Wi-Fi For Beginners Module 6

Wireless Control and Management

(Slide deck v2)

Introduction

Hello, my name's Nigel Bowden. Welcome to module 6 of the Wi-Fi for beginners podcast. This is a series of podcasts discussing the fundamentals of wireless LAN networking.

In each episode, we'll take a look at a different aspect of Wi-Fi to build your understanding and knowledge of wireless LAN networks.

Each episode is be accompanied by a set of slides describing the topics covered in that episode. Although you don't need to review these slides whilst listening to the podcast, they will be useful for reviewing the material we discuss and may provide some visual aids to more fully understand some of the concepts and equipment described.

All recordings and supporting material can be found at WiFiForBeginners.com

Aims of Podcast Series

- Present the fundamentals of Wi-Fi in a series of audio presentations
  - Hopefully in an easy-to-understand format
  - Useful to those on a daily commute, driving, running etc.
- Who is it aimed at?
  - Most likely IT professionals, students, people interested in career move
- Assumed knowledge:
  - Fundamentals of the 7 layer OSI model
  - Ethernet, switching and routing
  - IP addressing
  - Local Area Networks (LAN)
  - You have reviewed previous episodes! :)
- WiFi in commercial/professional environment - not home

Who Am I?

- Nigel Bowden
- UK Based
- IT Industry for 30+ years
- Specializing in Wireless LANs for 5+ years
- Industry certifications:
  - CWNP: Certified Wireless Network Expert (CWNE #135)
  - Cisco CCNP R&S
  - Cisco CCNP Wireless
  - Miscellaneous other vendor specific certs
- Roles: Design, Consultancy & Deployment of WLANs (mainly Cisco)
- Prolific social media participant:
  - @WiFiNigel (Twitter)
  - WiFiNigel.com (Blog)

In This Module

- The need for management & control (WLC)
- Reference model update
- Wireless LAN Controller History
- Control, Management & Data Planes
- What is a wireless LAN controller?
- WLC connectivity
  - Data plane paths
  - AP tunnels
- Other WLC functions
- Alternatives to WLCs
  - Pros and cons of various form-factors/implementations

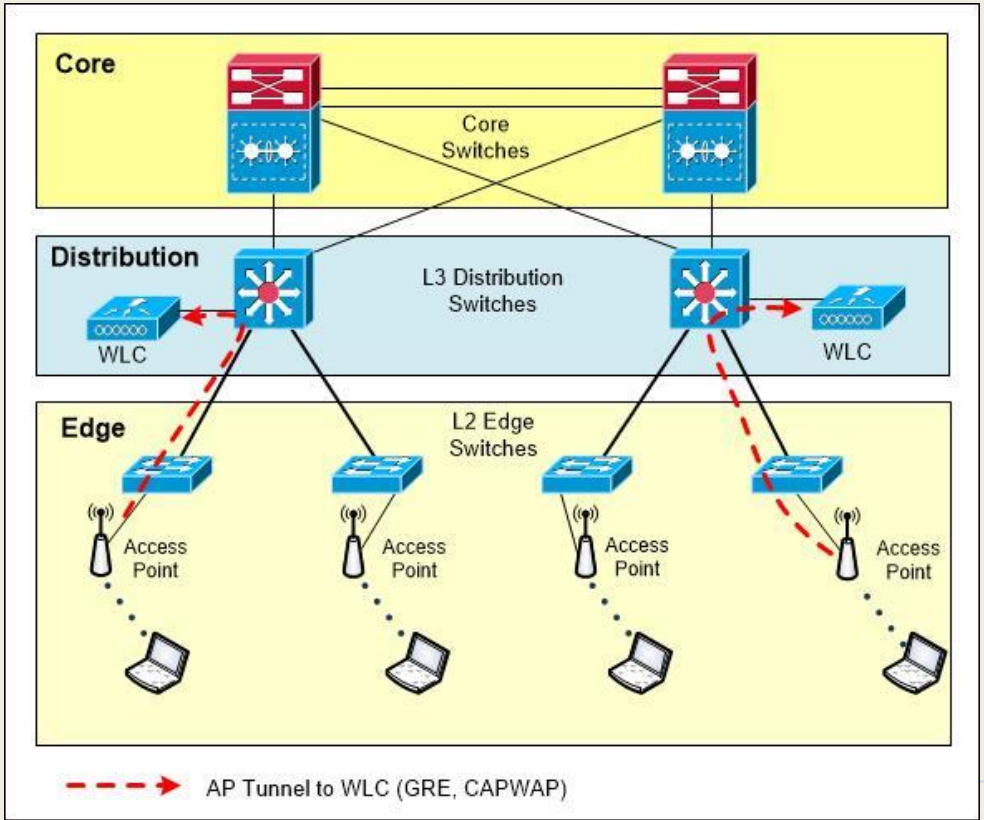
The Need For Control & Management

- Once we move beyond a handful of individual APs, managing them becomes very burdensome
  - time consuming
  - error-prone
- Need to replicate many aspects of the configuration:
  - SSID configurations
    - e.g. SSID name
  - Radio policy settings
    - e.g. bands, speeds supported
  - Security settings
    - e.g. authentication information, ACLs
- Only a centralised management technique can provide this

The Need For Control & Management

- Also, once we move beyond a handful of individual APs, there are many control functions (decisions) that may need to be coordinated
- Examples:
  - Channel assignments
    - auto-assignment to avoid co-channel interference with own APs and neighbouring APs
  - AP Power management
    - adjusting AP tx power to suit environment
  - Handling of roaming related functions
    - e.g. making encryption keys available to APs
  - Rogue detection & mitigation (WIPS)
- WLAN controller often (but not always) used for management & control

Reference Model - Update



Wireless LAN Controller History

- Brief history of wireless LAN controllers
- Early days of WLANs, APs provided in one or two areas of an organisation to provide convenience of wireless/mobile access
  - very small number of APs
  - easy to administer, low number users and traffic
  - little/no security
- Demand for wireless access grew, specialised equipment (e.g. hand scanners in warehouses, voice handsets in medical environments, some laptops)
  - more APs required but still small number of users, low data throughputs
  - security still minimal
  - starting to get more difficult to administer

Wireless LAN Controller History

- More widespread adoption of WLANs as became more commonplace in laptops.
  - Expectation of some mobility in Enterprise, medical, educational environments
  - Numbers of users growing
  - Security becoming a concern
  - More APs required as more coverage and more network throughput required
  - Trying to administer individual APs a major challenge
    - standardisation of configurations:
      - WLANs (SSIDs), security,
      - RF management
      - Channel planning

Wireless LAN Controller History

- Requirement for centralised management and coordinated control of access points and wireless users/clients
- Richer, co-ordinated set of services and features required
- Common administration point required as wireless networks grew to many hundreds or thousands of access points
- Wireless LAN controllers created to meet these requirements
  - instead of access points being standalone (“autonomous”), relied on WLC for their configuration settings
  - from single administration point, changes made to large numbers of APs in a few clicks on a web GUI
    - consistent policies easily & quickly applied across entire AP estate

Wireless LAN Controller History

- New breed of access points were created: “lightweight”
  - contained minimal code to get AP booted and on to network
  - AP forms (layer 3) connection back to wireless LAN controller once it has been powered on and has network connection
    - connection from AP to WLC generally some type of layer 3 tunnel (much like VPN tunnel) over which control, management and (optionally) user data flow between the AP and WLC
      - LWAPP, CAPWAP, GRE
  - WLC usually provides the operating configuration (and perhaps code) that the AP needs

Wireless LAN Controller History

- Earlier APs had been completely stand-alone
  - required each AP to be individually configured
  - held own operating code & config
  - no knowledge of other APs in same WLAN
  - no coordination of resources, RF, clients etc.
    - no control function across WLAN
    - very limited management
      - some basic management tools available
  - Known as “autonomous” APs
- Autonomous APs still available, but now used in very small networks or niche applications
  - e.g. bridge links

Wireless LAN Controller History

- WLCs were predominantly 19 inch hardware appliances that tended to be deployed at core of networks
- As demand for WLANs rose, smaller form factor WLCs emerged for branch applications
- With rise of virtualized services, WLCs became available as VMs to be deployed in existing virtualized environments
  - e.g. VMware, cloud hosted, cloud services
- As resources of AP hardware has increased, now have dual-function APs that can act as a WLC for a small number of APs

The Need For Control & Management

Decision making, co-ordination, signalling (e.g. co-ordination of AP channel assignments, co-ordination of client roaming (making keys available), client load balancing)

Administration and monitoring of devices (e.g. change configuration of devices using management system via SNMP, SSH etc,)

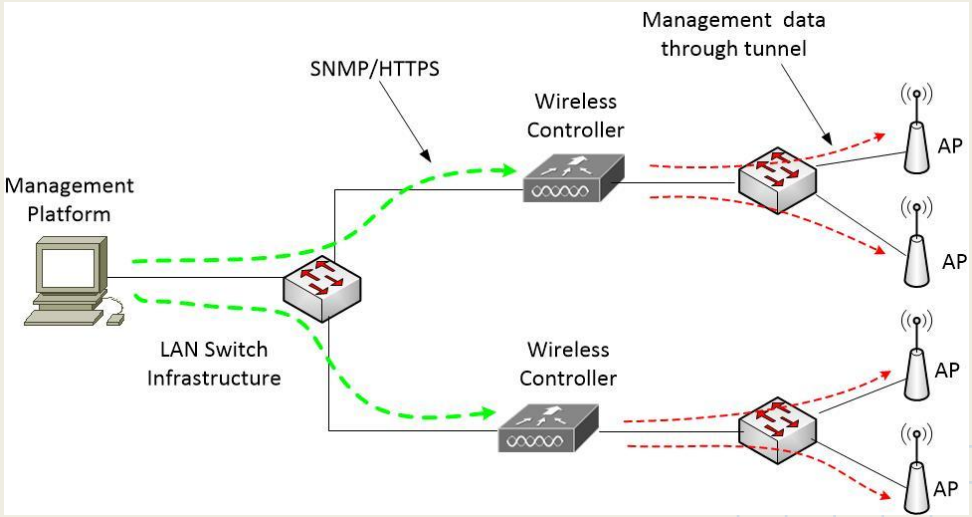
Path over which user data frames/packets flow (e.g. connection between AP & WLC, connection between AP and local edge switch)

Management Plane

- AP management may be provided by two methods:
  - central, dedicated network management system (NMS)
    - often uses SNMP protocol for management
    - may be on-premise or cloud management system
  - function of a wireless LAN controller (WLC)
    - management of APs only subset of WLCs function
      - NMS is dedicated only to management, WLC has control functions and also may be a data path for user traffic
- Management settings are static, fixed settings
  - e.g. SSID names, VLAN settings, supported 802.11 amendments, security methods, power settings, admin credentials
- The concept of the management function also known as the “Management Plane” of an 802.11 network.

Management Plane

- Management often performed via a combination of a dedicated management platform and WLCs
  - Mgt platform/service sends/gathers management data to/from WLC
  - WLC then acts as proxy to attached APs to forward/gather required data



Control Plane

- In addition to the management function, we also need a control function to provide dynamic services & change settings dynamically across the network, for example:
  - maintain client connections
  - adjust AP channels to changing conditions
  - change AP tx power settings to adapt to changing conditions
  - move security (encryption) keys around to facilitate roaming
- Control functionality known as “Control Plane” of wireless network
- Often a function provided in a “wireless LAN controller”
  - as WLC has global view of network, can make centralised decisions to enabled coordinated control activity:
  - e.g. AP channel planning: can see all neighbor reports from all APs to make channel planning decisions

Control Plane

- Centralized single WLC control is not the only option:
  - distributed control amongst APs (e.g. Aerohive)
    - “cooperative control” using network protocols
  - multiple WLCs across a WLAN infrastructure may exchange data to facilitate control decisions (e.g. cluster of WLCs on large campus)
- For anything beyond the most basic requirements, a WLC used by many manufacturers to centralize management and control
  - notable exception is Aerohive
    - Distributed (co-ordinated) control plane amongst APs
    - Uses set of protocols, analogous to routing protocols for routers

Data Plane

- Data plane is actual physical and logical path taken by user traffic
- Number of options in terms of implementation:
  - User data may be locally switched at AP
  - May travel to WLC and be centrally switched
- ...more later.

What is a wireless LAN controller?

Dedicated WLC Hardware

Virtualized/Cloud

Dual Role AP

Unified Access/Embedded

What is a Wireless LAN Controller?

- Number of form factors & implementations:
  - Traditional 19 inch hardware platform (1/2U)
    - Medium/Large Enterprise, Stadiums, high-end deployments
  - Smaller branch level hardware platform
    - SME/branch environments
  - Cloud-based
    - implementation hidden (hardware/VM), WLC service
    - Variable scale, mid-sized Enterprise down to SME level
    - Note: cloud based controller, not management platform

What is a Wireless LAN Controller?

- Number of form factors & implementations:
  - Virtualized
    - VM in DC instead of hardware platform
      - Variable scale (depending on resources available)
      - VMWare/Hyper V
    - Dual function APs
      - Acts as mini-WLC (limited number APs/clients)
      - Branch/SME scale
      - e.g. Aruba Instant, Cisco Mobility Express
      - Xirrus array (WLC with multiple radio modules)
    - Unified Access
      - WLC functionality built in to switch
      - Part of OS, native function of switch

What is a Wireless LAN Controller?

- Number of form factors & implementations:
  - Control function may be distributed amongst APs, in the case of Aerohive
    - No WLC required!

What is a Wireless LAN Controller?

- Model/architecture requirement for wireless controller (WLC) dependant upon
  - network size (e.g. number clients, number APs, throughput requirements)
  - Available vendor architecture
- Provides central coordination point for wireless network
  - Large number of APs difficult to configure and manage individually
  - Some functions of a WLAN require central coordination
    - AP channels being used
    - AP power settings
    - Roaming
    - Security

What is a Wireless LAN Controller?

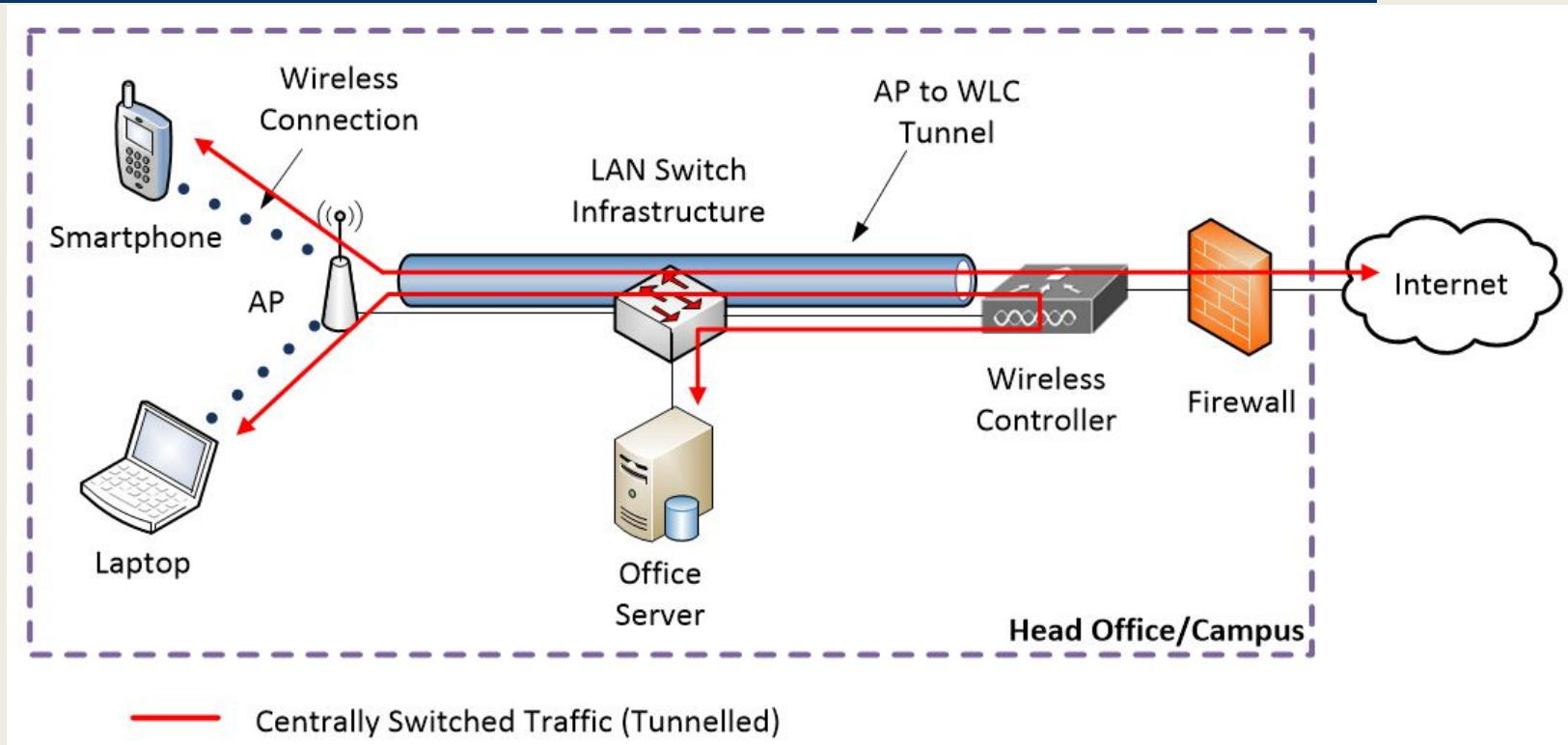
- Provides central coordination point for wireless network
  - Monitoring/management of APs centralized
  - Monitoring of clients centralized
  - Additional services that might be available from WLC:
    - Bonjour/Apple services
    - Traffic filtering
    - Rate limiting
    - Packet inspection/policy decisions
    - Gathering AP data for location services

Centralizing services/features *can* have great benefits depending on architecture & traffic flows

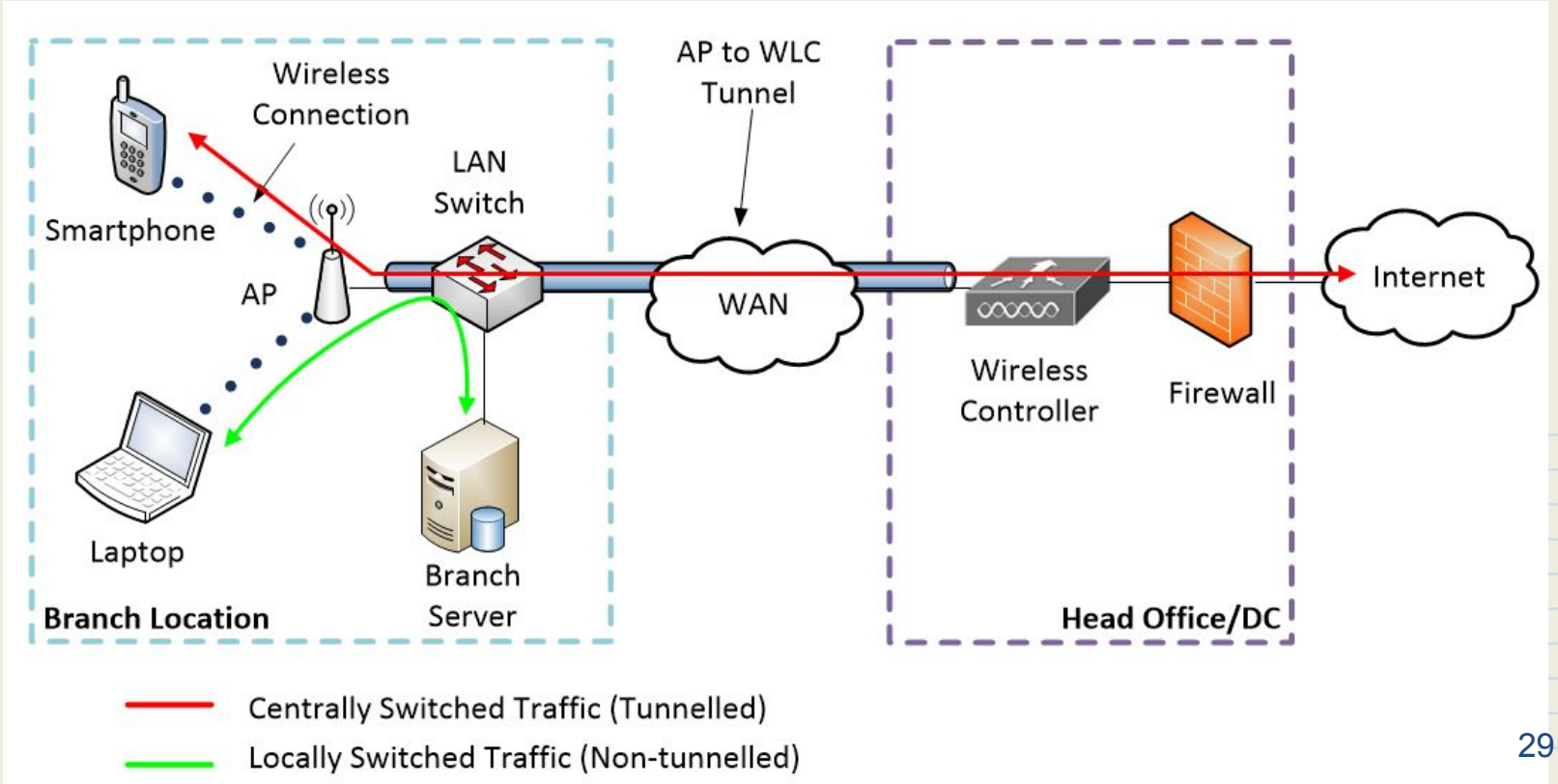
Wireless LAN Controller Connectivity

- How/where is WLC connected into the network?
  - will vary with size/topology of network
  - in large enterprises/campus, normally connected at the core/distribution of the network, often in DC
    - multiple GigEthernet, N-Base-T or TenGig trunk
  - branch environment:
    - small controller at each branch, or
    - large central WLC at DC with edge switched traffic
- AP connectivity to WLC
  - generally layer 3 connected - can be in different subnets
  - not physically connected in to front of WLC
    - form logical tunnel back to WLC, just need IP connectivity
      - LWAPP, CAPWAP, GRE

Wireless LAN Controller Connectivity (Data Plane) - Central Switching



Wireless LAN Controller Connectivity (Data Plane) - Central v Local Switching



Wireless LAN Controller Connectivity - AP Tunnels

- When using controller, APs build tunnel back to WLC
  - WLC cannot discover AP, AP has to “call home”
  - AP forms (layer 3) connection back to wireless LAN controller once it has been powered on and has network connection
    - finds it way to WLC using DHCP options, broadcast techniques and well known DNS names
  - connection from AP to WLC generally some type of layer 3 tunnel (much like VPN tunnel) over which control, management and (optionally) user data flow between the AP and WLC
    - LWAPP, CAPWAP, GRE
  - Once tunnel formed, often have a code download to sync with WLC, then user data flow once AP fully booted (can take a few minutes)
  - Once visible to WLC, can be managed from WLC (or NMS)

Data Plane Flows

- Client data flow known as “Data Plane”:
  - Management flows: “Management Plane”
    - e.g. static information: AP hostname, SSID, Security method etc.
  - Control flows: “Control Plane”
    - e.g. maintenance of client associations to AP, security keys availability during roams, co-ordination of channels
  - Client traffic flows: “Data Plane”
    - actual user/application data transported by wireless connection to wired network
- Centralizing data flows (“Data Plane”) allows in-line services such as application filtering, rate limiting, DHCP to be controlled from one point
  - easier to provision and manage, compared to edge provision of these services (i.e. must be done at AP or edge switch)

Data Plane Flows

- However, centralizing data flows has disadvantage:
  - all traffic sent to core, but may not need to go to core
  - bandwidth requirements at core for centralised traffic
    - WAN bandwidth considerations
- Due to advantages/disadvantages of centralized traffic flow, most WLC manufacturers provide two modes for data plane:
  - client traffic edge switched at AP: drops on to VLAN at AP on edge switch port
    - **Edge sw port must now be trunk**
  - client traffic centrally switched: client traffic travels all way from AP to controller and drops onto VLAN at WLC
  - in real-world deployments, may use combination of two:
    - guest traffic centrally switched
    - corporate traffic edge switched

Other Wireless LAN Controller Functions

- WLC provides opportunity to centralise number of services to wireless clients
  - Often easier than trying to provide or engineer at the edge:
    - RADIUS
    - DHCP
    - Security:
      - Firewall/ACLs
      - Wireless Intrusion detection system (WIDS)
- To centralise these services, for many of them the client data must also be centralised:
  - APs connect back to WLC over layer 3 tunnels (carrying client traffic)
  - Client traffic dropped on to VLAN at WLC

Other Wireless LAN Controller Functions

- In solutions that do not use a central controller (that is under your admin control):
  - Common services must be configured per AP or proxied by designate AP in a location
  - Requires higher admin overhead
    - Each AP has to be RADIUS client
    - Firewall/ACLs have to be configured per-AP
    - DHCP helpers need to be configured on wired LAN local to AP

Other Wireless LAN Controller Functions

- Guest portal
  - another common feature provided by WLCs
  - “coffee shop” WiFi experience
    - used to present web login page
    - guest users enter their credentials
      - self sign-up
      - maybe provided by reception staff
        - creation of guest accounts on WLC
      - open access
    - Web portal customised with organisation logos & colors
  - Portal may be hosted on the WLC itself or traffic may be re-directed to another guest management service

Other Wireless LAN Controller Functions

- Guest portal
  - Portal may be on dedicated on-premise server
    - separate application, not part of WLC function
  - Portal may be hosted on a cloud-based service
    - in addition to branded portal, may also offer content filtering
  - Portal may be hosted by 3rd party company (e.g. service provider) who will provide guest management as paid-for service

Other Wireless LAN Controller Functions

- WIPS
  - Wireless IPS/IDS (intrusion prevention/detection)
  - Built in to many WLC platforms
  - WIDS allows monitoring of “Rogue” devices
    - Other organisation nearby APs
    - Unauthorized APs on site or on corp network
  - WIPS allows proactive action to deny service to (“contain”) rogue devices
    - **Very** unadvisable to use containment for legal reasons

Other Wireless LAN Controller Functions

- Traffic inspection/marking
  - Inspection of traffic for specific applications & protocols
    - rate limiting
    - QoS marking
- Bonjour services (Apple)
  - WLC acts as gateway to Apple services, advertising available services on nominated VLANs
- Chromecast support

Alternatives to Wireless LAN Controllers

- Physical or virtualized WLCs in data centres or wiring closets not the only option
- WLCs may be in the cloud, embedded in other devices or not required at all
  - still used in large number of deployments
- Pros:
  - Easy to understand, easy to administer network from one central entity
  - Global view of the WLAN very useful for making control decisions
- Cons:
  - Single point of failure (HA may be used, but is additional cost)
  - Ongoing support, updating software
  - Possible licensing impact

Alternatives to Wireless LAN Controllers

- Alternatives:
  - Cloud controller
    - the management and control function still provided by a WLC, but is provided as a service (e.g. Meraki)
    - APs all need to have Internet access to talk to the controller
    - easy to use web GUI available to manage entire AP estate as long as you have an Internet connection

Alternatives to Wireless LAN Controllers

- Alternatives:
  - Cloud controller
    - disadvantages:
      - if lose Internet connection: no AP management, reduced features
      - security
        - admin access to network from anywhere
        - control/mgt data which passes to service provider
    - advantages:
      - no controller installation, maintenance
      - convenience of admin access from anywhere
      - No ongoing hardware support challenges
      - Opex cost rather than CapEx cost

Alternatives to Wireless LAN Controllers

- Alternatives:
  - Cooperative control (Aerohive)
    - No controller required
    - APs use cooperative protocols to make all control decisions and exchange control data
    - Still requires centralised management to push out config, software etc.
      - may be cloud-based management, or on-site appliance
    - Advantages:
      - no controller costs (licensing, power, hardware)
    - Disadvantages (arguably):
      - complexity of configuration?

Alternatives to Wireless LAN Controllers

- Alternatives:
  - Dual Function APs
    - Often used for smaller sites/branches
    - One AP is nominated as controller (other APs may be standby)
    - Advantages:
      - Controller failure impact limited to one site/area
      - Scalable, easy to deploy for orgs with many small sites
      - Keep control (& some management) traffic off WAN
    - Disadvantages:
      - Larger estate of controllers to manage
      - “Controller” AP limited in number of APs it can manage
      - May have a subset of functions of full, dedicated WLC platform

Summary

- The need for management & control (WLC)
- Reference model update
- Wireless LAN Controller History
- Control, Management & Data Planes
- What is a wireless LAN controller?
- WLC connectivity
  - Data plane paths
  - AP tunnels
- Other WLC functions
- Alternatives to WLCs
  - Pros and cons of various form-factors/implementations