitor
22.	□	[HP - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (HP)
23.	□	[Juniper Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Juniper)
24.	□	[Motorola - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Motorola)
25.	□	[Operator Login - Admin Users]	Application	Enforcement profile for Guest admin logins
26.	□	[Operator Login - Local Users]	Application	Enforcement profile for Guest operator logins
27.	□	[TACACS API Admin]	TACACS	API admin access for Policy Manager Admin

Enforcement Profiles 18 and 19 (Bounce and Disable) have been created.

If the Bounce is selected:



Configuration » Enforcement » Profiles » Edit Enforcement Profile - HP Comware Bounce Port

Enforcement Profiles - HP Comware Bounce Port

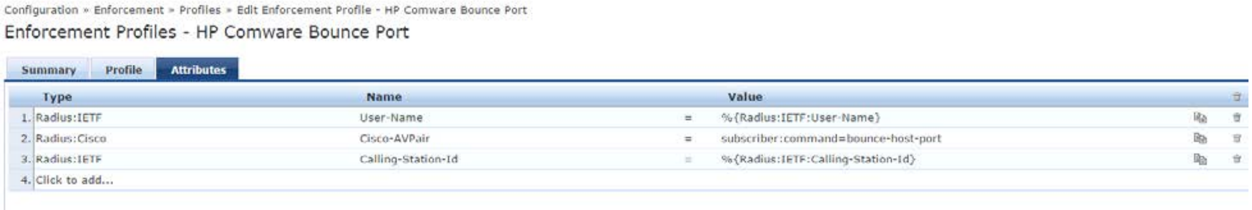
Profile:

Name:	HP Comware Bounce Port
Description:	
Type:	RADIUS_CoA
Action:	CoA
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:IETF	User-Name	=	%{Radius:IETF:User-Name}
2.	Radius:Cisco	Cisco-AVPair	=	subscriber:command=bounce-host-port
3.	Radius:IETF	Calling-Station-Id	=	%{Radius:IETF:Calling-Station-Id}

On the Attributes tab, the attributes can be added/deleted/modified:



Configuration » Enforcement » Profiles » Edit Enforcement Profile - HP Comware Bounce Port

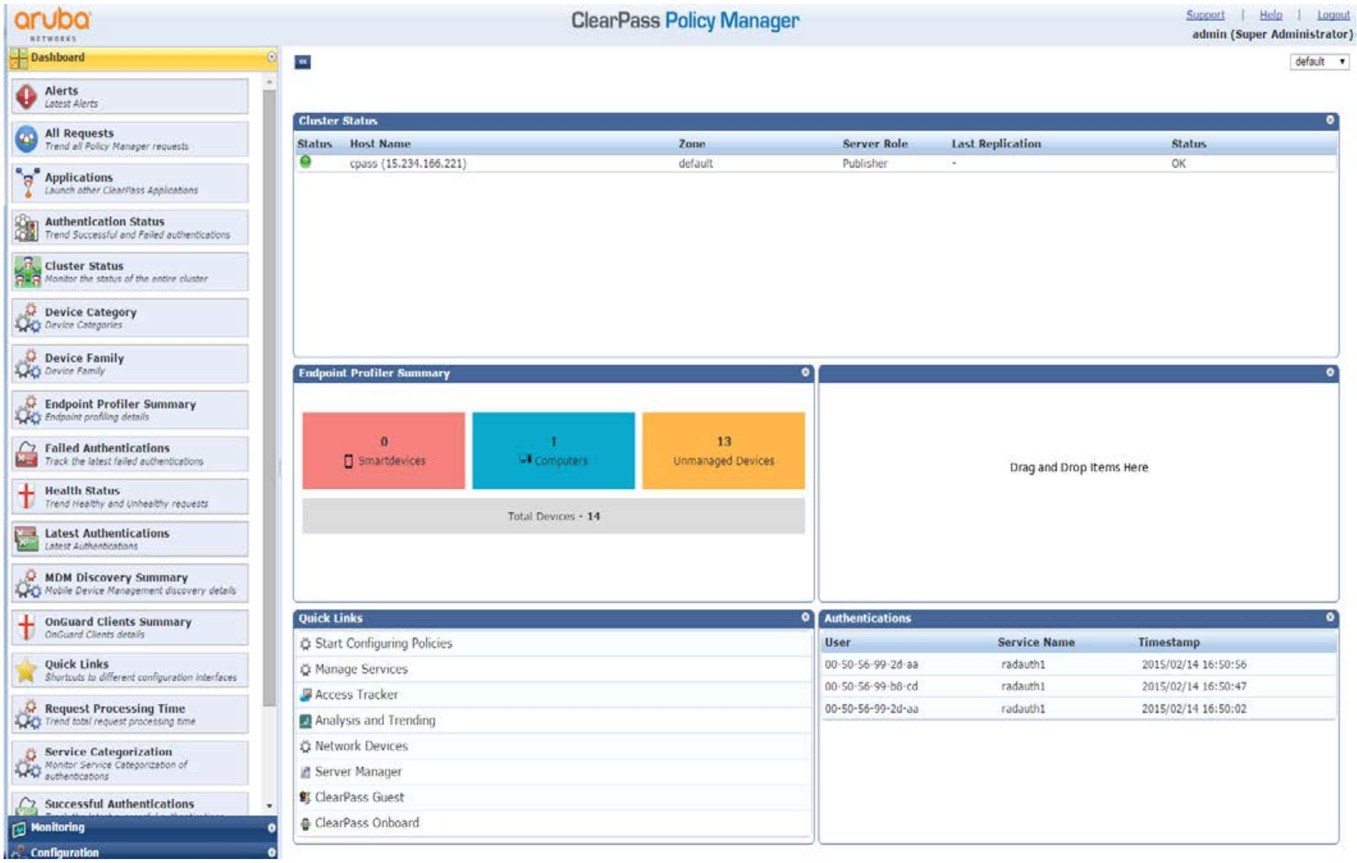
Enforcement Profiles - HP Comware Bounce Port

	Type	Name		Value
1.	Radius:IETF	User-Name	=	%{Radius:IETF:User-Name}
2.	Radius:Cisco	Cisco-AVPair	=	subscriber:command=bounce-host-port
3.	Radius:IETF	Calling-Station-Id	=	%{Radius:IETF:Calling-Station-Id}
4.	Click to add...			

Initiating COA Actions from CPPM

To see what mac-authentication and/or dot1x sessions are active in CPPM, perform the following:

Click on “Dashboard”. The following screen will appear:



aruba
NETWORKS
ClearPass Policy Manager
Support | Help | Logout
admin (Super Administrator)
default
Dashboard
Alerts
Latest Alerts
All Requests
Trend all Policy Manager requests
Applications
Launch other ClearPass Applications
Authentication Status
Trend Successful and Failed authentications
Cluster Status
Monitor the status of the entire cluster
Device Category
Device Categories
Device Family
Device Family
Endpoint Profiler Summary
Endpoint profiling details
Failed Authentications
Track the latest failed authentications
Health Status
Trend Healthy and Unhealthy requests
Latest Authentications
Latest Authentications
MDM Discovery Summary
Mobile Device Management discovery details
OnGuard Clients Summary
OnGuard Clients details
Quick Links
Shortcuts to different configuration interfaces
Request Processing Time
Trend total request processing time
Service Categorization
Monitor Service Categorization of authentications
Successful Authentications
Monitoring
Configuration

Cluster Status

Status	Host Name	Zone	Server Role	Last Replication	Status
●	cpass (15.234.166.221)	default	Publisher	-	OK

Endpoint Profiler Summary

Quick Links

Authentications

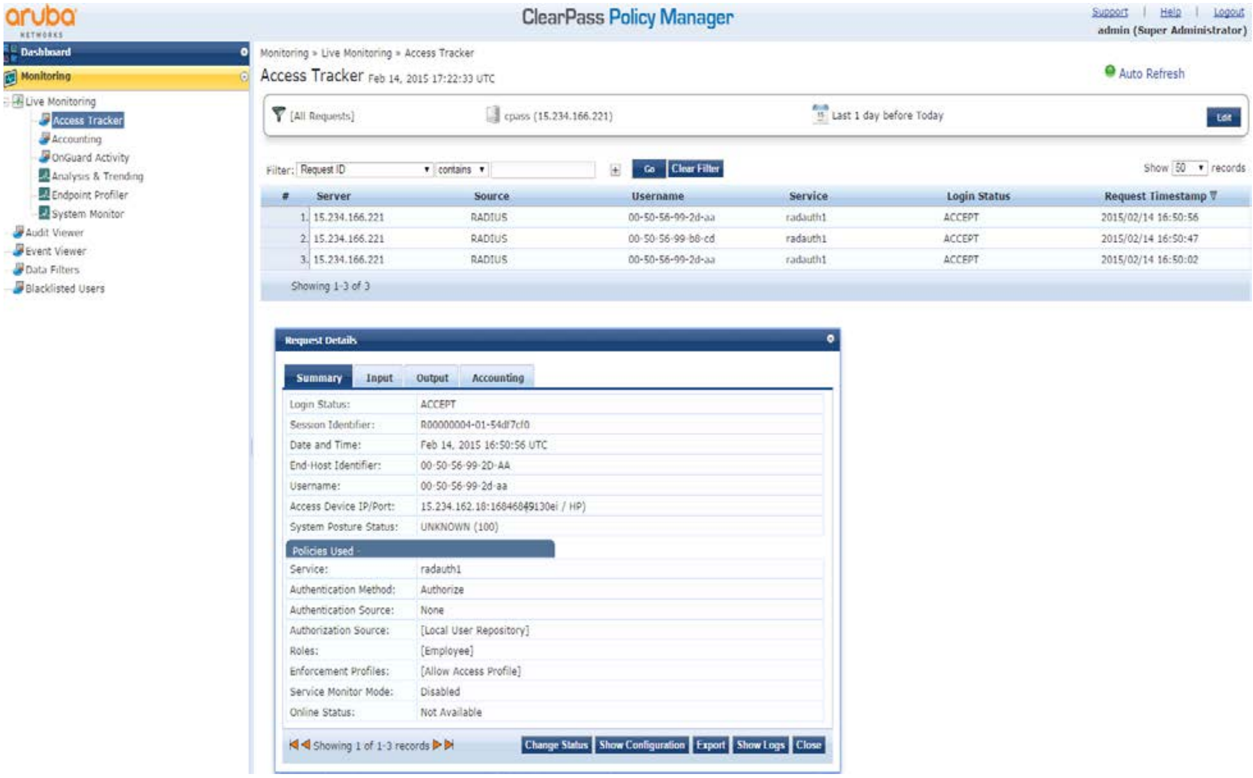
User	Service Name	Timestamp
00-50-56-99-2d-aa	radauth1	2015/02/14 16:50:56
00-50-56-99-b8-cd	radauth1	2015/02/14 16:50:47
00-50-56-99-2d-aa	radauth1	2015/02/14 16:50:02

Under “Authentication” on the bottom right is a list of the current sessions.

To modify (send COA) on these sessions, click on “Quick Links/Access Tracker”

Click on one of the active sessions, and another screen will appear.

On this screen, the “Summary” of the session is shown.



Access Tracker Feb 14, 2015 17:22:33 UTC

[All Requests] cpass (15.234.166.221) Last 1 day before Today

Filter: Request ID contains

Show 50 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	15.234.166.221	RADIUS	00-50-56-99-2d-aa	radauth1	ACCEPT	2015/02/14 16:50:56
2.	15.234.166.221	RADIUS	00-50-56-99-b8-cd	radauth1	ACCEPT	2015/02/14 16:50:47
3.	15.234.166.221	RADIUS	00-50-56-99-2d-aa	radauth1	ACCEPT	2015/02/14 16:50:02

Showing 1-3 of 3

Request Details

Login Status:	ACCEPT
Session Identifier:	R00000004-01-54df7cf0
Date and Time:	Feb 14, 2015 16:50:56 UTC
End-Host Identifier:	00-50-56-99-2D-AA
Username:	00-50-56-99-2d-aa
Access Device IP/Port:	15.234.162.18:16846849130ei / HP)
System Posture Status:	UNKNOWN (100)

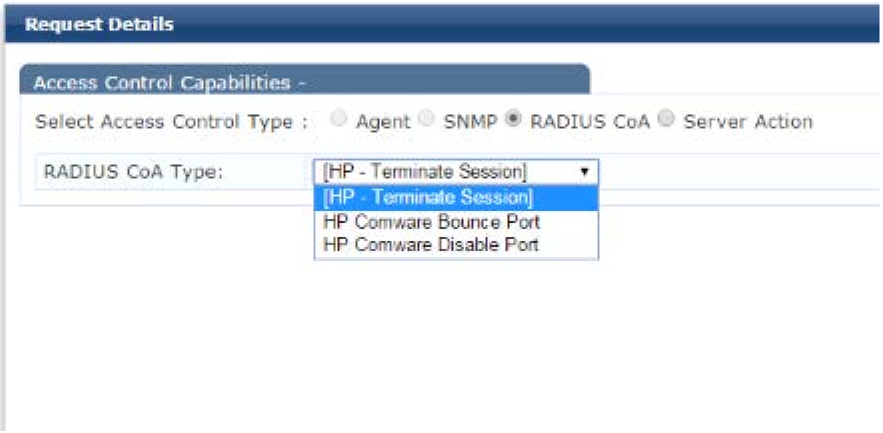
Policies Used -

Service:	radauth1
Authentication Method:	Authorize
Authentication Source:	None
Authorization Source:	[Local User Repository]
Roles:	[Employee]
Enforcement Profiles:	[Allow Access Profile]
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 1 of 1-3 records

To modify the session, click on “Change Status”

This will present choices for session modification:



Request Details

Access Control Capabilities -

Select Access Control Type : ○ Agent ○ SNMP ● RADIUS CoA ○ Server Action

RADIUS CoA Type: [HP - Terminate Session]

The three actions available are Terminate Session (Disconnect), Bounce, and Disable.

Choose the action desired, and then click “Submit”.

This will send the COA request to the switch which holds this session.

COA on Linux

COA is relatively easy to send from a Linux machine.

The command, radclient can be used to send the message.

The following example will send a Bounce to a switch:

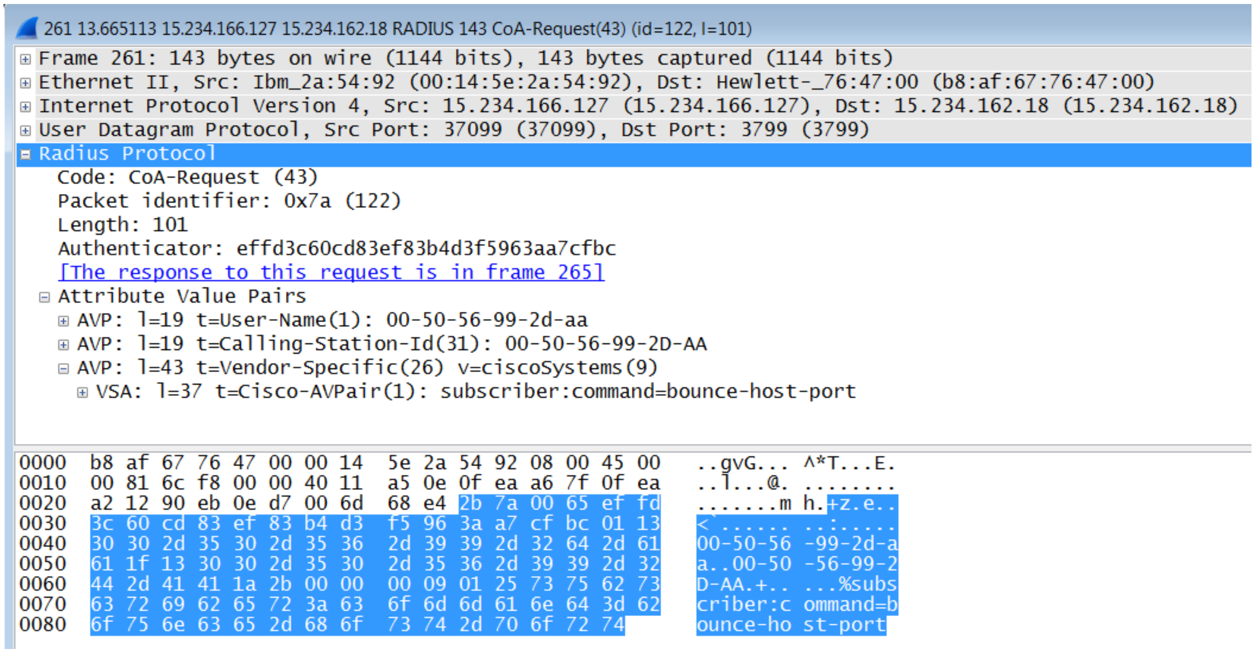
```
echo "User-Name=00-50-56-99-2d-aa, Calling-Station-Id=00-50-56-99-2D-AA, Cisco-AVPair=\"subscriber:command=bounce-host-port\"" | radclient -x 15.234.162.18  coa abc
```

It has the advantage of being easy to use. One disadvantage is that the User-Name and Calling-Station-Id must be entered manually each time. In CPPM those values are retained and ready to be sent as they were received in the Access-Request.

radclient is a very powerful testing tool, however.

COA in Wireshark

The following shows how a COA Request (in this example, a Bounce Port) appears.



```
261 13.665113 15.234.166.127 15.234.162.18 RADIUS 143 CoA-Request(43) (id=122, l=101)
⊞ Frame 261: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits)
⊞ Ethernet II, Src: Ibm_2a:54:92 (00:14:5e:2a:54:92), Dst: Hewlett-_76:47:00 (b8:af:67:76:47:00)
⊞ Internet Protocol Version 4, Src: 15.234.166.127 (15.234.166.127), Dst: 15.234.162.18 (15.234.162.18)
⊞ User Datagram Protocol, Src Port: 37099 (37099), Dst Port: 3799 (3799)
⊟ Radius Protocol
    Code: CoA-Request (43)
    Packet identifier: 0x7a (122)
    Length: 101
    Authenticator: effd3c60cd83ef83b4d3f5963aa7cfbc
    [The response to this request is in frame 265]
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=19 t=User-Name(1): 00-50-56-99-2d-aa
    ⊞ AVP: l=19 t=Calling-Station-Id(31): 00-50-56-99-2D-AA
    ⊟ AVP: l=43 t=Vendor-Specific(26) v=ciscoSystems(9)
      ⊞ VSA: l=37 t=Cisco-AVPair(1): subscriber:command=bounce-host-port

0000  b8 af 67 76 47 00 00 14  5e 2a 54 92 08 00 45 00   ..gvG... ^*T...E.
0010  00 81 6c f8 00 00 40 11  a5 0e 0f ea a6 7f 0f ea   ..l...@. ........
0020  a2 12 90 eb 0e d7 00 6d  68 e4 2b 7a 00 65 ef fd   .......m h.+z.e..
0030  3c 60 cd 83 ef 83 b4 d3  f5 96 3a a7 cf bc 01 13   <`...... ..:.....
0040  30 30 2d 35 30 2d 35 36  2d 39 39 2d 32 64 2d 61   00-50-56 -99-2d-a
0050  61 1f 13 30 30 2d 35 30  2d 35 36 2d 39 39 2d 32   a..00-50 -56-99-2
0060  44 2d 41 41 1a 2b 00 00  00 09 01 25 73 75 62 73   D-AA.+.. ...%subs
0070  63 72 69 62 65 72 3a 63  6f 6d 6d 61 6e 64 3d 62   criber:c ommand=b
0080  6f 75 6e 63 65 2d 68 6f  73 74 2d 70 6f 72 74      ounce-ho st-port
```

COA Troubleshooting

Switch debugging

"debug radius all"

will show all radius traffic in/out of the switch. It will also dump raw Radius packets.

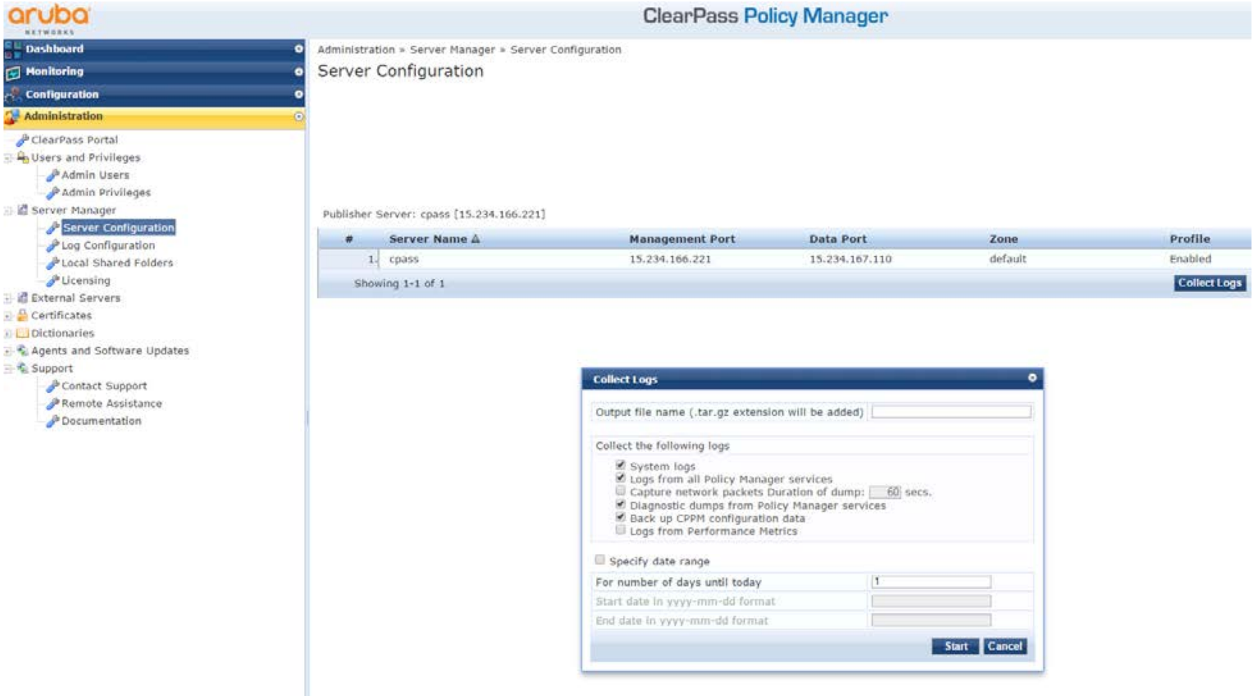
"debug mac-authentication all" and "debug dot1x all" may also be used to debug the authentication of the individual sessions.

CPPM Debugging

CPPM allows for network trace capture:

Administration/Server Manager/Server Configuration

Collect Logs



Administration » Server Manager » Server Configuration

Server Configuration

Publisher Server: cpass [15.234.166.221]

#	Server Name	Management Port	Data Port	Zone	Profile
1.	cpass	15.234.166.221	15.234.167.110	default	Enabled

Showing 1-1 of 1

Collect Logs

Output file name (.tar.gz extension will be added)

Collect the following logs

- ☑ System logs
- ☑ Logs from all Policy Manager services
- □ Capture network packets Duration of dump: 60 secs.
- ☑ Diagnostic dumps from Policy Manager services
- ☑ Back up CPPM configuration data
- □ Logs from Performance Metrics

□ Specify date range

For number of days until today: 1

Start date in yyyy-mm-dd format

End date in yyyy-mm-dd format

Will start a network capture which can be imported into Wireshark.

CPPM Support Report

CPPM allows for SSH access. Once connected, the command: “system gen-support-key” will gather all data necessary for a report to Aruba.