

ICS 33.040.40  
M 32

**YD**

# 中华人民共和国通信行业标准

YD/T 2544-2013

---

## 运营级 NAT44 设备技术要求

Technical specifications for carrier grade NAT (NAT44)

2013-04-25 发布

2013-06-01 实施

---

中华人民共和国工业和信息化部 发布



## 目 次

前 言	III
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	2
4 概述	3
4.1 设备定位	3
4.2 地址转换体系架构	3
4.3 设备形态	4
5 功能要求	5
5.1 资源分配模式	5
5.2 地址转换	6
5.3 行为要求	6
5.4 溯源	7
5.5 告警信息输出	8
5.6 应用层ALG	8
5.7 路由	8
5.8 网络时间同步	9
6 性能要求	9
6.1 设备容量	9
6.2 处理能力	9
6.3 可靠性	9
7 冗余备份要求	10
8 安全要求	10
8.1 访问控制和流量控制	10
8.2 路由安全	11
9 操作管理维护要求	11
9.1 基本管理功能	11
9.2 配置管理	11
9.3 性能管理	11
9.4 故障管理	12
9.5 安全管理	12

10	物理接口要求.....	12
10.1	插卡设备.....	12
10.2	独立设备.....	12
11	环境要求.....	12
12	电源与接地.....	12
13	例行试验.....	12

## 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：中国电信集团公司、工业和信息化部电信研究院、中国联合网络通信集团有限公司、华为技术有限公司。

本标准主要起草人：谭景华、杨国良、黄灿灿、李小洋、马季春、张桂玉、傅 瑜、郭大勇、马军锋、唐 浩。



## 运营级 NAT44 设备技术要求

### 1 范围

本标准规定了运营级NAT44设备的定位及其在运营级地址转换体系中的作用,规定了NAT44设备的功能、性能、安全、备份以及管理等基本的技术要求。

本标准适用于有线宽带网络中的整机NAT44设备,不适用于具有地址转换功能的单板。

### 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅所注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

YD/T 1097-2009 路由器设备技术要求 核心路由器

YD/T 1148-2005 网络接入服务器技术要求---宽带网络接入服务器

IETF RFC3022 传统IP网络地址翻译器(传统NAT)(Traditional IP Network Address Translator (Traditional NAT))

IETF RFC4787 单一UDP的网络地址转换(NAT)行为要求(Network Address Translation(NAT) Behavioral Requirements for Unicast UDP)

IETF RFC5382 TCP NAT动作要求(NAT Behavioral Requirements for TCP)

IETF RFC5508 ICMP的NAT动作要求(NAT Behavioral Requirements for ICMP)

IETF RFC5424 Syslog协议(The Syslog Protocol)

### 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文件。

##### 3.1.1

**NAT44 Network Address Translation 44**

实现IPv4地址到IPv4地址转换的技术。

##### 3.1.2

**NAT44设备 NAT44 Device**

运营级的IPv4到IPv4的地址转换设备。

##### 3.1.3

**NAT44用户 NAT44 Subscriber**

为实现地址共享而通过NAT44设备进行地址转换的用户。

##### 3.1.4

**用户地址 IP Address for User**



BNG、AAA、DHCP等系统分配给用户的IPv4地址。在运营级NAT44设备应用中通常是私有IPv4地址。

### 3.1.5

**外部地址 Exterior IP Address**

用户地址经NAT44设备转换后的IPv4地址。在运营级NAT44设备应用中通常是公有IPv4地址。

### 3.1.6

**地址映射关系 Address Mapping Relationship**

NAT44转换中绑定的（用户地址、传输层ID）与（外部地址、传输层ID）之间的映射关系，其中传输层ID可以是TCP/UDP端口号或者ICMP中的标识号。

### 3.1.7

**地址映射表 Address Mapping Table**

由地址绑定关系创建的映射表格。

### 3.1.8

**端口预留关系 Port Reservation Relationship**

NAT44转换中为用户预留的用户地址与（外部地址、端口块）之间的映射关系。

### 3.1.9

**端口预留表 Port Reservation Table**

由端口预留关系创建的映射表格。

### 3.1.10

**溯源关系/地址转换关系 Tracing Back Relationship / Address Translation Relationship**

能够根据（外部地址，传输层ID）追溯到用户地址的关系，包括地址映射关系和端口预留关系。

## 3.2 缩略语

下列缩略语适用于本文件。

AAA	Authentication、Authorization、Accounting	认证、授权、记账
ACL	Access Control List	访问控制列表
ALG	Application Layer Gateway	应用层网关
BNG	Broadband Network Gateway	宽带网络网关
CPE	Customer Premises Equipment	用户端设备
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DNS	Domain Name System	域名系统
ICMP	Internet Control Message Protocol	网际控制报文协议
IPv4	Internet Protocol Version 4	网际协议第四版
IPv6	Internet Protocol Version 6	网际协议第六版
NAT	Network Address Translation	网络地址转换
NTP	Network Time Protocol	网络时间协议
PC	Personal Computer	个人电脑
RADIUS	Remote Authentication Dial In User Service	远程认证拨号用户服务



TCP	Transfer Control Protocol
UDP	User Datagram Protocol

传输控制协议  
用户数据报协议

## 4 概述

### 4.1 设备定位

IPv4公有地址枯竭后，新增用户将无法得到IPv4公网地址，而当前IPv6部署尚未大规模开展，为了支持宽带互联网业务等IP地址相关的各种业务的持续发展，在运营商网络内需要部署NAT设备来解决地址短缺，这种NAT设备称作运营级NAT44设备。

与传统的企业网NAT应用环境不同，NAT44设备服务的用户规模更大、承载流量大、业务稳定性要求更高，因此要求NAT44设备具备更高的性能、稳定性和安全性。同时，NAT44设备也需要实现设备冗余功能以避免网络单点故障，以及实现用户溯源等方面的需求。另一方面，NAT44设备主要用于地址共享，因此可以简化传统NAT设备的安全防护功能，以提升设备的整体性能。

### 4.2 地址转换体系架构

运营商部署NAT44设备时，需要结合AAA服务器、网管服务器、日志服务器、溯源系统等配套系统，提供运营级NAT44转换，并支持用户溯源的要求。其体系架构如图1所示。

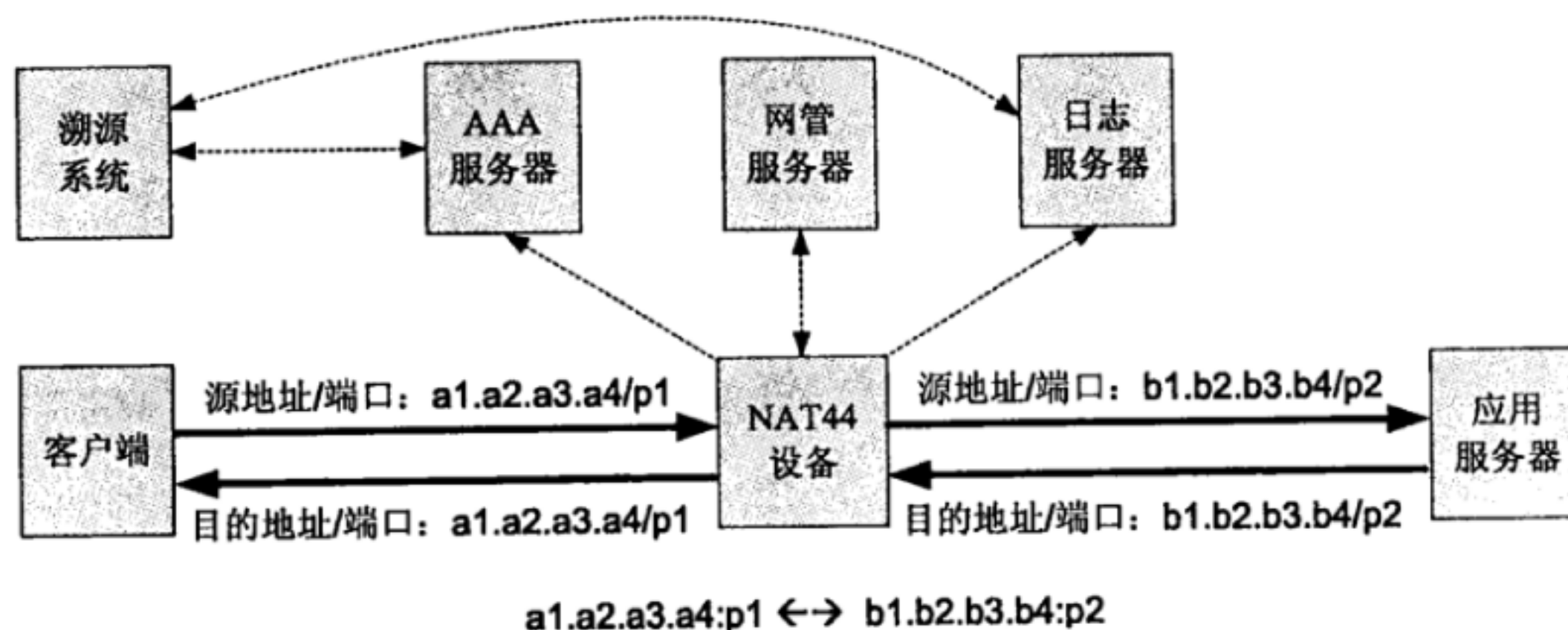


图1 地址转换系统架构

**NAT44设备：**生成和维护用户地址映射表，实现运营级NAT转换；并实现用户溯源关系向AAA服务器和日志服务器上报。

**AAA服务器：**负责记录和维护用户账号、用户地址等信息；接收或者生成用户溯源关系；响应用户的溯源关系查询。

**日志服务器：**接受和记录用户访问信息；响应用户访问信息查询。

**网管系统：**负责管理NAT44设备。

**溯源系统：**负责用户溯源；在需要进行用户溯源时，向AAA服务器或者日志服务器发起查询请求。

为实现用户溯源，NAT44设备的地址转换关系应该上报给AAA服务器或日志服务器，由AAA服务器或者日志服务器提供用户溯源的访问查询服务。如果NAT44设备的地址转换关系是静态的且可以计算出来，则AAA服务器可以采用与NAT44设备上相同的算法计算出地址转换关系，不再需要NAT44设备上上报地址转换关系。如图2所示。

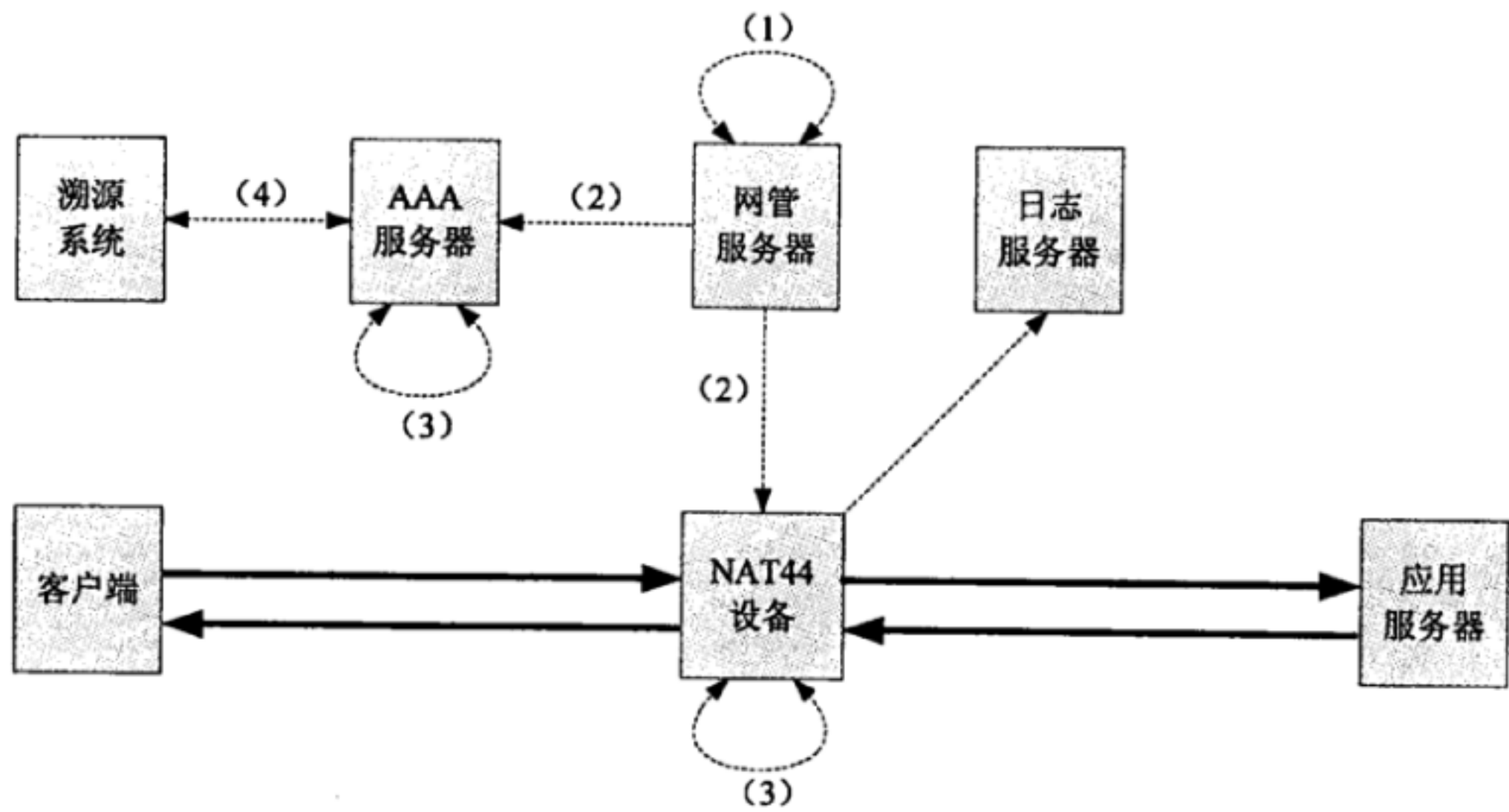


图2 静态地址转换关系生成

- (1) 网管系统统一配置用于确定地址转换关系的参数，如私有地址池、外部地址池、地址复用率等；
- (2) 网管系统分别向AAA服务器和NAT44设备下发配置参数；
- (3) AAA服务器、NAT44设备分别根据配置参数使用约定算法独立计算和生成地址转换关系，即溯源关系；
- (4) 溯源系统需要进行溯源查询时，可通过AAA服务器查找到溯源关系。

4.3 设备形态

NAT44设备有三种设备形态：独立设备、路由器插卡设备和BNG插卡设备。独立设备指只实现NAT44功能的独立设备，路由器插卡设备指路由器功能与NAT44功能合设的设备，BNG插卡设备指BNG功能与NAT44功能合设的设备。

独立设备在部署时需要考虑与BNG、路由器等网络设备的连接关系，比如采用串联的方式部署（见图3a），或者采用旁挂的方式部署（见图3b）。

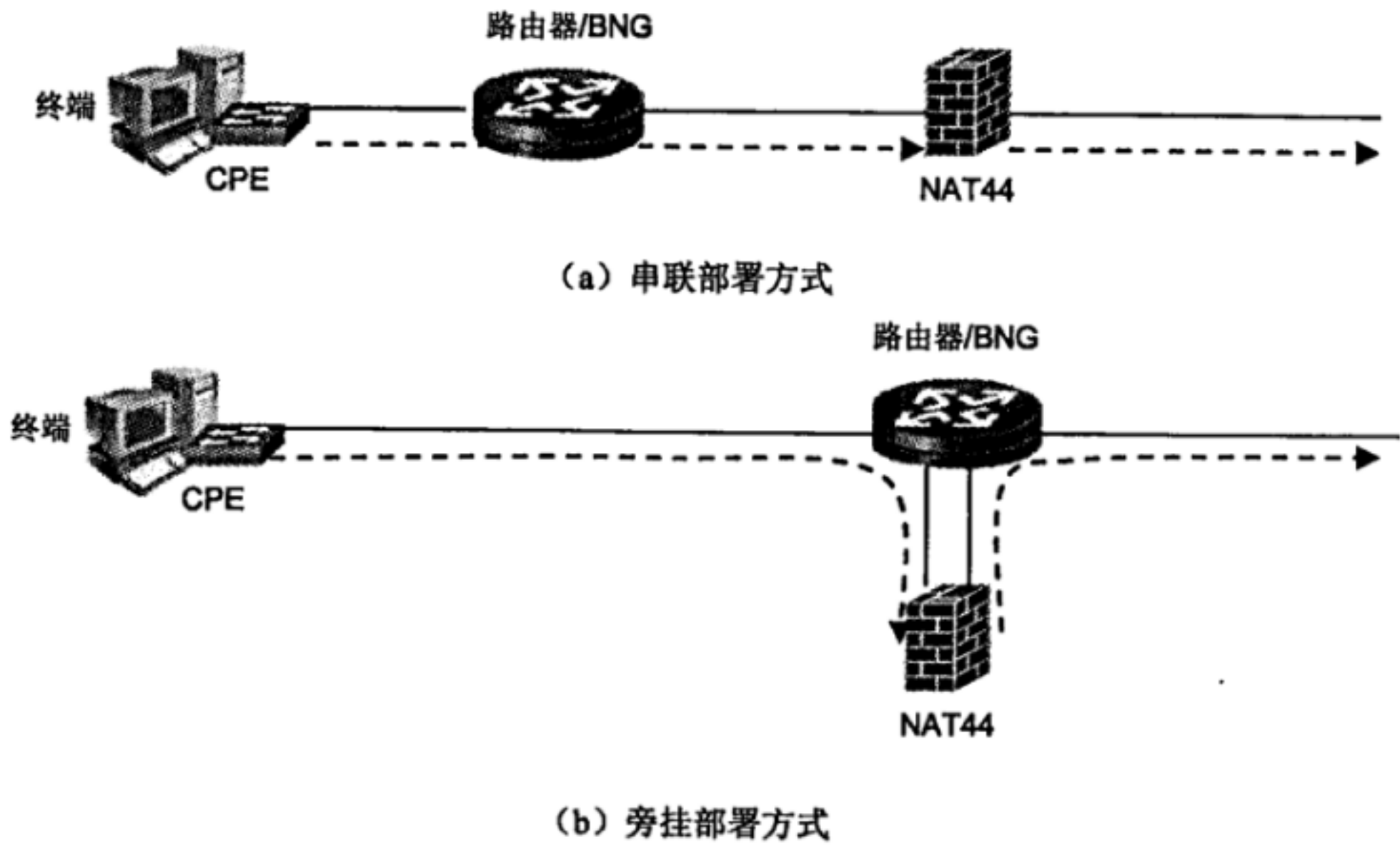


图3 独立设备 NAT44 部署方式

路由器插卡设备和BNG插卡设备由于其NAT44功能增设在路由器或者BNG设备之上，部署时除部分控制通道（如与网络管理、AAA服务器、Syslog服务器之间的接口）之外，无需考虑与其他网络设备的连接关系。图4是路由器插卡设备的部署示意图，图5是BNG插卡设备的部署示意图。

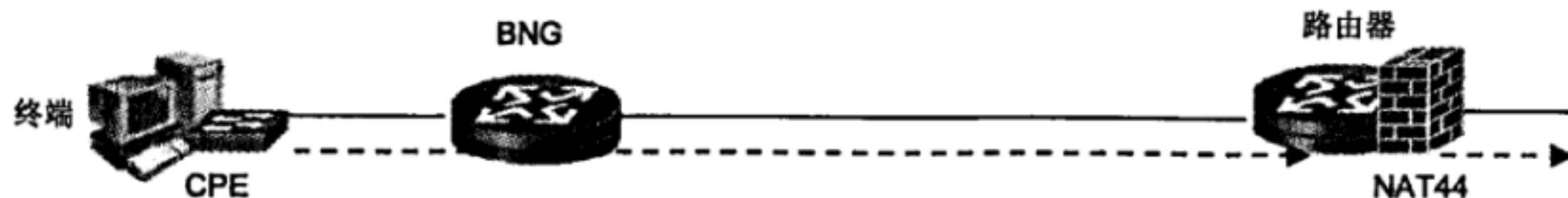


图4 路由器插卡 NAT44 部署方式

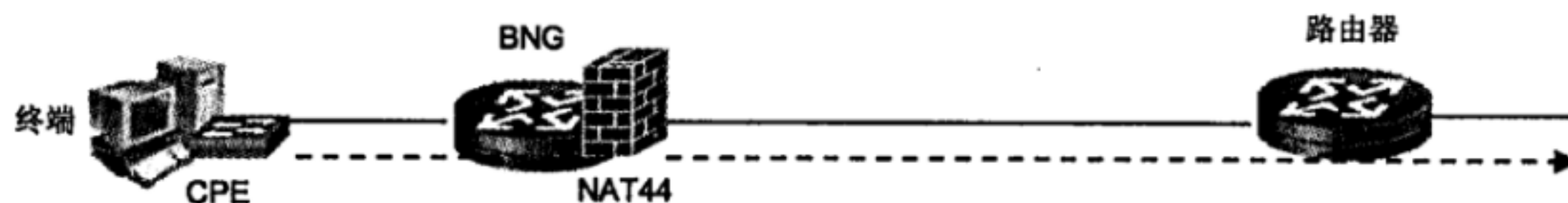


图5 BNG 插卡 NAT44 部署方式

本标准的所有技术要求，仅对NAT44功能模块有效，因而对于路由器插卡设备和BNG插卡设备中有关路由器和BNG的技术要求不在本标准的技术要求范围之内。

本标准所有的技术要求，对上述三类形态的设备要求内容不同者，会分别予以说明；无特别说明者，均为对所有形态设备的统一要求。

## 5 功能要求

### 5.1 资源分配模式

本节的资源是指可用于地址转换的外部地址和端口。

资源分配模式是指NAT44设备为用户地址转换分配外部地址和端口的方式。资源分配模式包括端口共享方式和端口预留方式。

#### 5.1.1 端口共享

端口共享方式是指所有的（外部地址、端口）资源被用户共享。在创建地址映射关系时，NAT44设备可以从未被使用且未被保留的（外部地址、端口）资源中任意选择一个（外部地址、端口）分配给用户进行地址转换。

NAT44设备必须支持端口共享的资源分配模式。

#### 5.1.2 端口预留

端口预留方式是指为用户预留一个或者若干个（外部地址、端口块）给用户使用。在创建地址映射关系时，NAT44设备只能从为该用户预留的（外部地址、端口块）中选择（外部地址、端口）分配给用户进行地址转换。同时，为该用户预留的（外部地址、端口块）资源不能再被其他用户使用。

例如，端口预留关系如下所示：

10.1.1.1 <-> (120.1.1.1, [1025, 2048])

10.1.1.2 <-> (120.1.2.1, [2049, 3072])

10.1.1.3 <-> (120.1.2.1, [3073, 4096])

端口预留方式可以分为动态预留和静态预留两种方式。

##### 5.1.2.1 动态预留



动态预留指端口预留关系是可变的。一个用户地址，在一个时期内为其预留某一个（外部地址，端口块）资源，在另一个时期为其预留另一个（外部地址、端口块）资源。

NAT44设备必须支持动态端口预留的资源分配模式。

NAT44设备采用的随机选择算法生成用户端口预留关系，可以是哈希算法，也可以是其他算法，但必须保证为每个用户地址预留不同的（外部地址，端口块）资源。

对于BNG插卡设备，在用户上线为用户分配地址时，应该同时为用户地址预留（外部地址，端口块）资源；当用户下线时，NAT44设备应该释放为此用户预留的（外部地址，端口块）资源。

对于其他形态的NAT44设备，用户应该在第一次通过NAT44设备发起会话时，为用户地址预留（外部地址，端口块）资源；当用户长时间没有会话时（例如用户在最后一个会话结束后经过老化时间仍然没有新的会话），应该释放为此用户预留的（外部地址，端口块）资源。

#### 5.1.2.2 静态预留

静态预留指端口预留关系是相对固定的。在NAT44设备配置参数不变的情况下，为用户地址预留的（外部地址、端口块）资源是固定不变的。

NAT44设备建议支持静态端口预留的资源分配模式。

NAT44设备需要根据配置的参数通过一种算法生成静态的端口预留关系。可配置的参数包括如下：

- 用户地址池：NAT44 设备配置的转换前的用户地址池信息，通常是私有地址池，也可以是公有地址池。如果是 BNG 插卡设备，一般是用户上线时 BNG 分配给用户的地址池；如果是其他形态的设备，一般应该包含可能通过该 NAT44 设备的所有用户地址的集合。

- 外部地址池：NAT44 设备配置的用户转换后的地址池信息。
- 端口块大小：NAT44 设备分配给用户使用的每个端口块的端口数量。
- 可用端口范围（s，t）：指用户地址转换时可使用的端口范围。s，t 分别表示开始和结束端口号。

根据静态端口预留关系的生成算法不同，需要配置的参数可以有所增减。

端口预留关系生成算法必须保证为每个用户地址预留不同的（外部地址，端口块）资源。算法也必须保证在配置参数不变的情况下，每次为相同用户地址预留的（外部地址，端口块）资源是不变的。

NAT44设备应该能够接受网管系统通过SNMP协议或者telnet协议下发配置参数，同时，NAT44设备也应该能够通过SNMP协议通知网管系统其已配置参数。

#### 5.2 地址转换

NAT44设备能够根据资源分配方式为用户TCP/UDP会话选择对应的（外部地址、TCP端口/UDP端口）资源进行地址转换，也能够为用户的ICMP会话进行地址转换。其特性应符合IETF RFC3022的规定。

无论采用哪种资源分配模式，对于同一个用户地址，NAT44设备为其TCP、UDP、ICMP会话分配的外部地址必须是同一个地址。

#### 5.3 行为要求

NAT44设备必须支持对TCP、UDP及ICMP报文进行地址转换的功能，其特性应符合IETF RFC4787、IETF RFC5382、IETF RFC5508的规定。

NAT44设备必须实现Endpoint-Independent Mapping及Endpoint-Independent Filtering特性。为了实现更好的安全性，建议实现Address-Dependent Mapping、Address and Port-Dependent Mapping、Address-Dependent Filtering、Address and Port-Dependent Filtering等特性。

NAT44设备支持设置UDP、TCP、ICMP会话的老化时间。

## 5.4 溯源

如果NAT44设备采用端口共享的资源分配模式，NAT44设备必须支持地址映射关系的上报，建议通过Syslog协议向日志服务器上上报地址映射关系。

如果NAT44设备采用动态端口预留的资源分配模式，NAT44设备必须支持用户端口预留关系的上报。当设备形态为路由器插卡或者独立设备时，建议通过Syslog协议向日志服务器上上报用户的端口预留关系；当设备形态为BNG插卡时，建议支持通过Syslog协议向日志服务器上上报端口预留关系，或者支持通过RADIUS协议向AAA服务器上上报端口预留关系。

如果NAT44设备采用静态端口预留的资源分配模式，由于AAA服务器可以通过与NAT44设备相同的算法生成与NAT44设备上完全一致的溯源关系，可以不上报溯源关系。

### 5.4.1 通过日志上报溯源关系

NAT44设备通过syslog协议上报溯源关系的日志有地址映射日志和端口预留日志两种，要求如下：

#### a) 地址映射日志

NAT44设备应该在用户新建一个会话时，发送“地址映射关系建立”的日志；在用户结束一个会话时，发送“地址映射关系拆除”的日志。

NAT44设备支持手工指定输出“地址映射关系建立”日志或“地址映射关系拆除”日志。

地址映射日志消息中至少包含用户地址、端口号、转换后的外部地址、转换后的端口号、时间戳。

#### b) 端口预留日志

NAT44设备应该在为用户创建端口预留关系时，发送“端口预留关系建立”的日志，在释放端口预留关系时，发送“端口预留关系释放”的日志。

NAT44设备支持手工指定输出“端口预留关系建立”日志或“端口预留关系释放”日志。

端口预留日志消息中至少包含用户地址、转换后的外部地址、转换后的起始端口号、转换后的终止端口号、时间戳。

日志的传输必须符合IETF RFC 5424定义的格式要求。

NAT44设备可以支持FTP方式定期打包发送日志信息。

### 5.4.2 通过 RADIUS 协议上报

BNG插卡设备通过RADIUS协议上报端口预留关系的过程如图6所示。

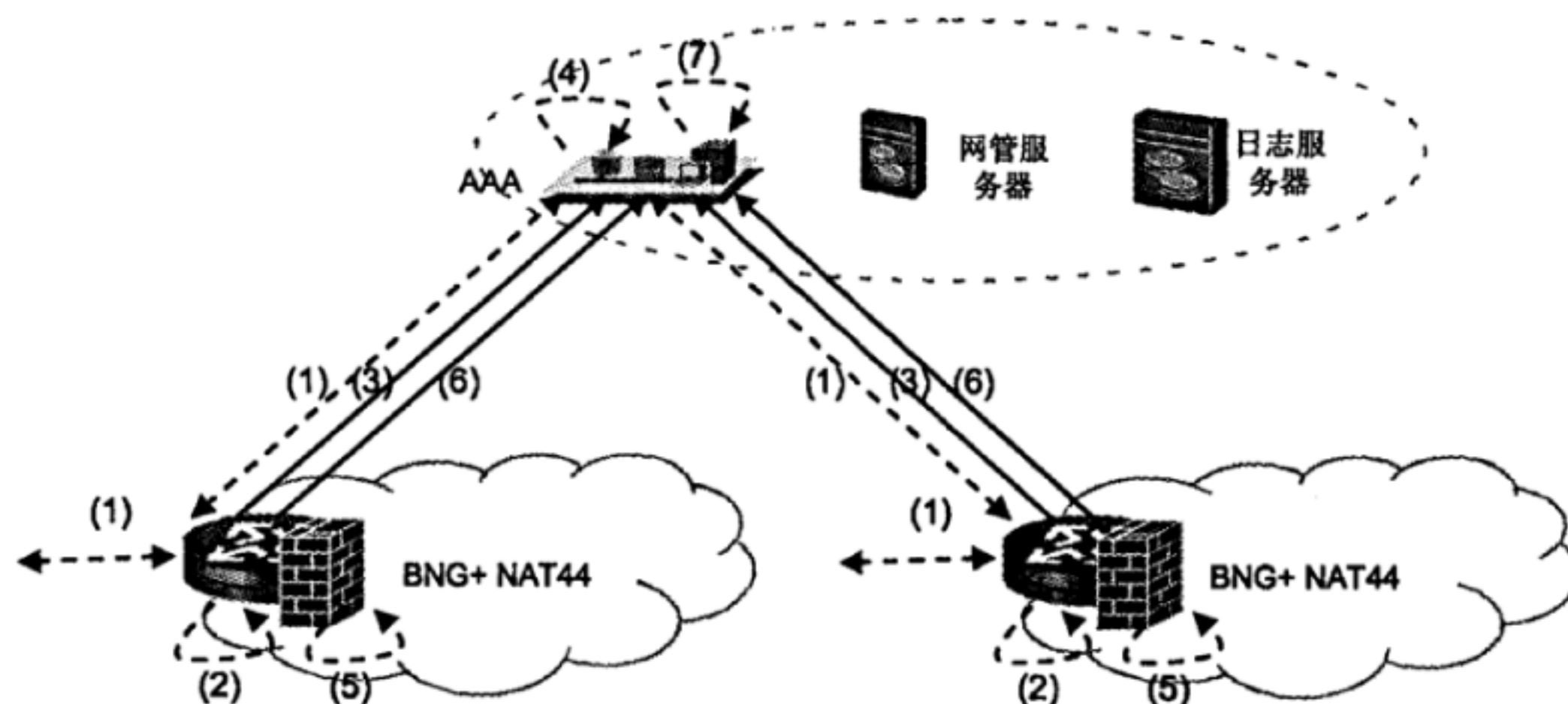


图6 通过 RADIUS 协议上报映射关系



第1步：用户上线，完成用户认证和地址分配。

第2步：BNG插卡设备为用户地址选择外部地址、端口块，创建用户端口预留关系。

第3步：BNG插卡设备在Accounting start消息中向AAA服务器上报告用户地址以及为其预留的外部地址、端口块等信息。这种上报方法要求新增如下的RADIUS属性：

- NAT-IP-Address: NAT 转换后的外部地址；
- NAT-start-Port: NAT 转换后的起始端口号；
- NAT-end-Port: NAT 转换后的终止端口号。

第4步：AAA服务器获得用户地址、外部地址、端口块等信息，生成该用户地址的溯源关系。

第5步：用户下线，BNG插卡设备删除该用户的端口预留关系。

第6步：BNG插卡设备在Accounting stop消息中向AAA服务器上报告用户地址以及之前为其预留的外部地址、端口块等信息。

第7步：AAA服务器删除该用户的地址溯源关系。

## 5.5 告警信息输出

NAT44设备支持通过Syslog协议或者SNMP Trap方式输出告警信息。

NAT44设备支持打开或者关闭告警输出功能。

NAT44设备建议支持FTP方式定期打包发送告警信息。

告警信息至少包括端口用满告警和资源用满告警，要求如下：

### a) 端口用满告警

在用户端口块的所有端口被用满的情况下，该用户后续会话由于没有端口而无法对其进行地址转换，该会话的报文被丢弃。NAT44设备在分配给用户的端口用满情况下，应该能够输出告警信息。告警信息中至少应包含用户地址的信息。

### b) 资源用户告警

在NAT44设备采用动态端口预留的资源分配模式的情况下，如果所有（外部地址、端口块）资源被当前用户预留之后，新的用户由于没有（外部地址、端口块）资源而无法为其预留资源，进而无法对其进行地址转换。NAT44设备在（外部地址、端口块）资源被用满时，应该能够输出告警信息。

## 5.6 应用层 ALG

NAT44必须能支持FTP ALG，其特性符合IETF RFC3022中4.4的规定。

NAT44建议支持的DNS ALG、SIP ALG、RTCP ALG、RTSP ALG、PPTP ALG。

NAT44的各个ALG功能应该能够独立地开启或者关闭。

## 5.7 路由

### 5.7.1 独立设备

独立设备与BNG、路由器互联时，NAT44设备、BNG或者路由器需要设置路由策略，对需要进行NAT44转换的流量转发到NAT44设备处理，对NAT44设备进行地址转换后的流量再转发到BNG和路由器处理。因此独立设备需要支持静态路由以及OSPF、ISIS、BGP等路由协议以及策略路由，实现对NAT44流量的引导。

### 5.7.2 BNG插卡设备

无路由功能方面要求。

### 5.7.3 路由器插卡设备

无路由功能方面要求。

### 5.8 网络时间同步

NAT44设备必须支持网络时间同步协议NTP，支持NTP认证和NTP服务器/客户端，建议支持IEEE1588v2和同步以太网技术。

## 6 性能要求

### 6.1 设备容量

NAT44设备具有多种设备形态，可以分布式部署在BNG层面，也可以集中式部署在网络出口，或者部署在网络汇聚层。因此，有必要将NAT44设备从容量上加以划分以适应网络中不同部署位置对设备容量的需要。

划分NAT44设备的容量级别主要是以NAT44设备所支持的在线用户数为依据。根据NAT44设备整机支持的在线用户数不同建议分为四类：

- A类：支持在线用户数为8万以上；
- B类：支持在线用户数为4万~8万；
- C类：支持在线用户数为1万~4万；
- D类：支持在线用户数为1万~内。

### 6.2 处理能力

对上述四类NAT44设备的会话处理能力要求和日志处理能力要求可参考表1所示指标。

表1 NAT44 设备处理能力要求

	A类	B类	C类	D类
会话处理能力要求				
最大并发会话数	3200万	1600万	800万	200万
流量转发能力	80Gbit/s ≥19.2Mpps	40Gbit/s ≥9.6Mpps	20Gbit/s ≥4.8Mpps	5Gbit/s ≥1.2Mpps
流量与并发会话数配比	每10G的NAT流量支持400万个活动NAT会话	每10G的NAT流量支持400万个活动NAT会话	每10G的NAT流量支持400万个活动NAT会话	每5G的NAT流量支持200万个活动NAT会话
分配端口块速率	≥2000块/秒	≥1000块/秒	≥500块/秒	≥125块/秒
新建 session 速率	≥32万/秒	≥16万/秒	≥8万/秒	≥2万/秒
拆除 session 速率	≥32万/秒	≥16万/秒	≥8万/秒	≥2万/秒
日志处理能力要求				
基于用户方式每秒生成日志数	≥4000条/秒	≥2000条/秒	≥1000条/秒	≥250条/秒
基于 session 方式每秒生成日志数	≥64万/秒	≥32万/秒	≥16万/秒	≥4万/秒

所有级别的NAT44设备均须具备线速处理能力。平均时延要求小于100微秒。

### 6.3 可靠性

NAT44设备必须具有高的可靠性，具体要求如下：

#### 1) 设备可用率

设备必须达到99.99%的可用率。



2) 无故障连续工作时间

设备的平均无故障工作时间: MTBF > 10000h。

3) 故障恢复时间

单板卡故障恢复时间 < 20min;

整机故障恢复时间 < 30min。

NAT44设备必须允许对运行系统进行所有适当的配置更改和软件升级而不影响在线用户。建议版本打补丁时不中断业务, 版本升级时业务中断时间少于30min。

NAT44设备所有元件必须支持热插拔; 支持从故障板卡到备份板卡的自动切换。

对于独立设备, 必须支持主控板、电源模块等关键部件冗余。从主用电源到备用电源的切换必须是自动的, 不能引起业务的中断; 在有冗余配置的情况下, 从机箱中抽走控制板卡及重新插入控制板卡时, 设备必须能够继续转发流量。

## 7 冗余备份要求

冗余备份要求如下:

a) 独立设备

独立设备必须支持设备之间的主备切换。建议支持设备之间会话的实时热备。

独立设备的NAT板卡之间建议支持负荷分担的备份方式。负荷分担方式时, 可采用按用户源地址散列的方式来选择NAT板卡。

独立设备所有元件必须支持热插拔。对于关键部件必须提供冗余备份功能, 包括:

- 控制部件;
- 交换单元;
- 电源模块;
- 风扇。

对于冗余备份部件, 必须支持从故障板卡到冗余板卡到自动切换, 手工切换应该作为选项支持;

b) BNG插卡设备、路由器插卡设备

BNG插卡设备、路由器插卡设备必须支持NAT44板卡之间的主备切换。建议NAT44支持板卡之间会话的实时热备。

BNG插卡设备、路由器插卡设备的NAT44板卡之间建议支持负荷分担的备份方式。负荷分担方式时, 可采用按用户源地址散列的方式来选择NAT板卡。

## 8 安全要求

### 8.1 访问控制和流量控制

NAT44设备必须实现基于源IP的并发会话数限制功能。也即, NAT44设备能够限制每个用户使用的UDP/TCP端口数量和ICMP标识号的数量, 限制的数目必须可以被设置。

建议实现指定会话不受并发会话数限制。该功能可以用于保证重要用户或者重要的应用(例如DNS请求等)不受并发会话数的限制。

必须支持通过ACL作为设定条件对NAT流量进行引导。例如对需要进行地址转换的流量转发到地址转换模块处理, 对不需要进行地址转换的流量(如在同一NAT44设备区域内的用户地址之间的流量)进

行旁路处理。对于独立设备，必须支持基于源地址，目的地址，源端口，目的端口，协议的ACL；对于路由器插卡设备和BNG插卡设备，该ACL功能可在路由器模块或者BNG模块中实现。

## 8.2 路由安全

独立设备必须实现路由协议安全功能，支持OSPF、ISIS、BGP等路由协议的MD5认证，保证路由信息的可信度。

## 9 操作管理维护要求

### 9.1 基本管理功能

NAT44设备应至少支持SNMP网管协议，可与网管配合完成配置管理、性能管理、故障管理和安全管理。

NAT44设备必须支持带外网管，可以将管理流量与用户流量从物理或逻辑上分开，带外网管与带内网管具有同等的功能。对于带外访问应实现访问控制，防止非法访问。

NAT44设备必须支持SNMPv1、v2、v3网管协议。

NAT44设备必须实现接口组MIB、IP MIB、SNMPv1 MIB、SNMPv2 MIB、SNMPv3 MIB等常用MIB库。

### 9.2 配置管理

配置管理要求如下。

#### a) 独立设备

独立设备要求具备可管理性，设备必须支持通过Console Port 或Telnet的模式实现配置管理。

在设备配置手段方面：

- 必须支持手动配置方式；
- 必须支持配置下发接口；
- 必须支持根据网管服务器下发的参数对外部地址的端口块进行预分配。

#### b) BNG插卡设备

BNG插卡设备必须满足BNG的相关配置管理技术要求。

#### c) 路由器插卡设备

路由器插卡设备必须满足路由器相关配置管理技术要求。

### 9.3 性能管理

设备应支持对其性能的管理，包括：

- 并发连接数（在线用户数）；
- 吞吐量；
- 连接超时时间；
- 端口块占用率；
- 资源占用率；
- 单板 NAT 流转发性能；
- 单板流表规格；
- 单板地址池数量；
- 单板建流速度；
- 单板 ALG 处理能力。



#### 9.4 故障管理

NAT44设备必须能够向网管服务器发送告警信息；在告警信息中提供足够的信息以协助排障，例如日期时间戳、严重程度、部件标识、软件/硬件/固件版本等。

NAT44设备必须在网管服务器无法工作时提供远程访问的手段；必须提供自检测或者故障诊断手段/工具。

NAT44设备必须能够支持网管服务器进行的设备配置轮询和状态轮询，发现设备问题时发送告警信息。

NAT44设备必须能够支持通过Syslog协议发送设备运行日志信息。

#### 9.5 安全管理

NAT44设备必须支持管理的安全功能，必须支持通过用户名和口令实现对设备的管理和控制；必须支持采用加密的方式进行安全的远程访问，如SSH。对于远程访问必须实现访问超时控制、远程访问连接数限制、远程登录尝试次数限制、远程访问的相关信息记录（如访问终端的地址，端口，用户名和密码）等。

对于通过console端口的访问，NAT44设备也应实现访问超时、访问连接数、登录尝试次数等安全控制。

NAT44设备必须支持分级分权管理。

NAT44设备建议支持通过RADIUS进行网管登录密码认证，对密码进行集中管理。

NAT44设备应提供对登录口令长度的控制要求，建议至少不少于8个字符。

NAT44设备必须具有良好的访问控制，对设备的所有网管操作都可配置为需要经过认证和授权方可进行；必须支持网管日志功能，对超越权限或者失败的关键操作进行登记并作为安全告警；操作失败必须提供安全性审计的功能；并提供一种方法来记录配置的改变及操作人员改变配置的时间。

### 10 物理接口要求

#### 10.1 插卡设备

路由器插卡设备和BNG插卡设备的NAT44功能板卡不需要物理接口。

#### 10.2 独立设备

独立设备对外物理接口应支持标准的千兆以太网光/电接口，其接口特性应符合YD/T 1097-2009的5.2.2的要求。可选支持10G以太网光/电接口，其接口特性应符合YD/T 1097-2009的5.2.3的要求。

可以灵活配置接口板卡数量，使接入带宽与NAT板卡流量转发能力保持一致。

### 11 环境要求

NAT44设备的环境要求与BNAS或中低端路由器的环境要求一致，见YD/T 1148-2005第11章。

### 12 电源与接地

NAT44设备的电源和接地要求与BNAS或中低端路由器的电源和接地要求一致，见YD/T 1148-2005第12章。

### 13 例行试验

NAT44设备试验要求与YD/T 1148-2005中第13章的要求一致。



中华人民共和国  
通信行业标准  
运营级 NAT44 设备技术要求  
YD/T 2544-2013

\*

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 7 月第 1 版  
印张: 1.25 2014 年 7 月北京第 1 次印刷  
字数: 30 千字

15115 • 242

定价: 15 元

本书如有印装质量问题, 请与本社联系 电话: (010)81055492