

ICS 01.040.35

L 04

YD

中华人民共和国通信行业标准

YD/T 2667-2013

基于 WEB 的以太网接入身份认证 技术要求

Technical specification for WEB based authentication of
Ethernet access

2013-10-17 发布

2014-01-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 术语、定义与缩略语	1
2.1 术语和定义	1
2.2 缩略语	2
3 体系结构	3
3.1 组成结构	3
3.2 逻辑体系结构	3
4 系统流程图	4
4.1 NAC登录流程	4
4.2 会话保活流程	8
4.3 NAC退出流程	8
5 消息格式和编码	9
5.1 NAC与Portal之间的消息格式和编码	9
5.2 认证客户端与认证服务器之间的消息格式和编码	10
5.3 NAD与Portal之间的消息格式和编码	10
6 级联、哑终端与直通问题	11
6.1 交换机级联的问题	11
6.2 哑终端设备的问题	11
6.3 直通协议	11
6.4 直通地址	12
7 安全性考虑	12
7.1 仿冒攻击	12
7.2 嗅探攻击	12
7.3 NAD的安全性	12
7.4 Web服务器的安全	12
7.5 其他攻击	12
附录A (资料性附录) RADIUS属性列表	13
附录B (资料性附录) 典型应用场景和参考实现	15

前 言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：清华大学、福建星网锐捷网络有限公司、杭州华三通信技术有限公司、赛尔网络有限公司、西安邮电学院。

本标准主要起草人：段海新、姚 辉、秦丰林、林 涛（杭州华三通信技术有限公司）、黄友俊、朱志祥、贾晓巍、祁正林、刘 武、姚星昆、林 涛（清华大学）、李 威、胡 松。

基于Web的以太网接入身份认证技术要求

1 范围

本标准规定了基于Web的以太网接入认证相关术语、接入认证系统的结构、协议交互流程、信息交换格式与编码方法、安全机制等。

本标准适用于有线以太网环境中的基于Web的接入认证，涉及接入终端中的Web浏览器、以太网交换机、Web服务器、认证服务器（如RADIUS）等产品或系统，包括对IPv4和IPv6协议的支持。

2 术语、定义与缩略语

2.1 术语和定义

下列术语和定义适用于本文件。

2.1.1

网络接入客户端 Network Access Client

网络链路上请求接入网络的计算机系统。本标准中指使用Web浏览器（如IE、Firefox、Opera等）访问网络的用户。

2.1.2

网络接入设备 Network Access Device

支持基于Web的接入身份认证技术的网络设备。本标准中指以太网接入交换机。

2.1.3

接入门户服务器 Access Portal Server或Portal

基于Web接入身份认证技术的Web服务器，用户在通过认证之前所有的访问都会被重定向到该门户服务器，用户输入认证信息（如用户名和口令）。

2.1.4

认证客户端 Authentication Client

向认证服务器发起身份认证请求，并接收认证服务器认证结果的设备。本标准中指RADIUS客户端。

2.1.5

认证服务器 Authentication Server

验证用户认证信息的服务器，用来接收认证客户端发起的身份认证请求，并返回认证结果。本标准中指RADIUS服务器。

2.1.6

保活页面 Keep Alive Web Page

在认证成功后，网络接入客户端需要周期性地向接入认证门户服务器请求该页面，保持认证会话的活跃状态。

2.1.7

认证凭证 Authenticated Ticket

在认证成功后，接入门户服务器发给网络接入客户端浏览器的一个凭证信息（比如一个经过数字签名的cookie），用于保存网络接入客户端的认证信息，包括身份标识符、IP地址、时间戳等字段。

2.1.8

授权的协议 Authorized Protocol

网络接入设备在网络接入客户端通过身份认证前就允许其通过的流量，比如DHCP、DNS等。

2.1.9

授权的地址 Authorized Address

网络接入设备在网络接入客户端通过身份认证前就允许其访问的地址，比如接入门户网站的地址等。

2.2 缩略语

下列缩略语适用于本文件。

ARP	Address Resolution Protocol	地址解析协议
AS	Authentication Server	认证服务器
CGI	Common Gateway Interface	通用网关接口
CHAP	Challenge Handshake Authentication Protocol	询问握手认证协议
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DHCPv6	Dynamic Host Configuration Protocol for IPv6	IPv6 动态主机配置协议
DNS	Domain Name System	域名系统
HTML	HyperText Markup Language	超文本标记语言
HTTP	HyperText Transfer Protocol	超文本传输协议
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer	基于安全套接层的超文本传输协议
IETF	Internet Engineering Task Force	互联网工程任务组
IP	Internet Protocol	互联网协议
IPv4	Internet Protocol Version 4	互联网协议版本 4
IPv6	Internet Protocol Version 6	互联网协议版本 6
MD5	Message Digest Algorithm MD5	消息摘要算法第五版
NAC	Network Access Client	网络接入客户端
NAD	Network Access Device	网络接入设备
NDP	Neighbor Discovery Protocol	邻居发现协议
PAP	Password Authentication Protocol	密码验证协议：
RADIUS	Remote Authentication Dial In User Service	远程用户拨号认证系统
SLAAC	Stateless Address Auto-configuration	无状态地址自动配置
TCP	Transmission Control Protocol	传输控制协议
UDP	User Datagram Protocol	用户数据包协议
URL	Uniform Resource Locator	统一资源定位符

3 体系结构

3.1 组成结构

基于Web的以太网接入身份认证系统包括五个逻辑组件：网络接入客户端、网络接入设备、接入门户网站、认证客户端、认证服务器。

在不同的网络环境下，网络接入设备的性能和配置不同、管理模式不同，五个逻辑组件在物理设备中的分配也不同。存在三种网络结构：

a) 网络接入设备与认证门户网站是两台独立的设备，由门户网站集成认证客户端(即RADIUS客户端)功能，如图1所示。该结构便于集中管理，网络接入设备因不实现RADIUS客户端而简单，但是认证门户网站的负载较高。

b) 网络接入设备与门户网站是两台独立的设备，由网络接入设备集成认证客户端(即RADIUS客户端)功能，如图2所示。该结构对认证门户网站的功能要求不高，但要求交换机需要支持认证客户端的功能。

c) 网络接入设备集成了门户网站的功能和认证客户端的功能(即RADIUS客户端)，如图3所示。该结构适用于工作组环境，不需要集中的认证服务器。

前两种网络结构统称为“瘦NAD”结构，主要用于大中型网络，第三种网络结构称之为“胖NAD”结构，主要用于小型网络。

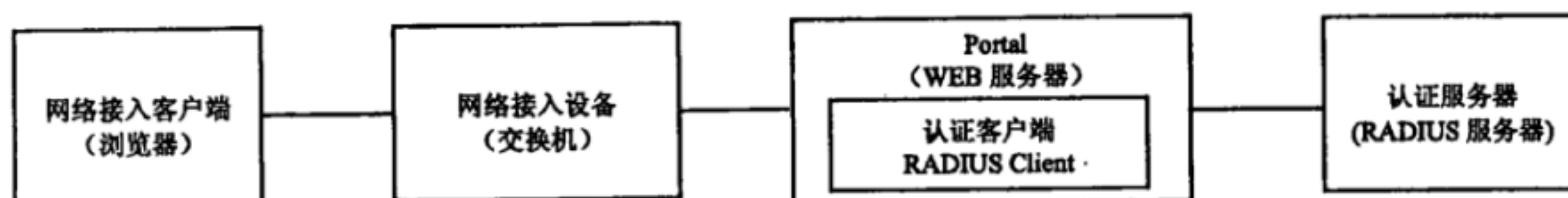


图1 网络结构一：精简交换机结构

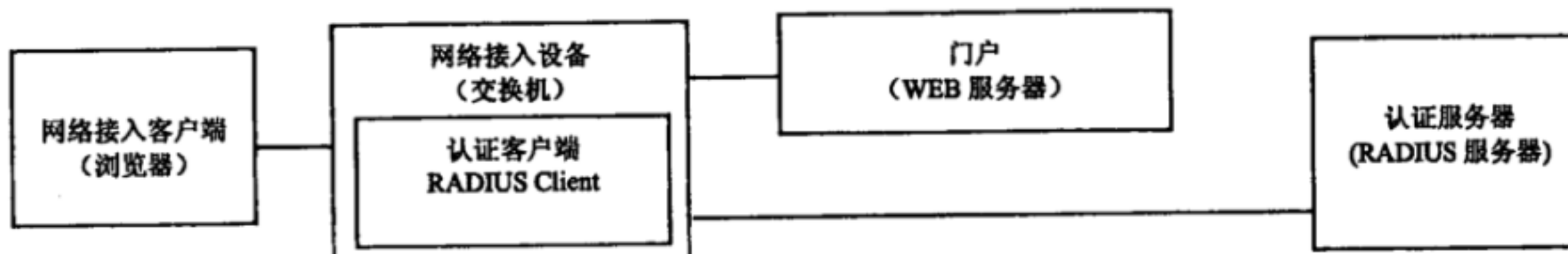


图2 网络结构二：交换机内置认证客户端结构

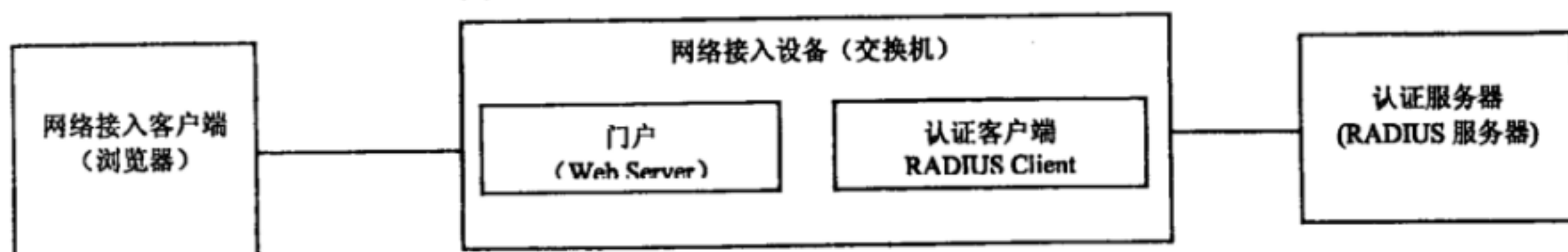


图3 网络结构三：交换机内置认证客户端和Web服务器结构

3.2 逻辑体系结构

逻辑体系结构由NAC、NAD、Portal、认证客户端和认证服务器五个逻辑组件组成如图4所示。对于设备包含逻辑组件组合关系，属于设备内部交互机制，本标准不涉及。

NAD应具备HTTP协议、TCP协议的侦听能力，支持Web认证的功能。NAD的受控逻辑端口，初始状态为关闭，不能访问受保护网络资源，认证成功后，受控逻辑端口打开，NAC访问受保护网络资源。受控逻辑端口宜控制到具体协议，例如IPv4协议、IPv6协议等。

NAD的非受控逻辑端口允许授权协议通过,例如IPv6的邻居发现协议(ICMP ND)、DHCPv6、DNS等,和IPv4下的ARP、DHCP等协议,见6.3规定的直通协议;非受控逻辑端口应允许通过访问门户网站的HTTP协议报文,见6.4规定的直通地址。

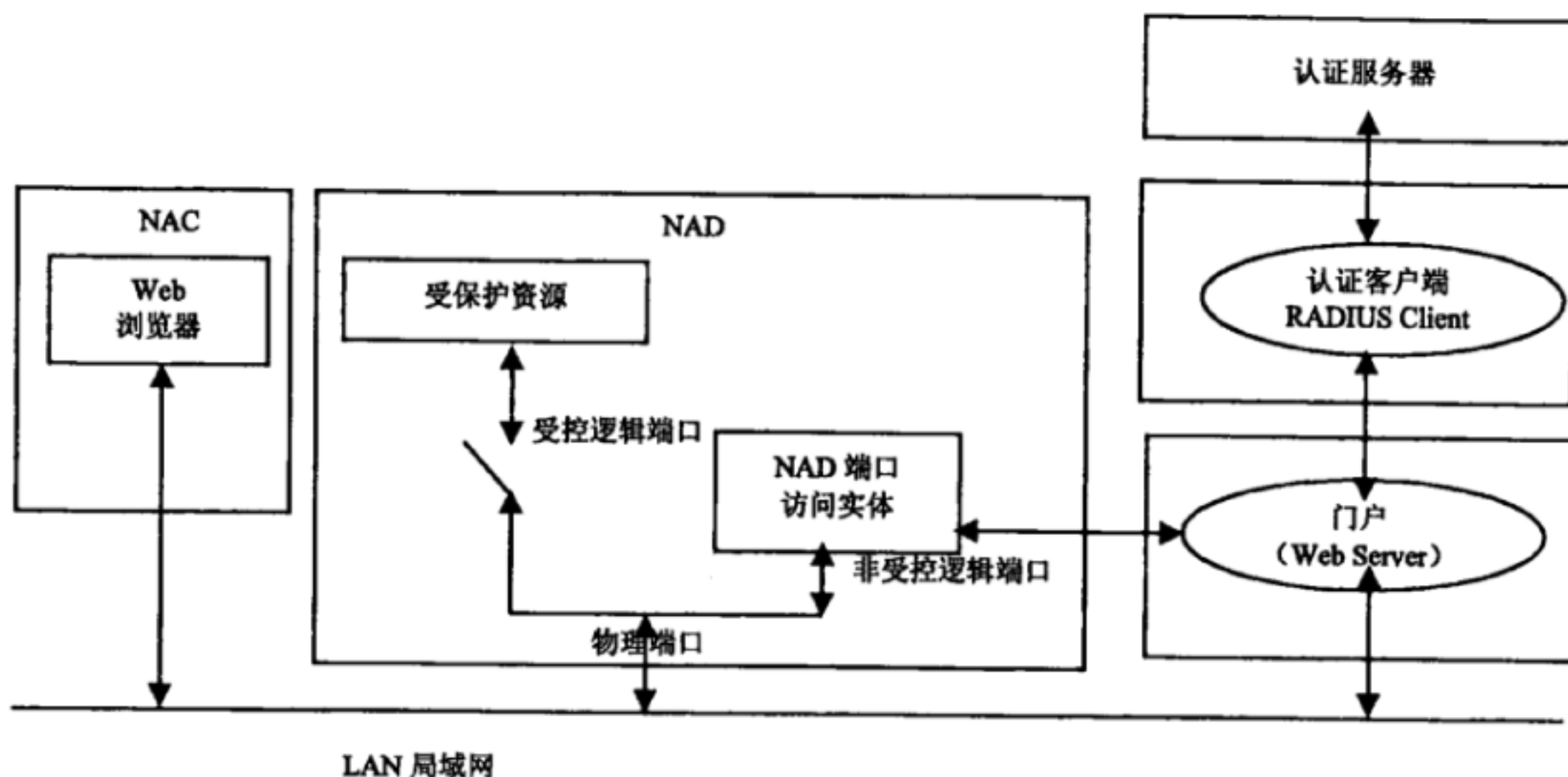


图4 逻辑体系结构图

4 系统流程图

针对4.1定义的三种网络结构,分别描述其系统流程。

4.1 NAC 登录流程

4.1.1 Portal 和认证客户端外置于交换机（网络结构一）的 NAC 登录流程

网络结构一的NAC登录流程如图5所示,该结构中Portal集成了认证客户端,外置于NAD交换机,向认证服务器发起身份认证请求,NAD开通HTTP服务,和Portal交互控制端口打开和关闭的命令。

1) NAC使用浏览器访问外网网页(假设为http://hostname/url),请求建立TCP连接。由于NAC允许DNS流量通过,因此本过程忽略DNS请求的过程,假设客户端域名解析得到hostname对应的IP地址为hostIP。

2) NAD截获到该请求后,判断该NAC是否为认证用户。若非认证用户,则以用户请求的外网地址(hostIP)与用户建立连接,完成标准的TCP三次握手过程。

3) NAC的浏览器发送HTTP GET/HEAD请求外网网页。

4) NAD向用户发送一个HTTP重定向响应,将用户的访问重定向到Portal,该重定向地址指向Portal的URL,其CGI参数详见5.1的NAC与Portal之间消息格式编码。

5) NAD关闭与NAC的TCP连接。

6) NAC的浏览器通过重定向地址来访问Portal。

7) Portal返回一个用户认证界面,该页面含有一个表单(Form),里面包含用户名和密码两个控件。

8) NAC输入用户名和密码,以GET或POST方式向Portal提交身份认证请求,该请求包括用户名、用户密码。

9) Portal根据接收到的用户名和密码封装成认证请求报文,采用PAP或者CHAP认证方式,向认证服务器请求认证。

- 10) 认证服务器依据请求报文内容和数据库信息判断用户合法性，返回认证结果报文。
- 11) 如果认证成功，Portal通过HTTP协议向NAD发送控制命令打开NAD的受控逻辑端口，允许该NAC正常访问网络。为了保证攻击者无法假冒Portal向NAD发送控制命令，Portal和NAD之间通过共享密钥来实现消息的认证。该HTTP命令的CGI参数和消息认证机制详见5.3的NAD与Portal之间消息格式和编码。
- 12) NAD向Portal返回执行HTTP端口打开命令的结果。
- 13) Portal向NAC返回认证结果页面，通知NAC认证结果。如果认证成功，NAC可以正常访问网络。同时，Portal可以选择向NAC写入一个认证cookie，该cookie可以用于保存NAC的认证信息，以用于增强系统的安全性。

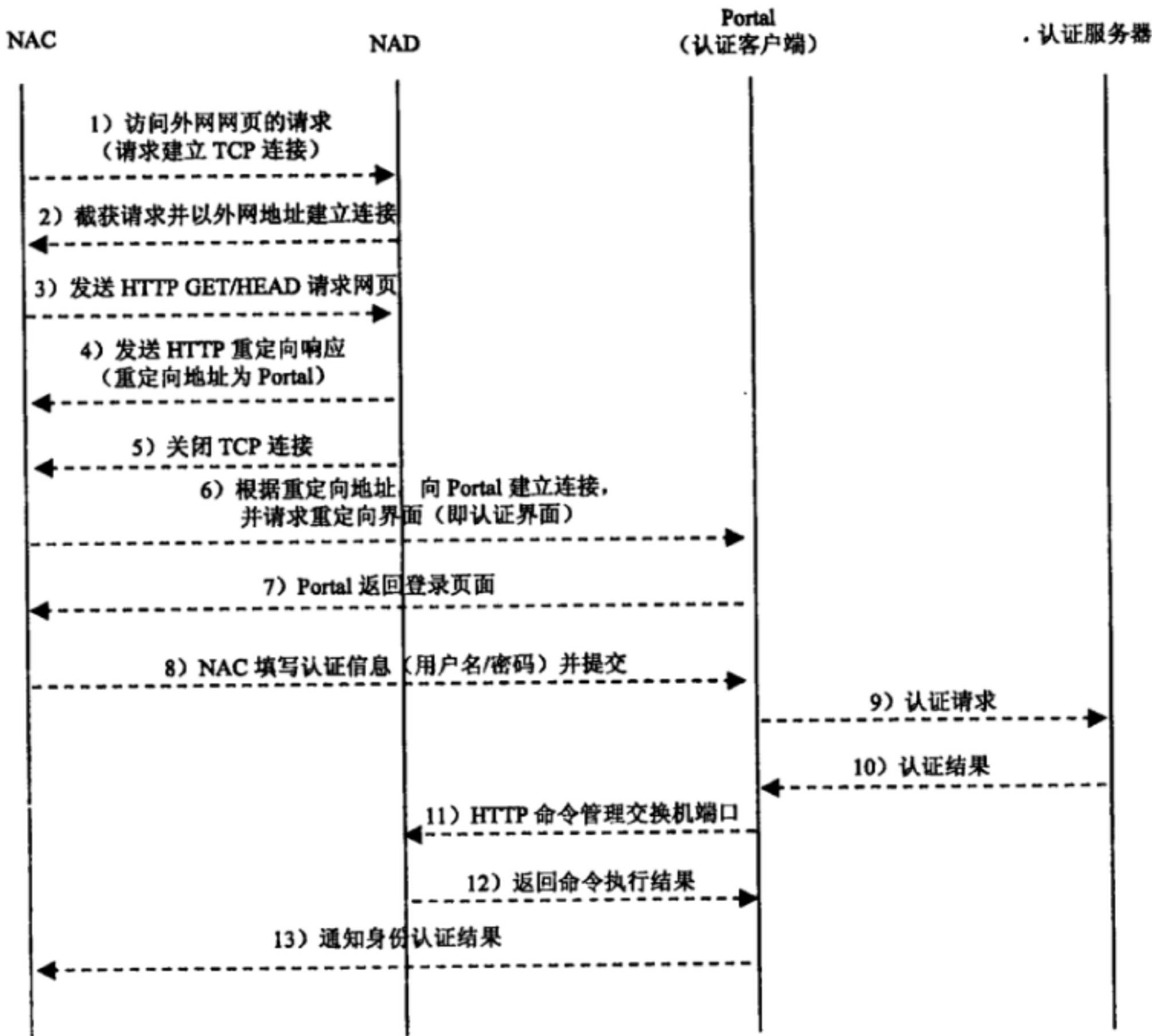


图5 网络结构一的NAC登录流程

4.1.2 Portal 外置于交换机（网络结构二）的 NAC 登录流程

网络结构二的NAC登录流程如图6所示，该结构NAD和Portal独立，NAD作认证客户端向认证服务器发起身份认证请求。NAD应开通HTTP服务，接收Portal发送的用户名和密码等信息。该结构中的端口控制功能由NAD自身完成。

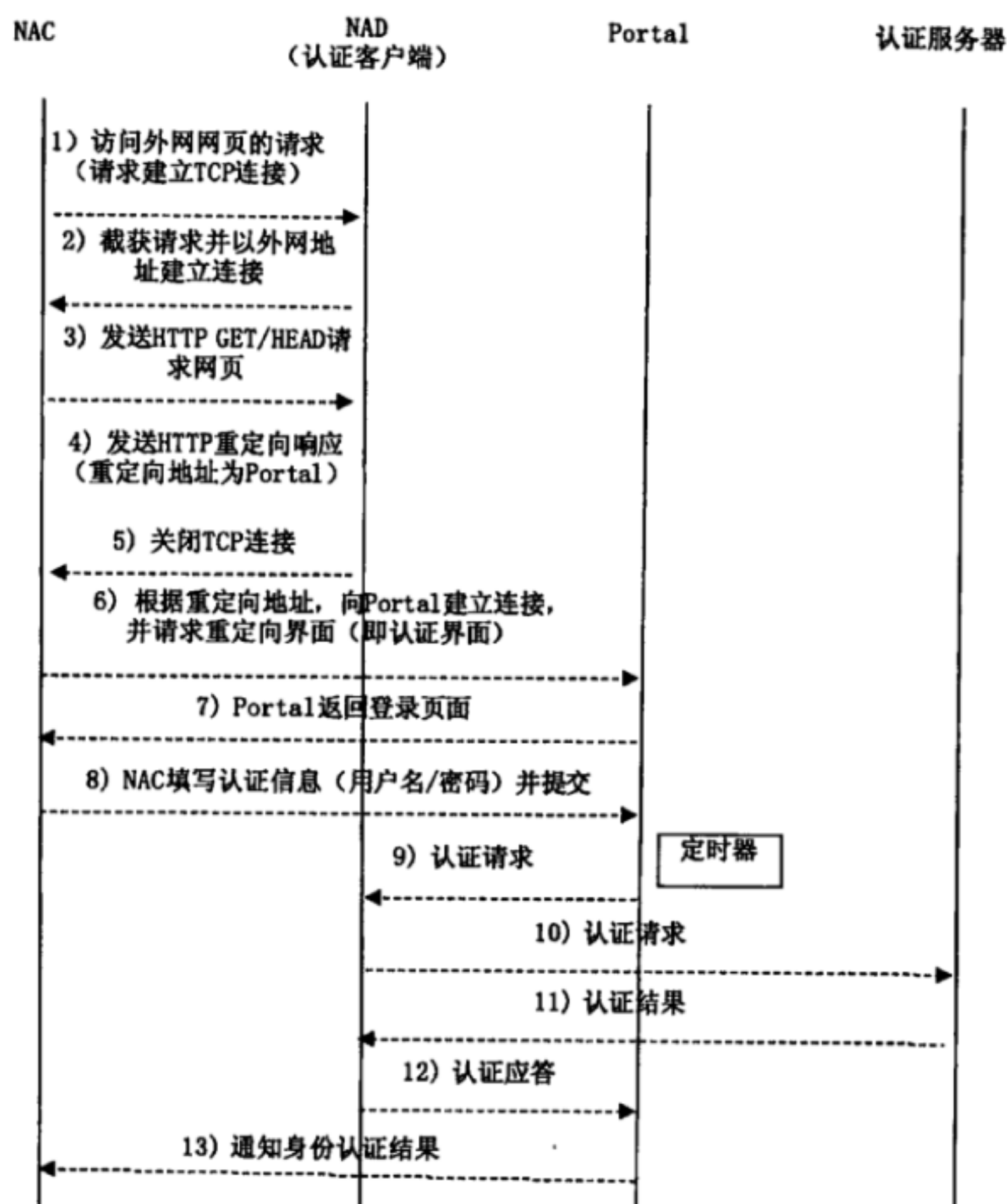


图6 网络结构二的NAC登录流程

- 1) NAC使用浏览器访问外网网页, 请求建立TCP连接。
- 2) NAD截获到该请求后, 判断该NAC是否为认证用户。若非认证用户, 则以用户请求的外网地址与用户建立连接。
- 3) NAC的浏览器发送HTTP GET/HEAD请求外网网页。
- 4) NAD向用户发送一个HTTP重定向响应, 将用户重定向到Portal, 该重定向地址指向Portal的URL, 其CGI参数详见5.1的NAC与Portal之间消息格式编码。
- 5) NAD关闭与NAC的TCP连接。
- 6) NAC的浏览器通过重定向地址来访问Portal。
- 7) Portal返回一个用户认证界面, 该页面含有一个表单, 里面包含用户名和密码两个控件。
- 8) NAC输入用户名和密码, 以GET或POST方式向Portal提交身份认证请求, 该请求包括用户名、用户密码。
- 9) Portal将用户输入的用户名和密码组装成认证请求报文发往NAD, 同时开启定时器等待认证应答报文。
- 10) NAD根据接收到的用户名和密码封装成认证请求报文, 向认证服务器请求认证。
- 11) 认证服务器依据请求报文内容和数据库信息判断用户合法性, 返回认证结果报文。
- 12) NAD向Portal发送认证结果, 如果认证成功, NAD打开受控逻辑端口。

13) Portal向NAC返回认证结果页面,通知NAC认证结果。如果认证成功,NAC可以正常访问网络。同时,Portal可以选择向NAC写入一个认证cookie,该cookie可以用于保存NAC的认证信息,以用于增强系统的安全性。

4.1.3 网络结构三的 NAC 登录流程

网络结构三的 NAC 登录流程如图 7 所示。NAD 内嵌认证客户端功能,由 NAD 作为认证客户端向认证服务器发起身份认证请求。

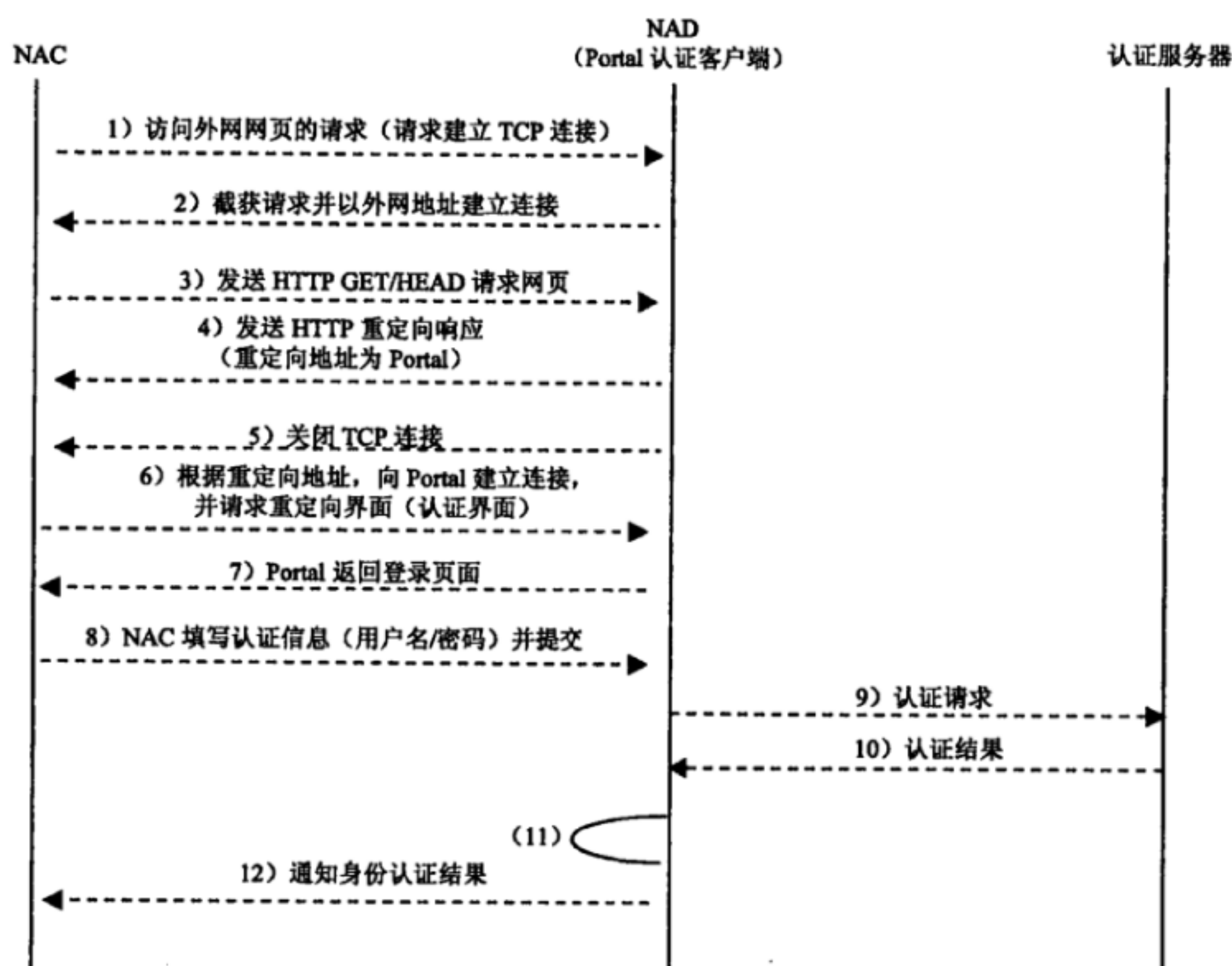


图7 网络结构三的NAC登录流程

- 1) NAC 使用浏览器访问外网网页, 请求建立 TCP 连接。
- 2) NAD 截获到该请求后, 判断该 NAC 是否为认证用户。若非认证用户, 则以用户请求的外网地址与用户建立连接。
- 3) NAC 的浏览器发送 HTTP GET/HEAD 请求外网网页。
- 4) NAD 向用户发送一个 HTTP 重定向响应, 将用户重定向到 Portal, 该重定向地址指向 Portal 的 URL, 其 CGI 参数详见 5.1 的 NAC 与 Portal 之间消息格式编码。
- 5) NAD 关闭与 NAC 的 TCP 连接。
- 6) NAC 的浏览器通过重定向地址来访问 Portal。
- 7) Portal 返回一个用户认证界面, 该页面含有一个表单, 里面包含用户名和密码两个控件。
- 8) NAC 输入用户名和密码, 以 GET 或 POST 方式向 Portal 提交身份认证请求, 该请求包括用户名、用户密码。
- 9) Portal 根据接收到的用户名和密码封装成认证请求报文, 向认证服务器请求认证。
- 10) 认证服务器依据请求报文内容和数据库信息判断用户合法性, 返回认证结果报文。
- 11) 如果认证成功, NAD 打开受控逻辑端口, 允许来自该 NAC 的报文通过。

12) NAD 向 NAC 返回认证结果页面, 通知 NAC 认证结果。NAC 正常访问网络。NAD 可向 NAC 写入认证 cookie, 该 cookie 用于保存 NAC 的认证信息, 以增强系统的安全性。

4.2 会话保活流程

NAC 与 Portal 服务器之间通过 HTTP 协议进行心跳握手, 设置心跳超时。当 Portal 服务器发现心跳超过设定的心跳超时时间 (默认时间为 1 分钟) 就通知交换机切断该 NAC 的连接, 用户可配置。会话保活流程如图 8 所示。

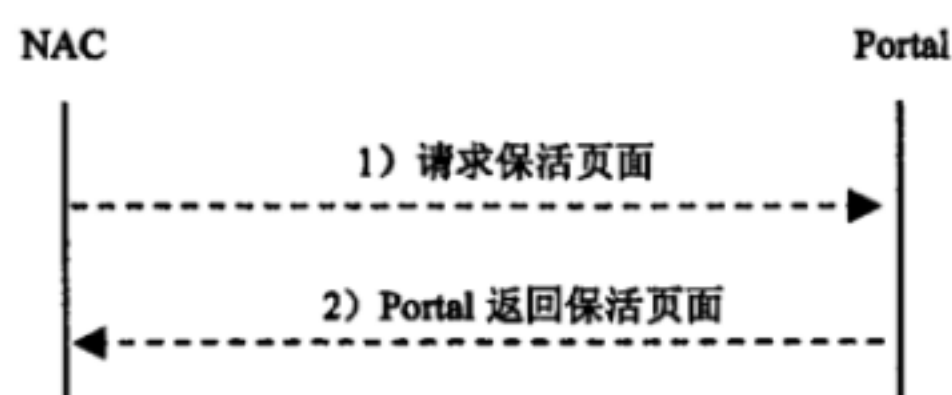


图8 会话保活流程

1) NAC 在认证成功后, 周期性地向 Portal 请求保活页面, 以保持该会话的活动状态。

2) Portal 返回保活页面。

4.3 NAC 退出流程

4.3.1 NAC 主动退出流程

NAC 主动退出是指用户通过 HTTP 页面请求下线, 主动断开与网络的连接。NAC 主动退出流程如图 9 所示。

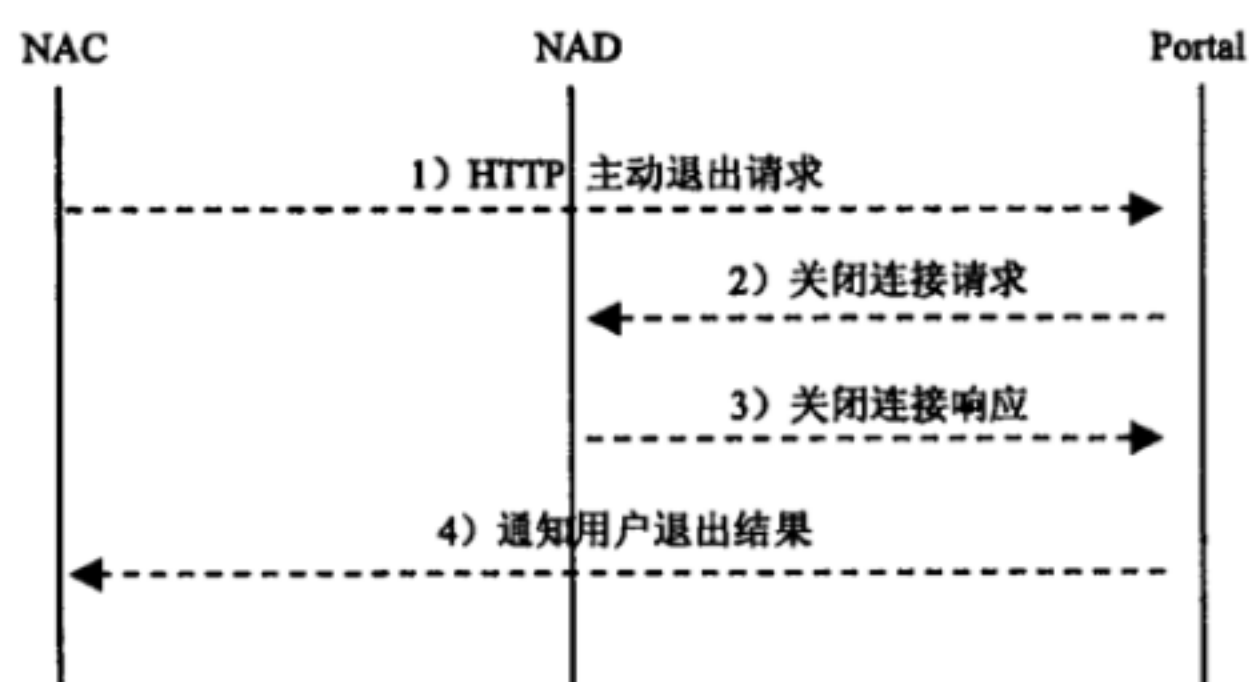


图9 NAC主动退出流程

1) NAC 通过 HTTP 协议向 Portal 发送退出请求, 该请求 URL 的 CGI 参数包括用户名、用户 MAC 等信息, 可选携带认证 cookie。

2) Portal 向 NAD 发送用户退出关闭连接请求。

3) NAD 收到 Portal 的下线请求后, 向 Portal 返回用户退出响应; 用户下线。

4) Portal 向 NAC 返回退出结果页面, 通知用户退出结果。

4.3.2 NAC 被动退出流程

NAC 被动退出是指用户未执行主动退出操作而断开网络连接的情形, 例如用户关机、重启、系统崩溃等。在这种情况下, 需要检测用户是否仍然在线, 检测方法:

——Portal 主动检测。用户和 Portal 之间周期性的传送保活页面, 在定义时间内未接收到保活页面请求 (默认为 5 分钟, 用户可配置), Portal 认为该用户已经下线。

——NAD 流量检测。NAD 检测 NAC 发出的流量, 在定义时间 (默认为 5 分钟, 用户可配置) 内未接收到任何流量, NAD 认为用户已经下线。

Portal 主动检测 NAC 被动退出流程如图 10 所示。

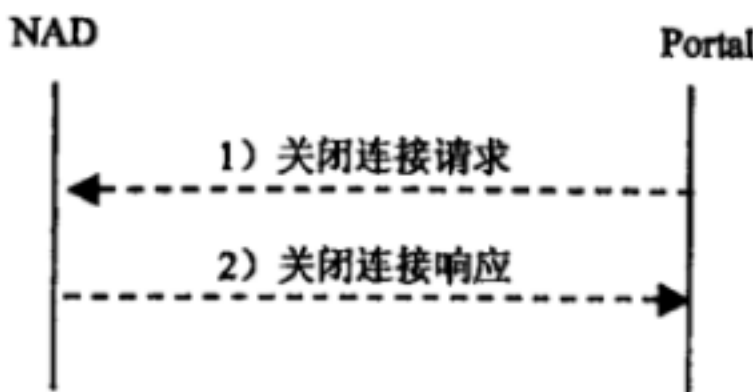


图10 NAC被动退出流程

- 1) Portal 向 NAD 发送用户退出关闭连接请求。
 - 2) NAD 收到 Portal 的关闭连接请求后，向 Portal 返回用户退出的关闭连接响应，用户下线。
- NAD 检测 NAC 被动退出流程：

NAD 通过流量检测发现 NAC 下线，关闭受控逻辑端口。

4.3.3 NAC 强制退出流程

NAC 强制下线是指 NAD 提供命令行强制切断用户连接，或者由于外部事件所引起的 NAC 设备发现用户已经异常，则需要及时通告 Portal。NAC 强制退出流程如图 11 所示。

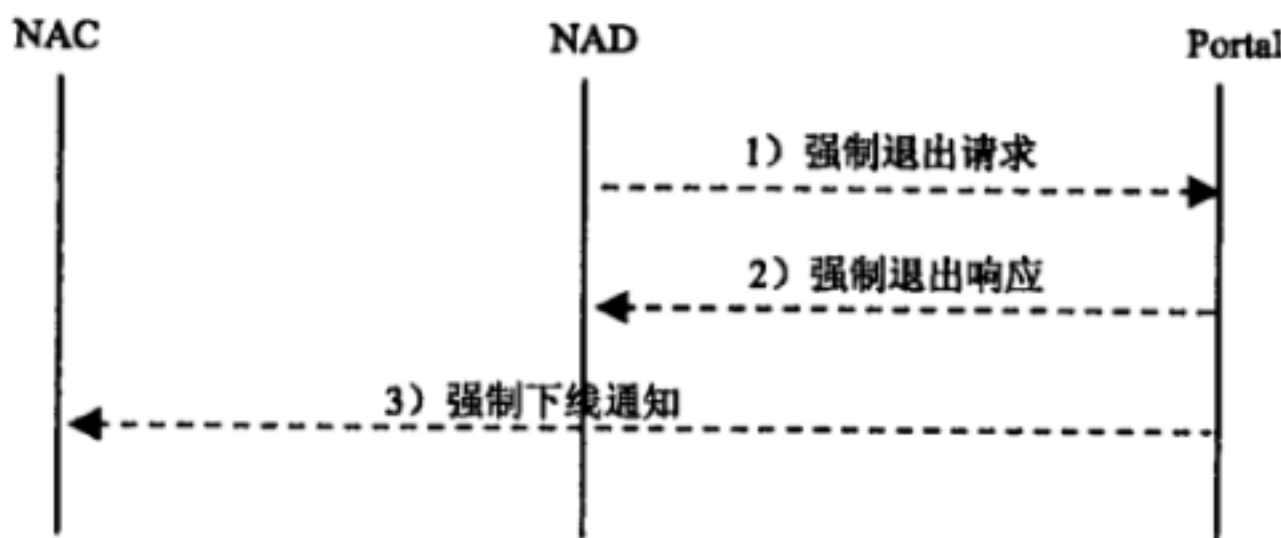


图11 NAC强制退出流程

- 1) NAD 设备向 Portal 发送强制退出请求报文通知用户已经下线。
- 2) Portal 收到强制退出请求报文，向 NAD 发送强制退出响应报文。
- 3) Portal 向 NAC 下发强制下线通知。

5 消息格式和编码

5.1 NAC 与 Portal 之间的消息格式和编码

Portal作为Web服务器，NAC与Portal之间采用HTTP协议进行通信，为增强安全性两者之间通信宜使用HTTPS协议。基本消息格式是URL+CGI参数（https://[Portal URL]/index.jsp?switch_ip=[switch ip]&switch_port=[switch port]）。表1给出NAC与Portal之间CGI参数中的参数名称、类型和编码方式。

表 1 NAC 和 Portal 之间的 CGI 参数表

名称	编码	说明	性质
NAD_IP	字符串如：202.112.50.112	NAD 的 IP 地址，即交换机的 IP 地址	结构 1 必选，结构 2 和 3 可选
NAD_Port	字符串如：FastEthernet0/15	有线网络中，NAC 连接到 NAD 的端口号	结构 1 必选，结构 2 和 3 可选
Mac	字符串如：22ab-ef3c-ea3a	NAC 的 MAC 地址	可选
VLAN_ID	字符串如：110	交换机端口所属的 VLAN 号	可选
URL	字符串如：www.sina.com.cn	用户最初要访问的 Web 服务器的 URL	可选

5.2 认证客户端与认证服务器之间的消息格式和编码

在结构1中, Portal与认证服务器之间采用标准的认证协议进行通信, 如RADIUS协议, 使用的RADIUS属性参见附录A。

5.3 NAD 与 Portal 之间的消息格式和编码

NAD与Portal之间有两种可行的通信方式:

1) HTTPS 协议。NAD 与 Portal 采用 HTTPS 协议通信, 需要 NAD 启用 Web 服务器功能。NAD 与 Portal 之间 HTTPS 协议基本的消息格式是 URL+CGI 参数的形式, 如:

https://[NAD URL]/index.jsp?portal_ip=[portal ip]

2) Portal 协议。NAD 与 Portal 之间可以使用 Portal 协议, 基于 UDP 协议进行通信。

Portal 协议主要描述了Portal和NAD设备之间的包交互, 主要内容包括如下三个方面:

a) 协议主体涉及 Portal 和 NAD 设备;

b) 协议采用非严格意义上的 Client/Server 结构, 大部分消息采用 Request/Response 形式进行交互。同时还定义了一种 Notify 报文, 提供 Portal 认证客户端和 NAD 设备间的消息通道。该类报文有两种, 一种是 Portal 发往 NAD 设备的, 另一种是 NAD 设备发往 Portal 的。

c) 承载协议。本标准中定义的承载协议基于 UDP。

Portal 协议承载在 UDP 上, 协议包采用固定长度头和可变长度的属性字段组成。属性字段采用 TLV 的格式, 格式如图 12 所示。

0	1	2	3	4	5	6	7
Ver	Type Pap/Chap		Rsvd	SerialNo		ReqID	
UserIP				UserPort		ErrCode AttrNum	
Authenticator							
Attributes*****							

图 12 Portal 协议报文格式

Portal 报文各属性说明:

- 1) Ver:
协议版本号, 1 字节。
- 2) Type:
报文的类型, 1 字节。
- 3) PAP/Chap:
用户的认证方式, 1 字节。
- 4) Rsvd:
保留字段, 1 字节。
- 5) SerialNo:
保留字段, 2 字节。
- 6) ReqID:
保留字段。2 字节。
- 7) UserIP:

接入用户的 IP 地址，4 字节。

8) UserPort:

接入用户的端口信息，2 字节。

9) ErrCode:

NAD 设备通知 Portal Server 用户认证的状态，1 字节。

10) AttrNum:

表示其后边可变长度的属性字段属性的个数，1 字节。

11) Authenticator:

验证字的长度固定为 16 字节，网络字节顺序。

12) 报文属性字段 (Attr):

Attr 字段 (属性字段) 是一个可变长字段，由多个属性依次链接而成，每个属性的格式为 TLV 格式，由属性类型 (AttrType)、属性长度 (AttrLen) 和属性值 (AttrValue) 三个字段构成。属性字段主要有用户名、用户的明文密码、用于标识 NAD 设备的 IP 地址。

6 级联、哑终端与直通问题

6.1 交换机级联的问题

在以太网中，可能存在支持 Web 认证的交换机下联一个不支持 Web 认证的交换机或者集线器的情况，其网络拓扑如图 13 所示。图中白色的 NAD 图标表示支持 Web 认证的交换机，而灰色的 NAD 图标表示不支持 Web 认证的交换机。

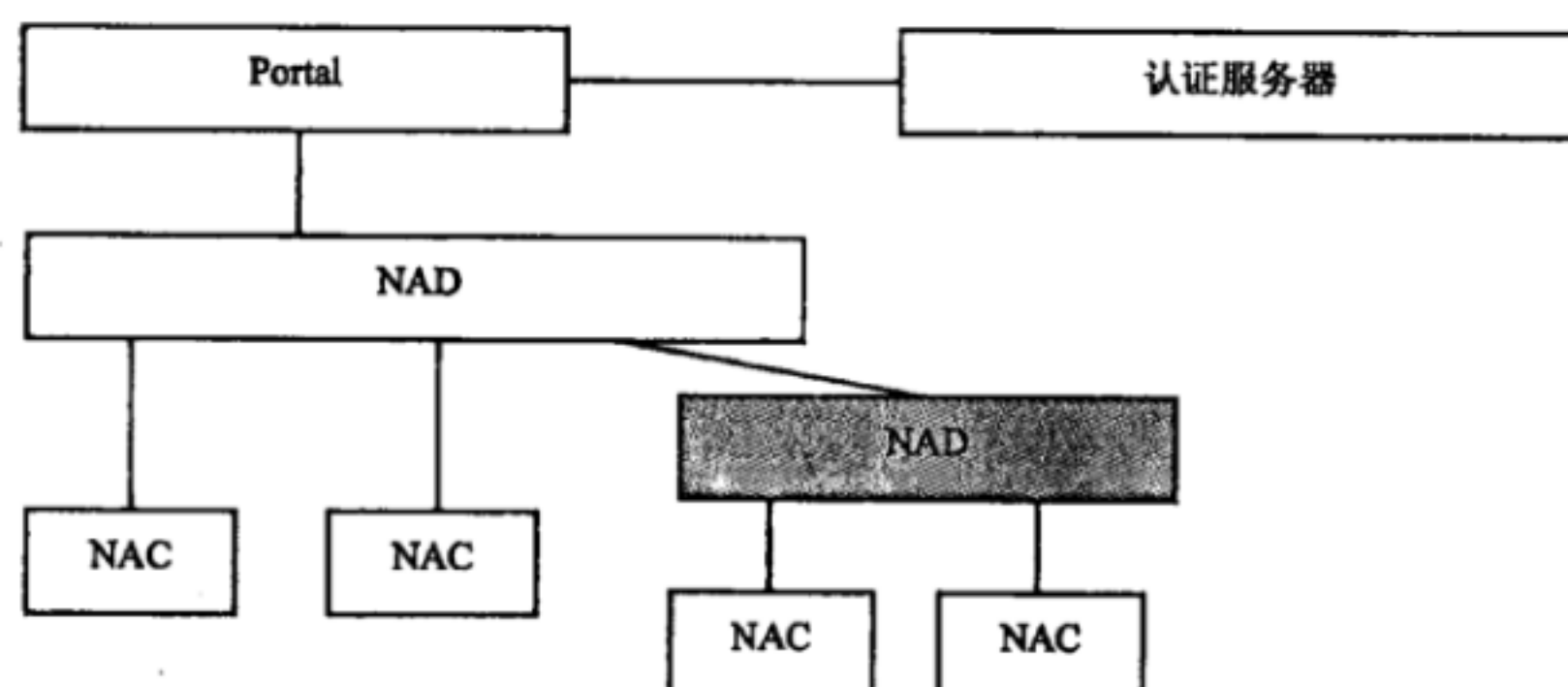


图 13 交换机级联问题的网络拓扑

在该情况下，支持 Web 认证的交换机需要支持基于 Mac 地址的网络接入身份认证，这样，不支持 Web 认证的交换机或集线器被看作是透明传输，不对身份认证结果产生影响。

6.2 哑终端设备的问题

在以太网中，可能存在打印机、VoIP 设备等哑终端设备。哑终端设备无法使用浏览器进行基于 Web 的接入身份认证，因此，建议采用“MAC 地址免认证”方式完成哑终端设备的身份认证。

6.3 直通协议

为支持基于 Web 的接入身份认证，需要 NAC 满足一定的网络基础条件。NAC 需要以手动配置或者自动配置的方式预先获得 IP 地址，且能够进行地址解析，使得浏览器能够正常发起网络的请求。为此，需要 NAD 允许 ARP 协议、自动地址配置协议（包括 DHCP 协议、IPv6 下的 SLAAC 协议和 DHCPv6 协议）以及 DNS 协议报文通过，这些协议统称为直通协议。

6.4 直通地址

为支持基于Web的接入身份认证，需要NAC具备一定的网络访问能力，NAC需要正常访问网关地址和Portal服务器地址。因此，需要NAD允许访问这些地址的报文通过，这些地址统称为直通地址。

7 安全性考虑

本标准主要存在下面几种可能的安全问题：仿冒攻击、嗅探攻击、NAD的安全性、Web服务器的安全、其他类型的攻击等。

7.1 仿冒攻击

a) 恶意用户可能通过仿冒 IP 地址来盗取服务，可通过 Portal 下发的认证 cookie 来解决。用户访问 Portal 时需要携带认证 cookie，如果用户的 IP 地址与认证 cookie 中包含的 IP 地址字段不一致，说明该地址是仿冒的。但是如果用户同时仿冒 IP 地址和认证 cookie，该安全方法将无效。

b) 恶意用户可能仿冒 Portal 向 NAD 发送打开端口等控制命令。

c) 恶意用户仿冒 NAD 向 Portal 发送用户退出请求等控制命令，可通过 NAD 和 Portal 之间设置共享密钥来解决。

7.2 嗅探攻击

在NAC和Portal之间采用HTTPS协议通信能够有效地避免这一问题。

7.3 NAD 的安全性

在本标准中，NAD作为网络设备，面临着网络攻击的风险，因此，宜通过在NAD上采用限制TCP连接数的方法，将单个NAC的最大TCP连接数设为500。

7.4 Web 服务器的安全

在本标准中，Portal提供Web服务器的功能，因此需要保证Web服务器的安全。

对于针对Web服务器的攻击，可以采取现有的安全防范措施来解决，不属于本标准的讨论范围。

7.5 其他攻击

NAD为支持Web认证的功能，必须允许一些特定的协议，比如直通协议通过，这会产生特定的安全问题，例如，在身份认证前，允许ARP协议通过，会造成ARP攻击的问题。

对于这些类型的攻击，可以针对性地采取现有的安全防范措施来解决，不属于本标准的讨论范围。

附 录 A
(资料性附录)
RADIUS属性列表

A.1 Access-Request认证请求包

属性名	属性编号	格式	具体定义
User-Name	1	string	必选。 被认证的用户名称
User-Password	2	string	必选。 用户用来认证的用户密码
CHAP-Password	3	string	可选。 该属性表示 PPP 挑战握手认证协议 (CHAP) 的用户回应的挑战值
Service-Type	6	integer	必选。 1. 该属性表示用户请求的服务类型, 或者 NAD 准备提供的服务类型。 根据 RADIUS 定义, 普通用户认证时该属性的取值为帧服务(Framed)。 2. 帧服务(Framed)
Framed-Protocol	7	integer	可选。 当前标准协议没有能很好的区别 PPPoE 和 VLAN, 暂时都填成 PPP。 点对点协议(PPP)
Framed-IP-Address	8	address	可选。 该属性表示配置给用户的 IP 地址
Framed-MTU	12	integer	可选, EAP 认证时需要 最大传输单元。范围: {64..65535}
Login-IP-Host	14	address	可选 Login 主机 IP 地址
State	24	string	必选。 在线重认证时必须使用
Calling_Station_Id	31	string	可选。 用户 MAC 地址
Proxy-State	33	string	可选。 认证漫游时必须提供
CHAP-Challenge	60	string	可选。 用于 CHAP 认证, 即使 Challenge 为 16 字节, 也应该在 Authenticator 和本属性中同时填入, 因为不同的服务器可能从请求包的不同地方去取 该值并进行 CHAP 认证
Message-Authentic ator	80	string	可选 EAP 认证时必须使用
Framed-IPv6-Prefix	97	string	可选 登录用户的 IPV6 地址的前缀 (IPV6 网络环境下使用)
Login-IPv6-Host	98	address	可选 用户登录到设备的 IPV6 地址 (IPV6 网络环境下使用)

A.2 Access-Accept认证接受包

属性名	属性编号	格式	具体定义
User-Name	1	string	可选。 被认证的用户名称
Service-Type	6	integer	可选。 1. 该属性表示用户请求的服务类型，或者 NAD 准备提供的服务类型。根据 RADIUS 定义，普通用户认证时该属性的取值为帧服务 (Framed)。 2. 帧服务(Framed)
Reply-Message	18	string	必选。 认证响应信息。可以用于设备上的调试信息，在使用 PPPoE/Web 认证时可以向用户显示接入失败的原因
Termination_Action	29	integer	可选。 指示业务结束后的处理方式
Proxy-State	33	string	可选。 漫游认证时必须使用
Message-Authenticator	80	string	可选。 EAP 认证时使用
Framed-IPv6-Prefix	97	string	可选 登录用户的 IPV6 地址的前缀 (IPV6 网络环境下使用)
Login-IPv6-Host	98	address	可选 用户登录到设备的 IPV6 地址 (IPV6 网络环境下使用)

A.3 Access-Reject认证拒绝包

属性名	属性编号	格式	具体定义
Reply-Message	18	string	必选。 认证响应信息。可以用于设备上的调试信息，在使用 PPPoE/Web 认证时可以向用户显示接入失败的原因

附录 B
(资料性附录)
典型应用场景和参考实现

图 B.1 显示一个典型的局域网应用场景，包含有 DHCP 服务器、DNS 服务器，以及进行 Web 身份认证需要的交换机、Portal 和 RADIUS 服务器，用户只有通过 Web 身份认证后才能够访问互联网。

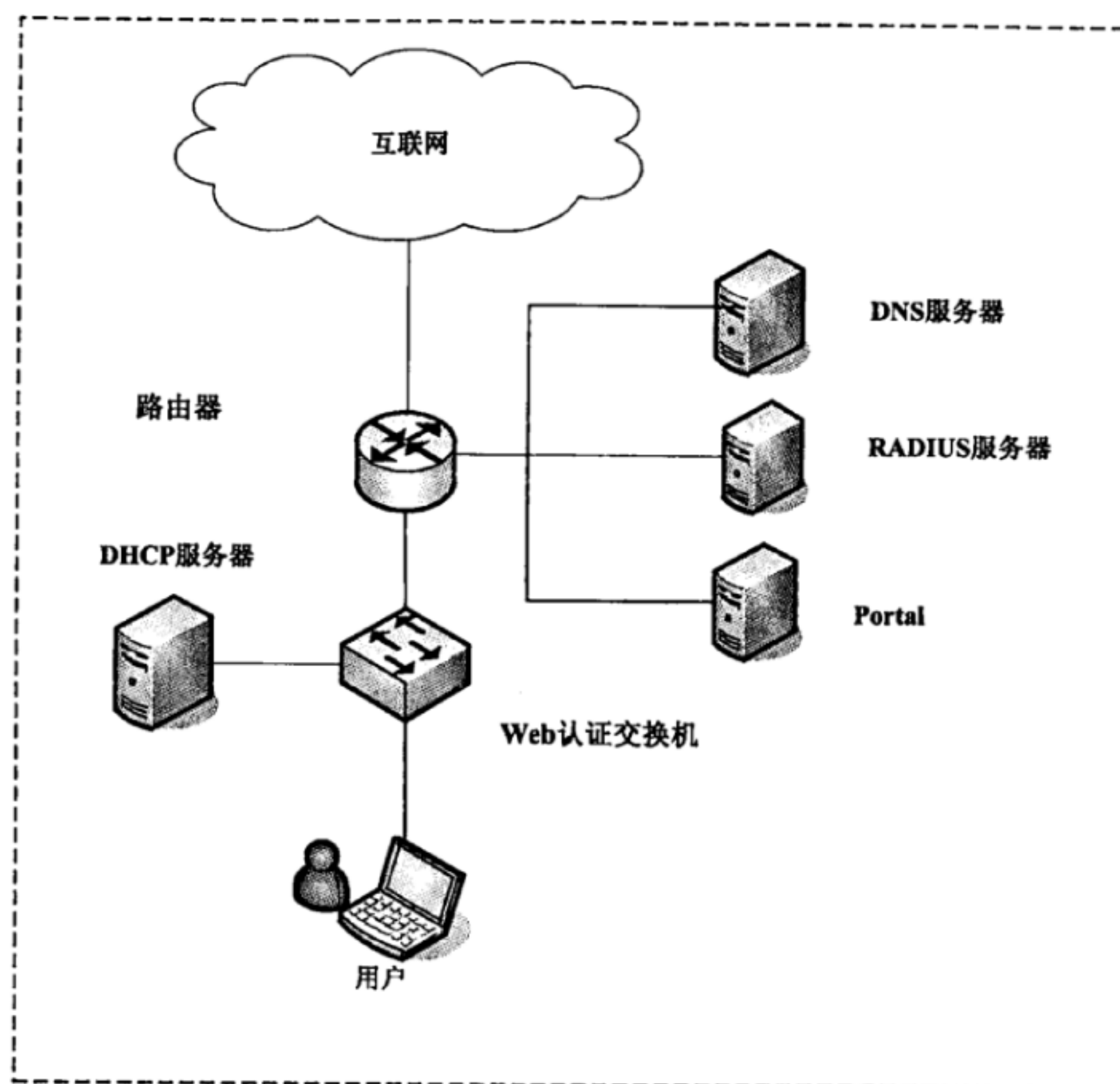


图 B.1 典型应用场景

通过一个用户身份认证、上网、下线完整的网络访问流程，给出一个具体的参考实现。

a) 用户在浏览器中输入 `www.baidu.com`，来请求访问外网网页。输入的 URL 为：

`http://www.baidu.com`

b) Web 认证交换机截获到该访问请求，由于该用户未认证，因此交换机向浏览器发送重定向响应，重定向地址为 Portal。重定向 URL 为：

`https://[url of portal]/index.jsp?switch_ip=192.168.1.1&switch_port=11&mac=002c2afe3c&url=www.baidu.com`

c) 用户浏览器根据重定向地址访问 Portal。

d) Portal 返回一个登录页面。

e) 用户输入用户名/密码，并以 GET 或者 POST 方式提交到 Portal。

`https: //[url of portal]/index.jsp?username=test&password=test&switch_ip=192.168.1.1&switch_port=11&mac=002c2afe3c&url=www.baidu.com`

f) Portal 接收到用户名/密码信息, 其集成的 RADIUS 客户端组件将用户名/密码组装成 RADIUS Access-Request 报文, 向 RADIUS 服务器请求认证用户身份。

g) RADIUS 服务器返回 RADIUS Access-Accept 或者 Access-Reject 报文, 表明身份认证结果。

h) 如果认证成功, Portal 打开交换机的端口, 允许该用户访问网络。打开交换机端口的命令为:

`http: //[url of switch]/openport.htm?switch_port=11&mac=002c2afe3c`

同时, 将用户的浏览器重定向到最初访问的 URL, 即 `www.baidu.com`。

i) 用户上网期间, 浏览器周期性的向 Portal 发送保活页面, 保活页面的 URL 表示为:

`http://[url of portal]/keepalive.htm&mac=002c2afe3c`

j) 用户结束上网, 向 Portal 发送断开网络连接的请求, 请求 URL 为:

`http://[url of portal]/close.htm&mac=002c2afe3c`

Portal 关闭交换机对应的端口。关闭交换机端口的命令为:

`http: //[url of switch]/closeport.htm?switch_port=11&mac=002c2afe3c`

中 华 人 民 共 和 国
通 信 行 业 标 准
基于 WEB 的以太网接入身份认证技术要求
YD/T 2667-2013

*

人民邮电出版社出版发行
北京市丰台区成寿寺路 11 号邮电出版大厦
邮政编码: 100164
宝隆元(北京)印刷技术有限公司印刷
版权所有 不得翻印

*

开本: 880×1230 1/16 2014 年 2 月第 1 版
印张: 1.5 2014 年 2 月北京第 1 次印刷
字数: 36 千字

15115 • 369

定价: 20 元

本书如有印装质量问题, 请与本社联系 电话: (010)81055492