科技开创蓝海 专业成就卓越

蓝海卓越

NE-80 系列

多功能出口网关

【产品概述】

NE-80 系列网关产品是蓝海卓越依托当前计算机领域内最为先进的数据包处理技术，开发出的高性能出口网关和流量分析引擎产品。

NE-80 采用 DPI 深层数据包和 DFI 深层数据流处理技术，对流经的数据报文进行最为精确的识别。整个系统主要由应用特征库、应用识别系统、应用管理系统、应用路由四大部份组成，并通过系统管理、网络管理、策略管理、监控统计、面板管理五大人机互动管理功能，对流经的所有应用数据进行实时监控与管理。多种部署方式可以适应各种复杂的网络环境，满足不同用户的组网需求；PPPOE、DHCP、免拨主机等多种上网方式可以为客户群体提供最合理的上网方式；智能 QOS 和策略路由等灵活的带宽管理方式,为用户调控网络带宽资源提供灵活、方便的手段；丰富的图表统计功能可以让管理员对用户的上网行为和各个应用的流量分布了如指掌；全中文化的 HTTPS 方式的 Web 界面可以让管理员可以随时随地安全的管理和配置系统；整个系统通过应用路由、应用分流、应用优先、DNS 管控、安全管理等功能实现各类网络尤其是复杂网络情况下的流量控制目标与网络安全保护。是 ISP 运营商、小区、企业、高校、酒店等上网场所网络管理员首选的出口网关产品！

【产品架构】

NE-80 系列网关产品是基于网桥架构而实现的路由及流量控制管理系统。系统架构主要由应用特征库、应用识别系统、应用管理系统、应用路由四大部分组成，并通过系统管理、网络管理、策略管理、监控统计、面板管理五大人机互动管理功能对流经的所有应用数据进行实时监控与管理。系统架构如右图：

【接入模式】

■ 路由(NAT) 模式

使用场景：

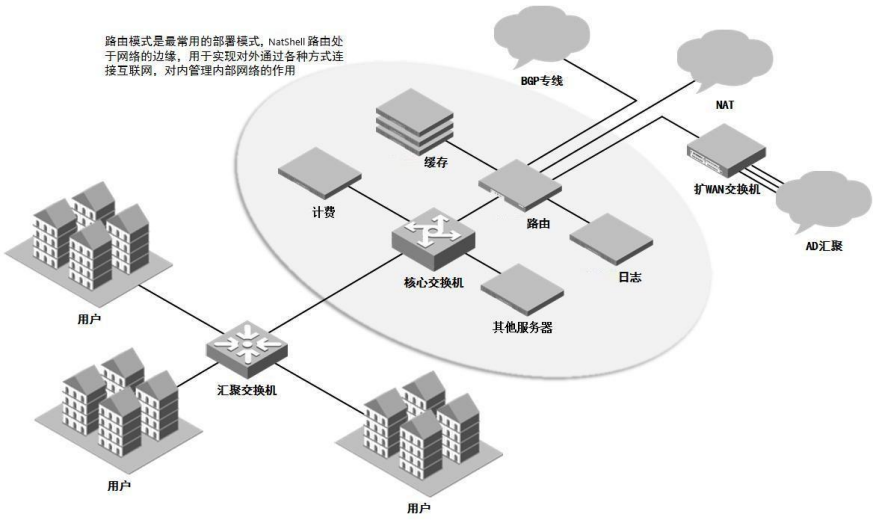
路由模式下的 NE-80 系列网关位于网络出口防火墙和核心交换机之间，其发挥的作用就是为下面的客户机提供上网功能和应用流量管理功能。这也是大部分项目所采用的接入模式。符合以下情况（包含一种或以上）的用户建议选择使用此模式：

1) 局域网内部网段间缺少路由设备互联；

2) 局域网内缺少统一拨号接入功能的设备；

3) 解决公用 IP 地址不足问题，提供 IP 地址复用功能；

4) 出于安全原因，需要将服务器（或者服务器群）做好隐藏和安全防御工作。



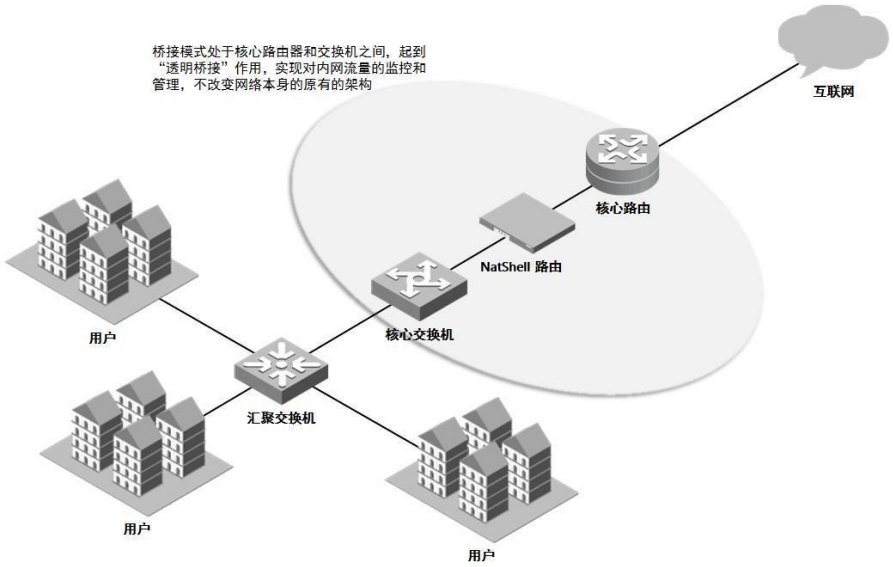
■ 网桥模式

网桥模式下的 NE-80 系列网关处于网络内部的位置是灵活多变的，其存在并不改变用户原有的网络架构，在下层的用户看来 NE-80 系列网关是“透明”的，其主要作用是实现对数据流量的监控、分流、过滤、分析等管理工作，此接口模式适合以下情况的用户使用：

1) 已有成熟的网络架构，但是缺少对用户和流量统一管理的设备；

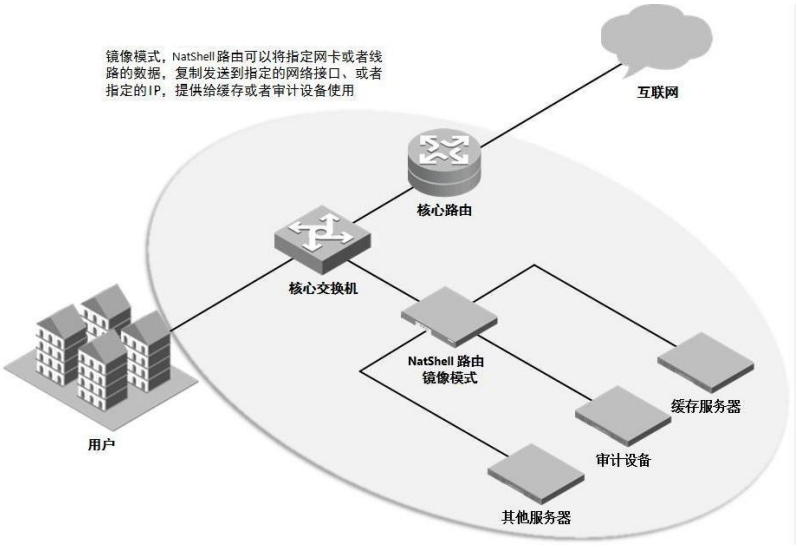
2) 想要对当前用户上网行为进行精确的监控和了解；

3) 想要对用户流量数据进行过滤、分析等工作。



■ 镜像模式

相比路由模式和网桥模式，镜像模式下的 NE-80 系列网关所扮演的角色是将流经路由的指定数据报文，通过镜像功能复制一份到指定目标设备，以供其进行数据监控或者安全分析，比如将 LAN 口下的用户上行请求中的 HTTP80 端口和 UDP17788 端口的数据镜像到 NatShell 缓存加速系统。镜像模式的部署依托于路由模式和网桥模式，在这两种模式下做数据镜像时应将相对应的物理接口的模式更改为镜像模式即可。



【主要特性】

- **精确的流量识别技术**

蓝海卓越 NE-80 高性能出口网关支持强大的七层协议识别引擎，不但可以识别各种明文的协议，如 BT、电驴下载，而且还可以识别经过加密的 P2P 协议，实用性超高。

- **高效的数据包处理技术**

不同于其他同类产品采用的传统的数据包处理技术，蓝海卓越 NE-80 高性能出口网关采用当前计算机领域内最先进的数据包处理技术，针对数据包可以实现最高效率的转发。

- **高可用性的操作系统**

蓝海卓越 NE-80 采用当前最新的 linux 内核及 DPDK 框架，并在此基础上开发出稳定、安全的路由专用 OS，为程序提供了稳定的运行平台。

- **灵活的接入方式**

蓝海卓越 NE-80 提供三种模式：路由模式、网桥模式、镜像模式。可适用多种不同的网络架构，满足不同用户的多种需求。

■ **灵活的带宽管理方式**

数据通道：定义带宽管理和调度方式。蓝海卓越 NE-80 同时提供基于应用或基于 IP 的带宽控制”、“带宽预留”、“带宽保证”三种机制，为用户灵活调控网络带宽资源提供更方便的功能。

流量策略：蓝海卓越 NE-80 支持将流量进行分类的机制，蓝海卓越高性能出口路由里定义的每一条策略可以包含源地址、目标地址、数据流向（上行/下行）、应用协议等因素。当匹配这些因素后，就会执行某个动作，如阻断、放行或将其注入某个数据通道。通过将符合这些条件的数据注入通道，实际上就已经对符合上述条件的数据包实施了流量管理。

■ **多链路负载均衡**

NE-80 的负载均衡机制能够提升应用系统的稳定性和可靠性，通过部署多条互联网链路来保证网络服务质量，消除单点故障，减少停机时间，更有效的实现链路负载，使网络运行更高效。基于出口时延、出口带宽、应用特性和应用协议等建立有效的负载均衡机制，可解决如下问题：

- 大量并发访问流量或数据流量将会被分担到多台设备上进行处理，进而减少用户等待响应的时间；
- 单个重负载的运算被分担到多台节点设备上做并行处理，每个节点设备处理结束后，将结果汇总返回给用户，系统处理能力得到大幅度提高。

多链路负载均衡特点：

- 最大支持 8000 条 WAN 线路，支持 ADSL 多线路捆绑
- 支持基于应用进行分流，国内应用识别率领先
- 支持基于域名进行分流，可实现关键域名加速
- 支持流量质量检测，实现实时业务性能分析

■ **双机热备**

由于路由设备的故障可能由各种原因引起，一般地讲，在技术人员在现场的情况下，恢复服务器正常可能需要至少 5 分钟、几小时甚至几天。从实际经验上看，除非是简单地重启服务器(可能隐患仍然存在),否则往

往需要几个小时以上。而对于运营网络来说，用户是很难忍受这样长时间的网络中断的。因此，就需要通过双机热备，来避免长时间的断网行为，保证网络安全、稳定、快速使用。

- **内网 IP 统计功能**

用户可在用户排名中查看当前在线用户流量的使用情况。支持在线时长、连接数、累计流出流量、累计流入流量、流出速率、流入速率等字段的排序。用户可以看到单个 IP 的应用流量、连接数，上行流量、下行流量、上行包数、下行包数。

- **BRAS 功能**

能连接 PPPoE 用户、汇聚用户流量，并且与认证计费系统、客户管理系统及策略控制系统相配 合实现用户接入的认证、计费和管理功能。实现网络的 IP 接入一体化，实现了宽带用户在业务、流量和管理的融合。

BRAS 功能支持场景：

- 入网人员身份认证
- 办公类哑终端
- 安防设备

- **多种认证方式支持**

PPPOE 服务器功能，最大单机支持 3 万用户

Portal 重定向，支持 CMCCPORTAl 协议认证

MAC 无感知认证支持

对接本地认证和 RADIUS 计费

对拉蓝海卓越认证计费平台及三方 RADIUS 系统

- **多运营商代拨支持**

- **代拨功能：**支持 PPPOE 代理拨号、支持 PORTAL 代拨拨号、支持一对一代拨、支持一对多代拨
- **AAA 转发：**支持接收从 AAA 下发转发参数后，对多家运营商同时实现 AAA 转发认证
- **性能强悍：**可支持 32000 个代拨账号，完全满足代拨场景。
- **一号一密、 一个账号多个终端：**用户只需记住用户密码即可；并且用户可以在不同终端(比如手机，PC 和 iPad)通过同一帐 号上网，同时支持不同运营商的拨号。

- **解决企业、高校和运营商账号不一致的问题：**比如高校场景：通过 NE-80 网关的代拨，在校内 BRAS 使用学校账号，而代拨后接入运营商 BRAS 时 候使用的是运营商 PPPoE 的账号信息，轻松解决学校和运营商账号不一致的问题。
- **流量可视化管理：**用户上网流量可视化，以直观的分析图形和报表展示网络运行的流量分布情况，业务应用、 网络状态一目了然。

■ **支持 AC 管理功能**

内置 AC 管理，可对 AP 进行管理

AP 自动发现，参数下发，固件统一升级

■ **防代理功能**

防代理检测功能能更好的控制内部私接的共享行为， 保企业、高校、小区、运营商的利益。

- 可协助运营商检测出同一个账号下有多少台电脑以及手机等终端设备共享上网；
- 能自动分析并获取用户登录账号，辨别出其中的非法共享行为；
- 能对非法共享行为用弹出警告、网页阻挡等引导方式；
- 基于综合多种检测方法，使用户无法逃避。

说明：本网关内置防代理功能，适用于小型场景，对于较大的网络场景或运营类场景，建议使用我司的专业防代理网关，以实现更强的防代理功能

■ **中英文化安全的 Web 管理**

在蓝海卓越 NE-80 中，所有的配置管理都是通过 HTTPS 方式的 Web 界面进行，管理员可以随时随地安全的管理和配置系统，不必担心数据信息的泄漏

产品界面支持中英文切换

支持自定义运营商 LOGO 和登录提示

■ **上网行为管理**

凭借业界领先的 DPI7 层应用识别技术，可获得每个用户、每个 IP、每个应用、每时每刻每个 Session 的管控能力。拥有 Web、微信、短信与 PPPoE 一体化认证技术，可对接业界主流 Radius 和 LDAP 服务。

通过智能 DNS 管控、HTTP 管控、二次实名认证、共享检测、终端发现、接入认证(802.1X 等)、行为审计、日志溯源等方式进行管理

- **上网行为管理功能**
  - **上网流量管控：**若存在带宽被滥用，网络拥堵，核心业务运行不畅等情况，对那些与企业工作无关且会消耗大量带宽的信息流，如 P2P 下载、网络视频、娱乐信息流、可疑数据流等进行必要的限制，减少其对网络资源的占用，合理法分配带宽资源，提高网络带宽利用率。
  - **上网行为审计：**上班时间关闭与工作无关应用，对网络中与工作无关的应用进行管控，人性化地提高员工的工作效率；管理记录终端用户的上网行为和轨迹，满足国家审计要求。
  - **信息管控：**对威胁情报进行识别并及时响应避免损失，若员工对外透露公司重要信息可通过日志泄密进行泄密追踪与取证规范员工行为。
  - **违规上网管控：**禁止上班时间访问非法、敏感网站，一旦发生网络违规违法事件可依据用户终端、上网行为进行追溯问责。
  - **终端接入管控：**识别终端类型并可视化展示，入网前检查终端安全性，并通过多种方式的接入认证和管理，阻止非法接入。
- **DNS 管控**

通过 DNS 重定向、丢弃等动作，能够快速恢复网络、日志告警、缓解 DNS 服务器压力、形成类 CDN 机制、域名封锁、保护服务器安全、镜像缓存、多运营商入口地址智能解析等效果。通过介入控制使用指定的 DNS 服务器去解析指定的域名地址。实现多线情况下有效的优化网内资源出口分布，合理利用资源，降低运营成本。

- **绿色节能的设计理念**

采用智能降频技术，灵活控制设备能耗，节约使用成本。

【硬件规格】

带机量	500 用户	2K 用户	3K 用户	5K 用户	10K 用户	20K 用户	30K 用户
处理器	双核 4 线程 1.8GHz 以上	四核 4 线程 2.0GHz 以上	四核 8 线程 2.2GHz 以上	四核 8 线程 2.2GHz 以上	12 核 24 线程 2.2GHz 以上	16 核 32 线程 3.0GHz 以上	20 核 40 线程 3.0GHz 以上
内存	≥4GB	≥8GB	≥16GB	≥16GB	≥16GB	≥32GB	≥64GB
硬盘	≥64GB	≥64GB	≥64GB	≥120GB	≥240GB	≥240GB	≥240GB
网口	6 个千兆	6 个千兆 2 个千兆 SFP	8 个千兆 2 个万兆 SFP+	8 个千兆 4 个万兆 SFP+	2 个千兆 8 个万兆 SFP+ 可扩展	2 个千兆 4 个万兆 SFP+ 2 个 40G 光 可扩展	2 个千兆 8 个万兆 SFP+ 4 个 40G 光 可扩展
尺寸（不含挂耳）	W252*D430*H45	W260*D430*H45	W400*D430*H45	W400*D435*H90	W460*D430*H45	W520*D430*H90	W520*D430*H90
重量	5KG	6KG	8KG	10KG	9KG	16KG	16KG
电源	AC220V	AC220V	AC220V	AC220V	AC220V 双冗余电源	AC220V 双冗余电源	AC220V 双冗余电源
电源功率	80W	150W	280W	400W	800W	800W	800W
产品示意							

【软件规格】

- 支持静态 IP、ADSL、DHCP 等多种接入方式
- 支持多 WAN 口、多 LAN 口
- 支持网卡链路聚合
- 支持桥模式下的应用分流
- 支持“一号多拨”（需要上级运营商支持）
- 支持外网线路定时重拨
- 支持外网线路最多三个 IP 地址的线路健康状态检测
- 支持 WAN、LAN 口的 VLAN 网络环境
- 支持 WAN、LAN 口的 QINQ 网络环境
- 支持多种线路群组负载（源 IP、源端口、目的 IP、目的端口、协议、TX、RX）
- 支持单线路对应多个线路群组
- 支持自定义协议（可以指定的 IP、端口、域名，是否通过 DNS 或 HOST 域检测）
- 支持自定义协议组（可以将多个协议自定义组名，方便策略调用）
- 支持策略路由、带宽叠加
- 支持按照时间分组来调度策略
- 支持高度智能化的一键流控
- 支持带宽通道的丢弃动作
- 支持多 LAN 口的 DHCP 服务
- 支持 DNS 管控（DNS 分流）
- 支持 DNS 重定向（将所有或者指定的 DNS 请求重定向到线路的 DNS）
- 支持端口映射（支持外网多个端口）
- 支持内网 LANtoLAN 映射
- 支持 DMZ 主机
- 支持指定数据报文镜像、牵引至指定 IP、端口

- 支持 DDNS 服务（花生壳、公云、每步）
- 支持 Flood 攻击防范
- 支持针对协议的连接数控制
- 支持针对 IP 的连接数控制
- 支持伪 IP 防护（可以指定合法的内网 IP）
- 支持 MAC 地址的黑名单、白名单
- 支持 URL、QQ、微信 ID、游戏的日志记录
- 支持消息推送（不会展示路由的地址）
- 支持 HTTP 管控（针对指定 URL 或 URL 群组重定向或者丢弃）
- 支持 DNS 代理，防止被运营商共享检测机制发现
- 支持 PPTP 客户端
- 支持 WEB 方式认证上网
- 支持多个 PPPOE 服务
- 支持不同 PPPOE 服务不同 VLAN
- 支持免拨号主机
- 支持 PPPOE 代理拨号（可以对接本地认证和 RADIUS 计费）
- 支持 Portal 二次认证，代理拨号（可以对接本地认证和 RADIUS 计费）
- PPPOE 服务器功能，最大单机支持 3 万用户
- Portal 重定向，支持 CMCCPORTAl 协议认证
- MAC 无感知认证支持
- 对接本地认证和 RADIUS 计费
- 对拉蓝海卓越认证计费平台及三方 RADIUS 系统
- 支持 AC 管理功能
- 支持 PPPOE 拨号账户批量创建和导入
- 支持本地认证、RADIUS 计费认证、先本地再 RADIUS 认证、免认证

- 支持 PORTAL 认证，本地 PORTAL 认证，第三方 PORTAL 认证
- 支持本地账户的 IP 和 MAC 地址绑定
- 支持本地账户的行为管控（不可登录、可登录不能上网、可登录可上网）
- 支持检测用户的代理私接行为，并对代理行为进行控制
- 支持账户到到期前、到期后提醒，可以自定义图片
- 支持拨号账户到期后指定 IP 或域名放行
- 支持外网线路、内网线路的 PING 工具
- 支持上网日志输出功能

【产品型号】

项目	描述	带机量
NE-80-1K	双核 4 线程 1.8GHz，4G 内存，64G 闪存 标配 1 个 CON，2 个 GE 光口，6 个 GE 电口，网络吞吐能力 4GB，支持 1000 用户并发上网	并发 1000 用户
NE-80-2K	四核 4 线程 2.0GHz，8G 内存，64G 闪存 标配 1 个 CON，2 个千兆 SFP+光口，6 个 GE 电口，网络吞吐能力 10GB，支持 2000 用户并发上网	并发 2000 用户
NE-80-3K	四核 8 线程 2.2GHz，16G 内存，64G 闪存 标配 1 个 CON，2 个千兆 SFP+光口，6 个 GE 电口，网络吞吐能力 10GB，支持 3000 用户并发上网	并发 3000 用户
NE-80-5K	10 核 20 线程，16G 内存，120G 闪存 标配 1 个 CON，4 个万兆 SFP+光口，2 个 GE 电口，网络吞吐能力 40GB，支持 5000 用户并发上网，可扩展光模块	并发 5000 用户
NE-80-10K	16 核 32 线程，32G 内存，120G 闪存 标配 1 个 CON，4 个万兆 SFP+光口，2 个 GE 电口，网络吞吐能力 40GB，支持 10000 用户并发上网，可扩展光模块	并发 10000 用户
NE-80-20K	20 核 40 线程，32G 内存，240G 闪存 标配 1 个 CON，8 个万兆 SFP+光口，2 个 GE 电口，网络吞吐能力 40GB，支持 20000 用户并发上网，可扩展光模块	并发 20000 用户
NE-80-30K	双 16 核 32 线程，64G 内存，240G 闪存 标配 1 个 CON，12 个万兆 SFP+光口，2 个 GE 电口，网络吞吐能力 120GB，支持 30000 用户并发上网	并发 30000 用户

【应用场景】

■ 宽带网络运营商

1) 告别普遍困扰各级 ISP 的两大难题：少数用户 P2P 滥用导致其他用户针对网速缓慢的频繁投诉、游戏用户对于网游速度得不到保证的频繁投诉；

2) 提升用户满意度：通过合理调控高峰期 P2P 类应用的带宽滥用，提升常规应用的网络体验，减少用户投诉，更加有利于市场竞争；

3) 提高带宽利用率：通过区分应用协议的精细化带宽管理，提升当前链路的用户承载能力，提高链路的收益能力；

4) 网络运营从此“可视”和“可控”：实时掌握网络运行状态，随时根据网络变化情况在最短时间内实施有效的技术应对策略；

5) 解决用户共享上网，即俗称的“一拖 N”检测问题：NatShell 路由基于应用协议的检测手段，能应对所有的共享、代理行为，精确度大大高于传统设备基于 IP、ID 的检测机制，为宽带运营商的合法收益提供技术保障。

■ 政府和企业网

1) 网络可视化管理能力提升：通过实时详尽的监控功能，掌控员工的网络应用情况，并具备行之有效的策略管理机制；

2) 规范员工网络应用，提升企业生产力：上班时间与工作无关的应用如开心农场、QQ、股票、土豆网、迅雷等通通不再是困扰企业管理者的问题；

3) 必要的安全防范机制：利用自身强大的性能优势，实时监控网络运行，识别阻断网络攻击，根据并发连接个数可以确定并阻断 DDOS 攻击等异常行为,为企业提供专门应对伪 IP 类木马攻击、IP 碎片攻击等检测和防护机制保护网络设备安全；

4) 优化网络运行管理：通过检测分析带宽使用状况，合理分配带宽资源；

5) 强化网络行为管理：根据各种应用业务的流量，制定相关策略限制非主流业务(例如可以对即时通讯、P2P 下载、网络游戏、网络电视等)在峰值时段进行限速、阻断，进一步规范员工上网行为，为人性化科学化管理提供基础保障；

6) 保障关键网络应用：根据企业需求保障关键应用(例如 ERP、CRM、视频会议等)，限制非主流业务占用过多的带宽，监测、阻断异常流量；

■ 高校及职校

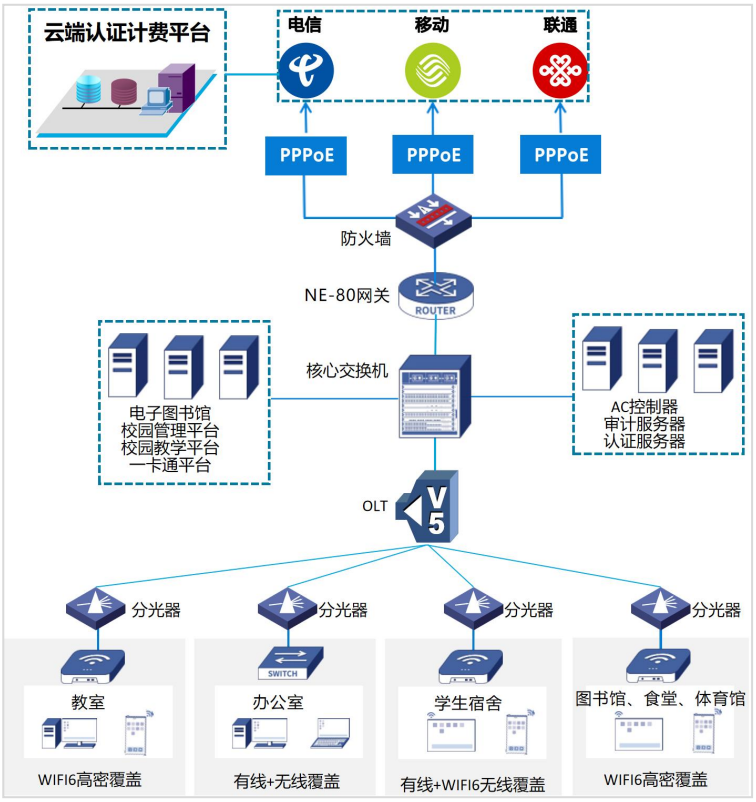
1) 网络可视化管理能力提升：通过实时详尽的统监控统计，掌控校园网的网络应用情况，并具备行之有效的策略管理机制；

2) 保障教学、科研、招生和远程教育等关键的网络应用，合理管控 P2P 类应用；

3) 提高学生宿舍使用校园网的管理水平；

4) 与运营商对接，实现 PORTAL 重定向认证，二次认证；

5) 多运营商接入分流，策略路由，运营商帐号二次认证。



■ 网吧

1) 评估与制定带宽方案：通过监控整个网络的应用情况，精确识别各类应用类型，确定主要应用与次要应用，评估带宽利用效率，掌控带宽资源的整体应用情况，明确流控目标是要增加带宽还是在现有基础上合理或是减少不必要的带宽支出成本。

2) 理解流控技术思路：根据评估结果，合理划分应用类型，合理分配带宽资源，确保主要应用的资源分配实时性，确保次要应用所占用资源的合理性与必要性，明确网吧用户的上网习惯和消费习惯，有针对性的制定符合本网吧特点的策略。

3) 调试策略施工成功：确保整个网络应用的掌控目标的技术实现，精细化设置与调整每条策略的运行情况，跟踪实际运行状况，改进策略，最终达成综合运营目标。

■ 酒店

1) 高峰期采取“通道和单 IP 限速结合的策略模式，既满足客人 P2P 下载应用的适度需要，也避免少数人的下载导致其他客人无法正常发送 e-mail 或浏览网页的商务需求；

2) 非高峰期采取针对应用协议做级别差异化的优先级调度策略模式，完美解决了有限的出口带宽下两类客户不同应用需求之间的矛盾，显著降低酒店关于网络的投诉率。