PPPoE、Web+Portal、802.1X常见三种认证方式对比分析案例

802.1X AAA Portal PPPoE 陈少华 2017-07-07 发表

PPPoE、Web+Portal、802.1X为常见三种认证方式，这三种方式使用找那个有哪些异同点呢？在此需要结合AAA初始步骤分析三种认证方式。
AAA（认证，授权，计费）的初始步骤，AAA一般包括用户终端、AAA Client、AAA Server和计费软件四个环节。用户终端与AAA Client之间的通信方式通常称为"认证方式"。目前的主要技术有以下三种：PPPoE、Web + Portal、802.1x。

三种方式有其产生的背景原因和技术特点，以下对这三种主要认证技术作一个简要的分析：
1. PPPoE
1998年后期问世的以太网上点对点协议（PPP over Ethernet）技术是由Redback 网络公司、客户端软件开发商RouterWare公司以及Worldcom子公司UUNET Technologies公司在IETF RFC制的基础上联合开发的。主要目的是把最经济的局域网技术、以太网和点对点协议的可扩展性及管理控制功能结合在一起。它使服务提供商在通过数字用户线、电缆调制解调器或无线连接等方式，提供支持多用户的宽带接入服务时更加简便易行。
通过PPPoE（Point-to-Point Protocol over Ethernet）协议，服务提供商可以在以太网上实现PPP协议的主要功能，包括采用各种灵活的方式管理用户。
PPPoE（Point-to-Point Protocol over Ethernet）协议允许通过一个连接客户的简单以太网桥启动一个PPP对话。
PPPoE的建立需要两个阶段，分别是搜寻阶段（Discovery stage）和点对点对话阶段（PPP Session stage）。当一台主机希望启动一个PPPoE对话，它首先必须完成搜寻阶段以确定对端的以太网MAC地址，并建立一个PPPoE的对话号（SESSION_ID）。
在PPP协议定义了一个端对端的关系时，搜寻阶段是一个客户-服务器的关系。在搜寻阶段的进程中，主机（客户端）搜寻并发现一个网络设备（服务器端）。在网络拓扑中，主机能与之通信的可能有不只一个网络设备。在搜寻阶段，主机可以发现所有的网络设备但只能选择一个。当搜索阶段顺利完成，主机和网络设备将拥有能够建立PPPoE的所有信息。
搜索阶段将在点对点对话建立之前一直存在。一旦点对点对话建立，主机和网络设备都必须为点对点对话阶段虚拟接口提供资源。
优点：
(1) 是传统PSTN窄带拨号接入技术在以太网接入技术的延伸
(2) 和原有窄带网络用户接入认证体系一致
(3) 最终用户相对比较容易接收
缺点：
(1) PPP协议和Ethernet技术本质上存在差异，PPP协议需要被再次封装到以太帧中，所以封装效率很低
(2) PPPoE在发现阶段会产生大量的广播流量，对网络性能产生很大的影响
(3) 组播业务开展困难，而视频业务大部分是基于组播的
(4) 需要运营商提供客户终端软件，维护工作量过大
(5) PPPoE认证一般需要外置BAS，认证完成后，业务数据流也必须经过BAS设备，容易造成单点瓶颈和故障，而且该设备通常非常昂贵。
2. Web+Portal
Portal认证的基本过程是：客户机首先通过DHCP协议获取到IP地址（也可以使用静态IP地址），但是客户使用获取到的IP地址并不能登上Internet，在认证通过前只能访问特定的IP地址，这个地址通常是PORTAL服务器的IP地址。采用Portal认证的接入设备必须具备这个能力。一般通过修改接入设备的访问控制表（ACL）可以做到。
用户登录到Portal Server后，可以浏览上面的内容，比如广告、新闻等免费信息，同时用户还可以在网页上输入用户名和密码，它们会被WEB客户端应用程序传给Portal Server，再由Portal Server与NAS之间交互来实现用户的认证。
Portal Server在获得用户的用户名和密码外，还会得到用户的IP地址，以它为索引来标识用户。然后Portal Server与NAS之间用Portal协议直接通信，而NAS又与RADIUS 服务器直接通信完成用户的认证和上线过程。因为安全问题，通常支持安全性较强的CHAP式认证。
优点：
(1) 不需要特殊的客户端软件，降低网络维护工作量
(2) 可以提供Portal等业务认证
缺点：
(1) WEB承载在7层协议上，对于设备的要求较高，建网成本高；
(2) 用户连接性差，不容易检测用户离线，基于时间的计费较难实现；
(3) 易用性不够好，用户在访问网络前，不管是 Telnet、FTP还是其它业务，必须使用浏览器进行Web认证；
(4) IP地址的分配在用户认证前，如果用户不是上网用户，则会造成地址的浪费，而且不便于多ISP的

支持。
(5) 认证前后业务流和数据流无法区分
3. 802.1X
优点：
(1) 802.1X协议为二层协议，不需要到达三层，而且接入层交换机无需支持802.1Q的VLAN，对设备的整体性能要求不高，可以有效降低建网成本。
(2) 通过组播实现，解决其他认证协议广播问题，对组播业务的支持性好。业务报文直接承载在正常的二层报文上；用户通过认证后，业务流和认证流实现分离，对后续的数据包处理没有特殊要求
缺点：
(1) 需要特定客户端软件
(2) 网络现有楼道交换机的问题：由于802.1X是比较新的二层协议，要求楼道交换机支持认证报文透传或完成认证过程，因此在全面采用该协议的过程中，存在对已经在网上的用户交换机的升级处理问题；
(3) IP地址分配和网络安全问题：802.1X协议是一个2层协议，只负责完成对用户端口的认证控制，对于完成端口认证后，用户进入三层IP网络后，需要继续解决用户IP地址分配、三层网络安全等问题，因此，单靠以太网交换机＋802.1X，无法全面解决城域网以太接入的可运营、可管理以及接入安全性等方面的问题；
(4) 计费问题：802.1X协议可以根据用户完成认证和离线间的时间进行时长计费，不能对流量进行统计，因此无法开展基于流量的计费或满足用户永远在线的要求。
三种认证技术比较:

认证方式	Web/Portal	PPPoE	802.1X
标准程度	厂家私有	RFC2516	IEEE标准
封装开销	小	较大	小
接入控制方式	设备端口	用户	用户
IP地址	认证前分配	认证后分配	认证后分配
多播支持	好	差	好
VLAN数目要求	多	无	无
支持多ISP	较差	好	好
客户端软件	不需要	需要	需要
设备支持	厂家私有	业界设备	业界设备
用户连接性	差	好	好
对设备的要求	高（全程VLAN）	较高（BAS）	低

综上所述，由于802.1X认证的突出优点就是实现简单、认证效率高、安全可靠。无需多业务网管设备，就能保证IP网络的无逢相连。同时消除了网络认证计费瓶颈的单点故障。在二层网络上实现用户认证，大大降低了整个网络的建网成本，目前基于802.1X的认证技术在校园网络应用非常普遍。