EAC660
SMB Smart Wireless Access Controller

Product Overview

The EAC660 is a smart access controller (AC) developed by Yunke China Information Technology Limited (hereinafter referred to as DCN) for SMB wireless networks and large enterprise branches. It can combine with DCN smart EAP series wireless access points (APs) to form a centrally managed wireless LAN (WLAN) solution.

The EAC660 supports 4*GbE Combo (SFP/RJ45), 12*1000M SFP ports and 4*10GbE SFP+ ports for uplink. It can manage up to 260 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.

A rich service array coupled with considerable cost efficiency positions the EAC660 as a wireless AC preferred for SMB networks as well as large enterprise branches.

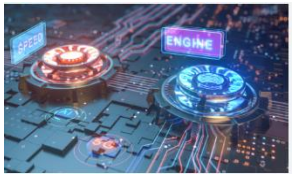
Manage APs 260

Friendly WEB GUI

Concurrent users 16K+

SMB Network

Switch + access controller



AC N+M redundancy

Key Features and Highlights

High-Performance and High-Reliability Wireless Network

More flexible data forwarding

The EAC660 may be deployed on a Layer 2 (L2) or Layer 3 (L3) network without changing existing network architecture. The local forwarding technology enables delay-sensitive data with high real-time transmission requirements to be forwarded through the wired network.

Automatic emergency mechanism of APs

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 helps wireless users to be always online.

Wireless Network of Intelligent Control and Automatic Perception

Intelligent RF management

The EAC660 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 with 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.

Intelligent control of terminals based on airtime fair

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 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's performance.

Easy-to-Manage Wireless Network

AP plug-and-play

When used with the EAC660, 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.

Product Specifications

Hardware Specifications

Item	EAC660
Service port	4*GbE Combo (SFP/RJ45) + 8*1000M SFP + 4*10GbE SFP+
Management port	One console port (RJ-45), one USB 2.0, one 10/100/1000M Base-T out-of-band port management port
Power supply	AC 100 V to 240 V, 50 Hz to 60 Hz, RPS:11V-13V
Maximum power consumption	30W
Working/Storage temperature	0℃ to +50℃
Working/Storage RH	5% to 90% (non-condensing)
Dimensions (W x D x H) (mm)	330 x 230 x 44

Software Specifications

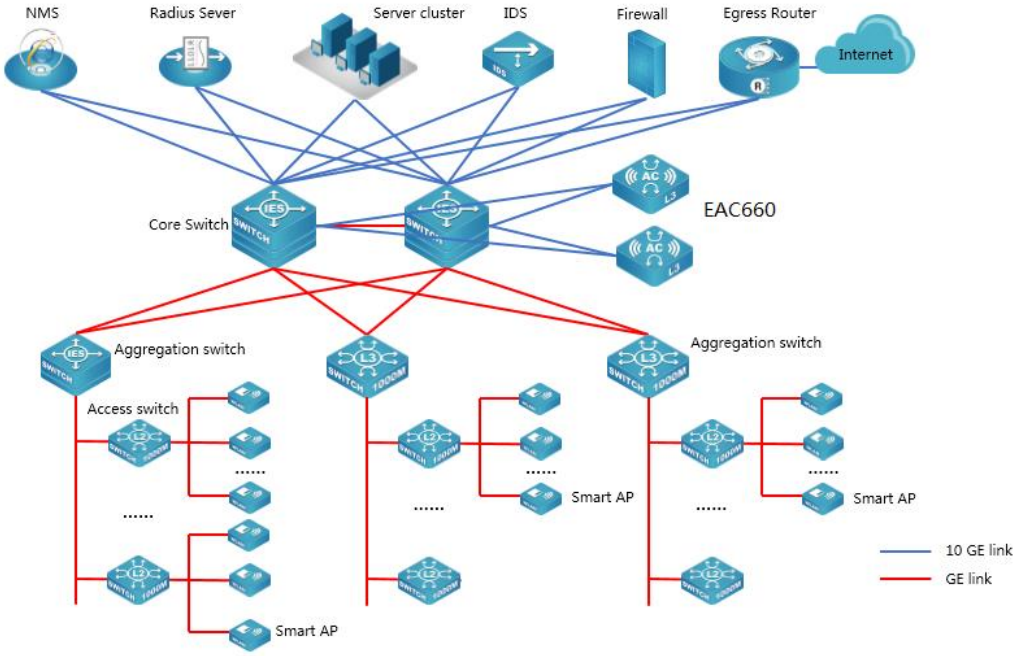
Item	EAC660
The base number of manageable APs	260
Maximum number of manageable APs	260
Maximum number of concurrent wireless users	5k
VLANs	4K
ARP table	8K
Switching time during roaming	< 30 ms
L2 protocols and standards	IEEE802.3 (10Base-T), IEEE802.3u (100Base-TX), IEEE802.3ab (1000Base-T), IEEE802.1Q (VLAN), IEEE802.1p (COS), IEEE802.1x (Port Control) IGMP Snooping, MLD Snooping GVRP, PVLAN
L3 protocols and standards	Static Routing RIPv1/v2, OSPF, 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.
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
	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
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 roaming between APs served by the same AC
	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

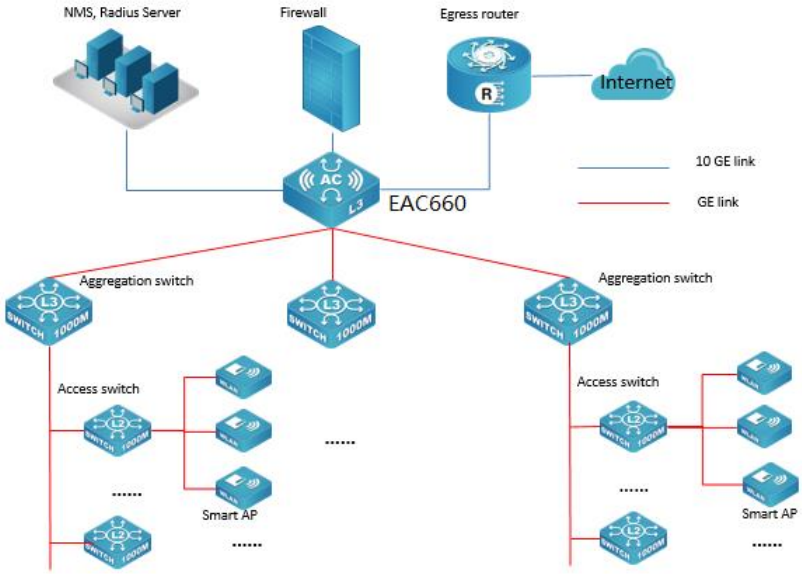
Typical Applications

Bypass Deployment Scenario



Trunk Deployment Scenario

Here the EAC660 is used as both the core switch and access controller.



Tel: +86-10-82707033 Fax: +86-10-82705112
Email: dcnsales@digitalchina.com, sales@dcnglobal.com Website://www.dcnglobal.com

Order Information

Product	Description
EAC660	DCN SMB Intelligent Access Controller (default with 260 units AP license, support controlling max. 260 AP), 4*GbE Combo (SFP/RJ45) + 8*1000M SFP ports+4*10GbE SFP+ ports, could manage EAP series access point