华为802.1X技术

白皮书

目录

1 概述.....1

2 802.1X 的基本原理.....1

2.1 体系结构.....1

2.1.1 端口 PAE.....2

2.1.2 受控端口.....2

2.1.3 受控方向.....2

2.2 工作机制.....2

2.3 认证流程.....3

3 华为 802.1X 的特点.....3

3.1 基于 MAC 的用户特征识别.....3

3.2 用户特征绑定.....4

3.3 认证触发方式.....4

3.3.1 标准 EAP 触发方式.....4

3.3.2 DHCP 触发方式.....4

3.3.3 华为专有触发方式.....4

3.4 TRUNK 端口认证.....4

3.5 用户业务下发.....5

3.5.1 VLAN 业务.....5

3.5.2 CAR 业务.....5

3.6 PROXY 检测.....5

3.6.1 Proxy 典型应用方式.....5

3.6.2 Proxy 检测机制.....5

3.6.3 Proxy 检测结果处理.....6

3.7 IP 地址管理.....6

3.7.1 IP 获取.....6

3.7.2 IP 释放.....6

3.7.3 IP 上传.....7

3.8 基于端口的用户容量限制.....7

3.9 支持多种认证方法.....7

3.9.1 PAP 方法.....7

3.9.2 CHAP 方法.....8

3.9.3 EAP 方法.....8

3.10 独特的握手机制.....8

3.11 对认证服务器的兼容.....8

3.11.1 EAP 终结方式.....8

3.11.2 EAP 中继方式.....9

3.12 内置认证服务器.....9

3.13 基于 802.1X 的受控组播.....9

3.14 完善的整体解决方案.....10

4 典型组网.....10

4.1 集中认证方案.....10
4.2 边缘分布认证方案.....10
4.3 内置服务器认证方案.....11
5 结论与展望.....11

摘要

802.1X 作为一种基于端口的用户访问控制安全机制，由于其低成本、良好的业务连续性和扩充性以及较高的安全性和灵活性，自从 2001 年 6 月正式成为 IEEE 802 系列标准开始，便迅速受到了包括华为在内的设备制造商、各大网络运营商和最终用户在内的广泛支持和肯定。

本文介绍了 802.1X 的基本概念和技术原理，以及华为公司 802.1X 解决方案的特点和组网情况。

关键词

802.1X 受控端口 RADIUS 客户端 设备端

缩略语

802.1X	本文指 IEEE 802.1X 标准
RADIUS	远程用户拨入认证服务（Remote Authentication Dial In User Service）
PAP	密码验证协议（Password Authentication Protocol）
CHAP	质询握手验证协议（Challenge Handshake Authentication Protocol）
EAP	扩展验证协议（Extensible Authentication Protocol）
MD5	消息摘要算法 5 版本（Message-Digest Algorithm 5）
PAE	端口认证实体（Port Authentication Entity）
CAR	承诺存取速率（Commit Access Rate）
AP	无线接入访问点（Access Point）

1 概述

802.1X，全称是 Port-Based Networks Access Control，即基于端口的网络访问控制。

802.1X 作为一种基于端口的用户访问控制机制，由于其低成本、良好的业务连续性和扩充性以及较高的安全性和灵活性，自从 2001 年 6 月正式成为 IEEE 802 系列标准开始，便迅速受到了包括华为在内的设备制造商、各大网络运营商和最终用户在内的广泛支持和肯定。

IEEE 802 协议定义的局域网不提供接入认证，一般来说，只要用户接入局域网就可以访问网络上的设备或资源。但是对于如电信接入、写字楼 局域网以及移动办公等应用场合，网络管理者希望能对用户设备的接入进行控制和配置，为此产生了基于端口或用户的网络接入控制需求。

目前 802.1X 技术在宽带城域网和园区网中获得了大量的应用。在现在竞争激烈的宽带网络建设中，基本业务类似的情况下，802.1X 及其扩展业务特性往往成为关键点。华为公司 VRP 平台的 802.1X 业务除兼容标准外，根据需要进行了多项扩充。

2 802.1X 的基本原理

2.1 体系结构

IEEE 802.1X的体系结构如图1 所示。802.1X系统共有三个实体：Supplicant（客户端），Authenticator System（设备端），Authentication Server System（认证服务器）。

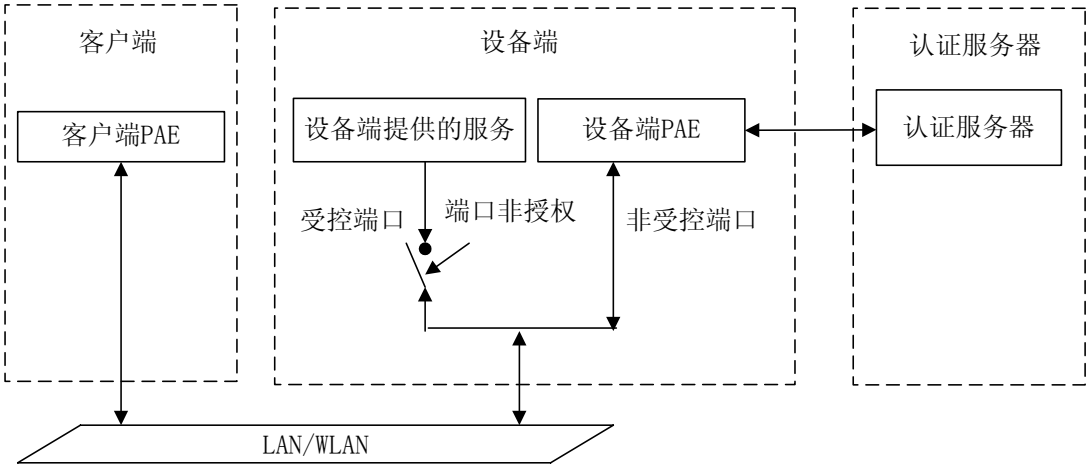

图1 IEEE 802.1X 认证系统体系结构

客户端是位于点对点局域网段一端的一个实体，由连接到该链接另一端的设备端对其进行认证。客户端一般为一个用户终端设备，用户通过启动客户端软件发起802.1X认证。客户端必须支持EAPOL协议。

设备端是位于点对点局域网段一端的一个实体，便于对连接到该链接另一端的实体进行认证。设备端通常为支持802.1X协议的网络设备，它为客户端提供接入局域网的端口，该端口可以是物理端口（如以太网交换机的一个以太网口或者AP的接入信道），也可以是逻辑端口（如用户的MAC地址、VLAN ID等）。

认证服务器是为设备端提供认证服务的实体。认证服务器用于实现用户的认证、授权和计费。本文中，认证服务器均以RADIUS服务器为例。

2.1.1 端口 PAE

端口PAE为802.1X系统中，一个给定的设备端口执行算法和协议操作的实体对象。

设备端PAE利用认证服务器对需要接入局域网的客户端执行认证，并根据认证结果相应地控制受控端口的授权/非授权状态。

客户端PAE负责响应设备端的认证请求，向设备端提交用户的认证信息。客户端PAE也可以主动向设备端发送认证请求和下线请求。

2.1.2 受控端口

设备端为客户端提供接入局域网的端口，这个端口被划分为两个虚端口：受控端口和非受控端口。非受控端口始终处于双向连通状态，用于传递EAP认证报文。受控端口在授权状态下处于连通状态，用于传递业务报文；受控端口在非授权状态下处于断开状态，禁止传递任何报文。受控端口和非受控端口是同一端口的两个部分；任何到达该端口的帧，在受控端口与非受控端口上均可见。如图2所示。

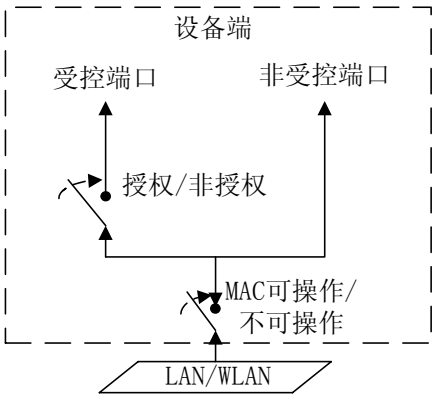

图2 非受控端口和受控端口

2.1.3 受控方向

在非授权状态下，受控端口可以被设置成单向受控和双向受控。实行双向受控时，禁止帧的发送和接收；实行单向受控时，禁止从客户端接收帧，但允许向客户端发送帧。

默认情况下，受控端口实行双向受控。

2.2 工作机制

IEEE 802.1X认证系统利用EAP协议，作为在客户端和认证服务器之间交换认证信息的手段。

在客户端PAE与设备端PAE之间，EAP协议报文使用EAPOL封装格式，直接承载于LAN环境中。

在设备端PAE与RADIUS服务器之间，EAP协议报文可以使用EAPOR封装格式（EAP over RADIUS），承载于RADIUS协议中；也可以由设备端PAE进行终结，而在设备端PAE与RADIUS服务器之间传送PAP协议报文或CHAP协议报文（参见IETF RFC 1994）。

设备端PAE和认证功能相分离,RADIUS服务器可以使用多种不同的认证机制对客户端PAE进行认证，包括MD5-challenge、TLS、PAP、智能卡、Kerberos、Public Key Encryption、One Time Passwords等等。在非共享网段的有线LAN中，一般实现MD5-challenge认证机制；在共享网段的有线LAN和WLAN中，通常实现双向认证。

设备端PAE根据RADIUS服务器的指示（Accept或Reject）决定受控端口的授权/非授权状态。

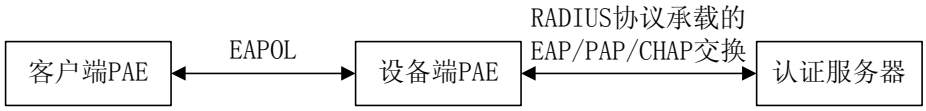

图3 IEEE 802.1X 认证系统的工作机制

2.3 认证流程

以设备端PAE对EAP报文进行中继转发为例，IEEE 802.1X认证系统的基本业务流程如图4所示。

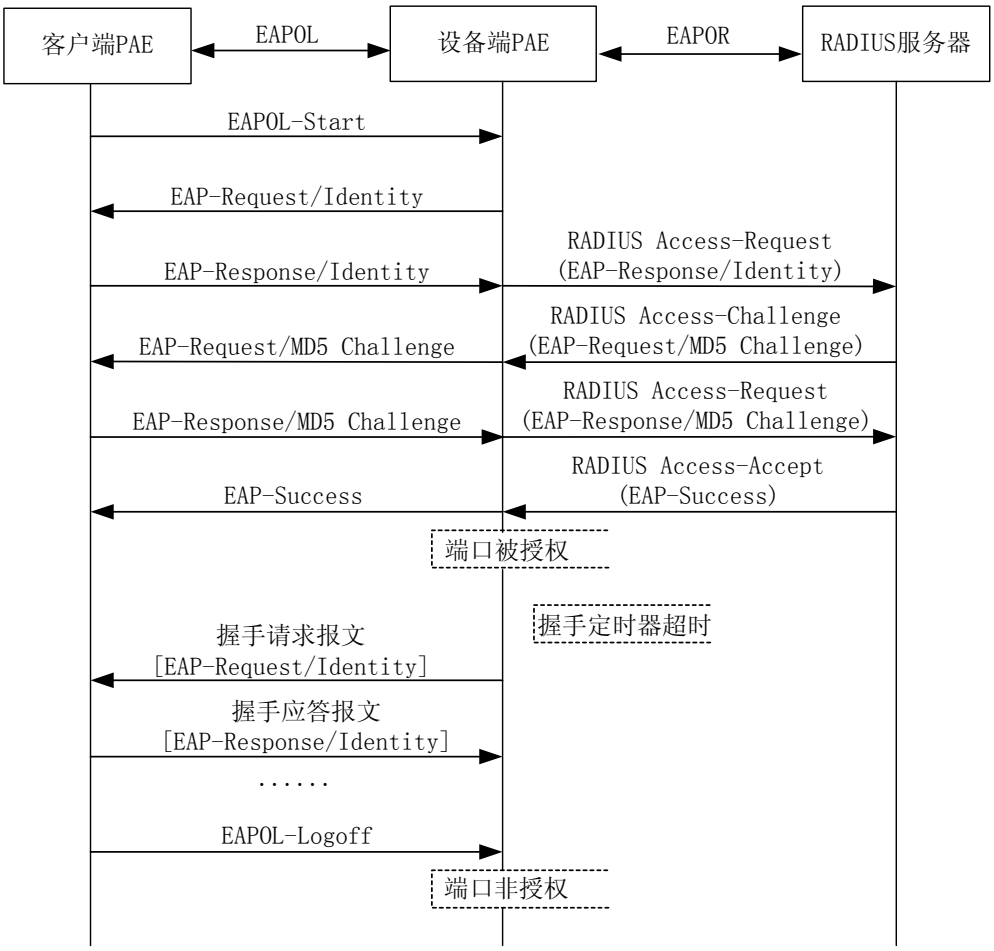

图4 IEEE 802.1X 认证系统的 EAP 方式业务流程

3 华为 802.1X 的特点

华为公司根据国内网络实际运营环境和特点，在符合标准的基础上，根据多项发明专利，有效地扩展了802.1X的业务支持能力和组网能力。

3.1 基于 MAC 的用户特征识别

IEEE 802.1X 的标准是一个基于端口的访问控制协议，其基本要求是对用户接入端口进行控制。这对无线接入访问点而言是足够的，因为一个用户占用一个信道。但在电信接入和酒店等环境中，以端口为对象的控制粒度难以满足要求，基于 MAC 地址逻辑端口控制势在必行。

华为 VRP 平台的 802.1X 特性不仅提供基于端口（Portbased）的用户访问控制，而且提

供基于用户 MAC 地址（Macbased）的访问控制。控制粒度为端口，组网非常灵活。

系统缺省为 Macbased 的控制方式。

3.2 用户特征绑定

无论是基于端口认证还是基于用户 MAC 地址的认证，服务器验证的都是用户帐号，即“用户名＋密码”。一旦帐号泄漏，会给用户带来很大的安全隐患。VRP 平台的 802.1X，可以与 CAMS（综合接入管理系统）等 RADIUS 服务器或者设备内置认证服务器配合，实现用户帐号和用户特征的多种绑定，从而增强用户安全性。

绑定方式可以是用户账号与 VLANID/MAC/PORT 的任意组合。例如：

1. 支持“用户账号＋VLANID”绑定
2. 支持“用户账号＋VLANID＋PORT”绑定
3. 支持“用户账号＋VLANID＋PORT＋MAC”绑定
4. 支持“用户账号＋VLANID＋PORT＋MAC＋IP”绑定

某些绑定方式，例如“用户账号＋IP”，需要华为扩展属性（VSA）支持。

3.3 认证触发方式

认证触发方式指用户通过何种报文来触发设备对用户进行认证。华为 802.1X 系统支持三种认证触发方式，即可标准 EAP、DHCP 和华为专有方式。

3.3.1 标准 EAP 触发方式

IEEE 802.1X 协议规定，可以通过 EAP-Start 报文触发认证。在以太网中，802.1X 认证 EAP 报文分配地址为“01-80-C2-00-00-03”。

这里有两种情况，其一是仅仅第一个 EAP-Start 报文采用这个多播地址，其他 EAP 报文采用单播地址。客户端和设备端分别采用对方报文的源地址作为向对方发送报文的目的地址。其二是整个认证过程报文都采用协议分配多播地址作为目的地址。

在有线 LAN 中一般采用前一种情况以减少广播；在 WLAN 中一般采用后一种方式。

华为客户端支持上述两种方式。

3.3.2 DHCP 触发方式

即采用 DHCP 报文作为触发设备对用户进行认证的条件。WIN XP 自带客户端即是这种情况。

3.3.3 华为专有触发方式

标准触发方式如上所述。但是有些通信设备不能透传上述多播报文，如果在用户和认证设备之间存在这类设备，就会阻断用户认证请求。

华为公司通过采用专利技术“广播触发认证方式”，成功的解决了上述问题，使用户可以通过这类设备到达认证服务器完成认证。这样就降低了对终端用户接入设备的要求，使已有设备在采用 802.1X 认证的网络中继续使用，给网络运营管理提供方便，从而降低运营商的总拥有成本。

3.4 Trunk 端口认证

802.1X 标准规定不支持 Trunk 端口认证。其原因是标准规定的认证控制对象是端口，对这种端口“复用”的情况，只要有一个 VLAN 中的用户认证通过，则复用该端口的其他所有 VLAN 中的用户也被相应授权，因此不能支持 Trunk 端口认证。

华为公司 802.1X 通过对控制粒度的细分和相关处理，可以支持在 Trunk 端口上进行认证（Macbased 方式）。此项功能扩展没有破坏标准的统一性，因为这是基于粒度细分添加的功能而不是减少了功能。另外，与其他厂商设备的对接也是没有问题的。

这一特性给组网带来三大优点：其一，非常有利于网络 VLAN 资源的规划利用。第二，有利于认证设备层次的集中。第三，通过“用户账号＋VLAN”的绑定提高用户安全性，同

时给运营商带来更大的可管理性。例如，对于大中型网络而言，VLAN 资源（最多 4K）是相对缺乏的，由于 Trunk 端口支持认证，就可以把 VLAN 终结和认证同时在汇聚层（或者核心层）设备完成。这样，通过给单个（或者少量）用户划分 VLAN 并绑定，对用户来说可以提高安全性；对运营商来说，可以防止用户在 VLAN 间漫游。

3.5 用户业务下发

目前支持的业务包括 VLAN 业务、CAR 业务和 Priority 业务等。

3.5.1 VLAN 业务

用户认证过程中，通过与 CAMS 等服务器配合，支持给用户重新指定 VLAN 并下发到设备。

在 LANSwitch 中，VLAN 与路由虚接口有映射关系，因此可以根据这一特性来规划某类用户的管理策略。例如，校园网中，给学生群体分配 VLAN 10，教师群体分配 VLAN 20 。通过分别给 VLAN 10 和 20 虚接口所在路由段指定不同的访问控制策略可增强可管理性。同时，由于 VLAN 资源是动态下发的，因此用户可以在园区网中漫游而不影响访问。

3.5.2 CAR 业务

CAR 业务即用户流量控制业务。目的是根据资费情况动态设定用户的上下行流量参数。

这一业务除了需要 CAMS 等服务器配合外，还需要设备本身支持流量控制功能。用户优先级 Priority 也是这样。

3.6 Proxy 检测

在宽带园区网环境中，特别是校园网中，用户通过Proxy上网来实现“一个账号多人使用”的方法较普遍，引起了运营商的强烈关注。这种通过Proxy来隐藏真实身份的方式使用网络，会产生两个方面的问题：一是利用Proxy发表反动言论，二是利用Proxy逃避计费。

3.6.1 Proxy 典型应用方式

Proxy的典型应用方式如图5。用户可以通过双网卡、NAT或者“单/双网卡＋代理软件（如Wingate）”等方式实现Proxy。

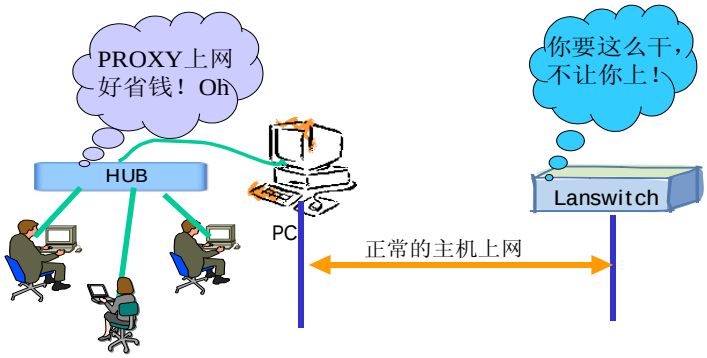

图5　通过 Proxy 上网方式

3.6.2 Proxy 检测机制

一般来说，Proxy功能运行在用户设备（如PC）中的软硬件完成。从原理上来说，网络侧设备可以通过两种方式探测用户是否通过Proxy上网：其一是网络侧设备发送某种探测报文；其二是通过驻留在用户设备中的软件主动上报。在本文中，采取两者结合的方式。

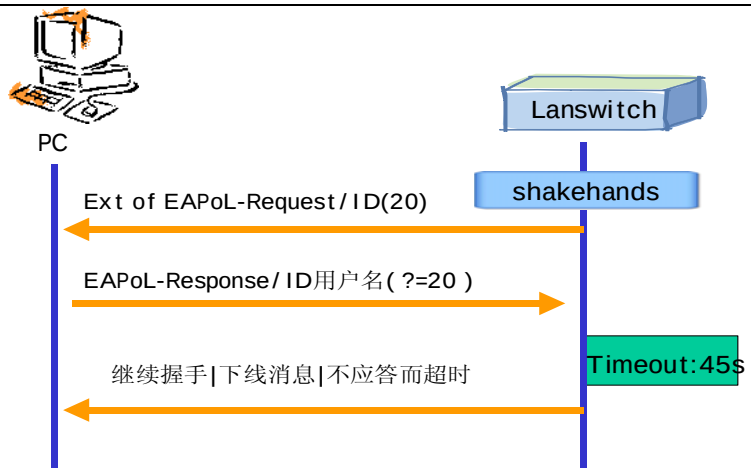

图6　Proxy 检测机制说明

1， 扩展客户端软件，使客户端软件可以进行Proxy识别；

2， 客户端软件的识别功能处于被动状态，由交换机按端口进行触发，802.1X客户端按标准流程进行，设备端收到触发报文后执行检测动作，不影响客户端效率；

3， 客户端将检测结果交由交换机或者AP处理；

3.6.3　Proxy 检测结果处理

根据客户端检测的结果，应答的结果有两种：通过Proxy上网或者正常上网。如果检测结果是正常方式上网，则设备继续与客户端握手；如果结果为Proxy上网，则根据设备端的配置给网管报送Trap信息或者发送下线消息Logoff把用户踢下线，拒绝用户上网。当然，这两种方式可以同时使用。

另外，如果应答报文的返回值是设备期望之外的其他值，则交换机拒绝接收这样的握手报文。设备会启动握手定时器（缺省45s）而使用户下线。这样就实现了对客户端Proxy的检测。

华为客户端与设备一起配合，实现对Proxy的检测，提高了网络的可运营性。

3.7　IP 地址管理

IP网络中，IP地址不仅是用户使用网络的依据，同时也是管理和安全控制的对象。华为802.1X系统IP地址管理机制包括如下方面，获取、释放和是否作为用户特征上传等。

3.7.1　IP 获取

华为客户端支持在用户认证过程中动态获得IP地址。这一过程可由客户端自动完成，不需要用户干预。

当然，如果网络采取静态分配IP地址的方式，客户端的相关选项不选中即可。

3.7.2　IP 释放

Microsoft公司的WINDOWS XP操作系统提供实现了基于IEEE 802.1X-2001协议的客户端软件，用于基于IEEE 802.1X-2001协议的用户接入。该客户端软件可以同时适用于有线和

无线（WLAN）领域。但该客户端软件在用户下线时不能提供用户IP地址的自动释放，用户下线后还一直占用着IP地址，造成了IP地址的浪费。在IP地址日益紧缺的今天，这个问题对于运营商和用户都是非常不利的。一方面会造成运营商所拥有的IP地址不能得到充分利用，另一方面也会因为分配不到地址或者地址冲突而使部分用户得不到服务。为解决这个问题。华为公司在其自主开发的802.1X客户端软件上增加了IP地址释放机制，用于保证用户下线后的IP地址得到及时的释放。在有线宽带网络中节约了IP地址，解决了IP地址很快耗光的问题，实现起来简单可靠，效率很高。

3.7.3 IP 上传

IP地址上传,这里指把用户的IP地址传给RADIUS服务器。分静态IP地址上传和动态IP地址上传两种情况。

对于静态分配IP地址的情况，可以把IP地址作为用户的一项特征属性与用户帐号一起送给服务器认证，实现“用户帐号＋IP”绑定认证。并在随后的计费（开始、更新和结束）报文包含该项属性，服务器的日志中记录信息可供管理查找。

对于动态分配IP地址的情况，则不能与用户帐号一起在认证报文中送给服务器，也不能进行“用户帐号＋IP”绑定认证。因为802.1X是二层认证协议，在认证通过之前，用户无法获得有效IP地址。华为802.1X系统可以在随后的计费更新报文和计费结束报文中把IP地址信息送给服务器。

3.8 基于端口的用户容量限制

设备根据其在网络中的层次和处理能力，有一个总体上的最大用户容量指标。802.1X是基于端口的控制协议。华为802.1X系统细化了控制粒度，可以设置指定端口的用户接入数，从而更好地进行管理控制。

3.9 支持多种认证方法

华为802.1X系统支持PAP、CHAP和EAP－MD5等多种认证方法。缺省设置是CHAP。

特点是客户端自动与设备自动适配，对终端用户透明。不需要用户设置，界面友好，使用简单方便。

3.9.1 PAP 方法

PAP即密码验证（Password Authentication Protocol）协议。其特点是密码通过明文的方式传输。

802.1X认证系统没有定义PAP认证方式，华为公司对此进行了扩展（提交国家标准）。通过扩展RFC 2284中的一种Type（等于0x07表示PAP）来提供PAP认证。

由于密码是通过明文的方式传输，相对来说，安全性不是很高。但是可以兼容某些传统

RADIUS服务器。

3.9.2 CHAP 方法

CHAP即质询握手验证（Challenge Handshake Authentication Protocol）协议。与PAP不同，其密码是通过密文方式传输。

华为802.1X系统CHAP认证遵循RFC1994。

3.9.3 EAP 方法

EAP即扩展验证（Extensible Authentication Protocol）协议，见RFC2284。即所谓的EAP中继认证方式。这种认证方法的好处是质询和计算过程交由服务器完成，从一定程度上减轻了设备的负担。

EAP认证可以由多种安全控制方法，例如MD5散列，TLS等。华为802.1X系统支持EAP MD5方式。

3.10 独特的握手机制

为了定期监测用户的在线情况，华为 802.1X 系统扩展并支持设备与客户之间的握手机制。这一办法有效地解决了有线网应用中的仿冒和时长计费准确性问题（其他厂商产品多数无法支持定期监测和基于时长计费）。

推荐的系统参数为：握手间隔（Interval）15 秒，握手次数（N）为 3 次。如果系统连续 N 次没有收到客户端的应答报文，则认为用户已经离线。

这一功能需要设备端和客户端共同支持。

3.11 对认证服务器的兼容

华为 802.1X 系统支持 EAP 终结方式和 EAP 中继方式。

3.11.1 EAP 终结方式

由华为 VRP 平台 802.1X 子系统扩展而成，将 EAP 在 LANSWITCH 设备终结并映射到 RADIUS 报文，利用标准 Radius 协议完成认证和计费。其运行过程如图 7。

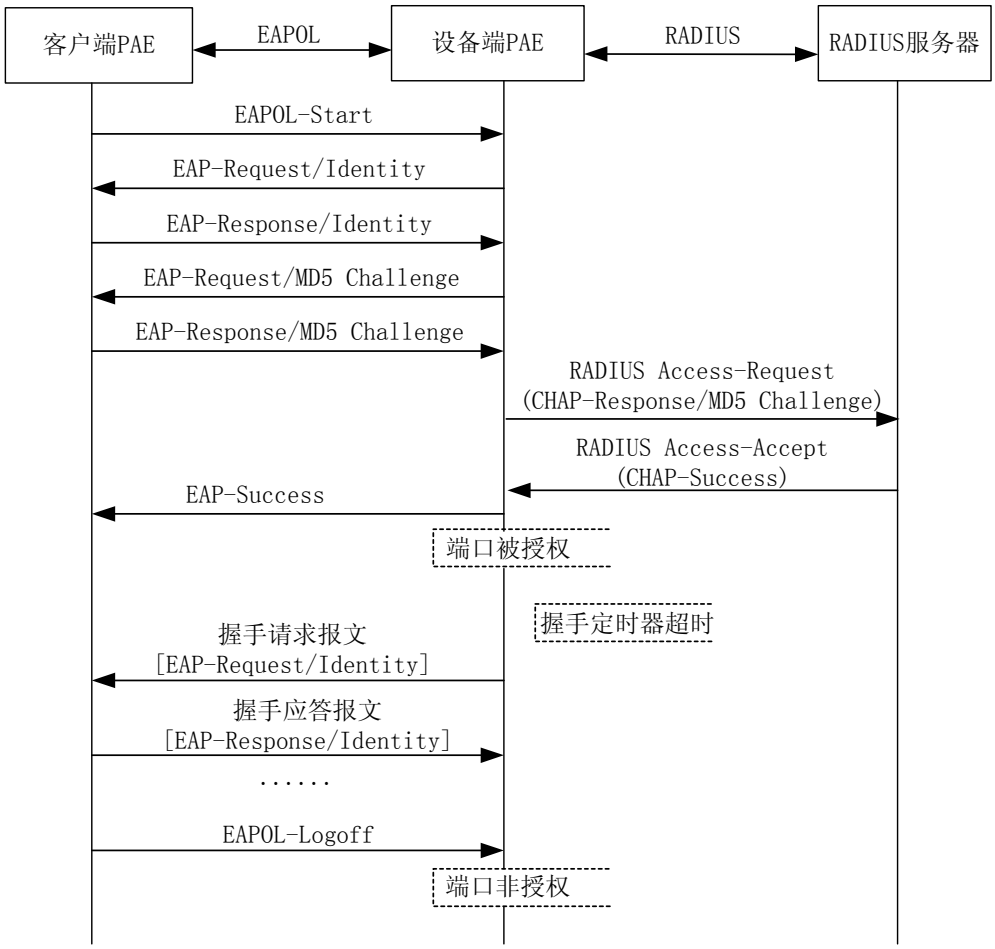

图7　802.1X EAP 终结认证流程图

这种方式的好处是可以采用标准的 RADIUS 服务器，可以保护用户的已有投资。PAP 和 CHAP 方法都是通过这种方式与服务器通信的。

3.11.2　EAP 中继方式

这种方式是 IEEE 802.1X 标准规定的，将扩展认证协议（EAP）承载在其他高层协议中，如 EAP over Radius，以便扩展认证协议报文穿越复杂的网络到达认证服务器 。处理流程如图 4。

一般来说，EAP 中继方式需要 RADIUS 服务器支持 EAP 属性：EAP_Message（79）和 Message_Authenticator（80）。如华为公司的 CAMS 或者 FreeRADIUS 组织的自由软件等。

3.12 内置认证服务器

可以在设备设置用户的账号与密码，对用户的认证直接响应，不需要 CAMS 或 RADIUS 的配合。交换机支持内置认证服务器，降低了小型网络的建设成本和管理成本。

为了降低设备的负载，内置服务器只支持认证功能，不支持计费功能。各个产品系列的用户容量指标请参考对应产品的规格说明书。

3.13 基于 802.1X 的受控组播

IP 组播技术实现了 IP 网络中点到多点的高效数据传送。由于能够有效地节约网络带宽、降低网络负载，IP 组播技术在实时数据传送、多媒体会议、数据拷贝、游戏和仿真等诸多方面都有广泛的应用。

但是，目前组播业务在运营方面还存在用户管理、业务管理和计费等多方面的问题。

华为公司基于组播可运营、可管理的理念，结合 802.1X 技术推出受控组播解决方案，

可以较好地解决用户管理和计费地问题。

3.14 完善的整体解决方案

华为公司具有完整的 802.1X 认证宽带网络解决方案，产品涵盖客户端、认证设备和认证服务器等完整系列。

客户端可是选择华为公司 802.1X 客户端产品，也可以是 XP 自带，或者其他第三方标准客户端。

认证设备包括Quidway S高中低系列和MA5200/5300等产品，服务器包括iTellin和CAMS等。根据组网需要和服务器是否支持EAP，可以选择在Quidway S系列设备上终结EAP或者透传。

4 典型组网

根据网络规模的大小以及认证记费和管理方面的要求，有三种典型的802.1X组网方式，即：集中认证、边缘分布认证和设备内置服务器认证。

4.1 集中认证方案

一般来说，集中认证适合于大中型网络，由于网络设备众多，集中认证有利于管理和集中控制；但是认证设备的负荷较重。如图 8 所示。

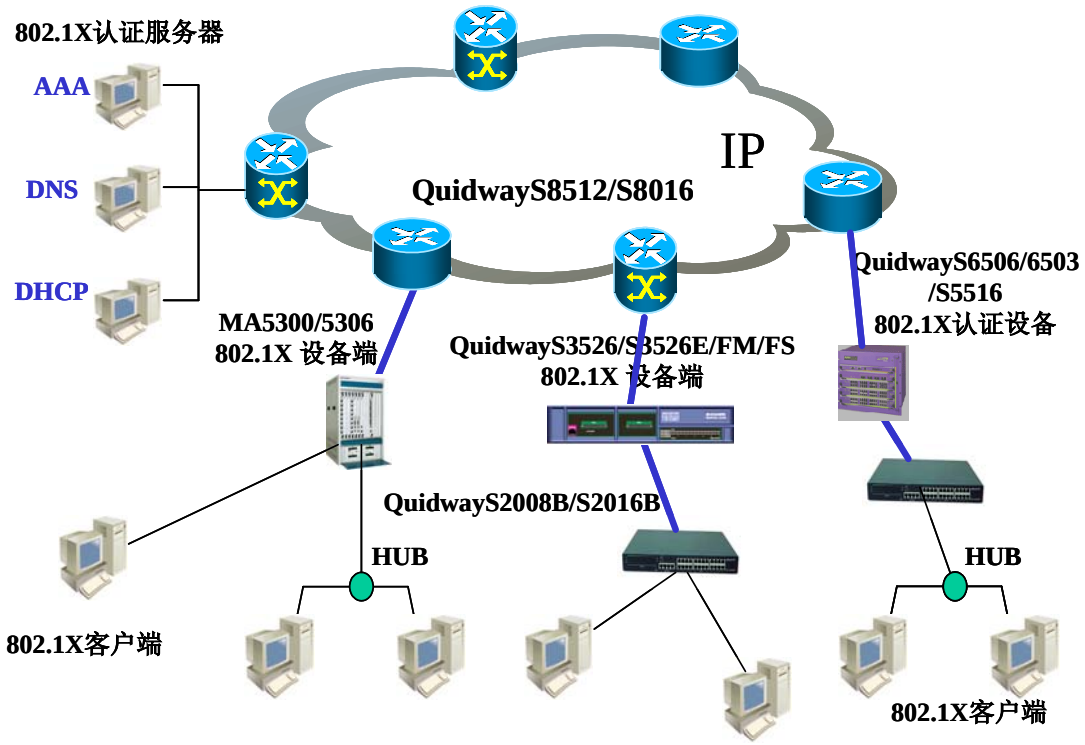

图8 802.1X 集中认证组网方案

如果使用 Trunk 端口认证功能，在认证设备上终结用户 VLAN，则可在单个认证设备上使用 4K VLAN 资源，从而大大提高 VLAN 资源的利用率，增强用户安全性。

4.2 边缘分布认证方案

对于结构复杂的网络，可以把认证操作边缘化，这样可以使得认证负荷在多个设备上均匀分担。当然，分布式认证会导致分布式网络管理。如图 9 所示。

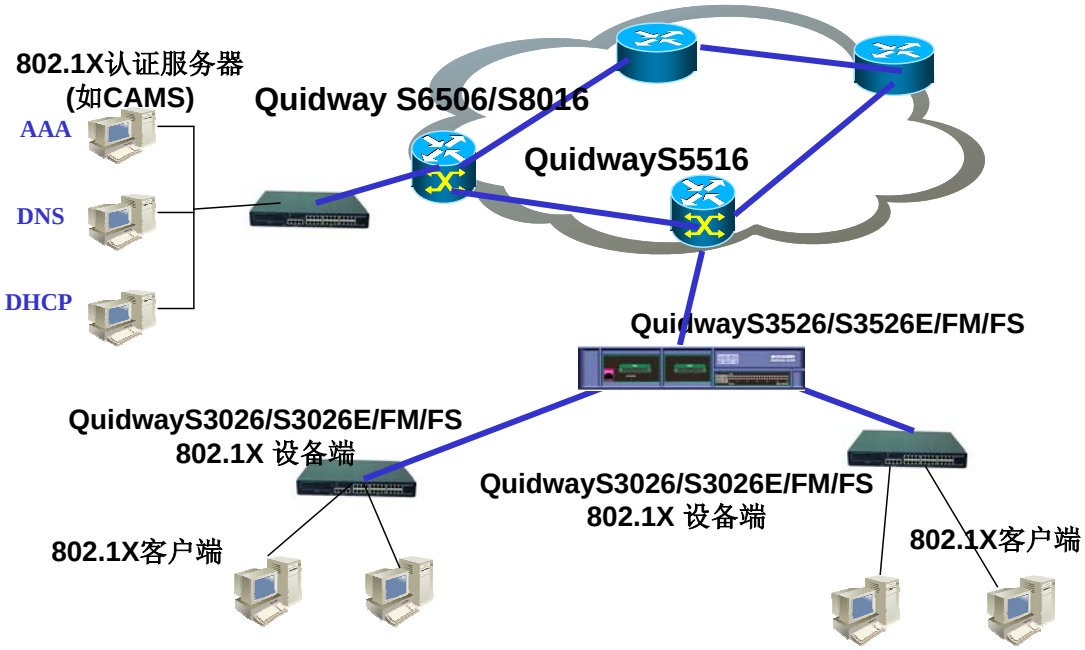

图9　802.1X 分布认证组网方案

对于接入和汇聚在物理为止相距很远的网络环境，边缘分布认证可以减少认证控制流占用传输带宽。

4.3　内置服务器认证方案

对于一些小型网络，从成本的角度考虑，外购专门认证服务器会显著增加网络成本。通过采用设备内置服务器认证可以较好地解决这个问题。

当然，根据具体情况，在同一网络中的不同层次和局点，这些方式可以集成使用。另外，设备在图中的层次也会根据网络规模变化，例如大型网络，S6000 系列可能处于汇聚层；在中小型网络，S6000 可能处于核心层，由 S3500 系列承担汇聚层的角色。

5　结论与展望

通过上述实例和分析可以看出，华为公司的 802.1X 解决方案具有完整的产品系列、出色的业务支持能力以及灵活的组网方案。

802.1X 由于其部署的经济性以及较低的设备开销，随着城域网、园区网的快速发展，以及 WLAN 的快速普及将越来越多地为人们的工作生活服务。