Контроллеры DCN серии DCWS

DCWS-6002

DCWS-6002 - это интеллектуальный контроллер доступа (AC), разработанный Yunke China Information Technology Limited для малых и средних беспроводных сетей и филиалов крупных предприятий. Может сочетаться с DCN Smart Wireless для формирования решения беспроводной локальной сети (WLAN) с централизованным управлением.

DCWS-6002 имеет два медных порта 10/100/1000Base-T и может управлять до 128 интеллектуальными беспроводными точками доступа. Устройство обеспечивает надежный контроль доступа WLAN с помощью таких систем, как ACL, полное управление RF и механизм безопасности, мощный QoS, бесперебойный роуминг и аутентификация на основе существующих сетей.

Устройство	DCWS-6002
Размерность	328.2 mm x 170 mm x 42.2 mm
Сервисные порты	Two 10/100/1000Base-T
Управление	One console port (RJ-45)
Источник питания	AC 100 V to 240 V, 50 Hz to 60 Hz
Энергопотребление (пик)	8 W
Рабочая температура Температура хранения	0℃to +50℃ –40℃to +70℃
Допустимая влажность	5% to 90% (non-condensing)
Программная спецификация	
Максимальное число подключаемых AP	16
Максимальное число AP для управления	128
Максимальное число AC в кластере	64
Число одновременно обновляемых AP	16
Максимальное количество конкурентных пользователей	5k
Максимальное количество VLAN	4K
Размер ARP-таблицы	8K
Время переключения в роуминге	< 30 ms
L2 протоколы и стандарты	IEEE802.3 (10Base-T), IEEE802.3u (100Base-TX), IEEE802.3z (1000BASE-X), IEEE802.3ab (1000Base-T), IEEE802.3ae (10GBase-T) IEEE802.3ak (10GBASE-CX4), IEEE802.1Q (VLAN) IEEEE802.1d (STP), IEEEE802.1W (RSTP), IEEEE802.1S (MSTP)

	IEEE802.1p (COS) IEEE802.1x (Port Control), IEEE802.3x (Flow Control) IEEE802.3ad (LACP), Port Mirror IGMP Snooping, MLD Snooping QinQ, GVRP, PVLAN Broadcast storm control
L3 протоколы и стандарты	Static Routing RIPv1/v2, OSPF, BGP, VRRP, IGMP v1/v2/v3 ARP, ARP Proxy PIM-SM, PIM-DM, PIM-SSM
Беспроводные протоколы и стандарты	802.11, 802.11a, 802.11b, 802.11g, 802.11n, 802.11d, 802.11h, 802.11i, 802.11e, 802.11k
Протокол CAPWAP	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 протоколы и стандарты	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
Высокая доступность	N+1 backup
	N+N backup
	Portal 1+1 backup
Беспроводное управление	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
	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
Безопасность	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
Маршрутизация	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
	IPv4 and IPv6 multicast forwarding
	WDS AP

Качество сервиса	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
Управление	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 Telne
	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

DCWS-6028(R2)

DCWS-6028 (R2) - это высокопроизводительный интеллектуальный контроллер доступа типа «ящик» (AC), разработанный независимой компанией Yunke China.
Данное решение разработано для средних беспроводных сетей. Интегрирует как проводные, так и беспроводные средства доступа, он предлагает 10 портов GE и может объединяться с интеллектуальными точками доступа (AP) DCN для формирования централизованно управляемого решения беспроводной локальной сети (WLAN).

Благодаря гибкой конфигурации портов DCWS-6028 (R2) предоставляет шестнадцать комбинированных портов GE, восемь фиксированных портов SFP и четыре 10G SFP + порта. С модульными резервными блоками питания 1 + 1 DCWS-6028 (R2) предпочтительнее для беспроводных образовательных сетей, департаментов, правительств и малых или средних предприятий, где высокая производительность, комплексные функции, высокий уровень безопасности и
требуется высокая надежность.

Item	DCWS-6028(R2)
Размерность	440mmx44mmx350mm; 19 inches, 1 U high, supporting rack installation
Коммутационная фабрика	208 Gbps
Сервисные порты	16 GE combo ports (GE/SFP)
	8 GE SFP ports
	4 10G SFP+ ports
Управление	One console port (RJ-45)
Источник питания	2 power slots, 1+1 Modular Redundan
Энергопотребление	90 W
Рабочая температура Температура хранения	0℃to +50℃ –40℃to +75℃
Допустимая влажность	10% to 90% (non-condensing)
Программная спецификация	
Максимальное число подключаемых AP	32
Максимальное число AP для управления	1024
Максимальное число AC в кластере	64
Число одновременно обновляемых AP	32
Максимальное количество конкурентных пользователей	60k
Максимальное количество VLAN	4K
Максимальное количество ACL	4K
Максимальное количество MAC-адресов	32K
Размер ARP-таблицы	16K
Время переключения в роуминге	< 30 ms
L2 протоколы и	IEEE802.3 (10Base-T), IEEE802.3u (100Base-TX), IEEE802.3z

стандарты	(1000BASE-X), IEEE802.3ab (1000Base-T), IEEE802.3ae (10GBase-T) IEEE802.3ak (10GBASE-CX4), IEEE802.1Q (VLAN) IEEEE802.1d (STP), IEEEE802.1W (RSTP), IEEEE802.1S (MSTP) IEEE802.1p (COS) IEEE802.1x (Port Control), IEEE802.3x (Flow Control) IEEE802.3ad (LACP), Port Mirror IGMP Snooping, MLD Snooping QinQ, GVRP, PVLAN Broadcast storm control
L3 протоколы и стандарты	Static Routing RIPv1/v2, OSPF, BGP, VRRP, IGMP v1/v2/v3 ARP, ARP Proxy PIM-SM, PIM-DM, PIM-SSM
Беспроводные протоколы и стандарты	802.11, 802.11a, 802.11b, 802.11g, 802.11n, 802.11d, 802.11h, 802.11i, 802.11e, 802.11k
Протокол CAPWAP	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 протоколы и стандарты	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
Высокая доступность	N+1 backup
	N+N backup
	Portal 1+1 backup
Беспроводное управление	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
	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
Безопасность	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
Маршрутизация	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
	IPv4 and IPv6 multicast forwarding
	WDS AP
Качество сервиса	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
Управление	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 Telne
	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