锐捷网络

敏锐把握应用趋势 • 快捷满足客户需求

星网锐捷网络有限公司

福州总部

福州市金山大道618号橘园洲星网锐捷科技园
邮编：350002
电话：0591-83057888　0591-83057000

北京市场中心

北京市海淀区复兴路33号翠微大厦东楼9层
邮编：100036
电话：010-51715999/68156699　传真：010-51715896

技术支持网站：http://support.ruijie.com.cn
技术支持信箱：service@ruijie.com.cn
技术支持电话：4008-111-000
客户投诉邮箱：claim@ruijie.com.cn

分销中心

北　京	010-51715999	长　春	0431-88996643	长　沙	0731-4428255	成　都	028-85400328	大　连	0411-84687815	福　州	0591-83057382
广　州	020-37600792	贵　阳	0851-5870013	哈尔滨	0451-87532700	杭　州	0571-88259262	合　肥	0551-5528521	深　圳	0755-83043874
济　南	0531-86161486	昆　明	0871-3161087	兰　州	0931-8457776	内蒙古	0471-3382678	南　昌	0791-8177610	南　京	025-83247911
南　宁	0771-2844846	上　海	021-64325691	沈　阳	024-31321335	石家庄	0311-89617960	苏　州	0512-62511139	太　原	0351-7924993
天　津	022-27422925	武　汉	027-87854855	西　安	029-87285471	厦　门	0592-2295501	新　疆	0991-2338406	郑　州	0371-65350175
重　庆	023-68889979	青　岛	0532-88029575								

如需了解更多产品信息，请浏览 http://www.ruijie.com.cn

解决方案

保险行业全网解决方案

www.ruijie.com.cn

敏锐把握应用趋势 · 快捷满足客户需求

1. 方案概述

国内保险企业特别是大型保险公司从2006 年以后相继启动全国数据集中工程建设，从省逻辑集中到全国逻辑集中，到目前为止逐渐形成以数据中心为核心的多业务支持的网络支撑平台。数据集中以后本文探讨如何考虑保险企业业务需求和发展的基础上，着眼长远的发展目标，为保险企业的业务发展搭建一个可靠、安全、稳定的网络传输平台。

2. 保险行业网络需求分析

2.1 业务数据分析

根据锐捷网络多年来在保险行业的服务经验，我们总结出保险行业主要有如下的业务数据。

第一类是业务系统应用，即为保险企业对外开展业务应用系统的集合，包括人险系统、财险公司的核心财险系统、再保系统、寿险公司的核心业务系统(意外险、健康险、个人寿险、团体寿险)等。第二类是信息管理类应用，是保险支持企业信息管理、企业决策的应用系统和办公自动化系统的集合，也是企业管理的核心应用平台，包括电子邮件系统、远程教育系统、数据采集系统、数据分析系统、财务管理系统、视频会议系统及IP电话等。

分析各类应用的特性，并考虑其业务的优先级、安全性，将上述应用分为以下几类。

1)数据类：包括核心业务系统、批量、业务类批量、管理类实时业务、管理类批量业务等数据。

2)视频类：公司内视频会议系统将根据各公司的业务需要从总公司延伸到省分公司及地市中支公司。这类应用重要性较高，实时性高，对延时和抖动比较敏感。

3)语音类：客服中心Call Center 和日常管理应用中包括的VoIP/IP 电话。语音类应用重要性较高，实时性高，对延时和抖动比较敏感。

2.2 整体需求分析

作为网络传输平台，为了满足业务的正常开展，必须满足如下几个需求：

- 高可用性需求，网络结构必须能够达到甚至超过业务系统对服务级别的要求。通过多层次的冗余连接考虑，以及设备自身的冗余支持使得整个架构在任意部分都能够满足业务系统不间断的连接需求。
- 高安全性需求，作为金融网络，在网络规划和建设方面，首先要考虑生产系统和办公系统数据的完整和安全。网络结构需要具有支持整套安全体系实施的能力，以确保用户、合作伙伴和员工生产、办公的安全。
- 可管理性，支持全域的网络管理，为了保证全网的设备得到实时监控，需要网管平台层面支持全网的监控，同时需要网络层面保证安全、可靠、高效的传输网管信息。
- 统一标准化需求，网络规范遵循业界公认的标准制度一个高兼容性网络结构，确保设备、技术的互通和互操作性，方便快速部署新的产品和技术，以适应业务的快速增长。

3. 锐捷网络保险行业解决方案

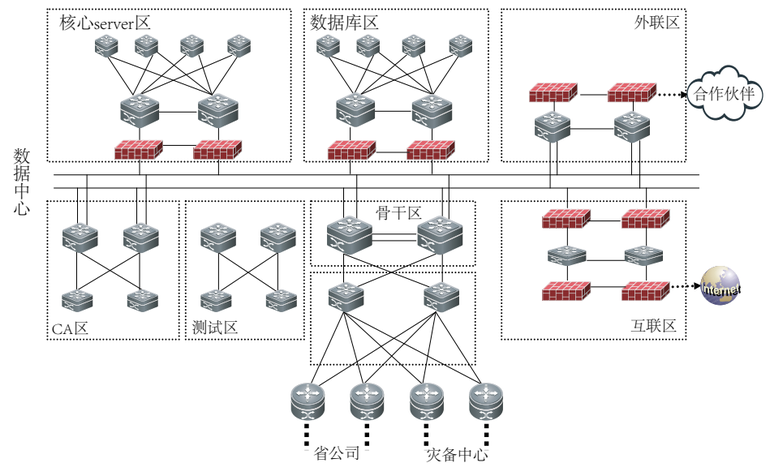
3.1 数据中心解决方案

3.1.1 需求关注点

- 数据大集中以后放置了大量的存储、业务系统、数据库、网络设备等各种资源，数量庞大，如何进行统一规划?
- 作为全国的网络运营枢纽，如何确保网络的安全性和高可靠性?
- 如何实现数据中心集中精细化管理?

3.1.2 网络结构图

数据中心网络结构图如下：

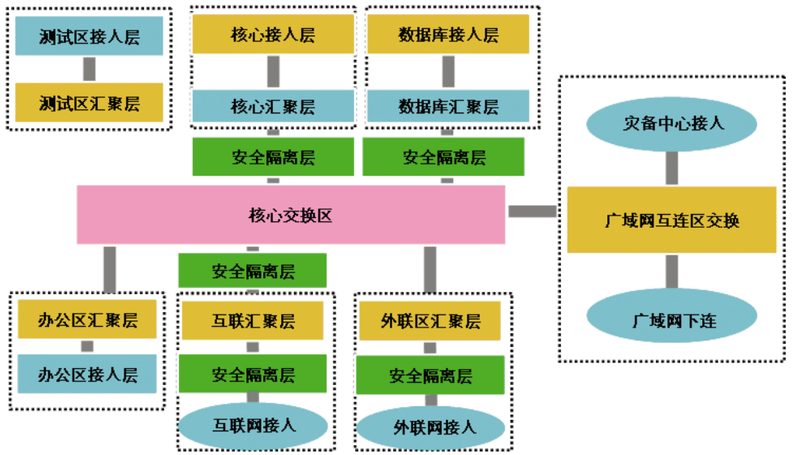


如上图所示：为了降低网络安全风险，提高核心设备的数据处理能力，按照业务功能的不同，对数据中心的网络进行整合分区，分别是骨干区、广域网区、办公区、核心SERVER区、数据区、测试区(考虑到安全性，测试网作为一块独立的区域不与生产网相连)、外联区及互联区。通过功能区的划分，既增强了网络的扩展性，又增强了网络的安全控制能力，在考虑全网安全规划的时候，可以在现有分区的基础上定义不同的安全域，为构建整网信息安全体系打下良好的基础。

3.1.3 方案要点

功能区优化整合

数据中心是全国的网络计算中心，数据大集中以后放置了大量的存储、业务系统、数据库、网络设备等各种资源，数量庞大、管理复杂；传统的网络只是简单通过VLAN 的划分，将内部系统逻辑的划分为业务办公区，外联区、互联区、Internet 办公区等若干网段，实际上核心设备既提供二层之间的交换又提供三层之间的转发，各个区域之间都是基于二层的直接连接，所有的安全策略(ACL)和QOS 也都设置在核心设备上，增大了核心设备的负担和安全风险，会出现任何一个区域出现问题就有可能导致影响全网的重大故障。



锐捷网络利用模块化的设计思路，采用分区、分层设计方法，实现数据中心逻辑功能的模块分区设计，如上图所示：网络功能区包括核心SERVER 区、测试区、数据库区、互联网区、外联网区、广域网接入区等；分层包括核心层、汇聚层、接入层和安全隔离层。通过分区、分层设计使整个数据中心网络层次清晰，实现数据中心高可靠、高安全、易管理的目标。

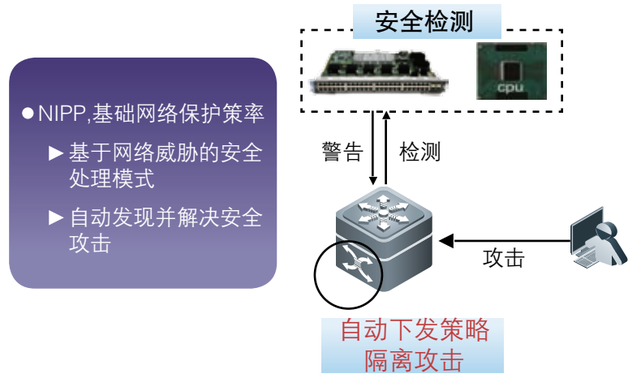
高安全性技术保证

信息安全是各企业构建信息系统时最为热衷的话题，对保险数据中心来说，也是最重要的技术关注点之一，锐捷网络数据中心解决方案的安全技术保证体现在如下几个方面：

- 功能分区优化设计大大提高了整网的安全性，根据功能区业务的重要性，可以直接继承分区优化以后的网络结构直接划分安全域，为整网部署统一安全体系打下了良好的基础。

- 核心区域增加安全隔离层。核心SERVER 区、核心数据库区、互联区、外联区等关键业务区域增加一道安全隔离层。特别是互联出口区域，双层防火墙的设置在中间形成了一个安全缓冲区，通讯前置机放置在本区域，通过访问控制策略实现访问用户对内网资源的合法访问。

- 保险企业网络是一套独立于外网的私有网络，具有很高的安全性，但是在日常工作中不可避免会使用COPY 盘的方式进行业务交互，不可避免会带来安全威胁的可能。锐捷网络NFPP(Network Foundation Protection Policy)基础网络保护策略，在局域网解决方案中可增强交换架构的整体安全的。NFPP 体制通过对攻击源头采取隔离措施，可以使交换机的处理器和信道带宽资源得到保护，从而保证报文的正常转发以及协议状态的正常。



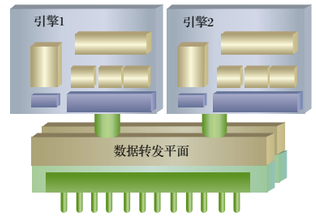
交换自防御系统—智能安全策略下放

高可用性技术保证

实现数据集中以后，保险企业的业务基本上实现了扁平化，终端用户垂直访问数据中心的业务系统和数据库，因此作为业务系统的传输承载平台，高可靠性的设计显得特别重要。

锐捷网络数据中心解决方案网络高可靠性方面的考虑主要基于如下几点：

- 设备级冗余：功能区汇聚采用双设备、双引擎、双冗余配置。



智能高可用IP设计—智能化版本升级

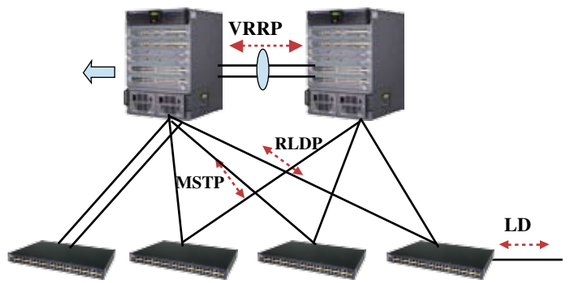
为了提高网络的高可用性，功能区汇聚采用双引擎、双设备互为热备。锐捷S86智能化软件版本升级，全程0 丢包。在线软件升级不中断任何业务，零丢包。主引擎运行补丁软件升级，备份引擎平滑热备切换，业务不间断转发。重启动主引擎，更新至最新软件版本接管设备，全程不丢包。因为可以安装过程不会对正常的分组转发产生任何影响，所以代码验证和部署的速度将会大幅加快。

● 链路、路由级冗余

数据中心各功能区均采用双核心双层网络构架，汇聚层+接入层。核心和汇聚采用全网状相连的方式，采用VRRP+MSTP 技术来提高网络的高可用性。

数据中心有规模大、业务应用多的特点，为了保证数据的转发效率，核心之间、汇聚之间及汇聚与接入之间均采用冗余的光纤相连。

在网络管理和维护资源有限的情况下，管理维护易用性需求变的更加突出。实际应用中如果接入网中发生网络环路、断路、单向链路等问题，故障定位将会变得十分困难。比如在光纤口上光纤接收线对接错，由于光纤转换器的存在，造成设备对应端口物理上是linkup的，但实际对应的二层链路却是无法通讯的。针对这种问题，锐捷有如下的考虑：



故障快速检测机制：RG-S86 系列支持故障快速检测机制RLDP+LD。

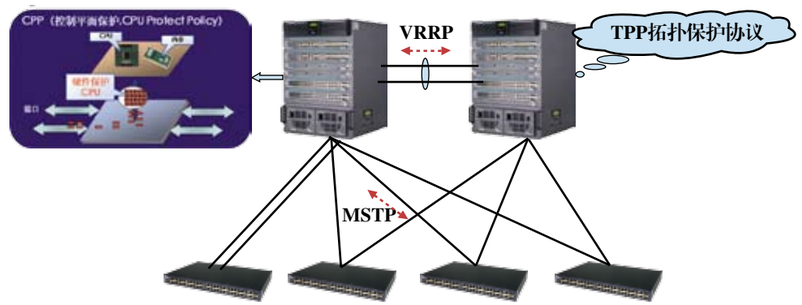
RLDP 实现端口环路检测、单向链路检测、双向链路检测以快速消除网络环路及检测出线路故障。BFD 快速链路检测关联动态路由协议。能快速实现路由、数据的切换。

LD 技术主要定位线缆断点。线缆一般是布置于墙壁内、地下等肉眼无法看到的地方，当发生断路的时候非常难以发现，对排除故障十分困难。线缆检测技术利用时域反射原理可判断线缆断路的地方，并通告管理员断路点到端口的距离，十分方便管理员进行故障判断，大大缩减了故障处理时间。

● 冗余增强型保证技术，CPP+TPP 技术

由于MSTP 和VRRP 等协议均使用定时报文通告机制来自动维护网络拓扑结构，自动适应网络中的拓扑变化。这也给网络攻击者对网络拓扑攻击有可乘之机。当受到人为的网络攻击时，因 CPU 利用率过高或帧通路阻塞等原因，可能造成定时报文的短暂中断，从而造成网络拓扑发生错误的振荡，这给网络的正常通信造成极大危害。当出现这种情况时，数据中心的业务正常运行无法得到有效地保证。锐捷网络数据中心解决方

案CPP+TPP 技术冗余增强型技术保证很好地解决了此一问题，如下图：



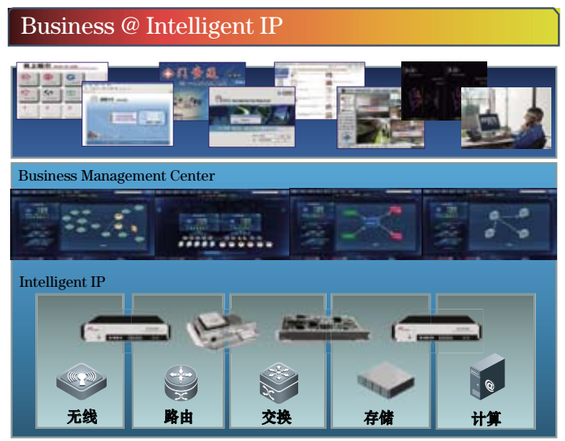
- RG-S8600的CPP功能可以实现对CPU硬件的自动防护，保证设备不会因为协议攻击导致宕机。
- 锐捷独有的 TPP—拓扑保护协议（已申请专利）可有效保证核心的STP和VRRP拓扑在复杂攻击环境中的稳定，防止业务动荡。

锐捷网络三级冗余设计充分保障了保险企业数据中心网络高可靠运行。

精细化管理的实现

对数据中心网络、安全、存储、主机、数据库、应用系统等等，采用传统的独立管理系统已经不能满足数据中心管理的需求，集中化IT 运维管理是数据中心实现精细管理的必然趋势。

锐捷BMCIT 运维管理系统是面向网络融合与虚拟化趋势精心打造的一个可分布式部署，兼容大规模复杂异构IP 网络和IT 计算环境的可扩展管理平台，系统基于标准开放的信息建模技术，实时分布式计算平台和SOA 架构实现，能够通过灵活丰富的管理协议对接各种主流IP 基础设施，包括多厂家IP 网络设备，IP 存储设备，中间件，服务器，数据库和关键应用系统，并提供强大的事件管理，拓扑关联分析和性能监控组件。以一个统一的平台全面地满足数据中心IT 管理的精细化集中管理。



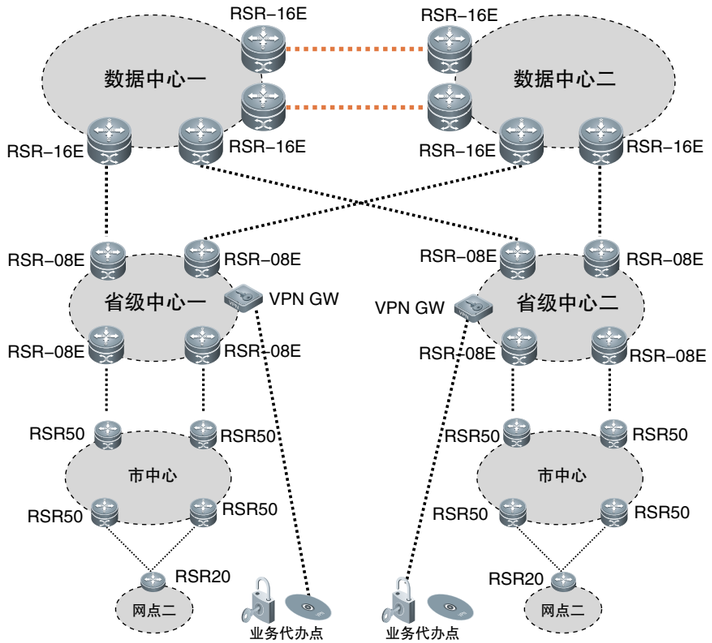
3.2 骨干网解决方案

3.2.1 需求关注点

- 提升业务扁平化后的数据传输效率，满足未来业务增长数据传输需求。
- 在业务逐渐增多的情况下，如何采用合适的服务质量保证技术，保障关键业务的可靠传输。
- 整合网络路由：在整合网络IP 地址的基础上，根据区域、应用、管理层次等原则，优化网络路由、减少管理复杂度、降低管理成本、提高效率。

3.2.2 骨干网结构图

骨干网络拓扑图如下所示：



如上图所示，在一级骨干网上的两个数据中心均通过双链路连接各个省公司，省级公司通过二级骨干网双链路连接下属的地市中支公司。流量从网点分级汇聚到省公司，省公司将流量进行区分，通过冗余链路分别汇聚到生产数据中心和灾备数据中心。为保证网络级的高可靠性，所有的双链路均应由不同运营商提供。

一级骨干网

在数据中心建立独立的广域网区，包括广域网区核心交换机，下联省公司路由器及数据中心互联的核心骨干网路由器。

一级骨干网，包括下联各个省公司的广域接入路由器和两个数据中心互联的核心骨干网路由器。在常态下，下联分公司路由器承载访问本数据中心的业务流量，核心骨干网路由器承载两个数据中心间的业务流量、办公流量和数据同步流量。在单中心广域网络出现故障时，下联分公司路由器除了承载本数据中心的流量外还承载部分访问另一数据中心的流量，这部分流量通过核心骨干路由器直接转发到对方数据中心。

二级网骨干网

在省公司网络中心建立独立的广域网接入区，包括广域网区核心交换机，上联数据中心及往下汇聚二级中支公司的路由器，为双层双路由结构。

如上图所示，省公司的广域下联路由器实现各个中支公司上联汇聚，双链路同时保证链路的高可用。

三级接入网

地市中支公司的下联路由器一般有两种接入方式：本机构的营业网点直接上联到中支公司的广域下联路由器；业务合作代办点一般通过IPSECVPN 的方式，直连省公司VPNSERVER。关于VPN 接入方案，详见后文描述。

3.2.3 方案要点

统一广域网接入平台

数据大集中以后，虽然省公司还有部分业务系统处于过渡状态，少量服务器还放置在省公司，但是总体来说大大减少了服务网点到地市中支公司、省公司数据访问的环节，业务趋于扁平化。通过构建独立的广域网接入平台，支持生产、OA 等多业务同时传输，统一的传输网络不但可以为各种应用提供负载均衡，还可以避免单点故障，增加网络的可靠性，提高防备灾难的能力。

通讯线路的选择

考虑到保险一级骨干网多业务服务以及业务增长的需求，网络带宽需要适应业务的变化。从目前国内电信服务的状况以及金融同行业的应用案例，目前业界常见的接入方式列入下表。对于二级骨干、三级网的线路资源选择。

	ATM/FR	SDH	MSTP
线路带宽	2M以内	2M	2-100M
带宽灵活调整	2M以内可平滑升速	固定2M（采用捆绑的方式进行扩容）	2-100M 可平滑升速
资费	较低	较低	较低，与带宽大小成正比
汇聚设备成本	ATM 板卡，成本较高	STM-1 板卡，成本高	以太网板卡，成本较低
下端设备成本	同步串口，成本较低	同步串口或E 板卡，成本较低	以太网口，成本低
线路维护成熟度	成熟较高，维护方便	成熟度高，维护方便	目前较稳定，维护相对不便

线路选型原则建议如下：

一级骨干网建议租用两家不同运营商的ATM 线路，每线路带宽20M+2*N。

二级骨干网建议租用两家不同运营商的ATM 线路，每线路带宽10M+2*N。根据当地MSTP 发展情况，成熟、稳定、覆盖率高的地区可以采用MSTP 线路。

三级网建议租用1-2 条2M SDH 或MSTP 线路。

路由协议的选择

省公司上联路由器到生产数据中心、灾备数据中心各具备一条通信链路，其中一条发生中断时，不会影响网络正常运行。业务数据流量可以被重路由到灾备中心核心网节点，通过数据中心间的骨干网络通信链路，连接生产数据中心。当故障通信链路恢复后，业务数据流量能恢复到常态路径。同理，二、三级骨干网的数据流向也必须遵循路径冗余原则。

锐捷网络保险企业骨干网解决方案在路由协议的选择和设计上，方法如下：

- 选择的广域网路由协议为非某厂商私有的路由协议，而是业界的标准协议，是众多设备厂商都支持的协议。
- 路由分区分界，实现路由隔离，为防止局部路由振荡对银行整个网络的影响，如二级骨干网选择OSPF，边界路由器定义在省公司下联路由器，每个地市一个AREA分区。这样能隔离不同层次的路由。

- 数据分流，省公司分别连接生产数据中心和灾备数据中心，地市中支到省公司也有冗余链路连接；为在多条连接上分别支持不同的数据流，通过策略路由的方式实现不同业务数据流在两条链路上负载均衡并互备。
- 在IP 地址规划完成的基础上，在各级广域网路由器上进行路由汇总、降低网络局部抖动对整个网络的影响；减少路由器的压力和路由表的维护。

全网业务保障策略

根据业务的优先级，对不同应用流量进行识别标记、进行不同业务的划分。对业务、语音、视频等不同业务的数据流量，进行不同传输优先等级、带宽占用比率以及不同数据丢弃优先级的区分服务，制定相应的服务质量保证策略。

流经广域网路由器的数据流，采用DSCP 技术对不同的业务数据流量，基于目标IP 地址、TCP 端口号进行标记。在各级分支机构的广域网出口方向，采用LLQ 以及WRED 技术对不同优先级和不同类别的业务流量进行实时优先队列输出控制，对不同优先级数据包进行丢弃控制。在语音网关路由设备上采用相应的压缩技术，进行带宽的优化利用，减少广域网带宽的费用。

锐捷网络RSR 系列路由器，支持广泛的QOS 拥塞管理和拥塞避免技术。

拥塞管理：FIFO、PQ、CQ、WFQ、CBWFQ、LLQ、RTPQ
拥塞避免：RED、WRED
流量监管：CAR、LCAR
流量整形：GTS
链路效率：CTCP、CRTP

统一软件平台RGOS 提供了REF（锐捷快转技术），保证了设备的高性能，提供了流表技术，可以保证在启用了ACL、QOS、NAT、PBR 等业务后，对性能没有影响。

3.3 局域网解决方案

数据大集中以后，保险公司各省分公司的服务器数量逐渐减少，信息中心局域网主要包括所有网络及安全设备、少量服务器及楼层生产和办公PC；作为省辖内办公、运营中心枢纽，网络要求具有很高的可靠性、安全性。主要有如下需求关注点：

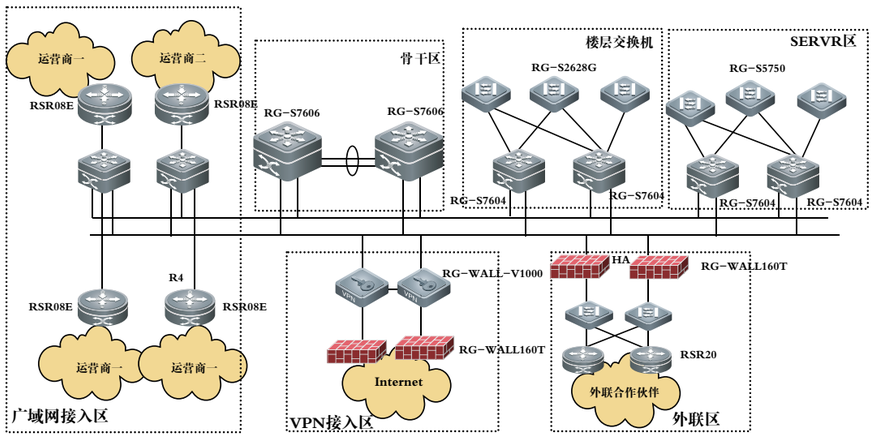
3.3.1 需求关注点

局域网的高安全、可靠性– –作为省运营中心枢纽，需要充分考虑设备本身的高安全性、冗余设备/引擎、网络构架的冗余链路、三层路由冗余等多级冗余设计方式，保证省中心网络高安全可靠。

统一互联出口 ––在金融行业里，保险企业在业务办理的时候需要和Internet 交互最多的企业，如何在提升工作效率的同时，保证整网的安全性，是省中心网络需要考虑的主要问题之一。

接入网安全控制––保险行业普遍存在两种接入方式：和外单位进行业务交互(如和保险协会)，为了降低接入成本，采用VPN 的方式和服务网点或业务代办点进行连接，如何控制此类接入的安全，也是省中心网络网络管理者需要考虑的问题。

3.3.2 局域网络结构图



为了便于网络管理及今后全网信息安全实施，对省公司局域网络也做了相应的功能分区，包括：广域网区、骨干区、外联区、VPN 接入区、SERVER 区、楼层接入区等六个分区。各功能区汇聚层均采用双核心构架。

3.3.3 方案要点

局域网络高可靠、安全性保证

RG–S7600 系列交换机是锐捷网络推出的以业务为核心、面向下一代网络的万兆骨干路由交换机，产品采用模块化设计和RG–S86 使用相同的RGOS 软件平台。设备本身和RG–S86 一样具有高安全性、稳定、高可用性等所有的特性。

在组网设计上，也参考了数据中心的组网模式，充分采用了如下的技术：

- 设备级冗余：功能区汇聚采用双设备、双引擎、双冗余配置。
- 链路、路由级的冗余：各功能区均采用双核心双层网络构架，汇聚层+接入层。核心和汇聚采用全网状相连的方式，采用VRRP+MSTP 技术来提高网络的高可用性。
- 冗余增强型保证技术，CPP+TPP 技术。可以避免因 CPU 利用率过高或帧通路阻塞等原因，可能造成定时报文的短暂中断，从而造成网络拓扑发生错误的振荡。保证业务正常运行。

网络边界的安全控制

包含如下几部分内容：

- 外联网的接入安全––省公司和外联合作单位有业务往来，如保险协会，对与保险企业内部来说，保

险协会的网络是不可信及不可控的，为了对内网资源进行更好地保护，建议在外联网入口部署两台100M 防火墙，配置为HA 模式。对外联单位对内网资源的访问进行安全控制。

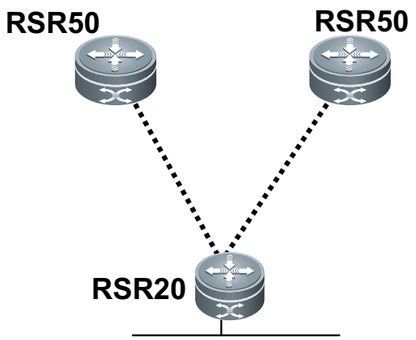
- VPN 接入的安全控制 ——VPN 接入是保险企业常见的接入方式之一，主要为企业、业务代办点建立业务往来关系，当用户成功拨入网络后，意味着成为了内网合法的用户，访问的资源不可控制。为了降低访问风险，建议在VPN入口处部署一台100M防火墙，对拨入用户需要访问的资源进行访问控制。

统一互联出口安全控制

保险行业在进行相关业务办理的时候，需要上Internet 进行相关的查询操作。现在互联出口组网模式比较松散，在辖内网中存在大量的威胁入口。因此需要对互联出口进行统一整合，严格实施安全控制策略，以保障整网的安全。详细的解决方案见锐捷网络“金融行业统一互联出口解决方案”。

3.4 网点解决方案

3.4.1 方案一：采用专线接入



保险企业统一核赔核保业务上收到省公司以后，由于保险企业业务的特殊性，特别是财险业务，进行业务的办理的时候，需要有大量的图片数据，因此三级网链路的带宽需求逐渐增大，建议至少采用2M。网点路由器使用RSR20 系列路由器，采用单设备单线路或双线路的方式上联地市中支公司。

该路由器融合了路由、交换、语音、安全、传输、视频等多种网络应用，满足用户不同应用环境的个性化需求。具有如下的技术特性优势：

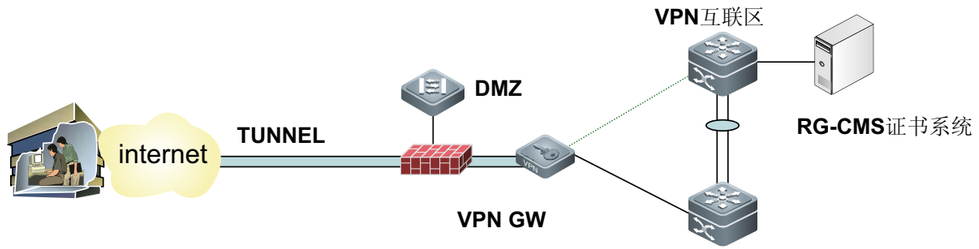
1、加载业务后的性能保证：锐捷RSR 系列路由器统一软件平台RGOS 提供了REF(锐捷快转技术)，保证了设备的高性能，提供了流表技术，可以保证在启用了ACL、QOS、NAT、PBR 等业务后，对性能没有影响。

2、数据平面转发平面分离V-CPU 技术：在网络负载大时，会导致设备CPU 利用率很高，在这种情况下将最终导致远端用户无法登陆设备，即使登陆成功也无法进行正常的操作。问题的根源是路由器上数据转发占用了所有的CPU 资源，这时管理和控制已经没有CPU资源来处理了。锐捷RSR 路由器的V-CPU 技术能很好地解决这个问题，在设备CPU 利用率很高的情况下，登陆设备、命令行操作依然流畅。

3、抗DDOS 攻击特性：锐捷RSR 路由器统一软件平台RGOS 提供了状态防火墙功能，让RSR20 在受到100M 的线速DDOS 攻击情况下，大幅度的降低路由器的CPU 利用率，提升设备稳定性。结合V-CPU 技术，保证在线速的DDOS 攻击下，不影响任何的数据转发性能和管理控制。

3.4.2 方案二：采用VPN 的方式接入

VPN 具有成本低廉、高安全性、部署方便等优势，因此VPN 接入是保险企业常见的接入方式之一，主要为企业、业务代办点建立业务往来关系。



VPN 隧道的建立

如上图所示：

在省分公司部署锐捷RG-WALL V1000 作为VPN SERVER 提供VPN 连接服务。客户端可用采用两种方式：

RG-WALL V50 和RG-WALL V1000 建立site to site 连接。采用动态的L2TP+IPSec的VPN 应用模式。

客户端加KEY 的方式，客户端PC 安装一个客户端软件，指定远端VPN SERVER，采用动态的L2TP+IPSec 的VPN 应用模式。

统一密钥管理–集中维护

安全证书和密钥的集中维护，管理员对生成的证书和密钥有各种操作的权力，如生成、查看、删除、下发等。普通用户只能对管理员分发给他的证书和密钥进行下载操作，这保证了证书和密钥的管理和使用是集中的。

统一密钥管理–远程分发

移动用户只要远程登录证书管理系统服务器，经过了身份验证，就可以下载VPN 安全远程接入系统（RG–SRA）软件，从而极大地减少了管理员分发软件的工作量。

统一密钥管理–支持多种CA 根

管理员在为VPN 设备生成证书之前，可以对生成证书的CA 根进行选择，比如可以选择系统本身自带的CA根，也可以导入第三方CA 根，同时还可以重新生成新的CA 根，从而对于某些特殊应用实现CA 证书的定制。

敏锐把握应用趋势 • 快捷满足客户需求