



# D-Link Certified Professional

[DWS-4026]

Version 1.0



**D-Link®**



## Course Outline

- Introduction to D-Link Unified Access System
- Unified System Deployment
- Unified System Usage
- Lab 1: Unified Switch Redundancy
- Working Principles of Basic Functions
- Lab 2: Advance Management
- New Functions Implementation (DWS-4026/DWL-8600AP)
- Lab 3: Cluster Controller
- Command Line Interface
- System Maintenance and Troubleshooting
- Lab 4: CLI and Dynamic VLAN Assignment



Session 1

# Introduction to Unified Access System



### **Session 1: Introduction to Unified Access System**

- Introduction
- Hardware Basis
- Working Concept





# Introduction

- D-Link Unified Access System is an integrated wired/wireless solution which provides:
  - Centralized management
  - Secure wireless connectivity
  - Seamless layer 2 and layer 3 wireless roaming
  - Automatic RF adjustment
  - Comprehensive statistics and report
  - Visualization management tool
- Users can easily deploy and manage their wireless network with this solution.

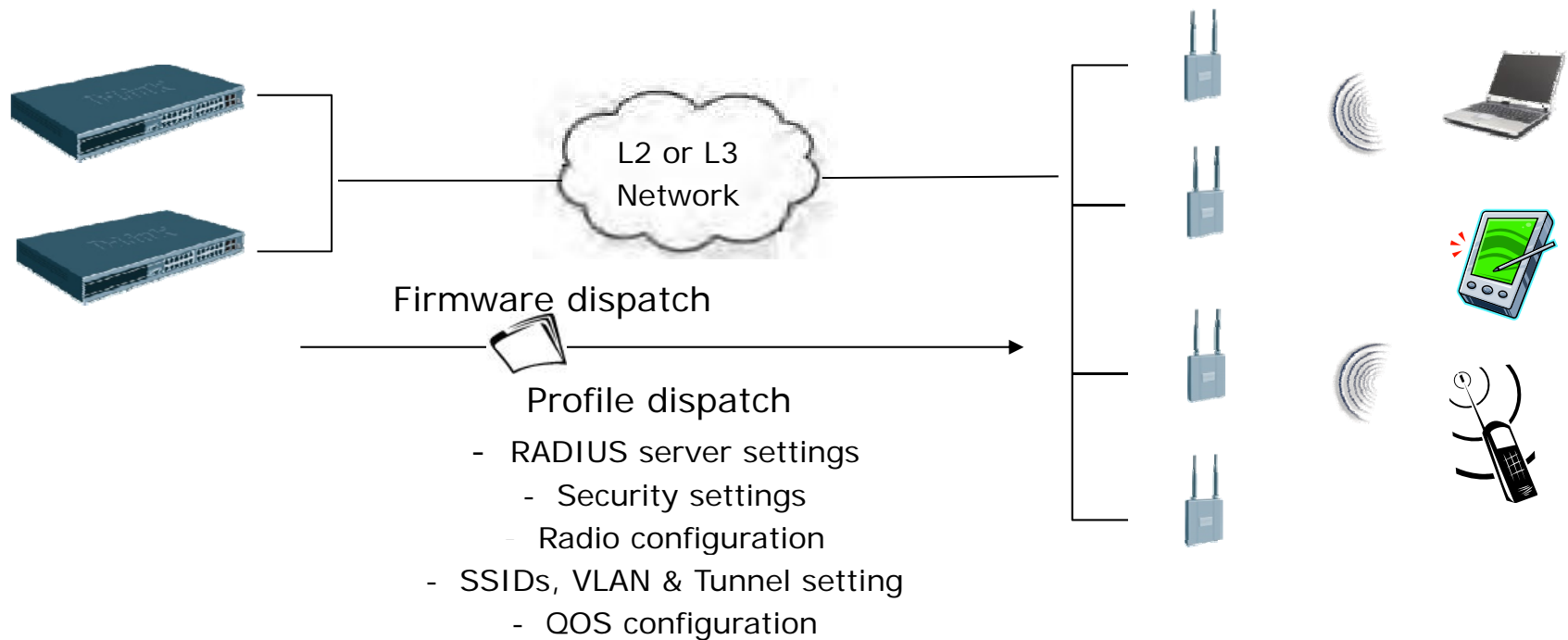




# Centralized Management

## ▪ Central Policy Control

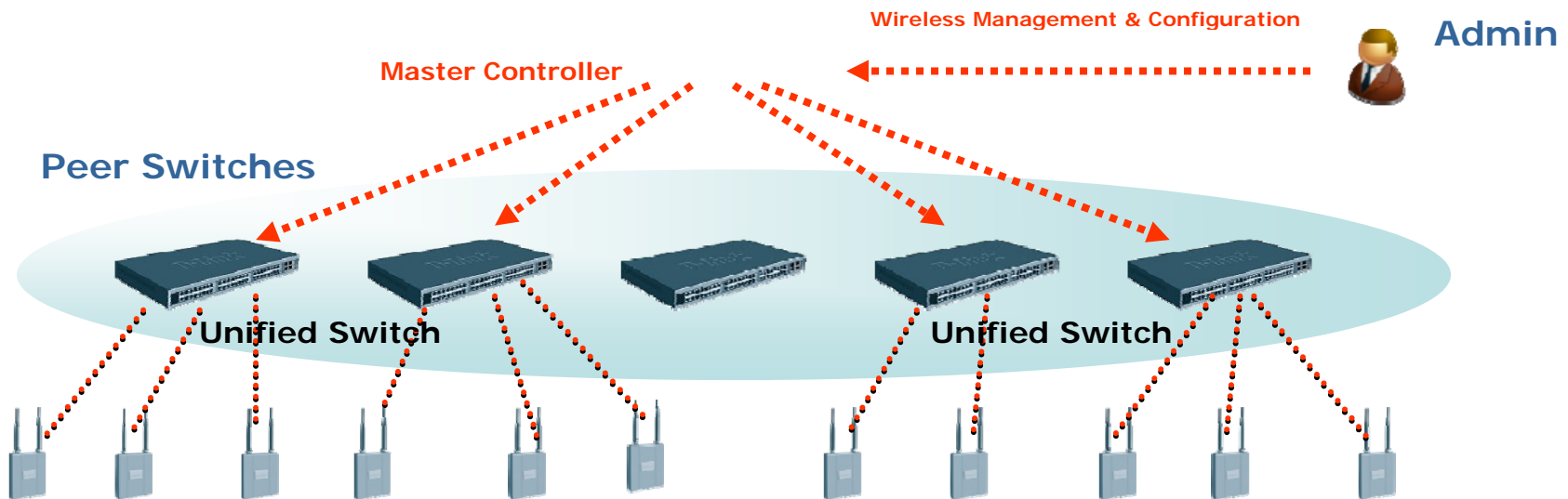
- Profile configuration is applied to a managed AP when an AP is in managed mode, or when an AP is reset. Users hence can enjoy the convenience of one-time configuration.





# Centralized Management – Switch Clustering

- DWS-4026 only
- Peer Switches can form a Cluster Group
  - All wireless configuration & management can be done from one switch
  - One Master gathers statistics and status from all APs and Clients in the group
  - Provides single point of management
- Similar to D-Link Single IP Management (SIM)





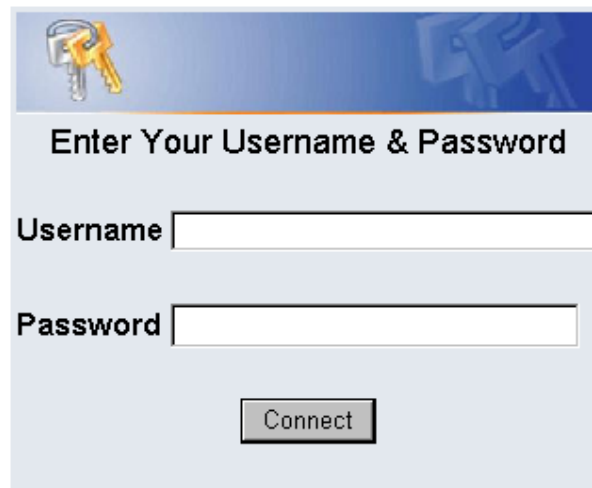
# Secure Wireless Connectivity

- Complete Security Features
- Support tradition wireless security
  - Managed AP MAC list
  - Wireless Client MAC list
  - WEP (Static/Dynamic)
  - WPA Enterprise/Personal
  - WPA2 Enterprise/Personal
- Also support D-Link proprietary security
  - Captive Portal
  - Wireless Intrusion Detection System (WIDS)
  - Wireless Intrusion Prevention System (WIPS)/Threat Mitigation – DWS-4026 only



# Secure Wireless Connectivity – Captive Portal

- A Web-based Authentication which provides intuitive, user friendly authentication
- An authentication web page is prompted to the HTTP client on the wireless network before surfing the Internet
- Authentication Web page could be customized
- No configurations needed for wireless clients



The login form features a blue header with a yellow key icon. Below the header, the text "Enter Your Username & Password" is displayed. There are two input fields: "Username" and "Password". A "Connect" button is located at the bottom of the form.

#### 1. INTRODUCTION

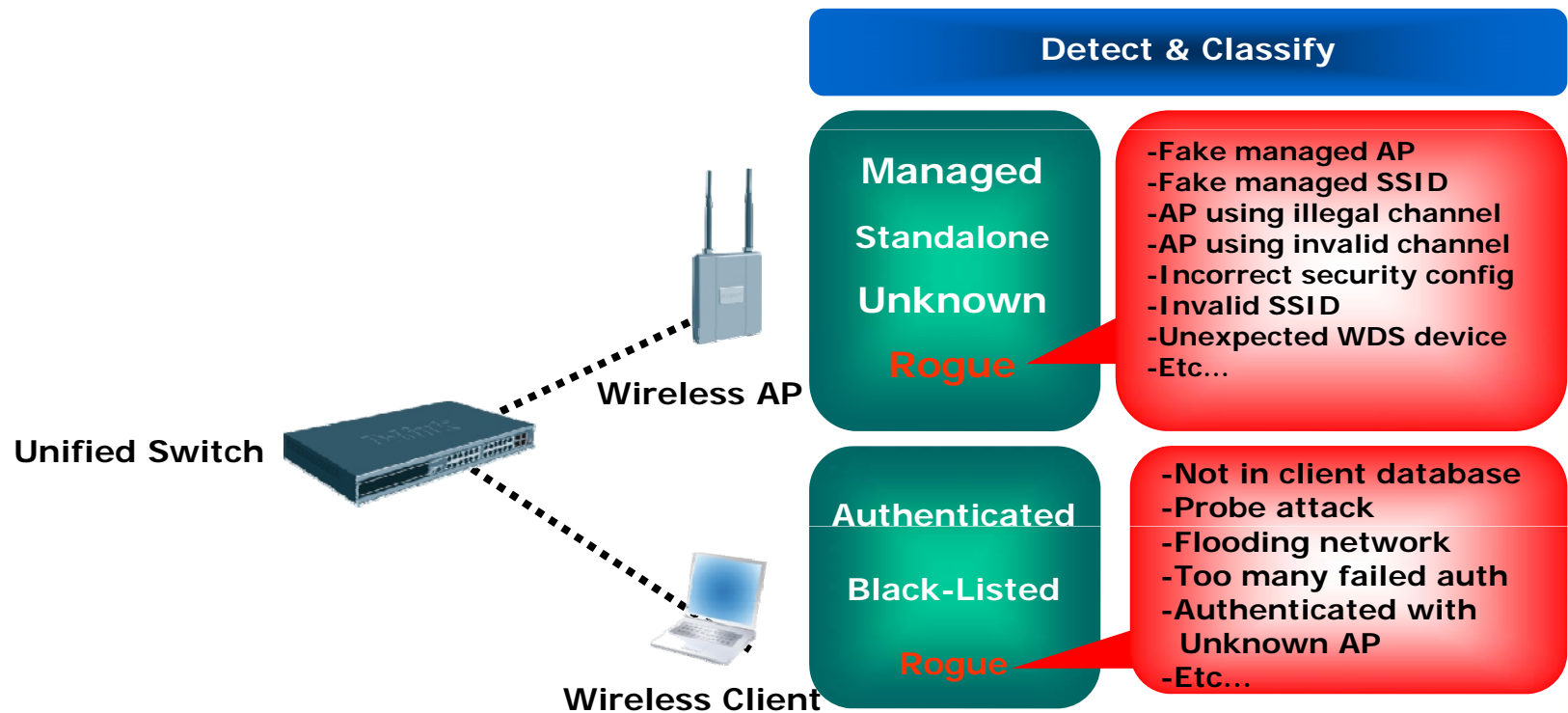
BestLodge's Acceptable Use Policy ("AUP") is intended to help enhance the use of the Internet by preventing unacceptable use. All users of BestLodge Internet services (the "Services") - those who access some of our Services but do not have accounts ("Visitors"), as well as those who pay a monthly service fee to subscribe to the Services ("Members") - must comply with this AUP. We support the free flow of information and ideas over the Internet and do not actively monitor use of the Services under normal circumstances. Similarly, we do not exercise editorial control over the content of any Web site, electronic mail transmission, news group, or other material created or accessible over or through the Services, except for certain proprietary websites. However, in accordance with our Internet

☐ Check here to indicate that you have read and accepted the Acceptance Use Policy.



## Secure Wireless Connectivity – WIDS

- DWS-4026 supports advanced Wireless Intrusion Detection and Mitigation:
  - Detect and classify **AP** :
    - Managed, Standalone, Unknown, Rogue (fake managed AP, fake SSID, illegal channel, etc...)
  - Detect and Classify **Wireless Client**
    - Authenticated, Black-listed, Rogue (probe attack, flooding network, etc...)





## Secure Wireless Connectivity – WIPS/Threat Mitigation

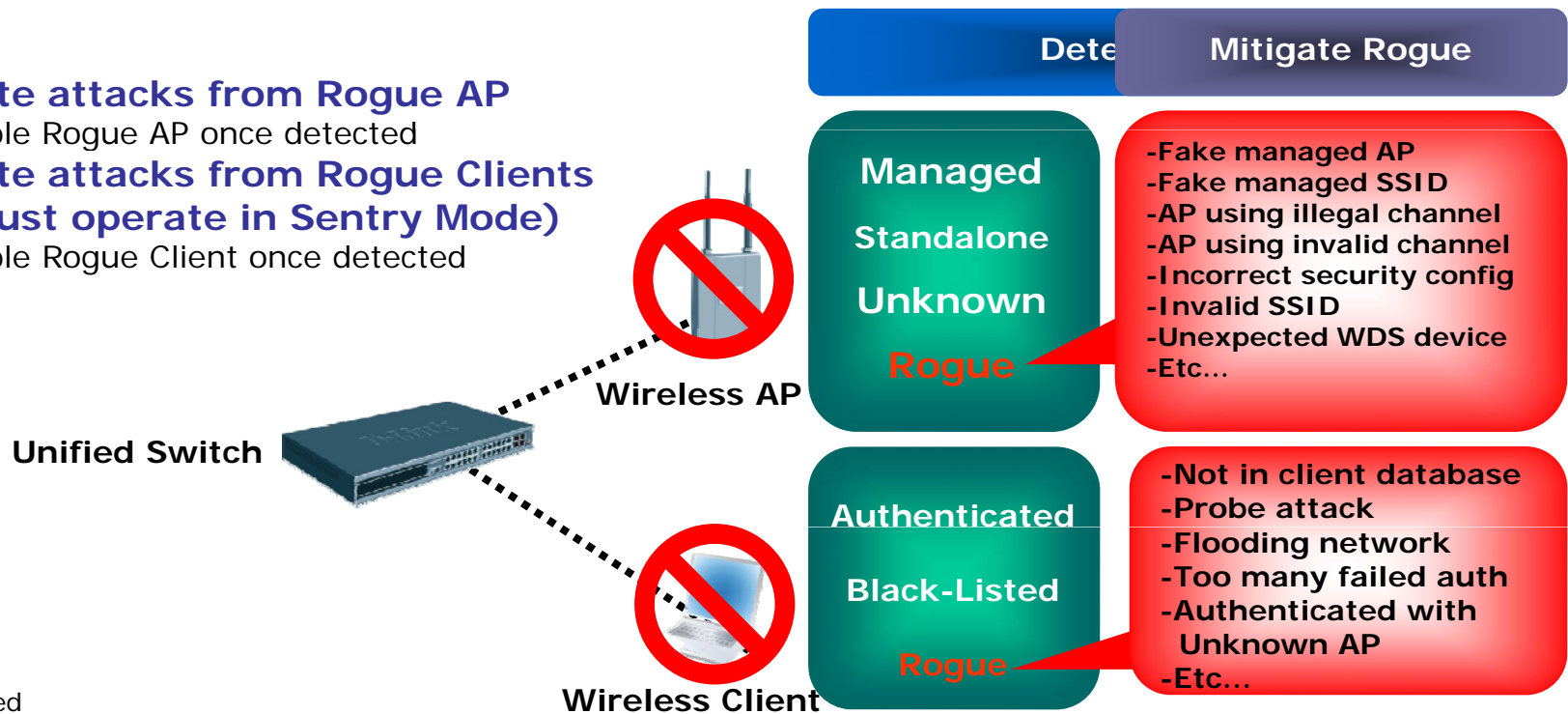
- DWS-4026 supports advanced Wireless Intrusion Detection and Mitigation:
  - Detect and classify **AP** :
    - Managed, Standalone, Unknown, Rogue (fake managed AP, fake SSID, illegal channel, etc...)
  - Detect and Classify **Wireless Client**
    - Authenticated, Black-listed, Rogue (probe attack, flooding network, etc...)

### Mitigate attacks from Rogue AP

- Disable Rogue AP once detected

### Mitigate attacks from Rogue Clients (AP must operate in Sentry Mode)

- Disable Rogue Client once detected

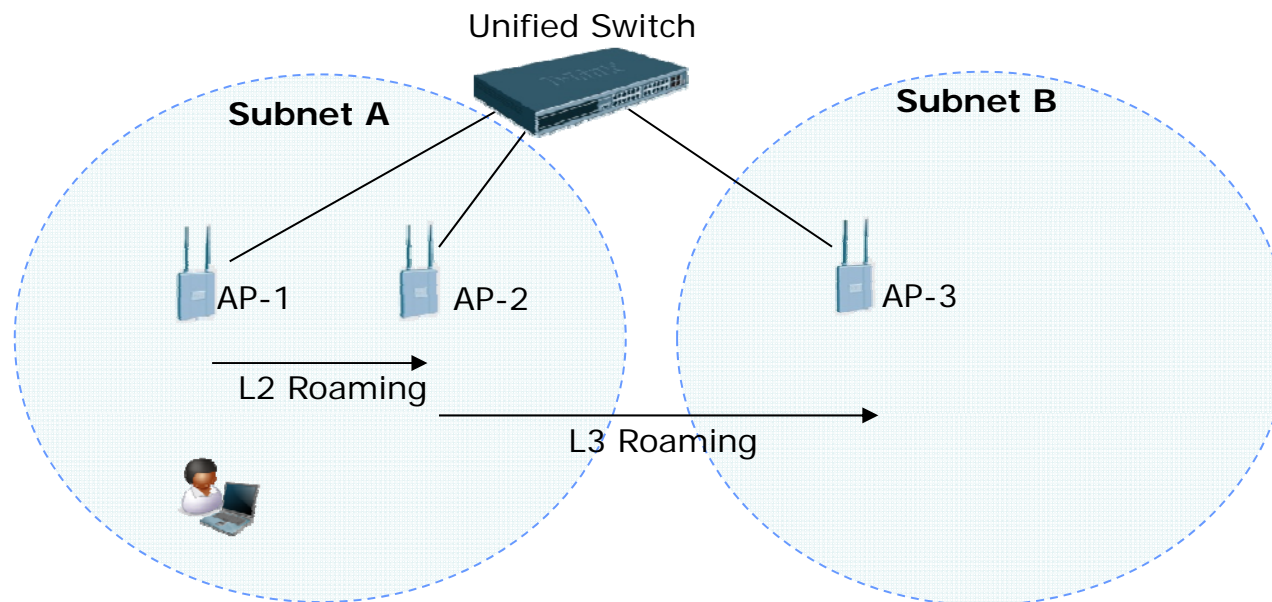






# Fast Roaming

- Ideal for VoIP Application
- Fast L2/L3 Roaming
  - Fast roaming can be supported within a subnet (Layer 2) or across subnet boundaries (Layer 3).
  - The APs need to be managed by Unified Switch to achieve fast roaming
  - One DWS-3000 switch can support fast roaming up to **48 APs**.
  - One DWS-4000 Switch can support fast roaming up to **64 APs**.

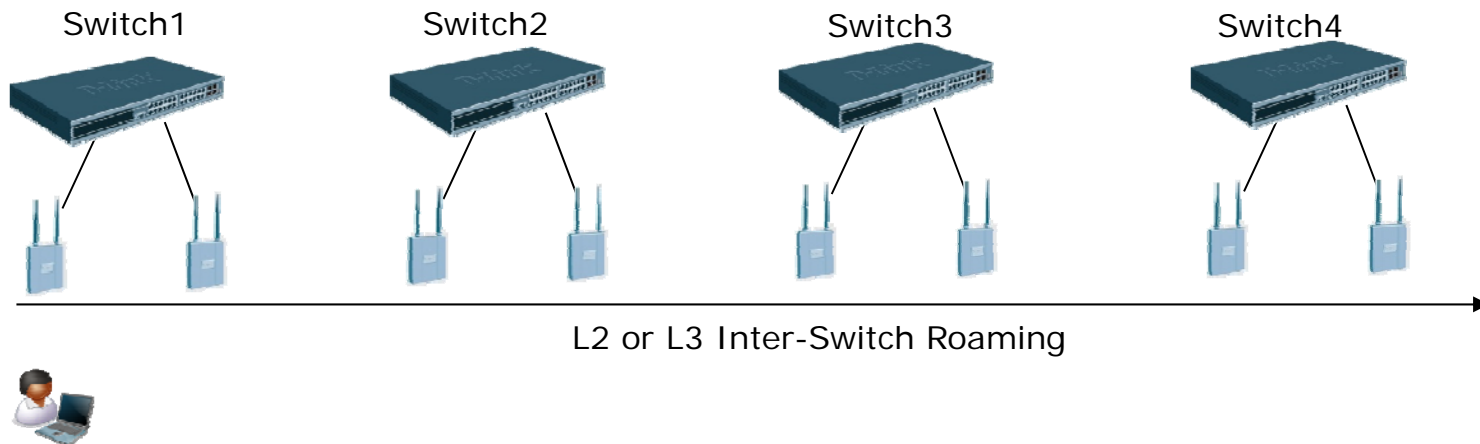






## Fast Roaming (Cont.)

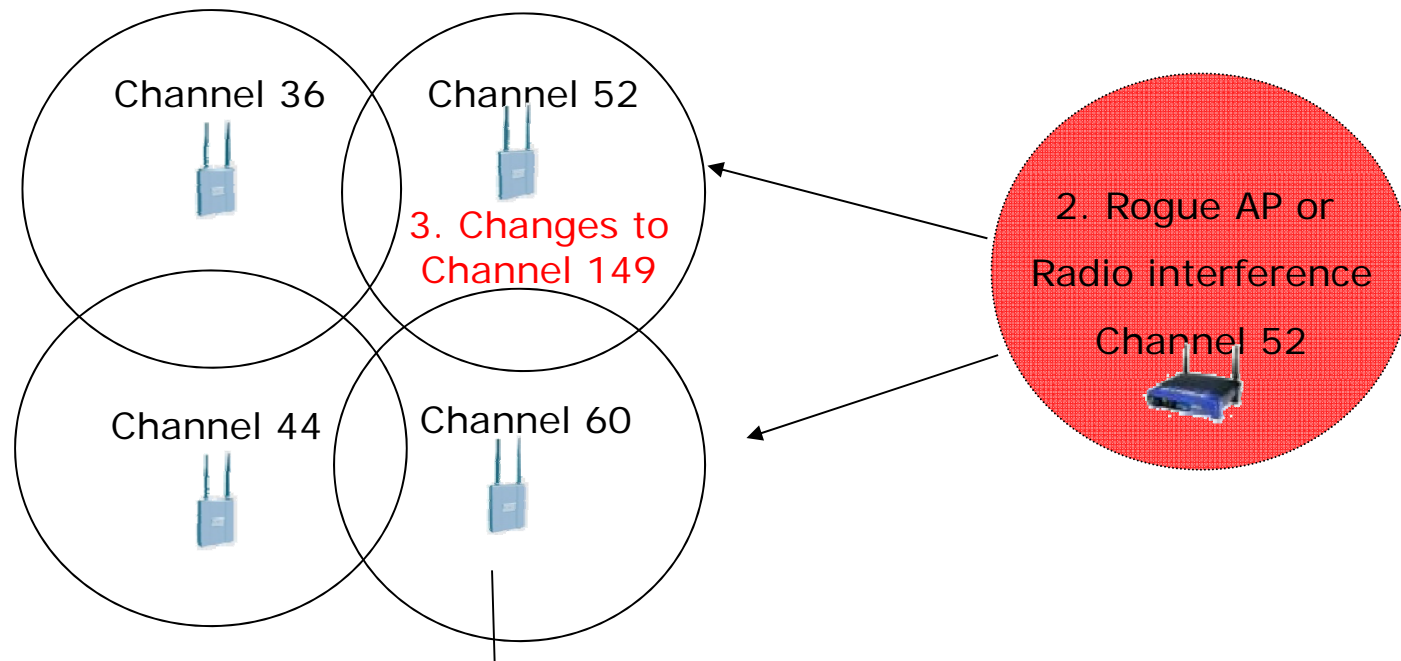
- Inter-Switch Roaming
  - DWS Series not only can support fast roaming between APs which are managed by the same switch, it can also support roaming between switches
  - For DWS-3000, 4 Peer Switches in the same Roaming group
  - DWS-3000 supports up to 192 APs
  - For DWS-4000, **8 Peer Switches** in the same Roaming group
  - DWS-4000 supports up to **256 APs**





# Automatic RF Adjustment – Auto Channel

- Channels will automatically be adjusted on any new event in the system such as an AP being added or removed, or the switch can be programmed to automatically readjust channels at certain times (i.e. 2:00am each day) of the day or upon a certain interval (i.e. every 6 hours)

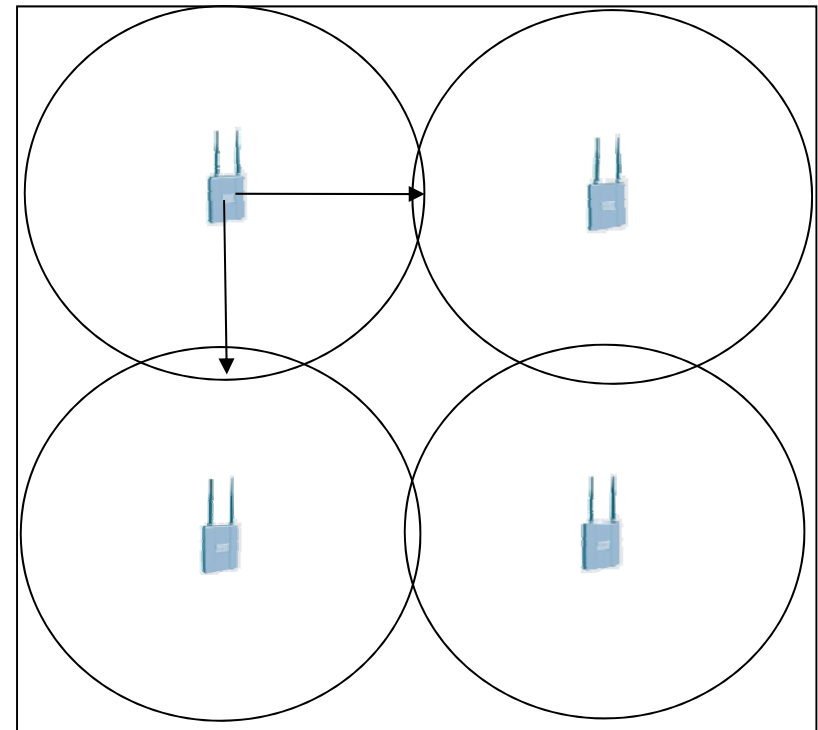
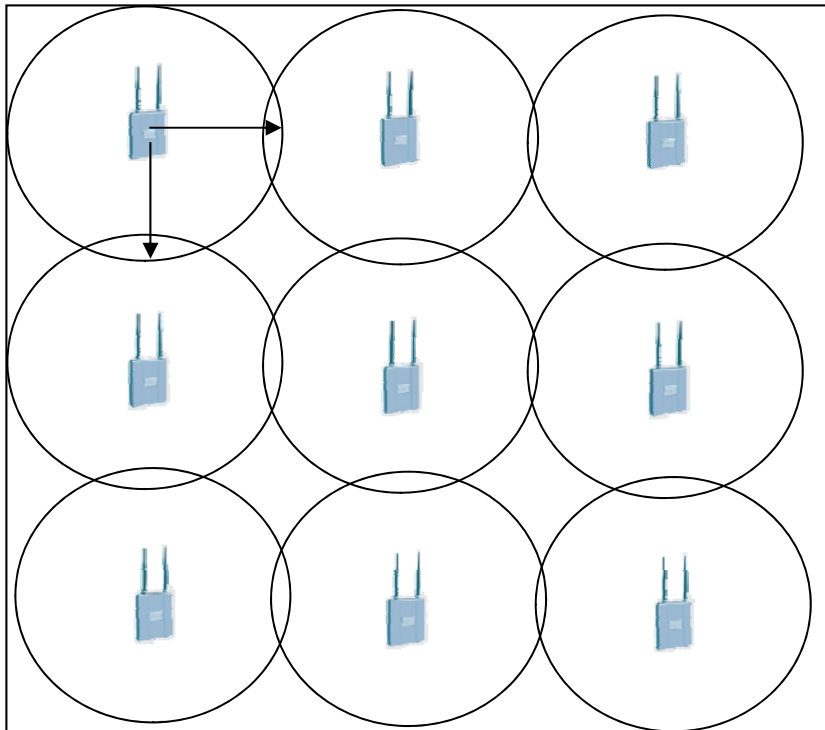


1. When first time implementing APs, the System selects different channels for APs at random to avoid interference



### Automatic RF Adjustment – Auto Power

- Automatic power uses a proprietary algorithm to automatically adjust the RF signal to broadcast far enough to reach wireless clients, but not so far that it interferes with RF signals broadcast by other APs.

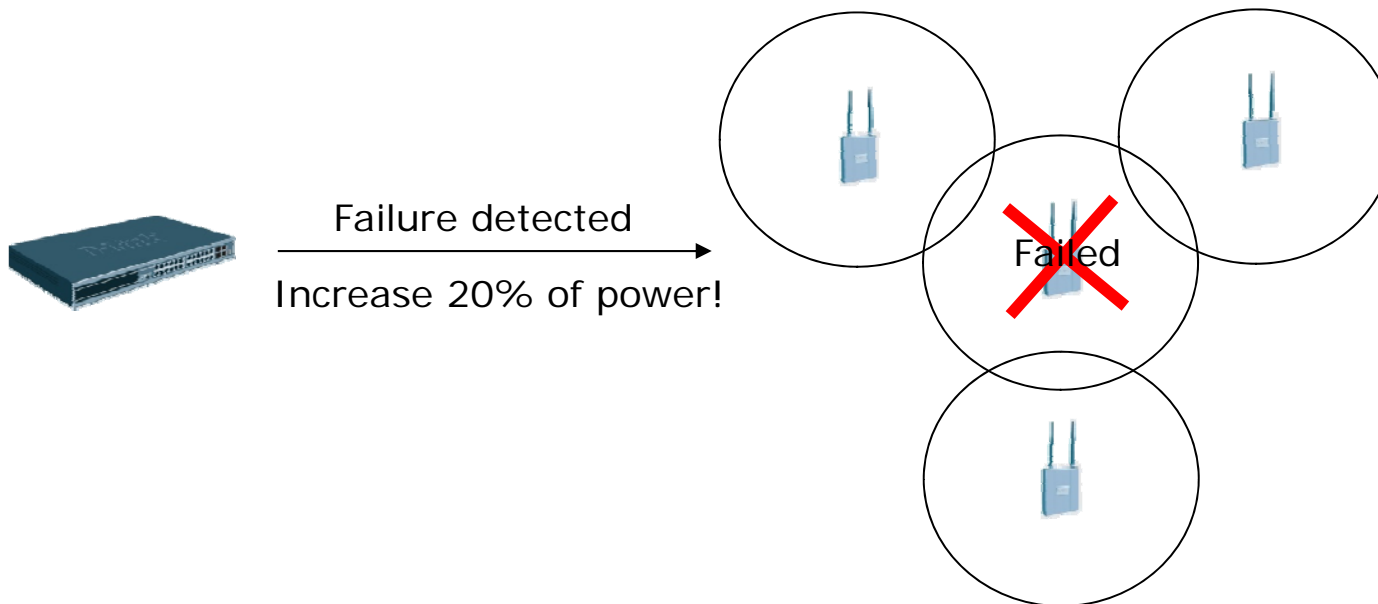




# Automatic RF Adjustment - Self-Healing Network

## ▪ Fail-Safe

- When a Managed AP is powered down, the power of its neighboring AP(s) managed by the same switch is immediately **increased by 20%**.
- The power level will adjust again every pre-configured Interval by sensing neighboring AP power status.





# Comprehensive Statistics/Alerts

- Logging for Dynamic RF Status
  - The administrator can benefit by the rich logging/trap function provided by DWS-4026. Information such as AP status, RF scan, and client status makes DWS-4026 a powerful RF monitor.

Wireless Global Status/Statistics	
Wireless Global Status	
WLAN Switch Operational Status	Enabled
IP Address	192.168.1.235
Peer Switches	<u>0</u>
Total Access Points	<u>4</u>
Managed Access Points	<u>4</u>
Connection Failed Access Points	<u>0</u>
Discovered Access Points	0
Rogue Access Points	<u>142</u>
Authentication Failed Access Points	<u>0</u>
Total Clients	<u>20</u>
Authenticated Clients	<u>20</u>
802.11a Clients	<u>0</u>
802.11b/g Clients	<u>20</u>
Black-listed Clients	0
WLAN Utilization	3 %
<small>Note: The Black-listed Clients are the clients that are configured to be disallowed to associate with any AP with the default profile.</small>	

Statistics on Web GUI



## Comprehensive Statistics/Alerts (Cont.)

**D-Link Building Networks for People**

**DWS-3026**

LAN WLAN

DWS-3026

- Monitoring
- Administration
- WLAN Visualization

Tool Help

Status SSID Status VAP Status Statistics

Summary Detail Neighbor APs

**Associated Client Status**

MAC Address	AP MAC Address	SSID	Tunnel IP Address	Location	Channel	Radio	Encryption Protocol	Status
<input type="checkbox"/> 00:04:23:57:0d:a1	00:17:9a:d2:05:70	D-Link		5F_David	1	2-802.11g	None	Auth
<input type="checkbox"/> 00:0c:f1:23:91:34	00:17:9a:d2:05:60	D-Link		5F_Arthur	6	2-802.11g	None	Auth
<input type="checkbox"/> 00:0c:f1:2e:e2:f5	00:17:9a:d2:05:70	D-Link		5F_David	1	2-802.11g	None	Auth
<input type="checkbox"/> 00:0c:f1:4a:65:26	00:17:9a:d2:05:70	D-Link		5F_David	1	2-802.11g	None	Auth
<input type="checkbox"/> 00:0e:35:35:9b:5d	00:17:9a:d2:05:70	D-Link		5F_David	1	2-802.11g	None	Auth
<input type="checkbox"/> 00:0e:35:49:76:65	00:17:9a:d2:05:60	D-Link		5F_Arthur	6	2-802.11g	None	Auth
<input type="checkbox"/> 00:0e:35:52:bf:cc	00:17:9a:d2:05:60	D-Link		5F_Arthur	6	2-802.11g	None	Auth
<input type="checkbox"/> 00:0e:35:5c:02:ab	00:17:9a:d2:05:60	D-Link		5F_Arthur	6	2-802.11g	None	Auth
<input type="checkbox"/> 00:0e:35:61:e9:ff	00:17:9a:d2:05:70	D-Link		5F_David	1	2-802.11g	None	Auth
<input type="checkbox"/> 00:0e:35:76:43:cb	00:17:9a:d2:05:60	D-Link		5F_Arthur	6	2-802.11g	None	Auth
<input type="checkbox"/> 00:0e:35:7d:74:be	00:17:9a:d2:05:60	D-Link		5F_Arthur	6	2-802.11g	None	Auth
<input type="checkbox"/> 00:0e:9b:25:df:31	00:17:9a:d2:05:70	D-Link		5F_David	1	2-802.11g	None	Auth
<input type="checkbox"/> 00:0e:9b:4a:c6:92	00:17:9a:d2:05:60	D-Link		5F_Arthur	6	2-802.11g	None	Auth
<input type="checkbox"/> 00:0e:9b:4a:c6:d2	00:17:9a:d2:05:60	D-Link		5F_Arthur	6	2-802.11g	None	Auth

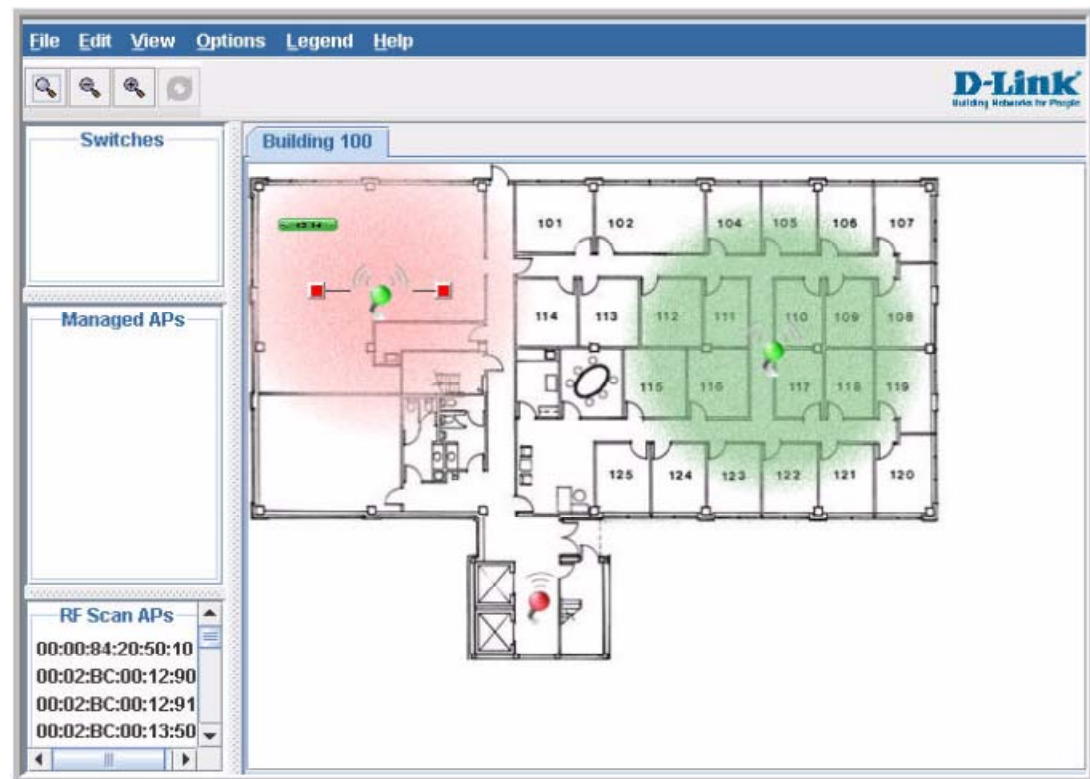
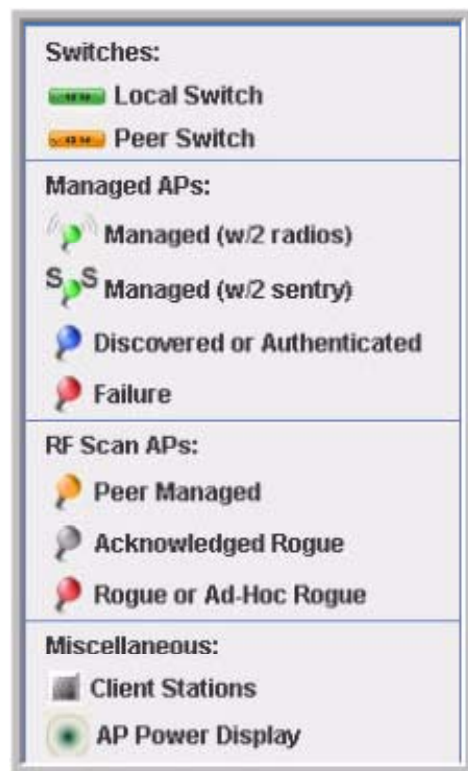
Associated Client Status on Web GUI





# Easy-to-Use Visualized Management Tool

- The diagram below shows an example of a floor plan and network with a D-Link Unified Switch that manages two APs. The graph also shows a peer switch and a rogue AP in the network.





### Hardware Basis

- D-Link Unified System consists of two components:
  - Unified Switch and Unified Access Point
- D-Link has four Unified Switch models
- Unified Switch = L2<sup>+</sup> Switch + Wireless Controller

Switch	DWS-3024L / 3024	DWS-3026	<b>DWS-4026</b>
Description	24-Port Gigabit L2 <sup>+</sup> PoE Unified Switch	24-Port Gigabit L2 <sup>+</sup> PoE Unified Switch with Two 10GE Open Slots	
Access Point	DWL-3500AP / DWL-8500AP <b>DWL-8600AP</b> *		<b>DWL-8600AP</b>
No. of APs	24 / 48	48	<b>64</b>
Note	PoE Capable		

\* Release 3.0





### Hardware Basis



- DWL-8600AP
  - Support 802.11n Wireless LAN
  - Up to 300Mbps wireless throughput, 5 times of 802.11g
  - Four-antenna design using MIMO Technology
  - Support up to 32 SSIDs
  - Support 802.3af Power over Ethernet



- DWL-3500AP
  - Support 802.11g Wireless LAN
  - Two 5dbi antennas
  - Support 8 SSIDs
  - Support 802.3af PoE

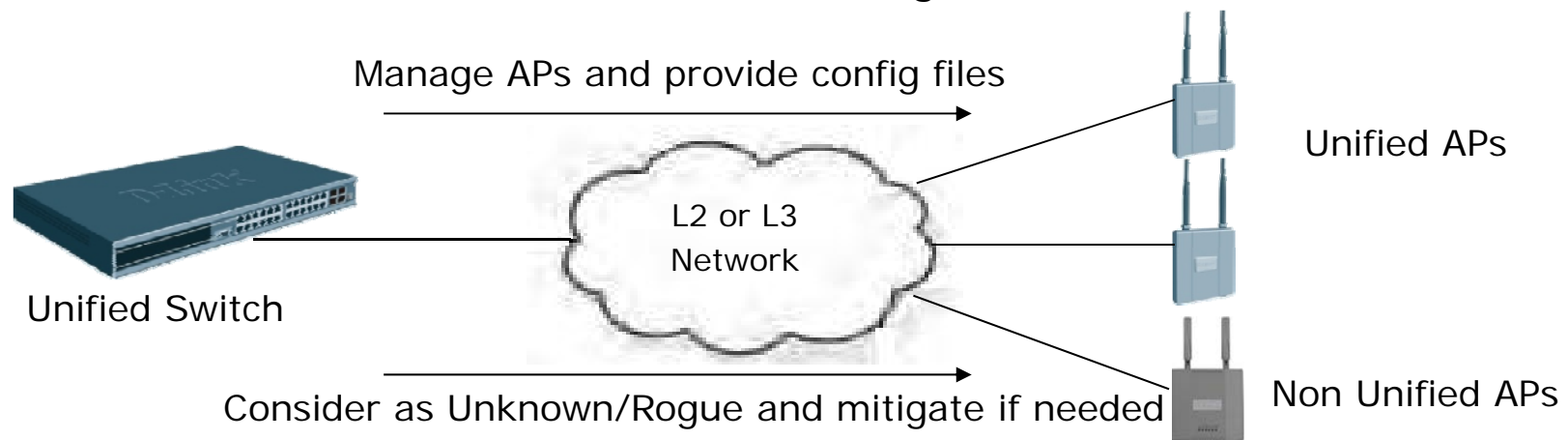


- DWL-8500AP
  - Support 802.11 a/g dual band Wireless LAN
  - Two 5dbi a/g dual band antennas
  - Support 16 SSIDs
  - Support 802.3af PoE



### Working Concept

- In D-Link Unified System, the Unified Switch works as wireless controller and centralized controls and manages all the APs.
- The switch provides the configurations, including SSIDs, radio settings, QoS, security, and more, to the Unified APs and Thin APs.
- D-Link Unified Access System works only when the APs are managed by D-Link Unified Switch.
- D-Link Unified Switch only can work with specific Unified APs, not all the APs can be managed by Unified Switches.
- DWS-3000 series (Release 3.0) can work with DWL-8600AP
- DWS-4026 doesn't work with (can't manage) DWL-3500/8500AP





Session 2

# Unified System Deployment



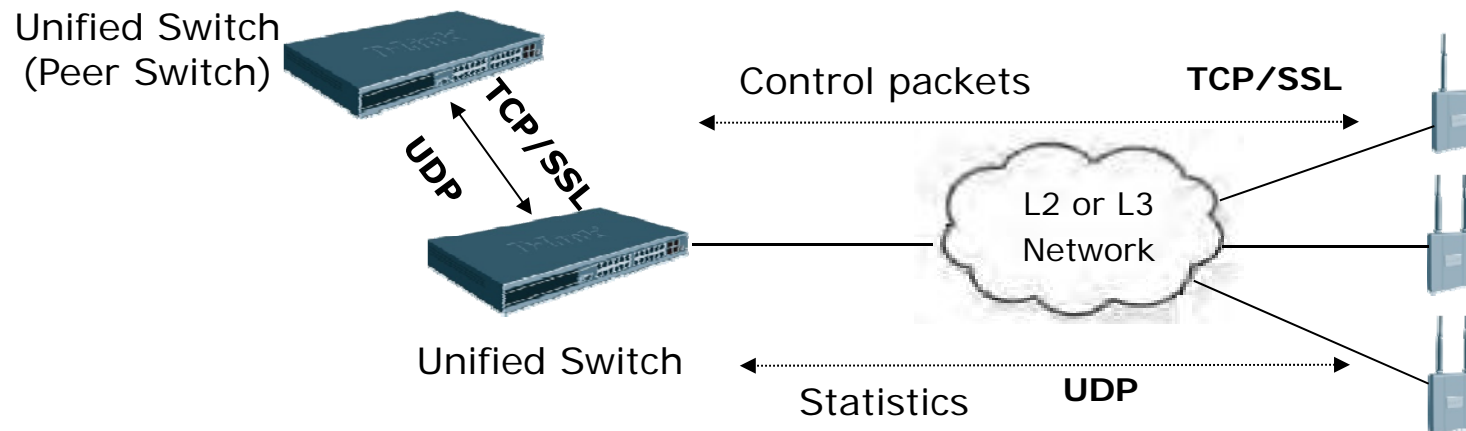
## Session 2: Unified System Deployment

- Protocol Basics
- Overlay and Unified Solution
- Tunnel and Non-Tunnel Modes
- AP Management and Client Data Network
- Switch Redundancy



## D-Link Wireless AP Protocol (DWAPP)

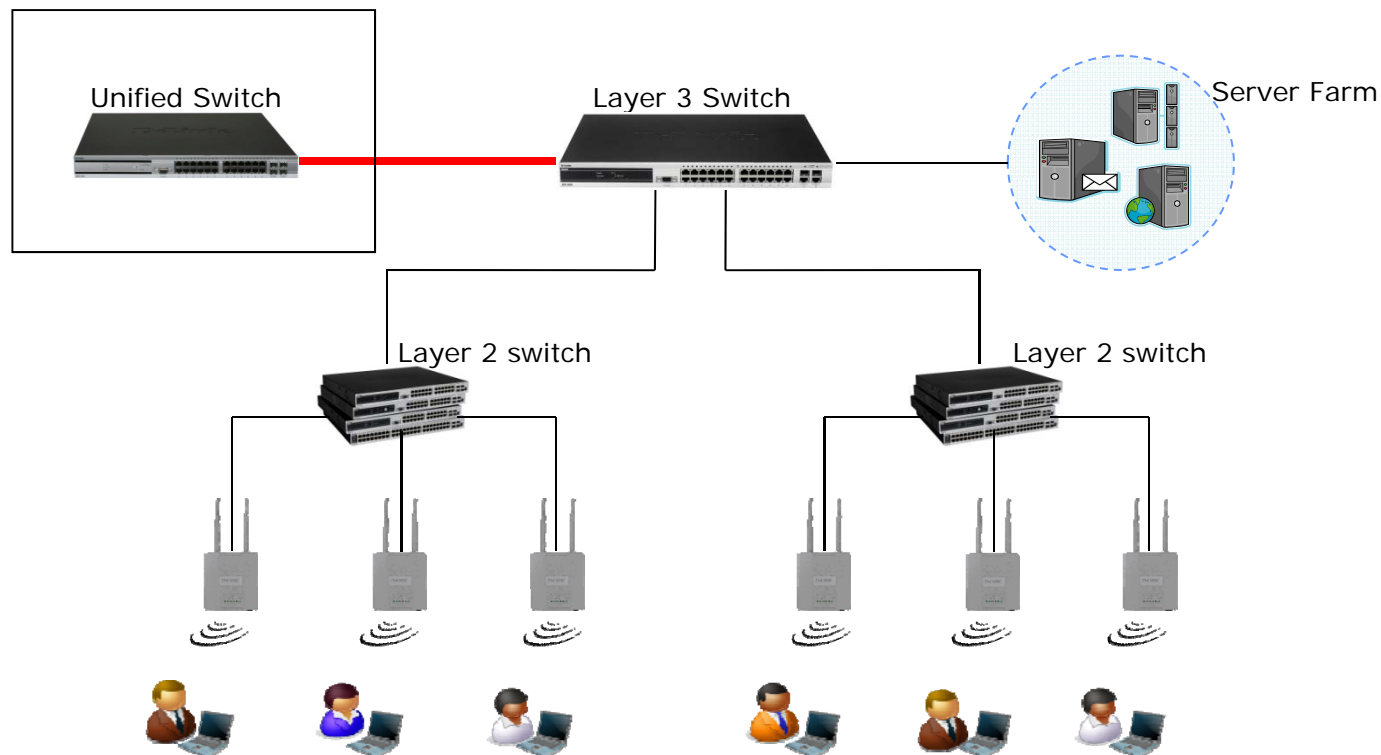
- CAPWAP like protocol
- Can cross L2 or L3 network
- Switch ↔ AP
  - TCP/Port 57777, SSL encryption
    - Firmware/Profile delivery/Heartbeat/Client session key sharing etc.
  - UDP/Port 57775, 57776
    - Report and Statistics
- Switch ↔ Switch
  - TCP/port 57777, SSL encryption
  - UDP/port 57775
    - Client data/AP data/RF status sharing within peer switches
- Note: Make sure there is no NAT device between AP and switch





## Overlay Solution

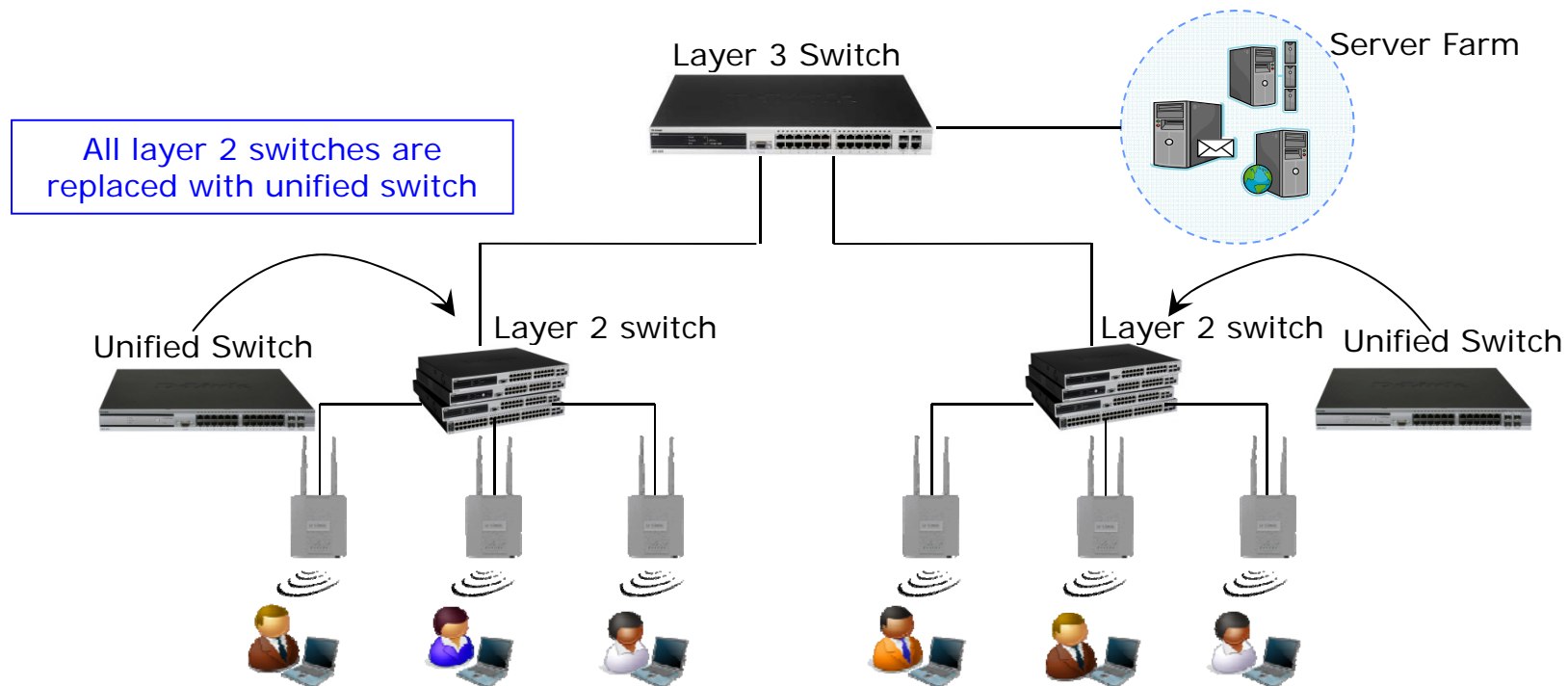
- In overlay solution deployment, unified switch is **introduced to existing network infrastructure** to protect current investment in network infrastructure with all the benefits of WLAN switching.
- The Unified Switch works as wireless controller here.





## Unified Solution

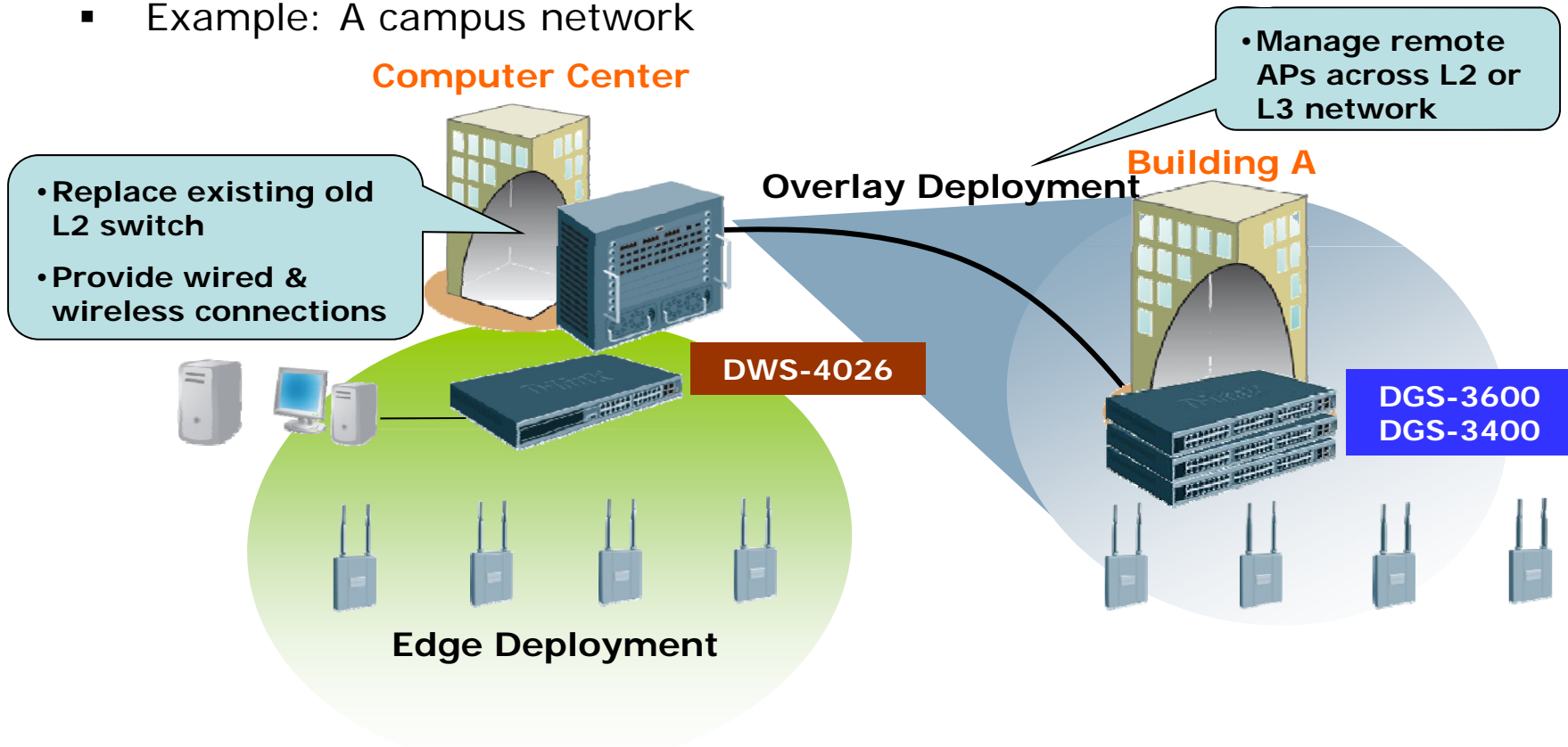
- Deploy at the **network edge** for greatest scalability
- Full Gigabit Ethernet speed is ready for 802.11n
- Unified Switch works as L2 edge switch and wireless controller at the same time





## Overlay + Edge Deployment

- Typical deployment topology – Mixture of Overlay and Edge deployments
- The unified switch to APs is reachable by routing
- Example: A campus network

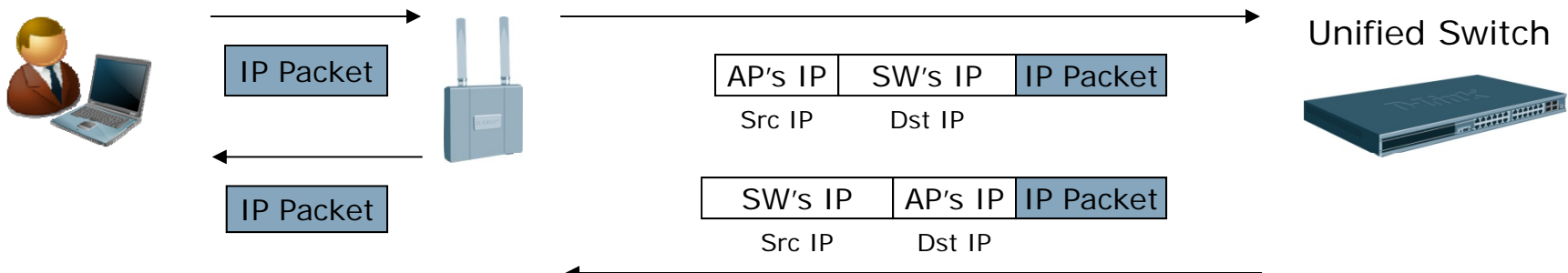
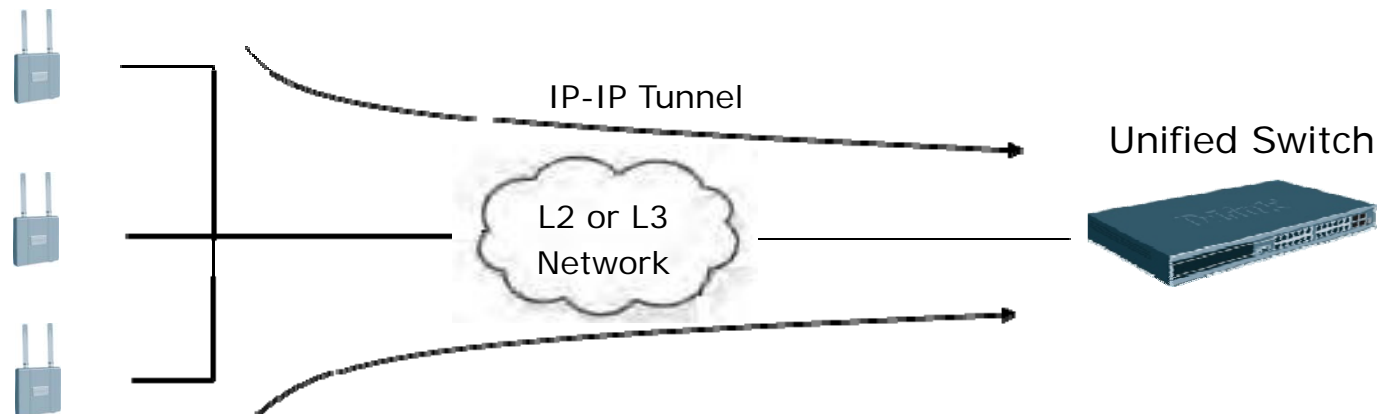






## Tunnel Mode

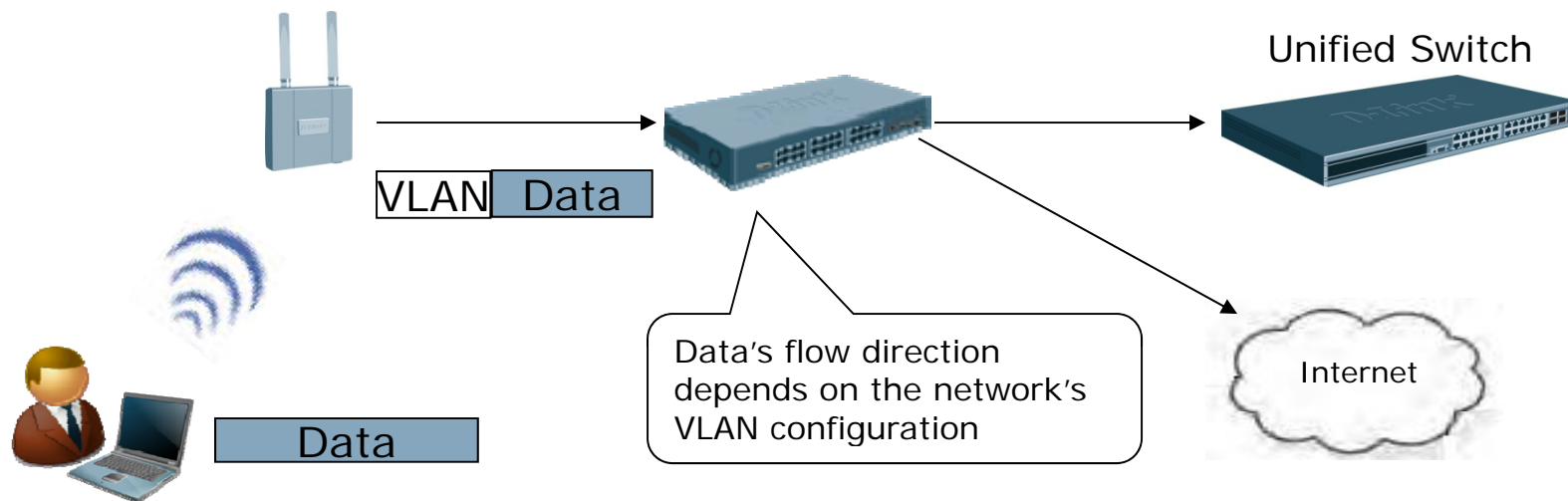
- Wireless client's data will go through IP-IP tunnel and back to the Unified Switch.





## Non-Tunnel Mode

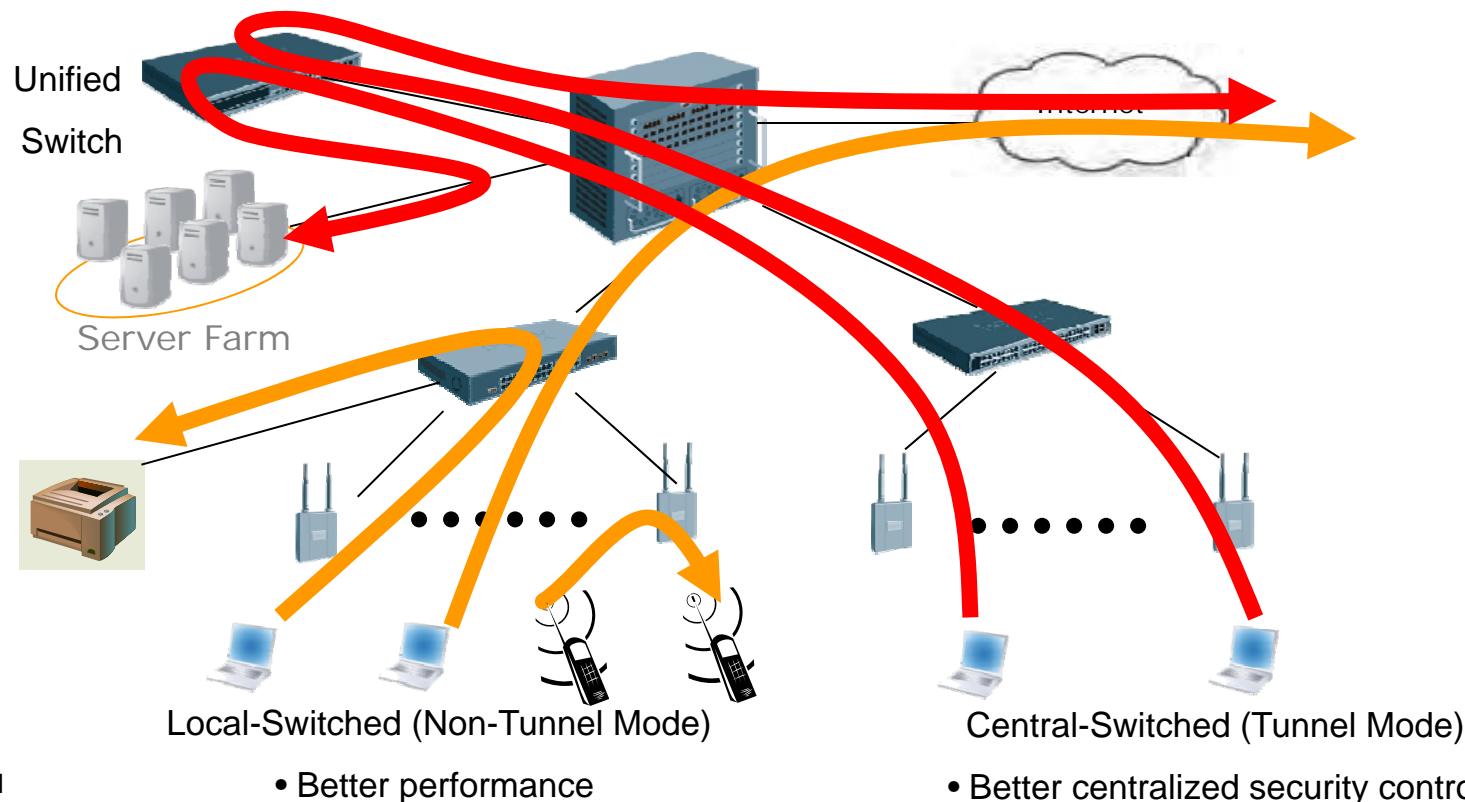
- Wireless client's data can be tagged with a VLAN but not necessarily goes back to the Unified Switch (depending on the network design).





## Flexible Deployment – Adaptable Wireless

- Wireless traffic can be local-switched at the AP or Central-switched at the Unified Switch depending on users' needs
- No need to purchase additional license or upgrade firmware





## Tunnel & Non-Tunnel Modes

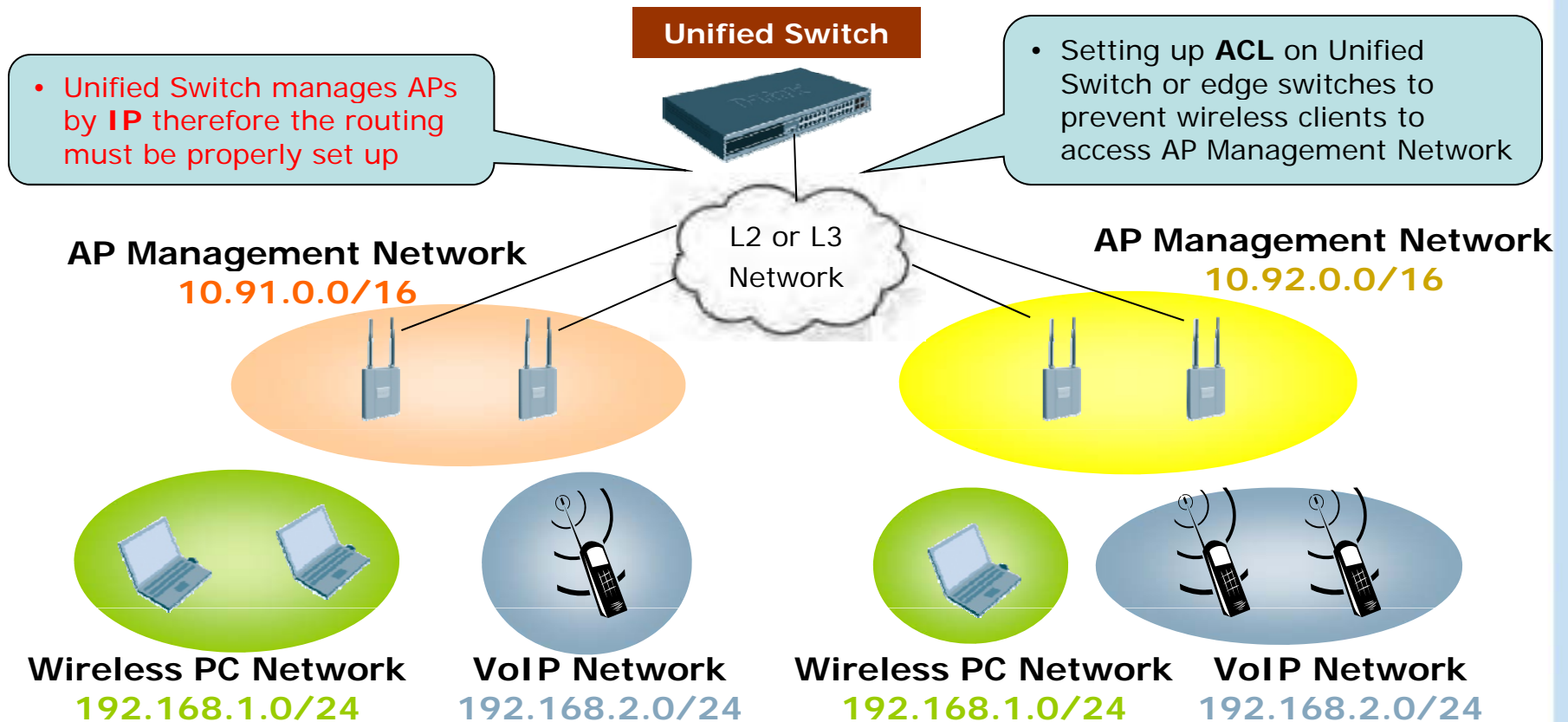
- Advantages and Disadvantages

	VLAN Forwarding	L3 Tunneling
Advantage	<ul style="list-style-type: none"><li>• Easier Unified Switch configuration</li><li>• Save more bandwidth in Overlay topology</li></ul>	<ul style="list-style-type: none"><li>• Better centralized policy with ACL, QoS, DHCP Server, etc</li><li>• Transparent to customer network (no 'VLAN explosion' issue)</li></ul>
Disadvantage	<ul style="list-style-type: none"><li>• May not use advanced features, such as ACL, QoS, DHCP Server, etc on the Unified Switch in Overlay topology</li><li>• 'VLAN explosion' issue – setting up VLAN membership across large network requires huge effort</li></ul>	<ul style="list-style-type: none"><li>• More complicated Unified Switch configuration</li><li>• May consume more bandwidth in Overlay topology</li></ul>



## AP Management and Client Data Network

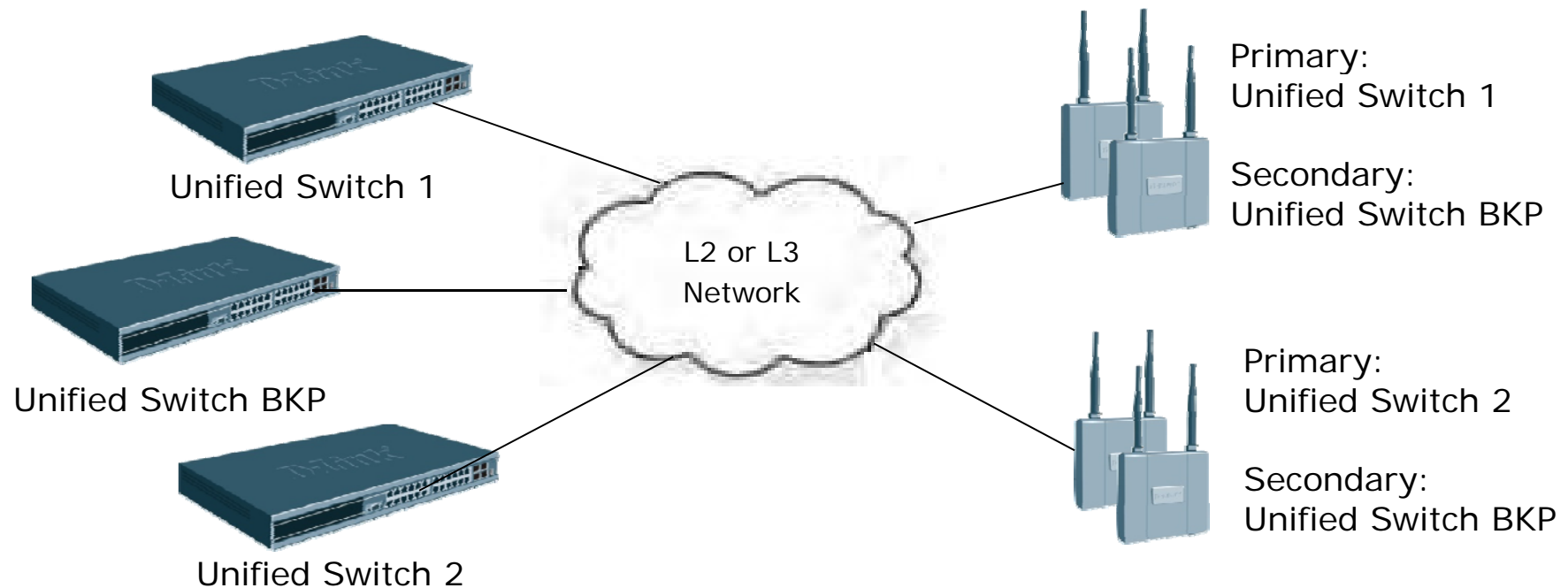
- AP and client data can be segregated into different networks to provide better security.





## Switch Redundancy Design – N + 1

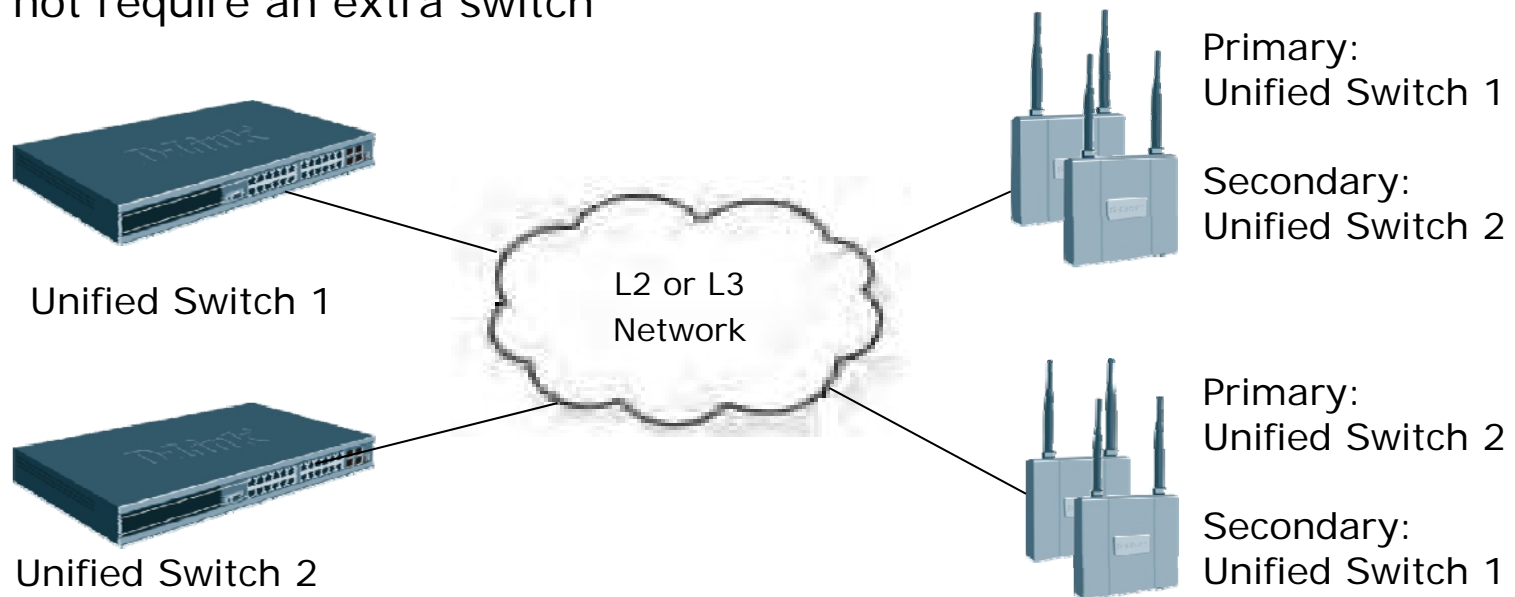
- One extra switch works only as backup
- Allow each switch manages its maximum number of APs





## Switch Redundancy Design – N + N

- Each switch backup its peer switches
- In order to backup peer switches, the switch needs to reserve some space for peer switch managed APs. Therefore, it cannot manage its maximum number of APs.
- Do not require an extra switch





Session 3

# Unified System Usage





## Session 3: Unified System Usage

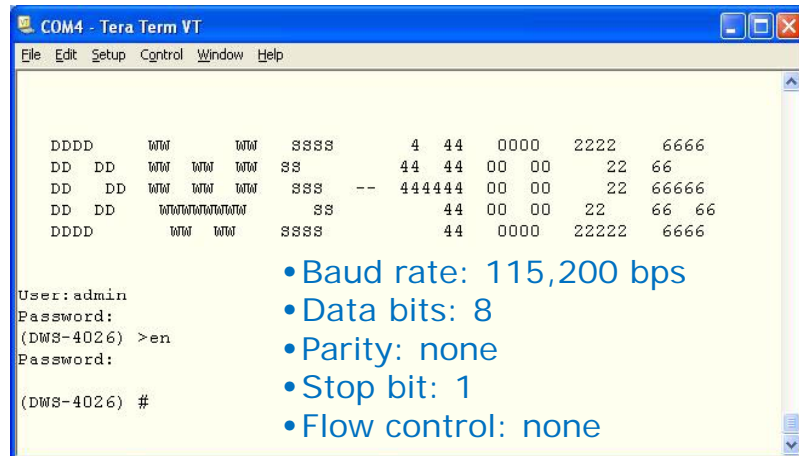
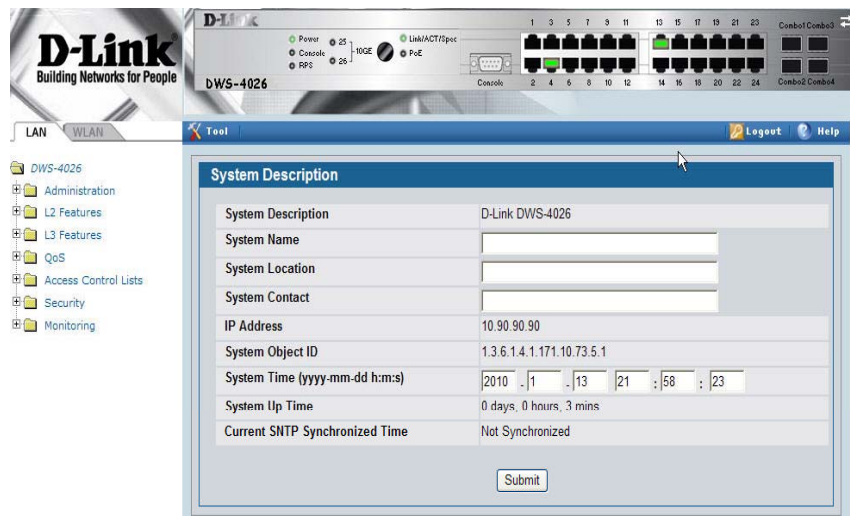
- User Interface
- AP Profile
- AP Discovery
- AP Validation
- Peer Switch



## Unified System Usage

- User Interface

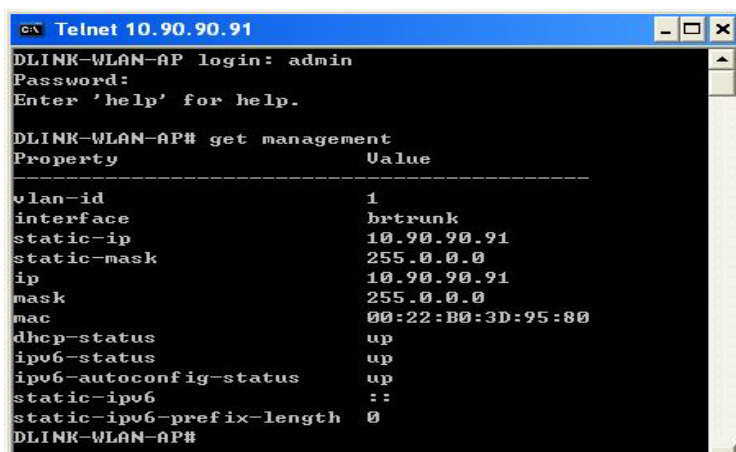
### User Interface – Unified Switch



- D-Link Unified Switch supports 3 kinds of user interface
  - Web GUI
  - CLI (telnet and console port)
  - SNMP v1/v2c/v3
- Default IP of the Unified Switch is **10.90.90.90**
- Default account is “admin” and blank for the password
- Provide MIB file for SNMP protocol



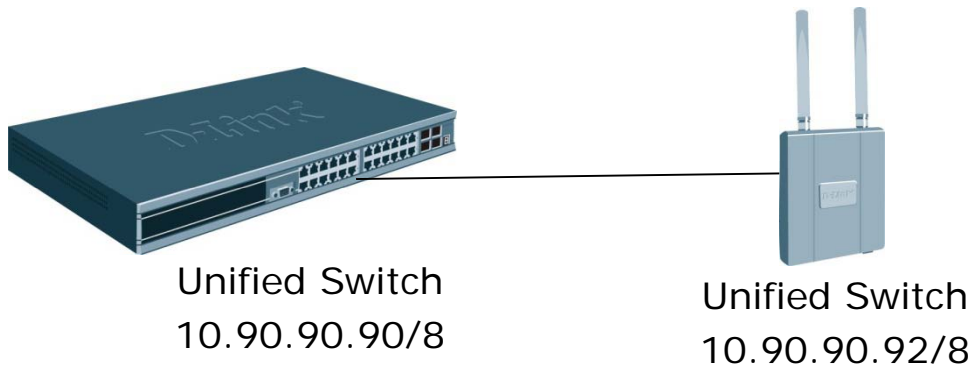
## User Interface – Unified Access Point



- D-Link Unified APs support three types of user interfaces:
  - Web GUI
  - CLI
  - SNMP v1/v2c/v3
- In Managed Mode, Web GUI and SNMP are disabled
- DHCP client is enabled by default
- If there is no DHCP server in the network, the AP will use its default IP as **10.90.90.91**
- Default username and password are both "**admin**"
- DWL-8600AP supports external console port (Baud rate 115,200 bps)



## AP Configuration Example



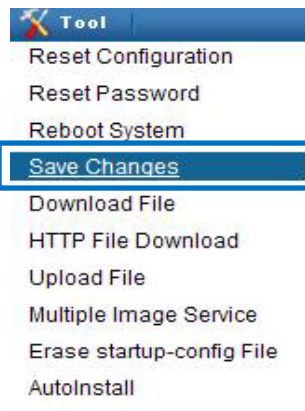
# **factory-reset**  
(set AP to factory default)  
# **reboot**  
(re-start AP)

```
# set management dhcp-status down
# set management static-ip 10.90.90.92 (Telnet again with new IP)
# set management static-mask 255.255.255.0
# set static-ip-route gateway 10.90.90.90
# save-running
# get management (Check the new configuration)
```

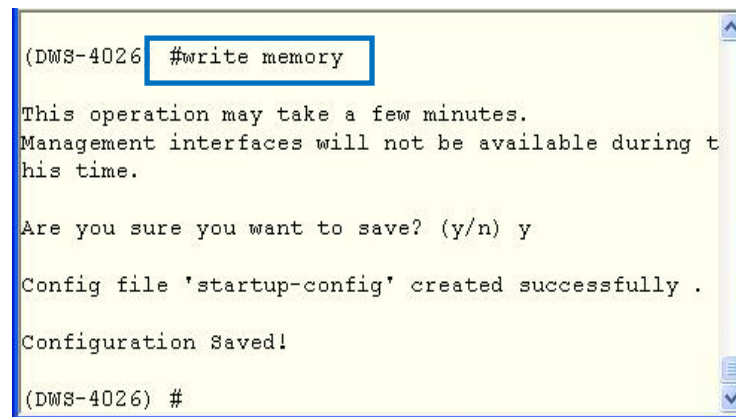


## Save Changes

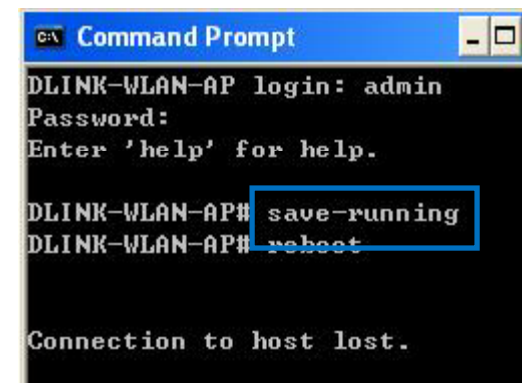
- After changing the configuration of the Switch or AP, it is necessary to save changes.
- If it is not saved, the Switch and AP will lose its configuration after the power cycle
- Save changes can be done through WEB UI or CLI
- Command:
  - "write memory" for Switch
  - "save-running" for AP



WEB UI of the Switch



CLI of the Switch



CLI of the AP



## AP Profile

- D-Link Unified Solution centralized manage all APs by using AP Profiles
- With AP Profiles, users can pre-configure the wireless parameters such as SSID, Security, QoS, and push configurations to all managed APs
- There is a default profile in switch, users may use it if their APs have the same settings

The screenshot displays the D-Link Unified System configuration interface. On the left, a tree view shows the navigation menu with 'Basic Setup' highlighted. The main panel is titled 'Wireless Default VAP Configuration' and shows the 'AP Profile 1-Default' configuration. The interface includes tabs for 'Global', 'Discovery', 'Profile', 'Radio', 'SSID', 'Valid AP', and 'OUI'. The 'Profile' tab is active, showing a table of AP profiles.

Network	VLAN	L3 Tunnel	Hide SSID	Security	Redirect
<input checked="" type="checkbox"/> 1 - dlink1	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 2 - dlink2	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 3 - dlink3	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 4 - dlink4	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 5 - dlink5	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 6 - dlink6	1-Default	Disabled	Disabled	None	None





## AP Profile

- If the users need to divide the APs into different groups, they can create several new profiles.

Support up to 16 profiles on each Switch

- Next, apply different profiles to different APs

MAC Address (*)	Peer Managed	Location	Switch Port	IP Address	Software Version	Age	Status	Configuration Status	Profile
00:22:b0:3d:95:80		Local AP	0/1	192.168.101.1	1.0.0.6	0d:00:00:03	Managed	Success	3-Local AP
00:22:b0:3d:97:00		Remote AP	Unknown	172.17.20.101	1.0.0.6	0d:00:00:05	Managed	Success	2-Remote AP



## Apply Settings to AP

- After configuring the profiles, the settings are saved in switch and not the APs. Remember to push the configurations to APs using the following two ways:

1. Reset the APs

MAC address	Location	IP Address	Status	Reset Status
<input type="checkbox"/> 00:22:b0:3d:98:40		10.90.90.91	Managed	Not Started

2. By clicking "Apply" button

Profile	Profile Status
<input checked="" type="checkbox"/> 1-Default	Configured





## AP Discovery

- To implement D-Link Unified Solution, the switch must manage the APs.
- To manage the APs, the switch needs to find out where are the APs.
- D-Link Unified Solution implements some mechanisms for switch and AP to discover each other:
  - L2 discovery – Switch discovers AP
  - L3 discovery – Switch discovers AP
  - L3 discovery – AP discovers switch
  - DHCP option 43
- With Default setting, the switch only discovers VLAN 1 (no default setting on APs). The users need to manually locate the AP if the AP is not in the default VLAN of the switch.



## AP Discovery – L2 Discovery

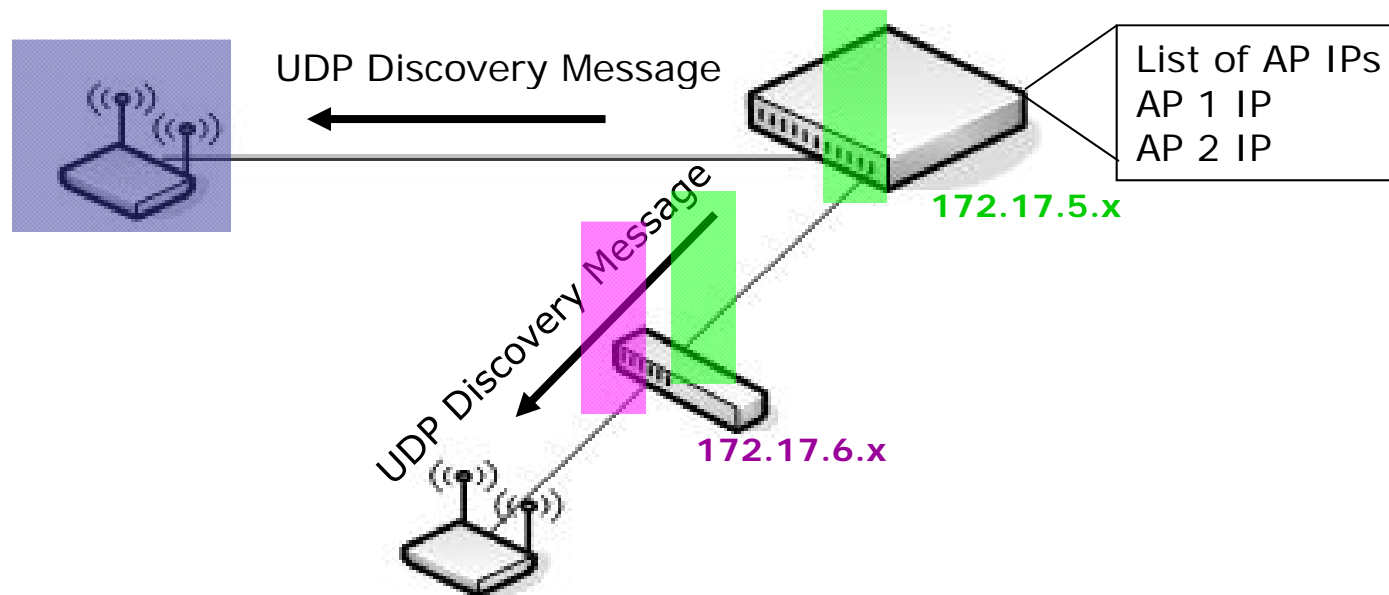
- APs need to be in the same L2 broadcast domain with switch.
- Switch sends a broadcast packet containing the discovery message every 30 seconds.
- Users need to input the AP's VLAN
- VLAN 1 is the default VLAN in the L2 discovery list

The screenshot shows the D-Link Unified System Configuration interface. On the left, a tree view under the 'WLAN' tab shows 'Administration' > 'Basic Setup' selected. The main panel is titled 'Wireless Discovery Configuration' and has tabs for 'Global', 'Discovery', 'Profile', 'Radio', 'SSID', 'Valid AP', and 'OUI'. The 'Discovery' tab is active. It contains two sections: 'L3/IP Discovery' and 'L2/VLAN Discovery'. Both sections have a checked checkbox. The 'L3/IP Discovery' section has an 'IP List' with an empty list and a 'Delete' button. The 'L2/VLAN Discovery' section has a 'VLAN List' with '1 - Default' and a 'Delete' button. Below the 'VLAN List' is a 'VLAN (1-3965)' input field with an 'Add' button. The 'IP Address Range' section has 'From' and 'To' input fields and an 'Add' button.



## AP Discovery – L3 Discovery

- If the AP and switch are in a L3 environment, the switch can discover the APs with their IP addresses.
- The switch and AP must be able to ping each other.
- Switch sends UDP message to AP.
- AP initiates an SSL TCP connection to the switch.



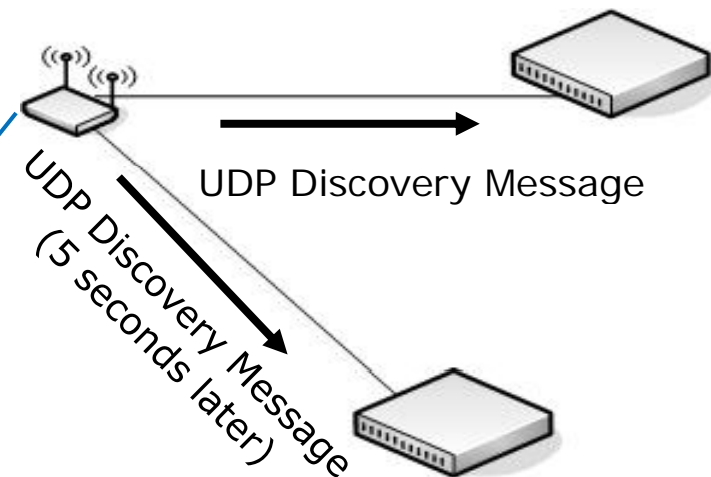


## AP Discovery – L3 Discovery

- It is possible to ask the AP to discover the switch.
- The users need to use CLI to achieve this.
- Login to the CLI of the AP and configure 1-4 Switch IP addresses using command "set managed-ap switch-address-1"
- Next, the AP will try to discover the switches in sequence with the IP address
- The switch and AP must be able to ping each other.

```
COM4 - Tera Term VT
File Edit Setup Control Window Help
DLINK-WLAN-AP# set managed-ap switch-address-1 10.90.90.90
DLINK-WLAN-AP# set managed-ap switch-address-2 10.90.90.91
DLINK-WLAN-AP# get managed-ap
Property      Value
-----
mode          up
ap-state      down
switch-address-1 10.90.90.90
switch-address-2 10.90.90.91
switch-address-3
switch-address-4
dhcp-switch-address-1
dhcp-switch-address-2
dhcp-switch-address-3
dhcp-switch-address-4
managed-mode-watchdog 0
DLINK-WLAN-AP# save-running
```

List of Switch IPs  
Switch 1 IP  
Switch 2 IP

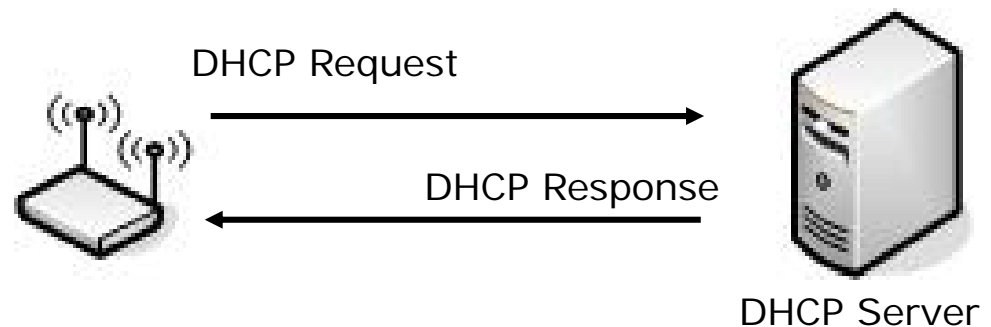




## DHCP Option 43

- It is a heavy loading to configure the switch's IP address on all APs, especially when there are many APs.
- D-Link Unified Solution provides an easy way to complete these settings automatically with DHCP option 43
- Format for DHCP option 43 values are defined by RFC 2132 as follows:
  - Data type code (01) + address length (04) + IP address in hexadecimal format
- DHCP Option 43 entry for 192.168.1.10 looks like 01 04 C0 A8 01 0A.
- DHCP Option 43 is not required if switch IP is statically configured in APs.

```
COM4 - Tera Term VT
File Edit Setup Control Window Help
DLINK-WLAN-AP# get managed-ap
Property      Value
-----
mode          up
ap-state      up
switch-address-1
switch-address-2
switch-address-3
switch-address-4
dhcp-switch-address-1 192.168.0.254
dhcp-switch-address-2 192.168.10.254
dhcp-switch-address-3
dhcp-switch-address-4
managed-mode-watchdog 0
DLINK-WLAN-AP#
```





## AP Discovery Limitation

- Routing between switch and APs is necessary.
- The correct L2 or L3 discovery setup is needed if the switch and APs are not in the same VLAN/network segment.
- AP discovery is **NOT** allowed when passing through NAT.
- Firmware versions of both Switch and APs must be the same.

The screenshot displays the D-Link Unified System Configuration interface. On the left is a navigation tree with folders for Security, Monitoring, Administration, Basic Setup (selected), AP Management, Advanced Configuration, and WLAN Visualization. The main window has tabs for Global, Discovery (selected), Profile, Radio, SSID, Valid AP, and OUI. The 'Wireless Discovery Configuration' section is active, showing two discovery methods: L3/IP Discovery and L2/VLAN Discovery. L3/IP Discovery is checked, with an empty IP List and an IP Address Range section. L2/VLAN Discovery is also checked, with a VLAN List containing '1 - Default' and a VLAN (1-3965) section. Both sections have 'Delete' and 'Add' buttons.

Wireless Discovery Configuration	
<b>L3/IP Discovery</b> <input checked="" type="checkbox"/>	<b>L2/VLAN Discovery</b> <input checked="" type="checkbox"/>
IP List: <empty list>	VLAN List: 1 - Default
IP Address Range: From [ ] To [ ]	VLAN (1-3965): [ ]
[Delete] [Add]	[Delete] [Add]



## AP Validation

Valid AP database

Add the MAC address of the AP manually here

MAC address	Location	AP Mode	Profile
<input type="checkbox"/> 00:22:b0:3d:95:80		Managed	1-Default

MACAddress: 00:00:00:00:00:00    Location:    Add

- Before applying configuration to the AP, the AP must be managed by the Unified Switch.
- To manage an AP, the MAC Address of the AP must be in "Valid AP" database.
- Valid AP database can be local or on a RADIUS server.
- There are two ways to add the MAC address of the AP to local Valid AP database, the first way is to add it manually.





## AP Validation

- Another way is to place a "tick" to the required AP from WLAN → Monitoring → Access points → All Access Points , and click "Manage"

MAC address	Location	Switch Port	IP Address	Software Version	Age	Status	Profile	Radio
<input checked="" type="checkbox"/> 00:22:b0:3d:95:80	N/A	N/A	10.90.90.91	N/A	0h:0m:10s	No Database Entry	N/A	N/A

Buttons: Delete All, Manage, Acknowledge, Refresh, Auto Refresh

- After completing the setup, remember to check the AP status from WLAN → Monitoring → Access points → Managed AP Status

MAC Address	Location	Switch Port	IP Address	Software Version	Age	Status	Configuration Status	Profile
00:22:b0:3d:95:80		0/4	10.90.90.91	1.0.0.6	0d:00:00:01	Managed	Success	1-Default

Buttons: Delete, Delete All, Refresh, Auto Refresh





## Debug Mode

- The APs managed by the unified switch are not accessible via Telnet.
- The users must enable “Debug Mode” if they want to access the AP.
- When the “Debug Mode” on the AP is enabled, it can be accessed via Telnet again.

The screenshot displays the D-Link Unified System Management interface. On the left, a navigation tree shows the hierarchy: LAN/WLAN > DWS-4026 > Administration > AP Management > Advanced Settings. The main content area is titled 'Managed AP Advanced Settings' and contains a table of AP configurations. The 'Debug' column for the selected AP is highlighted with a blue box and shows the value 'Disabled'. Below this, a 'Managed AP Debug' dialog box is open, showing fields for MAC address (00:22:B0:3D:98:40), Location, IP Address (10.90.90.91), Status (None), Password, and Confirm Password. The 'Enable Debug' checkbox is also highlighted with a blue box and is currently unchecked. At the bottom of the dialog are 'Cancel' and 'Apply' buttons.

MAC address	Location	Debug	Radio	Channel	Power (%)
00:22:b0:3d:98:40		Disabled	1-802.11a/n 2-802.11b/g/n	100 1	100 100

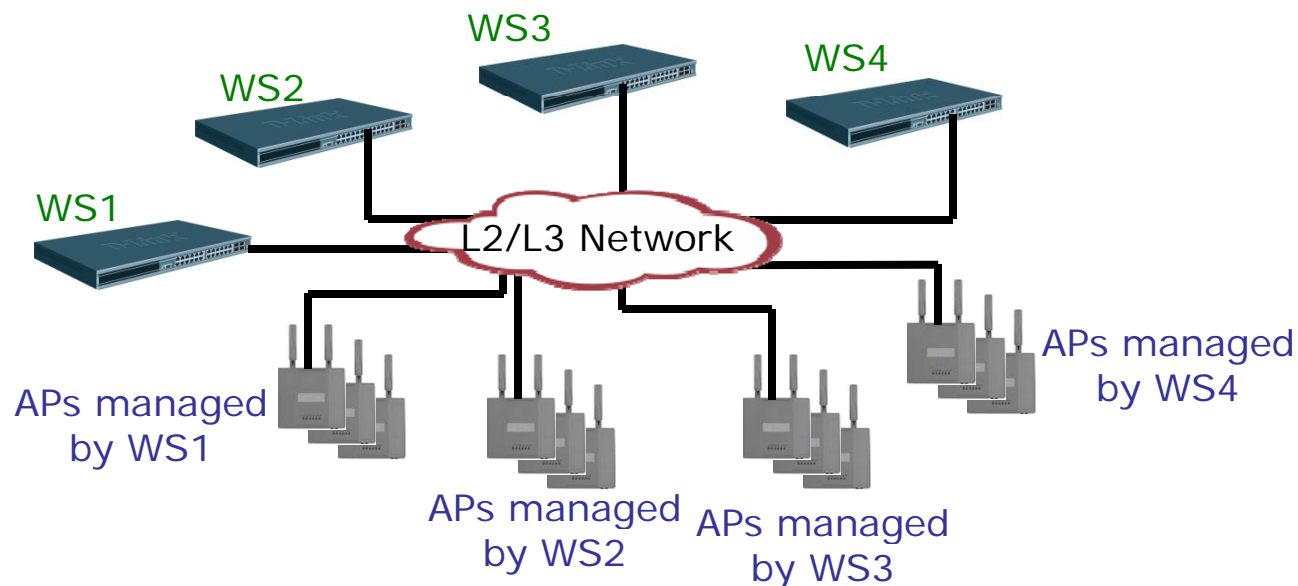
  

Managed AP Debug	
MAC address	00:22:B0:3D:98:40
Location	
IP Address	10.90.90.91
Status	None
Password	
Confirm Password	
Enable Debug	<input type="checkbox"/>



## Peer Switch

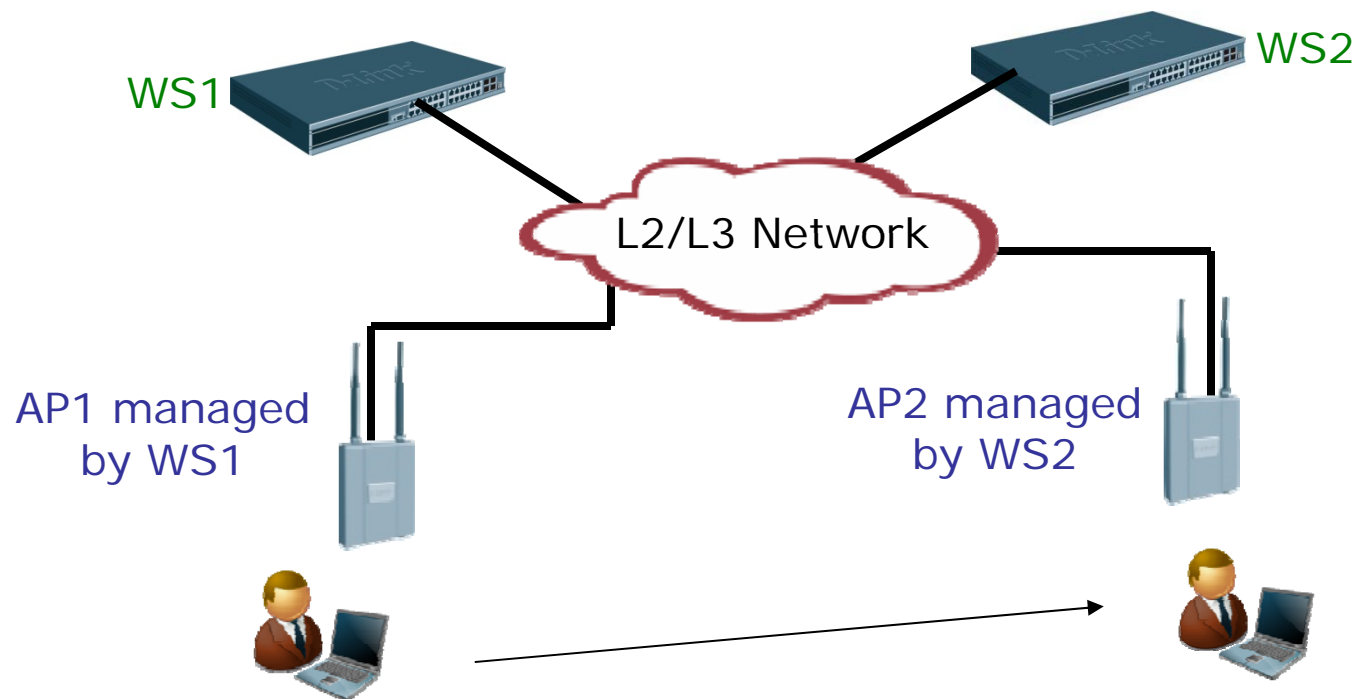
- D-Link Unified Solution allows users to group up to 4/8 Unified Switches to:
  - Share the information about the AP they managed
  - Share the information about wireless clients associated with the APs
  - Set Switches in a peer group can handle up to 8000 clients
  - Form an inter-switch roaming group (Need the same security setting)





## Inter-switch Roaming

- Inter-Switch roaming (formed by Peer Switch) can support fast roaming and pre-authentication across Switch.





## How to Set Up Peer Switch?

- Peer unified switches discover each other using similar method as unified switch discovering APs.
- In L2 network, they are able to find each other easily.
- In different VLANs or L3 network, the users need to set VLAN Discovery or L3 Discovery

<b>L3/IP Discovery</b> <input checked="" type="checkbox"/>		<b>L2/VLAN Discovery</b> <input checked="" type="checkbox"/>	
<b>IP List</b>	<div>&lt;empty list&gt;</div>		
<b>IP Address Range</b>	From <input type="text"/>	To <input type="text"/>	
<input type="button" value="Add"/> <input type="button" value="Delete"/>		<div><b>VLAN List</b></div> <div>1 - Default</div> <div><b>VLAN (1-4094)</b> <input type="text"/></div> <div><input type="button" value="Add"/> <input type="button" value="Delete"/></div>	



## Check the Peer Switch Status

- Check Peer Switch Status

IP Address	Vendor ID	Software Version	Protocol Version	Discovery Reason	Managed AP Count	Age
192.168.10.1	D-Link	1.0.0.6	2	IP Poll	1	0d:00:00:23
192.168.30.1	D-Link	1.0.0.6	2	IP Poll	1	0d:00:00:23

- Check Peer Switch's Managed AP Information

MAC Address	Location	IP Address	Firmware Version	Age	Status	Profile	Radio	Channel	Authenticated Clients
00:17:9a:d2:8d:70		10.90.90.21	1.0.2.3	0h:0m:3s	Managed	1-Default	1-802.11a	44	0
00:17:9a:d2:05:78	N/A	N/A	N/A	0h:1m:37s	Rogue	N/A	2-802.11g	1	0
00:17:9a:d2:3b:18	N/A	N/A	N/A	0h:0m:37s	Peer WS Managed	N/A	802.11g	1	N/A
00:19:5b:b0:c3:48	N/A	N/A	N/A	0h:2m:37s	Peer WS Managed	N/A	802.11g	1	N/A
00:50:18:21:d1:c7	N/A	N/A	N/A	0h:3m:37s	Rogue	N/A	802.11g	1	N/A

The color indicates the AP type

- Green: Managed AP
- Red: Rogue AP
- Amber: Peer Switch managed AP



Lab 1

# Switch Redundancy



### Equipment Requirement

- It is recommended to have four members in each group
- Equipment
  1. DWS-4026 x 3
  2. DWL-8600AP x 3 (with power adapter and console cable)
  3. DGS-3627 x 1
  4. Wireless Client with IEEE 802.11n and support WPA2-Enterprise x 2
  5. Windows XP desktop computer or laptop x 1 (as RADIUS Server)
  6. RS-232 console cable x 1 (USB to RS-232 if required)
  7. Network cable x 10



# Lab 1: Switch Redundancy

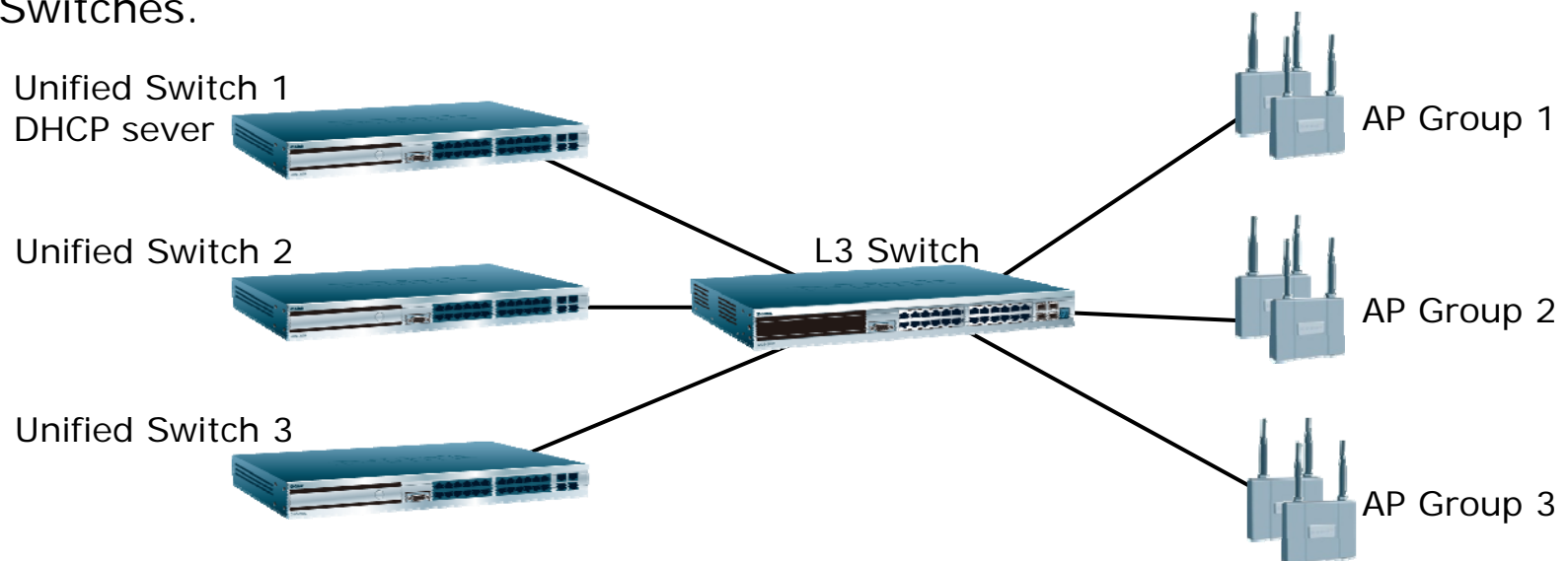
- This scenario shows how to setup fail over solution for DWS-4026 and how to use the AP Discovery with DHCP option 43
  
- **Objectives:**
  - Knowing how unified switches discover APs or how APs discover unified switches
  - Knowing the communication between Peer Switches
  - Understanding the configuration of DHCP option 43
  - Designing a correct redundancy solution for customer





### Network Topology

- Unified Switch 1 is in VLAN10, works as DHCP server and provides IPs for VLAN10, 20, 30.
- Unified Switch 2 is in VLAN20 while Unified Switch 3 is in VLAN30.
- L3 Switch creates three L3 Interfaces for VLAN10, 20 and 30, and handling the routing.
- To begin, the AP Group 1 is managed by Switch 1, AP Group 2 is managed by Switch 2, AP Group 3 is managed by Switch 3. If one of the Unified Switches crashes, its managed APs will automatically be managed by other Switches.





# Lab 1: Switch Redundancy

**Table 1: Physical Connection**

From Device	From Port	To Device	To Port
Unified Switch 1	1	L3 Switch	1
Unified Switch 2	7	L3 Switch	7
Unified Switch 3	13	L3 Switch	13
L3 Switch	4	AP Group 1	N/A
L3 Switch	10	AP Group 2	N/A
L3 Switch	16	AP Group 3	N/A

**Table 2: VLAN and Port Assignment**

Device	VLAN ID	VLAN Name	Tagged Ports	Untagged Ports
Unified Switch 1	10	VLAN10	N/A	1
Unified Switch 1	20	VLAN20	1	N/A
Unified Switch 1	30	VLAN30	1	N/A
L3 Switch	10	VLAN10	N/A	1-6
L3 Switch	20	VLAN20	1	7-12
L3 Switch	30	VLAN30	1	13-18



# Lab 1: Switch Redundancy

Table 3: IP Addressing

Device	Interface	VID	IP Address
Unified Switch 1	4/1	10	192.168.10.1/24
Unified Switch 1	4/2	20	192.168.20.2/24
Unified Switch 1	4/3	30	192.168.30.2/24
Unified Switch 2	Management	1	192.168.20.1/24
Unified Switch 3	Management	1	192.168.30.1/24
L3 Switch	ipif10	10	192.168.10.254/24
L3 Switch	ipif20	20	192.168.20.254/24
L3 Switch	ipif30	30	192.168.30.254/24

Table 4: DHCP Server

Device	Pool	Network	Excluded IP	Option 43
Unified Switch 1	VLAN10	192.168.10.0/24	192.168.10.1-100 192.168.10.200-255	0104.c0a8.0a01 0104.c0a8.1401 0104.c0a8.1e01
Unified Switch 1	VLAN20	192.168.20.0/24	192.168.20.1-100 192.168.20.200-255	0104.c0a8.1401 0104.c0a8.1e01 0104.c0a8.0a01
Unified Switch 1	VLAN30	192.168.30.0/24	192.168.30.1-100 192.168.30.200-255	0104.c0a8.1e01 0104.c0a8.0a01 0104.c0a8.1401



### Lab Scenario Discussion

- Is DHCP option 43 necessary in this scenario?
- Why need 3 VLANs?
- Why I need to create 3 VLANs on Unified Switch 1? Is that a necessary step?
- Why configuring tagged ports between Unified Switch 1 and L3 switch?
- Why disable L2 discovery but enable L3 discovery?



Session 4

# Working Principles of Basic Functions



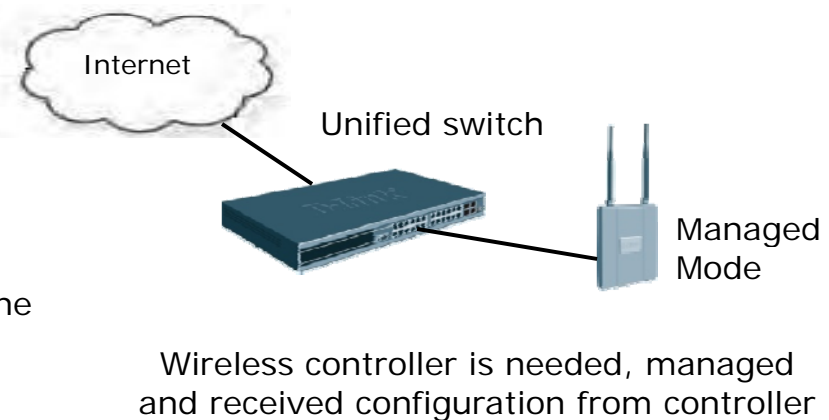
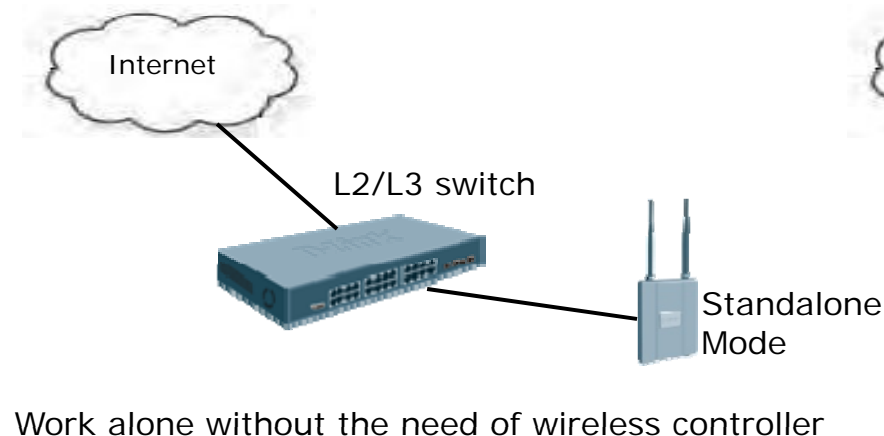
### **Session 4: Working Principles of Basic Functions**

- Standalone Mode and Managed Mode
- Virtual Access Point
- AP Channel and Power Management
- L3 Tunnel
- Fast Roaming
- Wi-Fi Multimedia
- Dynamic VLAN Assignment
- Advanced Management



## Standalone Mode and Managed Mode

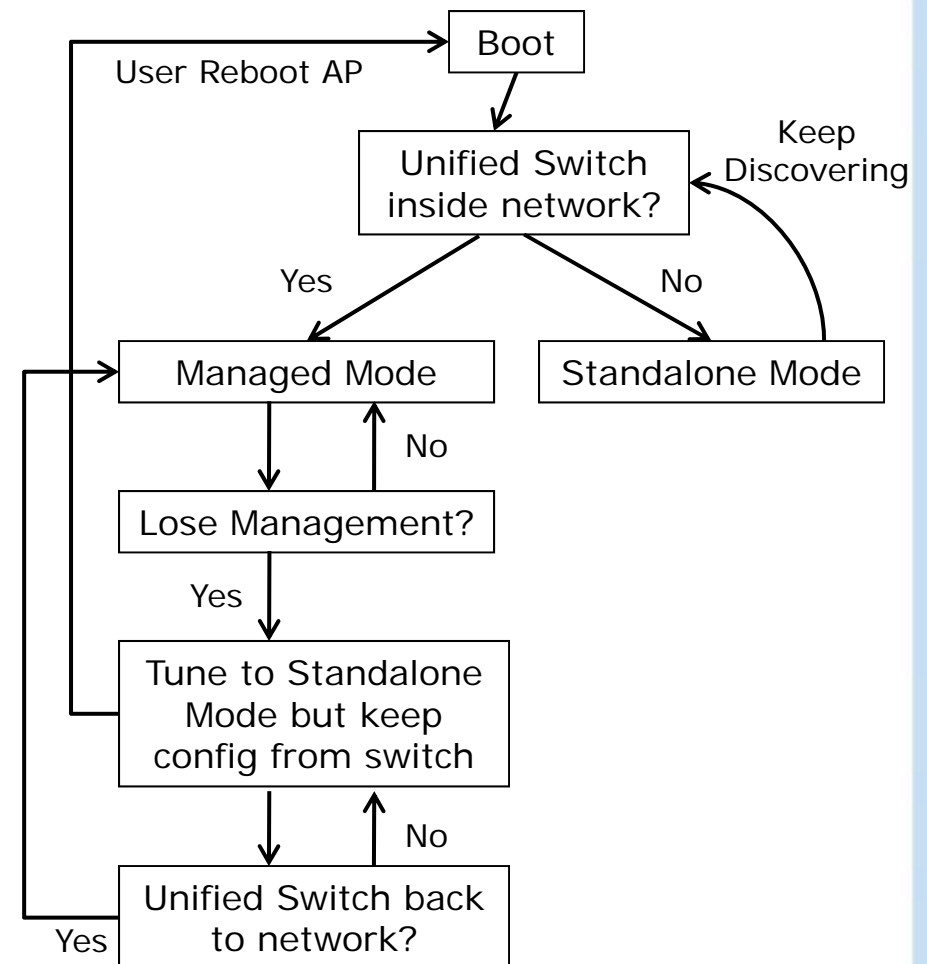
- D-Link Unified AP supports Standalone and Managed Modes.
- When the AP works as Managed Mode (often does), it works as a Thin AP. It is managed by Unified Switch and received configuration from the switch.
- When the AP be configured as Standalone Mode, it works as a Fat AP. It works alone, does not require a wireless controller.
- Standalone Mode supports WEB GUI but Managed Mode does not.





## Standalone Mode and Managed Mode (Cont.)

- When the Unified AP boots up, it will try to enter managed mode first. If there is no unified switch inside the network, it will turn to standalone mode.
- Once the managed AP loses the management from the switch, it will tune to standalone mode and **keep the current configuration until it reboots**.
- The current AP status can be checked by
  - Command “get managed-ap”, up is managed mode and down is standalone mode
  - WEB UI

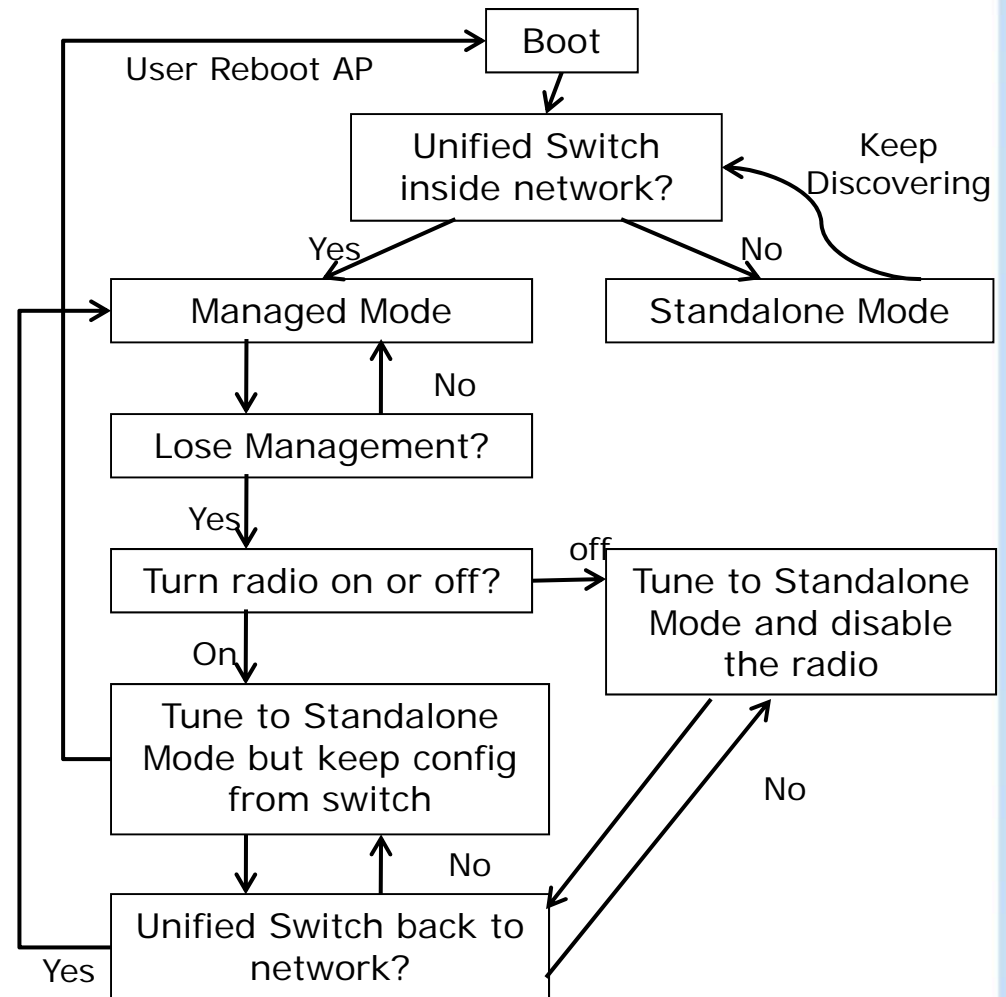






## Standalone Mode and Managed Mode (Cont.)

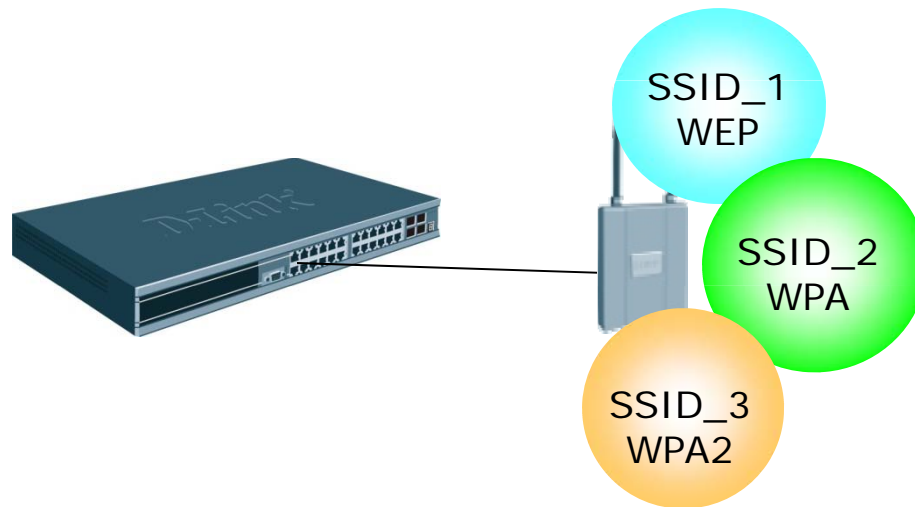
- For DWS-4026 R1 (currently), when the AP loses management from switch, the AP turn back to standalone mode and disable the radios.
- For DWS-4026 R2 (future release), when the AP loses management from switch, users will have a pre-option to disable the radio or not. If the radio is not disable, it will behave like DWS-3000 series.





# Virtual Access Point (VAP)

- It is also called SSID.
- A physical AP can provide multiple SSIDs.
- To the wireless clients, it appears to have many APs inside the network.
- Customer can classify users into different groups with VAP.
- It can isolate users by different SSIDs and security methods.



Site Survey

Available Network			
SSID	MAC(BSSID)	Sig	
Primary SSID	00:11:95:E0:EF:D8	Full	6
MSSID_1	00:11:95:E0:EF:D9	Full	6
MSSID_2	00:11:95:E0:EF:DA	Full	6

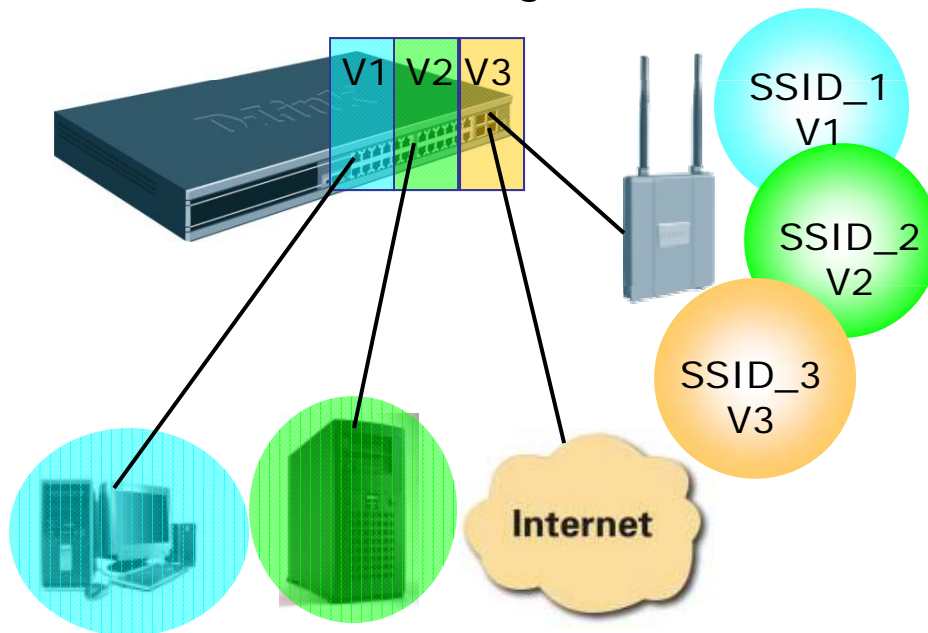


## Working Principles of Basic Functions

### ▪ Virtual Access Point

## Combine with VLAN Function

- An VID can be assigned SSID, wired and wireless users with the same VID form a VLAN group.
- When combining with VLAN function, the AP forwards wireless packets with the user-assigned tagged VID to wired network
- The AP must be connected to a switch which supports VLAN function with correct VLAN settings.



Global	Discovery	AAA / RADIUS	Radio	SSID	Valid AP
<b>Wireless Network Configuration</b>					
SSID	Dean			Security	<input type="radio"/> None <input type="radio"/> WEP <input checked="" type="radio"/> WPA/WPA2
Hide SSID	<input type="checkbox"/>				<input checked="" type="radio"/> WPA Personal <input type="radio"/> WPA Enterprise
VLAN	20 (1 to 4094)			WPA Versions	<input checked="" type="checkbox"/> WPA <input type="checkbox"/> WPA2
L3 Tunnel	<input type="checkbox"/>			WPA Ciphers	<input checked="" type="checkbox"/> TKIP <input checked="" type="checkbox"/> CCMP(AES)
L3 Tunnel Status	None			WPA Key Type	ASCII
L3 Tunnel Subnet	0.0.0.0			Passphrase	
L3 Tunnel Mask	255.255.255.0				
MAC Authentication	<input type="radio"/> Local <input type="radio"/> Radius <input checked="" type="radio"/> Disable				
RADIUS IP Address	0.0.0.0 <input checked="" type="checkbox"/> Use Profile				
RADIUS Secret					
RADIUS Accounting	<input type="checkbox"/>				



### VAP Features

- DWL-3500AP supports 8 SSIDs on 2.4GHz
- DWL-8500AP supports 8 SSIDs on both 2.4/5GHz, total 16 SSIDs
- DWL-8600AP supports 16 SSIDs on both 2.4/5GHz, total 32 SSIDs
- VAP function procedure:
  - Create and configure a new SSID
  - Assign this SSID to specific AP Profile
  - Apply the profile to APs
- DWS-3000 series create 8 SSIDs (VAPs) by default and DWS-4026 create 16 SSIDs. Users can choose to use the default VAP settings.
- Note: Same SSID can be assigned to different profiles or same profile with different radio



## Working Principles of Basic Functions

- Virtual Access Point

### Create New SSID (Wireless Networks)

LAN WLAN

DWS-4026

- Security
- Monitoring
- Administration
  - Basic Setup
  - AP Management
  - Advanced Configuration
    - Global
    - Networks**
    - AP Profile
    - Peer Switch
    - WIDS Security
  - Clients
- WLAN Visualization

ID	SSID	VLAN	Hide SSID	L3 Tunnel	Security	Redirect
1	dlink1	1-Default	Disabled	Disabled	None	None
2	dlink2	1-Default	Disabled	Disabled	None	None
3	dlink3	1-Default	Disabled	Disabled	None	None
4	dlink4	1-Default	Disabled	Disabled	None	None
5	dlink5	1-Default	Disabled	Disabled	None	None
6	dlink6	1-Default	Disabled	Disabled	None	None
7	dlink7	1-Default	Disabled	Disabled	None	None
8	dlink8	1-Default	Disabled	Disabled	None	None
9	dlink9	1-Default	Disabled	Disabled	None	None
10	dlink10	1-Default	Disabled	Disabled	None	None
11	dlink11	1-Default	Disabled	Disabled	None	None
12	dlink12	1-Default	Disabled	Disabled	None	None
13	dlink13	1-Default	Disabled	Disabled	None	None
14	dlink14	1-Default	Disabled	Disabled	None	None
15	dlink15	1-Default	Disabled	Disabled	None	None
16	dlink16	1-Default	Disabled	Disabled	None	None

SSID17

Configure up to 64 unique SSIDs (wireless networks)

LAN WLAN

DWS-4026

- Security
- Monitoring
- Administration
  - Basic Setup
  - AP Management
  - Advanced Configuration
    - Global
    - Networks
    - AP Profile**
    - Peer Switch
    - WIDS Security
  - Clients
- WLAN Visualization

Access Point Profile VAP Configuration

AP Profile 2-Profile

☒ 1-802.11a/n ☐ 2-802.11b/g/n

Network	VLAN	L3 Tunnel	Hide SSID	Security	Redirect
<input checked="" type="checkbox"/> 1 - dlink1 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 1 - dlink1 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 2 - dlink2 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 3 - dlink3 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 4 - dlink4 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 5 - dlink5 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 6 - dlink6 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 7 - dlink7 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 8 - dlink8 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 9 - dlink9 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 10 - dlink10 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 11 - dlink11 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 12 - dlink12 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 13 - dlink13 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 14 - dlink14 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 15 - dlink15 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 16 - dlink16 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 17 - SSID17 <input type="button" value="Edit"/>	1-Default	Disabled	Disabled	None	None

Apply different SSIDs for new AP profile manually (Apply to AP)



# AP Channel Assignment

- Two methods of Channel Assignment:
  - Static assign
    - Through valid AP database (fix the channel)
    - Managed AP Advanced (run-time only)

The screenshot displays the D-Link management interface. On the left, a sidebar shows a tree view with 'WLAN Visualization' selected. The main panel features tabs for 'Global', 'Discovery', 'Profile', 'Radio', 'SSID', 'Valid AP', and 'OUI'. The 'Valid AP' tab is active, showing a 'Valid Access Point Configuration' window. This window includes fields for 'MAC Address' (00:11:95:A3:7D:50), 'Managed Mode' (WS Managed), 'Location', 'Authentication Password', and 'Profile' (1 - Default). Below these are two radio configuration sections: 'Radio 1 - 802.11a' and 'Radio 2 - 802.11g'. Each has a 'Channel' dropdown and a 'Power (%)' field. The 'Radio 1' channel is set to 165 and 'Radio 2' to 11. A 'Delete' button and a 'Refresh' button are visible. A dropdown menu is open for the 'Radio 2' channel, showing options 1 through 11, with 'Auto' at the top. The 'Back' button is also visible.

- Automatic (two methods)
  - Initial Channel Selection (ICS)
  - Auto Channel Adjustment (ACA)



# AP Channel Assignment

- Initial Channel Selection (ICS)
  - Each time the AP reboot or managed by switch, the mechanism runs to select the initial operating channel.
  - In DWS-4026, the AP chooses one channel at random from eligible channels which could be configured by customer and makes this channel the operational channel.
  - For DWS-3000 series, only channels 1, 6, 11 are available.

The screenshot shows the D-Link web interface for configuring an AP. The left sidebar shows the navigation tree with 'AP Profile' selected. The main content area displays various configuration settings for the AP, including RF management parameters.

Setting	Value	Range/Options
RTS Threshold (bytes)	2347	(0 to 2347)
Load Balancing	<input type="checkbox"/>	
Load Utilization (%)	60	(1 to 100)
Maximum Clients	200	(0 to 200)
RF Scan Other Channels	<input checked="" type="checkbox"/>	
RF Scan Sentry	<input type="checkbox"/>	
RF Scan Interval (secs)	60	(30 to 120)
RF Scan Sentry Channels	<input checked="" type="checkbox"/> 802.11a/g <input checked="" type="checkbox"/> 2.11b/g	
RF Scan Duration (msecs)	10	(10 to 2000)
Rate Limiting	<input type="checkbox"/>	
Rate Limit (pkts/sec)	50	(1 to 50)
Rate Limit Burst (pkts/sec)	75	(1 to 75)
Channel Bandwidth	20 MHz	
Protection	Auto	
No ACK	Disable	
DTIM Period (# beacons)	10	(1 to 255)
Beacon Interval (msecs)	100	(20 to 2000)
Automatic Channel	<input checked="" type="checkbox"/>	
Automatic Power	<input checked="" type="checkbox"/>	
Initial Power (%)	100	(1 to 100)
U-APSD Mode	Enable	
Frag Threshold (bytes)	2346	(256 to 2346)
Short Retries	7	
Long Retries	4	
Transmit Lifetime (msecs)	512	
Receive Lifetime (msecs)	512	
Station Isolation	<input type="checkbox"/>	
Primary Channel	Lower	
Short Guard Interval	Enable	
Multicast Tx Rate (Mbps)	Auto	

Supported Channels	1	2	3	4	5	6	7	8	9	10	11	
Auto Eligible	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Rate Sets (Mbps)	1	2	5.5	6	9	11	12	18	24	36	48	54
Basic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Supported	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>





# AP Channel Assignment

- Auto Channel Adjustment (ACA)
  - The Unified Switch periodically evaluates the operational channel and changes the channel if the current channel is noisy
- Switch decide which channel to use by:
  - RSSI readings from managed APs
  - Comparing the transmission/reception error rates
- Three ways to configure ACA
  - Fixed Time (Plan is calculated once every 24 hours at the specified time)
  - Manual (Users initiate the calculation of the channel plan)
  - Interval (Switch periodically calculates the channel plan, 6-24 hours)

**Configuration** Channel Plan History Manual Channel Plan Manual Power Adjustments

**RF Configuration**

Channel Plan	<input checked="" type="radio"/> 5 GHz (802.11 a/n) <input type="radio"/> 2.4 GHz (802.11 b/g/n)
Channel Plan Mode	<input type="radio"/> Fixed Time <input checked="" type="radio"/> Manual <input type="radio"/> Interval
Channel Plan History Depth	5 (0 to 10)
Channel Plan Interval (hours)	6 (6 to 24)
Channel Plan Fixed Time (hh:mm)	0 : 0





## Automatic Channel Selection Limitation

- The automatic channel selection algorithm does not affect APs with the following conditions:
  - The channel is statically assigned.
  - The AP uses a profile that has the Automatic Channel field disabled (Radio Configuration Setting).
  - Channel plan algorithm does not support radios using Super A/G.
  - When running the ICS, the neighboring APs may use the same channel because the channel is randomly assigned.
  - If there is no wireless clients in the network, which means there is no wireless data in the network. The APs are not able to select the best channel (may choose the same channel) because the error rate database is insufficient to make the best decision.

State	<input checked="" type="radio"/> On <input type="radio"/> Off	Mode	IEEE 802.11a/n <span>▼</span>
RTS Threshold (bytes)	2347 (0 to 2347)	DTIM Period (# beacons)	10 (1 to 255)
Load Balancing	<input type="checkbox"/>	Beacon Interval (msecs)	100 (20 to 2000)
Load Utilization (%)	60 (1 to 100)	Automatic Channel	<input checked="" type="checkbox"/>
Maximum Clients	200 (0 to 200)	Automatic Power	<input checked="" type="checkbox"/>
RF Scan Other Channels	<input checked="" type="checkbox"/>	Initial Power (%)	100 (1 to 100)
RF Scan Sentry	<input type="checkbox"/>		



# AP Power Assignment

- Two methods to assign the power of AP
  - Static
  - Automatic
- Static Assignment
  - Web GUI has only four options to fix the power through valid AP database (same as static channel)
  - Command line can support more options
    - (Config-wireless)#ap database 00:17:9a:d2:8d:70
    - (Config-ap)#radio 2 power 70
  - Managed AP Advanced (run-time only)

LAN WLAN Tool

Global Discovery Profile Radio SSID Valid AP OUI

### Valid Access Point Configuration

MAC address	00:22:b0:3d:97:00		
AP Mode	Managed		
Location			
Authentication Password			
Profile	1 - Default		
Radio 1 - 802.11a/n	Channel	Auto	Power (%) 0
Radio 2 - 802.11b/g/n	Channel	Auto	Power (%) 0

Refresh Delete Submit

12.5% (Max-9db)  
25% (Max-6db)  
50% (Max-3db)  
100% (Max)



## AP Power Assignment

- Automatic Power Assignment
  - The Unified Switch monitors the AP's statistics to adjust the power when necessary, if the AP's power level is not manually setup.
  - Power level is a percentage of maximum power.
  - The switch sets the initial power of the AP to the value specified in the profile.
  - The algorithm increases or reduces the power level in 10% increments.
- The Unified Switch uses the following statistics to make the power adjustment decision:
  - Increase in duplicate packets from client (ACKs cannot reach clients)
  - Increase in re-transmissions (ACKs cannot reach AP)



# AP Power Assignment

- Two way to configure Auto Power Adjustment
  - Interval (15-1440 minutes)
  - Manual

The screenshot displays the D-Link AP Management web interface. On the left is a navigation tree with the following items: DWS-4026, Security, Monitoring, Administration, Basic Setup, AP Management, Reset, RF Management (highlighted), Software Download, Advanced Settings, Advanced Configuration, Global, Networks, AP Profile, and Peer Switch. The main content area is titled 'RF Configuration' and contains the following settings:

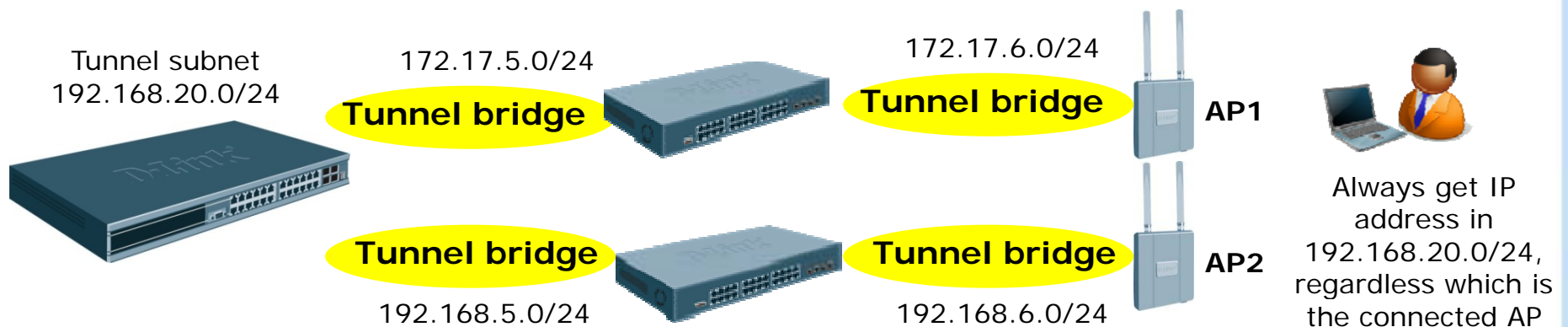
Configuration	
Channel Plan	<input checked="" type="radio"/> 5 GHz (802.11 a/n) <input type="radio"/> 2.4 GHz (802.11 b/g/n)
Channel Plan Mode	<input type="radio"/> Fixed Time <input checked="" type="radio"/> Manual <input type="radio"/> Interval
Channel Plan History Depth	5 (0 to 10)
Channel Plan Interval (hours)	6 (6 to 24)
Channel Plan Fixed Time (hh:mm)	0 : 0
Power Adjustment Mode	<input checked="" type="radio"/> Manual <input type="radio"/> Interval
Power Adjustment Interval (minutes)	15 (15 to 1440)
<input type="button" value="Submit"/>	

- Note: The algorithm never reduces the AP power below the initial power setting in the profile (Default is 100%). Therefore if the initial power setting is 100% in the profile then the auto power adjustment algorithm has no effect on the AP.



### Layer 3 Tunnel

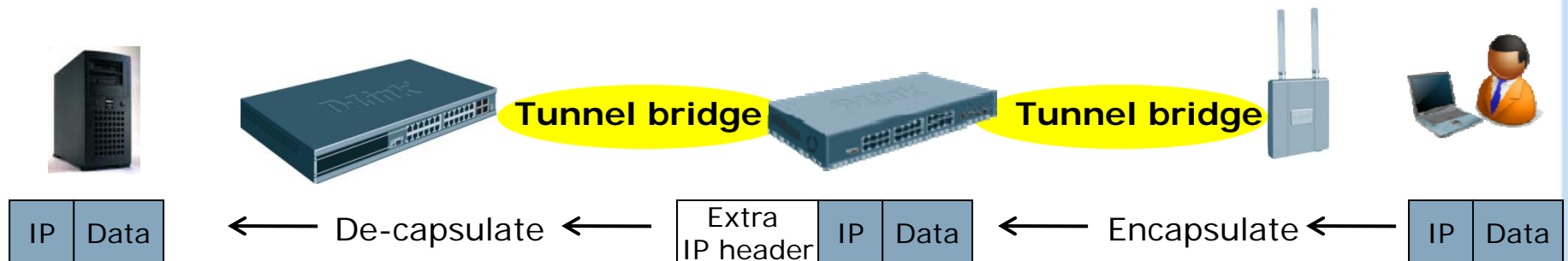
- Layer 3 (L3) Tunnel, also called IP-IP tunnel, is supported by D-Link Unified Solution to build a bridge between switch and APs regardless the number of L3 network subnets they pass through.
- Within this tunnel, the mobile stations can maintain the same IP connections while roaming from one AP to another AP even when these APs are attached to different IP subnets.
- This feature is especially useful for environments that use wireless Voice over IP (VoIP) on the 802.11 networks with multiple subnets.





## Layer 3 Tunnel

- When configuring L3 tunnel mode, the switch establishes an IP-IP tunnel to the APs that are configured for tunneling mode.
- The tunnel will encapsulate IPv4 packets inside an extra IPv4 packets.
- Both the switch and the AP perform tunnel encapsulation and de-encapsulation.
  - The AP uses the Unified Switch IP address as the destination IP in the outer IP header and itself as the source IP.
  - The Unified Switch uses the AP IP address as the destination IP in the outer IP header and itself as the source IP.

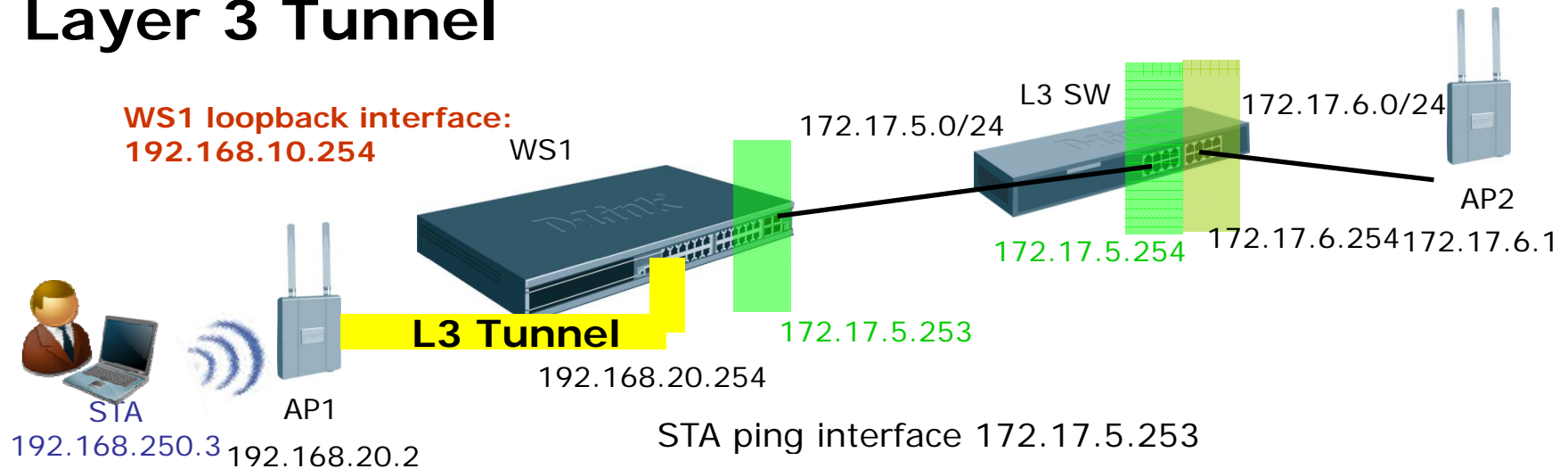




## Working Principles of Basic Functions

### ▪ Layer 3 Tunnel

# Layer 3 Tunnel



File Edit View Go Capture Analyze Statistics Help					
No. Time Source Destination Protocol Info					
12086	1070.583552	192.168.20.2	192.168.10.254	UDP	Source port: 57776 Destination port: 57776
12087	1070.588203	192.168.20.2	192.168.10.254	UDP	Source port: 57776 Destination port: 57776
12088	1071.038600	192.168.250.3	172.17.5.253	ICMP	Echo (ping) request
12089	1071.039352	172.17.5.253	192.168.250.3	ICMP	Echo (ping) reply
12090	1071.545257	192.168.20.2	192.168.10.254	UDP	Source port: 57776 Destination port: 57776

Frame 12088 (94 bytes on wire, 94 bytes captured)

Ethernet II, Src: 00:19:5b:00:00:00, Dst: 00:17:9a:95:01:ca

Internet Protocol, Src Addr: 192.168.20.2 (192.168.20.2), Dst Addr: 192.168.10.254 (192.168.10.254) **AP1 / WS1**

Internet Protocol, Src Addr: 192.168.250.3 (192.168.250.3), Dst Addr: 172.17.5.253 (172.17.5.253) **STA / Interface**

Internet Control Message Protocol





# L3 Tunnel Configuration

- To create an individual VLAN and IP subnet, the wired equipment and roaming wireless clients have to be in the same L3 tunnel subnet.
- Routing is enabled on each switch.
- L3 tunnel is enabled based on SSID (go through Basic Setup → SSID )
- NOTE: When L3 tunneling is enabled the VLAN ID is not used.

Global | Discovery | AAA / RADIUS | Radio | **SSID** | Valid AP

### Wireless Default VAP Configuration

AP Profile 1-Default

☐ 1-802.11a ☒ 2-802.11g

Network	VLAN	L3 Tunnel	Hide SSID	Security
<input checked="" type="checkbox"/> 1 - L3 Tunnel <span>Edit</span>	1-Default	Enabled	Disabled	None
<input checked="" type="checkbox"/> 2 - Managed SSID 2 <span>Edit</span>	1-Default	Enabled	Disabled	None
<input type="checkbox"/> 3 - Managed SSID 3 <span>Edit</span>	1-Default	Disabled	Disabled	None
<input type="checkbox"/> 4 - Managed SSID 4 <span>Edit</span>	1-Default	Disabled	Disabled	None
<input type="checkbox"/> 5 - Managed SSID 5 <span>Edit</span>	1-Default	Disabled	Disabled	None
<input type="checkbox"/> 6 - Managed SSID 6 <span>Edit</span>	1-Default	Disabled	Disabled	None
<input type="checkbox"/> 7 - Managed SSID 7 <span>Edit</span>	1-Default	Disabled	Disabled	None
<input type="checkbox"/> 8 - Managed SSID 8 <span>Edit</span>	1-Default	Disabled	Disabled	None

Refresh Submit Next

Global | Discovery | AAA / RADIUS | Radio | **SSID** | Valid AP

### Wireless Network Configuration

SSID	L3 Tunnel
Hide SSID	<input type="checkbox"/>
VLAN	1 (1 to 4094)
L3 Tunnel	<input checked="" type="checkbox"/>
L3 Tunnel Status	Not Configured - Routing Disabled
L3 Tunnel Subnet	192.168.1.0
L3 Tunnel Mask	255.255.255.0
MAC Authentication	<input type="radio"/> Local <input type="radio"/> Radius <input checked="" type="radio"/> Disable
RADIUS IP Address	0.0.0.0 <input checked="" type="checkbox"/> Use Profile
RADIUS Secret	<input type="text"/> <span>Edit</span>
RADIUS Accounting	<input type="checkbox"/>





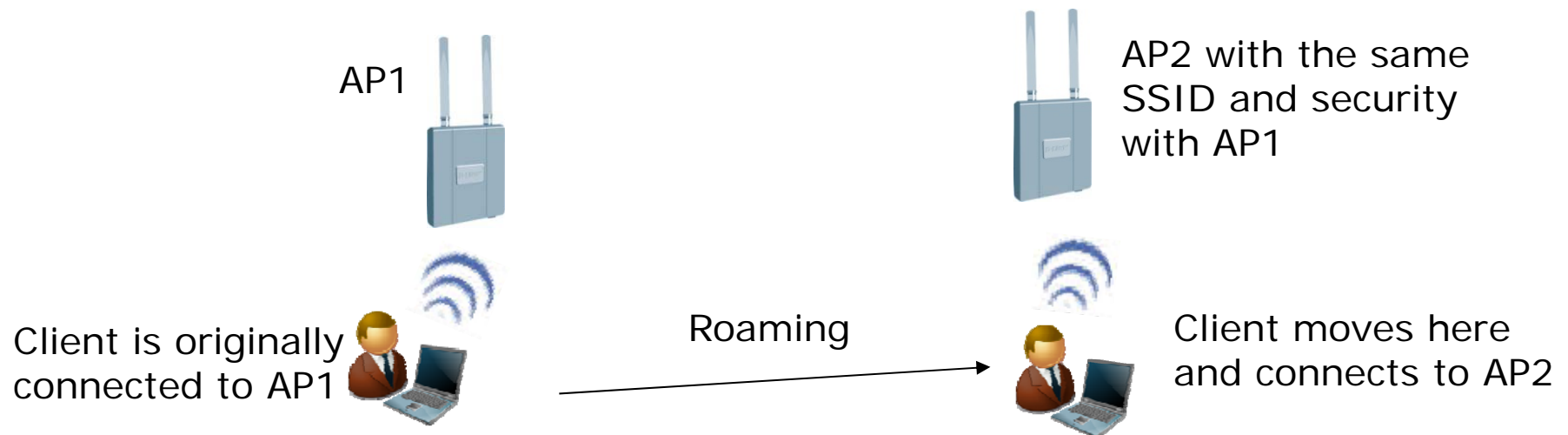
## Layer 3 Tunnel Limitation

- Tunneled packets have extra 20 bytes in header for all devices. It does TCP MSS Reduction to avoid the frame over-sizing issue.
- IPv6 clients are not supported on tunneled interfaces.
- Only unicast IPv4 traffic is tunneled in hardware.
- Multicast traffic and Non-IP traffic are tunneled in software.
  - Slower
  - Cause network congestion
- All devices that use the L3 tunnel network are stored in the ARP cache because the wireless subnet is local to the switch (ARP cache fills up faster than expected).



# What is Roaming?

- A wireless client connects to an AP first. Next, this client moves to another location which is too far from the original AP to keep connected, so this client disconnects from the original AP and tries to connect to a new AP.
- To allow wireless client to roam, all the APs need to have the same SSID and security.
- Roaming behavior is controlled by wireless client, D-Link Access Points provide solutions to speed up this behavior.



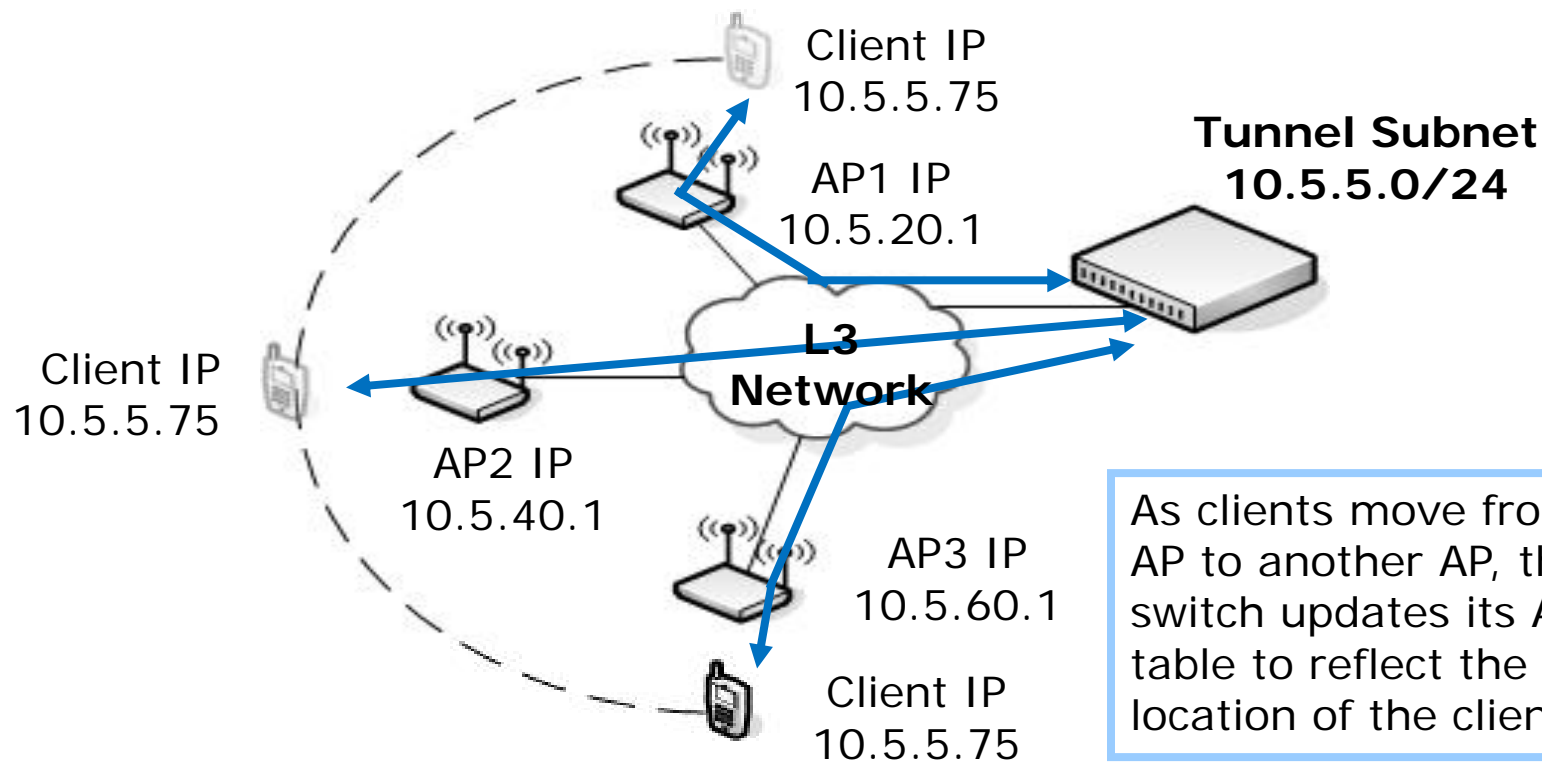


## Seamless Fast Roaming

- To speed up the hand over time of the roaming behavior, D-Link unified solution implements seamless roaming solution with the following.
  - Keep the client's IP address while it roams (L3 Tunnel Mode)
    - The wireless client can keep its IP address after roaming to another AP, regardless it is a L2 or L3 roaming. Even these two APs are in the different subnets, the client can continue keep the same IP address.
  - Re-authentication can be avoided or shorten re-authentication time
    - WPA2 Pre-Authentication (WPA2-PSK & Enterprise)
    - WPA2 Key Caching (WPA2-PSK & Enterprise)
    - Dynamic Key Forwarding (WPA2-Enterprise)
- Note: Dynamic WEP / WPA Enterprise does not supported by fast roaming function

# Seaming Fast Roaming – Keep IP Address

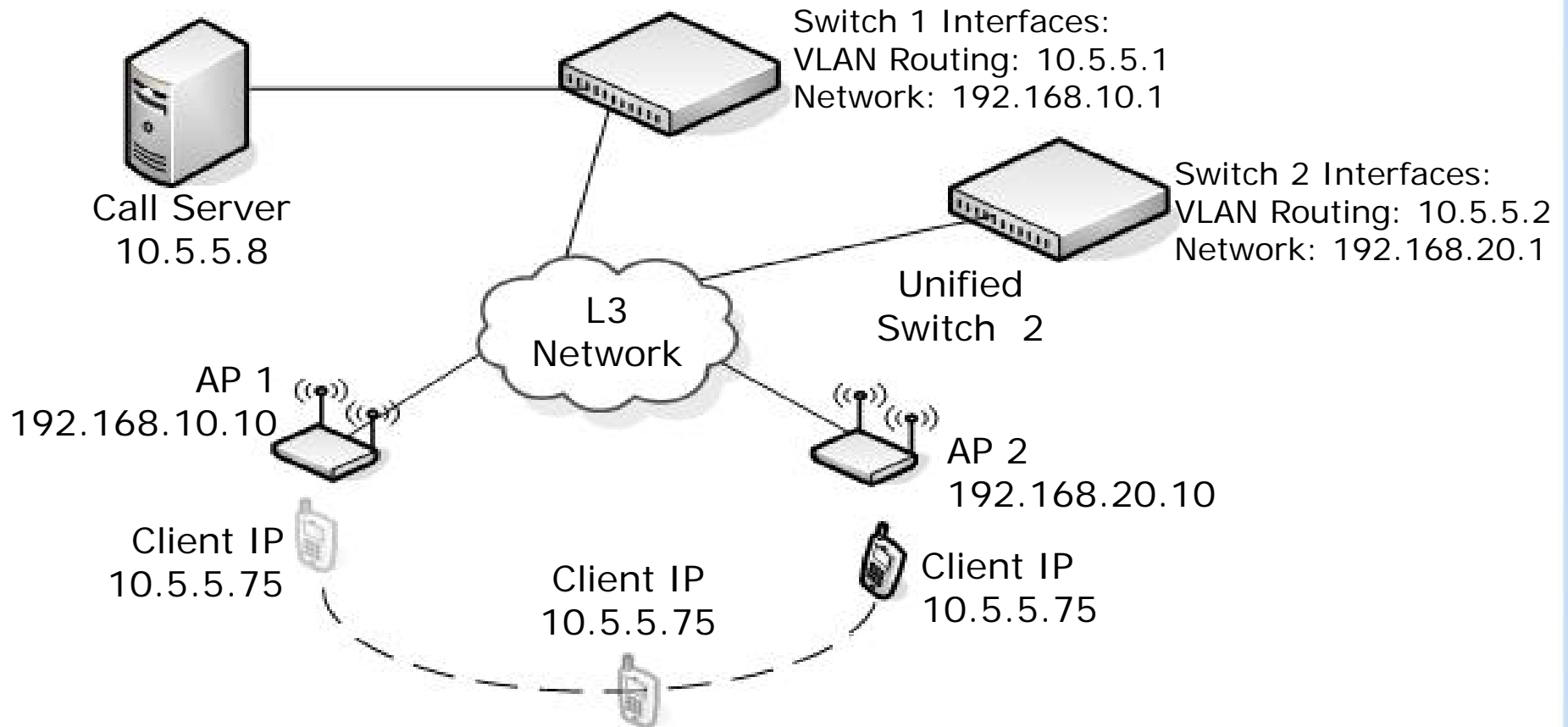
- With the tunnel function on D-Link Unified solution, the wireless clients can roam to different APs in different network subnets without renewing the IP address. This will save lots of updating time.





## Seaming Fast Roaming – Keep IP Address

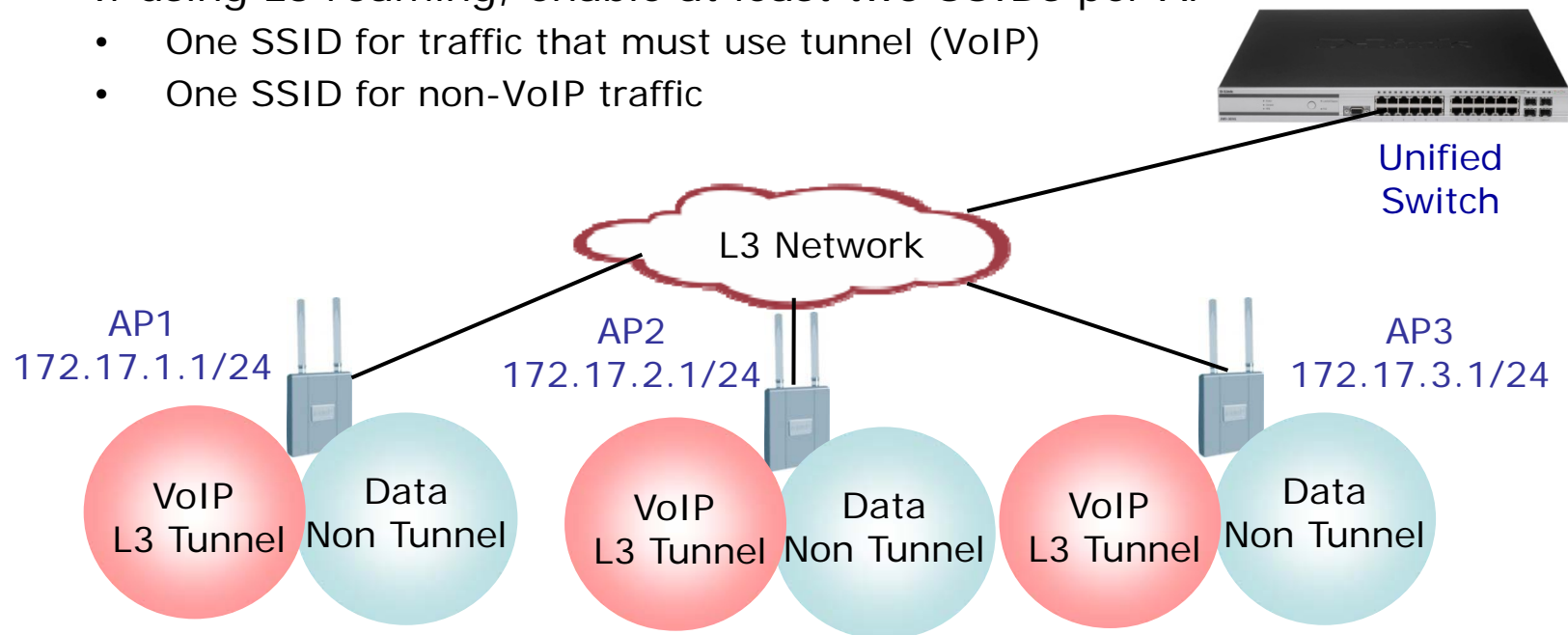
- It supports seamless roaming across peer switch too.





## Seaming Fast Roaming – Keep IP Address

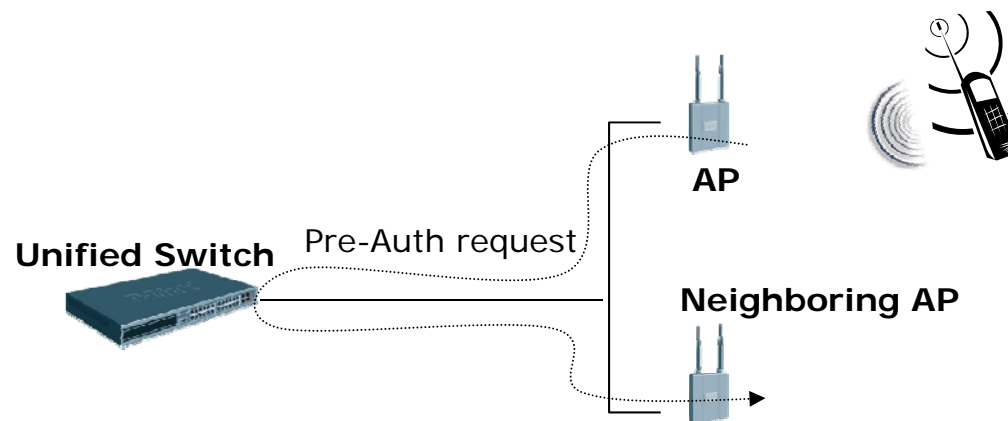
- It is only used for time-sensitive roaming traffic, such as IP mobile telephone.
- Typically this feature is for customer to deploy in VoIP environment, general data traffic does NOT necessary require this function.
- If using L3 roaming, enable at least two SSIDs per AP
  - One SSID for traffic that must use tunnel (VoIP)
  - One SSID for non-VoIP traffic





# Shorten Re-Authentication Time when Roaming

- WPA2 Pre-authentication (WPA2-PSK & Enterprise)
  - The client can attempt to authenticate to other APs within range.
  - D-Link's implementation – Pre-Auth request will be forwarded by the Unified Switch to the neighboring AP.

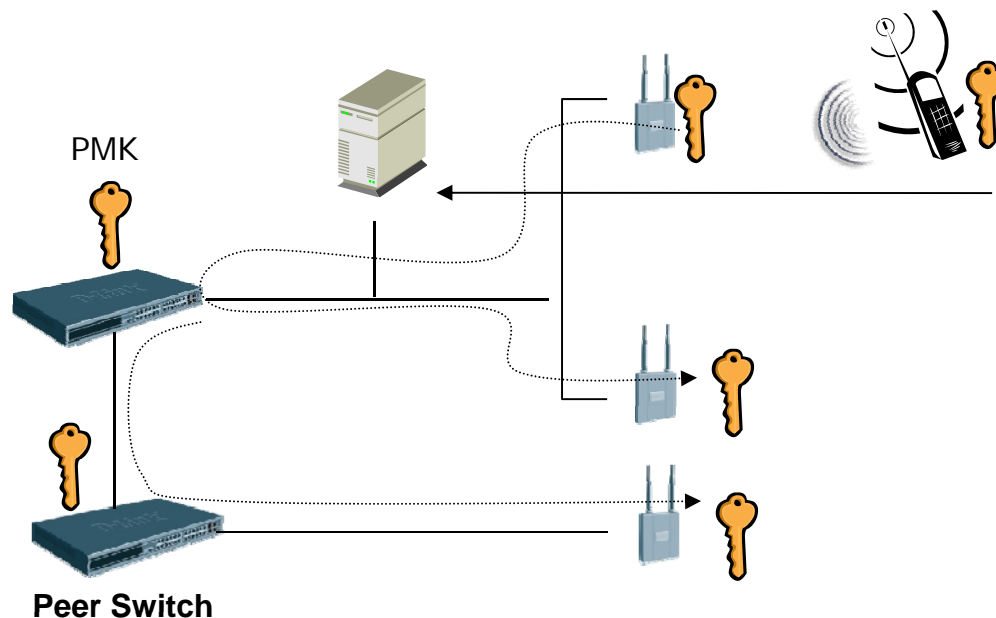


- WPA2 Key Caching (WPA2-PSK & Enterprise)
  - The AP & Clients will retain the PMK key generated for each session.
  - When the client roams to another AP and then roams back, re-authentication is not necessary



# Shorten Re-Authentication Time when Roaming

- Dynamic Key Forwarding (WPA2-Enterprise)
  - D-Link's implementation (Non-Standard)



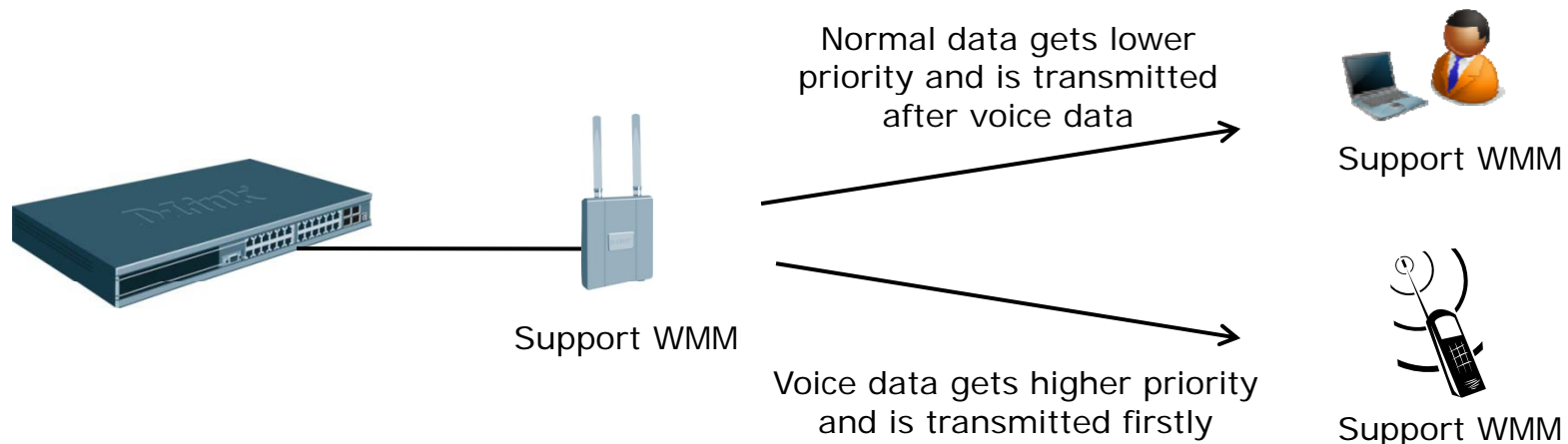
- Key Forwarding:
  - Authenticated with RADIUS Server
  - PMK key generated
  - PMK (Pair wise Master Key) can be cached in Switch and forwarded to APs in the same roaming group
  - When client roaming to other AP, it will send the PMK ID to the new AP.





# Wi-Fi Multimedia

- Wi-Fi Multimedia (WMM) is an optional Wi-Fi Alliance interoperability certification, based on Enhanced Distributed Channel Access (EDCA) of the IEEE 802.11e standard.
- WMM provides basic Quality of service (QoS) features to IEEE 802.11 networks, multimedia applications including voice, video data could get higher priority.
- Devices which pass the Wi-Fi WMM certification are guaranteed to work with each other.
- To make WMM works, both AP and client have to support it.





# WMM Operating

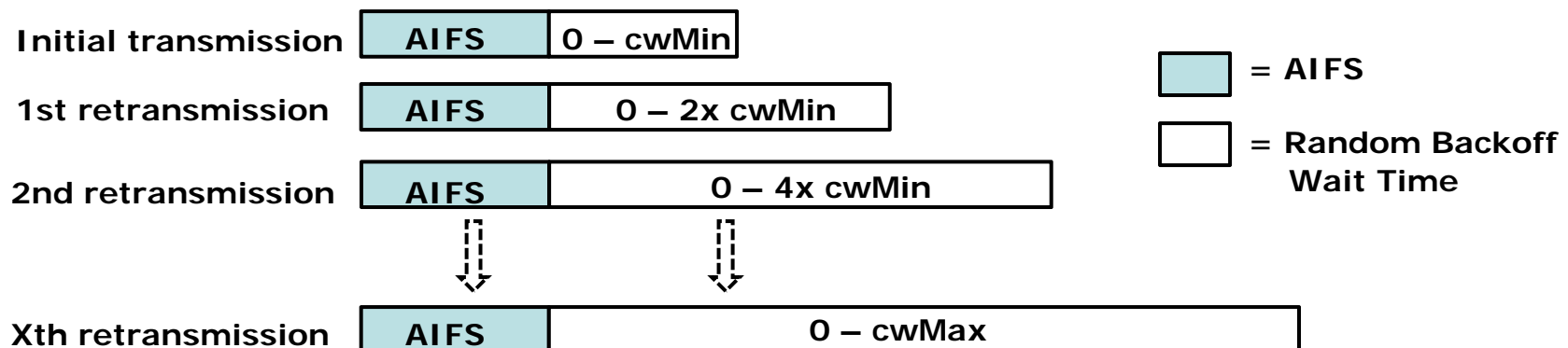
- For legacy 802.11 network, CSMA/CA-based Distributed Coordination Function (DCF) is used for transmit data which avoids the collision condition. Each client has to wait for a random backoff time. If there is no other clients transmitting, the client will get the permission and start to deliver the data
- With DCF, all the clients get the same priority
- WMM defines 4 Access Categories, Voice, Video, Best Effort, and Background. The categories are mapped to different priorities which are defined in IEEE 802.1p.
- The default priority is Best Effort

Access Category	Description	IEEE 802.1p priority
Voice	Highest priority	7, 6
Video	Prioritize video traffic above other data traffic	5, 4
Best Effort	Traffic from legacy devices, or traffic from applications or devices that lack QoS capabilities	0, 3
Background	Low priority traffic (file downloads, print jobs) that does not have strict latency and throughput requirements	2, 1



# WMM Operating

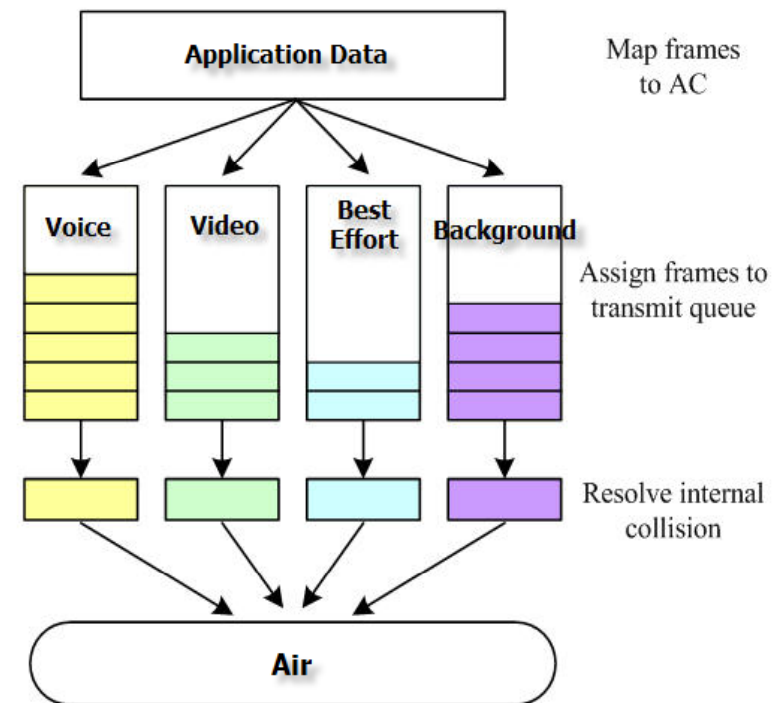
- WMM is an extension to the legacy CSMA/CA-based DCF mechanism
- Each time when AP transmits a packet, it wait for a specific period of time, defined by AIFS (Arbitration Interframe Space ) and listen for contention.
- After the waiting time of AIFS, AP starts to count down a random backoff wait time from 0 to the value defined by the Minimum Contention Window (cwMin).
- If the random backoff time ends and a collision is detected, the AP select a random time again and retry, but doubles the time range. The retry and doubling behavior continues (if collisions remain there) until reach the value specified in the Maximum Contention Window (cwMax) or packet has been sent/discarded.





## WMM Operating

- If the random backoff time ends and no collision is detected, AP starts to transmit this packet
- WMM enabled devices create four queues for different categories, data packets will be assigned to different queues according to its access category and priority.
- Each queue follows the described mechanism and is configured with different AIFS, cwMin, cwMax parameters.
- Queues with higher priority are configured with lower AIFS/cwMin/cwMax (lower waiting time) to make sure the packet has higher chances to be transmitted.





# WMM Setup

- WMM setup is base on AP Profile and enabled by default.
- Customer can setup AP EDCA Parameters which affect the traffics from AP to client or Station EDCA Parameters which affect the traffics from client to AP.
- TXOP: The Transmission Opportunity is the time period that a client who has won the control of the shared medium can retain it.
- Max. Burst: This value is the maximum burst time length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information.

LAN WLAN

DWS-4026

- Security
- Monitoring
- Administration
  - Basic Setup
  - AP Management
  - Advanced Configuration
    - Global
    - Networks
    - AP Profile
    - Peer Switch
    - WIDS Security
  - Clients
- WLAN Visualization

### Access Point Profile QoS Configuration

AP Profile 1-Default

☐ 1-802.11a/n ☒ 2-802.11b/g/n

AP EDCA Parameters				
Queue	AIFS (msecs)	cwMin (msecs)	cwMax (msecs)	Max. Burst (µsecs)
Data 0 (Voice)	1	3	7	1500
Data 1 (Video)	1	7	15	3000
Data 2 (Best Effort)	3	15	63	0
Data 3 (Background)	7	15	1023	0

WMM Mode ☒

Station EDCA Parameters				
Queue	AIFS (msecs)	cwMin (msecs)	cwMax (msecs)	TXOP Limit (msecs)
Data 0 (Voice)	2	3	7	47
Data 1 (Video)	2	7	15	94
Data 2 (Best Effort)	3	15	63	0
Data 3 (Background)	7	15	1023	0



### WMM Limitation

- Both AP and clients have to be certified by Wi-Fi for WMM and has WMM enabled.
- The source application on clients (for instance VoIP) must supports WMM.
- APs with WMM can accept IEEE802.1p priorities from wired network and could map its priorities to IEEE802.1p, too. But it doesn't take effect if WMM is disabled.
- IEEE802.1p has priorities from 0 to 7, higher number has higher priority, and same does WMM, but an exception existed that 0 is higher than 1&2.

#### Wi-Fi CERTIFIED™ Interoperability Certificate

Certification ID: WFA7771



This certificate lists the capabilities and features that have successfully completed Wi-Fi Alliance interoperability testing. Additional information about Wi-Fi Alliance certification programs is available at [www.wi-fi.org/certification\\_programs.php](http://www.wi-fi.org/certification_programs.php).

Tested Spatial Streams	Dual-Band Concurrent Maximum
Transmit	2
Receive	2

Certificate Date: August 28, 2009  
Company: D-Link Systems  
Product: D-Link Dual Band PoE Access Point / DWL-8600AP  
Model/SKU #: DWL-8600AP/  
Category: Enterprise Access Point, Switch/Controller or Router

IEEE Standard	Security	Multimedia
IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n draft 2.0 IEEE 802.11d IEEE 802.11h  <u>Optional 802.11n Capabilities</u> - Short Guard Interval - 40 MHz operation in 5 GHz - HT Duplicate (MCS 32)	WPA™ - Enterprise, Personal WPA2™ - Enterprise, Personal  <u>EAP Type(s)</u> EAP-TLS EAP-TTLS/MSCHAPv2 PEAPv0/EAP-MSCHAPv2 PEAPv1/EAP-GTC EAP-SIM	WMM®



## Dynamic VLAN Assignment

- The clients get assigned to the appropriate VLAN that is configured in the RADIUS server regardless which port or SSID they connect to.
- Flexibility for the clients to move around the network without much configuration required by the administrator.
- Users have to pass the 802.1X authentication before they can access the network.
- Based on the username, the RADIUS server will dynamically assign the clients to different VLANs.
- It forces the specific user be assigned to specific VLAN.
- It can authenticate both wired and wireless clients.
- It does not support fast roaming.





### Configuration Example

- Enable wired dynamic VLAN assignment globally from the Web GUI through LAN → Security → 802.1X → 802.1X Setting → VLAN Assignment Mode
- RADIUS Tunnel Attributes used
  - Tunnel-Type=VLAN (13)
  - Tunnel-Medium-Type=802
  - Tunnel-Private-Group-ID= VLANID
- Wireless dynamic VLAN function is supported by default, just leave the VID of the SSID as 1.

The screenshot shows the 'Edit Dial-in Profile' window with the 'Advanced' tab selected. Under the 'Attributes' section, a table lists RADIUS attributes. The 'Tunnel-Medium-Type', 'Tunnel-Pvt-Group-ID', and 'Tunnel-Type' rows are highlighted with a blue box.

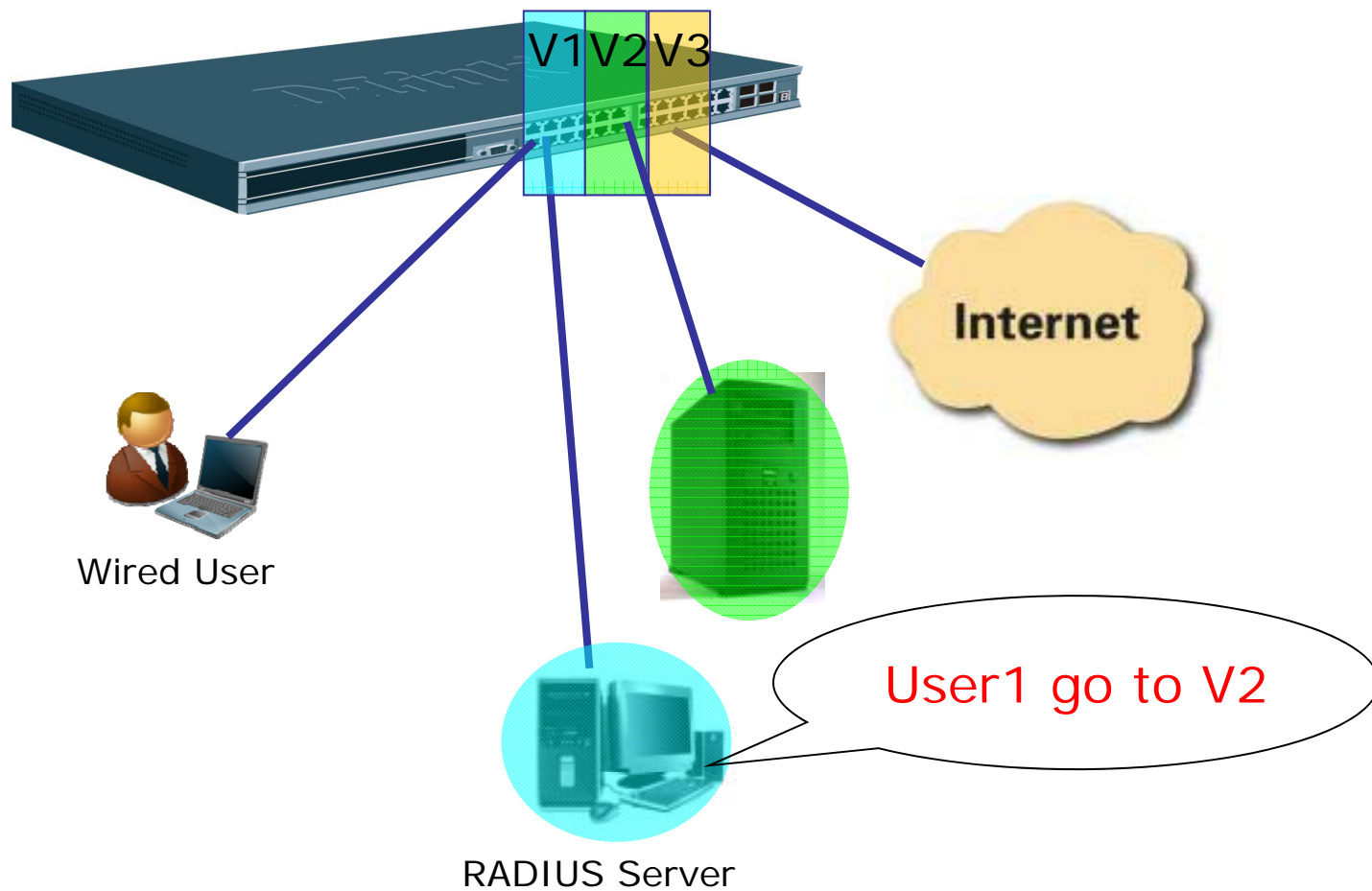
Name	Vendor	Value
Service-Type	RADIUS Standard	Framed
Tunnel-Medium-Type	RADIUS Standard	802 (includes all 802 m
Tunnel-Pvt-Group-ID	RADIUS Standard	502
Tunnel-Type	RADIUS Standard	Virtual LANs (VLAN)

Buttons at the bottom: Add..., Edit..., Remove, OK, Cancel, Apply.



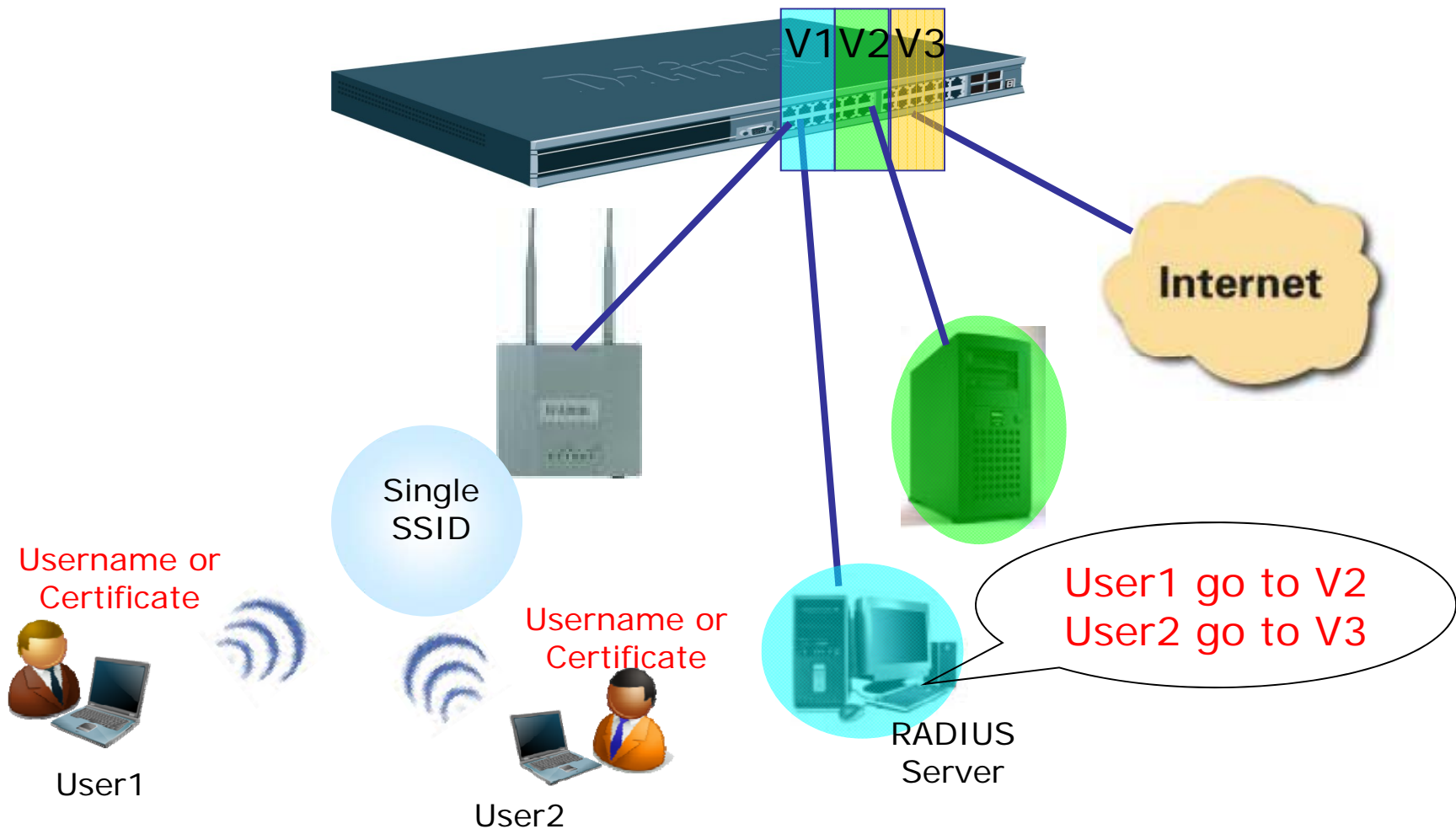


## Topology Example – Wired





## Topology Example – Wireless





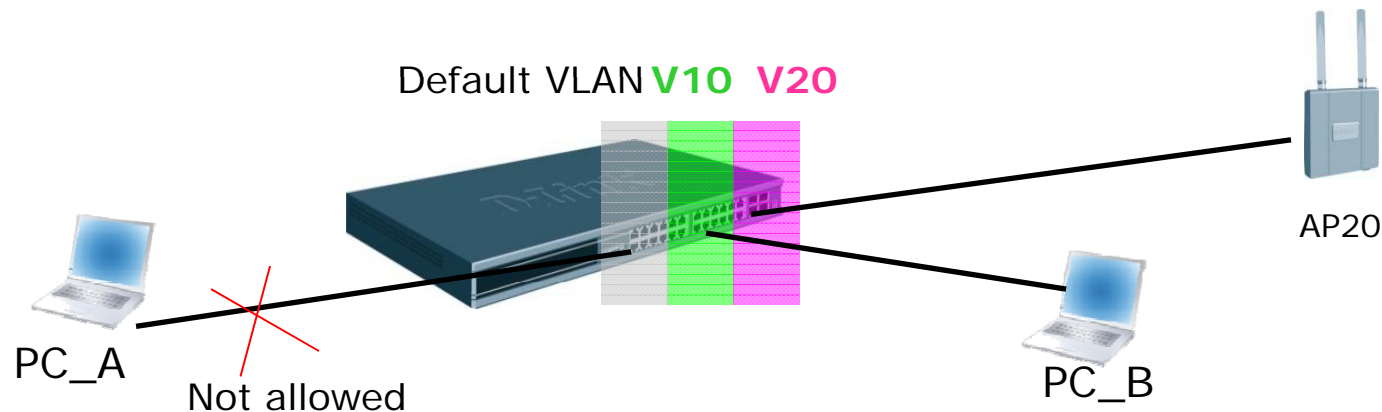
## Advanced Management

- There are three main types of interfaces that assign IP addresses in Unified Switch
  - VLAN routing interface
  - Network interface (network management IP address)
  - WLAN function interface
- VLAN routing interface routes data from different VLANs.
  - An interface that binds a VID, usually stands for a network subnet
  - Need to create VLAN first, then enable VLAN routing to create VLAN routing interface
  - DWS-4026 can show the VID of the interface using CLI but DWS-3026 series cannot
  - Command: show running-config
    - vlan database
    - vlan 10,20
    - vlan routing 10 10 → The 1st "10" is the VID, the 2nd "10" is the interface



## Network Interface and Management Network

- Network interface is the IP Address
  - Entered into browser address bar, or
  - For telnet client to configure switch
- The default network management interface is 10.90.90.90/8
- Management network is a subnet only for managing the switch.
- Operational network is the network where the box is responsible for routing/switching the traffic
- In D-Link's design, operational network traffic is not allowed to flow to the management network





# WLAN Function Interface

- It is the IP Address to communicate with AP.
- It is very important to make sure that the communication between AP and WLAN interface is routable.
- The IP address of WLAN function interface is chosen automatically.
  - IP address of the loopback interface has the first priority.
  - If user does not setup Loopback interface, the lowest VLAN routing interface will be selected, for example interface 4/1 has higher priority than 4/2.
  - If the switch works as L2 devices, which means there is no VLAN routing in this switch, the network management interface will be the WLAN function interface.
- A loopback interface is a permanent logical interface which must be always up. As such, it provides a mean to configure a stable IP address on the device that may be referred to by other switches. It is typically used by routing protocols.
- Make sure what is the IP address of WLAN interface before implementing APs.



## WLAN Function Interface Configuration

- Create Loopback interface

**Loopback Configuration**

Loopback	0
IPv4 Address	192.168.0.254
IPv4 Subnet Mask	255.255.255.0

Delete Loopback Submit

- Verify the WLAN interface status before implementing APs

DWS-4026

+

Security

+

Monitoring

+

Global

+

Peer Switch

+

Access Point

+

Client

+

Administration

Global

Switch Status

IP Discovery

Configuration Received

AP Hardware Capability

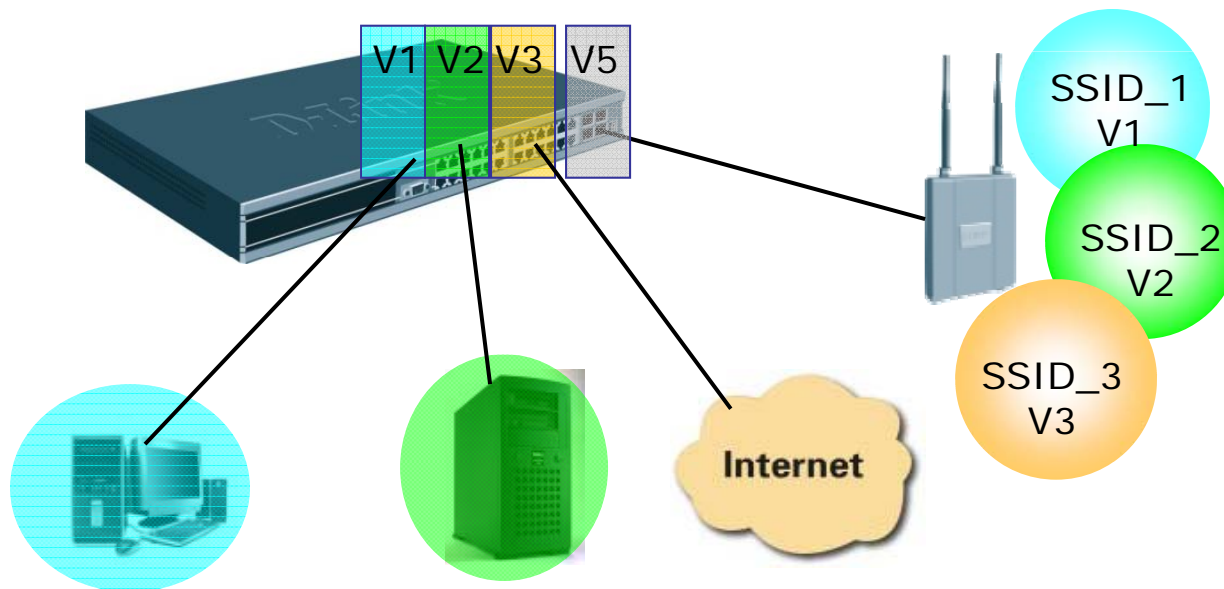
Wireless Global Status/Statistics

WLAN Switch Operational Status			
WLAN Switch Operational Status	Enabled	IP Address	192.168.10.1
Peer Switches	2		
Cluster Controller			
Cluster Controller	Yes	Cluster Controller IP Address	192.168.10.1



## Manage APs in VLAN Environment

- When using Unified Solution in a multiple VLAN environment, it is recommended to create a new VLAN for AP management network to separate the AP management network and client data.
- In this example, V5 is newly created and only for managing APs.
- The port connecting to the AP has tagged V1, V2 V3 and untagged V5 (Using untagged port to managed AP)

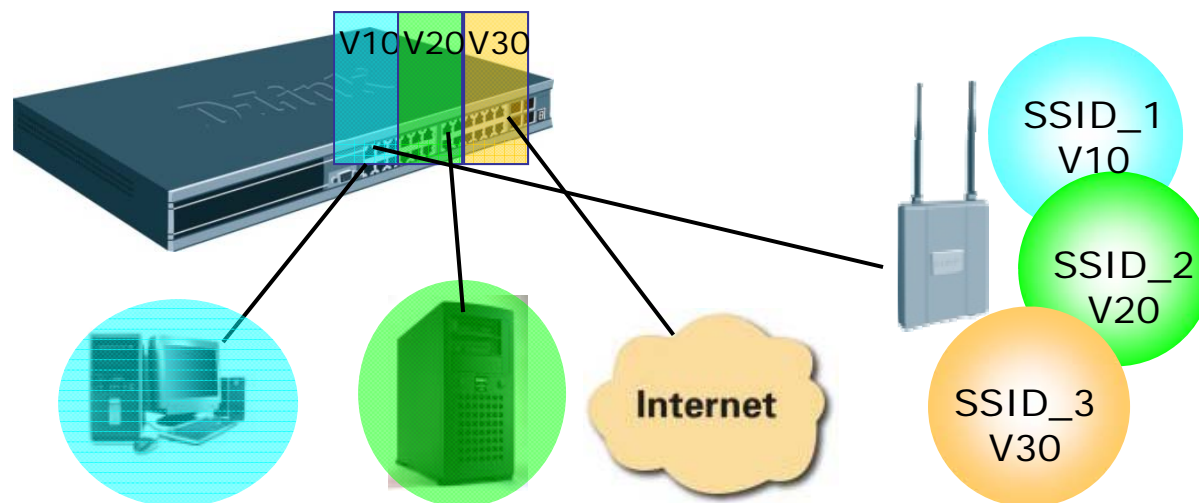






## Manage APs in VLAN Environment

- If the topology does not allow creation of a new VLAN, an existing VLAN can be used to manage the AP.
- An additional configuration is needed on the managed AP.
- Commands:
  - “set management vlan-id 10”, where the 10 equal to the vlan ID
- Disadvantage: Mixing the AP management network and client data network
- In this example, the port that connects the AP has to be tagged with V10, V20, V30 (Using tagged port to manage AP)





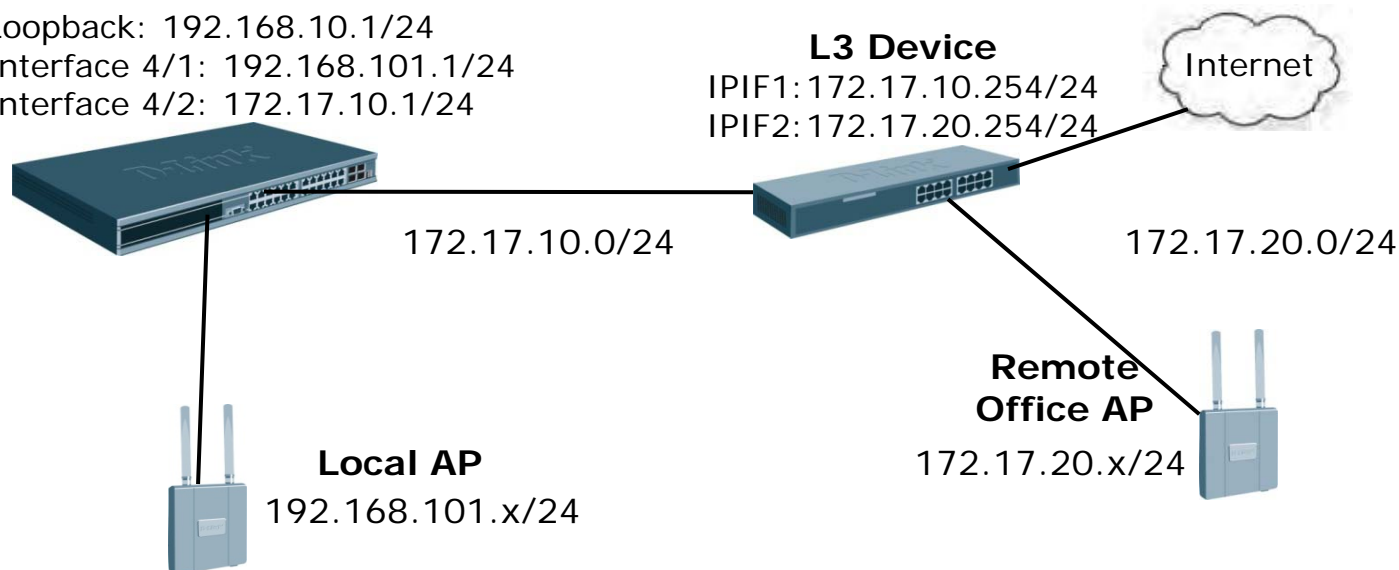


## Manage APs in Layer 3 Environment

- Always check the WLAN interface IP first.
- Configure the correct routing setting between AP and switch.
- Configure the correct gateway for APs (If DHCP server is not used).
- Ping AP to switch or from switch to AP. It must succeed.
- Could use tunnel mode or non-tunnel mode in L3 environment

### Unified Switch

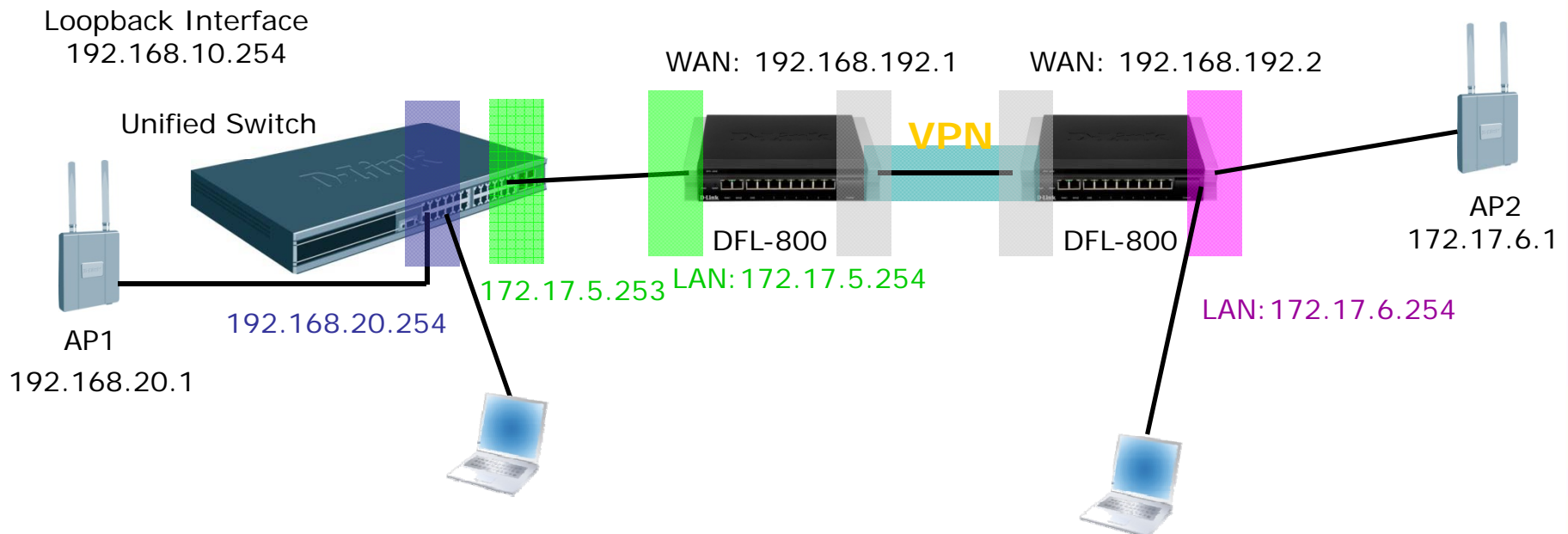
Loopback: 192.168.10.1/24  
Interface 4/1: 192.168.101.1/24  
Interface 4/2: 172.17.10.1/24





## Manage AP through VPN

- Able to manage AP through VPN.
- The AP management data are "don't fragment" packets, make sure the VPN devices do not drop "don't fragment" packets.





Lab 2

# Advanced Management



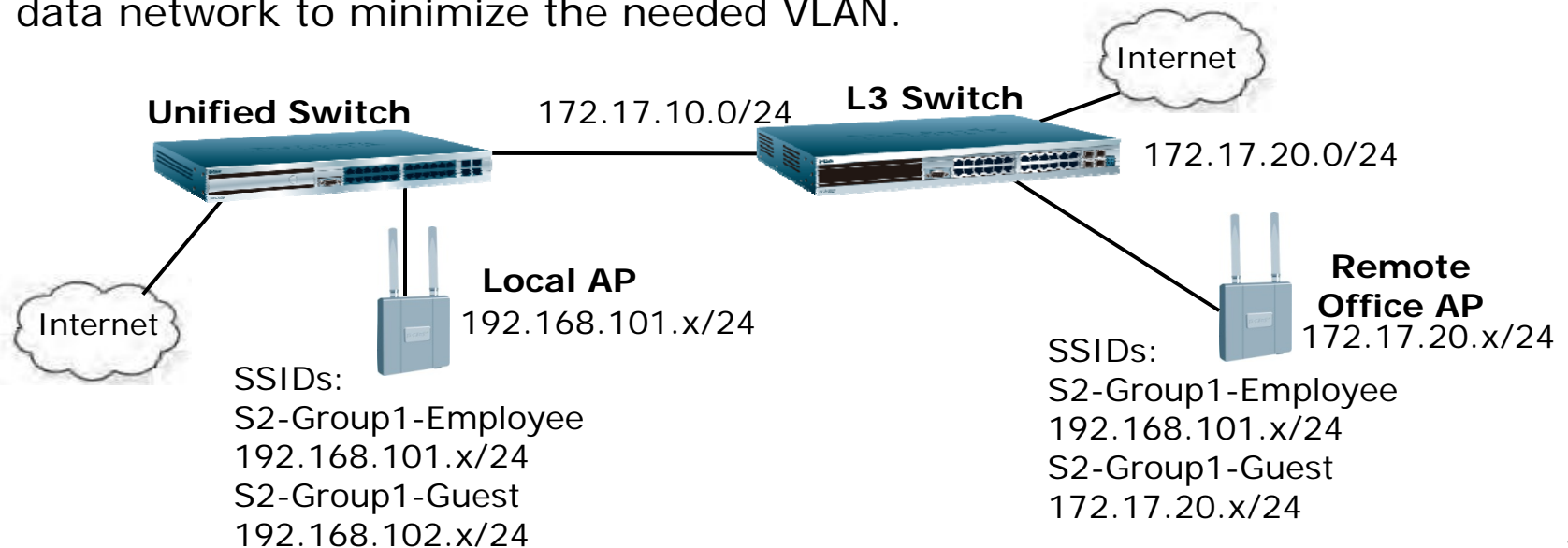
## Lab 2: Advanced Management

- This scenario shows how to manage AP in L2 and L3 environment, setup tunnel and non-tunnel modes, design management data and client data flow.
  
- **Objectives:**
  - Understand management network and client data network
  - Understand tunnel and non tunnel mode
  - Understand WLAN function interface
  - Design typical L2 + L3 wireless network



## Network Topology

- Wireless network in local office works in L2 environment, remote office is implemented with L3 network.
- All employees connect to SSID S2-Group1-Employee and assign to the same subnet regardless where they are.
- Guests connect to SSID S2-Group1-Guest and assign to different subnet according to their locations.
- Base on the design, remote office requires a L3 tunnel SSID and a non-tunnel SSID. Local office needs to mix the management network and client data network to minimize the needed VLAN.





## Lab 2: Advanced Management

Table 1: Physical Connection

From Device	From Port	To Device	To Port
Unified Switch	24	L3 Switch	1
Unified Switch	1	Local AP	N/A
L3 Switch	24	Remote AP	N/A

Table 2: VLAN and Port Assignment

Device	VLAN ID	VLAN Name	Tagged Ports	Untagged Ports
Unified Switch	10	Core10	N/A	24
Unified Switch	101	Tunnel101	1	N/A
Unified Switch	102	Client102	1	N/A
L3 Switch	10	Core10	N/A	1
L3 Switch	20	Client20	N/A	24



## Lab 2: Advanced Management

Table 3: IP Addressing

Device	Interface	VID	IP Address
Unified Switch	4/1	10	172.17.10.254/24
Unified Switch	4/2	101	192.168.101.254/24
Unified Switch	4/3	102	192.168.102.254/24
Unified Switch	Management	1	10.90.90.90/8
Unified Switch	Loopback	N/A	192.168.100.254/32
L3 Switch	ipif10	10	172.17.10.1/24
L3 Switch	ipif20	20	172.17.20.1/24

Table 4: DHCP Server

Device	Pool	Network	Excluded IP
Unified Switch	Tunnel101	192.168.101.0/24	192.168.101.200-255
Unified Switch	Client102	192.168.102.0/24	192.168.102.200-255
L3 Switch	Client20	172.17.20.0/24	172.17.20.1-100



### Lab Scenario Discussion

- The reason to create loopback interface on Unified Switch?
- Why employees need a tunnel, can I create a tunnel for guests?
- Why need to configure local AP? Is that necessary?
- Why need a static route on L3 switch?





Session 5

# **New Functions Implementation (DWS-4026/DWL-8600AP)**



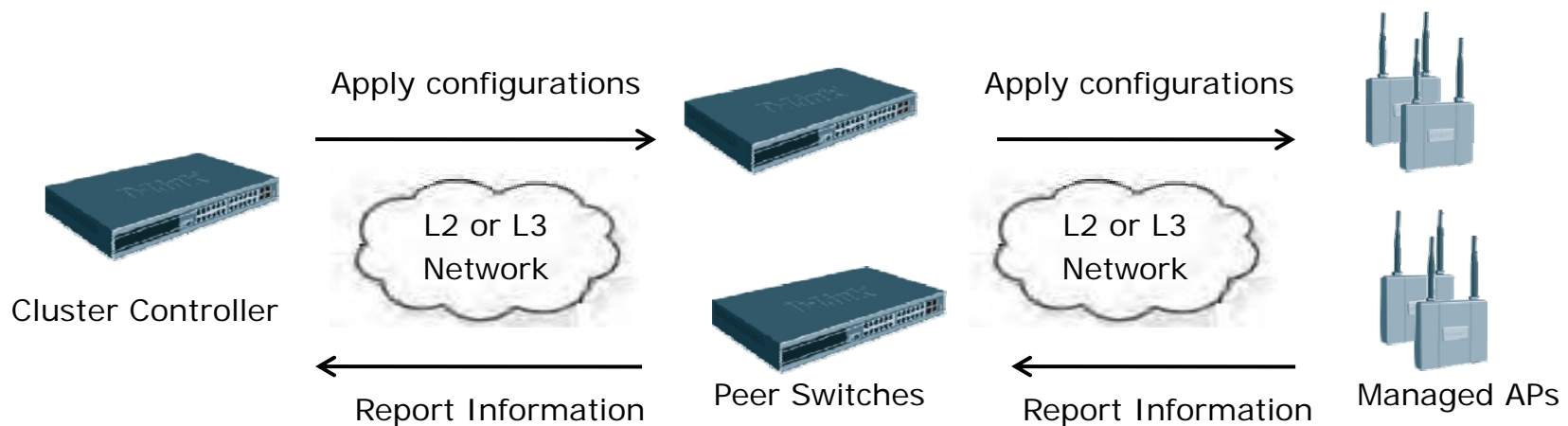
## **Session 5: New Function Implementation (DWS-4026/DWL-8600AP)**

- Switch Clustering
- Layer 2 Distributed Tunnel
- RF Scan and Rogue Management
- Wireless Intrusion Detection System
- Wireless Intrusion Prevention System
- IEEE 802.11n
- AP Clustering
- Wireless Distribution System
- Centralized IEEE 802.1x Authentication
- Other Features



## Switch Clustering

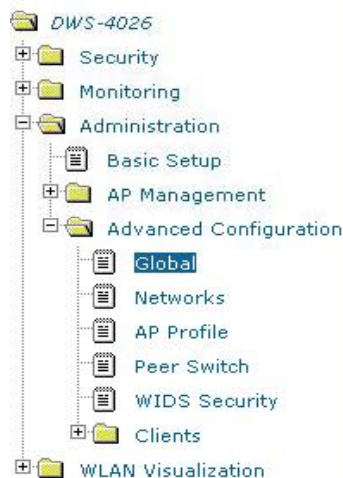
- Peer Switches can form a Cluster Group. Within this group, users can push the configurations from one switch to other peer switches.
  - It is not necessary to configure the same settings one by one.
- In a Cluster Group, a Cluster Controller will be selected. This Controller will gather all the AP and clients statistics in this group.
  - Single point of management is possible.
- Switch clustering is only supported by DWS-4026.





## Cluster Controller Selection

- The switches select the Cluster Controller by two ways:
  - Compare Cluster Priority. The switch with the highest priority becomes the Cluster Controller.
  - If the priority is the same, the switch with lower IP address becomes the Cluster Controller.
- The Cluster Priority can be 0 to 255. Setting 0 disables the Cluster function, the IP of the Controller will show 0.0.0.0.



General			SNMP Traps	Distributed Tunneling
<b>Wireless Global Configuration</b>				
Peer Group ID	1	(1 to 255)		
Client Roam Timeout (secs)	30	(1 to 120)		
Ad Hoc Client Status Timeout (hours)	24	(0 to 168)		
AP Failure Status Timeout (hours)	24	(0 to 168)		
MAC Authentication Mode	white-list	▼		
RF Scan Status Timeout (hours)	24	(0 to 168)		
Detected Clients Status Timeout (hours)	24	(0 to 168)		
Tunnel IP MTU Size	1500	▼		
Cluster Priority	1	(0 to 255, 0 - Disable)		
AP Client QoS	Disable	▼		



## Cluster Controller Selection (Cont.)

- A switch performs the election process when
  - It boots up.
  - It loses connection to the current Cluster Controller.
  - A new peer switch joins.
  - Cluster Priority changes in any of the peer switches.
- Each switch makes an independent decision about the Cluster Controller. If there is no peer switch, it will appoint itself as the Cluster Controller.
- Check status

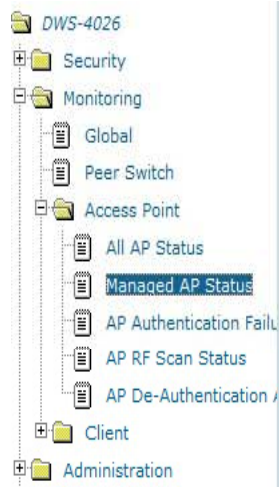


Global	Switch Status	IP Discovery	Configuration Received	AP Hardware Capability
Wireless Global Status/Statistics				
WLAN Switch Operational Status	Enabled	IP Address	192.168.10.1	
Peer Switches	2			
Cluster Controller	Yes	Cluster Controller IP Address	192.168.10.1	
Total Access Points	3	Managed Access Points	3	
Standalone Access Points	0	Rogue Access Points	6	
Discovered Access Points	0	Connection Failed Access Points	0	
Authentication Failed Access Points	0	Unknown Access Points	23	
Rogue AP Mitigation Limit	16	Rogue AP Mitigation Count	0	
Maximum Managed APs in Peer Group	256	WLAN Utilization	15 %	



### Cluster Controller Capabilities

- It can push the configurations to other peer switches.
- It can control the APs that managed by peer switch, for example to run auto channel/power adjustment, WIDS.
- It can display information of whole peer group.
  - The switches which are not Cluster Controllers can only show its locally attached devices. (Different with DWS-3000 series)
- The Cluster Controller is also responsible for assuring that there is not more than 256 APs in the unified system.



Status Statistics													
Summary Detail Radio Summary Radio Detail Neighbor APs Neighbor Clients VAP Distributed Tunneling													
Managed AP Status													
MAC Address (*)	Peer Managed	Location	Switch Port	IP Address	Software Version	Age	Status	Configuration Status	Profile	Radio	Channel	Authenticated Clients	
* 00:22:b0:3d:95:80			0/1	192.168.30.102	1.0.0.6	0d:00:00:01	Managed	Success	1-Default	1-802.11a/n	36	0	
										2-802.11b/g/n	11	0	
00:22:b0:3d:97:00			0/1	192.168.10.101	1.0.0.6	0d:00:00:04	Managed	Success	1-Default	1-802.11a/n	36	0	
										2-802.11b/g/n	6	0	
* 00:22:b0:3d:98:40			0/1	192.168.20.102	1.0.0.6	0d:00:00:04	Managed	Success	1-Default	1-802.11a/n	132	0	
										2-802.11b/g/n	11	0	



# Configuration Pushing

- Configurations are pushed manually by the admin, and it is not automatic.
- Configurations can be pushed from any peer switch to other peer switches in a cluster. It is not necessary from the cluster controller only.



Configuration Request

Configuration Enable/Disable

Peer Switch Configuration Request Status

Configuration Request Status	Not Started
Total Count	0
Success Count	0
Failure Count	0

Peer IP Address	Configuration Request Status
<input checked="" type="checkbox"/> 192.168.20.1	Not Started
<input checked="" type="checkbox"/> 192.168.30.1	Not Started

Start

Start All

Refresh





# Configuration Pushing

- Users can choose up to ten configuration items to push.

The screenshot displays the D-Link configuration interface. On the left is a tree view of the configuration hierarchy. The 'Peer Switch' option under 'Advanced Configuration' is selected. On the right, the 'Configuration Enable/Disable' tab is active, showing a table of configuration items and their status.

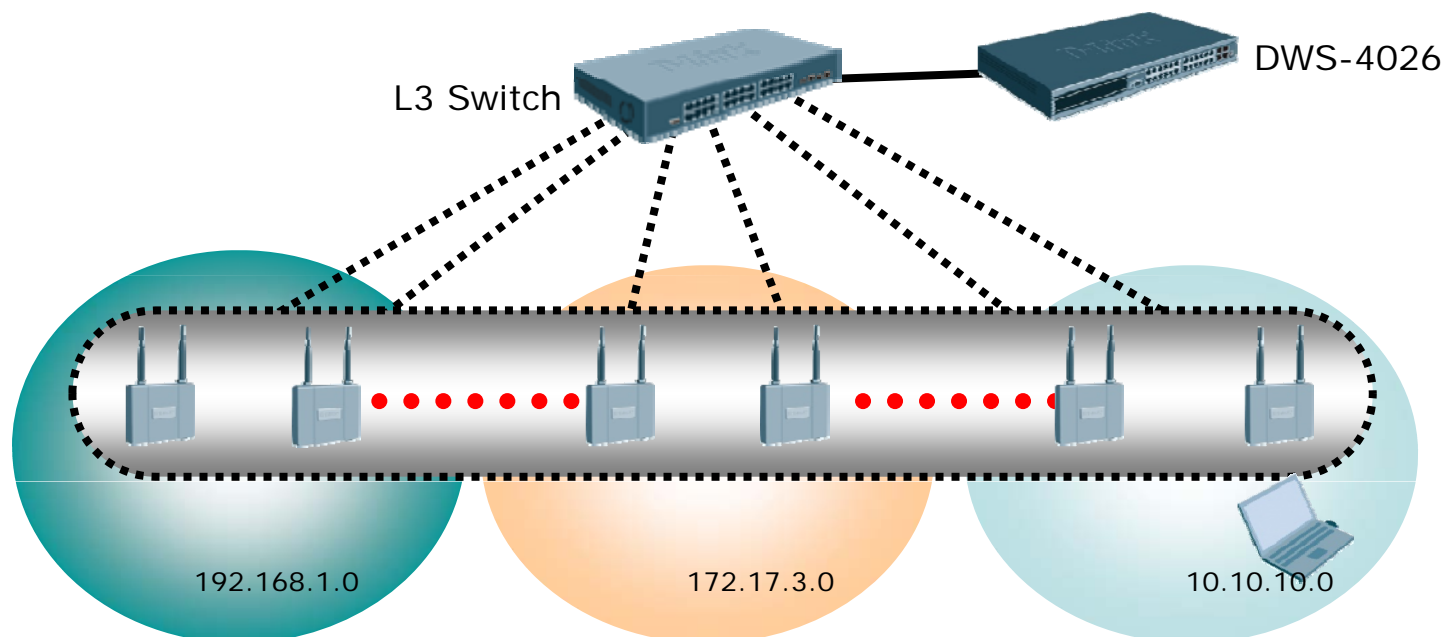
Peer Switch Configuration Enable/Disable	
Global	Enable ▼
Discovery	Disable ▼
Channel/Power	Enable ▼
AP Database	Enable ▼
AP Profiles	Enable ▼
Known Client	Enable ▼
Captive Portal	Enable ▼
RADIUS Client	Enable ▼
QoS ACL	Enable ▼
QoS DiffServ	Enable ▼





### Layer 2 Distributed Tunnel

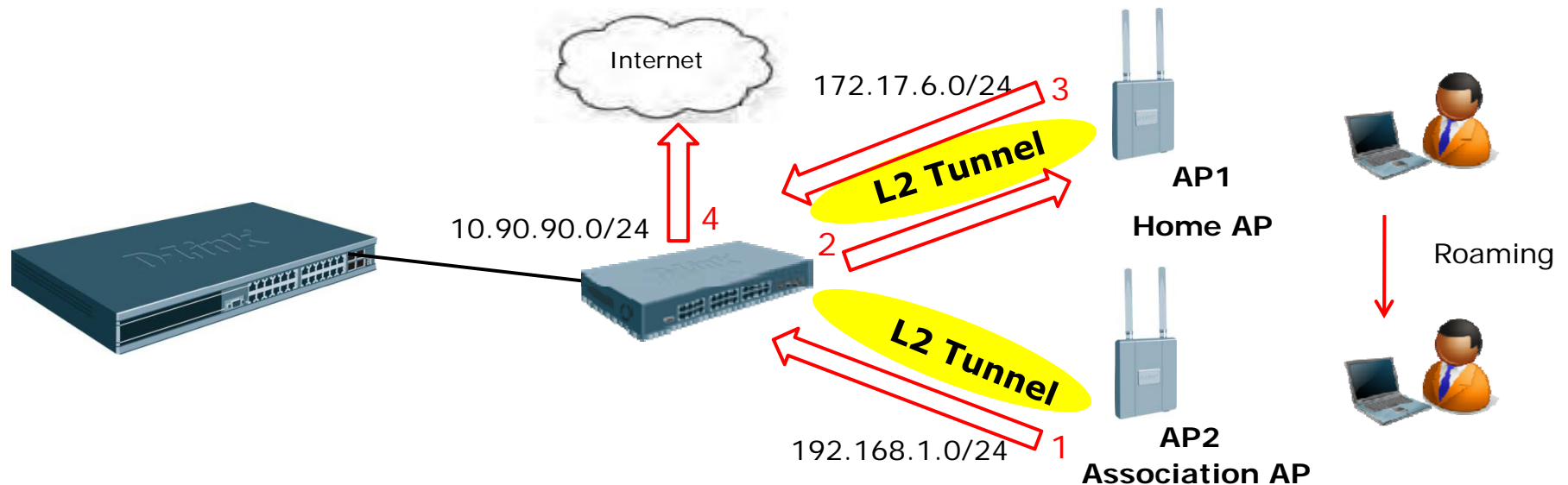
- Layer 2 (L2) Distributed Tunnel mode is used to support L3 roaming without forwarding any traffic to the Unified Switch.
- When clients roam to another AP which is not in the same network subnet, traffic from roamed clients is tunneled to the originally associated AP of the client.
- Roamed client remains on the same VLAN and has the same IP address.





## Layer 2 Distributed Tunnel Operation

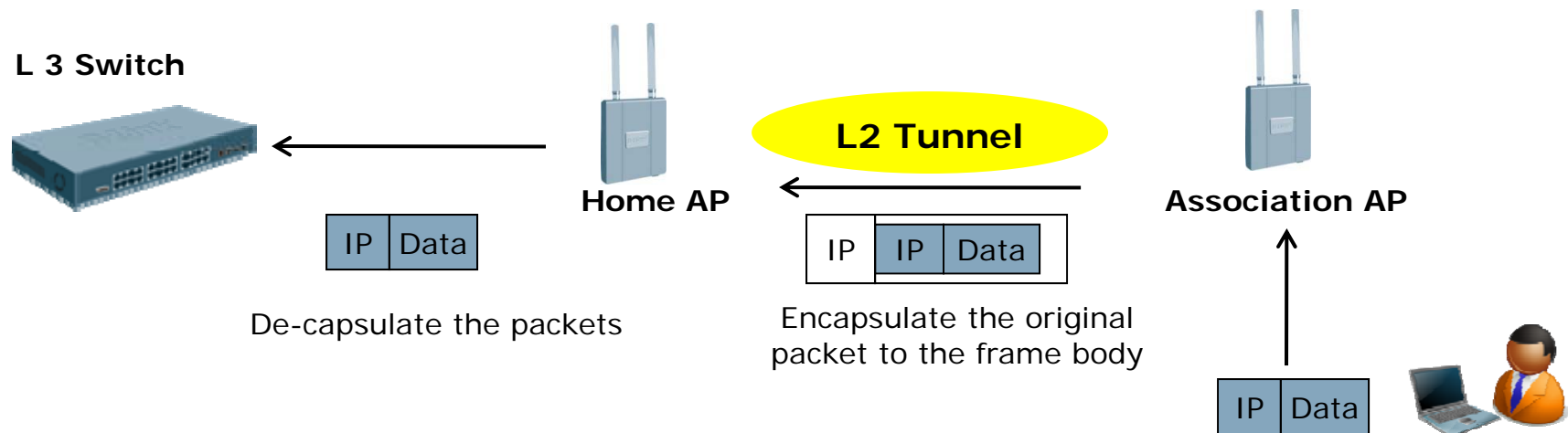
- The initial associated AP of the client is called the "Home AP". The AP which the client roams to is called the "Association AP".
- When a client roams to another AP in a different subnet, the Association AP tunnels all traffic from the client to the Home AP using L2 UDP tunnel. The Home AP injects the traffic received over the tunnel into the wired network.





## Layer 2 Distributed Tunnel Operation (Cont.)

- It uses CAPWAP tunnel encapsulation to forward L2 frames, no extra IP header is needed.
- Association AP encapsulates the packets into tunnel and Home AP de-capsulate the packets.
- Note: If a client roams to another AP in the same subnet, the tunnel is not created, and the new AP will become the Home AP.





## New Functions Implementation (DWS-4026/DWL-8600AP)

### ▪ Layer 2 Distributed Tunnel

## Layer 2 Distributed Tunnel Setup

- It is based on Virtual Access Point, VAP (SSID).
- Two APs form a roaming group.
- APs need to be in different VLAN and network subnet (AP's IP subnet and not client's IP subnet)
- APs attaching to different peer switches can establish a tunnel.

The screenshot displays the 'Wireless Network Configuration' page for a D-Link device. The left sidebar shows a tree view with 'WLAN' selected. The main panel contains the following configuration options:

Configuration Item	Value
SSID	dlink1
Hide SSID	<input type="checkbox"/>
Ignore Broadcast	<input type="checkbox"/>
VLAN	1 (1 to 4094)
L3 Tunnel	<input type="checkbox"/>
L3 Tunnel Status	None
L3 Tunnel Subnet	0.0.0.0
L3 Tunnel Mask	255.255.255.0
MAC Authentication	<input type="radio"/> Local <input type="radio"/> RADIUS <input checked="" type="radio"/> Disable
Redirect	<input checked="" type="radio"/> None <input type="radio"/> HTTP
Redirect URL	
Wireless ARP Suppression Mode	Disable
L2 Distributed Tunneling Mode	Disable



# Layer 2 Distributed Tunnel

- Some more parameters



- Advantages of Layer 2 distributed tunneling
  - Support fast roaming
  - Reduce network resources because traffic is forwarded locally
  - Reduce Unified Switch loading
- Disadvantages of Layer 2 distributed tunneling
  - Reduce AP performance due to the extra load on the APs for handling roamed clients.
  - If the Home AP fails, the L3 roaming does not work because the traffic is not tunneled to the Home AP.



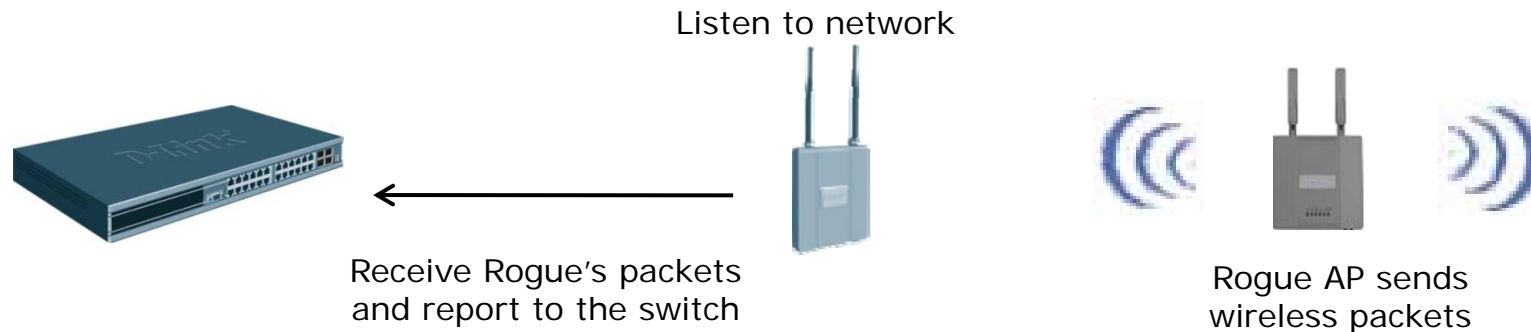
## **Wireless Intrusion Detection/Prevention System**

- DWS-4026 supports Wireless Intrusion Detection/Prevention System (WIDS/WIPS).
  - It detects intrusion of rogue AP and clients automatically.
  - It mitigates attacks from rogue AP and clients.
- Steps to use WIDS/WIPS
  - RF scan with active mode or sentry mode
  - Manually assign rogue devices or automatically defined rogue AP/clients by Unified System
  - Mitigate rogue devices if needed
- For intrusion mitigation, Unified System only mitigates the interference from rogue AP/clients
  - Automatically mitigate rogues.
  - AP/clients which are not classified as rogue are not influenced.



### Radio Frequency Scan

- Unified APs can scan the entire wireless network and list all the APs in the network.
- Two scanning modes:
  - Active mode: The AP primarily services wireless clients, performs RF scan periodically and reports the results to the Unified Switch.
  - Sentry mode: The AP performs only continuous RF scans and does not service Wireless Clients.
- Unified AP performs only passive RF scans by listening to the wireless traffic. APs do not perform active scans, which send probe requests.







## New Functions Implementation (DWS-4026/DWL-8600AP)

### ▪ Wireless Intrusion Detection System

## Sentry Mode Operation

- The AP is dedicated to perform RF scan and does not service any wireless clients.
- AP in sentry mode scans from the first to the last channel and repeat continuously.
- AP in sentry mode spends one second on each channel for RF scan.
- Radios that are configured in sentry mode scan all 802.11 channels, and not just the channels valid for the specific country
- Sentry mode is configured based on radio (profile).

The screenshot shows the 'Access Point Profile Radio Configuration' page for 'AP Profile 1-Default'. The 'Radio' tab is selected. The 'State' is set to 'On'. The 'Mode' is set to 'IEEE 802.11a/n'. The 'RF Scan Sentry' checkbox is highlighted with a blue box. The 'RF Scan Interval (secs)' is set to 60. The 'RF Scan Sentry Channels' are set to 802.11a and 802.11b/g.

Parameter	Value	Range
State	On	On / Off
Mode	IEEE 802.11a/n	IEEE 802.11a/n / 2-802.11b/g/n
RTS Threshold (bytes)	2347	(0 to 2347)
Load Balancing	<input type="checkbox"/>	
Load Utilization (%)	60	(1 to 100)
Maximum Clients	200	(0 to 200)
RF Scan Other Channels	<input type="checkbox"/>	
RF Scan Sentry	<input checked="" type="checkbox"/>	
RF Scan Interval (secs)	60	(30 to 120)
RF Scan Sentry Channels	<input checked="" type="checkbox"/> 802.11a <input checked="" type="checkbox"/> 802.11b/g	
RF Scan Duration (msecs)	10	(10 to 2000)
Rate Limiting	<input type="checkbox"/>	
DTIM Period (# beacons)	10	(1 to 255)
Beacon Interval (msecs)	100	(20 to 2000)
Automatic Channel	<input checked="" type="checkbox"/>	
Automatic Power	<input checked="" type="checkbox"/>	
Initial Power (%)	100	(1 to 100)
U-APSD Mode	Enable	Enable / Disable
Frag Threshold (bytes)	2346	(256 to 2346)
Short Retries	7	
Long Retries	4	
Transmit Lifetime (msecs)	512	





## New Functions Implementation (DWS-4026/DWL-8600AP)

### ▪ Wireless Intrusion Detection System

## Active Mode Operation

- It is enabled by default.
- It has three options:
  - RF Scan Other Channels: It scans other channels and AP only listens to its operational channel when the option disabled
  - RF Scan Interval: The interval that AP scan all the channels, in seconds. The default is 60.
  - RF Scan Duration: The duration that the AP stays in each channels, in millisecond. The default is 10.
- The AP scans only the supported channels in its country.



	MAC Address	SSID	Physical Mode	Channel	Status	Age
<input type="checkbox"/>	00:03:64:00:01:24	Ricky_4F	802.11b/g	11	Unknown	0d:00:00:05
<input type="checkbox"/>	00:0a:79:98:12:c3	rochet	802.11b/g	11	Unknown	0d:00:00:05
<input type="checkbox"/>	00:11:95:95:ca:28	SRV	802.11b/g	11	Unknown	0d:00:00:05
<input type="checkbox"/>	00:11:95:95:ca:29		802.11b/g	11	Rogue	0d:00:00:05
<input type="checkbox"/>	00:11:95:95:ca:2a		802.11b/g	11	Rogue	0d:00:00:05
<input type="checkbox"/>	00:11:95:95:ca:2b	ALPHA	802.11b/g	11	Unknown	0d:00:00:05
<input type="checkbox"/>	00:11:95:a3:7d:58	GuestTest	802.11b/g	11	Unknown	0d:00:52:17
<input type="checkbox"/>	00:13:46:ff:01:90	AP-syjh-T4	802.11b/g	11	Unknown	0d:00:00:05
<input type="checkbox"/>	00:16:01:6f:07:8d	Buffalo11gn	802.11b/g	11	Unknown	0d:01:17:55
<input type="checkbox"/>	00:17:9a:d2:3b:28	D-Link	802.11b/g	11	Unknown	0d:00:00:05



## New Functions Implementation (DWS-4026/DWL-8600AP)

### ▪ Wireless Intrusion Detection System

## Clients Detection

- The wireless clients are detected by the wireless system because the clients either attempt to interact with the system, or because the system detects traffic from the clients.
- The wireless clients are detected by following methods:
  - Clients attempt to associate with the Unified System.
  - Clients attempt to authenticate with the Unified System, but fail.
  - Clients pre-authenticate with the wireless system.
  - Clients send 802.11 management frames to the system.
  - Data traffic from/to clients is detected by Unified AP.

The screenshot shows the D-Link management interface with the WLAN tab selected. The left sidebar shows a tree view with 'Client' expanded, showing 'Associated Clients', 'Ad Hoc Clients', and 'Detected Clients'. The main area displays the 'Detected Client Status' table.

Detected Client Status				
MAC Address	Client Name	Client Status	Age	Create Time
<input type="checkbox"/> 00:02:6f:54:2d:55		Detected	0d:00:00:14	0d:03:09:32
<input type="checkbox"/> 00:02:d1:01:77:44		Detected	0d:00:20:22	0d:03:00:28
<input type="checkbox"/> 00:03:1b:58:f8:08		Detected	0d:00:00:14	0d:03:19:16
<input type="checkbox"/> 00:03:7f:10:48:0a		Detected	0d:00:32:52	0d:03:19:16
<input type="checkbox"/> 00:03:7f:be:f1:03		Detected	0d:03:04:31	0d:03:04:31
<input type="checkbox"/> 00:0c:e7:3fa8:90		Detected	0d:02:20:09	0d:02:28:09
<input type="checkbox"/> 00:0c:f1:2d:93:cc		Detected	0d:00:00:14	0d:01:23:08
<input type="checkbox"/> 00:0d:88:89:a1:09		Detected	0d:00:29:22	0d:03:19:16

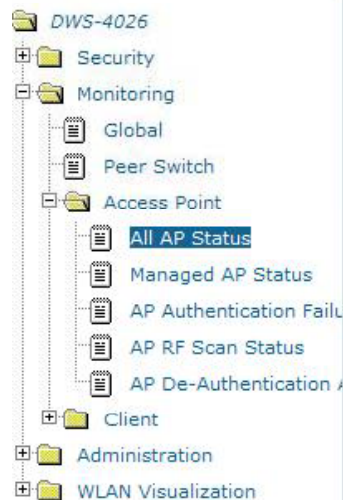


## New Functions Implementation (DWS-4026/DWL-8600AP)

### ▪ Wireless Intrusion Detection System

## Manual Detected AP Classification

- The detected APs are classified into the following categories:
  - Managed: AP is managed by the wireless system.
  - Standalone: Administrator classifies it as standalone AP in valid AP database.
  - Rogue: The AP is classified as a threat by threat detection algorithms.
  - Unknown: The AP is detected but not classified.
  - By default, detected AP is classified to unknown AP. Users can manually define the AP category.



Valid Access Point Configuration			
MAC address	00:22:B0:3D:95:90		
AP Mode	Managed		
Location	Standalone		
Authentication Password	Rogue		<input type="checkbox"/> Edit
Profile	1 - Default		
Radio 1 - 802.11a/n	Channel	Auto	Power (%) 0
Radio 2 - 802.11b/g/n	Channel	Auto	Power (%) 0



## New Functions Implementation (DWS-4026/DWL-8600AP)

### ▪ Wireless Intrusion Detection System

## Known Client Database

- Detected clients can be classified as known clients in Known Clients Database.
  - It is used to compare detected clients with known valid clients and generate traps when unknown clients are detected
  - It is used for MAC Authentication for associated clients.
  - It is used for Wireless Intrusion Detection System.
- It can reside on the switch or on the RADIUS server.
- It supports up to maximum 1024 entries.



Known Client Summary		
MAC Address	Name	Authentication Action
<input type="checkbox"/> 00:19:02:0e:0c:98		Grant
<input type="text" value="00:00:00:00:00:00"/>	<input type="button" value="Add"/>	
<input type="button" value="Delete"/> <input type="button" value="Delete All"/> <input type="button" value="Refresh"/>		





## New Functions Implementation (DWS-4026/DWL-8600AP)

### ▪ Wireless Intrusion Detection System

## Automatic Intrusion Detection – AP

- The threat classification algorithm allows Unified System classifies APs as rogue automatically.
- 11 types of threats are supported.
- The two threats “Unmanaged AP detected on wired network” and “AP is operating on an illegal channel” are only detected with sentry-mode AP. Other threats can be detected by either sentry mode or active mode.

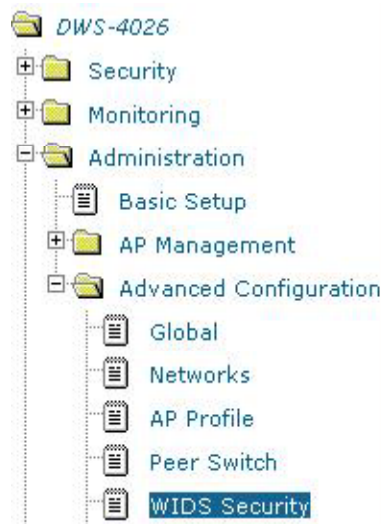
The screenshot displays the configuration interface for a D-Link Unified System. On the left, a tree view shows the navigation menu with categories like LAN, WLAN, Security, Monitoring, and Administration. Under Administration, the 'WIDS Security' option is selected. The main panel on the right is titled 'WIDS AP Configuration' and contains a list of 11 threat detection settings, each with an 'Enable' dropdown menu. The settings are:

Threat Type	Configuration
Administrator configured rogue AP	Enable
Managed SSID from an unknown AP	Enable
Managed SSID from a fake managed AP	Enable
AP without an SSID	Enable
Fake managed AP on an invalid channel	Enable
Managed SSID detected with incorrect security	Enable
Invalid SSID from a managed AP	Enable
AP is operating on an illegal channel	Enable
Standalone AP with unexpected configuration	Enable
Unexpected WDS device detected on network	Enable
Unmanaged AP detected on wired network	Enable
Rogue Detected Trap Interval (seconds)	300 (60 to 3600, 0 - Disable)
Wired Network Detection Interval (seconds)	60 (1 to 3600, 0 - Disable)
AP De-Authentication Attack	Enable



## Automatic Intrusion Detection – Clients

- Wireless clients can be classified automatically by Unified System, too.
- The wireless clients are classified into the following categories:
  - Authenticated – The wireless client is authenticated with the wireless system.
  - Detected – The wireless client is detected by the wireless system, but is not a security threat.
  - Black-Listed – The client with this MAC address is specifically denied access via MAC Authentication.
  - Rogue – The client is classified as a threat by one of the threat detection algorithms.



WIDS Client Configuration	
Not Present in Known Client Database Test	Disable ▼
Configured Authentication Rate Test	Enable ▼
Configured Probe Requests Rate Test	Enable ▼
Configured De-Authentication Requests Rate Test	Enable ▼
Maximum Authentication Failures Test	Enable ▼
Authentication with Unknown AP Test	Disable ▼
Client Threat Mitigation	Disable ▼
Known Client Database Lookup Method	Local ▼
Known Client Database RADIUS Server Name	Default-RADIUS-Server



## New Functions Implementation (DWS-4026/DWL-8600AP)

### ▪ Wireless Intrusion Prevention System

## WIPS/Threat Mitigation

- The function is disabled by default, system will automatically mitigate all rouge devices including rogue APs and rouge clients once you enable it.
- The basic technique of intrusion mitigation is to send de-authentication packets to rogue devices.
  - It sends de-auth packets to clients on behalf of the rogue AP.
  - It sends de-auth packets to the rogue AP on behalf of the clients associated with that AP.
  - It sends de-auth packets to known clients that associate with Unknown APs

Threat	Status
Managed SSID from a fake managed AP	Enable
AP without an SSID	Enable
Fake managed AP on an invalid channel	Enable
Managed SSID detected with incorrect security	Enable
Invalid SSID from a managed AP	Enable
AP is operating on an illegal channel	Enable
Standalone AP with unexpected configuration	Enable
Unexpected WDS device detected on network	Enable
Unmanaged AP detected on wired network	Enable
Rogue Detected Trap Interval (seconds)	300 (60 to 3600, 0 - Disable)
Wired Network Detection Interval (seconds)	60 (1 to 3600, 0 - Disable)
AP De-Authentication Attack	Disable



## New Functions Implementation (DWS-4026/DWL-8600AP)

### ▪ Wireless Intrusion Prevention System

## WIPS/Threat Mitigation

- APs in sentry mode send de-auth packets every seconds to mitigate the intrusion from both rouge AP and client
- APs in active mode send de-auth packets every ten seconds for intrusion mitigation and only for rouge AP in its operation channel. Rouge client and rouge AP in other channels won't be affected.
- Max 16 APs, 128 clients are attacked concurrently.
- Users could view AP De-Authentication Attack Status to check which rogue is attacked.

The screenshot shows the D-Link management interface with the 'WLAN' tab selected. The left sidebar shows a tree view with 'DWS-4026' expanded, followed by 'Security' and 'Monitoring'. Under 'Monitoring', 'Access Point' is expanded, showing 'All AP Status', 'Managed AP Status', 'AP Authentication Failure', 'AP RF Scan Status', and 'AP De-Authentication Attack Status'. The 'AP De-Authentication Attack Status' tool is open, displaying a table with the following data:

BSSID	Channel	Time Since Attack Started	RF Scan Report A
<a href="#">00:19:5b:8f:94:49</a>	11	0d:00:04:13	0d:00:01:13
<a href="#">00:17:9a:d2:93:19</a>	1	0d:00:01:13	0d:00:00:13
<a href="#">00:17:9a:d2:01:39</a>	1	0d:00:01:13	0d:00:00:13
<a href="#">00:19:5b:8f:94:b9</a>	1	0d:00:01:13	0d:00:00:13
<a href="#">00:19:5b:b1:3b:69</a>	1	0d:00:01:13	0d:00:00:13
<a href="#">00:17:9a:d2:8f:d9</a>	1	0d:00:01:13	0d:00:00:13
<a href="#">00:19:5b:8f:93:31</a>	1	0d:00:01:13	0d:00:00:13
<a href="#">00:1e:58:72:f9:19</a>	1	0d:00:01:13	0d:00:00:13

A 'Refresh' button is located at the bottom right of the table.





## New Functions Implementation (DWS-4026/DWL-8600AP)

### ▪ Wireless Intrusion Prevention System

## WIDS/WIPS Limitation

- Users must make sure that there is no legitimate APs which are classified as rogues before enabling the attack feature.
  - System shows the classified result and reason on WIDS AP Rogue Classification.
- De-auth messages are sent every ten seconds (active mode) or every second (sentry mode) for performance concern.
  - The function is to mitigate, not to block the rogues
- If the detected rogue is spoofing the BSSID of the valid managed AP then the wireless system doesn't attempt to use the attack.
- The de-authentication attack is not effective against Ad hoc networks.
- The APs operating on channels outside of the country domain are not attacked due to the law.

DWS-4026

Security

Monitoring

Global

Peer Switch

Access Point

All AP Status

Managed AP Status

AP Authentication Fail

AP RF Scan Status

AP De-Authentication

Client

Administration

WLAN Visualization

AP RF Scan Status

AP Triangulation Status

WIDS AP Rogue Classification

WIDS AP Rogue Classification

MAC Address : 00:22:b0:3d:95:d0

Status : Rogue

Test Description	Condition Detected	Reporting MAC Address	Radio	Test Config	Test Result
Administrator configured rogue AP	False	None	0	Enabled	Rogue
Managed SSID from an unknown AP	False	None	0	Enabled	
Managed SSID from a fake managed AP	False	None	0	Enabled	
AP without an SSID	True	00:22:b0:3d:97:00	2	Enabled	
Fake managed AP on an invalid channel	False	None	0	Enabled	
Managed SSID detected with incorrect security	False	None	0	Enabled	
Invalid SSID from a managed AP	False	None	0	Enabled	
AP is operating on an illegal channel	False	None	0	Enabled	
Standalone AP with unexpected configuration	False	None	0	Enabled	



## New Functions Implementation (DWS-4026/DWL-8600AP)

▪ IEEE 802.11n

### IEEE 802.11n

- IEEE 802.11n has ratified on Sep. 2009
- DWL-8600AP supports IEEE 802.11n.
- It has higher performance and more coverage.
- It can support maximum 300Mbps on both 5GHz/2.4GHz concurrently.
- Primary 802.11n feature implemented in DWL-8600AP.
  - 2X2 MIMO
  - Channel Binding
  - Guard Interval

#### Wi-Fi CERTIFIED™ Interoperability Certificate

Certification ID: WFA7771



This certificate lists the capabilities and features that have successfully completed Wi-Fi Alliance interoperability testing. Additional information about Wi-Fi Alliance certification programs is available at [www.wi-fi.org/certification\\_programs.php](http://www.wi-fi.org/certification_programs.php).

Tested Spatial Streams	Dual-Band Concurrent Maximum
Transmit	2
Receive	2

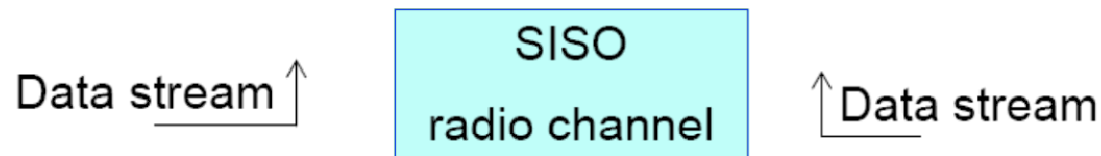
Certificate Date: August 28, 2009  
Company: D-Link Systems  
Product: D-Link Dual Band PoE Access Point / DWL-8600AP  
Model/SKU #: DWL-8600AP/  
Category: Enterprise Access Point, Switch/Controller or Router

IEEE Standard	Security	Multimedia
IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n draft 2.0 IEEE 802.11d IEEE 802.11h  <u>Optional 802.11n Capabilities</u> - Short Guard Interval - 40 MHz operation in 5 GHz - HT Duplicate (MCS 32)	WPA™ - Enterprise, Personal WPA2™ - Enterprise, Personal  <u>EAP Type(s)</u> EAP-TLS EAP-TTLS/MSCHAPv2 PEAPv0/EAP-MSCHAPv2 PEAPv1/EAP-GTC EAP-SIM	WMM®



## Antenna Technology Revolution

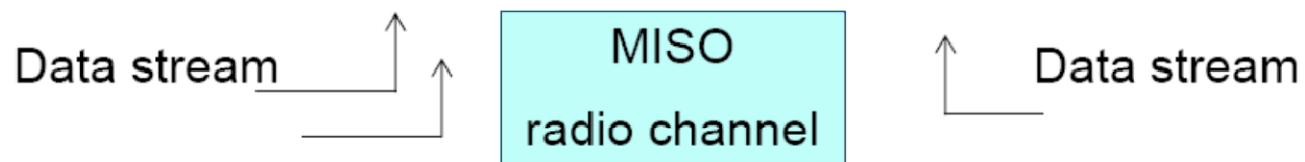
- Single Input, Single-Output channel suffers from fading



- Single-Input, Multiple-Output channel: Rx Diversity



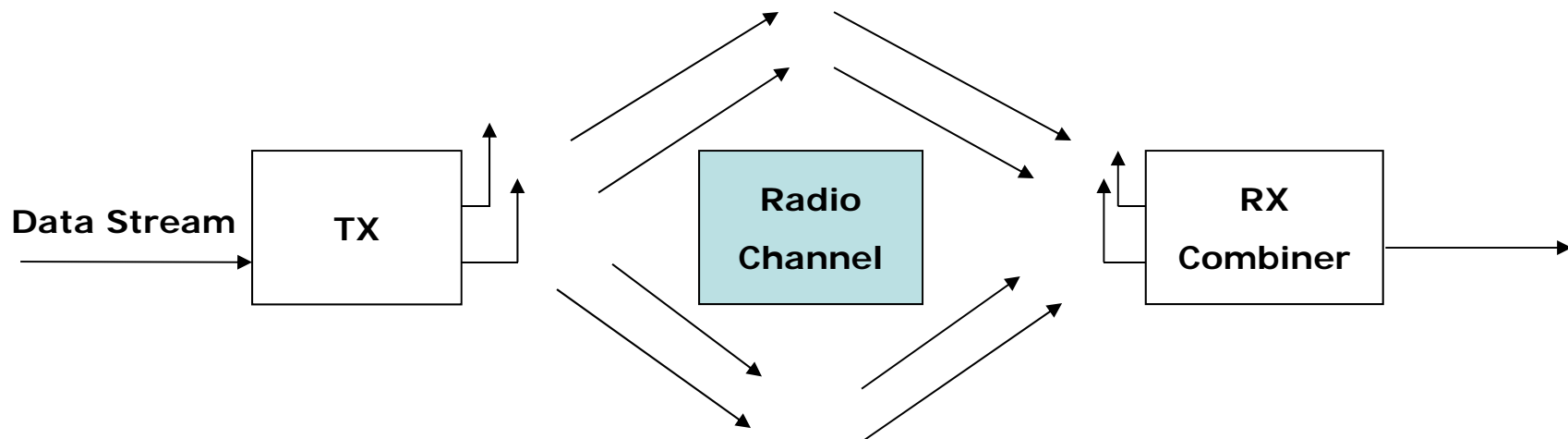
- Multiple-Input, Single-Output channel: Tx Diversity





## Multiple-Input, Multiple-Output (MIMO)

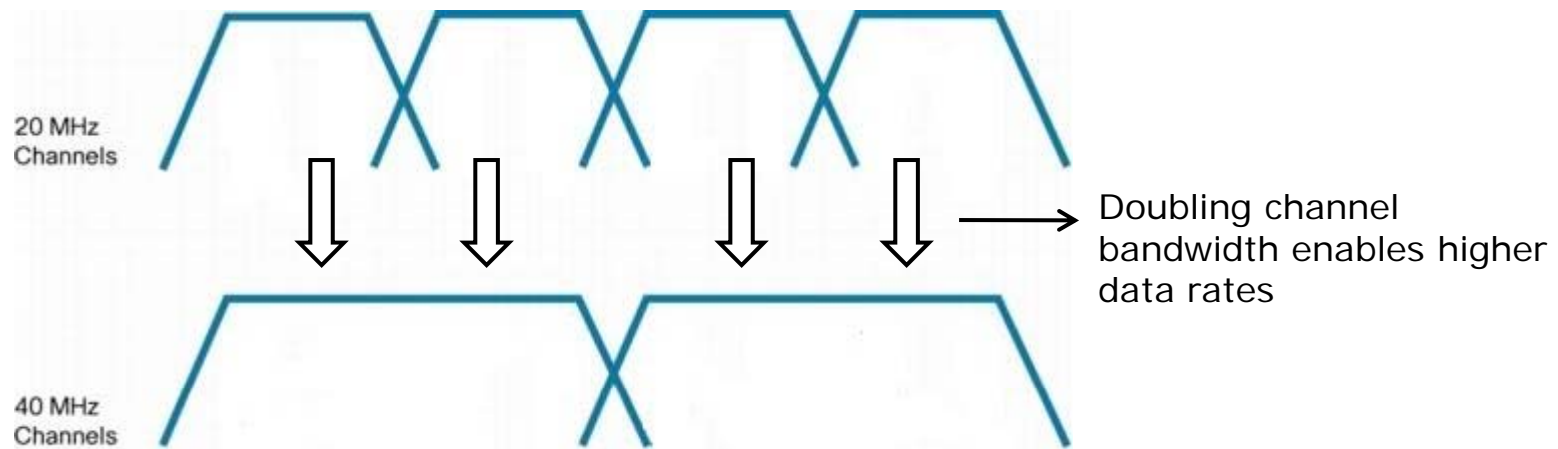
- It is the use of multiple transmitters and receivers (multiple antennas) on wireless devices to improve performance. When two transmitters and two or more receivers are used, two simultaneous data streams can be sent, which double the data rate. Multiple receivers alone allow greater distances between devices.
- DWL-8600 implemented two by two MIMO on both 2.4/5GHz.





## IEEE 802.11n Channel Bandwidth

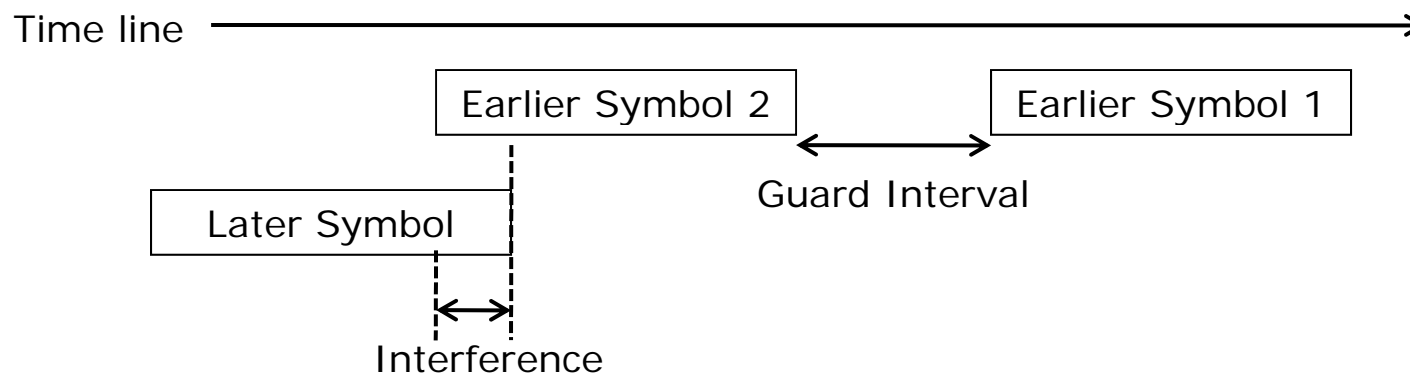
- 802.11a/g uses 20MHz frequency bandwidth per channel.
- 802.11n can use 40MHz channel (optional) which is consist of two 20-MHz channels that are contiguous in the frequency domain.
- With doubling channel bandwidth, the data transmitting/receiving speed is doubled.
- Due to the double channel bandwidth, there are lesser available channels (without interference) compared with 802.11a/g.





## Guard Interval

- Guard Interval is a time period between two transmitted symbols.
- The purpose is to prevent interference in multipath environments. When two symbols arrive over two different paths, the beginning of a new symbol may arrive at the receiver before the last symbol is completely received.
- The default setting of 802.11a/g/n is 800 nanoseconds.
- 802.11n supports short guard interval which shorten the time to 400ns
- It can improve around 10% of performance.







### IEEE 802.11n Parameters

- Go to WLAN → Administration → Advanced Configuration → AP Profile to configure 802.11n parameters (these parameters are not displayed in Basic Setup option).
- 20 or 40MHz Channel Bandwidth could be configured here. Note, the default setting of 5GHz is 40MHz and 2.4GHz is 20MHz.
- Short Guard Interval is enabled by default.
- Primary Channel is used for 802.11n clients that supports only a 20-MHz channel bandwidth and for legacy clients.

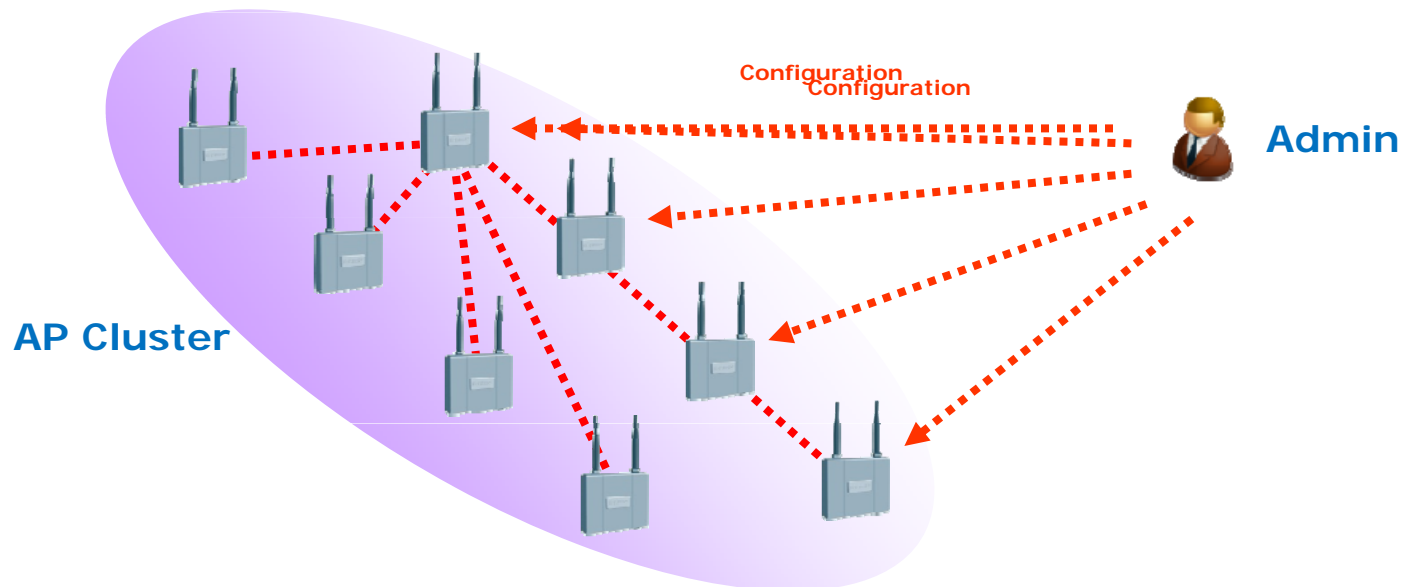
Parameter	Value	Range/Options
State	<input checked="" type="radio"/> On <input type="radio"/> Off	
Mode	IEEE 802.11b/g/n	
RTS Threshold (bytes)	2347	(0 to 2347)
Load Balancing	<input type="checkbox"/>	
Load Utilization (%)	60	(1 to 100)
Maximum Clients	200	(0 to 200)
RF Scan Other Channels	<input type="checkbox"/>	
RF Scan Sentry	<input type="checkbox"/>	
RF Scan Interval (secs)	60	(30 to 120)
RF Scan Sentry Channels	<input checked="" type="checkbox"/> 802.11a <input checked="" type="checkbox"/> 802.11b/g	
RF Scan Duration (msecs)	10	(10 to 2000)
Rate Limiting	<input type="checkbox"/>	
Rate Limit (pkts/sec)	50	(1 to 50)
Rate Limit Burst (pkts/sec)	75	(1 to 75)
Channel Bandwidth	40 MHz	
Protection	Auto	
No ACK	Disable	
DTIM Period (# beacons)	10	(1 to 255)
Beacon Interval (msecs)	100	(20 to 2000)
Automatic Channel	<input checked="" type="checkbox"/>	
Automatic Power	<input checked="" type="checkbox"/>	
Initial Power (%)	100	(1 to 100)
U-APSD Mode	Enable	
Frag Threshold (bytes)	2346	(256 to 2346)
Short Retries	7	
Long Retries	4	
Transmit Lifetime (msecs)	512	
Receive Lifetime (msecs)	512	
Station Isolation	<input type="checkbox"/>	
Primary Channel	Lower	
Short Guard Interval	Enable	
Multicast Tx Rate (Mbps)	Auto	





# AP Clustering

- Admin can treat a group of 8600APs in the same subnet as one single device.
- Previously, admin needs to configure every AP individually.
- AP Clustering
  - Same concept as Switch Clustering.
  - APs share configuration information with each other
  - It provides single point of management for the AP Cluster





# AP Clustering

- APs have to be connected on the same network subnet.
- APs that join the cluster need to have the same Cluster Name.
- Maximum 8 APs in a cluster.
- Clustering mode is enabled on all the APs (default disabled).
- Users can create multiple clusters in a network subnet.

The screenshot shows the D-Link web interface for configuring an access point. On the left is a navigation tree with the following items: Access Point, Basic Settings, Status, Manage, Services, SNMPv3, Maintenance, Client QoS, and Cluster. The 'Cluster' item is expanded, showing sub-items: Access Points, Sessions, Channel Management, Wireless, and Neighborhood. The main content area is titled 'Manage access points in the cluster'. It contains the following text: 'This access point is operating in stand-alone mode...'. Below this is a paragraph: 'This access point is operating in stand-alone mode, and is not managed as part of a cluster. You can choose to manage this access point as part of a cluster. To do this, press the "start clustering" button below.' A 'Start Clustering' button is located below the paragraph. To the right of the text is a status box showing 'Not Clustered' with a single antenna icon and '0 Access Points' with a group of three people icon. Below the status box is a section titled 'Clustering Options...'. It contains three fields: 'Location:' with a text box containing 'not set', 'Cluster Name:' with a text box containing 'default', and 'Clustering IP Version:' with two radio buttons, 'IPv6' and 'IPv4'. The 'IPv4' radio button is selected. An 'Update' button is located at the bottom of the 'Clustering Options...' section.



## AP Clustering Operation

- When multiple APs form cluster, the following arbitration rules determine the AP which control the cluster:
  - Clusters are formed when APs configure the cluster name and enable their clustering mode.
  - Clusters are formed between APs that have same cluster name and are joined by a wired network.
  - When APs start the cluster formation, the first AP that declares itself a member of the cluster wins the arbitration.
  - The AP that wins the arbitration pushes the configuration to the rest of the APs in the cluster.
  - When administrator configures one of the APs in the cluster, that AP will then push the configuration to the rest of the cluster and have control of the cluster.
  - When two disjoint clusters are joined, the first cluster that is created wins the arbitration for cluster control. The configuration on the newer cluster is overwritten by the larger cluster controller.



## AP Clustering Operation (Cont.)

- A single AP can be called as a cluster with one AP and the above rule of arbitration applies.
- APs can be dropped out of cluster if they lose the connectivity to other APs in the cluster. That means if they do not receive discovery packets for 60 seconds. The discovery packets are transmitted every ten seconds.
- If an AP loses connectivity and joins the cluster again before it is dropped from the cluster, any configuration changes to that AP during the lost connectivity will be propagated when connectivity resumes.
- If there is any changes in configuration in the disconnected AP, it will be propagated once the AP joins the cluster again. If there is change in configuration in two disconnected APs, the latest change will be selected and will be propagated across the cluster.



# AP Clustering – Channel Management

- With AP Clustering, the APs automatically assigns radio channels used by clustered access points to reduce interference.
- Administrator can configure the detecting interval and specify the minimum percentage of interference reduction. The proposed plan must be achieved in order to apply Channel Management.
- This mechanism takes the following parameters into consideration:
  - Signal strengths
  - Channel of the detected APs

The screenshot displays the 'Cluster' configuration page in the D-Link web interface. The left sidebar shows a tree view with 'Cluster' expanded, revealing sub-items: 'Access Points', 'Sessions', 'Channel Management', and 'Wireless Neighborhood'. The main content area is titled 'Automatically manage channel assignments' and includes a 'Channels ...' section with a 'Stop' button and the text 'automatically re-assigning channels'. Below this is a table for 'Current Channel Assignments'.

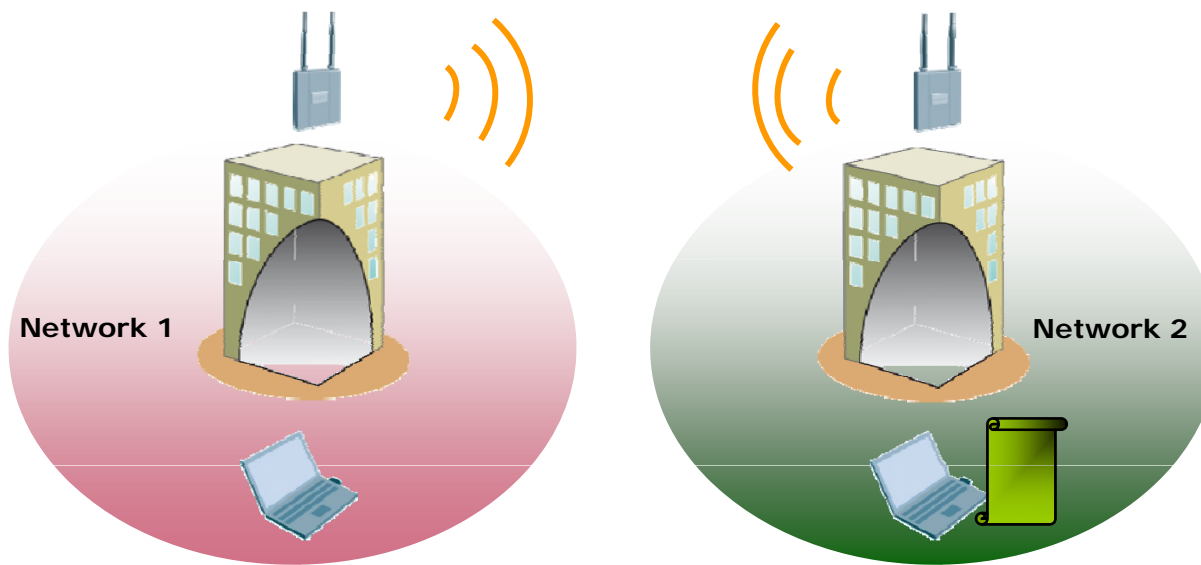
IP Address	Radio	Band	Channel	Locked
172.17.5.145	00:22:B0:3D:95:90	B/G/N	9 (Local Automatic)	<input checked="" type="checkbox"/>
172.17.5.145	00:22:B0:3D:95:80	A/N	116 (Local Automatic)	<input checked="" type="checkbox"/>

An 'Apply' button is located below the table. Below the table, a message states: 'No New channels proposed in the last iteration. Proposed Channel Assignments ( ago )'. This is followed by another table with columns 'IP Address', 'Radio', and 'Proposed Channel'. At the bottom, an 'Advanced' section contains two settings: 'Change channels if interference is reduced by at least' set to '75%' and 'Determine if there is better set of channel settings every' set to '1 Hour'. An 'Apply' button is at the bottom right of the advanced section.



## Wireless Distribution System (WDS)

- WDS allows standalone DWL-8600AP to act as wireless bridge and connect two networks wirelessly.
  - Data is encrypted when it is sent between two networks.
  - There is no need to run cables across two sites.
- Multiple WDS links can be enabled for redundancy
  - It supports 802.1d STP to prevent loops.





# Wireless Distribution System (WDS)

- WDS is only supported by Standalone Mode.
- WDS works in Layer 2 network and connects two or more physical network segments. However, these segments have to be in the same network subnet.
- To build the WDS link between two APs, it is needed to enter the correct MAC address of the opposite AP, and the channel, security of both APs must be the same.
- SSID on both sides must be the same when using WPA/WPA2-PSK.



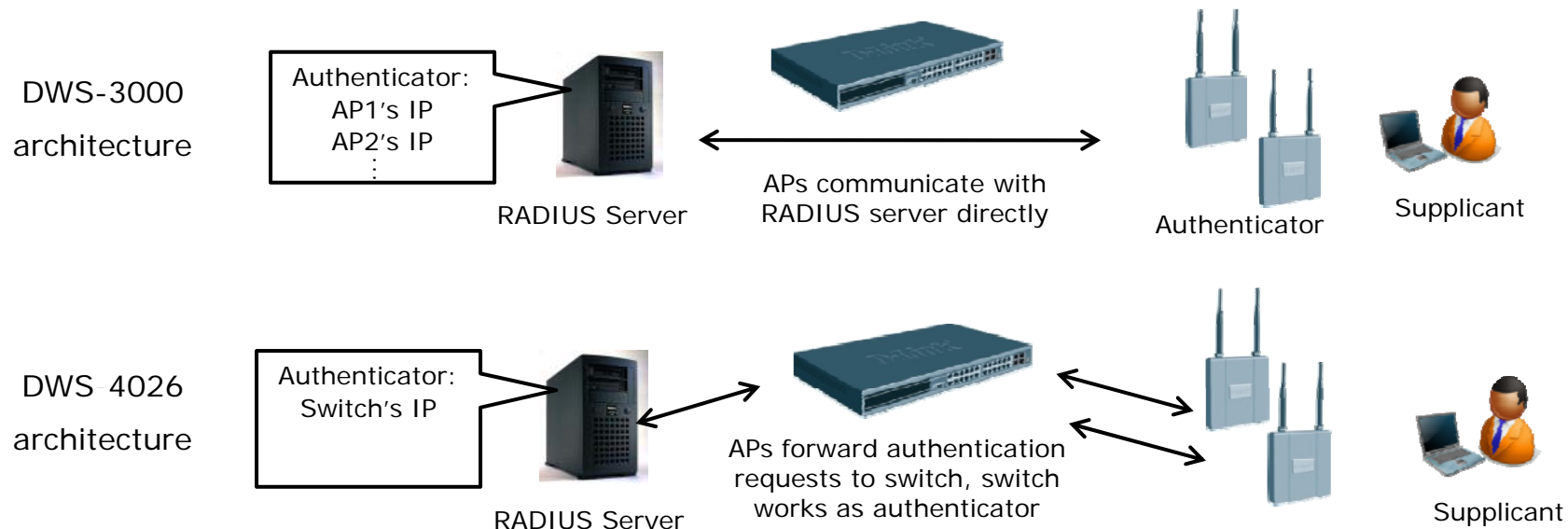


## New Functions Implementation (DWS-4026/DWL-8600AP)

### ▪ Centralized IEEE 802.1x Authentication

## Centralized IEEE 802.1x Authentication

- On DWS-3000's 802.1x process, each AP works as the 802.1x authenticator and authenticates clients individually.
  - All AP's IP have to be configured in RADIUS database.
- New software architecture on DWS-4026 enables Switch to act as 802.1x authenticator.
  - Switch will interface with RADIUS server instead of AP.
  - Only Switch's IP will need to be entered in RADIUS database.





## New Functions Implementation (DWS-4026/DWL-8600AP)

### ▪ Centralized IEEE 802.1x Authentication

## Centralized IEEE 802.1x Authentication

- DWS-3000 system has 1 RADIUS server for wireless authentication, 3 RADIUS servers for wired clients authentication.
- DWS-4026 has up to 32 RADIUS server support, for both wired and wireless authentication.
- DWS-4026 support group of RADIUS servers.
  - Customer configures a RADIUS Server Name first, then assign IP addresses to this RADIUS Server Name as an IP group, when using 802.1x authentication, designate this RADIUS Server Name as the RADIUS server.

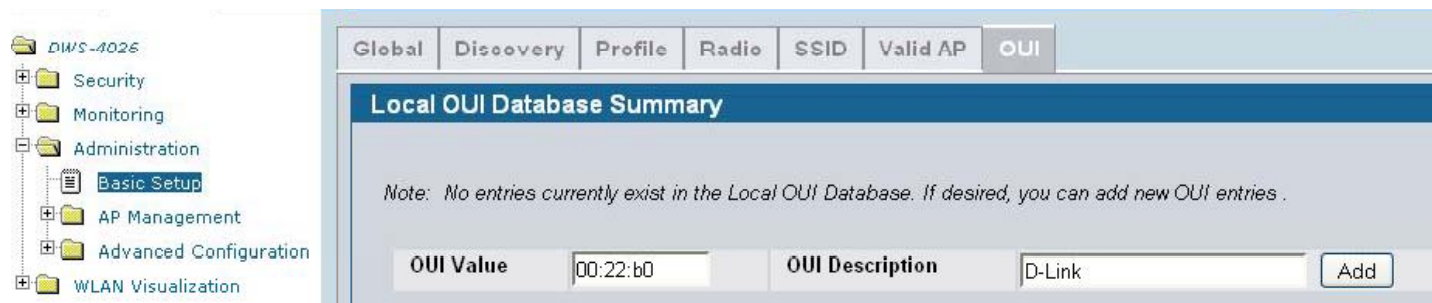
The screenshot displays the D-Link web interface for configuring RADIUS authentication. On the left, a navigation tree shows the 'RADIUS' section expanded, with 'RADIUS Authentication' selected. The main content area is divided into two tabs: 'Configuration' and 'Named Server Status'. The 'Configuration' tab shows the 'RADIUS Authentication Server Configuration' form, which includes fields for 'RADIUS Server Host Address' (with an 'Add' button), 'Host Address', and 'RADIUS Server Name' (set to 'Default-RADIUS-Server'). A 'Submit' button is at the bottom. The 'Named Server Status' tab shows a table of configured servers.

Named Server Status	
RADIUS Authentication Server Name	Default-RADIUS-Server
RADIUS Authentication Server Status	Configured
RADIUS Accounting Server Name	Default-RADIUS-Server
RADIUS Accounting Server Status	Not Configured
RADIUS Use Network Configuration	Enable
RADIUS Accounting	<input type="checkbox"/>



### Other Features

- OUI database
  - DWS-4026 contains a build-in database of registered Organizationally Unique Identifiers (OUIs) which can be used to identify the manufactures of the detected APs and clients.
  - If the detected devices are not in the database, customer can add a new one from the Local OUI Database Summary page, up to 64 user-defined OUIs can be added. The local database is searched first.





### Other Features

- Default SSL Certificate
  - A self-signed SSL certificate is generated by default on the switch.

Secure HTTP Configuration	
HTTPS Admin Mode	Disable
TLS Version 1	Enable
SSL Version 3	Enable
HTTPS Port	443 (1 to 65535)
HTTPS Session Soft Timeout (Minutes)	5 (1 to 60)
HTTPS Session Hard Timeout (Hours)	24 (1 to 168)
Maximum Number of HTTPS Sessions	16 (0 to 16)
Certificate Present?	True <a href="#">Delete</a>
Certificate Generation Status	No certificate generation in progress

[Download Certificates](#) [Generate Certificate](#) [Submit](#)

- IPv6 management of the switch
  - Customer can manage switch with IPv6 IP address.



## New Functions Implementation (DWS-4026/DWL-8600AP)

### ▪ Other Features

## Other Features

- NetBIOS Name Snooping
  - The managed AP snoops the clients' NetBIOS name and send it to the switch.

Associated Client Status

MAC Address	AP MAC Address	SSID	BSSID	Client IP Address	NetBIOS Name	Lo
<input type="checkbox"/> 00:13:46:76:ed:56	00:22:b0:3d:95:80	Dean1	00:22:b0:3d:95:80		DEAN-9D335C7352	

- Captive Portal
  - Allow user to log out of the CP with a pop-up logout button.
  - Support per-user bandwidth control.

Captive Portal Configuration

Enable Captive Portal	<input checked="" type="checkbox"/>	Idle Timeout (secs)	
Configuration Name	Default	Session Timeout (secs)	
Protocol Mode	<input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS	Max Up Rate (bytes/sec)	
Verification Mode	<input checked="" type="radio"/> Guest <input type="radio"/> Local <input type="radio"/> RADIUS	Max Down Rate (bytes/sec)	
User Logout Mode	<input checked="" type="checkbox"/>	Max Receive (bytes)	
Enable Redirect Mode	<input type="checkbox"/>	Max Transmit (bytes)	
Redirect URL		Max Total (bytes)	
RADIUS Auth Server	Default-RADIUS-Server		
User Group	1-Default		

Captive Portal - Logout - Windows ...

http://11.90.90.103/security/captive\_portal/cp\_logout.html

Web Authentication

You are now authorized and connected to the network. Please retain this small logout window in order to de-authenticate. Press the logout button when done.

Logout



### Other Features

- Client QoS

- The Client QoS feature allows users to apply the wired QoS features including access control lists (ACLs) and differentiated service (DiffServ) of the Unified Switch to the wireless clients associated to the AP.
- Enable AP Client QoS first

Peer Group ID	1	(1 to 255)
Client Roam Timeout (secs)	30	(1 to 120)
Ad Hoc Client Status Timeout (hours)	24	(0 to 168)
AP Failure Status Timeout (hours)	24	(0 to 168)
MAC Authentication Mode	white-list	
RF Scan Status Timeout (hours)	24	(0 to 168)
Detected Clients Status Timeout (hours)	24	(0 to 168)
Tunnel IP MTU Size	1500	
Cluster Priority	1	(0 to 255, 0 - Disable)
AP Client QoS	Disable	

- Apply ACL or Differentiated Service for wireless networks based on SSIDs

Client QoS	<input type="checkbox"/>
Client QoS Bandwidth Limit Down (bits-per-second)	0 (0 to 4294967295, 0 - Disable)
Client QoS Bandwidth Limit Up (bits-per-second)	0 (0 to 4294967295, 0 - Disable)
Client QoS Access Control Down	<none>
Client QoS Access Control Up	<none>
Client QoS Diffserv Policy Down	<none>
Client QoS Diffserv Policy Up	<none>



Lab 3

# Switch Clustering





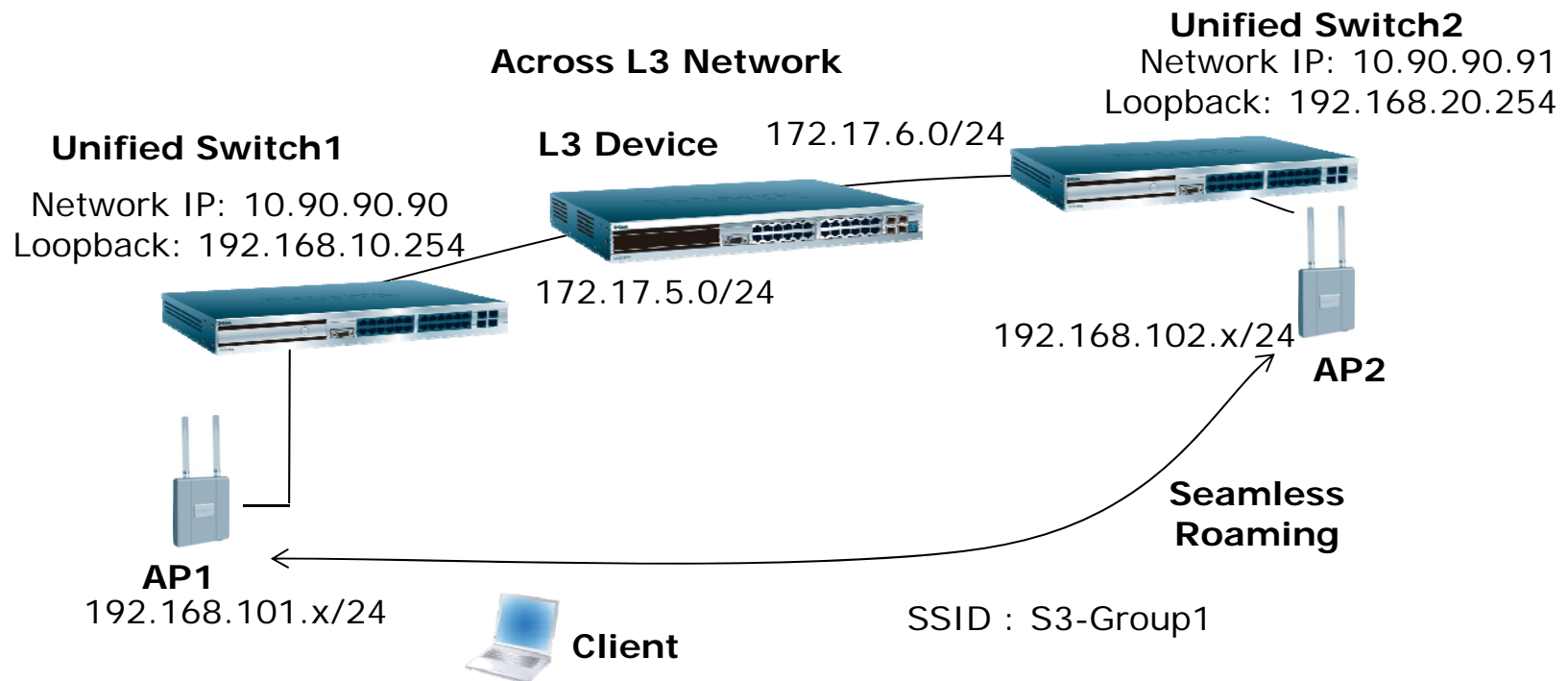
## Lab 3: Switch Clustering

- This scenario is an example to designing switch clustering and Layer 2 distributed tunnel environment.
  
- **Objectives:**
  - Understand how to design and setup a cluster environment.
  - Understand how to select the cluster controller and push configuration between the Unified Switches.
  - Understand the configuration of the Layer 2 distributed tunnel and when to use it.



### Network Topology

- With this topology, users can set up a cluster controller and push configurations to other switches in the same peer group.
- Instead of Layer 3 tunnel, wireless clients can get the same fast roaming result with Layer 2 distributed tunnel.





## Lab 3: Switch Clustering

Table 1: Physical Connection

From Device	From Port	To Device	To Port
Unified Switch 1	1	AP1	N/A
Unified Switch 1	24	L3 Switch	1
Unified Switch 2	1	AP1	N/A
Unified Switch 2	24	L3 Switch	24

Table 2: VLAN and Port Assignment

Device	VLAN ID	VLAN Name	Tagged Ports	Untagged Ports
Unified Switch 1	5	Core5	N/A	24
Unified Switch 1	101	AP1	N/A	1
Unified Switch 1	201	Client1	1	N/A
Unified Switch 2	6	Core6	N/A	24
Unified Switch 2	102	AP2	N/A	1
Unified Switch 2	202	Client2	1	N/A
L3 Switch	5	Core5	N/A	1
L3 Switch	6	Core6	N/A	24



# Lab 3: Switch Clustering

**Table 3: IP Addressing**

Device	Interface	VID	IP Address
Unified Switch 1	Management	1	10.90.90.90/8
Unified Switch 1	Loopback	N/A	192.168.10.254/32
Unified Switch 1	4/1	5	172.17.5.254/24
Unified Switch 1	4/2	101	192.168.101.254/24
Unified Switch 1	4/3	201	192.168.201.254/24
Unified Switch 2	Management	1	10.90.90.91/8
Unified Switch 2	Loopback	N/A	192.168.20.254/32
Unified Switch 2	4/1	6	172.17.6.254/24
Unified Switch 2	4/2	102	192.168.102.254/24
Unified Switch 2	4/3	202	192.168.202.254/24
L3 Switch	ipif5	5	172.17.5.1/24
L3 Switch	ipif6	6	172.17.6.1/24

**Table 4: DHCP Server**

Device	Pool	Network	Excluded IP
Unified Switch 1	101	192.168.101.0/24	192.168.101.200-255
Unified Switch 1	201	192.168.201.0/24	192.168.201.200-255
Unified Switch 2	102	192.168.102.0/24	192.168.201.200-255
Unified Switch 2	202	192.168.202.0/24	192.168.202.200-255



### Lab Scenario Discussion

- Can I push configurations from Unified Switch 2 (Non cluster controller) to Unified Switch 1?
- Can I see peer switch managed AP or run auto channel/power for peer switch managed AP on Unified Switch 2?
- Why need a static route on Unified Switch 1 and 2?
- AP1 and AP2 are in different IP subnets, what if they are in the same subnet?
- How to confirm L2 Tunnel is working?



Session 6

# Command Line Interface



## Session 6: Command Line Interface

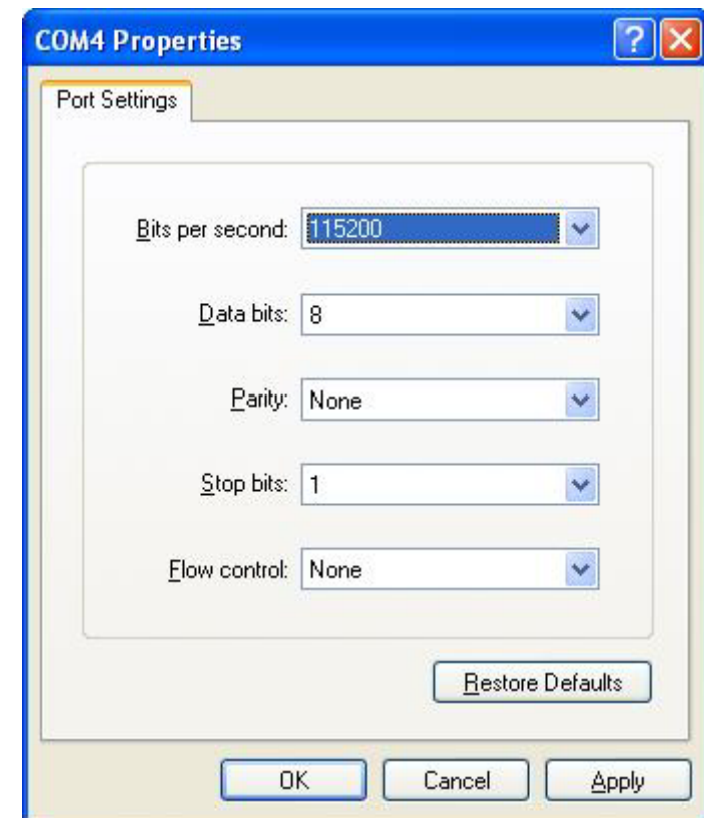
- Command Line Interface





# Command Line Interface

- Use the following settings to make a console connection:
  - Select the appropriate serial port (**COM port 1 or COM port 2**).
  - Set the data rate to 115200 baud.
  - Set the data format to **8 data bits**, **1 stop bit**, and **no parity**.
  - Set **flow control** to **none**.
- In command line interface, enter a question mark (?) at the command prompt to display the commands available in the current mode.
- The full command keyword appears when sufficient unique characters are typed. Once you have entered sufficient letters, press the **SPACEBAR** or **TAB** key to complete the keyword.





### CLI and Scenario

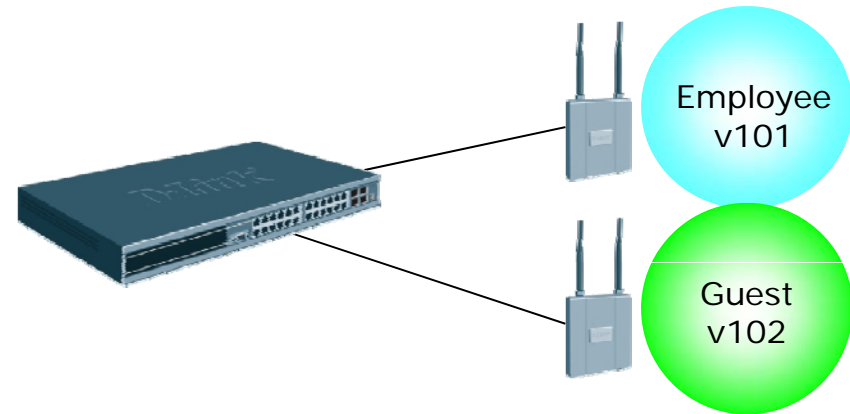
- There are three basic levels of Command Mode for users to classify user privilege. Different modes can run different level of commands.
- User EXEC mode is the first level that contains a limited set of commands to view basic system information, enter **enable** to get into Privileged EXEC mode.
- The Privileged EXEC mode allows you to enter any EXEC command or enter the Global Configuration mode with the command **configure**
- Global Config mode groups general setup commands and permits making modifications to the running configuration.

Command Mode	Prompt	Access Method	Exit or Access Previous Mode
User EXEC	(DWS-4026) >	This is the first level of access.	To exit, enter <b>logout</b>
Privileged EXEC	(DWS-4026) #	From the User EXEC mode, enter <b>enable</b>	To exit to User EXEC mode, enter <b>exit</b> or press <b>Ctrl-z</b>
Global Config	(DWS-4026) (Config) #	From the Privileged EXEC mode , enter <b>configure</b>	To exit to Privileged EXEC mode, enter <b>exit</b> or press <b>Ctrl-z</b>



### CLI Example

- The user wants to have two SSIDs to classify the wireless users, one with VLAN 101 for employees, the other one with VLAN 102 for guest. Different SSIDs have different security, the expected configurations are as follows:



VLAN ID	VLAN Name	Tagged Port	Untagged Port	Interface/IP
10	AP1	N/A	1	192.168.10.254/24
20	AP2	N/A	13	192.168.20.254/24
101	employee	1, 13	N/A	192.168.101.254/24
102	guest	1, 13	N/A	192.168.102.254/24

SSID	VLAN ID	Security	Key
employee	101	WPA-PSK	12345678
guest	102	WEP	12345



# CLI Example

### 1. Assign Switch IP Address

(DWS-4026) >enable

Password:

(DWS-4026) #network parms 192.168.1.241 255.255.255.0

### 2. Create VLANs

(DWS-4026) #vlan database

(DWS-4026) (Vlan)#vlan 10

(DWS-4026) (Vlan)#vlan 20

(DWS-4026) (Vlan)#vlan 101

(DWS-4026) (Vlan)#vlan 102

(DWS-4026) (Vlan)#vlan name 10 AP1

(DWS-4026) (Vlan)#vlan name 20 AP2

(DWS-4026) (Vlan)#vlan name 101 employee

(DWS-4026) (Vlan)#vlan name 102 guest

### 3. Create IP Interface by VLANs

(DWS-4026) (Vlan)#vlan routing 10

(DWS-4026) (Vlan)#vlan routing 20

(DWS-4026) (Vlan)#vlan routing 101

(DWS-4026) (Vlan)#vlan routing 102

(DWS-4026) (Vlan)#exit



# CLI Example

### 4. Assign VLANS settings to the ports

```
(DWS-4026) #configure
(DWS-4026) (Config)#interface 0/1
(DWS-4026) (Interface 0/1)#vlan participation include 10
(DWS-4026) (Interface 0/1)#vlan participation include 101
(DWS-4026) (Interface 0/1)#vlan participation include 102
(DWS-4026) (Interface 0/1)#vlan pvid 10
(DWS-4026) (Interface 0/1)#vlan tagging 101
(DWS-4026) (Interface 0/1)#vlan tagging 102
(DWS-4026) (Interface 0/1)#exit
(DWS-4026) (Config)#interface 0/13
(DWS-4026) (Interface 0/13)#vlan participation include 20
(DWS-4026) (Interface 0/13)#vlan participation include 101
(DWS-4026) (Interface 0/13)#vlan participation include 102
(DWS-4026) (Interface 0/13)#vlan pvid 20
(DWS-4026) (Interface 0/13)#vlan tagging 101
(DWS-4026) (Interface 0/13)#vlan tagging 102
(DWS-4026) (Interface 0/13)#exit
```

### 5. Setup the IP Routing Interface

```
(DWS-4026) (Config)#interface loopback 0
```



### CLI Example

```
(DWS-4026) (Interface loopback 0)#ip address 192.168.0.254 255.255.255.0
(DWS-4026) (Interface loopback 0)#exit
(DWS-4026) (Config)#interface 4/1
(DWS-4026) (Interface 4/1)#ip address 192.168.10.254 255.255.255.0
(DWS-4026) (Interface 4/1)#exit
(DWS-4026) (Config)#interface 4/2
(DWS-4026) (Interface 4/2)#ip address 192.168.20.254 255.255.255.0
(DWS-4026) (Interface 4/2)#exit
(DWS-4026) (Config)#interface 4/3
(DWS-4026) (Interface 4/3)#ip address 192.168.101.254 255.255.255.0
(DWS-4026) (Interface 4/3)#exit
(DWS-4026) (Config)#interface 4/4
(DWS-4026) (Interface 4/4)#ip address 192.168.102.254 255.255.255.0
(DWS-4026) (Interface 4/4)#exit
(DWS-4026) (Config)#ip routing
```

#### 6. Setup DHCP

```
(DWS-4026) (Config)#service dhcp
(DWS-4026) (Config)#ip dhcp pool AP1
(DWS-4026) (Config-dhcp-pool)#network 192.168.10.0 255.255.255.0
(DWS-4026) (Config-dhcp-pool)#default-router 192.168.10.254
(DWS-4026) (Config-dhcp-pool)#ex
```



### CLI Example

```
(DWS-4026) (Config)#ip dhcp pool AP2
(DWS-4026) (Config-dhcp-pool)#network 192.168.20.0 255.255.255.0
(DWS-4026) (Config-dhcp-pool)#default-router 192.168.20.254
(DWS-4026) (Config-dhcp-pool)#exit
(DWS-4026) (Config)#ip dhcp pool employee
(DWS-4026) (Config-dhcp-pool)#network 192.168.101.0 255.255.255.0
(DWS-4026) (Config-dhcp-pool)#default-router 192.168.101.254
(DWS-4026) (Config-dhcp-pool)#exit
(DWS-4026) (Config)#ip dhcp pool guest
(DWS-4026) (Config-dhcp-pool)#network 192.168.102.0 255.255.255.0
(DWS-4026) (Config-dhcp-pool)#default-router 192.168.102.254
(DWS-4026) (Config-dhcp-pool)#exit
(DWS-4026) (Config)#ip dhcp excluded-address 192.168.10.100 192.168.10.255
(DWS-4026) (Config)#ip dhcp excluded-address 192.168.20.100 192.168.20.255
(DWS-4026) (Config)#ip dhcp excluded-address 192.168.101.100 192.168.101.255
(DWS-4026) (Config)#ip dhcp excluded-address 192.168.102.100 192.168.102.255
```

#### 7.1 Configure wireless setting

```
(DWS-4026) (Config)#wireless
(DWS-4026) (Config-wireless)#country-code us
Are you sure you want to change the country code? (y/n) y
```





# CLI Example

## 7.2 Configure AP Discovery

```
(DWS-4026) (Config-wireless)#discovery vlan-list 10
```

```
(DWS-4026) (Config-wireless)#discovery vlan-list 20
```

## 7.3 Add the APs the valid AP database

```
(DWS-4026) (Config-wireless)#ap database 00:22:B0:3D:95:80
```

```
(DWS-4026) (Config-ap)#profile 1
```

```
(DWS-4026) (Config-ap)#location AP1
```

```
(DWS-4026) (Config-ap)#exit
```

```
(DWS-4026) (Config-wireless)#ap database 00:22:B0:3D:95:90
```

```
(DWS-4026) (Config-ap)#profile 1
```

```
(DWS-4026) (Config-ap)#location AP2
```

```
(DWS-4026) (Config-ap)#exit
```

## 7.4 Configure SSID

```
(DWS-4026) (Config-wireless)#network 1
```

```
(DWS-4026) (Config-network)#vlan 101
```

```
(DWS-4026) (Config-network)#ssid employee
```

```
(DWS-4026) (Config-network)#security mode wpa-personal
```

```
(DWS-4026) (Config-network)#wpa key 12345678
```

```
(DWS-4026) (Config-network)#exit
```



### CLI Example

```
(DWS-4026) (Config-wireless)#network 2
(DWS-4026) (Config-network)#vlan 102
(DWS-4026) (Config-network)#ssid guest
(DWS-4026) (Config-network)#security mode static-wep
(DWS-4026) (Config-network)#wep key type ascii
(DWS-4026) (Config-network)#wep key length 64
(DWS-4026) (Config-network)#wep key 1 12345
(DWS-4026) (Config-network)#exit
```

#### 7.5 Assign SSID to the correct profile and radio

```
(DWS-4026) (Config-wireless)#ap profile 1
(DWS-4026) (Config-ap-profile)#name Test
(DWS-4026) (Config-ap-profile)#radio 1
(DWS-4026) (Config-ap-radio)#vap 0
(DWS-4026) (Config-ap-profile-vap)#network 1
(DWS-4026) (Config-ap-profile-vap)#enable
(DWS-4026) (Config-ap-profile-vap)#exit
(DWS-4026) (Config-ap-radio)#vap 1
(DWS-4026) (Config-ap-profile-vap)#network 2
(DWS-4026) (Config-ap-profile-vap)#enable
(DWS-4026) (Config-ap-profile-vap)#exit
(DWS-4026) (Config-ap-radio)#exit
```



### CLI Example

```
(DWS-4026) (Config-ap-profile)#radio 2
(DWS-4026) (Config-ap-radio)#vap 0
(DWS-4026) (Config-ap-profile-vap)#network 1
(DWS-4026) (Config-ap-profile-vap)#enable
(DWS-4026) (Config-ap-profile-vap)#exit
(DWS-4026) (Config-ap-radio)#vap 1
(DWS-4026) (Config-ap-profile-vap)#network 2
(DWS-4026) (Config-ap-profile-vap)#enable
(DWS-4026) (Config-ap-profile-vap)#exit
(DWS-4026) (Config-ap-radio)#exit
(DWS-4026) (Config-ap-profile)#exit
(DWS-4026) (Config-wireless)#exit
(DWS-4026) (Config)#exit
```

#### 8. Save Configuration

```
(DWS-4026) #write memory
```



Session 7

# System Maintenance and Troubleshooting



### **Session 7: System Maintenance and Troubleshooting**

- Firmware Upgrade
- Backup Configuration File
- Factory Reset and Image Problem
- Logs



# Firmware Upgrade – Unified Switch

- Upgrade firmware from Tool → Download File of the Web UI



**Download File To Switch**

File Type	Code
Image Name	image1
Transfer Mode	TFTP
Server Address Type	IPv4
Server Address	10.90.90.100
Transfer File Path	
Transfer File Name	helio_switch_1006.opr
<input type="checkbox"/> Start File Transfer	

- Upgrade firmware from CLI
  - copy tftp://10.90.90.90/helio\_switch\_1006.opr image1
- D-Link Unified Switch supports dual image, users can select one of them as the operation image and the other as the backup image.
- Check and active images from Tool → Multiple Image Service



**Multiple Image Service**

**Active Image**

Image1 Ver	Image2 Ver	Current-active	Next-active
1.0.0.6		image1	image1

Image Name: Image1 Image2 Activate Delete

**Image Description**

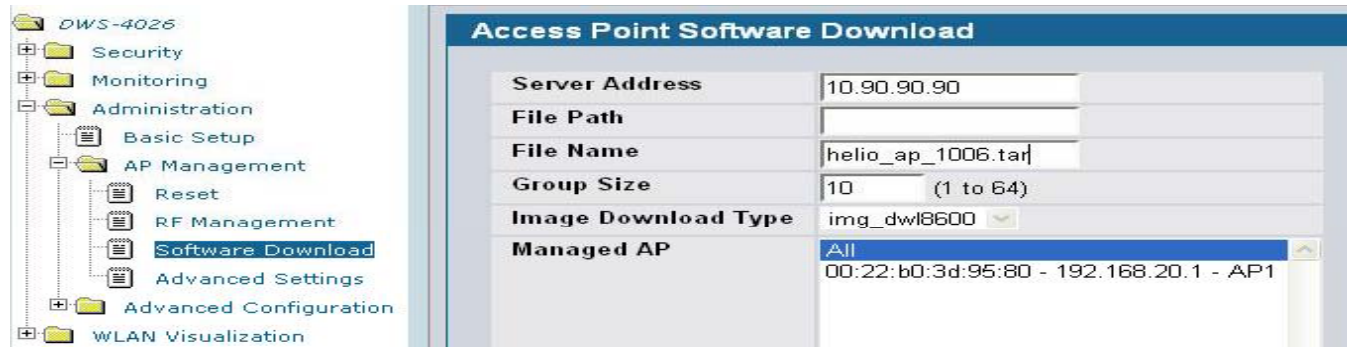
Image	Description
Image1	default image
Image2	

Change Change



# Firmware Upgrade – Unified AP

- Upgrade firmware from Unified Switch when the AP is in Managed Mode
- WLAN → Administration → AP Management → Software Download
- Able select the number of APs to be upgraded concurrently from group size



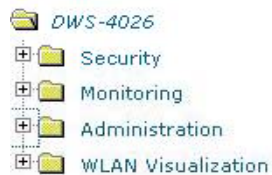
- The firmware could be upgraded from CLI
  - `firmware-upgrade tftp://10.90.90.100/ap_21012.tar`
- In Standalone Mode, firmware is upgraded from Tool → Upgrade of the Web UI
- Note: It needs approximately 12 minutes to complete the process. Do not power off the AP in this time, or firmware may be corrupted.





# Backup Configuration File

- Backup or recover the configuration file from Tool → Upload/Download of the WebUI.



- Backup configuration from CLI.
  - copy nvram:startup-config tftp://10.90.90.100/ConfigFile.txt
  - copy tftp://10.90.90.100/ConfigFile.txt nvram:startup-config
- Note: DWS-3000 only supports binary config file and DWS-4026 supports text-based file.



## Backup Configuration File – Script Files

- D-Link Unified Switch provides another type of text based configuration file called Script file.
- For DWS-3000 series, this is the only way to edit the configuration without using switch.
- Commands:
  - show running-config config.scr (config.scr is the name assigned for this config file)
  - copy nvram: script config.scr tftp://10.90.90.111/config.scr (config.scr is the config file to download to the PC, 10.90.90.111 is the PC's IP)
- The config.scr file can be edited with notepad or MS word.
- Upload the configuration back to switch.
  - copy tftp://10.90.90.111/config.scr nvram:script config.scr
  - script apply config.scr



## **Firmware and Configuration between DWS-3000/DWS-4000 Series**

- There is no upgrade path from DWS-3000 switch to DWS-4000 switch
- There is no conversion path from DWS-4000 switch to DWS-3000 switch
- The configurations for DWS-3000 and DWS-4000 are different in format and content
  - They do not inter-operate.
  - The binary configuration of DWS-3000 cannot be transferred to DWS-4000.
  - Similarly, the text/binary configuration of DWS-4000 cannot be transferred to DWS-3000.



## Switch Boot Menu and Reset Password

- There is no reset button, backdoor password or password recovery for Unified Switches.
- If the users forget the password, the configuration of the switch needs to be reset to factory default through console.
- When the switch is powered on, select option 2 to enter the Boot Menu through console.
- Select 16 to reset password to default
- For DWS-3000 series, option 16 is supported, the only way you can do is to reset all the configurations.
- Select 10 - Restore configuration to factory defaults (delete config files)

```
COM4 - Tera Term VT
File Edit Setup Control Window Help
Boot Menu Version (Date): 15 OCT 2009
Select an option. If no selection in 10 seconds then
operational code will start.

1 - Start operational code.
2 - Start Boot Menu.
Select (1, 2):2

Boot Menu Version (Date): 15 OCT 2009

Options available
1 - Start operational code
2 - Change baud rate
3 - Retrieve event log using XMODEM
4 - Load new operational code using XMODEM
5 - Display operational code vital product data
6 - Run flash diagnostics
7 - Update boot code
8 - Delete operational code
9 - Reset the system
10 - Restore configuration to factory defaults (delete config files)
11 - Activate Backup Image
16 - Restore Password to factory default and start operational code
[Boot Menu]
```



## AP Reset

- If the password of the AP is forgotten, there is no backdoor password, press the reset button to reset the configuration to factory default.
- Remember the password of the AP but forget the IP address.
  - Need to reset on DWL-3500/8500AP
  - For DWL-8600AP, go through console to check the IP
  - Command: get management
    - “static-ip” is the manually configured IP
    - “ip” is the current using IP which may be from DHCP server

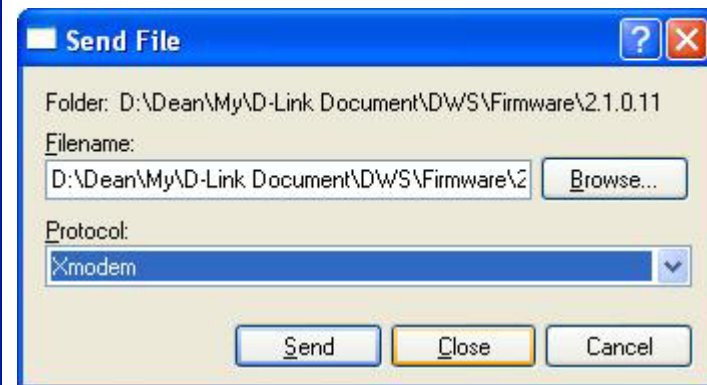
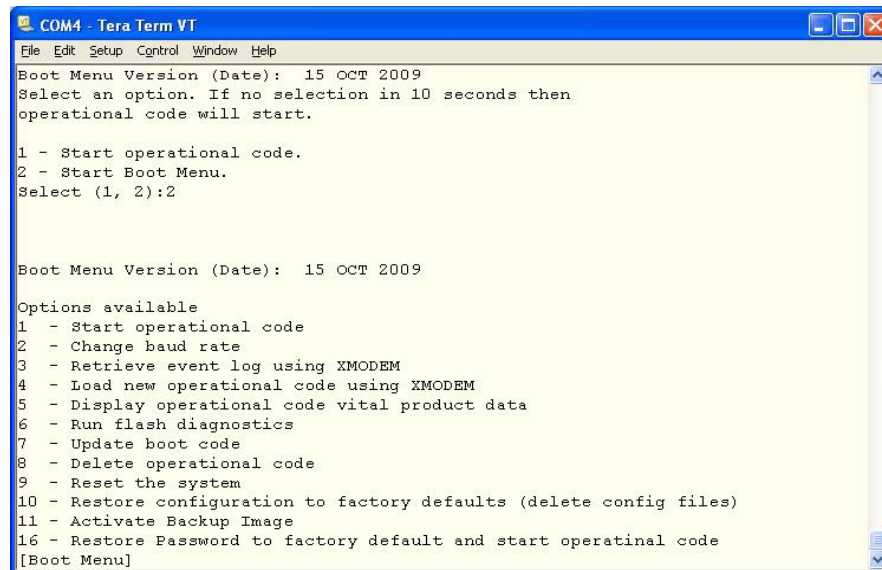
```
COM4 - Tera Term VT
File Edit Setup Control Window Help
DLINK-WLAN-AP login:
DLINK-WLAN-AP login: admin
Password:
Enter 'help' for help.

DLINK-WLAN-AP#
DLINK-WLAN-AP# get management
Property      Value
-----
vlan-id       1
interface     brtrunk
static-ip      10.90.90.91
static-mask    255.0.0.0
ip             192.168.20.1
mask           255.255.255.0
mac            00:22:B0:3D:95:80
dhcp-status    up
ipv6-status    down
ipv6-autoconfig-status up
static-ipv6    ::
static-ipv6-prefix-length 0
DLINK-WLAN-AP#
```



## Damage Image - Switch

- Enter the Boot Menu through console.
- Select 11 – Activate Backup Image.
- If there is no backup image or the backup image does not work, select “4 - Load new operational code using XMODEM” to upload a new firmware.
- Send the firmware file through the Hyper Terminal.







## Logs – Unified Switches

- There are several types of switch logs.



- System log
  - Contain error messages for catastrophic events
  - Not understandable to users, only for R&D troubleshooting

System Log						
Entry		Filename	Line	TaskID	Code	Time
00001:	EVENT>	bootos.c	256	0FFFFE00	AAAAAAAA	0 0 3
00002:	ERROR>	usmdb_sim.c	1541	0FFFFE00	00000000	0 0 2
00003:	EVENT>	bootos.c	256	0FFFFE00	AAAAAAAA	0 0 3
00004:	ERROR>	usmdb_sim.c	1541	0FFFFE00	00000000	0 0 2
00005:	EVENT>	bootos.c	256	0FFFFE00	AAAAAAAA	0 0 3
00006:	ERROR>	usmdb_sim.c	1541	0FFFFE00	00000000	0 0 2





## Buffered Log

- This log stores messages in memory based upon the settings for message component and severity.
- It is enabled by default.
- It disappears after rebooting.
- Only the latest 128 entries are displayed on webpage.

**Buffered Logs**

Total number of Messages 1962 (displaying only the last 128 messages)

<14> FEB 08 10:19:05 11.90.90.97-1 UNKN[157963528]: wsap\_stats.c(1330) 1838 %%  
wsapStatsClientStatsProcess(): AP for associated client mismatch requesting AP to resend client info.

<14> FEB 08 10:19:05 11.90.90.97-1 UNKN[148257352]: clientassoc.c(990) 1839 %% Dropping client  
disassociation message from AP:00:22:b0:3d:91:c0,client:00:23:76:41:30:54 is no more associated to this  
VAP:00:22:b0:3d:91:d1!

<14> FEB 08 10:20:05 11.90.90.97-1 UNKN[157963528]: wsap\_stats.c(1330) 1840 %%  
wsapStatsClientStatsProcess(): AP for associated client mismatch requesting AP to resend client info.

<14> FEB 08 10:20:05 11.90.90.97-1 UNKN[148257352]: clientassoc.c(990) 1841 %% Dropping client  
disassociation message from AP:00:22:b0:3d:95:c0,client:00:23:76:41:30:54 is no more associated to this  
VAP:00:22:b0:3d:95:d1!

<14> FEB 08 10:24:10 11.90.90.97-1 UNKN[157963528]: wsap\_stats.c(1330) 1842 %%  
wsapStatsClientStatsProcess(): AP for associated client mismatch requesting AP to resend client info.

<14> FEB 08 10:24:11 11.90.90.97-1 UNKN[148257352]: clientassoc.c(990) 1843 %% Dropping client  
disassociation message from AP:00:22:b0:3d:91:c0,client:00:23:76:41:30:54 is no more associated to this  
VAP:00:22:b0:3d:91:d1!

<14> FEB 08 10:25:05 11.90.90.97-1 UNKN[157963528]: wsap\_stats.c(1330) 1844 %%



## Persistent Log

- The persistent log is stored in persistent storage, which means that the log messages are retained even if the switch reboots.
- The first log type is the system startup log. The system startup log stores the first 32 messages received after system reboot. The log full operation attribute is always set to "stop on full". This log can store up to 32 messages.
- The second log type is the system operation log. The system operation log stores the last 1000 messages received during system operation. The log full operation attribute is always set to "overwrite". This log can store up to 1000 messages.

The screenshot displays the configuration interface for a D-Link switch. On the left, a tree view shows various configuration categories, with 'Log' expanded to show 'Buffered Log', 'System Log', 'Persistent Log' (selected), and 'Trap Log'. The main panel, titled 'Persistent Logs', shows the 'Number of Persistent Messages' set to 32. Below this, a list of log entries is displayed, each starting with a message ID, a timestamp, and a source IP address, followed by a description of the event.

Message ID	Timestamp	Source IP	Event Description
00001	JAN 01 00:00:29	11.90.90.97-1	TRAPMGR[163879856]: traputil.c(598) 20 %% Wireless switch enabled
00002	JAN 01 00:00:29	11.90.90.97-1	TRAPMGR[47282248]: traputil.c(598) 21 %% Link Up: 0/1
00003	JAN 01 00:00:29	11.90.90.97-1	TRAPMGR[47282248]: traputil.c(598) 24 %% Link Up: 0/2
00004	JAN 01 00:00:35	11.90.90.97-1	TRAPMGR[61982952]: traputil.c(598) 25 %% Cold Start: Unit: 0
00005	JAN 01 00:00:36	11.90.90.97-1	TRAPMGR[47282248]: traputil.c(598) 26 %% Link Up: 0/24
00006	JAN 01 00:00:44	11.90.90.97-1	TRAPMGR[163879856]: traputil.c(598) 27 %% Wireless switch disabled
00007	JAN 01 00:00:59	11.90.90.97-1	TRAPMGR[163879856]: traputil.c(598) 30 %% Wireless switch enabled
00008	JAN 01 00:01:04	11.90.90.97-1	TRAPMGR[148257352]: traputil.c(598) 31 %% Wireless managed AP MAC: 00:22:b0:3d:95:c0 discovered
00009	JAN 01 00:01:04	11.90.90.97-1	TRAPMGR[148257352]: traputil.c(598) 32 %% Wireless managed AP MAC: 00:22:b0:3d:91:c0 discovered
00010	JAN 26 10:53:07	11.90.90.97-1	SNTP[91395984]: sntp_client.c(1675) 33 %% SNTP: system clock



## Send to Log Server

- Enable System Log Configuration
  - LAN → Administration → Log → System Log Configuration
- Configure the IP address of the log server
  - LAN → Administration → Log → Host Configuration
- Debug (7) will include all log message

The screenshot displays the 'Hosts Configuration' web interface. On the left is a navigation tree with the following items: Authentication List Cor, User Login, Denial Of Service Prot, Multiple Port Mirroring, System Severity Setti, Telnet Sessions, Outbound Telnet Clie, Ping Test, SNTP, Port Configuration, Log, System Log Configu, Buffered Log Config, Command Logger C, and Host Configuration (which is highlighted). The main panel is titled 'Hosts Configuration' and contains the following fields:

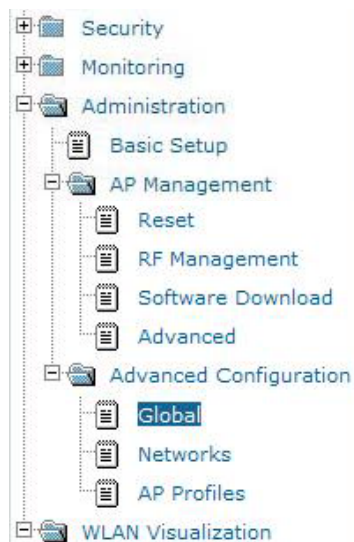
Field	Value
Host	10.90.90.100
IP Address	10.90.90.100
Status	Active
Port	514 (1 to 65535)
Severity Filter	Critical (2)

Below the 'Severity Filter' dropdown, a list of severity levels is visible: Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Informational (6), and Debug (7). The 'Subn' button is located at the bottom left of the configuration area, and the 'esh' button is at the bottom right.



# SNMP Trap Log

- SNMP Traps is defined to inform administrator of events such as entry addition, deletion and database full events.
- The administrator can choose the types of traps to receive.



Wireless SNMP Trap Configuration	
AP Failure Traps	Disable ▼
AP State Change Traps	Disable ▼
Client Failure Traps	Enable ▼
Client State Change Traps	Disable ▼
Peer Switch Traps	Disable ▼
RF Scan Traps	Disable ▼
Rogue AP Traps	Disable ▼
Wireless Status Traps	Disable ▼
<input type="button" value="Submit"/>	





## Logs – Unified AP

- From command line:
  - get log-entry - show logs on AP
- Using the syslog server:
  - set log relay-enabled 1
  - set log relay-host xx.yy.zz.aa, where xx.yy.zz.aa is the syslog server
  - set log severity 7

```
DLINK-WLAN-AP# set log relay-enabled 1
DLINK-WLAN-AP# set log relay-host 192.168.1.1
DLINK-WLAN-AP# set log severity 7
DLINK-WLAN-AP# get log detail
Property      Value
-----
persistence   yes
severity      7
relay-enabled  1
relay-host     192.168.1.1
relay-port    514
DLINK-WLAN-AP#
```



Lab 4

# Command Line Interface and Dynamic VLAN



### Lab 4: Command Line Interface and Dynamic VLAN

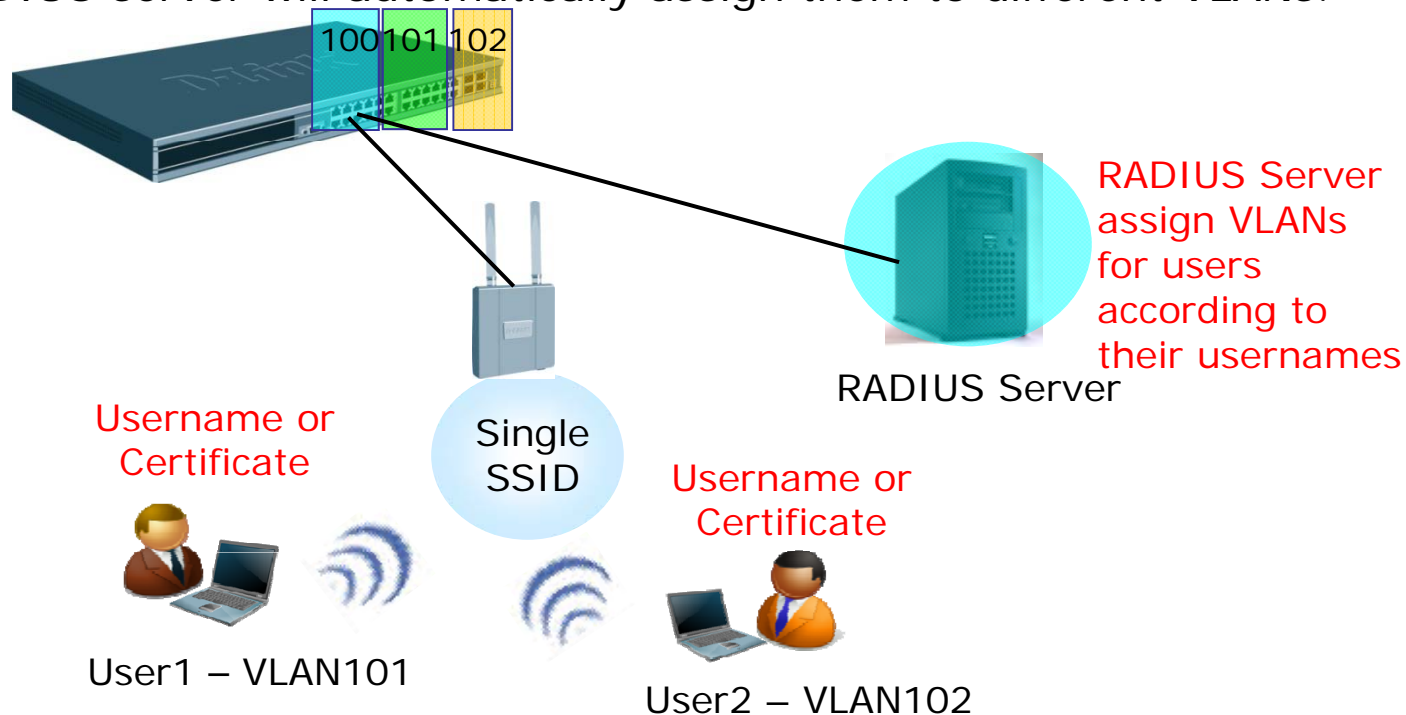
- This scenario shows when and how to use the Dynamic VLAN Assignment function.
  
- **Objectives:**
  - Understand how to use dynamic VLAN function.
  - Understand how to set up the RADIUS server for Dynamic VLAN environment.
  - Different users are assigned to different VLAN.





### Network Topology

- In this scenario, the users can group wireless users to different VLAN with only one SSID and multiply SSIDs are not required.
- End users need to support WPA/WPA2-Enterprise, and enter the WPA/WPA2 authentication according to the identifications.
- RADIUS server will automatically assign them to different VLANs.





### Lab 4: Command Line Interface and Dynamic VLAN

Table 1: Physical Connection

From Device	From Port	To Device	To Port
Unified Switch	1	AP	N/A
Unified Switch	9	RADIUS Server	N/A

Table 2: VLAN and Port Assignment

Device	VLAN ID	VLAN Name	Tagged Ports	Untagged Ports
Unified Switch	100	AP	N/A	1, 9
Unified Switch	101	UserGroup1	1	N/A
Unified Switch	102	UserGroup2	1	N/A



### Lab 4: Command Line Interface and Dynamic VLAN

Table 3: IP Addressing

Device	Interface	VID	IP Address
Unified Switch	4/1	100	192.168.100.254/24
Unified Switch	4/2	101	192.168.101.254/24
Unified Switch	4/3	102	192.168.102.254/24

Table 4: DHCP Server

Device	Pool	Network	Excluded IP
Unified Switch	AP	192.168.100.0/24	192.168.100.200-255
Unified Switch	UserGroup1	192.168.101.0/24	192.168.101.200-255
Unified Switch	UserGroup2	192.168.102.0/24	192.168.102.200-255



### Lab Scenario Discussion

- Must I use WPA-Enterprise for Dynamic VLAN?
- Are radius settings on DWS-4026 and DWS-3000 the same?