IDC 双线路网络方案

摘要：

由于中国电信和中国联通分别运营南方 21 省及北方 10 省互联网骨干网，运营商之间的网络访问瓶颈导致在南方和北方的网站互访速度非常缓慢，地处中国电信的**省广电网站一直深受此困扰。**省广电网站以视频新闻为主要宣传特色，绝对**、名师**全国选秀类节目会让网站访问量突起，每逢此时中国北方网络用户访问**省广电网站就会遭受严重的网络瓶颈制约。如果长此下去网站的事业传播与发展必会受到影响，在这种情况下，采用 IDC 双线路技术同时接入中国电信和中国联通已经成为解决问题的必要手段。本文作者利用**省广电城将即将投入使用的之际，利用**省广电的 IDC 机房机会提出了 IDC 双线路的解决方案。本文对 IDC 双线路关键技术进行了概述，然后着重介绍了根据防火墙接口地址制定策略路由、实现双线路的方法。

全文：

新落成的**省广电城于 2008 年 10 月投入使用，其中 IDC 机房建设子项目主要是为了满足各类服务器、交换机、路由器等设备的放置、内部人员使用网络等需求。该项目分为机房装修、机房电源建设、综合布线、送风和空调系统的建设、应用服务器建设等几个部分。我是**省广播电视总台信息系统部主任，平时主要负责**省广电系统的网络规划、设计以及运维工作。在该广电城建设的项目中，我负责**省广电城建设项目中的 IDC 机房建设子项目的规划和设计。

1. 问题的分析和提出

双线路技术就是通过特殊的技术手段把不同的网络接入商（ISP）服务接入到一个服务器集群或某一台服务器上面，使服务器所提供的网络服务访问用户能尽可能以本地所属 ISP 连接来进行访问，从而解决或者减轻跨 ISP 用户访问网站的缓慢延迟（南北网络瓶颈）问题。

老广电系统简单做法是采用双线路双网卡实现方式：在同一服务器上面配置双网卡，分

别连接两个网络服务提供商，在这两块网卡上设置一个联通 IP 和一个电信 IP，在服务器上配置路由表实现访问联通和电信的用户各自走不同的通道。在网站上设置联通 IP 地址链接和电信 IP 地址链接，联通用户和电信用户分别点击各自的 IP 访问服务器。

此方式缺点：服务器接入的是双网卡，需要由专业技术人员在服务器上设置路由表，在服务器数量很多是增加了维护量和维护的难度，而且所有数据包都要在服务上路由判断后再发往联通或电信的网卡。若访问量较大时，占用服务器的资源很大，导致网站性能降低。所以，此方式只能用于规模较小的网站。

现在**省广电网站服务器有几十台之多，以上方案已经不合适了。结合自身特点，考虑接入双线路后，首先解决南北运营商网络瓶颈，提高网站访问速度，使联通的用户通过联通网络访问**省广电网服务器，电信的用户通过电信网络访问**省广电网服务器。其次，能实现内部上网用户分流。由此产生的具体需求如下：

（1）每台服务器对外只提供唯一的域名，单域名双线路。

（2）每台服务器对外都具有合法的电信和联通 IP 地址，所有服务器如 WWW、FTP 以及 SMTP 等都能被外部网络正常访问。

（3）联通和电信用户以本地所属 ISP 连接来进行访问。

（4）内部员工上联通过双线路自动识别目的 IP 的归属，走最近的线路访问 INTERNET，提高访问速度。

（5）建立 VLAN 策略和入侵防御安全方案。

2. 关键技术介绍

本方案的关键技术有智能 DNS 建设、策略路由、地址映射。

（1）智能 DNS 建设

DNS 的主要功能是将难记的 IP 地址和容易记忆的域名进行转换，当用户在浏览器中输入主机域名时，DNS 服务器可以将此名称解析为与之对应的 IP 地址。这种 DNS 上的域名解析一般是静态的，即域名与 IP 地址是一一对应的。

智能 DNS 指的是基于一种策略，服务器根据请求解析的客户端所处在的网络，返回相

应的解析结果；或者是 DNS 服务器根据客户端所在网络的不同，应用不同的安全策略，比如对内网用户提供递归解析服务的同时忽略外网用户的递归解析请求等。

（2）策略路由

策略路由是基本路由功能的智能延伸，它不仅可以根据数据包目的地址、源地址、数据包大小等条件为依据来进行路由选择，还可以根据设备链路接口来选择路由。在外网访问内网服务器（Inbound）中，多采用基于设备接口的策略路由；内网访问外网（Out-bound）多采用基于目的地址的策略路由。策略路由可通过路由器、防火墙实现，配置策略路由通常包括以下几个步骤：

- 定义路由映射来控制数据包的出口；
- 为定义的路由映射设置匹配标准；
- 为与给定标准相符的数据包设定路由处理行为（选择路由路径）；
- 为需要进行策略路由的端口指定相应的策略路由；
- 设置相应的访问控制列表作为路由映射的匹配标准。

（3）地址映射

地址映射（NAT）主要有两种类型：动态映射及静态映射，通常在路由器或网关上实现。其中静态 NAT 是将内网的每个 IP 永久映射为外网中的某个合法 IP 地址。而动态 NAT 则是在公众网定义了一系列的合法地址，采用动态分配的方法映射到内部网络。本文采用静态 NAT 方式让内网的每一台服务器拥有电信和联通的 2 个公网 IP，采用动态 NAT 方式让内网的上网用户动态获取电信（联通）地址池中的随机地址。

3. 关键配置与实现

该项目方案以防火墙为核心出口设备，采用 4 口的阿姆瑞特防火墙，一口接电信，一口接联通，一口接服务器区 VLAN，一口接内网用户区 VLAN。在防火墙和服务器区之间串接入侵防御系统 IPS。网络布局主要是采用三层交换机 CISCO3560 建立 VLAN 的 VTP 域，划分多个 VLAN。一方面根据需要制定 VLAN 之间的访问控制策略，隔离服务器区和内网区，于是连接服务器区的 VLAN 和连接内网区的 VLAN 被隔离开来。另一方面采用端口划分 VLAN 的方式使得调整服务器和内网计算机数量变得非常便利，不会局限于某一台交换机的物理位置

和端口数量。

防火墙作为核心出口设备，同时接入电信和联通两路链路。上行和下行的网络数据传输全部通过防火墙来路由，外网访问服务器（Inbound）采用基于防火墙链路接口的策略路由，内网访问公网（Outbound）采用基于目的地址的策略路由。此方案采用阿姆瑞特防火墙实现双链路路由功能。服务器的内部地址为私有地址 192.168.1.80-192.168.1.110，电信公网地址为 218.94.74.1-218.94.74.32，联通公网地址为 58.240.127.160-58.240.127.192。

（1）对于每一台服务器，其电信和联通的两个公网 IP 地址同时静态映射到一个内部 IP 上，以 WWW 服务器为例，配置如下：

NAME sat_216_ 联通

SAT any all-nets any 58.240.127.180 webmail SETDEST 192.168.1.80

NAME sat_216_ 电信

SAT any all-nets any 218.94.74.20 webmail SETDEST 192.168.1.80

（SAT 为静态映射命令，58.240.127.180、218.94.74.20 为联通和电信的公网 IP 地址，ebmail 为预定义的端口，SETDEST 192.168.1.80 表示指向目的 IP，其它的服务器以此类推.....）

（2）对于外网访问服务器采用基于防火墙链路接口的策略路由制定回路路由。即对于从电信链路来的访问请求，回路路由走防火墙的电信链路接口；对于从联通链路来的请求，回路路由走防火墙的联通链路接口。主要配置命令如下：

▪电信用户访问内部服务器的电信公网 IP

NAME 电信 _in ROUTE {RET tel_out} any all-nets any tel_net Standard;

ROUTES;

PBRTABLE tel_out ORDERING Default;

lan_电信接口 all-nets 218.94.74.1;（电信出口网关 IP）

END.

▪联通用户访问内部服务器的联通公网 IP

NAME 联通_in ROUTE{RET cnc_out}any all-nets any cnc_net Standard;

ROUTES;

PBRTABLE cnc_out ORDERING Default;

lan_联通接口 all-nets 58.240.127.165;（联通出口网关 IP）

END.

（3）内部员工访问外网采用基于目的地址的策略路由技术。在防火墙中设置电信和联通的 IP 地址表，对于目标地址属于电信的 IP 则从电信的链路进行 NAT 后转发；对于目标地址属于联通的 IP 则从联通的链路进行 NAT 后转发；对于目标地址既不属于电信也不属于联通的通过电信出口转发。

4. 结语

省广电网站 IDC 双线路方案，服务器全部采用单网卡方式，基于智能域名解析，通过防火墙分别对应电信和联通接入，由此减少了双网卡方式带来的麻烦，实现了安全高效的对外视音频发布和内部用户访问 INTERNET，从而解决了不同运营商造成的南北方网络瓶颈问题。目前以省广电总台《绝对唱响》海选节目和《抗震救灾》的视频传播为测试，取得了良好的效果。