运营商骨干网扩容与优化

摘要：

目前国内运营商骨干网通常跨接很大的物理范围，它连接多个城市提供远距离通信。通常，骨干网容量非常大、承载的数据业务非常多、因此运营商大型的骨干网事非常复杂和庞大的。而且，随着计算机的普及程度越来越广泛，各行各业对网络的依赖性越来越大，各类互联网应用越来越多。因此，互联网骨干网的扩容与优化逐渐成为各级运营商需要解决的课题。本文主要根据**运营商的骨干网扩容与优化项目进行叙述。从分析的角度讲述了方案的目标和组网原则；从拓扑设计的角度讲述了局域网和广域网的拓扑结构设计、VPNRR 的设计。从 IGP 路由协议设计方面重点讲述了 ISIS 设置原则、NSAP 地址编码规范。从 BGP 路由协议设计方面重点讲述了与其他运营商互联互通（EBGP）的设计、I-BGP 设计。文章还讲述了项目中组播应用、组播应用、网络安全等实施手段。

全文：

******通信信息技术公司是北京市较大的网络信息系统集成公司，有着多年的网络设计经验，为多个省市的电信公司提供网络运行和维护服务。****公司是国内数一数二的互联网接入提供商，其主干网络承担着各类数据业务，而且每时每刻承载的数据量相当巨大。由于接入用户数量的巨增，2008 年 10 月，****公司提出了将其骨干网扩容与优化项目的计划，并由******通信信息技术公司设计与实施。因为本公司就负责该公司的网络运维，因此项目的设计和分析都很顺利，同时 2 个月的紧张实施本项目基本告一段落。本人作为******通信信息技术公司高级项目经理，全面负责该项目的设计与实施工作、并且全方位的和用户进行沟通。

1．方案设计的目标与原则

本方案的主要目标是为****公司优化一个广泛覆盖的 IP 基础设施平台，提高网络能力和运行质量，提高网络安全，满足互联网市场需求；为开展宽带数据业务以及 MPLS VPN、

视频通信、内容网站等各类增值业务提供平台；为继续扩大互联网市场份额，获取更大利润奠定基础。工程着重从以下几个方面展开。

（1）现有节点调整及扩容，进一步提高接入能力；

（2）IGP 路由结构的优化改造，合理化流量承载结构；

（3）扩大骨干网络覆盖面，节点数量增加 85%；

（4）进一步提升带宽，本次电路扩容总带宽 120G；

（5）优化对业务的承载能力。

本方案将继续贯彻所倡导的全程全网，集中管理的建网方针，坚持骨干网和城域网相结合的技术路线，并从以下几个方面加以考虑。

（1）模块化：每个网络组件和其他设备间分界清晰，类型标准化，节点设计标准化，使业务可以平行叠加。

（2）功能化：不同的设备特性各有特色，因此在网络中要有明确的角色，担负有限的相应功能。

（3）层次化：包括物理结构的层次化和路由结构的层次化。

（4）冗余性：骨干网任何单点故障不影响全网服务质量，实现带业务系统维护。

（5）一致性原则：有两个方面含义。

- 设计目标和技术实施的一致性；
- 管理体制和网络结构的一致性。

（6）业务驱动原则：节点设计可以打破以往行政区域的框架，充分考虑流量的大小、流量的走向。对部分紧密联系、直接通信量大的省份，跨省直连。

2. 拓扑结构设计

拓扑结构设计主要分为广域网设计、局域网拓扑设计、VPN RR 结构设计：

（1）广域网设计

拓扑方案将骨干网络分为 3 个层次，核心层、骨干层和接入层，相应节点分别以 A 类节点、B 类节点和 C 类节点表示。

A 类为核心层，包括 3 个 A1 类和 4 个 A2 类城市。A1 类城市采用环状连接；A2 类城市分别与 A1 类城市组成部分网状连接，提供骨干网路由汇聚和快速交换以及 Internet 互联。B 类为骨干层，承担省内网络汇接。C 类为接入层，负责就近网络接入。

（2）局域网设计

局域网设计主要是对 A、B、C 三类节点的设计。

·A 类节点设计

A 类节点包括北京、上海、广州、沈阳、成都、西安和武汉七节点。设计的内容有对北京、上海、广州的出口网关设备进行扩容。在北京、上海、广州设置 MPLS VPN 路由反射路由器组。在北京、上海和广州 NAP 点各设置一台具有高速接口的网关路由器 XGR。

·B 类节点设计

B 类节点设计为双核心结构，通过增加高速核心路由器提高核心转发能力，以及核心网络的稳定性。设计的内容有：双 CR 高速路由器间采用 N×GE 电路进行背对背连接。CR 的下联路由器均采用双路归属。在局域网内部连接中，所有 CR 和 AR 之间的链路加入 ISIS L2 路由。环回地址加入 ISIS L2 路由。

·C 类节点设计

C 类节点同样采用双核心、双归上联的拓扑结构。分别用 PoS 链路上连省内汇接节点或核心节点为保障承载业务的时延等性能指标，对两台设备进行业务分工，并相互形成备份。设计的内容有 AR 之间、AR 和交换机之间采用 GE 背对背点对点连接。AR5-1 和 AR5-2 之间 Link 采用 ISIS L2 路由。对于重要的业务，在 AR 相应的 VLAN 上启用 HSRP。

（3）VPN RR 结构设计

在上海、广州各新设一组 MPLS VPN 路由反射路由器组，以满足华东、中南、华南、西南大区 PE 路由器 MP-IBGP 全网状相连的要求。

3. IGP 路由设计

采用扁平化路由结构，贯彻骨干网、城域网相结合的建设思路，充分体现骨干网的灵活性和高效性，强化资源集中调度和全程全网管理。保留区域性特征，同经营管理体制相结合，

利于网络未来拓展全网采用 ISIS L2 Only 特性，即 CR、AR、GR、MPLS PE、RR、VRR 互连电路原则上均加入 Level2 路由。

ISIS 协议中采用 NSAP 地址作为路由设备标识，因此，每台路由器将配置唯一 NSAP 地址，其中可变字段由 domain 和 area 两段组成示。

4. I-BGP 设计

骨干网中由 BGP 路由协议承载用户路由，通过在北京、上海、广州使用专用路由反射器（RR）来减少 IBGP 会话进程。通过使用 2 级 RR 来减少 IBGP 会话进程。

第一级 RR Server 和 Client 分配如下：在北京、上海和广州分别各有两台路由器作为 RR Server，核心、汇接节点的核心路由器按区分别属于相应的 RR Cluster 的 Client。北京、上海和广州的 iGR、dGR、xGR 也是相应 RR Cluster 的 Client。第一级 RR Server 和 Client 之间不做路由过滤和控制。

第二级 RR 的 Server 为各个核心、汇接节点的核心路由器 CR。RR 的 Client 端为相应节点内的其他路由器和连接到该节点上的普通节点。第二级 RR 的 Client 会和用户运行 BGP。对于不同的用户，会有不同的路由控制、过滤。

5. 组播应用

实施 PIM-SM 组播方案将全国划分成三个 PIM-SM 区域：北京、上海和广州。北京、上海和广州节点的两台核心路由器在本区域内作为 RP 路由器，而区域之间采用 MSDP（Multicast Source Discovery Protocol）组播源头查找协议连接这些 PIM-SM 区域。通过 MSDP 在单个自治系统中为不同的组播区域部署不同的 RP 和用于 PIM-SM RP 的选一机制。采用 MSDP 划分区域后，每个组成员均可以选择本区域内的 RP 来加入组播网络，也避免了同区域组播会话长途绕道问题。

6. QoS 实施

QoS 的实施分为两部分：边缘和骨干。在边缘主要完成功能：指定业务类型与级别的策略；指定资源分配与控制的策略；业务分类与安全策略的实施；流量与资源利用的测量采集。在骨干主要完成功能：提供大容量、高性能和高可靠性；提供策略的管理与实施；提供流式排队与拥塞管理。

7．网络安全保障

为保证全网络路由表的安全性，防止路由更新及路由表的非法更改，确保整个网络系统路由的可靠和稳定，建议采取以下措施。

（1）路由协议的验证机制

在方案中所使用的路由协议 BGP4 及 IS-IS 都支持路由加密认证。

（2）路由信息过滤

在 Internet 出口处，Internet 接入路由器将通过 BGP4 协议和其他运营商交换路由信息，BGP 不会把私网路由信息扩散到公网中。

（3）禁止源路由方式

源路由是被设计用来进行测试和调试的，一般的路由器默认状态下都予以支持，必须注意在实施中将路由设备的源路由特性关闭掉。

8.项目小结与解决问题措施

本项目完成后，满足了用户对骨干网扩容与优化的要求。但是，网络中 DDos 的攻击还比较严重。DDoS 通常会利用任何一种通过发送单独的数据包就能探测到的协议缺陷，并利用这些缺陷进行攻击。我们采取了以下手段解决问题：

- 针对资源掠夺性攻击，在网络上的设备可以进行多层次的防范；
- 在网络设备上关闭所有带有安全隐患的端口检测和进程调用；
- 过滤进网和出网的流量；
- 可疑数据流带宽控制；
- 重要数据流带宽保证；
- 采用网络入侵检测系统 IDS。