网络管理与网络维护

网络管理 英文名称：Network Management 定义：监测、控制和记录电信网络资源的性能和使用情况，以使网络有效运行，为用户提供一定质量水平的电信业务。应用学科：通信科技（一级学科）；支撑网络（二级学科）网络管理概念解析　网络管理[1]，是指网络管理员通过网络管理程序对网络上的资源进行集中化管理的操作，包括配置管理、性能和记账管理、问题管理、操作管理和变化管理等。一台设备所支持的管理程度反映了该设备的可管理性及可操作性。　而交换机的管理功能是指交换机如何控制用户访问交换机，以及用户对交换机的可视程度如何。通常，交换机厂商都提供管理软件或满足第三方管理软件远程管理交换机。一般的交换机满足 SNMPMIBI / MIB II 统计管理功能。而复杂一些的交换机会增加通过内置 RMON 组（mini-RMON）来支持 RMON 主动监视功能。有的交换机还允许外接 RMON 探监视可选端口的网络状况。常见的网络管理方式有以下几种：[2]

(1)SNMP 管理技术

(2)RMON 管理技术

(3)基于 WEB 的网络管理

SNMP 是英文“**Simple Network Management Protocol**”的缩写，中文意思是“简单网络管理协议”。SNMP 首先是由 Internet 工程任务组织（Internet Engineering Task Force)(IETF)的研究小组为了解决 Internet 上的路由器管理问题而提出的。

SNMP 是目前最常用的环境管理协议。SNMP 被设计成与协议无关，所以它可以在 IP，IPX，AppleTalk，OSI 以及其他用到的传输协议上被使用。SNMP 是一系列协议组和规范（见下表），它们提供了一种从网络上的设备中收集网络管理信息的方法。SNMP 也为设备向网络管理工作站报告问题和错误提供了一种方法。

几乎所有的网络设备生产厂家都实现了对 SNMP 的支持。领导潮流的 SNMP 是一个从网络上的设备收集管理信息的公用通信协议。设备的管理者收集这些信息并记录在管理信息库（MIB）中。这些信息报告设备的特性、数据吞吐量、通信超载和错误等。MIB 有公共的格式，所以来自多个厂商的 SNMP 管理工具可以收集 MIB 信息，在管理控制台上呈现给系统管理员。

通过将 SNMP 嵌入数据通信设备，如交换机或集线器中，就可以从一个中心站管理这些设备，并以图形方式查看信息。可获取的很多管理应用程序通常可在大多数当前使用的操作系统下运行，如 Windows3.11.Windows95、Windows NT 和不同版本 UNIX 的等

。

一个被管理的设备有一个管理代理，它负责向管理站请求信息和动作，代理还可以借助于陷阱为管理站提供站动提供的信息，因此，一些关键的网络设备（如集线器、路由器、交换机等）提供这一管理代理，又称 SNMP 代理，以便通过 SNMP 管理站进行管理。

关于网络管理的定义很多，但都不够权威。一般来说，网络管理就是通过某种方式对网络进行管理，使网络能正常高效地运行。其目的很明确，就是使网络中的资源得到更加有效的利用。它应维护网络的正常运行，当网络出现故障时能及时报告和处理，并协调、保持网络系统的高效运行等。国际标准化组织（ISO）在 ISO/IEC7498-4 中定义并描述了开放系统互连（OSI）管理的术语和概念，提出了一个 OSI 管理的结构并描述了 OSI 管理应有的行为。它认为，开放系统互连管理是指这样一些功能，它们控制、协调、监视 OSI 环境下的一些资源，这些资源保证 OSI 环境下的通信。通常对一个网络管理系统需要定义以下内容：

- 系统的功能。即一个网络管理系统应具有哪些功能。
- 网络资源的表示。网络管理很大一部分是对网络中资源的管理。网络中的资源就是指网络中的硬件、软件以及所提供的服务等。而一个网络管理系统必须在系统中将它们表示出来，才能对其进行管理。
- 网络管理信息的表示。网络管理系统对网络的管理主要靠系统中网络管理信息的传递来实现。网络管理信息应如何表示、怎样传递、传送的协议是什么?这都是一个网络管理系统必须考虑的问题。
- 系统的结构。即网络管理系统的结构是怎样的。

分类功能

三代分类

事实上，网络管理技术是伴随着计算机、网络和通信技术的发展而发展的，二者相辅相成。从网络管理范畴来分类，可分为对网“路”的管理。即针对交换机、路由器等主干网络进行管理；对接入设备的管理，即对内部 PC、服务器、交换机等进行管理；对行为的管理。即针对用户的使用进行管理；对资产的管理，即统计 IT 软硬件的信息等。根据网管软件的发展历史，可以将网管软件划分为三代：

第一代网管软件就是最常用的命令行方式，并结合一些简单的网络监测工具，它不仅要求使用者精通网络的原理及概念，还要求使用者了解不同厂商的不同网络设备的配置方法。

第二代网管软件有着良好的图形化界面。用户无须过多了解设备的配置方法，就能图形化地对多台设备同时进行配置和监控。大大提高了工作效率，但仍然存在由于人为因素造成的设备功能使用不全面或不正确的问题数增大，容易引发误操作。

第三代网管软件相对来说比较智能，是真正将网络和管理进行有机结合的软件系统，具有“自动配置”和“自动调整”功能。对网管人员来说，只要把用户情况、设备情况以及用户与网络资源之间的分配关系输入网管系统，系统就能自动地建立图形化的人员与网络的配置关系，并自动鉴别用户身份，分配用户所需的资源（如电子邮件、Web、文档服务等）。

五大功能

根据国际标准化组织定义网络管理有五大功能：故障管理、配置管理、性能管理、安全管理、计费管理。对网络管理软件产品功能的不同，又可细分为五类，即网络故障管理软件，网络配置管理软件，网络性能管理软件，网络服务/安全管理软件，网络计费管理软件。

下面我们来简单介绍一下大家熟悉的网络故障管理、网络配置管理、网络性能管理、网络计费管理和网络安全管理五个方面网络管理功能：

ISO 在 ISO/IEC 7498-4 文档中定义了网络管理的五大功能，并被广泛接受。这五大功能是：

(1)故障管理(Fault Management)

故障管理是网络管理中最基本的功能之一。用户都希望有一个可靠的计算机网络。当网络中某个组成失效时，网络管理器必须迅速查找到故障并及时排除。通常不大可能迅速隔离某个故障，因为网络故障的产生原因往往相当复杂，特别是当故障是由多个网络组成共同引起的。在此情况下，一般先将网络修复，然后再分析网络故障的原因。分析故障原因对于防止类似故障的再发生相当重要。网络故障管理包括故障检测、隔离和纠正三方面，应包括以下典型功能：

网络管理

⑴故障监测：主动探测或被动接收网络上的各种事件信息，并识别出其中与网络和系统故障相关的内容，对其中的关键部分保持跟踪，生成网络故障事件记录。

(1)故障报警：接收故障监测模块传来的报警信息，根据报警策略驱动不同的报警程序，以报警窗口/振铃（通知一线网络管理人员）或电子邮件（通知决策管理人员）发出网络严重故障警报。

(2)故障信息管理：依靠对事件记录的分析，定义网络故障并生成故障卡片，记录排除故障的步骤和与故障相关的值班员日志，构造排错行动记录，将事件-故障-日志构成逻辑上相互关联的整体，以反映故障产生、变化、消除的整个过程的各个方面。

(3)排错支持工具：向管理人员提供一系列的实时检测工具，对被管设备的状况进行测试并记录下测试结果以供技术人员分析和排错；根据已有的排错经验和管理员对故障状态的描述给出对排错行动的提示。

(4)检索/分析故障信息：浏阅并且以关键字检索查询故障管理系统中所有的数据库记录，定期收集故障记录数据，在此基础上给出被管网络系统、被管线路设备的可靠性参数。

对网络故障的检测依据对网络组成部件状态的监测。不严重的简单故障通常被记录在错误日志中，并不作特别处理；而严重一些的故障则需要通知网络管理器，即所谓的"警报"。一般网络管理器应根据有关信息对警报进行处理，排除故障。当故障比较复杂时，网络管理器应能执行一些诊断测试来辨别故障原因。

⑵计费管理（Accounting Management)

计费管理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。网络管理员还可规定用户可使用的最大费用，从而控制用户过多占用和使用网络 资源。这也从另一方面提高了网络的效率。另外，当用户为了一个通信目的需要使用多个网络中的资源时，计费管理应可计算总计费用。

⑴计费数据采集：计费数据采集是整个计费系统的基础，但计费数据采集往往受到采集设备硬件与软件的制约，而且也与进行计费的网络资源有关。

⑵数据管理与数据维护：计费管理人工交互性很强，虽然有很多数据维护系统自动完成，但仍然需要人为管理，包括交纳费用的输入、联网单位信息维护，以及账单样式决定等。

⑶计费政策制定；由于计费政策经常灵活变化，因此实现用户自由制定输入计费政策尤其重要。这样需要一个制定计费政策的友好人机界面和完善的实现计费政策的数据模型。

⑷政策比较与决策支持：计费管理应该提供多套计费政策的数据比较，为政策制订提供决策依据。

(5)数据分析与费用计算：利用采集的网络资源使用数据，联网用户的详细信息以及计费政策计算网络用户资源的使用情况，并计算出应交纳的费用。

(6)数据查询：提供给每个网络用户关于自身使用网络资源情况的详细信息，网络用户根据这些信息可以计算、核对自己的收费情况。

(3)配置管理（Configuration Management)

配置管理同样相当重要。它初始化网络、并配置网络，以使其提供网络服务。配置管理是一组对辨别、定义、控制和监视组成一个通信网络的对象所必要的相关功能，目的是为了 实现某个特定功能或使网络性能达到最优。

(1)配置信息的自动获取：在一个大型网络中，需要管理的设备是比较多的，如果每个设备的配置信息都完全依靠管理人员的手工输入，工作量是相当大的，而且还存在出错的可能性。对于不熟悉网络结构的人员来说，这项工作甚至无法完成'因此，一个先进的网络管理系统应该具有配置信息自动获取功能。即使在管理人员不是很熟悉网络结构和配置状况的情况下，也能通过有关的技术手段来完成对网络的配置和管理。在网络设备的配置信息中，根据获取手段大致可以分为三类：一类是网络管理协议标准的 MIB 中定义的配置信息（包括 SNMP；和 CMIP 协议）；二类是不在网络管理协议标准中有定义，但是对设备运行比较重要的配置信息；三类就是用于管理的一些辅助信息。

(2)自动配置、自动备份及相关技术：配置信息自动获取功能相当于从网络设备中"读"信息，相应的，在网络管理应用中还有大量"写"信息的需求。同样根据设置手段对网络配置信息进行分类：一类是可以通过网络管理协议标准中定义的方法（如 SNMP 中的 set 服务）进行设置的配置信息；二类是可以通过自动登录到设备进行配置的信息；三类就是需要修改的管理性配置信息。

(3)配置一致性检查：在一个大型网络中，由于网络设备众多，而且由于管理的原因，这些设备很可能不是由同一个管理人员进行配置的。实际上'即使是同一个管理员对设备进行的配置，也会由于各种原因导致配置一致性问题。因此，对整个网络的配置情况进行一致性检查是必需的。在网络的配置中，对网络正常运行影响最大的主要是路由器端口配置和路由信息配置，因此，要进行一致性检查的也主要是这两类信息。

(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配置操作。

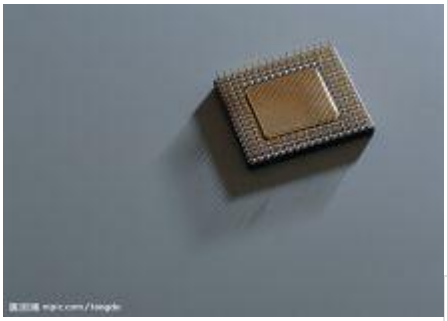
(4)性能管理(Performance Management)

性能管理估价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触发某个诊断测试过程或重新

配置网络以维持网络的性能。性能管理收集分析有关被管网络当前状况的数据信息，并维持和分析性能日志。一些典型的功能包括：

(1)性能监控：由用户定义被管对象及其属性。被管对象类型包括线路和路由器；被管对象属性包括流量、延迟、丢包率、CPU 利用率、温度、内存余量。对于每个被管对象，定时采集性能数据，自动生成性能报告。

(2)阈值控制：可对每一个被管对象的每一条属性设置阈值，对于特定被管对象的特定属性，可以针对不同的时间段和性能指标进



CPU 芯片

行阈值设置。可通过设置阈值检查开关控制阂值检查和告警，提供相应的阈值管理和溢出告警机制。

(3)性能分桥：对历史数据进行分析，统计和整理，计算性能指标，对性能状况作出判断，为网络规划提供参考。

(4)可视化的性能报告：对数据进行扫描和处理，生成性能趋势曲线，以直观的图形反映性能分析的结果。

(5)实时性能监控：提供了一系列实时数据采集；分析和可视化工具，用以对流量、负载、丢包、温度、内存、延迟等网络设备和线路的性能指标进行实时检测，可任意设置数据采集间隔。

(6)网络对象性能查询：可通过列表或按关键字检索被管网络对象及其属性的性能记录。

(5)安全管理(Security Management)

安全性一直是网络的薄弱环节之一，而用户对网络安全的要求又相当高，因此网络安全管理非常重要。网络中主要有以下几大安全问题：

网络数据的私有性（保护网络数据不被侵 入者非法获取），

授权（Authentication）（防止侵入者在网络上发送错误信息),

访问控制（控制访问控制（控制对网络资源的访问）。

相应的，网络安全管理应包括对授权机制、访问控制 、加密和加密关键字的管理，另外还要维护和检查安全日志。包括：

网络管理过程中，存储和传输的管理和控制信息对网络的运行和管理至关重要，一旦泄密、被篡改和伪造，将给网络造成灾难性的破坏。网络管理本身的安全由以下机制来保证：(1)管理员身份认证，采用基于公开密钥的证书认证机制；为提高系统效率，对于信任域内（如局域网）的用户，可以使用简单口令认证。

(2)管理信息存储和传输的加密与完整性，Web 浏览器和网络管理服务器之间采用安全套接字层（SSL）传输协议，对管理信息加密传输并保证其完整性；内部存储的机密信息，如登录口令等，也是经过加密的。

(3)网络管理用户分组管理与访问控制，网络管理系统的用户（即管理员）按任务的不同分成若干用户组，不同的用户组中有不同的权限范围，对用户的操作由访问控制检查，保证用户不能越权使用网络管理系统。

(4)系统日志分析，记录用户所有的操作，使系统的操作和对网络对象的修改有据可查，同时也有助于故障的跟踪与恢复。

网络对象的安全管理有以下功能：

(1)网络资源的访问控制，通过管理路由器的访问控制链表，完成防火墙的管理功能，即从网络层(1P）和传输层(TCP）控制对网络资源的访问，保护网络内部的设备和应用服务，防止外来的攻击。

(2)告警事件分析，接收网络对象所发出的告警事件，分析员安全相关的信息（如路由器登录信息、SNMP 认证失败信息），实时地向管理员告警，并提供历史安全事件的检索与分析机制，及时地发现正在进行的攻击或可疑的攻击迹象。

(3)主机系统的安全漏洞检测，实时的监测主机系统的重要服务（如 WWW，DNS 等）的状态，提供安全监测工具，以搜索系统可能存在的安全漏洞或安全隐患，并给出弥补的措施。

(6)上网行为管理

小草网管软件综合智能动态带宽保障，服务器流量分析与保障、虚拟多设备管理等多项突破性技术，涵盖流量分析、带宽管理、上网行为管理、DMZ 区服务器管理，专线集中管理、企业级防火墙与路由器、负载均衡等功能，在网络性能、质量、安全等方面为客户提供完整的解决方案。本产品已获得各行业客户的广泛认可，成为企业网关综合管理软件产品第一品牌。

1.企业网关统一管理系统

2. 支持在 windows 操作系统上安装与部署

3.安装与操作简单易用

4. 流量分析准确

5. 流控效果显著

6.市场上唯一支持对 DMZ 区与内网服务器管理的产品

7. 市场上唯一支持对多条专线统一集中管理的产品

管理协议

简介

随着网络的不断发展，规模增大，复杂性增加，简单的网络管理技术已不能适应网络迅速发展的要求。以往的网络管理系统往往是厂商在自己的网络系统中开发的专用系统，很难对其他厂商的网络系统、通信设备软件等进行管理，这种状况很不适应网络异构互联的发展趋势。20 世纪 80 年代初期 Internet 的出现和发展使人们进一步意识到了这一点。研究开发者们迅速展开了对网络管理的研究，并提出了多种网络管理方案，包括 HEMS、SGMP、CMIS/CMIP 等。下面进行简单介绍。

SNMP

简单网络管理协议（SNMP）的前身是 1987 年发布的简单网关监控协议（SGMP）。SGMP 给出了监控网关（OSI 第三层路由器）的直接手段，SNMP 则是在其基础上发展而来。最初，SNMP 是作为一种可提供最小网络管理功能的临时方法开发的，它具有以下两个优点：

(1)与 SNMP 相关的管理信息结构（SMI）以及管理信息库（MIB）非常简单，从而能够迅速、简便地实现；

(2)SNMP 是建立在 SGMP 基础上的，而对于 SGMP，人们积累了大量的操作经验。

SNMP 经历了两次版本升级，现在的最新版本是 SNMPv3。在前两个版本中 SNMP 功能都得到了极大的增强，而在最新的版本中，SNMP 在安全性方面有了很大的改善，SNMP 缺乏安全性的弱点正逐渐得到克服。

CMIS/CMIP

公共管理信息服务/公共管理信息协议（CMIS/CMIP）是 OSI 提供的网络管理协议簇。CMIS 定义了每个网络组成部分提供的网络管理服务，这些服务在本质上是很普通的，CMIP 则是实现 CMIS 服务的协议。

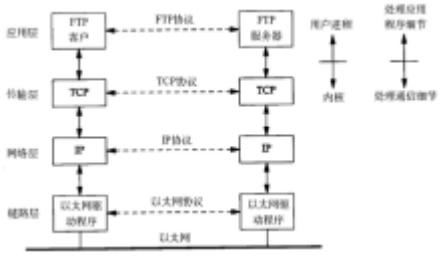
OSI 网络协议旨在为所有设备在 ISO 参考模型的每一层提供一个公共网络结构，而 CMIS/CMIP 正是这样一个用于所有网络设备的完整网络管理协议簇。

出于通用性的考虑，CMIS/CMIP 的功能与结构跟 SNMP 很不相同，SNMP 是按照简单和易于实现的原则设计的，而 CMIS/CMIP 则能够提供支持一个完整网络管理方案所需的功能。

CMIS/CMIP 的整体结构是建立在使用 ISO 网络参考模型的基础上的，网络管理应用进程使用 ISO 参考模型中的应用层。也在这层上，公共管理信息服务单元（CMISE）提供了应用程序使用 CMIP 协议的接口。同时该层还包括了两个 ISO 应用协议：联系控制服务元素（ACSE）和远程操作服务元素（RpSE），其中 ACSE 在应用程序之间建立和关闭联系，而 ROSE 则处理应用之间的请求/响应交互。另外，值得注意的是 OSI 没有在应用层之下特别为网络管理定义协议。

CMOT

公共管理信息服务与协议（CMOT）是在 TCP/IP 协议簇上实现 CMIS 服务，这是一种过渡性的解决方案，直到 OSI 网络管理协议被广泛采用。



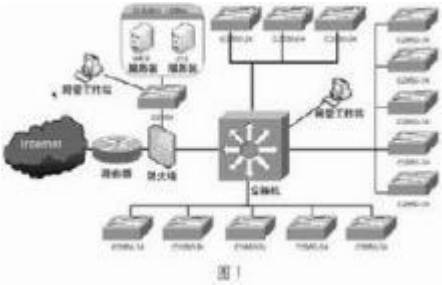
TCP/IP 协议

CMIS 使用的应用协议并没有根据 CMOT 而修改，CMOT 仍然依赖于 CMISE、ACSE 和 ROSE 协议，这和 CMIS/CMIP 是一样的。但是，CMOT 并没有直接使用参考模型中表示层实现，而是要求在表示层中使用另外一个协议--轻量表示协议（LPP），该协提供了目前最普通的两种传输层协议--TCP 和 UDP 的接口。

CMOT 的一个致命弱点在于它是一个过渡性的方案，而没有人会把注意力集中在一个短期方案上。相反，许多重要厂商都加入了 SNMP 潮流并在其中投入了大量资源。事实上，虽然存在 CMOT 的定义，但该协议已经很长时间没有得到任何发展了。

LMMP

局域网个人管理协议（LMMP）试图为 LAN 环境提供一个网络管理方案。LMMP 以前被称为 IEEE802 逻辑链路控制上的公共管理信息服务与协议（CMOL）。由于该协议直接位于 IEEE802 逻辑链路层（LLC）上，它可以不依赖于任何特定的网络层协议进行网络传输。



网络管理

由于不要求任何网络层协议，LMMP 比 CMIS/CMIP 或 CMOT 都易于实现，然而没有网络层提供路由信息，LMMP 信息不能跨越路由器，从而限制了它只能在局域网中发展。但是，跨越局域网传输局限的 LMMP 信息转换代理可能会克服这一问题。

简单协议

简单网络管理协议（SNMP）是最早提出的网络管理协议之一。SNMP 已成为网络管理领域中事实上的工业标准，并被广泛支持和应用，大多数网络管理系统和平台都是基于 SNMP 的。

一、 SNMP 概述

SNMP 的前身是简单网关监控协议（SGMP），用来对通信线路进行管理。随后，人们对 SGMP 进行了很大的修改，特别是加入了符合 Internet 定义的 SMI 和 MIB：体系结构，改进后的协议就是著名的 SNMP。SNMP 的目标是管理互联网 Internet 上众多厂家生产的软硬件平台，因此 SNMP 受 Internet 标准网络管理框架的影响也很大。SNMP 已经出到第三个版本的协议，其功能较以前已经大大地加强和改进了。

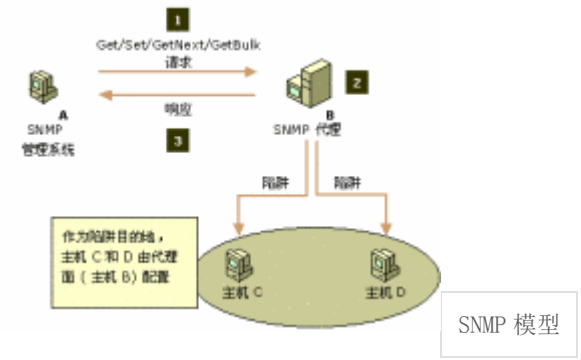
SNMP 的体系结构是围绕着以下四个概念和目标进行设计的：保持管理代理（agent）的软件成本尽可能低；最大限度地保持远程管理的功能，以便充分利用 Internet 的网络资源；体系结构必须有扩充的余地；保持 SNMP 的独立性，不依赖于具体的计算机、网关和网络传输协议。在最近的改进中，又加入了保证 SNMP 体系本身安全性的目标。

另外，SNMP 中提供了四类管理操作：get 操作用来提取特定的网络管理信息；get-next 操作通过遍历活动来提供强大的管理信息提取能力；set 操作用来对管理信息进行控制（修改、设置）；trap 操作用来报告重要的事件。

二、 SNMP 管理控制框架与实现

1．SNMP 管理控制框架

SNMP 定义了管理进程（Manager）和管理代理（Agent）之间的关系，这个关系称为共同体(Community）。描述共同体的语义是非常复杂的，但其句法却很简单。位于网络管理工作站（运行管理进程）上和各网络元素上利用 SNMP 相互通信对网络进行管理的软件统统称为 SNMP 应用实体。若干个应用实体和 SNMP 组合起来形成一个共同体，不同的共同体之间用名字来区分，共同体的名字则必须符合 Internet 的层次结构命名规则，由无保留意义的字符串组成。此外，一个 SNMP 应用实体可以加入多个共同体



SNMP 模型

。

SNMP 的应用实体对 Internet 管理信息库中的管理对象进行操作。一个 SNMP 应用实体可操作的管理对象子集称为 SNMP MIB 授权范围。SNMP 应用实体对授权范围内管理对象的访问仍然还有进一步的访问控制限制，比如只读、可读写等。SNMP 体系结构中

要求对每个共同体都规定其授权范围及其对每个对象的访问方式。记录这些定义的文件称为“共同体定义文件”。

SNMP 的报文总是源自每个应用实体，报文中包括该应用实体所在的共同体的名字。这种报文在 SNMP 中称为“有身份标志的报文”，共同体名字是在管理进程和管理代理之间交换管理信息报文时使用的。管理信息报文中包括以下两部分内容：

(1)共同体名，加上发送方的一些标识信息（附加信息），用以验证发送方确实是共同体中的成员，共同体实际上就是用来实现管理应用实体之间身份鉴别的；

(2)数据，这是两个管理应用实体之间真正需要交换的信息。

在第三版本前的 SNMP 中只是实现了简单的身份鉴别，接收方仅凭共同体名来判定收发双方是否在同一个共同体中，而前面提到的附加倍息尚未应用。接收方在验明发送报文的管理代理或管理进程的身份后要对其访问权限进行检查。访问权限检查涉及到以下因素：

(1)一个共同体内各成员可以对哪些对象进行读写等管理操作，这些可读写对象称为该共同体的“授权对象”（在授权范围内）；

(2)共同体成员对授权范围内每个对象定义了访问模式：只读或可读写；

(3)规定授权范围内每个管理对象（类）可进行的操作（包括 get，get-next，set 和 trap）；

(4)管理信息库（MIB）对每个对象的访问方式限制（如 MIB 中可以规定哪些对象只能读而不能写等）。

管理代理通过上述预先定义的访问模式和权限来决定共同体中其他成员要求的管理对象访问（操作）是否允许。共同体概念同样适用于转换代理（Proxy Agent），只不过转换代理中包含的对象主要是其他设备的内容。

2．SNMP 实现方式为了提供遍历管理信息库的手段，SNMP 在其 MIB 中采用了树状命名方法对每个管理对象实例命名。每个对象实例的名字都由对象类名字加上一个后缀构成。对象类的名字是不会相互重复的，因而不同对象类的对象实例之间也少有重名的危险。

在共同体的定义中一般要规定该共同体授权的管理对象范围，相应地也就规定了哪些对象实例是该共同体的“管辖范围”，据此，共同体的定义可以想象为一个多叉树，以词典序提供了遍历所有管理对象实例的手段。有了这个手段，SNMP 就可以使用 Get-next 操作符，顺序地从一个对象找到下一个对象。Get-next(Object-instance)操作返回的结果是一个对象实例标识符及其相关信息，该对象实例在上面的多叉树中紧排在指定标识符；Bject-instance 对象的后面。这种手段的优点在于，即使不知道管理对象实例的具体名字，管理系统也能逐个地找到它，并提取到它的有关信息。遍历所有管理对象的过程可以从第一个

对象实例开始（这个实例一定要给出），然后逐次使用 Get-next，直到返回一个差错（表示不存在的管理对象实例）结束（完成遍历）。

由于信息是以表格形式（一种数据结构）存放的，在 SNMP 的管理概念中，把所有表格都视为子树，其中一张表格（及其名字）是相应子树的根节点，每个列是根下面的子节点，一列中的每个行则是该列节点下面的子节点，并且是子树的叶节点，如下图所示。因此，按照前面的子树遍历思路，对表格的遍历是先访问第一列的所有元素，再访问第二列的所有元素……，直到最后一个元素。若试图得到最后一个元素的“下一个”元素，则返回差错标记。

管理关键

网络迅速发展，导致网络结构更为复杂；网络应用的日新月异，让网络管理员每天都要面对新的问题。很多企事业单位，在遇到网络问题不知道应该如何去解决，看流量，拔网线等手段，排查周期长，也很难真正找出问题。

网络发展到一定阶段，必然要考虑到网络性能、网络故障与网络安全性问题。只有通过运用网络分析技术对网络流通数据的清晰认识，才能为故障的排查，性能的提升，以及网络安全的解决提供可靠的数据依据。

信息应用与治理

网络最大的价值，是在于信息化的应用。当出现故障不能及时解决，即使有再好的电子商务、电子政务，也只是一个摆设。无论是安全、性能还是故障性问题，不能快速解决，给企业带来的是难以衡量的损失。

治理并不是简单的网络管理，它需要管理者对网络中所有设备完全掌握，包括每个网卡地址，以及所处的位置。通过对网络传输中的数据进行全面监控分析，才能从网络底层数据获取各种网络应用行为造成的网络问题，并快速的定位到网卡的位置。从而在安全策略上更好的防范，对故障和性能更合理的管理。

一劳永逸的误区

从管理角度的考虑，往往期望络故障和安全性问题可以自动解决。但历经多年，没有任何产品能做到。虽然许多企业部署了非常好的安全防护产品，但仍然会受到网络攻击和病毒危害。根本原因在于，网络应用本身就在不断的发展，新的病毒以及病毒变种，都很难被基于特征库或病毒库的产品所识别。要解决这些问题，则要求网络管理员随时都能查看到网络中真实的数据，最快的发现引起问题的原因。

网络拓扑图 VS 矩阵图

网络拓扑图要求这些交换设备都必须支持 SNMP（简单网络管理协议），它能直观能看到网络结构，但看不到终端主机；它能看到设备断网情况和粗略流量，但对网络问题的解决能力并不实用。

网络拓扑图

从技术趋势来看，矩阵图（Matrix）将更适合网络管理的需要。矩阵图也被称为主机连接图，可以监控每台主机（包括交换设备）之间的通讯连接，极大的提高了监控范围，监控范围深入到每台主机之间的各种应用，包括通讯、资源占用、活跃程度、服务应用等，管理者可以监控到每台主机的一举一动，各种网络问题都会在矩阵中表现出异常。如：BT 下载、DDOS 攻击、ARP 攻击、木马扫描等。

"诊断专家"快速提高解决能力

网络分析不仅提供网络依据，更重要的是帮助管理者提高问题的解决能力。"诊断专家"则是一个从问题原因到问题结果的完整解释。好的网络分析产品，可以自动提取问题的相关数据，并告诉管理者网络中存在有哪些问题，可能产生的原因，有什么办法可以解决，ARP 攻击的快速定位则是一个很好的证明。

网络数据的回放能力

好的网络分析产品，都具有网络数据的回放能力，将网络数据进行 7x24 小时记录，可以按每天或每小时来记录。如果要分析昨天某个时段出现的网络故障，只需要将当时保存的数据包进行播放，同时通过网络分析来追溯故障是如何发生的，使网络管理对历史问题追查能力得到明显提高。

局域网网络流量控制与管理办法[3]

1、局域网网络流量监控方法

网络流量监控的主要目的是对网络进行管理，其过程一般是：一、实时、不间断地采集网络数据。二、统计、分析所得数据。三、确认网络的主要性能指标。四、对网络进行分析管理。网络流量监控的方法主要有两种，一种是使用网络监控设备，另一种是使用网络流量监控软件。当前的局域网网络设备对于 P2P 这种模式没有很好的管理效果，导致 P2P 软件大行其道，占用了极多的带宽资源。当前，以下几种网络流量最为常见：

（1）P2P 流量：P2P 文件共享在网络带宽消耗方面是大户，夜间，有 95%的网络带宽被 P2P 占用。

（2）FTP 流量：FTP 这项服务的应用比较早，且重要程度只比 HTTP 和 SMTP 稍低。P2P 的出现，FTP 的重要性再次降低，但其重要性仍然不可忽视。

...

2、局域网流量控制与管理策略

2.1 通过路由控制流量

2.2 禁止 P2P 下载

2.3 进行时间段管理
2.4 限定局域网主机速度
3、局域网流量异常发现与处理
3.1 找出流量过大的电脑
3.2 对异常主机发出警告

局域网络管理

传统的局域网管理主要针对一定范围的局域网络，在这样的局域网络中包括的主要管理对象有：服务器、客户机、客户端 PC 机各种网络线路与集线器以及各种网络操作系统。由于在这样规模的局域网中，网络管理的对象有限，网络管理一般包括三个方面：了解网络，网络运行以及网络维护。1．了解网络

要管好一个局域网，就必须对该局域网有清楚的了解。对该网络的清晰了解以及对各种网络信息的资料化管理记录，是保证网络正常运转以及进行各种网络维护的前提与基础。

局域网

(1)识别网络对象的硬件情况：局域网是由各种节点组成，这样的节点主要是服务器和客户机，因此首先需要识别这些节点的硬件组成。硬件识别包括了解服务器和客户机的品牌、它们的芯片速率、网卡品牌与配置情况，以及集线器的型号与品牌，这样就可以了解局域网中硬件设备的提供商并对硬件设备所能达到的性能有大体的了解。另外，对服务器的硬件还必须有进一步的了解，包括服务器的外设配置情况、硬盘驱动器的容量以及内存大小等。

(2)判别局域网的拓扑结构：了解了网络中的关键部件之后需要进一步了解它们是如何连接运行的，即网络结构下的实际布线系统。常见的三种布线的拓扑结构是星形、总线和环型拓扑结构，另外也有无线和点对点的拓扑结构，但不常用。在了解局域网的布线结构后，针对每种结构各自的优缺点，应注意其将导致的性能与故障差异。然后需要了解的是实现网络传输的方式。常用的网络传输方式是 Ethernet，它是一种支持广泛的传输协议以及多种布线形式的成熟标准。Ethernet 是非确定型的，网络传送任务越重，越有可能发生冲突，而冲突将导致影响响应时间。所以网络上有大量活动节点时性能就会大大降低，如果 Ethernet 集线器上总是出现冲突信号的话，在熟悉网络布局后可能就得重新考虑分布网

络上的用户。Ethernet 的缆线包括：粗缆 Ethernet，或叫 10Base5 Ethernet，使用大号的同轴电缆；细缆 Ethernet，也叫 10Base2Ethernet，使用小口径的 RG-58 同轴电缆；10BaseTEthernet，在星形结构中使用非屏蔽双绞线。对于采用 Ethernet 方式的局域网，网络管理员不仅要清楚 Ethernet 的原理，还必须了解组网所用的 Ethernet 缆线和插头以及它们的特点，这样在网络出现故障时可以帮助故障点的寻找与排除。除了 Ethernet 之外，其他的网络传输方式还有标记环（Token Ring）、光纤分布数据接口（FDDI）以及 ARCNet 等。了解局域网使用的传输方式是局域网管理的基本条件之一。

⑶确定网络的互联：首先需要确定网络连接的设备和接入网络的方式。这些设备与接入方式包括：使用调制解调器(Modem），使用网络插座，使用 CSU/DSU 连接，使用网桥工作，使用路由器，使用网关。这些接入设备对于保证网络节点的连通以及该局域网与主干网连通有着重要作用，同时也是网络故障多发的故障点和影响网络性能的可能瓶颈所在。另一方面，还需要在网络服务器或其他网络设备上确定该局域网的所有子网和各客户机都能连通，并记录下网络中各子网以及客户机的 IP 地址分配。

⑷确定用户负载和定位：网络负载最重要的方面是用户的分布，因为每一网络和服务器上的用户数量是影响网络性能的关键因素，因此确定网络上有多少用户以及他们各自的定位尤其重要。首先，查看文件服务器上的负载，了解文件服务器正常运行的时间，查看服务器 CPU 的使用率，以及服务器上网络连接的数目，这些数据提供了网络负载的直接数据；然后，利用这些数据分析众多服务器中哪个使用率最高，哪些网络的负担最重，最后对网络用户以及负载分布情况有个大致的了解。

2．网络运行

要使一个局域网顺利运转必须完成很多工作，这些工作包括：配置网络，即选择网络操作系统，选择网络连接协议，并根据选择的网络协议配置客户机的网络软件；然后配置网络服务器及网络的外围设备，做好网络意外预防处理；最后还有网络安全管理、网络用户权限分配以及病毒的预防与处理。

⑴配置网络；配置网络就要选择网络操作系统。传统的网络操作系统包括 UNIX，Windows NT，NetWare，VINES，Windows for Workgroups，LANtastic，Personal NetWare 等，这些网络操作系统有各自的特点，相对而言，在局域两中 WindowsNT 和 NetWare 比较普遍。NT 最大的优势在于价格和支撑其发展的巨头 Microsoft。NT 支持 IPX 和 TCP/IP，因此在大多数网络环境中受到欢迎，另外，其安全性和网络管理功能也不错在硬件完全兼容时安装也比较方便。在现有网络中，大约 70%的网络操作系统采用了 Novell 公司的 NetWare 系列。NetWare 是一种快速而可靠的操作系统，十分类似于 DOS，它对多种网络协议和多种客户机操作系统有着完善的支持，其兼容性和模块化设计也使它领先于其它系统。

选择网络协议也是配置网络的重要组成部分。现在流行的局域网网络协议包括 IPX/SPX、TCP/IP、NETBIOS、NetBEUI 和 AppleTalk 等。比较普遍的协议是 IPX/SPX

和 TCP/IP，其中 IPX/SPX 是 NetWare 所采用的数据传输方式，在局域网中使用非常普遍；TCP/IP 是面向 Internet 所使用的网络协议，具有广泛的影响力。

在确定了网络操作系统和网络协议之后，需要配置该网络中每台客户机的网络软件。在 DOS 平台上，一般是安装相应网络协议的网络驱动软件，然后修改一些配置文件中的参数；在 GUI 的操作系统（例如 Windows 系列、Macintosh 和 OS2)中，则选择相应的对话框窗口配置网络参数；在 UNIX 系统中，主要靠修改系统配置文件来配置网络。

(2)配置网络服务器：在局域网中，服务器往往具有重要作用，一个配置良好的服务器可以顺利保障网络的运行。首先是在服务器上用磁盘和卷根据内容的性质与空间大小分配来划分工作，这样可以把不同的程序和数据按照一种顺序存放在磁盘中，而卷的使用不仅可以按一定的层次存放数据，而且可以控制用户的访问权，然后在服务器上启动网络服务进程，监测网络用户的访问。还有一些外围设备，比如共享打印机、共享外接磁盘或驱动器等，这些设备在服务器上都应正确配置。

最后还应该注意的是预防网络意外发生，首先是保证电源（特别是网络服务器的电源），一般的方式是配置 UPS 应急电源；然后是保证服务器的环境状况（比如维持机房的温度与湿度在一定的范围）；最后是做好重要数据和系统的备份工作。备份的硬件设备包括硬盘阵列和磁带、光盘驱动器等，备份的方法很多，常用的是磁盘镜像、磁盘双工或磁盘阵列等。在进行备份时一定要做好详细记录，对备份内容进行分类并做标记。

(3)网络安全控制：网络安全控制的首要任务是管理用户注册和访问权限。在局域网上，网络操作系统一般都提供用户管理和权限分配的工具。对于局域网内，部用户，利用这些工具可以检查和设置用户信息、进行账号限制，例如改变账号密码、设置组、确定组中的账号、修改组或账号的权限、设定账号有效时间等等。定时对网络当前访问情况进行检查并做好记录，及时发现异常情况。另外，管理局域网外部权限和连接也很重要，一般局域网外部用户可能会访问该局域网，如查看已有文件、传递他们的文件或使用其他网络资源，因此对这种用户也需要建立账号，但应根据其使用网络的目的详细控制其访问权限，然后定期检查哪些用户没有注册，对一些不再需要的账号及时注销。

病毒对局域网的危害非常严重，一种网络病毒可以通过网络迅速地传染到局域网的每一台客户机，因此及时发现并杀死病毒至关重要。有多种不同的方法可以识别病毒：在文件级上，用 CRC 技术可以将预期的文件大小或其他特征与文件被打开之前所看到的实际特征进行比较；最常用的方法是对文件进行扫描，发现已知病毒的标志、代码，从而辨认出每一种病毒的变形。一旦发现病毒，当然就要清除它。利用一些杀毒软件可以杀死病毒恢复原来的文件。另一种方法是删除有病毒的文件，然后用备份的无病毒文件替代。另外还必须对受病毒感染的服务器上的各卷进行扫描，如果在网络服务器之间或客户机之间存在通信联络，还必须去扫描其他系统。确定适当的持续的病毒防护是避免病毒侵害的最有效方法，这样的防护包括：建立和增强反病毒规则和程序；在客户机上安装和更新反病毒软件；安装基于网络的反病毒软件。

3．网络维护

网络维护是保障网络正常运行的重要方面，主要包括故障检测与排除、网络日常检查及网络升级。

(1)常见网络的故障和修复：在局域网中，最重要的故障检测工作是文件服务器的维护。只要服务器正常工作，集中存储的数据就是安全的，用户可以在需要时访问这些数据。当然，网络连接设备应保证用户能持续工作，而客户机本身也应能正常工作。

故障处理过程有四个主要部分：发现故障迹象，追踪故障的根源，排除故障，记录故障的解决方法。网络故障处理经常需要进行大量的调查研究，但相对而言只有很少的问题是真正比较复杂的。常见的情况是，故障的解决方法是很简单的，只不过被其他问题或不完全的信息掩盖了。在处理故障期间，可以参考图 1 中的流程图，以确保能对网络故障进行逻辑的和有条理的分析。

当网络管理人员收到故障报告时，首先应该检查别的用户是否也遇到同一问题，如果有多个用户报告了同类问题，那么很可能是出现了服务器或缆线故障，而不是用户客户机所引起的故障。

排除文件服务器上的错误非常关键，因为它通常会影响到很多用户，因此首先要对服务器进行认真检查：服务器是否在运行?监视器是否显示信息?服务器是否响应键盘输入?服务器控制台是否显示异常终止或其他信息?服务器 NIC（网络适配器）是否发送和接收数据? 服务器的卷是否已安装?

文件服务器通常是十分稳定的，但它们也特别容易出现三种类型的故障：第一类故障并不是网络操作系统本身的错误，而是由于配置的更改造成的，因此无论何时改变网络操作系统的配置都必须备份以前的配置并记录更改日期；第二类故障是部件失效，虽然 NIC 和磁盘失效是最为常见的，但从键盘端口到 SIMM 的任何部件都可能会发生故障，甚至在高品质服务器上也无法避免；第三类故障是服务器的软件模块引发的系统冲突故障，比如磁盘驱动程序或 LAN 驱动程序引发的内存故障等。

当服务器故障检查各方面都没有问题时，引起大量用户访问故障的问题很可能出现在网络缆线系统上。如果故障网络采用的是总线拓扑结构，那么故障检测工作可能会比较繁重；对于星形结构，则应检查集线器或 MAU 是否通电并能正常运行。如果连接设备本身运行良好，可检查它们与服务器的物理连接。一般而言，对于物理网络，电缆和按插件老化、电磁干扰、电缆长度限制是最常见的物理网络故障源；连接设备，如接插板、集线器和路由器也是故障多发点。

(2)网络检查：网络检查是在网络正常运转情况下对服务器状态和网络运行情况的动态信息收集和分析的过程。有些数据最好每天检查一次，而有些数据则较长时间检查一次即可。下面列出一些需要定期检查的网络关键信息：

频率 活 动	频率 活 动
每日 检查各服务器的卷空间	每日 去除旧用户

每日 列出前一天创建的文体	每月 检查用户账号安全性
每日 找出可被存档/删除的旧文件	每月 确保备份的完整性
每日 检查备份的执行情况	每月 更服务器模块
每日 检查服务器错误记录文件	每月 更新客户文件

(3)网络升级：网络升级是一个持续的过程，它需要考虑一些财务和预算因素。一般在网络管理中需要考虑的是必须进行的升级，这些升级能够保证网络正常运转。虽然网络操作系统的升级通常是最迫切的，但硬件和软件也可能需要升级。

服务器升级是最重要的。必须的服务器升级有三种：最简单的是用户许可证升级，如果网络服务器的能力已达到最大限度，并需要容纳更多的用户，就需要进行许可证升级；另二种服务器升级是网络操作系统的升级，如果使用的是过时的或有故障的网络操作系统，就应该升级为最新的版本；第三种服务器升级所指的范围相对来说要广泛一些，主要指硬件升级，硬件升级可能包括增加磁盘空间、改进容错措施或系统升级。另外，客户软件的升级有时也是很必要的，因为旧客户软件对于网络操作系统可能是一种沉重的负担。

在确定了最重要的升级之后，应决定需要购买的产品，并对升级费用进行评估，然后制定实施升级的工作步骤，最后应从成本和效益两方面总结新配置的优点。[4]

常见软件

提升国内网络管理的整体水平

相比海外而言，国内的网络管理起步较晚，用户的管理水平也不及海外。科来积极的将此项技术应用于网络 故障解决、网络性能提升与网络安全防护，旨在提升国内的网络管理水平，缩短与国外的差距，帮助用户实 现对其网络的全可视化，透过网络现象看到本质，真正的驾驭自己的网络。

帮助网络管理者精细化网络管理

网络分析技术是网络管理的关键，是网络进入深层次管理的必备技术，网络分析技术的普及也是必然趋势， 科来积极帮助用户建立在此项技术上的深入认知！在官网推出免费版本的软件供广大技术爱好者交流使用， 同时有针对性的提供大量的技术学习文档和视频资料，并组织力量在相关论坛解答用户的疑问及分享资源， 旨在推动该项技术在国内的普及程度，让用户切实的接触到先进的网络管理技术。

网络管理员

网络管理员主要针对目前国内机关，企事业单位的网络应用现状，如单位总出口带宽有限、网络滥用、员工无节制上网、聊天等等，提供了简单、有效的管理功能。

网盾 netsos3.0

网盾 netsos 是一款模块化架构的局域网管理软件，共包含 12 项强大的功能。根据实际需求，按需取用保证 IT 投资回报率。

管理维护

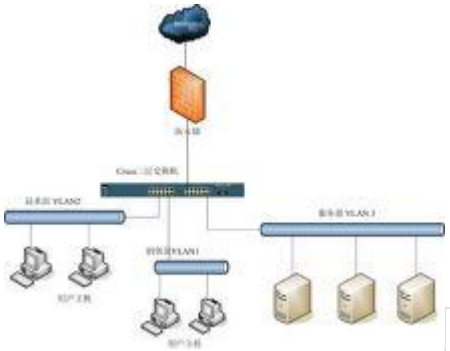
简介

网络管理和维护是一项非常复杂的任务，虽然关于网络管理既制订了国际标准，又存在众多网络管理的平台与系统，但要真正做好网络管理的工作不是一件简单的事情。下面我们将介绍网络技术发展下一些新形式的网络管理，以及在长期网络管理实践基础上总结出来的一些网络管理经验。

VLAN 管理

VLAN(虚拟局域网）就是一个计算机网络，其中的计算机好像是被同一网线连接在一起，而实际上它们可能分处于局域网的不同区域。VLAN 更多的是通过软件而非硬件来实现，因此这使得它具有很高的灵活性。VIAN 的一个主要特性就是提供了更多的管理控制，减少了相对日常管理开销，提供了更大的配置灵活性。

VLAN 的这些特性包括：①当用户从一个地点移动到另一个地点时，简化了配置操作和过程修改；②当网络阻塞时，可以重新调节流量分布；②提供流量与广播行为的详细报告，同时统计 VLAN 逻辑区域的规模与组成；④提供根据实际情况在 VLAN 中增加和减少用户的灵活性。



VLAN 管理

上面的这些操作必须透明地执行，同时需要不用具备太多实际网络复杂连接情况的了解，或者不用知道如何重新配置协议。虽然用户可以直接地通过设置或重置 VLAN 的端口来配置 VLAN，但缺乏智能网络管理工具的帮助；而保证 VLAN 在若干部门之间正常通信是很困难的。

VLAN 的配置如果根据交换机端口定义 VLAN，通常很容易用某种拖放软件把一个或多个用户分配到特定的 VLAN。在非交换环境里，移动、添加或更改操作很麻烦，有可能要改动接线板上的跳线充一个集线器端口移动到另一个端口。然而，改动 VLAN 分配仍然要靠人工进行：在大型网络里，这样做很费时，因而很多联网供应商鼓吹采用 VLAN 可以简化移动、添加和更改操作。

基于 MAC 地址的 VLAN 分配方案确实可使某些移动、添加和更改操作自动化。如果用户根据 MAC 地址被分配到一个 VLAN 或多个 VLAN，他们的计算机可以连接交换网络的任何一个端口，所有通信量均能正确无误地到达目的地。显然，管理员要进行 VLAN 初始分配，但用户移动到不同的物理连接不需要在管理控制台进行人工干预；例如有很多移动用户的站，他们并非总是连接同一端口——或许因为办公室都是临时性的，采用基于 MAC 地址的 VLAN 可避免很多麻烦。

传统的 Layer3 技术怎么样呢？这里离开 VLAN 最近的是 IP 子网：每个子网需要一个路由器端口，因为通信量只能通过一个路由器从一个子网移动到另一个子网。由于 IP32 位地址提供的地址空间很有限，所以很难分配子网地址，还有看你是否熟悉二进制算法。因此，在 IP 网络里执行移动、添加和更改操作很困难，速度慢，容易出错，而且费用大。另外，在公司更换 I 或者采用新安全策略时，可能有必要重新编号网络，这对于大型网络来说是无法想像的。

实际上，如果有人采用现有的有子网的路由 IP 网络，并根据 IP 地址访问任意 VLAN 成员，路由器就可能会被不必要的通信量淹没。

如果很多子网里都有 VALN 成员，常用的 VLAN 广播必须通过路由器才能达到所有成员。此外，糟糕的是广域链路会生成额外广播通信量；有 WAN 连接服务的 VLAN 成员数通常应该保持在最低水平。实际上， 基于 Layer3 地址的 VLAN 成员值有可能在增强和修改现有子网分布方面很有用，例如可通过一个全子网给 VLAN 添加两个新节点，或者可用两个子网组成一个 VLAN 而无须重新编号。

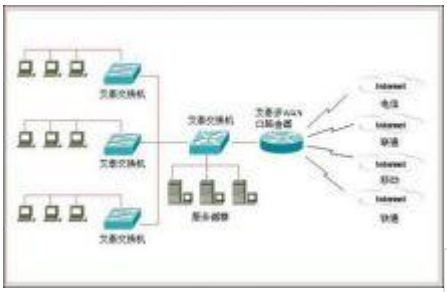
Cabletron 的 SecureFast Virtual Networking Layer3 交换技术采用路由服务器模型而不是传统的路由选择模型。第一个信息包传送到路由服务器进行常规路由计算，但交换机

能记忆路径，因而后续信息包可在 Layer2 交换，而无须查对路由表。由于有了基于纯 Layer3 地址的 VLAN，所以 IP 地址可以作为通用网络 ID，允许任何人连接任何数据链路，从而获得全网络访问，大大简化移动、添加和更改任务。

但是，还有其他方法解决 IP 子网引起的管理问题。DHCP（动态主机配置协议）已经在连接时给用户分配地址的其他技术，都可用于解决上述问题。

WAN 接入管理

在网络管理的解决方案中，我们知道一个大型网络，一般是 WAN，是通过分层进行管理的。比如在一个全国性的网络中心之下有许多地区性的网络中心，一般全国性的网络中心主要保证这个 WAN 的主干网正常运转，而地区性网络中心则主要负责各个网络用户的接入管理。



WAN 接入管理

对于每个想入网的用户而言，首先要考虑在网络连接上怎么接人这个网络。一般用户需要找到主管自己这片地区的地区性网络中心，然后提出申请，最后该地区性网络中心再进行用户的接入操作。这些操作一般包括：(1)联网用户必须租用一条网络线路，连接用户与地区性网络中心。该线路可以是已经存在的，属于某个商业网络公司或电信公司，也可以是单独为该用户铺设的一条线路。线路既可能是使用光纤的 DDN 专线，也可能是使用电话线的 DDR 线路。联网用户租用了网络线路就要向线路的经营者交纳租金，而线路的经营者可能不是提供接入服务的地 区性网络中心。

(2)联网用户需要向地区网络中心申请一段属于自己的 IP 地址，然后在全国网络中心注册域名。

(3)对于接入的联网用户，一般都要向地区性网络中心一次性交纳一笔接入费用，然后地区网络中心再对该用户进行网络接入的相关配置。

(4)在联网用户端也需要进行相应的配置，然后开通该用户的网络连接，最后联网用户需要根据其使用网络资源的流量交纳网络费用。

在上面的操作中可以看到，地区网络中心对新联网用户的接人需要进行相应的配置，这些配置操作一般包括：

(1)在接入路由器上，选择一个空闲端口，在该端口上进行相应的配置，然后再根据接人的拓扑关系，配置该端口的路由信息。

(2)在接入路由器上，根据用户的 IP 地址范围建立一个 Access-1ist 组，一旦用户要求或其他情况（如用户没有按规定交纳费用等）发生时，可以立即断掉该用户的网络连接。

(3)把该路由器端口和连接联网用户的线路加入网络管理监视对象集，以保障提供给用户可靠、稳定的网络接人服务。