DPtech WCS7000 and WAP902n

Overview

Ideal for demanding, complex deployments with multiple offices or with highly secure LAN requirements, the DPtech Wireless Controller System centrally manages and controls DPtech Wireless Access Point.

Key benefits

DELIVERS CONTROL: A REQUIREMENT FOR SEAMLESS SECURITY AND MOBILITY

The DPtech WCS7000 series provides refined user control and management, comprehensive RF management and security mechanism, fast roaming, strong Qualify of Service and IPv4/IPv6 features, and powerful WLAN access control functions provide the most ideal access control solutions for WLAN access of large enterprise campus networks, wireless MAN coverage and hot spot coverage.

The WCS7000 supports up to 512 APs. DPtech provides network services over an innovative, authentication-based networking structure. On the basis of user IDs instead of ports or devices, mobility and security are ensured over the whole network.

The WCS WLAN exchange user information to implement inter-WCS roaming and consistent access and security policies on the whole network. According to WPA/WPA2, encryption algorithms such as AES, TKIP, and WEP are also used together with 802.1X authentication to enhance network security.

Working together with DPtech Wireless Access Point 902n, WCS7000 series can be simply deployed on Layer 2 or Layer 3 networks without affecting existing configurations.

WAP902n support dual radio 802.11 a/b/g/n functionality

Wireless Controller System 7000 support to 512 Wireless Access Point

CENTRALIZES MANAGEMENT

The DPtech Wireless Manager eliminates the time consuming task of individually configuring each device. Simple and centralized setup makes initial deployment and long term management easier. Accessed from anywhere on the network, the Wireless Manager software lets administrators change parameters of hundreds of managed access points or dozens of wireless switches with just a few keystrokes.

ENHANCES STANDARDS-BASED SECURITY

The centralized security management of the DPtech Wireless LAN System can significantly enhance protection. The exchange of user-based information within the Network and Mobility Domain adds an additional level of control — beyond the existing IEEE 802.11i Wi-Fi® Protected Access 2 (WPA2™), Advanced Encryption Standard (AES), Temporal Key Interchange Protocol (TKIP), Wired Equivalent

Privacy (WEP) encryption and IEEE 802.1X authentication — for user and group access to network resources. Sharing user-specific security policies between WLAN controllers and switches enables consistent enforcement of user and group attributes as the user roams across the WLAN.

INTELLIGENT SWITCHING

An integral component of the DPtech Wireless LAN System, the DPtech WAP902n with intelligent switching offers both centralized and distributed data forwarding. It automatically determines the best alternative based on the requirements of the underlying application, allowing it to support the most demanding wireless applications indoors and outdoors, including VoWiFi and video distribution

PROVIDES ENTERPRISE-WIDE FLEXIBILITY

The DPtech Wireless System can be deployed on any existing Layer 2 or Layer 3 LAN topology with no backbone or hardware reconfiguration required.

The Wireless controller system and associated WAPs can reside anywhere in the network, separated by Layer 2/Layer 3 devices. The system can operate as an integrated infrastructure, making it easy to scale or change as business needs dictate.

The WCS7000 Controller comes configured to support 64 WAPs and is expandable in increments of 32 WAPs with support up to 512 active and configured WAPs per controller and scalable up to 5000 users per multiple controller to optimize the throughout and performance.

FLEXIBLE EXTENDED WIRELESS NETWORK

The DPtech WAP902n series wireless access points (APs) are the new generation PoE enabled gigabit wireless APs compatible with 802.11n. The Access Point can provide the wireless access speed six times that of the traditional 802.11a/b/g network or even a faster speed. Multiple Input Multiple Output (MIMO) technology with six built-in dual-band omni-directional antennas provides a larger scope. The series APs adopt the gigabit Ethernet interface as uplink interface, which breaks the restriction of the 100M Ethernet interface. As a result, wireless multimedia application becomes a reality. The WAP902n series APs support two work modes, Fat and Fit. The work mode can be shifted between Fat and Fit flexibly through command lines according to the requirement of network planning. As Fit APs, the WAP902n series products need to work with the WCS7000 series wireless controller developed by DPtech independently. As Fat APs, the series products can be used for independent networking. The feature of support of Fat/Fit work modes by the WAP902n series products benefits the smooth upgrade of customers' WLAN from a small network to a large network. The user investment is protected properly.

The WAP902n is a dual frequency multi-mode wireless AP. It can work simultaneously in the 2.4GHz band and the 5GHz band of the WLAN, and supports four modes, IEEE802.11a, IEEE802.11b, IEEE802.11g and IEEE802.11n.

Features

802.1a/b/g/n Access Point Management

In addition to 802.11a/b/g AP management, the WCS7000 series can work together with the 802.11n-based WAP902n series APs to provide wireless access at a speed six times that on a traditional 802.11a/b/g network. 802.11n covers a wider range and supports real WLAN multimedia applications.

Forwarding Modes

In a wireless network of centralized forwarding modes, all wireless traffic is sent to a WCS for processing. Therefore, the forwarding capability of the WCS may become the bottleneck. This is especially true on wireless networks where APs are deployed at branches, WCS are deployed at the headquarters, and APs and WCS are connected over a WAN.

However, distributed forwarding cannot provide traffic control as good as the centralized forwarding mode does.

The WCS7000 series support both forwarding modes. You can set SSID based forwarding as needed.

Carrier-Class Wireless User Access Control and Management

User-based access control is a feature of the WCS7000 series. The WCS7000 series use a user profile as a configuration template to save predefined configurations. For different application scenarios, you can configure different items in a user profile, such as Committed Access Rate (CAR) and QoS policies.

A client that wants to access a device needs to pass authentication first. During authentication, an authentication server assigns a user profile to the device. If the user passes authentication, the device uses the configuration contents in the user profile to restrict the accessible resources of the user. When the user goes offline, the device disables the user profile. Thus, user profiles are applicable to online users rather than offline users and users that fail to pass authentication.

The WCS7000 series support MAC-based access control, which allows you to configure and modify the access rights of a user group or a particular user. The refined user rights control method enhances the availability of WLANs and facilitates access right assignment.

MAC-based VLAN is another strong feature of the WCS7000 series. The administrator can assign users (or MAC addresses) with the same attribute into the same VLAN and configure a VLAN-based security policy on the WCS. This simplifies system configuration and refines user management to the per-user granularity.

Wireless Client Access Position Control

For security or accounting, the administrator may need to control the physical positions of wireless clients. The WCS7000 series can satisfy this requirement. During authentication, the WCS gets a list of permitted APs from the authentication server and then selects an AP for the requesting wireless client. In this way, the wireless client can only associate with that AP and thus its position is controlled.

High Reliability

N+1 redundancy is the best solution in terms of reliability and economy, in which, N WCS7000 series ACs operate independently, and another AC operates as a standby AC. When one of the N ACs fails, the standby AC will replace it. When the active AC recovers, APs will associate with it again.

N+N Redundancy can be deployed in a WLAN, the

N+N redundancy feature allows an AP to choose an optimal AC for access. If the optimal AC fails, the AP will choose another optimal AC for access. This mechanism implements both AC redundancy and load sharing. You can configure the AP to select the optimal AC according to the loads or predefined priorities of ACs. To implement N+N redundancy, the N-1 ACs must be capable of managing all the deployed APs.

Intelligent Channel Switching

In a WLAN, adjacent wireless APs should work in different channels to avoid channel interference. However, channels are very rare resources for a WLAN. There are a small number of non-overlapping channels for APs. For example, there are only three non-overlapping channels for a 2.4G network. Therefore, the key to wireless applications is how to allocate channels for APs intelligently. Meanwhile, there are many possible interference sources that can affect the normal operation of APs in a WLAN, such as rogue APs, radars and microwave ovens. The intelligent channel switching technique can ensure the allocation of an optimal channel to each AP, and minimize adjacent channel interference. Besides, the real-time interference detection function can help keep APs away from interference sources such as rogue APs.

Intelligent Load Sharing among APs

According to IEEE 802.11, wireless clients control wireless roaming in WLANs. Usually, a wireless client chooses an AP based on the Received Signal Strength Indication (RSSI). Therefore, many clients may choose the same AP for this AP has a high RSSI. As these clients share the same wireless medium, the throughput of each client is reduced greatly.

The intelligent AP load sharing function can analyze the locations of wireless clients in real time, dynamically determine which APs at the current location can share load with one another, and implement load sharing among these APs. In addition to load sharing based on the number of online sessions, the system also supports load sharing based on the traffic of online wireless users.

Wireless Intrusion Detection System

1. Rogue AP detection

The WCS7000 series can automatically detect rogue devices (such as rouge APs or Ad Hoc wireless terminals) and report to the network management center in real time.

2. White list function

The WCS7000 series support the white list function. With this function enabled, only the wireless clients on the white list are considered legal. Packets from illegal clients are all dropped at the APs.

3. Black list function

The WCS7000 series support the static blacklist and dynamic blacklist functions. You can manually add specific devices into the blacklist or configure the AC to add devices into the blacklist through real-time detection. Packets from devices in the blacklist are all dropped at the APs to minimize the impact of attack packets on the wireless network.

4. Protection against wireless protocol attacks

The WCS7000 series can detect many kinds of attacks, such as DOS attack, flooding attack, de-authentication and de-connection packet spoofing, and weak IV of wireless users. When an AC detects any of the above-mentioned attacks, it generates an alarm or log information to remind the administrator to deal with the attack accordingly. This function can work in conjunction with the dynamic blacklist function. That is, when the AC detects an attack, it adds the wireless client that initiated the attack into the blacklist so that

the WLAN will not be attacked by that wireless client any more.

5. 802.1X, MAC, Portal, and PPPoE Authentication

The WCS7000 series support multiple 802.1X authentication modes, such as TLS, PEAP, TTLS, MD5, and SIM card. The local 802.1X authentication mode supports MD5, TLS and PEAP and thus the user does not need to configure the AAA server. The WCS7000 series also support dynamic VLAN and ACL assignment to wireless clients after they pass 802.1X authentication. You can predefine the access control policies so that the system can automatically configure user rights during user authentication.

6. MAC address authentication

Authentication modes for computer users are not suitable for some hand-held terminals (such as WiFi phones and hand-held mobile terminals). By supporting MAC address authentication, the WCS7000 series can easily solve this problem. On a wireless access controller or CAMS server, you can configure which MAC addresses are allowed to access the wireless network. MAC addresses not configured are considered illegal and cannot access the wireless network. This function facilitates some wireless applications such as the wireless medicine system, where MAC address authentication can ensure that only the PDA terminals of the hospital can access the wireless network while those of patients cannot.

7. Portal authentication

For visitors who want to access the Internet through the wireless network of an enterprise but have no 802.1X client installed, portal authentication is a good solution.

8. PPPoE authentication

Using the mature PPPoE authentication and accounting functions, the WCS7000 series can conveniently implement advanced accounting for users, such as accounting by traffic, to satisfy certain carrier-level requirements.

Supporting IPv6

The WCS7000 series support access of IPv6 wireless users. As the gateway for IPv6 users is not on an access controller, a dedicated IPv6 gateway is needed. The access controller can recognize IPv6 packets on the tunnel start AP. Because the AP device can recognize IPv6 packets, it can map the IPv6 priority to the tunnel priority. The access controller side can also use ACLs to control and filter IPv6 packets.

The WCS7000 series can be deployed in IPv6 networks, in which an AC automatically negotiates an IPv6 tunnel with each AP. Although the AC and AP are working in IPv6 mode, the AC can still correctly recognize and process IPv4 packets from wireless clients. The flexible IPv4/v6 adaptability enables the WCS7000 series to satisfy various complicated applications in the process of IPv4 to IPv6 migration. When deployed on an IPv6 island, the AC can provide services for IPv4 wireless clients. When deployed on an IPv4 island, it can also allow wireless clients to log in to the network through IPv6.

End-to-End QoS

Developed based on the Conplat platform, the WCS7000 series support not only the Diff-Serv standard but also the IPv6 QoS.

The QoS Diff-Serv model includes traffic classification and traffic policing, completely implementing the six groups of services, EF, AF1 through AF4 and BE. This enables ISPs to provide differentiated services for users, making the Internet a true integrated network

carrying data, voice and video services at the same time.

Layer 2 and Layer 3 Roaming

Layer 3 roaming is hard to implement in a WLAN comprised of fat APs due to limited communication between APs. With the centralized forwarding and control architecture, the WCS7000 series support Layer-2 and Layer-3 roaming and solve the inter-subnet roaming problem. This excellent roaming feature allows you to plan a wireless network without worrying about the planning of the existing wired network. All you need to consider is wireless signal coverage. This greatly simplifies the early wireless network planning and reduces the network planning cost.

When a wireless terminal uses 802.1X for 802.11 access authentication and key exchange, there will be a large number of packets exchanged between the terminal and the AP. If the complete 802.1X authentication process is followed by a wireless terminal that roams from one AP to another, this results in a very long handover time. This is unacceptable for delay sensitive services such as VoIP. The WCS7000 series use Key Caching to implement fast handover of roaming wireless terminals. The Key Cache functionality allows wireless terminals to roam from one AP to another without following the complete 802.1X authentication process while it ensures user identification and the continuity of key use. With fast handover, the handover time is kept within 50 ms.

Specification

Item	WCS7000
Weight	• < 7.4 kg (16.31 lb.) (configured with two power modules)
Dimensions (H x W x D), excluding the plastic panel width	• 43.6 x 440 x 430 mm (1.72 x 17.32 x 16.93 in.)
Management Port	• One Console Port
Service Ports	• Four GE electrical ports • Four GE SFP optical ports
Input voltage ranges	• AC: • Rated input voltage range: 100 VAC to 240 VAC; 50 Hz or 60 Hz • Max. input voltage range: 90 VAC to 264 VAC; 47 Hz or 63 Hz
Max power consumption	• < 70 W
Operating temperature	• 0ºC–45ºC (32ºF–113ºF)
Relative humidity	• 10%–90% (non-condensing)
Storage temperature	• -40ºC–70ºC
Storage humidity	• 5%–95% (non-condensing)
Security standards	• UL 60950-1, • CAN/CSA C22.2 No 60950-1, • IEC 60950-1, • EN 60950-1/A11, • AS/NZS 60950, • EN 60825-1, • EN 60825-2, • FDA 21 CFR Subchapter J
EMC	• ETSI EN 300 386 V1.3.3:2005 • EN 55024: 1998+ A1: 2001 + A2: 2003 • EN 55022:2006 • VCCI V-3:2007 • ICES-003:2004 • EN 61000-3-2:2000+A1:2001+A2:2005 • EN 61000-3-3:1995+A1:2001+A2:2005 • AS/NZS CISPR 22:2004 • FCC PART 15:2005 • GB 9254:1998 • GB/T 17618:1998
MTBF	• ≥ 40 years

Item		WCS7000
Maximum number of managed APs	Standard configuration	• 64
	Extended configuration	• 512 (by upgrading the license)
	Size of each license	• 32
Network interconnection	802.3 LAN protocols	• ARP (gratuitous ARP)
		• VLAN (port/MAC-based VLANs)
		• 802.1p
		• 802.1Q
		• 802.1X
		• 802.1D, 802.1w, 802.1s
	802.11 LAN protocols	• 802.11
		• 802.11b
		• 802.11a
		• 802.11g
		• 802.11d
		• 802.11h
		• 802.11i
		• 802.11e
		• 802.11n
	CAPWAP	• Layer 2/Layer 3 network topology between AP and AC
		• Automatic AC discovery by APs
		• AP software version upgrade through the AC
		• AP configuration file download from the AC
		• IPv4/v6 networks supported between AP and AC
	Roaming	• Intra-AC roaming
		• Inter-AC roaming
		• Key cache fast roaming
	IP application	• Ping, tracert
		• DHCP server
		• BOOTP/DHCP client
		• DHCP relay
		• DHCP snooping
		• DNS client
		• NTP
		• Telnet

		• TFTP client
		• FTP client
		• FTP server
	IP routing	• Static routing
	Multicasting	• IGMP snooping
		• MLD snooping
	IPv6	• TCPv6, UDPv6, ICMPv6
		• Pingv6, tracertv6
		• Telnetv6
		• DNSv6
		• IPv6 ND
		• IPv6 PMTU
		• IPv6 ACL
		• IPv6 static routing
Network security	Security authentication	• MAC address authentication
		• 802.1X authentication (EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, and EAP-MD5, where EAP-TLS, EAP-PEAP, and EAP-MD5 are supported by local authentication)
		• Portal authentication
		• PPPoE authentication
	AAA	• RADIUS client
		• HWTACACS
		• Multi-domain configuration on the authentication server
		• Backup authentication server
		• ESS based authentication server selection
		• SSID to user account number binding
		• Local authentication
	802.11 security and privacy	• Multi-SSID support
		• SSID hiding
		• 802.11i (with 802.1X and PSK authentication)
		• WPA, WPA2
		• WEP (WEP64/WEP128)
		• TKIP
		• CCMP

	Encryption	• DES, 3DES, AES • TLS, SSL
	WIDS/WIPS	• Whitelist
		• Static/dynamic blacklist
		• Detection of and countermeasures against rogue wireless devices
		• Wireless attack prevention
	Others	• SSH V1.5/2.0
Forwarding		• Split MAC (Centralized forwarding modes)
		• Local MAC (Local forwarding modes)
		• AP based bandwidth/rate limit
		• Isolation of users with the same SSID
User Management		• User-based bandwidth limit
		• User-based access control
		• User-based QoS
RF Management		• Country code configuration
		• Manual transmit power configuration
		• Auto transmit power configuration
		• Manual operating channel configuration
		• Auto operating channel configuration
		• Auto transmit rate adjustment
		• Coverage hole correction
		• Traffic and user number based AP load sharing
		• Wireless RF interference detection and mitigation
Reliability		• Dual power supplies
		• 300 ms failover between ACs
		• Multiple AC redundancy modes (1+1, N+1, N+N)
QoS		• Layer 2 to Layer 4 packet filtering and traffic classification
		• User-based and SSID-based rate limit, with granularity of 64 kbps
		• WMM (802.11e)
		• Mapping between wired priority and wireless priority
		• Mapping between wireless user priority and CAPWAP tunnel priority
Maintenance	Network Management	• SNMPv1/v2/v3
		• Web management

		• Syslog
	User Access Management	• Login from the console port
		• Login through Telnet
		• Login through SSH
		• Login through HTTP, HTTPS
		• Upload through FTP
Performance	Switching capacity	• 8Gbps
	Number of VLANs	• 4000
	Number of ACLs	• 8000
	Number of wireless users	• 5000
	MAC address table	• 64000
	Jumbo frame size	• 4000
	ARP table	• 8000
	Roaming switchover time	• Less than 50 ms

Ordering Information

Ordering List

Part Number	Model Description	Remarks
02050168	DPtech WCS7000 4GE SFP+4GE Copper, Dual AC Power Supply (64 AP Lic, Support to up 512 AP Lic)	Required
53010378	DPtech WC7000 Upgrade License for an Additional Support of 32 Access Points	Optional
02050169	DPtech WAP902n Dual-Radio (3x3MIMO) 11a/b/g/n Access Point	Required