无

线

网

络

设

计

方

案

# 总体网络方案设计

## 网络系统设计原则

### 安全性

网络必须具有良好的安全防范措施和密码保护技术，灵活方便的权限设定和控制机制，使系统具有多种有效手段，防范各种形式对网络的非法入侵和内部攻击，以保证网络的实体安全、网络安全、系统安全和信息安全，有效地保障正常的业务活动和防止内部信息数据不被非法窃取、篡改或泄漏。因此系统应分别针对不同的应用和不同的网络通信环境，采取不同的措施，包括系统安全机制、数据存取的权限控制等。

### 先进性

系统设计既要采用先进的概念、技术和方法，又要注意结构、设备、工具的相对先进成熟，整个系统的生命周期应有比较长的时间，可以在信息技术不断发展的今天，在系统建成以后比较长的一段时间内能满足用户需求增长的需要；不但能反映当今的先进水平，而且具有发展潜力，能保证在未来若干年内占主导地位，保证网络建设的领先地位。 本方案的设计宗旨是“立足今日，着眼未来”，在保证技术成熟的前提下，充分先进技术，满足现有需求，充分考虑潜在扩充。从而最大限度保护用户投资。

### 开放性

采用开放的软硬件平台和数据库管理系统，遵循国际标准化组织提出的开放系统互联的标准，应用软件必须独立于软硬件平台，能集成任何第三方的应用，具有良好的可扩展性、可移植性和互操作性。

### 扩展性

系统必须具有良好的可扩充性，在系统结构、系统容量与技术方案等方面必须具有升级换代的可能，核心设备必须采用模块化的结构，符合网络的发展趋势并具有充分的扩展性。系统建设必须尽量保护现有的软、硬件资源，保证现有的计算机系统的使用，逐步过渡，有效保护用户投资。

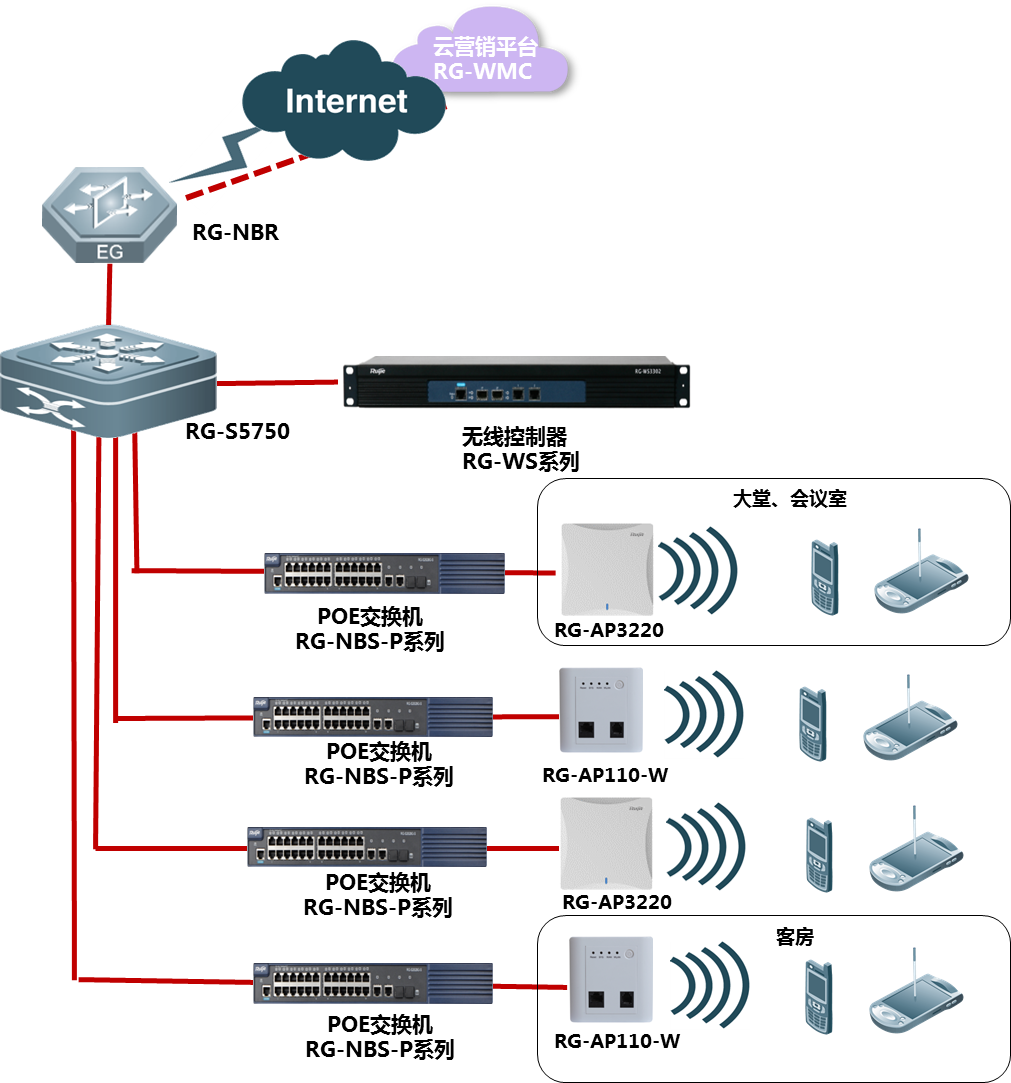
### 高性能

网络链路和设备具备足够高的数据转发能力，保证各种信息的高质量无阻塞传输；交换系统具有很高的交换容量与多服务支持的能力，保证网络服务的质量。

### 标准化

建立一个可靠、高效、灵活的计算机网络系统平台，不仅着重考虑数据信息能够讯速、准确、安全、可靠地交换，还要考虑同层次网络互连，远程分部的互联，以及与相关信息系统网际互联，以充分共享资源。这些需求体现在设计时，要求提供开放性好、标准化程度高的技术方案，设备的各种接口满足标准化原则。

## 方案拓扑



## 方案架构概述

方案分为核心机房与接入机房；对办公楼和住宿区实现有线无线网络的覆盖,并且通过不同的网络接入，区分办公内网及其它终端安全使用外网为设计原则。

* 接入机房：

核心机房采用高性能交换机作为核心数据汇聚及接入.楼层采用4台POE可网管交换机进行数据传输及对无线设备进行供电。

* 核心机房：

核心机房部署一台艾泰核心出口路由器。使用集中管理AP的控制器来管理所有的AP。

## 无线方案设计介绍

#### 稳定性

通过无线控制器，可以实现AP之间的负载均衡，保证在密集用户使用场景，AP不会因为过度的接入终端导致网络中断。

#### 安全性

强化的身份认证机制，保证无线网络安全,用户登录无线网需要管理员统一分配账号与密码，并根据不同用户部门、权限与级别，可分配不同的房屋权限，细致的权限划分技术，实现不同用户不同权限的资源访问

针对无线网络容易受攻击的现状，WAC-3100和无线接入点AP之间的数据都是在加密隧道中进行传输，保障数据安全。

#### 简化管理

传统的无线胖模式部署，需要对每台AP进行独立操作，管理维护复杂，工作量和难度大。方案中采用瘦模式部署，可以在AC上进行集中管理和维护，减少工作量和工作难度。

另外，传统网管人员采用命令行的方式对网络进行配置管理，命令难记，且容易打错。方案中AC支持命令行和web页面管理，让管理更灵活，更简单。

## 交换系统设计

#### 高性能

接入网交换机要保证所有端口的线速转发，至少要具有2个扩展插槽，支持百兆、千兆上联；要支持堆叠（采用专用堆叠模块和堆叠线缆闭环堆叠）和堆叠组跨设备链路聚合。支持802.1P、端口优先级、IP TOS、二到七层流过滤等QoS策略，具备MAC流、IP流、应用流等多层流分类和流控制能力，实现带宽控制、转发优先级等多种流策略。

#### 安全性

接入网交换机支持IEEE 802.1x，与认证系统结合，可严格实现用户身份识别，可根据用户账号、密码、MAC地址、IP地址、交换机IP、交换机端口号、用户所在VLAN的灵活组合，来识别用户身份。将网络中的虚拟用户和生活中的真实用户相对应，这样，当出现网络安全问题时，比如有人在网络上发表了非法言论，结合日志可以将安全事件到人，做到有据可查。特别是在认证通过后，接入网交换机可自动动态绑定用户MAC地址和IP地址，确保用户在通过身份认证后，无法私自篡改自己的MAC或IP地址，以便进行非法攻击或盗用网络资源等行为，保护 网络的安全性。要支持Option82功能，即可根据用户账号权限，由DHCP Server分配不同上网范围的IP地址，控制用户上校内、校外、国际网，实施不同的访问权限和收费策略，满足网络管理和运营需要。

同时支持接入级WEB认证，对于有些不能够安装IEEE802.1x客户端的用户终端可以采用基于网页的认证方式，不需要在用户终端安装任何应用程序甚至插件，只需凭借用户终端上的浏览器即可完成整个网络认证过程。在认证通过后，交换机会自动将通过认证的用户IP+MAC+端口对应的绑定规则下发到安全接入交换机内，对用户的报文做源地址检查和过滤，对于不符合绑定规则的报文直接在端口级拒绝转发，保证网络报文的真实有效。

接入网交换机要支持内在的多种安全机制，有效防止和控制病毒传播和网络流量攻击，控制非法用户使用 网资源，保证合法用户合理化使用 网资源，如端口安全、端口隔离、专家级ACL、时间ACL、端口ARP报文合法性检查、基于数据流的带宽限速、六元素绑定、嵌入式硬件过滤BT数据流技术等，满足 网加强对访问者进行控制、限制非授权用户通信的需求。

#### 防护性

核心交换机支持硬件方式提供多种安全防护能力，例如防DDOS攻击（Land攻击、非法TCP报文攻击等）、非法数据包检测、数据加密、防源IP地址欺骗等等，避免了传统软件实现方式对整机性能的影响。支持强大的ACL特性，提供IP标准、IP扩展、MAC扩展、时间、专家级等丰富的ACL技术，支持IPv4/IPv6双栈下的输入输出ACL。

核心交换机更是要支持实时检测CPU的使用状态，并提供硬件CPU保护技术（CPP，Control Plane Policy），CPP技术对发往CPU的数据进行流区分和流限速，避免非法攻击包对CPU的攻击和资源消耗。

易管理

接入网交换机要支持提供加密传输的SSH（Secure Shell），保证管理设备信息的安全性，防止黑客攻击和控制设备。支持SNMP V1/V2，可以通过SNMP远程对设备进行管理。

# 产品介绍

## 无线产品介绍

#### 无线网络集中管理

采用AC进行集中式管理，AC可部署于二层或三层网络中，且无需改动原有网络架构，与无线AP组成整体交换架构，方便控制和处理所有AP上的数据交换。

#### 智能终端识别

无线控制器内置Portal服务器，能根据终端特点，智能识别终端类型，自适应弹出不同大小、页面格局的Portal认证页面。终端智能识别技术免去了用户多次拖动，调整屏幕的操作，为用户提供更加智能的无线体验，并且全面支持苹果iOS、安卓和windows等主流智能终端操作系统。

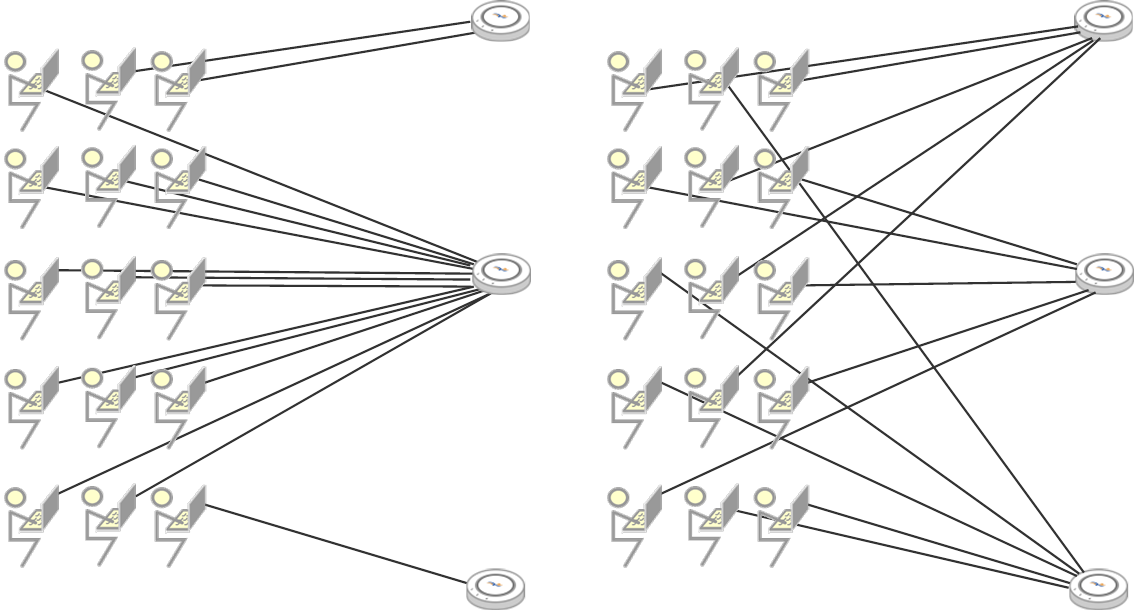


#### 终端公平访问

无线控制器协同锐捷无线接入点为802.11g、802.11n等不同类型的终端提供相同的访问时间，极大的解决了因终端无线网卡老旧或终端离AP较远而导致用户无线上网延时大、速度慢、AP整机性能低下的问题，有效的提升了低速终端的性能，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。

#### 基于用户、流量的智能负载均衡

在高密度无线用户的情况下，如会议室等，无线控制器智能实时的根据每个关联的AP上的用户数及数据流量调整分配到不同的AP上提供接入服务，平衡接入负载压力，提高用户的平均带宽和QoS，提高连接的高可用性。锐捷无线不仅能实现基于用户、流量的智能负载均衡，而且还能实现基于频段的负载均衡。大多数Wi-Fi设备缺省使用2.4GHz频段，而5GHz频段上（802.11a/n）却能获得更大的吞吐性能。基于频段的负载均衡，使支持双频的用户终端优先接入5GHz频段，在不增加成本的前提下，能够增加大约30-40%的带宽利用率，保证了用户的无线上网高速体验。



智能负载前 智能负载后

#### 智能射频管理

无线控制器可控制AP对无线网络进行按需射频扫描，可扫描无线频段与信道，识别非法AP和非法无线网络，并向管理员发出警报，以便对高安全性的环境提供全天候保护。同时，无线控制器可实时控制AP的射频扫描功能，进行信号强度和干扰的测量，并根据软件工具动态调整流量负载、功率、射频覆盖区域和信道分配，以使覆盖范围和容量最大化。

#### 产品性能列表

|  |  |
| --- | --- |
| **基本参数** | |
| **设备接口** | 4个10/100/1000Mbps以太网口  2个USB口  1个Console口  1个电源口 |
| **按键** | 1个RESET：重启/恢复出厂配置  1个LED： 控灯 |
| **管理AP数** | 默认固化64个AP |
| **最大AP数** | 最大管理128个AP |
| **用户接入数** | 4k |
| **物理层MAC层协议** | 802.1d、802.1s、802.1p、802.1q、802.1w、802.3、802.3ab、802.3u、802.3x、802.3z、ARPReverse ARP、multi-LAN ARP/Proxy ARP |
| **802.11协议** | 802.11n、802.11b、802.11a、802.11g、802.11d、802.11h、802.11i、802.11e |
| 功能参数 | |
| **系统参数** | VLAN数目：4K  ACL规则数目：1K  MAC表容量：4K  路由表容量：32K |
| **IP路由** | DHCP Server/Relay  NTP Server、FTP Server  IP静态路由  NAT/NPAT  NAT穿越 |
| **漫游** | 支持AC内二层、三层网络架构漫游能力 |
| **QoS** | 用户流量控，支持基于域的用户流量控制（以MAC、SSID作为配置域）  业务优先级，支持802.11e，对不同优先级的业务提供不同的服务 |
| **WLAN特性** | 自动信道选择  低质量用户过滤  用户数限制  无线终端识别  最大支持16个SSID  SSID隐藏  支持探针功能  定时关闭SSID功能  5G优先接入功能  11n用户优先接入功能 |
| **AAA** | RADIUS Client  支持认证服务器多域配置  支持认证/记费服务器主备连  支持认证和计费服务器分离 |
| **认证计费** | 支持PPPoE认证  支持Portal认证  支持AAA计费 |
| **网络安全** | 开放系统  支持WPA-Personal/Enterprise  支持WPA2-Personal/Enterprise  支持WEP 64/128-bit Encryption  用户业务隔离  支持静态/动态黑白名单 |
| **网络管理** | 支持基于WEB/SSH的本地关联  支持通过SNMP接入远程管理  支持SNMP v2/v3协议 |
| **AC冗余** | 基于负荷分担的1＋1备份 |
| 硬件参数 | |
| **尺寸** | 413×300×44 mm (1U) |
| **重量** | <4.5kg |
| **供电** | 功耗≤100W  供电：220V AC |
| **平均功耗** | 60W |
| **峰值功耗** | 100W |
| **温度** | 工作温度：0℃～45℃  存储温度：-40℃～70℃ |
| **湿度** | 工作湿度：5%～95% （非冷凝）  存储湿度：0%～95% （非冷凝） |

# 交换设备介绍

## 核心设备

交换机是基于网络安全和易用好管理的理念推出的新一代安全智能交换机，充分融合了网络发展需要的高性能、高安全、多业务、易用性特点，为用户提供全新的技术特性和解决方案。

交换机支持2层和3层线速交换，不但提供丰富的智能安全功能，同时提供丰富的三层功能，包括静态路由、动态路由、VRRP等技术，能够满足 网、企业网、政务网、业务网、宽带小区、商务楼宇等网络环境中作为服务器接入交换机，或中小型网络的核心交换机。在提供丰富的功能技术的同时， 同时提供WEB管理方式，能够大大降低设备的管理复杂度。

设备采用无风扇设计，大幅降低设备功耗，实现设备运行无噪音，减少机械故障点，同时免除凝露腐蚀和尘土侵害。

## 产品特征

#### 全方位立体安全防范

通过丰富的安全功能，消除安全威胁、攻击、病毒、ARP欺骗等侵害，还网络一片绿色，让用户更安心、省心上网；

业界领先的硬件CPU保护机制：特有的CPU保护策略（CPP技术），对发往CPU的数据流，进行流区分和优先级队列分级处理，并根据需要实施带宽限速，充分保护CPU不被非法流量占用、恶意攻击和资源消耗，保障了CPU安全，充分保护了交换机的安全；

硬件实现端口或交换机整机与用户IP地址和MAC地址的灵活绑定，严格限定端口上的用户接入或交换机整机上的用户接入问题；

支持DHCP snooping，可只允许信任端口的DHCP响应，防止私设DHCP Server的欺骗；并在DHCP监听的基础上，通过动态监测ARP和检查用户的IP，直接丢弃不符合绑定表项的非法报文，有效防范ARP欺骗和用户源IP地址的欺骗问题；

基于源IP地址控制的Telnet设备访问控制，避免非法人员和黑客恶意攻击和控制设备，增强了设备网管的安全性；

支持NFPP技术。NFPP (Network Foundation Protection Policy基础网络保护策略)是用来增强交换机安全的一种保护体系，通过对攻击源头采取隔离措施，可以使交换机的处理器和信道带宽资源得到保护，从而保证报文的正常转发以及协议状态的正常。

#### 易管理

灵活复用的多种千兆接口形式，可灵活满足需要多个千兆铜缆和多个千兆光纤链路的连接，方便用户灵活选择线缆；

网络时间协议保证交换机时间的准确性，并与网络中时间服务器时间统一化，方便日志信息和流量信息的分析、故障诊断等管理；

Syslog方便各种日志信息的统一收集、维护、分析、故障定位、备份，便于管理员网络维护和管理；

固化USB 2.0高速接口，便于通过USB接口保存日志；

CLI界面和WEB界面，方便高级用户配置和使用的同时也为普通用户提供简单人性化的界面进行配置和使用。

## 核心设备性能参数

|  |  |
| --- | --- |
| **主要参数** | [**产品类型 智能交换机**](http://detail.zol.com.cn/switches/p10858/) |
| [**应用层级 三层**](http://detail.zol.com.cn/switches/p11711/) |
| [**传输速率 10/100/1000Mbps**](http://detail.zol.com.cn/switches/p6808/) |
| **交换方式 存储-转发** |
| **背板带宽 256Gbps** |
| **包转发率 96Mpps** |
| **端口参数** | [**端口结构 非模块化**](http://detail.zol.com.cn/switches/p11716/) |
| **端口数量 32个** |
| **端口描述 24个10/100/1000M自适应电口，8个复用的SFP接口（SFP为千兆/百兆口）** |
| **控制端口 1个USB2.0接口** |
| **扩展模块 2个扩展槽** |
| **功能特性** | **网络协议 FTP，TFTP，DNS Client，DNS static** |
| **VLAN 支持4K个802.1Q VLAN** |
| **支持Super VLAN** |
| **支持Protocol VLAN** |
| **支持Private VLAN** |
| **支持Voice VLAN** |
| **支持基于MAC地址的VLAN** |
| **支持QinQ** |
| **QOS 支持端口流量识别** |
| **支持802.1p/DSCP/TOS流量分类** |
| **每端口4个优先级队列** |
| **支持优先级队列、轮询队列、优先级队列+轮询队列组合调度** |
| **支持流量整形** |
| **支持流量限速** |
| **支持层级QoS** |
| **支持输出qos** |
| **组播管理 支持IGMP v1，v2，v3，IGMP代理** |
| **支持IGMP v1，v2和v3 Snooping** |
| **支持IGMP过滤，IGMP快速离开** |
| **网络管理 SNMPv1/v2c/v3** |
| **CLI（Telnet/Console）** |
| **RMON（1，2，4，9）** |
| **SSH、Syslog、NTP/SNTP、SNMP over IPv6、IPv6 MIB support for SNMP 、SSHv6、Telnet v6、FTP/TFTP v6、DNS v6、NTP for v6、Traceroute v6** |
| **安全管理 支持IP、MAC、端口三元素绑定** |
| **支持IPv6、MAC、端口三元素绑定** |
| **支持安全通道** |
| **支持防网关欺骗** |
| **限制端口学习MAC地址数量** |
| **过滤非法的MAC地址** |
| **支持各种地址分配策略下的ARP-Check** |
| **支持DAI** |
| **支持防DHCP服务器私设** |
| **管理员分级管理和口令保护** |
| **设备登陆管理的AAA安全认证** |
| **支持IP源警告** |
| **支持控制平面保护** |
| **支持802.1x** |
| **支持各种地址分配策略下的ARP-Check** |
| **支持DoS保护** |
| **支持ARP报文限速** |
| **支持广播风暴抑制，多播风暴抑制** |
| **支持SSH v2.0** |
| **支持TACAS+，指定源IP** |
| **支持Radius（radius、EXEC授权、指定源IP）** |
| **支持BPDU Guard** |
| **支持NFPP技术** |
| **其它参数** | **电源电压 AC 90-264V，50-60Hz** |
| **电源功率 43W（不带扩展模块）** |
| **60W（带扩展模块）** |
| **产品尺寸 440×260×44mm** |
| **环境标准 工作温度：0-50℃** |
| **工作湿度：10%-90%RH** |
| **存储温度：-40-70℃** |
| **存储湿度：5%-90%RH** |
|  |  |

# POE交换机

POE交换机产品，是基于网络安全和易用好管理的理念推出的新一代安全智能交换机，充分融合了网络发展需要的高性能、高安全、多业务、易用性特点，为用户提供全新的技术特性和解决方案。

## POE产品介绍

#### 按需分配VLAN，网络更灵活

在办公网中，为了隔离不同部门之间的网络访问，避免部分PC中毒，影响全部的网络，常常需要根据部门、楼层等条件对内部网络进行VLAN划分，以此隔离广播域，提高网络的稳定性。RG-NBS系列交换机提供方便灵活的划分VLAN的方式，能够让您根据需要将端口划分到不同的VLAN中，不同VLAN中的用户互不干扰，为您创造一个更稳定的网络。

#### 网络安全隐患，自动隔离屏蔽

在基础网络中，常常会遇到PC中毒，自动对网络发起ARP欺骗、DOS攻击等行为，导致网络中其他PC无法访问网络，甚至是网络设备被攻击至瘫痪，而提供的NBS系列交换机，内部支持ARP防欺骗功能，防攻击功能，能够自动识别ARP欺骗报文，并进行隔离，避免了ARP等病毒对网络的影响，保障了网络的稳定。

在酒店中，经常遇到宾客自带家用无线路由器接入网络中，导致网络中存在非法DHCP服务器。提供的NBS系列交换机提供防非法DHCP服务器功能，对宾客自带的家庭无线路由器内置的DHCP服务器，自动进行屏蔽，不会出现其他宾客无法获取地址的情况。

#### Web管理，简单易用

在提供丰富功能的同时，提供的NBS系列交换机还致力于提供友好的配置界面，您能够在图形化界面中，运用鼠标，即可方便地实现以上的VLAN划分，地址绑定，安全防护等所有功能。的NBS系列交换机，旨在通过简单友好的操作界面，让您在基础网络上的投资能够发挥所有价值，物尽其用，物超所值。

#### 自动匹配连接设备的功耗

RG-NBS系列POE交换机支持802.3af和802.3at，最大可以为所连接的设备提供30W的供电。同时，如果所连接的设备功耗不足30W或15.4W，RG-NBS系列POE交换机将会和所连接的设备进行协商，自动匹配所连设备的功耗。

#### 丰富的POE保护功能，保障受电设备安全

RG-NBS系列POE交换机提供丰富的供电保护功能，保障受电设备安全。

短路保护：当线路发生短路时，RG-NBS系列POE交换机自动检测到线路上的电流超标，自动执行短路保护功能，停止对受电设备供电。

过载保护：当RG-NBS系列POE交换机检测到受电设备输出功率过大，超出可提供的最大功率时，自动执行过载保护，停止对受电设备供电。

过压保护：受电设备在开关机时，可能产生较高的瞬变电压，导致线缆上的电压过高而损坏POE交换机。RG-NBS系列POE交换机在每个端口上有过压保护电路，当瞬间电压过大时，端口输出电压被钳制在48V，从而保护POE交换机的安全。