

# MEN 中以太网业务的保护机制与运用

汪成义

(湖北经济学院 计算机科学与技术学院, 湖北 武汉 430205)

**摘要:**文章从对传统数据网络的保护机制和传送网的线路保护机制的分析入手,系统地描述了城域以太网(MEN)中以太网业务的保护机制,特别是对其保护参考模型和 4 类基本的保护机制进行了较详细的描述,并通过 MEN 保护机制的典型运用方案,结合分层网络的层间互操作关系,对层间的保护关系进行了综合分析。  
**关键词:**城域以太网;保护机制;保护参考模型;分层保护  
**中图分类号:**TN915      **文献标志码:**A      **文章编号:**1005-8788(2006)05-0025-04

## Protection mechanism for and applications of Ethernet services in metro Ethernet networks

Wang Chengyi

(School of Computer Science & Technology, Hubei University of Economics, Wuhan 430205, China)

**Abstract:**On the basis of the analysis of the protection mechanisms for conventional data networks and the line protection mechanism for transport networks, this thesis systematically describes the protection mechanism for Ethernet network services in the Metro Ethernet Network (MEN), especially its protection reference model and four basic protection mechanisms. Through the typical application scenarios of the protection mechanism for MEN and in connection with the interoperations between the layers of the layered network, it makes a comprehensive analysis of the protections between the layers.  
**Key words:**MEN;protection mechanism;protection reference model;layered protection

随着以太网技术在城域范围的不断渗透与延伸,相关业务的业务流量正在快速增长,业务类别也由单纯的传统数据业务向具有实时特征的业务(如 IPTV 业务等)扩展,由此带来对以太网业务保护的新需求,即有别于传统以太网业务保护的、能适应城域以太网(MEN)网络特点的业务保护需求。这里所说的以太网业务的保护与通常所说的网络保护的原理相同,都是要求网络能够发现替代传输路由,使信号通过保护通路仍保持有效。但由于 MEN 所涉及的技术层出不穷,可用的保护措施也门类繁多,如以太网业务的一个 EVC(Ethernet Virtual Connection,以太网虚连接)可以穿越基于多协议标签交换(MPLS)、同步数字体系(SDH)、波分复用(WDM)等技术的传送网,其端到端的保护可能包含有不同的机制。本文旨在理清以太网业务保护的基本机制,并以一个典型的 MEN 网络分层结构作为运用示例,对其保护机制进行针对性的具体分析。

### 1 传统数据网络的保护机制

在局域网中广泛使用的以太网技术,其基本结构是树形结构,为了提高网络系统的可靠性,可通过增加冗余链路来提供保护,具体可采用双树形结构或环形结构。由此会带来广播风暴、多重拷贝、媒体

访问控制(MAC)地址表不稳定等一系列问题,其原因是网络中出现了回路,针对性的解决办法是采用生成树协议(STP,IEEE 802.1d),其基本原理如图 1 所示,主要思想是依照规则选取一个网桥或交换机为根网桥,在每个与根网桥连接的非根网桥上指定一个开销最小的端口为根端口,并使其处于转发状态,而其它端口为非标志端口,处于阻塞状态,从而避免出现回路。图中的网桥协议数据单元(BPDU)以组播的方式发送,由此获得建立最佳树形拓扑结构所需的信息。如当一条链路发生故障时,该协议可激活备用路径,即通过调整端口的状态,实现其保护与恢复能力。由于其收敛时间高达 30 s 以上,不能满足时间敏感业务的需求,随后又出现了快速生成树协议(RSTP,IEEE 802.1w),其收敛时间最短降至 1 s。它们的共同特点是网络结构灵活,收敛时间相对较长。

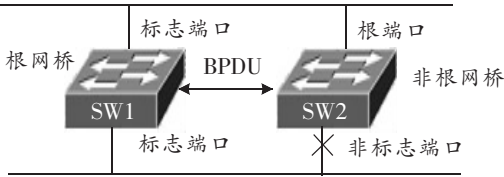


图 1 生成树工作原理示意图

此外,对三层网络设备来说,还可利用其对动态

路由协议的支持,通过迂回路径提供保护。对支持 MPLS 的设备来说,可利用其对标签交换协议的支持,通过迂回路径来提供保护。

2 传送网的保护机制

以 SDH 为代表的传送网具有较为成熟的保护机制,主要包括其自愈能力和自动保护倒换(APS)特性。其基本的线路保护倒换结构类型有:

(1) 1+1 结构:信号总是在工作通路和保护通路中同时发送(简称并发),在接收端则根据监视结果选择连接更为合适的一路信号(简称选收)。

(2)  $m:n$  结构:该保护类型通过  $m$  个保护通路给  $n$  个工作通路提供保护。保护通路并不专注于给工作通路提供保护,这意味着在保护通路没有替代有故障的工作通路来发送业务时,可以用于发送其他的业务。常见的结构有:1:1 结构,即给一个工作通路提供一个保护通路;1: $n$  结构,即由 1 个保护通路对  $n$  个工作通路提供保护。

对于环形网络结构的 SDH,主要采用二纤单向通道保护环和双向复用段共享保护环两类具有自愈能力的环形结构。

3 MEN 中以太网业务的保护机制

3.1 保护参考模型

针对 MEN 中以太网业务保护的复杂性,城域以太网论坛(MEF)提出了一个保护参考模型,以便能够按统一的保护结构进行描述。该保护参考模型(PRM)允许对业务的保护能力进行一致的描述,这些业务可能采用不同的传送技术、网络拓扑结构和策略。该模型是按分层结构来描述的,主要包括以太网业务(ETH)层和传送(TRANS)层,每层均能提供独立的保护,如 Ethernet over MPLS over SO-

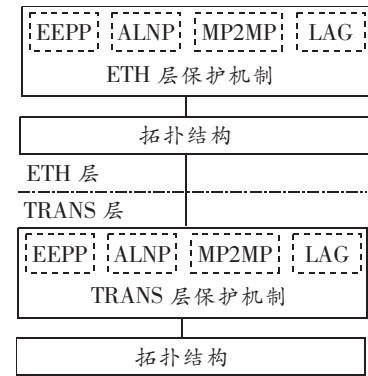


图 2 保护参考模型

SDH(EoS)中携带的以太网业务流,其保护是在

SDH 层完成。另一类是保护由传送层的以上层完成,该类型又可细分为两个子类型:(1) 传送层不具有保护能力,或者其保护能力被上层的保护机制忽略,如以太网传送,其保护可由在传送层之上的 ETH 层或 MPLS 层完成;(2) 传送层和上层的保护机制关联工作以满足所要求的保护业务等级规范(SLS),如具有保护机制的 ETH 层承载于具有 1+1 结构的 SDH 传送网,SDH 的 1+1 结构能修复链路上的本地故障,而 ETH 层保护用于 SDH 保护不能适用的地方或作为一个端到端的附加保护方式。此外,图 2 中的拓扑结构可以各不相同,但不能对所支持的端到端保护的 SLS 有阻碍。

3.2 以太网业务的保护机制

图 2 中并列画出了 4 种可能类型的网络保护机制:集合线路与节点保护(ALNP)、端到端通道保护(EEPP)、多点到多点(MP2MP)保护和基于链路聚合(LAG)的链路保护。它们可以在上、下层中构成任意的组合。

3.2.1 集合线路与节点保护

通过本地通道绕道机制,ALNP 可提供对链路和节点故障的保护,如图 3 所示,其中只画出了一个方向,实际为双向。其原理是,本地备用的绕道通道沿着主通道建立,并可旁路掉紧邻的下游网元(NE)

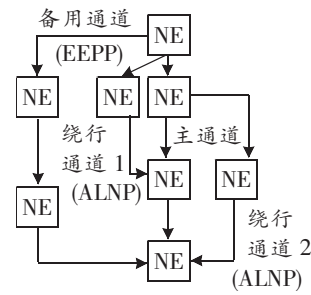


图 3 ALNP 与 EEPP 示意图(单向)

或逻辑链路,紧接着合并回主通道。绕道通道可以对网络中的主通道提供 1: $n$  保护或 1:1 保护。备用通道可以是显式预留的,也可以是隐含于技术之中的,前者如 RFC 3469 中所描述的基于 MPLS 的恢复机制,后者如 SDH 的双向线路共享保护倒换(BLSR),它们均可看作是 ALNP 的特例。

ALNP 可以提供低于 50 ms 的恢复时间和 1: $n$  的保护能力,根据所指定的保护 SLS 和故障检测能力,也可支持和请求其他长度的恢复时间。ALNP 和 ALNP 所在层的下一传送层中的其他保护机制可以提供类似的保护能力,其解决办法是通过配置 ALNP 机制的延迟时间来实现互操作,以便在上层的 ALNP 机制决定是否进行协同工作前,下层保护机制能够收敛。如果在 ALNP 所在层的下层中的传送子网不支持指定 SLS 的本地保护,那么

ALNP 机制可负责根据所请求的 SLS 进行保护。

3.2.2 端到端通道保护

EEPP 给主通道提供一个冗余的端到端通道，即通过不同的路由段建立替代通道，用以保护主通道。所需冗余通道的数目由保护策略确定并有所限制(因为每个冗余通道要消耗网络资源，如带宽、CPU 时间和内存)。冗余通道的计算可以由在线约束机制(如 CSPF)或离线流量工程工具来完成。每一条这类冗余通道实际上是端到端的，因此，EEPP 是以不同于 ALNP 的方式来提供冗余。

EEPP 可以采用的保护类型如下：

(1) 1+1 结构：这种类型的保护要求建立并始终使用冗余通道，即所有发送到主通道上的数据也复制到冗余通道上。

(2) 1：1 冷备用(Cold Standby)结构：这种类型的结构要求冗余通道提前进行路由信息的计算，冗余通道直到主通道出现故障时才建立；源节点只在主通道出现故障时才建立冗余通道，由此导致恢复时间较长。

(3) 1：1 热备用(Hot Standby)结构：这种类型的结构要求冗余通道提前进行路由信息的计算，并在主通道的业务有效时间内建立，而在等待主通道出现故障时，冗余通道一直保持有效，因其修复故障的主要时间是检测时间，故可以非常快地切换到冗余通道。针对热备用结构的冗余通道仍会消耗网络资源的情况，可以利用其占用少量资源，而对部分业务流提供快速恢复能力，随后可请求冷备用来恢复全部业务流。

(4) 共享冗余结构：即利用网络中一个故障可能只影响主通道的一个子集，在多个主通道中可共享同一保护资源。如 1：n、环和共享网路保护机制。

3.2.3 多点到多点保护

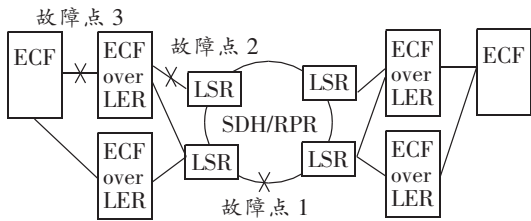
E-LAN(以太网 LAN)业务是一种多点到多点的以太网业务，要求在所有的用户网络接口(UNI)间具有连通性，因而上述保护方案就不足以对其进行保护。如 E-LAN 的实现可能与多个 ECF(Ethernet Connection Function，以太网连接功能)有关，它们通过多个 ETH 路径互连，这样的 ECF 故障就没有被以上描述的 EEPP 和 ALNP 所覆盖。典型地，有 3 种方法可用于以太网业务层或传送层的多点到多点保护：水平分割桥接、生成树或快速生成树和链路冗余。其中，基于生成树的保护与前述内容相同，其他两种方法在文献[1]中有详细描述。

3.2.4 基于链路聚合的链路保护

所谓链路聚合，是指允许连接同样的两个节点的多个以太网链路聚合成一个 LAG，一个 LAG 在逻辑上可作为一个链路。其故障保护过程是，当链路之一出现故障时，LAG 的两端节点改变它们的 LAG 分配功能，以便在剩余链路中分摊流量；而当一个链路恢复正常时，LAG 分配功能再一次改变，以便能将其加入。

4 运用与分析

MEN 中保护机制的运用要充分利用传送网网络分层的特点，即不同的层是相互独立的，可以有不同的保护机制。作为运用 MEN 的保护机制的例子，假定网络的 ETH 层是经由 MPLS 来传送，且 MPLS 通道横穿了 SDH 或弹性分组环(RPR)，这样就形成了一个 ETH/MPLS/RPR 或 ETH/MPLS/SDH 结构的分层网络，如图 4 所示。作为下层网络，SDH 和 RPR 能够对出现于网络的环形部分的任何故障(如故障点 1)进行快速保护，但是，如果故障是在环外的 MPLS 通道(如故障点 2)，它们将不能提供任何保护。MPLS 保护可以比 SDH 和 RPR 更慢(如基于 OA&M 的 EEPP)或者具有相同的性能(如 ALNP)，但是它将能保护整个的 MPLS 通道。同样地，利用运行于 ETH 层(如故障点 3)的保护机制，ETH 层将能够保护端到端的 ETH 业务的连接。



注：LSR：标签交换路由器；LER：标签边缘路由器

图 4 基于 ETH/MPLS/SDH 和 ETH/MPLS/RPR 的分层网络故障保护

层保护的一个重要特征是层越低，保护切换越快；而层越高，可以保护的通道越长。图 4 中的 SDH 或 RPR 的层最低，其保护倒换时间均可达到不超过 50 ms，而 ETH 层为 3 层中的最上层，通过 ECF 之间可实现端到端的长通道保护。为了建立一个合理有效的保护策略，可将上层保护机制设计为与下层保护机制协同工作的方式，即在上层采取任何保护动作前，允许其下层先修复故障，具体可以通过使用不同的恢复时间来实现，如 SDH 的恢复

时间设为低于 50 ms, MPLS 的恢复时间则应设得更长些, 如低于 200 ms, 它们均可看作是 ALNP 的特例, 通过配置 ALNP 机制的延迟计时器的时间来实现互操作。而 ETH 层可以采用 EEPP 机制实现端到端的保护, 其恢复时间可设置得更长, 如低于 2 s。

目前类似图 4 的结构在 MEN 网络环境中应用较多, 最典型的是基于多业务传送平台 (MSTP) 构建的 MEN, 其低层是 SDH, 依次可以包括 RPR、MPLS 和以太网二层交换等层, 其他类型的 MEN 的网络结构多为该结构的一个子集或与之相似, 故可参照此例, 进行保护关系的分析。

## 5 结束语

基于 MEN 的业务保护机制是在既有的以太网保护恢复技术和传输网保护恢复技术的基础上, 结

合 MEN 的分层网络特点发展而来。由于 MEN 的组网技术多种多样, 有的技术已很成熟, 有的技术较新, 有的恢复时间能满足传统电信运营的时间要求, 有的只能满足传统数据网络的时间要求。本文主要是对其保护机制作一个系统的介绍, 并通过一个典型的分层网络结构的运用进行具体的分析。

### 参考文献:

- [1] MEF Technical Specification MEF 2-2004, Requirements and framework for ethernet service protection in metro ethernet networks [S].
- [2] IEEE 802.1d-2004, Media Access Control (MAC) bridges [S].
- [3] IEEE 802.1w-2001, Part 3: Media Access Control (MAC) bridges-amendment 2: rapid reconfiguration [S].

## \* 简 讯 \*

# 烽火通信中标中国电信西北环 40×10G DWDM 国家一级干线

中国电信集团公司为了进一步完善其骨干传输网络的网络布局和覆盖范围, 于近日正式启动了 2006 年骨干传输网新建项目。烽火通信凭借差异性的解决方案、领先的技术优势, 以及灵活的商务策略等多方面的综合优势, 获得了覆盖甘肃、青海、新疆等重要省市地区、全长超过 5000 km 的西北环 40×10G DWDM 国家一级干线的建设权。

依据中国电信的业务需求以及今后的发展趋势, 结合多年建设国家一级通信干线的丰富经验, 烽火通信为这次的骨干传输网建设制定了个性化的解决方案。全网采用 FONST W1600 系列 40×10G DWDM 系统; 为了保证系统达到最优异的性能, 在工程中应用了 V-EDFA、超强 FEC、RAMAN 放大器等多项 ULH (超长距离) DWDM 技术; 采用波长严格控制光转发 OTU, 结合 AWG 模块和 Interleave 技术, 完成了 50GHz 波长间隔 40 波的系统容量设计; 提供 V-EDFA 及增益平坦和增益锁定的光放大器, 将多种 VOA 技术应用到 EDFA 当中, 可动态适应线路损耗因温度等因素所发生的变化, 极大地提升了系统的稳定性、可靠性, 为工程的运行维护提供了强大的保障。

烽火通信始终致力于国家通信基础网络的建设和优化完善, 并曾多次将最先进的技术产品和综合解决方案服务于中国电信的骨干传输网络。在中国电信 2005 年干线传输网新建项目中, 烽火通信以绝对优势取得了以北京为中心, 辐射东北、西北大部分重要省市、全长超过 8000 公里的东北环国家一级干线的建设权。随着这几条 80×10G DWDM 干线的顺利实施, 烽火通信的综合实力得到了中国电信的全面认可。本次西北环 40×10G DWDM 国家一级干线项目的实施, 是双方长期友好合作关系的进一步加深。工程完工后, 中国电信东北、西北地区的网络布局将得到进一步的优化, 并将发挥出巨大的经济效益。

据悉, 在 2006 年初, 烽火通信具备国际先进商用水平的 80×40G DWDM 系统率先装备中国电信“上海—杭州”传输干线, 这条国内第一条 80×40G DWDM 干线的建设不但使中国电信在网络应用方面又迈上了一个新的台阶, 也较大地推动了我国超大容量传输技术的发展和实用化进程。烽火通信将针对通信行业的转型和网络融合的发展趋势, 与中国电信等运营商积极探索固定网络的转型和业务增值, 挖掘网络潜力提供可盈利的整体解决方案, 与我国的运营企业共同描绘美好未来。