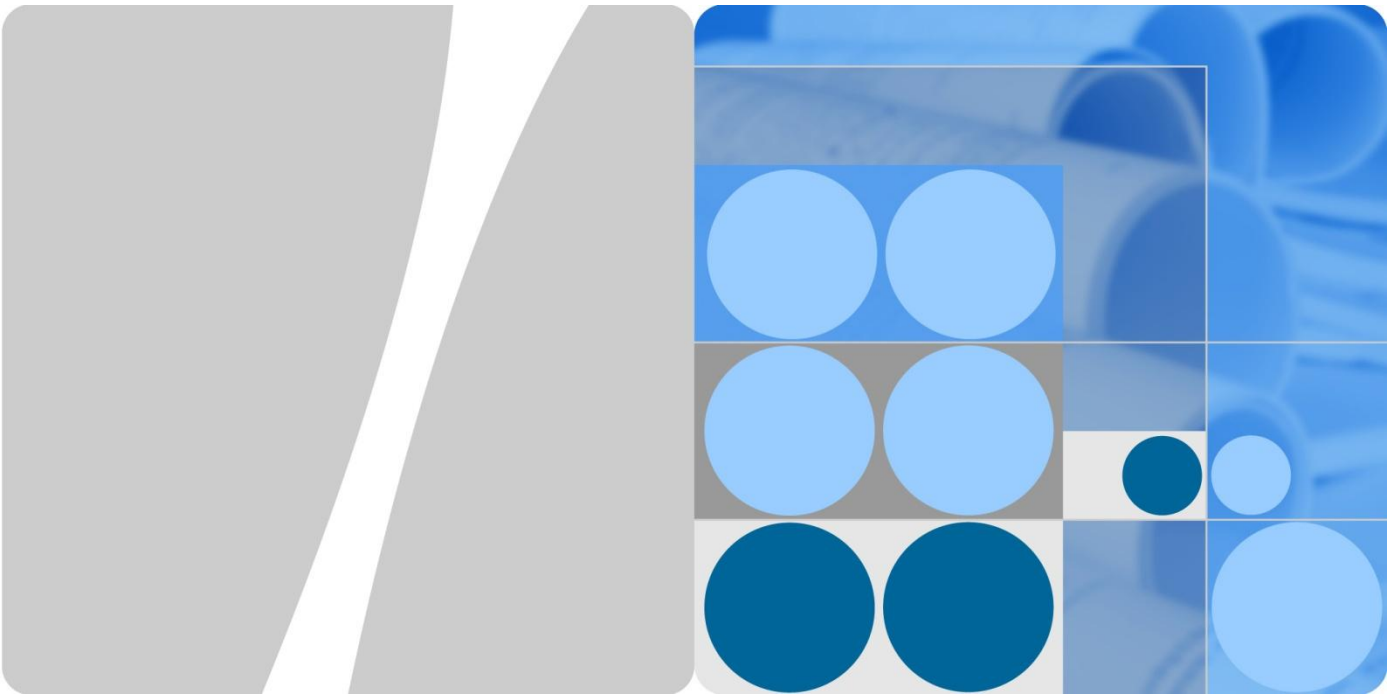
资料编码



广域互联方案

技术建议书

文档版本 01

发布日期 2011-07-12

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： 0755-28560000 4008302118

客户服务传真： 0755-28560111

目 录

1 广域互联概述

1.1 广域互联面临的挑战

随着企业信息化的建设及企业网络建设的纵深化，对于跨地区的广域网互联需求在不断扩大，企业的生产业务系统、经营管理系统、办公自动化系统均在大力发展，这些业务的发展对于企业广域网互联的建设要求越来越高。目前广域网互联面临如下挑战：

- 如何在一张 IP 承载网上承载企业的多种业务
- 如何保证 IP 承载网的高可靠性
- 如何保障 IP 承载网的安全性
- 如何保证 IP 承载网的可维护可管理

1.1.1 多业务承载

企业内部存在多种业务：

- 从实时性来说，可分为实时业务、非实时业务。
- 从重要性来说，可分为关键业务、非关键业务。
- 从业务类型来说，可分为语言业务、数据业务和视频业务等。

这些业务对 QoS 的要求也是不一样的，比如关键业务要求快速转发对带宽要求不高，比如办公的数据业务对时延要求不高，但有一定的带宽要求，如何在一张广域网上去承载所有的这些业务是构建 IP 承载网的关键。

1.1.2 高可靠性

部分大行业开展的业务对可靠性的要求比电信运营还要高，很多关系到民生工程，所以要求 IP 承载网必须具备 99.999%的可靠性，确保业务不中断，这就要求 IP 承载网络必须要消除单设备故障，单链路故障，及实现 200ms 的端到端倒换技术。

1.1.3 安全性

电子政务内网、石油、国电、银行等大行业的网络对安全性有很高的要求，不管是从网络内部的安全还是网络外部的安全都必须要防范，特别是 IP 网络的开放性决定的其相对传统网络更易受到攻击，所以如何保障这张 IP 承载网的安全性成了关键点。

1.1.4 易维护性

随着业务的扩充导致的网络扩展，使得网络的维护越来越复杂，需要非常专业的 IP 维护人员，这对于非通信专业的用户来说是一个很大的挑战，所以 IP 广域网互联方案必须具备完善的可维护性，包括可视化管理、简单管理、统一管理等等。

1.2 广域网主要需求

1.2.1 业务 QoS 需求

广域网 QoS 概述

传统的 IP 网络只能采用尽力而为（Best Effort）的方式进行包的转发，它只在能力范围内尽可能快地传送，对吞吐量、延迟、延迟抖动和丢包率没有任何保障，而把传输损失都留给终端系统来处理。由于没有 CAC 机制，很容易出现带宽过载导致大量用户质量下降，其采用的非连接机制/动态路由协议会造成很大的瞬时抖动。因此，传统 IP 网几乎没有端到端 QoS 保障能力。

随着 IP 网络上需求的不断变化，各种新型的实时性电信业务如 3G、VoIP、IPTV 等都要求 IP 广域网能提供高质量的端到端的 QoS 保障。传统的 IP 网络的尽力服务已不能满足应用的需要。

而且在 IP 网络上承载的各种业务的 QoS 需求也是不同的。比如 Email 和 FTP 对时间延迟并不敏感，但是对于 VoIP 业务，报文传送如果延时太长，将是用户所不能接受的。提供区别服务是保证所有应用数据流依据各自所提供的功能获得所需服务层次的关键。

QoS 就是针对各种不同的需求，提供不同的、可预测的服务质量的能力。可用性、延迟、抖动以及丢包率是衡量 IP 网络 SLA 的四个技术标准。

- 可用性（Availability）：指用户能够使用业务的时间占业务全部工作时间的百分数。在连续 5 分钟内，如果一个 IP 网所提供业务的丢包率≤5%，则认为该时间段是可用的，否则是不可用的。
- 延迟（Latency）：指在两个参考点间某一 IP 包从发送到接收之间的时间间隔。
- 抖动（Jitter）：指不同分组之间在延迟上的偏差。
- 丢包率（Packet loss）：指在两个参考点间传输时丢失的 IP 包数与已发送的 IP 包总数的比值。丢包主要是由网络拥塞引起的。

不同的用户及业务对 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，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。

IP 广域网 QoS 建设目标

IP 广域网建设应能满足各种电信业务及信令的 QoS 要求。目前，IP 广域网承载的主要业务中对于 QoS 要求较高的是企业实时关键业务，因此 IP 广域网 QoS 建设目标是满足企业多业务统一承载及实时业务的 QoS 的综合要求。

ITU-T 对 IP 广域网的 QoS 推荐值如所示。

表1-1 IP 广域网 QoS 建设目标

应用类型	典型业务	延迟（E2E 单向）	Jitter（E2E 单向）	丢包率（E2E 单向）	带宽
Real Time Voice/Video	VoIP Video Phone	150ms	20ms	0.1%	Guarantee
Real Time Data	Signaling	150ms	N/A	0.1%	Guarantee
Streaming Multi Media	IPTV/VoD	1000ms	N/A	0.1%	Guarantee
Normal Data	Internet Access	N/A	N/A	N/A	Self Adapt

1. 对于抖动值，考虑到低速链路，ITU-T 推荐是 50ms，对于大多数用户来说，真实抖动需求是 20ms。

2. 以上数据来自 ITU-T Y.1541，是 ITU-T 的推荐值。端到端的距离小于 5000km。

IP 广域网建设目标在实际的解决方案中，应避免完全依靠技术手段来解决 QoS 问题，要贯彻 IP 电信网建设思路，从话务模型综合分析，网络设计，服务质量保证技术和可靠性提升等各个方面综合考虑，以达到广域网 QoS 建设目标。

1.2.2 业务可靠性需求

随着 IP 广域网的业务种类不断增多，业务的重要性不断增加，业务对网络质量的敏感性不断加强，不仅仅要求网络出现故障后能够恢复，对网络恢复的时间也有很高的要求。IP 广域网规划必须要满足企业实时、非实时，关键、非关键业务的要求，以确保业务实施的可靠性。

IP 广域网的可靠性一般包括三个方面：

- 设备的可靠性
- 网络的可靠性
- 故障保护倒换时间

传统 IP 网络尽管有动态协议、冗余连接等可靠性技术，但是其程度远没有达到电信级要求，从可靠性的指标看，一个普通的 IP 网络故障，将导致业务中断几秒到分钟量级，这种指标可以满足传统 Internet 业务承载要求，但是无法满足实时话音、视频业务的服务质量需求。

电信级业务对于承载网可靠性要求为：

- 网络设备的可用性达到 99.999%
- 网络的可用性达到 99.999%
- 故障保护倒换时间：骨干网推荐链路保护小于 50ms（达到 SDH 要求）
- 网络设备的关键部件冗余，接口板件支持热插拔

- 关键的节点采用双节点冗余备份
- 关键的链路采用双归属链路

1.2.3 业务安全性需求

传统的IP网主要承载Internet互联业务，由于其是一个完全开放的网络，大量病毒泛滥，非法攻击和恶意的业务盗用情况非常普遍，很难保障业务的安全性。

而下一代的IP广域网将会承载各种实时的关键的业务，这些业务对于网络的安全性要求非常高。因此，安全性问题是网络规划时必须解决的问题。安全性主要包括一下三个方面的内容：

- 保密性：只有发信者想要的收信方才能识别通信内容。
- 数据完整一致性：信息在收发双方间传送过程中不被第三方修改。
- 业务可用性：通过防范对网络的各类恶意攻击来保障业务可用性。

要想提高业务的安全性，使其达到电信级的要求，IP广域网必须要满足以下几点要求 ：

- 业务安全隔离：物理网络隔离，或者单一的物理承载网实现基于业务的逻辑网络，逻辑网络之间以及逻辑网络到基础网络任何情况下没有泄漏；
- 逻辑网络内部：承载网提供安全防范手段保护逻辑网络内部关键系统安全，防止业务盗用；
- 基础网络可靠性：承载网基础网络（设备）能够有效防范各种非法攻击和病毒冲击，保证网络持续稳定运行，且性能不会劣化。

1.2.4 业务可运营可管理要求

IP网络具有承载网和业务网双重属性。传统的IP网络过多地注重了开放性，忽视了其可管理性。随着广域网中业务全面IP化的发展趋势，要求IP网能够承载更多更丰富的企业级业务，必然要求其能够为客户提供一套方便的网络业务运营管理手段。

所谓可管理，不仅仅指通常意义上的网络设备管理，更重要的是对于业务的管理能力，其中包括对于用户的管理能力、业务质量的管理能力、业务安全性的管理能力等等。这些业务管理功能如果仅仅体现在BSS/OSS中的一个模块上，而没有在网络设备和网络结构上加以考虑，是不可能实现的。因此，IP广域网的规划必须要考虑承载网具备开展各种灵活的用户管理、业务管理和安全性管理能力。

2 广域互联规划建议

2.1 广域网组网原则

2.1.1 建网模式

对于大型企业而言，在向 ALL IP 承载网的转型过程中，华为公司推荐客户新建一张 IP 广域网。具体建网过程请参考如下原则：

- 网络结构层次化

  网络结构分为三层，包括核心层、骨干层和业务接入层。二三层网络分离，构建物理和逻辑层次清晰的三层路由骨干网和二层城域网。

- 网络结构扁平化

  采用大容量设备，少节点，广覆盖，减少物理和逻辑级联数。

- 业务接入层采用二层的 Metro Ethernet 网络组网

  在业务接入层采用二层的 Metro Ethernet 网络。Metro Ethernet 采用 RPR/RRPP 环形组网，以节约光纤和提高可靠性。

- 关键节点和链路冗余备份

  对于业务量大的重要节点，采用双设备冗余。下层到上层链路采用双归属。

2.1.2 网络架构设计原则

网络拓扑设置原则

根据广域网互联设计原则，整个网络所有节点位于一个自治域内，采用扁平化组网原则，总体网络拓扑设计原则如下：

- 采用分层组网设计，分核心层、骨干层和业务接入层。
- 同层内尽量多互连，关键节点考虑多设备冗余。
- 下层双归或是多归到上层单点多设备或是多点设备。
- 局部根据业务流量情况适当调整。

核心节点设计原则

核心层设备可以组成网状网、半网状网或者 RPR 环网，骨干层设备通过双归属到核心层设备。核心节点的设置原则如下：

- 节点现有业务量现状和预测规模处于前列。
- 节点的传送资源丰富，处于传送干线交汇节点。
- 节点的地理位置是中心城市，具有区域辐射力。
- 核心节点原则上全连接。
- 根据业务量和传送资源情况不全连接，采用半连接。
- 根据可靠性保护要求和节约光纤要求采用 RPR 环网技术。
- 根据骨干层组网情况，核心单接点可以部署多设备。
- 两点之间流量大，确保一跳可达。
- 两点之间流量较小，可以考虑多跳可达。
- 传送距离对时延影响很大，少绕路。

骨干层设计原则

骨干层用来完成用户流量的汇聚，同时完成业务的汇聚，避免大量的接入层设备直接接入核心层。骨干层的设计原则如下：

- 根据流量流向的预测，以主要业务量城市（一般为区域中心城市）为中心设置骨干节点，充分考虑网络结构的优化，可以跨越行政区域的限制。
- 根据城市的大小和业务量可以设置多个骨干节点。
- 在设置了核心节点的城市，骨干节点可以视情况和核心节点合设。
- 根据骨干节点和核心节点之间的链路可靠性情况，还有核心接点的可靠性情况，可以让骨干节点分别连到不同的核心节点。
- 根据骨干节点间的流量大小情况，可以考虑直接在流量较大的汇聚之间增加链路疏导流量。

业务接入节点设计原则

业务接入层由二层的 Metro Ethernet 网络构成。Metro Ethernet 网络由以太网交换机组成，有以下设置原则：

- 为节约光纤和提高可靠性，采用 RPR/RRPP 环来组网。
- 在人口密集地区，采用一层环来组网：
  - 每个 PoP 点设置 1～3 个 AGG-Ring。
  - 每个 AGG-Ring 设置 4～8 台 UPE 设备。
  - 每个 UPE 设备设置 3～10 个 DSLAM。
- 在人口稀疏地区，为节约光纤，采用两层环来组网。
  - 每个 AGG-Ring 设置 3～10 个 ACC-Ring。
  - 每个 ACC-Ring 设置 4～8 台 UPE 设备。
  - 每个 UPE 设备设置 3～10 个 DSLAM。

流量承载原则

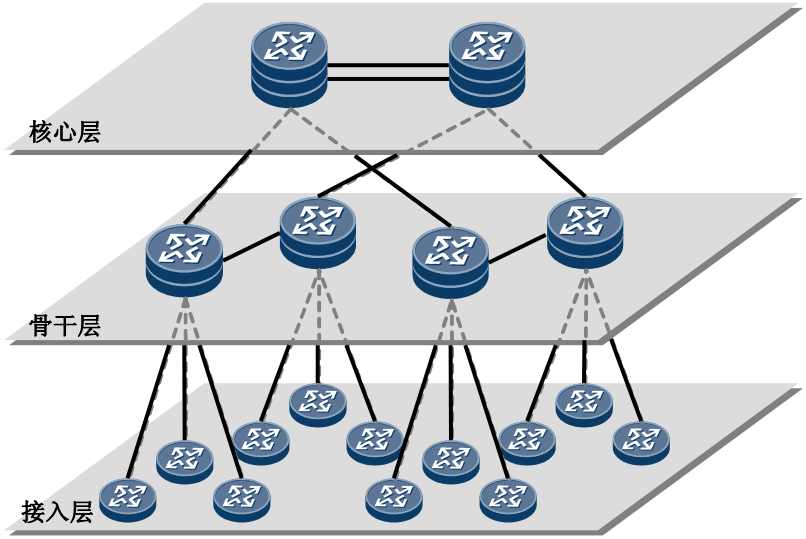
通过规划整网的链路 METRIC，可以科学的疏导整网的业务流量，建议流量疏导遵循以下原则：

- 路径角度：跳数≤最小跳数＋2。
- 分担角度：流量分担合理，且避开压力大的路径，例如：PoP 节点间流量不经过接入节点；节点内部流量不经过其他节点；宁可下层穿透，避免上层穿透。
- 备份角度：合理备份（备份路径大多数情况下也较短；尽可能通过压力小的节点和链路），PoP 节点间若连接全部中断，则其间流量应通过核心转发，而不是接入节点；PoP 节点内部若某台设备上联发生故障，则流量应经过同节点的另一台设备而不是其他节点。
- 分析和调整角度：对特定目的地，路径尽量是明确、便于分析和调整的。

2.1.3 广域网分层组网原则

广域网分为核心层、骨干层和业务接入层，如图 2-1 所示。

图2-1 广域网网络架构



核心层组网原则

核心层部分根据用户业务量、光纤资源情况等客观条件，可以采用全连接/半连接或者 RPR 环网的方式，并应该按照项目实际情况，进行部分结构混合式设计。

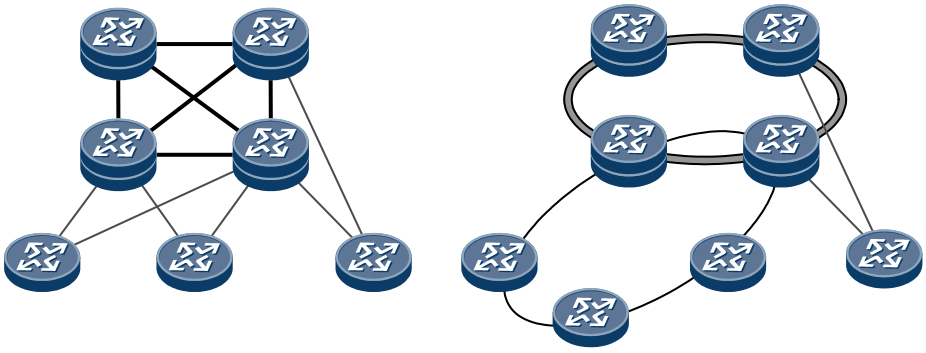
全连接方案中，核心层的任意两节点直接设置直连链路，同时支持链路捆绑，能够在两节点之间提供巨大的带宽能力，且具备向更高带宽扩展的能力。但是节点全连接需要大量的光纤资源，会造成网络的整体成本明显上升。建议业务量巨大、光纤资源丰富的企业采用这种方案。同时，可以根据实际项目情况采用部分全连接方式组网，以降低光纤资源的需求。

RPR 方案是一种先进的逆向双环组网方案，能够极大的节省光纤资源，提供 50ms 级的保护倒换能力，同时提供大量的先进特性，便于网络的部署实施以运营时的维护管理。

但是当前 RPR 技术只支持 10G 的接口，并且不支持链路捆绑，从而限制了 RPR 的扩展能力。对于海外企业，应该根据实际情况，在业务流量能够满足时，采用 RPR 组网。

我们可以结合两种方案的优势，以 RPR 组网为基础，当环上两节点间流量巨大时，在这两节点间设置直连链路，保证大容量提供。从而既节省了光纤资源，提供了高可靠性，又能够满足部分节点间高带宽需求。

图2-2 Full Mash and RPR Ring



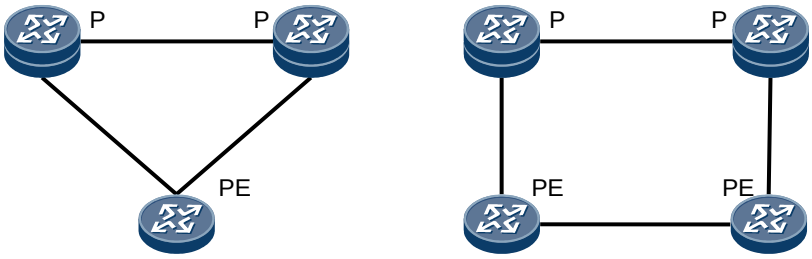
Full Mesh结构　　RPR环结构

骨干层组网原则

骨干层有两种组网模型，如图 2-3 所示。

- 模型一：只采用一台 PE 设备，PE 双归属到 P 设备上。
- 模型二：在一个 PoP 节点设置 2 台 PE 设备，用于冗余备份；每个 PE 设备连到一台 P 设备上，即一个骨干节点有 2 个链路连到 P 设备上。

图2-3 骨干网的两种组网模型

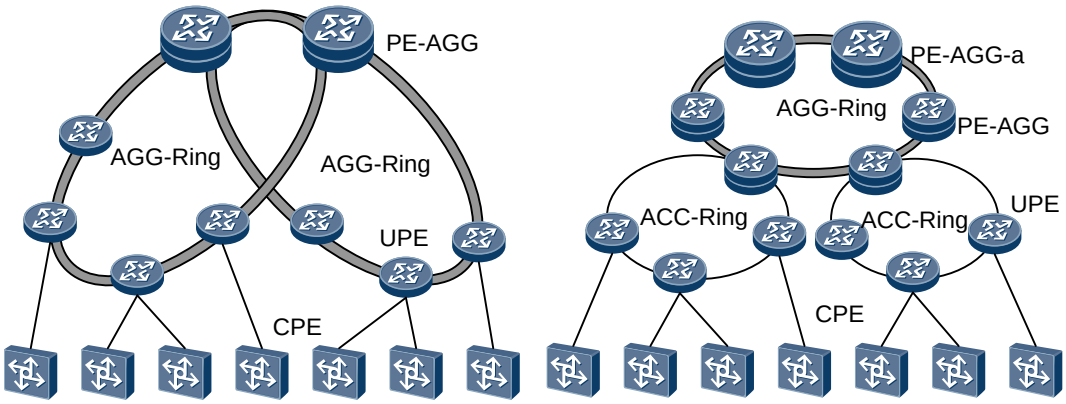


业务接入层组网原则

从接入的数量和设备的性能考虑，业务接入层的建网原则如下：

- 在业务密集的地域，站点相对集中，一般采用一层环网即可。
- 在业务稀疏的地域，站点相对分散，由于地理范围的因素可以采用二层环网。

图2-4 业务密集模式和业务稀疏模式的网络架构



2.2 IP 地址规划

2.2.1 IP 地址分配原则

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，将对城域网的可用性、可靠性与有效性产生显著影响，应充分考虑本地网对 IP 地址的需求，以满足未来业务发展对 IP 地址的需求。城域网 IP 地址规划遵循以下原则：

- IP 地址的规划与划分应该考虑到城域网业务的飞速发展，能够满足未来发展的需要；既要满足工程现状对 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 地址的分配需要有足够的灵活性，能够满足各种用户接入如拨号、专线用户等的需要。
- 地址分配是由业务驱动的，按照业务量的大小分配各地的地址段。
- IP 地址的分配必须采用 VLSM 技术，保证 IP 地址的利用效率。
- 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。
- 采用公有与私有、动态与静态相结合的混合地址分配方式，以缓解目前 IP 地址资源严重不足的压力。
- IP 地址的规划应尽可能和网络层次相对应，采用自顶向下的分配原则，同时应充分体现分层管理的思想。
- 充分合理利用已申请的地址空间，提高地址的利用效率。

2.2.2 IP 地址详细规划

公私地址混合

为了节省 IP 地址的使用和降低成本，应在城域网内采用公有和私有相结合的混合地址分配方式。

- 城域网内公有地址和私有地址完全混合使用，内部公有地址和私有地址之间不做地址转换，城域网的路由设备不区分公有/私有地址，同时支持公有/私有地址路由。
- 网络出口采用混合地址交换路由器进行地址转换，仅仅对私有地址数据报文进行地址转换，公有地址报文正常路由转发。
- 对于私有 IP 地址也应做统一规划，以免今后造成混乱。

自顶向下分层分配

- 根据网络结构、Area、地域划分及区域内用户数量等，把整个城域网划分为几个大区域。
- 大区域内又分为几个子区域。
- 每个区域从它的上一级区域里获取（子网段）。
- 考虑到网络的扩展性，应采用从两端向中间扩展的方式来分配地址。

这种方式充分考虑了网络层次和路由协议的规划，通过聚合网络减少网络中路由的数目和地址维护的数量，充分体现了分层管理的思想。

私有地址分配

以下情况通常配置私有地址：

- 小区用户通常分配私有地址，应该以 C 类地址为单位，分配几个连续的 IP 地址（便于聚合）。
- IP 语音和视频用户，由 FANAVA 在全国范围内统一分配私有 IP 地址，并做好今后几年 IP 地址的预留，在软交换系统中保存用户号码和私有 IP 地址以及媒体网关。接入网关公有 IP 地址对应关系，以便在呼叫接续时可以准确的路由到用户终端。
- VPN 用户主要是企业内部用的地址，其所需的 IP 地址采用私有 IP 地址来予以解决。

公有地址分配

以下设备分配公有地址，保证本地用户和本地以外的 Internet 用户都能够访问本地服务器，而不受 NAT 的限制。

- Internet 上的主机，如 IDC 里需要对 Internet 开放的 Web、FTP、MAIL 服务器等。
- 城域网的关口设备，需要使用公有地址连接 Internet。
- 需要对外广播的路径上的设备，如城域网同时连接到两个 AS，使用域间路由协议 BGP，而城域网作为中间 AS，则可能需要把 AS 出口间的路径向 Internet 上广播，这时路径的地址需要公有 IP 地址。
- 企业用户 NAT 用公有地址，企业内部一般已经采用私有地址建立内部网，并通过 NAT 设备接入 Internet。给企业分配公有地址可以不影响企业的地址规划。
- 用户通过 ADSL 或 FTTX+LAN 等宽带方式上网用公有 IP 地址。一般建议一个小区内 40 到 100 个用户分配 1 个公有 IP 地址，如果可以作 TCP 端口映射则一个 IP 地址可以支持更多用户。
- 用户通过窄带拨号方式上网需分配公有 IP 地址，一般给每个 RAS 端口分配一个公有 IP 地址。
- 专线用户上网用公有 IP 地址。一般一个用户分配一个公有 IP 地址。

NAT 设备部署

对于中、小规模的城市，建议将实现 NAT 功能和混合地址交换功能的设备设置在网络核心层，以降低设备投资，增强网络的可管理性。

对于大型城市，可考虑将该功能向汇聚层或接入层转移，以减轻核心层设备的压力。

地址冗余

在地址规划时，需考虑 50％～80％的 IP 地址冗余。

2.2.3 NGN 私网地址穿越

对于 IP 广域网，其承载的大量企业网和驻地网基本都采用私有 IP 地址通过出口的 NAT/FW 接入公网。而目前 IP 广域网中，如 H.323、SIP、MGCP、H248 等在 IP 上承载语音和视频的协议的控制通道或媒体通道在私网用户接入应用中难以穿越传统的 NAT/FW 设备与公网进行互通，或者说目前的 NAT/FW 大多支持 HTTP 的数据应用协议穿透，而无法支持会话业务的控制与媒体 NAT/FW 穿透。

而 NGN 网络最大的好处就是能为用户提供丰富的业务，特别是为企业用户提供语音、数据、视频融合的 IP Centrex 业务，因此上述问题正成为 NGN 网络业务开展最大的障碍。目前业界的解决方案有：

- NAT/ALG 方式（Network Address Translation / Application Layer Gateway）
- MIDCOM 方式（Middle box Communication）
- STUN 方式（Simple Traversal of UDP Through Network Address Translators）
- TURN 方式（Traversal Using Relay NAT）
- Full Proxy 方式（Signal proxy + Media relay）

四种方式的对比如表 2-1 所示。

表2-1 NGN 私网穿越方式对比表

项目	ALG	MIDCOM	STUN	TURN	FULL Proxy
性能	NAT 设备需要对所有包进行动态监控和解析，将极大增加 NAT 设备的负担。	NAT 设备不需要对包进行动态监控，只需要接收从 MIDCOM Agent 来的指令，基本不会增加 NAT 设备的负担。	NAT 设备不需要解析报文，不会增加 NAT 设备的负担，性能较好。	NAT 设备不需要解析报文，不会增加 NAT 设备的负担，性能较好。	Full PROXY 对所有呼叫报文和媒体流进行定向转发，效率要求较高，但只对会话类报文进行处理，不处理数据类业务。
可扩展性	每增加一种协议，需要升级 NAT 设备，可扩展性差。	Agent 上进行协议开发。	只支持 UDP 承载的协议，新的基于 UDP 承载的协议不要求对 NAT 设备升级。	可扩展性最好。	PROXY 上进行新协议的扩展。

项目	ALG	MIDCOM	STUN	TURN	FULL Proxy
组网应用	小区/企业网，规模不能太大。	小区/企业网/互通网关，视NAT 设备效率而定。	小区/企业网	小区/企业网	组网最灵活，小区/企业网/互通网关/其它各种 NGN 组网应用场合。
对现有设备改造	需要对NAT 设备升级，开发成本高。	需要对 NAT 设备升级支持 MIDCOM 协议，呼叫代理支持 MIDCOM 协议。	需要提供 STUN Server，同时终端需要支持 STUN Client 功能。	需要提供 TURN Server，同时终端需要支持 TURN Client功能。	提供 Full Proxy 设备即可，其他设备无需修改。
安全性	比较高	高	低	低	最高
QoS	无保证	有保证	无保证	无保证	有保证

根据上面的方案介绍和对比分析，推荐采用 Full Proxy 和 MIDCOM 两种解决方案，其它解决方案根据实际情况配合使用。

- Full Proxy 方式由于不用对现有网络设备进行任何改造，具有很强的适应性，组网灵活，可满足 NGN 网络初期多样化的组网和用户接入。除了解决 NAT 问题外，功能可以大大扩展，同时可完成在接入层实现对会话业务 QoS 和安全的处理，可以发展成为 NGN 网络的用户接入平台。
- MIDCOM 方式具有很强的扩展性，一旦 NAT/FW 设备支持 MIDCOM 协议，MIDCOM Agent 可内嵌于软交换中，可一劳永逸的解决 NGN 业务的 NAT/FW 穿透问题，同时由于软交换自身对用户呼叫协议的解析与处理，同样能动态下发呼叫的 QoS 和安全信息，下层的 Middle box（NAT/FW）设备根据这些信息采取必要的保证措施。

2.3 路由规划

2.3.1 关于跨域业务的规划

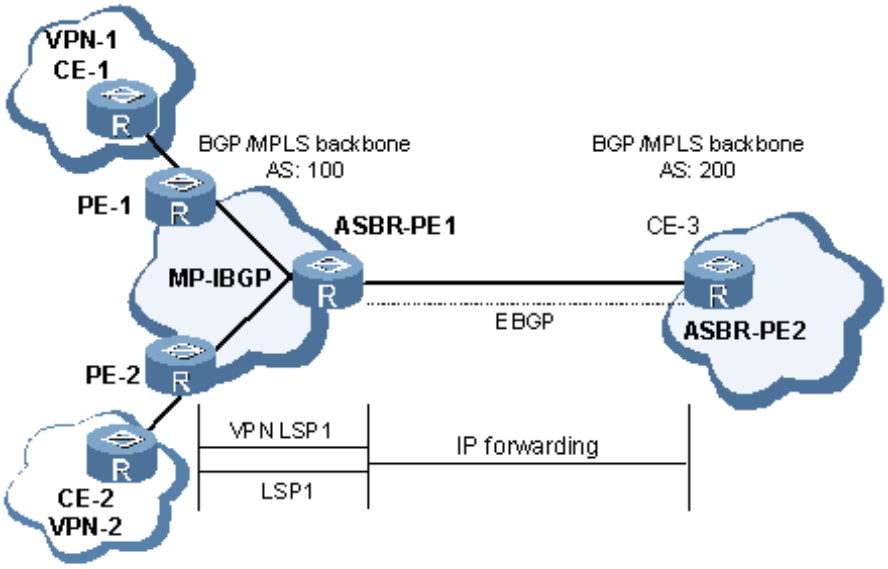
如果需要进行 MPLS VPN 的跨域构建（这种情况比较少见），由于 L3 MPLS VPN 路由是通过 BGP 携带的，有三种方式解决跨域问题：

- VRF to VRF 方式
- EBGP 方式
- Multi-hop BGP 方式。

VRF-to-VRF 方式

VRF-to-VRF 方式实际是基本 BGP/MPLS IP VPN 在跨域环境下的应用，不需要专门配置。这种方式下，两个 AS 的边界路由器 ASBR 直接相连，ASBR 同时也是各自所在自治系统的 PE。两个 ASBR 都把对端 ASBR 看作自己的 CE 设备，使用 EBGP 方式向对端发布 IPv4 路由。如图 2-5 所示。

图2-5 ASBR 间使用 VRF-to-VRF 方式管理 VPN 路由组网图



在图 2-5 中，对于 AS100 的 ASBR-PE1 来说，AS200 的 ASBR-2 只是它的一台 CE 设备。同样，对于 ASBR-PE2，ASBR-PE1 也只是一台接入的 CE 设备。

VRF-to-VRF 方式实现跨域 VPN 的优点是简单。两个作为 ASBR 的 PE 之间不需要为跨域进行特殊配置。

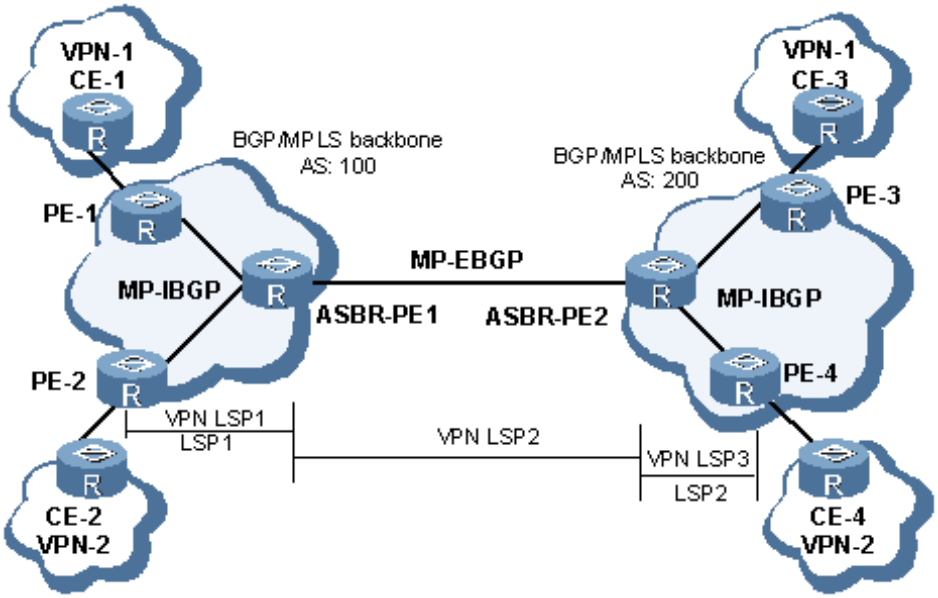
缺点是可扩展性差。作为 ASBR 的 PE 需要管理所有 VPN 路由，为每个 VPN 创建 VPN 实例。这将导致 PE 上的 VPN-IPv4 路由数量过于庞大。并且由于 ASBR 间是普通的 IP 转发，要求为每个跨域的 VPN 使用不同的接口（可以是子接口、物理接口、捆绑的逻辑接口），从而提高了对 PE 设备的要求。

配置 VRF-to-VRF 方式的跨域 VPN，需要在两侧 VPN 各配置相应的 VPN，根据接口或者子接口方式进行互通，不需要特殊配置。

ASBR 间通过 MP-EBGP 发布标签 VPN-IPv4 路由

这种方式下，两个 ASBR 通过 MP-EBGP 交换它们从各自 AS 的 PE 路由器接收的标签 VPN-IPv4 路由。ASBR 需要对标签 VPN-IPv4 路由进行特殊处理，因此也称为 ASBR 扩展方式。如图 2-6 所示。

图2-6 ASBR 间通过 MP-EBGP 发布标签 VPN-IPv4 路由组网图



路由发布过程可分为以下步骤：

1. AS1 内的 PE 先通过 MP-IBGP 方式把标签 VPN-IPv4 路由发布给 AS1 的边界路由器 PE，或发布给为 ASBR PE 反射路由的路由反射器 RR（Route Reflector）。
2. 作为 ASBR 的 PE 通过 MP-EBGP 方式把标签 VPN-IPv4 路由发布给 AS2 的 PE（也是 AS2 的边界路由器）。
3. AS2 的 ASBR PE 再通过 MP-IBGP 方式把标签 VPN-IPv4 路由发布给 AS2 内的 PE，或发布给为 PE 反射路由的路由反射器。

采用 MP-EBGP 方式时，需要注意以下两点：

- ASBR 之间不对接收的 VPN-IPv4 路由进行 VPN Target 过滤，因此，交换 VPN-IPv4 路由的各 AS 服务提供商之间需要就这种路由交换达成信任协议。
- VPN-IPv4 路由交换仅发生在私网对等点之间，不能与公网交换 VPN-IPv4 路由，也不能与没有达成信任协议的 MP-EBGP 对等体交换 VPN-IPv4 路由。

在可扩展性方面，通过 MP-EBGP 发布标签 VPN-IPv4 路由优于 ASBR 间通过子接口管理 VPN。

PE 间通过 Multi-hop MP-EBGP 发布标签 VPN-IPv4 路由

前面介绍的两种方式都能够满足跨域 VPN 的组网需求，但这两种方式也都需要 ASBR 参与 VPN-IPv4 路由的维护和发布。当每个 AS 都有大量的 VPN 路由需要交换时，ASBR 就很可能成为阻碍网络进一步扩展的瓶颈。

解决上述问题的方案是 ASBR 不维护或发布 VPN-IPv4 路由，PE 之间直接交换 VPN-IPv4 路由。

2.3.2 路由设计

路由设计原则

路由设计对 IP 广域网来说是非常重要的，路由设计会直接影响到广域网的可靠性和安全性。在进行路由设计时，应遵循如下原则：

- 避免局部路由变化引起整网的路由震荡。
- 通过路由设计更好的将网络流量在整网内分担。
- 避免路由孤岛现象出现。
- 路由条数尽量少，同时要考虑传输距离问题。
- 快速收敛，快速发现故障并做出响应，使得系统从故障中尽快恢复，避免路由黑洞和路由循环。
- 路由协议支持 GR。

路由详细设计

- 专网所有路由器位于一个域内，IGP 采用 ISIS 或是 OSPF 路由协议，平面路由设计，ISIS 采用分 LEVEL 方式，OSPF 采用分域方式。
- 专网域间路由协议采用 BGP-4，独立 AS 号，在 AS 边界通过 EBGP 控制路由的发送、接收、汇总和属性修改。
- 采用 1 级路由反射器（RR）设计，保证 BGP peer 数量小于 100/RR。当路由反射器客户较多时，考虑使用独立的路由器来做 RR。至少设置两台路由器反射器，避免单点故障，客户至少双归到两台路由反射器上
- 路由器管理地址和链路地址的路由使用 IGP 承载，其他路由使用 BGP 承载，如专线用户、3G/NGN 设备地址和地址池等。
- VPN 域内路由协议使用 MBGP 协议，反射器设置原则和普通的 BGP 相同。
- VPN 的 PE-CE 之间的路由协议根据网络规模可以选择 BGP，OSPF，从安全性角度考虑，推荐使用静态路由协议。
- 路由协议支持 MD5 认证，确保路由协议安全。

2.4 IP 承载层可靠性规划

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，承载层设备本身必须达到 99.999%可靠性要求。

华为公司在业界首家提供“可真正部署的端到端 ms 级倒换方案”，满足电信业务承载的可靠性要求（50ms ~ 500ms），解决标准技术在扩展性、可部署性等方面的不足，降低运营维护成本、保障业务运营效果。

2.4.1 故障检测技术

传统的故障检测技术是通过检测设备接口的状态来发现故障，这种方式只能检测简单的物理故障，而对于更深层的故障（如转发引擎故障、链路单通等）只能依靠上层的路由协议通过 Keep alive 或 Hello 报文来发现故障。这种机制不仅检测时间慢、开销大，而且存在应用场景的限制（不能跨协议）。

因此，为了提高 IP/MPLS 层的故障检测时间和效率，需要使用检测速度快、支持各种协议的故障检测机制。目前主要采用的机制有 MPLS OAM 和 BFD 技术。

BFD

BFD（Bi-directional Forwarding Detection）是一个简单的交互检测协议，用于快速检测系统之间的通信故障，并在出现故障时通知上层应用。

BFD 具有如下特性：

- 可以对相邻转发引擎之间的通道提供轻负荷、快速故障检测。这些故障包括接口故障，数据链路故障，甚至有可能是转发引擎本身故障。BFD 的故障检测时间一般在 50ms 以内。
- 提供一个单一的机制，能够用来对任何媒介、任何协议层进行实时地检测。实现 BFD for Everything，例如 IS-IS/OSPF、BGP、LSP、TE 等等。

在目前网络中，BFD 已经被广泛应用于各种链路、协议的故障检测。

MPLS OAM

MPLS OAM 是一个针对 MPLS 的 LSP 连通性的快速检测机制，通过 LSP 中各节点之间的 OAM 报文的快速交互，实现对于 LSP 连通性的检测。

MPLS OAM 不依赖于任何上层或下层的机制，主要实现以下功能。

- 有效检测、识别和定位 MPLS 用户层面故障。
- 衡量网络的利用率以及度量网络的性能。
- 在链路出现缺陷或故障时迅速进行保护倒换，以便能根据与客户签订的 SLA（Service Level Agreements）提供业务。

关于 MPLS OAM 的详细信息可参考 ITU-T Recommendation Y.1710 和 Y.1711。

2.4.2 业务保护技术

IP/MPLS 网络的每个部件都有可能出现故障，而采取的网络保护手段也有所不同。例如：

- 应用主控冗余、单板热插拔、GR 等保证设备层故障。
- 应用 VRRP、GLBP 等技术提高网关节点可靠性。
- 通过 IGP 快速收敛、TE FRR 保证网络路径的可用性。
- 通过 VPN FRR 保证 PE 节点可靠性。

下面就对各种常见的保护技术进行简单的说明。

IGP 快速收敛

IGP 快速收敛的目的在于当网络发生故障时，提高 IGP 重新计算和路由收敛的速度。IGP 快速收敛是由多项技术结合而成的，主要包括如下特性。

- I-SPF（Incremental SPF）：增量路由计算，它每次只对变化的一部分路由进行计算，而不是对全部路由重新计算。
- PRC（Partial Route Calculation）：PRC 的原理与 I-SPF 相同，都是只计算变化的那一部分。但 PRC 不需要计算节点路径，而是根据 I-SPF 算出来的 SPT 来更新叶子（路由）。
- LSP 快速扩散：路由器收到一个或多个比较新的 LSP 时，在路由计算之前，先将小于指定数目的 LSP 扩散出去，加快 LSDB 的同步过程。这种方式在很大程度上可以提高整个网络的收敛速度。
- 智能定时器：智能定时器可以根据路由信息变化的频率自动调整延迟时间，既保证了路由快速收敛，且不影响路由器效率。智能定时器包括 SPF 智能定时器和 LSP 生成智能定时器。

IP FRR

传统的 IP 网络中，从检测出故障，到路由系统完成路由收敛，一般需要几秒钟的时间。对于网络上某些对延时、丢包等非常敏感的业务来说，这种收敛速度无法容忍。比如 VoIP 业务所能容忍的网络中断时间为毫秒级。

IP FRR 特性能够保证转发系统快速地对于这种故障进行检测并采取措施，尽快让业务流恢复正常。IP FRR 的主要实现思想如下：

- 在主链路可用时，通过 Route-Policy 设置 IP FRR 策略，把备份路由的转发信息同时提供给转发引擎。
- 当转发引擎感知到主链路不可用时，能够在控制平面路由收敛前直接使用备份路径转发信息。

IGP Auto FRR

IP FRR 的备份下一跳是通过手工配置生成的，配置复杂，且需要依靠人为规划避免环路问题，容易出错。为了克服 IP FRR 的技术缺陷，引入了 IGP Auto FRR。

IGP Auto FRR 是 IGP 利用收集到的链路状态信息动态决策出 IP FRR 备份的技术，其 IP 备份下一跳完全由路由协议根据链路状态信息结合公式自动生成，无需人工干预，极大的节约了维护的成本。

BGP FRR

IGP /LDP FRR 技术对链路故障的情况，可以做到快速的路径切换，但是当 BGP 节点发生故障时，需要 BGP 控制层面收敛，然后重新下转发表，收敛时间可能达到秒级，BGP 下一跳分离技术可以加快控制层面的收敛速度，但仍然无法达到电信级的可靠性要求。

BGP FRR 技术采用转发层面的直接切换的方式, 将次优 BGP 邻居的 LDP Label/BGP Label 直接作为备份放置到转发表中，当 BFD 等快速检测机制检测到最优 BGP 邻居故障时，直接切换到备份的表项，实现业务的快速收敛。

LDP FRR

在 LDP 层面，通过 LDP FRR 可以实现 LDP LSP 的快速收敛，LDP FRR 是指将设备将 LDP 的最优路由作为转发表项的同时，将 LDP 的次优路由作为备份路径，同时放到转发表中。在最优的下一跳发生故障时，直接使用备份路径/标签进行转发。

通过 BFD 检测可以快速检测与最优下一跳的连接情况，可以实现 50ms 的收敛速度。

LDP FRR 收敛技术的使用是有一定限制的，比如在环网的情况，可能会出现次优下一跳将报文送回本节点从而形成转发环路的情况。

相比 RSVP TE 的 FRR 保护技术，LDP FRR 保护基于单点的行为，不需要端到端的保护。

MPLS TE FRR

MPLS TE FRR 是 MPLS TE 中一套用于链路保护和节点保护的机制。当 LSP 链路或者节点故障时，在发现故障的节点进行保护，这样可以允许流量继续从保护链路或者节点的隧道中通过，以使得数据传送不至于发生中断，同时头节点就可以在数据传送不受影响的同时继续发起主路径的重建。

MPLS TE FRR 的基本原理是用一条预先建立的 LSP 来保护一条或多条 LSP。预先建立的 LSP 称为 FRR LSP，被保护的 LSP 称为主 LSP。MPLS TE FRR 的最终目的就是利用 FRR 隧道绕过故障的链路或者节点，从而达到保护主路径的功能。FRR LSP 和主 LSP 的建立过程需要 MPLS TE 系统的各个构件参与。

MPLS TE FRR 是基于 RSVP TE 的实现，遵循协议 RFC4090。

VPN FRR

MPLS TE FRR 对于 TE 隧道起始点和终结点的两个 PE 设备之间的链路故障和节点故障，能够提供很好的保护，但是不能保护解决隧道起始点和终结点的 PE 设备。

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，在典型组网中一般在 5s 左右，无法达到节点故障端到端业务收敛小于 1s 的要求。

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 PE 故障快速探测，旨在解决 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 节点故障恢复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。

2.5 光传送层可靠性规划

广域网的可靠性规划一般是指对于 IP 承载网的可靠性规划，而底层的传送网是运营商的网络，企业用户不需要考虑其可靠性问题。

但是对于一些大型或特大型企业来说，有可能自建光传送网，此时除了 IP 承载网的可靠性之外，还需要考虑光传送网的可靠性。

光传送层是业务和数据的底层物理网络，它的设备和网络的可靠性直接关系到上层业务和数据网络的正常运行，因此光传送设备一般都具备较丰富的保护特性，具备较高的可靠性。

传送层的保护可分为设备级保护和网络级保护。设备级保护用于对单点设备进行保护，例如主控 1+1 保护、交叉 1+1 保护、输入电源保护和集中电源保护、风扇冗余保护、子架间通信保护等，本文不作详述。

网络级保护用于对整个网络的设备和链路进行保护，常见的保护技术如下：

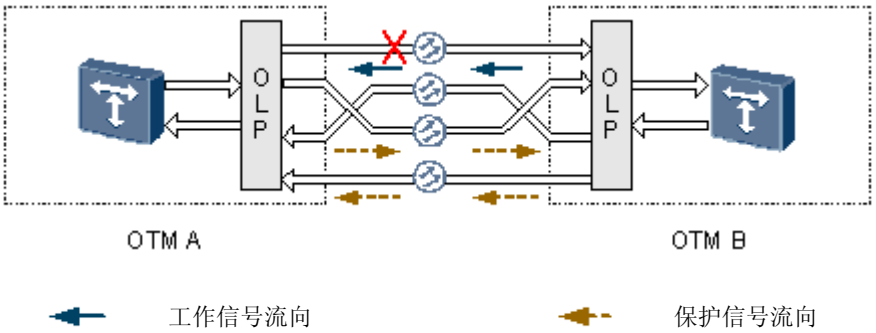
- 光线路保护
- 光通道保护
- 子网连接保护
- ASON 保护

2.5.1 光线路保护

光线路保护是指运用 OLP 单板的双发选收功能，在相邻站点间利用分离路由对线路光纤提供保护。

光线路保护采用两对光纤，一对为工作路径，在工作路径正常情况下传送业务信号；另一对为保护路径，在工作路径发生断纤或信号衰减过大情况下，承载业务信号，如图 2-7 所示。

图2-7 光线路保护应用



2.5.2 光通道保护

光通道保护包括客户侧 1+1 保护和板内 1+1 保护。

客户侧 1+1 保护

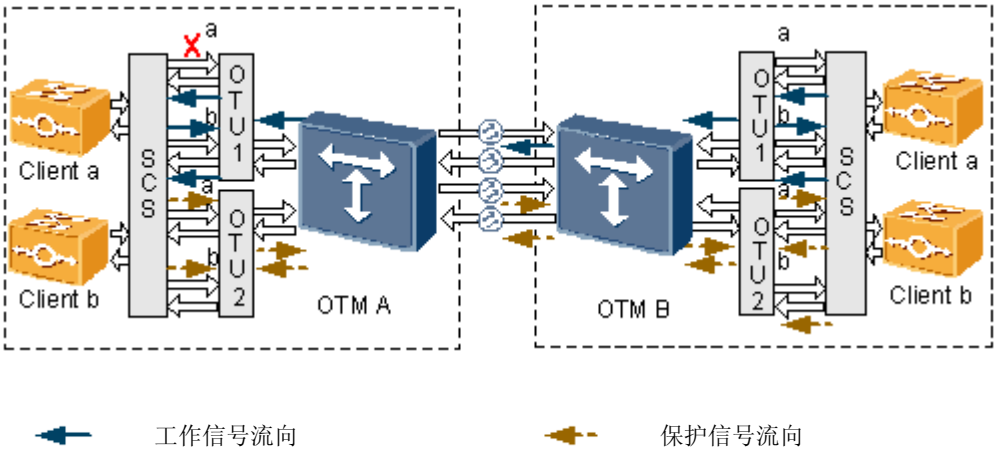
客户侧 1+1 保护通过运用 OLP/DCP 单板的双发选收或 SCS 单板的双发双收功能，对 OTU 单板其及 OCh 光纤进行保护。客户侧 1+1 保护通过占用工作及保护两个波长、两个波长采用不同的路由进行传输的方式，对 OTU 单板进行保护。

当使用 SCS 单板时，正常情况下，工作 OTU 单板的客户侧激光器打开，保护 OTU 单板的客户侧激光器关闭。当工作 OTU 单板检测到 SF 或 SD 信号时，工作 OTU 将上报

SCC 单板，SCC 单板关闭工作 OTU 单板的客户侧激光器，开启保护 OTU 单板的客户侧激光器。系统直接通过 SCC 单板实施保护倒换。

当使用 OLP 或 DCP 单板时，正常情况下，工作 OTU 单板和备用 OTU 单板的客户侧激光器都是打开的。当工作 OTU 单板检测到 SF 或 SD 信号时，工作 OTU 将上报 SCC 单板，SCC 单板关闭该 OTU 单板的客户侧激光器。OLP 或 DCP 单板检测到 R_LOS，实施保护倒换。

图2-8 客户侧 1+1 保护应用



板内 1+1 保护

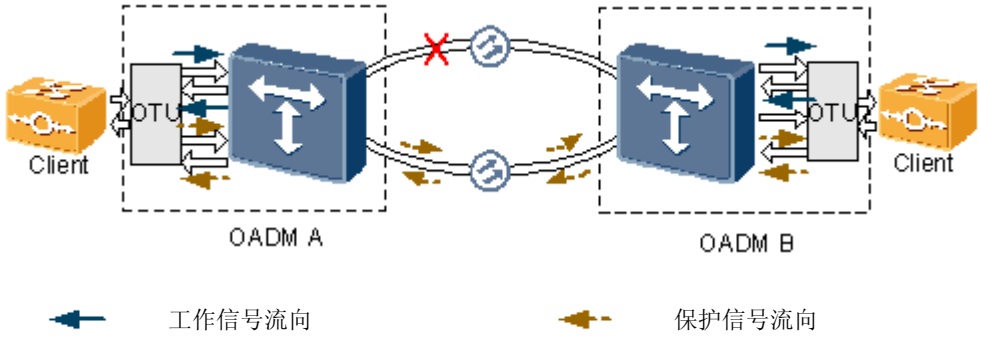
板内 1+1 保护运用 OTU/OLP/DCP 单板的双发选收功能，利用分离路由对业务进行保护。板内 1+1 保护采用双发选收、单端倒换方式，用于链形组网和环形网中。

当用于链型组网时，板内 1+1 保护和光线路保护类似，需要在相邻站点间提供分离路由。当用于环网时，板内 1+1 保护利用环网上分离的路径进行保护，即业务随顺时针、逆时针方向在环上传送，最终到达目的节点。

板内 1+1 保护包括两种：

- 利用具有双发选收功能的 OTU，实现对业务的保护，如图 2-9 所示。
- 利用具有双发选收功能 OLP 或 DCP，实现对业务的保护，应用与 OTU 类似。

图2-9 板内 1+1 保护应用



2.5.3 子网连接保护 SNCP

子网连接保护 SNCP（Sub-Network Connection Protection）是指对某一子网连接预先安排专用的保护路由，一旦子网发生故障，专用保护路由便取代子网承担在整个网络中的传送任务。

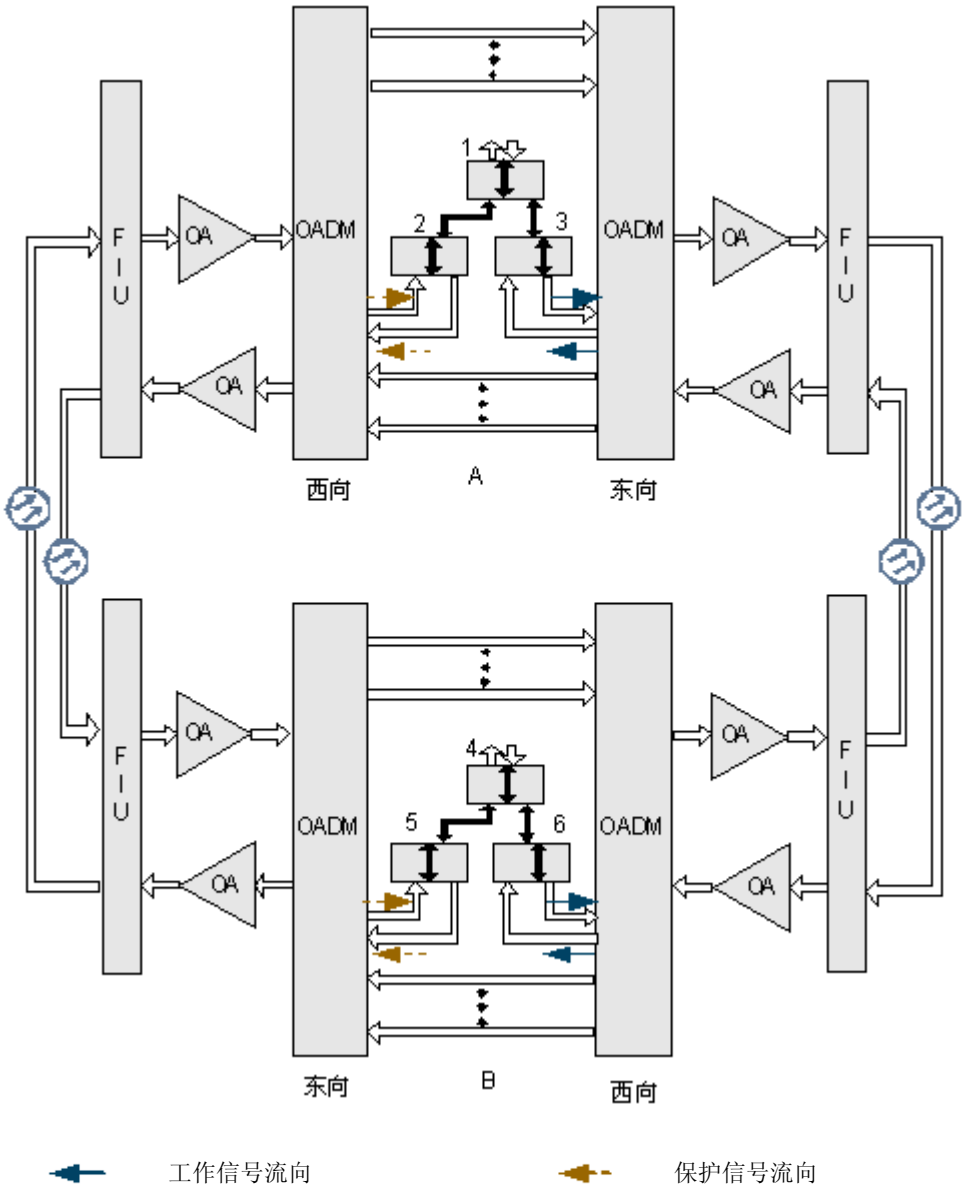
SNCP 是一种通道层的保护，无需 APS 协议，它可以应用在环网上形成二纤通道保护环。在网络结构日趋复杂的情况下，SNCP 是可适用于各种网络拓扑结构且倒换速度快的业务保护方式。

SNCP 通常可包括 SW（Sub-wavelength）SNCP、ODUk SNCP、VLAN SNCP、支路 SNCP、MS（Master Slave） SNCP 等。本节只以 ODUk SNCP 为例进行说明，其余内容可以参考对应传送设备（例如 OptiX OSN 6800）的产品文档。

ODUk SNCP 保护运用电层交叉的双发选收功能，对线路板和 OCh 光纤进行保护。要用于对跨子网业务进行保护，不需要协议。ODUk SNCP 可用于各种形式的组网，具有较大的灵活性。如图 2-10 所示。

- 在业务发送方向，需要保护的客户业务从支路板输入，通过交叉分成工作信号和保护信号，分别送往工作线路板和保护线路板。然后工作信号和保护信号分别在工作通道和保护通道里传输。
- 在业务接收方向，正常工作时，仅工作线路板对应的交叉连接生效，断开保护线路板的交叉连接。当工作通道故障时，线路单板检测并上报相关信号故障告警，产生 SF 或 SD 事件，主控板检测到 SF 或 SD 后，下发倒换命令，断开工作线路板交叉连接，保护线路板对应的交叉连接生效，业务信号工作在保护通道。
- 当工作路由恢复正常后，根据在网管上预先配置的恢复类型，业务信号可以恢复到指定的线路板所对应的交叉连接上。

图2-10 ODUk SNCP 保护



2.5.4 ASON 保护

在传统网络中，波分传输设备往往只作为光纤的替代，而现在已经开始直接承载用户业务，所以对设备的可运营的需求增加。传统网络中存在以下问题：

- 业务配置步骤复杂，扩容或新开通业务周期较长。
- 带宽利用率及效率低，环网结构需要预留一半的带宽。
- 保护单一，网络自愈保护性能差。

为了有效地解决上述问题，一种新型的网络体系应运而生，这就是自动交换光网络ASON（Automatically Switched Optical Network），也就是通常所说的智能光网络。它在传输网中引入了信令（GMPLS-UNI），并通过增加控制平面，增强了网络连接管理和故障恢复能力。它支持端到端业务配置和多种业务恢复形式。

ASON 相对传统 WDM 具备以下特点：

- 支持基于光学参数的路由计算策略，自动排除不满足光学参数要求的路径。
- 支持重路由和优化时波长自动调整，有效解决了波长冲突问题。
- 新建业务可自动分配波长。
- 支持端到端的业务自动配置。
- 支持拓扑自动发现。
- 支持 Mesh 组网保护，增强了网络的可生存性。
- 支持差异化服务，根据客户层信号的业务等级决定所需要的保护等级。
- 支持流量工程控制，网络可根据客户层的业务需求，实时动态地调整网络的逻辑拓扑，实现了网络资源的最佳配置。

下面着重描述基于 ASON 的传送层保护机制。

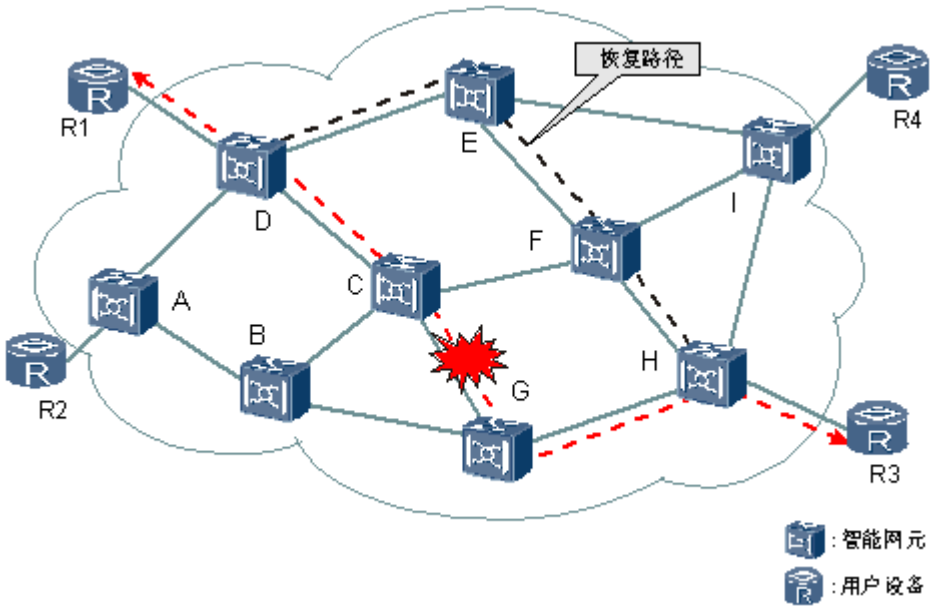
MESH 组网

Mesh 组网是 ASON 网络的主要组网方式之一，这种组网方式具有灵活、易扩展的特点。与传统 WDM 网络相比，在这种组网方式下，恢复路径可以有很多条，提高了网络的安全性，并最大程度上利用整个网络资源。

在 Mesh 组网中，为使中断业务得以重新接通，除延用传统的专用保护（如 1+1 保护）和共享保护外，还能够借助于重路由机制实现业务的即时恢复。也就是说，通过 MESH 组网，不仅可以提供传统的保护方式，还能够提供动态恢复的业务形态，甚至在保护失效的情况下还能提供业务恢复机制，使其只要有资源就不会中断业务。

如所示，C-G 之间的光纤断开时，为了达到业务恢复的目的，重新计算一条从 D 到 H 的路由。并建立新的 LSP，业务经新的 LSP 传送。

图2-11 MESH 组网的业务保护和恢复



动态重路由

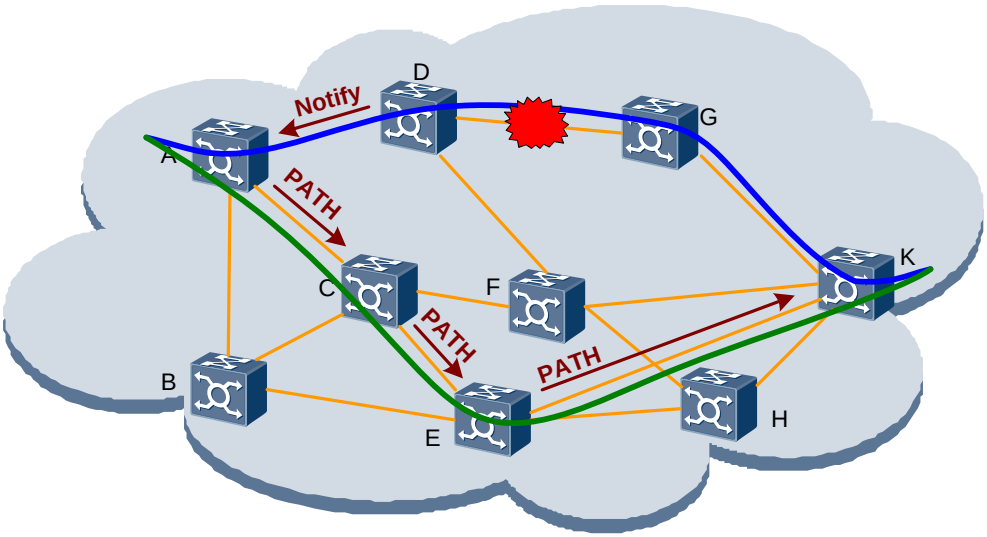
重路由是一种业务恢复方式。对于不可返回式业务，当 LSP 中断时，首节点计算出一条业务恢复的最佳路径，然后通过信令建立起一条新的 LSP，由新的 LSP 来传送业务。在建立了新的 LSP 后，删除原 LSP。

动态重路由是 GMPLS/ASON 带来的核心特性之一，是一种兼顾保护能力和资源利用效率的保护方式，也是对传统保护方式革命性的补充和改进。有了它，抗多次断纤的保护/恢复成为了可能。

如图 2-12 图所示组网拓扑，配置有一条从节点 A 经过 D、G 到节点 K 的 LSP，现在节点 D、G 之间断纤，那么其动态重路由过程为：

- 节点 D 的 FIU（对光层）或 OTU（对电层）检测到告警后，上报主控 GMPLS 模块；
- 节点 D 主控 GMPLS 模块检查受影响的智能业务，向首节点 A 发送 Notify 消息；
- 首节点 A 的 GMPLS 模块收到 Notify 消息后，计算出一条端到端恢复路径，然后沿计算好的路径，经中间节点向末节点 K 方向发送 PATH 消息，在沿途各节点建立反向交叉连接；
- 末节点 K 的 GMPLS 模块收到 PATH 消息后，经由中间节点向首节点 A 方向发送 RESV 消息，在沿途各节点建立正向交叉连接；
- 首节点 A 收到末节点发过来的 RESV 消息后，打开告警监视，再向下游节点发送开告警的 PATH 消息。下游节点收到该消息后均打开对新业务路径的告警监视。
- 整条 LSP 的告警监视打开后，如果是不可返回式业务则删除老路径，整个重路由过程结束。

图2-12 重路由关键流程



预置恢复路径

对于可靠性要求更高的业务，可预置其恢复路径。当路径发生故障时，GMPLS/ASON 将按照用户设定的恢复路径进行恢复，保证了 GMPLS/ASON 网络业务路径的可控性。如恢复不成功，则按照动态计算出的路径进行重路由。这样可在一定程度上满足用户对业务恢复路径进行控制的需要。

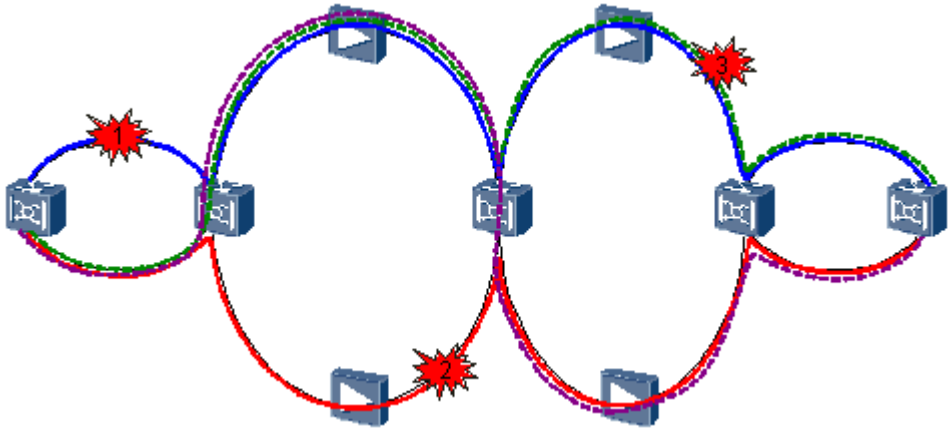
为保证多次断纤后重路由后的路由可控，ASON 软件支持对一条端到端可重路由（包括光层和电层智能）业务配置多条预置恢复路径。用户可以对一条 LSP 最多设置 2 条预置恢复路径，并且可以指定这两条预置恢复路径的优先级。

主备路径共享恢复

主备路径资源共享可以尽可能提供恢复资源。主要应用场景请参见图 2-13 所示的相切环组网拓扑。

蓝色和红色实线为主备路径，1、2 处断纤的发生使主备路径均失效，此时若主备路径不能共享，则该业务无法得到恢复资源。若能够共享，那么就可以将一部分主路径和一部分备路径拼凑起来找到一条恢复路径，即图中绿色虚线所示路径。同样地，3 处再断纤仍然能找到紫红色虚线所示路径将业务恢复。

图2-13 主备路径共享应用

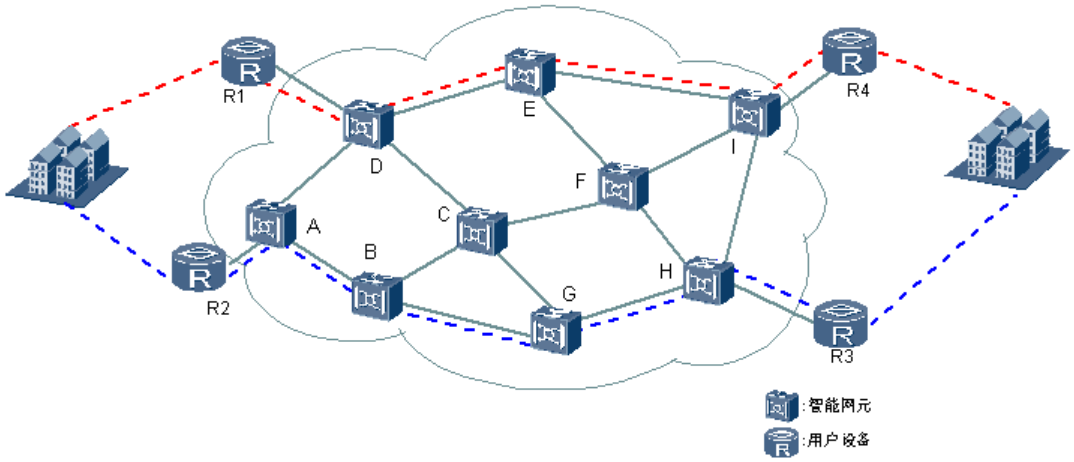


业务关联

业务关联是将两条 LSP 关联起来。在其中一条 LSP 重路由或优化时，尽量与另外一条 LSP 分离，而且不会与关联 LSP 完全重合。主要用来接入有两个接入点的业务（双归属业务）。

如图 2-14 所示，把 D-E-I 和 A-B-G-H 两条 LSP 关联。如果 B 和 G 之间断纤，则 A-B-G-H 这条 LSP 将进行重路由，而且会尽量避开 D-E-I 这条链路。

图2-14 业务关联



差异化服务 SLA

基于 WDM/OTN 的 GMPLS/ASON 可提供多种保护能力不同的业务，包括钻石、银和铜级业务。不同级别的业务，费用不同，这样的差异化服务可以更灵活地满足用户的不同需求。如表 2-2 所示。

表2-2 业务等级

业务	保护和恢复策略	实现方式	倒换时间
钻石级业务	保护与恢复	板内 1+1 保护，ODUk SNCP，SW SNCP 和重路由	小于 50ms
银级业务	恢复	重路由	-
铜级业务	无保护不恢复	-	-

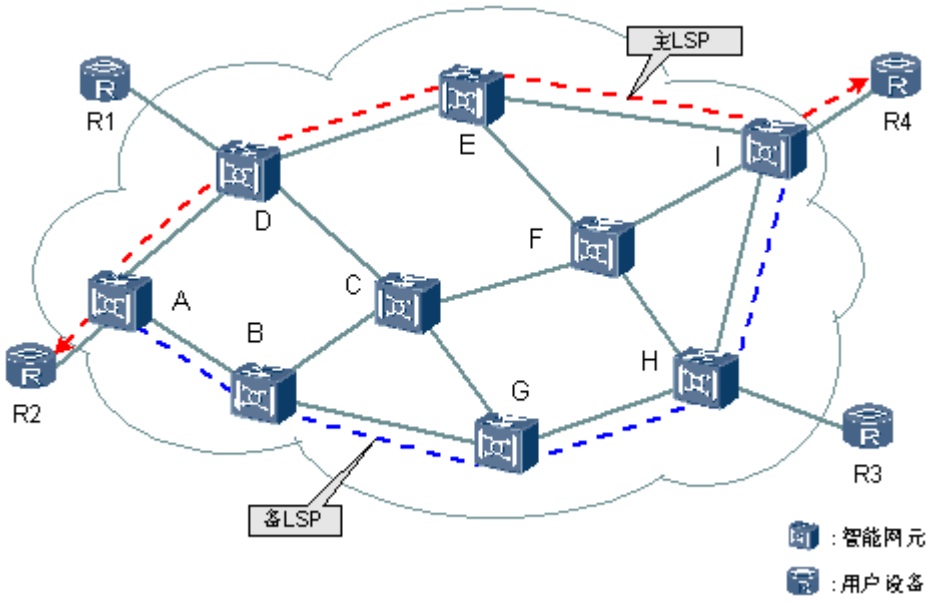
步骤 2 钻石级业务

钻石级智能波分路径的保护能力最强，在资源充足的前提下提供永久的 1＋1 保护。包括钻石级智能波分 ODUk 路径。主要用于传送重要的话音和数据业务，重要客户专线，如银行、证券、航空等。

钻石级业务是指一条从源节点到宿节点的具有 1+1 保护属性的业务，也叫 1+1 业务。在源节点和目的节点之间同时建立起两条 LSP，这两条 LSP 的路由尽量分离。一条称为主 LSP，另一条称为备 LSP。源节点和目的节点同时向主 LSP 和备 LSP 发送相同的业务。目的节点在主 LSP 正常的情况下，从主 LSP 接收业务；当主 LSP 失效后，从备 LSP 接收业务。

钻石级业务如图 2-15 所示。

图2-15 钻石级业务



钻石级业务的重路由策略有如下三种：

- 永久 1＋1 钻石级业务：任意一条 LSP 失效即触发重路由。
- 重路由 1＋1 钻石级业务：两条 LSP 都失效才触发重路由。
- 不重路由钻石级业务：不管 LSP 是否失效，都不触发重路由。

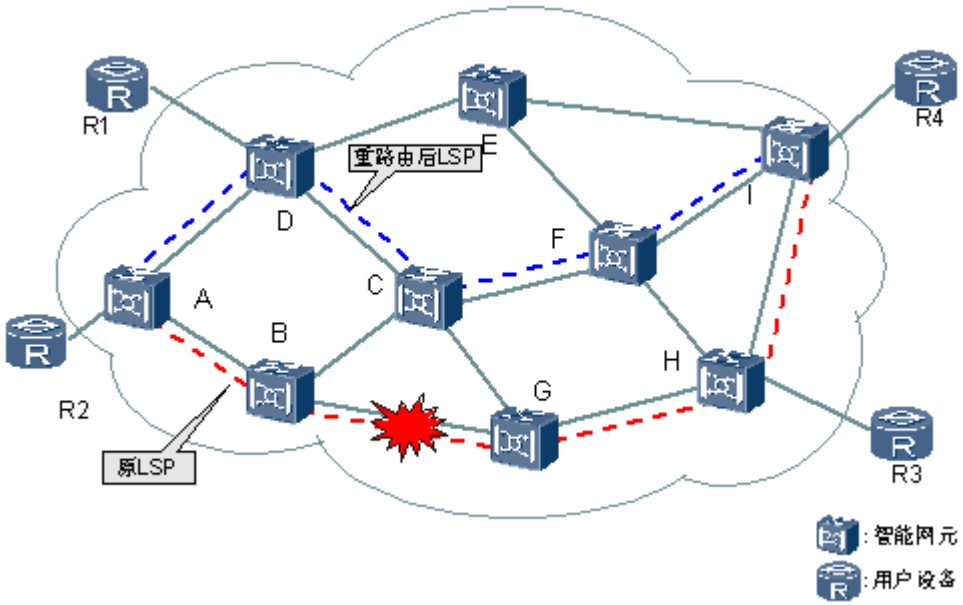
步骤 3 银级业务

银级智能波分路径包括光层智能波分 OCh 路径、电层智能 ODUk 路径和 Client 路径，恢复时间为秒级，适用于实时性要求不太高的数据业务、小区上网业务等。

银级业务指从源节点到目的节点的具有重路由保护属性的业务连接，也叫重路由业务。如果银级业务的 LSP 失效，会不断发起重路由进行业务恢复，直至重路由成功。由于银级业务实时计算恢复路径，勿需预先预留资源，故带宽利用率高。但如果网络资源不足，可能造成业务中断。

如图 2-16 所示，A-B-G-H-I 是一条银级业务。当 BG 之间断纤，则从 A 点发起重路由，避开 BG 这段光纤，重新建立一条业务连接，从而达到保护目的。

图2-16 银级业务



步骤 4 铜级业务

铜级智能波分路径应用很少，一般适用于配置临时业务，如节假日期间的突发业务。包括铜级光层智能波分 OCh 路径、电层智能 ODUk 路径和 Client 路径。

铜级业务就是无保护业务。如果 LSP 失效，不会发起重路由，业务中断。

2.6 IP+光保护协同规划

广域互联/骨干网的故障影响范围非常广泛，通常一个广域互联/骨干网络故障会影响到成千上万的企业业务，直接影响企业的生产效率和对市场变化的快速响应。因此广域互联/骨干网的可靠性对于企业的运营和竞争力有至关重要的影响。

虽然 IP 层和传送层各自都有丰富的保护，但是在保护的配合上存在一定的问题。或者是保护不成功，或者是重复保护，不仅浪费资源而且影响业务质量。

保护协同就是通过 IP 层和传送层的联合保护，根据广域互联/骨干网的不同需要，提供最优的联合保护方案，主要包括多层网络规划工具、静态/动态 SRLG 标识、控制层智能协同和层次化协同保护方案等。

2.6.1 多层网络规划工具

传统的广域互联/骨干网络是逐层规划的，因此存在网络资源利用率不高、QOS 及可靠性部署复杂的问题，并且网络规模很大时难以做到多人同时设计。

相比传统的单层网络规划工具，多层网络规划工具可大幅提高资源利用率和网络可靠性。

- 通过跨 IP 层和传送层的协同规划，可以根据业务流量统筹分配两层的带宽资源，实现业务流量的协同承载，提高资源利用率。
- 通过两层的协同规划，避免一个故障激发两层各自保护而导致资源浪费，实现高效保护，提高网络可靠性，是实现骨干网 IP 层和传送层智能协同的必要基础。

2.6.2 SRLG 标识

SRLG（Shared Risk Link Group）是指具有共同可靠性风险的一组链路。例如对于路由器的多个不同的链路，可能会存在经过了相同传送路径的情况。如果此传送链路故障，则路由器层面主备链路会同时故障。

为了避免上述情况的出现，就要求 IP 网络的在计算路径的时候，将有相同 SRLG 信息的链路不放在主备路径上，这样通过 SRLG 信息，以及 SRLG 计算，可以保证路径的主备链路一定不会因为一个底层链路的故障而同时故障，从而提高 IP 层保护的可靠性。

静态 SRLG 标识

静态 SRLG 标识是指在 IP 网络管理人员，通过与传送网的网络管理人员的人工交互后，进行人工的分析和规划，标识出相关的 SRLG 信息，并静态配置到 IP 设备上。

静态 SRLG 标识实现简单，无需额外的配置。但是静态 SRLG 标识存在如下问题：

- SRLG 的配置需要 IP 网络和传送网管理维护人员大量细致的信息交互和配置，工作量很大，而容易出错。
- 如果传送层面进行链路重新规划和调整，需要重新和 IP 网络管理人员交互，重新修改 IP 层的配置。
- 如果传送层使用了 ASON GMPLS 技术，传送路径有可能自动发生变化，变化的路径信息无法及时通知 IP 网络。

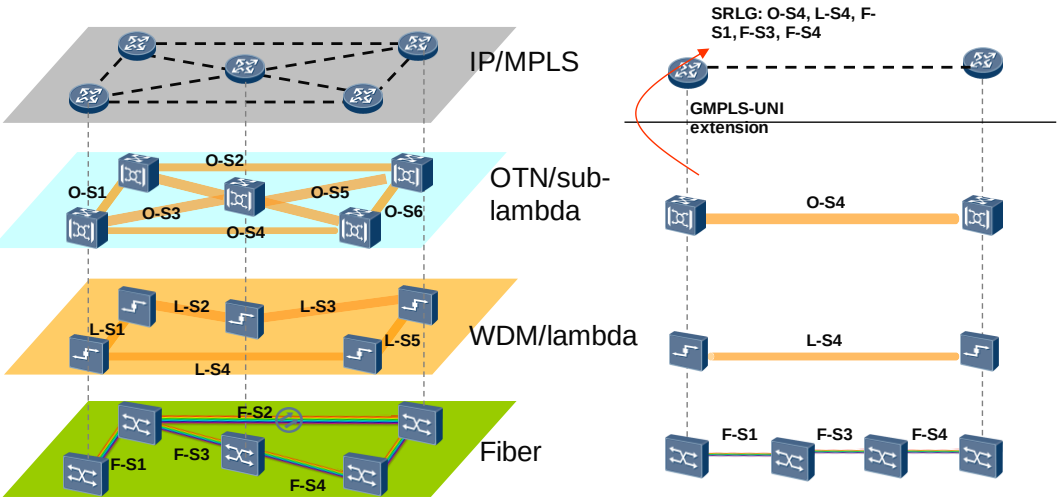
动态 SRLG 标识

由于静态 SRLG 标识存在一定的缺陷，因此华为公司提出了动态 SRLG 标识的解决方案。通过扩展路由器和传送设备间的 GMPLS-UNI，传送设备可以将 SRLG 信息自动传送给 IP 设备。这样上述三个问题都可以很好的解决。

- SRLG 信息由传送层直接发给 IP 层，不需要人工交互，提高效率和正确性。
- 传送层链路调整，传送会自动更新 SRLG 信息，无需人工重新修改。
- 传送层基于 GMPLS ASON 重新计算路由后，也会自动更新 SRLG 信息给路由器。

传送层上会根据链路实际情况上报 SRLG 信息，包含了此链路各个层次的信息，OTN 层、光层、以及光纤层面等。而 IP 设备则根据这些信息自动进行计算和更新主备链路的路径，以避开相同的 SRLG 链路。如图 2-17 所示。

图2-17 动态 SRLG 标识



2.6.3 控制层智能协同

在静态协同模式下不需要考虑控制平面，但是在动态协同模式下，控制平面将发挥关键作用。控制平面的关键技术主要包括 GMPLS-UNI 技术和 PCE 技术。

GMPLS-UNI

GMPLS-UNI 是 IETF 的标准，对于增强 IP 层和传送层的交互有着关键的作用。通过 GMPLS-UNI，IP 层可以直接驱动传送层建立通道或者删除通道。

以建立链路为例， IP 层只需通过 GMPLS-UNI 信令通知传送层新建链路的源和目的节点、新建链路的属性（例如带宽、保护属性等），传送层自动建立满足需要的传送通道。

PCE

在一个大型网络上，基于约束条件的路径计算很复杂，而且需要相关设备具备很强的计算能力。而如果使用分布式路径计算方式，每个节点都要具有强大的路径计算能力，但是这样的话会导致高成本。并且在多域的网络上，每个域的拓扑对其他域都不可见，因此要计算出最优的端到端路径，参与计算的设备必须互相协同。

PCE 就是为了满足上述需要的路径计算技术。PCE 具有强大的路径计算能力，可以部署在网络阶段或者外部服务器上。PCE 负责在一个域里的路径计算。每个域的路径计算请求都发送给这个域的 PCE。在完成路径计算以后，PCE 把结果发送给发出这个请求的客户端(PCC)。多个 PCE 协同工作可以计算出最优的路径。

2.6.4 层次化协同保护

通过 IP 层和传送层的不同保护技术的协同，IP+光协同方案可以提供不同等级的层次化的保护方案。包括如下几种：

- TE FRR+ASON 钻石级 1+1 保护
- TE FRR+ASON 银级重路由保护

- TE Hot Standby+光线路 1+1 保护

TE FRR+ASON 钻石级 1+1 保护

该方案用于业务可靠性需求等级高、光路资源和 IP 链路资源充足的场景。

IP/MPLS 层采用 TE FRR 方式保护关键路径，传送层采用 ASON 钻石级 1+1 保护方式。保护范围包括 IP 层节点和链路故障，传送层节点和链路故障，光层可以抗多次断纤。

TE FRR+ASON 银级重路由保护

该方案用于业务可靠性需求等级较高、光路资源较充足的场景。

IP/MPLS 层采用 TE FRR 方式保护关键路径，传送层采用 ASON 银级重路由保护方式。波分线路侧光纤发生故障时，IP/MPLS 层 TE FRR 先启动倒换，倒换到 Bypass Tunnel 上去，传送层使用银级重路由方式重新选择一条路径，当波分重路由结束后，IP 层切回主 Tunnel，回切过程中，路由器使用 Make Before Break，不会产生丢包。

TE Hot Standby+光线路 1+1 保护

该场景传送层的保护只局限在站点间光纤，不能对传送单板和整个站点故障进行保护，而且也只能抗一次断纤，可用于业务可靠性等级一般，设备资源一般的场景。

IP/MPLS 层采用 TE Hot Standby 方式保护端到到端路径，传送层采用光线路 1+1 保护方式，波分线路侧光纤发生故障时，波分层面先进行光线路 1+1 保护，将业务切换到备用光纤上。

2.7 QoS 规划

2.7.1 基础 QoS 规划

要规划设计整网的 QoS，需要按照特定的顺序，包括业务规划、资源预留、CAC 控制这 3 个主要步骤。

业务规划

确定广域网上实际承载的各种业务所需要的带宽情况，得出业务流量模型和流量带宽。以此为基础，合理规划流量，并可以实施流量工程，确保某些链路不会因为流量负担过大而发生拥塞，并提高整网链路的利用率。

以上数据主要来自于“现网评估”及“业务与流量分析”部分的输出。

资源预留

根据业务规划和流量模型，对于业务进行资源预留。对于一些高 QoS 要求的广域网，可以使用实时数据采集和分析设备，例如华为公司的 NetStream，用于实时调整资源预留情况，优化网络。资源预留主要的方法有 IP/MPLS DiffServ 和 MPLS TE 两种。

- IP/MPLS DiffServ

IP/MPLS DiffServ 方案是一种较流行的方法，应用较成熟，是一种基于统计模型的服务质量保证机制。

在实施 IP/MPLS DiffServ 方案前，首先要求有网络流量模型的分析，对网络不同业务的流量流向进行分析，为 QoS 部署提供基础。其次要求有 SLA 的测量机制，华为公司提供 HWping 解决方案，可针对业务提供延迟、抖动、丢包率的测量数据，为进行 QoS 再部署提供技术保障。

- MPLS TE

  MPLS TE 是一种更为先进的方法，在全网实施 MPLS VPN 和 MPLS TE。不同的业务封装在不同的 VPN 中，不同的 VPN 映射到不同的 MPLS TE 隧道中，从而提供了类似于专网级别的高 QoS。

  由于 TE 隧道本身具有端到端面向连接的特性，所以大规模部署 MPLS TE，其部署、维护的工作量较大。建议使用 VPN 与 MPLS TE 隧道灵活映射以及分层 TE，提高网络的灵活性，同时大大降低实施、配置及维护的工作量。

CAC 控制

对于高可靠的 IP 广域网而言，如果要承载实时业务，那么 CAC（Call Admission Control）就必须考虑。传统的 IP 网络是一个尽力而为的网络，不限制业务接入数量，从而导致过多的业务被接入，所有业务的资源都得不到保障。

而 IP 广域网继承了传统 TDM 电信网的思想，通过拒绝超额的业务呼叫请求，避免资源被过度使用，保证已经建立的业务连接的资源需求和服务质量。只有具备了 CAC 机制的多业务 IP 承载网，才能达到高可靠广域网的要求。

当前主流的多业务 IP 承载网通过业务系统来实现 CAC 功能，例如通过 Soft Switch 实现 CAC。而在将来的网络中，FMC（Fixed Mobile Convergence）是必然趋势，IMS（IP Multimedia Subsystem）架构是网络发展方向。在 IMS 时代的网络中，由承载控制层实现综合的 CAC 功能。

2.7.2 HQoS 规划

个人业务 HQoS 规划

个人业务的 HQoS 需要考虑不同业务类型的优先级调度（HSI、VoIP、VOD、BTV），可采用以下方式实现（对于 Triple-Play 业务，在 AGG 可以不部署 HQoS，基本的 Diff-Serv QoS 即可满足要求）：

- 用户+业务级

  同一端口下基于不同家庭用户以及不同业务可配置 CIR/PIR，不同业务之间进行优先级调度和带宽保证/控制；需要配置 QinQ 方式，即（S+C）两层 VLAN 方式来进行业务和用户的识别。

- 基于业务

  同一端口下用户的不同业务配置 CIR/PIR，并可进行优先级调度；只需要对业务 VLAN 进行识别。

企业业务 HQoS

针对企业 VPN 业务，HQoS 的应用可采用以下几种方式：

- 用户级

  同一端口下不同企业用户配置 CIR/PIR，不区分用户业务类型，其中用户以 VLAN/QinQ 进行区分。

  - VLAN 方式下，同一企业的各个 Site 采用不同的 VLAN，不同企业的 Site 也采用不同的 VLAN。
  - 在 QinQ 方式下，同一企业的外层 VLAN 相同，内层 VLAN 区分各个 Site。不同企业的外层 VLAN 不能相同，内层标示 Site 的 VLAN 可以相同。

- 用户+业务级

  同一端口下不同企业用户以及用户的不同业务（可分为 8 个等级）均可以配置 CIR/PIR，不同业务之间可进行优先级调度和带宽保证/控制。

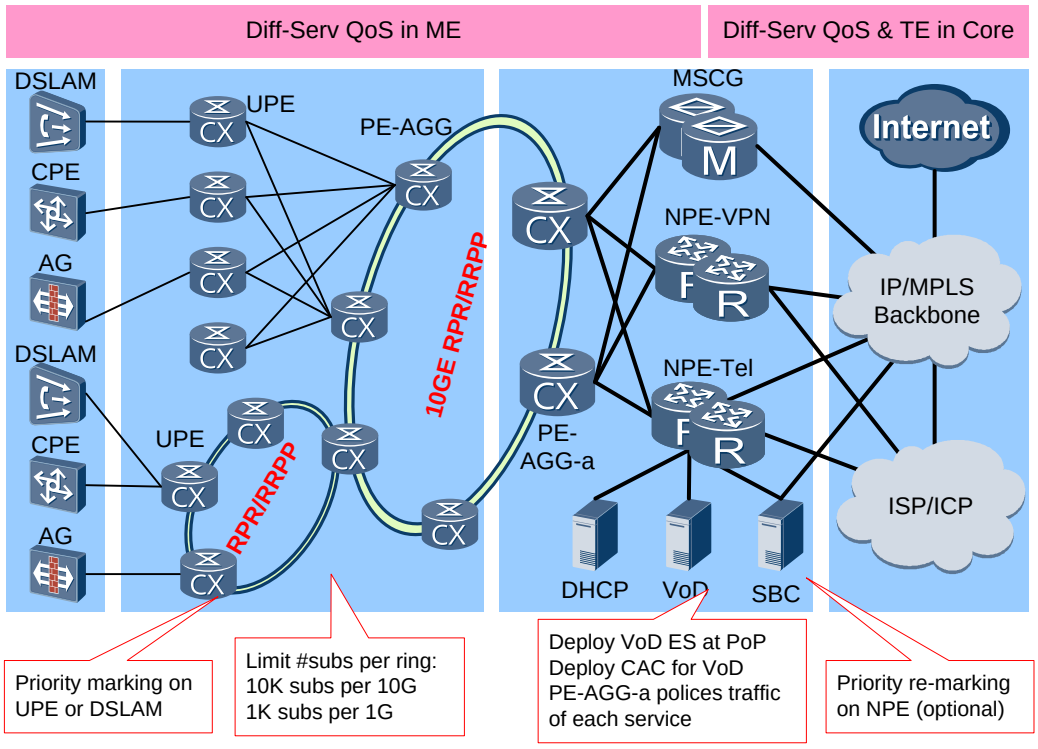
- 用户组+用户+业务级

  企业用户及用户的不同业务配置 CIR/PIR，并且同一个端口下的多个企业用户构成用户组进行带宽保证和控制。

2.7.3 华为 QoS 解决方案

华为城域网 QoS 解决方案如图 2-18 所示。

图2-18 华为城域网 QoS 方案



华为城域网 QoS 方案采用 Diff-Serv 模型，基本思想是在一个资源有限的网络中，通过适当的流分类和优先级处理，可以提供足够的质量保证。

Diff-Serv 模型把提高 QoS 可扩展性、降低实现的复杂性作为出发点。为此，Diff-Serv 模型并不要求获得绝对的质量保证，而是充分考虑了 IP 网络的特点，采用了基于流分类的会聚流处理方式。

DiffServ 模型主要完成以下功能：

- 报文分类
- 报文标记（着色）
- 拥塞管理
- 拥塞避免
- 流量调节，包括流量监管和流量整形
- 以太帧 COS 和 MPLS 报文的 EXP 映射

2.8 安全规划

广域网互联作为企业的业务承载网络，需要承载 VPN、Internet 访问等业务，不可避免的引入了安全隐患，需要采取完善的安全措施，以保护各种重要的增值业务的安全性。

从网络安全角度，首先需要保证设备本身的物理安全，其次保证设备的配置安全和防攻击能力。对于多业务 IP 承载网，最重要的问题是用 VPN 实现不同业务的隔离。

2.8.1 通用安全措施

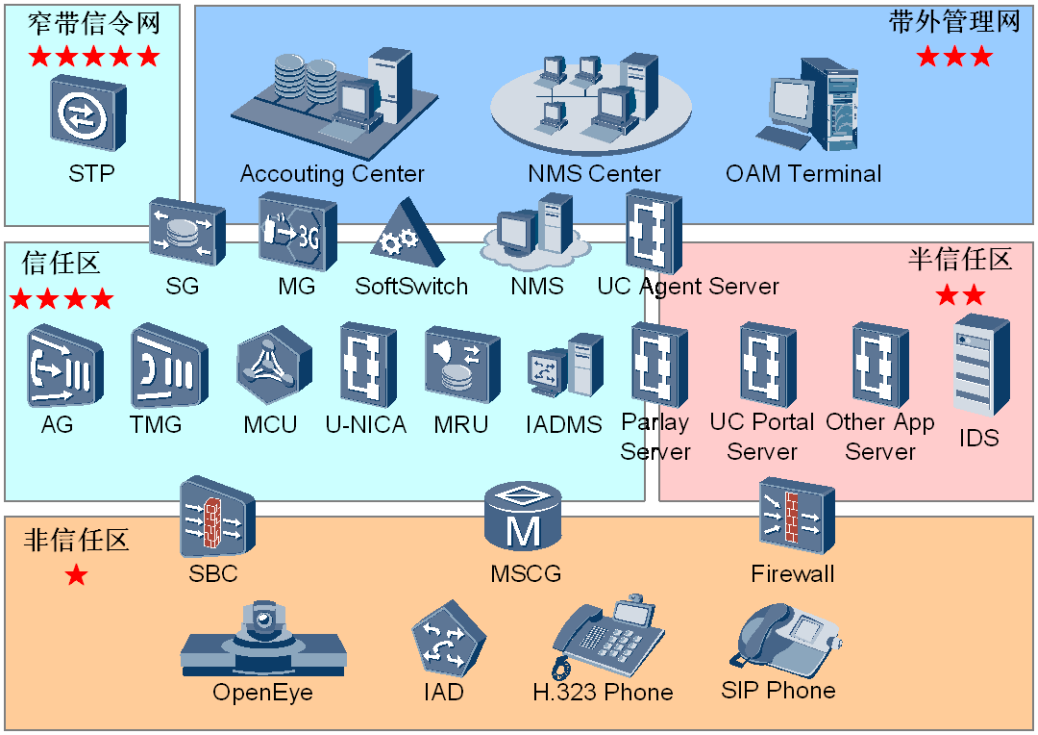
对于广域网来说，采取下列措施可以有效增强网络的安全性：

- 对网络设备的用户和权限进行接入访问控制（ACL）。
- 限制对网络设备的 SNMP 访问和 Telnet 访问。
- 互连设备的相互认证。
- 对路由信息交换进行认证（例如 IS-IS MD 加密认证）。
- 使用 Syslog 对所有重要事件进行记录。
- 采用 NTP 或 PTP 来同步整个网络设备的时钟。

2.8.2 网络安全架构

网络安全架构需要承载设备具备业务区分能力，将不同的业务区分在不同安全级别的区域中，包括非信任区，信任区，半信任区等。不同区域之间通过 FW、SBC 等安全网关设备进行隔离。如图 2-19 所示。（图中的星号表示安全级别）

图2-19 IP 广域网安全架构模型



AG: Access Gateway
IADMS: IAD Management System
MCU: Multipoint Control Unit
MRU: Media Record Unit
NMS: Network Management System
SG: Signaling Gateway
STP: Signaling Transfer Point
U-NICA: Universal Network Intelligent Core Architecture
IAD: Integrated Access Device
IDS: Intrusion Detection System
MG: Media Gateway
MSCG: Multi-Service Control Gateway
SBC: Session Border Controller
SIP: Session Initiation Protocol
TMG: Trunk Media Gateway
UC: Unified Communication

2.9 网络管理规划

传统的 IP 网络和传送网络是由不同的网管系统管理，并且由不同的组织维护，在业务的快速开通和故障定位上存在比较大的问题。例如：

- 当 IP 网络需要增加一个承载波长的时候，传送层可能需要一个多月的时间才能够提供，严重影响了业务的开通和快速上市。
- IP 承载网 80%以上由波分设备承载，当路由器业务发生中断，是 IP 承载网自身的问题还是波分设备的问题，目前缺乏快速有效的定位和隔离手段。
- 当传送设备发生故障时，传送层不清楚该故障是不是影响到 IP 链路，同时具体影响哪些 IP 链路。
- IP 网络运维复杂，承载 IP 的承载关系复杂，配置业务需要多次跳转页面。

运维协同以“以人为本，网络易运维”为主要理念，主要包括 IP 和光网络的融合管理以及承载业务的可视运维。

2.9.1 融合管理

以 U2000 为基础的融合网管系统，可以实现对于 IP 网络和传送网络的融合管理，包括网元融合共管、快速业务发放和故障快速定位等功能。

网元融合共管

U2000 能够对传送设备、接入设备和 IP 设备进行统一管理，可管理华为 MSTP、WDM、OTN、Microwave、Router、Switch、PTN、MSAN、DSLAM、FTTx、Firewall 等设备和业务。

快速业务发放

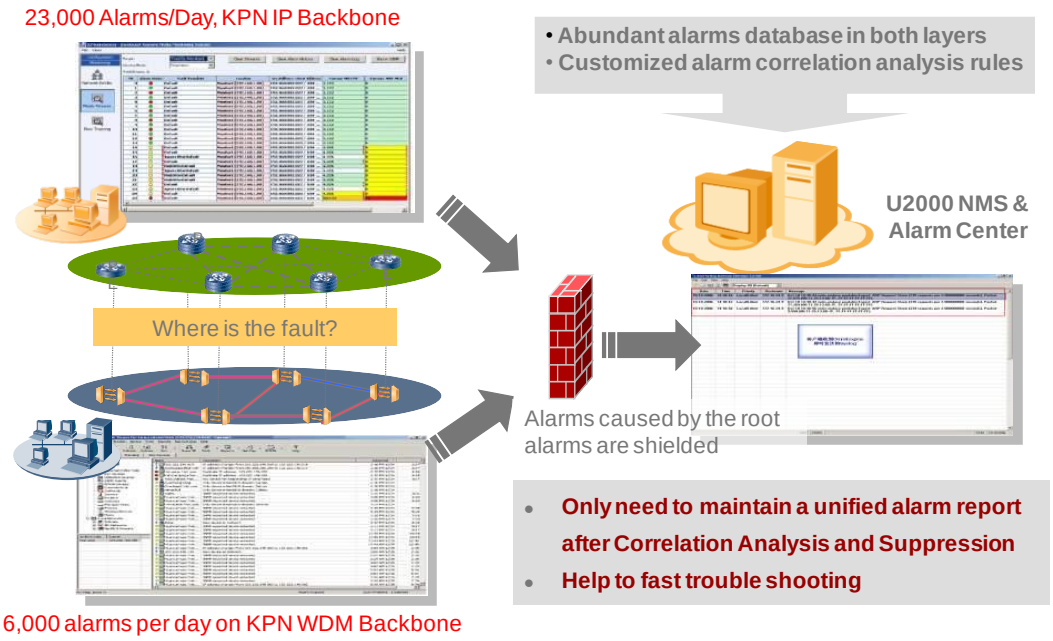
U2000 系统可以实现对于业务的端到端快速发放。U2000 的业务快速发放具有如下特点：

- 通过配置业务模板，例如 Tunnel 模板、L2VPN/ L3VPN/VPLS/PWE3 业务模板、QoS 策略模板等，可实现业务相关参数一站式配置，效率提升 3~6 倍。
- 可批量下发各种业务，提升配置效率，通常效率可提升 2~3 倍。
- 网管系统自动计算静态路由，并实现 MPLS 标签自动分配，0 人工干预。
- 提供跨域的 E2E 业务维护，实现不同技术业务的 E2E 管理，有利于故障的准确定责，精确定位。
- IP＋光的业务层次一键式切换，层次化展示，IP 和 WDM 业务承载关系可视化。

快速故障定位

U2000 可以提供 IP 网络的告警根因分析，通过对 IP 网络的海量告警清理，可以减少 85%的 IP 网络无效告警，提高 IP 域告警的可用性。U2000 可以实现对 IP+光的告警相关性分析和光告警所影响的 IP 链路，如图 2-20 所示。

图2-20 IP+光 告警关联和根因分析



2.9.2 可视运维

由于历史和技术原因，传统的 IP 网络的管理和运维，相比其他网络而言，要困难的多。

- IP 网络的业务路由不可视，没有可视化的直观路径事实展现；
- IP 故障定位困难，排查时间长，很多瞬间故障很难从根本上解决；
- IP 网络承载的业务，客户最终体验不可见，无法管理业务质量。

华为通过可视化运维的 SQM（Service Quality Management）方案，可极大提升 IP 网络的运维能力。SQM 方案通过 IP 业务质量管理系统 U2520 和集成网管系统 U2000 来共同实现。

SQM 方案包括如下的功能和特性：

- IP 网络指标监控

  SQM 可有效监控 IP 网络中各项 KPI 指标参数，例如延迟、抖动、丢包率等等。覆盖各种 IP 网络应用场景，客户体验可度量、可评估、可预警。

- IP 业务 E2E 管理

  SQM 可以针对各种 IP 业务，例如视频、语音、文件传送、生产业务等进行端到端的监控和呈现，故障和业务性能实时监控，现场指导排障。

- IP 路由实时呈现

  SQM 可以对全网的 IGP 路由、LSP 路径等进行实时采集和展示，历史瞬间故障可追踪，彻底解决瞬间故障的顽症。

- IP 故障自动定位

  SQM 基于华为的 IP 故障分析技术，可以实现对于 IP 故障自动定位。只要输入源/目的 IP 地址和源/目的端口，5 分钟内即可自动定位出故障根源。

3 设备介绍

本方案中所涉及的产品和部件如下：

- 核心路由器：NetEngine40E 核心路由器。
- 骨干路由器：NetEngine 80/40 系列通用交换路由器。
- 业务接入路由器：NetEngine20E/20 系列多业务路由器。

3.1 NetEngine40E 核心路由器

3.1.1 概述

NetEngine40E 系列核心路由器（以下简称 NE40E）是华为公司推出的高端网络产品，广泛适用于 IP 国干网、IP 省干以及其他各种大型 IP 网络的核心、汇聚层。

NE40E 基于分布式的硬件转发和无阻塞交换技术，采用华为自主研发的 Solar 系列芯片，具有良好的线速转发性能，优异的扩展能力，完善的 QoS 机制和强大的业务处理能力。NE40E 基于最新的可扩展 400G 平台，实现 40G/Slot 到 400G/Slot 的平滑扩展，且兼容现网所有线卡，最大限度保护客户的投资。

NE40E 具有强大的汇聚接入能力。凭借丰富的特性支持，可以灵活部署 L2VPN、L3VPN、组播、组播 VPN、MPLS TE、QoS 等，实现业务运营级的可靠性承载。同时 NE40E 全面支持 IPv6，可以实现 IPv4 到 IPv6 的平滑过渡。

NE40E 可以灵活应用在 IP/MPLS 网络的核心、汇聚，可以简化网络结构，提供丰富的业务类型和可靠的服务质量，是 IP/MPLS 网络向宽带化、安全化、业务化、智能化发展的重要源动力。

3.1.2 产品型号

NetEngine40E 核心路由器的产品型号如下。

表3-1 NetEngine40E 核心路由器系列产品型号

产品型号	描述
NE40E-X16	支持 16 块 LPU 交换网容量 12.58T（双向） 背板容量 30Tbit/s 转发能力 3200Mpps
NE40E-X8	支持 8 块 LPU 交换网容量 7.08T（双向） 背板容量 15Tbit/s 转发能力 1600Mpps
NE40E-X3	支持 3 块 LPU 交换网容量 1.08T（双向） 背板容量 1.35T 转发能力 300Mpps
NE40E-8	支持 8 块 LPU 交换网容量 640G（双向） 背板容量 2Tbit/s 转发能力 400Mpps

图3-1 NE40E-X16 外观图

图3-2 NE40E-X8 外观图

图3-3 NE40E-X3（直流）外观图

图3-4 NE40E-X3（交流）外观图

图3-5 NE40E-8 外观图

3.1.3 产品特点

400G 路由平台

NE40E 是目前业界最强的 400G 平台路由器，满足未来至少十年的发展需求。

- 最紧凑，端口密度最大，最高密度 1320*GE/机柜，达到业界 2 倍。
- 最绿色的 400G 平台，每 GE 端口功耗不到 9W，低于业界 10%。
- 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

NE40E 的全业务承载能力业界领先，可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。
- 业界最完整的 HQoS 解决方案，支持 HQoS、DS-TE、MPLS HQoS，保证多场景的 QoS 部署。

高可靠性

NE40E 提供完善的端到端可靠性解决方案，可保证业务不中断。

- 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 系列增强保护技术，保证业务端到端 200ms 保护倒换。

3.1.4 产品规格

表3-2 NE40E 系列产品主要指标/规格

指标/规格	NE40E-X16	NE40E-X8	NE40E-X3	NE40E-8
交换容量	12.58T（双向）	7.08T（双向）	1.08T（双向）	640G（双向）
转发性能	3200Mpps	1600Mpps	300Mpps	400Mpps
背板带宽	30T	15T	1.35T	2T
端口容量（双向）	3.2Tbps（双向）	1.6Tbps（双向）	240G（双向）	320G（双向）
业务槽位数	16	8	3	8
宽度（mm）	442	442	442	442
深度（mm）	770	770	750	669
高度（mm）	1420	620	直流机箱：175 交流机箱：220	886

指标/规格	NE40E-X16	NE40E-X8	NE40E-X3	NE40E-8
高度（U）	32U	14U	4U	20U
重量(满配）	267kg	130kg	直流机箱：41kg 交流机箱：51kg	147kg
最大功率	6500W	3300W	1100W	2200W

3.2 NetEngine80/40 系列通用交换路由器

3.2.1 概述

NetEngine 80/40 系列通用交换路由器（以下简称 NE80/NE40），采用分布式网络处理器技术和无阻塞交换 技术，具备优异的扩展能力，全面支持 IPv6，具备高速接口的线速转发能力、完善的 QoS 机制和运营级的可靠性。

NE80/NE40 融合核心路由器强大的 IP 业务处理能力和二层以太交换能力，可提供更丰富的业务、更灵 活的组网和更理想的性价比，主要应用在 IP 骨干网、IP 城域网以及各种大型 IP 网络的核心位置，是华为公司面向大型 企业网和行业网的高端网络产品。

3.2.2 产品型号

NE80/40 系列的产品型号如下。

表3-3 NE80 系列产品型号

产品型号	描述
NE80	支持 16 块 LPU 交换网容量 128G（双向） 转发能力 96Mpps
NE40-8	支持 8 块 LPU 交换网容量 128G（双向） 转发能力 48Mpps
NE40-4	支持 4 块 LPU 交换网容量 128G（双向） 转发能力 24Mpps
NE40-2	支持 2 块 LPU 交换网容量 16G（双向） 转发能力 12Mpps

图3-6 NE80 外观图

图3-7 NE40-8 外观图

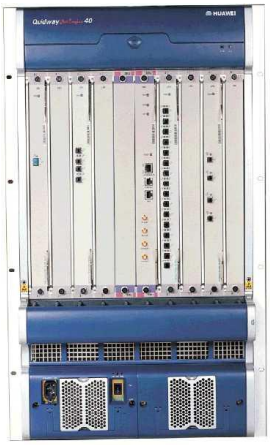


图3-8 NE40-4 外观图

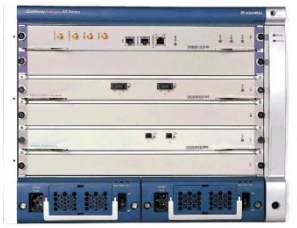


图3-9 NE40-2 外观图

3.2.3 产品特点

广泛部署、稳定应用

NE80/40 是广泛部署、稳定应用的经典之作。

- 大规模成熟商用 9 年，全球发货 15000 余套。
- 多年零质量事故，越用越放心。

全业务承载

NE80/40 是全系列多业务产品，可灵活满足企业客户需求。

- 16/8/4/2 槽位全系列产品，灵活满足客户不同场景需求。
- 全面的隧道、VPN、组播、NAT 等多业务能力，业务处理游刃有余。
- 集路由交换一体，提供高性价比的解决方案。

高可靠性

NE80/40 提供完善的端到端可靠性解决方案，可保证业务不中断。

- 设备级、网络级、业务级全方位的可靠性技术。
- 关键部件冗余备份，支持热补丁。
- 层次化的 HQoS，灵活保障业务质量。

3.2.4 产品规格

表3-4 NE80/40 系列产品主要指标/规格

指标/规格	NE80	NE40-8	NE40-4	NE40-2
交换容量	128Gbps	128Gbps	128Gbps	16Gbps
转发性能	96Mpps	48Mpps	24Mpps	12Mpps
业务槽位数	16	8	4	2
宽度（mm）	600	482.6	482.6	482.6
深度（mm）	800	420	420	420
高度（mm）	2200	797.3	352.8	219.5
高度（U）	46U	18U	8U	5U
重量(满配）	小于 400kg	小于 85kg	小于 50kg	小于 35kg
最大功率	小于 1800W	小于 1000W	小于 600W	小于 300W

3.3 NetEngine20E/20 系列多业务路由器

3.3.1 概述

NetEngine20E/20 系列路由器（以下简称 NE20E/20）是华为公司自主研发的通用高性能第五代多业务路由器。NE20E/20 采用 NP 硬件技术实现，具有卓越的转发性能。

NE20E/20 系列路由器旨在满足企业网汇聚和运营商边缘的电信级高可用性的要求。以其高性能、多业务、双主控和热备份优势，进行业务运营和支撑网络的建设。NE20E/20 具有很强的可伸缩性、可配置性，支持多种接口和业务特性，将 MPLS、VPN、QoS、流量工程、组播等技术融合起来。

在组网应用方面，NE20E/20 系列路由器作为高性能汇聚设备提供全面的业务处理能力，提供全方位的、灵活的网络解决方案，有效提高了网络价值并节约了网络建设成本。

3.3.2 产品型号

NE20E/20 系列路由器按业务槽位数可分为 NE20E-8、NE20-8、NE20-4、NE20-2 四款产品，NE20E 是 NE20 的增强型产品。

NE20E/20 系列的产品型号如下。

表3-5 NetEngine40E 核心路由器系列产品型号

产品型号	描述
NE20E-8	支持 8 块 LPU 交换网容量 16Gbps（双向） 转发能力 6Mpps
NE20-8	支持 8 块 LPU 交换网容量 8G（双向） 转发能力 4.5Mpps
NE20-4	支持 4 块 LPU 交换网容量 8G（双向） 转发能力 4.5Mpps
NE40-2	支持 2 块 LPU 交换网容量 8G（双向） 转发能力 3Mpps

图3-10 NE20E-8 外观图

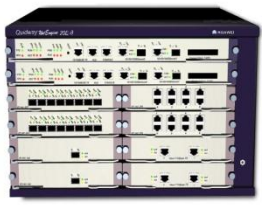


图3-11 NE20-8 外观图

图3-12 NE20-4 外观图

图3-13 NE20-2 外观图

3.3.3 产品特点

稳定成熟应用

NE20E/20 是多年成熟稳定应用的经典路由器。

- 大规模成熟商用 8 年，全球发货 10000 余套。
- 多年零质量事故，表现优异。

多业务接入和汇聚能力

NE20E/20 是全系列多业务产品，可灵活满足企业客户需求。

- 强大的汇聚能力，ATM、CPOS、CE1 等接口线速汇聚（可汇聚 96 个线速 E1/T1）。
- 强劲的安全隧道能力，IPSec 硬件加密，GRE、L2TP、NAT 性能灵活优异。
- 全面的路由处理能力，全面支持各种单播和多播路由协议。

高可靠性

NE20E/20 提供完善的端到端可靠性解决方案，可保证业务不中断。

- 业界首款控制引擎与转发引擎双备份设备，提供高品质业务保障。
- 设备级、网络级、业务级全方位的可靠性技术，保证网络运行高速可靠。
- 层次化的 HQoS，灵活保障业务质量。

3.3.4 产品规格

表3-6 NE20E/20 系列产品主要指标/规格

指标/规格	NE20E	NE20-8	NE20-4	NE20-2
交换容量	16Gbps	128Gbps	128Gbps	16Gbps
转发性能	6Mpps	48Mpps	24Mpps	12Mpps
业务槽位数	8	8	4	2
宽度（mm）	436.2	436.2	436.2	436.2
深度（mm）	480	420	420	420
高度（mm）	261	219.5	130.5	130.5
高度（U）	6U	5U	5U	3U
重量(满配）	32.5kg	27.5Kg	17.5Kg	15Kg
最大功率	350W	320W	240W	240W