Controller Lab

Eigil Obrestad

September 21, 2018

Introduction

This task set should introduce the student for controller-based configuration of Cisco wireless networks. For supporting litterature the chapters 9, 10, 11 and 15 of the CCNA:Wireless book is recommended. Cisco also publishes resources online [4] [5] [1] [3] [2].

Required infrastructure for all the labs are:

- A router (ex. Cisco 2901)
- A switch (ex. Cisco Catalyst 2960)
- 2 access points (ex. Cisco Aironet 1702i)
- A wireless controller (ex. Cisco 2504 WLC)

Passwords

Use only username/password cisco/cisco on switches/routers, and remember to clear the configuration when done!

The WLC's requires "complex" passwords. Use the username "admin" and the password "NTNUiG1" on the WLC.

1 Preliminary tasks

Use the result of LAB 1 as a base for this lab.

2 Initial WLC configuration

This task in intended to create an initial configuration for the WLC. It configures the base parametres, and helps to gain access to the web-interface and CLI of the WLC.

1. Connect the WLC to a trunk-port of the switch, where VLAN 11,12 and 13 is present. Set VLAN 11 as native.
2. Start the WLC, and run the initial configuration dialog.

- If LAG is enabled, all 4 ports of the WLC will work as a single aggregated port. Leave it disabled for now.
- When the management is the native VLAN at the switchport, should the management VLAN be tagged from the WLC, or not (untagged)?
- Use a RFC1918 IP address which is not in use anywhere else in your network as the virtual gateway IP address (ex. 192.168.255.254). It should be the same for all controllers in the same mobility group.
- The multicast IP used by the WLC is recommended to be in the range 239.0.0.0-239.255.255.255, which does not include 239.0.0.x and 239.128.0.x.
- Use 129.241.0.123 as NTP server

3. Log in to the controller's web-interface, and reconfigure the security parameters to use WPA2 with a PSK instead of the default 802.1x.

4. If for some reason the controller does not get its time and date set correctly, set it manually.

3 Controller discovery

Access points have multiple ways to discover the WLC. We are going to explore a couple of them in this task.

1. Connect an AP to VLAN 11 (Management), and observe the booting process including the joining of the controller. Verify that the AP appears in the controller, and that clients can connect to the SSID.

2. Connect another AP to VLAN 21 (AP network 1), and observe the boot process. Verify that the AP gets an IP address from a DHCP. Does it join the controller? Why/Why not? (Do not use the same AP as task 1)

3. Configure the DHCP server for VLAN 21 to send the WLC address to the AP's trough DHCP option 43. Verify that the AP in VLAN 21 now finds the WLC, and joins it. Verify that the AP appears in the controller webpage, and that clients can connect to the SSID.

4. Connect an AP to VLAN 22 (AP network 2), and verify that it cannot find the controller anymore. (If it finds the controller, it remembers the address from a previous attempt. Use the command "clear lwapp private-config" to force the AP to forget the controller. Use the command "sh capwap client config — i Configured Switchsh" to see which controller(s) the AP remembers.)

5. Reconfigure the router to send broadcasts from VLAN 22 as unicast to the controller, and make sure that broadcasts to the capwap ports also are sent. Make sure that the AP now can discover the controller, and connect to it. Verify that clients can join the WLAN.

6. The controller is equipped with two ports on the WLC which can provide PoE. Connect an AP to it (without the PoE injector which you use when AP's are connected to regular switches, of course), and verify that it boots. Which network does the AP appear on? Can it join the WLC?

7. Connect one AP directly to the WLC, and another to the switch in VLAN 21 or 22, and verify that both of them boots, and starts to broadcast their SSID. Enable "Cisco Clean Air" and give RRM some time to work, and verify that the AP's automatically selects different channels to operate on.

4 Expanding your WLAN

Currently a single SSID is broadcasted, and our clients can join. Now it is time to expand the network, by creating SSID's for employees and guests, and let them join these SSID's, and then appear in the correct VLAN's.

1. Create interfaces for the employee network, and the guest network, and configure them to be in the correct VLAN.

2. Create WLAN for the employee network, with WPA2+PSK as the security scheme. Enable it on both the 2.4GHz and 5GHz bands, but only for the OFDM modulations. Verify that the client can associate to it.

3. Create two WLAN's for the guest network. One for the 2.4GHz bands, and one for the 5 GHz band. Use no security scheme, and verify that a client can connect to them both.

4. Disable the WLAN that was configured during the initial controller configuration.

5 Clean up

1. Clear the configuration on all the equipment you have configured (WLC, Switch and Router).

2. Clean up cables etc.

References

[1] Cisco. *Cisco 2500 Series Wireless Controller Data Sheet*. http://www.cisco.com/c/en/us/products/collateral/wireless/2500-series-wireless-controllers/data_sheet_c78-645111.pdf. [Online; accessed 29-August-2018]. 2015.

[2] Cisco. *Cisco 2500 Series Wireless Controller Deployment Guide*. http://www.cisco.com/c/en/us/support/docs/wireless/2500-series-wireless-controllers/113034-2500-deploy-guide-00.html. [Online; accessed 29-August-2018]. 2015.

[3] Cisco. *Cisco 2500 Series Wireless Controller Getting Started Guide*. https://www.cisco.com/c/en/us/td/docs/wireless/controller/2500/quick/guide/ctr2504-qs.html. [Online; accessed 29-August-2018]. 2015.

[4] Cisco. *Cisco IOS Configuration Guide for Autonomous Cisco Aironet Access Points - Cisco IOS Release 15.3(3)JAB*. http://www.cisco.com/c/en/us/td/docs/wireless/access_point/15-3-3/configuration/guide/cg15-3-3.html. [Online; accessed 29-August-2018]. 2014.

[5] Cisco. *Data sheet - Cisco Aironet 1700 Series Access Point*. http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1700-series/datasheet-c78-732347.pdf. [Online; accessed 29-August-2018]. 2015.