

网络分析模块：网络分析的新工具

思科 IT 案例研究/网络管理/网络分析模块：本案例研究介绍了思科 IT 部门如何在思科全球网络中部署网络分析模块（NAM）。思科全球网络目前已经成为全球规模最大、最复杂、最先进的企业环境之一。思科客户可以利用思科 IT 部门在这个领域的实际经验支持类似的企业需求。

背景

随着思科多年来的不断发展，它发现了业务和网络之间的紧密联系——当业务发展时，对于网络基础设施的需求也会随之增长。从 1990 年到 2001 年，思科的年平均增长率达到了 160%。同时，需要网络连接的思科办公地点也在迅速增加。目前，思科在美国设有 127 个 WAN 办公地点，在除美国以外的美洲地区设有 25 个（11 个位于加拿大，14 个位于南美洲）；在欧洲、中东和非洲设有 76 个；在亚太地区设有 50 个。需求带来了新的挑战，进而催生了新的解决方案。它们建立在三个不断发展的因素的基础上：

- 越来越多的员工
- 更好、更新的业务应用
- 用以支持这些员工和应用的、不断发展的网络基础设施

办公地点和员工人数的迅速增加源于语音、视频在数据 IP 网络上的融合，以及用以支持思科发展的业务应用的不断增加。这样做的结果是产生了一个不断发展、不断变化的网络架构，而且越来越难以管理。

挑战

大规模企业网络为它们所支持的企业带来了许多好处，但是它们也为管理团队提出了很多严峻的挑战——思科也不例外。两个不同的主机之间的通信问题（包括网络流量问题或者应用故障）很难发现，除非管理员能够监测在这个指定的主机之间传输的、穿过某个特定网段的分组流量。

管理员很难在监控网段的同时观测流量或者应用的性能。过去，思科管理员使用的是基于远程监控（RMON）的分组捕获分析软件。尽管这种软件具有一定的作用，但是它也造成了很多实际的问题，因为它需要在存在故障流量的地点安装一台 PC，而这个地点可能是在另外一个办公楼、另一个城市或者另一个大陆。而且，这些方法很少能提供主动监控功能，因而无法在用户受到影响之前及时防止故障的发生。

思科网络设计和工程部门的网络工程师 Wilson Ng 介绍了管理员所面临的困境：“我们尝试了很多工具。我们面临的最主要的问题是分组捕获。但是即使拥有了分组捕获功能，你仍然缺乏很多信息，这造成了很多的不便。如果

我们想要进行远程分组捕获，我们必须让某个员工在现场放置一台笔记本电脑——有时现场位于另一栋办公楼或站点，甚至在几百英里以外。进行监控是一项需要实际操作经验的工作，但是我们拥有集中的团队。因为我们有 160 个销售办事处，所以我们需要可以进行远程分析的工具。”

网络分析需求一直在不断增长，但是利用笔记本来进行分组捕获的传统方法已经无法满足同时捕获来自于多个数据源的数据的要求。例如，一个多层应用可能包含多个组件。常见的多层应用是三层式应用，其中包含 Web 服务器、应用服务器和数据服务器。为了进行精确的诊断，必须从所有三个组件捕获数据。“传统的方法是使用三台运行分组捕获软件的笔记本电脑，以监控来自于所有三组服务器的网络流量：Web、应用和数据库。” Ng 表示。“使用三台笔记本电脑需要占用时间、硬件和其他资源。首先，这三台笔记本电脑必须可用。在笔记本电脑配置完毕之后，它们必须被放在检测现场，因而无法方便地从远程管理笔记本电脑上的网络分析软件。我们需要一种分布式网络分析设备，它必须能够进行多方位捕获，以解决这个问题。”

思科团队需要一个不仅能够提供分组捕获功能的解决方案。他们需要检测网络的应用层，以管理网络性能和诊断故障。他们需要集成对 LAN 和 WAN 的检测，提供实时的和对历史数据的监控。服务质量 (QoS) 的重要性在不断提高，随着 IP 语音 (VoIP) 的兴起，应用监控需求将变得比以往更加复杂。例如，监控 VoIP 需要能够监控每个电话呼叫的语音质量——包括抖动和丢包率。随着网络及其应用的日益复杂，对于监控的要求也将越来越高。

解决方案

思科网络分析模块 (NAM) 是解决这个问题的理想解决方案。NAM 是一种集成化的流量监控服务模块，需要占用 Cisco Catalyst 6500 系列交换机机箱中的一个插槽。它为思科网络管理员提供了全面的应用层可见度，并让网络工程师可以在网络的任何地方，利用一个浏览器获得这些信息。在安装之后，NAM 可以实现实时的和针对历史数据的应用监控，包括数据和语音。利用主动监控功能，它可以方便地捕获和解码分组、分析趋势、隔离网络故障和在故障发生之前发现应用响应延迟。新的 VoIP 和 QoS 监控功能让管理员可以分析 IP 电话进程和验证 QoS 策略。图 2 显示的 12 个演示界面表明，管理员可以直观地、轻松地进行网络分析。这些界面包括流量分析、端口监控、应用和 VLAN 监控，以及语音质量、分组捕获和解码。

概述

Ng 介绍了思科团队所采取的方法：“我们的过渡解决方案是采用另外一个供应商的分布式分组捕获系统。如果您需要获取某个故障的信息，您就必须到发生故障的现场。但是当我们与思科开发团队合作时，我们告诉他们我们希望不需要将实际的分组捕获设备带到故障现场。我们之中的某个人必须四处奔忙或者联系相关的工作人员。原先的想法是在每个办公楼中放置一台设备，但是现在，因为可以从远程启用 NAM，我们不需要再像过去那样赶赴现场了——我们能够更加轻松地获得同样的信息。” Ng 表示。“除了分组捕获和分析，我们需要更多的信息来了解实时流量。远程监控 (RMON) 数据有助于提供实时流量信息，而 Cisco Catalyst 6500 系列可以输出有限的 RMON 数据——但是这些并不够。要从 Cisco Catalyst 6500 系列——包括背板流量——获得所有的 RMON 数据，我们需要使用 NAM。NAM 可以为我们提供语音、数据和交换的统计信息。它可以每周 7 天、每天 24 小时地在所有端口上采集信息。其他的解

决方案只能采集某个端口的信息，而且当它们发现有数据穿过该端口时，它们无法判断这些数据的来源端口。”

通过在思科数据中心网络中部署 NAM 模块，思科团队可以全面地了解网络流量和网络状况。他们可以监控各种类型的应用。管理员不仅可以监控客户关系管理应用，例如 Siebel 和 Oracle，还可以监控前端 Web 应用，例如 Oracle Web Forms。随着越来越多的应用拥有 Web 接口，NAM 的这种功能变得非常重要，因为它让管理员可以监控企业的 Web 通信和行为。思科还利用 NAM 来监控 IP 电话，查找数据层中存在的问题。

在数据中心，NAM 在监控内容交换方面具有重要的意义。Ng 指出，思科 IT 部门正在设法监控数据中心的内容群，而 NAM 在这种环境中具有独特的优势。“过去，我们一直使用一个独立的 Web 服务器。通过独立服务器，Web 服务器可以进行负载平衡，以扩展 Web 应用。接下来，您可以选择特定的内容和使用多台服务器，构成一个服务器群。我们将这些 Web 服务器细分为更加具体的分类。届时，我们的内容将会按照数据和内容类型广泛地分发到不同的服务器上。在您使用这种分布式架构时，NAM 可以扮演一个非常重要的角色，因为它可以监控服务器之间的不同应用。因为在建立这种服务器群之后，网络将在这种分布式架构中扮演关键的角色，所以网络分析将会变得更加重要。我们需要了解网络组件的连接和通信方式，而 NAM 将帮助我们做到这一点。”

另外，思科团队还可以利用 NAM，从远程搜集 RMON-1 和 2 端口统计数据，而不需要使用一个单独的 RMON 探测器。与简单网络管理协议（SNMP）类似，RMON 可以在从第二层到第七层的设备之间的线路上设置陷阱并生成关于数据性能的报告，从而让管理员可以看到安装了 NAM 的第二层网络上的所有七层数据。因为 NAM 可以监控它所在的设备的背板上的所有七层流量，所以 NAM 可以找出线路上传输的流量所隐藏的信息：它可以监控两个设备之间的线路上的流量，以分析设备之间的网络性能。NAM 还可以利用 NetFlow 记录监控应用、主机和应用对话，以提高网络业务的可见度。

部署

NAM 已经被部署到思科目前使用的数据网络中（如图 1 所示）。作为标准化的 IT 基础设施的一部分，NAM 被安装于每个数据中心的生成树根分发交换机上，即一台 Cisco Catalyst 6500 系列交换机。因为采用了第二层交换架构，所以所有流量都必须流经根交换机。因此，可以将 NAM 放置在根交换机上。NAM 可以检测和分析流经该根交换机的所有流量。

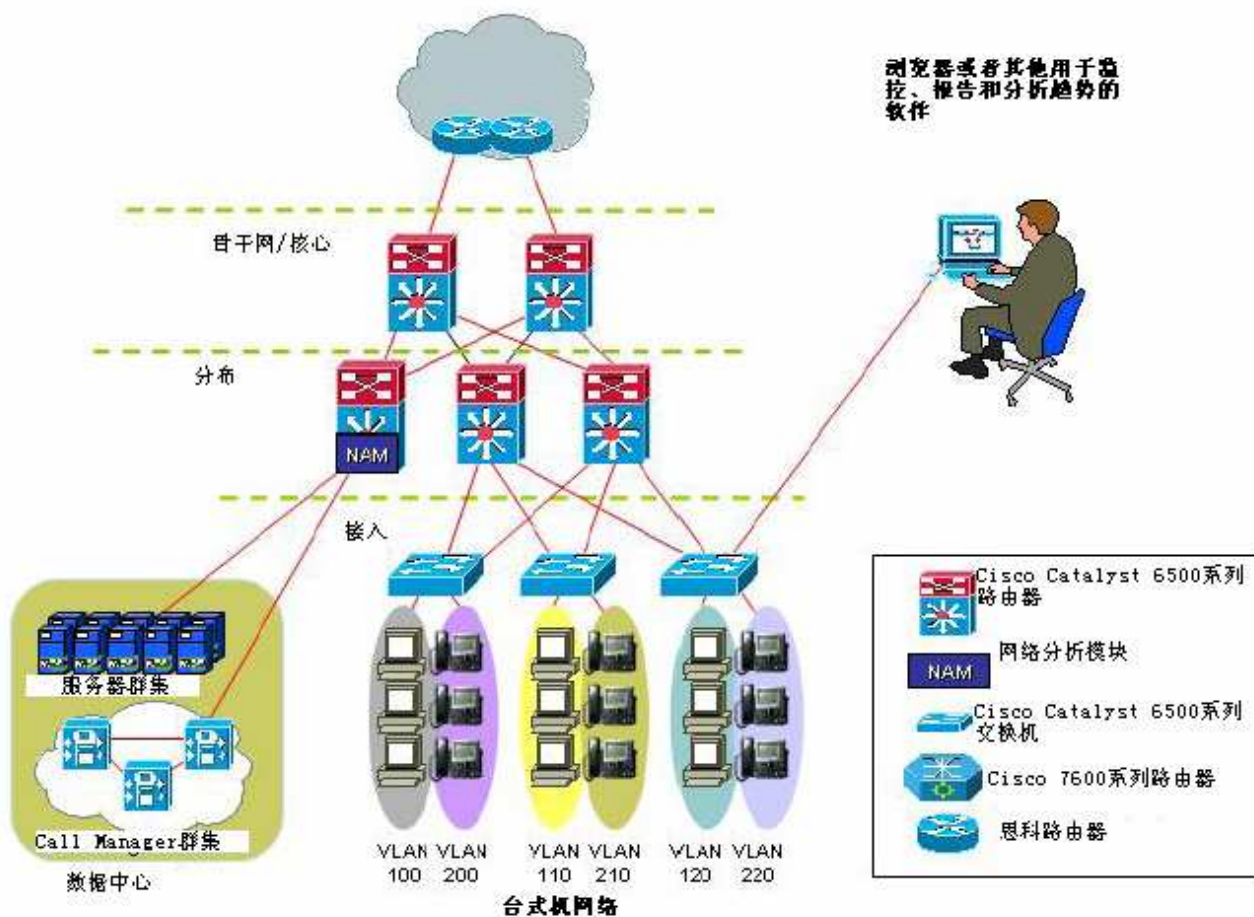
保障 NAM 的安全需要一些额外的工作。Ng 先生解释说：“为了提供必要的安全性，为不同的用户分配不同的分组捕获权限，必须在独立的、多层次的 TACACS 中使用 NAM。拥有 TACACS 帐号的应用支持部门和系统管理员将有权查看 NAM 显示界面。但是，分组捕获只能由网络工程师进行，因为需要在交换机和路由器上使用交换端口分析器和远程 SPAN 配置。”

为了从每个 NAM 获取数据，网络工程师或者管理员需要访问 NAM 上的、面向浏览器的 GUI，在相应的接口或者 VLAN 上设置数据捕获。可以利用一个互联网浏览器单独访问每个 NAM，以获取分组、解码分组和监控网络；另外，

可以利用 CiscoWorks 查看设备配置和布局。来自于多个 NAM 的数据可以被任何一个前端接口软件包搜集、存储和显示。思科 IT 部门最初选择 nGenius 实时显示器作为 CiscoWorks 打包解决方案的一部分，但是其他供应商的产品（包括 Concord、Infovista 和 NetScout）也可以有效使用。

NAM 刀片式模块使用 Cisco Catalyst 6500 或者 7600 系列机箱中的一个插槽。思科 IT 部门无法在高密度交换机中安装 NAM 刀片式模块，因而计划使用另外一个解决方案，即将 NAM 作为一个外置设备，采用一个配有 Supervisor Engine1 或者 2 模块的独立 Cisco Catalyst 6503 交换机机箱。但是，这个解决方案无法从交换机搜集 RMON 统计数据。当时，思科 IT 部门还没有发现搜集 RMON 统计数据的必要性。

图 1 思科 IT 部门目前使用的 NAM 监控数据中心网络



成效

尽管思科 IT 部门还没有具体评估使用 NAM 所带来的好处，但是 Ng 大概地介绍了他们所获得的成效：“到目前为止，这事儿一直很有意思。安装了 NAM 模块之后，我们在分组捕获方面遇到的问题少多了。利用 NAM，我们的管理员可以更加全面地了解背板的运行情况，从而得到了很多过去无法获得的信息。这些额外的信息让他们可以进行更

多的改动。通过分析背板的性能，我了解到了很多应用的情况。例如，在高峰期，我们的企业资源规划流量可能会达到 70% 的容量。在使用 NAM 之前，我只知道这个数字很高，但是我从来不知道它具体是多少。现在我终于知道了。它为我们增加了一个解决问题的工具。”

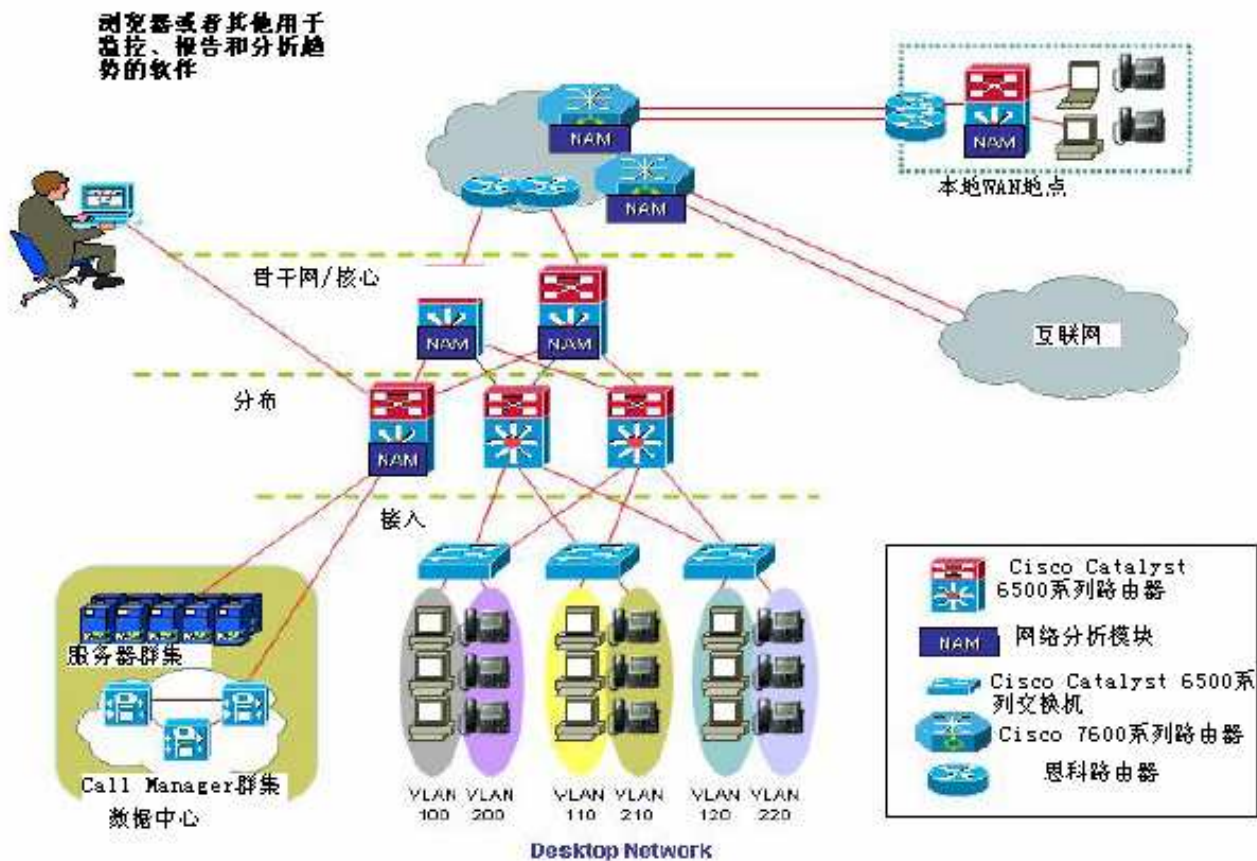
图 2 NAM 报告示例



下一步

思科 IT 部门正在设法为网络的功能和管理方式设计一个全面的、新一代的网络架构。NAM 是这种新的网络架构的重要组成部分。除了数据中心以外，IT 部门还计划在互联网环境（思科 CCO 和 Cisco.com）和核心骨干网中安装 NAM，因为 NAM 采用了独特的设计，可以在 Cisco Catalyst 6500 系列交换机和 Cisco 7600 系列路由器中使用（如图 3 所示）。它在这些环境中执行的功能都一样。思科正在计划将 NAM 推广到全球其他地方，包括亚太地区和欧洲。

图 3. 思科构想的未来 NAM 架构：监控数据中心、互联网接入和特定的 WAN 连接



思科 IT 部门还使用其他工具来进一步利用 NetFlow 信息，例如 Arbor PeakFlow 和 NetQoS Reporter Analyzer。“尽管 NAM 可以使用 NetFlow 数据和进行 NetFlow 分析，” Ng 表示。“但是如果现在要进行全面的网络分析，我相信我们需要使用 SNMP、NetFlow 细节信息、RMON、分组捕获和分析。我们还需要利用 NAM 数据来诊断 VoIP 流量。”

Ng 论述了思科关于进一步使用 NAM 的计划：“思科还将推出更多的网络分析技术。其中有些技术将被集成到 Cisco IOS 软件中，或者与其配合使用。随着这些技术的日益成熟，我认为我们将需要一种可以分析来自于不同来源的数据，构成完整的网络流量视图的网络管理软件。您必须关注所有网络组件——设备、应用、服务器和服务器群。它们的运行是否一切正常？NAM 可以帮助我们进行容量规划——利用 NAM 提供的信息，我们可以完成很多的任务。随着网络组件的不断增多，您需要更好的分析能力和分析工具。而 NAM 可以在这方面发挥关键的作用。”

如需查看思科的各个业务解决方案的更多 IT 案例研究，请访问 Cisco IT@Work 网站：

www.cisco.com/go/ciscoitatwork

注：

本文介绍了思科如何通过部署它自己的产品而获益。本文所介绍的成果和好处可能得益于很多因素；思科并不保证在其他场合下也能取得同样的成果。

思科是以原样提供本文的，不承诺任何明示或者默示的担保，其中包括对适销性或者适用性的担保。有些司法管辖区不允许排除明示或者默示的担保责任。在这种情况下，上述有关排除担保责任的规定可能不适用于您。



思科系统（中国）网络技术有限公司

北京

北京市东城区东长安街1号东方广场
东方经贸城东一办公楼19—21层
邮编：100738
电话：(8610)85155000
传真：(8610)85181881

上海

上海市淮海中路222号
力宝广场32—33层
邮编：200021
电话：(8621)33104777
传真：(8621)53966750

广州

广州市天河北路233号
中信广场43楼
邮编：510620
电话：(8620)85193000
传真：(8620)38770077

成都

成都市顺城大街308号
冠城广场23层
邮编：610017
电话：(8628)86961000
传真：(8628)86528999

如需了解思科公司的更多信息，请浏览<http://www.cisco.com/cn>

思科系统（中国）网络技术有限公司版权所有。

2005 ©思科系统公司版权所有。该版权和/或其它所有权利均由思科系统公司拥有并保留。Cisco, Cisco IOS, Cisco IOS标识, Cisco Systems, Cisco Systems标识, Cisco Systems Cisco Press标识等均为思科系统公司或其在美国和其他国家的附属机构的注册商标。这份文档中所提到的所有其它品牌、名称或商标均为其各自所有人的财产。合作伙伴一词的使用并不意味着在思科和任何其他公司之间存在合伙经营的关系。