基于 ICE 方式 H.323 信令穿越 Symmetric NAT 技术研究

陈晓铭　吴中福　陈　蕾
（重庆大学计算机学院　重庆 400044）

摘　要　基于 IP 的数据、语音、视频等业务在 NGN 网络中所面临的一个实际困难就是如何有效地穿越各种 NAT/FW 的问题。对此，H.323 协议以往的解决方法有 ALGs，STUN，TURN 等方式。本文探讨了一种新的 H.323 信令穿越 NAT/FW 的解决方案—交互式连通建立方式(ICE)。它通过综合利用现有协议，以一种更有效的方式来组织会话建立过程。并设计一个实例针对 H.323 信令协议穿越 Symmetric NAT 流程进行了描述，最后总结了 ICE 的优势及应用前景。

关键词　Symmetric NAT，H.323，STUN，TURN

Research of H.323 Signal Traverse Symmetric NAT Based-ICE

CHEN Xiao-Ming　WU Zhong-Fu　CHEN Lei
(Institute of Computer，ChongQing University，ChongQing 400044)

Abstract　In NGN Network，date，voice，video stream of Based-IP confront a fact difficulty that how to traverse efficient all kinds of NAT or FW. Generally resolve method of H.323 protocol include ALGS，STUN，TURN etc. This paper discuss a new resolve method—Interactive Connectivity Establishment(ICE) that it establish session efficienter by synthetizing other protocols's strongpoint and Design an example to illustrate the flow of H.323 protocol's signal traverse symmetric NAT，at last summarize ICE'S advantage and foreground of application.

Keywords　Symmetric NAT，H.323，STUN，TURN

1　问题背景

在 IP 语音和视频通讯中 NAT(网络地址转换)问题是常见的问题。一个 NAT 设备允许一个公司为局域网上设备分配私有的 IP 地址。不幸的是控制 Internet 上信息流向的路由设备仅仅能把数据送到具有可路由 IP 地址(公众 IP 地址)的设备。NAT 后的终端可以向位于相同局域网上的任何别的终端发起呼叫，因为在局域网内的这些 IP 地址是可路由的，然而他们的 IP 地址是私有的，对局域网外来说是不可路由的，因此 NAT 后的终端不能接收局域网外终端的呼叫。因此，如何穿越 NAT 是 H.323 体系需要解决的问题之一。

NAT 仍是解决当前公用 IP 地址紧缺和网络安全问题的最有力手段，它主要有四种类型：完全圆锥型 NAT(Full Cone NAT)，地址限制圆锥型 NAT(Address Restricted Cone NAT)，端口限制圆锥型 NAT(Port Restricted Cone NAT)，对称型 NAT(Symmetric NAT)。前三种 NAT，映射与目的地址无关，只要源地址相同，映射就相同，而对称型 NAT 的映射则同时关联源地址和目的地址，所以穿越问题最为复杂。

不少方案已经被应用于解决穿越 NAT 问题，例如：ALGs(Application Layer Gateways)、Middlebox Control Protocol、STUN(Simple Traversal of UDP through NAT)、TURN(Traversal Using Relay NAT)、RSIP(Realm Specific IP)、symmetric RTP 等。然而，当这些技术应用于不同的网络拓扑时都有着显著的利弊，以至于我们只能根据不同的接入方式来应用不同的方案，所以未能很好地解决 All-NAT 与 Efficiency 的问题，同时还会给系统引入了许多复杂性和脆弱性因素。所以我们目前需要一种综合的足够灵活的方法，使之能在各种情况下对 NAT/FW 的信令穿越问题提供最优解。事实上，ICE 正是符合这样要求的一种良好的解决方案。

2　ICE 技术

2.1　ICE 简介

交互式连通建立方式 ICE(Interactive Connectivity Establishment)并非一种新的协议，它不需要对 STUN、TURN 或 RSIP 进行扩展就可适用于各种 NAT。ICE 是通过综合运用上面某几种协议，使之在最适合的情况下工作，以弥补单独使用其中任何一种所带来的固有缺陷。

2.2　多媒体信令

媒体流穿越 NAT 的过程是独立于某种具体的信令协议的。通信发生在两个客户端—主叫端和被叫端。初始化报文(Initiate Message)包含了描述主叫端媒体流的配置与特征，并经过信令调停者(也叫信令中继)，最后到达被叫端。假设被叫端同意通信，接受报文(Accept Message)将产生并反馈至主叫端，媒体流建立成功。此外，信令协议还对媒体流参数修改以及会话终止报文等提供支持。对于 H.323，初始化报文对应 H.225.0 的 Setup，接受报文对应于 H.225.0 的 Connect，终止报文对应于 Release。

2.3　算法流程

2.3.1　收集传输地址　主叫端需要收集的对象包括本地传输地址(Local Transport Address)和来源传输地址(De-

陈晓铭　硕士研究生，主要研究方向：计算机网络与多媒体通信。吴中福　教授，博士生导师，主要研究方向：计算机网络与通信，现代远程教育技术。陈蕾　硕士研究生。

rived Transport Address)。本地传输地址通常由主机上一个物理(或虚拟)接口绑定一个端口而获得。主叫端还将访问提供 UNSAF(Unilateral self-address fixing)的服务器,例如 STUN、TURN 或 TEREDO。对于每一个本地传输地址,会话者都可以从服务器上获得一组来源传输地址。

显然,实现物理或虚拟连通方式越多,ICE 将工作得越好。但为了建立对等通信,ICE 通常要求至少有一个来源地址由位于公网上的中继服务器(如 TURN)所提供的,而且需要知道具体是哪一个来源传输地址。

2.3.2 *启动 STUN* 主叫端获得一组传输地址后,将在本地传输地址启动 STUN 服务器,这意味着发送到来源地址的 STUN 服务将是可达的。与传统的 STUN 不同,客户端不需要在任何其它 IP 或端口上提供 STUN 服务,也不必支持 TLS,ICE 用户名和密码已经通过信令协议进行交换。

客户端将在每个本地传输地址上同时接受 STUN 请求包和媒体包,所以发起者需要消除 STUN 报文与媒体流协议之间的歧义。在 RTP 和 RTCP 中实现这个并不难,因为 RTP 与 RTCP 包总是以 0b10(v=2)打头,而 STUN 是 0b00。对于每个运行 STUN 服务器的本地传输地址,客户端都必须选择相应的用户名和密码。用户名要求必须是全局唯一的,用户名和密码将被包含在初始化报文里传至响应者,由响应者对 STUN 请求进行鉴别。

2.3.3 *确定传输地址的优先级* STUN 服务器启动后,下一步就是确定传输地址的优先级。优先级反映了 H.323 终端在该地址上接收媒体流的优先级别,取值范围在 0 到 1 之间,通常优先级按照被传输媒体流量来确定。流量小者优先,而且对于相同流量者的 Ipv6 地址比 Ipv4 地址具有更高优先级。因此物理接口产生的本地 Ipv6 传输地址具有最高的优先级,然后是本地 Ipv4 传输地址,然后是 STUN、RSIP、TEREDO 来源地址,最后是通过 VPN 接口获得的本地传输地址。

2.3.4 *构建初始化报文(Initiate Message)* 初始化报文由一系列媒体流组成,每个媒体流都有一个缺省地址和候选地址列表。缺省地址通常被 Initiate 报文映射到 H.323 信令传递地址上,而候选地址列表用于提供一些额外的地址。对于每个媒体流来说,任意 Peer 之间实现最大连通可能性的传输地址是由公网上转发服务器(如 TURN)提供的地址,通常这也是优先级最低的传输地址。客户端将可用的传输地址编成一个候选地址列表(包括一个缺省地址),并且为每个候选元素分配一个会话中唯一的标识符。一旦初始化信息生成后即可被发送。

2.3.5 *响应处理:连通性检查和地址收集* 被叫端接收到初始化报文 Initiate Message 后,会同时做几个事情:首先,执行 2.3.1 中描述的地址收集过程。这些地址可以在呼叫到达前预收集,这样可以避免增加呼叫建立的时间。当获得来源地址以后,应答方会发送 STUN Bind 请求,该请求要求必须包含 Username 属性和 Password 属性,属性值为从“alt”中得到的用户名和密码。STUN Bind 请求还应包括一个 Message-Integrity 属性,它是由 Initiate Message 中候选元素的用户名和密码计算得来的。此外,STUN Bind 请求不应有 Change-Request 或 Response-Address 属性。

当一个客户端收到 Initiate Message 时,它将通过其中缺省地址和端口发送媒体流。如果 STUN Bind 请求报文引起错误应答,则需要检查错误代码。如果是 401,430,432 或 500,说明客户端应该重新发送请求。如果错误代码是 400,431 和 600,那么客户端不必重试,直接按超时处理即可。

2.3.6 *生成接受报文(Accept Message)* 应答者可以决定是接受或拒绝该通信,若拒绝则 ICE 过程终止,若接受则发送 Accept 报文。Accept 报文的构造过程与 Initiate Message 类似。

2.3.7 *接受报文处理* 接受过程有两种可能。如果 Initiate Message 的接受者不支持 ICE,则 Accept Message 将只包含缺省的地址信息,这样发起方就知道它不用执行连通性检查了。然而如果本地配置信息要求发起者通过 TURN 服务器发包来进行连通性检查,这将意味着那些直接发给响应者的包会被对方防火墙丢弃。为解决这个问题,发起者需要重新分配一个 TURN 来源地址,然后使用 Send 命令。一旦 Send 命令被接受,发起者将发送所有的媒体包到 TURN 服务器,由服务器转发至响应者。如果 Accept Message 包含候选项,则发起方处理 Accept Message 的过程就与响应方处理 Initiate Message 很相似了。

2.3.8 *附加 ICE 过程* Initiate 或 Accept 报文交换过程结束后,双方可能仍将继续收集传输地址,这通常是由于某些 STUN 事务过长而未结束引起,另一种可能是由于 Initiate/Accept 报文交换时提供了新的地址。

2.3.9 *ICE 到 H.323 的映射* 使用 ICE 方式穿越 NAT,必须映射 ICE 定义的参数到 H.323 报文格式中,同时对 Setup 报文进行简单扩展-在 Setup 报文中增加一个新的信息元素“Alternate Address”来支持 ICE。它包含一个候选 IP 地址和端口,Setup 可能包含多个 Alternate Address 信息元素,这时每个 Alternate Address 信息元素应该包括不重复的 IP 地址和端口。

3 实例设计

3.1 Symmetric NAT/FW

下面设计一个简化的基于 ICE 的对称式网络地址转换/防火墙(Symmetric NAT/FW)的穿越实例,进一步说明 ICE 的工作流程。

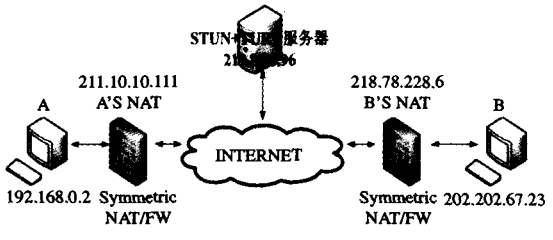


图 1 Symmetric NAT/FW 网络拓扑图

假设通信双方同时处于对称式 NAT/FW 内部,现在 H.323 终端 A 要与 B 进行 VoIP 通信。A 所在的内部地址是 192.168.0.2,外部地址是 211.10.10.100;B 的内部地址是 202.202.67.23,外部地址是 218.78.228.6;STUN/TURN 服务器的地址是 219.8.25.96。

首先 A 发起请求,进行地址收集,如图 2 所示。生成 A 的 Initiate Message 如下:

```
.....
alt;1 1.0 ; user 9kksj== 192.168.0.2 1010
alt;2 0.8 ; user1 9kksk== 211.10.10.100 9988
alt;3 0.4 ; user2 9kksl== 219.8.25.96 8076
```

其中本地地址的优先级为 1.0,STUN 地址的优先级为 0.8,

TURN 地址优先级为 0.4。当 B 收到报文后，也进行地址收集，过程和 A 类似。

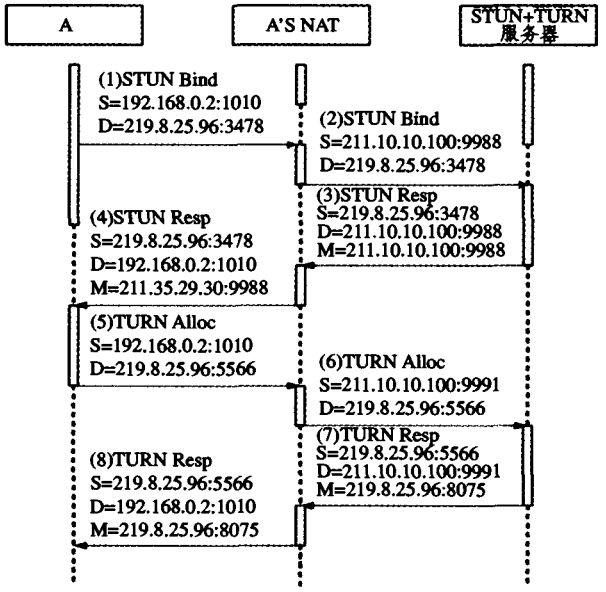


图 2　A 的地址收集过程时序图

然后 B 开始执行连通性检查，如图 3 所示。可是我们不难发现，到 192.168.0.2:1010 的 STUN 请求和到 211.10.10.100:9988 的 STUN 请求都将不可避免地失败。因为前者是一个不可路由的保留地址；而后者由于 Symmetric NAT 会对于每一个 STUN/TURN 请求都将分配不同的 Binding，当数据包抵达 A 的 NAT 时，NAT 会发现传输地址 211.10.10.100:9988 已经映射 219.8.25.96:3478 了。而此时 STUN 请求的源地址并非 219.8.25.96:3478，所以数据包必然会被 A 的 NAT/FW 所丢弃。然而，到 219.8.25.96:8076 的 STUN 请求却是成功的，因为 TURN 服务器用它收集到的原始地址来发送 TURN 请求。

完成连通性检查后，B 产生应答报文，当 A 收到应答后，它也执行连通性检查，过程和 B 的连通性检查类似。和前面一样，对于 B 的私有地址和 STUN 来源地址的连通性检查结果均为失败，而到 B 的 TURN 来源地址和到 B 的 peer-derived 地址成功（本例中它们都具有相同的优先级 0.4）。相同优先级下我们通常采用 peer-derived 地址，所以 A 发送到 B 的媒体流将使用 219.8.25.96:5556 地址，而 B 到 A 的媒体流将发送至 219.8.25.96:8076 地址。以上为基于 ICE 方式解决 Symmetric NAT/FW 穿越问题的一个简化后的典型实例。

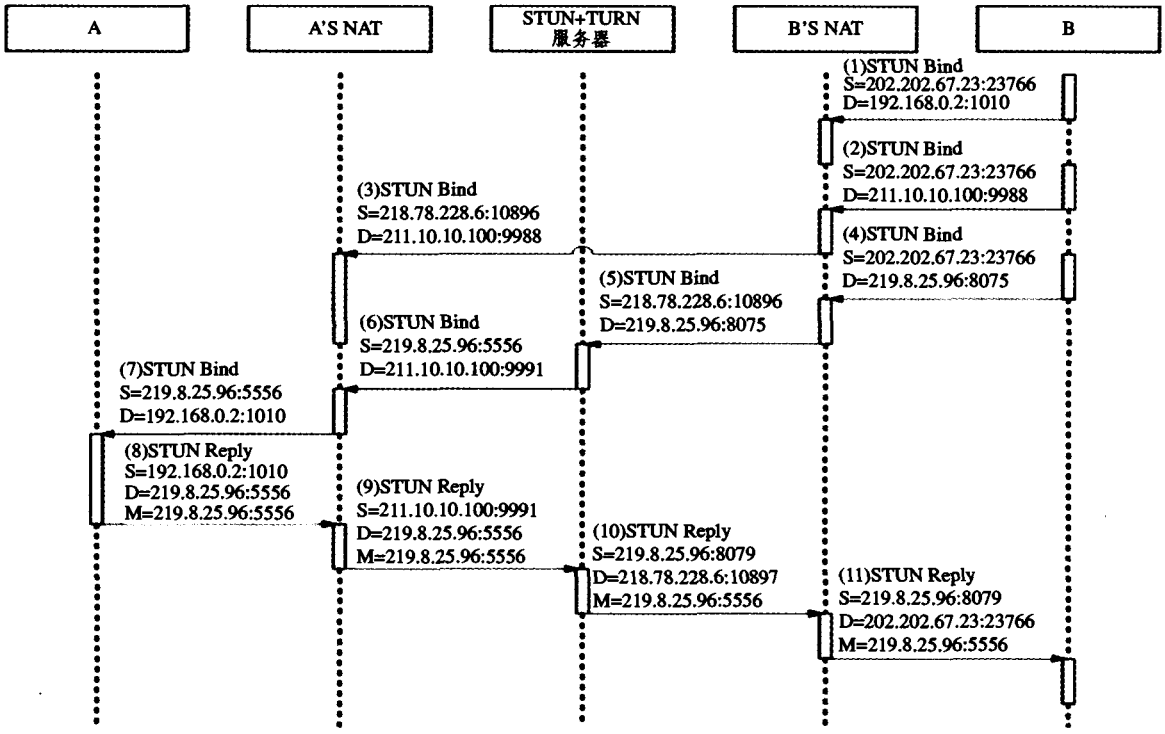


图 3　B 的连通性检查

3.2　其它类型 NAT/FW

基于 ICE 实现其它类型的 NAT/FW 穿越问题，其过程比 Symmetric NAT 还要简单，见参考文[1,2,6]。

结束语　ICE 方式的优势是显而易见的，它消除了现有的 UNSAF 机制的许多脆弱性。例如传统的 STUN 有几个脆弱点，其中一个就是发现过程需要客户端自己去判断所在 NAT 类型，这实际上不是一个可取的做法。而应用 ICE 之后，这个发现过程已经不需要了。另一点脆弱性在于 STUN、TURN 等机制都完全依赖于一个附加的服务器，而 ICE 利用服务器分配单边地址的同时，还允许客户端直接相连，因此即使 STUN 或 TRUN 服务器中有任何一个失败了，ICE 方式仍可让呼叫过程继续下去。此外，传统的 STUN 最大的缺陷在于它不能保证在所有网络拓扑结构中都正常工作，最典型的问题就是 Symmetric NAT。对于 TURN 或类似转发方式工作的协议来说，由于服务器的负担过重，很容易出现丢包或者延迟情况。而 ICE 方式正好提供了一种负载均衡的解决方案，它将转发服务作为优先级最低的服务，从而在最大程度上保证了服务的可靠性和灵活性。此外，ICE 的优势还在于对 Ipv6 的支持，目前 Cisco 等公司正在设计基于 ICE 方式的 NAT/FW 解决方案。由于广泛的适应能力以及对未来网络

的支持，ICE作为一种综合的解决方案将有着非常广阔的应用前景。

参考文献

1 Rosenberg J. Interactive Connectivity Establishment (ICE): A Methodology for Nettwork Address Translator(NAT) Traversal for the Session Initiation Protocol(SIP). draft-rosenberg-sipping-ice-01(work in progress), July 2003

2 Rosenberg J, Schulzrinne H, Camarillo G, et al. SIP: Session Initiation Protocol. RFC 3261, June 2002

3 Rosenberg J, Schulzrinne H. An Extension to the H. 323 for Symmetric Response Routing, RFC 3581, August 2003

4 Rosenberg J, Weinberger J, Huitema C, Mahy R. STUN - Simple Traversal of User Datagram Protocol(UDP) Through Network Address Translators(NATs). RFC 3489, March 2003

5 Rosenberg J. Traversal Using Relay NAT(TURN), draft-rosenberg-midcom-turn-02(work in progress), October 2003

6 Rosenberg J. Examples of Network Address Translation(NAT) and Firewall Traversal for the Session Initiation Protocol(SIP), draft-rosenberg-sipping-nat-scenarios-01

7 刘杨，姜琳颖，王中. 基于ICE方式的SIPNAT解决方案研究. 见：中科院第八届计算机科学与技术学术 研讨会论文集[C]，2004

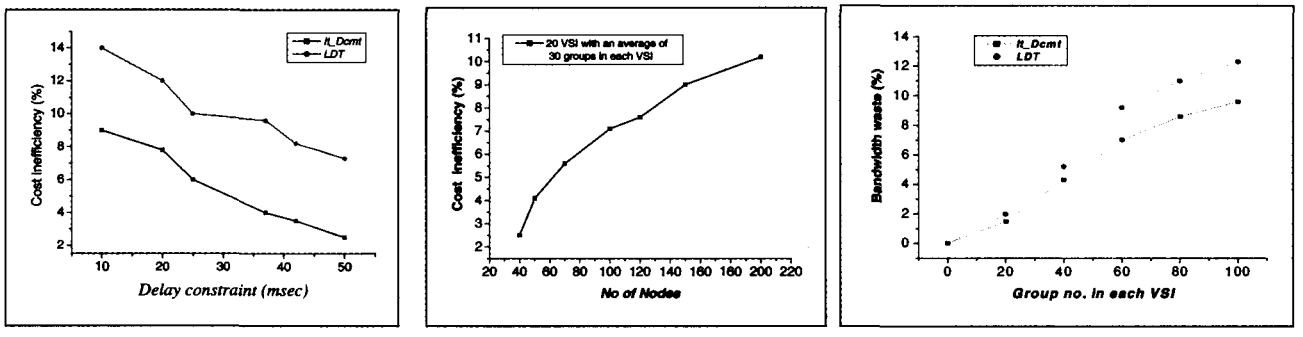
(上接第27页)

4.2 实验仿真

为了评估算法1的性能，VPLS网络采用Waxman所建议的拓扑随即生成模型[10,11]。确定两结点(u,v)间是否存在链路的概率函数由 $P(u,v)=\beta\exp(\frac{-d(u,v)}{aL})$ 定义，$d(u,v)$为结点u和v之间的距离。我们评估三种类型的VPLS网络，其结点数分别为50，100和200。同时为了评估采用了时延约束机制后给网络带来的额外开销，我们还定义了开销失效度(Cost inefficiency)：

$$inefficiency=\frac{Cost(T_{iter})-Cost(T_{LCT})}{Cost(T_{LCT})} \quad (5)$$

其中，$Cost(T_{LCT})$是用最小生成树作为洪泛树的开销，$Cost(T_{iter})$是算法1生成的洪泛树的开销。该式用作评估此条件下网络开销增加的百分比。时延约束参数则是由$\Delta v=d(P(s,v))\times\delta, v\in V$定义。我们发现，时延约束机制越严格，开销失效度就增大，意味着网络中将需要分配更多的资源来满足时延的约束。但是，算法1所生成的洪泛树造成的开销失效度要优于直接使用LDT，见图3(a)。另外，开销失效度还与网络的规模有一定的关系，在50个结点的网络中为2.7%，100个结点的网络中为4.5%，150个结点的网络中则达到了6.8%，见图3(b)。图3(c)则是为了证实剪枝机制的必要性。在50个结点、20个VPLS虚拟转发实例的网络中，设定bth为10%。图中表明，用算法1生成的洪泛树要优于直接使用LDT。实验过程中，剪枝机制并没有触发。因此，各个结点中维护的组播转发状态很少，因而开销也大大地减少。可以肯定，通过洪泛树和剪枝机制的结合，可以在城域以太网中取得较好的性能。



(a) (b) (c)

图3 实验

结束语 VPLS域中的组播是近期的研究热点。本文通过迭代法生成具有时延约束机制的组播洪泛树，并结合基于消息的剪枝机制完成VPLS域中组播的处理。这种处理机制充分的结合了VPLS网络的特点，从实际应用和实现的角度出发，建立具有时延约束机制的组播转发机制。同时为了抑制组播带来的网络开销，提出了一种较好的折中处理机制。文中算法的时间复杂度为$O(n^2)$，因此易于实现，适合城域以太网中VPLS的组播处理。

参考文献

1 Cormen T H, et al. Introduction to Algorithms. MIT Press, Cambridge, MA: 1990

2 Kabada B K, Jale J M. Routing to multiple destinations in computer networks. IEEE trans. Commun, 1983. 31～3

3 Estrin, D, et al. Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification, RFC 2362. June 1998

4 Aggarwal R, Morin T, Fang L. Multicast in BGP/MPLS VPNs and VPLS. work in progress, draft-raggarwa-l3vpn-mvpn-vpls-mcast-01. txt, 2004

5 Lasserre M, Kompella V. Virtual Private LAN Services over MPLS. work in progress, draft-ietf-l2vpn-vpls-ldp-06. txt, 2005

6 Serbest Y, Qiu R, Hemige V, Nath R. Supporting IP Multicast over VPLS. work in progress, draft-serbest-l2vpn-vpls-mcast-01. txt, 2004

7 Sajassi A, Salama H. VPLS based on IP Multicast. work in progress, draft-sajassi-mvpls-00. txt. 2002

8 Williamson B. Developing IP Multicast Networks, Volume I. Cisco press, 2000

9 Knuth D E. The Art of Computer Programming, Vol 3. London: Addison-Wesley Publishing Company, 1973

10 Waxman B M. Routing of multipoint connections. IEEE Journal of Selected Area in Communications, 1998. 1617～1622

11 Salama H F, Reeves D S, Viniotis Y. Evaluation of multicast routing algorithms for real-time communication on high-speed networks. IEEE JSAC, 1997, 15-3: 332～345

12 Kuipers F, Van M P. MAMCRA: A constrained-based multicast routing algorithm. Computer communications 25, 2002

13 Dong Ximing, Yu Shaohua . VPLS: An Effective Technology for Building Scalable Transparent LAN Services. In: Proceedings of SPIE, Network architectures, management, and applications II. 2004. 137～147

14 Fei Aiguo, Cui Junhong, Gerla M, Faloutsos M. Aggregated Multicast: an Approach to Reduce Multicast State. In: Proc. IEEE Global Internet (GLOBECOM'01), 2001