某市国土资源规划局外网链路优化

整体解决方案

2020-10-25

目录

第一章　某市国土资源规划局网络系统概述.....3
1.1　某市国土资源规划局网络系统的发展状况.....3
1.2　某市规划局当前网络存在主要问题.....3
第二章　网络方案设计.....5
2.1　互联网出口链路建设目标.....5
2.2　第二条互联网出口链路的选择建议.....5
2.3　某市规划局网络系统现状.....6
2.4　某市规划局出口优化后网络拓扑.....7
2.5　信息中心对应准备工作.....8
2.6　方案特点及相关产品优势.....9
第三章　链路负载均衡解决方案介绍：.....9
4.15　出站流量负载均衡（Outbound 方向）.....10
3.1.1　负载分担算法.....10
3.1.2　透明 DNS.....12
3.1.3　链路健康检查.....12
3.1.4　链路拥塞控制.....13
3.1.5　出站流量会话保持和 NAT.....13
4.16　入站流量负载均衡(Inbound 方向).....13
3.1.1　智能 DNS 解析流程.....14
第四章　产品选型及资料.....15

第一章 某市国土资源规划局网络系统概述

1.1 某市国土资源规划局网络系统的发展状况

随着某市国土资源规划局（以下简称“规划局”）的各项关键业务不断的增加，现在的网络性能将受到挑战，网络系统正日益承受着更大的压力，系统的可靠性、安全性以及高可用性都成为确保某市国土资源规划局业务管理和办公的关键点。

目前某市规划局外网有两条电信链路，其中 100M 电信链路作为主要业务专线，30M 电信链路作为内部用户办公上网链路。

1.2 某市规划局当前网络存在主要问题

目前网络出口存在以下问题：

- 核心业务链路（移动一张图等）只有一条 100M 电信链路，没有冗余机制，当链路发生故障的时候，互联网用户也不能够访问到规划局内部的服务器资源。
- 规划局移动终端用户大多采用的是联通的上网卡，联通用户访问电信 IP，存在跨运营商访问，导致访问速度比较慢；
- 中规协网站，由于中规协客户主要以北方联通用户为主，访问电信站点存在跨运营商访问，导致访问速度慢；

- 内网办公用户访问互联网，经常导致 30M 电信带宽占满，影响办公；
- 办公 OA 短信平台向外发送短信时，由于只能通过电信链路，导致发往联通平台手机号的信息有时无法顺利发出；

针对如上问题，规划局信息中心计划最近增加一条联通链路，并部署链路负载设备实现链路分担及冗余，并通过智能 DNS 技术避免跨运营商访问问题。

最终实现：

- 当一条链路故障时，可以快速切换到其他链路上，保证内网办公用户访问互联网资源，互联网用户访问到规划局内部的服务器资源不受影响；
- 实现把内网用户访问互联网的流量根据运营商信息、链路质量智能的分配在不同的链路上，并避免链路出现拥塞；
- 采用多条链路后，移动一张图、中规协网站等对外发布应用，可在一个域名下映射多个公网 IP，并根据访问用户的运营商不同返回用户不同的 DNS 响应，以避免跨运营商访问；
- 能够实时探测链路健康状态，当其中一条链路出现拥塞、中断时，外部用户访问域名自动调整到可用的公网 IP 上；

第二章 网络方案设计

2.1 互联网出口链路建设目标

目前在国内由于多家 ISP 的竞争，Internet 接入链路的成本大幅降低，多链路 Internet 的接入已成为许多数据中心在的选择网络连接方面的需求。因此在数据中心 Internet 网络出口连接方面将完成以下目标：

- 提高 Internet 网络链路的可用性：

当网络中心具有多条 Internet 链路后，应提高 Internet 网络链路可用性的智慧检查，防止出现由于某一条 Internet 链路的失效造成整体网络的不可访问。

- 提高 Internet 链路的网络吞吐量：

提高数据中心的 Internet 网络链路的吞吐量，申请多条 Internet 链路

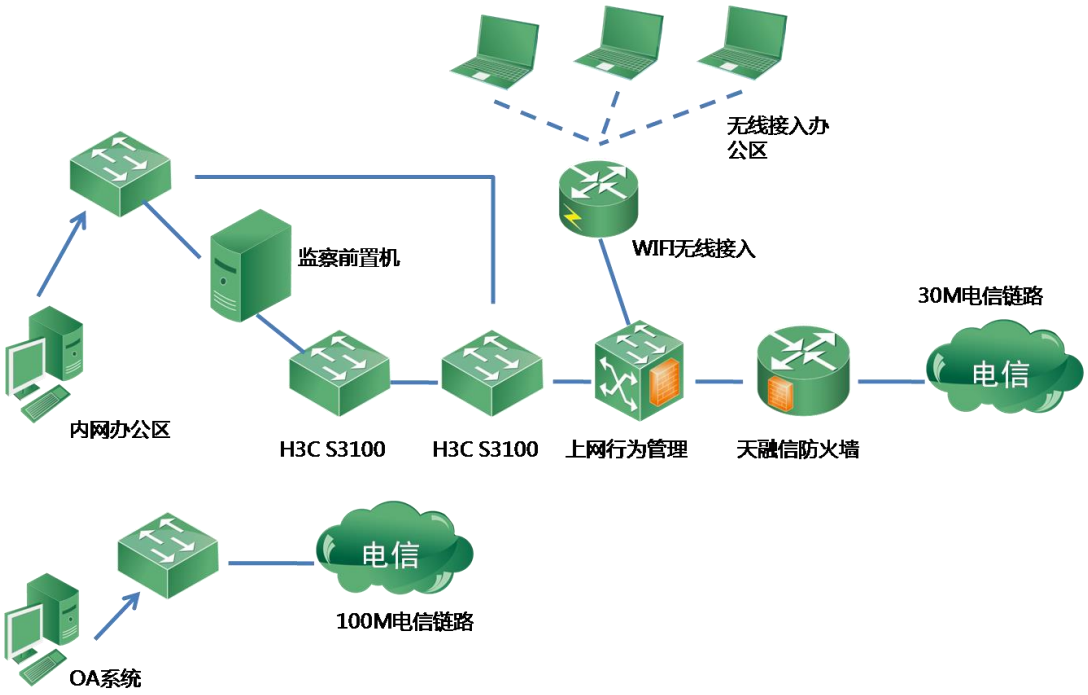
2.2 第二条互联网出口链路的选择建议

考虑到链路的品质，以及运营商的国际出口带宽的保障，对链路带宽以及运营商的选择依据如下：

- 运营商选择

从之前情况看，由于大量业务需要通过联通访问，建议增加一条联通链路，联通公司有与电信接近的国际出口带宽，具备全国骨干网络。链路质量和速度得以保证。

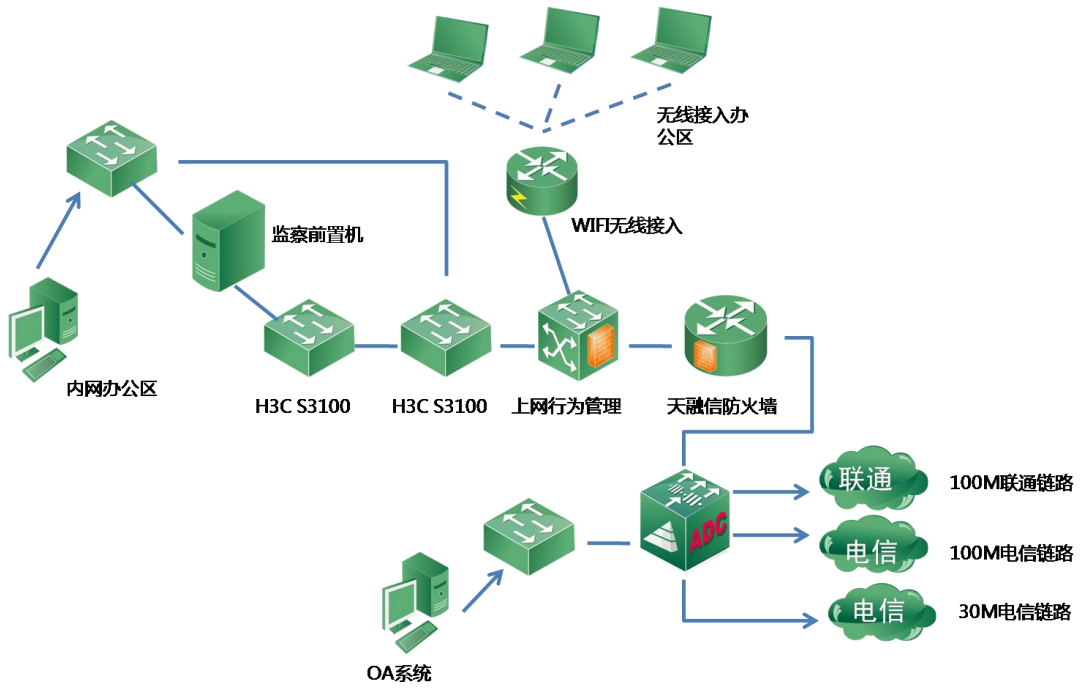
2.3 某市规划局网络系统现状



如图所示，内网办公用户，通过核心路由器，通过深信服上网行为管理连接天融信防火墙到 30M 电信链路上。

核心业务：“移动一张图“，OA 短信平台，中规协网站，使用公网地址直接连接到 100M 电信专线。

2.4 某市规划局出口优化后网络拓扑



如上图所示，调整后的网络部署方案是：

原有 100M 电信光纤、30M 电信办公专线以及新增 100M 联通链路，分别通过某厂的上网行为管理、某厂的防火墙连接到链路负载均衡器上。

为解决现网中存在的问题，需要在设备上开启下列功能：

- 核心业务链路（移动一张图等）只有一条 100M 电信链路，没有冗余机制，当链路发生故障的时候，互联网用户也不能够访问到规划局内部的服务器资源。

  对应配置功能：开启对链路的健康检查功能，开启智能 DNS 功能，探测对应链路是否失效，出现失效时，将流量迁移到其他链路；开启智能 DNS 访

问，判断用户所属运营商，并返回对应运营商 IP 地址。

- 规划局移动终端用户大多采用的是联通的上网卡，联通用户访问电信 IP，存在跨运营商访问，导致访问速度比较慢；

  对应配置功能：开启智能 DNS 访问，判断用户所属运营商，并返回对应运营商 IP 地址。

- 中规协网站，由于中规协客户主要以北方联通用户为主，访问电信站点存在跨运营商访问，导致访问速度慢；

- **对应配置功能：开启智能 DNS 访问，判断用户所属运营商，并返回对应运营商 IP 地址。**

- 内网办公用户访问互联网，经常导致 30M 电信带宽占满，影响办公；

  对应配置功能：开启链路拥塞保护功能，设置链路拥塞阀值，达到阀值后，自动将流量切换到其他链路上。

- 办公 OA 短信平台向外发送短信时，由于只能通过电信链路，导致发往联通平台手机号的信息有时无法顺利发出；

  对应配置功能：开启策略路由功能，根据 OA 平台的源 IP 地址、短信平台目的 IP 地址、端口，通过指定链路发送。

2.5 信息中心对应准备工作

- 申请联通 100M 链路

- 针对“移动一张图”等核心业务为保证，链路切换时可以正常访问，建议申请一个专门的域名，并修改手机客户端程序，将程序指向修改为域名访问方式；

- 修改对应域名的 NS 记录（需要在 DNS 服务商修改），将对应域名解析服务器 NS 地址修改为链路负载设备监听地址

2.6 方案特点及相关产品优势

该方案采用链路负载产品，通过链路状态探测、调度算法及智能 DNS 功能，可以解决当前信息系统中大量跨运营商访问问题，通过开启 TCP 单边加速等功能，对窄带用户访问也可以带来更好的访问体验。

如考虑存在“单点故障”的可能，建议后期可采用“主备”的方式实现链路负载设备的冗余，避免单点故障存在。

随着系统业务的发展，未来可以通过增加服务器负载功能，实现关键业务冗余及服务器加速功能。

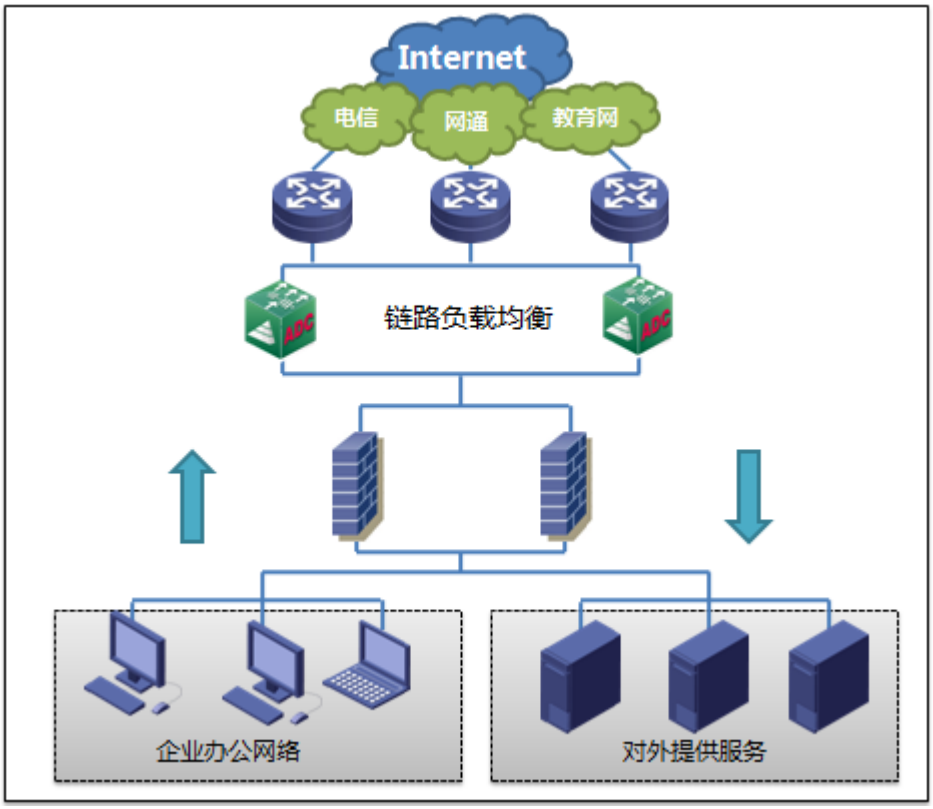
链路负载产品优势：

- 产品性能支持按需负载模式，未来可平滑升级；
- 产品基于模块化设计，支持万兆接口及外置硬件加速卡
- 产品支持可防火墙及应用防火墙功能，自身安全性好，可替代防火墙运行；
- 支持可编程扩展脚本，灵活度高
- 未来可升级设备功能，具备完整服务器负载和应用加速功能。

第三章 链路负载均衡解决方案介绍：

链路负载产品可以动态监控链路的实时状态，提供多种静态和动态流量分担方法，可以有效提升多链路接入的效率和整体性能。当企业部署对外提供服务的应用服务器

时，链路负载可以根据用户所处的运营商网络，或者地域的远近，或者当前链路的带宽质量进行智能 DNS 解析，帮助用户选择最优的链路进行访问，提供最佳的用户体验。



4.15 出站流量负载均衡（Outbound 方向）

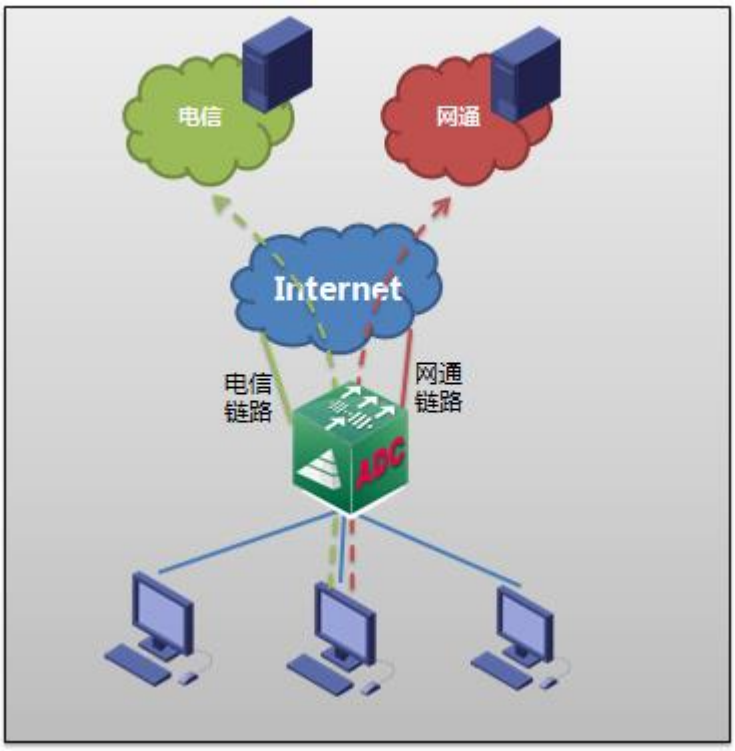
3.1.1 负载分担算法

链路负载分担算法是用来计算内网用户访问 Internet 时（出站流量），在多链路间进行流量分配的方案。链路负载分担的算法和服务器负载分担的算法有一致的地方，也存在一些差异，链路负载分担算法包括：

- **轮询（Round Robin）**-依次按照顺序把流量均匀的分配给每条链路。
- **比率（Ratio）**-根据每条链路的带宽，指定一个权值，按照这个比率给多条

链路分配流量。

- **优先级（Priority）-**为每条链路指定一个优先级，默认情况下优先向高优先级的链路分配流量，当该链路失效时选择备份链路。
- **加权最小连接（Weight Least Connection）**-首先为每条链路指定带宽的加权值，使连接数的分配符合权值的设定，对于新建的连接，选择权值内最小的链路分配流量。
- **加权最小流量（Weight Least Traffic）**-首先为每条链路指定带宽的加权值，使流量的分配符合权值的设定，对于新的流量，选择权值内最小的链路分配流量。
- **运营商路由（ISP Route）**-内置 IP 地址和运营商的对应表，根据内网用户访问的目的地址所属运营商，选择相应的链路，避免跨运营商的访问。



- **最快模式（Fastest）**-链路负载通过比对服务器返回数据包的延迟，跳数等情况，选择一个当前响应最快的链路来分配流量。
- **主备模式（Master-Slave）-**默认情况下流量都发送给主链路，当主链路失效时启用备份链路。

3.1.2 透明 DNS

企业内部用户配置的 DNS 往往是归属于某个指定的运营商，当采用运营商路由 作 为流量均衡算法时，内部用户的 DNS 请求都会发送到该运营商的 DNS 服务器， 造成内部用户的访问请求都会选择该运营商链路。由于内网用户设置的 DNS 问题而导致某个运营商链路繁忙，其他运营商链路出现闲置的流量不均衡情况。通过链路负载的透明 DNS 代理功能，可以对内网用户的 DNS 请求进行优化，按 照 预置的算法把向多个运营商的 DNS 服务器分别发送 DNS 请求，然后根据当前链 路 带宽占用情况，选择合适的目标服务器地址作为 DNS 响应返回给用户。可以有 效 避免内部流量请求都涌向一个特定运营商链路的情况发生。

3.1.3 链路健康检查

链路负载实时对出口链路进行监控和健康检查，可以及时发现端口 down 掉情况。除此之外，链路负载支持包括 ICMP，TCP SYN，UDP，HTTP Get 等多种协议对远端地址进行监控，即使是 ISP 内部网络出现故障，也可以及时发现并把流量切换到其他可用链路。

3.1.4 链路拥塞控制

实时监控各条链路的带宽占用，当某条链路的带宽占用达到预先设置的最大阈值后，后续流量将通过均衡算法分配给其他链路， 可以 有效的避免单纯依赖运营商路由或其他特定算法可能带来的某条链路过度拥塞，而其他链路出现闲置情况。

3.1.5 出站流量会话保持和 NAT

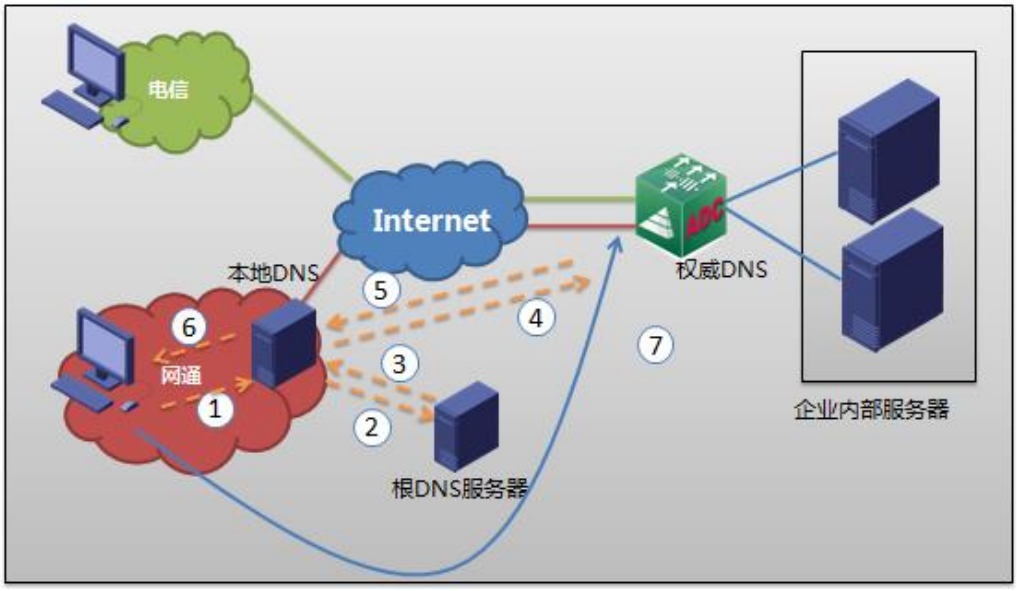
出接口流量会话保持是指当为某个数据流分配一个出接口链路以后，该种类型的后续相关流量都分配给同一条链路。链路负载支持是基于源地址的会话保持和基于 hash 的会话保持。

链路负载支持丰富的 NAT 转换策略，包括源 IP 地址转换，静态地址转换，和基于策略的地址转换。 会话保持和 NAT 地址转换，可以很大程度的避免源主机和某目标服务器通信的过程中，报文横跨多个运营商的情况出现。

4.16 入站流量负载均衡(Inbound 方向)

当企业租用多个运营商链路，以便内部的应用服务器向外部用户提供服务时，链路负载可以通过在内置的智能 DNS 服务器，把企业发布的域名绑定到多运营商的各自的公网 IP 上，并作为企业域名的权威发布服务器。当某个客户端访问应用服务器时，首先会进行 DNS 解析，链路负载可以根据客户端所处的运营商网络返回跟他匹配的 IP 地址，或者通过动态探测技术，选出到该用户通信质量最好链路，并返回对应的 IP 地址。这样可以保证每次客户端都可以通过通信质量最好的链路来访问内部的应用服务器，极大的改善用户体验，并提升整个系统的工作效率。

3.1.1 智能 DNS 解析流程



假定企业通过租用联通，电信两条链路向外部网络提供服务，企业的域名是 www.abc.com, 则整个解析流程如下：

1. 客户端向本地 DNS（Local DNS） 服务器发送域名为 www.abc.com 的 DNS 请求。
2. LDNS 没有该域名的 A 记录，向最长匹配结果的服务器发送该请求，这里假设最长匹配只有根服务器。
3. 根服务器没有“www.abc.com”的 A 记录，但是存放了“www.abc.com”的 NS 域名服务器记录——“www.abc.com IN NS master.abc.com”，将该 NS 记录返回给 LDNS。
4. LDNS 服务器根据该 NS 记录知道了去哪可以找到“www.abc.com ”的 A 记录，将请求发送到链路负载内置的智能 DNS 服务器。
5. ADC 设备判断 LDNS 的 IP 地址隶属于哪个运营商，此示例中 LDNS 隶属于于网

通，所以根据预先配置的规则，链路负载返回“www.abc.com”的 A 记录为网通链路所分配的公网 IP 地址。

6. LDNS 最终将刚收到的 DNS 响应发送回给客户端。

7. 客户端接下来访问企业的网通链路公网地址，链路负载上对应的虚拟服务（VS）接收数据，进入服务器负载分担的流程。

第四章 **产品选型及资料**

根据某市规划局链路情况，使用两条 100M 链路测算，那么网络的双向吞吐能力就是（100M＋100M）×2 ＝ 400M

所以建议选择吞吐至少为 1G 以上的链路负载均衡器产品