学习推荐

- 华为培训与认证官方网站
  - http://learning.huawei.com/cn/
- 华为在线学习
  - https://ilearningx.huawei.com/portal/#/portal/ebg/26
- 华为职业认证
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_31&lang=zh
- 查找培训入口
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_trainingsearch&lang=zh

更多信息

- 华为培训APP

华为认证系列教程

HCIP-Routing & Switching-IEEP

华为认证数通资深工程师 - 部署企业级网络工程项目

华为技术有限公司

版权声明

华为认证系列教程

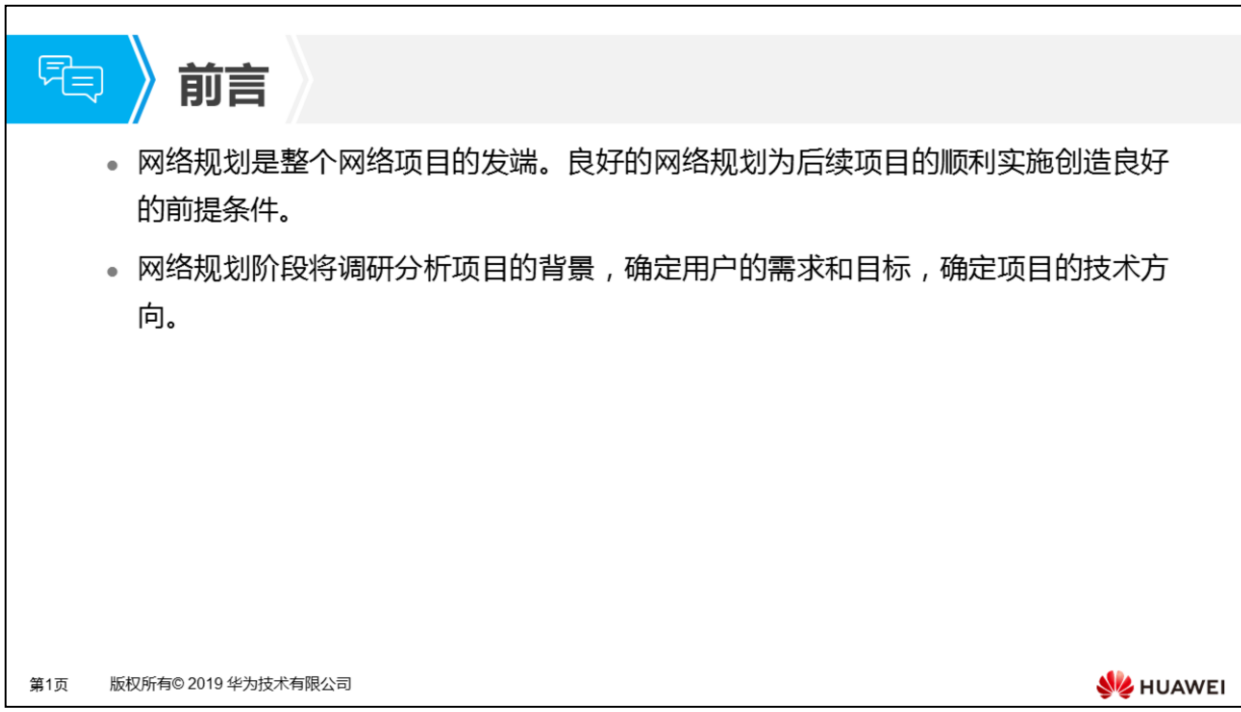
HCIP-Routing & Switching-IEEP

第 2.5 版 本

目录

网络规划

HUAWEI

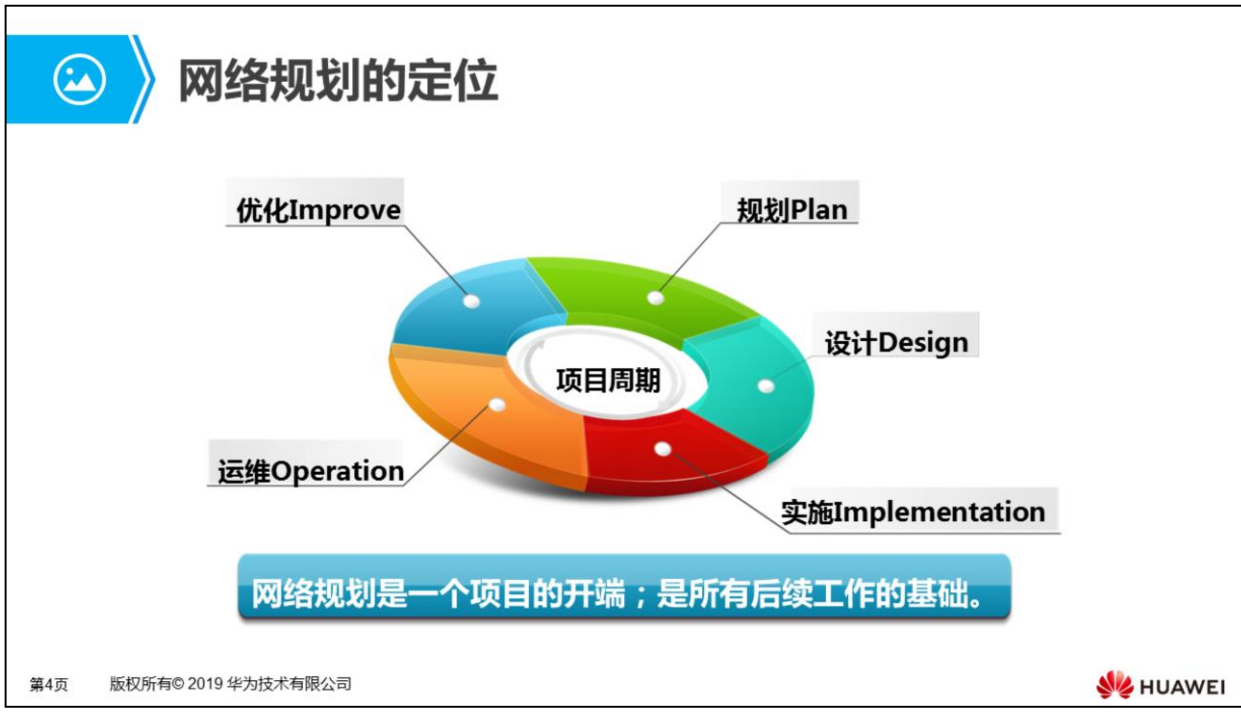


- 网络规划阶段的主要工作是调研分析项目的背景，确定用户的项目需求，确定项目的整体技术方向。
- 规划阶段从宏观的角度对项目进行评审，具有一定的抽象性，在该阶段一般不涉及到具体的技术。但是规划阶段的工作为整个项目建立了一个框架，今后的工作就是在这个框架的指导下充实各部分细节并落实具体的工作内容。
- 规划阶段确定工作的整体方向，直接影响到项目的成果。

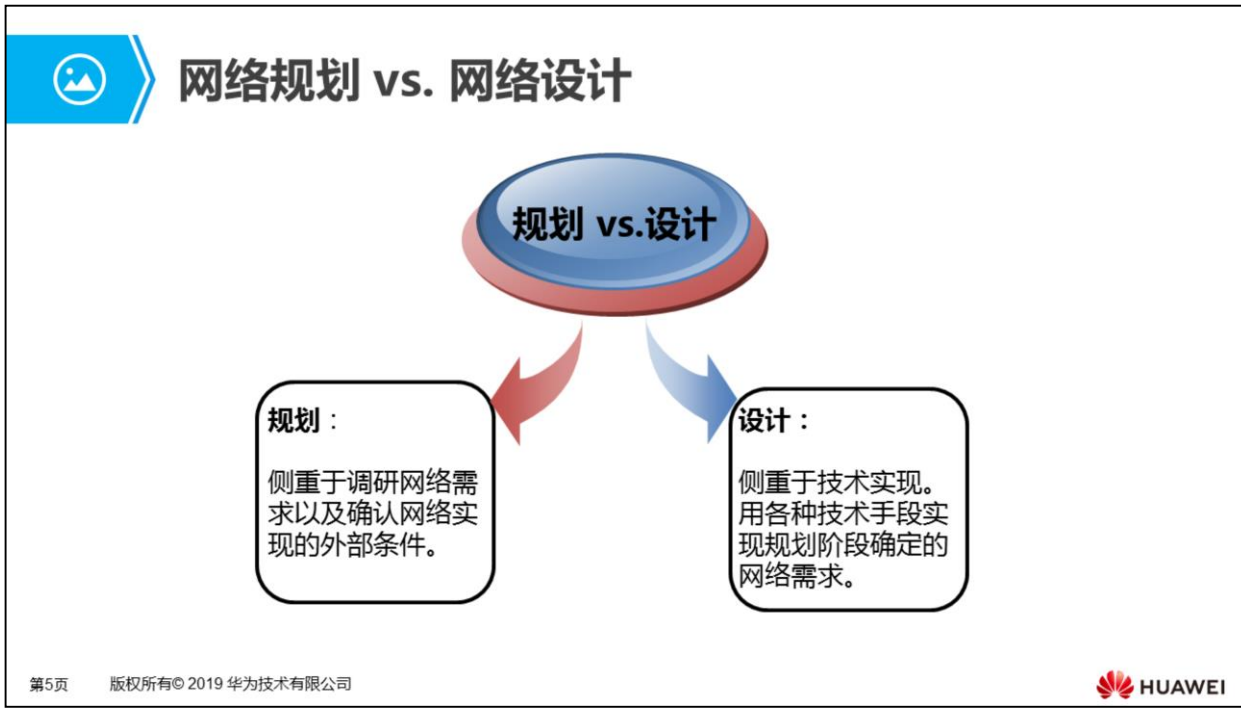
目标

- 学完本课程后，您将能够：
  - 了解网络规划的内容
  - 掌握网络规划的方法
  - 正确进行网络规划

目录



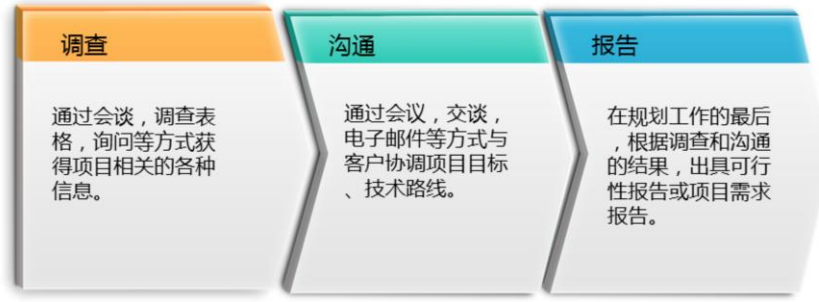
- 网络规划是一个项目的起点，完善细致的规划工作将为后续的项目具体工作打下坚实的基础。具体的工作内容如下：
  - 确定网络项目的目标是网络规划阶段最基本的工作内容。这个最终确定的目标必须是明确的，可量化的，而且是可实现的，不能够是一个笼统的，模糊的，大而化之的概念。
  - 在项目规划阶段需要调查掌握项目的背景。为项目实施提供良好的外部条件，保证项目的顺利推进。
  - 在项目规划阶段需要明确网络项目的实施工作范围，这是项目的预算，资源的调配的前提条件，也是与项目配套工程和相关系统的职责边界。
  - 需要根据项目目标，工程范围，工作内容等各方面的内容制订项目的预算。
  - 在项目规划阶段需要明确网络设计的指导思想，为后续的网络设计提供指导和依据。
- 对于大型的，创新型的网络工程项目，在网络规划阶段还需要进行可行性研究。对项目的经济性和准备采用的技术进行分析论证，保证投资的效益，保证整体项目的成功。



- 网络规划和网络设计是一个项目最开始的两个工作阶段，这两个阶段常常会引起混淆。事实上，规划阶段的工作更加宏观，更注重于要做什么和做这些需要什么条件，在怎么做上仅仅指出总体的技术方向；而设计阶段的工作则更关注具体的技术与实现细节，注重点在于怎么做。
- 规划和设计在总体上有一个前后次序，但是在实际工作中两者结合还是比较紧密的；譬如项目的预算，项目周期，人员的安排属于项目规划，但是它们都与后期具体的项目设计和操作有一定的关系，所以在规划阶段会涉及到后期具体实现的初步估计。

- 在网络规划阶段需要掌握项目背景和外部条件。网络项目并不是一个孤立的系统，它需要为业务服务，需要有相关的配套设施，实施过程中需要相关系统的管理维护人员的配合和协助，项目成果获得最终用户的肯定，所以在规划阶段需要调查确定相关背景和外部条件的详细情况，为今后项目的顺利实施打下良好的基础。
- 网络规划阶段要厘清客户的具体需求。客户在大多数时候只是有一个模糊的、笼统的设想，并不能够全面、精确、详细地描述项目目标。在这个阶段，项目组需要跟客户进行详细深入的交流，正确掌握客户的诉求，为网络设计等后续工作提供准确的目标信息。
- 在网络规划阶段虽然不进行详细的技术设计，但是需要跟客户沟通确定技术的方向与路线，明确客户的技术倾向，掌握客户的重大关切点和禁忌，避免在后续设计中走弯路，浪费时间和人力等资源。

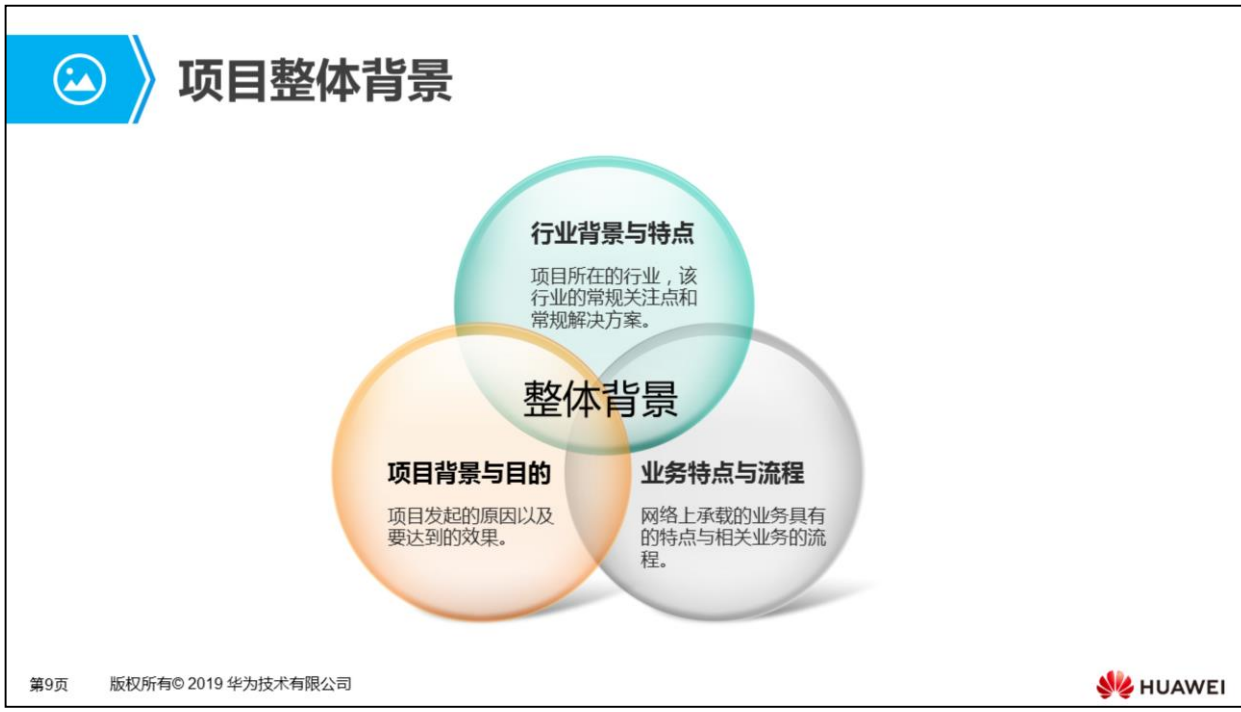
网络规划工作的方式



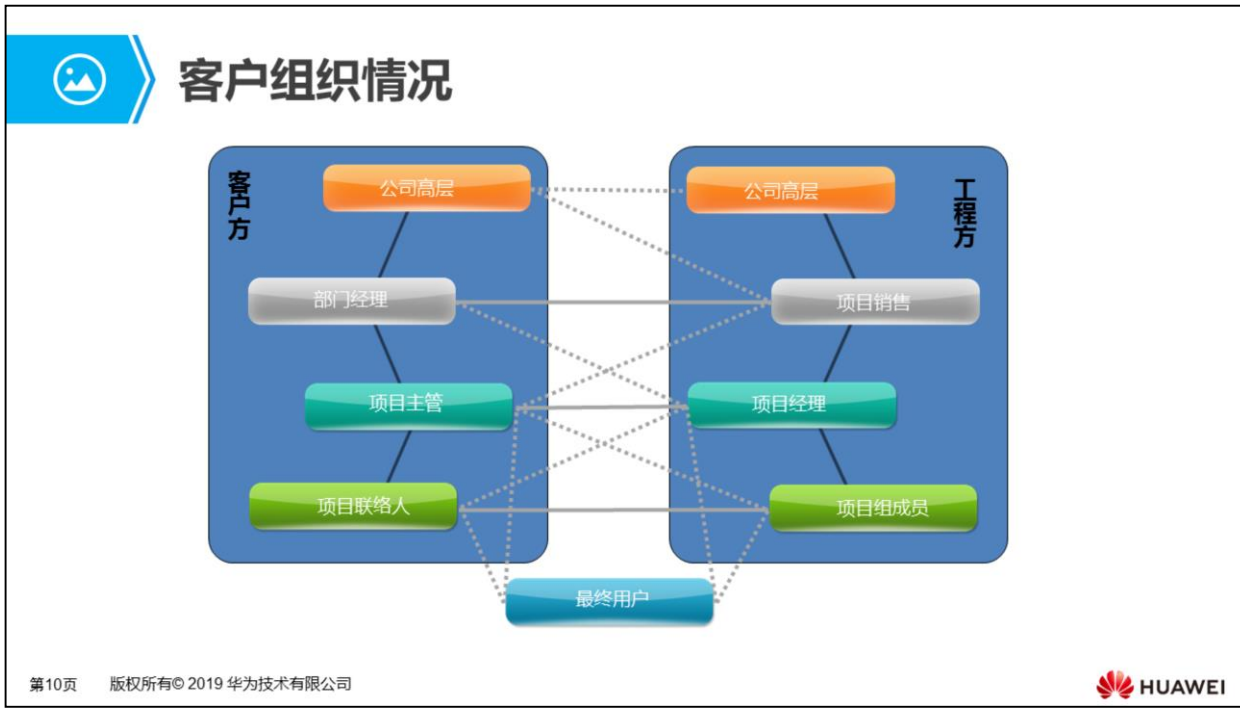
HUAWEI

- 网络规划阶段的主要工作方式是调查，通过调查获取各种项目相关信息。具体的调查方式可以采用与客户交谈，询问相关信息，这种方式客户感知较好，可以灵活设置话题，但是工作量较大，时间协商难度较大，一般针对客户中的重点人物采取这种方式；另外，还可以采用表格的方式进行调查，这种方式需要预先设计问题，但是调查对象的覆盖面会比较广。当然也可以采用电子邮件，即时通信工具等方式进行调查，但这些方式相对不正式，建议在与客户的交往有一定的深度后，作为项目调查的补充方式。如果为了深入了解客户的业务流程，网络需求和当前痛点，也可以考虑跟客户共同工作一段时间，以掌握跟项目相关信息的第一手资料。
- 在取得关于网络项目的各方面信息之后，需要对这些信息进行初步的分析，考虑各个需求的可实现性和相互之间的关系。譬如网络性能与项目经济性、网络的安全性与使用的便利性等相互之间的平衡与妥协。对这些需求的分析结果需要与客户分析讨论，对侧重点和妥协方式取得共识。另外，还需要同客户沟通确认项目实施所必须的一些前提条件，譬如进入机房的手续，环境配套的需求等，提前做好相应的准备工作，便于后续施工的顺利推进。
- 在规划阶段的最末，需要对规划阶段所取得的原始资料以及共识做一个归纳总结，以报告的形式知会客户与项目组成员。该报告将作为项目组的今后工作的目标，以及与客户协调后续工作的基准。

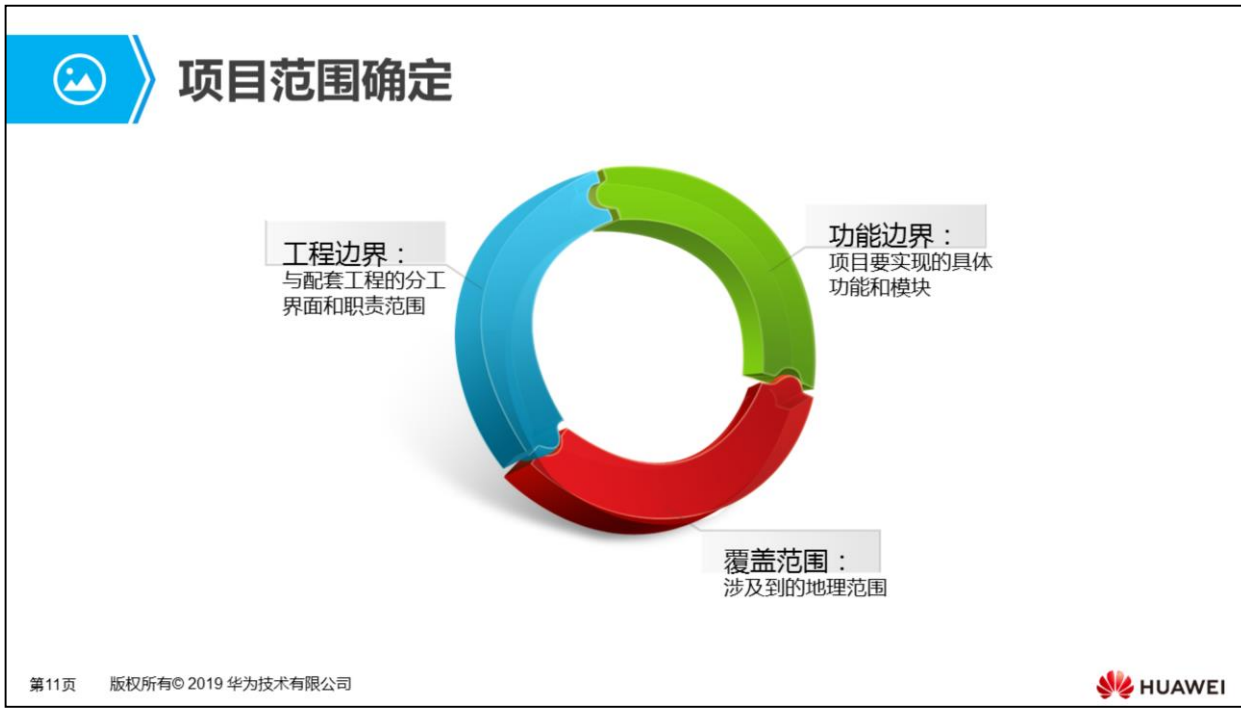
目录



- 在进行项目需求调研前，先对项目的背景进行一定的了解，在此基础上进行调查可以有的放矢，在调研的时候避免一些常识性错误，也能够给客户留下一个好印象。
  - 网络发展到今天，已经渗透到各行各业当中，成为公司业务的一个有机组成部分。因为各个行业的业务都有自己的特点，所以相应的网络解决方案也会有相应的差异。了解项目所处的行业，掌握各个行业的特点和当前行业中的典型解决方案，可以作为后续工作的一个参照。
  - 在正式开展项目前，与公司的销售人员合作，掌握客户启动该项目需要达到的目的。这样在后续工作开展时可以抓住关键，紧密围绕核心目的展开工作。在具体工作中，也可以灵活操作，优化某些细节以达到节约投资，提高效率的结果。
  - 企业的网络，一般都是用来承载具体的企业业务的。对这些业务进行基本的了解，掌握这些业务的数据流向和数据流的特点，能够在后续的设计及实施中提出有针对性的解决方案，规避风险。



- 客户作为一个组织，有众多的部门和人员。对于一个具体的项目，各个部门因为立场的差异，会有不同的意见。在项目前期对客户的组织结构进行大概的了解，掌握相关人员对项目的诉求差异，这样在推进具体工作时，能够抓住关键，做出正确的决定。
  - 在项目启动后，客户一般也会成立一个项目组，组内最主要的两位是项目主管和项目联络人。项目主管一般负责技术性工作，譬如技术方案的确定等；项目联络人一般负责事务性的工作，譬如接待工程人员出入工作场所等。在规划设计阶段，一般跟项目主管沟通交流比较多，在项目实施阶段，跟项目联络人的接触比较多。在一些小项目中，这两个角色可能由同一个人承担。
  - 项目的商务决策一般由客户单位中更高层级的人员负责，也许是项目部门的部门领导，或者分管该部分工作的高层领导。这个层面的沟通一般由销售人员或项目实施单位的高层领导负责，技术人员掌握基本情况主要是为了在某些特殊情况下避免出现不可控的意外。
  - 项目的最终用户，一般与客户的项目组成员并非同一组人；或者可以说最终用户常常也是客户项目组的客户，取得最终用户的认可是客户和实施方两个项目组共同的目标。
- 网络项目在各个工作阶段会涉及到客户内部的不同部门和各部门人员；弄清楚客户单位的项目操作流程，掌握各个阶段涉及到的部门和人员，特别是拥有签字权的负责人，在项目的推进过程中取得他们的认可和配合，对于项目有重要意义。



- 在项目规划阶段，需要确定项目的范围，后续的很多工作都是基于这个范围进行评估的，譬如整个项目的工作量，项目的预算等。从细的方面来说，项目的范围还可以从三个方面进行界定：
  - 覆盖范围：首先是网络的延伸范围。譬如要确定需要建设的网络究竟是一个全国性的网络还是仅覆盖一个省的网络，具体的延伸范围是到县一级还是要到乡镇级基层单位，这些都是在项目实施之前需要确定的。如果是一个园区网项目，也需要了解网络延伸到那些建筑，每个建筑又有多少信息点位等信息。
  - 工程边界：一个网络工程不可能孤立存在，网络设备的安装需要相关系统的配合，包括机房工程，配套电源，空调系统，弱电工程等，在规划阶段，需要明确项目主体与这些系统的职责和分工界面，避免在后期的工程中出现扯皮现象。
  - 功能边界：当前我们很难遇到一个从零开始建设的网络项目，很多网络的改造项目都是为了实现某个特定的功能需求，譬如接入某个业务系统，优化改造以提高网络的安全性等，在规划阶段需要确认本项目需要实现的功能，而其他相关部分则作为前提或外部条件出现在项目之中。

项目阶段与项目周期

- WBS：工作分解结构（Work Breakdown Structure）
  - 把整个项目分解成较小的，更易于管理的组成部分。
- 甘特图
  - 将分解后的工作活动排序，用图示的方式将活动与时间联系起来。

gantte.jpg

HUAWEI

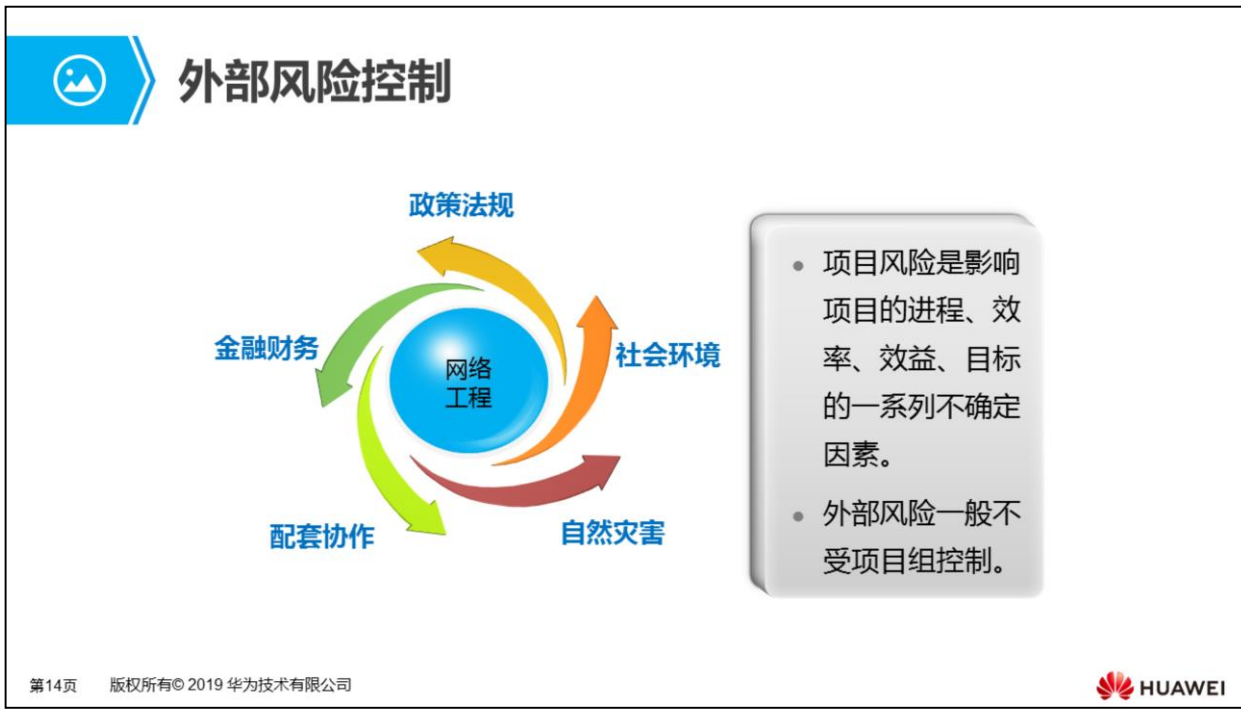
- 一般的项目过程如图所示，整个项目经过立项，规划，设计，实施试运行后验收，进入运维阶段。每一个阶段均有标志性的事件作为该阶段的起点和终点。
- 不同的项目可能会有某些的特殊步骤，但是总的来说，一个项目都要经历这些工作阶段。
- 项目时间安排和管理有一整套系统的方法，最常用的步骤首先要对工作进行分解，然后对每一个工作步骤进行估算，再对各个步骤进行统筹安排，完成工作计划。工作安排常用甘特图的方式进行表示。

项目配套工程

- 不是项目本身，但与项目紧密相关的系统。
- 不需要项目组实施，但是需要项目组关注确认。

  HUAWEI

- 一个网络项目并不能够独立存在，它需要一系列相关系统的配合。这些相关的系统，常常不是网络项目本身需要解决的问题，但是对于网络项目的顺利实施又是至关重要的，所以在网络项目的规划阶段，至少需要划定项目边界，给出清晰的边界条件。
- 对网络工程相关的主要为以下两个方面：
  - 设备安装条件：包括安装空间，供电，空调等。所有网络设备均有提供物理尺寸，功耗，重量，工作温度范围等一系列的参数。安装的机房需要提供相应的条件，包括机房的承重，电力的供应，空气质量要求等。
  - 网络线路：项目中需要使用到的连接线，包括客户自己负责的局域网布线和租用的广域网线路。局域网的布线一搬作为一个独立的弱电工程出现。

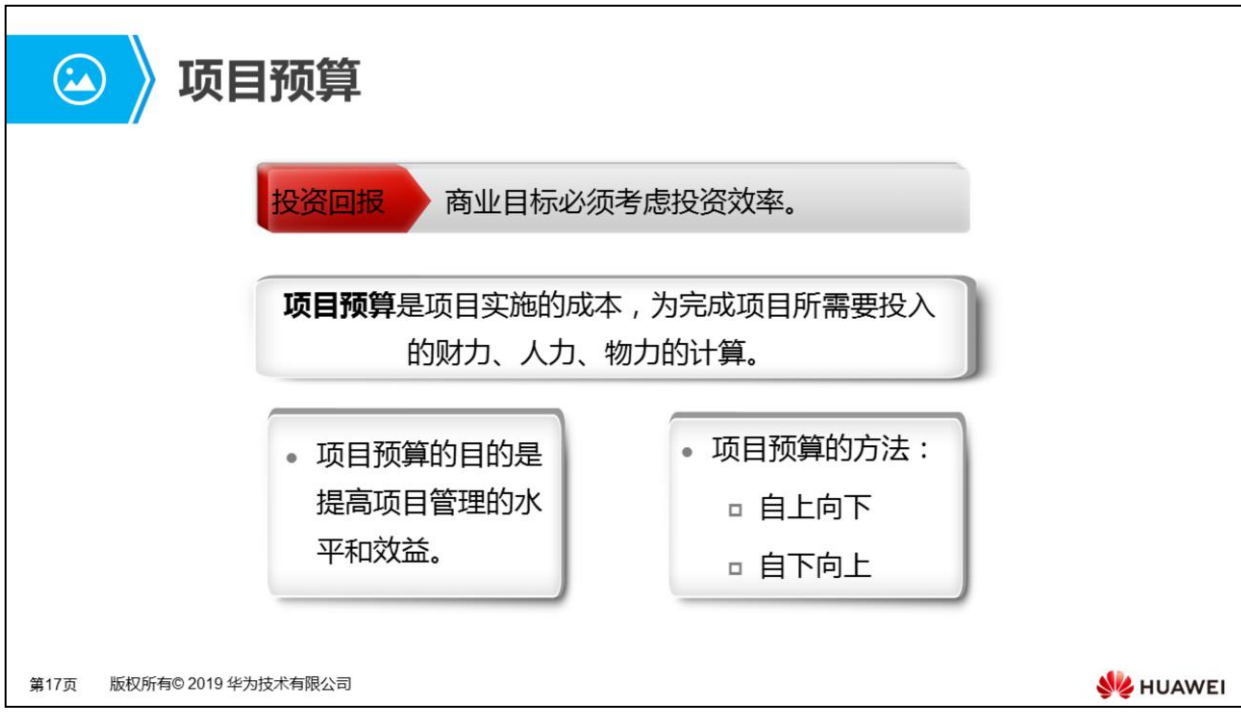


- 项目存在于一个复杂多变的环境中，通常项目组能够控制或影响的仅仅是一些跟项目直接相关的事件，而项目存在的大环境导致的风险对项目组来说只能采用预防规避等方法进行控制。
- 常见的外部风险如下：
  - 政策法规：任何项目都必须遵守政策法规，特别是一些国际性的项目，需要了解并遵守当地的法律法规。同时要注意法律法规的变动情况和当地真实的法律环境。
  - 社会环境：在项目实施过程中，项目组成员要了解并适应当地的社会环境，包括治安情况，宗教信仰，生活习俗以及民众的日常行为方式等。
  - 自然灾害：包括但不限于地震，风暴等各种自然灾害；这些灾害小则影响项目进度，大则毁坏整个项目成果。
  - 金融财务：宏观经济的变化可能会使项目的财务情况发生变化，譬如汇率的变动，国家利率调整以及通胀等因素都会导致项目利润率的变化。
  - 配套协作：项目涉及到的一些外部协作系统，譬如外贸周期问题，配套项目质量工期等问题。
- 在规划阶段，要识别这些风险。采用各种方法，削减这些风险导致项目失败的可能性。譬如在项目的商务合同中，把某些情况归类为不可抗力，作为免责条款出现。或者在项目规划方案中，划分各方职责，提供明确的工程界面和质量要求。

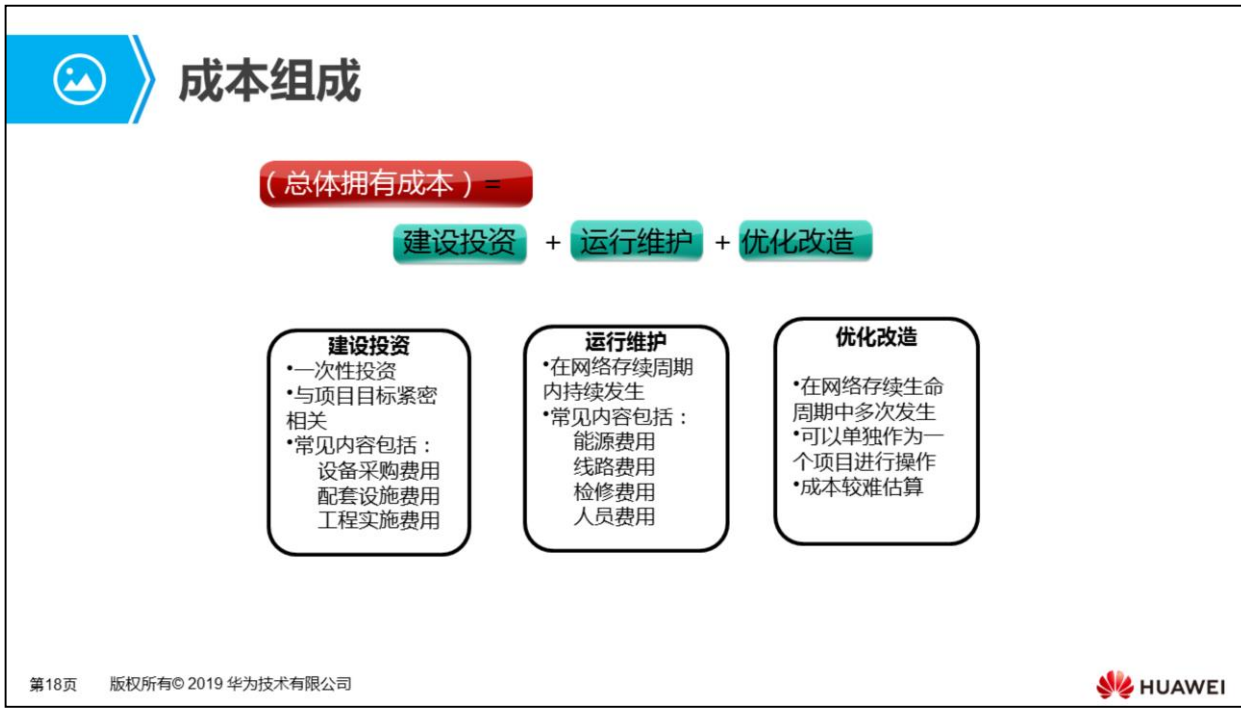
目录

HUAWEI

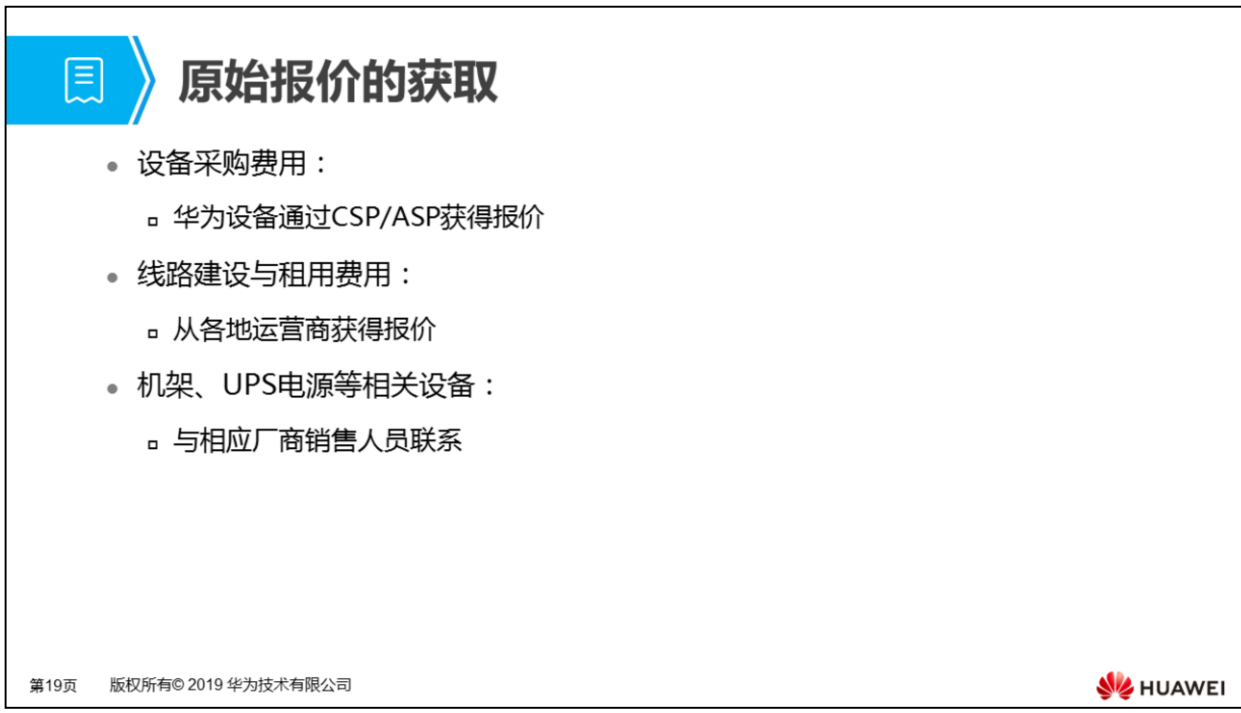
- 网络项目的商业意义是网络项目得以存在的最根本原因。一个项目产生都有来自商业层面的需求：增加利润、削减成本、提高生产效率等均是合理的商业出发点。
- 在规划阶段，明确客户的商业需求，在后续工作中尽量帮助客户达成目的，才是一个项目真正的成功标准。
- 网络项目的典型商业目标举例如下：
  - 削减企业运营成本，提高员工工作效率；
  - 加快业务的处理流程，提高企业的市场竞争力；
  - 支持业务的扩张，网络扩容至新的区域，或者网络扩容到更高的性能；
  - 支持新业务开展，扩展网络功能；
  - 提高网络的可靠性，保证业务的持续稳定；
  - 降低总体通信成本。



- 确定项目预算是项目规划阶段的重要工作。
- 项目预算的精细程度与项目的规划的确定性和精细度紧密相关。
- 确定项目预算对客户来说是财务管理的需要，对目标与成本的绑定有利于控制成本、提高资金的使用效率。
- 预算最常见的方法有两种：
  - 自上而下：基于项目人员的经验和历史数据，对项目成本进行估算。
  - 自下而上：基于具体项目各个部分的费用估算，汇总后得出项目的总费用。



- 网络项目的预算要考虑多个方面，对客户来说，建设并运行一个网络的总体成本主要由以下三方面组成：
  - 建设投资：网络的建设费用属于一次性的投资，这部分的投资与项目目标紧密相关，具体的内容包括：设备采购费用，配套设施的建设费用和工程的实施费用。
  - 运行维护：网络建设完成之后的运行维护需要持续投入，主要的投入能源消耗费用、线路维护费用、设备定期检修的费用和运维人员的费用。
  - 优化改造：在网络存续周期内，一般会经历多次优化改造。包括线路扩容、设备更新升级、加强加固等。这些改造工作也可以单独作为一个项目进行操作。因为后期改造一般基于当时的实际情况开展，在项目最初的建设阶段并不清楚今后会有什么样的改造，所以这部分成本在前期较难估算。



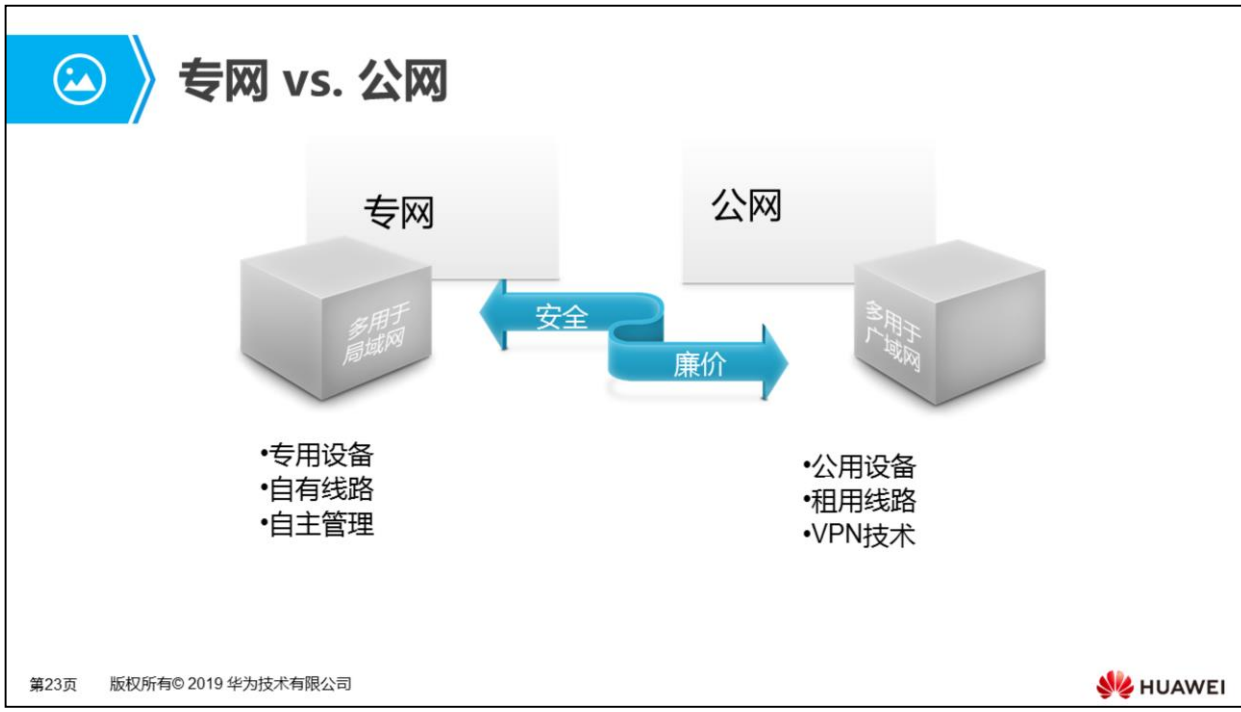
- 建设预算需要获得项目相关费用的原始报价，这个报价可以通过相应渠道获得。
  - 华为产品的采购方式可以登录华为官网查找，官网地址如下：http://e.huawei.com/cn/how-to-buy ；在该页面可以直接在线提交采购需求，也可以查找各地的华为合作伙伴，从合作伙伴处获得报价。
  - 网络工程中的线路建设是成本的一个重要组成部分，局域网部分一般客户是自行布线，那么布线部分将单独作为一个弱电工程出现，作为网络项目的配套项目，由承建方报价。广域网部分一般租用运营商链路，链路类型和价格可以联系当地的运营商，运营商有专门的政企客户部负责这部分的业务接洽。
  - 在网络工程中，客户可能合并采购一些配套设备，譬如机架，电源等；如果客户有这方面的需求，一般项目承建方的做法是接洽相关的厂商，将相应部分的采购与安装调试一并打包给供货商，然后做一个综合的报价。

目录

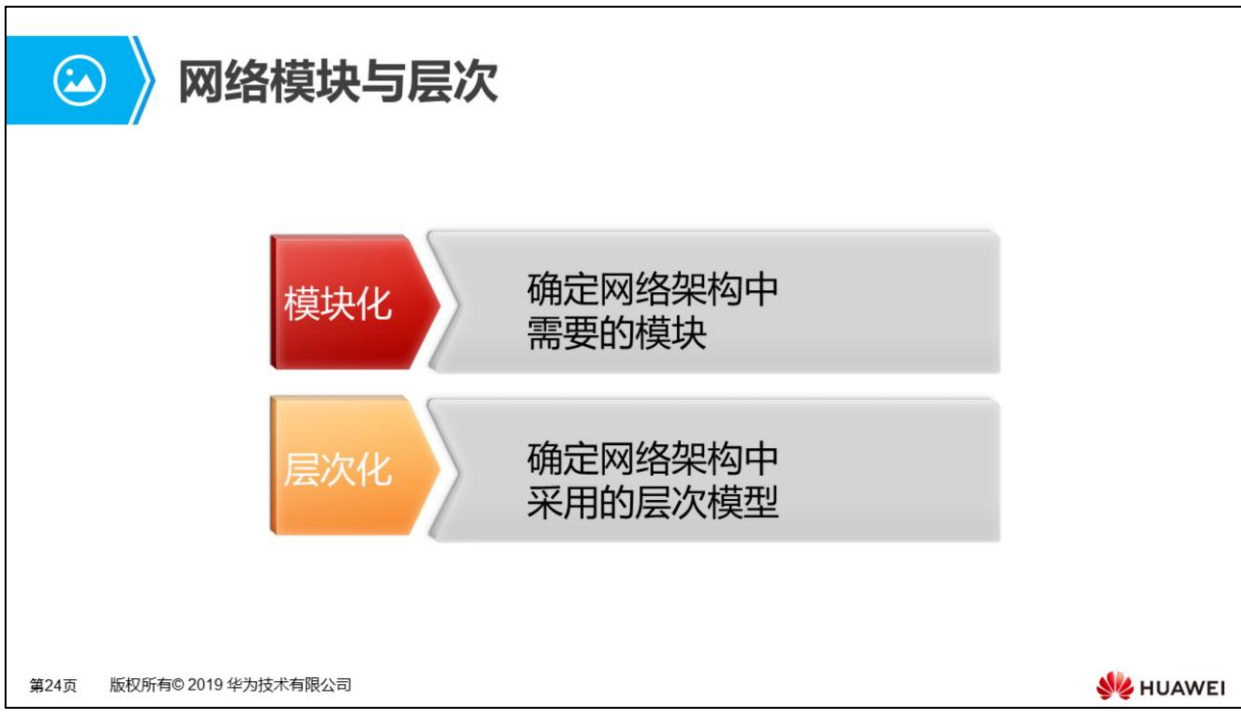
HUAWEI

- 项目目标最终要通过具体的技术来实现。而项目的技术标准在很多时候常常需要与商业目标进行折衷，譬如高性能与成本之间需要平衡。在规划阶段需要考量的技术目标简单罗列如下：
  - 功能：网络需要实现的功能是网络项目最基本的技术目标，所有其他的技术目标都是在网络功能实现了之后考虑的因素。就是因为它重要，所以网络需要实现的功能常常也作为项目目标出现。
  - 性能：网络性能是在网络功能之后的一种重要技术指标。网络的性能包括多个方面，最基本的是网络的吞吐量（带宽），网络的吞吐量在需求侧由网络业务提出要求，在技术侧由线路带宽和设备性能决定。网络的吞吐量要结合网络带宽的利用率综合考量，以保证投资的效率。网络性能还包括网络的延迟，丢包率等参数。
  - 可用性：可用性表示客户对网络故障的容忍度，当客户的业务开展依赖于网络系统的情况下，客户就会对网络的可用性提出很高的要求，譬如要求能够保证日常故障不影响业务。与可用性紧密相关的是可恢复性，是指当网络出现灾难性故障的时候，网络修复的难易程度。
  - 扩展性：基于客户业务在今后几年的扩张计划，在规划的时候需要留有一定的余量，保证在网络的生命周期内能够很好地适应业务增长的需求。扩展性分成两中类型，一种是站点数量的增长，接入用户数量增多；另一种是性能需求增长，业务流量增加。
  - 可实现性：作为一个工程项目，必须要考虑所有需求的合理性和可实现性。要折衷当前业界的技术发展水平和现实的实现能力，不提不切实际的指标和要求，做到可行可实现。

- 要设计出真正符合需求的网络，首先需要对网络即将承载的业务流量有深入的理解，通过对流量特征的分析，能够在满足性能要求的同时提高投资效率。
- 流量特征：
  - 对网络需要承载的业务进行统计，对各个业务的流量路径进行规划测算。
  - 关注网络业务的流量类型，对单播、组播、广播，对系统流量、协议流量和应用流量分别进行归类统计。
  - 综合各种流量的的需求统计，对各网段承载的业务容量进行估算。
- 行为特征：
  - 对最终用户使用网络的行为进行评估。对用户使用的应用类型进行统计和分类，如普通上网业务，P2P应用，终端业务等。
  - 调查明确网络流量的时间曲线，明确流量的峰谷时段和相应时段的流量值。
- QoS需求：
  - 评价不同业务类型对QoS的要求，排列各个业务的优先次序。
  - 确定每种业务的QoS指标，包括带宽，延迟，抖动等方面的要求。
  - 考虑采用何种QoS模型。



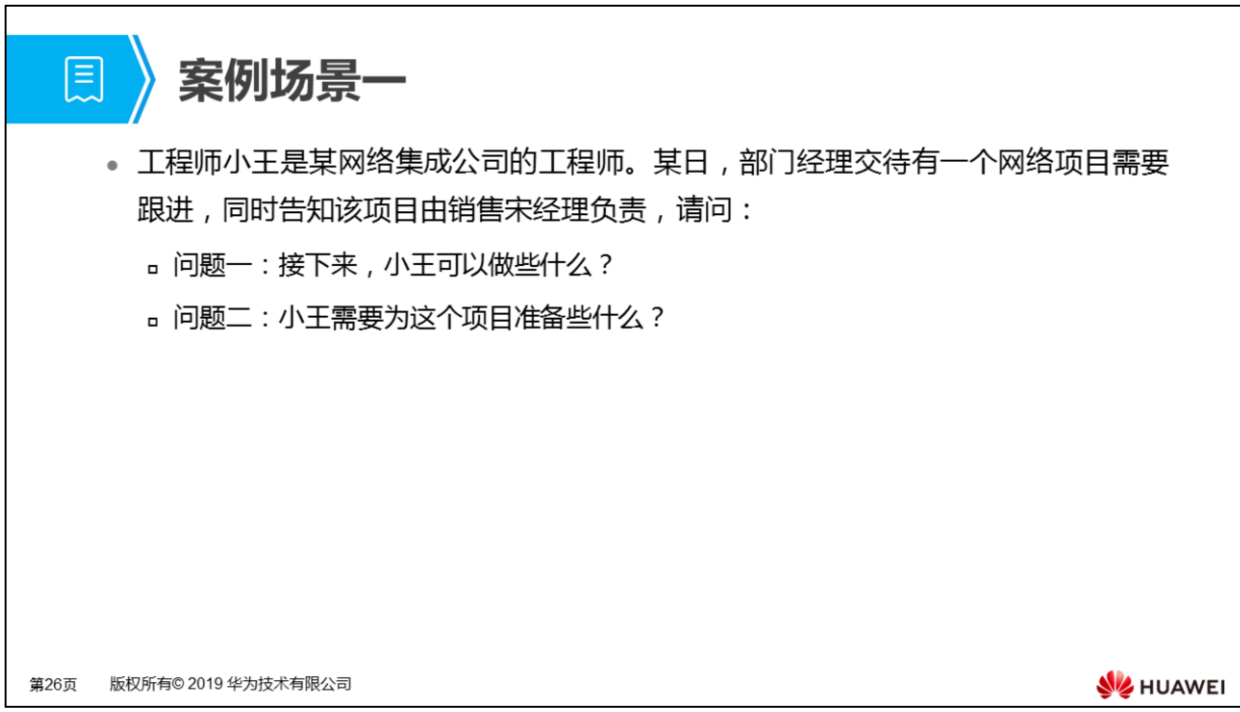
- 在网络规划阶段需要明确建设的网络是专网专用还是搭建在公共的业务平台之上。专网是指客户拥有网络基础设施的全部产权；公网是指客户租用部分公网的设备，或自行在公网上架构虚拟的私有网络。
- 专网最大的特点的安全，可控性好；公网最大的特点是廉价。
- 客户内部的局域网一般采用自建自管的专网方式实现；客户跨越广域的线路，因为成本的关系，一般租用公网线路。
- 一种特殊的公网方式是在公网上利用技术手段架构虚拟的私有网络（VPN），兼顾网络成本和安全性。



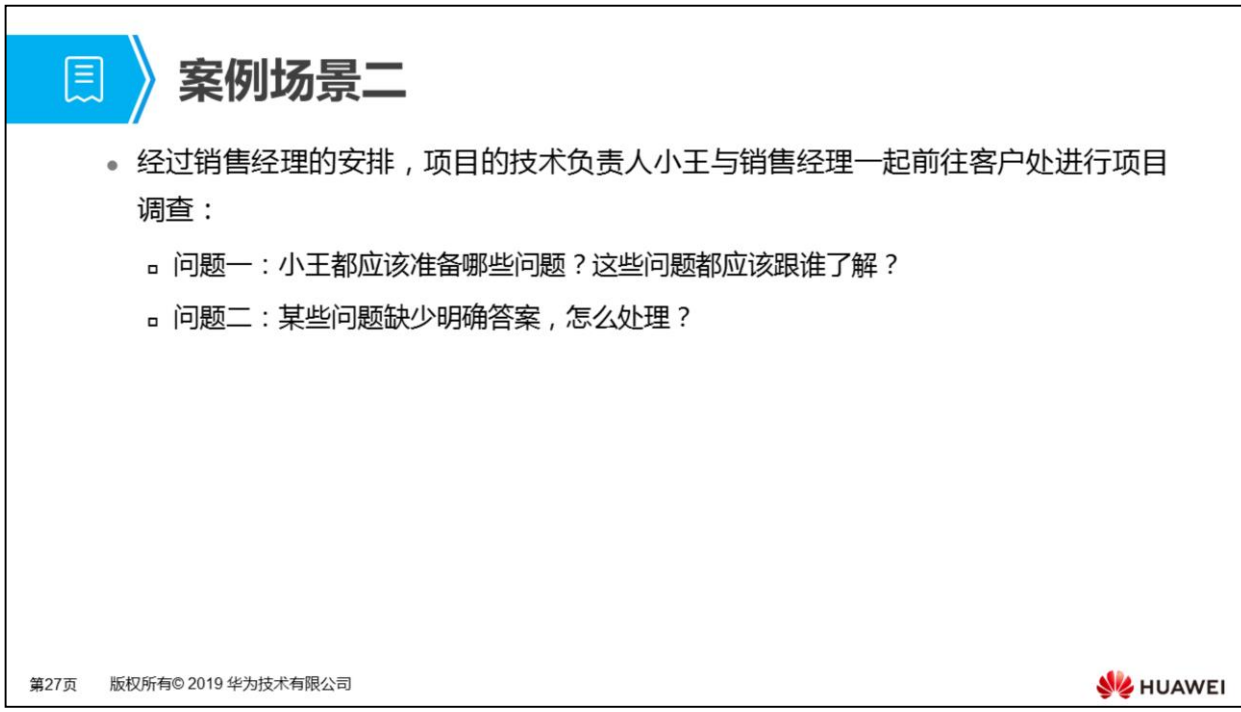
- 当前的网络，基本已经采用了模块化与层次化的设计方式，在规划阶段，需要确定整个网络需要哪些功能模块，同时确定采用何种层次模型。
- 当前网络常见的模块包括：园区网络模块，广域骨干模块，网络出口模块，数据中心模块，无线接入模块等。在具体项目中按照需求对各个模块进行取舍。
- 在各个网络模块内，网络一般采用层次化的设计方式。传统上一般采用三层结构组网；当前开始流行网络扁平化，采用两层结构组网。在网络规划阶段，需要确定采用哪种层次模型。

目录

HUAWEI



- 作为技术工程师，项目信息一般由直管领导分配，当然小型公司可能会有更灵活的方式，譬如会有销售直接搭档技术人员合作项目的做法。
- 销售经理和技术负责人两个人是项目组的最基本搭配，在中小型项目前期一般就是两个人介入，后期按照工作量适当配备人力。在获得项目信息后，负责技术的小王应该同销售经理密切合作，从销售经理出，小王至少可以获得客户的基本信息，从这些信息，小王可以知晓项目最基本的背景，如客户所处的行业、客户启动项目的目的等。因为定位的差异，销售经理一般并不太关注具体的技术实现内容，而且在项目介入的初期，销售经理可能也并不掌握更详细的信息，所以，作为技术负责人的小王需要与销售人员一起，对项目进行深入的跟踪和调研。
- 得到基本的客户信息之后，技术人员和销售经理需要安排对客户的拜访，拜访的日程和人员接洽部分一般会由销售经理负责联系，但是作为技术人员的小王，应该掌握相应的安排情况，同时准备好需要向客户咨询的问题，将这些问题在适当的场合向合适的人员提出来。具体的调研内容如本章正文所述，包括项目背景、项目目标、技术方向等方方面面的细节。



- 在项目进入正式操作阶段的时候，拜访客户基本是项目最基本的操作手段，在整个项目前期，与客户之间会有多次的接洽。前期调研一般也会有多次，第一次调研一般会比较正式，所以在拜访客户前需要做好各方面的准备工作，给客户留下一个好的印象，便于后续工作的开展和推进。
- 总体来说，本章正文中描述的内容在项目规划阶段都应该有所掌握，当然部分内容并不是通过客户调研获得，但是项目目标、项目范围、项目进度、人事组织、配套工程等方面的内容都需要与客户协商确定。一般在客户内部，角色也有分工，客户项目经理会全面协商整个项目，涉及到预算、进度、工程范围等，也许会与更高层的领导协商确定；而项目涉及到的技术细节，网络参数等技术方面的问题，客户项目经理一般会有一定的决定权，而现场随工，材料和资料的交接等环节一般由项目联系人操作。
- 在调研过程中，客户并不一定能够提供现成的答案，有部分可能是因为资料不全，也有部分可能是客户并不了解相关的技术问题。在这种情况下，工程方需要与客户合作，共同寻找问题的答案；如果是技术取向方面的问题，则需要详细解释，给出比较，引导客户做出选择。

思考题

1. 以下哪些项是在规划阶段需要解决的问题？（　　）
   A. 确定技术方案
   B. 了解项目背景
   C. 确定项目需求
2. 以下哪些项属于项目范围需要确定的边界？（　　）
   A. 功能边界
   B. 工程边界
   C. 覆盖范围

- 1、答案：BC。
- 2、答案：ABC。


谢 谢
www.huawei.com

网络设计

HUAWEI

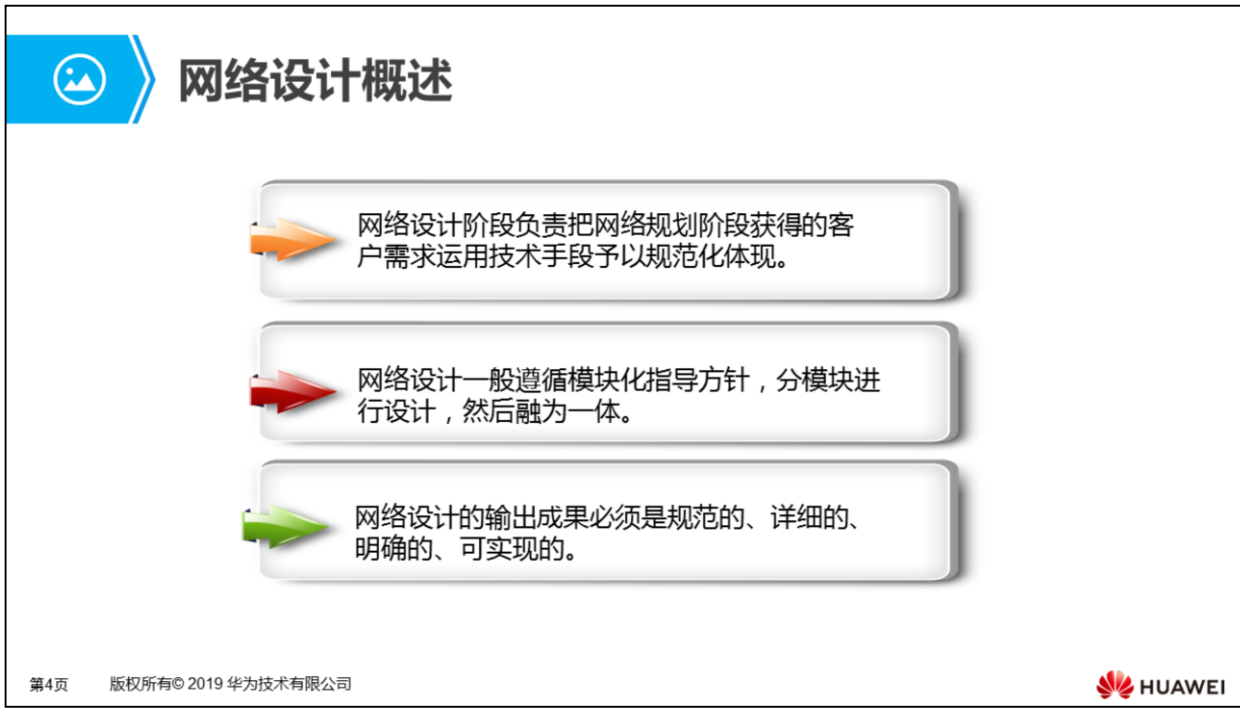
前言

- 在设计阶段，按照规划阶段明确的项目需求和指导思想，对网络进行具体的设计。
- 在设计阶段确定设备选型、技术路线，明确网络功能、性能指标，将需求落到实处。

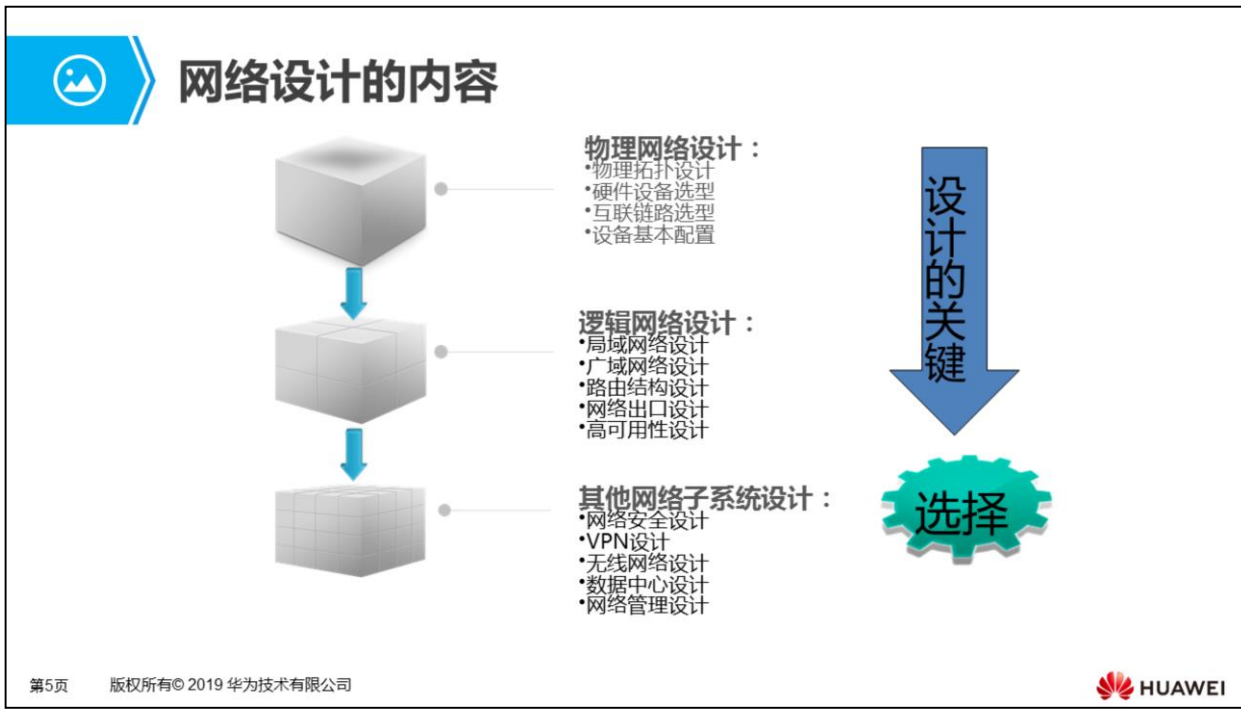
目标

- 学完本课程后，您将能够：
  - 了解常见的网络形态
  - 了解网络设计的各个层次
  - 了解常见的产品与技术
  - 掌握常用协议的优缺点
  - 掌握各技术模块的综合应用
  - 掌握网络设计的方法论

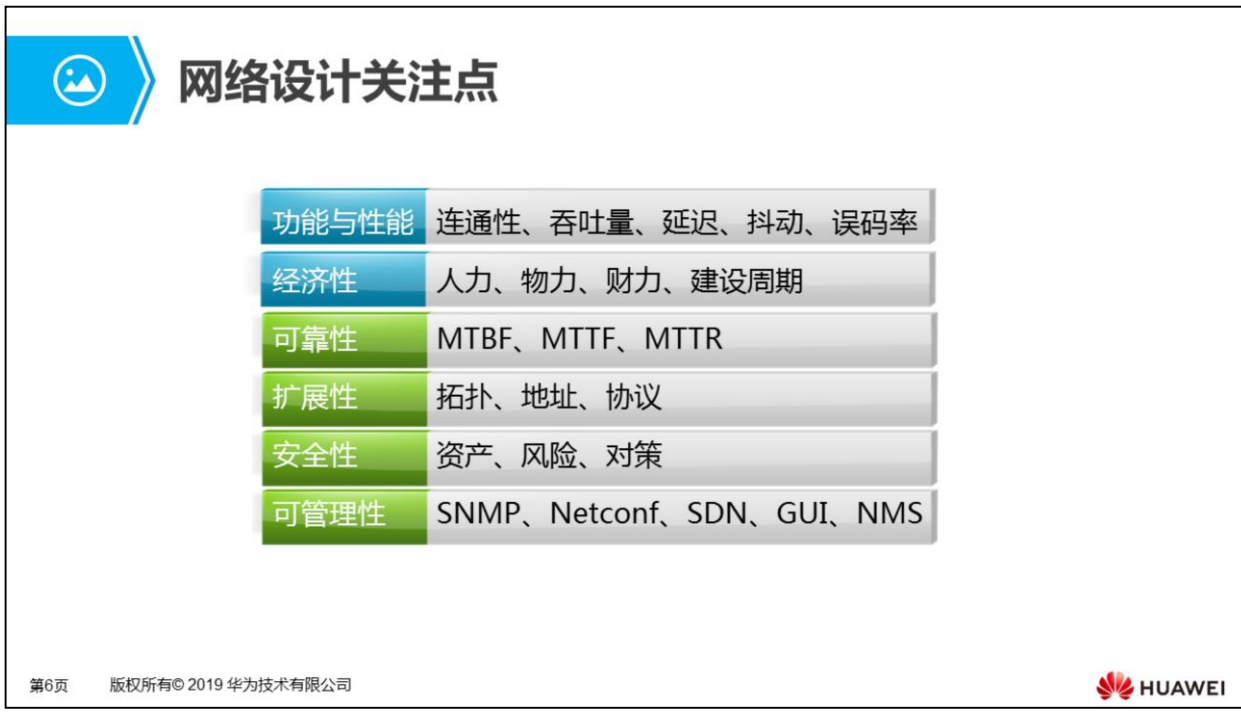
目录



- 网络设计是网络建设项目的第二个阶段，该阶段是在网络规划阶段所获得信息的基础上，用技术手段予以规范化体现。
- 当前，网络设计通常遵循模块化指导思想。在规划阶段确定网络中需要的模块，各模块的具体要求，然后在设计阶段对各个模块进行详细设计。在各个模块内部，常常采用层次化的结构。
- 网络设计的输出成果必须是规范的、具体的、明确的、可实现、可操作的。
- 网络设计对设计人员提出了较高的要求：
  - 设计人员需要熟悉网络产品，能够在方案设计时进行正确选型。
  - 设计人员需要理解各项网络技术，能够在方案设计时进行正确运用。
  - 设计人员需要具备一定的项目经验，了解在项目实施过程中的各关键环节。

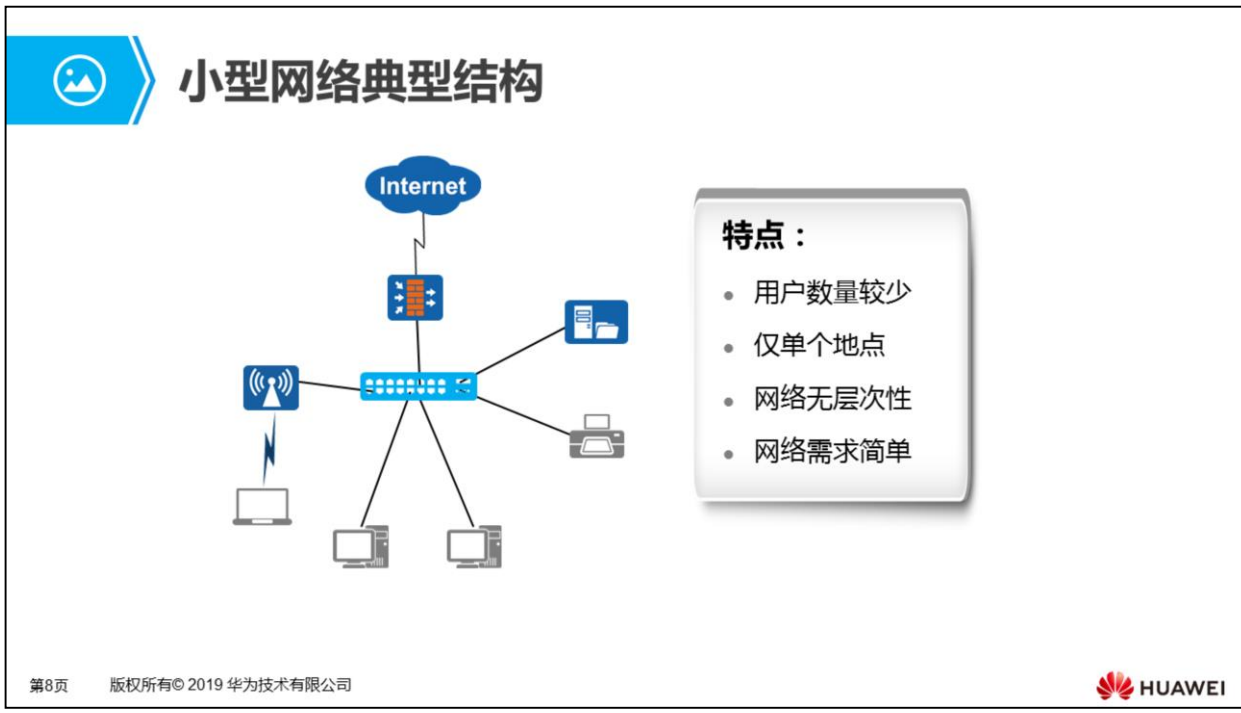


- 网络设计的工作在本章分成三大部分：
  - 物理网络设计：主要包括物理网络拓扑，硬件设备，互联链路等选型相关的部分。这一部分的设计，往往跟项目预算紧密相关，也跟网络性能相关。是整个网络的物质基础，后续所有的设计也建立在这一阶段的设计成果之上。
  - 逻辑网络设计：逻辑网络设计从协议和网络层次的角度对网络进行设计。网络按照工作层次划分为二层网络和三层网络，二层网络按照地域范围又分为局域网和广域网。三层网络的设计基于IP和路由协议。企业网络的出口部分有一些特别的技术，在这里单独讨论。网络设计中的高可用性是当前网络设计中的考虑重点。
  - 其他网络子系统：除了基础的网络架构之外，当前企业网络中还有其他各种子系统，包括网络安全子系统，无线网络子系统，数据中心子系统，网络管理子系统等，这些子系统是当前企业网络中的常见功能模块。



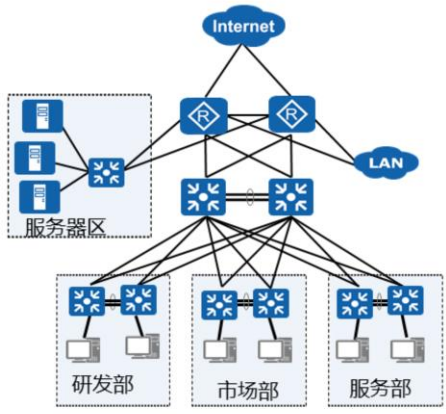
- 网络设计过程中，要始终围绕在网络规划阶段确定的网络需求，选择合适的技术实现，设计的网络方案需要把握以下要点：
  - 高性能：需要与经济性取得平衡。网络的性能常用可用带宽，延迟，抖动，误码率，利用效率等进行描述。
  - 经济性：首先需要遵从客户的预算，在预算范围内提供匹配的解决方案。
  - 可靠性：指网络正常工作的时间占比。跟可用性和可恢复性相关。常常用冗余的方式来提高系统的可用性。
  - 扩展性：指网络适应未来发展的能力。
  - 安全性：网络设计中需要考虑安全性，以提高网络的持续服务能力，防止承载信息的泄密。
  - 可管理性：网络管理包括设备管理，配置管理，故障管理，计费管理等多个方面，当前最常用的基于SNMP的网管系统。
  - 注释：
    - MTBF：平均故障间隔时间。
    - MTTF：平均故障时间。
    - MTTR：平均修复时间。

目录



- 小型网络应用于接入用户数量较少的场景，一般支持几个至几十个用户。网络覆盖范围也仅限于一个地点，网络不分层次结构。网络建设的目的常常就是为了满足内部资源（打印机、文件）共享及互联网接入。
- 当前的网络需求中，连接互联网的需求和提供WLAN无线接入的需求都是很常见的。在小型网络中，往往需要实现这两个功能。
  - 一般直接使用路由器或防火墙连接互联网，并采用地址转换（NAT）方式提供上网服务。
  - 一般直接使用Fat AP设备提供无线接入，采用WEP、WPA等密码验证方式。
- 设备选型方面，一般采用集成上述功能的设备，例如集成了交换、路由、WLAN、xDSL/EPON接入等功能的AR G3路由器。

中型网络典型结构

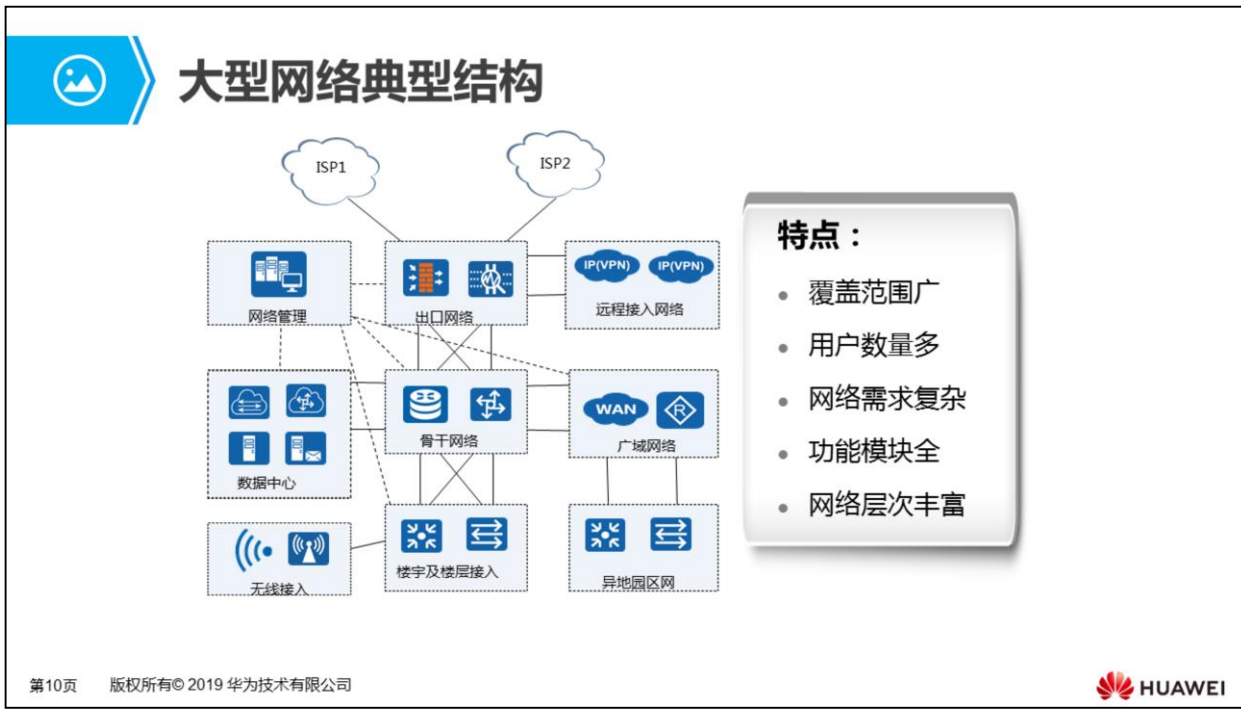


特点：

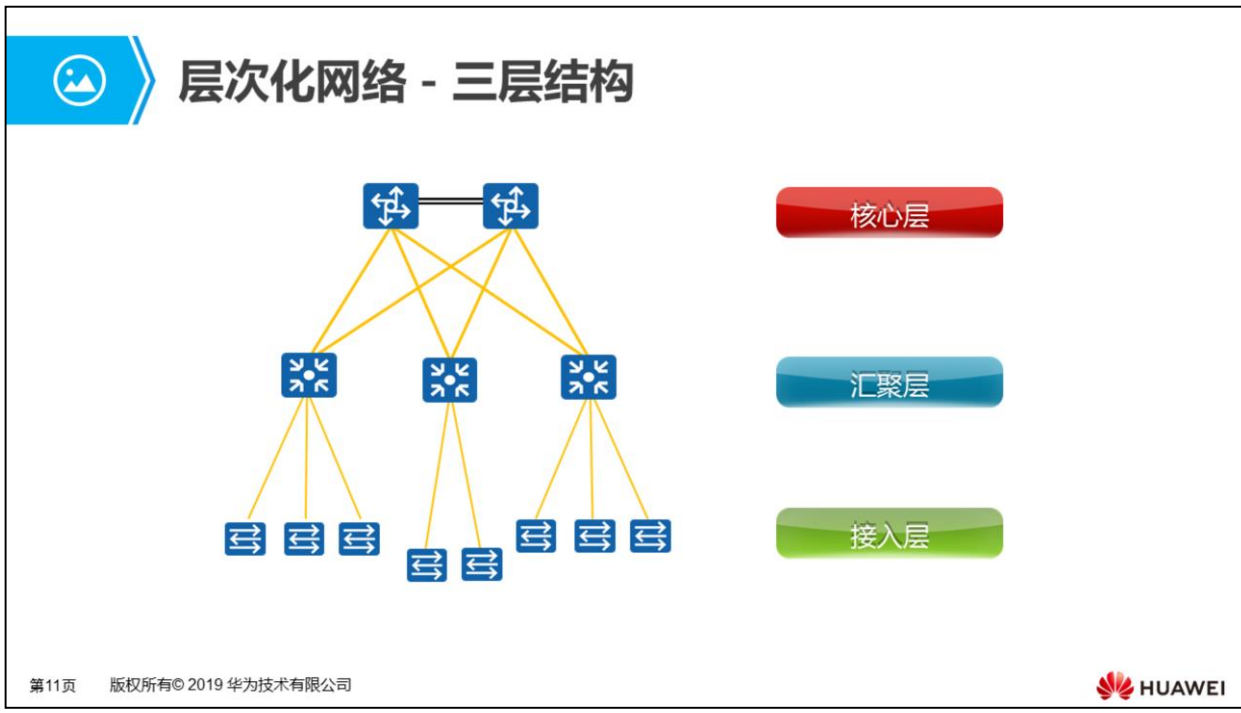
- 规模中等
- 使用场合最多
- 功能分区
- 初步分层

HUAWEI

- 中型网络是日常工程项目中碰到较多的类型，一般企业网络基本都可归入中型网络。中型网络一般能够支撑几百至上千用户的接入。
- 中型网络引入了按功能进行分区的思想，也就是模块化的设计思路，但功能模块相对较少。一般根据业务需要进行分区，并没有一定之规。
- 中型网络因为支撑更多的用户，所以相比小型网络，开始出现分层的设计思路，以提高网络的可扩展性。

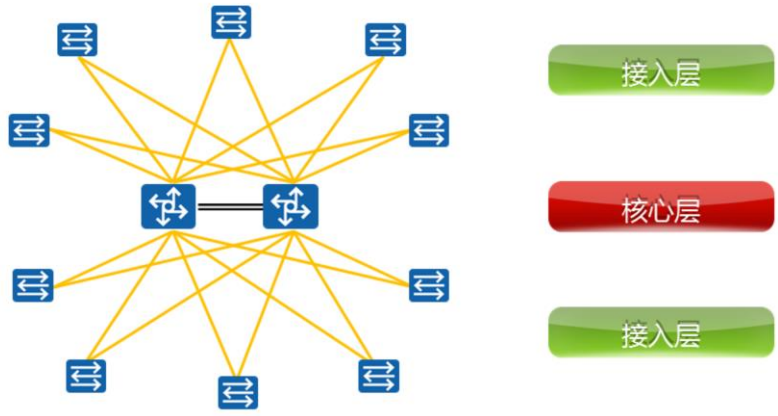


- 大型网络应用于大型企业，大型网络具有以下特点：
  - 覆盖范围广：大型网络可以是一个覆盖多幢建筑物的大型园区网络，也可以是通过广域网连接一个城市内的多个园区，乃至延伸、覆盖几个省的全国性网络。
  - 用户数量较为庞大，可以支持几千几万甚至更多的人员接入，大型网络具有很强的可扩展性，能够随用户数量的变化进行扩展。
  - 网络需求复杂：大型网络支撑多种类型的业务，包括实时业务、非实时业务、语音业务、视频业务等等。
  - 功能模块全：为了满足各种不同的业务需求，大型网络中的功能模块相对较全。
  - 网络层次丰富：网络结构的扩展性是通过网络的合理层次布置来实现的。譬如为了使网络支撑更多的接入，就需要对网络进行合理分层。
- 大型网络建设一般都不是一次性完成的，常常会历经建设、扩容、改造、检修等阶段。



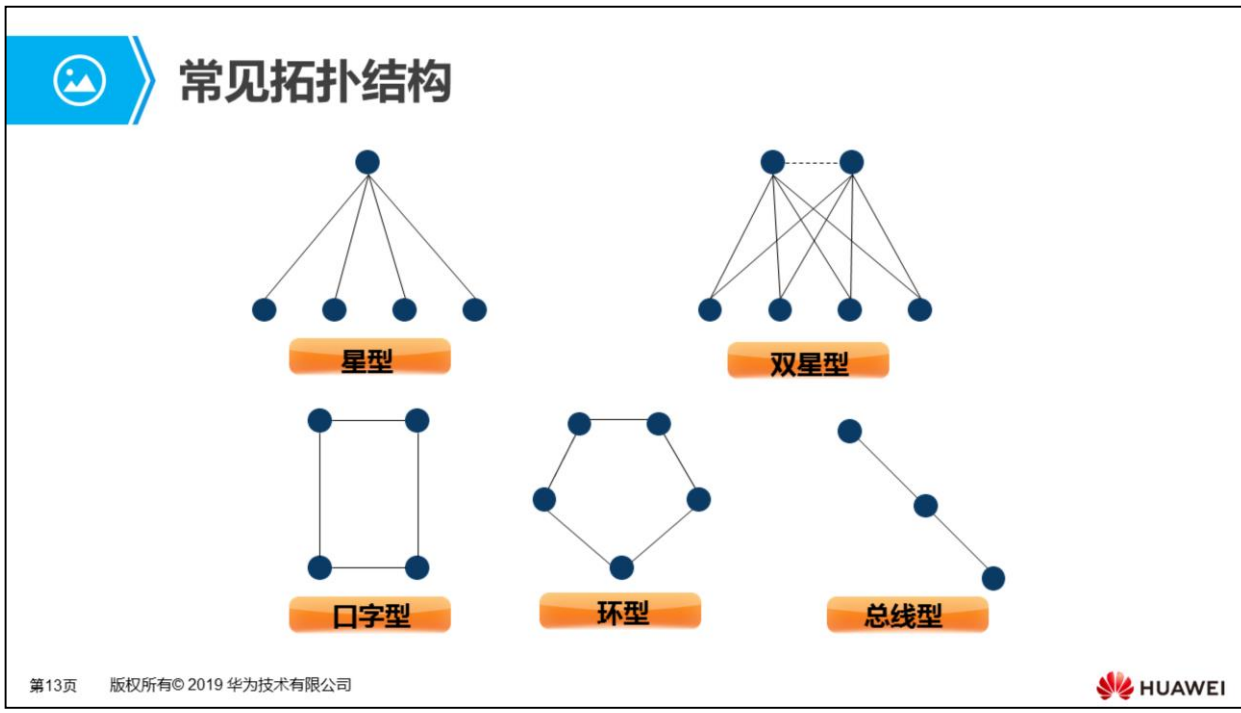
- 在大、中型网络中，通常通过模块化方式将网络功能结构进行分解。但是在各个模块内部，还是存在结构的扩展和弹性问题。譬如一个园区网络需要接入大量用户等，这个问题一般通过网络的层次化来解决。
- 传统的网络采用三个层次，核心、汇聚、接入各司其职，核心层提供数据高速通路，汇聚层进行流量汇聚和控制策略，接入层为终端提供多种接入方式。
- 三层网络提供良好的可扩展性，在当前网络中得到了广泛的应用。大量的园区网络，广域网都采用了这种架构。

层次化网络 - 二层结构



HUAWEI

- 随着业务需求的变化和网络技术的发展，网络结构开始逐渐呈现扁平化趋势，出现了二层架构网络。二层架构只有核心层和接入层。抽离汇聚层后，对网络设备提出了新要求，譬如核心设备需要能够提供更高的端口密度，以接入大量的接入设备。
- 二层结构主要应用于城域网、广域网、数据中心网络等场合。



- 一个大型网络常常是由多个拓扑片段搭接而成的。常见的网络拓扑如上图所示：
  - 星型：常见的分层网络结构，存在单点故障问题。
  - 双星型：常见的分层网络结构，常用于园区网内部二层互联，有一定的冗余性。
  - 口字型：常见的分层网络结构。常用于设备广域网互联，有一定冗余性。
  - 环型：在某些特别的协议或在线路资源受限的情况下使用，有一定冗余度。
  - 总线型：在线路资源受限的情况下使用，线路利用率较低，没有冗余性。

案例：校园网拓扑

- 某大学需要建设一个校园网，覆盖范围包括园区内的教学楼、学生和教师宿舍楼以及食堂等附属设施，另外还有分校、机房等相关设施。
  - 如何定义该案例的校园网规模？
  - 该案例的校园网基本结构如何设计？
  - 该案例的校园网拓扑结构如何选择？

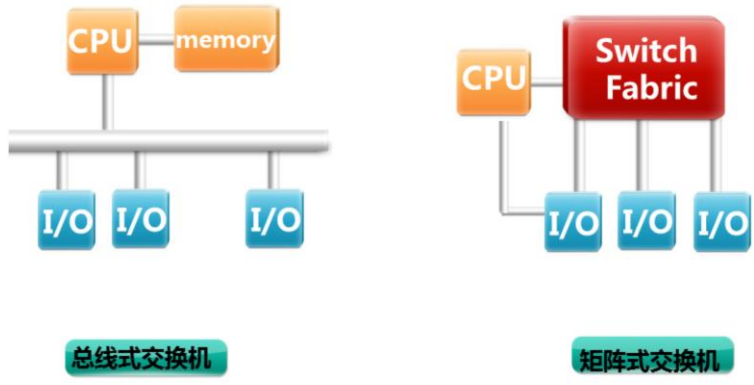
  HUAWEI

- 一个大学的校园网属于典型的园区网络。虽然覆盖范围有限，但接入的用户多，设备数量多，网络需要支撑的业务种类多，网络模块丰富，所以可以归属于大型网络。
- 首先确认校园网中需要采用的模块，然后根据模块的规模确定各模块内部的网络层次结构：
  - 核心模块作为全网的中心通路；
  - 教学楼、宿舍楼、食堂作为接入模块；
  - 教育网、广域网、互联网接入模块；
  - 数据中心模块；
  - 无线接入模块；
  - 网络管理、接入认证模块；
  - 其他相应的功能模块。
- 网络的拓扑结构采用星型或双星型拓扑结构。根据网络的可靠性要求及成本选择相应的冗余结构。

目录

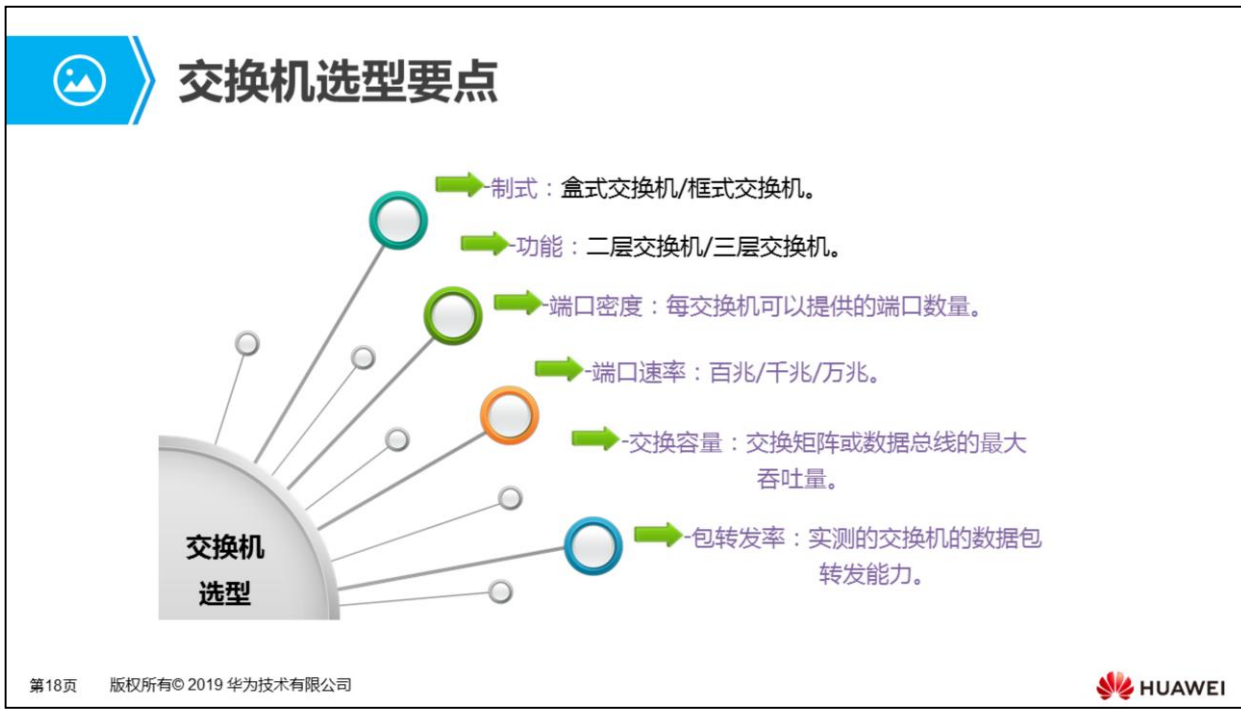
- 当前的网络基础设备，主要分两类，一类是交换机，提供局域用户的网络接入功能。交换机中又根据是否支持路由功能分为二层交换机和三层交换机两个小类；另一类是路由器，提供异构网络间的连接及路由功能。
- 除了这三类设备之外，当前网络中常常还能看到其他类型的网络设备，譬如防火墙、入侵检测/防御系统（IDS/IPS）等网络安全设备，AC、AP等无线设备。这些设备将在相应的章节分别介绍。
- 在网络技术的发展过程中，某些网络设备被淘汰了，譬如HUB、网桥、Token-Ring、ATM交换机等。
- 随着新的网络技术发展，也产生出了一些新兴的网络设备支持新技术，譬如数据中心交换机、SDN交换机等。

交换机体系架构



总线式交换机　　矩阵式交换机

- 当前的以太网是以交换机为中心的架构，在这之前曾经出现过总线式，HUB互连等多种方式。
- 当前常用的交换机从体系结构来说，可以分为两大类，一种是总线式交换机，一种是采用交换矩阵（Switch Fabric）的交换机。
  - 总线式交换机：这也是交换机最初的交换方式，在这种方式中，所有的接口均连接到交换机内部的共享背板总线上，各接口分时占用总线来传送数据，需要专门的仲裁机构来分配总线的带宽。这种方式结构简单，成本低廉，但是扩展性较差，当前主要用于低端交换机。
  - 交换矩阵式交换机：采用矩阵结构，可以同时在多个接口之间交换数据，消除了交换机内部的通路瓶颈。当前的高端交换机均采用这种结构。
- 除了这两类架构之外，还有其他架构，譬如共享内存交换机等。



- 当前局域网的二层技术经过竞争和淘汰之后，基本是以太网一统天下的局面。这里说到的交换机选型，主要指以太网交换机的选型。
- 一个厂家提供的交换机一般有很多型号，各个型号的交换机均有不同的定位，在工程中进行选型的时候，主要考虑以下因素：
  - 制式：当前的交换机主要分为盒式和框式，盒式交换机一般是固定配置，固定端口数量，较难扩展；框式交换机基于机框，其他配置如电源，引擎和接口板卡等都可以按照需求独立配置，框式交换机的扩展性一般基于槽位数量。

    盒式交换机为了提高扩展性，发展了堆叠技术，可以将多台盒式交换机通过特制的板卡互联，结合成为一台整体的交换机。
  - 功能：二层交换机和三层交换机是最大的功能区别，其他还有一些特别的功能，譬如链路捆绑、堆叠、POE、虚拟功能、IPv6等。
  - 端口密度：一台交换机可以提供的端口数量，对于盒式交换机每一种型号基本是固定的，一般提供24个或48个接入口，2-4个上连接口。框式交换机则跟配置的模块有关，一般指配置最高密度的接口板的时候每个机框能够支持的最大端口数量。
  - 端口速率：当前交换机提供的端口速率一般有100Mbps/1Gbps/10Gbps这三种。
  - 交换容量：交换容量的定义跟交换机的制式有关，对于总线式交换机来说，交换容量指的是背板总线的带宽，对于交换矩阵式交换机来说，交换容量是指交换矩阵的接口总带宽。这个交换容量是一个理论计算值，但是它代表了交换机可能达到的最大交换能力。当前交换机的设计保证了该参数不会成为整台交换机的瓶颈。
  - 包转发率：指一秒内交换机能够转发的数据包数量。交换机的包转发率一般是实测的结果，代表交换机实际的转发性能。我们知道以太帧的长度是可变的，但是交换机处理每一个以太帧所用的处理能力跟以太帧的长度无关。所以，在交换机的接口带宽一定的情况下，以太帧长度越短，交换机需要处理的帧数量就越多，需要耗费的处理能力也越多。
- 对于一个具体的交换机来说，除了以上这些最基本的指标参数，还有其他大量的参数，这些参数一般都会公布在官方网站上。

- 2700系列交换机：二层百兆以太网交换机，该系列中提供大量的具体型号，分别提供8/16/24/48个10/100M自适应接入端口，并提供1-4个千兆上联端口。各型号还提供PoE供电，AC/DC电源，光口/铜缆上联，基本/增强软件版本等不同选项。
- 3700系列交换机：三层百兆以太网交换机，该系列提供24/48个10/100M自适应接如端口，并提供2个千兆上联端口。各型号提供PoE供电，AC/DC电源，光口/铜缆上联，基本/增强软件版本等不同选项。
- 5700系列交换机：提供24/48个10/100/1000Mbps自适应以太接入端口。当后缀为为LI的时候表示是二层交换机，提供四个千兆上联接口；当后缀为EI的时候，表示是三层交换机，提供四个千兆上联接口；当后缀为HI的时候，表示是三层交换机，提供各种扩展插卡模块，可以选用10/40Gbps的上联接口。同样提供多种选项。
- 6700系列交换机：高性能万兆盒式交换机，提供24/48个全线速万兆接口，同时支持丰富的业务特性、完善的安全控制策略、丰富的QoS等特性，可用于数据中心，服务器接入及园区网核心。

华为框式交换机

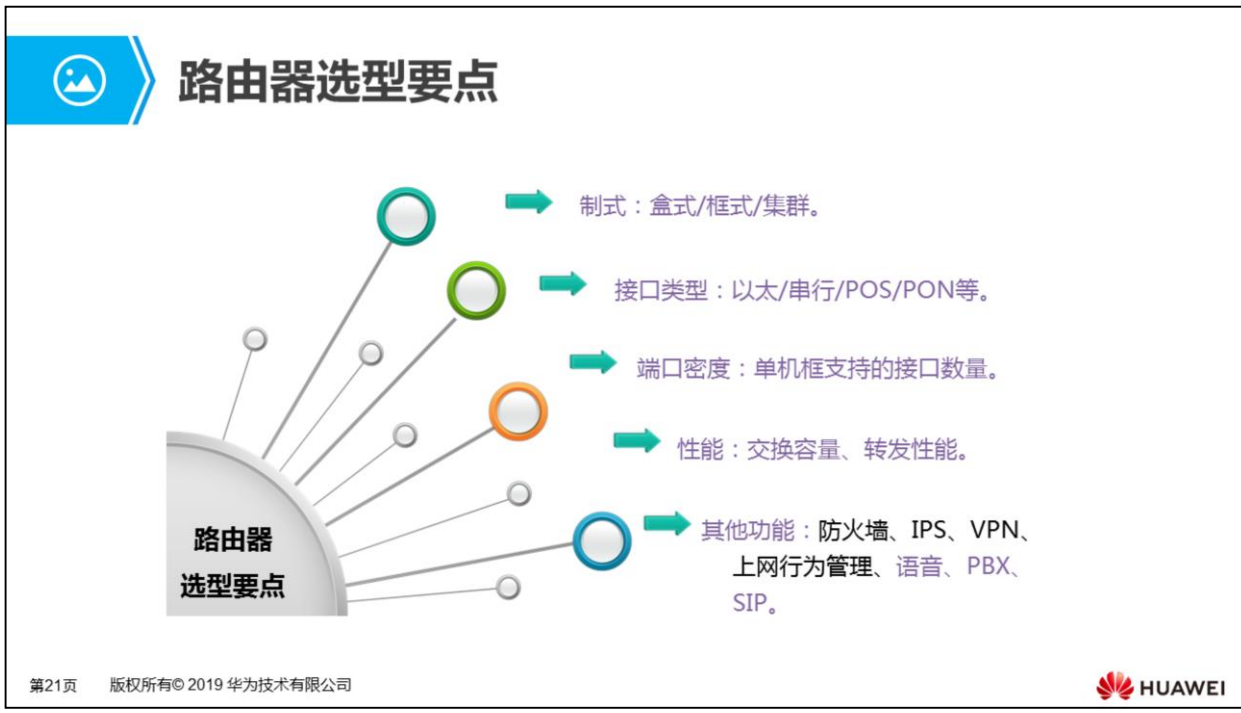
7700：
三个型号分别提供3/6/12个接口卡插槽；
主控、电源、风扇采用冗余设计，所有模块支持热插拔；
提供100M/1G/10G/40G接口卡，单一机框最多支持480个万兆接口；
提供MPLS VPN、业务流分析、QoS、组播等丰富特性。

9700：
三个型号分别提供3/6/12个接口卡插槽；
单一机框最多支持576个万兆接口，96个40GE接口；支持线速转发；
提供防火墙、入侵检测、无线控制等模块；
支持CSS集群技术。

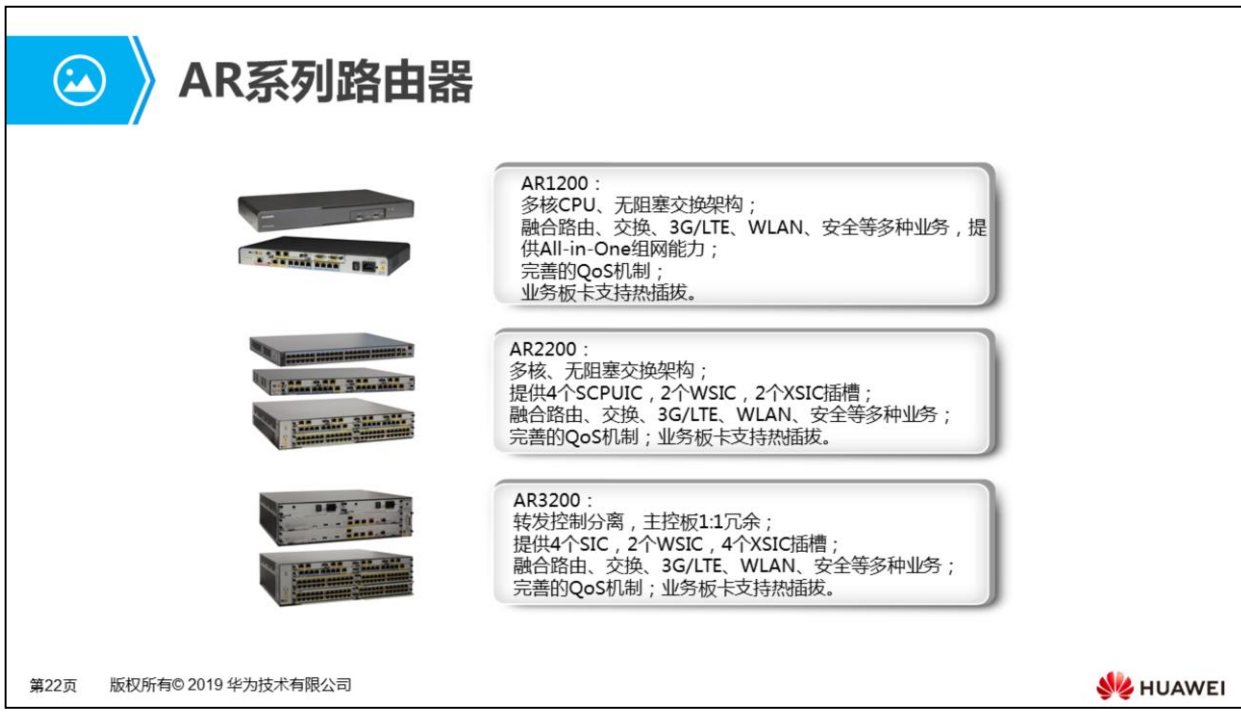
12700：
三个型号分别提供4/8/12个接口卡插槽；
单一机框最多支持576个万兆接口，96个40GE接口；支持线速转发；
支持TRILL、FCoE（DCB）、EVN、nCenter、EVB、SPB、VXLAN等数据中心特性。

HUAWEI

- 7700：支持100M/1G/10G/40G接口卡，单台设备最多支持480个万兆端口，支持单端口速率40G、100G平滑升级。具备大于0.99999的高可靠性，主控、电源、风扇等关键部件采用冗余设计，所有模块均支持热插拔；采用交换网集群技术；采用内嵌集中式防火墙板卡；支持组播，IPv6，无线AC，Netstream流量分析等特性。
- 9700：面向100G平台设计，满足高密度的千兆/万兆端口线速转发，单一机框最大支持96个40GE、576个10GE端口，支持100GE以太网标准。支持主控和业务口CSS集群技术。关键器件，如主控、电源、风扇等均采用冗余设计。支持组播，IPv6，无线AC，Netstream流量分析等特性。
- 12700：基于华为首款以太网络处理器ENP和自研的通用路由器平台VRP，采用CLOS架构，提供高达200Tbps的交换容量。支持高达1M的MAC表项和高达3M的FIB表项，满足核心大路由应用需求。实现随板AC功能，可管理4K AP，64K用户。支持CSS2交换网硬件集群，集群主控1+N备份，1.92Tbps集群带宽，4μs跨框时延。



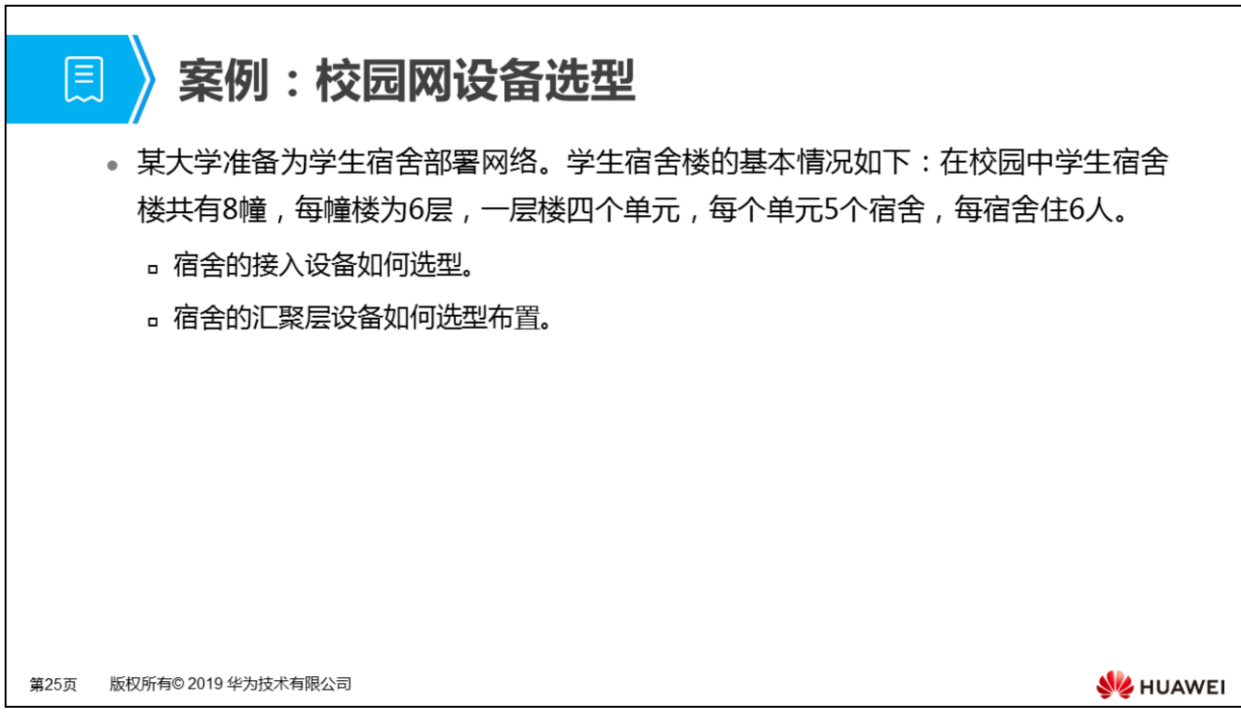
- 制式：当前的路由器制式主要分为盒式和框式两种，为了增加端口扩展能力，后来又发展出了集群路由器。
- 接口类型：对于低端路由器来说，当前最主要的用途是为了实现在不同类型的链路上承载IP。所以，路由器能够支持的链路类型成为重要的参考依据。当前华为的路由器能够支持以太网、POS/CPOS、EPON/GPON、同异步串口、E1/CE1、3G/LTE等接口。
- 端口密度：对于高端路由器来说，需要接入大量的线路，所以提供高速端口和高端口密度是高端路由器的重要参考。另外，当前的高速端口，类型并不多，发展最快的就是以太网，所以当前的高端路由器接入口也是以太网为主，少部分POS口。
- 性能：与交换机相似，路由器的性能也以交换容量和转发性能来标识。当前的高端路由器作为网络的核心设备，要求能够高速转发数据，所以基本采用无阻塞的结构。
- 其他功能：低端路由器当前有平台化的趋势，在其上集成了多种功能，譬如网络安全、语音等。但是这些功能基于软件实现，适用于小型网络，如果要大规模高性能地实现这些功能，仍然需要专用的设备。



- AR G3系列路由器是面向企业及分支机构的新一代网络产品，基于VRP平台，集路由、交换、无线WLAN、3G/LTE、语音、安全等功能于一身，采用多核CPU和无阻塞交换架构，拥有领先于业界的系统性能和可扩展能力，提供一体化的解决方案。常用的型号如下：
  - AR1200：提供2个SIC插槽。
  - AR2200：提供4个SIC插槽，2个WSIC插槽，2个XSIC插槽。
  - AR3200：提供冗余主控，提供4个SIC插槽，2个WSIC插槽，4个XSIC插槽。
- AR G3系列路由器除了这三个系列外，还有AR120&150&160&200等型号，可应用于小型企业、SOHO型企业。

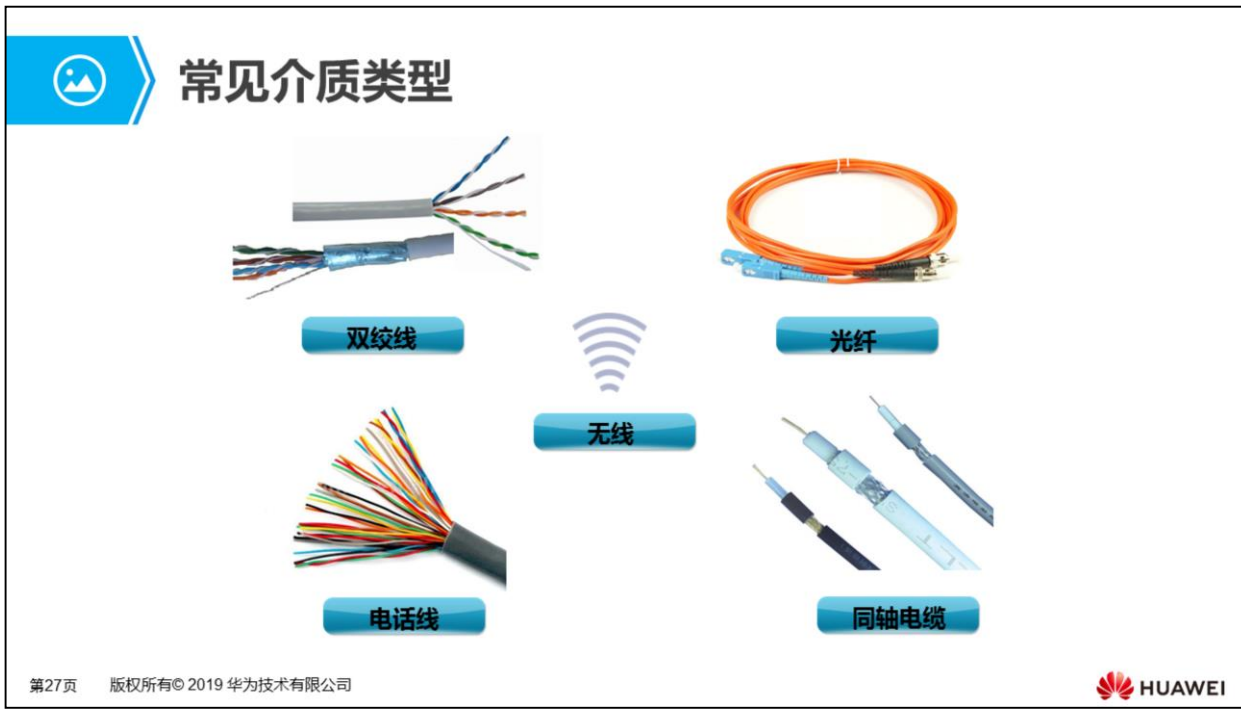
- NE系列路由器采用华为自研NP芯片，基于分布式硬件转发和无阻塞交换技术，具有良好的线速转发性能、电信级的可靠性、优异的扩展能力、完善的QoS机制和丰富的业务处理能力：
  - NE20E-S：面向各行业用户推出的高端网络产品，主要应用在IP骨干网汇聚，中小企业网核心，园区网边缘，中小校园网接入等。
  - NE40E：主要应用在企业广域网核心节点、大型企业接入节点、园区互联&汇聚节点以及其他各种大型IDC网络的边缘位置，与NE5000E骨干路由器、NE20E汇聚路由器产品配合组网，形成结构完整、层次清晰的IP网络解决方案。
  - NE5000E：面向网络骨干节点、数据中心互联节点推出的超级核心路由器产品。提供业界最大容量1T路由线卡，支持背靠背集群、混框集群等模式，以其大容量、高稳定、绿色设计，保证网络的健壮性、平滑演进。
- NE路由器除了这三个系列外，还有NE08E/ NE05E中端业务路由器，基于华为自研ENP芯片和SDN架构，体积小、带宽大，-40ºC~65ºC 宽温应用，能够适应各种恶劣环境。

- 路由器和交换机是当前网络中的基础设备，前面罗列了最常用的一些设备，除此之外，华为公司还提供其他型号的路由器和交换机，以及其他类型的网络设备，包括安全网关、DDoS防御等安全设备，AC、AP等无线网络设备。这些设备在华为官网上均有介绍，可以前往华为官网获得相关的信息。



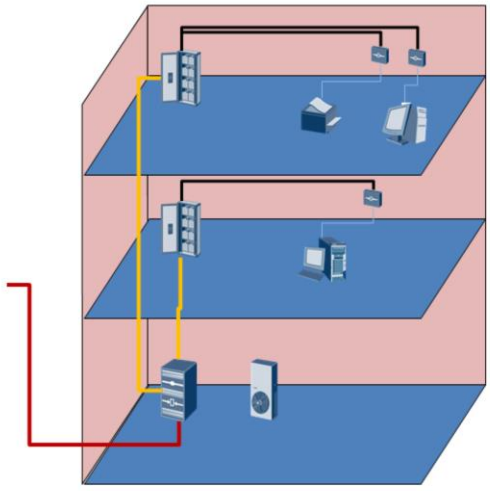
- 案例中展示的是工程中常见的情况，工程师掌握了跟选型相关的部分信息，但是并不充分，特别是与选型相关的客户习惯等并没有确定，所以难以完全确定设备型号。这种情况下，正确的处理方法是继续深入获取更多的相关信息，给出可能的选型，与客户沟通协商，解释不同选型之间的差异，以客户的需求为导向，共同确定最终选型。
- 当前的信息，可以确定以下推荐：
  - 接入交换机一般直接安装在楼道中，采用市电（交流电）可以节省费用。下联用户的接入口采用铜缆接口，上连接口采用光纤。按照学生宿舍的人口密度，一个单元大概住宿30个人，所以可以建议每一个单元安装一个48口的接入交换机，这样，一幢宿舍楼24个单元，需要安装24台接入交换机。在交换机具体选型的时候，还需确定交换机接入端口的速率，接入交换机是否需要三层功能等。这些可与客户协商确定。可能的推荐型号为：S2710-52P-SI-AC；S3700-52P-SI-AC。两者均能提供48个百兆接入口，4个千兆SFP插槽上行口，交流供电；其中S3700提供三层功能，并提供更丰富的特性和对IPv6的支持。
  - 汇聚交换机可以每一幢楼设置一台，与接入交换机的选择思路相似，汇聚交换机可以选择S5720-36C-EI-28S-AC；提供28个千兆SFP，4个复用的千兆10/100/1000Base-T以太网端口Combo，4个万兆SFP+，可插拔双电源，支持交流或直流供电。

目录



- 当前网络中常见的介质如下：
  - 双绞线：双绞线分为屏蔽双绞线（Shielded Twisted Pair，STP）与非屏蔽双绞线（Unshielded Twisted Pair，UTP）。根据线路的传输频率、带宽和串扰比等电气特性，双绞线又以此分类，当前常见的为五类（CAT5）、超五类（CAT5e）、六类（CAT6）。其中五类线用于快速以太网，超五类和六类线用于千兆以太网。
  - 光纤：分为单模光纤和多模光纤。单模光纤的传输距离最大可以达到2公里到70公里，多模光纤的传输距离一般在500米以下。在网络工程中经常接触的光纤尾纤，多模光纤为橙色，单模光纤为黄色。
  - 电话线：一般为两芯铜线。电话线并不能承载高速信号，但是因为历史原因，电话线部署的范围广数量大，所以在电话线上发展了很多技术用来承载数据信号，包括同异步串行技术，DSL技术等。
  - 同轴电缆：原先用于传送视频信号，同样为了承载数字信号发展了CABLE MODEM等承载技术。
  - 无线：无线通信是当前发展和应用最为迅猛的技术。从WLAN到LTE，在当前都得到了广泛的应用。

楼宇结构化布线

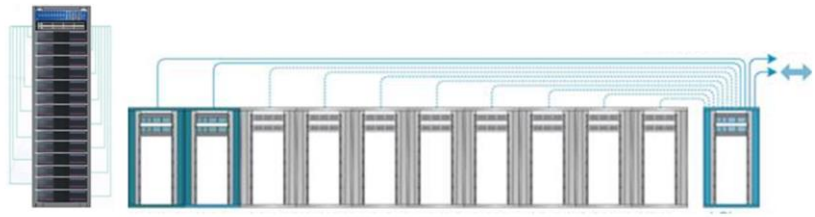


- 楼宇布线子系统：
  - 水平子系统：信息面板——楼层机房，一般使用双绞线。
  - 垂直子系统：楼层机房——中心机房，一般使用光纤。
  - 工作区子系统：终端设备——信息面板、网络跳线。

  HUAWEI

- 网络布线系统一般可以分为建筑群子系统，垂直子系统，水平子系统和工作区子系统。整个布线包括各种线路和器件。此处不展开。
- 在当前的布线系统中，水平系统一般使用双绞线，因为水平系统连接到客户终端，而各种终端设备的网络连接还是以双绞线为主。要注意，双绞线的距离一般不能超过100m，在机房定位时需要简单估算。
- 在当前的布线系统中，垂直系统一般使用光纤，一个是因为中心机房与各楼层之间的距离问题，另外一个是因为作为干线系统，要求提供较高的数据速率。
- 一般楼内布线，常常采用多模光纤以节省建设成本；但是考虑备品备件及运维成本，统一使用单模光纤也是可以考虑的。

数据中心布线结构



- ToR（Top of Rack）：在每一个机架顶部安装交换机。
- EoR（End of Row）：在每一排机架尾部安装交换机。

- ToR和EoR是当前数据中心比较流行的两种布线方式。ToR的接入交换机直接安装于每个机架，减少了接入布线量；而EoR则在一排机架的尾部安装交换机。
- 随着当前云计算的发展，数据中心的服务器密度提高很快，ToR的布线方式逐渐流行。

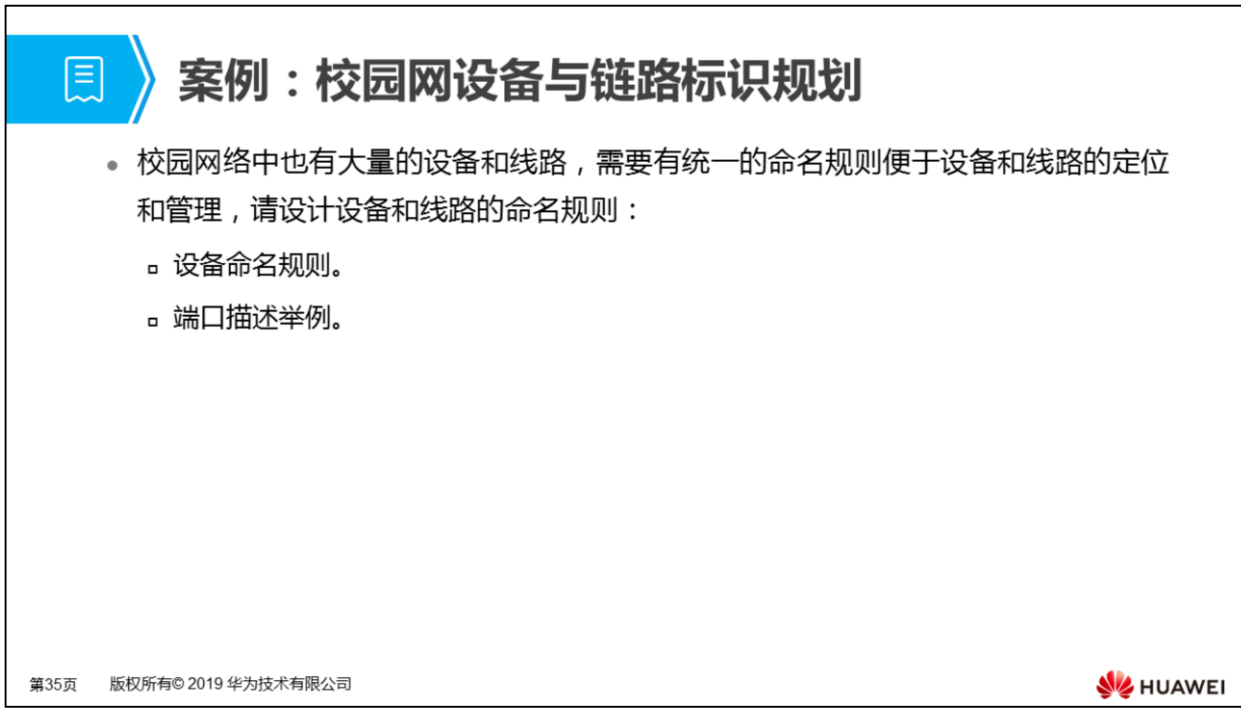
- 布线工程的端接点，在机房内一般是配线架，在工作区一般是信息面板。当使用时，两端用网络跳线连接到设备网络口上。双绞线的接口一般就RJ-45一种。
- 光缆接入机房后最后端接到光纤盘上，光纤的接口形式相对较多，当前最常见的是四种：
  - LC：小方口，当前设备接口，光模块常用；
  - SC：大方口，多用于设备接口，光模块；
  - FC：圆形螺口，当前光纤配线架常用；
  - ST：圆形卡口，多用于光纤配线架。
- 在布线完毕后，一般在验收的时候会进行测试，保证线路正常。但如果在连接网络时需要确认线路的状态，需要进行测试:
  - 网线测试仪：可以通过连接线路两端来查看线路的完好性。另外还有高档测试仪，可以通过连接网线的一端测试网线的长度，通过长度判断线路的情况；
  - 红光笔：在连接上光纤的一端后，可以从另一端看到红光。红光笔的功率较大，在测试时切勿在另一端连接设备，以防灼伤感光器件；
  - 光功率计：可以测试接收到的光功率。部分光功率计能够发送特定功率的光。光功率计进行测试时，需要先调整需要测试的光波长，功率一般以dbm的单位计数。能够正常传送数据的光功率范围一般在-5dbm到-20dbm之间。具体能工作的范围跟特定的光模块有关，可以查找相关的光模块参数。

- 电话线和同轴电缆不能直接传送数字信号，所以都需要调制解调器（MODEM）进行信号转换。最初时候的MODEM都是独立的，数字信号的输出最初以RS-232、V.35为主，后来集成了部分数据功能，常常用以太网的形式输出数据。现在路由器也有MODEM模块可以配置。
- 电话线和同轴电缆常常用作广域链路的接入，跟用于局域的双绞线相比，距离比较长，而且常常不归同一个机构管理，所以在测试的时候需要互相协作。最常用的测试方式是打环（LOOP）测试，测试的时候就是简单地在远端将两根线路短接即可。一般MODEM会有一个LOOP灯，短接后会点亮。另外一些MODEM面板上也会有打环按钮或菜单，可以选择向本端或向远端打环。
- 打环测试只能对广域链路进行定性的测试，提供链路的运营商有专门的设备，可以在线路环回的情况下，发送并同时接收流量，测试链路的误码率。
- 线路管理的责任边界一般就在调制解调器上，根据调制解调器的提供方确定调制解调器的责任方。

目录

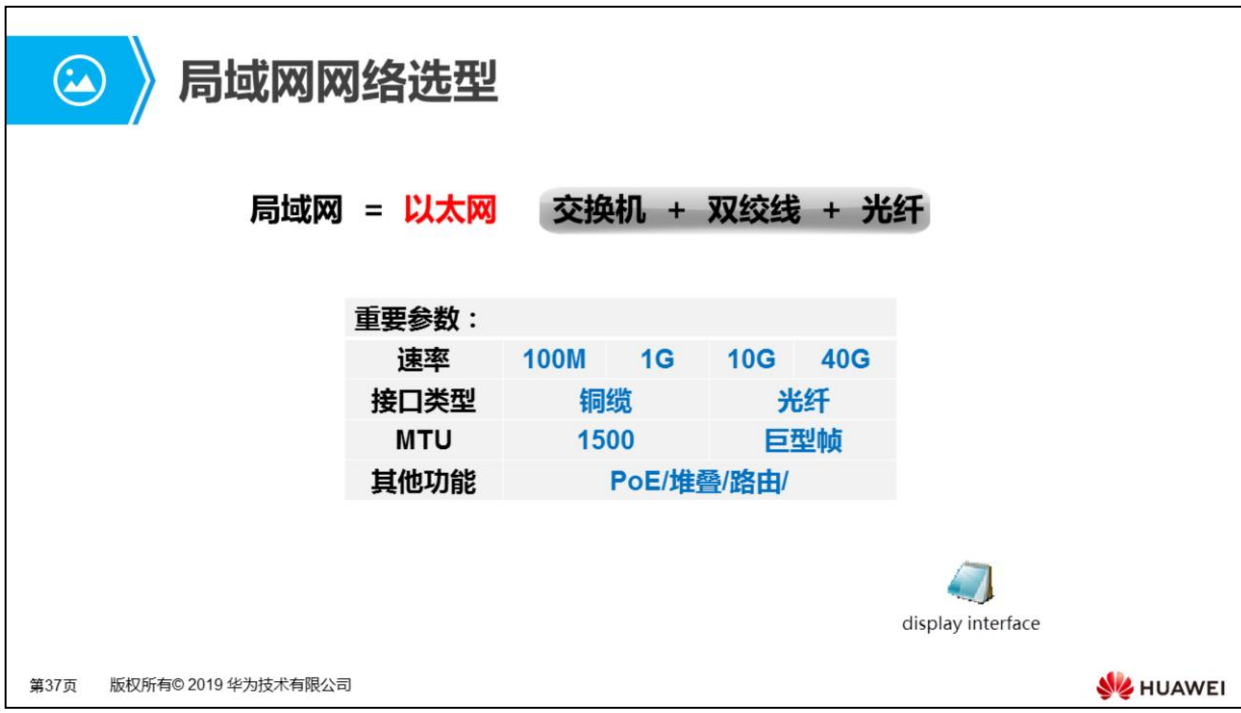
- 网络中的一台设备上线之后，需要有一定的标识。这种标识包括逻辑设备名和设备上的物理标签。逻辑设备名是在设备的配置上设置的，当管理人员登录设备的时候就可以知道该设备的一系列信息；物理标签一般直接贴在设备上，标明设备的一系列信息。
- 设备的标识方式并没有一个统一的标准，一般本着实用的原则进行定义，在一个企业内部，尽量做到统一规则。设备的逻辑名一般会包含以下信息：
  - 设备安装位置；
  - 设备角色；
  - 设备型号；
  - 设备编号。
- 设备的物理标签一样并没有统一的标准，各家企业按照各自的要求进行标识，常常包含以下信息：
  - 设备型号；
  - 设备编号；
  - 责任人/联系方式。

- 当前的网络中，设备间的连接复杂，网线的数量巨大，为了日常管理和排障的方便，需要对设备接口和网络线路进行标识。
- 设备端口下可以配置描述信息，这个描述信息一般用来描述线路的对端设备和接口，当然也可以根据需要添加更多的信息。
- 网络线路上一般采用标签的方式描述线路的走向，与设备端口描述不同，当前的网络线路一般会有分段，通过网络配线架进行跳接。



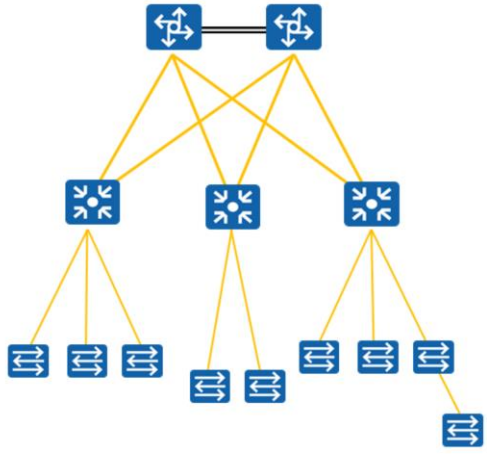
- 设备的命名规则可以采用：设备定位+设备位置+设备型号+编号的方式进行命名，举例如下：
  - ACC-B1F3U2-2710，其中各字段的含义如下：
    - ACC：接入交换机；
    - B1F3U2：1号楼3楼2单元；
    - 2710：设备型号。
- 线路的命名规则可以采用：对端设备名+对端端口号的方式，举例如下：
  - To-AGG-B1N1-G0/0/8：
    - AGG：汇聚交换机；
    - B1N1：1号楼1号机；
    - GE0/0/8：对端端口号。

目录



- 当前的局域网基本采用以太网。而当前局域网的实现方式也基本统一为交换机加五类线或光纤的方式。
- 在设计的时候，最关注的以太网参数是速率。当前的以太网速率常见的有100M、1G、10G、40G。
- 线路类型也是关注点，一般1G及1G以下较多采用双绞线，1G及1G以上较多采用光纤。
- 当采用铜缆的时候，交换机端口速率一般是自适应的方式，也就是说互联的两台交换机相互之间能够协商出一个最优的连接速率。采用光纤的时候，速率一般是固定的。
- 铜缆端口的双工模式一般是自适应的，作为优化，可以在两端的设备上手工指定双工模式，光纤连接一般都是全双工模式。
- 传统以太网的MTU是1500字节（不含帧头帧尾），但是当前各种隧道和封装技术发展迅猛，如MPLS、FCoE，VXLAN等技术，要求以太网能够承载更大的MTU，在有需求的特殊场合，要注意交换机支持的MTU。

局域网常用拓扑



核心层

双星型拓扑

汇聚层

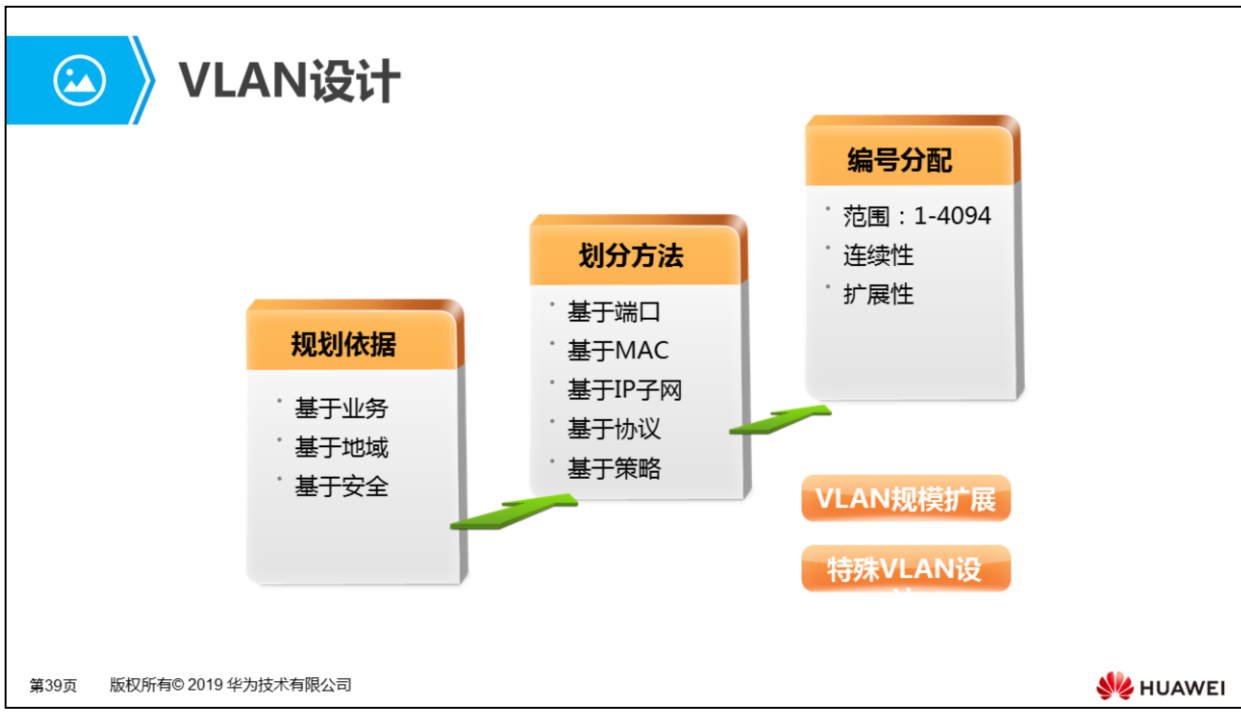
星型拓扑

接入层

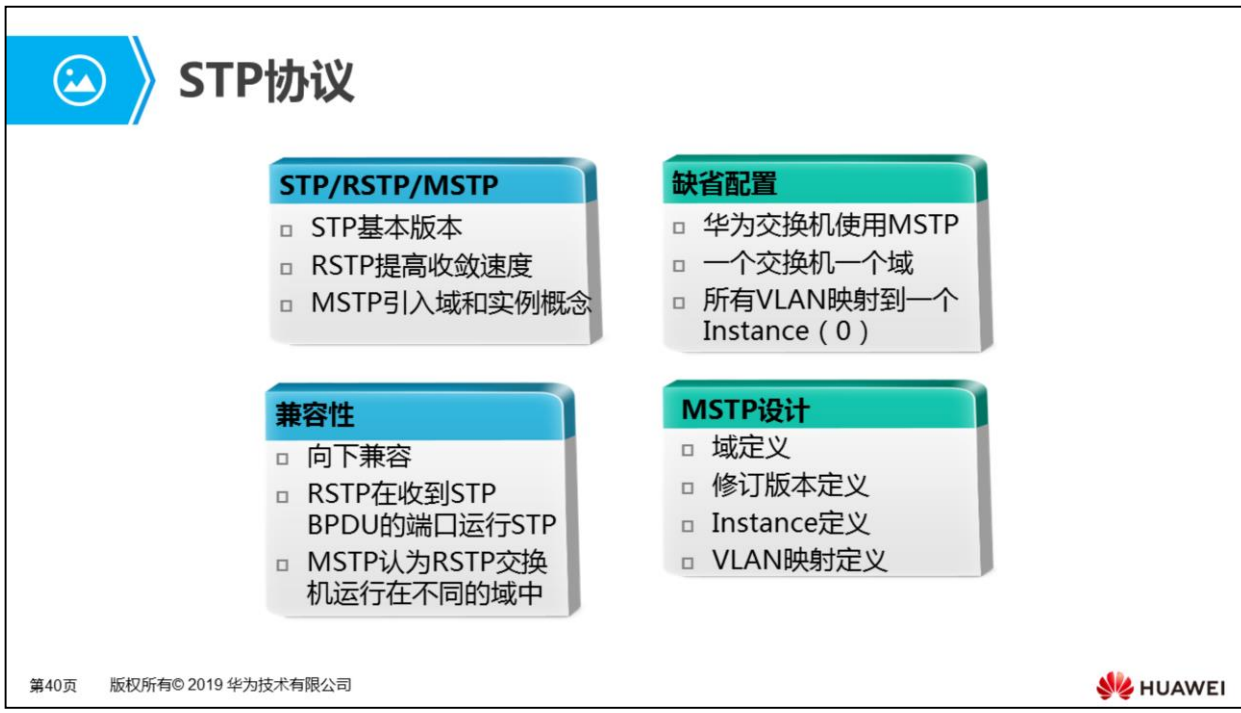
网络延伸
端口扩展

HUAWEI

- 图中所示为一个当前局域网常见的三层拓扑结构，核心层与汇聚层之间采用了有冗余性的双星型拓扑，汇聚层与接入层之间采用了无冗余的星型结构。
- 部分场所由于接入终端数量较多，在接入交换机上存在级联情况，不建议在网络中大规模地采用级联方式。
- 在实际网络中，可以在该拓扑结构的基础上进行变形。譬如本拓扑中只有核心层提供了设备冗余，如果汇聚层需要配置双机冗余，那么可以是局部采用全连接或口字型的网络拓扑。另外，如果汇聚层与接入层之间需要实现链路冗余，可以采用双链路或链路捆绑技术。
- 交换机间一般采用千兆以上光纤/双绞线互联。



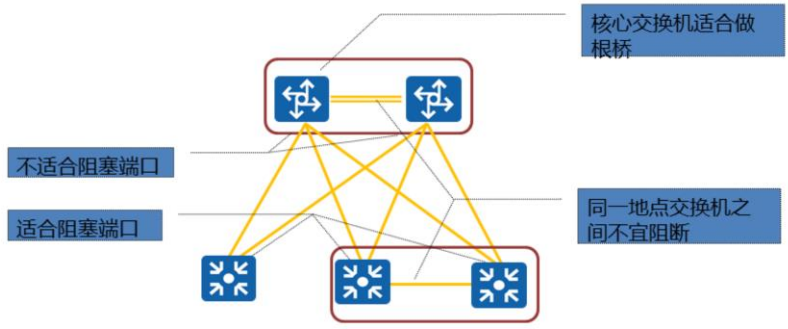
- VLAN设计包括确定VLAN的划分依据，具体的VLAN划分方法，以及VLAN编号的分配等几个方面。
- 首先明确依据何种条件划分VLAN，常见的划分方式一般是基于业务、基于地域。
  - 基于业务：一般的公司的行政架构基本是按照业务来进行划分的，所以基于业务的VLAN划分在真实网络中基本相当于基于公司的行政架构进行VLAN划分，这种划分方式也是最常见的。
  - 基于地域：按照网络的延伸范围来划分VLAN，譬如按照楼宇、楼层和房间来划分VLAN。
- 确定VLAN的具体划分方法，VLAN在技术上可以通过不同的方式进行划分。当然用得最多最广泛的是基于端口划分。这种方法简单直接，便于实施及管理。另外也可以基于MAC地址、IP地址、协议类型进行VLAN划分，这些方法可以用在有某些特殊需求的场景。
- VLAN编号的分配：VLAN编号可配置的范围是1-4094，注意每个端口需要一个PVID，缺省取值为1，建议VLAN1作为保留VLAN。其余编号分配的时候，在技术上并没有特别的规范，主要的考虑来自于管理和运维的方便性。分配时最好结合实际情况，譬如，如果是按照地域进行分配，那么园区内一幢楼内的VLAN最好分配连续的编号。
- 在很多时候，常常会出现4094个VLAN不够用的情况，针对这些情况，发展出了一些VLAN扩展技术，譬如接入侧的QinQ技术。
- 在VLAN技术中，各个厂商还各自设计了一些特殊的VLAN技术，用来实现一些特殊的需求，譬如MUX VLAN、VLAN Aggregation等。



- STP是一个有效解决二层网络环路的重要协议，当前该协议主要有三个版本：STP、RSTP、MSTP。这三个版本的基本算法是类似的，但是各个版本之间又存在差异。
- 华为交换机缺省采用MSTP。在缺省情况下，每一个交换机自成一个MSTP域，域名为该交换机的MAC地址。同时缺省情况下所有的VLAN均映射到Instance 0上。
- 当网络中混合了多种STP协议的时候，各个STP版本相互之间向下兼容，保证在混合组网的时候能够正常运行。
- 现网部署中经常会出现与友商设备STP协议对接的情况，需要关注相关的案例及产品特性。

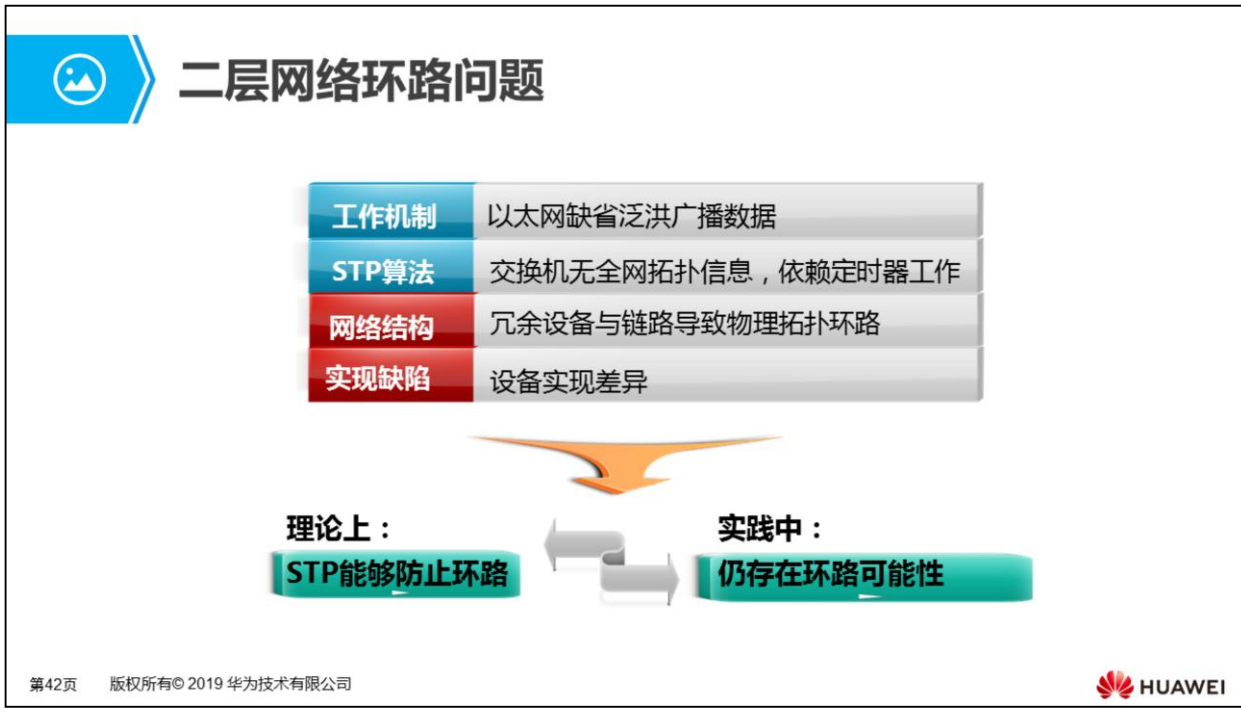
STP实用设置

关键点 根桥位置、阻塞端口位置。

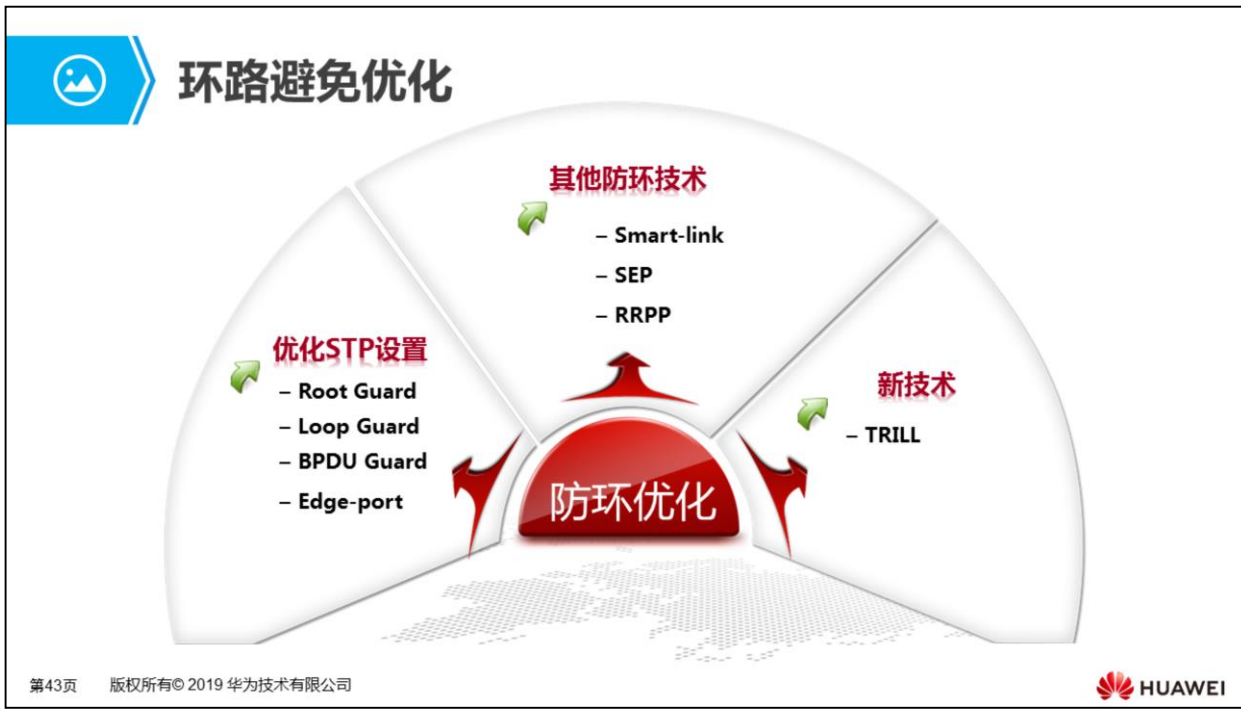


调整方法 BID优先级、COST等。

- 当网络中存在冗余链路时STP协议会通过将部分端口予以阻塞避免二层环路的产生。
- 阻塞端口应出现在次要、非关键链路上，而不是主干链路。
- 当网络中有设备冗余时，一般两台冗余设备之间的互联链路不应被阻断。
- 在设备冗余的环境中主、备核心交换机通常被配置为STP根网桥及备份根网桥。
- 双链路上联的接入交换机端口之一通常被STP协议选择为阻断的端口。



- STP协议具备一定的防止二层网络环路产生的能力，但在实际组网中，二层网络出现环路的可能性远远大于三层网络，那么二层环路是怎么导致的呢？
  - 拓扑环路：在大型网络设计的时候，为了提高可靠性，我们一般都会设计冗余链路和冗余设备，这些冗余设计的本质就是提供迂回路径。
  - STP算法问题：STP算法缺少对全网拓扑信息的了解，并不能从根本上避免环路。
  - 交换网络中交换机并不能知道全网的收敛状态，只是根据计时器估算全网的收敛情况，一旦定时器超时，即进行数据转发。
  - 实现缺陷：STP协议的具体实现是基于具体设备的实现的，产品和所运行网络中有可能出现各种不可预料的情况，导致环路的产生。



- 为了降低产生二层环路的可能性，我们可以采用多种方法。
- 优化STP设置：
  - STP缺省的时间常数是在建议的拓扑条件下的优化设置，这些常数可以修改，但是不建议修改。
  - STP在RSTP阶段发展出了各种保护技术，用来提高STP的收敛速度、稳定性以及防攻击的能力。
- 其他防环技术：
  - 为了规避STP防环收敛的一些问题，又出现了一些其他的防环技术，如Smart-link，SEP，RRPP等。这些技术解决了以太网双上行链路切换时收敛速度慢、算法不精确的问题；但是这些技术一般都有很大的局限性，如Smart-link主要解决单一设备主备双上连的问题，SEP主要解决环型拓扑的问题。
- 新技术中TRILL是当前比较优秀的二层多链路解决方案，通过在局域网中引入类似于路由的寻路技术，解决了STP收敛速度慢，链路利用效率低的问题。当前，TRILL技术主要应用于数据中心网络，且并不是所有的交换机都支持该技术。

二层网络安全设计

二层攻击类型	二层保护机制
针对设备的DoS攻击	交换机CPU保护
流量超载	流量抑制/风暴控制
MAC欺骗	Port Security
DHCP攻击	DHCP Snooping
ARP攻击	限速/固化/隔离/DAI
源伪造攻击	IPSG

针对不同行为选用相应的安全机制。

  HUAWEI

- 在二层网络中，也存在着各种攻击，华为对各种可能出现的恶性攻击提供了相应的解决方案。
- DoS攻击：这类攻击的目标是交换机本身，可以使用CPCAR（Control Plane Committed Access Rate）限制单位时间内上送CPU报文的数量，对交换机的控制面进行防护。
- 流量超载：当网络中出现广播风暴的时候，或者当网络中出现攻击的时候，交换机端口就会出现持续的超限流量。可以在交换机上进行流量遏制，可以分别针对单播、组播、广播指定限制的流量比例。
- MAC地址表攻击：交换机基于MAC地址表进行数据的传送，而MAC地址表是由交换机侦听网络中的数据流量获得的，攻击者常常利用这一点伪造MAC地址攻击地址表。我们可以使用端口安全功能管理交换机端口的MAC地址，通过限制单个端口可以学习到的MAC地址数量，配置静态MAC地址，或者使用sticky MAC地址，可以有效地防止MAC地址表攻击。
- DHCP攻击：当前的客户机大量使用DHCP分配IP地址，DHCP也常常处于被攻击的状态，可以在交换机上开启DHCP Snooping功能，防止大部分的DHCP攻击。
- ARP攻击：在局域网中，ARP扮演着重要的角色，但是因为ARP缺少认证机制，常常被利用作为攻击手段。ARP攻击可以采用多种方法进行遏制，对于ARP flooding攻击，可以用交换机对端口的ARP流量进行限速，也可以手工配置静态ARP阻止攻击。ARP基于广播工作，所以细分VLAN隔离广播域可以减少ARP攻击的影响，更有一些特殊的VLAN设计譬如MUX VLAN，Aggregation VLAN可以用来隔离用户。另外，使用DHCP Snooping，将MAC地址、IP地址动态地与交换机端口进行绑定，然后开启DAI，对通过端口的ARP响应包进行校验。
- 伪造源攻击：IP协议缺乏源地址校验，所以网络中可能会存在大量的伪造源地址的攻击，在三层网络设备中，一般使用uRPF进行遏制，在二层网络中，我们可以采用IPSG技术对源地址进行校验。

案例分析

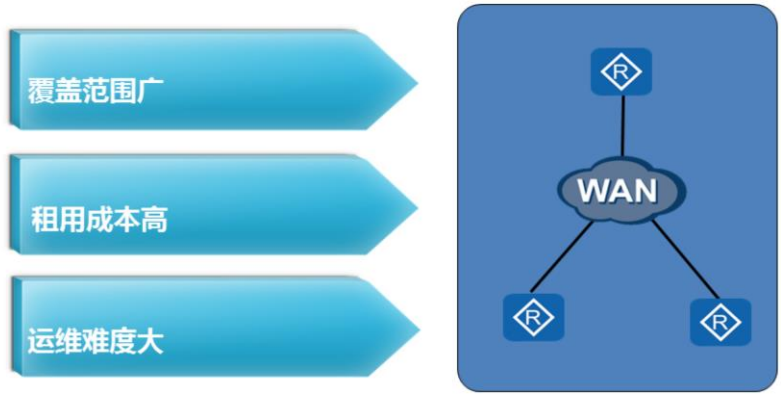
- 在校园网中，接入交换机到汇聚交换机之间采用二层互联，用户网关部署于汇聚交换机上，汇聚交换机与核心交换机间采用三层互联。为了进一步隔离广播域，请设计二层网络的VLAN划分方案。

  HUAWEI

- 校园网概况回顾：学生宿舍楼8幢，每个楼6层，一层楼4个单元，每个单元5间宿舍。计划在每个单元部署一台二层交换机，在每幢宿舍楼部署一台三层交换机。
- VLAN的划分方式并不唯一。为了提高安全性，可以尽量减小单个VLAN的规模，可以设计为一个寝室一个VLAN，甚至可以为每一个用户划分一个VLAN；如果为了管理方便，也可以每一台接入交换机划分一个VLAN，这样接入交换机就不需要VLAN配置了。
- 下面举例如果每一个宿舍划分一个VLAN的情况。在这种情况下，一台接入交换机上需要5个VLAN；一幢楼共24个单元，所以共有24个接入交换机，宿舍楼汇聚交换机终结二层网络，所以楼宇之间VLAN各自独立，VLAN编号在各个宿舍楼之间可以重用。一幢楼内需要120个VLAN，考虑扩展性和实意性便于后期管理，可以把楼层号规划为百位数，单元号规划为十位数，寝室号规划为各位数，合并起来组成VLAN编号。譬如VLAN425即为四楼二单元5号寝室的VLAN号。

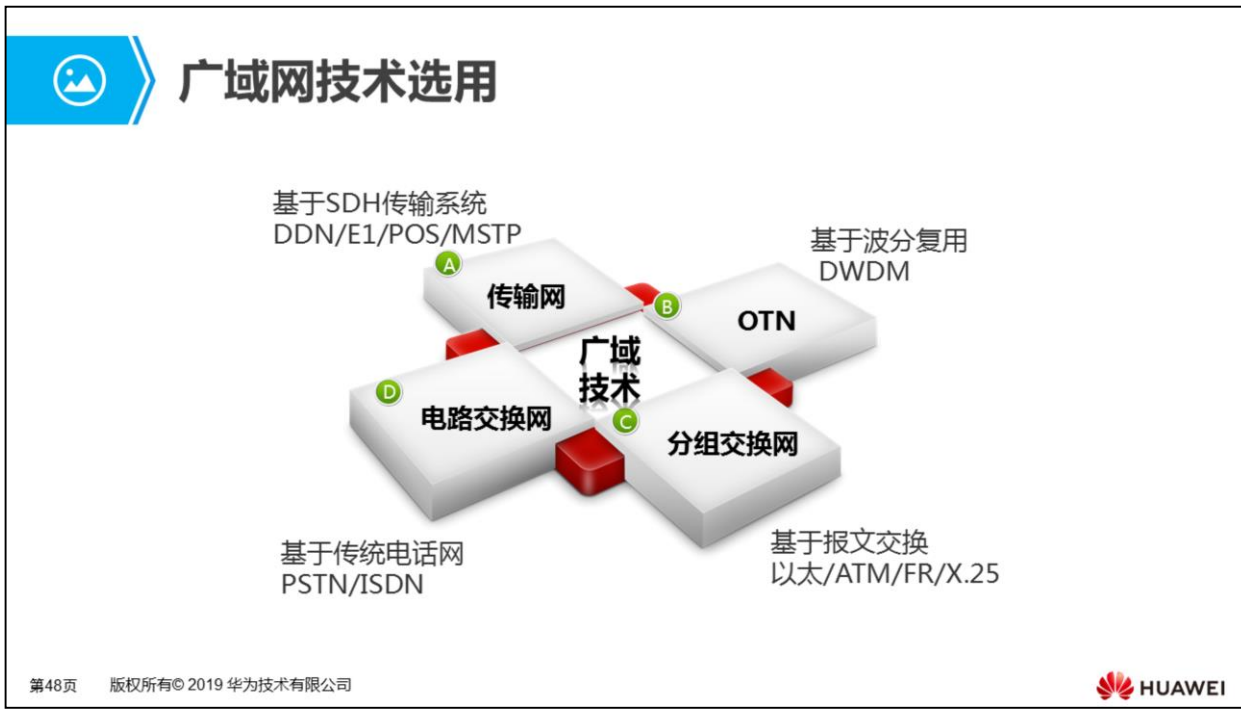
目录

广域网的特点



  HUAWEI

- 广域网地理跨度大，覆盖范围广。局域网一般位于一个房间、一层楼、一幢楼内，而广域网则常常可以跨越几十几百公里甚至更广。在局域网与广域网之间，按照地理覆盖范围，还有园区网这样的概念，园区网在企业中比较多见，一般覆盖一定范围内的多幢大楼，二层常常采用局域网技术。另外在运营商中还有城域网，接入网的概念，都是指特定的网络。
- 对一个企业来说，在很大的地理范围内自行铺设线路从经济上来看是不合算的，所以最常见的解决方案是租用运营商的链路，企业需要按月支付租用费用。
- 广域网的管理首先涉及到企业和运营商两个实体，在管理上涉及到界面和协商的问题。同时在大跨度的广域网中，大量的室外线路，跨越多个管理环节，故障率相对较高，修复时间相对较长。



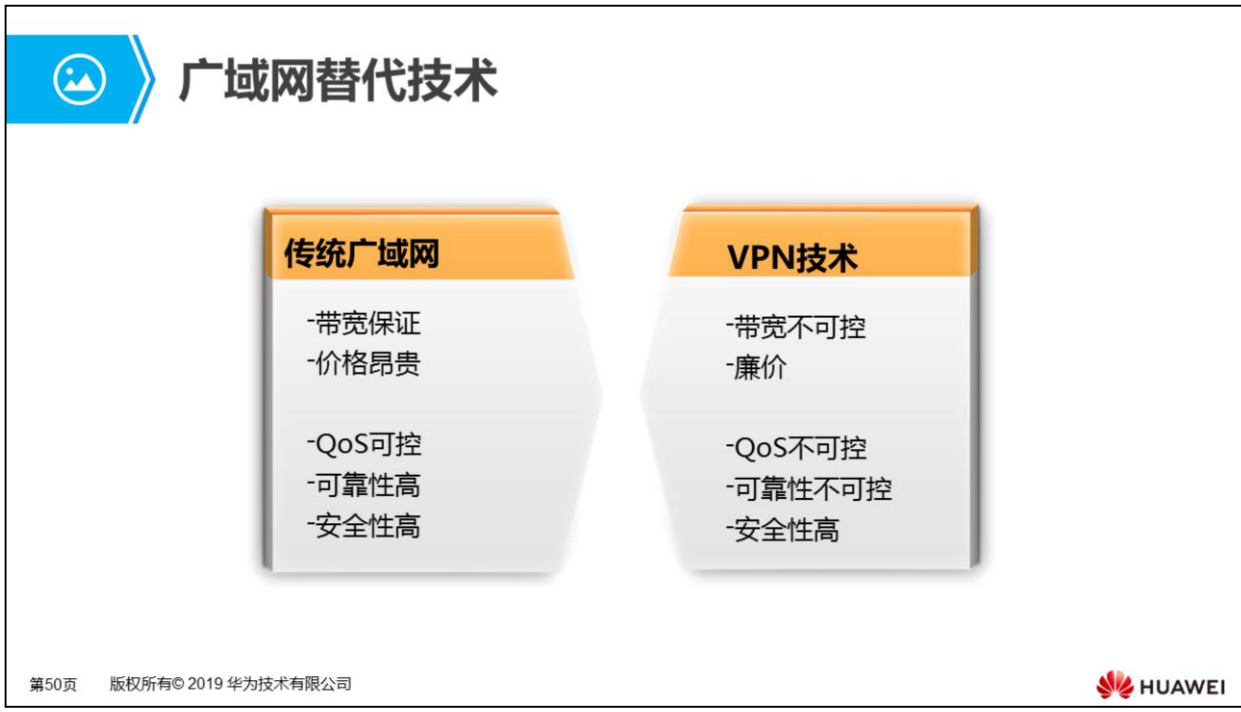
- 企业租用运营商的SDH传输网络时隙来传输业务数据，是最经典常用的广域网技术，是传输网络的分时复用技术。按照时隙的带宽大小可以分为多种类型。如DDN技术，一般以64Kbps为分配单位。E1线路，以2Mbps（64K*32）为分配单位。PoS链路，以155Mbps为基本单位，可以提供 622Mbps，2.4Gbps，10Gbps等传输链路。另外E1链路和PoS链路还提供信道化支持，例如一端为155Mbps的PoS链路，另一端可以按照信道分成63个E1链路。MSTP（Multi-Service Transfer Platform）（基于SDH的多业务传送平台）是在传统的SDH网络上，提供以太网、ATM等网络接口。
- OTN是采用波分复用（WDM）技术的光传输网络，提供大颗粒带宽的调度与传送，是替代当前SDH传输网络的下一代的骨干传输网。能提供GE/10GE级别的链路带宽，当前在各级网络干线上均有广泛的应用。
- ATM、帧中继、X.25等分组交换网基于PVC/SVC转发数据，可以在多个用户之间共享物理链路，网络自身具有一定的路由能力。不过当前因为效率、费用、质量控制等各方面的原因，用得相对较少。
- 电路交换网络利用传统的电话网络来传送数据。单路电话的带宽是64kbps，改进后的ISDN网络拥有144kbps的带宽。电路交换网络因为计时收费以及低带宽的特点，最初常常被用来作为备份链路。随着网络带宽需求的提升，当前电路交换技术已经基本不再使用。
- 部分运营商在一定范围内提供暗光纤出租业务。但是暗光纤的租用价格昂贵，而且在缺少中继信号放大器的情况下传输距离有限，所以使用并不广泛。

广域网二层协议

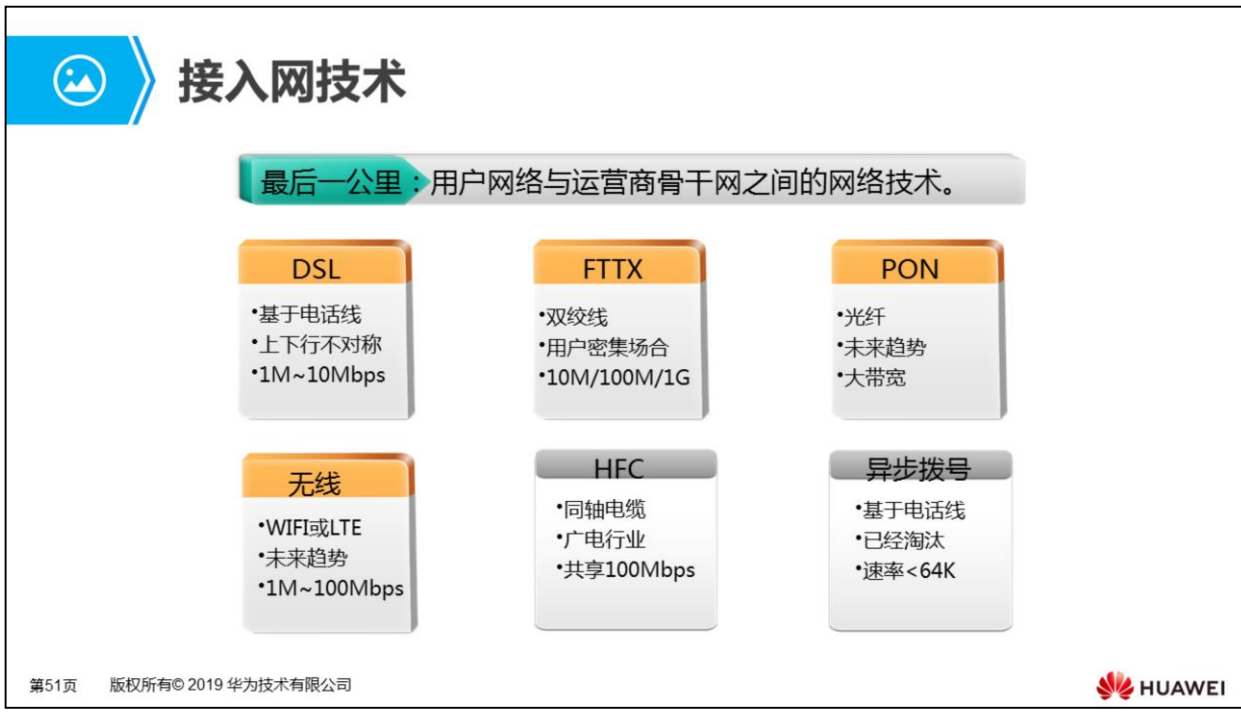
链路类型	结构特点	二层协议
DDN/E1/POS	点到点链路	HDLC/PPP
PSTN/ISDN	点到点链路	PPP
OTN	点到点链路	Ethernet
分组交换网	点到多点链路	以太 /X.25/FR/ATM

- 点到点链路是广域网络的主流链路。
- PPP协议是广域网点到点链路使用的主流协议。
- OTN网络可提供以太网接口接入。

- HDLC协议是面向BIT的链路层协议，适用于同步串行链路。缺少认证、多协议支持等功能，但是协议较为简练，承载效率高。当前数据网络中使用的HDLC协议是经过修改的。
- PPP协议是当前广域网络最常用的链路层协议，在同步串行链路和异步串行链路上均可以工作。PPP协议具有强大而丰富的扩展功能，譬如认证、链路捆绑、地址协商、数据压缩等。
- OTN网络作为新兴的大颗粒传输技术，在承载数据业务的时候，一般可直接提供以太网接口供用户接入使用。



- 前述均为传统广域网，不管哪种类型的传统广域网，均是基于带宽专用的基本思路，在时分复用的体系中划出一定的时隙，或者在波分复用的系统中划定一定的波长。这部分划分出来的带宽是专用的，如果用户暂时没有数据需要传输，这部分带宽就处于空闲状态。因为带宽专用，所以传统广域网线路的租用价格昂贵，但是也有QoS可控性好，安全可靠的特点。传统广域网中的分组交换网引入了部分统计复用的概念，但是一般都设计了很好的QoS机制，能够有效地保证用户带宽。
- VPN技术是传统广域网很好的替代方案，当前真实项目中的使用也比较广泛。这里的VPN技术是指利用因特网（Internet）建立虚拟私有网络的技术。采用VPN，客户只需要支付当地互联网的接入费用，就可以与世界上任何一个地点联网，极大地节省了网络成本。但是VPN数据子互联网上传送，缺少带宽的保证，QoS和可靠性也是基于互联网的基本特性，在互联网上的安全性相对较差，但是可以使用技术手段做一定的弥补。



- 严格来说，接入网并不是广域网。它仅仅解决从用户到骨干网那一段距离，一般形象地称为最后一公里。接入网一般为数据网络业务的接入提供服务。
- 运营商为了利用原有投资尽量节约成本，在原有线路上发展出了各种技术，譬如电信运营商在电话线路上提供异步拨号技术，提供64Kbps以下的带宽，后来又发展出了ISDN、DSL等技术，分别提供128Kbps和10Mbps以下的带宽。
- 广电运营商在同轴电缆上，发展出了HFC技术。提供以百兆计的带宽，但是带宽需要在一条同轴电缆的不同用户之间共享。
- FTTX利用以太网技术接入用户，以太网本身并非接入网技术，但是以太网廉价高速，很好地适应接入用户密集的情况。
- PON无源光网络是为用户提供光纤接入；随着移动互联网的发展，无线接入也越来越成为一种重要的接入方式。

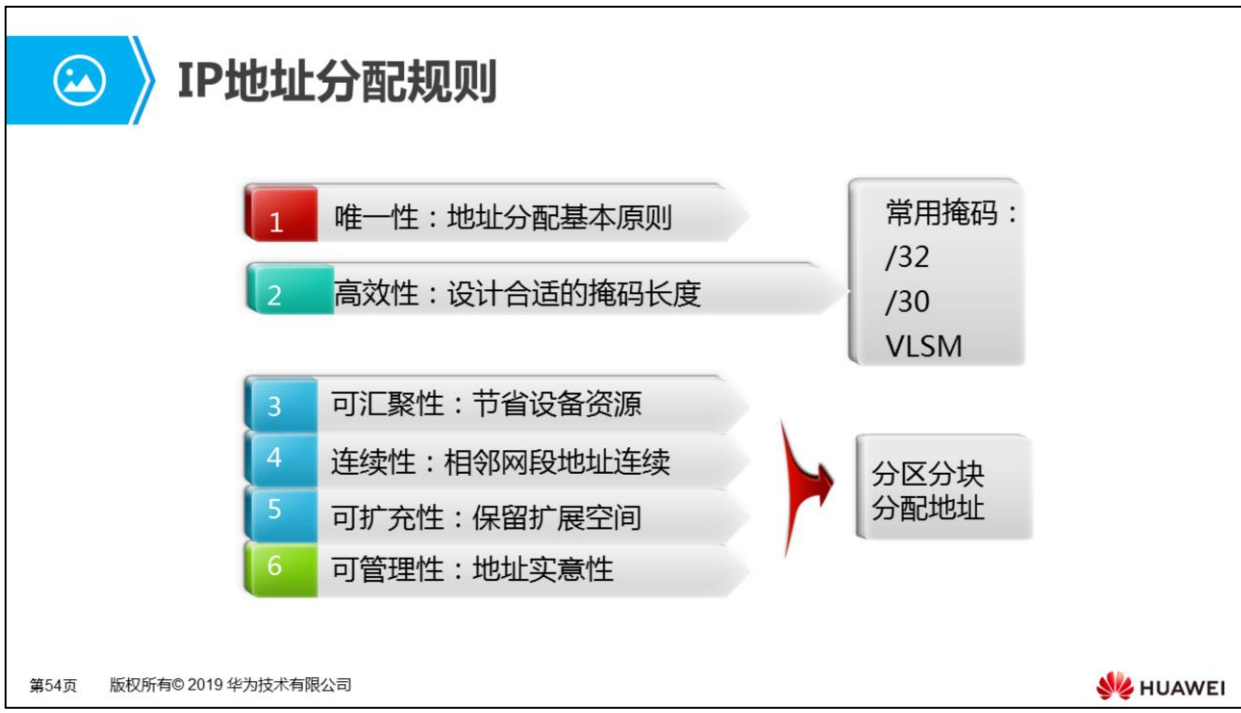
案例讨论

- 校园网需要与教育网连接 ，教育网的接入点位于同城，直线距离大约10km左右，带宽初步估计需要约1G，请问选用何种链路技术？

  HUAWEI

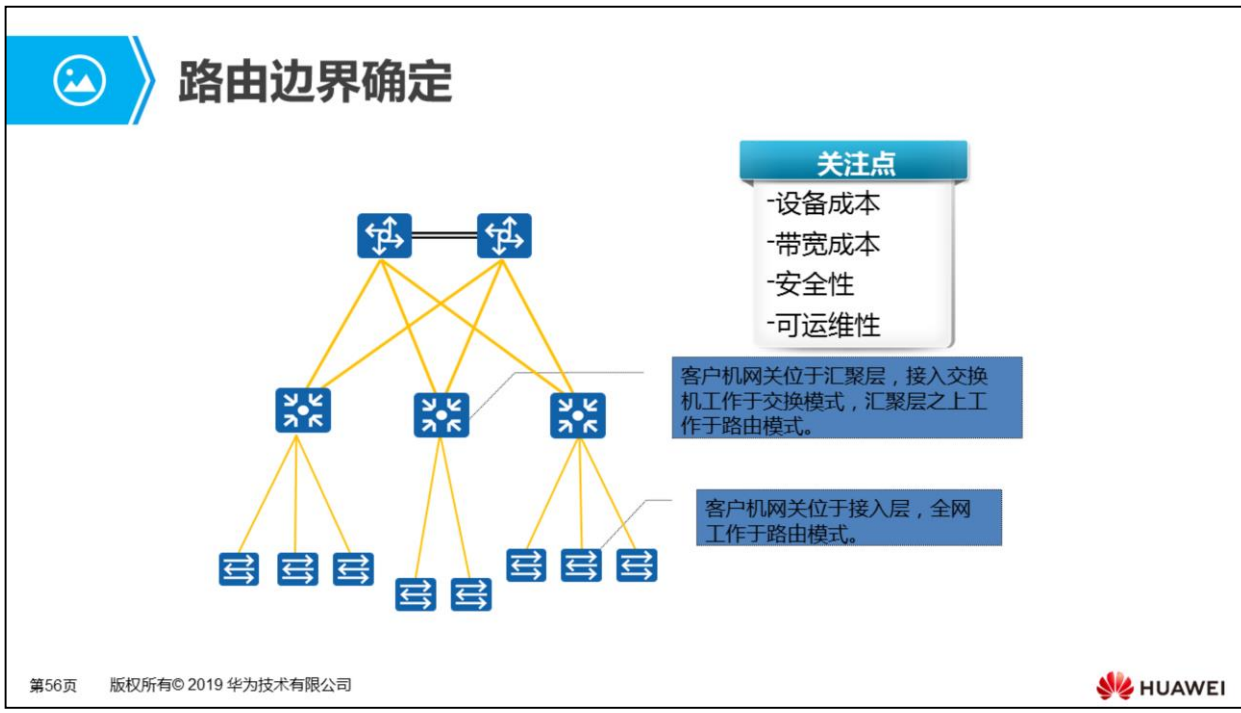
- 在工程实际中，链路的选择有多种可能，具体选择的时候需要考虑价格、成本、可得性等非技术因素，与客户紧密合作共同决定。
- 能提供1Gbps以上带宽的技术当前主要为以太网和POS两种技术。POS技术价格较为昂贵，目前用得较少。一般直接使用以太网。如果采用以太网的话，底层可以选择OTN；因为距离只有10km，所以也可以考虑裸光纤。这两者在承载效果上差别不大，所以主要考虑价格与可得性，可以与当地运营商联系协商确定价格，选择一个租金便宜的即可。如果当地运营商提供MPLS VPN，也可以考虑采用该种技术承载。
- 接入网技术在这个案例中可能会涉及，但是我们要知道接入网技术并不是一种端到端的技术，它仅仅解决从客户到运营商局端的链路，所以在本案例中可能会涉及接入网，但是不大可能从学校到教育网全程用接入网技术解决。

目录



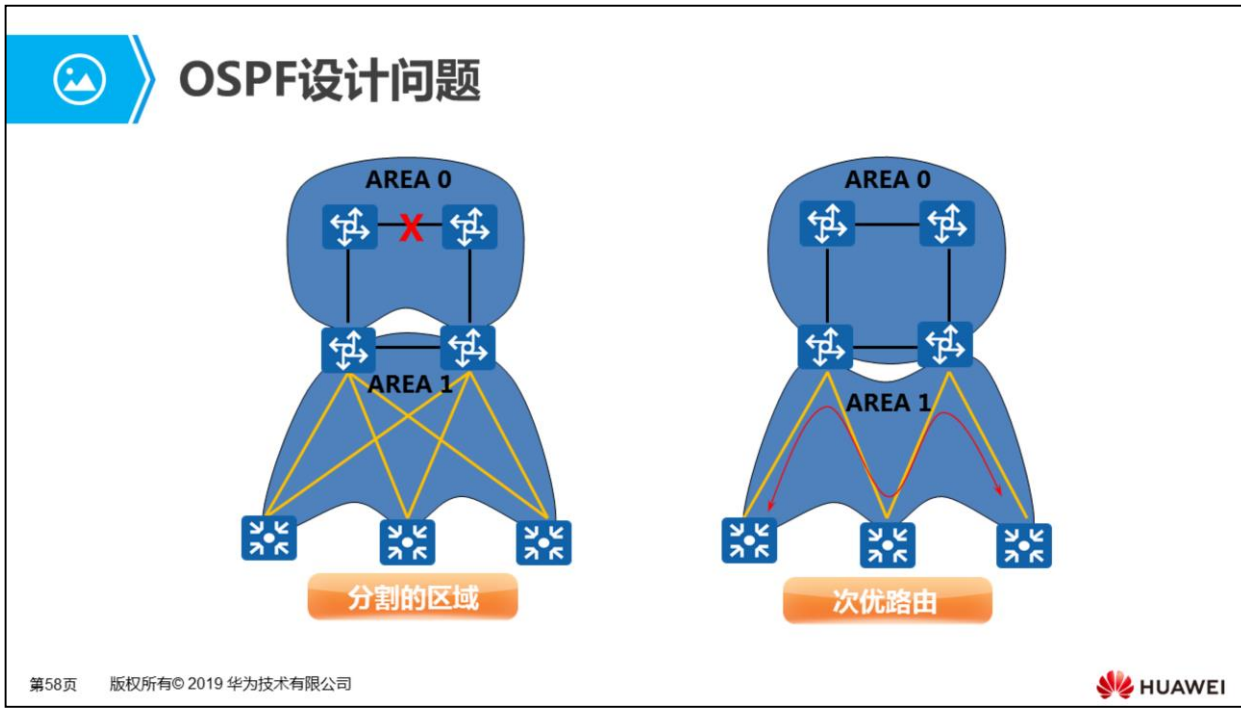
- IP地址分配设计是三层网络设计的最基本工作。
- 除了某些特殊的应用，IP地址要求在全网范围内具有唯一性。这是IP协议提供寻址功能的最基本条件。
- 最初IP单播地址被分为A、B、C三类，掩码分别固定为/8、/16、/24，导致地址严重浪费；路由协议也与此对应，称为有类路由。为了充分利用IP地址，发展了VLSM技术，我们可以根据需要设定掩码长度。当前网络设备上最常用的掩码长度为/32和/30，/32一般用来标识一台设备，称为主机路由，/30用在点对点链路的两端。对于局域网，一般根据用户的数量设计合适的掩码长度。
- 设计地址分配的时候，要考虑路由的效率，对于路由设备来说，路由条目越少，工作效率越高。所以在地址分配的时候，要考虑地址是否可以被汇聚。要保证地址可以被汇聚，则必须在网络分区中分配连续的地址块；为了保证后续扩容的时候地址不凌乱，还要在每一个网络分区保留扩展地址空间。分区分块地分配地址，还能够使地址具有一定的意义，便于后期运维。

- 网络设备上的IP地址，除了部分拨号VPN之外，其他地址一般都是手工静态配置的。手工静态配置地址，安全可靠，不易被攻击，但是配置工作量大。对于客户机来说，大量的手工工作容易出错，也容易造成地址冲突。
- DHCP是当前常用的客户机地址配置方式，DHCP服务可以启用在专门的服务器上或者路由端口上。如果使用专门的服务器，需要在各个网段的网关处配置DHCP中继。
- 使用DHCP可能会导致一定的攻击，但是针对这些攻击，有相应的安全机制，如DHCP snooping，可以防止仿冒Server攻击，同时，DHCP Snooping得到的绑定表，还可以用于DAI，防止ARP攻击；用于IPSG，防止伪造源IP攻击等。

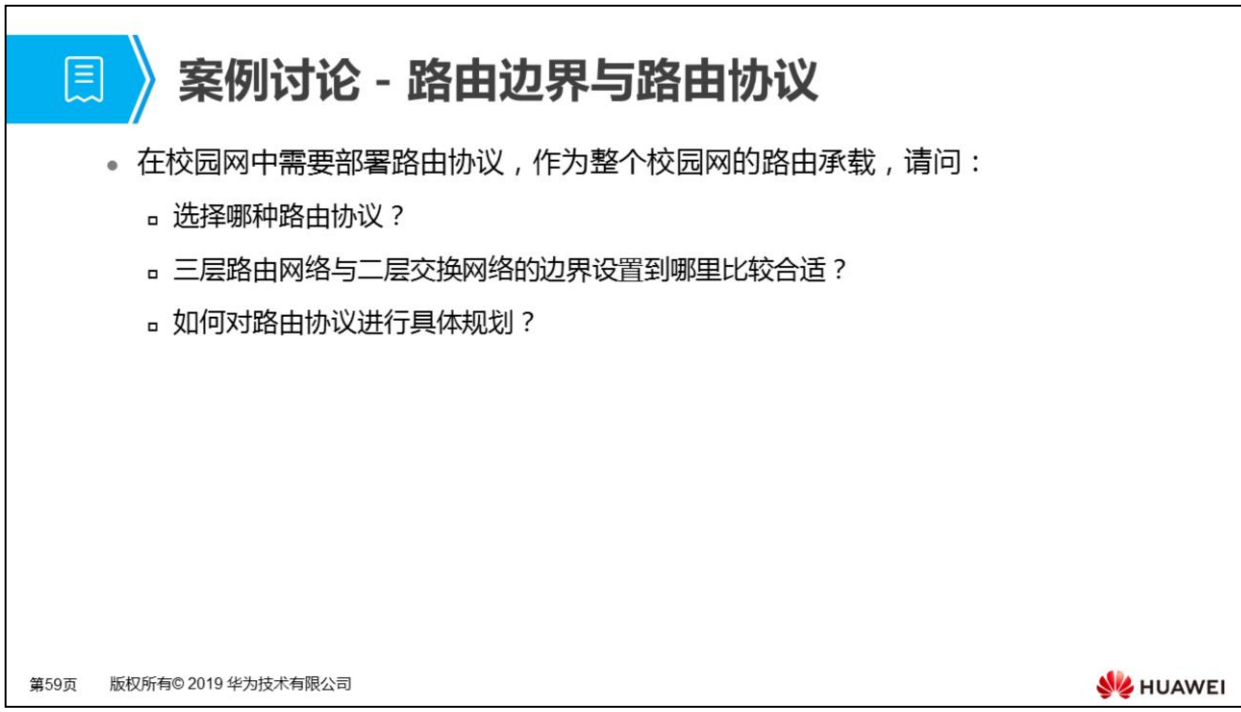


- 路由与交换相比，各有各的优势。三层网络需要采用路由器或三层交换机，而二层网络只需要二层交换机即可。交换机的处理能力和交换容量均大大高于路由器。但是二层网络的工作是基于广播的，每一个设备均会发送一定数量的广播数据包，当二层网络太大的时候，广播流量就会叠加。
- 二层网络出现链路冗余的时候，一般使用STP破环，跟路由协议相比，STP收敛速度慢，稳定性差。如果发生环路，广播风暴将使整个二层网络处于不可使用的状态。三层网络采用路由协议，当前一般采用链路状态路由协议，收敛迅速而且无环路隐患，稳定性优于二层网络。当然交换机也提供了链路捆绑，双机集群以及其他一些优化的防环机制，使得二层网络既能提供冗余提高可靠性，又尽量地避免了环路。
- 三层网络需要配置IP地址和路由协议，如果网关过于接近用户，又会导致地址段细分，管理维护工作量加大。
- 当前网络中，广域网基本都采用路由架构。因为广域链路价格昂贵，应该尽量遏制广播数据。
- 在园区网络中，需要综合考虑成本、带宽、可靠性、安全性和可运维性，根据不同的场景需求设定二三层的分界面。一般常规的做法是将网关设置于汇聚层，而接入常常不设冗余或仅仅是一个双上连冗余，避免或简化STP的使用；某些场合也有把网关设置于接入层的，最大限度地提供冗余和加快收敛。
- 在某些特殊的网络中，因为数据量的巨大或者接入用户的巨大，发展出了一些特殊的技术，譬如运营商的接入，为了降低设备成本和管理复杂度，二层规模设计得比较大，而为了提高安全性，于是采用QinQ技术实现用户之间的隔离；又譬如在数据中心，当前的趋势是采用大二层的设计，将网关上移至核心设备。

- 在当前的IPv4环境中，常用的路由协议为以下三个：OSPF、ISIS、BGP。
- OSPF与ISIS都是链路状态路由协议，OSPF是IETF设计的专用于IP网络的路由协议，ISIS是由ISO规范的，出现得比OSPF略早。这两个协议的框架和算法都非常相似，但是在细节上有很多的不同，导致它们在扩展性、收敛速度等方面有一些细微的差异，同时因为一些历史因素，使得ISIS在运营商的骨干网络中用得较多；其余场合，一般都采用OSPF。
- BGP是当前唯一在使用的外部路由协议，支持自治域间的路由能力。BGP一般用于多个企业或运营商的互联，在中小型的企业网络中很少使用。但是在大型企业中，如果网络规模超越了单个机构的管理能力或者超越了单个IGP的支撑能力，也会将内部网络分成多个自治域，然后用BGP进行互联。另一种在企业网内使用BGP的场景是当企业部署了MPLS/BGP VPN的时候，BGP作为该架构的必备组件出现。
- 除了动态路由协议之外，我们还可以配置静态路由，静态路由使用简单方便，常常用在没有冗余链路的网络末端或者网络出口。



- 一般来说，OSPF本身严谨的算法保证了网络中不会出现环路之类的严重问题，但是如果设计不当，还是会出现区域分裂、次优路由等问题。
- 拓扑图一是常见的路由设计场景，初始设计的时候并没有什么问题，但是骨干区域的连接比较薄弱，如果出现链路故障的时候，可能会导致区域分割，从而引发路由问题。
- 拓扑图二也是常见的路由设计场景，但是在这个场景中隐藏着次优路由问题，当两个接入层路由器互访时，并不会通过汇聚路由器之间的互连链路，而会选择双上联的接入路由器作为中间跳。
- 总的来说，OSPF是一个较为稳定、可靠的路由协议，在设计时充分考虑，可避免出现一些类似问题。



- 作园区网，可优先选择OSPF路由协议。OSPF协议对园区网络的适应性较好。
- 在实际组网中，用户网关设置在汇聚层较为普遍。这种设置方式，很好地折中了运维复杂性和网络性能。在当前校园网中，汇聚到接入交换机之间没有冗余链路，不会产生二层环路。
- 而汇聚与核心设备采用冗余链路，运行于路由模式可以提高网络收敛速度及链路的利用率。
- OSPF路由协议是一种层次化的路由协议，在部署时，可以划分不同的区域。
- 在校园网中，接入交换机工作在二层网络，所以不需要起用路由协议。
- 将校园网的汇聚层和核心层交换机划分到不同区域。
- 校园网核心配置为OSPF的骨干区域。园区中存在的其他模块的网络，可以适当地各自划分区域。

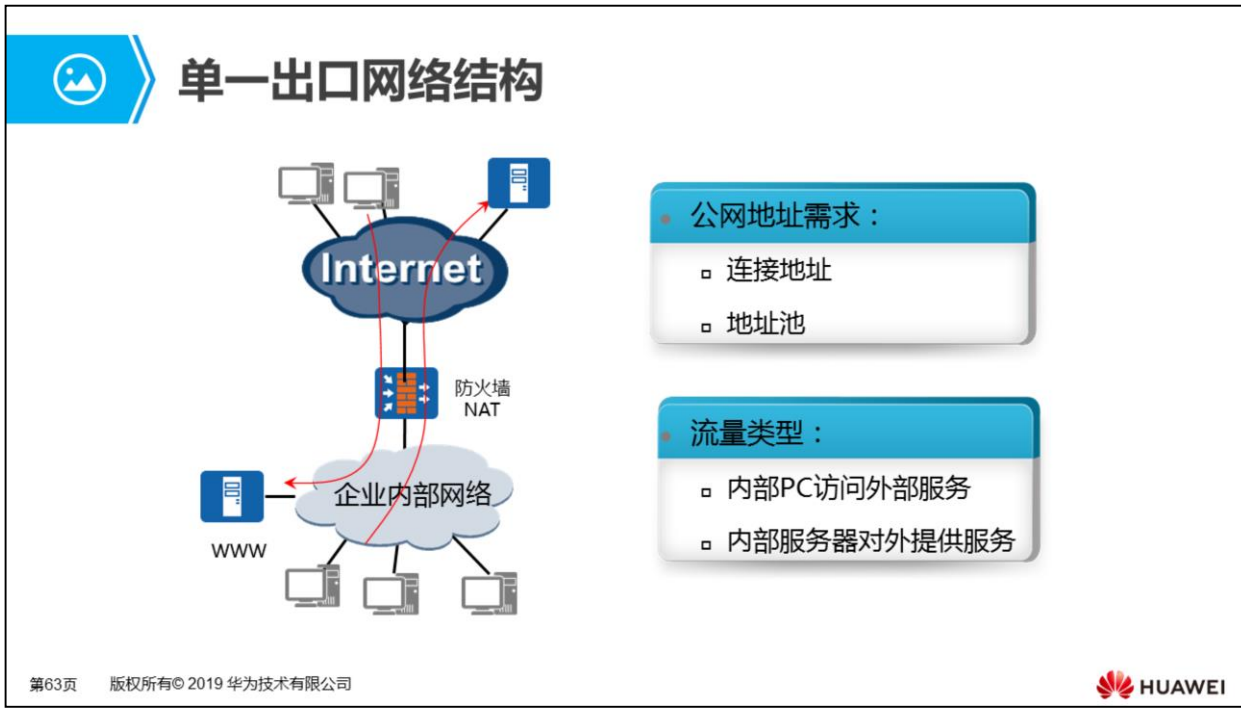
案例讨论 - IP地址分配

- IP地址分配方案。
  - 因为校园网的规模，建议使用10.0.0.0/8网段（如果有教育网地址段，请用相应的网段），此处按照一个寝室一个VLAN的方式划分网段。

楼号	楼层	单元号	房号	网段	网关地址
1号楼	1楼	1单元	1	10.11.11.0/29	10.11.11.1/29
			2	10.11.12.8/29	10.11.12.9/29
		2单元	1	10.11.21.0/29	10.11.21.9/29
			2	10.11.22.0/29	10.11.22.9/29
	2楼	1单元	1	10.12.11.0/29	10.12.11.1/29
			2	10.12.12.8/29	10.12.12.9/29
2号楼	1楼	1单元	1	10.21.11.0/29	10.21.11.1/29

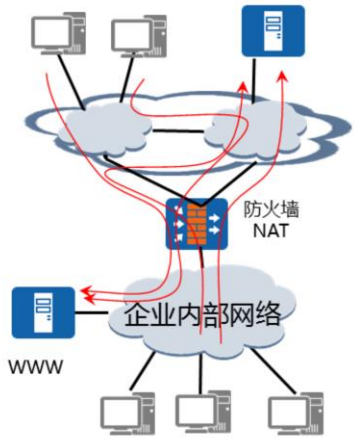
目录

- 连接互联网是当前企业网络的基本需求。互联网的连接需要解决以下问题。
- 链路的选用：理论上来说，连接互联网可以使用本文之前讨论过的任何一种链路。但是在现实中，我们需要综合考虑带宽，成本，质量，距离等各方面的因素，当前企业的出口常常采用光纤承载，PON网络和光以太网是常见的链路形式。对于部分小企业，也有采用DSL等家庭接入技术的。
- IP地址：当前IPv4的公网地址紧张，企业内网一般都是采用私网网段。为此，内网用户要访问互联网，必须进行地址转换，也就是NAT（Network Address Translation）。
- 设备配置：当采用不同的链路的时候，首先需要链路适配，譬如DSL链路需要配置DSL Modem，PON链路需要配置ONU。因为网络出口设备需要进行IP地址转换，除了某些框式交换机之外，一般交换机不提供NAT功能；所以出口设备常常选用路由器或者防火墙。
- NAT技术是一个需要大量处理能力的处理过程，对于大规模、大流量的NAT来说，防火墙比路由器更适用。同时，NAT一般出现在网络边界上，防火墙同时能够提供边界防护。所以在企业网络边界上，防火墙用得较多。



- 单一出口的网络虽然可靠性不高，但是成本低廉，结构简单，在非关键业务的大中小企业中均有广泛的应用。
- 连接到运营商的网络时，运营商一般会给出两类公网地址，一种是连接地址，这个地址一般是一个/30掩码长度的地址，用来配置在连接链路上；另外，运营商还会给出一个地址池，这个地址池就是用来给企业内部设备连接互联网时用来做地址转换的，一般来说，这个地址池的地址数量比较少，不够用来给内部的每一台PC分配一个公网地址。如果有小企业采用PPPoE的方式，一般就获得一个动态分配的公网IP地址。
- 对于只有一个出口的企业来说，一般使用静态配置的缺省路由指向互联网，对于运营商来说，因为存在信任边界的问题，所以一般也采用静态路由进行回指。
- 对于一个企业的互联网流量来说，一般可以分为两类：一类是内部用户访问外部服务器的流量；另一类是外部客户访问内部服务器的流量。这两类流量最大的区别是服务器必须要有固定的公网地址，保证客户机能够随时找到服务入口。在工程中，经常使用静态NAT将内网服务器地址映射到公网地址；而内网用户则使用动态PAT最大限度地复用公网地址。

同运营商多出口结构

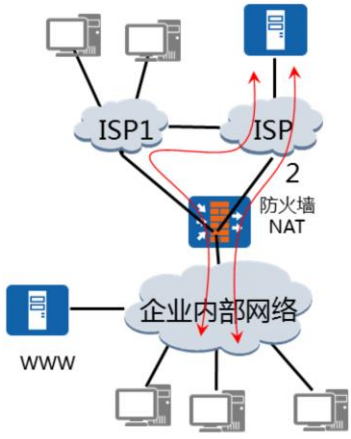


- 提供冗余
- 两个连接地址，一个地址池
- 出向路径选择
  - 路由指向
- 入向路径选择
  - 缺乏可控性

HUAWEI

- 部分企业为了提高冗余性，选用两路出口；如果双出口都是连接到同一个运营商的，那么运营商在提供链路的时候，一般会同时提供两个连接地址，但是地址池还是一个。所以当内外数据流通的时候，NAT地址的转换与单一出口一致，不同的地方是两条链路需要选路。
- 运营商因为信任边界的问题，一般还是不会与企业用户之间运行动态路由协议。对于访问企业的数据流，基本不会做特别的控制，按照自身网络路由协议的计算传送到相应的接口。
- 对于企业来说，可以用静态路由明细条目的方式对数据进行分流，因为两个出口均连接到同一个运营商，所以不管数据流走的是哪条链路，一般认为因路径差别导致的性能差距不大，分流的目的主要是为了充分利用出口带宽。
- 也有企业采用主备方式利用两条出口链路的，这种方式下，可以采用浮动静态路由来实现。

多运营商多出口结构 - 出向流量

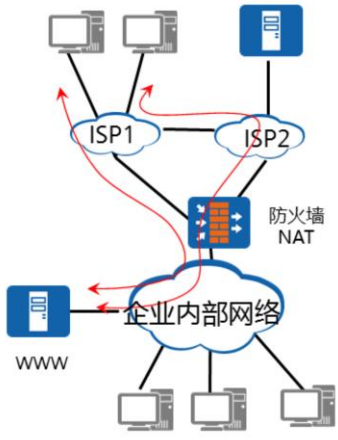


- 连接条件
  - 两个连接地址
  - 两个地址池
- 出向路径选择
  - 路由优选
- NAT地址池选择
  - 与路径选择对应

HUAWEI

- 当前大中型企业中，很常见采用两个运营商各一条链路的双出口解决方案。这种情况下，每个运营商都会提供一条连接链路，同时各自提供一组连接地址和一个地址池。
- 两个运营商之间一般会存在数据通路，但是这个通路一般不会存在于本地，而会在核心层面；而且两个运营商之间的连接不如运营商内部的连接强壮。所以当流量在运营商之间贯穿的时候，服务质量会出现较大的劣化。
- 当内网中出现访问外网的数据流量的时候，首先得指向正确的链路，防止流量走向错误的方向导致质量劣化。因为企业与运营商之间一般使用静态路由，所以这部分的实现需要收集运营商的公网地址空间。
- 还需要考虑返回流量，因为NAT的关系，返回流量其实是由地址池的选择决定的。如果出向流量选择的NAT地址池是由ISP1提供的，则返回流量必然使用ISP1的链路。所以NAT地址池与数据流的出端口需要绑定。

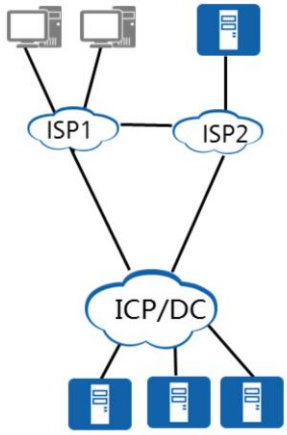
多运营商多出口 - 服务器访问流量



- NAT映射
  - 服务器地址同时静态映射到两个地址池的地址
  - 用户从哪条链路进入访问服务器与连接的地址有关
- 出向路径选择
  - 静态路由优选

HUAWEI

多运营商多出口结构 - 对等方式



- 常用于ICP，DC等场合
- 需要公网IP和AS号
- 无NAT
- BGP选路

HUAWEI

- 前面讨论的企业网络出口都是作为运营商的接入用户连入互联网，另一个解决方案是作为一个与运营商对等的实体接入互联网。但是这种方式的接入，需要从全球的网络信息中心（NIC）申请公网地址和公网AS号。这种连接方式常常是有大规模的服务器向互联网提供服务的场合，如ICP、数据中心等场合。
- 这种接入方式在对外提供服务的时候，不需要做NAT地址转换。与各个ISP使用BGP交换路由信息，在路径选路的时候遵循BGP的选路原则。

项目案例

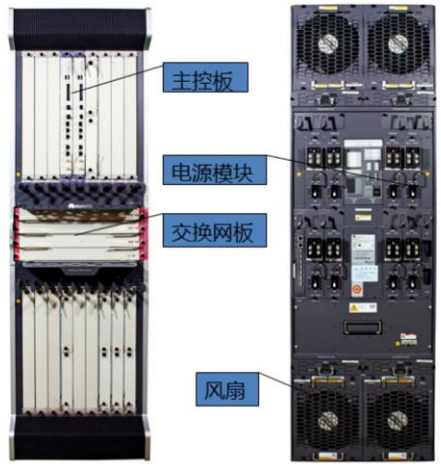
- 校园网通过单一链路连接至教育网，同时网内有服务器向教育网提供服务。请为校园网设计网络出口结构。

- 这是一个简单的单一出口设计。但是要考虑到两种类型的流量，一种是内部用户访问外部服务的流量，这种流量一般需要部署NAPT地址转换；另一种流量是外部用户访问内部服务器的流量，这种流量一般需要部署静态NAT。

目录

- 高可用（High Availability）网络是指网络设备和系统经过一定的设计之后，能够减少网络中断的时间，尽量保持网络提供服务的时间。高可用性一般用网络提供服务的时间长度与总时间的百分比作为指标。要提高网络的可用性，就需要提高网络能够正常提供服务的时间，或者缩短故障后网络不能提供服务的时间。
- 提高网络的可用性，首先需要采用高可靠性的设备，这些设备常常采用器件冗余的设计；另外在网络设计的时候，可以采用多设备冗余和多链路冗余，保证在单一设备或链路出故障的时候，网络服务不会中断，或者短暂中断后自动切换到备份链路上去；设备和链路的切换，都需要协议的配合，某些协议如生成树协议，路由协议等在完成动态选路的同时也完成了路径的切换，某些协议如VRRP、BFD则完全是为了提高网络系统的可用性而设计的。

器件与设备冗余



设备中的器件冗余

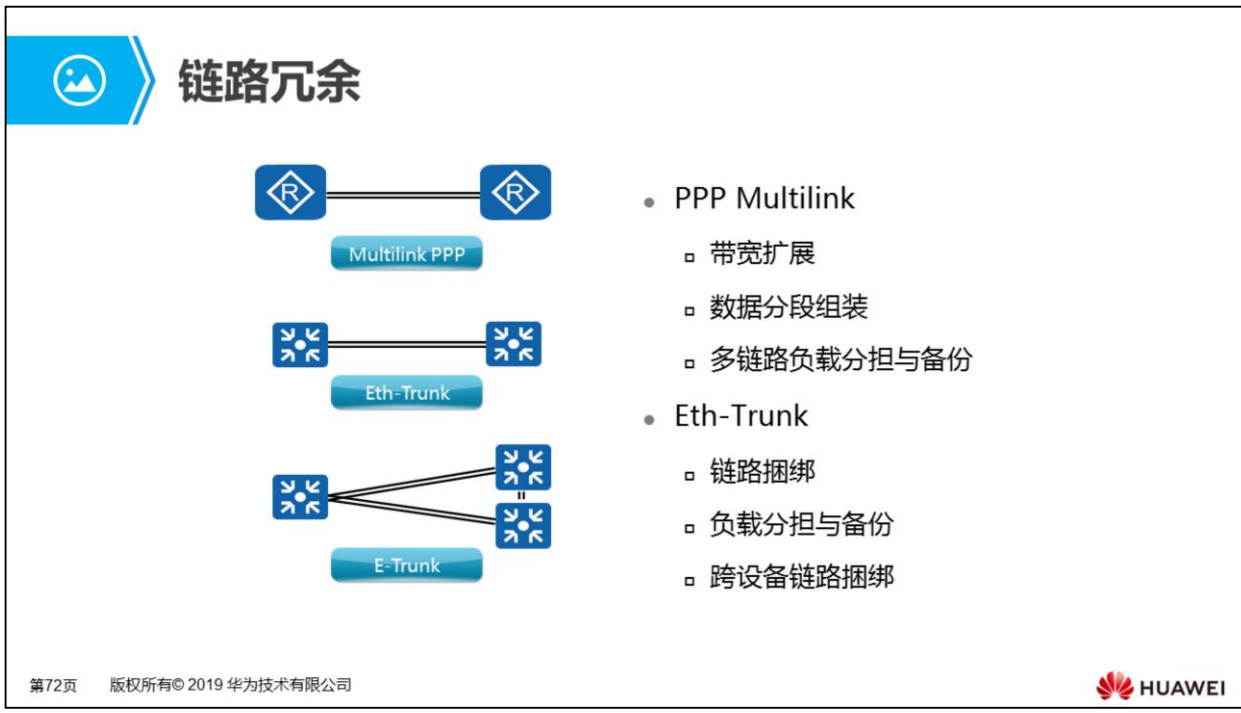
- 电源
- 风扇
- 主控板
- 交换板

网络设计中的设备冗余

- 堆叠
- 集群

HUAWEI

- 提高系统的可用性，首先是从设备上着手。单一器件总是不可避免出故障，所以，提高系统可用性的方法是提供冗余部件，一般盒式设备作为低端接入层设备，对可用性的要求不高，常常缺乏冗余器件设计；而框式设备，常用作汇聚层、核心层设备，出故障的话影响范围大，所以常常会设计冗余部件，如冗余电源，冗余风扇，冗余主控，冗余交换网板等。保证当单个器件出故障的时候，整个设备不至于停止服务。
- 在网络设计中，为了进一步提高网络系统的可靠性，还提供了双设备或多设备的集合技术。对于盒式设备来说，某些特定的型号有堆叠技术，可以将多台设备组合成一台设备工作；对于框式设备，华为提供了CSS（Cluster Switch System）功能，可以使两台框式交换机组成一个集群。

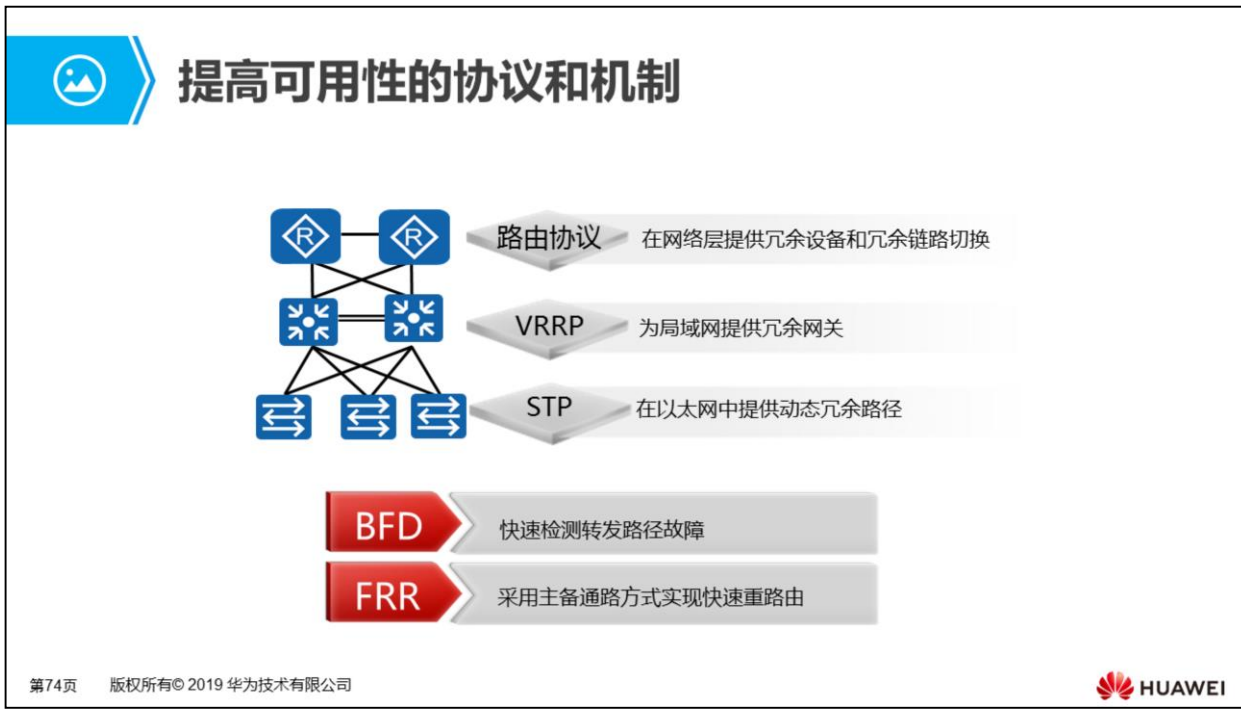


- 某些链路层协议提供了多链路捆绑的技术，这些技术最主要的目的是为了扩展带宽，减少网络延迟。但是在达到这些目标的同时，这些技术也提高了网络的可用性。捆绑的链路相互之间是负载均衡的关系，当其中一条成员链路中断时，流量能够动态地转移到仍能正常连接的链路上去。因为这种切换是在链路层完成的，所以切换速度远快于网络层的切换。
- 常见的链路捆绑包括PPP Multilink和Eth-Trunk；PPP能够动态维护链路，并对数据包进行分段和组装（LFI：Link Fragement and Interleave）。Eth-Trunk一般不对数据包分段，仅仅在不同链路之间负载均衡；Eth-Trunk有两种配置方式，一种是手工静态配置，一种是使用LACP协议动态协商，因为以太网本身缺乏OAM，所以建议使用动态协议。
- 华为还提供跨机框的以太链路捆绑技术E-Trunk，在某些高可靠性要求的场合使用。

项目案例

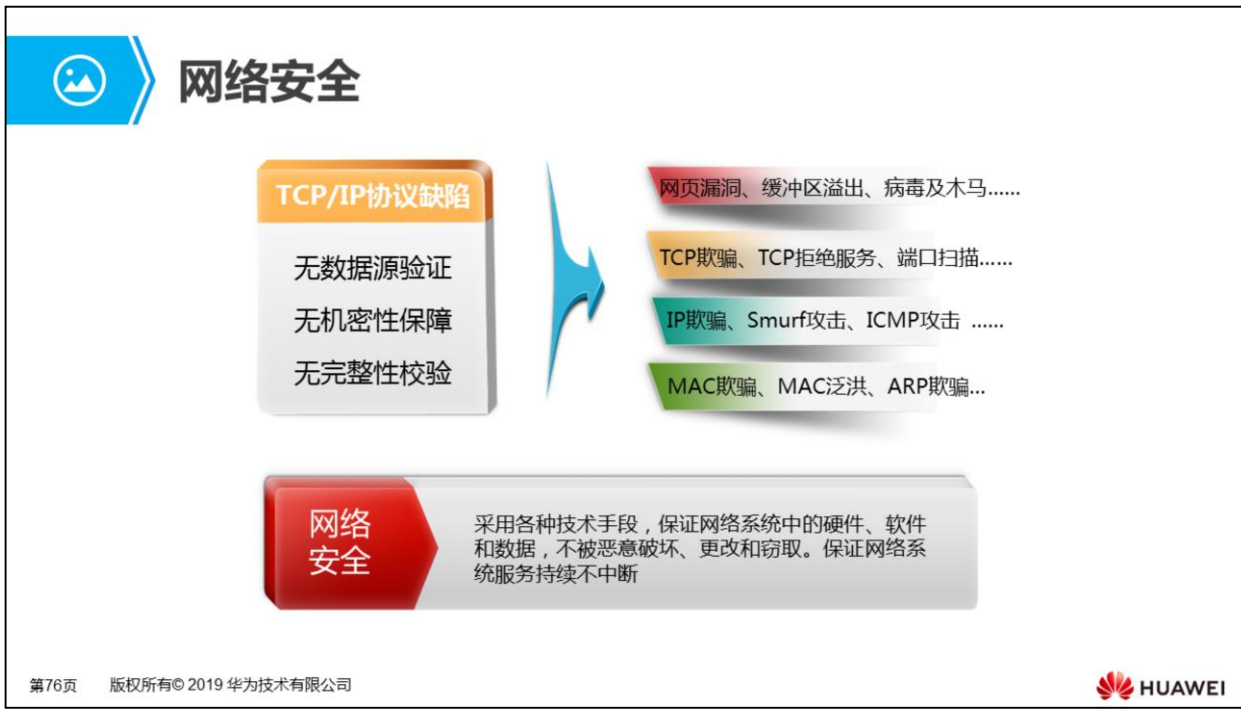
- 经双方评估后，工程人员与校园网项目组达成共识，对校园网可靠性的要求在各个部分是不同的，譬如学生宿舍接入对可靠性的要求并不高，在汇聚层之上要求具备一定的可靠性。请对该需求做出网络设计。

- 园区网络接入大量学生用户，业务并非关键，所以在接入层到汇聚层一般就不采用冗余设计。特别是设备不冗余。在链路上可以考虑根据带宽利用率，部分采用双链路捆绑的方式上联到汇聚层设备。在汇聚层往上连接到核心层采用双链路上联，核心层采用模块化交换机，双机冗余，正常情况下工作在负载分担模式。
- 接入到汇聚运行于二层，网关位于汇聚层设备，无冗余，运行STP，仅用于防止出现错误操作导致的环路；网关位于汇聚层设备，因汇聚层设备本身无冗余，所以网关设置也不需要冗余，三层部分由路由协议提供故障切换和保障。因用户的上网业务并非关键，所以不引入BFD/FRR等复杂技术。

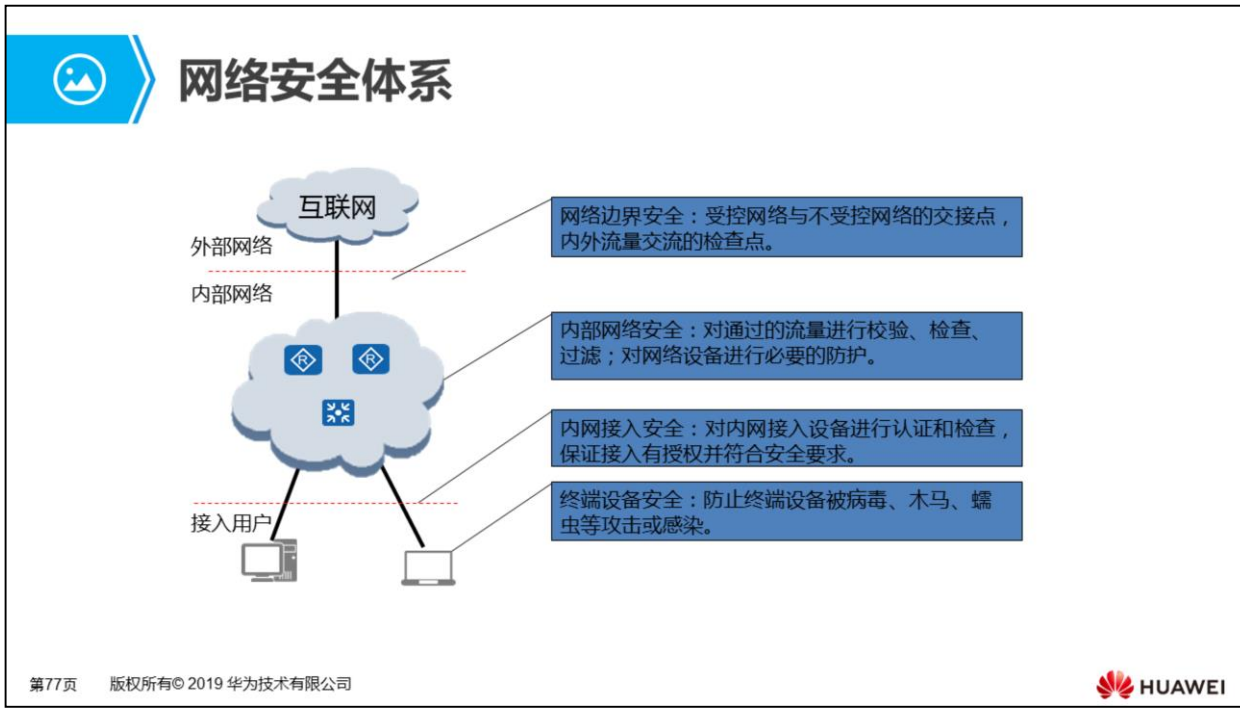


- IP协议进行设计的时候，本身就考虑到了节点故障的问题。所以路由协议和生成树协议在选路的同时，本身就提供了动态切换流量路径的功能，能够在网络有冗余链路的时候提供切换。保证网络可用。
- 终端设备一般不运行路由协议，采用静态的方式指向网关设备，为了提供网关设备的冗余，我们可以采用VRRP。VRRP的切换时间一般在3秒左右。
- 不管是路由协议还是VRRP，切换的前提条件是检测到故障，这些协议的检测思路一般是各设备定时发送特定的报文，同时在接口监听，如果持续一段时间未收到对端的报文，则认为对端设备故障。这种检测方式往往需要几秒到几十秒的时间。为了减少检测故障的时间，发展了BFD技术，BFD技术能够以毫秒为间隔发送检测报文，在几十毫秒内确认故障，能够极快地检测故障。
- FRR（Fast ReRoute）快速重路由预先计算好一条备份路由，对主路由提供保护，当主路由出现故障的时候，立刻切换到备份路由上，切换过程省去了路由更新、SPF计算、新路由加载这些步骤，极大地减少了切换延迟。
- 对一般的数通网络来说，并不一定要求毫秒级的收敛速度，所以BFD和FRR技术在普通数通网络中应用并不广泛，这些技术一般在IP承载网络中大量使用。

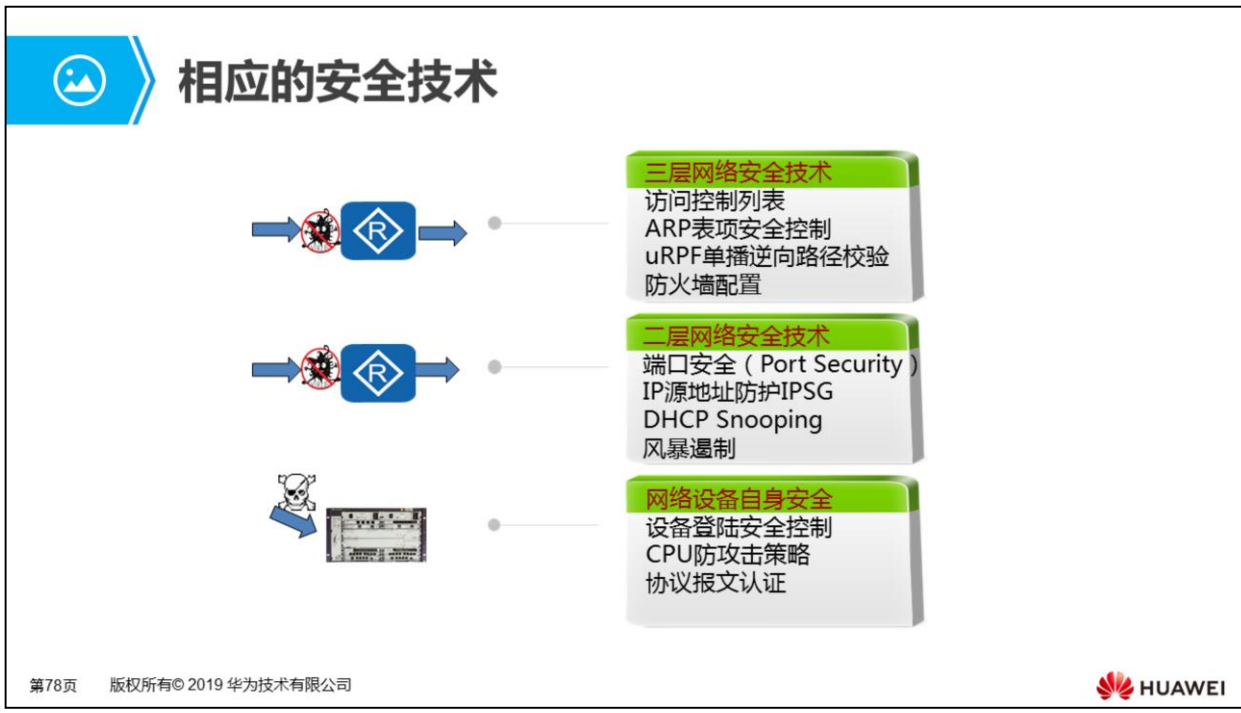
目录



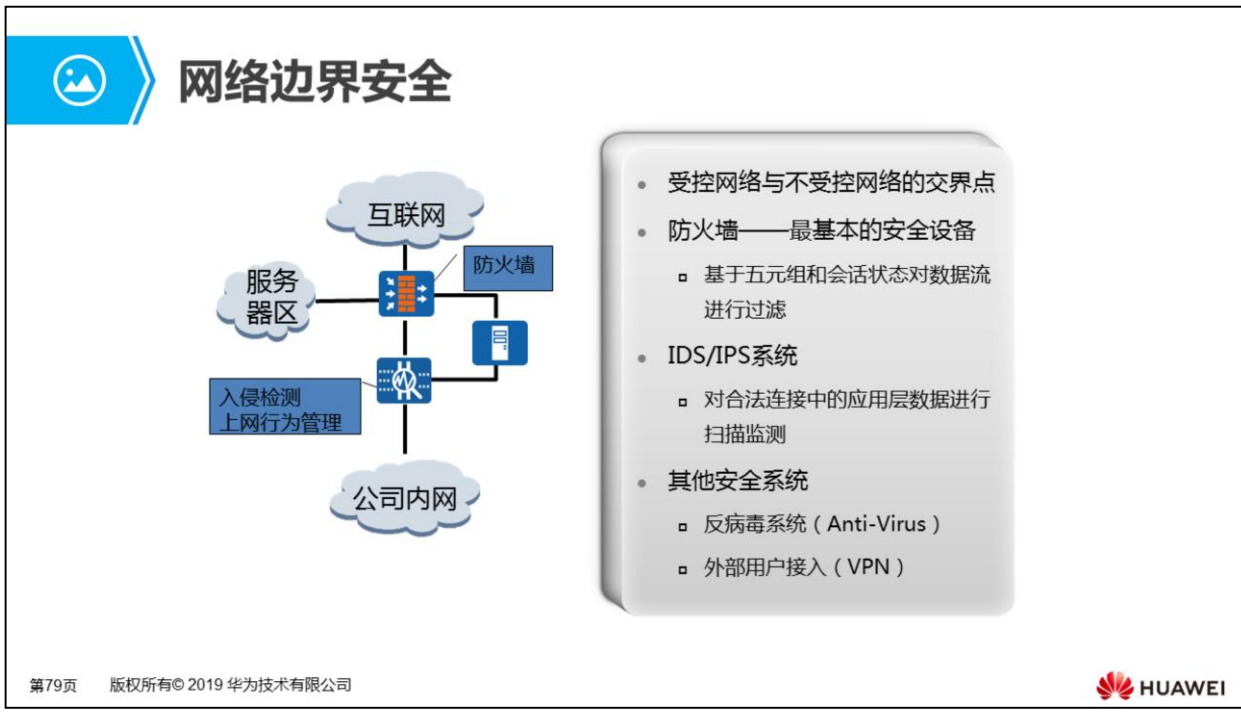
- 在TCP/IP协议栈中的绝大多数协议没有提供必要的安全机制，例如：不提供认证服务；明码传输，不提供数据保密性服务；不提供数据完整性保护；不提供抗抵赖服务；不保证可用性——服务质量（QoS）。
- 因为协议本身的各种缺陷以及具体实现的不完善之处，网络系统常常处于各种攻击之中。如图中所示，各个网络层次都存在相应的攻击。
- 网络安全是一个立体的防范系统，包括物理安全、安全管理等各个方面。安全技术是实现网络安全的一个方面，通过设备配置或安全设备达到防止网络攻击，维持网络服务的目的。



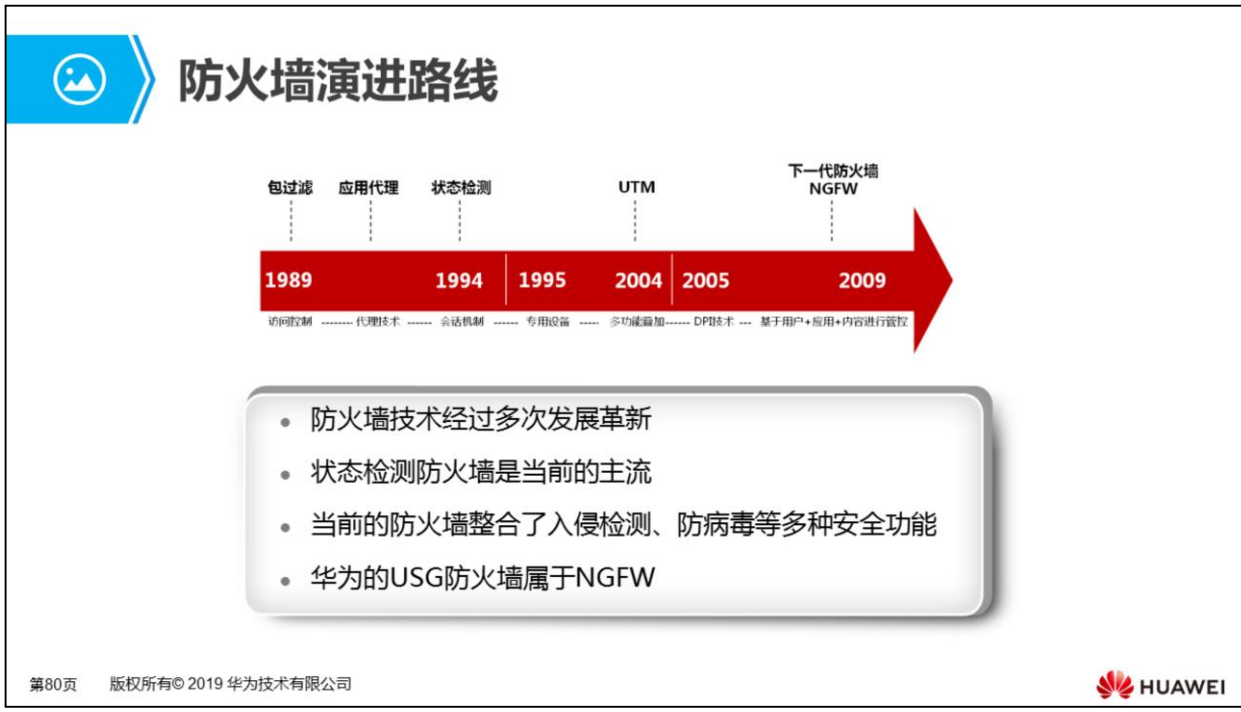
- 对一个企业网络来说，内部网络通常是可控的，企业外部网络是不可控的。所以最基本的安全措施是在内外网络边界上设置安全隔离和安全检查。
- 来自于内网安全威胁日趋增加，包括内部员工的违规和滥用导致信息泄露等，所以内网安全也是当前网络防护的重要方面。内网安全包括如下三个方面：
  - 内部网络安全：网络设备首先要保障自身的安全，保证自己不被攻击，持续正常工作；然后内部网络可以利用路由器和交换机自身的安全特性，对网络流量进行一定的安全操作。
  - 内网接入安全：对需要接入内网的设备进行认证，不允许未经授权的设备接入网络使用企业内网资源。
  - 终端设备安全：在终端设备上设置安全策略，部署安全软件等，防护终端设备。



- 网络中使用的基础网络设备，譬如路由器和交换机，本身就能够提供一定的安全特性。这些安全特性在工作网络中的实现不需要特别的硬件设备，只需要在当前设备上进行适当的配置即可。特别适合于需要一定安全特性，但预算较少，性能要求不高的场合。
- 路由器大量的运算是基于软件的，所以安装合适的软件之后，路由器能够提供很多的安全特性。譬如对ARP表项进行安全控制，可以限制ARP刷新的速度等；能够针对IP协议的源地址进行校验，防止伪造源地址攻击；访问控制列表是网络设备中的基本安全功能，能够根据数据包的五元组进行过滤，也能够利用来对路由协议进行特定的控制。部分防火墙还实现了更多的安全特性，譬如能够象防火墙一样工作，基于连接状态进行数据过滤；也能够提供IPSec接入等功能。
- 交换机工作在二层，针对二层的攻击，交换机也发展了很多安全特性，譬如端口安全技术防止MAC地址泛洪攻击；DHCP Snooping防止基于DHCP协议的攻击，也可以利用DHCP Snooping的结果防止ARP攻击，伪造源地址攻击等；风暴控制是网络流量异常时候的控制手段。
- 网络设备运行在网络中，自身也有可能遭受到恶意攻击。所以网络设备自身也需要提供一定的安全特性保障自己正常运行。譬如网络设备远程登陆的时候，需要进行身份认证，为了提高登陆的安全性，推荐使用SSH/HTTPS等加密协议进行登陆；网络设备中，控制面的防护尤其重要，当前的设备一般均提供对本机控制面的流量限速和过滤，防止本机受攻击而表现异常。另外网络设备运行包括路由协议在内的各种协议，为了防止有人利用正常的协议攻击网络，需要在协议中启用邻居认证，面向非合法网络设备的端口关闭协议。

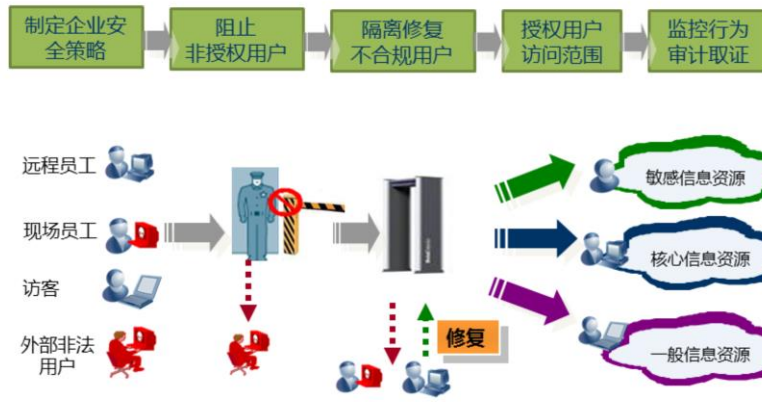


- 一个企业，一般都需要与外部网络相连，包括互联网，合作伙伴等。企业的内部网络一般具有完全的控制权，但是外部网络一般不受企业控制，所以对企业来说，外部网络是不安全的，需要进行一定的隔离。当前各个管理实体之间还涉及到地址管理等问题，需要进行地址转换（NAT）。
- 在网络边界上，最外层的一般都是防火墙，对外部网络进来的数据流量进行最基本的过滤，能够阻挡外部网络发起的大部分的攻击流量。防火墙划分不同的安全区域，各区域接入不同安全等级的设备。譬如将服务器置于单独的安全区域。
- 在当前的边界安全中。另一种常用的设备是IDS/IPS系统。防火墙可以基于数据流量的低层特性如协议和端口号等信息对攻击行为进行拦截，但对基于应用的深层攻击行为无能为力。IDS/IPS基于流量行为和攻击数据库对网络流量进行检测，能防御防火墙所不能防御的深层入侵威胁，提高网络边界的安全性。IDS系统一般旁挂于网络通路中，只对检测到的攻击流量进行报警和记录，而IPS系统则串行部署于网络中，直接阻断网络中的攻击流量。
- 网络出口还可以部署其他的专用安全设备，譬如反病毒墙，远程客户接入使用的专用VPN设备等。这些专用设备提供特定的功能，或在特定的方面提高安全性，但是在一般的网络部署中使用较少。



- 防火墙的出现可以追溯到上世纪80年代末期，在二十多年的发展过程中，防火墙大致可以划分为三个阶段。
  - 包过滤防火墙：工作原理类似于访问控制列表（ACL），针对数据流的五元组进行过滤。同时期还有另一个基于代理技术的防火墙，应用代理防火墙工作于应用层；安全性较高，但是处理速度慢，对每一种应用都需要独立进行开发，因此只有少量的大规模应用或者需要高安全性的特定应用才会使用代理防火墙。
  - 状态检测防火墙：划分安全区域并动态分析报文的状态来决定对报文采取的动作，首个数据包基于五元组并建立会话信息，后续数据包基于前面的会话信息进行转发，与包过滤防火墙相比，处理速度快而且提供更多的安全特性，同时不象应用代理防火墙需要为每个应用进行独立开发，所以迅速得到普及，其原理仍然是当前防火墙的基本功能。
  - UTM和NGFW：在防火墙之外，网络安全厂商发展了一些专用的安全设备，譬如入侵检测，反病毒墙等。于是有安全厂商提出了UTM（United Threat Management，统一威胁管理）的概念，将传统防火墙、入侵检测、防病毒、URL过滤、应用程序控制、邮件过滤等功能融合到一台防火墙上，实现全面的安全防护。NGFW（下一代防火墙）在UTM的基础上更进一步，解决了UTM在开启多个功能时性能下降的问题，同时，还可以基于用户、应用和内容来进行管控。
- 当前华为主推的USG6000系列防火墙属于NGFW。

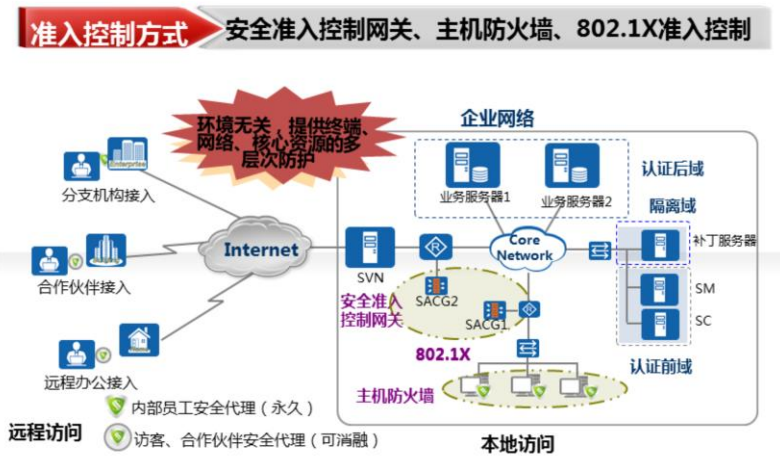
内网接入安全



HUAWEI

- 与普通的网络接入不同，在用户接入企业内部网络之前，首先需要接受身份验证，认证通过后进行第二步强制合规性检查（包括安全状态和系统配置检查），服务器依据检查结果作出仲裁，符合企业安全策略即可授权访问相应的网络资源；安全检查不合规的终端只能访问修复资源，完成必要的修复后才能接入网络。代理对所有接入网络的终端进行持续的行为监控，及时对违规行为作出响应，并进行记录。整个流程形成了内网安全保护的PDCA持续改进过程。

内网接入安全部件

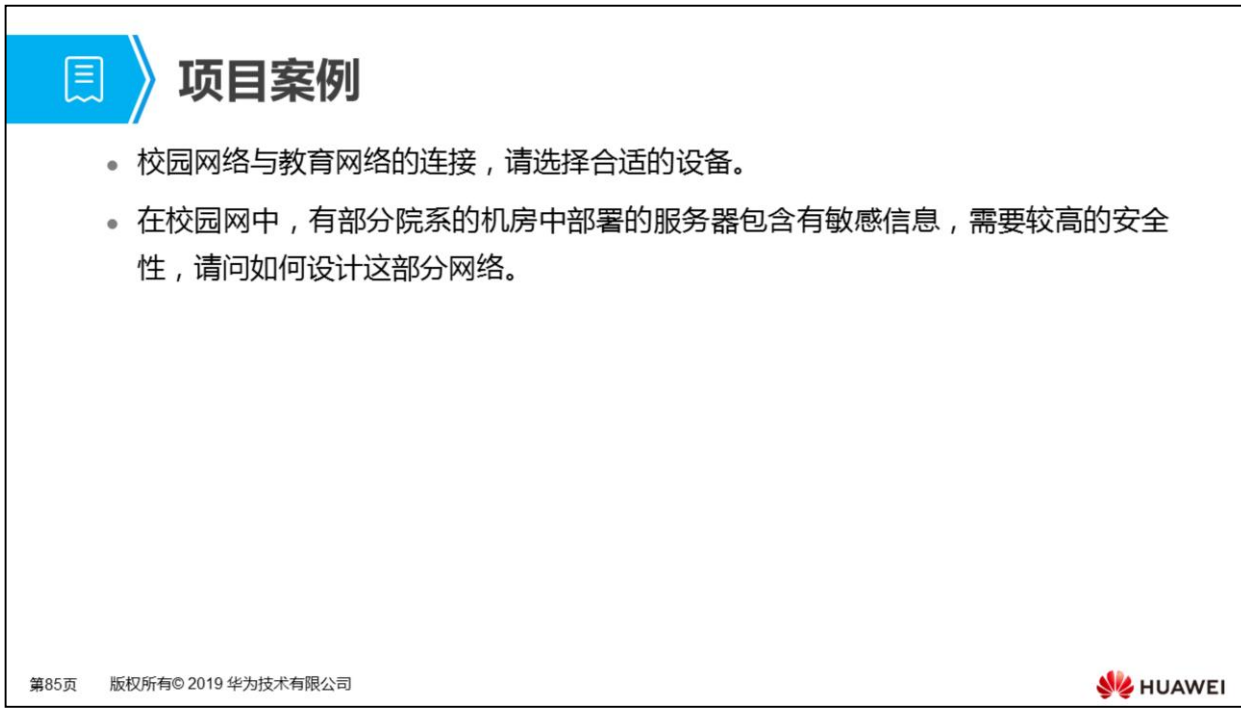


HUAWEI

- 内部网络接入安全是一个解决方案，不是一个单独的设备，完整实现该解决方案需要考虑五个要素：
- 身份认证：身份标识、角色定义、外部认证系统等；
- 准入控制：软件防火墙、802.1X交换机、网关准入控制、ARP、DHCP；
- 安全认证：防病毒软件、补丁管理、非法外联管理、存储介质管理、上网行为管理等；
- 业务授权：业务系统权限控制、业务文档权限控制；
- 业务审计：业务系统类审计、业务文档类审计。

- 华为USG6000系列防火墙采用下一代防火墙技术。单台设备集成了传统防火墙、VPN、入侵防御、防病毒、数据防泄漏、带宽管理、Anti-DDoS、URL过滤、反垃圾邮件等多种功能，可识别6000+应用，极供应用级别的访问控制精度，能够准确检测并防御网络中的漏洞和攻击，能对传输的文件和内容进行识别过滤，支持丰富高可靠性的VPN特性，如IPSec VPN、SSL VPN、L2TP VPN、MPLS VPN、GRE等。
- USG6000系列防火墙细分为三个系列，按照性能从低到高分为USG6300、USG6500、USG6600三个型号。其中USG6600支持多种安全业务的虚拟化，单一物理设备上可以虚拟出多个防火墙、入侵防御、反病毒、VPN设备。
- USG9000系列防火墙是华为公司推出的面向云服务提供商、大型数据中心和大型企业园区网络的新一代T级别防火墙，提供高达T级的处理性能和99.999%可靠性，集成NAT、VPN、IPS、虚拟化、业务感知等多种安全特性，帮助企业构建面向云计算时代的数据中心边界安全防护。支持CGN（Carrier Grade Nat），单一物理设备最多可虚拟4096台虚拟设备，集成包括应用层DDoS在内的多种DDoS攻击防范功能。

- 华为提供其他边界安全产品：
  - IDS/IPS：华为推出NIP6000作为下一代入侵防御系统，具有环境感知能力、深度应用感知能力、内容感知能力，以及对未知威胁的防御能力。能够有效防御蠕虫、木马、僵尸网络、跨站攻击、SQL注入等常见攻击，支持自定义签名，灵活快速应对突发威胁。支持识别主流P2P、IM、网络游戏、社交网络、视频、语音应用等6000+种应用协议。支持对HTTP、FTP、SMTP、POP3、IMAP、NFS和SMB协议进行病毒过滤和防护；能够从各个传输文件的协议（HTTP、SMB、FTP、SMTP、POP3、IMAP、NFS）中提取文件，并送入文件的检测引擎进行检测。支持对VLAN、QinQ、MPLS、GRE、IPv4 over IPv6、IPv6 over IPv4等隧道协议的报文解析及威胁检测与防护。
  - ASG2000是华为公司面向大中型企业和运营商推出的企业级专业上网行为管理产品。支持1200主流应用识别和8500万URL过滤，具备应用识别丰富，威胁防护全面，报表专业全面的特点，并集应用控制、带宽管理、URL过滤、恶意软件防护、数据防泄漏、行为审计等多种安全功能于一体。
  - USG2000BSR华为公司面向小型企业推出的企业级多业务安全网关，集安全、路由、交换、无线（WiFi/3G）等特性于一体，接口丰富，提供高密度交换接入，帮助企业实现全无线组网，同时为用户提供强大、可扩展、持续的安全能力，是SOHO企业、小型办公室互联网接入的最佳之选。
  - USG6000V是面向数据中心的一款基于NFV架构云化多业务综合业务网关产品。运行于虚拟机平台，提供与硬件防火墙相似的功能，并提供基于虚拟机的高速转发，支持1+1/N+1冗余。



- 当前校园网络与教育网络是一个互连出口，校园网络的普通用户并不需要特殊的安全特性，但是与外网相连，需要做地址转换等工作，所以在出口部分部署一个防火墙是必要的。具体型号，根据服务的用户数和并发会话数量估算，校园网需要服务大量的用户和海量的并发会话，建议使用高端的USG6600防火墙。因为用户量大，影响面大，所以建议使用双机冗余的方案。
- 大型网络中部分网络提高安全性，可以采用防火墙进行隔离，如果需要进一步提高安全性，也可以附加配置IPS设备，对于华为的USG防火墙来说，只需要开启相应的功能即可。

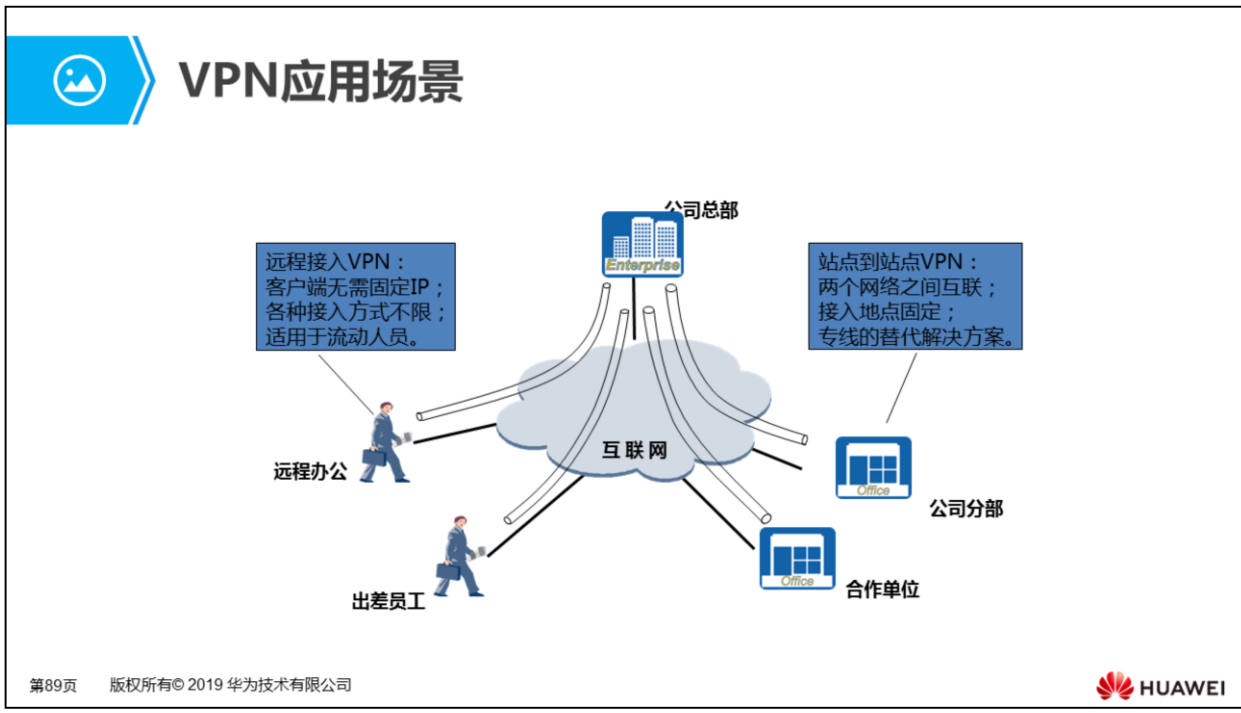
目录

VPN简介

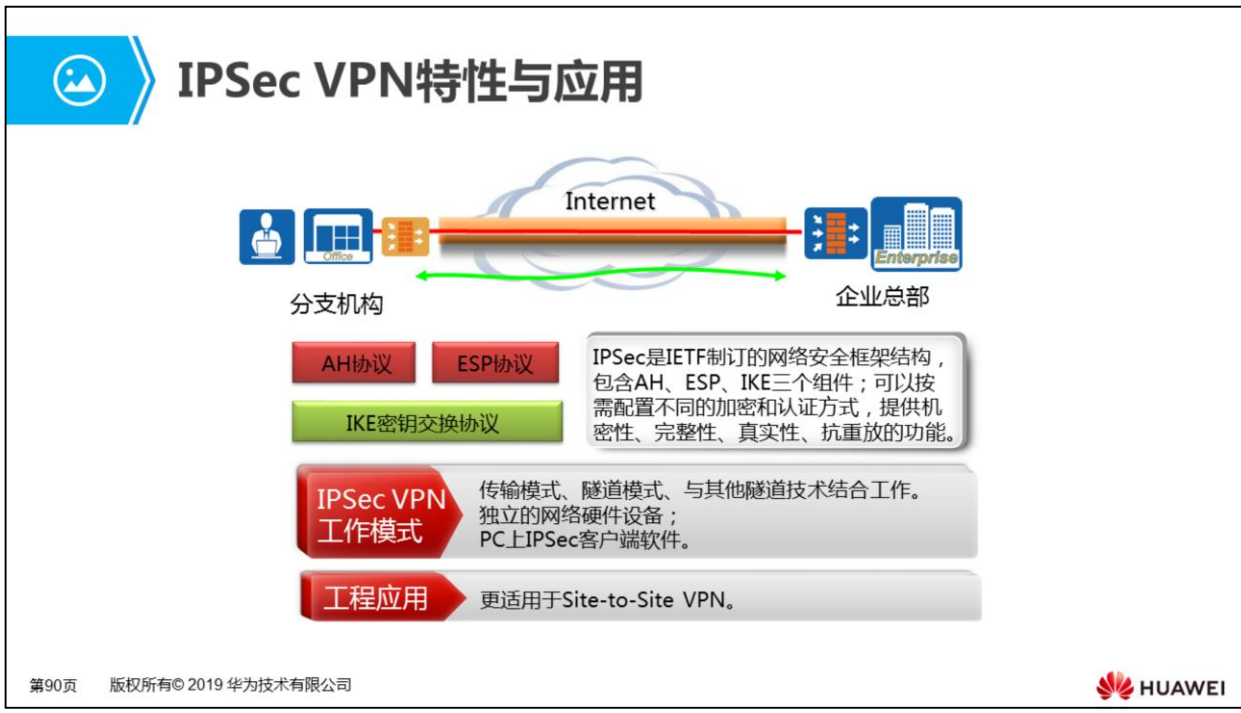
HUAWEI

- 虚拟专用网（VPN）是指通过共享的公共网络建立私有的数据通道，将各个需要接入虚拟网的网络或终端通过通道连接起来，构成一个专用的、具有一定安全性的网络。当前企业使用的VPN一般是基于互联网的。
- VPN主要通过隧道技术来实现，因为VPN中的企业数据要穿越公网，为了保证安全性，VPN还采用了大量安全技术，主要包括加解密技术、数据认证技术和身份认证技术等。
  - 隧道技术是VPN技术中最关键的技术。隧道技术是指在隧道的两端通过封装以及解封装技术在公网上建立一条数据通道，使用这条通道对数据报文进行传输。隧道是由隧道协议形成的，分为第二、三层隧道协议。L2TP是典型的二层隧道协议；GRE是典型的三层隧道协议。
  - 加解密技术是数据转变成不可识别的加密数据然后进行传输，到达目的地后再进行解密恢复，VPN技术可以借助加解密技术保证数据在网络中传输时不被非法获取。
  - 数据认证技术主要保证数据在网络传输过程中不被非法篡改。数据认证技术主要采用哈希算法，由于哈希算法的不可逆特性以及理论上的结果唯一性，因此在摘要相同的情况下可以保证数据没被篡改过。
  - 身份认证技术主要保证接入VPN的操作人员的合法性以及有效性，主要采用“用户名密码”方式进行认证，对安全性较高的还可以使用CA证书等认证方式。

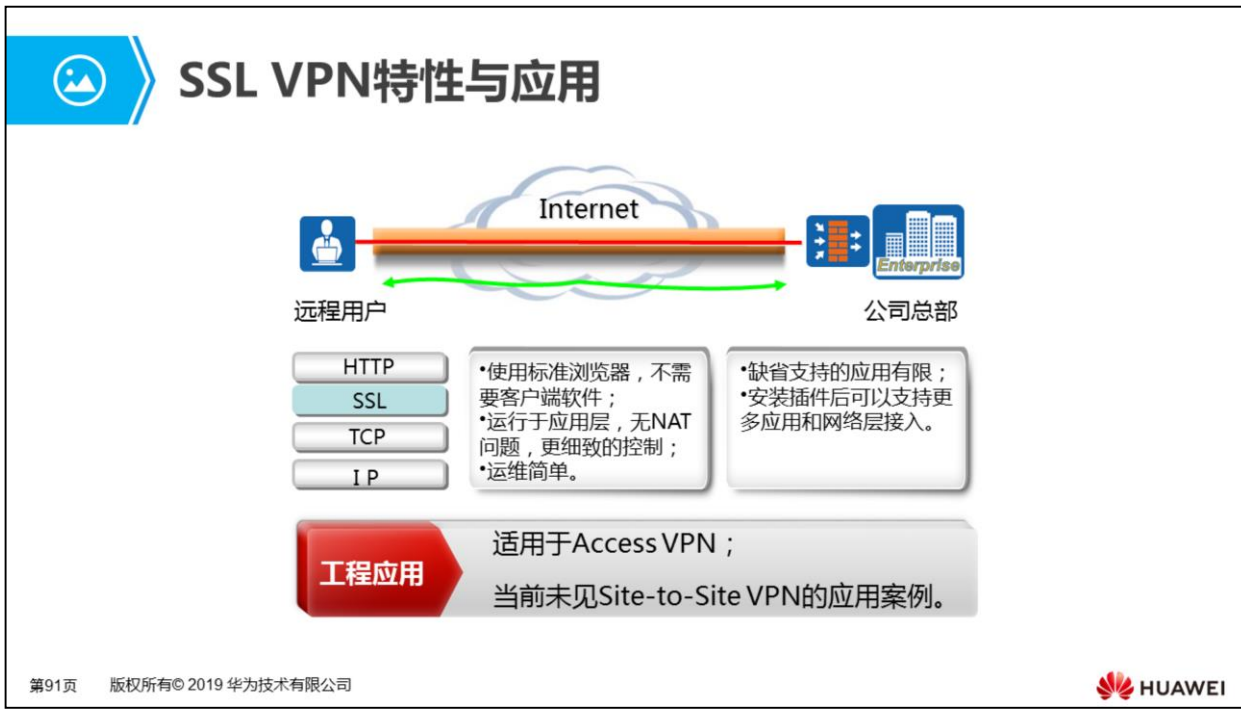
- VPN具有很多的优点，当前不管是在企业内还是企业间应用都很广。
  - VPN最大的优势是成本低廉，有了VPN，企业就不用再租赁价格昂贵的广域线路，可以直接通过无所不在的互联网架构跨越广大地理位置的区域；同时企业各个节点之间的连通性由互联网保证，企业减少了运维投入。
  - 有了VPN技术，大大增加了网络设计的灵活性。不管是企业内部还是企业外部，均可以使用VPN技术进行连接，连接条件只需要IP可达即可，不必再相互协商底层链路参数；因为不需要物理链路，所以VPN扩展网络的时候，成本很低。
  - 为了保证数据在互联网上传输的安全性，VPN采用身份认证技术来确认对端设备的身份；采用加解密技术来保证数据在互联网上传输时的保密性；用数据认证技术保证数据在互联网上传送时不被修改。
  - VPN也不全是优点，因为VPN架构于互联网上，所以中间这一段的网络可控性不好，最常见的是带宽、延迟等QoS质量难以保证。



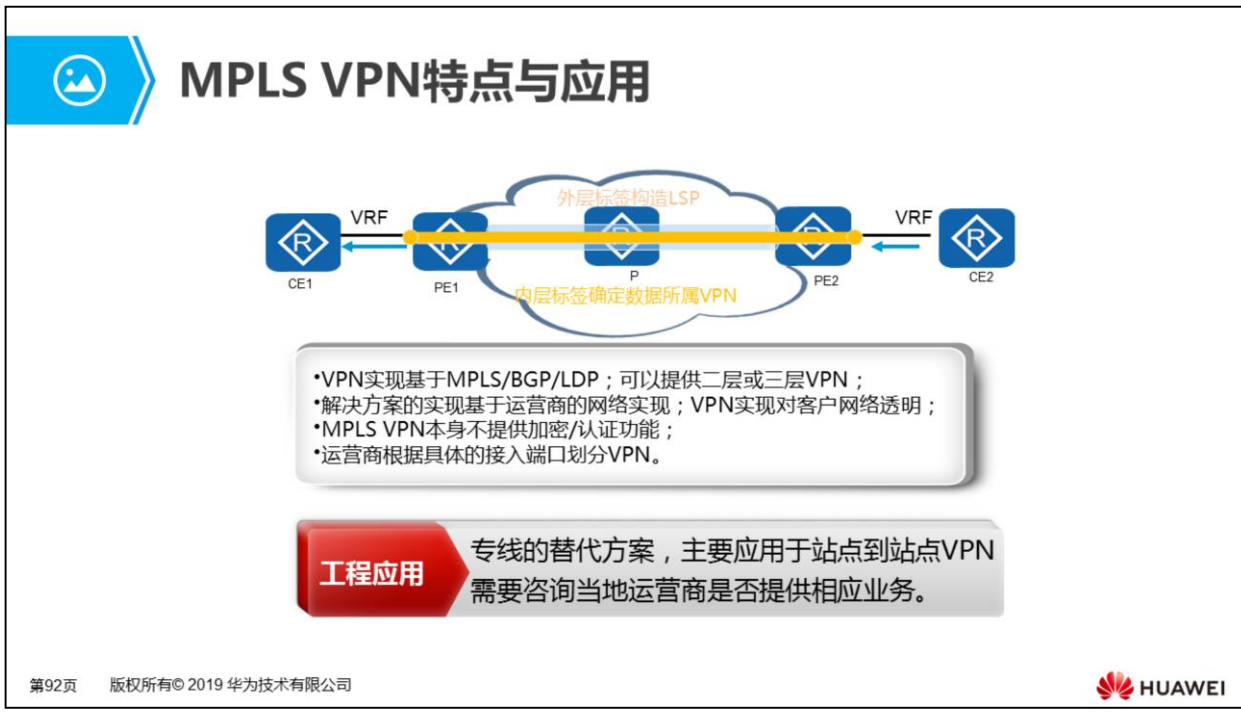
- VPN可以按照多种方式来进行分类，如按照工作层次来划分，可以划分为二层VPN、三层VPN等；按照实现技术来划分，可以划分为IPSec VPN、SSL VPN、MPLS VPN等；按照应用场景或者连接需求来说，可以分为两类：一类为远程接入VPN（Access VPN），另一类为站点到站点VPN（Site-to-Site VPN）。
- Access VPN是常见的VPN应用场景。如果企业的内部人员有移动或有远程办公需要，或者是商家要提供B2C的安全访问服务，就可以考虑使用Access VPN。Access VPN中的接入用户不需要固定的IP，可以通过模拟线路拨号、ISDN、数字用户线路（xDSL）、移动IP和电缆等各种技术远程接入，使用户可以随时、随地以其所需的方式访问企业资源；适用于公司内部经常有流动人员远程办公的情况。Access VPN的接入端设备一般是PC机或其他终端设备，公司接入服务器一般采用专门的网络设备，可以是路由器、防火墙、或者专门的VPN接入设备。Access VPN的接入服务器一般采用固定的IP地址，接入客户端的IP地址一般不固定。
- Site-to-Site VPN是另一种常见的VPN应用场景。这种类型的VPN用来连接两个网络，这两个网络可以是一个公司的总部和分部，也可以是两个公司之间互联。两个固定网络互联的传统解决方式是租用运营商的专线，这种类型的VPN是专线的替代方案。Site-to-Site VPN的两端一般都采用专门的网络设备，两端的设备至少一端采用固定IP地址。
- 对于这两种VPN应用场景，有各种技术实现与他们相对应，其中很多技术是可以同时适用于两种应用场景的，但相对来说，每种技术均有它自身的特点，对各种场景的适用情况会有一定的差异。



- IPSec VPN是应用最广的VPN技术之一。它是IETF制定的一种开放标准的框架结构，包含一系列IP安全协议，提供的功能包括数据加密、数据完整性检查、数据真实性验证和防止重放攻击等。
- IPSec VPN有多种工作模式，常见的包括传输模式和隧道模式，可以适用于多种应用场景，另外，IPSec技术还能够与其他隧道集成以完成相应的功能。
- IPSec VPN在部署的时候，可以应用于Site-to-Site VPN和Access VPN。应用于站点到站点VPN的时候，一般在特定的网络设备之间启用IPSec VPN，两侧的网络通过隧道连通。这种方式需要网络设备支持IPSec，一般当前的路由器、防火墙均可以支持IPSec，因为涉及数据加密，部分产品需要购买许可（licence）。
- 当前流行的桌面操作系统自身一般不附带IPSec客户端，所以，如果要将IPSec VPN应用于Access VPN的时候，需要在客户端上安装独立的IPSec客户端软件。对于大量用户接入的企业来说，增大了维护工作量。所以IPSec VPN更多地用于站点到站点VPN。



- SSL是一个安全协议，为基于TCP（Transmission Control Protocol）的应用层协议提供安全连接，SSL介于TCP/IP协议栈的传输层和应用层之间。为HTTP（Hypertext Transfer Protocol）协议提供安全连接。因为工作于高层，所以SSL VPN不受NAT限制，能够穿越防火墙，使用户在任何地方都能够通过SSL VPN虚拟网关访问内网资源。
- SSL VPN接入用户使用标准的浏览器，如IE、Netscape、chrome等，就可以访问企业的内部应用。所以移动办公人员只需要一台基本配置的电脑，并不需要安装特定的VPN客户端就能实现安全的远程访问。安全、简单、易用，极大地减少了网络运维工作量，提高了企业办公效率。
- SSL VPN当前仅用于远程接入VPN（Access VPN），当前未见SSL用于站点到站点VPN。



- MPLS VPN基于MPLS标签交换实现VPN功能。可以提供二层和三层VPN。实现三层VPN的时候，MPLS与BGP结合，通过BGP协议在运营商骨干网上发布VPN路由，使用MPLS在运营商骨干网上转发VPN报文。当实现二层VPN的时候，可以通过LDP或BGP在运营商的边缘设备之间传递二层控制信息，建立LSP路径，然后通过MPLS在运营商骨干网上转发VPN报文。
- 整个MPLS的实现都是在运营商网络中，对于客户网络来说，整个实现机制是透明的，客户不了解数据在运营商网络内的传递过程。从客户的感知上，MPLS VPN，特别是二层VPN类似于运营商专线。
- 与IPSec VPN和SSL VPN不同，MPLS VPN本身不提供加密和认证功能，仅仅是利用MPLS标签提供的LSP隧道在运营商网络中传递数据，实现数据层面的隔离。如果要实现数据加密，需要客户自行实现。
- MPLS VPN更多的是作为运营商的一种服务，而不是作为企业自身的远程连接解决方案而存在。如果企业需要远程链路的时候，可以联系运营商，把MPLS VPN链路作为一个可选项。

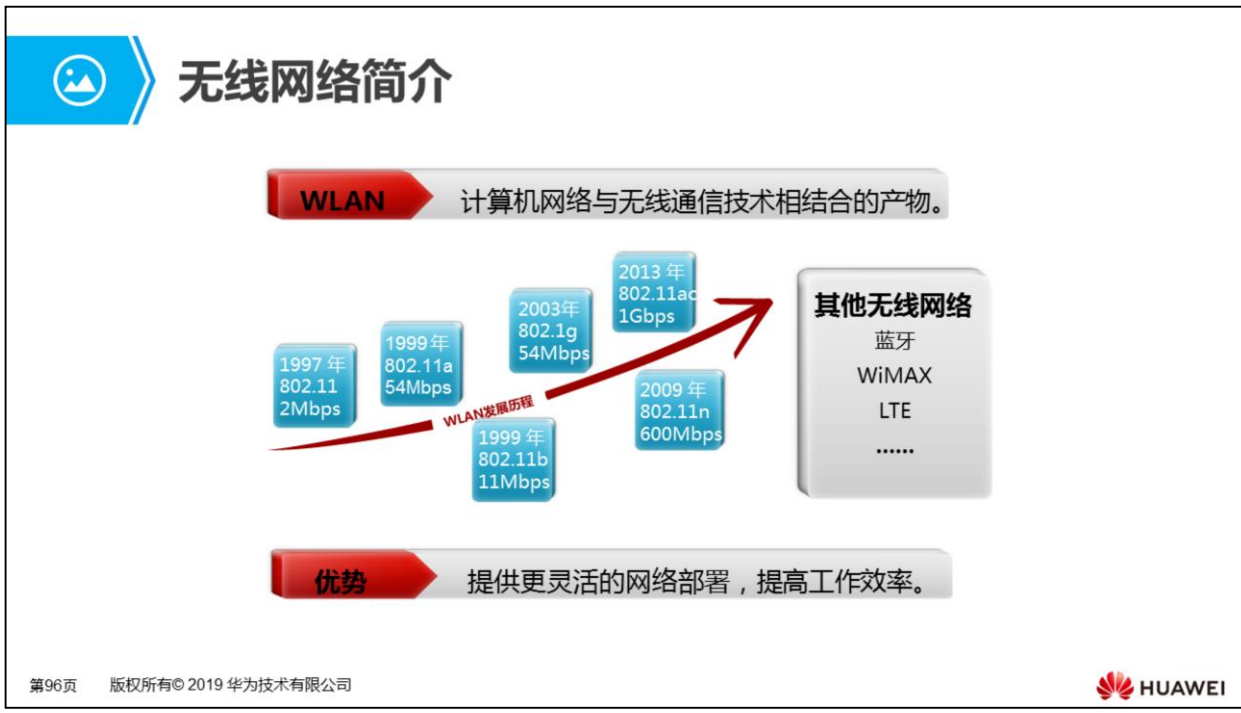
- VPN在很多情况下并没有专用的设备，因为VPN的加解密一般都是软件实现的，所以很多VPN技术在通用硬件平台上就能实现，当然在配置设备的时候，需要注意licence的问题，很多网络设备提供的VPN功能都是需要单独购买licence的。VPN中的加解密功能需要大量的处理能力，为了支持更大规模的VPN接入，还需要注意硬件平台的性能问题，部分高端设备为了提高连接数量和加解密能力，对硬件做了优化。
- 华为提供专用的VPN平台：SVN5600/5800系列。最高支持10万并发用户接入，最大可支持512个虚拟网关；支持Android、Windows、iOS、MacOS、Linux、Symbian、Blackberry等主流操作系统平台；支持SSL VPN、IPSec VPN、GRE VPN、L2TP VPN、MPLS VPN，一体化VPN解决方案；支持10种认证方式，支持多级认证、混合认证，用户可自由选择使用，身份认证更加安全；支持Web代理、网络扩展、文件共享、端口转发、多媒体隧道应用集成；全方位立体防护，覆盖终端、数据管道以及服务器安全，远程接入安全无忧；智能多出口选路，分布式部署网关动态优选，接入带宽管理，敏捷接入体验 。

项目案例

- 该校分校位于其他城市，与学校本部之间需要进行业务数据交流，请问采用何种方案解决经济性较好？
- 院校的部分老师希望在家或在出差途中仍然能够登录校园网络进行一些工作处理，请问采用何种方案进行解决？

- 各分校间连通，可以采用传统的广域网技术，如租用专线的方式来解决。但是租用专线，特别是长途专线的费用是比较昂贵的，比较经济的做法是采用VPN的方式利用互联网进行连接。因为是两个园区之间的互连，建议使用IPSec VPN。在园区网络出口部署网络硬件设备，譬如可以选用华为的USG系列防火墙，按照流量确定性能要求。
- 对于移动用户的远程接入，我们也可以采用VPN的方式进行。对于众多的移动用户，可以采用SSL VPN，免去维护移动客户端的工作量。

目录



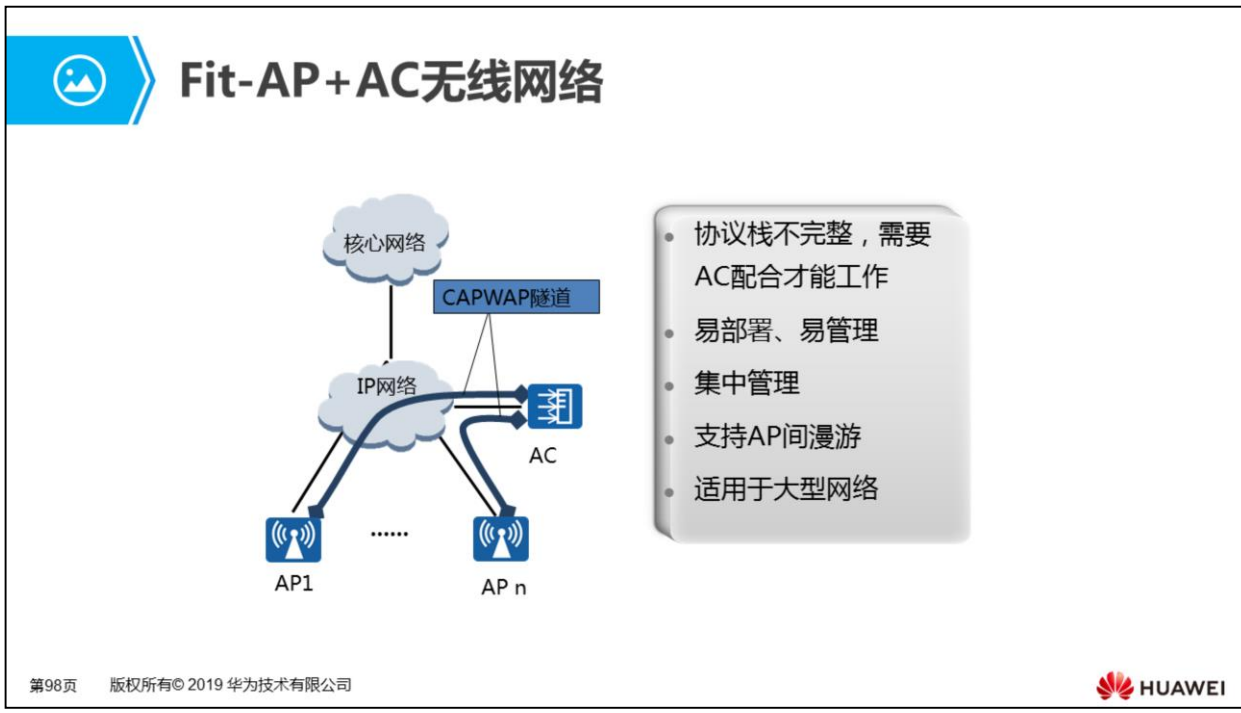
- WLAN技术最早出现在美国，主要应用于家庭。因为WLAN不需要铺设线路，所以WLAN技术的普及速度很快。近几年，WLAN在各地的家庭、办公、学校与企业等场景得到了广泛的应用。
- WLAN技术经过十多年的推进和发展，其标准和产品已经日渐成熟。IEEE的802.11工作组为WLAN制订了一系列的标准，从最初2Mbps的802.11标准一直到现在高达1Gbps数据速率的802.11ac标准。
- 与有线接入技术相比，WLAN拥有以下优势：
  - 移动性：WLAN可以使得使用者不受制于网线接入位置，可以在一定范围内四处移动而不中断网络连接，大幅提高生产率。
  - 灵活性：传统有线网络在某些场所布线有难度。而WLAN在这些场合则可以灵活布放；另外WLAN还可以迅速构建小型、临时性的群组网络。
  - 经济性：采用WLAN技术可以节约成本。最主要是网线的成本，WLAN不需要采购大量的网线，也节约了布线工程的成本。另外在特定的场合，比如相聚不远的两栋建筑间互通，可以用无线网桥替代传统的运营商专线，可以节约大量的网络运营成本。
- WLAN技术中单个AP（接入点）的覆盖范围大概为100米半径，很好地适合了大多数企业网络应用场合；除了WLAN之外，无线网络还有如下一些常见技术：
  - 蓝牙技术，工作在2.4GHZ频段。供个人区域无线连接使用，距离一般在10米以内。
  - WiMax（802.16）：一种无线城域网技术，接入范围可达10公里，速率可达几十兆bps。
  - 移动数据网：包括GPRS/EVDO/HSDPA/LTE等广泛使用的移动接入技术。

Fat-AP无线网络

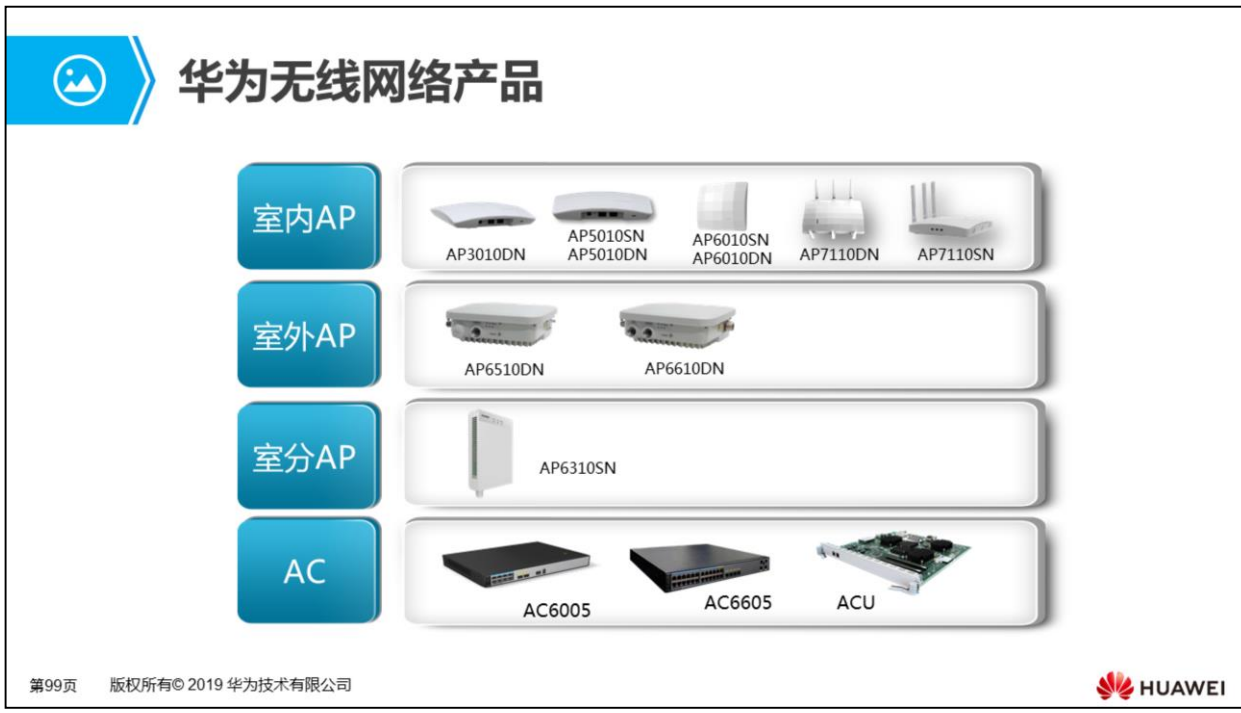
- 协议栈完整，能独立运行
- 功能完整丰富
  - DHCP
  - FW-NAT
- 每个AP独立管理
- 不支持AP间漫游
- 适用于小型网络

HUAWEI

- Fat-AP本身具有完整的协议栈实现，能够不依赖其他网络设备独立运行。另外Fat-AP在实现无线接入的同时，还能同时提供DHCP、NAT等功能，完成为客户端分配地址等工作。
- 如果一个网络中存在多个Fat-AP，这些胖AP之间相互是独立的。在管理的时候需要各自独立管理，每一台设备需要单独配置。当然可以采用网管的方式进行批量处理。
- Fat-AP不支持AP之间的漫游，如果用户从一个AP的接入范围移动到另一个AP的接入范围，需要重新进行连接。
- Fat-AP常常用在家庭或者SOHO等所需要的无线覆盖范围小的场合。



- Fit-AP是不能单独配置或者使用的无线AP产品，它仅仅是一个WLAN系统的一部分，要实现完整的无线接入功能必须要有AC配合一起工作。
- AC和Fit-AP之间运行的协议一般为CAPWAP协议。AC管理AP的控制报文必须采用CAPWAP隧道进行转发；而数据报文有两种转发方式：通过CAPWAP隧道转发或者直接转发。AC在部署的时候，可以串行部署在网络中，也可以旁挂于网络之中。
- 一个AC下的Fit-AP全部由AC管理，极大地减少了管理负担。Fit-AP支持零配置安装，新增AP只需物理安装，就可以自动发现AC并由AC进行管理和配置。
- 同一个AC下的AP之间支持漫游，也就是说无线用户在AP之间移动时，不需要重新接入。
- 与Fat-AP（独立AP）相比，Fit-AP实现了WLAN网络的快速部署、网络设备的集中管理和精细化的用户管理，从可运维的角度看，更适合于大型企业的无线组网。

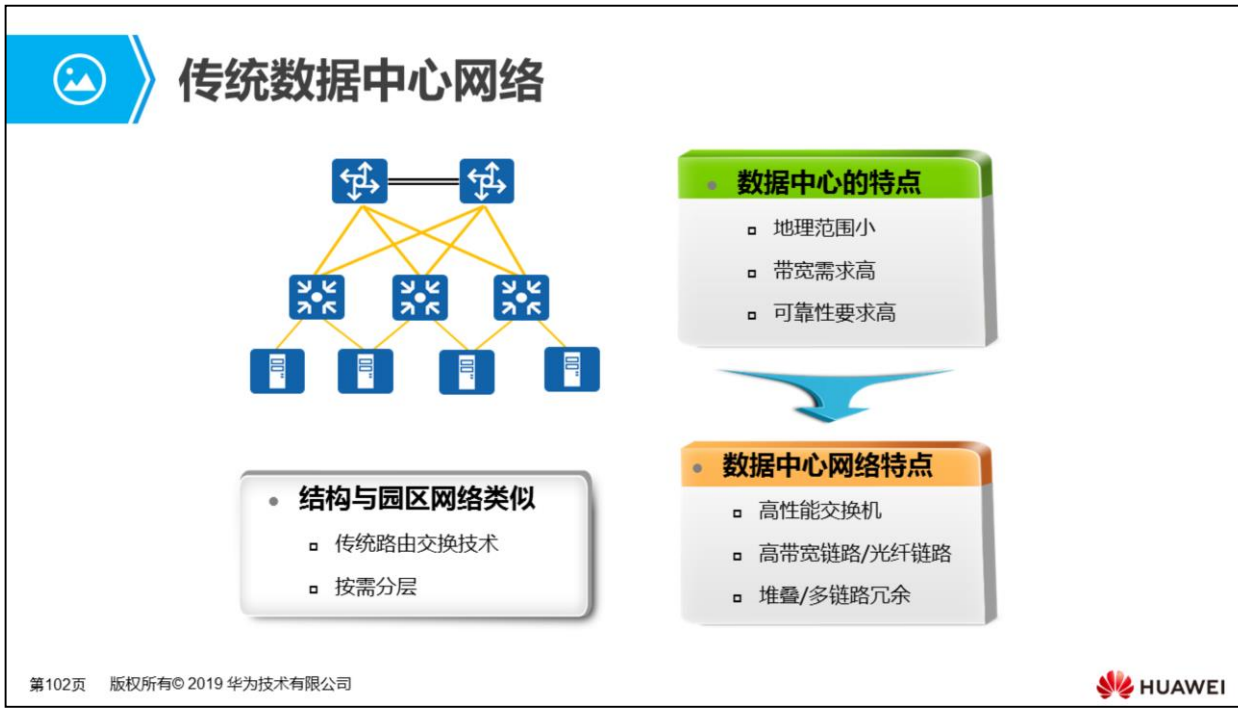


- 室内AP：室内放装型AP设备。对于建筑结构较简单、面积相对较小、用户相对集中的场合及对容量需求较大的区域，如小型会议室、酒吧、休闲中心等场景宜选用室内放装型AP设备，该类型设备可根据不同环境灵活实施分布，也可同时工作在AP和桥接等混合模式下。
- 室外AP：室外分布型AP设备。对于接入点多，用户量大，且用户分布较为集中的场合下，如学校、大型会展中心等大型场所，宜选用室外AP设备组网。
- 室分AP：室内分布型AP设备。对于建筑面积较大、用户分布较广且已建有多系统合用的室内分布系统的场合，如大型办公楼、商住楼、酒店、宾馆、机场、车站等场景宜选用室内分布型AP设备，该类型设备接入室内分布系统作为WLAN系统的信号源，以实现对室内WLAN信号的覆盖。
- AC6005系列无线接入控制器AC（Access Controller），提供大容量、高性能、高可靠性、易安装、易维护的无线数据控制业务。可管理4～128个AP，具有4Gbps的无线处理能力。
- AC6605无线接入控制器，提供大容量、高性能、高可靠性、易安装、易维护的无线数据控制业务，可管理4～512个AP的数量；具有最大128Gbps的交换容量；最多支持10K无线用户接入。
- 用于WLAN的SPU（Service Process Unit）又称为ACU。提供WLAN无线接入控制器功能，可插在S9300中，SPU默认支持管理128个AP，通过购买License，可支持最多管理1024个AP；最多支持32K无线用户接入。

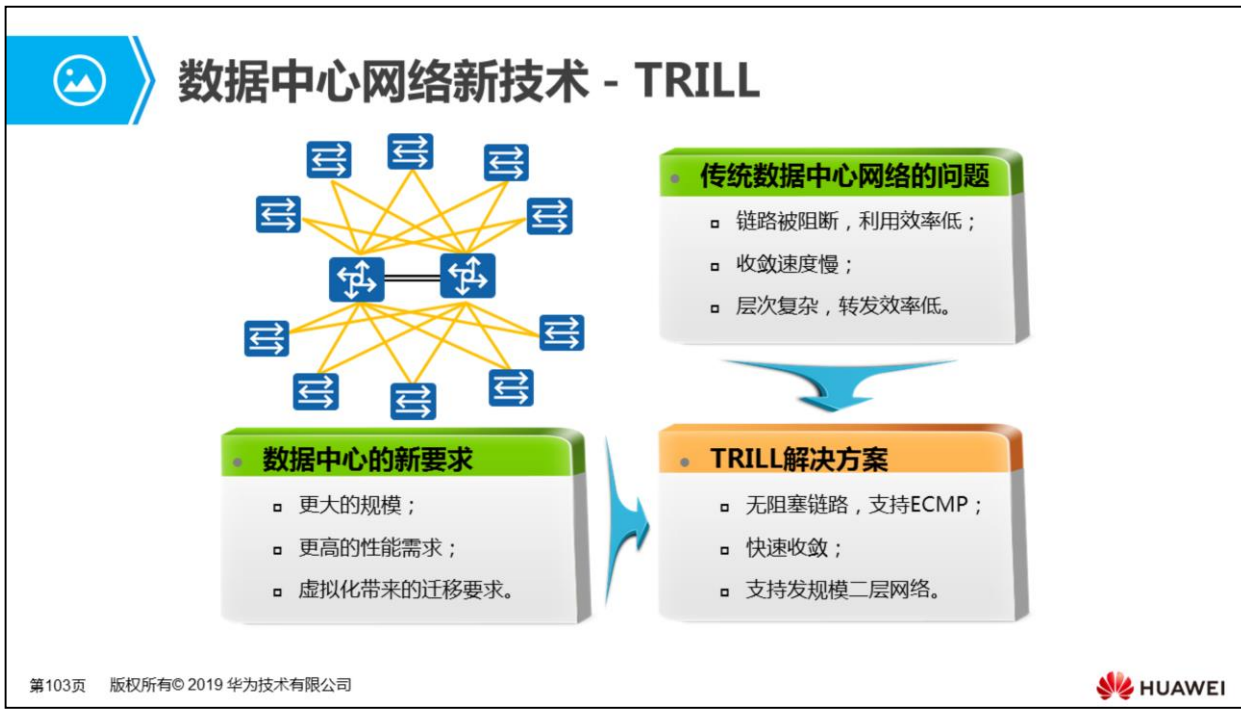
目录

HUAWEI

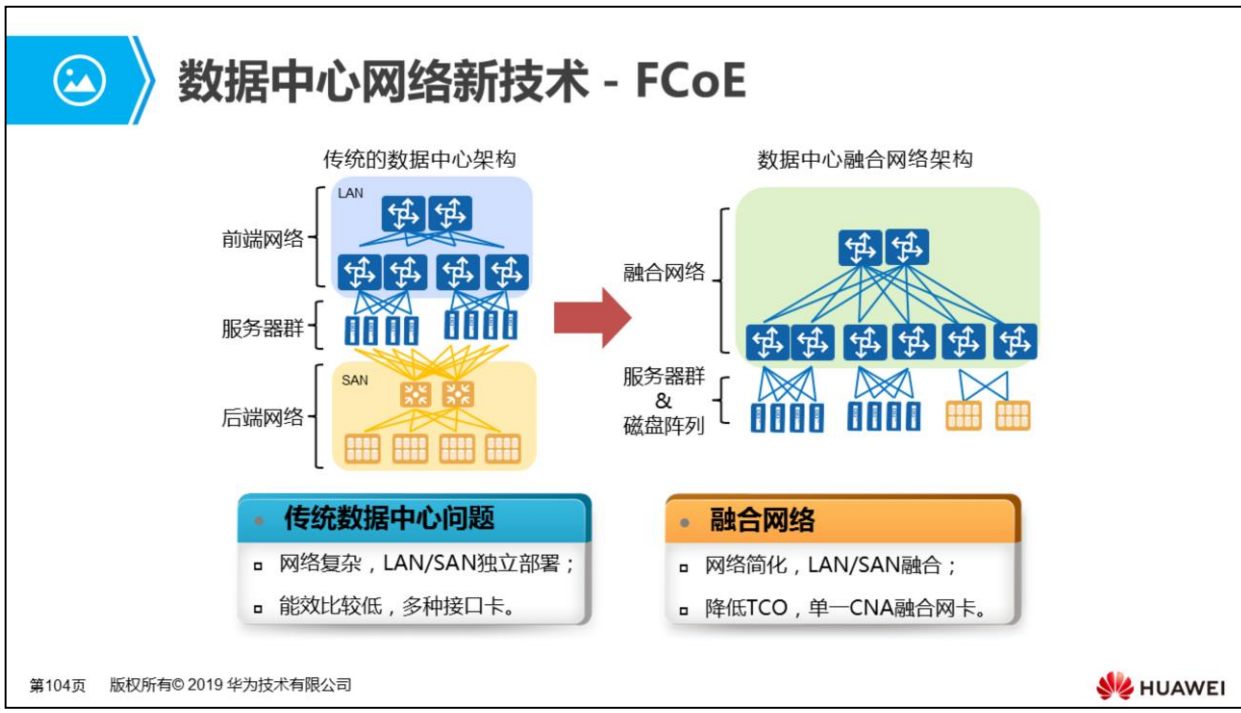
- 企业内部的服务器一般会集中安装于一个特定的场地，通常称为机房，达到一定规模的也常称为数据中心。
- 数据中心是一个综合性的IT基础设施，包含众多子系统，譬如供电、制冷、布线等，都是数据中心不可或缺的设施。在我们这里关注的网络系统，是数据中心各大系统中的一个组成部分。



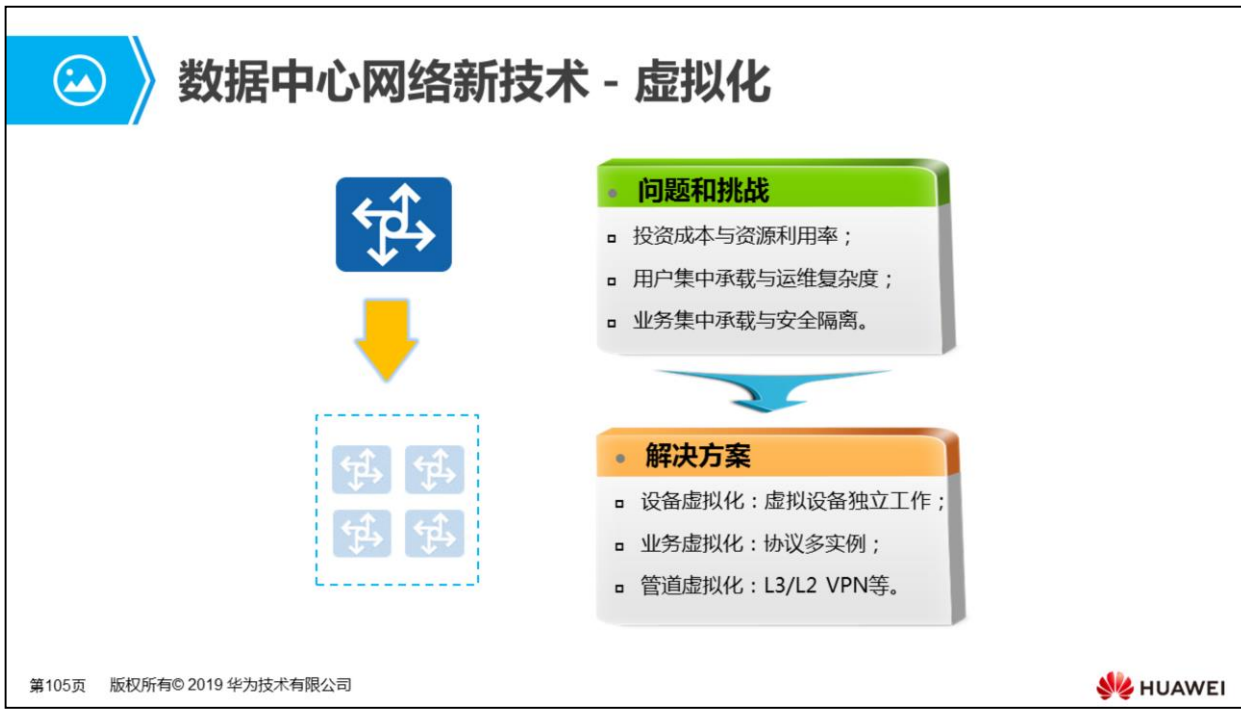
- 传统的数据中心直接采用与园区网络类似的路由交换架构,并没有引入特殊的新技术。同样按照网络的规模对网络进行分层。
- 数据中心也有它自身的特点，譬如，数据中心的地理范围很小，相比园区网更小，对一个企业来说常常就是一个或几个机房；所以数据中心的设备以交换机为主，一般在出口处会部署一定的路由和安全设备。
- 数据中心中的设备一般都是为企业提供各种服务的服务器，网络中的数据流量相对更大，而且，服务器一般不允许中断服务，所以数据中心对网络性能和可靠性的要求较高，在设计时，一般会采用高性能高端口密度的设备，采用高带宽的光纤链路；同时，采用多链路冗余、设备堆叠、集群等技术提高网络的可靠性。



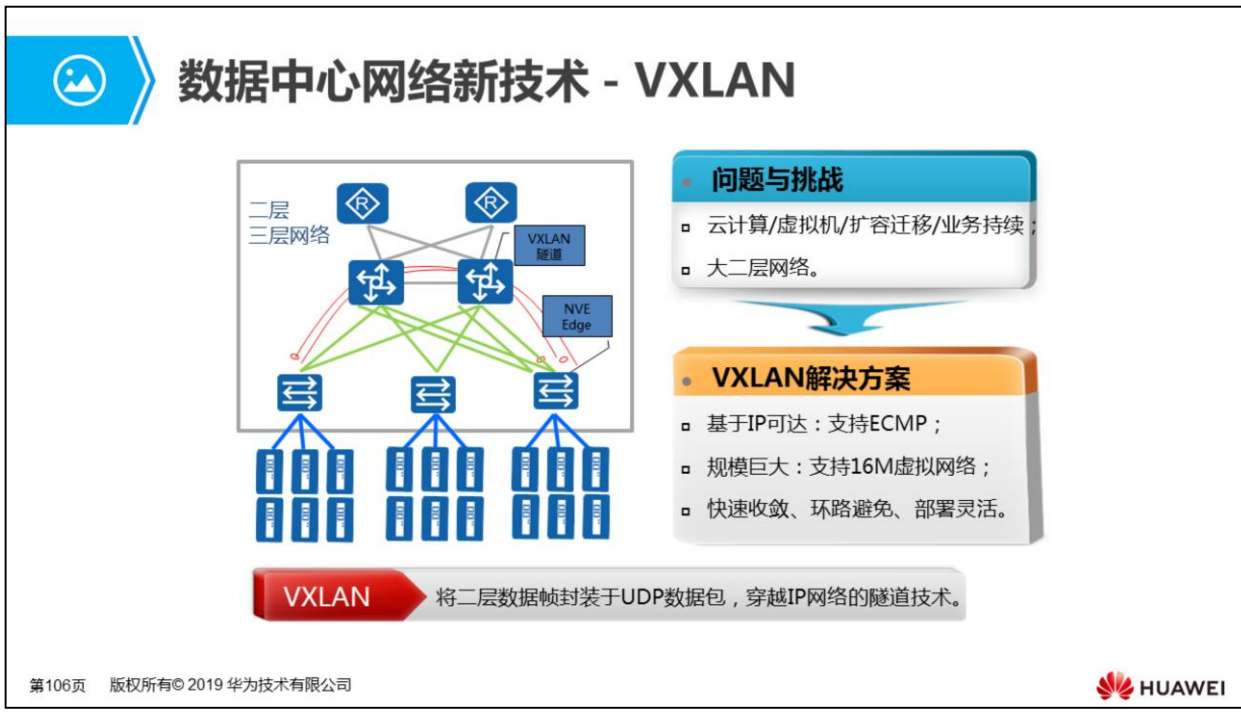
- 对于中小型企业来说，传统的数据中心架构是足够的。但是传统的路由交换网络架构存在一定的问题，譬如：在二层网络中，传统交换网络通过STP阻断链路来避免环路，STP的收敛速度较慢，对于关键应用服务来说，几十秒的收敛速度是难以接受的；同时STP是通过阻断链路来保证网络无环的，阻断的链路不承载流量，导致了一定的浪费。而数据中心，作为企业中的关键业务，一般在设计中都引入了较多的冗余，导致收敛和浪费问题更加严重。另外，传统的网络扩展采用层次化的扩展，二三层结合的方式，每多一个层次都会导致网络的复杂度上升，而三层转发的性能和代价更是远远无法跟二层转发相比。
- 另一方面，数据中心的计算模型发生了巨大的变化，特别是云计算等新技术得到了广泛的应用，使得数据中心规模和流量模型都发生了巨大的变化。譬如，数据中心中服务器的数量急剧增多，数据中心内部的数据交换也快速增长；另外，由于虚拟化技术的应用，数据中心内部的虚拟机迁移要求二层网络尽量扩展。
- TRILL(Transparent Interconnection of Lots of Link)多链接透明互联，IETF推荐的链路层（L2）网络标准。致力于在大型以太网络中解决多路径问题，很好地适应了当前数据中心具有的以下特点：
    - 单播流量转发为最短路径。TRILL基于SPF算法，计算到达各个目的节点的出接口；
    - 支持ECMP，带宽利用率高。目前我司产品最大支持16条等价路由；
    - 收敛时间快。TRILL网络中节点的故障路由收敛时间达到毫秒级；
    - 支持更大规模的网络。目前我司支持的TRILL节点的指标为500个；
    - TRILL头部有TTL，可以进一步避免环路风暴。



- 从传统数据中心的网络结构看，至少存在相对独立的两张网：数据网（Data）和存储网（SAN）：
  - 数据中心的前端访问接口通常采用以太网进行互联，构成了一张高速运转的数据网络；
  - 数据中心的后端存储更多的是采用NAS、FC SAN等；
  - 服务器则至少需要配置4 - 6张接口卡，两张HBA卡用来连接FC SAN，两张以太网卡用于连接数据网。
- FCoE(Fiber Channel over Ethernet)技术实现了存储网络与数据网络的融合，只需要一张网，同时提供数据通信和存储转发功能：
  - FC存储只需要FC交换机提供接入功能，转发过程运行在以太网（LAN）上；
  - 服务器只需要一种提供融合功能的CNA网卡。
- FCoE对数据网络的要求：
  - 大带宽：服务器与存储之间访问数据量很大，需要大的带宽支持，目前的以太网单接口带宽有10GE、40GE、未来有100GE，另外还有链路聚合，负载均衡等技术，能够满足存储的访问带宽需求；
  - 低时延：以太网现有的Cutthrough的转发机制能够保证数据的低延迟转发；
  - 无丢包：传统的以太网技术无法保证，即使使用了QoS技术也无法保证完全不丢包，要构建一个完全不丢包的FCoE网络，业界发展了DCB（Data Center Bridge）技术。
- 华为的数据中心系列交换机支持FCoE技术。

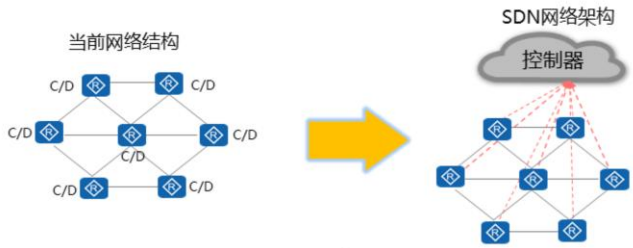


- “虚拟化”是云计算的关键技术，通过物理资源的抽象，达到资源的共享并隔离的好处。与此同时极大地提高了资源利用率，大幅降低资源运行和管理维护成本。云时代的虚拟化包括多个方面，计算虚拟化、存储虚拟化和网络虚拟化是其中的组成部分。网络虚拟化使得网络资源可以像计算资源一样按需供给。网络虚拟化在形态上分为“多虚一”和“一虚多”。 其中“多虚一”模式的虚拟化是把多个物理网络资源虚拟出一个逻辑资源，比如各种堆叠，集群技术；而“一虚多”模式相反地是把一个物理网络资源虚拟出多个逻辑资源。
- “一虚多” 在传统的网络技术中就有相应的例子，从应用角度可以分为管道虚拟化和业务虚拟化。管道虚拟化的例子包括各种VPN以及VLAN/QinQ等技术，它们提供各种逻辑管道实现对用户流量的承载和隔离；业务虚拟化的例子包括MSTP多实例MP-BGP多实例等，通过特定业务的多实例实现业务的逻辑隔离。 无论管道虚拟化还是业务虚拟化，都只是局部虚拟化，网络设备的虚拟化是一种更彻底的系统级的虚拟化，它不限于具体特定的业务或管道，而是提供一个完整的设备级的虚拟化。



- 云计算大量运用虚拟机。虚拟机启动后，可能由于服务器资源等问题（如CPU过高，内存不够等），需要将虚拟机迁移到新的服务器上。为了保证虚拟机迁移过程中业务不中断，则需要保证虚拟机的IP地址、MAC地址等参数保持不变，这就要求业务网络是一个二层网络，且要求网络本身具备多路径的冗余备份和可靠性。TRILL技术在一定程度上缓解了大二层的迫切需求，但是云计算往往要求在一个更广的范围内实施迁移，譬如跨机房，跨数据中心等，以实现资源共享和容灾。
- VXLAN（Virtual eXtensible Local Area Network）是VLAN扩展方案草案，采用MAC in UDP（User Datagram Protocol）封装方式，是NVo3（Network Virtualization over Layer 3）中的一种网络虚拟化技术。通过VXLAN可以构建大二层网络，支持扁平化胖树拓扑组网方式，链路带宽利用率高。
- 二层网络的扩展有多种技术，相比之下VXLAN具有以下有点：
  - 基于IP/UDP进行封装，可以在IP可达的范围内进行二层网络的扩展，需要的条件相对较低。
  - 普通802.1Q技术用12比特来表示VLAN；VXLAN引入了类似VLAN ID的用户标识，称为VXLAN网络标识VNI（VXLAN Network ID），由24比特组成，支持多达16M（(2^24-1)/1024^2）的VXLAN段，可以满足更大规模的用户标识。
  - 二层数据封装在IP数据包中，所以在数据传送过程中，可以充分利用IP网络的优势，譬如快速收敛、ECMP等特性。由于基于IP数据包，跟普通二层网络相比避免了环路的产生。

未来的数据中心 - SDN

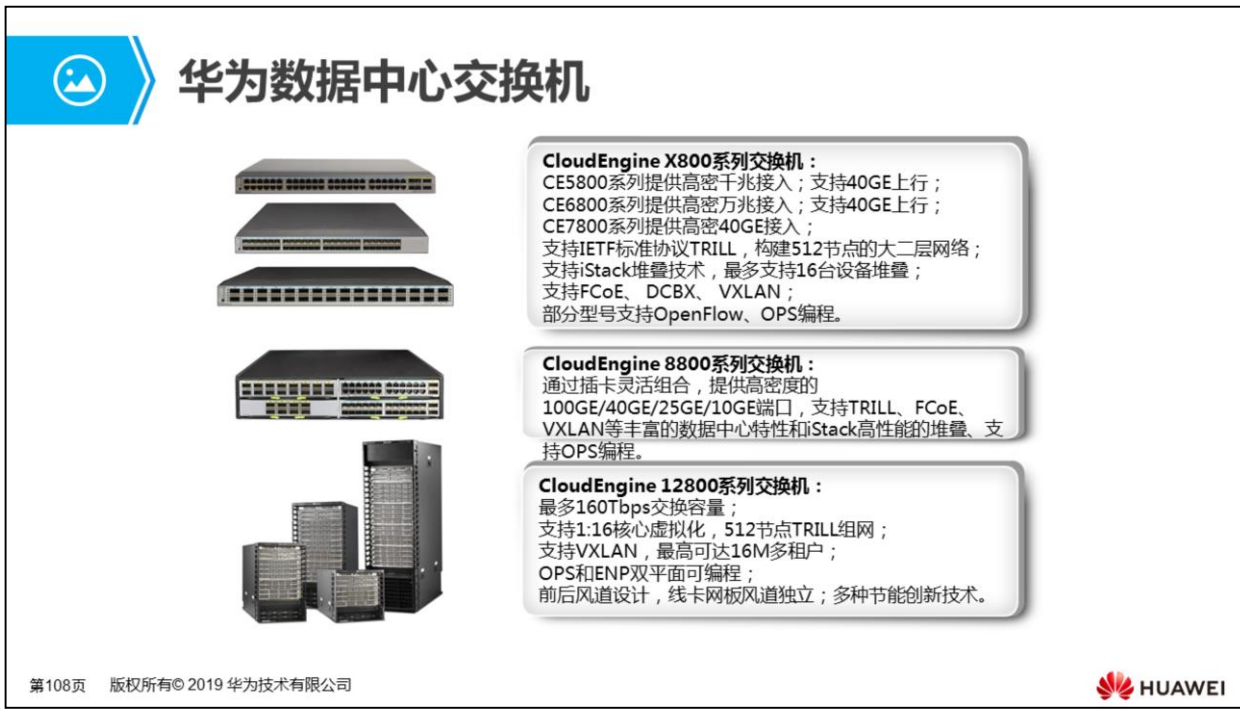


ONF解决方案	IETF解决方案
控制面转发面分离	管理面智能化，网络架构平滑过渡
OpenFlow标准	PCEP、I2RS、SNMP、netconf
互联网公司、新兴公司、运营商	传统设备厂商

SDN　通过全网统一控制，实现简化网络设备，灵活调度流量的目的。

HUAWEI

- 传统的IP网络采用分布式处理的模型，使得网络能够自愈，具有很高的可靠性。但是这种特点也带来了一些负面影响：
  - 管理运维复杂。IP技术缺乏统一管理和运维方面的设计，网络设置需要逐台设备进行调整。
  - 网络创新困难。IP网络设备中控制平面和数据平面深度耦合，引入新技术需要全网设备协同，使得新技术的部署周期较长（通常需要3~5年），严重制约了网络的演进发展。
  - 设备日益臃肿。IP分组技术基于IETF发布的RFC文件，目前RFC标准超过7000个，其实现复杂度很高。
- SDN的本质是给网络构建一个集中的大脑，通过全局视图和集中控制，实现全局流量和整体最优。SDN的关键价值在于：智能节点集中，简化运维；自动化调度，提高网络利用率；网络开放，支撑QoS等带宽和流量管理。
- 当前的SDN解决方案主要有两个流派：
  - ONF（Open Networking Foundation）建议将网络设备的控制功能(如路由计算)集中到一个Controller上去处理，转发表由Controller生成下发到设备上。设备功能大大简化，只负责转发，变成了一个傻瓜式的设备，Openflow是Controller和设备之间的控制接口。ONF主要由互联网公司、新兴厂商和运营商推动。
  - IETF则强调平滑过渡，在当前的网络架构上，实现网络管理层面的自动化和智能化，通过传统的管理接口，实现网络流量的灵活调度。该解决方案主要由传统网络设备厂商推动。
- SDN技术并不是专门为数据中心开发的技术，但是数据中心地理范围小，流量密度大，业务模型复杂的特点正是SDN技术擅长处理的，所以当前SDN技术在数据中心的应用进展很快。



- CloudEngine系列是华为公司面向下一代数据中心推出的“云”级高性能交换机，包括旗舰级核心交换机CloudEngine12800系列，以及高性能的汇聚/接入交换机CloudEngine8800/7800/6800/5800系列。CloudEngine系列软件平台基于华为新一代的VRP8操作系统，支持丰富的数据中心业务特性，如TRILL，FCoE，VXLAN等；还支持SDN编程。
- CloudEngin5800/6800/7800系列是固定配置交换机。其中CE5800系列交换机提供24/48个GE接口，同时提供4个10GE或2个40GE作为上联接口；CE6800系列交换机提供24/48个10GE接口，同时提供2/4/6个40GE上联口；CE7800交换机提供32个40GE接口。
- CloudEngin8800交换机是一款2U高度的TOR交换机，支持4个半宽灵活插卡；整机最高支持32个100GE、64个40GE，128个25GE或128个10GE接口。
- CloudEngine12800系列交换机是华为公司面向数据中心和高端园区网络推出的新一代高性能核心交换机。提供CE12816、CE12812、CE12808、CE12804、CE12808S和CE12804S六种产品形态，整机最大支持160Tbps交换容量，可以平滑升级到320Tbps，最高支持576个100GE、576个40GE、2304个25GE或2304个10GE全线速接口。具备业界领先的Clos交换架构和工业级的可靠性，以及严格的前后风道设计，采用了多种绿色节能创新技术，大幅降低设备能源消耗。

案例讨论

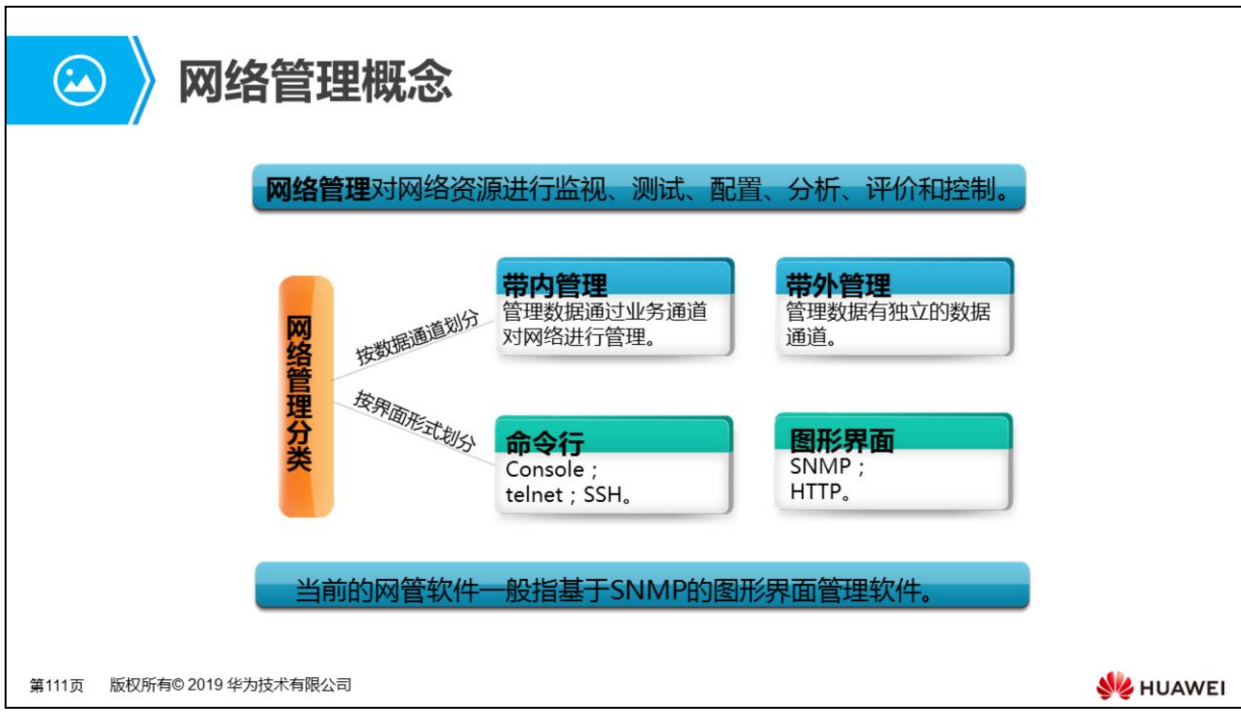
- 校园中计划设立一个中心机房，将个院系服务器集中到中心机房内统一管理，服务器数量大概会有1000台左右，将来仍有增加可能，请设计机房的网络结构。

  HUAWEI

- 首先确定数据中心的架构，究竟是选用传统架构还是新型的数据中心架构。从工程实践来说，要均衡技术成本稳定性等各个方面。对于该校的数据中心规模来说，采用传统架构还是可以满足要求的。当然如果出于试验目的，也可以采用新技术。
- 网络架构建议采用传统架构，考虑数据中心的规模，建议采用核心、接入两层架构，因为机房内集中了各个院系，所以建议按照院系进行网段划分，便于业务隔离。网关位置可以置于接入层设备，按照院系分配接入交换机。

目录

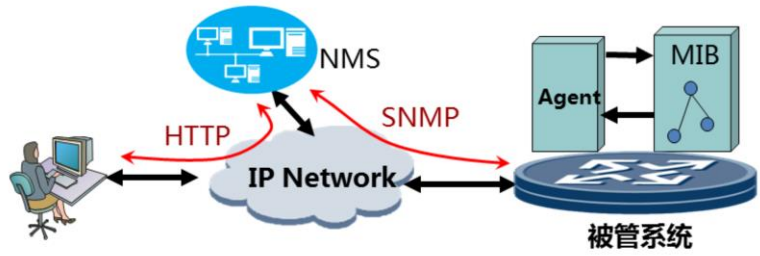
HUAWEI



- 不管是网络构建过程中还是网络建成之后，网络设备都需要配置。另外，在网络运行过程中，对网络资源的监测和控制不可少。这些工作都可以归类为网络管理。
- 网络管理有多种方式，这些方式可以通过多个维度进行分类。譬如新设备进行初始配置的时候，我们一般通过设备的console接口用终端设备接入进行配置，这种方式可以归类为字符界面的带外管理；当设备在运行状态下，我们通过Telnet/SSH等方式远程登录设备进行管理，这种方式可以归类为字符界面的带内管理。我们说网络管理的时候，当前一般指采用SNMP协议进行网络运行状态数据采集和配置参数下发的网管软件系统，它可以归类为图形界面的带内管理。
- 各种类型的网络都需要进行管理，但是对于小型网络，并不一定必须配置独立的网络管理系统，因为设备数量少，用户数量也较少，所以网络的管理工作量并不大，完全可以采用人工方式单独登陆每一台设备的字符界面进行管理；但是当网络的规模到达一定的程度，配置独立的网管系统可以很好地减轻网络管理的工作量。

网络管理体系架构

- 当前网管主流基于SNMP协议。
- 当前网管产品多提供WEB界面，提供图形化的随处接入管理功能。



  HUAWEI

- 基于SNMP的网络管理由多个网络组件组成：
  - 在网络设备上，将包含一个网管代理程序（Agent）和一个管理信息库（MIB），管理信息库将维护被管理设备端设备状态信息集，按照层次式树形结构组织存储。运行在被管理设备上的代理程序负责与网管设备NMS通信，响应NMS的请求并做出相应的操作。主要操作内容包括：收集设备状态信息、实现NMS对设备的远程操作、向网管端发出告警消息等。
  - NMS（Network Management System），是运行在网管端工作站上的网络管理软件。网络管理员通过操作NMS，向被管理设备发出请求，从而监控和配置网络设备。
  - SNMP是简单网络管理协议，在网管工作站NMS和被管理设备之间提供标准化的通信接口。
- 以上部分是网管体系的基本组件。当前为了提高网络管理的便利性，一般NMS都会集成WEB服务器，便于管理人员随时随地登录网管系统的图形界面查看管理网络。

华为网管产品 - eSight

序列	功能特性
1	用户管理
2	日志管理
3	资源管理
4	拓扑管理
5	告警管理
6	性能管理
7	物理资源
8	报表管理
9	自定义设备管理
10	配置文件管理
11	智能配置工具
12	WLAN业务管理
13	SLA业务管理
14	MPLS VPN业务管理
15	下级网管管理
16	单网元特性管理
17	系统Portal首页
18	数据转储与备份
19	网元适配包管理

  HUAWEI

- 华为eSight提供统一的企业网管平台，通过标准的网管协议管理不同厂商的产品。能够对应用软件系统、IT设备（服务器、打印机）与网络设备统一进行管理。
- eSight应用平台采用B/S架构，实现了功能模块的组件化和解耦，客户端只需要浏览器即可，系统升级或维护时只需更新服务器端软件。系统的规模弹性很强，便于在企业网中适用于不同场景。
- eSight提供丰富的管理功能，从常规的系统管理、网络管理到面向业务的WLAN/MPLS VPN管理。

eSight产品差异比较

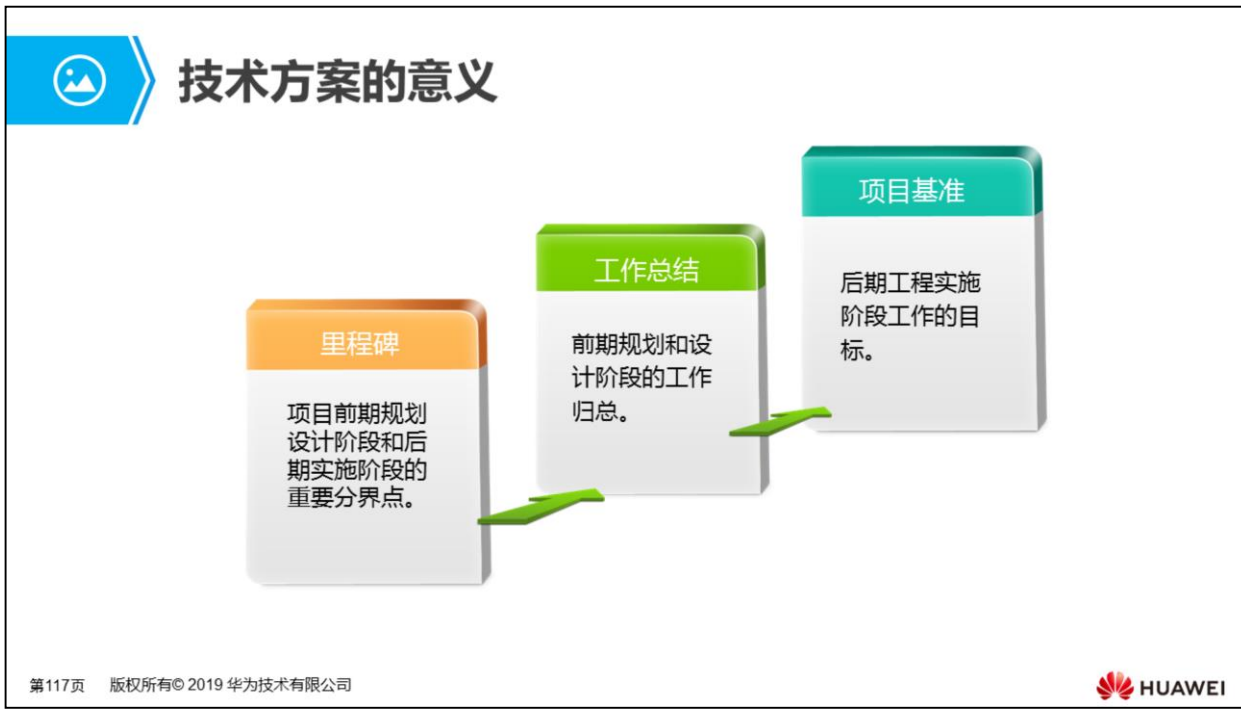
项目		精简版	标准版	专业版
管理规模		60个节点	5000个节点	20000个节点
功能		拓扑管理、网元管理、链路管理、物理资源、电子标签、告警管理、性能管理、配置文件管理、日志管理。 仅支持单用户。	精简版功能、自定义设备管理、报表管理、智能配置工具、IPSec VPN、MPLS VPN、WLAN、SLA、IP 拓扑、SNMP 告警北向接口、安全管理。提供数据库备份工具、故障采集工具。 支持多用户管理。	标准版功能 分级网管
面向市场		小网络，仅仅需要把设备管理起来，廉价。	中大型网络，主流应用平台，方案灵活，各组件灵活销售。	超大型网络，有分级管理的需求。
存储容量	当前告警容量	2万条	2万条	2万条
	历史告警容量	---	150 万条	150 万条
	日志数据容量	100万条	100万条	100万条
	性能数据容量	---	6000万条	6000万条

- 华为eSight网络管理平台提供三个版本供市场选择，精简版提供简化的网管功能，适用于小型网络；标准版提供完整的网管功能，是当前主流的网管应用平台；专业版提供分级网管功能，可以管理超大型网络。

- 建议配置eSight标准版。
- 配置网管软件的同时，需要确认网管运行平台。可以直接购买华为的预安装版（即包含服务器硬件）。或者自行采购服务器硬件，请根据管理节点数配置相应的服务器CPU、内存和硬盘容量；并按要求安装好操作系统和数据库软件。

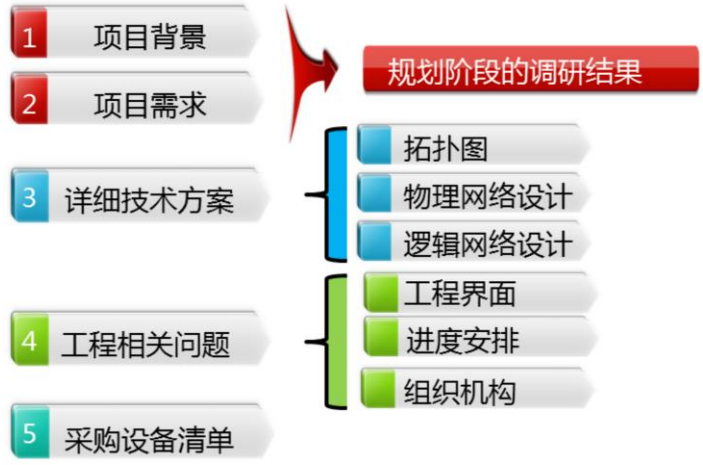
目录

HUAWEI



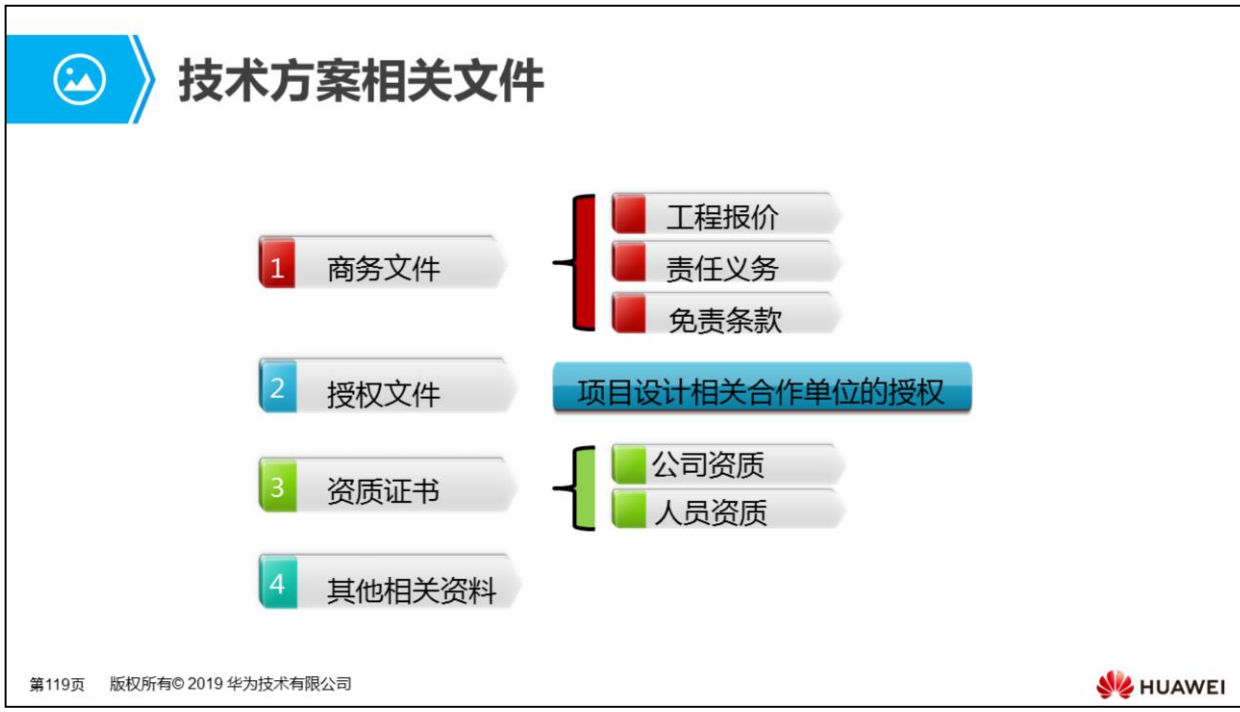
- 网络技术方案是整个项目周期中重要的里程碑，它代表着前期的规划设计阶段告一段落，也是前期规划设计工作的一个总结。在技术方案中，将完整罗列项目目标和实现细节，作为后续实施工作的基准。
- 在正式的工作运作中，项目的技术方案是作为投标文件中的一部分内容，而且是所有投标文件中最重要的文件之一。很多时候，技术方案的优劣会决定评标的结果。

技术方案内容



  HUAWEI

- 总体来说结束方案中将包含规划阶段和设计阶段的所有工作成果。
- 规划阶段的部分工作是直接决定项目的技术设计的，譬如项目的需求和技术方向的选型等，这些部分需要在技术方案中体现出来，是整个技术方案的前提。
- 主体是整个网络设计的详细内容，包括本章中前面提到的所有内容，当然应该根据项目的实际需求，适当增减网络模块。
- 在技术方案中，还要涉及到与工程实施相关的内容。当时，这部分内容并不是具体的工程实施步骤，而是保障整个网络技术方案的顺利实现的一些条件，譬如人员组织、进度安排等。
- 在技术方案的最后，一般会罗列整个方案中设计到的采购清单，包括网络设备、辅材如光纤尾纤，双绞线等。在这个清单中，一般不涉及到报价，报价部分在商务方案中体现。



- 一个项目的整套文件中，除了技术方案之外，还有其他的相应配套材料。这些材料提供跟项目相关的其他信息。保证工程各方确认项目能够顺利成功地实施。
- 商务文件，包括整个工程的报价，以及各方的责任和义务划分，分歧解决仲裁机制等法律方面的相关问题。
- 授权文件，工程中涉及到的相关合作方，譬如设备供应商等方面对相应项目的授权，保证设备供应和后期保修等方面的问题。
- 资质证书，工程实施方的资质证书和项目组成员的个人证书，保证实施单位具有权威机构认证的实力来成功实施该项目。
- 其他相关资料，包括本工程中设计的一些设备、产品的技术参数等，可以作为附件提供。

思考题

1. 数据中心当前流行的布线方式有哪些？（　　）
   A. TOR
   B. DOD
   C. EOR
   D. NSF
2. 在楼宇布线中，存在以下哪些子系统？（　　）
   A. 水平子系统
   B. 垂直子系统
   C. 接入子系统

HUAWEI

- 1、答案：AC。
- 2、答案：AB。


谢 谢
www.huawei.com

网络实施

HUAWEI

前言

- 项目实施是工程师交付项目的具体操作环节，系统的管理和高效的流程是确保项目实施顺利完成的基本要素。
- 本章将主要针对项目交付流程、高危操作流程、工程师服务规范三个方面进行介绍。
- 项目交付流程确保了项目管理的高效；高危操作流程最大程度上降低了实施环节中可能出现的风险；工程师服务规范为工程师树立了良好的职业素养标准。

目标

- 学完本课程后，您将能够:
  - 掌握项目交付流程
  - 熟悉高危操作流程
  - 了解工程师服务规范

目录

HUAWEI

项目交付流程的重要性

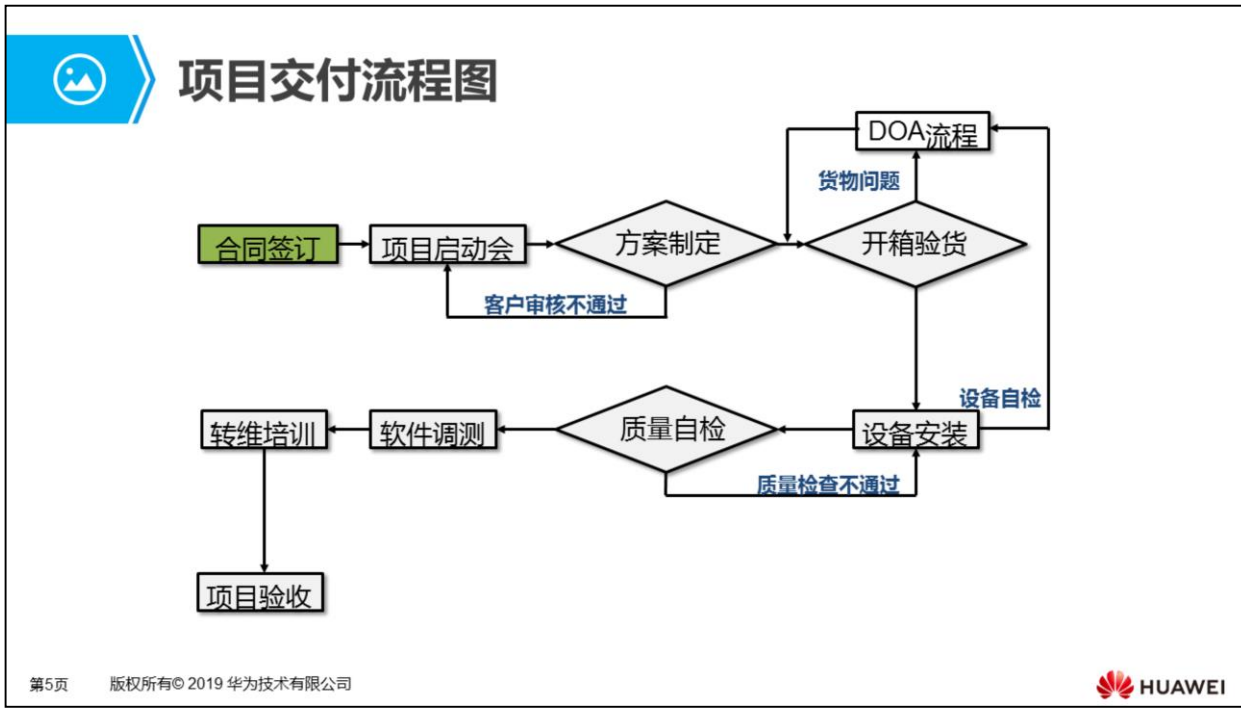
- 项目交付流程的定义：
- 项目交付流程规定了对项目实施的管理和作业控制要求，保证了工程项目实施按照规定的程序进行。

增加客户满意度

提高工作效率

降低项目风险

- 规范的项目交付流程有利于：
  - 提高客户满意度。
  - 提高工程效率，节约成本。
  - 降低项目交付风险。



- 合同签订：
  - 输出招标文件、投标文件、设计方案、设备清单，并成立项目组，明确项目成员。
- 项目启动会：
  - 了解客户需求，确认项目计划及周期，明确交付主体，了解客户相关实施要求，确定项目管理制度，如日报制度、周报制度、问题管理跟踪制度、项目例会制度等。
- 方案制定：
  - 项目实施人员了解客户需求后编写实施方案，并由项目TD进行初步审核，审核通过后交由客户评审，若客户评审不通过则需再次进行沟通修改，直到通过评审。
- 开箱验货：
  - 到货后由供货方、客户方、监理方共同对设备进行开箱验货，并签署货物签收单或装箱单。如存在货物问题，则需由供货方联系华为服务热线（400-822-9999）并按照DOA流程进行处理。
- 设备安装：
  - 设备安装前需对其安装环境进行检查，如明确设备安装位置、检查机房承重、检查机房温湿度、检查机柜空间、检查电源功率等。完成后对设备进行安装并连线打标签、加电检查等操作。

- 质量检查：
  - 设备安装完成后由实施方与客户共同对设备安装质量进行检查。设备安装质量需符合工程规范及客户机房相关规范，例如强弱电走线规范、设备标签规范、线缆标签规范等。
- 软件调测：
  - 包括单机调试，业务联调，割接。
- 转维培训：
  - 主要培训网络组网与配置，日常维护，紧急故障处理等。
- 项目验收：
  - 整理项目相关资料移交给客户，如拓扑图、设备清单、设备配置、设备连线表、IP地址规划表、设备用户名密码等，完成项目后需由客户签署验收证书。

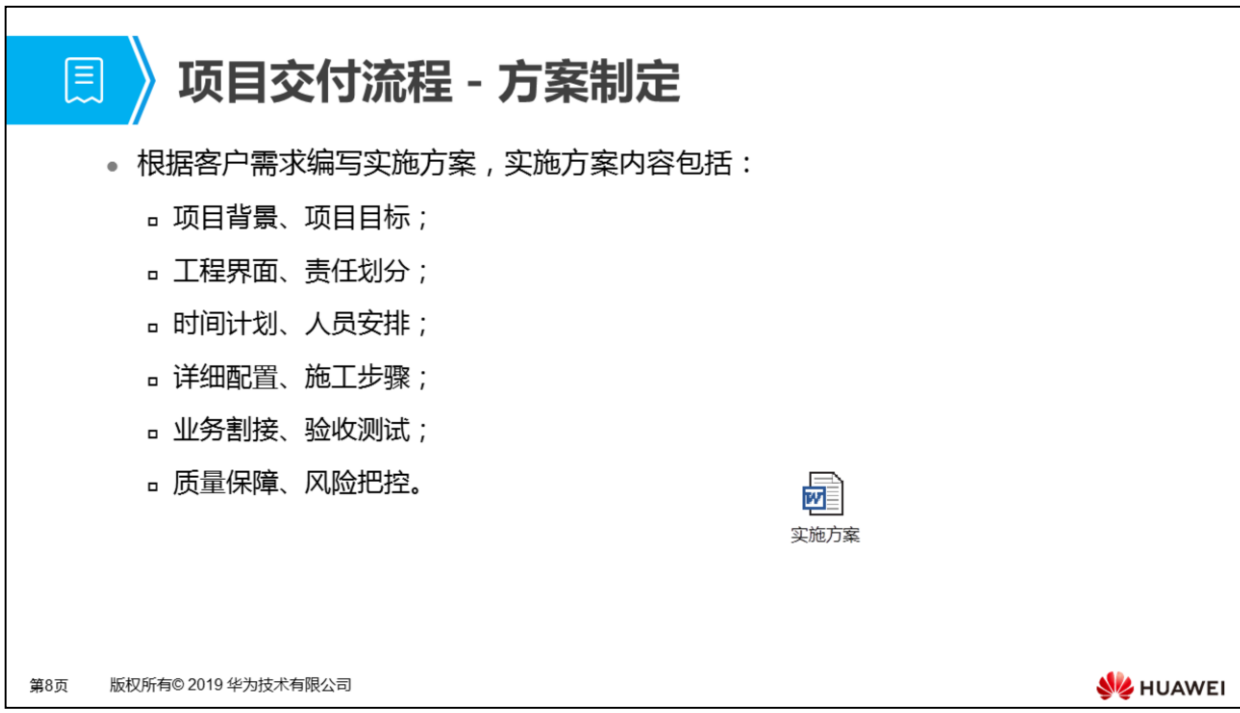
项目交付流程 - 项目启动会

- 合同签订完成后，与客户召开项目启动会：
  - 根据招投标方案明确客户需求；
  - 确认项目计划及周期；
  - 确定项目甲乙双方责任人及项目组成员；
  - 确定项目管理制度；
  - 确认设备安装环境。

项目启动会

HUAWEI

- 由项目经理组织与客户召开项目启动会，了解客户需求，明确相关技术实现方式。
- 开工前必须与客户确认设备安装需要具备的环境条件，避免因安装环境问题导致窝工。
- 开工前获取装箱单，了解清楚交付设备的范围。
- 确定项目管理制度：例如日报、项目问题反馈、例会等项目管理规范。
- 提醒用户进行项目工勘准备，以及工勘要求。



- 实施方案需根据招投标文件，网络现网环境以及客户需求编写。
- 项目背景、项目目标：
  - 主要说明现网状况以及存在的问题，项目建设目标等。
- 时间计划、人员安排：
  - 根据客户需求制定实施计划，明确关键时间点需完成的工作内容。
  - 项目组成员确认及职能定位。
- 详细配置、施工步骤：
  - 确认设备的物理设计，逻辑设计，脚本配置。
  - 制定施工的每个环节的具体操作步骤包括硬件安装、软件调试等。
- 业务割接、验收测试：
  - 根据实施方案进行业务割接，并配合客户对相关业务进行测试。
- 质量保障，风险把控：
  - 相关项目管理制度在一定程度上保证了实施工程质量，降低了项目风险。

项目交付流程 - 清点货物

- 到货清点需核对如下信息：
  - 到货数量和物流清单是否一致；
  - 设备数量和装箱单是否一致；
  - 设备数量和合同货物清单是否一致。
- 若实际发货与订单需求不一致，则定义为差错货，需要联系厂商处理。

- 主要核对装箱单如下内容：
  - 项目名称：核对项目名称是否正确。
  - 合同号：每个项目有唯一的合同号。
  - 箱名及数量：大件设备可能存放于好几个纸/木箱中，每个纸/木箱都有唯一箱名，需核对箱名及相关部件、数量。
  - 产品型号：核对是否与现场到货设备型号一致。

项目交付流程 - 开箱验货

- 核对装箱单的部件编码、型号、数量等是否与现场到货一致；
- 核对货物部件是否有物理损伤；
- 验货无误后需安装督导、客户代表共同在装箱单上签字确认。

局 点 装 箱 单

装箱单号：

地址：深圳市龙岗区坂田华为技术有限公司
电话：+86-755-28780808转发货管理部
传真：+86-755-28781889 邮编：518129

最终用户项目名称：
客户项目名称：
产品型号：NetEngine80E
站型/站点：

发票客户：
用户单位：
用户地址：自提
联系方式：
经 办 人：

客户合同号				最终用户订单号		箱单总件数	3	装箱制单	
华为合同号				机器编号		执行标准		流水号	35608084

大箱号	箱名	类型	小箱号	部件编码	型号	描 述	订货数	实发数	验货数	欠货数	单位	备 注
1	C0012694149	纸箱		03030KJY	CR52-LPUF-21-A	成品板-NetEngine80E-CR52L		1			PCS	
2	C0012694150	纸箱		03030KJY	CR52-LPUF-21-A	成品板-NetEngine80E-CR52L		1			PCS	
3	C0012694151	纸箱		03030GSH	CR52-P20-12x10	成品板-NetEngine80E-CR52		2			PCS	
				34060473	eSFP-1310nm-10	光模块-eSFP-1310nm-	14	14			PCS	
				S4016965	QM.0D5002	光收发一体模块(eSFP,850n		6			PCS	

备注：
安装督导（签字）： 客户代表（签字）： 监理代表（签字）： 开箱验货日期：____年__月__日
请安装督导将此单随工作手册一同返回安装工程部 表格编号：SC/DB-PP/W02/F01 V1.2

- 数量和型号检查：
  - 部件编码：华为针对设备部件的唯一标识编码。
  - 型号：设备或板卡的具体型号。
  - 实发数：实际发货数量。
  - 若货物外包装损坏需停止开箱，拍照并联系办事处进行处理。
  - 图中为NE80E装箱单，从此页可以看出这台设备包含了3个纸箱，箱号分别为C0012694149/C0012694150/C0012694151，其中C0012694151纸箱中装有两块板卡，20个光模块。
- 完整性检查：
  - 外包装变形。
  - 外包装破损。
  - 货物本体损坏。

项目交付流程 - DOA流程

- DOA（Dead On Arrival）到货即损的定义：
  - 设备无外观损坏且第一次上电不能正常工作或上电运行48小时之内出现故障。
- DOA处理方式：
  - 第一时间拨打华为服务热线400-822-9999联系TAC处理；
  - 由TAC（技术支持中心）鉴定是否为DOA情况；
  - 将货物问题反馈表发送给TAC，由TAC协助完成后续流程。
- 货物问题反馈表：
  - 表中“问题详细描述”行需详细描述货物问题；
  - 保证”补货地址”、”要求到货时间”、”收货人”、”联系电话”正确。

货物问题反馈表

HUAWEI

- DOA受理条件：
  - 非测试产品、非样机。
  - 必须提供原外包装箱和包装材料。
  - 原外包装箱完好无损（无撕裂，无破口，无受潮，无坍塌，无凹陷）。
  - 包装材料完整无缺（包括泡沫塑料及塑料袋）。
  - 随机附件完整无缺（以装箱清单为准）。
  - 产品外观必须完好，无物理损伤（注：若有物理损伤请联系运输商索赔）。
  - 主机上所有封条未启封。
  - 机体上各类标签完整无缺。
  - 必须为原厂装配的硬件、预装的软件（操作系统）和驱动程序。

项目交付流程 - 设备安装环境检查

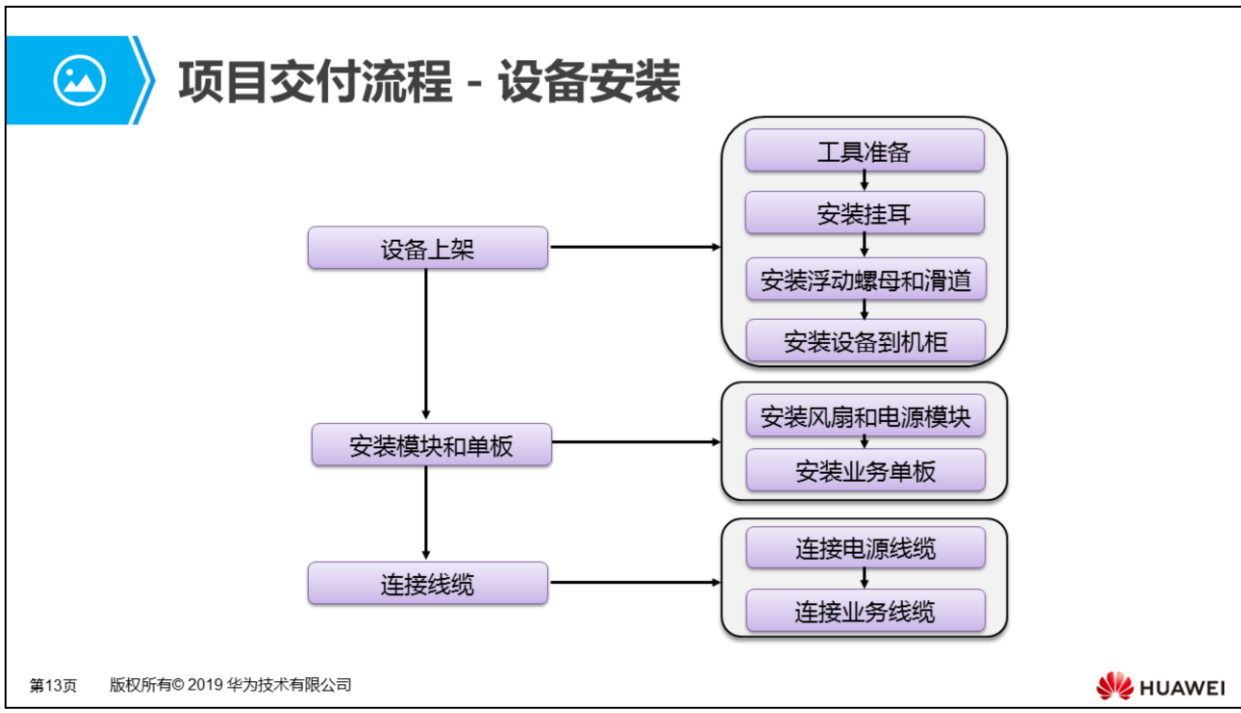
机房整体环境(空间、温度、湿度）

配电状况（电压、功耗）

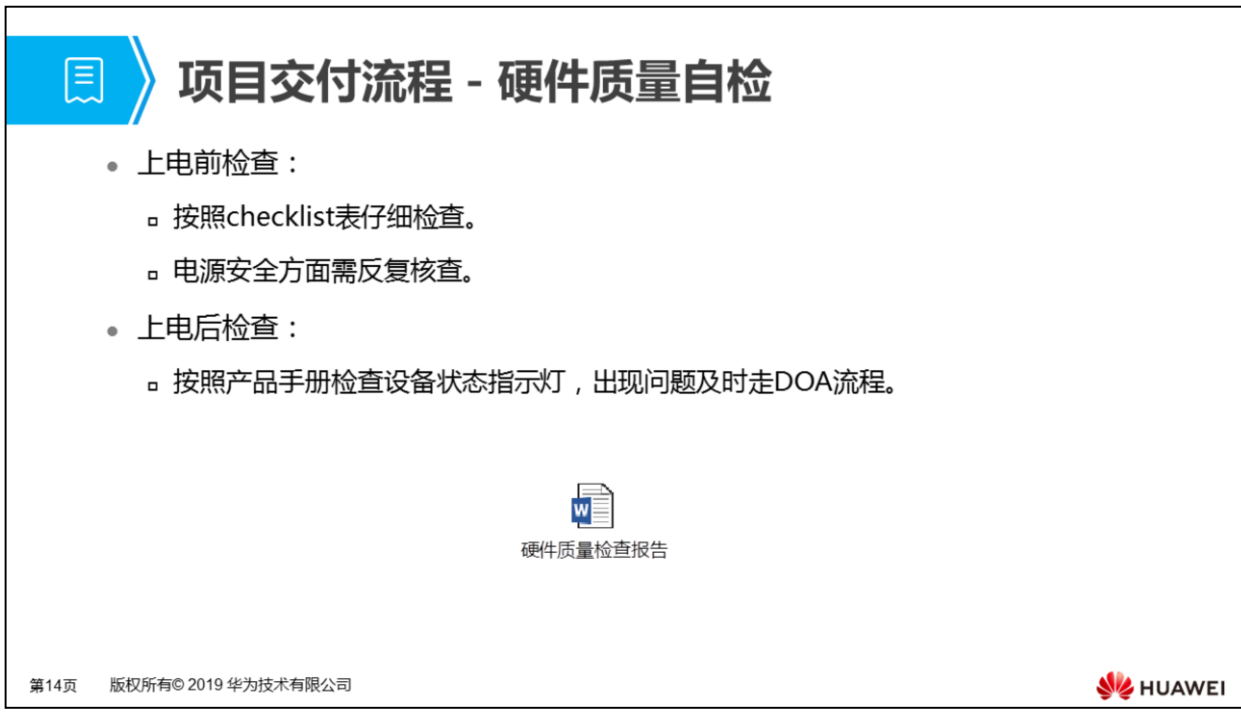
机柜状况
（尺寸、走线、接地状况）

现场实施条件确认表

- 设备安装前需对设备所属安装环境进行检查，保证设备能够顺利上架安装，且能够提前规避相关隐患。
  - 机房环境：主要包括机房温湿度、洁净度、高度、地板类型及高度、承重、布线方式等。
  - 设备机柜：主要包括设备对于机柜的尺寸需求，具体设备尺寸可参考产品文档中的硬件描述部分。
  - 设备电源：根据设备配置确认设备所需的电源接口数量和规格，如标配线缆-16A、设备侧C19、电源侧C20。
  - 设备功率：确认设备功率是否超出通信电源规格，根据设备最大功耗计算，实际功耗可参考如下链接：华为网络产品功耗计算机&配电工具 http://support.huawei.com/onlinetoolsweb/pda_cn 。
  - 互联线缆：确认线缆的提供方及数量。
- 设备安装前若机房环境不能满足安装需求，请尽早告知客户风险并提醒用户整改。

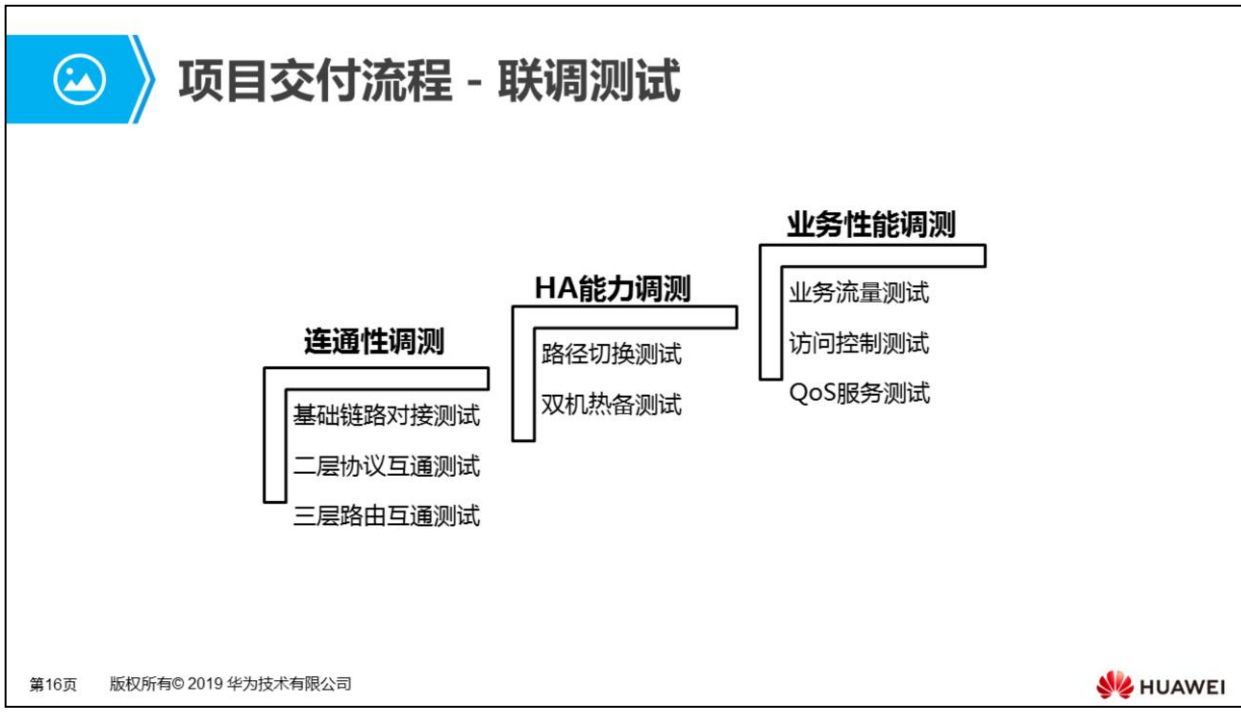


- 准备相关工具：
  - 可参考相关设备产品文档准备安装工具和附件，主要包括：剪刀、一字螺丝刀、十字螺丝刀、记号笔、安装模板、浮动螺母及配套的螺钉、滑道及配套的螺钉（需用户自行准备）、设备抬手等。
- 安装挂耳：
  - 测量从前方孔条到前门内侧的距离，并按照距离适当调整挂耳安装位置，将挂耳安装到设备上。
- 安装浮动螺母和滑道：
  - 根据设备自带安装模板安装浮动螺母。
  - 从安装附件包中取出安装模板（安装模板随设备自带），根据对应设备型号的安装模板安装浮动螺母。
  - 将滑轨固定到机柜中。
- 安装设备到机柜：
  - 大型设备需多人合作将设备抬到机柜前门，先将设备的背面底部搭接在滑道上，再缓慢地将设备沿着滑道推入机柜，并通过螺钉将设备固定在机柜上。
- 安装模块和单板：
  - 一般风扇和电源模块都有固定的安装插卡位，而业务单板需根据业务需求进行安装，同时注意触摸单板必须佩戴防静电手腕带。
- 安装线缆：
  - 电源线缆要确认电源的功耗是否满足需求，正负极连接正确，注意出孔位置黏贴防火泥。业务线缆走线要清晰，安装完成后需打好标签，用于后续工程操作参考。



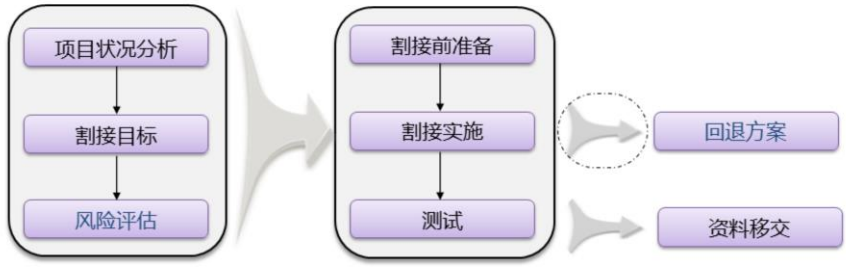
- 上电前检查：
  - 设备安装完成后需针对设备安装质量进行检查，且设备安装需符合客户相关要求，如走线标准、设备标签标准、线缆标签标准等。
  - 机柜安装主要检查机柜的安装是否固定可靠；门及门锁开关顺畅；机柜垂直偏差应小于3cm，整行机柜在同一水平面上；机柜外形不能出现变形等。
  - 线缆布放：线缆需理顺，间距均匀，松紧适度，线扣整齐，不留尖刺；信号线缆在机柜内的走线正确，不影响维护和扩容；电源线、地线与信号线分开布放，一般间距大于3cm；标签制作模板需符合客户要求，标签位置整齐、朝向一致。
  - 接地：机柜采用大于16mm的保护地线就近连接机房地排；设备、机箱外壳保护地线可靠连接至机柜接地点；机柜前后门、侧门可靠接地，线径不小于6mm 。
  - 机房环境：供电电压及空开容量满足设备长期安全运行要求；机房环境温度和相对湿度满足设备长期安全运行要求 。
- 上电后检查：
  - 设备上电后检查的重点是关注各种指示灯的状态，重点观察电源指示灯、风扇指示灯、主控板指示灯、业务板指示灯、接口板指示灯等。
  - 如果指示灯状态异常，则需要登录设备进一步查看设备工作状态。
  - 如果设备正常上电却无法正常启动，或上电运行48小时内出现故障，则定义为DOA，需要联系厂商进一步处理。

- 指示灯查看：
  - 图1为电源模块，INPUT/OUTPUT绿色常亮表示电源输入输出正常。ALARM常灭表示电源模块正常，红色常亮表示异常。
  - 图2为监控板，RUN/ALM（运行状态指示灯）绿色慢闪表示该单板系统处于正常运行状态，快闪表示该单板的系统处于未注册状态。ACT（主备状态指示灯）绿色常亮表示该单板为主用状态，常灭表示该单板为备用状态。
  - 图3为交换网板，RUN/ALM绿色常亮表示该单板已经上电，但是软件未运行；绿色慢闪表示该单板处于正常运行状态；绿色快闪表示该单板处于上电加载或者复位启动状态。黄色常亮表示该单板处于下电状态。
  - 设备单板指示灯的更多显示状态信息需查阅相关设备的操作手册。
- 运行状态查询：
  - 使用display device查看设备板卡的注册状态，确认Status为Normal状态。
  - 使用display device slot xxx（xxx表示槽位号）查看具体槽位板块状态。
  - 使用display power查看设备电源状态。
  - 使用display power system查看设备功率。
  - 使用display version查看设备的版本信息。
  - 使用display esn查看设备序列号。
  - 更多查看和测试命令需查阅相关设备的操作手册。
- License申请：
  - 如需申请License，请收集设备ESN和License纸质文件上的ActivationPassword，登录http://app.huawei.com/isdp进行License申请。
  - 申请成功后，加载License到设备，并核实相关功能授权是否生效。



- 联调测试内容：
  - 链路测试主要使用display interface brief查看接口是否up，如接口down请检查线缆连接、端口协商模式及光功率等。
  - 二层协议主要检查802.1Q配置，生成树配置及链路切换测试，LLDP邻居状态检查等。
  - 三层主要包括直连互通测试，路由协议邻居状态检查，路由条目是否缺失，并模拟路径故障进行演练测试。
  - 双机热备测试主要测试链路和设备等出现异常时，备用设备是否能成功切换为主用状态，目的在于测试双机热备的可靠性。
  - 业务流量测试主要测试业务流量走向，一般可用tracert命令查看。
  - QoS服务测试主要检查针对用户流量做的QoS是否生效，是否达到预期效果。
  - 访问控制测试主要测试用户访问网络的权限，如是否成功认证，授权，审计等。
  - 其他业务测试，如组播、MPLS、SNMP等需根据客户需求执行。
- 联调思路：
  - 先南北，再东西。
  - 先基础再协议。
  - 核心-汇聚-接入-边缘。
  - 先内网，再外网　　。

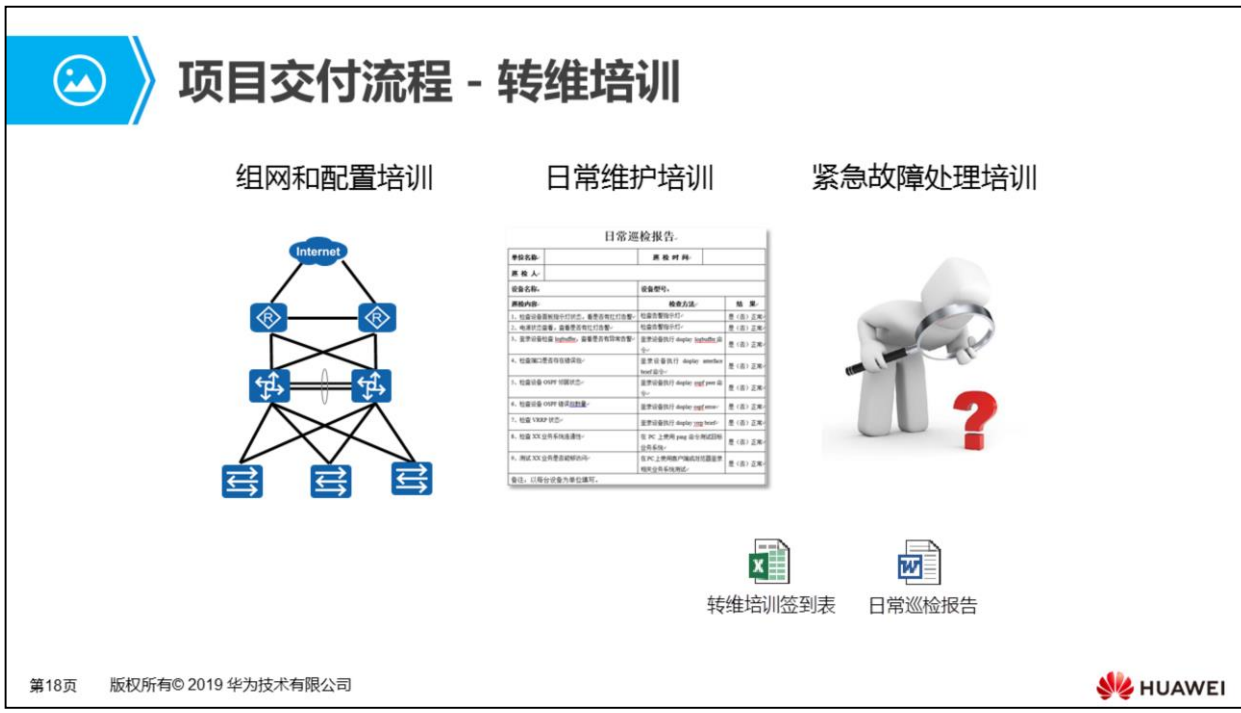
项目交付流程 - 割接并网



- 风险评估往往是最关键的环节。

HUAWEI

- 割接并网注意点：
  - 避开用户业务高峰期进行操作。
  - 提前准备好割接配置文件并搭建测试环境验证。
  - 提前准备好回退配置文件，防止割接失败。
  - 做好相关操作人员安排及操作时间点规划。
  - 完成割接后进行网络侧验证测试。
  - 测试完成后由用户对应用业务进行测试。



- 组网和配置培训：
  - 主要培训网络拓扑结构、技术原理、地址规划、流量走向、信息安全等。
- 日常维护培训：
  - 主要培训日常维护操作的工作，如对设备环境、设备基本信息、设备运行状态、业务运行情况等进行检查。
- 紧急故障处理培训：
  - 培训客户当遇到一些紧急故障时，可以快速处理的方法。

项目交付流程 - 验收

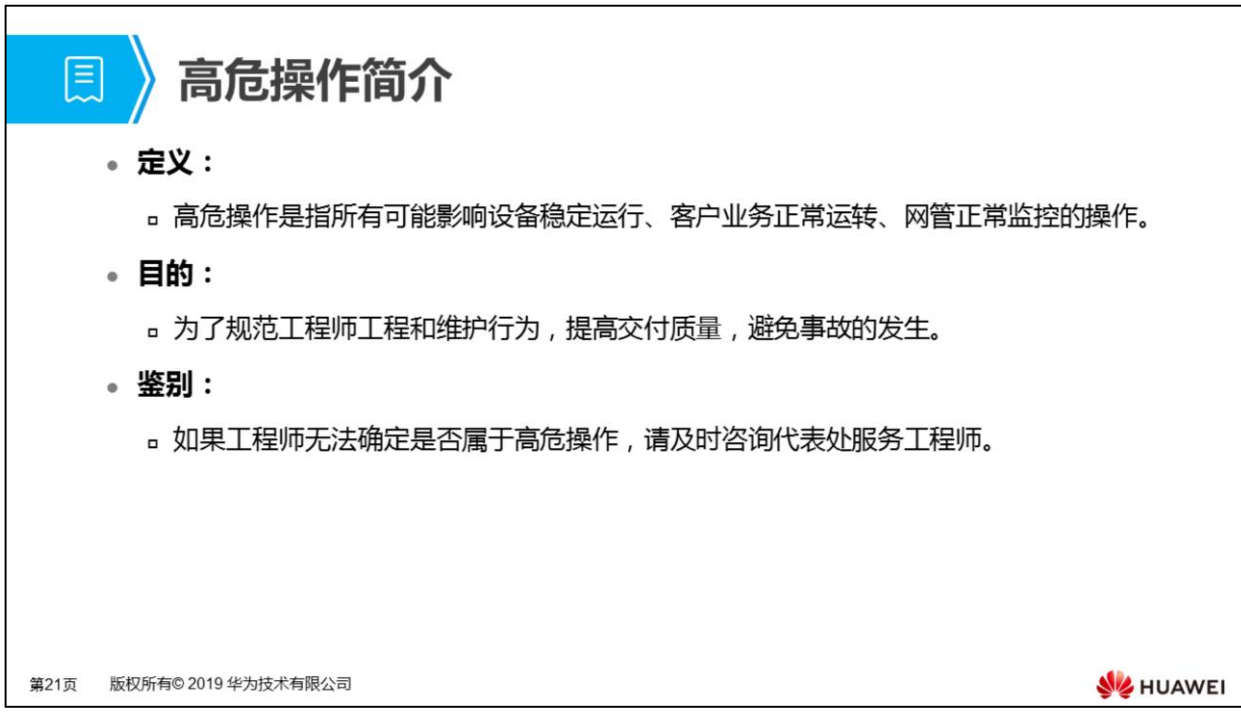
项目验收会

验收交接

- 项目交付完成后，由项目经理组织客户、监理、施工方等召开项目验收会。
- 项目验收会主要议程：
  - 项目概况介绍。
  - 施工单位介绍施工情况及质量情况。
  - 监理单位阐述监理情况及质量评估。
  - 查看现场。
  - 资料归档。
  - 签署验收证书。

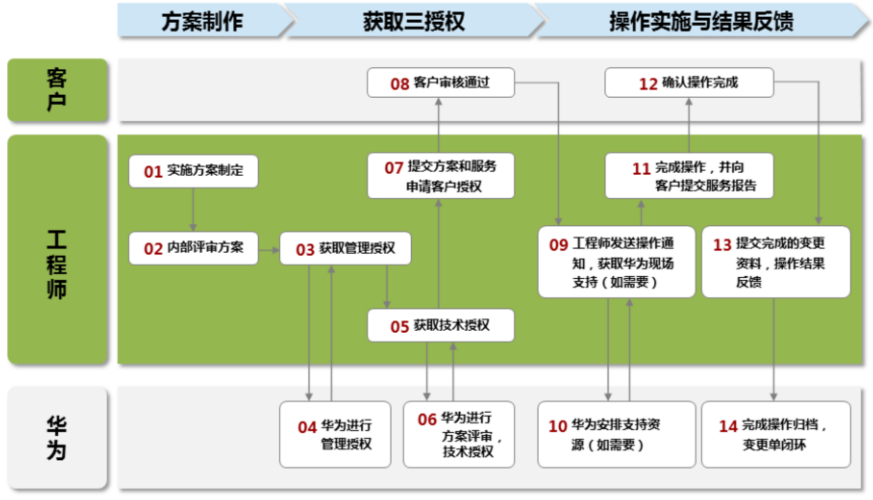
目录

HUAWEI



- 高危操作的范围：
  - 包括但不限于数据调整、数据迁移、数据恢复、业务割接、系统扩容、软件升降级、带电拔插、关电复位、主备倒换、容灾演练、与现网设备物理端口的连接或断开操作（即网元物理端口的连接变化）、对承载业务的电源、中继线缆、光纤等硬件进行的操作等。
- 高危操作级别分类如下：
  - 一级：所有重大项目、重点网络的割接、改造、扩容、升级等操作。
  - 二级：其它高危操作。重要保障通讯时间段、版本首次应用、前次操作失败后的再次操作、故障频发网络等场景下的高危操作。

高危操作流程

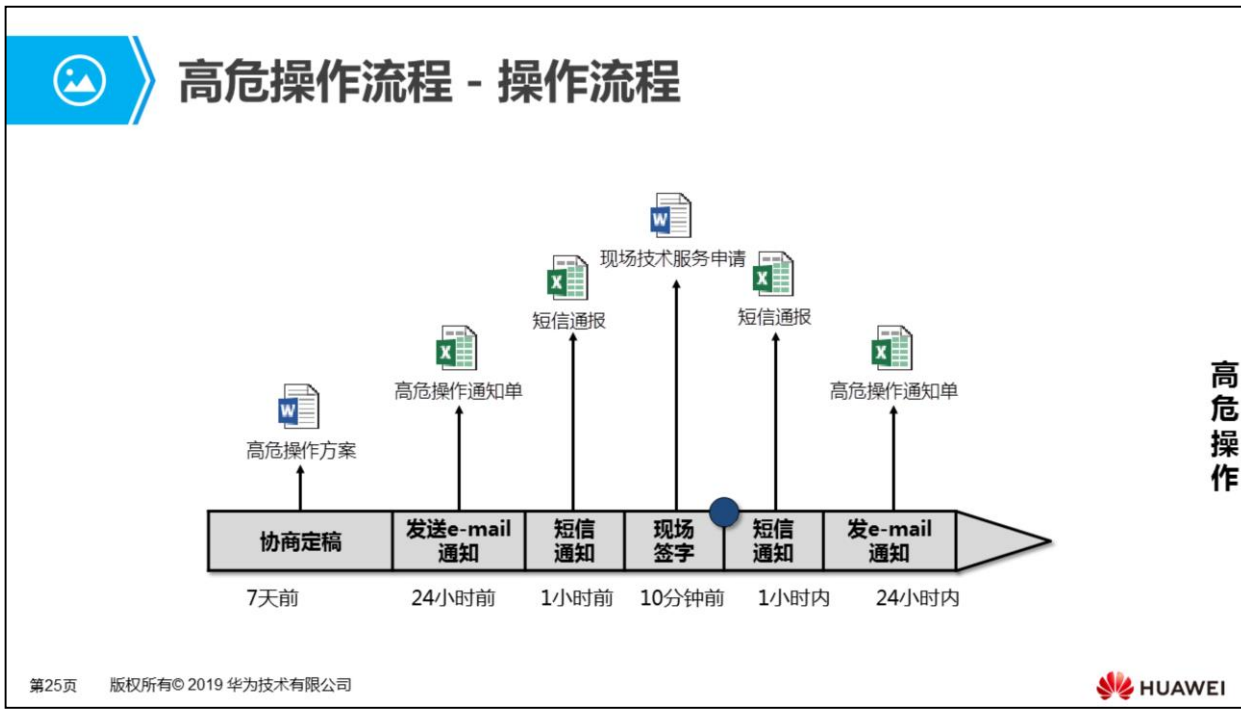


高危操作流程 - 方案制作

高危操作方案

高危操作流程 - 获取三授权

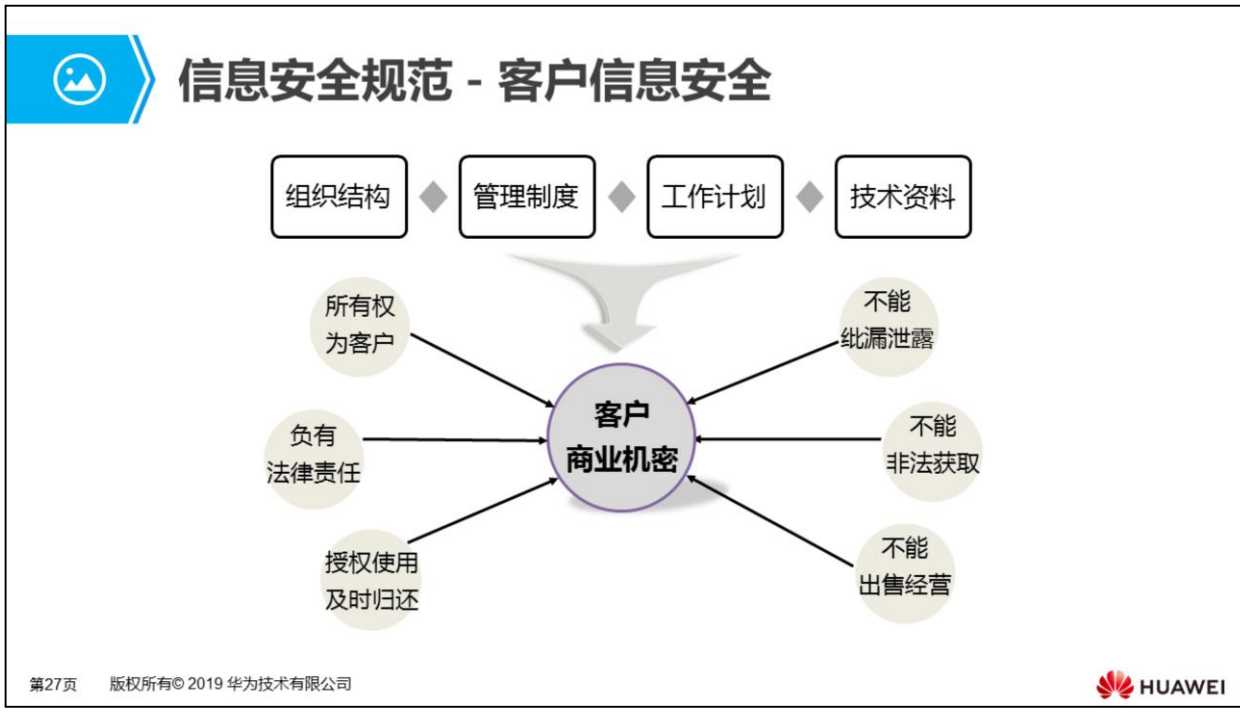
- **管理授权：**
  - 结合项目情况，发送邮件给华为项目经理进行管理授权。
- **技术授权：**
  - 邮件发送技术方案给华为技术专家进行技术授权，且必须在操作前三天提交方案申请审核。
- **客户授权：**
  - 客户项目建设负责部门进行操作审批，以书面或邮件方式进行确认。



- 实施前：
  - 《高危操作方案》至少在一周前定稿并获得甲乙双方签字同意。
  - 工程师应在操作24小时前，邮件发送《高危操作通知单》到客户及代表处产品接口人处。
  - 实施前准备好相关工具、板件、软件版本、人员安排及保障备件。
  - 高危操作实施前，工程师需在操作前1小时短信通知客户单位授权人、代表处/系统部网络维护接口人、代表处/系统部服务Leader。
  - 通过书面向客户递交《现场技术服务申请》客户签字/签章后，工程师才允许进行现网设备的操作。
- 实施中：
  - 实施中如果遇到初始未预料到的问题，需及时联系代表处/系统部网络维护接口人寻求帮助。若未能按时完成，需按实施方案进行回退操作。
- 实施后：
  - 实施动作完成后，需及时短信通知客户单位负责人、代表处/系统部网络维护接口人。
  - 高危操作实施完成后，需及时将变更材料提交给客户。操作完成24小时之内邮件发送《高危操作反馈单》到代表处产品接口人处。

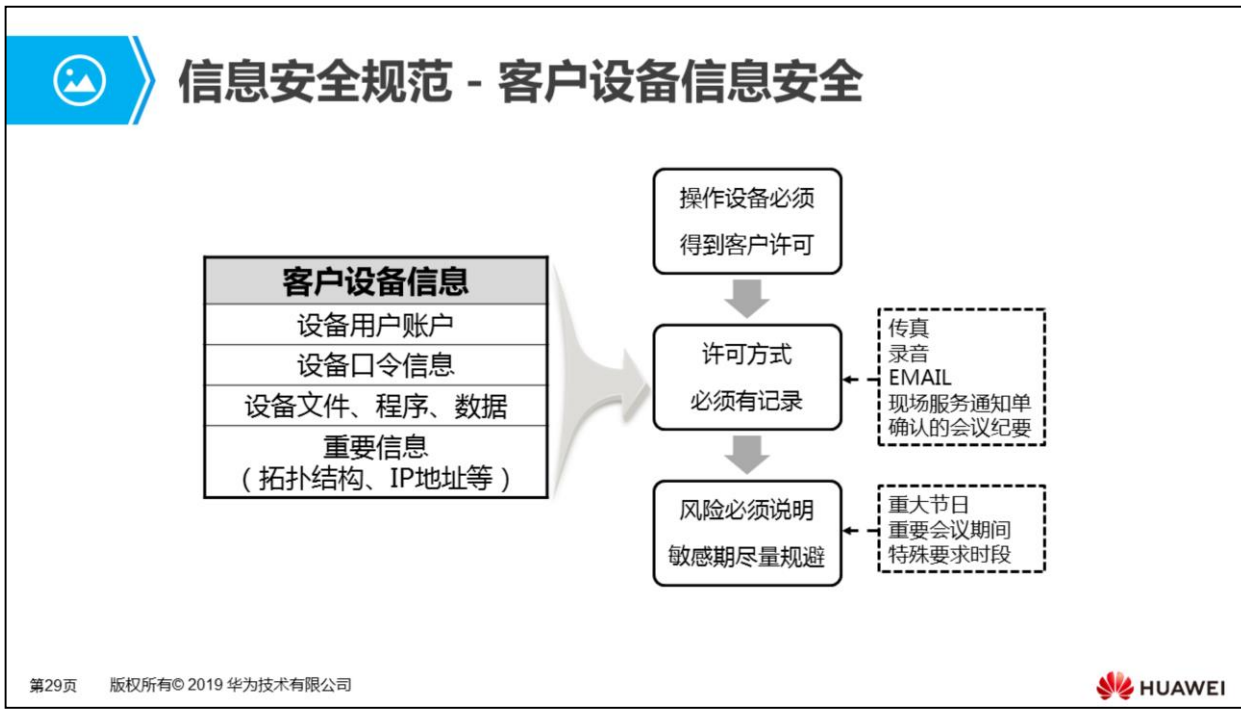
目录

HUAWEI



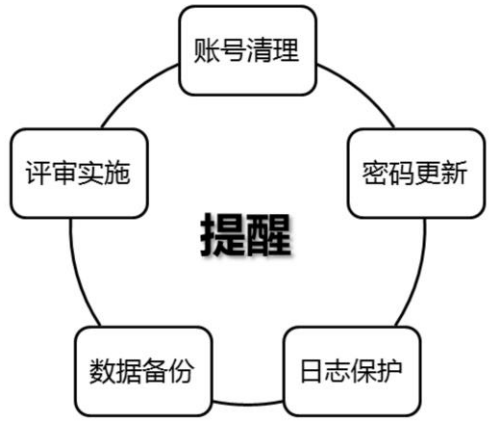
- 客户的商业机密主要包括如下：
  - 客户业务运作体系、组织结构，以及业务关系及工作职责。
  - 客户管理制度、业务流程。
  - 客户工作规划（计划）、作业计划。
  - 技术档案与资料、工作记录。
  - 设备维护技术指标。
  - 质量管理制度及数据。
  - 客户所有的、具备法律规定的商业秘密性质的其他信息。

- 针对客户商业机密的规范要求为：
  - 工程服务人员在日常工作中，对从客户获知的商业秘密有保密责任。
  - 客户的相关帐号密码要及时归还客户并建议立即修改。
  - 不得以盗窃、利诱、胁迫或者其他不正当手段获取客户信息保密范围内的商业秘密。
  - 不得违反客户有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的客户信息保密范围内的商业秘密。
  - 不得随意监听客户电话，因业务需要监听电话时，必须遵守客户相关管理规定执行。
  - 不得以任何方式向任何第三方泄露、出售、出租、转让、许可使用或共享客户的技术信息、经营信息，或提供可接触客户技术信息、经营信息的手段。
  - 如果因交付合作项目，需要向合作单位提供客户的保密信息，应先获得客户的书面同意，并确保该合作单位不向任何与项目无关的人泄露信息。
  - 合作项目结束时，应根据客户的具体要求返还全部或部分含有“技术信息”、“商业秘密”的书面、电子资料。
  - 对客户的保密义务不应因项目合作结束而终止。只要客户的相关信息还属于法律上规定的商业秘密，则对该信息的保密义务就一直存在。
  - 对于以上规范要求，所有工程服务人员应严格执行，对违反客户信息保密规定并给客户造成损失的，责任人应承担赔偿客户损失并负相关的法律责任，包括民事责任或刑事责任等。



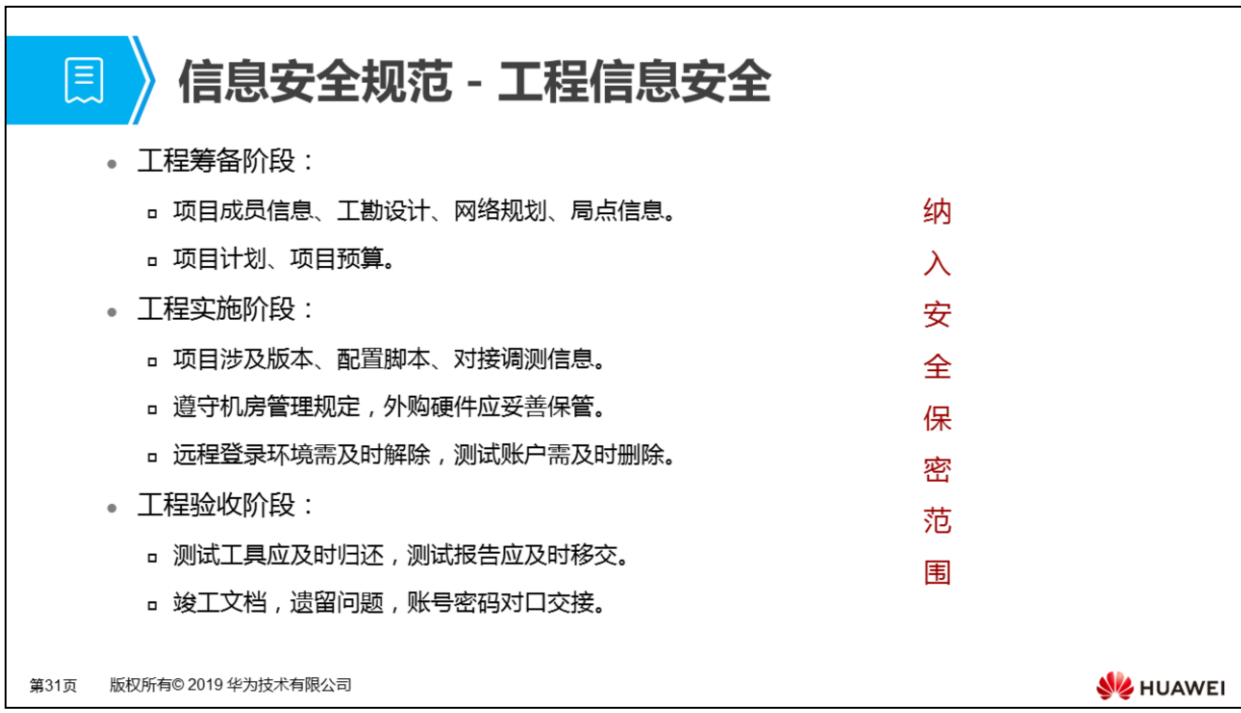
- 客户设备信息安全主要有：
  - 未经客户许可，不得持有和传播客户设备口令信息。
  - 不得持有和传播客户设备中的加解密程序、算法以及加解密的数据文件，确为工作所必需的文件和程序应及时从便携机中删除。
  - 所有对外资料内容应注意不侵犯他人的商业秘密，不贬低、攻击竞争对手和其它企业，不侵犯他人的著作权。公司内部使用的培训资料应注意保密，对内（即员工培训资料）与对外（即客户培训资料）要严格区分，对外培训资料应不含有具体客户信息、项目案例、专题等技术资料中不得包含任何具体客户信息。
  - 经过客户授权获得的设备秘密以上级别文档，未经许可不得传递给其他人员。
  - 客户设备的重要信息（如客户网络拓扑，IP地址等）严禁传播，私自打听。
- 客户设备信息安全操作要求：
  - 未获得客户许可，不得将自己的便携设备接入到客户设备所在网络；工程和维护过程中，需要得到客户许可并指定明确端口和IP地址后才能进行维护；该许可必须是传真、录音、现场服务确认通知单、确认的会议纪要以及EMAIL等方式之一。
  - 处理问题过程中，未经客户许可，不得对客户设备程序、配置文件、数据以及日志进行修改。
  - 对客户设备进行有风险性的操作时，应事先书面向客户说明，得到同意后，才能执行；维护过程中，对设备有重大影响的操作应该在客户规定时间范围（通常为0:00 - 5:00，具体视客户规定）中进行。
  - 在敏感的通信保障期间（默认为重大节日、重要会议期间、业务流量高峰期以及客户特殊要求时段）对设备的操作应该谨慎。
  - 不得利用客户网络玩网络游戏或者使用对网络有明显影响的软件等。

信息安全规范 - 提醒客户信息安全



  HUAWEI

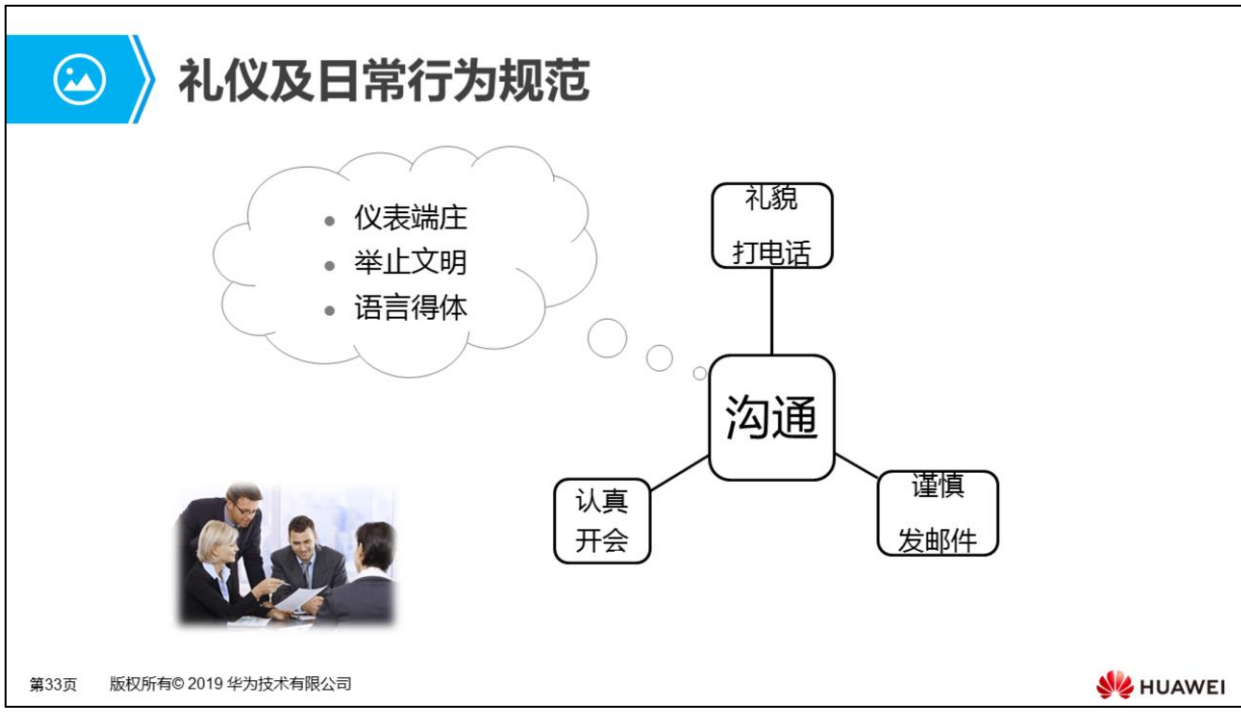
- 提醒客户信息安全：
  - 提醒客户对设备帐号进行及时清理，清除不用的帐号。
  - 提醒客户按照日常维护指导定期地对设备的所有密码进行更新，并保证密码的复杂度。
  - 提醒客户不得私自更改设备日志设置，不得私自关闭产品记录和日志的程序，不得对客户设备的日志进行增加、删除和修改等操作。
  - 提醒客户定期对设备进行系统和数据备份，并对备份数据进行妥善保存。
  - 提醒客户自行编写的且需在设备上运行的脚本必须通过办事处向华为公司研发部门进行评审后才能实施。



- 准备阶段：
  - 项目组织结构涉及的成员和通讯信息。
  - 工勘设计、网络规划和局点信息调查的输出件涉及到的客户通信信息。
  - 项目计划、预算文件都涉及到客户的商业机密。
- 实施阶段：
  - 版本申请License文件中涉及客户商业信息，如：用户数量信息、业务功能信息等，需要严格保密。
  - 各个模块的调试阶段，从客户处获得的对接信息和调测信息必须在调试结束后对其进行删除，如系统登陆帐户信息、网络设备接入信息等。
  - 安装阶段不得在非客户设备上安装使用和非法占用客户购买的操作系统、数据库等软件，同时不得将客户购买设备的序列号、相关软件License信息用于非本项目中。
  - 安装阶段产生的文档涉及外购件硬件信息的设备序列号、设备条码等，这些也被纳入文档的安全保密范围。
  - 安装调试阶段进出客户机房时必须遵守客户的机房管理规定。

- 调试阶段从客户获得的测试工具（测试手机）和测试卡，需要专人登记造册进行保管和使用，且只能用于系统测试，不能用于其他用途。调试结束后必须归还用户，要求客户签字验收无误。
- 调试阶段建立的一切远程登录环境涉及的登录信息在调试结束后必须修改或者删除并经客户签字确认。
- 调试阶段建立的测试帐户信息、余额修改信息等，仅在客户要求保留并签字确认后方可保留。
- 调试阶段未经客户允许不得随意增设测试帐户信息和为帐户开通业务功能，如开通彩铃业务测试、国际呼叫测试、国际短信测试等。
- 调试阶段任何接入终端必须安装防病毒软件，即将割接和商用设备必须按照合同配置及时安装防病毒软件，未经客户允许不得在任何客户设备上安装其他软件和工具，并要向客户讲解安装软件和工具可能带来的危害。
- 调试阶段生成的验收手册包含了客户的业务特性、计费信息等，属于客户商业机密，必须纳入文档的安全保密范围。

- 验收阶段：
  - 工程移交之前，统一修改调试用密码后提交客户；移交清单中涉及密码的移交内容，并要求客户自行修改后签字确认。
  - 工程内部和外部移交资料，只能交给指定的内部和外部接口人。
  - 该阶段中输出的遗留问题信息涉及客户商业机密，应纳入文档安全保密范围。
  - 该阶段中的输出文件涉及到项目名称、上线时间、商用时间等敏感信息，应纳入文档安全保密范围。

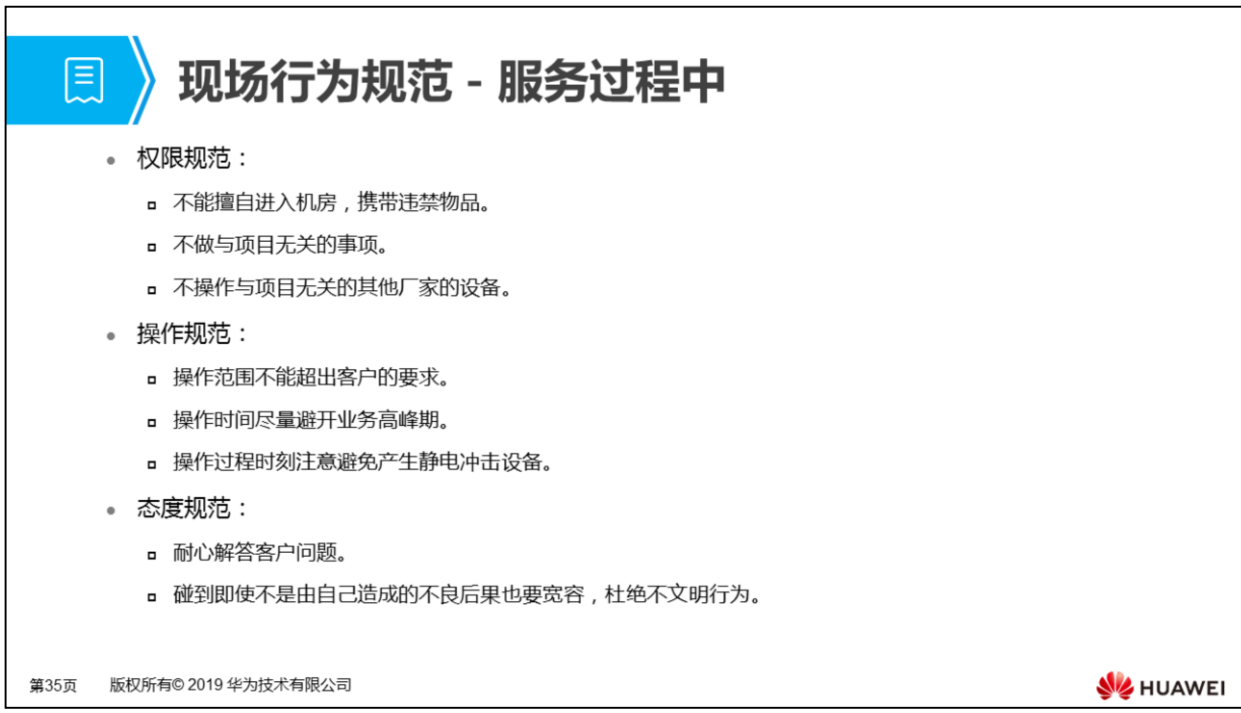


- 语言：
  - 言而有信，注意分寸，诚恳会谈，尊重对方，善于倾听，使用普通话，简练意明，注意场合。
- 仪表：
  - 着商务正装或商务休闲装，讲究个人卫生，举止文雅庄重，微笑示人。
- 举止：
  - 站立时抬头挺胸，走路莫摇晃，急事莫慌张；坐下时不要跷二郎腿，不可抖动双腿，不可仰坐在沙发或座椅上；守时赴约，遵守社会公德和当地习俗。
- 沟通：
  - 接听电话：应首先问好，然后通报自己的姓名，结束前主动说“再见”；电话用语礼貌、简练、声音适中；保证通讯24小时通畅。
  - 参加会议：开会时应认真听讲，发言人发言结束应鼓掌致意；发言应简短，观点应明确；礼貌作答提问，对提问人的批评和意见应认真听取，即使提问者的批评是错误的，也不应失态；中途退场应注意不影响他人。
  - 收发邮件：收件人、主题、发件人等要明确；给客户的邮件、传真中的用词应仔细斟酌，避免生硬、尖刻、不礼貌；涉及商务机密要考虑邮件的发送人员范围。

现场行为规范 - 行前准备

  HUAWEI

- 行前准备规范：
  - 收到现场服务任务后，请在出发前先做好相关准备，包括服务方案、操作步骤、工具、备件等，尽量避免到用户现场才临时查资料、翻文档、借工具、等候备件、打求助电话等情况。
  - 提前与客户确认安装/维护环境是否具备，产品及其配件是否齐备，避免到现场才发现无法实施服务的情况。
  - 提前与客户确认上门安装或维护时间，考虑交通堵塞等不可控原因，预约时间时向客户说明有半个小时误差。
  - 与客户确定了上门时间，就需要履行承诺，准时上门并带齐提供服务所必须的工具、备件等。
  - 严格按预约时间（提前3～5分钟）到达约定地上门服务，由于特殊原因不能守时的应该至少提前30分钟和客户解释清楚，并且明确告知客户到达时间。同时电话知会该项目的服务项目经理。



- 权限规范：
  - 进机房要征得客户同意，按照客户要求办理相关手续，出入机房所携带物品应严格登记。
  - 严格遵守用户的各项规章制度，如进机房是否带鞋套、是否穿着工作服等规定。
  - 不允许在客户现场处理与本次工作无关的事情，严禁在机房或办公场所抽烟、玩游戏、浏览与工作无关的网站，严禁在客户机房或办公场所睡觉。
  - 严禁擅自使用客户电话，如确实需要，需经客户同意后方可使用。
  - 禁止操作与本次服务不相关的设备，禁止操作其它厂家的设备。
  - 禁止向客户提供和安装非法来源的软件，如客户求助且确为业务需要安装其它非法来源的软件时，必须要求客户提供免责证明。
- 操作规范：
  - 对设备进行维护操作时，需经用户同意并要求客户陪同，原则上应使用客户给予的临时帐号和密码，禁止在用户面前使用超级密码和口令。原则上操作范围不能超过用户预先审批过的操作规程，如有额外操作，需向客户提出申请，并解释操作可能带来的影响。

- 进行设备操作时，应尽量注意避开用户业务高峰，用户业务敏感时间，并要求客户做好备份工作。
- 开机箱、操作面板、插拔板卡、控制器、硬盘等部件须做好防静电工作，如：穿防静电服、带防静电手腕带和手套。
- 备件更换完毕，坏件需要使用备件的包装包装好，有防静电袋必须将备件放入防静电袋。
- 在客户现场时，工程师必须严格遵守客户方的管理规范和管理制度，不准私自带走客户物品。

- 态度规范：
  - 在服务过程中，对于用户提出的任何问题，需要从专业的角度给用户做耐心的解释，决不允许对用户冷嘲热讽，不理不睬，在用户没有接受以前，只能耐心说服，决不能自作主张，若在现场解释不通，需要打电话向华为服务接口人或400热线反馈并等待处理结果。
  - 对于客户提出的技术咨询问题如果没有把握，切忌不能盲目随意的答复，可以先向客户说明“对不起，我对这个问题不太熟悉，待我了解后给您答复”，之后请联系华为400专家进行咨询，再将答复转告客户。
  - 需要留心客户提出产品功能、性能方面的问题，对于产品目前不具备的相关功能、性能，不能直接答复不具备，而应该首先联系华为服务接口人，协商如何答复。
  - 尊重客户，面对客户态度不好或出言不逊，要宽容、理解，无论如何不允许和客户发生争吵。如无法达成一致，请向华为服务接口人求助。
  - 如果在现场遇上陌生的情况和问题，请直接向华为400专家进行咨询或求助，不可盲目寻找其他非正规渠道的外援，也不可独自在现场采取非常规方法进行尝试，这可能导致客户对您的技术能力产生怀疑。

现场行为规范 - 服务结束



当面交接 → 确认离开 → 礼貌再见

HUAWEI

- 服务结束行为规范：
  - 如因客观原因导致项目暂时无法交付，离开现场时需要与客户、集成商、华为服务接口人当面或者电话沟通，留下联系方式，经过允许后方能离开。
  - 为客户服务完毕，应及时清理好服务现场，整理好各种物品，与客户当面交接相关物品和文档资料，并告知客户对产品后期的使用与维护保养的方法。最后请客户在《服务报告》上反馈意见并签字。
  - 离开时要求再次表示感谢（“谢谢，给您添麻烦了，再见。”、“很高兴为您服务。”、“如有问题，请随时拨打我们的售后服务热线电话。”）。

思考题

1. 项目交付流程的主要步骤有哪些？
2. 高危操作的三授权是什么？
3. 提醒客户的信息安全有哪些？

- 1、答案：项目启动会，方案制定，开箱验货（DOA流程），设备安装，质量自检，软件调试，转维培训，项目验收。
- 2、答案：管理授权，技术授权，客户授权。
- 3、答案：提醒对无用账号进行清理，提醒密码更新，提醒日志保护，提醒数据备份等。


谢 谢
www.huawei.com

网络维护

HUAWEI

前言

- 要保证网络各项功能正常运行、从而支撑用户业务的顺利开展，需要对网络进行日常的维护工作和故障处理，前者是预防性的有计划的维护工作，而后者则是基于事件触发的维护工作。
- 本课程将介绍日常维护的工作方法、规范和技巧。

目标

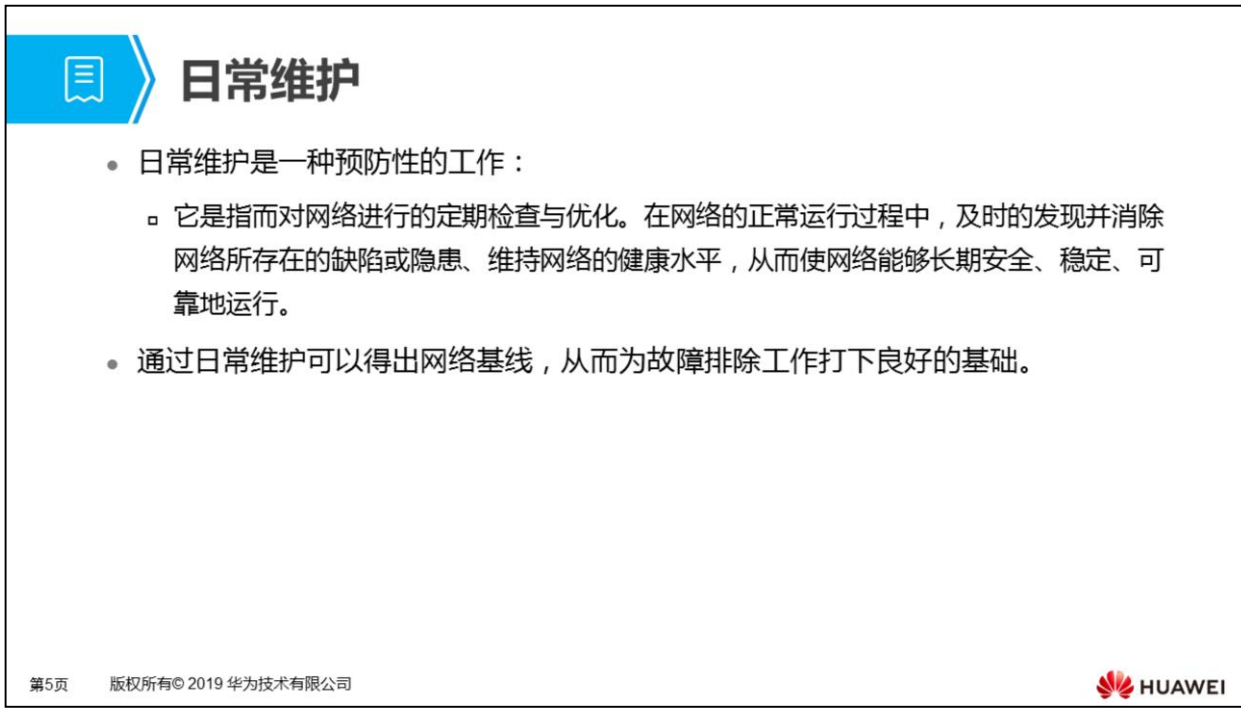
- 学完本课程后，您将能够:
  - 熟悉日常的维护任务
  - 熟悉使用网管软件进行网络维护
  - 掌握执行设备软件升级的方法
  - 熟悉例行维护报告的格式

目录

维护阶段 - 概述

- 运维阶段（Operate）的工作内容包括日常维护和故障排除：
  - 日常维护是例行的计划的工作。
  - 故障排除是事件驱动的工作。

- 项目验收以后进入维护阶段。根据事件触发原因的不同，运维阶段的任务可以分为两类：日常维护和故障排除。这两方面的工作并没有先后顺序。日常维护是例行的计划的工作；而故障排除则是事件驱动的工作。日常维护是为了预防问题发生，尽量减少突发的故障；从故障排除工作中找到的问题原因，可为日常维护工作提供参考，有一些问题的处理也可以合并到日常维护工作中（如为了避免网络设备操作系统bug引起的网络故障，可以定期进行系统软件升级）。维护阶段又有“运维”、“运营”、“操作与维护”等不同的叫法，但表达的是同一个概念。



- 日常维护是一种预防性的工作。它是指而对网络进行的定期检查与优化。在网络的正常运行过程中，及时的发现并消除网络所存在的缺陷或隐患、维持网络的健康水平，从而使网络能够长期安全、稳定、可靠地运行。建议根据网络现状建立日常维护制度，确保网络维护有序、规范的进行。
- 网络的维护不仅仅是技术问题，而且也是管理问题。日常维护对操作人员的技术要求不高，但对操作的规范性要求比较高。
- 通过日常维护可以得出网络基线（是指网络在正常情况下的各种参数，包括网络设备、网络性能、网络安全等各种参数），从而为故障排除工作打下良好的基础。

日常维护 - 内容和方法

- 现场观测
  - 观察设备硬件运行环境。
- 远程操作
  - 了解设备软件运行情况。

```
[AR3260]display current-configuration
[V200R003C00]
#
 sysname AR3260
#
 snmp-agent local-engineid
800007DB03000000000000
 snmp-agent
#
 clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load portalpage.zip
#
 drop illegal-mac alarm
#
 set cpu-usage threshold 80 restore 75
#
```


- 日常维护分为设备环境维护和设备软件维护两大部分。
  - 设备硬件运行环境：
    - 硬件运行环境是指设备运行的机房、供电、散热等外部环境，这是设备运行的基础条件。
    - 对于设备环境的维护，工作人员需要亲临现场，甚至借助一些专业工具进行观察、测量。
  - 设备软件运行情况：
    - 设备软件运行情况与设备运行的具体业务密切相关。华为数通设备使用了通用的VRP平台，网络工程师应该掌握VRP平台的常用维护命令。
    - 对于设备软件的维护，工作人员可以现场操作，也可以远程操作，主要通过设备的display命令实现。

日常维护 - Checklist

Checklist

- 应针对各项操作整理一份操作清单（Checklist）。

HUAWEI

- 日常维护工作是有计划的例行工作，因此，针对各项操作整理一份操作清单（Checklist）是十分必要的。
- 不同网络设备的Checklist可以参考相应的产品文档。

设备环境检查

设备环境检查表

No.	检查项	方法/工具	评估标准和说明	检查结果	备注说明
1	设备位置摆放是否合理、牢固	观察	设备应放在通风、干燥的环境中，且放置位置牢固、平整。设备周围不得有杂物堆积。		
2	机房温度状况	观察/温度计	通常要求机房长期工作环境温度：0℃～45℃；短期工作环境温度：-5℃～55℃。 注意：不同设备可能有所差异，以各自产品文档为准。		
3	机房湿度状况	观察/湿度计	通常机房的长期工作环境相对湿度应在5%RH～85%RH之间，不结露；短期工作环境相对湿度应在0%RH～95%RH之间，不结露。 注意：不同设备可能有所差异，以各自产品文档为准。		
4	机房内空调运行是否正常	观察/空调	空调可持续稳定运行，使机房的温度和湿度保持在设备规定范围内。		
5	清洁状况	观察	所有项目都应干净整洁无明显尘土附着。 注意防尘网的清洁状况，及时清洗或更换，以免影响机柜门及风扇框的通风、散热。		

- 重点关注温度、湿度、清洁等状况。
- 发现情况应及时记录和反馈，疑难问题请专业人士处理。
- 建议执行周期：每天。

- 设备运行环境正常是保证设备正常运行的前提。
- 温度和湿度对设备正常运行有重大影响，标准的机房都应该配备温度计和湿度计，并且应每天安排人员例行检查和记录。
- 机房的清洁和整齐也影响着设备的正常运行。
  - 清洁问题影响设备的散热。
  - 整齐主要是指设备、线缆的布放。按照规范的安装部署要求，设备和线缆都需要规范布放。但是在网络运行过程中，时常会有临时的调整，比如临时跳线测试。这些活动积累一段时间后，机房就会变乱。设备环境检查就是发现这些问题并及时纠正。
- 另一方面，非标准的机房更要注意设备环境检查，比如楼层的设备间，需要特别注意清洁和散热问题。

设备基本信息检查

设备基本信息检查表

No.	检查项	检查方法	评估标准	检查结果	备注说明
1	设备运行的版本	执行display version命令	单板PCB版本号、软件版本号与要求相符。		
2	检查软件包	执行display startup命令	检查下述系统文件名是否正确： - 当前启动大包名 - 下次启动大包名 - 备份大包名 - 配置、许可文件、补丁、语音的当前启动文件名和下次启动文件名		
3	License信息	执行display license命令 执行display license state命令	查看GTL License文件名、版本及配置项是否符合要求，确认是否需要升级。 - “Master board license state”项为“Normal”。“Master board license state”项为“Demo”或“Trial”时，确认License在有效期内。		
4	检查补丁信息	执行display patch-information命令	- 补丁文件必须与实际要求一致，建议加载华为公司发布的该产品版本对应的最新的补丁文件。 - 补丁必须已经生效，即补丁的总数量和正在运行的补丁数量一致。		

- 重点关注版本信息、启动信息、License信息、存储空间等。
- 发现情况应及时记录和反馈，查明原因，做好整改计划。
- 建议执行周期：每周/每月。

HUAWEI

- 关于设备运行的软件版本：
  - 设备运行版本在项目建设时就应确认，正常情况下版本信息不会变化。在检查过程中若发现版本信息有变化，应重点关注。这种情况通常是由于不规范的管理造成的。
  - 如果是新添加的设备，可能采用不同的软件版本；也有可能由于其他原因升级或降级了部分设备。特别是在网络规模较大的场景下，网络中同一款设备可能运行不同版本的软件。这时就需要重点关注不同版本是否能够满足同样的网络功能需求。
- 关于启动信息：
  - 设备上可能存在多个版本或多个配置文件，这种情况下冒然变更启动信息的会对网络的正常运行造成较大的风险。设备一旦重启（比如供电故障），则可能影响整个网络的运行。
- 关于License信息：
  - 不同设备的License规则可能不同，需要区别对待。某些设备的License是有期限的，需要重点关注。
- 关于存储空间：
  - 尽管大部分设备提供了数十G甚至数百G的存储空间，但是由于设备运行过程中会不断生成一些文件，如日志文件等。在某些异常情况下，如设备遭受攻击或设备信息频繁变更时，日志文件会急剧增加，如果这种现象持续存在，就可能会导致设备的存储空间耗尽、关键信息丢失。

设备运行状态检查

设备运行检查表

No.	检查项	检查方法	评估标准	检查结果	备注说明
1	单板运行状态	执行display device命令	重点关注单板在位信息及状态信息是否正常。 - 单板"Online"为"Present"。 - 单板"Power"为"PowerOn"。 - 单板"Register"为"Registered"。 - 单板"Alarm"为"Normal"。		
2	设备复位情况	执行display reset-reason命令（AR路由器和S系列框式交换机） 执行display reboot-info命令（S系列盒式交换机）	通过查看复位信息（包括复位时间、复位原因），确认无非正常复位。		
3	设备温度	执行display temperature命令（AR路由器、NE路由器和S系列框式交换机） 执行display environment命令（S系列盒式交换机）	对于AR路由器和S系列交换机，各模块当前的温度应该在上下限之间，即"Temperature"的值在"Upper"和"Lower"之间。 对于NE路由器，如果Temp(C)长时间高于Minor则需要检查设备的运行环境（如空调、通风口、防尘网等）。		

- 重点关注告警信息，板卡、电源、风扇、温度、CPU、内存等。
- 发现情况应及时记录和反馈，设备硬件问题及时联系供应商处理。
- 建议执行周期：每周/每月。

HUAWEI

- 在进行设备运行状态检查时，重点关注设备硬件的运行状态，如板卡、电源、风扇、温度、CPU、内存等。一般设备上都设置了告警灯，通常硬件故障都会导致告警灯亮（具体状态因产品而异）。因此，也可以通过现场观察发现设备运行异常状态。
- 对于板卡、电源、风扇等部件的运行状态，应遵照厂商的相关指导进行判断，有必要时联系厂商进行指导。如果确认为硬件故障，可以联系供应商处理（由于不同项目、不同设备的维保方案不同，有的硬件故障可直接联系厂商更换，有的则需要联系供应商协助处理）。

设备端口内容检查

端口内容检查表

No.	检查项	检查方法	评估标准	检查结果	备注说明
1	接口错包	执行display interface命令	业务运行时，要检查接口有无错包，包括CRC错包等。		
2	端口协商模式	执行display interface命令	端口协商模式正确，两边端口要一致，不能有半双工模式。		
3	接口配置	执行display current-configuration interface命令	接口的配置项合理，如接口双工模式、协商模式、速率、环回配置等。		
4	接口状态	执行display interface brief命令	接口的Up/Down状态满足规划要求。接口的收发流量是否过大？（长期超过70%）		
5	PoE供电	执行display poe power-state interface interface-type interface-number命令	PoE供电状态正常，"Port power ON/OFF"为"ON"的接口，其"Port power status"为"Delivering-power"。		

- 重点关注错包统计、双工模式、流量统计等。
- 发现情况应及时记录和反馈，异常情况及时分析原因。
- 建议执行周期：每周/每月。

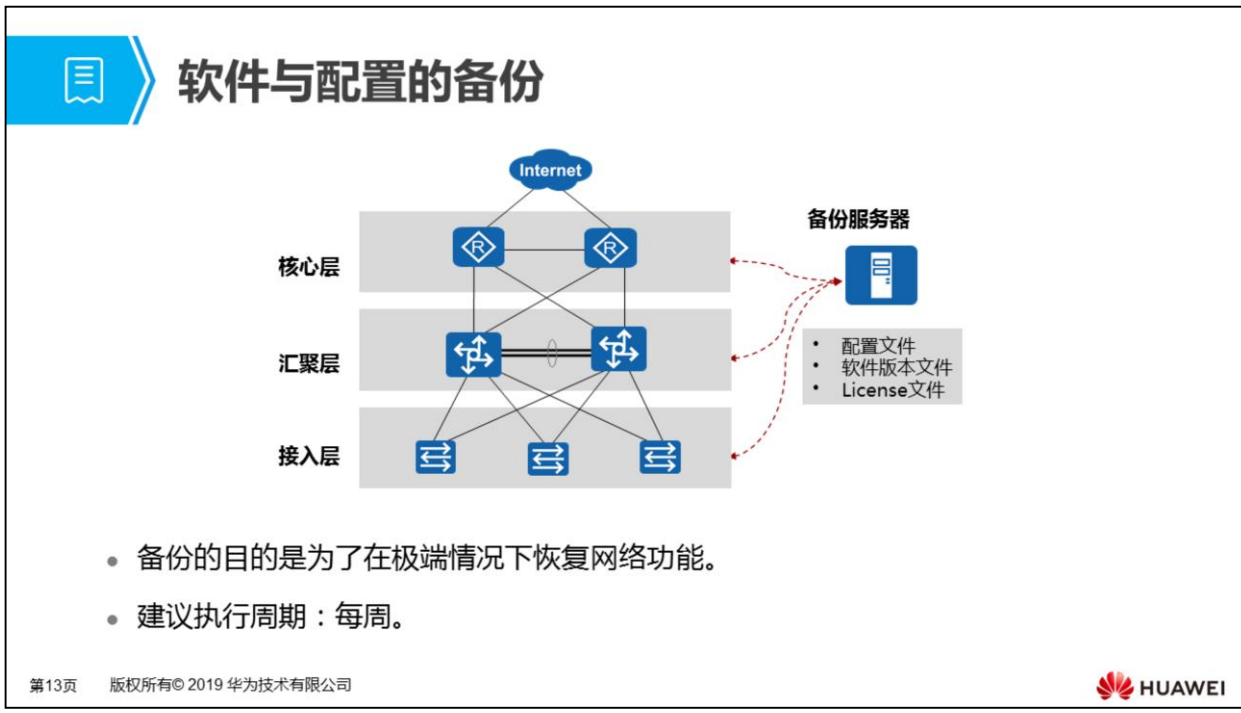
- 网络设备通过端口来交换数据报文。因此，端口的信息非常重要。端口状态异常会影响到网络的功能。
- 端口如果出现大量错包，并且在短时间内不断增加，通常是由于链路（包括物理端口）的问题造成的。

业务运行状态检查

业务检查表					
No.	检查项	检查方法	评估标准	检查结果	备注说明
1	组播成员接口和路由器接口	<HUAWEI> display igmp-snooping port-info	静态成员接口、动态成员接口、静态路由器接口和动态路由器接口的信息正确。		
2	组播报文统计信息	<HUAWEI> display igmp-snooping statistics vlan	VLAN接收/发送的IGMP报文和PIM Hello报文个数，以及所有VLAN内发生的二层事件次数统计合理。		
3	组播转发表信息	执行display l2-multicast forwarding-table命令查看二层组播转发表项。 执行display multicast forwarding-table命令查看三层组播转发表项。	组播转发表项正确。		
4	组播路由协议	执行display multicast routing-table命令。	域内组播路由协议采用PIM-SM。 与组播相连的接口都必须要使能IGMP。		
5	DHCP Snooping绑定表	<HUAWEI> display dhcp snooping user-bind all	静态表项和动态表项正确。		
6	MAC地址表信息	<HUAWEI> display mac-address	MAC地址表信息正确。		

- 重点关注与实际运行的业务相关的内容，如组播、OSPF、BGP等。
- 发现情况应及时记录和反馈，对异常情况及时分析原因。
- 建议执行周期：每周/每月。

- 业务运行状态主要是指网络协议的运行状态。这就与具体的业务相关。如通常规模稍大的网络会启用OSPF等路由协议，大规模路由型网络会使用BGP路由协议，总之根据具体部署的业务来设置Checklist。
- 不同的协议都有自己的状态机制，比如正常情况下两台使用OSPF互通的路由器，其OSPF邻居关系应该维持在FULL状态；如果使用BGP，那么邻居关系应该维持在Established状态等。

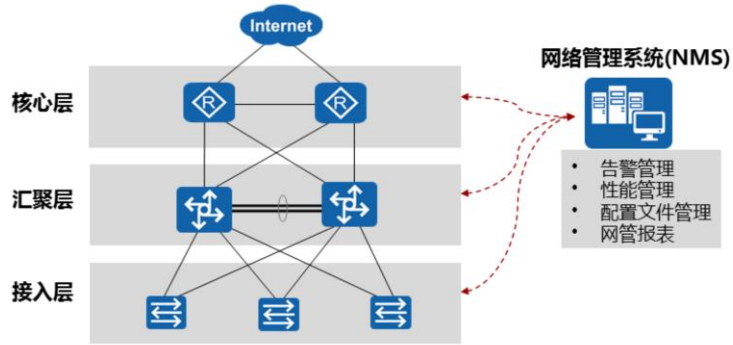


- 软件与配置（包括License文件）都需要备份。备份的目的是为了在极端情况下恢复网络功能。
  - 当设备因硬件故障无法启动，或更换同型号的设备后，如果没有备份的配置文件，业务将很难快速恢复。
  - 软件版本也有必要备份，但同一个产品、同一个版本只需要备份一次即可；也可以从厂商官网获取对应的版本文件保存到本地。
  - License文件是一类特殊的文件，它针对具体的产品进行了设置，一旦意外丢失（如误删除），则需要经过厂商的流程重新申请，通常这个流程需要提供一些证明材料（如合同号，设备SN等），因此申请周期也会比较长。如果有备份的License文件则可以快速地恢复到设备上。
- 备份的实质是把对应的文件传输到备份服务器上，因此方法有很多。通常将设备作为FTP或TFTP客户端，通过命令行将相应的文件传输到服务器上。
- 对于配置文件的备份，建议每周例行进行；同时在设备的配置有变更之前，应进行配置文件的备份。

目录

HUAWEI

网管系统（以华为eSight网管软件为例）

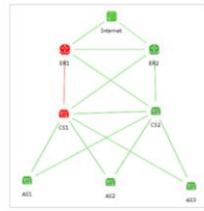


- 日常维护有大量重复简单的工作，可以通过网管软件来提升工作效率。

HUAWEI

- 大部分软件操作都可以通过网管软件来完成。
  - 告警管理功能：如设备端口的UP/DOWN变化，可以通过TRAP消息立刻反馈给网管软件。能够及时发现网络故障。
  - 性能管理功能：如设备CPU/内存的占有率，网管软件可以自动进行例行搜集和统计。可以辅助分析网络性能瓶颈。
  - 配置文件管理：进行配置文件的自动备份、比较、恢复等。可以自动批量的备份配置文件。
  - 此外网管还可以根据用户需求，定期输出报表，为网络优化参考。

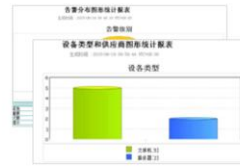
网管系统 - 常用功能



- 告警管理

- 性能管理

- 配置文件管理

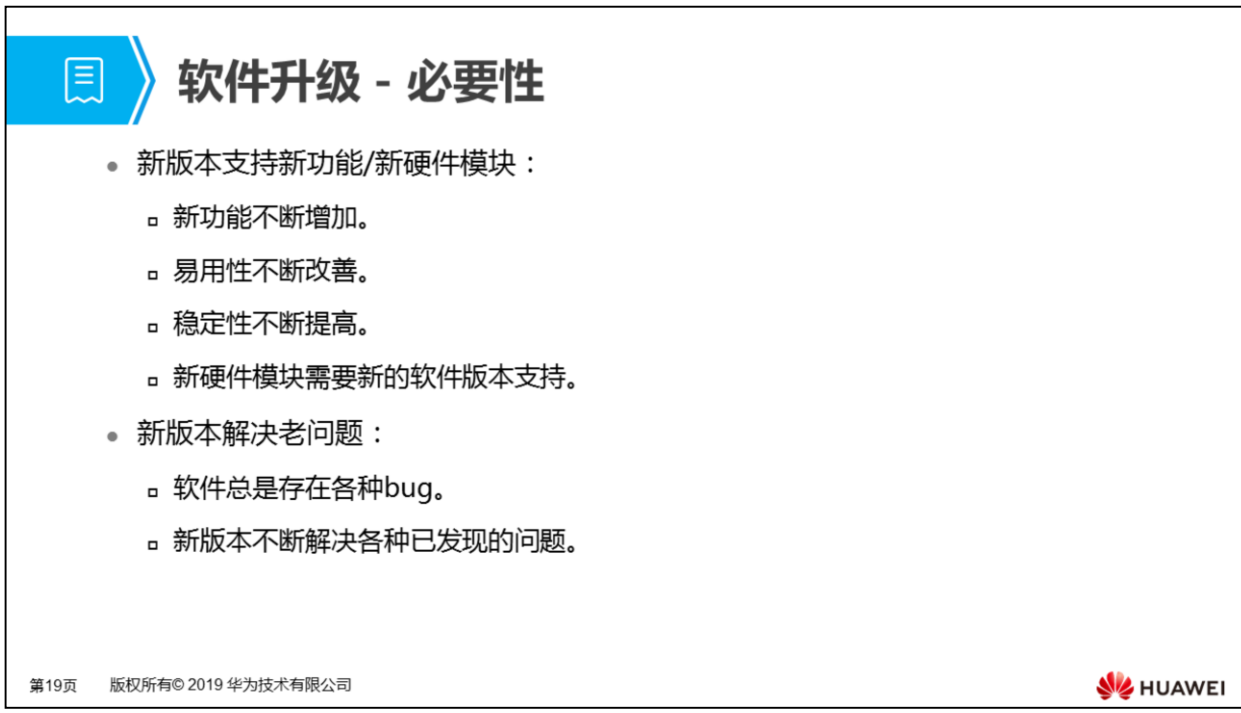


- 网管报表

- 告警管理：
  - 告警管理包含以下功能：
    - 通过全网告警监控、远程告警通知等方式，将故障信息第一时间通知给维护人员，从而保证故障处理的实时有效性。
    - 通过提供告警屏蔽、告警过滤、级别重定义等个性化定制功能，满足不同场景下的个性化需求。
  - 通过网管的高级管理功能，可以将全网设备的告警信息统一管理，并且能够直接将相应设备、端口的告警信息直观地体现在拓扑图上，极大地提升了工作效率。
  - 单个设备的单个告警可能被看作孤立事件，但是这些信息（多个设备同时发生的告警，或者同一设备在某一段时间内发生的一系列告警）一旦进行汇总处理（即网管告警管理），潜在的问题就很容易被发现，从而避免更大的网络故障发生。
- 性能管理：
  - 网络在正常运行过程中，内部与外部原因的影响都可能会导致网络性能的下降，进而引发网络的可用性故障。为保证当前网络的性能，并为网络未来的性能需求作准备，需要规划、监控与衡量网络效率，如通断率、利用率等。通过性能管理可以提前发现网络性能劣化的趋势，并在故障发生前主动排除隐患，规避网络故障风险。通过网管软件可视化的操作界面，能够对网络的关键性能指标进行监控，并对采集到的性能数据进行统计，从而方便用户对网络性能进行管理。
  - 通常，网管系统会预先设定关键性能指标的默认阈值，一旦超过阈值，便会给予用户警示。用户也可以修改这些阈值以满足实际业务的需求。通常需要经过一段时间的运行观察才能设定合适的阈值。

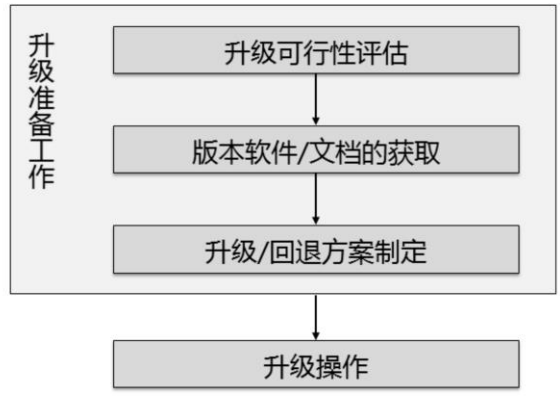
- 配置文件管理：
  - 配置文件管理指对设备的配置信息进行管理，提供对设备配置文件的导入、备份、恢复、比较、基线化管理等功能。当网络出现问题时，可以将之前备份的配置文件与当前设备的配置文件进行比较，从而快速定位并恢复当前出现的配置故障。同时，还可以进行配置变更管理。配置文件备份后自动进行差异比较，获取到配置变更信息后，可以通过软件告警与邮件通知到预先设定的联系人，从而使网络管理员即时的了解到网络的配置变更情况。
  - 使用网管对配置文件进行管理可以极大地提升日常维护的工作效率。
- 网管报表：
  - 以华为的eSight网管软件为例，可以通过执行报表任务来生成报表。eSight支持周期执行报表任务、手工执行报表任务；生成的报表支持导出为PDF、Excel、Word等常见文件格式。eSight预集成了丰富的报表模板，可以满足常见的网络运维报表需求。用户也可以自定义报表输出的内容和样式，从而满足定制化的业务需求。
  - 通过分析报表，用户在时间上和空间上对全网都可以有更好的了解和把控。
    - 时间上：可以对一段时间内指定的信息进行汇总和分析。
    - 空间上：可以对全网的信息进行汇总和分析。

目录



- 厂商在设计设备时，往往会采用比较领先的硬件架构，通过不断升级软件来完善/优化产品功能。
- 设备的功能由硬件和软件共同实现：
  - 设备的硬件特性相对固定；
  - 设备的软件特性则不断更新；
  - 设备的硬件特性是通过软件表现出来的。
- 虽然采用的新版本的软件有很多好处，但并不意味着新软件版本就比正在运行的版本好。只要当前版本能够支撑正常的业务运行，且没有重大安全隐患，就没有必要升级软件。建议在进行软件升级前咨询厂商或服务提供商的意见。

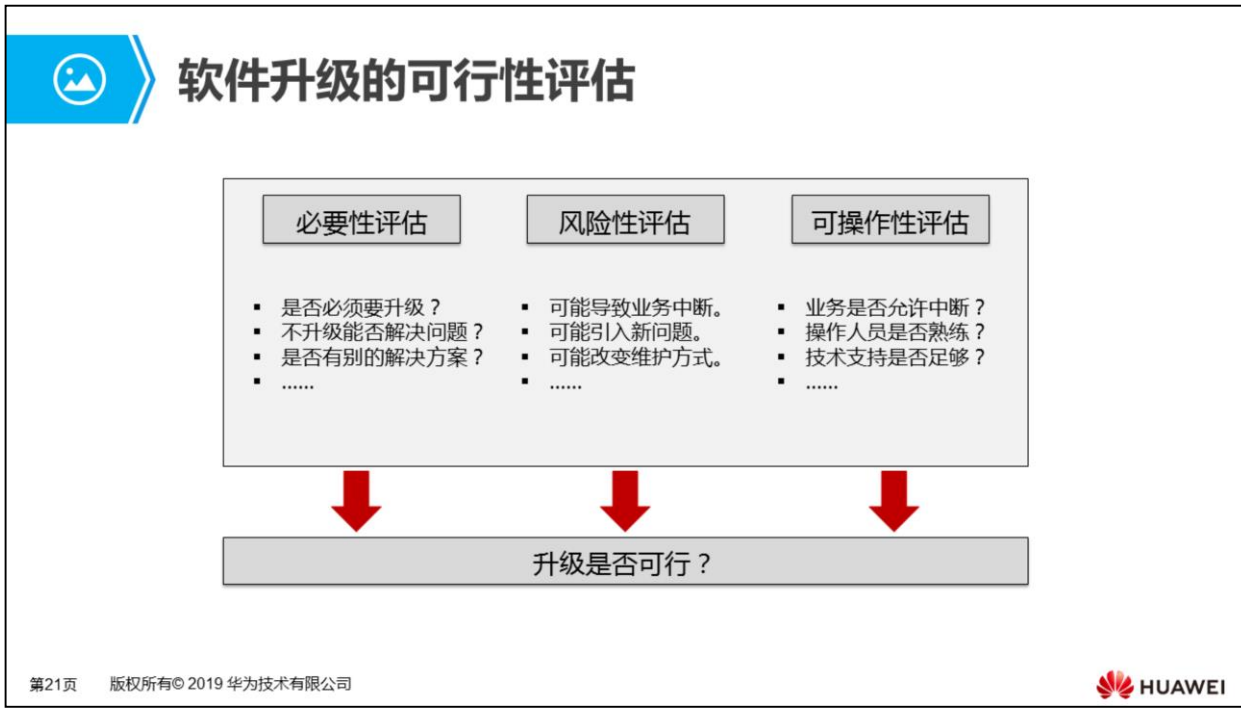
软件升级的准备工作



- 在软件升级前，必须做好充分的准备工作。

  HUAWEI

- 在网络设计和实施的时候，往往前期的设计工作做的越细致，部署工作就越简单。软件升级也类似，升级的准备工作做好了之后，就可以稳妥的按部就班的进行升级操作。
- 在软件升级前，必须做好充分的准备工作：
  - 评估软件分析的可行性，确定是否要升级软件；
  - 通过官方渠道获取软件拷贝及相关的说明文档；
  - 制定软件升级方案，包括回退的应急预案；
  - 最后执行升级操作。



- 为了保障网络设备的稳定运行，若非必要，不建议对设备软件进行升级。下述情况可考虑对设备进行软件升级：
  - 设备上新增了硬件模块而旧版本的软件不支持；
  - 业务有了新的需求，只有新版本的软件才能支持的所要求的新功能；
  - 旧软件版本存在不可规避的bug，只能通过软件升级来解决。
- 是否应该进行软件升级应该遵循厂家或服务提供商的专业建议。
- 设备的软件升级可能会对网络的稳定运行造成威胁，在升级前应做好充分的风险评估和风险规避措施。在评估风险时应从技术、业务等全方位进行考虑，并采取必要的风险规避措施；如果有不可规避的风险，则应寻求技术支持，而不应贸然执行软件升级操作。软件升级常见的风险有：
  - 新版本与旧版本存在特性差异，可能影响业务；
  - 软件升级需要重新启动设备，从而导致业务的暂时中断；
  - 软件升级过程中的错误操作导致设备无法启动。
- 软件升级的风险控制：
  - 在升级前咨询专业人员确定是否能升级；
  - 做好升级计划及准备好升级工具、软件；
  - 做好运行配置、License等的备份和回退计划。

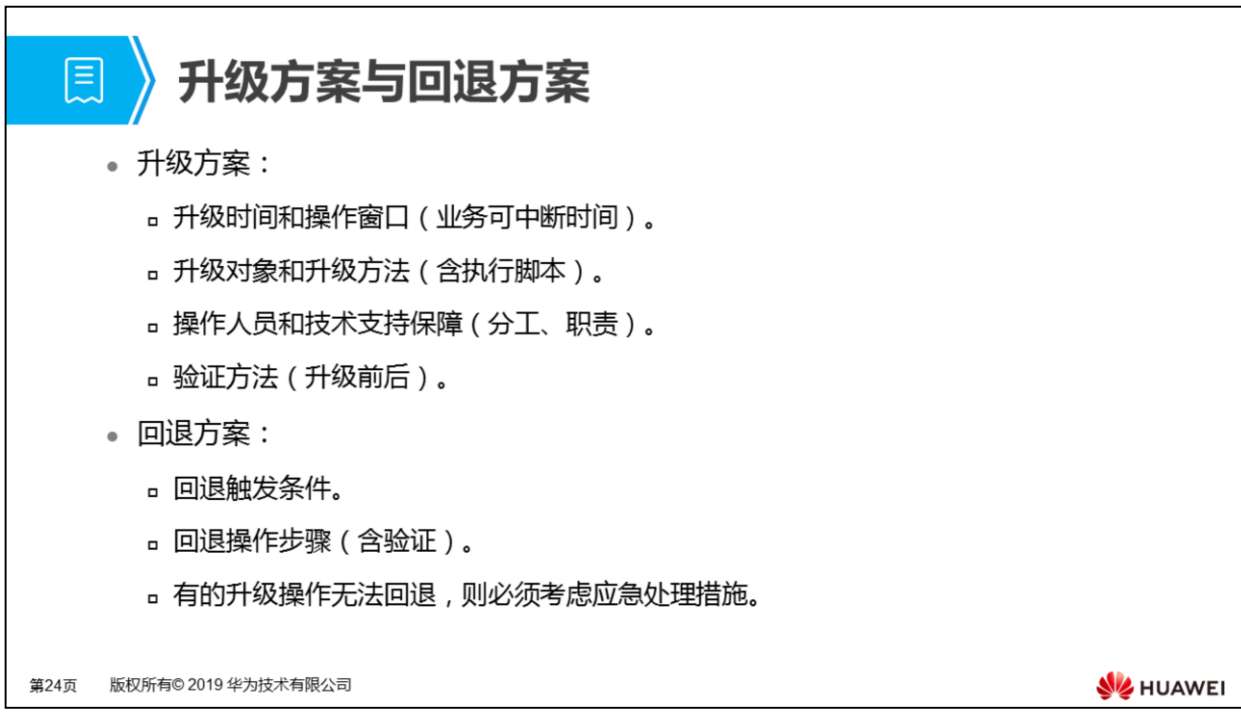
- 升级的可操作性是指在软件升级技术条件满足的情况下，执行升级操作的可行性。应该从用户的业务、运维人员的维护计划，操作者的技术水平、技术支持的保障力度等多方面考虑是否执行升级操作。设备的在线升级会影响到业务的正常运行，需要注意的事项有：
    - 升级可能导致短暂的业务中断，升级前应与用户确认是否能接受业务中断；
    - 升级后可能会造成设备操作方式的变化（如命令行变化），应确认是否能接受这样的变更；
    - 根据升级的重要性和复杂程度，操作者应有能力处理升级过程中的突发事件；
    - 在执行升级操作时，应协调相关的技术支持人员进行支持保障；
    - 如进行重大或较复杂的升级操作，应预先在模拟环境中进行调试和升级方案、应急预案的测试。

获取设备软件和升级指导文档

- 通常可以从网络设备厂商的网站上获取到较新版本的软件。

HUAWEI

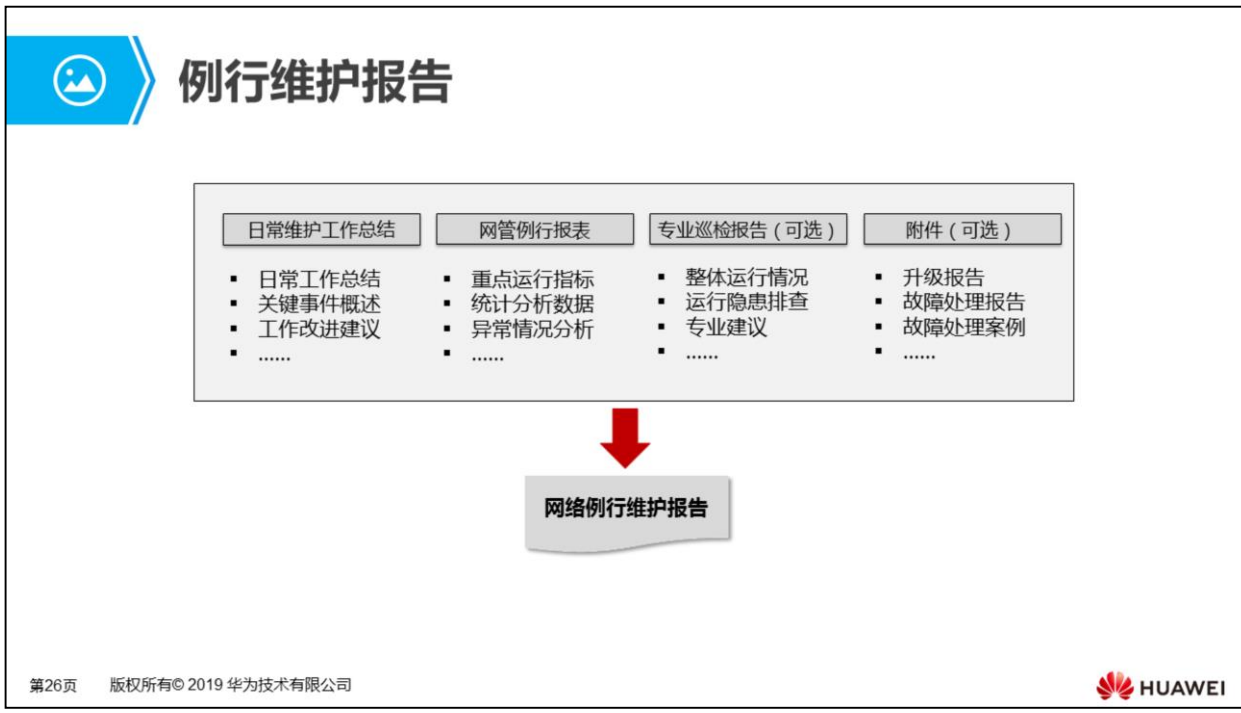
- 通常可以从网络设备厂商的网站上获取到较新版本的软件。以华为设备为例，可以在华为网站下载到最新的设备软件和配套的资料文档，一般包括：
  - 版本升级指导书。用于指导升级操作，通常华为数通产品的操作步骤都是类似的，但也不排除有例外情况，所有在执行软件升级前应仔细阅读版本升级指导书。
  - 版本命令、告警、MIB变更说明。用于描述该版本命令、告警、MIB的变更。
  - 版本特性变更说明。用于描述产品特性和规格的变更。
  - 版本说明书。主要为版本的配套描述、版本遗留问题说明等。



- 升级时间和操作窗口：
  - 升级时间的安排通常由问题的紧急程度决定。在非紧急的情况下，应预留足够的准备时间；
  - 操作窗口由用户业务可中断时间确定，该时间必须大于升级操作的执行时间，同时要预留一定的排错时间。
- 升级对象和升级方法：
  - 升级的对象是指待升级设备的数量是多少、地理位置如何分布、当前运行什么版本的软件、支持哪些升级方式、是否可直接升级到新版本、是否可以远程操作等；
  - 升级方法的选择与升级对象密切相关。通常般采用命令行的方式在线升级。
- 操作人员和技术支持保障：
  - 确定由谁来执行升级操作。该操作员是否具备必要的技术能力；
  - 重复评估升级的关联风险，提前联系相关技术支持人员，如有必要，可成立技术支持保障小组。
- 在通过软件升级来排除故障的时候，需要进行验证：
  - 升级前需要先确定问题所在，并保证没有其他问题；
  - 升级后需要验证解决了老问题，并且没有引入新问题。

目录

HUAWEI



- 基于日常维护工作包括：
  - 日常工作的总结，比如日常的机房环境检查是否正常进行，发现异常情况是否做了正确处理等；
  - 对于关键事件，特别是影响业务的关键事件应重点表述；
  - 对于工作中遇到的问题总结出改进建议也是必要的，作为一名网络运维人员应该不断总结进步。
- 基于网管的报表：
  - 如果部署了网管软件，可以将网管软件生成的报表作为例行维护报告的一部分。
  - 网管软件虽然能够及时准确地输出统计数据，但是对数据的分析和判断仍然需要网络运维人员来执行。如当网管软件发现某些设备的CPU占用率较高时，通常无法判断直接原因，也无法给出进一步的运维建议。只有通过运维人员对这些统计信息进行综合分析后，才能定位根本原因（如是遭受攻击或性能不足），进而采取下一步措施（排除攻击源或考虑更换更高性能的设备）。
- 专业巡检工具：
  - 作为领先的网络设备厂商，华为提供专业的巡检工具，这些工具可以全面检查设备及网络的运行情况，并输出专业的报告。通过这些报告，可以即时发现网络运行中的隐患，提前规避故障。
  - 这类巡检方式通常是以专业服务的形式出现，需要单独购买。

思考题

1. 关于网络维护的作用，以下的说法正确的有哪些？

   A. 日常维护是一种预防性的工作。

   B. 通过日常维护可以得出网络基线，从而为故障排除工作打下良好的基础。

   C. 日常维护对操作人员的技术要求很高，但对操作的规范性要求不高。

   D. 网络的维护不仅仅是技术问题，而且也是管理问题。

- 1、答案：ABD。


谢 谢
www.huawei.com

网络故障排除综述

HUAWEI

前言

- 网络基础设施的平稳运行对于大多数现代企业来说都非常重要。由于网络故障而导致的业务中断常常意味着产出、利润和声誉的损失，因而PDIOI模型把网络故障排除作为其中一个重要的组成部分。

目标

- 学完本课程后，您将能够：
  - 掌握结构化的网络故障排除流程
  - 掌握以业务流量路径为核心的网络故障排除方法

目录

什么是网络故障？

- 网络故障是指由于某种原因而使网络丧失规定功能影响业务的现象。
- 从用户的角度出发，凡是影响业务的现象都可以定义为故障。

- 网络故障是指由于某种原因而使网络丧失规定功能影响业务的现象。
- 从用户的角度出发，凡是影响业务的现象都可以定义为故障。因而故障不一定只是设备问题，也有可能是系统或兼容性等问题。

网络故障的分类

现象 / 分类	告警	环路	业务不通	业务中断	业务瞬断	丢包	协议异常	协议震荡	路由异常
硬件类	√			√		√			
配置类		√	√				√		√
网络类		√	√	√	√	√	√	√	√
性能问题	√				√	√		√	√
软件类							√		√
对接类		√	√				√		
其他	√		√	√	√	√			

- 网络故障可以分为硬件类、配置类、网络类、性能问题、软件类、对接类以及其他故障。不同的网络故障所引起的异常现象如表所示。

PDIOI与网络故障排除

- Operate:
  - 日常维护
  - 故障排除

- 网络故障排除是PDIOI中维护阶段（Operate）的重要工作。
- 日常维护的目的是预防故障发生；故障处理是指在故障发生之后，采取措施，使系统尽快恢复正常。
- 故障处理是事件驱动的工作任务，通常会比较突然地出现，对工程师的技术能力也提出了更高的要求。
- 尽管良好的日常维护可以规避大量的突发故障，但是由于网络运行受到多方面条件限制，再好的日常维护也不可能完全避免突发故障的发生。因此网络维护人员具备关键的技术，并掌握故障处理流程和方法是非常必要的。

目录

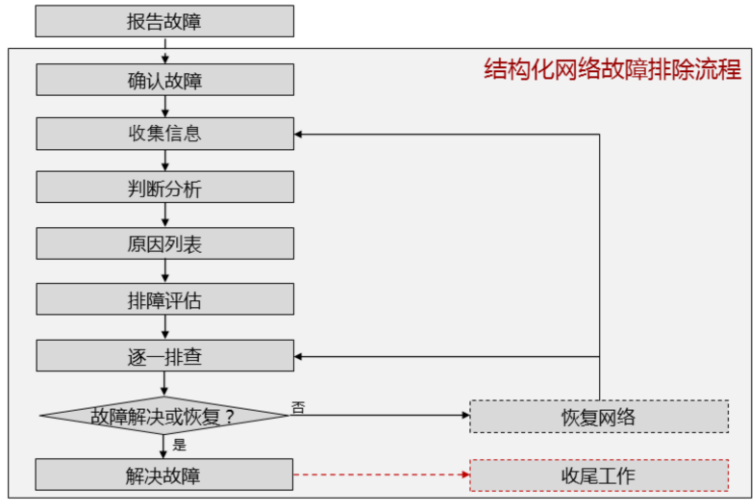
问题的提出

- 凭直觉或个人经验采取网络故障排除措施：
  - 难于进行团队协作。
  - 没有故障排除工作的文档总结。
  - 无法保证故障排除工作的连续性。

HUAWEI

- 只是凭直觉或个人经验采取网络故障排除措施，虽然最终也可能找出解决方案，但很难将排障工作转交给其他人，不利于团队协作。已经实施过的排障结果也可能遗忘或丢失。甚至过了一段时间，该人员再次检测与排除同样的故障时都有可能无法继续下去。

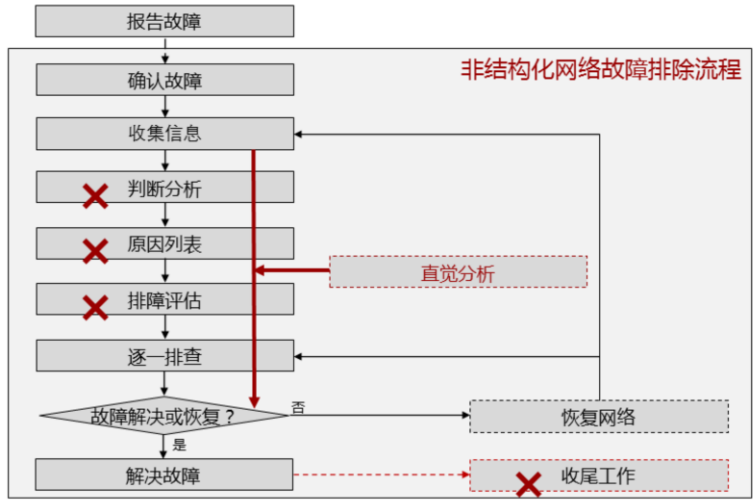
结构化的网络故障排除流程



HUAWEI

- 结构化的网络故障排除流程由报告故障触发，是合理地一步一步地找出故障原因，并解决故障的总体流程。基本步骤是确认故障、收集信息、判断分析、原因列表、排障评估、逐一排查、解决故障，其基本思想是系统地将故障的所有可能原因缩减或隔离成几个小的子集，从而使排障的复杂度迅速下降。
- 排除了故障之后，还需要进行收尾工作，如输出故障处理报告，向相关部门汇报、通告故障处理情况等。

非结构化的网络故障排除流程



HUAWEI

- 如果采取非结构化的网络故障排除流程，就只是凭直觉在这些步骤之间重复执行，虽然最终也可能找到解决故障的方法，但没有办法保证效率。
- 在复杂的网络环境中，有可能会由于非结构化的网络故障排除流程而导致新的故障，从而使网络故障的排除变得更加困难。

报告故障

- 周一上午你接到一名公司员工的故障申报电话，内容是“无法通过PC访问互联网，希望尽快解决问题。”

- 接到这个电话，你需要做什么？

报告故障 - 主动沟通确认

故障报告者	姓名、所在的部门、职位级别、所负责的工作内容、使用电脑的位置（楼层、房间、无线接入还是有线接入）、在使用电脑访问什么网站时发现的问题。
故障频率	故障是突发的、偶尔的、还是频繁的。
用户操作	出现故障之前和之后，用户对自己的终端做了哪些操作，如是否更改了IP地址和DNS、是否安装了桌面防火墙软件、安全控制软件等。

- 在电话里询问用户上面的内容，并记录在排障报告中。

- 网络故障排除通常是从用户报告故障开始的，而用户报告故障主动提供的信息经常是模糊、笼统的，所以需要进行主动沟通、确认。

报告故障 - 预先推测

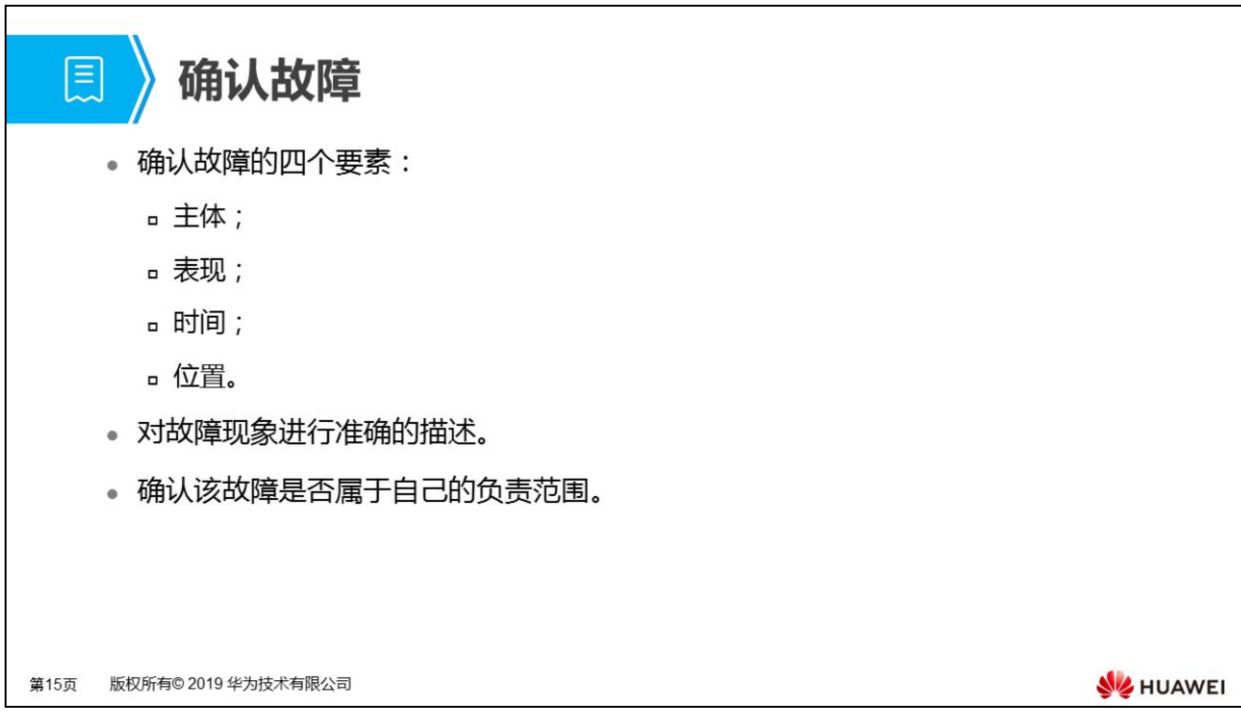
- 思考：
  - 为什么需要了解用户的职位级别、工作内容等信息？
- 答案：
  - 在企业环境中，不同级别的用户可能会有不同的网络访问权限。即使相同级别的用户，可能也只有权限使用自己工作内容相关的网络服务。

为什么要确认故障

- 用户的描述可能是含糊不清的，报告的故障也不一定是真实的故障点，所以需要有经验的工程师进行确认故障的工作。

  HUAWEI

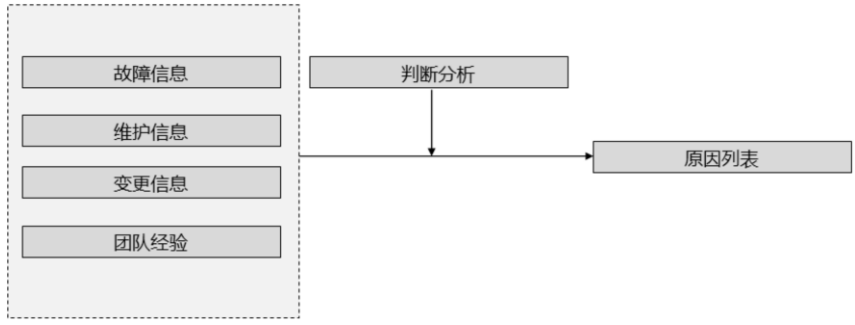
- 以图中所示的一个最简单网络环境为例，用户可能会报告说：“服务器出故障了，因为现在我无法访问它”，而真实的情况可能是某条链路的故障而导致服务器无法访问。



- 确认故障需要了解这些信息，确定故障现象：
  - 故障的主体：哪个网络业务出现了故障；
  - 故障的表现：故障的现象是什么样的；
  - 故障的时间：用户是什么时间发现的故障，以及专业人员推测的故障出现的真实时间；
  - 故障的位置：哪个网络组件出现了故障；
- 应对故障现象进行准确描述。
- 最后应确认该故障是否属于自己的负责范围，即自己是否被赋予了相应的权限来处理该故障。

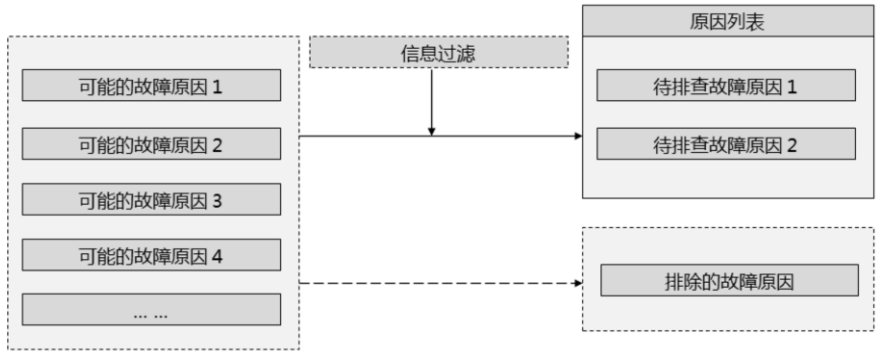
- 需要收集哪些信息：收集信息阶段主要是收集与故障相关的信息，如文档、网络变更情况等。
- 如何收集这些信息：是使用设备自身的操作命令，还是需要使用到额外的信息收集工具，如抓包工具、网管软件等。
- 是否需要授权：在对信息安全要求较高的网络环境中，对信息的收集是需要得到授权的，有时需要签署书面的授权文件。
- 收集信息阶段的风险评估：有些收集信息的操作，如对路由器或交换机执行“debug”命令，会导致设备的CPU占用率过高，严重的情况下甚至会使设备停止响应用户的操作指令，从而引入额外的故障现象。所以在收集信息的时候应评估这些风险，平衡引入新故障的风险与解决现有故障的紧迫性之间的关系，并明确的告知用户这些风险，由用户来决定是否进行风险较大的信息收集工作。

判断分析



- 判断分析阶段是对收集到的信息进行分析整理。
- 通过对故障信息、维护信息、变更信息的汇总，结合团队经验（或个人经验）进行综合的判断和分析，得到可能导致网络故障的原因列表。

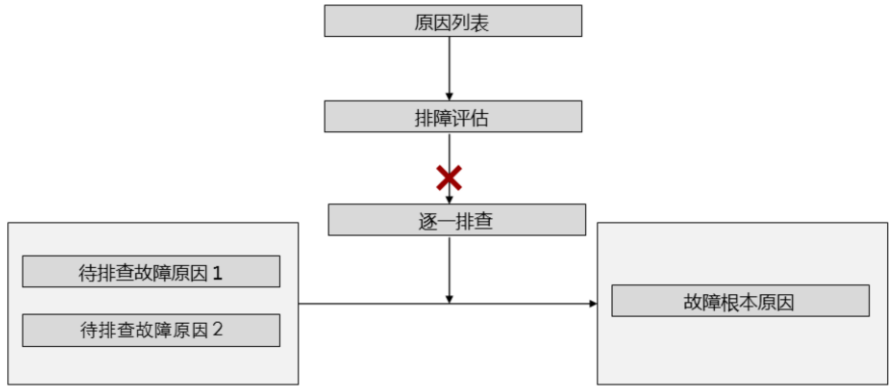
原因列表



HUAWEI

- 在原因列表阶段，首先需要列出所有可能的故障原因，然后通过信息过滤，列出最可能的待排查故障原因，同时排除掉当前最不可能的故障原因，从而缩小故障的排除范围。

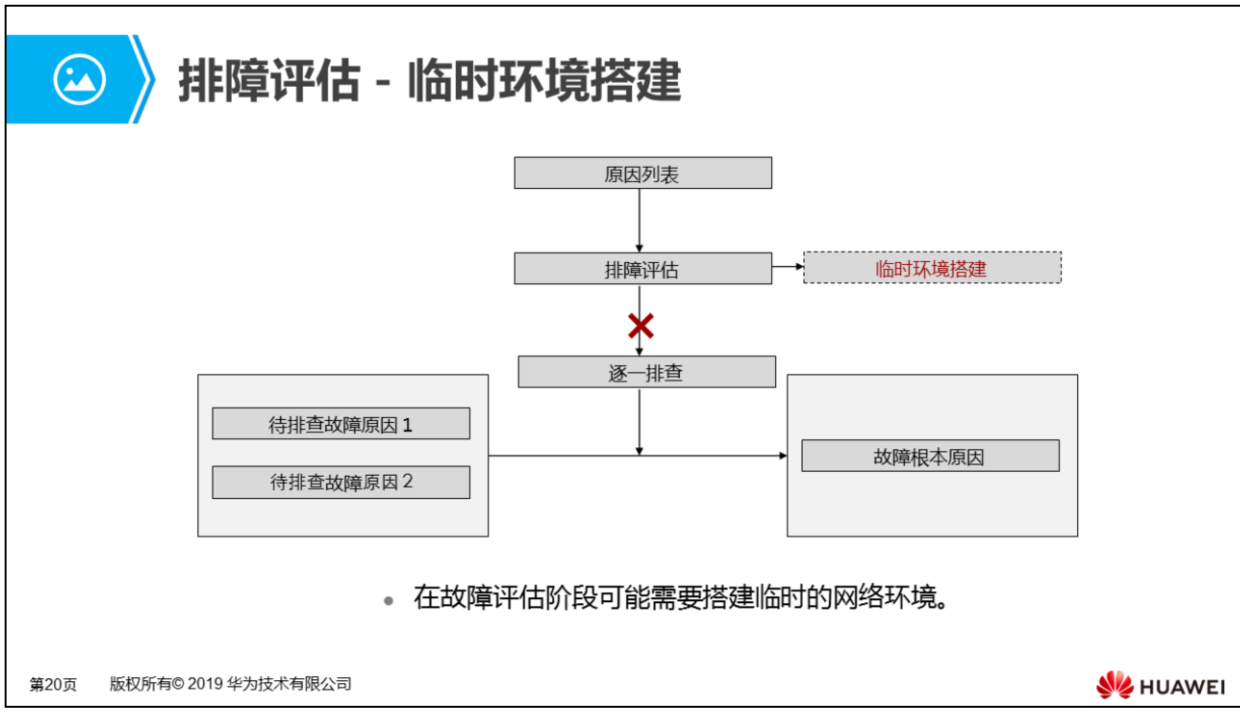
排障评估



- 需要在逐一排查前进行故障评估工作。

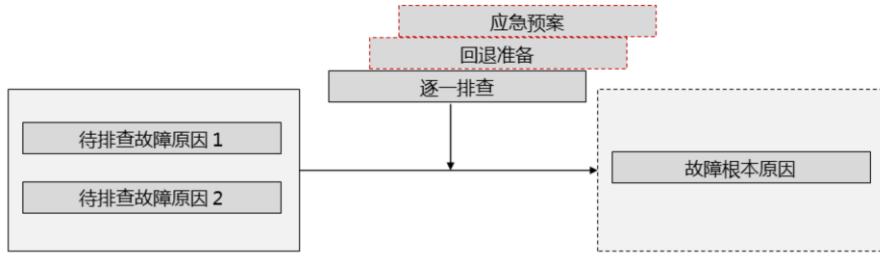
HUAWEI

- 列出待排查的故障原因清单后，应该首先评估故障排除工作的复杂程度（如排除网络故障的难度和所需解决时间等），而不是马上开始进行逐一排查。



- 对复杂的网络故障，如果经过评估认为短时间内无法排除故障，而用户又需要马上恢复网络的可用性，这时可能需要临时跳过故障节点，搭建替代的网络环境。
- 搭建临时网络环境的时候，应充分考虑到解决问题的迫切性与绕过某些安全限制措施的危险性，应与用户进行充分的沟通，明确必要的信息，并在得到许可的情况下才能执行。

逐一排查



- 逐一排查的过程可能涉及到网络变更。

- 在逐一排查阶段同样需要平衡解决问题的迫切性与引入新故障的风险性之间的矛盾。所以，应该明确告知用户排查工作可能带来的风险，并在得到许可的情况下才能执行操作。
- 有些情况下，通过逐一排查验证推断的过程涉及到网络变更，这时必须做好完善的应急预案和回退准备。

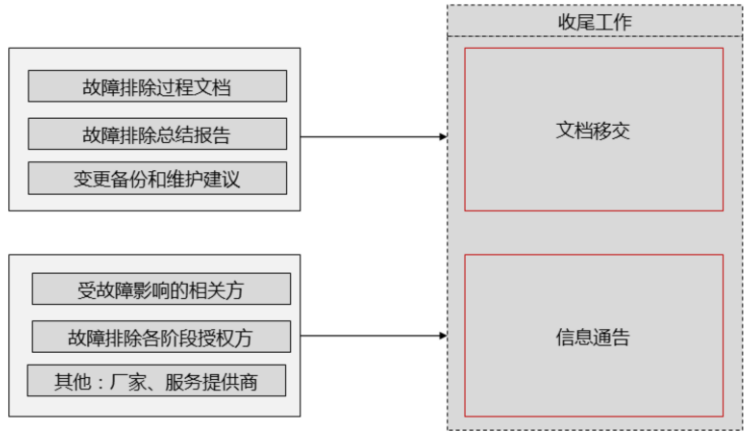
解决故障

- 有时解决故障后仍需要持续观察一段时间。

HUAWEI

- 如果通过逐一排查找到了故障的根本原因，并排除了故障，网络故障排除的流程就可以结束了。
- 复杂的网络环境中，故障现象消失后仍然需要观察一段时间，一方面确认用户报告的故障已经得到了解决，另一方面确认故障排除的过程中没有引入新的故障。

解决故障 - 收尾工作

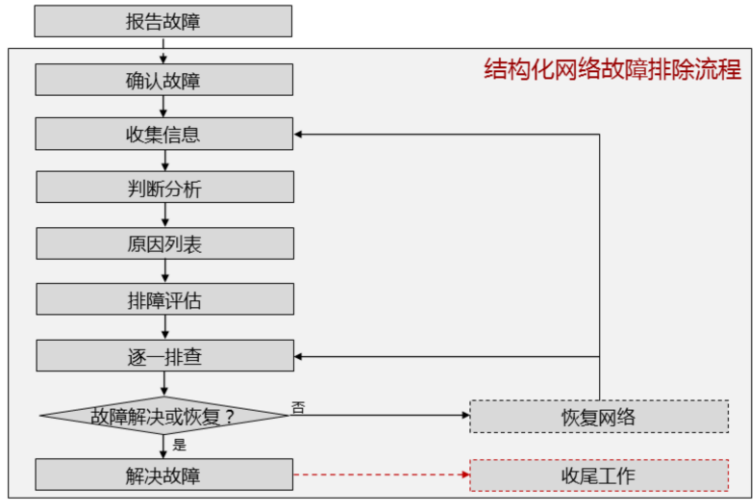


- 故障排除之后的收尾工作同样重要。

HUAWEI

- 收尾工作包括相关文档的整理、信息的通告等。需要对之前网络故障排除流程中所有进行了变更的配置或软件进行备份，并做好故障排除文档的整理和移交工作。为了避免同样的故障再次发生，在此阶段应该向用户提出改进建议。

回顾：结构化的网络故障排除流程



HUAWEI

- 相对于非结构化的网络故障排除流程来说，结构化的网络故障排除流程所产生的结果是可预期的，排障过程中所造成的影响是可控的，引入新故障的风险是可评估的。

目录

HUAWEI

TCP/IP参考模型与网络故障排除

- TCP/IP参考模型是网络故障排除的理论基础，OSI参考模型的物理层和数据链路层也是需要我们关注的。

HUAWEI

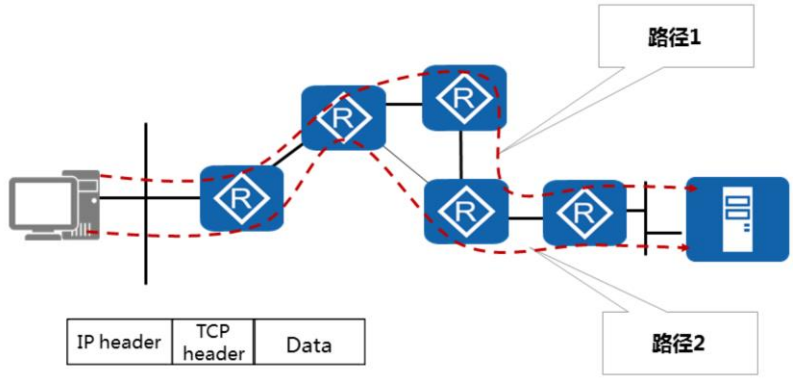
- TCP/IP参考模型是网络故障排除的理论基础，OSI参考模型的物理层和数据链路层（这两层对应于TCP/IP参考模型的网络接口层）也是需要我们关注的。推荐的故障排除方法是从TCP/IP参考模型的网络接口层和网络层分别确认并测试业务流量的路径，然后采用自顶向下法或自底向上法进行故障排除。

以业务流量路径为核心的故障排除思想

  HUAWEI

- 在复杂的网络环境中，网络故障排除该从何着手？
- 如图所示，在一个有着财务、OA（Office Automation System，办公自动化系统）、生产、甚至更多业务系统的复杂网络环境中，网络故障排除首先需要关注的是各业务系统的数据流方向。
- 在企业环境中，网络存在的作用即是服务于业务，只需要知道受到网络故障影响的业务的流量往返路径，跟踪此路径，逐步排除即可。
- 通常情况下，网络中业务流量的路径是在网络规划阶段就已经设计好的，在网络故障排除过程中可以首先向用户询问受影响的业务流量路径是如何规划的，然后使用ping和tracert工具进行测试，验证当前的业务流量路径是否与预期的业务流量路径相一致。

确认业务流量路径 - 网络层

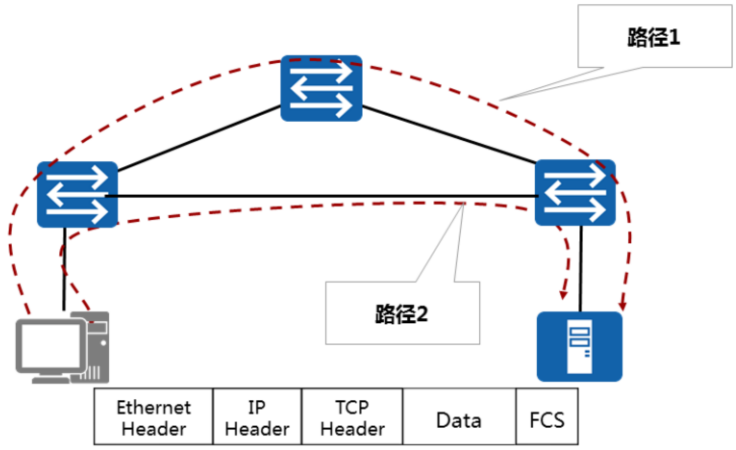


- 网络层确认业务流量路径需要了解报文是如何被路由的。

HUAWEI

- 在网络层，确认业务流量路径的工作内容是了解数据报文在网络中的可路由设备（路由器、有路由功能的交换机、防火墙等）上是如何被路由的。

确认业务流量路径 - 数据链路层



- 网络接口层确认业务流量路径需要了解数据帧是如何被交换机转发的。

HUAWEI

- 在数据链路层，确认业务流量路径需要了解数据帧是如何被交换机转发的。要确认数据帧在交换机之间的转发路径需要查看交换机上的MAC地址表、了解生成树协议收敛的情况，有时还需要抓包工具的协助。

自顶向下法

- 如果网络层的连通性没有问题，可以使用自顶向下法进行故障排除。

HUAWEI

- 在确认业务流量路径的过程中，同时也验证了网络层的连通性。
- 如果网络层的连通性没有问题，可以使用自顶向下法进行故障排除。即从应用层开始，对比相同应用的工作状态、检查是否存在应用层代理、应用层防火墙等导致故障现象的因素。

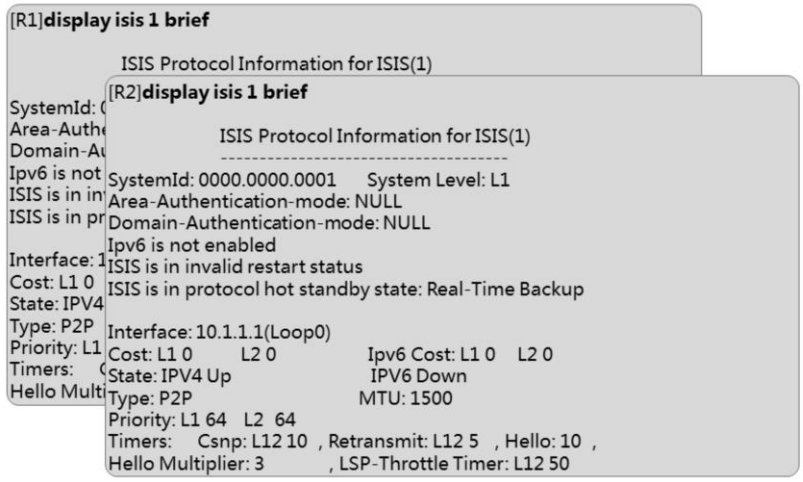
自底向上法

- 如果网络层的连通性有问题，可以使用自底向上法进行故障排除。

HUAWEI

- 如果网络层的连通性有问题，说明支持网络层的下一层或网络层本身可能存在问题，这时可以使用自底向上法进行故障排除。在物理层，检查是否存在网络线缆故障等问题；在数据链路层，检查是否存在二层环路故障、链路层协议不匹配等问题；在网络层，检查是否存在路由协议配置错误、防火墙过滤等问题。

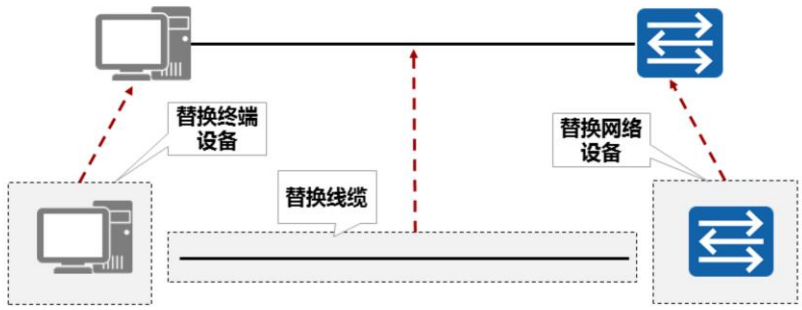
对比配置法



  HUAWEI

- 对比配置法是指对比正常状态与故障状态下的配置、软件版本、硬件型号等内容，检查两者之间的差异。
- 经验较少的网络故障排除人员在实践中会更多的使用到这种方法。

替换法



- 替换法是检查硬件问题常用的方法。

HUAWEI

- 替换法是检查硬件问题常用的方法。在没有条件收集到更多信息的环境下可以使用替换法隔离故障范围。
- 应用层也可以使用替换法。如财务部门的用户无法访问财务服务器，可以检查其他同部门的用户是否也存在同样问题。

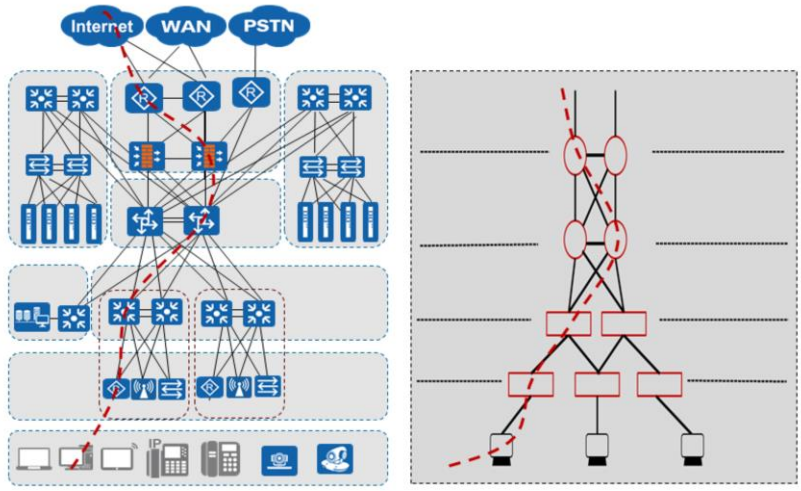
分块法

- 对网络设备的配置文件进行分块分析：

配置	内容
管理部分	路由器名称、口令、服务、日志等。
端口部分	地址、封装、cost、认证等。
路由协议部分	静态路由、RIP、OSPF、BGP、路由引入等。
策略部分	路由策略、策略路由、安全配置等。
接入部分	Telnet登录等。
其他应用部分	QoS配置等。

- 华为的交换机和路由器等网络设备的配置文件具有清晰的组织结构。这些网络设备的配置文件可包括如下部分：
  - 管理部分：路由器名称、口令、服务、日志等；
  - 端口部分：地址、封装、cost、认证等；
  - 路由协议部分：静态路由、RIP、OSPF、BGP、路由引入等；
  - 策略部分：路由策略、策略路由、安全配置等；
  - 接入部分：Telnet登录等；
  - 其他应用部分：QoS配置等。
- 当网络故障的排除范围已经缩小到某台具体的网络设备时，可以用分块法分析此网络设备的配置文件，从而进一步缩小故障的排除范围。

分段法



- 当排除大型网络环境中的网络故障时，可以基于受到故障影响的业务流量路径，使用分段法将故障的排除范围缩小。

思考题

1. 在结构化的网络故障排除流程的收尾工作中，下列哪几项是需要主要进行信息通告的相关方？

A. 受故障影响的相关方。

B. 故障排除各阶段授权方。

C. 厂家、服务提供商。

D. 对故障根源感兴趣的其他无关人员。

- 1、答案：ABC。


谢 谢
www.huawei.com

常见网络故障排除

HUAWEI

前言

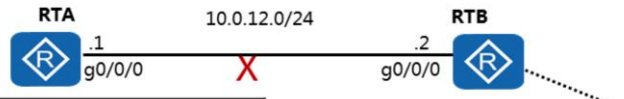
- 当网络发生故障时，最困难的不是修复网络故障本身，而是如何迅速地查出故障所在，并确定发生的原因。在本课程中，您将学习到常见网络故障的排除方法，掌握如何快速地查出问题的根源，从而排除故障，恢复网络的正常运行。

目标

- 学完本课程后，您将能够：
  - 掌握常见网络故障的排除方法。

目录

Telnet登录故障



序号	配置步骤
1	配置Telnet服务器功能及参数。
2	配置Telnet用户登录的用户界面。
3	配置Telnet类型的本地用户（AAA验证方式）。
4	从终端通过Telnet登录设备。

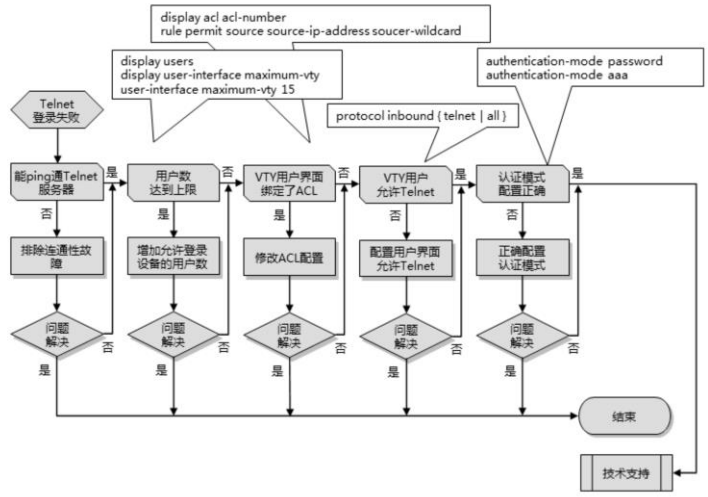
```
acl number 2001
 rule 5 permit source 10.0.12.1 0
 rule 10 deny #
aaa
 local-user admin1234 password cipher huawei
 local-user admin1234 privilege level 3
 local-user admin1234 service-type telnet
#
user-interface maximum-vty 8
#
user-interface vty 0 7
 acl 2001 inbound
 authentication-mode aaa
```

- 路由不可达，客户端和服务器无法建立TCP连接。
- 登录设备的用户数到达了上限。
- VTY用户界面下绑定了ACL。
- VTY用户界面下允许接入的协议不正确。如配置为protocol inbound ssh。

HUAWEI

- Telnet协议在TCP/IP协议族中属于应用层协议，通过网络提供远程登录和虚拟终端功能。以服务器/客户端（Server/Client）模式工作，Telnet客户端向Telnet服务器发起请求，Telnet服务器提供Telnet服务。设备支持Telnet客户端和Telnet服务器功能。
- 缺省情况下，用户不能通过Telnet方式直接登录设备。如果需要通过Telnet方式登录设备，可以先通过Console口本地登录设备，并完成以下步骤：
  - 确保终端和登录的设备之间路由可达。
  - 配置Telnet服务器功能及参数。
  - 配置Telnet用户登录的用户界面。
  - 配置Telnet类型的本地用户（AAA验证方式）。
  - 从终端通过Telnet登录设备。
- Telnet登录故障常见原因有：
  - 路由不可达，客户端和服务器无法建立TCP连接。
  - 登录设备的用户数到达了上限。
  - VTY用户界面下绑定了ACL。
  - VTY用户界面下允许接入的协议不正确。如配置为protocol inbound ssh时，使用Telnet将无法登录。

Telnet登录故障 - 排障流程

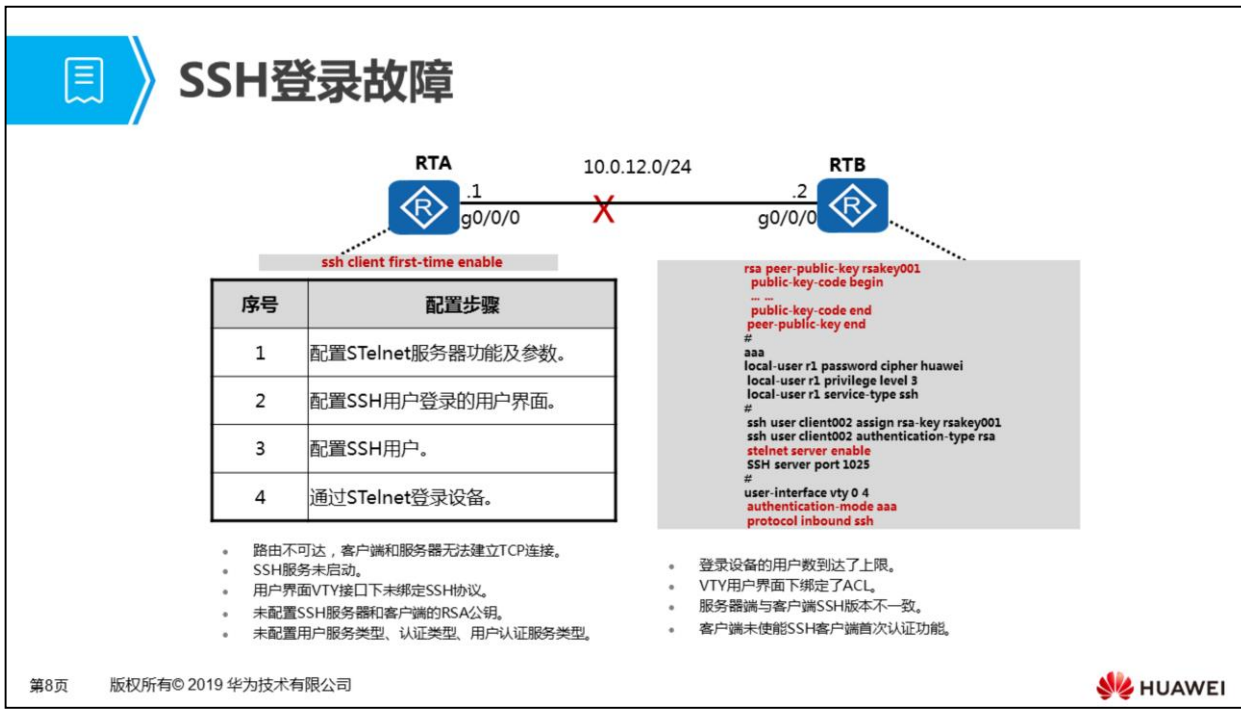


  HUAWEI

- 检查客户端能否Ping通服务器。
  - 在客户端使用ping命令查看网络连接情况。如果不能Ping通，则Telnet连接也将失败。
  - 如果Ping不通，应先排除客户端到服务器的连接性故障，使Telnet客户端能Ping通服务器端。
- 查看登录设备的用户数是否到达了上限。
  - 从Console口登录到设备，执行命令display users，查看当前的VTY通道是否全部被占用。缺省情况下，VTY通道允许的最大用户数是5个，可以先执行命令display user-interface maximum-vty，查看当前VTY通道允许的最大用户数。
  - 如果当前的用户数已经达到上限，可以执行命令user-interface maximum-vty 15，将VTY通道允许的最大用户数扩展到15个。
- 查看设备上VTY类型用户界面视图下是否配置了ACL。
  - 在Telnet服务器端上执行命令user-interface vty进入用户界面视图，执行命令display this，查看VTY用户界面是否配置了ACL限制，如果配置了ACL限制，请记录该ACL编号。
  - 在Telnet服务器端上执行命令display acl acl-number，查看该访问控制列表中是否deny了Telnet客户端的地址。如果deny客户端的IP地址，则在ACL视图下，执行命令undo rule rule-id，删除deny规则，再执行命令rule permit source source-ip-address soucer-wildcard，修改访问控制列表permit客户端的IP地址访问。

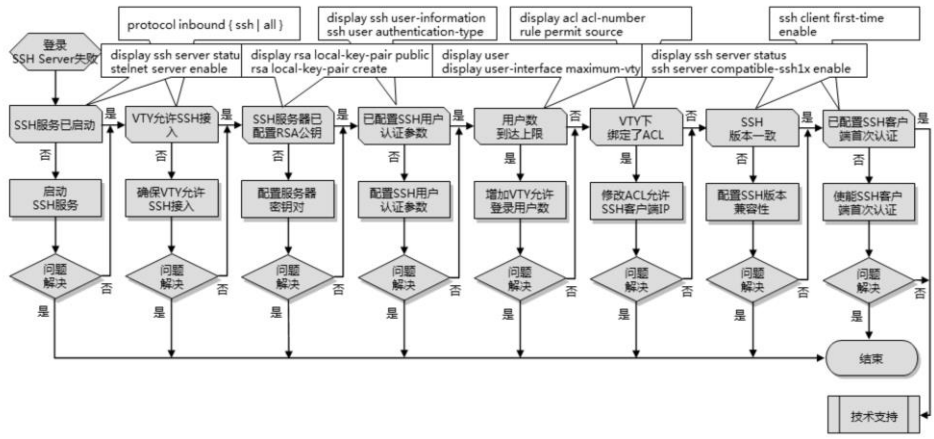
- 查看VTY类型用户界面视图下允许接入的协议配置是否正确。
  - 在Telnet服务器端上执行命令user-interface vty进入用户界面视图，执行命令display this，查看VTY用户界面的protocol inbound是否为telnet或者all（缺省情况下，系统支持协议SSH和Telnet）。如果不是，执行命令protocol inbound { telnet | all }修改配置，允许telnet类型用户接入设备。
- 查看用户界面视图下是否设置登录认证。
  - 如果使用命令authentication-mode password配置了VTY通道下的登录认证方式为password，则必须在登录时输入此密码。
  - 如果使用命令authentication-mode aaa设置认证方式为aaa，则必须使用命令local-user user-name password创建AAA本地用户。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
  - 上述步骤的执行结果。
  - 设备的配置文件、日志信息、告警信息。

目录



- Telnet传输过程采用TCP协议进行明文传输，缺少安全的认证方式，容易招致DoS（Denial of Service）、主机IP地址欺骗和路由欺骗等恶意攻击，存在很大的安全隐患。
- 相对于Telnet，STelnet基于SSH2协议，客户端和服务器端之间经过协商，建立安全连接，客户端可以像操作Telnet一样登录服务器端。
- 缺省情况下，用户不能通过STelnet方式直接登录设备。如果需要通过STelnet方式登录设备，可以先通过Console口本地登录或Telnet远程登录设备，并完成以下步骤：
  - 确保终端和登录的设备之间路由可达。
  - 配置STelnet服务器功能及参数。
  - 配置SSH用户登录的用户界面。
  - 配置SSH用户。
  - 通过STelnet登录设备。
- SSH登录故障的常见原因主要包括：
  - SSH Client与SSH Server之间没有可达路由，无法建立TCP连接。
  - SSH服务未启动。
  - 用户界面VTY接口下未绑定SSH协议。
  - 没有配置SSH服务器和客户端的RSA公钥。
  - 没有配置用户服务类型、认证类型、用户认证服务类型。
  - 设备上登录用户数达到允许用户数的上限。
  - user-interface vty下绑定了ACL规则。
  - 服务器端与客户端SSH版本不一致。
  - 客户端未使能SSH客户端首次认证功能。

SSH登录故障 - 排障流程

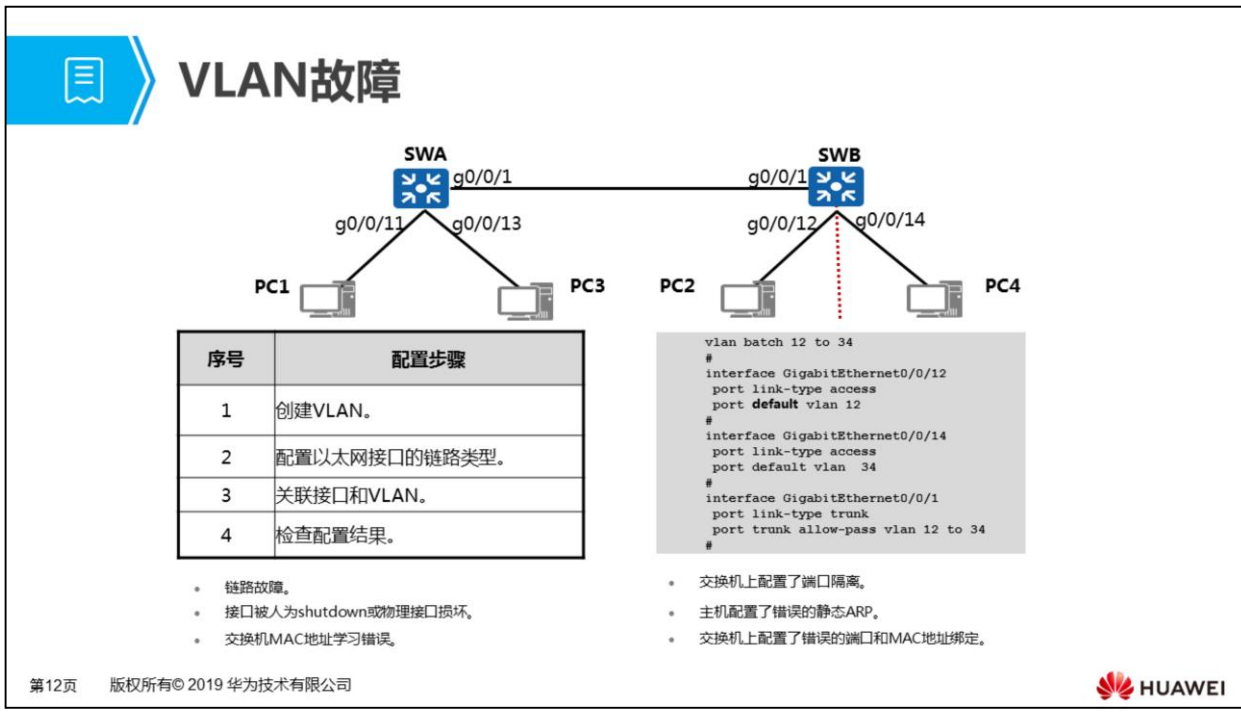


HUAWEI

- 查看SSH服务器端的SSH服务是否启动。
  - 通过Console口或Telnet方式登录SSH服务器端，执行命令display ssh server status，查看SSH服务器端配置信息。
  - 如果STelnet没有使能，执行如下命令stelnet server enable，使能SSH服务器端的STelnet
  - 服务。
- 在SSH服务器端上查看VTY类型用户界面视图下允许接入的协议配置是否正确。
  - 在SSH服务器端上执行命令user-interface vty进入用户界面视图，执行命令display this，查看VTY用户界面的protocol inbound是否为ssh或者all。如果不是，执行命令protocol inbound { ssh | all }修改配置，允许STelnet类型用户接入设备。
- 查看在SSH服务器端是否配置了RSA公钥。
  - 设备作为SSH服务器时，必须配置本地密钥对。
  - 在SSH服务器端上执行命令display rsa local-key-pair public查看当前服务器端密钥对信息。如果显示信息为空，则表明没有配置服务器端密钥对，执行命令rsa local-key-pair create创建。

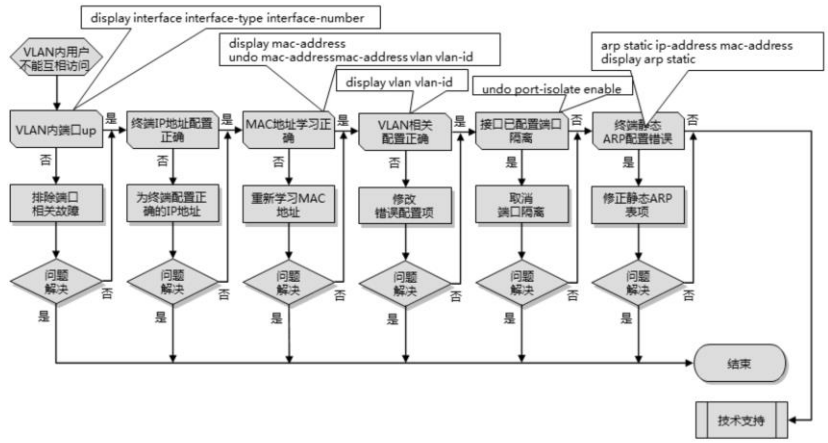
- 查看SSH服务器端上是否配置了SSH用户。
  - 执行命令display ssh user-information，查看SSH用户的配置信息。如果不存在配置信息，请在系统视图下执行命令ssh user authentication-type，新建SSH用户并配置SSH用户的认证方式。
- 查看登录SSH服务器端的用户数是否到达了上限。
  - 从Console口登录到设备，执行命令display users，查看当前的VTY通道是否全部被占用。缺省情况下，VTY通道允许的最大用户数是5个，可以先执行命令display user-interface maximum-vty，查看当前VTY通道允许的最大用户数。
  - 如果当前的用户数已经达到上限，可以执行命令user-interface maximum-vty 15，将VTY通道允许的最大用户数扩展到15个。
- 查看SSH服务器端上VTY类型用户界面下是否绑定了ACL。
  - 在SSH服务器端上执行命令user-interface vty进入SSH用户会使用的界面视图，执行命令display this，查看VTY用户界面是否配置了ACL限制，如果配置了ACL限制，请记录该ACL编号。
  - 在SSH服务器端上执行命令display acl acl-number，查看该访问控制列表中是否deny了STelnet客户端的地址。如果deny客户端的IP地址，则在ACL视图下，执行命令undo rule rule-id，删除deny规则，再执行命令rule permit source source-ip-address soucer-wildcard，修改访问控制列表permit客户端的IP地址访问。
- 查看SSH客户端和服务器上SSH版本信息。
  - 在SSH服务器上执行命令display ssh server status，查看SSH版本信息。
  - 如果使用SSHv1版本的客户端登录服务器，则执行命令ssh server compatible-ssh1x enable配置服务器端版本兼容使能。
- 查看SSH客户端是否使能了首次认证功能。
  - 在SSH客户端的系统视图下执行命令display this，查看SSH客户端是否使能SSH客户端首次认证功能。
  - 如果没有使能SSH客户端首次认证功能，则STelnet客户端第一次登录SSH服务器时，由于对SSH服务器的RSA公钥有效性检查失败，而导致登录服务器失败。执行命令ssh client first-time enable使能SSH客户端首次认证功能。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
  - 上述步骤的执行结果。
  - 设备的配置文件、日志信息、告警信息。

目录



- 以太网是一种基于CSMA/CD（Carrier Sense Multiple Access/Collision Detection）的共享通讯介质的数据网络通讯技术。当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降甚至造成网络不可用等问题。通过交换机实现LAN（Local Area Network）互连虽然可以解决冲突严重的问题，但仍然不能隔离广播报文和提升网络质量。这种情况下出现了VLAN技术，这种技术可以把一个LAN划分成多个逻辑VLAN。每个VLAN是一个广播域，VLAN内的主机间通信就和在一个LAN内一样，而VLAN间则不能直接互通，这样，广播报文就被限制在一个VLAN内。
- 配置VLAN的步骤为：
  - 创建VLAN。
  - 配置以太网接口的链路类型。
  - 关联接口和VLAN。
  - 检查配置结果。
- VLAN故障常见原因有：
  - 链路故障。
  - 接口被人为shutdown或物理接口损坏。
  - 交换机MAC地址学习错误。
  - 交换机上配置了端口隔离。
  - 主机配置了错误的静态ARP。
  - 交换机上配置了错误的端口和MAC地址绑定。

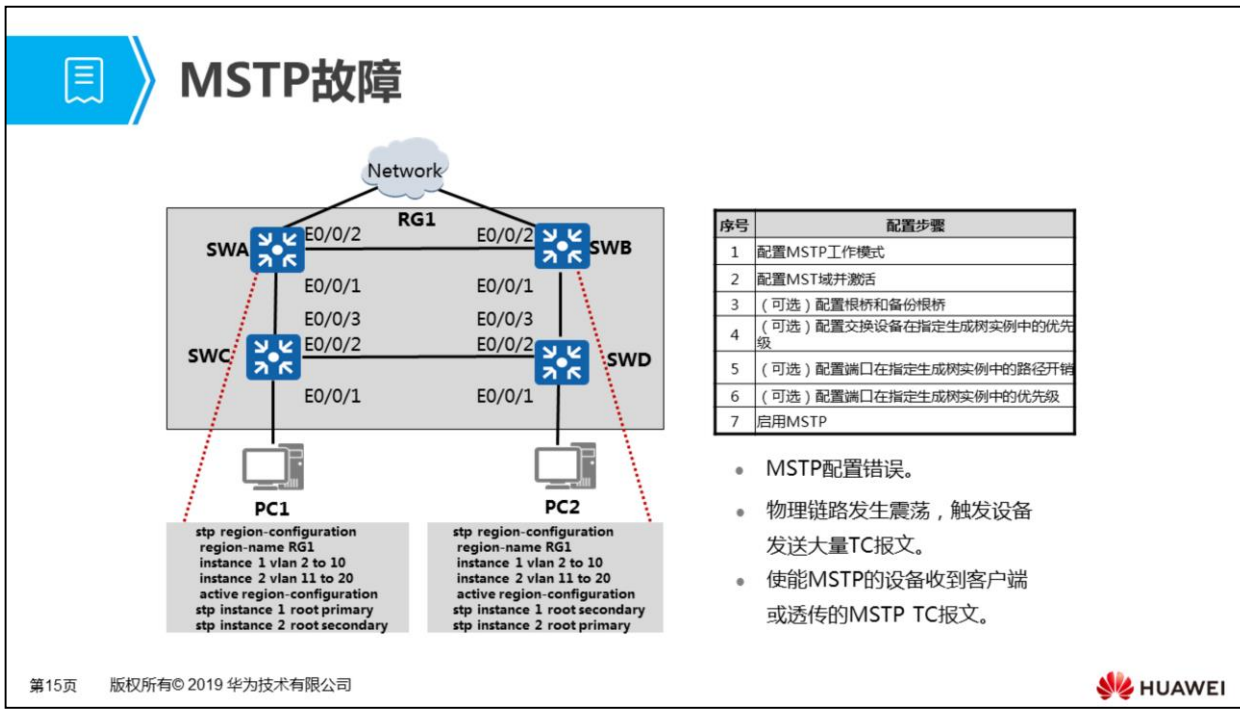
VLAN故障 - 排障流程



  HUAWEI

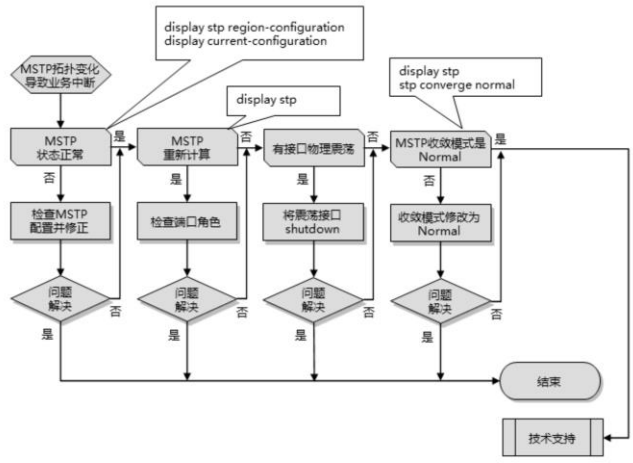
- 检查VLAN内需要互通的端口是否Up。
  - 在任意视图下执行display interface interface-type interface-number命令查看需要互通的端口的运行状态。如果接口的状态为Down，先排除接口Down的故障。
- 检查需要互通的终端IP地址是否在同一网段，如果不是则修改为同一网段。
- 检查Switch上MAC地址表项是否正确。
  - 在Switch上执行display mac-address检查设备学习到MAC地址、MAC地址对应接口、所属VLAN是否正确，如果不正确则在接口上执行undo mac-addressmac-address vlan vlan-id 命令使Switch重新学习指定的MAC地址。
- 检查VLAN相关配置是否正确。
  - 检查需要互通的端口所在的VLAN是否已经创建。在任意视图下执行display vlan vlan-id查看需要互通的端口所在的VLAN是否已经创建，如果未创建则在系统视图下执行vlan命令创建VLAN。
  - 检查需要互通的接口是否加入VLAN。执行display vlan vlan-id检查需要互通的接口是否已经加入指定VLAN，如果未加入则将接口加入指定VLAN。如果需要互通的接口不在同一个交换机，还需要考虑交换机互联的接口允许指定的VLAN通过。
- 检查设备上是否配置了端口隔离。
  - 在系统视图下执行interface interface-type interface-number进入故障接口视图，然后执行display this命令查看接口是否配置了端口隔离。如果配置了端口隔离，使用undo port-isolate enable命令取消端口上端口隔离配置。
- 检查终端设备上是否配置了错误的静态ARP表项，如果终端设备上配置了错误的静态ARP表项则修正。
  - 使用display arp static命令查看静态ARP配置，使用命令arp static ip-address mac-address修改静态ARP配置。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
  - 上述步骤的执行结果。
  - 设备的配置文件、日志信息、告警信息。

目录



- 在一个复杂的网络中，由于冗余备份的需要，网络规划者一般都倾向于在设备之间部署多条物理链路，其中一条作为主用链路，其他作为备份链路。这样就难免会形成环路，若网络中存在环路，可能会引起广播风暴和MAC表项被破坏。为此，可以在网络中部署MSTP协议预防环路。MSTP可阻塞二层网络中的冗余链路，将网络修剪成树状，达到消除环路的目的。
- MSTP的配置步骤为：
  - 配置MSTP工作模式。
  - 配置MST域并激活。
  - （可选）配置根桥和备份根桥。
  - （可选）配置交换设备在指定生成树实例中的优先级。
  - （可选）配置端口在指定生成树实例中的路径开销。
  - （可选）配置端口在指定生成树实例中的优先级。
  - 启用MSTP。
  - 检查配置结果。
- MSTP故障的常见原因有：
  - MSTP配置错误。
  - 物理链路发生震荡，触发设备发送大量TC报文。
  - 使能MSTP的设备收到客户端或透传的MSTP TC报文。

MSTP故障 - 排障流程



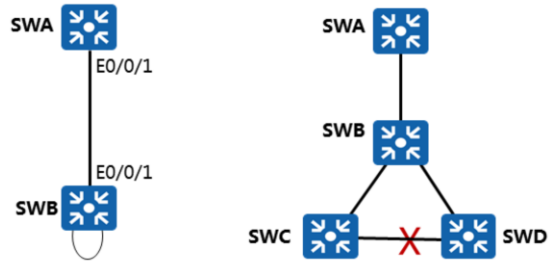
- 检查MSTP组网内的端口状态是否正常。
  - 查看MSTP的端口状态，确认每个端口在每个实例的连通性。
- 检查MSTP配置是否正确。
  - 执行命令display stp region-configuration检查VLAN与实例之间的映射关系。
    - 查看VLAN与实例之间的映射关系是否正确。若出现映射关系错误，则执行命令instance将指定VLAN映射到指定的生成树实例上，并执行命令active region-configuration激活instance命令配置的VLAN与实例之间的映射关系。
  - 执行命令display current-configuration获取设备的配置文件，查看设备上MSTP的相关配置。
    - 查看端口配置，确认使能MSTP的端口是否使能了协议报文上送命令。如：bpdu enable。
    - 与用户终端设备相连的端口MSTP是否是处于去使能状态或配置为边缘端口。
    - 如果使能MSTP的设备上配置了BPDU Tunnel，则确认BPDU Tunnel配置是否正确。
    - 查看设备端口是否加入正确的VLAN。

- 查看组网中是否有MSTP重新计算。
    - 在任意视图下执行命令display stp查看设备是否收到TC报文。
        - 如果上述显示信息中TC or TCN received、TC count per hello、TC received、TC count per hello中的数值增长，说明设备收到TC报文，网络拓扑发生变化。则查看日志MSTP/6/SET_PORT_DISCARDING和MSTP/6/SET_PORT_FORWARDING，通过日志查看使能MSTP的端口角色是否有变化。
        - 如果上述显示信息中TC or TCN received、TC count per hello、TC received、TC count per hello中的数值是0，说明设备没有收到TC报文，则应联系上级技术支持工程师。
- 查看是否有端口震荡。
    - 如果使能MSTP的端口状态在Up与Down之间不停的变动，则说明端口存在震荡。物理端口频繁的Up/Down将导致组网内设备的MSTP状态不稳定，并产生大量的TC报文，频繁删除ARP和MAC地址表项，导致业务中断。shutdown震荡的物理端口。
- 检查MSTP的收敛模式是否是Normal。
    - 在任意视图下执行命令display stp查看设备MSTP收敛模式。如果是Fast模式，则执行命令stp converge normal将收敛模式修改为Normal模式。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
    - 上述步骤的执行结果。
    - 设备的配置文件、日志信息、告警信息。

目录

环路故障

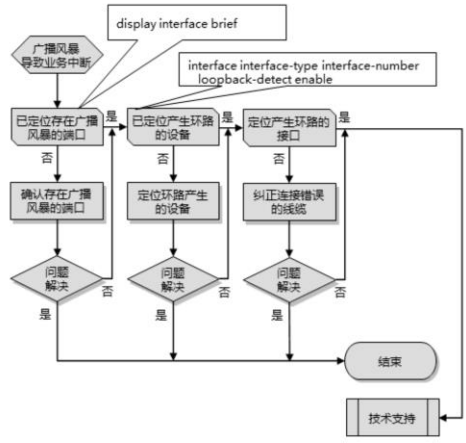
- 环路如果导致广播风暴会导致用户通信质量较差，甚至通信中断。



HUAWEI

- 以太网是一个支持广播的网络，在没有环路的环境中，广播报文在网络中以泛洪的形式被送达到网络的每一个角落，以保证每个设备都能够接受到它。每台二层设备在接收到广播报文以后，都会向除接收端口以外的其他所有接口转发这个广播报文，一旦网络中有环路，这种简单的广播机制就会引发灾难性后果。
- 环路中一个广播报文被反复转发了千万次，产生了广播风暴并且很快达到或接近接口最大转发速率，并迅速消耗链路带宽。根据转发规则，这些广播报文不仅仅只是在环路上无限转发，环路设备还会向其他端口转发一份，造成整个网络中都充斥着大量重复广播报文。例如，全网络都采用千兆端口互连，出现广播风暴后，几乎每一条链路上都充斥着1000Mbit/s的广播报文，正常的数据报文将很难再获得转发的机会。进而影响正常业务，导致用户通信质量较差，甚至通信中断。
- 可能会有如下现象产生：
  - 设备无法远程登录。
  - 在设备上使用display interface命令查看接口统计信息时发现接口收到大量广播报文。
  - 使用串口登录设备进行操作时，操作比较慢。
  - CPU占用率超过70%。
  - 通过ping命令进行网络测试时丢包严重。
  - 设备上发生环路的VLAN的接口指示灯频繁闪烁。
  - PC机上能收到大量的广播报文。
  - 设备部署环路检测后，设备出现环路告警。
- 本类故障的常见原因主要为设备线缆连接错误导致环路。

环路故障 - 排障流程



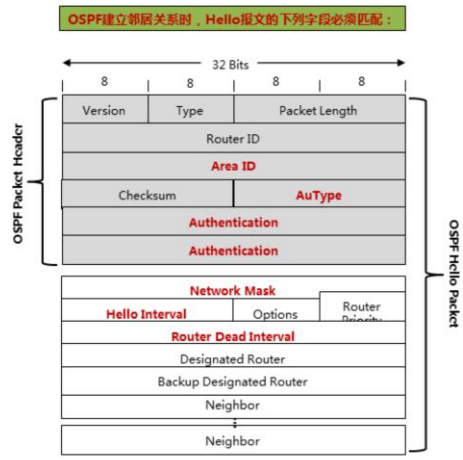
HUAWEI

- 确认存在广播风暴的接口。
  - 可以采用如下方式确认存在广播风暴的接口。
    - 通过观察接口指示灯状态，如果接口指示灯频繁闪烁，可以判断该接口可能存在广播风暴。
    - 在设备上执行display interface brief命令查看接口接收方向和发送方向最近一段时间的带宽利用率。显示信息中“InUti”字段表示入方向上的带宽利用率，“OutUti”字段表示出方向上的带宽利用率。接口接收方向和发送方向最近一段时间的带宽利用率接近100%的接口可能是存在广播风暴的接口。
- 判断环路产生的设备。
  - 如果存在广播风暴的接口没有下连其他Switch，此时可以判断环路发生在该Switch上。
  - 如果存在广播风暴的接口下连其他Switch，此时环路可能发生在该Switch上也可能发生在下连Switch上，此时可以选择如下方式进行环路检测：

        - 在Switch上针对指定VLAN部署Loopback Detection协议，检测存在环路的接口，并且Loopback Detection的处理动作配置为发现环路后产生告警。如果Switch产生LDT 1.3.6.1.4.1.2011.5.25.174.3.3 hwLdtPortLoopDetect告警，则根据告警中提示的接口信息确认产生环路的接口。如果产生环路的接口是下连其他Switch的接口，证明环路发生在下连Switch。如果未产生告警，证明环路产生在本Switch。
        - 执行完上述操作后如果本Switch还下连其他Switch，并且发生环路的设备为下连Switch，则重复执行上述操作。
        - 如果存在多个接口下连其他Switch，并且该接口产生广播风暴，说明环路可能发生在设备与设备之间。
    - 在下连接口上执行shutdown命令，观察本设备和整个网络是否存在广播风暴。
        - 执行上述操作后如果本设备存在广播风暴，下连Switch不存在广播风暴，证明环路发生在本Switch3。
        - 执行上述操作后如果存在广播风暴的接口没有下连其他Switch，此时可以判断环路发生在该Switch上。
        - 执行上述操作后如果本Switch和整个网络中广播风暴消失，证明环路发生在设备和设备之间。
        - 如果下连其他Switch，并且下游设备仍存在广播风暴，则继续在下连Switch上重复执行上述操作。
- 判断产生环路的接口并破环。
    - 如果环路发生在单个设备上，说明环路是因为本设备两个属于相同VLAN的接口直接连接导致，可以采用如下方式进行环路排除：
        - 根据广播风暴产生的接口逐个排查该接口连接的线缆对端是不是本设备的其他接口，如果是则拔出线缆。
        - 在产生广播风暴的接口执行shutdown命令，如果此时广播风暴消失，并且在执行shutdown命令时设备上另外一个接口变成Down状态，此时证明这两个接口为产生环路的接口，此时和管理员确认后拔出接口线缆。
    - 如果确认环路发生在设备之间，此时参考网络规划，排查和本设备相连的其他设备之间是否存在错误的连接导致网络形成环路。根据广播风暴产生的接口逐个排查该接口连接的线缆对端设备是不是和规划中的一样，查找出错误连接并拔出线缆。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
    - 上述步骤的执行结果。
    - 设备的配置文件、日志信息、告警信息。

目录

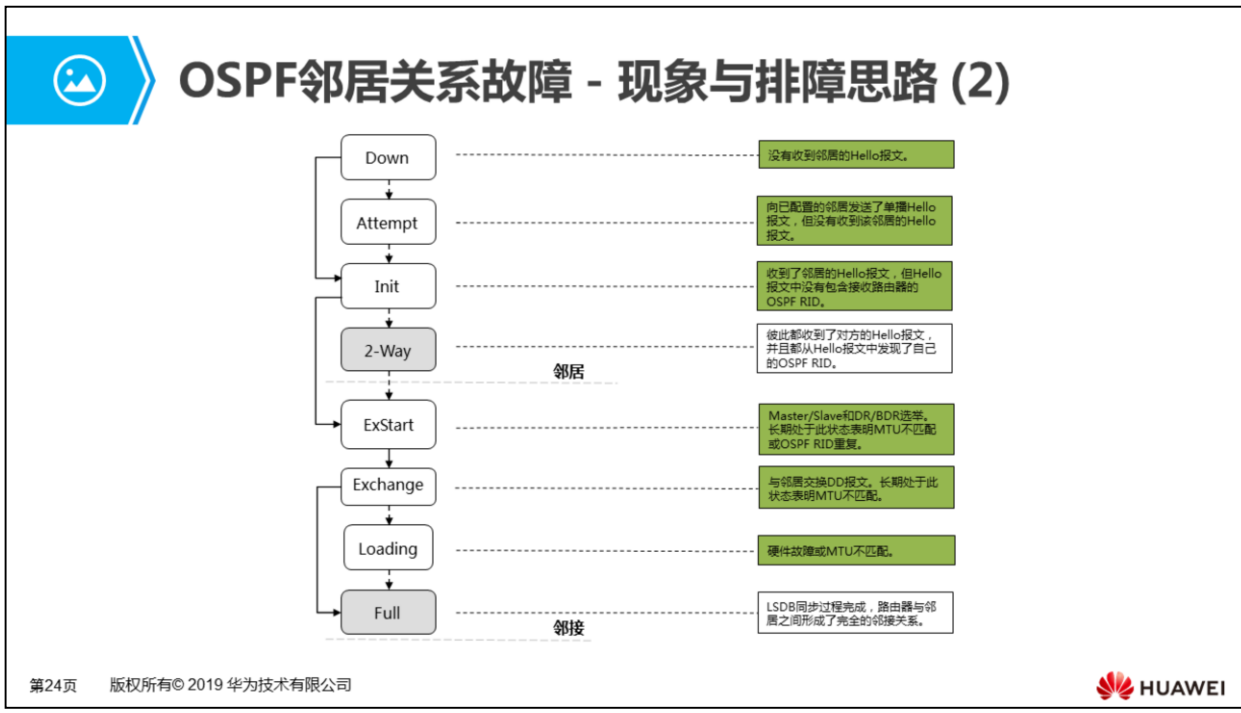
OSPF邻居关系故障 - 现象与排障思路 (1)



- OSPF邻居关系故障现象：
  - OSPF邻居表为空。
  - OSPF邻居停滞于INIT状态。
  - OSPF邻居停滞于2-WAY状态。
  - OSPF邻居停滞于EXSTART/ EXCHANGE状态。

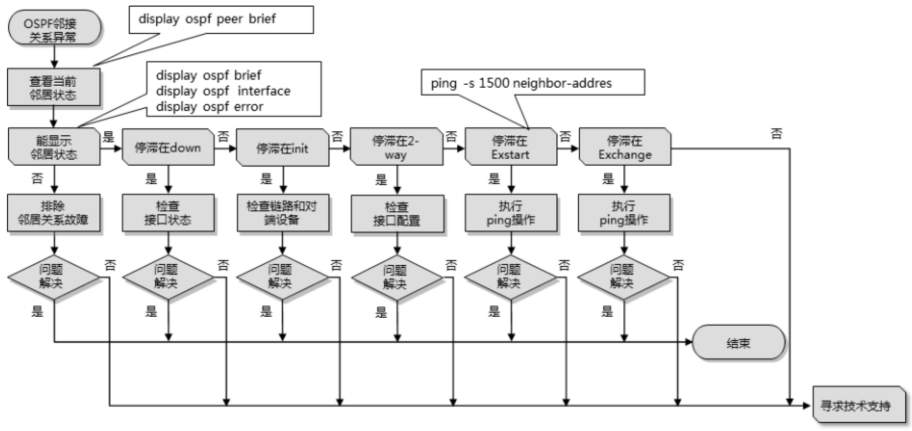
HUAWEI

- OSPF建立邻居关系时，将检验Hello报文中的Area ID、AuType、Authentication、Network Mask、Hello Interval、Router Dead Interval字段以及可选项的值是否和接收接口上配置的对应值相匹配。如果它们不匹配，那么该数据包将被丢弃，而且邻接关系也无法建立。
- OSPF邻居关系故障的常见现象为：
  - OSPF邻居表为空。
  - OSPF邻居停滞于INIT状态。
  - OSPF邻居停滞于2-WAY状态。
  - OSPF邻居停滞于EXSTART/EXCHANGE状态。



- 如果一个邻居停滞于以下某个状态并且持续很长时间，就代表着OSPF的邻居关系可能出现了故障。
  - Down：这是邻居的初始状态，表示路由器还没有从邻居收到任何信息。停滞于此状态表明路由器没有从邻居处接收到Hello报文。
  - Attempt：此状态只在NBMA网络上存在，表示路由器没有收到邻居的任何信息，但是已经周期性地向邻居发送了Hello报文；如果在Router Dead Interval的时间间隔内未收到邻居的Hello报文，则转为Down状态。停滞于此状态表明路由器向已配置的邻居发送了单播Hello报文，但没有收到该邻居的Hello报文。
  - Init：表示路由器已经从邻居收到了Hello报文，但是自己不在所收到的Hello报文的邻居列表中。这说明自己尚未与邻居建立起双向通信关系。停滞于此状态表明路由器收到了邻居的Hello报文，但Hello报文中没有包含接收路由器的OSPF RID（Router ID）。
  - 2-Way：表示路由器与邻居的双向通信关系已经建立（即已经建立起了邻居关系），但是尚未建立起邻接关系。停滞于此状态表明路由器彼此都收到了对方的Hello报文，并且都从Hello报文中发现了自己的OSPF RID。对于以太网链路上的非DR/BDR路由器来说，这种状态是可以接受的。
  - ExStart：邻居状态变成此状态以后，路由器开始向邻居发送DD报文。Master/Slave关系是在此状态下形成的，初始DD序列号也是在此状态下确定的。在此状态下发送的DD报文不包含链路状态描述。停滞于此状态表明邻居路由器之间的MTU不匹配或OSPF RID重复。
  - Exchange：在此状态下，路由器与邻居之间相互发送包含链路状态信息摘要的DD报文。停滞于此状态表明邻居路由器之间的MTU不匹配。
  - Loading：在此状态下，路由器与邻居之间相互发送LSR报文、LSU报文、LSAck报文。停滞于此状态表明可能存在硬件故障或硬件故障或MTU不匹配。
  - Full：表示LSDB同步过程完成，路由器与邻居之间形成了完全的邻接关系。

OSPF邻居关系故障 - 排障流程



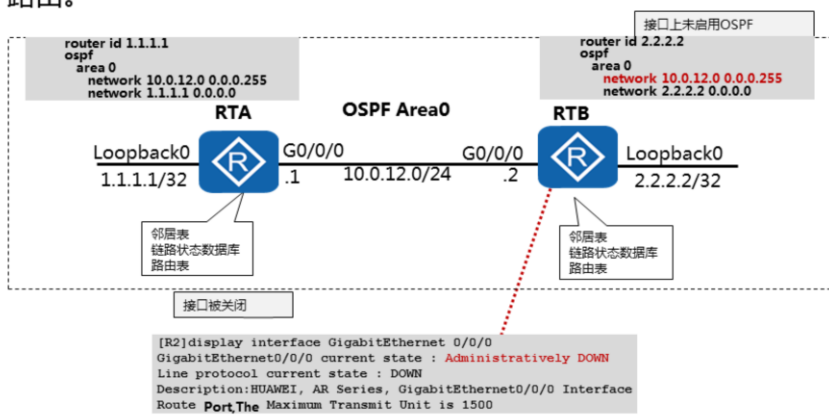
  HUAWEI

- 无法显示OSPF邻居：
  - 执行display interface [interface-type [interface-number]]命令查看接口物理层状态，检查设备链路是否故障（包括传输设备故障）。
  - 如果接口连接的是广播网络或NBMA网络，检查两端IP地址是否在同一网段。
  - 如果在接口上使能了ospf mtu-enable，则要求接口的MTU一致，否则OSPF邻居无法协商成功。在接口视图下执行mtu mtu命令，修改链路两端的MTU值为一致。
  - 对于Broadcast和NBMA类型的网段，各接口的优先级至少有一个是非零的，以确保能够正确的选举出DR，否则两边的邻居状态只能达到2-Way。执行命令display ospf interface，查看接口的优先级。
  - 检查两端OSPF的配置是否有错误：
    - 检查两端OSPF RouterID配置是否相同：display ospf brief。如果相同则执行ospf router-idrouter-id命令修改配置使Router ID在AS域内唯一。
    - 检查两端OSPF Area配置是否一致：display ospf interface。
    - 检查两端OSPF的其他配置是否一致：每10秒钟执行一次命令display ospf error，持续5分钟。

        - 查看Bad authentication type字段，如果这个字段对应的计数值一直增长，表示建立邻居的两台设备配置的OSPF认证类型不一致，需要在两端设备上执行area-authentication-mode命令配置相同认证的类型。
        - 查看Hello timer mismatch字段，如果这个字段对应的计数值一直在增长，表示接口上hello timer配置不一致，需要通过检查两端设备接口配置，执行ospf timer hello命令将hello timer间隔配置一致。
        - 查看Dead timer mismatch字段，如果这个字段对应的计数值一直在增长，表示接口的dead timer配置不一致，需要通过检查两端设备接口配置，执行ospf timer dead命令将dead timer间隔配置一致。
        - 查看Extern option mismatch字段，如果这个字段对应的计数值一直在增长，表示区域类型配置不一致（一端配置为普通区域，另一端配置为stub或nssa区域），需要将两端区域类型配置一致（在OSPF区域视图下，如果有stub命令，表示区域类型为stub；如果有nssa命令，表示区域类型为nssa）。
- 停滞在down：
    - 执行display interface [interface-type [interface-number]]命令查看接口物理层状态，如果接口物理层状态为Down先处理接口故障问题。
    - 如果接口物理层状态是Up，执行display ospf interface查看接口在OSPF协议下状态是否为Up。
- 停滞在init：
    - 如果查看邻居状态时显示一直是init，表示对端设备收不到本端发送的hello报文，此时需要排查链路和对端设备是否故障。
- 停滞在2-way：
    - 如果查看邻居状态一直是2-way，则执行命令display ospf interface查看设备在OSPF下面使能的接口配置的dr-priority是否为0。如果OSPF下使能的接口配置的dr-priority是0且State为DROther，则说明他们都不是DR或BDR，两者之间不需要交换LSA，2-way为正常状态，无需处理。
- 停滞在Exstart：
    - 如果查看邻居状态一直是Exstart，表示设备一直在进行DD协商，但无法进行DD同步，出现该情况有两种可能性：
        - 超大报文包无法正常收发。可以通过执行命令ping -s 1500 neighbor-address查看超大报文收发情况。如果无法Ping通，需先解决链路问题。
        - OSPF MTU值配置不同。如果OSPF接口下配置了ospf mtu-enable，检查两端的OSPF MTU值是否相等，如果不相等则修改接口下的MTU值。
- 停滞在Exchange：
    - 如果查看邻居状态一直是Exchange，表示设备在进行DD交换，通过单播交换DD报文。此时需要排查链路和对端设备是否故障。
- 如果故障无法排除，收集如下信息，联系上级支持工程师。
    - 上述步骤的执行结果。
    - 设备的配置文件、日志信息、告警信息。

OSPF域内路由故障 - 现象与排障思路

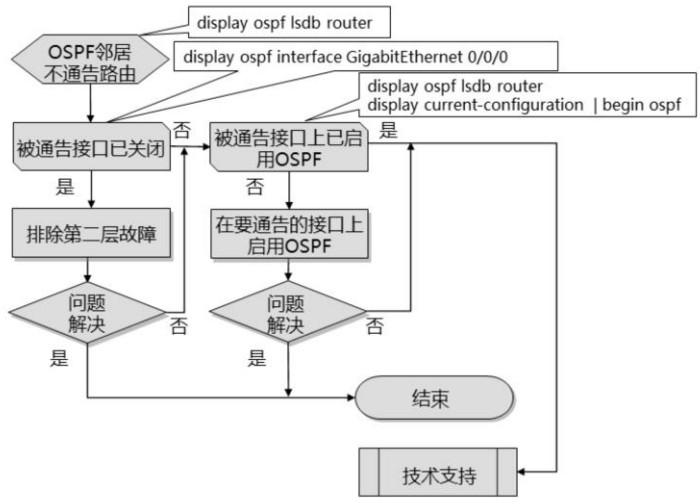
- OSPF的域内路由故障常表现为邻居路由器不通告部分或全部路由。



HUAWEI

- OSPF的域内路由故障常表现为邻居路由器不通告部分或全部路由。可能的原因通常为：
  - 拟通告的接口上未启用OSPF。
  - 拟通告接口被关闭。
- OSPF是一种基于链路状态的内部网关路由协议，存在链路状态数据库。在运行了OSPF的路由器中需要重点关注邻居表、链路状态数据库（通常也会把它叫做“链路状态表”）、路由表。如果邻居不通告某条路由，那么这条路由将无法显示在本地路由器的路由表和OSPF链路状态数据库中。同时，这也表示邻居没有把这条路由包含到它自己的OSPF链路状态数据库中。

OSPF域内路由故障 - 排障流程

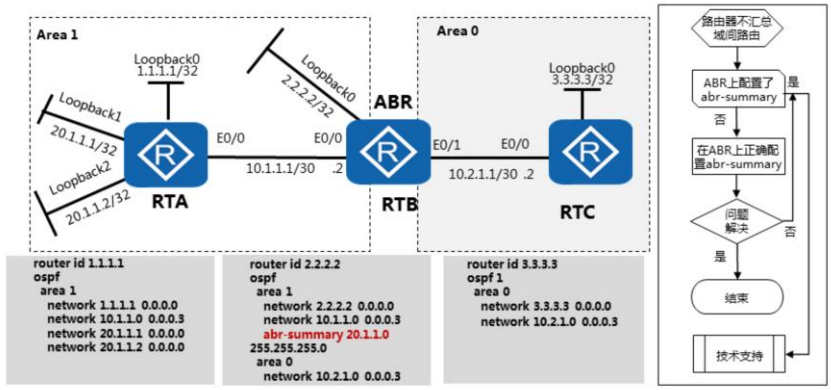


  HUAWEI

- 检查被通告接口是否被关闭。
  - OSPF不会通告断开的网络。所以如果一个接口被关闭了，那么分配给这个接口的网络不会被OSPF通告给邻居路由器。
  - 使用命令display ospf lsdb router检查链路状态数据库中是否存在此网络的条目。
  - display ospf interface GigabitEthernet 0/0/0命令的输出结果可以显示链路协议状态。
  - 解决方法是启用被关闭的接口、排除第二层的故障。
- 检查被通告接口上是否已启用OSPF。
  - 只有在接口上启用了OSPF的时候，链路状态数据库中才会包括这个接口的网络。network语句的缺失或者配置错误都会导致链路状态数据库中缺少这个接口所在网络的路由。
  - 使用命令display ospf lsdb router可以看到链路状态数据库中是否缺少某个网络的信息。
  - 使用命令display current-configuration | begin ospf显示OSPF的配置命令，可以检查其中的network语句是否配置正确。
- 如果故障无法排除，收集如下信息，联系上级支持工程师。
  - 上述步骤的执行结果。
  - 设备的配置文件、日志信息、告警信息。

OSPF域间路由故障 - 现象与排障流程

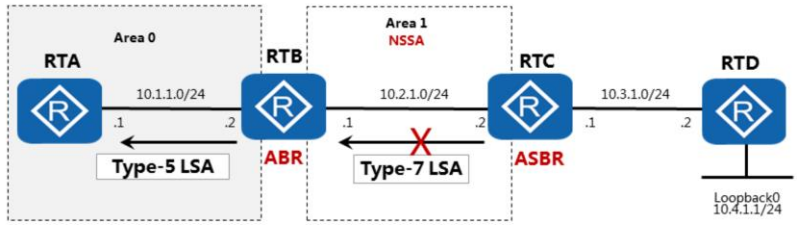
- OSPF区域间路由故障常表现为ABR路由器不能正常完成路由汇总功能。



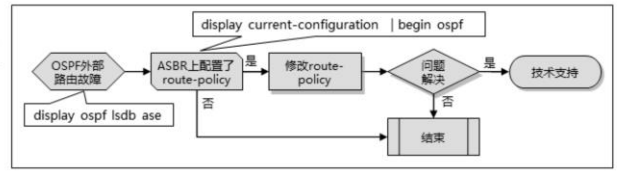
HUAWEI

- OSPF ABR路由器同时属于多个区域，并为它所连接的每个区域维护一个LSDB。ABR路由器会将所连接的非骨干区域内的链路状态信息（Router LSA和Network LSA）抽象成路由信息（Network Summary LSA），并将此路由信息发布到骨干区域中，再由骨干区域进一步发布到其他非骨干区域中。同时，ABR也会将骨干区域的链路状态信息抽象成路由信息，并将此路由信息发布到所连接的非骨干区域中。
- OSPF区域间路由故障常表现为ABR路由器不能正常完成路由汇总功能。此时需要使用命令display current-configuration | begin ospf检查ABR上是否正确配置了abr-summary命令。

OSPF域外路由故障 - 现象与排障流程



- ASBR不通告被重发布的路由。

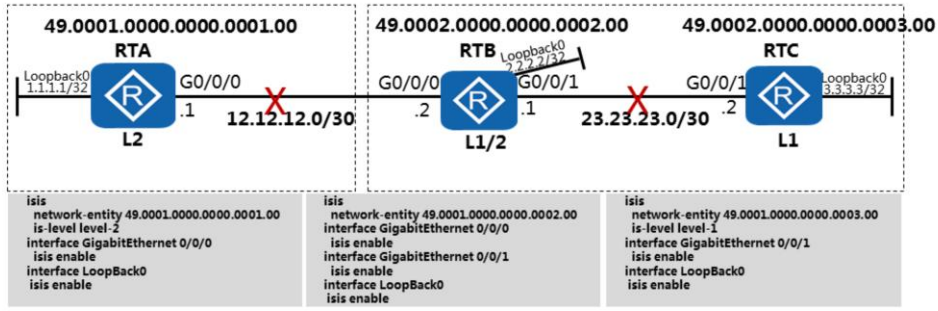


  HUAWEI

- NSSA区域中的ASBR可以引入外部路由，并通过Type-7 LSA（NSSA LSA）在本区域内进行宣告。NSSA区域中的ASBR不能产生并宣告Type-5 LSA（AS External LSA），只能产生并宣告Type-7 LSA（NSSA LSA）。在区域边界，NSSA区域的ABR会将该Type-7 LSA转换成一条Type-5 LSA，并向所有的其他区域进行泛洪。
- OSPF域外路由故障常表现为NSSA区域的ASBR不通告被重发布的路由。可以使用命令display ospf lsdb ase显示OSPF的AS外部连接状态数据库信息。当ASBR上配置的filter-policy阻止了OSPF将外部路由安装到链路状态数据库时，需要通过修改访问控制列表来解决。

目录

IS-IS邻居关系故障 - 现象与排障思路

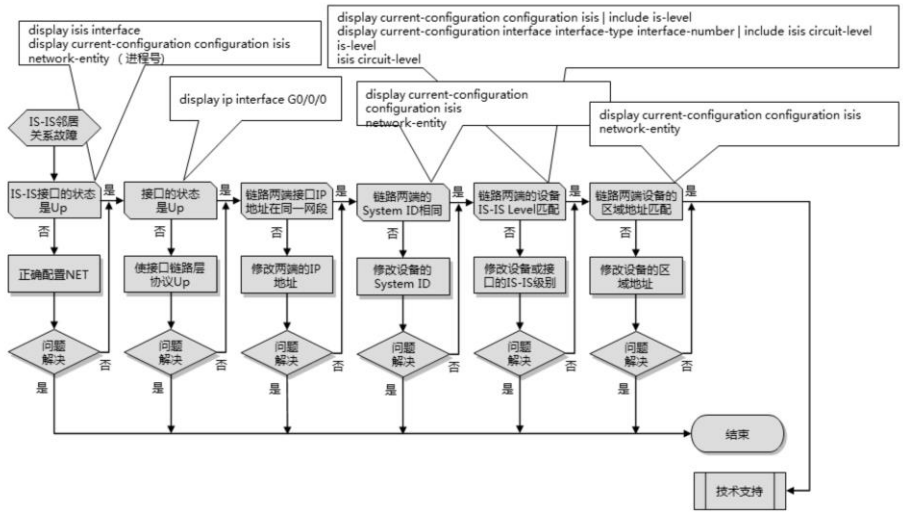


- 设备底层故障或者链路故障导致IS-IS无法正常的收发Hello报文。
- 链路两端的设备配置的System ID相同。
- 链路两端的IS-IS Level不匹配。
- 建立IS-IS Level-1邻居时，链路两端设备的区域ID不匹配。
- 链路两端的接口的IP地址不在同一网段。

HUAWEI

- IS-IS网络采用了骨干区域与非骨干区域两级分层结构。IS-IS路由器分为：Level-1路由器，Level-2路由器，Level-1/2路由器（L1路由器，L2路由器，L1/2路由器）。L1路由器负责区域内的路由，只与属于同一区域的L1和L1/2路由器形成L1邻居关系，属于不同区域的L1路由器之间不能形成邻居关系。L2路由器负责区域间的路由，可以与位于同一区域或者不同区域的L2和L1/2路由器形成L2邻居关系。L1/2路由器同时属于L1和L2的路由器称为L1/2路由器，可以与同一区域的L1和L1/2路由器形成L1邻居关系，也可以与同一或者不同区域的L2路由器形成L2邻居关系，还可以与同一或不同区域的L1/2路由器形成L2的邻居关系。
- IS-IS邻居关系故障的可能原因如下所述，在这里我们重点关注前面五种原因。
  - 设备底层故障或者链路故障导致IS-IS无法正常的收发Hello报文；
  - 链路两端的设备配置的System ID相同；
  - 链路两端的IS-IS Level不匹配；
  - 建立IS-IS Level-1邻居时，链路两端设备的区域地址不匹配；
  - 链路两端的接口的IP地址不在同一网段；
  - 链路两端的接口的MTU设置不一致或者接口的MTU小于发送的Hello报文的长度；
  - 链路两端的IS-IS接口认证方式不匹配。

IS-IS邻居关系故障 - 排障流程

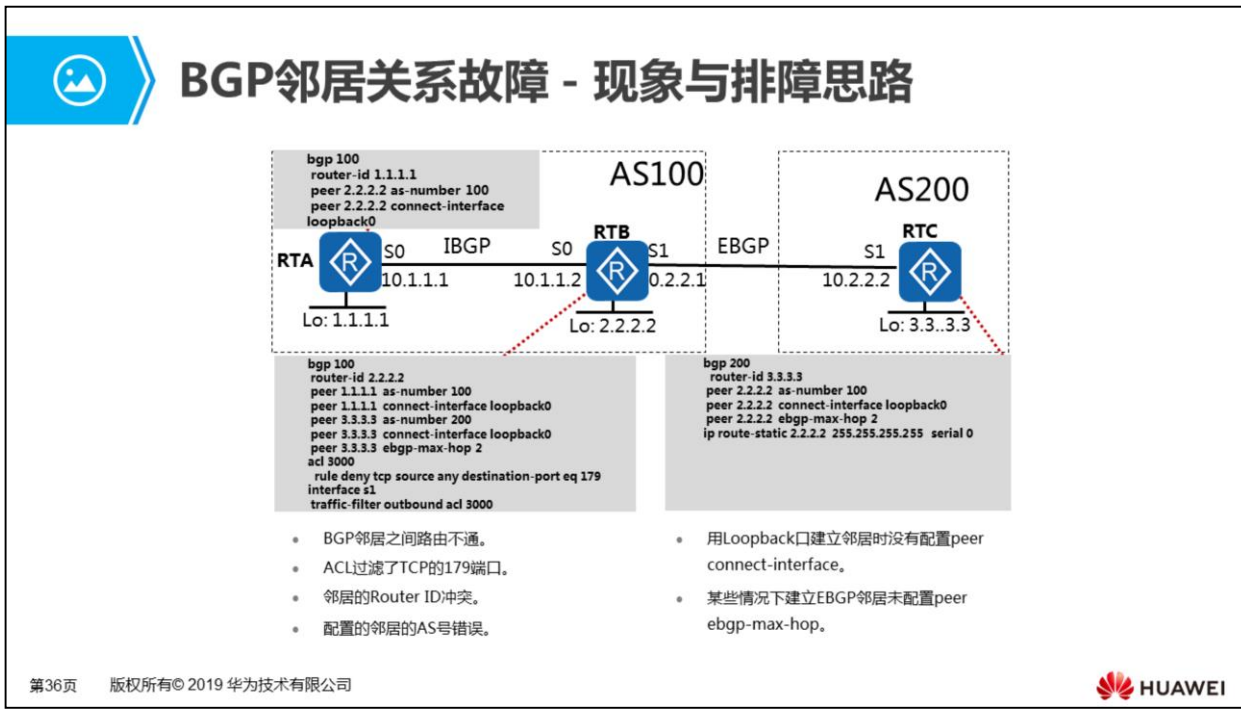


  HUAWEI

- 检查IS-IS接口的状态。
  - 执行display isis interface命令，检查使能了IS-IS的接口的状态（ “IPv4.State” 字段）。如果状态为Down，执行display current-configuration configuration isis检查是否配置了NET，如果没有配置，执行network-entity命令配置NET。
    - 当接口未正确配置IP地址时，接口的ISIS状态如下。
    - [R1-Serial1/0/0]display isis interface
    - Interface information for ISIS(10)
    - ---
    - Interface Id IPV4.State IPV6.State MTU Type DIS
    - Loop0 002 Up Down 1500 L1/L2 --
    - S1/0/0 001 Mtu:Up/Lnk:Dn/IP:Dn Down 1500 L1/L2 --
- 检查接口是否Up。
  - 执行display ip interface [interface-type [interface-number]]命令，查看指定接口的状态。如果接口链路层协议状态（Line protocol current state字段）不是Up，先处理接口故障，使接口链路层协议状态为Up。
    - 对于以太接口这里面的Line protocol指的不是链路层协议，而指的是三层协议，检查接口是否正确配置了IP地址
    - [R1]display ip int g0/0/0
    - GigabitEthernet0/0/0 current state : UP
    - Line protocol current state : DOWN

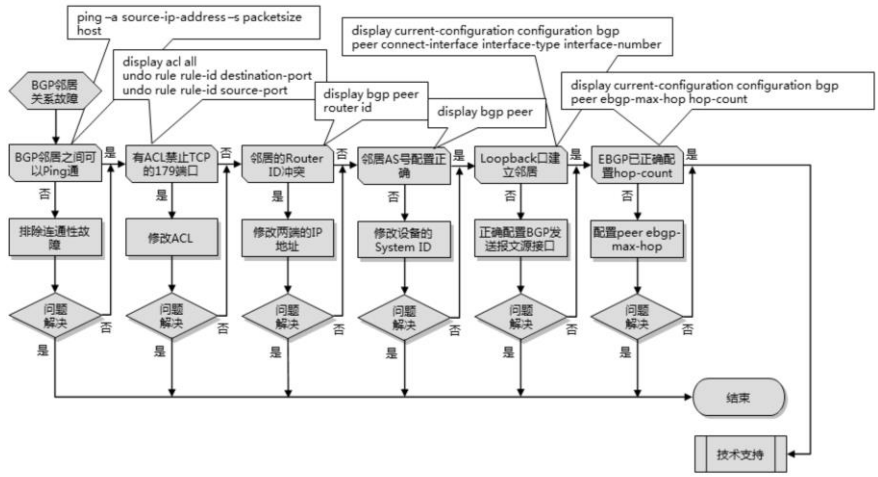
        - 而对于广域网接口，两段的封装不一致时line protocol状态才是down状态。例如一端是HDLC一端是PPP，应先检查链路
        - 两端的链路层协议是否一致，联系通信维护人员检查传输电路是否正常。
        - [R1-Serial1/0/0]display int se1/0/0
        - Serial1/0/0 current state : UP
        - Line protocol current state : DOWN
        - Description:HUAWEI, AR Series, Serial1/0/0 Interface
        - Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
        - Internet Address is 33.1.1.1/24
        - Link layer protocol is nonstandard HDLC
- 检查链路两端接口的IP地址是否在同一网段。（只有以太网链路要求两段在同一网段，点对点链路可以通过[R1-Serial1/0/0]isis peer-ip-ignore命令去掉这个限制。）
    - 如果IP地址不在同一网段，修改两端的IP地址，保证两端的IP地址在同一网段。
- 检查链路两端的设备配置的System ID是否相同。
    - 执行display current-configuration configuration isis查看链路两端设备的IS-IS配置的System ID是否相同。如果两端System ID相同，修改配置，使两端的System ID不同。
- 检查链路两端的设备的IS-IS Level是否匹配。
    - 执行display current-configuration configuration isis | include is-level命令查看两端IS-IS进程的Level，执行display current-configuration interface interface-type interface-number | include isis circuit-level命令，查看接口的IS-IS Level的配置，需要保证链路两端的Level匹配才能建立起IS-IS邻居。
    - 如果链路两端Level不匹配，在IS-IS视图下使用命令is-level修改设备的IS-IS级别，或者在接口视图下使用命令isis circuit-level修改接口的Level级别。
        - 在接口配置模式中，使用display this查看两端接口的isis接口网络类型是否一致。
        - interface GigabitEthernet0/0/1
        - ip address 10.1.1.2 255.255.255.0
        - isis enable 10
        - isis circuit-type p2p
- 检查链路两端设备的区域地址是否匹配。
    - 如果链路两端建立Level-1邻居，需要保证链路两端设备在同一个区域内。建立IS-IS Level-2邻居时，不需要判断区域地址是否匹配。
    - 如果链路两端无相同区域地址，在IS-IS视图下使用命令network-entity修改设备的区域地址。
- 如果故障无法排除，收集如下信息，联系上级支持工程师。
    - 上述步骤的执行结果。
    - 设备的配置文件、日志信息、告警信息。

目录



- BGP按照运行方式分为EBGP（External/Exterior BGP）和IBGP（Internal/Interior BGP）。运行于不同AS之间的BGP称为EBGP。为了防止AS间产生环路，当BGP设备接收EBGP对等体发送的路由时，会将带有本地AS号的路由丢弃。运行于同一AS内部的BGP称为IBGP。为了防止AS内产生环路，BGP设备不将从IBGP对等体学到的路由通告给其他IBGP对等体，并与所有IBGP对等体建立全连接。BGP邻居无法建立是指BGP邻居状态无法到达Established状态。
- BGP邻居关系故障的常见原因主要包括：
  - BGP报文转发不通。
  - ACL过滤了TCP的179端口。
  - 邻居的Router ID冲突。
  - 配置的邻居的AS号错误。
  - 用Loopback口建立邻居时没有配置peer connect-interface。
  - 用Loopback口建立EBGP邻居未配置peer ebgp-max-hop。
  - 对端发送的路由数量是否超过peer route-limit命令设定的值。
  - 对端配置了peer ignore。
  - 两端的地址族不匹配。
- 后三种故障并不是很常见，在这里我们重点关注前面六种BGP邻居关系故障的解决方法。

BGP邻居关系故障 - 排障流程



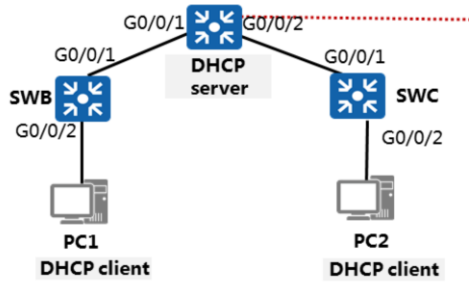
  HUAWEI

- 使用ping命令检测BGP邻居之间是否可以Ping通。
  - 使用命令ping –a source-ip-address –s packetsize host来检测两端的互通性，因为带源地址可以同时检测两端路由是否正常，指定ping的字节可以检查大包在链路上传输是否正常。
  - 如果可以Ping通，则说明BGP邻居之间有可达的路由并且链路传输也没有问题。
- 检查是否配置ACL禁止TCP的179端口。
  - 在两端执行display acl all命令查看是否禁止TCP的179端口。如果有禁止TCP的179端口的ACL，执行undo rule rule-id destination-port和undo rule rule-id source-port命令取消配置。
- 检查邻居的Router ID是否冲突。
  - 在两端分别查看无法建立的BGP邻居的情况，执行display bgp peer命令查看Router ID是否冲突。
  - 如果Router ID冲突，在BGP视图下运行命令router id将Router ID修改为不同（一般会用Loopback口的地址作为本端的Router ID）。

- 检查邻居AS号配置是否正确。
  - 在两端分别执行display bgp peer，检查邻居的AS号是否是对端的AS号。如果AS号配置错误，将AS号配置为对端的AS。
- 用Loopback口建立邻居时，检查是否正确配置peer connect-interface。
  - 通过display current-configuration configuration bgp查看BGP的配置，如果邻居两端使用Loopback口建立邻居，则需要使用命令peer connect-interface interface-type interface-number指定相应的Loopback口为发送BGP报文的源接口。
- 如果直连设备用Loopback口建立EBGP邻居，或者非直连多跳设备建立EBGP邻居，则需要配置命令peer ebgp-max-hop hop-count指定允许的最大跳数hop-count。通过display current-configuration configuration bgp查看BGP的配置，进行如下检查：
  - 直连设备使用Loopback口建立连接时，hop-count只要大于1即可。
  - 非直连设备建立连接时需要指定hop-count为相应的跳数。
- 如果故障无法排除，收集如下信息，联系上级支持工程师。
  - 上述步骤的执行结果。
  - 设备的配置文件、日志信息、告警信息。

目录

DHCP Server故障




```
ip pool 1
 gateway-list 10.1.1.1
 network 10.1.1.0 mask 255.255.255.128
 excluded-ip-address 10.1.1.2
 excluded-ip-address 10.1.1.4
 lease day 10 hour 0 minute 0
 dns-list 10.1.1.2
ip pool 2
 gateway-list 10.1.1.129
 network 10.1.1.128 mask 255.255.255.128
 lease day 2 hour 0 minute 0
 dns-list 10.1.1.2
 nbns-list 10.1.1.4
```

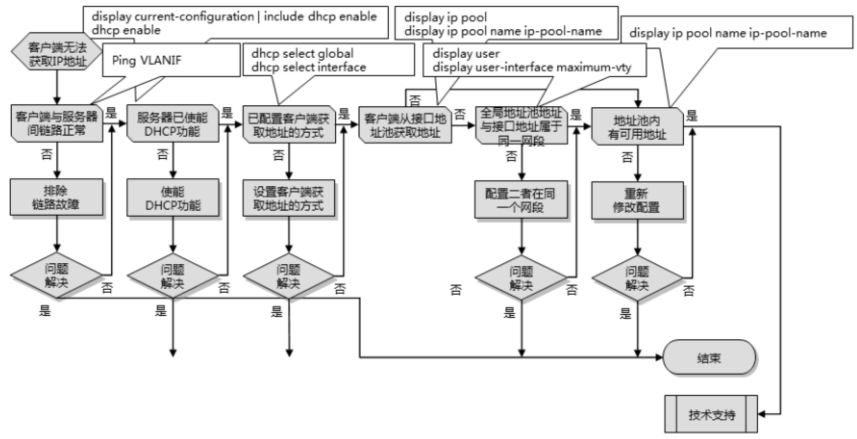
序号	配置步骤
1	配置全局地址池
2	配置接口工作在全局地址池模式
3	（可选）静态配置DHCP客户端的DNS服务
4	（可选）静态配置DHCP客户端的NetBIOS服务
5	（可选）配置全局地址池DHCP自定义选项
6	（可选）配置防止IP地址重复分配功能
7	（可选）配置DHCP数据保存功能

- 客户端与服务器之间的链路故障。
- 未使能DHCP功能。
- VLANIF接口下没有选择DHCP分配地址的方式。
- 全局地址池中的IP地址与VLANIF接口的IP地址不在同一个网段中。
- 地址池中没有可用的IP地址可分配。

HUAWEI

- 随着网络规模的扩大和网络复杂度的提高，网络配置变的越来越复杂，再加上计算机数量剧增且位置不固定（如移动便携机或无线网络），引发了IP地址变化频繁以及IP地址不足的问题。为了实现网络可以动态合理地分配IP地址给主机使用，需要用到动态主机配置协议DHCP（Dynamic Host Configuration Protocol）。
- DHCP是一种用于集中对用户进行动态管理和配置的技术。DHCP采用客户端/服务器通信模式，由客户端向服务器提出配置申请（包括IP地址、子网掩码、缺省网关等参数），服务器根据策略返回相应配置信息。DHCP技术实现了计算机快速、动态地获取IP地址功能，提高了IP地址的使用效率。
- DHCP故障的常见原因主要包括：
  - 客户端与服务器之间的链路有故障。
  - 设备未使能DHCP功能。
  - 设备VLANIF接口下没有选择DHCP分配地址的方式。
  - 当选择从全局地址池中分配IP地址时：
  - 如果客户端与服务器在同一个网段内，中间没有中继设备时，全局地址池中的IP地址与设备VLANIF接口的IP地址不在同一个网段中。
  - 如果客户端与服务器不在同一个网段内，中间存在中继设备时，全局地址池中的IP地址与中继设备的VLANIF接口的IP地址不在同一个网段中。
  - 地址池中没有可用的IP地址可分配。

DHCP Server故障 - 排障流程



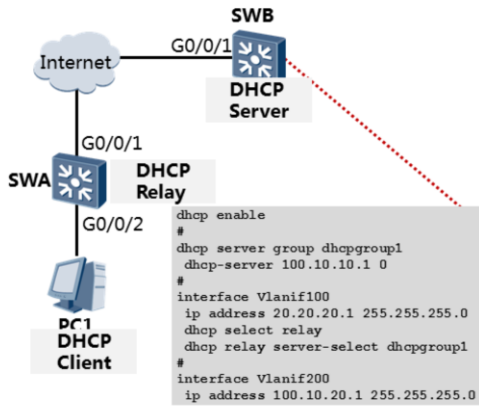
  HUAWEI

- 检查客户端与DHCP服务器之间的链路是否有故障。
  - 客户端与服务器在同一个网段内，中间没有中继设备时，在客户端与服务器连接的网卡上配置IP地址，确保该IP地址与服务器用户侧的VLANIF接口的IP地址在同一网段，从客户端Ping VLANIF接口的IP地址。 如果Ping不通，先排除链路的故障。
  - 客户端与服务器不在同一个网段内，中间存在中继设备时，分别Ping客户端与中继设备、中继设备与服务器之间的链路状态。如果Ping不通，先排除链路的故障。
- 检查DHCP功能是否处于使能状态。
  - 执行命令display current-configuration | include dhcp enable，检查DHCP功能是否已经使能。如果无任何DHCP相关显示信息，说明DHCP功能未使能，执行命令dhcp enable，使能DHCP功能。缺省情况下，DHCP功能未使能。
- 检查VLANIF接口下是否选择DHCP分配地址的方式。
  - 如果VLANIF接口下没有选择DHCP分配地址的方式，则客户端不能通过当前VLANIF接口以DHCP的方式来获取IP地址。
  - 在VLANIF接口视图下，执行命令display this，检查是否选择DHCP分配地址的方式。
    - dhcp select global：VLANIF接口已经选择全局地址池为DHCP客户端分配IP地址。
    - dhcp select interface：VLANIF接口已经选择接口地址池为DHCP客户端分配IP地址。
    - 无上述显示信息说明VLANIF接口没有选择DHCP分配地址的方式。执行命令dhcp select global或者dhcp select interface，配置VLANIF接口选择DHCP分配地址的方式。

- 检查全局地址池中的地址和接口地址是否属于同一个网段。
  - 执行命令display ip pool，查看全局地址池是否存在。
    - 如果全局地址池不存在，执行命令ip pool ip-pool-name和命令network ip-address [mask { mask | mask-length }]，创建全局地址池和配置全局地址池中可动态分配的IP地址范围。
    - 如果全局地址池存在，获取ip-pool-name参数值，执行下一步。
  - 执行命令display ip pool name ip-pool-name，查看全局地址池中的IP地址是否与VLANIF接口的IP地址在同一个网段中。
    - 客户端与服务器在同一个网段内，中间没有中继设备时，如果全局地址池中的IP地址与S2700&S3700 VLANIF接口的IP地址不在同一个网段中，则执行命令ip address ip address修改VLANIF接口的IP地址，使二者在一个网段中。
    - 客户端与服务器不在同一个网段内，中间存在中继设备时，如果全局地址池中的IP地址与中继设备的VLANIF接口的IP地址不在同一个网段中，则执行命令ip address ip address修改VLANIF接口的IP地址，使二者在一个网段中。
- 检查地址池内是否有可用IP地址。
  - 执行命令display ip pool name ip-pool-name，检查全局/接口地址池中IP地址使用情况。
  - 如果Idle（Expired）值等于零，就说明地址池中的IP地址已经用尽。
    - 如果VLANIF接口选择全局地址池为DHCP客户端分配IP地址，可以重新创建一个全局地址池，该地址池的网段不能和前一个地址池的网段重叠，但网段可以相连。
    - 如果VLANIF接口选择接口地址池为DHCP客户端分配IP地址，可以重新为VLANIF接口配置一个IP地址，该IP地址不能和前一个IP地址在同一个网段。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
  - 上述步骤的执行结果。
  - 设备的配置文件、日志信息、告警信息。

目录

DHCP Relay故障



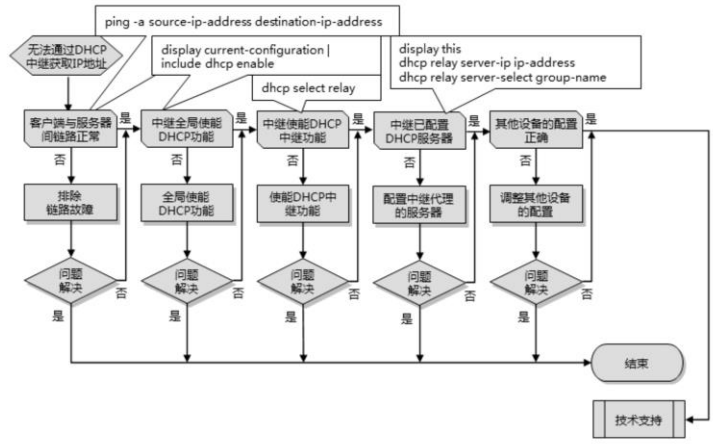
序号	配置步骤
1	配置指定接口工作在DHCP中继模式
2	配置DHCP中继转发的目的服务器组
3	配置DHCP中继接口绑定DHCP服务器组
4	（可选）配置DHCP中继请求DHCP服务器释放客户端的IP地址
5	（可选）配置DHCP中继对Option82信息的处理策略

- 客户端与DHCP服务器之间的链路有故障。
- 未全局使能DHCP功能，导致DHCP功能没有生效。
- 未使能DHCP中继功能，导致DHCP中继功能没有生效。
- DHCP中继没有配置所代理的DHCP服务器。
- 链路上其他设备配置错误。

  HUAWEI

- 当设备作为DHCP中继时，客户端可以通过DHCP中继与其他网段的DHCP服务器通信，从DHCP服务器的全局地址池中获取IP地址及其他配置信息。这样，多个网段的DHCP客户端可以使用同一个DHCP服务器，既节省了成本，又便于集中管理。
- DHCP Relay故障的常见原因主要包括：
  - 客户端与DHCP服务器之间的链路有故障。
  - 客户端与DHCP中继之间的链路有故障。
  - DHCP中继与DHCP服务器之间的链路有故障。
  - 设备未全局使能DHCP功能，导致DHCP功能没有生效。
  - 设备未使能DHCP中继功能，导致DHCP中继功能没有生效。
  - DHCP中继没有配置所代理的DHCP服务器。
  - DHCP中继没有配置所代理的DHCP服务器的IP地址。
  - DHCP中继VLANIF接口没有绑定DHCP服务器组，或者绑定的DHCP服务器组中没有配置所代理的DHCP服务器。
  - 链路上其他设备配置错误。

DHCP Relay故障 - 排障流程



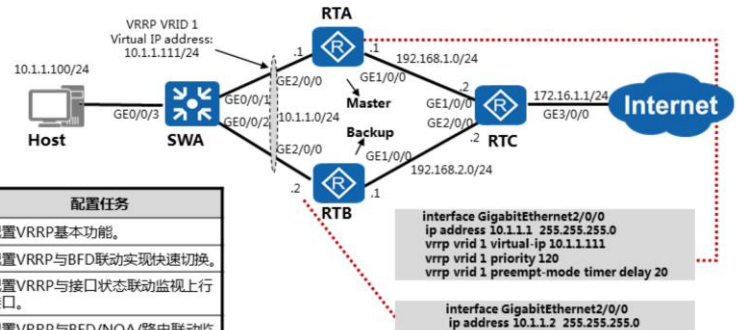
  HUAWEI

- 检查客户端与DHCP服务器之间的链路是否有故障。
  - 检查客户端与DHCP中继之间的链路是否有故障。在客户端手工配置与DHCP中继用户侧VLANIF接口位于同一网段的IP地址（不能与已经分配的IP地址冲突），然后在任一侧ping对端检查两者之间的链路是否有故障。如果Ping不通，先排除链路的故障。
  - 检查DHCP中继与DHCP服务器之间的链路是否有故障。在DHCP中继上执行命令ping -a source-ip-address destination-ip-address，source-ip-address为DHCP中继用户侧接口的IP地址，destination-ip-address为DHCP服务器的IP地址。如果Ping不通，先排除链路的故障。
- 检查DHCP中继是否全局使能DHCP功能。
  - 执行命令display current-configuration | include dhcp enable，检查DHCP功能是否已经使能。如果无任何显示信息，说明DHCP功能未使能，执行命令dhcp enable，使能DHCP功能。缺省情况下，DHCP功能未使能。
- 检查DHCP中继是否处于使能状态。
  - 如果DHCP中继未使能，则客户端无法跨网段来获取IP地址。
  - 如果同时选择了global/interface和relay功能，则设备优先选择DHCP Server角色，当DHCP Server分配IP地址失败后，则会切换到DHCP Relay角色，开始DHCP Relay功能。
  - 在VLANIF接口视图下，执行命令display this，检查DHCP中继是否处于使能状态。如果显示dhcp select relay，说明DHCP中继已经处于使能状态，如果无上述显示信息，说明DHCP中继处于未使能状态，执行命令dhcp select relay，使能DHCP中继功能。

- 检查DHCP中继是否配置了所代理的DHCP服务器。
  - 如果DHCP中继没有配置所代理的DHCP服务器，则没有DHCP服务器能够给该DHCP中继下的客户端分配IP地址。
  - 在VLANIF接口视图下，执行命令display this，检查DHCP中继是否配置了所代理的DHCP服务器。
    - 如果显示dhcp relay server-ip ip-address，说明DHCP中继已经配置了所代理的DHCP服务器。
    - 如果显示dhcp relay server-select group-name，说明DHCP中继VLANIF接口绑定了DHCP服务器组。
    - 如果无上述显示信息，说明DHCP中继没有配置DHCP服务器，从以下两种配置方法中选择一种来配置DHCP服务器：1）执行命令dhcp relay server-ip ip-address，配置DHCP中继所代理的DHCP服务器地址；2）执行命令dhcp relay server-select group-name，绑定DHCP服务器组；3）执行命令dhcp-server，在DHCP服务器组中添加DHCP服务器。
- 检查DHCP服务器组中是否配置了DHCP服务器。
  - 如果DHCP中继VLANIF接口绑定了DHCP服务器组，但是该服务器组中没有配置DHCP服务器，同样没有DHCP服务器给该DHCP中继下的客户端分配IP地址。
  - 执行命令display dhcp server group group-name，检查DHCP服务器组中是否配置了DHCP服务器。
    - 如果显示Server-IP字段，说明DHCP服务器组中配置了DHCP服务器。
    - 如果无上述显示字段，说明DHCP服务器组中没有配置DHCP服务器，执行命令dhcp-server，在DHCP服务器组中添加DHCP服务器。
- 检查链路上其他设备的配置是否正确，主要包括DHCP服务器、DSLAM、LAN Switch、客户端等设备，如不正确则修改相关配置。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
  - 上述步骤的执行结果。
  - 设备的配置文件、日志信息、告警信息。

目录

VRRP备份组震荡故障



序号	配置任务
1	配置VRRP基本功能。
2	配置VRRP与BFD联动实现快速切换。
3	配置VRRP与接口状态联动监视上行接口。
4	配置VRRP与BFD/NQA/路由联动监视上行链路。

```
interface GigabitEthernet2/0/0
 ip address 10.1.1.1  255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode timer delay 20
```

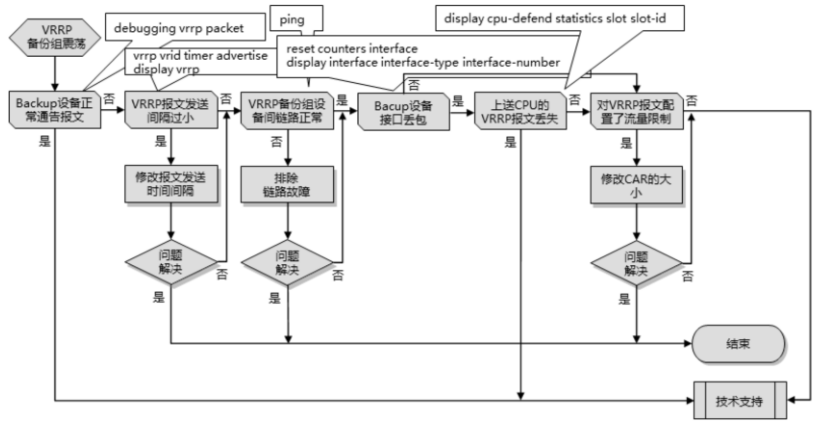
```
interface GigabitEthernet2/0/0
 ip address 10.1.1.2  255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
```

- 链路原因：
  - 传输VRRP通告报文的链路震荡。
  - 报文拥塞导致VRRP报文被随机过滤掉。
- 协议原因：
  - 通告报文的发送时间间隔过小。
- 其他原因：
  - Backup设备接口丢包。

HUAWEI

- VRRP能够在不改变组网的情况下，采用将多台路由设备组成一个虚拟路由器，通过配置虚拟路由器的IP地址为默认网关，实现默认网关的备份。当网关设备发生故障时，VRRP机制能够选举新的网关设备承担数据流量，从而保障网络的可靠通信。
- VRRP备份组震荡的可能原因有：
  - 传输VRRP通告报文的链路震荡。
  - 通告报文的发送时间间隔过小。
  - Backup设备接口丢包。
  - 报文拥塞导致VRRP报文被随机过滤掉。

VRRP备份组震荡故障 - 排障流程



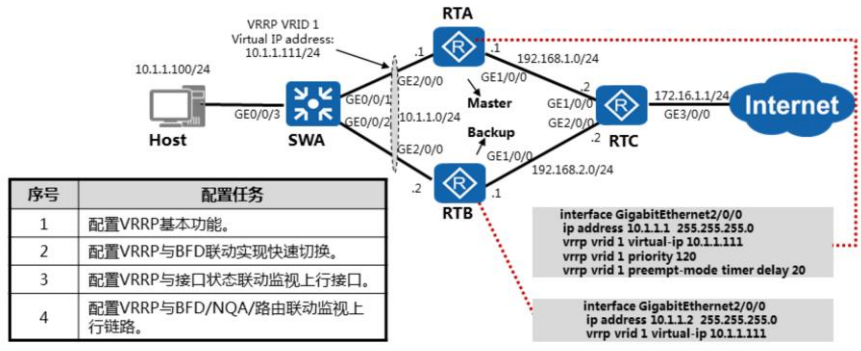
  HUAWEI

- 查看Backup设备是否接收到了VRRP通告报文。
  - 在Backup设备上执行debugging vrrp packet命令，查看是否接收到了VRRP通告报文。
  - 默认情况下，Master设备都是1秒发送1个通告报文。
- 查看是否由于VRRP通告报文发送间隔时间设置过小。
  - 执行vrrp vrid timer advertise命令，将VRRP报文发送间隔时间调大后在Backup设备上重复执行display vrrp命令查看State字段，显示信息一直保持不变说明Backup设备的状态稳定。
  - 如果Backup的状态稳定，说明可能由于时间间隔过小导致Backup设备的状态的震荡。
  - 如果Backup的状态不稳定，将时间间隔恢复。
- 查看VRRP备份组设备间的链路是否有故障。
  - 反复执行ping命令查看同一VRRP备份组实地址是否能ping通。
    - 如果ping不通，先排除链路的故障。
    - 如果时断时通，说明可能存在环路，需要进行相关环路检查。
- 查看Backup设备接口是否有丢包。
  - 执行display interface interface-type interface-number命令，通过查看端口显示信息Input和Output中的Discard字段可知端口是否存在丢包。
  - 在执行display interface命令前，先使用reset counters interface命令清除当前端口的统计信息。

- 查看上送CPU的VRRP报文是否丢失。
  - 执行display cpu-defend statistics slot slot-id命令，查看送CPU的VRRP报文是否丢失。
    - 如果显示信息中的Drop(Packets)字段不为0，说明上送CPU的VRRP报文丢失。
    - 如果显示信息中的Drop(Packets)字段为0，说明上送CPU的VRRP报文没有丢失。
- 查看是否对VRRP报文配置了流量限制。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
  - 上述步骤的执行结果。
  - 设备的配置文件、日志信息、告警信息。

目录

VRRP备份组双主故障



序号	配置任务
1	配置VRRP基本功能。
2	配置VRRP与BFD联动实现快速切换。
3	配置VRRP与接口状态联动监视上行接口。
4	配置VRRP与BFD/NQA/路由联动监视上行链路。

```
interface GigabitEthernet2/0/0
 ip address 10.1.1.1  255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode timer delay 20
```

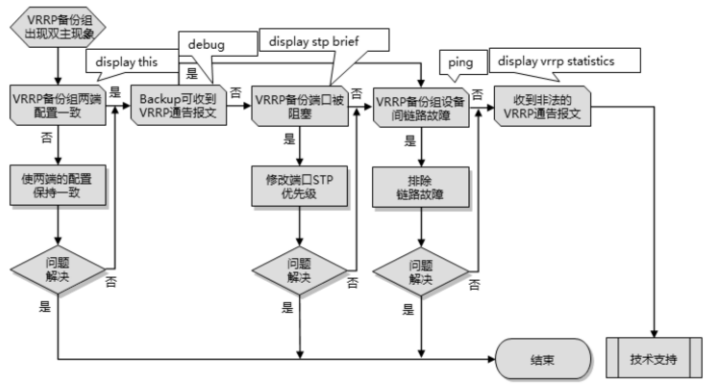
```
interface GigabitEthernet2/0/0
 ip address 10.1.1.2  255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
```

- 链路原因：
  - 传输VRRP通告报文的链路故障。
  - 链路形成环路。
- 配置原因：
  - 两端的VRRP备份组配置不一致。
- 协议原因：
  - 低优先级的VRRP备份组将收到的VRRP通告报文被作为非法报文丢弃。

HUAWEI

- VRRP备份组将两台设备虚拟成一台网关设备，虚拟网关设备具有虚拟IP地址和虚拟MAC地址，主机只感知这个虚拟网关设备的存在，以它为网关与外部进行通信。正常情况下，用户侧的流量通过Master设备转发。当Master设备出现故障时，通过VRRP协商，从Backup设备中选举出新的Master设备，继续承担流量转发工作。
- VRRP备份组双主的可能原因有：
  - 两端的VRRP备份组配置不一致。
  - 传输VRRP通告报文的链路故障。
  - 链路形成环路。
  - 低优先级的VRRP备份组将收到的VRRP通告报文作为非法报文丢弃。

VRRP备份组双主故障 - 排障流程

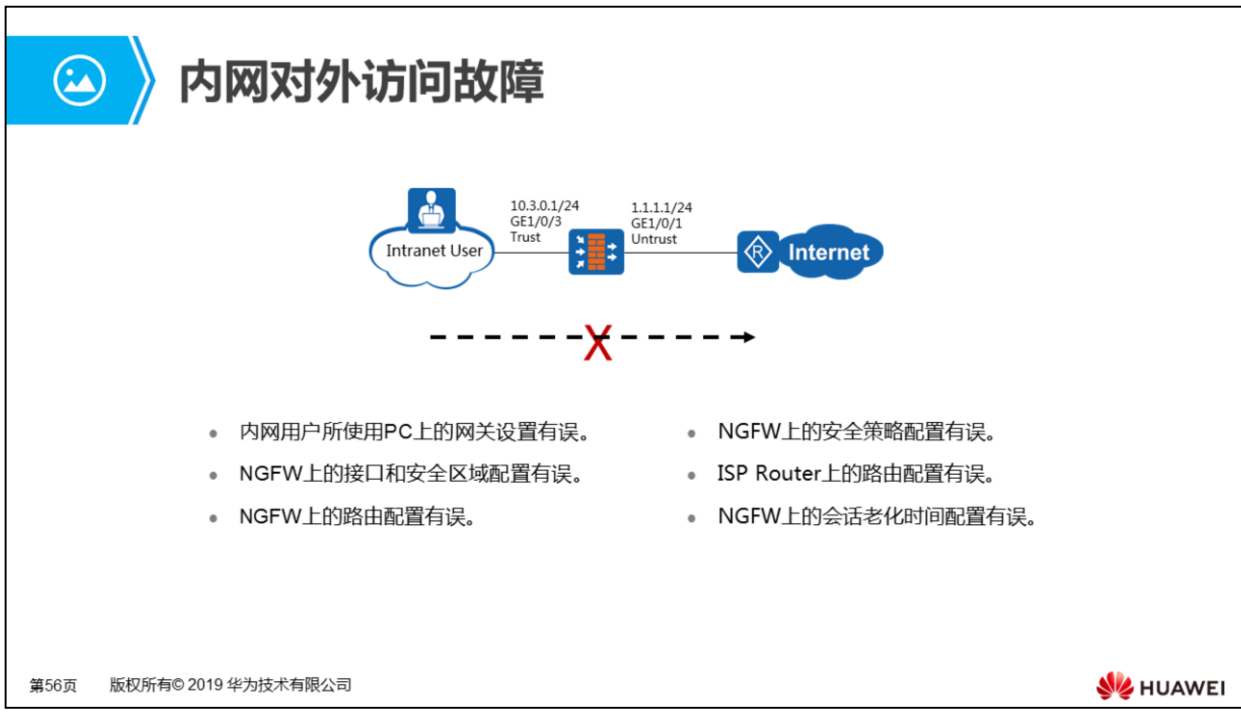


  HUAWEI

- 检查VRRP备份组两端的配置是否一致。
  - 在配置VRRP备份组两端的VLANIF接口上，执行display this命令，查看备份组两端的如下配置：
    - ip address：接口IP地址是否在同一网段，如果IP地址不在同一网段，执行ip address来修改配置。
    - vrid：接口上的备份组ID是否相同，如果不同，执行vrrp vrid virtual-router-id virtual-ip virtual-address命令修改配置。
    - Virtual IP：VRRP组的虚拟IP地址是否相同，如果不同，执行vrrp vrid virtual-router-id virtual-ip virtual-address命令修改配置。
    - TimerRun：VRRP中通告报文时间间隔是否相同，如果不同，执行vrrp vrid virtual-router-id timer advertise adver-interval命令修改配置。
    - Auth Type：VRRP报文认证方式是否相同，如果不同，执行vrrp vrid virtual-router-id authentication-mode { simple key | md5 md5-key }命令修改配置。
- 查看Backup设备是否能够收到VRRP通告报文。
  - 打开Backup设备的debug开关，查看是否有如下显示信息。
    - *Aug 27 19:45:04 2010 Quidway VRRP/7/DebugPacket:
    - Vlanif45 | Virtual Router 45:receiving from 45.1.1.4, priority = 100,timer = 1,
    - auth type is no, SysUptime: (0,121496722)
  - 默认情况下Master设备都是1秒发送1个通告报文。

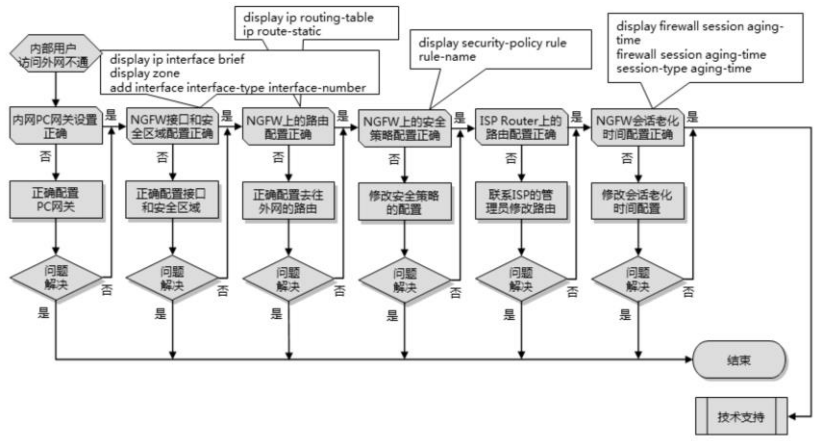
- 在配置VRRP备份组两端设备及传输VRRP通告报文的所经过的设备上，检查是否有端口被阻塞。
  - 执行display stp brief命令，查看STP State字段。
    - 如果STP State字段的值为FORWARDING，说明端口没有被阻塞。
    - 如果STP State字段的值为DISCARDING，说明端口被阻塞，修改端口STP优先级以保证互连端口能够正常进行VRRP协议报文转发。
- 执行ping命令查看VRRP备份组设备间的链路是否有故障。
  - 如果ping不通，先排除链路的故障。
- 查看低优先级的VRRP备份组是否收到了非法的VRRP通告报文。
  - 执行display vrrp statistics命令，查看Received invalid type packets字段，记录收集到的信息。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
  - 上述步骤的执行结果。
  - 设备的配置文件、日志信息、告警信息。

目录



- NGFW可以作为企业的出口网关，部署在网络边界处。企业内部网络中的用户通过NGFW提供的NAT功能来访问Internet。配置完成后，如果发现企业内部网络中的用户不能访问Internet，可能的原因有：
  - 内网用户所使用PC上的网关设置有误。
  - NGFW上的接口和安全区域配置有误。
  - NGFW上的路由配置有误。
  - NGFW上的安全策略配置有误。
  - ISP Router上的路由配置有误。
  - NGFW上的会话老化时间配置有误。

内网对外访问故障 - 排障流程



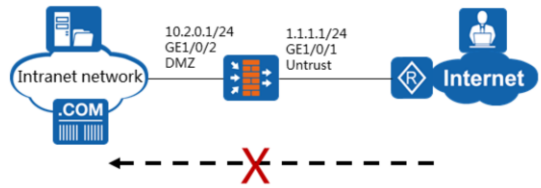
  HUAWEI

- 检查PC的网关是否设置为NGFW连接内部网络的接口的IP地址。
- 检查NGFW上连接内部网络和Internet的接口是否配置了正确的IP地址并加入安全区域。
  - 在NGFW的CLI环境中使用display ip interface brief命令查看接口是否配置了正确的IP地址。
  - 检查IP Address一列的信息，如果配置有误，在接口视图下使用ip address ip-address mask命令重新配置IP地址。
  - 使用display zone命令查看接口是否正确的加入安全区域。
  - 如果配置有误，在安全区域视图下使用add interface interface-type interface-number命令将接口加入安全区域。
- 检查NGFW上是否存在去往Internet的路由。
  - 在NGFW的CLI环境中使用display ip routing-table命令查看路由表项。
  - 如果配置有误，请使用ip route-static命令重新配置路由。
- 检查NGFW上配置的安全策略以及安全策略所引用的配置文件是否正确。

    - 在NGFW的CLI环境中使用display security-policy rule rule-name命令查看安全策略的配置信息。
    - 检查安全策略的匹配条件是否可以正确匹配到用户发出的流量，同时查看安全策略的动作是否为permit。如果配置有误，在安全策略规则视图下使用source-address命令调整安全策略规则的源地址，或者使用命令action调整安全策略规则的动作。
    - 如果安全策略中引用了内容安全的配置文件，使用display profile type { app-control | av | data-filter | file-block | ips | mail-filter | url-filter } name name命令查看内容安全配置文件的配置信息，是否将用户发出的流量阻断。如果阻断，则调整安全配置文件的配置。
- 联系ISP的网络管理员，检查ISP Router上是否配置了去往NGFW的路由。如果配置有误，联系ISP的网络管理员修改路由。
- 检查NGFW上的会话老化时间配置。
    - 用户使用某种业务访问Internet中的服务器，用户与服务器之间通过交互报文来防止连接因为无数据传输而中断。在NGFW的CLI环境中使用display firewall session aging-time查看会话表的老化时间，如果发现承载该业务的协议的老化时间小于服务器发送响应报文的时间间隔，那么响应报文还未到达NGFW，会话表就已经老化，服务器的响应报文因为不能命中会话而被丢弃。
    - 在NGFW的CLI环境中使用firewall session aging-time session-type aging-time命令适当增大相应协议的老化时间。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
    - 上述步骤的执行结果。
    - 设备的配置文件、日志信息、告警信息。

目录

外网对内访问故障

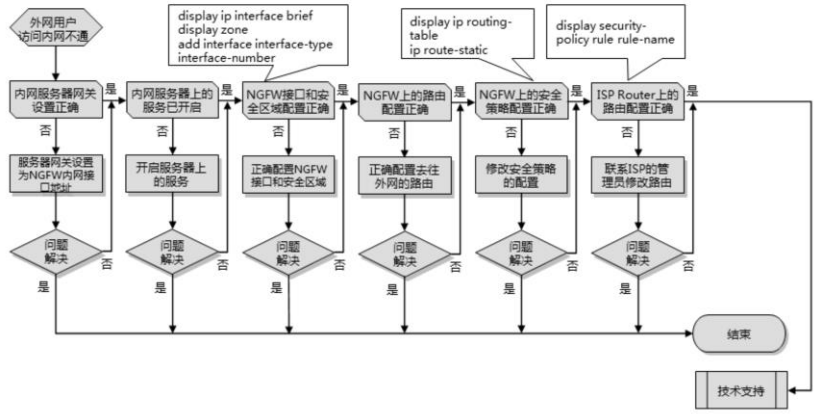


- 内网服务器上的网关设置有误。
- 内网服务器上的服务没有开启。
- NGFW上的接口和安全区域配置有误。
- NGFW上的路由配置有误。
- NGFW上的安全策略配置有误。
- ISP Router将报文丢弃。

HUAWEI

- 如果发现企业内部网络中的用户不能访问Internet，可能的原因有：
  - 内网服务器上的网关设置有误。
  - 内网服务器上的服务没有开启。
  - NGFW上的接口和安全区域配置有误。
  - NGFW上的路由配置有误。
  - NGFW上的安全策略配置有误。
  - ISP Router将报文丢弃。

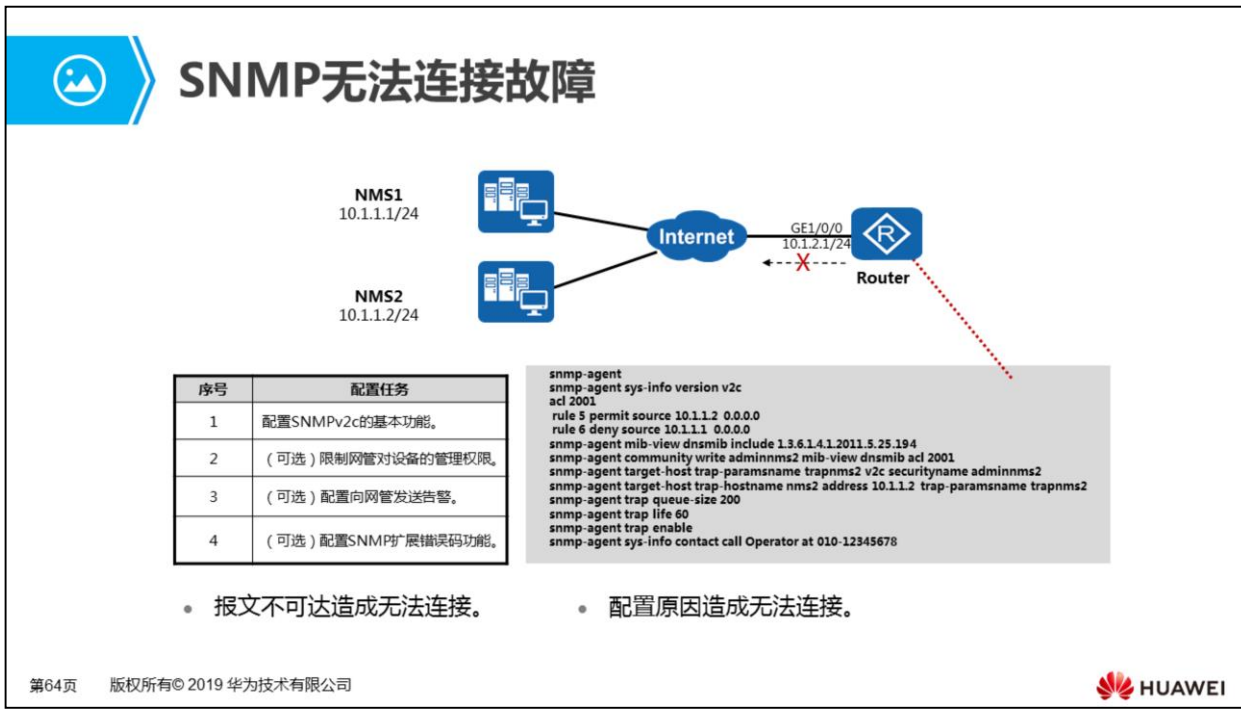
外网对内访问故障 - 排障流程



- 检查内网服务器的网关是否设置为NGFW连接内部网络的接口的IP地址。
- 检查内网服务器上的服务是否开启。
- 检查NGFW上连接内部网络和Internet的接口是否配置了正确的IP地址并加入安全区域。
  - 在NGFW的CLI环境中使用display ip interface brief命令查看接口是否配置了正确的IP地址。如果配置有误，则在接口视图下使用ip address ip-address mask命令重新配置IP地址。
  - 使用display zone命令查看接口是否正确的加入安全区域。如果配置有误，则在安全区域视图下使用add interface interface-type interface-number命令将接口加入安全区域。
- 检查NGFW上的路由配置。
  - 在NGFW的CLI环境中使用display ip routing-table命令查看路由表项。如果配置有误，使用ip route-static命令重新配置路由。
- 检查NGFW上配置的安全策略以及安全策略所引用的配置文件是否正确。
  - 在NGFW的CLI环境中使用display security-policy rule rule-name命令查看安全策略的配置信息。
  - 检查安全策略的匹配条件是否可以正确匹配到外网用户访问内网服务器的流量，此处的目的地址应该是内网服务器的私网地址，同时查看安全策略的动作是否为permit。如果配置有误，则在安全策略规则视图下使用source-address命令调整安全策略规则的源地址，或者使用命令action调整安全策略规则的动作。
  - 如果安全策略中引用了内容安全的配置文件，使用display profile type { app-control | av | data-filter | file-block | ips | mail-filter | url-filter } name name命令查看内容安全配置文件的配置信息，是否将外网用户与内网服务器之间的流量阻断。

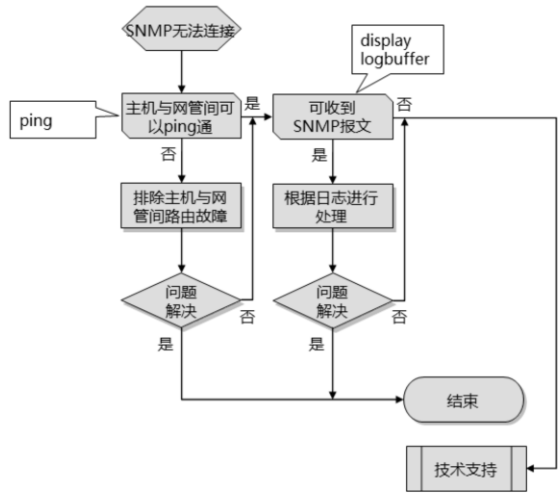
    - 如果阻断，则应调整安全配置文件的配置。
- 联系ISP的网络管理员，检查ISP Router上是否过丢弃了外网用户访问内网服务器的报文。如果报文被ISP Router丢弃，应联系ISP的网络管理员处理。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
    - 上述步骤的执行结果。
    - 设备的配置文件、日志信息、告警信息。

目录



- 简单网络管理协议SNMP是广泛用于TCP/IP网络的网络管理标准协议。SNMP提供了一种通过运行网络管理软件的中心计算机（即网络管理工作站）来管理网元的方法。共有三个版本SNMPv1、SNMPv2c和SNMPv3，用户可以根据情况选择配置一个或多个版本。
- 要在组网中配置SNMP协议，需要在管理端配置SNMP管理程序NMS，同时在被管理设备端配置SNMP代理程序Agent。网络管理系统NMS可以通过Agent在任何时候及时地获得设备的状态信息，实现远端控制被管理设备；Agent可以及时地向NMS报告设备的当前状态信息。
- SNMP无法连接故障的常见原因主要包括：
  - 报文不可达造成无法连接。
  - 配置原因造成无法连接。

SNMP无法连接故障 - 排障流程

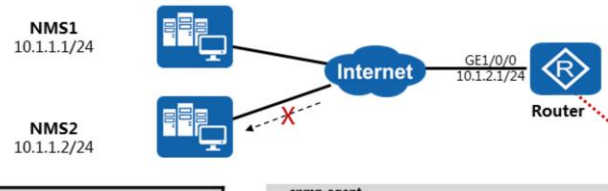


  HUAWEI

- 执行ping命令查看主机和网管之间是否可以Ping通。
  - 如果可以Ping通，说明主机和网管之间有可达的路由。
  - 如果无法Ping通，先排除链路的故障。
- 执行display logbuffer命令查看主机上是否有提示登录失败的日志。
  - Failed to login through SNMP, because the version was incorrect. (Ip=[STRING], Times=[ULONG])（主机不支持网管发送登录请求所使用的SNMP协议版本）。
    - 执行display snmp-agent sys-info version命令查看主机是否支持网管发送登录请求所使用的SNMP协议版本。
    - 执行snmp-agent sys-info version命令配置主机所支持的SNMP协议版本。
  - Failed to login through SNMP, because the packet was too large. (Ip=[STRING], Times=[ULONG])（设备接收到的报文超过设备所设置的阈值）。
    - 执行snmp-agent packet max-size命令增大报文阈值。
  - Failed to login through SNMP, because the community was incorrect. (Ip=[STRING], Times=[ULONG])（团体字配置错误）。
    - 执行display snmp-agent community命令查看主机配置的团体字。
    - 执行snmp-agent community命令配置读写团体名，使之与网管端配置一致。
  - Failed to login through SNMP, because of the ACL filter function. (Ip=[STRING], Times=[ULONG])（该IP被ACL禁止）。
    - 执行display acl命令查看主机ACL配置，如果网管端发送请求所使用的IP被ACL禁止访问，则执行rule命令配置允许网管端IP访问主机。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
  - 上述步骤的执行结果。
  - 设备的配置文件、日志信息、告警信息。

目录

收不到SNMP告警故障



序号	配置任务
1	配置SNMPv2c的基本功能。
2	（可选）限制网管对设备的管理权限。
3	（可选）配置向网管发送告警。
4	（可选）配置SNMP扩展错误码功能。

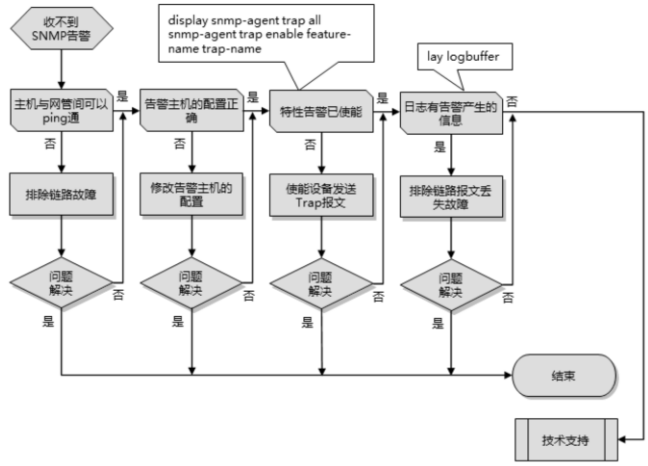
```
snmp-agent
snmp-agent sys-info version v2c
acl 2001
 rule 5 permit source 10.1.1.2  0.0.0.0
 rule 6 deny source 10.1.1.1  0.0.0.0
snmp-agent mib-view dnsmib include 1.3.6.1.4.1.2011.5.25.194
snmp-agent community write adminnms2 mib-view dnsmib acl 2001
snmp-agent target-host trap-paramsname trapnms2 v2c securityname adminnms2
snmp-agent target-host trap-hostname nms2 address 10.1.1.2  trap-paramsname trapnms2
snmp-agent trap queue-size 200
snmp-agent trap life 60
snmp-agent trap enable
snmp-agent sys-info contact call Operator at 010-12345678
```

- 报文丢失。
- 主机侧SNMP配置错误。
- 主机侧业务模块没有产生告警，或者产生的告警格式错误。

HUAWEI

- 收不到SNMP告警故障的常见原因主要包括：
  - 报文丢失造成网管主机无法接收到这条告警。
  - 主机侧SNMP配置错误，造成告警无法发送。
  - 主机侧业务模块没有产生告警，或者产生的告警格式错误导致告警无法发送。

收不到SNMP告警故障 - 排障流程



- 确保主机与网管间可以ping通。
- 检查设备上告警主机的配置是否正确。 如果告警主机配置错误，参考产品文档的配置说明进行修改。
- 查看告警的使能情况。
  - 执行display snmp-agent trap all命令查看到所有特性下的告警的使能情况。如果特性告警没有使能，执行snmp-agent trap enable feature-name trap-name命令使能设备发送Trap报文，并设置Trap的相关参数。
- 取主机上的日志，检查是否有告警产生的信息。如果存在期望获取的告警的记录，说明告警已经产生但是网管没有收到，则需要查看链路上是否存在报文丢失的情况。
- 如果执行完上述操作后故障仍然存在，则收集如下信息，并联系上级支持工程师。
  - 上述步骤的执行结果。
  - 设备的配置文件、日志信息、告警信息。

思考题

1. 下述哪些原因可能引起BGP邻居关系故障？

   A. ACL过滤了TCP的179端口。

   B. 邻居的Router ID冲突。

   C. 用Loopback口建立EBGP邻居未配置peer ebgp-max-hop。

   D. 用Loopback口建立邻居时没有配置peer connect-interface。

- 1、答案：ABCD。


谢 谢
www.huawei.com

网络故障排除场景案例

HUAWEI

前言

- 本章主要包括网络故障排除场景案例课程推荐采用的教学步骤、场景案例的拓扑设计、待排故障的描述等内容。
- 本章最后的附件列表中包括了排障案例答案、eNSP模拟器拓扑文件、以及场景案例的故障点设置说明等文件，可供学员和教师参考使用。

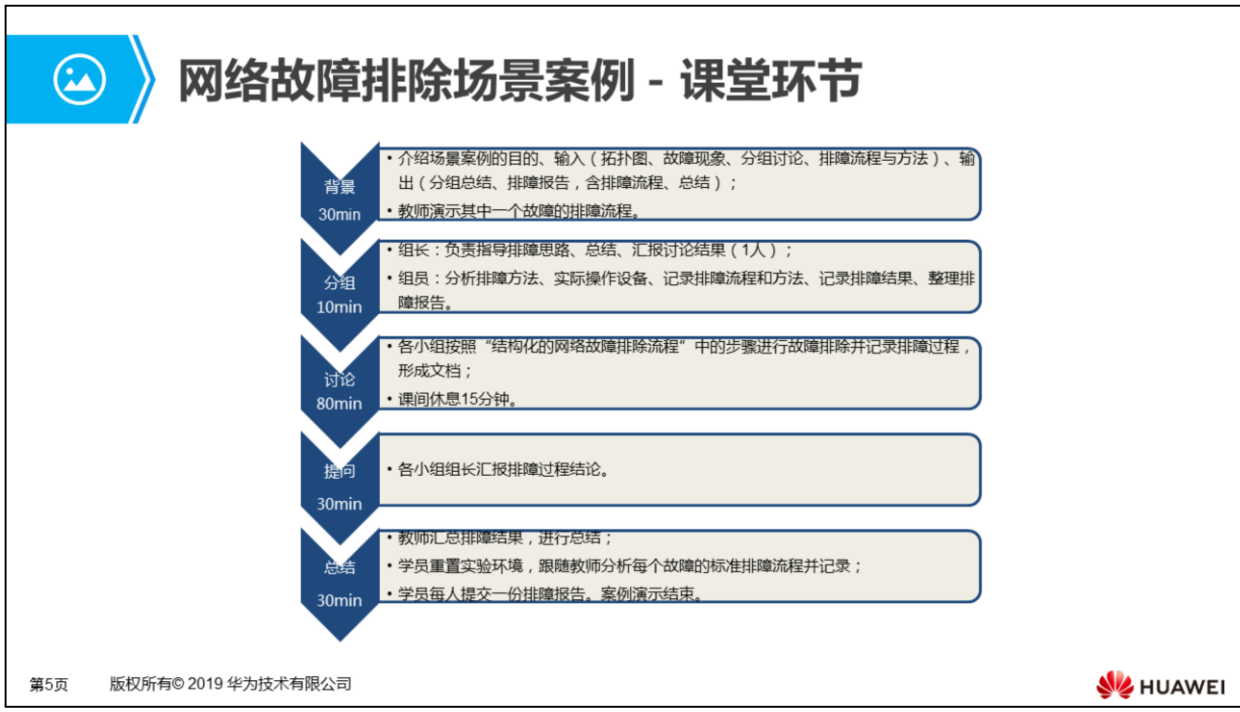
目标

- 通过网络故障排除的实际演练，掌握如何灵活应用各种网络故障排除方法。

目录

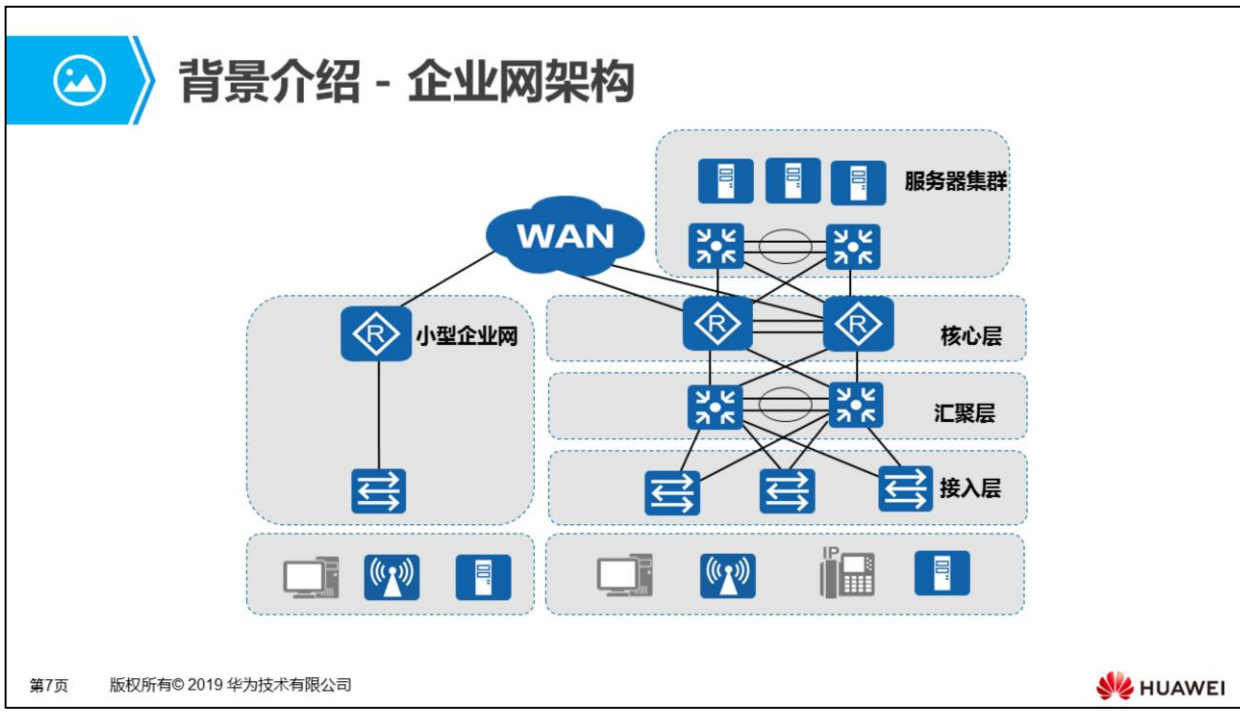
网络故障排除场景案例 - 注意事项

- 教师会根据课堂进度提出若干故障报告。
- 重点是通过实践来掌握排障的流程和方法，而不是追求能在最短的时间内排除多少故障。
- 排障操作必须得到授权、必须写排障文档。保证每个排障操作都按照流程进行、都留有记录。
- 排障的要求并不是必须独立的现场解决故障，而是通过清晰的排障思路最快的定位到故障点。定位到某台设备后，对自己无法解决的故障应及时请求高级工程师或服务提供商、厂商（课堂上为教师）的协助。



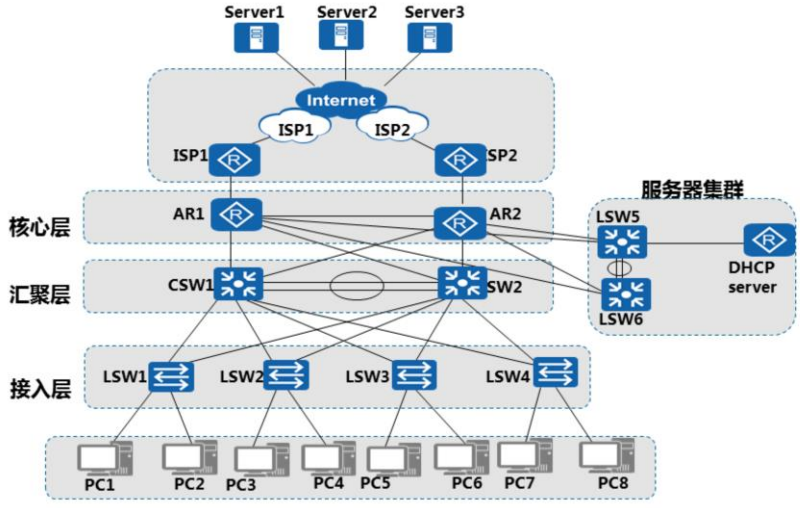
- 每个案例共90分钟，4个故障点。

目录



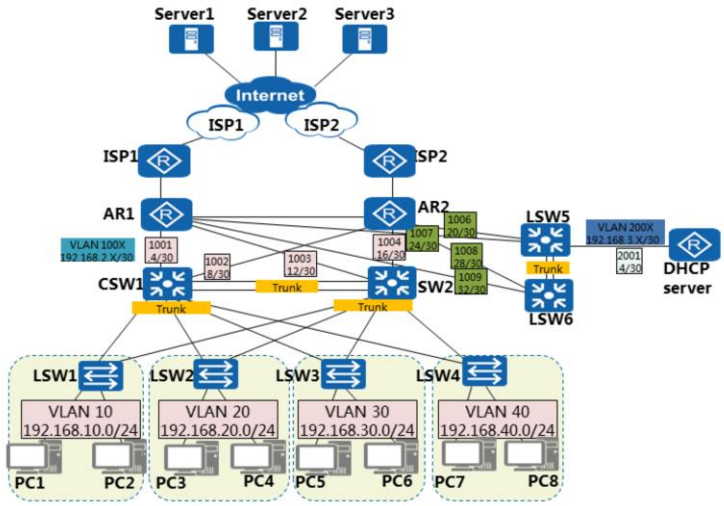
- 企业网络架构很大程度上取决于企业或机构的业务需求。小型企业通常只有一个办公地点，一般采用扁平网络架构进行组网。这种扁平网络能够满足用户对资源访问的需求，并具有较强的灵活性，同时又能大大减少部署和维护成本。小型企业网络通常缺少冗余机制，可靠性不高，容易发生业务中断。
- 大型企业网络对业务的连续性要求很高，所以通常会通过网络冗余备份来保证网络的可用性和稳定性，从而保障企业的日常业务运营。大型企业网络也会对业务资源的访问进行控制，所以通常会采用多层网络架构来优化流量分布，并应用各种策略进行流量管理和资源访问控制。多层网络设计也可以使网络易于扩展。大型企业网络采用模块化设计能够有效实现网络隔离并简化网络维护，避免某一区域产生的故障影响到整个网络。

背景介绍 - 网络架构



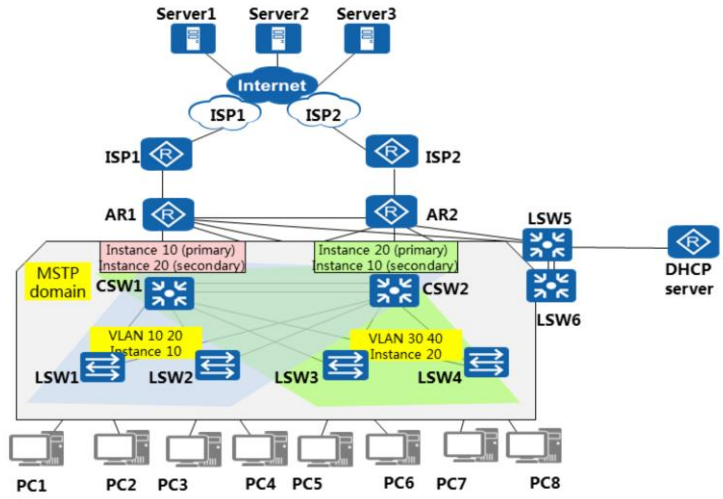
HUAWEI

背景介绍 - VLAN设计



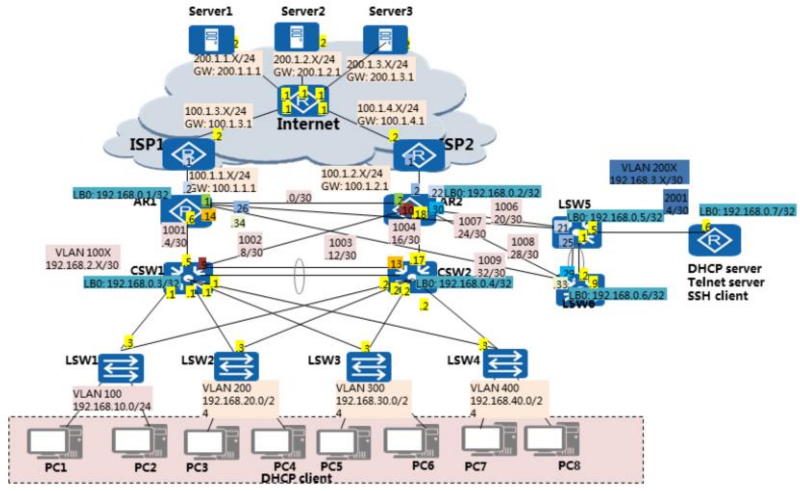
HUAWEI

背景介绍 - MSTP设计

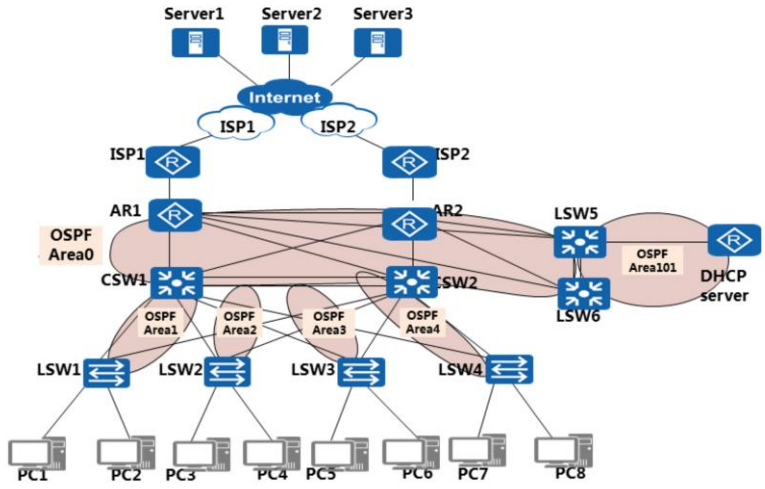


HUAWEI

背景介绍 - IP地址设计

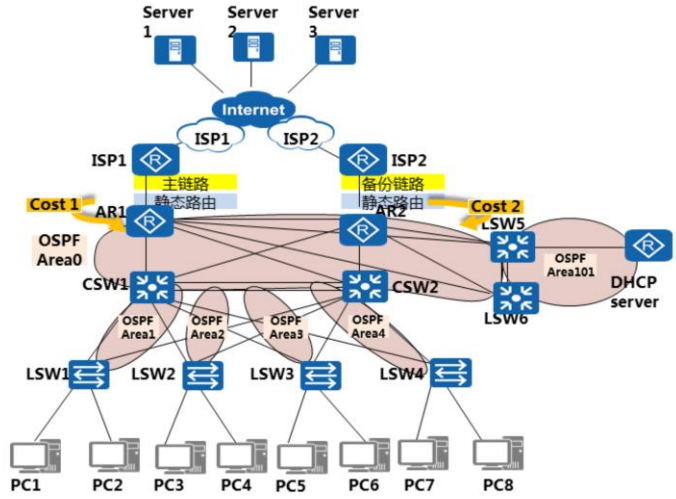


背景介绍 - 内网路由设计



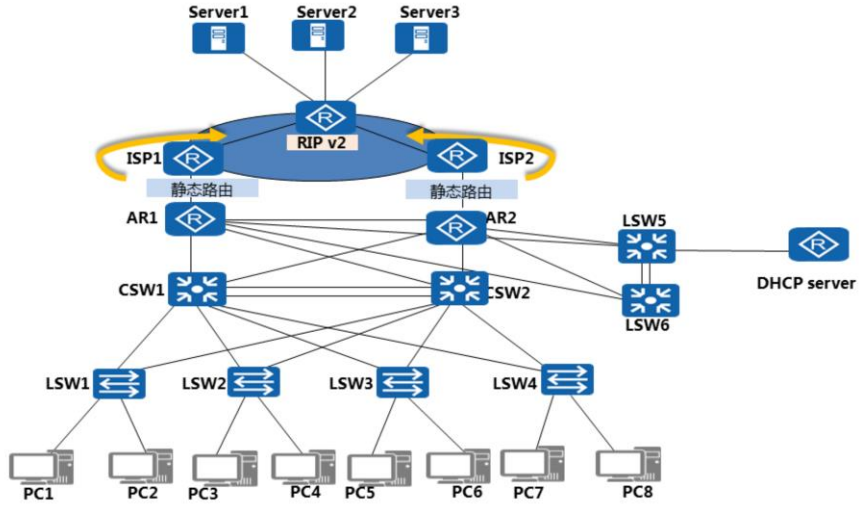
HUAWEI

背景介绍 - 出口路由设计



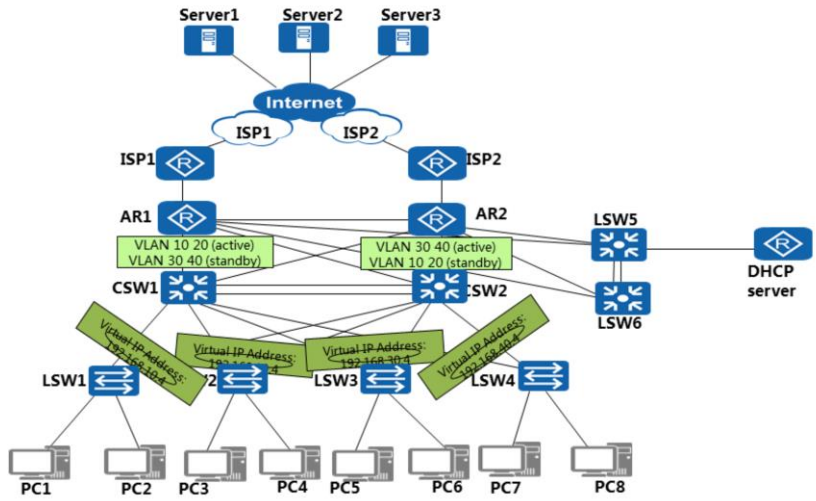
HUAWEI

背景介绍 - WAN模拟



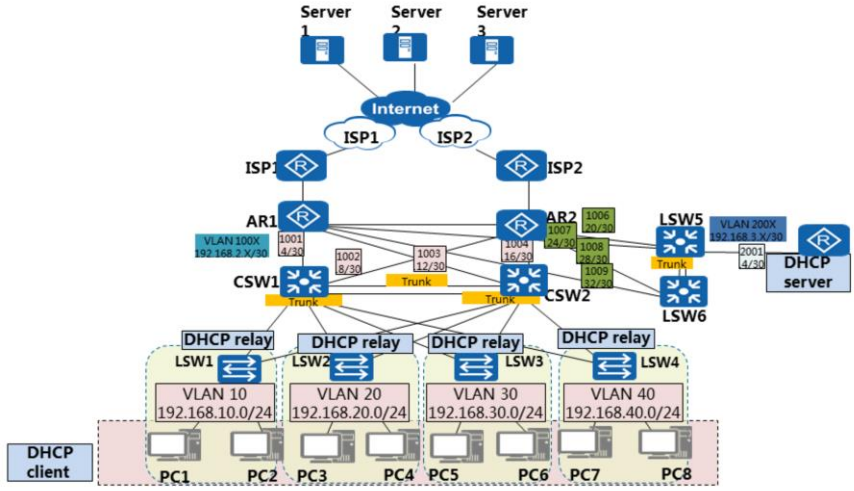
HUAWEI

背景介绍 - VRRP设计



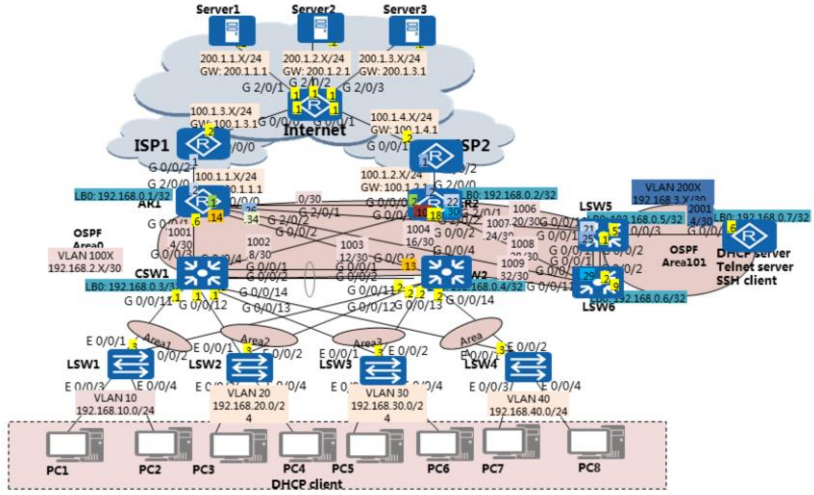
HUAWEI

背景介绍 - DHCP设计



HUAWEI

背景介绍 -拓扑总览



目录

场景案例1 - 待排故障

- 公司换了两家新的ISP服务商，周末进行了线路切换。不排除网络管理员对网络做了其他操作。
- 周一的上午，你在办公座位接到电话，一名公司的员工说他无法通过终端（PC7）访问互联网（Server1）。

场景案例2 - 待排故障

- 周日，网络管理员在进行设备维护操作的时候，发现如果断开LSW3与CSW2的连接线缆，PC5的用户无法正常访问互联网（Server1）。
- 经过周日的网络维护后，用户报告说访问互联网的速度变得很慢。现在希望你能找出故障的根源，并排除这个故障。

目录

HUAWEI

附件列表

文件说明		文件列表
场景案例1	eNSP模拟器拓扑文件，已预配故障点。	场景案例1模拟器拓扑.rar
	场景案例1参考答案。	场景案例1参考答案.rar
场景案例2	eNSP模拟器拓扑文件，已预配故障点。	场景案例2模拟器拓扑.rar
	场景案例2参考答案。	场景案例2参考答案.rar
学生排障报告	网络故障排除报告（模板）。	网络故障排除报告（模板）.rar
故障点设置说明（场景案例设计过程，供教师参考）	eNSP模拟器拓扑文件（无故障的正常网络。已预配置）。	模拟器拓扑.rar
	网络基础配置与故障点设置。	网络基础配置与故障点设置.rar

思考题

1. 在结构化的网络故障排除流程的确认故障阶段中，下列哪项说法是正确的？

   A. 应关注如何更好的解决故障，而不论该故障是否属于自己的负责范围。

   B. 应重视用户的意见，以用户的判断为依据来判断故障问题。

   C. 应使影响最小化，尽量不让其他人知道网络出现了故障。

   D. 应确认排障工作是否属于自己的负责范围。

- 1、答案：D。


谢 谢
www.huawei.com

网络优化

HUAWEI

前言

- 用户的业务在不断发展，因此用户对网络功能的需求也会不断变化。当现有网络不能满足业务需求，或网络在运行过程中暴露出了某些隐患时，就需要通过网络优化来解决。
- 与新建网络不同，网络优化基于现有的正在运行的网络，在优化方案设计和实施上有许多需要注意的地方。
- 本课程将介绍网络优化的基本概念，并以安全性和用户体验的优化为例，介绍网络优化的典型思路和方法。

目标

- 学完本课程后，您将能够:
  - 了解网络优化专业服务的内容
  - 了解常见的网络优化思路
  - 掌握提升网络的安全性的方法
  - 掌握提升网络的用户体验的方法
  - 熟悉网络优化方案包含的内容

目录

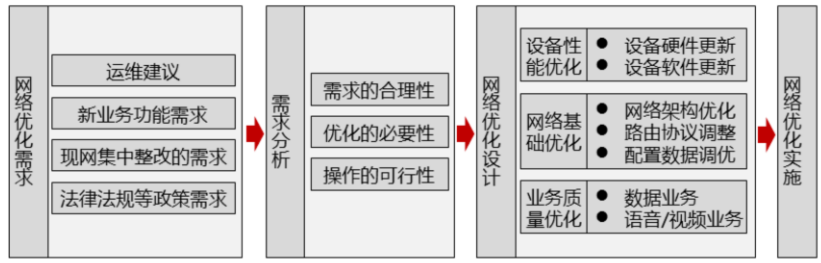
网络优化概述

- 网络优化的目的是提升网络的性能、增强网络安全性以及提升网络的用户体验。
- 网络优化主要包括：
  - 硬件优化。
  - 软件优化。
  - 网络扩容。
  - 新技术更新。

- 网络优化是指通过各种硬件或软件技术使网络性能达到我们需要的最佳平衡点。网络优化主要包括硬件优化、软件优化、网络扩容和新技术更新。
  - 硬件优化指在合理分析对新硬件的需求后在性能和价格方面作出最优解决方案。
  - 软件优化指对软件的参数进行设置，从而使系统性能达到最优的过程。
  - 网络扩容是指在原有网络的基础上，增加新的网络建设项目，包括设备的替换、设备的增加、组网改变等等。
  - 新技术更新是指将原有网络中的全部或部分技术更替的过程。
- 网络优化可以看作是一个新的项目进入新的PDIOI循环。

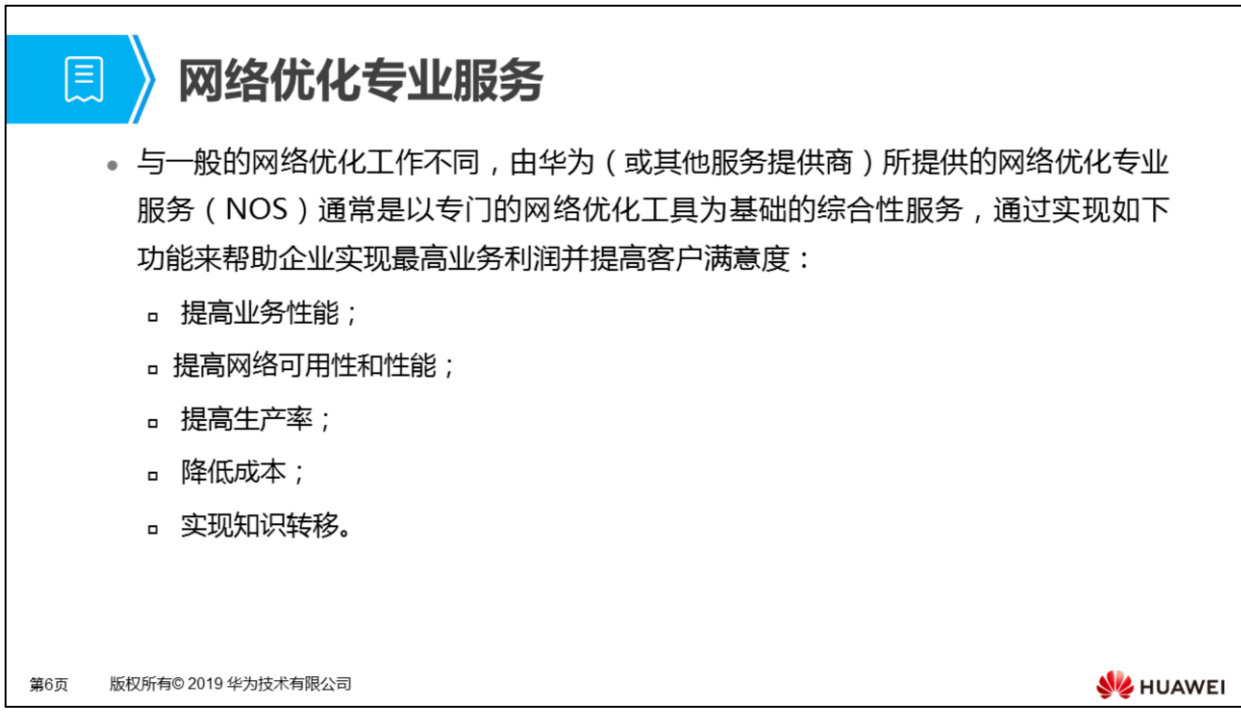
网络优化思路

- 通过网络优化，能够整体提升网络的可靠性、健壮性，更好的支撑企业业务的发展。



HUAWEI

- 网络优化的需求来源主要有：运维建议、新业务功能需求、现网问题集中整改、法律法规政策需求等。
  - 运维建议：经过一段时间的网络维护工作后，总结所遇到的问题，从而进行集中的整改。
  - 新业务功能需求：例如网络中需要开展视频会议业务（会导致二层网络组播报文太多），需要增加支持二层组播功能的交换设备来优化网络性能（当然，交换机开启igmp-snooping功能可以减少泛洪，但是也会增加设备的负担，这需要在实际部署中进行综合考虑）。
  - 现网问题集中整改：如某弱电井因环境问题导致信号线老化严重，需要集中更换。
  - 法律法规问题需求，如因企业信息安全需要，需要增加新的安全设备等。
- 需求分析主要包括：
  - 需求的合理性：网络优化的需求是否匹配实际的业务需求和投入产出比。
  - 优化的必要性：是否是紧急且必要的需求。
  - 操作的可行性：现网条件下的可操作性、政策的可行性分析。
- 在对网络优化的需求进行分析后，可以进行网络优化设计，并根据设计方案实施网络优化，从而做到：
  - 提高网络安全性：如满足企业增加边界网关的安全需求。
  - 提升网络的用户体验：如对网络的流量进行服务质量优化，提高VOIP业务的通信质量。
  - 增加网络功能：如企业增加WIFI功能，全网部署WLAN组网。



- 华为网络优化服务（NOS）是一个综合性服务，致力于优化网络的性能、可扩展性和可用性，帮助企业实现最高业务利润并提高客户满意度。
- 提高业务性能：
  - 提高企业的网络可用性和服务质量，进而提高了企业的竞争优势。
  - 帮助企业聚焦于网络核心竞争力，实现长短期的业务战略目标。
- 提高网络可用性和性能：
  - 确保持续的容量规划管理支持，提高网络可用性。
  - 采用最佳实践经验，在不影响网络可用性的同时，加速应用领先的网络解决方案。
- 提高生产率：
  - 利用华为在业界累积的经验和相关软硬件设备或工具，主动解决性能规划、可用性和优化问题，大幅度延长正常运行时间，提高生产率。
- 降低成本：
  - 通过规划和维护网络，获得网络的最佳可用性，最大限度地降低硬件升级和网络重新设计的成本。
  - 通过专家级的支持和维护，大幅度延长网络正常运行时间和使用周期、提高性能。
  - 缩短企业的网络运维人员所需培训时间。
- 实现知识转移：
  - 通过培训确保负责维护企业网络的员工及时了解新的网络技术和解决方案，同时，通过经验和技术的积累，在提升网络运维能力的同时，也能够提升网络部门自己的核心竞争力。

网络优化专业服务内容

- 核心价值：旨在全面提升企业网络的核心竞争力，从而使企业在业务领域取得优势地位。

HUAWEI

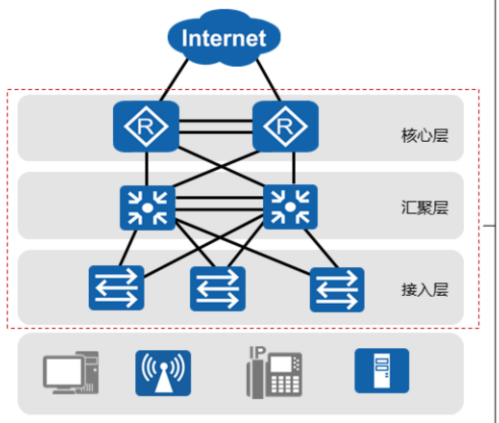
- 华为网络优化服务（NOS）的核心价值旨在全面提升企业网络的核心竞争力，从而使企业在业务领域取得优势地位。
- 客户技能需求：
  - 网络知识转移：
    - 网络知识转移服务就是基于客户运维自己的网络所需要的知识，加上华为在全球的网络运维和建设经验，而提供给客户的知识转移服务。
- 网络级别需求：
  - 网络架构评估：
    - 华为的技术专家采用业界领先的最佳经验为客户审核全网架构的合理性、安全性和可扩展性，并根据评估结果提出改进建议。
  - 网络可用性评估：
    - 通过对客户网络进行可用性评估分析，给出网络可用性的指标体系，建立适合客户使用的网络可用性模型，并探讨持续改进可用性的流程与方法。
  - 专家技术保障：
    - 华为技术专家通过过硬的故障处理能力和强大的技术支持团队，可以在最快的时间内帮助客户解决业务异常时存在的问题，从而避免影响业务。同时在特定

        - 时段提供驻场技术支持服务。

- 网元级别需求：
    - 生命周期评估：
        - 定期检查和分析现网设备的软硬件生命周期，对将处于停止销售生产、停止软件更新及停止技术支持的产品做相应的应对措施。防止由于生命周期原因引起的运行风险。
    - 软件评估推荐：
        - 针对服务期内甲方所用的所有软件平台进行评估分析，并结合评估情况推荐软件版本，避免因已知BUG导致异常事件的发生。
    - 网络健康检查：
        - 网络健康检查的目的是帮助用户从网络技术角度对本身正在运行的网络系统的技术特征、故障隐患有一个全面的了解，以便根据业务发展需求和目前网络资源状况，制订合理、可行的网络扩容、改造及维护计划，提高网络生产的安全性。
    - 配置评估优化：
        - 根据客户要求开发并定期持续维护设备配置模板。结合定期软件评估推荐的结果，将相关使用的软件特性具体到相应推荐目标版本的命令行，实现配置的精细化管理。

目录

提升网络安全性

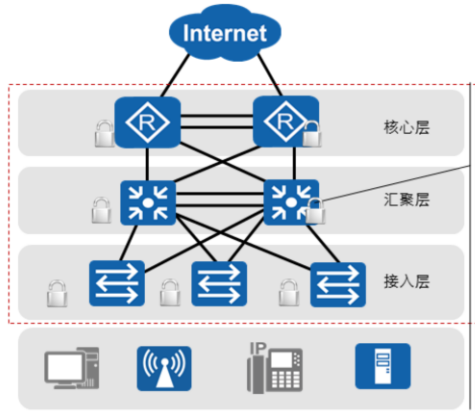


- 网络安全是一个系统性问题：
  - 涉及全网所有设备；
  - 涉及到安全管理。
- 网络安全包括若干子项：
  - 管理安全；
  - 边界安全；
  - 访问控制；
  - 接入安全；
  - 流量监控。

HUAWEI

- 提升网络的安全性，主要从以下几个方面考虑：
  - 管理安全；
  - 边界安全；
  - 访问控制；
  - 接入安全；
  - 流量监控。

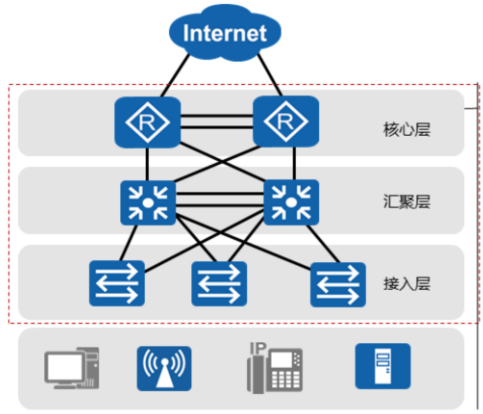
管理安全优化



- 管理安全优化：
  - 目的：保障敏感的管理信息不被非法窃取。
  - 位置：所有设备。
  - 手段：采用安全强度高的协议和完善的管理制度。

- 这里的管理安全不是指管理制度，而是指在技术层面上保障管理手段的安全。安全管理制度不在此讨论。如某企业希望增强网络设备管理的安全性，防止非网管人员恶意访问网络设备、修改配置等。为了实现该需求，需要完善网络安全管理制度，增加网络设备访问控制的安全策略。

边界安全优化

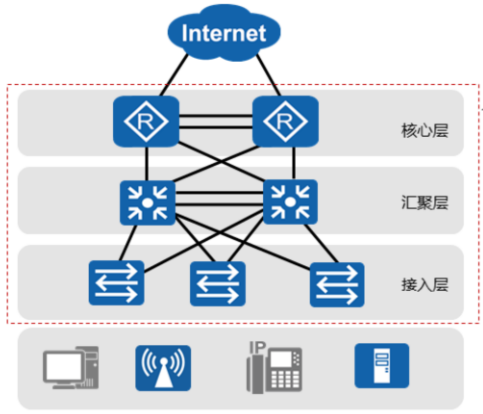


- 网络边界安全优化：
  - 目的：为了防止和减少外部网络的攻击和危害。
  - 位置：网络边界。
  - 手段：攻击防范技术、包过滤技术、硬件防火墙。

HUAWEI

- 网络边界安全优化主要是指保护网络内部的资源（包括网络设备和信息资产）和用户终端不受到来自外部的攻击危害。如某企业的内部服务器经常受外部的DDoS攻击，为了防止此类攻击，应该在网络边界部署防御措施，像增加防火墙设备或其它防护策略等。

访问控制优化

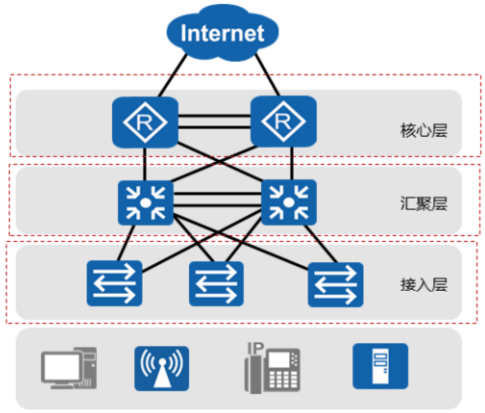


- 访问控制优化：
  - 目的：保证关键业务的访问安全。
  - 位置：网络各个层面均可能涉及。
  - 手段：包过滤技术、独立防火墙。

HUAWEI

- 访问控制是指在网络路由可达的基础上，基于业务管控的需要，对特定的访问流量进行限制或阻断。如企业可以通过技术手段禁止其他部门访问财务部门的服务器。

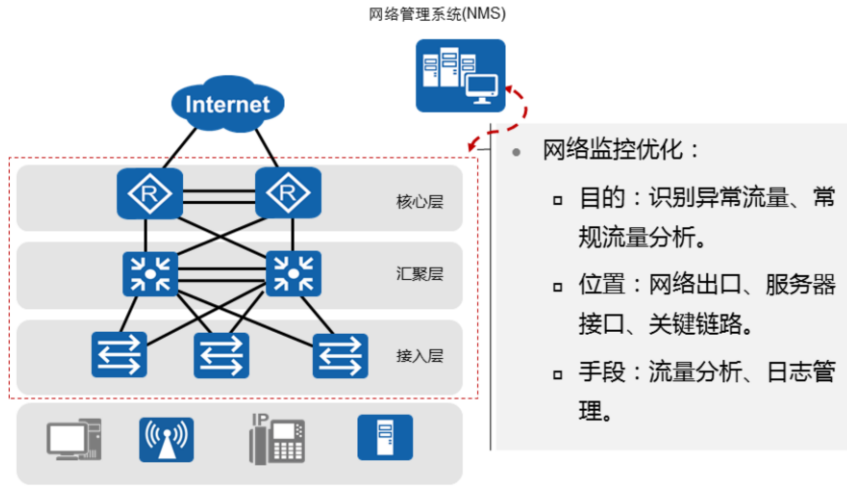
接入安全优化



- 接入安全优化：
  - 目的：实现用户的安全接入控制。
  - 位置：接入层设备。
  - 手段：NAC、用户绑定、端口隔离等。

- 网络接入安全主要是指保护网络资源（包括网络设备和信息资产）不受来自内部用户有意或无意的危害。如可以通过技术手段，防止外来访问人员随意接入公司网络。该需求可以通过NAC的方式来进行控制，用户接入网络必须通过用户名/密码认证。

网络监控优化

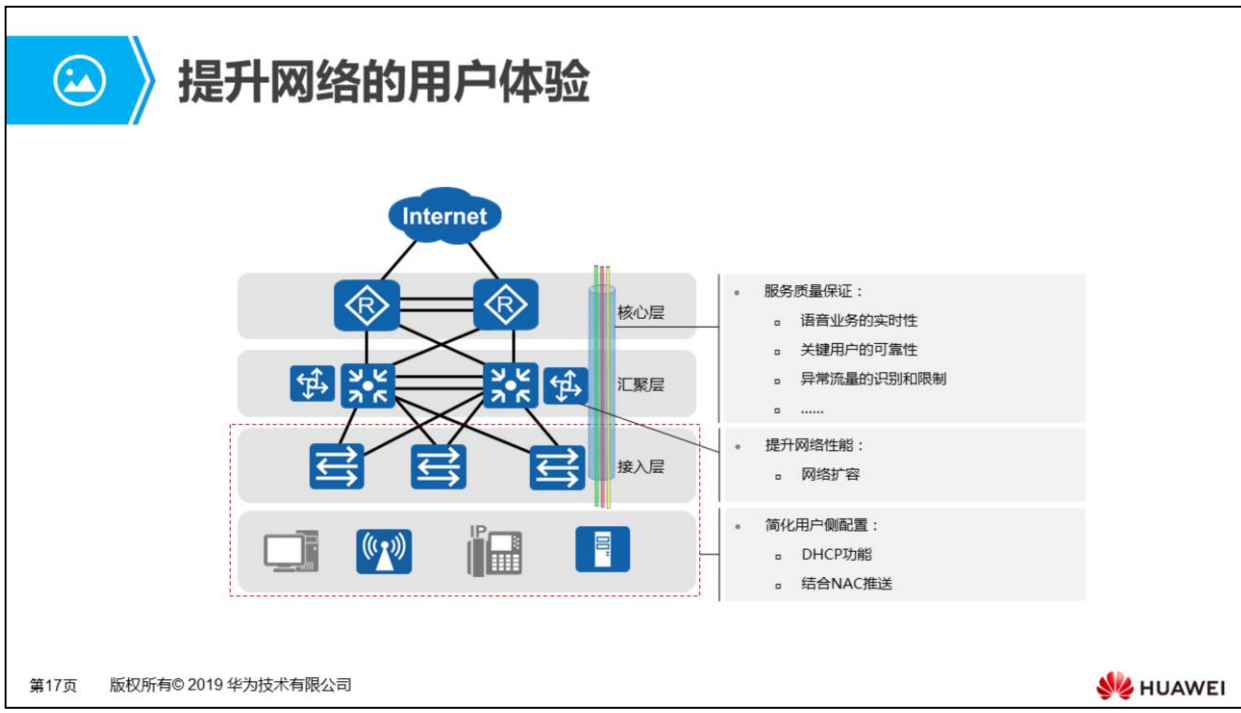


- 网络监控优化：
  - 目的：识别异常流量、常规流量分析。
  - 位置：网络出口、服务器接口、关键链路。
  - 手段：流量分析、日志管理。

HUAWEI

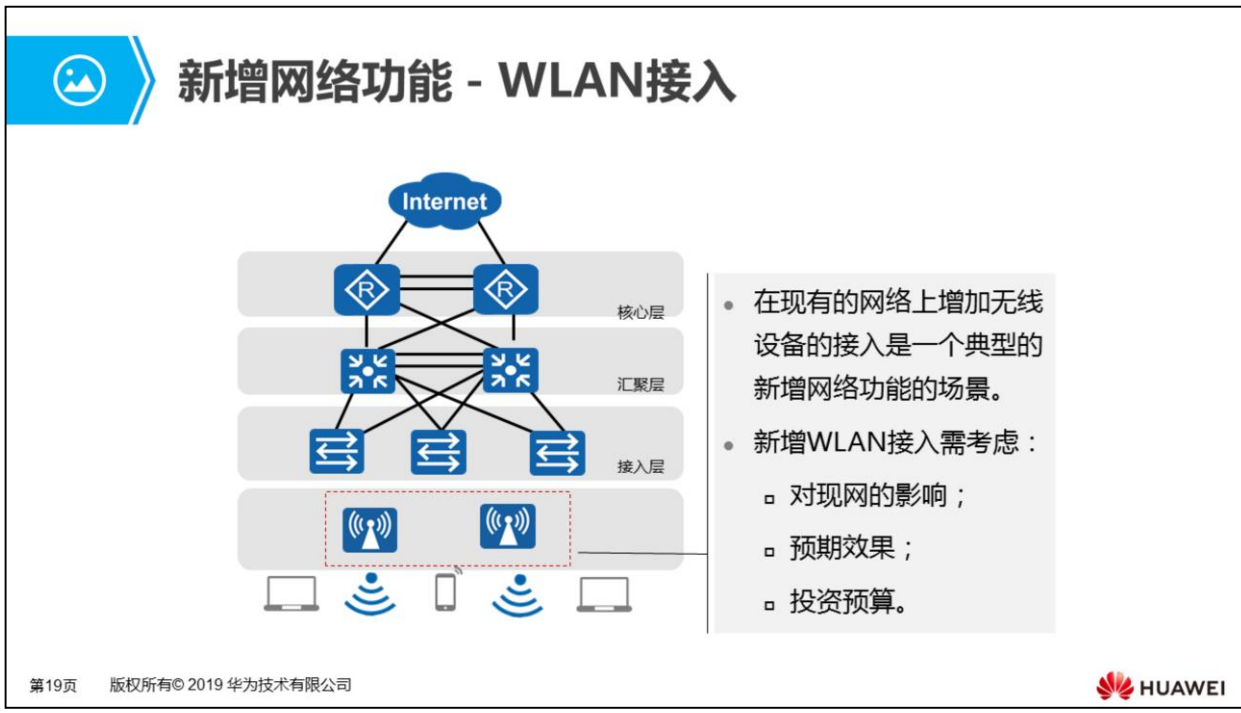
- 网络监控是指对网络的流量进行实时的或周期性的监控和分析。如某企业希望监控网络流量，能够及时对异常流量做阻断。为了实现网络监控，可以通过部署网络监控软件/硬件对流量做分析。

目录



- ISO 9241-210标准将用户体验定义为 “人们对于针对使用或期望使用的产品、系统或者服务的认知印象和回应”。通俗来讲就是“这个东西好不好用，用起来方不方便”。因此，用户体验是主观的，且其注重实际应用时产生的效果。
- 服务质量保证：
  - 服务质量是一个系统性的问题。企业网络中，除了传统的WWW、E-Mail、FTP等数据业务，还承载着视频监控、电视会议、语音电话、生产调度等业务。这些业务有一个共同特点，即对带宽、延迟、延迟抖动等传输性能有着特殊的需求。比如视频监控、电视会议需要高带宽、低时延抖动的保证。语音业务虽然不一定要求高带宽，但非常注重时延，在拥塞发生时要求优先获得处理。
- 提升网络性能：
  - 随着企业的不断扩大、业务的不断更新，如果原有的网络已经无法高效的支撑公司的业务运营，那么就需要根据业务需求，对网络规模或设备型号等进行扩容或升级。
- 简化用户侧配置：
  - 这里的用户是指网络的最终用户，即接入网络的PC使用者。
  - 为了提升用户体验，简化用户的终端配置，可以通过一些方法来实现。比如网络中部署DHCP Server，让用户终端都能够动态的获取网络地址。当然为了保证业务的可用性，网络服务器、打印机等通过必须MAC与IP绑定的方式固定IP地址。

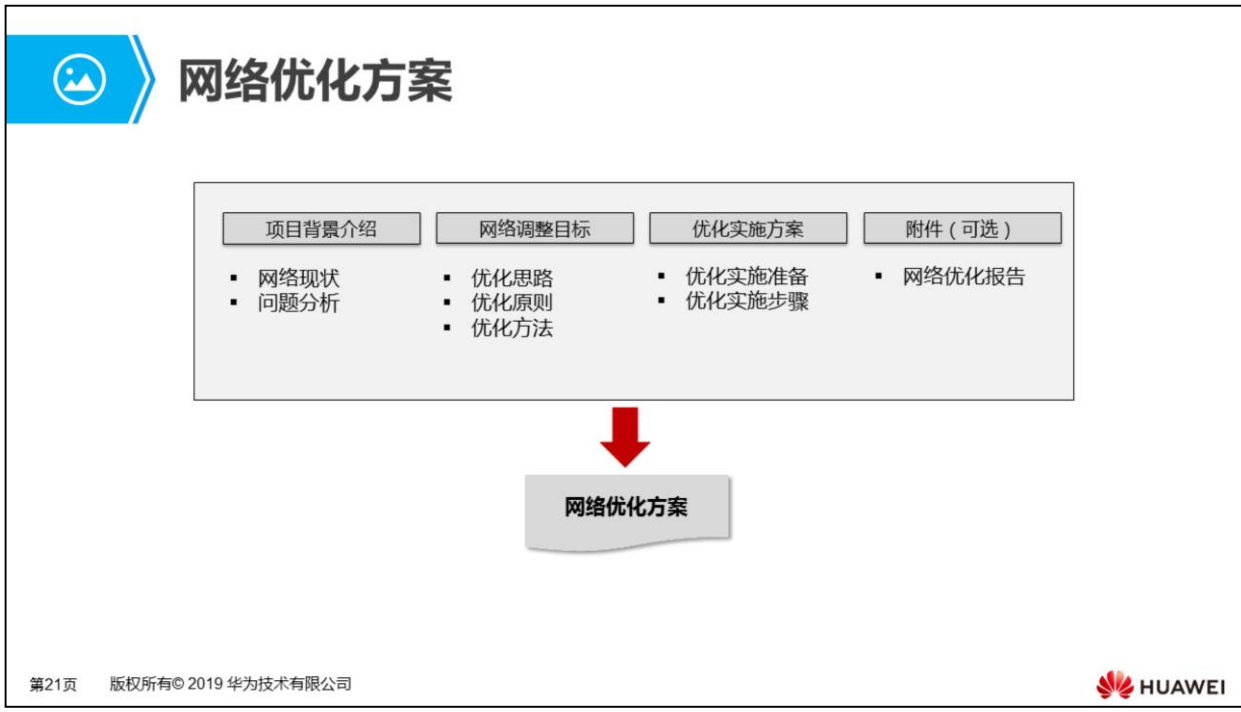
目录



- 任何新增网络功能的需求首要需要考虑对现网的影响问题。在新增网络功能时切忌顾此失彼，任何新增功能都不能够对现有正常业务造成长期影响。当然，可控范围内的短期影响是可以接受的。
- 需要充分评估新增网络功能的预期效果。以实现WLAN接入为例，目的是为了实现所有办公场所的全覆盖，还是仅覆盖重点区域（如会议室）？这些预期效果需要进行充分的评估，因为这直接影响对应的技术方案，进而影响到投资预算。如果需要大面积全覆盖，那么采用瘦AP（Fit AP）方案是必须的，如果只有少量的区域覆盖，那么采用胖AP（Fat AP）方案可能更合理。
- 投资预算是根据需求和计划采取的技术方案决定的，也是企业在进行任何网络优化时都必须考虑的问题。在现有网络上新增网络功能，“多快好省”是基本的原则。即在不追加或尽量少追加投资的情况下增加新的功能。比如，要让网络支持组播功能。大多数情况下只需要制定一个技术方案即可以实施，因为绝大多是网络设备本身是支持组播功能的。但是在更多的情况下，只有通过增加设备才能满足新的功能需求，如图所示，必须增加AP甚至AC（无线接入控制器）才能满足无线接入的需求。
- 通常新增一项网络功能，可以先在小范围试点，确认没有问题再大面积部署。例如，当需要实现WLAN功能大面积覆盖时，可以先在某一些办公室部署AP，充分评估是对当前网络的影响之后再大面积部署。

目录

HUAWEI



- 项目背景介绍：
  - 网络现状：主要介绍现网网络的架构、业务简介、现网存在的问题等。
  - 问题分析：主要详细分析当前网络无法支撑业务的关键点。
- 网络调整目标：
  - 优化思路：是针对现网当前的问题，概述性的描述解决方法。
  - 优化原则：主要介绍网络优化前后区别、投入产出比等内容。
  - 优化方法：是详细介绍优化的策略和方法，比如替换核心交换机。
- 优化实施方案：
  - 优化实施准备可以参照新建网络实施准备。比如施工前，进行深入调研、输出优化方案等。

思考题

1. 下列哪些是网络优化的需求来源？

A. 经过长期的网络维护，总结一些问题和改进点，提出相关建议，进行集中的整改。

B. 网络中需要开展视频会议业务，需要增加支持二层组播功能的交换设备。

C. 某弱电井因环境问题，信号线老化严重，需要集中更换。

D. 企业信息安全需要，增加新的安全设备。

- 1、答案：ABCD。


谢 谢
www.huawei.com

网络割接

HUAWEI

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。

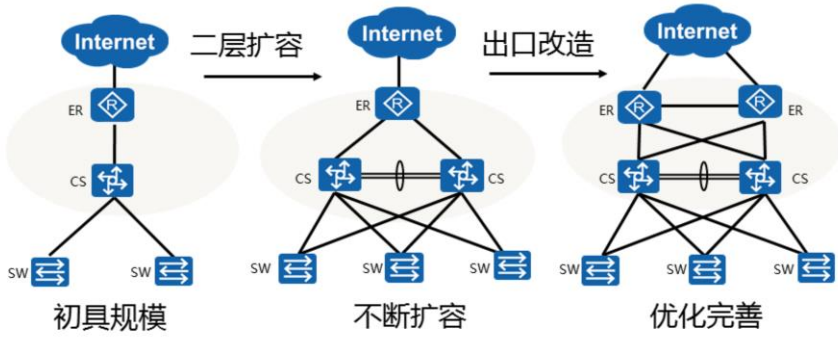
目标

- 学完本课程后，您将能够：
  - 理解割接的含义
  - 掌握割接的操作流程规范
  - 熟悉割接的常见场景

目录

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。



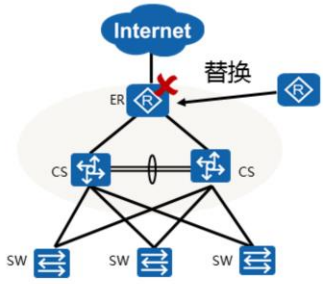
- 如此不断地升级、扩容、整改，怎样保障业务的平稳过渡？

HUAWEI

- 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。

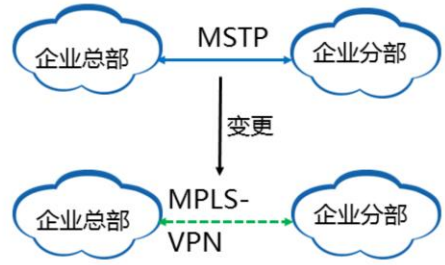
维护网络的手段

- 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



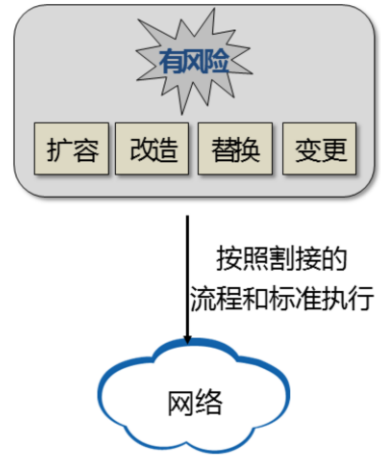
- 链路的变更不仅是物理线路的切换，还需要进行业务配置的调整。

HUAWEI

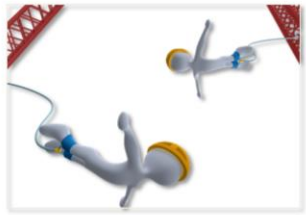
- 任何产品都是有生命周期的，一般为了安全起见，运行5-10年的ICT设备基本都要考虑退网，并由新的高性能设备替代，所以怎样实现安全平稳的过渡是个需要重点关注的问题。
- 网络线路是结合市场环境和自身需求来不断升级的，如先前大部分大型公司的企业总部和分支机构间通信需要支付高昂的费用来租用ISP的MSTP（SDH）线路，但是目前租用MPLS VPN线路已成为主流，为企业节省了大笔的开支，所以为保证不影响业务，安全地从MSTP线路切换为MPLS VPN线路的这个过程就是一个需要考虑的问题。

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

HUAWEI

- 割接的难点：
  - 控制业务影响的范围。
  - 把控风险规避措施。
  - 制定完善的割接方案。
  - 顺利地执行割接。

目录

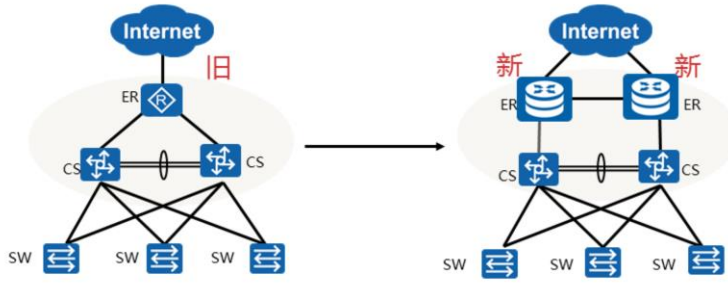
HUAWEI

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

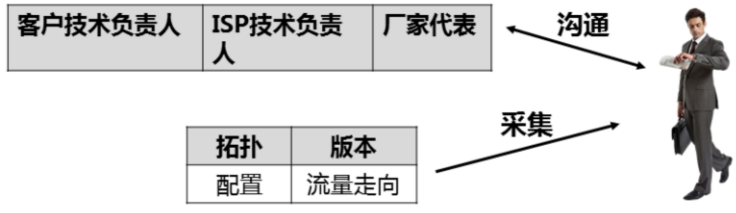
- A公司网络已运行多年，随着业务的不断发展，出口核心路由器承载的业务量越来越大，并且设备投产的年限已经快达到A公司的规范年限，对此客户提出在网络核心层新增两台高性能路由器并替换掉原来运行的老旧路由器。



HUAWEI

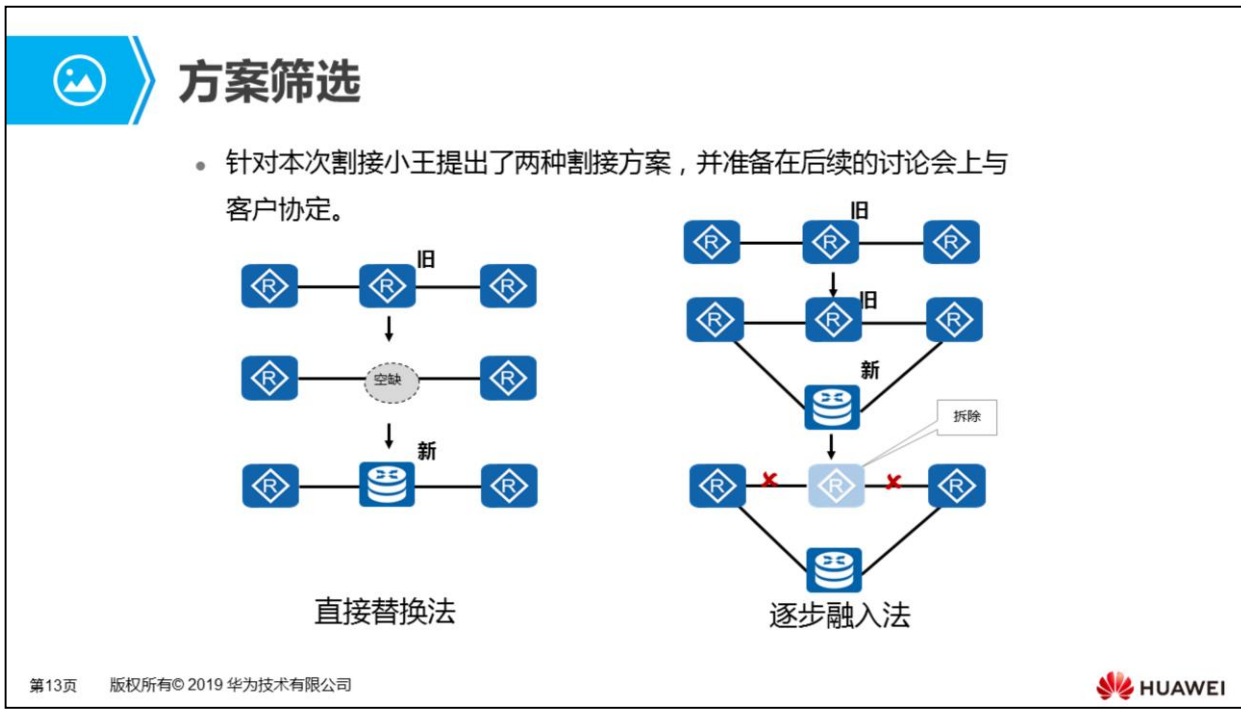
项目调研

- 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，故需要更换和改造。
  - **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得出是可以操作的。
  - **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，故定义为割接操作。



- 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。
监理：大家互相配合，共同合作，顺利完成本次改造项目。	

乙方 

监理 

方案编写

HUAWEI

方案验证和审定


搭建实验局测试

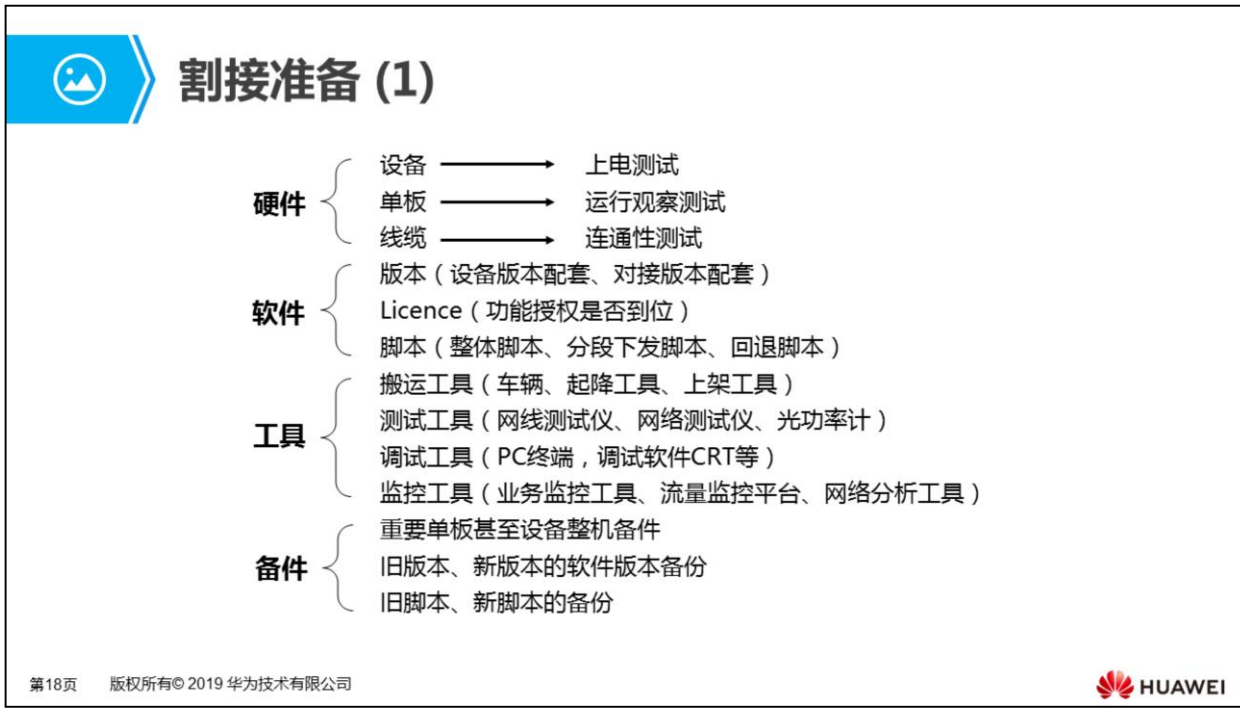

各方技术评审


原厂专家审核

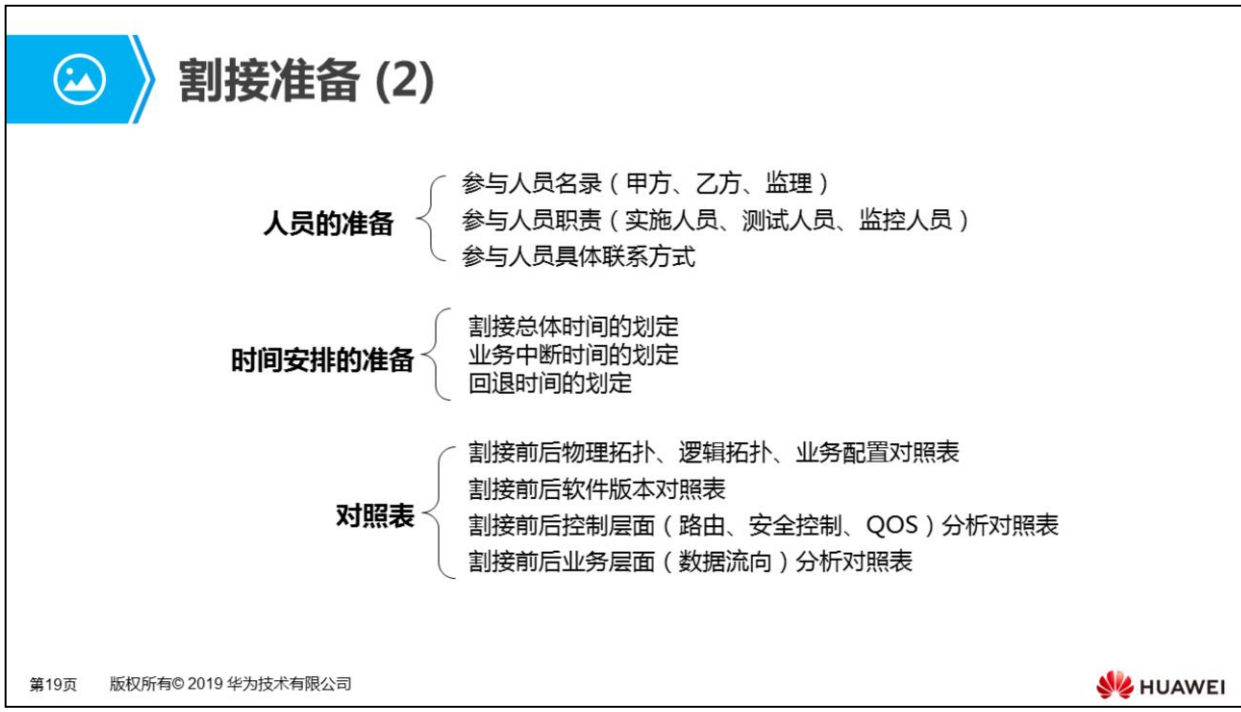

方案定稿

HUAWEI

- 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。

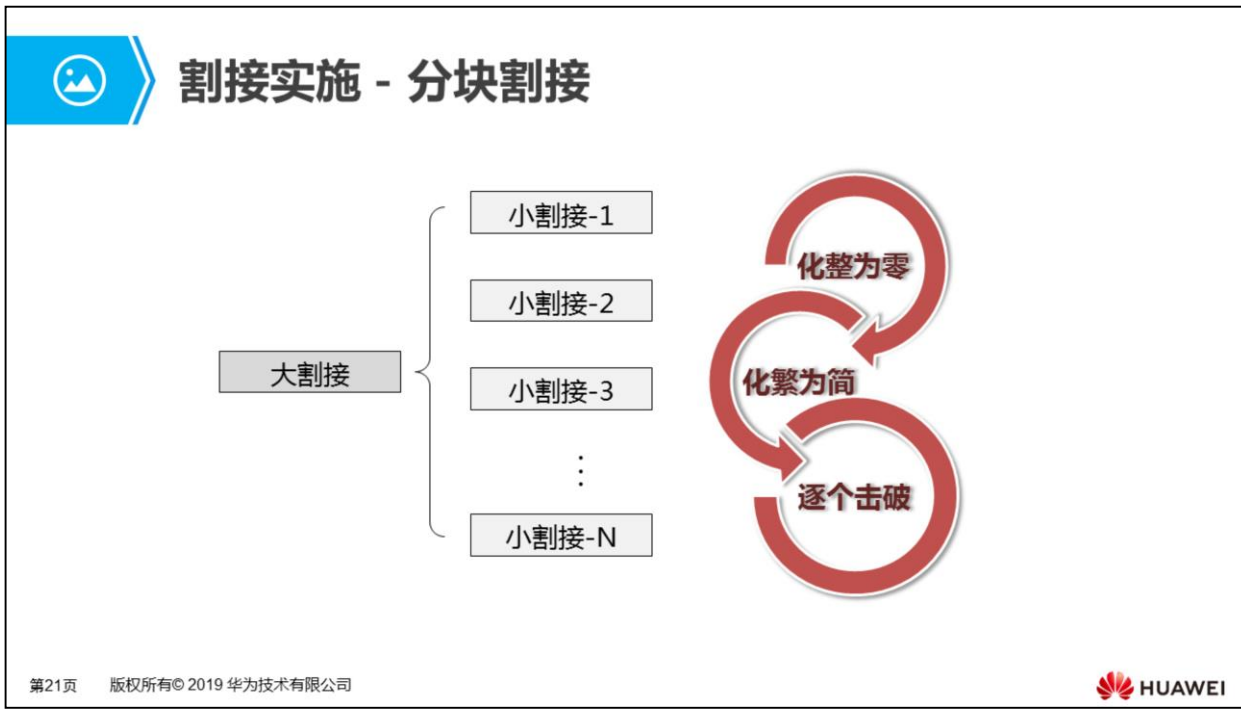


- 人员的准备：
  - 人员责任的划分能够保障各方人员实施过程中沟通顺畅，不会导致责任推卸问题。
- 时间安排的准备：
  - 时间安排必须与客户沟通，并获得客户的同意。
  - 制定总的时间安排表。
  - 规定出每个时间段执行的具体动作。
  - 割接执行阶段的时间要精细到分钟。
  - 重大操作的时间段要预留部分时间，避免因超时引发工程事故。
  - 割接时间点的选择尽量避免业务高峰期（如节假日，非正常上班时间等）。

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。

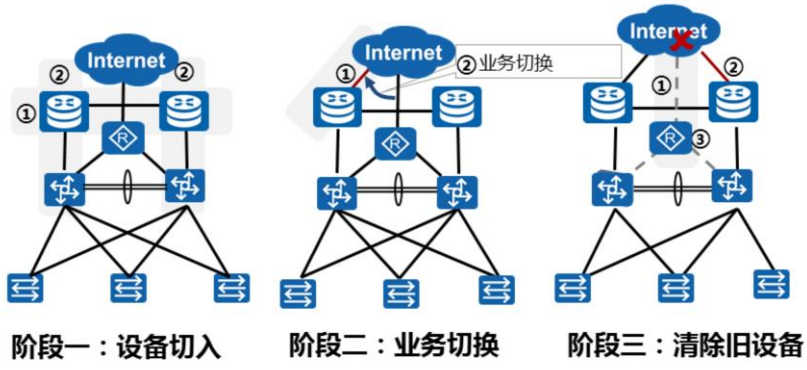
一些不容忽视的环节！



- 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：



  HUAWEI

- 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。

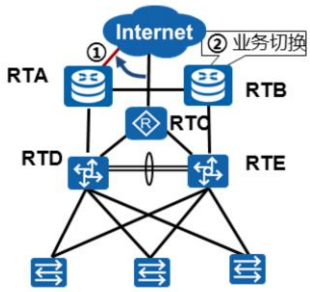
割接实施 - 割接步骤 (1)

- **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）

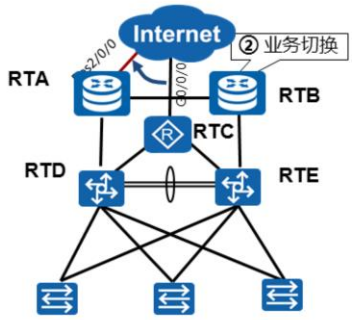
```
<RTC>display ip routing-table #查看路由
<RTC>display time-range all #查看当前时间段状态
<RTC>display log all #查看用户操作记录
<RTC>display device #查看设备的部件状态信息
<RTC>display version #查看设备版本信息
<RTC>display ospf peer  #查看路由器邻居信息
<RTC>display acl all #查看访问控制信息
. . .
```

- 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。

HUAWEI

- 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）

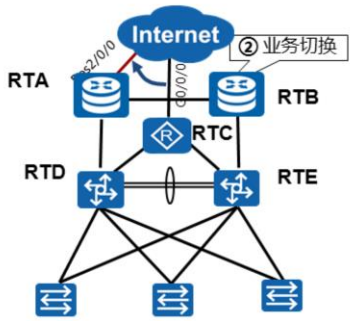
```
<RTD>display ip routing-table #查看路由表
<RTD>display ospf lsdb ase 0.0.0.0
#查看OSPF数据库默认路由
```

- 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。

HUAWEI

- 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RTC。
- 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）

HUAWEI

- 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。

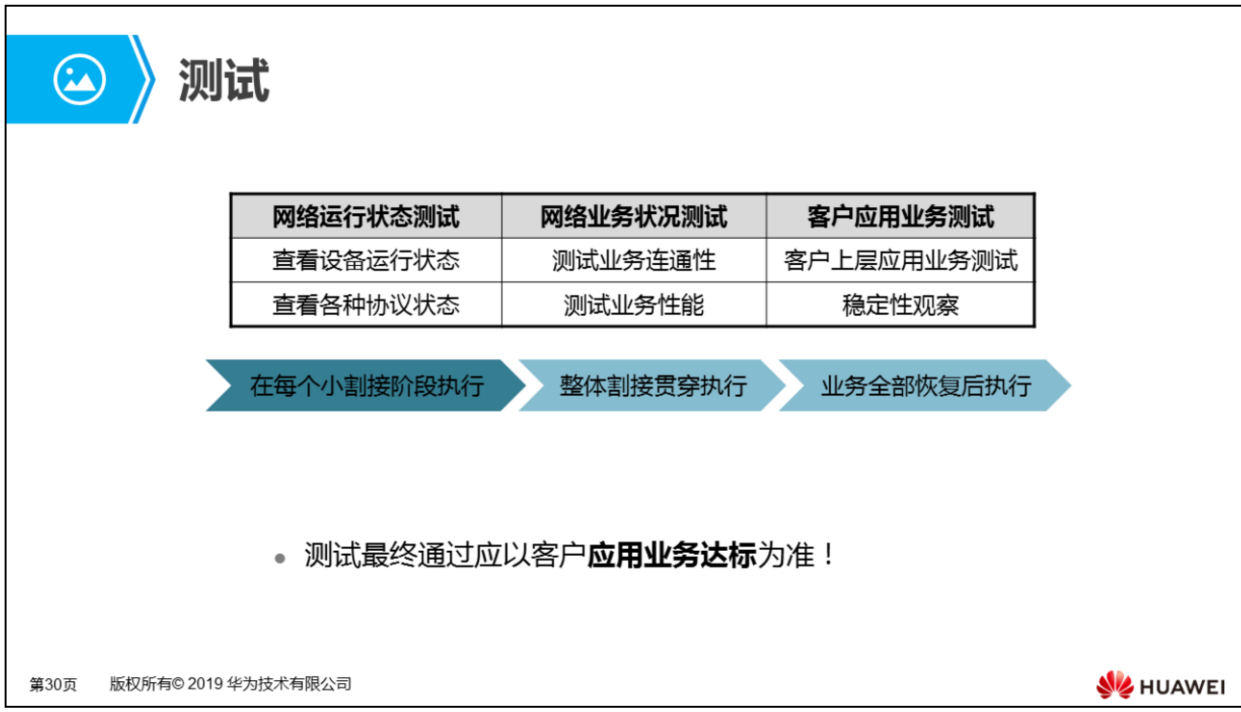
回退时机

根据现场环境做出预判	把握好回退时间点避免超时	回退操作说明应提前写入《割接方案》中

- 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

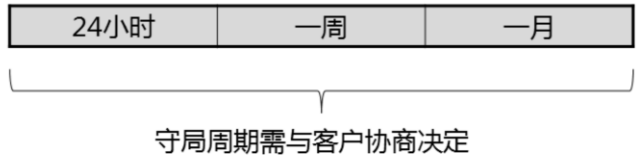
- 正常情况下如果割接失败是可以回退到原始的运行状态的。
- 当割接中出现由于不可抗因素造成割接失败时，若无法回退可采用应急预案。
- 应急预案需体现在《割接方案》中。
- 应急预案中的应急措施主要有：重新加载系统软件，替换现场备件，紧急调用设备等。



- 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

目录

HUAWEI

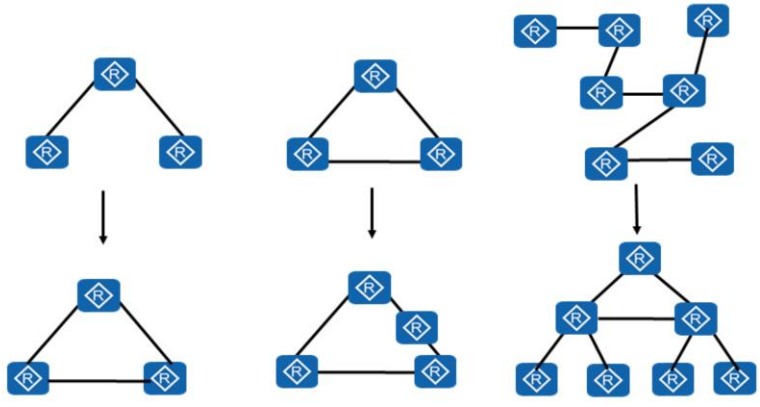
常见割接场景 - 设备升级

- 此类割接建议申请厂家进行技术支持。

HUAWEI

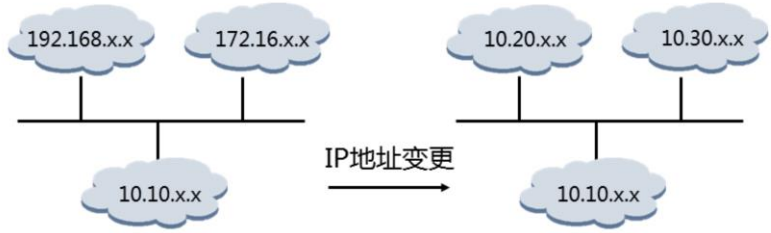
- 设备升级类割接：
  - 设备升级时要注意新增或替换的板件的版本型号是否与设备匹配，软件版本是否达到现有设备的版本配套表里面的版本要求，并确认单板是否支持热插拔操作等。
  - 设备软件升级必须得到厂家的授权，并下载官方的软件版本。设备软件升级最好准备有物理备件并且有回退预案。

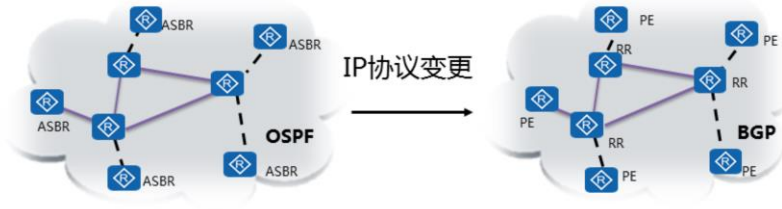
常见割接场景 - 网络物理结构改造



- 新增链路
- 新增设备
- 结构调整

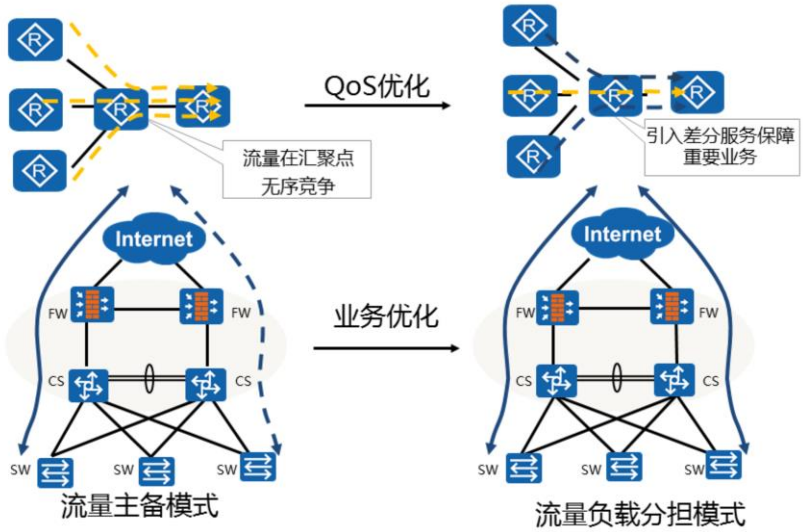
常见割接场景 - 网络系统调整





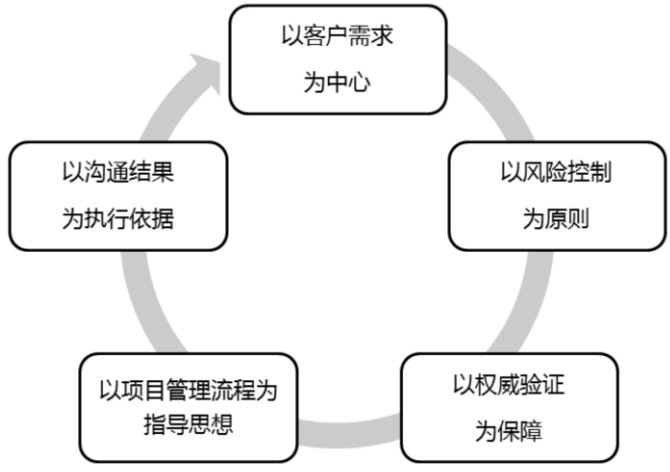
HUAWEI

常见割接场景 - 网络性能优化



流量主备模式　　流量负载分担模式

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？

HUAWEI

- 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。


谢 谢
www.huawei.com

学习推荐

- 华为培训与认证官方网站
  - http://learning.huawei.com/cn/
- 华为在线学习
  - https://ilearningx.huawei.com/portal/#/portal/ebg/26
- 华为职业认证
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_31&lang=zh
- 查找培训入口
  - http://support.huawei.com/learning/NavigationAction!createNavi?navId=_trainingsearch&lang=zh

更多信息

- 华为培训APP