基于 COPS 协议的 IP 组播接入控制研究

王栋平　曹　争

（东南大学计算机科学与工程系 江苏省计算机网络技术重点实验室 210096 南京）

摘 要： 组播接入控制的重要性随着基于 IP 网络的多媒体业务迅速发展而显得更加迫切。COPS 协议的发展，为实现组播接入控制提供了新的途径。该文提出了一种基于 COPS 协议实现 IP 组播接入控制的设计方案。论文通过与现有接入控制实现的比较，阐明了该方案的优点。

关 键 字： 接入控制，IP 组播，COPS

The Research of IP Multicast Access Control based on COPS Protocol

WANG Dongping　　CAO Zheng

(Southeast University, Computer Science and Engineering Dept.,
JIANGSU Province Key Laboratory of network technology, 210096 Nanjing)

Abstract: The IP multicast access control becomes more important as the increasing of multimedia services based on IP network. The presentation of COPS protocol offers some new methods to implement IP multicast access control. In this paper, the design of IP multicast access control is proposed basing on COPS protocol. Comparisons are made between the existing implementations and this solution to show its advantages.

Key words: Access Control, IP multicast, COPS.

引　言

随着 Internet 的飞速发展，基于 TCP/IP 网络的多媒体业务也日益增多。因而能够更有效地利用网络带宽资源的 IP 组播技术研究成为当前技术科研领域的一个热点。到目前为止，不仅仅是教育研究机构在进行 IP 组播的技术探索，越来越多的企业也参与到这一领域的研究工作之中。例如，Cisco、VBrick、RealNetworks、Microsoft 等公司均推出了支持 IP 组播的多媒体业务系统【1】。这表明，基于 IP 组播技术的增值服务已经成为当前的现实需求。商业软件公司看重的是经济利润，而实施有效的接入控制是保证商业收入的重要手段，因此，接入控制成为其系统中必不可少的组成部分。

1. 组播接入控制的现状及缺陷

由于现行的基于 TCP/IP 网络的组播协议族中缺乏对接入控制的有效支持，因此上述公司都是在应用层实现接入控制功能，这种实现机制存在着如下问题：

- 实现与特定应用软件相绑定，通用性和开放性不好；
- 实现方法是各个公司的商业秘密，不利于对实现进行广泛深入的研究，因而其安全性存在隐患；
- 实现局限在应用层，往往不能提供足够的安全保障。
- IP 组播的管理与服务的提供相绑定，而现行管理域的划分往往是不考虑使用情况的，实现与需求之间存在矛盾。

2. 基于 COPS 协议的组播接入控制实现

综上所述，要从根本上解决 IP 组播接入控制的问题，就必须从协议入手。基于上述分析，我们提出一种基于 COPS 协议的 IGMP 改进模型来实现安全的接入控制。

作者简介：王栋平，男，1975 年生，东南大学计算机系硕士研究生； 曹　争，东南大学计算机系副教授，硕士研究生导师，主要研究方向包括网络管理、网络体系结构、开放分布式处理等。

2.1 COPS 协议简介

COPS(Common Open Policy Service)协议在策略服务器即策略决定者（Policy Decision Point，PDP）及其客户即策略执行者（Policy Enforcement Point，PEP）之间协调策略信息的交换。其基本模型如图 1 所示【3】。协议提供了报文级的安全，可以进行认证、重发保护和维护报文的完整性。它也能使用 IP Security[IPSEC]或者 Transport Layer Security[TLS]等已有的安全机制来保证 PEP 和 PDP 间的认证和信道安全。图中的 LPDP(Local Policy Decision Point)是可选件。

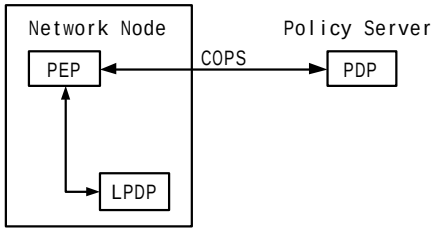

图1 COPS协议模型

2.2 IGMP 协议简介

IGMP(Internet 组管理协议) 是一种主机－路由器协议，规范主机如何向路由器通知成员信息，以及路由器如何向直连的主机请求成员信息。到目前为止，该协议有 3 个版本（v1、v2 和 v3），IGMPv1 和 IGMPv2 已经成为正式标准【4】【5】，IGMPv3 还在制定之中【6】。IGMPv2 的基本工作机制如下。子网中的主机通过 IGMP 协议向组播路由器报告它所属的群，从而使组播路由器知道需要向这个子网转发有关的报文。组播路由器使用 IGMP 对子网内的主机进行定期探询，以了解这个群成员是否依然存在，在子网附接多个组播路由器的情况下，则要选一个作为探询的代表，通常为 IP 地址大者。探询组播路由器一旦收到成员报告，系统就认为需要对组播报文进行转发，而不去验证改成员报告的真实性以及该用户是否被允许加入该组。IGMPv3 中引入了组播源过滤的概念，制定了由主机发起的组播源过滤行为，使组播路由器可以不转发来自某些特定源地址的组播报文【6】，但是，仍然没有解决对用户接入的控制。

2.3 接入控制实现模型

基于上述介绍，我们想到，如果在 IGMP 中嵌入 PEP 来实现接入控制将是一种可行的办法。因此，我们提出图 2 所示的接入控制实现模型。该模型的核心思想是对 IGMP 协议进行改进，组播路由器在收到来自主机的 IGMP 成员报告后，不再直接将对应组播地址加入转发链，而要首先经过接入控制模块，依据成员信息（如三元组<主机 IP 地址，加入组地址，组播源地址>）PEP 将构造请求，待得到 PDP 的决策后，如果接受才能进入 Members Present 状态，即接受该成员的加入，否则将忽略该成员报告而返回原状态。

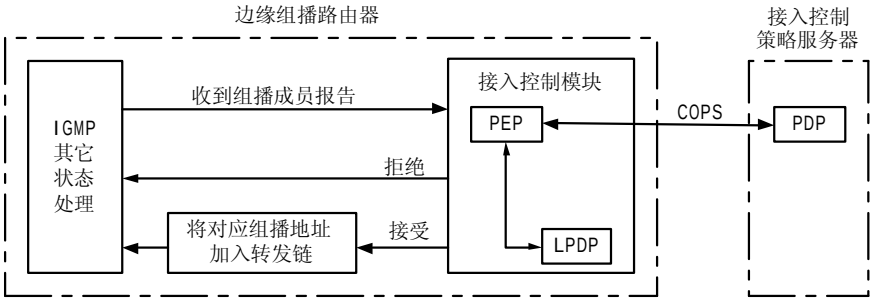

图2 基于COPS的组播接入控制实现模型

在效率方面，采取了两方面的保障措施。一方面，将组播路由器划分为核心组播路由器和边缘组播路由器，仅仅在边缘组播路由器上实现接入控制。由于边缘组播路由器直连的主机数量相对较少，因而增加接入控制带来的效率损失也相对较少。另一方面，在边缘组播路由器内配置 LPDP，PEP 首先询问 LPDP，如果没有决策信息，再发送请求到远端的 PDP。对于某一边缘组播路由器负责的子网内的主机的接入控制决策信息，可以事先由远端的 PDP 配置到 LPDP，这样，对于合法用户，其请求将很快得到接受，可以保证较高的实现效率。

在安全方面，用户可以通过与接入控制策略服务器交换信息，实现用户身份与 IP 地址的绑定和拆除，而且这种绑定是动态的，因为策略服务器可以随时修改策略信息库的相关内容，并通过 COPS 协议将修改传递到

有关的远端 PEP 和 LPDP。这样，用户提交的请求信息就不需要包含过多的用户信息，因而减少了安全威胁。用户与接入控制策略服务器交换信息可以通过 IPSEC、TLS、HTTPS、甚至带外方式，保障其安全性。因而，接入控制的安全性就依赖于 PEP 与 PDP 的信息交互的安全性，回顾 2.1 节所述，其安全性也是有保障的。综上所述，整个系统的安全性是有保障的。

在可扩展性方面，可分为垂直扩展和水平扩展。当不同管理域之间存在隶属关系时，可以采用级连 PDP 的方式进行垂直扩展。当管理域过于庞大时，我们可以将其划分为多个子管理域，从而减小每个 PDP 需要同时管理的 PEP 数量，避免 PDP 成为系统瓶颈。当不同管理域之间不存在隶属关系，而组播请求的对象又是跨越管理域的，水平扩展的做法是在管理域边缘重新进行接入控制检验，依据新的管理策略决定是否提供服务。

3. 测试模拟系统

3.1 测试网络拓扑结构

组播接入控制系统测试网络由 3 台主机，1 台 Linux 路由器和 2 台 HUB 组成。系统的拓扑结构如图 3 所示。其中组播源（由 realserver 软件提供组播多媒体流）位于子网 1，而组播客户（由 realplayer 软件接收并显示组播多媒体流）位于子网 2，组播流必须经过组播接入路由器的转发才能到达组播客户。

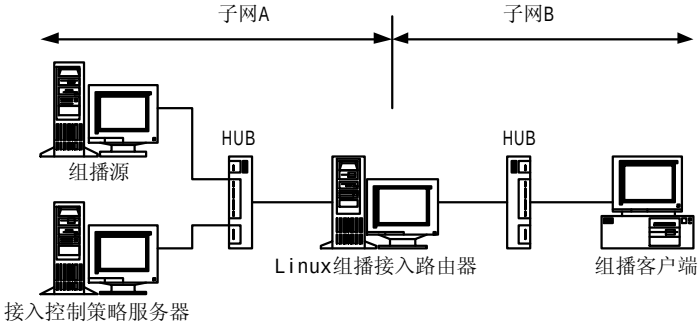

图3　组播接入控制测试系统结构图

3.2 测试方法

通过预先或实时改变策略服务器中 PIB（策略信息库）的配置，观察不同决策对组播接入控制的影响。

- 预先配置策略服务器中 PIB（策略信息库），允许组播接入路由器为子网 2 转发组播流。
  结果：组播客户端能够正常接收组播流。
- 预先配置策略服务器中 PIB（策略信息库），不允许组播接入路由器为子网 2 转发组播流。
  结果：组播客户端不能够接收组播流。
- 实时改变策略服务器中 PIB（策略信息库）的配置，由允许改为不允许组播接入路由器为子网 2 转发组播流。
  结果：组播客户端中断原来的正常接收，并且无法再次接收组播流。
- 实时改变策略服务器中 PIB（策略信息库）的配置，由允许改为不允许组播接入路由器为子网 2 转发组播流。
  结果：组播客户端由不能接收变为能够正常接收组播流。

试验结果表明通过修改策略服务器中的决策信息，可以有效的控制组播接入路由器的行为，从而实现精确可靠的接入控制功能。

4. 结 束 语

随着网络多媒体业务的迅猛发展，IP 组播展示出广阔的应用前景，作为其应用的一项关键技术，接入控制也正在成为大家关注的焦点。协议是网络通信的基础，本文提出的以协议为基础的 IP 组播接入控制模型，综合考虑了系统的可以性，效率，安全性和可扩展性，相信能够在今后的到广泛的应用。

参 考 文 献

【1】 http://multicast.internet2.edu/wg-multicast-applications.shtml

【2】 http://video.dlut.edu.cn/tvzx/

【3】 Durham D, and Boyle J, Cohen R, et al, “The COPS (Common Open Policy Service) Protocol”, RFC 2748, January 2000.

【4】 Deering S, “Host Extensions for IP Multicasting”, RFC 1112, August 1989.

【5】 Fenner W, “Internet Group Management Protocol, Version 2”, RFC 2236, November 1997

【6】 Cain B, Deering S, Fenner B, et al, "Internet Group Management Protocol, Version 3", INTERNET-DRAFT, May 2002.