

## 摘要

网络中任何资源都有可能发生故障,为了提供一个高可靠性的网络,MPLS 故障恢复机制能在网络故障发生后,快速进行修复。随着实时业务在网络中的大量应用,MPLS 故障恢复机制已成为当前研究热点,同时也是下一带网络发展的技术基础。快速重路由技术是 MPLS 故障恢复机制的核心技术,本文以此为研究对象,提出了一种基于备份资源信息共享和带宽约束路由算法的优化方案,并进行了仿真实验实现和验证。论文具体的研究内容与研究工作包括以下三个方面:

(1) MPLS 故障恢复机制中快速重路由技术的研究,主要为经典快速重路由方案的研究分析。目前著名的快速重路由方案有 Makam 方案、Haskin 方案以及 RSVP 方案,其它故障恢复方案都是在此基础上发展的。Makam 方案和 Haskin 方案存在一个共同的缺陷,即当故障点离恢复切换点较远时会出现问题, Makam 方案会产生较大的丢包率, Haskin 方案会产生包失序和较大的时延,同时这三种方案均存在备份路径资源的闲置,从而造成了网络带宽资源的重复消耗。

(2) 基于备份资源信息共享的快速重路由优化方案研究和实现,该方案在继承经典方案良好的恢复性能同时提高网络带宽资源利用率。论文针对经典快速重路由方案共同存在的备份带宽资源浪费问题,提出了一种优化方案,该方案包含两个方面内容:一为优化的备份资源信息共享机制,该机制通过使网络中的关键节点掌握有限范围内的节点与链路的相关信息,实现备份资源在网络中全局性的共享;二为优化的备份路径选择算法,该算法基于经典最短路径算法,通过在链路权重中添加带宽的限制,优先选择备份资源带宽大的链路,可进一步降低对网络预留资源的需求。

(3) 优化方案的仿真实验实现和验证。论文搭建了针对 MPLS 快速重路由的 OPNET 网络仿真平台,建立仿真网络模型,设置仿真参数,配置运行仿真,应用对比方法,从丢包率、业务流切换时间、网络资源利用率三方面对所提出的方案与现有方案进行了对比分析。仿真结果证明新方案相比 Makam 方案、Haskin 方案具有更低的丢包率及更低的业务流切换时间,同时在网络资源利用率上相比 RSVP 方案具有更优的性能,有效减少备份资源的消耗,提高网络资源利用率。

**关键词:** 多协议标签交换; 快速重路由; 流量工程; 故障恢复

## ABSTRACT

Any resources of network might go wrong. For providing networks with sufficiently high reliability, MPLS-based Fault Recovery mechanism with rapid restoration capacity is executed in Network. Recently, as more and more real-time service applications of network, MPLS-based Fault Recovery has became a hot spot, and also technical basis of NGN. This paper proposed a optimization Fast Reroute scheme based on optimized backup resources information sharing mechanism and bandwidth-constrained routing by studying of FRR, the core technology of MPLS-based Fault Recovery. The main research contents and works of this paper include the following two aspects:

(1)Research on Fast Reroute of MPLS-based Fault Recovery, focus on the classical Fast Reroute schemes. Recently, the most famous FRR schemes include Makam、Haskin and RSVP, other schemes are all on the basis of those famous schemes. Makam and Haskin have a common drawback, that is a lot of problems appear when Point of Switch is far away from the place faults occur. Makam scheme has a great of packets lost, while Haskin scheme has very high delay and leads packets disorder. Meanwhile, those three famous schemes have a drawback in common, that is idle backup path cause large amount of waste in bandwidth resources.

(2)Proposed a optimization Fast Reroute scheme. Inheriting better rapid restoration ability of classical schemes and effectively improving the utilization of network resources. After study and analysis of classical schemes, aiming at the problem of waste in backup bandwidth resources in common, proposed a optimization Fast Reroute scheme called OFRR, it contains two other aspects, one is optimized backup resources information sharing mechanism, it achieves efficient sharing of backup resources information by making key nodes of backup path know the available information of links and routes in that rage. This solution allows bandwidth

global sharing. The other side is optimized backup path selecting algorithm based on the classical SPF algorithm, it selects the link with more backup bandwidth resources as priority by adding limitation of bandwidth to the link weight. Farther achieving reduction of network reservation bandwidth resources.

(3) Demonstration and implementation of optimization scheme simulation experiment. Build the OPNET network simulation platforms, includes construction of network simulation model, setting of simulation parameter, configuration and run of simulation. Simulate Makam、Haskin、RSVP、OFRR those schemes in packet loss rate, switching time of traffic stream and utilization of network resources by comparing method. Simulation results show that OFRR can reduce packet loss rate and switching time of traffic stream compared with Makam and Haskin scheme. Comparing with RSVP scheme, OFRR has less backup resources consumption, effectively improves the utilization of network resources.

**Keywords:** MPLS; Fast Rerouting; Traffic Engineering; Fault Recovery

# 江苏大学学位论文版权使用授权书

## 学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权江苏大学可以将本学位论文的全部内容或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

保 密 ，在 年解密后适用本授权书。

本学位论文属于

不保密 。

学位论文作者签名: 

2010年6月11日

指导教师签名: 

2010年6月11日

## 独 创 性 声 明

本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已注明引用的内容以外，本论文不包含任何其他个人或集体已经发表或撰写过的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

学位论文作者签名： 陈林

日期：2017年6月11日

# 第一章 绪论

## 1.1 课题研究背景与意义

近年来，伴随着互联网（Internet）的蓬勃发展，出现了“Everything over IP”的局面。话音、数据及图像等各种业务均能在 IP 网上进行传输，IP 业务成为通信业务的主流。但由于 IP 协议是无连接协议，不能保证足够的吞吐量和符合要求的传送时延，只能尽最大努力（Best effort）来满足用户的需要，所以出现服务质量难以保证、路由器成为瓶颈等问题。随着网络数据业务量和用户量的急速增长，对信息和网络依赖程度日益增大，网络可靠性问题逐渐凸显。目前，Internet 上开展的实时业务对网络失效后的快速恢复提出了尖锐的挑战，提供连续可靠的网络操作已成为流量工程的一项重要目标。因此，网络应当提供业务保护和恢复机制，保证网络在发生故障时不会对数据流的传送造成大的影响。传统 IP 网络依靠动态路由协议来实现网络故障恢复，当节点或链路发生故障时，IGP 协议把拓扑变化扩散给各路由器，网络收敛后，路由器通过使用 SPF 算法更新路由表就能将业务流绕过故障点传输到目的地，整个收敛过程需要秒级甚至上分钟时间。对于目前的实时业务而言，一致认同的最大故障恢复时间应该在 50ms 左右，而传统的 IP 网络故障恢复耗时太长，显然不能满足实时业务的要求。

多协议标签交换（Multi-Protocol Label Switching, MPLS）<sup>[1]</sup>是一种在开放的通信网上利用标签引导数据高速、高效传输的新技术。MPLS 能以无连接或显式路由的方式提供面向连接的业务。作为下一代核心网络的主要技术，MPLS 通过标签交换<sup>[2]</sup>机制，不仅可以提供比传统 IP 更有效的 QoS 保证和流量工程，而且具有很强的网络生存性能力。MPLS 的保护机制在网络故障发生以后，可比 IP 层提供更快的反应时间。MPLS 能够在保证在 50ms 时间内恢复故障。简单而言，在一个 MPLS 网络中修复故障的关键目的就是尽可能地缩短故障引起的网络数据传输中断的时间。如果可能的话，建立起来的标签交换路径（可能正在传输数据）应该能不中断的进行故障恢复。这就意味着链路以及交叉连接的设备应该不会受到故障的影响，并且很少有数据丢失。为了实现这个目的，很多 MPLS 故障恢复方案被提出并有效地解决了网络故障恢复中的若干问题。同时 MPLS 故障恢复机制可

以选择保护流量的类型并且能提供非常灵活的保护流量颗粒度。

## 1.2 课题国内外研究现状

1997 年, 互联网工程任务组 (IETF) 专门成立了 MPLS 工作组, 负责开发和制定有关 MPLS 的标准。目前形成的标准草案主要关于 MPLS 技术的基本实现, 包括标签的定义及编码、标签分发协议规范、MPLS 体系机构、MPLS 基本应用等。

目前, MPLS 工作组的工作重点已经从原理技术的基本实现转移到 MPLS 技术的应用中来, 主要面向 MPLS 如何更有效地提供增值服务, MPLS 在局域网中的应用、MPLS 与光传输网的融合、MPLS 流量工程技术的具体应用等。在故障恢复方面, MPLS 作为未来骨干网的核心技术, 其故障恢复机制对于保证整个网络的运作以及保证关键应用的 QoS 至关重要, 因此 MPLS 工作组将 MPLS 故障恢复机制作为重要研究目标之一。目前 IETF RFC3469 已规定了 MPLS 故障恢复的框架, 定义了故障恢复中一些基本概念、基本类型以及基本原则等, 但具体的实现机制、策略、方案, 多层修复, 跨不同网络的故障恢复以及各种不同的算法仍在研究之中。

国外方面, 目前已提出了各种具体 MPLS 故障恢复方案。Kini 等提出了使用共享的备份 LSP 进行故障恢复的多种模型。Makam 等提出通过在发生故障时向上游发送故障指示信号将流量切换到备份 LSP 实现故障恢复的方案。Haskin 等提出在建立备份 LSP 时构成回路实现快速恢复, 降低丢包率。Rabbat 等在研究 MPLS 区分服务的基础上提出根据不同类别和优先级进行故障恢复的方案。Chen 等研究了修改 LDP 消息的分布式快速故障恢复方法。在对目前方案研究总结的基础上, Sharma 等给出了 MPLS 故障恢复机制的框架。Awduchets 等将 MPLS 故障恢复机制分为链路保护、节点保护、路径保护和网段保护 4 种类型, 分析了 LSP 信道属性的恢复属性, 并根据备份 LSP 和保护 LSP 的数量分析了几种选项。为了使 MPLS 中的信令协议支持故障恢复, Hellstrand 等扩展了 CR-LDP 和 RSVP-TE 信令协议, Owens 等扩展了 RSVP-TE 信令协议, 使其支持建立备份 LSP 并可在 LSP 发生故障时传播故障指示信号。仿真实验方面, Srikitja 等通过扩展网络仿真器 NS 对两种故障恢复机制, 即为每个 QoS 连接事先建立可共享的备份路径和仅在收到故障通知时进行动态恢复作了性能比较。

国内方面, 近年来也有很多关于 MPLS 故障恢复机制的研究。主要有: 王勤

民等基于链路监控的 MPLS 保护机制的研究；杨天乐，杨爱英关于 MPLS 网络中 M:N 方式保护与恢复方案的研究；黄维华针对 MPLS 网络的可靠性及恢复机制进行了研究；常新杰等有关 MPLS 网络中的故障保护措施的研究；黄河等针对故障恢复与区分服务相结合的故障恢复模型的相关研究；袁泉等有关 MPLS 网络中错误恢复机制的研究与分析；朱树人等进行了基于 MPLS-DiffServ 流量工程的故障恢复模型的相关研究；许先斌研究了基于 MPLS 快速重路由机制的故障恢复方案等等。

MPLS 作为未来骨干网的核心技术，发展很快，其故障恢复机制能够保证整个网络的运作以及保证关键应用的服务质量 QoS，因此 MPLS 工作组将 MPLS 故障恢复机制作为了一项重要研究目标。

### 1.3 论文研究内容与研究工作

MPLS 快速重路由作为 MPLS 故障恢复机制的核心技术，能够在网络发生故障时实现快速恢复，保证 50ms 内的切换速度，减少由于网络失效而导致的长时间流量转发中断。目前各种快速重路由方案相继被提出，其中经典方案有 Makam 方案、Haskin 方案以及 RSVP 方案，其它方案都是在此基础上发展的。论文分析总结了经典方案各自的优点与局限性，具体针对各方案所具有的一个共同的缺陷，即备份带宽资源大量浪费的现象，提出一种快速重路由优化方案，该方案包含两方面的内容，一为优化的备份资源信息共享机制，该机制通过使网络中的关键节点掌握有限范围内的节点与链路的相关信息，实现备份资源在网络中全局性的共享；二为优化的备份路径选择算法，该算法基于经典最短路径算法，通过在链路权重中添加带宽的限制，优先选择备份资源带宽大的链路，可进一步降低对网络预留资源的需求。本文具体研究内容与研究工作如下：

(1) MPLS 及其故障恢复机制的研究。论文研究了 MPLS 技术，简要介绍 MPLS 基本原理、技术特点以及关键技术应用，同时对 MPLS 流量工程技术进行相关研究，简要介绍 MPLS 流量工程的概念、技术特点以及技术优势。详细研究并介绍了 MPLS 故障恢复机制，内容包括 MPLS 故障恢复机制的基本思想、技术术语，并针对目前国内外研究现状对 MPLS 故障恢复机制进行了分类，详细描述了各分类的特点与局限性。

(2) MPLS 快速重路由及其经典方案的研究。MPLS 快速重路由 FRR 作为 MPLS

故障恢复机制的核心技术，论文集中对其进行了研究，分析了 FRR 技术相比传统故障恢复技术所具有的优势。研究比较了几种 FRR 保护模式，FRR 技术分为路径保护以及局部保护两种保护模式，局部保护又可以分为链路保护和节点保护。路径保护是采用集中化管理系统来实施故障恢复，局部保护是由检测到故障的上游节点直接发起恢复，恢复的过程是局部的。经典 FRR 方案有 Makam 方案、Haskin 方案以及 RSVP 方案，论文对各方案分别进行研究，分析比较了各方案的优点与缺点。Haskin 方案优点是丢包少，缺点是恢复路径较长导致时延较高同时极易造成分组失序。Makam 方案优点是分组失序少，缺点在于故障信息的传播会导致时延较高同时造成较大数目的丢包。RSVP 方案优势是丢包率小同时故障恢复快，缺点是备份路径闲置造成大量带宽资源浪费。分析结果说明各方案均具有一个共同的缺陷，即备份资源利用率低，造成了极大的网络带宽资源耗费。

(3) 提出一种快速重路由优化方案。论文在对经典快速重路由方案研究的基础上，具体针对所存在的备份带宽资源浪费的问题，提出一种快速重路由优化方案，即 OFRR 方案，该方案包含两个方面内容：1. 优化的备份资源信息共享机制，通过使备份路径中的关键节点掌握有限范围内的节点与链路的相关信息，实现对备份资源的有效共享管理，可以支持备份带宽资源在网络中全局性共享；2. 优化的备份路径选择算法，该算法基于经典最短路径算法 Dijkstra 算法，通过在链路权重中添加带宽资源的限制，优先选择预留带宽资源大的链路，可进一步降低对网络预留资源的需求。

(4) 仿真试验实现与验证。论文搭建了针对 MPLS 快速重路由的 OPNET 网络仿真平台，建立仿真网络模型，设置仿真参数，配置运行仿真，应用对比方法，对原有方案以及 OFRR 方案进行了仿真，仿真结果表明 OFRR 方案在故障恢复期间具有更好的恢复性能，OFRR 方案相比 Haskin 方案、Makam 方案具有更低的丢包率及更低的服务中断时间，同时在网络资源利用率上比 RSVP 方案具有更优的性能，有效减少了备份资源的消耗，提高网络资源利用率。

## 1.4 论文组织结构

论文共分六章，各章节的具体安排如下：

第一章：绪论。简要描述了课题的研究背景、选题意义、国内外发展现状以

及本文主要的研究内容与研究工作以及具体章节安排。

第二章：分别对 MPLS 及其故障恢复机制进行相关研究与介绍。本章首先简要描述 MPLS 技术的工作原理、技术术语、技术特点以及关键技术应用，然后针对其应用方面引出流量工程，概述了流量工程的必要性以及 MPLS 流量工程相对于传统流量工程所具有的技术特点以及技术优势。接着，简要叙述了 MPLS 故障恢复机制的基本思想、技术术语同时根据目前对该机制的研究现状对其进行分类并简要描述了各分类的特点与局限性。最后是对本章内容的总结。

第三章：主要研究介绍 MPLS 快速重路由技术及其经典方案。首先，针对 MPLS 故障恢复机制中的核心技术，即 MPLS 快速重路由 FRR 技术进行相关研究。FRR 分为路径保护以及局部保护两种模式，其中局部保护还可分为链路保护以及节点保护，本章分别对这几种保护模式进行详细描述。接着，介绍了目前经典 FRR 方案，在对经典 FRR 方案进行研究基础上，分析总结了各自的优点与缺点并分别进行了详细叙述。最后是对本章内容的总结性概述。

第四章：提出一种 MPLS 快速重路由优化方案。本章，首先简要回顾了经典快速重路由方案的特点与局限性。具体针对共同存在的备份资源浪费问题，提出一种 MPLS 快速重路由优化方案（OFRR 方案）。该方案包含两方面的内容，即优化的备份资源信息共享机制以及优化的备份路径选择算法。本章具体针对这两方面对 OFRR 方案进行了详细描述。最后，对新方案在可扩展性以及网络资源利用率两方面进行了分析与评价。

第五章：仿真实验实现与结果分析。本章主要基于 OPNET 软件搭建出网络仿真平台，设置仿真参数，应用对比方法，对 Makam 方案、Haskin 方案、RSVP 方案与本文所提出的新方案做了丢包率、业务流切换时间和网络资源利用率三方面的仿真，根据仿真曲线对其性能进行了比较分析，得出本文的结论。

第六章是全文总结与展望。对全文的工作与成果做了总结，并对未来工作做出了展望。

## 第二章 MPLS 故障恢复机制相关研究

为了提供更多、更稳定、更有效率的网络环境，在新一代骨干网络中引进了 MPLS<sup>[3]</sup>技术，该技术萃取了 ATM 快速交换的精神，并能很好地与目前最普遍的 IP 网络环境相整合。提供的显式路由技术使得流量工程可以方便在 IP 网络中实施，为流量工程实施提供了一种新的途径。

目前，随着网络上应用越来越多，网络必须能够在故障发生时保证其连续性和服务质量。传统的方法是由内部网关协议 IGP<sup>[4]</sup>负责在发生失效时，对剩余拓扑进行汇聚，快速产生路由。但是，由于 IGP 协议需要相当长的几秒钟时间进行汇聚，造成分组大量丢失、延时过长，甚至发生网络拥塞。使用 SONET 的 IP 网络可以使用自动保护切换 APS 机制将流量切换到备用链路，实现快速恢复。但是，APS 直接在路由器上运行，IGP 需要针对链路另一段的新邻居进行汇聚，因此在新的 IGP 邻居启动之前，仍然会有重大流量丢失。APS 还带来附加成本，即实现 APS 的增/减复用器 ADM 的硬件成本。MPLS 故障恢复机制是 MPLS 流量工程的一种重要应用特性，能够保证发生故障时在期望的时间内恢复数据传输，同时在恢复后能够保持所需的 QoS。

### 2.1 MPLS 技术简介

各种网络通讯服务对网络性能的要求越来越高，要求网络能够传输语音、图像，要求传输速度快，延时少，要求网络具有很好的 QoS 性能等等。MPLS 结合了第二层的高速交换能力和第三层的灵活特性，使 IP 网具备高速交换、流量控制、QoS 等性能，更好地满足网络各种业务的需求。

#### 2.1.1 MPLS 技术工作原理

MPLS 是一个可以在多种第二层媒质上进行标签交换的网络技术。这一技术结合了第二层交换和第三层路由的特点，将第二层的基础设施和第三层的路由有机结合起来。在 MPLS 网络的边缘实施第三层的路由，而在网络核心采用第二层交换。MPLS 通过在每一个节点的标签交换来实现包的转发。MPLS 允许不改变现有

的路由协议，同时可以在多种第二层物理媒质上实施，如 ATM、FR、Ethernet 以及 PPP。

MPLS 是一种特殊的转发机制，它为进入网中的 IP 数据包分配标签，并通过对标签的交换实现 IP 数据包的转发。标签作为 IP 包头在网络中的替代品而存在，在网络内部 MPLS 在数据包所经过的路径沿途通过交换标签来实现转发，当数据包要退出 MPLS 网络时，数据包被解封装，继续按照 IP 包的路由方式到达目的地。

如图 2-1 所示为一个基本的 MPLS 网络，在该网络中，包含一些基本的元素。网络边缘的节点叫做标签边缘路由器（LER），网络的核心节点称为标签交换路由器（LSR）。LER 节点在 MPLS 网络中完成的是 IP 包的进入和退出过程；LSR 节点在网络中提供高速交换功能。MPLS 节点之间的路径称为标签交换路径（LSP）。一条 LSP 可以看成是一条贯穿网络的单向隧道。

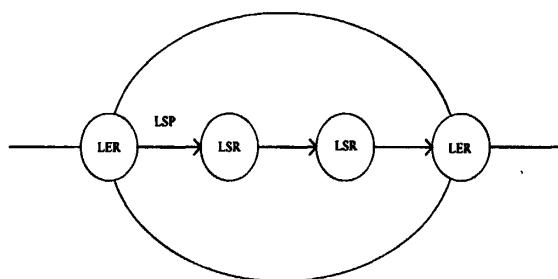


图 2-1 MPLS 网络基本模型图

MPLS 工作流程可以分为几个方面，即网络的边缘行为、网络的中心行为以及标签交换路径的构建。

网络的边缘行为：当 IP 数据包到达一个 LER 时，MPLS 第一次应用标签。首先，LER 要分析 IP 包头的信息，并且按照它的目的地址和业务等级加以区分。在 LER 上，MPLS 使用转发等价类（FEC）这一概念来将输入的数据流映射到一条 LSP 上去。简单而言，FEC 就是定义了一组沿着同一条路径，有相同处理过程的数据包。这就意味着所有 FEC 相同的包都可以映射到同一个标签中。对于每一个 FEC，LER 都建立一条独立的 LSP 穿过网络，到达目的地。数据包分配了一个 FEC 后，LER 就可以根据标签信息库（LIB）来为其生成一个标签。LIB 将每一个 FEC 都映射到 LSP 下一跳的标签上。如果下一跳的链路是 ATM 的话，则 MPLS 将使用 ATM VCC 里的 VCI 作为标签。转发数据包时，LER 检查 LIB 中的 FEC，然后将数据包用 LSP

的标签封装，从 LIB 所规定的下一个接口发送出去。

网络的核心行为：当一个带有标签的包到达 LSR 时，LSR 提取出局标签，同时以它作为索引在 LIB 中查找。当 LSR 找到它的相关信息后，取出出局的标签，并由出局标签替代出局标签，从 LIB 中所描述的下一跳接口送出数据包。最后，数据包到达了 MPLS 域的另外一端，在这一点，LER 剥去封装的标签，仍然按照 IP 包的路由方式将数据包继续传送到目的地。

标签交换路径构建：建立 LSP 的方式主要有两种，一种是以 Hop-by-Hop 路由方式建立 LSP；另外一种就是以显式路由方式建立 LSP。第一种方式所建立的 LSP 是所有从源节点到一个特定目的节点的 IP 树的一部分。对于这些 LSP，MPLS 模仿 IP 转发数据包的那种面向目的地的方式建立了一组树。不同于传统的 IP 路由，每一跳路由器都要检查包的目的地址，并且选择一条合适的路径将数据包发送出去，MPLS 中，数据包虽然也沿着 IP 路由所选择的同一条路径进行传送，但是它的数据包头在整条路径上从始至终都没有被检查。在每一个节点，MPLS 生成的树是通过一级一级为下一跳分配标签，并与它们的对等层交换标签而生成的。交换是通过标签分配协议（LDP）的请求以及对应的消息完成的。第二种方式构建 LSP 不同于 Hop-by-Hop 路由方式，显式路由方式不会形成 IP 树。而是从源端到目的端建立一条直接的端到端的路径，MPLS 允许网络的运行人员在源节点就确定一条显式路由的 LSP，以规定数据包将选择的路径。其最大的优点就是可以利用流量设计“引导”数据包，从而可以避免拥塞或者满足业务的 QoS 等。

MPLS 是一种使用 IP 路由信息基于标签交换的技术。在 MPLS 中定义了一些相关技术术语，以下是对一些关键性术语的简要介绍：

（1）多协议。MPLS 位于传统的第二层和第三层协议之间，其上层协议与下层协议可以是当前网络中的各种协议。如：第三层协议 IPv4，IPv6，IPX 等，第二层协议 ATM，FrameRelay，Ethernet 等。图 2-2 为 MPLS 协议栈示意图。

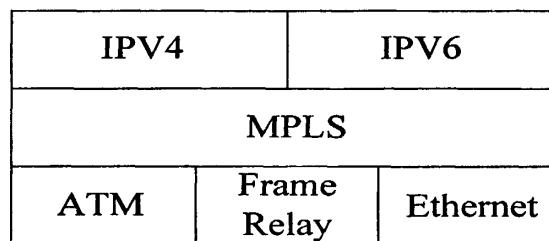


图 2-2 MPLS 协议栈示意图

(2) 标签 (Label)。是一个比较短的, 定长的, 非结构化的, 通常只具有局部意义的标识。这些标签通常位于数据链路层的数据链路层封装头和协议数据单元 (Protocol Data Unit, PDU) 之间, 用来提高数据分组的分发性能, 标签通过一个特定过程和 FEC 相映射, 在每个节点, 通过标签的切换来转发分组数据。图 2-3 为 MPLS 标签格式。

LABEL 20bits	EXP 3bits	S 1bits	TTL 8bits
32bits			

图 2-3 MPLS 标签格式

(3) 等效转发类 (Forwarding Equivalence Class, FEC)。转发对等级别。将若干等同的数据流合并起来, 就称为转发等价类。例如目的地址前缀相同的数据分组, FEC 的归类方法可以各不相同, 粒度也有差别, 例如, 我们可以按照一定的方法把具有同一目的地址前缀的分组按照 QoS 划分为不同的具有不同 QoS 的 FEC。

(4) 标签分配协议 (Label Distribution Protocol, LDP)。根据数据流的要求, 负责在标签交换路由器之间分发标签的协议。

(5) 标签交换路由器 (Label Switching Router, LSR)。能够交换带有 MPLS 标签的分组的设备。

(6) 标签边缘路由器 (Label Edge Router, LER)。接受没有标签的数据分组 (IP 分组), 并在入口处加入标签。LER 在网络边缘会移除标签, 发送没有标签的分组到 IP 网络的出口。

(7) 标签交换路径 (Label Switched Path, LSP)。使用 MPLS 协议建立起来的分组转发路径, 相当于一隧道, 由标记分组源 LSR 与目的 LSR 之间的一系列 LSR 以及它们之间的链路构成。

(8) 标签信息库 (Label Information Base, LIB)。用来存放 LSR 通过 LDP 协议接收到的各种标签绑定的数据表。类似于路由表, 包含各个标签所对应的各 种转发信息, 如入口标签, 入口设备等。图 2-4 为标签信息库示意图。

FEC	Label In	If In	Label Out	If Out
-----	----------	-------	-----------	--------

FEC:转发等价类

Label In 入口标签

If In 入口设备

Label Out 出口标签

If Out 出口

图 2-4 标签信息库

### 2.1.2 MPLS 技术特点及应用

MPLS 可以在路由器、支持标签交换的 ATM<sup>[5]</sup>交换机上，仅仅根据一个简单的标签的内容实现数据包转发，而不必执行基于目的 IP 地址的复杂的路由查找算法。这项技术给 IP 网络带来了许多好处，例举如下：

(1) 虚拟专用网络 (VPN): 利用 MPLS 技术，服务提供商可以利用其通常的体系结构，在骨干网上为多个客户创建基于第三层技术的虚拟专用网络，而不需要用户端再另外实施加密技术或特别的应用程序。

(2) 流量工程 (TE): 可以对网络上的特定流量显式地设定一条或多条路径，也可以为某类流量设定性能特性参数。对于带宽没有被充分利用的路径，这个特性可以优化带宽的利用率。

(3) 服务质量保证 (QoS): 利用 MPLS 过硬的服务质量保证技术，服务提供商对 VPN 的客户提供多样化的质量保证。

(4) 集成 IP 网和 ATM 网: 大多数运营商的网络都采用了重叠模型 (Overlay Model)，即 ATM 运行在第二层，IP 运行在第三层。这种实现方式存在扩展性问题。利用 MPLS，运营商可以把 ATM 的控制平面移入到第三层，简化网络的控制管理以及网络的复杂性。这项技术具有非常好的扩展性，消除了承载 IP 流量时 ATM 信元标识的额外负载。

MPLS 结合了数据链路层交换的速度、性能以及网络层路由选择的可扩展性。MPLS 支持所有的网络层协议，并且其可扩展性超越了现今的典型网络。MPLS 使服务提供商能很好地应对现代网络爆炸性增长所带来的挑战，在不牺牲现存网络基础结构的前提下提供差异性服务。MPLS 支持在 ATM 交换网络上有效地运行 IP 服务。MPLS 可以在一个基于路由器的 Internet 骨干网上对一个给定的源地址和目的地址创建不同的路由。通过集成 MPLS 到网络体系中，许多服务提供商降低

了成本，增加了利润，提供了差异服务，在与没有提供 MPLS 服务的，如没有提供基于三层的 VPN 或没有提供流量工程的运营商的竞争中取得了优势。

MPLS 所拥有的技术优点可以为广大运营商和企业带来很多益处。国内外的运营商以及大型企业有些已经开始在它们的骨干内部利用 MPLS 来提高网络资源利用率。随着 MPLS 技术越来越走向成熟，应用领域会越来越广，会有更多的价值被开发出来。以下简要罗列 MPLS 目前主要技术应用：

### （1）利用 MPLS 实现流量工程（TE）

流量工程可以说是 MPLS 的最大优点之一。利用 MPLS 实现流量工程，可以使网络管理员从繁琐的手动调节困境中解脱出来，使流量工程自动化成为可能；另一方面，MPLS TE<sup>[6-9]</sup>使流量工程的目的的实现变得很容易，即使是在一个复杂的运营商网络中。同时可以为关键业务避免或减轻拥塞所带来的影响，并且可以保证端到端的 QoS。MPLS 流量工程的实现较之于其他方案有着更低的维护费用

### （2）利用 MPLS 实现端到端的 QoS

利用 MPLS 实现端到端的 QoS，是 MPLS 工作组的一个重要课题，也是 MPLS 的一个主要应用方向。MPLS 支持综合业务 (Int-serv)<sup>[10]</sup> 和区分服务 (Diff-serv)<sup>[11][12]</sup> 两种 QoS 模型。当 MPLS 应用于边缘网络中时可以提供对 Int-serv 模型的支持，在此情况下，MPLS 可以通过使用扩展的 RSVP 作为其控制信令直接实现各种 Int-serv 所规定的业务。MPLS 的标签分配机制与 Diff-serv 中对服务质量的分类与标记机制相近，同时两者的控制机制也相类似并且网络的运算工作都在网络边缘执行。因此，MPLS 通过将 Diff-serv 分配与标签分配过程相融合来实现对 Diff-serv 的支持。

### （3）利用 MPLS 实现虚拟专用网（VPN）

VPN<sup>[13]</sup>是指利用隧道技术和访问控制技术在公共网络中建立的专用通信网络。在虚拟专用网中，任意两个节点之间的连接并没有传统专用网所需的端到端的物理链路，而是利用某种公网的资源动态组成，虚拟专用网络对用户端透明，用户好像使用一条专用线路进行通信。

MPLS VPN 是基于网络服务供应商<sup>[14]</sup>的主干网络所提供的一种高性能的虚拟专用网技术，与其他 VPN 相比，它的网络配置更简单，提供用户与网络更高的安全性，可以直接构架于现有路由体系之上，而无须任何改动，具备更加良好的可

扩展性。MPLS 可以利用其流量工程和 QoS<sup>[15]</sup>的能力实现支持流量工程和 QoS 的 VPN，当面向对服务质量有着更高要求的实时业务时，MPLS VPN 将会成为更优的选择。

## 2.2 MPLS 流量工程技术

MPLS 能很好地与 IP 网络结合，为流量工程实施提供了一种新的途径。MPLS 通过在网络中使用约束路由建立显式路径引入流量工程，控制 IP 包在网络中的转发路径，实现网络中流量的合理分配，网络资源的有效利用，同时保证用户申请的服务质量得到满足。MPLS 在流量工程方面所具有的优势已成为 MPLS 发展的主要动力。

### 2.2.1 MPLS 流量工程概述

随着 Internet 的迅速发展，因特网服务提供商（ISP）面临着日益激烈的商业竞争，他们必须向用户提供像电话一样可靠的服务，同时，还必须满足向不同用户提供不同服务的需求。ISP 获得更大利润的方式就是必须提供具有竞争力的服务。对 ISP 来说，有效利用网络基础设施，尤其是可用带宽影响着商务的效率和代价。ISP 可以通过更加有效地使用带宽资源达到更少的运营费用，获得超过其竞争者的优势的目的。于是，在 IP 网络中引入流量工程，通过增强基本流量转发机制使得网络具备合理利用资源、均衡负载的能力。

传统的运营商网络中经常会出现这样的情况，在两点之间的多条链路中，其中一部分链路上的业务量已经接近容限，而另一部分链路却几乎闲置，另外，网络中的某些节点已经发生拥塞，而另外一部分节点却几乎没有流量通过。这样既降低了网络的性能，又浪费了网络的物理资源。流量工程的实施不但可以避免上述现象的发生，提高物理设施的使用效率，而且还可以增加网络的健壮性，避免由于拥塞而引起的网络瘫痪。这些改善对于网络更为健壮、运营商进一步降低运营成本大有益处。

将业务流有策略地映射到现有物理链路上的任务称为流量工程，流量工程是 ISP 一个强有力的工具，通过它可以平衡网络中不同链路、路由器和交换机之间的业务负荷，使所有这些网络设备既不会被过度使用，也不会未被充分使用。这

样 ISP 就可以有效利用整个网络的资源。在未来的主干网络中，流量工程将成为路由结构中一个重要的辅助部分，它能够在沿网络中备选路径转发业务时提供辅助信息。流量工程是目前理论研究的热点，它的目的是在满足 QoS 要求的前提下使网络资源尽可能均匀使用，避免出现部分网络拥塞而其余链路空闲或利用率很低的不均衡状态，从而能够接入更多的业务，提高全网利用率，降低网络运营成本。

2000 年 9 月，IETF 发布的草案规定了 Internet 上实施流量工程的框架和目标。ATM 作为目前宽带网络的核心技术之一，可以支持综合服务，在网络工程设计方面具有高度的灵活性，提供流量管理和 QoS，支持 VPN 和多重业务类型。但 ATM 缺点是信令过于复杂，给广泛应用带来了不利。IP 技术简单、高效从而得以广泛应用并迅速成为网络的主导技术，其灵活的路由体系结构，非面向连接尽力而为的分组传送方式，特别适合非实时数据信息的传输。但 IP 技术的流量管理能力很弱，无法提供 QoS 服务保证，无法满足语音、视频图象等实时信息的传输要求。因此，初期在网络中主要是利用 ATM 的流量管理能力，使用基于 ATM 技术的重叠方式（IP over ATM）实现流量工程。在重叠模型中，路由和流量工程分别在不同的系统上完成，路由在路由器上执行，流量工程在 ATM 交换机上执行。由于需要分别对两个网络进行管理，导致了网络更高的复杂性，更大的开销。

MPLS 作为能与 IP 很好结合的下一代网络技术，它具有类似 ATM 技术建立面向连接传输路径的能力，能预先建立明确路径的显式路由。它的吸引人之处主要在于通过手工的网管配置或是下层协议的自动配置，可以很容易的建立起不受传统逐跳路由协议限制的显式 LSP，可以较容易的实现约束路由，所以它保留了重叠模型流量工程技术的优点，而且还能提供超越第二层流量工程的服务，如负载均衡和非等价路径的使用。由于重叠模式的各种局限性以及 MPLS 在流量工程方面体现出来的优势，MPLS 成为目前流量工程最佳的解决方案。

### 2.2.2 MPLS 流量工程技术特点

在 Internet 业务流测量和动态控制等特定方面，MPLS 对 TE 都非常有用。由于联网资源的高成本以及服务提供商所面临的竞争环境，所以动态性能优化成为使服务提供商能够在竞争中取胜的一个决定性因素。TE 的一个重要方面是引进

了简单的负载平衡技术。但是, TE 也需要将其他一些因素考虑在内, 例如使用服务提供商的网络影响总输入产量的因素。这就要求一些机制来支持一个比简单负载平衡方案更复杂的策略。MPLS 提供了一种方法, 这种方法较其他可供选择的技术而言可以在一个更低的成本上实现更复杂的 TE 解决方案。

MPLS 提供了动态的机制用于建立显式路由的 LSP, 这种显式路由的 LSP 能够独立操作 IGP 确定的路由。这就减少了网络中路由协议行为存在拥塞限制的影响。由于 MPLS 机制是动态的, 所以 LSP 的建立可以具有期望的伸缩性, 并且可以根据需要将 LSP 重新优化。MPLS 流量工程特别具有吸引力的特征是:

- (1) 采用 MPLS, 流量工程功能是被集成到第三层, 这样可以优化 IP 数据流的路由限制, 这些限制是由骨干容量和拓扑结构强加给 IP 数据流路由的。
- (2) 根据数据流需要的资源以及网络中可用的资源, 它可以在网络中路由 IP 数据流。
- (3) 它使用基于约束的路由选择 (constraint-based routing), 其中, 数据流的路径是最短的路径, 路径满足资源需求或者带宽需求、媒介需求以及数据流优先级带来的约束。
- (4) 它可以从链路或者节点故障中动态恢复, 通过适应一套新的约束来改变骨干网的拓扑结构, 即使离线预先计算出了好几条主要路径。
- (5) 它启用了不相等成本负载分担, 允许使用不是由 IGP 学到的路径。
- (6) 在确定穿越骨干网的显式路由时, 它计算链路带宽以及数据流的规模。
- (7) 它不需要手工配置网络设备来建立显式路由。而且, 我们可以依靠 MPLS 流量工程功能来理解骨干网络的拓扑结构以及自动的信令进程。

## 2.3 MPLS 故障恢复机制

MPLS 故障恢复机制<sup>[16]</sup>能够保证网络发生故障后在期望的时间内恢复数据传输, 同时保证所需的 QoS。由于 MPLS 是面向路径的, 因而相比传统的逐级跳的路由模式能提供更快、更可预测的保护和恢复能力。

### 2.3.1 MPLS 故障恢复机制概述

网络有时会发生故障, 有很多因素会导致网络部分失效。这些失效涉及的范

围很广，如电缆连接松脱、光纤断裂，路由器崩溃等等。当网路发生故障时，需要将发生故障处的数据流量尽快转移到其它网络路径去，避免产生大量数据包丢失。当网络发生故障时，虽然有些可以通过低层协议进行修复，但往往满足不了 MPLS 的要求，如低层协议只有针对链路的保护而没有针对节点的保护。另外通过第三层路由协议也可以进行重路由得出新的传输路由进行数据传输，但该过程往往时间较长，无法满足对传输时延要求很小的服务，如语音传输等，从而影响业务的 QoS。

为了克服上述缺陷，MPLS 提供了故障恢复机制，它通过一种快速修复方法建立一条 LSP 来当作备份路径<sup>[17]</sup>，当故障发生后，数据流被快速重定向到备份路径上。同时 MPLS 中也提供比其他协议更快速更有效的故障诊断和修复机制。由于 MPLS 在 LSP 上建立的多样性保证，可以在微秒级内将流量转发到备份路径上。同时这种转发机制提供了成熟的 QoS 和流量工程特性。

MPLS 故障恢复机制的基本思想是在工作路径之外建立备份路径，备份路径从路径切换节点 (PSL, Path Switch LSR) 开始，到路径聚合节点 (PML, Path Merge LSR) 结束。PSL 是负责工作路径和备份路径之间流量切换和复制的标签交换路由器，工作路径发生故障时由 PSL 将流切换到备份路径。PML 是既接收工作路径又接收备份路径上流量的 LSR，如果 PML 不是目的节点，它将从备份路径上收到的流量汇聚到工作路径上，如果是目的节点，则将数据分组交由高层协议处理。MPLS 故障恢复机制保证发生故障时能在期望的时间内恢复数据传输，同时在恢复后能保持所需的 QoS。由于 MPLS 是面向路径的，因而比传统的逐级跳的路由模式能提供更快、更可预测的保护和恢复能力。

MPLS 故障恢复机制一直是 MPLS TE 的研究重点之一。2003 年 2 月，IETF 针对 MPLS 故障恢复机制的架构定义了 RFC3469<sup>[18]</sup>。在已经对 MPLS 故障恢复机制简要了解基础上，以下主要介绍该机制中的基本技术术语：

- (1) LSR (Label Switching Router): 标签交换路由器，如图 2-5 所示。MPLS 网络里的路由器，负责建立标签交换路径与利用标签交换传送数据包。
- (2) Ingress LSR: 入口路由器，如图 2-5 所示。位于 MPLS 网络与其它异质网络的交接点，负责将未附上标签的数据包加上标签封装成带有标签的数据包，再放到所属的标签交换路径上传送。

(3) Egress LSR: 出口路由器, 如图 2-5 所示。位于 MPLS 网络与其他异质网络的交接点, 负责从标签交换路径上接收到的带有标签的数据包还原成原来的数据包。Ingress LSR 为标签交换网络的起点, Egress LSR 为标签交换网络的终点。

(4) LSP (Label Switching Path): 标签交换路径, 如图 2-5 所示。在 MPLS 网络里, 数据包从入口路由器到出口路由器间所经过的路径称为标签交换路径。在图 2-5 中, Working Path, Backup Path 均为 LSP。

(5) Working path: 工作路径, 如图 2-5 所示。入口路由器为数据包所建立到出口路由器的路径, 又称为 Primary Path 或是 Active Path。

(6) Backup Path: 备份路径, 如图 2-5 所示。当工作路径发生断线或是故障时, 用来替代工作路径的 LSP。又称为恢复路径 Recovery Path, 在全局修复时又称为 Alternative path, 在局部修复时又称为 Backup Tunnel。

(7) PSL (Path Switch LSR): 路径切换路由器, 当工作路径发生断线或是故障时, 负责将数据流切换到备份路径上。图 2-5 中的 Ingress 即为 PSL, 但 PSL 不一定是 Ingress LSR。

(8) PML (Path Merge LSP): 路径聚合路由器, 负责备份路径与工作路径合并的 LSR, 同时负责将备份路径上的数据转向往工作路径上传送。如图 2-5 的 Egress LSR 即为 PML, 但 PML 不一定为 Egress LSR。

(9) POR (Point of Repair): 故障修复路由器。负责执行 MPLS 故障恢复的 LSR, 通常为 PML 或是 PSL, 根据具体的故障恢复机制而定。

(10) NHop (Next-hop router): 下一跳路由。与目前路由器距离一跳远的路由器。

(11) NNHop (Next-Next-hop router): 下下一跳路由。与目前路由器距离两跳远的路由器。

(12) FIS (Fault Indication Signal): 故障指示信号。用来通知工作路径发生故障的信息, 由发生故障的两端的 LSR 发现, 该信息依照不同机制, 往 LSP 上游传送或是下游传送给 POR, 通知 POR 立即做出故障恢复程序。

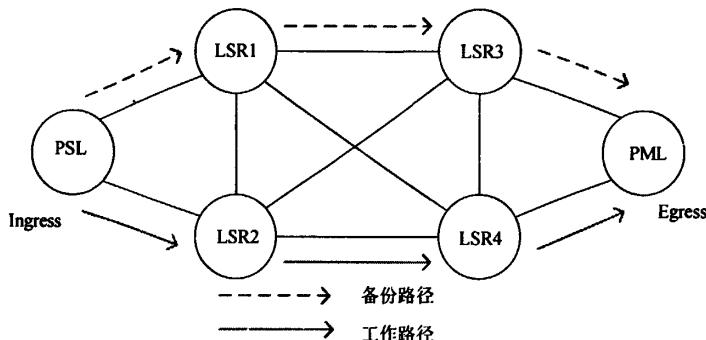


图 2-5 MPLS 网络示意图

### 2.3.2 MPLS 故障恢复机制分类

近年来有很多针对 MPLS 故障恢复机制的研究，本文根据目前的研究现状与内容对其进行分类。

根据 MPLS 备份路径建立方式的不同，MPLS 故障恢复机制分为三类：分别为事先选择并建立路径 (Pre-Established)<sup>[19]</sup> 方式、事先选择但不建立路径 (Pre-Qualified)<sup>[20]</sup> 方式以及按需计算并建立路径 (Establish-on-Demand)<sup>[21]</sup> 方式。

(1) Pre-Established (事先选择并建立路径)，是指在故障发生前选择并建立好备份 LSP。其优点是故障恢复时间短，缺点是资源利用率低，且预先建立备份路径在使用时不见得是最佳的路径，同时还可能会发生带宽不足的情况。该方法适用于对实时性要求较高的业务。

(2) Pre-Qualified (事先选择但不建立路径)，是指在故障发生前备份路径预先确定，且其上资源已经有效，但不建立备份 LSP，等故障发生后再依据计算结果建立备份路径。对 Pre-Established 方法的改进，提高了资源利用率，但故障恢复的时间会比前者稍长，同时该方式下建立的备份路径也不一定是故障发生时的最佳的路径。

(3) Establish-on-Demand (按需计算并建立路径)，是指在故障发生后，按需进行重路由计算并建立备份路径和备份 LSP。该方法资源利用率是最好的，备份路径也是故障发生时的最佳路径，其缺点是故障恢复时间较长，主要适用于尽最大努力 (Best-Effort) 类型的服务。

根据工作路径和备份路径之间的关系，MPLS 故障恢复机制分为以下三类，分

别是：1+1<sup>[22]</sup>保护模型、1: 1<sup>[23]</sup>保护模型和N: M<sup>[24]</sup>保护模型。

(1) 1+1 保护模型，在这种模型中，PSL 将数据流复制成二份，同时在工作路径和备份路径上进行传送，再由 PML 选择其中的一份数据流向出口端送出，当工作路径上有故障发生时，PML 只要将接受数据流来源改为备份路径便可继续接收，该方式是最佳的保护方式，其恢复时间短，数据包丢失少，缺点是由于该方式需使用两倍的带宽传送数据流，造成了很大的网络资源浪费。

(2) 1: 1 保护模型，在这种模型中，只利用工作路径传送数据流，当故障发生后，PSL 才把数据流送往备份路径进行传送。该方法是目前较常用的方法，相比 1+1 保护模型，拥有更好的网络资源率，但故障恢复的时间会较长。

(3) N: M 保护模型，在这种模型中，N 条工作路径共同使用 M 条备份路径，但其带宽并没有共享。其中 N: 1 保护模型是 N: M 保护中的一个特例，相比前两种模型，拥有最好的网络资源率，但网络计算复杂度高。

备份路径的建立是实现自愈恢复的基础，根据备份路径建立时机的不同，现有 MPLS 故障恢复机制又可分为快速重路由(FRR)<sup>[25]</sup>和重路由<sup>[26]</sup>两种模式。

(1) 重路由：在该模式中，备份路径是在故障发生以后按需计算出来的，备份路径的计算是基于故障信息、网络路由策略和网络拓扑信息等等，当一个故障被检测出来，或者收到一个故障通告信号(FIS)，故障处上游的 LSR 作为一个路径恢复点(POR)负责建立一条备份路径，这条备份路径需要绕过故障点并且要与工作路径在故障点下游的某个 LSR 合并。POR 使用最短路径树算法并从树中剪去故障链路或故障节点，找到一条备份路径。当备份路径建立之后，POR 会转发流量到备份路径中去。重路由模式不会去等关于故障的更新在网络中发布，然后再重新计算备份路径，所以在该模式下能够进行快速的故障恢复。

重路由的优点就是适应性较强，在备份路径建立之前并不需要占有任何备份资源，故障发生前无资源浪费。同时通过采用合理的路由算法，重路由可以计算出一条最优路径，能够更好地利用网络资源和均衡业务。其缺点就是可能遇到没有足够的资源去建立备份路径，从而导致恢复失败。重路由模式并不保证备份路径一定能够发现，如果备份路径需要的资源在网络中已经被使用并比备份路径中的流量具有更高的优先级，备份路径建立将失败。网络也就无法在故障后进行及时恢复。

(2) 快速重路由：也可称为保护切换。这种模式是在故障发生前通过在线或离线的管理工具预先为要保护的路径建立备份路径，也可由 PML 或中间节点通过一定算法建立，其主要依据是路由策略、对恢复的要求以及管理方面的考虑因素。备份路径最好与工作路径不重叠，否则可靠性会降低。执行故障恢复操作时，将流量切换到备份路径。由于故障发生时备份路径已经存在，因此其速度较快，但在故障尚未发生时，备份路径会造成资源浪费。对于保护切换，根据保护的发起点不同，又分为局部保护和路径保护两种。下表是关于 MPLS 故障恢复机制两种模式的比较。

表 2-1 MPLS 恢复模式比较

恢复模式	保护路径建立方法	保护路径建立时间	资源利用率	恢复时间	服务类型
保护切换	1+1	出现故障前	最低	快	高优先级
保护切换	1:1	出现故障前	较低	快	较低优先级
保护切换	M:N	出现故障前	较低	快	较低优先级
重路由	预先计算路径	出现故障后	较高	较快	较高优先级
重路由	按需建立	出现故障后	最高	慢	尽力而为

## 2.4 本章小结

随着 IP 网络规模的不断扩展，各类新的网络应用和业务对网络的服务质量提出的要求愈来愈高。MPLS 技术及其特有的流量工程能力发挥着越来越重要的作用。MPLS 的故障恢复机制一直是 MPLS 流量工程的研究重点之一，具有提供比其他协议更快速更有效的故障诊断和修复机制的能力，它通过在工作路径之外建立一条 LSP 来当作恢复路径，当故障发生后，数据流被快速及时地重定向到恢复路径上，保证在期望时间内恢复数据传输以及业务流的 QoS。本章首先简要介绍了 MPLS 技术，具体内容包括 MPLS 基本概念、相关技术术语、技术特点以及技术应用，其次概要介绍了 MPLS 流量工程技术，指出了流量工程的必要性，论述了 MPLS 流量工程相比传统的流量工程所具有的技术优势，最后详细介绍 MPLS 故障恢复机制，包括其基本概念、技术术语，并根据目前研究现状对其进行分类并对各分类进行了详细描述。

### 第三章 MPLS 快速重路由及其经典方案相关研究

快速重路由 FRR 技术能在网络发生故障前预先建立好备份路径，链路或节点失效后，无需执行任何信令，直接由检测到故障的节点负责将业务流切换至备份路径继续进行转发，最大限度地减少分组丢失、降低延时，保证服务质量，同时没有附加硬件成本问题。FRR 技术是目前研究的热点，很多著名的 FRR 方案被提出。本章主要研究 MPLS FRR 技术，重点研究经典 FRR 方案并分析总结各方案的特点与局限性。

#### 3.1 MPLS 快速重路由

MPLS 快速重路由 (FRR) 技术基本思想是在工作路径之外网络故障发生前预先建立备份路径。故障发生后，业务流量快速从工作路径切换至备份路径，实施故障恢复。由于网络故障发生时，备份路径已预先建立，因此其恢复速度较快。MPLS FRR 根据其保护的的范围不同，又分为本地保护 (局部保护) 和路径保护 (端到端保护)。

##### 3.1.1 MPLS 快速重路由的必要性

网络中的任何资源都有可能发生故障，为了减少网络故障引起的负作用，如分组丢失，提供一个足够高可用性的网络是非常应该的。重路由技术可以尽量提供在最短时间内恢复链路或者节点故障。但是，该技术中故障指示信号需要从检测到故障的节点一直穿过网络传递到故障修复点，并由故障修复点临时计算建立一条备份路径用以实施流量的切换，这样就会带来很大的延迟以及丢包，而且可能会遇到没有足够的资源去建立备份路径而导致恢复失败。这些对于网络应用，尤其是实时应用，如语音、视频等是无法忍受的。

MPLS FRR 技术，不同与重路由技术，其基本思想是在工作路径之外网络故障发生前预先建立备份路径，故障发生后，业务流量快速从工作路径切换至备份路径，实施故障恢复。由于网络故障发生时，备份路径已预先建立，因此其恢复速度较快，从而减少数据丢失，保障数据传输不会突然中断，提高网络可靠性。当

网络故障修复好后，流量又重新切换到工作路径上继续进行转发。MPLS FRR 通过预先建立一条 LSP 来保护一条或多条 LSP。预先建立的 LSP 称为备份路径，被保护的 LSP 称为保护路径或工作路径。MPLS FRR 根据其保护的范围不同，又分为本地保护（局部保护）和路径保护（端到端保护）。

### 3.1.2 路径保护

路径保护<sup>[27]</sup>又称为端到端的保护，其基本思想是通过和保护路径并行建立一条备份路径，从而保护保护路径中的所有节点和链路。每一条保护路径都有一条备份路径。保护路径以及备份路径都是在首端配置，都是预先在控制平面建立的。备份路径是沿着与保护路径尽可能不同的路径建立的。这样就确保沿着保护路径发生的失效不会同时影响到备份路径。备份路径只会在网络发生失效时使用，备份路径除了在失效情况下，是不会承载流量的。在路径保护中，负责流量切换的节点称为 PSL；保护路径和备份路径的终点称为 PML。路径保护机制见图 3-1。

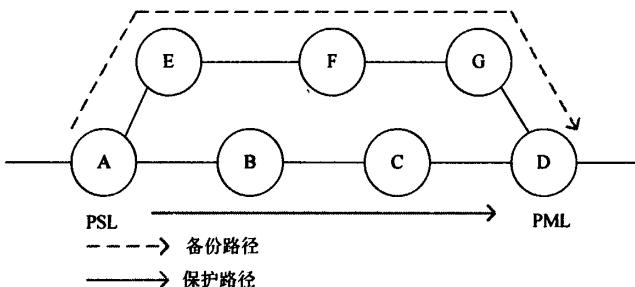


图 3-1 路径保护（端到端的保护）

如图 3-1 所示，保护路径为 {A-B-C-D}，备份路径为 {A-E-F-G-D}。在网络失效前，数据被沿着保护路径上转发。备份路径作为备选的路径，在故障发生前预先建立好，并随时做好准备接替保护路径继续工作。一旦保护路径上发生故障，并且报告给入口节点时，数据就迅速地被切换到备份路径上继续进行转发。在路径保护模式中，保护路径和备份路径享有同样的带宽特性，二者都需要预留相同的带宽。这样无论承载流量的是保护路径还是备份路径，都基本上保持了端到端特性的一致。但同时，由于对每条保护 LSP 都必须建立另外一条备份 LSP 且在两条路径上分别预留相同的带宽，而备份路径仅仅在网络发生失效时才起作用，因此在网络中保留了大量不会使用到的带宽，造成了网络其他 LSP 没有带宽可用，

使网络资源利用率降低。另外，由于在路径保护中不管故障出现在何处，都必须将故障信息传递给入口 LSR 并由其负责进行流量切换，这将造成较大的时延，因此路径保护故障恢复周期较长。

### 3.1.3 局部保护

局部保护<sup>[28]</sup>是由检测到故障的上游节点直接发起恢复，将流量从保护路径切换到备份路径中继续进行转发。检测到故障并且发起恢复的节点称为 PLR (Point of Local Repair)，由于 PLR 直接把流量切换至备份路径上，因此减小了故障信息的传输时间，其优势在于恢复的周期短。在局部保护中，有两种保护方式，链路保护以及节点保护，前者是备份路径从失效链路的附近通过，而后者是备份路径从失效节点的附近通过。

链路保护是为容易损坏的物理链路在其附近建立一条穿过网络并且绕过该被保护物理链路的标签交换路径，以提供一条并行备份路径。一旦链路发生故障，上游节点就将业务流从物理链路上切换到备份路径，这样，数据流就经过一个微小的中断继续传输了。图 3-2 描述了这样一个示例网络。

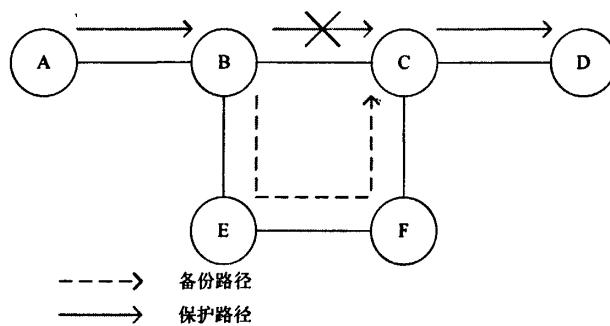


图 3-2 链路保护

如图 3-2 所示, 链路 {B-C} 是保护路径上至关重要的链路, 为了保护这条链路, 在这条链路旁边建立一条备份路径 {B-E-F-C}, 这样当链路 {B-C} 发生故障后, 数据流将被重新定向到这条事先建立好的备份路径上继续传递。备份路径的首端即是被保护链路的上游节点, 备份链路的尾端则直接成为被保护链路的下游节点。在图 3-2 中, 备份路径的首端是节点 B (PLR), 尾端是节点 C (MP)。链路保护基于以下事实: 即使被保护链路已经失效了, 在被保护链路的另一端的路由器仍然正常工作。链路保护使用 NHop 备份路径, 备份路径在被保护链路另一端的节点上终结。显然, 这种方式只能防止链路失效而不能避免节点失效。如果备份

路径终结处的节点失效，链路保护就无效了。

链路保护只适用于在两个标签交换路由器之间的链路发生故障的情况。但是，标签交换路由器也有可能发生故障，而这时，链路保护的方法就不能适用了，就必须使用节点保护。图 3-3 描述了一个节点保护的示例网络。

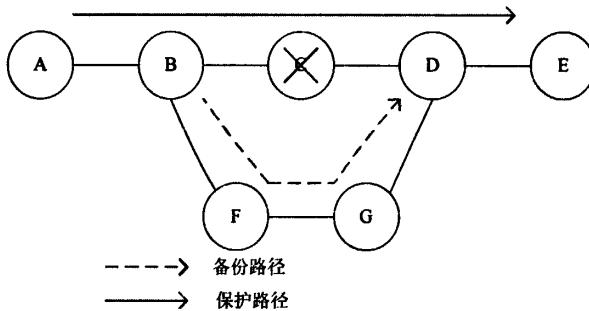


图 3-3 节点保护

图 3-3 表示了一条从节点 B 到节点 D 的备份路径 {B-F-G-D}，这条备份路径是为了保护节点 C 一旦发生故障而建立的。当节点 B 检测到故障之后，原来的标签交换路径就切换到备份路径上，继续进行数据转发。如图 3-3 所示，当检测到节点 C 发生故障，那么数据流将被转发到链路 {B-F-G-D} 上继续转发。在此，节点 B 为 PLR，结点 D 为 MP。显然，在节点保护模式下，既实现了对下游链路节点的保护，同时也必须要自动实现对与失效节点直接相连的下游链路的保护。节点保护和链路保护在很多方面相似。节点保护与链路保护相比区别在于其 MP 是 NNhop，而不是 NHop，因为需要防止 NHop 失效。

### 3.2 MPLS 快速重路由经典方案的研究与分析

MPLS FRR 技术旨在利用预建立的备份路径对工作路径实施保护，更快捷地实现业务流切换。由于不同的 FRR 方案涉及到不同的备份路径，在故障检测，流量切换，路由策略，故障恢复等方面均会存在系列差异。因此，导致 FRR 方案有着各自不同的恢复性能。目前有许多的 FRR 方案被讨论，比较著名的有 Makam 方案、Haskin 方案、Hundessa 方案、RSVP 方案等等。其中 Makam 方案属于路径保护方式，Haskin 方案、RSVP 方案属于局部保护方式，Hundessa 方案是对 Haskin 方案的优化改进。

### 3.2.1 Makam 方案

Makam 提出的 MPLS FRR 方案，被称为 Makam<sup>[29]</sup>方案。该方案通过路径保护方式在入口 LSR 和出口 LSR 之间建立起端到端的 LSP 保护。这种备份路径让节点与链路彻底与保护路径分离。当保护路径失效被检测到后，一个 FIS 会携带着关于刚发生的故障信息被传递到 PSL。PSL 将会负责把流量从保护路径切换到备份路径上。保护路径的入口称为路径切换路由器（PSL），保护路径和备份路径交汇处称为路径合并路由器（PML）。

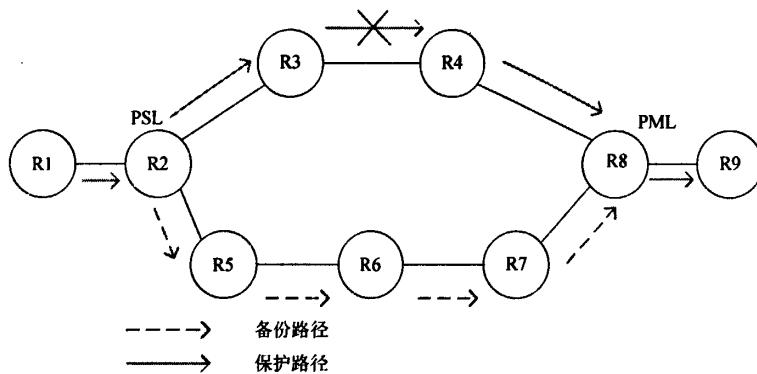


图 3-4 Makam 方案

在 Makam 方案中，备份路径在图 3-4 中就是 {R2-R5-R6-R7-R8}，PSL 为节点 R2，PML 为节点 R8。当保护路径上链路 {R3-R4} 失效时，R3 将会立即检测到失效并马上向 PSL 即节点 R2 发送一个故障通知消息 FIS，告诉 PSL 保护路径出现故障，PSL 则迅速将分组转发到事先为这条保护路径建立的备份路径上去。若保护路径故障解决，同样向上游传递故障修复信号 FRS，分组又会回到保护路径上。

Makam 方案的主要优点是失序的分组较少，且用于故障恢复的备份路径较短，因而时延较低；但由于需要将故障通知消息传递到 PSL 才进行流量切换，因此这段时间将造成较大的丢包。

### 3.2.2 Haskin 方案

在 Makam 方案中，当检测到失效时，LSR 向上游节点发送 FIS 信号的同时，数据直到 FIS 被 PSL 收到前仍然在向故障的 LSP 上发送。这就意味着有大量的数据包会在 FIS 到达 PSL 前丢失，如果失效的节点距离 PSL 越远或者数据传输速率极快时，那将会有更多的数据包会丢失。

Haskin<sup>[30]</sup>方案的中心思想就是在链路失效后沿着保护路径反向传递数据流，一直传递到 PSL，再由 PSL 转移到与保护路径平行的备份路径上去，相比 Makam 方案丢包率大大降低。Haskin 模型如下图 3-5 所示。

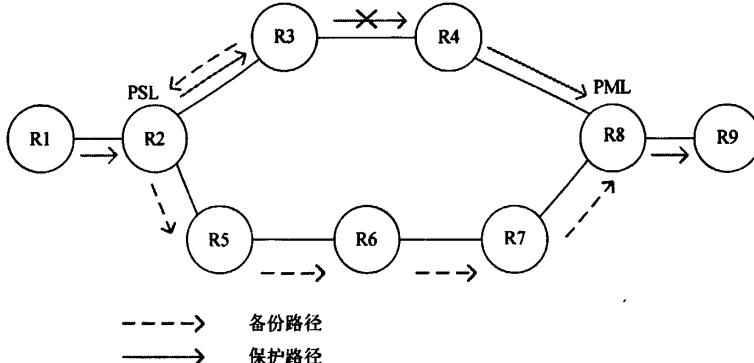


图 3-5 Haskin 方案

在 Haskin 方案中，备份路径由两段组成：前一段从 PML 或其前一跳节点开始至 PSL 结束，通常可沿着保护路径的反向建立；另一段从 PSL 开始到 PML 结束，与保护路径不相交，即保护路径中各个节点除 PSL、PML 之外，其他节点在该段路径中均不承载流量。这两段路径连接成保护路径的备份路径。如图 3-5 所示，从源节点 R1 发送至目的节点 R9 的业务流在 MPLS 网络中沿着保护路径 {R2-R3-R4-R8} 传递。如果在某时刻，节点 R3 和节点 R4 之间链路突然失效，节点 R3 会立即检测到失效并快速将业务流沿保护路径的反方向 {R3-R2} 传递到入口节点 PSL，即节点 R2。然后再沿着备份路径 {R2-R5-R6-R7-R8} 传递到目的节点，这样从节点 R1 发往节点 R9 的数据在 MPLS 网络中将沿着备份路径 {R2-R3-R2-R5-R6-R7-R8} 传递。当 R3 和 R4 之间的链路恢复以后，业务流又会重新回到保护路径上传送。

Makam 方案是直接从 PSL 向 PML 建立备份路径，而 Haskin 方案建立的备份路径是在 PSL 与 PML 之间环绕，它的优势在于可在发生故障时对流量进行快速切换，降低了丢包率；缺点是恢复路径长，时延较高。此外，当故障解决，流量从备份路径切换到保护路径时，会造成分组的失序。

### 3.2.3 Hundessa 方案

Lemma Hundessa 和 Jordi domingo Pascual 在研究 Haskin 方案的基础上并

对其进行了一定的优化，提出了 Hundessa<sup>[31]</sup>方案，它利用缓存和加标签的方法解决 Haskin 方案中会出现的数据包逆序的问题。其算法中心思想是在每一个 LSR 额外加上缓存 buffer 来储存数据包，当工作路径上的每一个 LSR 收到反方向的数据包后便将从上游传来的数据流进入缓存 buffer 内，然后在往下游传送的最后一个数据包加上标签 tag，在此标签从反方向接收到时，都一直将上游的数据流送缓存里储存起来。直到收到从反方向回来的 tag 后便将缓存里的数据流切换到往入口路由方向的备份路径上传送。当入口路由器收到 tag 后表示工作路径上的 LSR 都已经往回传送数据流且都已经由入口路由器切换到备份路径上了，此时入口路由器便将往工作路径上传送的数据流切换到备份路径上。该方法在每一个 LSR 上均增加一个缓存使得 LSR 的负担加大，成本也增加，而且当缓存出现溢出 overflow 时，仍然会产生数据包丢失还有逆序的情况。

### 3.2.4 RSVP 方案

RSVP<sup>[32]</sup>方案可以基于两种不同的思想实现快速重路由，即一对备份（One-to-One Backup）思想以及设施备份（Facility Backup）思想。前者分别为每一条被保护 LSP 提供保护，即为每一条被保护 LSP 创建一条备份路径（该备份路径称为 Detour LSP）；后者用一条备份路径保护多条 LSP（该备份路径称为 Bypass LSP）。两者区别如图 3-6 所示。

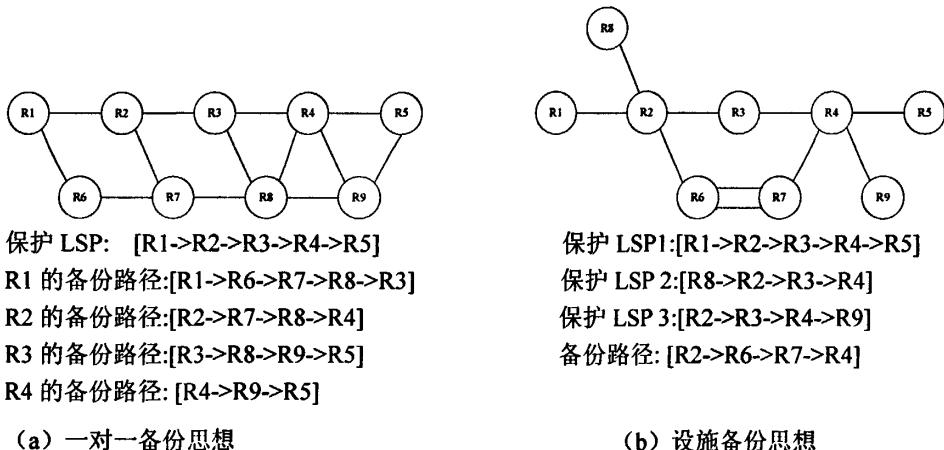


图 3-6 RSVP 方案两种不同保护思想

如图 3-6 (a) 所示为一对备份思想，在利用该思想为网络提供保护时，为保护一条具有 N 个结点的保护路径，需建立 N-1 条备份路径。图示为保护路径

{R1-R2-R3-R4-R5}，分别建立了四条备份路径，如当节点 R2 失效（或链路 {R1-R2}、{R2-R3} 失效）时，流量将被切换到 R1 的备份路径 {R1-R6-R7-R8-R3}。图 3-6 (b) 所示为设施备份，该思想对网络提供保护是用一条备份路径保护多条保护路径。如图 3-6 (b) 所示，网络中有 3 条保护路径，它们均经过链路 {R2-R3-R4}。因此可以在节点 R2 处预先建立备份路径 {R2-R6-R7-R4}，在节点 R3 失效（或链路 {R2-R3}、{R3-R4} 失效）时同时为三条保护路径提供保护。显然，这两种保护思想均可提供节点保护与链路保护。RSVP 方案的优点是丢包率小、故障恢复时间快。缺点是由于为了对网络实行快速恢复，需要预先建立大量的备份路径并预留足够的带宽资源，而备份路径仅仅只在保护路径发生失效后才会承载业务流，因此在故障发生前，备份路径的闲置会造成大量的网络带宽资源浪费。

### 3.3 本章小结

网络发生故障时需要有一种恢复机制对网络进行保护，维持网络数据流的正常转发。MPLS 故障恢复机制的出现很好地解决了这一问题，其可通过两种不同方式实行恢复故障，即重路由以及保护切换（又称为快速重路由 FRR）。其中重路由方式虽然能尽可能地对网络故障进行快速恢复，但依然避免不了分组丢失以及较大的延时，同时由于不能保证备份路径每次都建立成功而导致网络恢复失败。这是实时应用所难以忍受的。FRR 可以很好地解决这个问题，它通过预先建立好备份路径可以在网络失效后提供快速响应、及时切换，保证业务数据的平滑过渡以及 QoS。因此 MPLS FRR 技术是目前的一个研究热点。本章首先详细介绍 MPLS 快速重路由技术，论述了该技术的必要性，介绍该技术两种保护模式并分析了各自的特点与局限性。最后，详细描述了 MPLS FRR 几种经典方案，即 Makam, Haskin, Hundessa, RSVP 方案，在对各个方案进行研究的基础上分析比较了各自的优点以及缺点。

## 第四章 一种 MPLS 快速重路由优化方案

MPLS 故障恢复机制已成为当前研究热点, 同时也是下一代网络发展的技术基础。快速重路由作为 MPLS 故障恢复机制的核心技术, 目前国内外有很多相关文献对其进行研究, 并且提出了很多经典快速重路由方案, 如 Makam 方案、Haskin 方案以及 RSVP 方案, 其它故障恢复方案都是在此基础上发展的。本章具体针对经典方案共同存在的备份带宽资源浪费问题, 提出了一种快速重路由优化方案, 该方案包含两个方面内容, 一为优化的备份资源信息共享机制, 该机制通过使网络中的关键节点掌握有限范围内的节点与链路的相关信息, 实现备份资源在网络中全局性共享; 二为优化的备份路径选择算法, 该算法基于经典最短路径算法, 通过在链路权重中添加带宽的限制, 优先选择备份资源带宽大的链路, 可进一步降低对网络预留资源的需求。

### 4.1 问题的提出

MPLS FRR 故障恢复的思想是在网络故障发生之前就建立好可代替保护路径的备份路径。一旦网络出现失效, 检测到故障的网络设备同时负责将业务流快速及时地切换到备份路径上继续转发, 从而能保证更低的延时, 更少的分组丢失。因此, 对于 MPLS FRR 故障恢复方案的研究一直是目前的一项重要研究热点。国内外学者建议了各种不同的方案用于故障后快速重路由。其中比较著名的有 Makam, Haskin, Hundessa, RSVP 等方案。

在 Haskin 方案中, 网络出现故障后, 流量将沿保护路径的反向传送至 PSL, 再由 PSL 切换至备份路径(与保护路径不相交)。在故障恢复后, 再将流量切换回保护路径。Haskin 方案为一种局部保护方案, 优点是故障后可快速切换, 因而丢包较少。缺点是恢复路径较长, 时延较高, 流量切换时将导致分组失序。另外, 网络未发生失效前, 备份路径的闲置造成了极大的资源浪费。

Makam 方案是一种路径保护方案, 其备份路径建立于 PSL 与 PML 之间。网络发生故障后, 检测到故障的节点会向上游传送故障指示信号(FIS)至 PSL。由 PSL 负责将流量切换至备份路径, 故障恢复后同样向上游发送故障恢复信号(FRS),

以告之 PSL 将流量切换回原工作路径。Makam 方案主要优点为失序分组较少，其缺点是 FIS 必须传至 PSL 后才会实施切换，因而会造成较大时延和丢包。同样，与 Haskin 方案相同，网络发生故障前备份路径的闲置会造成网络带宽资源的大量浪费。

RSVP 方案有两种两种不同的思想实现快速重路由，即一对一备份思想以及设施备份思想。在为网络提供保护时，前者为保护一条具有 N 个结点的保护路径，需建立 N-1 条备份路径，后者是用一条备份路径保护多条保护路径。RSVP 方案优点是丢包率小、故障恢复时间快。缺点是由于为了对网络实行快速恢复，需要预先建立大量的备份路径并预留足够的带宽资源，而备份路径仅仅只在保护路径发生失效后才会承载业务流，因此在故障发生前，备份路径的闲置会造成大量的网络带宽资源浪费。

三种方案均存在一个共同的缺陷，即备份路径的闲置造成网络带宽资源大量浪费。在网络中，带宽资源是极其宝贵的，因此，在保证网络故障及时恢复的同时应更加注重备份带宽资源的合理使用，更好地提高网络资源利用率。

为了提高故障恢复方案中的网络资源利用率，很多优化方案相继被提出。针对路径保护方式，文献[33]提出了一种优化的路径抢占方案，该方案以优先选择消耗资源少的路径实现资源的合理利用。针对 RSVP 方案，IETF RFC4090<sup>[34]</sup>中提出使用合并技术，用以提高网络的带宽资源利用率。即在网络中当发生以下两种情形：(1) 当一条备份 LSP 与保护 LSP 在具有同一出口的路由器上相交时；(2) 当一条保护路径的备份路径经过同一条链路时，网络就实行合并技术通过将具有相同入口与出口路由器的备份链路或备份链路与保护链路相合并降低网络带宽资源的耗费，提高网络资源利用率。

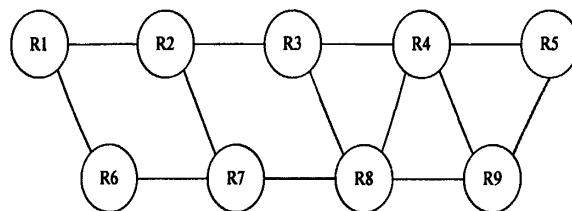


图 4-1 IETF RFC4090 方案网络示例模型图

如图 4-1 所示，使用 RSVP 方案保护路径 {R1-R2-R3-R4-R5}，当这条路径上任何一处发生故障，该方案都能够进行快速恢复。备份路径 {R1-R6-R7-R8-R9} 被

用来保护节点 R2，备份路径 {R2-R7-R8-R4} 被用来保护节点 R3，备份路径 {R3-R8-R9-R5} 被用来保护节点 R4，备份路径 {R4-R9-R5} 用来保护链路 {R4-R5}。如果节点 R2 发生故障，R1 会负责进行故障恢复，R1 会将数据流切换到备份路径 {R1-R6-R7-R8-R3} 上，在 R3 处与原来的保护路径进行合并。其它故障恢复类似。{R7-R8} 和 {R9-R5} 这两条链路同时做了两次保留，{R3-R8} 虽然做了两次保留但是两次保留的方向并不一样。为了降低不必要的带宽资源耗费，IETF RFC4090 提出在 RSVP 方案中使用合并技术，使得链路 {R7-R8} 和 {R9-R5} 共享同一资源。这样原先的十二处保留减少为现在的十处，有效地提高了网络资源的利用率。

IETF RFC4090 提出在 RSVP 方案中通过合并技术解决了同一保护路径的备份资源共享问题，实现了网络带宽资源合理应用。但该方案只能支持网络带宽资源在同一条保护路径的备份路径上进行共享。为了更好地节约备份资源，达到更高的网络带宽资源利用率的目的。本文在 RSVP 方案基础上，提出了一种快速重路由优化方案，即 OFRR 方案，该方案基于 One-to-One 备份思想，具体包含两个方面的内容，一是优化的备份资源信息共享机制，二是优化的备份路径选择算法。OFRR 方案能支持备份带宽资源在网络中实现全局性共享，不仅保证良好的恢复性能，同时能更加合理有效地利用备份带宽资源，更好地提高了网络资源利用率。

## 4.2 优化的备份资源信息共享机制

### 4.2.1 机制思想介绍

在同一网络中，同时发生多处故障的概率是非常小的，甚至是不存在的，所以当两条以上保护路径的备份路径拥有共同的链路时，那么便可以在此共同链路上进行备份带宽资源共享。这样可以大大提高网络资源的利用。

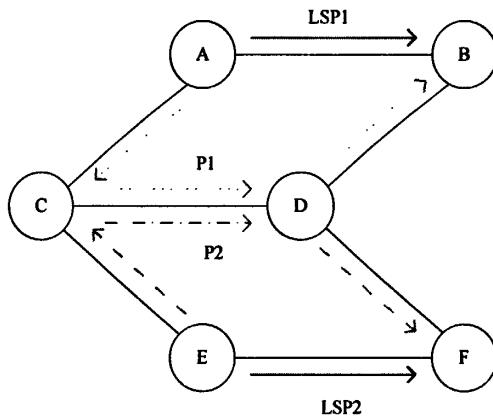


图 4-2 优化的备份资源信息共享机制模型图

如图 4-2 所示为本文所提出的优化的备份资源信息共享机制的简单模型说明。图示为一个 MPLS 网络，该网络具有 6 个节点、7 条链路，有两条保护路径 LSP1: {A-B} 及 LSP2: {E-F}，带宽均为 1 个单位，且各自的备份路径分别为 P1: {A-C-D-B} 及 P2: {E-C-D-F}，可见这两条不同保护路径的备份路径同时经过链路 {C-D}。因 LSP1、LSP2 同时发生故障的几率很小，因此在链路 {C-D} 上只需预留 1 个单位带宽。这样该网络只需预留 5 个单位带宽就能保证网络在发生故障后及时恢复，相比传统机制需预留 6 个单位带宽资源，显然该方案更能节省备份资源。

#### 4.2.2 机制相关定义说明

为详细说明本文所提出的机制方便起见，做如下相关定义：

网络模型图  $G(V, E, C)$ ：MPLS 有向网络模型图， $V$  代表所有节点集合， $E$  代表所有链路集合， $C$  为相关约束条件。

关键结点  $KN$ ：在每条备份链路上，流量输出的节点，预留带宽信息及流量信息在备份路径的所有关键节点中被保存并及时更新。

流量信息  $R_{(l)}[f]$ ：保存在备份路径的关键节点中的一组数组。指故障  $f$  发生后，备份路径上链路  $l$  需要切换的总流量。这里  $f \in \{E\} \cup \{V\}$ ,  $l \in \{E\}$

预留带宽资源  $C_{(l)}(F)$ ：在故障  $f$  发生后，为及时恢复网络，链路  $l$  上所需预留的资源。实际上，

$$C_l(F) = \max R_{(l)}[f] = \max \{R_{(l)}[f_0], R_{(l)}[f_1], \dots\} \quad (4-1)$$

重要性指数  $p$ ：网络的每个部分都具有各自不同的重要性，本文规定：

$$p = \begin{cases} 100\% & \text{(具有很高重要性)} \\ 50\% & \text{(具有较高重要性)} \\ 25\% & \text{(具有高重要性)} \end{cases} \quad (4-2)$$

预约因子  $\alpha$ ：根据网络不同部分不同的重要性指数  $p$ ，对不同部分的局部保护备份资源进行不同预约分配，具体分配数值等于所需带宽与预约因子的乘积，本文规定：

$$\alpha = \begin{cases} 1 & p = 100\% \\ 0.5 & p = 50\% \\ 0.25 & p = 25\% \end{cases} \quad (4-3)$$

#### 4.2.3 机制实现详细步骤

优化的备份资源信息共享机制设计目标如下：(1) 同一保护路径的备份路径在共同链路上应进行资源共享；(2) 基于在同一网络中，同时发生多处故障的概率非常小，甚至是不存在的。不同保护路径的备份路径在共同链路上可进行资源共享；(3) 网络链路上必须预留足够的带宽资源保证网络发生故障时能及时进行恢复；(4) 网络所需预留的总带宽资源尽可能最小化。图 4-3 为机制实现详细步骤图。

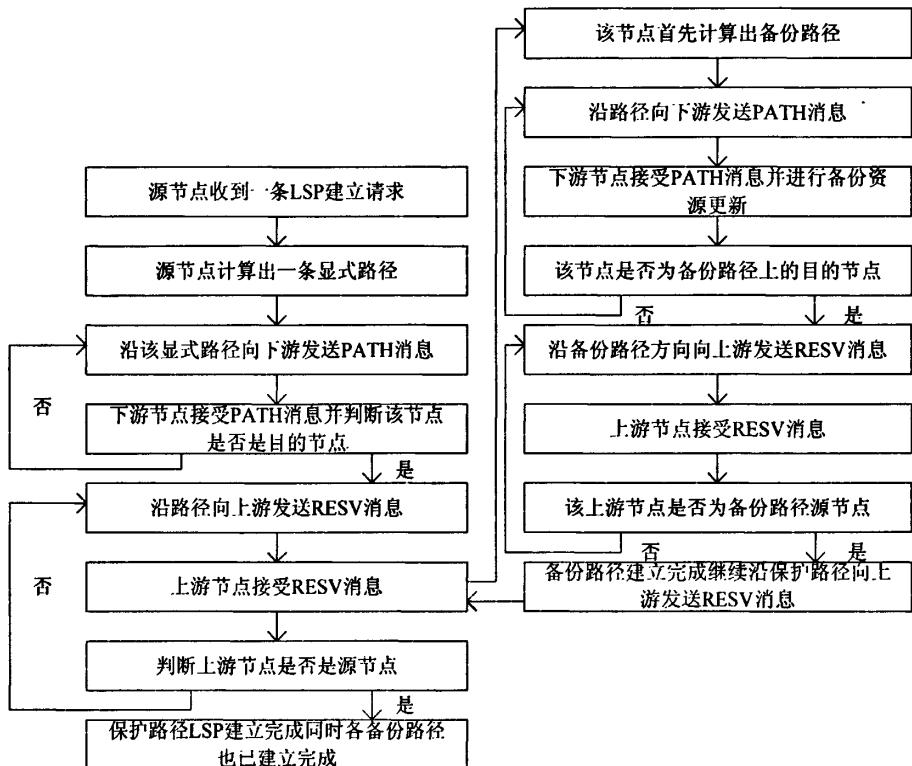


图 4-3 优化的备份资源信息共享机制实现步骤

在优化的备份资源信息共享机制中，所使用的信令协议是基于流量工程扩展的资源预留协议（RSVP-TE）。该机制最重要的一点便是链路上关键节点对备份资源信息，即预留带宽资源  $C_{(l)}(F)$  的更新，该数值保存在备份路径的所有关键节点中，具体指故障发生后为及时很好地恢复网络，链路<sup>l</sup>上所需预留的带宽资源。为了在关键节点中很好地对备份带宽资源进行管理，该机制设定用于构建备份路径的 PATH 消息携带保护路径上故障检测节点的直接下游节点以及直接下游链路的消息，具体指直接下游链路/节点所承载的全部流量。

在备份路径的建立过程中，备份路径上的各关键节点根据 PATH 携带的消息对  $C_{(l)}(F)$  进行如下更新：

$$C_{(l)}(F) \leftarrow \max(C_{(l)}(F), b * \alpha) \quad (4-4)$$

在式 (4-4) 中， $b$  具体指发生故障的链路或节点所承载的全部流量，实际上  $b = R_{(l)}[f_a]$ ， $\alpha$  为发生故障部分的预约因子。当网络中某一源节点收到 LSP 的撤销消息，网络必须同时撤销保护 LSP 以及相应的备份路径。同时释放这些路径上

的带宽资源。在备份路径的撤销过程中，同样也应用到的是 RSVP-TE 协议。具体执行时，保护路径的源节点会沿着保护路径发送一条 PATHTEAR 消息给目的节点。收到 PATHTEAR 消息的保护路径中的各个节点相应会沿着各自的备份路径发送 PATHTEAR 消息。为了释放掉备份路径上预留备份带宽资源，该机制设定各节点发送的 PATHTEAR 消息携带各个节点的直接下游节点以及直接下游链路的相关信息，具体指直接下游节点/链路承载的总的流量。备份路径上的关键节点可以依据此信息对各自的数据信息进行如下的更新：

$$C_{(l)}(F) \leftarrow \max(C_{(l)}(F) - b, R_{(l)}[f]), R_{(l)}[f] = \{R_{(l)}[f_0], R_{(l)}[f_1], \dots\} \quad (4-5)$$

在式 (4-5) 中， $b$  指的是备份路径上 PATHTEAR 消息所携带的信息，即直接下游链路/节点承载的总的流量值。

#### 4.2.4 机制具体实现

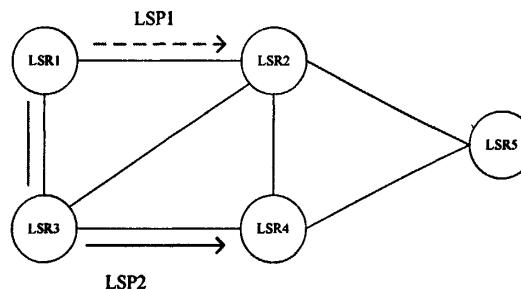


图 4-4 优化的备份资源信息共享机制示例

图 4-4 所示为一个具有 5 个节点及 7 条链路的 MPLS 网络。假设该网络已经存在一条保护路径 LSP1：{LSR1-LSR2} 且为其分配 1 个单位带宽，记为  $A_{(LSR1-LSR2)} = 1$ 。同时存在 LSP1 的备份路径 P1：{LSR1-LSR3-LSR2}，且链路 {LSR1-LSR3}、{LSR3-LSR2} 上预留备份带宽资源均为 1 个单位带宽，记为  $B_{(LSR1-LSR3)} = B_{(LSR3-LSR2)} = 1$ 。现在另一条 LSP 请求到达节点 LSR1，要求 LSR1 建立一条从 LSR1 到 LSR4 的 LSP2 且带宽同样为 1 个单位。此时网络状态为：节点 LSR1 中含有信息： $C_{(LSR1-LSR3)}(F) = 1$ ，在此  $F = \{LSR1-LSR2\}$ ；LSR3 具有信息： $C_{(LSR3-LSR2)}(F) = 1$ ， $F = \{LSR1-LSR2\}$ 。

节点 LSR1 首先计算出具体 LSP2：{LSR1-LSR3-LSR4}，接着 LSR1 发送 PATH

消息并沿着计算好的保护路径 {LSR1-LSR3-LSR4} 发送, 当目的节点 LSR4 收到该消息后立即沿着路径 LSP2 向上游回送 RESV 消息, 节点 LSR3 首先收到 RESV 消息, 立即计算出用以保护链路 {LSR3-LSR4} 的备份路径  $P21$ : {LSR3-LSR2-LSR4}, 随后 LSR3 沿着该备份路径发送携带有链路 {LSR3-LSR4} 相关信息的 PATH 消息, 根据此 PATH 消息备份路径上的所有关键节点分别对各自所需备份资源数值进行更新, 在此分别列出为:

节点 LSR3:

$$C_{(LSR3-LSR2)}(F) \rightarrow C_{(LSR3-LSR2)}(F) = \max(C_{(LSR3-LSR2)}(F), b * \alpha) = 1, b = 1, \alpha = 1 \quad (4-6)$$

节点 LSR2:

$$C_{(LSR2-LSR4)}(F) = 1 \quad (4-7)$$

完成后, RESV 消息继续沿路径 LSP2 向上游发送, 最后节点 LSR1 收到 RESV 消息, 同样节点 LSR1 开始计算相关备份路径, 而对于该节点, 根据节点保护和链路保护的定义, 需分别建立两条不同的路径  $P22$ : {LSR1-LSR2-LSR4} 及  $P23$ : {LSR1-LSR2-LSR3} 分别用以在节点 LSR3 以及链路 {LSR1-LSR3} 发生故障后的网络恢复。由于实际操作过程中, 节点 LSR1 无法辨别具体是直接下游节点还是直接下游链路发生故障, 因此本文只单纯考虑节点保护, 那么只需建立备份路径  $P22$ : {LSR1-LSR2-LSR4} 用以在节点 LSR3 发生故障后网络及时恢复, 显然对节点的保护也必然包含了对在该条保护路径上与该节点相连的所有链路的保护。计算好备份路径后接着 LSR1 沿着这条备份路径发送 PATH 消息, PATH 消息携带节点 LSR3 相关信息 (即节点 LSR3 承载的总的流量), 在此本文假设节点 LSR3 的重要性指数为  $\rho = 50\%$ 。备份路径上的关键节点依据此 PATH 消息进行备份带宽资源的数据更新, 分别列出为:

节点 LSR1:

$$C_{(LSR1-LSR2)}(F) = b * \alpha = 1 * 0.5 = 0.5, F = LSR3 \quad (4-8)$$

节点 LSR2:

$$C_{(LSR2-LSR4)}(F) \rightarrow C_{(LSR2-LSR4)}(F) = \max(C_{(LSR2-LSR4)}(F), b * \alpha) = \max(1, 0.5) = 1$$

$$F \in \{LSR3-LSR4\} \cup LSR3 \quad (4-9)$$

在网络所有的保护路径以及备份路径均建立好后，网络最后的资源消耗情况为：

$$\begin{aligned}
 A_{(LSR1-LSR2)} &= A_{(LSR1-LSR3)} = A_{(LSR3-LSR4)} = 1 \\
 B_{(LSR1-LSR3)} &= B_{(LSR3-LSR2)} = B_{(LSR2-LSR4)} = 1 \\
 B_{(LSR1-LSR2)} &= 0.5
 \end{aligned} \tag{4-10}$$

因此总的消耗资源为 Total=6.5. 在链路 {LSR3-LSR2} 上只需预留 1 个单位的带宽是因为保护路径 LSP1 和 LSP2 同时出现故障的概率非常小，甚至不存在。若不能根据不同的重要性指数选择性进行资源分配，则需消耗总资源为：Total=7；若网络不能提供备份资源全局性共享则总共需消耗资源为：Total=9. 显然本文所提出的优化的备份资源信息共享机制可以明显降低对备份资源的消耗度，有效节约网络资源。

当备份路径撤销时，备份路径上的关键节点也需要及时对预留带宽资源信息进行更新。针对本示例网络，此时假设节点 LSR1 收到保护路径 LSP1 的撤销请求，节点 LSR1 需要同时进行对保护路径以及相关的备份路径的撤销。在用 RSVP-TE 执行撤销请求过程中，节点 LSR1 首先沿着保护路径 LSP1 发送 PATHTEAR 消息给目的节点，保护路径上沿途收到 PATHTEAR 消息的各个节点会执行保护路径的撤销，于此同时会沿着各自的备份路径发送 PATHTEAR 消息实现备份路径的撤销。在本示例网络中，节点 LSR1 的下一个节点 LSR2 也即目的节点会受到上游发送过来的 PATHTEAR 消息，节点 LSR2 立即执行保护路径的撤销同时沿着备份路径发送 PATHTEAR 消息，为了释放掉备份路径上预留备份带宽资源，优化的备份资源信息共享机制设定备份路径上发送的 PATHTEAR 消息携带各个节点的直接下游节点以及直接下游链路的相关信息（在本例中具体指的是链路 {LSR1-LSR2} 上承载的总的流量），这样备份路径上的关键节点就可以依据此信息对各自的备份带宽资源信息进行更新，本例中节点 LSR1、LSR3 分别对备份带宽资源信息作如下更新：

节点 LSR1：

$$\begin{aligned}
 C_{(LSR1-LSR3)}(F) &\leftarrow \max(C_{(LSR1-LSR3)}(F) - b, R_{(LSR1-LSR3)}[f]) = \max(1 - 1, 0) = 0 \\
 R_{(LSR1-LSR3)}[f] &= \emptyset \\
 b &= 1
 \end{aligned} \tag{4-11}$$

节点 LSR3：

$$C_{(LSR3-LSR2)}(F) \leftarrow \max(C_{(LSR3-LSR2)}(F) - b, R_{(LSR3-LSR2)}[f]) = \max(1-1, 1) = 1$$

$$R_{(LSR3-LSR2)}[f] = \{R_{(LSR3-LSR2)}[f_1]\}, f_1 = \{LSR3-LSR4\}$$

$$b = 1 \quad (4-12)$$

路径撤销请求以及相关备份带宽资源更新执行完后的网络状态为：

$$A_{(LSR1-LSR3)} = A_{(LSR3-LSR4)} = 1$$

$$B_{(LSR3-LSR2)} = B_{(LSR2-LSR4)} = 1$$

$$B_{(LSR1-LSR2)} = 0.5$$

$$(4-13)$$

网络总的资源消耗为  $Total=4.5$ ，显然优化的备份资源信息共享机制既保证了网络预留充分足够的带宽资源确保发生故障后的及时恢复，也杜绝了造成对网络带宽资源不必要的浪费。

### 4.3 优化的备份路径选择算法

#### 4.3.1 算法思想介绍

前文所提出的优化的备份资源信息共享机制可以使预留备份带宽资源全局性地在备份路径间共享，基于此性能，通过对备份路径选择算法进行优化从而达到进一步降低对网络预留资源需求的目的。

优化的备份路径选择算法同样也是基于一对备份思想，其设计目标为：(1) 尽最大可能保证为最短跳数路由，降低延时；(2) 尽最大可能保证对链路备份带宽资源进行充分利用，提高网络带宽资源利用率；(3) 保证备份路径的链路带宽满足应用的需要，确保故障发生后能及时切换流量，降低丢包率。

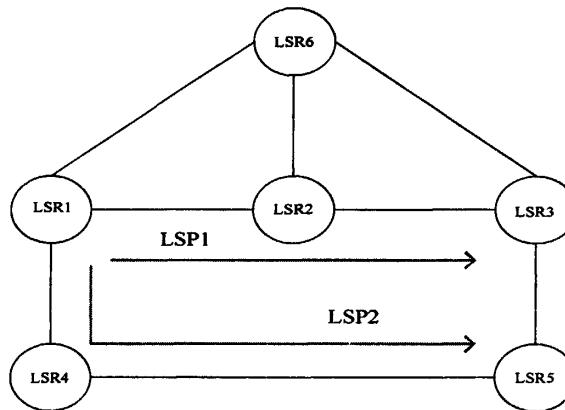


图 4-5 路由算法网络模型示例图

图 4-5 是对本思想方案的一个简略介绍。如图所示为一个 MPLS 网络，具有 6 个节点和 7 条链路。假定网络中已存在一条保护路径 LSP1，从节点 LSR1 到节点 LSR3 并且消耗的资源为 1 个带宽单位，同时 LSP1 的备份路径  $P1$ 、 $P2$  均已建立好，分别为： $P1 = \{LSR1-LSR6-LSR3\}$ ； $P2 = \{LSR2-LSR6-LSR3\}$ 。接着节点 LSR1 又收到一条保护路径 LSP2 的建立请求，要求建立一条从节点 LSR1 到节点 LSR5 的保护路径 LSP2，同时要求所消耗的带宽资源为 2 个带宽单位。节点 LSR1 根据相应路由算法计算好保护路径后后，该 LSP2 为  $\{LSR1-LSR4-LSR5\}$ ，接着开始进行备份路径的建立，假定在此首先选择  $\{LSR1-LSR2-LSR3-LSR5\}$  作为节点 LSR1 的备份路径  $P11$ ，节点 LSR4 选择  $\{LSR4-LSR1-LSR2-LSR3-LSR5\}$  作为它的备份路径  $P12$ ，这样总的所消耗的备份带宽资源为 11 个带宽单位。假如节点 LSR1 不是选择  $P11$  而是选择  $P21 = \{LSR1-LSR6-LSR3-LSR5\}$  作为它的备份路径，同样节点 LSR4 选择  $P22 = \{LSR4-LSR1-LSR6-LSR3-LSR5\}$  作为它的备份路径。由于在网络中这两条保护路径同时发生故障的几率很小，甚至是不存在的。因此备份路径可以共享共同链路上的预留带宽资源。那么，整个网络所需的备份预留资源为 9 个带宽单位。显然，相比前一种备份路径选择算法，本文所提出的优化算法就节省了 2 个带宽单位的预留资源，减少网络资源不必要的消耗，相应提高了网络资源利用率。

#### 4.3.2 算法具体描述

Dijkstra(迪杰斯特拉)<sup>[35]</sup>算法是典型的单源最短路径算法，用于计算一个节

点到其他所有节点的最短路径。主要特点是以起始点为中心向外层层扩展，直到扩展到终点为止。Dijkstra 算法是很有代表性的最短路径算法，其优点是简单，适用于拓扑变化不大的网络中运行。本文所提出的备份路径优化选择算法基于 Dijkstra 算法。

在本章 4.2.2 小节规定了两个数据信息概念，分别为预留带宽资源  $C_{(l)}(F)$  以及流量信息  $R_{(l)}[f]$ ，它们均保存在网络备份路径的关键节点中。前者指网络发生故障后为了及时进行恢复，在备份路径链路  $l$  上所需预留的总的带宽资源；后者指某条保护路径发生故障后，需要在备份路径链路  $l$  上切换的总流量。实际上  $C_{(l)}(F) = \max R_{(l)}[f]$ 。在此，本文定义另一数据信息概念，即链路  $l$  上可共享的备份带宽资源  $r(l)$ ， $r(l)$  可通过下式计算得出：

$$r(l) = C_{(l)}(F) - R_{(l)}[f_a] \quad (4-14)$$

那么，链路  $l$  上的权重则定义为：

$$w(l) = \begin{cases} [b - r(l)] * W_{ij} & \text{if } (b > r(l)) \text{ and } l \notin \{e_1\} \\ W_{ij} & \text{if } (b \leq r(l)) \\ \infty & \text{if } (l \in \{e_1\}) \\ 0 & \text{if } (l \in \{e_2\}) \end{cases} \quad (4-15)$$

在式 (4-15) 中， $b$  表示故障发生节点上所承载的总流量值， $\{e_1\}$  表示在保护路径上与故障发生节点直接相连的所有链路集合， $\{e_2\}$  表示在保护路径上与故障发生节点不直接相连的所有链路集合，式中  $W_{ij}$  规定为：

$$W_{ij} = \begin{cases} 1 & \text{节点 } i \text{ 与节点 } j \text{ 之间直接相连} \\ \infty & \text{节点 } i \text{ 与节点 } j \text{ 之间不直接相连} \end{cases} \quad (4-16)$$

优化的备份路径选择算法具体描述如下：

算法输入：源节点  $S$ 、临时节点集合  $\{T\}$ 、预留带宽资源  $C_{(l)}(F)$ 、流量信息  $R_{(l)}[f]$ 、链路可共享的备份带宽资源  $r(l)$ 、最短路径值  $d(n)$ 。

算法输出：符合当前条件的备份路径。

算法详细步骤：

## (1) 初始化

$M = \{S\}$ , 即临时节点集合中只有源节点。 $d(S) = 1$

## (2) 取下一个节点

找到不在  $\{T\}$  中且到源节点  $S$  有最短路径值的相邻节点, 把它加入到临时节点集合  $\{T\}$  中, 把依附于该节点和  $\{T\}$  中某节点构成路径的边也加入到  $\{T\}$  中。

## (3) 更新最短路径值

$$d(n) = \min[d(n), d(i) + w(l)] \quad (4-17)$$

最短路径值的更新根据式 (4-17), 在该式中,  $d(i)$  就是从  $S$  到  $i$  的最短路径值,  $l$  具体指链路  $\{i-n\}$ 。对所有  $i: i \notin \{T\}$ , 如果第二项小, 则从  $S$  到  $n$  的路径从现在起就是从  $S$  到  $i$  再连上  $i$  与  $n$  之间的边。当所有的节点都加入到  $\{T\}$  以后, 算法结束。

步骤 (2) 和步骤 (3) 要重复执行, 直至  $\{T\} = \{N\}$ ,  $\{N\}$  表示所建立的备份路径上所有节点集合。也就是说, 步骤 (2) 和步骤 (3) 在重复到网络中所有节点都已经找到最终路径为止。

#### 4.3.3 相关重要说明

无论保护路径的建立或是备份路径的建立都是基于路由器获得网络状态信息的基础上。而网络状态信息一般是通过路由协议发布的。路由协议一般在以下三种情况下对路由信息进行发布: (1) 当链路生效或失效时; (2) 当链路配置发生变化时 (例如, 链路代价得到更新); (3) 当到达周期性对路由器的路由信息进行发布的时候。一般, 将路由信息分为最小化信息、部分信息、完整性信息三种。其中最小化信息仅包括每条链路上的可用带宽资源, 部分信息包含每条链路上的可用带宽资源<sup>[36]</sup>以及总的预留带宽资源, 完整性信息包括保护路径以及备份路径上的所有网络状态信息。

本文所提出的备份路径选择优化算法中, 是通过在相邻路由器之间发送及接受网络部分信息, 并且在整个网络中以分布式的方式构建备份路径。前文相继详细描述了优化的备份资源信息共享机制以及备份路径优化选择算法, 分别涉及到这几类数据  $C_{(l)}(F)$ ,  $b$ ,  $r(l)$ ,  $R_{(l)}[f]$ 。 $C_{(l)}(F)$  相当于网络中链路上的总预留

带宽资源信息，通过目前的路由协议便可以在网络中发送及接受。 $b$  表示故障发生部分所承载的总的流量， $R_{(l)}[f]$  表示当某条保护路径发生故障后，需要在备份路径链路  $l$  上切换的总流量，实际上， $b = R_{(l)}[f]$ 。在已获知  $R_{(l)}[f]$ 、 $C_{(l)}(F)$  信息的基础上，就可以直接计算出  $r(l)$  的值为：

$$r(l) = C_{(l)}(F) - R_{(l)}[f] \quad (4-18)$$

因此，关键的一点便是  $R_{(l)}[f]$  信息获知以及在网络相邻路由器之间的发送以及接收。本文所提出的优化方案通过 RSVP-TE 协议实现该数据信息在网络中发送以及接收。

资源预留协议 RSVP 是与 20 世纪 90 年代中期，为了防止网络阻塞，实现 IP QoS 而开发的。它通过路由器事先判断网络资源是否能够满足数据流传输的需求，如果可以的话，RSVP 协议将会为数据流预留出相应的资源，以保证其在网络中的服务质量。作为已经有十多年历史的技术，RSVP 几乎已经成了企业网 IP QoS 的标准。在标签分配协议信令选择上，采取了基于流量工程 TE 扩展的资源预留协议 RSVP-TE<sup>[37]</sup>的方案，因为 RSVP-TE<sup>[38]</sup>的 QoS 能力可以很好地与现有的企业网的 IP QoS 融合。同时 RSVP-TE 拥有很多优点，RSVP-TE 可以支持最基本的标签交换路径 LSP 的建立，在自动地绕开网络故障及阻塞等方面有着其独特的优势；同时，RSVP-TE 通过使流量工程处理自动化简化了网络的运行。RSVP-TE 支持要求资源预留和不要求资源预留的显式路由标签交换路径 ER-LDP，RSVP-TE 也支持 LSP 的重路由，资源抢占和环路检测。同时为了克服其自身在扩展性方面的缺陷，还提出了一系列卓有成效的解决措施。总之，作为 MPLS 的信令协议，尤其是为了能够在 MPLS 流量工程中应用，RSVP-TE 发挥了很重要的作用。

RSVP-TE 协议有两类不同的消息，分别是表示路径方面的 PATH 消息与表示预留方面的 RESV 消息。为了在网络中实现分发与接收  $R_{(l)}[f]$  信息。分别在 PATH 消息中添加 ASK 对象，在 RESV 消息中添加 REPLY 对象，并且另设定一个 INFORM 消息，以下是对此三种信令的具体功能描述：

INFORM：在备份路径构建/撤销前，从检测到故障发生的节点沿备份路径发送。告知下游节点保护路径的相关信息，即保护路径上的所有节点/链路。

ASK: 在备份路径构建前, 检测到故障发生的节点沿保护路径向直接下游节点发送, 询问相关资源信息, 即直接下游节点上所承载的总流量值。

REPLY: 收到 ASK 的节点沿保护路径反向发送给检测到故障发生的节点, 告知该节点所要询问的相关信息。

#### 4.4 OFRR 方案的分析与评价

论文在对经典快速重路由方案研究的基础上, 具体针对所存在的备份带宽资源浪费的问题, 提出一种快速重路由优化方案, 即 OFRR 方案, 该方案包含两个方面内容, 一是优化的备份资源信息共享机制, 通过使备份路径中的关键节点掌握有限范围内的节点与链路的相关信息, 实现对备份资源的有效共享管理, 可以支持备份带宽资源在网络中全局性共享; 二是优化的备份路径选择算法, 该算法基于经典最短路径算法 Dijkstra 算法, 通过在链路权重中添加带宽资源的限制, 优先选择预留带宽资源大的链路, 可进一步降低对网络预留资源的需求。

##### 4.4.1 OFRR 方案的可扩展性好

OFRR 方案可扩展性好, 主要表现在两个方面, 首先, OFRR 方案不需要网络中所有的 LSR 保存有关所有保护 LSP 以及备份 LSP 相关的所有信息, 而只需在网络的关键节点 KN 上保留两类信息, 即:  $R_{(t)}[f]$ 、 $C_{(t)}(F)$ ; 其次, OFRR 方案不需要在整个网络中广播路由信息, 只需在网络相邻节点间进行三种信令交换。OFRR 方案通过 RSVP-TE 信令协议进行所需信息的交换, 因为信令交换仅在相邻节点间执行, 同时 OFRR 方案所引进的三种信令在实际执行过程中, ASK 信令以及 REPLY 信令均是被嵌入在 RSVP-TE 自带的 PATH 信令、RESV 信令中, 仅仅只有 INFORM 信令是需额外添加的, 因此传输信令开销非常小。

##### 4.4.2 OFRR 方案网络资源利用率高

OFRR 方案基于 One-to-One 备份思想, 采用分布式快速重路由方法, 对 MPLS 网络中每个节点按照不同的业务流量需求在故障出现之前预先建立好备份路径并预留充分的备份带宽资源, 如果存在路径必然在其备份路径中, 所以 OFRR 方

案比 Makam 方案、Haskin 方案具有更高的重路由成功率，由于预先建立好备份路径，OFRR 方案在发生故障时能够实现数据流快速切换，因而丢包率很小。另外，OFRR 方案支持备份带宽资源在同一保护路径以及不同保护路径的备份链路上全局性进行共享，因此，相比原有 FRR 方案，具有更高的网络资源利用率。

## 4.5 本章小结

本章首先回顾了经典快速重路由方案，简要分析了各方案的优点与缺点。接着，具体针对各方案所存在的一个共同的缺陷，即备份路径的闲置所造成的大带宽资源浪费的问题，提出了一种快速重路由优化方案，该方案具体包含两方面的内容，即备份资源信息共享机制以及备份路径优化选择算法。本章分别就这两个方面对新方案进行了详细的叙述。最后是对新方案的分析与评价。

## 第五章 仿真实验实现与结果分析

为了研究各种 MPLS FRR 方案的性能, 本章利用 OPNET 网络仿真工具搭建了一个 MPLS 仿真平台, 建立仿真网络模型, 设置仿真参数, 配置运行仿真, 应用对比方法, 分别对 Makam 方案、Haskin 方案、RSVP 方案几种经典快速重路由方案和新方案在丢包率、业务流切换时间和网络资源利用率三方面进行了仿真。

### 5.1 OPNET 仿真环境介绍

OPNET Modeler<sup>[39]</sup>是 OPNET 公司的第一个商用化产品, 为通信网络和分布式系统建模提供了全面的模拟仿真开发环境。OPNET Modeler 相比 NS-2, 在软件功能及操作易用性两方面具有较好的优势。首先在软件功能方面, OPNET Modeler 做的比较完备, 可以对分组到达时间分布、分组长度分布, 网络节点类型和链路类型等进行很详细的设置, 可以通过不同厂家提供的网络设备和应用场景设计不同的仿真环境。而 NS2 只能根据实际仿真环境通过脚本建立逻辑的网络结构, 而且查看结果需要其他软件的辅助。在操作易用性方面, OPNET Modeler 可以使用比较少的操作得到比较详尽和真实的仿真结果。而 NS2 则要通过编写脚本和 C++ 代码来实现网络仿真。

#### 5.1.1 仿真软件介绍

OPNET 公司起源于麻省理工学院 (MIT), 成立于 1986 年。1987 年 OPNET 公司发布了第一个商业化的网络性能仿真软件, 提供了具有重要意义的网络性能优化工具, 使得具有预测性的网络性能管理和仿真成为可能。OPNET 公司的第一个商用化产品为 Modeler, 在此基础上又开发出了其他产品, 使得其产品得种类更加丰富。在 OPNET 各种产品中, Modeler 主要面向研发, 其宗旨是加速网络研发。Modeler 几乎包含其他产品的功能, 并且针对不同领域, 表现出不同用途。

OPNET Modeler10.0 和其他的网络仿真软件进行比较, 具有如下的突出特点, 使得它能够满足大型复杂网络的仿真需要:

- (1) 层次化的网络模型。使用无限嵌套的子网来建立复杂的网络拓扑结构。

(2) 简单明了的建模方法, 提供三层建模机制, 底层为 Process 模型, 以状态机来描述协议; 其次为 Node 模型, 由相应的协议模型构成, 反映设备特性; 最上层为网络模型。在进程层次模拟单个对象的行为, 在节点层次中将其互连成设备, 在网络层次中将这些设备互连组成网络。几个不同的网络场景组成“项目”, 用以比较不同的设计方案。这也是 Modeler 建模的重要机制, 这种机制有利于项目的管理和分工。三层模型和实际的网络、设备、协议层次完全对应, 全面反映了网络的相关特性;

(3) 有限状态机。在进程层次使用有限状态机来对协议和其他进程进行建模。在有限状态机的状态和转移条件中使用 C/C 十字语一言对任何过程进行模拟。用户可以随心所欲地控制仿真的详细程度。有限状态机加上标准的 C/C++ 以及 OPNET 本身提供的 400 多个库函数构成了 Modeler 编程的核心。OPNET 称这个集合为 Proto C 语言

(4) 对协议编程的全面支持。支持 400 多个库函数以及书写风格简洁的协议模型。OPNET 的核心已经嵌入了众多协议, 因此对于很多协议, 无需进行额外的编程;

(5) 系统的完全开放性。Modeler 中源码全部开放, 用户可以根据自己的需要添加、修改已有的源码。

(6) 高效的仿真引擎。使用 Modeler 进行开发的仿真平台, 使仿真的效率相当高。采用混合建模机制, 把基于包的分析方法和基于统计的数学建模方法结合起来, 既可得到非常细节的模拟结果, 也大大提高了仿真效率;

(7) OPNET 具有丰富的统计量收集和分析功能。它可以直接收集常用的各个网络层次的性能统计参数, 能够方便地编制和输出仿真报告;

(8) 提供了和网管系统、流量监测系统的接口, 能够方便的利用现有的拓扑和流量数据建立仿真模型, 同时还可对仿真结果进行验证。

(9) 集成调试器。快速地验证仿真或发现仿真中存在的问题, OPNET 本身有自己的调试工具——OPNET Debugger(ODB)。另外, OPNET 在 Windows 平台上还支持和编程语言 VC 的联合调试。

OPNET Modeler<sup>[40]</sup>是 MIL3 公司的 OPNET 仿真系列产品中的一个, 它为设计通信协议、设备、网络和应用提供了十分强大的 R&D 平台。它可运行在 SUN、HP、

WindowsNT/2000/XP 等多种工作站平台上。本论文中仿真实验使用 OPNET Modeler 的版本是 10.0.A。

### 5.1.2 仿真实现过程

使用 Modeler 仿真可以大体分为 6 个步骤, 分别是配置网络拓扑(Topology)、配置业务 (Traffic)、收集结果统计量 (Statistics)、运行仿真 (Simulation)、调试模块再次仿真 (Re-simulation)、最后发布结果和拓扑报告 (Report)。OPNET Modeler 面向对象的建模方法和图形化的编辑器反映了实验网络和网络组件的结构, 因此, 实际的系统可以直观地映射到模型中, OPNET Modeler 支持所有的网络类型。图 5-1 显示了使用 Modeler 进行仿真的一般过程图, 给出了本文仿真实验从建立模型、运行仿真到收集最后结果的一整套具体步骤。

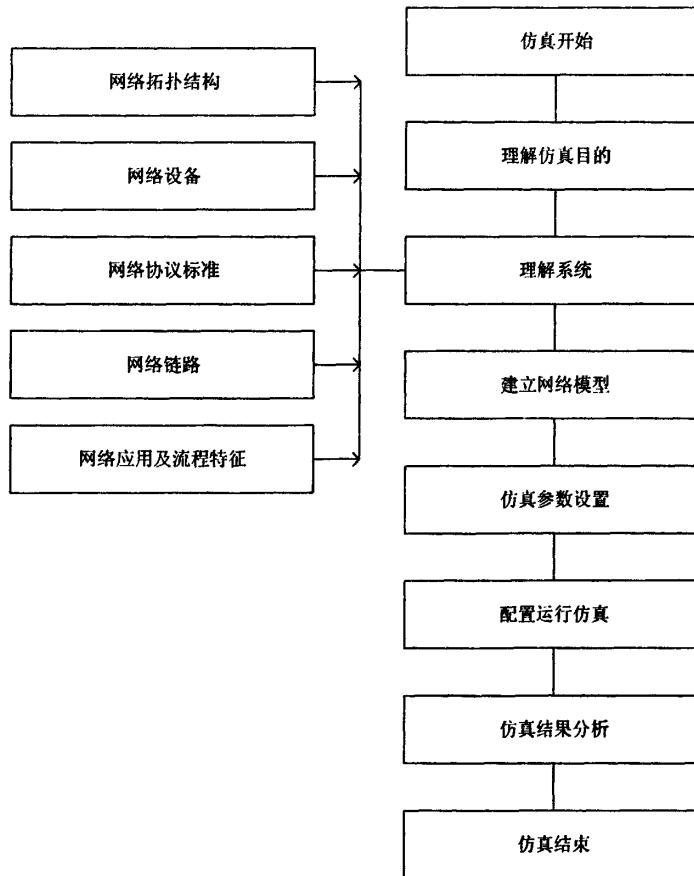


图 5-1 网络仿真过程

## 5.2 仿真环境设计

### 5.2.1 网络模型建立

本文使用 OPNET 网络仿真软件，利用该软件原有的网络模块建立仿真网络模型，并在该模型下设定四种场景，分别用以分析 Makam 方案、Haskin 方案、RSVP 方案以及本文提出的 OFRR 方案的丢包率、业务流切换时间以及网络资源利用率性能并将各个方案性能进行了分析比较。图 5-2 所示为本文仿真所用网络模型。

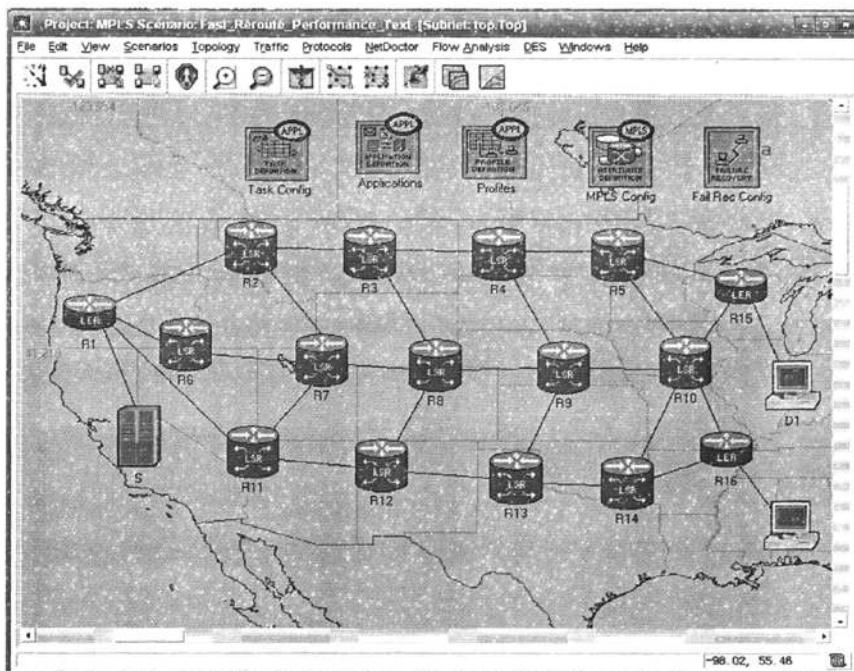
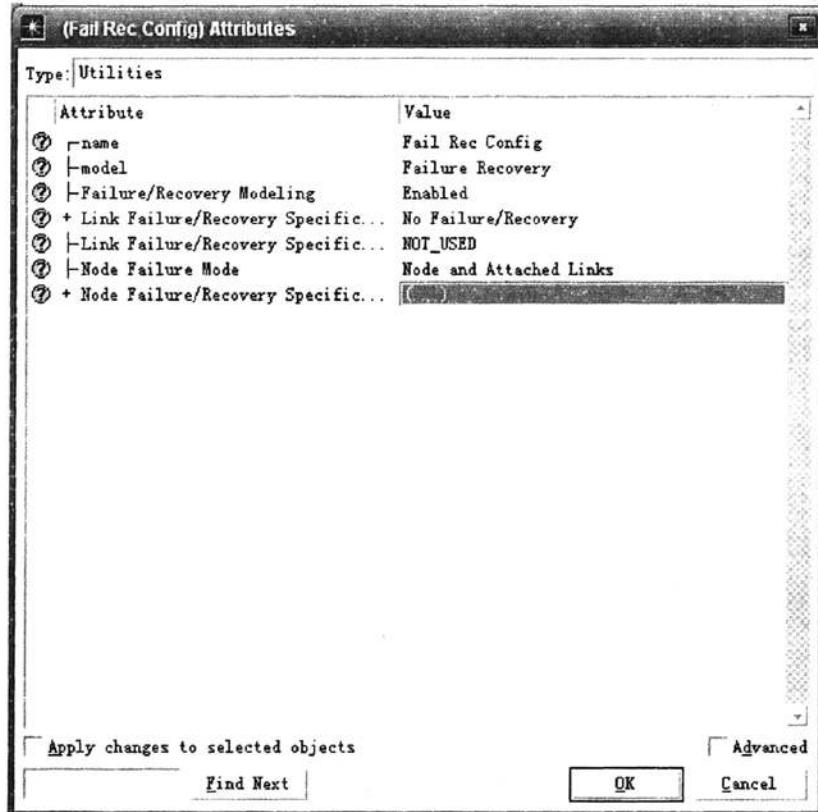


图 5-2 网络仿真模型

如图 5-2 所示，R2-R14 是标签交换路由器，R1、R15、R16 是边缘标签交换路由器，共同组成了 MPLS 域。网络模型中共有 19 个路由节点，包括 3 个 LER(边缘标签交换路由器)，13 个 LSR(标签交换路由器)，2 个工作站，一个服务器。边缘链路采用 PPPDS3，核心链路采用 PPPOC3。节点 S 作为服务器，节点 D1、D2 作为两个客户端，由服务器和客户端构成的流量源，宿模型，服务器 S 分别向向客户端 D1、D2 发送数据包。数据包的大小为 512 个字节。MPLS 域内运行 RSVP-TE 协议，同时根据需求建立两条保护路径，分别为：LSP1={R1-R2-R3-R4-R5-R15}；LSP2={R1-R11-R12-R13-R14-R16}。网络模型配置完成后，使用该网络模型图进行 4 个场景的仿真：场景 1 采用 Makam 方案实行故障恢复功能；场景 2 采用 Haskin

方案实现故障恢复功能；场景3采用RSVP方案对网络实行故障恢复功能。场景4采用本文提出的优化方案OFRR方案实现故障恢复功能。接着在对象“Failure/Recovery”的属性中配置好相关节点的故障和恢复动作。如下图5-3所示，本文设置是使节点在仿真时间的400s时故障，在800s时恢复工作。



(a) 对象 Failure/Recovery 的属性界面

Name	Time	Status
Unspecified	400	Fail
Unspecified	800	Recover

(b) Node Failure/Recovery 属性配置界面

图5-3 配置节点的故障和恢复动作

### 5.2.2 仿真参数设置

在本文的仿真过程中,选取了丢包率、业务流切换时间和网络资源利用率这三个定量指标作为统计指标,其定义分别为:

#### (1) 丢包率

丢包率  $d_p$  指所丢失数据包数量占所发送数据包的比率。 $d_p = \frac{N_{sp} - N_{rp}}{N_{sp}}$ ,

在此,  $N_{sp}$ =发送的数据包数;  $N_{rp}$ =接收到的数据包数。该值越小,说明丢包越少,方案性能越好。

#### (2) 业务流切换时间

业务流切换时间  $T_s$  指从链路故障之前目的节点收到的最后一个数据包到目的节点收到的第一个从备份路径传来的数据包之间的时间。 $T_s = T_a - T_b$ , 在此,  $T_b$  为链路发生故障之前目的节点收到的最后一个数据包的时间,  $T_a$  为目地节点收到从备份路径传来的第一个数据包的时间。该值表示方案的快速修复能力,值越小,表明修复速度越快,方案恢复性能越好。

#### (3) 网络资源利用率

网络资源利用率  $r_b$  指备份路径中预留的带宽资源占网络总消耗带宽资源的比值。 $r_b = \frac{B_t - B_p}{B_t}$ , 在此,  $B_t$ =网络总消耗的带宽资源;  $B_p$ =保护路径上消耗的带宽资源。在MPLS快速重路由的各种方案中均涉及到保护路径以及备份路径的概念,虽然是在网络发生故障后才将流量切换到备份路径上进行转发,但是仍然需要在备份路径上预留足够的带宽资源用以保证网络发生故障后快速进行恢复。网络带宽资源是非常宝贵的,因此如何更好地合理地利用带宽资源对网络恢复方案而言至关重要。在仿真结果中,该值越小说明方案性能越好,更好地减少了对备份带宽资源的需求,更有效地节约了网络带宽资源。

### 5.2.3 仿真配置运行

实际运行仿真时,参数配置如图 5-4 所示,仿真时间为 30 minutes,发送

UDP 数据流从节点 S 经 MPLS 域分别发往节点 D1、D2。在仿真内核(Simulation Kernel)选用 Optimized 方式,这种方式可以对仿真内核进行优化。根据工程改造要求需要得到部分既定测试项目的仿真结果,同时要保证收集到的结果尽可能接近在线网络当中的实际值,这样我们所做的仿真试验需要进行多次,每次改变 seed 的值(Seed 是仿真内核使用的伪随机种子,以模拟真实世界中每次实际运行存在的客观差异)。当对多次改变 seed 值进行仿真测试所得到的值进行分析后,发现结果同一或十分接近,则认为收集到的结果真实可信。

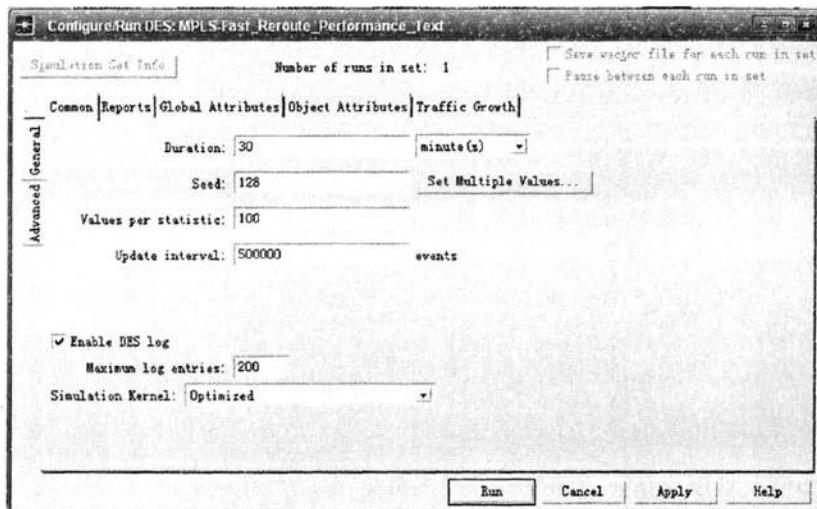


图 5-4 配置运行 DES

### 5.3 仿真结果分析

衡量故障恢复机制的性能指标通常为丢包率,业务流切换时间和网络带宽资源利用率。针对故障发生点不同的情况,分别对 Makam 方案、Haskin 方案和 RSVP 方案以及本文新提出的 OFRR 方案这四种不同的快速重路由方案在故障恢复期间的丢包率、业务流切换时间、网络带宽资源利用率等性能参数进行分析与比较。

本文仿真分析了在不同节点发生故障条件下各个方案的丢包率情况。仿真结果统计数据如下图 5-5 所示。

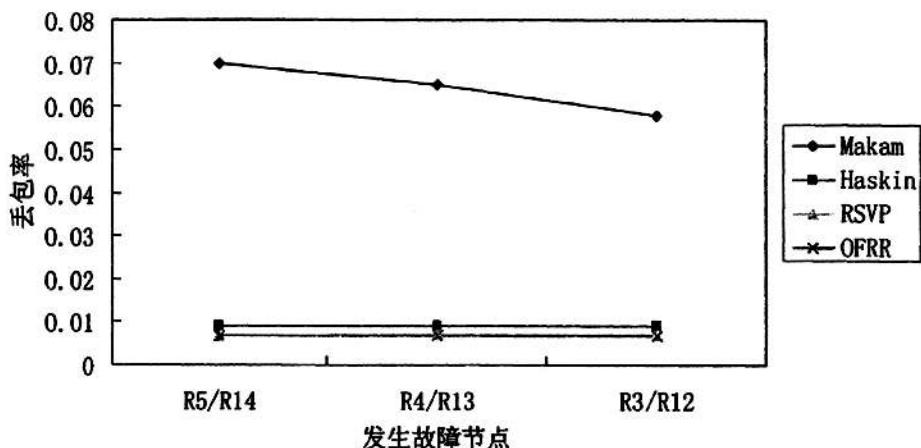


图 5-5 不同节点发生故障条件下各个方案的丢包率

图 5-5 显示不同故障恢复方案的丢包率随着故障发生地点变动呈现不同的数值。丢包率从大到小依次为：Makam 方案、Haskin 方案、RSVP 方案、OFRR 方案。其中 OFRR 方案与 RSVP 方案在丢包率上拥有几乎良好的良好性能。Haskin 机制和 RSVP 机制中，流量被检测到故障的 LSR 切换到一条提前设置好的备份路径上，所以这两种机制中丢失的数据包都是在故障检测时间之间丢失的。对于 Makam 机制，故障发生地点离入口 LSR 越远，丢失的数据包的数量越大，这是因为入口节点在收到 FIS 信号之后才开始将流量切换到备份路径。在 Makam 机制中，只有当故障恰巧在入口处发生时，丢包数量才与 Haskin 和 RSVP 方案一样，因为这时切换到备份路径前不需要发送 FIS 信号。

如图 5-6 所示，不同方案在不同故障发生点情况下各自的业务流切换时间，从大到小依次为：Makam 方案、Haskin 方案、RSVP 方案、OFRR 方案。对 RSVP 方案以及 OFRR 方案，在业务流切换时间上具有良好的良好性能，同时这两个方案在业务流切换时间上基本是个常量，因为检测到故障的节点也就是负责切换流量的节点，而且因为备份路径是在故障发生前设置的，所以不需要时间去设置备份路径。不同的节点发生故障，恢复的时间都是一样的。任何一个节点出现故障，Haskin 和 Makam 机制的故障服务中断时间都很长，而且故障发生地点离入口节点越远，时间越长，因为不管是回传的数据包还是 FIS 信号，都需要向上游回传至入口，才将流量切换到全局恢复路径上。

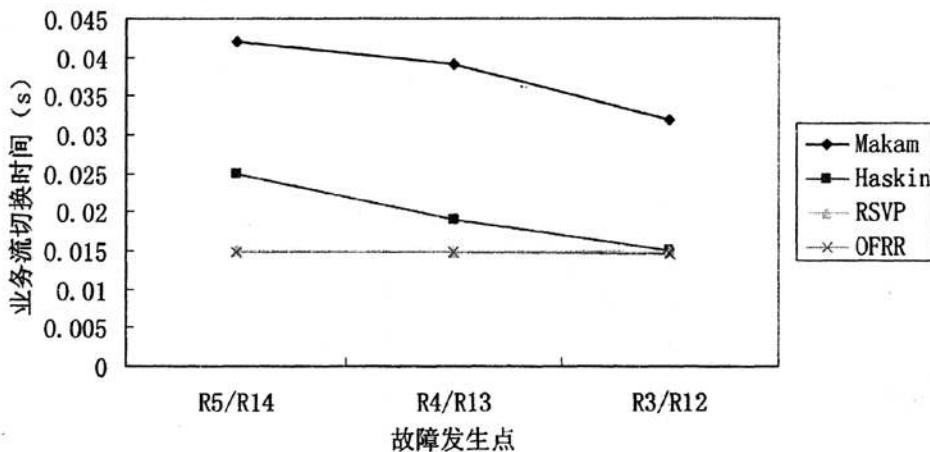


图 5-6 不同方案在不同故障发生点情况下各自的业务流切换时间

MPLS 快速重路由方案基本思想是在故障发生前预先建立备份路径保证网络失效后业务流快速及时的切换。备份路径是在预先建立好的，虽然在网络发生故障后才将流量切换到备份路径上进行转发，但是仍然需要在备份路径上预留足够的带宽资源用以保证网络发生故障后快速进行恢复，这样备份路径的闲置造成了极大的带宽资源浪费。网络的带宽资源是非常宝贵的，因此如何更好地合理地利用带宽资源对网络恢复方案而言至关重要。本文分别对 Haskin 方案、Makam 方案、RSVP 方案及 OFRR 方案在网络资源利用率上进行性能比较。仿真结果统计数据如图 5-7 所示。

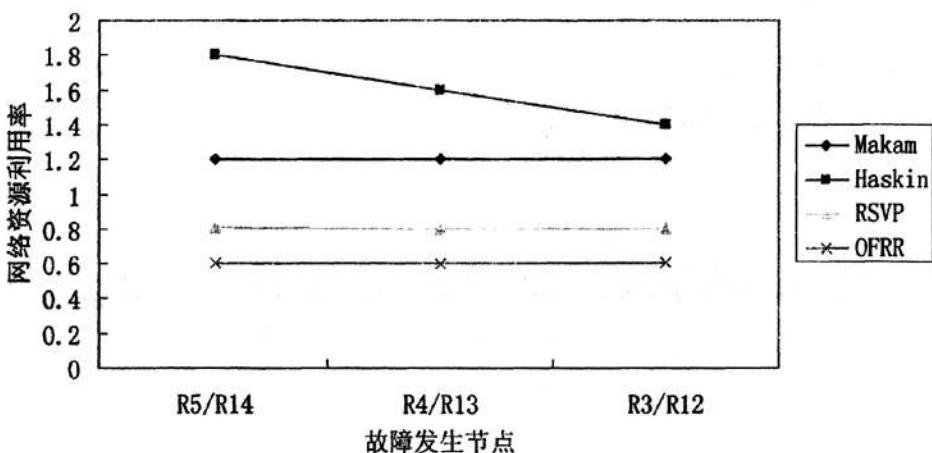


图 5-7 不同方案在不同节点发生故障条件下的网络资源利用率

如图 5-7 所示为四种方案在不同节点发生故障后的网络资源利用率。各种恢

复方案对备份资源的消耗按以下顺序递增：OFRR、RSVP、Makam、Haskin。Makam 模型是一种全局恢复方式，它的恢复方式是从主路径上直接切换至备份路径上，因此无论哪个节点发生故障，所应用的备份路径都是同一条，因此网络资源利用率几乎是不变的。Haskin 模型是一种局部恢复方式，根据故障发生点的不同，所应用到的备份路径也不同，因此网络资源利用率也相应不同，并且随着故障发生节点离源节点越远，网络资源利用率越大。RSVP 方案是由检测到故障发生节点直接将流量从保护路径切换至备份路径，并且备份路径是在故障发生前预先设定好的，因此无论是那个节点发生故障，该方案所占用的备份路径以及在备份路径上所预留的备份资源是不变的。本文提出的方案也是预先建立备份路径，并在故障发生后，由检测到故障发生的节点直接将流量从保护路径切换至备份路径。但是由于 RSVP 方案仅支持同一条保护路径的备份路径在共同链路上共享备份带宽资源，而 OFRR 方案支持同一保护路径及不同保护路径的备份资源共享，因此在网络资源利用率性能上要优于 RSVP 方案，同时也是这四种方案中，网络资源利用率性能最好的一个。

通过对 OFRR 方案和现有方案的仿真分析和比较，证明了 OFRR 方案在故障恢复期间具有更好的恢复性能，具有比 Haskin 方案、Makam 方案更低的丢包率及更低的服务中断时间，同时在网络资源利用率上比 RSVP 方案具有更优的性能，有效减少了备份资源的消耗，提高网络资源利用率。

## 5.4 本章小结

本章利用 OPNET 仿真软件搭建了网络仿真平台，建立仿真网络模型，设置仿真参数，配置运行仿真，用对比方法，从丢包率、业务流切换时间、网络资源利用率三方面对 OFRR 方案以及现有方案进行了仿真。根据仿真结果分析研究了这几种方案在丢包率、业务流切换时间和网络资源利用率三方面性能优劣，总结出的结论证明 OFRR 方案在故障恢复期间具有良好的性能，相比 Makam 方案、Haskin 方案具有更低的丢包率及更低的业务流切换时间，同时在网络资源利用率上相比 RSVP 方案具有更优的性能，有效减少了备份资源的消耗，提高网络资源利用率。

## 第六章 总结与展望

### 6.1 总结

MPLS 故障恢复机制目标是满足业务流恢复需求的同时保证网络的服务质量，其快速重路由 FRR 技术通过故障前预先建立好备份路径，在网络失效时快速将业务流切换到备份路径上继续转发，保证更低延时，更少分组丢失。因此 FRR 技术是网络可靠性研究的一项重要指标。本文主要分析研究了经典 FRR 方案，总结了各方案的特点与局限性。在此基础上，具体针对共同存在的备份路径闲置所造成的带宽资源大量浪费问题，提出一种 FRR 优化方案，该方案具有良好的故障恢复性能，同时有效降低备份带宽资源浪费，提高网络资源利用率。

本论文主要完成的研究工作分别为以下几方面：

(1) 研究了 MPLS 及其流量工程技术。论文研究了 MPLS 技术，简要介绍了 MPLS 基本原理、技术特点以及关键技术应用，同时对 MPLS 流量工程技术进行相关研究，简要介绍了 MPLS 流量工程的概念、技术特点以及技术优势。

(2) 研究了 MPLS 故障恢复机制及其快速重路由技术。本文对 MPLS 故障恢复机制做了较为详细的介绍，内容包括 MPLS 故障恢复机制的相关概念、技术术语，并针对目前国内外研究现状对 MPLS 故障恢复机制进行了分类。MPLS 快速重路由作为 MPLS 故障恢复机制的核心技术，论文集中对其进行了研究，分析了 FRR 技术相比重路由所具有的优势。研究比较了几种 FRR 保护模式，FRR 技术分为路径保护以及局部保护两种保护模式，局部保护又可以分为链路保护和节点保护。路径保护是采用集中化管理系统来实施故障恢复，局部保护是由检测到故障的上游节点直接发起恢复，恢复的过程是局部的。目前有很多著名 FRR 方案被提出，如 Makam 方案、Haskin 方案、RSVP 方案等，论文对各个方案分别进行研究，分析比较了各方案的优点以及缺点。Haskin 方案优点是丢包少，缺点是恢复路径较长导致时延较高同时极易造成分组失序。Makam 方案优点是分组失序少，缺点在于故障信息的传播会导致时延较高同时造成较大数目的丢包。RSVP 方案优势是丢包率小同时故障恢复快，缺点是备份路径闲置造成大量带宽资源浪费。分析结果说明各方案均具有一个共同的缺陷，即备份资源利用率低，造成了极大的网络带宽资

源耗费。

(3) 提出一种快速重路由优化方案。论文在对经典快速重路由方案研究的基础上, 针对所存在的备份带宽资源浪费的问题, 提出一种快速重路由优化方案, 即 OFRR 方案, 该方案包含两个方面内容: 1. 优化的备份资源信息共享机制, 通过使备份路径中的关键节点掌握有限范围内的节点与链路的相关信息, 实现对备份资源的有效共享管理, 可以支持备份带宽资源在网络中全局性共享; 2. 优化的备份路径选择算法, 该算法基于经典最短路径算法 Dijkstra 算法, 通过在链路权重中添加带宽资源的限制, 优先选择预留带宽资源大的链路, 可进一步降低对网络预留资源的需求。

(4) 基于 OPNET 软件搭建出网络仿真平台, 建立仿真网络模型, 设置仿真参数, 配置运行仿真, 应用对比方法, 对原有方案以及 OFRR 方案进行了仿真, 仿真结果表明 OFRR 方案在故障恢复期间具有更好的恢复性能, OFRR 方案相比 Haskin 方案、Makam 方案具有更低的丢包率及更低的服务中断时间, 同时在网络资源利用率上比 RSVP 方案具有更优的性能, 有效减少了备份资源的消耗, 提高网络资源利用率。

## 6.2 展望

MPLS 目前已成为 IP 骨干网的核心技术, 作为 ATM 与 IP 结合的产物, 继承了 IP 技术的灵活性, 可扩展性, 同时利用现有的二层硬件交换技术提供了对流量管理和 VPN 的支持, 具有 QoS 保证。为运营商提供了一个方便管理且具有增值效应的交换平台。MPLS 是流量工程目前最佳的解决方案, 可以使网络流量均衡地分布在网络中, 提高网络性能。MPLS 流量工程提供的故障恢复机制能在故障发生后为 IP 网络提供流传输的连续性和 QoS 保证, 快速重路由是其一项重要技术手段同时也是目前的研究热点, 具有相当广阔的应用前景。本文的研究尚处在理论和性能模拟阶段, 在实用化过程中还有许多问题与实现技术需要研究和解决。因此, 如何将 MPLS 快速重路由技术与实际的网络应用很好地结合仍然有待进一步的研究与解决。

相信未来随着 MPLS 技术应用的不断发展与成熟, MPLS 故障恢复机制及其快速重路由技术将在实际的网络应用中发挥越来越重要的作用。

## 参考文献

- [1] 吴江, 赵慧玲. 下一代的 IP 骨干网络技术—多协议标记交换, 北京:人民邮电出版社, 2001.1
- [2] 李文正. 下一代计算机网络技术, 北京: 中国水利水电出版社, 2008
- [3] 史忠值. 高级计算机网络, 电子工业出版社, 2002.1
- [4] 邓永平, 徐建峰. IGP 路由收敛分析及优化[J], 电信科学, 2005.21(4): 13-15
- [5] 陈跃斌, 白凤山, 陈克林. 基于 ATM 的 IP 交换技术, 云南民族学院学报(自然科学版), 2000.9(4): 203-205
- [6] Eric Osborne, Ajay Simha 著, 张辉, 卢炜译. 基于 MPLS 的流量工程, 北京:人民邮电出版社, 2003.7
- [7] G.Swallow. MPLS advantages for traffic engineering[J], IEEE Communications Magazine, 1999.12, 37(12): 54-57
- [8] Xipeng Xiao, A.Hannan, B.Bailey, L.M.Ni. Traffic engineering with MPLS in the Internet[J], IEEE Network, 2000.3/4, 14(2): 28-33
- [9] D AWduche, J Agogbua, M O'Dell, J McManus. Requirements for Traffic Engineering Over MPLS, IETF RFC2702, 1999.9
- [10] J Wroclawski. The Use of RSVP with IETF Integrated Services, IETF RFC2210, 1997.9
- [11] S Blake, D Black, M Carlson, E Davies. An architecture for Differentiated Services, IETF RFC2475, 1998.12
- [12] Li T, Y Rekhter. Provider Architecture for Differentiated Services and Traffic Engineering(PASTE), IETFRFC2430, 1998.10
- [13] 吴荣生, 郭联志. MPLS VPN 的探究与应用[J], 重庆科技学院学报(自然科学版), 2009.11(2): 130-133
- [14] 程兰芳, 刘玉宾, 互联网宽带接入市场的博弈行为分析[J], 中国物价, 2009(11): 67-70
- [15] 林闯, 单志广. 计算机网络的服务质量, 北京: 清华大学出版社, 2004
- [16] 陈雪非, 李蓬, 黄河. MPLS 故障恢复机制及其仿真研究[J], 计算机工程与设计, 29(16), 2008.8: 4188-4193
- [17] 卢联强, 黄河, 李伟琴. 支持自愈恢复的 MPLS 路由算法[J], 计算机工程与应用,

2003.19(5): 53-57

- [18] V.Ed.Sharma, F.Ed.Hellstrand. Framework for Multi-Protocol Label Switching(MPLS)-based Recovery, IETF RFC3469, 2003.2
- [19] S.Makam, V.Sharma, K.Owens, C.Huang. Protection/Restoration of MPLS Networks, Internet-Draft(draft-makam-mpls-protection-OO.txt), 1999.10
- [20] Sangsik Yoon, Hyunseok Lee, Deokjai Choi, Youngcheol Kim, Gueesang Lee, Mike Lee. An efficient recovery mechanism for MPLS-based protection LSP[J], 4th IEEE International Conference on ATM and High Speed Intelligent Internet Symposium, 2001: 75-79
- [21] T.H.Oh, T.M.Chen, J.L.Kennington. Fault restoration and spare capacity allocation with QoS constraints for MPLS networks[J], IEEE Global Telecommunications Conference, 2000.12(3): 1731-1735
- [22] David G, Kyoung S L. A 1+1 protection architecture for optical burst switched Networks[J], IEEE Journal on Selected Areas in Communications, 2003
- [23] Makam S, Sharma V, Owens K. Restoration of MPLS Networks. Internet Draft, draft-makam-mpls-protection-01, 1999
- [24] 杨天乐, 杨爱英. MPLS 网络的一种 M:N 方式保护与恢复方案[J], 2006 年国防光学及光电子学学术研讨会暨中国兵工学会光学专业委员会成立 25 周年年会论文集, 北京, 2006: 321-325
- [25] Slosiar R, Latin D. A Polynomial-Time Algorithm for the Establishment of Primary and Alternate Paths in ATM Networks[J], IEEE Journal on Selected Areas in Communications, 2003, 26(21):1011-1020
- [26] D.Gan. A method for MPLS LSP fast-reroute using RSVP detours, Internet Draft(draft-gan-fast-reroute-OO.txt), 2001.4
- [27] Atsushi Norihiro. MPLS Signaling Extensions for Shared Fast Rerouting, draft-iwata-mpls-shared-fastreroute-00.txt, 2002
- [28] 李晓东. MPLS 技术与实现, 北京: 电子工业出版社, 2002.12
- [29] Changcheng Huang, V Sharma, Srinivas Makam. A Path Protection/Restoration Mechanism for MPLS networks, IETF Draft<draft-chang-mpls-Protection-03.txt>, 2000.7
- [30] D Haskin, R Krishnan. A method for setting an alternative label switched paths to Handle fast

reroute, IETF Draft<draft-haskinmpls-fast-reroute-05.txt>, 2001.7

[31] L.Hundessa, J.Pascual. Fast Rerouting mechanism for a protected label switched path. Proceedings of the IEEE International Conference on Computer Communications, 2001.10

[32] R. Braden, L. Zhang, S. Berson. Resource ReSerVation Protocol (RSVP), IETF RFC 2205, 1997.9

[33] 何晓明, 唐宏, 叶梧. MPLS 流量工程中的最小化抢占路径选择方法[J], 北京邮电大学学报, 32(1), 2009.2: 19-23

[34] P. Pan, G. Swallow, A. Atlas. Fast Reroute Extensions to RSVP-TE for LSP Tunnels, IETF RFC4090, 2005.05

[35] 谢系仁. 计算机网络, 北京: 电子工业出版社, 2004.10

[36] 刘光磊, 裴正定. 基于 MPLS 的网络流量工程[J], 现代电信科技, 2001.4(4): 20-23

[37] Pan Ping Ed, Der-Hwa Gan. Fast Reroute Techniques in RSVP-TE. draft-pan-rsvp-fastreroute-00.txt, 2001

[38] Ping P, Der-Hwa G, Markus J. Fast Reroute Extensions to RSVP-TE for LSP Internet draft, draft-ietf-mpls-rsvp-lsp-fastreroute-02, 2003

[39] 陈敏. OPNET 网络仿真, 北京: 清华大学出版社, 2004.04

[40] 王文博, 张金文. OPNETModeler 与网络仿真, 北京: 人民邮电出版社, 2003.10

## 攻读硕士学位期间发表论文

- [1] 周莲英,周琳.基于 One-to-One 的有效备份资源共享管理机制[J].光通信研究. 2010. 04:28-30.

## 致 谢

首先，我要感谢我的导师周莲英教授在整个学习过程中的指导与建议、生活上的关心与帮助！本课题的顺利进行，离不开周老师的悉心指导，周老师对学术前沿的广阔视野和独到见解让我受益匪浅，这些必将对我今后的学术和学习产生重要的影响。

其次，感谢实验室已毕业的各位师兄师姐，从他们那里我学到很多宝贵的知识；感谢同窗霍婷婷、张晓、冀伟伟和孙隆基，以及陈凯等师弟，在与他们的交流与讨论中使我得到很多启发；感谢计算机与通信工程学院提供的学习平台，以及关心和帮助过我的各位老师、同学和朋友！

最后，要特别感谢我的家人，是他们在我最困难的时候一直用无私的爱关心、支持和鼓励我，给予我前进的力量与信心。

谢谢大家！