## Wireless Controllers

Wireless controllers allow for a single point of management of wireless access points rather than managing them individually. In addition to allowing for a single point of management, many implementations have data traffic flowing through the wireless controller as well. Wireless controllers can take on many forms including cloud-based, built into access point(s), virtual controllers, and physical controllers. The type of controller we will be using in the lab is a physical controller. This controller has two data ports which will be configured as trunk ports to the 3560 Switch. Each of these ports can handle up to 48 Access Points each. We will not use the service port for this lab, however there are five different types of logical interfaces which are shown in *Appendix A*.

Hint: Plan out each of your VLANs, subnets, and connections before starting. This will make your time 10x more 'fun'. Please view *Appendix A* for the specifics on the wireless controller interfaces and VLANs before you get started. As always, ask for help if you need it!

Equipment

- 2x friends or new friends!
- 3x Bench PCs and a laptop
- Cisco 4402 Wireless Controller
- Cisco 3560 Switch
- 2x Cisco 1142 Access Points (APs)
- 2x matching SFPs (SFP-GE-S or GLC-LH-SM or SFP-GE-T) from the cage
- 2x Wireless USB dongles

Topology
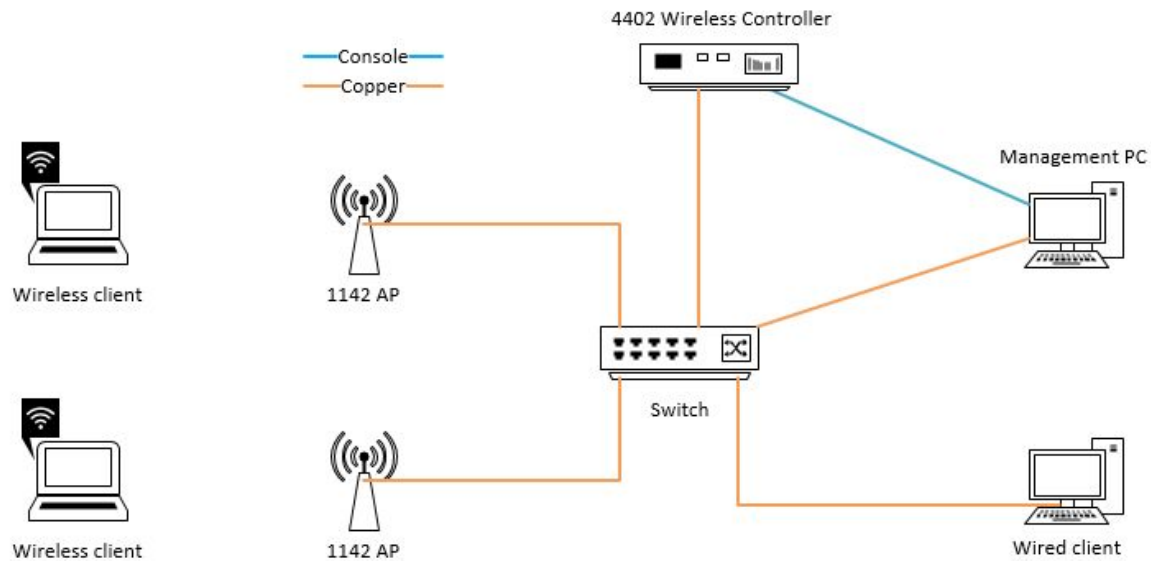
Switch setup
1. Console into your switch
2. Create a VLAN for: Management/ap-manager, and wired clients
3. Create a DHCP scope for: APs (ap-manager network/interface), and wired clients
4. Enable `ip routing`
5. Pause setting up your switch for now. We will come back to this later.

Controller Basic Setup
1. Console into the controller
2. Erase the current configuration and reboot
3. Configure IP addresses on the controller's *management* and *ap-manager* interfaces (these can be in the same subnet or in different subnets)
4. Connect your Management-PC to the Management network/VLAN
5. Browse to the IP of the controller's *management* interface (https) and login (admin:admin)

Controller and AP Setup
1. Once connected to the controller's web interface, browse around
2. Enable DHCP Proxy and DHCP option 82 for *ap-manager*
   a. `Controller menu > Interfaces > Edit`
   b. This allows the controller to act as a DHCP relay agent
3. Once you connect your APs to the switch, they should obtain an IP address in the same network as the controller's *ap-manager* interface
   a. If this does not occur, ensure the switchport is an access port for that VLAN
4. Check the summary page to see APs recognized by the controller
5. Configure the controller as a "Master Controller"

      a. `Controller menu > Advanced > Master Controller Mode >`
         `Check/apply`

6. Create a *dynamic* interface for your WLAN
    a. Tie the *dynamic* interface to a physical port on the controller
    b. Assign a VLAN and IP address
    c. Create this same VLAN on your switch, assign the VLAN interface a different IP address and create a DHCP scope for the WLAN
7. Create a new Wireless LAN profile with a new SSID (Under the WLANs menu)
    a. Enable this WLAN profile and configure WPA2-PSK
    b. In your WLAN profile, Advanced settings: set the DHCP server as the VLAN interface IP on your switch
8. Create an AP group and add APs to this group (note their MAC addresses)
    a. Tie the WLAN and AP group together
    b. Tie your WLAN to your *dynamic* interface
9. APs may need to be rebooted after this step
10. Configure the radios

WLAN clients
1. Connect to your SSID using a wireless dongle or your laptop
    a. Be careful: Cisco/Linksys USB adapters can use 5GHz frequencies while the Trendnet adapters are only 2.4GHz. Modify your WLAN profile and radios if you get stuck with the Trendnet adapter
2. Ping between your wired client and your wireless clients
3. If you made it this far see us for a pat on the back

Bonus
1. Integrate the pre configured VMs provided by an Eboard member
    a. Migrate DHCP from the switch to Windows
2. Create a 2nd WLAN Profile and SSID - this should be on a totally different network as well
3. Gain connectivity between both your WLANs and the wired network
4. Configure Internet access for your clients
5. Capture CAPWAP and LWAPP frames in Wireshark and investigate their purpose and operation

Appendix A - Controller interfaces
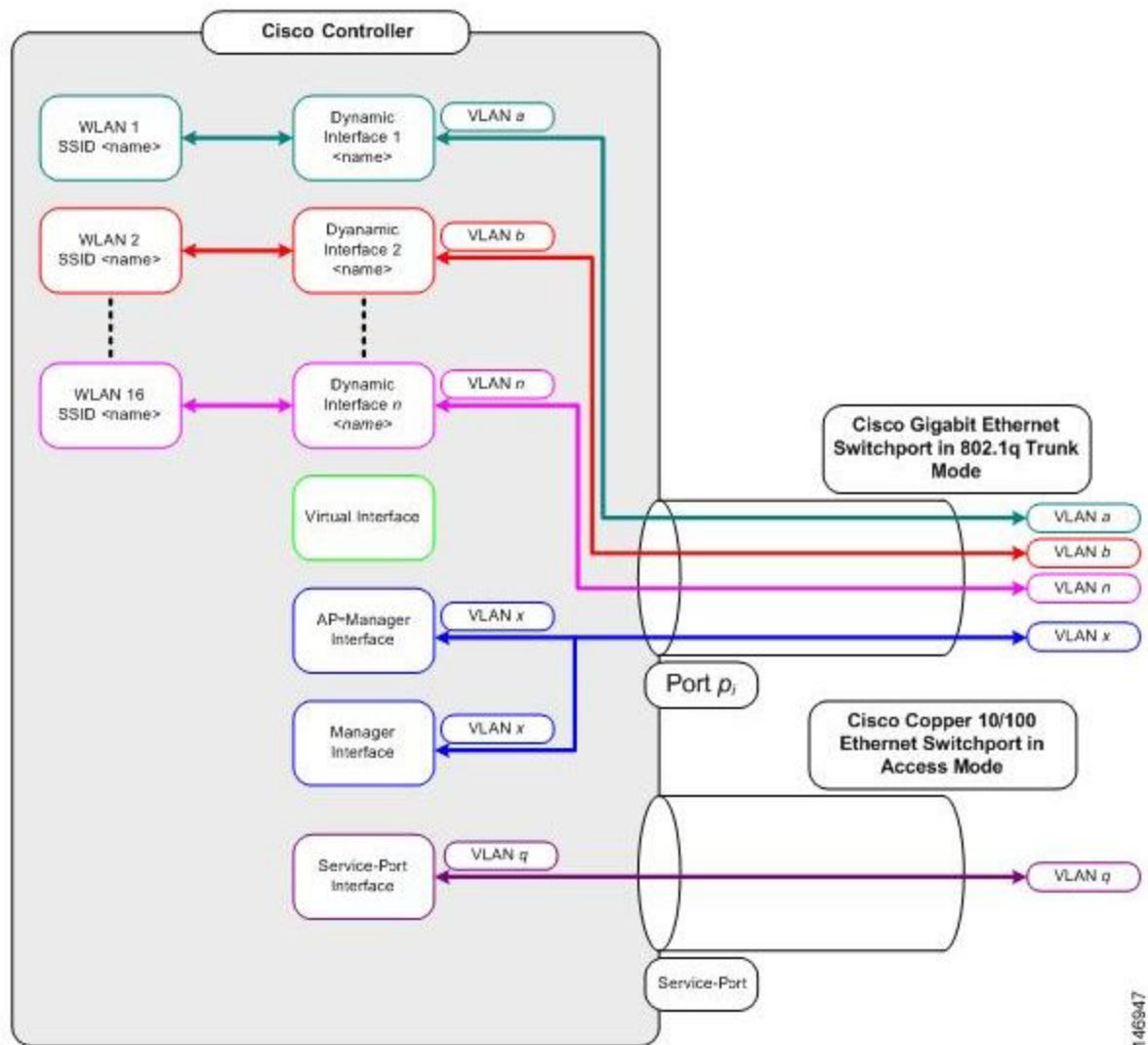
Appendix B - Controller configuration/setup

Step 1 Connect your computer to the controller using a DB-9 null-modem serial cable.

Step 2 Open a terminal emulator session.

1. Boot the controller. Watch the screen and when you see "Hit ESC for more boot options", hit ESC.
2. Select #5 – Clear Configuration and then allow the system to boot. It takes about one minute.
3. Answer [yes] to terminate the autoinstall.

Step 3 At the prompt, log into the CLI. The default username is *admin* and the default password is *admin*.

Step 4 If necessary, enter **reset system** to reboot the unit and start the wizard. [Not Necessary]

Step 5 The first wizard prompt is for the system name. [Not Necessary – the system may be pre-named]

Step 6 Enter an administrator username and password, each up to 24 printable ASCII characters. Username: admin Password: admin

Step 7 Enter the service-port interface IP configuration protocol: **none** or **DHCP**. If you do not want to use the service port or if you want to assign a static IP Address to the service port, enter **none**. Use [none].

Step 8 If you entered **none**, enter the service-port interface IP address and netmask on the next two lines. If you do not want to use the service port, enter a fictitious IP address that is not routable anywhere on your network. Ex. 1.1.1.B 255.0.0.0 where B is your bench number.

  If LAG comes up , answer NO

Step 9 Enter the management interface IP Address, netmask, default router IP address, and optional VLAN identifier (a valid VLAN identifier, or **0** for untagged). For the network use 192.168.B.0 255.255.255.0. Just make sure that the IP addresses used by the other team are different.

Step 10 Enter the Network Interface (Distribution System) Physical Port number. For the controller, the possible ports are 1 through 4 for a front panel GigE port. You should be using port 1.

Step 11 Enter the IP address of the default DHCP Server that will supply IP Addresses to clients, the management interface, and the service port interface if you use one. For DHCP, use the same address as the router. For the AP-Manager, use an IP address on the same network as the management interface.

Step 12 Enter the LWAPP Transport Mode, **LAYER2** or **LAYER3** (refer to the Layer 2 and Layer 3 LWAPP Operation chapter for an explanation of this setting). ***This step will not be part of our setup.***

Step 13 Enter the Virtual Gateway IP Address. This address can be any fictitious, unassigned IP address (such as 2.2.2.B where B is your bench number) to be used by Layer 3 Security and Mobility managers.

Step 14 Enter the Cisco WLAN Solution Mobility Group (RF group) name.

Step 15 Enter the WLAN 1 SSID, or network name. This is the default SSID that lightweight access points use to associate to a controller. Pick an SSID that you will all recognize.

Step 16 Allow or disallow Static IP Addresses for clients. Enter **yes** to allow clients to supply their own IP addresses. Enter **no** to require clients to request an IP Address from a DHCP server. Answer yes.

Step 17 If you need to configure a RADIUS Server, enter **yes**, and enter the RADIUS server IP address, the

communication port, and the shared secret. Answer no.

Step 18 Enter a country code for the unit. Enter **help** to list the supported countries or use US.

Step 19 Enable and disable support for 802.11b, 802.11a, and 802.11g. Say no to 802.11b/g

Step 20 Enable or disable radio resource management (RRM) (auto RF). Answer no. You may also say no to NTP and system time.

When you answer the last prompt, the controller saves the configuration and reboots with your changes.

Test your login by browsing to your controller using Internet Explorer. Use the management interface IP, the correct VLAN/port and https.

Appendix C - Management and AP-Manager interfaces

Management Interface

The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers. The management interface has the only consistently "pingable" in-band interface IP address on the controller. You can access the controller's GUI by entering the controller's management interface IP address in Internet Explorer's Address field. The management interface is also used for Layer 2 communications between the controller and Cisco 1000 series lightweight access points. It must be assigned to distribution system port 1 but can also be mapped to a backup port and can be assigned to WLANs if desired. It may be on the same VLAN or IP subnet as the AP-manager interface. However, the management interface can also communicate through the other distribution system ports as follows:

• Sends messages through the Layer 2 network to autodiscover and communicate with other controllers through all distribution system ports.

• Listens across the Layer 2 network for Cisco 1000 series lightweight access point LWAPP polling messages to autodiscover, associate to, and communicate with as many Cisco 1000 series lightweight access points as possible.

When LWAPP communications are set to Layer 2 (same subnet) mode, the controller requires one management interface to control all inter-controller and all controller-to-access point communications, regardless of the number of ports. When LWAPP communications are set to Layer 3 (different subnet) mode, the controller requires one management interface to control all inter-controller communications and one AP-manager interface to control all controller-to-access point communications, regardless of the number of ports.

AP-Manager Interface

A controller has one or more AP-manager interfaces, which are used for all Layer 3 communications between the controller and lightweight access points after the access points have joined the controller. The AP-manager IP address is used as the tunnel source for LWAPP packets from the controller to the access point and as the destination for LWAPP packets from the access point to the controller.
For Cisco 4404 and WiSM controllers, configure the AP-manager interface on all distribution system ports (1, 2, 3, and 4). For Cisco 4402 controllers, configure the AP-manager interface on distribution system ports 1 and 2. In both cases, the static (or permanent) AP-manager interface is always assigned to distribution system port 1 and given a unique IP address. Configuring the AP-manager interface on the same VLAN or IP subnet as the management interface results in optimum access point association, but it is not a requirement.

The AP-manager interface communicates through any distribution system port by listening across the Layer 3 or Layer 2 network for lightweight access point (LWAPP) join messages to associate and communicate with as many lightweight access points as possible.

Special thanks to Prof. Hartpence for his Wireless Controller Lab