

# Wi-Fi 6 搬迁替换指导

文档版本

01

发布日期

2020-12-28



版权所有 © 华为技术有限公司 2020。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <https://e.huawei.com>

---

# 目录

---

<b>1 文档概述</b> .....	<b>1</b>
<b>2 传统 WLAN 网络搬迁典型场景</b> .....	<b>2</b>
<b>3 搬迁原则和搬迁思路</b> .....	<b>4</b>
<b>4 搬迁需求分析</b> .....	<b>5</b>
<b>5 现网调研</b> .....	<b>10</b>
5.1 搬迁前网络测试.....	10
5.2 搬迁前工勘.....	10
5.3 搬迁前网规.....	11
5.4 现网信息收集.....	12
<b>6 搬迁评估分析和搬迁对策</b> .....	<b>14</b>
<b>7 搬迁方案和搬迁计划</b> .....	<b>16</b>
7.1 搬迁方案.....	16
7.2 搬迁策略.....	17
7.3 搬迁计划.....	17
7.4 回退计划.....	18
<b>8 搬迁实施</b> .....	<b>19</b>
8.1 硬件安装.....	19
8.2 现网配置分析和配置翻译.....	19
8.3 认证对接指导.....	19
8.4 第三方网管对接指导（SolarWinds）.....	19
8.4.1 SolarWinds 简介.....	19
8.4.2 适用的产品和版本.....	19
8.4.3 网络规划.....	20
8.4.4 添加设备.....	21
8.4.4.1 添加单个设备.....	21
8.4.4.2 添加自动发现的设备（批量添加）.....	27
8.4.5 管理设备.....	32
8.4.5.1 配置 SolarWinds NCM 管理设备使用的 SSH/Telnet 凭据.....	32
8.4.5.2 将设备添加到 SolarWinds NCM.....	34
8.4.5.3 下载设备的配置文件.....	35

8.4.5.4 日常备份设备的配置文件.....	36
8.4.5.5 上传配置文件至设备.....	38
8.4.5.6 上传配置变更至设备.....	39
8.4.5.7 比较设备配置文件之间的差异.....	40
8.4.6 日志和告警管理.....	41
8.4.6.1 查看设备上报的日志和告警.....	41
<b>9 搬迁后验收.....</b>	<b>43</b>
<b>10 搬迁实例.....</b>	<b>44</b>
10.1 搬迁项目概况.....	44
10.1.1 项目范围.....	44
10.1.2 搬迁计划.....	44
10.2 网络评估.....	45
10.2.1 搬迁前网络分析.....	45
10.2.1.1 网络拓扑结构.....	45
10.2.1.2 网规和工勘.....	46
10.2.1.3 业务模型.....	50
10.2.2 搬迁后网络分析.....	51
10.2.2.1 网络拓扑结构.....	51
10.2.2.2 端口前后映射表.....	56
10.2.3 风险分析和规避措施.....	57
10.3 搬迁前准备.....	57
10.3.1 搬迁申请.....	57
10.3.2 线缆布放和连接测试.....	57
10.3.3 硬件、软件和辅助材料准备.....	58
10.3.4 设备预配置.....	59
10.3.5 设备上电和功能测试.....	59
10.3.6 账号密码和远程登录.....	59
10.3.7 数据备份和流量采集.....	59
10.3.8 网络冻结.....	59
10.3.9 设备信息收集与测试.....	60
10.3.10 业务验证和测试.....	61
10.4 搬迁步骤.....	61
10.5 回退计划.....	63
10.6 搬迁后验收.....	64
10.7 现场支持计划.....	65

# 1 文档概述

企业的日常运营、办公、会议和交流等活动都离不开网络，园区网络是现代企业必不可缺的最重要的基础设施之一。园区网络的规模和功能存在差异，从园区网络建设的过程来看，存在以下特点：

- 园区网络是一个复杂的生态，是由多厂商的设备、终端和系统集成的结果，这些不同厂商的设备和系统共同构成了园区网络。
- 网络分为不同层级，每层功能不同，层级之间有交互关系，不同层级更新周期不一样。
- 大多数的园区网络通常是增量逐步建成的，园区网络会随着业务发展的需要不断地更新、扩容和融合。
- 网络设备生命周期不一样，不同的更新周期要求部分系统的更新，必然需要兼容周围的设备和系统。

技术上，新搬迁的网络设备需要满足客户的主要诉求：

- 原有功能和方案的继承
- 满足于现网环境互联互通及兼容性需求，包含终端设备、网络设备、管理系统和应用系统

基于上述特点，本文档提供了华为Wi-Fi 6搬迁替换场景下的交付指导，帮助网络工程师快速掌握搬迁替换的流程和方法，从而更好地对园区网络进行更新换代。

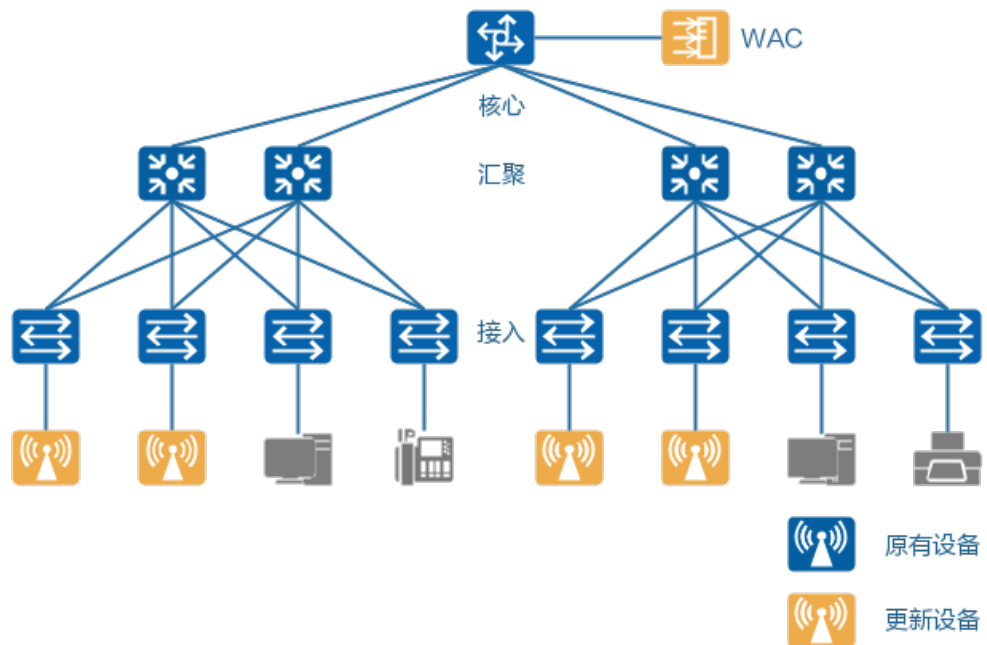
# 2 传统 WLAN 网络搬迁典型场景

现有传统WLAN网络的搬迁从场景上可以分为整体替换和局部替换：

- 无线网络整体替换

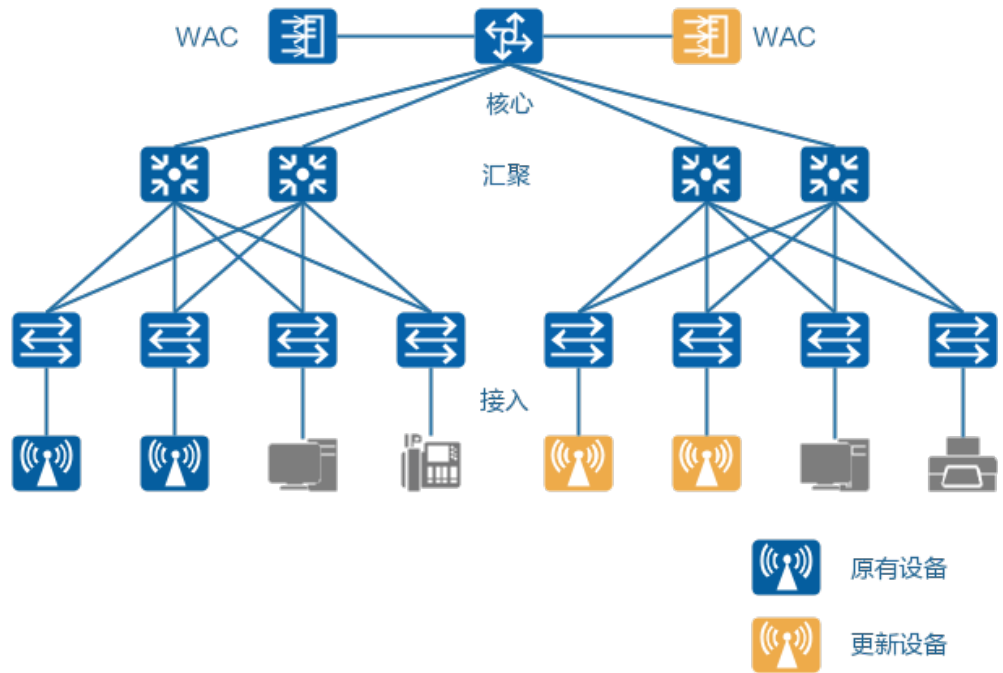
指的是WLAN网络整体替换，保持现有的有线网络，需要考虑搬迁后的WLAN网络与现有网络的兼容性。

主要针对现有WLAN网络中已经不适用于园区网络发展的需要，用户出于对网络容量、性能、安全性、可靠性、可维护性等维度更高的诉求，希望对当前的WLAN网络进行整体替换升级的场景。这种场景在园区网络比较集中或者规模比较小的情况下比较常见。



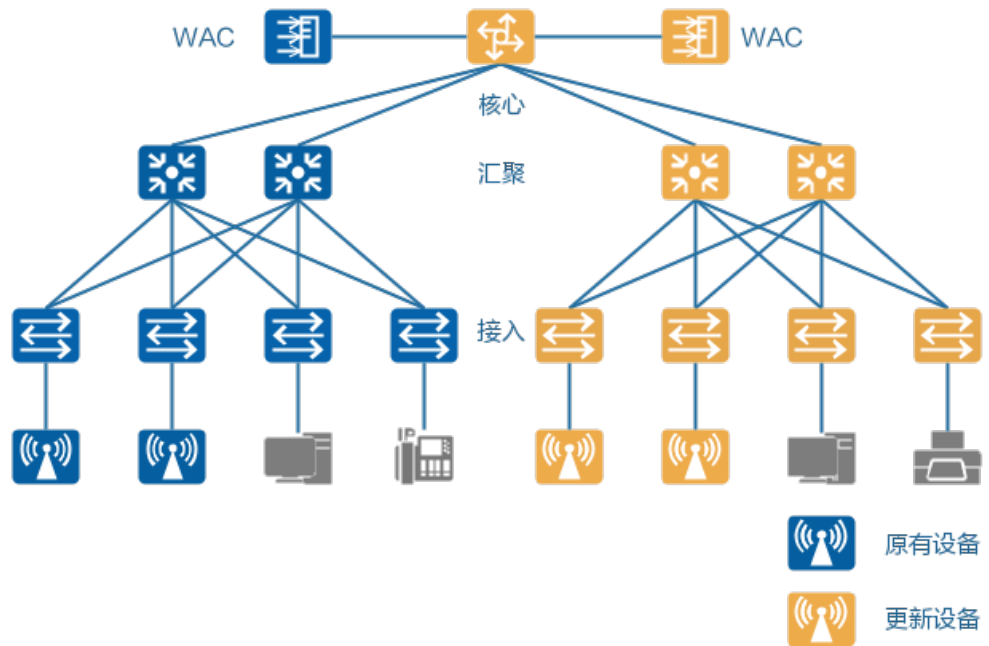
- 无线网络局部替换

指的是局部WLAN网络的替换更新，局部替换会存在多个WLAN设备并存的情况，不同的WLAN网络进行单独的配置、管理和运维，同样也是保持现有的有线网络。例如某大楼WLAN网络到期，用户计划引入新的WLAN厂商来逐步替换现有的WLAN厂商，进行WLAN网络的局部替换，到后续旧的WLAN网络到期后，就逐步切换到新的WLAN网络。



- 有线无线整网替换

指的是有线和无线网络的整体搬迁，这种场景既要考虑无线网络的兼容性，也要考虑有线网络的兼容性。



对于传统WLAN AC + FIT AP组网搬迁替换为云化管理组网的场景，请参考[WLAN AC 部署云化管理方案（公有云）操作指导](#)。

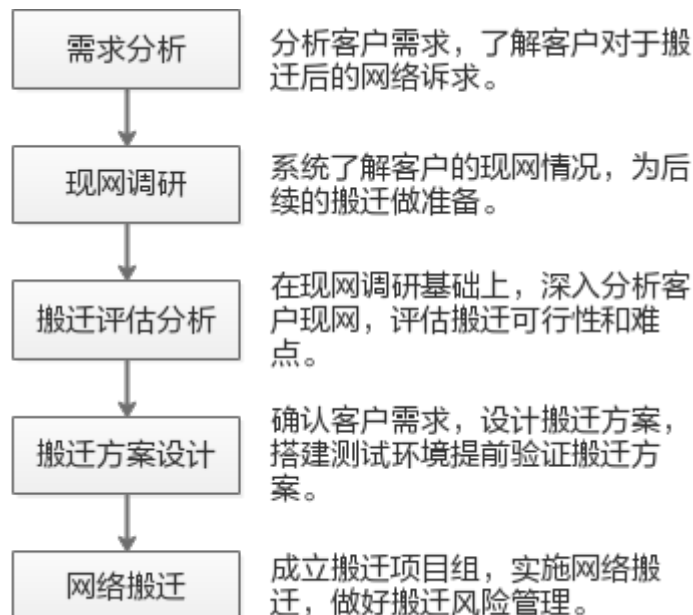
# 3 搬迁原则和搬迁思路

园区网络搬迁的一般原则如下：

- 减少网络架构变动
- 进行网络与设备解耦
- 对可以解耦的设备先进行替换
- 局部增加设备以实施新特性
- 对紧耦合部分最终一次性整体搬迁

对于传统的WLAN网络，由于AC和AP是配套使用的，所以AC和AP需要整体搬迁。整体的搬迁思路如图3-1所示。

图 3-1 搬迁思路





# 4 搬迁需求分析

搬迁替换类项目需求收集checklist如表4-1所示。

表 4-1 搬迁替换项目需求收集 Checklist

需求分类	目标	需求收集关注点	需求分析关注点
项目背景	确定交付责任	历史遗留问题	收集替换前现网维护历史问题，替换前先用CloudCampus APP参考 <a href="#">WLAN项目验收指导</a> 进行现网测试，输出搬迁前网络情况报告。
网络痛点	确定网络需要割接替换的原因	网络容量和性能：网络是否拥塞	确定网络带宽以及设备支持的802.11协议和并发用户数等规格。
		网络质量：业务经常中断，网络不稳定	需要考虑采用网管或网络分析软件，找出具体原因，并在方案设计时加以重点考虑，比如，可以考虑采用具有硬件OAM功能的产品。同时，需要根据客户所在的行业特色来分析其业务对网络质量的要求，以保证网络质量满足其业务要求。
网络环境	确定网络架构和设计方案	现网替换设备	<p>明确需要替换、保留和移除的设备。</p> <ul style="list-style-type: none"> <li>针对替换的设备，了解现网业务情况，用于新设备方案设计时参考。</li> <li>针对保留的设备，识别保留设备的型号及其对应版本，识别设备使用协议，评估新设备与保留设备的对接可行性。</li> <li>针对移除的设备，评估移除设备角色与功能，评估替换后设备配置正确性。</li> </ul>
		网络类型：有线网络、无线网络或者有线无线深度融合网络	<p>明确是否需要同时建设无线网络，是否需要建设成有线无线深度融合网络。</p> <p>如果需要统一认证，则推荐采用有线无线深度融合方案。</p>

需求分类	目标	需求收集关注点	需求分析关注点
		园区地理分布：集中或分散	初步确定基础网络架构，明确出口、骨干、核心、接入等网络层次规划。如果地理位置比较集中的话，考虑单核心架构；如果地理位置比较分散，如存在多栋大楼时，而且每个分布点的网络规格都比较大、各点之间的内部流量也比较大时，可能需要设置多个核心或汇聚。
		机房或网络设备弱电间分布情况	当机房或弱电间比较多时，通常可以将网络各层分布式部署到各个机房或弱电间，即将核心或汇聚部署到各个机房或弱电间，通常可以在每个机房或弱电间部署一个汇聚点；当采用多核心互联时，也可以将多核心分别部署在不同机房。除此之外，还要考虑设备摆放布局及其间隔距离等问题。
		网络环境	针对无线网络：确认室外场景还是室内场景，识别周边干扰因素（雷达、非Wi-Fi干扰等）。确认温度、湿度，有无抗震、防雷防电等特殊要求，明确AP工作环境。明确AP安装位置、摆放角度、接地条件、AP供电方式等。 针对有线网络：确认机房供电条件，散热条件，每个机架的供电能力。确认设备间距满足标准。确认替换设备与被替换设备的设备高度以保证机架有足够的空间。
		工勘网规方案	确认是否有明确的工勘网规方案，无线网络必须基于可靠的网规方案才能保障交付质量。
网络业务	确定网络带宽和业务特性	现网业务环境	现网运行的主要网络协议、网络拓扑和设备类型、数量、配置，了解现网网络质量及其对当前业务的支撑情况，了解现网网络设备表项条目（路由表、ARP表、MAC表），接口状态，供设计时参考。
		设备功能	出于各种原因，替换后的网络可能需要新增一些设备功能，需要确认是否需要部署MPLS/IPv6/NQA/随板AC/PPPoE等License控制项。
		常用业务类型：办公、E-mail、上网	正常的办公业务对网络带宽要求不高，通常4Mbps左右，普通的网络接入基本上就能满足要求。更具体的带宽要求可以参考Wi-Fi 6各场景下的建网标准。

需求分类	目标	需求收集关注点	需求分析关注点
		关键业务类型：数据、VoIP、视频、桌面云	通常园区网属于局域网，基本不用考虑网络时延问题；部署VoIP、视频和桌面云时如果涉及到分支、城域或广域类型的连接时，则需要重点考虑网络时延问题。另外，部署VoIP时需要考虑是与PC共网络，还是独立网络？是否需要PoE供电？这涉及到交换机的数量和规格。 如果需要部署桌面云，则需要重点考虑网络的可靠性或可用性。 如果有视频需求，则需要充分考虑带宽要求。
		多播业务类型	如果有，需要设计相应的多播/组播方案。
		需要特别关注的业务	识别重点业务需求，判断方案满足度、业务流量大小、业务走向、可靠性保护等，包括认证方案、组播业务、终端定位等。
		未来3~5年之内新增业务类型	网络需要考虑3~5年内业务发展的可能性，实现业务平滑升级和扩容，避免资源浪费或不能满足使用。
业务安全	确定业务隔离和网络安全防护建设方案。	业务安全：业务隔离与互通要求	网络业务是否需要隔离？如何隔离，物理隔离还是逻辑隔离？ 如果采用物理隔离，则相当于同时建设多张网，分别按照独立的网络进行设计即可；如果采用逻辑隔离，则需要采用VLAN/VPN等技术进行隔离，一张网承载多种业务，虚拟成多个园区网。 同时，还需要考虑不同业务之间是否存在互通要求。如果有，需要事先制定好互通策略和方案。
		网络安全：外部安全防护	主要需要考虑网络边界安全，需要部署防火墙、IPS/IDS、网络日志审计、防毒墙等安全设备。 如果对网络安全要求比较高，比如需满足安全等级保护要求，则推荐采用独立的安全设备；否则，可以采用集成安全设备如UTM或安全增值业务插卡。
		网络安全：内部安全防护	主要用于防止网络内部用户导致的安全事故，可以推荐采用上网行为管理的软件或专用设备。
		网络安全：终端安全防护	包括终端接入安全以及终端安全检查，确定是否需要采用终端NAC方案。

需求分类	目标	需求收集关注点	需求分析关注点
网络规模	确定网络架构与设计方案。	设备选型、设备版本、设备数量、用户规模	<p>针对无线网络：确定AC的规格和AP的数量，无线用户规模；特定新款型AP需关注与AC的版本配套满足度；在一些重点区域（如会议室）是否需要考虑高密度接入。</p> <p>针对有线网络：确认有线终端类型以及数量，有线用户数量。确认用户接入速率，接口类型。以此来确认交换机型号，数量。确认客户需要使用的交换机基本功能（堆叠、VLAN、路由协议）和高级功能（SVF、iPCA、用户认证授权和计费、业务随行、业务编排、零配置部署、策略联动等），确保网络方案能满足客户功能上，可靠性上的需求，以此确认交换机型号、版本。</p>
		3~5年后的网络规模，或最近几年的最高增长率	<p>网络设计要满足可扩展性要求，应当考虑园区网未来3~5年的发展需要，在设计时其网络接口、容量和带宽均需要有一定裕量，以便将来平滑扩容。</p> <p>网络规模既包括用户规模（即网络用户的数量或终端数量），也包括业务规模（业务的类型、带宽、数量及其使用范围）。</p>
		分支机构	<p>需要考虑分支与总部的连接方式。总部是否需要采用专线和互联网线路两类线路？是否需要线路备份？</p> <p>分支机构远程接入时要考虑业务应用场景，是个人移动办公远程接入，还是分支机构固定接入，从而确定采用SSL VPN还是IPsec VPN，或者两者都需要。</p>
终端类型	确定网络接入方案	终端类型：笔记本电脑、智能手机、移动智能设备PAD	需要考虑支持的接入频段（2.4G还是5G）和接入能力（802.11a/b/g/n/ac/ac Wave2/ax）
		终端认证计费方案	需要考虑接入认证模式，考虑是否采用有线无线统一认证。若涉及认证服务器，确认有无服务器冗余方案以及服务器并发性能需求；若涉及第三方认证服务器，确认产品名称及对应版本。
		终端接入权限	需要考虑是否允许访客接入以及访问区域。
		哑终端类：IP电话、网络打印机、IP摄像头等	需要考虑此类终端的接入和认证方案。
		其他/特殊类型的终端：如工业控制机、现场测控仪等	可能会影响接入交换机的选型，如工业园区/生产网可能会要求采用工业交换机、室外机构，可能会影响设备的供电方式。

需求分类	目标	需求收集关注点	需求分析关注点
		特殊的网络设备：如专用的网络加密设备、工业交换机等	主要考虑兼容性以及性能上的匹配，避免规格不一致。
第三方配套	识别兼容性风险	对接的周边产品信息及其版本信息	识别兼容性风险，包括第三方认证服务器、网管系统、安全监控平台、特殊行业终端等。
验收指标	明确验收指标	基于业务特性评估各项指标的最低验收指标	<p>针对无线网络：验收Ping包延迟、接入或认证成功、单用户或多用户性能等指标。</p> <p>针对有线网络：功能性验收，保证客户所有业务能正常运行；可靠性验收，保证单点故障情况下网络能快速恢复正常运行；性能验收，终端并发认证，话机通话效果，视频流畅不卡顿等。提前了解到客户认可的验收标准。</p>

# 5 现网调研

## 5.1 搬迁前网络测试

在搬迁前请务必对当前网络进行一轮测试，并输出测试报告，为后续的搬迁工作提供参考，以保证搬迁后的网络体验。

推荐使用CloudCampus APP进行测试：

1. 使用APP进行单点的网络体检，可以多选择几个点进行测试，收集信号强度、Wi-Fi干扰、Ping延时、互联网性能、网页连通性、AP关联等网络KPI指标。
2. 使用APP进行漫游测试与整网验收，并导出相关测试报告。
3. 分析网络指标KPI与测试报告，定位出存在问题的区域，供后续搬迁参考。

## 5.2 搬迁前工勘

向客户获取建筑图纸，按照[现场工勘](#)的要求对现场进行工勘，在工勘过程中需要重点收集以下信息：

- 检查实际环境中和图纸是否存在不一致的地方，尤其是障碍物和各种干扰。
- 检查机房或弱电间环境（如温度、湿度等）是否符合WAC、交换机等设备的工作环境要求。
- 检查接入交换机的安装位置，并检查PoE交换机或PoE电源能否满足AP供电标准。AP的供电需要满足其供电标准，如果供电不足，会导致AP性能下降或无法正常工作。AP支持的供电标准请查看[WLAN硬件安装与维护指南](#)中对应AP的基本参数。
- 检查线缆走线架或走线管路是否正常，并检查当前网络中光纤、网线等线缆资源是否满足网络调整。重点关注线缆的连通性和规格。连通性可以借助工具进行测试，如网线测试仪；网线规格则需要查看网线外皮上的标注，如CAT 5e表示超五类。

如果满足，则线缆可以利旧使用；如果不满足，则需要进行线缆改造或重新布放。一般情况下，5GE/10GE场景下，网线需要升级，需要重新布放网线；2.5GE及以下场景下，网线可以直接利旧。常见场景如下：

**场景1：**原点位直接升级Wi-Fi 6 AP，工作在1Gbps。



**场景2:** 升级2.5GE接入交换机和Wi-Fi 6 AP, 工作在2.5Gbps。



**场景3:** 升级10GE接入交换机、Wi-Fi 6 AP和网线, 工作在10Gbps。



- 在建筑图纸上标注现网AP的安装点位, 并检查AP的安装孔位是否可以利旧。室内放装型Wi-Fi 6 AP的新安装件可以兼容华为AP老安装件和部分友商安装件的安装孔位。如果可以利旧, 则可以减少现场打孔的时间和费用, 提升替换效率。

## 5.3 搬迁前网规

按照正常的网络升级的思路, 搬迁使用的AP的覆盖指标要优于现网的AP, 所以, 一般情况下, 推荐按照1:1原点位替换, 这样可以节省新增的走线改造、安装施工等费用。但是为了在搬迁前能够看到搬迁后的覆盖效果, 仍然有必要进行网规, 具体步骤如下:

1. 在华为网规工具WLAN Planner中导入建筑图纸, 按照当前AP的安装点位1:1替换成新AP。
2. 网规方案局部优化
  - a. 根据5.1 搬迁前网络测试中输出的测试报告, 针对问题区域进行专门优化, 包括AP点位调整与信道功率调优。
  - b. 根据需求分析结果, 关注是否有新频段的覆盖要求, 例如原本只要求2.4G频段, 搬迁后希望有5G信号覆盖。
3. 进行信号仿真渲染, 查看仿真效果并输出优化后的网规设计方案。

## 5.4 现网信息收集

在制定搬迁方案前，需要对当前WLAN网络情况进行摸底，尽可能多地收集现网信息。一方面作为后续制定搬迁方案的依据，另一方面根据现网信息提取排查可能存在的搬迁风险并制定改进措施。需要收集的现网信息请参考表5-1。

表 5-1 现网信息收集

信息类型	具体信息	关注点
客户基本信息	人员数量及结构	初步了解网络的规模，使用网络的人员分类，是否有需要重点关注的重要客户
	人员使用网络的主要方式	了解主要人员使用网络的方式
	主要网络应用	主要承载的网络应用类型
	园区网络结构，无线覆盖区域	了解网络主要覆盖场景，是否有需要重点覆盖的区域，与用户需求结合起来
网络拓扑及设备信息	网络拓扑结构和网络功能分区（比如接入，汇聚，核心，DMZ等）	<ul style="list-style-type: none"> <li>• 详细的网络拓扑图</li> <li>• 各分区之间以及各设备之间的连接关系，被替换的设备位于哪个位置</li> <li>• 网络规划数据：VLAN、IP地址、接口、路由等</li> </ul>
	网络拓扑中各设备信息（核心交换机、汇聚交换机、接入交换机、AC、AP等）	<ul style="list-style-type: none"> <li>• 设备型号、板卡型号、设备数量、软件版本、设备规格、设备上的配置文件等信息</li> <li>• 接入交换机的PoE供电标准</li> <li>• AP的安装点位</li> </ul>
	端口带宽和链路连接方式	客户带宽升级需求
网络连接	接入网络中的无线终端类型	不同终端对网络的需求，比如认证类型、PoE标准等
	网络采用的链路协议、路由协议	如果有私有协议，需要考虑协议对接或替换方案
	网络中是否有组播和IPv6的应用	搬迁设备对组播和IPv6的支持
网络策略	接入网络采用的认证方式（802.1X/MAC/Portal）	网络提供哪些认证方式
	是否提供访客接入功能	是否提供访客接入功能
	是否支持BYOD	是否支持BYOD



信息类型	具体信息	关注点
	防火墙的部署位置和安全策略	防火墙的型号和部署用途、防火墙策略
	网络中的主要业务、流量和QoS策略	网络QoS策略
网络管理	网络设备的管理方式和运维方式	使用了什么的网管软件，主要用途
	曾经出现的网络问题以及解决方法 网络故障排查的流程	如何对网络监控，监控软件是什么，网络排障工具
增值服务	网络中存在的增值功能（如网络导航，资产管理，广告推送，计费等） 以及对应的合作厂商	集成了哪些网络增值服务，具体的增值服务方案是怎样的

# 6 搬迁评估分析和搬迁对策

## 搬迁评估分析

在搬迁前进行端到端网络分析，对网络现网收集到的信息进行分析，定位搬迁难点，确定搬迁对策。

对于WLAN网络而言，需要重点关注的主要是如下内容：

- 终端层兼容性

终端层兼容性主要指的是各类通过WLAN接入网络的移动设备的兼容性，主要是无线终端的Wi-Fi协议兼容性和认证协议的兼容性。例如，有一些扫码枪要求支持PPSK认证方式。

华为WLAN产品的终端兼容性请参考[华为WLAN产品终端兼容性测试报告](#)。根据现网调研时收集的无线终端信息，对比测试报告中的终端，确认是否存在不兼容的无线终端。

- 网络层兼容性

网络层兼容性主要指的是通信协议层面的互联互通能力，例如，AC和AP之间中间网络设备上的MTU值；物理层PoE供电能力，例如，接入交换机需要满足AP的PoE供电标准。

对于WLAN网络，网络层的兼容性需要重点评估的是AC和AP之间的中间网络以及接入交换机的PoE供电能力。

- 应用层兼容性

- 认证系统兼容性

主要涉及认证服务器的兼容能力，例如Cisco的ISE、Aruba的ClearPass。需要重点考虑替换后的WLAN网络与现网中NAC系统的集成，包括AAA服务、各类认证方式等。例如，MAC认证、Portal认证和802.1X认证。

华为WLAN产品的认证服务器兼容性请参考[华为WLAN产品认证服务器互通测试报告](#)。

- 网管系统兼容性

主要涉及第三网管系统的兼容能力，例如Solarwinds等。需要重点考虑替换后的WLAN设备能否被现有的网管系统纳管。

- 增值系统兼容性

包括各种增值业务系统的兼容能力，包括AD、LBS、行业应用等等。需要考虑替换后的WLAN网络与增值业务系统的集成。

更多互联互通相关的信息请参见：[互联互通测试报告](#)。

## 搬迁注意事项

在进行搬迁评估时还需要关注如下搬迁注意事项：

- 对于旧AP是吸顶安装的场景，需要注意AP的选型，AirEngine 5760-22W和AirEngine 5760-22WD不支持吸顶安装方式。如果是原点位替换，建议使用其他AP型号；否则，需要将AP的安装方式改造为挂墙安装方式或暗盒安装方式。
- 不同AP的PoE供电标准是不一样的，如果是原点位替换，需要确保当前的供电标准符合新AP的供电要求。

## 搬迁对策

根据现网调研收集的现网信息，在搬迁前提前搭建镜像环境，根据搬迁评估分析出的搬迁难点，提前进行验证，确认搬迁后的设备与现网中的网络设备和无线终端之间是否存在不兼容的情况。

对于部分不兼容的情况，以下提供了相应的搬迁对策：

- 终端不兼容：可以尝试更新无线终端的网卡驱动，目前已经发现部分Intel网卡无法接入802.11ax协议的AP，华为公司已经发布预警并提供了解决方案：[【ENW-P-C-2019111】关于Intel部分无线网卡无法接入11ax协议AP问题的预警](#)。
- PoE标准不兼容：如果现网中的接入交换机无法满足新AP的PoE供电标准，则需要考虑同步替换合适的接入交换机或采用新AP支持的其他供电方式，如PoE电源适配器。
- NAC/网管系统不兼容：可以与客户协商同步搬迁NAC系统和网管系统，例如，使用华为公司的SDN控制器来提供NAC功能，使用华为公司的CampusInsight作为网管系统。

# 7 搬迁方案和搬迁计划

---

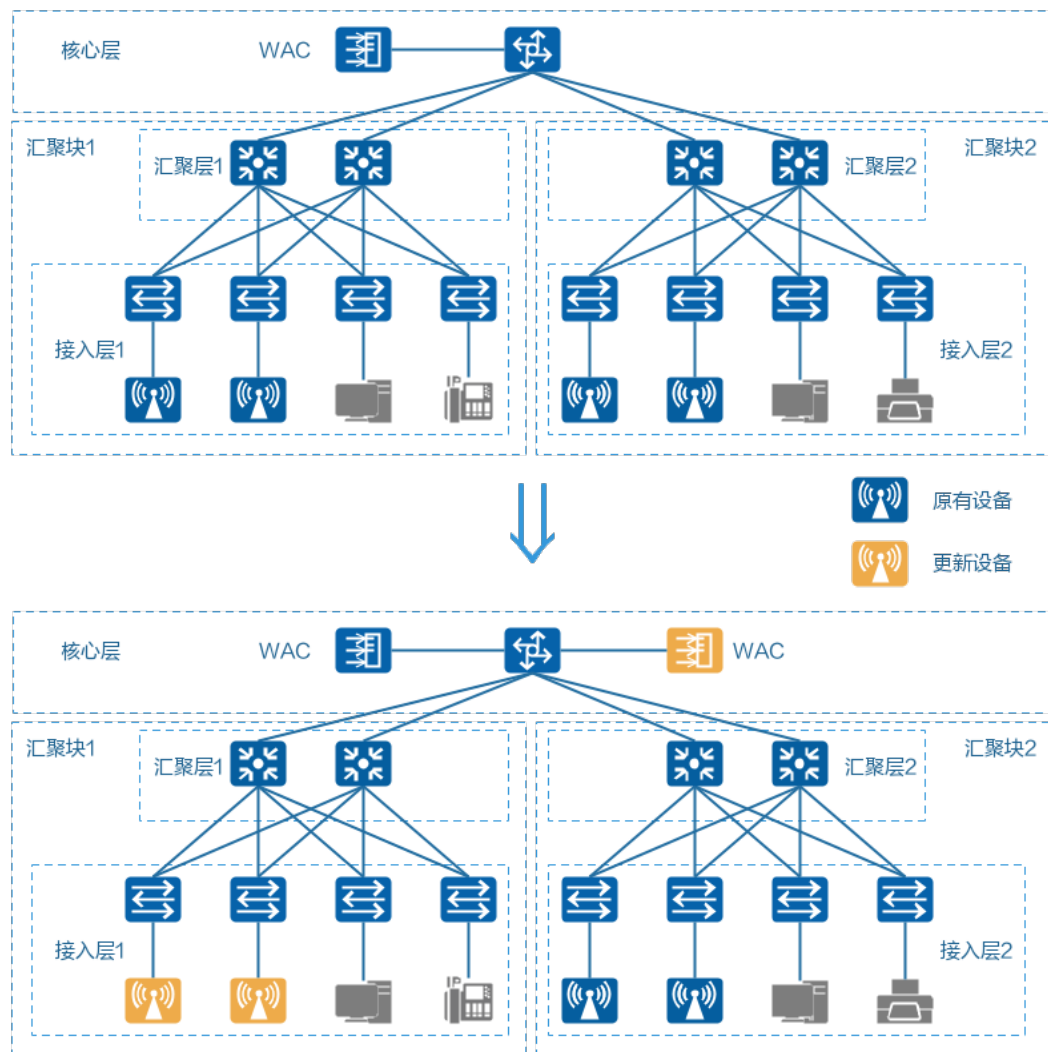
## 7.1 搬迁方案

WLAN网络的搬迁方案如图7-1所示，以汇聚块为单元（考虑物理位置在一起的AP，例如同楼层、同大楼的AP），将同区域的AP整体进行搬迁，逐个汇聚块进行替换，最终实现全部替换。

按照这个搬迁方案，WLAN网络搬迁的基本流程如下：

1. WAC上线，推荐以旁挂方式组网，旁挂组网能最大程度地降低网络改造成本。
2. 替换汇聚块1下的AP。
3. 在WAC上配置AP上线、WLAN业务以及WAC和NAC系统对接。
4. 逐步替换其他汇聚块下的AP。
5. 被替换的无线控制器下线。

图 7-1 WLAN 网络搬迁方案



## 7.2 搬迁策略

搬迁策略需要根据客户的要求进行定制，一般分为以下几种情况：

- 搬迁过程中不影响正常的办公业务。  
这种情况下，需要参考搬迁方案分区域、分时段（如非办公时间段）进行搬迁。
- 整网替换，直接拆除旧设备，全新部署新网络。  
这种情况下，搬迁难度相对较小，建议按照搬迁方案有序地进行搬迁。

## 7.3 搬迁计划

在和客户明确了搬迁方案和策略后，需要和客户一起制定搬迁计划。

1. 与客户共同制定搬迁顺序和搬迁时间。
2. 按搬迁顺序制定基于区域的搬迁时间计划表，确保物料准备时间。
3. 例行和客户沟通搬迁进展，共享搬迁信息，确保客户能够配合进行项目推进。

## 7.4 回退计划

搬迁前需要制定好回退计划，针对搬迁过程中的每一个步骤出现失败情况提供处理方法。根据迁移计划的规模、重要性和复杂性，对迁移计划进行调整。同时，需要考虑故障的处理时间，并纳入计划。每一步执行完成后，确认结果并填写备注。

在风险分析阶段，对搬迁阶段高风险步骤进行优先级排序，在制定回退计划时针对这些关键步骤制定回退计划。

动作	操作步骤	预期结果及验证方法	结果确认
.....	.....	.....	.....

# 8 搬迁实施

## 8.1 硬件安装

按照搬迁方案和搬迁计划进行WLAN设备安装，安装指导请参见[WLAN 硬件安装与维护指南](#)。

## 8.2 现网配置分析和配置翻译

对现网调研时收集的配置文件进行配置分析，以确认搬迁后是否会导致功能丢失。

对于搬迁其他WLAN厂商的情况，建议获取对应厂商的产品文档和[企业网络配置翻译工具](#)对现网配置进行翻译，从而将第三方设备的配置文件转换为华为设备的配置文件。

对于华为WLAN旧网升级改造，则需要对比升级前后的功能差异，如Wi-Fi 5 AP和Wi-Fi 6 AP之间的功能差异。

## 8.3 认证对接指导

WLAN产品和Huawei Agile Controller-Campus服务器以及第三方认证服务器的对接指导请参考[WLAN产品对接配置专题](#)。

## 8.4 第三方网管对接指导（SolarWinds）

### 8.4.1 SolarWinds 简介

SolarWinds是一个网络管理软件，能够对各类规模的企业网络进行配置、管理、监控、维护和故障排查。

### 8.4.2 适用的产品和版本

本文档适用于所有支持SNMP和Telnet协议的华为S系列交换机、CloudEngine数据中心交换机、AR路由器、WLAN产品和USG防火墙。

本文档仅以S系列交换机为例，向您展示华为企业数通产品能够很好地与SolarWinds对接、被SolarWinds管理并提供部分功能的对接配置指导。

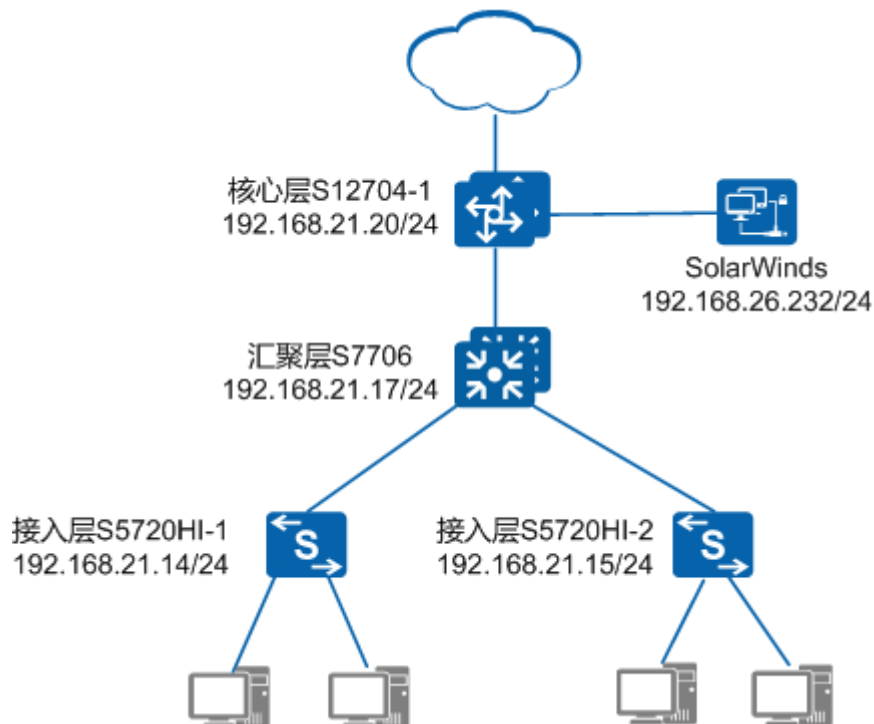
### 8.4.3 网络规划

#### 说明

- 本文档基于实验室环境写作，组网及数据规划仅为示例，应用时请以实际需求为基础进行网络规划。
- 本文档仅提供S系列交换机与SolarWinds对接相应功能的核心配置，网络基础数据如VLAN、IP地址和路由等配置均不再体现，应用时请根据实际的数据规划进行配置。
- 本文档使用的SolarWinds Orion Platform的版本为2016.2.100，NCM的版本为7.5.1。

#### 组网规划

图 8-1 华为 S 系列交换机与 SolarWinds 对接指导组网





## 数据规划

表 8-1 SNMP 和 Telnet 数据规划

项目	数据
SNMP	<ul style="list-style-type: none"> <li>• SNMP版本: SNMPv2c</li> <li>• SNMP读写团体名: Huawei@2018</li> <li>• 上送告警的目的主机: 192.168.26.232</li> <li>• SNMP告警开关: 打开所有模块的SNMP告警开关, 则所有模块的告警都会上报给SolarWinds</li> </ul>
Telnet	<ul style="list-style-type: none"> <li>• 认证方式: AAA, 即用户名+密码的认证方式</li> <li>• 用户名: huawei</li> <li>• 密码: Huawei@123</li> <li>• 用户级别: 15</li> </ul>

## 8.4.4 添加设备

### 8.4.4.1 添加单个设备

#### 配置思路

1. 配置华为S系列交换机:
  - a. 配置SNMP参数, 确保SolarWinds能使用这些参数与交换机进行通信。
  - b. 配置Telnet参数, 确保SolarWinds能使用这些参数登录交换机。
2. 在SolarWinds上添加单个设备。

#### 操作步骤

**步骤1** 配置华为S系列交换机。操作步骤仅以S系列交换机为例, 其他产品的配置请参见[配置文件](#)。

1. 配置SNMP参数。

```
<HUAWEI> system-view
[HUAWEI] sysname S5720HI-1
[S5720HI-1] snmp-agent sys-info version v2c //允许SolarWinds使用SNMPv2c协议与交换机进行通信
[S5720HI-1] snmp-agent community write cipher Huawei@2018 //配置SNMPv2c团体名为Huawei@2018
[S5720HI-1] snmp-agent trap enable //打开所有模块的SNMP告警开关, 则所有模块的告警都会上报给SolarWinds
Warning: All switches of SNMP trap/notification will be open. Continue? [Y/N]:y
[S5720HI-1] snmp-agent target-host trap address udp-domain 192.168.26.232 params securityname cipher Huawei@2018 //配置交换机上报告警给SolarWinds
```

## 📖 说明

您可以执行 `display snmp-agent trap [ feature-name feature-name ] all` 命令查看指定或所有模块的SNMP告警开关状态。如果您仅希望将指定模块的告警上送给SolarWinds，不需要执行 `snmp-agent trap enable` 命令，执行 `snmp-agent trap enable feature-name feature-name [ trap-name trap-name ]` 命令打开指定模块的SNMP告警开关即可。

### 2. 配置Telnet参数。

```
[S5720HI-1] user-interface maximum-vty 15 //配置能够远程登录交换机的最大用户数
[S5720HI-1] user-interface vty 0 14
[S5720HI-1-ui-vty0-14] authentication-mode aaa //配置用户的认证方式为AAA认证，即用户名+密码的认证方式
[S5720HI-1-ui-vty0-14] protocol inbound telnet //允许SolarWinds使用Telnet协议登录华为S系列交换机
[S5720HI-1-ui-vty0-14] quit
[S5720HI-1] aaa
[S5720HI-1-aaa] local-user huawei password cipher Huawei@123 //配置用户名和密码
[S5720HI-1-aaa] local-user huawei privilege level 15 //配置用户的级别为15级（最高级）
[S5720HI-1-aaa] local-user huawei service-type telnet //允许该用户使用Telnet协议登录设备
[S5720HI-1-aaa] quit
```

## 步骤2 在SolarWinds上添加单个设备（节点）。

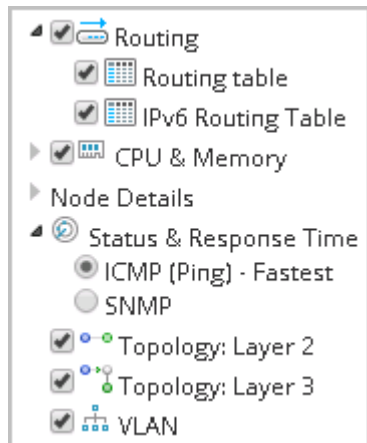
1. 通过管理员账号登录SolarWinds。
2. 单击“SETTINGS > Manage Nodes”，然后单击“ADD NODE”。
3. 在“DEFINE NODE”页签下定义节点信息。
  - a. 提供节点名称或IP地址。

- b. 选择轮询方法，并指定相应的参数。您可以单击“TEST”检查SolarWinds是否能够通过该方法与节点进行通信，完成后单击“Next”。

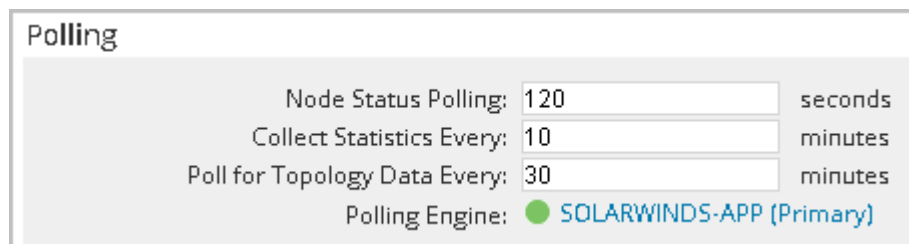
## 📖 说明

SolarWinds上指定的SNMP参数，必须与华为S系列交换机的配置的SNMP参数一致，否则二者无法通信。

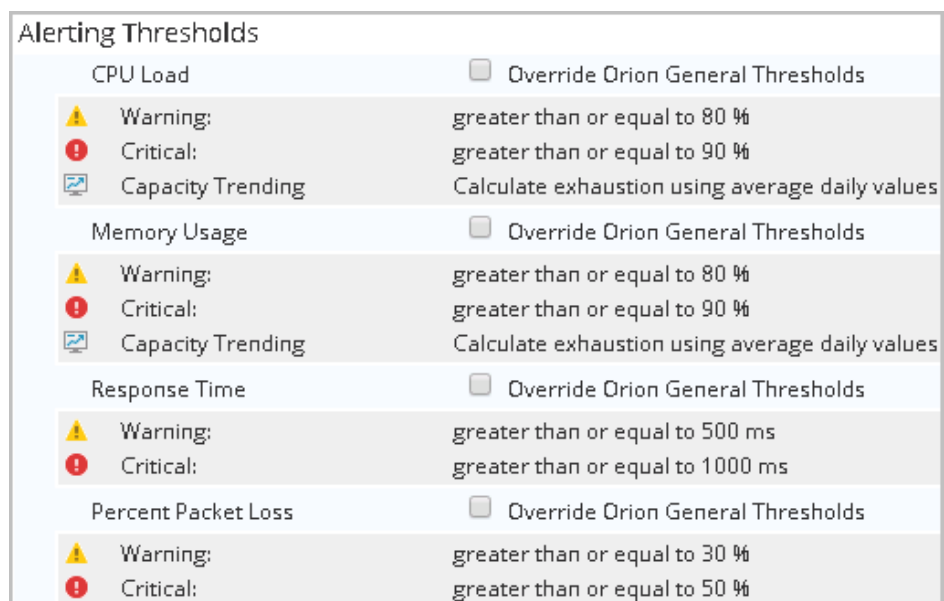
4. 在“CHOOSE RESOURCES”页签下选择需要监控的统计信息和资源，然后单击“Next”。



5. 如需调整“ADD POLLERS”页签下的配置，请参考SolarWinds的产品文档，此处不再介绍。
6. 在“CHANGE PROPERTIES”页签下预览并调整节点的属性。
- 如需编辑更新节点状态、监控统计信息或拓扑详细信息的频率，请更改**Polling**区域的数值。



- 如需调整节点状态何时更改为**Warning**或**Critical**，请选择相应度量标准的“Override Orion General Thresholds”，并调整其警报阈值。



- 将节点添加至SolarWinds NCM。下拉至“Manage Node(s) with NCM”，如需通过SolarWinds NCM管理该节点（如配置备份和恢复），请选择**Yes**。添加新的凭据模板或选择已有的凭据模板均可，但请确保“Connection

Profile”中的凭据必须与华为S系列交换机上配置的SSH/Telnet参数一致，否则您将无法通过SolarWinds NCM对其进行管理，您可以单击“TEST”进行测试。

- d. 单击“OK, ADD NODE”完成节点添加。您可以在节点列表中看到该节点的“Status”为“Node status is Up。”。

Name	Polling IP Address	Status
AC6005_14_3	192.168.14.3	Node status is Up.
S5720HI-1	192.168.21.14	Node status is Up.

----结束

## 配置文件

- S系列交换机的配置文件

```
#
sysname S5720HI-1
#
aaa
local-user huawei password irreversible-cipher $1a$hg'4WjC):$#8{[]XH!m3FS2>/)s1ft<iM*
\&cWHv6m3ab0^z8|l$
local-user huawei privilege level 15
local-user huawei service-type telnet
#
snmp-agent
snmp-agent community write cipher %^%#77G5T7GZy@/wk^B^P.+P5y7G%=^1!3:|qFg|/K,z#[\!
i&@*!a]pCG$Ms!+bZ>M-i/Wv>".E-Hh6ujM%^%#
snmp-agent sys-info version v2c
snmp-agent target-host trap address udp-domain 192.168.26.232 params securityname cipher %^
```

```

%#qvV,Vaw-Q*,'D=U!6+Fw>'N'Loa/JnZB{~r1}};%^%#
snmp-agent trap enable
#
user-interface maximum-vty 15
user-interface vty 0 14
authentication-mode aaa
user privilege level 15
protocol inbound telnet
#
return

```

- CloudEngine数据中心交换机的配置文件

```

#
sysname CE6850HI
#
aaa
local-user huawei password irreversible-cipher $1c$S.^kQy$PAP$5TfM6r!
Go#a#0%D#C6MDvG]BQYdGG6Um\t4)CkB.$ //密码为用户@123
local-user huawei service-type telnet
local-user huawei level 3
#
snmp-agent
snmp-agent local-engineid 800007DB03200BC7391301
snmp-agent community write cipher %^%#[R95"jd3)"=FB).{guT7-:cqN`Tq1"yIzIj/
qPj8OpE5N{O'tSkMbUAR}hi3*P3{+\h`RUakPdE9iT3J%|^%#
#
snmp-agent sys-info version v2c v3
snmp-agent target-host host-name __targetHost_1_60298 trap address udp-domain 192.168.26.232
params securityname cipher %^%#O{/W5F7cHF}3s8Vbc{5}q7]j4]6b#7NG=JU.P[\%^%|^%#
#
snmp-agent trap enable
#
user-interface maximum-vty 15
#
user-interface con 0
#
user-interface vty 0 14
authentication-mode aaa
user privilege level 3
protocol inbound telnet
#
return

```

- AR路由器的配置文件

```

#
sysname Router
#
telnet server enable
#
interface GigabitEthernet1/0/0 #与网管对接的接口
ip address 192.168.21.24 255.255.255.0
#
user-interface maximum-vty 15
user-interface vty 0 14
authentication-mode aaa
user privilege level 15
protocol inbound telnet
#
aaa
local-user huawei password irreversible-cipher $1a$K7'+1lo)-X$Mh.V(YGta6Qk%E&Z8
UG9j2A|~y"8R-!!T9#)`vn2$
local-user huawei privilege level 15
local-user huawei service-type telnet
#
snmp-agent community write %^%#BV]UGa7[MWAN9!;_AN66"=:1AcEy$Fj,rInWd`Y-@mr-lhk
]X(aQ_"E&+S3#ss8:!\_%4EkVJFP+`Q#%^%#
snmp-agent sys-info version v2c
snmp-agent target-host trap-hostname inform address 192.168.26.232 udp-port 162 trap-
paramsname abc
snmp-agent target-host trap-paramsname abc v2c securityname %^%#/-eY4+a4.@SI%->

```

```

+$YSV@qY1'_jm50u%S10w|\9,%^%#
snmp-agent trap enable
snmp-agent
#
return

```

- WAC/FAT AP产品的配置文件

```

#
aaa
local-user huawei password irreversible-cipher $1a$I>iICGZu^N$.9O{<rZ<0,,5uyKo"VCCnLld:KshSIZ
%Po)|^kqM$
local-user huawei privilege level 15
local-user huawei service-type telnet
#
snmp-agent community write %^%#s`lfQ5XRiMW`gQVRnCo'F[x$-h0XxLI&%,#p(8CH[<IO-[6:6;${>tR
\}."<tx_78Q6b]JWf.KVU!Q<%^%#
snmp-agent sys-info version v2c
snmp-agent target-host trap-hostname snmp address 192.168.26.232 udp-port 162 trap-
paramsname huawei
snmp-agent target-host trap-paramsname huawei v2c securityname %^%#Rxc\w<:GW]"G\K
\}n<VcW:l8hUa.JCaxh+tfaPM%^%#
snmp-agent trap enable
snmp-agent
#
telnet server enable
#
user-interface maximum-vty 5
user-interface vty 0 4
authentication-mode aaa
protocol inbound telnet
#

```

- USG防火墙的配置文件

```

#
telnet server enable
#
interface GigabitEthernet1/0/3 #与网管对接的接口
undo shutdown
ip address 192.168.26.22 255.255.255.0
service-manage enable
service-manage telnet permit
service-manage snmp permit
#
user-interface vty 0 4
authentication-mode aaa
protocol inbound telnet
user privilege level 15
idle-timeout 5
#
aaa
authentication-scheme default
#
manager-user huawei
password cipher $1a$"hg'4WjC):$#8[]XH!m3FS2>/)s1ft<iM*\&cWHV6m3ab0^z8|I$
service-type telnet
level 15
#
firewall zone trust
set priority 85
add interface GigabitEthernet1/0/3
#
snmp-agent
snmp-agent community write cipher %^%#77G5T7GZy@/wk^B^P.+P5y7G%=^1!3:_|qFg|/K,z#[\!
i&@*|a]pCG$Ms!+bz>M-i/Wv>".E-Hh6ujM%^%# mib-view mib2view
snmp-agent sys-info version v2c
snmp-agent target-host inform address udp-domain 192.168.26.232 params securityname cipher %^
%#qvV,Vaw-Q*,'D=U!6+Fw>'N'Loa/JnZB{~r1}};%^%# v2c
snmp-agent mib-view included mib2view system
snmp-agent trap enable

```

```
#
return
```

## 8.4.4.2 添加自动发现的设备（批量添加）

### 配置思路

1. 配置华为S系列交换机：
  - a. 配置SNMP参数，确保SolarWinds能使用这些参数与交换机进行通信。
  - b. 配置Telnet参数，确保SolarWinds能使用这些参数登录交换机。
2. 配置SolarWinds自动发现网络中的设备。
3. 添加自动发现的设备。

### 操作步骤

**步骤1** 配置华为S系列交换机。操作步骤仅以S系列交换机为例，其他产品的配置请参见[配置文件](#)。

1. 配置SNMP参数。

```
<HUAWEI> system-view
[HUAWEI] sysname S5720HI-1
[S5720HI-1] snmp-agent sys-info version v2c //允许SolarWinds使用SNMPv2c协议与交换机进行通信
[S5720HI-1] snmp-agent community write cipher Huawei@2018 //配置SNMPv2c团体名为
Huawei@2018
[S5720HI-1] snmp-agent trap enable //打开所有模块的SNMP告警开关，则所有模块的告警都会上报
给SolarWinds
Warning: All switches of SNMP trap/notification will be open. Continue? [Y/N]:y
[S5720HI-1] snmp-agent target-host trap address udp-domain 192.168.26.232 params
securityname cipher Huawei@2018 //配置交换机上报告警给SolarWinds
```

#### 说明

您可以执行**display snmp-agent trap [ feature-name feature-name ] all**命令查看指定或所有模块的SNMP告警开关状态。如果您仅希望将指定模块的告警上送给SolarWinds，不需要执行**snmp-agent trap enable**命令，执行**snmp-agent trap enable feature-name feature-name [ trap-name trap-name ]**命令打开指定模块的SNMP告警开关即可。

2. 配置Telnet参数。

```
[S5720HI-1] user-interface maximum-vty 15 //配置能够远程登录交换机的最大用户数
[S5720HI-1] user-interface vty 0 14
[S5720HI-1-ui-vty0-14] authentication-mode aaa //配置用户的认证方式为AAA认证，即用户名+密码
的认证方式
[S5720HI-1-ui-vty0-14] protocol inbound telnet //允许SolarWinds使用Telnet协议登录华为S系列交换
机
[S5720HI-1-ui-vty0-14] quit
[S5720HI-1] aaa
[S5720HI-1-aaa] local-user huawei password cipher Huawei@123 //配置用户名和密码
[S5720HI-1-aaa] local-user huawei privilege level 15 //配置用户的级别为15级（最高级）
[S5720HI-1-aaa] local-user huawei service-type telnet //允许该用户使用Telnet协议登录设备
[S5720HI-1-aaa] quit
```

**步骤2** 配置SolarWinds自动发现网络中的设备。

1. 通过管理员账号登录SolarWinds。
2. 单击“SETTINGS > Network Discovery”，单击“Add New Discovery”，然后单击“START”。
3. 在“NETWORK”页签下指定网段或IP地址，单击“NEXT”。

<b>IP RANGES</b>	<b>Start address:</b> 192.168.21.10	<b>End address:</b> 192.168.21.20	
	+ Add Range		
<b>SUBNETS</b>	+ Add ▾		
<b>IP ADDRESSES</b> ⓘ	+ Add IP Address		

- 如需调整“AGENTS”和“VIRTUALIZATION”页签下的配置，请参考SolarWinds的产品文档，此处不再介绍。
- 将设备添加至SolarWinds NCM。如需要通过SolarWinds NCM管理设备，如配置备份和恢复，您需要在“CONFIG MANAGEMENT”页签下添加SSH/Telnet凭据。单击“Add SSH/Telnet Credentials”添加新的凭据模板或选择已有的凭据模板均可，但请确保该凭据与华为S系列交换机上配置的SSH/Telnet参数一致，否则您将无法通过SolarWinds NCM对其进行管理。此处以添加新的凭据模板为例，完成后单击“ADD”，然后单击“NEXT”。

### Add New Connection Profile

**Profile Name:**  
HUAWEI LSW

**CLI Login/User Name:**  
huawei

**CLI Password:**  
\*\*\*\*\*

**Enable Level:** ⓘ  
<No Enable Login> ▾

**Enable Password**  
\_\_\_\_\_

**Execute Commands and Scripts Using:**  
TELNET ▾

**Request Config Files Using:**  
TELNET ▾

**Transfer Config Files Using:**  
TELNET ▾

**Telnet Port:**  
23

**SSH Port:**  
22

Automatically test this profile against monitored nodes that allowed it. ⓘ



- 在“SNMP”页签下添加SNMP凭据，请确保该凭据与华为S系列交换机上配置的SNMP参数一致，否则SolarWinds与华为S系列交换机之间将无法通过SNMP进行通信，完成后单击“NEXT”。



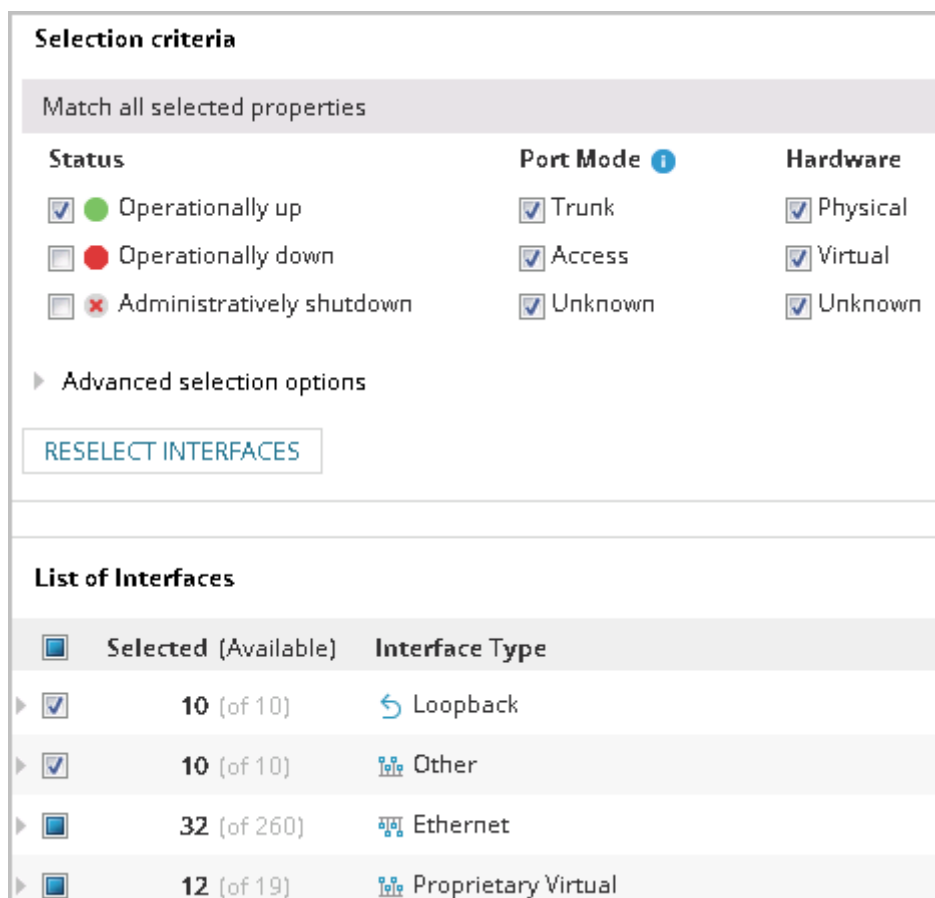
- 如需调整“WINDOWS”、“MONITORING SETTINGS”和“DISCOVERY SETTINGS”页签下的配置，请参考SolarWinds的产品文档，此处不再介绍。
- 在“DISCOVERY SCHEDULING”页签下调整自动发现的频率及执行时间，完成后单击“DISCOVER”开始发现网络中的设备。

### 步骤3 添加自动发现的设备。

- 单击“NEXT”。

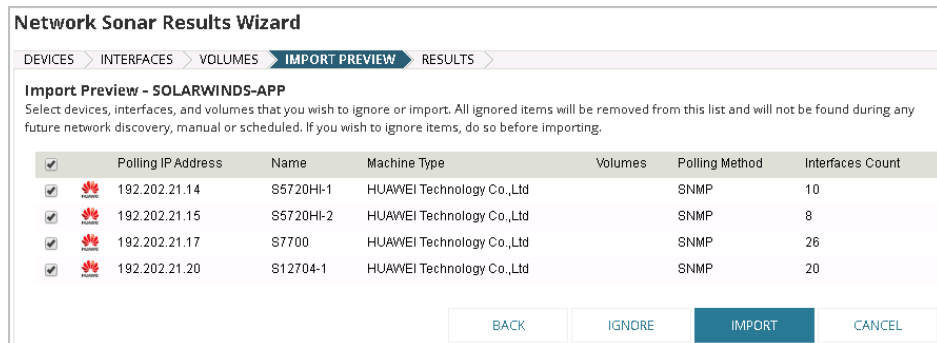


- 在“INTERFACES”页签下选择需要监控的接口，单击“NEXT”。

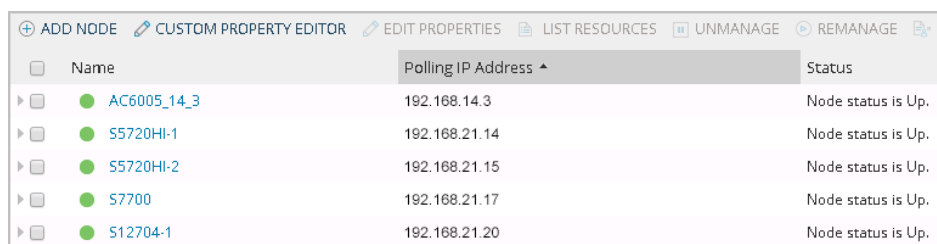


- 如需调整“VOLUMES”页签下的配置，请参考SolarWinds的产品文档，此处不再介绍。

4. 选择需要添加的设备，单击“IMPORT”，然后单击“FINISH”。



5. 单击“SETTINGS > Manage Nodes”，可以发现自动发现的设备已添加成功，且“Status”均为“Node status is Up。”



----结束

## 配置文件

- S系列交换机的配置文件

```
#
sysname S5720HI-1
#
aaa
local-user huawei password irreversible-cipher $1a$hg'4WjC):$#8[]XH!m3FS2>/)s1ft<iM*
\&cWHv6m3ab0^z8|$
local-user huawei privilege level 15
local-user huawei service-type telnet
#
snmp-agent
snmp-agent community write cipher %^%#77G5T7GZy@/wk^B^P.+P5y7G%=^1!3:|qFg|/K,z#[!
i&@*!a]pCG$Ms!+bZ>M-i/Wv>".E-Hh6ujM%^%#
snmp-agent sys-info version v2c
snmp-agent target-host trap address udp-domain 192.168.26.232 params securityname cipher %^
%#qvV, Vaw-Q*,='D=U!6+Fw>'N'Loa/JnZB{~r1}};%^%#
snmp-agent trap enable
#
user-interface maximum-vty 15
user-interface vty 0 14
authentication-mode aaa
user privilege level 15
protocol inbound telnet
#
return
```

- CloudEngine数据中心交换机的配置文件

```
#
sysname CE6850HI
#
aaa
local-user huawei password irreversible-cipher $1c$S.^kQy$PAP$5TfM6r!
Go#a#0%D#C6MDvG]BQYdGG6Um{t4}CkB.$ //密码为用户@123
local-user huawei service-type telnet
local-user huawei level 3
```

```
#
snmp-agent
snmp-agent local-engineid 800007DB03200BC7391301
snmp-agent community write cipher %^%#[R95"jd3]"=FB).{guT7-:cqN`Tq1"yIZil/
qPj8OpE5N{O'tSkMbUAR}hi3*P3{+\h`RUakPdE9iT3J%^%#
#
snmp-agent sys-info version v2c v3
snmp-agent target-host host-name __targetHost_1_60298 trap address udp-domain 192.168.26.232
params securityname cipher %^%#O{/W5F7cHF}3s8VBc{5}q7}j4}6b#7NG=JU.P[\%^%#
#
snmp-agent trap enable
#
user-interface maximum-vty 15
#
user-interface con 0
#
user-interface vty 0 14
authentication-mode aaa
user privilege level 3
protocol inbound telnet
#
return
```

- AR路由器的配置文件

```
#
sysname Router
#
telnet server enable
#
interface GigabitEthernet1/0/0      #与网管对接的接口
ip address 192.168.21.24 255.255.255.0
#
user-interface maximum-vty 15
user-interface vty 0 14
authentication-mode aaa
user privilege level 15
protocol inbound telnet
#
aaa
local-user huawei password irreversible-cipher $1a$K7`+1lo)-X$Mh.V(YGTa6Qk%E&Z8
UG9j2A|~y"8R-!!T9#)`vn2$
local-user huawei privilege level 15
local-user huawei service-type telnet
#
snmp-agent community write %^%#BV]UGa7[MWAN9!;_:AN66":=1AcEy$Fj,rInWd`Y-@mr-lhk
]X(aQ_"E&+S3#ss8:!\_%4EkVJFP+`Q#%^%#
snmp-agent sys-info version v2c
snmp-agent target-host trap-hostname inform address 192.168.26.232 udp-port 162 trap-
paramsname abc
snmp-agent target-host trap-paramsname abc v2c securityname %^%#/-eY4+a4.@SI%->
+$YSV@qY1'_jm50u%S10w|\9,%^%#
snmp-agent trap enable
snmp-agent
#
return
```

- WAC/FAT AP产品的配置文件

```
#
aaa
local-user huawei password irreversible-cipher $1a$!>iICGZu^N$.9O{<rZ<0,,5uyKo"VCCnLld:KshS!Z
%Po)|^kqM$
local-user huawei privilege level 15
local-user huawei service-type telnet
#
snmp-agent community write %^%#s`IfQ5XRiMW`gQVRnCo'F[x$-h0XxLI&%,#p(8CH[<IO-[6:6;${>tR
\]."<tx_78Q6b[JWf.KVU!Q<%^%#
snmp-agent sys-info version v2c
snmp-agent target-host trap-hostname snmp address 192.168.26.232 udp-port 162 trap-
paramsname huawei
snmp-agent target-host trap-paramsname huawei v2c securityname %^%#Rxc\w<GW]"G\K
```

```

\n<VcW:l8hUa.JCaxh+tfaPM%^%#
snmp-agent trap enable
snmp-agent
#
telnet server enable
#
user-interface maximum-vty 5
user-interface vty 0 4
authentication-mode aaa
protocol inbound telnet
#

```

- USG防火墙的配置文件

```

#
telnet server enable
#
interface GigabitEthernet1/0/3  #与网管对接的接口
undo shutdown
ip address 192.168.26.22 255.255.255.0
service-manage enable
service-manage telnet permit
service-manage snmp permit
#
user-interface vty 0 4
authentication-mode aaa
protocol inbound telnet
user privilege level 15
idle-timeout 5
#
aaa
authentication-scheme default
#
manager-user huawei
password cipher $1a$"hg'4WjC):$#8{XH!m3FS2>/)s1ft<iM*\&cWHv6m3ab0^z8|l$
service-type telnet
level 15
#
firewall zone trust
set priority 85
add interface GigabitEthernet1/0/3
#
snmp-agent
snmp-agent community write cipher %^%#77G5T7GZy@/wk^B^P.+P5y7G%=^1!3:~qFg|/K,z#[\!
i&@*!a]pCG$Ms!+bZ>M-i/Wv>".E-Hh6ujM%^%# mib-view mib2view
snmp-agent sys-info version v2c
snmp-agent target-host inform address udp-domain 192.168.26.232 params securityname cipher %^
%#qvV,Vaw-Q*,"=D=U!6+Fw>'N'Loa/JnZB{-r1}};%^%# v2c
snmp-agent mib-view included mib2view system
snmp-agent trap enable
#
return

```

## 8.4.5 管理设备

### 8.4.5.1 配置 SolarWinds NCM 管理设备使用的 SSH/Telnet 凭据

#### SSH/Telnet 凭据简介

如果您需要通过SolarWinds Network Configuration Manager ( NCM ) 管理设备，如配置备份和恢复，需要先配置SolarWinds NCM管理设备使用的SSH/Telnet凭据，并[8.4.5.2 将设备添加到SolarWinds NCM](#)。

SSH/Telnet凭据由三部分组成：设备登录信息（即用户名和密码）、通信传输协议和传输端口。

## 📖 说明

SolarWinds NCM使用的SSH/Telnet凭据必须与华为S系列交换机上配置的SSH/Telnet参数一致，否则您将无法通过SolarWinds NCM对其进行管理。

## SSH/Telnet 凭据配置方式

- 全局默认的SSH/Telnet凭据：如果将设备添加到SolarWinds NCM时，未指定SSH/Telnet凭据，则SolarWinds NCM使用全局默认的SSH/Telnet凭据管理设备。
- SSH/Telnet凭据模板：SolarWinds NCM可以使用同一个模板管理多个设备。

## 操作步骤

**步骤1** 单击“SETTINGS > All Settings”。

**步骤2** 单击“PRODUCT SPECIFIC SETTINGS”选项下的“NCM Settings”。

- **配置全局默认的SSH/Telnet凭据**  
# 单击“Global Device Defaults”选项下的“Global Device Defaults”，按需配置各项参数，完成后单击“SUBMIT”。

### Device Login Information

Devices and scripts can use these  
» [Learn more about Global Macros](#)

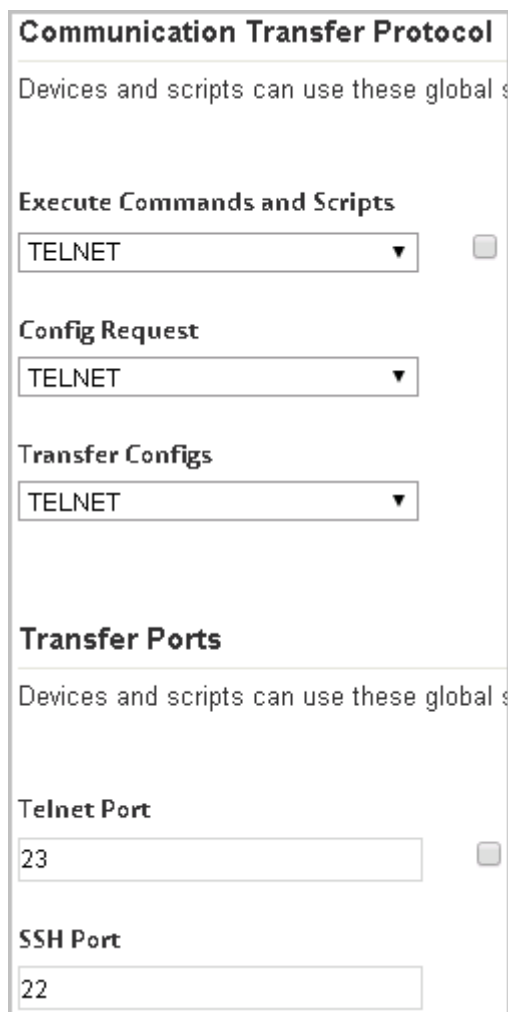
**Username**

**Password**

**Confirm Password**

**Enable Level**

**Enable Password**



**Communication Transfer Protocol**

Devices and scripts can use these global s

**Execute Commands and Scripts**

TELNET

**Config Request**

TELNET

**Transfer Configs**

TELNET

**Transfer Ports**

Devices and scripts can use these global s

**Telnet Port**

23

**SSH Port**

22

- **创建SSH/Telnet凭据模板**  
# 单击“Global Device Default”选项下的“Connection Profiles”，单击“CREATE NEW”创建SSH/Telnet凭据模板，按需配置各项参数，完成后单击“SUBMIT”。

----结束

## 8.4.5.2 将设备添加到 SolarWinds NCM

### 背景信息

如果您需要通过SolarWinds NCM管理设备，如配置备份和恢复，需要先[8.4.5.1 配置 SolarWinds NCM管理设备使用的SSH/Telnet凭据](#)，并将设备添加到SolarWinds NCM。

### 操作步骤

- 添加单个设备时，同步将其添加至SolarWinds NCM。
- 添加自动发现的设备时，同步将其添加至SolarWinds NCM
- 如果添加设备时，未同步将其添加到SolarWinds NCM，需要在设备添加完成后，单独将设备添加至SolarWinds NCM。

- a. 单击“SETTINGS > Manage Nodes”。
- b. 选中一个或多个设备，单击“EDIT PROPERTIES”。
- c. 下拉至“Manage node(s) with NCM”，选择**Yes**。
  - 如果选中多个设备，则只能使用全局默认的SSH/Telnet凭据。
  - 如果选中一个设备，可以使用全局默认的SSH/Telnet凭据、已存在的SSH/Telnet凭据模板、创建新的SSH/Telnet凭据模板或者单独为该设备指定SSH/Telnet凭据。

- d. 单击“SUBMIT”。

### 8.4.5.3 下载设备的配置文件

#### 前提条件

#### 8.4.5.2 将设备添加到SolarWinds NCM。

#### 操作步骤

- 步骤1** 单击“MY DASHBORADS > CONFIGS > Configuration Management”。
- 步骤2** 选中一个或多个设备，单击“DOWNLOAD”，选择需要下载的配置文件的类型。**Running**表示设备正在运行的配置文件，**Startup**表示设备启动时加载的配置文件。
- 步骤3** 单击弹出的对话框“DOWNLOAD CONFIGS”中的“YES”，开始下载配置文件。

**步骤4** 单击设备名称下的时间点，可以查看该时间点下载的配置文件。

Name ▲	IP Address	Last	Last action date
<span style="color: green;">●</span> S12704-1	192.168.21.20		2018/12/1 14:15:43
2018/12/1 14:15:45	Running		
<span style="color: green;">●</span> S5720HI-1	192.168.21.14		2018/12/1 14:15:43
2018/12/1 14:15:45	Running		

----结束

## 8.4.5.4 日常备份设备的配置文件

### 前提条件

**8.4.5.2 将设备添加到SolarWinds NCM。**

### 操作步骤

**步骤1** 单击“MY DASHBORADS > CONFIGS > Jobs”。

**步骤2** 单击“CREATE NEW JOB”。

1. 输入任务名称，任务类型选择**Download Configs from Devices**，设置运行周期，然后单击“NEXT”。

**CREATE JOB** > CHOOSE NODES > ENTER NOTIFICATION DETAILS > ADD JOB SPECIFIC DETAILS > REVIEW >

**New Job Details**

**Name of Job**  
Daily Configuration Backup

**Job Type**  
Download Configs from Devices [» Help me decide](#)

**Schedule Type:** Basic

ONCE **DAILY** WEEKLY MONTHLY

**EVERY** 1 day(s)

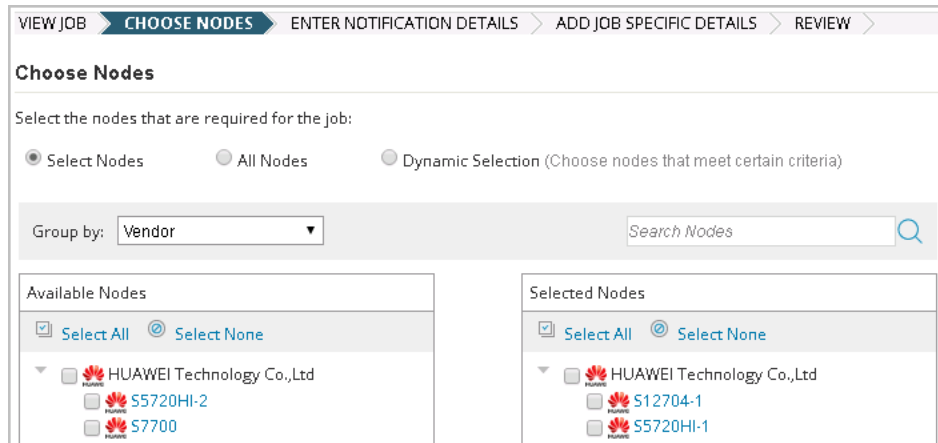
**EVERY WEEK DAY**

Start time 00:00 Enter time values from 00:00 through 24:00. Use HH:MM format (NCM Server time: 14:41 UTC +8)

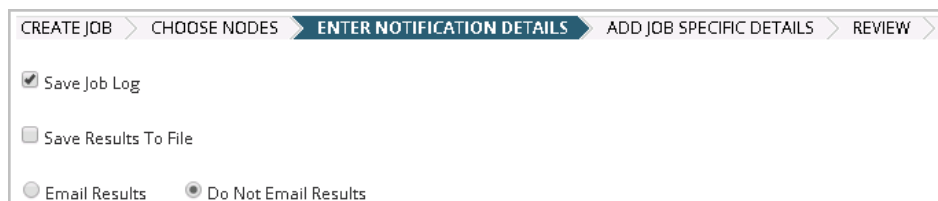
Starting On: 2018/12/2 Ending On: 2028/12/1

2. 选择需要执行该任务的设备，然后单击“NEXT”。

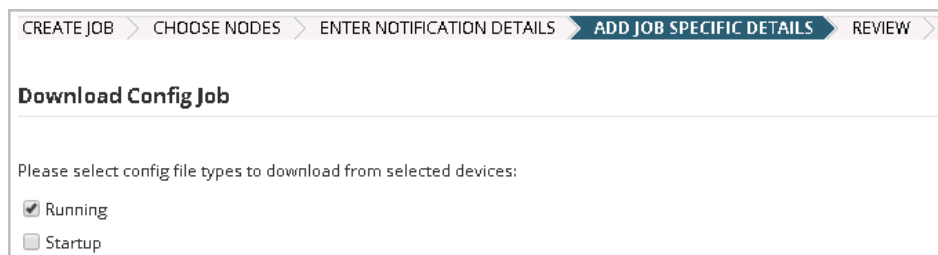




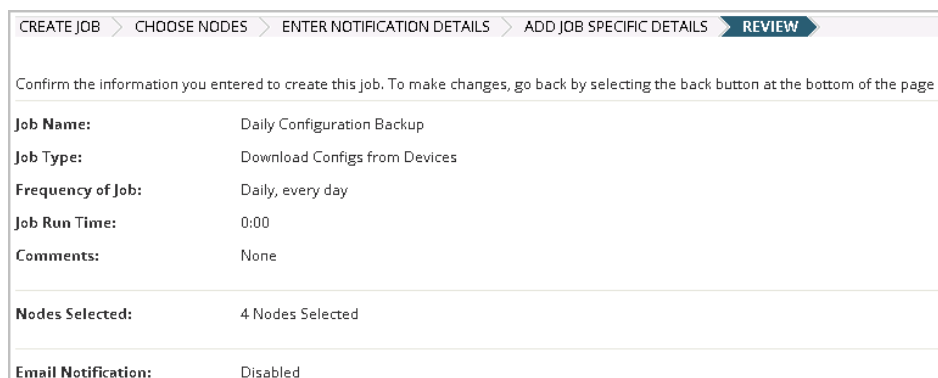
3. 选择任务完成后的通知方式，然后单击“NEXT”。



4. 选择下载的配置文件类型，然后单击“NEXT”。



5. 检查该任务的设置，然后单击“FINISH”。



**步骤3** 任务创建完成，此后任务会根据您的设置周期性运行。您还可以选中任务，单击“START JOB”，该任务会立即执行一次。

Job Name	Status	Job Type	Author	Last Date Run
<input checked="" type="checkbox"/> Daily Configuration Backup	Scheduled	Download Configs from Devices	admin	2018/12/1 15:14

**步骤4** 单击“MY DASHBORADS > CONFIGS > Configuration Management”，单击设备名称下的时间点，可以查看该时间点备份的配置文件。

Name ▲	IP Address	Last	Last action date
● S12704-1	192.168.21.20	🔗	2018/12/1 14:15:43
🕒 2018/12/1 15:14:42	Running		
● S5720HI-1	192.168.21.14	🔗	2018/12/1 14:15:43
🕒 2018/12/1 15:14:41	Running		

----结束

### 8.4.5.5 上传配置文件至设备

#### 前提条件

8.4.5.2 将设备添加到SolarWinds NCM。

#### 操作步骤

- 步骤1** 单击“MY DASHBORADS > CONFIGS > Configuration Management”。
- 步骤2** 选中需要上传配置文件的设备，单击“UPLOAD”。
- 步骤3** 选中待上传的配置文件。如有需要，可直接编辑右侧的配置文件。

#### Upload config

Applies to 1 node(s)

Select config to upload

GROUP BY:

Vendor ▼

Device Status ▼

Select 3rd Criteria ▼

- ▶ HUAWEI Technology Co.,Ltd (4)
  - ▶ Up (4)
    - ▶ S12704-1
      - 🕒 2018/12/1 15:42 - Running
    - ▶ S5720HI-1
    - ▶ S5720HI-2
    - ▶ S7700
  - ▶ Unknown (1)

CONFIG NAME: 2018/12/1 15:42 - RUNNING

```

1 !Software Version V200R009C00SPC500
2 #
3 sysname S12704-1
4 #
5 FTP server enable
6 #
7 info-center loghost source-port 10101
8 info-center loghost 192.168.26.234
9 #
10 vlan batch 12 to 16
11 #
12 authentication-profile name default_authen_profile
13 authentication-profile name dot1x_authen_profile
14 authentication-profile name mac_authen_profile
15 authentication-profile name portal_authen_profile
16 authentication-profile name dot1xmac_authen_profile
17 authentication-profile name multi_authen_profile

```

- 步骤4** 单击“Advanced”，根据需要选择可选项，然后单击“UPLOAD”上传配置文件。

▼ Advanced UPLOAD

Save config to file  Write to NVRAM  Reboot Device

- 步骤5** 上传完成之后，可以看到上传记录。

Name ▲	IP Address	Last	Last action date
● S12704-1	192.168.21.20	🔗	2018/12/1 16:05:03

----结束

## 8.4.5.6 上传配置变更至设备

### 前提条件

[8.4.5.2 将设备添加到SolarWinds NCM。](#)

### 配置变更上传方式

- 在SolarWinds上编辑设备的配置文件，然后将编辑后的配置文件上传至设备。
- 执行脚本将变更的配置上传至设备。

### 操作步骤

- 在SolarWinds上编辑设备的配置文件，然后将编辑后的配置文件上传至设备。本举例以在S12704-1上创建VLAN 100为例。

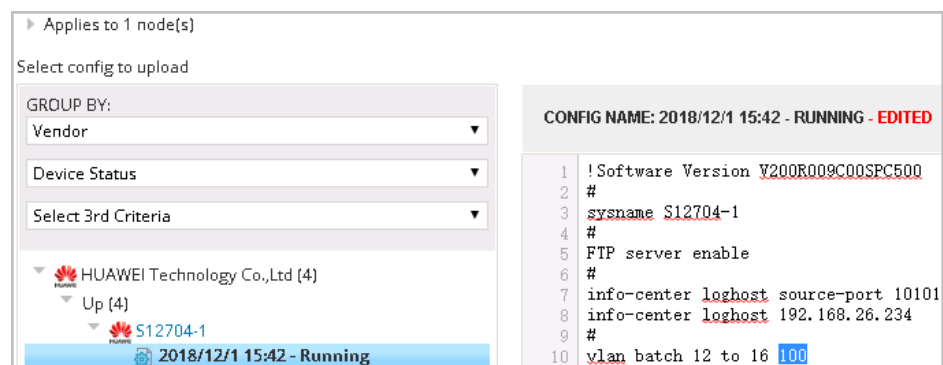
- [8.4.5.3 下载设备的配置文件。](#)
- 上传配置文件之前，查看S12704-1上的VLAN配置。

```
[S12704-1] display vlan summary
Static VLAN:
Total 6 static VLAN.
 1 12 to 16

Dynamic VLAN:
Total 0 dynamic VLAN.

Reserved VLAN:
Total 0 reserved VLAN.
```

- [8.4.5.5 上传配置文件至设备。](#)上传时，请选择第1步中备份的配置文件，并进行编辑。



- 配置文件上传成功之后，再次查看S12704-1上的VLAN配置。可以发现S12704-1上已成功创建了VLAN 100。

```
[S12704-1] display vlan summary
Static VLAN:
Total 7 static VLAN.
 1 12 to 16 100

Dynamic VLAN:
Total 0 dynamic VLAN.

Reserved VLAN:
Total 0 reserved VLAN.
```

- 执行脚本将变更的配置上传至设备。本举例以在S12704-1上创建VLAN 100为例。
  - 单击“MY DASHBORADS > CONFIGS > Configuration Management”。

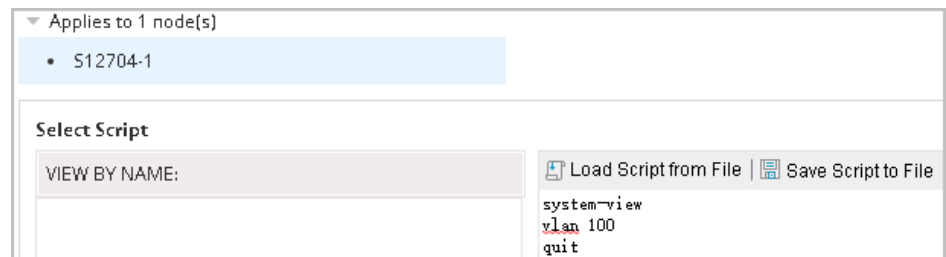
- b. 选中设备，单击“EXECUTE SCRIPT”。
- c. 执行脚本之前，查看S12704-1上的VLAN配置。

```
[S12704-1] display vlan summary
Static VLAN:
Total 6 static VLAN.
 1 12 to 16
```

```
Dynamic VLAN:
Total 0 dynamic VLAN.
```

```
Reserved VLAN:
Total 0 reserved VLAN.
```

- d. 编辑脚本内容，即您希望在设备上执行的命令，完成后单击“EXECUTE”。



- e. 单击弹出的“EXECUTE SCRIPT”对话框中的“YES”。
- f. 脚本执行完成之后，再次查看S12704-1上的VLAN配置。可以发现S12704-1上已成功创建了VLAN 100。

```
[S12704-1] display vlan summary
Static VLAN:
Total 7 static VLAN.
 1 12 to 16 100
```

```
Dynamic VLAN:
Total 0 dynamic VLAN.
```

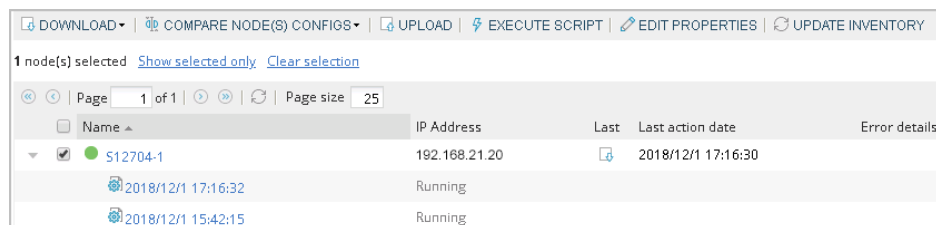
```
Reserved VLAN:
Total 0 reserved VLAN.
```

### 8.4.5.7 比较设备配置文件之间的差异

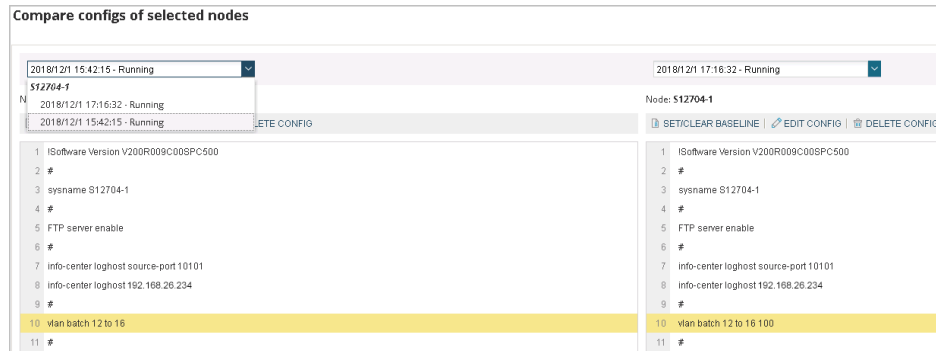
#### 操作步骤

**步骤1** 单击“MY DASHBORADS > CONFIGS > Configuration Management”。

**步骤2** 选中设备，单击“COMPARE NODE(S) CONFIGS”，然后单击“Compare node(s) configs”。



**步骤3** 在左右两侧选择待比较的配置文件之后，即可查看二者之间的差异。



---结束

## 8.4.6 日志和告警管理

### 8.4.6.1 查看设备上报的日志和告警

#### 操作步骤

**步骤1** 本举例通过在S12704-1上关闭/开启接口，查看SolarWinds能否接收到设备发送的告警。

```
[S12704-1] interface GigabitEthernet 1/1/1/2
[S12704-1-GigabitEthernet1/1/1/2] shutdown
```

**步骤2** 单击“ALERTS & ACTIVITY > Traps”。SolarWinds已接收到S12704-1的GE1/1/1/2接口Down之后而产生的接口Down以及OSPF链路状态变化的告警。

2018/12/1 17:38:18	192.168.21.20	192.168.21.20	Huawei@2018	OSPF-MIB:ospfOriginateLsa	ospfLsdbRouterId.0.0.0.0.1.10.10.2.2.10.10.2.2 = 10.10.2.2 ospfLsdbLsId.0.0.0.0.1.10.10.2.2.10.10.2.2 = 10.10.2.2 ospfLsdbType.0.0.0.0.1.10.10.2.2.10.10.2.2 = routerLink(1) ospfLsdbAreaId.0.0.0.0.1.10.10.2.2.10.10.2.2 = 0.0.0.0 ospfRouterId = 10.10.2.2 snmpTrapOID = OSPF-MIB:ospfOriginateLsa sysUpTime = 50 days 2 hours 25 minutes 17.85 seconds
2018/12/1 17:38:18	192.168.21.20	192.168.21.20	Huawei@2018	OSPF-MIB:ospfIfStateChange	ospfIfState.10.10.4.1.0 = down(1) ospfAddressLessIf.10.10.4.1.0 = 0 ospfIfIpAddress.10.10.4.1.0 = 10.10.4.1 ospfRouterId = 10.10.2.2 snmpTrapOID = OSPF-MIB:ospfIfStateChange sysUpTime = 50 days 2 hours 25 minutes 17.85 seconds
2018/12/1 17:38:18	192.168.21.20	192.168.21.20	Huawei@2018	IF-MIB:linkDown	ifDescr.120 = Vlanif14 ifOperStatus.120 = down(2) ifAdminStatus.120 = up(1) ifIndex.120 = 120 snmpTrapOID = IF-MIB:linkDown sysUpTime = 50 days 2 hours 25 minutes 17.84 seconds
2018/12/1 17:38:18	192.168.21.20	192.168.21.20	Huawei@2018	IF-MIB:linkDown	ifDescr.200 = GigabitEthernet1/1/1/2 ifOperStatus.200 = down(2) ifAdminStatus.200 = down(2) ifIndex.200 = 200 snmpTrapOID = IF-MIB:linkDown

**步骤3** 将S12704-1的GE1/1/1/2接口恢复Up。

```
[S12704-1-GigabitEthernet1/1/1/2] undo shutdown
```

**步骤4** 再次查看SolarWinds的告警中心，可以发现SolarWinds已接收到S12704-1的GE1/1/1/2接口恢复Up之后而产生的接口Up、OSPF链路状态变化、LLDP邻居变化、设备配置变化以及MSTP拓扑变化的告警。

2018/12/1 17:46:01	192.168.21.20	192.168.21.20	Huawei@2018	HUAWEI-DATASYNC- MIB:hwCfgChgNotify	hwCfgChgTableMaxItem = 4095 hwCfgChgSeqIDReverlCount = 0 hwCurrentCfgChgSeqID = 100 snmpTrapOID = HUAWEI-DATASYNC-MIB:hwCfgChgNotify sysUpTime = 50 days 2 hours 33 minutes 0.41 second ifName.200 = GigabitEthernet1/1/1/2 hwMstpPortIndex.0.13 = 13 hwMstpInstanceID = 0 snmpTrapOID = HUAWEI-IPDSLAM-MSTP-MIB:hwMstpCommonTraps sysUpTime = 50 days 2 hours 33 minutes 0.24 second
2018/12/1 17:46:01	192.168.21.20	192.168.21.20	Huawei@2018	HUAWEI-IPDSLAM-MSTP- MIB:hwMstpCommonTraps	snmpTrapOID = BRIDGE-MIB:topologyChange sysUpTime = 50 days 2 hours 33 minutes 0.24 second
2018/12/1 17:46:01	192.168.21.20	192.168.21.20	Huawei@2018	BRIDGE-MIB:topologyChange	lldpStatsRemTablesAgeouts = 0 lldpStatsRemTablesDrops = 0 lldpStatsRemTablesDeletes = 0 lldpStatsRemTablesInserts = 1 snmpTrapOID = LLDP-MIB:lldpRemTablesChange sysUpTime = 50 days 2 hours 32 minutes 58.51 seconds
2018/12/1 17:45:59	192.168.21.20	192.168.21.20	Huawei@2018	LLDP-MIB:lldpRemTablesChange	ifDescr.120 = Vlanif14 ifOperStatus.120 = up(1) ifAdminStatus.120 = up(1) ifIndex.120 = 120 snmpTrapOID = IF-MIB:linkUp sysUpTime = 50 days 2 hours 32 minutes 56.44 seconds
2018/12/1 17:45:57	192.168.21.20	192.168.21.20	Huawei@2018	IF-MIB:linkUp	ospfLsdbRouterId.0.0.0.1.10.10.2.2.10.10.2.2 = 10.10.2.2 ospfLsdbLsid.0.0.0.1.10.10.2.2.10.10.2.2 = 10.10.2.2 ospfLsdbType.0.0.0.1.10.10.2.2.10.10.2.2 = routerLink(1) ospfLsdbAreaId.0.0.0.1.10.10.2.2.10.10.2.2 = 0.0.0.0 ospfRouterId = 10.10.2.2 snmpTrapOID = OSPF-MIB:ospfOriginateLsa sysUpTime = 50 days 2 hours 32 minutes 56.45 seconds
2018/12/1 17:45:57	192.168.21.20	192.168.21.20	Huawei@2018	OSPF-MIB:ospfOriginateLsa	ifDescr.200 = GigabitEthernet1/1/1/2 ifOperStatus.200 = up(1) ifAdminStatus.200 = up(1) ifIndex.200 = 200 snmpTrapOID = IF-MIB:linkUp sysUpTime = 50 days 2 hours 32 minutes 56.43 seconds
2018/12/1 17:45:57	192.168.21.20	192.168.21.20	Huawei@2018	IF-MIB:linkUp	

---结束

# 9 搬迁后验收

---

搬迁完成后，根据收集的现网业务情况，对搬迁后的现网业务进行验证，确保所有搬迁前的业务在搬迁后能够正常运行。

参考[WLAN项目验收指导](#)进行验收，验收过程中发现的问题参考[无线网络优化](#)进行处理。完成后输出搬迁前后效果对比。

# 10 搬迁实例

以某搬迁项目为例介绍整个搬迁过程，供后续搬迁项目参考。

## 10.1 搬迁项目概况

### 10.1.1 项目范围

项目范围说明：该项目属于有线和无线整体搬迁，本次搬迁包括：将A局点中现有的核心交换机、接入交换机和WLAN设备替换成华为设备，并进行业务测试和现场支持，确保业务平滑迁移。

业务影响预估：预计割接时间约3天，期间可能会由于布线变化等原因导致业务短暂中断。

### 10.1.2 搬迁计划

#### 计划概况

ID	任务	开始时间	完成时间	工期	2020-05-01	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	搬迁方案设计	2020-05-01 09:00	2020-05-07 18:00	5 d	[Gantt bar from Day 1 to Day 5]																									
2	搬迁方案确认	2020-05-08 09:00	2020-05-11 18:00	2 d	[Gantt bar from Day 8 to Day 10]																									
3	设备运输	2020-05-01 09:00	2020-05-08 18:00	6 d	[Gantt bar from Day 1 to Day 6]																									
4	AP安装	2020-05-11 09:00	2020-05-14 18:00	4 d	[Gantt bar from Day 11 to Day 14]																									
5	交换机安装	2020-05-11 09:00	2020-05-12 18:00	2 d	[Gantt bar from Day 11 to Day 12]																									
6	搬迁前预配置	2020-05-12 09:00	2020-05-15 18:00	4 d	[Gantt bar from Day 12 to Day 15]																									
7	准备验收报告	2020-05-01 09:00	2020-05-20 18:00	14 d	[Gantt bar from Day 1 to Day 14]																									
8	搬迁实施	2020-05-15 09:00	2020-05-20 18:00	4 d	[Gantt bar from Day 15 to Day 19]																									
9	搬迁后网络测试	2020-05-18 09:00	2020-05-21 18:00	4 d	[Gantt bar from Day 18 to Day 21]																									
10	常规检查	2020-05-22 09:00	2020-06-09 18:00	13 d	[Gantt bar from Day 22 to Day 35]																									

#### 搬迁项目团队

为了后续沟通方便，和客户一起组建搬迁团队并建立如表10-1所示的联系单，需要包括华为侧和客户侧联系人以及可能涉及的系统集成商或其他厂商的联系人信息。



表 10-1 联系单

姓名	公司	办公位置	联系方式	项目职责
张三	华为	xx	xx	搬迁交付项目经理
.....	.....	.....	.....	.....

## 搬迁原则

为了保证搬迁项目顺利实施，需要遵循如下搬迁原则：

- 充分准备，满足所有搬迁条件
- 流程简单可行
- 支持快速回退
- 对现网影响可控

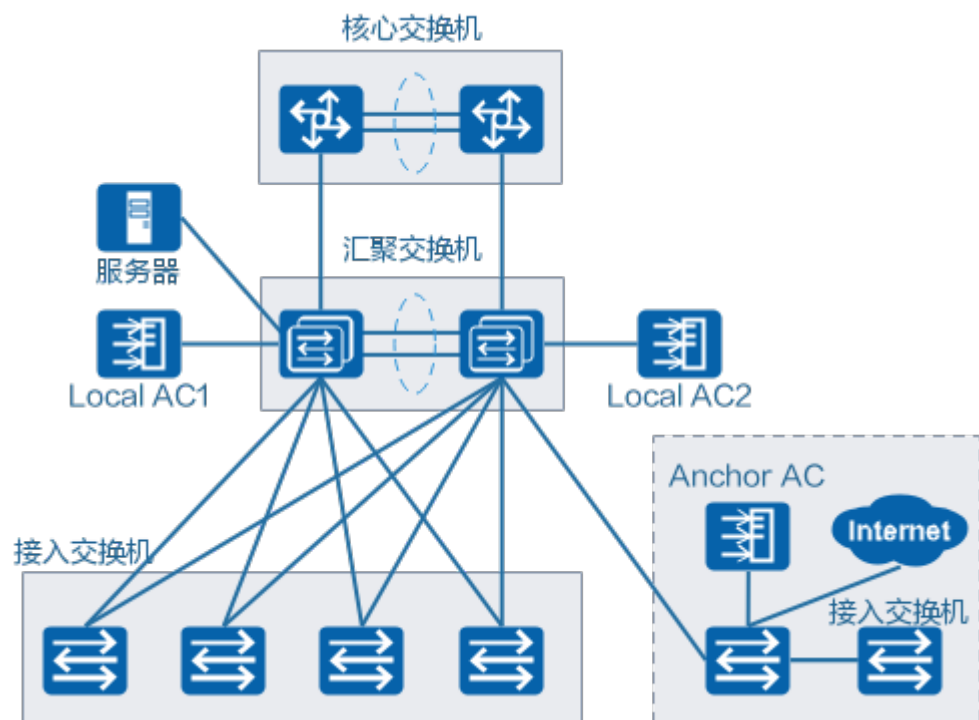
## 10.2 网络评估

### 10.2.1 搬迁前网络分析

当前网络分为核心/汇聚和接入两层。备份组中的两台AC分别连接到两个核心/汇聚交换机堆叠。

#### 10.2.1.1 网络拓扑结构

向客户获取现网网络拓扑图，按照核心层、汇聚层和接入层梳理网络拓扑结构。



如上图所示，当前组网描述如下：

- 当前接入层包括4组思科交换机，每组采用2\*GE上行连接核心/汇聚交换机。接入交换机工作在二层，业务VLAN透传到核心/汇聚交换机。
- 核心/汇聚层包含2个堆叠组，每个堆叠组包含2台思科交换机。两组通过2\*GE链路连接。业务网关配置在两个Group上，两个Group之间运行HSRP。每台核心/汇聚交换机使用1\*GE链路连接到IT办公机房核心/汇聚交换机，其中4芯汇聚交换机二层互联，采用Rapid-PVST避免环路。
- 两台AC工作在主备模式，通过1\*GE链路分别接入两个核心/汇聚堆叠组。
- AP与AC三层互通，AP通过Local AC上线。一部分无线用户业务转发集中在Local AC上，另一部分无线用户业务指向Anchor AC。

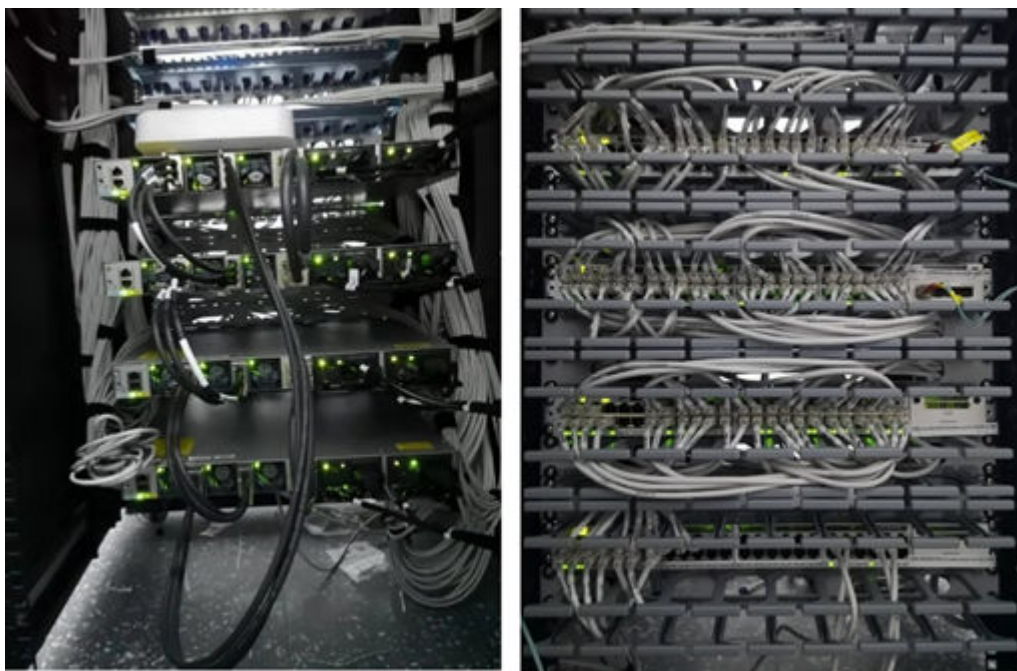
### 10.2.1.2 网规和工勘

**步骤1** 检查机房的电源是否正常。



**步骤2** 检查机房布线。

按照如下表格记录当前的端口对接情况，供后续搬迁参考。

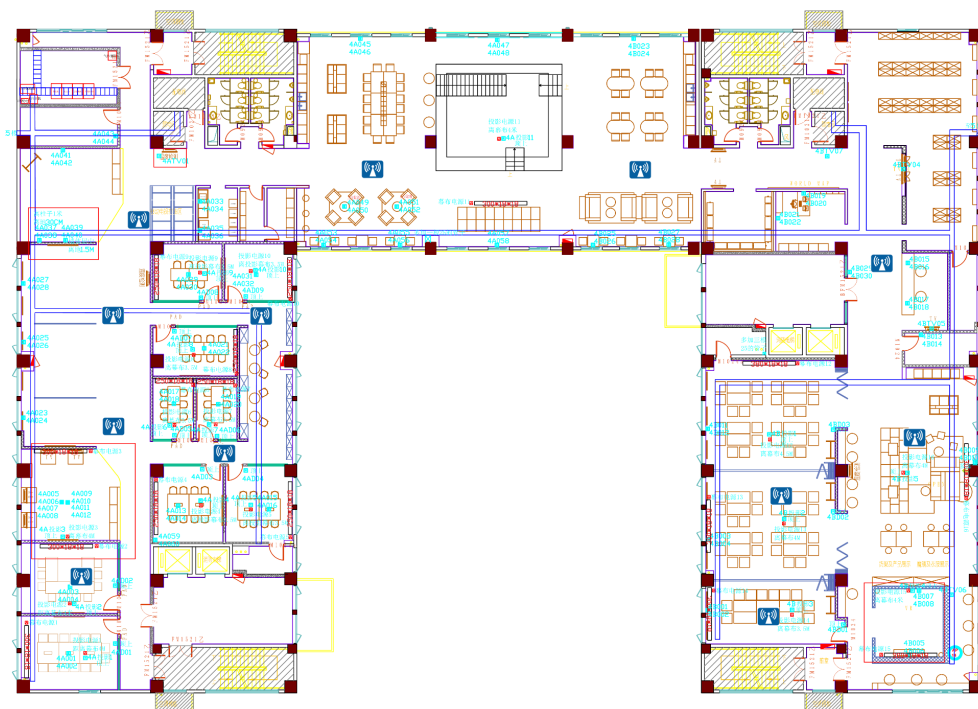


搬迁前					对端设备接口				
设备	接口	IP	VLAN	Link Type( trunk, access, hybrid)	设备	接口	IP	VLAN	Link Type
.....	.....	.....	.....	.....	.....	.....	.....	.....	.....

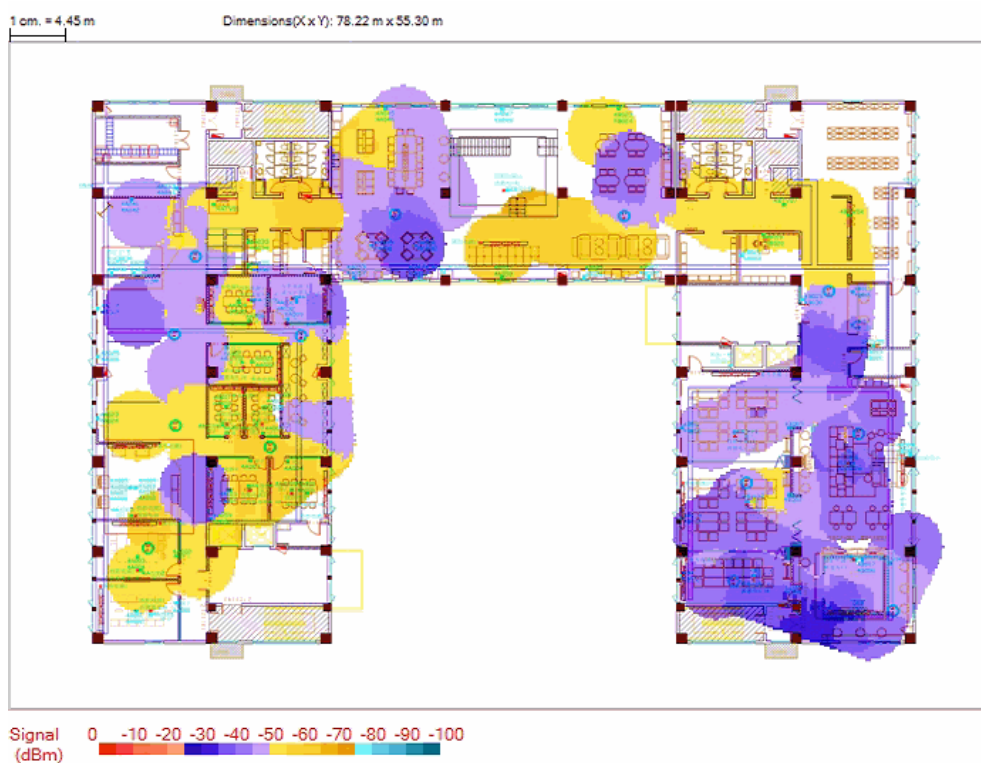
**步骤3** 检查当前WLAN网络信号覆盖情况和AP点位。

使用WLAN Planner按照当前AP点位进行原点位替换，并进行信号仿真。

- 当前AP点位如下图所示。

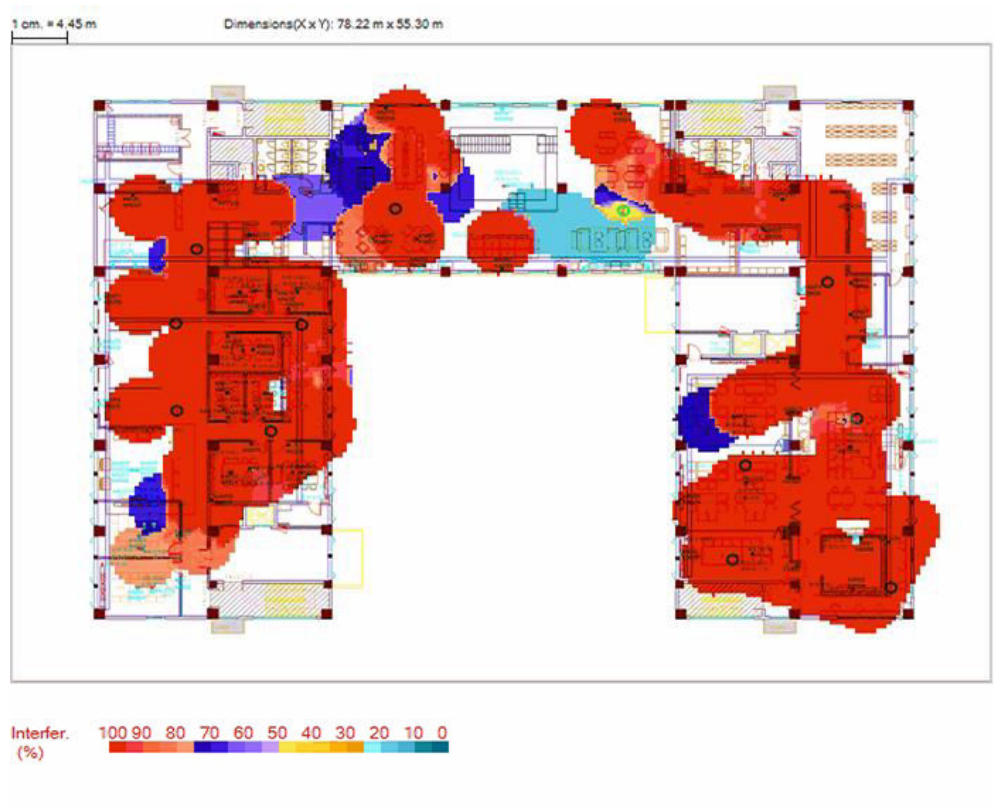


- 当前信号覆盖情况如下图所示，可以看出，当前的信号覆盖存在明显的盲区，需要重新进行WLAN网规。



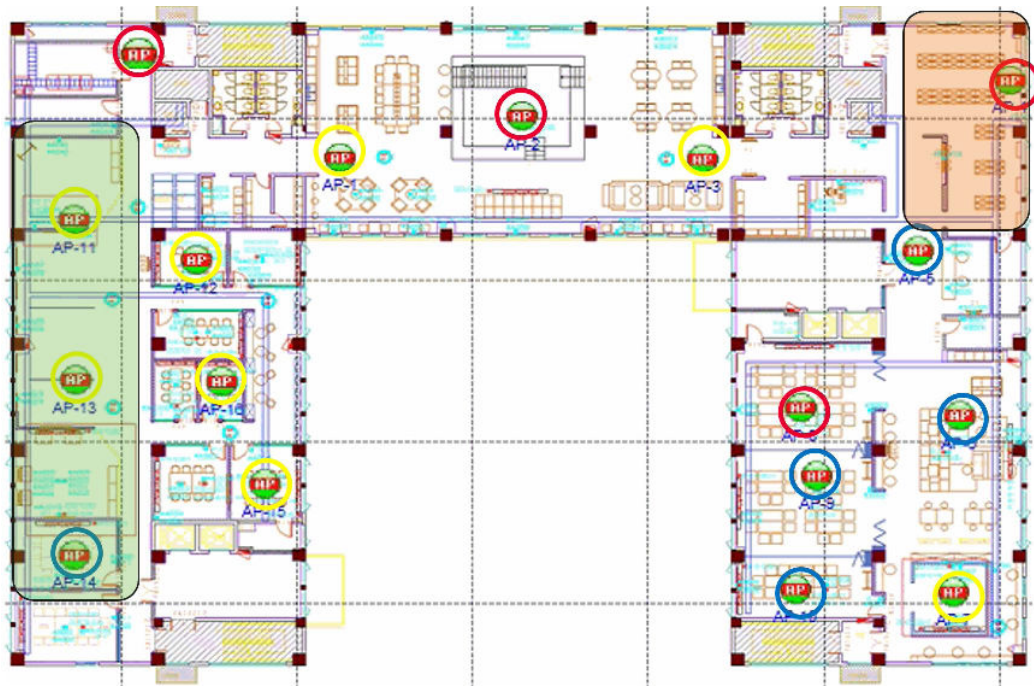
- 当前WLAN网络干扰情况：从图中可以看出，当前网络中存在严重干扰，需要排查干扰源或重新进行信道规划。



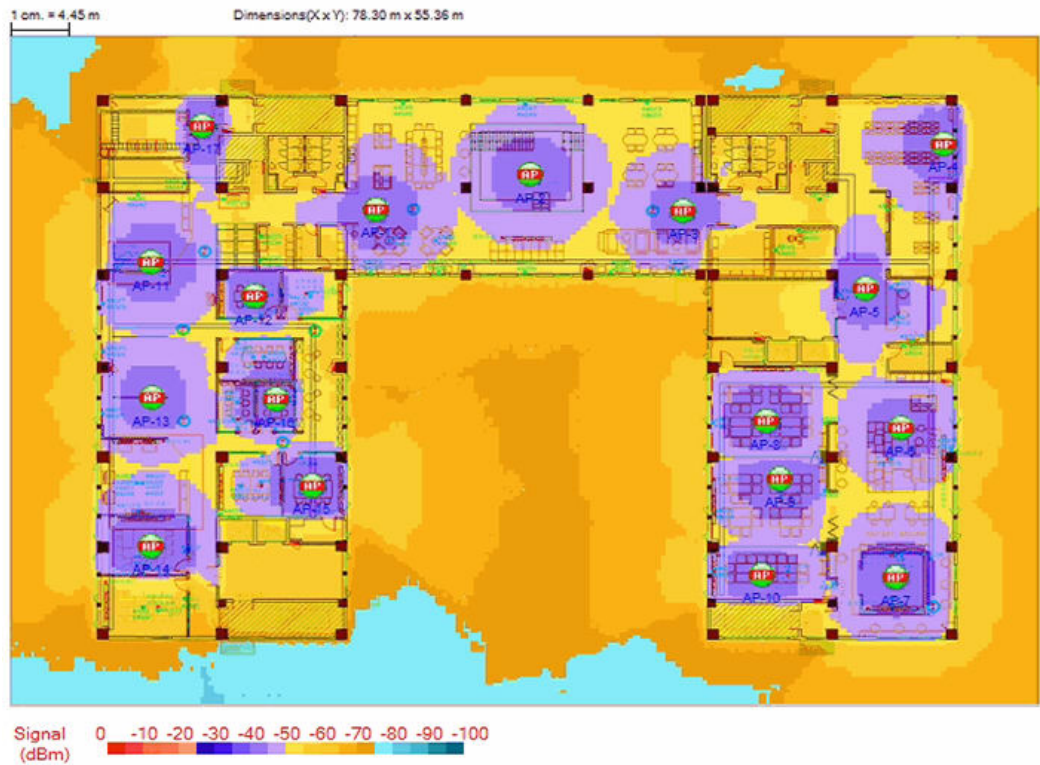


**步骤4** 结合当前网络信号覆盖情况和AP布放点位，重新进行WLAN工勘和网规。

重新进行网规后的AP点位如下图所示，标记蓝圈的AP是可以复用当前点位的；标记黄圈的AP是需要重新部署的；标记红圈的AP是需要新增的点位的。



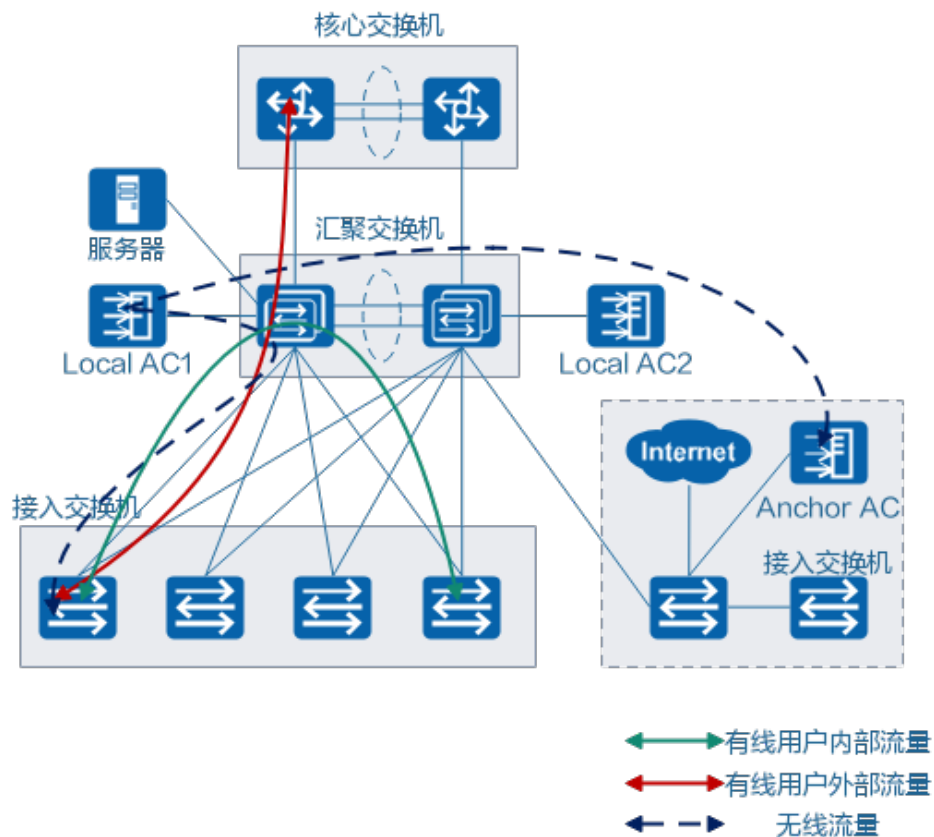
信号仿真结果如下图所示，信号强度满足要求，没有覆盖盲区。



----结束

### 10.2.1.3 业务模型

当前的网络业务流量模型如下图所示。



## 10.2.2 搬迁后网络分析

### 10.2.2.1 网络拓扑结构

搬迁过程中，会对网络拓扑结构进行如下操作：

**步骤1** 完成华为接入交换机、核心/汇聚交换机、WLAN AC之间的连接和组网，核心/汇聚交换机和接入交换机之间运行VBST。

新的网口连线请参见下表。

设备名称	设备型号	本地接口	连接方式	对端设备名称	对端设备型号	远端接口	连接方式
<b>AGG--ACC</b>							
AGG-01	S6730-H24X6C	XG1/0/1	10GE-SFP+	ACC-01	S5731-H48P4XC	XG1/0/1	10GE-SFP+
AGG-01	S6730-H24X6C	XG1/0/2	10GE-SFP+	ACC-04	S5731-H48P4XC	XG1/0/1	10GE-SFP+
AGG-01	S6730-H24X6C	XG1/0/3	10GE-SFP+	ACC-02	S5731-H48P4XC	XG1/0/1	10GE-SFP+
AGG-01	S6730-H24X6C	XG1/0/4	10GE-SFP+	ACC-03	S5731-H48P4XC	XG1/0/1	10GE-SFP+

设备名称	设备型号	本地接口	连接方式	对端设备名称	对端设备型号	远端接口	连接方式
AGG-02	S6730-H24X6C	XG1/0/1	10GE-SFP+	ACC-01	S5731-H48P4XC	XG2/0/1	10GE-SFP+
AGG-02	S6730-H24X6C	XG1/0/2	10GE-SFP+	ACC-04	S5731-H48P4XC	XG2/0/1	10GE-SFP+
AGG-02	S6730-H24X6C	XG1/0/3	10GE-SFP+	ACC-02	S5731-H48P4XC	XG2/0/1	10GE-SFP+
AGG-02	S6730-H24X6C	XG1/0/4	10GE-SFP+	ACC-03	S5731-H48P4XC	XG2/0/1	10GE-SFP+
<b>AGG--WLAN AC</b>							
AGG-01	S6730-H24X6C	XG2/0/1	10GE-SFP+	LocalAC 1	AC6508	XG0/0/1	10GE-SFP+
AGG-02	S6730-H24X6C	XG2/0/1	10GE-SFP+	LocalAC 2	AC6508	XG0/0/1	10GE-SFP+
<b>AGG--Exist Core</b>							
AGG-01	S6730-H24X6C	XG2/0/24	GE-SFP	Core-01	-	G1/0/3	GE-SFP
AGG-02	S6730-H24X6C	XG2/0/24	GE-SFP	Core-02	-	G1/0/3	GE-SFP
<b>AGG--AGG</b>							
AGG-01	S6730-H24X6C	XG1/0/23	10GE-SFP+	AGG-02	S6730-H24X6C	XG1/0/23	10GE-SFP+
AGG-01	S6730-H24X6C	XG2/0/23	10GE-SFP+	AGG-02	S6730-H24X6C	XG2/0/23	10GE-SFP+
<b>AGG--Internet Zone</b>							
AGG-01	S6730-H24X6C	XG2/0/2	10GE-SFP+	ACC-05	S5731-H48P4XC	XG0/0/1	10GE-SFP+
ACC-05	S5731-H48P4XC	XG0/0/2	10GE-SFP+	ACC-06	S5731-H48P4XC	XG0/0/1	10GE-SFP+
ACC-05	S5731-H48P4XC	XG0/0/3	10GE-SFP+	NaviAC1	AC6508	XG0/0/1	10GE-SFP+

**步骤2** 华为核心/汇聚交换机增加2条临时链路，运行LACP协议，连接现网核心/汇聚交换机；思科核心交换机与华为核心交换机之间的互联链路部署BPDU filter；接入端口部署BPDU guard；将现有思科接入交换机上的用户链路迁移到新的华为接入交换机上。

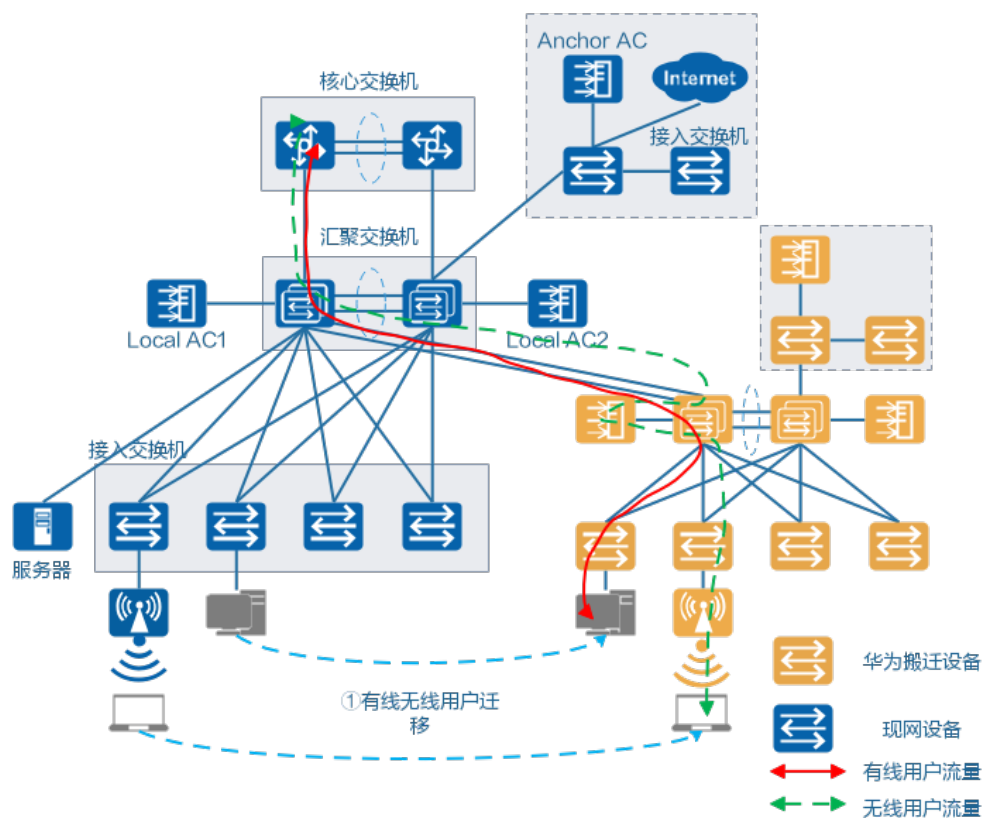
有线接入用户迁移后，需要在华为核心/汇聚交换机与现网核心/汇聚交换机之间的链路上开启WLAN业务和管理VLAN，实现华为WAC和AP上线，完成WLAN业务迁移。



(首先关闭华为AP的射频; 其次, 在搬迁过程中打开华为AP的射频, 关闭思科的射频)

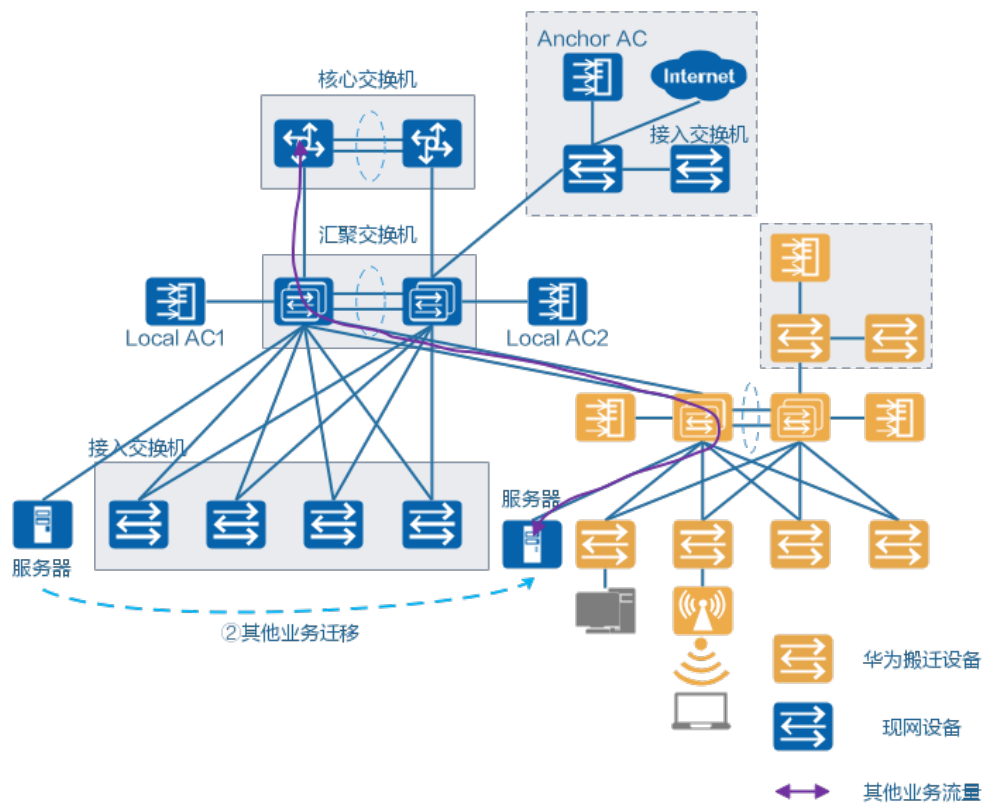
思科核心交换机与华为核心交换机之间没有生成树, 因此在核心交换机上跳接线缆时要小心。

有线无线用户接入迁移拓扑如下图所示:



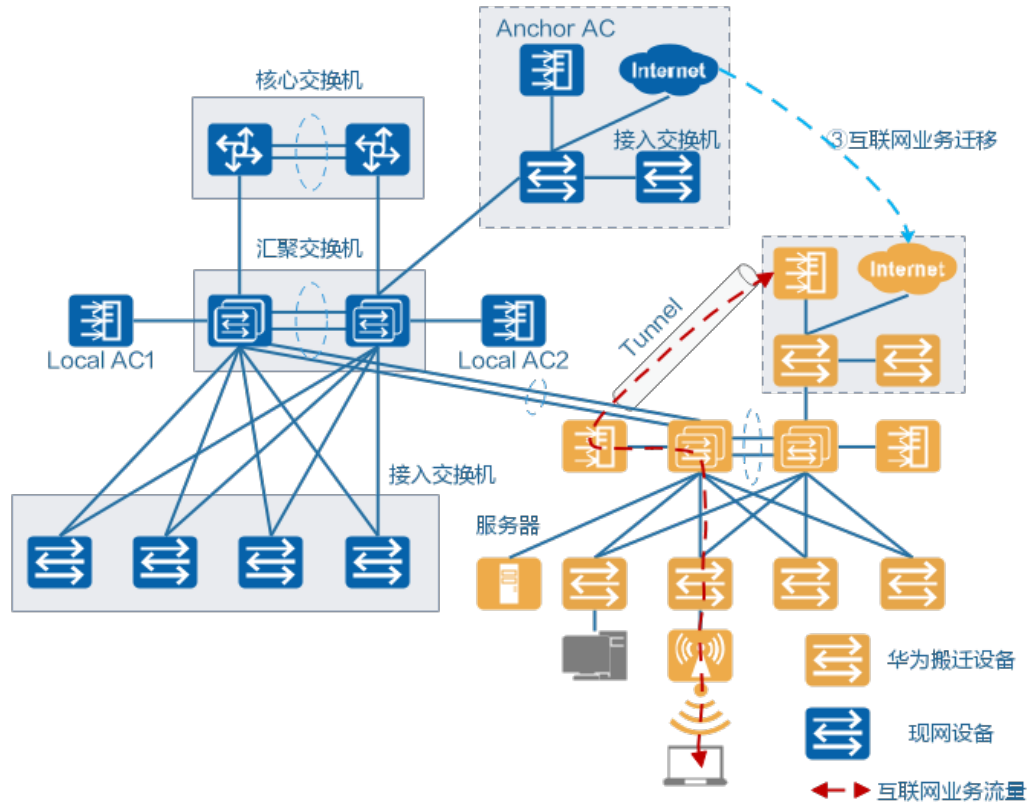
**步骤3** 接入交换机业务全部迁移完成后, 将核心/汇聚交换机下挂的其他业务迁移到华为核心/汇聚交换机上。

核心/汇聚其他业务迁移拓扑如下图所示:



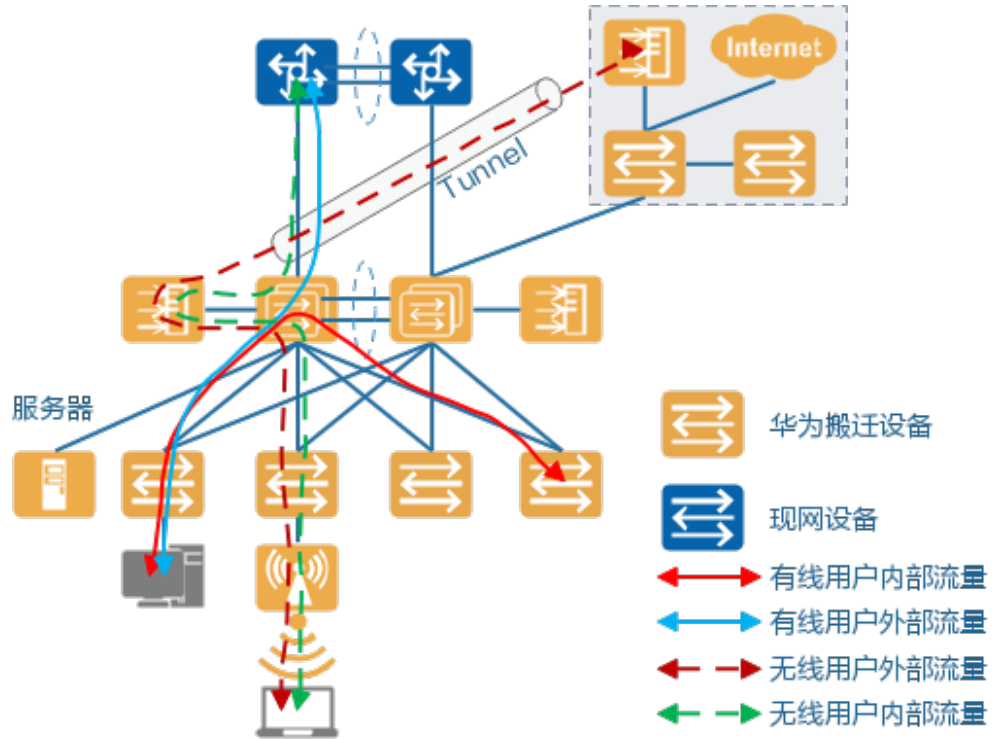
**步骤4** 接入交换机、核心/汇聚交换机业务迁移完成后，将Internet出口和当前Internet区接入交换机的业务迁移到华为Internet区。

互联网区业务迁移拓扑图如下：



**步骤5** 核心/汇聚上行链路迁移。除核心/汇聚上行链路外，所有业务迁移完成后，关闭华为为核心/汇聚交换机与现网核心/汇聚交换机之间的临时链路；将当前思科核心交换机上的两条上行链路移到华为核心交换机上。

核心/汇聚交换机上行链路迁移后的拓扑图如下：



----结束

### 10.2.2.2 端口前后映射表

按照如下表格样式梳理搬迁前后各设备端口的映射关系表。

Before Migration					After Migration(Huawei)					Peer Device Port				
De vic e	Port	IP	VL AN	Lin k Ty p e (t ru nk, acc ess , hy bri d )	De vic e	Port	IP	VL AN	Lin k Ty p e	De vic e	Port	IP	VL AN	Lin k Ty p e
.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....

## 10.2.3 风险分析和规避措施

### 业务中断分析

- 迁移时，先迁移接入交换机业务。割接时，需要将原有物理链路改造成新的接入交换机。每个端口预计会关闭约2分钟。
- 无线业务迁移过程中，Wi-Fi信号会断开和重新连接。预计每个无线STA将停机约2分钟。
- 服务器业务迁移时，需要将现网核心/汇聚交换机上已有的物理链路拔出，插入到华为核心/汇聚交换机上。每台服务器预计将停机约2分钟。
- 核心/汇聚交换机搬迁时，需要变更物理链路，与现网核心交换机对接，修改业务网关配置，VRRP主备切换。预计业务中断时间约30分钟。
- 如果割接过程中发生事故，请立即触发回退。停机时间不超过60分钟，包括正常迁移所需的30分钟，以及故障识别和协议收敛所需的时间。

### 设备及版本风险

无设备及版本风险。

### 第三方对接风险

- 现网需要和思科核心交换机互通，需要部署协议避免环路（华为VBST和思科Papid-PVST互通）：在与思科核心交换机对接的端口上配置命令**stp no-agreement-check**。
- 与TACACS认证互通，需要提前验证对接可行性。
- 老终端兼容性测试。

## 10.3 搬迁前准备

### 10.3.1 搬迁申请

提前两周将搬迁方案和搬迁计划发给客户，征得客户同意，并建议客户半冻结网络，记录从当前开始到正式搬迁之前的所有业务和网络变更。

客户对搬迁方案和搬迁计划进行审核，批准搬迁。

### 10.3.2 线缆布放和连接测试

任务	责任人	标准	完成时间点
制作并布放线缆，并做好线缆标签	华为/客户	所有线缆按要求布放，并有线缆标签	搬迁前一天
连接测试	华为/客户	所有链路正常	搬迁前一天

### 10.3.3 硬件、软件和辅助材料准备

在搬迁前2天确认所需的硬件、软件和各种辅助材料，包括硬件型号和数量、软件版本等。

#### 软件

设备型号	软件版本	当前状态
S6730-H24X6C	V200R19C00SPC500	Ready
S5731-H24P4XC	V200R19C00SPC500	Ready
AC6508	V200R010C00SPC700	Ready
AP7060DN	V200R010C00SPCa00	Ready

#### 硬件

设备型号	数量	用途	是否升级到目标版本	当前状态
S6730-H24X6C	4	核心/汇聚交换机	在x月x日完成升级	Ready
S6730-H48X6C	1	核心/汇聚交换机	在x月x日完成升级	Ready
S5731-H48P4XC	15	接入交换机	在x月x日完成升级	Ready
S5731-H24P4XC	1	接入交换机	在x月x日完成升级	Ready
AC6508	3	WAC	在x月x日完成升级	Ready
AP7060DN	34	WLAN AP	在x月x日完成升级	Ready

#### 辅助材料

名称或规格	数量	用途	当前状态
10GE光模块	38	设备对接	Ready
GE光模块	20	设备对接	Ready
GE电模块	96	服务器接入	Ready
单模跳纤	10	设备对接	Ready

名称或规格	数量	用途	当前状态
多模跳纤	10	设备对接	Ready

### 10.3.4 设备预配置

根据配置翻译结果，提前配置新的核心/汇聚交换机、接入交换机、WLAN AC，核心/汇聚交换机去使能VLANIF接口。

### 10.3.5 设备上电和功能测试

1. 至少提前5天完成单台设备调测和新设备测试。
2. 华为核心/汇聚交换机与接入交换机之间新增链路对接测试。
3. 华为AP和WAC上线，测试信号。
4. 完成华为核心/汇聚交换机与xx厂商核心/汇聚交换机之间新增链路的对接和业务测试。在新建链路两端配置**stp bpdu-filter**命令，防止现网端口收发BPDU报文导致业务震荡。
5. 所有接入端口配置BPDU guard功能，防止出现环路风险。

### 10.3.6 账号密码和远程登录

1. 割接前1天向客户获取割接设备临时用户名和密码，用于修改割接设备的配置文件。迁移完成后通知客户更改用户名和密码。
2. 获取新的管理IP地址段，确保华为交换机在迁移前能够上线。
3. 如果需要研发/总部远程支持，需要提前1天确认如何远程登录（带外拨号/公网telnet/other），修改设备上的登录控制列表（telnet ACL），并测试远程登录。同时，需要获得客户授权进行远程登录和数据处理。

### 10.3.7 数据备份和流量采集

1. 迁移前备份配置文件、路由和相关协议状态。
2. 提前3天采集关键接口（如上行口）的收发流量数据，用于与迁移后流量数据对比。
3. 白天采集网络流量，用于与迁移后网络流量对比。

上述流量数据可以从网管获取。

### 10.3.8 网络冻结

1. 协调客户在搬迁前2天完成网络半冻结。半冻结期间，所有业务/网络变更需要客户维护部门详细记录，并及时邮件知会华为，以便调整迁移计划和相关配置。
2. 协调客户在搬迁前3天完成网络冻结。冻结期内，不得进行业务/网络变更。如因特殊原因需要变更，需尽快邮件知会华为。
3. 华为应根据变更细节调整迁移计划，并在迁移前2天提交客户相关部门审批。

### 10.3.9 设备信息收集与测试

测试目标	测试命令	测试结果
收集设备信息 (Cisco)	show running-config	OK
	show ip route summary show ip route show ip route static	OK
	show standby brief show standby	OK
	show ip arp show mac address-table	OK
	show interface summary show interface show ip interface brief	OK
	show version	OK
	show module	OK
	收集设备信息 (Huawei)	display current-configuration
display ip routing-table statistics display ip routing-table		OK
display vrrp brief display vrrp		OK
display arp display mac-address		OK
display interface display interface brief display ip interface brief		OK
display version		OK
display device display memory display cpu-useage		OK
采集网络信息		执行show interface命令采集流量信息
	ping业务网段IP地址，观察时延	OK
	trace业务网段IP地址，观察trace信息	OK



### 10.3.10 业务验证和测试

迁移前，客户需要准备待测试终端，并按照如下业务验证和测试项目检查所有业务是否正常。

序号	测试项目	测试工具	测试方法	预期结果
1	打印业务	打印机	打印测试	正常
2	电子邮件	Outlook	发送电子邮件	正常
3	其他哑终端 (IOT, VR, etc.)	TV	哑终端关联网络	正常
4	办公桌/会议电话	IP phone	发起语音呼叫	正常
5	WLAN业务	Huawei P30 Phone	使用手机关联无线网络	正常
6	会议业务	平板电脑	预定会议	正常
7	.....	.....	.....	.....

## 10.4 搬迁步骤

迁移分两个阶段完成：

阶段一：将新核心网除上行链路外的所有业务全部割接到IT办公核心网，并开启华为AP的无线射频，关闭思科AP的无线广播。

阶段二：将核心/汇聚上行链路从华为新核心割接到IT办公核心，并开启华为AP的无线射频，关闭思科AP的无线广播。

搬迁的关键步骤如表10-2所示，在搬迁过程中需要详细记录各个步骤的操作结果。

表 10-2 搬迁步骤

时间	动作	操作步骤	预期结果及验证方法	结果确认
第一天 9:00-10:00	迁移前数据备份	参考 <b>10.3.9 设备信息收集与测试</b> 采集近端设备的配置、版本、路由表、CPU、内存、接口出入流量数据； <b>设备配置、路由表、CPU、内存、远端接口入方向和出方向流量数据</b> 。	数据备份成功。	OK
第一天 10:00-11:00	迁移前业务验证	参考 <b>10.3.10 业务验证和测试</b> 进行迁移前业务验证，ping和跟踪关键服务器及业务测试。	业务验证成功。	OK

时间	动作	操作步骤	预期结果及验证方法	结果确认
第一天 11:00- 18:30	区域A接入交换机下行割接	<ol style="list-style-type: none"> <li>1. 根据端口映射表，将接入交换机下行端口业务迁移到华为接入交换机对应端口。</li> <li>2. 检查接入业务是否正常。</li> <li>3. 将区域A的AP上行割接到对应的华为AP上。原AP下线。</li> <li>4. 检查华为AP是否在线。</li> </ol>	<b>display interface brief</b> <b>display interface</b> <b>display mac-address</b> <b>display ap all</b> 接入交换机下行正常，端口UP，MAC学习正常，AP正常上线。	OK
第一天 18:30- 22:00	区域B接入交换机下行割接	<ol style="list-style-type: none"> <li>1. 根据端口映射表，将接入交换机下行端口业务迁移到华为接入交换机对应端口。</li> <li>2. 检查接入业务是否正常。</li> <li>3. 将区域B的AP上行割接到对应的华为AP上，原AP下线。</li> <li>4. 检查华为AP是否在线。</li> </ol>	<b>display interface brief</b> <b>display interface</b> <b>display mac-address</b> <b>display ap all</b> 接入交换机下行正常，端口UP，MAC学习正常，AP正常上线。	OK
第一天 22:00- 24:00	WLAN业务迁移	<ol style="list-style-type: none"> <li>1. 华为与思科核心/汇聚交换机互联链路上开启WLAN业务和管理VLAN。</li> <li>2. 检查WLAN业务是否正常。</li> </ol>	WLAN业务正常，用户可以搜索到SSID并接入网络。	OK
第二天 9:00-1 0:00	迁移服务器服务	<ol style="list-style-type: none"> <li>1. 根据端口映射表，将现网到核心/汇聚交换机的服务器链路割接到华为核心/汇聚交换机。</li> <li>2. 根据业务测试方案，检查服务器业务是否正常。</li> </ol>	<b>display interface brief</b> <b>display interface</b> <b>display mac-address</b> 端口状态正常，链路状态正常。	OK

时间	动作	操作步骤	预期结果及验证方法	结果确认
第二天 10:00- 13:30	迁移 Internet 区服务	<ol style="list-style-type: none"> <li>1. 将到Internet区交换机的链路割接到华为Internet交换机上。检查链路状态是否正常，MAC地址表是否正常。</li> <li>2. 关闭核心/汇聚交换机与现网接入交换机ACC-05之间的链路。</li> <li>3. 将Internet链路从接入交换机ACC-05割接到华为交换机。检查链路是否正常，Internet出口是否正常。</li> <li>4. 在华为核心/汇聚交换机与Internet交换机之间的链路上启用Internet业务VLAN。检查路由表是否正常，Internet业务是否正常。</li> </ol>	<b>display interface brief</b> <b>display interface display mac-address display ip routing-table</b> 端口状态正常，链路正常，上网业务正常。	OK
第三天 20:30- 21:00	核心/汇聚交换机上行链路迁移	<ol style="list-style-type: none"> <li>1. 关闭华为核心/汇聚交换机与思科核心/汇聚交换机之间的临时链路。</li> <li>2. 根据端口映射表，将现网核心/汇聚交换机上行链路割接到华为核心/汇聚交换机。</li> <li>3. 检查链路状态是否正常，STP状态是否正常。</li> </ol>	<b>display interface brief</b> <b>display interface display stp bridge</b> 端口状态正常，链路状态正常，STP状态正常。	OK
第三天 21:00- 21:30	完成核心/汇聚交换机的配置	<ol style="list-style-type: none"> <li>1. 根据VLAN表，使能各业务和管理VLAN对应的VLANIF。</li> <li>2. 检查路由表、VRRP状态、MAC地址表。</li> </ol>	<b>display interface brief</b> <b>display mac-address display ip routing-table display vrrp binding admin-vrrp</b> 所有业务正常。	OK

## 10.5 回退计划

故障处理包括现场处理和回退计划。每一个步骤，以及它的失败处理，都需要经过详细思考和测试。根据迁移计划的规模、重要性和复杂性，对迁移计划进行调整。同

时，需要考虑故障的处理时间，并纳入计划。每一步执行完成后，确认结果并填写备注。

在风险分析阶段，对迁移阶段高风险步骤进行优先级排序，在制定回退计划时针对这些关键步骤制定回退计划。

动作	操作步骤	预期结果及验证方法	结果确认
回退接入交换机业务	将接入交换机上的用户下行割接回原思科交换机。	接入交换机链路状态和业务正常。	迁移期间一切顺利
核心/汇聚交换机业务回退	<ol style="list-style-type: none"> <li>1. 关闭华为为核心/汇聚交换机与现网核心交换机的互联端口。</li> <li>2. 将核心/汇聚交换机上行割接到思科核心/汇聚交换机。</li> </ol>	现网核心/汇聚交换机的路由表、MAC表、HSRP状态正常。	迁移期间一切顺利

## 10.6 搬迁后验收

### 搬迁后数据备份

参考[10.3.9 设备信息收集与测试](#)采集近端设备的配置、版本、路由表、CPU、内存、接口出入流量数据；设备配置、路由表、CPU、内存、远端接口入方向和出方向流量数据。

### 搬迁后业务验证

参考[10.3.10 业务验证和测试](#)进行迁移后业务验证，ping和跟踪关键服务器及业务测试。

同时参考下表进行业务可靠性测试：

序号	测试项目	测试方法	操作及预期结果
1	接入设备链路可靠性测试	关闭接入交换机与核心/汇聚主交换机之间的链路。	业务切换到核心/汇聚交换机备链路，业务运行正常。
2	核心/汇聚设备链路可靠性测试	关闭核心/汇聚交换机与主核心交换机之间的链路。	业务切换到备用核心交换机链路，业务运行正常。
3	WAC可靠性测试	关闭主用WAC。	AP在备WAC上线，业务运行正常。
4	核心/汇聚设备可靠性测试	关闭主核心/汇聚交换机。	业务切换到备核心/汇聚交换机，业务运行正常。
5	电源可靠性测试	双电源设备，拔下其中任意一个电源。	设备运行正常。

## 10.7 现场支持计划

搬迁后5个工作日内，保障团队在客户现场处理突发事件。主要工作如下：

1. 通过CampusInsight监控网络状态。
2. 登录各设备，每2小时采集一次硬件状态、路由表、MAC表、接口状态等信息。

序号	需要收集的数据	指令	描述
1	设备运行状态	<b>display device</b>	检查主控板和业务板状态，检查主控板、业务板、电源和风扇模块是否运行正常。
2	告警信息	<b>display alarm active</b>	收集设备告警，确认主控板和业务单板是否运行正常。
3	CPU利用率、内存利用率	<b>display cpu-usage</b> <b>display memory-usage</b>	收集CPU利用率和内存利用率。
4	端口信息	<b>display interface</b> <b>display interface brief</b> <b>display ip interface</b> <b>display ip interface brief</b> <b>display current-configuration interface</b>	收集所有接口的状态和光功率。
5	路由信息	<b>display ip routing-table</b>	收集路由表。
6	MAC信息	<b>display mac-address table</b>	收集MAC表。

3. 分析上述信息，检查是否存在网络问题，如果存在问题，则在现场进行处理。