Cisco Unified Wireless Network Administration: VLAN and WLAN Administration
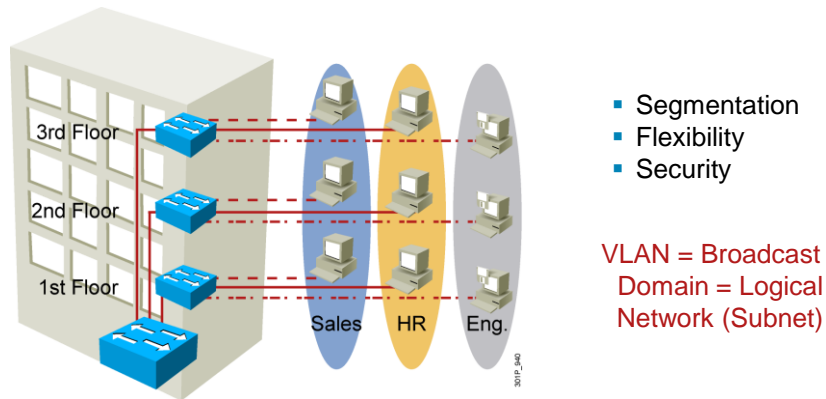
Lesson Overview & Objectives

- **Overview** –This lesson provides a detailed overview of incorporating and managing VLANs in a Cisco Unified Wireless Network environment. The lesson also provides detailed instructions on wireless LAN (WLAN) administration in a Cisco Unified Wireless Network environment.

- **Objectives** - Upon completing this lesson, you will be able to understand VLANs as required to support the CUWN environment. You also will be able to establish WLANs as required for effective CUWN administration. This ability includes being able to meet these objectives:

  – Identify and explain the purpose of VLANS

  – Explain the purpose of VLANs on the controller

  – List the VLAN recommendations for the controllers

  – Explain the purpose and administration of Wireless LANs

  – Summarize the purpose of AP Groups and its configuration

Virtual Local Area Networks

- Segmentation
- Flexibility
- Security

VLAN = Broadcast Domain = Logical Network (Subnet)

- A VLAN permits a group of network devices to share a common broadcast domain (subnet) regardless of their physical location on the network.
- Requires a router to allow connectivity between VLANs.
- VLANs will have different subnetwork or network IP addresses.
- Cisco WLCs support up to 512 VLANs.

Access Links and Trunk Links
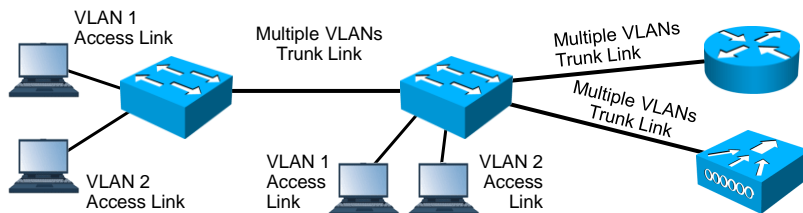
- In a VLAN-based network, network links may carry traffic for a single VLAN or multiple VLANs may share a single physical link.
- IEEE 802.1Q specification defines how each Ethernet frame for each VLAN on a trunk link can be tagged with a VLAN identifier.
- On an 802.1Q trunk link, the traffic for one VLAN—the "native VLAN" will not be tagged. Any untagged traffic is assumed to belong to the native VLAN.

VLANs on the Controller

- Each interface (except the Virtual Interface) on the controller will be associated with one VLAN ID on one DS Port.
- Multiple VLAN IDs (including 0 for the native VLAN) will exist on a trunked link.
- The VLAN ID will always be 0 on an access link.
- The WLAN controllers can support up to 512 VLANs on a single distribution port.
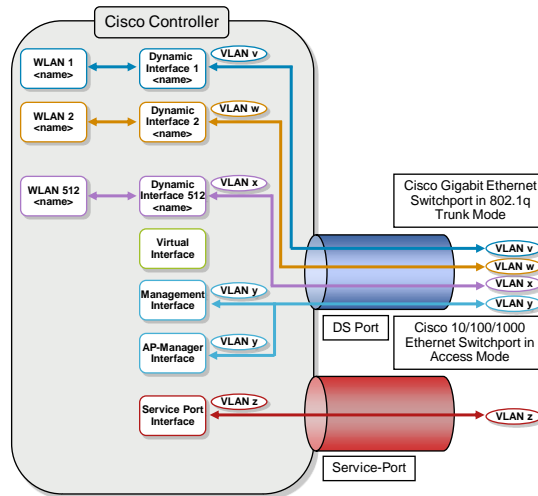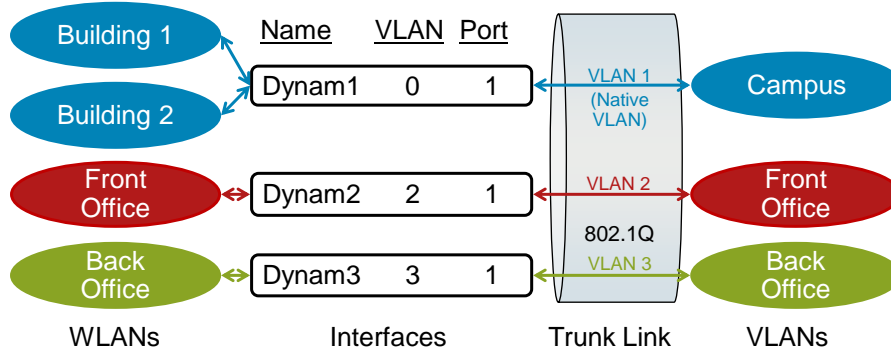
CUWN v7.0—3-5

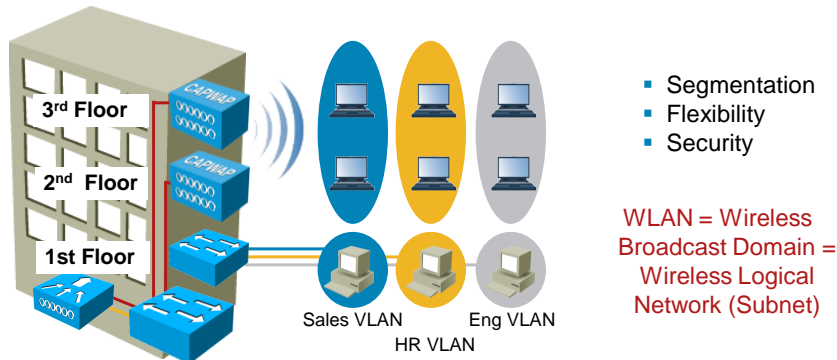# VLAN Recommendations for the Controllers

- Use 802.1Q trunks to carry multiple VLANs from the Ethernet switch to the controller distribution system ports.
- Configure the Ethernet switch trunk ports to allow only the VLANs that are used by the controller interfaces.
- Remember that the native VLAN on an 802.1Q trunk is untagged, and the single VLAN on an access link is untagged—use VLAN ID 0 for either.

CUWN v7.0—3-6

Wireless Local Area Networks

3rd Floor
2nd Floor
1st Floor

Sales VLAN
HR VLAN
Eng VLAN

- Segmentation
- Flexibility
- Security

WLAN = Wireless Broadcast Domain = Wireless Logical Network (Subnet)

- A WLAN permits a group of wireless network clients to share a common wireless domain.
- A single WLAN usually ties to a single VLAN, but may tie to multiple VLANs.
- Multiple WLANs may tie to a single VLAN.
- WLANs usually have different subnetwork or network IP addresses.

WLAN Traffic Flow—WLAN to VLAN

- Each WLAN has an associated identifier (SSID). When stations want to join a WLAN, they identify their desired WLAN by its SSID.
  - As a result, the SSID is often thought of as the WLAN name.
- Lightweight access points pass traffic for each WLAN (identified by SSID) from the wireless clients over a wired (CAPWAP) tunnel back to a Cisco WLC.
- The wireless LAN controller uses the management, AP-manager, or dynamic interfaces to map the client traffic from a WLAN to a corresponding VLAN on the wired network infrastructure.
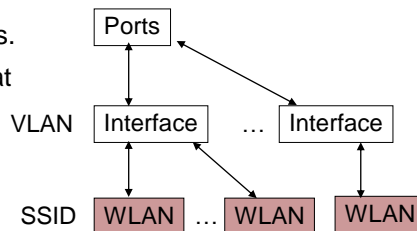

CAPWAP Tunnel

VLAN 5

SSID: Staff

VLAN5
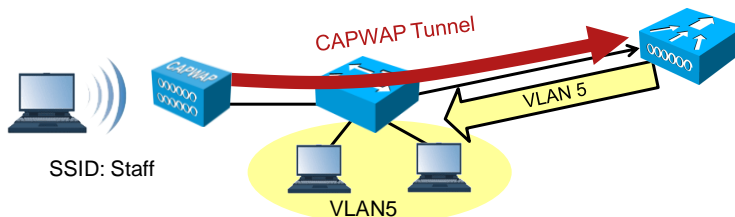
WLANs on the Controller

- Cisco wireless uses the WLAN configuration to associate a SSID to an interface.
  - Multiple WLANs can be assigned to an interface.
  - If Allow AAA Override is enabled, the VLAN for the client traffic may be dynamically assigned by an authorization value (IBN).
- WLAN configuration will also define the security policies that will be applied to the group of WLAN clients.
- Controllers running version 5.2 or later will support 512 WLANs.
  - Only 16 WLANs are active at one time on an AP.

Ports

VLAN   Interface   ...   Interface

SSID   WLAN   ...   WLAN   WLAN

WLAN Administration

cisco   MONITOR   WLANs   CONTROLLER   WIRELESS   SECURITY   MANAGEMENT   COMMANDS   HELP   FEEDBACK

WLANs

WLANs   WLANs   Entries 1 - 3 of 3

▼ WLANs
  WLANs
▼ Advanced
  AP Groups

Current Filter: None   [Change Filter] [Clear Filter]   Create New ▾ Go

Create New
Disable Selected
Enable Selected
Remove Selected

	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
☐	1	WLAN	secure8	secure8	Enabled	[WPA2][Auth(802.1X)]
☐	2	WLAN	open7	open7	Enabled	None
☐	8	WLAN	secure8x	secure8x	Enabled	802.1X

Remove
Mobility
Anchors

A WLAN will default to security policy of [WPA2][Auth(802.1X)] to secure WLAN access.

1. From **WLANs>WLANs**, you can view the existing WLANs on the controller.
2. Use the drop-down box to create new WLANs, enable or disable WLANs, and remove WLANs.
3. Select the WLAN ID to edit an existing WLAN.

Filtering the WLAN List

- Select **Change Filter** to filter the WLAN list results.
- From the filter menu, you can search for WLANs that match a particular profile name, SSID, or are at a particular status (enabled or disabled).

WLANs–General Configuration Tab

At the General configuration tab:
- Enable or disable the WLAN
- Define which radios the WLAN will support
- Associate the WLAN to a Dynamic Interface
- Enable or disable SSID broadcasting

WLANs—Advanced

General	Security	QoS	**Advanced**

Allow AAA Override   ☐ Enabled

Coverage Hole Detection   ☑ Enabled

Enable Session Timeout   ☑ 1800
         Session Timeout (secs)

Aironet IE   ☑ Enabled

Diagnostic Channel   ☐ Enabled

IPv6 Enable [7]   ☐

Override Interface ACL   None ▾

P2P Blocking Action   Disabled ▾

Client Exclusion [3]   ☑ Enabled 60
         Timeout Value (secs)

Off Channel Scanning Defer

Scan Defer Priority   0 1 2 3 4 5 6 7
     ☐ ☐ ☐ ☐ ☑ ☑ ☑ ☐

Scan Defer Time(msecs)   100

HREAP

H-REAP Local Switching [2]   ☐ Enabled

Learn Client IP Address [5]   ☑ Enabled

DHCP

DHCP Server   ☐ Override

DHCP Addr. Assignment   ☐ Required

Management Frame Protection (MFP)

MFP Client Protection [4]   Optional ▾

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)   1

802.11b/g/n (1 - 255)   1

NAC

State   ☐ Enabled

Load Balancing and Band Select

Client Load Balancing   ☐

Client Band Select [8]   ☐

Passive Client

Passive Client   ☐

Voice

Media Session Snooping   ☐ Enabled

Re-anchor Roamed Voice Clients   ☐ Enabled

AP Groups—WLANs vs. VLANs

- APs provide a common WLAN (SSID) across the enterprise.
- APs are clustered together based on AP group name.
- Mapping ties each AP group WLAN or WLANs to differing VLAN interfaces.

AP Group 1
VLAN 1

WLAN1

AP Group 2
VLAN 2
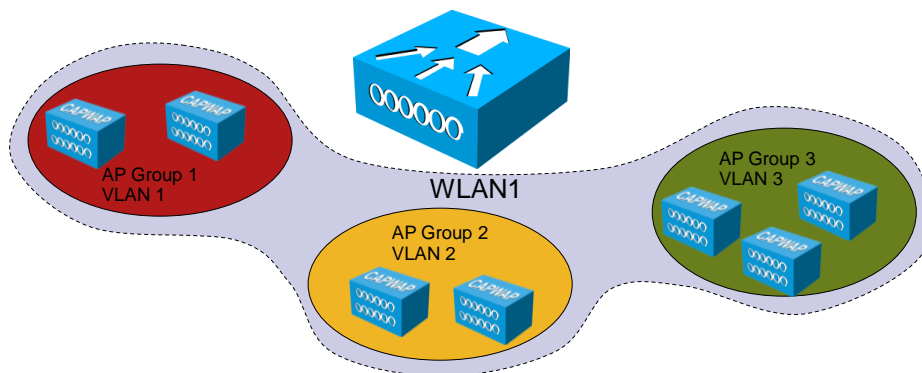
AP Group 3
VLAN 3

AP Groups VLAN Effect

- Allows usage of a single SSID over the entire infrastructure.

- Client 1, when associating with an AP in Building 1, will be placed on VLAN 1 and receive an appropriate IP address.

- Client 2, while associating to the same WLAN in Building 2, will be placed on VLAN 2 and receive an IP address from a different network or subnetwork.

- If Client 1 were to disassociate from the APs in Building 1 and move from Building 1 to Building 2, it would also be put on VLAN 2 because it moved to another AP group VLAN.
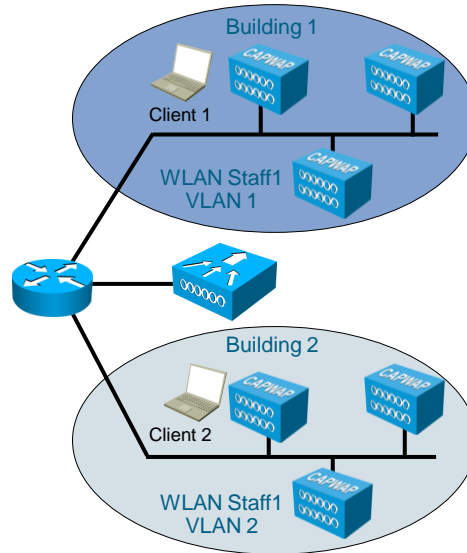
Creating AP Groups

1. To create new AP groups, go to **WLANs>Advanced>AP Groups.**
2. Select **Add Group**.
3. Give the new AP group a name and description.

Configuring AP Groups—
WLAN-to-Interface Mapping

- Click on an AP Group Name to edit the group.
- Under the WLAN tab, create the WLAN-to-Interface mappings that are specific for the AP group.
- Each AP group can have up to 16 WLANs (and interfaces) defined.

Configuring AP Groups—
The Default-Group AP Group

- All controllers running 5.2 or later will have the "default-group" AP group created automatically.
- All APs are automatically assigned to the default-group.
- WLANs with ID 1 through 16 will always belong to the default group.
- Accommodates transparent upgrades for existing deployments.
- The default-group WLANs can not be modified; it will always contain the first 16 WLANs (by WLAN ID).

Configuring AP Groups—Assigning APs to an AP Group

Ap Groups > Edit 'Building1'   < Back

| General | WLANs | APs |

APs currently in the Group   [Remove APs]   Add APs to the Group *   [Add APs]

☐ AP Name   Base Radio Mac   ☐ AP Name   Group Name

☐ AP23   00:1d:a1:cc:0b:a0   ☐ AP21   default-group
                                         ☐ AP22   default-group

Foot Notes
1 Changing AP Group requires AP restart

In **AP Group Configuration**, select the **APs** tab to add associated APs to the group.

or

All APs > Details for AP23   < Back   Apply

| General | Credentials | Interfaces | High Availability | Inventory | Advanced |

In **AP Configuration**, select the **Advanced** tab to assign an associated AP to an AP group.

Regulatory Domains   802.11bg:-A   802.11a:-A   **Power Over Ethernet Settings**
Country Code   US (United States) ▾   Pre-Standard State   ☑
Mirror Mode   Disable ▾   Power Injector State   ☐
Cisco Discovery Protocol ☑   **AP Core Dump**
MFP Frame Validation   ☑ (Global MFP Disabled)
AP Group Name   Building1 ▾   AP Core Dump   ☐ Enabled
Statistics Timer   default-group
Rogue Detection   ☑ Building1

© 2010 Cisco Systems, Inc. All rights reserved.

CUWN v7.0—3-21

AP Groups—Details

- May affect roaming characteristics.
  - Roaming between APs on same Controller will keep the same VLAN and be treated as a Layer 2 event.
    - Configure all WLAN overrides (WLAN-to-Interface mappings) consistently across APs if a lot of roaming between APs is expected.
  - Roaming between APs on different Controllers will be handled as normal roaming event, Layer 2 or Layer 3.
- Each AP can only be mapped to a single AP group name.

© 2010 Cisco Systems, Inc. All rights reserved.   CUWN v7.0—3-22

Summary

- VLANs allow multiple subnets to share a physical network infrastructure.
- Each interface on the controller will be associated with one VLAN ID on one DS Port.
- Consider the VLAN recommendations for the controllers.
- WLANs permit a group of wireless network clients to share a common wireless domain.
- AP Groups allow the administrator to create these new mappings.