

TS-01-0001

# 科来网络分析系统 6.9 技术白皮书

本档属商业机密文件，所有内容均为科来软件独立完成，属科来软件机密信息。未经科来软件做出明确书面许可，不得为任何目的、以任何形式或手段（包括电子、机械、复印、录音或其他形式）对本文档的任何部分进行复制、修改、存储、引入检索系统或者传播。

© 2009 科来软件 保留所有权利

技术支持部

科来软件

电话：86-28-85120922

传真：86-28-85120911

网址：<http://www.colasoft.com.cn>

邮件：[support@colasoft.com.cn](mailto:support@colasoft.com.cn)

# 目 录

目 录.....	1
1. 应用背景.....	3
2. 系统概述.....	3
3. 设计思想与工作原理.....	4
4. 关键技术.....	5
4.1 数据采集 .....	5
4.2 数据分析 .....	6
4.3 数据输出 .....	7
5. 安装部署.....	7
5.1 共享式网络 .....	7
5.2 交换式网络 .....	8
5.2.1 具备镜像功能的交换式网络 .....	8
5.2.2 不具备镜像功能的交换式网络 .....	9
5.2.3 定点分析一个部门 .....	10
5.3 代理服务器共享上网 .....	11
6. 主要功能特点.....	12
6.1 自动检测部署是否正确 .....	12
6.2 专家诊断 .....	12
6.3 流量分析 .....	13
6.4 协议分析 .....	13
6.5 节点浏览器 .....	13
6.6 自定义节点 .....	14
6.7 数据包过滤器 .....	14
6.9 数据包解码 .....	14
6.9 会话分析 .....	14
6.10 矩阵显示 .....	15
6.11 TCP数据流重组 .....	15
6.12 日志分析 .....	15
6.13 报表输出 .....	15
6.14 支持多工程和多网卡 .....	16
7. 技术指标.....	16
7.1 系统要求 .....	16
7.2 支持的协议 .....	16
7.3 解码的协议 .....	17
7.4 支持的网络类型 .....	17

---

7.5	支持的网络适配器 .....	18
7.6	支持的数据包格式 .....	18
7.7	日志分析模块 .....	18
7.8	TCP数据重组格式 .....	19
7.9	实时捕获解码分析 .....	19
7.10	时间精度 .....	19
<b>8.</b>	<b>备注.....</b>	<b>19</b>

# 1. 应用背景

目前，计算机网络的发展异常迅猛，各政府部门和企事业单位，都大量通过网络进行信息查询、邮件收发、数据共享等各种办公操作。由于计算机网络通信具备信息量大、更新速度快、信息价值高、信息处理和利用方便等优点，使得计算机网络通信已逐渐成为企事业单位日常工作不可或缺的一部份，整个社会已步入网络信息化时代。

网络的飞速发展给企业和用户带来了便利，但同时也对网络管理提出了严峻的挑战。局域网内部以及局域网与互联网之间过多的数据通信，使网络及网络设备在负载、工作效率以及安全性方面都承受着巨大的压力，网络时断时续、网络速度慢、网络遭受攻击却无法定位攻击源等故障一直制约着网络的正常运行。在这种情况下，管理人员必须对网络的流量占用、协议分布、通讯连接、数据包原始内容以及整个网络的运行情况了如指掌，才能在网络出现时断时续、不能正常上网、遭受攻击故障出现时，快速准确地定位故障点并将其排除。

网络中的数据传输是不透明的，在不借助网络分析系统的情况下，很难完成上述要求。所以，随着网络规模的不断扩大和网络应用的不断增多，网络故障必将变得日益复杂，网络攻击事件也必会不断增加。此时，保障整个网络的持续可靠和安全运行，将变得至关重要。在这种大的网络环境下，网络分析系统的普及将成为必然。

## 2. 系统概述

科来网络分析系统是一个集故障诊断、安全分析、性能评估于一体的综合网络分析系统，它通过捕获并分析网络中传输的底层数据包，有效反映网络通讯状况，帮助网络管理人员快速准确定位故障点并解决网络故障，同时，系统的专家诊断功能，可以使不具备技术能力的非技术人员，也能快速排查网络故障，从而规避网络安全风险，提高网络性能，增大网络可用性价值，并确保整个网络的持续可靠运行。

科来网络分析系统具备了行业领先的网络分析技术，它可以对当前复杂的网络进行精确分析，为排查网络故障、提升网络安全、评估网络性能提供最全面和深入的数据依据，是网络管理人员的必备工具。

科来网络分析系统的主要功能有：

- 分析网络中的流量占用情况；
- 分析内部网络和出口带宽的利用率情况；
- 分析网络中特定应用的数据通讯；

- 分析网络中特定主机的数据通讯；
- 分析网络中的异常数据通讯；
- 分析网络中的伪造 IP 和 MAC 地址攻击；
- 分析网络中的碎片和溢出攻击；
- 分析网络中的 DOS/DDOS/DRDOS 攻击；
- 分析网络中的 TCP 通信；
- 分析网络中的邮件收发是否正常；
- 分析网络中的 DNS 通讯是否正常；
- 分析网络中的 HTTP 网页访问是否正常；
- 分析网络中的 MSN 通讯是否正常；
- 网络中的 Yahoo Message 通讯是否正常；
- 分析网络中是否存在广播/组播风暴；
- 分析网络中传输的数据包是否正常；
- 分析网络的传输是否存在故障；
- 分析查找网络存在的环路故障；
- 分析查找网络中的蠕虫病毒攻击；
- 分析查找网络中感染病毒的机器；
- 分析查找网络速度慢故障；
- 分析查找网络时断时续故障；
- 分析查找内部用户无法上网故障；
- 分析网络中潜在的安全隐患；
- 分析查找网络中运行的扫描器以及扫描攻击；
- 分析查找网络中暴力破解用户名与密码攻击；
- 分析查找网络中针对 Web 服务器的攻击；
- 分析查找网络中的网卡、线路以及对端设备速率故障；
- 分析查找网络中是否存在使用 HTTP 代理的程序，如 QQ、MSN；

### 3. 设计思想与工作原理

在以太网中，所有通讯都是以广播方式工作，即任何主机发出的任意数据包，都会到达同一个网段内上的所有机器。每一个网络接口都有一个唯一的硬件地址，即 MAC 地址。在正常的情况下，一个网络接口只可能响应以下两种数据包：与自己 MAC 地址相匹配的数据包和发向所有机器的广播数据包。在实际的工作中，数据的收发一般都是由网卡完成的，网卡的工作模式有以下 4 种：

- 广播：这种模式下的网卡能接收发给自己的数据包和网络中的广播数据包。（默

认)

- 组播：这种模式下的网卡只能够接收组播数据包。
- 直接：这种模式下的网卡只能接收发给自己的数据包。
- 混杂：这种模式下的网卡能接收通过网络设备上的所有数据包。

从上面可知，虽然网卡在默认情况下仅能接收发给自己的数据和网络中的广播数据，但我们可以强制将网卡置于混杂模式工作，那么此时该网卡便会接收所有通过网络设备的数据，而不管该数据的目的地是谁。

科来网络分析系统的设计思想严格遵循以太网工作模式。在系统中，我们将网络中的每一部分都抽象为一种对象，如 IP 地址、物理地址、协议、数据包，将这些对象有机地结合起来，就构成了系统中用到的术语“工程”，而工程文件中不断变化的对象，则表示网络中相应数据通讯的实时变化。

科来网络分析系统基于以太网嗅探技术，以旁路接入的方式工作。系统首先将安装科来网络分析系统的机器上的网卡置为混杂模式，使其通过嗅探技术捕获网络中传输的所有数据包，然后将这些数据包传递到系统内部进行分析，再将分析结果实时显示在系统界面中，并自动诊断出网络中存在的故障。

## 4. 关键技术

### 4.1 数据采集

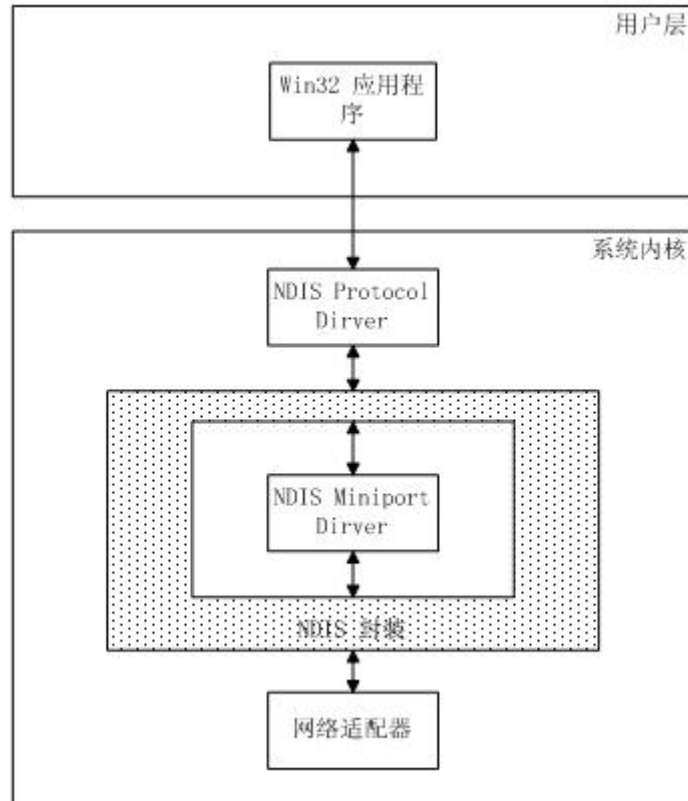
要对网络进行分析，首先需要对流经网络的数据包进行采集，数据采集工作在链路层进行，通过此操作能够获得网络中底层的以太网数据包。

科来网络分析系统可以通过三种方式完成数据的采集工作：

系统在 Windows 平台安装 Colasoft NDIS Protocol Driver，通过安装的协议驱动采集从网卡传送过来的数据包；系统在 Windows 平台安装 Colasoft NDIS intermediate Driver，通过安装的中间层驱动采集从网卡传送过来的数据包；系统在 Windows 平台安装 Colasoft TDI Driver，通过此驱动系统可采集不经过网卡的本地环回数据包；系统默认采用 Colasoft NDIS Protocol Driver 和 Colasoft TDI Driver，用户可依次选择工具>数据采集驱动>Colasoft NDIS intermediate Driver>安装，手动安装中间层驱动。

数据包采集的关键是效率，科来网络分析系统在内核层就对数据包进行过滤，并将不匹配过滤条件的数据包丢弃，以避免内核层到用户层的数据传送造成的资源浪费，以提高数据

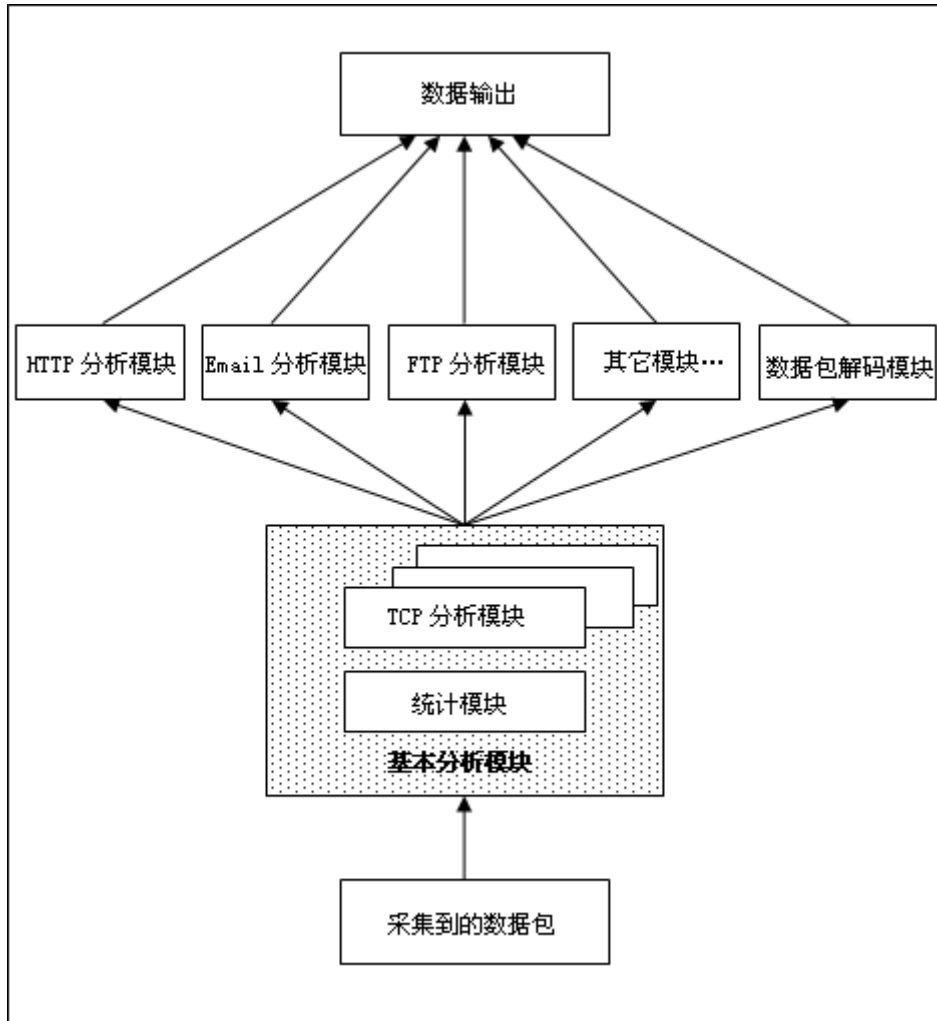
采集的效率。默认情况下科来网络分析系统的数据采集流程简图如图 1 所示。



(图 1 科来网络分析系统数据采集流程图)

## 4.2 数据分析

系统采集到符合过滤条件的数据包后，立即将这些数据包传送到系统内部进行分析。数据分析包括对数据包的统计、检测、解码、TCP 重组、协议分析等。科来网络分析系统的数据分析流程简图如图 2 所示。



(图 2 科来网络分析系统数据分析流程图)

## 4.3 数据输出

系统内部完成对数据包的分析后，立即将该数据包的分析结果通过系统界面反馈给用户，反馈的途径主要有视图、图表、日志、工程文件、数据包文件。

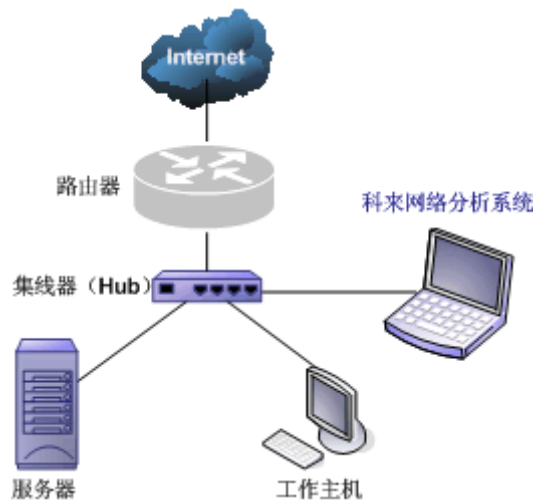
# 5. 安装部署

科来网络分析系统的典型部署方式有共享式网络，交换式网络和代理服务器共享上网三种类型。

## 5.1 共享式网络

如果网络的中心交换设备是集线器（Hub），那么数据包（所有数据包）都会发往除源

主机以外的所有机器。在这种情况下，科来网络分析系统可以安装在网络中任何机器上，相应的部署简图如图 3 所示。



(图 3 共享式网络安装部署图)

这种部署方式可以捕获网络中全部的通讯，其优缺点如下：

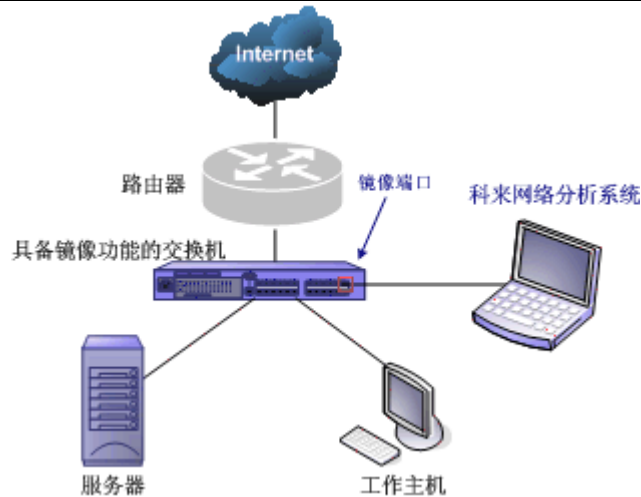
- **优点：** 不需添加设备、不用改变网络拓扑、安装位置任意。
- **缺点：** 网络瓶颈、信息泄密。

## 5.2 交换式网络

在交换式网络中，我们需要借助交换机的端口镜像功能，来帮助我们完成数据捕获。同时我们知道，某些交换机本身并不具备镜像功能。所以，下面我们从交换机具备镜像、交换机不具备镜像、以及定点分析一个部门这三个方面，说明科来网络分析系统在交换式网络中的部署情况。

### 5.2.1 具备镜像功能的交换式网络

如果中心交换设备是交换机，且该交换机具备镜像功能，则称此网络为具备镜像功能的交换式网络。在这样的网络中，请首先在交换机上配置好端口镜像，然后将科来网络分析系统安装在连接交换机镜像端口的机器上，其部署简图如图 4 所示。



(图 4 具备镜像功能的交换式网络安装部署图)

镜像端口的设置不同，捕获到的数据也会存在差异，而镜像端口的设置原则，请根据用户的需求而定。

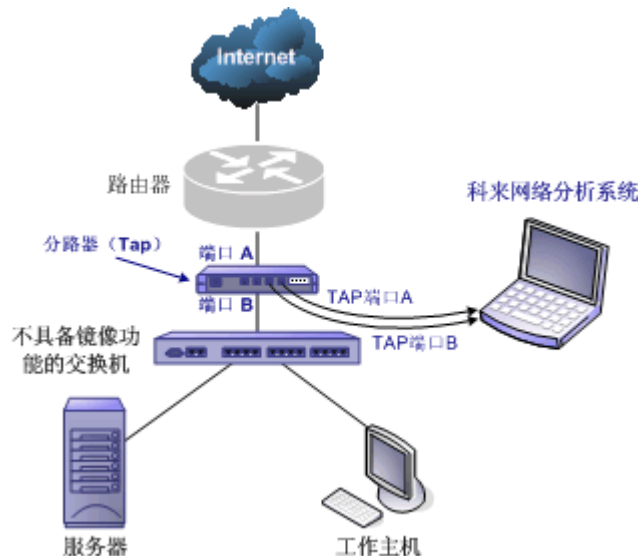
- 如果需要查看整个网络与 Internet 的通讯情况，请将与路由器相连的交换机端口设置为被镜像口；
- 如果需要某几台机器的通讯情况，请将连接这几台机器的交换机端口设置为被镜像端口；
- 如果需要查看整个网络的通讯情况（包括访问 Internet，以及内部通讯），请将交换机上除镜像端口和连接路由器的端口以外的所有端口设置为被镜像端口。

这种部署方式的优缺点如下：

- **优点：** 不需添加设备、不用改变网络拓扑。
- **缺点：** 交换机必须具备镜像功能。

## 5.2.2 不具备镜像功能的交换式网络

如果中心交换设备是交换机，但该交换机不具备镜像功能，则称此网络为不具备镜像功能的交换式网络。在这样的网络中，需要在交换机与路由器之间串接一个分路器（Tap）或集线器（Hub），然后将安装科来网络分析系统的机器连接到这个分路器（Tap）或集线器（Hub）上，最终的部署简图如图 5 所示。



(图 5 不具备镜像功能的交换式网络安装部署图)

图 5 中串接在路由器和交换机之间的分路器 (Tap)，也可以用集线器 (Hub) 替换。

分路器 (Tap) 内部能自动完成单向或双向的数据复制，从而使科来网络分析系统能捕获分析单向或双向的网络通讯。

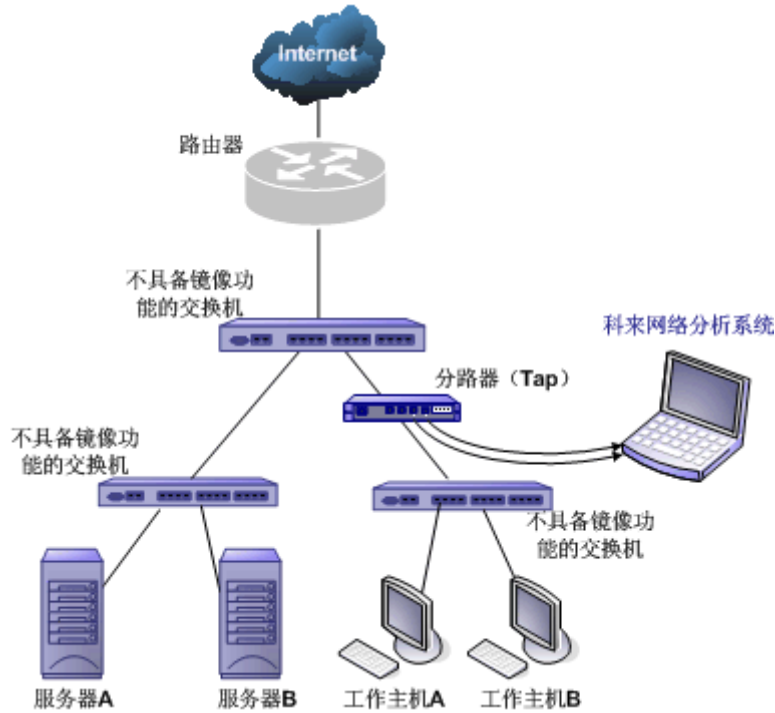
请注意，此时交换机内部主机间的通讯将不会到达分路器，所以这种情况下，科来网络分析系统只能捕获进出的数据通讯。

这种部署方式的优缺点如下：

- **优点：** 部署灵活方便、可捕获单向数据。
- **缺点：** 需添加分路器，只能捕获进出通讯。

### 5.2.3 定点分析一个部门

实际网络中，可能拓扑结构非常复杂，在进行网络分析时，往往并不需要分析整个网络的数据，而只需对某些异常的部门进行定点分析。在这种情况下，可以将科来网络分析系统安装在笔记本上，同时配备一个分路器 (Tap) 或集线器 (Hub)，参照 5.2.2 的方法，就可以轻松地对一个部门进行定点分析了，其部署简图如图 6 所示。

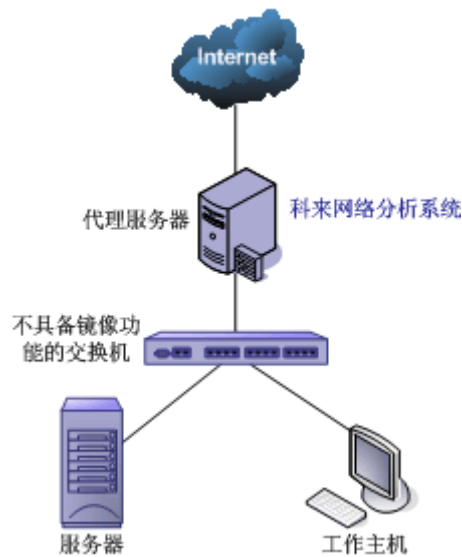


(图 6 定点分析一个部门的安装部署图)

这种部署方式实际上是 5.2.2 的放大，其优缺点和 5.2.2 完全一致。

### 5.3 代理服务器共享上网

目前，存在许多使用代理服务器共享上网的小型网络。如果需要对这样的网络进行分析，请直接将科来网络分析系统安装到代理服务器上，其部署如图 5 所示。



(图 5 代理服务器共享上网的安装部署图)

注意：这种情况下，需要同时对代理服务器的内网卡和外网卡进行数据捕获。且此时交换机内部主机间的通讯将不会到达代理服务器，科来网络分析系统只能捕获进出的数据通讯。

这种部署方式的优缺点如下：

- **优点：**简单方便。
- **缺点：**降低分析效率，只能捕获进出通讯。

## 6. 主要功能特点

科来网络分析系统与其它同类产品相比，具备许多独创功能，现在将其中最主要的几点简单介绍如下：

### 6.1 自动检测部署是否正确

科来网络分析系统提供了安装部署检测向导，通过该向导，用户可以快速检查自己的安装部署是否正确，以保障数据捕获的完整性。

### 6.2 专家诊断

专家诊断是科来网络分析系统 6.9 的特色功能之一，它可以将捕获到的数据进行智能化的分析，对网络内的错误信息或故障信息，进行自动提示，用户不必去了解数据包的详细内容，便可以对网络故障进行排查。

诊断视图分为上下两个视图，上面的视图是按照 OSI 七层协议对错误信息进行分组，目前产品支持四个层次的故障诊断：应用层、传输层、网络层和数据链路层。同时，网络错误和故障都有安全级别的划分，如下表所示。

安全级别	描述
消息	普通信息通知，只是用来记录某个事件，并没有网络错误。
注意	对网络事件或特定事件进行提示，需要用户引起重视的内容。
警告	对错误或故障进行警告提示，用户应该及时处理。
危急	这是对严重错误或严重故障进行提示，用户需要及时处理。

## 6.3 流量分析

流量分析是科来网络系统的主要功能之一，通过此功能，用户可以快速找定位通讯量最大的 IP 主机点和物理主机。系统还支持每个网络协议的端点流量明晰统计排名，比如用户可以知道 HTTP 协议下前 5 个 IP 主机。

科来网络分析系统的流量分析功能，可以分析出网络中的具体流量占用情况，如总流量最大的主机、发送流量最大的主机、接收流量最大的主机、收发数据包数最多的主机、发送数据包最多的主机、接收数据包最多的主机、内部流量、以及广播流量最大的主机等信息。通过这些信息，我们可以确定网络中是否广播/组播风暴，并帮助用户排查网络速度慢、网络时断时续、蠕虫病毒攻击、DOS 攻击、以及用户无法上网等网络故障。

## 6.4 协议分析

科来网络分析系统的协议分析功能，根据实际的网络协议封装顺序，层次化展现给用户，每个协议有自己的色彩，除了全局的协议统计，还可提供每个网络端点下的协议统计数据。

协议视图可以有效显示网络中数据通讯所使用的协议，协议采用树状层级方式显示，对每一种协议，都对其占用的流量、使用此协议的数据包个数、此协议的流量在总流量中的百分比、以及使用此协议的数据包在总数据包中的百分比进行了统计。通过协议视图对各视图占用流量及百分比的统计，用户可以得出当前网络中占用流量最多的协议，即当前网络中占用流量最多的服务类型；并帮助用户排查网络速度慢、邮件蠕虫病毒攻击、网络时断时续以及用户无法上网等网络故障。

## 6.5 节点浏览器

节点浏览器是科来网络分析系统的最主要特色功能之一，它的界面类似于 Windows 资源管理器，简单易用。节点浏览器主要为用户提供显示过滤功能。通过该功能，用户可以快速查看一个 MAC、一个 IP、一个网段、一个部门甚至一个范围的通讯情况。

节点浏览器的节点类型有三种，它们是协议、物理端点和 IP 端点。每种节点类型，均从其特殊的视角对网络进行分析。

- 按协议浏览。以网络中通讯的服务为观察视角，查看网络中通讯服务的具体情况。
- 按物理端点浏览。以网络物理拓扑为观察视角，查看网络中物理主机的通讯情况。
- 按 IP 端点浏览。以逻辑子网为观察视角，查看网络中 IP 主机和 IP 子网的通讯情况。

## 6.6 自定义节点

科来网络分析系统具备自定义节点功能，当使用自定义节点后，节点浏览器将根据用户自定义的方式显示节点，从而提高分析效率。如公司有研发部、技术部、市场部、行政部，那么我们可以在网络配置对话框中，对这几个部门进行定义，配置好后，节点浏览器中将直接显示研发部、技术部、市场部、行政部节点。

## 6.7 数据包过滤器

科来网络分析系统的数据包过滤器，是一种根据用户定义的规则和策略，从而实现数据筛选的技术。通过使用过滤器，可以减少数据干扰、利于网络分析、降低系统负载，从而提高分析效率。默认情况下，系统不会使用任何过滤器，此时，网络中的所有数据包都会被系统捕获分析。

科来网络分析系统的数据包过滤器，提供接受和拒绝的两种状态，同时系统允许同时使用接受和拒绝的过滤条件，同时添加两种过滤条件后，系统将首先匹配拒绝条件，再匹配接受条件。

科来网络分析系统可自定义的过滤条件有 6 种，它们是地址、端口、协议、数据包大小、数据包值、数据包值和数据包模式匹配。其中，地址、端口和协议三种过滤条件，由于其使用的频率较高，且相对易用，故我们称它们为简单过滤器，另外三种称为高级过滤器，在高级过滤器，用户可以对上述的 6 种过滤条件进行任意逻辑（与、或、非）组合。

## 6.8 数据包解码

科来网络分析系统可以对捕获到的数据包进行实时解码，解码的格式包括概要解码、字段解码、十六进制解码，ASCII 和 EBCDIC 解码。通过查看数据包解码信息，用户可以更全面地了网络中传输的原始解数据包信息，并确定是否伪造网络攻击。

## 6.9 会话分析

科来网络分析系统的会话功能，可以统计会话的源地址、目标地址、该会话收发的数据包及这些数据包的大小等信息。通过对会话视图的查看，管理人员可以：

- 查看两台 MAC 主机和 IP 主机之间的通讯内容。
- 分析网络中是否存在 TCP 端口扫描攻击。
- 分析网络中是否存在基于 TCP 协议的服务的账户用户名密码破解攻击。
- 分析网络中是否存在邮件蠕虫病毒攻击。

- 分析网络中是否存在长时间连接且流量小的 TCP 连接(QQ/MSN 等程序使用 HTTP 代理即为此现象)。
- 网络中是否存在 UDP 端口扫描攻击。

## 6.10 矩阵显示

科来网络分析系统提供的矩阵视图,可以直观地统计网络中通讯的节点和会话信息。通过矩阵视图,可以看到如下信息:

- 整个网络通讯的节点信息。
- 整个网络通讯的会话信息。
- 某台物理主机的通讯节点信息。
- 某台 IP 主机的通讯会话信息。
- 某台物理主机的通讯节点信息。
- 某台 IP 主机的通讯会话信息。
- 某条会话的主机信息。

## 6.11 TCP数据流重组

科来网络分析系统可以将捕获到的 TCP 数据数据包,按照数据传输的原始顺序,重组成为 TCP 流。通过查看 TCP 数据流中的具体信息,你可以轻松地跟踪每个网络通讯的整个过程,并确定网络中的乱序传输故障。从而有效地掌控网络中的数据通讯情况。

## 6.12 日志分析

科来网络分析系统的日志分析功能,可对网络中的 HTTP 网页访问、Email 邮件收发、DNS 域名解析、MSN 通讯和 Yahoo Message 的通讯进行快速分析,并将分析结果输出到系统的日志视图,同时还允许用户将这些信息保存为日志,以备存档和日后查看。

## 6.13 报表输出

科来网络分析系统的报表功能,可以将任意节点的分析结果以报表的形式输出。

报表信息主要包含统概要统计的全部内容、协议使用统计明细、流量最大的前 10 个 IP 地址、前 10 个 MAC 地址以及各种图形统计结果。同时,系统还允许用户将报表以 html 格式保存在硬盘。

## 6.14 支持多工程和多网卡

系统网络分析系统支持多个工程同时运行，且在每个工程中，都可以设定同时采集一个或多个网卡的数据包，多个工程也可以同时采集一个网卡的数据包。

# 7. 技术指标

科来网络分析系统的技术指标有以下几点：

## 7.1 系统要求

### 1. 最低配置：

- P4 1.2G CPU
- 512 MB RAM
- Internet Explorer 5.5 or higher

### 2. 推荐配置：

- P4 3.0G CPU
- 1 GB RAM or more
- Internet Explorer 6.0 or higher

### 3. 支持的操作系统：

- Windows 2000 (SP 4 or later)
- Windows XP (SP 1 or later) and 64bit Edition
- Windows Server 2003 and 64bit Edition
- Windows Vista and 64bit Edition
- Windows Server 2008 and 64bit Edition

## 7.2 支持的协议

科来网络分析系统支持非常多的协议，几乎包括了常见的所有协议，包括：AARP, AARP Prbe, AARP Request, AARP Response, ACNET, AFP, AH, AIM, ARP, ARP Request, ARP Response, Auditd, BFTP, BGP, BOOTP, Biff, BitTorrent, CDC, CDP, CFS, CFTP, CGMP, CIFS, CMIP-Agent, CMIP-Man, COPS, CRIP, CRTP, CRUDP, CTF, Cisco-fna, Cisco-sys, Cisco-tna, Citrx ICA, DCCP, DCP, DDP, DECnet, DHCP, DIAG, DNS, DNS Error, DNS Query, DSR,

Daytime, Discard, EGP, EIGRP, EIGRP Hello, EIGRP Query, EIGRP Reply, EIGRP Update, ESP, Echo, Emfis-cntl, Emfis-data, Ethernet - Other, Ethernet 802.2, Ethernet 802.3, Ethernet II, Ethernet SNAP, Ethernet SNAP - Other, eMule, FC, FCoE, FCP, FTP, FTP Ctrl, DTP Data, Finger, GDP, GGP, GRE, GTP, Gopher, H.225, H.323, HMP, HSRP, HTTP, HTTP Proxy, HTTPS, Http-mgmt, IBM-app, ICMP, ICMP DestUnreach, ICMP Echo Reply, ICMP Echo Req, ICMP Redirect, ICMP Time Ex, ICMPv6, ICP, IDFP, IDPR, IDRP, IGAP, IGMP, IGRP, IMAP, IAMP3, IAMP4, IMAP4/SSL, IP, IP - Other, IP Fragment, IPX, IPv6, IRC, IRC/SSL, IRTP, ISL, ISMP, ISO-IP, ISO-TP0, ISO-TP4, Kerberos, L2F, L2TP, LDAP, LDAPS, LPD, La-maint, Login, Loopback, MGCP, MPLS, MPLS Etype2, MPM, MPM-snd, MPP, MSN, MSP, MSRDP, MSSQL, Mcidas, Mit-ml-dev, Mnet-discovery, Mobile IP, Msg-auth, NAMP, NARP, NBDGM, NBIPX, NBNS, NBSSN, NCP, NETBLT, NFS, NLSP, NMSP, NNTP, NNTP/SSL, NPP, NSRMP, NTP, Nameserver, NetBEUI, NetBIOS, Ni-ftp, OSPF, OSPF DDs, OSPF Hello, OSPF LSA, OSPF LSR, OSPF LSU, PIM, PIP, PIPE, POP2, POP3, POP3/SSL, PPP, PPP CHAP, PPP FCC, PPP IPCP, PPP LCP, PPP LQP, PPP PAP, PPP Padding, PPPoE, PPPoE Discovery, PPPoE Session, PPTP, PPlive, PRM, PTP, PUP, PVP, Password-chg, Pdap, Pwdgen, Q.931, QQ, QQ keep Alive, QQ Login, QQ Logout, QQ Other, QQ Recv Msg, QQ Send Msg, Qotd, RAMP, RAP, RARP, RARP Request, RARP Response, RCP, RDP, RGMP, RIP, RIP Reply, RIP Request, RIPX, RIPv1, RIPv2, RIPv3, RIPv4, RIS, RJE, RLOGIN, RLP, RPC, RSH, RSVP, RSVP\_tunnel, RTCP, RTELNET, RTP, RTP AV, RTP Audio, RTP CelB, RTP DVI4, RTP Dynamic, RTP G.711, RTP G.723, RTP G.728, RTP G.729, RTP GSM, RTP H.261, RTP H.263, RTP JPEG, RTP MP2T, RTP MPV, RTP Video, RTSP, Radius, Radius-acct, Radius-dynauth, Re-mail-ck, Rexec, Rtsps, Rwhois, SAP, SAP, SAP Reply, SAP Request, SCC Security, SCCP, SCTP, SDRP, SER, SFTP, SGMP, SGMP-traps, SIP, SKIP, SLP, SMB, SMTP, SMTP/LSA, SMTP/SSL, SNMP, SNMP Trap, SNP, SNPP, SPS, SPX, SQL, SSDP, SSH, SShell, STP, Send, Sflow, Statsrv, Submission, Supdup, Swift-rvf, Systat, T.120, TCP, TCP - Other, TELNET, TFTP, TLSP, TNS, TRIP, Tacacs, Tacacs-ds, Tacnews, Time, Tunnel, UDP, UDP - Other, ULS, UMA, VLAN, VLAN EType2, VRRP, WINS, Who, WhoIs, Windows NLB, X-Window, X.400, XDAS, XNS, XNS-auth, XNS-ch, XNS-mail, XNS-time, Yahoo Messenger

## 7.3 解码的协议

AH, ARP, BGP, BitTorrent, BOOTP, CDP, CGMP, CIFS, COPS, DHCP, DNS, EGP, EIGRP, eMule, ESP, Ethernet 802.2, Ethernet 802.3, Ethernet II, Ethernet SNAP, Finger, FCoE, FTP Ctrl, FTP Data, GGP, Gopher, GRE, HSRP, HTTP, ICMP, ICMPv6, ICP, IGMP, IGRP, IP, IPv6, IPX, ISL, ISMP, L2F, L2TP, LPD, MPLS, MSN, MSSOL, NBDGM, NBNS, NBSSN, NCP, OSPF, POP3, PPP, PPP CHAP, PPP IPCP, PPP LCP, PPP PAP, PPPoE, PPPoE Discovery, PPPoE Session, PPTP, QQ, RARP, RGMP, RIPv1, RIPv2, RSVP, SAP, SCTP, SMB, SMTP, SPX, SSH, TCP, TELNET, TFTP, TNS, UDP, VLAN, VRRP。

## 7.4 支持的网络类型

科来网络分析系统支持的网络类型有：

- 10M 以太网
- 100M 以太网
- 1000M 以太网

## 7.5 支持的网络适配器

科来网络分析系统支持以下两种类型的网络适配器：

- 10M/100M/1000M 以太网适配器
- 本地回环接口（Windows 2000/XP/2003）

## 7.6 支持的数据包格式

科来网络分析系统支持多种类型的数据包文件，具体如下：

- Colasoft Capsa packet file (\*.cscpkt)
- Colasoft Capsa 4.0 packet file (\*.cpf)
- Sniffer packet file (\*.cap)
- EtherPeek packet file (\*.pkt)
- AiroPeek packet file (\*.pkt)
- Omnipeek packet file (\*.pkt)
- Raw packet file (\*.rawpkt)
- Libpcap (\*.cap)
- Libpcap (\*.dmp)
- Microsoft Network Monitor 2.x (\*.cap)

## 7.7 日志分析模块

科来网络分析系统包含 5 个日志分析模块：

- 1) 邮件分析
- 2) HTTP 分析
- 3) DNS 分析
- 4) MSN 通讯
- 5) 雅虎通通讯

## 7.8 TCP数据重组格式

TCP 数据流的重组信息，可使用 ASCII 或者 EBCDIC 两种格式进行显示。

## 7.9 实时捕获解码分析

科来网络分析系统对网络中的数据包进行实时捕获、实时解码、实时分析。

## 7.10 时间精度

科来网络分析系统的数据包捕获时间精确到微秒级。

# 8. 备注

科来网络分析系统是一个网络分析系统，对使用人员有一定的网络技术要求。只有在最大掌握一定前置知识的情况下，才能最大限度发挥该系统在网络管理、网络分析以及网络故障排查方面的作用。

使用人员需具备的网络技术知识包括：

- 以太网基础：了解以太网工作原理。
- TCP/IP：了解 IP 地址、MAC 地址、常用协议的使用。
- 网络设备：了解集线器、交换机、路由器、防火墙等设备的工作原理。
- 端口镜像：了解常见交换机的端口镜像配置。

关于科来网络分析系统更多更详细的信息，请参见系统的官方网站<http://www.colasoft.com.cn>。