网络中部署组播应用

在网络中部署了组播应用时，总要接触这些词汇：DVMRP、PIM、IGMP以及IGMP Snooping。它们都和组播寻路相关。作为动态组播协议的DVMRP和PIM有些类似单播路由协议中的OSPF，也会生成路由树，只不过组播路由用来告知本地路由器或三层交换机在网络中还有哪些路由器上有组播组的存在。而在这个拥有组播组的路由器上，可能有很多个接口，组播组到底位于哪个接口上呢？IGMP用来回答这个问题。而IGMP Snooping和IGMP并没有什么关系，这项功能在二层交换机上都是默认打开的，而IGMP是基于IP的协议，往往在路由器或三层交换机上是默认关闭的。具有组播组的路由器的IGMP接口常常延伸到接入层交换机上（比如一个二层交换机），但又不能把所有组播包扔到所有接入交换机的端口上，因为有些端口仅有广播和单播通信。为了提高效率，二层交换机采用了IGMP Snooping。

现在建网，由于视频会议等应用已必不可少，很多用户都会进行不同形式的组播测试。记者曾接触过银行和高校的用户，他们在测试组播时往往是实际部署组播源，然后看接收效果。如果效果不好的话，再进行网络升级或QoS等优化配置。应该说，如果网络中的流量比较稳定的话，这样的测试也是能达到目的的。而我们在实验室中的组播测试，由于有了高端测试仪表的帮助，则可以测试得更为充分。可以支持IGMP的不同版本，可以使用不同的组播路由协议，可以向某个路由器接口灌入指定数目的组播组，可以按带宽的一定比例发流，可以混入一定数目的单播流量。测试仪实现的测试方法是根据目前的多播测试标准制订的，比如RFC 2432，在这个RFC中，描述了多播测试的多个方面：吞吐量、延迟、组播组容量等。有兴趣的读者可以看看这篇RFC，我在这里给您一个使用测试仪测试组播的概述。

堆积（accumulated）测试：它测试的是当客户端以某种速率加入大量组的情况下组播路由器或三层交换机（我们称之为DUT：Device Under Test）的吞吐量。测试使DUT快速地更新它的IGMP组cache，然后向所有组转发流量。

分发（Distributed）测试：DUT应该具备这样的能力：把数据转发到特定端口上正确的组播客户手中。此测试完成这项任务。

组播容量（Group Capacity）测试：顾名思义，它测试DUT能够注册并转发组播帧的最大组数量。

组加入时延（Group Join Delay）测试：它记录的是DUT收到IGMP加入请求到组播客户端收到该组流量间的时延。你可以调节不同的发帧速率来观察不同情况下的时延。与此相对应，还可以测试组撤出时延（Group Leave Delay）。

延迟（Latency test）测试：这项测试量度的是组播帧发向多个路由器接口的平均延迟。它揭示了DUT多播转发的平均开销。此外，还可以测试最大和最小时延，从而模拟应用的延迟范围。

混合（Mixed）吞吐量测试：测试仪多个端口与DUT相连，同时发送、接收单播和组播数据，测试此种情况下DUT的吞吐量。这项压力测试模拟了现实网络环境，对于用户来说，可以认为是必测的一项。

此外，用户可以根据自己的网络流量特点和所采用的组播设备，在上述项目的基础上构造出某些特定测试。

一代网络的必选技术　　IP组播已成熟

随着宽带的发展，多媒体的相关服务需求的日益增长刺激了 IP组播技术的普及和发展，成为新一代网络的不可缺少的关键技术。目前的 IP组播技术已经相当成熟，这意味着运营商和企业已经可以通过该技术获得经济效益了。

成熟的 IP组播组网

1. 主机和组播路由器之间的组播技术

IGMP是惟一可选的协议，路由器通过使用该协议与主机进行通信，以了解局域网上的组播组，主机通过向路由器发送消息告诉路由器它希望 听 到哪个组的报文。目前，成熟版本为 2，IETF工作组正在开发版本 3。

2. 路由协议

对于大型的 IP组播网，第三层的 IP路由协议一般要分为域内组播协议和域间组播协议。域内由运营商或企业自行管理，域间通过共同的约定域间组播协议实现域间的组播。

（1） 域内组播路由协议

包括 DVMRP、PIM-DM、PIM-SM、MOSPF和 CBT。

随着技术的进步和市场的选择，其中的 PIM-SM协议脱颖而出，成为广泛支持的组播协议。该协议的 显示加入 特性只会向需要组播报文的网络传播报文，同时组播源到接收者的网络延迟小，正是这两点因素使之成为域内组播协议的首选。另外，占有市场份额最大的 Cisco仅支持 PIM-SM和 PIM-DM，而 PIM-DM由于其带有 广播 的特点，不适合大型网络，因此 Cisco也推荐使用该协议作为域内组播协议。

（2） 域间路由协议

MBGP对 BGP进行了一些扩展使之适合于多种协议的路由交换，但目前主要用于组播。该协议增加了路由信息的状态，每一条路由可以标记为是单播的还是组播的路由。这样就可以为组播维护其路由信息和状态，解决域间的组播路由问题。

要完成域间组播，除了要使用 MBGP解决路由问题，对于 PIM-SM域互联还要辅助使用 MSDP，该协议如其名字一样主要用于解决不同域之间的组播源的发现问题。通过组播源的发现，域之间可以互相知道存在的每一个域内的组播源，从而建立从组播源到组播接收者的组播分发树。

3. 对以太网交换机的要求

组播技术的出现对以太网交换机也提出了一定的要求。在堆叠以太网交换机时，如果仅仅把组播报文当作广播报文进行泛洪式传播的话，势必造成局域网中不必要的流量。解决这个问题有两种成熟技术可供选择：IGMP窃听和 CGMP。它们都是为了解决老式交换机无法知道组播组成员分布的问题。IGMP窃听是使交换机具有第三层意识，窃听主机和路由器之间发送的 IGMP消息，从而确定组成员所在的位置。CGMP则是通过路由器和交换机之间的协议交互而使交换机了解组成员分布，但 CGMP是 Cisco的专有协议。

组播的高层协议

IP组播不能保证数据的可靠传输，可能会出现报文的丢失、乱序、重复的情况。针对不同类型的应用，人们开发了相应的协议来支持。

1. 流媒体应用中的常见协议

流媒体的应用是组播重要的应用，譬如音频和视频的播放、视频会议、远程教学等，都属于这一范畴。针对于这种类型的应用有一整套的协议支持。

RTP是用于 Internet上针对多媒体数据流的一种传输协议。它既可以使用单播，也可以使用组播作为下层传输协议。RTP被设计为一对一或一对多的情况下工作，主要提供了时间信息和实现流同步，通常使用 UDP来传送数据。RTCP属于 RTP协议的一部分，它提供了流量控制和拥塞控制服务。

RTSP是由 RealNetworks和 Netscape共同提出的一个开放的标准，它扩展了现有的 Web架构，提供了一种可控制的音频、视频的点播服务。它是应用层的协议，与 HTTP很相似， HTTP传送 HTML，而 RTP传送的是多媒体数据。

RSVP是 Internet上的资源预留协议，使用 RSVP预留一部分网络资源（即带宽），能在一定程度上为流媒体的传输提供 QoS。 RSVP技术在可扩展性上倍受质疑，因此目前还仅限于小型内部网上使用。

2. 可靠组播协议

流媒体应用中，对少量丢失组播报文不是很敏感。然而对于数据组播应用来说，组播的可靠性是十分重要的。如组播报文差错恢复、所有组播接收者收到的报文数量一致、顺序一致、实时性等。这方面的研究是一个热点，目前还没有统一的标准， IETF正在努力推出标准，也有很多组织在积极地开发自己的协议。常见协议有： SRM、 MDR、 Bimodel Multicast等。

可靠组播的应用前景是非常广泛的，在可靠的媒体流发布、经卫星信道的信息发布、机场空中管制系统、股票行情的发布、大型分布式网站的数据更新、分布式数据库的同步、分布式对象间消息的传递、军事战场指挥系统，甚至网络游戏等，都有这一技术的应用领域。

组播技术应用现状与未来

着眼于组播技术良好的表现和广阔的应用前景，许多服务提供商先行一步，获利不菲。意大利的 FastWeb、香港的香港宽带（ HKBN）、瑞典的 Bredbandsbolaget（ B2）就是其中的佼佼者。一般运营商提供电话会议、电视和视频点播服务，向商业用户提供视频会议和其他视频流服务。在实践中，组播情况下可以向 3万个用户传送电视节目，而不会引起网络流量的激增。如果使用单播技术，所需的网络带宽是难以想象的。

目前， IP组播技术在商业应用中还面临着一些需要解决的问题，如组播服务的收费方式和方法；组播网络的监控；组播成员的身份认证；如何保证组播的 QoS；采用何种商业模式向用户推销组播服务等。但可以预见的是，人们日益认识到组播技术所带来的优点和长处，组播技术必将成为人们工作和生活中不可缺少的网络技术之一。

- ICMP：关闭时无法进行 PING的操作，即别人无法用 PING的方法来确定你的存在。当有 ICMP数据流进入机器时，除了正常情况外一般是有人利用专门软件进攻你的机器，这是一种在 Internet上比较常见的攻击方式之一。 主要分为 Flood攻击和 Nuke攻击两类。 ICMP Flood攻击通过产生大量的 ICMP数据流以消耗您的计算机的 CPU资源和网络的有效带宽，使得您的计算机服务不能正常处理数据，进行正常运作； ICMP Nuke攻击通过 Windows的内部安全漏洞，使得连接到互联网络的计算机在遭受攻击的时候出现系统崩溃的情况，不能再正常运作。也就是我们常说的蓝屏炸弹。该协议对于普通用户来说，是很少使用到的，建议关掉此功能。
- IGMP：和 ICMP差不多的协议，除了可以利用来发送蓝屏炸弹外，还会被后门软件利用。当有 IGMP数据流进 入你的机器时，有可能是 DDOS的宿主向你的机器发送 IGMP控制的信息，如果你的机器上有 DDOS的 Slave软件，这个软件在接收到这个信息后将会对指定的网站发动攻击，这个时候你的机器就成了黑客的帮凶。
- TCP监听：关闭时，你机器上所有的 TCP端口服务功能都将失效。这是一种对付特洛依木马客户端程序的有效方法，因为这些程序也一种服务程序，由于关闭了 TCP端口的服务功能，外部几乎不可能与这些程序进行通讯。而且，对于普通用户来说，在互联网上只是用于 WWW浏览，关闭此功能不会影响用户的操作。但要注意，如 果你的机器要执行一些服务程序，如 FTP SERVER、 HTTP SERVER时，一定要使该功能正常，而且，如果你用 ICQ来接受文件，也一定要将该功能正常，否则，你将无法收到别人的 ICQ信息。另外，关闭了此功能后，也可以防止大部分的端口扫描。
- UDP监听：失效时，你机器上所有的 UDP服务功能都将失效。不过好象通过 UDP方式来进行蓝屏攻击比较少见，但有可能会被用来进行激活特洛依木马的客户端程序。注意，如果你使用了 ICQ，就不可以关闭此功能。
- NETBIOS：有人在尝试使用微软网络共享服务端口（ 139）端口连接到您的计算机，如果您没有做好安全措施，可能是在你自己不知道和并没有允许的情况下，你的计算机里的私人文件就会在网络上被任何人在任何地方进行打开、修改或删除等操作。将 NETBIOS设置为失效时，你机器上所有共享服务功能都将

关闭，别人在资源管理器中将看不到你的共享资源。注意：如果在失效前，别人已经打开了你的资源，那么他仍然可以访问那些资源，直到他断开了这次连接。

建议：在局域网中打开该功能，在互联网关闭。