Portal技术白皮书

关键词：Portal，CAMS，安全，认证

摘　要：Portal认证也叫Web认证，即通过HTTP页面接受用户输入的用户名和密码，对用户进行认证。本文档主要介绍了Portal认证的基本流程和典型组网应用。

缩略语：

缩略语	英文全名	中文解释
AAA	Authentication, Authorization, Accounting	认证/授权/计费
ACL	Access Control List	访问控制列表
BAS	Broad Access Server	宽带接入服务器
CAMS	Comprehensive Access Management Server	综合访问管理服务器
HTTP	Hypertext Transfer Protocol	超文本传输协议
RADIUS	Remote Access Dial in User Service	远程认证拨号用户服务

目 录

1 概述

Portal在英语中是入口的意思。Portal认证通常也称为Web认证，一般将Portal认证网站称为门户网站。

未认证用户上网时，设备强制用户登录到特定站点，用户可以免费访问其中的服务。当用户需要使用互联网中的其它信息时，必须在门户网站进行认证，只有认证通过后才可以使用互联网资源。

1.1 产生背景

在传统的组网环境中，用户只要能接入局域网设备，就可以访问网络中的设备或资源，为加强网络资源的安全控制和运营管理，很多情况下需要对用户的访问进行控制。例如，在一些公共场合、小区或公司的网络接入点，提供接入服务的供应商希望只允许付费的合法用户接入，所以供应商为每个用户提供一个接入网络的账号和密码。另外，一些企业会提供一些内部关键资源给外部用户访问，并且希望经过有效认证的用户才可以访问这些资源。

现有的802.1x和PPPoE等访问控制方式，都需要客户端的配合，并且只能在接入层对用户的访问进行控制。

Portal认证技术则提供一种灵活的访问控制方式，不需要安装客户端，就可以在接入层以及需要保护的关键数据入口处实施访问控制。

1.2 技术优点

与现有的802.1x、PPPoE等认证技术相比，Portal认证技术具有以下优势：

- 不需要部署客户端，直接使用 WEB 页面认证，使用方便；
- 可以定制“VLAN+端口+IP 地址池”粒度级别的个性化认证页面，同时可以在 Portal 页面上开展广告业务、服务选择和信息发布等内容，进行业务拓展，实现 IP 网络的运营；
- 关注对用户的管理，可基于用户名与 VLAN ID/IP/MAC 的捆绑识别来认证，并采用 Portal server 和 Portal client 之间，BAS 和 Portal client 之间定期发送握手报文的方式来进行断网检测；
- 二次地址方式可以实现灵活的地址分配策略和计费策略，且能节省公网 IP 地址；

- 三层认证方式可以跨越网络层对用户作认证，可以在企业网络出口或关键数据的入口作访问控制。

2 Portal技术实现

2.1 概念介绍

如图1所示，Portal认证过程涉及到了认证客户端（Portal client），Portal服务器（Portal server），BAS和AAA服务器四个基本要素。

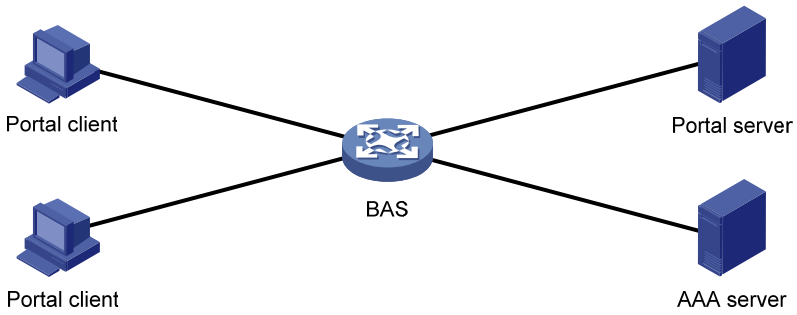

图1 Portal系统组成示意图

- Portal client：Portal组网中发起认证请求的客户端系统，为运行HTTP协议的浏览器。
- Portal server：Portal组网中接受客户端认证请求的服务端系统，提供免费门户服务和基于WEB认证的界面，与BAS设备交互认证客户端的身份信息。
- BAS：宽带接入服务器，用于向Portal server重定向HTTP认证请求，并且与Portal server、AAA服务器交互完成用户的认证/授权/计费功能。
- AAA服务器：认证/授权/计费服务器，与BAS进行交互，对用户进行认证/授权/计费。

以上四个基本要素的交互过程为：

(1) 未认证用户访问网络时，在 IE 地址栏中输入一个互联网的地址，那么此 HTTP 请求在经过 BAS 设备时会被重定向到 Portal server 的 Web 认证主页上；

(2) 用户在认证主页/认证对话框中输入认证信息后提交，Portal server 会将用户的认证信息传递给 BAS；

(3) 然后 BAS 与 AAA 服务器通信进行用户认证和计费；

(4) 认证通过后，BAS 会打开用户与互联网的通路，允许用户访问互联网。

2.2 协议框架

Portal协议包括Portal接入和Portal认证两部分，协议框架如图2所示：

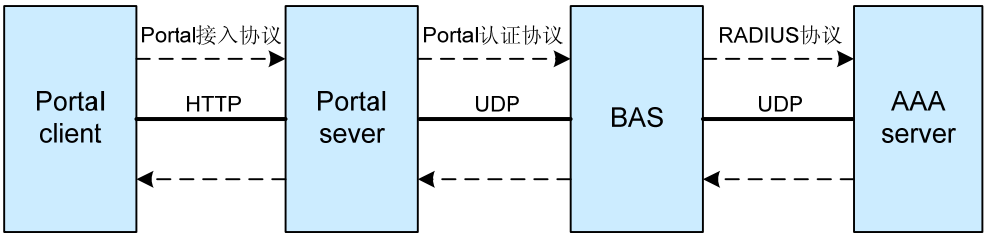

图2 Portal协议框架

Portal接入协议描述了Portal client和Portal server之间的协议交互，主要内容包括：

(1) Portal client 通过 HTTP 协议向 Portal server 提交认证信息。

(2) Portal server 通过 HTTP 协议向 Portal client 推出认证成功或者认证失败页面。

(3) Portal server 与 Portal client 之间通过握手检测用户是否在线。

Portal认证协议描述了Portal server和BAS之间的协议交互，主要内容包括：

(1) Portal 认证协议采用了非严格意义上的 Client/Server 结构，大部分消息采用 Request/Response 进行交互。同时还定义了一种 Notify 报文，提供 Portal sever 和 BAS 设备之间的消息通道。

(2) Portal 认证协议承载在 UDP 报文上。

(3) Portal server 使用本地的特定 UDP 端口监听 BAS 设备发送的非响应类报文，并向 BAS 设备特定的端口发送所有报文。BAS 使用本地的特定的 UDP 端口监听 Portal server 发送的所有报文，并向 Portal server 的特定端口发送非响应类报文。响应类报文的目的端口号使用对应的请求报文的源端口号。

2.3 认证流程

Portal认证有两种认证方式：二层认证方式和三层认证方式。二层认证方式又包括直接认证方式和二次地址方式。

1. 二层认证方式

二次认证方式下，Portal client与BAS直连，或它们之间只有二层设备存在。

- 直接认证方式

用户通过手工配置或DHCP获取的一个公网IP地址进行认证，在认证通过之前，只能访问Portal服务器以及设定的免费访问地址，认证通过后可使用此IP地址访问外部网络。

直接认证流程简单，但由于限制了Portal client只能与BAS通过二层交换设备互连，降低了组网的灵活性。

- 二次地址方式

用户通过DHCP获取一个私网IP地址进行认证，在认证通过之前，只能访问Portal服务器以及设定的免费访问地址，认证通过后，释放原有私网IP地址，使用重新分配的公网IP地址访问外部网络。

二次地址方式流程较为复杂，认证通过之前用户可使用私网IP地址，节省了公网IP地址，但组网方式不灵活。

2. 三层认证方式

这种认证方式允许Portal client和BAS之间跨接三层转发设备，组网方式灵活。因为三层认证流程与直接认证方式相同，下面将仅对直接认证方式的认证流程和二次地址方式的认证流程做详细描述。

2.3.1 直接认证方式的认证流程

1. 流程图

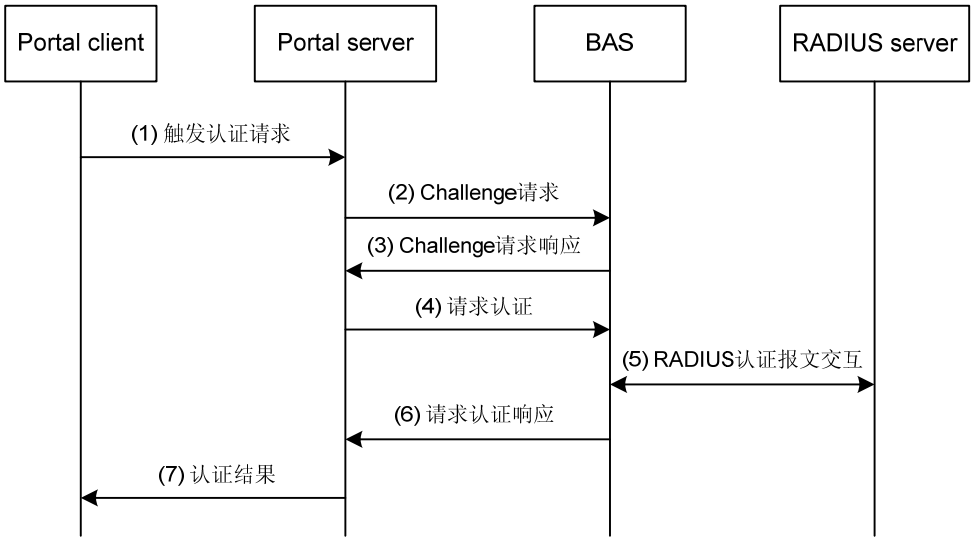

图3 Portal直接认证方式认证流程图

2. 具体步骤

下面认证流程以CHAP认证为例，对于PAP认证方式，步骤（2）、（3）、（4）可以省略。

(1) Portal client 通过 HTTP 协议触发认证请求。

(2) Portal sever 收到认证请求后，首先向 BAS 设备发送 Challenge 请求报文，并启动定时器等待 BAS 设备的响应。如果在一定时间内没有收到 BAS 设备的回应报文，则重传此报文，若到达最大重传次数仍没有回应，则通知 Portal client 认证失败。

(3) BAS 设备收到 Challenge 请求报文后，检查报文的合法性，对合法的报文进行响应。

(4) Portal server 收到 Challenge 请求报文的响应报文后，根据 CHAP 算法，计算 CHAP-PASSWORD，然后向 BAS 设备发送请求认证报文，并启动定时器等待 BAS 设备的响应。如果在规定的时间内没有收到 BAS 设备的回应报文，Portal server 会重发一定次数的认证请求报文，当达到最大重传次数时仍没有回应，则通知用户认证失败。

(5) BAS 设备收到请求认证报文后，首先进行合法性检查，对合法的报文进行认证处理，即根据认证方式（CHAP）构造 RADIUS 认证请求报文发给

RADIUS server，然后开启定时器等待 RADIUS server 的认证回应。如果在规定的时间内 RADIUS server 无响应，则 BAS 设备向 RADIUS server 重发一定次数的认证请求报文，当达到最大重传次数时仍没有回应，则认为本次认证失败。

(6) BAS 设备根据认证的结果向 Portal sever 发送认证请求响应报文。

(7) Portal server 根据认证请求响应报文表示的认证结果（成功，失败）通知 Portal client 是否认证成功。

2.3.2 二次地址方式的认证流程

1. 流程图

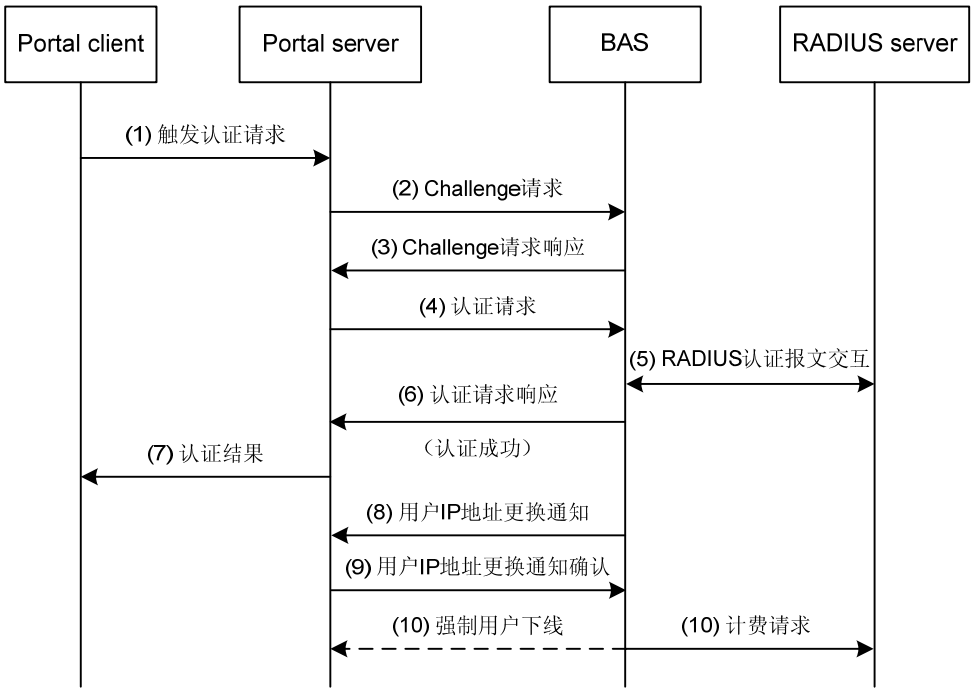

图4 Portal二次地址方式认证流程图

2. 具体步骤

(1) Portal client 通过 HTTP 协议触发认证请求。

(2) Portal sever 收到认证请求后，首先向 BAS 设备发送 Challenge 请求报文，并启动定时器等待 BAS 设备的响应。

(3) BAS 设备收到 Challenge 请求报文后，检查报文的合法性，对合法的报文进行响应。

(4) Portal sever 向 BAS 发送请求认证报文，并启动定时器等待 BAS 设备的回应。

(5) BAS 设备与 RADIUS server 之间进行 RADIUS 协议报文的交互。

(6) BAS 设备根据认证的结果以及定时器的信息向 Portal server 发送请求认证响应报文，同时在报文中增加控制信息。若认证成功，则控制信息表示要求 Portal server 通知 Portal client 释放 IP，并重新申请 IP 地址。

(7) Portal server 向 Portal client 发送认证通过报文，收到该报文后，Portal client 释放原私网 IP 地址，并申请新的公网 IP 地址。

(8) BAS 设备通过 Portal client 发送的免费 ARP 报文可以检测到 Portal client 的 IP 地址的状态，一旦检测到 Portal client 的 IP 地址成功更换成公网 IP 地址，就向 Portal server 发送用户 IP 地址更换的通知报文，并开启定时器等待地址更新回应报文。

(9) Portal server 在收到 BAS 的用户 IP 地址更换通知，以及客户端的 IP 地址更新通知后，向 BAS 发送确认报文，并向客户端进行地址更新确认。如果只收到一方的报文，Portal server 认为用户 IP 地址没有更新。

(10) BAS 收到的确认报文中携带标识地址切换是否成功的信息，若该信息表示地址切换成功，则 BAS 向 RADIUS server 发送计费请求，请求上线；如果表示地址切换失败，则 BAS 会向 Portal server 发送报文来强制用户下线。

2.4 下线流程

Portal用户下线流程包括两种方式：由Portal client发起的主动下线和由Portal server或BAS发起的强制下线。

2.4.1 主动下线流程

具体步骤如下：

(1) Portal 用户通过 HTTP 协议发起下线请求。

(2) Portal server 发送请求下线报文后，开启定时器等待 BAS 设备的回应，如果 BAS 设备在规定的时间内没有回应，则 Portal server 一直重发下线请求。报文的重传次数可以根据网络的实际情况调整。

(3) 当 BAS 设备收到 Portal server 的下线请求后，向 Portal server 发送请求下线回应报文，同时向 RADIUS sever 发送停止计费报文。

一般来说，下线不存在成功和失败的说法，用户要选择下线，肯定是要允许的，所以Portal server收到用户的下线请求后，会通知Portal client下线成功，而不需要等

待BAS设备对下线的确认。

2.4.2 强制下线流程

当管理员通过命令行切断连接，或BAS设备主动探测发现用户已经离线，以及BAS设备接入用户的接口被拔出、接口板被拔出等事件发生时，BAS设备需要通知Portal server强制用户下线。具体步骤如下：

(1) BAS 设备向 Portal server 发送用户被强制下线的通知报文来告知 Portal client 已经下线。

(2) Portal server 收到通知报文后，向 BAS 设备发送确认报文来确认，同时通知 Portal client 网络连接已中断。

由于Portal server可能会因网络问题等原因收不到BAS的通知报文，从而无法得知用户已下线的消息。因此BAS设备会向Portal server重复发送通知报文有限次数。若有限次数的重复过程结束之后，BAS设备仍然未收到Portal server的确认，那么BAS设备会停止发送通知报文。虽然BAS发起的通知过程失败了，但由于Portal server和Portal client之间存在心跳检测机制，最终Portal server也可得知用户已下线。

3 典型组网应用

3.1 Portal二层组网方案

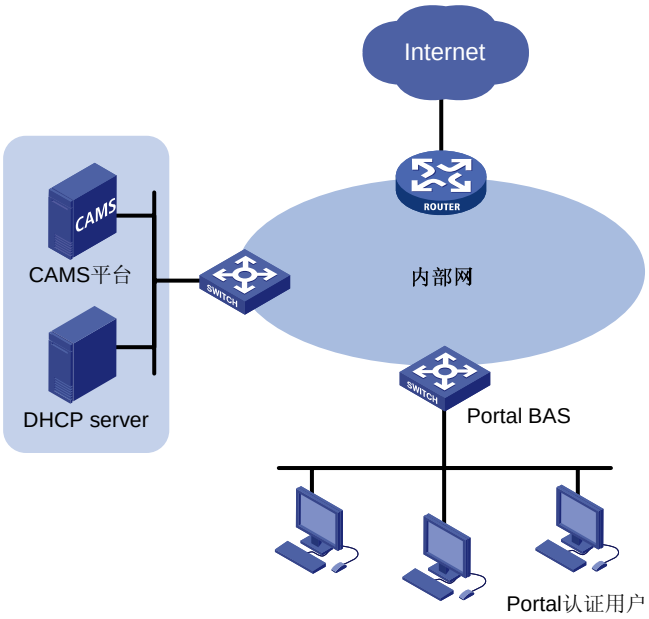

图5 Portal二层组网方案

在用户接入的二层BAS设备上部署Portal，可以实现对内部网络接入的Portal认证用户进行认证和计费。CAMS平台需要部署Portal业务组件。

3.2 Portal三层组网方案

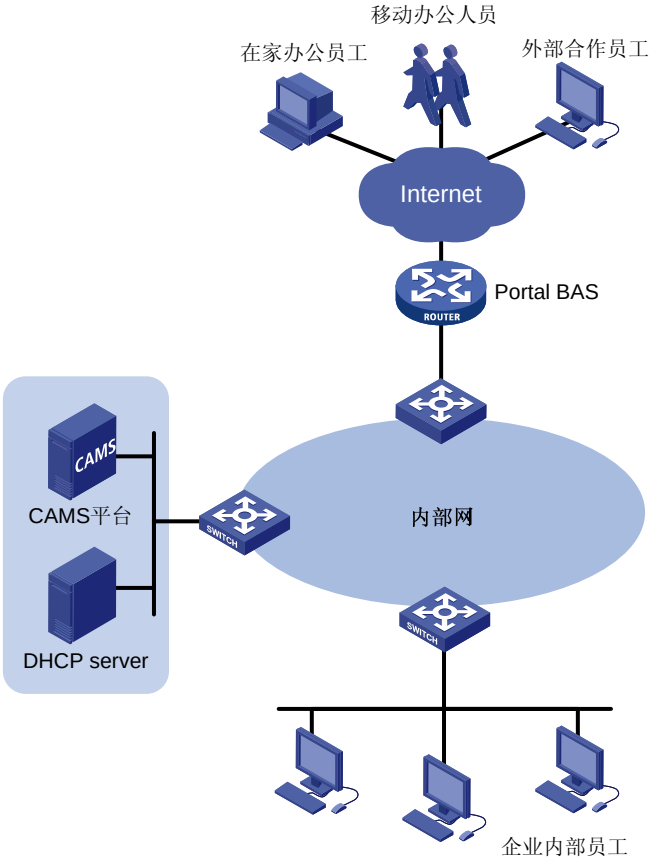

图6 Portal三层组网方案

在企业入口的BAS设备上部署Portal，可以对外部网络中访问企业网内部关键业务区域的用户进行认证和计费，也可以对企业内部网络中访问Internet的用户进行认证和计费。这种组网方式下，部署Portal的设备和用户之间可以跨越三层交换设备。

4 参考文献

RFC 2865：Remote Authentication Dial In User Service (RADIUS)