

# 科来网络回溯分析系统

## 技术白皮书

# 科来网络回溯分析系统

## 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。

© 2011 科来软件 保留所有权利

科来软件 北京营销中心  
电话 : 010-82601814  
传真 : 010-82601614  
网址 : <http://www.colasoft.com.cn>

# 目录

目录 .....	1
<b>1. 科来网络回溯分析系统 .....</b>	<b>2</b>
1.1 应用背景 .....	2
1.2 产品概述 .....	2
<b>2. 系统组成及架构 .....</b>	<b>3</b>
2.1 系统组成 .....	3
2.2 功能架构 .....	3
2.3 产品部署 .....	4
<b>3. 系统亮点 .....</b>	<b>5</b>
3.1 分布式集中监控分析 .....	5
3.2 长期的数据存储 .....	5
3.3 快捷的历史数据回溯 .....	6
3.4 快速易用的数据挖掘 .....	7
3.5 持续的网络流量监控 .....	8
3.6 全面深入的精细分析 .....	8
<b>4. 技术特性 .....</b>	<b>11</b>
4.1 灵活的系统架构，易于部署 .....	11
4.2 高性能的数据采集 .....	11
4.3 海量的网络数据存储 .....	11
4.4 直观的流量趋势导航 .....	11
4.5 基于时间的数据过滤 .....	12
4.6 基于网络对象的数据挖掘 .....	12
<b>5. 应用价值 .....</b>	<b>12</b>
5.1 网络运行状态，全面掌握 .....	12
5.2 网络历史回溯，主动出击 .....	12
5.3 网络数据存储，轻松实现 .....	13
5.4 网络故障挖掘，追本溯源 .....	13
<b>6. 联系我们 .....</b>	<b>13</b>

# 1. 科来网络回溯分析系统

## 1.1 应用背景

随着网络信息化的全面建设和快速发展，网络中承载了越来越多的关键业务及应用，企业随时面临因网络故障而导致的业务中断、经济损失等各种运营威胁，传统的便携式网络分析产品虽然能够实时监控运行状态，及时发现网络异常通讯行为，快速定位网络及应用故障，对保障企业关键业务的高效运行起到了非常关键的作用，但是，面对越来越复杂的网络问题，如何从海量的网络数据中快速发现异常，如何在网络故障发生后快速重现故障现象并分析故障原因，如何提供长期的数据存储并快速提取历史数据进行精细的数据挖掘分析，是当前企业网络管理面临的新的挑战，便携式实时网络分析产品面对新的网络管理需求时，存在以下不足：

- ☒ 无法实现长期的数据保存
- ☒ 无法实现持续的流量监控
- ☒ 无法查看分析历史通讯数据
- ☒ 无法还原历史故障现象
- ☒ 无法进行网络链路统一集中管理
- ☒ 故障回溯分析能力欠缺

因此，针对新的网络管理挑战，科来软件提供了高性能的网络回溯分析系统，使用灵活、简单的系统架构，实现了长期、大容量的数据存储、历史数据回溯及持续的网络流量监控，为企业网络管理提供了全新的解决方案。

## 1.2 产品概述

科来网络回溯分析系统是科来软件全新推出的网络回溯分析产品，实现了海量的数据存储及快速的历史数据回溯分析功能。系统提供千兆网络流量数据实时采集、实时分析、高效存储，提供历史问题回溯以及简单高效的数据挖掘技术，帮助用户重现发生故障时的历史网络通讯状态，快速分析当时的网络故障原因。同时，系统支持与便携式网络分析系统进行无缝结合，能够对挖掘的网络数据进行精细化的二次分析，实现集中、高效的网络管理需求。科来网络回溯分析系统主要功能包括：

- ☒ 网络原始通讯数据实时采集、分析；
- ☒ 大容量的数据存储；
- ☒ 长期的网络流量监控与统计；
- ☒ 历史数据回溯分析；
- ☒ 网络数据挖掘与检索；
- ☒ 远程实时分析、监控与管理；

## 2. 系统组成及架构

### 2.1 系统组成

科来网络回溯分析系统由三部分组成，包括回溯分析服务器、回溯分析控制台以及分布式网络分析中心。

#### 回溯分析服务器：

回溯分析服务器主要负责目标网络的流量采集、分析和存储，同时，提供通讯口分别与回溯分析控制台与分布式网络分析中心进行数据交互，是整个系统的核心。

#### 回溯分析控制台：

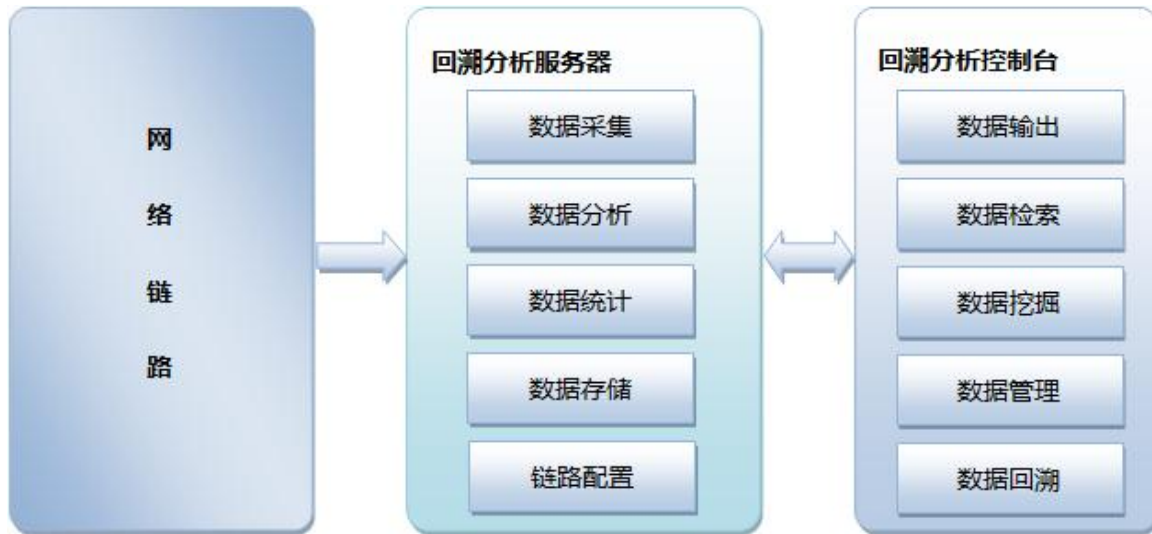
回溯分析控制台采用了全新的界面与布局，提供人机交互界面，用于连接回溯分析服务器并实时输出各类通讯数据。网络管理员通过控制台可以连接到不同支干网中的分析服务器，以查看和分析该支干网的网络通讯状况。

#### 分布式网络分析中心：

分布式网络分析中心提供统一、集中的监控分析平台，通过定期收集与统计部署在各网络链路中的回溯分析服务器上报的数据，提供集中的数据展现，同时实现对回溯分析服务器的集中管理和配置，提供集中管理、监控、分析报表、警报等功能。

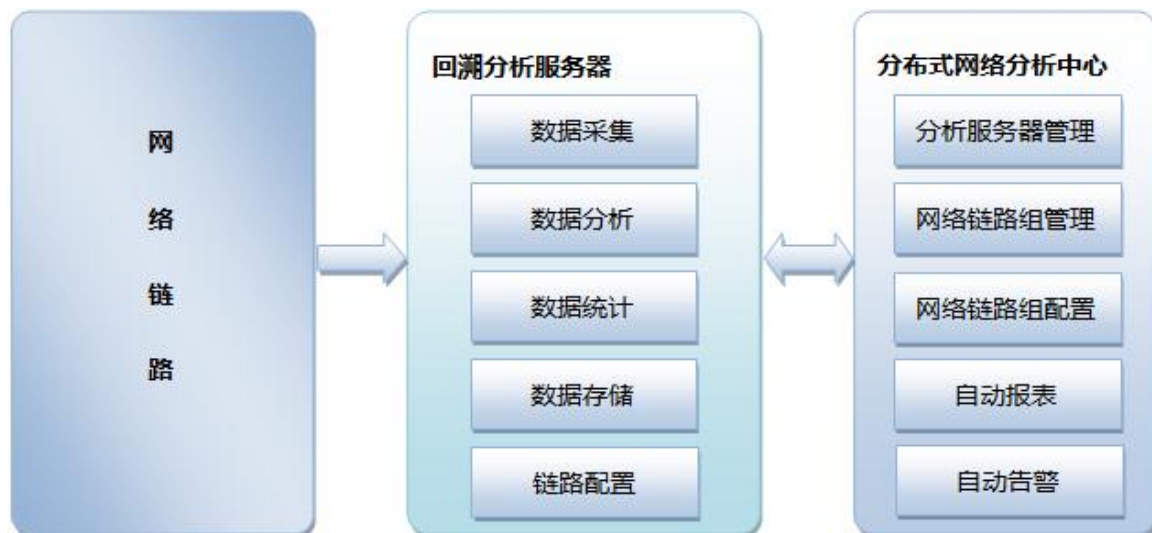
### 2.2 功能架构

回溯分析服务器与分析控制台采用 C/S 技术架构，服务器实时响应控制台命令并及时返回相应数据，当管理员需要监控分析指定的目标网络时，则可通过回溯分析控制台连接到服务器进行远程实时分析和回溯分析。回溯分析服务器与控制台的功能架构如下图所示：



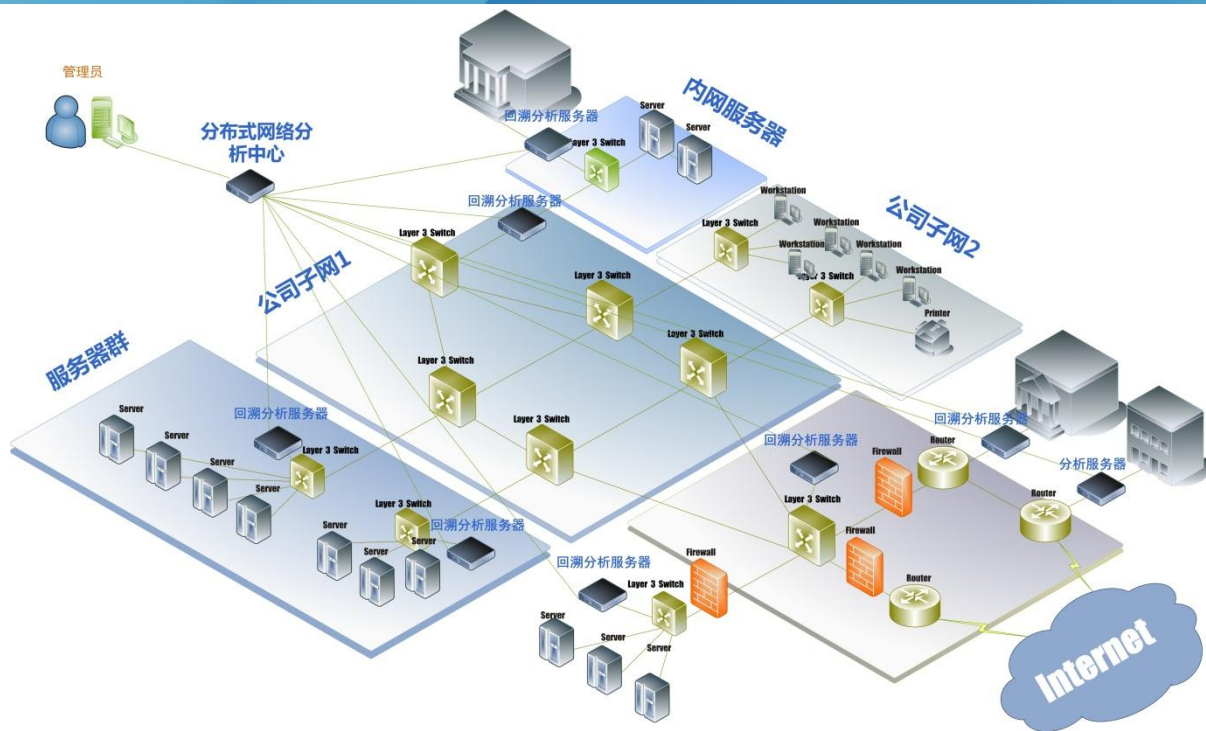
回溯分析控制台支持与服务器进行一对多并发连接,即一个回溯分析控制台可以同时管理和分析多个服务器的数据。

分布式网络分析中心与回溯分析服务器则采用了 B/S 架构,通过定期的心跳进行数据交互,实现全局的网络通讯监控。二者的功能架构如下图所示:



## 2.3 产品部署

系统基于“分布式部署、集中管理”的设计理念,安装部署简单,在需要监控的网络链路中部署回溯分析服务器用于网络流量的采集和分析;分布式网络分析中心对部署在各个网络链路中的服务器进行管理并展现其上报的各类统计数据,用户通过分析中心可实现网络整体的分布式集中管理。同时,系统提供回溯分析控制台,可连接网络中的任意一个回溯分析服务器,进行实时分析和回溯分析。产品部署如下图所示:



## 3. 系统亮点

### 3.1 分布式集中监控分析

根据网络规模及分析范围的不同,系统不仅能够实现本地网络的数据采集与存储,而且支持分布式远程部署与监控,针对网络中的关键链路,可部署多个分析服务器,用户能够随时随地通过分析控制台任意连接远程分析服务器,实现远程网络的数据分析与管理,同时,通过分析管理控制中心,可对各个关键网络链路的流量进行整体实时监控,一旦出现流量异常,及时发现及告警。

### 3.2 长期的数据存储

系统具备长时间、大容量的数据存储能力,能长期实时保存捕获的原始数据包、数据流、网络会话、应用日志等各种统计数据,同时具备快速的数据检索能力,能够方便的对已发生的网络行为、应用数据和主机数据进行回溯分析,用户可以随时分类查看及调用任意时间段的数据,当发现问题时,提供一定时间范围内的回溯分析,为迅速定位问题发生原因提供了更全面的分析依据,同时为网络安全提供了强有力的数据分析保障。

#### ☐ 数据包存储

数据包是网络通讯最真实、最原始的数据,系统支持全千兆流量的数据包长期存储功能,全面保存所有通讯的数据包,同时,系统具备灵活的扩展性,可以不断增加分析服务器的存储空间以适应存储容量的增加。

## ☑ 网络会话存储

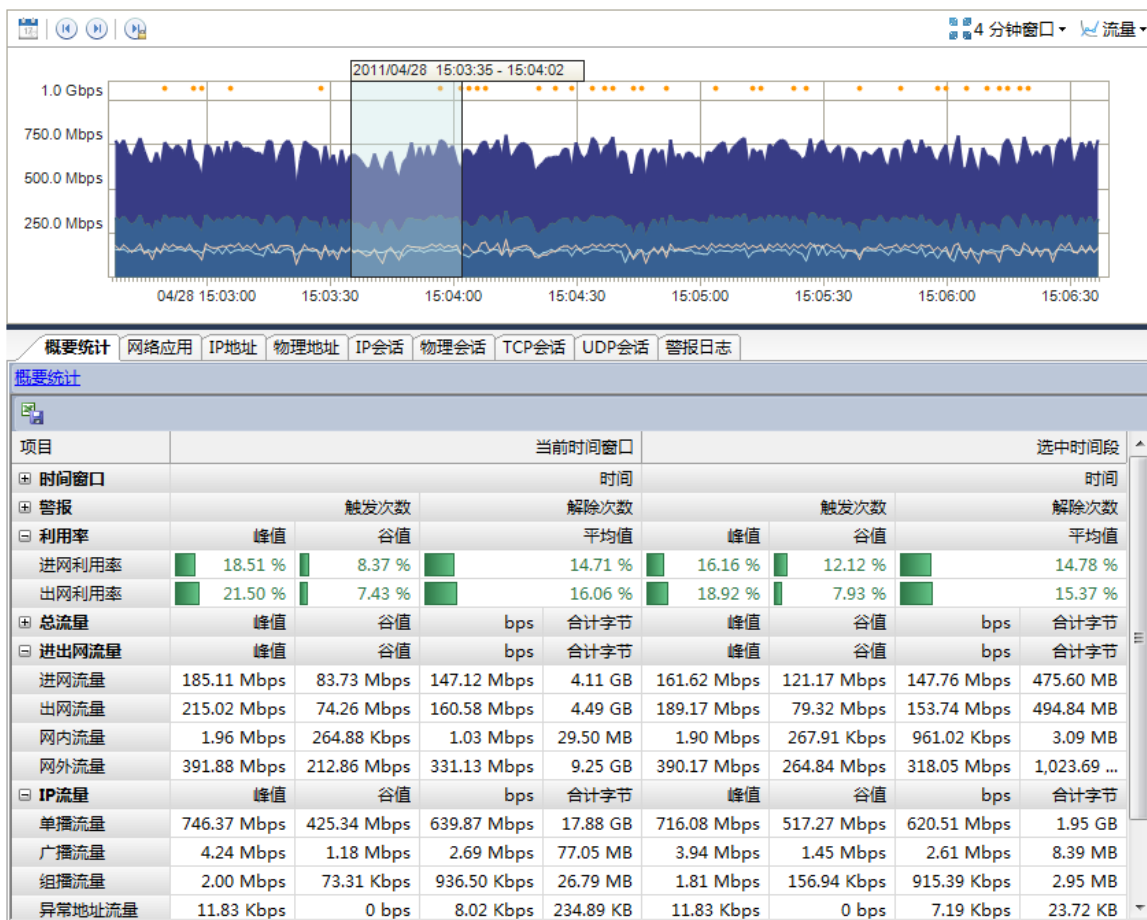
网络通讯会话是分析网络问题的关键数据之一，通过对网络会话的存储，用户可以查看和了解任意时间的网络会话信息，及时发现异常的通讯会话，快速查找各种网络问题。

## ☑ 统计数据存储

系统实时分析、统计和存储各种网络通讯数据，如协议统计、总流量、广播/组播流量、上行/下行流量、数据包、利用率等多种网络数据，帮助用户快速了解和掌握网络运行状态，及时发现异常数据。

## 3.3 快捷的历史数据回溯

当发现问题或被报告出现问题时，由于没有保存当时的数据，往往错过了最佳分析时机，不能得到有效的分析数据。科来网络回溯分析系统有效的解决了这一问题。利用存储的数据，系统能够再现历史故障现象、对稍纵即逝的问题进行精细重现，能真实再现问题产生时的异常信息，帮助用户快速发现并解决网络问题。如关键网络业务在某个时间段间歇性出现问题时，可直接将该时段的通讯数据提取出来进行分析，快速分析定位问题产生的原因。



## ☑ 回溯分析

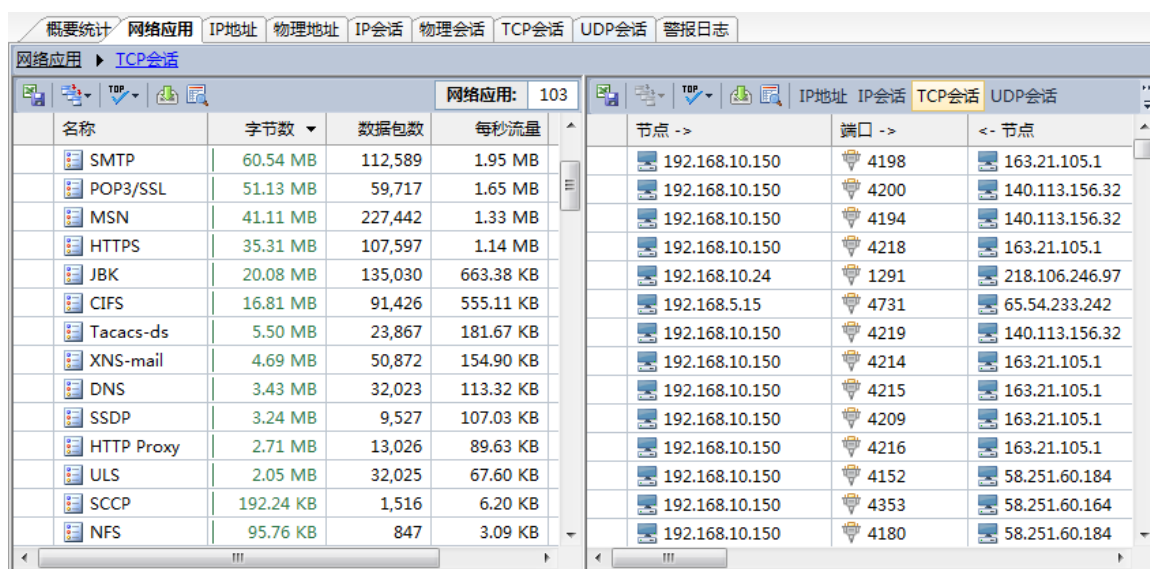
当发现网络中出现突发流量或异常流量时，及时回溯分析该时段的流量，能够及时掌握网络异常的原因，避免问题的进一步扩大；同时，对于发生的历史问题，能够快速提取该时段数据进行历史数据精细分析，不管是突发流量检测还是历史数据回溯，一切都变得轻而易举。

## ☑ 历史流量检索

某些网络问题可能并不会以异常的流量而表现，比如在过去某个时间数据库服务器响应慢，要分析此问题的原因，就需要调取分析该时段的通讯数据，正是有了长时间的数据存储能力，系统能够挖掘调取过去任意时段的历史数据，快速检索历史信息并进行精细的二次分析，快速分析并查找产生问题的原因。

## 3.4 快速易用的数据挖掘

要在海量网络数据中快速查找需要的数据，就好比在大海捞针。科来网络回溯分析系统支持快速、易用的数据挖掘功能，能引导用户从不同的视角，不同的层次快速挖掘所需要的数据。



The screenshot shows the 'Network Applications' (网络应用) tab selected, displaying a list of applications and their traffic statistics. The right pane shows a detailed view of TCP connections between nodes.

名称	字节数	数据包数	每秒流量
SMTP	60.54 MB	112,589	1.95 MB
POP3/SSL	51.13 MB	59,717	1.65 MB
MSN	41.11 MB	227,442	1.33 MB
HTTPS	35.31 MB	107,597	1.14 MB
JBK	20.08 MB	135,030	663.38 KB
CIFS	16.81 MB	91,426	555.11 KB
Tacacs-ds	5.50 MB	23,867	181.67 KB
XNS-mail	4.69 MB	50,872	154.90 KB
DNS	3.43 MB	32,023	113.32 KB
SSDP	3.24 MB	9,527	107.03 KB
HTTP Proxy	2.71 MB	13,026	89.63 KB
ULS	2.05 MB	32,025	67.60 KB
SCCP	192.24 KB	1,516	6.20 KB
NFS	95.76 KB	847	3.09 KB

节点 ->	端口 ->	<- 节点
192.168.10.150	4198	163.21.105.1
192.168.10.150	4200	140.113.156.32
192.168.10.150	4194	140.113.156.32
192.168.10.150	4218	163.21.105.1
192.168.10.24	1291	218.106.246.97
192.168.5.15	4731	65.54.233.242
192.168.10.150	4219	140.113.156.32
192.168.10.150	4214	163.21.105.1
192.168.10.150	4215	163.21.105.1
192.168.10.150	4209	163.21.105.1
192.168.10.150	4216	163.21.105.1
192.168.10.150	4152	58.251.60.184
192.168.10.150	4353	58.251.60.164
192.168.10.150	4180	58.251.60.184

## ☑ 简单易用的挖掘分析

系统提供简单易用的人机操作界面，从服务器链路到数据包库的选择，从时间趋势图到各挖掘子视图的展现，都一气呵成，轻松上手。其中时间趋势图能提供直观的网络数据流量历史展现。根据选择不同的时间窗口，流量类型，系统能自动过滤出该时间段的网络流量数据供进一步挖掘分析。

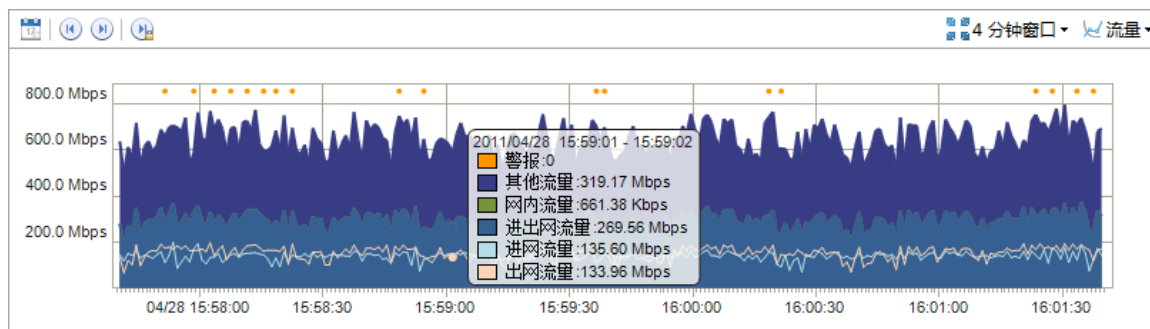
## ☑ 多角度，多层次挖掘

系统提供从网络协议，物理端点，IP 端点，物理会话，IP 会话，TCP 会话，UDP 会话等多个角度进行数据挖掘，能直观地看到各网络对象间的关联关系和数据统计结果。如通过某个协议可挖掘出其下的 IP 端点，再到 IP 端点下

的会话和最底层的数据包，层层递进，逐级挖掘。系统还支持在各层次间进行快速跳转，可方便的回溯至任意挖掘路径节点。

### 3.5 持续的网络流量监控

系统对关键网络链路提供持续的图形化流量监控功能，能够对流量数据进行长期的统计分析，主动分析网络和应用运行规律，网络行为规律，以及运行的趋势，从而帮助确立网络运行的基线，更容易发现异常。



#### 直观的流量趋势图

系统采用全新的图表控件直观的展现网络流量运行趋势，趋势图是以时间为单位，能够对各种网络流量参数进行监控和趋势展现，包括利用率（上/下行）、比特率（上/下行）、每秒数据包数（上/下行）、每秒 TCP 同步包数、TCP 同步确认包数、TCP 同步重置包数，用户可查看任意时段的流量数据。

### 异常流量检索

通过对网络流量的监控，可及时发现网络中的异常流量并进行告警，告警种类包括利用率（上/下行）、每秒数据包数（上/下行）、每秒 TCP 同步包数、每秒 TCP 同步确认包数、TCP 同步重置包数等参数报警，报警参数的阈值可以根据用户需要进行调整，同时警报可通过 email 发送给指定接收者。

### 3.6 全面深入的精细分析

在数据挖掘过程中，从选取的历史时间段得到的数据可方便的进行下载并进行二次精细分析。精细分析提供如下主要功能：

#### 专家诊断

专家诊断系统提供智能的网络故障诊断，能够根据各种网络故障、应用故障的流量特征主动发现网络中的异常，自动提示用户发生的网络故障信息，大大提高用户的故障分析效率。

我的图表 概要 诊断 x 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			
诊断条目		诊断发生地址	
诊断: 12		统计: 42	
名字	数量	名字	物理地址
所有诊断	464	192.168.0.203	00:1C:23:75:6D:7D
应用层	22	192.168.5.178	00:25:90:08:C3:52
HTTP 请求没找到	2	192.168.0.208	00:1C:23:75:6D:7D
HTTP 服务器响应	20	192.168.5.10	00:1F:D0:8C:66:50
传输层	431	192.168.0.183	00:1C:23:75:6D:7D
TCP 连接被拒绝	6	199.7.51.190	00:1C:23:75:6D:7D
TCP 重复的连接尝试	12	199.7.52.190	00:1C:23:75:6D:7D
TCP 重传数据包	19	208.77.208.79	00:1C:23:75:6D:7D
TCP 慢应答	351	203.208.37.22	00:1C:23:75:6D:7D
严重程度	类型	层别	事件描述
性能	性能	传输层	太慢的TCP应答(数据包[71289]与数据包[71...
性能	性能	传输层	太慢的TCP应答(数据包[71290]与数据包[71...
性能	性能	传输层	TCP重传数据包(请看数据包: 71362)
性能	性能	传输层	太慢的TCP应答(数据包[71366]与数据包[71...
性能	性能	传输层	太慢的TCP应答(数据包[71367]与数据包[71...
性能	性能	传输层	太慢的TCP应答(数据包[71421]与数据包[71...
性能	性能	传输层	太慢的TCP应答(数据包[71422]与数据包[71...
性能	性能	传输层	太慢的TCP应答(数据包[71458]与数据包[71...

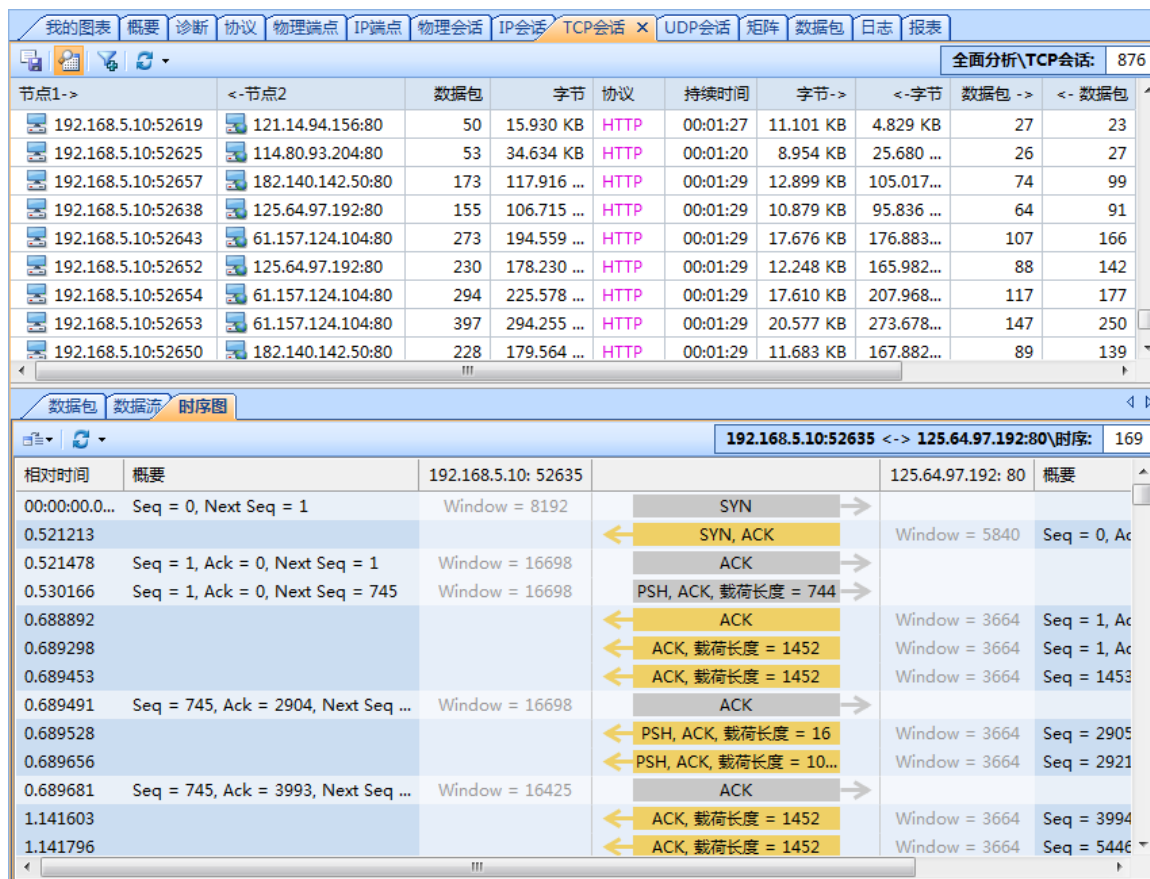
☐ 数据包解码

精细分析提供详细、直观的数据包解码分析视图，科来提供 300 多种各类网络通讯协议的解码分析能力，并且是业界唯一——一个提供中/英文双语协议解码的厂商，为用户判断分析网络问题和应用问题提供最可靠的数据依据。

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 x 日志 报表							
全面分析 数据包: 53,647							
编号	绝对时间	源	目标	协议	大小	解码字段	概要
111032	11:06:31.413699	6C:F0:49:14:CF:A3	33:33:00:01:00:03	UDP	93	FCS=0xE9E675C1	源端口=60230;目标端口=535
111033	11:06:31.413789	192.168.5.14:62621	224.0.0.252:5355	UDP	73	FCS=0xB356F4E1	源端口=62621;目标端口=535
111034	11:06:31.413873	6C:F0:49:14:CF:A3	33:33:00:01:00:03	RTCP	88	FCS=0x5B1AC9FA	源端口=55969;目标端口=535
111035	11:06:31.414019	192.168.5.14:50618	224.0.0.252:5355	RTCP	68	FCS=0x9F2BD372	RTCP_TYPE_SR   SR - Sender
111036	11:06:31.416111	6C:F0:49:14:CF:A3	33:33:00:01:00:03	UDP	91	FCS=0x0FE11FDD	源端口=49168;目标端口=535
111037	11:06:31.416545	6C:F0:49:14:CF:A3	33:33:00:01:00:03	UDP	86	FCS=0x497CA63A	源端口=63036;目标端口=535
111038	11:06:31.416742	192.168.5.14:54719	224.0.0.252:5355	UDP	71	FCS=0x3F8764ED	源端口=54719;目标端口=535
111039	11:06:31.416909	192.168.5.14:53869	224.0.0.252:5355	UDP	66	FCS=0x6849A3F2	源端口=53869;目标端口=535
<b>Packet:</b> Num:111,041 Length:92 Captured:88 Time:2011/03/10 11:06:31							
<b>以太网 - II [Ethernet Type II]:</b> [0/14]							
目标地址: [Destination Address:]: 33:33:00:01:00:03 [0/6]							
源地址: [Source Address:]: 6C:F0:49:14:CF:A3 [6/6]							
协议类型: [Protocol:]: 0x86DD [12/2]							
<b>IPv6 - 互联网协议第6版 [IPv6 - Internet Protocol Version 6]:</b> [14/40]							
版本: [Version:]: 6 [14/1] 0xF							
优先级: [Traffic Class:]: 0 [14/2] 0x0							
流标签: [Flow Label:]: 0 [15/2] 0xF							
负载数据长度: [Payload Length:]: 34 [18/2]							
上层协议: [Next Header:]: 17 [20/1]							
跳数: [Hop Limit:]: 1 [21/1]							
源地址: [Source Address:]: FE80:0000:0000:0000:64A9:1BEB:26.175.159.129 [22/16]							
目的地址: [Destination Address:]: FF02:0000:0000:0000:0000:0000:0.1.0.3 [38/16]							
<b>UDP - 用户数据报协议 [UDP - User Datagram Protocol]:</b> [54/8]							
源端口: [Source port:]: 63709 [54/2]							
目标端口: [Destination port:]: 5355 [56/2]							
长度: [Length:]: 34 [58/2]							
检验和: [Checksum:]: 0x5A66 [60/2]							
<b>Extra:</b> Bytes:26 bytes							
<b>FCS - Frame Check Sequence:</b> FCS:0xD8BC569							

## ☐ 数据流分析

数据流分析能够帮助用户快速分析网络和应用故障，系统支持对 TCP 数据流和 UDP 数据流进行深入的数据分析，对数据的传输情况，应用的交易处理过程进行深入分析，提供时序图等图形化展示，使用户对应用的数据传输过程一目了然，更加方便直观的分析定位网络应用问题。



## ☐ 日志

精细分析提供强大的应用日志分析功能，通过分析网络中的应用通讯数据对网络用户的应用访问情况进行详细分析，包括 DNS、Email、FTP、HTTP、MSN、Yahoo Messenger 等应用的详细应用日志进行分析，提供强大的网络行为分析能力。

日志	客户端	服务器地址	服务器	请求URL	方法	状态码	服务器应答
<a href="#">全局日志</a> <a href="#">DNS日志</a> <a href="#">Email信息</a> <a href="#">FTP 传输</a> <a href="#">HTTP请求日志</a> <a href="#">MSN 日志</a> <a href="#">Yahoo 日志</a>	192.168.5.10:52027	221.236.31.162	d1.sina.com.cn - http	http://d1.sina.com.cn/jianyu1/TaoBao/NB...	GET	304	HTTP/1.0 304
	192.168.5.10:52020	221.236.31.162	d1.sina.com.cn - http	http://d1.sina.com.cn/201103/09/288555 ...	GET	304	HTTP/1.0 304
	192.168.5.10:52068	221.236.31.162	d2.sina.com.cn - http	http://d2.sina.com.cn/200908/17/185943 ...	GET	304	HTTP/1.0 304
	192.168.5.10:52006	221.236.31.156	comment.sina.com.cn - http	http://comment.sina.com.cn/cmnt_embed_v5...	GET	304	HTTP/1.0 304
	192.168.5.10:51980	221.236.31.143	sports.sina.com.cn - http	http://sports.sina.com.cn/g/2011-03-10/0...	GET	200	HTTP/1.0 200
	192.168.5.10:51983	221.236.31.144	news.sina.com.cn - http	http://news.sina.com.cn/iframe/87/new20...	GET	304	HTTP/1.0 304
	192.168.5.10:51984	221.236.31.144	news.sina.com.cn - http	http://news.sina.com.cn/iframe/87/20080...	GET	304	HTTP/1.0 304
	192.168.5.10:51988	221.236.31.144	news.sina.com.cn - http	http://news.sina.com.cn/iframe/87/20080...	GET	304	HTTP/1.0 304
	192.168.5.10:51990	221.236.31.144	news.sina.com.cn - http	http://news.sina.com.cn/iframe/js/sinasav...	GET	304	HTTP/1.0 304
	192.168.5.10:51989	221.236.31.144	pfp.sina.com.cn - http	http://pfp.sina.com.cn/iframe/14/2011/02...	GET	200	HTTP/1.0 200
	192.168.5.10:51994	221.236.31.144	pfp.sina.com.cn - http	http://pfp.sina.com.cn/pfpnew/info/res_1...	GET	200	HTTP/1.0 200
	192.168.5.10:52004	221.236.31.144	pfp.sina.com.cn - http	http://pfp.sina.com.cn/iframe/tblog/new/...	GET	304	HTTP/1.0 304
	192.168.5.10:52003	221.236.31.143	sports.sina.com.cn - http	http://sports.sina.com.cn/iframe/906/201...	GET	200	HTTP/1.0 200
	192.168.5.10:51996	121.14.1.19	pfpip.sina.com - http	http://pfpip.sina.com.cn/ipjs	GET	301	HTTP/1.0 301
	192.168.5.10:51998	221.236.31.144	pfp.sina.com.cn - http	http://pfp.sina.com.cn/cpfp/sinanews_ne...	GET	200	HTTP/1.0 200
	192.168.5.10:51993	221.236.31.144	pfp.sina.com.cn - http	http://pfp.sina.com.cn/pfpnew/resstyle/re...	GET	304	HTTP/1.0 304
	192.168.5.10:52000	221.236.31.160	d3.sina.com.cn - http	http://d3.sina.com.cn/iframe/5/2008/070...	GET	200	HTTP/1.0 200
	192.168.5.10:52028	221.236.31.143	sports.sina.com.cn - http	http://sports.sina.com.cn/iframe/409/200...	GET	200	HTTP/1.0 200
	192.168.5.10:52030	221.236.31.144	pfp.sina.com.cn - http	http://pfp.sina.com.cn/iframe/sports/200...	GET	200	HTTP/1.0 200
	192.168.5.10:52029	221.236.31.144	pfp.sina.com.cn - http	http://pfp.sina.com.cn/iframe/contentpfp...	GET	200	HTTP/1.0 200
192.168.5.10:52025	221.236.31.144	pfp.sina.com.cn - http	http://pfp.sina.com.cn/iframe/sports/200...	GET	200	HTTP/1.0 200	
192.168.5.10:52008	58.63.237.245	pay.sports.sina.com.cn - h...	http://pay.sports.sina.com.cn/livepay/ma...	GET	200	HTTP/1.1 200	

## 4. 技术特性

### 4.1 灵活的系统架构，易于部署

科来网络回溯分析系统采用软硬件一体化设计，易于使用和部署。系统以分析服务器为核心，实时采集、分析、统计及存储网络数据，采用 C/S 技术架构，实时接收和响应分析控制台命令，及时返回数据。分析管理控制中心与分析服务器则采用 B/S 架构，实现定期的数据交互，从而完成全局的集中监控和管理。

### 4.2 高性能的数据采集

系统支持 10M/100M/1000M 网络流量的实时采集和分析，实现千兆骨干链路大流量时的线速分析能力，同时，支持多网卡捕捉，同时汇聚分析多路网络流量。

### 4.3 海量的网络数据存储

系统采用 RAID5/RAID6 存储技术，提供大容量的数据存储系统，可提供从 500GB 或 21TB、42TB 至 63TB 的专用网络回溯分析系统硬件，完整的存储数天、数周甚至数月的网络数据。同时，根据用户的需求，我们提供更大容量存储系统的硬件定制，保障用户对关键链路网络通讯数据的长期存储。

### 4.4 直观的流量趋势导航

网络流量趋势可以直观的反应出网络通讯的正常与否，系统以时间为单位直观的展现该时段的流量趋势，用户可自由的放大或缩小时间窗口，系统提供从 4 分钟、20 分钟、1 小时到 10 天的时间窗口选择，配合时间选择器的使用，

快速过滤隔离异常数据。

## 4.5 基于时间的数据过滤

基于时间的数据过滤技术能够帮助用户快速选择提取特定时间段的通讯数据，系统提供时间选择器、时间窗口以及时间选择控件，用户可灵活方便的选择任意历史时间段。如果有用户抱怨在晚上 21:00 到 21:10，数据库访问中断，此时，网络管理员可定位该时段，将该时段的数据单独隔离分析而不必等待该故障再次出现。

## 4.6 基于网络对象的数据挖掘

系统提供基于网络对象的数据挖掘技术，网络对象包括通讯协议、IP 端点、物理端点、IP 会话、TCP 会话、UDP 会话，用户可通过网络对象进行层次化的逐级数据挖掘，这有助于帮助用户快速挖掘到特定关键数据并解决实际的网络问题。

# 5. 应用价值

## 5.1 网络运行状态，全面掌握

用户的网络规模在不断升级与发展，同时，各种业务应用也在不断的加入到网络当中，一旦某个业务出现问题，轻则导致业务瘫痪，重则带来重大的经济损失。如何全面掌握关键业务、关键网络链路的通讯运行状态，这是企业网络管理面临的新的挑战，同时也会对企业网络管理起到积极的防患作用。

基于用户的应用角度，系统通过分析控制台与分析管理控制中心提供统一、集中的监控平台，用于企业网络的集中监控管理，全面掌握各类关键通讯数据，一旦发现异常，及时处理，防止问题进一步恶化。

## 5.2 网络历史回溯，主动出击

网络故障不可避免，也是网络管理的重中之重，同时，网络的日益复杂，导致网络故障频发，面对各种复杂的网络故障，网络管理员已经疲于应付，对于已经发生的故障，更是一头雾水，只有被动的等待故障再次发生。但是，网络故障稍纵即逝并且发生周期不定，被动的等待也许会徒劳无功。

针对网络故障的特殊性，产品提供快速的故障还原，网络管理员能够精确定位故障发生时间，及时重现网络故障现象，变被动为主动，及时回溯故障点并分析故障发生的原因，避免相同故障的再次发生。

科来网络回溯分析系统以时间为基点，能够帮助用户轻易返回到特定的历史时间，精确的将时间定格到过去的某一周，某一天，某一小时，某一分，某一秒，轻而易举的查看特定历史时间的特定事件。

## 5.3 网络数据存储，轻松实现

网络通讯数据，真实的反应了网络的运行状态，网络中的每一个会话、每一个连接，每一个数据包，每一个时间段的统计数据，都会被详细的记录，因此，对于网络数据的存储，是实现网络回溯的基础。产品支持所有本地或远程网络链路的数据实时采集和存储，从几小时，几天，几周甚至几个月的数据，都能完整的保存。

根据用户的实际网络环境，我们提供不同容量的存储系统，同时，产品采用高性能的磁盘阵列存储技术，支持高达63TB 的数据大小存储并支持存储空间扩展，保障网络数据最大限度的存储到本地系统。

## 5.4 网络故障挖掘，追本溯源

大多数时候，我们需要在网络故障发生之后查找故障原因，追寻网络故障发生的根源，然而，面对海量的网络数据，要想获取关键的有效数据，犹如大海捞针，无迹可寻。产品从数据追踪入手，以时间范围过滤为基础，配合网络对象的数据层级挖掘，能够快速、准确的定位到故障发生时间、地点以及当时的网络操作行为和特征，结合与便携式分析系统的联动，对当时的网络事件进行更细致的诊断、解码，追本溯源，快速发现故障根源。

# 6. 联系我们

### 科来软件 北京营销中心

地址：北京市海淀区彩和坊路8号天创科技大厦407A1

电话：010-82601814

传真：010-82601614

邮编：100080

官方网站：<http://www.colasoft.com.cn>