文章编号：1005-8451（2004）02-0014-03

铁路对外服务系统可靠性网络设计与实现

田绵石
（铁道部 信息技术中心，北京 100844）

摘 要：研究分析目前铁路对外服务系统在实现可靠性网络连接中所面临的技术难题，设计并实现以多宿主方案为基础的高可靠性网络系统。

关键词：铁路对外服务系统；可靠性网络；多宿主；智能NAT；DDNS
中图分类号：TP393 文献标识码：A

Design and implementation of reliable networks for Railways External Services System

TIAN Mian-shi
(Information Technology Center of Ministry of Railways, Beijing 100844, China)

Abstract: It was examined and analyzed the inevitable technical problems involved when implementing reliable network connection for Railways External Services System, Designed and developed a high reliable network system based on the multi-homed connections.

Key words: Railways External Services System; reliable networks; multi-homed; smart NAT; DDNS

为了提高铁路系统的运输竞争力和社会影响力，铁道部、各铁路局都在利用互连网来组建自己的铁路对外服务网络系统，即通过部属电子商务网站、铁路门户网站等WWW服务器群，利用ISP提供的互连网线路向各界提供铁路运输业务信息和铁路宣传信息，同时为铁路内部员工提供访问互连网的服务。这种铁路对外服务系统对业务的不可中断性的要求越来越高。为了保证对外服务业务的可用性，保持铁路行业的社会形象，要求该网络系统做到7*24 h的连通，并发挥网络线路的最大利用率，让各界用户能够在任意时刻以最快方式访问到铁路的对外服务系统，同时保证铁路内部员工能够在任意时刻以最快方式访问到互连网。

1 可靠性网络需求分析

目前，铁路的对外服务网站大多采用一条Internet接入，即使用1个ISP的链路。所有铁路内部用户收发邮件，访问Internet资源，以及社会用户访问对外服务网络中的WEB服务器，都要通过这条Internet链路，这条链路经常会出故障而中断，影响了内部用户收发外部电子邮件及对Internet的访问和社会用户对铁路WEB服务器的访问。

为社会客户提供不间断的内容和服务是至关重要的。一个网站不仅需要保证网站内所有的WEB服务器、应用服务器和数据库服务器的高可用性，还要保证Internet接入的可靠性和稳定性。显然，一个ISP无法保证它提供的Internet链路的持续可用性，从而可能导致对外服务系统的网站与Internet接入的中断，对用户和铁路则意味着巨大的损失。

在此引入“多宿主”（Multi-Homed）的概念，即通过采用多宿主的解决方案来避免Internet接入中断所造成的损失。在这里所提及的“多宿主”方案指同时使用不同ISP（至少2个）提供的多条Internet接入链路。可用性的提高来自于多条链路的使用，而性能提高则是因为同时使用多条链路增加了带宽。采用多宿主接入Internet的方案要实现的目标是将多条接入链路的带宽累加，同时使用，不分主干线路、备份线路；每一条线路为另外的线路做容错；任何一条线路出现问题，另一条线路会自动接管，消除单点故障；实现数据的就近访问，数据流入和流出信息平台时都会选择最佳路径；保证对外发布的服务如WWW、FTP、EMAIL等网络应用不会因为一条链路的中断而中断，实现了服务的永远在线和性能优化。

2 多宿主方案所面临的技术问题

收稿日期：2003-07-10
作者简介：田绵石，工程师。

多宿主方案能够提高铁路对外服务网络的可用性和性能，但这种方案也面临着特殊的问题和挑战。铁道部对外服务网络有2条Internet接入，一条通过ISP1，另一条通过ISP2。这样的网络结构看起来很普通，但是仔细分析之后就会发现一些问题。

首先是IP地址管理的问题。

可能会采用2种IP地址管理方式：提供对外服务的各个网站(Server)使用同一个子网地址。采用这种方式需要2个ISP之间相互配合协作，以便在Internet网络上发布到达该网段的正确路由信息；多个ISP分配给对外服务的各个网站不同的地址段。这种方式下，各个网站要同时使用2个地址段的IP地址。

对第一种方式来说，2个ISP之间必须相互配合协作，以便在Internet网络上发布到达该网段的正确路由信息，并且还要保证2条链路的双向同时使用。尤其对于入站流量（从Internet到网站）来说，如果不能保证链路的同时使用，多宿主解决方案的部分优点就无法实现。

对于第二种方式（目前使用较多的解决方式），内部网络（包含网站和内部上网用户）同时使用2个ISP提供的地址，一部分内部用户（A组）使用ISP1提供的地址，另一部分内部用户（B组）使用ISP2提供的地址。问题在于出站的（从该网络去Internet）流量处理，当ISP1的链路中断时，A组的用户将无法访问Internet。更进一步，如果提供对外服务的网站只使用其中一组的地址（如B组），则ISP1的链路无法用于流入的流量，因为只有ISP2提供的链路是通过Internet能流入该网络能访问该网站的唯一路径。例如，网络中有一个WEB服务器供Internet用户访问，如何注册该服务器的地址？如果只使用一个ISP的地址，则ISP链路中断时，用户将无法访问该服务器。

如果为对外服务的网站注册多个ISP所提供的公网地址，那么在Internet较高级别的DNS服务器的数据库中会有多个A记录，即同样一个网站域名对应多个IP地址。当Internet用户访问网站时，该较高级别的DNS将优先选择排在最前面的地址记录，此时与ISP的连接可能已经中断，但域名解析是成功的，此时用户仍然无法访问网站。

其次，多宿主解决方案面临的不仅仅是地址管理问题。使用BGP作为路由器之间进行可用性和可达性通信的机制，则只能处理入站的流量，同样无法动态处理，并且管理维护费用高昂。

除去以上的问题，多宿主网络的一些优势还没有完全实现，例如：

（1）多条ISP链路采用“冷备份”的方式，通常只能使用一条链路，当该链路发生问题时，必须人工进行切换。一方面人工切换有一定的时间延迟，另一方面需要每天安排人员，24 h值班，不仅链路没有得到充分利用，还带来许多管理上的负担和不便，无法保证网络的持续连接。

（2）多条ISP链路分别传送不同种类的网络流量。通常的情况是一条链路负责内网向外网的访问，另一条链路负责外网向内网的访问，这种方法从一定程度上提高了链路的利用率，但可靠性问题无法保证。例如，一条链路发生问题时，某个方向的流量就完全中断了。当然，这时可以将所有流量切换到另外一条链路，但这时和第一种情况面临同样的问题，而且由于需要重新配置，切换时间比第一种情况更长。此外，在这种情况下经常出现流量严重不均衡的情况，一条链路可能非常繁忙，速度极慢，而另一条链路此时可能基本处于空闲状态。

3　解决办法

采用多宿主方案，需要引入动态链路均衡功能和智能NAT功能，同时调整网络结构和DNS部署方案。

目前网络产品中能够实现动态链路均衡功能的产品比较多，统称为链路均衡器，多个链路均衡器还能实现集群功能，避免链路均衡器自身单点失效。

图1为多宿主对外服务网络系统通过ISP1和ISP2接入Internet的示意图。每个ISP都分配给该网络一个IP地址网段。

为了实现前面所述的方案目标，网络结构做如下调整：

（1）在接入路由器和外网防火墙之间部署链路均衡器（单机或双机HA）；

（2）外网防火墙工作在透明模式或路由模式（适用于多网段），不启用NAT，而由链路均衡器完成智能NAT功能；

（3）各个上网PC机和对外服务器（门户网站、DNS、电子商务、邮件服务器等）通过一个3层或2层交换机与外网防火墙连接，并根据具体需求分属于防火墙不同的Security Zone，防火墙对不同Zone之间做严格地访问控制策略；

（4）网络中的PC机和对外服务器都属于私有网段10.1.0.0/16。

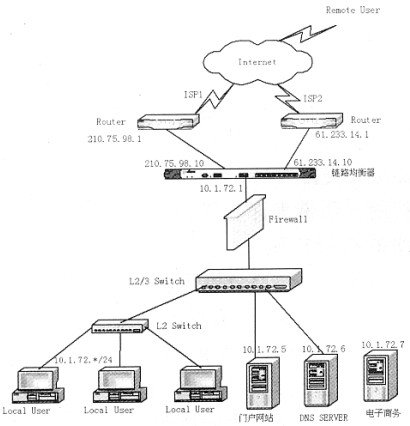

图1 多宿主对外服务网络系统

流出（Outbound）流量处理：对于流出的流量，链路均衡器使用智能NAT的算法，即当选定一个路由器（某一个ISP）传送流出流量时，链路均衡器将选择该ISP提供的地址。在图1中，如果链路均衡器选择ISP1作为流出流量的路径，则它将把内部的PC机地址10.1.X.X/16翻译为61.233.14.10/27，并作为流出数据包的源地址。同样，如果链路均衡器选择ISP2作为流出流量的路径，则它将把内部的主机地址翻译为210.75.98.10/24，并作为流出数据包的源地址。

为了优化流出的流量，链路均衡器还为流出的流量，实施就近性运算。如果内部PC机要访问某一Internet站点，可能通过某一个ISP的路径比通过其他ISP的路径有效。因此，链路均衡器根据路由的跳数、路径的延迟和负载状况来进行对每个目的地的就近性运算，选择最佳的流出流量传输路径。

流入（Inbound）流量处理：对于流入的流量，即社会上Internet用户访问铁路对外服务网络中的门户网站服务器、电子商务服务器等，其技术难点是域名解析。

一般情况下，铁路对外服务网络系统中的，各个服务器的域名解析任务由本地DNS服务器完成，或委托一家可靠的ISP代为完成。在本文多宿主的方式下，DNS部署方案要做如下调整：从2个ISP所提供的公网地址池中各拿出一个地址，比如61.233.14.11/27和210.75.98.11/24，在到域名注册机构注册DNS Server时就可以把NS记录注册为这2个公有的IP。采用2条NS记录分别是2个ISP的IP地址，目的是可以在一条ISP链路失效时，Internet用户的DNS请求能够通过另一条ISP到达链路均衡器。为了尽量缩短由于ISP链路中断而引起的DNS请求延迟的时间，要把DNS的TTL值设为0或1，这样用户就不会使用DNS的缓存。

链路均衡器在接到用户的DNS请求后会采用如下的2种方式之一来完成最后的DNS解析任务：

（1）链路均衡器直接完成最后的DNS解析任务

在链路均衡器上增加A记录，如A www.sinorail.com 10.1.72.5，和2条Static Nat：NAT1 10.1.72.5 210.75.98.11；NAT2 10.1.72.5 61.233.14.11，当链路均衡器接收到Internet用户的www.sinorail.com DNS请求时，链路均衡器根据此时这2条ISP线路的通断情况和负载情况回应用户一个最优的IP地址，从而完成流入流量的负载均衡。

（2）本地DNS服务器采用DDNS技术完成最后的DNS解析任务

在链路均衡器上增加2条Static Nat：NAT1 10.1.72.6 210.75.98.11；NAT2 10.1.72.6 61.233.14.11，当链路均衡器接收到Internet用户的www.sinorail.com DNS请求时通过Static Nat将请求转交给内部的本地DNS服务器。将本地DNS服务器升级到可以支持动态DNS更新的DNS服务器（DDNS，RFC2136），链路均衡器将根据链路状态对这台DNS服务器的地址记录进行安全的动态更新，使DNS服务器始终回应给用户较快的链路所对应的IP地址。

4 结束语

采用上述方案可以在很大程度上提升对外服务网络的可靠性，能够解决流入流量和流出流量的实时备份和负载均衡问题。为了使对外服务网络系统达到或接近关键商业网站的运行级别，还可以在上述方案的基础上采用防火墙的集群功能，以及引入4层交换机实现服务器群的内容负载均衡，进一步消除单点失效。

参考文献：

[1] 范宏伟、须 德. Intranet防火墙和安全[J]. 铁路计算机应用，1998，7（6）.

[2] 高健媛、华 勇、韩 臻，等.网络地址转换的应用及其局限性分析[J]. 铁路计算机应用，2002，11（5）.

[3] P. Vixie, Jim Bound. Dynamic Updates in the Domain Name System (DNS UPDATE)[J]. RFC2136, April 1997.