

## 网络管理系统及其软件设计开发

### 摘 要

2M 数字专线网安全可靠, 业务内容由用户决定, 传输速率有保障, 并且目前专线价格大幅度下调, 市场需求大幅度增长。但缺乏端到端的统一管理和测试手段, 故障排除困难。基于 2M 数字专线网现状, 北京宽广电信公司提出了以 SDXC4/4/1 设备为核心, 以 SDH 传输网络作为基础平台, 以光纤和铜线作为接入手段, 通过统一的网络管理平台和业务平台, 为运营商提供易于管理、维护和运营的 2M 专线的端到端的解决方案。

本文旨在阐述该 2M 专线的网管软件的客户端设计开发。此网管软件目标是实现对整个系统的管理。目前此项目只实现了对核心层设备 (Tetra-X) 和汇接层设备 (SEApoinT) 的管理, 在逻辑上和业务上都没有进行整合。由于对这两个设备的管理基本相似, 因此本文只着重谈论了 Tetra-X 设备管理系统客户端的设计与实现。

本文从网络管理理论入手, 讲述网络管理的概念和 5 大功能, 分析当前的网络管理模式和体系结构, 通过比较它们的优缺点, 确定不同模式和体系结构的适用对象。在项目中我们采用的是集中网络管理模式和基于 Internet/SNMP 的网络管理体系结构, 在此基础上介绍了简单网络管理协议 SNMP, 分析了该协议的原理和优缺点。本项目是以 SDH 传输网络作为基础平台, 实现的是对传输网设备的管理, 因此在第三章主要介绍了有关传输网的知识, 分析了传输网的典型网管分级及传输网设备管理的系统功能。从第四章开始本文围绕项目展开, 介绍了 Tetra-X 设备管理系统的网络环境和 Tetra-X 设备。第五章主要着重介绍该网络管理系统的客户端软件的设计和实现, 其中包括客户端的功能设计和程序实现。本文在最后还分析了在软件设计实现过程中遇到的问题及解决方法。

**关键词:** 网络管理、简单网络管理协议、2M 数字专线网、客户端

## NETWORK MANAGEMENT SYSTEM AND ITS SOFTWARE DESIGN

### ABSTRACT

2M digital private line has the qualities of safety, reliability, content decided by users, reliable rate. Recently its price has fallen down much. Its market requirement is increasing much. But there is short of uniform manners of managing and testing. Beijing Broad Telecommunication Company brings forward the end-to-end resolution of SDH 2M digital private line on the base of status quo.

The purpose of this document is to expatiate on client software programming of the network management system on the 2M private line. The aim of this system is to manage the whole system. But until now, it only can manage the DXCS device (Tetra-X) and the ADM device (SEApont), and the operation of the two devices is not integrated. The managements of the two devices are similar. So this document focuses the management system design and implement of Tetra-X.

This document starts with the network management It tells the network management concept and 5 management functions, and analyzes the network management modes and network management frames so that to confirm their objects in point. In the project, we use the centralized manage mode and the Internet/SNMP frame. Then, the document tells the SNMP protocol and analyzes its advantages and disadvantages. The project is based on the transport net, so the third chapter tells the knowledge about transport net. From beginning of the fourth chapter, the document concentrates the project, it tells the network in which the Tetra-X device works, and also tells about the Tetra-X device. In fifth chapters, it tells the client software design and implement of the management system.

At last, this document analyzes the problems in the progress of the software implement.

**KEY WORDS:** Network Management, SNMP, 2M Digital Private Line, Client

### 独创性（或创新性）声明

本人声明所呈交的论文是本人在导师指导下进行的研究工作及取得的科研成果。尽我所知，除了文中特别加以标注和致谢中所罗列的内容以外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得北京邮电大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

申请学位论文与资料若有不实之处，本人承担一切相关责任。

本人签名：黄颖 日期：2005.3.15

### 关于论文使用授权的说明

学位论文作者完全了解北京邮电大学有关保留和使用学位论文的规定，即：研究生在校攻读学位期间论文工作的知识产权单位属北京邮电大学。学校有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许学位论文被查阅和借阅；学校可以公布学位论文的全部或部分内容，允许采用影印、缩印或其它复制手段保存、汇编学位论文。（保密的学位论文在解密后遵守此规定）

保密论文注释：本学位论文属于保密在  年解密后适用本授权书。非保密论文注释：本学位论文不属于保密范围，适用本授权书。

本人签名：黄颖 日期：2005.3.15

导师签名：李 日期：2005.3.28

## 第一章 绪论

### 1.1 课题背景

随着网络应用的发展和普及,随着信息技术的飞速发展,计算机网络的应用规模呈爆炸式增长,硬件平台,操作系统平台,各种各样的网络层出不穷,各大电信运营商都相继建起了自己的网络,问题也就应运而生,很多企业把过多的精力都投入到网络的建设中,而忽视了网管建设,认为网络建成能够投入运行便是成功了。然而在网络应用十分广泛的今天,仅仅靠原来网管人员的亲力亲为、现场维护和人工排查是远远不能满足网管的要求的。简单的人工网管投入更大,大量人工投入、现场管理维护等技术支持使费用大幅增加。同时由于网点较多,如果有几处同时出现问题或需要更新升级,则人工无法同时进行,势必要停业,造成不良影响,造成企业服务水平和信誉的降低、客户信心和好感的降低等,这些损失是无法用金钱来衡量的。

如果运用网络管理技术开发先进的网络管理系统,就会使这个问题得到极大的改善。当监视程序报告网络出现故障时,就会通过提供故障和监视设备的距离来告诉您诸如短路和断路等故障的位置,通过网络拓扑还会告诉您发生故障设备名称和地址。这样,您就能十分容易得到所需的故障信息,对故障的查找和处理将变得十分轻松,效率也将大幅提升。网络管理从简单人工管理到系统管理,不仅仅是一个从人工到系统的简单过程,而是一个质的飞跃。虽然,网管系统并不是万能的,但有了网管系统,网络就多了一个“管家”,必然会为网络正常运行起到非常重要的保障作用。

网络管理已成为计算机网络、电信网络和广播电视网络等系统管理和建设中的一个非常重要且必不可少的部分,它决定着网络资源的利用率和效益的发挥。网络管理系统是网络维护的主要手段,也是网络正常运行的根本保证,是各种网络之间互联互通的准则。

### 1.2 课题任务

从 2003 年 6 月开始本人进入实验室参与了网管系统的开发,此网管系统是基于 SDH 传输网的 2M 数字专线网的网络管理系统。目标是实现对整个 2M 数字专线网系统的管理,该系统使用基于 SNMP 协议的管理模型。系统架构分为三层:客户端、服务器、设备层。我在刘新闻老师的带领下,以 JAVA 语言

为开发工具，使用面向对象的程序设计方法，与同学张姝共同进行了客户端的软件开发。至 2004 年的 9 月，此项目只实现了对核心层设备 Tetra-X 和汇接层设备 SEApont 的管理，并且对 Tetra-X 设备和 SEApont 设备的管理还是相对独立的，在逻辑上和业务上都没有进行整合。此期间本人独立承担了 Tetra-X 设备的节点、端口、中继、查询，SEApont 设备的电路板等功能模块的设计开发。这一系列开发涉及到网络管理中的故障管理、配置管理、性能管理等诸多方面，共完成代码约 7 万行左右，并完成代码的测试与优化工作。

### 1.3 论文结构

本课题任务涉及到网络管理、传输网设备的网络管理、SDH 传输网的相关知识。因此论文在第二章和第三章主要介绍了与课题设计相关的背景知识，从第四章开始论文将围绕课题展开，分析网络管理知识在具体网络管理系统中的应用及其实现。论文的具体章节安排如下：

第二章主要讲述了与课题相关的网络管理的知识，其中包括网络管理的概念、网络管理的 5 大功能、网络管理的结构模式、网络管理的体系结构、简单网络管理协议及网络管理系统的发展方向。

第三章介绍 SDH 传输网和传输网网管知识。

第四章介绍 Tetra-X 设备网管系统及 Tetra-X 设备。

第五章介绍 Tetra-X 设备网管系统的客户端软件设计。

## 第二章 网络管理概述

### 2.1 网络管理概念

随着大规模互连网络的建设及应用的迅猛发展,新技术、新设备的广泛应用使网络变成一个多厂商混合网络,网络的类型、服务的种类和设备的来源更加复杂化。在这种环境下,资源分布程度和共享程度大大提高,任何微小的故障都可能导致用户应用的失败。如何及早发现并排除潜在的故障隐患,有效地管理好网络,是网络设备和网络服务提供者共同关心的问题。事实证明,管理好一个网络与网络的建设同等重要。人们迫切需要功能完善、安全可靠、使用方便灵活的网络管理工具来加强网络管理的能力,提高网络的使用效率。

直观的讲,网络管理就是对网络的性能、品质进行监测和控制的过程。监测即跟踪网络的行为;控制即调整和改进网络的性能。其内容包括对组成网络的各个单元设备(硬件和软件)的性能进行监测,对网络中流通的业务进行监测,在发现设备故障时进行处理,如启用备用设备,在发现网络过载(拥塞)时进行调度处理,包括路由调度和业务调度(组织一些相对不重要的业务进入)网络管理中,一般采用管理者-代理的管理模型如下:

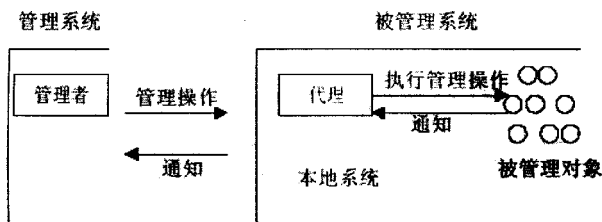


图 2-1 网络管理模型

管理者可以是工作站,微机,一般位于网络系统的主干或接近主干的位置,它负责发出管理操作的指令,并接收来自代理信息。

代理则位于被管理的设备内部,把来自管理者的命令或信息请求转换为本设备特有的指令,完成管理者的指示,或返回它所在设备的信息。另外代理也可以把在自身系统中发生的事件主动通知给管理者。

管理者将管理要求通过管理操作指令传送给位于被管理系统中的代理,代

理则直接管理被管理设备。代理可能因为某种原因拒绝管理者的指令。管理者和代理之间的信息交换可分为两种：从管理者到代理的管理操作，从代理到管理者的事件通知。

管理者和代理之间交换管理信息必须遵循统一的通信规约，我们称这个通信规约为网络管理协议。网络管理协议是高层网络协议，它是建立于具体物理网络及其基础通信协议基础之上的，为网络管理平台服务。目前，网络界使用两大网管协议，即基于 Internet 及 TCP/IP 的 SNMP 和 OSI/ISO 的 CMIP。

现在，我们可以从管理者—代理的角度对网络管理再进行一次定义：网络管理为控制、协调、监督网络资源提供的手段，就是管理者（Manager）与代理（Agent）之间利用网络实现管理信息交换，完成管理功能。管理者从各代理处收集管理信息，进行加工处理来获取有价值的管理信息，达到让代理代理管理之目的。

网络管理平台是指一个包含网络管理进程软件和基本网络管理应用的主管系统，网络平台就是满足最低管理需求的主管系统，有了网络平台，管理人员就可以经管理者与被管系统中的代理通信。

## 2.2 网络管理 5 大功能

国际标准化组织（ISO）定义了网络管理的 5 个功能域：

- 故障管理
- 配置管理
- 性能管理
- 计费管理
- 安全管理

下面分别进行简要介绍。

### 2.2.1 故障管理

故障管理（Fault Management）是基本的网络管理功能。故障管理是网络管理功能中与故障检测、故障诊断和故障恢复等工作有关的部分，其目的是保证网络能够提供连续可靠的服务。网络服务的意外中断往往对社会或生产造成很大的影响。另一方面，在大型计算机网络中，发现故障时，往往不能具体确定故障所在的具体位置，这就需要故障管理提供逐步隔离和最后定位故障的一整套方法和工具。有时候，所发现的故障是随机性的，需要经过很长时间的跟踪和分析，才能找到其产生的原因。这就需要有一个故障管理系统，科学地管理网络所发现的所有故障，具体记录每个故障的产生，跟踪分析以至最后确定并修复故障。所以，故障管理应包含以下 5 项典型功能：



- 维护并检查错误日志
- 接受错误检测报告并作出响应
- 跟踪、辨认错误
- 执行诊断测试
- 纠正错误

### 2.2.2 配置管理

配置管理（Configuration Management）是维护网络正常有序运行的重要手段。它初始化网络、配置网络，以使其提供网络服务。目的是为了实现某个特定功能或使网络性能达到最优。配置管理的内容包括：

- 设置开放系统中有关路由操作的参数
- 对被管对象或被管对象组名字的管理
- 初始化或关闭被管对象
- 根据要求收集系统当前状态的有关信息
- 获取系统重要变化的信息
- 更改系统的配置

配置管理的任务是识别网上设备和用户，收集必要的数据库，为通信系统的初始化提供数据，而且要提供连续可靠的连接。配置管理主要关心的是维护网上软件、硬件和电路的精确清单，修改清单的能力以及响应改变业务需求的可靠方法。

### 2.2.3 性能管理

性能管理（Performance Management）是对网络性能的管理，要求做到对网络的特性、资源利用率以及有关通信活动进行分析，以帮助网络管理人员评价网络资源及相关的通信活动的情况和效率。有效的性能管理能优化网络的性能，最大限度地满足不同层次用户对网络的需求。

性能管理可从3个方面着手：

- 建立对当前网络性能测量的基准
- 寻找识别网络与应用软件不匹配的方法
- 进行分析测量，寻找可能改进网络性能的对策

性能管理包括系统资源的运行状况及通信效率等系统性能，其能力包括监视和分析被管网络及其所提供服务的性能机制。性能分析的结果可能会启动某个诊断测试过程或重新配置网络，以便维持网络的性能。性能管理收集、分析有关被管网络当前状况的数据信息，并维护和分析性能日志，其典型的功能包括：

- 收集统计信息
- 维护并检查系统状态日志
- 确定自然和人工状态下系统的性能
- 改变系统操作模式以进行系统性能管理的操作

#### 2.2.4 计费管理

计费管理 (Accounting Management) 负责记录网络资源的使用, 目的是控制和监测网络操作的费用和代价, 它对一些公共商业网络尤为重要。它可以估算出用户使用网络资源可能需要的费用和代价, 以及已经使用的资源。网络管理员还可以通过向户收取费用来控制用户过多地使用和占用网络资源。这也从另一方面提高了网络的效率。另外, 当用户需要使用多个网络资源时, 计费管理应能计算总费用。

计费管理在局域网上不那么重要, 因为局域网主要在一个单位内部使用, 计费也不那么严格, 所以计费系统比较简单, 多数都包括在网络操作系统内。

计费管理是对网络资源和通信资源的使用进行计费, 包括对用户使用的各种资源进行跟踪, 统计用户对资源的使用数量和占用时间, 计算费用及对收费用户进行确认。该系统能对用户的访问活动建立详细记录, 这既是对用户收费的依据, 又是对网络极有用的信息, 因为发生问题后可根据记录查找原因。

计费系统还具有安全管理功能。它能告诉网络管理员谁在网上的什么地方、什么时候, 做了什么工作, 哪个用户在什么时间用了哪些资源等。管理员可以用它检查某个用户对某服务器、目录或文件的操作。该系统还提供错误报告清单, 利于防止故障发生。

#### 2.2.5 安全管理

安全管理 (Security Management) 是网络管理中非常重要的内容。安全性一直是网络的重要环节之一, 而用户对网络安全的要求也相当高。

安全管理有两层含义。一方面, 网络安全管理要保证网络用户和网络资源不被非法使用; 另一方面, 网络安全管理也要确保网络管理系统本身不被未经授权地访问。网络安全管理的主要内容包括:

- 与安全措施有关的信息发布 (如密钥的分发和访问权设置等)
- 与安全措施有关的事件通知 (如网络有非法侵入、无权用户对特定信息的访问企图等)
- 安全服务设施的创建、控制和删除
- 与安全措施有关的网络操作事件的记录、维护和查阅等日志管理工作等等。

## 2.3 网络管理结构模式

国际上的网络管理结构模式可以分为：集中式网络管理、分级式网络管理、分布式网络管理三种类型。这三种类型各自有其优缺点。

### 2.3.1 集中式网管

集中式系统是传统的网管方法，它是由一个大系统去运行大部分所需应用程序，运行在管理系统中的每个应用程序将信息存储在位于网络中心的同一数据库中。

事实上集中式体系结构中的管理者可以划分成两部分：管理平台和各种管理应用程序。管理平台作为处理管理数据的第一级，主要涉及信息收集，提供诸如监控、流量计算等关键管理服务，同时向应用程序提供数据处理报告摘要。应用程序运行在数据处理的第二级，提供各种系统管理功能，处理决策支持等比信息收集和简单计算等更高级的功能。两部分通过公共应用程序接口 API 进行通信。这种体系结构的特点是具有方便的系统维护性和扩展性，并简化了在异种主机、多厂商、多管理协议环境中综合程序的开发工作。异构性和协议复杂性只在平台级管理，不必在每个应用程序中考虑。

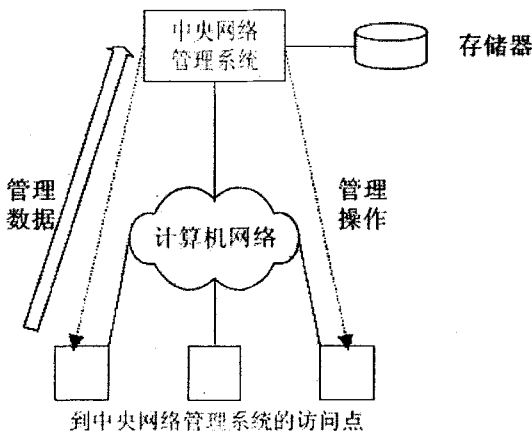


图 2-2 集中式网管结构

其主要优点为：

- 操作终端的地点不受限制，当操作终端与服务器在异地时，可以通过 VPN 访问
- 网管中心保持的数据始终是最新的，免去了数据同步的问题

- 只需要开发和安装一种 Server 软件

其主要缺点为:

- 即使操作终端离设备很近,例如在一个机房里,也要先登录到网管中心,再折回来与设备通信。这带来了附加的通信负载。

### 2.3.2 分级式网络管理系统

这种网络管理模式,是由一个网络管理系统(NMS),即管理站(manager)作为另外几个网络管理系统管理站(managers)的总管理站。由各管理站管理各自所管辖(managed entity)的领域,而出总管理站总的管辖对其它管理站所应管辖的部分。这种系统的优点是分散了网络/资源(network/resource)的负荷,使得各个网络管理可更接近被管单元,降低了总网络管理系统需收集传送的业务量;该系统比集中式网管系统更可靠。这种网络管理系统的缺点是比上述集中式系统更为复杂,系统设备价格也相应有所提高。

### 2.3.3 分布式网络管理

分布式结构中,几个对等的网络管理系统同时运行在计算机网络中。在这种体制下,每一个系统可以管理网络中的一个特定部分。而且,可以由不同的系统管理不同的网络设备,并不一定要求其结构在地理上是分布的。

这种结构的主要特点是扩展性好,通过建立更多的管理域以及增加相应数量的管理者就可以满足更多的性能要求和扩充性。

其主要优点为:

- 企业用户可以就近管理自己的网络资源,网管网故障时,本地网管终端随时可以执行功能。
- 设备的某些软件功能可以简化,转移到本地服务器中,本地服务器与网管中心可采用内部接口/SNMP/XML等接口。

其主要缺点为:

- 网管中心的服务器需要和企业用户的服务器保持数据一致。
- 增设本地服务器也就增加了一个不可靠点,并且增加成本,性能也会有所降低。
- 可能需要开发和安装两种 Server 软件(分别用于网管中心和企业用户)。

### 2.3.4 网管结构模式的比较

如前所述,三类模式各有其优缺点,并有其各自的应用范围:第一类适用于规模较小的网络系统、第二类适用于单一业务和网络拓扑结构简单的网络系统;而第三类适用于多业务信息量大而且能灵活扩容、容易升级,能异构处理

的网络系统。显然第三类分布式网络结构模式，更适合于未来的通信信息网络管理采用。由于海量信息、多种信息类型和异构并行信息处理的需求日益增加，这必将促使未来的网络管理具有灵活升级和易于扩展的功能，而这正是分布式网络管理模式的优势所在。

## 2.4 网络管理体系结构

### 2.4.1 基于 INTERNET / SNMP 的网络管理体系结构

SNMP 管理体系结构由管理者、代理和管理信息库 (MIB) 三部分组成。管理者 (管理进程) 是管理指令的发出者, 这些指令包括一些管理操作。管理者通过各设备的管理代理对网络内的各种设备、设施和资源实施监视和控制。代理负责管理指令的执行, 并且以通知的形式向管理者报告被管对象发生的一些重要事件。代理具有两个基本功能:

- 从 MIB 中读取各种变量值;
- 在 MIB 中修改各种变量值。

MIB 是被管对象结构化组织的一种抽象。它是一个概念上的数据库, 由管理对象组成, 各个代理管理 MIB 中属于本地的管理对象, 各管理代理控制的管理对象共同构成全网的管理信息库。

SNMP 有许多缺点, 是它自身难以克服的: SNMP 不适合真正大型网络管理, 因为它是基于轮询机制的, 这种方式有严重的性能问题; SNMP 不适合查询大量的数据; SNMP 的 trap 是无确认的, 这样有可能导致不能确保非常严重的告警是否发送到管理者; 安全管理较差; 不支持如创建, 删除, 动作等类型的操作, 要完成这些操作, 必须用 set 命令间接的触发; SNMP 的 MIB 模型不适合比较复杂的查询。正是由于 SNMP 协议及其 MIB 的缺陷, 导致 INTERNET / SNMP 网络管理体系结构有以下问题: 没有一个标准或建议定义 INTERNET / SNMP 网络管理体系结构; 定义了太多的管理对象类, 管理者必须面对太多的管理对象类。为了决定哪些管理对象类需要看, 哪些需要修改, 管理者必须明白许多的管理对象类的准确含义; 缺乏管理者特定的功能描述。INTERNET 管理标准仅仅定义了一个个独立管理操作。

### 2.4.2 基于 OSI / CMIP 的网络管理体系结构

OSI / CMIP 系统管理体系结构中, 基本概念有系统管理应用进程 (SMAP)、系统管理应用实体、层管理实体和管理信息库 (MIB)。系统管理应用进程是执行系统管理功能的软件。它管理系统的各个方面并与其他系统的 SMAP 相互协调。系统管理应用实体负责与其他系统的对等 SAME 间交换管理信息。层管理提供对 OSI 各层特定的管理功能。MIB 是系统中属于网络

管理方面的信息的集合。对于SMAL 可以根据其在系统间交互时的作用不同,分为管理者 and 代理两种角色。

OSI / CMIP 管理体系结构是以更通用更全面的观点来组织一个网络的管理系统,它的开放性、着眼与网络未来发展的设计思想,使得它有很强的适应性,能够处理任何复杂系统的综合管理。然而正是OSI 系统管理这种大而全的思想,导致其有许多缺点:如OSI 系统管理太复杂,CMIP 的功能极其灵活强大,使得OSI 系统管理方法太复杂,从而OSI 系统管理与实际的应用有距离,OSI 在实际应用中不成功;缺乏相应的开发工具,这种开发工具可以使开发者不需了解OSI 管理。代理系统花费太高;OSI 系统管理虽然管理信息建模是面向对象的,但管理信息传送却不是面向对象的,OSI 系统管理不是纯面向对象的等。

#### 2.4.3 TMN 网络管理体系结构

电信管理网(TMN)是一个逻辑上与电信网分离的网络,它通过标准的接口(包括通信协议和信息模型)与电信网进行传送/接收管理信息从而达到对电信网控制和操作的目的。TMN 为电信网络和服务提供管理功能,并提供自身与电信网络和服务间的通信。TMN 的基本思想是提供一个有组织的体系结构,实现各种运营系统(OS)以及电信设备之间的互连,利用标准接口所支持的体系结构交换管理信息。从而为管理部门和厂商在开发设备以及设计管理电信网络和业务的基础结构时提供参考。

TMN 从 80 年代中期提出后,已成为全球接受的管理电信公众网的框架。尽管 TMN 有技术上先进、强调公认的标准和接口等优点,但随着计算机和通信技术的不断发展,TMN 自身也暴露出许多问题如:目标太大、抽象化程度太高、MIB 的标准化进度慢等。

#### 2.4.4 管理体系结构比较

如前所述各种体系结构均有各自的优缺点,SNMP 由于其简单易实现,在计算机网络应用非常广泛,成为事实上的计算机网络管理的标准。主要是因为 SNMP 协议有如下几个特点:

首先,相对于其它种类的网络管理体系或管理协议而言,SNMP 易于实现。SNMP 的管理协议、MIB 及其它相关的体系框架能够在各种不同类型的设备上运行,包括低档的个人电脑到高档的大型主机、服务器、及路由器、交换器等网络设备。一个 SNMP 管理代理组件在运行时不需要很大的内存空间,因此也就不需要太强的计算能力。SNMP 协议一般可以在目标系统中快速开发出来,所以它很容易在面市的新产品或升级的老产品中出现。尽管 SNMP 协议缺少其

它网络管理协议的某些优点，但它设计简单、扩展灵活、易于使用，这些特点大大弥补了 SNMP 协议应用中的其他不足。

其次，SNMP 协议是开放的免费产品。只有经过 IETF 的标准议程批准（IETF 是 IAB 下设的一个组织），才可以改动 SNMP 协议；厂商们也可以私下改动 SNMP 协议，但这样作的结果很可能得不偿失，因为他们必须说服其他厂商和用户支持他们对 SNMP 协议的非标准改进，而这样做却有悖于他们的初衷。

第三，SNMP 协议有很多详细的文档资料（例如 RFC，以及其它的一些文章、说明书等），网络业界对这个协议也有着较深入的理解，这些都是 SNMP 协议近一步发展和改进的基础。

最后，SNMP 协议可用于控制各种设备。比如说电话系统、环境控制设备，以及其它可接入网络且需要控制的设备等，这些非传统装备都可以使用 SNMP 协议。

正是由于有了上述这些特点，SNMP 协议已经被认为是网络设备厂商、应用软件开发者及终端用户的首选管理协议。

## 2.5 简单网络管理协议

在网络管理中，Manager 和 Agent 之间需要进行通信以传递管理信息，因此定义统一的通信协议标准就成为一项非常重要的课题。从 80 年代中期开始，许多研究人员希望通过标准化过程，完善和加强网络管理功能，其中包括 IETF（Internet Engineering Task Force）的简单网络管理协议 SNMP 以及后来的 SNMPv2、SNMPv3 和 ISO（International Standard Organization）的开放系统互连公共管理信息协议（OSI CMIP）等。这些协议标准的出发点各不相同，表现出的框架结构和内容亦有所差异。其中，SNMP 的目标是为基于 TCP/IP 协议的网络增加一种简单实用的管理方法；而 OSI/CMIP 则是为 OSI 的七层开放互联模型设计的管理模型。由于 TCP/IP 协议已成为事实的工业标准，因此，SNMP 是目前使用最广泛的网络管理模式。SNMP 协议（Simple Network Management Protocol）的第一个版本即 SNMPv1 于 1988 年公布，由于它的简单性和有效性，该协议得到了广泛的应用。但与此同时，它的缺陷也日益明显，这其中包括：不能实现 Manager 和 Manager 之间的通信，不能进行大量数据的传输，缺乏安全管理机制等等。1993 年，SNMP 的第二个版本即 SNMPv2 正式发表。SNMPv2 对 SNMPv1 进行了完善，它一经发表就很快得到各网络产品生产厂家的广泛支持，并使之成为了事实上的网络管理工业标准。SNMPv3 指的是简单网络管理协议的第三版，他在安全和管理这两个方面对 SNMP 进行扩

展，解决了以前SNMP 版本的缺陷和问题，是它更具有实际应用价值。

### 2.5.1 SNMP 网络管理结构

SNMP采用请求/响应的方式，工作于UDP之上。使用SNMP进行网络管理需要下面几个重要部分：管理基站，管理代理，管理信息库（MIB），SNMP 协议。

**管理基站：**从管理代理处获取设备信息并将对设备的控制信息发送给管理代理。

**管理代理：**提供给管理基站管理信息库中存储的设备信息并接受管理基站发来的对设备的控制数据。

**管理信息库（MIB）：**我们通常很少把在一个被管理设备中的数据库称为一个数据库。在 SNMP 术语中它通常被称为管理信息库（MIB）。MIB 是对象的集合，它代表网络中可以管理的资源和设备。每个对象基本上是一个数据变量，它代表被管理的对象的一方面的信息。

**SNMP 协议：**网管工作站 Manager 同 Agent 之间通信的 SNMP 协议。

SNMP 管理模型具备典型的C/S（客户机/服务器）体系结构。

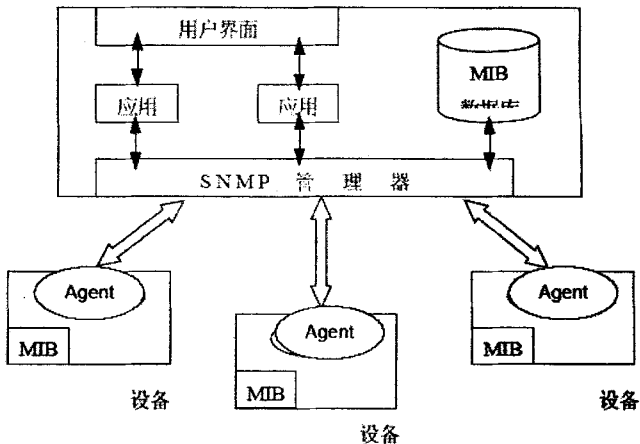


图 2-3 SNMP 网络管理结构

网管工作站运行SNMP 管理软件的客户端（通常称为Manager，管理者），而被管的网络设备运行软件的服务端（通常称为Agent，代理）。SNMP 的设计原则是：把所有智能和复杂性放在管理器（客户端）上，使代理（服务器端）尽可能简单，以尽量减少对被管设备的影响，即不要让被管设备因执行网



络管理功能而影响其完成本职工作。

网管工作站可以是一般的计算机，它运行复杂的管理器软件，对网络设备进行监控，它是这个网络的集中控制点。SNMP 没有规定网管工作站的构成，但是一般来说，它至少具有下述功能：

- 一组能够分析数据的管理应用 网络管理员的操作界面。
- 一组同 Agent 进行通信的进程，这些进程向 Agent 发出命令并得到响应结果。
- 所有收集到的管理对象数据的管理。

被管对象（网络设备）可以多种多样，如主机、被管设备、网桥、终端服务器等。Agent 是驻留在被管对象上的通常以守护进程形式在后台运行的进程，负责接收有关信息，并给 MIB 中的相应变量赋值，在接收到网管工作站发来的请求时将这些值回传给网管工作站。

MIB 是被管对象的状态信息集，由一组变量构成，每个变量表示被管对象属性状态的一个方面。从数据库的角度来看，MIB 是组织成分级的数据库，它将被管数据存储存储在树叶中。SNMP 网管实际就是针对被管对象 MIB 的管理。网管工作站和众多的 Agent 之间通过网络管理协议相连接。SNMP 协议很简单，只包含几条原语。

#### 2.5.2 SNMP 通信协议

SNMP 位于应用层，利用 UDP 的两个端口（161 和 162）实现管理员和代理之间的管理信息交换。UDP 端口 161 用于数据收发，UDP 端口 162 用于代理报警（即发送 Trap 报文）。

SNMP 代理和管理站通过标准消息通信，这些消息中的每一个都是单个的数据包。由此，SNMP 使用 UDP（用户数据报协议）作为传输层协议，使用有限的 PDU 完成其简单的管理消息的通信功能。UDP 使用无连接的服务，因此 SNMP 不需要依靠代理和管理站之间保持连接来传输消息。

在标准中共定义了五种 PDU：

- Get-Request：管理者要求被管理实体代理给出网络信息
- Get-Next-Request：管理者要求给出管理信息库存放的下一个信息
- Set-Request：改变被管理实体中的变量的值
- Get-Response：代理对 Get-Request、Get-Next-Request、Set-Request 要求作出响应，响应包含错误和状态信息
- Trap：代理向管理者发出事件报告

图 2.2 示意了这 5 种消息。

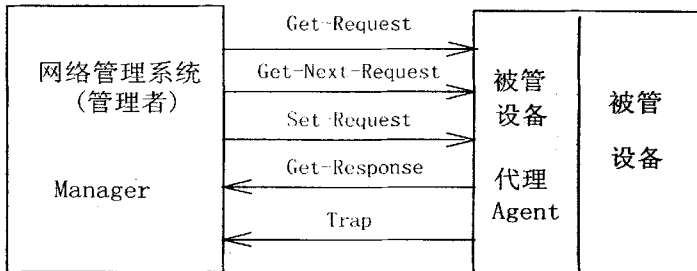


图 2-4 SNMP 消息

Manager 不停地通过 Get、GetNext 原语从 Agent 中读取被管对象在 MIB 中的每个变量，从而综合获得当前网络的状态；每当出现异常情况时，Agent 利用 Trap 原语向 Manager 发出报警；SNMP 协议没有直接控制 Agent 行为的原语，但是 Manager 能够通过 Set 原语设置 MIB 中的某些变量的值以达到简单的控制目的。

虽然 Get 和 GetNext 原语都是用来从 MIB 中检索数据的，但它们之间是有区别的：Get 必须直接通过它们的路径识别符去规定被管变量组，这有利于非表格格式数据的检索，在那里路径是静态已知的；GetNext 用于在表格格式的数据中移动。

管理者收集信息的方式有两种：轮询和事件报告。

轮询即 Manager（管理者）和 Agent（代理）之间的请求 / 响应交互作用。Manager 实体向 Agent 实体发出查询请求，即向 Agent 实体发送封装有 SNMP\_PDU\_GET 或 SNMP\_PDU\_GETNEXT 类型的 PDU 的 IP 包。Agent 收到内含该 PDU 的 IP 数据包后，进行解析，从 MIB 库中取出各自对应的 Value 值，以相反的过程送给 Manager 实体作为响应。Manager 收到数据并经过分析之后，就可以知道网络各性能参数的变动情况，即网络的当前运行状态。

网络中被管的设备经过相应的配置设定后，运行于其上的代理进程即可向某一特定的管理者实体发送事件报告，即 Trap 信息。事件报告用以阶段性地说明被管对象的当前状态，报告有重要事件或故障发生。管理者实体在创建 Session 时，对其作 Register 操作后，即可接收 Trap 信息。管理者实体对收到的 SNMP\_PDU\_TRAP 类型的 PDU 作解析，取出网络的当前运行状态信息。

### 2.5.3 SNMP 的缺点

由于 SNMP 的简单和灵活，使得 SNMPv1 的应用非常广泛，成为事实标

准。SNMP 似乎有无穷的扩充能力,使得许多网络设备出厂时就安装了SNMP的Agent,许多设备厂商也为自己的产品设计网管应用。但是,当网络规模增大时,各种管理应用变多时,SNMP 的网络管理模式暴露出许多不足:

#### 1. 管理的不一致 SNMP

网络管理模型实际只定义了管理信息的传递方法,没有定义管理功能和基本策略,使其处于一种自由发展的状态。当网络中的设备和应用增多时,不同的设备厂商为各自设备设计的管理应用同时运行在同一个管理工作站上,这些网络管理应用缺乏统一的设计思想,造成管理界面和使用方法不同,相互间的管理动作不能协调和沟通,信息不能共享,从而使得它们的集成化程度较低。

#### 2. 网管工作站逐步成为“瓶颈”

网管工作站是SNMP 网管框架中的信息收集和处理中心,它的性能就是网络管理系统的性能。网管工作站不仅要及时轮询每个被管对象的状态,读取它们的MIB,还要通过相应的网管应用对获得的信息进行分析、处理和存储,有时还要对Agent 发来的Trap 报警信息进行响应,因此当被管对象很多时,网管工作站的负荷很重,轮询一次需要的时间很长,导致Trap 信息得不到及时的响应,会造成严重后果,而且网管工作站得到的不同被管对象的信息不能综合形成某一时刻系统的状态。

#### 3. 加重被管网络的流量负荷

由于网络设备种类和复杂性不断提高,MIB 的数量以及每个MIB 中包含的变量不断增加。当网管工作站收集这些信息时,会带来很大的网络信息流量。例如,有1000 个被管对象,每个MIB 包括20 个变量,每个UDP 包的长度为100 个字节,则轮询一次的流量是: $1000 \times 20 \times 100 \times 8 \times 2 = 32\text{Mbits}$ 。如果简单网络管理协议工作站处于一个10Mbps 的以太网,并且工作在40%的效率下,则传输这些网管信息需花费的时间是 $32 / (10 \times 40\%) = 8\text{s}$ 。另外,网管工作站读取MIB 完全是机械盲目的,没有一定的目的性,只是从头读到尾,往往其中有用的变量只是几个,却不得不重复,结果浪费了网络资源。

#### 4. SNMP 不提供选择(过滤)被检索数据的方法

一个检索机制理论上应该允许管理者选择所要的数据,而不是迫使它们检索大量的无用数据。应该在数据源最大限度地压缩数据,而不是把数据通过网络送给管理者。把SNMP扩展到支撑有选择的检索意味着代理功能和协议接口方面需要有稍大的复杂性。

##### 2.5.4 SNMP 的发展趋势

为了弥补SNMP 的不足,研究人员作了大量的改进工作。RaoufBoutaba 等

提出利用Domain/Policy 的集成网络管理方案，使网络资源的管理具有层次化结构，并将网络管理功能定义为在Policy指导下的计划（Plan）和执行

（Executive）过程；Tschichholz 等从网络管理信息角度提出TMN和SNMP两种网络管理模型集成的思想：在广域网上利用TMN 进行管理，在局域网上用SNMP 进行管理；Columbia 大学的Goldszmidt 和Yemini 等人探讨了分布式管理和集中管理的关系和利弊，提出了Management by Delegation 的管理方法；IBM 公司则利用智能代理（Intelligent Agent）来加强其网络管理软件的能力，允许Agent 按照一定的规则对异常事件进行分析处理。在改进和完善SNMP 时，应该注意以下几个方面：

- 必须延续简单实用的策略；
- 保持同 SNMP 的兼容，因为目前已经有大量的遵循 SNMP 协议的网络管理系统被使用，完全抛弃 SNMP 是不行的；
- 分布式管理。分布管理的直接好处是每个 Manager 管理的范围较小，管理的内容和目标明确，反应速度快；
- 移动（Mobile）Agent 技术。Agent 不再是功能固定的，而是可以在接受用户的意图后，自主地在网络上移动。这样网管工作站可以按照一定策略将网络管理功能分派给不同的 Agent，从而呈现出很大的灵活性，因此移动 Agent 技术具有很大的潜力。

## 2.6 网络管理系统的发展方向

尽管目前各种网络管理系统在结构上存在或大或小的差异，技术上各具特色，但是随着标准化活动的开展，系统互联的需要，这些产品和技术在许多方面逐渐走向统一，主要体现在以下几个方面：

- 综合性

现有的通信网一般是由许许多多多个独立管理的专用网和多个公用交换网互连组成的，有的专用网已经建立起网络管理系统，有的则正在建立之中。每个网管系统的建立往往是根据专业网各自的需要逐个进行的。把这些互相割裂的独立网管系统综合起来，实现他们的互连、互通和互操作，是一体化的网络管理的主要目标。实现综合可以实现资源共享、实现信息互换、简化管理操作。

如同综合业务网络一样，不论什么业务，用户希望看到的只是一个网络，甚至只是一个终端。网络管理也一样，网络管理系统的综合已经成为人们的共识，也是世界上网络管理系统发展的方向。TMN 就是电信网综合管理的极好例子。

- 集中化

电信网网络管理在建设初期由于计算机硬件性能的限制,软件开发成本和难度过高,以及组建网管系统所需数据网络的匮乏,只能以物理分散的方式实现。这样分散的管理机制,不利于网络运营者全面综合的监测、分析网络的情况,无法有效的优化网络,提高业务质量,随着计算机技术的飞速发展,软件行业日趋成熟,通信网络已经具备,制约电信网集中管理的因素都已经化解,使得集中网络管理的方式成为可能。网络管理将会朝着尽量集中的方式发展,集中监视、集中控制、集中配置、集中调度,减少人力,加快响应速度,提高效率。

- 智能化

现在通信网络的迅速发展使网络的维护和操作变得相当复杂,人工维护和诊断往往费时费力,而且对于间歇性故障无法及时检错排除。人工智能技术可用于解释网络运行的差错信息、诊断故障和提供处理建议,而不是给出故障的原始数据。性能专家系统将能够分析运行参数和数据,在用户发现网络故障之前预测和排除故障。

- 可扩展

电信网的管理内容、管理方式是变化发展的,因此,网管的建设是持续的、长期的,电信网网管的建设应该注意可扩展性,保证在网络的规模扩大、网络的业务增长、网络的管理变动时,网管系统在较少的调整下仍然可以适用。

- 标准化

电信管理网的建设应符合 ITU-T 的相关建议,符合我国已经制定的各种标准,以利于网管系统的可持续性建设和发展,尽可能的实现管理信息模型与数据的标准、开放、以便于适应管理各种各样的网络设备和与其他系统的互联互通。

- 基于 WEB 的管理

在许多网络管理领域的主要管理系统中都提供了融合 Web 的管理技术还并不成熟,但是基于 Web 的管理以其统一、友好的界面风格,地理和系统的可移动性和系统平台的独立性吸引着越来越多的用户和开发商。

## 第三章 传输网网络管理

### 3.1 SDH 传输网

同步数字体系 (SDH——Synchronous Digital Hierarchy) 是一整套可进行同步数字传输、复用和交叉连接的标准化数字信号的结构等级。SDH 传输网所传输的信号由不同等级的同步传输模块 (STM-N) 信号所组成。

STM-1 信号是 SDH 的第一级, 是基本同步传送模块信号, 比特率为 155520kbit/s。

STM-N 信号是 SDH 的较高等级的同步传输模块信号, 比特率是 STM-1 信号的 N 倍。

一个 STM-1 帧分组共计 9 行, 270 列, 每列中一个字节 (8bit), 帧周期, 即帧频为 8000 帧/秒。STM-1 的传输速率为:  $270 \times 8 \times 9 \times 8000 = 155.520 \text{Mbit/s}$ 。帧结构中设置了两种开销, 分别是段开销 (SOH) 和通道开销 (POH)。



×国内保留使用的字节

\* 非扰码字节

△媒体相关字节

图 3-1 SDH 开销字节

SDH 网络的设备主要有: 同步终端复用器 (STM), 分插复用器 ADM (add/Drop Mutiplexer) 和同步交叉连接设备 SDXC (Synchronous Digital Cross Connect)。

STM 有两类。一类提供 G.703 接口到 STM-N 的复用功能，另一类是高阶复用，将低 STM 信号复用成高阶 STM 信号。

分插复用器是 SDH 中应用最广、最富特色的设备。它是一个三端口设备，具有两个 SDH 光接口，通过另一端可以灵活地上/下路复用 STM 信号中的低速率信号。ADM 内部还具有时隙交换功能，允许两个 STM 信号之间不同 VC 的互联，并能方便地进行带宽管理。在实际网络中，根据 ADM 的结构特点，它可灵活的用在网络中不同位置。作为终端复用器时，可将两个 SDH 光接口分别作为主备用，实际复用设备往往既可配置成终端复用器又可配置成分插复用器。利用 ADM 还可构成各种自愈环。

数字交叉连接设备 (DXC) 是现代数字通信网中非常重要的设备之一，DXC 并不是 SDH 网独有的设备，新研制的 DXC 设备往往既可以用 SDH 网也可以用于 PDH 网络。SDXC 是一种兼有复用、配线、保护、监控和网管多功能的传输设备。它能代替配线架，对 VC 进行交叉连接。动态调整网络，实现半永久连接；SDXC 还能对业务进行集散。利用 SDXC 的自动配置功能也可以构成 SDH 的自愈网，在网络出现故障后自动重选路由，恢复业务。干线网中就常采用由 SDXC 构成自愈网。SDXC 可分为 3 种类型，通常简单地表示成 SDXC 4/4 (该类型设备仅提供高阶通道 (VC-4) 的交叉连接)、SDXC 4/1 (该类型设备仅提供低阶通道 (VC-12、VC-3) 的交叉连接) 和 SDXC 4/4/1 (该类型设备可提供高阶通道 (VC-4) 和低阶通道 (VC-12、VC-3) 两种交叉连接)。

## 3.2 传输网网管

### 3.2.1 传输网网管概念

传输网管就是借助计算技术对传输设备的运行进行管理，最初建立 PDH 网管时，就是基于这样一种对网管的认识。当时，系统功能相对简单，仅仅处理端机告警、保护倒换和告警的人工应答，网管低层平台也只要基于 PC 的 DOS 操作系统即可。实体之间的通信使用三层协议，网元实体内部由 8 位单片微处理器通过内部总线完成信息收集、处理，并使用三层通信协议实现对外信息传送，这种使用计算技术实现网元设备自动管理与 FDM 传输系统的半自动管理相比已经是一大进步。此外，由于整体网络简单、业务单一，传输网络的调度配置和改造也只需借助人工对网络资料进行处理即可完成。网络、业务和网管机理的简单也使得传输网管停留在对设备运行状态实施监视这一狭义网管概念上。

SONET/SDH 的出现和计算技术的飞速发展基于 TDM 传送网的传送时

隙和管理开销处理打开了广阔而灵活的空间,此时的传送系统不仅提供设备运行状态监视,还提供时隙交叉、路由配置、保护方式配置和性能监测等功能,传输网也变得灵活、高效和可靠,伴随而来的电信业务也经历了前所未有的飞速发展。

### 3.2.2 典型传输网网管分级

一个典型的传输网网络管理等级有三层,从上至下为网络管理层、网元管理层(EM)和网元层(NE)。当然这里网络管理层仅仅是从网络角度看到的最高管理层,若从服务和商务角度看,则上面还应有服务管理层和商务管理层两层,这里就不详细介绍了。至于网络管理层也可以根据需要进一步划分为子网管理层和网络管理层,原则上前者负责各个地区范围的网管,而后者通过各个子网管理系统来管理全网。至于像 DXC 恢复之类的管理尽管征层次上可以归于子网管理层、但因涉及全网统一行动,管辖的实际是全网。

#### 1. 网络管理层

网络管理层负责对所辖网络进行集中式或分布式控制管理;例如电路指配、网络监视和网络分析统计等功能可以实现集中控制,而维护、告警处理和保护等功能则可以分配给地区性网管理中心来控制。

#### 2. 网元管理层

网元管理直接控制设备,其管理控制功能由网络管理层分配。诸如保护规划、告警过滤、协议转换等。主要目标是减少直接流进网络管理系统的信息流,防止其过载,同时也尽量减少网络响应时间。

#### 3. 网元

网元本身一般也具有此一管理功能。特别是在分布式管理系统、网络管理系统,可能将很多管理功能经软件下载给网元,使网元具有强的管理功能。此时,网络对各种事件的反应十分迅速、特别是用于保护目的的通道恢复可以实时地完成。使传送业务不受影响。

### 3.2.3 传输网设备管理系统功能分析

按照ITU-T建议中对电信管理网的功能域方面的规定,对传输网设备的网管应从配置管理、告警管理、性能管理和安全管理等四个方面入手。

- 配置管理在网管系统里是一个较为重要的方面,他涉及网元各项参数的设置,包括对网络单元的控制识别和数据交换。以及物理位置参数、设备规格的编辑管理。
- 故障管理指能够对不正常的网络运行状况或环境条件进行检测、隔离、校正等一系列功能。这是 SDH 网管中相当重要和最常用的系列功能。各厂家网管



对故障管理各项功能表现形式各不相同，但基本包括以下几方面内容：故障方位显示、故障屏蔽、故障测试、故障过滤、故障设置等。

- 性能管理包括利用 SDH 结构有关的性能基元采集误码性能、缺陷和监视项目数据，15 分钟、24 小时性能监视，历史数据寄存和纪录等。它是考核系统运行正常与否的重要指标之一。目前各厂家的 SDH 网管基本上是根据 ITU 建议的几个性能参数进行监测。

- 安全管理是保护系统安全运行的重要手段。一般系统会给操作员分配不同的等级，根据不同的等级安排可管理的内容。

## 第四章 Tetra-X 设备网络管理系统

### 4.1 网络环境

2M 数字专线网安全可靠，业务内容由用户决定，传输速率有保障，并且目前专线价格大幅度下调，市场需求大幅度增长，但其对资源缺乏统一的管理，资源调配困难，接入设备品牌和型号太多，管理复杂，跨厂商和跨环的人工转接多，故障率高，缺乏端到端的统一管理和测试手段，需要大量的人工配合测试，故障排除困难。

基于以上 2M 数字专线网现状，北京宽广电信公司提出了以 SDXC4/4/1 设备为核心，以 SDH 传输网络作为基础平台，以光纤和铜线作为接入手段，通过统一的网络管理平台 and 业务平台，为运营商提供易于管理、维护和运营的 2M 专线的端到端的解决方案（CELL 系统）。

CELL 系统共分为三个层次：核心层、汇接层、接入层。

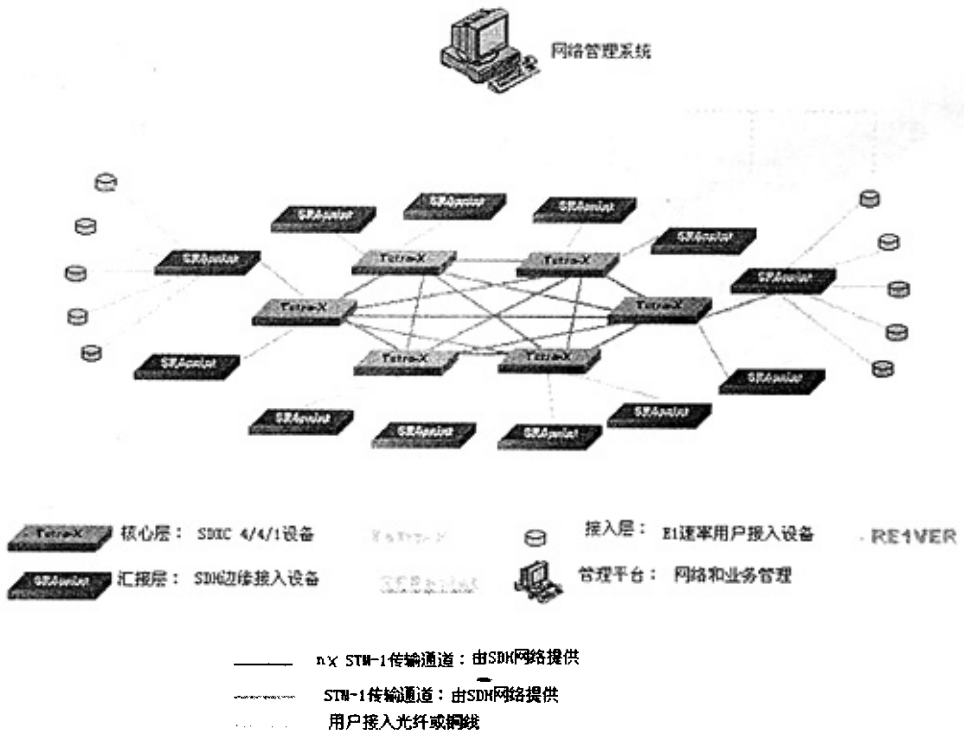


图 4-1 CELL 系统组成

- 核心层: SDXC 4/4/1 设备 - Tetra-X, 128 个 STM-1 端口, 端口间无阻塞的 VC-12 交叉连接, 64 个 STM-1 端口用于核心节点互联, 64 个 STM-1 端口用于连接汇接节点, 核心节点之间的 STM-1 中继电路按需扩容, 节约资源, 减少初期投资, 降低建设风险。

- 汇接层: 提供 2M 数字专线的局端接入、汇集上传功能, 汇接层设备为 SDH 边缘接入设备 - SEApont, SEApont 通过传输网络提供的 STM-1 通道上连接到核心 Tetra-X, SEApont 通过用户光纤或铜线下连接到用户 2M 接入设备。

- 接入层: E1 速率用户接入设备 - REIVER(FibeREIVER - 光纤线路接口, CoppeREIVER - 用户铜线接口)。

## 4.2 网络管理系统的引入

CELL NMS 就是上面提到的 CELL 系统的网络管理系统, 作为宽广电信开发的 2M 专线网的管理系统, 目标是实现对整个 CELL 系统的管理。此项目目前只实现了对 Tetra-X 设备和 SEApont 设备的管理, 并且对 Tetra-X 设备和 SEApont 设备的管理还是相对独立的, 在逻辑上和业务上都没有进行整合。对于 Tetra-X 设备和 SEApont 设备的管理基本相似, 因此本文后面只谈论了 Tetra-X 设备管理系统的设计与实现。

网络管理系统采用的是集中网络管理, 可以使用统一的网络管理系统对传输网中的 Tetra-X 设备和其他 SDH 网元进行集中管理, 集中式的网络管理可以提供以下功能:

- 远端配置

减少运行投入, 缩短工作完成之间的时间。

- 带宽管理

可以在网络中的多个 Tetra-X 设备上插入和抽取, 提高网络的带宽利用率。

- 基于数字交叉连接的网络恢复

为最大限度地减少网络故障造成的损失, 网络恢复的时间应尽可能的短。而对于主要的网络故障, 基于数字交叉连接的网络恢复是一种非常高效的方式。例如, 如果线缆被切断, 基于数字交叉连接的网络将可以在几秒钟到几分钟之间恢复业务, 时间的长短主要取决于网络中用于保护的空闲电路的数量以及网络的自动化程度。

- 测试

Tetra-X 设备所具有的测试能力可以有效地隔离网络故障, 缩短维修时间。使用 Tetra-X 设备的桥接功能可以将任意传输端口的信号连接到外部设备进行

测试，无论是正要投入使用还是正承载业务。SEApont 设备所具有的测试能力可以有效地隔离网络故障，缩短维修时间。

#### ■网络状态监视

在集中管理点上，可以集中监测网络中的告警和管理信息。网络中心的管理人员可以根据这些信息作出正确的决定并执行相应操作。

### 4.3 Tetra-X 设备简介

#### 4.3.1 Tetra-X 设备技术特点

Tetra-X 为核心层的 SDXC 4/4/1 数字交叉连接设备。该设备提供 128 个 STM-1 等效容量，即同时提供对 VC-4 和 VC-12 进行交叉连接的能力。Tetra-X 属于一种中等规模的 SDXC 4/4/1，主要提供在 SDH 环境中的灵活带宽管理能力。Tetra-X 设备提供各种传输接口和对 VC-12 的交叉连接能力。Tetra-X 设备提供 VC-4、VC-12 业务流量的汇聚疏导能力和网络恢复能力。

Tetra-X 设备具有灵活的物理结构，高可靠的设计，稳定的运行表现，强大的软硬件系统，并能够平稳有效的扩容。应用 Tetra-X 设备，可以简化网络结构，快速适应网络变化，提高服务质量，快速调度路由，有效利用网络带宽。Tetra-X 设备可以应用于传输管理、通道监视、测试接入、保护倒换以及网络恢复等方面。

该设备具有如下的基本特点：

- 交叉连接等级为 SDXC 4/4/1；
- 可同时提供基于 AU-4 和 TU-12 的交叉连接；
- 交叉连接容量等效于 128 个 STM-1，阻塞系数为零；
- 提供单向、双向、广播、环回和分离接入等交叉连接；
- 外部提供 STM-1、STM-4 光接口，STM-1 电接口，PDH 139264Kbit/s、34368Kbit/s、2048Kbit/s 接口；
- 设备采取多种冗余保护功能；
- 提供 1+1 复用段保护和子网连接保护功能；
- 提供设备控制器软件在线升级功能；
- 提供强制风冷和温度监测，确保设备稳定运行；
- 提供丰富的告警和故障检测、处理、输出和记录功能；
- 提供多级时钟功能；
- 提供标准 SNMP 网管接口；

#### 4.3.2 Tetra-X 设备交叉连接方式

Tetra-X 设备可以提供如下类型的交叉连接：

- 单向：将任意一个接收端口的 VC-n 信号连接到任意一个发送端口上；
  - 双向：对两个不同传输方向上的 VC-n 信号分别进行连接；
  - 广播式：将任意一个接收端口的 VC-n 信号连接到一个以上的发送端口上；
  - 环回：对某个方向来的 VC-n 信号进行连接，使其沿接收方向环回；
  - 分离接入：终接输入信号中的 VC-n，并在相应输出的 VC-n 上提供测试信号。
- 信号。

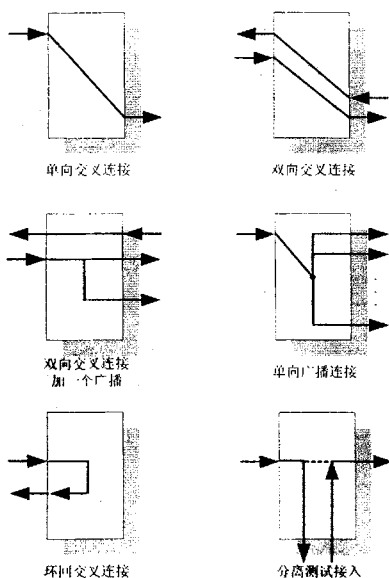


图 4-2 Tetra-X 设备的交叉连接类型

#### 4.3.3 Tetra-X 设备的应用场合

##### 1. 集中、汇聚和疏导

Tetra-X 设备可用于在网络中设置中极点，进行集中调度，将大大减少节点间点对点链路的数量。如图 4-3 所示为使用 Tetra-X 设备进行集中调度的一种应用。

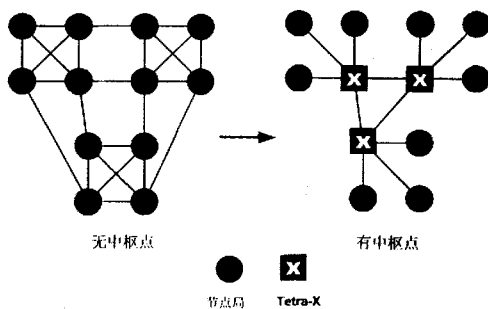


图 4-3 使用 Tetra-X 进行集中调度

如图 4-4 所示，可以使用 Tetra-X 设备进行 SDH 环间电路调度，同样可以大大减少点对点链路的数量。

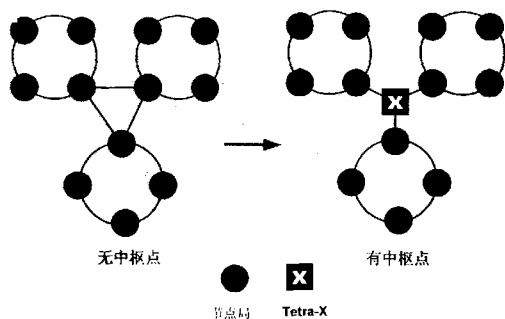


图 4-4 使用 Tetra-X 调度环间电路

使用 Tetra-X 设备建立集中调度中枢, 网络扩展将极为方便。如果是小规模扩展, 只需要将新增加的节点连接到 Tetra-X 设备上即可。如果需要同时扩充多个节点, 则可能需要在网络中增加新的 Tetra-X 设备。无论何种扩容情况, 有 Tetra-X 设备进行集中调度的中枢型网络都将比点对点网络更容易操作维护, 而投入更少。

使用 Tetra-X 设备建立集中调度中枢有以下附加的好处:

- 网络规划更为简单, 对不确定性变化的适应能力大大增强;
- 交叉连接的管理更为容易。

Tetra-X 设备可以大大提高网络的效率, 设备具有对 VC-4 和 VC-12 进行汇聚和疏导的功能。Tetra-X 设备能够将去往同一目的的零散的 VC-4 和 VC-12 集中于两点间的有限链路容量之中, 此种功能称为汇聚, 反方向则称为疏导。Tetra-X 设备的汇聚和疏导功能能够使网络带宽得到充分有效的利用。如 4-5 所示。

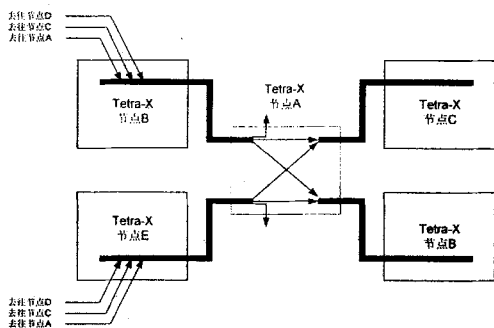


图 4-5 Tetra-X 设备的疏导和汇聚功能

## 2. 替代人工配线

Tetra-X 设备可完全替代人工配线架的所有功能并有以下优点:

- 一旦被连接到 Tetra-X 设备, 信号就可以与其他连接到 Tetra-X 的设备之间进行任意的交叉连接, 不必在配线架上进行手工电路调度;
- 基于计算机控制界面的交叉连接管理;
- 有远端配置能力, 可以根据需要改变交叉连接, 而技术工程师不必在现场;
- Tetra-X 设备比人工配线架占用更少的安装面积。

## 第五章 Tetra-X 设备网管系统客户端软件设计

### 5.1 网络管理系统结构

在网络管理中，一般采用管理者-代理的模型，根据通用的网络管理模型，Tetra-X 设备的网络管理系统结构如下：

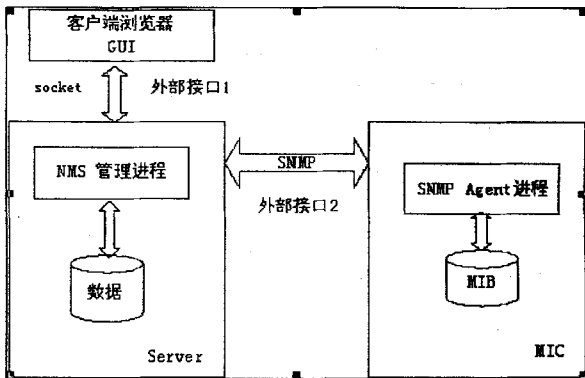


图 5-1 网络管理系统的系统结构

由上图可知此网管系统主要采用三层结构：客户端，服务器，设备。

下面分别对这三层作简要介绍：

#### 1. 客户端

客户端与用户直接进行交互，将设备的状态和配置信息以直观的方式显示给用户，并接受从用户发来的对设备的操作命令传送给服务器。客户端和服务端之间的通信采用 socket（网络套接字）方式，客户端从服务器端读取设备的配置和状态信息，并向服务器发送用户的命令。

#### 2. 服务器

服务器作为中间层，主要负责信息的收集和处理，服务器端与设备端采用的是 SNMP 的通信方式，从设备读取信息，并向设备发送命令。服务器端主要完成的是数据库管理，采用 Microsoft SQL Server 7.0。数据库采用面向对象的关系数据库的设计方法，设计数据对象模型、数据对象行为、功能模型、操作描述等。



### 3. 设备

设备的状态和配置信息主要由主控板的 agent 进程进行管理，通过 SNMP 方式提供给服务器。在 Tetra-X 设备内，每一块电路板上均存在一个微处理器，该处理器可以收集本板各端口的线路状态和电路板自身的工作状态，并在面板上以 LED 告警指示灯显示，同时将这些状态向主控板上的主控处理器报告。主控处理器收集各电路板处理器上报的信息，以及时钟、交换板的主备信息等，并将这些信息同时通过内部通信线路发送到告警板，通过管理接口发送到网络管理系统。

## 5.2 客户端软件功能设计

按照网络管理的功能应该有五大功能模块，对于具体的此系统而言，拓扑管理，电路管理显得尤为重要因此在模块划分时将其提炼出来做单独的介绍以下是 CELL NMS 管理系统项目中 Tetra-X 设备的管理系统功能模块结构：

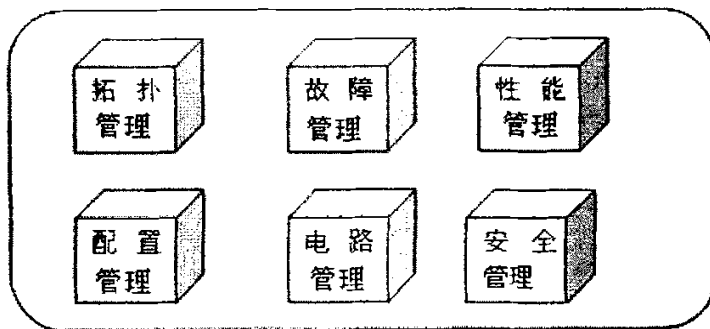


图 5-2 Tetra-X 设备的管理系统功能结构

### 5.2.1 拓扑管理

拓扑包括的元素有：在网络管理系统的界面上代表实际设备的节点（被一图标标识）、代表设备间连接关系的链路。支持任意拓扑结构，两个节点间可存在多条中继线；中继线可以为不同的类型，但无方向，即都是双向。

该模块可以控制节点和中继线的增加和删除，当在网络中增加新的节点设备时，拓扑模块将需要向设备下载有关配置数据。

拓扑管理功能用例图如下所示：

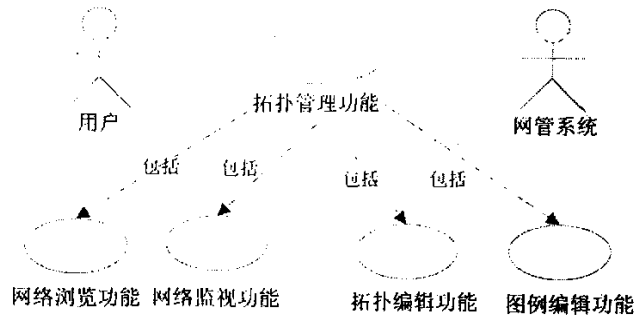


图 5-3 拓扑管理功能

## 1 网络浏览功能

网络拓扑图应能显示专线电路情况，在电子地图的背景上反应专线电路所经过的各主要节点的连接关系。拓扑图的浏览主要又可分为以下几个方面：

- 操作员通过点击节点或中继图标，可获得该节点或中继详细配置信息、故障信息和其它管理功能；
- 拓扑图的背景地图可以定制，拓扑图可以放大和缩小，并且能上下、左右移动；
- 当同时存在显示不同内容的多个窗口时，只有一个激活窗口接受用户的操作和输入，激活窗口的标题栏以高亮度显示；
- 系统在菜单中按照打开的先后顺序列出所有窗口，用户可从菜单中直接激活某个窗口；
- 系统保证窗口显示内容的一致性，当多个用户同时操作系统的相同对象时，不同用户看到的窗口显示内容相同。

## 2 网络监视功能

网络拓扑能够动态、实时显示专线网的运行状态和状况，包括：节点/中继告警状态，告警以可视形式提醒维护人员，当有告警时，节点会根据不同的告警级别显示不同的颜色。如图 5-4 所示。

- 红色表示立即维护告警（主要告警）；

立即维护告警或主要告警是需要维护人员立即处理的紧急告警，影响业务的故障都将导致设备发出立即维护告警。

- 橙色表示延迟维护告警（次要告警）；

延时维护告警或次要告警是可延迟处理的非紧急告警。

以下故障中的一种或者组合将导致设备发出延迟维护告警：

- a). 导致设备性能下降，但不影响设备的正常运行的故障；
  - b). 导致设备进行保护切换的故障。
- 黄色表示维护提示

指示有新的维护信息产生。操作维护信息的详细内容只在控制终端或者网络管理系统的界面上显示，并可按日志查询和打印。

- 蓝色表示设备失连

指示该设备和网管系统失去联系，网管对该设备失去控制。

- 灰色表示设备没有告警



图 5-4 不同的告警状态

### 3 拓扑编辑功能

在拓扑显示区可以根据实际的网络配置来设置和显示网络拓扑结构。网络拓扑的操作主要包括节点管理和中继管理。包括如下功能：

- 手工添加节点/中继到拓扑图上；
- 从拓扑图中去除节点/中继；
- 在拓扑图中手工定义、修改、移动节点/中继位置、名称等；
- 保存当前视图。

### 4 图例编辑功能

用户可通过图例管理功能对图例进行管理，包括：查询各种图例及其颜色的意义。

#### 5.2.2 配置管理

设备配置指的是设备的系统级、电路板级、端口级的可更改的物理属性。操作员可以通过网管系统更改这些属性。

配置管理的基本功能：

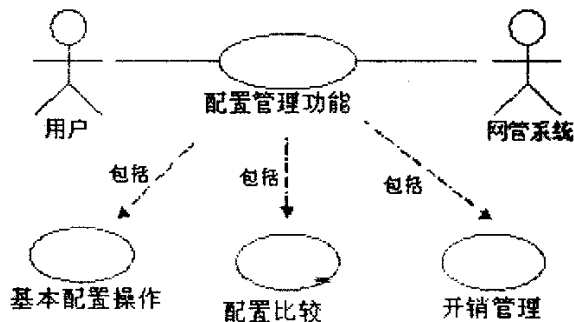


图 5-5 配置管理功能

## 1 基本配置操作

操作节点：

- 查询节点配置，状态；
- 配置节点；
- 查询节点的告警信息。

操作电路板：

- 查询电路板配置，状态；
- 设置接口板。

操作 E1 端口：

- 查询 E1 端口配置，状态；
- 查询 E1 端口的详细告警信息；
- 配置 E1 端口。

操作 STM1 端口：

- 查询 STM1 端口配置，状态；
- 查询 STM1 端口的详细告警信息；
- 配置 STM1 端口。

查询中继线：

- 查询中继配置；
- 配置中继。

网管软件启动时初始化界面：

- 从服务器处获得所有的配置状态数据。

## 2 配置比较

在一定的情况下，可能发生网管系统保存的配置和设备那保存的配置不同的情况。通过比较配置的功能，可以获知二者是否相同。

在比较配置的对话框中，可以进行以下内容的比较：

- 单节点的系统配置；
- 单端口的配置；
- 单节点内所有端口的配置。

## 3 开销管理

SDH 系统的一个重要特点是帧结构中具有丰富的开销比特，包括段开销（SOH）和通道开销（POH）等，用于监控设备的告警和性能，进行设备配置、倒换、公务联络等。

通过网管系统可以查看和配置以下的开销字节内容：

- 高阶通道信号标记字节 C2: 用来指示 VC 帧的复接结构和信息净负荷的性质。

- 再生段踪迹字节 J0: 该字节被用来重复地发送段接入点标识符, 以便使接收端能据此确认与指定的发送端处于持续连接状态。在同一个运营者的网络内, 该字节可为任意字符, 而在不同两个运营者的网络边界处, 要使设备收发两端的 J0 字节相匹配。通过 J0 字节, 可使运营者提前发现和解决故障, 缩短网络恢复时间。

- 高阶通道踪迹字节 J1: 该字节的作用与 J0 字节类似, 被用来重复发送高阶通道接入点标识符, 使该通道接收端能据此确认与指定的发送端处于持续连接。收发两端 J1 字节相匹配可认为该通道处于持续连接状态。J1 字节可按需要进行设置和更改。

Tetra-X设备的处理方式:

- 线路发送方向: 可设置 C2 的内容; 可以设置发送的再生端踪迹内容; 可设置高阶通道踪迹识别符为 16 字节或者 64 字节方式, 并设置高阶通道踪迹识别符的内容;

- 线路接收方向: 可设置期望收到的 C2 的内容, 并将收到的内容和期望内容进行比较, 当二者不一致时, 发出高阶通道信号标记失配告警。可以设置期望收到的再生端踪迹内容, 当收到的再生端踪迹内容和期望不符时, 产生再生端踪迹识别符失配告警; 可设置高阶通道踪迹识别符为 16 字节或者 64 字节方式, 并设置期望收到的高阶通道踪迹内容, 当收到的高阶通道踪迹内容与期望内容不一致时, 产生高阶通道踪迹识别符失配告警。在实际配置中, 应使收发端保持一致。

#### 4 用户操作记录功能

配置系统的安全性是整个网络管理系统安全的核心, 因此, 必须对用户进行的每一配置操作进行记录。在配置管理中, 需要对用户操作进行记录, 并保存下来。管理人员可以随时查看特定用户在特定时间内进行的特定的操作。操作记录的写入在服务器端完成。客户端只能进行查询操作。

##### 5.2.3 故障管理

故障管理功能用例图如下所示。

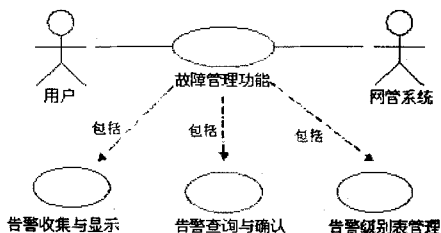


图 5-6 故障管理功能

### 1 告警收集与显示

网管系统能对告警进行实时监视，并在网络拓扑图上将相应的告警信息清晰直观地显示出来。

- 在拓扑图上使用不同的颜色表示不同级别的告警(在上面的拓扑模块得网络监视功能中已详细介绍过)。
- 采用多层图形、逐层激活的方式，实时显示当前告警位置：对于界面系统不可能将可视的元素过分细化，因此在拓扑区只能看到节点和中继，当故障发生时，可以点开节点看机架图，再进一步点开机架图上的端口可查看端口的状态。
- 对同一网络资源，当有多个告警发生时，图标的颜色应与当前最高级别的告警相对应。
- 当较高级别告警清除后，再顺序显示次等级告警的对应颜色。
- 对于当前告警和历史告警，用户可以指定查询条件进行查询，查询条件包括告警对象（单选或多选）、时间范围、告警原因、告警级别、告警类型、告警是否确认，告警是否清除等。

### 2 告警查询与确认

网管系统提供了对当前告警或者历史告警的查询和统计功能，并以表格的方式显示查询和统计结果。查询或统计的条件为以下信息或以下信息的任意‘与’/‘或’组合：

- 标识（节点号，端口号，VC 编号等）
- 告警发生时间
- 告警结束时间
- 告警严重等级
- 告警原因
- 告警状态
- 告警确认时间

- 确认用户

网管系统支持如下告警查询/统计报告的输出方式:

- 打印机打印;
- 保存为一个 Excel 文件。

网管系统还提供了告警确认功能,支持操作用户对所有接收到的告警进行单条或批量确认。未经确认的告警保留对用户的提示,直到用户进行确认。

### 3 告警级别表管理

网管系统提供了对接收到的告警级别进行设置的功能,通过对告警级别表的设置,用户可以根据实际情况灵活地改变告警的级别。当要上报告警时,首先查询与之相关联的告警级别表中相应告警类型的级别有没有设置,如果有设置,则使用告警级别表中指定的级别;若没有设置,则使用原有告警中的级别。

#### 5.2.4 电路管理

Tetra-X 的主要功能是向最终用户提供 E1 速率专线。所以电路管理是核心功能。经过多个设备向用户提供的端到端的电路(Circuit)是由这些设备内部的交叉连接(connection)和连接这些设备的中继线上的子速率链路(link)构成。即:电路(Circuit)=多个链路(link)+多个设备内部的交叉连接(connection)。

Tetra-X 设备的交叉连接矩阵具有全交叉、无阻塞的功能特点,其交叉连接容量等效于 128 个 STM-1。

交叉连接有以下 3 种基本类型:

1. 点对点的单向连接;
2. 点对点的双向连接;
3. 一点对多点的单向连接;

每个点只能存在一条以它为目的的连接,所以多点对一点连接和一点对多点的双向连接都是不允许的。

STM-1 端口上目前可以建立 3 种带宽的连接: VC-4、VC-3、VC-12。

电路管理功能用例图如下图所示。

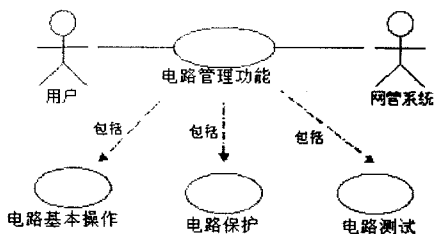


图 5-7 电路管理功能

### 1 电路基本操作

#### ■ 建立电路：建立电路的 2 个步骤

1. 在数据库中生成电路数据——这是一个在数据库中建立电路数据的过程，此时，在网络中并没有实际建立电路。
2. 激活电路——使电路在网络中生效。此时，下面 2 种情况下，还应选择路由：

- 1) 是跨节点电路，但路由信息不存在；
- 2) 电路受保护，但保护电路不存在；

#### ■ 拆除电路的 2 个步骤

1. 关闭电路——在网络中拆除电路，用户可以选择是否需要保留路由信息；
2. 在数据库中删除电路数据——在数据库中彻底删除电路的相关信息（基本信息和路由信息）；

#### 分成 2 个步骤的目的：

1. 方便操作需要频繁断开、接通的电路（例如，用户只想在某一段时间内开通电路）。这可以通过下面的过程来实现：
  - a) 要接通时，建立并激活电路；
  - b) 不要接通时，关闭电路，且保留路由信息；
 这样，不必每次建立电路时，都需要输入电路的信息（例如，用户信息、源端、目的端等），因为这些信息在第一次接通电路时，就已经保存在数据库里了。
2. 方便重新选择路由。例如，当监测到某个端口出现故障时，需要为该端口的所有电路选择其他路由，此时可以进行如下操作：
  - a) 关闭电路，且不保存路由信息；
  - b) 激活电路，网管可以自动选择其他的路由；
3. 方便预先配置电路数据，然后批量激活；



目前的做法：为了使功能尽可能地简单（减少用户操作时的参数），关闭电路时，不提供是否保存路由信息的选择。但将来可以扩充该功能。

- 修改和查询电路信息：用户可以修改电路的基本信息和保护路由信息，并可以设置查询条件进行查询。

## 2 电路保护

理论上，保护路由应经过不在工作路由上的节点，或者至少经过不同的中继线。但实际中，在某些情况下，这种要求可能很难满足，例如，图 5-8 的所示的拓扑图就是如此。图中，一条边就表示一条中继线。

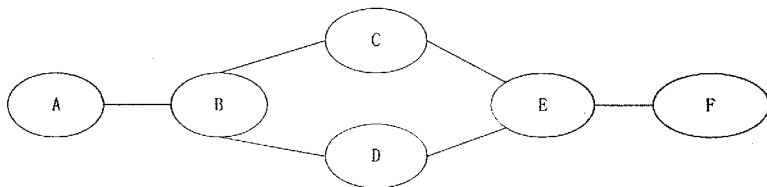


图 5-8 工作路由和保护路由对不同节点数的要求

图 5-8 中，A-F 之间 1 条电路的工作路由为 A-B-C-E-F，它的保护路由有 2 种：

- 1) 方法 1：为 A-B-D-E-F，此时，保护切换发生在 A、F；
- 2) 方法 2：为 A-B-D-E，此时，保护切换发生在 B、E；

目前，为了简化设计，只实现方法 1 的保护，即只实现保护切换发生在源端、目的端的保护。

- 工作路由和保护路由对不同节点数的要求可以是下面之一：

要求 1：除源和目的端的节点外，其他节点都不相同；

要求 2：除源和目的端的节点外，至少要有一个节点不相同；

建议选择要求 2，否则，当出现图 5-8 的情况时，就无法建立保护路由了。

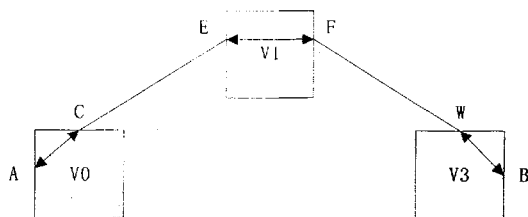
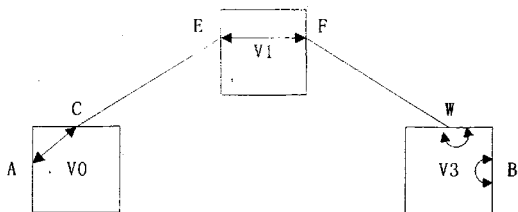
- 工作路由和保护路由对不同中继线的要求

当工作路由和保护路由经过了相同的节点（源和目的端的节点外），此时，应尽可能选择不同的中继线，如果只有一条中继线，就使用同一条中继线。

## 3 电路测试

环回测试的连接必须是双向连接。环回的连接禁止保护切换。如果对受保护的连接进行测试，则 NMS 发送的测试点必须是电路的 2 个端点之一，或者是中间的连接点。

- 对无保护的连接

图 5-9 无测试的、不受保护的  $A \leftrightarrow B$  连接图 5-10 测试的、不受保护  $A \leftrightarrow B$  连接

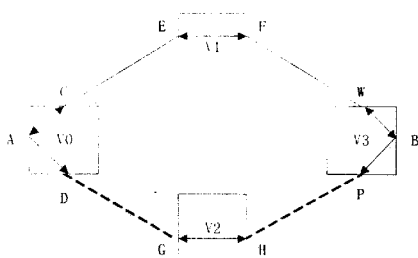
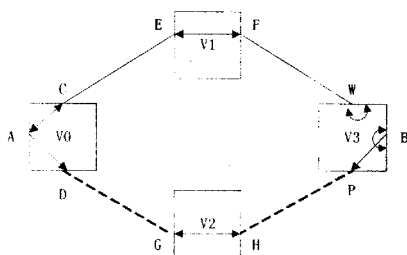
从图 5-9 进入图 5-10 的过程中, 发生的事情如下, 各模块可见的交叉连接信息见表 5-1:

- 1) NMS 设置 B 点测试;
- 2) MIC 拆除  $W \leftrightarrow B$  的连接, 建立  $W \rightarrow W, B \rightarrow B$  的连接;
- 3) MIC 设置 W、B 点为测试状态;

表 5-1 两种情况下, 各模块可见的交叉连接信息

| 模块  | 无测试时, 显示的交叉连接   | 测试时, 显示的交叉连接   |
|-----|---|--|
| 交换阵 | $A \leftrightarrow C, E \leftrightarrow F, W \leftrightarrow B$ | $A \leftrightarrow C, E \leftrightarrow F, W \rightarrow W, B \rightarrow B$ |
| MIB | 1) 同上;<br>2) W、B 无测试;   | 1) 同左;<br>2) W、B 测试;   |
| NMS | 显示为 $A \leftrightarrow B$ 的连接, 无测试                              | 显示为 $A \leftrightarrow B$ 的连接, V3 节点在测试                                      |

- 对受保护的连接: 工作通道

图 5-11 无测试的, 工作通道的  $A \leftrightarrow B$  连接图 5-12 测试的, 工作通道的  $A \leftrightarrow B$  连接

从图 5-11 进入图 5-12 的过程中, 发生的事情如下, 各模块可见的交叉连接信息见表 5-2。

表 5-2 两种情况下, 各模块可见的交叉连接信息

| 模块  | 无测试时, 显示的交叉连接  | 测试时, 显示的交叉连接   |
|-----|--|--|
| 交换阵 | 1) $A \leftrightarrow C$ , $E \leftrightarrow F$ , $W \leftrightarrow B$ ;<br>2) $A \rightarrow D$ , $G \leftrightarrow H$ , $B \rightarrow P$ ; | 1) $A \leftrightarrow C$ , $E \leftrightarrow F$ , $W \rightarrow W$ , $B \rightarrow B$ ;<br>2) 同左; |
| MIB | 1) 同上;<br>2) $W$ 、 $B$ 无测试;<br>3) $A$ 、 $B$ 受保护;   | 1) 同左;<br>2) $W$ 、 $B$ 测试;<br>3) 同左;   |
| NMS | $A \leftrightarrow B$ , 无测试, 处于工作通道  | $A \leftrightarrow B$ , $V3$ 节点测试, 处于工作通道  |

- 对受保护的连接: 保护通道

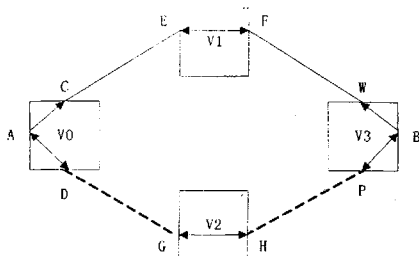


图 5-13 无测试的、保护通道的 A ↔ B 连接

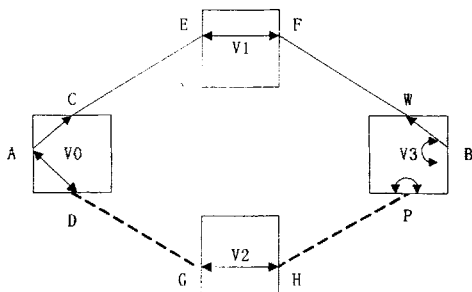


图 5-14 测试的、保护通道的 A ↔ B 连接

从图 5-13 进入图 5-14 的过程中，发生的事情为：

- 1) NMS 设置 B 点测试；（如果在 V0 测试，则测试点必须是 A）；
- 2) MIC 拆除 B ↔ P 的连接，建立 B → B，P → P 的连接；
- 3) MIC 设置 W、B 点为测试状态；

这 2 种情况下，各模块的交叉连接信息不再详细说明。

### 5.2.5 性能管理

设备性能数据指的是体现设备端口信号质量的参数，操作员通过网管系统，可以查看这些数据。

性能分析主要是对当前采集的性能数据和历史性能数据进行处理而评估 SDH 系统及网元的性能水平，这对于是否开始维护行动和故障报告是非常有用的。为了便于性能分析，性能数据需要向网管操作系统进行报告。性能数据的报告可分为 3 种方式。第一种方式是指令报告，第二种方式是周期性报告，第三种方式是自动报告。所谓指令报告就是根据网管系统的需要，操作系统发指令，网元中的性能数据便通过操作系统 / 网元接口进行报告。所谓周期性报告

就是网元的性能数据周期性地向操作系统报告,对于某些特定端口的性能数据也可按操作系统的指令进行周期性的报告,这对于及时进行性能趋势分析、预测将来可能发生的故障非常有用。所谓自动报告就是性能事件门限突破后,性能数据自动地经操作系统/网元接口报告给操作系统。这对于及时了解 SDH 系统及网元的性能情况和是否采取维护行动非常必要。端口的性能监测数据包括再生段、复用段、高阶通道段和指针调整的数据。

性能管理功能用例图如下图所示。

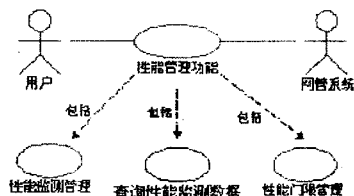


图 5-15 性能管理功能

### 1 性能监测管理

性能监测管理完成如下功能:

- 性能监测复位: 为使设备和网管系统的时刻保持一致,在进行性能监测前,需要首先进行监测复位。

- 提供实时监测的性能曲线及数值,性能数据的统计周期为 15 分钟,开始监测后,则每隔 15 分钟,设备报告一次性能数据,数据显示在对话框下方的表格中,同时在上方的曲线图中显示,曲线图中超过阈值的数据以红色显示,低于阈值的数据以绿色显示,阈值以蓝色显示。

- 性能监视使能: 选中该选择项,表示允许设备向网管系统发送性能数据,否则为不允许。

### 2 查询性能监测数据

- 端口性能数据的查询: 性能数据查询的时间间隔为  $n \times 15$  分钟。
- 端口性能数据的累积查询: 查询一段时间内的性能数据累积结果。

### 3 性能门限管理

在对话框中,可以对再生段、复用段、高阶通道段和指针调整事件的性能数据设置阈值。

### 5.2.6 安全管理

此系统中提供的安全管理主要实现了操作员管理和功能组管理。

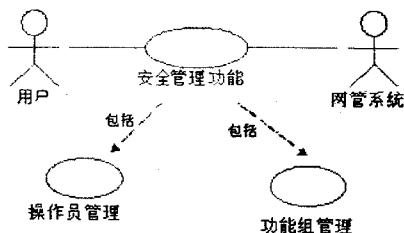


图 5-16 安全管理功能

#### 1 操作员管理

NMS 中的操作员指的是接入网络管理系统的管理者，他们通过浏览器，在一定的权限范围内配置和监视被管设备。

对操作员的管理包括如下功能：

- 登录/退出管理：此功能用于验证操作员的身份，没有登陆成功的操作员不能执行对设备的操作，只能查看设备状态。登陆成功的操作员可以根据操作员的级别对设备进行符合他级别的操作。
- 增加操/删除操作员：工号在合法范围内的操作员可以增加新的操作员和删除废弃的操作员。
- 锁定解锁操作员：此功能用于锁定/解锁特定的操作员。操作员被锁定后，不能登录。除非由权限高的操作员解锁。
- 修改操作员：此功能用于修改操作员的信息。在 GUI 上单独提供了一个供任何操作员修改自己口令的界面。
- 查询操作员：此功能用于按照查询条件，查询有关操作员的所有信息。

系统为了防止所有的操作员都过期；删除了最后一个高级操作员两种情况。在建立操作员数据库表时，自动创建一个操作员（ID="btcroot"，密码="tetraroot"，有效期为尽可能的长（如 2099-12-31），功能组为 0）。禁止删除该操作员。禁止修改其有效期和功能组。

#### 2 功能组管理

网管系统中的“功能组”类似于 Windows 操作系统中的“用户组”，不同的功能组具有不同的操作权限。每个网管操作员都隶属于某功能组，同一功能组中的所有操作员具有相同的操作权限。

对操作员的管理包括如下功能：

- 功能组的增加/删除：工号在合法范围内的操作员可以增加新的功能组，删除废弃的功能组。
- 修改功能组：可以修改功能组的以下信息：组名、描述、权限。网管系统规定编号“0~9”为内置功能组编号区域。这些功能组均不能被删除，也不能修改它们的操作权限。
- 查询功能组：网管系统支持操作员的精确查询和全查询功能。
- 查询功能组包含的成员：此功能用于查询隶属于指定功能组的所有操作员信息。

### 5.3 客户端软件程序实现

#### 5.3.1 客户端软件程序框架

客户端的每个功能模块在实现时都采用三层的程序结构：用户接口，结构体，通信接口。

这里对这3个模块做简要介绍，后面将会对三个模块做较为详细的阐述。

- 用户接口模块。该模块提供用户操作界面，响应用户的有关操作。
- 结构体模块。该模块完成上层接口模块与底层通信模块之间的数据和消息的传递。
- 底层通信模块。该模块通过网络套接字 socket 实现客户端与服务器端的通信。它一方面，获得服务器传来的数据；另一方面，向服务器发送设备配置数据。

三者之间的信息处理过程如下：

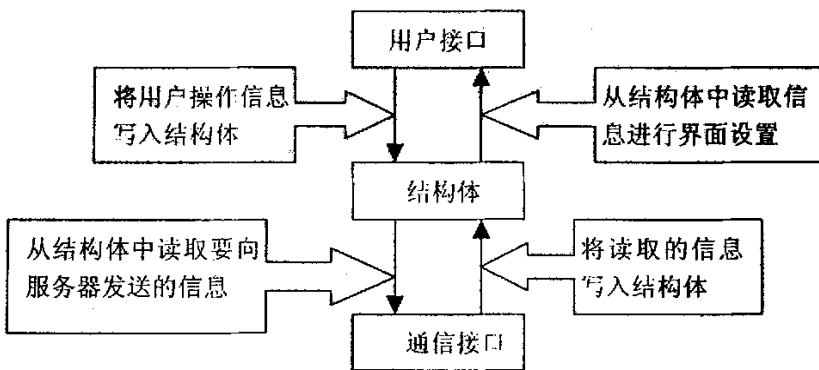


图 5-17 客户端软件框架

#### 5.3.2 用户接口

用户接口直接与用户打交道，属于界面窗口设计，对于这样一个复杂的网络管理系统，它包括性能管理、配置管理、故障管理、安全管理等诸多方面，如何把这些管理信息以图形化的方式直观的呈现给用户，并且，使用户能够方

便快捷地完成一系列操作成为界面实现的关键。

界面设计一般要遵循以下交互性原则：

(1) 用户原则。人机界面设计首先要确立用户类型。划分类型可以从不同的角度，视实际情况而定。确定类型后要针对其特点预测他们对不同界面的反应。这就要从多方面设计分析。

(2) 信息最小量原则。人机界面设计要尽量减少用户记忆负担，采用有助于记忆的设计方案。

(3) 帮助和提示原则。要对用户的操作命令作出反应，帮助用户处理问题。系统要设计有恢复出错现场的能力，在系统内部处理工作要有提示，尽量把主动权让给用户。

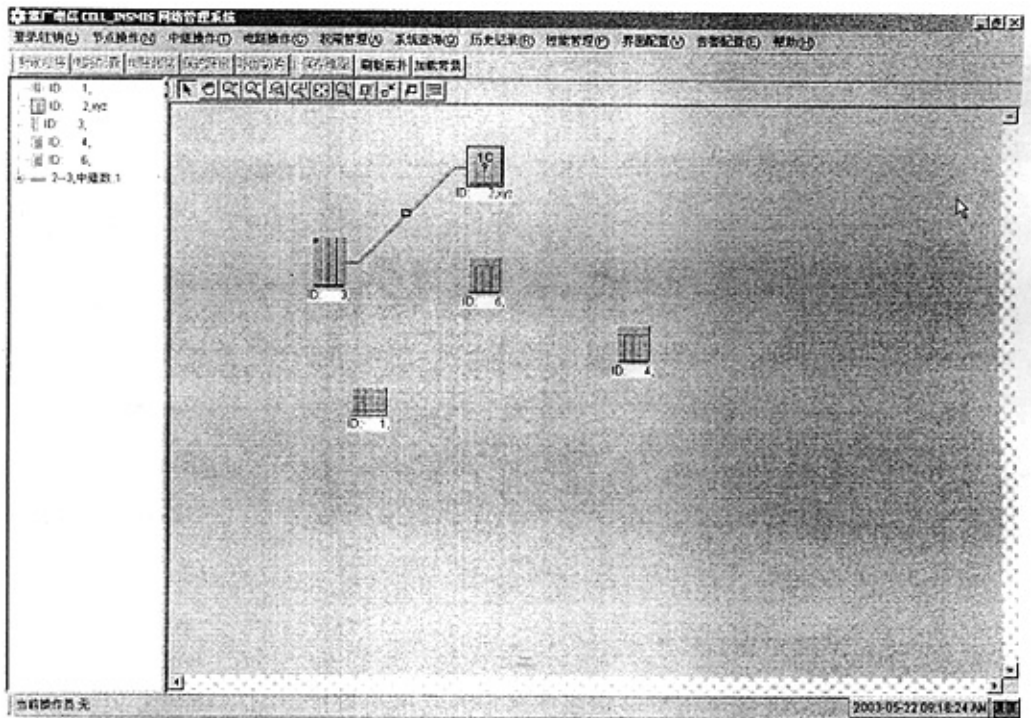
针对以上原则，我们在界面接口实现时作了以下工作：

1. 用户原则：

CELL NMS 的用户使用群体为网络管理人员，从事的是专业的网络管理工作，因此屏幕和窗口设计要尽量做到简单明确，决不能过分的修饰。

在屏幕颜色的选择上我们采用的主要基调是灰色，给人以稳重大方的感觉，画面应对称，显示命令、对话及提示行在系统的设计中统一规范。

主界面系统如图所示：





## 2. 信息量最小原则

网络管理系统中数据输入界面往往占终端用户的大部分使用时间，而且很容易出错。这些实现时我们采用了列表选择法。只要能预知答案，尽可能设置默认值，节省用户工作。

屏幕上所有对象，如窗口、按钮、菜单等处理一致化，使对象的动作可预期。如下所示：



## 3. 帮助和提示原则：

随时将当前操作的信息告知用户（尤其是响应时间十分长的情况下，例如网络中的发送配置操作一般要经过比较长的时间，像这种耗时的操作我们都要弹出等待对话框）；在用户操作出错时，可返回并重新开始。对于操作要提示用户成功与否，如果不成功，则给出详细的出错信息。如下图所示：

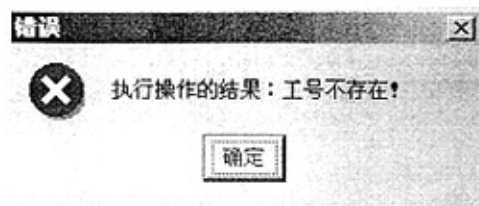


图 5-20 登录失败-操作员不存在

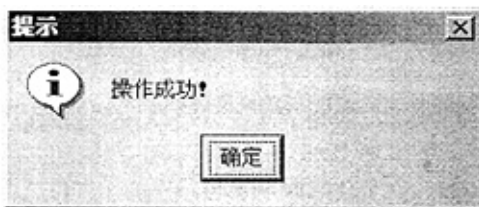


图 5-21 修改配置成功信息

对于关键性操作，要提示用户是否继续，并告知操作可能带来的后果。如下：

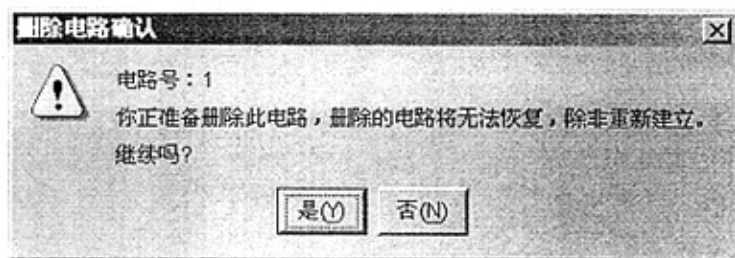


图 5-22 确认删除电路对话框

### 5.3.3 结构体

结构体是位于用户接口和通信接口之间的承载信息的实体，以结构体的方式将各个模块的故障信息、配置信息等封装在一个类中作为私有变量，这样设计体现了面向对象程序设计的优点。

结构体被用户接口模块的调用发生在以下两个地方：

- 界面有数据信息需要传递给服务器，界面程序会将其配置、状态等信息在其相应的结构体中以规定的格式写入结构体。
- 当界面需要从服务器获取信息时，界面程序会从相应的结构体中，以规定好的格式和顺序将数据读出并设置。

结构体对底层通信模块的调用发生在以下两个地方：

- 当通信函数被调用，需要向服务器端发送数据信息时，通信函数会按照规定从相应的结构体中以规定好的格式和顺序读取信息并发送给服务器。
- 当服务器端有信息需要读入时，通信函数会把读入的信息放入相应的结构体中。

### 5.3.4 通信接口

通信接口负责处理客户端和服务端之间的数据传输，客户端与服务端相互之间的通信采用的是 Socket 通信方式。网络套接字（socket）提供了网络上的两个程序之间交互通信的可靠连接，通常的网络通信的模型是多客户/单服务器方式。java.net 程序包提供了 Socket 类实现 java 与其他程序在网络上的通信。socket 类实现了客户端功能。如果要实现服务器，就要用到 ServerSocket 类。Socket 通信过程如下：

- 1) 建立 Socket 连接
- 2) 获得输入/输出流
- 3) 读/写数据
- 4) 关闭输入/输出流
- 5) 关闭 Socket

作为网络管理系统，对于故障的敏感度应该很高，当设备发生故障时应该及时地通知给网络管理人员，以便及时解决。因此使用 Socket 通信需开辟了两条路径，即两个端口，一个用于客户端主动的与服务器交换信息；一个用于服务器及时通知客户端设备的报警信息；对此主程序 MAIN 必须重新开启新的线程用于随时监听告警事件。

客户端的通信机制如下图：

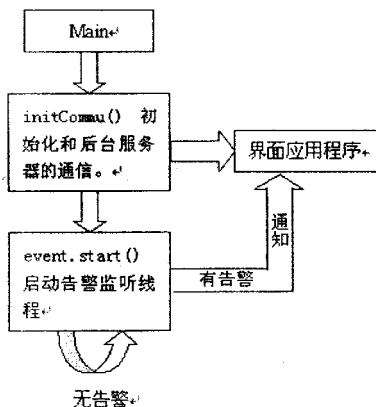


图 5-23 客户端的通信机制

## 5.4 软件实现中问题研究

### 5.4.1 界面操作与通信冲突

客户端的程序主要完成两个功能：上层界面与客户友好交互、下层通信与服务器交换数据，因此存在两层操作发生冲突的情况。当用户向服务器发送命令的时候，通信程序开始启动占用了内存，界面即停止响应不能够及时刷新和接受客户的命令。如果通信过程能够顺利地在短时间内完成，此种冲突影响不大，但一旦通信有一定的延时，客户面对停止响应的界面系统会不知所措，而且此种情况会经常发生，因为很多操作需要服务器再将由客户端发来的命令发送给设备，设备执行完命令后再向服务器报告并由服务器转发给客户端，此一系列操作，无论哪个中间环节出现问题都可能造成界面无限期地等待结果而停止响应。

通过上述阐述，我们可以发现在界面端需要解决的问题主要有两个方面：

1. 如何解决在通信过程中界面短期停止响应的问题。
2. 如何解决界面无限期待操作结果的问题。

#### 问题 1 解决方法和实现

##### ■ 解决方法

对于通信过程中界面停止响应的问题，我们的解决方法是在界面调用通信函数处重新启动一个线程，这样界面程序和通信程序轮流占用内存并行的方式友好的共处，但此时又要面临一个新的问题，即此时如果用户再进行操作，由于数据的传送是在同一端口按照顺序接收和解析的，所以两种命令的两种数据同时发送，会使服务器端无法分辨而产生异常。对于此情况，可在一种操作过程中限制其他操作，有两种方式：

1. 设置信号量。如果有操作在进行，信号量就置位，否则归零。操作进行时监测信号量的情况，如果为零则立即操作，如果不为零则进入等待队列。此种实现方式涉及到队列、等待时限的设置、信号量的监测等一系列问题，实现起来比较麻烦。
2. 在一种通信过程进行时，弹出等待对话框，此对话框设置为模态——即它在消失前不能进行其他操作，此种方式实现起来简单，并且对客户来讲还会有友好的界面。

##### ■ 实现

考虑到实际应用，和实现难度等因素，最终我们选择了第二种方法，具体的实现过程是在某项操作开始时，在通信函数中开始的位置就弹出等待对话框，在函数结束处关闭等待对话框，此时要考虑到通信发生 exception 的情况，

因此在 catch 的时候也要将等待对话框关闭。

对于普通的操作在一切正常的情况下一般在 5000ms 内就可以完成，这么短的时间内没有必要弹出等待对话框，还没看清楚就会消失了，因此对于普通的操作我们一般在操作超出 5000ms 时才弹出等待对话框。对于一次刷新多项状态的操作耗时比较长，因此在操作已开始就弹出等待对话框。

由于每次重新生成和关闭对话框也很耗时，并占用内存十分的不经济，而且会经常用到此对话框，因此我们想到了使用隐藏的方式，即当初始化界面时就生成等待对话框，只是使其处在不显示的状态，即 `setVisible(false)`。当需要调用它的时候只要 `setVisible(true)` 就可以了。在退出主程序时，关闭此对话框。

程序中实现的流程如下：

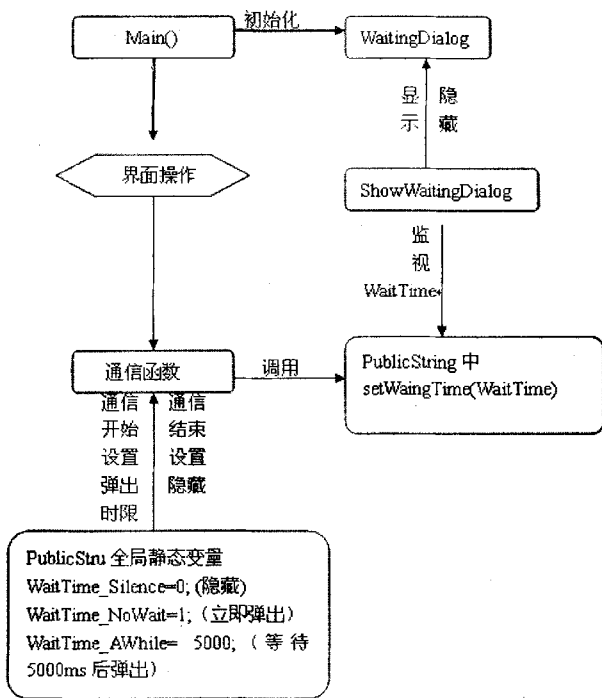


图 5-24 问题 1 解决方案

## 问题 2 解决方法和实现

造成界面无限期等待操作结果的问题的原因有很多，一是通信线路故障，不能及时将信息反馈到客户端；二是服务器故障，没能正确接收或处理客户请

求；三是设备故障，没能及时上报信息。对于服务器端、设备端、服务器和设备之间的通信线路故障，可以由服务器和设备自己解决，出现故障它会向用户报告故障的，而对于客户端和服务器的通信故障就需要客户端对通信时间进行限制。

- 解决方法

对于界面无限期待操作结果的问题，我们的解决方法是设置通信时限，即对每个通信过程限制其最长通信时间，如果超出此时间限制，则自动退出，并通报用户，操作超时。

- 实现

具体的实现过程是 socket 通信一开始根据时限要求通过函数 `socket.setSoTimeout(int)` 来设置中断 socket 通信的时限，如果通信超时，便会产生 `SocketTimeoutException`，通过捕捉到此类 exception 可以向用户报告他的操作超时。

根据操作类型，操作超时的时限可以分成三种情况：

1. 在刷新多项的操作时（例如当刷新节点状态时，同时要刷新的还有电路板和端口状态。），经过测试分析在正常情况下，最长可以在 100000ms 内完成操作。
2. 在发送配置操作时，经过测试分析在正常情况下，最长可以在 300000ms 内完成操作。
3. 除了以上两种情况其他的操作，经过测试分析在正常情况下，最长可以在 20000 ms 内完成操作。

根据以上操作时限，我们只要在公有类 `PublicStru` 里面定义三个静态的全局变量，在使用过程中只要使用这三个变量即可。

程序中实现的流程如下：

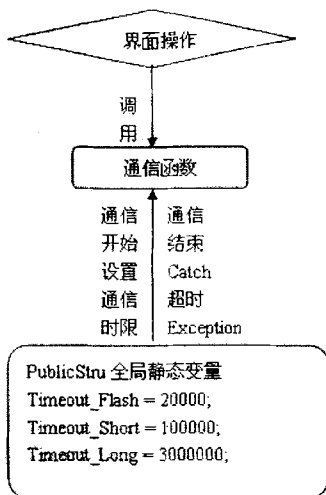


图 5-25 问题 2 解决方案

#### 5.4.2 Socket 通信冲突

前面讲过 socket 通信是通过输入输出流进行信息交互的，并且在解决界面操作与通信冲突的问题的时候我们不难发现有一个漏洞：对于在 5000ms 内可以完成的一般的操作我们在 5000ms 内时不弹出等待对话框的，这样如果在这段时间内，用户进行其他操作，就可能造成输入输出流冲突。

对于这个问题的解决方法有两个：

1. 设置信号量，当要调用时检测通信是否被占用，如果被占用则马上通知用户请稍后再试。
2. 设置信号量，当要调用时检测通信是否被占用，如果被占用则等待一定的时间，在此期间不断检测信号量的状态，如果信号量被释放，则继续进行此操作，如果在等待期间信号量始终被占用，那么当时限到达时，再通知用户请稍后再试。

对于第一种方法省去了检测信号量的麻烦，实现起来非常简单；第二种方法看似难实现，但实际代码只比第一种方法多 5 行左右，但却免去不断弹出请用户请稍后再试对话框的杂乱、用户使用的麻烦，因为实际操作中，只要稍稍等一下，冲突就可以避免，用户不会有太多的时延感觉。综上所述最终选用第

二种方法。

程序的流程图如下：

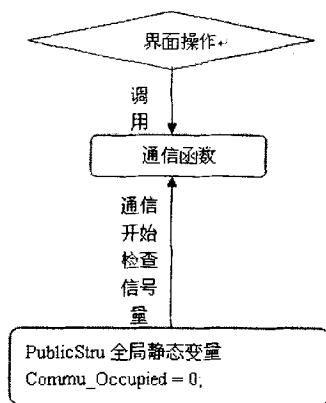


图 5—26 通信冲突解决方案



## 参考文献

- [1] 岑贤道 安常青,《网络管理协议及应用开发》,清华大学出版社,1998, P25-28
- [2] 孟洛明 亓 峰,《现代网络管理技术》,北京邮电大学出版社,1999,P15-P16
- [3] 郭 军,《网络管理与控制技术》,北京邮电大学出版社,1999, P89-P100
- [4] 韦乐平,《光同步数字传输网》,人民邮电出版社,1993, P3-P10
- [5] 李兴明,《SDH 网络管理及其应用》,人民邮电出版社,1999, P10-15

## 附录 A 缩略语

|      |  |          |
|------|--|----------|
| DXC  | Digital Cross-Connect System           | 数字交叉连接设备 |
| IP   | Internet Protocol                      | 互连网协议    |
| ITU  | International Telecommunication Union  | 国际电联     |
| MIB  | Management Information Base            | 管理信息库    |
| MIC  | Microprocessor In Charge               | 主控微处理器   |
| OSI  | Open System Internetworking            | 开放式系统互连  |
| SNMP | Simple Network Management Protocol     | 简单网络管理协议 |
| CMIP | Common Management Information Protocol | 公共管理信息协议 |
| TCP  | Transmission Control Protocol          | 传输控制协议   |
| UDP  | User Datagram Protocol                 | 用户数据报协议  |

## 致 谢

在宽广电信技术研究中心的两年，是我受益匪浅、获益良多的两年，宽广电信技术研究中心教会了我很多东西，给我将来的工作和学习打下了良好的基础。

在中心做了一年多的软件编程，使我在软件开发方面有了长足的进展。通过实际开发学习到了软件开发的流程增长了我在软件开发方面的经验，同时通过通信系统的软件开发设计，也使我对通信系统的概念从书本上应用到实际中，进一步掌握了通信知识。我很高兴，我能在宽广电信公司从事我的毕业设计，这里有优秀的老师和优秀的员工、良好的学习氛围，让我充实地在这里度过了我关键的研究生生涯。

在这里，我要感谢导师雷振明教授，他严谨的治学态度、深湛的学识、诲人不倦的精神和身体力行地努力工作常常激励着我；要感谢李东强和刘新闻老师，他们都在实际的软件开发上不厌其烦地教导过我，使我在实际能力上获得了进步。当然还要感谢实验室的很多其他老师给了我很多帮助。

在这里，要感谢的同学很多。比如王新良、刘辉等。在我困惑的时候，他们给我以启示，帮我解决一个个难题。另外，也得感谢张妹等其他同学的配合。

最后，我得感谢我的朋友和家人，他们给了我关心和支持，让我感觉到了生活的意义和生活的情趣，他们是我坚实的后方。