

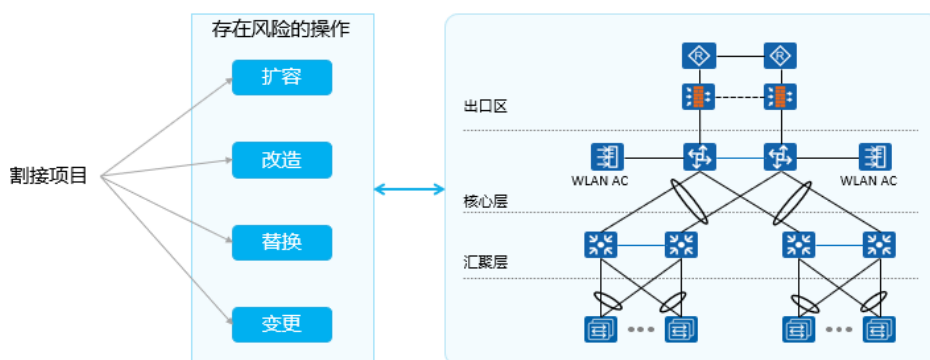
网络割接

- 随着企业业务的不断发展，企业网络为了适应业务的需求不断的改造和优化，例如：IPv4 网络升级为 IPv6 网络、IS-IS Level 修改、VPN 架构整改。无论是硬件的扩容、软件的升级、配置的变更，凡是影响现网运行业务的操作（如造成业务的中断），企业都会根据业务的安全等级要求，制定严格的操作流程和风险规避措施，并将其定义为割接项目。
- 本课程介绍了割接的流程和操作规范、风险把控措施，学习如何高效、顺利地完成网络割接。



基本概念

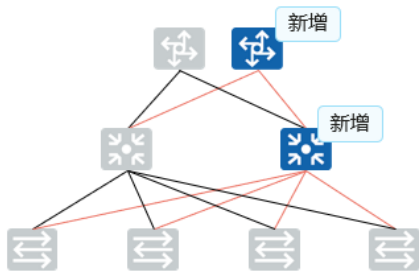
割接项目：如果对网络执行的技术迁移动作会影响现网运行业务，则在技术迁移项目实施时需严格地遵循预先设定的操作流程和风险控制措施，一般将此类项目定义为割接项目。





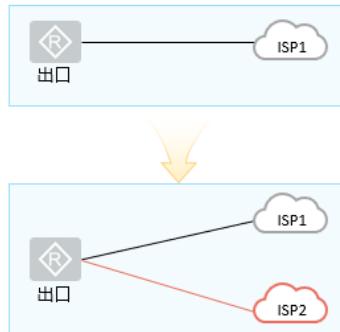
割接常见场景 (1)

网络扩容



随着业务流量的增加，对网络进行扩容，增加网络设备、添加链路。

网络改造

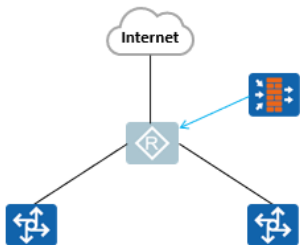


涉及对网络结构的调整，包括物理结构、逻辑结构。



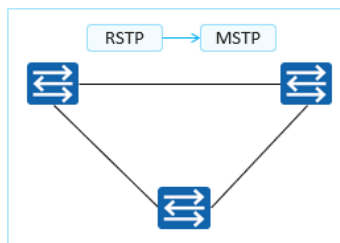
割接常见场景 (2)

设备替换



将原有老旧设备升级替换为新设备，或者更换为其他厂家设备，或者使用其他类型设备代替。

配置变更



在不改变物理拓扑结构的情况下，对设备配置进行变更，对正在运行的业务可能会产生影响。



割接流程

前期准备阶段

1. 项目调研
2. 项目分析
3. 风险评估
4. 输出割接方案
5. 方案验证、评审
6. 割接准备

中期实施阶段

1. 割接前快照
2. 割接执行
3. 割接回退
4. 割接测试、检查

后期收尾阶段

1. 守局
2. 割接验收

项目调研

准备阶段 实施阶段 收尾阶段

项目调研

项目分析

风险评估

输出割接方案

方案验证、评审

- 在割接开始前需要与客户网络信息负责人、一线维护工程师、ISP的技术接口人以及设备厂家代表等多方进行沟通，同时进行客户网络信息的收集。

静态信息采集分析

动态信息分析

业务模型分析

现网硬件环境勘察

信息采集分析

准备阶段 实施阶段 收尾阶段

项目调研

项目分析

风险评估

输出割接方案

方案验证、评审

- 现网的静态、动态信息用于分析网络情况以及割接前后网络情况进行对比分析，判断割接前后业务量是否正常。

静态信息采集分析

详细拓扑信息

设备类型

license

设备配置

设备版本

接口类型

动态信息采集分析

网络流量

带宽信息

协议状态

协议表项

时延、抖动

丢包率

业务模型分析

准备阶段 实施阶段 收尾阶段

项目调研

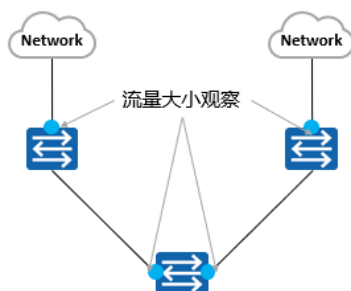
项目分析

风险评估

输出割接方案

方案验证、评审

- 在调研阶段还需要对客户的业务流量走向、业务流量大小进行观察，包括流量走向的变化和链路流量大小，可用于割接前后进行对比。



准备阶段 实施阶段 收尾阶段

现网硬件环境观察

项目调研

项目分析

风险评估

输出割接方案

方案验证、评审

- 在调研的最后阶段还需要对网络的现场环境进行观察，主要包括以下内容：
 - 光纤接口对应关系
 - ODF位置
 - 接口标识
- 对现网环境的观察便于割接时操作，同时相应的接口对应关系要进行记录，涉及到设备替换、线缆替换等割接操作便于割接完进行检查。

- ODF (optical distribution frame , 光纤配线架)：光纤配线架(柜)主要应用于骨干网、城域网及接入光纤光缆网络，具有主干光缆的连接、成端、分配、分光和调度功能。



项目分析



项目调研



项目分析



风险评估



输出割接方案



方案验证、评审

- 完成对项目的调研之后，需要对客户的需求进行分析、梳理，分析客户对割接后网络的新需求，如带宽，网络KPI指标，新业务承载能力等；
- 同时在该阶段将割接方案中的割接变更需求进行明确。
- 输出《客户需求分析表》。



风险评估



项目调研



项目分析



风险评估



输出割接方案



方案验证、评审

- 根据调研结果、需求分析结果，以及割接方案的框架进行割接风险分析与评估，针对可能出现的风险项目提前制定应对措施，并将对应的风险项对应措施责任人确认。
- 风险评估需要涉及的技术人员参与讨论，将各个风险的责任人明确到具体的技术人员。

输出割接方案

准备阶段

实施阶段

收尾阶段

项目调研

项目分析

风险评估

输出割接方案

方案验证、评审

- 根据调研结果、项目分析结果、技术人员风险评估编写相应的割接方案。
- 割接方案中需要将割接前准备阶段、实施阶段、收尾阶段的详细步骤、过程进行明确。



实施方案

准备阶段

实施阶段

收尾阶段

项目调研

项目分析

风险评估

输出割接方案

方案验证、评审

- 为进行高效、规范地割接，割接中的每个实施步骤都要提前规划，按照割接操作顺序到最小操作动作，细化到具体的命令行，以及每一个操作步骤执行所需的时间。
- 割接实施方案中需要制定相应的割接操作确认记录表，针对每一模块操作的时间点，完成后的结果确认和异常信息记录。

割接执行步骤

步骤	操作	操作时间
旧设备下线	旧设备下电、线缆拆除	0:00-0:30
新设备上架	新设备上电、线缆连接	0:30-1:00
新设备配置	新设备刷入提前配置好的脚本	1:00-1:20
网络状态检查	检查网络各项表项	1:20-2:00
业务测试	协调甲方人员测试业务、应用	2:00-2:30



回退方案

准备阶段 实施阶段 收尾阶段

项目调研

项目分析

风险评估

输出割接方案

方案验证、评审

- 回退方案：当割接失败时（割接之后业务测试失败、割接时间结束未完成割接...）需要将网络退回到割接前初始状态，此时需要按照回退方案进行操作，将网络恢复。
- 在制定割接方案时需要包含详细的回退方案，同割接操作一样，需要精确到每一步操作这样当割接失败时可以有条不紊地进行回退。

割接回退步骤

步骤	操作	操作时间
新设备下架	新设备下电、线缆拆除	3:00-3:20
重上架旧设备	旧设备上电、线缆连接	3:20-3:40
业务测试	协调甲方人员测试业务、应用	3:50-4:00



方案验证和审定

准备阶段 实施阶段 收尾阶段

项目调研

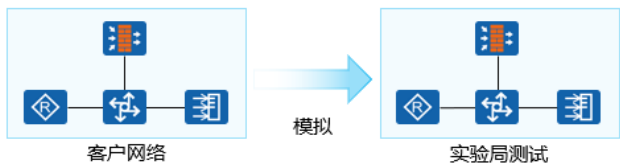
项目分析

风险评估

输出割接方案

方案验证、评审

- 一般大型的、重要的割接项目，都要求在实验室内搭建环境进行提前验证，将之前的风险点进行测试，并对整个方案的可行性确认，这种使用实验室环境验证的被称为实验局测试。
- 除了实验局方案验证之外，还需要和客户、实施方进行技术评审会，对割接方案中的技术进行论证，同时了解双方的实际需求和存在困难，面对面解决问题。





割接准备

准备阶段

实施阶段

收尾阶段



项目分析



风险评估



输出割接方案



方案验证、评审



割接准备

- 割接准备是割接实施前的重要步骤，同时充分地准备也是顺利完成割接的基础。
- 割接的准备分为环境准备（硬件，软件，工具，备件等）、人员准备（甲方，乙方，监理）和流程准备（执行时间划分），只有充分考虑周全，才会确保万无一失。

准备内容

硬件

软件

工具

备件

人员准备

时间安排

对照表



软、硬件准备

准备阶段

实施阶段

收尾阶段



项目分析



风险评估



输出割接方案



方案验证、评审



割接准备

硬件

设备

上电测试

单板

运行观察测试单板是否正常

线缆

连通性测试

软件

版本

设备版本配套、对接版本配套检查

License

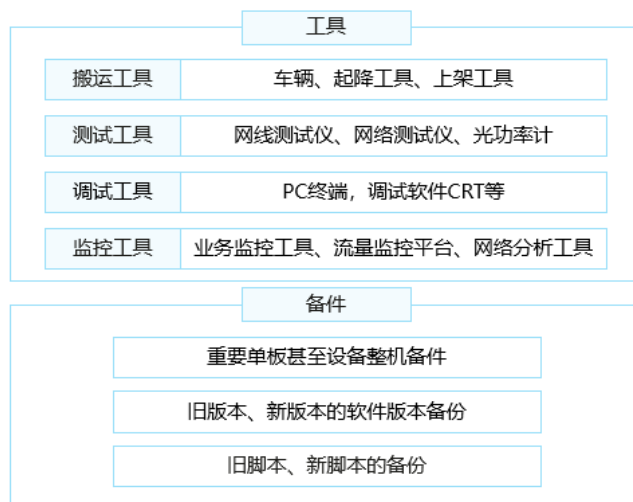
检查授权License是否到位

脚本

整体脚本、分段配置脚本、回退脚本



工具、备件准备



人员准备

- 在割接前应将人员责任划分清楚，确保割接实施中沟通顺畅，让割接能够顺利进行。



- 时间安排的准备：
- 时间安排必须与客户沟通，并获得客户的同意。
- 制定总的时间安排表。
- 规定出每个时间段执行的具体动作。
- 割接执行阶段的时间要精细到分钟。
- 重大操作的时间段要预留部分时间，避免因超时引发工程事故。
- 割接时间点的选择尽量避免业务高峰期（如节假日，非

正常上班时间等)。

准备阶段

实施阶段

收尾阶段

目录

割接前快照

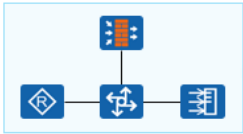
割接前快照

割接执行

割接回退

割接测试、检查

- 为便于割接回退以及割接之后对比业务是否正常，在正式开始割接之前需要对现网配置、现网数据再进行一次快照，具体包括以下内容：
 - 现网配置进行备份
 - 现网动态数据采集（端口状态、流量、各路由协议状态、路由数量、STP协议状态、各端口ARP/MAC地址表项）。
 - 割接前对业务进行测试，确保割接涉及的业务在割接前属于正常状态。



备份

现网配置

现网动态数据

端口状态、流量

路由协议状态

路由数量

STP协议状态

ARP、MAC表项

准备阶段

实施阶段

收尾阶段

目录

割接执行

割接前快照

割接执行

割接回退

割接测试

- 现场割接人员按照提前准备好的割接步骤一步步严格执行，无特殊原因不能临时更改实施步骤。
- 每一步骤的执行记录下割接实际操作过程的时间点、执行动作、执行结果。

Step 1

Step 2

Step 3

Step 4

0:00

1:30

2:00

3:00

已完成75%

割接回退

准备阶段 实施阶段 收尾阶段

割接前快照

割接执行

割接回退

割接测试、检查

- 如果在指定的时间前未完成割接，需按照提前准备的回退方案一步步进行回退，将网络恢复。
- 具体回退范围可根据实际情况，与客户协商部分回退或全部倒回退。



割接测试

准备阶段 实施阶段 收尾阶段

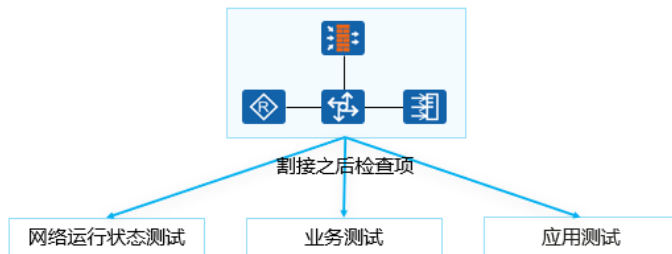
割接前快照

割接执行

割接回退

割接测试、检查

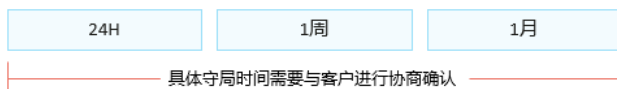
- 割接实施完成后为测试割接是否成功，需要从以下几个方面对网络、业务进行测试：
 - 网络运行状态测试：对现网的动态数据在进行一次采集，与割接前进行对比。
 - 业务测试：通过ping、tracert或者客户侧的第三方软件测试网络连通性、延迟、抖动等指标是否到达业务要求
 - 客户应用测试：测试由网络承载的客户应用，检查是否正常。



守局

准备阶段 实施阶段 收尾阶段

- 割接操作完成且通过客户应用业务测试后，网络需进入一个特殊的观察期，在此期间工程师一般驻守在客户局点，观察网络运行状态，防止出现意外故障。

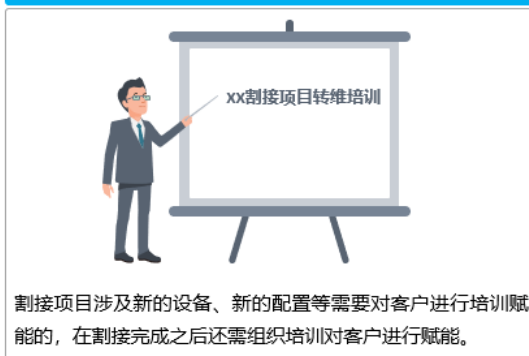




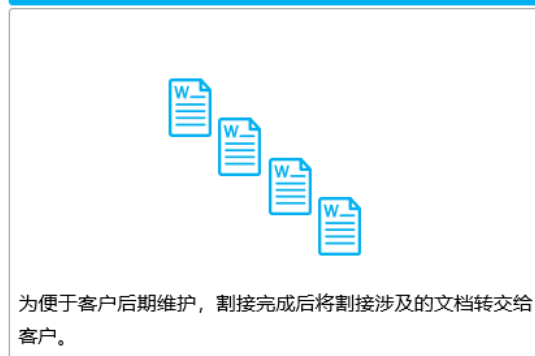
割接验收

- 割接顺利完成并在守局观察无异常之后还需要对客户进行维护培训以及资料移交。

转维护培训



资料移交



割接场景案例 - 注意事项

- 该场景案例重点是通过实践对真实的割接案例进行体验，掌握割接的流程和方法，而不仅仅只是完成割接要求的设备配置规划。
- 对于给出的割接场景，需要按照割接流程进行讨论，并按照《项目割接方案模板》输出割接文档，包含以下内容：
 - 项目调研、分析：包含现网拓扑、业务分析，以及应采集哪些设备的动态、静态信息。
 - 风险评估：割接中可能出现的风险，以及风险如何规避。
 - 割接方案：细化到每个步骤执行哪些命令，以及每个操作步骤的时间节点。
 - 测试、检查项：割接之后应检查哪些内容，测试哪些内容。



课堂环节

背景介绍 15min

- 教师介绍割接案例的场景，输入（拓扑图、业务规划、分组讨论）、输出（分组总结、割接流程、割接相关文档）。

分组 5min

- 分小组进行讨论，选举组长，组长负责最终的总结、汇报。

讨论 30min

- 各小组按照割接操作中的步骤进行讨论，商讨应该执行的步骤，设计设备应配置哪些内容，以及编写割接文档。

总结 20min

- 各小组汇报讨论结果，汇报本小组讨论的结果，并提交相应文档。

项目改造前期介绍

某公司存在多个分支机构，这些分支机构通过专线与总部网络相连接，现存在如下问题：

专线速率较低，无法应对新业务的高带宽要求。

分支机构出口采用单出口设备，单上行链路（专线）的方式，存在单点故障。

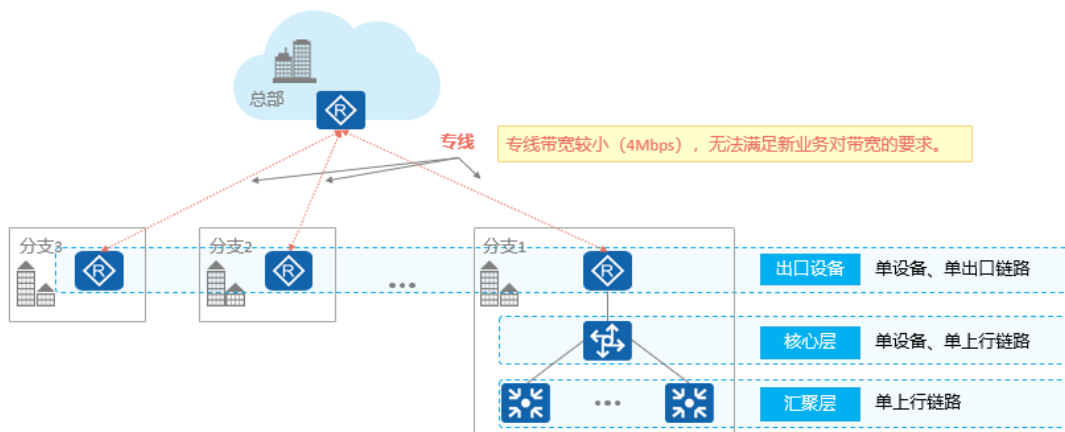
若对专线提速，费用较高。

核心交换机为单机部署，存在单点故障。

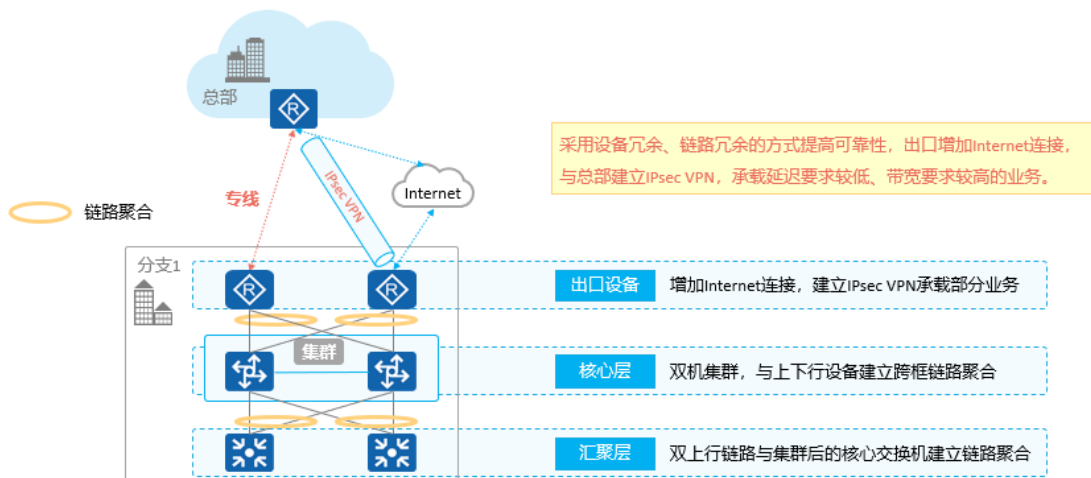
分支结构终端用户增加，核心交换机、出口路由器已经呈现出性能不足的现象。

为解决这些问题，现该公司决定对分支机构网络进行改造，提升分支机构网络的可靠性，提高与总部通信的带宽。

原拓扑介绍

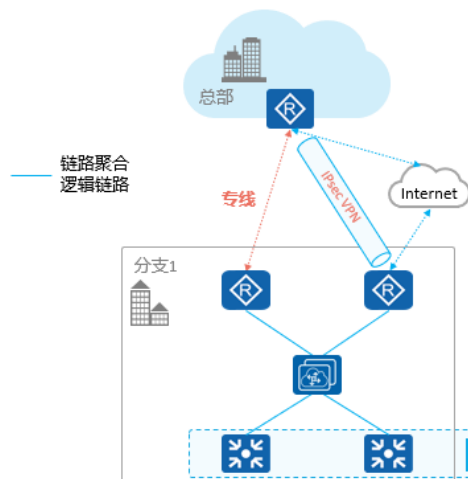


目标拓扑





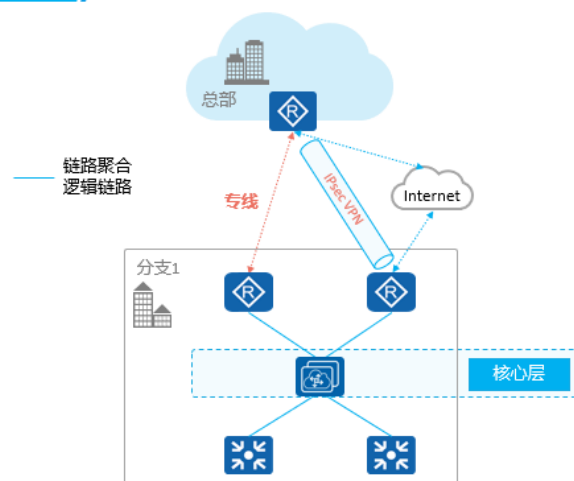
目标逻辑拓扑 (1)



汇聚层采用双上行接入，与集群后的核心交换机建立链路聚合。
网关设置在核心交换机的VLANIF接口上，依赖核心交换机的集群，
链路聚合提高可靠性，无需部署VRRP。



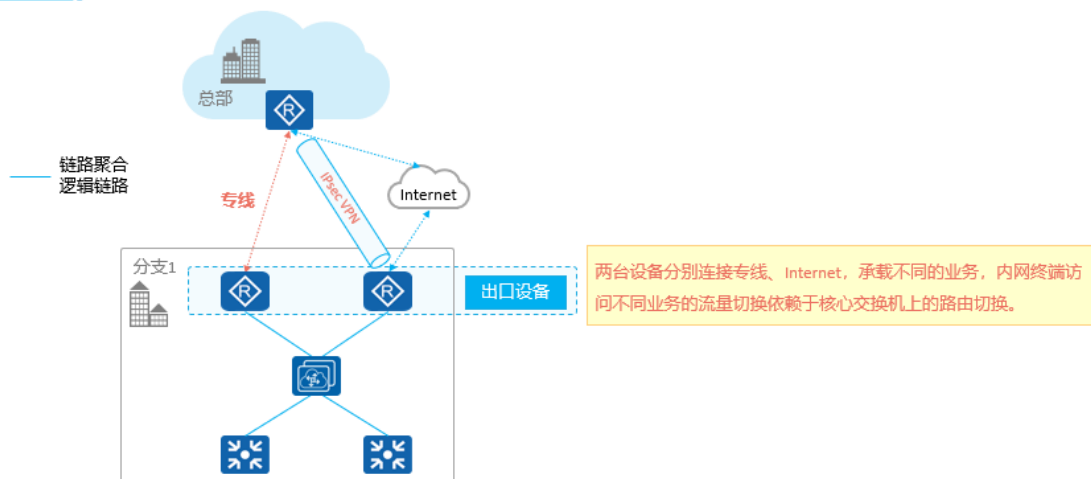
目标逻辑拓扑 (2)



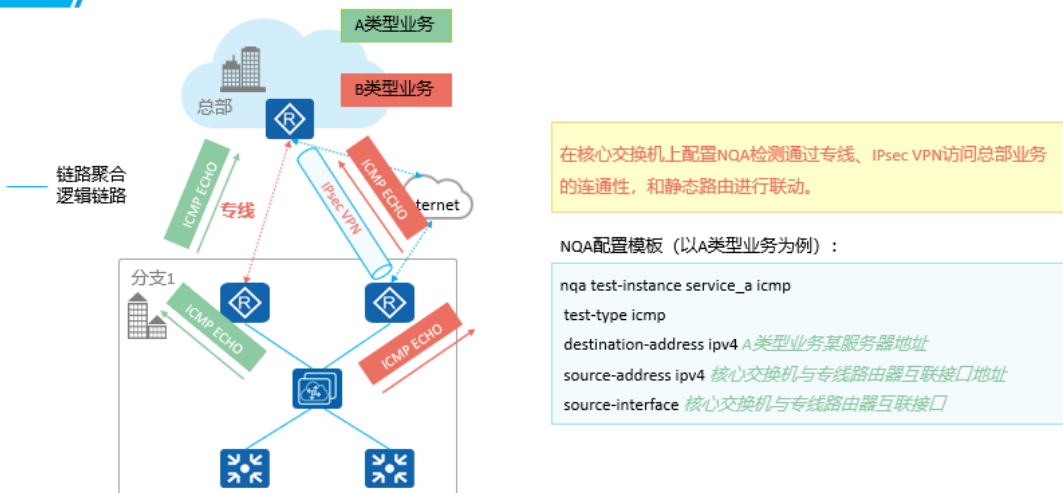
作为内网终端的网关，配置静态路由将不同业务的流量分别指向
专线、IPsec VPN出口设备上，并配置浮动路由作为路由备份。
配置NQA分别检测专线、IPsec VPN的可用性，静态路由Track NQA
以实现当链路故障时，可以将流量切换到备份路径。



目标逻辑拓扑 (3)



NQA检测设计

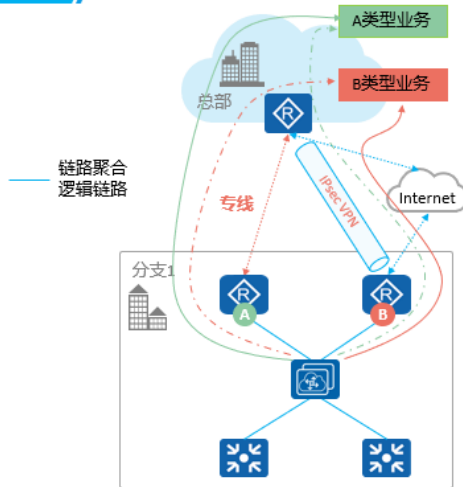


NQA配置模板 (以A类型业务为例) :

```
nqa test-instance service_a icmp
test-type icmp
destination-address ipv4 A类型业务某服务器地址
source-address ipv4 核心交换机与专线路由器互联接口地址
source-interface 核心交换机与专线路由器互联接口
```

- A 类型业务：对延迟要求较高，但是对带宽要求较低的业务，该类业务使用专线进行承载。
- B 类型业务：对延迟要求较低，但是对带宽占用较多的业务，该类业务使用 IPsec VPN 进行承载。
- 总部的回向路由同样通过手动指定静态路由，结合 NQA 的方式进行备份路径切换，本案例中重点关注分支部分，对于总部不涉及。

路由备份设计



→ A类型业务主路径 → B类型业务主路径
 - - - A类型业务备用路径 - - - B类型业务备用路径

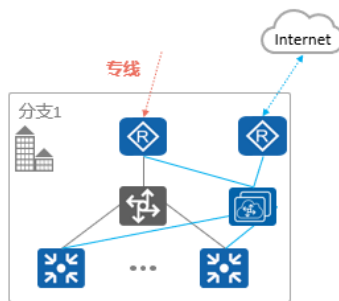
核心交换机上将前往A类型业务、B类型业务的路由分别指向不同的出口设备，由不同的链路承载，并通过设置浮动路由使得两个出口设备互为路径备份。

核心交换机静态路由配置模板：

```
ip route-static A类型业务地址 mask A track nqa service_a icmp
ip route-static A类型业务地址 mask B preference 70

ip route-static B类型业务地址 mask B track nqa service_b icmp
ip route-static B类型业务地址 mask A preference 70
```

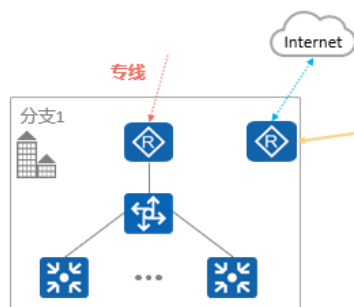
割接方案 (1)



按照如下步骤将原有网络迁移到目标网络（概览）：

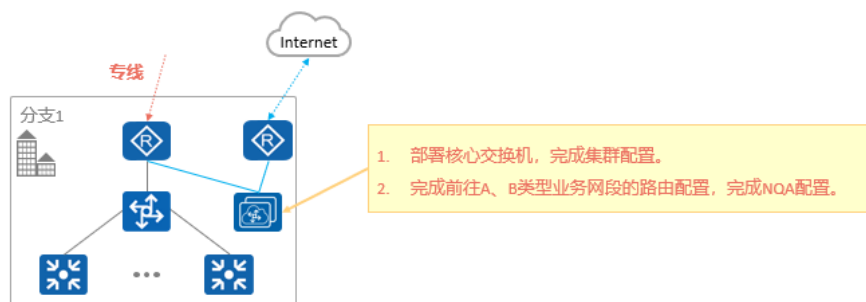
- 部署新的出口路由器，与Internet连接，完成IPsec VPN的建立，完成路由的配置。
- 部署新的两台核心交换机，完成集群的配置，路由的配置，与出口路由器之间完成跨框聚合的配置，此时不与汇聚交换机连接。
- 断开原核心交换机与上下行设备的连接，将汇聚交换机与新的集群核心交换机连接。

割接方案 (2)

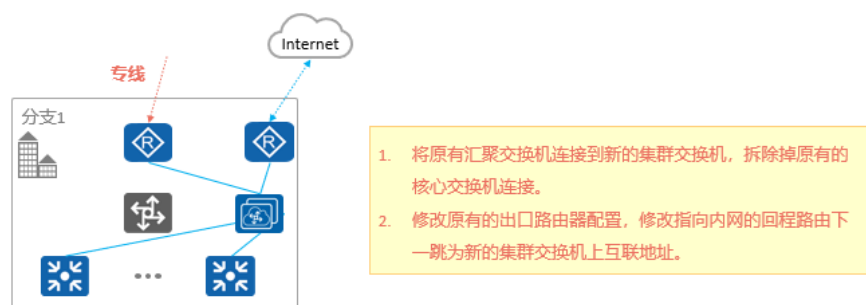


- 出口路由器接入Internet。
- 完成与总部的IPsec VPN部署。
- 配置前往总部业务网段（A、B都包含）的路由。
- 配置前往内网的回程路由。

割接方案 (3)



割接方案 (4)



思考题：

- 割接前为验证风险点可以在本地进行什么样的操作？
- 在割接开始前需要对客户网络进行哪些内容备份？

参考答案：

- 可以在本地搭建实验局，模拟客户的网络进行验证，确认整个割接方案的可行性。
- 需要对现网的配置进行备份，同时为方便割接前后对网络状态进行验证，还需要对现网动态数据进行采集（端口状态、流量、各路由协议状态、路由数量、STP 协议状态、各端口 ARP/MAC 地址表项）。
-