D-Link®
Building Networks for People

Produktmerkmale

Sicherheit
Höhere Sicherheit mit Captive Portal-Funktion und RADIUS-Unterstützung

Zentrales Management
Konfiguration und Management von Access Points an einem Ort

Skalierbarkeit
Erweiterbar auf Steuerung von bis zu 24 Access Points pro Controller

Gastmanagement
Ermöglicht die Bereitstellung eines drahtlosen Internet-Gastzugangs mit Verwaltungsfunktionen für Konten, Nutzung und Zugriff

DWC-1000
Wireless Controller

Leistungsmerkmale

Netzwerkarchitektur
- Verwaltung von bis zu 6 Wireless Access Points (APs), erweiterbar auf bis zu 24 Access Points (APs)1 pro Controller
- Steuerung von bis zu 24 WLAN-APs, maximal 96 Access Points (APs)1 pro Cluster

Robuste Netzwerksicherheit
- Wireless Instruction Detection System (WIDS)
- Erkennung und Klassifizierung unautorisierter Access Points (Rogue APs)
- Captive Portal
- Gastmanagement
- WEP, WPA Personal/Enterprise, WPA2 Personal/Enterprise
- 802.1x
- Firewall-Richtlinie[2]
- IPSec/PPTP/L2TP/SSL-VPN[2]
- Filterung von Webinhalten[2]

Sicherheit
- WPA/WPA2 Personal
- WPA/WPA2 Enterprise
- 802.1X-Benutzerauthentifizierung
- Filterung von MAC-Adressen
- Erweiterte Sicherheitsfunktionen wie Erkennung unautorisierter
- APs (Rogue APs) und Intrusion Protection[2]

Ausfallsicherheit
- Failover für Datenverkehr an Option-Anschlüssen[2]
- Outbound Load Balancing[2]

Freigabe
- USB-Anschluss für Datei- und Druckerfreigabe

Kompatible Wireless Access Points von D-Link
- DWL-8600AP (802.11n/g/b/a)
- DWL-6600AP (802.11n/g/b/a)
- DWL-3600AP (802.11n/g/b)
- DWL-2600AP (802.11n/g/b)

[1] Die Anzahl verwalteter APs kann durch den Erwerb von Lizenz-Upgrades erweitert werden.
[2] Funktionen werden durch den Erwerb des VPN/Router/Firewall-Lizenz-Upgrades aktiviert.
[3] Der erste Option-Port ist standardmäßig aktiviert. Der zweite Option-Port wird durch den Erwerb des VPN/Router/Firewall-Lizenz-Upgrades aktiviert.

Der Wireless Controller DWC-1000 von D-Link ist ein zentrales WLAN-Managementsystem, das speziell für Campus-Gelände, Zweigstellen und Unternehmen entwickelt wurde, die eine leicht zu bedienende und skalierbare Lösung für das Management und die Konfiguration ihres drahtlosen Netzwerks benötigen. Der DWC-1000 ist auch die ideale Lösung für Unternehmen, die an öffentlichen Orten drahtlosen Internetzugang für Gäste bereitstellen möchten. Mit seiner Fähigkeit zur Verwaltung von bis zu sechs Wireless Access Points (erweiterbar auf 24) und einem Maximum von 96 Wireless Access Points in einem Controller-Cluster stellt der DWC-1000 eine kostengünstige Mobilitätslösung für kleine und mittlere Umgebungen dar. Dank automatischer AP-Erkennung und Verwaltung an einem zentralen Ort erhalten Kunden ein System der Enterprise-Klasse, ohne sich mit umfangreichen und komplexen Konfigurationen belasten zu müssen. Mit seinem robusten und umfassenden Sicherheitserkennungssystem ist der DWC-1000 in der Lage, potenzielle Angriffe durch unautorisierte Nutzer und Geräte an den verwalteten APs zu blockieren, insbesondere in Wireless-Umgebungen. Mit der Gastmanagement-Funktion können Konten erstellt, die Nutzung kontrolliert und die Zugriffssicherheit verwaltet werden. Damit können Unternehmen einen leicht einzurichtenden, aber dennoch sicheren drahtlosen Internetzugang an öffentlichen Orten wie Hotels, Kaffeebars und Flughäfen bereitstellen.

Robustes und optimiertes Netzwerk

Der DWC-1000 ist mit Funktionen zur Selbstorganisation, Selbstoptimierung und Selbstheilung des Netzwerks ausgestattet, um die Stabilität des gesamten drahtlosen Netzwerks zu verbessern. Der DWC-1000 führt regelmäßig Funkscans und Performanceanalysen durch und passt Funkkanäle und Sendeleistung automatisch an, um Störungen zu vermeiden den optimalen Zustand des drahtlosen Netzwerks aufrechtzuerhalten. So verstärkt der DWC-1000 bei einem plötzlichen Funkfrequenz-Signalverlust durch einen fehlerhaften Access Point die Sendeleistung benachbarter Access Points, um die sichere Funkabdeckung zu gewährleisten.

Umfassende Sicherheit

Der DWC-1000 stellt eine umfassende drahtlose Sicherheitslösung für jedes Netzwerk dar. Auf WLAN-Seite verfügt der DWC-1000 über ein Wireless Instruction Detection Systems (WIDS), mit dem er unautorisierte Access Points (Rogue APs) und Clients erkennt und drahtlose Angriffe im Voraus erkennt, sodass potenzielle Schäden und illegale Zugriffe zuverlässig verhindert werden. Neben grundlegenden drahtlosen Sicherheitsfunktionen

wie WEP, WPA Personal/Enterprise, WPA2 Personal/Enterprise und MAC-Authentifizierung zur Überprüfung der Identität drahtloser Geräte können Sie mit der Captive Portal-Funktion den Zugriff von Clients auf das Netzwerk verhindern, bis die Identität der Clients verifiziert wurde. Diese Authentifizierung und Autorisierung auf zwei Schichten bildet eine robuste Schutzfunktion, mittels derer auch Angriffe aus dem Innern des Netzwerks verhindert werden können.

Hohe Skalierbarkeit, Verfügbarkeit und Flexibilität

Viele Unternehmen unterliegen häufigen Änderungen im Hinblick auf die Größe und die Unternehmensstruktur. Um derart wechselnden Anforderungen gerecht zu werden, bietet der DWC-1000 eine neue Dimension an Wahlmöglichkeiten bezüglich der Funktionen: Administratoren können zusätzliche Lizenzen erwerben, um die Fähigkeiten des DWC-1000 nach Wunsch zu erweitern. D-Link bietet zwei Arten von Lizenzen an: ein AP-Lizenz-Upgrade und ein VPN-Lizenz-Upgrade..

Das AP-Lizenz-Upgrade erhöht die Anzahl verwalteter Access Points. Standardmäßig verwaltet der Wireless Controller DWC-1000 bis zu sechs Access Points. Mit dem AP-Lizenz-Upgrade können bis zu 24 Access Points pro Controller verwaltet werden.

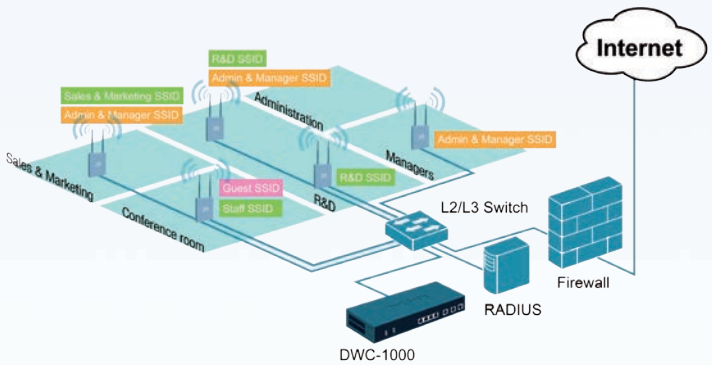
Das VPN-Lizenz-Upgrade erweitert den DWC-1000 um VPN-, Router- und Firewall-Funktionen. Mit der Firewall-Funktion können Administratoren den Netzwerkzugriff steuern, indem sie Regeln für die Klassifizierung festlegen. Die beiden Option-Anschlüsse sind mit Link-Failover und Redundanz für die Internetverbindung ausgestattet, um die ständige Verfügbarkeit des Internetzugangs sicherzustellen. Die Funktionen für virtuelle private Netzwerke (VPN) ermöglichen sicheren Fernzugriff zur Verwaltung von Access Points, die sich in Zweigstellen befinden. Site-to-Site-VPN-Tunnel verwenden IPSec (IP Security), PPTP (Point-to-Point Tunneling Protocol) oder L2TP (Layer 2 Tunneling Protocol), um die Konnektivität für Zweigstellen über verschlüsselte virtuelle Verbindungen sicherzustellen. Darüber hinaus können Sie Ihren mobilen Benutzern mit SSL-VPN-Tunneln Remotezugriff auf eine zentrale Unternehmensdatenbank zur Verfügung stellen.

Beide Lizenzoptionen bieten Skalierbarkeit, Flexibilität und erweiterten Funktionsumfang für potenzielles Unternehmenswachstum.

Vereinfachtes Management

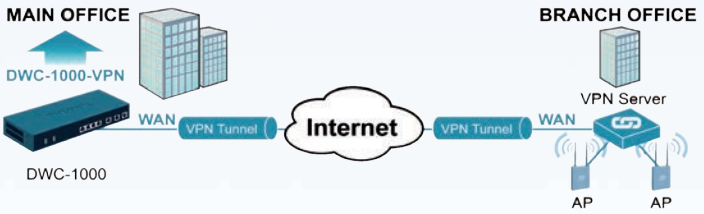
Über die zentrale Fernsteuerung verwalteter Access Points können kompatible Wireless Access Points von D-Link auf einfache Weise automatisch erkannt, zur Liste verwalteter Access Points hinzugefügt und mit einmalig festgelegten Einstellungen für die Erstkonfiguration versehen werden. Dank der Cluster-Funktion für Controller können sich Administratoren bei einem Wireless Controller anmelden und wichtige Konfigurationseinstellungen auf anderen Controllern innerhalb der Gruppe vornehmen. Die Echtzeitüberwachung von Access Points und den zugeordneten Client-Stationen ermöglicht die effiziente Ausnutzung der Netzwerkressourcen. Systembenachrichtigungen und statistische Berichte zu den verwalteten Access Points unterstützen den Administrator bei der Verwaltung, Steuerung und Optimierung der Netzwerkperformance mithilfe des DWC-1000. Darüber hinaus unterstützt der DWC-1000 eine Vielzahl verschiedener verwalteter Access Points für den Inneneinsatz von D-Link, einschließlich Dualband- und Singleband-Modellen.

Netzwerkimplementierung innerhalb eines L2/L3-Netzwerks in einer Unternehmensumgebung



AP-Implementierung mit Verwaltung per Fernzugriff

(VPN/Router/Firewall-Lizenz-Upgrade erforderlich)



D-Link®
Building Networks for People

DWC-1000
Wireless Controller

Technische Daten

Schnittstelle		
Ethernet	• 2 10/100/1000-Option-Anschlüsse (WAN-Anschlüsse)[3]	• 4 10/100/1000-LAN-Anschlüsse
USB	• 2 USB 2.0-Anschlüsse	
Konsole	• RJ-45	
Kapazität und Leistung		
Maximale Anzahl Access Points pro Gerät (Standardwert/Erweiterung)	• 6/ 24[1]	
Maximale Anzahl Access Points pro Cluster (Standardwert/Erweiterung)	• 24/ 96[1]	
Anzahl gleichzeitiger Captive Portal-Authentifizierungsnutzer (drahtgebunden/drahtlos)	• 124/400	
Dedizierte IPSec-VPN-Tunnel[2]	• 70	
Dedizierte PPTP/L2TP-VPN-Tunnel[2]	• 25	
Dedizierte SSL-VPN-Tunnel[2]	• 20	
Access Point-Management		
Kompatible verwaltete APs	• DWL-8600AP • DWL-6600AP	• DWL-3600AP
AP-Erkennung und -Steuerung	• Schicht 2	• Schicht 3
AP-Überwachung	• Verwalteter AP • Unautorisierter AP (Rogue AP)	• Authentifizierungsfehler beim AP • Eigenständiger AP
Client-Überwachung	• Authentifizierter Client • Unautorisierter Client (Rogue Client)	• Authentifizierungsfehler beim Client • Ad-hoc-Client
Zentrale Verwaltung von Funkabdeckung/ Sicherheitsrichtlinien	• Unterstützt	
Roaming		
Fast Roaming	• Unterstützt	
Intra-Controller/Inter-Controller-Roaming	• Unterstützt	
Intra-Subnet/Inter-Subnet-Roaming	• Unterstützt	
Sicherheit		
WLAN-Sicherheit	• WEP • Dynamisches WEP	• WPA Personal/Enterprise • WPA2 Personal/Enterprise
Wireless Instruction Detection und Prevention System (WIDS)	• Klassifizierung unautorisierter und gültiger APs	• Schutz vor unautorisierten APs
LAN-Sicherheit	• portbasierte Zugriffskontrolle nach 802.1x und Gast-VLAN	
Authentifizierung	• Captive Portal • MAC-Authentifizierung	• Gastmanagement4
VLAN		
VLAN-Gruppe	• Bis zu 255 Einträge	
VLAN-Tagging nach 802.1q	• Unterstützt	
Subnetz-basiertes VLAN	• Unterstützt	
Portbasiertes VLAN	• Unterstützt	
Firewall-System[2]		
Richtlinie	• Jede Funktion unterstützt 100 Regeln	• Unterstützung für bis zu 600 Firewall-Regeln
Dynamische Route	• RIPv1, RIPv2	
Dynamisches DNS	• Unterstützt	
NAT, PAT	• Unterstützt	
Filterung von Webinhalten	• Statische URL	• Schlüsselwörter

DWC-1000
Wireless Controller

Technische Daten	
Netzwerk[2]	
Routen-Failover	• Unterstützt
Outbound Load Balancing	• Unterstützt
Virtuelle private Netzwerke (VPN)[2]	
Verschlüsselungsverfahren	• DES, 3DES, AES, Twofish, Blowfish, CAST-128, NULL
IPSec-NAT-Traversal	• Unterstützt
Dead-Peer-Erkennung	• Unterstützt
IP Encapsulating Security Payload (ESP)	• Unterstützt
IP Authentication Header (AH)	• Unterstützt
Keep-Alive für VPN-Tunnel	• Unterstützt
Hub and Spoke	• Unterstützt
Virtuelle private SSL-Netzwerke (SSL-VPN)2	
SSL-Verschlüsselungsverfahren	• DES, 3DES, AES
Integrität von SSL-Nachrichten	• MD5, SHA1
Systemmanagement	
Webbasierte Benutzeroberfläche	• HTTP
Befehlszeilenschnittstelle	• Unterstützt
SNMP	• v1, v2c, v3
Umgebungsbedingungen	
Stromversorgung	• Integriertes Netzteil DC, 12 V/2,5 A
Max. Leistungsaufnahme	• 19,3 W
Abmessungen	• 180 × 280 × 44 mm
Betriebstemperatur	• 0 bis 40 °C
Lagertemperatur	• –20 bis 70 °C
Luftfeuchtigkeit im Betrieb	• 5 bis 95 % (nicht kondensierend)
EMV	• FCC Klasse B, CE Klasse B, VCCI, C-Tick, IC
Sicherheit	• cUL, LVD (EN60950-1)

Optionale Produkte		
Kompatible Wireless Access Points von D-Link		
DWL-8600AP	• Unified Concurrent Dualband Access Point	• 802.11n/g/b/a
DWL-6600AP	• Wireless N Dualband Unified Access Point	• 802.11n/g/b/a
DWL-3600AP	• Wireless N Unified Access Point	• 802.11n/g/b
DWL-2600AP	• Wireless N Unified Access Point	• 802.11n/g/b
Kompatible Lizenzen		
DWC-1000-AP6-LIC	• Ermöglicht die Verwaltung sechs zusätzlicher APs	
DWC-1000-VPN-LIC	• Aktiviert VPN-, Router- und Firewall-Funktionen	

[1] Die Anzahl verwalteter APs kann durch den Erwerb von Lizenz-Upgrades erweitert werden. Nur in Gruppen von sechs Lizenzen pro Upgrade erhältlich.
[2] Funktionen werden durch den Erwerb des VPN/Router/Firewall-Lizenz-Upgrades aktiviert.
[3] Der erste Option-Port ist standardmäßig aktiviert. Der zweite Option-Port wird durch den Erwerb des VPN/Router/Firewall-Lizenz-Upgrades aktiviert.
[4] Unterstützt ab Firmware 4.2.0.3 oder höher. Weitere Informationen finden Sie in der Konfigurationsanleitung im Download-Bereich zum DWC-1000.

Weitere Informationen: www.dlink.de

D-Link®
Building Networks for People