

ICS 33 040
M 33

YD

中华人民共和国通信行业标准

YD/T 1616-2007

IP 组播业务技术要求

Technical Requirements for IP Multicast Service

2007-04-16 发布

2007-10-01 实施

中华人民共和国信息产业部 发布

目 次

前 言..... II

1 范围..... 1

2 规范性引用文件..... 1

3 定义和缩略语..... 1

4 IP组播业务类型..... 2

5 IP组播网络的组网要求..... 3

6 IP组播业务的控制模型..... 5

7 IP组播业务的控制要求..... 6

8 IP组播业务的管理模式..... 10

9 IP组播业务的性能要求..... 12

10 IP组播业务的监控要求..... 12

附录A（规范性附录） 用于组播认证的RADIUS扩展属性..... 16

参考文献..... 17

前 言

本标准是“IP 组播”系列标准之一。该系列标准的名称及结构预计如下：

- 1. YD/T1177-2002 IP 组播路由协议
- 2. IP 组播业务技术要求

本标准的附录 A 为规范性附录。

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：华为技术有限公司

本标准参加单位：中国电信集团公司

中兴通讯股份有限公司

上海贝尔阿尔卡特股份有限公司

本标准主要起草人：刘恩慧 钟 凯 徐 岗 郭 锋 张海涛 钱 浩 管红光 鲁林丽

IP 组播业务技术要求

1 范围

本标准规定了在IPv4网络上运营组播业务的技术要求,包括IP组播业务的控制模型、方法和一般原则,还规定了IP组播网络的组网和配置要求、IP组播业务的认证、控制、管理、性能和监控要求。

本标准适用于应用IP组播技术传送数据的公众运营业务。

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。

YD/T 1177-2002	IP组播路由协议
IETF RFC 2865 (2000)	远程认证拨入用户服务协议

3 定义和缩略语

下列定义和缩略语适用于本标准。

3.1 定义

IP 组播网络 (IP Multicast Network) IP 组播网络是指支持 IP 组播技术及其应用的 IP 网络。

IP 组播业务 (IP Multicast Service) IP 组播业务是指应用 IP 组播技术传送数据的各种应用。

组播泛滥 (Multicast Diffusion) 组播泛滥指未加入组播组的主机或网络设备在二层或三层接收到了发往该组播组的信息包,引发信息安全和主机资源浪费等问题。

用户接入认证 (User Access Authentication) 用户接入认证是指对用户接入网络的权限在本地或者远程认证。

用户组播认证 (User Multicast Authentication) 用户组播认证是指对用户加入组播组的权限在本地或者远程认证。

组播 VLAN (Multicast VLAN) 基于 IEEE802.1Q 标准对以太网端口进行 VLAN 划分,以保证不同组播组的流量在二层相互隔离。一个 VLAN 可以包含一个组播组或多个组播组,该 VLAN 的 ID (TAG) 可用于识别组播组流量。

用户 VLAN (User VLAN) 基于 IEEE802.1Q 标准对以太网端口进行 VLAN 划分,以保证不同用户的流量在二层相互隔离。一个 VLAN 可以包含一个用户或多个用户,该 VLAN 的 ID (TAG) 可用于识别用户流量。

3.2 缩略语

ACL	Access Control List	访问控制列表
AS	Autonomous System	自治系统
ASM	Any Source Multicast	任意源组播

BRAS	Broadband Remote Access Server	宽带接入服务器
BSR	BootStrap Router	自举路由器
CAR	Committed Access Rate	接入速率限制
DiffServ	Differentiated Service	有差别服务
DoS	Deny of Service	拒绝服务
DSLAM	Digital Subscriber Line Access Multiplexer	数字用户线接入复用器
DR	Designated Router	指定路由器
IANA	Internet Assigned Numbers Authority	因特网编号分配委员会
IETF	Internet Engineering Task Force	因特网工程师任务组
IGMP	Internet Group Management Protocol	互联网组管理协议
IP	Internet Protocol	互联网协议
MAC	Media Access Control	介质访问控制
MBGP	Multicast Border Gateway Protocol	组播边界网关协议
MIB	Management Information Base	管理信息库
MSDP	Multicast Source Discovery Protocol	组播源发现协议
PIM-SM	Protocol Independent Multicast-Sparse Mode	协议无关组播-稀疏模式
PPP	Point-to-Point Protocol	点到点协议
QoS	Quality of Service	服务质量
RADIUS	Remote Authentication Dial In User Service	远程认证拨号用户服务
RP	Rendezvous Point	汇集点
SA	Source Active	“源有效”报文
SLA	Service Level Agreement	服务等级协定
SPT	Shortest Path Tree	最短路径树
SSM	Source-Specific Multicast	源特定组播
TCP	Transport Control Protocol	传输控制协议
VLAN	Virtual Local Area Network	虚拟局域网
VPN	Virtual Private Network	虚拟专用网

4 IP 组播业务类型

IP组播技术能使主机发送IP信息包到IP网络中任何一组主机上。这组主机用一个IP组播地址标识。主机只需发送一份组播数据流，组内的主机都能收到。IP组播技术实现了网络中点到多点的高效数据传送，能够有效地节约带宽，降低网络设备负载和服务器负载。

IP组播技术具有以下基本特征：

- (1) 组播源只负责发送，目的地址为一个组播地址（D类IP地址），组播源可以是或不是组成员；
- (2) 接收者通过向所在子网负责组成员信息查询的网络设备发出申请，加入组播组成为组成员；
- (3) 数据包要发送给所有组成员，只有组成员才能收到数据包；
- (4) 网络设备协同工作，负责将组播数据从发送方传送到所有组成员；
- (5) 组播地址作为对组播组的标识，接收者和组播源之间可以不了解对方的地址，但必须知道组播

地址。

组播技术特别适合流量大、接收者众多的数据传送。在多媒体业务日渐增多的情况下，组播技术有着巨大的市场潜力。目前IP网络上适合应用组播技术的业务主要有：

(1) 音频/视频流发布：演讲、演出和会议等预定的多媒体新闻报道与实况转播。组播信息流包括音频信息和视频信息，其中音频的优先级高于视频信息。

(2) 短消息发布：广告、消息、新闻、天气预报、比赛结果等动态信息发布。

(3) 数据分发：数据库内容、网站内容、文件等采用Push模式可靠地传送到各个网络节点组进行同步更新。

(4) 实时信息发布：股票价格、探测结果（如地震、遥感、气象和海洋监测）、安全系统等实时信息发布。

(5) 多媒体会议：多媒体会议包含音频、视频信息的交互以及电子白板等功能。由于涉及到会议进程控制等问题，因此使业务的开发和应用更为复杂。

(6) 电子白板：允许处于不同地理位置的人共享一个电子白板传递信息。

(7) 远程教学：教学本身是一对多的业务，但系统若允许学生提问，则构成多对多业务。

(8) 聊天组：基于文本的会议系统，但许多业务提供模拟环境，传送每个会话者的“化身”图像。

(9) 多方网络游戏：通过为游戏玩家建立基于IP组播的分布式虚拟环境，提高游戏玩家之间的交互能力和游戏所能接收的最大玩家数量。

从组播源的分布特点划分，上述组播应用主要分为两类：一对多组播和多对多组播。大多数组播业务都是组播源相对固定的一对多组播应用。本标准内容主要针对组播源数量有限且相对固定的一对多和多对多组播应用。对于组播源数量无限且动态变化的多对多组播应用，以后根据需要研究。

5 IP 组播网络的组网要求

IP组播网络是指支持IP组播技术及其应用的IP网络。构建IP组播网络不需要额外增加网络设备，只须现有IP网络设备支持组播标准协议。关于IP组播地址、转发机制和组播标准协议的规定，参见YD/T 1177-2002《IP组播路由协议》（该标准规定了支持IPv4的组播路由协议，包括组成员关系协议、域内组播路由协议及组播路由协议互操作的技术要求）。

IP组播网络建议采用PIM-SM/MSDP/MBGP方式组网，跨域组网模型如图1所示。

城域网和骨干网内部运行PIM-SM协议，建立内部MBGP对等；各城域网和骨干网之间建立外部MBGP对等，RP之间建立外部MSDP对等。对于大的自治域，在域内应当设立多个RP实现负载分担和备份，在备份RP之间应当建立内部MSDP对等，执行Anycast RP机制。MBGP负责在域间交换组播路由信息，MSDP负责在RP之间交换组播源信息。

接收者终端设备必须支持IGMP协议。网络接入服务器必须支持IGMP和PIM-SM协议，或者可以支持IGMP Proxy。网络接入服务器与接收者终端设备之间的所有二层交换设备都应当支持IGMP Snooping或IGMP Proxy，或者本系列标准后续提供的其他可以有效抑制二层网络中组播泛滥问题的二层组播控制协议。

对于只在一个域内应用组播技术的IP网络（一般是一个城域网），域内路由器只须支持PIM-SM协议。在跨域组建组播网络时，骨干路由器还应当支持MBGP和MSDP协议。

PIM-SM/MSDP/MBGP方式具备以下优势：扩展性好；RP之间无须配置隧道，RP点的负担减轻；RP

节点之间运行MBGP和MSDP协议，不存在组播流量定期扩散问题。缺点是会在骨干网中建立大量的组播路由状态，增加骨干网络的不稳定因素。

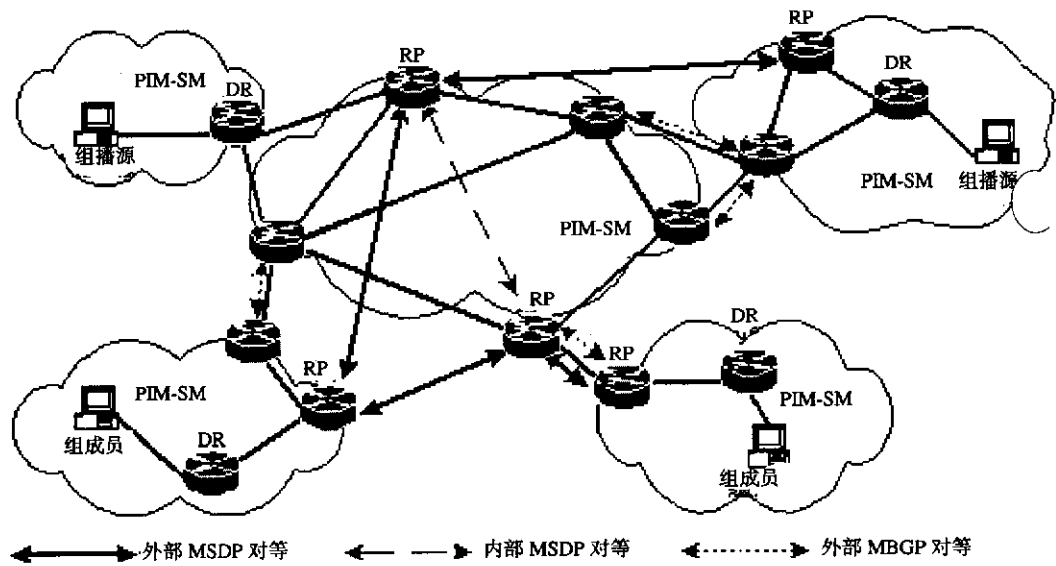


图1 PIM-SM/MSDP/MBGP方式跨域组网模型

在IP骨干网不支持或者不启用组播协议的情况下，可以采用PIM-SM隧道方式作为实现跨域组播的替代组网方案。即：在城域网内部运行PIM-SM协议，各个城域网的RP节点之间通过隧道构成虚拟网络，只在此虚拟网络中运行PIM-SM或者PIM-SM/MBGP/MSDP协议。

如果采用PIM-SM v2协议支持源特定组播模式，则接收者终端设备和所有执行IGMP Snooping、Proxy或终结设备必须支持IGMP v3协议，但跨域组建组播网络时可以不运行MSDP协议。

在图1所示的跨域组网模型中，除了支持组播标准协议的要求外，还应当注意以下组播配置问题。

1. RP的选取和配置

在PIM-SM网络中RP的选取非常重要，直接影响组播路由性能。使用PIM-SM前必须先确定RP的位置。RP在PIM-SM协议中，负责把组播源与接收者联系起来，接收者先通过RP得到组播源信息，再向组播源建立最短路径。

RP和备份RP尽量处于从组播源到接收者的最短路径上，这样即便使用稀疏模式，也不会影响组播路由性能。建议把RP和备份RP放置到最靠近组播源的路由器或以太网三层交换机上。对于大型IP组播网络，静态RP方式不利于维护管理，应当采用自举路由器（BSR）方式自动选取RP。

RP的配置应当注意以下三点：

- （1）将RP宣告范围设置为网络最大直径，使网络中每一台路由器都能接收到RP宣告；
- （2）在网络边界设置过滤器防止本域的RP宣告溢出网络边界而对其他域造成欺骗；
- （3）在网络的RP映射代理中设置进入过滤器，防止其他域的非宣告进入本域。

应当采用Anycast RP机制实现域内RP间的负载均衡和冗余配置，以提高可靠性。

2. 二层交换设备的配置

在接入网环境中由于二层交换设备（包括以太网二层交换机和DSLAM）无法确定哪一个端口有组成员，会引起组播信息广播到二层交换设备的所有端口。为了有效抑制组播在接入网中的泛滥问题，二层交换设备应当支持IGMP Snooping或IGMP Proxy，或者本系列标准后续提供的其他可以有效抑制二层网

络中组播泛滥问题的二层组播控制协议。

应用IGMP Snooping或IGMP Proxy时，二层交换设备必须能够检测IP帧头，监听和解读所有IGMP报文。

6 IP 组播业务的控制模型

基于组播数据流量较大、接收者众多的特点，在IP组播网络上要实现组播业务的运营，必须对组播源和接收者进行严格的管理，控制组播数据的传播方向和范围。否则，开展组播业务不仅会对现有IP网络造成冲击和影响，也不可能为接收者提供预期的业务质量。

IETF定义的IP组播标准协议不涉及组播的控制和管理方面的机制，接收者可以随意加入并可以任意离开一个组播组，运营商不知道接收者何时加入何时退出组，无法统计出某个时间网络上共有多少个组成员在接收组播流量。在网络上的任何用户都可以作为组播源发送组播流量，因此存在非法组播源问题以及组播信息冲突问题。

本标准结合IP网络模型和IP组播技术的特点，在完全符合IP组播标准协议的基础上，规定了IP组播业务的控制模型（如图2所示）和控制机制，使得组播业务可控制可管理可运营。组播业务控制机制包括组播地址分配、组播源控制、组播流量控制、组播接收者控制和组播安全控制。

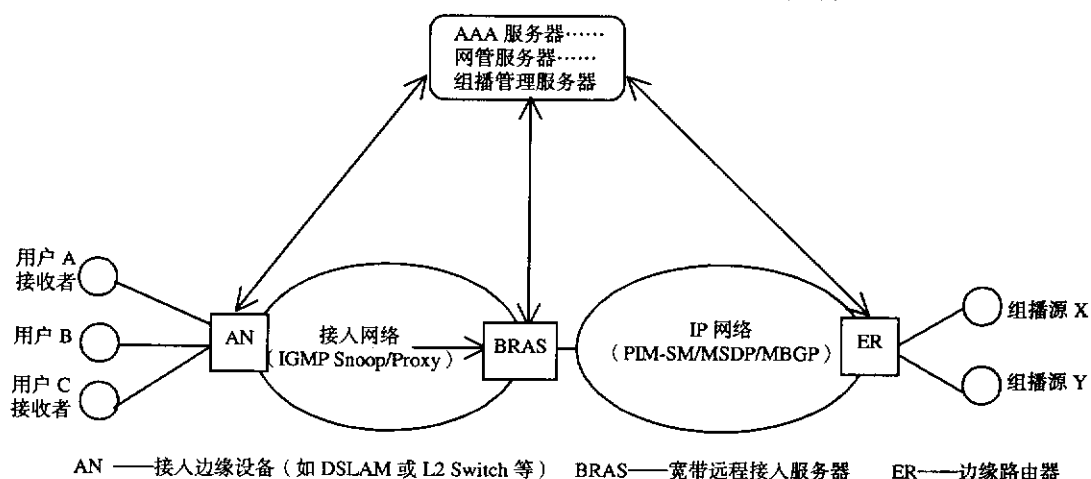


图2 IP组播业务的控制模型

组播业务控制所涉及的认证、授权、计费 and 配置等管理功能，可以分布集成在认证服务器和网管服务器中，也可以集中在一台独立设备上实现（称之为组播管理服务器）。

网络管理员通过网管或命令行在与组播源直接相连的路由器上配置必要的组播源认证、授权和流量控制参数；在与接收者直接相连的接入边缘设备（如DSLAM等）或者接收者的网络接入服务器（即BRAS）上配置必要的接收者认证、授权和流量控制参数。

与组播源直接相连的边缘路由器检测发向网络的组播流，根据本地或远程认证结果控制组播源能否向网络发送组播流，对组播流量丢弃或按流量控制参数转发到网络中。

接入边缘设备或者网络接入服务器检测用户发向网络的IGMP报文，根据本地或远程认证结果控制用户能否加入组播组，对用户抑制或按流量控制参数从网络接收组播组的流量。

接入网二层交换设备应当支持IGMP Snooping或IGMP Proxy，或者其他二层组播控制标准协议，抑制二层网络中的组播泛滥，防止未经授权的用户收到组播流量。

此控制模型主要针对组播源数量有限且相对固定的一对多和多对多组播应用，能够满足以下要求：

- (1) 能够严格控制和记录组播源的组播数据发送、流量及目的组地址；
- (2) 能够严格控制和记录具体接收者加入和离开具体组播组；
- (3) 用户接入认证和用户组播认证可捆绑也可分离，以便接入控制和业务控制分离；
- (4) 认证机制严格可靠并能防伪冒；
- (5) 在网络接入层，二层交换设备应当支持IGMP Snooping或IGMP Proxy，或者其他的二层组播控制标准协议，抑制组播报文在二层网络中的泛滥，隔离接收者以保障组播信息安全；
- (6) 接收者终端设备支持IGMP协议，接入设备能够识别IGMP报文；
- (7) 与现有接入、认证和计费设备能够平滑连接。

在此控制模型基础上，建议IP组播业务管理和监控遵循以下原则：

- (1) 组播业务作为IP网络的增值业务运营；
- (2) 组播源一般为内容提供商；
- (3) 网络运营商建设、维护和管理支持组播的IP网络；
- (4) 内容提供商与网络运营商对组播业务的管理和计费达成授权协议；
- (5) 网络运营商集中管理组播源、接收者用户和组播地址；
- (6) 通过接入边缘设备或者网络接入服务器、认证服务器和网管服务器配合，实现组播源控制、接收者控制和计费数据收集，保证信息安全防止非法组播源；
- (7) 通过状态监控、会话和成员监控、路由和流量监控、协议监控、拓扑和地理位置监控，规划和平衡全网负载和业务，并及时分析、诊断、预防和修复网络错误；
- (8) 通过地址空间监控，合理分配和管理组播地址。

对于多对多的组播业务应用，参考上述原则。

7 IP 组播业务的控制要求

IP组播业务的控制主要包括组播地址分配、组播源控制、组播流量控制、组播接收者控制、组播安全控制等方面。

7.1 组播地址分配

在IGMP v1和v2中，组播地址Gx作为一个组播组的惟一标识（称为任意源组播模式），组播信息流的接收方、发送方之间可以不了解对方的地址，但必须知道组播地址。用户发送IGMP Join (*,Gx)加入组播组Gx，就能收到组播源发送给Gx的信息流。在IGMP v3中，组播地址和源地址的组合（Sx, Gx）作为一个组播组的惟一标识（称为源特定组播模式）。

根据组播应用的情况，目前对IP组播技术需求较多的是组播源数量有限且相对固定的一对多和多对多组播应用，组播源一般是相对固定长期发送组播信息流的内容服务器。因此在实际的组播业务商业化运营中，一个或一组组播源应当被静态分配一个或多个固定的组播地址，发送特定类型的组播信息流；对于其他未来可能逐渐广泛的多对多组播应用，组播源也应当是范围和地址可控的。

网络运营商必须在全网范围内管理组播地址的分配与回收，在一项组播业务申请创建时为其分配特定组播地址，在该业务申请终止时回收所分配的组播地址，保证各种组播信息流不发生冲突。如果要支持跨运营商域的组播业务，则必须由IANA给网络运营商预先分配组播地址范围，以避免网络运营商之间发生组播地址分配冲突问题。

可供分配的用户组播地址范围见图3所示。

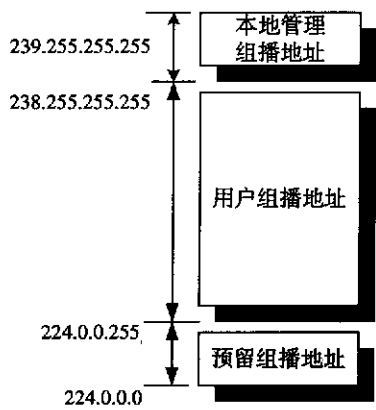


图3 用户组播地址范围

尽管目前IETF已给出了动态组播地址分配协议的相关推荐性或试验性标准，但目前跨域组播业务为数极少。因此，网络运营商近期应当采用静态组播地址分配方法，由人工管理组播地址的分配与回收，保证域内不发生组播地址冲突。随着组播应用的推广以及标准的不断完善，再考虑动态组播地址分配协议。

IANA将MAC地址范围 01:00:5E:00:00:00~01:00:5E:7F:FF:FF分配给组播使用,这就要求将28位的IP组播地址空间映射到23位的MAC组播地址空间中,具体的映射方法是IP组播地址中的低23位放入MAC组播地址的低23位。这样会有32个IP组播地址映射到同一MAC组播地址上。因此在分配IP组播地址时，还应尽量避免多个IP组播地址映射到相同MAC组播地址的冲突问题。

7.2 组播源控制

组播业务创建前，组播源必须向网络运营商进行组播业务申请，包括申请组播源地址、组播地址、带宽、优先级和组播路由。组播业务终止后，组播源必须向网络运营商申请回收组播源地址、组播地址、带宽、优先级和组播路由。

组播业务的创建包括组播业务的发布和组播源的授权。组播源应当准备组播信息流发送端和接收端软件，并将接收端软件公布给用户。

组播业务的发布是指将组播地址与业务的对应关系以及业务类型发布给网络用户。组播业务的发布有以下两种方法：

- (1) 一种是将这些对应关系用一个众所周知的组播地址组播出去，用户主机监听这些组播报文；
- (2) 另一种是将这种对应关系发布到一个或多个众所周知的Web站点上，用户主机到该Web站点上查询。

从网络资源占用和管理角度，建议采用Web方式发布，可以将业务分类分级发布给用户，并同时发布各业务对应的用户侧接收软件，便于业务发布的维护和更新。

组播源的认证授权必须保证只有已申请并被授权的组播源才能够发送组播报文进入网络。

根据组播源授权方式的不同，组播源的认证授权有以下两种方法：

- (1) 静态长期授权。网络管理员为组播源分配源地址、组播地址、带宽、优先级和组播路由之后，通过网管（或组播管理服务器）或命令行在与组播源直接相连的边缘路由器上配置组播ACL和CAR，完成长期性的授权，直到组播源申请终止组播业务时才删除配置和授权。边缘路由器监测下行来的组播报文，执行组播ACL和CAR。

(2) 动态认证授权。网络管理员为组播源分配源地址、组播地址、带宽、优先级和组播路由之后，将组播源发送权限列表配置在认证服务器（或组播管理服务器）上。在组播源用户接入网络时或者开始发送组播报文前（通过监测RP注册报文得知），组播源用户信息被发送给认证服务器（或组播管理服务器）进行远程认证，认证服务器（或组播管理服务器）进行认证后将组播源发送权限授权结果发送给边缘路由器。边缘路由器监测下行来的RP注册报文和组播报文，根据组播源发送权限授权结果处理下行来的RP注册报文，对下行来的组播报文执行组播ACL和CAR。

边缘路由器与认证服务器（或组播管理服务器）之间的认证、授权和计费信息交互可以采用RADIUS或类似功能的协议，附录A定义了用于组播认证授权的RADIUS扩展属性。

从管理角度，对于组播源数量有限相对固定的一对多和多对多组播应用，静态长期授权方法较为稳定简单。

组播源控制要求所有接入边缘设备和边缘路由器在缺省状态下禁止转发下行来的组播报文，除非符合所配置的组播ACL和CAR参数。当主机向网络发送组播报文时，第一个接收到该数据的边缘路由器利用组播ACL和CAR对组播报文进行过滤，只有满足通过要求的报文才能被转发到组播分发树。

组播路由配置使组播数据能从组播源经过组播分发树到达组成员，采用不同的组播路由协议有不同的配置命令和方法。对于安全性要求较高的组播业务，可以配置静态组播分发树，以便严格控制组播包的路径、范围及流量。

当组播源不再发送组播报文且申请释放了组播地址和删除了组播授权时，该项组播业务终止。

7.3 组播流量控制

基于组播数据流量较大接收者众多的特点，为避免对网络和单播业务造成冲击，应当采取措施控制网络中的组播流量。

(1) 配置组播报文进入网络的优先级，使用网络的DiffServ等QoS转发处理方法；同时在边缘路由器上配置ACL和CAR（包括组播组标识和承诺速率），禁止转发未经授权的组播报文，对组播报文进入网络的流量进行限制；如果实际流量超出承诺速率，边缘路由器根据SLA（业务等级协定）对数据流进行整形或丢弃；

(2) 对域间组播报文的流量进行控制，在边界路由器上使用组地址和出接口匹配形式的ACL和CAR限制域间组播报文的转发流量；

(3) 在接入网中可以通过VLAN划分离组播流量和单播流量；可以通过端口限速和VLAN限速对组播流量进行控制；

(4) 在接入网中通过VLAN划分离用户端口之间的流量时，应当支持跨VLAN的组播复制；

(5) 在骨干网中可以通过隧道或VPN隔离组播流量和单播流量；可以通过限制隧道和VPN的带宽对组播流量进行控制；

(6) 用户申请加入组播组时进行资源准入控制，只有用户与网络运营商约定带宽、接入链路带宽和网络带宽满足组播流量所需带宽时，才能接受用户的加入请求，以防止因过量提供服务而不同保证服务质量；

(7) 通过限制接入网中组播组最大数量、组播组的最大成员数和二/三层网络设备上组播表项的最大规模，可以在一定程度上控制组播分发树的数量和规模，防止针对组播设备的DoS攻击；如果需要，可以采取配置组播静态分发树的方式。

7.4 组播接收者控制

接入边缘设备或者网络接入服务器负责对用户加入组播组进行本地或远程认证和授权，在网络层实现组播接收者控制，并收集可供计费的数据信息。组播业务可由网络运营商统一管理，应用层的组播用户控制不在本标准范围之内。

用户访问一项组播业务的完整过程如下：

- (1) 接入认证——用户接入网络的认证；
- (2) 业务选择——用户登陆Web网页或通过组播接收端软件，选择组播业务；
- (3) 组播认证——用户加入组播组的认证；
- (4) 组播接收——用户通过组播接收端软件接收和解读组播信息流；
- (5) 组播退出——用户退出组播组；
- (6) 接入退出——用户断开网络下线。

用户接入认证主要有三种方式：基于物理端口认证、基于用户账号认证、用户账号和物理端口认证。其中，基于物理端口认证的方式，不需要用户输入账号和密码。基于用户账号认证目前主要有三种方式：PPP认证方式、802.1x认证方式和基于Web的强制Portal认证方式。不同的接入认证方式所采用的用户接入身份标识可能不同，如用户接入账号、VLAN ID、物理端口号、MAC地址及其绑定信息。

无论哪种用户接入认证方式，负责组播认证的网络设备都必须检测用户发向网络的IGMP Join报文，才能在网络层实现本地或远程认证组播用户能否加入组播组，并根据组播接收权限授权结果处理用户的IGMP Join报文。组播接收者的认证授权必须保证只有已申请并被授权的组播接收者才能够从网络接收到所授权的组播组流量。

如果组播认证通过，该IGMP Join报文被通过透传或者代理方式发往组播路由器，或者该IGMP Join报文被终结后依靠组播路由协议PIM-SM加入到组播分发树中；接入边缘设备将所授权的组播组流量按照流量控制参数向该用户转发复制，该用户成为组播组的接收者。如果组播认证不通过，该IGMP Join报文被直接丢弃或做其他特殊处理，用户不会收到所请求加入的组播组流量。

当检测到用户发来的IGMP Leave报文或者通过定时器查询到用户已退出某组播组时，接入边缘设备停止对用户转发该组播组的流量。

7.4.1 组播接收者认证和控制点

按照组播认证节点的不同，组播接收者的认证授权有以下两种方法：

(1) 在接入边缘设备处进行组播认证。接入边缘设备可以对IGMP报文终结、代理或者透传。在组播接收者用户接入网络时或者开始接收组播报文前（通过监测IGMP Join报文得知），组播接收者用户信息被发送给认证服务器（或组播管理服务器）进行远程认证，认证服务器（或组播管理服务器）进行认证后将组播接收权限授权结果发送给接入边缘设备。接入边缘设备监测用户发出的IGMP Join报文，根据用户的组播接收权限授权结果处理IGMP Join报文，执行组播组流量向授权用户的转发复制。

(2) 在网络接入服务器处进行组播认证。这种方法要求接入设备必须能将用户的IGMP报文透传到网络接入服务器。在组播接收者用户接入网络时或者开始接收组播报文前（通过监测IGMP Join报文得知），组播接收者用户信息被发送给认证服务器（或组播管理服务器）进行远程认证，认证服务器（或组播管理服务器）进行认证后将组播接收权限授权结果发送给网络接入服务器。网络接入服务器监测用户发出的IGMP Join报文，根据用户的组播接收权限授权结果处理IGMP Join报文，执行组播组流量向授权用户的转发复制。在接入网络存在多用户共享组播带宽的情况下，网络接入服务器还需要主动控制接入

边缘设备的组播转发行为以防止非经授权的用户收到组播组流量。

7.4.2 组播接收者授权方式

按照组播接收授权方式的不同，组播接收者的认证授权有以下两种方法：

(1) 静态长期授权。网络管理员通过网管（或组播管理服务器）或命令行在接入边缘设备或者网络接入服务器上，为申请开通组播业务的用户配置组播接收权限列表和流量控制参数，完成长期性的授权，直到用户申请终止组播业务时才删除配置和授权。接入边缘设备或者网络接入服务器监测用户发来的IGMP Join报文，根据配置和授权处理IGMP Join报文。

(2) 动态认证授权。网络管理员为申请开通组播业务的用户在认证服务器（或组播管理服务器）上配置组播接收权限列表和流量控制参数。在组播接收者用户接入网络时或者开始接收组播报文前（通过监测IGMP Join报文得知），组播接收者用户信息被发送给认证服务器（或组播管理服务器）进行远程认证，认证服务器（或组播管理服务器）进行认证后将组播接收权限授权结果发给接入边缘设备或网络接入服务器。接入边缘设备或网络接入服务器监测用户发出的IGMP Join报文，根据用户的组播接收权限授权结果处理IGMP Join报文，执行组播组流量向授权用户的转发复制。

接入边缘设备或者网络接入服务器与认证服务器之间的认证、授权和计费信息交互，可以采用RADIUS或类似功能的协议。附录A定义了用于组播认证授权的RADIUS扩展属性。

7.5 组播安全控制

在接入网环境中，二层交换设备应当支持IGMP Snooping或IGMP Proxy，或者其他二层组播控制标准协议，抑制二层网络中的组播泛滥，防止未经授权的用户接收到组播流量。否则，即便实现了组播认证与授权，如果接入设备以广播方式转发组播报文，未经授权的用户依然可能收到组播信息流。

在网络接入服务器处进行组播认证的情况下，如果不是配置了每个VLAN只包含一个用户，那么网络接入服务器在处理IGMP报文时或者通过定时器检测到用户已退出组播组时，应当主动控制接入边缘设备的组播转发行为，抑制接入边缘设备将组播流量转发给未通过组播认证的用户。

配置了VLAN的情况下，如果一个VLAN内含有多个用户端口时，接入设备每个端口应当单独维护组播组列表，抑制组播报文在VLAN内部各端口之间的泛滥；如果需要进一步节省组播流量所占用的网络资源，接入设备需要支持跨VLAN组播复制。

为了保证组播认证的有效性，网络接入服务器和二层交换设备应当能检测出不同VLAN下的MAC地址仿冒情况。为了防止不同VLAN下其他用户的MAC地址仿冒，用户认证通过后应当进行基于MAC地址和用户信息的绑定。

接入设备必须抑制未经授权的组播源用户发送的组播报文。接入设备在缺省状态下禁止转发下行来的组播报文，除非符合所配置的组播ACL和CAR参数（包括组播组标识和承诺速率）。

应用层组播信息流的加密解密不在本标准的范围内。

8 IP 组播业务的管理模式

组播业务作为IP网络的增值业务，用户在申请到NSP接入身份标识后，可以申请该接入身份标识的组播权限列表。如果网络运营商允许用户在线维护自己的组播权限列表，可以设置一台发布组播业务的Web服务器，用户登录Web网页注册或取消加入某业务组播组的权限。说明：在本节用户特指组播接收者用户。

按照接入管理和组播管理的独立性，组播业务管理可分为捆绑模式和分离模式。

按照业务管理的粒度，组播业务管理可分为简单模式和精细模式。

8.1 捆绑模式和分离模式

捆绑模式——用户的接入认证和组播认证管理集成在一台认证服务器上。用户的接入认证和组播认证请求都发给同一台认证服务器，用户的组播权限列表作为用户接入身份标识的增值属性管理。

分离模式——认证服务器只负责用户的接入认证管理，用户的组播认证管理由专门的组播管理服务器负责。用户的组播认证由接入边缘设备或者边缘路由器，根据网管和命令行的配置参数在本地进行，或者发给组播管理服务器远程认证。

8.2 简单模式和精细模式

简单模式——组播认证仅控制用户是否有权接收组播信息，不控制用户是否有权加入某个具体组播组。用户有权接收组播信息，表示用户有权加入任意组播组。简单模式下，所有组播组费率一致，网络运营商只能按接收组播信息的时长、流量或包月制计费，不能按不同组播组分别计费。各组播组接收者的认证和计费可由各组播源的提供者通过应用层软件实现。

精细模式——组播认证控制用户是否有权加入某个或某类组播组，网络运营商负责认证和计费，组播源只须负责发送组播信息流给所属的组播组。精细模式下，各个或各类组播组的加入费率可以不同，网络运营商可以对用户加入不同（类）组播组按时长、流量或包月制分别计费。认证服务器为每个用户维护一个组播权限列表，保存和维护该用户所允许加入的所有组播组地址。

无论哪种模式下，除了包月制计费，按时长或流量计费都必须保证计费信息的准确性。负责组播认证的接入边缘设备或者网络接入服务器必须为组播业务计费系统收集信息并提供接口，精确记录用户加入组播组的时刻、用户离开组播组的时刻、用户接收组播信息的时长或流量。

通过用户组播认证和授权过程能够精确记录用户加入某组播组的时刻，但用户离开某组播组必须考虑以下多种情况：

- a) 用户接入断开则用户离开所有组播组；
- b) 用户显式发送IGMP Leave退出组播组；
- c) 通过IGMP查询检测到用户未发送IGMP Leave异常离开组播组；
- d) 检测到用户组播授权中定时时间到，强制用户离开组播组；
- e) 检测到用户长时间未收到组播报文，定位为网络异常或业务终止。

为支持组播认证，采用RADIUS协议作为汇聚设备和计费系统之间的接口协议，必须对RADIUS协议予以适当的扩展以携带组播认证信息，具体扩展参见附录A所规定的用于组播认证的RADIUS扩展属性。

8.3 计费模式

IP组播业务的计费可以由组播源通过应用层软件和密钥分发技术实现，也可以由网络服务提供商在网络层实现，或者两者同时进行以便费用核算。本标准主要关注由网络服务提供商在网络层实现计费的机制和模式。

IP组播业务的计费模式可以划分为三类：

- (1) 统一费率模式：不计连接时间和收发流量，按用户订购的组播组的数量和业务类型定价。
- (2) 连接时间模式：不计收发流量，按用户加入的组播组的数量、业务类型、连接时间定价。
- (3) 基于使用的模式：按用户对网络资源的占用量及占用时间收费，包括用户加入的组播组的数量、业务类型、连接时间、组播流量，组播树大小等成本因素。

除了统一费率模式，其他模式都要求接入边缘设备或者网络接入服务器提供计费数据接口并精确收

集计费信息，包括业务发生地点、发生时间、业务成本、用户身份标识和组播组标识。其中，业务成本一般只考虑组播业务流量，不考虑组播树大小。尽管收集组播树的大小并且在组成员之间分摊网络资源的占用成本，可以实现更公平合理的价格，但由于组播树是动态变化的，收集和计算的成本高，进行估计即可。另外，组播业务流量对QoS的要求也是应该考虑的成本因素之一，需要QoS保证的组播流量的费率因成本高可以相应地提高。

网络服务提供商根据公平性、可预见性、可审计性、复杂性、网络成本、用户需求、竞争性和商业模式等因素出发，制订适合自己的计费方式和费率。

9 IP 组播业务的性能要求

9.1 IGMP 处理能力

接入边缘设备应当具备足够的IGMP处理能力，满足大量用户同时进行组播组切换。对于IPTV业务来说，组播组切换通常被称为频道切换。

9.2 组播组加入时延

接入边缘设备应当支持组播组快速加入，保证用户的使用体验。自用户设备发出IGMP Join报文至用户设备收到所选组播组第一个组播数据报文的时延至少 $<200\text{ms}$ 。说明：不包含用户设备处理时延。

9.3 组播组离开时延

接入边缘设备应当支持组播组快速离开，保证非包月制收费模式下的计费准确性可达到秒级。自用户设备发出IGMP Leave报文至用户设备不再收到该组播组组播数据报文的时延至少 $<200\text{ms}$ 。

9.4 组播组数

接入边缘设备应当支持足够多的组播组数，至少大于1000个可供用户选择。对于IPTV业务来说，组播组数即频道数。

9.5 组播带宽

接入边缘设备应当保证足够的组播带宽，实现组播流量无阻塞转发，满足宽带流媒体业务需求。

9.6 组播流丢包率

从组播源发出至用户接收设备收到组播数据流的网络传送丢包率至少应 $<1\times 10^{-3}$ ，满足 IP 多媒体业务的需求。

9.7 组播流错包率

从组播源发出至用户接收设备收到组播数据流的网络传送错包率至少应 $<1\times 10^{-4}$ ，满足 IP 多媒体业务的需求。

9.8 组播流时延

从组播源发出至用户接收设备收到组播数据流的网络传送时延至少应 $<1\text{s}$ ，满足 IP 多媒体业务的需求。

10 IP 组播业务的监控要求

组播业务的监控是指收集组播相关的信息，分析它们并根据分析结果对组播网络做出必要的调整和管理。

组播监控的具体内容应当包括以下各方面。

10.1 状态监控

组播状态的监控应包括组播设施中的各实体的统计信息，主要包括：

- a) 当前的组数、组播源数、接收者数、RP数、AS数等；
- b) 某时间段内，组成员最多的组及其成员数；
- c) 某时间段内，加入组最多的主机及其加入的组数；
- d) 某时间段内，拥有最多MBGP Route-Flaps的网络；
- e) 某时间段内，广播最多主机信息的AS；
- f) 某时间段内，发送SA消息最多的AS；
- g) 某时间段内，发送SA信息最多的RP等。

10.2 会话和成员监控

组播会话和加入者特征的监控，主要包括：

- a) 某时间段内，具有某种特征的成员数；
- b) 某时间段内，具有某种特征的组数；
- c) 某时间段内，具有某种特征的组播源数；
- d) 当前某些特定组的接受者数、发送者数等。

10.3 路由与流量监控

路由与流量的状态监控，针对所监控的路由器进行，主要包括：

- a) 组播路由项数；
- b) 通过MSDP广播的（S，G）项数；
- c) 在密集模式运行方式时的路由表项数；
- d) 有直连成员的路由表项数；
- e) 路由器本身是组成员的路由表项数；
- f) 被剪枝的路由表项数等；
- g) 最近某时间段上从活动源来的流量占用带宽的情况。

10.4 协议监控

对用到的每个组播路由协议都应有相应的监控数据。在此主要提出对域间组播路由协议MBGP和MSDP的监控要求。

1. MBGP协议监控

MBGP协议的一般统计数据主要包括：

- a) 掩码长度为32的MBGP路由数；
- b) 掩码长度在25~31之间的MBGP路由数；
- c) 掩码长度为24的MBGP路由数；
- d) 掩码长度在1~23之间的MBGP路由数；
- e) 与所监控的路由器（可能有多个）之一有组播路由的网络数；
- f) 所检测到的特定路由（具备某种指定特征）数等。

MBGP协议的稳定性统计数据主要包括：

- a) 与上一次收集的数据相比较而言，丢失的路由数；
- b) 与上一次收集的数据相比较而言，获得的路由数和改变的路由数；

c) 当前来自各AS的MBGP路由数等。

MBGP协议监控的目的是检测路由抖动。

2. MSDP协议监控

MSDP协议的统计数据主要包括：

a) 路由器可见的SA消息数，每个消息用(S, G, RP)标识；

b) 产生SA消息的不同的组播源数；

c) SA消息发送到的不同的组数；

d) 从不同的RP发来的重复的SA消息数，即满足下列条件的消息，(Si1, Gj1, RPk1), (Si2, Gj2, RPk2)，且Si1 = Si2, Gi1 = Gi2, RPk1 \neq RPk2。

e) 发布SA消息的RP所在的不同AS数；

f) 发布AS消息的不同RP数；

g) 每10000个SA广播中重复的SA数。

MSDP协议的状态可以从路由器的SA状态表中提取，路由器将SA状态存在缓存中，所以数据的准确性依赖于缓存机制。不同SA的数目可以用来衡量整个组播设施的活动情况，重复的SA消息数可以指示MSDP的运行状况。

MSDP协议监控的主要目的是检测MSDP SA消息风暴。检测风暴的方法是发现MSDP TCP会话的频繁重置，监测风暴的起源，可以通过以下几方面的信息综合分析：MSDP控制消息的总速率、MSDP SA的重复消息数、MSDP消息包含的数据大小、组播组数、(S, G)数和RP数。

10.5 地址空间监控

组播地址空间的统计数据主要包括：

a) 各AS拥有的组播地址范围，其中已分配的组播地址，尚空闲的组播地址；

b) 某地址范围的活动的组数（至少有一个接收者），占有所有组的百分比；

c) 某地址范围的通过MSDP广播的活动的组数；

d) 某地址范围各组的主机数（即接入者数）和组播源数等。

这些信息可以描绘出各地址范围空间的使用及分布情况，从主机数和组播源数还可以看出组的使用情况。

10.6 拓扑与地理位置监控

拓扑与地理位置监控主要以可视化的图形直观地显示组播网的结构等信息，包括：

a) MBGP的局部与全局视图；

b) 重要组播设施的地理位置视图，例如组播源、成员主机、MBGP网、PIM-SM网和RP分布；

c) 组播分发树的视图等。

10.7 组播监控对设备和网管的要求

网络监控工具的目标是提供并组织网络相关的信息，包括：协议、地址、数据流、统计和异常。要求没有很深网络配置知识的人也能监控网络操作，在问题发生时容易标识出来，并根据相关信息解决问题。

组播监控的基础是遵循标准MIB，提供统一的基于SNMP的监控和管理。因此要实现组播监控，对设备和网管的要求是：

a) 实现了IGMP的设备应当支持IGMP MIB；

- b) 实现了IGMP PROXY的设备应当支持IGMP MIB;
- c) 实现了PIM的设备应当支持PIM MIB;
- d) 实现了MBGP的设备上应当支持MBGP MIB;
- e) 实现了MSDP的设备上应当支持MSDP MIB;
- f) 所有支持IP组播的设备都应当支持IP Multicast Routing MIB;
- g) 除了支持MIB外, 设备还应当提供一些组播调试工具或手段, 如TRACE和路由信息查询;
- h) 网管应当支持IGMP、PIM-SM、PIM-DM、MBGP、MSDP和组播路由表的配置和查询功能;
- i) 网管应当支持组播树发现、组播流量统计、支持MSDP SA消息风暴的检测、组播组发现与统计功能;
- j) 网管应当支持PIM RP点的配置功能。

附 录 A
(规范性附录)
用于组播认证的 RADIUS 扩展属性

本附录规定了用于组播认证的RADIUS扩展属性。报文类型定义和属性包含关系遵循RADIUS标准协议RFC2865。对RADIUS 的 Vendor-Specific 属性（26）进行扩展，遵循 RFC2865 建议的扩展方式。

	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0								
0	Type								Length								Vendor-ID																							
1	Vendor-ID (Continue)																Vendor Type								Vendor length															
2	Attribute-Specific...																																							

Vendor-ID为厂商在IANA所申请的ID。

Vendor Type取值97 ~ 99时用于本标准的组播认证，定义见下表。

扩展属性名	Vendor Type值	Access-Request	Access-Accept	Access-Reject	Access-Challenge	Accounting-Request	Accounting-Response	Session-Control
Multicast_Source_Group	97	0	0+	0	0	0	0	0
Multicast_Receive_Group	98	0	0+	0	0	0	0	0
Reserved（保留待用）	99	0	0	0	0	0	0	0

表中，“0”表示属性一定不会出现在该报文类型中；

“0+”表示0个或多个属性可能会出现在该报文类型中。

Multicast_Source_Group 属性

String 类型，用于组播源认证，长度最短为 36 个字节，且字符串中必须是 0~9 之间的数字，不能含有其他字符。前 4 个字节为 IP 地址，表示用户作为组播源要加入的组播组 IP 地址；后 32 字节为组播 CAR，分成 4 个 8 字节，从左至右 4 个 8 字节依次表示用户作为组播源所发送组播流量的上行峰值速率、上行平均速率、下行峰值速率和下行平均速率，速率的单位为 bps。该属性可以在 RADIUS Access-Accept 类型报文中多次出现，表示用户作为组播源属于多个组播组。

Multicast_Receive_Group 属性

Integer 类型，用于组播接收者认证。长度为 4 个字节，表示用户作为组播接收者要加入的组播组地址。该属性可以在 RADIUS Access-Accept 类型报文中多次出现，表示用户作为组播接收者属于多个组播组。

参 考 文 献

- IETF RFC 1112 (1989) Host extensions for IP multicasting, (Standard), 互联网组管理协议 (版本一)
- IETF RFC 2236 (1997) Internet Group Management Protocol, Version 2, (Proposed Standard), 互联网组管理协议 (版本二)
- IETF RFC 2362 (1998) Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification, (Experimental), 协议无关组播 - 稀疏模式协议
- IETF RFC 2365 (1998) Administratively Scoped IP Multicast, (Best Current Practice), 可管理范围的IP组播
- IETF RFC 2715 (1999) Interoperability Rules for Multicast routing Protocols, (Informational), 组播路由协议互操作规则
- IETF RFC 2908 (2000) The Internet Multicast Address Allocation Architecture, (Informational), 因特网组播地址分配架构
- IETF RFC 2932 (2000) IPv4 Multicast Routing MIB, (Proposed Standard), IPv4组播路由MIB
- IETF RFC 2933 (2000) Internet Group Management Protocol MIB, (Proposed Standard), 互联网组管理协议MIB
- IETF RFC 2934 (2000) Protocol Independent Multicast MIB for IPv4, (Experimental), IPv4协议无关组播MIB
- IETF RFC 3170 (2001) IP Multicast Applications: Challenges and Solutions, (Informational), IP组播应用挑战和解决方案
- IETF RFC 3171 (2001) IANA Guidelines for IPv4 Multicast Address Assignments, (Best Current Practice), IPv4组播地址分配指导
- IETF RFC 3180 (2001) GLOP Addressing in 233/8, (Best Current Practice), GLOP寻址
- IETF RFC 3228 (2002) IANA Considerations for IPv4 Internet Group Management Protocol (IGMP), (Best Current Practice), IPv4因特网组管理协议考虑
- IETF RFC 3353 (2002) Overview of IP Multicast in a Multi-Protocol Label Switching (MPLS) Environment, (Informational), MPLS环境中的IP组播概述
- IETF RFC 3376 (2002) Internet Group Management Protocol, Version 3, (Proposed Standard), 互联网组管理协议 (版本三)
- IETF RFC 3446 (2003) Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP), (Informational), 采用协议无关组播和组播源发现协议的任播汇集点机制
- IETF RFC 3559 (2003) Multicast Address Allocation MIB, 组播地址分配MIB
- IETF RFC 3569 (2003) An Overview of Source-Specific Multicast (SSM), (Informational), 源指定组播概述
- IETF RFC 3575 (2003) IANA Considerations for RADIUS (Remote Authentication Dial In User Service), RADIUS协议考虑
- IETF RFC 3618 (2003) Multicast Source Discovery Protocol (MSDP), (Experimental), 组播源发现协议
- IETF RFC 4271 (2006) A Border Gateway Protocol 4 (BGP-4), (Draft Standard), 边界网关

	协议4
IETF RFC 4541 (2005)	Considerations for IGMP and MLD Snooping Switches , (Informational) , 交换机监听互联网组管理协议和组播监听发现协议的考虑
IETF draft-ietf-magma-igmp-proxy-06 (2004)	(Internet Draft to be Proposed Standard) , 基于互联网组管理协议或组播监听发现协议的组播转发 (即 “IGMP/MLD代理”)
IETF draft-ietf-mboned-addrarch-04 (2006)	Overview of the Internet Multicast Addressing Architecture, (IETF draft to be Best Current Practice) , 因特网组播地址分配架构概述
IETF draft-ietf-mboned-msdp-deploy-06 (2004)	Multicast Source Discovery Protocol (MSDP) Deployment Scenarios, (IETF draft to be Best Current Practice) , 组播源发现协议布署
IETF draft-ietf-mboned-msdp-mib-01 (2005)	Multicast Source Discovery protocol MIB, (Internet Draft to be Experimental) , 组播源发现协议MIB
IETF draft-ietf-pim-anycast-rp-07 (2006)	Anycast-RP using PIM, (Internet Draft to be Proposed Standard) , 仅采用协议无关组播协议 (版本二) 的任播汇集点机制
IETF draft-ietf-pim-mib-v2-06 (2006)	Protocol Independent Multicast MIB, (Internet Draft to be Proposed Standard) , 协议无关组播MIB (版本二)
IETF draft-ietf-pim-sm-bsr-08 (2006)	Bootstrap Router (BSR) Mechanism for PIM, (Internet Draft to be Proposed Standard) , 协议无关组播协议族的自举路由器机制
IETF draft-ietf-pim-sm-v2-new-12 (2006)	Protocol Independent Multicast - Sparse Mode (PIM-SM) : Protocol Specification (Revised) , (Internet Draft to be Proposed Standard) , 协议无关组播 - 稀疏模式协议 (版本二)