

网络割接



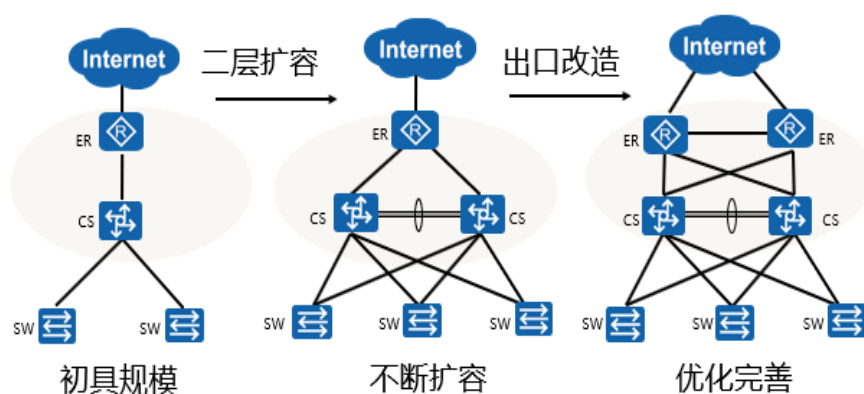
前言

- 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。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。
- 通过本课程的学习能够使学员熟悉割接的流程和操作规范、掌握风险把控措施，从而能够高效、顺利地完成网络割接。



企业网络的不断变化

- 网络是承载企业业务的基础，其自身也是在不断发展和变化的。



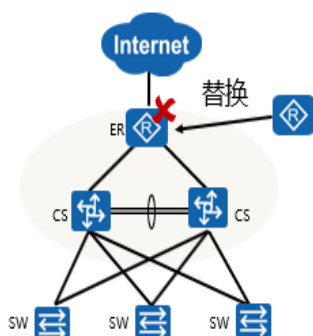
- 如此不断地升级、扩容、整改，怎样保障业务的平稳过渡？
- 以上为某公司网络的发展史：
- 某公司在 2012 年时只有一个小型的办公区域，且业务流

量较小，只需要进行简单地网络接入即可。

- 经过两年的发展，公司员工的数量越来越多，业务流量越来越大，且业务也越来越重要，故对网络进行了扩容，新增了一台交换设备，并形成了汇聚层负载分担的网络架构。
- 到了2016年，企业网络出口带宽已经不能满足业务需求，于是在网络出口处又增加了一台核心路由器，并形成了主备模式的网络出口架构。

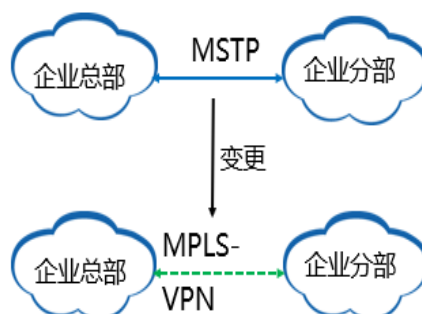
维护网络的手段

- 设备是有生命周期的



- 核心出口设备的更换，存在中断大量业务的风险。

- 链路是不断变化的



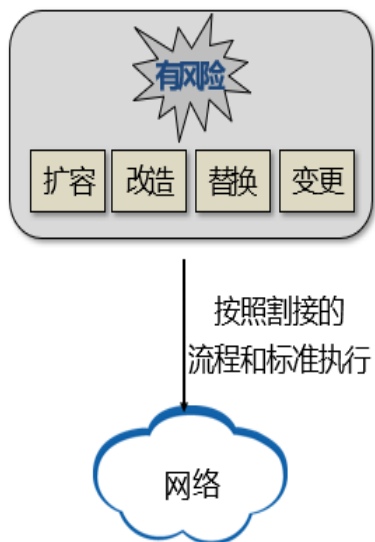
- 链路的变更不仅是物理线路的切换，还需要进行业务配置的调整。

- 任何产品都是有生命周期的，一般为了安全起见，运行5-10年的ICT设备基本都要考虑退网，并由新的高性能设备替代，所以怎样实现安全平稳的过渡是个需要重点关注的问题。
- 网络线路是结合市场环境和自身需求来不断升级的，如先前大部分大型公司的企业总部和分支机构间通信需要支付高昂的费用来租用ISP的MSTP (SDH) 线路，但是目前租用MPLS VPN线路已成为主流，为企业节省了大笔的开支，所以为保证不影响业务，安全地从MSTP线路切换为MPLS VPN线路的这个过程就是一个需要考虑的问题。



割接概述

- 如果执行的技术迁移动作会影响现网运行业务，此时就需要在实施时严格地按预先设定的操作流程和风险控制措施进行执行，一般将此类项目定义为割接项目。



割接难点



风险在哪里？



方案怎么写？



实施怎么做？

- 预估风险→制定方案→严格执行



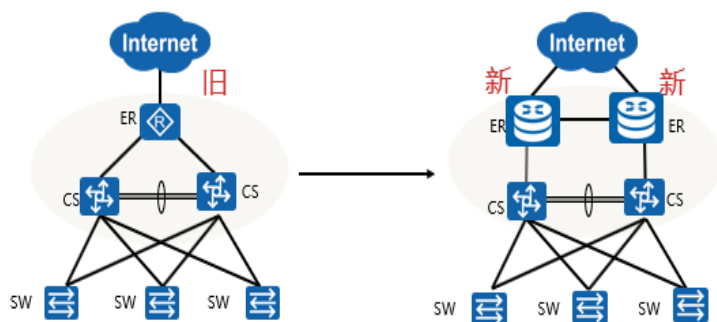
割接的操作流程

- 前期准备阶段：
 - 项目调研、需求分析、风险评估、方案编写、方案审定。
- 中期实施阶段：
 - 割接准备、割接实施、业务测试。
- 后期收尾阶段：
 - 守局、项目验收。



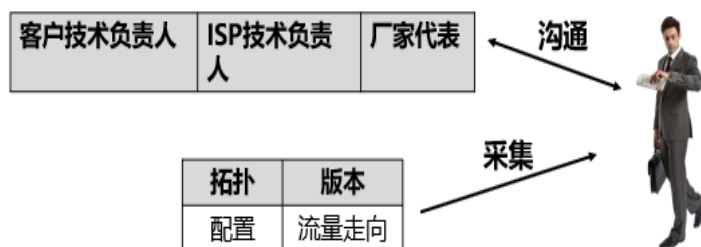
网络现状分析

- A公司网络已运行多年，随着业务的不断发展，出口核心路由器承载的业务量越来越大，并且设备投产的年限已经快达到A公司的规范年限，对此客户提出在网络核心层新增两台高性能路由器并替换掉原来运行的老旧路由器。



项目调研

- B公司是负责A公司的网络建设及维护的单位，获得A公司的改造需求后，派遣公司资深网络专家小王前来分析调研。
- 小王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，并现场采集全网信息（拓扑、配置、版本、流量类型、流量路径等）。



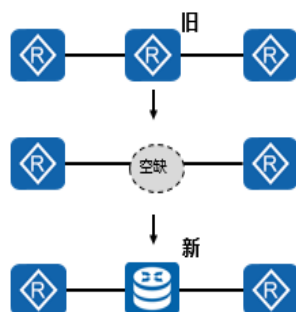
项目分析

- 小王经过一周调研，结合自己多年的工程经验对客户需求进行分析：
 - ◻ **必要性**-核心出口路由器运行时间过长且承载的业务越来越多，故需要更换。
 - ◻ **可行性**-与厂家代表进行技术沟通并结合自己多年经验以及历史成功案例分析，可以操作的。
 - ◻ **风险性**-核心出口路由器的更换需要执行业务切换动作，存在业务中断的风险。
 - ◻ **项目定性**-由于网络的架构变动比较大而且是核心出口，故定义为网改项目。
 - ◻ **技术定位**-由于核心出口的改造对全网业务的正常运行可能造成很大风险，故需要谨慎操作。

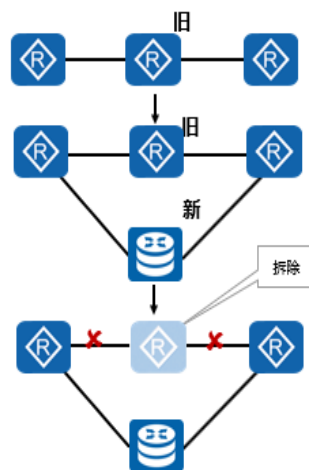


方案筛选

- 针对本次割接小王提出了两种割接方案，并准备在后续的讨论会上与客户协定。



直接替换法



逐步融入法

- 直接替换法：
- 优点：执行效率高，割接整体周期较短，消耗资源较少。
- 缺点：风险大，中断时间长。
- 适用场景：网络规模较小，影响的业务重要性一般，项目费用要求较低的情况。
- 逐步融入法：
- 优点：风险小，回退方便。
- 缺点：割接整体周期较长，效率低下。
- 适用环境：网络规模较大，影响的业务重要性较高，项目费用比较宽裕的情况。






风险评估

- 在割接方案中，小王对本次割接操作的风险做了详细的分析和评估。

风险方面	A公司割接项目
主要风险点	业务切换操作
风险影响的范围	全网
风险影响的时间	中断时间5-120分钟
风险带来的损失	公司业务无法正常恢复运行
如何避开风险	逐段割接+回退操作+现场备件更换

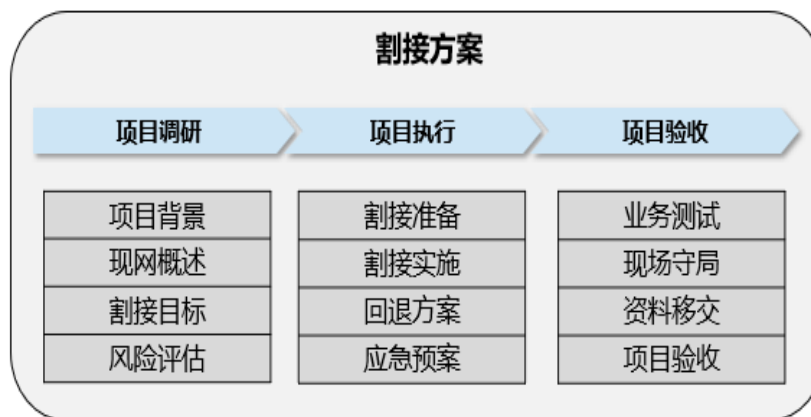
- 风险评估的要点：
- 中断的时间长短和影响的业务范围是分析的重点，必须定位清楚，并给予客户明确的说明和应对措施。

沟通协调会

厂家 		ISP 	
甲方 	设备选型	厂家：我司提供的新型路由器性能很高，适于各种场景，有质量报告和案例证明。	
	出口对接	ISP（运营商）：之前成功配合完成过很多类似的项目。	
	风险评估	甲方（客户）：时间、资金都相对宽裕，但最重要的是能保证业务正常运行。	
	方案筛选	乙方（承建方）：用逐步融入法进行割接风险最小。	
乙方 			
监理：大家互相配合，共同合作，顺利完成本次改造项目。			
监理 			



方案编写



方案验证和审定



搭建实验局测试



各方技术评审



原厂专家审核



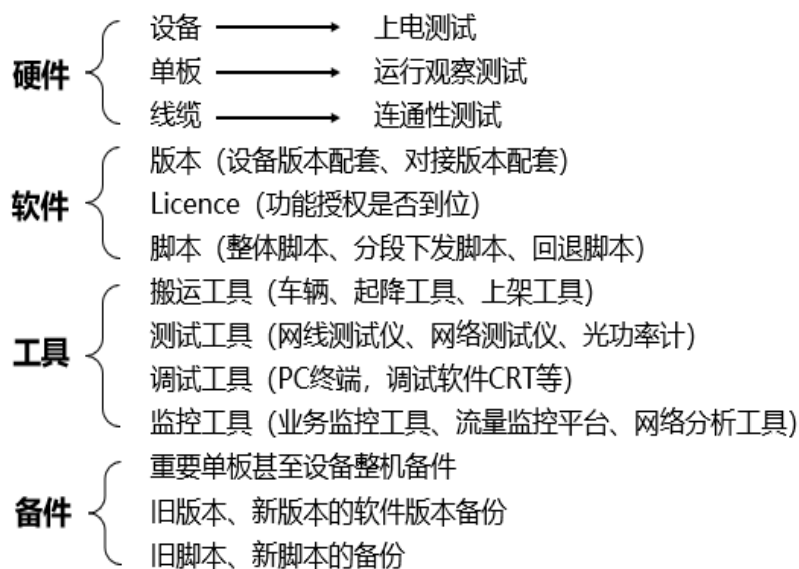
方案定稿

- 搭建实验局测试：
- 如果是大型割接项目，客户常常会要求搭建实验局提前进行验证测试。实验局环境要求和真实网络环境保持一致。
- 各方技术评审：

- 各方技术评审主要是让客户、施工方积极互动，了解双方的实际需求和存在困难，面对面解决问题。
- 原厂专家审核：
- 一般涉及到设备版本的变更，设备新功能的添加等都要求送原厂专家审核。
- 本案例情况：
- 本例中由于新增的路由器为新设备，需在割接前上架加电并测试运行状态。
- 必要时，可申请厂家专业工程师做现场技术评定，查看设备运行情况。



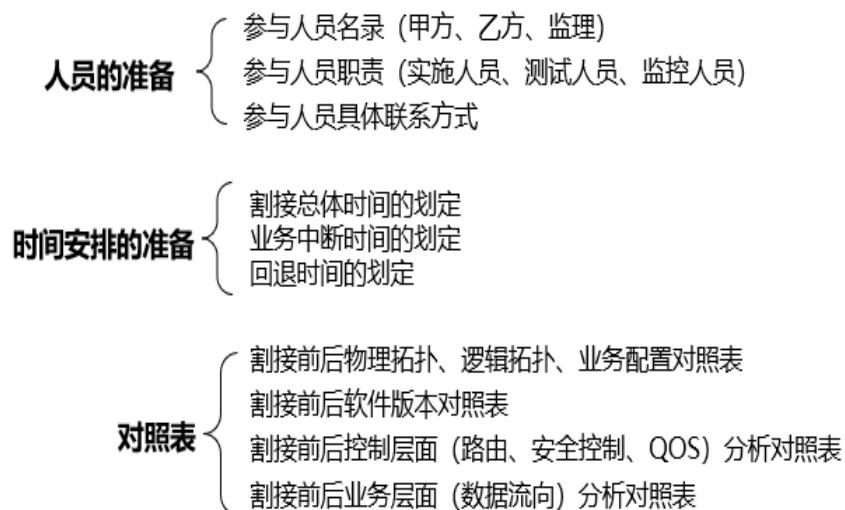
割接准备 (1)



- 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。



割接准备 (2)



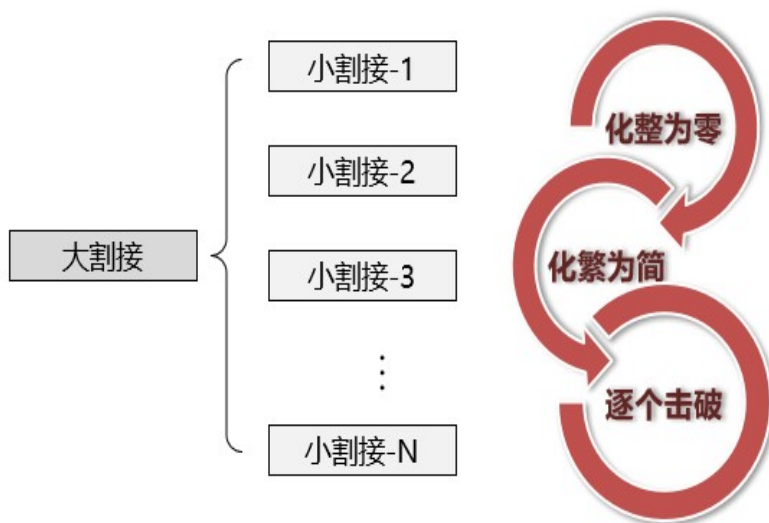
- 人员的准备：
- 人员责任的划分能够保障各方人员实施过程中沟通顺畅，不会导致责任推卸问题。
- 时间安排的准备：
- 时间安排必须与客户沟通，并获得客户的同意。
- 制定总的时间安排表。
- 规定出每个时间段执行的具体动作。
- 割接执行阶段的时间要精细到分钟。
- 重大操作的时间段要预留部分时间，避免因超时引发工程事故。
- 割接时间点的选择尽量避免业务高峰期（如节假日，非正常上班时间等）。

实施签发

- 整体的《割接方案》审定通过后必须有客户的签字。
- 每次在进行具体的实施操作之前必须提交《变更申请表》。
- 提交的《变更申请表》必须有客户具体负责人的签字。
- 每次割接变更前必须以邮件、电话、短信等方式通知到位。

一些不容忽视的环节！

割接实施 - 分块割接

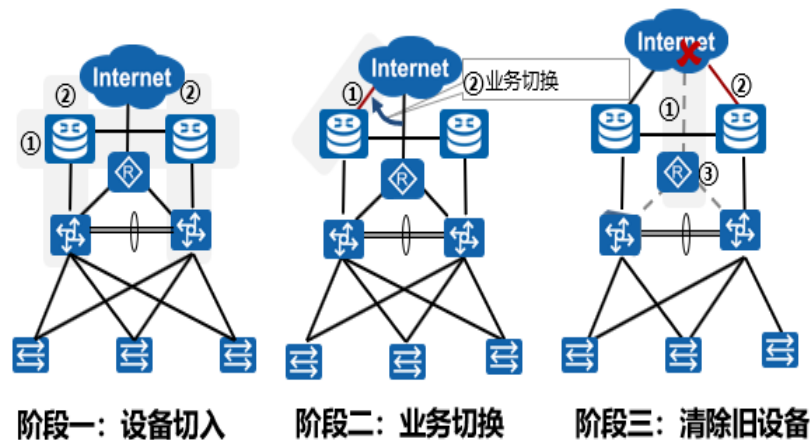


- 分块割接：
- 定义为割接的项目，业务的复杂性往往都很高，风险的把控需尽量细化到每个步骤。
- 化整为零，把大割接分成几个小割接，每个小割接之间

既相互独立又前后承接，且每个小割接也需严格地细化执行步骤。

割接实施 - 割接思路

- 小王将本次割接分成三个阶段：



- 设备切入：
 - 步骤 1：新增两台核心路由器，并对接好链路。
 - 步骤 2：新核心路由器与原有旧汇聚交换机对接链路。
 - 步骤 3：进入阶段一的稳定观察期，新设备运行时间至少要设置两周左右。
- 业务切换：
 - 步骤 1：核心路由器与 ISP 进行物理线路的对接。
 - 步骤 2：执行业务切换操作，让流量从旧核心路由器出口转换成从新核心路由器出口，具体方法可利用双方下发的默认路由来实现。
 - 步骤 3：进入阶段二的稳定观察期，业务切换的观察周期最好持续 2-24 小时。
- 清除旧设备：
 - 步骤 1：断开旧核心路由器出口，空出原有连接 ISP 的线路。

- 步骤 2：将第二台新核心路由器对接空出的 ISP 的链路，并配置连通业务。
- 步骤 3：旧核心路由器下架以及相关物理线缆清除等。



割接实施 - 割接步骤 (1)

- **割接前快照**

- 割接操作前需将操作对象的状态（端口、线路、协议、流量）记录下来，同时再次备份配置文件。

- **割接中执行**

- 下发配置命令或者执行物理操作。
- 每个步骤的“执行时间”都要有明确标注。

- **割接后检查**

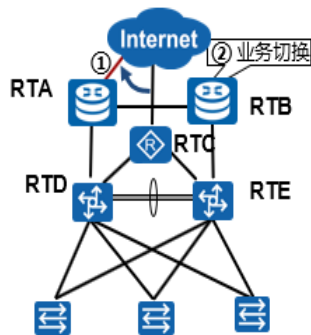
- 通过display/ping/tracert等命令查看以及用仪器仪表测试。

- 割接前快照：
- 割接前快照主要目的用于记录设备当前运行状态，若割接失败能及时分析失败原因和能够快速的回退。
- 割接中执行：
- 割接中执行的命令下发要根据实际的网络环境，决定是逐条下发，还是批量下发。
- 物理动作的执行需注意人身安全以及设备和线路的保护，做到精细、认真。
- 割接后检查：
- 割接后的检查要利用各种方法配套进行测试，避免只使用一种方法成功完成测试后就认为此次割接已经成功，严格情况下需设置一定的观察时间。



割接实施 - 割接步骤 (2)

- 本示例的阶段二中的业务切换是割接中的关键点，可参考如下步骤：



① 快照 (2016年6月8日02:30-02:35)

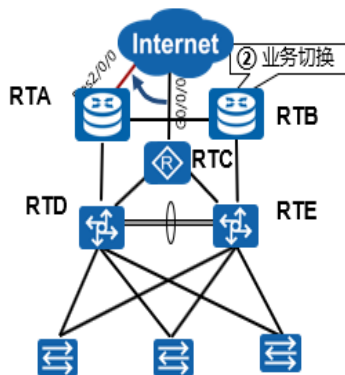
```
<RTC>display ip routing-table #查看路由
<RTC>display time-range all #查看当前时间段状态
<RTC>display log all #查看用户操作记录
<RTC>display device #查看设备的部件状态信息
<RTC>display version #查看设备版本信息
<RTC>display ospf peer #查看路由器邻居信息
<RTC>display acl all #查看访问控制信息
...
```

- 本示例中与本网络环境相关的信息一定要进行快照。快照操作命令以RTC为例，其他路由器类似。
- 快照：
- 本示例中在割接命令下发前可快照 RTC、RTD、RTE 等相关路由器的当前配置信息和配置状态，特别是与本网络环境相关的信息一定要快照。



割接实施 - 割接步骤 (3)

② 动作 (2016年6月8日02:35-02:40)



```
[RTA]ip route-static 0.0.0.0 0.0.0.0 pos2/0/0
#配置RTA默认路由到互联网
[RTA-ospf-1]default-route-advertise cost 5
#配置RTA在OSPF路由域下发默认路由
```

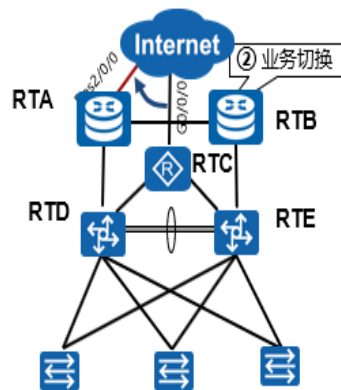
③ 验证 (2016年6月8日02:40-02:45)

```
<RTD>display ip routing-table #查看路由表
<RTD>display ospf lsdb ase 0.0.0.0
#查看OSPF数据库默认路由
```

- 下发默认路由的时候设置cost为5的原因是让RTC暂时仍然为网络业务的出口。
- RTA虽然此时还未成为网络业务出口，但是已经“潜入”进OSPF的数据库中。
- 动作：
- 本例中需先在 RTA 上配置去往互联网的默认路由，再向 OSPF 区域内下发默认路由，传递到全网路由器。该操作有三种可选方案：
- 第一种配置方法是直接让 RTA 下发的默认路由优先级低于原有的默认路由，如配置：[RTA-ospf-1]default-route-advertise type 2。因为 type 2 类型的外部路由优先级低于 type 1 类型的外部路由，从而实现了 RTA 下发的新路由暂时不被优选。
- 第二种配置方法是让 RTA 下发的默认路由开销高于原有的默认路由，虽然不会抢占原先的默认路由，但是可以作为备份，潜伏在 OSPF 的 LSDB 库中，随时准备抢占主用默认路由；(本案例选择的是该种配置方法)。
- 第三种配置方法是让 RTA 下发的默认路由与原先默认路由形成等价，使两条默认路由形成负载分担的形式。由于不能掌控具体流量的走向，在割接项目中不建议采用这种操作。
- 验证：

- 查看 RTD 和 RTE 的路由表，确认默认路由还是指向 RT C。
- 查看 RTD 和 RTE 的 OSPF 的 LSDB，核实生成默认路由的 5 类 LSA 除 RTC 之外还应该有 RTA。

割接实施 - 割接步骤 (4)



④ 动作 (2016年6月8日02:45-02:50)

[RTC-ospf-1]undo default-route-advertise #取消RTC在 OSPF路由域下发的默认路由

⑤ 验证 (2016年6月8日02:50-02:59)

<RTD>display ip routing-table #查看路由表
<RTD>tracert 119.145.15.60 #确认流量走向
若未割接成功，则需要进行回退操作。

⑥ 回退 (2016年6月8日03:10-03:15)

- 动作：
- 在原有默认路由出口 RTC 上执行关闭下发默认路由的操作，于是 RTD 和 RTE 没有了指向 RTC 的默认路由，所以此时指向 RTA 的默认路由会马上进入它们的 IP 路由表。
- 验证：
- 若查看 RTD 和 RTE 的路由表，发现它们去往 Internet 的默认路由确实都已指向 RTA，再用 tracert 命令测试数据层面流量，确实是经过 RTA 到达网络出口的，再测试用户业务是否可用，若都可用，则初步表明此次割接成功；否则表示割接失败，需进行回退操作。

回退

- 定义
 - 回退是指将当前变更改回到执行前的状态。
- 场景
 - 当割接失败或某一步骤出现失败，回退将不可避免，且必须执行。
- 例子

⑥ 回退 (2016年6月8日03:10-03:15)

```
[RTC-ospf-1]default-route-advertise  
#重新在RTC上下发默认路由到全网
```

- 要求
 - 在每个小割接的步骤中最后一项都为回退操作说明。

回退时机



- 本示例中由于规划为三个大阶段，需在三个大阶段设定各自的回退要求和执行时间。



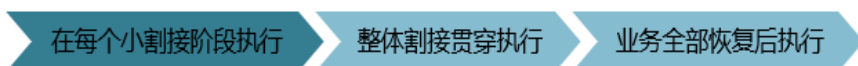
回退失败

- 正常情况下如果割接失败是可以回退到原始的运行状态的。
- 当割接中出现由于不可抗因素造成割接失败时，若无法回退可采用应急预案。
- 应急预案需体现在《割接方案》中。
- 应急预案中的应急措施主要有：重新加载系统软件，替换现场备件，等等。



测试

网络运行状态测试	网络业务状况测试	客户应用业务测试
查看设备运行状态	测试业务连通性	客户上层应用业务测试
查看各种协议状态	测试业务性能	稳定性观察



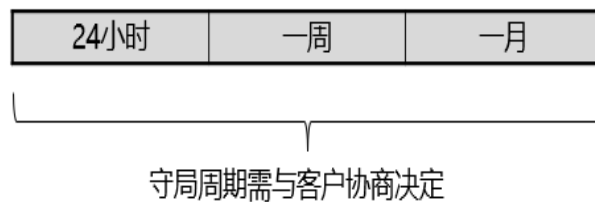
- 测试最终通过应以客户**应用业务达标**为准！

- 网络运行状态测试：
- 主要使用 display 命令查看设备的状态，如版本、日志、接口、各种协议的邻居关系，路由表，各种 feature 的状态（NAT、VRRP、NQA、VPN、QoS）。

- 网络业务状况测试：
- 用 ping 测试业务连通性，用 tracert 命令测试业务路径，用第三方软件或网络分析仪测试业务宽带和时延指标等是否达到业务要求（常用仪器如 SmartBits、IXIA 网络测试仪等）。
- 客户应用业务测试：
- 割接完成后网络上层承载的业务测试需由客户自主进行，若客户对相关业务测试指标有特殊要求，需尽力通过调整网络满足客户要求。

守局

- 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



转维培训



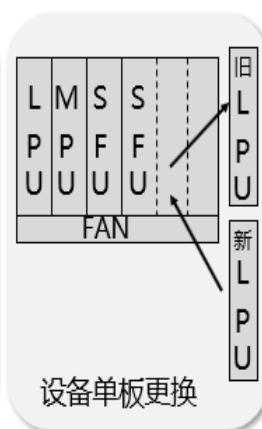
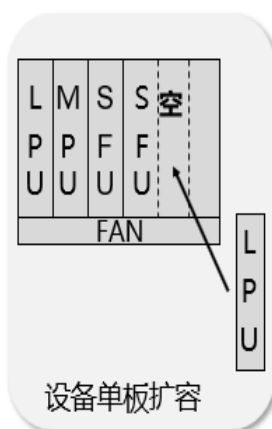
资料移交



验收总结会



常见割接场景 - 设备升级



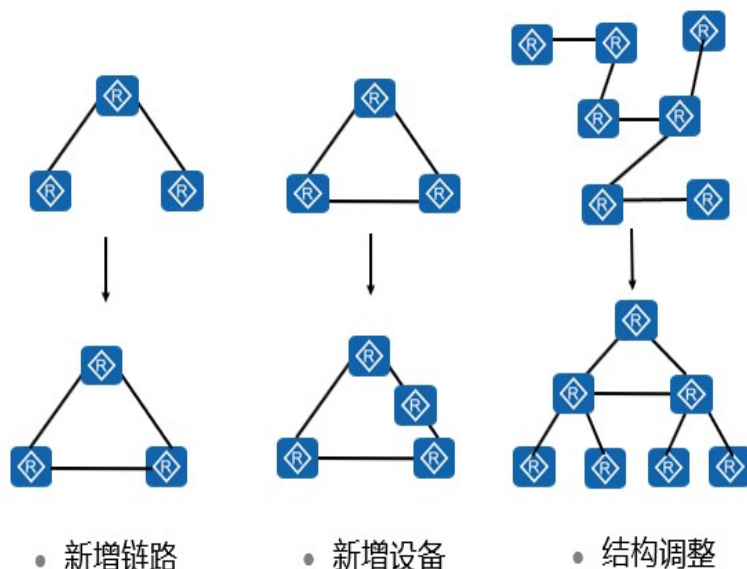
- 此类割接建议申请厂家进行技术支持。

- 设备升级类割接：
- 设备升级时要注意新增或替换的板件的版本型号是否与设备匹配，软件版本是否达到现有设备的版本配套表里面的版本要求，并确认单板是否支持热插拔操作等。

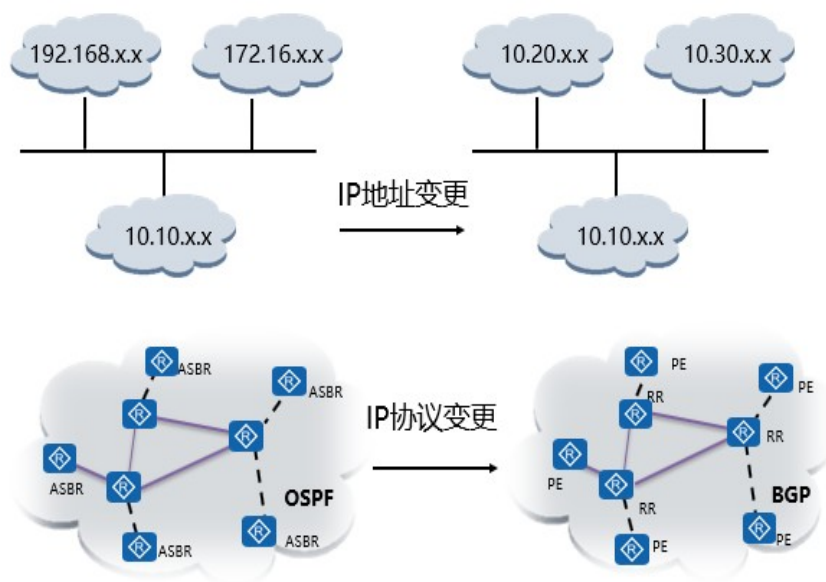
- 设备软件升级必须得到厂家的授权，并下载官方的软件版本。设备软件升级最好准备有物理备件并且有回退预案。



常见割接场景 - 网络物理结构改造

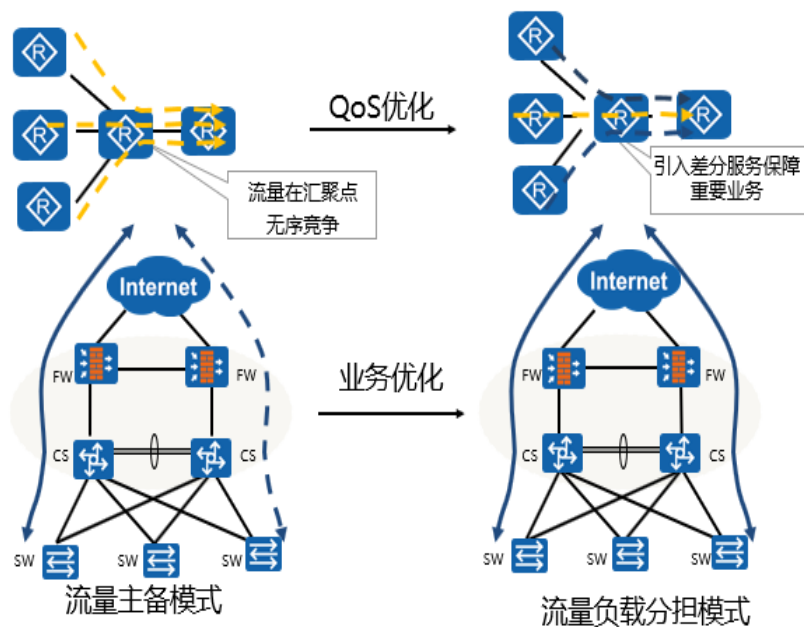


常见割接场景 - 网络系统调整

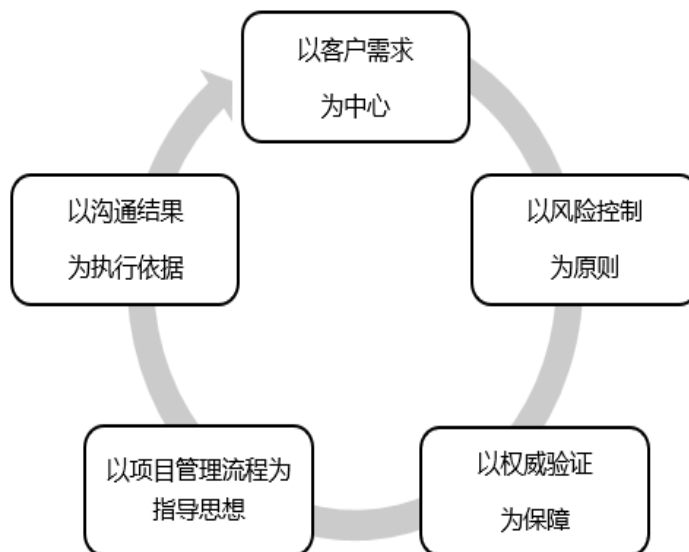




常见割接场景 - 网络性能优化



割接总结





思考题

1. 割接方案验证和审定主要有哪些方法?
2. 具体割接操作步骤的三部曲是 ()。
3. 如果割接失败需要怎么做才能规避风险?

- 1、答案：主要方法有搭建实验局，各方技术评审，原厂专家审核。
- 2、答案：割接前快照，割接中执行，割接后检查。
- 3、答案：割接失败就要执行回退，回退失败执行应急预案。