DCWS-6002 Wireless Access Controller

Product Overview

The DCWS-6002 is a smart box-type access controller (AC) developed by Yunke China Information Technology Limited (hereinafter referred to as DCN) for small and medium wireless networks and large enterprise branches. It can combine with DCN smart wireless access points (APs) to form a centrally managed wireless LAN (WLAN) solution.

The DCWS-6002 supports two 10/100/1000Base-T electrical ports, and can manage up to 128 smart wireless APs. The device provides strong WLAN access control through systems such as precise user control and management, complete RF management and security mechanism, powerful QoS, seamless roaming, and authentication based on existing networks. Underpinned by a smart cluster management technology, the solution automatically adjusts AP power and channels by monitoring and controlling the RF environment of each AP in real time, and balances loads based on the number of users or traffic to minimize interference to wireless signals and stabilize wireless network loads.

Powered by DCN cutting-edge IPv6 technology, the DCWS-6002 is designed with full IPv6 compatibility. The device supports a broad range of static routing protocols including RIP, OSPF, BGP and PIM, as well as dynamic routing protocols such as IPv6 RIPng, OSPFv3 and PIM6.

A rich service array coupled with considerable cost efficiency positions the DCWS-6002 as a wireless AC preferred for small and medium networks as well as large enterprise branches.

Highlights

High-Performance and High-Reliability Wireless Network

- **More flexible data forwarding**

  The DCWS-6002 may be deployed on a Layer 2 (L2) or Layer 3 (L3) network without changing existing network architecture. Boasting of a local forwarding technology, the DCWS-6002 has thoroughly broken through the traffic bottleneck of wireless ACs. The local forwarding technology enables delay-sensitive data with high real-time transmission requirements to be forwarded through the wired network. In the 802.11n high traffic throughput scenario, this greatly alleviates the traffic pressure on the wireless AC and better meets higher traffic transmission requirements of future wireless networks, such as high-definition Video on Demand (VoD) and Voice over WLAN (VoWLAN) transmission.

- **High-reliability backup mechanism**

  The DCWS-6002 supports the following high-reliability backup mechanisms to ensure that a wireless network runs reliably:

  - 1+1 fast backup
  - N+1 backup
  - N+N backup
  - Portal 1+1 backup
  - DHCP server hot backup

- **Automatic emergency mechanism of APs**

  In a centralized network architecture where fit APs and a wireless AC are deployed, the APs will be unable to operate normally when the wireless AC is down and then the entire wireless network will crash. DCN wireless APs support an automatic emergency mechanism. This mechanism enables an AP to intelligently detect links. When detecting that the wireless AC is down, the AP quickly switches its operating mode so that it may continue to forward data while enabling new users to access the network. This mechanism attains high availability in the entire wireless network and really helps wireless users to be always online.

- **Dual-OS backup mechanism**

  The DCWS-6002 supports a dual-OS backup mechanism. When the DCWS-6002 fails to start from the active OS, it can immediately start from a standby OS, thereby improving the long-term running reliability of equipment in an adverse environment.

Wireless Network of Intelligent Control and Automatic Perception

- **Intelligent RF management**

  The DCWS-6002 provides an automatic power and channel adjustment function. It employs particular RF detection and management algorithms to attain a better RF coverage effect. When the signals of an AP are interfered by strong external signals, the AP may automatically switch to an appropriate operating channel under the control of the AC to avoid such interference, thereby guaranteeing wireless network communications. The system also supports wireless network blackhole compensation. When an AP on the network accidentally stops operating, the RF management function of the AC compensates the resulting blind area of signals so that the wireless network can still operate normally.

- **Intelligent control of terminals based on airtime fair**

  When some outdated 802.11b and 802.11g terminals are used on a wireless network or some terminals are far way from APs, negotiation rates will be low, causing a large number of users to experience a long WLAN access delay, low rates, or poor overall

AP performance. The AP performance problem in a low-rate terminal access environment, however, cannot be resolved by simply employing rate control and traffic shaping. DCN smart APs have essentially resolved this problem by using intelligent control of terminals based on airtime fairness, ensuring that a user can always enjoy the same joyful WLAN experience in the same location, no matter what type of the terminal the user is holding.

The intelligent control of terminals based on airtime fairness greatly improves the performance of both the client and the entire network. It enables all clients with high data transmission rates to attain strikingly higher performance while low-rate clients are almost not affected at all. The performance will be even more obviously higher on an open wireless network. Once high-rate clients finish data transmission, fewer clients will be transmitting data on the wireless network. In this case, there will be less contention and retry on the network, thereby greatly improving overall AP performance.

- **Intelligent load balancing mechanism**

In general, a wireless client will select an AP according to the signal strength of APs. When this uncontrolled access mode is applied, however, a large number of clients could be connected to the same AP simply because the AP provides strong signals. As more clients are connected to an AP, the bandwidth available to each client will be smaller, thereby greatly affecting user experience of the clients. DCN wireless products support diversified intelligent load balancing means:

- AP load balancing based on traffic
- AP load balancing based on the number of users
- AP load balancing based on frequency bands
- Access control based on signal strength of terminals
- Mandatory roaming control of terminals to direct terminals to APs with stronger signals

- **Intelligent identification of terminals**

DCN wireless ACs may combine with DCN smart APs and a unified authentication platform to intelligently identify the size, system type, and type of each terminal; and comprehensively support mainstream smart terminal operating systems, such as Apple iOS, Android, and Windows. They intelligently identify the size of a terminal and adaptively present a portal authentication page of the corresponding size and page pattern, freeing users from multiple times of dragging to adjust the screen and enabling users to enjoy more intelligent wireless experience. They can also intelligently identify the system type of each terminal and present the system type of each terminal such as Windows, MAC OS, or Android on the unified authentication platform, exhibiting every detail of intelligence to users. In addition, they can intelligently identify the type of each terminal such as the mobile phone, tablet, or PC, and implement dynamic policy control of terminals according to different types of the terminals, making possible more intelligent user control at a finer granularity.

- **Comprehensive support for IPv4/v6 dual-stack networks**

Powered by DCN cutting-edge IPv6 technology, the DCWS-6002 may be deployed on an IPv6 network.

- **Network-wide seamless roaming**

  The DCWS-6002 supports an advanced wireless AC cluster technology. This technology enables multiple DCWS-6002 devices to synchronize online connection information and roaming records of all users with one another in real time. This technology implements not only L2 seamless roaming inside a wireless AC but also fast roaming across wireless ACs. As client IP address information does not change and re-authentication is not required in the roaming process, the continuity of real-time mobile services is well guaranteed.

Secure and Controllable Wireless Network

- **User isolation policy**

  The DCWS-6002 supports the isolation of wireless users from one another. If this user isolation function is enabled, two wireless clients cannot directly communicate with each other but can only access an upstream wired network. This further guarantees the security of wireless network applications.

- **Wireless intrusion detection and intrusion defense**

  The DCWS-6002 supports wireless intrusion detection and intrusion defense features, such as detection of unauthorized wireless devices, intrusion detection, blacklist, and white list, as well as anti-DoS for various wireless management packets, thereby greatly improving security management of an entire wireless network.

- **Wireless user management at a fine granularity**

  Under the management of the DCWS-6002, each AP supports a maximum of 32 WLANs to implement multi-layer multi-service management of wireless users at a fine granularity. Each WLAN supports access control and uplink/downlink rate limit based on MAC or IP addresses. These WLANs may be bound to VLANs. In addition, different authentication and accounting policies can be implemented. This feature is practically significant in a multi-WLAN environment.

- **Operational-level permission management mechanism**

  An SSID-based user permission management mechanism enables a network to be divided into multiple virtual wireless networks based on multiple SSIDs according to actual application requirements. This mechanism sets specific management and viewing permissions for specific users, so that users are completely isolated from one another in terms of operation and management.

- **Secure user admission**

  The DCWS-6002 provides multiple secure access, authentication, and accounting mechanisms for various application environments. These mechanisms include:

  - 802.1x authentication
  - Captive portal authentication, including built-in portal, external portal, and custom portal authentication modes

- MAC address authentication
- LDAP authentication
- WAPI encryption and authentication
- Wired/wireless integrated authentication and accounting

- **Wireless SAVI**

  DCN wireless network products support a source address validation (SAVI) technology to deal with spoofed packet attacks that keep emerging on today's campus networks. As users' IP addresses are obtained through an address allocation protocol, users access the Internet using correct addresses in subsequent applications and cannot spoof others' IP addresses, thereby guaranteeing the reliability of source addresses. In addition, the SAVI technology is combined with a portal technology to further guarantee the authenticity and security of packets of all users accessing the Internet.

- **PEAP user authentication**

  With the popularization and application of smart terminals, wireless terminal users require authentication mechanisms of higher usability and convenience. Using a mechanism that combines portal authentication and MAC address authentication, DCN wireless network products support Protected Extensible Authentication Protocol (PEAP) authentication to attain better user experience. Initially a user needs to manually perform portal authentication and later the user gets authenticated through PEAP in automatic mode. DCN wireless network products feature high terminal adaptation and provide good authentication compatibility. They adapt to the majority of WLAN terminals and do not need to adapt to clients. DCN wireless network products are compatible with existing portal authentication modes.

- **Secure access mechanism of APs**

  An AP is usually deployed in a public area and therefore requires a strict security mechanism to guarantee the legality of access devices. The following secure access mechanisms may be applied between a DCN wireless AC and a smart AP:

  - AP MAC address authentication
  - AP password authentication
  - Bidirectional digital certificate authentication

- **Real-time spectrum protection**

  DCN smart APs support a built-in RF collection module that integrates RF monitoring and real-time spectrum protection. By implementing communications and data collection through the respective AP, the RF collection module performs wireless environment quality monitoring, wireless network capability tendency evaluation, and unexpected-interference alarms. It resorts to a graphical means to actively detect and identify RF interference sources (Wi-Fi or non-Wi-Fi) and provides a real-time spectrum analysis diagram. In addition, it can automatically identify interference sources and determine the locations of problematic wireless devices, ensuring that a wireless network attains optimal performance.

Easy-to-Manage Wireless Network

- **AP plug-and-play**

  The DCWS-6002 smart AC can be seamlessly integrated with existing switches, firewalls, authentication servers, and other network devices. DCN smart APs are able to automatically discover the DCWS-6002. A wireless network function can be enabled on an AP without performing any configuration on the AP at all.

  When used with the DCWS-6002, DCN smart APs support plug-and-play and zero configuration. The wireless AC undertakes all the management, control, and configuration of the APs. Network administrators do not need to separately manage or maintain a huge number of wireless APs. All actions, such as configuration, firmware upgrade, and security policy updating, are performed uniformly under the control of the wireless AC.

- **Remote probe analysis**

  The DCWS-6002 supports remote probe analysis of APs. It listens to and captures Wi-Fi packets in the coverage and mirrors them to a local analysis device in real time to help network administrators better perform troubleshooting or optimization analysis. The remote probe analysis function can perform non-convergence mirroring of a working channel and sampling of all channels in polling mode as well to flexibly meet various wireless network monitoring, operation, and maintenance requirements.

- **Multiple management modes and uniform management platform**

  The DCWS-6002 supports various management modes such as command lines and web. It can be used to plan, deploy, monitor, and manage APs on an entire network centrally and effectively at low costs. It may also be used with a DCN platform for integrated management of wireless and wired devices, so that administrators can monitor and manage the entire network in a data center as follows:

  - Generating topologies
  - Checking the working states of APs and the states of online users
  - Planning RF resources on the entire network
  - Locating users
  - Generating security alarms
  - Checking link loads, device usage and roaming records
  - Outputting reports

Product Specifications

Hardware Specifications

Item	DCWS-6002
Service port	Two 10/100/1000Base-T
Management port	One console port (RJ-45)
Power supply	AC 100 V to 240 V, 50 Hz to 60 Hz
Maximum power consumption	8W
Working/Storage temperature	0℃ to +50℃ –40℃ to +70℃
Working/Storage RH	5% to 90% (non-condensing)
Dimensions (W x D x H)	328.2 mm x 170 mm x 42.2 mm

Software Specifications

Item	DCWS-6002
Base number of manageable APs	16
Maximum number of manageable APs	128
Number of manageable ACs in a cluster	64
AP upgrade step	16
Maximum number of concurrent wireless users	5k
VLANs	4K
ARP table	8K
Switching time during	< 30 ms

roaming	
L2 protocols and standards	IEEE802.3 (10Base-T), IEEE802.3u (100Base-TX), IEEE802.3ab (1000Base-T), IEEE802.1Q (VLAN), IEEE802.1p (COS), IEEE802.1x (Port Control) IGMP Snooping, MLD Snooping GVRP, PVLAN
L3 protocols and standards	Static Routing RIPv1/v2, OSPF, BGP, VRRP, IGMP v1/v2/v3 ARP, ARP Proxy PIM-SM, PIM-DM, PIM-SSM
Wireless protocols and standards	802.11, 802.11a, 802.11b, 802.11g, 802.11n, 802.11d, 802.11h, 802.11i, 802.11e, 802.11k
CAPWAP protocol	Supports L2/L3 network topology between an AP and an AC.
	Enables an AP to automatically discover an accessible AC.
	Enables an AP to automatically upgrade its software version from an AC.
	Enables an AP to automatically download configurations from an AC.
IPv6 protocols and standards	IPv4/v6 dual-stack, manual tunnel, ISATAP, 6to4 tunnel, IPv4 over IPv6 tunnel, DHCPv6, DNSv6, ICMPv6, ACLv6, TCP/UDP for IPv6, SOCKET for IPv6, SNMP v6, Ping /Traceroute v6, RADIUS, Telnet/SSH v6, FTP/TFTP v6, NTP v6, IPv6 MIB support for SNMP, VRRP for IPv6, IPv6 QoS, static routing, OSPFv3, IPv6 SAVI
High reliability	1+1 fast backup
	N+1 backup
	N+N backup
	Portal 1+1 backup
	DHCP server hot backup
RF management	Setting country codes
	Manually/automatically setting the transmit power
	Manually/automatically setting the working channel

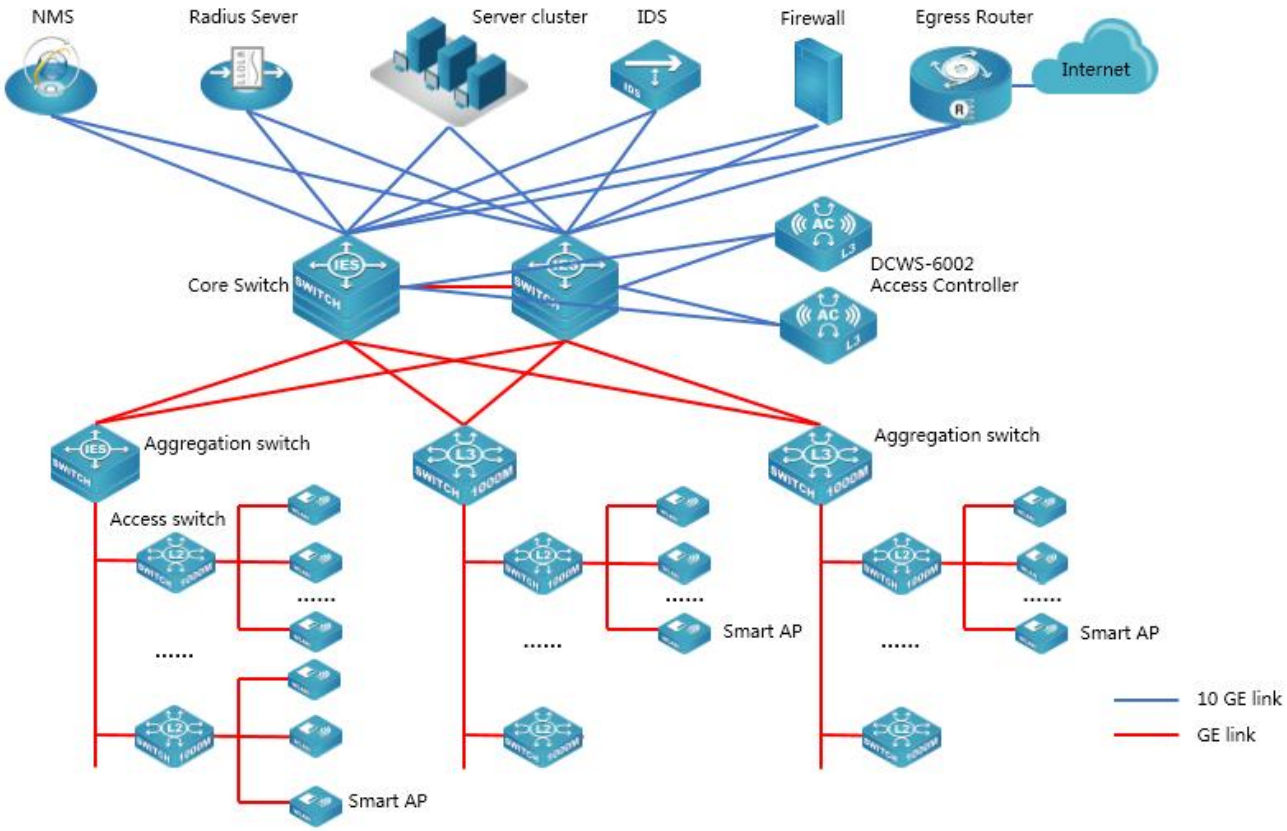
	Automatically adjusting the transmission rate
	Blind area detection and repair
	RF environment scanning, which enables a working AP to scan the surrounding RF environment
	RF interference detection and avoidance
	11n-preferred RF policy
	SSID hiding
	20 MHz and 40 MHz channel bandwidth configuration
	Airtime protection in hybrid access of 11bg and 11n terminals
	Terminal-based airtime fairness scheduling
	Spectral analysis
	Terminal locating (A terminal locating algorithm can be embedded in the AC)
	Spectral navigation (5 GHz preferred)
	11n only
	SSID-based or Radio-based limit on the number of users
	User online detection
	Automatic aging of traffic-free users
	Prohibiting the access of clients with weak signals
	Remote probe analysis
	Forced roaming of clients with weak signals
Security	64/128 WEP, dynamic WEP, TKIP, CCMP, and SMS encryption
	802.11i security authentication and two modes (Enterprise and Personal) of 802.1x and PSK
	WAPI encryption and authentication
	LDAP authentication
	MAC address authentication
	Portal authentication, including built-in portal, external portal, and custom portal

	authentication modes
	PEAP user authentication
	Forwarding security control, such as frame filtering, white list, static blacklist, and dynamic blacklist
	User isolation
	Periodic Radio/SSID enabling and disabling
	Access control of free resources
	Secure admission control of wireless terminals
	Access control of various data packets such as MAC, IPv4, and IPv6 packets
	Secure access control of APs, such as MAC authentication, password authentication, or digital certificate authentication between an AP and an AC
	Radius Client
	Backup authentication server
	Wireless SAVI
	User access control based on AP locations
	Wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS)
	Protection against flooding attacks
	Protection against spoofing attacks
Forwarding	IPv6 access and forwarding; constructing IPv6 WLAN access service on an IPv4 network; providing IPv4 WLAN access service on an IPv6 network; and constructing private IPv6 WLAN network service on an IPv6 network
	Fast L2/L3 roaming between APs served by the same AC
	Fast L2/L3 roaming between APs served by different ACs
	IPv4 and IPv6 multicast forwarding
	WDS AP
QoS	802.11e (WMM); and 4-level priority queues, ensuring that applications sensitive to the

	real-time effect, such as voice and video services, are transmitted first
	Ethernet port 802.1P identification and marking
	Mapping from wireless priorities to wired priorities
	Mapping of different SSIDs/VLANs to different QoS policies
	Mapping of data streams that match with different packet fields to different QoS policies
	Access control of MAC, IPv4, and IPv6 data packets
	Load balancing based on the number of users
	Load balancing based on user traffic
	Load balancing based on frequency bands
	Bandwidth limit based on APs
	Bandwidth limit based on SSIDs
	Bandwidth limit based on terminals
	Bandwidth limit based on specific data streams
	Power saving mode
	Multicast-to-unicast mechanism
	Automatic emergency mechanism of APs
	Intelligent identification of terminals
Management	Web management
	Configuration through a console port
	SNMP v1/v2c/v3
	Both local and remote maintenance
	Local logs, Syslog, and log file export
	Alarm
	Fault detection
	Statistics
	Login through Telnet
	Login through SSH

	Dual-image (dual-OS) backup
	Hardware watchdog
	AC cluster management; automatic information synchronization between ACs in a cluster, and automatic or manual push of configuration information
	SSID-based user permission management mechanism

Typical Applications



Product Purchase Information

Product Model	Description	Remarks
DCWS-6002	DCN wireless AC (including a license for managing 16 APs by default)	Mandatory
DCWS-L16	Upgrade license of the DCN wired/wireless integrated smart AC (for upgrading 16 Aps, minimum number of upgrade step is 16 APs)	Optional