ICS 33.040
M 32

YD

中华人民共和国通信行业标准

YD/T 2817-2015

宽带网络接入服务器（BNAS）设备流量分析控制技术要求

Technical specification for flow awareness and service controlling of broadband network access server（BNAS）

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

本标准按照 GB/T1.1-2009 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、中国联合网络通信集团有限公司、中兴通讯股份有限公司。

本标准主要起草人：陈华南、袁　博、范　亮、朱　鹏、贾聿庸、朱永庆。

宽带网络接入服务器（BNAS）设备流量分析控制技术要求

1 范围

本标准规定了在城域网中智能管道的部署对宽带网络接入服务器（BNAS）设备的要求。

本标准适用于需要部署智能管道技术的 BNAS 设备。

2 规范性引用文件

下列文件对于本文件的应用时必不可少的，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 1365-2012 智能型通信网络 总体框架和要求

YD/T 1899 深度包检测设备技术要求

YD/T 2271 深度包监测（DPI）设备联动需求与体系架构

3 术语、定义和缩略语

3.1 术语和定义

下列术语定义适用于本文件。

3.1.1

网络接入服务器 Network Access Server

一种远程访问接入设备，它位于公共电话网与 IP 网之间，将拨号用户接入 IP 网，它可以完成远程接入、实现拨号虚拟专网（VPDN）、构建企业内部 Internet 等应用。

3.1.2

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

一种面向宽带网络应用的新型接入网关，它位于骨干网的边缘层。其可以完成用户宽带的 IP/ATM 网的数据接入、实现 VPN 服务、构建企业内部 Intranet、支持 ISP 向用户批发业务等应用。

3.2 缩略语

下列缩略词适用于本文件。

AAA	Authentication Authorization and Accounting	认证授权计费
AC	Access Circuit	接入链路
ACL	Access Control List	接入控制列表
AFTR	Address Family Translation Router	地址族翻译路由
ANCP	Access Node Control Protocol	接入点控制协议
ARP	Address Resolution Protocol	地址解析协议
BNAS	Broadband Network Access Server	宽带网络接入服务器
CGN	Carrier Grade NAT	运营级网络地址翻译
CoA	Change of Attribute	属性变更

DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DPI	Deep packet Inspection	深度报文解析
H-Qos	Hierachical Quality of Service	层次化服务质量
IDC	Internet Data Center	互联网数据中心
IGMP	Internet Group Management Protocol	因特网组管理协议
L2CM	Layer 2 Control Mechanism	二层控制机制
L2TP	Layer 2 Tunneling Protocol	二层隧道协议
LAC	L2TP Access Concentrator	访问接入控制器
IMS	IP multimedia subsystem	IP 多媒体子系统
LNS	L2TP Network Server	L2TP 网络服务器
IPTV	Internet Protocol Television	互联网电视
LSP	Label Switching Path	标签交换路径
NAT	Network Address Translation	网络地址翻译
Qos	Quality Of Service	服务质量
PW	Pseudo Wire	伪线
RG	Residential Gateway	家庭网关
Session ID	Session Identifier	会话标识
VLAN	Virtual Local Area Network	虚拟局域网
VRF	Virtual Routing Forwarding	虚拟路由转发
VPN	Virtual Private Network	虚拟专用网
VSI	Virtual Switch Instance	虚拟交换实例

4 智能型网络的发展需求

见 YD T1365-2012 第 4 章。

5 BNAS 智能业务感知和控制技术

5.1 概述

BNAS 设备在智能型通信网络中利用和智能通信网络能力开放平台之间的策略服务器为信令中转设备，为运营商网络提供用户流量分析、业务感知和动态控制的功能，为不同类型的用户和业务类型提供差异化服务，实现对 BNAS 网络资源的高效利用。

BNAS 通过网络流量的智能虚拟管道划分和映射来实现业务感知和控制，智能管道在 BNAS 设备上表现为对一组具有相同特征的流量的逻辑映射，BNAS 设备为管道流量提供静态或动态的 QOS 保障，同时可以提供不同类型的增值服务，即在业务感知的基础上实现业务控制。而业务的动态感知和管道的动态划分策略的动态控制，正是 BNAS 设备“智能的体现”。

5.2 BNAS 设备支持智能通信网络的功能架构

BNAS 通过智能管道划分和映射来实现业务感知和控制，因此相对无法支持智能通信的哑网络，BNAS 可以为宽带网络的用户提供更智能的基于流量分析控制技术的差分服务。在智能通信网络中 BNAS 必须和策略服务器适配。

BNAS 设备的功能架构如图 1 所示。它主要包括如下几类功能：

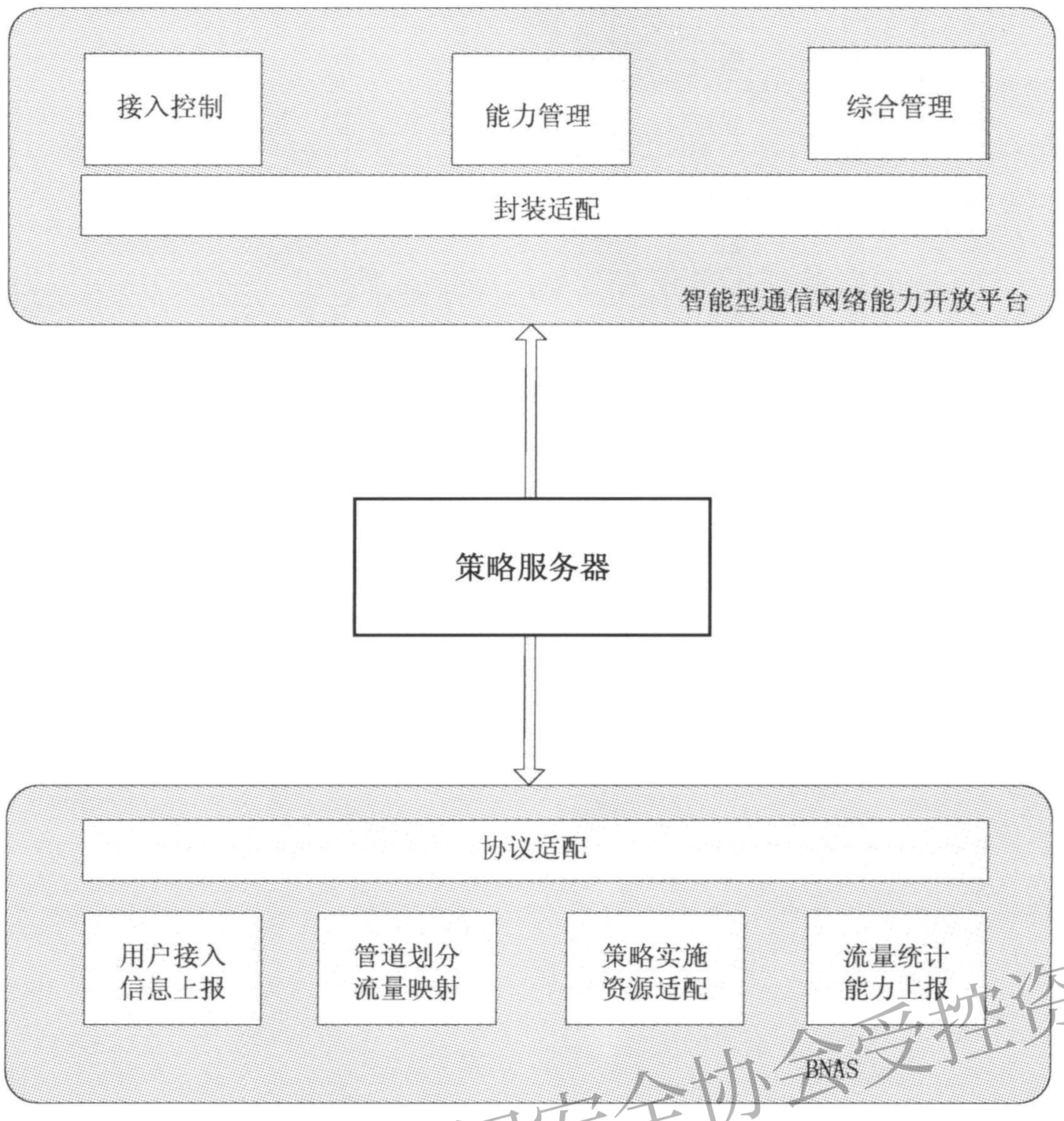

图 1　BNAS 支持智能通信通信网络功能架构

a）　与策略服务器适配功能。

－　开放接口功能:BNAS 支持多种策略下发相关的接口协议，BNAS 必须支持 Radius COA、可选支持 Diameter、SNMP 及 Openflow 等接口。

－　协议适配功能:BNAS 适配不同的策略接口协议，并解析为相同或者不同的流量策略，最终映射到用户流量。

b）　用户接入和信息上报功能。

－　用户接入功能：BNAS 支持传统的 PPPoE、IPoE、L2TP、IP 专线等 IPv4/IPv6 用户接入智能通信网络，同时 BNAS 支持将 L2VP/ L3VPN 的隧道流量映射为 BNAS 的逻辑用户接入智能通信网络。

－　用户信息上报:BNAS 并支持将标识不同用户的信息上报给策略服务器，策略服务器保存并作为策略下发对象的标识。

c）　管道映射和流量划分功能。

－　管道映射功能:BNAS 支持根据本地或者智能通信网络开放平台下发的控制策略，根据不同的用户和应用类型，实现动态的管道划分。

－　策略实施和资源分配：BNAS 根据本地或者智能通信网络开放平台下发的控制策略，对设备的资源进行再分配

d）　流量统计和能力上报功能。

－ BNAS 统计不同用户的流量并依据要求上报到智能通信网络开放平台，同时 BNAS 也支持将自身的能力和资源状态上报智能通信网络开放平台。

5.3 智能通信网络控制资源定义

BNAS 设备的智能业务感知和控制，最终目的是对 BNAS 设备的资源进行合理的调度分配。对于 BNAS 设备而言，在智能通信网络中可以被动态监控和控制的资源，不仅仅是传统意义上 QOS 资源，设备上任何可以提现差异化服务的资源都可以作为智能网络中策略管理和控制分配的资源，为运营商实现差异化的业务运营提供条件。BNAS 的智能控制资源包括但不限于以下几种（根据各运营商的实际需求的差异性，不强制要求支持全部资源的智能控制）：

a） BNAS 设备转发面资源，包括：

1）端口带宽资源；

2）BNAS 设备线卡的 QOS 队列、缓存资源；

3）BNAS 设备交换队列调度资源；

4）BNAS 支持 NAT/SBC/DPI/Firewall 等业务时可控制和修改的资源；

5）视频 Cache 资源；

6）隧道控制资源。

b） BNAS 设备控制面资源，包括：

1）宽带用户管理相关资源；

2）路由表/VPN 路由表容量；

3）隧道会话容量；

4）L2 Switch/L2 VPN MAC 表容量；

5）网络协议消息通道带宽/数量/速率。

BNAS 设备对网络流量的智能化处理，实际上就是在业务感知的基础上、为不同类型的业务分配不同的设备资源，以达到提供差异化服务的目的。

5.4 BNAS 智能管道适配和策略执行基本流程

BNAS 通过和策略服务器的北向接口，执行智能网络管开放平台下发的智能管道映射策略，这个过程的基本流程如图 2 所示。

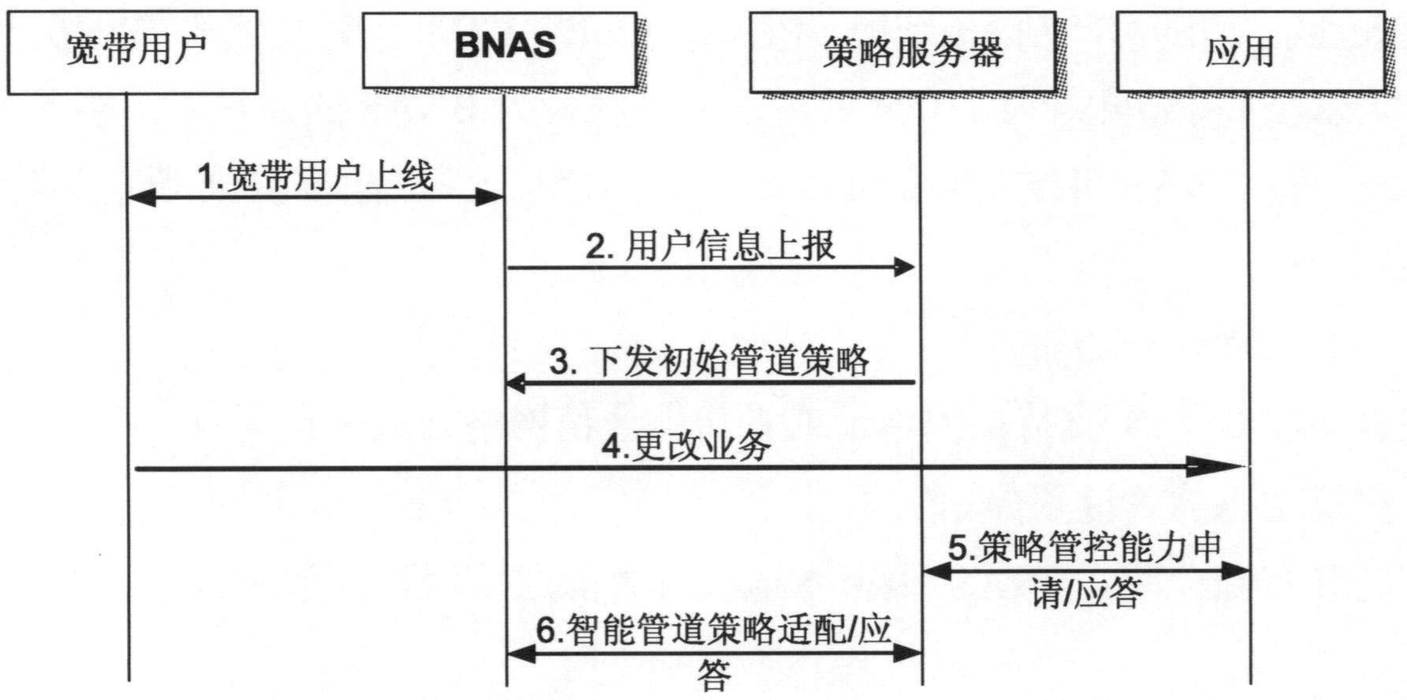

图 2 管道映射和策略下发

图 2 中流程说明如下：

1） 宽带用户上线，在 BNAS 设备上认证通过；

2） BNAS 设备向策略服务器上报用户的关键信息，策略服务器依据这个关键信息识别宽带用户；

3） 策略服务器向 BNAS 设备下发初始智能管道适配映射策略，BNAS 将不同的网路流量映射成虚拟管道，并执行相应的资源分配策略；

4） 用户通过网络应用（例如 Portal）更改所需的业务策略；

5） 网络应用通知策略服务器进行策略管控能力申请；

6） 策略服务器向 BNAS 设备更新智能管道适配策略，BNAS 根据适配策略中的映射规则将不同的业务流量映射成虚拟管道，并执行相应的资源分配策略。

6 网络流量划分

6.1 基于业务的层次划分

运营商网络的网络流量如图 3 所示，可以划分为几个不同的层次。

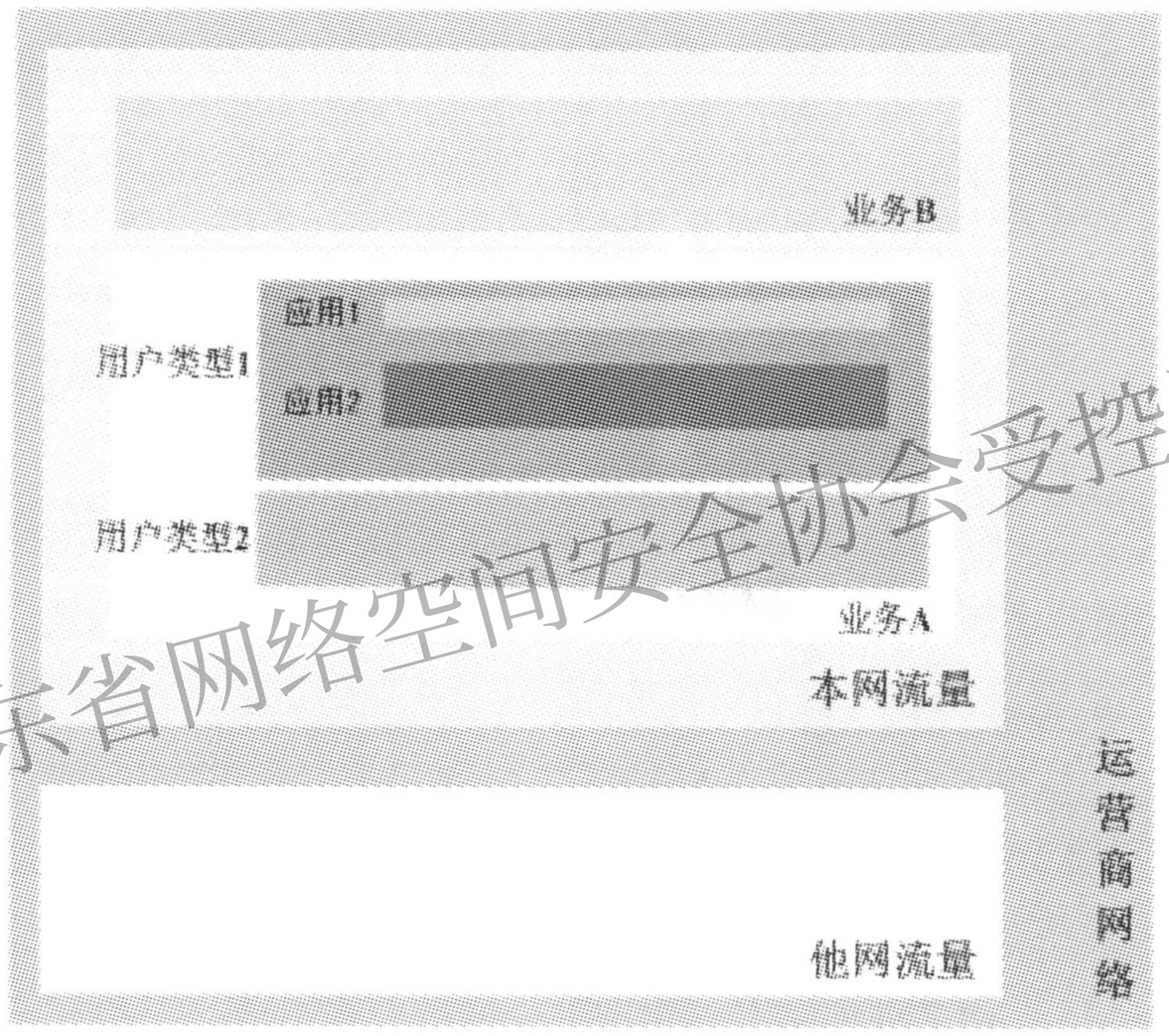

图 3 运营商网络流量的划分

在智能通信网络中，BNAS 设备首先必须支持对不同类型网络流量的感知，并在此基础上将网络流量划分入不同类型的管道，划分的原则如下：

— BNAS 必须支持根据本运营商的网络流量和其他运营商的网络流量来划分管道，依据可以是接入的物理信息或者用户的 domain 信息。

— 在本运营商的网络流量内部，BNAS 支持根据不同的业务类型和用户类型进行网络流量的管道划分，例如 IPTV 业务、VOIP 业务和 HSI 业务或者 SR 专线业务。

— 对于同一类型业务的网络流量，BNAS 根据用户类型的不同还可以做进一步的管道划分，例如将 PPPoE 用户区分为金牌用户和银牌用户。

— 对于同一类型用户的网络流量，根据应用类型的不同还可以做进一步的区分，例如根据网站地址及对应的 IP 优先级来划分虚拟管道。

当根据业务和用户类型划分管道的时，BNAS 支持把多种类型的用户虚拟成一个逻辑的用户处理。例如，把 PPPoE 和 IPTV 用户虚拟成一个家庭用户，此时 BNAS 对这个逻辑用户进行智能管道流量的映射和策略的实施。

如图 4 所示，在运营商网络中同时存在多种不同类型的用户和应用。在这种层次化的业务感知和智能策略映射系统中，运营商可以根据自身的需求，灵活的选择网络流量的划分方式，同时也可以进行灵活的组合，例如可以将同一用户的几种应用组合成一个新的业务类型。

图 4　运营商网络中的多种类型的用户和应用

6.2　基于 TCP/IP 的层次划分逻辑管道

根据 TCP/IP 的层次化模型，BNAS 设备可以支持根据 TCP/IP 层次划模型对管道进行逻辑划分，这种逻辑划分一般可以通过 ACL 技术实现，或者获取流量在 BNAS 上本身的物理和逻辑信息识别。图 5 所示是一个基于 TCP/IP 协议栈的网络流量划分模型，包括五种划分方式。

a）　TCP/IP 物理层：

根据接收流量的物理接口或者逻辑接口的不同划分不同的网络流量；

b）　TCP/IP 数据链路层：

BNAS 设备根据 MAC 地址来划分不同的管道网络流量；

BNAS 设备也可以通过 VLAN 信息划分不同的管道；

BNAS 设备也可以通过 VLAN 的 802.1p 信息划分不同的管道流量。

c）　TCP/IP 网络层：

BNAS 支持根据 IP 地址匹配划分不同的管道流量；

BNAS 支持根据 IPv4/IPv6 网络协议的不同来划分不同的管道流量；

BNAS 支持根据 TOS/DSCP/TC 字段划分不同的管道流量；

BNAS 支持根据 L2VPN 和 L3VPN 的 VPN 信息划分不同的管道流量、例如 GRE。

d）　TCP/IP 传输层：

BNAS 支持根据不同的协议类型和源/目的端口来划分不同的网络流量。

e）　5、TCP/IP 应用层：

BNAS 支持根据应用协议的应用层字段来识别不同的管道流量，例如利用 DPI 深度报文分析技术，识别出某一应用的网络流量后，将其 5 元组信息在设备上转换成 ACL 规则、实现对该应用的网络流量识别。BNAS 设备支持内置 DPI 功能，或与外置 DPI 设备联动，外置 DPI 设备的要求见 YD/T 2271 和 YD/T 1899。

此外，对于 IPinIP 隧道流量，例如 DS_Lite 用户流量，BNAS 需要获取内层封装的真实 TCP/IP 信息，再进行管道策略控制。

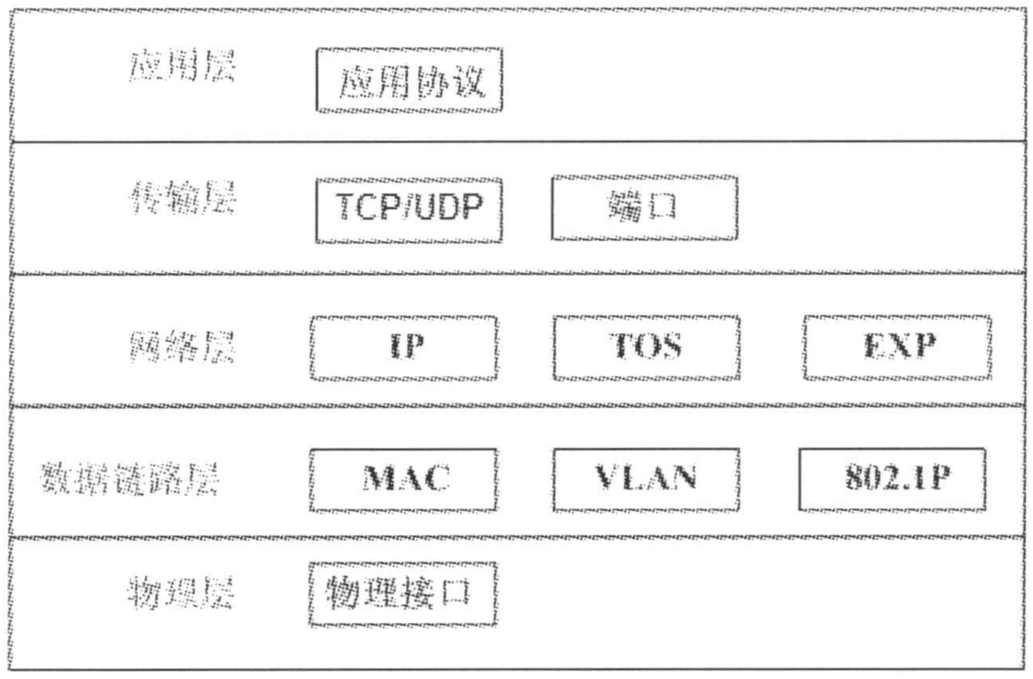

图 5　基于 TCP/IP 协议栈的网络流量划分模型

6.3　各种类型隧道流量的层次划分

6.3.1　MPLS 隧道流量

MPLS 隧道和伪线是一种把网络流量重封装的技术，不同的隧道可以对应不同的业务类型或用户类型，本身就是一种管道，如图 6 所示。当智能管道技术应用于隧道内的网络流量时，隧道内的网络流量划分规则应该只作用于该 VPN 内，因此策略服务器应该位于 VPN 内部，当管道策略服务器位于 VPN 之外时，管道策略的下发必须带上 VPN 的信息，可以通过在管道策略服务器上绑定 IP 或者接口和 VPN 的关系来实现。

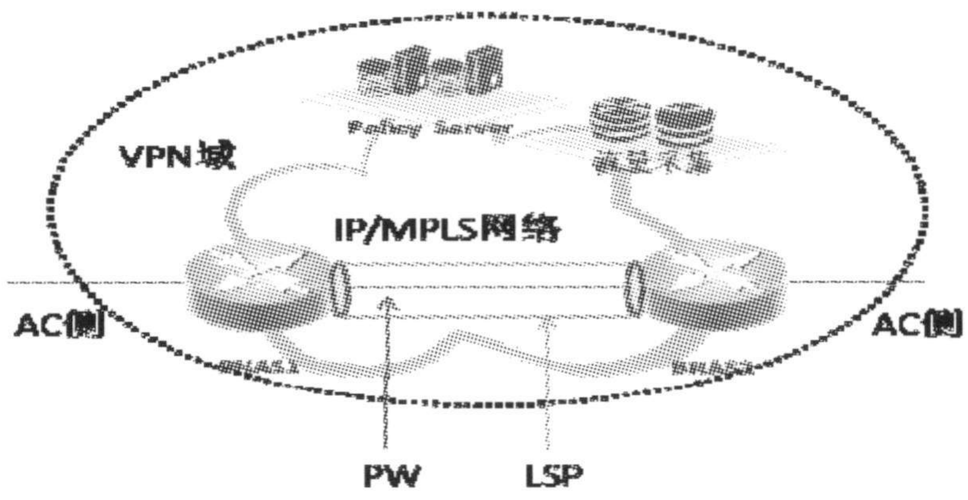

图 6　MPLS LSP/PW 承载模型

对于隧道/伪线的 AC 侧网络流量的感知，必须在上行流量入隧道封装前和下行流量出隧道解封装后进行，采用业务层次化或 TCP/IP 的层次化感知方法，与非隧道承载的网络流量采用相同的处理方法。

对于隧道和伪线内的网络流量，BNAS 设备不再处理封装的净荷，层次划分如图 7 所示。

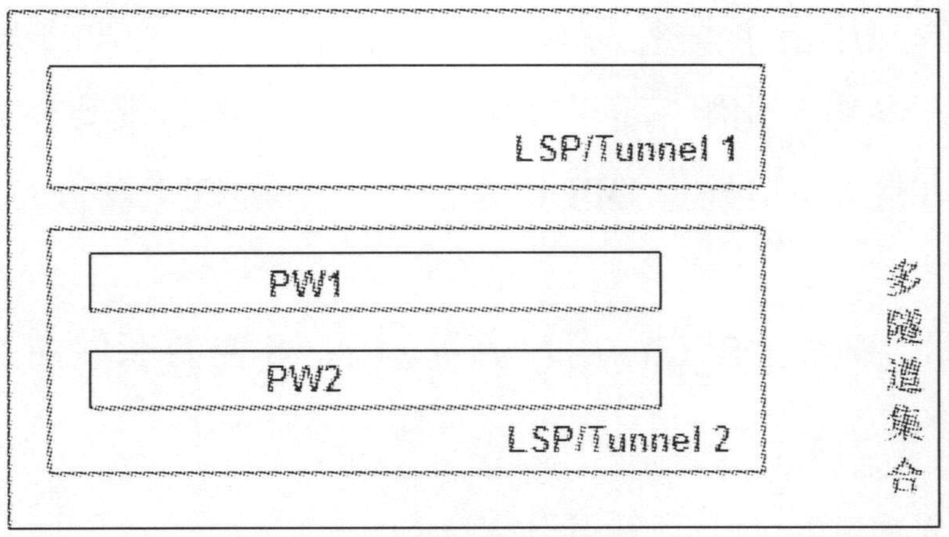

图 7　MPLS 隧道流量的层次划分模型

在运营商的智能通信网络的实际部署中，可以采用 6.1 节和 6.2 节的各种方法的任意组合。

6.3.2　L2TP 隧道流量

L2TP 技术是一种 PPP 用户接入的网络侧延伸技术，通常用于企业网的用户远程接入，或运营商间的接入线路和网络租用，用户通过 PPP 方式接入本地运营商的 BNAS/LAC 设备，并通过本地运营商的 BNAS/LAC 设备和线路租用运营商或企业的 BNAS/LNS 设备间建立的 L2TP 隧道访问 BNAS/LNS 设备的网络侧业务。同时，在 L2TP 隧道内为每个 PPP 接入建立一个 L2TP 会话。L2TP 网络模型如图 8 所示。

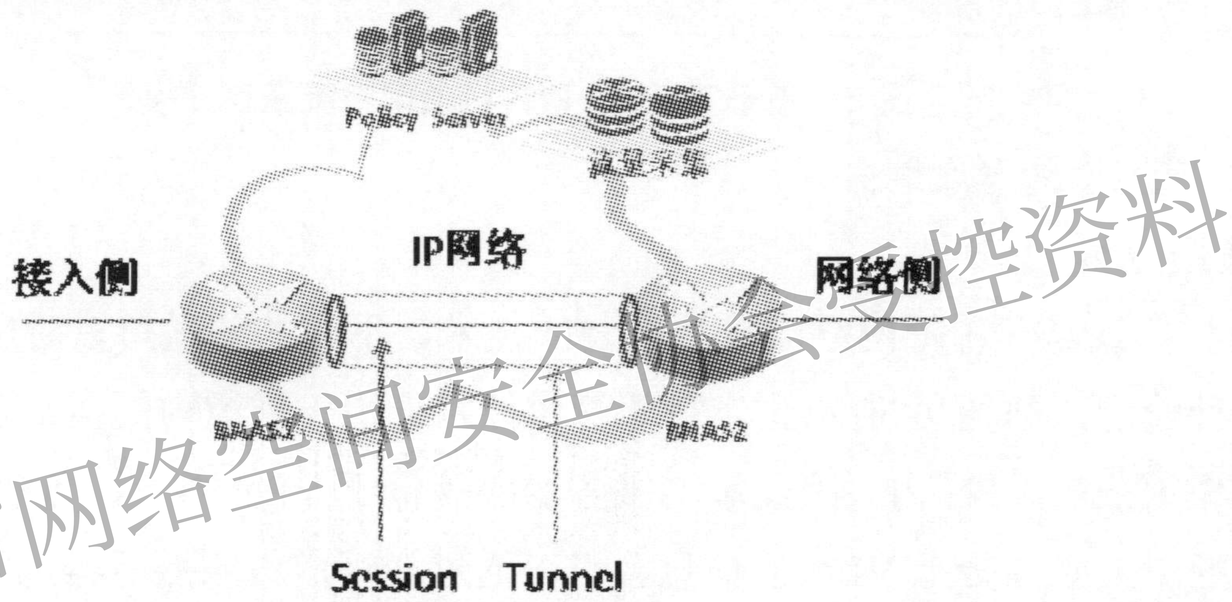

图 8　L2TP 网络模型

对应本地运营商 BNAS/LAC 设备的用户接入侧网络流量及线路租用运营商或企业 BNAS/LNS 设备的网络侧网络流量的感知，采用业务层次化或 TCP/IP 的层次化感知方法，与非隧道承载的网络流量采用相同的处理方法。

对于隧道和会话内的网络流量，BNAS 设备不再处理封装的净荷，层次划分如图 9 所示。

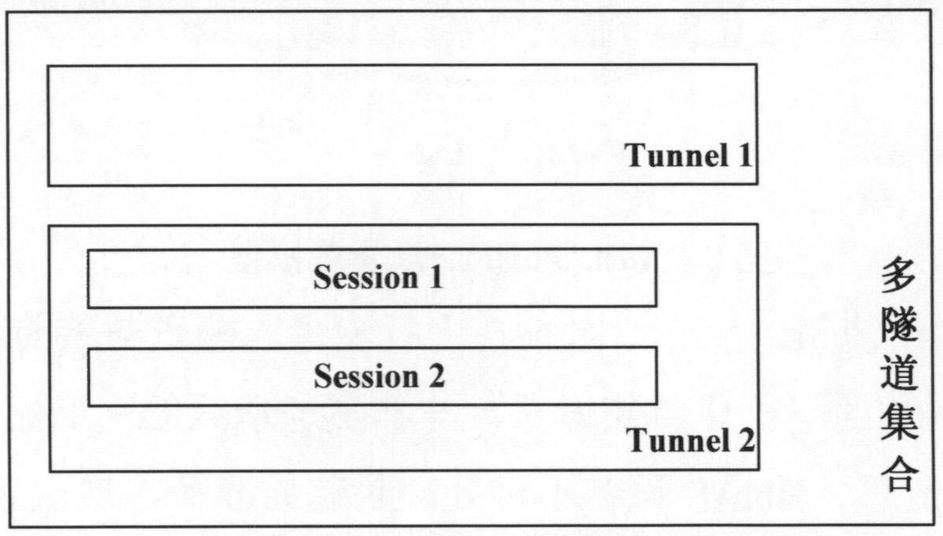

图 9　L2TP 隧道流量的层次划分模型

7 用户的识别

7.1 BNAS 上报用户和 BNAS 信息

在宽带用户接入 BNAS 时，通常情况下，BNAS 需要将 BNAS 地址信息、用户网络信息和用户 BNAS 标识上报给策略服务器（流程如图 10 所示）：

a) 在下发管道策略时策略服务器依据 BNAS 地址信息用来找到 BNAS 位置；

b) 当用户访问网络应用时，“用户的网络信息”用于标识网络中的唯一的用户，应用服务进行策略管控能力申请时把用户网络信息带给策略服务器，策略服务器，依据这个网络信息获取用户标识信息；

c) 而策略服务器在下发管道适配策略时，会携带用户在 BNAS 上的标识信息，BNAS 根据这个标识将管道策略映射到 BNAS 生效。

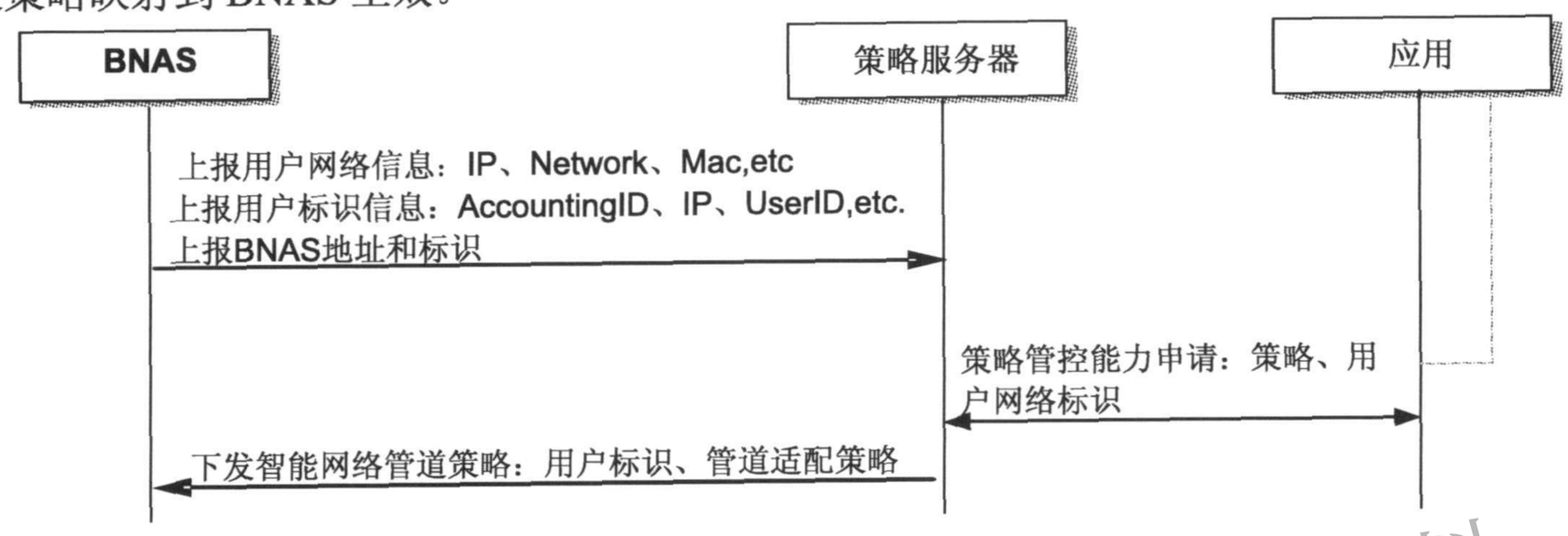

图 10 用户信息上报和策略下发、策略执行

BNAS 上报的用户的网络信息可以但不限于包含：

a） IP 地址信息或者 IP 网段信息；

b） NAT 和 DS_Lite 转换后的公网 IP 地址和公网端口范围信息；

c） L2 网络中的二层用户信息，例如 MAC 地址等；

d） 用户的 VPN 信息。

BNAS 用户标识信息可以但不限于包含：

a） 计费用户的计费 ID 信息；

b） IP 地址信息或者 IP 网段信息；

c） L2 网络中的二层用户信息，例如 MAC 地址等；

d） 用户的二三层 VPN 信息，配合用户的网络信息标识 BNAS 的 VPN 用户，包括 VPN 实例名/隧道 ID 等；

e） 用户流量在 BNAS 上的物理位置信息，如接口、子接口、逻辑接口或者 PPPoE 和 IPoE 用户的 LinID 等；

f） 用户在 BNAS 上生成的唯一标识，例如 BNAS 为用户生成的用户 ID。

BNAS 上报的用户网络信息和用户标识信息，其中的一些是现有策略下发协议（如 Radius、Diameter、COPS 等）已支持的属性，有些需要扩展这些策略下发协议的公有属性，或者利用设备商的私有属性实现。

7.2 手动绑定 BNAS 和策略下发对象

对于三层 VPN 和二层 VPN 业务，可以在策略服务器上手工配置下发用户标识和策略信息,在手动配置的情况下，用户的网络标识就是用户标识，BNAS 根据用户网络标识可以获取管道策略生效的接口。

如图 11 所示，针对普通 L3VPN 生效时（非拨号用户），需要在策略服务器上手工配置 VPN 信息和转发表信息，用户无需上报用户标识。此时用户的私网 IP 同时作为用户的网络信息和 BNAS 上的用户标识。当 BNAS 收到策略服务器下发的管道策略时，通过 VPN 和私网 IP 信息反查管道策略作用接口，从而让管道策略生效。同样地，对于 L2VPN 业务，可使用 MAC 地址来反查管道策略作用接口。

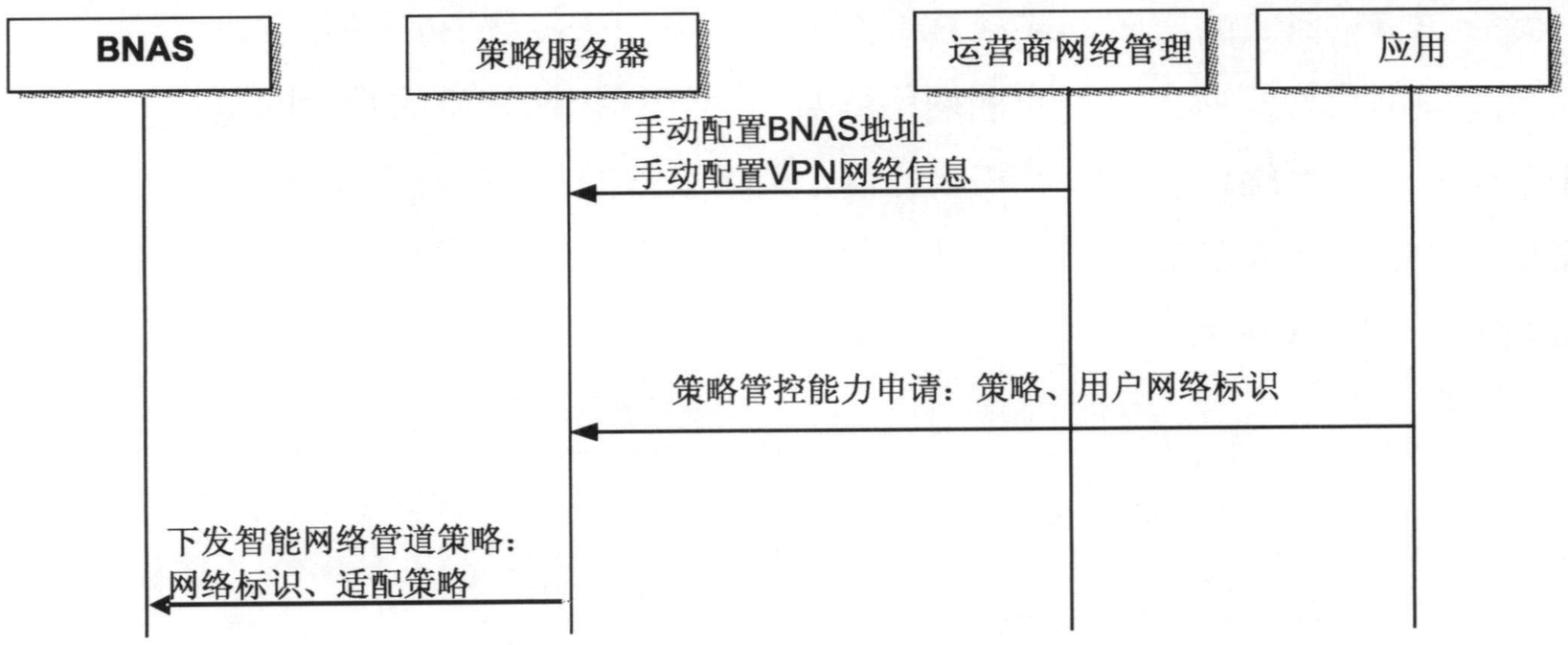

图 11　L3VPN 手动绑定和策略下发

8　业务感知和映射

8.1　业务感知手段

根据智能通信网络中对 BNAS 设备业务感知控制技术要求，BNAS 设备通过管道适配策略将流经 BNAS 的流量映射成不同的虚拟管道，来实现对业务、用户和应用的感知。如感知用户的行为特征、位置信息、忙闲状态、各业务流量占比、甚至应用类型和是否正在进行网络攻击等等。

当 BNAS 设备根据管道适配策略中的流量映射规则识别出不同类型的网络流量后，BNAS 设备可以把对网络流量的处理和层次化 QOS 及其它策略相结合，根据管道层次的不同，采取不同的策略动作。因此，BNAS 设备如果需要根据用户或运营商的需求执行管道适配策略，首先需要根据管道适配策略生成虚拟管道。

8.2　静态映射

静态映射是指设备通过静态配置管道适配策略直接在设备上映射出虚拟的管道，如图 12 所示，BNAS 设备把管道适配策略分为 2 部分。

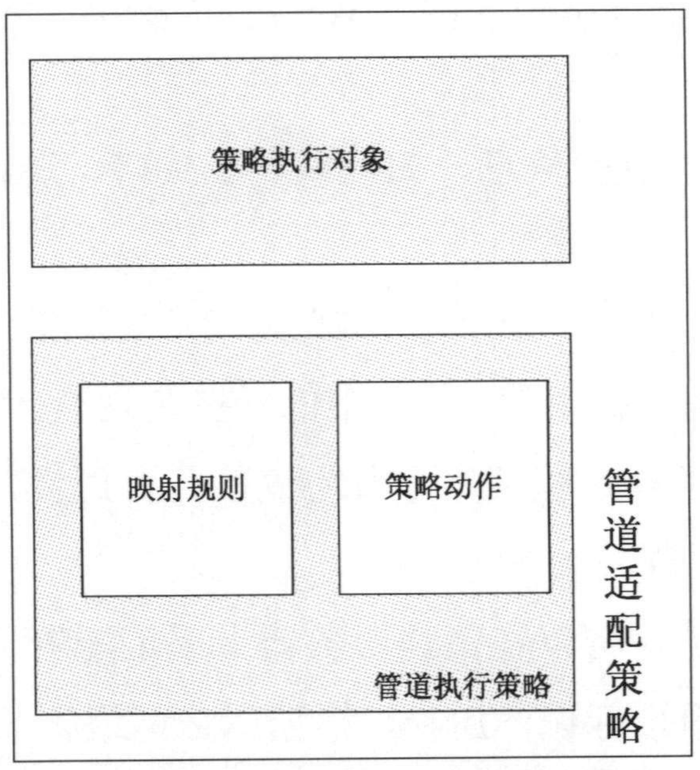

图 12　管道适配策略适配策略的组成

— 策略执行对象：标识一个层次化管道适配规则的执行实体，就是前面描述的用户标识；

— 管道执行策略：标识设备对策略执行对象需要的执行动作，一般作为一个“策略实体”配置在设备上，包含映射规则和策略动作两部分。

管道执行策略的映射规则，即网络流量的区分和识别方法，见第 6 章。

管道执行策略的策略动作，即网络流量的控制方法，见第 9 章。

静态配置的管道适配策略，策略的执行对象可以是物理接口或者虚接口、认证用户的 domain、隧道和伪线、隧道和会话等。

静态管道的适配过程是这样的：

a） 通过命令行或网络管理系统在网络设备上配置管道适配策略；

b） 把管道映射策略和策略执行对象在 BNAS 设备上绑定；

c） 网络设备生成虚拟的层次化管道；

d） 流量经过 BNAS 设备时，根据管道映射策略的映射规则，匹配不同的策略动作。

8.3 动态映射

8.3.1 动态映射规则的组成和匹配

动态映射是指在 IP 设备转发流量的过程中，通过策略服务器，动态的给 BNAS 设备下发管道适配策略，一般可以通过 Radius COA、Diameter 协议或 COPS 等协议进行下发，动态管道适配策略和静态配置的管道适配策略的构成相同。

当 BNAS 设备收到信任的策略服务器发送的管道适配策略后，BNAS 设备的处理过程应该是这样的：

— 根据策略服务器下发的管道适配策略中的用户标识找到策略执行对象；

— 根据在所述的策略执行对象和映射规则中的匹配条件，生成虚拟管道；

— 对虚拟管道执行策略动作。

对于管道映射规则，在动态映射时根据 IP 优先级和不同 TCP/IP 层次的 ACL 匹配是最常见的方法。如图 13 所示，策略服务器可以下发 BNAS 设备上已存在的某个管道执行策略的名称，此时管道执行策略的具体内容配置已储存在 BNAS 设备上，BNAS 根据管道映射策略名从 BNAS 的配置中获取实际的策略内容，再执行相应的管道策略。

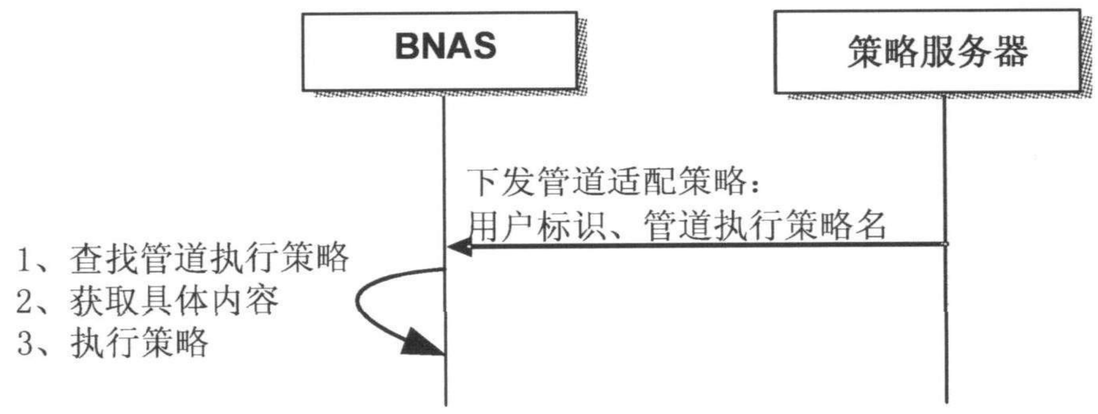

图 13 下发策略名来进行智能管道适配

此外，如果 BNAS 设备支持更开放的策略配置接口，策略服务器可以下发管道执行策略的内容给 BNAS，BNAS 先依据管道映射策略内容生成实际的管道执行策略，再根据用户标识找到对应的用户并执行相应的管道策略，如如 14 所示。

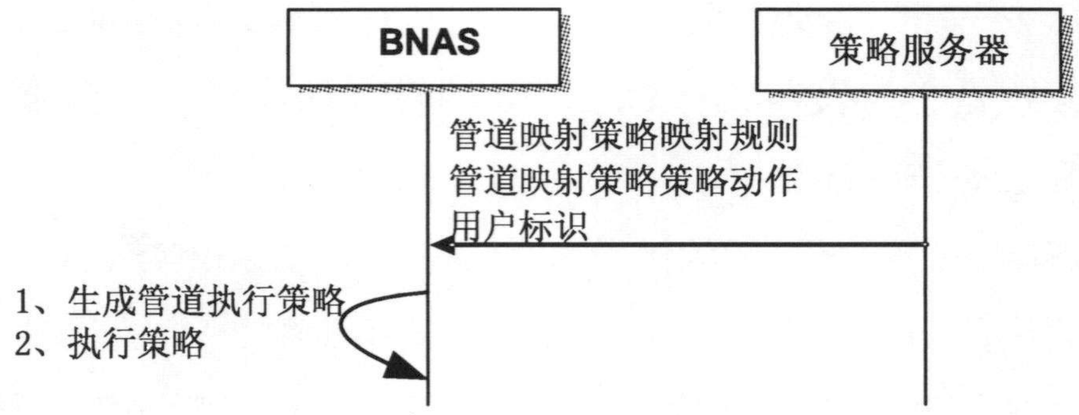

图 14　下发策略内容来进行智能管道适配

8.3.2　动态映射规则触发条件

动态的管道适配策略从策略服务器下发，下发的规则需要通过外部因素触发，对于 BNAS 设备来说，触发条件至少包含 3 种：

a）　用户主动触发管道适配策略下发；

b）　设备触发管道适配策略下发；

c）　运营商网络管理实体触发适配策略下发。

8.3.3　用户主动调整映射规则

在用户触发管道适配策略更改的过程中，运营商可以通过在第三方网站和应用中嵌入运营商信息来提示用户定制和更改运营商的智能管道策略，用户也可以通过访问策略服务器关联的 Web 页面来进行管道适配策略的更改，过程如下：

a）　用户访问第三方应用或者策略服务器提供的 Web 页面；

b）　用户根据自己感兴趣的内容（用户、业务和应用的组合规则）来更改管道适配策略；

c）　策略服务器将管道适配策略下发到 BNAS 设备；

d）　BNAS 设备为该用户流量生成虚拟管道，并适配策略。

BNAS 设备也需要支持基于内容的动态推送 Portal 页面的服务，通过与用户特征流量分析设备、Portal 服务器及策略服务器的相互配合来实现。其中，用户特征流量分析设备可以是 BNAS 设备上的业务分析线卡或模块，也可以是外置的 DPI 设备。服务提供步骤如图 16 所示，包括：

a）　在用户特征流量分析设备上设置用户感兴趣的流量类型；

b）　用户特征流量分析设备上捕获这些流量，用户特征流量分析设备根据捕获的流量，分析用户的行为；

c）　当某用户感兴趣的流量达到某一阀值，用户特征流量分析设备通知策略服务器给用户下发重定向 Portal；

d）　策略服务器通知 BNAS 设备通过重定向的方式向用户推送 Portal 页面，告知用户流量分析结果，用户可以通过订购管道策略提升服务质量；

e）　用户在 Portal 页面上订购特征流量的管道适配策略，Portal 服务器和运营商的后台策略服务器交互，后台策略服务器据此生成管道适配策略，并下发到 BNAS 设备；

f）　BNAS 设备在针对特定的用户流量上生成虚拟管道，并进行流量和规则的匹配。

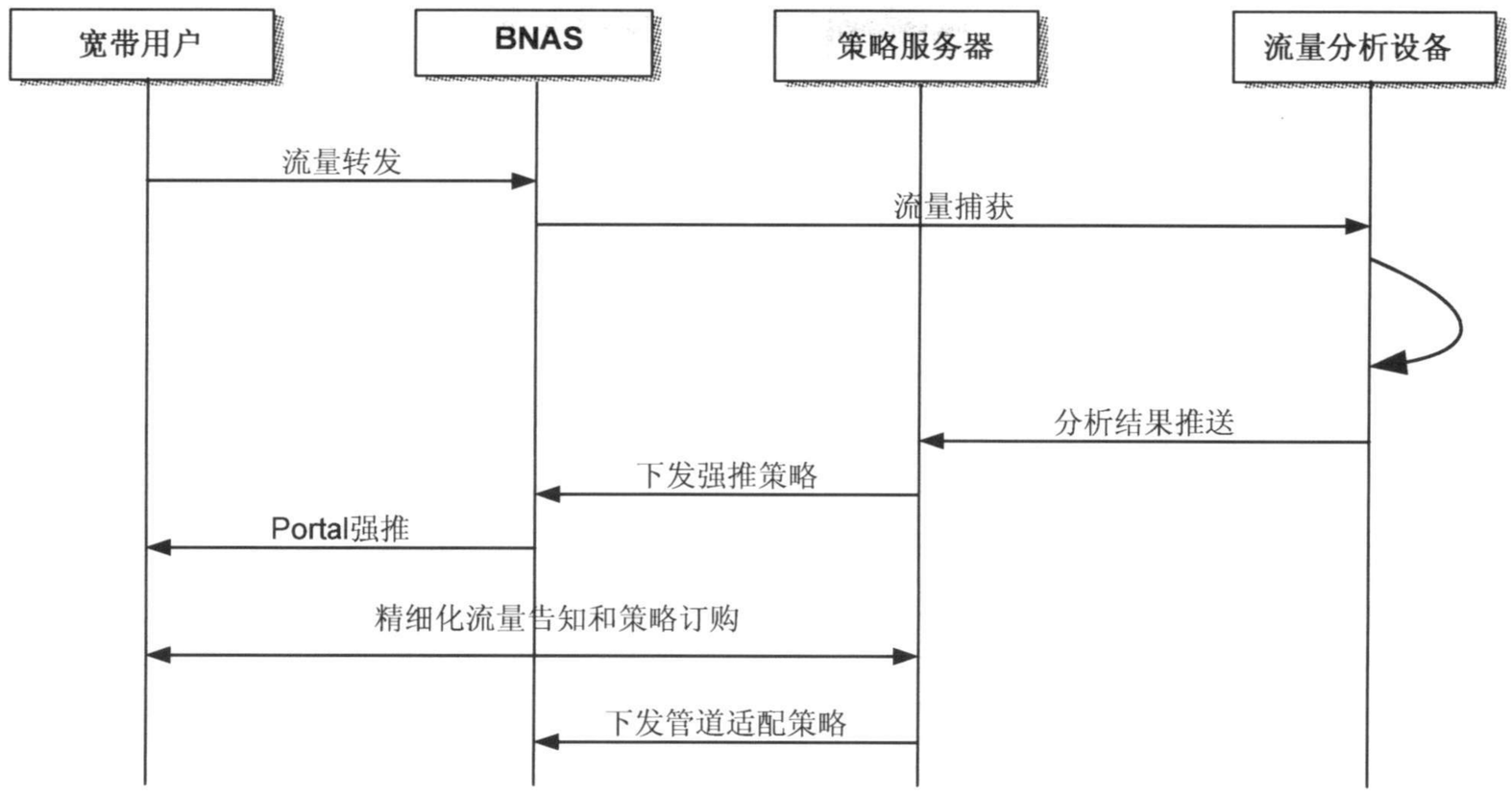

图 16　动态推送 Portal 页面

8.3.4　设备触发规则下发

为了实现端到端的智能型通信网络的管道流量策略管控，BNAS 在业务感知和规则映射的基础上，可以支持进一步实现设备间的动态规则调整，通过设备间的消息通道或策略服务器实现。如图 17 所示，路由器 1 在管道资源超负荷后，可要求 BNAS 对管道资源做同步调整。

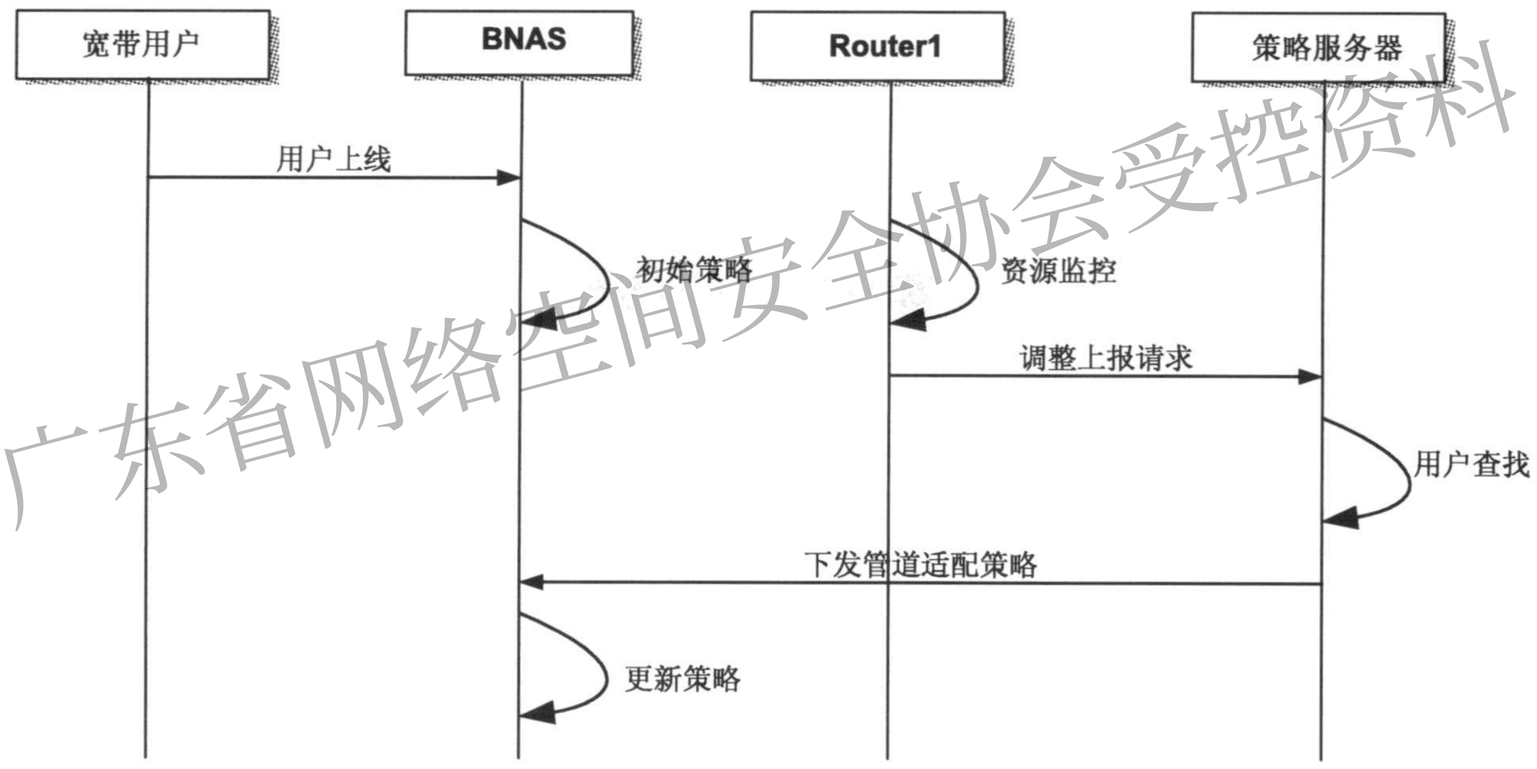

图 17　端到端管道资源调整

图 17 的流程说明如下：

a）　BNAS 和路由器 1 配置初始映射规则和虚拟管道；

b）　路由器 1 监控自身设备资源

c）　路由器 1 判断管道资源超负荷，BNAS 用户的管道资源需要调整；

d）　路由器 1 将资源调整要求上报策略服务器；

e）　路由器 1 通过策略服务器给 BNAS 动态下发管道适配策略，动态更改 BNAS 的管道策略。路由器 1 也可以通过信令协议直接请求 BNAS 更改管道适配策略。

这种设备触发规则的下发可以广泛应用于隧道技术或者和 BNAS 用户强相关技术，如 CGN 或者 DPI 技术，BNAS 设备和 CGN/DPI 网关联动的模式如图 18 所示。

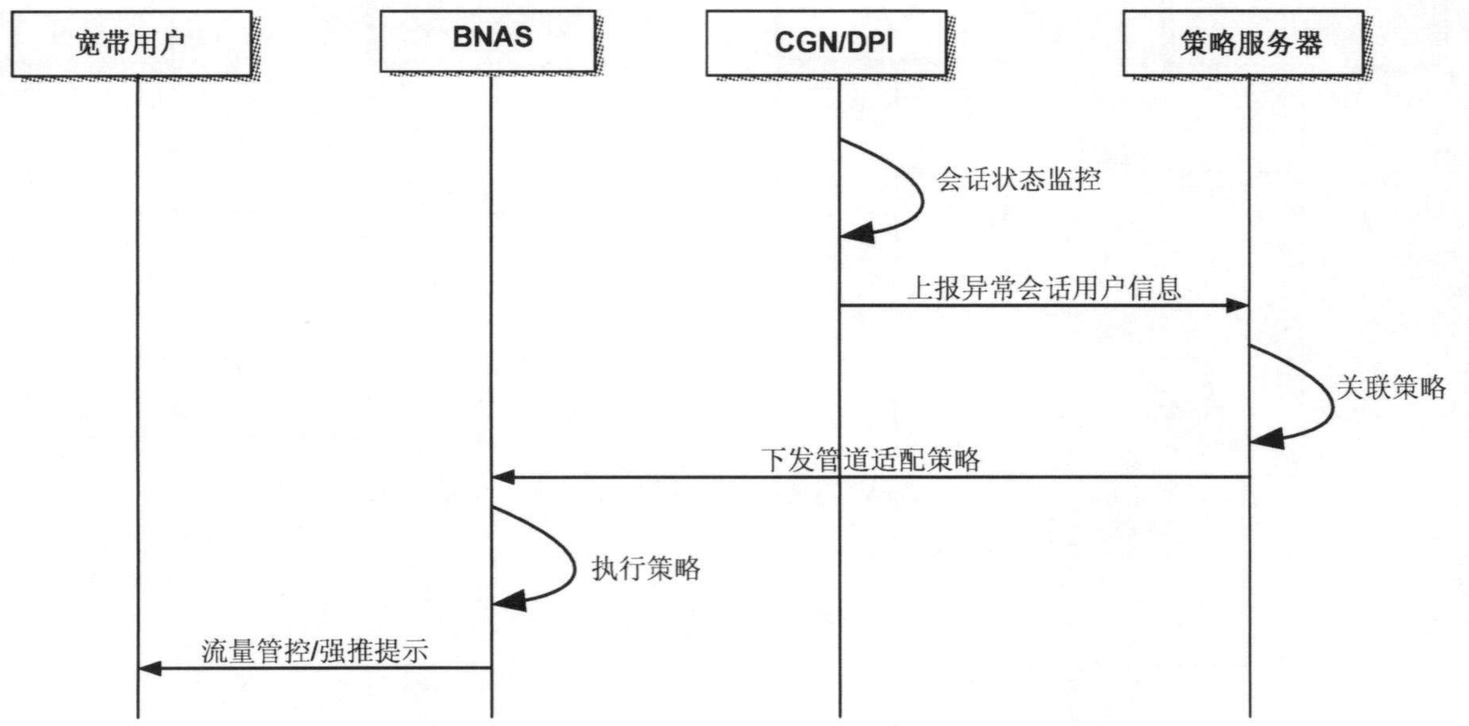

图 18　BNAS 设备与 CGN/DPI 网关联动

图 18 的流程说明如下：

a）　CGN/DPI 网关检测用户会话；

b）　当发现特定用户会话状态异常，上报相关信息给策略服务器；

c）　策略服务器根据上报信息，选择合适的管控策略下发给 BNAS 的特定用户；

d）　BNAS 根据管道适配策略的对象和策略内容执行管控策略；

e）　BNAS 对异常用户流量管控并可以通过 Portal 强推技术提示用户。

图 19 所示是 BNAS 作为 LAC 和时，通过 LAC 和 LNS 之间的协议交互对 LAC 下发管道策略，这个策略可以是更改 L2TP 隧道会话限制策略，也可以是更改 LAC 下用户的 QOS 策略。因为 LNS 分配地址，因此只有 LNS 可以向管道策略服务器上报用户的 IP 网络信息，管道策略服务器只能向 LNS 下发管道策略。因此 LNS 和 LAC 直接可以通过 Radius Proxy 等接口传递管道策略。

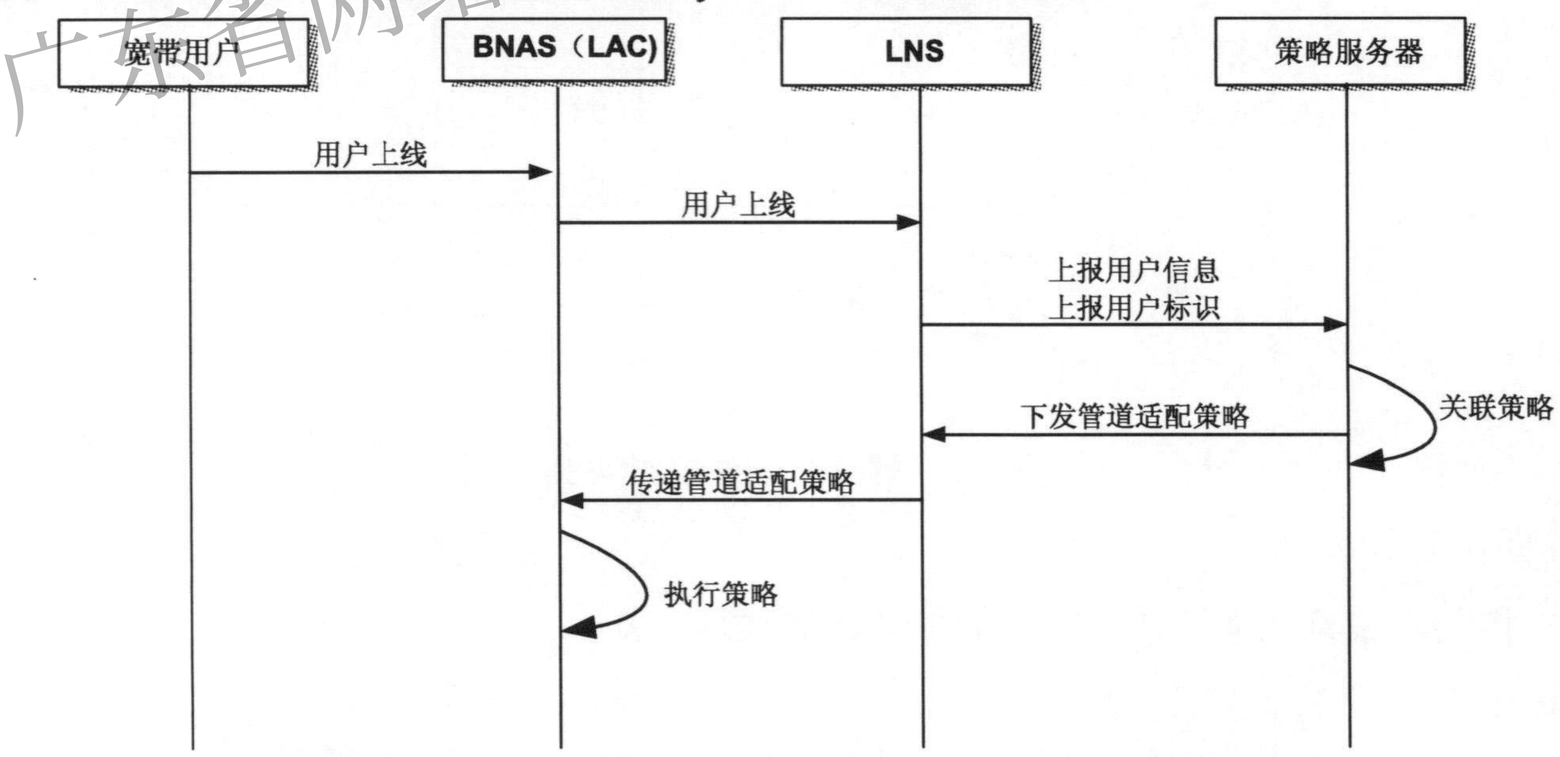

图 19　BNAS 设备作为 LAC 与 LNS 设备的联动

特别的，当 BNAS 设备本身融合了其它设备功能，例如融合式 CGN 或者融合式 DPI 的 BNAS 设备，BNAS 本身可以作为触发管道策略规则下发的设备。

8.3.5　网管触发规则下发

BNAS 设备支持接收通过 SNMP 或者其它管理协议接口发送来的映射规则并根据接收到的规则进行业务感知和流量映射、控制策略执行。

9 网络流量和设备资源控制

9.1 设备对管道流量的处理

当 BNAS 设备根据管道适配策略在设备上生成虚拟管道时，根据规则中的匹配策略，需要对匹配的管道流量进行处理。

9.2 QOS 资源的管道策略的实施

管道最常调整的资源是带宽资源和转发优先级，因此动态的对管道流量进行带宽和优先级调整是 BNAS 设备必须支持的。BNAS 设备必须能够根据策略服务器的需求对所需的管道流量进行动态的 QOS 调度：

— BNAS 设备必须支持接收通过 Radius COA 下发的动态策略，可选支持 Diameter 等其他策略控制协议；

— 策略服务器下发管道适配策略中包含 QOS 策略，BNAS 设备把策略映射到层次化管道。QOS 的层次化规则和管道映射层次规则一一对应，图 20 所示是一个层次化规则和层次化管道映射一一对应的例子。

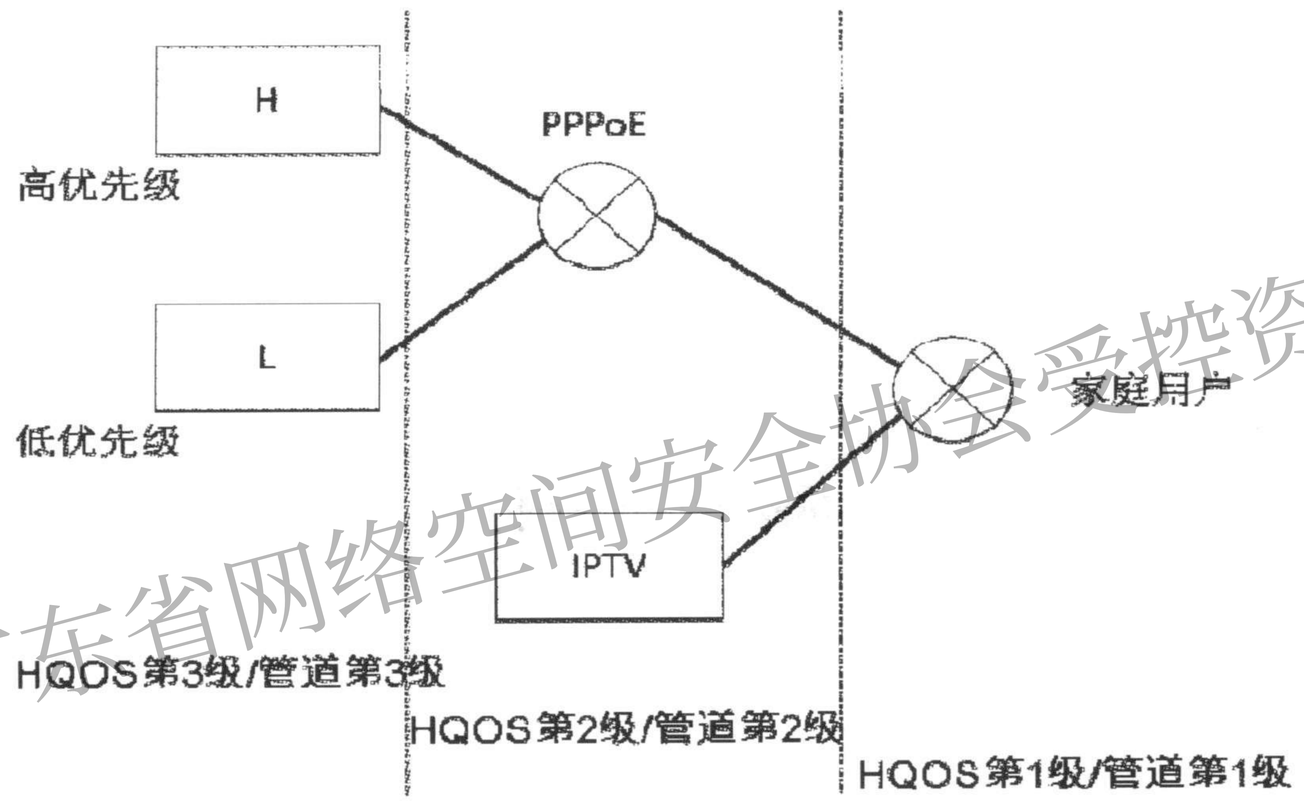

图 20 层次化管道规则映射模型

这种动态的 QOS 处理，不仅仅适用于需要认证计费的传统宽带业务，也适用于无需认证计费的普通网络侧业务和 VPN 业务，且同时支持 CGN、DS-Lite 等 IPv6 演进方案。

9.3 动态的设备资源控制

BNAS 设备需要支持虚拟管道的其他资源的控制，前面描述过了如果设备映射出了虚拟管道，除 QOS 和带宽资源之外，BNAS 设备可以对 5.3 节定义的设备上的其他资源进行动态的控制。

如果设备上的智能管道映射对象为 L3VPN 或者 L2VPN 的隧道，那么设备应该支持和管道质量相关的隧道属性动态下发，而传统 BNAS 设备的隧道资源是不能动态调整的，比如说隧道带宽或者隧道内的业务控制资源。

在智能管道的组网中，BNAS 设备需要支持对隧道资源的动态控制，需要把一些隧道本身具有的资源控制功能属性化，例如对于 VPLS 单 VSI 的 MAC 表资源，可以按如下步骤进行控制：

a） 初始限制某企业 VSI 的 MAC 表容量；

b） 企业动态改变 MAC 表限制，策略服务器向 BNAS 设备下发策略；

c） BNAS 设备增加 MAC 表容量。

当 BNAS 设备融合了 CGN 业务时，每个用户将面临会话表资源和会话表建立速率资源的限制，此时 BNAS 设备可以动态控制这些资源，很典型的一种控制方法如图 21 所示。

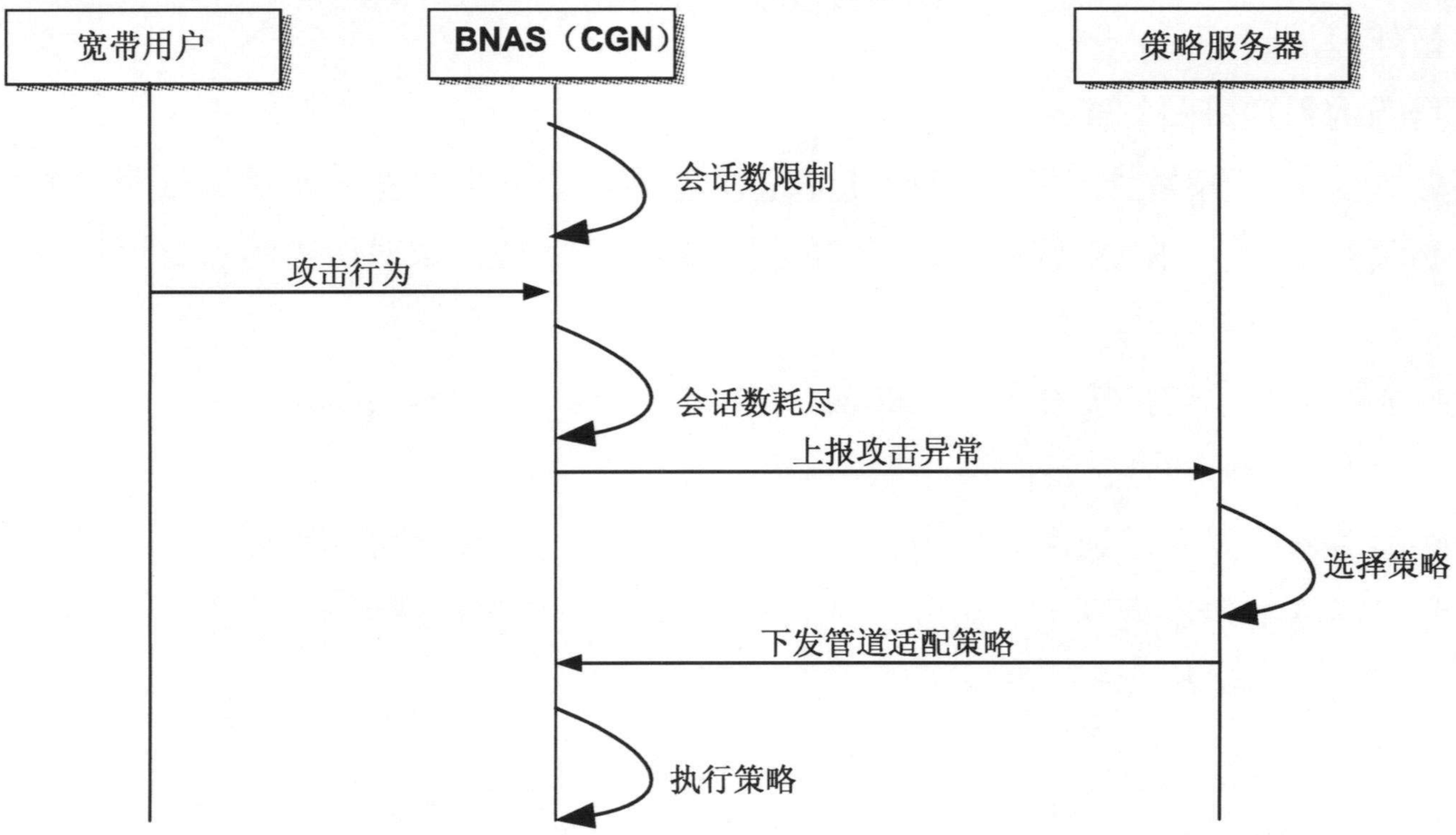

图 21 BNAS（CGN）设备的攻击防范策略

图 21 的流程说明如下：

a） 初始对用户的会话表资源简单控制，例如当用户上线时控制用户的会话数；

b） 用户攻击行为导致会话表耗尽，无法访问网络；

c） BNAS 把攻击行为上报管道策略服务器，管道策略服务器根据用户等级选择合适的管道策略，这里把用户映射为管道，策略主要是 CGN 安全策略；

d） 管道策略服务器给 BNAS 下发策略；

e） BNAS 根据下发的策略，把用户流量引入不同的虚拟管道，执行不同的管道策略，这个策略可以是保证 CGN 用户访问知名端口，可以是再次划分一段端口资源给 CGN 用户，也可以是强推页面告知用户因为攻击无法访问网络

9.4 管道流量业务分流

如图 22 所示，根据用户接入的类型不同，BNAS 设备可以根据流量映射策略把用户流量分流到不同的设备处理，根据接入用户和处理机制不同，BNAS 设备将不同类型的用户的流量映射成不同的管道分流到不同的路由器，以方便对不同的用户提供差异化服务。

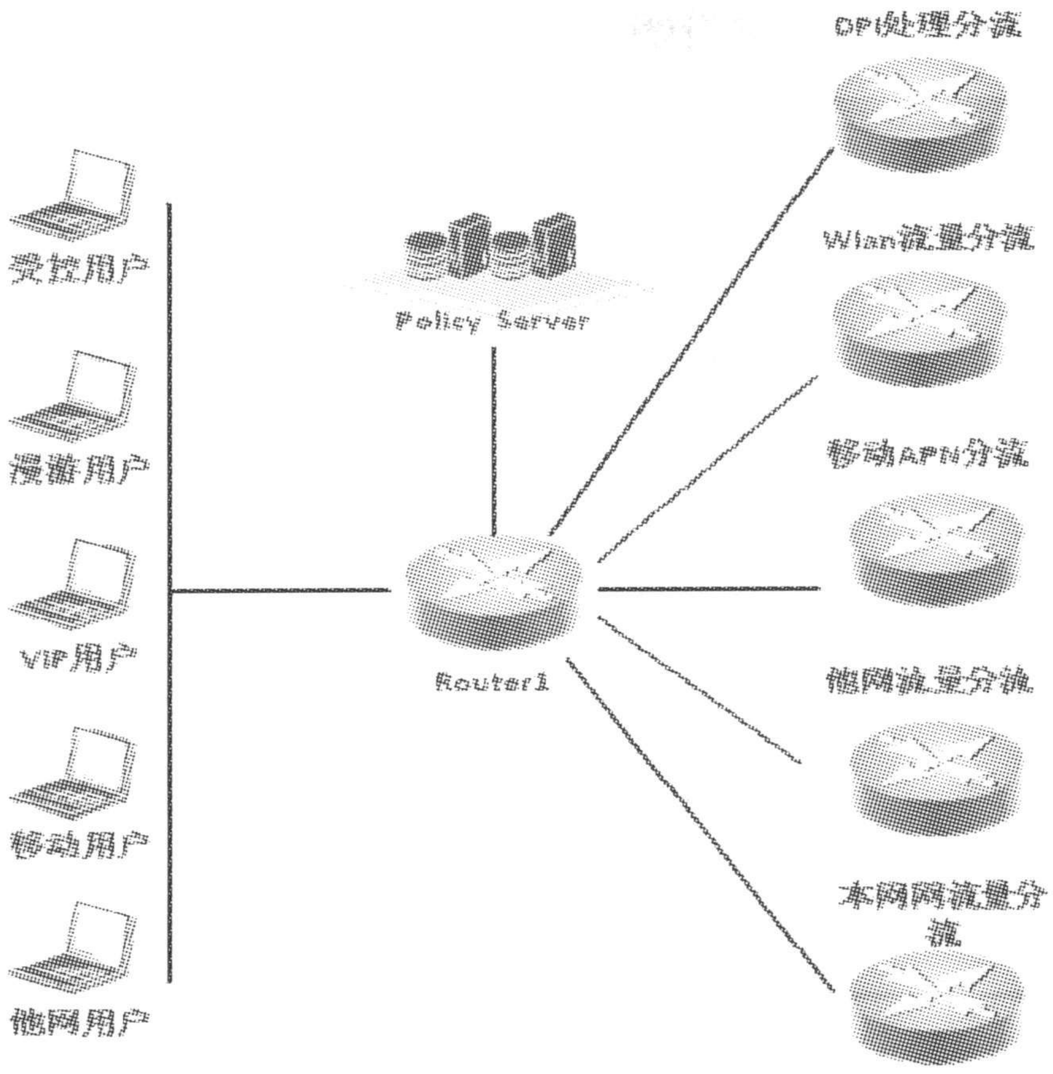

图 22　根据流量映射策略分流

如图 23 所示，用户可以通过动态改变套餐类型来更改归属分流管道，当然，这种分流也可以通过 BNAS 的配置接口临时配置新的通道，将用户分流到这个新的通道。

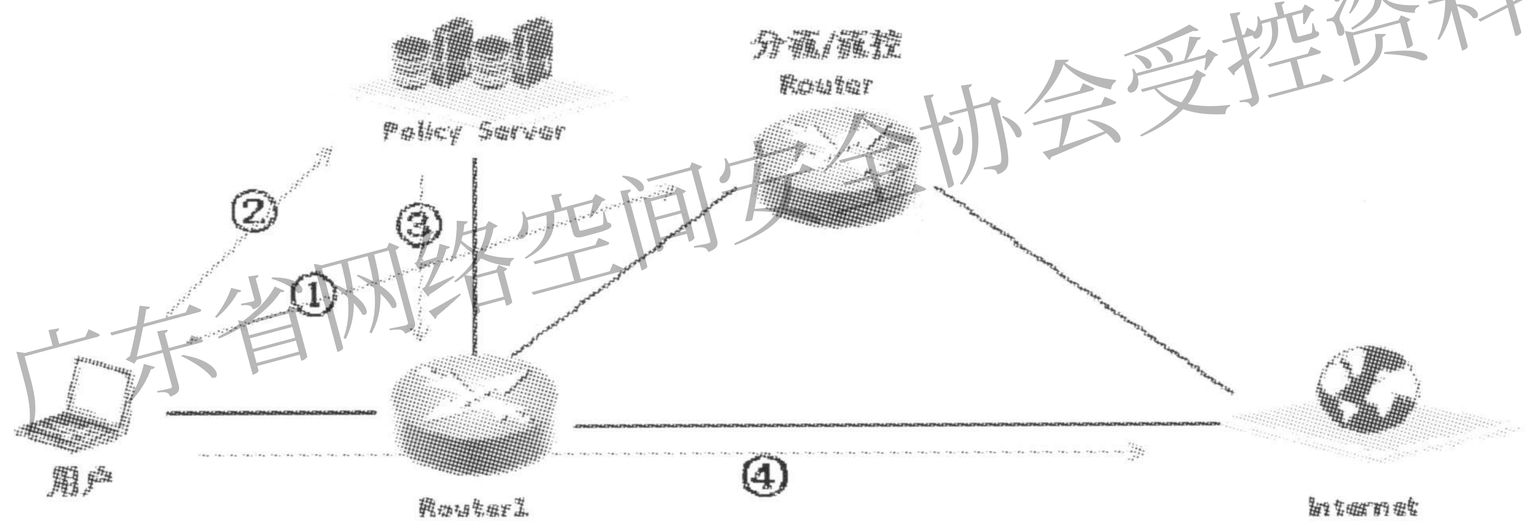

图 23　用户主动更改套餐类型

图 23 的流程说明如下：

①低优先级用户接入设备，初始 BNAS 设备把用户流量分流到普通用户共享的分流路由器，用户流量受限；

②用户在策略服务器上更改套餐类型，升级为高等级用户；

③策略服务器下发映射策略，通知 BNAS 设备将用户流量分流到负载较轻，高带宽少用户的分流管道；

④用户后续流量转发可以享受更高 QoS 的服务。

部署上述方案后，运营商可以根据不同的 QoS 服务等级制定不同的计费策略。

不同等级用户的分流策略按照用户类型的不同可以采用两种不同方式实现。

第一种，如图 24 所示，对认证计费用户，BNAS 设备通过 Domain（用户域）关联不同的 L2TP 隧道实现不同等级用户流量的分流。

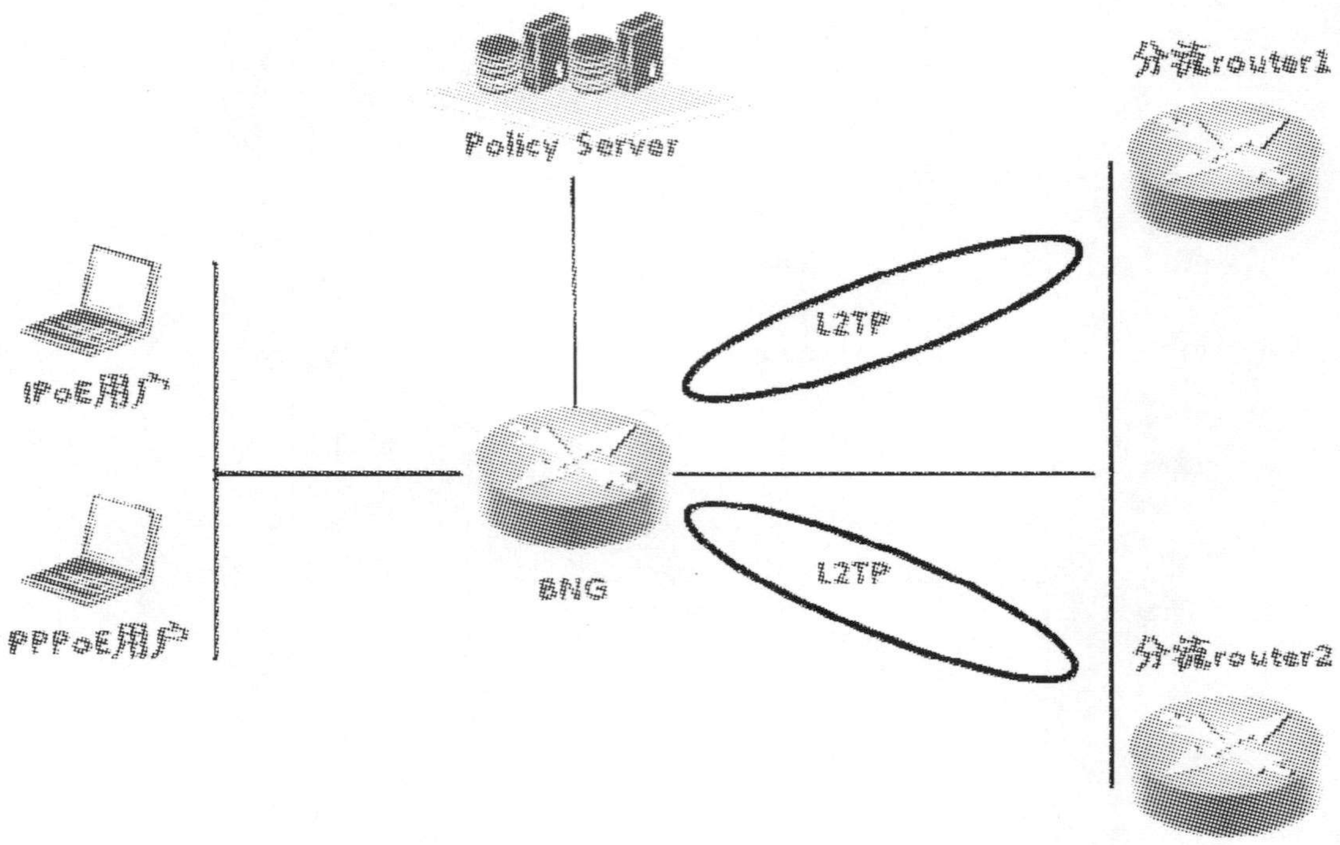

图 24　认证用户的 L2TP 分流

第二种，如图 25 所示，而对于非认证用户，BNAS 网络设备通过用户侧接口关联不同的 VPN 属性来实现基于 MPLS Tunnel/PW 的分流，当用户需要变更业务等级时只需更改用户侧接口的 VPN 属性即可。

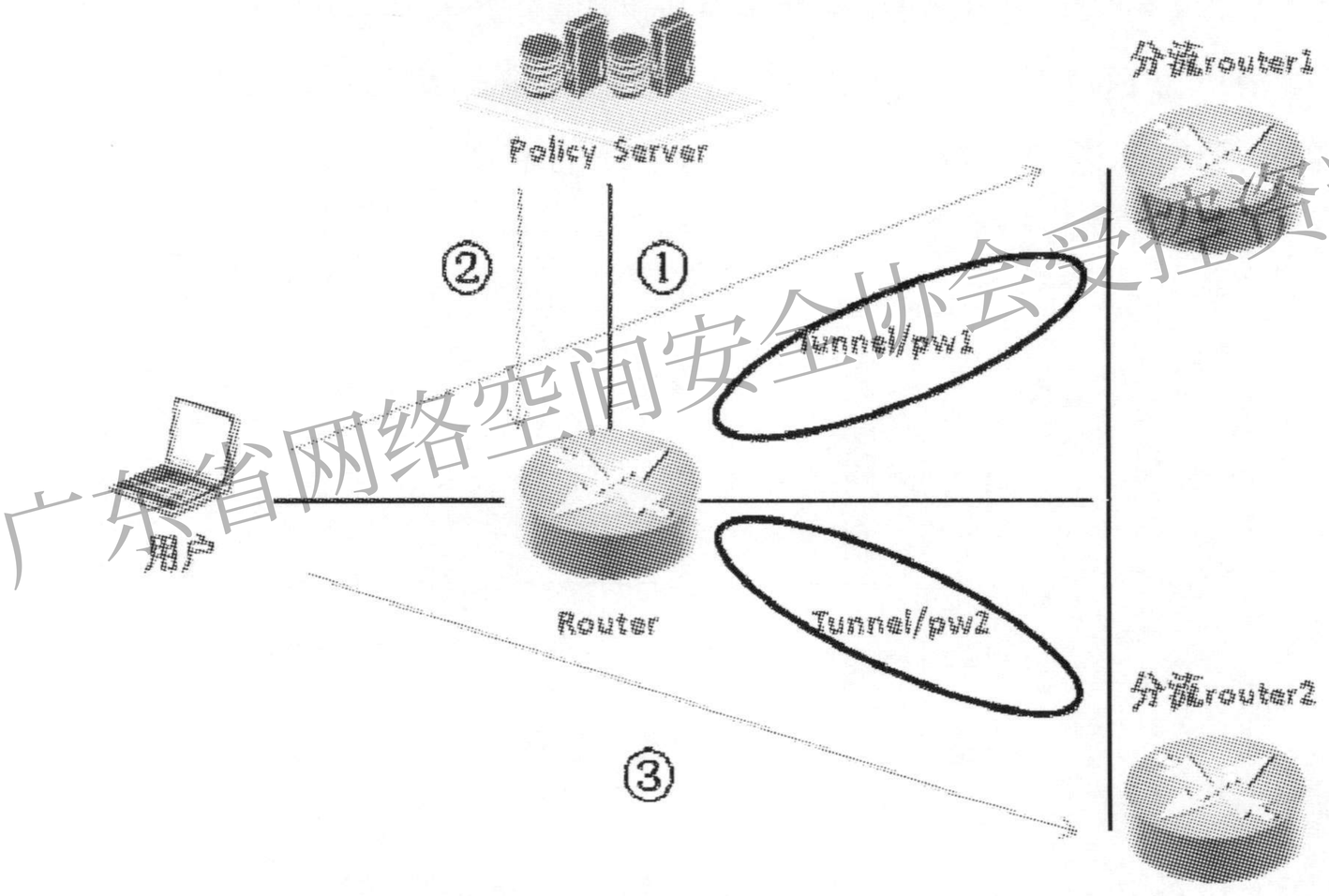

图 25　非认证用户的 MPLS 分流

图 25 的说明如下：

①用户初始使用 PW1；

②策略服务器更改用户接口绑定的 VPN 属性；

③用户后续流量使用 PW2 分流。

9.5　与接入设备联动

9.5.1　协议和技术框架

BNAS 设备与接入设备之间已存在控制面信令的框架和协议，即 BBF 的 L2CM 机制以及与之对应的 IETF 的 ANCP 协议，BNAS 设备通过这个信令面工具可以实现智能管道功能向接入网络的延伸。

图 26 为 L2CM/ANCP 机制的网络框架和消息交互示意图，BBF 网络中的 BNG 设备即为 BNAS 设备，Access Node 为接入设备（如 DSLAM，OLT 等），两者之间存在三种类型的消息：BNAS 向接入设备发送

的控制消息，接入设备返回的响应消息，以及接入设备的信息上报消息。

利用 L2CM/ANCP 现有的功能及与 BNAS 策略执行功能的联动，可以将部分智能管道功能延伸到接入网络，大部分 L2CM/ANCP 功能同时适用于 DSL、以太网和 PON 接口。

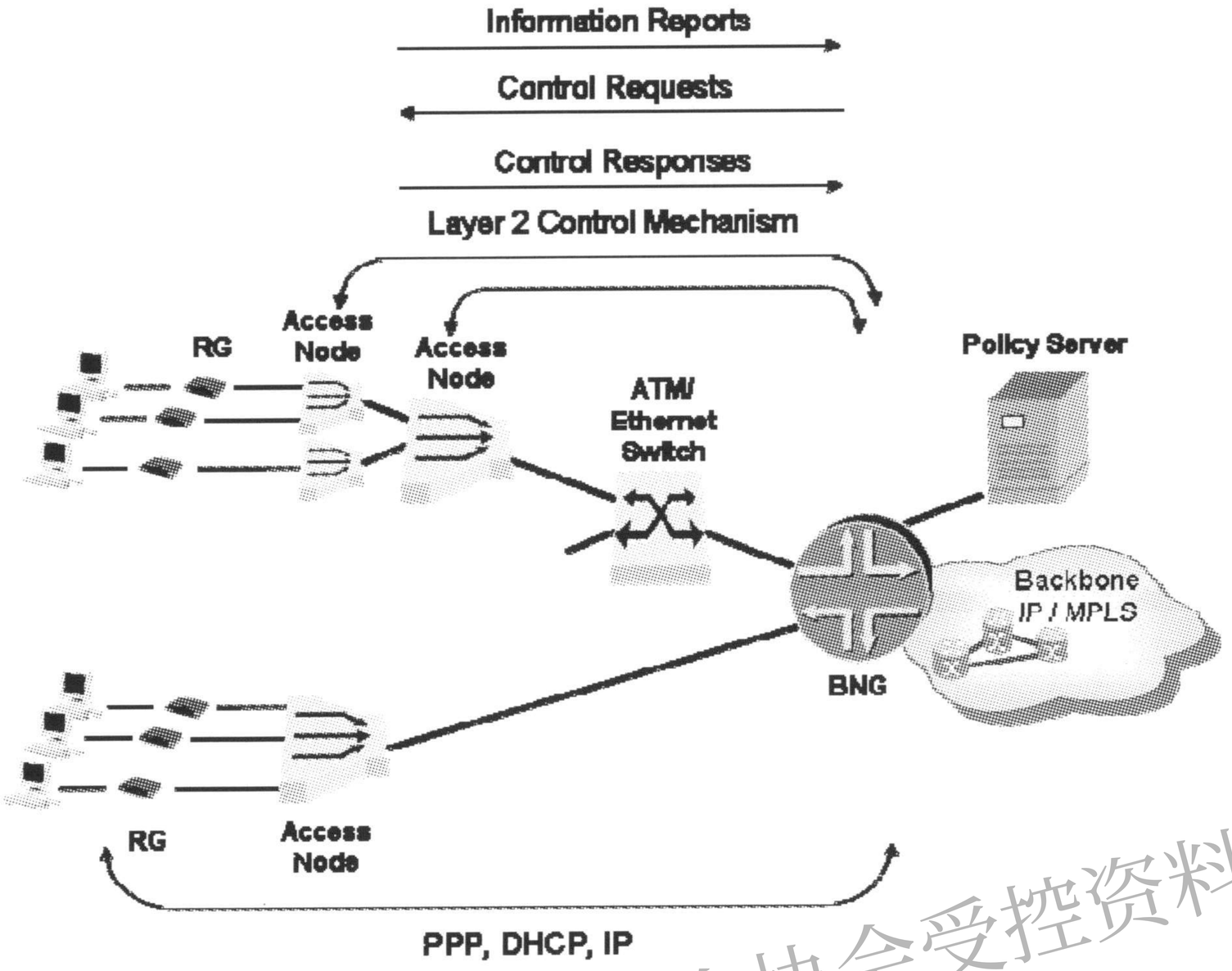

图 26　L2CM/ANCP 机制的网络框架和消息交互

9.5.2　BNAS 对接入链路状态智能感知

如图 27 所示，接入链路在状态就绪之后，接入设备通过信息上报消息向 BNAS 发送用户接入链路的物理参数，BNAS 在处理用户的 BoD、VoD 等需要对用户带宽进行调整的业务前，通过 L2CM/ANCP 机制可以感知到用户接入链路的物理带宽情况，为用户业务提高了质量保障。

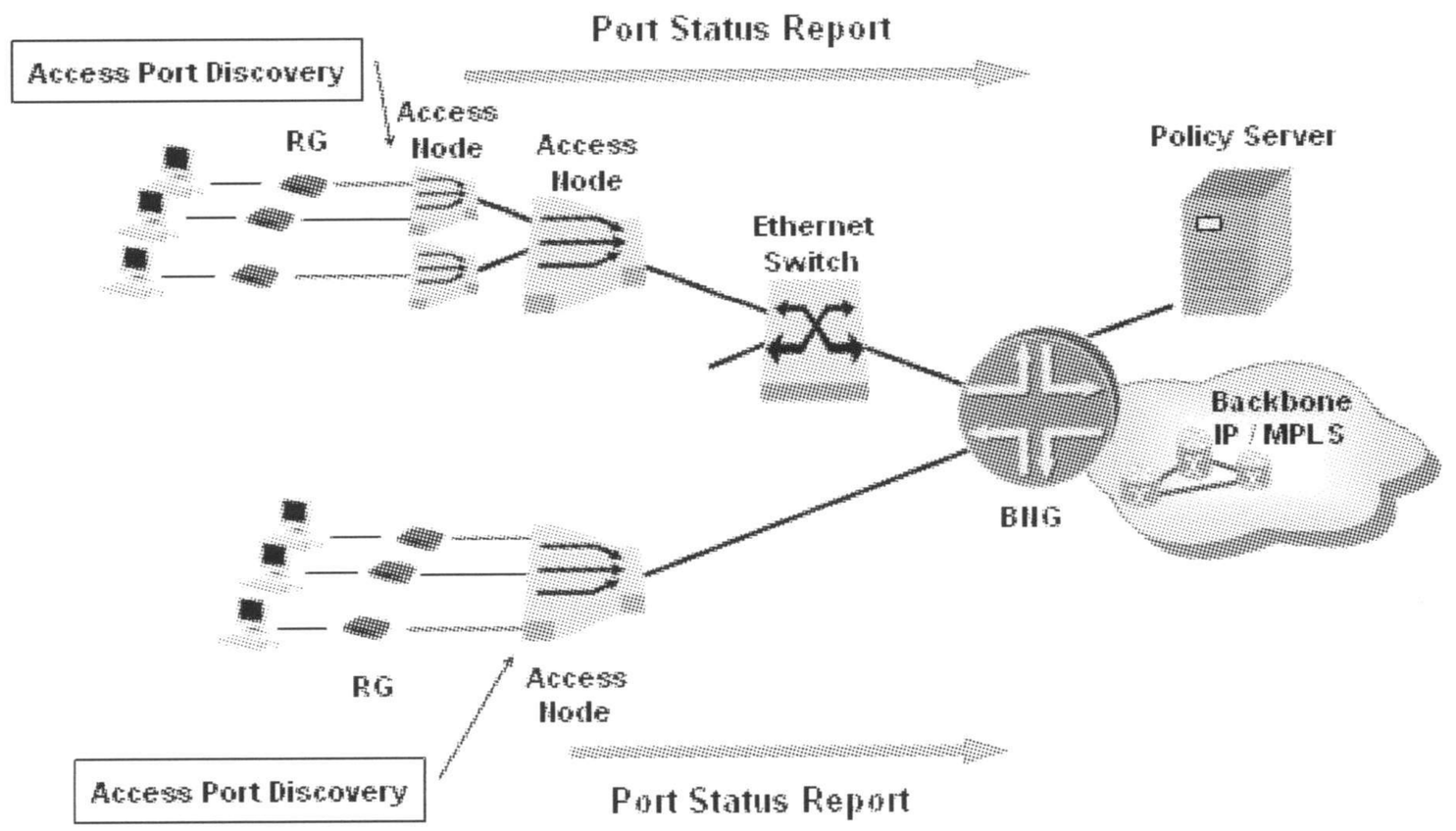

图 27　BNAS 对接入链路状态智能感知

9.5.3 接入链路带宽智能更改或重训

如图 28 所示，当 BNAS 设备发现用户的业务 QoS 需求变更（如 BoD、VoD 业务的带宽需求）且接入链路的物理参数可以满足变更后的用户总需求时，BNAS 设备通过控制消息要求接入设备更改用户接入链路的 QoS 参数。当 BNAS 设备发现接入链路的物理参数低于变更后的用户总需求时，BNAS 设备通过控制消息要求接入设备对该用户的接入链路进行重训（仅限 DSL 接口）。

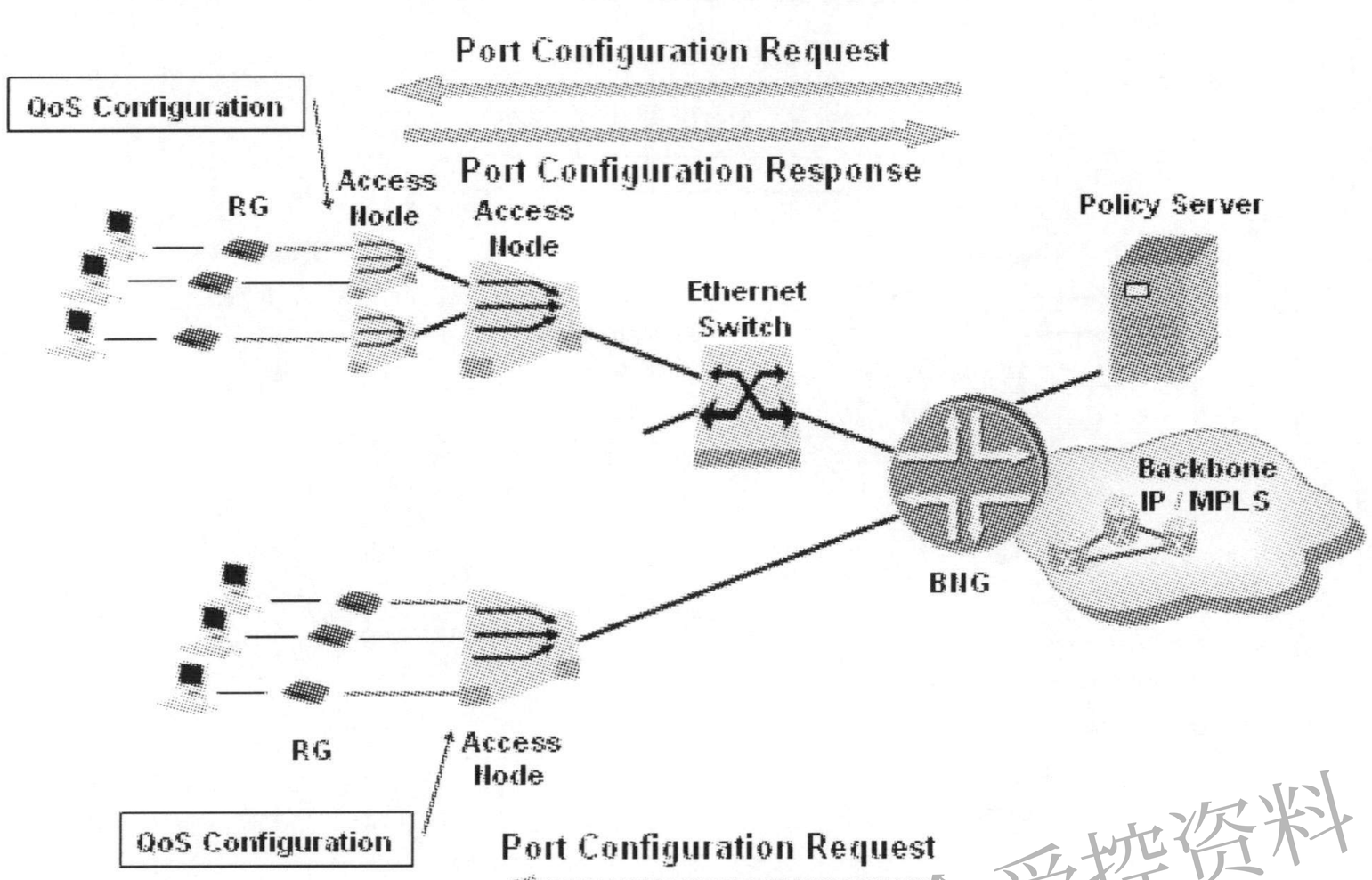

图 28 接入链路带宽智能更改或重训

9.5.4 智能攻击防范

如图 29 所示，当 BNAS 设备在确定有用户在进行网络攻击后，通过控制消息将与该用户进行的网络攻击对应的防范策略发送给接入节点。BNAS 设备对攻击的感知可以通过内置或外置 DPI 设备实现。接入节点执行该防范策略后将执行结果通过控制响应消息发送给 BNAS 设备。通过这种集中感知和分布式处理的方式，可以减少网络攻击流量对 BNAS 设备造成的处理压力。

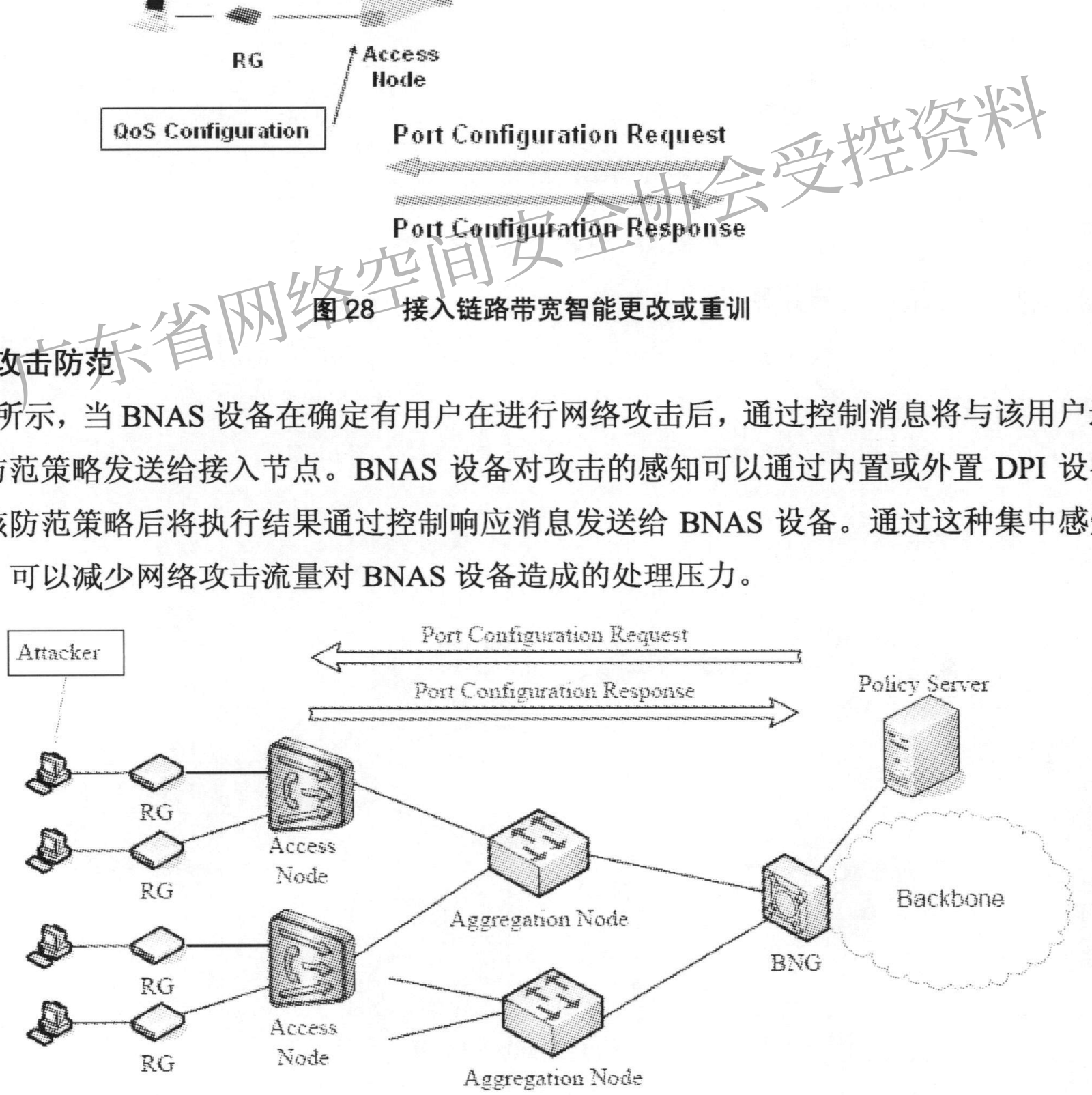

图 29 智能攻击防范

9.5.5 智能组播计费

如图 30 所示，实际网络中 IPTV 组播流量的复制点在接入设备，目的是减少 BNAS 设备的性能压力。此时，如果需要对用户点播的组播业务进行按时长计费时，那么接入设备在将组播业务数据提供给用户的过程中记录该数据流的开始时刻和结束时刻，并通过信息上报消息携带该用户的计费信息中发送给 BNAS 设备。BNAS 收到计费信息后，通过 Radius 计费消息将其发送给计费服务器。

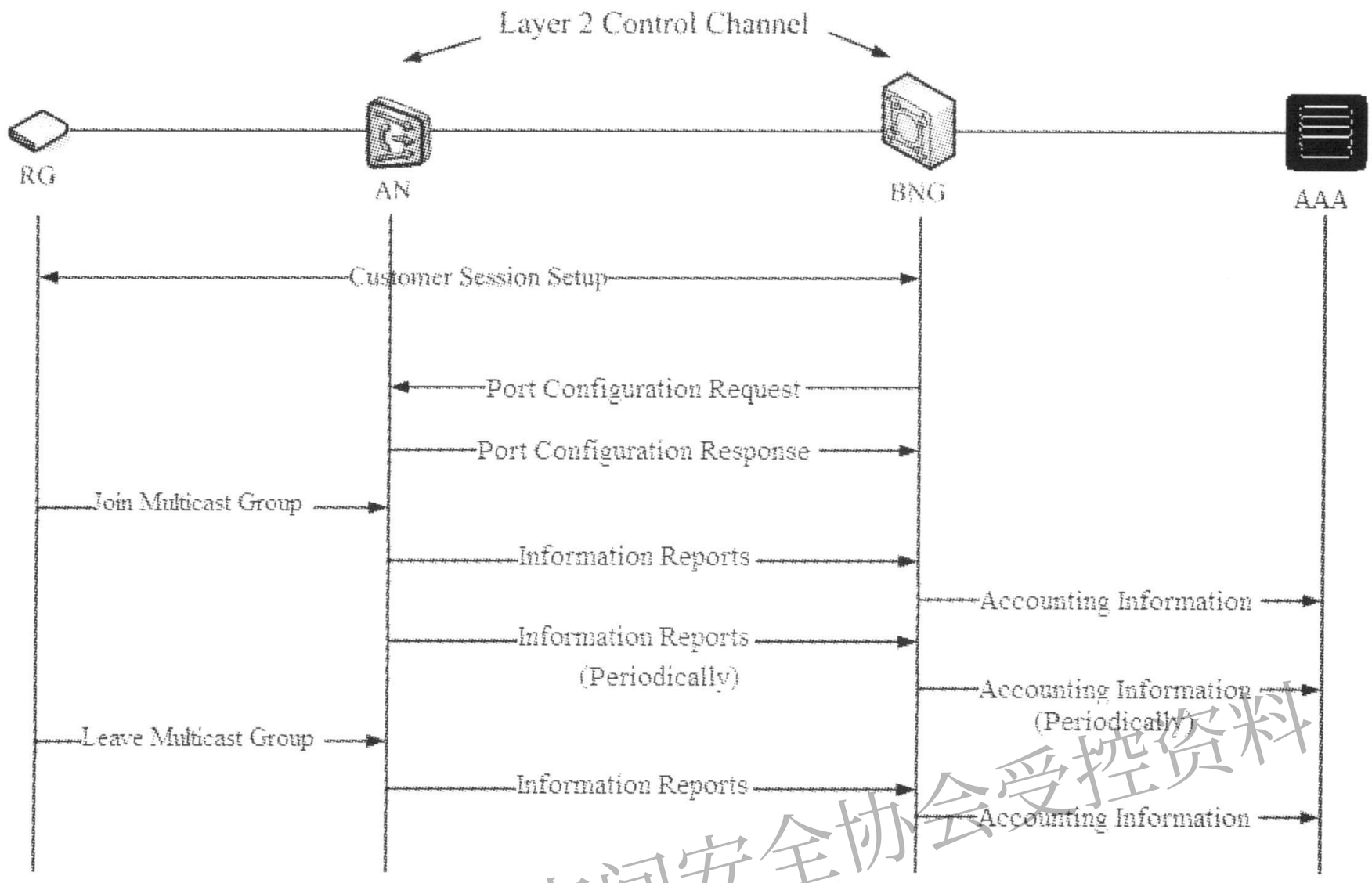

图 30 智能组播计费

中华人民共和国
通信行业标准
宽带网络接入服务器（BNAS）设备流量分析控制技术要求
YD/T 2817-2015
*
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：1.75　　2015年12月北京第1次印刷
字数：45千字
15115·683
定价：20元