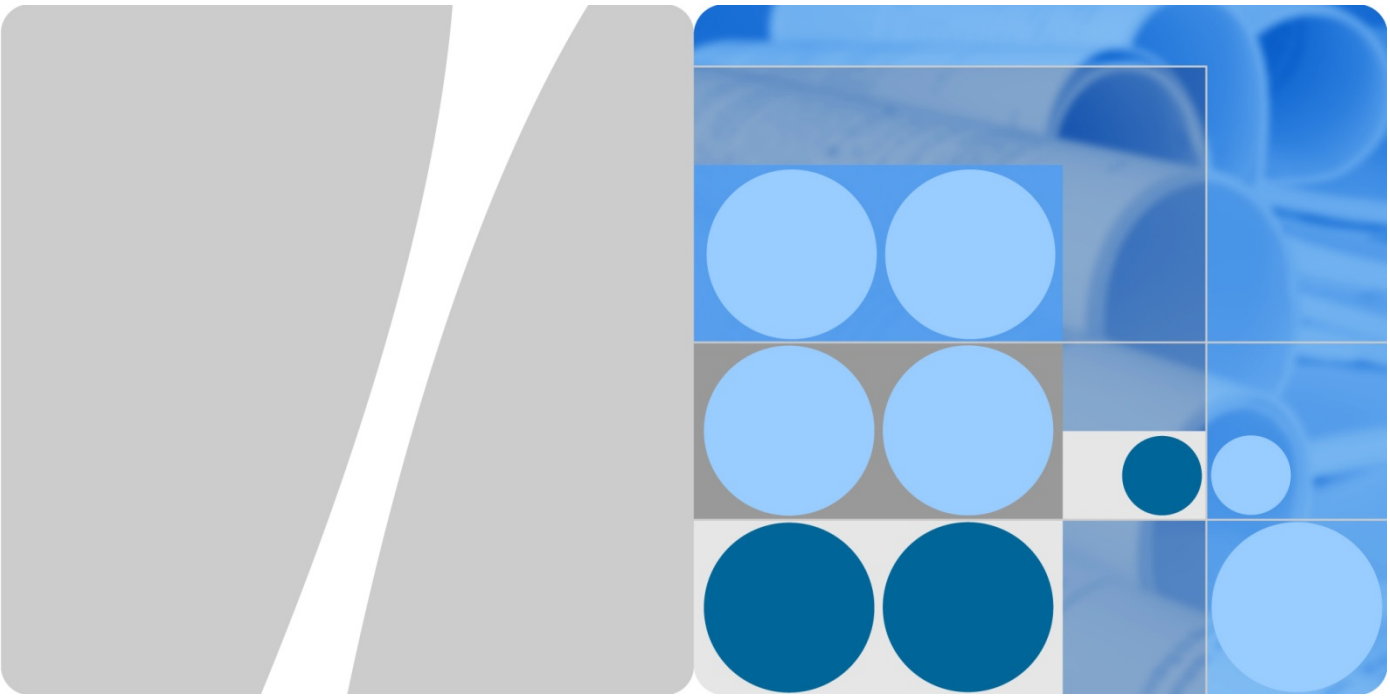


虚拟园区网解决方案
V100R001C00
技术建议书

文档版本 02

发布日期 2012-01-05

华为技术有限公司

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

1 虚拟园区网方案概述

1.1 方案背景

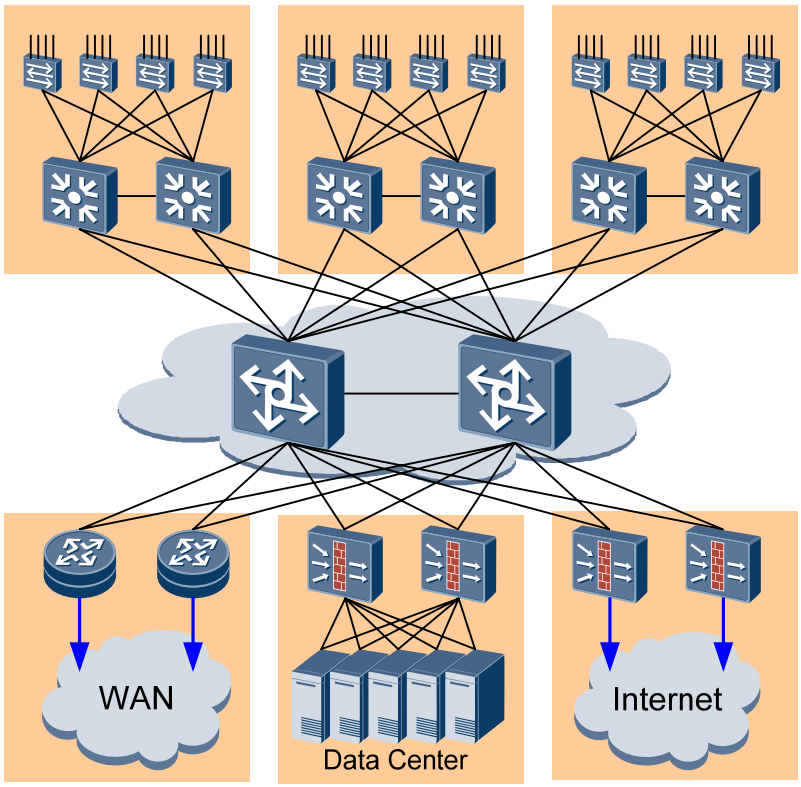
企业园区网作为企业网络的核心部分，连接企业的办公、生产、研发、财务等多个部门和机构，在企业信息化建设中具有重要地位。

企业园区网是一个密集型的网络，在固定的空间内，聚集了大量的接入用户和种类众多的终端，因此对于网络的性能、可靠性、可管理性都有较高的要求。随着 IT 在企业活动中重要性越来越高，建设简洁、可靠、高性能的园区网成为企业信息化的重要目标。

当前的园区网建设，采取的组网形式主要是分层、分模块的部署模式，如图 1-1 所示。

- 分层部署就是将网络按接入、汇聚、核心规划为多层结构，各层网络部署不同的功能特性，使网络结构清晰，便于扩展。
- 接入层网络一般采用二层设计将用户的三层网关设置在汇聚层设备上，为了保证节点的可靠性，汇聚层和核心层采用双节点组网。
- 园区网的模块化设计是指以企业的物理结构或逻辑结构，采用统一的设计方式，形成模块化的网络结构，这样设计使园区网的管理及扩展更加的容易。

图1-1 传统的园区网组网结构



但是，随着业务的发展，这种经典的园区网设计也逐渐体现出一些不足，主要表现为：

- 汇聚层、核心层的双节点冗余设计，虽然提高了网络的可靠性，但是也使得网络结构和互联关系变得复杂，网络的扩展也变得困难。
- 冗余结构使得网络的树形结构中出现环路，并且随着企业的不断发展，环网规模不断扩大。因此一般都需要部署 MSTP 等协议消除环路，同时运行 VRRP 等来支持节点冗余备份，导致网络协议的部署变得复杂。
- 不同部门/群组用户的资源访问权限需要进行控制，不同业务间的访问、传输和应用也需要进行端到端的隔离。但是传统的物理隔离技术已经无法满足这种需求，导致网络重复建设、管理分散、安全策略难以部署。

为了解决上述问题，华为公司提出了虚拟园区网解决方案，来解决上述问题。

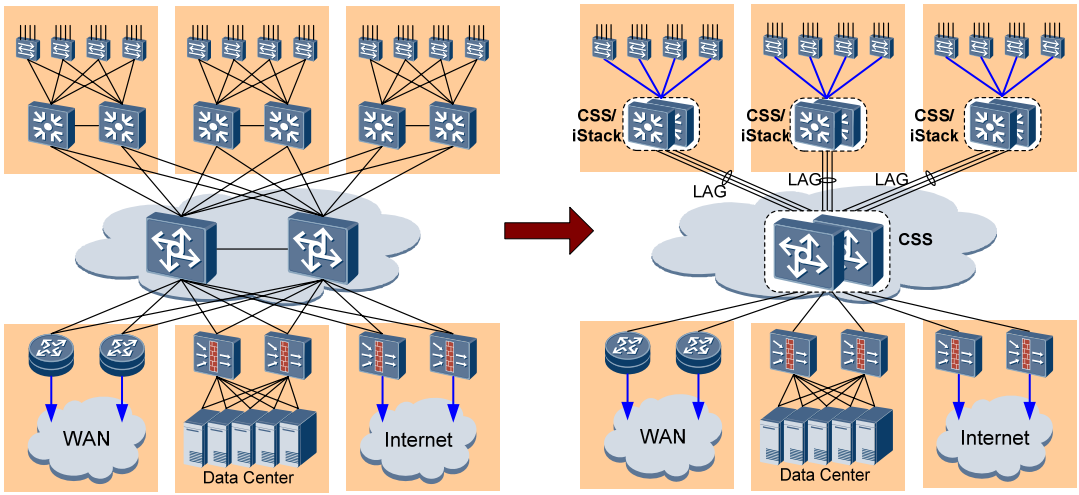
1.2 虚拟园区网解决方案

华为虚拟园区网解决方案包括横向虚拟化方案和纵向虚拟化方案两部分。

1.2.1 横向虚拟化方案

横向虚拟化方案是指在园区网的核心层、汇聚层、接入层分别采用集群/堆叠技术，将多台物理设备虚拟化成单台逻辑设备，达到简化网络结构、简化网络协议部署、提高网络可靠性和可管理性的目的。横向虚拟化方案如图 1-2 所示。

图1-2 横向虚拟化方案



在横向虚拟化方案中：

- 在核心层采用 CSS（Cluster Switch System）技术，将多台核心交换机（S9300）组合成一台逻辑设备。
- 在汇聚层和接入层，采用 CSS 或者 iStack 堆叠技术，将多台汇聚/接入交换机组合成一台虚拟的逻辑交换机。
- 互联方面，可采用 LAG（Link Aggregation Group）技术，将多个物理接口捆绑在一起作为一个逻辑接口来增加带宽。

简化网络结构

通过图 1-2 可以看出，通过集群/堆叠技术，原先复杂的网络拓扑结构和互联关系，被简化为层次分明、互联关系单一简明的网络结构，可极大提升网络的可维护性。

简化协议部署

传统园区网的汇聚和核心层设备为了高可靠性，一般都采用双节点冗余备份的组网结构。这种结构致使网络中出现许多环路，必须要部署 MSTP、VRRP 等协议来消除环路，支持冗余备份结构，导致部署极为复杂。

采用横向虚拟化方案后，通过 CSS/iStack 技术对汇聚与核心层进行横向整合，将多台冗余设备虚拟化为单台逻辑设备。网状结构优化为简洁的树形结构，网络各层之间通过 LAG 捆绑链路互联，自然消除环路。因此不再需要部署 MSTP 和 VRRP 等协议。

链路负载分担和冗余备份

采用 CSS/iStack 对网络节点进行堆叠之后，网络各层之间可通过 LAG 捆绑 Trunk 链路进行互联，可实现链路的负载分担和冗余备份，主要有以下几种方式：

- 手工配置模式：手工配置 Trunk 链路和负载分担方式。这种情况下，Trunk 中所有链路均参与负载分担，无冗余备份。

- LACP 模式：通过 LACP 协议自动协商机制，自动协商负载分担和冗余备份参数。这种情况下，Trunk 链路可实现 M:N 的负载分担和冗余备份功能，其中 M 条链路处于活动状态，负责转发数据并进行负载分担，另外 N 条链路处于非活动状态作为备份链路，不转发数据。

网络灵活扩展

使用 CSS/iStack 技术进行横向虚拟化后，如果需要扩展端口、扩展系统处理能力、扩展上行带宽时，只需要在集群/堆叠系统中增加新的成员交换机即可实现，而不需要对网络拓扑进行大的调整。

另外，通过跨越空间的堆叠系统（使用光纤远程连接），将各楼宇的交换机虚拟化成一个逻辑设备，网络结构变得更加简单，网络变得更加健壮、可靠，管理和维护得到降低。

1.2.2 纵向虚拟化方案

纵向虚拟化方案是通过各种隔离技术，将一个物理网络划分成几个相互独立的逻辑网络，实现了终端和业务的安全隔离、应用资源的按需分配等。

纵向虚拟化方案实际上包括了以下四个方面的内容：

- 用户接入控制方案
- 用户接入安全方案
- 业务安全隔离方案
- 资源虚拟化方案

说明

其中关于用户接入控制和用户接入安全方面，另有专题方案进行描述，请参考《有线无线一体化技术建议书》和《用户安全接入技术建议书》。本文档中只对后两个方面的内容进行描述。

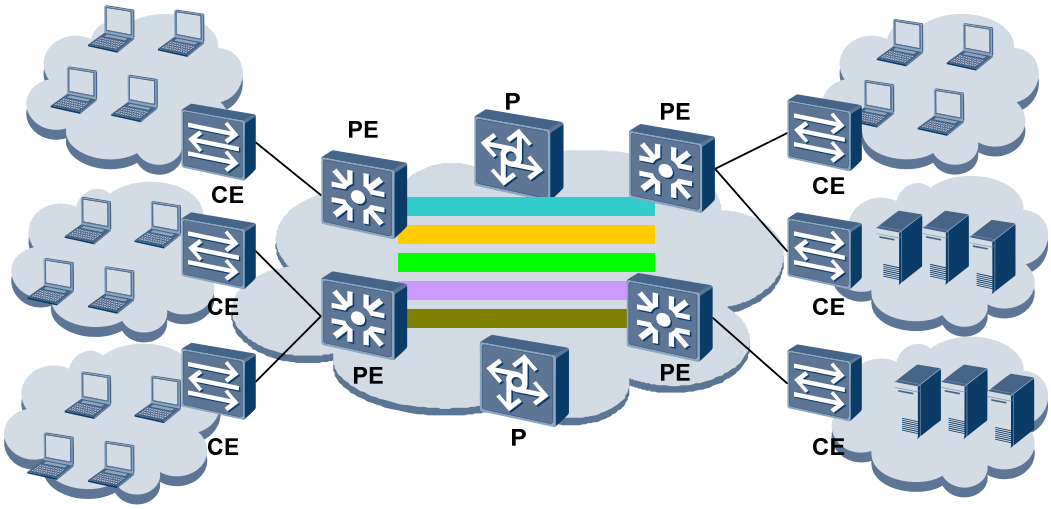
业务安全隔离

对园区内共用一个物理网络传输各种应用数据的横向逻辑隔离，有 VLAN、隧道、MCE、VPN 等多种方式，但从业务隔离灵活性、配置管理复杂度、扩展性、组网对设备的要求等多方面综合对比，MPLS L3VPN 技术最适合应用在大、中型园区内进行业务隔离。

MPLS L3VPN 原来是广泛应用于服务提供商 VPN 解决方案中基于 PE 的技术，它使用 BGP 在服务提供商骨干网上发布 VPN 路由，使用 MPLS 在服务提供商骨干网上转发 VPN 报文。MPLS L3VPN 组网方式灵活、可扩展性好，并能够方便地支持 MPLS QoS 和 MPLS TE，因此得到越来越多的应用。

在园区网中，通过三层交换机同样可以构建 MPLS VPN 网络，承载所有业务的传输数据，并进行安全隔离。如图 1-3 所示。

图1-3 MPLS L3VPN 网络



- 接入用户通过网络边缘的接入交换机接入，认证通过后策略服务器根据认证用户名下发策略把用户端口加入到相应的 VLAN 中，通过 VLAN 接口与 VPN 的绑定关系，把用户加入到相应的 VPN 中去；
- 服务器端根据应用和访问用户的不同，也把数据分配到相应的 VPN 中传输，并且 PE 设备会为每个 VPN 建立独立的转发表项，各 VPN 进行独立的数据转发，这样就为用户到服务器提供了一种端到端业务传输通道，把不同用户、不同应用的数据横向隔离开来，保证数据传输的私密性和安全性。

资源虚拟化

传统物理隔离网络造成的一个后果，是必然的安全策略分别部署、管理复杂度增加、应用服务器需要重复部署且数据同步困难，本方案中各种虚拟化技术的综合应用，有效解决了以上难题。

在园区虚拟化解决方案中，我们为用户提供集中的数据中心服务、统一的 Internet/广域网出口、统一的网络监控/管理软件，提高资源的利用率：

- 园区内所有用户共享统一的 Internet/广域网接口，通过虚拟防火墙、NAT 多实例等部署方案，为不同群组的用户和业务提供灵活的安全策略服务。
- 集中的数据中心，通过计算虚拟化、存储虚拟化、虚拟安全等技术，屏蔽底层硬件服务器、存储设备间的差异，根据业务使用分配资源。
- 统一的网络管理、监控软件，通过专门的管理 VPN，实现对整网资源的配置管理和对各种业务流量的监控、规划。

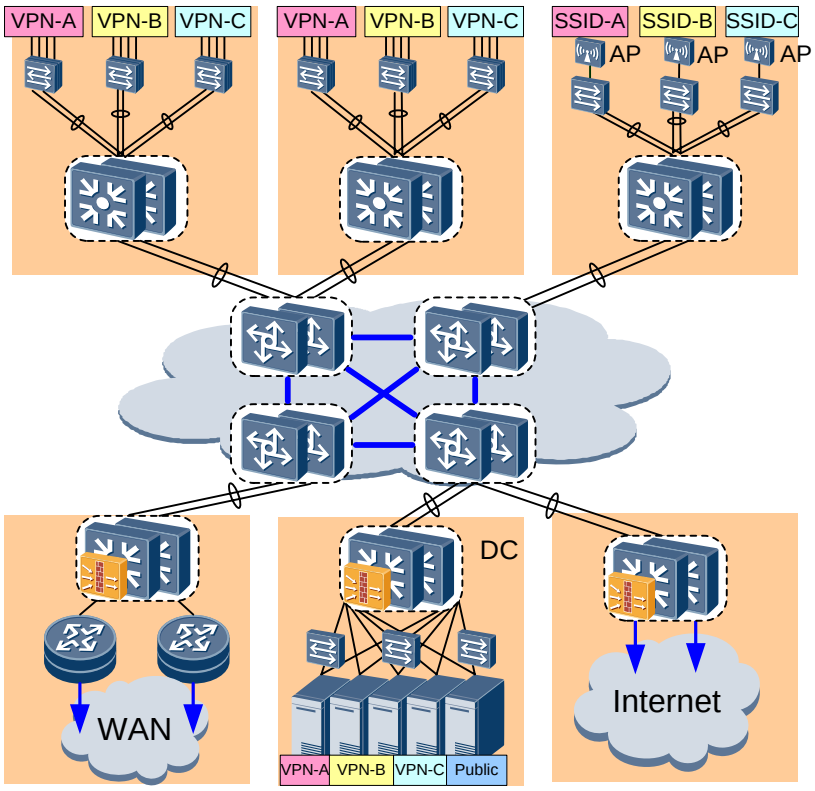
1.2.3 整网综合部署

综合横向虚拟化及纵向虚拟化技术之后，虚拟园区网的整体网络架构如图 1-4 所示。

- 在核心层、汇聚层、接入层分别通过 iStack/CSS 技术进行硬件设备的虚拟化，达到简化网络结构、简化网络协议部署、提高网络可靠性和可管理性的目的。
- 在各边缘网络（WAN 出口、Internet 出口）以及数据中心的安全方面，通过在汇聚交换机上部署 FW（Firewall）单板或者部署独立的 FW 设备来保证。

- 整网通过 MPLS L3VPN 进行路径虚拟化，完成对网络资源的隔离。

图1-4 虚拟园区网整体部署



1.3 市场定位和面向客户群

虚拟园区网解决方案可有效提升网络的可维护性、可靠性、安全性。通常适用于业务部门众多、网络复杂庞大的企事业单位，例如企业大型园区、高校校园、大型矿区和油田、政府行政中心等等。

2 横向虚拟化规划建议

2.1 概述

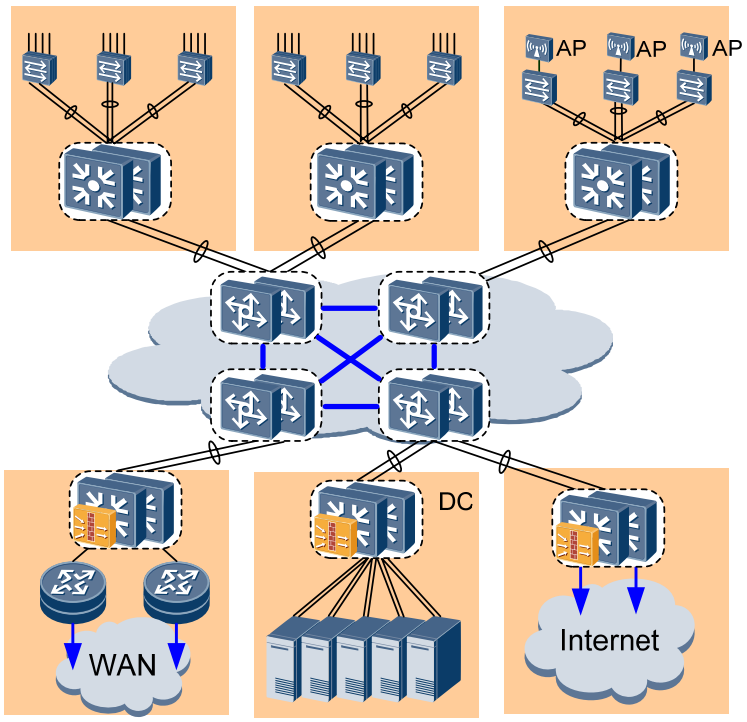
指在园区网的核心层、汇聚层、接入层分别采用集群/堆叠技术，将多台物理设备虚拟化成单台逻辑设备，达到简化网络结构、简化网络协议部署、提高网络可靠性和可管理性的目的。

对于横向虚拟化的规划建议，主要是物理组网方面的规划。

2.2 网络拓扑规划

横向虚拟化之后，典型的网络拓扑结构如图 2-1 所示。

图2-1 横向虚拟化网络拓扑结构



横向虚拟化园区网继承传统网络的分层和分模块设计思路，但是通过集群和堆叠技术，将简化各层和各模块之间的连接关系，简化网络协议部署。

分层规划

整个网络按照网络层次划分为接入层、汇聚层和核心层。

- 接入层是最靠近用户的网络，部署二层接入设备，负责不同用户终端的接入。
- 汇聚层负责将大量用户接入互联网络，扩展核心层设备接入用户的数量，并承担用户三层边缘网关的角色。
- 核心层负责整个园区的互联，核心层设备之间采用 Mesh 方式互联。核心层一般只承担高速互联的作用，一般不承担用户管理和其他应用方面的职责。

分模块规划

整个网络按照功能划分成不同的部件，包括内部网络、数据中心、边缘网络和核心网络几大部件。

- 内部网络是企业员工工作所依赖的网络，提供用户接入网络的接口。
- 数据中心是园区网的一个重要部件，企业的应用服务器都部署在这里。
- 边缘网络是园区网对外部分，分支、远程用户、合作伙伴、客户都从这里接入。
- 核心网络也叫互连核心，完成园区网其它部件的互联。

说明

关于数据中心的详细规划，另有专题方案描述，本文不再详细描述。详细信息可参考《数据中心技术建议书》。

集群/堆叠规划

通过 CSS/iStack 技术，将接入、汇聚和核心层设备进行横向整合，减少网络拓扑节点，简化网络连接关系，简化网络协议部署。

- 核心层设备的冗余备份双节点，通过 CSS 整合为单台逻辑设备。各 CSS 节点之间依然采用 Mesh 组网结构。
- 汇聚层设备的冗余备份双节点，通过 CSS 或 iStack 技术（视采用的设备而定）整合为单台逻辑设备。每个汇聚节点通过 Trunk 链路上行接入核心节点。不再需要考虑汇聚设备和核心设备之间的口字形或三角形连接结构。
- 接入层设备是否使用堆叠视具体情况而定。而上行链路的设计则依赖于汇聚层节点的堆叠情况。
  - 在成本允许的情况下，建议使用支持堆叠的交换机进行堆叠，减少管理节点。在成本不允许的情况下，可采用普通交换机接入。
  - 如果汇聚层设备是 CSS/iStack 节点，则接入设备上行通过 Trunk 链路接入汇聚节点；如果汇聚层设备是普通的冗余双节点，则接入设备通过口字形或三角形结构双归接入汇聚节点。

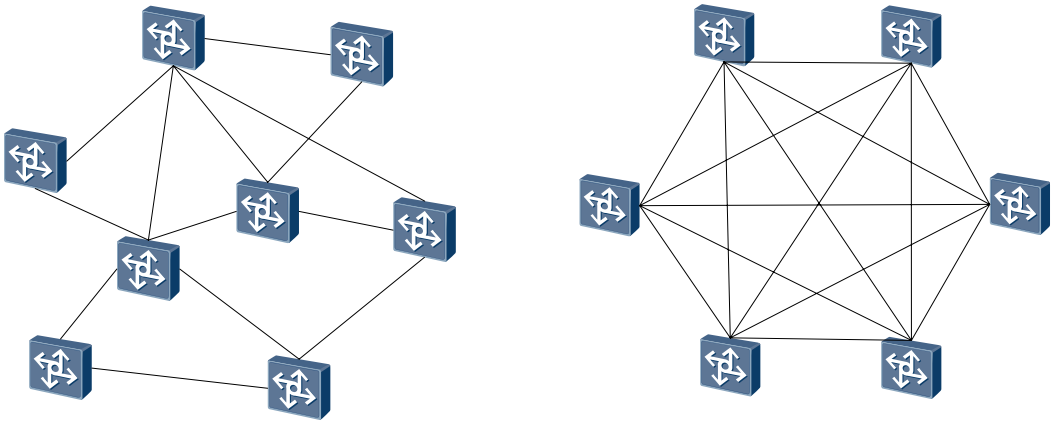
2.3 核心层规划

核心层负责整个园区网的高速互联，一般不部署具体的业务。核心网络需要实现带宽的高率用率和故障的快速收敛。

核心网络的规划相对简单，一般来说需要考虑设备备份和链路备份两个方面：

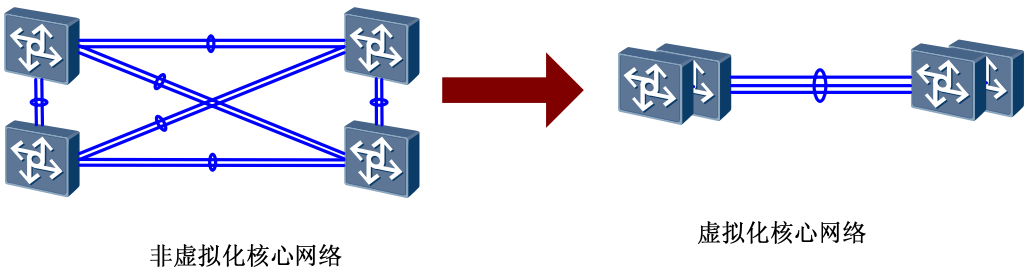
- 设备备份：核心层的设备是不能单独的一台设备，这样在出现故障的时候，就会导致大面积的网络瘫痪。一般需要在每个物理位置上部署冗余备份的两台设备，互为备份。
- 链路备份：核心层的设备间一般都是 Full Mesh 或 High Mesh 组网结构，如图 2-2 所示，这样即使其中的一条或多条链路故障，也不会导致节点失效，从而引起网络瘫痪。

图2-2 Full Mesh 和 High Mesh 组网结构



而在横向虚拟化的方案中，冗余备份的两个核心节点可以通过 CSS 技术，使用专用堆叠线缆进行连接，虚拟化成单台设备，减少了网络管理节点，提升网络的可靠性。而在互联方面，则依然采用 Mesh 组网结构，如图 2-3 所示。

图2-3 虚拟化核心网络



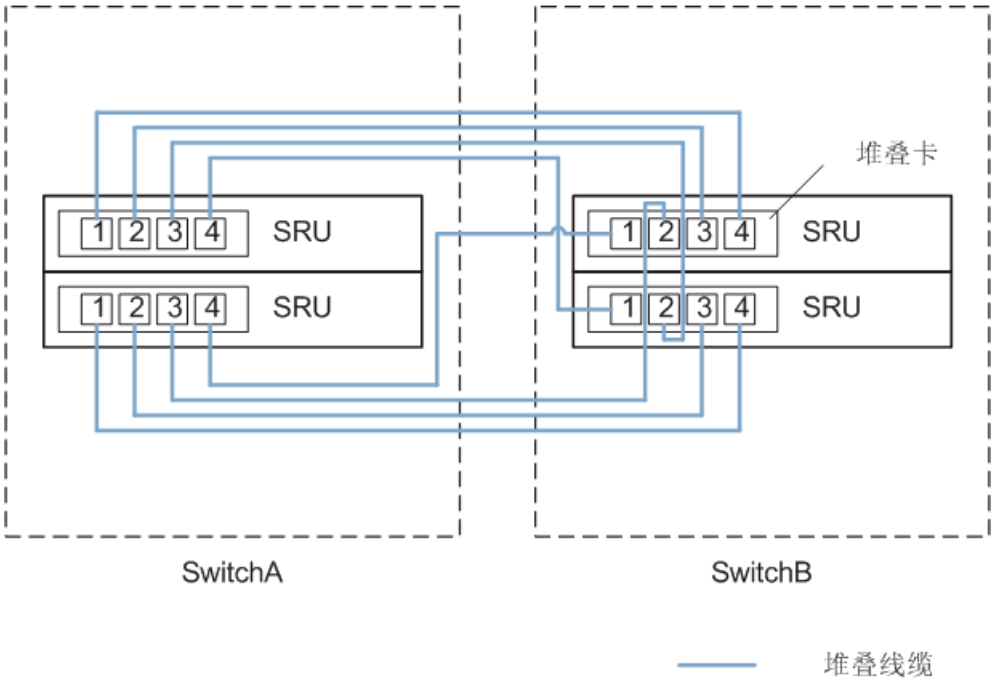
以 S9300 系列交换机为例，两台 S9300 交换机在满足如下条件时，可以进行堆叠。

- 设备型号为 S9306 或者 S9312，不能是 S9303。

- 每台设备上配置两块相同的主控板（SRUA 或 SRUB），两台设备之间可以不同。
- 在每块主控板上都插入堆叠卡。（四个插口）
- 两台设备之间采用专用的 QSFP（Quad Small Form-Factor Pluggable）高速线缆，按照图 2-4 所示线序，将两台设备进行连接。

此时堆叠系统的交换机在已使能堆叠功能的情况下，上电时堆叠系统会自动建立。通过竞争，一台成为堆叠主交换机、另一台成为堆叠备份交换机。

图2-4 堆叠线缆连接规则



2.4 汇聚层规划

核心设备的物理端口总是有限的，汇聚层存在的理由就是将众多的接入设备和大量用户经过一次汇聚后再接入到核心层，扩展核心层接入用户的数量。

汇聚层通常还作为用户三层网关的位置，承担 L2/L3 边缘的角色，提供用户管理、安全管理、QoS 调度等各项跟用户和业务相关的处理。

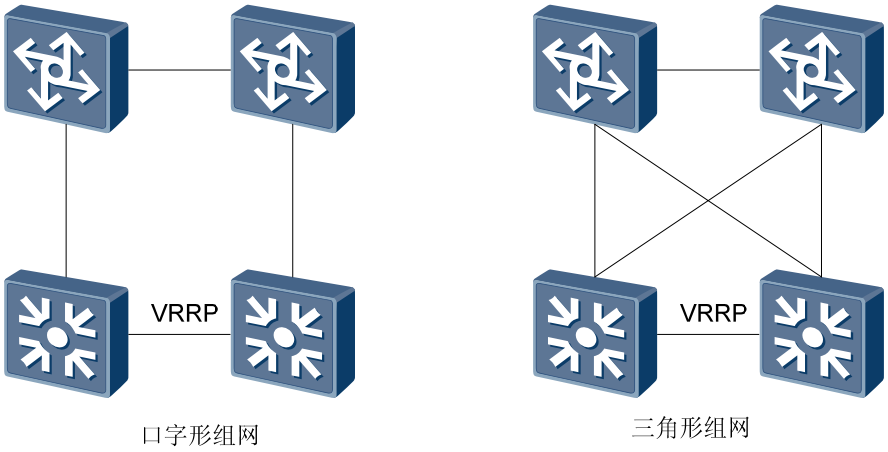
汇聚层在组网规划上一般要考虑一下几个方面：

- 支撑接入层的双归接入，作为网关设备，汇聚层故障会直接导致部分网络的瘫痪，所以汇聚层的设备一般都要支持主备，并运行主备协议 VRRP。
- 双归接入到核心层，汇聚层的设备之间是不会全互联的（通常情况下，连互联都不会），所以在可靠性上，都需要支撑双归到核心层。

传统的汇聚层设计中，每个节点都采用运行 VRRP 的主备两台设备，上行通过口字形组网或者三角形组网方式双归接入核心层。如图 2-5 所示。

- 口字形组网的思想是在核心层和汇聚层构建一个环网，对于汇聚双归到核心的情况，相当于构成主备的汇聚设备分别和一台核心设备互联。口字形组网部署成本较低，但是整体链路利用率低，对汇聚交换机的要求高（单点，并且路由信息复杂。
- 三角形组网的思想是每台汇聚设备单独双归到核心设备，汇聚层设备之间应该互联。三角形组网对汇聚交换机要求较低，路由信息简单，但是部署成本较高（较多的链路），另外上行端口利用率低（有一个口是备份口）。

图2-5 口字形和三角形组网



口字形组网　　三角形组网

而在横向虚拟化的方案中，对于同一物理位置的汇聚层冗余备份节点采用 CSS 或 iStack 技术进行虚拟化，形成一个逻辑节点，从而降低网络复杂度，提升网络可靠性。

如果汇聚层节点使用的是 S9300，则堆叠方案“2.3 核心层规划”的方案相同。

如果汇聚层节点使用的是 S5700，则多台 S5700 在满足以下条件的情况下，可以建立多设备之间的堆叠：

- 所有设备属于同一系列（EI 或者 SI）。
- 所有设备中都插入 EPTC-堆叠后插卡。（两个插口）
- 多台台设备之间采用专用的 PCI-E 线缆，以链形或环形结构连接。如图 2-6 和图 2-7 所示。

此时堆叠系统的交换机在已使能堆叠功能的情况下，上电时堆叠系统会自动建立。通过竞争，一台成为主交换机、一台成为备份交换机，其余的为从交换机。

图2-6 链型堆叠

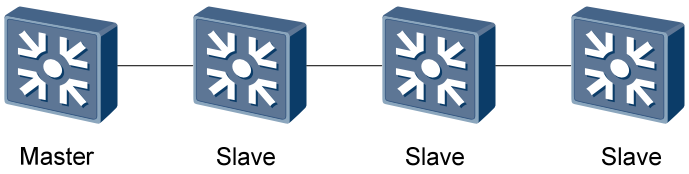
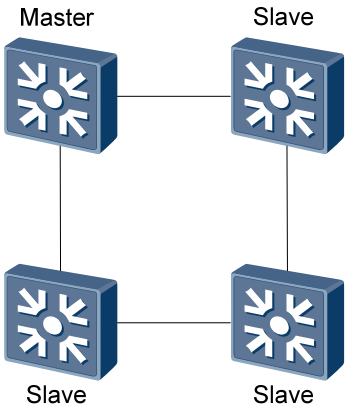


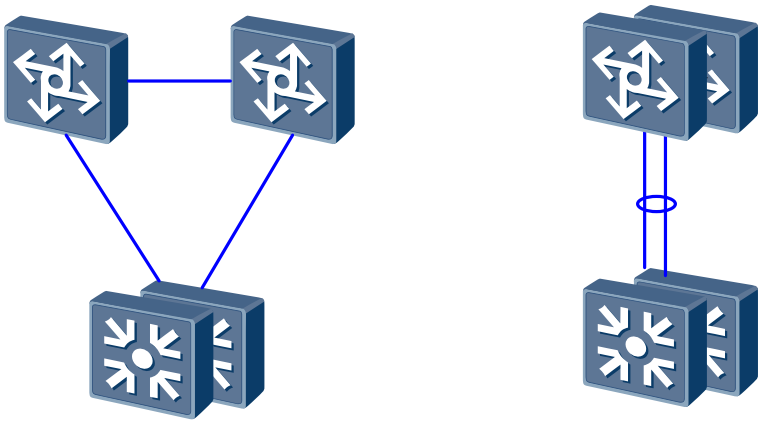
图2-7 环形堆叠



当汇聚层设备堆叠后，上行双归接入核心层时，根据核心层是否采用堆叠的情况，有以下两种组网形式，如图 2-8 所示：

- 如果双归到不支持 CSS 堆叠的核心层设备时，采用两条独立的链路。
- 如果双归到支持 CSS 堆叠的核心层设备时，采用 Trunk 链路。

图2-8 堆叠汇聚设备双归到核心设备



2.5 接入层规划

接入层是最靠近用户的网络，部署二层接入设备，负责不同用户终端的接入。

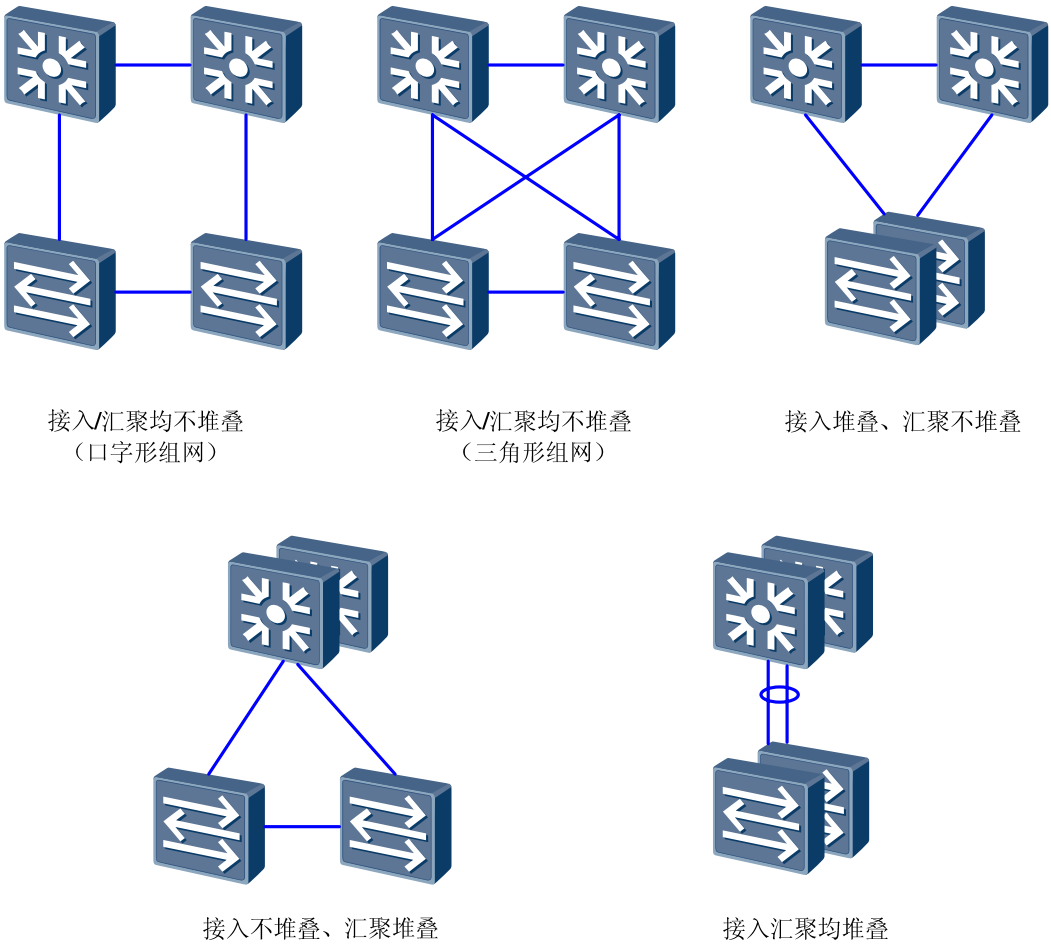
和汇聚层类似，传统的接入层设计中，每个接入设备上行也是通过口字形组网或者三角形组网方式双归接入核心层。具体的描述参见“2.4 汇聚层规划”。

而在横向虚拟化的方案中，对于接入层设备，接入层设备是否使用堆叠视具体情况而定。

- 在成本允许的情况下，建议使用支持堆叠的交换机进行堆叠，减少管理节点。

- 在成本不允许的情况下，可采用普通交换机接入。
- 如果汇聚层设备是 CSS/iStack 节点，则接入设备上行通过 Trunk 链路接入汇聚节点.
- 如果汇聚层设备是普通的冗余双节点，则接入设备通过口字形或三角形结构双归接入汇聚节点。

图2-9 接入层双归接入汇聚层各种组网形式



接入层设备（例如 S2700/S3700/S5700）具体的堆叠方案，与汇聚层中所描述的堆叠方案相同。请参见“2.4 汇聚层规划”。

2.6 边缘网络规划

边缘网络是园区网络到外部公网的边界，园区网的内部用户是通过边缘网络接入到公网的，外部用户（包括客户、合作伙伴、分支机构、远程用户等）也是通过边缘网络接入到内部网络的。

边缘网络的规划一般包括如下场景：

- 内部用户访问公网

- 合作伙伴访问园区网络
- 分支机构访问园区网络
- 远程用户访问园区网络
- SOHO 办公访问园区网络
- 客户访问园区网络

关于边缘网络的详细规划，基本上和经典的园区网规划一致，请参考《园区网技术建议书》。本文不再详述。

3 纵向虚拟化规划建议

3.1 概述

纵向虚拟化方案是通过各种隔离技术，将一个物理网络划分成几个相互独立的逻辑网络，实现了终端和业务的安全隔离、应用资源的按需分配等。在纵向虚拟化的方案中，华为推荐使用的是 MPLS VPN 技术。

3.2 物理组网规划

在纵向虚拟化园区网方案中，物理组网方面和可以采用传统的园区网设计，如图 1-1 所示，详细的规划内容可以参考《园区网技术建议书》。

也可以按照横向虚拟化的园区网进行设计，如图 2-1 所示，详细的规划请参考“2 横向虚拟化规划建议”。

3.3 VLAN 规划

在纵向虚拟化方案中，VLAN 是 MPLS L3VPN 在二层网络中的延伸，通过 VLAN 实现用户在二层接入网络中的隔离。并通过 VLAN 与 VPN 实例（VRF）的绑定，实现端到端的业务隔离，达到共用交换机端口的目的。

规划 VLAN 时，通常有如下几种方式：

- 按业务划分 VLAN：如语音 VLAN、数据 VLAN、管理 VLAN 等。
- 按职能部门划分：如财务部 VLAN、销售部 VLAN 等。
- 混合型：综合按照业务和职能部门划分，比如语音 VLAN 整个网络相同，数据业务则为了不同部门间的隔离，不同部门采用不同的数据 VLAN。

对于虚拟化的园区网来说，建议使用混合型的 VLAN 划分方式，并且更注重在职能部门的 VLAN 规划上。

注意

在 VLAN 规划中，除了业务 VLAN，还要规划管理 VLAN，以及安全用途的 VLAN，如 802.1x 认证时的 Guest VLAN 和 DMZ VLAN 等。

在纵向虚拟化方案中，VLAN 的部署分为两个部分：

- PE 侧（例如汇聚交换机）的 VLAN 部署，作为 PE 的三层交换机边缘接口配置成子接口或者 VLANIF 接口，根据不同的部门划分不同的 VLAN ID。
- CE 侧的 VLAN 部署，作为 CE 的二层接入交换机上行接口配置成 VLANIF 接口，根据不同的业务部分划分不同的 VLAN ID，与 PE 设备边缘接口的 VLAN 相对应。

对于 MPLS L3VPN 的不同 Site 来说，建议每个 Site 的 CE 的上行 VLANIF 接口配置为相同 VLAN ID，便于管理。

3.4 IP、DHCP、DNS 规划

请参见《园区网技术建议书》。

3.5 IGP 规划

3.5.1 IGP 选择

IS-IS 和 OSPF 是目前使用最广泛、最成熟的两个 IGP 协议。尽管两者的实现机制不同，但无论从功能还是性能来说，二者都没有太大差别。

根据业界的统计，在封闭性质的企业网络中，OSPF 使用的频率要高于 IS-IS。但这并非是完全是技术上的原因，而是与历史和厂商的市场策略有关。

从技术上来分析，OSPF 和 IS-IS 进行对比，有如下一些细微的区别：

- IS-IS 比 OSPF 更加安全。IS-IS 报文封装在链路层，属于二层组播报文，不可路由；而 OSPF 报文由 IP 报文承载，可路由，这就为远端攻击 OSPF 提供了可能。
- IS-IS 可扩展性更强。IS-IS 通过新增 TLV 就可以容易地支持 IPv6，而 OSPF 需要升级到 OSPFv3 才能支持 IPv6。

但在企业网中，一方面，远端攻击 OSPF 的风险较小；另一方面，如果企业使用的是私网 IPv4 地址，尚无部署 IPv6 的需求，通常可以不考虑 IPv6 的因素。因此这两方面的因素都可以忽略。在这种情况下，企业可以自由选择 IS-IS 还是 OSPF。

说明

华为公司全系列网络产品均已支持 IPv6，可助力企业完成向 IPv6 的演进。有关这方面的内容，可访问华为公司网站 www.huawei.com 中的“解决方案 > IPv6”部分。

3.5.2 OSPF 规划

区域划分

在企业网中，部署 OSPF 时，需要根据网络的规模来考虑是否进行分层设计。

- 如果网络规模不大，例如终端数量<2k，则建议不进行分层设计，所有网络节点统一规划为 Area 0。
- 如果网络规模较大（或者未来扩展的规模较大），可以考虑对 OSPF 进行分层设计。其中核心层节点设置为 0 区域，而其余的汇聚网络节点设置为非 0 区域。

Cost

Cost 设计比较灵活，可以根据距离的远近、链路带宽的大小等进行设计。除此之外，更重要的是考虑企业业务对网络流量走向的需求。

在这方面，需要根据企业自身的业务特点和网络拓扑等综合考虑来规划链路的 Cost 值，本文不作详细建议。

可靠性

参见“3.9.1 IGP 可靠性规划”。

安全性

在企业网内，一般不需要特别考虑 OSPF 协议的安全性。

3.5.3 IS-IS 规划

NET

网络实体名称 NET（Network Entity Title）同时定义了当前 IS-IS 的区域地址和路由器的系统 ID。一般 NET 的格式为：AA.BBBB.CCCC.DDDD.SSSS.SSSS.SSSS.00，其中 ABCD 部分表示 Area ID，S 部分表示 System ID。

在企业网内部，在没有特殊考虑的情况下，Area ID 可以设置为全 0，而 System ID 可以由设备的 Loopback0 地址来生成。例如 Loopback0 地址为 10.112.58.113，则 System ID 可以表示为 0101.1205.8113。

区域划分

在企业网中，部署 IS-IS 时，需要根据网络的规模来考虑是否进行分层设计。

- 如果网络规模不大，例如终端数量<2k，则建议不进行分层设计，所有节点统一工作在 Level-2 模式（使用 Level-2 而不是 Level-1，是为了方便以后的网络扩展）。
- 如果网络规模较大（或者未来扩展的规模较大），可以考虑对 IS-IS 进行分层设计。其中核心层节点设置为 Level-2 模式，而其余的汇聚网络设备设置为 Level-1 模式。（一般不需要设置 Level-1-2 模式的路由器）

Cost

Cost 设计比较灵活，可以根据距离的远近、链路带宽的大小等进行设计。除此之外，更重要的是考虑企业业务对网络流量走向的需求。

在这方面，需要根据企业自身的业务特点和网络拓扑等综合考虑来规划链路的 Cost 值，本文不作详细建议。

可靠性

参见“3.9.1 IGP 可靠性规划”。

安全性

在企业网内，一般不需要特别考虑 IS-IS 协议的安全性。

3.6 BGP 设计

传统的企业园区网通常不会进行多路由域的设计，因此一般不涉及 BGP 的设计。但是在横向虚拟化方案中，由于需要使用 MPLS L3VPN，需要在 PE 之间传递 VPN 私网路由，因此需要使用 MP-IBGP 协议。

MP-IBGP 是对传统 BGP 的扩展，增加了对 VPNv4 和 IPV6 地址族的支持。在 L3VPN 中，主要用于私网路由的发布。

- 需要在 PE 上部署 MP-IBGP，并配置对端 PE 为对等体。
- 园区网内，一般不需要特别配置路由策略。
- 园区网中，路由数量有限，一般不需要部署 RR。
- 园区网内，路由安全性不是首要考虑因素，因此可以不部署路由的认证。

3.7 MPLS 规划

纵向虚拟化方案需要使用 MPLS L3VPN 技术来实现网络的逻辑划分和隔离，因此必须在部署 VPN 的区域部署 MPLS。

说明

对于 MPLS 的可靠性方面（例如快速收敛、故障检测、保护等）的规划，后面有专题描述，本节不再包含。

MPLS 域规划

MPLS 域的范围由划分 VPN 的 PE 节点位置决定（详细说明请见 VPN 规划）。

- 如果 PE 位置是在汇聚层，则 MPLS 域包含核心层设备和汇聚层设备。
- 如果 PE 位置是在核心层，则 MPLS 域只包含核心层设备。

MPLS 域中的每一台设备均需启用 MPLS 功能，LSR ID 建议设置为该设备的 Loopback0 接口的 IP 地址。

LSR ID 规划

使能 MPLS 的设备，需要配置 LSR ID。通常可以使用设备的某个 Loopback 地址作为 LSR ID（例如 Loopback0）。

LSP 规划

LSP 是每一个沿着从源端到终端的路径上的结点的标签序列。LSP 可以通过手动逐跳建立，也可以通过标签分发协议建立，如 LDP、RSVP 或者建于路由协议之上的一些协议，如 BGP 及 OSPF。

静态 LSP 的配置工作量巨大，扩展性不好，而且很容易引入认为操作错误，所以现在网络应用除非特殊情况，基本不会采用静态 LSP。

基于 RSVP 的 MPLS TE 隧道（CR-LSP）可以预留资源、保证带宽，同时可以提供高可靠性的保护措施。但是 RSVP-TE 对网络和设备的要求很高，一般运用在典型运营级的骨干网络之中。对于企业来说，通常不需要部署 MPLS TE。

因此，在企业中，推荐采用简单易部署的 LDP 协议来创建 LSP。

LDP 会话规划

如果采用 LDP 协议来创建 LSP，则需要进行对 LDP 会话进行规划。

在本方案中，不需要部署 VPWS 或者 VPLS，或者是 LDP over TE，所以不需要规划远端 LDP 会话。只需要在相邻的 LSR 之间（核心层设备之间、核心层和汇聚层设备之间）建立本地 LDP 会话。

3.8 VPN 规划

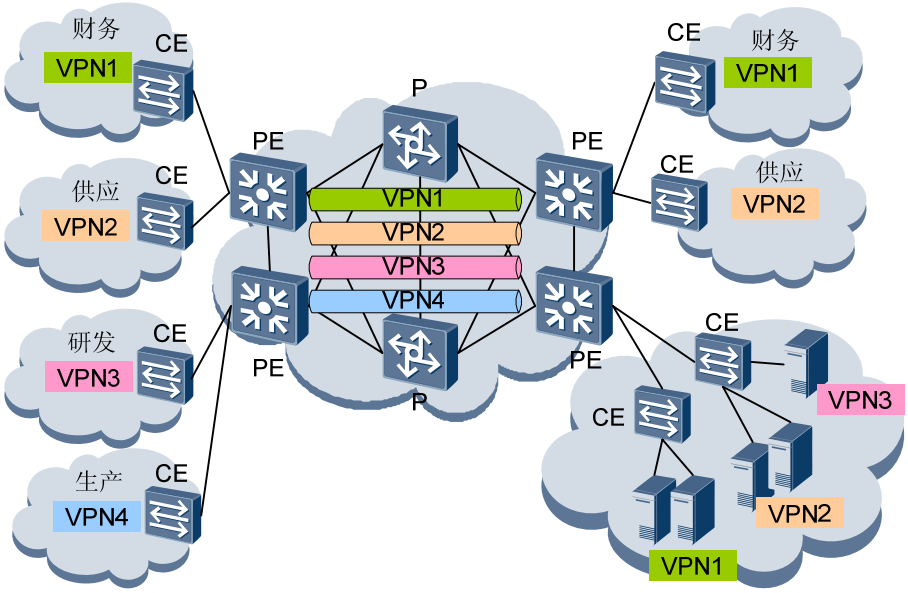
在纵向虚拟化方案中，最基本的部署是通过 MPLS L3VPN，划分不同的将不同部门的终端、服务器、网络资源等划分到不同的 VPN 中，实现业务的安全隔离。

另外，企业网络中划分了 VPN 之后，还需要考虑 VPN 用户的对外访问、外部分支/用户等接入 VPN 网络等方面的问题。

3.8.1 内网业务隔离

内网业务隔离的场景较为简单，通过标准的 MPLS L3VPN 即可实现。如图 3-1 所示。

图3-1 MPLS L3VPN 内网隔离



- 接入用户通过网络边缘的 CE 设备接入，通过固定配置或者策略服务器动态下发策略，将用户端口加入到相应的 VLAN 中，并配置或下发访问控制策略。
- 在接入或汇聚设备上，通过配置 VLAN 接口与 VPN 的绑定关系，把用户加入到相应的 VPN 中去。
- 服务器端根据应用和访问用户的不同，也把端口加入到相应的 VPN 中，并在 VPN 中传输业务数据。
- PE 设备会为每个 VPN 建立独立的路由转发表项，从而保证 VPN 内用户组的路由信息不会扩散给其它 VPN 用户，各 VPN 独立进行数据转发。
- 这样就为用户到服务器提供了一种端到端业务传输通道，把不同用户组、不同应用的数据横向隔离开来，完成了园区网的纵向虚拟化。

3.8.2 VPN 之间互访

当构建了 MPLS L3VPN 之后，通常情况下，VPN 用户只能访问本 VPN 内的其他用户或者网络资源，实现了业务的安全隔离。

但是在一些特殊的情况下，有可能需要实现不同 VPN 之间的互访。这种情况下，通过改变 VPN 实例所关联的 VPN Target 属性（Export Target 和 Import Target）设置，就可以实现不同 VPN 之间的路由发布和引入，实现不同 VPN 之间的灵活访问，从而实现多种 VPN 组网拓扑，如 Intranet、Extranet 和 Hub & Spoke。

关于这方面的描述，可以参考华为公司任意一款支持 MPLS L3VPN 的产品（例如 NE 系列路由器或 S9300 系列交换机）的 VPN 配置内容。本文不作详细描述。

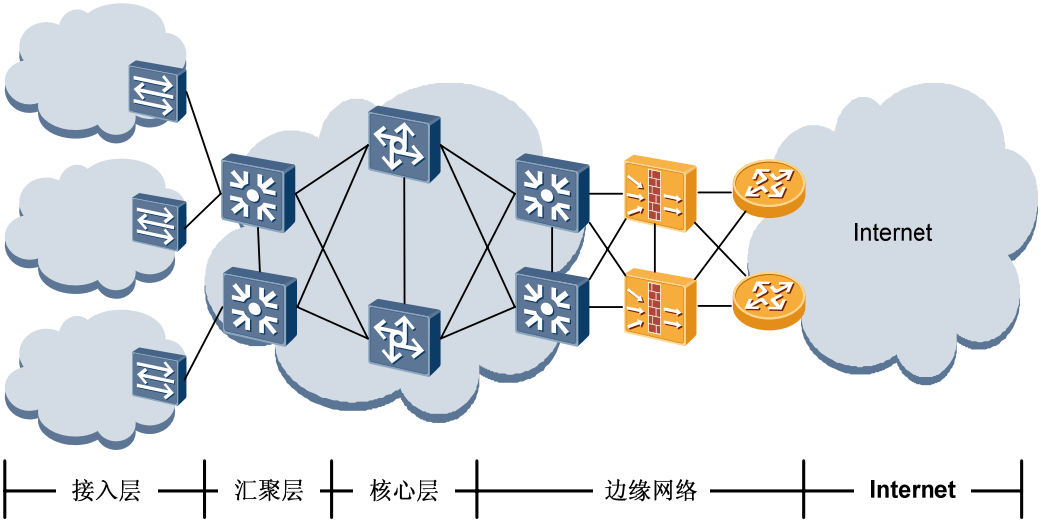
3.8.3 内部用户访问公网

在未部署纵向虚拟化方案之前，内部用户访问公网，首先通过园区网的核心层访问 Internet 边缘网络，然后再通过 Internet 出口路由器访问 Internet。由于 Internet 边缘网络直接连接 Internet，为了保障内部网络的安全，一般需要部署防火墙设备。

另外，由于 IPv4 地址的紧缺，所以在大型的园区网之中，内部一般都采用私网 IP 地址，因此当内部用户访问公网时，需要在边缘网络中部署 NAT 设备。NAT 可以是独立的设备，可以是集成在防火墙或者 Internet 出口路由器中的功能模块。

部署 NAT 和 FW 可以选用 S9300 的 FW 板卡，出口路由器可以选择 NE40E 系列的路由器或 AR 系列的接入路由器。

图3-2 非 VPN 内部用户访问公网



当企业内部网络以 MPLS L3VPN 形式进行纵向虚拟化之后，则需要增加考虑 VPN 用户对 Internet 的访问。

由于一般 VPN 的用户只能访问 VPN 内的资源，而普通的 Internet 属于 Public 资源，并不属于某个 VPN。而如果为每个 VPN 都构建一个属于指定 VPN 的 Internet 出口，无论从成本还是网络建设复杂度上来说，都是不现实的。

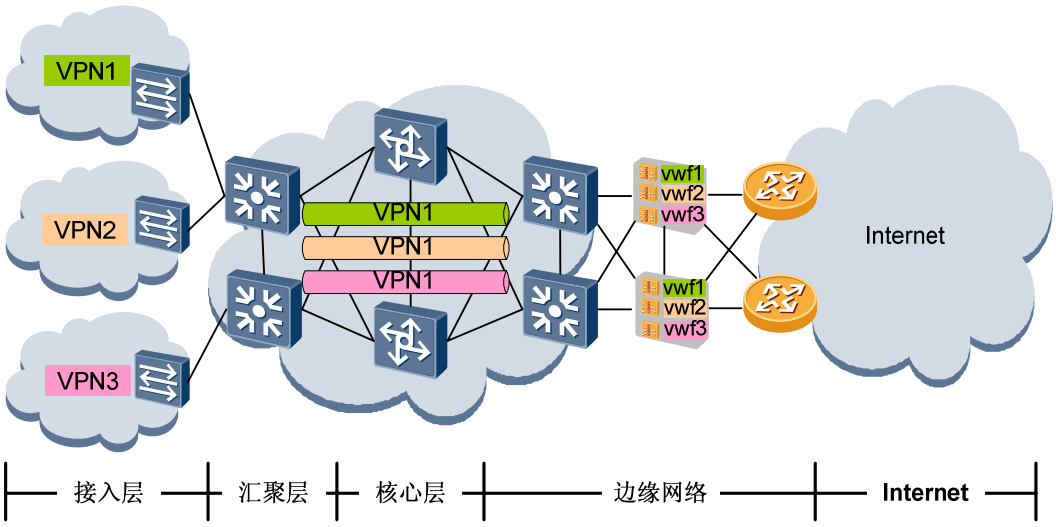
所以最佳的解决方案是所有的 VPN 都共享一个 Internet 出口，并且通过技术手段实现 VPN 用户对共享 Internet 出口的访问。这一般有两种方式：

- 通过在 VPN 内部署 Internet 网关服务器，并配置默认和静态路由的方式实现 VPN 到 Internet 的访问。这方面的部署可以参考华为公司任意一款支持 MPLS L3VPN 的产品（例如 NE 系列路由器或 S5700/S9300 等交换机）的 VPN 配置内容。

  这种方式是单纯基于 MPLS L3VPN 特点所衍生的访问方式，一方面成本很高，另一方面部署非常不灵活，对于企业来说，不建议采用。
- 通过在防火墙上部署虚拟防火墙（VPN 实例、安全实例和配置实例的综合体），实现与 VPN 的关联。相当于把一台防火墙虚拟化成多个防火墙，分别为每个 VPN 提供 Internet 出口服务，如所示。

  这种部署方式成本低廉，并且部署灵活，推荐使用。

图3-3 VPN 用户通过虚拟防火墙访问 Internet



3.8.4 分支机构访问园区网络

分支机构能不受约束地访问园区网的资源，我们可以将分支机构看成园区网的延伸。所以分支网络连接到园区网络一般不需要部署防火墙。分支网络一般是通过 WAN 接入到园区网的，但也有通过 Internet 接入到园区网的，如图 3-4 所示。

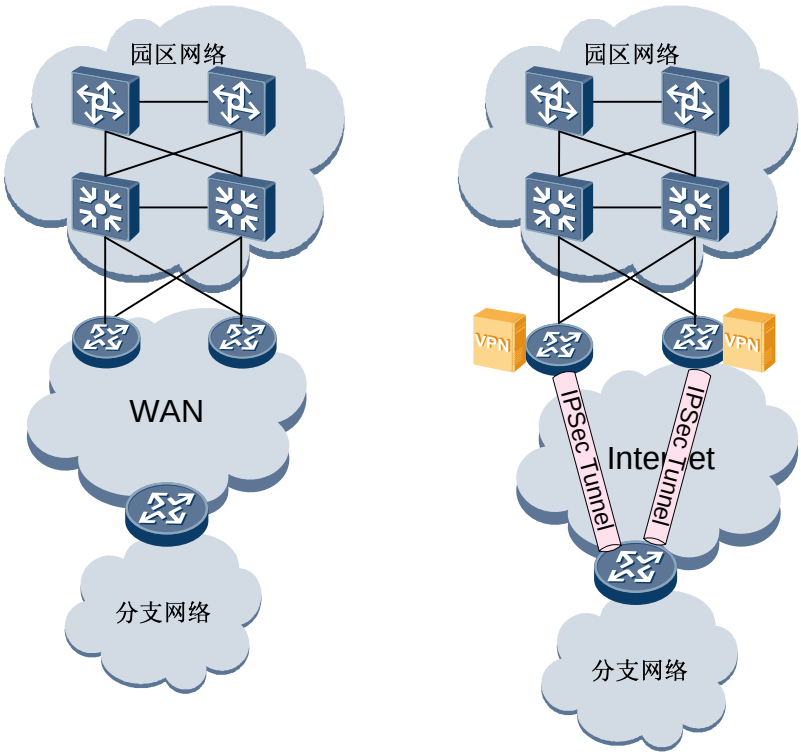
如果分支网络通过 Internet 接入园区网，则需要考虑安全加密的问题，通常可以通过 IPSec VPN 的方式接入。此时需要在园区的 Internet 出口处部署 VPN Server，负责用户的接入。

具体 VPN Server 的部署可以使用单独的 VPN Server 设备，或者防火墙上部署 Server 模块。单独的 VPN Server 设备可以旁挂在防火墙上，也可以旁挂在 Internet 边缘网络的汇聚交换机上。

说明

华为 AR 路由器产品支持 IPSec VPN 功能，用于分支网络和小型总部网络边缘，而在总部园区网中可使用 S9300/S9300 的增值业务卡（SPU 卡）作为 IPSec VPN 网关。

图3-4 分支结构接入园区网络



分支接入到园区网络一个比较普遍的问题就是用户的隔离问题。比如在总部，出于安全的考虑，可能通过 MPLS L3VPN 将一个物理网络虚拟化成几个逻辑网络使用。这样的需求相对较为复杂。通常可以考虑两种方案：

- 在分支机构部署 MPLS L3VPN。这种方式要求分支机构的设备支持 MPLS L3VPN，在大部份情况下，这一点可能无法满足。
- 在分支结构部署 MCE。这种方式也能满足隔离的要求。但是如果不同 MCE 如果需要互通，必须借助 MPLS L3VPN，这样只能在总部进行互通，会浪费 WAN 口带宽。

如果分支结构通过 Internet 接入园区网，也需要考虑用户的隔离问题，通常有以下两种解决方案：

- 通过部署多个 IPSec 隧道来解决。
- 通过部署多个 GRE over IPSec 隧道来解决。

3.8.5 远程用户访问园区网络

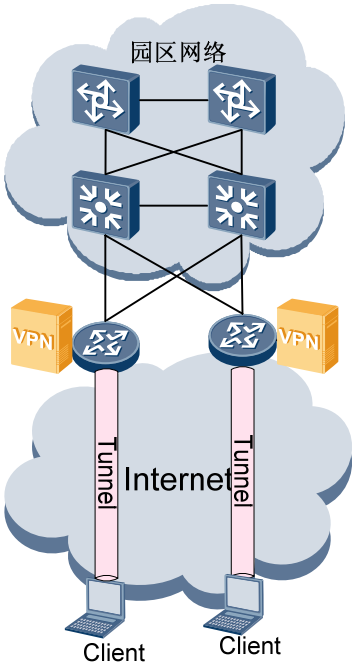
远程用户访问网络，很大程度上希望能和在园区完内部一样不受限制。

远程用户一般都是通过 Internet 接入到园区网的。此时用户的接入访问必须经过加密才行，目前远程用户访问园区网所使用的技术主要有两种：

- SSL VPN：主推荐的方案。
- L2TP VPN：次推荐的方案。

对于这两种方案，都需要在用户接入的边缘网络中部署 VPN Server，VPN Server 可以挂在 Internet 边缘网络的防火墙或者汇聚交换机上。如图 3-5 所示。

图3-5 远程用户接入园区网络



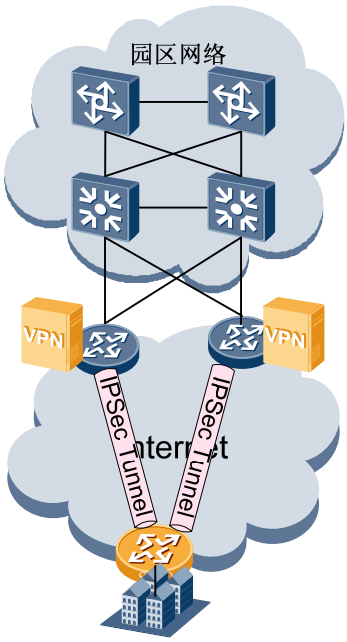
说明

对于 SSL VPN 而言，不需要专门的客户端软件，通过 Web 浏览器即可访问 VPN Server。而 L2TP VPN 则需要安装 L2TP 拨号软件。

3.8.6 SOHO 办公访问园区网络

SOHO 办公访问网络，很大程度上希望能和在园区完内部一样不受限制。而且一般都是通过 Internet 接入到园区网的。通过 Internet 接入到园区网必须经过加密， SOHO 办公访问园区网所使用的技术推荐使用 IPSec VPN。具体的部署方式和分支接入类似，请参考“3.8.4 分支机构访问园区网络”。

图3-6 SOHO 办公通过 IPSec VPN 接入园区



3.8.7 客户访问园区网络

外部客户能访问的网络区域就是平时常说的 DMZ。客户能访问的园区内部网络资源可能有 Web 服务器、Email 服务器、FTP 服务器等。这些服务器都会被部署在防火墙后面。这里有两种部署方式：

- 直接挂接在边缘网络的汇聚交换机上。如图 3-7 所示。
- 在数据中心专门划出一块 DMZ 区，放置这部分服务器，如图 3-8 所示。

图3-7 DMZ 区部署在边缘网络

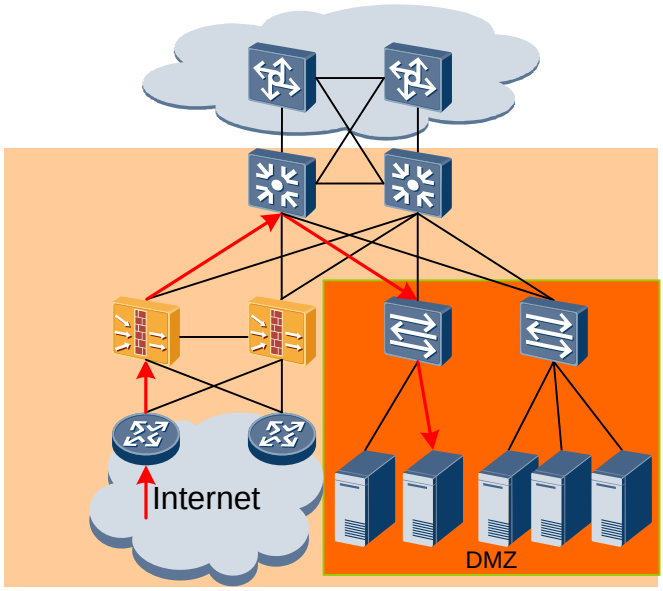
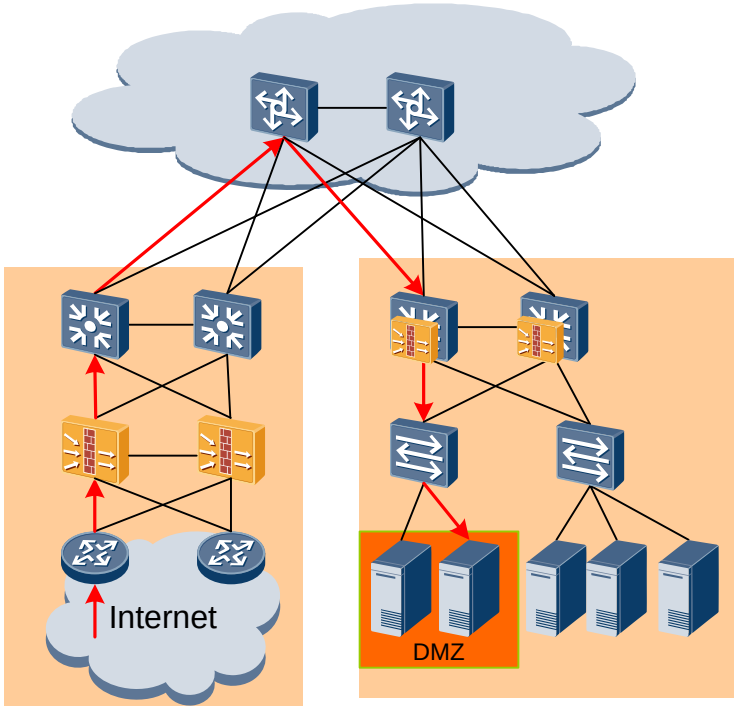


图3-8 DMZ 区部署在数据中心



DMZ 部署可以使用私网的 IP 地址，也可以使用公网的 IP 地址，如果使用私网的 IP 地址，那么外部用户访问需要经过 NAT，部署 NAT 和防火墙建议选用 S9300 的 FW 板卡，出口路由器可以选择 NE40E 系列的路由器或 AR 系列的接入路由器。

3.9 可靠性规划

说明

本节中的可靠性规划只描述了纵向虚拟化方案中相关的可靠性方案，园区网中非虚拟化方案方面的可靠性规划，请参见《园区网技术建议书》。

3.9.1 IGP 可靠性规划

对于企业园区网来说，IGP 通常有 OSPF 和 IS-IS 两种选择，下面分别对其可靠性的规划给出建议。

OSPF 协议可靠性

建议配置 OSPF 快速收敛功能，包括如下几项特性：

- BFD For OSPF：用于对链路故障进行快速检测。
- PRC（Partial Route Calculation）：可加快 OSPF 的路由收敛速度。
- 智能定时器：可加快路由收敛，增强网络稳定性。

IS-IS 协议可靠性

建议配置 IS-IS 快速收敛功能，包括如下几项特性：

- BFD For IS-IS：用于对链路故障进行快速检测。
- ISPF（Incremental SPF）：可加快 IS-IS 的路由收敛速度。
- PRC（Partial Route Calculation）：可加快 IS-IS 的路由收敛速度。
- LSP 快速泛洪：可加快 LSDB 同步的速度。
- 智能定时器：可加快路由收敛，增强网络稳定性。

其中 ISPF 和 PRC 是系统默认特性，无需配置，其余特性需要配置。

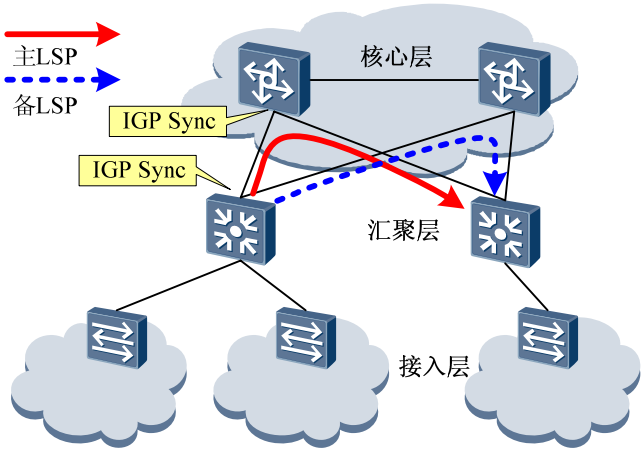
3.9.2 MPLS 可靠性规划

如果采用 LDP LSP 作为 VPN 的承载隧道，则需要在 LDP 协议上部署可靠性措施。

对于企业网来说，LDP 协议的可靠性建议如下：

- 如果 LSP 有主备路径（例如汇聚层设备双归接入核心层设备），则建议在主 LSP 的分叉节点和对端配置 LDP 和 IGP 同步功能。防止主备流量切换时，由于 IGP 收敛快于 LDP，导致流量丢失的问题。如图 3-9 所示。

图3-9 LDP 和 IGP 同步功能



- 在 LDP LSP 的故障检测方面，动态 BFD 可以提供 ms 级的快速故障检测，并且降低手工配置工作量，推荐在 LSP 两端配置动态 BFD 来检测 LDP LSP。
- 如果 LSP 有主备路径，如图 3-9 所示。则推荐在 LSP 的入节点上配置 LDP Auto FRR 功能，自动建立备份 LSP，可以在出现故障时流量的快速切换，减少流量丢失。

另外，如果 LSR 是双主控的配置，则可以考虑在 LSR 上部署 LDP GR 功能，保证在 LSR 的主备倒换或者软件升级过程中，MPLS 转发不会中断。

4 产品建议

对于虚拟园区网方案所涉及的各节点和网元，华为公司推荐使用的产品如下：

表4-1 部件产品建议表

部件	产品/型号
接入交换机	S5700、S3700、S2700
汇聚交换机	S9300、S5700
核心交换机	S12800、S9300
WLAN AC	S9300 AC 插卡
边缘路由器	AR3200、NE40E
防火墙	S9300 FW 插卡
网管	iTec 专业版