ICS 33.040.01
M 19

YD

中华人民共和国通信行业标准

YD/T 2820-2015

智能型通信网络
固定网络策略控制设备
和策略执行设备技术要求

Technical specification of fixed policy control and enforcement equipments in the intelligent telecommunication network

2015-04-30 发布　　2015-07-01 实施

中华人民共和国工业和信息化部　发布

目　　次

前　言

本标准是智能型通信网络策略管控系列标准之一,该系列标准的名称和结构预计入下：

——《智能型通信网络 总体框架和要求》；

——《智能型通信网络 策略管控能力开放需求》；

——《智能型通信网络 策略管控能力开放架构与技术要求》；

——《智能型通信网络 策略控制系统架构和技术要求》；

——《智能型通信网络 固定网络策略控制设备和策略执行设备技术要求》。

本标准按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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、华为技术有限公司、中国联合网络通信集团有限公司、中兴通讯股份有限公司、武汉邮电科学研究院。

本标准主要起草人：王　茜、徐向辉、薛　莉、杜宗鹏、朱　鹏、范　亮、朱国胜。

智能型通信网络
固定网络策略控制设备和策略执行设备技术要求

1 范围

本标准规定了固定网络策略控制系统在智能型通信网络的定位和组成，固定网络策略控制系统的应用场景和能力需求、固定网络的策略配置方案、以及固定网络策略控制和策略执行设备的技术要求。

本标准适用于固定网络策略控制系统中的策略控制设备和策略执行设备。

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。

GB 9254　　信息技术设备的无线电骚扰限值和测量方法

YD/T 1148-2005　网络接入服务器技术要求——宽带网络接入服务器

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

认证授权计费服务器　Authentication, Authorization, and Accounting Server

一个能够处理用户访问请求的服务器，它提供认证、授权以及计费服务。

3.1.2

宽带网络接入服务器　Broadband Network Access Server

面向宽带网络应用的接入网关，它位于骨干网的边缘层，负责用户宽带网络的数据接入。

3.1.3

固定网络策略控制节点　Fixed Policy Decision Point

固定网络策略控制系统中制定策略的逻辑实体，用于控制策略执行节点，可以是一个独立的设备或者与其他设备合并部署。

3.1.4

固定网络策略执行节点　Fixed Policy Enforcement Point

固定网络策略控制系统中执行策略的逻辑实体，PEP部署在固定网络的已有网元中，支持PEP功能的固定网络网元可以在策略控制节点的控制下执行策略。

3.1.5

策略服务器　Policy Server

一个包含PDP功能的网络服务器，通常会为多个PEP服务。

3.1.6

深度包检测　Deep Packet Inspection

一种基于应用层的流量检测和控制技术，它能更精细地识别网络中的各种应用，并为网络运营中的业务识别、业务控制和业务统计服务。

3.1.7

会话　Session

一个逻辑概念，代表网络节点上的一个网络连接服务实例，是策略应用的对象。

3.2　缩略语

以下缩略语适用于本文件。

AAA	Authentication, Authorization, and Accounting	认证授权计费
AC	Access Controller	WLAN接入控制节点
ANCP	Access Node Control Protocol	接入节点控制协议
AP	Access Point	WLAN接入节点
APN	Access Point Name	接入点
ATM	Asynchronous Transfer Mode	异步传输模式
BBF	Broadband Forum	宽带论坛
BNAS	Broadband Network Access Server	宽带接入网关
CDN POP	Content Delivery Network Point Of Presence	内容分发网络访问点
COA	Change of Authorization	会话授权更改
DoS	Denial of Service	拒绝服务
DPI	Deep Packet Inspection	深度包检测
DSCP	Differentiated Services (Diffserv) Code Point	差分服务代码点
DSLAM	Digital Subscriber Line Access Multiplexer	数字用户线接入复用设备
IDC	Internet Data Center	互联网数据中心
IPoE	IP over Ethernet	以太网承载的IP
LI	Lawful Interception	合法监听
LPDP	Local Policy Decision Point	本地策略控制节点
MPLS	Multi-Protocol Label Switching	多协议标签交换
NAT	Network Address Translation	网络地址转换
P2P	Peer-to-Peer	点到点
PCRF	Policy and Charging Rules Function	策略与计费规则功能单元
PDP	Policy Decision Point	策略控制节点
PEP	Policy Enforcement Point	策略执行节点
PPPoE	Point to Point Protocol over Ehternet	以太网上的点对点协议
QoS	Quality of Service	服务质量
RADIUS	Remote Access Dial-In User Service	远程用户拨号认证系统
RG	Residential Gateway	家庭网关
SR	Service Router	业务路由器

STB	Set Top Box	机顶盒
VCI	Virtual Channel Identifier	虚通道标识符
VLAN	Virtual Local Area Network	虚拟本地网
VoD	Video on Demand	视频点播
VoIP	Voice over Internet Protocol	IP电话
VPI	Virtual Path Identifier	虚路径标识符
VPN	Virtual Private Network	虚拟专用网络
VRF	Virtual Routing Forwarding	VPN路由转发表

4 固定网络策略控制系统的定位和组成

4.1 固定网络策略控制系统在智能型通信网络中的定位

智能型通信网络策略控制系统既包括固定网络的策略控制，也包括移动网络的策略控制。本标准规定的固定网络策略控制系统属于其中的固定网络的策略控制部分。

根据智能型通信网络总体框架和要求，智能型通信网络的架构和接口如图1所示。

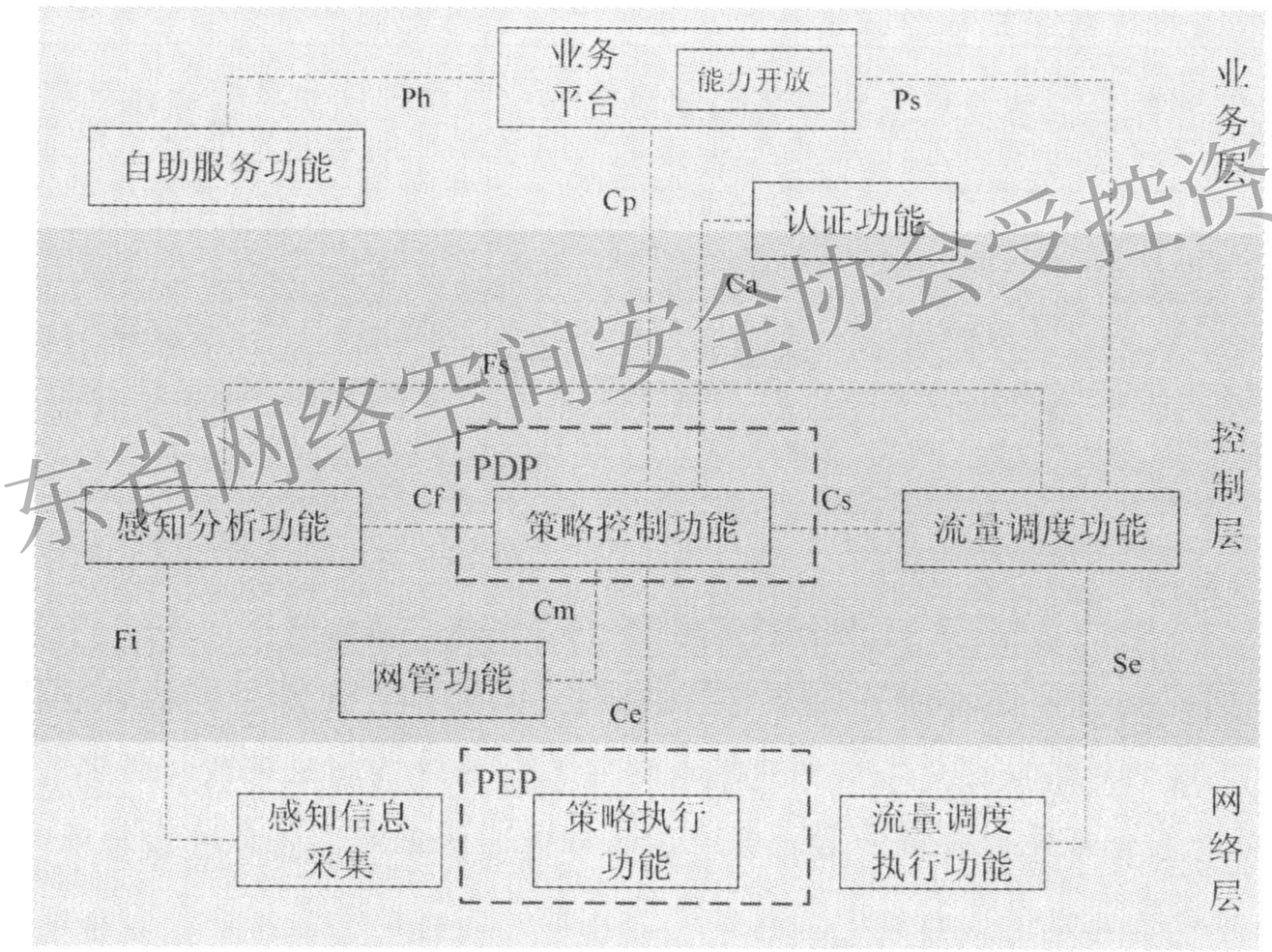

图1 智能型通信网络架构接口图

固定网络策略控制系统主要包括策略控制节点PDP和策略执行节点PEP。对应到智能型通信网络体系架构中，固定网络策略控制系统涉及在PDP设备实现的控制层的策略控制功能，以及在PEP设备实现的网络层的策略执行功能。固定网络策略控制系统涉及的接口包括Cp，Ce，Ca，Cm，Cf，Cs。

固定网络策略控制系统属于智能型通信网络架构中统一的策略控制实现的第一个阶段。在这个阶段中，移动网络和固定网络的统一策略控制采用3GPP和BBF定义的互通方式实现，如图2所示。

因此，固定网络策略控制系统除了可以对固定网络的业务进行策略控制之外，还可以通过S9a接口与移动策略控制系统互通，对流经固定网络的移动业务流量进行策略控制。

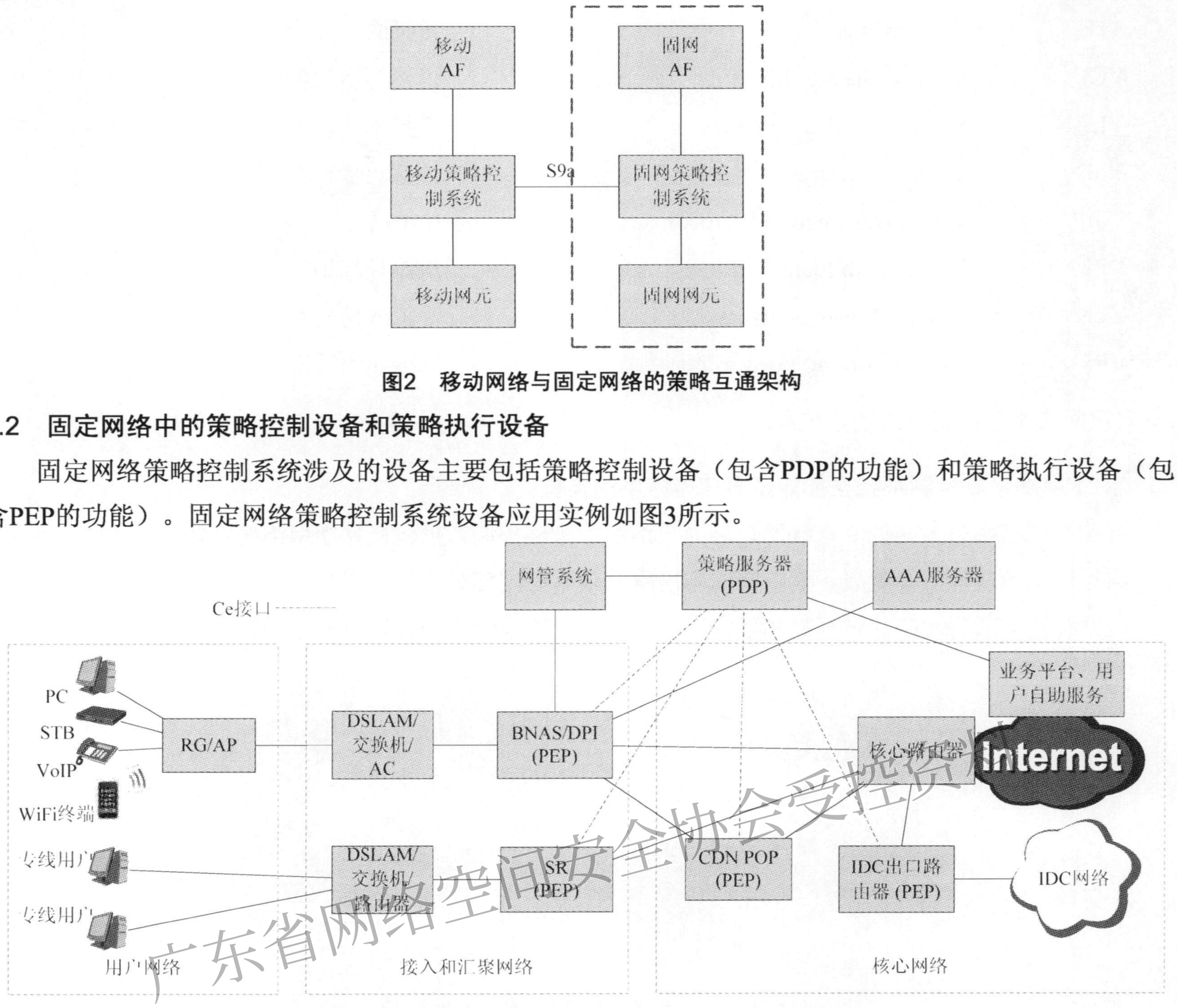

图2　移动网络与固定网络的策略互通架构

4.2　固定网络中的策略控制设备和策略执行设备

固定网络策略控制系统涉及的设备主要包括策略控制设备（包含PDP的功能）和策略执行设备（包含PEP的功能）。固定网络策略控制系统设备应用实例如图3所示。

图3　固定网络策略控制系统设备应用实例

PDP和PEP都是逻辑实体，可以在固定网络不同的网元中实现。在固定网络中，PDP设备负责策略制定,可以是一个独立的设备（Policy Server），或者部署在AAA服务器中。PDP设备也可能和PEP设备合并部署，例如在BNAS设备中既部署PDP的功能，也部署PEP的功能。此外，即使部署了独立的PDP设备，也不排除在PEP设备上（如BNAS）实现本地的PDP（LPDP）功能的策略控制部署方式。

PEP设备对应固定网络中的个人用户接入、专线用户接入、VPN、组播等各种业务涉及的相关网络设备，包括BNAS/DPI、SR、IDC出口路由器、CDN POP等。这些实现了PEP功能的固定网络设备，可以在策略服务器的控制下执行动态的策略，以实现固定网络中端到端的QoS保障。

5　固定网络策略控制系统应用场景和能力需求

5.1　固定网络策略控制应用场景

固定网络策略控制系统的主要功能是针对宽带接入用户，基于用户/用户群或特定应用，进行带宽配置、QoS标记、接入控制、用量管理、安全性管理、灵活计费、重定向等动态控制；其主要的应用场景如下：

5.1.1　场景一：对特定用户或特定应用进行带宽按需调整

用户在具有高带宽需求时，如临时观看高清电影，用户下行带宽从原来的4M提升到20M，以获得流畅的观看效果。

针对特定应用，使用该应用的所有用户均获得自动的带宽提升。根据应用类型，可调整上行带宽或下行带宽。

5.1.2 场景二：对特定用户或特定应用打 QoS 标记

运营商的VIP用户在使用运营商自营业务时，获得高优先级标记，在网络中得到优先转发和更好的体验。

5.1.3 场景三：对访问特定地址的流量或特定应用的流量区分计费

对于访问特定地址或者特定应用的流量执行单独的计费策略，以实现基于应用类型的精细化计费，例如对特定应用采用按流量计费或定制灵活的计费套餐，或对WiFi方式访问的流量进行单独的流量计费。

5.1.4 场景四：低值高消耗流量在达到一定流量门限时，进行接入控制、限速或降级

普通用户的P2P流量超过套餐中规定的门限后，对其P2P流量进行丢弃、降低速率或降低优先级。

5.1.5 场景五：对非法流量进行安全性控制或接入控制

检测到攻击性流量、非法VoIP等流量后，对其进行阻截。

5.1.6 场景六：在用户流量或特定应用流量达到一定门限时，采用不同的费率

当用户总流量或协约应用的流量超过套餐限额后，超出部分按一定费率计费，使用量越多，费率越低，从而鼓励用户使用流量（适合流量计费场景）。

5.1.7 场景七：对特定用户访问进行重定向

特定账号的用户访问禁止类网站时，如绿色上网用户的孩子访问黑名单网站，自动转向到固定网页。

欠费用户访问网站时，自动转向到运营商付费门户。

5.1.8 场景八：对企业用户带宽进行按需调整

租用互联网专线的企业用户，在有视频会议或数据备份等大带宽应用需求时，可以动态调整接入带宽，并提升QoS优先级。

5.2 固定网络策略控制系统能力需求

固定网络策略控制系统应提供基于策略的宽带网络服务，能够灵活的配置、生成、动态的或者静态的激活、管理、执行这些策略。对应上文中的应用场景，固定网络策略控制系统的主要能力需求包括：

——根据用户账号/用户组、五元组、应用层信息、维度组合等对匹配流量进行带宽调整；

——根据用户账号/用户组、五元组、应用层信息、维度组合等对匹配流量打 QoS 标记；

——根据用户账号、五元组、应用层信息、维度组合等对匹配流量进行计费；

——根据用户账号/用户组、五元组、应用层信息、维度组合等对匹配流量进行用量管理，当用量达到门限时，进行限速、QoS 标记修改、接入控制等操作；

——对检测分析到的非法流量进行安全性控制；

——根据用量报告进行费率控制；

——根据用户账号、五元组、应用层信息、计费信息等对匹配的网页访问流量进行重定向；

——对企业专线进行带宽调整及 QoS 标记。

6 固定网络策略配置方案

6.1 静态配置的方式

固定网络的策略控制系统应支持基于静态配置的策略控制方式。在这种方式中，网络管理员可以在设备上使用命令行，或者通过远程的网管系统为每个PEP节点配置静态的策略和QoS。具体网络管理员需要配置策略执行的对象，策略的触发方式和策略的行为。相关的策略和QoS配置属性都在本地节点保存（该节点包含LPDP的功能），这种方式适用于很少发生改变的策略的配置和执行。

基于静待配置的策略控制配置方案如图4所示，此处使用BNAS设备作为PEP设备的代表，这种配置方案也适用于其他类型的PEP设备的策略配置场景。

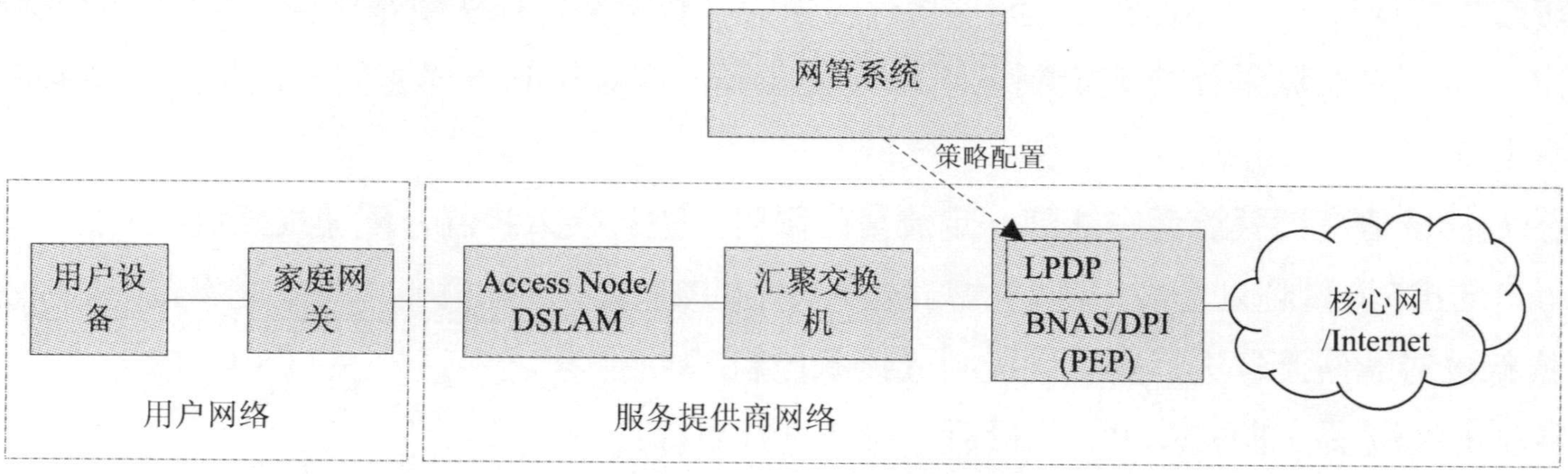

图4 基于静态配置的策略控制

这种方案的配置特点是每个节点保持静态配置的策略和QoS，仅在网络管理员对其进行修改时发生变化，不支持策略的动态更改。这种策略配置和执行的方式执行对象一般不会精细到每个用户，而是针对在同一个物理接口或者虚接口上线的用户。

6.2 动态配置的方式

6.2.1 AAA 动态控制的方式

基于AAA的动态策略控制配置方案通过AAA服务器来维护策略和QoS，AAA服务器包含PDP的功能。在该方式中，当用户的PPPoE或者IPoE的会话在BNAS建立时，AAA服务器响应BNAS的请求，可以向其提供该会话的策略和QoS配置，BNAS根据收到的策略和QoS配置对用户执行策略。

这种配置方案如图5所示，这种配置方案用于用户上线需要认证的场景，因此仅适用BNAS设备作为PEP设备的场景。

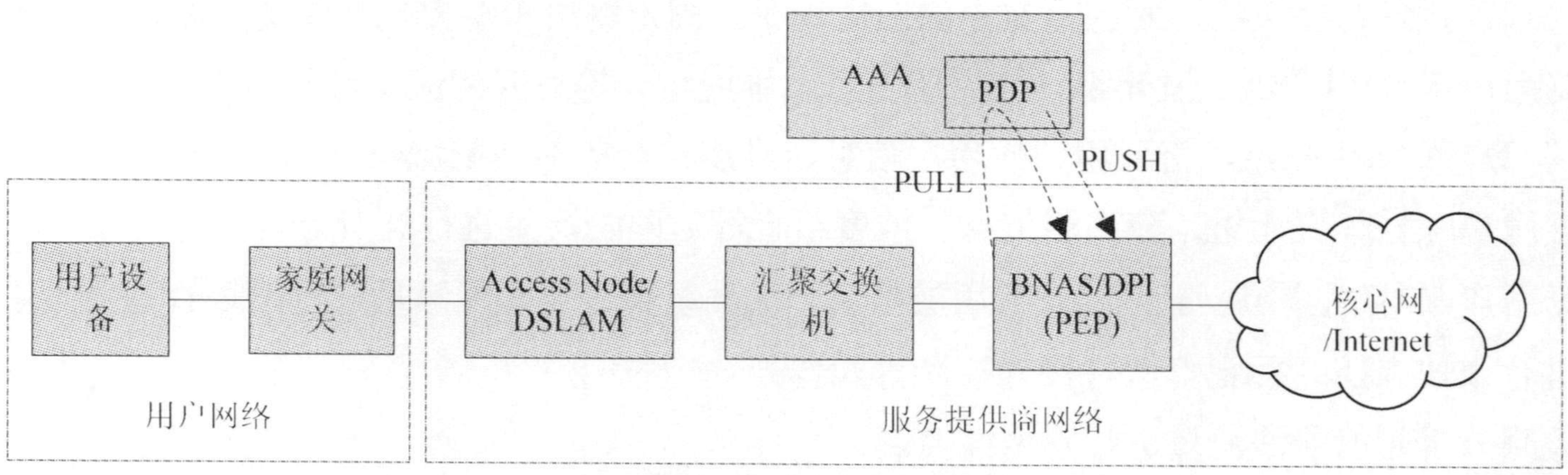

图5 基于 AAA 的动态策略控制

具体的，如果使用了RADIUS协议，在用户认证时，BNAS会发送RADIUS Access Request消息给AAA，其中携带了用户的相关标示；之后如果AAA通过用户认证，则AAA会回复Access Accept消息给BNAS，

其中携带了该用户相关的策略和QoS配置信息，对应图中PULL的方式。当策略发生变化时，AAA通过RADIUS COA消息动态修改用户的相关策略，对应图中PUSH的方式。

6.2.2 策略服务器动态控制的方式

策略服务器动态控制策略配置方案假设网络中部署了独立的策略服务器，其中包含PDP的功能。策略服务器支持动态地下发策略，例如策略服务器使用RADIUS的COA消息下发策略到BNAS，对应PUSH方案；同时也支持BNAS在网络事件发生或者会话状态变化时，从策略服务器动态的获取策略和QoS配置信息，对应PULL方案。

PUSH方案的触发可能有三种情况：第一种是网络管理员通过网管系统配置策略控制节点触发策略的执行；第二种是用户通过自服务系统申请策略的改变，导致策略控制节点进行策略的动态修改；最后一种是在用户接入特定的应用时，业务平台模块触发的用户会话的策略改变。

PULL方案由会话或网络事件触发，如用户接入的时长或者流量达到配额，或者DPI探测到特定的用户应用，此时固定网络策略控制系统的策略执行节点上报事件给策略控制节点触发策略的执行。

这种方案如图6所示，此处使用BNAS设备作为PEP设备的代表，这种配置方案也适用于其他类型的PEP设备的策略配置场景。

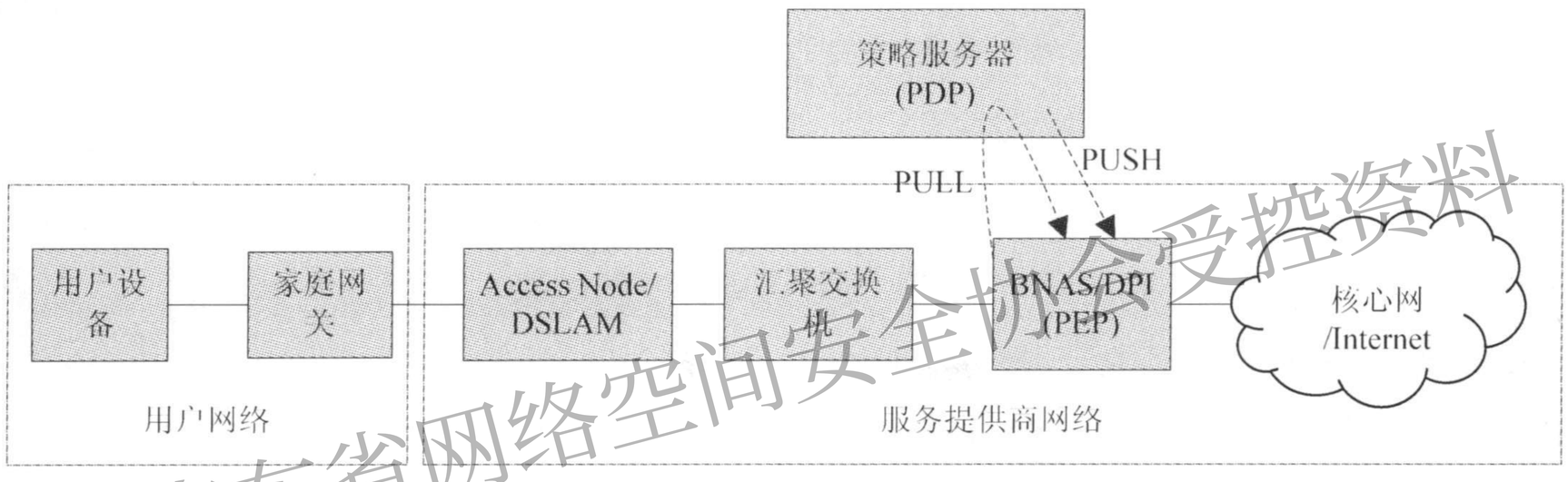

图6 基于策略服务器的动态策略控制

在这种策略配置方案中，BNAS设备与策略服务器交互来获得用户对应的策略和QoS。固定网络中的策略的生成和下发的基本流程如下：用户上线之后，BNAS设备会上报用户的用户/用户组信息给策略服务器（例如从AAA获得），策略服务器根据用户标示匹配策略数据库中的策略，生成相应的策略下发给BNAS设备执行。

固定网络策略控制系统中的策略服务器支持下发完整的策略模板和相关参数给BNAS设备执行，同时也支持在BNAS设备上的LPDP中预先配置相应的策略模板和模板名称，策略服务器/AAA服务器可以仅下发策略模板名称和必要的参数，在BNAS上生成相应的策略。

6.3 ANCP

固定网络中的BNAS设备应支持通过ANCP实现接入链路上的策略和QoS策略的配置和执行。这种方案如图7所示，仅适用BNAS设备作为PEP设备的场景。

BNAS设备在与AAA服务器/策略服务器交互获得策略之后，可以再通过ANCP协议将其提供给接入线路上的AN/DSLAM执行相应的策略。例如，用户的PPPoE或者IPoE会话的建立会触发BNAS发送端口配置请求，BNAS设备也可以在AN/DSLAM配置相应的组播策略。

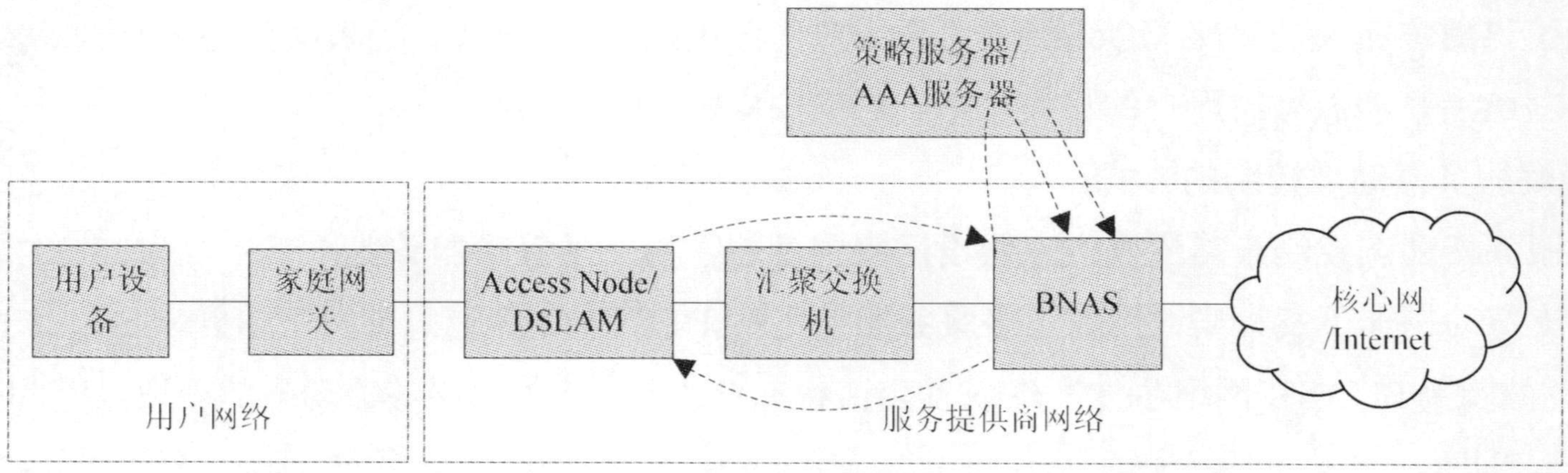

图7　基于策略服务器/AAA 和 ANCP 策略控制

7　PDP 设备功能技术要求

7.1　感知分析功能联动技术要求

固定网络中的 PDP 设备应支持与感知分析系统联动，根据感知系统的识别结果执行动态的策略。在固定网络策略控制系统中，感知分析功能模块可以将感知信息的分析结果输出到策略控制功能模块，作为策略动态调整与制定的一个输入条件。

7.2　策略制定和下发

7.2.1　策略制定技术要求

根据感知分析功能的输出结果和策略控制节点与相关网元的交互，策略控制节点 PDP 执行策略控制和应用保障功能。PDP 设备应支持根据以下信息制定策略：

——从感知分析功能模块得到的用户/业务/网络信息的分析结果；

——从业务平台模块得到的信息，例如会话和用户相关信息；

——从 PEP 设备得到的信息，例如会话属性、请求类型和用户相关信息；

——从 AAA 服务器得到的信息；

——从用户数据库得到的信息，例如用户和服务相关的信息。

7.2.2　策略下发技术要求

PDP 设备策略下发的相关技术要求包括：

——PDP 设备应支持将制定的策略下发给策略执行节点。具体的，PDP 设备应支持控制 PEP 设备对特定的会话执行策略操作，包括策略的安装、激活、去活、修改和删除；PDP 设备应支持对上行和下行的流量执行动态实时的策略修改。

——PDP 设备应支持 PEP 触发的策略下发，即在收到 PEP 报告的网络事件或者会话状态改变之后，PDP 设备支持相应策略的下发。

——对于一个用户会话，可能会有几个策略连续执行。PDP 设备应支持嵌套策略的触发，例如在分配给一个媒体流需要的带宽时，也会触发相应的计费策略。

7.2.3　PDP 设备发给 PEP 设备的消息

PDP 设备应支持提供以下的消息及其参数给 PEP 设备：

——用户会话建立时，PDP 设备应支持向 PEP 提供策略规则；

——特定的网络事件发生或者会话状态变化时，PDP 设备应支持向 PEP 提供用户会话的策略更新；

——订阅特定事件的请求消息。

7.3 流量调度功能联动技术要求

PDP 设备应支持与流量调度功能联动，相关技术要求包括：

——PDP 设备应支持根据感知分析功能提供的信息，触发流量调度相关的策略。具体的，PDP 设备应支持按照网络情况对用户流量进行分流，以及保证高优先级用户的 QoS。

——PDP 设备应支持按照业务类型、用户/用户组、或者用户特定应用的粒度控制网络流量的流向。

7.4 应用接入控制技术要求

当用户接入有QoS要求的应用（例如VoD）时，业务平台模块的服务应用通过与固定网络策略控制系统的信令交互来参与网络资源的分配。网络运营商使用固定网络策略控制系统，根据相应的策略来控制服务应用的接入请求。PDP在收到应用的资源申请时应考虑运营商的业务策略和网络资源的使用情况，接受或者拒绝应用的接入请求。

PDP设备的应用会话接入控制相关设备技术要求包括：

——PDP 设备应支持业务平台的应用会话请求的资源分配。

——PDP 设备应支持根据运营商的业务策略来授权应用请求。具体的，PDP 设备支持在特定的时间允许接入，或者允许属于特定的用户组的用户接入。

——PDP 设备应支持根据网络资源情况来接受或者拒绝服务应用的接入请求。具体的，PDP 设备在接入控制中应考虑的因素包括：

- 应用的要求，例如带宽和 QoS 等；
- 用户预订带宽的剩余量；
- 网络带宽使用情况；
- 网络拓扑；
- 可用的网络容量。

——PDP 设备支持的资源预留模型可以是基于预配置的静态网络拓扑和带宽，也可以基于动态学习的网络拓扑和带宽。

——在部分网络节点失效时，PDP 设备应支持自动重新建立带宽预留。

——PDP 设备在分配网络资源时，应支持高优先级的应用请求抢占低优先级应用的资源预留。

7.5 多播控制技术要求

多播是固定网络应支持的一个重要能力，策略控制节点PDP应支持多播的策略控制。具体的，针对每一个多播组，PDP设备应能够控制多播的复制策略，即在何处用何种方式来进行多播的复制。

8 PEP 设备功能技术要求

8.1 PEP 设备总体技术要求

8.1.1 策略执行技术要求

PEP设备应支持的策略执行相关的设备技术要求包括：

——PEP 设备应支持 PDP 下发的策略的执行。具体的，策略执行节点 PEP 应支持对上行和下行的流量执行动态的策略；策略执行节点 PEP 在 PDP 的管理下执行策略的安装、激活、去活、修改和删除，并且支持上报 PDP 策略的执行结果。

——PEP 设备应支持静态配置的策略和动态执行的策略。具体的，PEP 设备应支持通过网管系统配置静态的策略，以及在用户认证时从 AAA 服务器得到静态的策略；PEP 设备应支持从 AAA 服务器得到

更新的策略，以及在 PDP 设备的控制下执行动态的策略，并且支持修改配置策略的参数。

——PEP 设备应支持基于用户或者业务类型执行策略，或者基于时段、应用持续的时间以及网络链路的拥塞状况等因素执行策略。

——PEP 设备应支持在识别用户/业务后按照 PDP 的控制，在不同的粒度上执行策略，其策略执行的对象可以是用户账号/用户组、五元组、应用层信息、维度组合等，相关的策略包括 QoS 和带宽控制、流量转发和计费等。

8.1.2 策略执行的对象

PEP设备应支持按照一个IP会话，IP流或者流量集合的粒度执行策略。PEP设备可以根据会话的标识，按照PDP下发的策略对一个或者多个会话执行策略；也可以根据PDP提供的流量过滤器对会话的部分流量执行策略。PEP设备应支持按照以下流量标示识别用户和业务以执行相应的策略：

——物理接口；

——Ethertype；

——Ethernet VLAN-ID，ATM VPI/VCI，MPLS 标签；

——源/目的 MAC 地址；

——源/目的 IP 地址；

——PPPoE 会话 ID；

——802.1p、DSCP、MPLS EXP；

——源/目的 TCP/UDP 端口；

——IP 头的协议类型；

——其他分组中的相关信息。

8.1.3 QoS 和带宽控制

策略执行节点PEP应支持QoS和带宽控制相关策略的执行，具体包括：

——PEP 设备应支持用户和业务的 QoS 策略，包括带宽控制、流量标记和优先级调度等。具体的，PEP 设备应支持用户分等级的 QoS 机制，按需保障高等级用户或高价值业务的服务质量，可以基于用户的等级、流量或接入时长等执行 QoS 策略。

——PEP 设备应支持在 PDP 设备的控制下动态的调整 QoS 策略。

——PEP 设备应支持用户业务的带宽保证能力，即 PEP 设备应支持在策略控制节点的控制下分配接入网络带宽。具体的，策略执行节点应了解目前带宽资源的使用情况，并且可以接受或者拒绝策略控制节点的策略更改请求或者网络资源分配请求。

8.1.4 流量转发策略

PEP设备应支持用户流量转发策略的执行。策略执行节点应支持将特定的用户或者业务的流量转发到后端连接的功能模块，例如：

——特定的 VRF；

——NAT 功能模块；

——DPI 模块；

——合法监听 LI 模块；

——HTTP 重定向特性模块；

——连接到移动核心网的特定的隧道。

8.1.5 计费策略

策略执行节点 PEP 应支持计费策略的执行，相关技术要求包括：

——PEP 设备应支持生成计费信息，并且通过 RADIUS 或者 Diameter 协议与 AAA 服务器交互。

——PEP 设备应支持按照用户的流量或者接入时长情况生成计费信息。

——PEP 设备应支持监测服务的使用情况，支持用户/业务相关的时间/流量的配额。

——PEP 设备应支持精细化的计费能力，具体包括按 QoS 策略生成计费信息、按应用生成计费信息、按访问地址生成计费信息、按时段生成计费信息、按内容类型生成计费信息。

8.1.6 应用流量检测和上报

PEP 设备应支持上报网络情况和会话的相关事件，这些事件可以是 PDP 设备事先订阅的，也可以是无条件地报告给 PDP 设备。

——PEP 设备应支持 PDP 订阅的事件的上报，具体包括用户的累计接入时长或者流量超过限额，用户接入特定应用的时长或者流量到达门限等。

——PEP 设备应支持网络事件或者用户会话事件的上报，具体包括网络异常，网络拥塞，和用户离线等。

8.2 BNAS 作为 PEP 设备的技术要求

8.2.1 感知信息采集

PEP 功能在 BNAS 上实现时，为了支持对特定的用户或特定应用执行策略，BNAS 应支持对用户/业务/应用等的精确感知，以及在特定的网络事件发生时上报 PDP 设备。此时，PEP 设备应实现智能型通信网络中感知信息采集功能模块中与策略相关的信息的感知。PEP 设备应支持的感知信息采集功能如下：

——PEP 设备应支持用户信息的感知和采集，这些用户信息包括：

- 用户属性信息，如用户身份、用户 IP 地址、用户优先级、用户订购的业务及费用信息；
- 用户位置信息，如用户所属的区域、用户所处的地理位置、用户所属的接入网络及其子网（如 VLAN ID）、用户接入的业务网络（如 APN，在与移动网络互通时使用）、用户线端口信息；
- 用户行为信息，如用户喜好、用户访问习惯；
- 用户终端信息，如设备厂商、设备类型、操作系统。

——PEP 设备应支持业务信息的感知和采集，这些业务信息包括：

- 业务属性信息，如业务类型、业务优先级、应用 ID 信息、业务流描述信息；
- 业务对网络资源的要求，如需要的带宽。

——PEP 设备应支持网络信息的感知和采集，这些网络信息包括：

- 网络资源信息，如链路带宽、带宽利用率；
- 网络拓扑信息，如不同类型接入网的拓扑、业务路径、路由开销。

8.2.2 DPI

为了感知识别用户具体的业务类型，例如语音通话，VoD会话，游戏会话或者P2P会话等，应对IP分组进行L4-7的深度包检测（DPI）。在网络部署时，DPI模块可以部署在BNAS或者单独部署在BNAS

之后。如果单独部署，DPI节点就是一个单独的PEP设备，BNAS应执行相应的流量转发策略将需要执行DPI操作的流量转发给DPI设备。

PEP设备应支持的DPI相关技术要求包括：

——支持 PEP 功能的 DPI 设备应支持应用层特征字的识别。

——支持 PEP 功能的 DPI 设备应支持将业务分析结果上报给 PDP 设备。

——支持 PEP 功能的 DPI 设备应支持由业务分析结果触发的基于业务流的策略，这种策略在数据分组匹配某个特定的条件时触发，随后 DPI 设备会对该数据分组执行某种操作，如接入/阻塞等安全规则，或者优先级调度、整形和限速等 QoS 策略。

——当支持 PEP 功能的 DPI 设备通过 DPI 技术检测到特定的需要 QoS 保障的业务时，DPI 设备应支持上报 PDP 设备申请相应的 QoS 策略。

8.2.3 接入节点控制

当 BNAS 作为 PEP 节点接受到 PDP 的策略之后，BNAS 可以通过 L2CM/ANCP 机制控制接入节点的策略执行。PEP 设备应支持的接入节点控制技术要求包括：

——作为 PEP 设备的 BNAS 应支持 BBF 定义的 L2CM 机制以及 IETF 定义的 ANCP 协议。具体的，BNAS 应支持向接入设备发送控制消息，接受接入设备的反馈，以及接受接入设备的信息上报。

——为了解决 BNAS 设备 ANCP Peer 过载问题，BNAS 下挂的 PEP 设备应支持 ANCP Proxy 功能，汇聚 ANCP 链接。

8.3 其他 PEP 设备技术要求

当 BNAS/DPI 以外的设备作为 PEP 设备（如 SR、IDC 出口路由器、CDN POP）时，应支持的 PEP 设备技术要求如下（这些设备不会包含 BNAS 与 AAA 交互，即用户认证和计费相关的技术要求）：

——SR 作为 PEP 设备，应支持基于专线用户、业务、VPN 等网络拓扑信息的感知，以及基于专线用户的 QoS 控制、VPN 带宽控制等执行能力；

——IDC 出口路由器作为 PEP 设备，应支持基于 IDC 下行流量的策略执行能力，包括基于五元组和应用层信息的感知能力、QoS 策略执行能力等；

——CDN POP 作为 PEP 设备，应支持用户、内容和内容源的感知能力，以及内容分发、内容过滤、QoS 处理、热点选择等相关的策略执行能力。

9 固定移动网络互通技术要求

固定网络策略控制系统应该支持固定网络和移动两个网络协同工作的能力。移动网络中的策略控制模块是PCRF，它通过S9a接口与固定网络策略控制设备通信。固定网络策略控制系统在移动终端接入时应支持和PCRF互通，接收移动用户的相应策略，在固定网络中执行。

PDP设备的移动网络互通相关设备技术要求包括：

——当移动终端通过固定网络接入时，PDP 设备应支持通过 S9a 接口接受移动网络网元 PCRF 提供的用户策略相关信息，包括用户标示、用户等级、带宽需求、用户的流量标示等。

——对于 PCRF 下发的策略，PDP 设备应支持根据目前固定网络的情况对移动用户申请的资源进行评估，如果接受就分配资源并且返回确认消息，如果不接受就返回拒绝。在拒绝时，PDP 设备可以返回一个可接受的上行或者下行带宽。

——当移动终端通过固定网络接入时，PDP 设备应支持按照用户请求和业务类型控制 PEP 设备执行

对应的流量转发策略。

PEP 设备的固定移动网络互通相关设备技术要求包括：

——当移动终端通过固定网络接入时，PEP 设备应支持按照 PDP 设备下发的策略对其进行识别和 QoS 保障。

——当移动终端通过固定网络接入并且向固定网络请求资源预留时，PEP 设备应支持按照 PDP 设备下发的策略，结合设备的资源使用情况进行资源预留。

——当移动终端通过固定网络接入时，PEP 设备应支持按照 PDP 的策略执行相应的流量调度。具体的，PEP 设备可以将移动终端的流量转接到移动核心网，或者执行本地卸载，直接接入 Internet。

10 IPv6 技术要求

固定网络策略控制系统应支持 IPv6 网络，以及支持 IPv6 分组的流量识别和分组过滤能力。固定网络策略控制系统的 IPv6 相关技术要求包括：

——固定网络策略控制系统应支持运营商部署的 IPv6 网络，以及双栈网络。具体的，固定网络策略控制系统应支持内部不同网元（如 PDP 设备和 PEP 设备）之间基于 IPv6 的策略信息交互。

——固定网络策略控制系统的 PDP 设备和 PEP 设备应支持基于 IPv6 分组头的流标示和策略下发或执行。

11 安全性和隐私技术要求

宽带接入网络通常具有识别恶意用户，保护网络不受恶意攻击的能力。固定网络策略控制系统应支持基于运营商定义的策略动态地执行这些特性。具体包括：

——对于网络上的泛洪攻击，安全入侵或者病毒感染，策略控制系统中的 PEP 设备应支持识别这些网络攻击，并且上报 PDP 设备请求策略执行，通过阻塞端口或者限速的方式进行处理。

——固定网络策略控制系统中策略分发的过程应被保护，应保证通信的对端设备可信，PDP 设备和 PEP 设备应通过授权才可以进行策略信息的交互。

——PDP 设备和 PEP 设备之间的策略请求和决定的通信消息的安全性应被保证。策略控制系统的通信消息应被保护不受到窃听或者篡改，并且可以抵御 DoS 攻击。

——为了定位错误的需要和安全性考虑，PDP 设备和 PEP 设备应支持记录所有的网络事件。

在策略控制的过程中，用户特定的信息会在网络上传输，具体包括用户的权限和正在接入的业务，用户的配置以及业务的接入时长等。这些诸如用户正在收看的电视频道，在线游戏的持续时间等信息涉及用户隐私，策略控制系统应该提供相应的隐私保护和安全机制保护这些信息。

——固定网络策略控制系统应采用安全机制保护用户隐私，具体包括 PDP 设备和 PEP 设备的安全防护机制，以及 PDP 设备和 PEP 设备之间的通信安全机制。

12 设备管理要求

12.1 配置管理

PDP 设备和 PEP 设备应支持管理员在本地或者远程登陆，通过命令行或者图形界面对设备的配置进行管理。

12.2 故障告警

PDP 设备和 PEP 设备应支持故障告警机制。告警管理系统能够实时检测和上报设备的故障或异常等告警信息，根据告警的种类和级别驱动相应的告警终端设备（如告警箱、告警台等）发出不同的声光信号，并将经过解析后的告警消息通过网管接口送往网管中心。此外，故障告警管理还具有以下功能：

——支持存储告警信息、查询告警历史记录、设置告警处理方式等功能，并且当 CPU 使用率过高时，在上报的告警信息中提供 CPU 门限数据。

——在告警操作台显示告警处理建议，方便用户迅速定位与处理设备故障。

12.3 安全管理

PDP设备和PEP设备的安全管理功能包括身份验证和访问控制：

——设备用户在系统认证过程中，用户名和密码将与授权的列表进行比较。如系统检测到项目匹配，系统将权限列表中指定范围的权限授予给用户。

——系统支持预定义的用户组，用户组内的成员将被限制访问某些信息项或限制进行某些操作。

13 其他设备要求

13.1 性能要求

PDP 设备接收感知分析功能模块、业务平台、PEP 设备等的策略请求。PEP 设备应支持 PDP 下发的策略的执行，以及将执行结果反馈给 PDP 设备。PDP 设备和 PEP 设备应满足的性能要求包括：

——每秒接收的并发请求数量不低于 1000 个；

——平均请求处理时间不超过 500ms；

——请求处理成功率不低于 99.99%。

13.2 可靠性要求

固定网络策略控制系统中的 PDP 设备和 PEP 设备应满足系统的可用性大于 99.999%。

13.3 设备接口协议要求

PDP 设备与 PEP 设备的 Ce 接口应支持 RADIUS、Diameter、COPS 等协议。

PDP 设备的 Ca 接口应支持 RADIUS、Diameter 等协议。

PDP 设备的 Cf，Cp 等接口应支持 Diameter 等协议。

13.4 设备环境要求

PEP设备部署在固定网络的已有网元中，遵守所属网元的设备环境要求。PDP设备如果独立部署，应满足如下设备环境要求。

13.4.1 温度、湿度条件

长期工作条件：温度保持15℃～30℃，相对湿度保持40%～60%。

短期工作条件：温度保持0℃～45℃，相对湿度保持20%～90%。

13.4.2 防尘要求

直径大于5μm的灰尘浓度≤3×10^4 粒/m^3；灰尘粒子是非导电、导磁和腐蚀性的。

13.4.3 电磁兼容性

设备的电磁兼容性应符合GB 9254。

参 考 文 献

[1] 2012-1365T-YD 智能型通信网络 总体框架和要求

[2] 2012-YDB-20 智能型通信网络 策略管控能力开放需求

[3] 2012-YDB-21 智能型通信网络 策略管控能力开放架构与技术要求

[4] ITU-T Y.2111(2006) 下一代网络的资源和接入控制系统（Resource and admission control functions in next generation networks (RACF)）

[5] IETF RFC 2475(1998) 区分服务架构（An Architecture for Differentiated Service）

[6] IETF RFC 3084(2001) 用于策略提供的COPS（COPS Usage for Policy Provisioning (COPS-PR)）

[7] IETF RFC 5176(2008) RADIUS的动态授权扩展（Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)）

[8] ETSI 282 003(2009) 电信和互联网融合业务及高级网络协议 资源与接入控制子系统 基础架构（Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture）

[9] 3GPP TS 23.139 3GPP系统 固定宽带接入网络互通 步骤2（3GPP System-Fixed Broadband Access Network Interworking; Stage 2）

[10] 3GPP TS 23.203 策略与计费控制架构（Policy and Charging Control Architecture）

[11] 3GPP TR 23.839 支持BBF接入网络互通研究（Study on Support of BBF Access Interworking）

[12] BBF TR-101(2006) 向基于以太网的DSL聚合迁移（Migration to Ethernet-Based DSL Aggregation）

[13] BBF TR-144(2007) 宽带多服务架构和框架需求（Broadband Multi-Service Architecture & Framework Requirements）

[14] BBF TR-203(2012) 下一代固定和3GPP无线网络互通（Interworking between Next Generation Fixed and 3GPP Wireless Networks）

中华人民共和国
通信行业标准

智能型通信网络
固定网络策略控制设备和策略执行设备技术要求

YD/T 2820—2015

*

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
北京康利胶印厂印刷

*

开本：880 × 1230　1/16　　2015 年 12 月第 1 版
印张：1.5　　2015 年 12 月北京第 1 次印刷
字数：36 千字

15115 • 686
定价：15 元