Course Overview

- The D-Link Certified Specialist: Wireless LAN (DCS) course is designed to give the students a firm understanding of Wireless LAN (WLAN) fundamentals and give them skills to deploy simple D-Link Wireless solutions.
- The students will get familiar WLAN technology basics and learn how to install, configure, operate and maintain a basic wireless network based on D-Link equipment.
- Participants will have the opportunity to practice working with the material hands-on.
Participant Prerequisites

- For an effective and efficient learning experience, the participants need to have the following prerequisites:
  - Understanding of networking and routing
  - Working knowledge of the Microsoft Windows operating system

Syllabus

- Chapter 1: Introduction to Wireless LAN Technology
- Chapter 2: Standalone AP Operation Modes
- Chapter 3: Standalone AP Management
- Chapter 4: Introduction to Unified Wireless Solution
- Chapter 5: Unified Wireless Setup
D-Link Certifications

D-Link Certification

- D-Link Certified Professional (DCP)
  - Switching
  - Security
  - Wireless
  - IP Surveillance
  - Storage

- D-Link Certified Specialist (DCS) / D-Link Sales Specialist (DSS)
  - Switching
  - Security
  - Wireless
  - IP Surveillance
  - Storage

- D-Link Network Associate (DNA)

D-Link Icons – Switch & Router, Wireless, Security, People

- **Wireless**
  - Wireless Switch
  - Access Point
  - Wireless Controller
  - Radio Station
  - Radio Wave 1
  - Radio Wave 2
  - Radio Wave 3

- **Switch and Router**
  - Switch
  - Stackable Switch
  - Chassis Switch
  - Router

- **Security**
  - Firewall
  - VPN Server
  - Virus
  - Worm

- **People**
  - Male
  - Female
Course Introduction

D-Link Icons - Building, Storage, PC and Server, Misc.

Building
- Generic Building
- School

Storage
- Generic Storage
- IP NAS
- IP SAN (Rack)

PC and Server
- PC
- Laptop
- Workstation
- Server

IP Surveillance
- Network Video Recorder
- Network Camera
- Video Management Station

Misc.
- Cloud 1
- Cloud 2
- Cloud 3
- Phone
- Internet

Participant Introduction

- Your name
- Your company
- Your job responsibilities
- Your background
- What you’d like to get out of this course
Overview and Objectives

- Introduce Wireless LAN (WLAN) technology and identify the verticals for WLAN technology
- By the end of this chapter, you will have learned how to:
  - Describe WLAN in general, typical uses for WLAN technology and identify different vertical markets for WLAN solutions
  - Describe how users benefit from WLAN networks and discuss mobility
  - Describe typical WLAN deployment considerations and challenges
  - Describe D-Link WLAN product line
Wireless LAN Technology Overview

- Wireless Local Area Network (WLAN) definition
  - Network infrastructure where all data is transmitted and received using radio signals over the air instead of via network cables
- Advantages of implementing WLAN technology
  - Mobility
  - Simple network expansion
  - Scalability
- Differences between wired LAN and wireless LAN

<table>
<thead>
<tr>
<th>Wired LAN</th>
<th>Wireless LAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network cable installation required</td>
<td>Free of network cabling</td>
</tr>
<tr>
<td>Limited by network media</td>
<td>Not limited by network media</td>
</tr>
<tr>
<td>Depends on physical location</td>
<td>Independent of physical location</td>
</tr>
<tr>
<td>Data sent through network cable</td>
<td>Data sent over the air</td>
</tr>
</tbody>
</table>

History of Wireless LAN

- Following is the evolution of Wireless LAN:

  1970 – ALOHAnet developed at the University of Hawaii
  1985 – Federal Communications Commission (FCC) announces authorized license-free wireless bands
  1991 – First workshop held by IEEE; WLAN products launched, and IEEE starts developing a wireless standard
  1997 – FCC announces authorized wireless equipment that uses the license-free bands
Basic Components of a Wireless Network

- **Wireless client/station (STA)**
  - Wi-Fi phone, Smart phone or PDA...etc. with Wi-Fi built in.
  - Wireless adapter for client devices (used only for clients that do not support wireless)
    - Wireless USB Adapter
    - PCMCIA Adapter
    - Express Card and PCIe
- **Wireless device**
  - Access point
  - Wireless router
- **Antenna**

Benefits of WLAN Solutions

- Mobility
- Flexibility
- Scalability
- Ease of deployment
- Simple network management
Mobility
- Network resources can be accessed without being restricted to a single physical area

- Mobile client stays connected to the network while being able to move around

Flexibility
- WLANs can flexibly connect with LANs

1. Sends document to the network printer
2. AP receives the packet and forwards it to the switch
3. Switch receives the packet and forwards it to the network printer
4. Receives the packet, prints the document

Get documents from file server
Scalability

- Network expansion is scalable by adding more wireless devices

Ease of Deployment

- Customers are not limited to the physical area when deploying a wireless network infrastructure; for example, connecting different locations in the same building, or connecting two buildings via wireless infrastructure
- Less effort required – customers don’t need to handle as much cable installation
Simple Network Management

- Administrator or authorized user can simply manage the network infrastructure
- Easy to monitor tasks and control network traffic

Manage any wireless devices and control network traffic through client’s device

Summary

- When building a network infrastructure, some requirements from the customer that need to be fulfilled are quite common. Generally, the customer wants the network built to be deployed easily, to provide flexibility and scalability, and to be easy to manage and monitor.
- D-Link provides solutions for all these customer needs. D-Link wireless products provide many advantages for customers and are widely known as powerful devices.
WLAN Market Verticals

- Home/SOHO WLAN
- Corporate office WLAN
  - Voice over WLAN
  - Video over WLAN
- Education
  - Outdoor WLAN
- Healthcare
- Industry and manufacturing
  - Location tracking services
- Public WLAN services

Home/SOHO WLAN

- Most cost-effective solution
- Easy to install
- Simple to connect and use
- Provides all the major features
- Poor or no security
Voice and Video over WLAN

- Video or voice deployment requires careful planning
- Started with Skype and similar products
- Early stage of deployment
- HD video streams are bandwidth-hungry

Location Tracking Services

- Offers visibility over assets in your company
- Uses WLAN infrastructure
- RFID tags attached to assets/personnel
- Location tracking use cases:
  - Manufacturing
  - Retail
  - Pharmacy
  - Healthcare
  - Transport
Public WLAN Services

- Enables wireless access in parks, shopping centers, bars, hotels, etc.
- Also known as “hotspots”
- Open network
- Network designers can implement additional traffic filters
- Does not guarantee any bandwidth
- Can be combined with commercial services (full access, voice, video surveillance, etc.)
Standalone 802.11n Wireless Solution

- **DAP-2690**
  - 2.4/5 GHz 802.11a/b/g/n dual band concurrent
  - 3T3R 2.4GHz: 300Mbps 5 GHz: 300Mbps
  - 1 GbE ports
  - Metal desktop housing
  - 802.3af PoE support

- **DAP-2553**
  - 2.4/5 GHz 802.11a/b/g/n selectable dual band
  - 2T3R 300Mbps
  - AP/WDS/WDS with AP/wireless client modes
  - PoE support

- **DAP-3690**
  - 2.4 GHz 802.11b/g/n single band
  - 2T2R 2.4GHz: 300Mbps
  - 1 GE ports
  - Metal housing
  - 802.3af PoE support
  - IP67 certified

Standalone 802.11ac Wireless Solution

- **DAP-2695**
  - 2.4/5 GHz 802.11a/b/g/n/ac dual band concurrent
  - 3T3R 2.4GHz: 450Mbps 5 GHz: 1300Mbps
  - 2 GbE ports
  - Metal desktop housing
  - 802.3at PoE support

- **DAP-2660**
  - 2.4/5 GHz 802.11a/b/g/n/ac dual band concurrent
  - 2T2R 2.4GHz: 300Mbps 5 GHz: 900Mbps
  - 1 GbE ports
  - Plastic ceiling housing
  - 802.3af PoE support

- **DAP-3662**
  - 2.4/5 GHz 802.11a/b/g/n/ac dual band concurrent
  - 2T2R 2.4GHz: 300Mbps 5 GHz: 900Mbps
  - 2 GbE ports
  - Plastic housing
  - 802.3af PoE support
  - IP68 certified
Standalone AP Management - CWM

- Central Wi-Fi Manager (CWM) is a software solution for standalone AP centralised management
- Feature highlight
  - Managing up to 1K access points
  - Centralised management
    - Configuration update
    - Firmware upgrade
  - Centralised monitoring
  - Multiple languages support
  - Multi-tenancy
  - Bandwidth optimization
  - Customizable captive portal

Unified Wireless Solution: Controller and Switch

- Wireless Controller
  - DWC-1000
    - Support 6~24 APs per device
    - Support 24~96 APs per peer group
  - DWC-2000
    - Support 64~256 APs per device
    - Support 256~1024 APs per peer group

- Unified Switch
  - DWS-4026
    - Support 64 APs per device
    - Support 256 APs per peer group
  - DWS-3160
    - Support 12~48 APs per device
    - Support 48~192 APs per peer group
Unified Wireless Solution: Unified Access Point

- **DWL-8600AP**
  - 11n concurrent dual band
  - 2 x 2 antennas
  - 802.3af PoE

- **DWL-6600AP**
  - 11n concurrent dual band
  - Internal 2x2 PIFA antennas w/ external antenna connectors
  - 802.3af PoE

- **DWL-3600AP**
  - 11n 2.4GHz single band
  - Internal 2 x 2 antennas
  - 802.3af PoE

- **DWL-2600AP**
  - 11n 2.4GHz single band
  - Internal 2 x 2 antennas
  - 802.3af PoE

- **DWL-8610AP**
  - 11ac concurrent dual band
  - Internal 3 x 3 antennas
  - 802.3at PoE

- **DWL-6610AP**
  - 11ac concurrent dual band
  - Internal 3x2 antennas
  - 802.3at PoE

- **DWL-6700AP**
  - Outdoor
  - 11n concurrent dual band
  - 2 x 2 antennas
  - 5GHz 8dbi directional
  - 2.4GHz omni-directional
  - Non-standard PoE
  - IP55 rated

D-View 7 Wireless Management

- A unified management platform for D-Link Wireless Controller, Unified Switches, Unified APs and Standalone APs
- D-View 7 provides both unified and standalone wireless configuration and monitoring functions.
Summary

- WLANs are based on 802.11 standards; key feature is mobility
- Most common WLAN deployment is home/SOHO WLAN
- Enterprise WLAN focuses on more advanced users and features
- Public WLAN, also called Wi-Fi "hotspots," can be found in shopping malls, hotels, airports, other public places
- D-Link product family includes various types of access points and unified switches and a controller
- Access points can be Standalone APs (standalone, fat APs) or Unified APs (controller-based, thin APs).
Overview and Objectives

- Identify the Standalone AP operation modes
- Describe the WDS operation modes
- Explain Universal Repeater mode and identify typical use cases
- Describe the Wireless Client mode and typical use cases
- Explain the WISP operation modes and typical use cases

Different Modes For Different Situations:

- Access Point mode
- Wireless Distribution System (WDS) mode
- WDS with AP mode
- Universal Repeater mode
- Wireless Client mode
- Wireless Internet Service Provider (WISP) Client Router mode
- WISP Repeater mode
Access Point Mode

- AP acts as a central connection point for any WLAN devices
- Default operation mode
- Most common operation mode

Typical use cases
- Home
- SOHO
- Hotspots

Wireless Distribution System (WDS) Mode

- Wirelessly connects two separate LANs
- APs establish a wireless bridge
- WLAN clients cannot connect to AP in WDS mode

Typical use case
- Connecting another location at low cost
WDS Mode Application

- The branch office of a training center at site A wants to connect its network to the head office at site B across the street, at minimal cost.
WDS with AP mode

- Characteristics of WDS mode with AP
  - Same functionality as WDS mode, and allowing wireless client connection at the same time
  - Clients with a wireless adapter can wirelessly connect to the AP and then connect to another LAN

- Benefits of using WDS mode with AP
  - Easy deployment of the network extension
  - Less expensive – customers can connect to the remote network wirelessly at minimal cost
  - Flexibility – connect to any type of network (wired or wireless)

WDS with AP Mode Application

- A small company has expanded their office space by buying additional offices across the hall. They now wish to extend their wireless network to the new offices. However, they are not allowed to install additional cabling. They will use D-Link Standalone AP in WDS with AP mode to extend their network.
### WDS with AP Mode Application

- Change the Old Office AP to WDS with AP mode
- Install a new AP in the New Office
- Set the New Office AP to WDS with AP mode

![Diagram showing WDS with AP Mode Application](image)

### Universal Repeater Mode

- Repeats signal of the root AP
- Extends wireless coverage
- 50% signal-coverage overlap required
- Same WLAN settings must be used on repeater AP
- Can work with non-D-Link AP

**Typical use cases**

- Home
- SOHO

![Diagram showing Universal Repeater Mode](image)
Universal Repeater Mode Application

- Operation Mode: Universal Repeater

Standalone AP Operation Modes

- Operation Mode: Universal Repeater

Wireless Client Mode

- Enables wired device to communicate wirelessly
- Not visible as an AP to wireless clients

Typical use case:
- Connecting wired devices (printers, network cameras)
**WISP Client Router Mode**
- AP acts as a router connecting wired users to WISP
- Uses NAT to share Internet connectivity among clients
- Runs DHCP server for LAN clients
- Supported only on DAP-1160, DAP-1360 and DAP-3250

**WISP Repeater Mode**
- AP connects to WISP via wireless interface
- Provides Internet connectivity to wired and wireless users
- Uses NAT and DHCP
- Supported only on DAP-1160 and DAP-1360
Configuration Example

Summary

- Different operation modes fulfill different customer needs
- AP mode provides default basic mode of operation
- WDS mode establishes wireless bridge between APs
- Universal Repeater mode extends wireless coverage
- Wireless Client mode connects a wired device wirelessly
- WISP mode connects AP to WISP and shares Internet connectivity
LAB : Standalone AP in WDS with AP Mode

- In this activity, you will configure an Standalone AP for WDS with AP mode.

D-Link Certified Specialist

[Chapter 3: Standalone AP Management]
Overview and Objectives

- Identify the tools for Standalone AP Management
- Describe the use of AP Array and explain the mechanisms behind it
- Describe AP Manager II and explain how to install and control it

Available Tools for WLAN Management

- Standalone access points (APs) managed manually are inconvenient
  - Time-consuming
  - Error-prone
- D-Link wireless management solutions
  - Built-in functions:
    - AP Array
    - AP Clustering
  - Software solution: AP Manager II
  - Unified solution
    - Unified Switch
    - Wireless Controller
  - D-View Network Management System (NMS)
    - Wireless Control module (WCM) for wireless solutions
AP Array Basics

- Standalone AP configuration management solution
- Built into the AP
- Manages up to eight APs simultaneously

AP Array Features and Requirements

- Part of firmware
- Each array group contains up to eight APs
- Correct array name and password required to join an array group
- Each AP can be in only one array group
- Array group members must be in the same subnet
- All members of an array group must be the same AP model
AP Array Architecture Roles

- Master
- Backup Master
- Slave

AP Array Roles

- **Master AP** – each array group has only one Master AP, where configuration for the group is performed
- **Backup Master AP** - takes over the Master AP functions if the Master AP is not available
- **Slave AP** - syncs to settings from the Master AP
AP Array Configuration Synchronization

- Master AP syncs configuration with other array group members
- Certain settings are **not** synced
  - AP operation mode
  - Channel settings
  - LAN settings
- All other settings can be synced
- Administrator chooses which settings to sync

AP Array Protocol Details

- Works only through Ethernet interface
- UDP port 55000 used for broadcast communication
- Configuration revision number
  - If slave AP’s revision number differs, Master AP syncs configuration
  - Can be verified via CLI access with command `get arraycfg`
AP Array Configuration

- Enable AP Array and then select AP's array role
- Enter array group’s name and password
- Click **Scan** button to search existing array groups
- View details about current array members
- **Save** AP Array Settings

Troubleshooting AP Array Synchronization

- Check AP Array name and password
- Check connection status
- Check array role (via CLI)
- Capture Ethernet traffic and verify UDP packet transmission
**Verifying AP Array Log**

<table>
<thead>
<tr>
<th>Time</th>
<th>Priority</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uptime 0 day 20:38:13</td>
<td>[SYSACT]</td>
<td>Web login success from 192.168.0.101</td>
</tr>
<tr>
<td>Uptime 0 day 20:14:53</td>
<td>[SYSACT]</td>
<td>Web login success from 192.168.0.101</td>
</tr>
<tr>
<td>Uptime 0 day 20:04:47</td>
<td>[SYSACT]</td>
<td>Web login success from 192.168.0.101</td>
</tr>
<tr>
<td>Uptime 0 day 17:08:22</td>
<td>[Wireless]</td>
<td>Initiate Wireless success</td>
</tr>
<tr>
<td>Uptime 0 day 17:08:53</td>
<td>[SYSACT]</td>
<td>Do array receive config and update config</td>
</tr>
<tr>
<td>Uptime 0 day 16:58:42</td>
<td>[SYSACT]</td>
<td>Do array Connect to Master</td>
</tr>
<tr>
<td>Uptime 0 day 16:57:30</td>
<td>[SYSACT]</td>
<td>Do array/Master disconnect, Backup Master become Master(1)</td>
</tr>
<tr>
<td>Uptime 0 day 16:57:27</td>
<td>[SYSACT]</td>
<td>Do array/Master disconnect, Backup Master become Master(1)</td>
</tr>
<tr>
<td>Uptime 0 day 00:29:35</td>
<td>[Wireless]</td>
<td>Initiate Wireless success</td>
</tr>
<tr>
<td>Uptime 0 day 00:06:14</td>
<td>[SYSACT]</td>
<td>Do array receive config and update config</td>
</tr>
<tr>
<td>Uptime 0 day 00:06:06</td>
<td>[SYSACT]</td>
<td>Do array/Master disconnect, Backup Master become Master(1)</td>
</tr>
<tr>
<td>Uptime 0 day 00:06:06</td>
<td>[SYSACT]</td>
<td>Do array/Master disconnect, Backup Master become Master(1)</td>
</tr>
<tr>
<td>Uptime 0 day 00:00:19</td>
<td>[SYSACT]</td>
<td>Do array/Master disconnect, Backup Master become Master(1)</td>
</tr>
<tr>
<td>Uptime 0 day 00:00:03</td>
<td>[Misc]</td>
<td>Ethernet ETH LINK UP</td>
</tr>
<tr>
<td>Uptime 0 day 00:00:03</td>
<td>[Misc]</td>
<td>Ethernet ETH LINK UP</td>
</tr>
<tr>
<td>Uptime 0 day 00:01:31</td>
<td>[SYSACT]</td>
<td>Do array/Master disconnect, Backup Master become Master(1)</td>
</tr>
<tr>
<td>Uptime 0 day 00:00:19</td>
<td>[SYSACT]</td>
<td>Do array/Master disconnect, Backup Master become Master(1)</td>
</tr>
<tr>
<td>Uptime 0 day 00:00:02</td>
<td>[SYSACT]</td>
<td>Web login success from 192.168.0.101</td>
</tr>
</tbody>
</table>

**AP Array Case Study 1**

- Only one Master AP allowed in array group
- Second Master AP to join group ends in **unknown** status
AP Array Case Study 2

- If Master AP fails, Backup Master AP takes over Master AP role

AP Array Group
Array ID: D-Link
Password: *****

- Master AP
- Backup Master AP
- Slave APs

Verifying Status

Verifying Log

16:58:42 [SYSACT] [ap array] Connect to Master
16:58:36 [SYSACT] [ap array] Slave AP1 (slave) (slave, I backup)
16:57:37 [SYSACT] [ap array] Slave AP1 (slave) (slave, I backup)
16:56:37 [SYSACT] [ap array] Slave AP1 (slave) (slave, I backup)

AP Manager II Basics

- Software solution for Standalone AP centralized management
- For SMB environments
- Features
  - Centralized configuration
    - Configuration comparison
    - Firmware upgrades
  - Centralized monitoring
    - Log
    - Syslog
  - Built-in tools
    - Topology

Centralized configuration
Centralized monitoring
Built-in tools
AP Manager II Installation

- PC requirements
  - PostgreSQL database
  - PostgreSQL ODBC Driver
- AP requirements
  - SNMP must be enabled
- Additional requirements
  - AP Manager II modules
- Default login credentials
  - admin/admin

Discovering AP Devices

Click to access Advanced Discover Options:
Real-Time Reports

Access Point Report displays current list of discovered APs

Station Report is a graphical representation of associated WLAN stations

Model Report is a graphical representation of the discovered AP models

Band Report is a graphical representation of distribution of WLAN bands

Configuring Discovered APs
Upgrading APs

Topology Tool
Topology Tool: Custom Maps

- Enables us to illustrate signal strength and channel selection
- Optimizing radio settings
- Simplifies future planning

When one of the APs experienced failure, the change is reflected on the map.

Topology Tool: Details

Device can be precisely positioned on the topology map manually.
Configuration Template

Configuration template is a group of settings that you can schedule to push to multiple APs:

- Configuration consistency
- Time savings

Task Scheduling

1. Step: Select devices you want to configure
2. Step: Select the configuration template
3. Step: Schedule the upgrade
AP Array vs. AP Manager II

<table>
<thead>
<tr>
<th>Product</th>
<th>When to Use</th>
<th>Selling Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Array</td>
<td>• Small office level</td>
<td>• Free</td>
</tr>
<tr>
<td></td>
<td>• Manage up to 8 APs</td>
<td>• Integrated in firmware</td>
</tr>
<tr>
<td></td>
<td>• Same AP model in group</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No additional PC</td>
<td></td>
</tr>
<tr>
<td>AP Manager II</td>
<td>• SMB level</td>
<td>• Free</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Bundled with AP</td>
</tr>
</tbody>
</table>

Summary

- The AP Array and AP Management II are wireless management solutions for D-Link Standalone access points.
- AP Array is a built-in centralized management solution
  - Manages up to eight APs of the same type
- AP Manager II is a software solution for centralized management
  - Requires PostgreSQL database, supports different AP types
  - Centralizes configuration, monitoring and firmware upgrades
  - Included topology tool graphically visualizes network layouts
LAB : AP Array and AP Manager II

- In this activity, you will install AP Manager II and use it to configure your Standalone AP. You will also configure the AP array between your Standalone APs.
Overview and Objectives

- Describe the concepts behind the D-Link Unified Wireless Solution
- Describe the basic components of a Unified Wireless Solution
- Compare Standalone and Unified AP
- Identify Unified AP models
- Describe WLAN architecture using a Wireless Controller
- Describe WLAN architecture using a Unified Switch

Legacy WLAN Challenges

- Setting up standalone APs in mid-to-large business
- Firmware updates
- Signal and channel monitoring
- Consistent policies for APs and stations
- Roaming interruptions
D-Link Unified Wireless Solution

- Unified APs and Unified Switch and/or Wireless Controller
- Unified **wired and wireless** access systems
  - Better WLAN performance
  - Seamless roaming
- Unified **management** and **security**
  - Centralized AP and client management
  - Rogue AP detection/mitigation

D-Link Unified Switch

- Switch manages up to 64 APs*
- Switch cluster manages up to 256 APs*
- Switching and routing for traffic on LAN
- Keeps consistent configurations of APs in the network
- Monitoring AP settings
- Discovery, validation, and authentication of APs and peer Unified Switches

* DWS-4026; refer to the next slide for DWS-3160 capacity
D-Link Unified Switch Models

<table>
<thead>
<tr>
<th>Switch</th>
<th>DWS-3160</th>
<th>DWS-4026</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>20 10/100/1000Base-T ports Unified Switch with 4 Combo 1000Base-T/SFP ports (PoE and non-PoE model)</td>
<td>24-Port Gigabit L3 PoE Unified Switch with two (2) 10GE Open Slots</td>
</tr>
<tr>
<td>Access Point</td>
<td>DWL-2600AP/3600AP/6600AP/8600AP/8610AP</td>
<td></td>
</tr>
<tr>
<td>Number of APs</td>
<td>Up to 48</td>
<td>Up to 64</td>
</tr>
<tr>
<td>Number of APs per cluster</td>
<td>Up to 192</td>
<td>Up to 256</td>
</tr>
</tbody>
</table>

Wireless Controller

- 1 Controller manages up to 256 APs*
- Controller cluster manages up to 1024 APs*
- Keeps consistent configurations of APs in the network
- Monitoring AP settings
- Discovery, validation, and authentication of APs and peer controllers
- Configuration via GUI; CLI mainly for troubleshooting

* DWC-2000; refer to the next slide for DWC-1000 capacity
D-Link Wireless Controller Models

<table>
<thead>
<tr>
<th>Controller</th>
<th>DWC-1000</th>
<th>DWC-2000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>4 LAN + 2 Option 10/100/1000 Based-T</td>
<td>4 10/100/1000 Base-T 4 Combo 100/1000 Base-T/SFP</td>
</tr>
<tr>
<td>Access Point</td>
<td>DWL-2600AP/3600AP/6600AP/6610AP/8600AP/8610AP</td>
<td></td>
</tr>
<tr>
<td>Number of APs</td>
<td>Up to 24</td>
<td>Up to 256</td>
</tr>
<tr>
<td>Number of APs per cluster</td>
<td>Up to 96</td>
<td>Up to 1024</td>
</tr>
</tbody>
</table>

D-Link Access Point

- **Standalone mode**
  - Managed by connecting to it (GUI/CLI)
  - Useful for small networks

- **Managed mode**
  - Part of Unified Wireless Solution
  - Managed by D-Link Unified Switch/Wireless Controller
  - Upgrades and configuration profiles pushed via switch
  - Useful for any network size
Unified AP Models – Indoor 802.11n AP

<table>
<thead>
<tr>
<th>DWL-2600AP</th>
<th>DWL-3600AP</th>
<th>DWL-6600AP</th>
<th>DWL-8600AP</th>
</tr>
</thead>
</table>
| • 802.11b/g/n  
  • 2.4GHz radio  
  • 10/100 Mbps LAN interface  
  • PoE support  
  • Integrated antenna with 2X2 MIMO  
  • Up to 16 Virtual APs (VAP) per radio | • 802.11b/g/n  
  • 2.4GHz radio  
  • 10/100 Mbps LAN interface  
  • Up to 300Mbps  
  • PoE support  
  • Integrated antennas with 2X2 MIMO  
  • Up to 16 Virtual APs (VAP) per radio | • 802.11a/b/g/n  
  • 2.4GHz and 5GHz radios  
  • Up to 300Mbps  
  • PoE support  
  • Integrated antennas with 2X2 MIMO  
  • Optional external antennas  
  • Up to 16 Virtual APs (VAP) per radio | • 802.11a/b/g/n  
  • 2.4GHz and 5GHz radios  
  • Up to 300Mbps  
  • PoE support  
  • Four high gain antennas, two for 2.4GHz, two for 5GHz  
  • 2X2 MIMO on dual band  
  • Up to 16 Virtual APs (VAP) per radio, 32 per APs |

Unified AP Models

Indoor 802.11ac  
Outdoor 802.11n

<table>
<thead>
<tr>
<th>DWL-6610AP</th>
<th>DWL-8810AP</th>
<th>DWL-6700AP</th>
</tr>
</thead>
</table>
| • 802.11a/b/g/n/ac  
  • Concurrent 2.4 GHz and 5 GHz radios  
  • Up to 900 Mbps  
  • 802.3af PoE support  
  • Integrated antennas with 2X2 MIMO  
  • Up to 16 Virtual APs (VAP) per radio, 32 per APs | • 802.11a/b/g/n/ac  
  • Concurrent 2.4 GHz and 5 GHz radios  
  • Up to 1300Mbps  
  • 802.3at PoE support  
  • Integrated antennas, with 3X3 MIMO  
  • Up to 16 Virtual APs (VAP) per radio, 32 per APs | • 802.11a/b/g/n  
  • Concurrent 2.4 GHz and 5 GHz radios  
  • Up to 600 Mbps  
  • Proprietary PoE  
  • 2 x 2 antennas  
  • 5GHz 8dBi directional  
  • 2.4GHz omni-directional  
  • IP55 rated |
Unified Wireless Solution Implementation

- Customer networks and requirements are very different
- Customer may not want to replace existing switches
- D-Link Unified Wireless Solution provides high level of flexibility
- Two possible solutions
  - Deploy Unified Switch as addition to the existing network infrastructure
  - Replace the existing edge switches with Unified Switches
- Both solution types are commonly used in large environments

Overlay Solution

Wireless switch installed into the existing network infrastructure

- Benefits of WLAN switching
- Protect current investment in network infrastructure
- Unified Switch works as Wireless Controller only
**Unified Solution**

Wireless switches deployed at network edge
- Replace existing L2 edge switches
- Full utilization of D-Link Unified wireless solution
- Unified Switch works as both L2 edge switch and Wireless Controller

Typical Scenario
- Typical deployment topology is a combination of Overlay and Unified deployments
- APs have L3 connectivity to Unified Switch
Deployment Using Wireless Controller

- Single Site deployment

- Multiple Sites deployment

Single Point of Configuration

- Unified Switch or Controller manages APs
  - Configuration profile is applied to an AP
  - Unified Switch or controller automatically detects attached APs
  - When AP is replaced, Unified Switch and Controller automatically configures new AP with profile of replaced unit

- Configuration profile features
  - RADIUS server settings
  - MAC authentication list
  - RF interface and configuration
  - QoS configuration
  - VAP configuration
Dynamic Power Adjustment

- RF power level
  - If it is too low, WLAN clients cannot connect
  - If it is too high, it might cause interference with other APs
- Dynamic power adjustment corrects RF power level

Self-Healing Network: Fail Safe

- Power level adjusted by sensing status of nearby APs
- When an AP fails, the switch or controller increases power of neighboring APs
- Benefits
  - Less interference
  - Smaller blind spots in case of AP failure
Load Utilization

- Unified Switch performs load utilization by individual AP
- APs report bandwidth utilization to the Unified Switch regularly
- If threshold is breached, new client associations are rejected
  - New client connects to a neighboring AP

Dynamic Channel Assignment

Unified Switch automatically adjusts channels in certain cases

- New AP added
- AP removed
- Predefined time for channel adjustment (e.g., 2 AM every day)
Fast Roaming

- Mobile stations maintain IP connectivity while roaming between APs
  - Enables VoIP deployment on 802.11 network
- Unified Switch/Wireless Controller needed for roaming
  - Multiple Unified Switches can be used in a solution
- No need for re-authentication or IP reallocation
  - Key caching
  - Pre-authentication
- Fast roaming variations
  - Within subnet (L2)
  - Across subnet (L3)

Summary

- D-Link Unified Wireless Solution offers centralized management
  - Unified Switch or Wireless Controller and Unified APs
  - D-Link DWC-1000 Wireless Controller is a solution for small to medium-sized business
- Overlay solution keeps current network infrastructure
- Unified solution replaces existing L2 edge switches
- Two D-Link Access Point modes
  - Standalone AP configurations are made one device at a time
  - Managed AP managed by Unified Switch/Wireless Controller
- Unified Wireless Solution features
  - Dynamic power adjustment (self-healing network)
  - Dynamic channel assignment
  - Fast roaming
LAB : Unified Switch Setup

- In this activity, you will configure D-Link Unified Switch and will use it to manage the Unified access points.

D-Link Certified Specialist

[Chapter 5: Unified Wireless Usage]
Overview and Objectives

Explore graphical user interfaces (GUIs) of D-Link Unified Switch and D-Link Wireless Controller:
- Basic configuration
- AP profiles
- AP discovery and validation

Unified Wireless Basic Case Study

- Company implementing Unified Wireless Solution wants to replace existing switch with Unified Switch and connect Unified Access Points directly to Unified Switch
- You will deploy Unified Wireless Solution and establish basic wireless connectivity
- Implementation consists of three tasks
  1. Configure basic connectivity between Unified Switch and Unified APs
  2. Discover and validate all Unified APs
  3. Configure and deploy a basic WLAN
An Example of Unified Wireless Topology

Unified Wireless Usage

• Introduction to Unified Wireless Configuration

Unified Access Point User Interface

• Two interface types
  • WEB GUI
  • CLI
• In managed mode, WEB GUI and CLI disabled
• DHCP client enabled by default
• Default IP: 10.90.90.91
• Default username/password: "admin"/"admin"
Unified Switch User Interface

- Three interface types
  - WEB GUI
  - CLI (Telnet or console port)
- Default IP: **10.90.90.90**
- Default username/password: “admin”/[blank]

- Baud rate: 115200 bps
- Data bits: 8
- Parity: none
- Stop bit: 1
- Flow control: none

Configuring Basic DHCP Connectivity

Choose Unallocated, Dynamic or Manual

Displayed if dynamic binding is selected

Set either Network Mask or Prefix Length to specify subnet mask

DWS-4026 ONLY
Configuring Basic WLAN Connectivity

- Configuring the Unified Switch

Unified Wireless Usage

WLAN functionality is Enabled by default

AP validation can be Local or RADIUS

Enabled, Enable-Pending, Disabled or Disable-Pending (if status is pending, refresh GUI)

Correct country code should be selected for equipment to comply with local regulations

Enabling the VLAN list definitions for Layer 2 discovery

Enabling the IP list definitions for Layer 3 discovery
AP Discovery and Validation

- **L2 discovery** - switch/controller discovers AP
- **L3 discovery** - switch/controller discovers AP or vice versa
- **DHCP option 43** - automated discovery
  - AP must be managed by switch/controller
  - Prerequisite: valid MAC in the switch’s database
  - Database can be local or on a RADIUS server

UDP Discovery Message

AP Validation

- Adding MAC address of the AP manually
- List of APs with their statuses and applied profiles
- After AP is fully managed, check its status under **Managed AP Status**
By default, radio 1 operates in 802.11a/n mode and radio 2 operates in 802.11b/g/n mode.

If enabled, you can control the amount of allowed traffic once specified level is breached, new client associations will not be accepted.

Automatic Power algorithm chooses best-suited power level of the RF radio.

Multiple SSIDs can be defined for each AP profile.
Applying an AP Profile to the Access Point

- Configuring the Unified Switch

After managing valid APs, you can push the profiles. After clicking Apply, you can reset the AP to apply the new AP profile. By resetting APs, you also apply the reconfigured APs’ profiles. Configurations can be applied via the AP profile’s Advanced Configuration.

Wireless Controller User Interface

- Default IP address: 192.168.10.1/24
- Default credentials: “admin”/“admin”
Configuring Basic DHCP Connectivity

- Configuring the Wireless Controller

Unified Wireless Usage

- Configuring the Wireless Controller

Configuring Basic WLAN Connectivity

- Configuring the Wireless Controller

Unified Wireless Usage

- Configuring the Wireless Controller
Creating an AP Profile

- Configure radio settings for the selected AP profiles
- Configure SSID settings for the selected AP profiles
- List of existing AP profiles
- Add a new AP profile with this option
- Apply a profile to access point(s)

AP Discovery

- Enable Layer 3 discovery
- Enable Layer 2 discovery
- Add IP addresses for the wireless controller to search
AP Validation

Unified Wireless Usage
Configuring the Wireless Controller

AP Profile Radio Settings

Unified Wireless Usage
Configuring the Wireless Controller
AP Profile SSID Settings

Unified Wireless Usage

• Configuring the Wireless Controller

AP Profile whose SSID settings you’re managing

Multiple SSIDs can be set up for an AP; dlink1 is set by default

Summary

- Always save configuration after making changes
- Unified Wireless devices have three types of configuration interfaces: WEB GUI, CLI, SNMP
- Unified Access Point profiles apply SSID settings and 802.11 radio configuration to APs
- AP discovery mechanisms: L2 discovery, L3 discovery, DHCP option 43
- AP validation can be done locally or via RADIUS server
LAB : Wireless Controller Setup

- In this activity, you will configure D-Link Wireless Controller and will use it to manage the Unified access point.