核心网络及 VPN 技术在广东气象业务中的应用

肖文名 阮惠华 孙周军 李素丽 陈晓宇 (广东省气象信息中心)

摘要:本文详细阐述了广东省气象局局域网中核心网络技术的应用,同时详细阐述了 VPN 技术在我省省、市、县气象三级远程通信中的应用,并阐述了通过互联网安全访问内部网的远程访问 VPN 技术。

关键词:VPN 技术 核心网络 远程访问

1 引言

随着业务的不断发展,业务信息量的不断增加,对与业务流程息息相关的网络通信能力的要求也越来越高。近年来,我们对省气象局大院局域网及省、市、县三级气象通信网络做过多次升级改造。大院局域网先是在 9210 工程基础上 1998 年升级到 100M,通过 VLAN 技术建立虚拟三层交换网络,2004 年又升级为千兆,建立了双核心的多层交换局域网。省、市、县三级气象通信网从模拟专线转为分组网,2001 年建立了省、市基于 MPLS 的宽带 VPN 通信网络,同时通过互联网建立了基于 IPSec、L2TP、PPTP 的 VPN。2004 年计划完成市、县宽带通信网建设工作。本文简要介绍了我局最近进行的网络升级方案及相关 VPN 技术在我局通信业务中的应用。

2 核心网络

此次网络的升级改造的主要目的是提高核心网络的交换能力,建立冗余的核心网络,在网络中心消除单点故障,建立统一、有效、安全、可靠的网络管理系统。核心网络采用的是千兆以太网技术。

2.1 网络结构

按照目前国际标准的以太局域网设计规范,一个大型网络系统应分三层进行设计,分别是:核心层(CORE)、分布层(DISTRIBUTE)、接入层(ACCESS),我们根据实际情况合并了核心层与分布层的功能,用结构清晰,易于维护的两层星型结构实现局域网的网络拓扑,即网络结构采用两层结构:核心层和接入层。

2.2 核心层双核心冗余机制

核心网络是我们一切业务的基础,它承担着我局高性能、高可靠性的数据转发,是网络稳定高效运行的关键,其重要性远高于业务计算机系统,因为计算机系统的故障只影响到该计算机所承担业务的正常运行,而核心网络的故障导致的则是所有业务的停顿,因此,核心网络系统的处理性能、稳定性等因素决定了整个网络的性能。为充分保证整个网络的可靠性及可用性,核心网络我们设置了 2 台 Cisco Catalyst6509 千兆骨干路由交换机,采用双机热备份机制,通过双 1000M 光纤链路,为骨干路由交换机提供双链路可靠性。完整网络结构图见图 1。

2.3 接入层双链路冗余机制

接入层按单位或楼层划分,每个接入层交换机采用 Cisco Catalyst3550 – EMI 交换机,并用 1000M 光纤链路与核心交换机互联,形成冗余备用。

2.4 核心层与接入层连接技术方案

在我们实际的网络业务中,每个接入层基本上是一个独立的业务单位,也就是说,每个接入层是一个独立的 IP 网段,处在同一个 VLAN(虚拟局域网)中。因此,核心层与接入层之间的连接技术可采用两种方案:第二层交换方案和第三层路由交换方案。

2.4.1 第二层交换方案

采用第二层交换技术作为核心层和接入层之间的连接技术,接入层交换机只需具备二层交换功能即可。方案中首先要考虑的是如何充分发挥接入层到核心层的双链路效益,双链路最好能负载均衡。由于第二层交换网络中不能出现环路,而我们的方案中为了达到冗余处处存在环路,所以需要运行生成树协议来堵塞冗余链路以避免环路。在 Cisco 交换机实现中,可以采用每 VLAN 一个生成树协议实例,或某几个 VLAN 一个生成树实例,所以在 Cisco 交换网络中,二层交换技术

对冗余链路可以实现 VLAN 级别的负载均衡，即某些 VLAN 流量通过一条链路，其余 VLAN 流量通过另一条链路，此时需要细致规划生成树协议运行效果，通过手工配置改变相关交换机和交换机上联端口对不同 VLAN 的优先级，使得生成树协议按我们的规划生成相应 VLAN 的生成树，来达到按我们预设计的负载均衡策略分配网络流量。在我们的方案中要实现双链路的负载均衡，必须在接入层建立多个 VLAN，但是，我们实际的业务网络中每个接入层由于处于同一 IP 网段，故只划分了一个 VLAN，这意味着在我们的方案中如果采用第二层交换方案，生成树协议会堵塞双链路中的一条链路，因此是无法做到负载均衡的，只能作为热备份使用。这一方面影响连接带宽（接入层与核心层此时只有千兆连接，而不是负载均衡时的两千兆），另一方面也不能充分发挥双核心的投资效益。同时在第二层交换中，主链路故障需要切换到备用链路时要重新进行生成树协议运算，在 Cisco 交换环境下，这至少需要 45 秒钟的收敛时间，45 秒的时间足以使很多 IP 应用连接中断。因此，我们最终的方案中没有采用第二层交换技术方案，而采用了第三层交换技术方案。

2.4.2 第三层路由交换方案

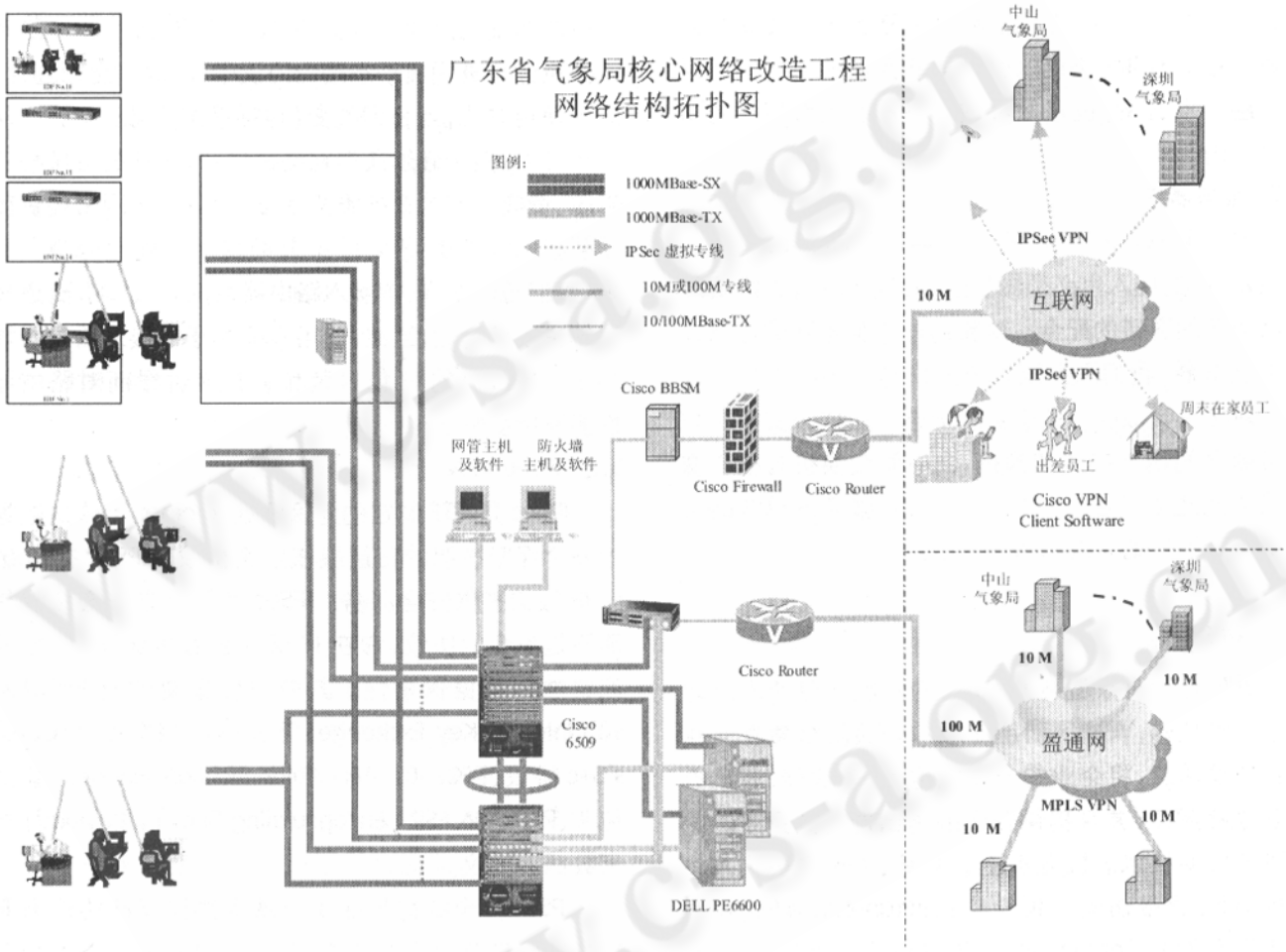

图 1　网络结构拓扑图

采用三层路由交换方案要求接入层交换机具备三层交换功能。对于三层路由技术而言，是可以存在冗余链路的，为了做到在冗余链路上实现负载均衡和相互备用，就必须采用动态路由，才、需要选择适当的路由协议。目前常用的路由协议有多种，如 RIP、OSPF、IS－IS、IGRP、EIGRP、BGP 等等，不同的路由协议有各自的特点，分别适用于不同的条件之下。RIP 收敛慢，OSPF 收敛快又是标准协议，但 OSPF 只支持等价路径负载均衡，不支持非等价路径负载均衡，EIGRP 是 Cisco 专用

协议，收敛快支持非等价路径负载均衡，因此，我们的网络方案中路由协议采用 EIGRP。考虑到路由协议的网络开销，我们只在接入层交换机 Cisco3550 和核心交换机 Cisco6509 上启用 EIGRP 路由协议，达到接入层与核心层之间双链路的负载均衡和相互备份功能，而并不是全网使用 EIGRP 动态路由协议，在对台站接入路由器等其他路由器上还是采用静态路由和缺省网关，只是需要在相关交换机和路由器上将有关静态路由重分布进 EIGRP 协议以达到全网互通的目的。相对第二层交换方案，链路故障时 EIGRP 的收敛时间在 5 秒钟之内。

2.5 服务器接入

要做到核心交换机故障时并不影响正常业务运行，服务器的接入也必须做相应的冗余设计，这需要服务器网卡的容错的配合。对新购进的服务器或可以改造的服务器，我们采用双网卡分别与双核心交换机连接。对无法升级改造的服务器则通过在核心交换机与服务器之间增加中间交换机，由中间交换机与核心交换机之间建立二层或三层冗余连接，服务器单链路接入中间交换机的方法来达到目的。

3 VPN 技术

VPN 是近年来随着 internet 的发展而迅速发展起来的一种技术，VPN 是利用开放的公共网络建立专用数据传输通道，将企业的分支机构、商业伙伴、移动办公等连接起来，并且提供安全的端到端的数据通信的一种广域网技术。按业务用途划分，VPN 可分为：Access VPN（远程访问虚拟专网），Intranet VPN（企业内部虚拟专网），Extranet VPN（扩展的企业内部虚拟专网）。按在 OSI 模型中实现隧道的层次划分为：第二层隧道协议和第三层隧道协议。现有的第二层隧道协议有 PPTP（点到点隧道协议），L2F（二层转发协议），L2TP（二层隧道协议），现有的第三层隧道协议有 GRE（通用路由封装协议），IPSec（IP 安全协议），在我们的省市县远程通信中使用到了 MPLS（多协议标记交换）VPN，IPSec VPN，L2TP VPN，PPTP VPN。

3.1 MPLS VPN

2001 年，我们利用基于 MPLS 的 VPN 技术，建立了省、市气象宽带通信网，省气象局端 100M 光纤接入，接入设备采用的是 Cisco 36 系列路由器，市气象局端 10M 光纤接入，接入设备采用的是 Cisco 26 系列路由器。在该方案中，有关 VPN 的所有复杂性都在网络服务提供商端设置，VPN 起点标记也是由网络服务提供商端的 PE（提供商边界）路由器负责，我们的接入路由器（在 MPLS VPN 中叫 CE 路由器，即客户边界路由器）配置非常简单。由于在 PE 和 CE 之间没有启用动态路由协议，因此，我们必须告诉网络提供商我们内部的 IP 网段的详细划分使用状况，以便其在 PE 上将相应静态路由重分布进相应动态路由协议中，以做到全网连通。这种使用方式，当我们改变（包括增加或减少）了 IP 网段地址时，由于必须通知网络提供商，让其配合做相应修改，造成一定的业务维护困难，同时由于网络提供商了解我们内部的 IP 地址细节而增加了安全隐患。后来，我们通过在省、市接入路由器之间建立 GRE 隧道技术解决了该问题，当然，使用 GRE 由于在接入路由器增加了一层额外的 IP 包封装和解封装过程而对路由器性能有所影响。

3.2 IPSec VPN

IPSec 是 IETF 制定的为保证在 Internet 上传送数据的安全保密性能的三层隧道加密协议。IPSec 在 IP 层对 IP 报文提供安全服务。IPSec 实际上是一套协议包而不是单个的协议，它在 IP 层提供数据源验证、数据完整性和数据保密性。其中比较重要的有 RFC2409 IKE（Internet Key Exchange）互连网密钥交换、RFC2401 IPSec 协议、RFC2402 AH（Authentication Header）验证包头、RFC2406 ESP（Encapsulating Security Payload）加密数据等协议。

IPSec 安全结构包括 3 个基本协议：AH 协议为 IP 包提供信息源验证和完整性保证；ESP 协议提供加密保证；密钥管理协议（ISAKMP）提供双方交流时的共享安全信息。ESP 和 AH 协议都有相关的一系列支持文件，规定了加密和认证的开放框架，没有定义某种指定的算法，可采用所有工业标准算法。如 AH 协议中哈希散列算法可以采用 MD5 或 SHA。ESP 协议可以选择多种加密算法包括 DES、Triple－DES、RC5、RC4、IDEA 和 Blowfish。

IPSec 提供两种工作模式：传输模式和隧道模式。在传输模式中，只有 IP 负载即高层协议（TCP，UDP，ICMP 等）及数据是加密的。在这种模式下，源地址、目的地址及 IP 包头的内容都不加密。在隧道模式中，整

个用户的 IP 数据包被用来计算 ESP 包头，整个 IP 包被加密并和 ESP 包头一起被封装在一个新的 IP 包内。基于 IPSec 的 VPN 省气象局端是在 Cisco PIX－525 防火墙上实现的(省气象局出 Internet 带宽为 10M)，即防火墙作为 VPN 网关，使用的自然是 IPSec 的隧道模式。基于 IPSec 的 VPN 中有所有关于 VPN 的设置全部在用户端进行，网络提供商只是提供公共的 IP 连通性，看不到任何用户内部网细节。在我们实际应用中，对有条件的市局(指有固定互联网 IP)，我们建立网关到网关的内部网虚拟专网，作为省、市备用通信方案。同时利用 Cisco VPN 客户机软件建立了基于 IPSec 的远程 VPN 访问，使得出差在外的人员通过互联网可以安全访问省气象局内部网，并通过省气象局内部网访问到各市局内部网，移动用户通过 GRPS 或 CDMA 加上 VPN 客户软件实现随时随地安全访问内部网。

3.3 L2TP PPTP VPN

在我们最近的网络升级前，我们是用 Windows2000 来建立通过 Internet 的 VPN 通信的。Windows 在 NT 版本时只支持建立基于 PPTP 的 VPN，在 2000 中增加了支持 IPSec、L2TP 协议。在 Windows2000 中，对于一端只是拨号没有固定 Internet IP 地址也可以建立网关到网关的 VPN 连接，并且是动态按需的 VPN 连接(基于 L2TP 或 PPTP)。在 Windows2000 中建立基于 IPSec 的 VPN 也是非常方便的。在我们的应用中，L2TP、PPTP 也是在防火墙上实现的。采用 L2TP 和 PPTP 的主要目的是实现一端是拨号情况下 VPN 网络互联，同时也为了增加远程客户访问的适应性。

4 结束语

核心网络建立冗余对我们的业务应用是非常必要和关键的。当然核心网络可以有不同级别的冗余方案，不一定非得双核心，主要看经费投资情况，经费许可的情况下，双核心自然是很好的选择，单核心也可以有冗余方案，比如可以实现部件冗余。在 Cisco 设备中就专门设计了部件冗余功能，即在核心交换机上关键部件(电源、引擎、模块)均可以实现冗余备份，在网络中心点消除单点故障。值得一提的是，Windows2000 中的 IPSec 功能在内部局域网中建立关键主机之间的安全加密通信是非常方便有效的。它是通过采用 IPSec 的传输模式工作方式来实现的，不需改变或增加 IP 地址，可以非常方便地实现对关键主机之间的不同类型流量实施不同的安全策略。

参考文献

1 张舒、肖田元，网络化制造平台中的跨平台计费管理系统[J]，微计算机信息，2007，(3).

2 杨开程，网络核心技术在通信电源设备监控系统中的应用[J]，芜湖职业技术学院学报，2007，(1).

3 李兆祥，高校万兆核心网络设计要点[J]，林区教学，2007，(3).

4 张智、李瑞轩，基于 JXTA 架构的对等网络关键技术研究[J]，计算机应用研究，2007，(3).

5 孙军、胡飞，基于 MPLS VPN 构建合肥市电子政务专网[J]，计算机与信息技术，2006，(Z1).

6 安计勇、张明胜，VPN 在高校校园网中的应用[J]，计算机与信息技术，2006，(8).

7 刘伟、李大兴，Windows 平台中 IPSec VPN 的设计与实现[J]，微计算机信息，2006，(36).

8 何亚辉、肖路、陈凤英，基于 IPSec 的 VPN 技术原理与应用[J]，重庆工学院学报，2006，(11).

9 陈爱和、徐敬东、刘晓欣、张建忠，支持多路负载平衡的 SSL VPN 系统的设计与实现[J]，计算机工程与设计，2006，(21).