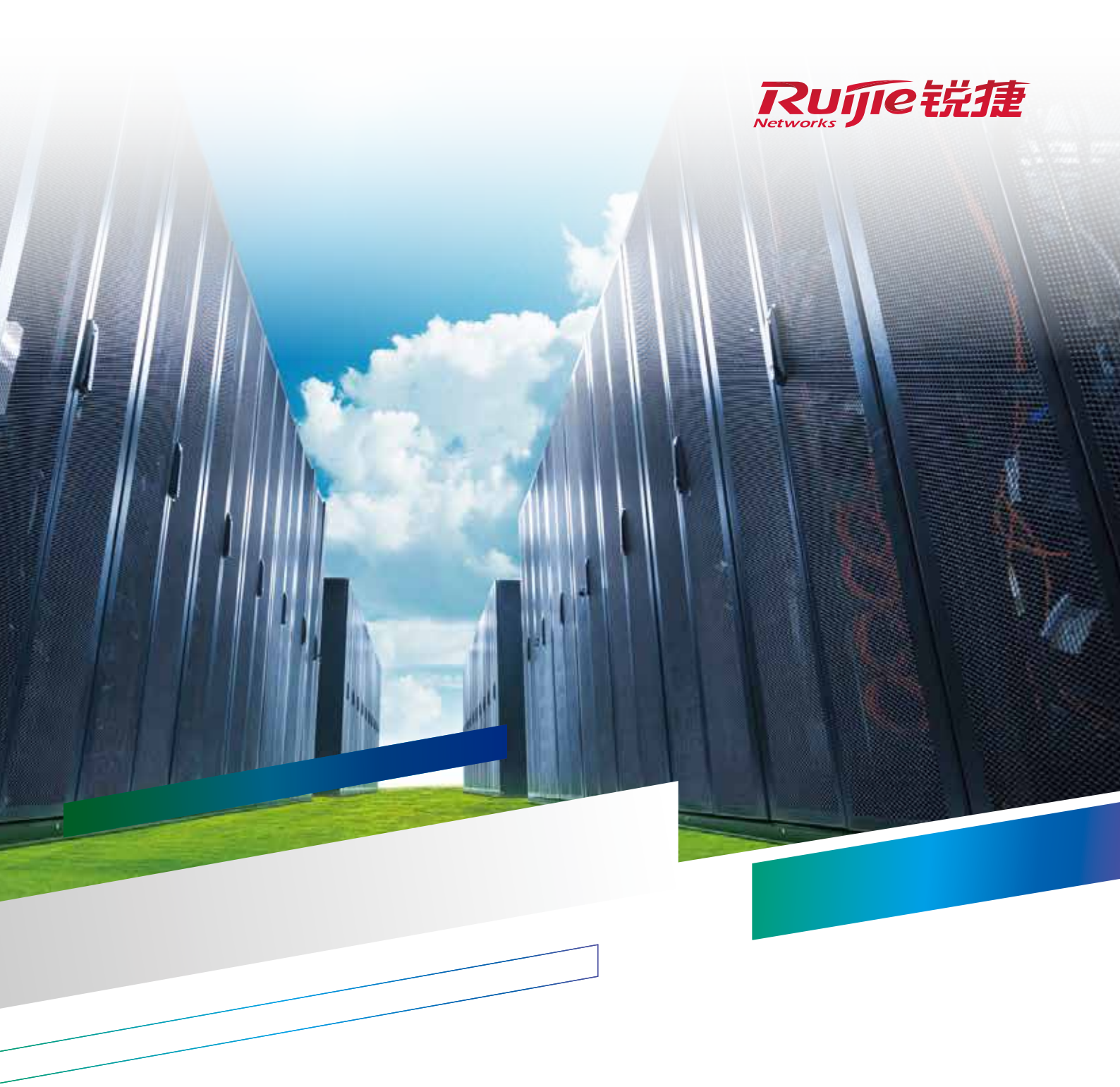


Ruijie Networks 锐捷

按需定义
简单您的网络

锐捷SDN专刊

www.ruijie.com.cn

目录
Catalogue

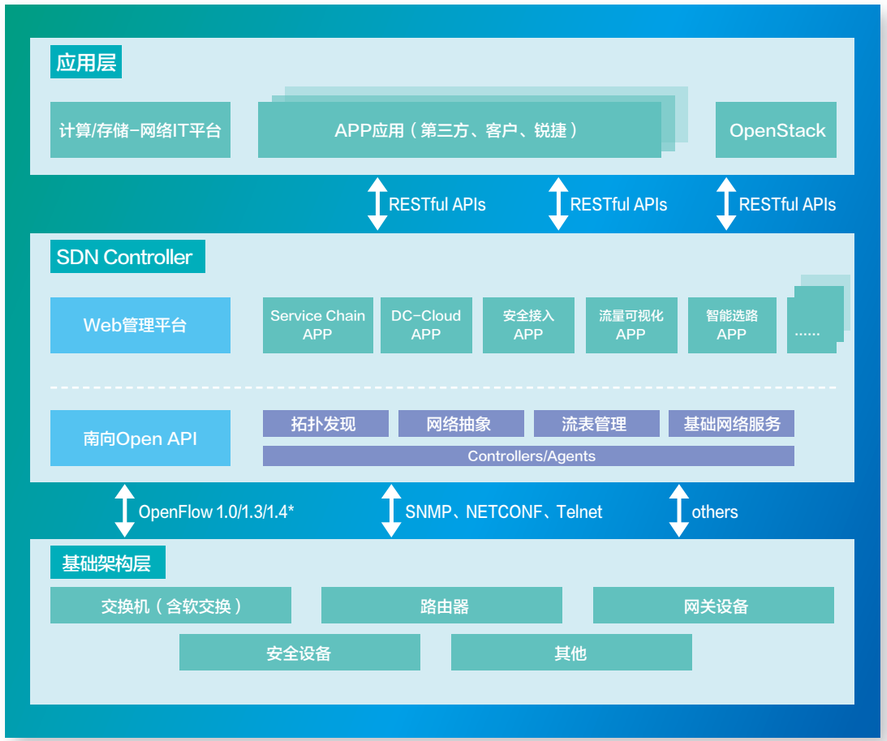
- **锐捷ONP开放网络平台介绍** 01
- **锐捷网络RG-ONC开放网络控制器介绍** 03
  - 开放
  - 可编程
  - 灵活交付
  - 支持 NFV
  - 高可用
- **锐捷云园区方案** 07
  - 接入控制
  - 策略随行
  - 虚拟业务网
  - ServiceChain
- **锐捷云数据中心方案** 18
  - 自动化部署
  - 租户网络按需创建
  - 网络资源统一管理
  - SDN 精细化运维
  - 安全资源池
  - 双活数据中心
- **VXLAN技术篇** 21
  - VXLAN 背景及起源
  - VXLAN 解决的问题
  - VXLAN 技术简介
- **锐捷网络SDN开放合作，构建生态圈** 24
- **锐捷SDN行业故事会** 25
  - 中科院高能物理研究所
  - 某国家网络中心
  - 山西省政务大厅
  - 武汉大学
  - 四川大学
  - 湖北中医药大学
  - 福建省广播影视集团
  - 中烟工业山东卷烟厂
  - 昆山二院
  - 华山医院
  - 中国邮储银行
  - 歌华有线
  - 郑州教育城域网

01
锐捷ONP
开放网络平台介绍

RG-ONP（Open Networking Platform），是锐捷网络遵循SDN理念，全面拥抱未来而推出的新一代开放网络平台。此平台主张开放化、虚拟化和智能化，旨在让未来网络更简单。

ONP 开放网络平台
- OPEN NETWORK PLATFORM -

锐捷ONP开放网络平台，主要包含开放网络控制器RG-ONC和支持SDN特性的交换机、路由器、防火墙等产品，可构建覆盖园区、数据中心、广域网络场景的特色APP化解决方案。



锐捷网络SDN研究发展历程

2011 年

开始投入研发力量
做 SDN 相关的技术储备
做 SDN 相关的产品预研

2012 年

作为“中国 SDN 与开放网络专业委员会”12 家初始会员之一，参加第一届高峰会议

2013 年

3月:
开始研究企业内网SDN通信技术及方案
10月:
参加中国首届SDN测试大会，ShowCase控制器原型

2014 年

3月:
和中科院高能物理研究所共同开发SD-WAN方案
开始研究数据中心虚拟化，进行多租户网络方案开发
5月:
参加全球SDN技术大会，展示RG-ONC控制器、多租户网络、广域网链路负载均衡、企业网L2/L3层通信等多种解决方案
7月:
提出“服务链解决方案”
参加电信研究院SDN控制器内部测试

2015 年

2月:
参加EANTC和北京邮电大学联合举行的SDN测试
5月:
参加ONF组织的SDN ShowCase，并首个在会上展示SDN网络下的Web接入准入控制方案、SDN+VXLAN的云数据中心方案
7月:
领先业界推出可商用SDN控制器
推出园区网接入控制方案

2016 年

4月:
参加中国SDN/NFV大会
推出数据中心SDN+VXLAN多租户方案
5月:
参加全球SDN/NFV大会，并进行ServiceChain方案ShowCase，SDN数据中心方案展示
Newton 18000等10款产品获得OF1.3认证
12月:
获工信部和51CTO主办的 “IT印象·技术成就梦想” 最具创新力奖

02
锐捷网络RG-ONC开放网络控制器介绍

RG-ONC （Ruijie Open Networking Controller ）是锐捷开放网络平台RG-ONP（Open Networking Platform）的核心控制组件，即SDN控制器。

锐捷开放网络控制器RG-ONC采用Java OSGi模块化技术架构，在满足软件包可扩展的同时，支持组件在线升级，并可兼容多个版本同时运行。通过开放的北向API接口，RG-ONC开放网络控制器还可支持各类APP应用扩展，从而满足园区网、数据中心、城域网、广域网等各类场景的业务部署需求。

锐捷开放网络控制器RG-ONC可支持数千个网络设备节点的集中管理调度；可支持百万条流表、上万个子网；适应各种规模的SDN网络控制需求。

开放

锐捷开放网络控制器RG-ONC采用开放的、业界通用的标准协议来管理和控制整张网络。RG-ONC支持ONF组织定义的标准框架、协议（如Openflow）。RG-ONC通过Openflow协议进行流表下发，进而对网内所有支持SDN的网络转发设备进行控制。目前可支持最新的Openflow版本V1/V2/V3，并且向下兼容。

RG-ONC北向接口采用标准的RESTful API接口。此接口遵循标准HTTP协议，调用起来简单、易用；调用者与被调用者之间完全松耦合关系，无需传统复杂的调用过程（包括无需SDK库函数加载、识别，不受编程平台与编程语言约束）。因此，RG-ONC采用RESTful API能够让SDN控制器提供的北向API接口更加容易与各类云平台、网络运营／运维平台、大数据分析平台以及其他第三方应用进行对接调用。

可编程

锐捷开放网络控制器RG-ONC具备极强的可编程性，并提供一系列完善的调用接口，用户可通过详细的调用案例模拟和学习，完成与上层平台对接并感知软件定义网络的魅力。通过调用RG-ONC提供的北向API接口，可以对网络资源进行个性化定义，并且可以编写多个应用对整个网络进行重新定义。这样使得网络、控制、管理、运维等系统形成完整的链条，并且能够通过不同场景所需的APP来优化、控制和管理整网。

灵活交付

锐捷开放网络控制器RG-ONC提供软硬件一体和纯软件两种交付方式。软硬件一体化交付，硬件采用通用X86服务器，预灌装RG-ONC软件；用户仅需上电开机，激活不同APP授权，即可部署不同场景的特色化解决方案。

同时，软硬件一体交付方式的硬件载体RG-ONC-AIO-E机箱可支持最多四个控制节点插卡，每个控制卡均配置6核CPU，32GB以上的内存。满足高性能的同时，提供最优的部署方式选择。客户初次部署时，可先部署一张控制节点。随着规模扩大，可继续添加新的控制节点。因控制节点为X86架构，且有不同性能的配置，未来可以将需要的NFV功能放入其中，让网络组建更灵活。对客户而言，采用此套方案，客户可以轻松的对网络功能、性能进行灵活增减。这样对于SDN的灵活度又有了很大的提升。

支持NFV

锐捷开放网络控制器RG-ONC支持NFV功能，并且能够利用网络功能虚拟化技术将多个不同网络设备提供的功能进行抽离。例如虚拟防火墙，虚拟应用网关等一起放入RG-ONC内部进行运行。这样不仅管理简便，而且成本得到大幅缩减。不仅如此，未来如果虚拟防火墙等NFV产品用处不大，完全可以直接登陆SDN控制器进行功能卸载，同时也可以采用类似手机安装APP的方式将新增功能加入RG-ONC。一台控制器具备了NFV功能后，不仅可以灵活控制网络资源，而且可以将很多网络功能加入到统一的控制器内部，这样全网即可实现统一化管控。

高可用

锐捷SDN控制器支持主备、集群等部署方式。采用此方式能够解决部署单点SDN控制器带来的风险。当控制器组成集群后，只要网络中还有控制器存在，都不会存在网络不可控，不可管的状态。当然，如果所有控制器均失去作用，原流表依然会在所有支持Openflow交换机中进行正常通讯。换而言之，控制平面的失效不会影响数据平面的正常通讯。

标配2块1600W电源，单块电源可满足4个控制器节点满负载供电，2块电源可实现1+1冗余

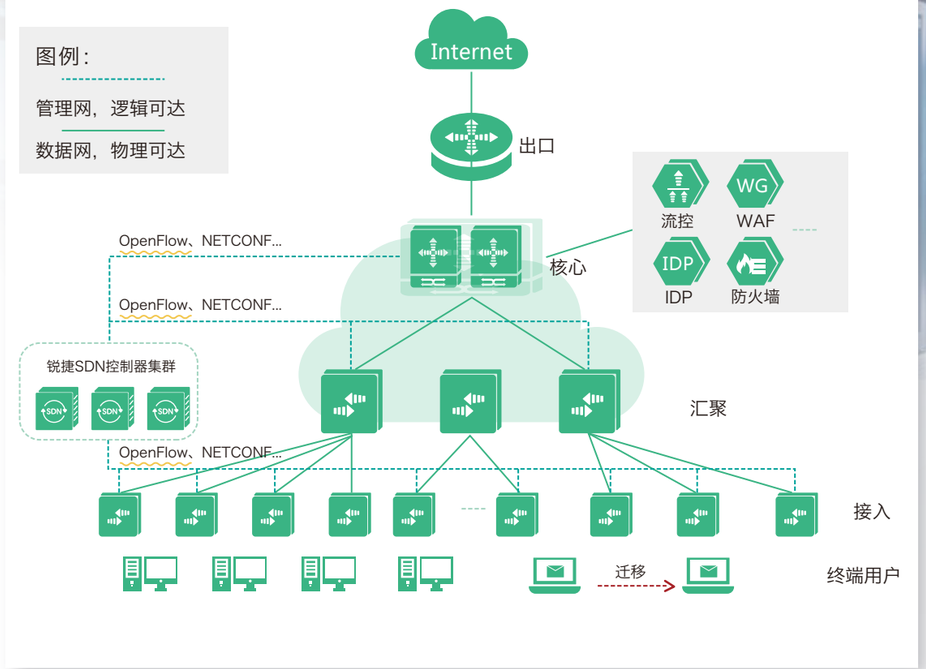
支持最大12个独立硬盘槽位，每个控制器节点对应3块槽位，可实现硬盘1+2冗余

最大支持64台控制器进行群，保证控制器系统的可靠性

03 锐捷云园区方案

随着移动互联全面兴起、云服务逐步普及，企业需要高效、灵活、易扩展的基础网络。SDN因其快速（快速完成网络部署）、灵活（灵活进行业务调整）、高效（大幅提升网络运维效率）、可视（全网流量可视）、开放（开放的第三方对接接口）等特点，将网络控制与转发解耦，构建开放可编程的网络架构。SDN重构基础网络，让基础网络随时为业务调整而就绪。

锐捷云园区（Campus-Cloud）方案秉承极简的理念，融入SDN相关技术和产品，旨在让基础网络进入场景化时代，包含接入控制、策略随行、虚拟业务网、ServiceChain等组件，通过按需部署，实现基础网络快速部署、全网资源统一管理、按需调度，面向业务提供更加快捷、灵活的基础网络支撑和服务。



接入控制

随着企业信息化水平的提高，企业为了更好的服务于用户，会引入各种类型终端接入网络，以提升员工的工作效率。同时，企业会尽可能把网络铺设到办公区的每个角落，满足随时随地的移动办公需求。但是大量的终端接入网络，给企业带来了很大的信息安全隐患。如何满足终端随时随地的安全接入网络成为关键。

传统网络接入准入控制现状

IP地址分配方式：分为静态IP和动态IP两种方式。基于安全考虑，通常会进行终端的准入控制，合法的终端才允许接入网络。而通常的准入控制方案一般使用准入认证（802.1X/WEB等），但准入认证会引入诸如稳定性差及维护麻烦等问题（认证服务器故障可能导致终端无法入网从而导致业务中断），因此部分客户会在接入设备上进行IP+MAC绑定替代准入认证。

对于IP地址静态分配的场景下，IP+MAC绑定作为准入控制方案，存在的问题

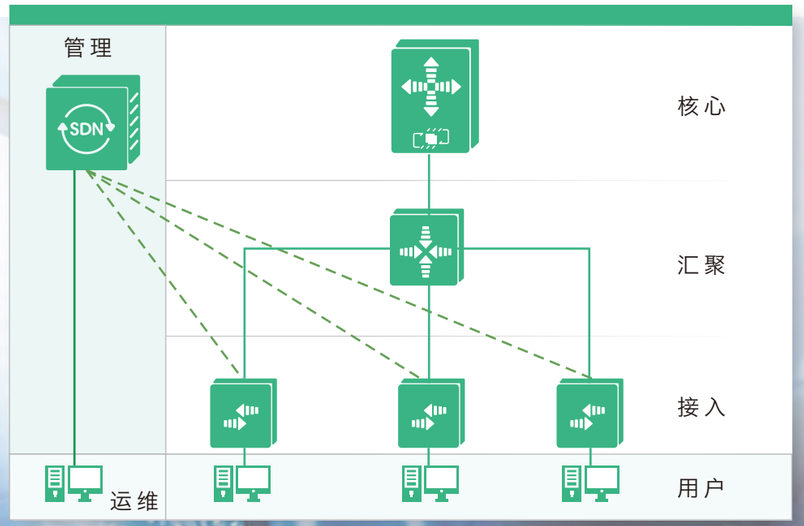
- 效率低，易出错：IP规划完毕以后，需逐台在接入交换机进行手工IP+MAC绑定，执行过程繁琐且易出错，维护困难。
- 灵活性差：员工因为部门调整、办公区装修、移动办公等需求带来的终端位置发生变化。此时，不仅终端的IP地址需要重新分配，而且需要在新位置所属的交换机上重新进行IP+MAC绑定。如果迁移用户数非常多的话，就会给网络信息部门带来极大的工作压力。

对于IP地址动态分配的场景下，IP+MAC绑定作为准入控制方案，存在的问题

- 灵活性差：DHCP无法基于合法用户进行IP地址分配（对应的MAC固定分配相应的IP地址，实现类似静态IP的效果）。
- 配置繁琐：地址分配完成后如果要进行IP+MAC绑定则需要在接入交换机上配置DHCP Snooping + IP Source Guard。

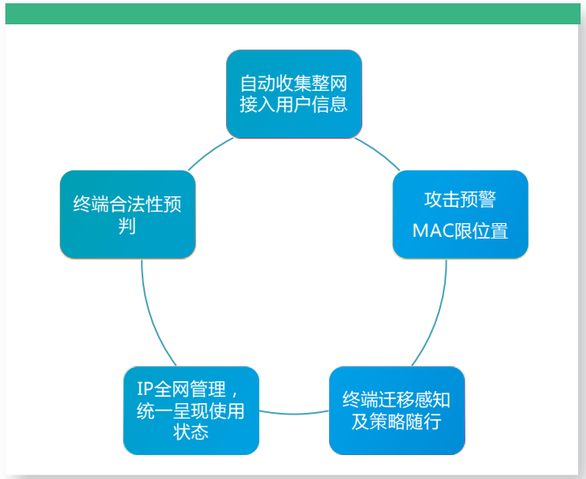
SDN接入准入控制方案

通过SDN控制器替代手工操作，通过SDN控制器和接入交换机设备的联动，有效提升工作效率的同时，确保准备性和及时性。



整个方案带来的效果

- SDN控制器通过0penflow下发ARP代答指令给接入交换机，同步收集整网接入终端的网络信息，如IP、MAC、VLAN、PORT等。同时，网络信息以及资产管理等台账信息也可以按照模板进行批量导入导出操作，方便管理员集中管理。
- 终端接入网络时，SDN控制器会把新用户的信息和控制器维护的用户信息库进行自动匹配，通过管理员提前设置的模板和阀值，来判断终端的合法性，并执行放行、隔离、待审批等动作。
- 在判断终端合法的同时，进而判断终端的位置变化信息，确保策略跟随用户移动。同时，可以将同一个业务部门，或者相同业务类型的终端拖进同一个策略组中，实现统一管理，减少管理员重复工作的效率浪费。
- 对于网络中打印机等哑终端，可以通过MAC地址限位的方式，阻止非法用户通过模拟哑终端的地址发起的攻击行为。
- 无论是静态分配IP，还是动态分配IP，SDN控制器可以自动统计，并图形化呈现IP资源使用状态，方便管理员对IP资源及时回收、统一管理。



以上仅为接入控制组件的关键功能，其通过图形化界面勾选点拽的方式，可以实现更多人性化的操作，帮助运维人员轻松实现各种终端的安全准入控制和统一管理。

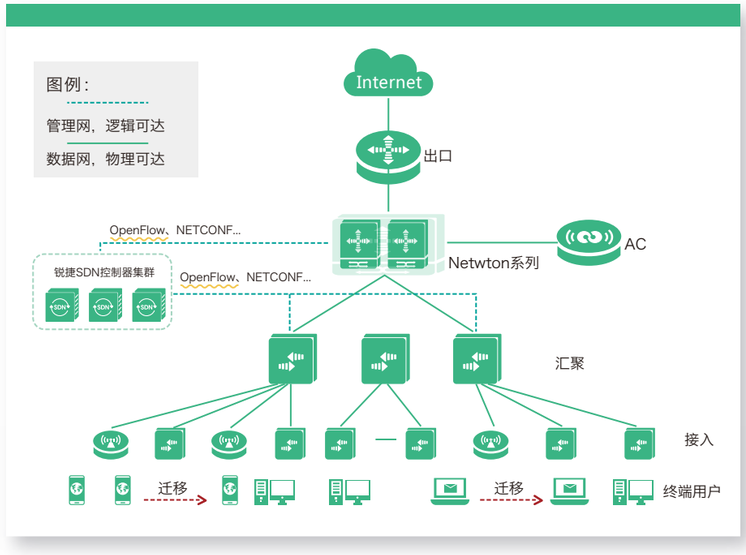
策略随行

由于BYOD、移动办公、企业组织架构调整等原因，导致员工及终端办公设备的物理位置不再固定，对于办公体验和运维来说会带来一系列问题：

- 员工跨分支机构出差，或者移动办公后，原本可以访问的业务系统访问不了了，本来不能访问的涉密系统却可以访问了；
- 员工部门调整，或者公司组织架构调整，运维人员需要重新配置每个终端的访问策略。如果涉及到IP地址静态分配情况，且访问策略按照物理办公区域规划，调整会非常大，运维人员的工作量也会多而繁琐，且很容易出错。

如何保证员工在不同的位置接入网络，都能享有相同的办公体验，而且可以有效避免非法终端的接入，成为提升企业效率的关键因素。

锐捷网络策略随行组件，可以在尽可能不改变原有网络架构的前提下，实现全网策略的统一部署与自动同步，确保全网策略一致，让用户自由移动的同时享有一致性业务体验。同时，基于用户组的QoS策略部署，在网络资源有限的情况下，优先转发VIP用户的流量，保障关键用户的业务体验。



如何最大化减少现有网络的影响，进行SDN网络平滑升级？

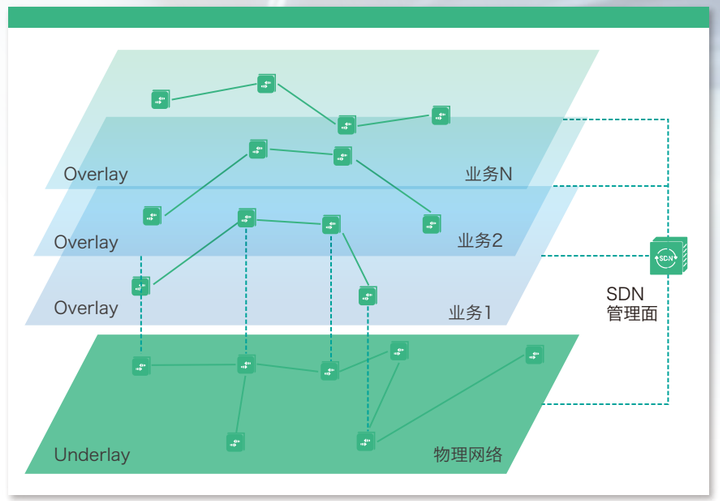
锐捷策略随行组件，利用开放网络控制器RG-ONC统一下发策略

- 可以根据客户现有的网络结构决定策略下发到接入设备还是核心设备
- 可以支持静态、动态分配IP地址场景下的策略随行，全网终端任意迁移，IP不变、策略随身、体验一致
- 可以支持有线环境下的策略随行，亦可以支持无线环境下的策略随行

策略随行带来的好处不仅如此，在新时代的办公环境下，通过开放网络控制器RG-ONC配套的精细化、人性化细节设计，让运维人员得到更高效的管理体验，让网络人员得到更随心的移动办公体验。

业务虚拟网

何为虚拟业务网？即为每一种业务都赋予一张逻辑上独立的网络，让每一种业务都有独立网络体验的同时，提升物理网络的资源使用率、运维人员效率，让物理网络随时为业务就绪。



目前，由于业务所需，用户会基于不同业务新建物理网络。如在一个高校环境中，学生上网需要一张物理网络、老师教学需要一张物理网络、校园安防监控需要一张物理网络、校园广播需要一张物理网络，甚至不同院系为了满足各自的需求，还会去新建一些小规模的独立物理网络。这么多张物理网络让网络信息中心在运维的时候情何以堪！维护吧，不是自己建的，没绩效。不维护吧，属于网络范畴，且应用使用方并不专业，维护不起来。而这些物理网络不能融合在一起的原因除了组织架构边界外，还有网络技术本身的问题，无法简单、有效的为不同业务进行隔离、并保证其传输体验。

锐捷网络虚拟业务网组件，采用SDN和VXLAN技术，实现在一张物理网络上构建出多张逻辑虚拟网络，每张虚拟网络承载不同的业务，每虚拟网络都有其自己的带宽、优先级等QOS保障机制，让承载其上的业务享有和物理独立组网一致的体验。

其次，多网融合之后，SDN控制器提供统一的规划和管理界面，可以大幅简化网络管理的复杂度，提升运维人员的工作效率。避免不同部门之间的扯皮，网络部门就专心做自己最专业的网络规划和运维工作，其他业务部门只需向网络部门提出需求，不需要干涉网络内部的事情。

最后，让用户的资源合理的投入，最大化发挥价值。

ServiceChain

随着企业业务的不断发展，网络规模也在逐步扩大，对于网络流量安全性的要求也是越来越严格，如何实现安全设备的统一调度，最大化的发挥其价值？如何精细化的调度流量，确保所有流量都能够按需防护？如何保证业务变动时，基础网络可以随时就绪，达到业务与基础网络解耦？ 这些都是ServiceChain方案需要回答的问题。

目前传统的网络建设中，网络出口一般游走在两种模型之间

第一种模型：安全设备部署在各个区域的边界，做物理上的安全隔离，或者部署在网络出口设备与核心设备之间，呈糖葫芦串的方式，让流量物理上只有一条流路径。但无论哪种方式部署，带来的结果都是安全设备僵硬化，无法按需调度安全资源，带来资源的极大浪费。总结起来，这几点是现有网络存在的通用性问题：

- 单点故障：安全设备串行部署，串行链路中任何一台设备，或者链路故障，整个出口都会Down掉,故障点非常多
- 动网断网：设备升级，设备更换，网络割接，业务都需要中断
- 性能瓶颈：串行链路上，安全设备品牌不一，性能参差不齐，整个出口性能就低不就高
- 利用率低：对于串行链路上的设备，不管流量是否与自己相关，都得处理，客户无法按需定义流量，并绕过不相干节点
- 功能伸缩性差：因业务上线等，需要增加、升级安全设备，会造成断网，且需要重新规划出口，无法弹性伸缩
- 运维复杂：多品牌安全设备，无统一网管辅助，需独立维护，运维复杂且效率低

第二种部署模型：安全设备旁挂部署，形成安全资源池，通过策略路由的方式按需引流。但由于策略路由的复杂性，在使用过程中亦存在如下问题：

- 略复杂：需要逐个设备进行策略配置，复杂度高，易出错
- 技术门槛高：需要提前对整个区域做整体规划，定义好流路径，技术门槛要求高，且理解困难
- 功能伸缩性差：扩容或者替换安全设备，需要调整整体规划，并且重新做策略，不够灵活
- 运维复杂：没有清晰的界面和逻辑流路径呈现，全凭纸质记录或者CLI分析

ServiceChain方案

一改传统串行部署的方式，所有的安全设备采用旁挂的方式，部署在核心交换机周围，形成安全资源池。安全设备可根据用户需要，选择采用二层透明模式或者三层路由模式部署，实现流量自由定义，并按需牵引。同时，可通过RG-ONC 界面勾选，实现流量来回路径一致，保证安全策略处理的正确性。

ServiceChain组网方案和传统组网方案的优劣势对比

方案	出口安全设备串行部署	出口安全设备旁挂部署，PBR策略引流	出口安全设备旁挂部署，SDN引流
物理灵活性	单点故障多	单点故障少	单点故障少，可Bypass
部署复杂性	较简单	简单	简单
性能伸缩性	非常差，加设备、减设备必然断网	差、	非常简单，加、减设备不断网，即加即用，策略简单
设备利用	非常低， 串行部署，性能就低不就高，新设备上线，老设备很难利旧	加、减设备不断网，但是策略配置复杂 高 按需分配资源	高 按需分配资源 新老设备可负载，充分利旧
运维难度	多品牌，维护难度大	PBR逻辑关系复杂，很难维护，规模越大越复杂	非常简单，图形化界面，基于业务逻辑关系维护
技术门槛	一般	高 需要对PBR细节原理非常了解、配置也复杂	简单 图形化界面，勾选可实现效果
可扩展性	非常低 动网必须断网	高	高
业务灵活性	差 所有业务只有一条流路径	高 PRB策略引流	高 SDN流标动态引流
适用网络国模	中小	小	中大

以下从物理、业务、运维角度，让网络出口更加自由

物理自由：

・旁挂部署，天然消除单点故障，旁挂安全设备出现问题，可利用SDN智能Bypass功能，保证业务不中断。

・安全设备无品牌限制，因为RG-ONC都是标准开放的接口，且引流策略主要下发给引流交换机，所以旁挂的安全设备可以选择多种品牌，充分保护用户投资。

业务自由：

・增加、删除、升级安全设备，永不断网。可在 RG-ONC 图形化界面先修改服务链，再一键触发引流策略更新；或者重新定义新的服务链，和需要牵引的流量进行匹配，业务均可无中断完成切换

・ 按需引流，根据实际业务需要，动态牵引流量到需要的安全资源上，充分利用设备和带宽资源。不会再出现不相关的流量大量占用设备和链路资源的现象。

・ 多链路冗余备份，在按需引流的基础上，可以给同一业务流分配多条流路径，可以按照主备、负载均衡等方式部署，满足业务级的可靠性备份。

运维自由：

・RG-ONC会提供精细化的图形化界面，对于维护人员技术门槛要求低，满足不同类型运维人员的个性化需求，大大减轻运维的压力，有效提升运维效率。

・抽象业务层面，用户只需要关注业务层面，不需要关注底层物理拓扑的连接方式、逻辑关系，真正站在业务的角度去定义业务流的处理方式，物理网络会根据SDN控制器的指令快速就位。

・整体运维层面，为客户打造FAAS（功能即服务）的新体验。

全网安全协防

如何实现全网的流量任意调度，牵引至对应的安全设备，进行必要的防护和清洗？

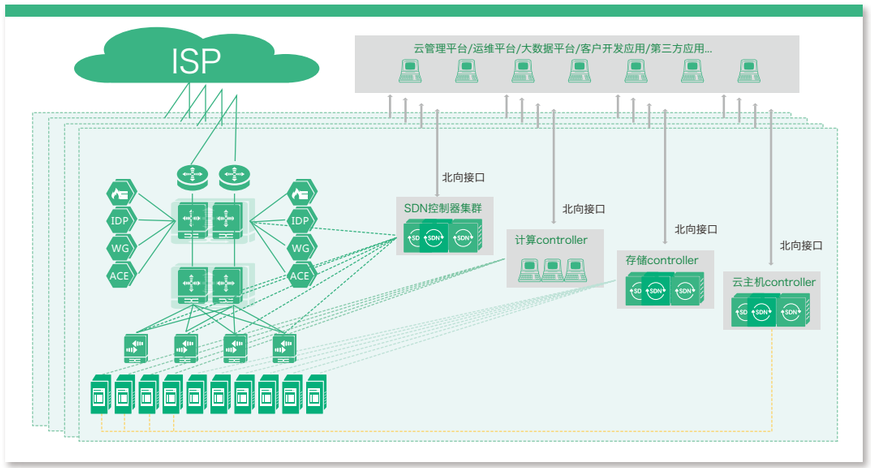
ServiceChain方案组件可以支持牵引全网任意位置的流量至安全资源池进行清洗，一次投入，无限利用，为用户打造无处不在的业务安全使用体验。

04 锐捷云数据中心方案

随着云计算、大数据、移动互联网的兴起，数据中心流量与日俱增，东西向流量约占到数据中心总流量的80%，数据大集中的同时，也带来灾难大集中。作为承载云业务的核心管道设施，数据中心基础网络面临着新的挑战与变革，如何才能够为业务应用提供更加灵活可靠的支撑，成为变革的关键。

在数据中心基础网络的变革过程中，SDN技术将扮演非常重要的角色，据市场研究机构IDC预测，到2020年，全球数据中心领域软件定义网络SDN市场（包括物理网络基础架构、虚拟化/控制软件、SDN应用（网络和安全服务）、以及专业服务等）的年复合增长率将高达53.9%，并将在2020年达到125亿美元，其中SDN软件市场规模至少达59亿美元。

锐捷云数据中心（DC-Cloud）方案，旨在以锐捷开放网络控制器RG-ONC为核心，融合云平台、基础网络设备、计算虚拟化平台等，实现数据中心基础网络和IT资源的统一管理、按需调度和弹性扩展。



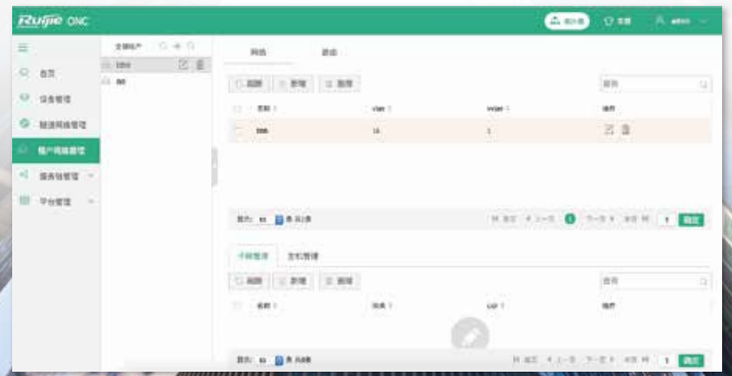
自动化部署

Underlay（承载网络）和Overlay（业务网络）不再需要通过传统的CLI命令行进行配置，仅需要在RG-ONC控制器界面上进行图形化填写、拖拽等操作，即可完成配置。

Overlay网络采用VXLAN技术建立隧道，亦不需要在设备上通过CLI命令行进行配置，通过在RG-ONC控制器界面上指定VXLAN相关设备的角色、属性，即可完成配置自动下发，VXLAN邻居关系自动学习。Overlay网络控制面全部由RG-ONC承担。相比BGP-EVPN作为Overlay网络的控制面来说，SDN方案对Underlay网络的要求更低，配置更加灵活，也更具扩展弹性。

租户网络按需创建

图形化界面完成全部操作



每个业务可以按照租户的概念分配网段、划分更细颗粒度的子网，每个业务对应一个虚拟路由器，虚拟路由器的创建会自动创建一条VRF实例。此处无论是通过RG-ONC创建的虚拟路由器，还是通过云平台创建的虚拟路由器，其最终的存在形式都是体现在VXLAN三层网关上的ARP信息。以该种方式创建业务之后，初始状态下，默认所有业务是不能互通的，因为VRF没有给予互通策略，可以大幅减少手工配置大量ACL策略的工作量。如果后续涉及到不同的业务之间需要互访，只需要打通相应的VRF路由策略即可，直接在VXLAN三层网关上将路由拖拽导入Underlay路由即可完成互通。

网络资源统一管理

SDN可实现Underlay、Overlay、租户网络的统一管理。SDN控制器会通过Openflow下发ARP代答的规则，所有VM上线的ARP探测请求全部上送RG-ONC统一代答，以此来完成主机的L2/L3层信息的同步和统一管理。

SDN精细化运维

对于所有试图应用在数据中心的网络运维技术和运维工具来说，主要关注几个层面

- 数据中心南北向、东西向流量纵横交错，且流量异常巨大，必然不可能手工处理，对于各种运维技术、工具，首先要看其大数据下的处理分析能力。
- 数据中心的流量不仅多，而且重要，任何一个区域出现问题，都有可能影响到其承载的业务。传统运维更多是后知后觉，业务出现问题，业务部门找上门了，网络才各种焦头烂额的加班、排错、寻故障源，但很多时候故障还没定位就消失了，一次次的排错，一次次的折磨。如果能够快速、准确的定位故障源，让运维部门比业务部门提前感知可能出现的故障，那网络运维将会简单很多。
- 工具的易用性(容易理解、简单操作和精细化智能呈现)如何？自动化到什么程度？是否智能的感知、分析和处理一些故障、告警等。

这里面比较关键的是对流量的采集、处理和分析的过程。传统的流量分析，故障定位，有几种方式

- SFLOW，IPFIX等流量采集技术，缺点是信息量大，精度低，实时性差，只能作为流量宏观监控，或者微观监控辅助。
- 包守恒探测技术，缺点是无法精确到链路级，轮询统计的实时性差，无法定位到受影响的会话，无法发现延迟。
- 持续探测，缺点是轮询统计的实时性差，无法定位到受影响的会话，无法发现延迟，无异于守株待兔。

以上方式即使数据都拿到，无法第一时间分析处理，下发策略，等于是浪费带宽。且面对数据中心流量极具增长的今天，均显得力不从心。利用 SDN 技术，做流量级可视化 能够在网络出现拥堵或者瞬时拥堵导致丢包或延迟时，第一时间将 (时刻，设备，链路，会话，丢包或延迟) 5 要素信息上送 SDN 控制器，协助客户快速准确定位故障，并下发执行预配置的策略，或提醒管理员进行调整。

以下列举几种精细化数据采集、分析、呈现和处理的方式

- 所有网元（此处主要指交换机）设备，可按照SDN控制器下发的指令采集设备的软硬件信息，包括但不限于设备的CPU、内存、温度、版本和物理端口等使用情况，并在RG-ONC界面统一呈现，智能排序，异常情况自动告警。同时，对于特定的流量进行逐跳的丢包、延迟、速率等信息统计，第一时间上送RG-ONC，呈现端到端网络流量路径，精准及时定位影响业务流转发的具体原因。
- 基于业务，直观查看各时刻带宽情况。根据流量的起伏下跌变化，判断可能出现的网络问题。同时，通过查看网络事件库，确认是否是某异常事件引起。
- 智能排序各租户（用户）连接数排行，若某租户（用户）超出正常范围，则可能出现中毒，或被攻击等问题。
- 同步查看各业务负载情况，确认故障时刻，如某个关键业务延时较大，肯可能是某业务占用过多带宽导致（如P2P下载，视频等）。可进一步通过策略限制非关键业务的带宽使用来进行排查。
- 进行历史数据横向对比，分析差异化原因，判断到底是业务问题还是网络故障。

以上只是用户关注的一些关键数据，锐捷开放网络控制器RG-ONC提供更多网络层面数据分析处理机制，帮助运维人员实现更轻松的运维。

安全资源池

对于传统的数据中心安全防护机制，主要有两种部署模型

- 在网络出口串行部署安全设备实现南北向流量的安全防护
- 在数据中心各个区域的边界串行部署安全设备，实现东西向流量的安全防护

无论哪种方式，基本都是硬件安全设备的堆积，即使可以做一些按需防护机制，也是采用重定向或者策略路由等方式干预业务流路径，实现不同种类流量的按需牵引。当业务种类数量较多时，策略会比较复杂，且不可视，很容易出错。特别是租户、虚拟化网络引入之后，这种问题更加明显。

利用锐捷开放网络控制器RG-ONC，可以在数据中心实现多品牌安全设备的资源池化，由RG-ONC统一灵活调度，达到安全资源的最大利用。同时，对于南北向流量、东西向流量、租户之间的流量均可通过SDN控制器统一牵引，实现按需防护。这样做不仅按需、弹性，也会让网络更稳定、运维更简单、业务调整速度更快。

双活数据中心

很多行业（比如金融和政府）的用户建立了自己的数据中心，为了确保数据中心出现故障时业务不间断，还会建立一个备用中心。正常情况下，主数据中心对外提供服务，备用数据中心处于闲置状态。只有在发生灾难宕机的情况下，业务系统才从主中心迁移到备中心来。然而，灾难往往只是小概率事件，企业投入大量人力和物力建设的备份中心大多时候都是处于闲置状态，资源使用率极低。无论采用怎样的优化方式，主备模式的建设思路对可用性的提高和业务连续性的保证只能实现量变，却一直没有实质性的跨越。

所以对当前主备数据中心的基本需求如下

- 灾备切换（网络级切换和服务器级切换）能够在最短时间完成，代价最小。
- 多中心网络互相影响的风险，比如一个数据中心的广播风暴影响另一个数据中心。
- 分支机构访问数据中心任何业务时需求保证来回路径一致，避免被安全设备误判，避免遭受拒绝服务攻击，影响业务转发。
- 双中心服务器资源利用率的问题，在业务繁忙期间能够充分利用备份中心的服务器资源。
- 双中心断裂的时候，业务不能中断。

锐捷网络于2015年推出“ARP同步+VRRP双活”解决方案，通过在两个中心核心设备上部署相同网关，核心设备既做二层互联同时也做网关，通过VRRP双主提供双活网关架构，在两个网关之间同步ARP信息，提供虚拟机迁移检测、RHI路径引导、故障域隔离、故障检测等功能，这里二层互联用VLAN实现。

锐捷网络于2016年对“ARP同步+VRRP双活的解决方案进行精进，通过在两个中心部署网关设备和DCI设备分开(即网关和中心二层互联设备分开)，网关设备功能无变化(同上面描述)，新增DCI设备支持VXLAN封装和解封装。通过开启EVPN VXLAN功能打通两个数据中心之间的二层。两个数据中心分别都处于运行状态，可同时承担相同业务，提高数据中心的整体服务能力和系统资源利用率，并且互为备份。当单数据中心故障时，业务自动切换到另一存活的数据中心，存活数据中心自动接管业务，业务连续运行，数据零丢失，保护信息资产，解决了传统灾备中心不能承载业务和业务无法自动切换的问题。

同年，锐捷网络提出SDN场景下的双活解决方案，利用AnycastGateway技术实现双活网关的同时，减少DC之间的广播域范围。中心间广播域互相隔离，包括STP域、未知名单播、组播、广播。将广播域限制在本中心内，避免广播间互相影响，防止广播域在中心间链路泛洪。同时解决传统灾备中心不能承载业务和业务无法自动切换的问题。

05 VXLAN 技术篇

VXLAN背景及起源

要揭示VXLAN的起源就不得不从虚拟化技术本身说起。目前在数据中心内部应用最广泛的主机虚拟化技术实现了软件、硬件的分离。单个应用程序无需绑定在硬件主机上，能够在不同服务器之间自由漂移。但这种做法仅仅是简单打破了服务器软件和硬件的紧耦合，一个完整的应用系统包括网络、存储、安全等，单纯的主机虚拟化必然会同其它没有发生变化的传统领域发生冲突。因此，近年来虚拟化热潮带动了数据中心内部方方面面的变革，使得这些原来没有变化的领域开始主动发生变化，以更好地为虚拟化主机提供服务，数据中心网络的大二层技术就是这些变化中的一种。

应用软件被移植到虚拟化平台后，要求虚拟机的三层地址在漂移前后不发生改变，这样同其它应用程序的互访就无需变更，对外提供服务的网关也保持一致。当虚拟机部署越来越多，越来越广的时候，二层网段就变得越来越大，这就是大二层网络的由来。这种需求催生出OTV、TRILL、大地址表等网络技术，促进基础网络不断变化以适应不断增长的虚拟机数量。

VXLAN解决的问题

1.二层网络边界限制

二层网络边界限制一直以来都是虚拟化部署中不可触碰的红线，虚拟机无法在不同网段之间迁移，导致数据中心内部的大二层越大越好。大二层的扩张不但带来老生常谈的STP协议问题，而且对接入交换机的MAC地址表施加了很大的压力。接入交换机需要学习每一个虚拟机的MAC地址，一旦MAC地址表学习满，交换机便不再主动学习MAC地址，这时一个目的MAC地址未知的数据帧就会引发全网的广播。

二层网络边界的限制还体现在对业务的影响上。本来主机虚拟化实现了服务器软硬件的分离，但在设计虚拟机的迁移策略时却要时时考虑到网络边界的限制。

2.VLAN数量不足

在数据中心网络中，虚拟机是通过VLAN来划分流量的，不同的虚拟机被划分到不同的VLAN中。实际上可分配的VLAN数量为4094，这个数字在某些大规模数据中心内是不够用的，严重限制了数据中心的规模扩展需求。

3.多租户问题

数据中心通过主机虚拟化为不同的用户提供不同的服务，而这些用户使用的有可能是相同的VLAN ID和IP地址段。为了隔离这些用户的流量，必须添加额外的三层网关以及地址翻译等策略，这些都会增加额外的运维成本。

对于网络管理员来说，更倾向于使用IP来互联物理网络（比如可以通过ECMP等价多路径来实现多路访问）。在这样的需求背景下，要跨过VLAN的缺陷，就要对现有的二层标签技术进行彻底的改革。在保留二层转发模型的基础上提出Overlay网络。

VXLAN技术简介

基于IP网络构建Fabric网络。无特殊拓扑限制，IP可达即可；承载网络（Underlay）和业务网络（Overlay）分离；对现有网络改动较小，保护用户现有投资。

1.VXLAN技术关键点

- 它是建立在物理IP网络之上的虚拟网络，使用UDP封装完整的内层以太网报文，即所谓的MAC-in-UDP，共50字节的封装报文头
- 总共有24位的VXLAN网络标识符（VNI），相比最多4094个可用VLAN的上限，VNI可以扩充到16M个
- 利用IP组播封装广播、租户、未知名单播报文，从而限制虚拟网络中的广播域
- 可以对不同的数据流使用不同的UDP源端口，实现ECMP（等代价多路径）实现负载均衡

2.VXLAN从三个方面解决虚拟化环境下存在的问题

- 解决虚机迁移范围受到网络架构限制的问题

  Overlay把二层报文封装在IP报文之上，因此，只要物理网络IP路由可达就可以部署Overlay网络，而IP路由网络本身已经非常成熟，且在网络结构上没有特殊要求。而且IP网络本身具备良好的扩展能力，很强的故障自愈能力和负载均衡能力。采用Overlay技术后，企业不用改变现有网络架构即可支撑新的云计算业务，极大方便用户部署。
- 解决虚机规模受网络架构限制的问题

  部署Overlay网络之后，虚拟机数据进行VXLAN封装，对网络只表现为封装后的网络参数，即隧道端点的地址。因此，对于承载网络（特别是接入交换机），MAC地址规格需求极大降低，最低规格也就是几十个（每个端口一台物理服务器的隧道端点MAC）。当然，对于核心/网关处的设备表项(MAC/ARP)要求依然极高，当前的解决方案仍然是采用分散方式，通过多个核心/网关设备来分散表项的处理压力。
- 解决租户（业务）隔离数量限制的问题

  针对VLAN只能支持4094个可用ID的限制，在Overlay技术中扩展了隔离标识的位数，可以支持高达16M的用户，极大扩展了租户的数量规模。

06

锐捷网络SDN开放合作构建生态圈

锐捷网络始终秉承以客户为中心的理念，积极构建SDN上下游生态系统，为客户提供一体化的解决方案。锐捷网络SDN已与全球多家知名IT厂商及标准组织展开合作，构建了完整的SDN生态链，打造全方位的开放云网络生态系统。

锐捷开放网络控制器RG-ONC以开放的ODL平台为基础，采用组件松耦合架构，可开放对接各种商用Openstack平台，目前除了锐捷自身的JCOS平台之外，锐捷已经和Esaystack、海云捷迅、IBM、中科曙光、浪潮等完成对接，并在积极促成合作。同时，RG-ONC开放网络控制器对外提供丰富的北向API能力，帮助用户和合作伙伴开发集成、快速创新。

07
锐捷SDN各行业故事会

锐捷SDN在过去6年的摸爬滚打中，积累了丰富的可商用部署经验，同时也帮助很多客户与合作伙伴取得成功，在这里选择在锐捷SDN成长过程中的部分客户进行分享，也是由衷的感谢。

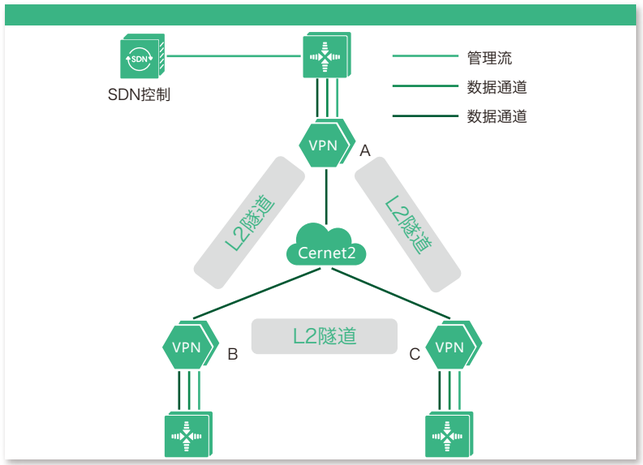
（此处分享排名不分先后）

中科院高能物理研究所 SDN之广域网负载均衡

中国科学院高能物理研究所是我国高能物理研究、先进加速器技术的研究开发、先进射线技术及射线应用的综合性研究基地。

1.客户需求

由于客户之前是通过二层隧道方式与各个高校进行报文交互，因此按照传统二层网络协议，面临广域网链路利用率低，无法进行动态负载均衡的问题。这就好比在北京堵车严重的情况下，即走直线距离还不如绕其他不堵的路线抵达目的地。如下图，当A点与C点之间的流量超过二者之间的互联带宽时，将会出现网络拥塞，同时A点到B点以及B点到C点之间的链路可能是空闲的。这时A点、C点两站点采用传统的网络设备，则根本无法实时将A点、C点之间拥塞的流量切换到经由B点的链路上，导致整体上的带宽利用率不高。因此，客户想用SDN技术方案对网络进行优化。



2.解决方案

同样当A点和C点之间进行通信时，由SDN控制器根据当前各条链路的负载状况，实时对新建业务流选择更适合的网络链路进行通信。如上所述的当A点和C点的流量超过二者之间的带宽时，将有部分流量会迁移到B点绕行（假设B点此时空闲）。这样任意站点之间的通信将会利用到所有可能可达的路径，有效提升整网带宽利用率。

3.客户价值

- 全网调度（而非传统的出口双链路调度），任意两点之间有多条链路，整网路径可视化调度（而非逐条的计算）
- 充分利用了整个广域网的带宽资源，降低了广域网的带宽成本
- 区分业务进行优先级带宽保障，有效提升业务体验

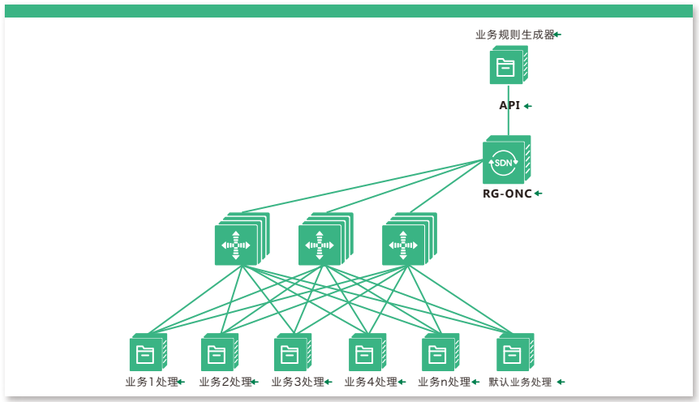
某国家网络中心
SDN之PIF与协议无关转发

1.客户需求

目前，国家某网络中心国际互联网出口涉及对至少几百G级别的流量进行清洗，面临极大流量清洗压力。但由于服务器的采购时间不同，导致性能参差不齐，有高有低，且任何Server都具备处理所有业务流量的能力。这样的情况下就会面临由于网络协议固化带来的路径固化问题，导致某一个/组服务器性能过载产生处理瓶颈。

另外，国家某网络中心国际互联网出口收到的报文种类多种多样，因此需要按照不同规则分类不同业务，并且按照优先级去让性能不一的服务器按照客户制定的规则进行处理。

因此，国家某网络中心目前采用的是服务器方式进行业务分类，互联，软件自定义一套协议，全网通过服务器网卡转发，识别，处理。但服务器性能有限，无法在识别业务的情况下达到像专业网络设备一样几十G甚至上百G的转发能力，因此，服务器实现方式不仅转发延时大、不稳定、而且整体扩容成本及管理复杂性都非常大。



2.解决方案

锐捷网络通过了解客户的业务类型及客户的需求后深度分析客户的相关问题，通过软件定义网络方式来解决。客户通过其业务分类器与SDN控制器的北向API进行对接，通过业务分类器中定义的分类和规则，利用SDN控制器将自定义的协议告知所有流交换设备，所有设备按照要求进行转发。最终，全网可以通过交换机上传的采样数据来告知控制器接口目前的状态和链路状态，TCP链接状态等进而判定服务器是否超载，并且控制器通过交换机，了解到全网状态及服务器状态后，动态的调整交换设备流表进而将不同的流量引向能够处理的设备进而提升全网服务器资源利用率。

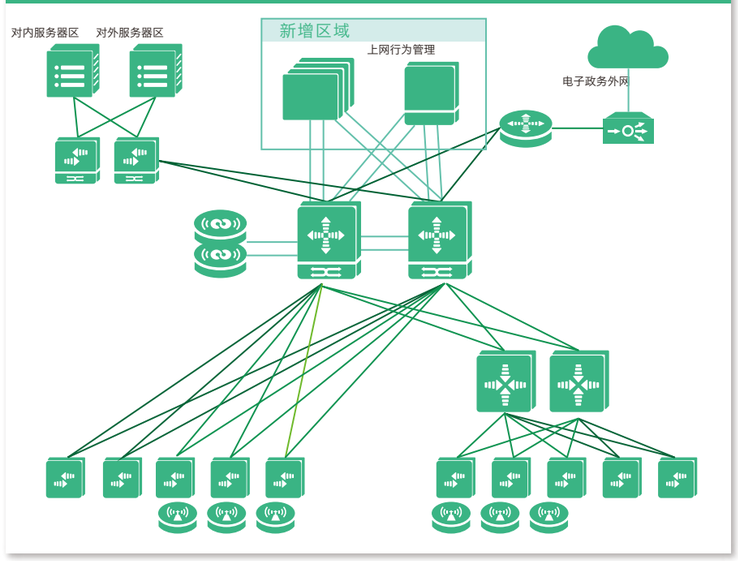
3.客户价值

业务定义了网络，摆脱传统网络协议束缚，使网络为应用提供了灵活可变的通路利用交换机高性能的转发能力来进行负载均衡，提升转发效率。

山西省政务大厅
SDN之安全资源池化

山西政务大厅总建筑面积 60600 平米，其中地上 15 层，53000 平米，地下 1 层约 7000 平米。“两平台”办公大楼依托省电子政务外网，整合 52 个部门、单位，3090 项行政职权 。

出口区网络部署拓扑



1.客户需求

- 业务需求：快速的业务上线，无需改动网络，仅仅需要很简单的配置变更即可；
- 安全需求：多个部门委办接入，不同的委办局的安全级别也不相同，可以灵活实现安全策略；
- 运维需求：在进行网络割接，排错时，不能中断网络；

2.解决方案

核心采用 2 台 Newton 18000 做 VSU；SDN 控制器接入管理网，与 Newton 18000 管理互通；深信服上网行为管理设备和迪普安全设备均旁挂到 Newton 18000 上，所有进出数据通过核心交换机时，都会根据 L2-L4 因素对其进行分流，使对应的数据走对应的安全设备。

3.客户价值

- 提高安全设备的使用率，提高出口的可靠性；
- 物理网络快速响应业务的调整；
- SDN控制器图形化界面操作，割接安全资源池，不断网。

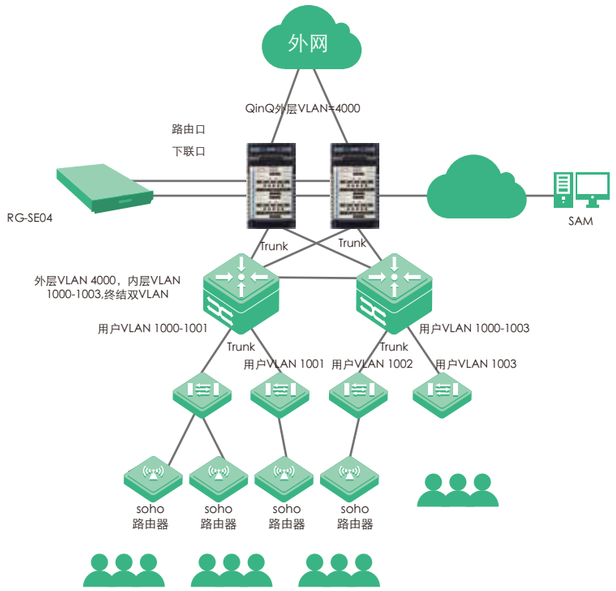
武汉大学
业界首个SDN NFV之vBras组网

2014年8月，我公司发布了业界首款可商用化SDN NFV产品－PPPoE扩展机箱以及vPPPoE解决方案。该方案可兼容不同时期，不同厂商的核心交换设备，而且采用旁挂核心交换，与设备松耦合不会因设备性能、故障导致断网，因此广受高教领域客户关注。

武汉大学于2015年有扁平化改造的需求，而且也想通过锐捷极简网络来解决其统一认证等问题。因此客户核心采用Newton 18000做扁平化认证交换机，用于办公区无线网络的统一认证和管理。

1.客户需求

由于学生宿舍区的终端不一，对于802.1x认证客户端兼容性不算太好、维护量巨大，因此客户选择锐捷vPPPoE解决方案。锐捷的vPPPoE方案给用户提供了很好的认证体验，而且还提供了完善的web界面供用户配置并且还提供了北向Rest API方便客户单向对接运营系统，真正可视化认证，优化运维。而且在安全、稳定、可控层面又通过QinQ技术实现了每个用户一个VLAN，很好的实现了“二层进行彻底隔离，三层可控高速互访”。



2.解决方案

武汉大学采用锐捷 vPPPoE 方案以后，整网广播域控制在接入交换机单端口的单一用户下，不存在广播风险。原来宿舍区每一个用户一个 VLAN，即接入交换机每个端口规划了独立 VLAN；汇聚与核心之间的原路由转发模型改为 TRUNK 透传所有接入交换机的用户 VLAN 通信，其他都裁减掉，达到 PPPoE Server 和 PPPoE Client 之间的通路都是纯二层转发。而且校园内其他区域如办公网，家属区以及有线无线网络的扁平化部署完全不影响，只需要 Newton 18000 预留一个 VLAN，PPPoE 都可随时部署。

3.客户价值

锐捷 vBras 方案为武汉大学建设了易维护、易管理、高效率、高体验的 vBras 网络平台，大大减轻了网络中心管理人员的维护工作量，并且极大的提升了用户的使用体验，让校园网真正成为全校师生想用、爱用的网络，也让网络中心成为学院服务师生的典范。

四川大学
SDN NFV之vBras组网

四川大学（Sichuan University），简称“川大”，由中华人民共和国教育部直属，中央直管副部级建制，位列“211 工程”、“985 工程”，入选“2011 计划”、“珠峰计划”、“111 计划”、“卓越工程师教育培养计划”、“海外高层次人才引进计划”，设有研究生院，拥有研究生自主划线资格，是一所综合性全国重点大学。

1.客户需求

随着近几年有线无线网络的大力建设，设备数量多，用户规模大，网络的运维管理对网络中心提出了较大挑战，需要打造有线无线统一认证统一管理的融合平台至关重要。

2.解决方案

通过对四川大学校园网的整体规划，采用锐捷的扁平化极简方案，有线认证采取锐捷 SDN NFV 的 vBras 解决方案。使得有线网络和无线网络的认证和管理策略均上收到 Newton 18000 扁平化认证交换机，实现了有线无线的统一认证和管理。

3.客户价值

- 简单拨号，即可上网。
- 界面化的管控方式，降低运维复杂度，使得网络管控清晰简单。
- 每用户之间的VLAN隔离，提升了网络的安全性。

湖北中医药大学
SDN NFV之vBras组网

随着学校的不断发展，各业务处室和部门的信息化应用水平不断提高，师生员工对信息化建设提出了更高的期望与要求，而现有校园网及应用系统已无法满足这些需求，新的数字化校园建设的重点内容之一即是建立搭建学校统一的基础网络平台，建设高质量的数据中心。为此目标，2015 年锐捷网络携手湖北中医药大学，共建智慧校园的方式对网络进行了全新规划与改造。

1.客户需求

认证是高校最核心的业务，因此客户对于认证要求较高。核心故障，不能影响认证。即便是核心交换软件的认证模块故障，也不能影响认证。因此将软件认证计费模块单独提取出来，采用新的方式去认证成为其关注的重点。

2.解决方案

锐捷 SDN vPPPoE 方案天然满足客户的需求。核心单独旁挂一台 vPPPoE 服务器，使得网络认证和核心分离。不会担心核心设备认证性能、核心认证模块故障而影响认证。

3客户价值

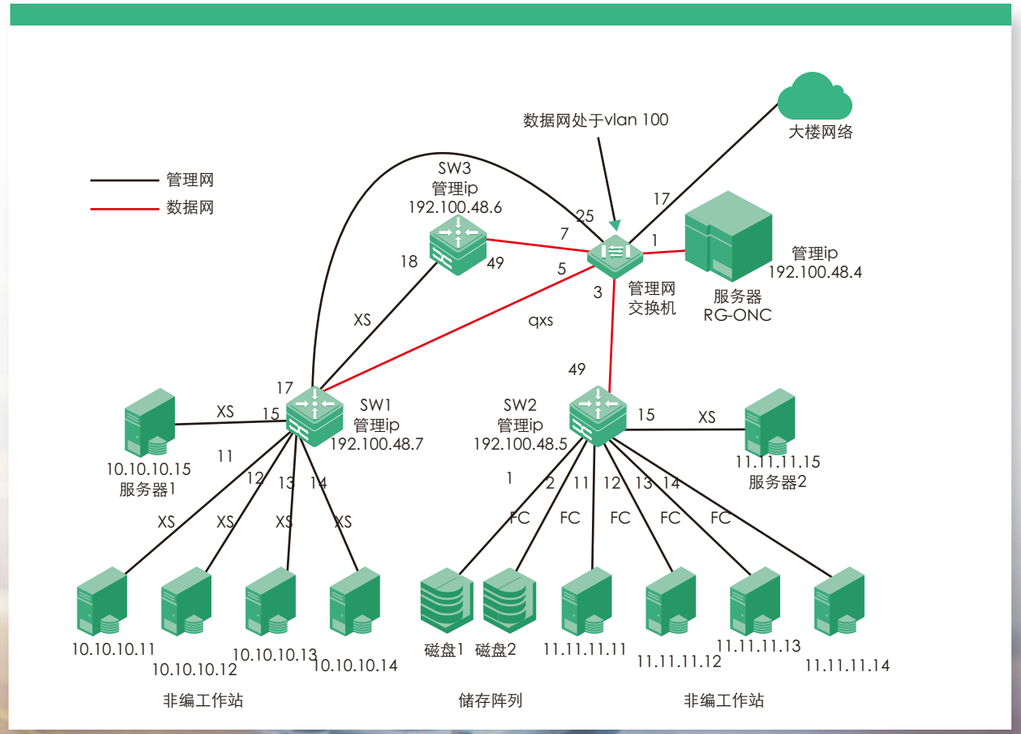
利用 SDN vPPPoE 方案降低了核心设备认证模块故障风险，提升了湖北中医药大学的管理和运营效率，同时有效提升了全校师生校园网接入及认证的稳定体验，为智慧校园的建设提供了统一、开放、稳定可靠的基础认证平台。

福建省广播影视集团
SDN之PTDN集中数据中心控制

目前，福建广电整个系统网络为一张制作网，制作网功能单一，只有节目制作和演播室录制两大业务（注 不承载内网通信，内网通信在办公网，办公网是与制作网完全物理隔离的，所有的办公电脑都在办公网）。制作网和办公网间有少量的文稿和视频文件的交互。文稿是通过 WEB 服务访问，视频文件用 FTP，办公网和制作网间的所有交互都会过网闸或是摆渡设备，制作网和办公网间只有一条 1G 的线路。

1.客户需求

将目前的光纤＋以太网双网架构，改造为以太网单网架构，目的是为了简化网络布线、减少投入成本、简易维护管理、便于业务扩展；对于管理层面，需要基于业务的网络性能监控；能够基于业务的网络流量精细化呈现；能够实现网络资源分片功能，将不同业务分布在不同网络切片上，实现 QoS 保障。而且具备网络资源预留功能，可为关键业务预留网络资源，保障关键业务的网络资源需求。



2.解决方案

锐捷网络采用 SDN 控制器进行集中控制，进而实现基于业务的流量精细化呈现：实时的流量图，展示某一分片的当前流量态势图（1 天、1 周、1 月，可自定义展示周期），流量采样的时间间隔足够小（eg.<5s，即具有一定的实时性）。锐捷 SDN 集中控制可基于业务对应用进行性能监控，支持业务聚合监控，可查看某一业务的所有分片聚合后的流量情况（如查看整个存储区域流量情况、线编业务流量情况）。此模型实现了网络资源分片功能，将不同业务分布在不同网络切片上，实现 QoS 保障。SDN 集中控制实现了网络资源预留功能，可以为关键业务预留网络资源，保障关键业务的网络资源需求。在支持资源预留的基础上，支持限速功能，资源预留后当资源使用将达到上限时可告警。

采用锐捷 SDN 架构对网络改造后，顺应了未来数据中心统一、融合、绿色节能的架构趋势，提升了集团制作网系统业务扩展能力，更好的适应了集团未来业务发展。

3.客户价值

- 更少的硬件和更简易的管理：采用SDN方案后，交换机数量减少约50%，网卡和布线减少约50%，网络管理和维护复杂度降低约30%，网络基础设施成本降低约33%。
- 更高的灵活性、可靠性和可扩展性：摆脱两套网络系统协同控制困境，只需在融合的单一架构下规划和布局，网络系统扩容更简单、快捷，新业务上点时间缩短40%。
- 更低的能耗：网卡、交换机及布线的大幅减少，意味着更低的电能消耗、更少的空间占用及制冷设备。部件总数减少近一半规模能够带来可观的能耗降低，网络设备类基础设施能耗降低30%。

中烟工业山东卷烟厂
SDN构建网络安全资源池

济南卷烟厂是山东中烟工业公司最大直属厂，创办于1928年，其“泰山”品牌香烟为全国卷烟重点品牌，该厂也是全国四家定点雪茄烟生产企业之一。2012年，山东中烟生产规模全国第五。

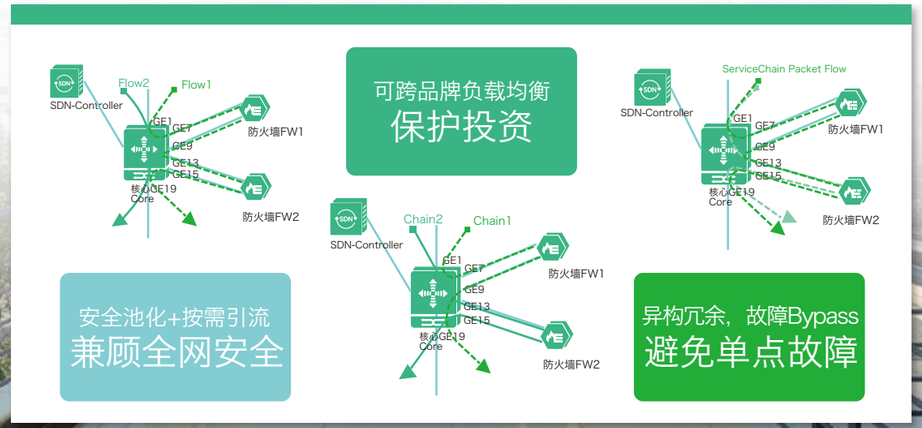
1.客户需求

客户原为全网思科设备, 其中骨干核心设备已运行近 10 年, 设备老化, 需要替换升级。同时, 随着业务的发展、IT 环境变化, 原网络也遇到一些难以解决的问题，如:

- 内网安全防护不均衡，频现安全隐患。原网虽有7台安全设备，但功能各异且分散在多个出口/分区，单个分区防护依然薄弱、设备利用率低。用户近一年已两次检测到内网终端中毒，并对外攻击，存在安全隐患。
- 用户近期有大规模办公室搬迁的计划，对应网络配置变更、维护很麻烦；同时，移动办公逐渐普及，而移动端的IP地址不固定，导致网络权限难管理、难识别，安全性较弱。
- 信息中心有自行开发的简易认证系统(IP/MAC绑定)，希望即使更换网络设备品牌，也能很方便的兼容新网络设备、甚至二次开发个性化功能。

2.解决方案

采用锐捷 Newton 18000 核心交换机，配合 SDN 控制器可实现 Service Chain 安全服务链功能。用户可将原分散的安全设备统一旁挂至核心交换机上，由 SDN 控制器来设定不同的 IP 或业务流量需要发送至哪些安全设备处理，实现全网安全资源共享、按需防护, 并且还能实现跨品牌安全设备冗余、负载均衡、故障 bypass 等功能。此外, 此方案通过软件升级, 还能平滑演进为 SDN 云园区架构，实现全网 IP 即用户、安全策略随行等特性



3.客户价值

- 安全资源池化：全网业务按需防护，提升设备利用率，并简化部署管理
- 避免单点故障：支持安全服务链故障自动Bypass、安全设备割接/维护不断网
- 兼容任意品牌安全设备，保护用户投资：可实现跨品牌设备负载均衡、主备冗余
- 可平滑升级至SDN云园区网络，进一步提升移动办公、多业务安全体验
- 开放SDN网络平台，支持第三方程序对接，可灵活适应未来新业务需求、变化

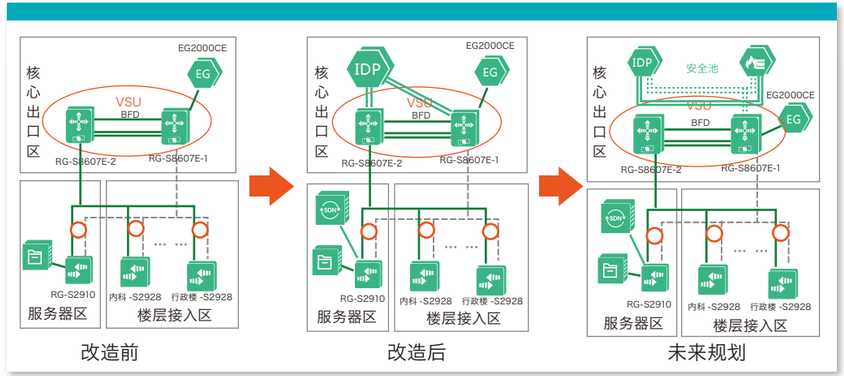
昆山二院
SDN之安全资源池

昆山第二人民医院历史悠久，始建于 1958 年，是一所以中西医结合为主的综合性二级甲等医院。承担了玉山镇及周边地区几十万人口的医疗、预防、保健任务，并拥有正仪、巴城两家分院，是昆北地区的医疗集团中心，在社会上享有良好的声誉。

1.客户需求

二院十分重视信息网络安全，为了使网络安全达到更高层次，并顺利通过等级保护评测，医院决定对网络进行安全整改。客户面临着如下问题：

- 一次性不知道买多少安全设备，希望分批购买，通过测试选择最合适的设备
- 希望实现定制化服务，只对网络边界流量进行防护
- 部署灵活，割接测试尽可能减少对医院业务的开展



2.解决方案

SDN ServiceChain方案实现上线安全设备不断网，可按需引流。医院部署该方案，可分期采购安全设备，即使频繁测试选型，也不会影响医院正常业务开展。前期将医保前置机、银医通HIS前置机等到卫生专网的流量引入到IDP进行入侵检测和防御，提高了安全设备利用率，保护客户投资。

3.客户价值

- 安全设备部署灵活，割接不断网，降低运维压力
- 降低等保投入，轻松实现分批选型安全设备

华山医院
SDN之内外网融合安全资源池

复旦大学附属华山医院创建于1907年，是国家卫生计生委委属医院、复旦大学附属教学医院和中国红十字会冠名的医院，1992年首批通过国家三级甲等医院评审，连续多年位列百强医院前十。为全国文明单位，是国内最著名、最具国际化特征的医教研中心之一，也是全国首家通过JCI认证的部属公立医院，在国内外享有很高声誉。2014年门急诊量逾384万人次（全国及世界各地患者占一半以上），出院病人6万余人次，手术4万余台。

1.客户需求

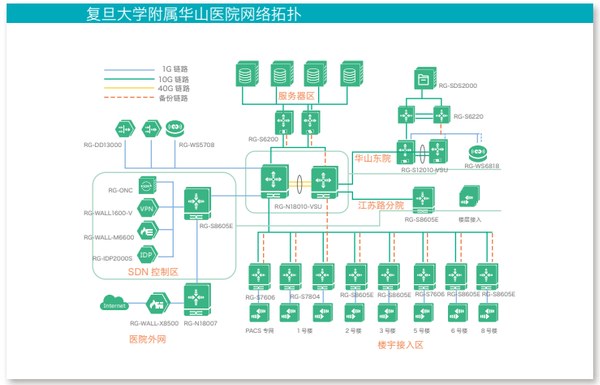
作为国际化医院，华山医院开展越来越多的互联网 + 业务，需要对外开放一些数据，内网和外网逐步打通，意味着将承受来自外部的攻击与破坏。医院信息系统从以财务为主线的模式转变成以医疗信息为主线，信息覆盖面广，数据量大，信息种类繁多，这些数据一旦泄露或破坏，就会给医院造成不可估量的损失。所以继续按照等保的要求，部署互联网 + 区域的安全，包括内网和外网互联区域，外网出口区域等。根据三级等保的要求，网络边界处的安全需要做到以下几点：

- 部署访问控制设备，控制粒度为端口级与用户级，并实现对进出网络信息内容过滤；
- 非法联入与联出检查，并能定位与阻断；
- 检测常见攻击，并对其记录与报警；
- 攻击、木马病毒防范，并保持恶意代码库的升级和检测系统的更新。

2.解决方案

针对内外网融合互通的趋势，在内外网之间建立一个安全加固区，部署 SDN 安全资源池，将多种不同类型的安全设备（防火墙、入侵检测、流控、审计等）资源池化，通过 SDN 技术对网络流量进行可视化控制，按需分配给各种内外网互通业务保障安全。原外网的安全保护可复用安全资源池，实现设备共用，不用新增购买，实现安全投入有效保护，降低投资。

复旦大学附属华山医院网络拓扑



3.客户价值

采用ServiceChain方式在网络边界处部署安全加固区具有以下价值点：

- 按需引流，把特定的流量引到特定的安全设备，发挥出安全设备的最高性能，提高设备利用率。
- 解决单点故障，安全设备故障可以自动旁路，保障医院业务正常开展。
- 安全设备上下线不断网，部署简单。可实现现网部署、测试安全设备，解决医院对上线安全设备望而生畏之痛
- 安全设备资源池化，内外网融合安全设备实现复用，保护投资，避免增加网络复杂性，同时兼容不同厂商安全设备，自由选择。

中国邮储银行
云计算数据中心SDN网络构建

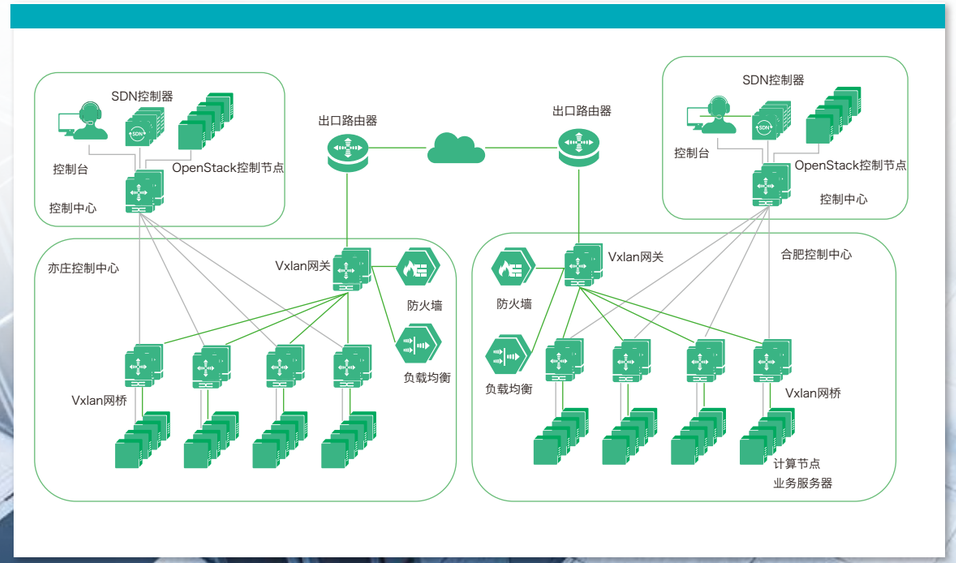
2015 年中国邮储银行，在丰台、亦庄、合肥准备采用云的架构构建两地三中心。客户渴望在这个两地三中心的环境下，计算资源可以不受网络边界的限制，可以与物理位置解耦（服务器随便插，自动归入所需网络环境），可以自动在云平台上对计算、网络、存储资源进行配置、管控来简化运维等等。

1.客户需求

2015年中国邮储银行，在丰台、亦庄、合肥准备采用云的架构构建两地三中心，渴望在这个两地三中心的环境下，计算资源可以不受网络边界的限制，可以与物理位置解耦（服务器随便插，自动归入所需网络环境），可以自动在云平台上对计算、网络、存储资源进行配置、管控来简化运维等等。

- 项目建设目标：
- 提升物理资源利用率
- 统一管理，降低运维的复杂度，提高运维工作效率
- 建立基础应用环境、方便测试
- 构建灵活的开发、测试集成环境

2.解决方案



如上图所示，锐捷网络通过5台SDN控制器做集群，三台放入亦庄数据中心，另外两台放入合肥数据中心互相做集群。如果一旦一个数据中心失灵，另外一个数据中心的SDN控制器即可接管控制。接入、核心均采用Newton 18000，服务器位置可以不受物理位置限制，通过打隧道做VxLAN的方式来解决物理位置和逻辑位置不符的问题。另外，通过EasyStack云平台与SDN控制器对接的方式，来达到业务上线、自动隧道映射、自动业务隔离的目的。最终经过2016年全年的三次大型测试（云核心性能测试、云核心功能测试、EasyStack平台对接测试），最终助力邮储银行完成邮储云数据中心的构建。

3.客户价值

- 物理网络与逻辑网络分离，灵活、可控。
- 服务器位置不受原有网络固化限制，服务器接入后自动归入所需网络。
- 业务上线，自动隔离，保证上线业务不会影响原有业务。

歌华有线
全媒体聚合云服务平台安全资源池

2013年，歌华有线制订了《歌华有线全媒体聚合云服务平台总体规划》（以下简称《总体规划》），2014年完成了歌华全媒体聚合云服务平台（以下简称云平台）一期建设，通过对“云计算”、“新媒体”技术的融合、吸收，面向全媒体、面向移动化应用建成了“跨终端、跨平台”的视频能力体系，展现了云平台作为开放服务能力平台的业务潜力，为公司进一步发展奠定了良好的技术基础。

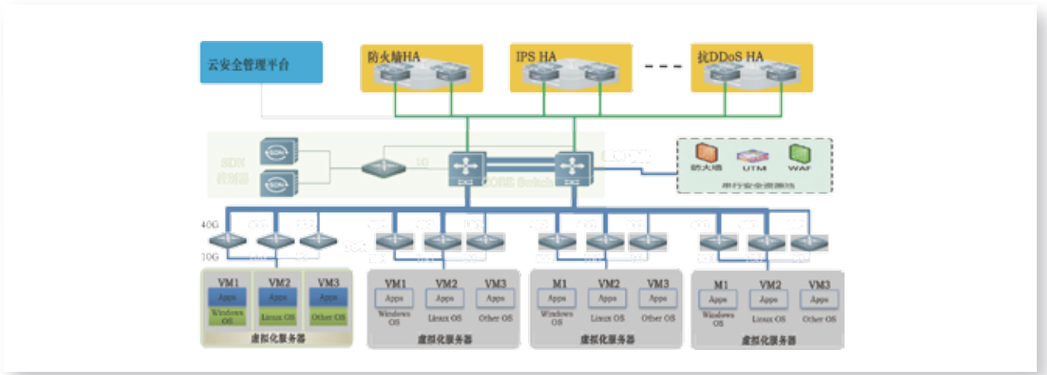
1.客户需求

根据歌华有线云服务战略，公司定投项目云服务平台升级及应用拓展项目规划，弥补一期项目建设中欠缺的能力和存在的不足。信息安全是云平台建设中的重要组成部分，而云平台的信息安全与传统系统安全体系建设又有着很大的区别，经过我们对全媒体聚合云服务平台一期项目的了解和分析，认为在信息安全方面主要存在以下几方面的不足和欠缺：

- 云内不同安全级别系统之间无法做到按需安全防护
- 云内业务系统安全态势不可见，云内安全管控效率低
- 云安全运维体系不够完善

2.解决方案

在云平台内部署的业务系统（安全域）对安全的需求与传统部署业务系统是一致的，主要包括主机安全、网络安全、出口安全、数据安全、应用安全等，通常采用的设备包括防火墙、UTM、IDS、WAF、日志审计、数据库审计、病毒扫描等。有的设备是采用旁路方式接入（例如IDS、日志审计、数据库审计等），有的设备是串行接入（例如防火墙、UTM、WAF等）。但是在云环境中，传统安全设备无法接入而提供应有的服务，需要构建面向云计算特性的安全资源池。



如上图，虚拟机上联虚拟交换机，虚拟交换机通过打VLAN的方式来给不同业务提供不同标识，并且在接入交换机相关端口通过Trunk到核心。通过核心交换机Newton 18000进行引流，并且通过周边安全设备旁挂的方式动态的定义针对不同业务的不同服务链，来解决云计算环境下的不同业务安全无法灵活、动态调整的问题。并且，此项目通过SDN控制器与启明星辰安全厂商进行安全云平台对接，包括服务节点定义、策略下发、服务链定义的方式，让用户只需要关注安全云平台与云环境下的业务关系，达到按需安全资源供给、灵活安全设备策略下发的目的。

另外，通过此方案，客户在安全设备升级、扩容都可以达到在线割接不断网。因为SDN控制器会告诉核心交换机对周边安全设备进行流量检测，一旦发现安全设备下线或异常，即可自动进行Bypass。

3.客户价值

- 统一配置管理，通过统一安全云平台界面统一管理、配置并能将网络、策略统一部署，简化配置管理。
- 灵活资源调度，按业务进行安全防护。
- 安全资源升级扩容，简单高效。

郑州教育城域网
SDN之安全设备引流

近年来，郑州市教育局“以教育信息化带动教育现代化”为指导思想，大力支持教育城域网建设，确保全市覆盖、高速互联、校校通达。在教育教学管理、应用、研究等方面取得了显著的成果。但是随着城域网规模的扩大、业务的快速增长，现有的网络急需进行升级改造来满足新的变化。

1.客户需求

- 当前核心交换机稳定性不够，替换的核心交换机作为全网互联关键设备需要考虑稳定和扩展性。
- 安全设备众多，包括防火墙、IPS、流控等不同的安全设备统一进行管控。
- 下联中小学需要增强安全访问控制增加防火墙重新划分安全域。

2.解决方案

2台Newton 18000替换原有友商核心。作为城域网核心，同时也作为SDN交换机使用。1套SDN控制器管理网部署。

ServiceChain作为整网安全引流设备并完全兼容第三方品牌，包括山石防火墙、DP多业务防火墙。

3.客户价值

- 2台Newton 18000组成虚拟化云平台实现50ms快速切换，解决了核心的稳定性问题。
- SDN融合性好，把所有不同品牌安全设备统一进行管控。
- Newton 18000既是一台核心交换机同时也是SDN交换机，一台多用云平台设备性价比超高。
- 健壮，稳定可靠，ServiceChain负载均衡主备冗余，控制器失联业务不中断节点自动Bypass。
- 弹性，利用SDN改变架构网络弹性伸缩可以灵活扩展。
- 具有良好的扩展性全网最高支持9万终端并发。

Ruijie Networks 锐捷

中 国 数 据 通 信 解 决 方 案 领 导 品 牌

锐捷网络股份有限公司

欲了解更多信息，欢迎登陆www.ruijie.com.cn，咨询电话：400-620-8818。

*本资料产品图片及技术数据仅供参考，如有更新恕不另行通知，具体内容解释权归锐捷网络所有。