WLAN ARCHITECTURES

There are two major approaches today for deploying WLAN Networks in the enterprise.

The two approaches have some basic philosophical differences which can have a major impact on deployment costs, security and manageability.

The first architecture to be presented is the so-called "Centralized" WLAN architecture. The Centralized architecture requires one or more servers or special purpose switches (Mobility controller) to be deployed in conjunction with wireless access points. By Default In the centralized approach, all wireless traffic is sent through the WLAN Switch. In either case, the centralized approach is considered to be an "Overlay" architecture. That is, it rides on top of the existing Ethernet Network.

Another approach is the "Distributed" WLAN architecture. AP have Built-in WLAN Security, layer 2 bridging, and access control features. Depending on the number of Aps required, Centralized management may be required. Distributed AP vendors may provide Centralized management tools or the AP's will act as Virtual Mobility Controller.

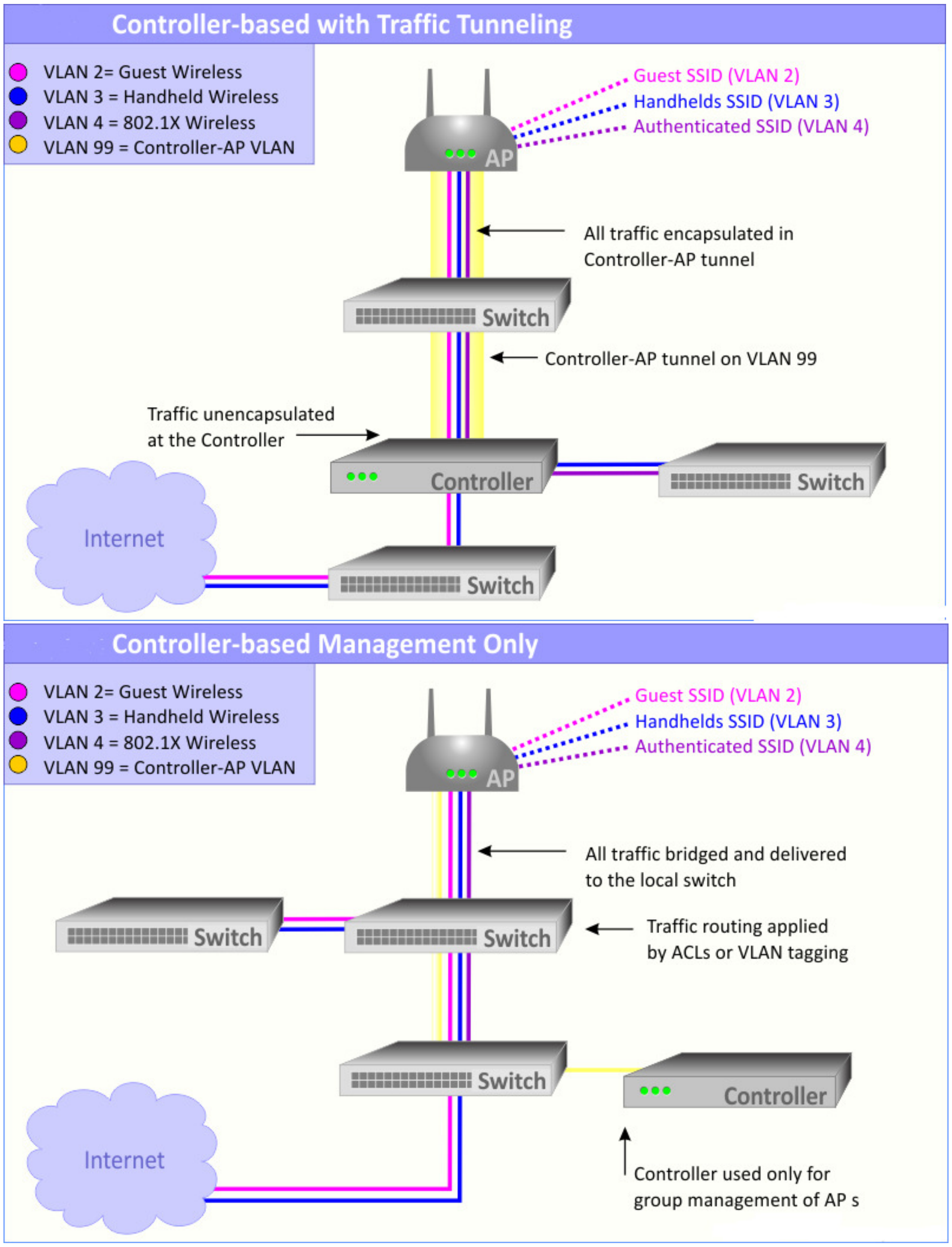
1. **Data Forwarding:**
   The "Distributed" WLAN architecture approach is that the wireless traffic load is literally distributed across the Aps and does not depend on a centralized element to process all of the wireless traffic.
   A "Centralized" WLAN architecture offers more choices, and thus more flexibility, than a "Distributed" WLAN architecture model. With a controller, organizations can choose to forward traffic locally at the APs (similar to the method used in "Distributed" WLAN architecture),
   Or they can choose to tunnel certain types of traffic back to the controller for security reasons.
   With a "Centralized" WLAN architecture organizations have the flexibility to mix and match these approaches as appropriate.

2. **Deployment Scenario:**
   In a "Distributed" WLAN architecture, you need to reconfigure your access layer with the addition of each new AP. Since it is necessary to configure all virtual LANs (VLANs) on the switch port that is needed by each new AP, your network administrator needs to configure the wiring closet switches that each new AP connects to. For example, you may have a VLAN for guest access, a VLAN for corporate access, and a VLAN for special access (such as VoIP). All these VLANs must be configured each time you add a new AP.

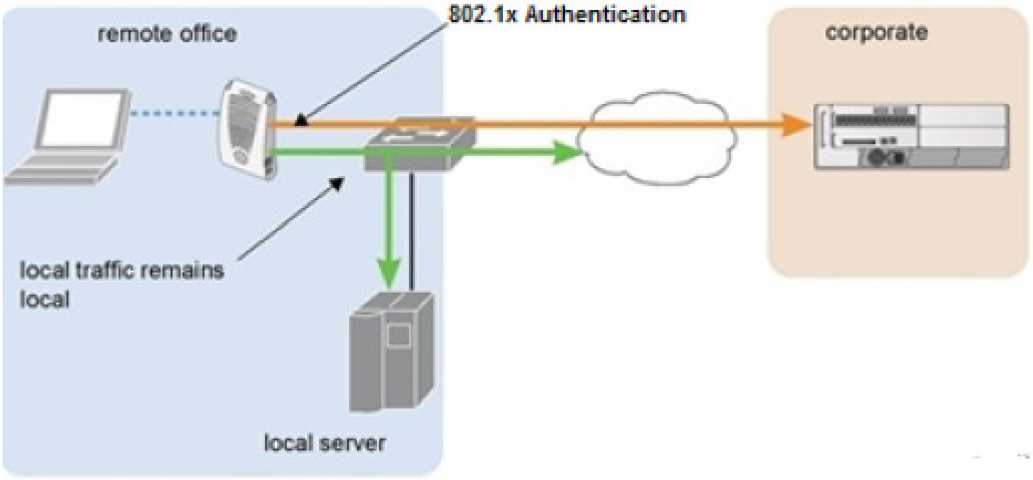
   With a "Centralized" WLAN architecture, it is infinitely easier to add Aps when we send traffic to controller with Tunnel mode. The access layer is configured once at the handoff to the controller and the system manages the rest. The centralized controller provides rich functionality for automating deployment complexity, eliminating the need for frequent, error-prone changes to the access layer. You simply plug in the AP and it automatically self-configures.

   Still if we required some AP to be configured for (bridge mode) sending traffic locally in "Centralized" WLAN architecture, those AP's it is necessary to configure all virtual LANs (VLANs) on the switch port that is needed.

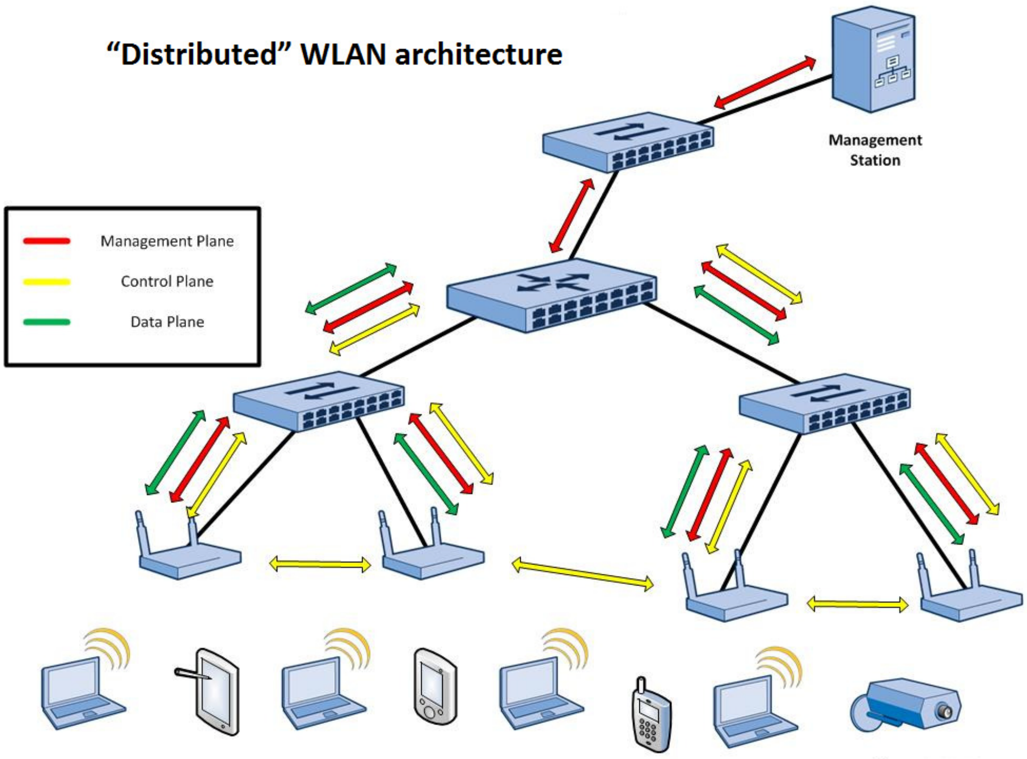
Reference Diagram as Below:


Controller-based with Traffic Tunneling
VLAN 2= Guest Wireless
VLAN 3 = Handheld Wireless
VLAN 4 = 802.1X Wireless
VLAN 99 = Controller-AP VLAN
Guest SSID (VLAN 2)
Handhelds SSID (VLAN 3)
Authenticated SSID (VLAN 4)
AP
All traffic encapsulated in Controller-AP tunnel
Switch
Controller-AP tunnel on VLAN 99
Traffic unencapsulated at the Controller
Controller
Switch
Internet
Switch
Controller-based Management Only
VLAN 2= Guest Wireless
VLAN 3 = Handheld Wireless
VLAN 4 = 802.1X Wireless
VLAN 99 = Controller-AP VLAN
Guest SSID (VLAN 2)
Handhelds SSID (VLAN 3)
Authenticated SSID (VLAN 4)
AP
All traffic bridged and delivered to the local switch
Switch
Switch
Traffic routing applied by ACLs or VLAN tagging
Switch
Controller
Internet
Controller used only for group management of AP s

Controller Based with AP in Bridge Environment



“Distributed” WLAN architecture


Management Station
Management Plane
Control Plane
Data Plane