

EAC660 智能无线控制器

企业级无线产品系列



产品型号：EAC660

产品概述

EAC660 无线控制器(AC, Access Controller)是神州数码网络(简称 DCN)自主研发的智能无线控制器，专为中小型无线网络环境和大型企业分支机构设计，配合 DCN 智能无线 AP，组成集中管理的无线局域网(WLAN)解决方案。

EAC660 支持 4 个千兆 Combo 端口，8 个千兆光口，4 个万兆光口，最多可管理 500 台智能无线 AP，集精细的用户控制管理、完善的 RF 管理及安全机制、超强的 QoS、真正的无缝漫游，与现有网络融合一体的认证机制等多功能于一体，提供强大的 WLAN 接入控制功能。基于集群智能管理技术，对每个 AP 的射频环境进行实时监测、管控，从而实现 AP 功率，信道的自动调节以及基于用户数或流量的负载均衡策略，最大程度减少对无线信号的干扰，使无线网络的负载能力均衡、稳定。

凭借丰富多样的业务支持，以及较高的性价比，EAC660 是中小型无线网络和大型企业分支机构等应用环境理想的无线控制器。

产品特点

高性能高可靠的无线网络

- 更灵活的数据转发方式

EAC660 可部署于二层或三层网络中，且无需改动原有网络架构。通过本地转发技术，突破了无线控制器的流量瓶颈限制。本地转发技术将延迟敏感、传输要求实时性高的数据通过有线网络转发，在 802.11n 的大流量吞吐下，可以大大缓解无线控制器的流量压力，更好地适应未来无线网络更高流量传输的要求，诸如高清视频点播、VoWLAN 传输等。

- 支持 AP 自动逃生机制



对于“瘦 AP+无线控制器”的集中式网络体系架构，当无线控制器发生故障宕机后，AP 无法正常工作，导致整个无线网络瘫痪。DCN 无线 AP 支持自动逃生机制，使 AP 能够智能的进行链路感知，当发现无线控制器故障宕机后，AP 快速切换工作模式，继续进行数据转发，同时可以支持新的用户接入，实现了无线网络的高可用性，真正做到了无线用户永不掉线。

● 支持双 OS 的备份机制

EAC660 支持双 OS 的备份机制，在主用 OS 启动失败时可以立即采用备份 OS 启动和运行，提高了设备在恶劣环境下长期运行的可靠性。

智能控制和自动感知的无线网络

● 智能射频管理

EAC660 提供自动功率和信道调整功能。通过专有的射频检测和 RF 管理算法，优化射频覆盖效果。当 AP 信号收到外界强信号干扰时，通过控制 AP 自动切换到合适的工作信道以规避干扰，以保障无线网络通信的畅通；支持无线网络黑洞补偿功能，当网络中有 AP 意外停止工作时，通过 AC 的射频管理功能可补偿由此带来的信号盲点区域，使无线网络仍可正常工作。

● 终端时分公平智能控制

无线网络中由于部分 802.11b、802.11g 老旧终端协商速率低或者终端离 AP 较远协商速率低，导致大量用户无线上网延时大、速度慢、AP 整机性能低下。简单地采用速率控制和流量整形，无法解决低速率终端接入环境下的 AP 性能问题。DCN 智能无线 AP 通过基于终端空时公平的智能控制，根本性的解决了这个问题，保证用户无论使用何种类型的终端，都将在相同的位置上获得同样良好的无线上网体验。

通过基于终端时分公平的智能控制，网络性能无论是对客户端还是对整个网络都极大地提高了。所有高数据传输率客户端的性能都有极大提升，而低速率客户端几乎没有受到负面影响。在开放的无线网络中，性能提升的效果甚至会更明显。一旦高速客户端完成传输，在无线网络中正在传输的客户端数量就更少，因此竞争和重试就会减少，从而大幅度提升了 AP 整机性能。

● 智能负载均衡机制

一般情况下，无线客户端会根据 AP 信号强度选择接入 AP，这种无控制情况下的接入方式容易导致大量客户端仅因为某个 AP 信号较强而集中连接到同一个 AP 上。而同一台 AP 接入客户端越多，每个客户端分享到的带宽就越窄，从而大大影响客户的使用感受。DCN 无线产品可实现灵活多样的智能负载均衡：

- 支持基于流量的 AP 负载均衡；
- 支持基于用户数的 AP 负载均衡；
- 支持基于频段的 AP 负载均衡；
- 支持基于终端信号强度的接入控制；
- 支持基于用户数的 CAC (Call Admission Control)，保证高优先级应用的终端接入和带宽保证；
- 支持对终端的强制漫游控制，引导终端连接到信号更强的 AP。

● 智能终端识别

配合 DCN 智能无线 AP 和统一认证平台，可以智能识别终端尺寸，系统和类型，全面支持苹果 iOS、安卓和 windows 等主流智能终端操作系统。智能识别终端尺寸，自适应弹出不同大小、页面格局的 Portal 认证页面，免去了用户多次拖动，调整屏幕的操作，让用户感受到更加智能的无线体验。智能识别终端系统，在统一认证平台上看到终端的系统类型，例如



windows、MAC OS，Android，细节处体现智能。智能识别终端类型，例如手机，平板或 PC 机，依据不同终端类别进行动态策略控制，用户控制更加智能和精细化。

- **全网无缝漫游**

EAC660 支持先进的无线控制器集群技术，在多台 EAC660 之间可实时同步所有用户在线连接信息和漫游记录。不仅可实现单无线控制器内的 L2/L3 无缝漫游，更可完美实现跨无线控制器的快速漫游。漫游过程中不改变客户端 IP 信息，无需重新认证，可充分满足实时移动类业务不间断。

安全可控的无线网络

- **支持用户隔离策略**

EAC660 支持无线用户之间的隔离。当启用了此功能后，两个无线客户端之间无法直接通讯，无线客户端只能访问上游的有线网络，实现了更安全的无线网络应用。

- **支持无线入侵检测和入侵防御**

EAC660 支持非法无线设备检测、入侵检测以及黑名单和白名单等无线入侵检测和无线入侵防御特性，支持各种无线管理报文的防 DoS 攻击，增强了整个无线网络的安全管理。

- **提供精细的无线用户管理**

通过 EAC660 的管理，每台 AP 最多支持 32 个 WLAN，实现对无线用户的多层次多业务精细管理。每个 WLAN 可基于 MAC 地址和基于 IP 地址实现不同的接入控制权限，上下行速率限制，与 VLAN 的绑定，并可实现不同的认证计费策略。对于多个 WLAN 共存环境下，具有非常实际的使用价值。

- **用户安全准入**

EAC660 可为不同的应用环境提供了多种安全接入、认证计费机制：

- 支持 802.1X 认证；
- 支持 Captive Portal 认证，支持内置 Portal，外置 Portal，定制 Portal 等多种方式；
- 支持 MAC 地址认证；
- 支持 LDAP 认证；
- 支持 WAPI 加密和认证；
- 实现有线无线一体化统一认证计费。

- **支持用户无感知认证**

随着各种智能终端的普及应用，无线终端用户对认证机制的易用性和便捷性提出了更高的要求。结合 Portal 认证和 MAC 地址认证的机制，DCN 无线网络支持用户无感知认证：用户体验改善，首次用户需手动 Portal 认证，后续使用无感知认证（自动认证）；终端适配较好，适配大部分 WLAN 终端，无需适配客户端；认证兼容性较好，兼容现有 Portal 认证方式。

- **支持 AP 安全接入机制**

AP 一般部署在公共区域，需要有严格的安全机制确保接入设备的合法性。DCN 无线控制器和智能无线 AP 之间支持如下安全接入机制：

- 支持 AP MAC 地址认证机制；
- 支持 AP 密码口令认证机制；
- 支持 AP 和 AC 之间双向数字证书认证机制。



管理便捷的无线网络

- **AP 即插即用**

EAC660 智能无线控制器能够和现有的交换机、防火墙、认证服务器以及其他的网络架构无缝集成。DCN 智能无线 AP 能够自动发现 EAC660，AP 零配置即可启用无线网络。

在 EAC660 的配合下，DCN 智能无线 AP 可实现即插即用，AP 零配置，AP 设备的管理、控制、配置全部由无线控制器来完成，网管人员不必再对数量庞大的无线 AP 进行单独管理和维护，所有的配置、固件升级、安全策略更新等动作都可通过无线控制器统一下发完成。



产品规格

项目	参数规格
业务端口	4 个千兆 Combo 端口, 8 个千兆光口, 4 个万兆光口
管理端口	1 个 Console 口(RJ-45), 1 个千兆网管端口, 1 个 USB 2.0 端口
电源	交流 90V - 240V, 50-60Hz; RPS: 11V~13V DC
最大功耗	30W
工作/存储环境温度	0°C~50°C/-40°C~70°C
工作/存储环境湿度	5% ~90% 无凝露
尺寸 (长宽高)	330mm x 230mm x 43.6mm
基础可管理 AP 数(台)	20
最大可管理 AP 数(台)	500
AC 集群管理数(台)	64
AP 升级步长	20
最多无线并发用户数(个)	10k
VLAN	4K
ARP 表	8K
用户漫游切换时间	小于 30ms
二层协议规范	IEEE802.3(10Base-T)、IEEE802.3u(100Base-TX)、IEEE802.3ab(1000Base-T)、 IEEE802.1Q(VLAN)、IEEE802.1p(COS)、IEEE802.1x(Port Control) IGMP Snooping、GVRP, PVLAN
三层协议规范	Static Routing RIPv1/v2、OSPF、VRRP、IGMP v1/v2/v3 ARP、ARP Proxy PIM-SM、PIM-DM、PIM-SSM
无线协议规范	802.11, 802.11a, 802.11b, 802.11g, 802.11n, 802.11d, 802.11h, 802.11i, 802.11e, 802.11k
CAPWAP 协议	AP 和 AC 之间支持 L2/L3 层网络拓扑
	AP 可以自动发现可接入的 AC
	AP 可以自动从 AC 更新软件版本
	AP 可以自动从 AC 下载配置
射频管理	支持国家代码设置
	支持手动/自动设置发射功率
	支持手动/自动设置工作信道
	支持自动调整传输速率
	支持盲区探测与修复
	支持射频环境扫描, AP 边工作边扫描周围的射频环境信息
	支持无线射频干扰监测和规避
	支持 11n 优先 RF 策略
	支持隐藏 SSID 设置
	支持 20MHz 和 40MHz 信道带宽配置



	支持 11bg 和 11n 终端混合接入环境下的空口时间保护
	基于终端的空口时间公平调度
	终端定位，支持 AC 内置终端定位算法
	频谱导航（5G 优先）
	支持 11n only
	基于 SSID、Radio 的用户数限制
	用户在线检测
	用户无流量自动老化
	禁止弱信号客户端接入
	弱信号客户端强制漫游
安全特性	支持 64/128WEP、动态 WEP、TKIP、CCMP、SMS 加密方式
	支持 802.11i 安全认证，支持 802.1x 和 PSK 两种方式，即 Enterprise 和 Personal 方式
	支持 LDAP 认证
	支持 MAC 地址认证
	支持 Portal 认证，支持内置 Portal，外置 Portal，定制 Portal 三种方式
	支持用户无感知认证
	支持帧过滤，白名单，静态黑名单，动态黑名单等转发安全控制
	支持用户隔离
	Radio、SSID 的定时开启和关闭控制
	Free Resource 访问控制
	支持无线终端安全准入控制
	支持 MAC，IPv4，等各种数据类型报文的 ACL 访问控制
	支持 AP 和 AC 之间的 mac 认证，password 认证，数字证书认证等 AP 设备安全接入方式
	支持 radius Client
	支持备份认证服务器
	基于 AP 位置的用户接入控制
	支持 WIDS/WIPS（无线入侵检测和无线入侵防护）
	防无线泛洪攻击(Flooding Attack)
	防仿冒攻击(Spoof Attack)
转发特性	支持同一 AC 内,不同 AP 下二、三层快速漫游；
	支持不同 AC 间,不同 AP 下二、三层快速漫游；
	支持 IPv4，组播转发；
	支持 WDS AP；
服务特性	支持 802.11e（WMM）；支持 4 级优先级队列，保证语音、视频等实时效果敏感应用的优先传输
	支持以太网 802.1p 识别和标记
	支持无线优先级到有线优先级的映射
	支持不同 SSID/VLAN 映射不同的 QOS 策略
	支持匹配不同报文字段的数据流映射不同的 QOS 策略
	支持 MAC，IPv4，各种类型报文的 ACL 访问控制
	支持基于用户数的负载均衡；
	支持基于用户流量的负载均衡；



	支持基于频段的负载均衡；
	支持基于用户数的 CAC (Call Admission Control) ；
	支持基于 AP 的带宽限制；
	支持基于 SSID 的带宽限制；
	支持基于终端的带宽限制；
	支持基于特定数据流的带宽限制；
	支持省电模式
	支持组播转单播机制
管理特性	支持 AP 自动逃生机制
	支持智能终端识别
	支持 WEB 管理
	支持 Console 口配置
	SNMP v1/v2c/v3
	维护方式，支持本地维护，远端维护
	日志功能，支持本地日志、Syslog、日志文件导出
	支持告警功能
	支持故障检测
	支持统计信息
	支持 Telnet 登录
	支持 SSH 登录
	支持设备的 Dual image 备份机制，即双 OS 备份
	支持硬件 Watchdog (看门狗) 监控功能
	支持 AC 的集群管理；支持集群内 AC 之间信息自动同步和配置自动推送或手工推送

