

ICS 33.040.40

M 32

**YD**

# 中华人民共和国通信行业标准

YD/T 1908-2009

---

## 基于可扩展认证协议（EAP）的 动态地址分配扩展协议（DHCP+） IP 网接入认证鉴权技术要求

AAA Technical Requirements for Public IP network  
——Access Control by DHCP+ based on EAP

2009-06-15 发布

2009-09-01 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 规范性引用文件	1
3 术语、定义和缩略语	1
4 系统结构	2
5 组网模型	3
6 通信流程	5
7 通信协议	9
附录 A (资料性附录) NAT 支持方案	18
附录 B (资料性附录) 防伪 DHCP 检测方案	20
附录 C (资料性附录) 用户业务选择与带宽控制方案	22
附录 D (资料性附录) 相关设备要求	23
附录 E (资料性附录) 推荐的配置与性能参考实例	27
附录 F (资料性附录) 受限地址资源考虑	28
附录 G (资料性附录) 重放攻击的防范	29

## 前 言

本标准是公众 IP 网络安全要求系列标准之一，本系列的标准结构和名称预计如下：

1. YD/T 1613-2007 公众 IP 网络安全要求——安全框架
2. YD/T 1614-2007 公众 IP 网络安全要求——基于数字证书的访问控制
3. YD/T 1615-2007 公众 IP 网络安全要求——基于远端接入用户验证服务协议（RADIUS）的访问控制
4. 公众IP网络安全要求——基于802.1x的访问控制要求
5. 基于EAP的动态地址分配扩展协议（DHCP+）IP网接入认证鉴权技术要求

本标准的附录 A、附录 B、附录 C、附录 D、附录 E、附录 F、附录 G 均为资料性附录。

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：北京润汇科技有限公司、工业和信息化部电信研究院、上海贝尔阿尔卡特股份有限公司、华为技术有限公司

本标准主要起草人：姚宏亮、聂秀英、佟立群、王 地、陈 晓、厉益舟

# 基于可扩展认证协议（EAP）的动态地址分配扩展协议（DHCP+） IP 网接入认证鉴权技术要求

## 1 范围

本标准规定了基于EAP的DHCP+ IP网络接入认证系统的体系结构、组网方式、通信流程，通信协议以及对相关设备的要求。

本标准适用于链路层采用IEEE 802局域网技术、xDSL技术和HFC技术的公用IP接入网，也适用于基于EAP的DHCP+认证、鉴权软件和设备。本标准不适用于IPv6网络环境。

## 2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

IETF RFC 1938 (1996)	一次性密码 (OTP) 系统
IETF RFC 2284 (1998)	PPP 可扩展认证协议 (EAP)
IETF RFC 3046 (2001)	DHCP 中继代理信息选项协议 (DHCP option 82)

## 3 术语、定义和缩略语

### 3.1 术语和定义

下列术语和定义适用于本标准。

#### 3.1.1

##### 受限地址

某一范围的IP地址（通常为私有地址），获取受限地址的接入用户仅能访问被资源提供者定义为受限的网络资源。

#### 3.1.2

##### 非受限地址

某一范围的IP地址（可以使用公网地址或私有地址），获取非受限地址的接入用户，可以访问资源提供者所提供的相应网络资源。

### 3.2 缩略语

下列缩略语适用于本标准。

AAA	Authentication, Authorization and Accounting	认证、鉴权和计费
ACL	Access Control List	访问控制表
ADSL	Asymmetric digital subscriber line	非对称数据用户业务线
CHAP	Challenge Handshake Authentication Protocol	质询握手认证协议
CMTS	Cable modem termination system	同轴电缆调制解调器终结系统

DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DSLAM	Digital Subscriber Line Access Multiplexer	数字用户线接入复用器
EAP	Extensible Authentication Protocol	可扩展认证协议
EAPOR	EAP over Radius	RADIUS协议承载的EAP
ECP	ENUS Control Protocol	ENUS控制协议
ENUS	EtherNet User Management System	以太网用户管理系统
HMAC	Keyed-Hashing for Message Authentication	用于信息身份验证的密钥-散列算法
LAN	Local Area Network	局域网
MAC	Media Access Control	媒体访问控制
MIB	Management Information Base	管理信息库
NAT	Network Address Translation	网络地址转换
PAE	Port Access Entity	端口接入实体
PAP	Password Authentication Protocol	密码认证协议
PAT	Port Address Translation	端口地址转换
PPP	Point-to-Point Protocol	点对点协议
RADIUS	Remote Authentication Dial In User Service	远端拨入用户认证服务
SNMP	Simple Network Management Protocol	简单网络管理协议
SPEC	Standard Performance Evaluation Corp	标准性能评估公司
TLS	Transport Level Security	传输层安全
TPC	TransactionProcessing Performance Council	事务处理性能委员会
UDP	User Datagram Protocol	用户数据报协议
WLAN	Wireless LAN	无线局域网

#### 4 系统结构

本标准规定的认证系统由 DHCP 服务器和 ECP 认证服务器组成，客户端和认证系统之间使用 ECP 协议和标准 DHCP 协议，如图 1 所示。

当用户端（用户客户端）接入网络时，首先按照 DHCP 协议发出获得地址的请求（广播包），当认证系统接收到该请求后分配一个受限的网络地址给用户端，此受限地址根据网络层的三层设备上所设置的 ACL，限制用户端只能访问有限的网内资源；客户端成功接收到此受限地址后，向认证系统发送认证请求；认证系统接收到认证请求后通过 AAA 协议（如 RADIUS 协议）向 AAA 系统转发认证请求；当认证系统从 AAA 系统接收到认证成功消息后，认证系统给用户分配一个非受限的地址；用户端获取此地址后，与认证系统建立一个有效的会话连接。通过此连接，用户端定时向认证系统发送状态消息，认证系统根据收到的状态消息判断用户端是否处于激活状态。若连接中断意味着用户端已经退出，认证系统可以据此终止对此用户端的服务并回收相应的地址资源。

本标准是建立在 EAP-MD5 方法之上，融合用户认证、地址分配策略控制、用户会话控制等实现的应用部署灵活且具有高安全性的互联网接入认证管理协议，在本协议中并没有使用到 EAP 协议的全部特性；其中认证流程遵循的是 CHAP 协议，为了增强用户使用安全而采用重认证方式也同样遵循 CHAP 协议。

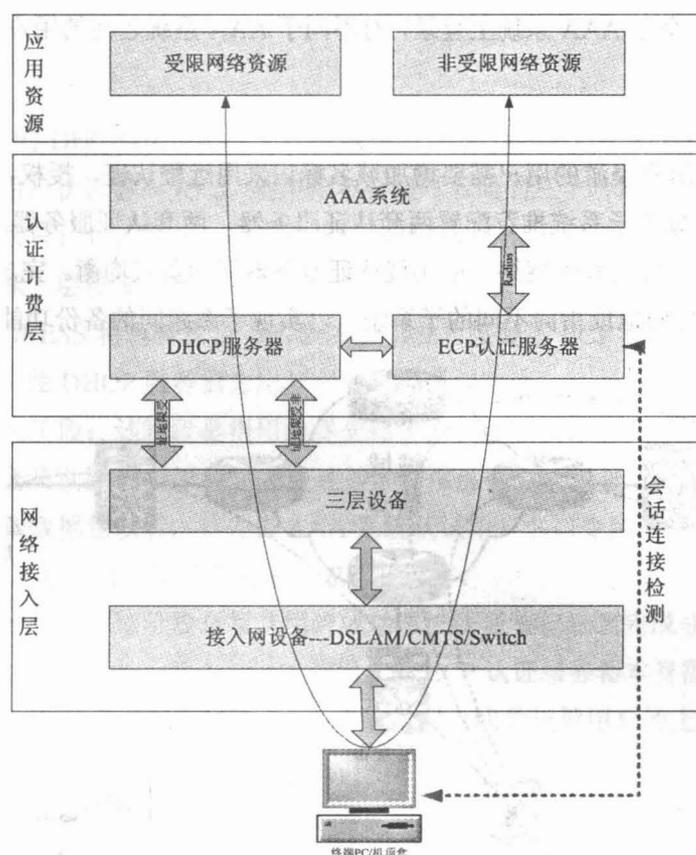


图1 系统结构

## 5 组网模型

### 5.1 概述

在实际配置中可采用集中式组网和分布式组网两种组网模式。集中组网模式是指在一个网络中仅配置一个集中的用户接入认证鉴权系统，该系统负责该网络上的所有用户的接入鉴权认证服务。分布式组网方式是指在一个网络中根据需要配置两个或多个用户接入认证鉴权系统，每个系统负责部分用户的接入认证鉴权服务，在提供用户漫游接入服务时，需配置一中心管理系统。

### 5.2 集中式组网模式

系统可以集中部署在网络任意交换机下，为全网各种接入方式提供接入认证服务。并且该系统可以通过增加服务器数量进行平滑扩展，如图 2 所示。

在这种部署方式中推荐配置两套认证服务器，两套认证服务器之间可以热切互备；这两套服务器通过四层交换机接入骨干网络，以实现服务器间的负载均衡。

### 5.3 分布式组网

左右两个子系统为独立的子系统。子系统是可以平滑扩展的。即可以建立任意多个，但是这些系统之间处理的用户群是不一样的，如图3所示。

子系统的内部的服务器数量在图中只是一个示意，是可以任意多的，取决于系统的性能要求。AAA系统采用本地数据库方式来为用户提供认证，授权，上下线操作。带来的业务影响包括：

1) 开户或者销户行为将变为准实时生效。在中心 AAA 系统发生了这些操作时，中心 AAA 系统将对应的 AAA 子系统发送更新消息。

2) 要求用户只能在一个子 AAA 系统上登录, 对不同于 AAA 系统之间的用户使用进行漫游限制。提供的策略一般为:

- 禁止漫游;
- 允许漫游, 但是所有漫游的用户需要增加域名标识采用远程认证, 授权, 上下线的方式进行。

在这种部署方式中, 每个子系统推荐配置两套认证服务器, 两套认证服务器之间可以热切互备; 这两套服务器通过四层交换机接入骨干网络, 以实现认证服务器间的负载均衡。完成 DHCPRELAY 的设备可以配置主备的 RELAY 目的地址指向不同的子系统, 以实现子系统间的备份功能。

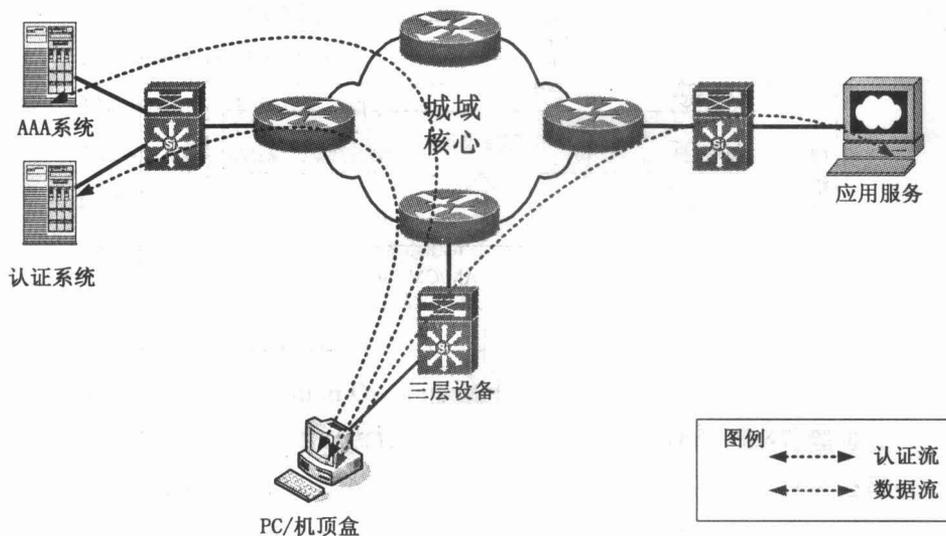


图2 集中式组网拓扑结构

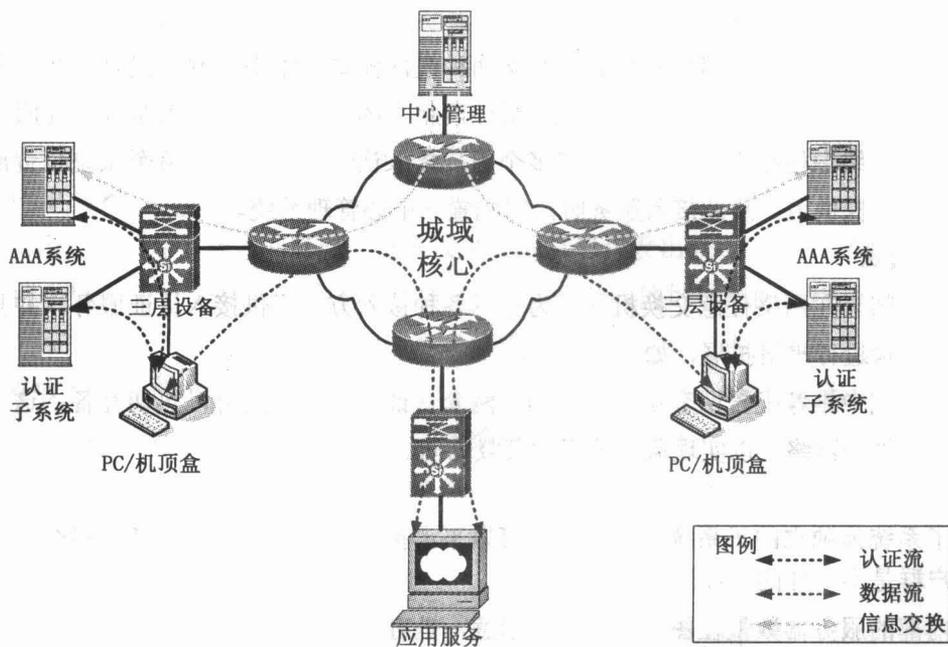


图3 分布式组网拓扑结构

## 6 通信流程

### 6.1 认证鉴权阶段

用户使用基于 EAP 的 DHCP+认证鉴权系统时包括如下 5 个阶段。后 3 个阶段是在用户成功地通过认证和鉴权后进行，若用户认证鉴权失败，则用户不会经过后面的三个阶段。

1) 分配受限地址阶段：该阶段为从用户请求连接到网络到用户获得受限地址为止的一个阶段。在该阶段中用户首先向边缘三层设备发送 DISCOVERY 消息，边缘三层设备收到该消息后，根据配置在端口上的 IP-HELPER-ADDRESS 将包转发给 DHCP 服务器并直接到达 ECP 认证服务器。ECP 认证服务器收到了用户的数据包以后使 DHCP 服务器为用户分配可用受限地址。

2) 用户认证和鉴权阶段：该阶段是指用户提交相关的认证鉴权信息到用户收到认证鉴权结果的阶段。在该阶段中，用户登录直接与 ECP 认证系统连接的前端通信，发送登录数据包给 ECP 认证服务器。ECP 认证服务器收到这个数据包以后，首先去 AAA 系统认证用户名口令和要求 AAA 系统为用户授权，这个调用的过程中，AAA 系统会调用数据库来完成这些操作。

3) 分配非受限地址阶段：该阶段是指从用户成功通过认证鉴权后到完成非受限地址分配的阶段。该阶段相比分配受限地址阶段，多了两个异步的调用，即 ECP 认证服务器本身需要异步调用数据库记录在线用户；另外一个 ECP 认证服务器通知 AAA 系统用户上线并记录用户的上线时间，AAA 系统会调用数据库完成这个操作。

4) 地址续租和会话阶段：该阶段是指获得了非受限地址的用户通过与 ECP 认证服务器之间交换用户状态信息以实现地址续租和会话连接刷新阶段。

5) 用户下线阶段：该阶段是指用户下线并释放非受限地址的阶段，在该阶段，除了接入子系统完成了用户下线修改权限的过程以外。还有三个异步操作，首先是 ECP 认证服务器异步调用数据库删除对应的在线用户的操作；其次 ECP 认证服务器会异步调用 AAA 系统的下线接口；最后 ECP 认证服务器系统会异步调用 AAA 系统的计费接口。AAA 系统和数据库之间都是同步调用。

### 6.2 分配受限地址阶段通信流程

用户获取受限 IP 地址通信流程如图 4 所示。

流程说明：

- 1) 客户端开机，发送 Discovery 请求，此请求中包括客户机的 MAC 地址；
- 2) 三层设备接收到请求后，转发给 DHCP 服务器；
- 3) DHCP 服务器将地址请求发给 ECP 认证服务器；
- 4) ECP 认证服务器根据客户机的 MAC 地址权限，返回该客户端应该获得的受限 IP 地址；
- 5) DHCP 服务器给用户分配受限 IP 地址；
- 6) 三层设备转发 Offer 包，客户机获取受限 IP 地址。

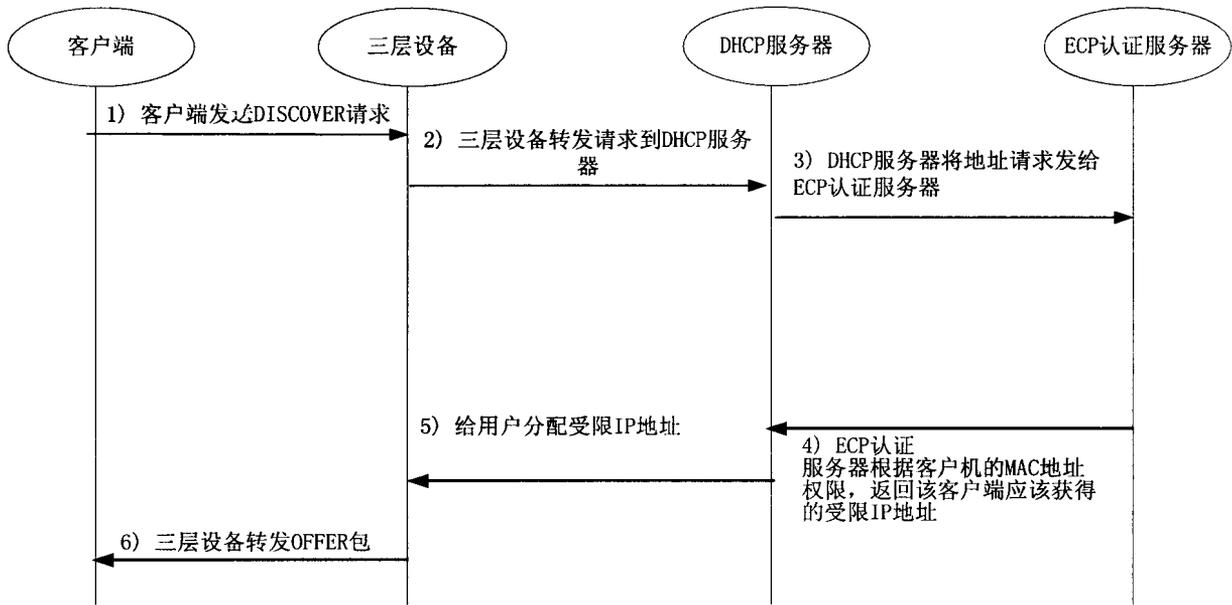


图4 用户获取受限 IP 地址通信流程

### 6.3 用户认证和鉴权阶段和分配非受限地址通信流程

用户认证、授权及上线通信流程如图 5 所示。

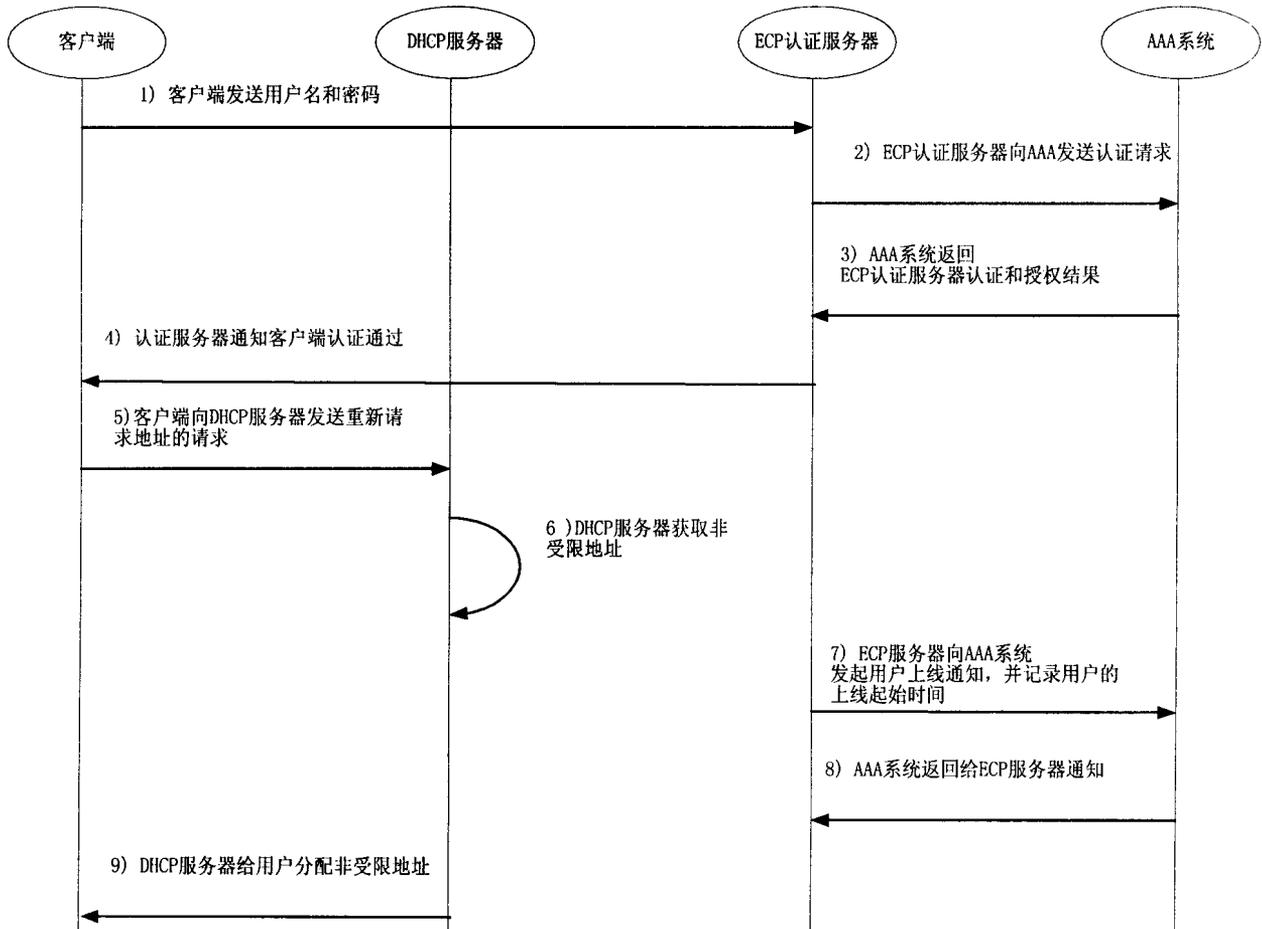


图5 认证、授权及上线通信流程

流程说明：

- 1) 启动客户端，输入客户端名和密码后，向 ECP 认证服务器发送认证请求。
- 2) ECP 认证服务器调用认证接口，向 AAA 系统发送认证请求；
- 3) 认证通过，AAA 系统返回 ECP 认证服务器认证和授权结果；
- 4) ECP 认证服务器通知客户端认证通过；
- 5) 客户端向 DHCP 服务器发送重新请求地址的请求；
- 6) DHCP 服务器获取非受限地址；
- 7) ECP 认证服务器向 AAA 系统发出用户上线通知，并记录用户的上线起始时间；
- 8) AAA 系统返回给 ECP 认证服务器通知响应；
- 9) DHCP 服务器给用户分配非受限地址。

其中 ECP 模块（处理 ECP 协议）与 DHCP 模块部署在一台服务器上，地址一致，客户端发起 ECP 认证后，由 ECP 模块给客户端返回任务分配服务器地址。

#### 6.4 地址续租和会话阶段通信流程

地址续租和会话连接刷新阶段通信流程如图 6 所示。

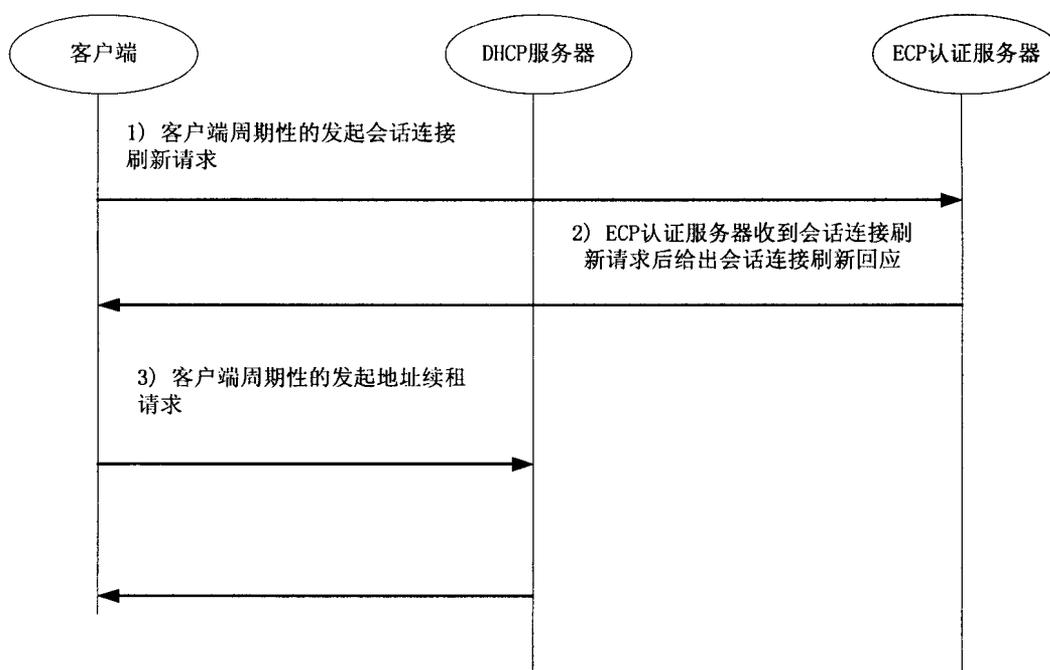


图6 地址续租和会话连接刷新阶段通信流程

流程说明：

- 1) 客户端周期性的发起会话连接刷新请求；
- 2) ECP 认证服务器收到会话连接刷新请求后给出会话连接刷新响应。
- 3) 客户端周期性的发起地址续租请求；
- 4) DHCP 服务器收到地址续租请求后给出地址续租响应。

会话连接刷新功能主要是完成主机是否在线的检测，也可以通过其它方式来实现，例如通过设备使用 ARP 问询方式定时检测主机是否在线，然后以带内或带外的方式通知 DHCP 服务器的方法来完成。

### 6.5 用户下线阶段通信流程

#### 6.5.1 用户正常下线通信流程

用户正常下线通信流程如图 7 所示。

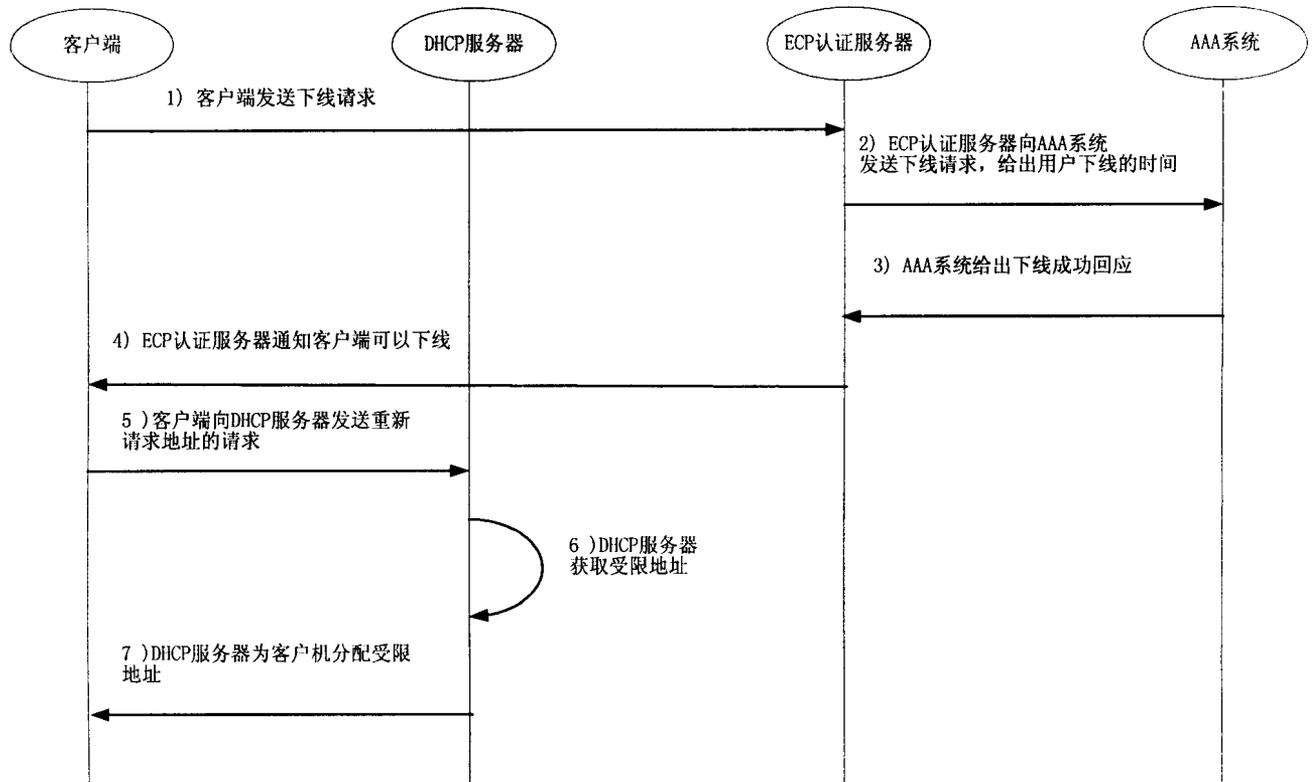


图7 用户正常下线通信流程

流程说明：

- 1) 客户端向 ECP 认证服务器发送下线请求；
- 2) ECP 认证服务器向 AAA 系统发送下线请求，并给出下线时间；
- 3) AAA 系统给出下线成功响应；
- 4) ECP 认证服务器通知客户端可以下线；
- 5) 客户端向 DHCP 服务器发送重新申请地址请求；
- 6) DHCP 服务器获取受限地址；
- 7) DHCP 服务器将分配的受限 IP 地址返回给客户端。

注：客户端下线以后通过在用户 PC 机上执行一条 DOS 下的 DHCP RENEW 命令来重新发起一个标准 DHCP 流程。

#### 6.5.2 用户异常下线通信流程

用户异常下线通信流程如图 8 所示。

流程说明：

- 1) ECP 认证服务器周期性的检测客户端的会话连接刷新是否收到，当 3 次没有收到客户端的会话连接刷新时，判定用户已经下线；
- 2) ECP 认证服务器向 AAA 系统发送下线请求，并给出下线时间；
- 3) AAA 系统给出下线成功响应；
- 4) ECP 认证服务器通知 DHCP 服务器，用户已经下线成功；

## 5) DHCP 服务器回收地址资源。

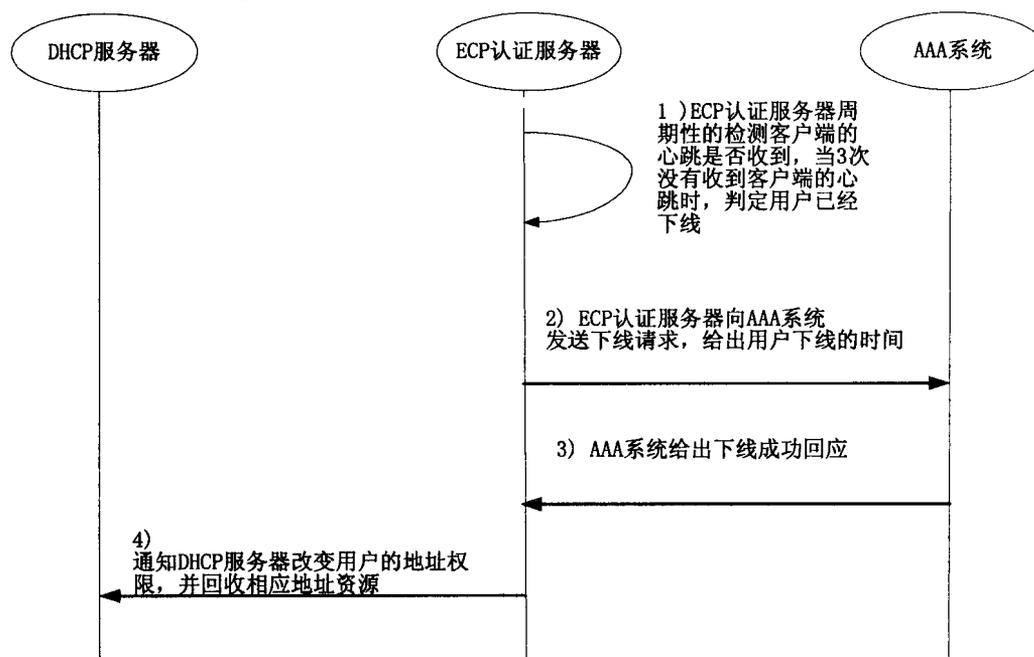


图8 用户异常下线通信流程

## 7 通信协议

## 7.1 协议概述

DHCP 扩展协议是在 DHCP 应用层面上扩展的一套协议。标准的 DHCP 协议只规定了用户的计算机如何获得 IP 地址, 没有提供认证、授权、计费等方法。为了适应网络运营的要求, 除了运行标准的 DHCP 协议之外, 采用网络应用层通信的方式传递用户、Session 等信息, 实现完整的认证、计费流程。这种 DHCP 协议加应用层协议的方式简称 DHCP 扩展协议。DHCP 扩展接入认证技术相对于标准的 DHCP 协议相比, 做了以下的扩展。

1) 引入了多权限地址的概念, 即在一个三层设备端口下, 用户可以根据不同的权限情况得到不同的 IP 地址池中的地址。

2) 引入了用户的业务使用流程, 即打通了用户 AAA 流程和 DHCP 流程之间的关系, 通过 MAC+物理端口来表示一个用户, 在用户登录以后改变 MAC+物理端口的权限, 为其变化对应的 IP 地址。

3) 用户采用 ECP 协议遵循 CHAP 流程完成基于用户名和用户口令的认证, ECP 认证服务器根据认证结果授权 DHCP 服务器为用户分配受限或非受限地址。

4) 完成了用户使用时长的采集, 即通过和用户之间定义采集时长信息的协议, 完成了开始使用到终止使用的时长确认。

## 7.1.1 协议构成

通过客户端与 ECP 认证服务器协同通讯完成用户的认证、授权和计费, 使用 UDP 协议传送 ECP 协议数据单元; 同时配合使用动态主机配置协议在 TCP/IP 宽带网络上使客户机获得网络配置信息。

服务器端 UDP 监听端口为 2167。如图 9 所示, ECP 协议数据单元由固定长度的头部分和可变长度的属性域部分组成。头部分规定了数据包的版本号、类型等信息, 属性域规定了各种属性的值。

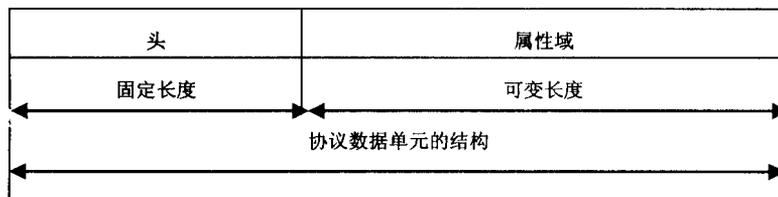


图9 ECP 协议数据单元组成

本标准规定了如下 8 个协议数据单元类型，见表 1。

表 1 MSG\_TYPE 说明

序 号	协议数据单元	源 端	宿 端	取 值
1	分配任务请求 (RequestTask)	客户端	ECP 认证服务器端	1
2	返回任务分配列表 (TaskRes)	ECP 认证服务器端	客户端	2
3	用户身份认证请求(LogonReq)	客户端	ECP 认证服务器端	3
4	用户身份认证响应(LogonRes)	ECP 认证服务器端	客户端	4
5	发送会话连接刷新请求(HeartbeatReq)	客户端	ECP 认证服务器端	5
6	会话连接刷新请求响应(HeartbeatRes)	ECP 认证服务器端	客户端	6
7	用户下网请求(LogoffReq)	客户端	ECP 认证服务器端	9
8	用户下网请求响应(LogoffRes)	ECP 认证服务器端	客户端	10

### 7.1.2 客户端状态转移

客户端的状态转移图如图 10 所示。图中文字的有关定义如下。

1) 超时重发：客户端发出数据包后等待服务器响应。在等待一定的时间没有响应的情况下，重新发送数据包。

2) 重发超次：客户端超时重发数据包，在重发了一定次数之后，超过规定的次数。

3) 成功/失败：客户端正确接收到了服务器的响应包，响应包中标识客户端请求的结果。

图10中的实线表示所发生的事件造成的状态转移。

客户端从 Init 状态开始，向任务分配服务器发送 RequestTask 消息，收到 RaskRes 消息后，进入 Offline 状态。这时，客户端知道了 ECP 认证服务器的 IP 地址。

客户端登录上网，向 ECP 认证服务器发送 LogonReq 消息，ECP 认证服务器要求采用 MD5-challenge 方式进行认证，同时发送 challenge 到客户端。客户端将密码加密的结果发送到 ECP 认证服务器，接收到成功的消息后进入到 Online 状态。如果接收到认证失败的消息，客户端重新回到 Offline 状态。

客户端在 Online 状态中，每隔 HeartbeatInterval 时间发送一个会话连接刷新包。在 Client-Timeout 时间没有接收到会话连接刷新的情况下，客户端下网，返回到 Init 状态。

客户端在 Online 状态，用户进行下网操作，发送 LogoffReq 消息到 ECP 认证服务器，在接收到 LogoffRes 后下网。如果一定时间后没有接收到 LogoffRes 消息，超时重发 LogoffReq 消息。在重发超次后，客户端下网。客户端从 Offline 状态转移到 Init 状态。

客户端的退出应当从 Init 或者 Offline 状态下退出。

在状态 Selecting、Requesting、Challenging、Logoff-waiting 中，如果在一定时间内没有接收到 ECP 认证服务器的响应，应重新发送消息。

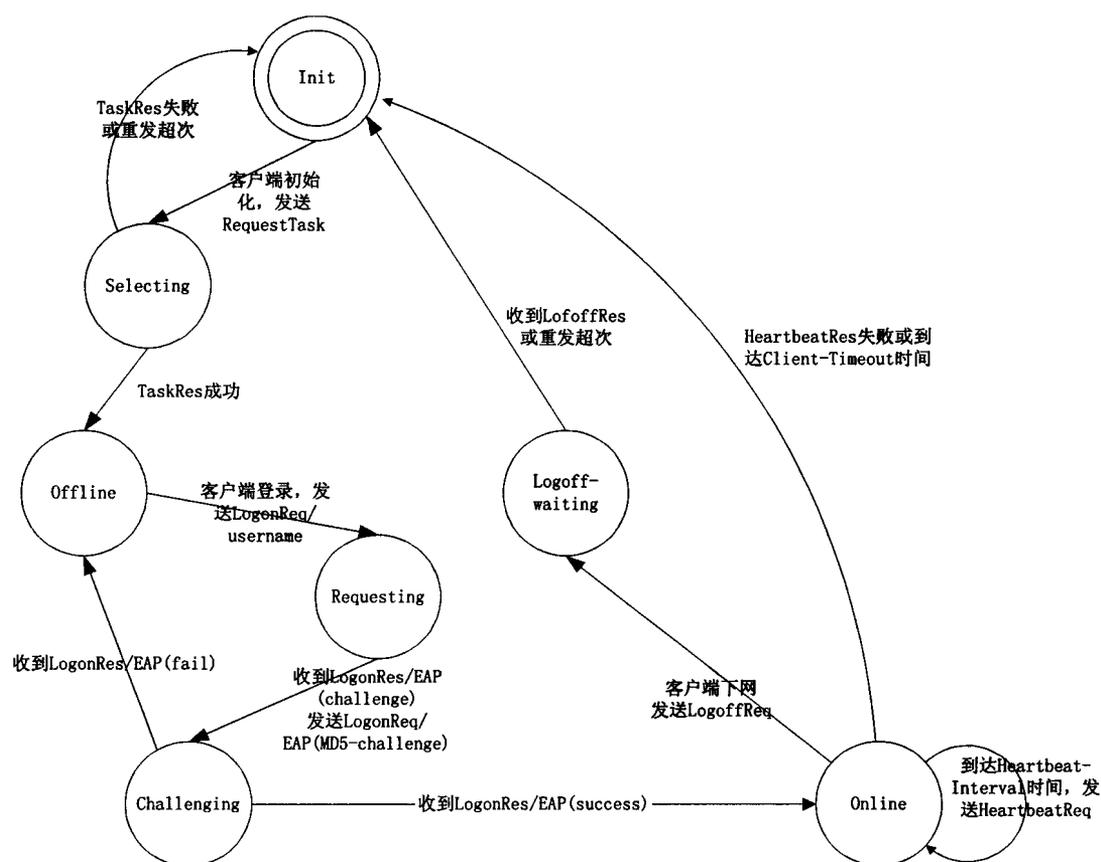


图10 客户端状态转移图

### 7.1.2.1 重发机制

网络传输的不可靠性，会发生数据包的丢失。由于本协议采用 UDP 的传输方式，因此在丢包的情况下，客户端应当具有自适应性，提供重发机制，保证网络接入的质量。同时，客户端不能发送过多的数据包，造成系统过大的压力，危害系统的稳定性。

客户端的 RequestTask、LogonReq 和 LogoffReq 都应当有重发机制，重发的间隔不能少于 10s，重发次数不能大于 3。

客户端的会话连接刷新报文不采用重发机制。在 ECP 认证服务器返回会话连接刷新间隔属性的情况下，一直按照该间隔发送会话连接刷新。否则按照默认的会话连接刷新间隔发送。在客户端没有接收到 ECP 认证服务器会话连接刷新请求响应的情况下，发送会话连接刷新间隔不变，直到会话连接刷新超时或者得到响应。

### 7.1.2.2 异常数据的处理

对于格式不符合协议标准的数据包，包括包头格式不对、属性域长度与实际长度不符等情形，该数据包将被简单丢弃。

为了保证协议的向后兼容性，对于符合协议格式、但是属性类型无法识别的情形，该属性被忽略，仅对已知的属性类型进行解析、操作。

### 7.1.3 认证方式

采用 challenge 的认证方式具有安全、防止重放攻击的特点，它可以有效地避免密码在网络中传输所

造成的密码泄漏等问题。本标准规定所有的 MD5-challenge 认证数据都是在 EAP 的数据包进行传输的。EAP 的格式见表 2。

表 2 EAP 的格式

Code (1)	Identifier (1)	Length (2)	Data
----------	----------------	------------	------

其中：

Code 的长度为一个字节，表明 EAP 的类型。指定的类型如下：

- 1 Request
- 2 Response
- 3 Success
- 4 Failure

Identifier 长度为一个字节，用来帮助匹配 request 和 response。

Length 为 EAP 数据包的总长度，包括 Code、Identifier、Length 和 Data。

Data 的长度为 0 或多个字节，具体的格式由 Code 域的值决定。

在 Code 为 request 和 response 的时候，EAP 的格式见表 3。

表 3 Code 为 request 和 response 时 EAP 的格式

Code (1)	Identifier (1)	Length (2)	Type(1)	Type-data
----------	----------------	------------	---------	-----------

其中 type 为一个字节，表明 request/response 的类型。定义的 type 类型如下：

- 1 Identity
- 2 Notification
- 3 Nak (Response only)
- 4 MD5-Challenge
- 5 One-Time Password (OTP) (RFC 1938)
- 6 Generic Token Card

具体 EAP 数据的封装参见 RFC2284。认证过程中 EAP 数据的传递放在 EAP 数据属性中。采用 MD5-challenge 的认证交互过程如下。

1) 首先客户端发送的认证请求中包括用户名属性。

2) ECP 认证服务器接收到认证包后，根据用户名产生一串随机数，作为 challenge，在 EAP 数据属性中返回，其中 EAP 的 code 为 request，type 为 MD5-challenge 方式。数据属性格式见表 4。

表 4 数据属性格式

Code	Identifier	Length	Type	Size	Type-data
1	Id1	EAP 总长度	4	Challenge 字节数	Challenge

3) 客户端发送 EAP 数据属性，EAP 的 code 为 response，type 为 MD5-challenge 方式。Type-data 包含经过 MD5-challenge 加密过的密码密文和用户名。其中所采用的加密方法为：

MD5(Identifier, password, challenge)

数据包格式见表 5。

表 5 数据包格式

Code	Identifier	Length	Type	Size	Type-data	
2	Id1	EAP 总长度	4	密文字节数	密码密文	用户名

4) ECP认证服务器端发送EAP数据属性, 如果认证成功, EAP的code为success; 如果失败, EAP的code为request, type为notification, type-data为出错原因的字符串。

认证成功的数据包格式见表 6。

表 6 认证成功的数据包格式

Code	Identifier	Length
3	Id2	4

认证失败的数据包格式见表 7。

表 7 认证失败的数据包格式

Code	Identifier	Length	Type	Size	Type-data
1	Id2	EAP 总长度	2	字符串字节数	错误类型码, 错误信息字符串 例如: "1: System error!"

#### 7.1.4 二次地址分配

为了控制用户认证前后访问资源权限, 在用户认证成功前后所获得的 IP 地址是不一样的。用户认证前获得的 IP 地址只具有访问 ECP 认证服务器的权限, 和某些指定的资源, 不具备访问 Internet 的能力, 此 IP 地址称为受限 IP 地址。用户认证通过后, 要重新获取 IP 地址, 此时所获得的 IP 地址和认证前获得的 IP 地址属于不同的 IP 地址段, 该 IP 地址具备访问 Internet 资源的能力, 此 IP 地址称为非受限 IP 地址。

通过二次地址分配, 可以采用分配不同地址池中地址的方式使客户端具有不同的网络访问能力。

#### 7.1.5 用户会话的建立与维护

为了维护客户端在线的状态, 需要在客户端和 ECP 认证服务器之间保持会话连接。通过客户端在 ECP 认证服务器之间定期的会话连接刷新数据包的方式来保证。

1) 在用户认证成功后, ECP 认证服务器会返回客户端如下的会话属性:

- 客户端会话连接刷新的间隔;
- 客户端会话超时时长;
- 客户端据此设置本次会话的属性。

2) 用户获得非受限 IP 地址以后, 开始发送会话连接刷新包。无论前一个会话连接刷新数据包是否得到响应, 下一个会话连接刷新数据包的发送间隔都为预设的会话连接刷新间隔。

3) 如果客户端超过预设的会话超时时长的时间没有接收到 ECP 认证服务器的会话连接刷新响应, 表明跟 ECP 认证服务器之间的会话中断, 则断开网络通知用户。

4) 在用户下线的时候, 客户端发送下线请求, 结束本次会话。

## 7.2 通信协议 ECP

### 7.2.1 ECP 通信协议数据单元格式

组成通信协议数据单元的格式如图 11 所示。

MSG_VERSION	MSG_TYPE	MSG_LENGTH	MSG_CODEMODE	MSG_RESERVED	MSG_SEQNUM	MSG_APPID	MSG_PROPS
头部							属性域

图 11 组成通信协议数据单元的格式

协议数据单元字段说明见表 8。

表 8 通信协议数据单元组成部分内容说明

名 称	长度 (字节)	描 述	示例内容
MSG_VERSION	1	协议版本号。必须为 127	127
MSG_TYPE	1	消息类型	3
MSG_LENGTH	2	消息中 MSG_PROPS 部分的长度	0x00 0x08
MSG_CODEMODE	1	消息编码方式。必须为 0	0
MSG_RESERVED	1	预留字节	0
MSG_SEQNUM	1	消息编号	23
MSG_APPID	1	消息应用编号。必须为 127	127
MSG_PROPS	0~任意长度	消息属性组列表。不同类型的包可能不带参数，也可能带有不同内容的参数。详见“消息属性列表描述”	

#### 1) MSG\_VERSION

客户/ECP 认证服务器版本域长度是一个字节，表示客户端或 ECP 认证服务器端通信协议的版本号。这个版本号主要用于 ECP 认证服务器和客户端确定通信所采用的格式。该值必须为 127。

#### 2) MSG\_TYPE

消息类型域是一个字节，确定协议数据单元的类型。在接收到一个无效消息类型域的数据包后，该数据包只是会被简单地丢弃。

MSG\_TYPE 的取值如下：

- 1 (客户端) 分配任务请求 (RequestTask)
- 2 (ECP 认证服务端) 返回任务分配列表 (TaskRes)
- 3 (客户端) 用户身份认证请求(LogonReq)
- 4 (ECP 认证服务端) 用户身份认证回应(LogonRes)
- 5 (客户端) 发送会话连接刷新请求(HeartbeatReq)
- 6 (ECP 认证服务端) 会话连接刷新请求回应(HeartbeatRes)
- 9 (客户端) 用户下网请求(LogoffReq)
- 10 (ECP 认证服务端) 用户下网请求回应(LogoffRes)

#### 3) MSG\_LENGTH

本域的长度为两个字节，数值为属性域的总长度。

#### 4) MSG\_CODEMODE

消息编码格式，该值必须为 0。

#### 5) MSG\_RESERVED

本域的长度为一个字节，预留，建议为 0。

#### 6) MSG\_SEQNUM

本域的长度为一个字节，数值为消息编号。消息编号用于标识会话过程，为 0~255 之间的无符号整数。客户端随机选择一个初始值，每次发送新的数据包将消息编号加 1；重发的数据包消息编号不变。ECP 认证服务器端回复的消息编号和客户端发送的消息编号相同。

#### 7) MSG\_APPID

本域的长度为一个字节，数值必须为 127。

## 8) MSG\_PROPS

属性域的长度是可变的，包含一个消息类型所必须的属性列表，和其他任何希望的可选属性。

ECP 属性在请求和回复中携带详细的认证、授权等信息。

由于每个属性是由三个部分组成的，因此我们又称之为“三元属性”。

## 7.2.2 ECP 通信协议域属性格式

ECP 通信协议域属性格式描述见表 9。

表 9 协议域属性格式描述

名称	长度(字节)	描述	示例内容
PROP_TYPE	1-2	属性类型。这个字节是可扩展的，如果小于 127，用 1 个字节表示；如果大于 127，自动变成两个字节，将两个字节按照网络顺序拼接为一个 16 位整数，并去掉最高位，所得的结果是真正的长度值。(如 0x81 0x80 表示 384)	0x20 或者 0x81 0x80
PROP_LENGTH	1-2	属性长度。表示每个属性中 PROP_VALUE 的长度。这个字节是可扩展的，目前规定<127，如果大于 127，自动变成两个字节，将两个字节按照网络顺序拼接为一个 16 位整数，并去掉最高位，所得的结果是真正的长度值。(如 0x81 0x80 表示 384)	0x04 或者 0x81 0x80
PROP_VALUE	0~任意	属性值。属性值的数据类型包括：整数（高位在前）、UTF-8 格式编码的字符串	

本标准目前规定 9 个属性类型。

属性类型 PROP\_TYPE 的取值如下：

- 1 (全局) 客户端本地 IP(Client-IP)
- 3 (ECP 认证服务端) 任务分配响应(Task-Flag)
- 4 (ECP 认证服务端) ECP Server 的 IP 地址组(ServerIPs)
- 8 (客户端) 用户名(Username)
- 11 (ECP 认证服务端) 用户在线时长(会话连接刷新响应)(Online-Time)
- 12 (ECP 认证服务端) 客户端会话连接刷新的间隔(Heartbeat-Interval)
- 13 (ECP 认证服务端) 客户端超时时长(Client-Timeout)
- 18 (客户端) 客户端的 DHCP server 的 IP 地址(DHCP-sIP)
- 26 (ECP 认证服务端) EAP 数据(EAP-Data)

1) 客户端本地 IP(Client-IP)

客户端本地 IP(Client-IP)见表 10。

表 10 客户端本地 IP 地址格式

类型	长度	值
1	4	客户端的 IP 地址

必须出现本属性的消息：无。

可选出现本属性的消息：所有的协议数据单元。

IP 地址采用 4 字节整型数值进行表示，以网络字节顺序传送。在发送本属性的情况下，ECP 认证服务器针对属性中指定的 IP 地址进行认证、授权等操作。

2) 任务分配响应(Task-Flag)

任务分配响应属性格式见表 11。

表 11 任务分配响应属性格式

类 型	长 度	值
3	1	响应标志

必须出现本属性的消息：TaskRes。

可选出现本属性的消息：无。

响应标志：

- 0 任务分配失败
- 1 任务分配成功
- 2 客户端所用的地址不是ECP认证服务器分配的（分到了伪IP）
- 3) ECP 认证服务器的 IP 地址组(ServerIPs)

ECP 认证服务器的 IP 地址组属性格式见表 12。

表 12 ECP 认证服务器的 IP 地址组属性格式

类 型	长 度	值
4	IP 地址长度*IP 数目	IP 地址序列

必须出现本属性的消息：无。

可选出现本属性的消息：TaskTes。

所依赖的属性：Task-Flag=1。

IP 地址采用 4 字节整型数值进行表示，以网络字节顺序传送。在传递多个 IP 地址的时候，每 4 字节为一个 IP 地址。各 IP 地址之间地位均等，没有优先级的关系。

4) 用户名(Username)

用户名属性格式见表 13。

表 13 用户名属性格式

类型	长度	值
8	任意	用户名字符串

必须出现本属性的消息：第一个 LogonReq、HeartbeatReq、LogoffReq。

可选出现本属性的消息：无。

5) 用户在线时长（会话连接刷新响应）(Online-Time)

用户在线时长属性格式如表 14 所示。

表 14 用户在线时长属性格式

类 型	长 度	值
11	4	用户在线时长（会话连接刷新响应）

必须出现本属性的消息：HeartbeatRes。

可选出现本属性的消息：无。

用户在线时长（会话连接刷新响应）：

- 2 表示会话连接刷新抛出异常。
- 1 表示用户余额不足，ECP 认证服务端已经断开该用户。
- 1 表示 ECP 认证服务器处于开始计时或者无法计时的状态。
- >1 表示该用户的上网时长，单位：μs（毫秒）。

## 6) 客户端会话连接刷新的间隔(Heartbeat-Interval)

客户端会话连接刷新闻隔属性格式见表 15。

表 15 客户端会话连接刷新闻隔属性格式

类 型	长 度	值
12	4	会话连接刷新闻隔

必须出现本属性的消息：无。

可选出现本属性的消息：HeartbeatRes、LogonRes。

表示客户端进行会话连接刷新的时间间隔，单位：s（秒）。

客户端应当具有默认的会话连接刷新闻隔，建议为 30 秒。

## 7) 客户端 session 超时时长(Client-Timeout)

客户端 session 超时时长属性格式见表 16。

表 16 客户端 session 超时时长属性格式

类 型	长 度	值
13	4	超时时长

必须出现本属性的消息：无。

可选出现本属性的消息：HeartbeatRes、LogonRes。

表示客户端进行 session 超时的时间间隔，单位：秒。

客户端应当具有默认的超时时长，建议为 120 秒。

说明：session 超时时长规定的是客户端未收到 ECP 认证服务器端响应的最大等待时间。在没有超时之前，客户端应当一直按照会话连接刷新闻隔发送会话连接刷新，并等待响应。在客户端超时后，应断开网络并通知用户。

## 8) 客户端的 DHCP server 的 IP 地址(DHCP-sIP)

客户端的 DHCP server 的 IP 地址属性格式见表 17。

表 17 客户端的 DHCP server 的 IP 地址属性格式

类 型	长 度	值
18	4	DHCP 服务器 IP 地址

必须出现本属性的消息：无。

可选出现本属性的消息：RequestTask。

客户端向 ECP 认证服务器端发送本属性，ECP 认证服务器端用来确定客户端所用的 IP 是否是伪 DHCP 服务器分的 IP 地址。

## (9) EAP 数据(EAP-Data)

EAP 数据属性格式见表 18。

表 18 EAP 数据属性格式

类 型	长 度	值
26	任意	EAP 数据包

必须出现本属性的消息：LogonReq（除了第一个）、LogonRes。

可选出现本属性的消息：无。

属性的值为 EAP 格式的数据，用于认证过程。

**附录 A**  
(资料性附录)  
**NAT 支持方案**

对于公网 IP 地址资源不丰富的运营商，出口通常通过 NAT 设备进行地址转换。NAT 设备放到本地网络的出口处，DHCP 分配的受限地址和非受限地址都是私有地址，用户非受限地址通过 NAT 设备访问外网资源。

### A.1 PAT

NAT 设备具有多种配置方式，这里讨论私有地址和公网地址进行端口变换的 PAT 方式，在这种工作模式下，地址的申请和续租都存在问题：

- 在 DHCP 地址申请过程中，服务器要把回复的消息发送到 NAT 地址的 67 端口，造成无法回复；
- 在 DHCP 地址续租过程中，服务器要把回复的消息发送到 NAT 的 68 端口，无法正常续租。

为了解决 DHCP 消息穿越 NAT 设备的问题，可以采用建立 GRE Tunnel 的方式实现穿越 NAT。为了实现 NAT 设备的穿越，需要在 NAT 设备和 Router-A 之间建立一个 VPN tunnel，让所有指向 DHCP+ 系统的流量通过 tunnel 到达，其他的数据通过 NAT 进行访问。如图 A.1 所示。

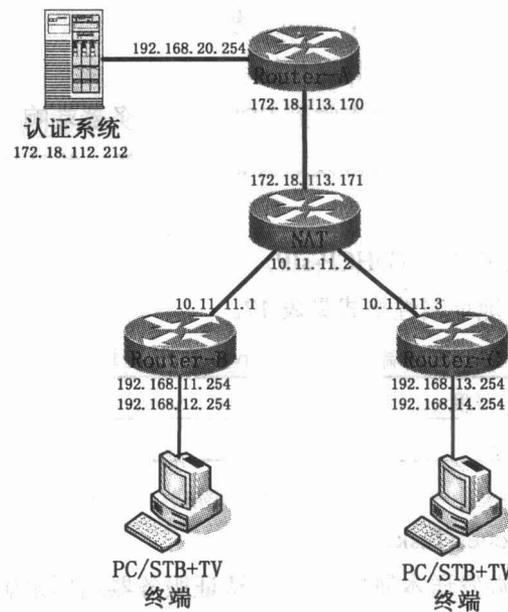


图 A.1 系统穿透 NAT 示意

● NAT 设备配置参考

```
interface Tunnel1
  ip address 2.2.2.1 255.255.255.0
  tunnel source Ethernet0/0
  tunnel destination 172.18.113.170
!
interface Ethernet0/0
  ip address 172.18.113.171 255.255.255.0
```

```

ip nat outside
full-duplex
arp timeout 240
!
interface Serial0/2
ip address 10.11.11.2 255.255.255.0
ip nat inside
encapsulation ppp
!
ip nat inside source list 111 interface Ethernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.113.170
ip route 172.18.112.0 255.255.255.0 Tunnel1
ip route 192.168.11.0 255.255.255.0 10.11.11.1
ip route 192.168.12.0 255.255.255.0 10.11.11.1
ip route 192.168.13.0 255.255.255.0 10.11.11.3
ip route 192.168.14.0 255.255.255.0 10.11.11.3
no ip http server
!

```

## A.2 pooled-NAT

这种 NAT 模式是端口不变的，私网地址和公网地址一一映射。由于端口不变，因此 DHCP 请求过程不会存在问题，但是 DHCP 的续租由于地址变化可能存在问题。修改这个问题只需要 DHCP Server 接收到续租请求的时候认为该请求是数据包里面的 ciaddr 是真正的用户地址，就能够达到 DHCP 正常通信。

附录 B  
(资料性附录)  
防伪 DHCP 检测方案

本方案采用终端安装和运行客户端程序，并在获得 IP 地址以后，检测 relay-agent 参数的方式来识别伪 DHCP 服务器和 DHCP 服务攻击，如图 B.1 所示。

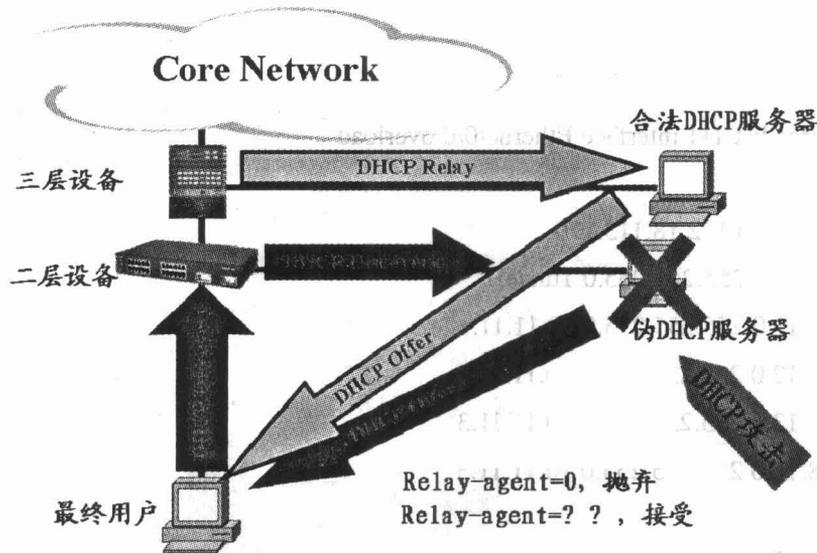


图 B.1 防伪 DHCP 检测方案示意

## 附录 C

(资料性附录)

## 用户业务选择与带宽控制方案

DHCP+系统针对用户业务选择与带宽控制的功能，可以通过用户的接入的二三层网络设备与DHCP系统得交互来实现。

用户带宽控制，在网络设备上可以对用户的IP地址，MAC地址或某种类型的流量进行带宽限制。策略适用于网络边界，用作实施QoS策略的组成部分。策略使边界设备能够识别并分类信息包，将输入流量的速率限制为某个特定的速率。

网络设备与系统之间的交互流程如图C.1所示。

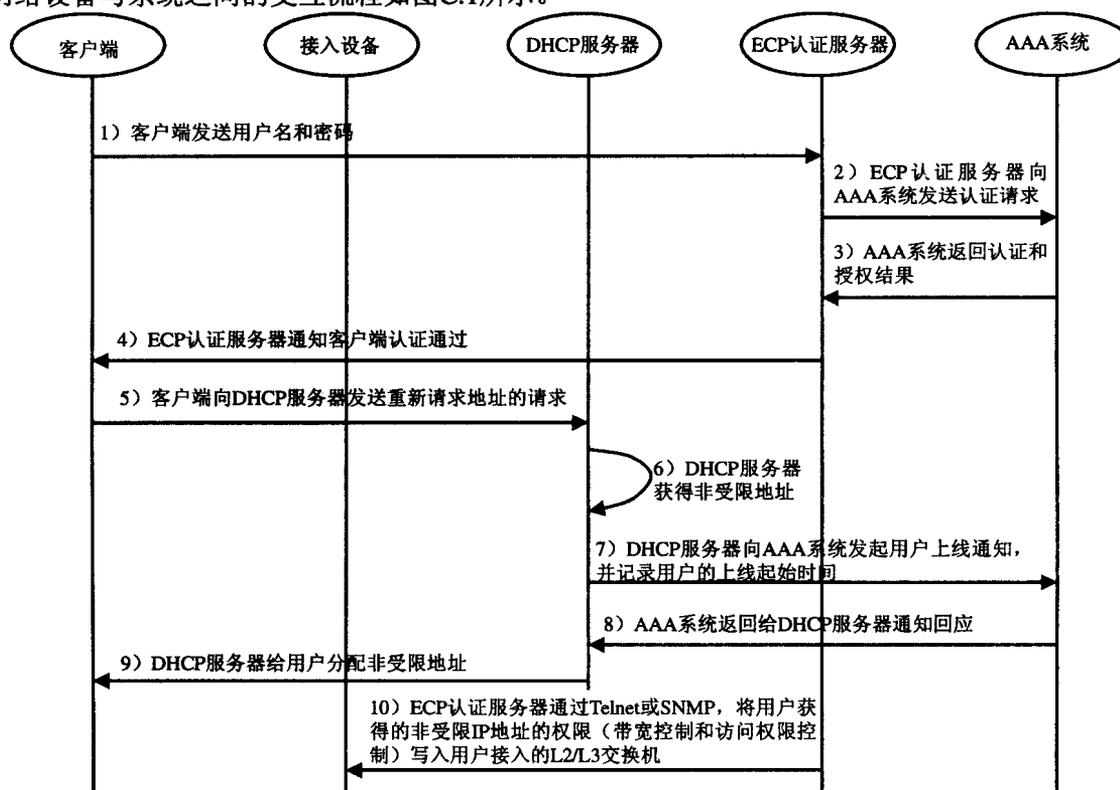


图 C.1 网络设备与系统之间的交互流程

流程说明：

- (1) 客户端启动客户端，输入客户端名和密码后，向 ECP 认证服务器发送认证请求；
- (2) ECP 认证服务器调用认证接口，向 AAA 系统发送认证请求；
- (3) 认证通过，AAA 系统返回 ECP 认证服务器认证和授权结果；
- (4) ECP 认证服务器通知客户端认证通过；
- (5) 客户端向 DHCP 服务器发送重新请求地址的请求；
- (6) DHCP 服务器获取非受限地址；
- (7) DHCP 服务器向 AAA 系统发起用户上线通知，并记录用户的上线起始时间；
- (8) AAA 系统返回给 DHCP 服务器通知响应；
- (9) DHCP 服务器给用户分配非受限地址。

(10) ECP 认证服务器通过 Telnet 或 SNMP，将用户获得的非受限 IP 地址的权限（带宽控制和访问权限控制）写入用户接入的 L2/L3 交换机；

(11) 当用户下线后（正常下线、异常下线），ECP 认证服务器通过 Telnet 或 SNMP，将该用户的非受限 IP 地址的权限从用户接入的 L2/L3 交换机中清除。

附 录 D  
(资料性附录)  
相关设备要求

### D.1 对认证客户端的要求

基于 DHCP+的认证客户要求通常为终端设备（如 PC、机顶盒+TV），该设备需要运行 DHCP+的客户端软件，如专用的 DHCP+客户端软件。该客户端要支持并符合 DHCP+协议的规范要求。

### D.2 三层设备必须具备的功能要求

DHCP+系统通过和边缘三层设备的配合实现用户的 AAA 流程。对于边缘三层设备，DHCP+ 系统有如下要求：

- 支持 ACL 设置；
- 支持 DHCP Relay 设置；
- 支持 SNMP 或 Telnet 方式读写 ARP 表。

### D.3 三层设备推荐功能的要求

#### D.3.1 防止ARP欺骗

DHCP+系统针对 ARP 欺骗的防范，可以通过用户的接入的二三层网络设备来实现。

##### D.3.1.1 ARP 欺骗的原理和危害

ARP 是用来实现 MAC 地址和 IP 地址的绑定，这样两个工作站才可以通讯，通讯发起方的工作站以 MAC 广播方式发送 ARP 请求，拥有此 IP 地址的工作站给予 ARP 应答，送回自己的 IP 和 MAC 地址。ARP 协议同时支持一种无请求 ARP 功能，局域网段上的所有工作站收到主动 ARP 广播，会将发送者的 MAC 地址和其宣布的 IP 地址保存，覆盖以前 cache 的同一 IP 地址和对应的 MAC 地址，主动式 ARP 合法的用途是用来以备份的工作站替换失败的工作站。由于 ARP 无任何身份真实校验机制，黑客程序发送误导的主动式 ARP 使网络流量重指经过恶意攻击者的计算机，变成某个局域网段 IP 会话的中间人，达到窃取甚至篡改正常传输的功效。黑客程序发送的主动式 ARP 采用发送方私有 MAC 地址而非广播地址，通信接收方根本不会知道自己的 IP 地址被取代。为了保持 ARP 欺骗的持续有效，黑客程序每隔 30 秒重发此私有主动式 ARP。

##### D.3.1.2 防范方法

这些攻击都可以通过动态 ARP 检查（DAI, Dynamic ARP Inspection）来防止，它可以帮助保证接入交换机只传递“合法的”的 ARP 请求和应答信息。DHCP Snooping 监听绑定表包括 IP 地址与 MAC 地址的绑定信息并将其与特定的交换机端口相关联，动态 ARP 检测（DAI—Dynamic ARP Inspection）可以用来检查所有非信任端口的 ARP 请求和应答(主动式 ARP 和非主动式 ARP)，确保应答来自真正的 ARP 所有者。交换机通过检查端口纪录的 DHCP 绑定信息和 ARP 应答的 IP 地址决定是否真正的 ARP 所有者，不合法的 ARP 包将被删除。

DAI 配置针对 VLAN，对于同一 VLAN 内的接口可以开启 DAI 也可以关闭，如果 ARP 包从一个可信任的接口接受到，就不需要做任何检查，如果 ARP 包在一个不可信任的接口上接受到，该包就只能在

绑定信息被证明合法的情况下才会被转发出去。这样，DHCP Snooping 对于 DAI 来说也成为必不可少的，DAI 是动态使用的，相连的客户端主机不需要进行任何设置上的改变。对于没有使用 DHCP 的服务器个别机器可以采用静态添加 DHCP 绑定表或 ARP access-list 实现。

另外，通过 DAI 可以控制某个端口的 ARP 请求报文频率。一旦 ARP 请求频率的频率超过预先设定的阈值，立即关闭该端口。该功能可以阻止网络扫描工具的使用，同时对有大量 ARP 报文特征的病毒或攻击也可以起到阻断作用。

### D.3.2 防止MAC泛滥攻击

DHCP+系统针对 MAC 泛滥攻击的防范，可以通过用户的接入路径中的二三层网络设备来实现。

#### D.3.2.1 MAC 泛滥攻击的原理和危害

交换机主动学习客户端的 MAC 地址，并建立和维护端口和 MAC 地址的对应表以此建立交换路径，这个表就是通常我们所说的 CAM 表。CAM 表的大小是固定的，不同的交换机的 CAM 表大小不同。MAC/CAM 攻击是指利用工具产生欺骗 MAC，快速填满 CAM 表，交换机 CAM 表被填满。黑客发送大量带有随机源 MAC 地址的数据包，这些新 MAC 地址被交换机 CAM 学习，很快塞满 MAC 地址表，这时新目的 MAC 地址的数据包就会广播到交换机所有端口，交换机就像共享 HUB 一样工作，黑客可以用 sniffer 工具监听所有端口的流量。此类攻击不仅造成安全性的破坏，同时大量的广播包降低了交换机的性能。

#### D.3.2.2 防范方法

限制单个端口所连接 MAC 地址的数目可以有效防止类似 macof 工具和 SQL 蠕虫病毒发起的攻击，macof 可被网络用户用来产生随机源 MAC 地址和随机目的 MAC 地址的数据包，可以在不到 10 秒的时间内填满交换机的 CAM 表。采用交换机的端口安全 (Port Security) 和动态端口安全功能可被阻止 MAC 泛滥攻击。例如交换机连接单台工作站的端口，可以限制所学 MAC 地址数为 1；连接 IP 电话和工作站的端口可限制所学 MAC 地址数为 3；IP 电话、工作站和 IP 电话内的交换机。

通过端口安全功能，网络管理员也可以静态设置每个端口所允许连接的合法 MAC 地址，实现设备级的安全授权。动态端口安全则设置端口允许合法 MAC 地址的数目，并以一定时间内所学习到的地址作为合法 MAC 地址。

通过配置端口安全 Port Security 可以控制：

- 端口上最大可以通过的 MAC 地址数量；
- 端口上学习或通过哪些 MAC 地址；
- 对于超过规定数量的 MAC 处理进行违背处理。

### D.3.3 防止IP地址盗用

DHCP+系统针对 IP 地址盗用攻击的防范，可以通过用户的接入的二三层网络设备与 DHCP 系统得交互来实现。

#### D.3.3.1 IP 地址盗用的危害

除了 ARP 欺骗外，黑客经常使用的另一手法是 IP 地址欺骗，其目的一般为伪造身份或者获取针对 IP/MAC 的特权。此方法也被广泛用作 DOS 攻击，目前较多的攻击是：Ping Of Death、Syn flood、ICMP Unreachable Storm。如黑客冒用 A 地址对 B 地址发出大量的 ping 包，所有 ping 应答都会返回到 B 地址，通过这种方式来实施拒绝服务 (DoS) 攻击，这样可以掩盖攻击系统的真实身份。富有侵略性的 TCP SYN 洪泛攻击来源于一个欺骗性的 IP 地址，它是利用 TCP 三次握手会话对服务器进行颠覆的又一种攻击方式。

一个 IP 地址欺骗攻击者可以通过手动修改地址或者运行一个实施地址欺骗的程序来假冒一个合法地址。

另外病毒和木马的攻击也会使用欺骗的源 IP 地址。互联网上的蠕虫病毒也往往利用欺骗技术来掩盖它们真实的源头主机。

### D.3.3.2 防范方法

源地址保护 (IP Source Guard) 技术可以根据 DHCP 侦听记录的 IP 绑定表动态产生 PVACL, 强制来自此端口流量的源地址符合 DHCP 绑定表的记录, 这样攻击者就无法通过假定一个合法用户的 IP 地址来实施攻击了, 这个技术将只允许对拥有合法源地址的数据包进行转发, 合法源地址是与 IP 地址绑定表保持一致的, 它也是来源于 DHCP Snooping 绑定表。因此, DHCP Snooping 功能对于这个功能的动态实现也是必不可少的。

IP Source Guard 不但可以配置成对 IP 地址的过滤也可以配置成对 MAC 地址的过滤, 这样, 就只有 IP 地址和 MAC 地址都于 DHCP Snooping 绑定表匹配的通信包才能够被允许传输。此时, 必须将 IP 源地址保护 IP Source Guard 与端口安全 Port Security 共同使用, 并且需要 DHCP 服务器支持 Option 82 时, 才可以抵御 IP 地址+MAC 地址的欺骗。

### D.3.4 防止伪DHCP

DHCP+系统针对伪 DHCP 的防范, 可以通过用户的接入的二三层网络设备来实现。

DHCP 服务器欺诈可能是故意的, 也可能是无意启动 DHCP 服务器功能, 恶意用户发放错误的 IP 地址、DNS 服务器信息或默认网关信息, 以此来实现流量的截取。

#### D.3.4.1 DHCP Snooping 技术

DHCP Snooping 技术是 DHCP 安全特性, 通过建立和维护 DHCP Snooping 绑定表过滤不可信任的 DHCP 信息, 这些信息是指来自不信任区域的 DHCP 信息。通过截取一个虚拟局域网内的 DHCP 信息, 交换机可以在用户和 DHCP 服务器之间担任就像小型安全防火墙这样的角色, “DHCP 监听”功能基于动态地址分配建立了一个 DHCP 绑定表, 并将该表存贮在交换机里。

#### D.3.4.2 防范方法

为了防止这种类型的攻击, DHCP 侦听 (DHCP Snooping) 可有效阻止此类攻击, 当打开此功能, 所有用户端口除非特别设置, 被认为不可信任端口, 不应该作出任何 DHCP 响应, 因此欺诈 DHCP 响应包被交换机阻断, 合法的 DHCP 服务器端口或上连端口应被设置为信任端口。

首先定义交换机上的信任端口和不信任端口, 对于不信任端口的 DHCP 报文进行截获和嗅探, DROP 掉来自这些端口的非正常 DHCP 响应报文, 如图 D.1 所示。

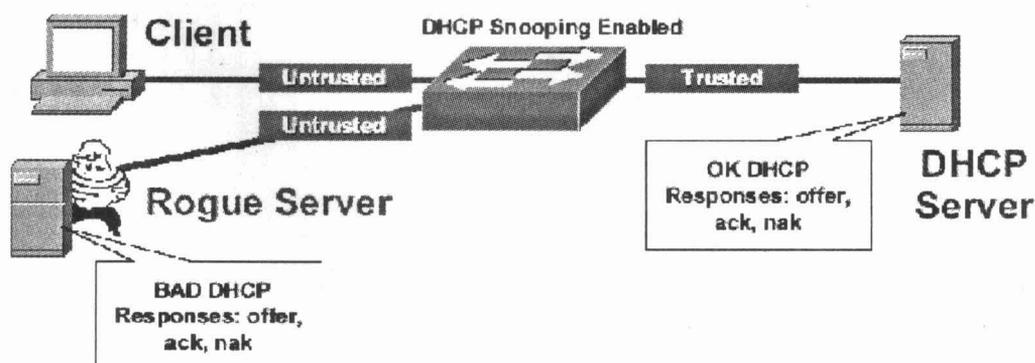


图 D.1 防范方法示意

#### D.4 对计费的要求

本节用于对计费 AAA 接口的规范和要求。具体参考如下：

(1) 计费方式：认证点配合认证服务器，应能够提供多种灵活的计费方式，包括基本费、包月费、计时费、计量费、费用峰顶以及以上基本计费方式的组合；

(2) 应用量统计：认证点配合认证服务器，应能够精确的统计用户对网络资源的使用量，包括时长、流量等原始计费信息；

(3) 计费保护机制：认证点配合认证服务器，应能提供完善的计费保护机制，包括主备认证服务器、话单本地保存、实时计费、无响应超时切断以及无响应重传等，保证话单抄送的可靠性。

## 附 录 E

(资料性附录)

## 推荐的配置与性能参考实例

推荐的服务器配置的计算方法为：根据系统的实际运行测试结果，即某一固定配置的服务器在实际运行中所能够支持的用户数量，得出该测试服务器的实际处理能力，然后根据计划支持的用户数量的要求，计算出系统对服务器的要求，即计算出测试服务器和实际建议的服务器之间的性能指标的折算关系，折算关系可以按照国际通用的服务器评测体系（如 TPC 体系和 SPEC 体系）所标定的服务器性能指标参数进行换算得出。

在实际运行测试中得出的服务器基准支持能力如下：

在 ECP 认证服务器配置 1 个 PIII 1G CPU、512M 内存时,且 CPU 具有 70% 的 24 小时平均空闲率的情况下，各模块支持的同时在线用户数为：

- 后台服务模块（策略控制、功能控制等模块）：15 000 用户
- 客户端登录前端模块（DHCP、ECP 模块）：6 000 用户
- 监控器/远端控制模块（防地址盗用模块）：10 000 用户

在实际组网设计中配置 ECP 认证服务器时，按照实际需要支持的用户数量与上述的各模块所支持的用户数量之间的折算关系即可计算出所需要的同等配置的服务器数量，再根据不同服务器的性能指标折算出使用其他服务器时需要的配置；各个模块即可部署在同一台服务器上也可分别部署在多台服务器上。

**附 录 F**  
**(资料性附录)**  
**受限地址资源考虑**

**F.1 建议配置受限地址资源**

首先，客户端必须获得受限地址，然后才能够与 ECP 认证服务器进行通信，从而发起认证，所以客户端获得受限地址是能够进行认证的前提；其次客户端获得受限地址可以访问运营商提供的自服务网站，使用费用查询、密码更改、客户端软件更新、FAQ、投诉等自助服务，可以提高运营商的服务质量和用户满意度；另外一个考虑是，客户端下线以后将继续发送获得地址的请求包，此时若不给客户端分配地址将会在网络中产生大量的无用请求包。

**F.2 受限地址安全性考虑**

连接在网络中的用户只要一开机即可获得受限地址，此时虽然用户不能够访问非受限的网络资源，但在可访问的受限网络资源范围内是可以互相通信的，用户可以对目标资源进行攻击，并且此时用户没有经过用户名与口令认证，用户若进行非法攻击的话将无法精确追查。

针对上述安全问题的解决方法如下：

(1) 认证系统与网络设备通过支持 OPTION82 (RFC3046)，来对用户进行定位、控制与追查；其中认证系统能够根据 OPTION82 (RFC3046) 对 DHCP 请求包进行限速，既能够限制在一定时间内同一 OPTION82 (RFC3046) 所发送的地址请求包数量，超出设定阈值的将被丢弃不予处理；

(2) 在网络设备中针对受限地址做相应的访问控制，既受限地址只允许访问特定的资源（如自服务网站），且受限地址之间不能够进行互通。

附 录 G  
(资料性附录)  
重放攻击的防范

用户认证过程中的重放攻击主要是攻击者在网络中对正常用户的上网过程进行侦测窃听，然后重发模拟正常用户的认证包，达到仿冒或干扰正常用户上网的目的，针对这种类型的攻击采用以下几种方法进行防范。

(1) 对用户窃听的防范由设备完成，二层设备通过划分 802.1Q VLAN 或 PORT VLAN 即可将用户隔离，只要用户不在同一个广播域中就无法进行窃听；目前各运营商宽带接入网中的 DSLAM 等设备均在二层将所有用户隔离。

(2) 用户认证过程采用标准 CHAP 流程，ECP 认证服务器每次发给客户端的 challenge 字串都是随机生成的是不一样的，非法用户难于模拟重放。

(3) ECP 认证服务器具有 SESSION 唯 N 性控制功能，两个账号不能够同时上线。

(4) 若网络中设备支持 OPTION82 (RFC3046) 功能，则可对用户的 OPTION82 (RFC3046) 属性进行认证，因为 OPTION82 (RFC3046) 属性可以对用户进行唯一标识，且不可通过伪造进行仿冒，将 OPTION82 (RFC3046) 属性加入认证流程几乎可以解决目前各种认证方式中存在的安全问题。

攻击者还可能在用户端利用软件工具对 ECP 认证服务器发送大量的认证仿冒报文，以达到影响服务器处理性能的攻击目的，对于这一类的攻击，ECP 认证服务器采取针对 OPTION82 (RFC3046) 电路号进行认证报文限速的方式来解决，通过设置每 OPTION82 (RFC3046) 单位时间内可以发送的认证报文数量，超出设置数量的认证报文将被丢弃；并且，因为每个用户都有固定的网络带宽，用户的攻击流量局限于有限的带宽中，服务器也可以只通过强大的冗余处理能力即可应对此类攻击。