# Avaya VoIP Phone with Cisco Switch and CPPM

The purpose of this document is to provide the setup and methodology on how to configure CPPM, the Cisco Switch, and DHCP server in order for the phone to be MAC authenticated and the Computer behind the phone to be authenticated via 802.1x. This document assumes that basic configuration has been completed (switch, dhcp relay for profile information, 802.1x authentication, Profiling Service1, Cisco 802.1x Switch Authentication2, and a generic catch-all radius service). This document will focus on an Avaya 4600 VoIP phone, though the process should be similar for any VoIP phone.

For the most part, VoIP phones do not do 802.1x authentication. Instead, the 802.1x authentication is passed from the computer through the phone to the switch. But how do we authenticate that phone without opening up the port to a situation where multiple clients could connect to a single 802.1x port? In the Cisco world, the answer is multi-domain authentication. This is designed specifically for a VoIP phone. The port on the Cisco switch does MAC authentication for the VoIP phone, detects the LLDP on the phone, works with RADIUS responses from CPPM, and tags the port for the Voice VLAN. In conjunction with that, the DHCP server sends the phone specific VLAN instructions when it tries to connect on the default (untagged) VLAN of the port. Here is a breakdown of the process:

1. Switch port does a MAC authentication of the Phone, Phone must pass to go further
2. CPPM sends back information to the switch that this is a phone, to be handled specially (as not to cause a port violation, hence the multi-domain)
3. Phone attempts to connect to VLAN 0 (this just means no VLAN, untagged traffic)
4. Phone gets a DHCP response with the VLAN it should be on
5. Phone resets and attempts to connect to Voice VLAN
6. Again CPPM responds with information to the switch that this is a phone
7. Phone is allowed onto the Voice VLAN

This should all happen with minimal interruption to the computer plugged into phone. The computer will need to re-authenticate when the phone restarts after it has received the proper VLAN information from the DHCP server.

## Step 1: Additional Cisco Switch Configuration

Several additional settings need to be configured on the Cisco switch. First we need to enable LLDP and QoS for Voice. Here are the commands for that:

CPPM-Demo-3750(config)# mls qos

CPPM-Demo-3750(config)# lldp run

The next step is to configure the port to handle voice traffic on a different (tagged) VLAN. In the Cisco world, we do this without making the port a trunk port. The port remains in access mode but tags traffic for the voice VLAN. Here are the commands to set that up (keep in mind we created the voice VLAN 200 in the Cisco Switch document2):

CPPM-Demo-3750(config)# interface fastEthernet 1/0/24

CPPM-Demo-3750(config-if)# switchport voice vlan 200

CPPM-Demo-3750(config-if)# authentication host-mode multi-domain

CPPM-Demo-3750(config-if)# exit

One thing to note is the “authentication host-mode multi-domain” command. This command may differ on different Cisco switch models. On other switches, such as the 2960, the command may be the following: dot1x host-mode multi-domain. This “multi-domain” option allows us to MAC authenticate the phone on the same port as we 802.1x authenticate the computer.

## Step 2: DHCP Options for Avaya Phones

In my case, I am using an Aruba 3200 controller as a basic DHCP server (this is not recommended for production). In my DHCP scope for VLAN 333 (initial VLAN) and VLAN 200 (voice VLAN) I added the following options:

option 176 text "L2Q=1,L2QVLAN=200,VLANTEST=0"

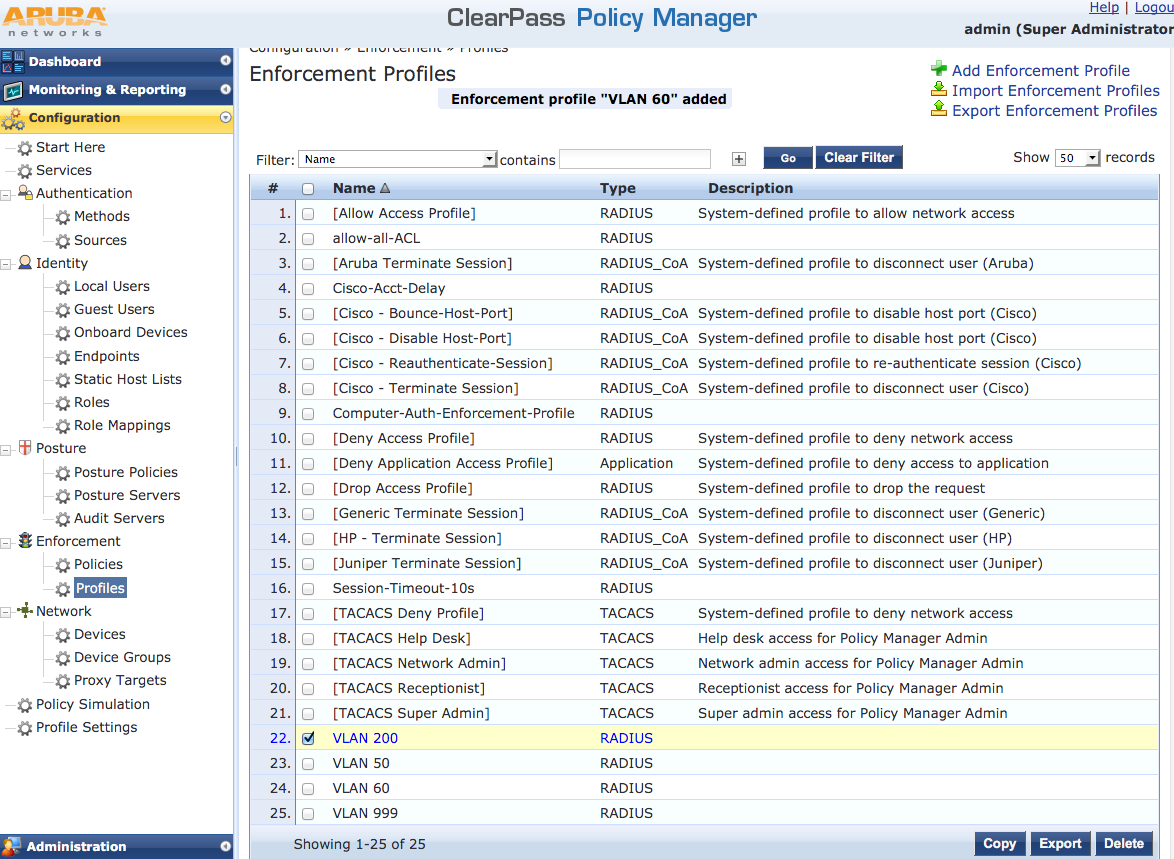
option 242 text "L2Q=1,L2QVLAN=200,VLANTEST=0"

Option 176 is used for most Avaya phones. Option 242 is used for the 9XXX series phones. L2QVLAN is the voice VLAN. Make sure you add these options to both VLANs that the phone will hit (initial VLAN then the voice VLAN).

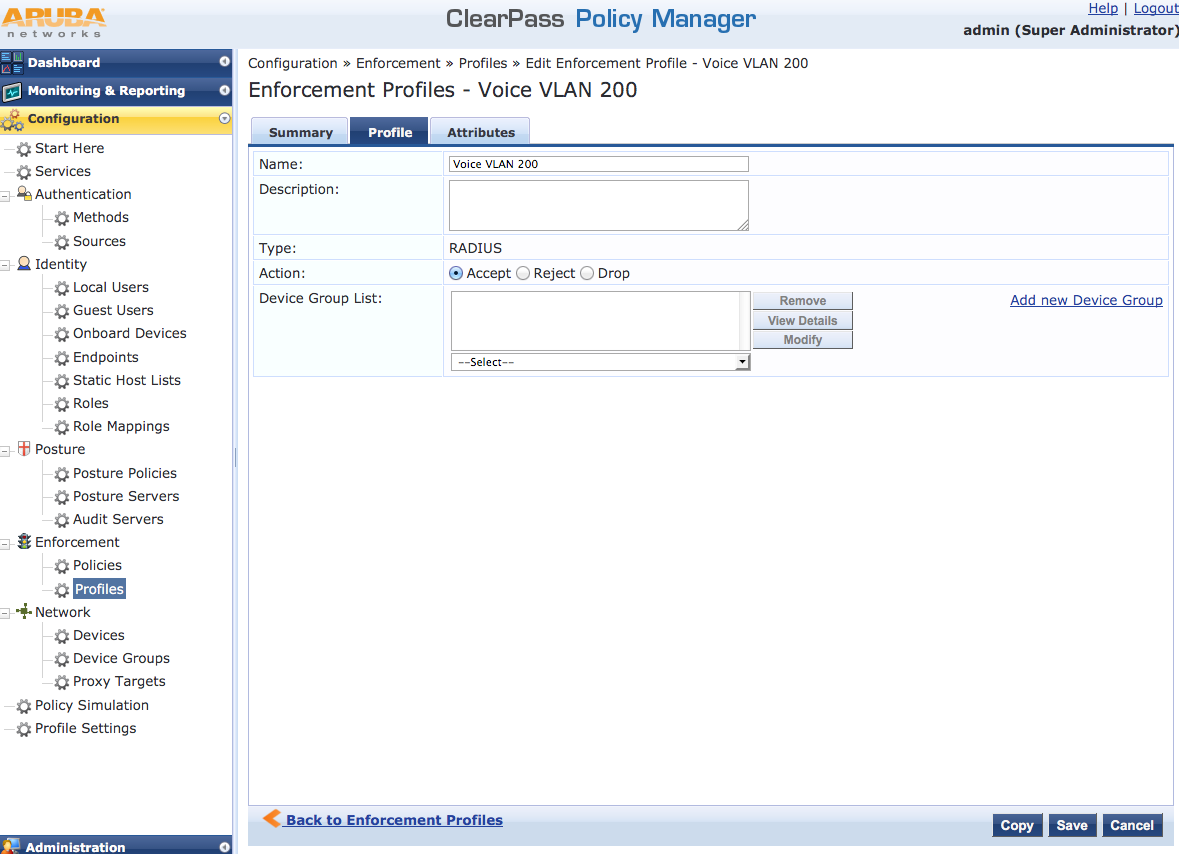
## Step 3: CPPM Service Configuration

The next step is to make some modifications to our services in CPPM. Specifically, we need to pass back information telling the switch to classify this device as a voice device. Along with that information, we need to pass back the voice VLAN, even though this information is on the switch.

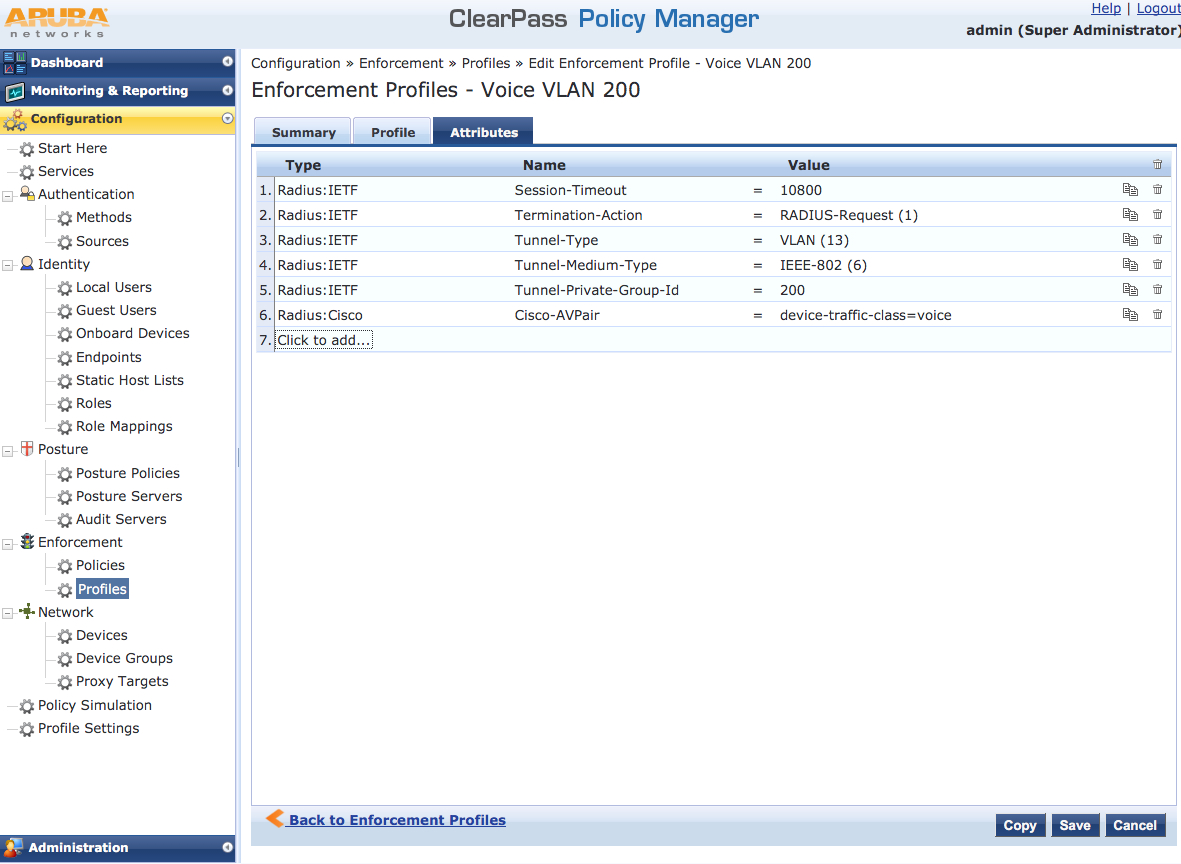
Let’s start by copying our VLAN 200 profile that we created in the Profile setup documentation. This is accomplished by clicking the box at the beginning of the line for VLAN 200:



Now click Copy. You should now see a new profile called Copy\_of\_VLAN 200. Select that profile to edit it. On the Profile tab, change the name to Voice VLAN 200. See image below:



Now click on the Attributes tab. Here we need to add a line that tells the switch that this is a Voice over IP phone. This is done with an additional RADIUS attribute that we will send back to the switch. Click on line 6 where it says “Click to add…” Choose Radius:Cisco for Type, Cisco-AVPair for Name, and enter “device-traffic-class=voice” without the quotes in the Value section. **REMEMBER:** you need to click the disk at the end of that line to save this new attribute! See image below for example:



Now click Save to save the new profile.

Now that we have created this profile, we need to apply it in several different places. We need the profile to apply both for MAC authentication (before and after being profiled) and for 802.1x (just in case there is a phone on the port where the 802.1x device is authenticating.