

ICS 33.040.01
M 32

YD

中华人民共和国通信行业标准

YD/T 2297-2011

IPv6 用户会话技术要求

Technology specification for IPv6 session

2011-06-01 发布

2011-06-01 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.....2

 3.1 术语和定义.....2

 3.2 缩略语.....2

4 概述.....4

5 用户会话.....4

 5.1 会话生命周期.....4

 5.2 会话类型.....5

 5.3 IPv6 会话和 IPv6 流.....5

 5.4 IPv6 会话侦测.....5

 5.5 IPv6 会话恢复.....7

 5.6 IPv6 会话终止.....8

6 IPv6 会话管理.....9

 6.1 IPv6 会话认证，授权和计费（AAA）.....9

 6.2 IPv6 会话分组.....11

 6.3 IPv6 会话监控.....12

 6.4 会话的流量策略.....17

7 IPv6 会话用户认证模式.....17

 7.1 基于 DHCP 的认证.....17

 7.2 基于 PANA 的认证.....18

 7.3 基于 RS 的认证.....20

附录 A（规范性附录） IP 会话创建和认证的用例.....21

参考文献.....23

前 言

本标准是在 BBF 所制定的 IPv6 会话相关标准基础上参考了 IETF 的相关标准制定而成的。

本标准是“IPv6 协议”系列标准之一，该系列标准预计的结构及名称如下：

1. YD/T 1341-2005 IPv6 基本协议——IPv6 协议 (IETF RFC2460:1998, MOD)
2. YD/T 1915-2009 IPv6 技术要求——移动 IPv6 快速切换
3. IPv6 技术要求——IPv6 路由器重编号协议 (IETF RFC2984:2000, NEQ)
4. IPv6 技术要求——IPv6 反向邻居发现协议 (IETF RFC3122:2001, NEQ)
5. IPv6 技术要求——IPv6 路径最大传输单元发现协议 (IETF RFC1981:1996, NEQ)
6. IPv6 动态主机配置协议
7. IPv6 技术要求——支持计算机移动部分
8. YD/T 1442-2006 IPv6 网络技术要求——地址、过渡及服务质量
9. YD/T 1343-2005 IPv6 邻居发现协议——基于 IPv6 的邻居发现协议 (IETF RFC2461:1998, MOD)
10. IPv6 邻居发现安全性技术要求
11. IPv6 用户会话技术要求
12. YD/T 1344-2005 IPv6 地址结构协议——IPv6 无状态地址自动配置
13. YD/T 1612-2007 IPv4 网络向 IPv6 网络过渡中的互联互通技术要求
14. YD/T 2029-2009 基于软线技术的互联网 IPv6 过渡技术框架
15. YD/T 1635-2007 IPv6 网络技术要求——面向网络地址翻译 (NAT) 用户的 IPv6 隧道技术
16. YD/T 1656-2007 采用边界网关协议多协议扩展 (BGP-MP) 的基于 IPv6 骨干网的 IPv4 网络互
联 (4 over 6) 技术要求

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：华为技术有限公司、工业和信息化部电信研究院。

本标准主要起草人：丁一兰、唐 浩。

IPv6 用户会话技术要求

1 范围

本标准规定了在宽带接入汇聚网中基于 TR-101 架构的 IPv6 用户会话和 IPv6 会话组的概念，定义了相关网元的技术要求。本标准还规定了在 IPv6 用户会话周期中，通过用例、机制、协议和相关的交互来保证 IPv6 用户会话的实现及针对 IPv6 流所需要采取的流量特殊处理。本标准中涉及的 IPv6 流的分类仅限于在 IP 网络层和传输协议层。

IPv6 用户会话周期包括下面一系列可能的阶段：

- IPv6 用户会话的侦测和创建；
- IPv6 用户会话策略的应用和改变，包括认证授权和计费，监控，会话组等；
- IPv6 用户会话的恢复和终止。

本标准适用于 IPv6 网络或在宽带接入时使用 IPv6 的情况。

本标准中除明确说明外，IP 协议、PPP 协议和 DHCP 协议版本均指版本 6。

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。

IETF RFC 2131	动态主机地址配置协议（DHCP）
IETF RFC 2684	ATM 适配层 5 承载的多协议封装（IPoEoA）
IETF RFC 2710	组播监听者发现协议（MLD）
IETF RFC 3315	IPv6 的动态主机地址配置协议（DHCPv6）
IETF RFC 3633	DHCPv6 的 IPv6 前缀委派选项
IETF RFC 3736	IPv6 的无状态 DHCP 业务
IETF RFC 3748	PPP 可扩展认证协议（EAP）
IETF RFC 4649	DHCPv6 中继代理的 Remote-ID 选项
IETF RFC 4861	IPv6 的邻居发现
IETF RFC 4862	IPv6 无状态地址自动配置
BBF TR-59	DSL 演进—支持 QoS 使能 IP 业务的架构需求
BBF TR-92	宽带接入服务器需求
BBF TR-101	以太网为基础的 DSL 汇聚网的迁移
IEEE802.1ad	局域网和城域网 站点和媒体访问控制连通性发现
IEEE802.1Q	局域网和城域网 虚拟桥接局域网

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

会话 Session

一个逻辑结构，表示一个提供给用户设备终端网络连接服务，关联到用户数据和控制面策略。会话可以动态创建和撤销。

3.1.2

IPv6 会话 IPv6 Session

一个会话，其数据面分类器由至少一个 IPv6 源地址和目的地址分类器组成，用户的 IPv6 地址前缀可作为会话的标识之一。

3.1.3

IP 流 IP Flow

由一个 5 元组 IP 参数流分类器定义，一个 IP 流是应用在会话上的流量策略的分类要素。

3.1.4

流分类 Flow Classify

采用一定的规则来识别符合某类特征的报文。

3.1.5

流分类器 Flow Classifier

在网络设备上对报文流进行分类的一组规则的集合。

3.1.6

会话保活 Session Keepalive

用来维护设备间的会话不被超时关闭的机制，例如周期性发送探测报文。

3.1.7

IP 边缘设备 IP Edge Device

服务提供商描述从会话结构中所收集信息的概要。IP 边缘设备可以根据其计费策略在会话开始、结束和会话存在过程中的中间每隔一段时间创建计费记录。每个计费记录包括一个标识符，用于将这个计费记录唯一地匹配于生成它的会话。

3.2 缩略语

下列缩略语适用于本文件。

AAA	Authentication, Authorization and Accounting	认证授权计费
AN	Access Node	接入节点
BFD	Bi-directional Forwarding Detection	双向转发检测
BNG	Broadband Network Gateway	宽带网关
BRAS	Broadband Access Server	宽带接入服务器
DAD	Duplicate Address Detection	重复地址探测
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议

DHCPv6	Dynamic Host Configuration Protocol for IPv6	IPv6 的动态主机配置协议
DHCP-PD	DHCP Prefix Delegation	动态主机配置协议前缀委派
DHCPv6-PD	DHCPv6 Prefix Delegation	IPv6 动态主机配置协议前缀委派
DoS	Deny of Service	拒绝服务攻击
DRL	Default Router List	默认路由列表
DSL	Digital Subscriber Line	数据用户业务线路
EAP	Extensible Authentication Protocol	可扩展认证协议
GUA	Global Unicast Address	全局单播地址
GUID	Global User ID	全局用户标识
IP	Internet Protocol	互联网协议
IPoE	IP over Ethernet	以太网承载的 IP
IPv6	Internet Protocol version 6	互联网协议版本 6
ISP	Internet Service Provider	互联网服务提供商
L2CP	Layer 2 Control Protocol	第二层控制协议
LAN	Local Area Network	局域网
LLA	link-local address	链路-局部地址
MAC	Media Access Control	媒体访问控制
MLD	Multicast Listener Discovery	组播监听者发现
NA	Neighbor Advertisements	邻居通告
NAP	Network Access Provider	网络访问提供商
NAT	Network Address Translation	网络地址翻译
NC	Neighbor Cache	邻居缓存
ND	Neighbor Discovery	邻居发现
NS	Neighbor Solicitation	邻居请求
NUD	Network Unreachability Detection	网络不可达探测
PAA	PANA Authentication Agent	PANA 认证代理
PaC	PANA Client	PANA 客户端
PANA	Protocol for Carrying Authentication for Network Access	接入网认证信息承载协议
PAP	Password Authentication Protocol	密码认证协议
PC	Personal Computer	个人电脑
PIO	Prefix Information Option	前缀信息选项
PL	Prefix List	前缀列表
PPP	Point-to-Point Protocol	点对点协议
PPPoA	PPP over ATM	ATM 承载的 PPP
PPPoE	PPP over Ethernet	以太网承载的 PPP
PSTN	Public Switched Telephone Network	公共交换电话网
RA	Router Advertisement	路由器通告

RADIUS	Remote Authentication Dial In User Service	远端拨入用户认证服务
RG	Residential Gateway	家庭网关
RS	Router Solicitation	路由器请求
SLAAC	StateLess Address AutoConfiguration	无状态地址自动配置
STB	Set-Top Box	机顶盒
UDP	User Datagram Protocol	用户数据报协议
WAN	Wide Area Network	广域网

4 概述

本标准的目的是为了定义适用于宽带接入环境下，IPv6 用户会话及 IPv6 流的分类相关的基本概念，并且包括 IPv6 会话的认证以及管理方法，用于帮助网络运营商提供一套更广泛的可控制和可计量的 IPv6 业务。

本标准列举了各个网元的基本要求，用来确保整体功能的完整实现和制造商之间的互操作性。

5 用户会话

会话一般用于描述和一个给定用户相关联的所有通信流量，不管是何种接入类型或接入技术。会话一旦创建，可以看作是一个网络边缘到用户的专用接口。创建的会话提供了用户策略的供应环境。用户策略与接入方法无关，用于接入一个网络服务。一个会话由一组参数标识，这些参数直接从用户数据面、物理设备接口或控制面信息得到，或者从上述几个途径综合得到。每个会话和一个用户身份参数集关联，并称为具有一个生命周期。

5.1 会话生命周期

一个会话生命周期一般可以由如下几个阶段组成：

- 会话侦测和创建；
- 决定并执行适用的会话策略（包括认证）；
- 会话的恢复和终止。

上面各个阶段中，会话策略的决定和执行阶段可以伴随其他阶段进行，例如会话创建过程中可以进行认证、授权。这些阶段将在下面描述，以便了解上述 IPv6 会话的会话周期的意义和机制。

会话通常是由某个数据面或控制面的事件来发起创建的，这个事件必须符合一个预先确定的初始化方法，即初始化事件。例如，对 IP 边缘设备来说，初始化事件可以是收到一个特定的报文，并且网元能从中得到创建一个用户会话所需的足够信息。会话开始和创建阶段通常伴随着一些会话开始策略的执行，认证是其中之一。这些策略的目的在于，以会话创建过程中得到的参数、会话策略的执行情况以及计费条件为基础，评估接入权限。

一旦会话创建，为保持对用户网络连接性的精确监控，要运行针对监控会话连接性的策略，并在控制面或数据面事件指示会话不再延续的时候终止会话，例如，会话的流量超过定量配额或达到固定超时时间，或者当用户断开连接等情况下，终止会话。另外还有一种情况是，由于某些特殊原因（如用户短期故障下线）或者运营商的需求，用户会话会在特定事件或者策略指导下进入禁用状态，但是会话的各项参数仍然被保留。在这种情况下，该用户会话可以被特定事件重新激活，从而恢复用户会话。

在会话生存期间，也可以通过会话以外的控制面或策略面事件或者两者的共同操作来改变会话状态

或相关策略。服务提供商事件可以造成这种改变，例如操作员干预或用户流量达到配额。

会话创建、监控和特定改变事件之后采取的预先确定动作构成用户会话策略。这些策略分成几类专用策略：控制策略，处理来自控制协议和会话相关过程的事件；流量策略，处理用户发送/接收的流量。流量策略要求用一种方法对服从策略规则的流量进行分类，通常所说的“流”的概念可以用于这种分类。

每个会话还需要有某种方法进行恢复或者终止，从而在适当的时候重置或者消除用户的上下文和策略。这可以通过数据或控制平面上由用户策略/终止规则所支配的动作来做到。不过，如何通过不同的会话保活机制来定义 IPv6 会话终止的规则，会有一定的困难。一方面，保活协议的失败能表明会话终止的合理性，而另一方面，由于会话又和控制协议比如 DHCP 耦合在一起，所以只要该控制协议的状态处于有效，那么即便保活失败，会话应该仍然持续。

这两种观点事实上都是合理的，可以应用于不同的 IPv6 会话使用实例。

5.2 会话类型

在宽带环境下，用户 IPv6 地址可以静态分配或动态地通过 DHCP 分配。用户 IPv6 地址在识别 IPv6 会话参数中担任重要部分，所以 IPv6 会话创建阶段需要考虑这些分配机制。因此，基于地址获取方法和会话的总体用途，定义出 IPv6 会话的两种类型。

— 固定会话：特定业务，通常提供给商业终端客户，要求一个固定的 IPv6 地址和一个总是连接的 IPv6 会话，以便连续地允许外部成员或系统拥有到终端客户的连接性。这类固定 IPv6 会话某种程度上类似一条虚拟租用线路，除了最初的会话初始操作以外，没有终端用户上线/下线（登入/登出）操作或动作。

— 动态会话：在典型的家庭业务中，终端用户使用明确的登入/登出，发起到网络提供商的会话连接。接着，网络提供商对终端用户进行动态认证和授权，并分发合适的用户策略。这种会话类型可以模型化为动态 IPv6 会话，类似传统的 PPP 会话，动态配置实现。

按照 BBF TR-59 和 BBF TR-101 的架构，IPv6 会话通常在 BRAS 或者 BNG 上提供。本标准使用 IP 边缘设备这个术语指代 BRAS 或 BNG 这个位置的具体设备。

5.3 IPv6 会话和 IPv6 流

将一般会话概念扩展到 IPv6 协议领域即产生了 IPv6 会话的概念。IPv6 会话表示一个用户的 IPv6 流量，该流量和用户的 IPv6 地址等参数相关联。IPv6 会话是网络提供商和用户 IPv6 端点间的连接及资源的一个抽象表达，并且允许对 IPv6 会话进行策略应用。

如前面提到的，流量策略要求一个通过“流”定义的流分类机制。在 IPv6 会话中，就是通过 5 元组的 IPv6 流分类机制来定义 IPv6 流。

从上述的介绍可以得到，一个基本的 IP 边缘设备功能需求如下：

IP 边缘设备必须能支持 IPv6 用户会话并且必须支持 IPv6 流分类的流量策略的配置。

5.4 IPv6 会话侦测

本节讲述用户会话的侦测机制。运营商使用的架构可能是仅为 IPv6、仅为 PPP 或是 IPv6 与 PPP 混合接入的模式。下面将 PPP 和 IPv6 会话对网元的功能需求分别列出，以便于适应接入模式的灵活性。

用户会话的概念独立于处理用户流量的物理接口类型，但需要在连接 IP 边缘设备到汇聚网的物理和逻辑接口上支持适当的会话侦测机制。特别当用户会话流量是通过 DSL 的汇聚网到达 IP 边缘设备时，这个接口相当于 TR-92 和 TR-101 架构中的 V 参考点。IP 边缘设备需要在下面的协议栈支持 IPv6 用户会话侦测，必要时也要支持 PPPv6 用户会话侦测。

- IPo802.1ad 用 IEEE802.1ad(QinQ)承载 IP 会话
- PPPoEo802.1ad 用 IEEE802.1ad 承载 PPPoE 会话
- IPo802.1Q 用 IEEE802.1Q(VLAN)承载 IP 会话
- PPPoEo802.1Q 用 IEEE802.1Q 承载 PPPoE 会话
- IP over RFC2684 bridged 用 IETF RFC2684 所述桥接模式承载 IP 会话
- IP over RFC2684 routed 用 IETF RFC2684 所述路由模式承载 IP 会话 ATM 的多协议封装
- PPPoE over RFC2684 bridged 用 IETF RFC2684 所述桥接模式承载 PPPoE 会话
- PPPoA ATM 承载的 PPP 会话

另外，为了处理个别用户可同时使用 PPPoE 和 IPoE 两种协议（例如 PPPoE 用于互联网接入，IPoE 用于机顶盒连接）这种情况下的混合的协议部署，IP 边缘设备要在给定接口上同时支持两种协议。

5.4.1 静态 IPv6 会话侦测

拥有绑定在逻辑接口上并且不与其他用户共享的静态 IPv6 配置的用户，可以通过对应逻辑接口的静态 IPv6 会话来描述。当逻辑接口和用户之间是 1:1 关系时就是这种情况。这种情况下，操作员配置 IPv6 用户会话的动作视为 IPv6 会话开始事件。

IP 边缘设备必须支持在专用逻辑接口上配置永久或静态 IPv6 用户会话。

5.4.2 动态 IPv6 会话侦测

IP 本身没有能在用户传送数据包之前发信号通知会话开始的控制协议。在特定条件下，例如 IP 边缘作为 DHCP 中继/客户端，即将建立的 IPv6 会话由相关协议事件提前通知，但有时无法做到，例如当用户使用的是静态 IPv6 地址的时候。因此，要为动态 IPv6 会话定义一个可当作“生命第一信号”的事件，并决定其后的处理，该事件允许后续对会话应用策略。

下面的事件可以用于定义“生命第一信号”或 IPv6 会话的开始。

— IP 边缘设备收到的一个 DHCPv6 包。当满足以下条件时，该事件标志着一个新 IPv6 会话的开始：

- 1) IP 边缘设备也就是 IPv6 会话连接端点设备是用于客户 IPv6 地址分配的 DHCPv6 中继或服务器；
- 2) 客户配置成使用 DHCPv6；
- 3) 该报文是从客户端收到的第一个 DHCPv6 报文。

— IP 边缘设备接收到的一个 IPv6 报文，该报文的源 IPv6 地址与已经建立的会话不相关。

在没有 DHCPv6 机制的情况下，一个新的 IPv6 会话可以通过 IP 边缘接收一个用户源 IPv6 地址与已经建立的会话不相关的 IPv6 报文的方法来侦测。

对于依靠接入段的以太网承载的纯 IPv6 的网络来说，既要控制 SLAAC 地址分配流程，也要控制 DHCPv6 流程，以每个用户为基础，但是限制与 AAA 子系统的交换次数，因此要求仅当 IP 边缘收到足够多的认证和授权用户的凭证之后，才触发会话开始过程，而不是每次获取部分凭证后立即开始与 AAA 子系统交互，并且触发会话开始过程之后只能继续进行地址分配程序。

附录 A 描述了伴随 AAA 的 IPv6 会话创建的用例。

如果一个 IPv6 用户会话不是显式地通过配置明确绑定在一个专门逻辑接口上，那么 IPv6 用户会话流量就可以被一个或多个逻辑接口接收，从而允许运营商进行会话和实际接口的分离。

根据上述内容，针对不同网元的要求如下所述：

当收到合法用户发起的 DHCPv6 报文时，IP 边缘设备必须支持用户 IPv6 会话的创建。

当收到用户发起的路由器请求 Route Solicitation (见 IETF RFC4861)报文时, IP 边缘设备应支持用户 IPv6 会话的创建。

IP 边缘设备必须按 IETF RFC3315 支持 DHCPv6 有状态地址。

IP 边缘设备的 AAA 接口必须支持接收每个用户的 IPv6 前缀和分配的前缀委派,并分别放在 ICMPv6 RA 和 DHCPv6-PD 选项 (IETF RFC3633) 中通告。

IP 边缘设备应当能发送单播 RA 报文,在前缀信息选项中列出从 AAA 得到的前缀,并标明这个前缀可以用于 SLAAC。单播 RA 必须发给 DHCP 或者 ND 报文中的客户端源地址。

IP 边缘设备必须支持发送不包含前缀信息选项 (PIO) 的 RA 组播报文。

对每个 IPv6 会话, IP 边缘设备必须为接口前缀和委派前缀创建并维护适当的 IPv6 转发表项。

面向客户端的接口上,对于落入分配链路和/或委派 IPv6 前缀范围内的地址, IP 边缘设备必须能将去往或来自于这些地址的流量作为属于一个 IPv6 会话对待,并对这些流量进行分类。

RG 必须分别按照 IETF RFC4861 和 IETF RFC4862 中的规定支持 Neighbour Discovery 和 IPv6 无状态地址分配。

RG 必须按照 IETF RFC3315 和 IETF RFC3736 支持 DHCPv6 协议,并按照 IETF RFC3633 支持 DHCPv6 的 IPv6 前缀选项。

5.4.3 PPPv6 会话侦测

侦测 PPP 会话的机制为人所熟知,并已归纳为 BBF TR-92 和 BBF TR-101 中描述的特性。PPPv6 会话主要直接依赖 PPP 和 PPPoE 协议。

IP 边缘设备必须按照 BBF TR-92 的 4.4 支持 PPPv6 会话侦测和建立。

5.5 IPv6 会话恢复

IPv6 用户会话在某些情况下会出乎意料地中断,比如用户突然非正常下线后又上线、三层或二层连接由于未知原因中断。这些临时的中断并不是由于 IPv6 会话的时效到期造成的。这些中断会引起会话保活机制的失败。运营商可以出于自己的策略考虑,在保活失败的时候选择终止原 IPv6 会话或者仍保留原会话直至租约/会话时长到期。

为进一步说明会话恢复在会话生存周期中的含义,引入如图 1 的简单的状态图来描述会话生存周期中的主要状态。

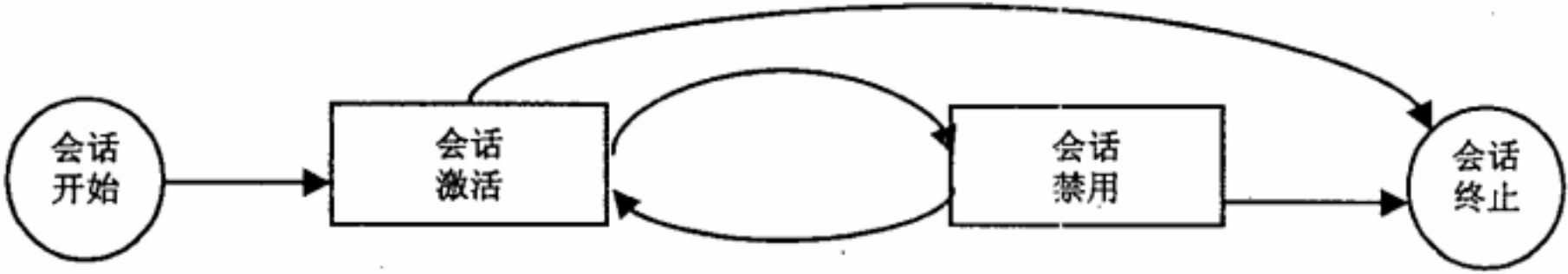


图 1 会话状态示意图

如图 1 所示,会话的主要状态为激活或者禁用,这些状态可以在一定的触发条件下转化。比如,会话侦测和创建后进入激活状态,当监控动作检测到三层连接失败,如端口流量的闪断,则会话将从激活状态进入禁用状态;当会话处于禁用状态时,监控动作检测到三层连接已恢复,则会话重新回到激活状态;若会话处于激活状态,当用户 DHCP 租约到期或者用户发出 DHCPv6 Release 报文时,会话终止;若会话处于禁用状态情况下,用户租约到期或在一段可配置的时间内用户没有再次激活该会话;会话终止。会话终止后,用户被视为下线。会话从禁用状态通过某些条件触发回到激活状态,这个过程是会话恢复。

下面的事件可以看作是 IPv6 会话恢复的信号：

— IP 边缘设备收到的一个 DHCPv6 Solicit 或者 DHCPv6 Request 报文。当满足以下条件时，这个事件标志着一个 IPv6 会话的恢复：

- 报文发自一个已建立 IPv6 会话的客户端；
- 该会话目前处于禁用状态。

这个用例对应于由 DHCP 创建的会话进行会话恢复且该会话恢复由客户端触发。由于 IP 边缘设备存储了相关联的原 IPv6 会话的会话信息，IP 边缘设备接收到 DHCP 客户端发送的报文后根据预设策略（例如基于 MAC 和/或用户线路信息）进行认证，认证成功后恢复原会话并将原会话信息和参数（例如租约信息）下发给用户。在接收到恢复的请求时，IP 边缘设备也可以选择终止原会话从而发起一个新的 IPv6 会话创建。

— IP 边缘设备收到的一个非 DHCP 的 IPv6 报文。当满足以下条件时，这个事件标志着一个 IPv6 会话的恢复：

- 报文的源 IPv6 地址与某个已建立的会话相关；
- 该会话目前处于禁用状态。

如果相关联的原会话起初不是由 DHCP 创建的，会话的恢复只需要将会话的状态设为使能即可，并保留原来的参数设置（例如带宽分配等）。这个用例对应于不是由 DHCP 创建的会话进行会话恢复。

如果相关联的原会话起初是由 DHCP 创建的，那么 IP 边缘设备向用户终端发送 DHCPv6 更新报文以触发用户终端开始上线的恢复流程的协商。这个用例对应于由 DHCP 创建的会话进行会话恢复且该会话恢复由 IP 边缘设备触发。

根据上述内容，针对不同网元的要求如下所述：

当收到用户发起的 DHCPv6 Solicit 或 DHCPv6 Request 报文时，如果已有相关联 IPv6 会话并且该会话处于禁用状态，IP 边缘设备必须支持用户 IPv6 会话的恢复。进行会话恢复时，IP 边缘设备必须根据预设策略对 DHCP 客户端进行认证，认证成功后恢复客户端的 IPv6 会话。

当收到源 IP 地址与已建立会话相关的非 DHCP 的 IPv6 报文时，如果已有相关联 IPv6 会话并且该会话处于禁用状态，IP 边缘设备必须支持用户 IPv6 会话的恢复。

当收到源 IPv6 地址与已建立会话相关的 IPv6 报文时，如果已有相关联 IPv6 会话并且该会话处于禁用状态，IP 边缘设备必须支持向客户端发送 DHCPv6 更新报文来指示用户终端开始上线的配置。

5.6 IPv6 会话终止

IPv6 会话的终止和 IPv6 会话的特性密切相关，例如，会话的侦测和创建方法、保活机制、动态或是静态的会话特性。下列的几个方法可以触发 IPv6 会话的终止。

— DHCP 租约到期或者接收到用户端发出的 DHCPv6 Release 报文

当会话是用 DHCP 的方法来创建的时候，会话终止也是由 DHCP 租约过期的各种事件来标志的。

— 会话保活协议失败

这点将会在会话监控章节(见 6.3)详细说明。

— 命令性的会话终止

这个方法指的是 IP 边缘处理一个自动生成或者由操作员发出的会话终止命令。这种命令可能是用户策略下的时长或流量配额用完触发，也可能是由于用户动作产生（比如用户通过网络入口页面进行登出），

或者是操作员的动作导致。IP 边缘接收到这种 IPv6 会话的接入提示信息时，会做出相应的中断会话的处理。IP 边缘将 IPv6 会话终止原因填充到 DHCPv6 报文的选项字段中，将该报文发送至用户终端来指示终端进行会话终止。

— 接口的下层结构终止

如果用户会话或会话组所依赖的某种下层结构出现故障，比如链路中断，那么会话或会话组可以被终止或者暂时处于禁用状态。

根据以上所述，可以得到下列要求：

当收到来自 DHCP 客户端的 DHCPv6 Release 报文时，IP 边缘设备必须终止相应的 IPv6 会话。

当检测到会话连接的配置 IPv6 地址租约到期时，IP 边缘设备必须终止相应的 IPv6 会话连接。

当检测到会话连接的配置 IPv6 地址续租失败时，IP 边缘设备必须终止相应的 IPv6 会话连接。

当 IP 边缘设备作为 DHCP 服务器时，必须遵从 IETF RFC 2131。

IP 边缘设备接收到 IPv6 会话终止原因的提示信息后，将会话终止原因填充到 IPv6 会话控制信令报文中，例如填充到 DHCP 相应选项字段，发送至用户终端。

当检测到二层或者三层连接中断的时候，IP 边缘必须支持终止相关 IPv6 会话或会话组的配置，或者将相关 IPv6 会话或会话组设置为禁用。

6 IPv6 会话管理

同 IPv4 类似，IPv6 数据平面和控制平面事件也会触发对 IPv6 会话的相应管理。

IPv6 边缘设备必须能够对每个会话分别按配置进行管理，包括认证、授权、计费 and IPv6 地址管理；必须能够由会话控制平面事件来触发会话监控。

IPv6 边缘设备必须支持根据会话的使用环境来配置和进行 IPv6 流量管理。

6.1 IPv6 会话认证，授权和计费（AAA）

为了鉴别 IPv6 用户身份，决定用户的访问权限，请求或触发会话参数的下发，IPv6 会话的管理可以混合使用各种会话侦测机制。

AAA 流程通常是通过 Radius AAA 协议来进行认证、计费、授权，但也可以扩展为支持其他 AAA 协议，如 Diameter。

在不需要对单个用户进行认证而只需要授权的业务的的情况下，IPv6 会话需要某种获取用户凭证信息的机制来进行完整的认证。为了能够收集到用户凭证信息，需要建立一个 IPv6 会话用户认证模型，见第 7 章。

服务提供商可以对未完全识别身份的用户开放业务，比如依据用户线路号来提供业务，这种情况可以直接使用触发会话建立报文中的会话标识符。在这里，IPv6 会话可以使用如下一条或多条的标识符策略：

- a) DHCPv6 报文中包含的 DHCPv6 选项（如 IETF RFC3315 定义的 Interface ID 选项）；
- b) DHCPv6 或 ND 报文中包含的源 MAC 地址；
- c) 报文的源 IPv6 地址；
- d) 报文的入接口标识，如 VCI/VPI；
- e) ND 报文所包含的选项，例如接入线路信息；
- f) 用户的 IPv6 前缀信息。

报文的源 MAC 地址是一种有用的标识符。对于 IPv6 报文，报文的源 MAC 地址是上述标识的重要的补充。源 MAC 地址和 IPv6 地址或前缀绑定是应有的安全机制的一个部分，如 BBF TR-101 的 5.7。

上述方法表明一个 IPv6 会话有可能使用多个标识符，所以更好的方式是使用与用户的接入方式无关的标识符，比如，用户全局 ID (Global User ID - GUID)。GUID 可以用于 AAA 报文来传递其他一些信息，如端口号及其他有用信息。

若使用 DHCPv6 用于地址分配和侦测会话建立，还需要下面一些额外考虑：

- IP 边缘设备需要具有 DHCP relay, proxy 或者 server 功能。
- IP 边缘设备需要监控 DHCP 或 SLAAC 协商过程。当地址分配后，IP 边缘设备能对 IPv6 地址，邻居缓存和前缀列表表项进行维护。同样的，IPv6 地址或前缀与 MAC 地址也需要在 IP 边缘设备上上进行绑定，来防止 spoof 攻击、服务窃取攻击和 DoS 攻击。
- 在三层批发场景下，为支持 DHCPv6 不同 IPv6 地址段分配，IP 边缘设备需要支持为每个会话指定地址池或将 DHCP 报文直接转到特定 DHCP 服务器的机制。
- IP 边缘设备需要保留 DHCP 租期信息，这和 IPv6 会话的状态密切相关。
- IP 边缘设备需要支持在 DHCP 或 SLAAC 程中为每个会话指定前缀信息或者为每个会话从外部获取前缀。
- IP 边缘设备需要为 DHCP 或 SLAAC 过程保留前缀的生存周期信息。
- DHCP 租期时间或前缀的生存周期信息需要与 AAA 服务器提供的会话超时时间(session timeout)同步，来避免会话连接的长时间丢失，特别是当在本地网关和 IP 边缘设备间没有保活协议运行的情况下。

对于 DHCP 或 SLAAC 的 IPv6 会话流的计费，可以使用通用的开始/中间更新/结束的 AAA 机制来完成。

IP 边缘设备可以支持对 Radius 授权 IPv6 会话机制的策略配置。

IP 边缘设备可终止在可以配置的时间内认证失败的会话。

对于 DHCP 建立的会话，IP 边缘设备可具备 DHCP Relay 或 Proxy 的功能。

IP 边缘设备可支持根据 AAA 认证授权过程中 Radius 服务器返回的信息，对 DHCP 过程将 DHCPv6 Solicit 报文转发到 Radius 指定的 DHCP 服务器上，或者，对 SLAAC 过程进行邻居发现报文的后继处理。

IP 边缘设备必须支持可以配置的会话标识，并应该支持下面所列的标识符的混合：

- DHCPv6 或邻居发现报文中的选项；
- DHCPv6 Solicit 或邻居发现报文的路由请求的源 MAC 地址；
- 报文的源 IPv6 地址；
- 报文的源 MAC 地址；
- 报文的源 IPv6 地址前缀。

IP 边缘设备可使用上述标识符来触发 IPv6 会话的认证授权。

对于使用 DHCP 建立的会话，IP 边缘设备必须能够根据会话认证和授权所返回的信息，在特定地址池中为一个会话分配地址。另外，IP 边缘设备必须支持根据认证和授权所返回的参数，将 DHCPv6 Request 报文转发给特定 DHCP 服务器。

对于使用 DHCP 建立的会话，IP 边缘设备可以支持能在 DHCP 续约前或前缀生存周期到期前重新向 AAA 服务器请求授权的配置。

IP 边缘设备应该支持为会话指定一个全局用户标识 (GUID) 用于认证授权。这个 GUID 在会话周期内一直存在, 并且也可以为外部系统所感知。

IP 边缘设备可支持通过某种方式在 AAA 数据库中查找 IPv6 流分类标识的方法, 并在会话认证/授权阶段, 使用该 IPv6 流分类标识来进行针对会话的流量管理的应用。

IP 边缘节点可根据控制层面事件, 如 AAA 服务器报文, 触发对用户权限进行动态管理。

IP 边缘节点可用作动态授权服务器。

IP 边缘设备可以支持 IPv6 和 PPP 会话的 Radius start/stop/interim 计费。

6.2 IPv6 会话分组

用户会话在某些场景下可逻辑归到某个组中, 这个组共享整个流量, 也进行相同管理。一个典型的场景是单个用户接入线路通过一个二层 RG 连接几个 IPv6 主机, 每个主机代表一个 IPv6 会话, 但所有的会话是根据接入线路的逻辑组捆绑在一起的。会话分组主要包括两类:

a) IP 边缘设备通过一个共同的逻辑接口承载所有会话流量, 这个逻辑接口对应一个接入线路 (例如 1:1VLAN 的情况)。在这种情况下, 逻辑接口自然地成为这个会话的分组。

b) 多个用户接入线路的多个会话承载在一个共享的逻辑接口, 例如 N:1 VLAN 的情况。这种情况下, 会话根据其 DHCPv6 选项传送的接入线路的参数进行分组。

a)和 b)的组合分组的情况也存在。根据以上两种情况, 可以得出如下要求:

IP 边缘设备必须支持根据 DHCPv6 选项对会话逻辑分组。

IP 边缘设备必须支持根据会话控制和数据面策略构建会话组。

在一个双栈的 IPv4/IPv6 环境下, 不同的 QoS 策略会需要形成不同的会话逻辑分组。这种情况下的逻辑分组可以通过下面几种方式标识:

a) 一组 IPv4 会话。

b) 一组 IPv6 会话。

c) 一组由相同接入线路标识的所有的 IPv4 会话和 IPv6 会话。

在 IPv6 环境下, DHCPv6 的 option 项可以作为分组的信息。下面 DHCPv6 定义的 option 提供了 DHCPv4 的 circuit-id 和 remote-id 等同的信息。

— Interface-ID option (IETF RFC 3315 定义) 可以由 2 层的 DHCPv6 中继代理增加用于标识接收到客户端报文的接口;

— Relay Agent Remote-ID option (IETF RFC 4649 定义) 可以由 DHCPv6 中继代理增加用于标识远程主机的线路信息。

为了能把 IPv4 和 IPv6 会话捆绑起来, 在 IP 边缘上需要提供根据 DHCPv4 和 DHCPv6 的接入线路信息识别和分组的机制。IP 边缘需要实现下面的要求:

IP 边缘设备必须支持根据 DHCP Relay Forward 报文携带的 DHCPv6 Interface-ID 和 Remote-ID 选项创建会话分组。

IP 边缘设备必须支持根据从 DHCP 获取的 DHCPv6 Interface-ID 和 Remote-ID 选项信息分组 IPv4 和 IPv6 会话。

当 IP 边缘获知某个共享的 DHCPv6 Interface-ID 和 Remote-ID 选项, IP 边缘必须支持根据会话协议类型分组会话的能力, 例如 IPv4 的会话或者 IPv6 的会话。

6.3 IPv6 会话监控

会话监控的主要目的是优化资源的使用和为用户的会话状态提供一个精确的描述。OAM 功能不是监控的主要目的，会话监控是传输网络 OAM 功能上的一个潜在的能力。

没有一个严格捆绑的通用控制协议可以监控 IPv6 会话的存在，需要引入某些机制执行会话健康检查或保活功能。

这样的机制也有助于会话保活失败情况下确保 IPv6 会话的终止。这样既可以保护 IP 边缘设备的资源，也有利于防止欺骗性的攻击。理想的健康检查机制需要执行下面的需求：

- a) 被 RGs 和/或终端用户主机广泛支持
- b) 与会话的发起和探测方法无关。
- c) 和 IPv6 寻址方法（静态或动态）无关。
- d) 和传输协议或拓扑（例如 ATM 或以太网）无关。
- e) 能够容忍有限的丢包。
- f) 应为操作人员可配置的探测间隔，范围从秒到分钟（或更长）
- g) 可以触发需要的机制。
- h) IP 边缘节点和目标用户间的任何中间设备都能允许该机制的报文通过。

符合上述多项条件的机制可分为如下三类，并可组合到一起。

- 监控常规用户会话的流量，操作空闲定时器
- 使用主动协议作为监控检查机制。
- 使用链路层状态信息和 OAM 机制。

不管会话监控报文是否被处理，在发送完预配置数量的保活报文后，如果没有收到来自用户的回应，则 IP 边缘就为会话产生一个会话失效事件。根据定义的策略执行会话失效处理，例如撤销会话，解除会话相关的所有业务。

当 IP 边缘设备发送保活请求并接收到对端的回应时，在 IP 边缘上要设置两个定时器。一个定时器用于发送请求报文，另一个用于接收回应报文。处理过程如图 2 描述。

在图 2 中，定时器 1 代表发送保活请求的定时器。每次定时器 1 超时后，IP 边缘设备发送一个保活请求。定时器 2 代表等待客户端回应的定时器。如果在定时器 2 到期前接收到期望的回应，IP 边缘设备认为客户端在线。如果定时器 2 超时后没有收到期望的回应，则 IP 边缘认为客户端离线并触发对应的事件。为了避免由于报文丢失引起的误判，IP 边缘设备在认定客户端掉线前应该进行重试。图 2 中 IP 边缘连续三次没有收到回应后才终止 IPv6 会话。

尽管两个定时器可以简化成一个，但两个定时器更具有灵活性，更适合使用。定时器 2 的超时时间应较短，这样在考虑到网络延迟情况下能更精确地记录用户离线时间。而定时器 1 的超时时间应比较长，以便降低网络负担，尤其在 IP 边缘设备下有很多用户的情况下；同时确保适当的用户离线误差。

根据上述描述，有如下需求：

- 每个会话发送保活报文的频率应该是以每用户为基础可配置的。
- 每个会话的回应报文超时时间应该是以每用户为基础可配置的。
- 当保活失败时 IP 边缘设备必须支持终止会话的配置。
- 当保活失败时 IP 边缘设备必须支持禁用会话状态的配置。

- IP 边缘节点必须支持 NUD 用于 IPv6 被动会话监控。
- RG 必须支持 NUD 用于 IPv6 被动会话监控。

6.3.2 BFD 协议保活

BFD 保活协议是用于 IP 边缘和 RG/STB 间的。BFD 承载在 IP/UDP 协议之上，并具有如下的优越性。

- 不依赖 VLAN 架构，且对所有链路层协议透明。
- 探测间隔时间可变，且能够动态配置并随流量情况调整。
- BFD 探测由事件来驱动（命令模式）时，可以单向或者双向关闭定期 Poll。
- 如果 RG 并不关心连通性，BFD 回应功能允许单侧维护 BFD 会话的状态。此时对端设备只需在转发层面将 BFD 报文发回。
- BFD 设计了高速的保活消息并有良好的扩展性。
- BFD 支持认证选项，可以防止 DoS 攻击。
- BFD 独立于 DHCP，因此也同样适用于其他场景，如静态 IPv6 等。

具有路由功能的 RG 的 IPv4 和 IPv6 家庭网络有很大不同。在 IPv4 的家庭网络中，三层的 RG 在 WAN 接口有一个公网 IP 地址并且具有 NAT 功能，家庭网络的终端获取私有的 IPv4 地址。IPv4 用户可以和公网 IP 地址捆绑在一起。在 IPv6 的家庭网络中，如果 RG WAN 接口是 unnumbered 模式的，则 WAN 接口没有全局单播地址；每个终端都可获取一个全局单播地址。具有路由功能的 RG 通过 DHCP-PD 获取 IPv6 前缀。用户信息和前缀捆绑，IPv6 前缀信息可以标识一个用户。采用 IPv6 前缀作为 IPv6 会话标识具有以下优势：

- 用户和前缀存在严格的捆绑信息，授权的用户才能获取前缀。
- 前缀作为会话标识管理方便，并且不会产生 IPv6 地址作为会话标识导致的扩展性问题。
- 会话保活机制简单，一个会话保活可以保证当前会话下所有设备可用。
- 会话管理（认证，授权，计费等）方便，根据前缀或用户信息下发策略和配置信息。
- 适用于不同粒度的会话，不同前缀可以代表不同业务或家庭网络的分区。

在 IPv6 的家庭网络中，具有路由功能的 RG 可能由于获取的前缀丢失或 RG 的 LAN 接口故障等原因导致用户设备不能访问网络。

当 RG 和 IP 边缘设备采用 BFD 保活时，分两种情况考虑：

- 如果 RG 为 Numbered 模式，WAN 接口除了有 LLA，还有一个通过 DHCP-PD 获取的前缀生成的 GUA，则 RG 和 IP 边缘的保活可以探测到前缀丢失。
- 如果 RG 为 Unnumbered 模式，则 WAN 接口只有 LLA，RG 和 IP 边缘设备的 BFD 保活机制不能探测到前缀丢失。如果此时 RG 的管理地址（Loopback address）是根据委派的前缀生成，则 BFD 探测在 loopback 地址和 IP 边缘的地址间进行，能够探测到前缀丢失。

IP 边缘和 RG 的 BFD 保活需求可参考 YDB 043-2010《IPv4 用户会话技术规范》中的 IP 边缘的 BFD 保活需求和 RG 的 BFD 保活需求。

如果 RG 的 loopback 地址生成和委派的前缀无关，则 RG 和 IP 边缘的保活机制不能探测到前缀丢失和 LAN 接口失效的问题。这时候需要用户设备和 IP 边缘间的 IPv6 保活机制。由于 RG 是路由设备，所以用户主机和 IP 边缘间的保活是一种多段的保活机制。由于新的终端主机可以支持 BFD 协议，所以终端主机和 IP 边缘设备的保活可采用 BFD 保活。

为了简化会话管理和保活信息，IPv6 会话需要会话鉴别值（discriminator）来标识会话。会话鉴别值可以是 IPv6 前缀或一个能够标识前缀信息的值。

图 3 为 IPv6 的多段保活机制，其中 x 为会话鉴别值，用于标识一个 IPv6 会话。

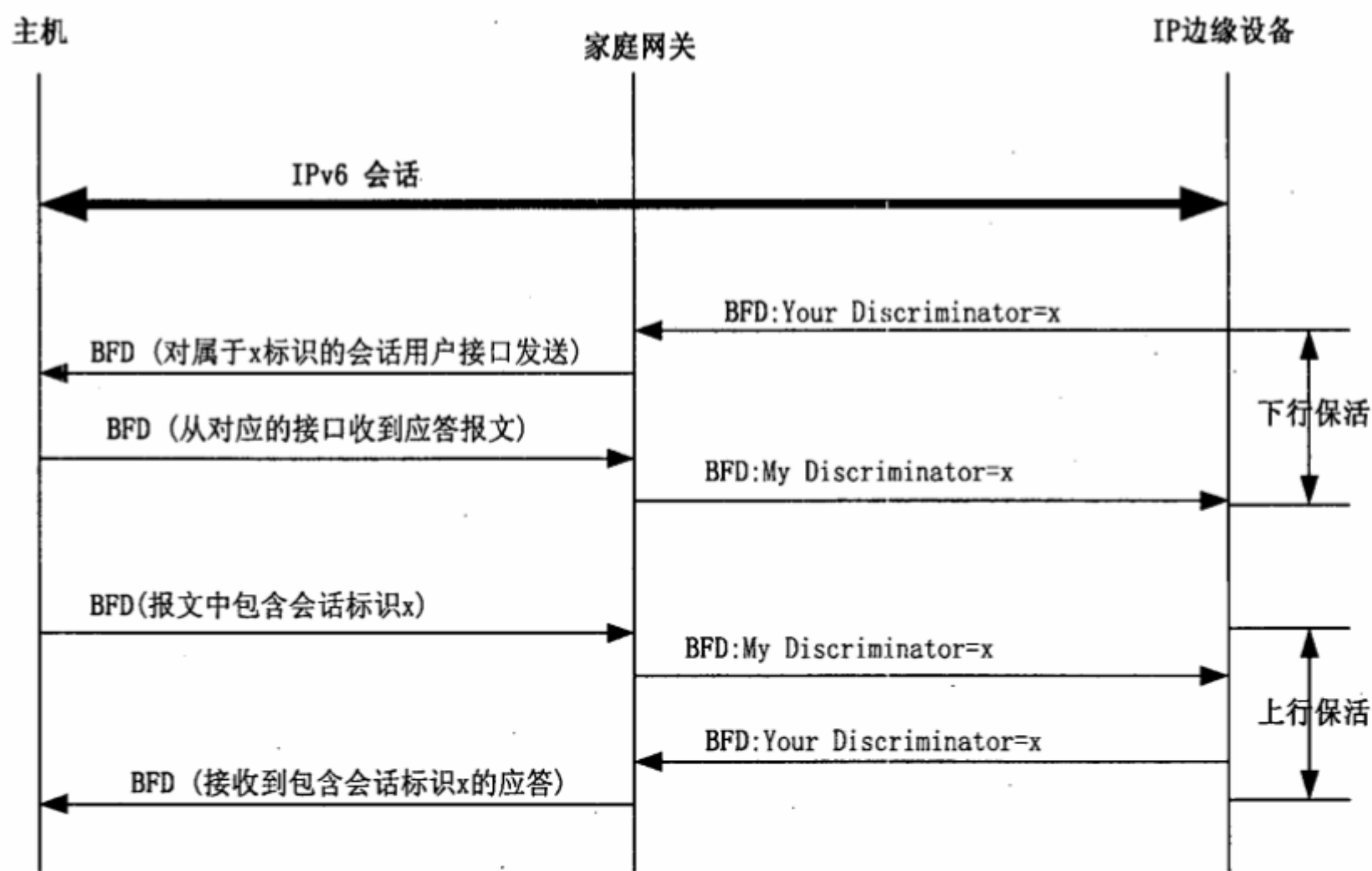


图 3 IPv6 的多段保活机制

在下行的保活过程中，当 IP 边缘设备发送一个 Discriminator 字段设置为 x 的 BFD 报文给 RG 后，RG 根据 BFD 报文中的 Discriminator 字段值，确定需要保活的前缀信息。IP 边缘设备向根据该前缀生成 GUA 的主机发送 BFD 报文，可以探测网络中是否有 IPv6 设备可用。如果从某个端口接收到 IPv6 终端设备的 BFD 应答报文，则表明有用户设备可以使用当前的前缀信息，则 RG 构建一个 BFD 报文并将 Discriminator 字段设置为 x 发送给 IP 边缘设备，表明会话处于存活状态。如果 RG 没有收到终端的应答，则表明终端不可访问网络或用户下线。此时 RG 回复一个带有诊断码信息的 BFD 报文给 IP 边缘设备。

在上行的保活过程中，用户终端发送 BFD 报文给 RG 或 IP 边缘设备，报文中可以隐式地包含会话标识，如 IPv6 源地址。家庭网关根据 BFD 的会话标识信息或保存的用户信息识别出该用户会话所属前缀。RG 根据前缀信息发送 Discriminator 字段设置为 x 的 BFD 报文到 IP 边缘设备，IP 边缘查看该前缀所对应的网络和业务信息，如果可用，则 IP 边缘回复一个 BFD 报文到家庭网关。RG 接收到 BFD 报文则认为网络可用，则从对应的接口回复 BFD 报文给对应的用户终端。

根据上述内容，可以得到如下需求：

- 用户终端设备应该支持双向转发检测机制的 IPv6 会话保活；
- RG 必须支持双向转发检测报文包含鉴别值或隐式的鉴别值（如源 IPv6 地址）信息，并根据双向转发检测报文中的第一鉴别字段值，监控 IP 边缘节点与用户终端之间的 IPv6 会话是否存活；
- RG 必须支持会话保活代理功能，会话保活代理根据前缀或会话鉴别值关联两侧的会话保活机制并更改会话的鉴别值信息，使 RG 两侧可以根据需要使用不同的会话监控机制；
- RG 必须支持双向转发检测报文中携带诊断码信息，通知会话的不同状态信息；
- IP 边缘设备必须支持支持双向转发检测报文包含鉴别值或隐式的鉴别值（如源 IPv6 地址）信息，

并根据双向转发检测报文中的第一鉴别字段值，监控 IP 边缘节点与用户终端之间的 IPv6 会话是否存活；

- IP 边缘设备必须支持双向转发检测报文中携带诊断码信息，根据不同的诊断码进行相应的处理。

6.3.3 基于组播的保活

在 IPv6 网络中，每个 IPv6 终端可以获取一个 GUA。如果采用 IPv6 地址标识每个 IPv6 会话，则 BNG 需要维护很多 IPv6 会话状态。在 IPv6 设备不支持 BFD 会话的情况下，IPv6 会话可以利用已有的技术机制达到保活的目的，MLD 协议就是这样一种 IPv6 保活机制。选择 MLD 作为保活机制具有以下优点：

- MLD 协议被 IPv6 节点和终端广泛支持；
- 具有 MLD 代理和探听功能的设备保存有组播接收者的状态；
- MLD 代理设备的状态维护可以把 IP 边缘设备从维护大量的会话终端信息中解放出来，从而提高了系统的扩展性。

MLD 的保活原理，如图 4 所示。针对某组用户，在系统中需要配置某个特定组播组，需要保活的会话下所有设备都加入到该组播组中。接入节点作为 MLD 的代理功能，保存用户终端设备（主机）的状态信息。

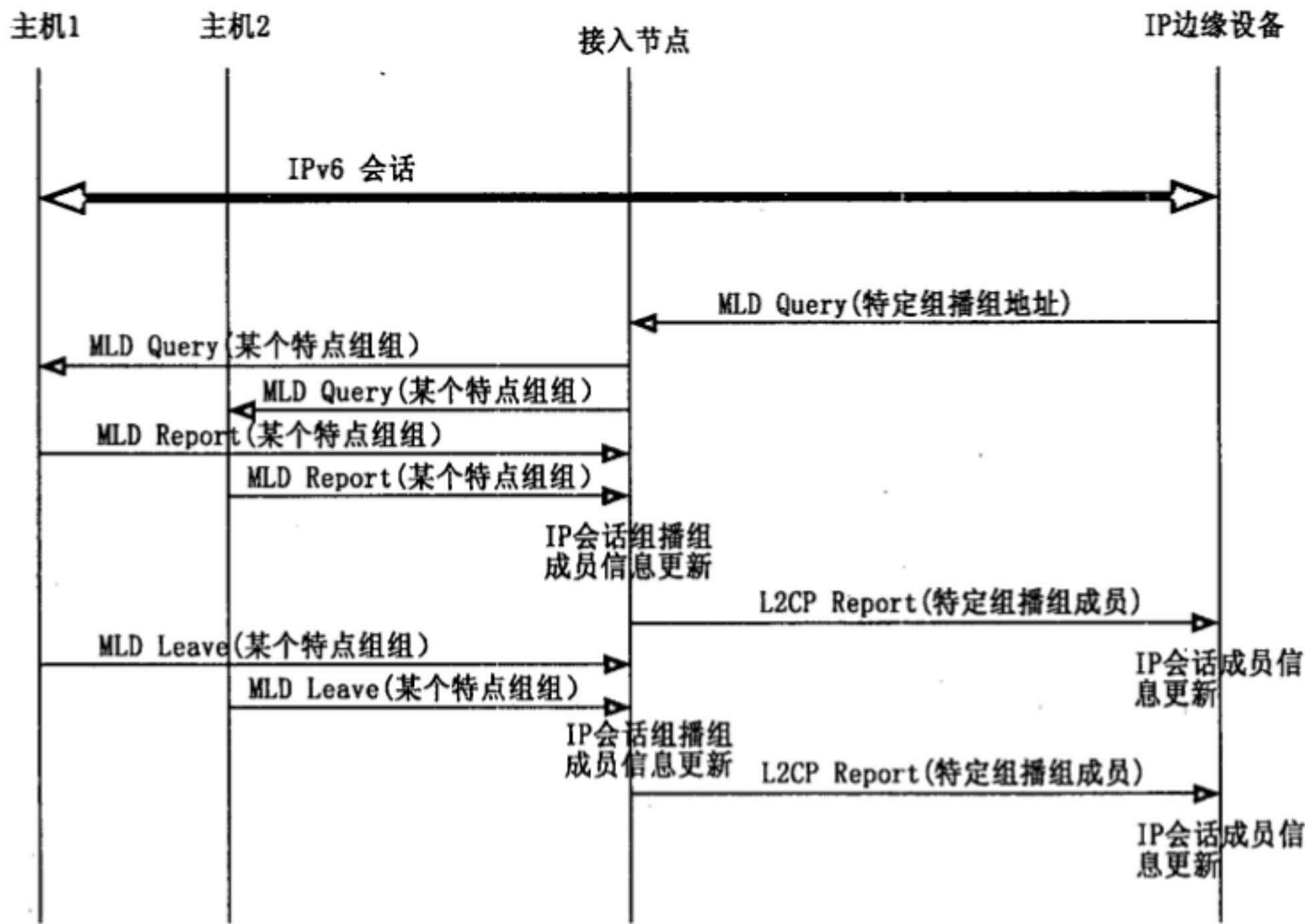


图 4 MLD 保活机制

当接入节点接收到来自 IP 边缘对某个组播组的查询请求时，它对该会话下所有的设备发送这个特点组播组的 MLD 查询报文。当收到对应主机设备的 MLD 报告报文后，接入节点更新本地保存的组播组成员信息。接入节点采用 L2CP 上报组播组成员信息给 IP 边缘设备。IP 边缘设备根据 L2C 的组播成员信息更新本地的会话成员信息。

当接入节点从下行接口接收到来自用户终端设备的 MLD 离开报文后，更新本地的组播组成员信息。接入节点在合适的时机采用 L2CP 上报这个特定组播组的成员给 IP 边缘。IP 边缘设备根据 L2CP 的特定组播组成员信息更新本地的会话成员信息。

当用户终端设备和 IP 边缘设备间采用 MLD 作为保活协议时，如果中间没有 MLD proxy 设备，则由 IP 边缘保存用户终端的信息。

根据上面的保活原理可以得到如下需求:

IP 边缘设备需要支持 MLD 的保活机制, 发送 MLD 查询报文, 确定 IPv6 会话是否存活;

IP 边缘设备需要支持接收和存储 L2CP 上报的用户状态信息并进行处理。

接入节点作为 MLD proxy 设备, 需要根据用户终端的报告报文保存状态用户终端的状态信息, 并实时上报状态信息给 IP 边缘。

接入节点作为 MLD proxy 设备需要根据 IP 边缘的 MLD query 报文, 向用户终端发送包含组播组地址的查询报文, 查询会话组播组的成员信息, 并采用 L2CP 报告的方式反馈查询结果信息。

接入节点作为 MLD proxy 设备需要支持用户终端发送的离开报文, 并根据报文更新用户状态信息。

6.4 会话的流量策略

会话的流量策略决定了 IPv6 会话的流量处理方式, 通常这些策略是直接面向提供给用户的网络服务的。比如简单的策略会把所有未经授权的会话的流量全部丢弃, 而转发所有经过授权的会话的流量。流量策略可应用于用户会话。IP 边缘设备需要支持更具体的流量策略。

一个 IPv6 流通过流分类器定义, 并且视条件用作会话流策略的组成要素。策略动作是通过 IP 流分类的用户会话流量的子集。这些动作从 IP 边缘设备支持的流量动作中得出, 例如管制、丢弃。一个流量策略对基于用户会话相关的全部网络业务来说, 应当是激活的/有具体例子说明的, 例如到目的地 XYZ 的 UDP 包被管制为 64kbps。

多个用户会话可共用同一个流策略定义, 但每个策略仅在其会话场景中生效, 也就是说流量策略并不与共用同一 IPv6 流分类器的用户会话结合。

7 IPv6 会话用户认证模式

为鉴别 IPv6 会话的用户, 需要一个清晰的模型和协议以及必需的协议扩展。理想情况下, 这样一个模型允许服务提供商使用最少的机制在一个支持 IPv6 会话的网络节点上鉴别用户。

IPv6 与 IPv4 的一个重要区别是 IPv6 可以进行无状态地址分配。当采用无状态地址分配时, IPv6 会话的用户认证需要特别考虑。此外, IPv6 用户会话采用的认证方式也存在多种选择, 例如 DHCP 方式或者 PANA 方式。地址分配和认证如何结合, 会影响认证方法和流程的选择。考虑到这些因素, 有如下几种认证方法。

7.1 基于 DHCP 的认证

IPv6 可以采用无状态地址分配, 在选择使用 DHCP 方式进行用户认证时, IP 边缘设备作为 DHCP 代理或服务器, 通过 IETF RFC 3748 定义的 EAP 消息实现用户认证。用户终端作为 DHCP 客户端, 触发 EAP 认证, 并通过承载在 DHCPv6 协议上的 EAP 消息与作为 DHCP 代理或服务器的 IP 边缘设备进行 EAP 消息交互, 完成认证。认证成功后, 用户终端接收 DHCP 代理或服务器通过无状态地址分配方式为其分配 IPv6 地址, 利用分配的 IPv6 地址访问网络, 如图 5 所示。

根据上述内容, 得出如下要求:

作为 DHCP 代理或 DHCP 服务器时, IP 边缘设备必须支持将 EAP 消息承载于 DHCPv6 协议上, IP 边缘设备利用该消息与用户终端进行交互执行认证功能。

用户终端必须支持 EAP 消息承载于 DHCPv6 协议上, 与 IP 边缘设备进行消息交互。

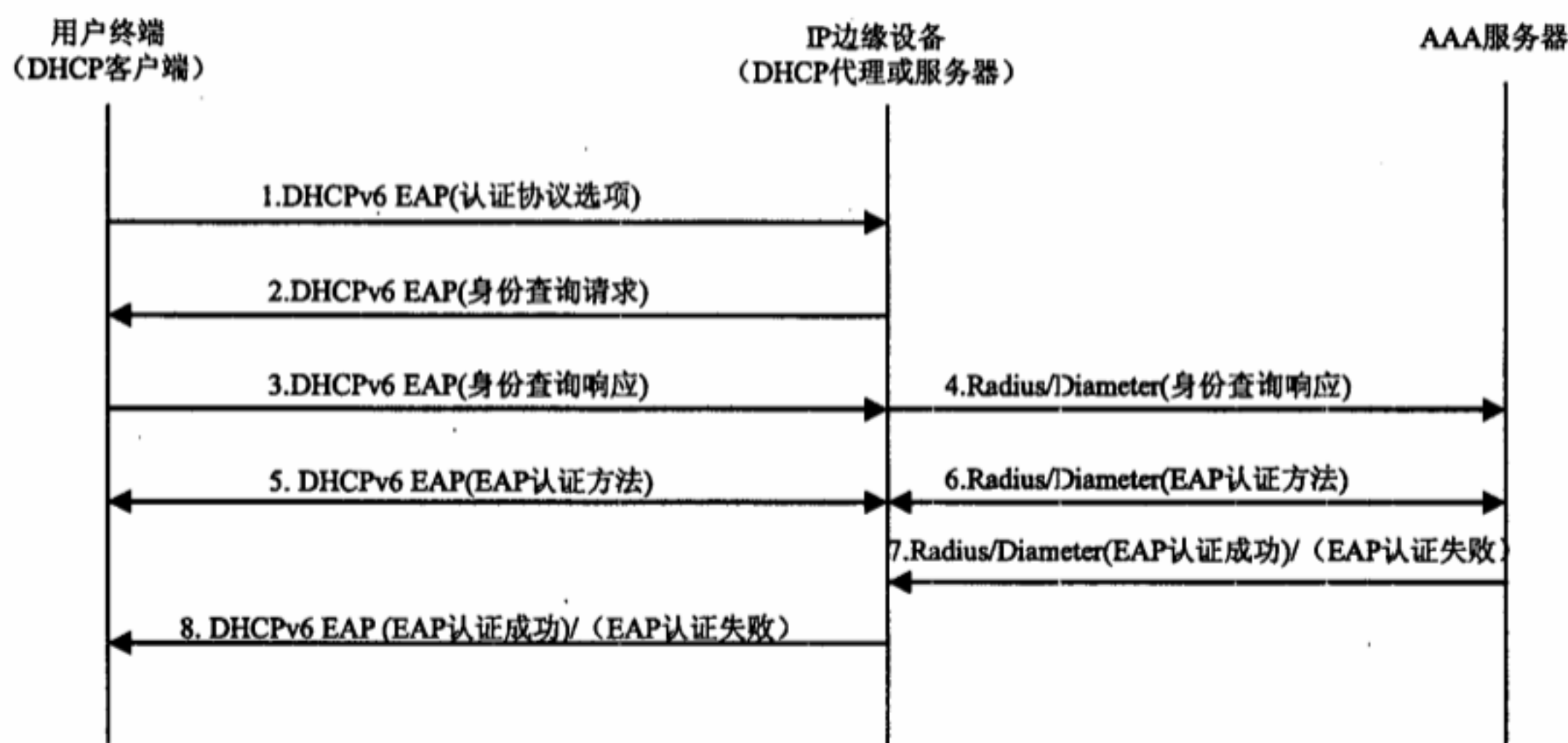


图 5 SLAAC 情况下采用 DHCP 认证

认证成功后分配地址时，可以采用无状态 IPv6 地址分配的技术，比如：链路-局部地址 LLA 自动配置和全局 IPv6 地址自动配置，通常采用 IPv6 邻居发现协议实现；也可以采用有状态 IPv6 地址分配方式为 DHCP 客户端分配 IPv6 地址。

认证成功后，IP 边缘设备必须支持通过无状态地址分配方式为用户终端分配 IPv6 地址，供用户用于访问 IPv6 网络。

认证成功后，IP 边缘设备还可支持通过全球 IPv6 地址自动配置方式或有状态 IPv6 地址分配方式为用户终端分配 IPv6 地址，供用户用于访问 IPv6 网络。

7.2 基于 PANA 的认证

IPv6 用户接入 IPv6 网络，可采用 PANA 认证方式，这种方式不分配地址，在 IPv6 网络中，用户终端的 IPv6 地址/前缀一般由家庭网关分配，若家庭网关是不支持 NAT 的路由器，IP 边缘节点通常不知道用户终端的 IPv6 地址/前缀。而为便于管理，IP 边缘设备需要知道 IPv6 用户会话的用户终端的 IPv6 地址或前缀。为此，用户终端与认证服务器进行消息交互时，可在认证过程中将分配得到的用于数据通信的 IPv6 地址信息通过认证消息发送给 IP 边缘节点，使 IP 边缘节点获取用户终端的 IPv6 地址信息。这样，家庭网关后面的用户上的 IPv6 会话可以穿越家庭网关，使用户的 IPv6 地址/前缀为 IP 边缘节点所感知，便于 IP 边缘设备对 IPv6 会话进行管理。

IPv6 用户进行 PANA 认证的网络示意图如图 6 所示，家庭网关为三层路由器，可集成 DHCP 服务器或无状态地址自动分配 SLAAC 路由器，支持 PANA 认证中转(Relay)和 PANA 认证监听，IP 边缘设备支持 DHCP-PD 监听并担任 PANA 认证的认证者 (Authenticator)，用户终端为 PANA 客户端。IPv6 会话建立在用户终端（特别是游牧用户）和宽带网络网关之间。

家庭网关 RG 的地址前缀为 56 位，用户终端的地址前缀为 64 位。家庭网关通过 DHCP-PD 申请得到 IPv6 地址前缀。在认证之前，家庭网关为其后的用户终端分配专门用于用户认证的 IPv6 地址前缀，并用此前缀生成全局 IPv6 地址进行用户认证。RG 在用户终端和 IP 边缘设备之间中转 PANA 认证消息。用户认证成功后，家庭网关为用户终端分配用于用户认证后数据通信的 IPv6 地址/前缀，如图 7 所示。

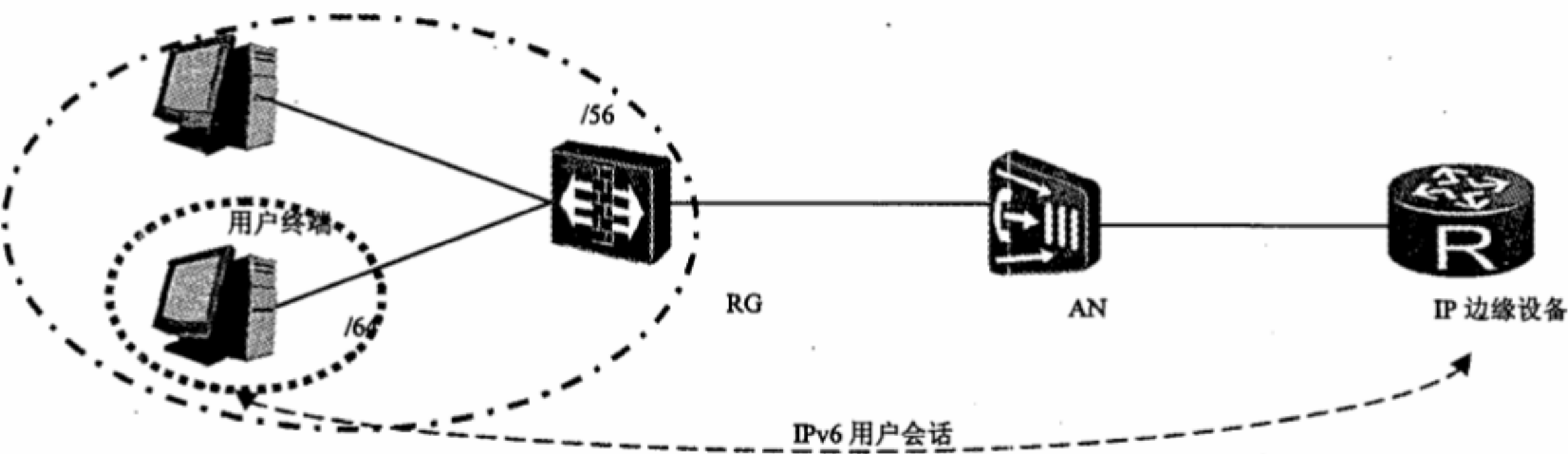


图 6 IPv6 用户进行 PANA 认证的网络示意图

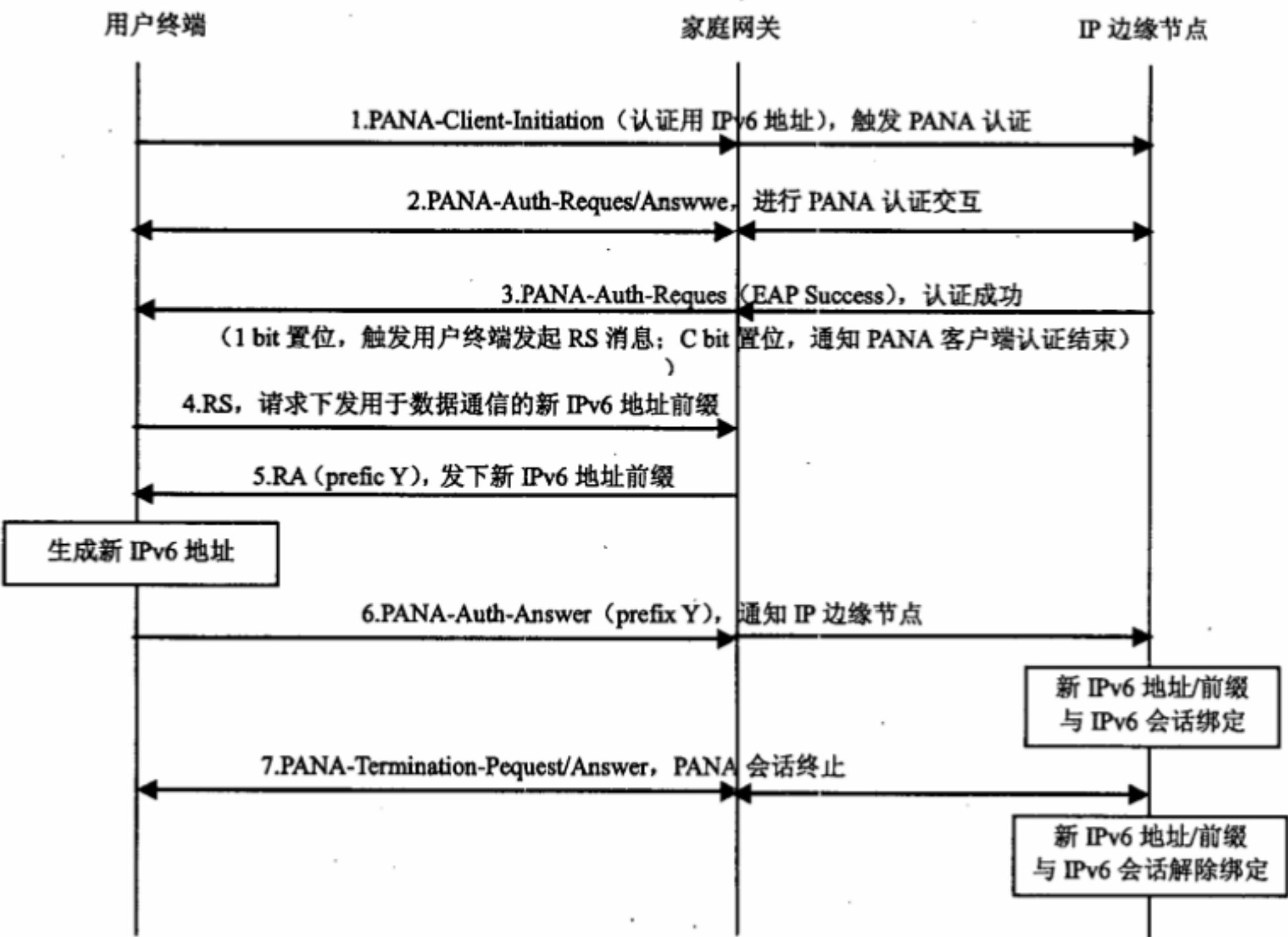


图 7 PANA 认证方式下的 IPv6 用户会话认证

认证成功后，家庭网关为用户终端分配用于数据通信的 IPv6 地址，除采用通过路由器通告方式外，还可采用 DHCP 方式或 DHCP-PD 方式进行分配。IP 边缘设备接收到家庭网关为用户终端分配的用于数据通信的 IPv6 地址信息后，将该 IPv6 地址信息与对应的用户终端 IPv6 会话绑定。当会话终止时，IP 边缘设备为 IPv6 用户会话解除对应的绑定关系。

- 根据上述内容，得出各网元的要求如下：
- IP 边缘设备必须支持充当 PANA 认证的认证者（Authenticator）并必须支持 DHCP-PD 监听。
 - IP 边缘设备必须支持接收携带用户终端 IPv6 地址的 PANA 认证消息并从中获得用户终端的 IPv6 地址信息。
 - IP 边缘设备必须支持根据用户 IPv6 地址信息绑定与用户终端之间的 IPv6 会话，并在会话结束后解除对应的绑定关系。
 - RG 必须支持 PANA Relay 和 PANA 认证监听。

RG 必须支持在用户终端向认证服务器认证前，为用户终端分配用于认证的 IPv6 地址前缀。

RG 可以支持无状态地址自动分配 SLAAC 路由器功能。

RG 必须支持通过路由器通告方式、DHCP 方式或者 DHCP-PD 方式为用户终端分配 IPv6 地址，用于数据通信。

用户终端支持将 IPv6 地址信息通过 PANA 认证消息发送给 IP 边缘节点。

7.3 基于 RS 的认证

在无状态地址分配的情况下，用户（RG 或 IPv6 主机）初始化接口时，会向 IP 边缘设备发送 RS 消息，随后可以再发送一个 NS 消息用于重复地址检测，以确认主机的链路-局部地址合法。然后，用户通过 IPv6 SLAAC 机制创建自己的全局 IPv6 地址。之后，RG 或主机收到 RA 消息，获得必要的参数。

在这个过程中，RS 可以看作是接入网络的请求消息，而 RA 可以看作对该请求的授权。同时，用户的前缀也分发下来。这一过程类似于 IPv4 中的 DHCP 创建用户会话。之后，类似于 option 82，IPv6 可以根据用户的接入线路信息对用户进行隐式认证，识别用户并进行授权。

RG/用户主机访问网络过程中，接入节点 AN 接收到用户设备发送的包含链路-局部地址 LLA 的请求消息之后，从中获取与用户设备对应的用户接入线路 ID，并将其插入 RS 消息，发送给 IP 边缘设备。IP 边缘设备继而携带此接入线路 ID 向 AAA 服务器发送消息，对用户进行认证和授权。

认证成功后，IP 边缘设备为用户分配必要的服务参数，包括前缀、配置信息等。

根据上述内容，得出如下规定：

IP 边缘设备必须支持接收接入节点发送的包含用户线路信息的路由请求消息，并从中获取用户线路信息。

IP 边缘设备必须支持根据从路由请求消息中获得的用户线路信息，向 AAA 服务器发起接入请求，对用户进行认证和授权。

IP 边缘设备必须支持向用户设备发送包含用户线路信息的路由通告消息，或通过接入节点向用户设备发送包含用户线路信息的路由通告消息。

接入节点必须支持接收用户设备发送的包含 LLA 的路由请求消息，根据 LLA 获取用户设备对应的用户线路信息。

接入节点必须支持向 IP 边缘设备发送包含用户线路信息的路由请求消息，用于 IP 边缘设备对用户设备进行接入认证。

附录 A
(规范性附录)

IP 会话创建和认证的用例

本附录提供的信息详细说明涉及 IPv6 会话和流量策略的用例和消息流。

A.1 动态 IPv6 会话

DHCPv6 触发的会话开始和前缀分配

IP 边缘节点在接收到用户发出的 DHCPv6 报文后，可以取得授权一个用户的充分信息。同 IPv4 的例子，DHCPv6 允许利用用户标识（也就是接入线标识）和那些包含在 ICMPv6 或规则的 IPv6 报文中的信息。尽管需要类似 DHCPv6 接入线路标识一样的方法还需要标准化，一个用户发起的路由请求报文也可以用于标识用户和授权用户。

授权完成后并且 IP 边缘为用户分发了需要的业务参数，如 IP 地址/前缀，可以使用 DHCPv6 继续进行分发过程。除此之外，如果它期望通过 SLAAC 方式指定前缀给 RG 或主机，IP 边缘可以发送路由通告报文给用户并携带一个来自 AAA 的前缀项给用户。在 N:1 VLAN 的场景下，这样的路由通告报文要由 IP 边缘单播给用户，否则通过组播发送。寻址机制和 PPP 基础的接入情况下的相同，并且具有简化操作和问题定位的优点。而且，它不论客户端是路由的 RG 还是直连的终端主机都保持相同。

当 SLAAC 寻址不使用的情况下，这个机制也不排除使用。例如当客户端希望通过有状态的 DHCPv6 获取 IPv6 地址时，组播的路由通告报文的用户的前缀信息被忽略掉。

上面的一系列描述可以通过图 A.1 的流程说明。注意流程是通过 DHCP SOLICIT 驱动的例子，任何 DHCP 客户端发起的报文，只要提供了线路标识信息都可以用于发起会话。

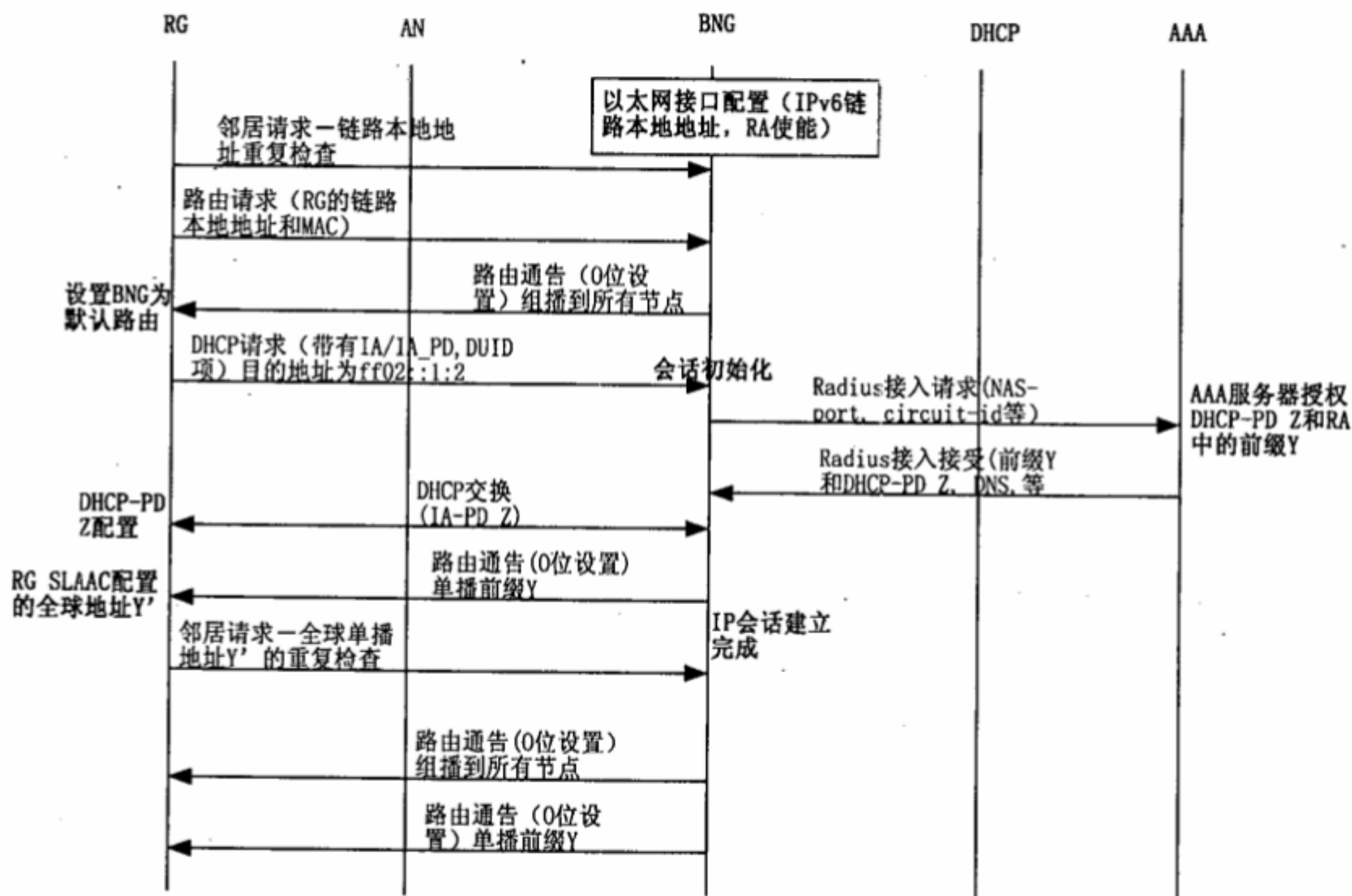


图 A.1 DHCPv6 触发的会话开始和前缀分配过程

会话的创建和使用单播的路由通告报文使终端通过 SLAAC 获取主机地址是完全和 IETF RFC4861 和 IETF RFC3315 兼容的。注意到会话创建的顺序，和 AAA 的交互过程是和 PPP 的情况等同的。这就允许了操作员使用同样的 AAA 节属性并进行 PPP 相同的 IPv6 会话接入。

注：邻居请求的重复地址探测（DAD）是可选的。分配前缀给 WAN 接口也是可选的。所有 BNG 和外部服务器的协议交互也是可选的，并且只是作为例子说明。

参 考 文 献

[1]	IETF draft-ietf-bfd-base-11	双向转发检测（BFD）
[2]	IETF draft-ietf-bfd-v4v6-1hop-11	IPv4 和 IPv6 的 BFD
[3]	IETF RFC 3046	DHCP 中继代理信息选项协议（DHCP option 82）
[4]	IETF RFC 4014	DHCP 中继代理信息选项的 RADIUS 属性子选项
[5]	YDB 043-2010	IPv4 用户会话技术规范

中华人民共和国
通信行业标准
IPv6 用户会话技术要求
YD/T 2297-2011

*

人民邮电出版社出版发行
北京市崇文区夕照寺街 14 号 A 座
邮政编码: 100061
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 2012 年 1 月第 1 版
印张: 2 2012 年 1 月北京第 1 次印刷
字数: 48 千字

ISBN 978 - 7 - 115 - 2336/ 11 - 287

定价: 20 元

本书如有印装质量问题, 请与本社联系 电话: (010)67114922