Scalable Unified Wired/Wireless Network Architecture

- 20 10/100/1000BASE-T Gigabit Ports
- Up to 48 Wireless AP Direct/Indirect Connections
- Mixed Wired/Wireless Connection From Any Port
- 4 Combo SFP for Flexible Fibre Connection
- Expandable to 4 Peer Switches

Simplified & Resilient Network Deployment

- 802.3af Power Over Ethernet Simplifies AP Installation
- Gigabit Connection Ready for 802.11n AP Deployment
- Redundant Power Supply Support Maximises Network Uptime

Security Management

- 64/128/152-Bit WEP Data Encryption
- WPA/WPA2 Personal
- WPA/WPA2 Enterprise
- MAC Authentication
- Rogue AP Classification & Detection
- Wireless Threat Mitigation
- Captive Portal Authentication

Centralised Wireless Network Managemement

- Tracks & Maintains User Authentication As Users Roam Throughout the Network
- Intelligently Designates Users to Virtual Groups Based on User's Authenticated Identity
- Provides Scaled, Resilient, Integrated Management Infrastructure
- Centrally Manages User Authentication/ Security Policies
- Provides Key Management for Each Security Protocol
- Configures and Controls All Connected Access Points

L2+ Unified Wired/Wireless Gigabit Switches

D-Link's DWS-3024/3024L L2+ Unified Wired/ Wireless Gigabit Switches are optimised for wireless network deployment in business environments. With these devices, businesses can create a high-performance, secure, manageable and scalable unified wired/wireless LAN switching infrastructure. Equipped with a combo SFP, Power over Ethernet (PoE), and redundant power supply (RPS) support, these switches provide enterprises with an easy upgrade to next-generation 802.11n wireless LAN, simple deployment of wireless devices regardless of physical locations, and centralised management/policy enforcement of wireless mobility.

Core Units Controlling Entire Wireless Network

The DWS-3024/3024L switches are the core units that consolidate the security, manage the bandwidth, and maintain the integrity of an entire wireless network. In addition to monitoring users' identities and maintaining their authentication as they roam, these switches can configure and control all aspects of the wireless access points, including their RF channel/power management, wireless traffic segmentation, AP roaming/AP load balancing, rogue AP detection, and AP access security.

Designed for Easy Deployment of High-Performance Wireless LAN

Designed for distributed deployments in the wiring closet, each switch can support up to 24 or 48 wireless access points. AP connections can be made directly to the wireless AP switch ports, or indirectly through any LAN switch. With 802.3af PoE integrated into every port, the switch allows for the placement of APs in areas with limited access to AC power sources. Gigabit transmission ensures future compatibility and hardware protects investments when the network is installed with next-generation higher-speed 802.11n wireless standard devices.

20 Gigabit Ports, No Restriction on Port Usage

Each switch has 20 10/100/1000BASE-T Gigabit ports and 4 combo SFP slots. Each of the 10/100/1000BASE-T ports can be connected to a wireless access point, or to a wired LAN device such as a server, a network storage device, or another LAN switch. The combo SFP allows for flexible fibre connection.

Scalable Expansion & Unified Wired/Wireless Deployment

Small to Medium Enterprises (SME) may begin with only one switch to manage their AP or to use for mixed wired/wireless LAN purposes. When the number of APs is augmented, up to 4 switches can be combined to form a large mobility domain. The switch's many features such as easy expansion, Gigabit speed to support next-generation high-speed APs, and packet routing to support enterprise-wide inter-subnet roaming, lets it provides an architecture that unifies and simplifies an otherwise complex WLAN environment, and readily prepares an existing network for future upgrades.

RF & Power Management

To minimise the need for intervention from IT personnel, the switch provides automatic selection of unoccupied or least-used Radio Frequency (RF) channels for each wireless access point to avoid interference with other AP and RF devices. For each AP, it also sets a transmitter output power strong enough for RF signals to reach wireless clients, yet weak enough to minimise interference with other wireless devices' RF signals. The switch auto-adjusts the RF channels and transmitter output power of all wireless access points every time an AP is added to or removed from the network. This automatic adjustment can be programmed to take effect at a certain time or at specific intervals, minimising the need for network administrators to manually intervene.

Bandwidth & Power Management

- Auto-Adjusts RF Channels for AP
- Provides Fast Intra-Switch Roaming
- Advanced Inter-Subnet Roaming
- Auto-Adjusts Transmit Output Power for AP

LAN Management

- L2+ Features: Spanning Tree, 802.3ad Link Aggregation, Port Mirroring, Jumbo Frames, RIP, Voice VLANs
- IPv4 Packet Routing
- QoS with 802.1p Priority Queues, Granular Bandwidth Control
- LAN Security with ACL, RADIUS, TACACS+ Authentication, DoS Prevention, Broadcast Storm Control

Secure & Versatile Management

- Web Access Using HTTP
- Telnet Server/Client
- SSH v2, SSL v3
- SNMP v1, v2c, v3, RMON
- SYSLOG, Dual Image

L2+ Unified Wired/Wireless Gigabit Switches

Self-Healing and Load Balancing

The "self healing" process and AP load balancing functions increase the resiliency of a wireless network. To make up for a sudden RF signal vacuum created by any "dead" AP (AP with DC power failure, for example), the switch automatically increases the transmitter output power of all neighboring APs to expand their RF coverage, thereby "healing" the network "wound." To ensure a continuous connection for current clients, the switch performs load balancing across access points when network traffic reaches a certain threshold, while rejecting new client-to-AP associations to avoid bandwidth overcrowding.

Simplified Configuration & Deployment

The process of network maintenance and configuration have been made more efficient through the implementation of a centralised management platform. By running an Internet browser on any PC connected to the network and typing in the IP address of a managed switch, administrators can view the topology map and pinpoint the locations of the AP and the switch itself. The map uses AP icons which administrators can click on to select, and which show different colors to differentiate the different RF channels used by the AP. For quick replacement of a failed AP, administrators can easily locate the AP on the map, swap it with a new one, and apply the same configuration profile to the new unit.

Maximised Wireless Connection

The DWS-3024/3024L switches can effectively manage the wireless bandwidth to optimise WLAN traffic using centralised RF policies, auto-selection of the least utilised channels, and AP load balancing. The switch maintains a centralised database of wireless users' access information such as their MAC addresses and authentication keys. On a network site deployed with multiple peer switches, this information is also shared among the switches themselves. As wireless users roam around the office using wireless equipment, they may change their connection from AP to AP. By constantly monitoring the APs' status, the switch can establish an AP-to-AP roaming for these users without re-establishing authentication keys. This fast roaming process results in disruption-free, reliable wireless connectivity crucial for mobile applications such as Wi-Fi IP phone and wireless PDA connection.

Adaptable Wireless

Most of the current wireless LAN controllers' architecture requires wireless traffic to return to the controller for centralised processing, causing unnecessary traffic delay. The DWS-3024/3024L switches offer administrators additional options. Depending on the wireless application, wireless traffic can either be tunneled back to the switch for better security control, or locally forwarded at the access point for optimal performance. This device offers administrators maximised flexibility with options to tunnel guest traffic to the switch for centralised security control, or forward VoIP traffic directly from the access point for optimal performance.

Maximised Network Security

Each client connecting to the wireless network goes through a strict authentication process to ensure maximum security. Whether the client is an assigned user, a visiting guest, or a client with only departmental access, the switch protects the entire network infrastructure with numerous security mechanisms. These mechanisms include WEP data encryption, 802.1X user authentication, 802.11i standard WPA/WPA2 security, Captive Portal, and MAC Authentication. The switches provide a means to define and detect rogue APs to prevent illegal intrusion into the internal network. It provides user-based services such as virtual private group (SSID) membership, encryption type, authentication, and associated network statistics. Authorisations stay with users wherever they roam because all deployed DWS-3024/3024L switches share stored information, ensuring secure access and connectivity to the right services. In addition to checking the identity of a connecting user from the switch's local database, user authentication policies can be sent to an external RADIUS server for complete verification. This offloading capability ensures that the switch will not be overloaded when numerous clients simultaneously connect to the network.

Maximised Flexibility

In addition to acting as the controller unit in a wireless switching system, the DWS-3024/3024L switches can also function as advanced L2+ wired switches. Complete with packet routing, ACL security features, multi-layer QoS, 802.1q VLAN traffic segmentation, IGMP snooping for IP multicast streams, 802.3ad redundant load-sharing Gigabit links, the switches allow businesses to totally integrate their enterprise wireless networks with their wired network infrastructure. Businesses contemplating upgrading their current 10/100Mbps desktop connections to Gigabit capability can deploy the DWS-3024/3024L to take advantage of their ability to flexibly act as a wireless controller, a dedicated, full-featured multi-layer LAN switch or as a dual-role device.

Technical Specifications		DWS-3024L	DWS-3024
			
Hardware Interfaces	Size	19-inch Standard Rack-Mount Width, 1U Height	
	Interfaces	20 10/100/1000BASE-T 4 Combo 10/100/1000BASE-T/SFP	
	Console Port	RS-232 Console Port	
Performance	Switching Fabric	48 Gbps	
	Packet Forwarding Rate	35.7 Mpps	
	MAC Address Table Size	8 K	
	Packet Buffer	750 KB	
	Static Routing Table Size	128	
	Jumbo Frame Size	9.216 Bytes	
Physical	MTBF	174.272 hours	
	Acoustic	< 52.4 dB	
	Heat Dissipation	1664.08 BTU/hr	
	Dimensions	441 x 389 x 44 mm (17.32 x 15.31 x 1.73 inches))	
	Weight (without optional module)	5.42 kg	
	Ventilation	2 DC Fans (40 x 40 mm)	
	Operating Temperature	0 to 40°C (32 to 104°F)	
	Storage Temperature	-10 to 70°C (14 to 158°F)	
	Operating Humidity	10% to 90% RH	
	Storage Humidity	5% to 90% RH	
Power	Input	100 to 240 VAC, 50 to 60 Hz Internal Universal Power Supply	
	Consumption	488 watts	
Certifications	EMI/EMC	C-Tick, CE, EN60601-1-2, FCC Class A, ICES-003, VCCI	
	Safety	CB, UL/cUL	

L2+ Unified Wired/Wireless Gigabit Switches

Software Features

WLAN Management Capability
- DWS-3024L: Up to 24 APs (Directly or indirectly connected through LAN switch)
- DWS-3024: Up to 48 APs (Directly or indirectly connected through LAN switch)
- Up to 2,048 Wireless Users (1,024 Tunneled Users or 2,048 Non-Tunneled Users)

Roaming
- Fast Roaming
- Intra-Switch/Inter-Switch Roaming
- Intra-Subnet/Inter-Subnet Roaming

Access Control & Bandwidth Management
- Up to 32 SSID per AP (16 SSID per RF Frequency Band)
- AP Load Balancing based on the number of users or utilisation per AP

Managed AP
- DWL-3500AP
- DWL-8500AP
- DWL-8600AP

AP Management
- AP Auto-Discovery
- Remote AP Reboot
- AP Monitoring: List Managed AP, Rogue AP, Authentication Failed AP
- Client Monitoring: List Clients associated with each Managed AP
- Ad-hoc Clients Monitoring
- AP Authentication Supporting Local Database and External RADIUS Server
- Centralised RF/Security Policy Management
- Automatic AP RF Channel Adjustment
- Automatic AP Transmit Output Power Adjustment

WLAN Security
- WPA Personal/Enterprise
- WPA2 Personal/Enterprise
- 64/128/152-bit WEP Data Encryption
- Wireless Station and AP Monitoring on RF Channel, MAC Address, SSID, Time
- Rogue and Valid AP Classification based on MAC Address
- Encryption Type Support: WEP, WPA, Dynamic WEP, TKIP, AES-CCMP, EAP-FAST, EAP-TLS, EAP-TTLS, EAP-MD5, PEAP-GTC, PEAP-MS-CHAP v2, PEAP-TLS
- Captive Portal
- MAC Authentication
- Station Isolation
- Rogue AP Mitigation

L2 Features
- MAC Address Table Size: 8K entries
- IGMP Snooping: 1K Multicast Groups
- Spanning Tree:
  - 802.1D Spanning Tree
  - 802.1w Rapid Spanning Tree
  - 802.1s Multiple Spanning Tree
- 802.3ad Link Aggregation:
  - Up to 32 Groups
  - Up to 8 Ports per Group
- 802.1ab LLDP
- Port Mirroring:
  - One-to-One Port Mirroring
  - Many to One Port Mirroring
- Jumbo Frame Size: Up to 9 KB

VLAN
- 802.1Q VLAN Tagging
- VLAN Groups: Up to 3965
- 802.1V Subnet-based VLAN
- MAC-based VLAN
- GVRP
- Double VLAN
- Voice VLAN

L3 Features
- IPv4 Static Route
- Routing Table Size: Up to 128 Static Routes
- Floating Static Route
- VRRP
- Proxy ARP
- RIP v1/v2

Quality of Service
- 802.1p Priority Queues (Up to 8 Queues per Port)
- CoS Based on: Switch Port, VLAN, DSCP, TCP/UDP Port, TOS, Destination/Source MAC Address, Destination/Source IP Address
- Minimum Bandwidth Guarantee per Queue
- Traffic Shaping per Port
- WMM (WiFi Multimedia)

ACL (Access Control List)
- ACL Based on: Switch Port, MAC Address, 802.1p Priority Queues, VLAN, Ethertype, DSCP, IP Address, Protocol Type, TCP/UDP Port

LAN Security
- RADIUS Authentication for Management Access
- TACACS
- Authentication for Management Access
- SSH v1, v2
- SSL v3 , TLS v1
- Port Security:
  - 20 MAC Addresses per Port
  - Trap Violation Notification
- MAC Filtering
- 802.1X Port-Based Access Control and Guest VLAN
- Denial of Service Protection
- Broadcast Storm Control in Granularity of 1% of Link Speed
- Protected Port
- DHCP Filtering

Management Methods
- Web-Based GUI
- CLI
- Telnet Server: Up to 5 Sessions
- Telnet Client
- TFTP Client
- SNMP v1, v2c, v3
- Multiple Configuration Files
- RMON v1: 4 Groups (Statistics, History, Alarms, Events)
- BOOTP/DHCP Client
- DHCP Server
- SNTP
- SYSLOG
- Dual Images

ACN 052 202 838