Certified Wireless Network Professional

CWNP

MARCH 9, 2016

ESSAY #3
SECURITY AROUND DEPLOYING A NEW WI-FI INFRASTRUCTURE

BY FRANÇOIS VERGÈS
CWNE APPLICANT

It took me quite some time and studies to grasp some security concepts used in Wi-Fi such as IEEE 802.1X. The CWSP book really helped me in this process. This is why I wanted to focus this last essay on security.

IT security is often defined by the three (3) following words: availability, integrity and confidentiality. I believe this can certainly be applied to Wi-Fi as well.

One of the VAR I work with started to deploy a new Cisco Wi-Fi infrastructure for one of their customer. The installation involved two (2) Cisco WLC 5508 in high availability and about a hundred (100) access points. They had physically installed the controllers but the high availability was not working. So my job was to fix the problem and configure all the other different pieces in order to integrate the new Wi-Fi infrastructure.

In this essay, I will talk about two (2) security aspects of this project:

- Troubleshooting and setting up high availability for the wireless controllers
- Implement a wireless local area network using WPA2-enterprise and IEEE 802.1X

High availability is great when it works but it can, sometimes, be tricky to setup. This is mainly due to the fact that there usually are some restrictions when using equipment in a HA mode. So before going onsite, I prepared a list of validations I needed to make on the cisco controllers in order to make sure we were on track. This list included things such as “validate the licensing”, “validate that the OS version matches on both units” and so on. I built my list according to the specifications and according to the information I had found on Cisco’s website. Before going on-site, I also prepared a HA configuration template I could use if I needed to re-configure everything from scratch.

Arriving on-site, I had a good plan that I could follow in order to troubleshoot the issue. Like any other network issues, I started my troubleshooting at layer 1 and moved up the OSI model. I also apply this principle for Wi-Fi issues. I am a big fan of starting troubleshooting a Wi-Fi issue looking at the spectrum.

Multiple network interfaces are used on a Cisco WLC 5508. An extra two (2) of them are used for HA (the ones outlined below):

- Management: main network interface
- Service: network management interface
- Virtual: used for mobility management, DHCP relay and embedded L3 security
- **Redundancy-management**: keep alive between the two (2) WLC units
- **Redundancy-port**: connects both HA WLC units and used for configuration and states synchronization

After validating the configurations and performing some troubleshooting, it turned out that the configurations on the switches were not completed. So I configured the switches and re-enabled HA on the Cisco WLC to fix the initial issue.

The part, I was most interested in, was the testing! Both controllers were supposed to exchange Wi-Fi client’s status and connections in order to maintain connection even if the active controller were to fail. So I configured a WLAN profile for testing purposes, connected a client to this Wi-Fi network and continuously pinged a IP address located on the wired network.

I then used the “**`redundancy force-switchover`**” command in order to trigger a manual switchover where the active WLC will reboot and the standby will take over. I lost one (1) ping in the process. I used the same command in order to revert back to the primary controller. When I reverted back, I didn’t lose any ping.

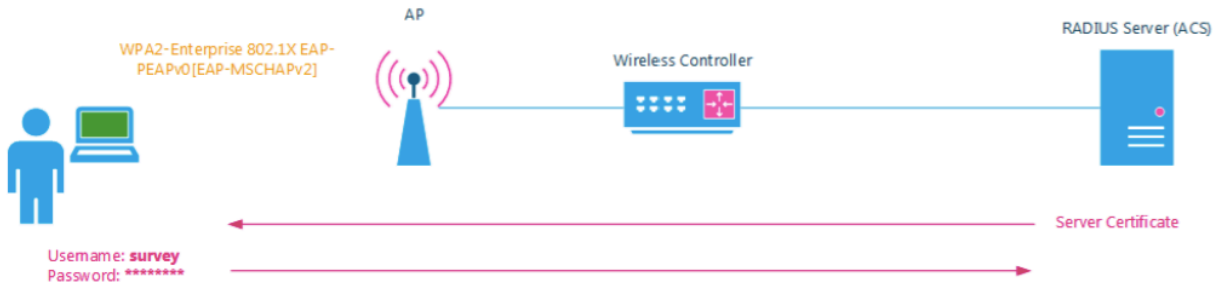
The client wanted to upgrade their Wi-Fi infrastructure because they were about to bring on VoIP devices and Automated Guided Vehicle. These new devices supported WPA2-Enterprise and IEEE 802.1X. This is great for security but the IEEE 802.1X authentication process can generate some delays while roaming especially for real time applications such as VoIP.

Thankfully, with my CWNP studies, I knew that some protocols were available in order to reduce these delays and help in the 802.1X authentication process while roaming. I was thinking about IEEE 802.11r Fast Transition (FT) Roaming, Opportunistic Key Caching (OKC), Pairwise Master Key Caching (PMK Caching) or Cisco Centralized Key Management (CCKM). These protocols can be very useful, but I have learned from the CWDP book that you always design a Wi-Fi network for the clients. So it was important to validate which client was compatible with which protocols.

In this case, we were able to use Cisco Centralized Key Management (CCKM), a Cisco proprietary protocol, with the VoIP phones and Automated Guided Vehicle (AGV). With CCKM, roaming delays are very short since there is no authentication nor 4-way handshake happening after the reassociation process.

Concerning the 802.11X authentication, the client was using a Cisco Access Control Server (ACS) as their Radius platform. The method of authentication chosen was PEAP[EAP-MSCHAPv2]. This was chosen because each device had an account in the active directory of the company and it was, therefore, more convenient.

With PEAP[EAP-MSCHAPv2] we still have a double authentication happening between the supplicant and the authentication server. This level of security was sufficient in this case. The Radius server is authenticated towards the client presenting a certificate and the client is authenticated toward the server presenting credentials:



Part of the work I had to do, was to perform a validation survey (or exit survey). Unfortunately, at the time of the validation survey, the VoIP had not been integrated yet so I could not test VoIP communications. However, I performed the exit survey carrying around one (1) of the new VoIP phone. I was able to validate the received signal strength indicator (RSSI) and compare it to whatever I would get on my surveying computer. This way, I was able to make sure that I had the proper coverage and that it was meeting all the requirements previously defined. Since then, the customer has been using VoIP on the new Wi-Fi network without any issues.

A Quality Of Service (QoS) "**Platinum**" has been configured on the Wireless Local Area Network (WLAN) profile used for the VoIP. This means that the Lightweight Access Point (LWAP) tunnel used for the VoIP SSID will be tagged with a Differential Service Code Point DSCP value of 46 (High Priority Expedited Forwarding or EF). This VoIP SSID will then be prioritized over the other SSIDs on the wired network between the APs and the wireless LAN controller.

Now what happens on the wireless side? The access point has to translate the DSCP of the LWAP tunnel into a IEEE 802.11e User Priority (UP) value. In our case here, the DSCP 46 is translated to an 802.11e UP of 6 (Voice or AC_VO). This tagging will ensure that the packet is prioritized to access the medium (RF) and therefore is transmitted faster. On a Cisco controller, under the 802.11a radio settings, I configured the Enhanced

Distributed Channel Access (EDCA) parameter to “Custom Voice”. This prioritizes voice traffic on the 5Ghz band (which was what we wanted in our case since the VoIP SSID was only enabled on the 5GHz band).

Apart from the security aspects of this project, I still had to used the Wi-Fi knowledge that I acquired from the CWNP program for things such as:

- Radio Frequency settings (Including transmit power, channel plan, the configuration of RRM)
- IEEE 802.11 settings (Data rates, advanced options)