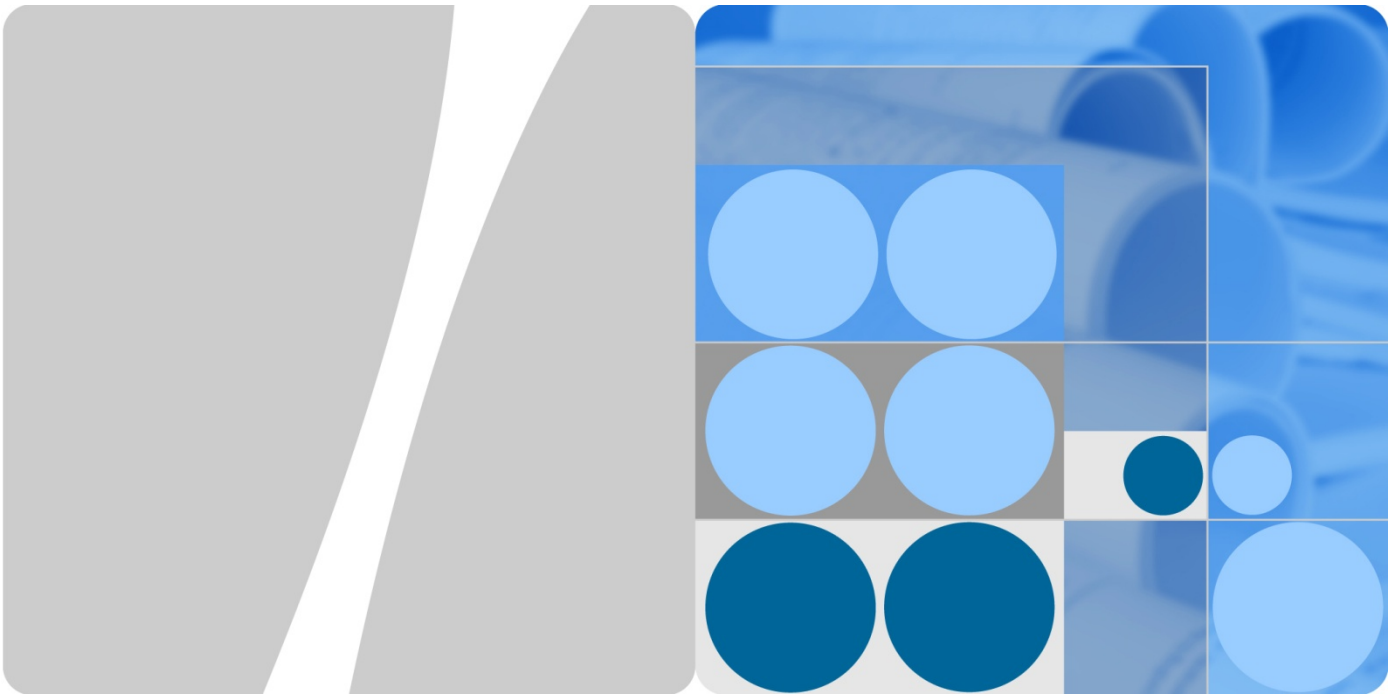


智能电网-地调接入网解决方案
V100R001C00
技术建议书

文档版本 02

发布日期 2012-01-06

华为技术有限公司

版权所有 © 华为技术有限公司 2012。 保留一切权利。

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

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

版权所有 © 华为技术有限公司

版权所有 © 华为技术有限公司

1 地调接入网概述

1.1 地调接入网概述

中国电力系统的信息化从 20 世纪 60 年代就已经开始起步，早期主要集中在发电厂和变电站自动监测/控制等方面，20 世纪 80～90 年代开始进入电力系统专项业务应用，涉及电网调度自动化、电力负荷控制、计算机辅助设计、计算机仿真系统等的使用。20 世纪末，电力信息技术进一步发展到综合应用，各级电力企业开始建立管理信息系统，实现管理信息化，电力信息化逐渐从生产操作层走向管理层，并向更深层次拓展。

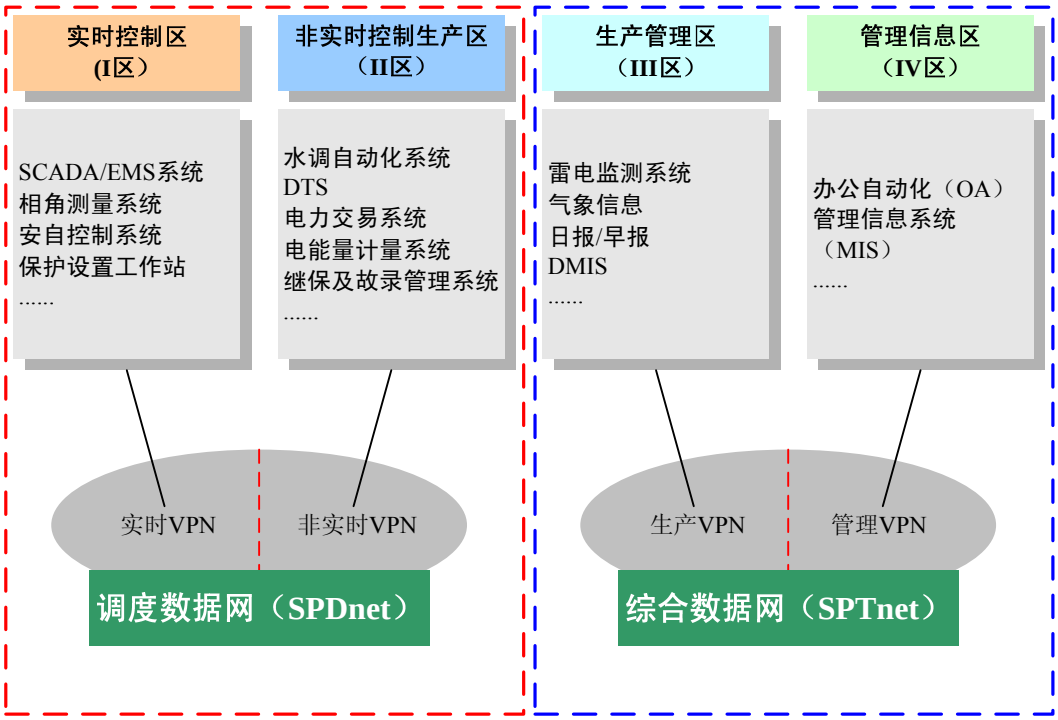
相对于传统行业，我国电力行业的信息化建设发展较早，已经有了一定的规模，到目前为止，电力企业的网络普遍建立，电力专用通信网已日趋完善，形成了微波、卫星、光纤、无线移动通信等多种类通信手段，通信范围覆盖全国。在此基础上，基本建成从国家电网公司——区域电网中心——省电力公司——地市电力公司——变电所（局）的四级计算机网络和电力生产调度网络，成为生产控制、电力调度以及信息传输和交换的重要基础设施。

电力系统的生产自动化和信息化依赖于电力数据网。电力数据网络承载的业务按照其性质和对安全的要求分为实时控制业务、非实时控制生产业务、生产管理业务和管理信息业务。目前网络上所有业务都承载在同一网络上，存在安全隐患，服务质量也难以保证。按照国家电力公司的统一规划，提出了“两网分开”的措施。

电力数据网又可分为调度数据网（SPDnet）和综合数据网（SPTnet），它们各自承担的职能如图 1-1 所示。其中实时控制业务和非实时控制生产业务属于电力生产和控制的关键业务，对可靠性、实时性、安全性的要求非常严格，由调度数据网承载。而生产管理业务和管理信息业务由综合数据网承载。两个网络之间物理分离。

版权所有 © 华为技术有限公司

图1-1 电力数据网职能



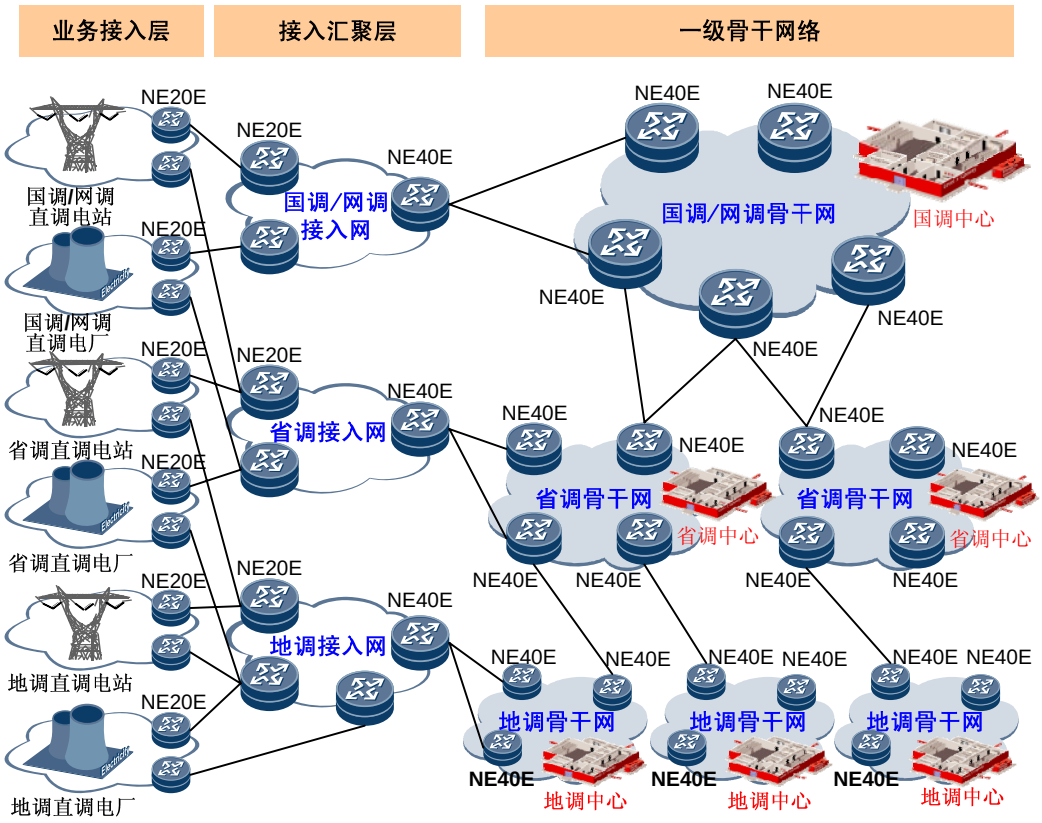
无论对于调度数据网还是综合数据网，建立一个综合、经济、可靠、有效的通信网络，既能满足现在电力系统语音、数据、图像等各种业务的需求，又能面向未来，支持不断增多的用户、更大的带宽以及多种新业务的广域数据网是关键所在。

本章主要描述调度数据网的相关内容。调度数据网是电力的生产控制网络，通过 MPLS VPN 分为实时控制区（I 区）和非实时控制生产区（II 区），是电力信息化的核心网络之一。

电力调度系统分为国家调度中心（国调）、大区网局级调度控制中心（网调）、省级调度控制中心（省调）、地区调度控制中心（地调）和各级接入网。各级直接管理和调度其下一层调度中心，如图 1-2 所示。

版权所有 © 华为技术有限公司

图1-2 调度数据网整体架构



本文档只描述地调接入网的组网方案和部署。地调接入网是负责地区电力厂站接入的业务网络，覆盖所属县调、集控站以及 110KV（66KV）、35KV 变电站。

1.2 地调接入网网络需求

全国电力调度系统发展的指导思想是：“安全第一、预防为主”，确保电网安全。电网调度最根本的职责在于保证电网的安全稳定运行，做为电力调度系统的承载网，地调接入网的首要要求就是可靠、稳定、安全的运行，保证调度自动化系统对电网的准确监控、不间断进行。

地调接入网的建设，是在现有省电力通信传输网络的基础上，建设一个覆盖省级地调及所辖厂站的数据网络，实现该地区电力系统生产调度信息资源的共享以及与全省调度数据网络的合理整合。

现有电力通信传输网络，主要包括 SDH2.5G/622M/155M 光纤通信传输网络、SDH155M 及 PDH34M/17M/8M 微波通信传输网络，通信传输网络主要提供 N*2M 方式供电力调度数据专网使用，部分偏远地区厂站或电力微波/光纤传输网络未覆盖厂站将采用租用电信运营商提供的 2M 通道，所有 2M 数字通道均符合 ITU G.703 标准。

华为公司提供的调度数据网方案本着先进性、实用性和经济性统一的原则进行设计，设计的网络具有高性能、高可靠性、扩展性、标准化和可管理性的特点，能灵活地根据需求提供不同的服务等级并保证服务质量。该网络将采用最先进的 IP/MPLS 技术和高速设

版权所有 © 华为技术有限公司

备，为各类信息系统提供统一的综合业务网络平台，与原有设备和网络实现良好互通的网管一体化解决方案，实现新、老设备的统一网管，降低管理成本和提高管理效率。

1.3 网络建设目标

考虑到地调接入网的定位，应在专用通道上利用专用网络设备组网，采用 PDH/SDH、以太光纤/电缆等方式，实现物理层面上与公用信息网络的安全隔离；地调接入网络只允许传输与电力调度生产直接相关的数据业务。为确保其所承载电力调度各类业务系统安全可靠地运行，华为建议的地调接入网应具备如下特点：

- **具备强大的处理能力、业务能力及平滑演进能力**

  地调接入网应具备承载各类业务系统所需的性能、各种特性及业务能力（如 MPLS VPN、MPLS HQoS、安全特性、ACL 等），同时应具备强大的业务演进及扩展能力；对于带宽的提升，可以通过升级或扩容单板；对于新特性、新业务的提供（如 QoS、IPv6），可通过软件升级的方式提供。最大限度地保护现网投资，满足可持续发展的要求。

- **严格保证实时业务的 QoS**

  全网端到端单向时延小于 50ms、端到端时延抖动小于 10ms、丢包率小于 0.1%，能够为所承载的各类业务系统按需提供 QoS 保证（EF、AF）。

- **严格保证数据平面的安全性**

  保证电力调度业务系统传送时的可靠性、完整性和保密性。

- **可管理性**

  地调接入网必须具有完善的流量统计与监测、故障定位、故障排查等功能，为网络日常维护管理、网络优化提供依据；同时应提供 VPN、QoS 等策略部署工具，简化管理、降低维护成本。

通过上述目标的实现，最终打造一个可运营、可管理、安全可靠、具备多业务承载能力的电信级 IP 网络，实现“实体物理网、虚拟业务网”，整合网络资源、降低运营维护成本。

1.4 网络设计原则

为达到网络优化和将来扩展的目标要求，在网络设计构建中，应始终坚持以下建网原则：

- 高可靠性

  网络系统的稳定可靠是应用系统正常运行的关键保证，在网络设计中应选用已规模商用的高可靠性网络产品，合理设计网络架构，制订可靠的网络备份策略，保证网络具有故障自愈的能力，最大限度地支持系统的正常运行。

- 标准开放性

  支持国际上通用标准的网络协议(如 TCP/IP)、国际标准的大型的动态路由协议(如 BGP、OSPF)等开放协议，有利于保证与其它网络之间的平滑连接互通以及将来网络的扩展。

- QoS

版权所有 © 华为技术有限公司

对于所承载的每种业务，要能够按需提供 QoS；对于生产调度类实时业务，要能够提供类似于传统 PSTN 网络的服务质量。

- 安全性

  通过设备机制及组网方案提高网络整体的安全性，对于所承载的各类业务系统提供类似于传统专线一样的安全性。

- 灵活性及可扩展性

  根据未来业务的增长和变化，网络可以平滑地扩充和升级，最大程度的减少对网络架构和现有设备的调整。

- 可管理性

  对网络实行集中监测、分权管理，并统一分配带宽资源。选用先进的网络管理平台，具有对设备、端口等的管理、流量统计分析，及可提供故障自动报警。

以上原则应全面考虑，做到多重兼顾，重在保证总体效率，不能因片面强调某些性能而牺牲其它方面，最大限度地发挥网络平台的效率。

版权所有 © 华为技术有限公司

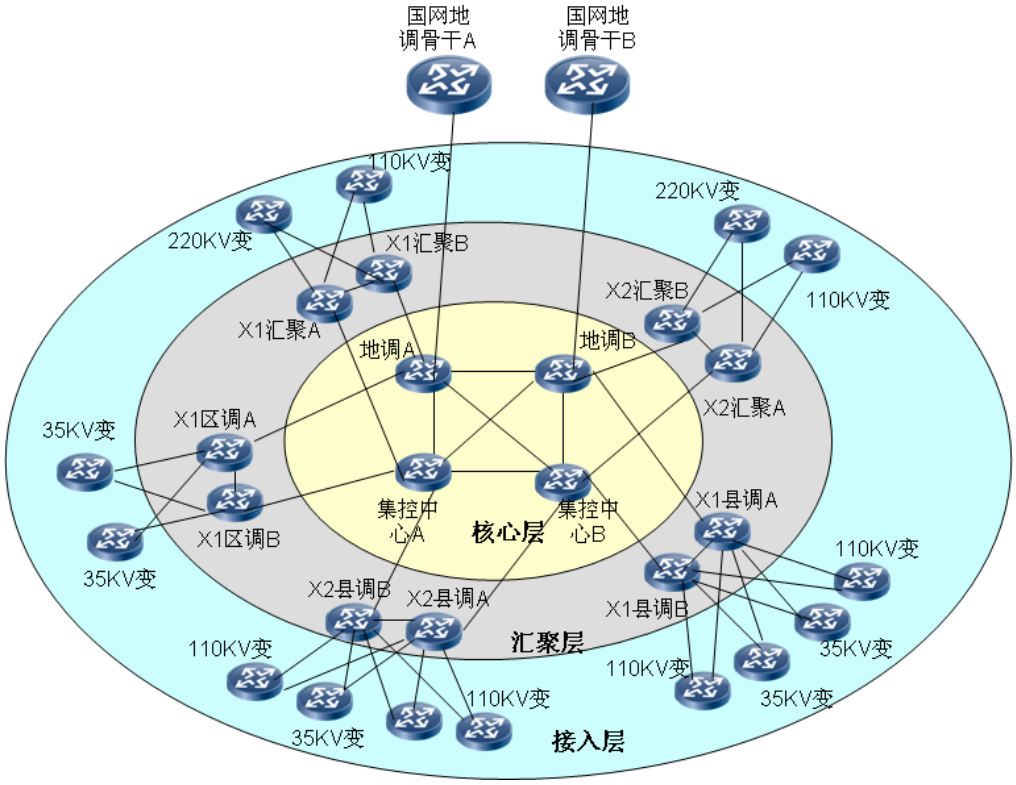
2 网络总体方案设计

2.1 网络结构

电力工程组网拓扑建议如下：

各级调度数据网络拓扑结构分为 3 层，即核心层、汇聚层、接入层。

图2-1 工程组网拓扑



- 核心层

  地调核心以及地区集控中心，每个站点采用双机配置，节点之间通过 155M POS 建立全连接，每个节点采用双引擎双电源冗余配置。

版权所有 © 华为技术有限公司

- 汇聚层

  地调直调 220KV/110KV 变汇聚节点、县调、区调汇聚节点组成地调接入汇聚层，每个站点采用双机配置，通过 155M POS 上连至核心层。

- 接入层

  由各地调、县调、区调下属 220kV 变、110kV 变、35kV 变组成。每个接入节点由单机双引擎组成，双链路上连至汇聚层节点。

2.2 实施原则

实施中网络拓扑有可能根据线路会发生一定变化，比如说线路带宽变化，端口变化，网络实施规划原则如下：

1. 核心节点双链路分别上联到调度数据网的 A、B 平面。
2. 汇聚层至少双链路连接到不同的核心节点。
3. 接入层尽量就近接入到汇聚节点。
4. 接入层交换机通过双链路连接到接入路由器。
5. 根据不同业务选择合适的设备。

版权所有 © 华为技术有限公司

3 地调接入网技术设计

3.1 路由设计

3.1.1 路由设计原则及要点

华为地调接入网路由设计需要考虑以下几点：

- 网络的可靠性

  通过动态路由协议的实施，在网络拓扑的配合下，避免网络中出现的单故障点，提高网络的生存能力。

- 流量的负载分担

  必须使网络的流量能够比较合理地分布在各条电路上。

- 网络的扩展性

  使得网络的扩展可以在现有的网络的基础上通过简单的增加设备和提高线路带宽的方法来解决。

- 对业务流量模型变化的适应性

  未来网络的业务流量模型将会随业务的发展而不断发生变化，因此路由策略可以根据流量变化方便进行调整。

- 降低管理复杂程度

  路由协议应使得故障定位和流量调整的难度和复杂性降低。

3.1.2 IGP 路由协议

在大型网络中，选择适当的路由协议是非常重要的。目前常用的路由协议有多种，如 RIP、OSPF、IS-IS、BGP、DVMRP、PIM 等等。不同的路由协议有各自的特点，分别适用于不同的条件之下。选择适当的路由协议需要考虑以下因素。

- 路由协议的开放性

  开放性的路由协议保证了不同厂商都能对本路由协议进行支持，这不仅保证了目前网络的互通性，而且保证了将来网络发展的扩展能力和选择空间。

- 网络的拓扑结构

  网络拓扑结构直接影响协议的选择。例如 RIP 这种比较简单的路由协议不支持分层次的路由信息计算，对复杂网络的适应能力较弱。

版权所有 © 华为技术有限公司

- 网络节点数量

  不同的协议对于网络规模的支持能力有所不同，需要按需求适当选择，有时还需要采用一些特殊技术解决适应网络规模方面的扩展性问题。

- 管理和安全上的要求

  通常要求在可以满足功能需求的情况下尽可能简化管理。但有时为了实现比较完善的管理功能或为了满足安全的需要，对路由的传播和选用提出一些人为的要求，就需要路由协议对策略路由的支持。

在目前，可以用于大规模网络部署同时又基于标准的 IGP 的路由协议有 OSPF 和 IS-IS。两种路由协议均是基于链路状态计算的最短路径路由协议，采用同一种最短路径算法（Dijkstra）。两种协议在实现方法、网络结构上均相似，在大型网络中都有成功案例。

在 IGP 路由协议的选择上，要求尽量不采用扩展性差的(如 RIP)和厂家的私有路由协议(如 IGRP 和 EIGRP)，尽量采用 OSPF 或 IS-IS。

OSPF 和 IS-IS 的特点如下，可以根据实际需要进行选择：

1. 基本原理相同(基于链路状态算法)，OSPF 用于 IP， IS-IS 用于 ISO 的 CLNP，也支持 IP(“集成 IS-IS”)；
2. IS-IS 结构严谨，OSPF 更加灵活，OSPF 协议是基于接口的，而 IS-IS 路由器只能属于一个 Area，并且不支持 NBMA 网络；
3. IS-IS 占用网络资源相对较少，支持网络规模大于 OSPF，在网络相当庞大时能体现出优势；一个 IGP 域运行的三层交换机及路由器的数量一般不会超过 200 台，因此从实际情况来看，运行 OSPF 和 IS-IS 对宽带城域网的建设不会有差异；对于网络的稳定性、可扩充性，两种协议都能很好地支持；在大型网络上，IS-IS 与 OSPF 二者均获得普遍应用；
4. 从 MPLS 草案及现实运行来看，如果要运行 MPLS 网络的话，OSPF 经常被选用做内部 IGP，当然 IS-IS 也有，但是 MPLS 草案中认为在 MPLS 环境中运行 OSPF 更合适；使用 MPLS TE 的时候，采用 IS-IS 扩展的较多；
5. 从目前很多厂商的设备来看，存在这样一个问题，很多用户的中低端路由器及三层交换机不支持 IS-IS，从这个角度讲 OSPF 比 IS-IS 有优势，所有的主流路由器及三层交换机都支持 OSPF。

3.1.3 BGP 路由协议

BGP-4 是目前域间路由协议的事实标准（RFC1711）。BGP-4 是一种用来在自治系统之间传递选路信息的路径向量协议。路径矢量协议的概念来源于 BGP-4 的选路信息中有一个自治系统（Autonomous System Protocol ）为传送协议，TCP 端口（Port）号为 179，这样就保证了所有 BGP-4 消息传送的可靠性，诸如消息出错重传等机制由 TCP 传送协议管理，而不需要 BGP-4 自己来实现。

两个运行 BGP-4 协议的路由器建立相互间传送协议的 TCP 连接以后，这两个路由器就成为相邻体或对等体（Peer）。BGP 连接建立之后，对等体之间首先交换各自路由表的全部信息。运行 BGP-4 协议的路由器不会定期发送路由选择更新信息，只有当路由表发生变化，才将发生变化的路由信息发送出去。因此 BGP-4 协议对网络的负荷影响不大。

IBGP 设计目标是追求网络的稳定性，减少路由振荡；可扩展性，降低路由器开销，允许支持更多的设备；简单性，使网络易于管理。

版权所有 © 华为技术有限公司

IBGP 采用了特殊水平分割方式来避免出现路由循环，即 IBGP 路由器不向其他 IBGP Peer 转发从某个 IBGP peer 学习到的路由，因此要求所有 BGP 路由器之间必须构成 Full Mesh 全连接才能够保证路由的正确传递。这种 IBGP 全连接会增加系统 CPU 和网络传输开销，降低系统性能，严重影响网络的可扩展性。解决 IBGP 的全连接问题有两种方式：路由反射器和自治域联盟，前者的可扩展性和简单性都好于后者，因此在可以企业网中采用路由反射器（Route Reflector, RR）的方式。

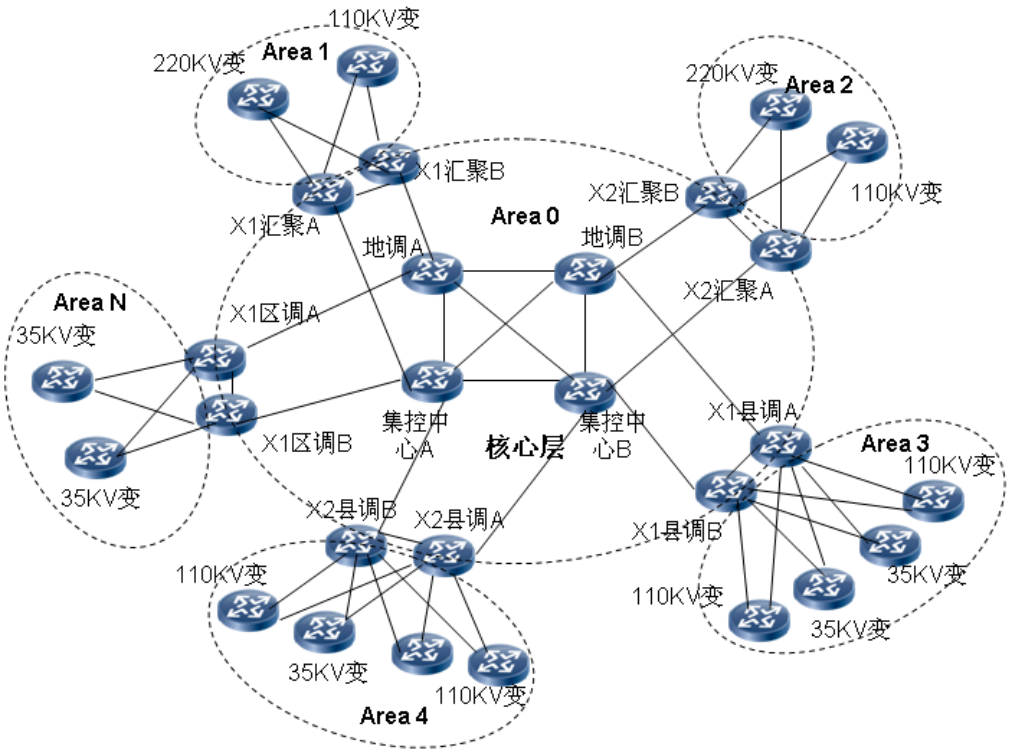
IBGP 主要用于将国调或网调路由传递到骨干、接入层。同时将本网路由传递到国调或网调。由于所有路由器运行在同一个 BGP 的 AS 中，按照 BGP 协议的要求，所有这些路由器必须保证是全连通的，即：任意两台路由器之间都必须配置邻居关系。这样会导致 N 平方问题，为了解决这个问题，必须使用 BGP 反射器技术。RR 的设计模式基本上是遵循网络的物理结构，一方面可以达到最佳的路由转发效率，提高可扩展性，同时也可以避免路由决策和数据转发的分离造成的次优路由现象。

3.1.4 OSPF 路由协议部署方案

区域划分

综合 IGP 路由部署经验以及地区调度网现状，建议采用 OSPF 作为地区调度网 IGP 路由协议。整个地区调度网在一个 OSPF 进程中，核心节点与国网地调骨干节点之间可通过静态路由互相引入 Loopback 地址。考虑到 OSPF 区域节点不宜太多，将核心层和汇聚层划分在 Arae0，汇聚层下行端口与接入路由器划分成不同的区域，如图 3-1 所示。

图3-1 IGP 路由部署方案



版权所有 © 华为技术有限公司

Router ID 规划

每台设备的 router id 设置为与该设备的 loopback 地址相同。

OSPF 路由聚合

为了减少在整个 OSPF 路由域中的路由条目，在区域边界路由器（ABR）和 ASBR 处，可以进行路由聚合操作，向区域外部发送聚合后的路由信息。

本次工程中可以考虑在 ABR 处对如下路由进行聚合后发布：

- 核心区域中的互联地址
- 核心节点与骨干节点之间的互联地址
- 骨干节点和接入层节点之间的互联地址

本次工程中可以考虑在 ASBR 处对如下路由进行聚合后发布：

- 所连交换机的网管地址。

说明

路由聚合可以视现场更具体的情况而定。

引入其他路由协议的路由

OSPF 可以引入其他路由协议产生的路由，包括直连路由、静态路由、RIP。本次工程的具体路由引入情况视现场情况而定。

统一路由尺度（COST）的计算

为确保路由器选择最优路径，统一 OSPF 路由尺度（cost）的计算，计算公式为：1000/带宽，带宽的单位是 Mbps，各种接口的路由尺度如表 3-1 所示。

表3-1 接口路由尺度

接口类型	Cost
GE	1
155M POS	6
100M FE	10
N×E1	600/N

通过设置合理的 Cost 值来实现流量的负载或分担，比如把接入节点连接省调节点和骨干节点的链路设置不同的 Cost，来实现正常情况下流量从接入节点到骨干节点，而接入节点到省调节点的链路作为备份。

3.1.5 BGP 路由协议部署方案

在实际部署中中，需要采用 MP-BGP 路由协议承载 VPN 业务路由。建议 PE 和 CE 互连采用直连路由方式，只需给 MPLS 网络分配一个 AS 号即可。

版权所有 © 华为技术有限公司

部署路由反射器

如果地调接入网的规模较大，为了减少 BGP 对等体的数量，可以采用路由反射机制。

根据接入网的规模不同，可以采用一级或两级路由反射规划。

- 两层结构的接入网采用一级路由反射规划，路由反射器为接入网的核心节点，客户为接入节点。
- 三层结构的接入网采用两级路由反射规划，一级路由反射器为接入网核心节点，客户为接入网汇聚节点；二级路由反射器规划为接入网汇聚节点，客户为接入网接入节点。

路由控制

接入网到骨干网跨域 MPLS-VPN 互联方案目前采用单跳 MP-EBGP 方式。

跨域时，只有 ASBR 间接口地址互通，此段地址不引入任何动态路由协议中。公网 BGP 不传递任何路由，在 ASBR 上设到对端聚合公网网段的静态路由，并将此静态路由导入本 AS 的 OSPF 路由中，在本 AS 内扩散。骨干网和接入网做对等操作。

接入网核心设备只向骨干网发送本 AS 始发的路由。在骨干网对接设备上向接入网发布路由时指定接收者不向其他 AS 传播路由(设置 no-export 团体属性)，并且只接收接入网中只经过一个 AS 的路由。

在接入网核心设备上增加骨干网 RT，保持本地 RT 不变，骨干网边界设备增加接入网 RT，边界路由器实施 RT 互导。

接入网在 ASBR 处对私网路由聚合后发送给远端。

接入网对骨干网同一平面存在双出口的情况下，接入网中 ASBR 节点通过设置 LP 来确定优先使用的出口路由器。

3.1.6 IP 地址规划方案

IP 地址规划

IP 地址空间的分配与合理使用与网络拓扑结构、网络组织及路由政策有非常密切的关系，将对网络的可用性、可靠性与有效性产生显著影响。在分配 IP 地址时，应该注意以下几点：

- 地址的规划与划分应该考虑到局域网的飞速发展，既要满足对 IP 地址的需求，同时要充分考虑未来业务发展，预留相应的地址段。
- IP 地址的分配必须采用 VLSM 技术，保证 IP 地址的利用效率。
- 应该采用 CIDR 技术，这样可以减小路由器路由表的大小，加快路由器路由的收敛速度，也可以减小网络中广播的路由信息的大小。

具体网络 IP 规划将根据用户原有网络环境而定。

IP 地址分配方案

IP 地址的划分主要考虑设备 Loopback 地址的分配、设备互联地址的分配、核心、骨干局域网地址的分配，业务地址可以保持不变。

版权所有 © 华为技术有限公司

- 设备 Loopback 地址的分配

  各路由器的 Loopback 地址的使用，在不同的方面都需要它的参与，这主要包括了以下的几种情况：

  - 路由器的 Loopback 地址，是保证内部路由协议的正常运行的重要条件；路由器的 Loopback 地址，是建立 iBGP 会话的主要参数的选择。
  - 选择 Loopback 地址作为 iBGP 会话建立的基本，对于会话的稳定性能够提供很好的支持。

  综合这些方面，各路由器的 Loopback 地址，对于整个网络的正常运行，有着至关重要的作用，因而对于各个路由器的 Loopback 的分配和管理，应当采取统一的专有地址空间。通过为所有的路由器分配一个专有的地址空间，能够更为有效地进行路由器的路由配置和管理，以及方便今后的故障的诊断和排除。

  Loopback 地址分配采用 32 位掩码的原则。

  具体选址方式以及相应号段遵循省网地址分配原则。

- 设备间链路地址的分配

  路由器间链路的 IP 地址，从业务的相关性上，他们一般不具有全局的功能，而只是提供完成两个路由器之间的连接。因而从这个角度上讲，这部分的地址空间的分配应当考虑以下的方面：

  - 尽可能以分层次的方式分配地址。

    由于链路地址空间不具有全局性，因而并不需要在全网范围内为每个链路保持精确路由。而采取分层次的地址分配方式，能够将链路地址逐级汇总，从而使得这些地址在各路由器的路由表中占有较少的空间。以降低对路由器的要求，并保证路由器的处理效率。

  - 提供足够的预留空间，以满足今后新增链路的需要。

    采用上面的分层次的链路地址分配结构，能够保证路由处理的高效性。而在实施的过程中，应当考虑到在根据业务需要新增链路的时候，这种分层次的结构尽量不会被打破。那么，就需要在初期分配的时候，考虑到不远的将来可能进行的扩容，从而进行相应的预留。

  互连链路地址采用 30 位掩码的分配方式。

  遵从省网 IP 地址划分的原则，核心层地址划分一个 C 类地址段，汇聚层地址划分两个 C 类地址段，接入层划分两个 C 类地址段，总共 5 个 C 类地址段即可满足地区调度数据网的需求。

3.2 VPN 设计

3.2.1 MPLS VPN 技术简介

MPLS 的一个重要应用是 VPN，采用 MPLS VPN 技术可以把现有的 IP 网络分解成逻辑上隔离的网络，这种逻辑上隔离的网络的应用可以是千变万化的：可以是用在解决企业互连、政府相同/不同办事部门的互连、也可以用来提供新的业务，如为视频、IP 电话业务专门开辟一个 VPN、以此解决 IP 网络地址不足和 QoS 的问题，也可以为用 MPLS VPN 为 IPv6 提供开展业务的可能。

版权所有 © 华为技术有限公司

根据扩展方式的不同 MPLS VPN 可以分为 BGP 扩展实现的 MPLS VPN 和 LDP 扩展实现的 VPN。根据 PE（Provider Edge）设备是否参与 VPN 路由又细分为二层 VPN 和三层 VPN。从实用情况来看，三层 MPLS BGP VPN 相对来说比较成熟，商用较多。

基于 BGP 扩展实现的三层 VPN，其标准是基于 rfc2547 及相关草案 rfc2547 draft-rosen-bis。

MPLS BGP VPN 用于解决用户网络 IP 层互连问题、地址隔离问题 VRF - PE 设备上多个路由表，保证用户路由独立性/私有性。通过 MP-BGP 协议分发 VPN 路由和标记。通过 Route-Target 实现 VPN 拓扑发现、并过滤不同 VPN 的路由。

MPLS BGP VPN 是目前应用较多的一种 MPLS VPN 技术，目前各主流厂商基本都支持。华为公司产品支持完善的 MPLS BGP VPN 功能，并且能够与业界主流厂商设备实现互通。

3.2.2 VPN 安全隔离和受控互访

调度数据网需要在同一物理网络上承载多个相对独立的业务系统，通过该系统平台实现统一的业务提供和管理。各业务系统为不同的职能部门开展业务提供服务，其数据流程和管理方式都存在差异，不同业务系统，需要网络平台提供差别服务，如对带宽、实时性有不同的要求，各应用系统的业务网络拓朴模型是不同的，有的应用的需求为星型结构，有的系统为网状结构。不同业务系统之间需要提供安全隔离，不同业务系统之间还可能有相互访问的需求。

其中最重要的可以归结为两点：各业务系统的独立性以及合作关系；对网络平台而言，技术上需要重点实现的也是两个方面：

- 安全隔离

  要保证各业务系统逻辑网络的相对独立性，以满足不同业务系统对安全性、服务质量、管理、拓朴结构的要求。

- 受控互访

  各业务系统之间的流程整合又需要提供相互访问的途径，而且要保证访问的安全性。

经过业界多年的实践，MPLS VPN 技术已被证实是在调度数据网中实现业务系统隔离最有效、最易管理和扩展的技术手段，打造多业务承载平台－实体物理网、虚拟业务网，整合网络资源、降低运营维护成本，已在各级调度数据网中广泛使用。通过 MPLS VPN 可以满足调度数据网的需求，实现在一张物理网上模拟多种逻辑网，分别承载不同的业务。

根据目前地调接入网建设和业务发展的情况，现有的网络有三个 VPN：实时 VPN（一区）、非实时（二区）VPN 以及应急 VPN。由于不同的业务系统之间既要通过 VPN 隔离，又需要保证某些主机能够访问多个 VPN 系统的资源，因此在 VPN 的设置以及受控互访方面建议参照以下原则：

- 按照业务的性质和类型划分 VPN，业务性质相似（访问与被访问）的系统可归为一类，安全一区系统和安全二区系统之间最好完全隔离。
- 根据不同业务之间的互访需求，适当将存在较多互访的业务合并在一个 VPN，以减少 MPLS VPN 受控互访造成的维护管理问题。
- 全网 VPN 数量尽量不要太多，尤其是全国性或跨域的业务。

版权所有 © 华为技术有限公司

- 全网 VPN 的业务设置需要统一，对于开展的 VPN 业务需要申请，自行配置，但是不能影响其他的 VPN。
- 在调度数据网全网中，尽量减少互访的系统数量和用户数量，以保证不同业务系统的安全性。
- 受控访问的控制点建议尽量集中设置，以利于部署策略服务器和防火墙等安全系统。
- 对于多业务系统的终端，建议最好采用认证的方式，不同的业务系统采用不同的帐号接入，其终端的安全策略由其缺省所属的业务系统控制；
- VPN 可以解决业务系统访问的安全性，可以防止非本系统的非法用户对业务系统的访问，但是对于终端的安全性，如病毒攻击泛滥等则需要通过防火墙、IDS 等安全产品解决。

对于受控互访业务，主要包括两类：

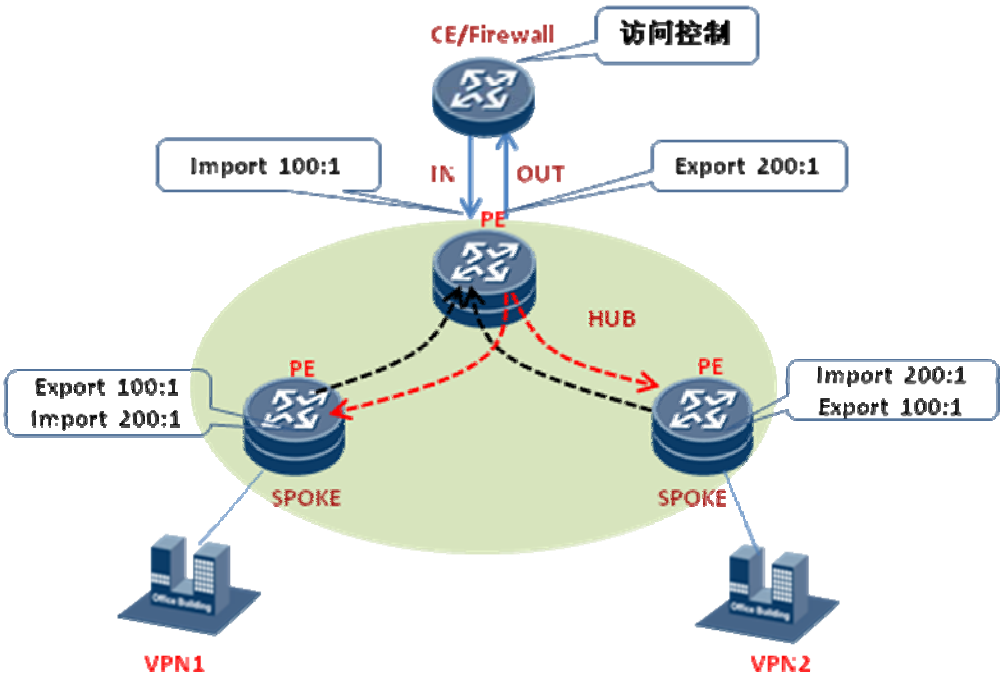
- 业务系统之间部分主机和服务器之间需要交换信息，但没有公共部分，如 OA 系统的部分主机需要访问网管系统的部分主机。
- 业务系统之间有公共部分，部分主机或服务器属于多个业务系统，如分公司某业务系统与电力公司业务系统之间需要互访，而分公司业务系统之间不需要互访。

在部署 MPLS VPN 时，要实现不同业务系统，即不同 VPN 之间的业务受控互访，可以采用如下两种控制方式：

- Hub-Spoke

  Hub-Spoke 方案需要外置 CE 设备，两个 SPOKE 分别对应不同的业务系统的 Site，为了达到受限互通的目的，首先把两个 Site 中的路由通过 IN 接口导入到 CE 设备中。在 CE 设备上采用策略路由等路由过滤机制，然后从 OUT 口将过滤后的路由发布到 SPOKE 上去，从而实现业务系统间的受限访问。

图3-2 HUB-SPOKE 示意图



版权所有 © 华为技术有限公司

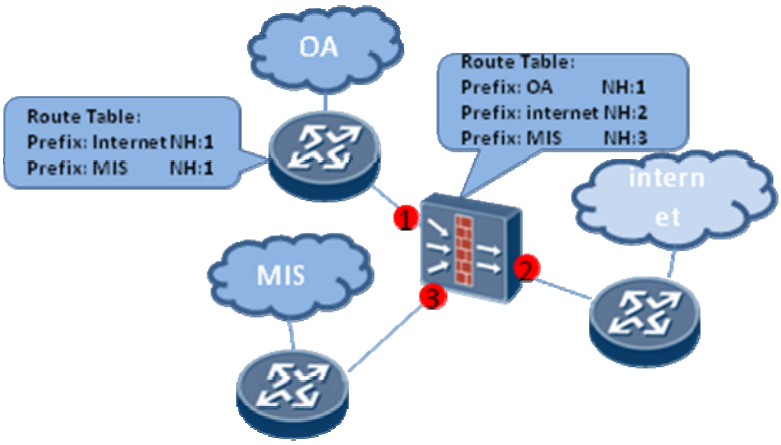
- Extranet

  对于属于多个业务系统的业务互访控制，可以将多个业务系统的公共部分（共享数据库 Site）同时配置到多个业务系统的 VPN 中；通过对 Route-Target 的灵活配置和运用，构建各种特殊的 VPN。另外还需要配合路由策略的过滤，隔离掉各业务系统之间其它 Site 之间的访问。

  对于没有公共部分的互访需求，如不同业务系统之间的互访可以采用 HUB-SPOKE 的实现方案；对于属于多个业务系统的业务互访控制，如电力公司和分公司业务系统之间互访，可以将多个业务系统的公共部分（共享数据库 Site）同时配置到多个业务系统的 VPN 中，采用 Extranet 的实现方案。

  在 Extranet 方式中，可以采用 PE 外挂防火墙的方式，实际上外挂的防火墙类似 MCE，所有的互访策略在防火墙上配置，如图 3-3 所示。

图3-3 Extranet 示意图



  对于图中的三个 VPN，防火墙将出三个端口（可以是 802.1q 的逻辑端口），接到 PE 上，然后 PE 将连防火墙的三个端口分别划入三个 VPN，即每个 VPN 此时将有两个 VRF 接口，一个是接原来的业务服务器的，另一个是接防火墙的。防火墙工作在路由模式，在防火墙上配置各业务服务器的路由指向相应的端口，然后在 OA 站点中配置另外两个站点的路由指到防火墙的端口上，同样的，另外两个站点上也做对等的配置，这样一来，三个站点如果要实现互相访问就会通过防火墙到达对端，我们可以在防火墙上配置过滤规则来实现安全控制以及必要的 NAT 转换。

  如果有多个 VPN 之间需要互访，只需要在防火墙上增加逻辑接口并把它归入相应的 VPN 即可。目前防火墙一般都支持多个域，一个域对应一个端口，并在域之间进行策略部署。这种方案中，防火墙成了连接各个 VPN 的一个枢纽，我们推荐以此方案为主来实现调度数据网受控互访。

另外，对于没有公共部分的互访，也可以采用华为多角色主机方案，在各 VPN（VRF）间泄漏、引入路由，实现各业务系统间的受控互访，可用于“超级首长”访问多个业务系统。与 HUB-SPOKE 方案相比，无须外置 CE 设备，可以由 PE 进行控制。

多角色主机包括三种模式：

- 客户端动态选择 VPN

  通过客户端不同的接入认证方式，包括 L2TP 接入 PE、PPPoE 接入 PE、802.1X 与 VPN 映射、VLAN+Web 等办法，由 PE 根据用户名和密码动态导入不同的 VPN，

版权所有 © 华为技术有限公司

分配不同的 IP 地址。这种方式的 CE 与 VPN 的关系可以是静态的，也可以是动态的。

- PE 选择进入不同的 VPN

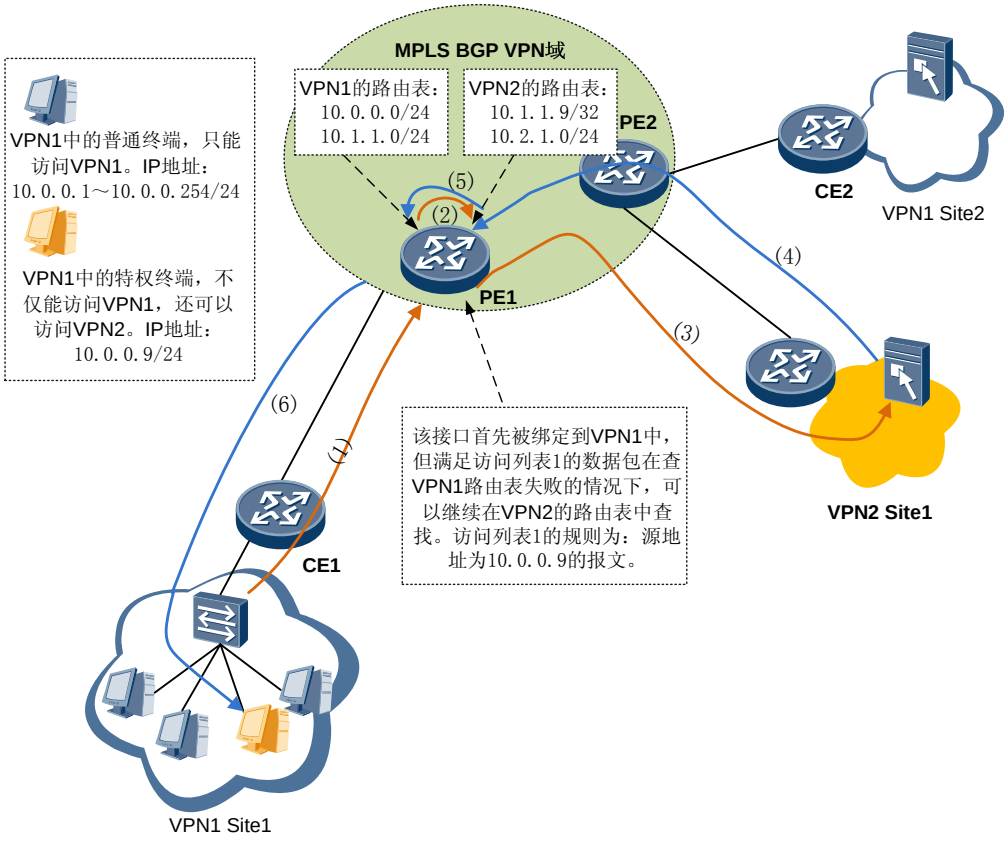
  实现办法可以是基于 ACL 识别 VPN，PE 根据 ACL 区分不同的 VPN 流量，导入不同的 VPN。

- 超级终端或共享服务器

  指的是行政首长或网络管理员，他们可以访问几乎任意资源，或指被多个 VPN 共享的服务器，与 VPN 的关系可以是静态的。实现方式是为终端配置一个专用 VRF，与多个 VPN 交换路由 VRF，并配置 Firewall 保护该终端或服务器，在这里，也可以对超级用户进行认证（L2TP/PPPOE/802.1X/VLAN）。

多角色主机技术，通过在 PE 上，将某个 VPN 的某条路由发布到另外一个 VPN 当中，不同 VPN 的站点间可以学习到个别主机的路由，从而实现特殊服务器可以同时被多个 VPN 来访问，这种互访不经过防火墙，减轻了防火墙的压力，针对需要跨 VPN 访问的且数据流量大的个别主机应用多角色主机技术，如下图：

图3-4 多主机角色



VPN 网关控制的方式就是客户端动态选择 VPN，通过客户端不同的接入认证方式，如 L2TP 接入 PE 的办法，由 PE 根据用户名和密码动态导入不同的 VPN，分配不同的 IP 地址。缺省情况下，用户仅能访问所属的业务系统，当用户需要访问其他业务系统时，通过 L2TP 接入到 VPN 网关，由 VPN 网关控制用户的接入。可以在全网统一部署 VPN

版权所有 © 华为技术有限公司

网关设备，网关设备需要支持 LNS，并对用户实现不同的策略控制，用户端需要支持 LAC 功能。VPN 网关设备的部署比较灵活，所需设备量少，可以集中部署。

3.2.3 MPLS VPN 跨自治域方案

目前业界对与两个自治系统之间的 MPLS/VPN 互联方式主要有以下三种方案，Option A、B、C，下面将详细说明。

Option A（vrf-to-vrf 方式）

这种方法一般都为天然支持，其对于 VPN 路由的转发是首先由一个 AS 的 PE 把 VPN 路由发给该 AS 的 ASBR，ASBR 与对方 AS 的 ASBR 通过多个接口或子接口绑定到 VPN 实例中（需要实现多少个 VPN 跨域就要绑定多少个接口），ASBR 之间在不同 VPN 实例的链路上运行 EBGP（注意不是 MP-eBGP），两个 AS 的 ASBR 都会认为对方是自己的一个 CE 设备。这样 VPN 路由就会像普通路由一样传递，最后两个 ASBR 会把学到的 VPN 路由导入到相应的 VPN 实例中，然后发给各自的 PE。

这种方式虽然属于天然支持，但是由于需要在 ASBR 上需要为每个 VRF 配置独立的链路，因此扩展性比较差，所以这种跨域技术只适合 VPN 数量很少的情况下。

Option B（MP-eBGP 方式）

这种方式在两个 ASBR 之间运行 MP-EBGP 协议，MP-EBGP 协议将一个域内的所有的 VPN 信息传递给另外一个域，传递的是私网路由和标签信息，因为 MP-EBGP 在传递路由时，是要改变路由的下一跳，根据一个标签分配的原则，当一个 FEC 的下一跳被改变时，必须在本地更换标签，因此 ASBR 在收到域内的 VPN 路由信息，再向外发布时，必须给这些 VPN 路由信息重新分配标签，VPN 路由信息伴随着新的标签被发布出去，而在 ASBR 本地，新旧标签形成一个标签的交换操作。

对端的 ASBR 收到从 MP-EBGP 来的 VPN 路由信息后，在本地保存，再继续向自己域内的 PE 设备扩散，当这个 ASBR 向域内的 MP-IBGP 邻居发布路由时，它可以选择不改变路由的下一跳，或是将路由的下一跳改为自己，如果改变了路由的下一跳，同上面的标签分配原则，也需要为这些 VPN 路由重新分配标签，在本地形成标签的交换操作。因此，可以看出不改变下一跳的实现方式的效率比较高，比改变下一跳的方式少了一次标签交互的过程，部署 MP-eBGP 跨域的时候要采用不改变下一跳地址的实现方式。

这种方式的缺点是 ASBR 需保留 VPN 路由，对 ASBR 设备性能要求较高。

Option C（Multi-hop MP-eBGP 方式）

在 MP-EBGP 方案中，存在对 ASBR 设备性能要求问题，因此自然而然想到最好的解决办法就是在跨域情况下，也和一个域的 MPLS VPN 网络一样，VPN 路由是直接可以扩散的，不需要中间设备的保存和扩散。

通过多跳 MP-EBGP 可以解决上述问题，但是这种方式需要有两种标准支持：Labeled EBGP (RFC 3107)和 MP-BGP（RFC2283），Labeled BGP 传递 PE Loopback 路由并携带标签，华为 NE 路由器产品的 BGP 协议对这两个标准已经进行了很好的实现。

多跳 MP-EBGP 又分为 PE 间多跳 MP-EBGP 与 RR 间多跳 MP-EBGP。部署这种跨域的时候需要注意以下情况：RR 间 MP-EBGP 不能更改下一跳，保证 VPN 路由下一跳不发生变化，通过 BGP 的属性控制 VPN 流量。

版权所有 © 华为技术有限公司

三种跨域方案的比较与选择

下面从几个方面比较上述三种方式：

表3-2 VPN 跨域方案比较

比较项目	VRF-to-VRF 方式	MP-eBGP 方式	Multi-Hop 方式
ASBR 转发方式	最长匹配算法查找 FIB，PUSH 标签	精确匹配算法查找 ILM，SWAP 内层标签	精确匹配算法查找 ILM，SWAP 中间层标签
ASBR 维护 VPN 路由	维护 VPN 路由	维护 VPN 路由	不维护 VPN 路由
AS 间分布 VPN 路由的方式	多个 IGP/BGP 实例，每个实例分布一个 VPN 的路由	ASBR 间采用 MP-EBGP	PE/RR 间采用 Multi-Hop MP-EBGP
ASBR 间(子)接口数目	至少同 VPN 数目相当	最少需要 1 个	最少需要 1 个
提高可扩展性的方法	采用多个 ASBR	采用多个 ASBR	采用 RR
提高冗余性的方法	采用多个 ASBR	采用多个 ASBR	采用多个 RR/ASBR
ASBR 的开销	最大	中间	最小
PE 的开销	小	小	若不采用 RR，非常大
ASBR 是否同 RR 合设	可以	可以	不推荐
方案的可靠性	一般	一般	最高
PE 上标签栈深度	2	2	3

综上所述，第一种方式适合于跨域 VPN 数量较少，对扩展性要求不高。在网络发展到较大规模，跨域 VPN 数量不断增多的时候，扩展性、可管理性就是至关重要的。从可管理性的角度，第二种方式较优，从扩展性的角度，第三种方案最佳。

- VRF to VRF：该方案只适合小型网络之间的互联，不适合省调大型网络部署。
- MP-EBGP：该方案配置较为简单，易于维护。但对于 ASBR 路由器来说需要维护全网 VPN 的所有路由，负担较重。
- Multi-Hop：该方案需要 BGP 支持公网发送标签的能力，配置比较复杂。但是其好处在于可靠性高，收敛速度快，且 ASBR 不需要维护 VPN 路由，负担较轻。

版权所有 © 华为技术有限公司

华为路由器对于跨域三种模式都能全面支持。实际部署可根据现网设备情况选择不同的跨域方式。

3.2.4 华为分层 PE（HoPE）方案

BGP/MPLS VPN 中，由于 PE 设备要汇聚多个 VPN 的路由，在大规模部署时，尤其在 PE 设备容量较小的情况下，容易形成瓶颈；而且，目前的 MPLS VPN 模型基本上是一种平面式模型，PE 设备无论处于网络的哪个层次，对其性能要求是相同的；由于路由逐层聚合，甚至在 PE 向边缘方向扩展时，要维护更多的路由。典型网络是核心—汇聚—接入三层模型，设备性能依次下降，网络规模依次扩大，这就为 PE 设备向网络边缘的扩展带来了困难。

针对以上问题，华为公司提出了一种全新的 VPN 拓扑方案，是一种分层式 PE 的概念。在这种方案中，PE 设备所连的不再仅仅是一个客户接入设备 CE，而也可以是一个 PE 设备，更普遍的说可以是一个 MPLS VPN 的网络，这个网络中的 PE 同原来的 PE 形成一种层次关系，称为下层 PE (Underlayer PE)，简写为 UPE，相对的，原来的 PE 称为上层 PE(Superstratum PE)，简写为 SPE。这种框架结构称为 PE 的分层结构(Hiberarchy of PE)，简写为 HoPE。

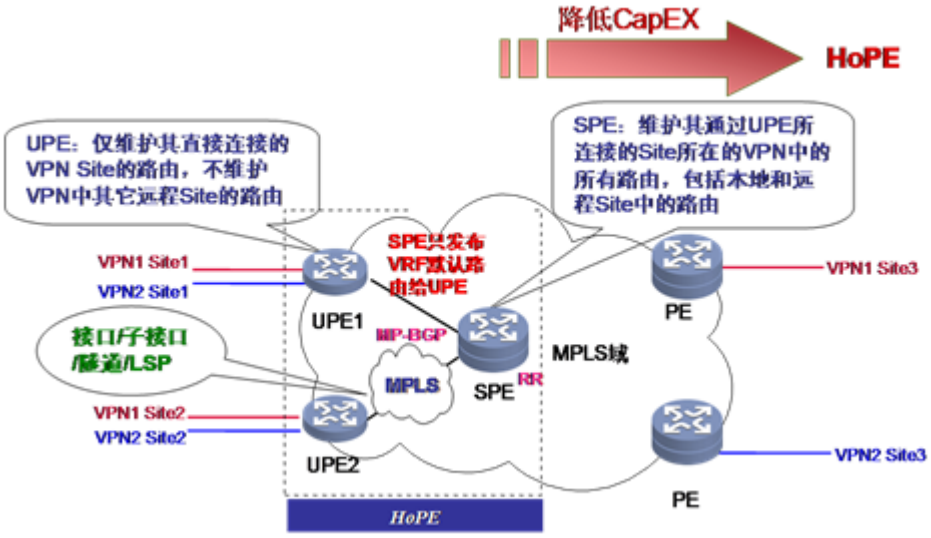
多个 UPE 同 SPE 构成分层式 PE，共同完成传统上一个 PE 的功能。它们之间的分工是：

- UPE 维护其直接连接的 VPN Site 的路由，但不维护 VPN 中其它远程 Site 的路由或仅维护它们的聚合路由；SPE 维护其通过 UPE 所连接的 Site 所在的 VPN 中的所有路由，包括本地和远程 Site 中的路由。
- UPE 为其直接连接的 Site 的路由分配内层标签，并通过 MP-BGP 随 VPN 路由发布这个标签给 SPE；SPE 不发布远程 Site 中的路由给 UPE，而是只发布 VRF 默认路由或聚合路由给 UPE，并携带标签。
- UPE 和 SPE 之间可以采用 MP-IBGP，也可以采用 MP-EBGP。在采用 MP-IBGP 时，SPE 作为各个 UPE 的路由反射器(RR)，UPE 作为路由反射器的客户端(RR Client)，但 SPE 不作为其它 PE 的路由反射器。在采用 MP-EBGP 时，UPE 一般使用私有自治系统号。

如下图所示：

版权所有 © 华为技术有限公司

图3-5 HoPE 示意图



UPE 和 SPE 之间采用标签转发，因而只需要一个(子)接口相互连接。这个接口可以是物理接口，子接口(如 VLAN、PVC)或者隧道接口(如 GRE、LSP)。在采用隧道接口的时候，SPE 和 UPE 之间可以相隔一个 IP 网络或是 MPLS 网络。

分层式 PE 从外部来看同传统上的 PE 没有任何区别，因此它可以同其它 PE 在一个 MPLS 网络中共存。

本方案采用多个设备组成分层式 PE，它们承担不同的角色，分担一个集中式 PE 的功能。对处于较高层次的 PE 的路由和转发性能要求高，而对处于较低层次的 PE 的路由和转发性能要求低，同典型的网络模型相吻合。分层 PE 方案解决了在部署网点 UPE－SPE－P 三级 BGP/MPLS VPN 时的可扩展性问题，可以实现调度数据网向分公司延伸，具有以下优势：

- 保证了传统网络的分层结构。
- 降低了边缘 PE 设备的档次和成本，方便 VPN 向末端延伸，大幅度提高 MPLS VPN 的用户容量和接入能力，扩大 MPLS VPN 覆盖范围。
- 大大减少等效 PE 数目及 MPLS LSP，降低了 MPLS VPN 部署的复杂度。
- 可以无限级联，扩展性良好。
- 降低对传输资源的需求，UPE 就近接入 VPN 用户，采用本地专线甚至宽带接入，更低价格、更大带宽、高性价比、具备良好的扩展性。

3.2.5 华为 MCE 方案

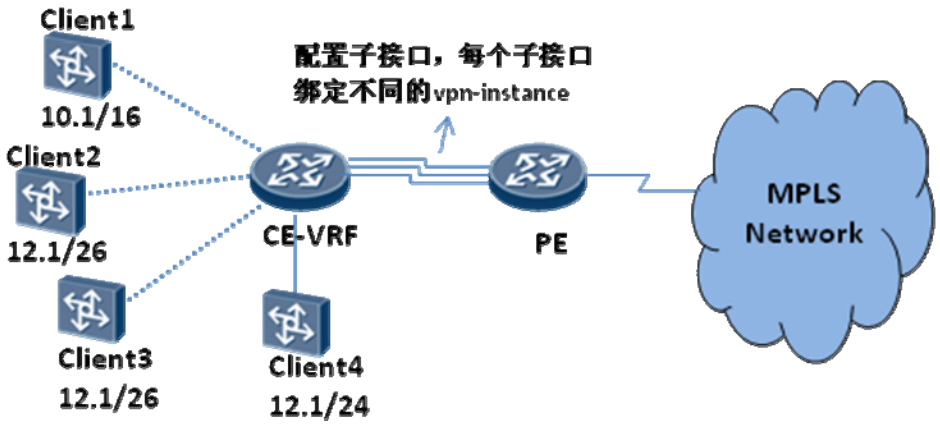
在实现不同业务系统之间的隔离方式上，还可以采用 MCE（多实例 CE）的解决方案。MCE 是基于 MPLS-VPN 中多实例的概念提出的，通俗的讲就是分层 CE，也就是在传统意义上的一个 CE 上实现多个 CE 的功能，MCE 就是在一个上 CE 实现在不同机构或着业务之间的隔离，而且每个机构或者业务有自己私有地址空间，这样可以通过不同的接口或者子接口分别绑定到不同的 VPN-Instance 来实现业务和地址的分离。

版权所有 © 华为技术有限公司

MCE 特性了扩展 CE 的功能，具备 VRF 能力：一个 CE 接入多个 VPN 用户，模拟多个 CE 设备；MCE 同 PE 通过多个(子)接口连接；MCE 只需要维护本地 Site 的路由，另外对上接的 PE 没有特殊的要求，PE 不需要做任何修改。

MCE 可以通过多实例的 IGP 协议（例如： RIP、OSPF、BGP）来实现。如图 3-6 所示：

图3-6 MCE 配置示意图



在 MCE 上配置多个 VRF，对应多个 VPN 站点。在每个 VRF 下，有若干个下行接口（或子接口），同时有一个(也可以是多个接口或子接口)上行接口，这个接口同 PE 连接。在 PE 上，对应的配置同样的 VRF，每个 VRF 有一个(也可以是多个接口/子接口)接口，这个接口同 MCE 连接。这样，一个具有多实例特性的 CE 实际上模拟了多个 CE，各个虚拟的 CE 相互隔离，可以接入多个 VPN 用户，而 PE 设备是不会感知这是多个 CE，还是一个 CE，因而不需要做扩展。

这种方案的最大问题是配置复杂，需要在 PE 与 CE 之间建立多条逻辑通道，通常是 GRE 或者 802.1q 隧道，另外在 CE 与 PE 上要做重复的配置。

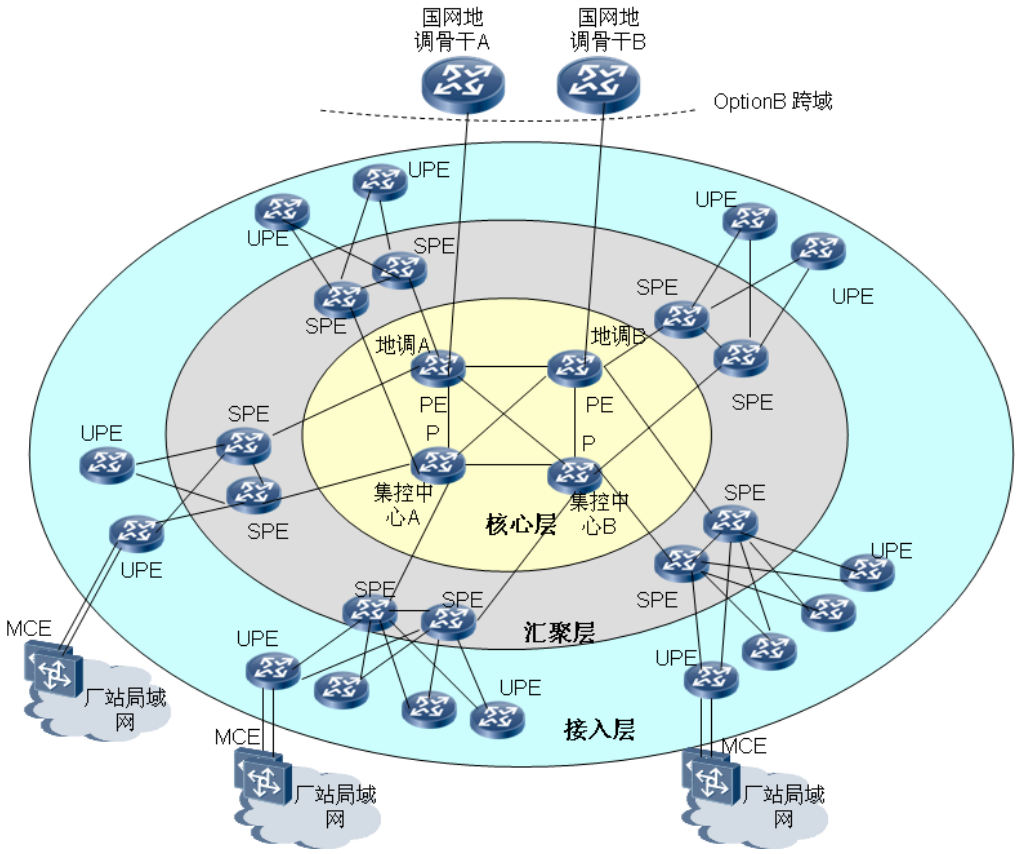
3.2.6 MPLS VPN 部署方案

基于以上 MPLS VPN 相关技术介绍，结合地区调度网现状，根据现网层次划分，建议采用分层 VPN 的方案，用于简化配置，降低厂站 PE 路由器负担，减轻厂站接入对整网路由的冲击。

接入路由器作为 PE，为不同业务构建不同的 VPN，包括实时 VPN、非实时 VPN 和应急 VPN。为了控制 VPN 路由数量，可以采用 HoPE 组网方案，其中接入路由器作为 UPE，核心路由器作为 SPE。对于厂站内网局域网，使用 S57 交换机堆叠，并采用 MCE 方式接入不同的 VPN。

版权所有 © 华为技术有限公司

图3-7 VPN 部署方案



- 核心层

  两台地调核心作为 PE 设备，分别与每一台汇聚层路由器建立 MPLS BGP 连接，两台集控中心路由器作为 P 设备。其中地调核心 A、B 分别上连至国网地调骨干 A、B 平面，由于地调接入网采用独立的 AS 编码，因此需要跨域才能跟骨干网互通。考虑到现网设备互通，建议采用 OptionB 方式跨域。ASBR 之间可通过静态路由方式互相通告 Loopback 地址并建立 MPLS 隧道。

- 汇聚层

  各地调 110KV/220KV 变汇聚路由器，以及区、县调汇聚路由器作为 SPE，上行与地调 A、B 核心路由器建立 MPLS BGP 连接，并正常发布和接收 VPN 路由；下行与各厂站接入层 UPE 建立 MPLS BGP 连接，只对其发布默认路由。由于每个汇聚点有两台路由器，因此每个 UPE 会收到两条默认路由，因此需要通过 Cost 的设置使其按照最优路径选择。

- 接入层

  各 35KV/110KV/220KV 变接入路由器作为 UPE，与上层汇聚层设备建立 MPLS BGP 连接，按照普通 MPLS VPN 进行部署，无需专有配置。

- 厂站局域网

  厂站内网使用三层交换机进行汇聚，为增强可靠性，扩展带宽，可将多台 S5700 交换机进行堆叠。采用 MCE 方案，在一台交换机或一组交换机部署多个 VPN。

版权所有 © 华为技术有限公司

在电力的调度数据网，调度骨干网和各级调度接入网分属不同的 AS 域，例如 A 平面的调度骨干网 AS 号为 20000，各级调度接入网的编号则是 2XXYY 格式，XX 为国网省编码，YY 为各地区编码。因此在构建 MPLS VPN 时，需要进行跨域 VPN 部署。

跨域 VPN 有 OptingA（VRF-to-VRF）、OptionB（MP-EBGP）和 OptionC（Multi-hop MP-EBGP）三种部署方式。而根据电力调度网的相关规范，在电力调度网中，主要采用 OptionB 方式。

在 OptionB 方式下，两个 ASBR 之间运行 MP-EBGP 协议，MP-EBGP 协议将一个域内的所有的 VPN 信息传递给另外一个域，传递的是私网路由和标签信息。对端的 ASBR 收到 VPN 路由信息后，在本地保存，再继续向自己域内的 PE 设备扩散。

所有的 PE、SPE、UPE 节点都应运行 MP-IBGP，为了减少 IBGP 的链接数量，采用分层 PE，VPN 路由信息的更新仅在核心和汇聚层的路由器（SPE 和 PE）间进行，收敛时间更快；同时各个厂站的路由器（UPE）仅需知道直连的 VPN 路由，不需要知道和处理所有的 VPN 信息，大大减少了直调厂站节点路由器的处理压力，可以使用处理能力相对较小的设备。

SPE 和 UPE 之间可以直连，也可相隔一个 IP 网络或是 MPLS 网络。

UPE 是遵循通常 MPLS VPN 标准的普通 PE 设备，目前华为 NE 系列路由设备可以作为 SPE 设备。

3.3 QoS 设计

3.3.1 QoS 概述

IP QoS (Quality of Service) 是指 IP 网络的一种能力，即在跨越多种底层网络技术（FR、ATM、Ethernet、SDH 等）的 IP 网络上，为特定的业务提供其所需要的服务。衡量 IP QoS 的技术指标包括：

- 带宽/吞吐量：指网络的两个节点之间特定应用业务流的平均速率；
- 时延：指数据包在网络的两个节点之间传送的平均往返时间；
- 抖动：指时延的变化；
- 丢包率：指在网络传输过程中丢失报文的百分比，用来衡量网络正确转发用户数据的能力；
- 可用性：指网络可以为用户提供服务的时间的百分比。

不同的用户及业务对 IP QoS 技术指标的要求是不同的，通过有效地实施各项 IP QoS 技术，使得用户能够有效地控制网络资源及其使用，能够在单一 IP 网络平台上融合语音、视频及数据等多种业务，能够在现有网络上细分客户、针对不同的客户需求提供特色的差别业务、以便能迅速获得利益回报、从而进一步扩大市场占有率、提高市场竞争力。目前 IP QoS 主要包括 InterServ 和 DiffServ 两种模式。

对于采用 MPLS 转发，在 MPLS 中有以下几种 QoS 的技术：

- MPLS DiffServ 方案

  MPLS 与 DiffServ 都具有很好的可扩展性、处理过程也类似。在网络边缘聚合（DSCP 或 Label）、在网络核心处理（基于 DSCP 的 PHB 或基于 Label 的转发）；如果将 DS

版权所有 © 华为技术有限公司

字节的设置融入 MPLS 的标记分配过程中，MPLS 的标记将具备区分分组服务质量的能力。MPLS 与 DiffServ 的结合称为 MPLS CoS。

IP 报文头的 DS 字节对 MPLS 设备（LSR）是不可见的，因此必须存在某种机制让 DS 字节对 LSR 是可见的，根据将 IP DiffServ 信息通过 Label 传达给 LSR 方式的不同，业界存在两种 MPLS CoS 的解决方案：

- E-LSP ：在 LER 上将 IP DS 字节映射到 MPLS Label 的 EXP 位，通过 EXP 位向 LSR 表示分组的 QoS 要求，这样一个 LSP 最多可支持 8 个服务等级；LSR 根据 Label 和 EXP 对分组进行队列调度，根据 EXP 进行报文丢弃，同一 LSP 中的分组可能被分到不同的队列；E-LSP 是通过 LDP 协议建立的普通的 LSP。
- L-LSP：在 LER 上将 IP DS 字节映射为一个 LSP，通过 Label 和 EXP 位向 LSR 表示分组的 QoS 要求；LSR 根据 Label 对分组进行队列调度，根据 EXP 进行报文丢弃，同一 LSP 中的分组被分到同一个队列；L-LSP 需要通过 CR-LDP 或 RSVP 扩展来建立，有一定的 QoS 能力。

选择上述两种方案主要取决网络所规划的业务类别数目、分组丢弃值以及 MPLS 运行的模式（帧模式或信元模式）。当采用信元模式的 MPLS 操作时，Label 与 VPI/VCI 相对应，只能采用 L-LSP，此时将 Label 的 EXP 映射为信元的 CLP；当采用帧模式的 MPLS 操作时，采用 E-LSP 或 L-LSP 方案都可以；目前大部分网络所使用的业务等级都在 4 个以内，所以 E-LSP 基本能够满足应用，又能很容易与 IP Precedence 和 802.1p 做到互通； L-LSP 与 MPLS DS-Aware TE 使用了很多相同的机制，DS-TE 本身就使用 L-LSP，两者都可以为不同服务等级的业务提供不同的 LSP、满足业务要求，但 DS-TE 比 L-LSP 功能更为强大，例如：DS-TE 可以对整个网络的资源进行优化。目前 MPLS DiffServ 的相关 RFC 草案尚未形成标准，业界趋向于采用 E-LSP 方式。

- MPLS TE 方案

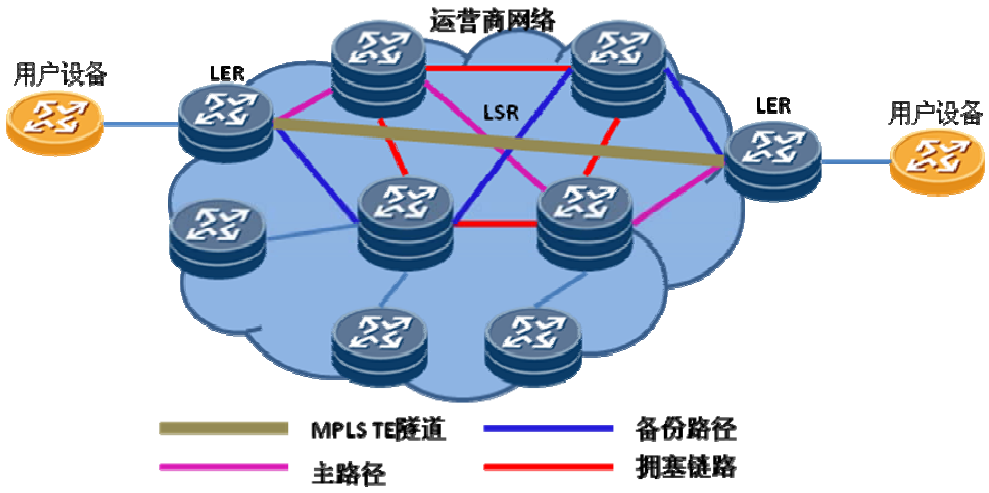
  MPLS TE 是一种间接改善网络 QoS 的技术。传统路由协议（如 OSPF 或 IS-IS）主要是保障网络的连通性和可达性，通常选取不是非常灵敏的参数作为 SPF 计算根据，导致网络负载不均衡、路由动荡等缺陷；MPLS TE 利用了 LSP 支持显示路由的能力，在网络资源有限的前提下，将网络流量合理引导，达到实际网络流量负载与物理网络资源相匹配，间接改善了网络的服务质量。

  MPLS TE 通过对 IGP 协议（OSPF 或 IS-IS）进行扩展，使其能够收集网络流量信息（包括最大链路带宽、最大保留带宽、当前保留带宽和链路类别等）形成流量工程数据库（TED），每个 LER 根据自己的 TED、结合各类策略实施在线约束路由计算，得到显示路由（从它开始的 LSP 路径），最后显示路由（LSP）通过信令协议 CR-LDP 或 RSVP 扩展来部署。

  根据用户需求（显示路由、带宽等）及网络资源的情况，MPLS TE 能够自动通过 CR-LDP 信令（或 RSVP 扩展）建立一条跨越骨干层的从 LER 到 LER 的隧道，同时可完成隧道的维护、统计、属性修改（如带宽）及备份等功能；LER 与 LER 设备之间，可以认为通过一个隧道直连；MPLS TE 隧道可广泛应用于 VPN、各类接入及互联业务中。MPLS TE 隧道如图 3-8 所示。

版权所有 © 华为技术有限公司

图3-8 MPLS TE 隧道示意图



通过 MPLS TE，可为用户创建具有带宽保证的隧道，但如果在隧道中同时传送 EF、AF 及 BE 业务时，业务之间会相互干扰，也就是说 MPLS TE 存在一个严重的问题，即 MPLS TE 隧道不能够感知业务类型。

- MPLS DiffServ-Aware TE 解决方案

  DiffServ 提供了基于类的 QoS，具有良好的可扩展性，但缺乏有效的端到端部署的机制。MPLS TE 通过有效地管理带宽资源间接改善网络服务质量，但其带宽管理以及 MPLS TE 隧道都无法做到基于业务类别（时延），如果 EF、AF、BE 业务都承载在一个 MPLS TE 隧道中 EF 和 AF 业务将受到严重的影响。MPLS DiffServ-Aware TE 在原来 MPLS TE 的基础上，增加了基于类别的资源管理，例如：可根据带宽及时延的不同将接口资源划分为 EF、AF、BE 三类，通过 IGP 协议对每个类别的资源使用情况进行收集、分别建立 TED，通过信令协议携带类别建立 LSP。MPLS DS-TE 充分利用了 DiffServ 的可扩展性以及 MPLS 的显示路由能力，是解决骨干层 QoS 的有效技术，网络资源可根据用户的需求，得到最优的利用。

业界解决 QoS 问题的思路：

如果网络单点出现拥塞，可通过 Metric 做局部调整，或采用 DiffServ；如果网络多点出现拥塞，应全面提升链路带宽；如果网络多点出现拥塞又不升级网络，此时应采用 MPLS TE，确保关键业务的 QoS 及可靠性。

目前，华为 VRP 平台及数据设备已经实现了对上述 IP DiffServ、MPLS DiffServ（E-LSP）、TE 以及 MPLS DS-TE 的支持。

3.3.2 流分类及流量监管

实现 QoS 分类一般根据源 IP 地址、目的 IP 地址、IP 层协议端口、应用层源端口/目的端口及在边缘接入设备上按照接入接口等进行流量标记。

对经过分类的流量作标记，对于路由器组成的 IP 核心网络 Diffserv 域，用 DSCP 和 IP Precedence 相兼容的标记方式；对于路由器组成的 MPLS 核心网络 Diffserv 域，用 MPLS 包头的 EXP 作标记。标记在整个调度数据网 Diffserv 域全局有效，并与骨干层相衔接，在 Diffserv 域中的路由器根据标记提供不同优先级的转发处理。

版权所有 © 华为技术有限公司

对于从 IP 转发到 MPLS 转发，及 L2 层 QoS 到 IP QoS 之间的映射，需要考虑映射关系，对标记出来的各种业务，可以采取直接对应拷贝的方式，也可基于配置进行业务等级的映射关系。

通过上面的流量分类、业务标记及流量业务映射，达到全程全网的端到端 QoS 保证。QoS 规划的重点是实时调度、网管等实时多媒体业务。

流量监管也就是业界通常使用的 CAR，是流分类之后的动作之一。通过 CAR，可以限制从网络边沿进入的各类业务的最大流量，控制网络整体资源的使用，从而保证网络整体的 QoS。其中包含每种业务流的承诺速率、峰值速率、承诺突发流量、峰值突发流量等流量参数，对超出 SLA 约定的流量报文可指定给予 pass（通过）、drop（直接丢弃）或 markdown（降级）等处理，此处降级是指提高丢弃的可能性（标记为丢弃优先级降低），降级报文在网络拥塞时将被优先丢弃，从而保证在 SLA 约定范围之内的报文享受到 SLA 预定的服务。

在路由器上实施流量监管，配置约定平均速率和突发速率，超过平均速率但小于突发速率的流量重标记为 BE 类型，超过突发速率的流量直接丢弃。流量分类和监管建议尽可能在直接接入的设备上执行，以减少核心汇接路由器的负担。

3.3.3 拥塞避免和拥塞管理

对于电力实时调度等业务必须提供严格的 QoS 保证，由于调度数据网上同时存在 IP 转发和 MPLS 转发流量，因此，应该同时开启 IP DiffServ 和 MPLS E-LSP 功能，实际上，这两种功能的底层 QoS 实现是完全相同的，仅仅是设备识别业务类别时分别察看 DSCP 和 MPLS EXP，后续的队列调度、拥塞避免、流量整形等工作都是相同的。

队列管理的主要目的就是通过合理控制 Buffer 的使用，对可能出现的拥塞进行控制。其常用的方法是采用 RED/WRED 算法，在 Buffer 的使用率超过一定门限后对部分级别较低的报文进行早期丢弃，以避免在拥塞时直接进行末尾丢弃引起 TCP 全局同步问题，同时保护级别较高的业务不受拥塞的影响。

在 PE 设备上，将不同优先级的报文送到不同的 QoS 队列进行调度，并配置合适的带宽。其中，实时调度业务按照严格优先队列(PQ)的方式调度，无需配置带宽，只要有流量就优先转发；其它业务和 VPN 流量的带宽按照实际需要进行配置，在运营中根据实际情况逐步调整，以达到最佳匹配。对于 OA 等办公应用业务流量，除配置队列外，还应当配置拥塞避免，可以避免由于突发流量所造成的网络震荡。

华为数据设备对于时延要求严格的实时业务等，可以利用内部特有的低时延调度算法满足业务要求；对于带宽要求的业务，数据产品的带宽保证算法可以实现严格的带宽保证。应用时用户不必关心内部抽象的调度算法，只需要描述业务的流量特征，比如保证多少兆的带宽、峰值最多多少兆的带宽、要占剩余带宽的比例权重等，路由器会根据配置的流量参数选用不同的调度算法来严格保证要求的服务质量。

华为数据设备队列调度使用 PQ+WFQ 方式，第一级是 PQ（Preference Queueing）模型，严格按优先级进行调度，实时业务作为高优先级可以在处理时通过绝对优先调度而时延极低；第二级采用基于权重的调度模型，带宽保证的要求能够严格地满足。

上述算法在完成队列调度的同时，也通过带宽分配和保证实现了流量整形。

对于 DiffServ 模型，系统为每个端口预留 6 个业务队列，分别对应 BE、AF1-AF4、EF 等业务类别，对 AF1~AF4 以及 EF 队列用户可配置其流量参数，数据报文根据由流分类得到的业务类别进入不同的队列，队列根据所配置的流量参数采用不同的调度算法调度报文。

版权所有 © 华为技术有限公司

3.3.4 QoS 部署方案

在电力调度网中，QoS 采用 Diff-Serv 机制，在 PE（或 UPE）上完成流分类和重标记，在上层网络中按照报文优先级进行队列调度和拥塞控制。

网络业务分类按 VPN 划分，确保安全区 I（控制区）中的业务优先传输。例如在 PE（或 UPE）配置 DSCP 标记如下：

- 实时业务既保证带宽又保证时延，设为 AF4，保证 60%接口带宽。
- 非实时业务设为 AF3，保证 30%接口带宽。
- 应急业务设为 AF2，当其他流量中断时，可使用网络所有带宽。

3.4 可靠性设计

3.4.1 IGP 快速收敛

IGP 路由协议可以堪称 IP 网络的神经系统，也是 IP 网络技术中比较成熟的技术，未来电力网络中的视频监控等业务的高可靠性要求，也对 IP 路由协议提出了更加苛刻的要求，因为普通的 IGP 协议收敛时间根据网络规模等一般都是在 10 秒级别以上，这个是不能满足视频业务对承载网的要求的。IGP 路由协议引进了大量的快速收敛，快速检测技术大大的提高了路由的收敛速度，收敛时间一般可以达到 1-2 秒左右（不同的网络规模，收敛时间有差异），基本上可以满足 NGN 的业务要求。

IGP 快速收敛引进了大量的新技术，包括邻居故障的快速检测技术 BFD，包括增量 SP 计算(i-SPF)，局部路由计算(PRC)等。为了确保 IGP 的快速收敛，在网络 METRIC 设计时，应该尽量让路由的切换点离故障点尽量的近，这样可以进一步的加快收敛速度。如果网络中 LDP 等标签信令协议和 IGP 结合使用，也需要确保相关的标签信令协议的快速收敛。

3.4.2 故障快速检测

电力调度系统中实时业务对数据通信设备的可靠性提出了越来越苛刻的要求，需要在毫秒级别检测故障，通过 IP 快速重路由实现流量倒换和保护。

为满足电力调度高可靠性网络的建设要求，需要一种能够快速检测故障，使流量快速切换到备份链路的快速重路由技术。建议设备提供链路备份技术，实现快速感知端口故障、从而实现流量在 50ms 内倒换到备份接口的 IP/MPLS FRR 技术。提供低代价、更快的链路故障检测机制，支持链路热备份，在链路故障时快速将流量切换到备份链路中，保证业务不中断，提高了数据设备的可靠性。

可采用 APDP/BFD 技术，BFD 提供一种检测链路或系统转发传输流能力的简单方法，BFD 是从基础传输技术中经过逐步发展而来的，因此它可以检测网络各层的故障。它可以用于检测以太网、多协议标记交换（MPLS）路径、普通路由封装以及 IPSec 隧道在内的多种类型的传输正确性。APDP 是华为公司针对于多业务承载网的一种 BFD 的实现方案，已经经过运营商和各大行业的实际应用和验证，在中国移动第二国干网、中国网通 NGN、中国联通国二干上成功商用。

从本质上讲，BFD 是一种高速的独立 HELLO 协议（类似于那些在路由协议中使用的协议，如 OSPF 协议，或可以与链路、接口、隧道、路由或其他网络转发部件建立联系的

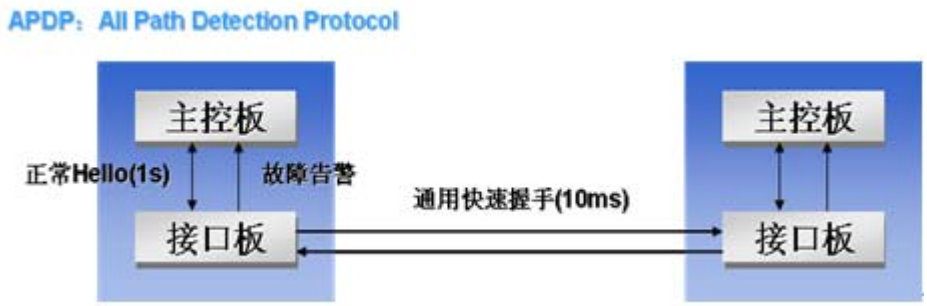
版权所有 © 华为技术有限公司

中间系统到中间系统协议）。BFD 能够与相邻系统建立对等关系，然后，每个系统以协商的速率监测来自其他系统的 BFD 速率。监测速率能够以毫秒级增量设定。当对等系统没有接到预先设定数量的数据包时，它推断 BFD 保护的软件或硬件基础设施发生故障，不管基础设施是标记交换路径、其他类型的隧道还是交换以太网络。

BFD 部署在路由器和其他系统的控制平面上，BFD 检测到的网络故障可以由转发平面恢复（例如在 MPLS 快速重启路由中）或由控制平面恢复（例如当 BFD 用于加快路由协议运行速度时）。

在地调接入网核心骨干节点 P/PE 设备和接入层 PE 设备启动 APDP/BFD，进行节点和链路故障的快速检测，实现备份链路的保护。APDP 原理如图 3-9 所示：

图3-9 APDP 原理



3.4.3 IP 快速重路由

为提高网络可靠性，在网络链路、节点故障时快速响应，采用 IP 快速重路由技术。IP 快速重路由针对被保护接口上的 IP 流量实施快速倒换，速度可达 50ms 以内。

IP FRR 其原理是采用一个接口作为另外一个接口的备份。当主用接口失效，或主用接口连接的邻居失效后，本路由器通过硬件技术快速感知，并马上将通过这个接口转发的流量快速倒换到备份接口上。由于备份接口的下一跳路由器能够对倒换过来的 IP 流量重新路由，报文不会丢弃。

IP 快速重路由部属方便灵活，切换速度快，设备开销小，主要应用于 IP 转发的网络，配合 APDP/BFD 实现链路的备份保护。

3.4.4 MPLS VPN 快速收敛

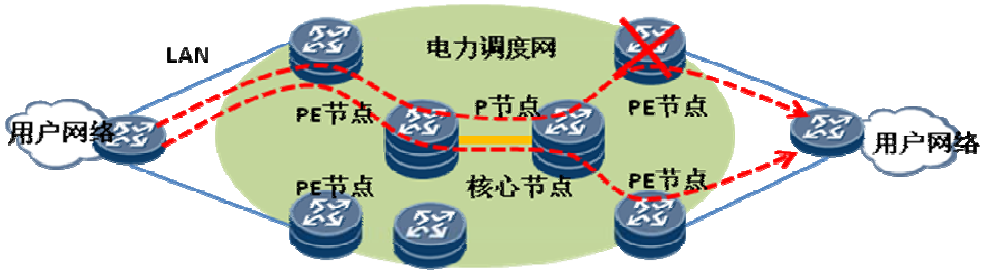
在一般 MPLS VPN 中，由于 CE 双归到两个 PE 路由器，这样在 MPLS VPN 中就存在两条路由，一条选中，一条备份，但是当被选中的 PE 路由器故障后，远端的其他 PE 因为和它不直接相连，因此无法感知到故障因此无法快速实现优选路由和备份路由的切换，只能依赖 BGP 的连接超时（180 秒）来实现路由的切换。一旦 PE 节点发生故障，只能通过端到端的路由收敛、LSP 收敛来恢复业务，其业务收敛时间与 MPLS VPN 内部路由的数量、承载网的跳数密切相关，一般在 5s 左右，收敛时间长，无法满足实时调度业务的要求。

MPLS VPN 快速收敛－VPN FRR 利用基于 VPN 的私网路由快速切换技术，通过预先在远端 PE 中设置指向主用 PE 和备用 PE 的主备用转发项，并结合在两个 PE 之间使用多跳的 BFD 来实现不相邻的 PE 路由器之间的故障快速检测，和预先在远端 PE 中设置指

版权所有 © 华为技术有限公司

向主用 PE 和备用 PE 的主备用转发项，解决 CE 双归 PE 的 MPLS VPN 网络中，PE 节点故障导致的端到端业务收敛时间长（大于 1s）的问题，同时解决 PE 节点故障收敛时间与其承载的私网路由的数量相关的问题，在 PE 节点故障情况下，端到端业务收敛时间小于 1s，从而就可以实现 MPLS VPN 路由在故障时的快速切换。一般 VPN FRR 需要在两个方向同时部署，如图 3-10 所示。

图3-10 VPN FRR 部署方案



建议在调度数据网的 PE 上部署 VPN FRR，保证调度以及其他业务的可靠性。

总之，在可靠性方面，主要采用 BFD 快速故障检测/MPLS OAM＋IP FRR /VPN FRR/TE FRR 快速切换(<50ms)＋IGP 快速收敛，可以保证网络的高可靠性，实现实时调度业务的承载，实现策略为：

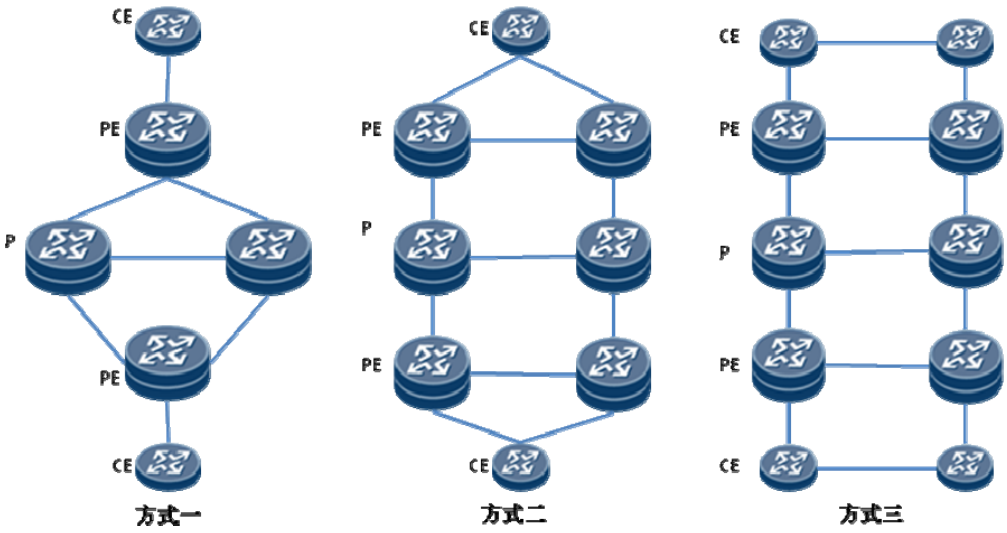
- 首先通过网络设计，采用节点双设备设置和节点设备间对称连接，备份路径预先设定，为实施快速切换提供网络拓扑基础。
- 然后在节点之间部署故障快速检测机制 APDP/BFD，迅速检测到链路或者节点故障。
- 最后通过 IP/VPN/TE FRR 技术切换到预先设定的备用链路，对于 VPN，需要采用 MPLS VPN 快速收敛，使得整个故障切换过程一般保持在 50ms 级别，无须路由协议收敛重新选路。
- 切换结束后，普通路由能够通过 IGP 快速路由收敛到已经切换的链路。

3.4.5 业务系统接入可靠性方案

调度数据网中业务系统通过 CE 接入到 PE 设备，CE 和 PE 之间的连接结构主要包括三种：

版权所有 © 华为技术有限公司

图3-11 CE 和 PE 连接结构



- 方式一中 PE 和 CE 之间采用单链路的连接方式，结构实现简单，但不利用实现基于业务的负载分担。
- 方式二中 CE 采用双归上联的方式与一对 PE 进行连接，CE 可通过动态路由协议调节到两台 PE 路由器的路由优先级，来实现业务的负荷分担和可靠性，可以满足大部分业务的需求。
- 方式三采用双 PE 和双 CE 的全冗余连接结构，CE 和 PE 之间采用动态路由协议，实现负荷分担和链路备份，可以用来保证关键业务的可靠性。

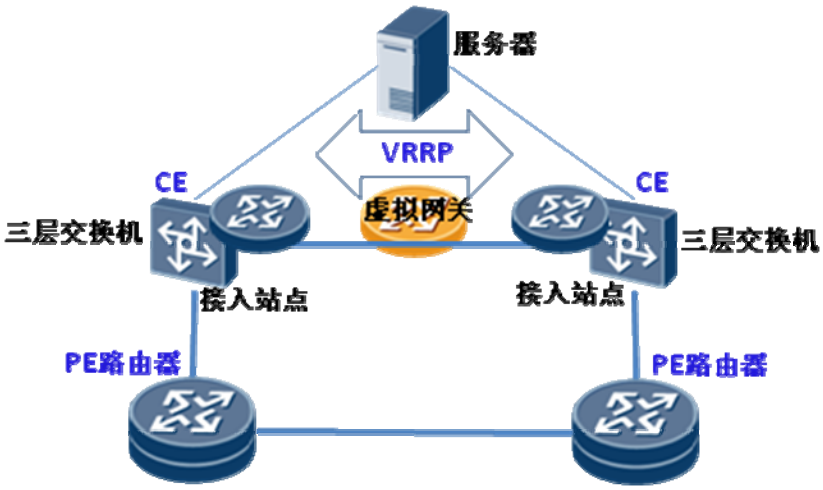
在实际业务系统接入时，主要有以下几种模式：

- 两个专用的三层交换机或支持交换的路由器做 CE，仅仅接入同一种业务的服务器，专用 CE 通过 EBGP/静态路由方式分别与 PE 互连，根据路由策略优选路由，CE 上起用 VRRP 作为网关接入主机。

  这种接入方式适用于大型关键性业务子系统，如：计费、网管，具有高的可靠性保障。

版权所有 © 华为技术有限公司

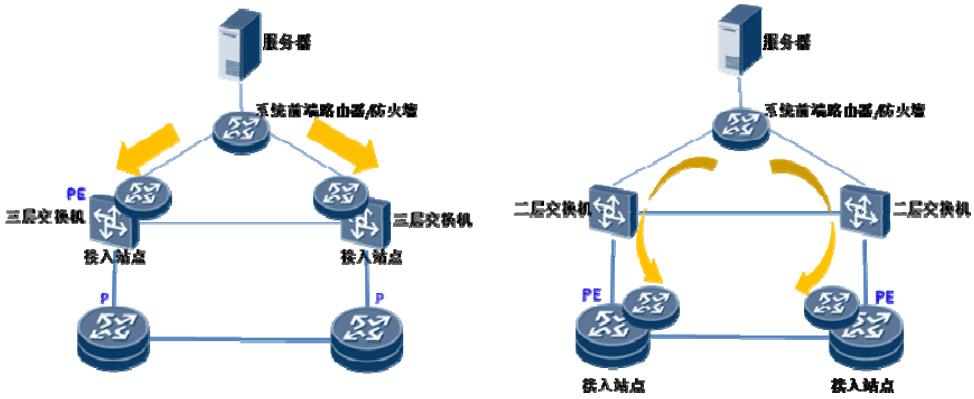
图3-12 双 CE 路由交换机接入方式



- 采用单路由器作为 CE 接入的方式

  如果业务系统前端有路由器或者防火墙（三层模式），通过它们接入骨干层络时，则可使用配置两条路由的方法来实现可靠接入。当配置两条路由等价时，则可实现基于流方式的负载分担；当配置两条路由不等价时，则可实现两条链路的主备冗余。目前在调度数据网中一般采用这种方式接入。如果接入的设备不支持三层功能，仅作为二层使用，则需要下面的路由器与 CE 完成路由的交互。

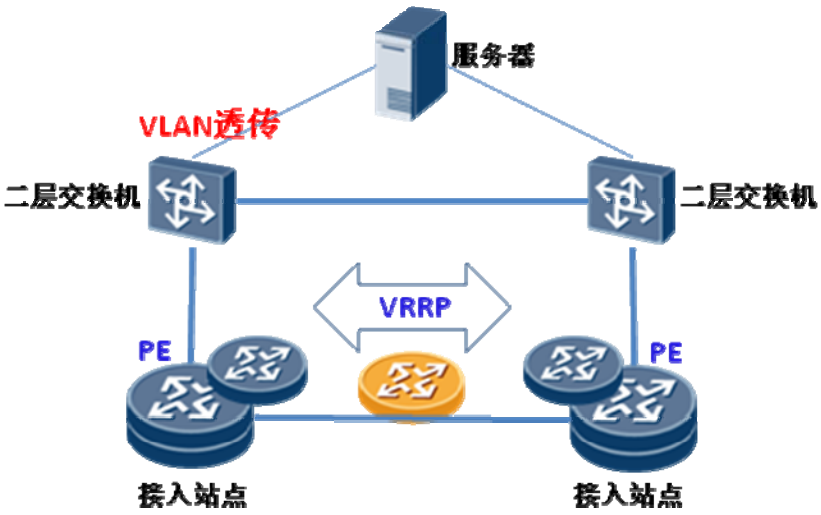
图3-13 单路由器 CE 接入方式



- 多个业务共用 CE，CE 仅仅当二层设备使用，不同业务采用不同的 VLAN，不同 VLAN 分别终结与 PE 不同 VRF 之上。CE 仅仅单归接入某个 PE，或者通过双归连接到 PE，考虑在 PE 上启用 VRRP，以提高可靠性。

版权所有 © 华为技术有限公司

图3-14 二层交换机接入方式



当 CE 双归接入到 PE，可以实现流量备份和负载分担，具体的复杂分担包括两种实现方式：

- 基于流的负载分担

  在某些不对称的网络中，不好实现基于业务的分流，可以采用基于数据流的负载分担。如果只实现网络的主备使用，带宽利用率低，如果将来业务开展需要占用大量网络资源时，就必须采用设备扩容的方式，浪费资金，通过在业务系统的前端设置等价路由，进行基于流的负载分担，可以充分利用网络资源。缺点是不同业务系统之间可能存在互相干扰。

- 基于业务的负载分担

  基于业务负载分担就是在同级别的两台 PE 设备上都设置相同的站点，但是可以通过配置不同 PE 站点具有不同的优先级，继而实现关键业务与非关键业务的承载分离，提高关键业务的可靠性。如可以配置使得网管和是时调度两个关键业务系统在 PE A 设备上的站点优先级高（通过 VRRP 或者路由来实现），这样可以使得实时 VPN 和网管的流量优先上 PE A，而非实时 VPN 流量则优先上 PE B。

3.4.6 可靠性部署方案

对于地调网络结构来说，任意两台 PE 之间都存在两条或以上路径，因此可以在其上部署 LDP FRR，在任意一条链路发生故障后迅速切换到备用路径。PE 之间起硬件 BFD 探测，可保证在短时间内故障感知并快速切换。

对于汇聚层和核心层来说，都是采用双机冗余备份，因此 PE 会发送两条外部路由给 CE，CE/PE 通过 IP FRR/VPN FRR 来实现路由的备份，并通过 BFD for OSPF 加速探测，在 PE 节点故障时 50ms 内感知并迅速切换到备份路由上。

对于厂站接入 UPE 节点来说，由于是双上行到两台 PE，可在 UPE 节点上部署 UCMP 非等价分担，使得流量按照预定的策略分担到两个不同的平面。

版权所有 © 华为技术有限公司

3.5 安全设计

3.5.1 华为产品安全特性

安全验证

- PPP 支持 PAP 和 CHAP 验证方式。
- 路由协议（RIPv2、OSPF、IS-IS、BGP）支持报文明文认证和 MD5 密文认证。
- LDP 和 RSVP 支持 MD5 密文认证。
- SNMP 支持 SNMPv3 的加密和认证。

RPF/URPF 检测

单播反向路径查找 URPF（Unicast Reverse Path Forwarding），防止基于源地址欺骗的网络攻击行为。

一般情况下，路由器接收到报文，获取报文的目的地址，针对目的地址查找路由。如果找到了就转发报文，否则丢弃该报文。URPF 通过获取报文的源地址和入接口，以源地址为目的地址，在转发表中查找源地址对应的接口是否与入接口匹配，如果不匹配，认为源地址是伪装的，丢弃该报文。通过这种方式，URPF 就能有效地防范网络中通过修改源地址而进行的恶意攻击行为的发生。

MAC 限制

华为路由器支持丰富的 MAC 限制功能，可以为大型的二层网络和 VPLS 网络提供多种安全解决方案。

- MAC 地址限制

  随着城域以太网（Metro Ethernet）市场的高速增长，安全在城域网络的入口位置扮演着愈发重要的角色。城域以太网中，大量的个人用户通过以太链路接入 Internet，网络上的黑客和病毒进行 MAC 攻击比较普遍。华为路由器提供的 MAC 地址限制能够有效防范这些攻击，保证用户网络的安全。

  强大的 MAC 表项限制功能，一方面能够限制一个用户接入的 MAC 数目，防止挤占其它用户的 MAC 地址空间；另一方面又能将攻击报文在入口处丢弃，禁止非法报文消耗带宽资源。

  MAC 地址学习是二层转发的基本特性，完全自动进行，使用简单，但必须谨慎规划，以防招致攻击。

  华为路由器支持对 MAC 地址的学习限制功能，包括：

  - 限制最多允许学习的 MAC 数量
  - 限制 MAC 学习的速度
  - 基于端口的 MAC 地址限制
  - 基于 VLAN+端口的 MAC 地址限制
  - 基于端口+VSI 的 MAC 地址限制
  - 基于双层 VLAN（QinQ）的 MAC 地址限制

版权所有 © 华为技术有限公司

MAC 地址学习限制可以应用于接入用户固定但又不够安全的网络环境，如小区接入或缺乏安全管理的企业内部网。当接入的用户数量达到限制值后，新接入的用户 MAC 将不被学习，该用户的流量将全部采用广播方式，速度有限。

- MAC 地址删除

  在 VPLS 和二层组网中，MAC 地址表是转发的关键，同时也是一种易受攻击的稀缺资源，尽管 MAC 地址表项有定时老化机制，但仍然需要为 MAC 地址表提供丰富的表项删除功能，以保证在尽可能少的影响其它正常业务的条件下，快速删除失效的表项，释放 MAC 资源。

  华为路由器提供如下的 MAC 地址表项删除功能：

  - 基于端口+VSI 删除 MAC 地址
  - 基于端口+VLAN 删除 MAC 地址
  - 基于 Trunk 接口删除 MAC 地址
  - 基于 QinQ 出接口删除 MAC 地址

DHCP Snooping

DHCP Snooping 是一种 DHCP 安全特性，可以过滤不信任的 DHCP 消息并建立和维护一个 DHCP Snooping 绑定表。该绑定表包括 MAC 地址、IP 地址、租约时间、绑定类型、VLAN ID、接口信息。DHCP Snooping 的作用就如同在 Client 和 DHCP Server 之间的建立一道防火墙。

DHCP Snooping 主要是解决设备应用 DHCP 时遇到 DHCP DoS 攻击、DHCP Server 仿冒攻击、ARP 中间人攻击及 IP/MAC Spoofing 攻击的问题。

根据不同的攻击类型，DHCP Snooping 提供不同的工作模式，如所示。

表3-3 DHCP Snooping 防攻击模式

攻击类型	DHCP Snooping 工作模式
DHCP 饿死攻击	MAC 地址限制
DHCP Server 仿冒者攻击	信任（Trusted）/不信任（Untrusted）
中间人攻击/IP/MAC Spoofing 攻击	DHCP Snooping 绑定表
改变 CHADDR 值的 DoS 攻击	检查 DHCP 报文的 CHADDR 字段

本机防攻击特性

华为高端路由器提供统一的本机防攻击功能模块完成整个设备防攻击策略的管理和维护，可以为用户提供一套可操作和可维护的全方面防攻击解决方案。

- 白名单

  白名单指合法用户或者是高优先级用户的集合。通过设定白名单信息可主动保护现有业务、保护高优先级用户业务。通过 ACL 可以设置自定义的白名单，后续匹配白名单特征的报文会被采用高速率高优先级上送。

版权所有 © 华为技术有限公司

可将确定为正常使用设备的合法用户或者是高优先用户业务设置到白名单中。

- 黑名单

  黑名单指非法用户的集合。通过 ACL 可以设置自定义黑名单，后续匹配黑名单特征的报文会被丢弃或者低优先级上送。

  可将确定为攻击的非法用户设置到黑名单中。

- 用户自定义流

  用户自定义流指用户自定义防攻击 ACL 规则。主要应用于当后续网络中出现不明攻击时，用户可灵活指明攻击流数据特征，将符合此特征的数据流进行上送限制。

- 动态链路保护特性

  路由器支持通过白名单特性保护所有基于 TCP 的应用层协议的 Session 数据。当 Session 建立时，系统会将 Session 信息同步加入到白名单中，保证当前系统的所有 Session 都受到白名单的保护，以高优先级上送。该特性统称为动态链路保护特性 ALP(Active Link Protection)。通过动态链路保护特性可保护设备已有业务在攻击发生时的正常运行。

  当设备检测到 Session 删除时，会将此 Session 信息从白名单中删除。

- 统一的 CAR 参数配置

  CAR 用来设置上送 CPU 的报文的分类限速上送规则，针对每类报文可设置均值速率、峰值速率、优先级信息等。通过对不同的报文设置不同的 CAR 规则，可以降低报文的相互影响，达到保护 CPU 的目的。

  华为路由器提供更加方便的 CAR 参数配置方法：

  - 可以对不同接口板提供统一的 CAR 参数配置。
  - 对用户提供统一的配置界面。
  - 并且提供常用协议的协议级粒度的 CAR 参数配置，使用户配置界面更加友好。

- 最小包补偿

  华为高端路由器通过最小包补偿功能有效解决小报文攻击问题。路由器收到上送 CPU 的报文后，进行报文长度检测：

  - 如报文实际长度小于预设的最小包长，便使用设定长度计算报文上送速率。
  - 如报文实际长度大于预设的最小包长，便使用报文实际长度计算报文上送速率。

- 应用层联动

  华为高端路由器支持应用层联动功能。路由器可以动态检测开启的上层应用协议业务信息。如果检测到上层业务开启，路由器接收该类业务应用报文并上送 CPU；如果检测到上层业务关闭，路由器直接丢弃此类报文或者以指定带宽限制上送该类报文。

- 本机 URPF

  URPF 功能是在网络入接口同时对转发报文和本机报文进行检测。在大型网络中，为了避免对转发性能造成较大的影响，可以部署本机 URPF。即只对本机报文进行源地址合法性检查，不合法的报文进行丢弃处理，起到防源地址欺骗攻击的效果。

- 管理和业务平面保护

  路由器接口可以分成两类，一类是管理口（管理报文可以通过该接口访问路由器），一类是非管理口。比如城域网的部署，一般来说，下行接用户的接口是非管理口。

版权所有 © 华为技术有限公司

为了防止黑客从非管理口控制设备，或者进行管理报文的 Flood 攻击，华为路由器支持管理平面保护功能，指定只有管理接口可接收管理流量，使管理流量进一步可控。

- TCP/IP 类网络报文防攻击

  当前网络中，基于 TCP/IP 网络的攻击日益增多，造成的影响越来越大。华为路由器支持对如下 TCP/IP 类网络攻击的防范功能。

  - 畸形报文攻击：

    通过向目标系统发送有缺陷的 IP 报文，使得目标系统在处理这样的 IP 包时会出现崩溃，给目标系统带来损失。系统支持对如下畸形报文的转发引擎和软件识别并丢弃：载荷为空的 IP 报文、空 IGMP 报文、LAND 攻击（源 IP 地址和目的 IP 地址一致的 TCPSYN 报文）、Smurf 攻击（目的地址为广播地址或子网广播地址的 ICMP echo request 报文）、满足如下条件的任意一种 TCP 标志位非法攻击（6 个标志位（URG、ACK、PSH、RST、SYN、FIN）全为 1；6 个标志位全为 0；SYN 和 FIN 位同时为 1）。

  - 分片报文攻击

    分片报文攻击造成路由器 CPU 特别忙，使得系统无法接受正常用户的请求，或者系统崩溃不能正常的工作。系统支持对如下分片报文攻击的转发引擎和软件识别，并通过 CPCAR 保证重复分片上送的速率，软件保证重组正确，或丢弃重组有错误的报文。系统支持的分片报文攻击包括：分片数量巨大的攻击和巨大 offset 报文的攻击、重复分片报文攻击、Tear Drop 攻击、syndrop 攻击、nesta 攻击、fawx 攻击、bonk 攻击、NewTear 攻击、Rose 攻击、死亡之 ping 攻击、Jolt 攻击。

  - TCP SYN

    系统支持对 TCP SYN 泛洪攻击的识别，并在接口板上进行限速 CAR 处理。

  - UDP FLOOD

    系统支持对 Fraggle 攻击和 UDP 诊断端口攻击报文的识别，并丢弃或进行基于接口板的过滤。

- 攻击溯源特性

  华为高端路由器支持在设备自身受到恶意攻击时，提取、存储可疑报文，并能格式化显示（包括设备命令行和离线工具显示两种手段），为安全攻击定位攻击源头提供一种简单、易用的辅助手段。

  在攻击发生时，系统自动将攻击报文裁剪掉传输层后面的数据，缓存在内存中。当内存中缓存的报文数目到达一定数量（如 20000 条/板）时，覆盖最先缓存的数据。

ARP 防攻击

在现今的大型网络中，Ethernet 是最常用的接入手段，而 ARP 作为 Ethernet 网络上的开放协议，为恶意用户的攻击提供了可能。恶意用户的攻击主要从空间与时间两方面进行。

空间方面的攻击主要利用路由器 ARP 缓存的有限性，通过发送大量伪造的 ARP 请求、应答报文，造成路由器设备的 ARP 缓存溢出，从而无法缓存正常的 ARP 表项，进而阻碍正常转发；时间方面的攻击主要利用路由器计算能力的有限性，通过发送大量伪造的 ARP 请求、应答报文或其他能够触发路由器 ARP 处理的报文，造成路由器设备的计算资源长期忙于 ARP 处理，影响其他业务的处理，进而阻碍正常转发。

- 基于接口的 ARP 表项限制

版权所有 © 华为技术有限公司

基于接口的 ARP 表项限制能够在 ARP 表项溢出攻击发生的情况下有效的限制攻击影响的范围，使攻击范围局限在接口之内，从而保证整板或整机的其他端口不受影响。

- 基于时间戳的防扫描

  基于时间戳的防扫描特性能够在扫描（无论是 ARP 扫描还是 IP 报文扫描）攻击发生时，及时识别并抑制对扫描产生的请求的处理，从而保护 CPU 免受攻击。

- ARP 双向分离

  由于 ARP 请求报文来自设备外部，并且可以在任意时间由外部设备主动发起，因此，对于 ARP 请求报文，只要它的 IP 地址合法，一般无法区分是正常报文还是攻击报文。

  通过对一些在网上实际发生的 ARP 攻击案例分析知道，在 ARP 攻击流量中，ARP 请求报文和 ARP 响应报文几乎各占 50%。因此，要想有效解决大流量 ARP 攻击问题，必须从 ARP 请求报文和 ARP 响应报文两方面同时入手。

  ARP 双向分离处理是将 ARP 请求和 ARP 响应分开处理。

  - ARP 请求进行“无状态应答”，即在进行 ARP 应答之后不产生 ARP 表项及相关的状态，不上送 CPU 进行处理，而防止了使用 ARP 请求报文对网关设备 ARP 表进行地址欺骗的可能；
  - ARP 响应只上送 CPU 请求过的 ARP 报文，非 CPU 发出的 ARP 请求的 ARP 响应报文将被丢弃，有效地保证了来自正常主机的 ARP 请求报文被及时响应处理。

- 过滤非法 ARP 报文

  华为高端路由器支持对三种 ARP 报文进行过滤，这三种 ARP 报文为：

  - 非法 ARP 报文。包括：目的 MAC 地址为单播的 ARP 请求报文、源 MAC 地址为非单播的 ARP 请求报文、目的 MAC 地址是非单播的 ARP 响应报文。
  - 免费 ARP 报文。
  - 接收方 MAC 地址是非空的 ARP 请求报文。

  可以通过命令行配置同时对上述一种或几种非法报文进行过滤。

镜像功能

镜像是在不影响原有转发的情况下，将网络中通过当前节点的报文复制一份到指定的观测端口。用户可以根据需要定义被镜像的端口号，然后将报文分析设备与观测端口相连，进行流量观测。

根据复制报文满足的条件，镜像分为端口镜像和流镜像两种：

- 端口镜像：指将镜像端口接收或发送的报文完整地复制输出到指定的观测端口。
- 流镜像：指将镜像与流分类相结合，只复制满足特定条件的报文，过滤报文分析设备不关心的报文，为报文分析提供更精细的控制，提高报文分析设备的工作效率。

根据复制报文的方向，镜像又可分为上行镜像和下行镜像两种：

- 上行镜像：指将镜像端口接收到的全部报文或满足特定流分类条件的报文完整地复制输出到指定的观测端口。
- 下行镜像：指将镜像端口即将发送出的全部报文或满足特定流分类条件的报文完整地复制输出到指定的观测端口。

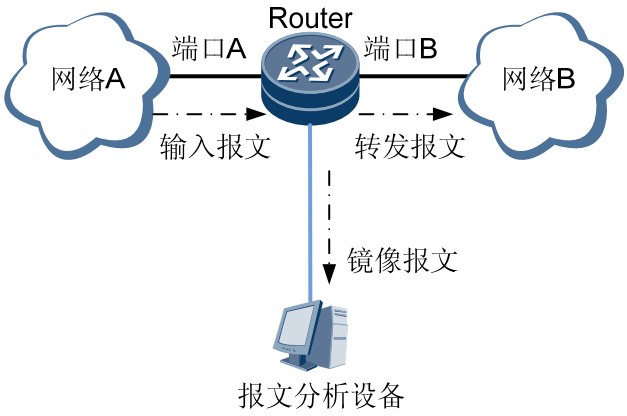
版权所有 © 华为技术有限公司

如果观测端口与镜像端口在同一设备，称为本地镜像；如果观测端口与镜像端口在不同的设备，称为远端镜像。华为路由器既支持本地镜像，也支持远程镜像功能。

- 本地镜像

  本地镜像的典型组网环境如下图所示：

图3-15 本地镜像典型组网示意图



网络 1 和网络 2 通过路由器连通，要监控端口 A 上网络 1 的输入流量，可以将端口 A 的上行流量复制一份镜像报文，流量正常转发的同时，镜像报文可以从端口 C 转发到报文分析设备处理。某些情况下，需要对网络 1 的输入输出流量同时进行监控，路由器需要将端口 A 的上下性流量同时镜像一份到观测端口。

对于本地镜像，系统一个接口板允许配置一个物理观测端口以及多个逻辑观测端口；一个接口板允许配置多个镜像端口。

在进行本地下行镜像时，系统支持跨板镜像，即观测端口和镜像端口可以配置在不同的单板上。并且，如果观测端口是逻辑口，系统还支持对本地镜像报文做限速 CAR。

- 远端镜像

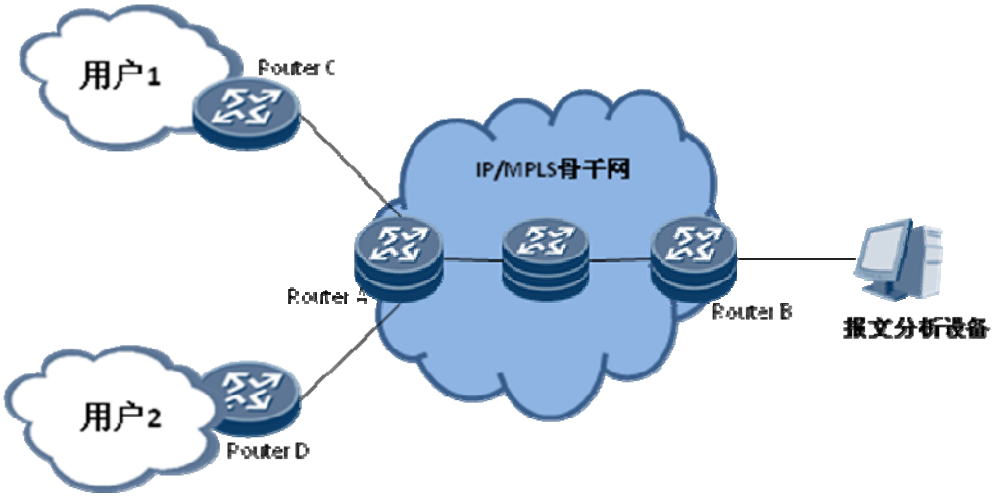
  相对于本地镜像，远端镜像有如下好处：

  - 网络维护人员不需要赶到现场，能够远程分析镜像报文。
  - 一个网络维护人员同时可以处理不同站点设备的镜像操作，节省了维护人力。

  远端镜像的典型组网环境如下图所示：

版权所有 © 华为技术有限公司

图3-16 远端镜像典型组网示意图



RouterA 和 RouterB 是 IP/MPLS 骨干网络的边界路由器，客户端网络 customer 通过 RouterC 和 RouterD 接入骨干网络，出于维护、分析攻击或定位问题的需要，可能需要查看 RouterA 发出或接收的协议报文是否正确，或者察看 RouterC 的一个绑定客户 VPN 的子接口是否受到攻击，这时就需要将 RouterA 收到的某一类协议报文，或者 RouterA 发出到 RouterC 的协议报文，或者 RouterA 的子接口收到的报文镜像到远端 RouterB 的报文分析设备进行分析。

在远端镜像中，远端镜像源的镜像接口的数据会被复制一份从指定的隧道发出，到达远端的一个目的路由器（即远端镜像观测口所在的路由器），然后由该远端镜像观测口输出至报文分析设备。并且每一个远端镜像源和一个远端镜像观测口组成一条流；如果有 2 个远端镜像源的数据都从一个远端镜像观测口输出，那么就是 2 条流。

华为高端路由器支持做为远端镜像的隧道类型有 MPLS LSP，MPLS TE 和 GRE。

对于远端镜像，系统一个接口板支持配置多个观测端口和多个镜像端口。

3.5.2 Netstream

Internet 的高速发展为用户提供了更高的带宽资源，同时要求用户对自己的网络资源进行更细致的监控和管理，因此就需要一种技术来满足此需求。

Netstream 技术就是这样一种基于网络流量信息的统计技术，它可以对网络中的通信流量和资源使用情况进行分类统计，基于各种业务和资源进行网络的监控和管理。
Netstream 支持如下应用：

- 计费

  Netstream 为基于资源（如线路、带宽和时段等）占用情况的计费提供了精细的数据，这些数据包括 IP 地址、包数、字节数、时间、ToS 和应用类型等。ISP 可以利用这些信息来实行灵活的计费策略，如基于时间、带宽、应用、服务质量等。企业客户可以使用这些信息计算部门费用或分配成本，以便有效利用资源。

- 网络规划和分析

  Netstream 可以为先进的网络管理工具提供关键信息，以便优化网络设计和规划，实现以最小的网络运营成本达到最佳的网络性能和可靠性。

版权所有 © 华为技术有限公司

- 网络监控

  Netstream 技术能够实现实时的网络监控功能。RMON、RMON-2 和基于信息流的分析技术可以用来形象化地表示单个路由器和全网范围内的流量模式，并提供预先故障检测、高效故障排除和快速问题解决功能。

- 应用监控和分析

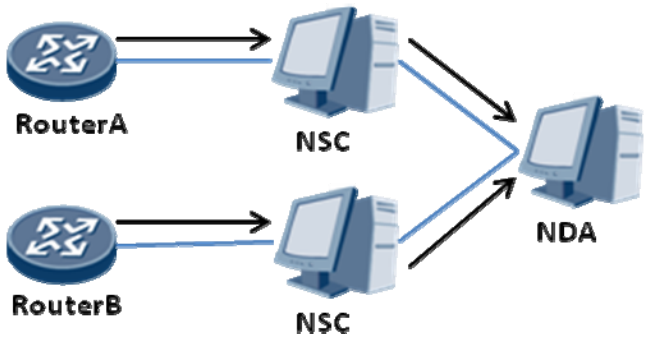
  通过 Netstream 技术，可以获得详细的网络应用信息。例如，网络管理员可以查看 Web、FTP、Telnet 和其它著名的 TCP/IP 应用所占通信流量的百分比。Internet 内容和服务提供商可以根据这些信息来规划和分配网络和应用资源以满足用户需求。

- 异常流量检测

  通过对 Netstream 流进行分析，可以实时检测网络中的异常流量，比如各种网络攻击，通过网管侧的告警，以及与设备的联动，可以对网络安全进行保障。

Netstream 主要包括三个设备 NDE（Netstream Data Exporter），NSC（Netstream Collector），NDA（Netstream Data Analyzer），三个设备之间的关系如下图所示。

图3-17 NetStream 设备之间关系示意图



NDE 负责流量的采集和发送；NSC 设备负责收集和存储 NDE 发来的流量统计数据信息；NDA 对统计信息进行分析，分析的结果为网络计费、网络规划、网络监控、应用监控和分析等提供依据。

华为数据设备实现的是 NDE 功能，需要完成报文采集、流聚合和流输出功能。根据报文采集和流处理的位置不同，华为路由器的 Netstream 功能分为分布式 NetStream 和集中式 NetStream 两种。分布式 Netstream 可以支持多块 Netstream 板进行负载分担。

- 分布式 Netstream

  部分 LPU 单板可以独立完成报文的采集、流聚合和流输出功能，在本板支持完整的 Netstream 功能，因此称为分布式 Netstream。

- 集中式 Netstream

  部分 LPU 单板不支持 Netstream 流处理功能，只支持对报文进行采样，然后将采样报文送到 Netstream SPU 板集中进行流聚合和流输出的处理。因此称为集中式 Netstream。

在采样方面主要支持如下的功能：

- 支持入接口和出接口两个方向的采样。部分单板只支持入接口采样。
- 支持简单的接口采样和基于流分类策略采样。

版权所有 © 华为技术有限公司

- 支持 IPv4 单播/组播报文、分片报文、MPLS、MPLS L3VPN 等多种报文的采样。
- 支持固定报文、随机报文、固定时间、随机时间四种采样方式。
- 支持多种接口的采样：包括 POS、Ethernet、VLAN 子接口、CPOS 接口提供的 Serial/MP/FR PVC/FR MP 等接口、ATM、FR、Trunk、VLANIF、GRE 等各种物理接口和逻辑接口。

在聚合输出方面主要支持如下功能：

- IPv4 支持 as、as-tos、protocol-port、protocol-port-tos、source-prefix、source-prefix-tos、destination-prefix、destination-prefix-tos、prefix、prefix-tos 10 种聚合方式。
- MPLS 报文支持基于三层标签的聚合。
- 对生成的统计信息可以按照 V5、V8、V9 三种报文格式输出。并且，在采用 V9 报文格式输出时，既支持 16 位 Netstream 接口索引，也支持 32 位 Netstream 接口索引。可以根据实际情况通过命令行控制选择。
- 每种聚合流可以配置输出到两个网管服务器。

3.5.3 安全特性部署方案

通过 MPLS VPN 确保不同类型业务及地域之间的有效隔离

VPN 技术具有天然的安全特性，不同的 VPN 用户之间由于无法获知对方的路由信息，从而可以理解为存在于不同的私有网络之中，而 MPLS VPN 由于在公网中使用 LSP 隧道进行标签交换，较之普通的 IP 转发具有更好的安全级别。

本次工程通过规划两大类 VPN（实时与非实时），确保两种不同业务之间的设备无法获知对方的路由信息。在同一种业务中通过对 MPLS VPN 中 RT（Route-Target）属性的合理设置，可以保证即使是相同的业务，如果没有互访需求，也无法相互访问。

通过用户级别控制保证设备控制安全

华为系列路由器和交换机的命令行提供分级保护功能，禁止低优先级的用户更改设备的重要配置，进入高优先级模式时进行密码验证。

用户的用户级别与命令优先级的关系是：用户只能使用命令优先级不大于用户级别的命令。用户可以根据自己的需要定义命令的优先级，使其在不同的用户级别下使用。

限制对 SNMP 和 Telnet 用户访问

对远程登录用户，提供了 LINE 验证、本地验证和 AAA 验证三级验证。不同的用户可设置不同的用户级别，从而对设备有不同的操作权限（见上）。对 Telnet 用户还可进行的限制有：

- 配置 VTY 类型 LINE 的呼入呼出限制 telnet 用户访问。
- 通过在 PE 设备上设置 ACL，限制只允许源地址为公网，并禁止其他所有 VPN 内部用户的私网地址进行登录。此项措施可以简单有效的防止 VPN 用户通过 CE 对 PE 设备进行非法访问。
- 配置团体名限制对设备的 SNMP 访问。

  SNMP 采用团体名认证，与设备认可的团体名不符的 SNMP 报文将被丢弃。SNMP 团体（Community）由一字符串来命名，称为团体名（Community Name）。不同的

版权所有 © 华为技术有限公司

团体可具有只读（read-only）或读写（read-write）访问模式。具有只读权限的团体只能对设备信息进行查询，而具有读写权限的团体还可以对设备进行配置。

路由信息交换的认证

在运行路由协议的路由器上，有些端口具有不安全的属性，最据代表性的如以太网口，该类型的接口由于需要发布本接口网段的路由信息，所以需要启动路由协议，但由于以太网的广播属性，攻击者很容易将一台同样运行 OSPF 协议的路由设备连接到以太网中，并进而获得整网的路由信息及拓扑结构。所以必须在上述端口上启用 silence interface 命令，启动该命令后，该接口的网段路由可以照常发布出去，但该接口不会再收发 OSPF 协议报文，也就不会再与任何其他路由设备建立邻居关系，从而避免了路由泄漏。

对所有重要事件记录日志

对于网络安全，不仅要关注网络的事前防范能力，更要做好对事后跟踪能力方面的考虑，在安全事件发生前后，可以通过对用户上网端口、时间、访问地的记录，全面提供用户上网的追溯能力，从而为后期的分析提供第一手的资料。

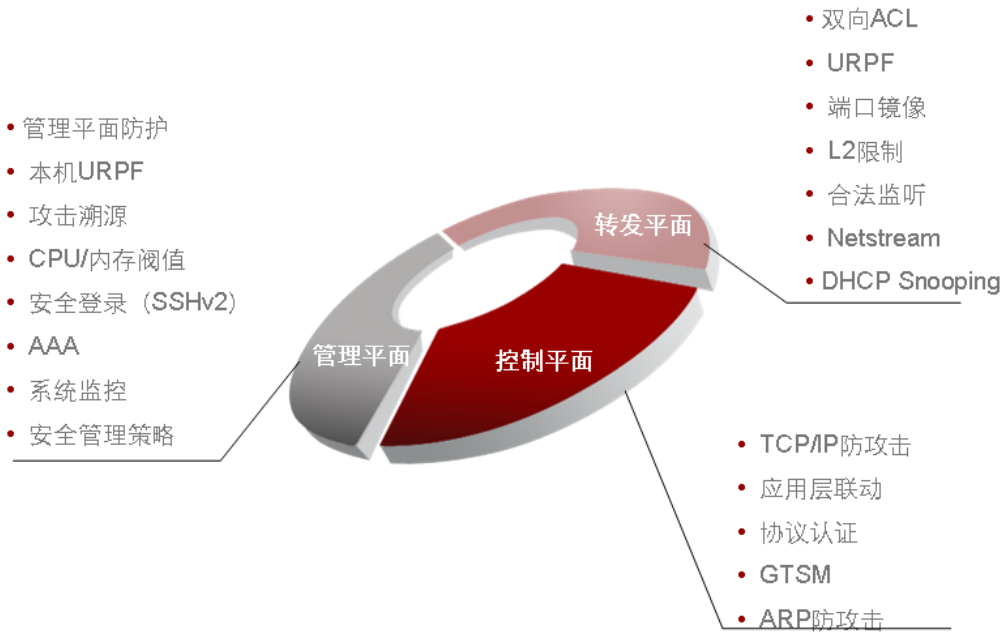
实际上，日志记录功能是一个非常良好的追溯手段：在出现问题时可以根据记录迅速查找源头，防止事态进一步扩大；同时可以通过法律惩治罪犯，以警后人；利用 Syslog 记录重要的设备信息（如告警、设备状态变化信息），可以为故障定位排除提供有利数据。

日志记录支持控制台(console)、Telnet 终端和哑终端(monitor)、日志缓冲区(logbuf)、日志主机(loghost)等多个方向的日志输出。在条件允许的情况下，对关键设备的日志输出建议采用日志主机的方式。

3.5.4 安全特性部署汇总：

在核心层和汇聚层上面，路由器部署多种安全特性组合，如图 3-18 所示：

图3-18 路由器安全部署方案



版权所有 © 华为技术有限公司

3.6 网络管理设计

3.6.1 网络管理设计原则

在进行网络管理系统方案设计时，应遵循以下原则：

- 开放性、兼容性原则
- 整体性原则
- 模块化原则
- 易操作性原则

华为网管系统 iManager eSight 提供了华为网络设备的统一管理平台，不但实现了数通、传送和接入设备的融合管理，还实现了网络层与网元层的融合管理。同时支持分权分域管理，可对各域单独管理，这样适合用户不同的网络，不同的部门管理，相互之间没有干扰。通过统一网管、分布式的软件设计、模块化的软件架构，eSight 能最大程度降低客户的运维成本。

3.6.2 网络管理需求分析

随新技术的应用和可用性的提升，网络管理的复杂度也在持续提升。对电力网络管理不仅依赖于规范的管理制度，同样依赖于合适的运维工具。只有实现对网络的全面监控，才能真正化被动为主动的网络管理。

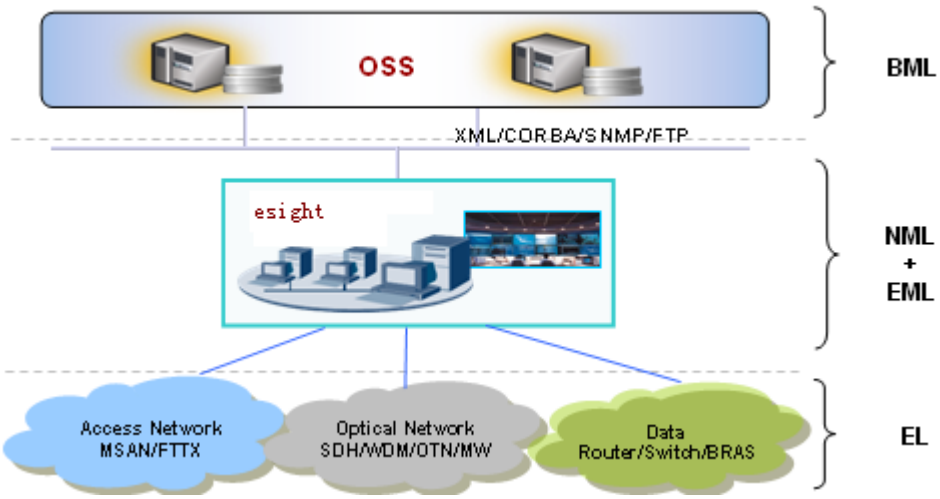
针对电力行业网络实际应用，网络管理系统应该提供以下能力：

- 如何统一监控全网（包括数据网络和传输网络），快速掌握网络现状？
- 如何能快速响应故障，快速定位问题并修复故障？
- 如何完善配置信息、资产信息管理，实时、准确了解资源现状？
- 如何改变救火队式的运维现状，提前感知存在的网络性能瓶颈？
- 如何对 MPLS VPN 关键业务的状态和服务质量进行管理？

eSight 是华为公司网络产品线所有设备统一、融合的管理平台，定位于华为公司网络设备的管理系统，具备强大的网元层、网络层管理功能，eSight 网管是华为网络产品线面向未来网络管理的主要产品和解决方案，能够全面解决电力网络管理的诉求。

版权所有 © 华为技术有限公司

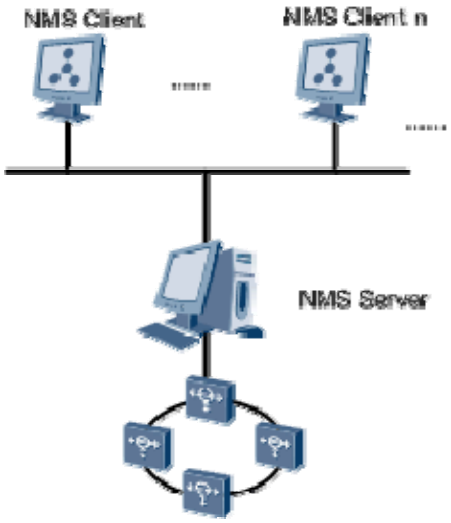
图3-19 eSight 系统概览



3.6.3 网络管理部署方案

eSight 采取成熟、应用广泛的 Client/Server 结构，客户端与服务器之间通过局域网或者广域网互联。eSight 服务器与各个被管设备之间采用带内组网或者带外组网方式进行通讯。eSight 支持 Windows、Solaris 操作系统下的单机系统集中式部署模式，即一个 eSight 网管系统只部署在一个服务器上。

图3-20 网管部署方案



版权所有 © 华为技术有限公司

3.7 华为 eSight 企业运维解决方案

3.7.1 概述

eSight 是华为推出的新一代的网络管理系统，实现对企业资源、业务、用户的统一管理以及智能联动。

eSight 支持对 IT&IP 以及第三方设备的统一管理，同时对网络流量、接入认证角色等进行智能分析，自动调整网络控制策略，全方位保证企业网络安全。同时 eSight 提供灵活的开放平台，为企业量身打造自己的智能管理系统提供基础。

针对企业网场景，华为 eSight 提供多种应用，包括：多厂商的设备管理；企业资源统一管理；可视化的企业统一视图；全方位的企业故障监控；机房精细化监控；辅助智能楼宇安防监控；企业网络监控性能管理；分权-分域-分时的用户管理。

- 多厂商的设备管理

  eSight 预集成业界主流设备，默认已包含 Cisco20 个系列 140 余款设备、H3C14 个系列 130 余款设备、其他厂商 100 余款设备、以及数十款打印机、服务器。企业运维人员不做任何配置，即可管理全网设备，大大提升管理效率。

  eSight 拥有厂商新款设备自动配套能力，通过 eSight 厂商类型自动识别能力，对于友商新发布的设备也可实现拓扑、告警、性能等管理能力。

  针对业界主流设备深入分析，不仅支持标准的流量采集，还同时支持设备面板、设备 CPU 利用率等私有属性的管理。

- 企业资源统一管理

  如图 3-21 所示，华为 eSight 提供全方位的企业资源管理，针对不同网络设备、不同业务、不同服务器、工作站等 PC 资源进行管理。

图3-21 企业资源统一管理示意图

- 可视化的企业统一视图

  IP 网络是开放的，各厂商混合组网成为企业组网普遍情况。大部分企业不会像运营商一样建设综合网管，新厂商进入导致企业运维人员将面对多套厂商管理系统分而

版权所有 © 华为技术有限公司

治之的情况。如果不具备全网设备统一监控的能力，出现网络故障后需要登录到多个网管查看状态，会导致管理效率低下。

eSight 预集成业界主流设备，默认已包含 Cisco20 个系列 140 余款设备、H3C14 个系列 130 余款设备、其他厂商 100 余款设备、以及数十款打印机、服务器。企业运维人员不做任何配置，即可管理全网设备，大大提升了管理效率。

eSight 拥有厂商新款设备自动配套能力，通过 eSight 厂商类型自动识别能力，对于友商新发布的设备也可实现拓扑、告警、性能等管理能力。

- 自动发现：自动发现网络资源，网络链路自动创建。
- 统一视图：提供 IT&IP 一体化拓扑视图，全面管理企业资源。
- 实时呈现：呈现子图、网元、链路、网元状态，实时了解网络的运行情况。
- 灵活定义：按用户信息保存网元位置，支持拓扑背景图和自定义图标功能。各种 Tips 信息，企业结构一目了然。

针对业界主流设备深入分析，不仅支持标准的流量采集，还同时支持设备面板、设备 CPU 利用率等私有属性的管理。

- 全方位的企业故障监控

  华为 eSight 提供全方位的故障监控，提供包括基于 IP 设备、基于 IT 设备、基于业务应用等丰富的告警，同时提供 7*24 不间断的故障监控，实时故障提醒和实时故障远程通知，同时也能提供丰富的故障统计功能。

- 机房精细化监控

  传统用户机房的设备管理都是亡羊补牢型的，如：设备高温烧毁了才发现网络故障；电源坏了才赶去维修。

  而如果能够在温度或电源发生异常时就及时知会网络管理员，就会避免最终设备失效带来的长时间断网以及重大维修。

  电力不稳地区，设备突然掉电重启，管理员无法判断具体原因。设备掉电前瞬间如果能上报网管掉电，则可以使网络管理员及时处理。

  华为 eSight 解决方案，通过引入 S3700-28TP-EI-MC 盒式交换机，支持环境监控口，支持 4 路信号输入和 3 路信号输出，实现机房环境在网络平台上的统一监控，提前对异常进行感知并上报网管，同时根据需要进行声光告警。如与接入网 E 系列机柜一起实现可以实现机柜门、温度、湿度的告警监控。

  Dyinggasp 功能（S3700-28TP-EI-MC 和 S5700-6TP-LI）实现断电瞬间告警发送，通知管理员设备复位是由于供电异常所致。

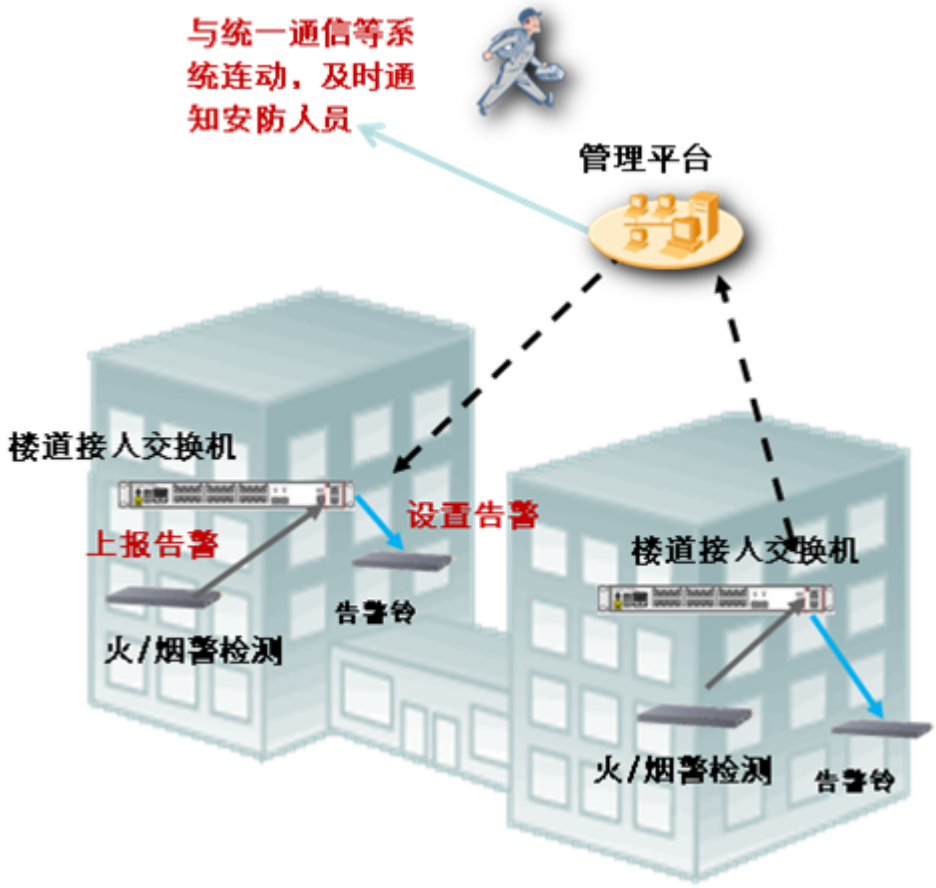
- 辅助智能楼宇安防监控

  智能楼宇建设中，对火警、盗警等安防检测主要是通常的闪灯、声音报警等手段，如何能够将各种报警信息汇总到统一管理平台，以便进行灵活处理？华为 eSight 通过网络设备监控口，实现安防告警信息 IP 化，灵活处理告警。在触发声光告警的同时，短信及时通知安防人员。

  还支持与 IP 视频监控联动，实现统一安防。网络管理平台通过上报告警的网络设备判断告警位置，切换视频监控查看现场状态，指挥救援。

版权所有 © 华为技术有限公司

图3-22 辅助智能楼宇安防监控示意图



- 企业网络监控性能管理能力

  华为 eSight 提供强大的企业网络监控管理能力、提供图形方式呈现性能数据，可以直观了解企业设备、服务器等资源设备性能情况；提供性能阈值告警能力，可以对企业网络健康度实时了解，保障企业业务承载网络健康性；自动创建设备基本性能监控；支持批量创建同类性能监控实例，方便客户轻松操作。

- 分权-分域-分时的用户管理

  为不同用户分配不同权限，并记录操作日志；设置用户管理区域；限定用户管理范围；限定用户帐户有效时间、有效期。

3.7.2 网络日常维护场景

日常维护概述

对于网络运维人员而言，日常维护工作不仅繁杂，而且工作量大，涉及的工作内容包括监控拓扑对象、监控网元、配置网元、监控业务、诊断故障、监控性能、查看资源、报表生成等。

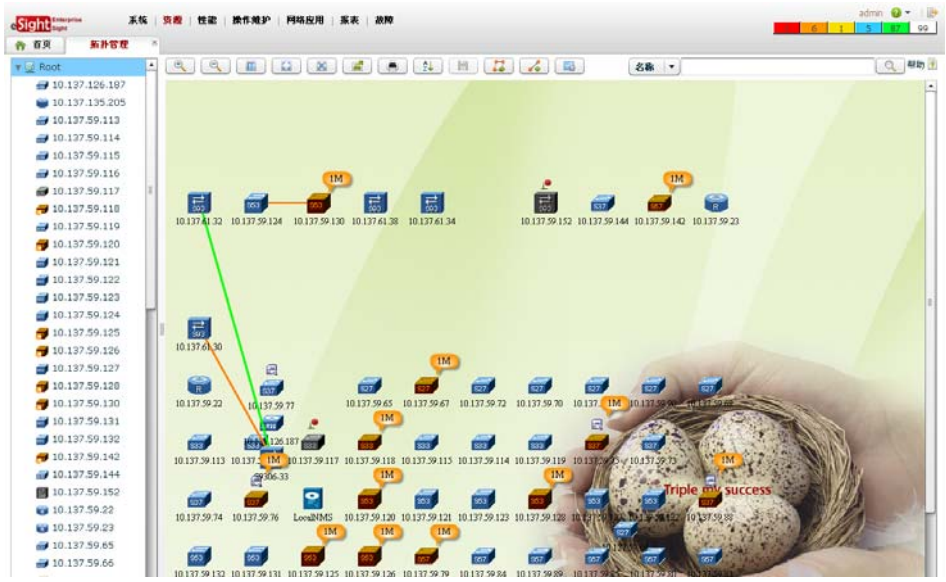
版权所有 © 华为技术有限公司

华为公司推荐 eSight 网络管理系统，可以准确、快捷的提供运维人员所需要的信息，大大减轻运维人员的工作量。通过 eSight 网络管理系统丰富的管理功能和灵活多样的维护手段，可以轻松实现网络日常维护。

拓扑管理

如图 3-23 所示，eSight 以左树右图的方式组织整个视图，其中左边导航树以树型直观的体现出网络结构的层次关系。右视图在背景图上将指定网络层次的对象显示在不同的坐标上，可直观了解对象部署。

图3-23 监控 TOPO 对象



eSight 的拓扑图提供以下功能：

- 支持对拓扑上子网、网元、链路、虚拟网元等的增、删、改、查。
- 支持移动拓扑上的元素。
- 支持显示告警状态及 Tips 信息。
- 支持排列、浏览属性、放大缩小、打印等常用基本操作。
- 支持在拓扑图中提供其他功能的快捷操作入口，如：进入网元管理器查看设备相关告警等。

eSight 的拓扑告警提供以下功能：

- 支持通过拓扑节点的颜色监控设备的轮询状态（正常、未知、离线等）。
- 支持屏蔽显示低级别告警，当网元或子网同时产生多条告警时，系统只显示最高级别告警。

网元监控

网元管理器首页提供设备基本信息、TOPN 告警、接口流量、带宽利用率、CPU、内存等性能图表，用户可进行定制是否显示各图表。

版权所有 © 华为技术有限公司

图3-24 网元管理

eSight 针对各种不同类型的设备，支持丰富的网元监控和管理功能，如表 3-4 所示。

表3-4 eSight 网元监控功能

设备类型	支持的功能
华为路由器、交换机	• 提供完整的性能采集、告警监控能力。 • 提供设备基本信息管理功能。 • 支持通过适用仿真图片的设备面板查看设备状态，并支持单板、端口状态的联动显示。 • 支持查看设备的接口数据、IP 地址数据。 • 支持单网元的配置管理功能。 • 提供设备配置文件的查看、备份、恢复、比较的功能。 • 提供设备、机框、单板、子卡、端口的资源管理功能。
华为防火墙	• 提供基于标准实现的性能采集、告警监控能力。 • 提供设备基本信息管理功能。 • 支持通过仿真图片的设备面板查看设备状态，并支持单板、端口状态的联动显示。 • 支持查看设备的接口数据、IP 地址数据。 • 支持调用设备的 Web 网管提供单网元的配置管理功能。 • 提供对设备配置文件的查看、备份、恢复、比较的功能。

版权所有 © 华为技术有限公司

设备类型	支持的功能
预集成的主流CISCO、H3C设备	• 提供基于标准实现的性能采集、告警监控能力。 • 提供设备基本信息管理功能。 • 支持通过使用仿真图片的设备面板查看设备状态，并支持单板、端口状态的联动显示。 • 支持查看设备的接口数据、IP地址数据。 • 支持调用设备的Web网管提供单网元的配置管理功能。 • 提供应设备配置文件的查看、备份、恢复、比较的功能。 • 提供设备、机框、单板、子卡、端口的资源管理功能。
未预集成的第三方设备	• 提供基于标准实现的性能采集、告警监控能力。 • 提供设备基本信息管理功能。 • 支持通过基本图片查看设备面板，基于设备定制提供单板、端口状态的联动显示。 • 基于设备定制功能，用户可以通过输入定制数据实现并支持设备图标展示、设备自身的性能采集、告警上报、配置文件备份。
服务器、打印机	• 提供基于标准实现的性能采集能力。 • 提供设备基本信息管理功能，例如设备基本属性。 • 支持通过使用仿真图片的设备面板查看设备状态，并支持单板、端口状态的联动显示。 • 支持查看设备的接口数据、IP地址数据。 • 支持调用设备的Web网管提供单网元的配置管理功能。 • 提供服务器、打印机的设备存量管理功能。

配置网元

eSight网络管理系统可以通过三种方式完成单点网元配置工作：

- 使用简单配置框架实现单点网元配置。
- 使用智能配置工具进行设备单点配置。
- 通过Web网管进行单点配置。

在开局、网络维护等多个场景，用户有对集中部署的设备的业务进行批量操作的需求，如图 3-25 和图 3-26 所示，用户通过智能配置工具能够对多台设备的业务进行批量配置，提高用户的运维效率。

版权所有 © 华为技术有限公司

图3-25 网元批量配置 1

图3-26 网元批量配置 2

监控业务

eSight 网络管理系统能够对业务进行实时监控，根据业务类型进行流量、信息统计，极大的方便网络运维人员实时监控业务状况。

监控性能

eSight 可以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。通过可视化的操作界面，方便用户对网络性能进行管理。

通过监视模板管理性能监视指标，并设定告警的阈值。通过性能监视模板，用户可以方便的将性能采集规则应用到多个对象中。性能监视模板包括以下内容：

- 性能指标组

  将多种性能指标集成到一个性能指标组中，可以支持分场景定制指标组，包含场景相关的所有性能指标，便于根据业务场景建立对应的监视任务。

- 性能指标

  定义具体的性能采集的指标。

- 采集周期

  提供多种采集周期供采集性能指标时选择。

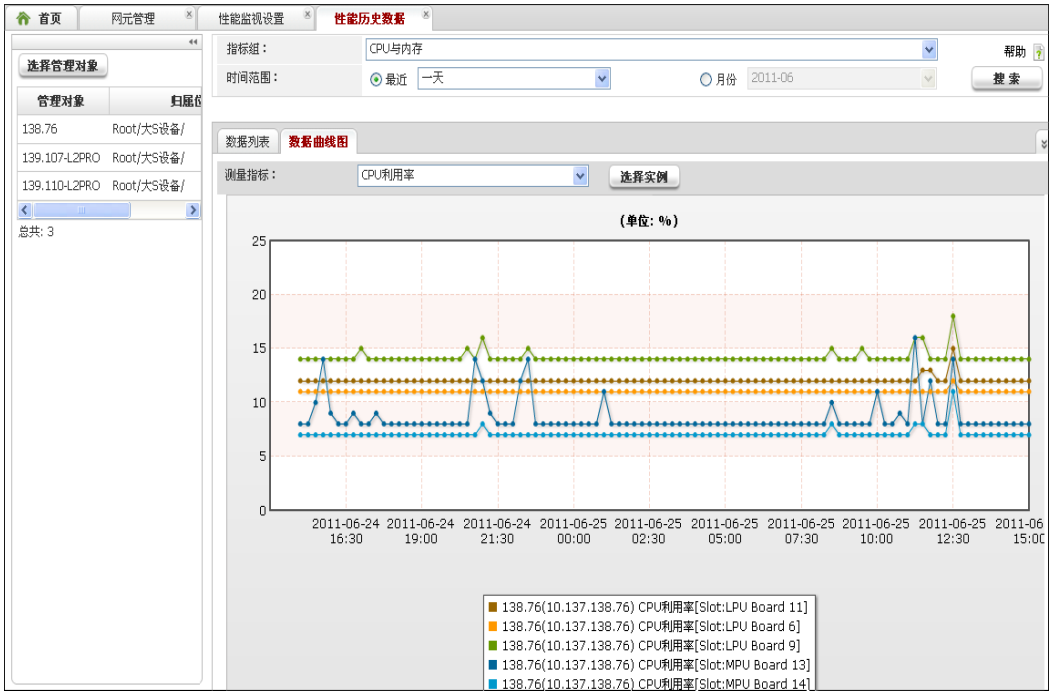
- 性能阈值

  通过设置性能门限值，可以在网络的性能数据低于门限值时及时预警，避免网络性能的持续恶化。

通过性能监视的设置，实现网络性能数据的采集。支持周期性性能指标采集，可以了解网络在指定时间范围内的性能状况，并为预测网络的性能变化提供数据依据。如图 3-27 所示。

版权所有 © 华为技术有限公司

图3-27 性能监控



通过性能监视设置获取网络性能数据后，可以通过性能监视视图以图形化的方式进行指标值查看。用户可以了解网络在指定时间范围内的性能状况，为预测网络的性能变化提供数据依据。

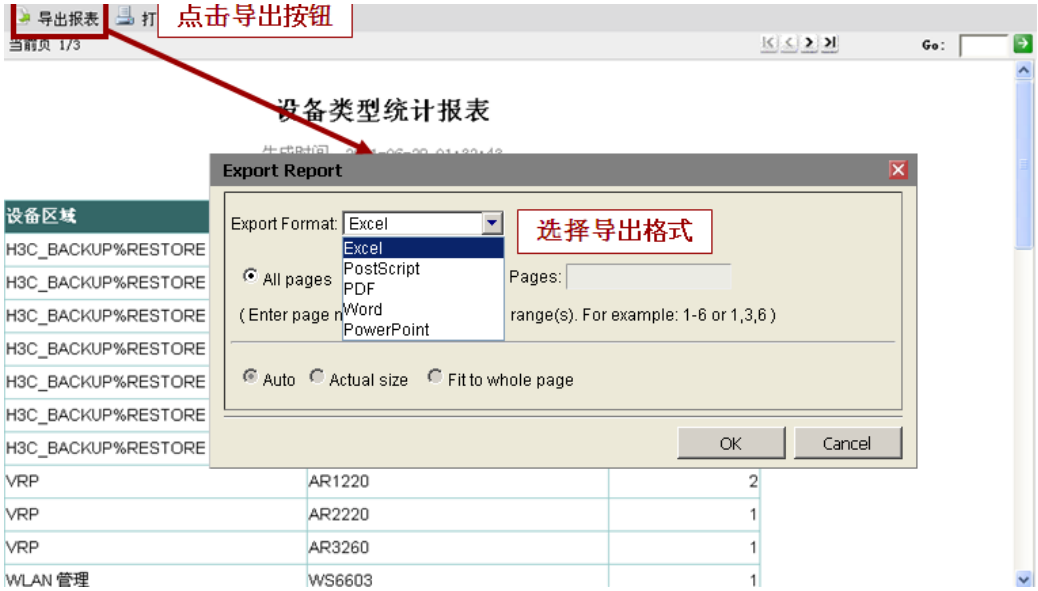
资源查看和报表管理

eSight 提供丰富的资源查看和预定义报表，同时提供强大易用的报表设计功能，用户可根据行业特点和自身运维要求进行客户报表定制。如图 3-28 和图 3-29 所示。

图3-28 查看物理资源

版权所有 © 华为技术有限公司

图3-29 导出报表



阶段维护

eSight 提供配置文件管理和备份功能，可以快速的进行文件备份和设备登录管理。同时还提供系统巡检工具，能够定时对设备进行自检，减轻网络维护人员的工作量。

3.7.3 第三方设备定制场景

企业网络设备来自不同厂商，无法统一采用预集成的方式管理第三方设备，需要提供定制的能力。如果使用各自的网管系统进行管理，不仅增加了运维成本，而且极大的增加了网络维护人员的工作量。

华为公司 eSight 网管系统提供了对第三方设备管理能力的定制功能，包括对设备厂商信息、设备型号信息、告警参数、性能指标、设备面板、设备配置文件管理的定制功能，方便用户实际网络设备进行定制化的管理。满足对第三方设备的管理需求。

- 厂商信息定制

  eSight 网管系统可以定制厂商的名称、联系人等信息，用于后续的设备类型定制。如图 3-30 所示。

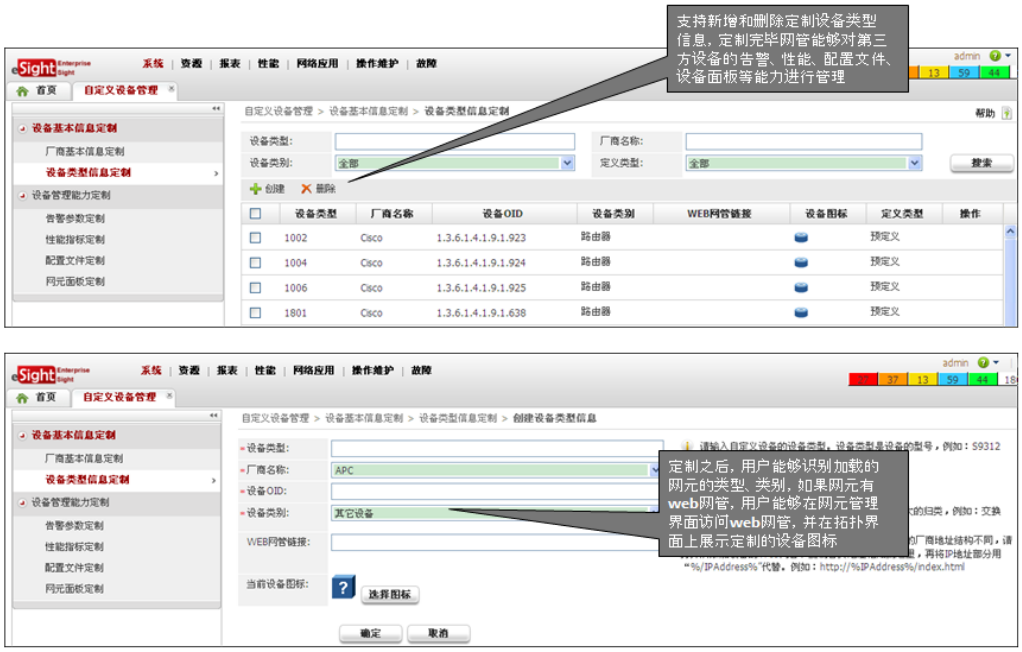
版权所有 © 华为技术有限公司

图3-30 厂商信息定制

- 设备类型定制

  eSight 网管系统可以定制设备类型的描述、设备图标、Web 网管链接信息，定制的设备图标能在拓扑上显示。如图 3-31 所示。

图3-31 设备类型定制

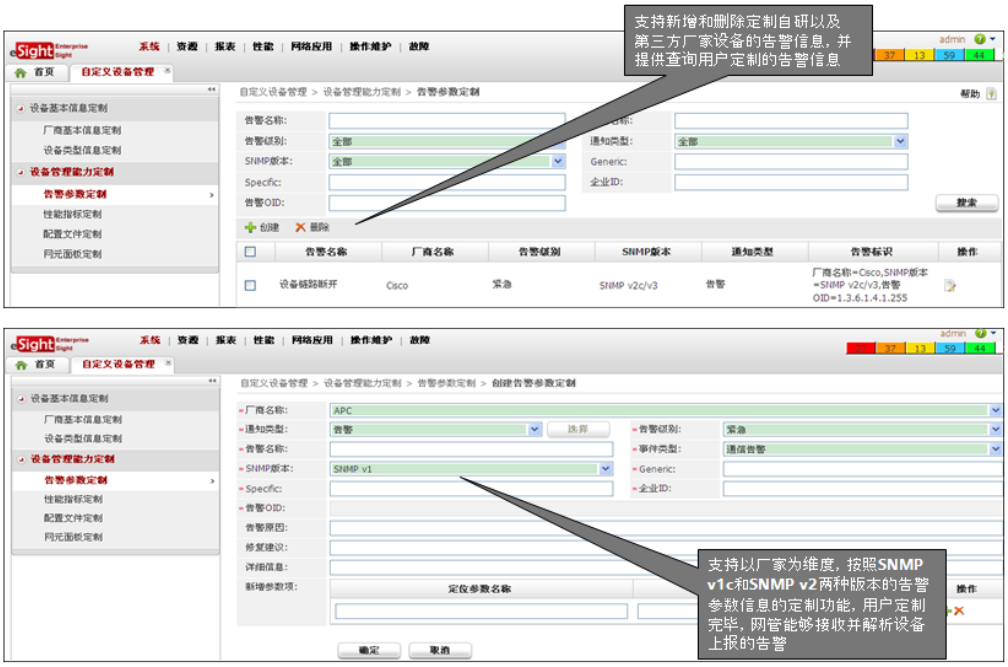


- 告警定制

版权所有 © 华为技术有限公司

eSight 网管系统可以对上报告警格式进行定制，定制后的告警能支持告警报文解析，并在告警管理界面上进行显示。如图 3-32 所示。

图3-32 告警定制



- 性能指标定制

  eSight 网管系统可以对设备上支持的采集指标进行定制，定制后的性能指标能通过性能任务进行采集，在性能界面中进行数据浏览。如图 3-33 所示。

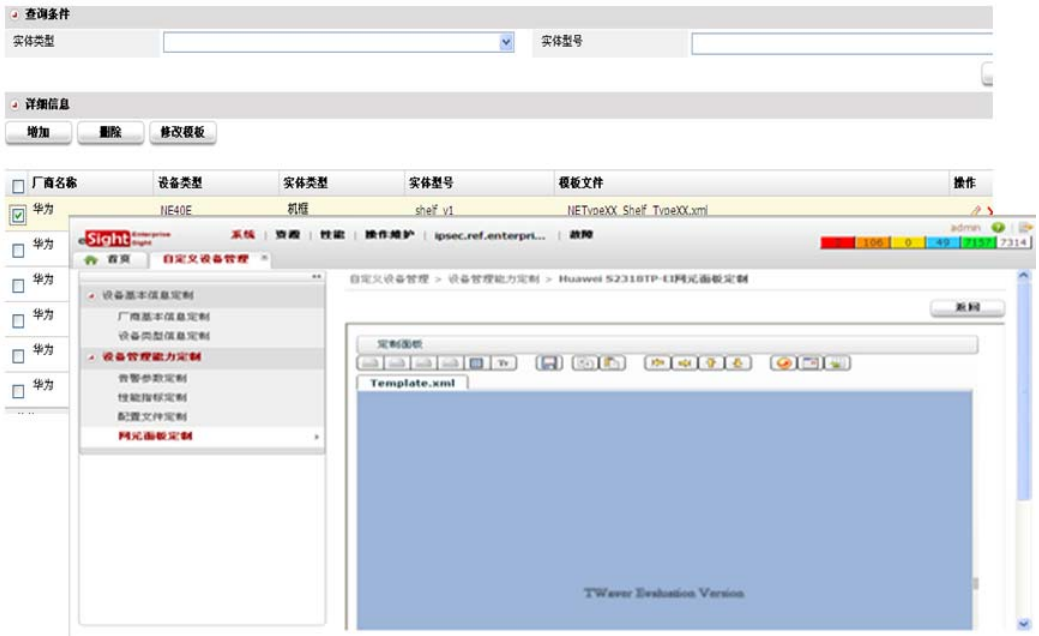
版权所有 © 华为技术有限公司

图3-33 性能指标定制

- 设备面板定制

  eSight 网管系统可以对设备框、单板、子卡、端口进行仿真图定制，定制后的面板将显示新的仿真图。如图 3-34 所示。

图3-34 设备面板定制

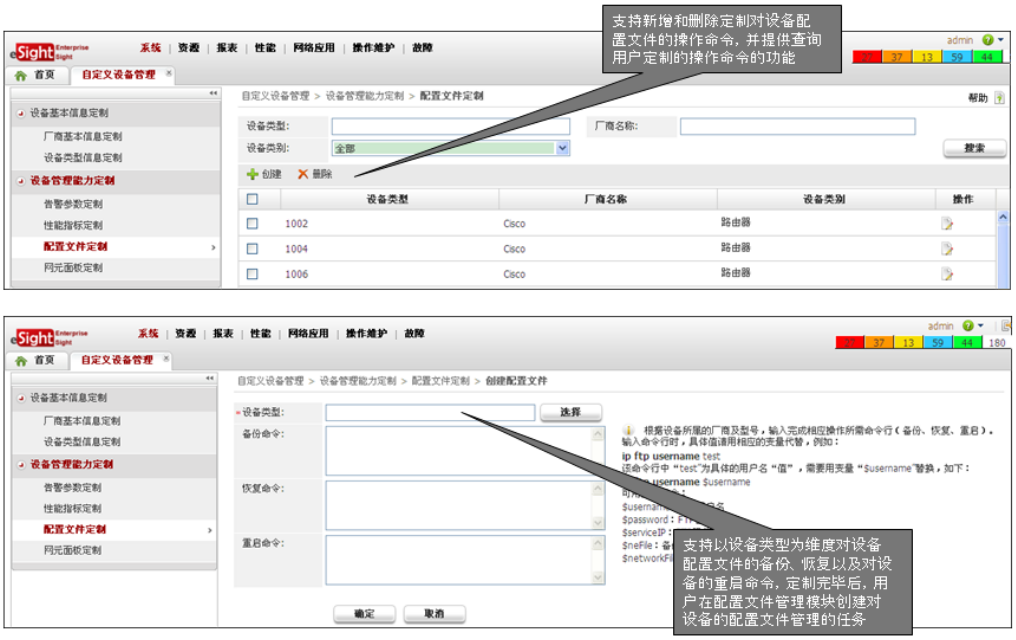


版权所有 © 华为技术有限公司

- 设备配置文件定制

  eSight 网管系统可以针对第三方设备定制关于配置文件的备份、恢复、重启命令，支持配置文件自动备份。如图 3-35 所示。

图3-35 配置文件备份和恢复定制

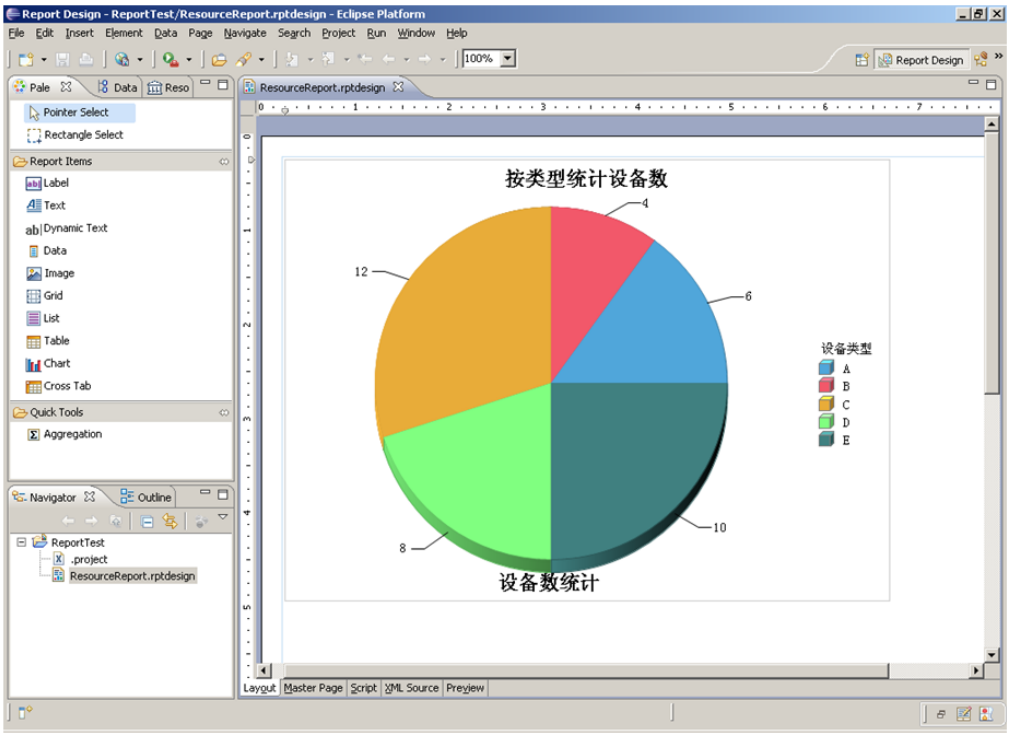


- 报表定制

  eSight 提供强大的自定义报表能力。提供所见即所得的报表设计环境，可以修改现有的报表设计文件，生成新的设计文件。如图 3-36 所示。

版权所有 © 华为技术有限公司

图3-36 报表定制



3.7.4 软件升级和补丁加载场景

企业网络设备众多，如果使用一台一台的方式去升级和加载补丁，不仅耗时耗力，而且容易出现人为原因造成的升级失败，需要考虑通过远程集中式进行统一升级和加载补丁。

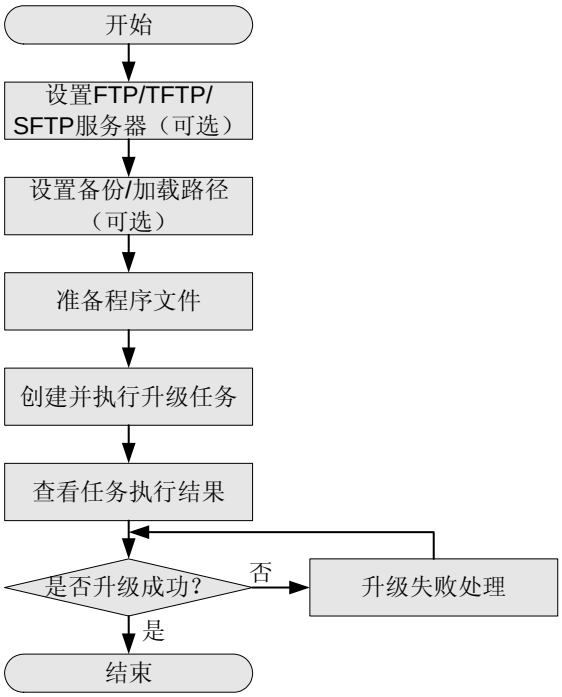
eSight 网管系统提供了远程集中式软件升级和补丁加载机制，极大的减轻网络维护人员工作量，避免了人为原因造成的升级失败和补丁加载失败。

- 软件升级

  eSight 网管系统提供远程集中式的软件升级功能，按照操作向导，轻松完成设备升级，并且对升级失败有相应的处理，避免升级失败后的设备状态异常。如图 3-37 所示。

版权所有 © 华为技术有限公司

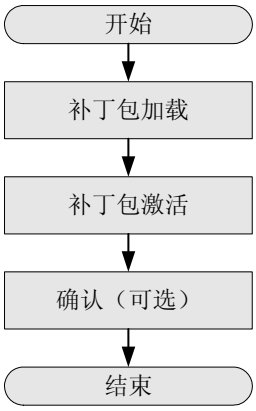
图3-37 软件升级流程



- 补丁加载

  eSight 网管系统提供远程集中式的补丁加载功能，按照操作向导，轻松完成补丁加载，并且具有补丁回滚功能，可以将网元恢复到补丁升级前的状态。如图 3-38 所示。

图3-38 补丁升级流程



3.7.5 故障处理

企业网络系统是由网络设备、连接设备间链路和一些相关服务器组成。因此出现网络系统故障的原因也基本上从链路、网络设备状态、是否受病毒攻击、服务器状态等方面来查找。这些组件的任何一个出现故障，都会导致上层应用无法正常工作。

版权所有 © 华为技术有限公司

3.7.6 网络设备故障处理

网络设备发生故障可以分为几种：

- 设备宕机：设备上的电源或者其他指示灯都不亮，没有任何工作时的声响。
- 设备 CPU 使用率高：监控软件或者登录设备时，发现设备的 CPU 利用率很高，同时相关应用响应较慢。
- 有错误消息：查看日志服务器或者登录设备时，发现设备有错误消息。
- 有报警信息：设备状态指示灯报警，显示为红色等。

针对以上几种设备故障，可以做如下处理：

- 设备宕机

  如果发现一旦发现设备宕机，首先检查电源连接线和机房电源。如果电源连接线和电源均正常，立即拨打设备提供商和服务提供商的服务号码，请求支持。如果发现设备硬件存在问题，可要求设备提供商和服务提供商在最短时间内做备件更换服务。

- 设备 CPU 利用率高

  立即报告服务提供商，要求提供技术支持。待技术支持工程师远程处理或到场后，协助工程师找出设备 CPU 利用率高的原因。一般情况下，可以判断为设备受到病毒的攻击。

- 有错误消息

  将错误消息发送给服务提供商，并跟踪进度。经过服务提供商分析后，给出错误消息的原因，如果设备有隐形的故障，可以预先做好相应的准备工作或者更换设备。

- 报警信息

  报告服务提供商和设备提供商，要求对设备进行报警故障排除或者更换硬件。

3.7.7 服务器故障处理

跟网络系统相关的服务器主要有 DHCP 服务器、ACS 服务器、外网代理服务等。常见的故障现象包括：

- 不能正确获取 IP 地址。
- 不能正常登录网络设备。
- 不能通过代理服务器上网。

可以按照如下步骤进行故障处理：

- 不能正确获取 IP 地址
  - 首先查看 DHCP 服务器的连通性，可以用 Ping 的办法确定。如果 DHCP 服务器连通性正常，则可以登录服务器。
  - 查看该服务器的 DHCP 服务是否正常；如果服务正常，可以查看是否网络当中有病毒，导致 DHCP 的请求消息超时。
  - DHCP 服务器有备份服务器，在当前服务器不可用的情况下，可以替换当前的服务器。
  - 在 DHCP 服务器恢复正常工作前，我们也可以采用手动静态配置 IP 地址的方法来临时解决电脑访问网络的问题。

版权所有 © 华为技术有限公司

- 不能正常登录网路设备
  - 首先查看该网络设备是否具有连通性。
  - 如果该设备可以 Ping 通，可以尝试登录服务器，看 ACS 的服务器的服务是否正常。
  - 如果服务不正常，可以考虑使用网络设备上的 Console 端口登录设备，临时去掉 AAA 认证服务相关配置，启用网络设备的内置本地认证数据库进行临时登录认证。
- 不能通过代理服务器上网
  - 首先查看网络是否连通，是否可以访问其他的应用；然后测试到代理服务器的连通性。
  - 如果代理服务器连通性正常，则可以登录服务器，查看该服务器的代理服务和相关系统服务是否正常。如果发现服务不正常的，可以尝试重启服务或者服务器来解决。
  - 如果重启代理服务器服务或系统后问题仍无法解决的，则需进一步检查代理服务器硬件是否存在故障，例如网卡等关键硬件。
  - 如果代理服务器硬件或者系统存在问题的，我们可以临时使用备用代理服务器来满足代理上网的需求。
  - 如果前述问题均不存在，一切正常，则可以测试到 Internet 的访问是否正常。我们应该对提供 Internet 服务的 DNS 和 ISP 网关进行 Ping 测试。如果 DNS 或 ISP 网关存在连通性问题，则及时联系 ISP 商排查解决。对于 ISP 提供的当前线路出现问题的，我们可以使用备份线路进行 Internet 访问。

3.7.8 网络扩容

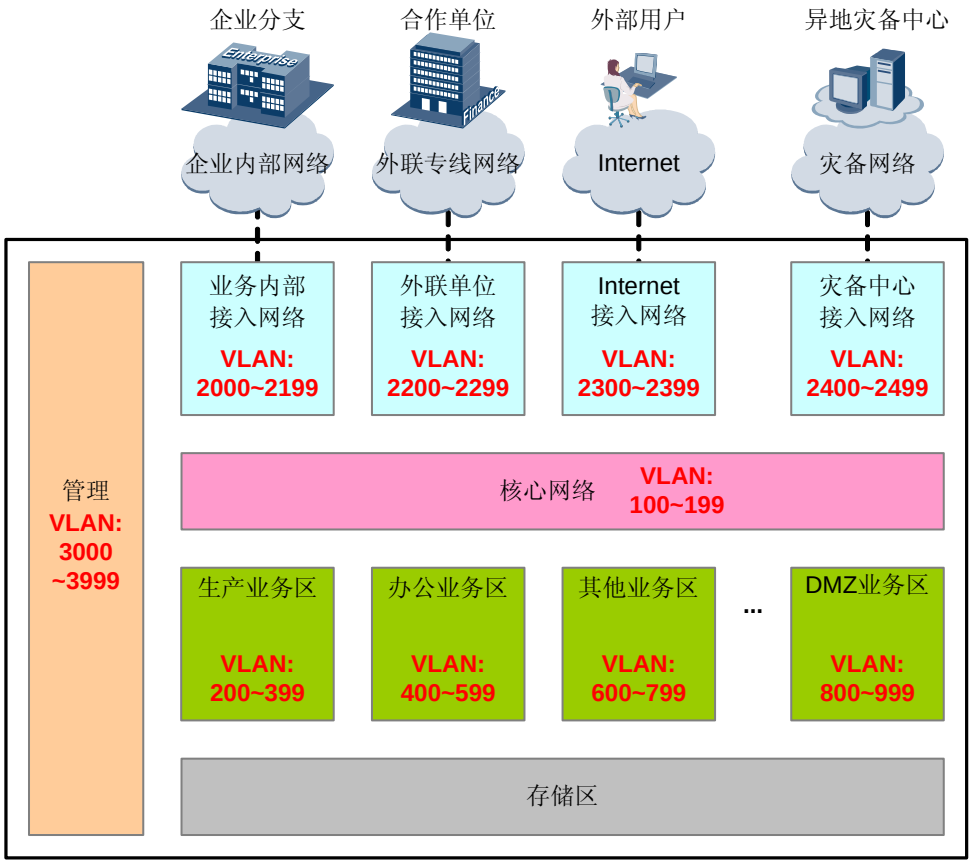
随着企业网络业务、规模的不断增加，现有网络容量已经不能满足企业网络的长期发展，在不影响现有业务的情况下实现平滑扩容，是企业网络扩容的基本要求。

服务器扩容

服务器扩容包含在原区域扩容服务器和在新区域新建服务器两种情况，针对这两种情况，所采取的扩容策略不尽相同。

版权所有 © 华为技术有限公司

图3-39 企业网络内部架构



- 原区域扩容服务器

  随着生产业务的不断发展，当前生产业务区的服务器资源已经不能满足业务发展需要，需要进行生产业务区服务器的扩容，实现平滑扩容需要使用该区域初期规划好的 VLAN，保持 VLAN 的连续性，并且 IP 地址使用该区域初期规划好的地址段，这样做可以保证上游路由和防火墙策略不需要进行修正，便于维护的同时也减轻了扩容工作量。

- 新区域新建服务器

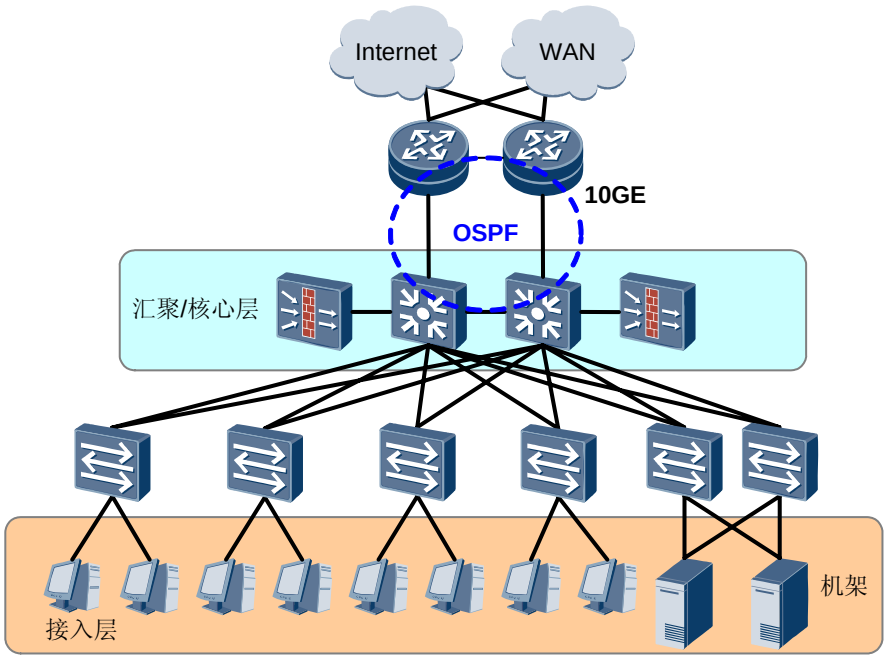
  假设 DMZ 区是新建区域，那么就需要为该区域重新规划 VLAN 资源和 IP 地址资源，重新进行路由和防火墙策略规划，这样做可以确保新区域的建设不会影响到现有业务，实现现有业务的平滑扩容，划分新的区域也便于今后运维管理。

网络设备扩容

图 3-40 所示为通用的企业网络架构。可以看到在接入与汇聚层存在众多环网，一旦由于业务增长需要增加服务器资源，就需要增加接入层交换机并连接到汇聚/核心层，增加网络复杂度的前提下还要使用破环技术，不可避免的会对现网的业务产生影响。

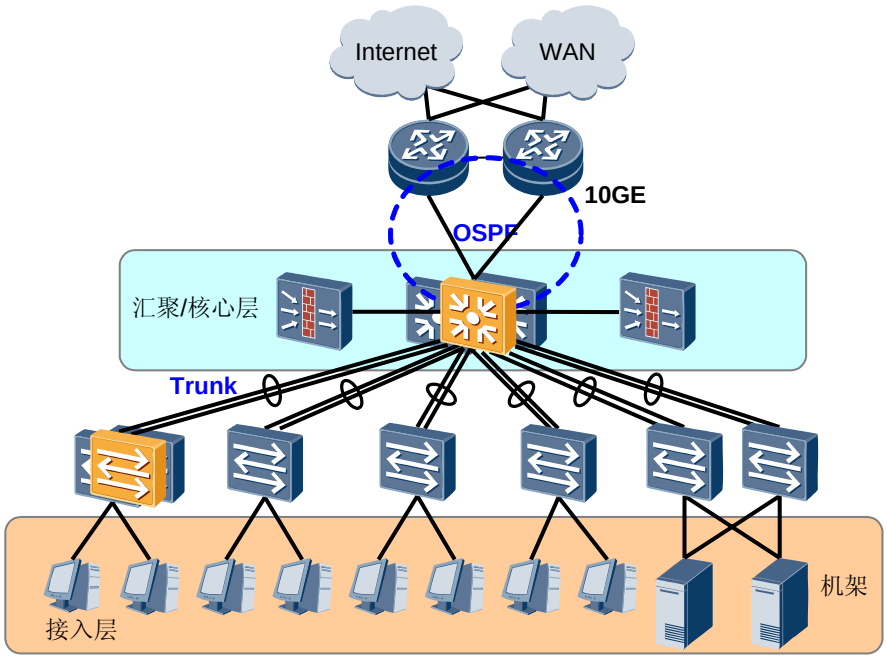
版权所有 © 华为技术有限公司

图3-40 通用企业网络架构



华为公司推荐在企业网络架构采用堆叠和集群技术，首先消除破环协议，其次简化网络规模，并且利于网络设备扩容。如图 3-41 所示。

图3-41 堆叠/集群化的企业网络架构



版权所有 © 华为技术有限公司

使用堆叠和集群技术后，网络结构由环形简化为树形。首先利于网络运维管理，其次网络设备扩容时，只需要在原有的堆叠环境下新增设备，对网络结构不产生影响，也不需要添加物理链路到汇聚/核心层，实现企业业务的平滑扩容。

链路带宽扩容

随着企业业务的扩展，链路带宽也会成为企业业务的瓶颈，除了使用更换高性能、高带宽单板外，还可以通过链路捆绑技术进行链路带宽扩容，在不影响现网业务的情况下实现链路带宽的平滑扩容。

版权所有 © 华为技术有限公司

4 设备说明

4.1 S5700 系列

Quidway®S5700 系列以太网交换机（简称 S5700）是华为公司推出的集接入、汇聚和传送功能于一身的以太网交换机，满足企业网对多业务可靠接入和高质量传输的要求。

S5700 定位于企业网多业务的接入汇聚层，具有大容量、高密度、高性价比的分组转发能力。借助 S5700 可构建高可靠的环网拓扑，具有多业务接入能力、良好的扩展性、QoS、强大的组播复制能力和运营级的安全性。

表4-1 S5700 系列交换机

产品型号	设备外观图	备注
S5700-28C-EI		三层交换机 • 下行24个GE电 • 上行支持三种插卡 1、4个XGE光 2、2个XGE光 3、4个GE光 • 增强三层功能
S5700-28C-EI-24S		三层交换机 • 下行24个GE光 • 上行支持两种插卡 1、4个XGE光 2、2个XGE光 3、4个GE光 • 增强三层功能

版权所有 © 华为技术有限公司

产品型号	设备外观图	备注
S5700-52C-EI		三层交换机 • 下行48个GE电 • 上行支持两种插卡 1、4个XGE光 2、2个XGE光 3、4个GE光 • 增强三层功能
S5700-24TP-SI	DC  AC 	三层交换机 • 24个GE电 • 基本三层功能
S5700-24TP-PWR-SI		三层交换机 • 24个GE电 • 基本三层功能 • 支持PoE
S5700-48TP-SI		三层交换机 • 48个GE电 • 基本三层功能
S5700-48TP-PWR-SI		三层交换机 • 48个GE电 • 基本三层功能 • 支持PoE
S5700-28C-PWR-EI		三层交换机 • 下行24个GE电 • 上行支持两种插卡 1、4个XGE光 2、2个XGE光 3、4个GE光 • 增强三层功能 • 支持 PoE

版权所有 © 华为技术有限公司

产品型号	设备外观图	备注
S5700-52C-PWR-EI		三层交换机 • 下行48个GE电 • 上行支持两种插卡 1、4个XGE光 2、2个XGE光 3、4个GE光 • 增强三层功能 • 支持 PoE
S5700-28C-SI		三层交换机 • 下行24个GE电 • 上行支持两种插卡 1、4个XGE光 2、2个XGE光 3、4个GE光 • 基本三层功能
S5700-52C-SI		三层交换机 • 下行48个GE电 • 上行支持两种插卡 1、4个XGE光 2、2个XGE光 3、4个GE光 • 基本三层功能

S5700 系列交换机的特点是：

- 电信级的可维护性
  - S5700 遵循电信级标准设计，风扇、电源可现场更换，方便维护；机箱重量轻，可以安装在 600mm 深机柜中，且安装方便。
  - S5700 提供软件热补丁技术，实现设备软件在线平滑升级。
  - S5700 支持快速保护倒换机制 RRPP（Rapid Ring Protection Protocol），可以快速实现链路级和业务级保护倒换，满足运营级的可靠性要求。
- 强大的多业务接入能力
  - S5700 通常部署在企业网的汇聚层，可直接接入来自下游 AMG（Access Media Gateway）和 LSW（LAN Switch）等设备的业务，并汇聚到上游设备。可接入的业务包括：VoIP、IPTV/VOD（Video On Demand）视频业务以及宽带上网业务。

版权所有 © 华为技术有限公司

- S5700 采用成熟、经济的 IP 内核技术，借助高性能 ASIC（Application Specific Integrated Circuit）芯片，提供大容量的数据交换能力，满足传统电信业务对低时延抖动、高可靠性的需求。S5700 采用以太网组网技术，支持组播业务，提供良好的 QoS 机制和多种保护倒换技术，实现了良好的带宽保证和多业务支持能力。

- 灵活的组网能力
  - S5700 提供 10/100/1000BASE-T 以太网电接口、100/1000BASE-X 以太网光接口及万兆以太网光接口，支持 Access、Trunk 和 Hybrid 等多种接口类型。
  - 对于千兆光纤连接，S5700 提供可插拔的 SFP（Small Form-Factor Pluggable）类型光模块。对于万兆光纤连接，S-switch 提供可插拔的 XFP（10Gigabit SmallForm Factor Pluggable）和 SFP+（SmallForm-Factor Pluggable Plus）类型光模块。光纤长度可以根据用户对传输距离的需求灵活选配。
  - S5700 可以组成树状、星型和环状以太网。对于环状以太网，S5700 提供 STP（Spanning Tree Protocol）和 RRPP，消除环路并提供快速保护倒换。
- 网络级 QoS 保障

  S5700 具备完善的 QoS 机制。S5700 能够智能感知业务，能够对 OSI 模型 2～4 层信息进行流分类，根据流分类结果提供访问过滤、流量监管、队列调度策略，从而确保不同业务对差别服务的要求。
- 多层面的扩展能力
  - S5700 以华为公司拥有自主知识产权的 VRP（Versatile Routing Platform）平台为基础，结合设备和网络管理技术，提供高速的交换能力和丰富的业务特性。
  - S5700 支持灵活业务插卡和多功能插槽，满足未来业务的扩展需求。
- 周密的安全措施

  S5700 保障设备和数据传输的安全，有效的防止恶意用户对网络的攻击。
  - 支持基于 MAC 地址的过滤。
  - 提供丰富的 ACL 策略。
  - 提供“VLAN＋MAC”的查表机制。
  - 支持流量抑制。

  S5700 提供安全的用户登录操作保护。
  - 对登录用户提供口令保护，口令可加密功能。
  - 通过配置用户级别和命令级别实现对命令的分级保护。
  - 通过命令锁定当前配置终端，防止设备被非法使用。
  - 对影响系统性能的重要命令，提供确认和提示。

  S5700 提供 ALS（Automatic Laser Shutdown）功能，在光纤连接断开时停止发送激光，有效避免激光对用户的伤害。
- 便捷的操作维护

  S5700 不仅自身提供基于接口的流量统计功能，支持 IP 网络中 Ping、Tracert 等故障检测和定位技术。而且还能配合华为公司 eSight 企业网络管理系统，提供丰富的性能监视、告警和快速的故障定位能力。

  S5700 还支持基于 GUI 的 Web 网管界面，为用户提供友好的配置和管理界面。通过 Web 网管，用户可以很方便的通过 GUI 界面管理设备，降低对初级维护人员的要求。

版权所有 © 华为技术有限公司

此外，S5700 还支持 HGMP（Huawei Group Management Protocol）集群管理，通过自动收集设备拓扑的方法以及集中的维护管理通道，使一台设备可以管理多台二层交换机。

- 绿色节能设计

  S5700 采用多种节能措施，包括：

  - 采用静音风扇，风扇转速自动调整，降低系统的噪音，节省风扇功耗。
  - 当检测不到业务端口对端连接设备，即端口空闲，则芯片进入省电模式，以减小功耗。
  - 采用先进工艺、高集成度、低功耗芯片，并配合智能设备管理系统充分利用芯片的低功耗特性，在提升系统性能的同时还降低了整机功耗。

- 先进的防雷技术

  S5700 采用华为专利内置防雷技术，可以应对各种恶劣环境，如架空走线。从而降低设备在雷击天气中的损坏概率，大大提高设备可靠性，将安全系数提高 30 倍。

- 人性化的 PoE 供电方式

  S5700 支持 PoE（Power over Ethernet）功能，即可以通过双绞线向远端下挂的 IP 电话、无线 AP(Access Point)、便携设备充电器、刷卡机、摄像头、数据采集等终端设备提供集中式的电源供电，降低用户的初期投资成本。

  S5700 支持 802.3af 标准和 802.3at 标准，解决不同厂家设备远端供电问题。其中，802.3at 标准支持最大 30W 的供电能力，可以为新一代的 IP 可视电话、双频 WiFiAP，视频监控摄像机，多功能 STB11，RFID 读卡器等大功率设备提供电力，降低网络复杂度。

  S5700 提供基于时间段的供电控制能力，有效管理网络设备和电力消耗，降低运营成本。

4.2 S3700 系列

Quidway®S3700 系列以太网交换机（简称 S3700）是华为公司推出的集接入、汇聚和传送功能于一身的以太网交换机，满足企业网对多业务可靠接入和高质量传输的要求。

S3700 定位于企业网多业务的接入汇聚层，具有大容量、高密度、高性价比的分组转发能力。借助 S3700 可构建高可靠的环网拓扑，具有多业务接入能力、良好的扩展性、QoS、强大的组播复制能力和运营级的安全性。

表4-2 S3700 系列交换机

产品型号	设备外观	备注
S3700-28TP-SI	AC  DC 	三层交换机 • 下行24个FE电 • 上行2个GECombo和2个GE光 • 基本三层功能

版权所有 © 华为技术有限公司

产品型号	设备外观	备注
S3700-28TP-EI		三层交换机 • 下行24个FE电 • 上行2个GECombo和2个GE光 • 增强三层功能
S3700-28TP-EI-24S		三层交换机 • 下行24个FE光 • 上行2个GECombo和2个GE光 • 增强三层功能
S3700-52P-SI		三层交换机 • 下行48个FE电 • 上行4个GE光 • 基本三层功能
S3700-52P-EI		三层交换机 • 下行48个FE电 • 上行4个GE光 • 增强三层功能
S3700-52P-EI-24S		三层交换机 • 下行24个FE光和24个FE电 • 上行4个GE光 • 增强三层功能
S3700-52P-EI-48S	AC:  DC: 	三层交换机 • 下行 48 个 FE 光 • 上行 4 个 GE 光 • 增强三层功能
S3700-28TP-PWR-EI		三层交换机 • 下行24个FE电 • 上行2个GECombo和2个GE光 • 增强三层功能 • 支持PoE

版权所有 © 华为技术有限公司

产品型号	设备外观	备注
S3700-52P-PWR-EI		三层交换机 • 下行48个FE电 • 上行4个GE光 • 增强三层功能 • 支持PoE
S3700-28TP-EI-MC		三层交换机 • 下行24个FE电 • 上行2个GECombo和2个GE光 • 增强三层功能 • 支持监控和掉电告警

由于采用相同的软件平台，S3700 在软件功能特性方面和 S5700 基本一致，在此不再重复。下面主要介绍一下 S3700 与 S5700 不同的特点：

- 电信级可维护性方面，S3700 机箱采用前向维护结构，方便日常操作和维护。
- 灵活组网方面，S3700 提供 10/100BASE-T 以太网电接口、10/100/1000BASE-T 以太网电接口和 100/1000BASE-X 以太网光接口（S5700 支持万兆以太网接口）。
- 绿色节能设计方面，S3700-28TP-SI/EI 采用自然散热，无噪声污染，产品可靠性高；节省风扇功耗，并避免定期维护风扇，节省维护费用；无风扇等额外功耗，使产品达到更好的能效功耗比；还可以有效的避免单板腐蚀。

4.3 S2700 系列

Quidway®S2700 系列以太网交换机（简称 S2700）是华为公司推出的集接入和传送功能于一身的以太网交换机，满足企业网对多业务可靠接入和高质量传输的要求。

S2700 定位于企业网多业务的接入层，具有大容量、高密度、高性价比的分组转发能力。借助 S2700 可构建高可靠的环网拓扑，具有多业务接入能力、良好的扩展性、QoS、强大的组播复制能力和运营级的安全性。

表4-3 S2700 系列交换机

产品型号	设备外观	备注
S2700-9TP-EI	AC  DC 	以太网交换机 • 下行8个FE电 • 上行1个GECombo • 支持ACL

版权所有 © 华为技术有限公司

产品型号	设备外观	备注
S2700-9TP-SI		以太网交换机 • 下行8个FE电 • 上行1个GECombo
S2700-18TP-EI		以太网交换机 • 下行16个FE电 • 上行2个GECombo • 支持ACL
S2700-18TP-SI		以太网交换机 • 下行16个FE电 • 上行2个GECombo
S2700-26TP-EI	AC  DC 	以太网交换机 • 下行 24 个 FE 电 • 上行 2 个 GECombo • 支持 ACL
S2700-26TP-SI		以太网交换机 • 下行 24 个 FE 电 • 上行 2 个 GECombo
S2700-52P-EI		以太网交换机 • 下行 48 个 FE 电 • 上行 4 个 GE 光 • 支持 ACL
S2700-9TP-PWR-EI		以太网交换机 • 下行 8 个 FE 电 • 上行 1 个 GECombo • 支持 ACL • 支持 PoE
S2700-26TP-PWR-EI		以太网交换机 • 下行 24 个 FE 电 • 上行 2 个 GECombo • 支持 ACL • 支持 PoE

由于采用相同的软件平台，S2700 在很多软件特性上与 S3700 基本一致，最大的不同在于 S2700 为二层交换机，因此不具有三层相关的特性和功能，而 S3700 同时支持二层和

版权所有 © 华为技术有限公司

三层的硬件线速转发。在硬件设计上，S2700 大部分型号采用自然散热的无风扇设计，包括 S2700-9TP-PWR-EI、S2700-9TP-SI/EI、S2700-18TP-SI/EI、S2700-26TP-SI/EI 等。

4.4 AR 系列

Quidway®AR12/22/32 系列路由器是华为公司为满足新一代企业分支、中小企业的 WAN 接入和运营商转售市场多业务承载需求而推出的新一代接入路由器产品。

AR12/22/32 系列路由器基于新一代高性能硬件和华为公司统一的 VRP 软件平台，支持丰富的广域网接口，提供高密度以太、语音等用户接入，支持 IPSec VPN 和防火墙等安全功能，可充分满足企业分支互联、中小企业广域接入和运营商转售等多种场合的需求。

Quidway®AR12/22/32 分为 AR12、AR22 和 AR33 三个系列产品。

表4-4 AR 系列产品

产品型号	设备外观	备注
AR1220		整机容量：8Gbps 转发性能：350Kpps/200Mbps(64byte)
AR1220V		整机容量：8Gbps 转发性能：350Kpps/200Mbps(64byte)
AR1220W /1220VW		整机容量：8Gbps 转发性能：350Kpps/200Mbps(64byte)
AR2220		整机容量：32Gbps 转发性能：1Mpps/500Mbps(64byte)
AR2240		整机容量：80Gbps 转发性能：2Mpps/1333Mbps(64byte)
AR3260		整机容量：160Gbps 转发性能：3.5Mpps（SRU80高性能主控板）/2000Mbps(64byte)

AR 系列产品的特点如下：

- 高性能

  华为 AR 产品采用最新的 ASIC 芯片和多核 CPU。LAN 模块内接口之间线速转发，LAN 模块之间具有高带宽 Fabric。CPU 采用 500MHz 两核到 750MHz12 核的 MIPS

版权所有 © 华为技术有限公司

处理器，25M 到 1G 的 WAN 转发性能，CPU 内置高性能加解密模块，具有 25M 到 300M 的加解密性能。

- 多业务集成

  华为 AR 产品除了提供对数据业务的支持外，还可以同时作为 IP PBX、IPSec VPN 网关和防火墙使用，AR12 还有支持 WLAN AP 的型号，真正做到数据、语音、视频、安全、无线等多业务的统一集成。

- 强大的 QoS

  华为 AR 产品支持 3 级 HQoS，其中 3260 通过 TM 硬件提供更强的转发性能。

- 高密度接入

  华为 AR 提供高密度的语音和数据接入，通过不同类型的插卡组合，可以充分满足各种场景下语音和数据的混合接入。

- 丰富的广域网接口

  华为 AR 提供丰富的广域网接口，包括 E1/T1、ISDN BRI、FR、3G 等各种主流接口，并支持作为 MPLS VPN 的 CE 和 PE 设备。

4.5 NE 系列

HUAWEI Net Engine40E 全业务路由器，简称 NE40E，是华为公司推出的高端网络产品，主要应用在各种大型企业网的边缘位置。

NE40E 的操作系统采用功能强大的通用路由平台 VRP，具有业务丰富、超大容量、高性能和高可靠性的特点。

表4-5 NE40E 系列路由器

产品型号	设备外观	备注
NE40E-X16		交换容量：2.56T 转发性能：1600Mpps

版权所有 © 华为技术有限公司

产品型号	设备外观	备注
NE40E-X8		交换容量：1.44T 转发性能：800Mpps
NE40E-X3		交换容量：1.08T 转发性能：300Mpps
NE40E-8		交换容量：640G 转发性能：400Mpps

版权所有 © 华为技术有限公司

产品型号	设备外观	备注
NE40E-4		交换容量：320G 转发性能：200Mpps

NE 系列产品的特点如下：

- 400G 平台，满足未来十年的发展需求
  - 设备紧凑，端口密度大，最高密度 1320GE/机框。
  - 绿色的 400G 平台，大容量低功耗。
  - 兼容设计，从 40G 升级到 400G 平台，单板、软件完全兼容。
- 全业务承载业界领先，为电信级业务运营保驾护航
  - 支持 BRAS、DPI 等功能模块，保证多业务接入能力。
  - 完整的 HQoS 解决方案，HQoS、DS-TE 和 MPLS HQoS，保证多场景的 QoS 部署。
  - 领先的增强视频解决方案，实现 FCC、RET、iRSM、iVSE 等技术，增强用户视频体验。
- 完善的端到端可靠性解决方案，保证业务永不中断
  - 设备级可靠：关键部件冗余备份，配合 ISSU/NSR/GR 等技术，最大限度避免业务中断运行。
  - 网络级可靠：华为独有的 BFD For anything、E-系列等技术，保证业务端到端 200ms 保护倒换。
  - 业务级可靠：业界领先的 BRAS Pool 解决方案，保证视频等高端业务永远在线，增强用户体验。

4.6 防火墙系列

E1000E-X 系列防火墙采用万兆多核全新硬件平台，轻松实现海量业务处理，打造业务永续的办公网络；融合 Symantec 先进的入侵防御和反病毒技术，重新演绎专业内容安全防御，营造更安全的办公网络；集成华为业界领先的 DPI 识别技术，精细管理超千种应用程序，创建更高效的办公环境。

版权所有 © 华为技术有限公司

表4-6 防火墙系列产品

产品型号	设备外观	备注
E1000E-U2		• 4个GE光电互斥接口、1个Console口、2个USB口； • 2个扩展槽； • 支持2GE、4FE接口板； • 吞吐量：2Gbps；
E1000E-U3		• 固定接口：4GE电+4GECombo • 支持万兆接口 • 标配双电源(AC/DC可选) • 扩展槽：2*FIC • 吞吐量：6Gbps
E1000E-U5		• 固定接口：4GE电+4GECombo • 支持万兆接口 • 标配双电源(AC/DC可选) • 扩展槽：2*FIC • 吞吐量：10Gbps
E1000E-U6		• 固定接口：4GE电+4GECombo+8GE光 • 支持万兆接口 • 标配双电源(AC/DC可选) • 扩展槽：2*MIC+5*FIC • 吞吐量：20Gbps

防火墙系列产品的特点是：

- 万兆多核全新硬件平台，打造业务永续的网络
  - 性能优异，实现海量业务处理

    15G 防火墙吞吐；200K 每秒新建连接数；400 万并发连接数；15K 并发 VPN 隧道；大容量 NAT 转换能力；轻松实现海量业务处理。
  - 高密度万兆接口，适应不同应用场景需求

    64 千兆+14 万兆的高密度接口，为提前跨入万兆时代的您提供不同组网情况下的安全防护，方便您细化安全区域。
  - 超长无故障运行时间，确保客户业务连续性

    关键部件冗余配置，成熟的链路转换机制，支持光、电两类内置 Bypass 插卡，为您提供超长无故障硬件保障；商用 10 年以上的超稳定软件平台，全球在线设备超过 10 万台，为您打造永续的办公环境。
- 超千种应用程序的精细管理，创建更高效的网络

版权所有 © 华为技术有限公司

- 广泛应用识别，实现网络可视化：150 名应用识别专家，超过 850 种可识别应用分类，让您一目了然网络带宽应用。
- 海量网站分类，营造绿色上网环境：6500 万海量网站，超过 130 种内容分类，屏蔽挂马、钓鱼等恶意网站，防范员工不当操作危害内网安全；隔离赌博色情等不良网站，营造绿色上网环境。
- 精细应用管理，创建高效办公网络：基于时间、应用、用户、带宽、连接数的多方位调控手段，可有效保障关键业务带宽，提升带宽利用率和员工工作效率，让 P2P/IM/Web 网站随您掌控。

- 专业内容安全防御技术的重新演绎，提供更安全的网络
  - 业界领先反病毒引擎，提供 99%高精准检出率：基于 Symantec 多年积累的反病毒技术，采用文件级内容扫描的 AV 引擎，结合全球领先的仿真环境虚拟执行技术，提供高达 99%的精准检出率，多次荣膺国际评测组织好评。
  - 专业漏洞补丁技术，让“变形”无所遁形：传统基于攻击代码的防护方式，因为攻击种类的频繁变形，需要维护更新庞大签名库，使得 IPS 引擎不堪重负，检测性能低下，误报漏报率较高。E1000E-X 采用 Symantec 领先的漏洞防护技术，针对漏洞（而非攻击代码）提供“虚拟补丁”，让各种攻击变形无所遁形。
  - 专业团队实时更新，实现零日攻击防护：全球部署的蜜网系统和超过 300 人的专业安全分析团队，持续追踪最新、最热门、最高危的系统漏洞和软件漏洞，以最快速的应对方案实现零日攻击防护，为您提供更安全的办公网络。
- 一键式配置，让策略调优化繁为简
  - 图形化配置界面，从此告别命令行：基于 Web 界面配置管理，更直观、更简单，彻底摆脱繁琐的配置。
  - 专业配置向导，轻松搞定策略配置：每项独立业务，均提供专业配置向导，让管理员轻松搞定策略配置。
  - 一键开启 IPS 和 AV，减轻维护工作量：基于 99%高精准检出率的 IPS/AV 规则库，无需调测，直接开启，将管理员从费时、费力、繁复的策略调优中彻底解放出来，真正实现快速部署，即插即用。

版权所有 © 华为技术有限公司