

科来网络分析系统 2010

快速入门指南

科来网络分析系统 2010

快速入门指南

本档属商业机密文件，所有内容均为科来软件独立完成，属科来软件内部机密信息，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	2
引言	3
1. 分析引导	4
1.1 分析模式	4
1.2 选择网络适配器	4
1.3 过滤器	5
1.4 网络档案	5
1.5 分析方案	5
1.6 开始分析	6
2. 整体布局	7
2.1 标题栏	7
2.2 功能区	8
2.3 节点浏览器	9
2.4 主视图区	10
2.5 警报浏览器	24
2.6 状态栏	25
3. 分析方案设置	26
3.1 分析对象	26
3.2 数据包存储	27
3.3 日志	27
3.4 诊断	28
4. 数据管理	29
4.1 数据包	29

引言

网络分析是一门非常专业的技术，不仅需要网络分析工程师具备相当的网络知识，并且对网络分析软件使用的熟悉程度，也在很大程度上决定着网络故障排查的效率性和准确性。“工欲善其事，必先利其器”，要做好网络分析，应该首先熟悉网络分析软件的使用。对于初次使用网络分析软件的用户，可能就会存在许多疑问：怎样使用网络分析软件捕获数据、通过网络分析软件能分析到什么信息，这些信息能帮助我们做些什么，我们如何使用这些数据信息等等。因此，针对初次接触科来网络分析系统的用户，我们制作了快速入门指南，对科来网络分析系统的使用进行了简单介绍，希望对初次使用该系统的用户有所帮助。

科来网络分析系统 2010 是科来软件全新打造的网络分析系统，采用了全自主研发的第二代网络分析引擎，提供海量数据采集和高性能实时诊断分析，并且采用了全新的 UI 界面设计和新的分析理念。因此，熟练使用科来网络分析系统 2010，将会大大提高用户的网络分析效率。

提示：关于科来网络分析系统 2010 的详细使用介绍，请参考《科来网络分析系统 2010 产品使用手册》。

1. 分析引导

科来网络分析系统 2010 引入了分析模式、网络档案和分析方案概念。打开系统，主界面如下图所示：



在系统的分析引导界面中，提供了分析模式选择、网络适配器选择，过滤器选择，网络档案选择和分析方案选择。用户可以根据实际的分析任务选择或创立相应的网络档案和分析方案。

1.1 分析模式

☑ 实时分析

实时分析以网络适配器作为数据采集来源，实时捕获网络通讯的数据包，并提供实时分析、实时诊断、实时报警等。

☑ 回放分析

回放分析以数据包存储文件作为第二分析数据源，提供历史问题回溯分析，并支持原速和快速两种回放模式。

1.2 选择网络适配器

系统能够自动检测和显示当前的网络适配器及其 IP 地址、每秒数据包数，并图形化的显示当前网络适配器的流量趋势，您可以根据实际情况选择用于采集数据的网络适配器。系统支持多网卡的数据采集，您可以同时选择多块网卡进行数据源的采集。

1.3 过滤器

过滤器可以按照您的需求来捕获数据，如果您需要捕获和分析特定的数据信息，您可以设置过滤器，以排除不需要的数据。合理的设置过滤器不仅能够提高您的分析效率，而且也能提高系统的分析性能。

1.4 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。网络档案用于保存某个特定网络的分析配置信息，包括该网络的带宽，内部网络节点的分组配置，对应的名字表以及针对该网络的警报设置。

如果你使用科来网络分析系统在不同的网络位置进行实时抓包分析，你可以为每个网络创建对应的网络档案。当回放一个或者多个来自外部网络的数据包文件时，你也可以为其创建专门的网络档案，更有效更准确的分析相应的流量数据。



系统默认提供了 4 个网络档案配置文件，用户可选择其中一个开始网络分析任务。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，以此保存网络环境中的各项关键数据信息。此外，您可以单击右键进行添加、编辑、删除或者复制网络档案，在后续的分析任务中，可直接调用新的网络档案进行分析。

1.5 分析方案

分析方案用于保存某个特定分析需求的配置信息，包括分析引擎的参数配置、加载的高级分析模块以及每个高级分析模块的详细参数设置。

科来网络分析系统针对典型的分析使用场景内建了若干的分析方案供用户选择，每个分析方案对应一个特定的分析需求。

分析方案由若干分析设置集合而成，包括网络对象数据统计设置，分析模块设置，诊断设置，日志设置，图表设置等。您可根据自己实际的分析任务，选择合适的分析方案，这样，不仅能够提升系统分析性能，而且有助于提高您的分析效率。

科来网络分析系统 2010 提供了全新的分析方案功能，系统初始提供 7 个分析方案。一个分析方案可由多个分析模块组成，系统提供自定义分析方案，您可以根据实际分析需求新建分析方案，也可编辑和修改系统初始的分析方案，可自定义添加或删除不同的分析模块，以达到最佳的分析结果。不同的分析方案提供不同的视图表现和数据组合。



在上图中，单击右键，将会弹出“编辑”、“新建”、“副本”以及“删除”菜单选项，用户可根据实际需求对分析方案进行自定义操作。

☑ 全面分析

全面分析方案针对网络全局、单个网络对象、网络应用等进行全面、细致的分析和统计，包括通讯流量、会话、协议、常规的通讯参数等所有数据。

☑ 高性能分析

高性能分析方案主要针对大流量网络环境而提供的快速流量统计分析方案，以较高的性能分析网络中的主要对象，包括物理地址、IPv4 地址、物理地址分组、IPv4 地址分组、协议、物理流、IPv4 流、TCP 流和 UDP 流以及每个对象的流量，绘制用户选定的图表和报表。

☑ 安全分析

安全分析方案主要针对网络通讯进行安全评估、攻击检测，快速发现潜在的网络安全隐患，以多种方式报告给网络管理者。

☑ DNS 应用分析

DNS 应用分析方案主要分析 DNS 网络应用、诊断 DNS 网络应用故障、性能并对 DNS 做日志记录的保存。

☑ Email 高级分析

Email 高级分析方案主要针对基于 SMTP 及 POP3 协议的 Email 应用流量统计与故障诊断分析。

☑ FTP 高级分析

FTP 高级分析方案主要针对 FTP 网络应用进行流量统计、日志记录与故障诊断。

☑ HTTP 应用分析

HTTP 应用分析方案主要分析 HTTP 应用的流、客户端与服务器的流量、诊断 HTTP 网络应用的故障与性能。

1.6 开始分析

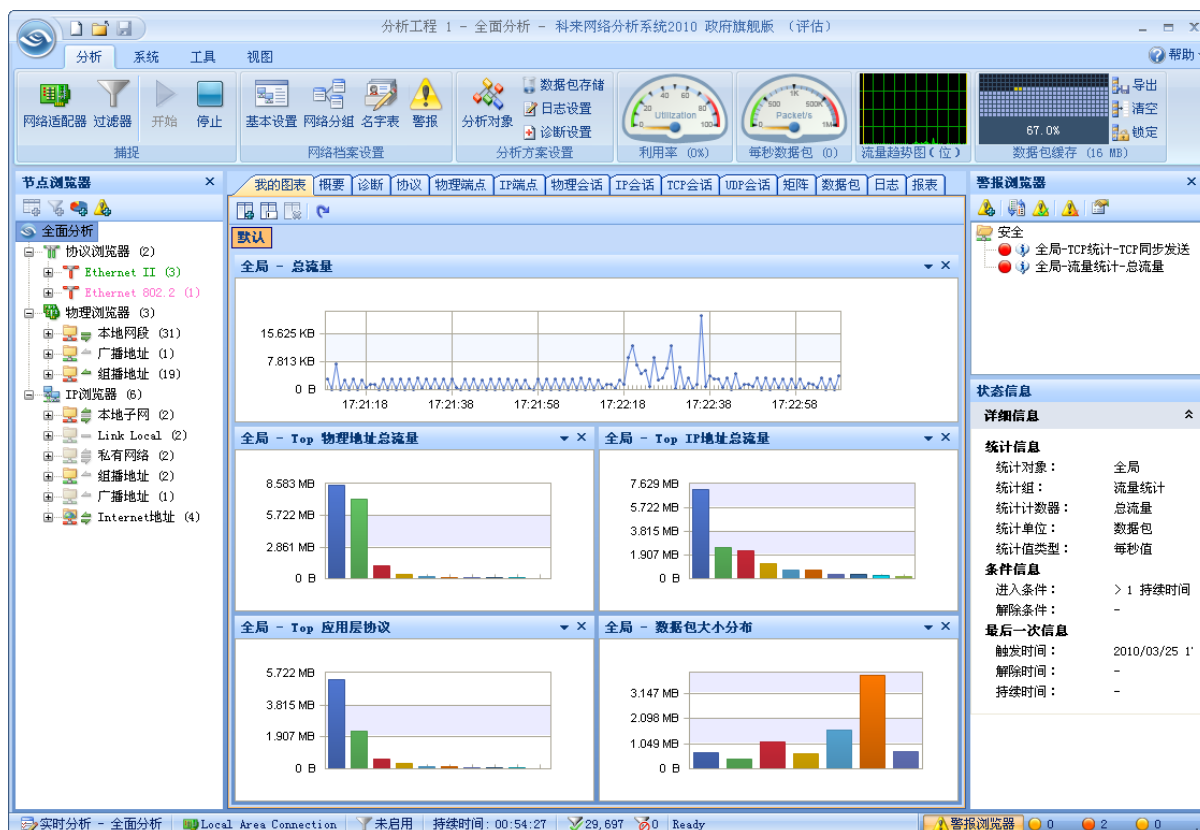
分析工程是分析任务的载体，它包括数据源，网络环境，过滤器，分析方案和分析结果，其中的分析方案是整个分析工程的重点。用户是通过启动分析工程来实施一个分析方案。

工程可以被理解为一个分析任务。捕获数据之前，用户需要创建一个新工程。系统在启动时默认创建一个新工程，用户也可以在标题栏中单击“新建工程”（快捷键：Ctrl + N）进行手动创建新工程。

我们必须要对网络中的数据包进行捕获，然后才能分析整个网络，才能了解当前的网络状况。通常，在引导界面中设置好分析参数后，就可以单击“开始”按钮开始捕获数据包。

2. 整体布局


开始捕获数据包后，此时显示的是科来网络分析系统 2010 的主界面，如下图。



在产品主界面中，主要由 6 个部分构成：标题栏、功能区、节点浏览器，主视图区、警报浏览器以及状态栏。

- ☑ 标题栏：提供系统菜单命令、显示分析工程及应用的分析方案；
- ☑ 功能区：包括分析、系统、工具以及视图4个页面，详见功能区介绍；
- ☑ 节点浏览器：提供协议端点、物理端点以及IP端点进行节点数据过滤及快速定位；
- ☑ 主视图区：包括图表、概要统计、诊断、物理端点、IP端点、物理会话、IP会话、TCP会话、UDP会话、矩阵、数据包、日志以及报表视图；
- ☑ 警报浏览器：创建、删除在线警报以及显示警报状态及信息，默认为隐藏状态；
- ☑ 状态栏：工程状态栏，包括显示分析方案、采集数据的网络适配器、过滤器状态、捕获时间以及捕获状态等信息。

2.1 标题栏

标题栏除了显示当前的分析工程以及使用的分析方案外，单击标题栏左边的  按钮，将显示系统菜单，下面的表格是菜单命令以及相应说明：

命令	快捷键	描述
文件...		
新建	Ctrl+N	创建一个新的工程
最近打开的工程文件		显示最近使用的工程文件，用户可以快速的打开这些历史文件
打印...		
打印预览	Ctrl+P	打印当前的工程视图数据
打印设置...		预览打印效果
		设置打印时的选项
本地引擎设置...		
定制协议		配置和自定义网络协议
格式		查看或修改数据显示格式
报表		配置报表页头或页脚等报表模板参数
资源...		
科来软件主页		访问科来软件官方网站
网络分析论坛		访问 CSNA 网络分析社区
消息历史		显示官方消息历史
产品...		
授权号		产品相关信息
激活		重新设置授权号，注册产品
更新		激活产品
关于		检查产品更新
		显示产品版本及版权信息
关闭...		退出当前分析工程，回到开始页面。

2.2 功能区

系统功能区包括了分析、系统、工具以及视图 4 个页面，分析栏的显示界面如下图：



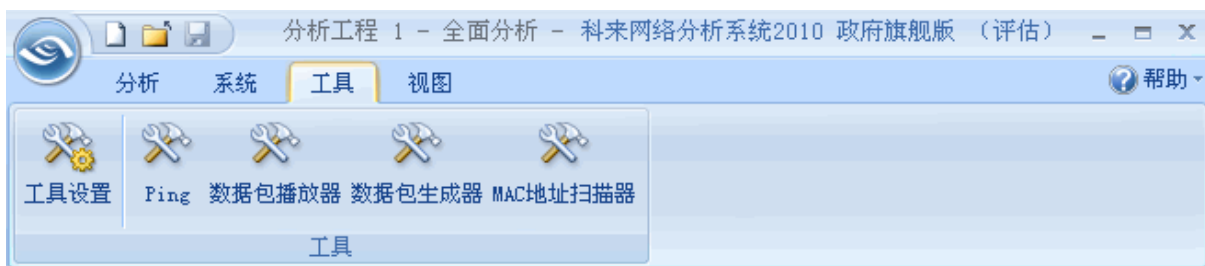
分析栏中，包括数据包捕捉、网络档案设置、分析方案设置、全局仪表盘以及数据包缓存状态显示，您可以从该栏中进行各项分析设置、快速查看网络全局利用率、每秒数据包、网络流量趋势以及数据包缓存状态等信息。

而在系统页面中，则包括了系统配置、资源、产品信息，其界面如下图：

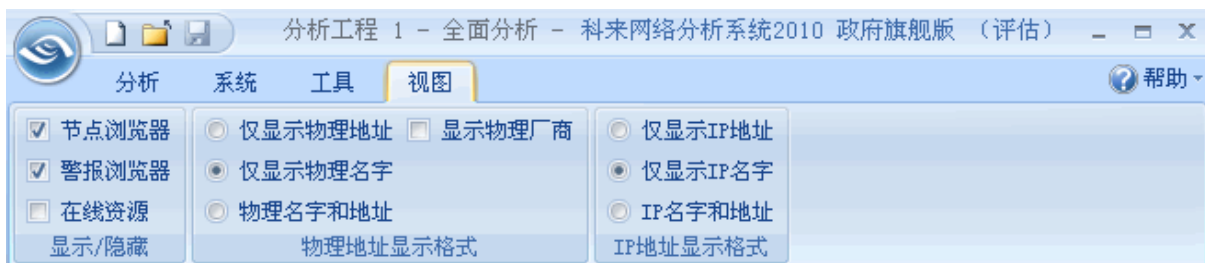


您可以在系统页面中进行全局系统配置，包括定制协议、过滤器库管理以及常规系统选项设置，此外，可以快速访问科来软件官方网站、CSNA 网络分析社区，重新注册、激活产品等。

科来网络分析系统 2010 同样免费提供了 4 个网络小工具：科来 Ping 工具、MAC 地址扫描器、数据生成器以及数据包播放器，您可以在工具页面中打开运行这些小工具并可自定义添加常用网络工具，如下图：



在功能区的视图页面中，提供了物理地址及 IP 地址的显示格式选择以及节点浏览器、警报视图、在线资源页面的显示或隐藏选择，如下图：



2.3 节点浏览器

节点浏览器可以按协议浏览、按物理端点浏览、按 IP 端点浏览三类方式，实时的反映网络中出现的协议、主机及该主机的物理地址和 IP 地址，以及主机当前是否正在通讯。如下图。



节点浏览器以树状层级方式显示当前通讯的网络协议、物理地址以及 IP 地址。通过节点浏览器，您可以快速定位和查看节点数据信息，如查看某个 IP 组信息、某个 VLAN 信息，单个 IP 地址、物理地址或协议的信息。

2.4 主视图区

系统所有分析、诊断以及统计数据均在主视图区显示，主视图区包括概要统计视图、节点统计视图、协议统计视图、会话统计视图、矩阵视图以及数据包解码视图。点击相应的视图标签，则可以查看相应的网络分析数据。

我的图表

科来网络分析系统 2010 提供了强大的自定义图表配置以及灵活的图表视图布局。

系统提供的默认提供了 4 个 TOP 10 图表，您可以自定义添加图表面板。每个图表面板又可任意添加新的图表。除了添加全局的图表，您还可以从多个视图对选中的网络对象进行图表创建并在图表视图中进行显示。

通过灵活的设置图表，您可以更直观的对所关心的网络对象和应用的重要流量参数进行实时的监控。系统图表视图如下图所示：



☐ 概要统计

概要统计视图对网络流量及常见网络应用进行详细的统计显示。通过概要统计视图，您可以快速的查看当前的网络流量、数据包大小分布、TCP 通讯情况、HTTP 通讯、DNS 通讯等 12 种类型的数据统计。

此外，配合节点浏览器的使用，您可以快速查看单个网络对象或对象组的概要统计信息。在节点浏览器中选择某个网络对象，系统会自动过滤出该对象的统计数据，能极大的提高您的分析效率。

我的图表 概要 诊断 协议 物理端点 IP端点 物理会话 IP会话 TCP会话 UDP会话 矩阵 数据包 日志 报表							
						全面分析\概要统计	27
统计项						当前值	
报警统计						数量	
诊断统计						数量	
信息类诊断						5,635	
注意类诊断						430	
警告类诊断						39	
错误类诊断						0	
流量统计	字节数	数据包数	利用率	每秒位	每秒包数		
总流量	45.009 MB	100,849	0.000%	0 bps	0		
广播流量	1.155 MB	11,311	0.000%	0 bps	0		
多播流量	1.784 MB	8,313	0.000%	0 bps	0		
平均包长						467.984 字节	
数据包大小分布	字节数	数据包数	利用率	每秒位	每秒包数		
<=64	2.002 MB	33,396	0.000%	0 bps	0		
65-127	2.155 MB	24,587	0.000%	0 bps	0		
128-255	1.908 MB	10,222	0.000%	0 bps	0		
256-511	1.460 MB	4,120	0.000%	0 bps	0		
512-1023	2.834 MB	4,248	0.000%	0 bps	0		
1024-1517	13.293 MB	9,523	0.000%	0 bps	0		
>=1518	21.358 MB	14,753	0.000%	0 bps	0		
地址统计						数量	
协议统计						数量	
数据流统计						数量	
TCP统计						数量	
DNS分析						数量	
Email高级分析						数量	
FTP高级分析						数量	
HTTP应用分析						数量	

☐ 诊断

科来网络分析系统 2010 提供了全新的诊断视图布局，分为诊断分层、诊断发生地址以及详细事件描述 3 个分隔子窗口，您可以非常方便和直观的查看到当前网络中发生的网络事件。诊断模块同样严格遵循 OSI 模型对网络事件进行分层显示，目前产品支持四个层次的故障诊断：应用层、传输层、网络层、数据链路层。

诊断视图中，您可以了解到以下信息：

- 1) 每条诊断的参考信息，提供该诊断的描述，存在原因与解决方法。
- 2) 每个诊断信息提供关联的 Top N 主机排行显示。可直观得到每个诊断事件是由哪些主机触发。
- 3) 与主机关联的诊断事件日志，帮助您更迅速的发现问题主机。
- 4) 与事件相关的数据包挖掘，您可以双击某条诊断日志弹出该日志相关的数据包通讯，快速分析问题。

系统诊断视图如下图所示：

我的图表				诊断				协议				物理端点				IP端点				物理会话				IP会话				TCP会话				UDP会话				矩阵				数据包				日志				报表			
诊断分层																诊断发生地址																																			
诊断 15																统计 134																																			
名字																名字																																			
所有诊断 6,117																CAIZY-PC 3,461																																			
应用层 462																物理地址 IP地址 数量																																			
DNS服务器慢响应 44																ca.colasoft.com 00:1F:D0:8C:66:50 192.168.5.10 6																																			
HTTP可疑会话 26																kb.colasoft.com 00:21:9B:BC:C7:C6 192.168.0.230 7																																			
HTTP请求没找到 17																crm.colasoft.com 00:21:9B:BC:C7:C6 192.168.0.204 171																																			
HTTP服务器慢响应 375																192.168.0.208 00:21:9B:BC:C7:C6 192.168.0.208 2,029																																			
传输层 5,644																192.168.5.17 00:21:70:BB:33:91 192.168.5.17 24																																			
TCP重复的连接尝试 435																192.168.5.107 00:15:17:CA:1C:4C 192.168.5.107 5																																			
TCP重传数据包 2,143																192.168.5.8 00:1F:D0:8C:66:50 192.168.5.8 26																																			
TCP非法的校验和 1																192.168.5.5 00:19:ED:75:28:9D 192.168.5.5 12																																			
TCP慢应答 3,052																192.168.5.56 00:24:21:18:61:92 192.168.5.56 38																																			
TCP重复的确认 4																192.168.5.105 00:15:17:CA:1C:64 192.168.5.105 12																																			
																192.168.5.13 00:24:21:18:5F:D9 192.168.5.13 10																																			
事件																事件 3,462																																			
严重程度 类型 层别 事件描述 源IP地址 源物理地址 目标IP地址 目标物理地址																																																			
性能 传输层 太慢的TCP应答(数据包[166]与数据包[68]相隔7416毫秒) 192.168.5.10 00:1F:D0:8C:66:50 192.168.0.183 00:21:9B:BC:C7:C6																																																			
性能 传输层 太慢的TCP应答(数据包[167]与数据包[68]相隔7416毫秒) 192.168.5.10 00:1F:D0:8C:66:50 192.168.0.183 00:21:9B:BC:C7:C6																																																			
性能 传输层 太慢的TCP应答(数据包[239]与数据包[201]相隔10657毫秒) 192.168.5.10 00:1F:D0:8C:66:50 192.168.0.183 00:21:9B:BC:C7:C6																																																			
性能 传输层 太慢的TCP应答(数据包[242]与数据包[240]相隔804毫秒) 192.168.5.10 00:1F:D0:8C:66:50 192.168.0.183 00:21:9B:BC:C7:C6																																																			
性能 传输层 太慢的TCP应答(数据包[363]与数据包[256]相隔56776毫秒) 192.168.5.10 00:1F:D0:8C:66:50 192.168.0.183 00:21:9B:BC:C7:C6																																																			
性能 传输层 太慢的TCP应答(数据包[448]与数据包[418]相隔23194毫秒) 192.168.5.10 00:1F:D0:8C:66:50 192.168.0.183 00:21:9B:BC:C7:C6																																																			
性能 传输层 太慢的TCP应答(数据包[475]与数据包[467]相隔384毫秒) 192.168.5.10 00:1F:D0:8C:66:50 192.168.0.183 00:21:9B:BC:C7:C6																																																			
性能 传输层 太慢的TCP应答(数据包[476]与数据包[467]相隔384毫秒) 192.168.5.10 00:1F:D0:8C:66:50 192.168.0.183 00:21:9B:BC:C7:C6																																																			
性能 传输层 太慢的TCP应答(数据包[477]与数据包[467]相隔384毫秒) 192.168.5.10 00:1F:D0:8C:66:50 192.168.0.183 00:21:9B:BC:C7:C6																																																			
性能 传输层 太慢的TCP应答(数据包[525]与数据包[507]相隔8756毫秒) 192.168.5.10 00:1F:D0:8C:66:50 192.168.0.183 00:21:9B:BC:C7:C6																																																			
性能 传输层 太慢的TCP应答(数据包[653]与数据包[610]相隔27173毫秒) 192.168.5.10 00:1F:D0:8C:66:50 192.168.0.183 00:21:9B:BC:C7:C6																																																			

☐ 协议视图

协议视图提供全局的协议统计，遵循 OSI 七层协议分析，根据实际的网络协议封装顺序，不同的协议赋予不同的色彩，层次化的展现给用户，并且，能够单独统计每一个层次下所使用的协议，方便用户查看。

协议视图下方提供了物理端点与 IP 端点子视图，选择某个协议后，在子视图中会显示使用该协议的物理地址或 IP 地址的端点流量统计。

通过协议视图对各协议占用流量及百分比的统计，您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；并帮助您排查网络速度慢、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。

协议视图如下图所示：



☐ 物理端点视图

科来网络分析系统 2010 提供了全新的物理端点视图，按 MAC 地址类型统计网络中物理端点之间的通讯情况，物理端点视图统计参数多达 46 种，您可以自定义显示统计参数，也可以按每个参数进行排序显示。

物理端点视图中，增加了物理会话子视图，方便您查看每个物理端点详细的通讯会话信息。

物理端点视图如下图所示：

我的图表 概要 诊断 协议 物理端点 IP端点 物理会话 IP会话 TCP会话 UDP会话 矩阵 数据包 日志 报表							
							全面分析\物理端点: 50
名字	字节	数据包	每秒位	接收字节	接收数据包	发送字节	发送数据包
本地网段	25.436 MB	49,148	20.592 Kbps	0 B	0	598.276 KB	6,192
00:1F:DO:8C:66:50	23.437 MB	39,442	16.816 Kbps	7.825 MB	17,218	15.612 MB	22,224
00:21:9B:BC:C7:C6	23.128 MB	44,032	17.328 Kbps	14.020 MB	22,887	9.109 MB	21,145
00:0C:29:A5:A5:08	1.851 MB	1,669	0 bps	1.828 MB	1,352	23.905 KB	317
本机	1.456 MB	3,717	0 bps	1.155 MB	1,327	308.193 KB	2,390
00:21:70:BB:33:91	105.260 KB	585	0 bps	7.534 KB	36	97.726 KB	549
00:0A:EB:6B:B6:E3	42.961 KB	390	0 bps	6.307 KB	47	36.654 KB	343
00:0C:29:D1:AF:AF	38.956 KB	357	0 bps	9.727 KB	72	29.229 KB	285
00:21:85:FC:B3:CD	28.205 KB	261	3.264 Kbps	0 B	0	28.205 KB	261
00:24:21:18:61:CF	25.991 KB	301	0 bps	0 B	0	25.991 KB	301
00:1D:7D:D5:4A:55	17.338 KB	106	0 bps	0 B	0	17.338 KB	106
00:15:5D:00:83:03	17.259 KB	108	0 bps	0 B	0	17.259 KB	108
00:0C:29:C4:80:90	14.234 KB	74	0 bps	0 B	0	14.234 KB	74
00:EO:81:B7:A8:02	13.695 KB	71	0 bps	0 B	0	13.695 KB	71

物理会话							
							本地网段\物理会话: 76
节点1->	<节点2	持续时间	字节	字节->	<字节	数据包	数据包->
00:0C:29:6B:D3:9C	FF:FF:FF:FF:FF:FF	00:11:00	3.400 KB	3.400 KB	0 B	33	33
00:0C:29:A5:A5:08	00:1F:DO:8C:66:50	00:00:01	1.848 MB	19.952 KB	1.828 MB	1,641	289
00:0A:EB:6B:B6:E3	01:00:5E:00:00:16	00:04:33	256 B	256 B	0 B	4	4
00:0A:EB:6B:B6:E3	00:0C:29:FD:85:BD	00:00:54	7.456 KB	2.511 KB	4.945 KB	54	18
00:0A:EB:6B:B6:E3	00:1F:DO:8C:66:50	00:00:54	2.856 KB	1.495 KB	1.361 KB	22	11
00:0C:29:D0:99:3F	01:00:5E:00:00:16	00:00:00	128 B	128 B	0 B	2	2
00:1B:24:EF:F0:04	00:0C:29:FD:85:BD	00:00:00	517 B	301 B	216 B	4	2
00:21:9B:BC:C7:C6	00:0C:29:6B:D3:9C	00:00:04	320 B	320 B	0 B	5	5

☐ IP 端点视图

IP 端点视图按 IP 类型统计 IP 地址之间的通讯情况。与物理端点视图类似，IP 端点的统计参数同样可以提供自定义统计参数显示以及按参数大小排序。

通过 IP 端点视图，您可以快速找定位通讯量最大的 IP 节点和物理节点，可以清楚地得出当前网络中所有主机（包括某个网段、某个 VLAN、某个 IP）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，您可以确定网络中是否广播/组播风暴，并帮助您排查网络速度慢、网络时断时续、蠕虫病毒攻击、DOS 攻击、以及无法上网等网络故障。

IP 端点视图包括 IP 会话、TCP 会话、UDP 会话 3 个分隔子窗口，您可以非常方便的查看每个 IP 端点关联的会话信息，如下图所示：

我的图表 概要 诊断 协议 物理端点 IP端点 物理会话 IP会话 TCP会话 UDP会话 矩阵 数据包 日志 报表									
									全面分析VIP端点: 13
名字	字节	数据包	每秒位	接收字节	接收数据包	发送字节	发送数据包	发送/接收(字...	
本地子网	25.055 MB	44,325	0 bps	8.967 MB	18,139	14.035 MB	22,963	1.57	
192.168.5.0/24	25.055 MB	44,325	0 bps	8.967 MB	18,139	14.035 MB	22,963	1.57	
私有网络	20.575 MB	34,745	0 bps	13.608 MB	19,344	6.908 MB	15,015	0.51	
192.168.0.0/16	20.561 MB	34,668	0 bps	13.608 MB	19,344	6.908 MB	15,014	0.51	
10.0.0.0/8	14.939 KB	77	0 bps	0 B	0	93 B	1	0.00	
Internet地址	2.495 MB	6,776	0 bps	420.604 KB	3,506	2.084 MB	3,270	5.07	
中国	2.035 MB	5,706	0 bps	359.144 KB	2,995	1.685 MB	2,711	4.80	
美国	470.451 KB	1,070	0 bps	61.461 KB	511	408.990 KB	559	6.65	
组播地址	41.173 KB	249	0 bps	41.173 KB	249	0 B	0	0.00	
管理范围块	29.132 KB	74	0 bps	29.132 KB	74	0 B	0	0.00	
本地网络控制块	12.041 KB	175	0 bps	12.041 KB	175	0 B	0	0.00	
广播地址	858 B	10	0 bps	858 B	10	0 B	0	0.00	
255.255.255.255	858 B	10	0 bps	858 B	10	0 B	0	0.00	

IP会话 TCP会话 UDP会话									
									本地子网\IP会话: 100
节点1->	<节点2	持续时间	字节	字节->	<字节	数据包	数据包->	<- 数据包	开始发包时间
192.168.5.10	124.115.5.210	00:00:00	796 B	482 B	314 B	9	5	4	13:16:1
192.168.5.10	74.125.15.26	00:01:04	4.504 KB	2.791 KB	1.713 KB	20	10	10	13:21:0
192.168.5.224	192.168.5.255	00:11:00	3.213 KB	3.213 KB	0 B	30	30	0	13:13:5
192.168.5.10	74.125.153.100	00:04:04	2.308 KB	1.358 KB	972 B	11	6	5	13:21:0
192.168.5.10	192.168.5.207	00:00:01	1.847 MB	1.828 MB	19.890 KB	1,640	1,352	288	13:29:2
192.168.5.100	224.0.0.22	00:04:33	256 B	256 B	0 B	4	4	0	13:26:0
192.168.5.119	192.168.5.100	00:00:54	7.394 KB	4.945 KB	2.448 KB	53	36	17	13:30:2
192.168.5.10	192.168.5.100	00:00:54	2.794 KB	1.361 KB	1.433 KB	21	11	10	13:30:2

☐ 物理会话视图

科来网络分析系统 2010 提供全新的物理会话视图，详细统计网络中物理地址之间的通讯会话情况。

物理会话视图提供了详细的会话参数统计，包括通讯节点、通讯持续时间、通讯流量、通讯数据包个数、发送流量、接收流量、发送数据、接收数据包等丰富的数据信息。

物理会话如下图所示：

我的图表 概要 诊断 协议 物理端点 IP端点 物理会话 IP会话 TCP会话 UDP会话 矩阵 数据包 日志 报表									
									全面分析\物理会话: 79
节点1->	<节点2	持续时间	字节	字节->	<字节	数据包	数据包 ->	<- 数据包	
00:0A:EB:6B:B6:E3	00:0C:29:FD:85:BD	00:00:54	7.456 KB	2.511 KB	4.945 KB	54	18	36	
00:0A:EB:6B:B6:E3	00:1F:DO:8C:66:50	00:00:54	2.856 KB	1.495 KB	1.361 KB	22	11	11	
00:0C:29:DO:99:3F	01:00:5E:00:00:16	00:00:00	128 B	128 B	0 B	2	2	0	
00:1B:24:EF:FO:04	00:0C:29:FD:85:BD	00:00:00	517 B	301 B	216 B	4	2	2	
00:21:9B:BC:C7:C6	00:0C:29:6B:D3:9C	00:00:04	320 B	320 B	0 B	5	5	0	
00:21:70:BB:33:91	33:33:FF:C2:66:7A	00:00:00	82 B	82 B	0 B	1	1	0	
00:21:70:BB:33:91	33:33:00:00:00:02	00:00:09	222 B	222 B	0 B	3	3	0	
00:21:70:BB:33:91	01:00:5E:00:00:16	00:00:27	704 B	704 B	0 B	11	11	0	
00:21:70:BB:33:91	33:33:00:00:00:16	00:00:37	1.193 KB	1.193 KB	0 B	13	13	0	
00:1F:DO:8C:66:50	33:33:FF:C2:66:7A	00:00:00	90 B	90 B	0 B	1	1	0	
00:21:70:BB:33:91	33:33:00:01:00:02	00:01:03	1.053 KB	1.053 KB	0 B	7	7	0	
00:21:70:BB:33:91	33:33:00:00:00:0C	00:00:45	12.404 KB	12.404 KB	0 B	12	12	0	
00:1F:DO:8C:66:50	33:33:00:00:00:0C	00:00:45	8.461 KB	8.461 KB	0 B	12	12	0	
00:1F:DO:8C:66:50	01:00:5E:7F:FF:FA	00:00:45	8.227 KB	8.227 KB	0 B	12	12	0	

IP会话 TCP会话 UDP会话									
									00:0C:29:A5:A5:08 <-> 00:1F:DO:8C:66:50\IP会话: 1
节点1->	<节点2	持续时间	字节	字节->	<字节	数据包	数据包 ->	<- 数据包	
192.168.5.10	192.168.5.207	00:00:01	1.847 MB	1.828 MB	19.890 KB	1,640	1,352	288	

☐ IP 会话视图

IP 会话视图详细统计了 IP 地址间的通讯会话情况。通过查看每条会话，我们可以分析其源地址、目标地址、会话时间、会话流量、收发的数据包及这些数据包的大小等信息。我们可以通过这些信息快速分析出当前网络中某个会话的通讯情况。

IP 会话视图如下图所示：

我的图表 概要 诊断 协议 物理端点 IP端点 物理会话 IP会话 TCP会话 UDP会话 矩阵 数据包 日志 报表										
										全面分析VIP会话: 29
节点1->	<-节点2	持续时间	字节	字节->	<-字节	数据包	数据包 ->	<- 数据包	开始发包R	
192.168.5.103	192.168.5.255	00:00:00	257 B	257 B	0 B	1	1	0	15:15	
192.168.5.206	192.168.5.255	00:00:16	919 B	919 B	0 B	8	8	0	15:15	
192.168.5.24	192.168.5.255	00:00:01	288 B	288 B	0 B	3	3	0	15:16	
192.168.5.119	65.55.239.164	00:00:01	2.018 KB	1.434 KB	598 B	13	10	3	15:16	
192.168.5.119	207.46.49.134	00:00:05	4.144 KB	2.805 KB	1.339 KB	23	18	5	15:16	
192.168.5.10	219.133.60.243	00:00:00	218 B	129 B	89 B	2	1	1	15:16	
192.168.5.10	119.147.6.15	00:00:00	218 B	129 B	89 B	2	1	1	15:16	
192.168.5.225	192.168.5.255	00:00:00	247 B	247 B	0 B	1	1	0	15:16	
192.168.5.119	61.129.48.110	00:00:00	2.237 KB	1.461 KB	795 B	14	10	4	15:16	
192.168.5.119	115.238.55.253	00:00:01	6.706 KB	1.576 KB	5.130 KB	20	12	8	15:16	
192.168.5.14	192.168.5.255	00:00:01	288 B	288 B	0 B	3	3	0	15:16	
192.168.5.119	125.65.77.233	00:00:08	108.613 KB	7.867 KB	100.74...	168	92	76	15:16	
192.168.5.10	61.139.2.69	00:00:02	588 B	168 B	420 B	4	2	2	15:16	
192.168.5.10	221.236.31.151	00:00:01	8.303 KB	1.158 KB	7.145 KB	15	7	8	15:16	

TCP会话 UDP会话										
										192.168.5.119 <-> 118.123.0.243\TCP会话: 45
节点1->	<-节点2	持续时间	字节	字节->	<-字节	数据包	数据包 ->	<- 数...		
192.168.5.119:1206	118.123.0.243:80	00:00:13	7.541 KB	1.854 KB	5.688 KB	24	16	8		
192.168.5.119:1209	118.123.0.243:80	00:00:13	5.581 KB	1.734 KB	3.847 KB	21	14	7		
192.168.5.119:1210	118.123.0.243:80	00:00:13	5.283 KB	1.734 KB	3.549 KB	20	14	6		
192.168.5.119:1191	118.123.0.243:80	00:00:17	9.516 KB	3.102 KB	6.414 KB	32	22	10		
192.168.5.119:1161	118.123.0.243:80	00:00:27	9.265 KB	3.992 KB	5.272 KB	31	22	9		
192.168.5.119:1174	118.123.0.243:80	00:00:23	7.958 KB	2.863 KB	5.095 KB	27	18	9		
192.168.5.119:1177	118.123.0.243:80	00:00:23	10.114 KB	3.102 KB	7.013 KB	32	22	10		
192.168.5.119:1176	118.123.0.243:80	00:00:23	15.573 KB	3.340 KB	12.233 KB	40	26	14		

☐ TCP 会话视图

科来网络分析系统 2010 提供了详细的 TCP 通讯会话分析。通过 TCP 会话视图，您可以详细的了解到每个 TCP 通讯连接的会话情况。

通过分析 TCP 会话，可以帮助我们快速分析网络中的安全隐患，如网络明文传输、扫描型蠕虫病毒、DDOS 攻击等。在 TCP 会话视图中，包括了数据包、数据流以及时序图 3 个子视图窗口，您可以详细查看某条会话的原始通讯数据包、TCP 的数据流重组以及 TCP 连接的时序图，有效的展现 TCP 连接通讯双方的 SYN 和 ACK 响应状态，帮助您更容易理解 TCP 通讯内容和直观地发现问题。

TCP 会话视图如下所示：

我的图表 概要 诊断 协议 物理端点 IP端点 物理会话 IP会话 TCP会话 UDP会话 矩阵 数据包 日志 报表									
全面分析\TCP会话: 76									
节点1->	<节点2	持续时间	字节	字节->	<字节	数据包	数据包 ->	< 数据包	协议
192.168.5.119:1149	207.46.49.134:80	00:00:01	2.026 KB	1.418 KB	623 B	13	10	3	HTTP
192.168.5.119:1150	65.55.239.164:80	00:00:01	2.018 KB	1.434 KB	598 B	13	10	3	HTTP
192.168.5.119:1154	61.152.242.233:80	00:00:00	5.177 KB	2.615 KB	2.562 KB	16	10	6	HTTP
192.168.5.119:1157	61.129.48.110:80	00:00:00	2.237 KB	1.461 KB	795 B	14	10	4	HTTP
192.168.5.119:1155	115.238.55.253:80	00:00:01	6.706 KB	1.576 KB	5.130 KB	20	12	8	HTTP
192.168.5.119:1172	61.152.242.233:80	00:00:01	6.446 KB	3.049 KB	3.397 KB	18	12	6	HTTP
192.168.5.119:1173	61.152.242.233:80	00:00:02	8.739 KB	3.055 KB	5.685 KB	19	12	7	HTTP
192.168.5.119:1152	118.123.0.243:80	00:00:10	3.210 KB	1.688 KB	1.522 KB	17	12	5	HTTP
192.168.5.119:1180	61.152.242.233:80	00:00:01	3.105 KB	2.578 KB	540 B	15	10	5	HTTP
192.168.5.119:1184	61.152.242.233:80	00:00:02	4.265 KB	2.721 KB	1.544 KB	15	10	5	HTTP
192.168.5.119:1185	61.152.242.233:80	00:00:01	4.228 KB	2.725 KB	1.503 KB	15	10	5	HTTP
192.168.5.119:1186	61.152.241.136:80	00:00:01	3.236 KB	1.602 KB	1.635 KB	15	10	5	HTTP
192.168.5.119:1187	61.152.242.233:80	00:00:01	4.631 KB	1.600 KB	3.031 KB	16	10	6	HTTP
192.168.5.119:1188	61.152.242.233:80	00:00:01	6.762 KB	1.723 KB	5.039 KB	19	12	7	HTTP

数据包 数据流 时序图							
192.168.5.119 <-> 207.46.49.134\数据包: 13							
编号	绝对时间	源	目标	协议	大小	解码字段	概要
182	15:16:10.772278	192.168.5.119:1149	207.46.49.134:80	HTTP	66		序列号=2335876036, 确认号=...
183	15:16:10.772631	192.168.5.119:1149	207.46.49.134:80	HTTP	66		序列号=2335876036, 确认号=...
184	15:16:11.208645	207.46.49.134:80	192.168.5.119:1149	HTTP	64		序列号=2431693581, 确认号=...
185	15:16:11.208717	192.168.5.119:1149	207.46.49.134:80	HTTP	58		序列号=2335876037, 确认号=...
186	15:16:11.208919	192.168.5.119:1149	207.46.49.134:80	HTTP	64		序列号=2335876037, 确认号=...
187	15:16:11.209110	192.168.5.119:1149	207.46.49.134:80	HTTP	477		C: GET /c.gif?di=361pi=33...
188	15:16:11.209236	192.168.5.119:1149	207.46.49.134:80	HTTP	477		C: GET /c.gif?di=361pi=33...
189	15:16:11.484108	207.46.49.134:80	192.168.5.119:1149	HTTP	495		S: HTTP/1.1 302 Redirect
190	15:16:11.484168	207.46.49.134:80	192.168.5.119:1149	HTTP	64		序列号=2431694019, 确认号=...

☐ UDP 会话视图

与 TCP 会话类似，UDP 会话视图详细展现了网络中的 UDP 通讯情况。

通过对 UDP 会话的分析，同样可以帮助我们分析网络中的蠕虫病毒、DDOS 攻击等安全问题，UDP 会话视图如下图所示：

我的图表 概要 诊断 协议 物理端点 IP端点 物理会话 IP会话 TCP会话 UDP会话 矩阵 数据包 日志 报表										
全面分析\UDP会话: 1,736										
节点1->	<-节点2	持续时间	字节	字节->	<-字节	数据包	数据包 ->	<- 数据包	协议	
CAIZY-PC:63477	61.139.2.69:53	00:00:00	414 B	80 B	334 B	2	1	1	DNS	
192.168.5.17:51776	224.0.0.252:5355	00:00:00	136 B	136 B	0 B	2	2	0	Other	
CAIZY-PC:59099	61.139.2.69:53	00:00:00	446 B	95 B	351 B	2	1	1	DNS	
CAIZY-PC:61820	61.139.2.69:53	00:00:00	373 B	93 B	280 B	2	1	1	DNS	
192.168.5.17:57410	224.0.0.252:5355	00:00:00	140 B	140 B	0 B	2	2	0	Other	
192.168.5.13:2222	239.255.255.250...	00:00:05	537 B	537 B	0 B	3	3	0	SSDP	
CAIZY-VM:65213	61.139.2.69:53	00:00:00	392 B	172 B	220 B	3	2	1	DNS	
192.168.5.7:2275	239.255.255.250...	00:00:06	537 B	537 B	0 B	3	3	0	SSDP	
192.168.4.7:2276	239.255.255.250...	00:00:06	537 B	537 B	0 B	3	3	0	SSDP	
192.168.200.7:2277	239.255.255.250...	00:00:06	537 B	537 B	0 B	3	3	0	SSDP	
192.168.2.7:2278	239.255.255.250...	00:00:06	537 B	537 B	0 B	3	3	0	SSDP	
192.168.3.7:2279	239.255.255.250...	00:00:06	537 B	537 B	0 B	3	3	0	SSDP	
192.168.5.7:2334	239.255.255.250...	00:00:06	537 B	537 B	0 B	3	3	0	SSDP	
192.168.4.7:2335	239.255.255.250...	00:00:06	537 B	537 B	0 B	3	3	0	SSDP	
192.168.200.7:2336	239.255.255.250...	00:00:06	537 B	537 B	0 B	3	3	0	SSDP	

数据包 数据						
192.168.5.56 <-> 222.215.75.169\数据包: 66						
编号	绝对时间	源	目标	协议	大小	概要
8614	10:43:50.667451	222.215.75.169:13901	192.168.5.56:11762	UDP	85	源端口=13901;目标端口=11762;长度=47;...
8631	10:43:53.564855	222.215.75.169:13901	192.168.5.56:11762	UDP	64	源端口=13901;目标端口=11762;长度=25;...
8633	10:43:54.360832	222.215.75.169:13901	192.168.5.56:11762	UDP	169	源端口=13901;目标端口=11762;长度=131;...
8634	10:43:54.368752	222.215.75.169:13901	192.168.5.56:11762	UDP	71	源端口=13901;目标端口=11762;长度=33;...
8635	10:43:54.371375	222.215.75.169:13901	192.168.5.56:11762	UDP	71	源端口=13901;目标端口=11762;长度=33;...
8636	10:43:54.515845	222.215.75.169:13901	192.168.5.56:11762	UDP	64	源端口=13901;目标端口=11762;长度=25;...
8637	10:43:55.421706	222.215.75.169:13901	192.168.5.56:11762	UDP	85	源端口=13901;目标端口=11762;长度=47;...
8638	10:43:55.423274	222.215.75.169:13901	192.168.5.56:11762	UDP	71	源端口=13901;目标端口=11762;长度=33;...
8639	10:43:55.425168	222.215.75.169:13901	192.168.5.56:11762	UDP	71	源端口=13901;目标端口=11762;长度=33;...
8640	10:43:55.575537	222.215.75.169:13901	192.168.5.56:11762	UDP	64	源端口=13901;目标端口=11762;长度=25;...
8642	10:43:56.302266	222.215.75.169:13901	192.168.5.56:11762	UDP	169	源端口=13901;目标端口=11762;长度=131;...

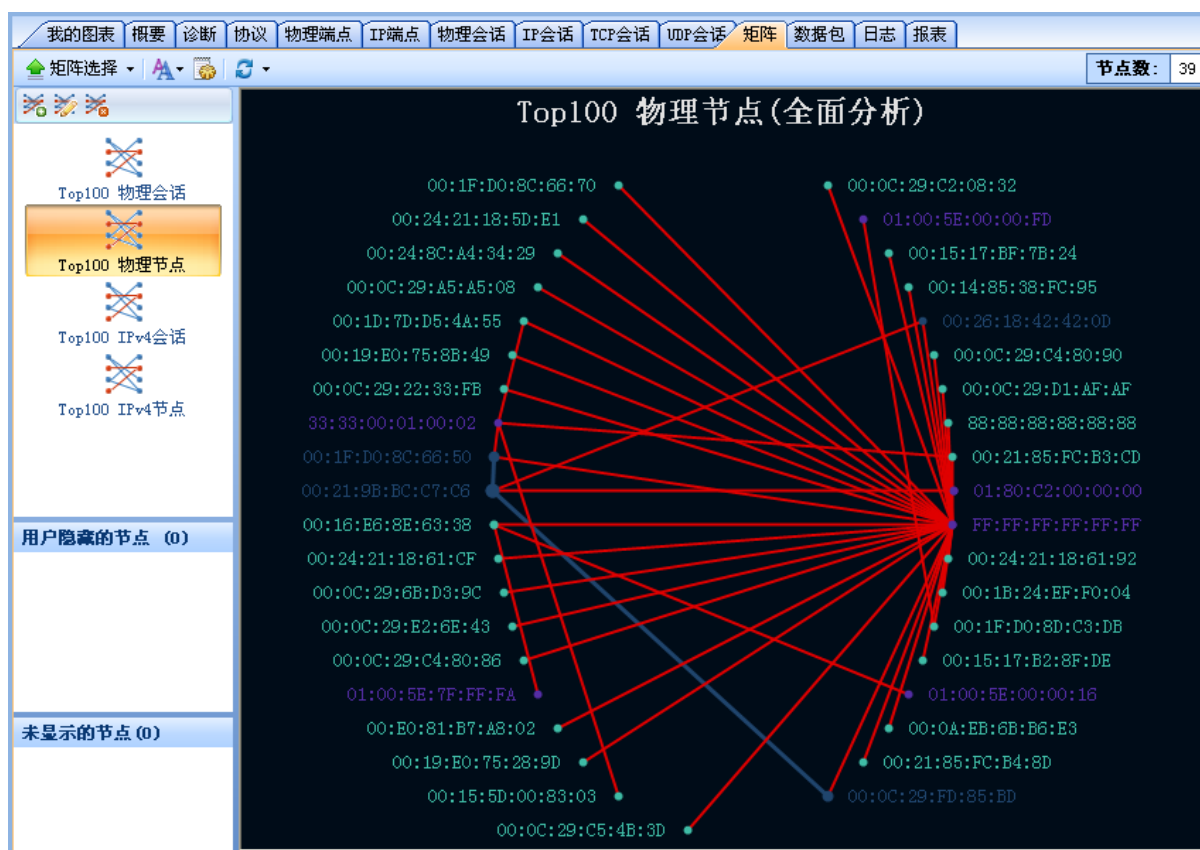
☐ 矩阵

矩阵视图用于实时显示网络通讯的节点和会话信息。用户可以选择不同的类型来查看矩阵视图，矩阵类型有物理矩阵和IP矩阵两种，同时只能选择查看一种类型的矩阵。

- ☐ 物理：根据物理地址（MAC地址）节点显示矩阵内容；
- ☐ IP地址：根据IP地址节点显示矩阵内容。

科来网络分析系统 2010 默认提供了 TOP 100 物理会话矩阵与物理节点矩阵以及 TOP 100 IPv4 会话矩阵与 IPv4 节点矩阵。您可以通过矩阵视图工具栏的“添加矩阵”按钮自定义矩阵显示。

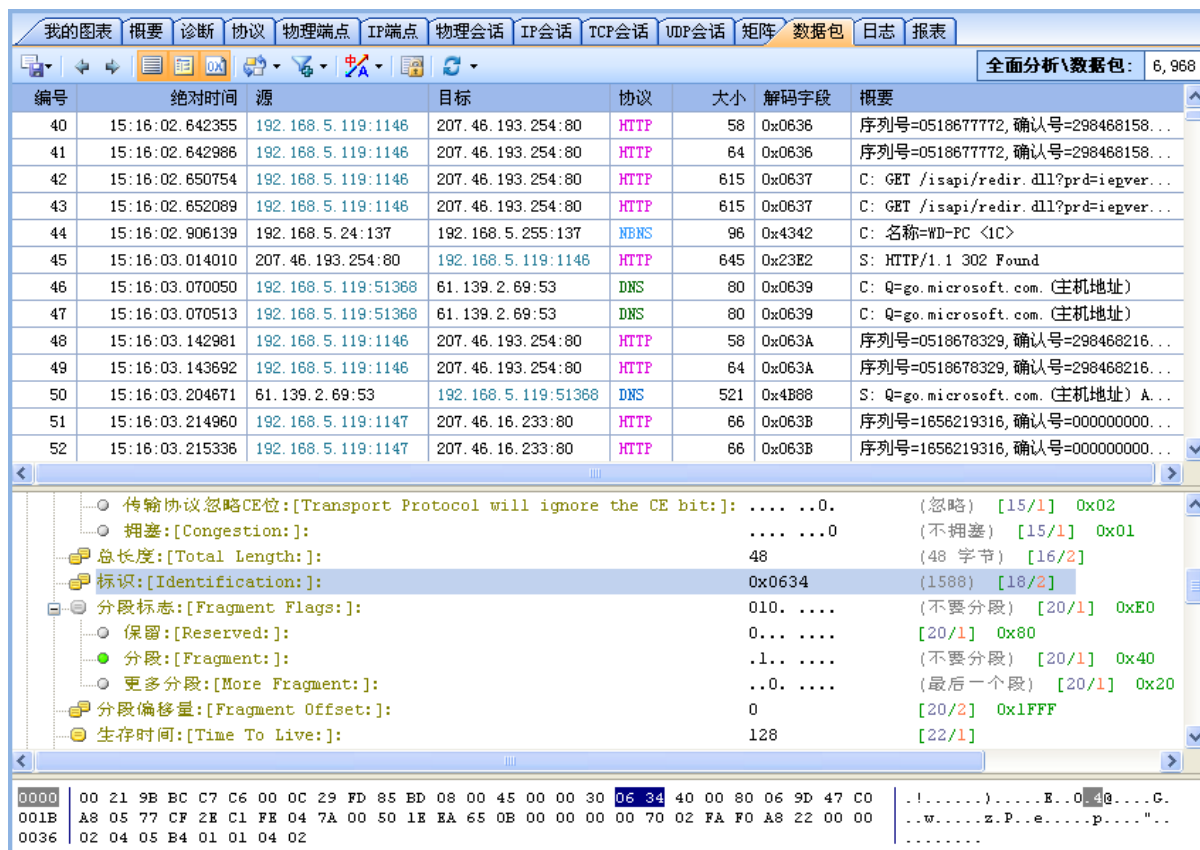
矩阵视图如下图所示：



☐ 数据包

在数据包视图中,我们可以详细查看网络中原始的数据包通讯情况,系统对每个数据包进行详细分析和界面,包括:概要解码,字段解码,十六进制解码。

科来网络分析系统 2010 提供实时捕捉、实时解码功能,对捕获到的每个数据包进行实时分析和解码,帮助您快速分析网络通讯,如下图所示:



从上图可以看到：数据包视图包括概要解码、详细字段解码、HEX 解码以及 ASCII 解码。您也可以通过详细的字段解码分析原始的数据通讯，以帮助快速定位可疑的网络数据包。此外，概要解码中的解码列字段可以帮助您进行数据包之间的解码对比。通过对数据包的详细解码分析，即便是精心伪造的网络攻击、欺骗数据包在这种模式下也无所遁形。

☐ 日志

科来网络分析系统提供常见网络应用的日志显示及保存。每个日志由相应的分析模块提供，是否显示该日志由分析方案的设置决定。日志包括以下类型：

- 全局日志
- DNS 日志
- Email 日志
- HTTP 日志
- FTP 日志

系统提供全局日志汇总显示，将各应用分析方案提供的日志汇总显示，也可单独显示某种类型的日志，方便您发现数据关联，帮助网络问题排查。日志视图如下图所示：

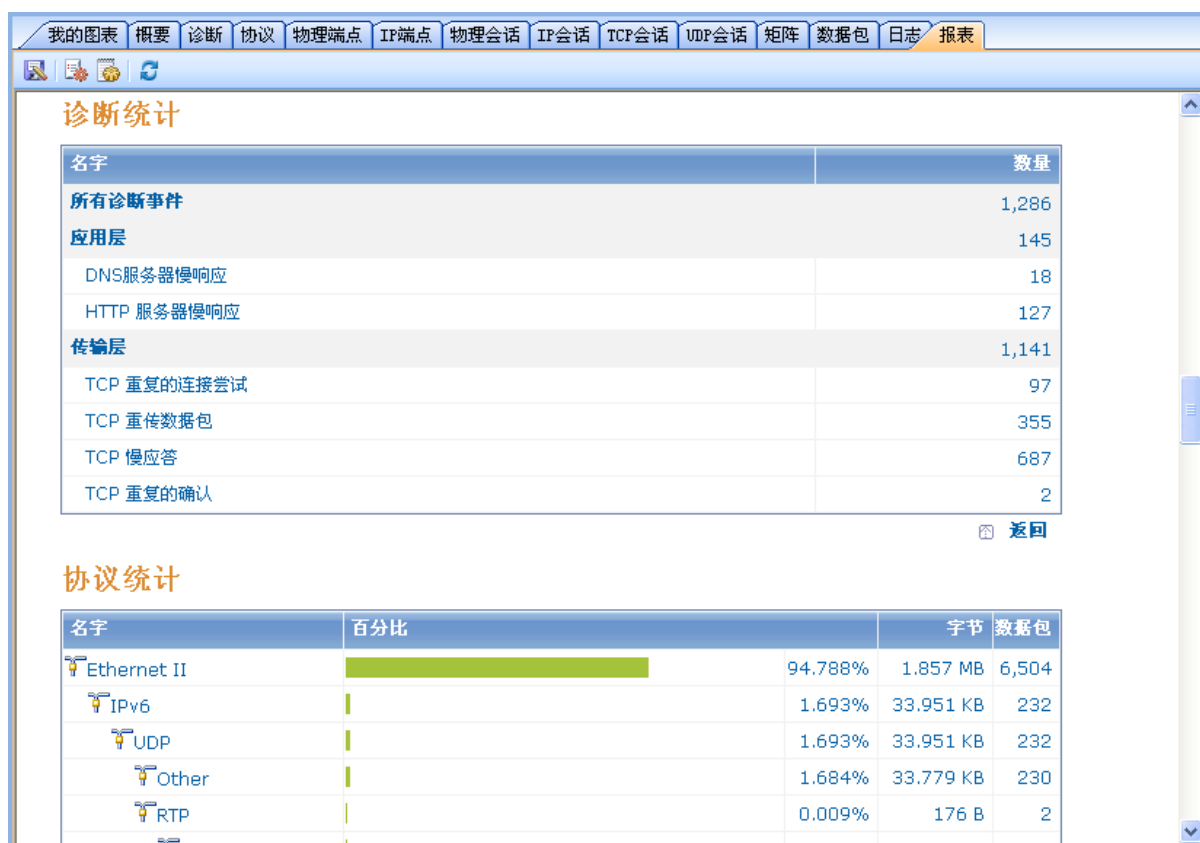
我的图表 概要 诊断 协议 物理端点 IP端点 物理会话 IP会话 TCP会话 UDP会话 矩阵 数据包 日志 报表			
全局日志			全面分析\日志: 238
日志	时间	协议	信息
全局日志	2010/01/07 13:12:12	DNS	DNS查询 : www.colasoft.com.cn 成功
DNS日志	2010/01/07 13:12:13	HTTP	GET http://www.colasoft.com.cn/pub/css/base.css
Email信息	2010/01/07 13:16:13	DNS	DNS查询 : groupfile2.qq.com 成功
FTP传输	2010/01/07 13:20:52	DNS	DNS查询 : pop3.colasoft.com 成功
HTTP请求日志	2010/01/07 13:21:02	DNS	DNS查询 : safebrowsing.clients.google.com 成功
	2010/01/07 13:21:03	DNS	DNS查询 : safebrowsing-cache.google.com 成功
	2010/01/07 13:21:03	HTTP	GET http://safebrowsing-cache.google.com/safebrowsing/rd/goog-phish...
	2010/01/07 13:21:03	HTTP	GET http://safebrowsing-cache.google.com/safebrowsing/rd/goog-phish...
	2010/01/07 13:12:12	HTTP	GET http://www.colasoft.com.cn/onlineresource.html?session=csnas_ult...
	2010/01/07 13:23:06	DNS	DNS查询 : secure.colasoft.com.cn 成功
	2010/01/07 13:20:52	HTTP	GET http://www.wildpackets.com/rss/news.xml
	2010/01/07 13:20:53	HTTP	GET http://blog.wildpackets.com/atom.xml
	2010/01/07 13:21:03	HTTP	GET http://safebrowsing-cache.google.com/safebrowsing/rd/goog-phish...
	2010/01/07 13:20:52	HTTP	GET http://www.ctocio.com.cn/index.xml
	2010/01/07 13:21:02	HTTP	POST http://safebrowsing.clients.google.com/safebrowsing/downloads?...
	2010/01/07 13:49:28	DNS	DNS查询 : safebrowsing.clients.google.com 成功
	2010/01/07 13:49:29	DNS	DNS查询 : safebrowsing-cache.google.com 成功
	2010/01/07 13:49:29	HTTP	GET http://safebrowsing-cache.google.com/safebrowsing/rd/goog-phish...
	2010/01/07 13:50:46	DNS	DNS查询 : office.microsoft.com 成功
	2010/01/07 13:51:05	DNS	DNS查询 : pop3.colasoft.com 成功
	2010/01/07 13:52:09	DNS	DNS查询 : www.microsoft.com 成功
	2010/01/07 13:52:09	DNS	DNS查询 : go.microsoft.com 成功
	2010/01/07 13:52:41	DNS	DNS查询 : www.google.cn 成功
	2010/01/07 13:52:41	HTTP	GET http://www.google.cn/
	2010/01/07 13:52:48	HTTP	GET http://www.google.cn/gen_204?atyp=ighp=fbg
	2010/01/07 13:52:49	HTTP	GET http://www.google.cn/extern_js/f/CgV6aC1DThICY24rMAo4UEACLCSwDj...
	2010/01/07 13:52:59	DNS	DNS查询 : images.google.cn 成功

☐ 报表

科来网络分析系统 2010 提供丰富的报表定制,可以帮助您生成各种统计数据的报表。并且,您可以配合节点浏览器的选择,自定义生成各种网络对象的报表显示。

此外,您可以自定义报表显示,可指定报表中的公司标识,名称,报表前缀,创建人员和生成时间。还可以指定 TOP-N 类型的显示数量。

报表输出存储类型支持常见的 PDF 电子文档, MHT 复合文档和 HTML 格式文档,如下图所示:



2.5 警报浏览器

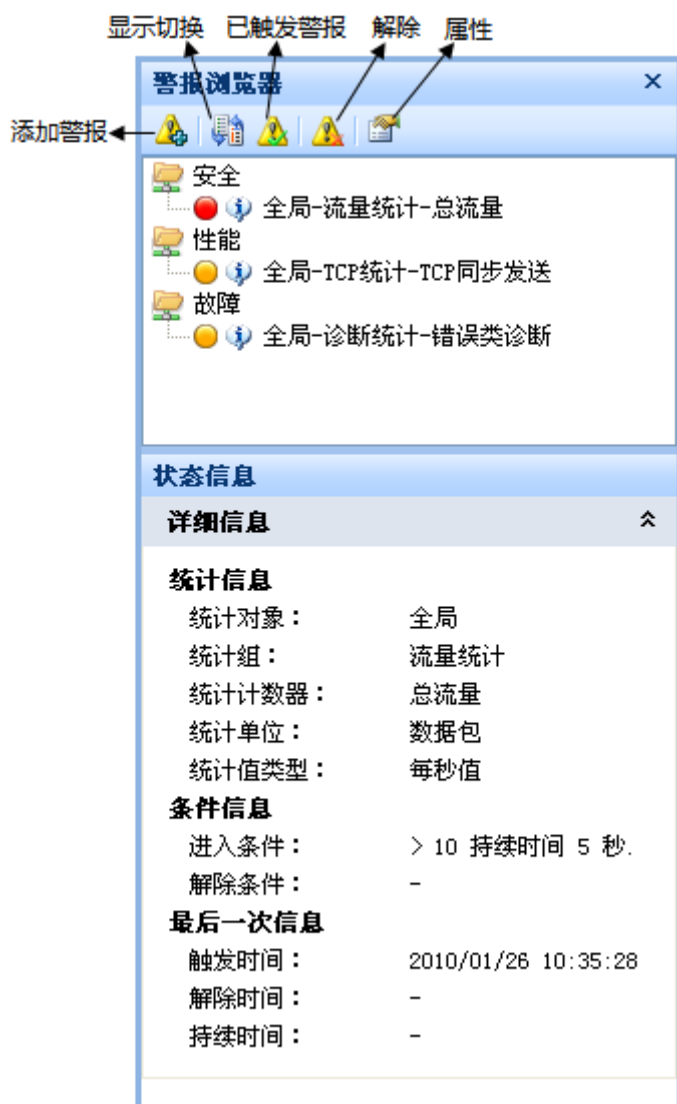
系统提供实时全局实时警报，以醒目的方式提醒管理员当前事件。并在主视图右下角显示当前触发的警报数量。

您可以按照安全、性能、故障 3 种类型自定义创建各种警报，并且可从多个视图中对选中的网络对象进行警报创建及警报日志自动保存。

每种警报有以下属性：

- 警报对象
- 警报类型（安全，性能，故障），严重程度（信息，通知，警告，错误）。
- 丰富的警报统计数据来源。
- 设置警报进入条件
- 设置警报解除条件
- TOP10 流量统计（触发警报时各种 TOP10 流量的统计快照）

系统警报浏览器下图所示：



2.6 状态栏

系统提供全局状态栏显示，状态栏包括以下信息：

- 当前分析模式与分析方案名称
- 网络适配器或回放文件再选择及状态显示
- 数据包捕捉过滤器状态显示与设置
- 工程数据统计，包括持续时间，包捕捉过滤统计
- 警报状态显示与设置

状态栏如下图所示：



您可以在状态栏中单击网络适配器或过滤器图标，快速进入网络适配器选择及过滤器设置。

3. 分析方案设置

分析方案设置是对网络数据捕捉时进行条件设置的地方，用户在进行数据包捕获的时候，可以自定义设置网络分析对象、数据包缓存大小及保存、网络事件的诊断设置以及日志设置。分析方案设置主要包括以下 4 部份：

- ☑ 分析对象设置 - 主要设置是否启用网络对象分析和统计以及分析对象的数量设置
- ☑ 数据包存储设置 - 主要设置数据包缓存及自动保存数据包
- ☑ 日志设置- 主要设置是否分析各种应用日志以及日志记录与保存
- ☑ 诊断设置 - 自定义需要诊断的网络事件，对网络内的错误信息或故障信息进行自动提示

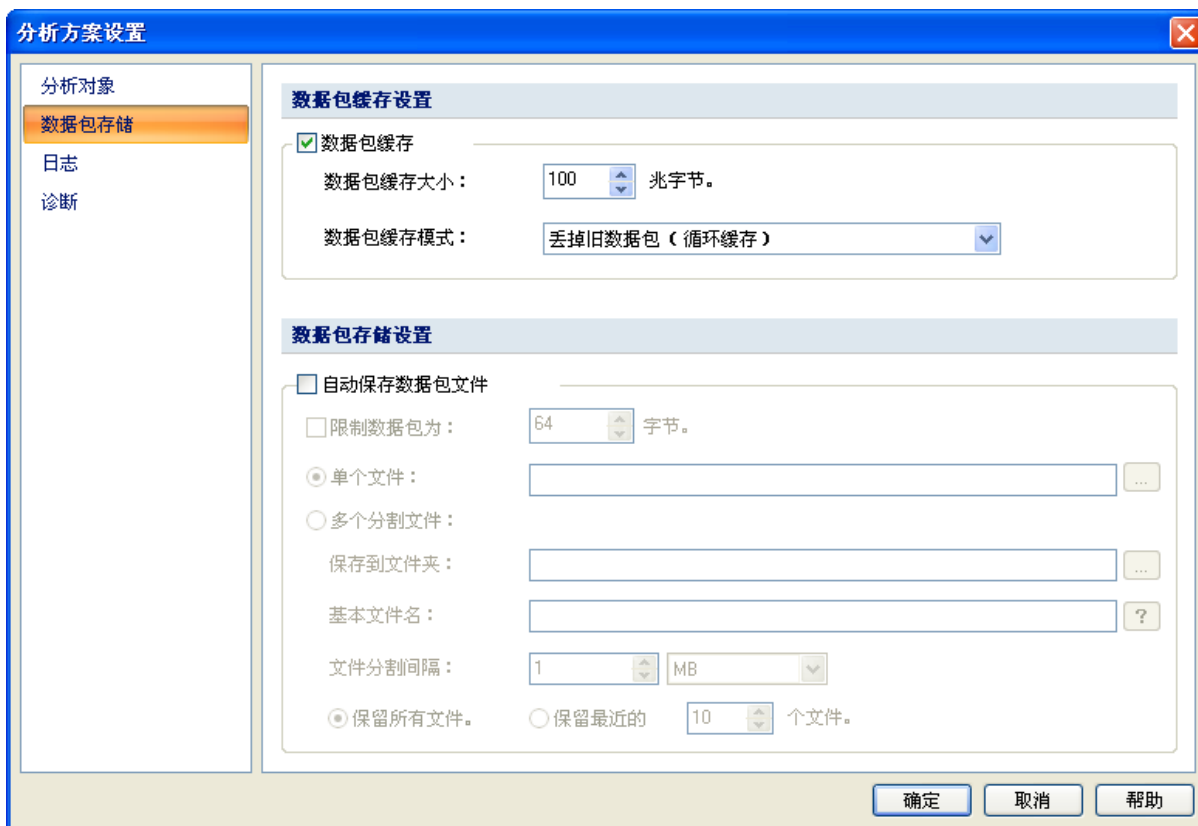
3.1 分析对象



分析对象设置对话框中，您可以设置需要启用和分析的网络分析对象、分析协议明细以及分析的最大对象数量设置。

系统默认开始全部分析对象，您可以关闭某些不需要的网络对象数据分析，如远程 IP 地址、物理地址组、IP 地址组等，也可以关闭网络对象的分析协议明细。如果您关闭分析对象中的物理会话，那么，系统将不会统计和分析网络中的所有物理会话，如果您打开物理会话而关闭物理会话的分析协议明细，那么将不会统计通讯协议的物理会话，即当您在节点浏览器中选择某个协议的时候，其物理会话视图为空。此外，您还可以设置网络对象的分析数量，最大分析数量为 10000 个。

3.2 数据包存储



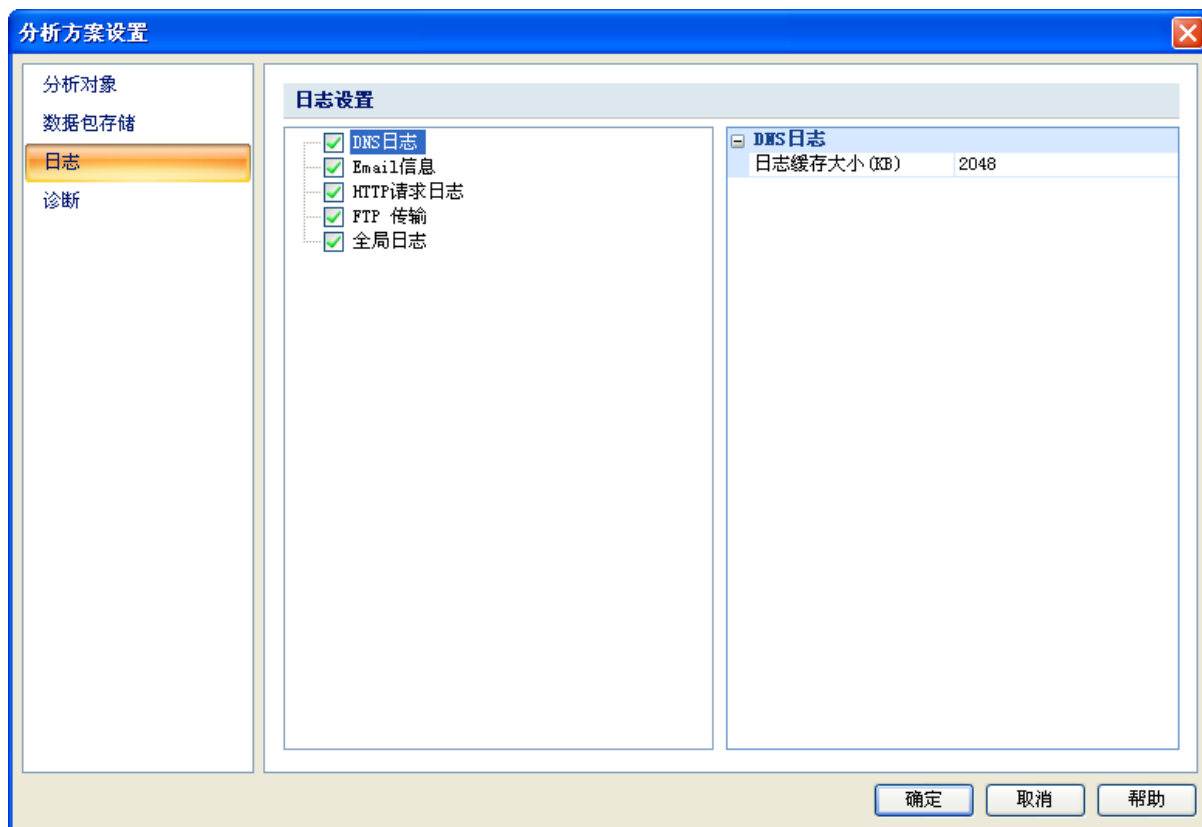
在数据包存储设置对话框中，主要针对数据包缓存设置（默认 16M）以及数据包缓存模式设置，系统默认设置为：当缓存满时，丢掉旧数据包，即循环缓存。

您也可以设置自动保存数据包文件，将采集到的数据包进行自动保存，以便将原始数据信息保存下来供以后分析；保存的数据包文件可以是单个的文件，也可以按照时间或大小分隔保存为多个文件。

3.3 日志

日志设置对话框中，您可以开启或关闭某种日志的自动保存。如果您在该对话框中关闭某种日志，那么，在系统主界面的日志视图中，将不会显示该日志。

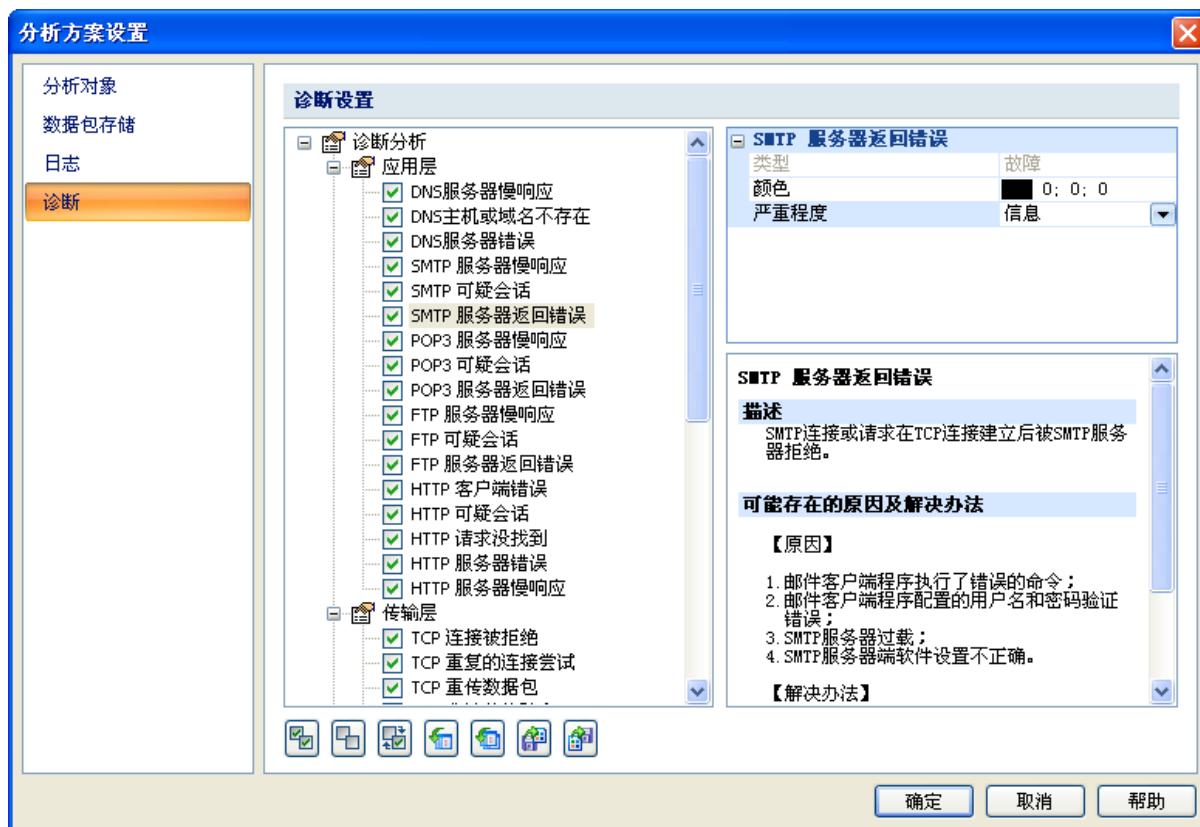
您也可以在该对话框中设置保存日志的缓存大小以及设置自动保存日志文件。



3.4 诊断

诊断设置对话框中，包含了系统支持的所有诊断事件，用户可以根据自身的网络情况，更改诊断事件的设置，如颜色、严重程度、条件阈值等。如果不想进行诊断的事件，用户也可以在列表中，取消该事件的诊断应用。

诊断设置中，所有的诊断事件都是以协议层来分类，即应用层、传输层、网络层、数据链路层。这样我们对于网络出现的故障，我们便能很快判断出是网络的哪一层出了问题。系统对每个诊断事件都提供了事件描述、可能发生的原因，以及可采取的解决方案，这些信息对故障的排除是非常有参考价值的。



4. 数据管理

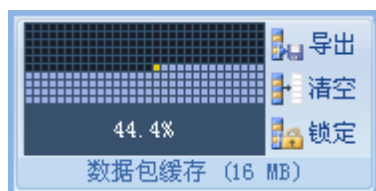
科来网络分析系统 2010 可以对捕获的数据包文件进行有效管理。

4.1 数据包

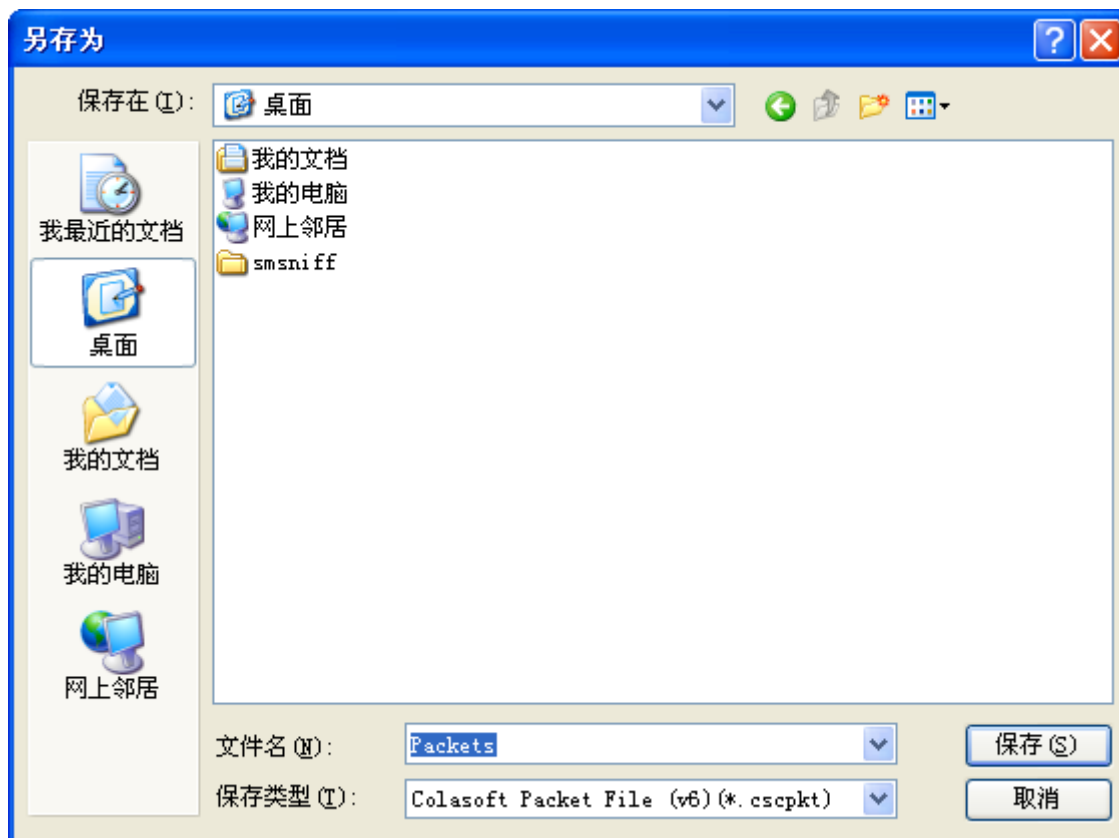
科来网络分析系统 2010 支持对工程中单个和多个数据包以特定的格式保存，同时也可以导入多个数据包文件。

☐ 导出数据包

单击工具栏中数据包缓存状态显示旁的“导出”按钮，或者在主视图区的数据包视图的工具条中，单击“导出”，则可以将捕获的数据包导出保存。



对于捕获数据的保存，你也可以将数据内容导出到一个特定格式的文件。科来网络分析系统 2010 除了支持基本的 cscpkt 格式的文件，也支持通用的 Sniffer、Omnipeek 等工具的文件格式。用户也可以设置需要导出的数据内容，如下图所示：



单击保存类型的下拉列表框，可以保存为以下类型的数据包格式：

- Colasoft Packet File (v6) (*.cscpkt)
- Colasoft Raw Packet File (*.rawpkt)
- Accellent 5Views Packet File (*.5vw)
- 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)

导入数据包

科来网络分析系统 2010 支持多种通用数据包格式的回放导入和分析，你可以在引导界面中选择“回放分析”模式导入数据包文件，如下图。



单击“添加”按钮选择需要导入分析的数据包文件，在进行回放分析之前，您可以设置过滤器来分析特定的数据。并且，回放分析同样也可以选择不同的分析方案、网络档案以及多种回放速度，在设置相关的条件后，单击“开始”打开相应的分析方案，就可以开始数据包的导入了。

科来网络分析系统 2010 支持导入回放的数据包格式如下：

- ☑ Colasoft Packet File (v6) (*.cscpkt)
- ☑ Colasoft Raw Packet File (*.rawpkt)
- ☑ 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 LANalyzer (*.tr1)
- ☑ Network Instruments Observer v9.0 (*.bfr)
- ☑ NetXRay2.0,and Windows Sniffer (*.cap)
- ☑ Sun_Snoop (*.Snoop)
- ☑ Visual Network Traffic Capture (*.cap)