

科来网络分析系统 2010

技术白皮书

本档所有内容均为科来软件独立完成,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)对本档的任何部分进行复制、修改、存储、引入检索系统或者传播。

© 2010 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

目录

目录	1
1. 前言	3
2. 工作原理	3
3. 技术架构	4
3.1 总体架构	4
3.2 第二代分析引擎	4
3.3 数据采集	5
3.4 数据分析	6
3.5 数据输出	7
4. 系统技术特性	7
4.1 全新的分析引导体验	7
4.2 实时分析和回放分析	8
4.3 全新的网络档案	8
4.4 实用的分析方案	8
4.5 灵活的图表设置	9
4.6 自定义协议	9
4.7 专家诊断	9
4.8 流量分析	10
4.9 协议分析	10
4.10 在线实时警报	10
4.11 节点浏览器	11
4.12 自定义节点分组	11
4.13 数据包捕捉过滤	11
4.14 数据包解码	12
4.15 会话分析	12
4.16 矩阵显示	12
4.17 TCP 会话时序图	12
4.18 TCP 数据流重组	13
4.19 日志分析	13
4.20 报表输出	13
4.21 支持多工程和多网卡	13
5. 系统核心功能	13
5.1 全面的流量分析	14
5.2 智能的故障诊断	14
5.3 清晰的协议分析	15

5.4 详细的连接分析.....	15
5.5 强大的安全分析.....	15
5.6 精细化的性能评估	16
5.7 丰富直观的报表.....	16
6. 技术指标.....	17
6.1 网络类型	17
6.2 运行环境.....	17
6.3 支持的网络适配器	17
6.4 支持的数据包格式	17
6.5 支持的诊断事件.....	18
6.6 支持的协议.....	18
6.7 解码的协议.....	19
6.8 实时捕获解码分析	20
6.9 时间精度.....	20
7. 联系我们.....	20

1. 前言

近二十年来，计算机网络技术得到了飞速的发展，网络速度越来越快，使用越来越简单方便，越来越多的关键业务运行在计算机网络基础之上，越来越多的重要信息通过网络传送，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。网络规模的不断扩大，网络越来越复杂，应用环境也越来越复杂，网络中的数据流量越来越大，如何保障网络的持续、安全、高效运行是网络运行维护人员面临的巨大挑战。在这种情况下，网络运行维护人员必须对网络的流量占用、应用分布、通讯连接、数据包原始内容等所有网络行为以及整个网络的运行情况进行充分的了解和掌握，才能在网络出现性能和安全问题时，能够快速准确的分析问题原因，定位故障点和攻击点并将其排除，从而实现网络价值最大化。

科来网络分析系统通过对捕获到的底层数据包进行全面、系统的解码、分析、诊断，并将结果体现于直观、易懂的界面或报表中，让管理者可以快速地了解网络状况。通常，网络分析能为管理者提供故障、安全、性能、升级规划、网络监控、网络基线等关键数据。通过这些数据可以获取网络的全景信息，建立主动防御机制，为保障网络的持续可靠运行提供夯实的数据基础，并且极大的降低网络管理成本。

2. 工作原理

在共享式以太网中，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

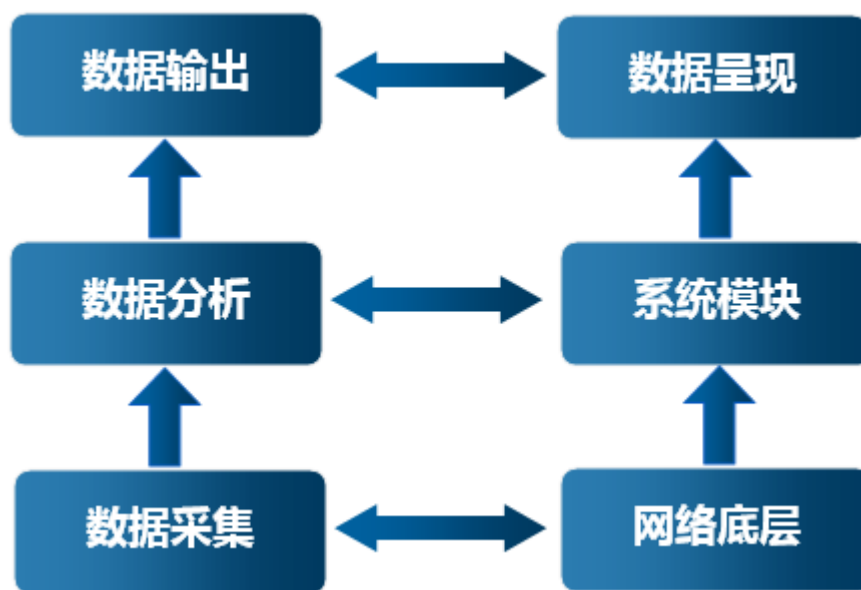
工程文件中不断变化的对象，则表示网络中相应数据通讯的实时变化。

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。

3. 技术架构

3.1 总体架构

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 2010 通过对网络底层数据包的实时采集、检测及分析，最后直观的输出分析结果。系统的整体架构如下图所示。



- ☐ 首先，系统在网络底层进行实时的数据采集，以获得真实、准确的数据来源；
- ☐ 采集到数据来源后，交给系统的各种分析模块进行实时诊断和分析，如专家诊断模块、统计模块、数据包解码模块等进行详细的分析；
- ☐ 最后将分析结果输出，通过各种方式直观的呈现给用户。

系统架构清晰、直观，将复杂、抽象的网络通讯信息以简单明了的方式输出呈现给用户。

3.2 第二代分析引擎

科来网络通讯分析平台依托科来第二代网络分析引擎，它采用科来自主研发的 CSDOM 动态对象模型，大幅度

提高程序执行效率，保证了海量数据下的分析性能，同时还拥有以下多种新技术，新特性。

多线程并发分析

- 由原来单线程分析提升到多线程分析，充分利用 CPU 多核化实现并发分析，大幅提高分析性能

MCB 多循环缓存技术

- 多个缓存区循环使用
- 分析和访问数据并行化，避免分析和查询相互等待的情况
- 大幅提高抓包效率和分析效率，同时减少内存碎片的产生

异步通讯机制

- 分离分析和视图显示，提高分析性能

协议速查技术

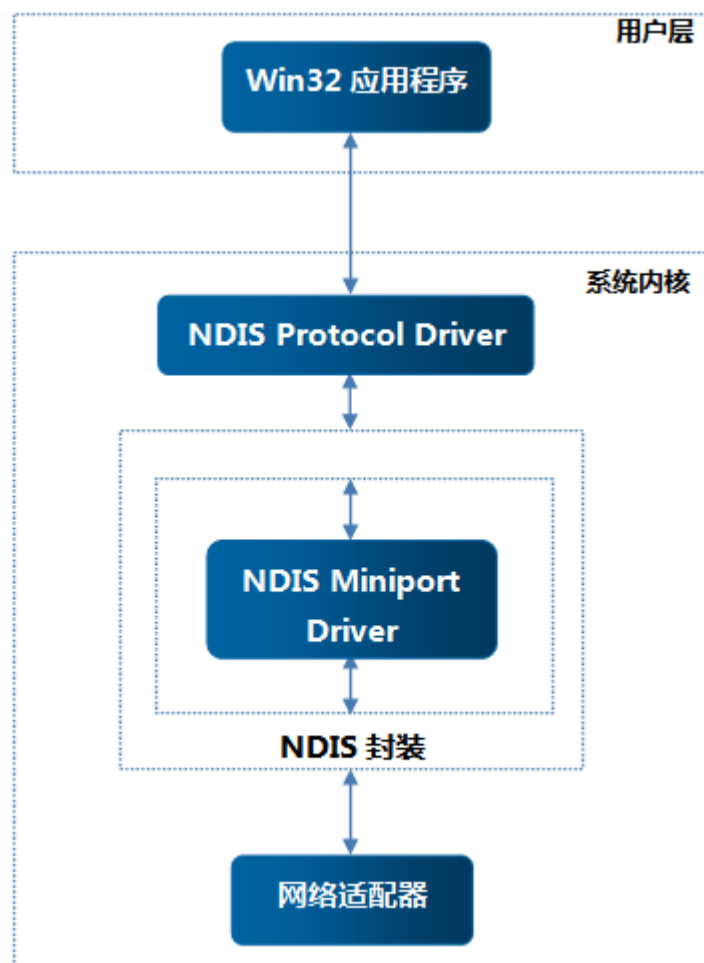
- 动态生成协议树
- 高效识别
- 支持用户自定义协议

3.3 数据采集

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。

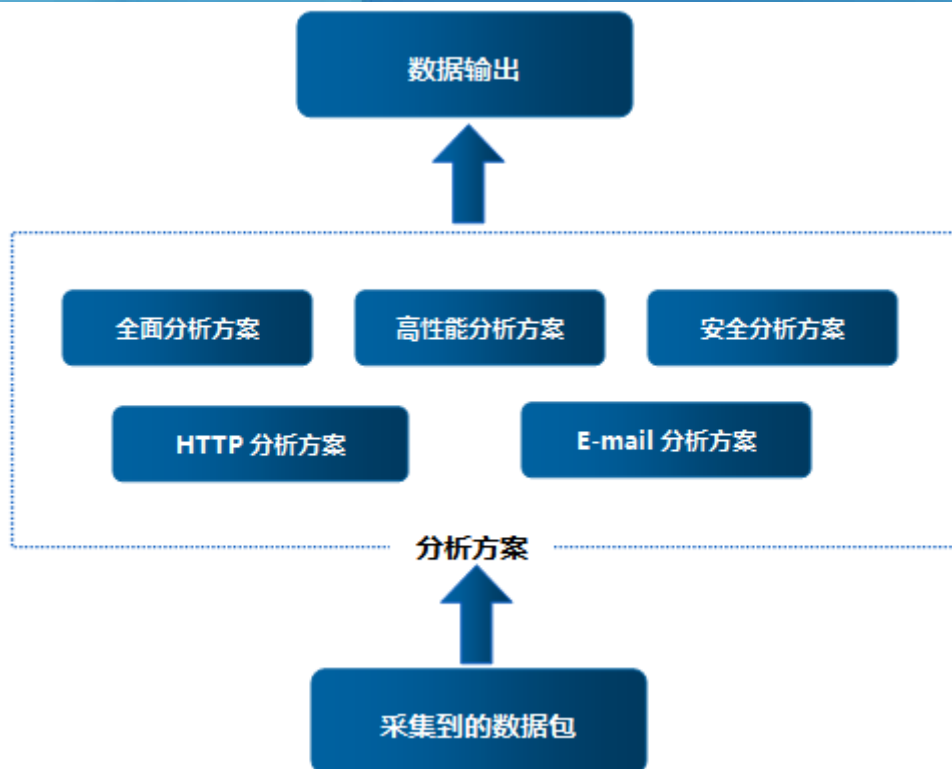
数据包采集的关键是效率，科来网络分析系统在内核层就对数据包进行过滤，并将不匹配过滤条件的数据包丢弃，以避免内核层到用户层的数据传送造成的资源浪费，以提高数据采集的效率。默认情况下科来网络分析系统的数据采集流程简图如图 1 所示。



(图 1 科来网络分析系统数据采集流程图)

3.4 数据分析

科来网络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 数据流重组、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)

3.5 数据输出

如图 2 所示，系统将采集到的数据包经过详细、深入的分析后，将分析结果以多种方式输出，即通过系统主视图区、对话框界面等呈现各类数据信息，输出方式包括图表、报表、数据分组/分类等多种方式，而输出内容包括数据包解码，端点，协议，IP 流，TCP 流、会话、日志等详细的各类通讯数据。

4. 系统技术特性

科来网络分析系统具备许多独创功能，下面将介绍其中最主要的功能：

4.1 全新的分析引导体验

在程序初始的开始页中以简单、直观的视图引导用户完成网络分析任务；通常一个分析任务采用以下 6 步完成：

1) 选择分析模式

- 提供两种数据采集分析模式，实时分析和回放分析
- 在实时分析模式中可选择设置网络适配器
- 在回放分析模式中可选择文件和回放速度

- ☒ 两种模式都可以另外设置数据包捕捉过滤器
- 2) 选择网络适配器
 - ☒ 选择用于采集数据的网络适配器，可以同时选择一块或多块网卡进行数据捕获
- 3) 设置数据包捕捉过滤器
 - ☒ 新建数据包捕捉过滤器，快速捕获数据来源
- 4) 选择网络档案
 - ☒ 新建空白网络档案
 - ☒ 导入保存的网络档案
- 5) 选择分析方案
 - ☒ 根据实际需求，有针对性地选择相关分析方案，以达到最佳分析应用。
- 6) 开始分析

4.2 实时分析和回放分析

科来网络分析系统 2010 提供实时和回放两种分析策略，实时分析以网络适配器作为数据采集来源，提供直观的适配器流量状态显示；回放分析以数据包存储文件为第二分析数据源，支持原速回放和快速回放，方便用户进行回溯分析。

4.3 全新的网络档案

科来网络分析系统 2010 提出了全新的网络档案概念。网络档案是针对不同网络环境的一组设置，包括网络带宽、网络分组、名字表以及警报设置。

在实际的网络环境中，用户可以自定义配置和保存网络档案，用于保存网络环境中的各项关键数据信息。您可以导入/导出网络档案，在后续的分析任务中，可直接调用保存网络档案进行分析。

4.4 实用的分析方案

科来网络分析系统 2010 提供常见的面向网络业务应用的分析方案，包括高性能分析，精确分析，常见应用协议分析。详见下表：

方案类型	分析方案	描述
基本分析	高性能分析	提供最高性能的分析。包括物理地址，IPv4 地址，分组统计，IP/TCP/UDP 流分析。支持全千兆的实时分析。
	全面分析	全面、详细的分析网络中所有应用及流量
应用分析	HTTP 应用分析	面向 HTTP 应用分析。提供客户端，服务器端流量统计，故障和性能诊断，日志保存。
	FTP 高级分析	面向 FTP 应用分析，提供日志保存。
	邮件应用分析	面向 SMTP/POP3 应用分析，提供长期日志和邮件副本保存。
	DNS 应用分析	提供 DNS 应用诊断分析，日志保存
内置分析	TCP 性能分析	提供 TCP 响应时间分析，为基于 TCP 传输的上层应用提供精准的分析报告。

4.5 灵活的图表设置

科来网络分析系统 2010 提供了强大的图表自定义功能，为用户提供丰富的图形化流量实时监控视图。您可以非常方便的自定义添加图表面板，每个图表面板又可任意添加各种类型的图表。

系统不仅支持全局的图表设置，也可针对具体的网络对象进行图表创建和添加，并且，包括 TCP 会话的详细数据信息、应用流量信息以及告警数据信息等，都可创建实时的图表监控，使用户能够更直观的看到各种网络参数的实时运行数据。

4.6 自定义协议

科来网络分析系统 2010 具有强大的自定义协议功能，用户可以跟据实际情况按以下 4 种类型字段进行协议自定义。

- 1) 以太网类型
- 2) IP 协议编号
- 3) TCP
- 4) UDP

4.7 专家诊断

专家诊断是科来网络分析系统的特色功能之一，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全部内容，便可以对网络故障进行排查。

诊断视图进行了全新的视图布局，不仅提供详细的诊断事件、与主机关联的诊断事件日志，而且详细显示每个诊断事件的详细信息以及事件参考信息。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。

4.8 流量分析

流量分析是科来网络分析系统的主要功能之一，通过此功能，用户可以快速查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，比如用户可以快速定查找网络中使用 HTTP 协议的前 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。

4.9 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。

4.10 在线实时警报

科来网络分析系统提供实时全局警报，以醒目的方式提醒管理员当前事件。并在主视图右下角显示当前触发的警报数量。

提供用户自定义警报功能。用户可对从多个视图中对选中的网络对象进行警报创建。

每种警报有以下属性：

- 1) 警报对象
- 2) 警报类型（安全，性能，故障），严重程度（信息，通知，警告，错误）。
- 3) 丰富的警报统计数据来源。
- 4) 设置警报进入条件
- 5) 设置警报解除条件

4.11 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。

4.12 自定义节点分组

科来网络分析系统具备自定义节点分组功能，当使用自定义节点分组后，节点浏览器将根据用户自定义的方式显示节点分组，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。

4.13 数据包捕捉过滤

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。

4.14 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,并对每一个字段提供中英文双语解码,极大的提高了易用性。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。

4.15 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,管理人员可以快速分析会话过程,科来网络分析系统 2010 的会话功能包括:

- 物理会话
- IP 会话
- TCP 会话
- UDP 会话

4.16 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。

4.17 TCP 会话时序图

为了更加直观理解 TCP 会话的过程,科来网络分析系统在会话视图分隔子视图中增加了 TCP 时序图显示,有效的展现 TCP 连接通讯双方的 SYN 和 ACK 响应状态,帮助用户更容易理解 TCP 通讯内容和直观地发现问题。

4.18 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。

4.19 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、FTP 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。

4.20 报表输出

科来网络分析系统支持多种类型的报表输出,报表包括概要统计报表,诊断统计报表,协议统计报表以及 TOP N 系列报表,并且支持自定义公司标识,公司名称、报表标题前缀、报表创建人员、生成时间和报表显示条数等参数。

4.21 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。

5. 系统核心功能

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能力如下:

5.1 全面的流量分析

- 详细的概要统计分析
- 网络的总共流量
- 网络的广播流量
- 网络的组播流量
- 网络中的内部流量
- 网络中一个 IP 端点 (IP 主机) 的流量
- 网络中一个 MAC 端点的流量
- 网络中一个部门的流量
- 网络中一个 VLAN 的流量
- 网络中一种应用 (协议) 的流量
- 网络中的接收 (上行) 流量
- 网络中的发送 (下行) 流量
- 网络中的接收 (上行) 数据包
- 网络中的发送 (下行) 数据包
- 网络中的数据包数
- 物理层会话统计
- IP 会话统计
- TCP 会话统计
- UDP 会话统计
- 网络中的每秒数据包数
- 网络中流量的接收和发送比
- 网络中数据包的接收和发送比
- IP 地址国家分组
- 提供流量, 协议, 诊断等丰富的报警提醒

5.2 智能的故障诊断

- 自动识别 ARP 扫描
- ARP 中间人攻击
- ARP 断网攻击
- TCP 扫描攻击
- UDP 扫描攻击
- ICMP 扫描攻击
- 数据链路层的专家诊断
- 网络层的专家诊断
- 传输层的专家诊断
- 应用层的专家诊断
- P2P 应用分析
- 基于 IP 地址冲突
- 网络环路
- 蠕虫病毒攻击
- DNS 服务故障

- 邮件收发故障
- HTTP 访问故障
- FTP 文件传输故障
- 自动识别基于 80, 23, 25, 53, 110 端口的代理访问
- 异常流量分析
- 垃圾流分析
- 提供流量, 协议, 诊断等丰富的报警提醒

5.3 清晰的协议分析

- 支持自定义协议
- 自动识别网络应用
- 自动分析网络应用
- 自动分析网络应用的带宽占用情况
- 自动统计网络应用的数据包数
- 自动定位特定网络应用的主机
- 自动对协议进行字段解码、16 进制解码、ASCII 解码、EBCDIC 解码
- 识别非正常的协议应用
- 识别伪造的数据包
- 按 OSI 七层分层及统计显示协议
- 提供流量, 协议, 诊断等丰富的报警提醒

5.4 详细的连接分析

- 分析网络中物理端点间的通讯连接
- 分析网络中 IP 端点间的通讯连接
- 分析网络中 TCP 通讯连接
- 重组并还原 TCP 通讯
- 确定 TCP 数据传输是否乱序
- 分析网络中 UDP 通讯数据
- 分析网络中的 BT 下载
- 矩阵方式显示网络中的通讯连接
- 直观的 TCP 会话、TCP 连接性能分析 (TCP 连接时序图)
- 提供流量, 协议, 诊断等丰富的报警提醒

5.5 强大的安全分析

- 快速定位分析网络攻击
 - ◆ 分片/乱续分析
 - ◆ 数据传输行为分析
 - ◆ TCP 扫描分析
 - ◆ UDP 扫描分析
 - ◆ ICMP 扫描分析

- ◆ 邮件蠕虫分析
 - ◆ 拒绝服务分析
 - ◆ MAC 泛洪分析
 - ◆ 可疑会话分析
 - ◆ 明文传输
 - ◆ 分片攻击分析
 - ◆ 非授权访问
 - ◆ DOS 及 DDOS 攻击分析
 - ◆
-
- 分析网络其它异常行为
 - 分析网络中潜在安全隐患
 - 网页访问安全性分析
 - 邮件收发安全性分析
 - DNS 安全性分析
 - FTP 文件传输安全性分析
 - 终端访问安全性分析
 - 快速设定网络安全基准
 - 提供流量，协议，诊断等丰富的报警提醒

5.6 精细化的性能评估

- 确定网络出口带宽的最大值
- 确定网络出口带宽的利用率
- 确定网络内部带宽使用情况
- 数据包大小分布分析
- 确定网络升级效果
- TCP 连接成功率分析
- 垃圾应用与业务应用流量比量
- 评估网络传输性能的高低
- 帮助网络管理人员设定网络性能基准
- 精确分析应用性能
- 提供流量，协议，诊断等丰富的报警提醒

5.7 丰富直观的报表

- 提供 27 种报表
- 基本分析报表
- 专家分析报表
- 协议分析报表

6. 技术指标

6.1 网络类型

Ethernet II , Ethernet 802.3 , 802.1Q VLANs , 802.11 WLAN 无线网

适用于 10M/100M/1000M 高速以太网

两层和三层交换网络环境

6.2 运行环境

CPU : Inter CoreDuo 2.0GHz 以上

RAM : 2GB 以上

Disk : 4GB 空间或更多

Windows 2000 /XP /2003/Vista/2008/Windows 7 和 64bit 版本

6.3 支持的网络适配器

科来网络分析系统支持以下类型的适配器 :

- 10M 以太网适配器
- 100M 以太网适配器
- 1000M 以太网适配器

6.4 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 Packet File (v6) (*.cscpkt)
- Colasoft Raw Packet File (*.rawpkt)
- Colasoft Packet File (v7) (*.cscpkt)
- Accellent 5Views Packet File (*.5vw)
- EtherPeek Packet File (V7) (*.pkt)
- EtherPeek Packet File (V9) (*.pkt)

- HP Unix Nettl Packet File (*.TRCO;TRC1)
- Libpcap (tcpdump,Ethereal,etc.) (*.cap)
- Microsoft Network Monitor2.x (*.cap)
- Novell LANalyer (*.tr1)
- Network Instruments Observer v9.0 (*.bfr)
- NetXRay2.0,and Windows Sniffer (*.cap)
- Sun_Snoop (*.Snoop)
- Visual Network Traffic Capture (*.cap)

6.5 支持的诊断事件

科来网络分析系统 2010 支持应用层、传输层、网络层以及数据链路层故障诊断，支持 39 种不同类型的事件：

应用层		
HTTP 可疑的会话	HTTP 服务器出错	DNS 服务器慢响应
HTTP 服务器慢响应	HTTP 客户端出错	DNS 服务器错误
HTTP 请求没找到	DNS 主机或域名不存在	SMTP 服务器慢响应
SMTP 可疑的会话	SMTP 服务器返回错误	POP3 服务器慢响应
POP3 可疑的会话	POP3 服务器返回错误	FTP 服务器慢响应
FTP 可疑的会话	FTP 服务器返回错误	
传输层		
TCP 连接被拒绝	TCP 重复的连接尝试	TCP 慢应答
TCP 重传数据包	TCP 非法的校验和	TCP SYN 风暴
TCP 重复的确认	TCP 端口扫描	
网络层		
IP 非法的校验和	IP TTL 太小	ICMP 源抑制
ICMP 目的地不可达	ICMP 网络不可达	ICMP 主机不可达
ICMP 端口不可达	ICMP 主机重定向	ICMP 网络重定向
数据链路层		
ARP 扫描	ARP 请求风暴	ARP 太多无请求应答
ARP 格式违规	ARP 地址冲突	

6.6 支持的协议

科来网络分析系统支持协议包括：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

6.7 解码的协议

科来网络分析系统解码的协议包括：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。

6.8 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。

6.9 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。

7. 联系我们

成都科来软件有限公司

总部地址：成都市高新区府城大道西段 399 号天府新谷 5 号楼 10F

全国咨询热线：400-6869-069

售前咨询电话：028-85310277

电话：028-85120922

传真：028-85120911

北京营销中心

地址：北京海淀区中关村东路 18 号财智国际大厦 C 座 611 室

电话：010-82601814

传真：010-82601614

邮编：100083

官方网站：<http://www.colasoft.com.cn>

电子邮件：support@colasoft.com.cn