Colasoft
Maximize Network Value

nChronos

Network Performance Analysis Solution

White Paper

Colasoft reserves the right to make changes in the product design without reservation and without notification to its users.

Contact Us

Sales
sales@colasoft.com

Technical Support
support@colasoft.com

Website
http://www.colasoft.com/

Contents

Preface 1

Introduction 3

Overview 3
Components 3
Architecture 4
Deployment 4

Technical characteristics 5

Retrospective Analysis 5
Application Monitoring 6
Traffic Statistics 7
Intelligent Alarm 7
Intelligent Report Management 7

Application Advantages 8

Security Analysis 8
Fault Diagnosis 8
Network Alarm 8
Decision Basis 8
Responsibility delimitation 9
Application Review 9
Application Monitoring 9
Digital Forensics 9

Preface

Summary

This paper describes the software components, the architecture, the features, the technical characteristics and the advantages of nChronos.

Who should read this paper

This paper is written for:

System Engineers
Technical Support Engineers

Glossary

The commonly used terms in this paper are described in Table 1.
Table 1 Glossary

Term	Description
nChronos Server	The core of nChronos, for capturing, analyzing and storing the traffic data of target network which is also called as network link. Communicates with nChronos Console via the communication port. Also called as *Server*.
nChronos Console	A data presentation platform. Connects to nChronos Server, provides various statistics for users to view and analyze the network traffic status, and provides retrospective analysis, refine analysis and data drilldown. Also called as *Console*.
Analysis object	The network elements, including protocols, addresses, ports, conversations, applications, hosts, network segments, target network, and other elements.
Capture interface	A network interface/port on nChronos Server, generally connected with the mirror port, for capturing the traffic of the target network.
Management interface	A network interface/port on nChronos Server, generally for accessing the Internet such that nChronos Consoles and third-party apps can access the nChronos Server to obtain statistics and analysis data.
Network link	A network object for nChronos to collect captured network traffic and to make statistics and analysis.
Back-in-time analysis	Also called as retrospective analysis. Provides detailed analysis presentation, data drilldown, refine analysis and various statistics for historical network data.

Term	Description
Time Window	A time range with specific span which could be 4 minutes, 20 minutes, 1 hour, 4 hour and other time spans. Smaller time span provides less data volume and finer data granularity. With the Time Window, network data of historical time can be retrieved easily.
Filter	A group of user-defined data screening conditions or rules to accept the required data.
IP pair	A pair of IP addresses, without the identification of source address and destination address.
Drilldown	Level-by-level progressive analysis on selected network objects which include applications, network segments, addresses and conversations.
Expert Analyzer	A packet-level analysis system. Provides lots of statistics about selected network objects and original decoding information of the packets.
Web application	URL-based applications and defined by host name, IP address, port number and URL parameters.
Signature application	Applications defined by the feature codes of original data flow, in ASCII, Hex, UTF-8 or UTF-16.
Performance analysis	The analysis on the service performance of an application.

Introduction

As the network retrospective analysis product from Colasoft, nChronos provides innovative solutions for the management of enterprise-level networks. Colasoft nChronos is a high-performance packets capturing and intelligent analysis platform integrated with high-capacity storage. It can be deployed distributively at the key nodes in the network to realize high-performance and real-time intelligent packet-level analysis of network communication. It provides real-time analysis of the key parameters of various network performance and application performance, captures and stores network communication traffic at the same time. With the capacity of rapid data-mining and retrospective analysis of long-term network communication data, it can detect network anomalies, application performance anomalies and analyze the reasons of them intelligently and retrospectively, enhancing the capacity of guaranteeing the running of key application systems and problem-handling efficiency.

Overview

Colasoft provides nChronos of high performance, aiming at solving complex network management problems and overcoming the disadvantages of portable network analysis products. It can store network data for a long time without interruption and retrieve historical data of a specific time range just by a few clicks, thereby benchmarking network performance and auditing network user activities with forensics.

Colasoft nChronos includes main features as below:

- Monitoring the network status in real-time
- Retrospectively analyzing network traffic based on time
- Drilling down and retrieving network data level by level
- Remotely viewing network statistics across LAN and Internet
- Alerting network anomalies in time with email notifications
- Saving budget and improving efficiency in network management

Components

Colasoft nChronos consists of nChronos Server and nChronos Console.

nChronos Server

Colasoft nChronos Server is the core of nChronos, like a background data center, for capturing, analyzing and storing the traffic data of target network. An nChronos Server contains at least two network adapters, one called as capture interface and the other as management interface. With the capture interface, nChronos Server captures all packets on the target network via the mirror ports on switches or taps, and then delivers the packets to analysis and statistical modules to analyze and store. With the management interface, nChronos Server communicates with nChronos Consoles and third-party applications. One nChronos Server can be accessed by more than one nChronos Console, simultaneously.

nChronos Console

Colasoft nChronos Console is just like a data presentation platform. It accesses nChronos Servers to obtain statistics and other network for presentation and secondary analysis. It provides the up-to-the-second trend charts of the network traffic, the real-time network utilization, the top applications, top hosts and top network segments, and various custom alarms to alert the network anomalies.

Furthermore, nChronos Console can analyze the network data of historical time, drill down a network object level by level, download packets from a Server and decode the packets with Expert Analyzer. One nChronos Console can access multiple nChronos Servers, simultaneously.

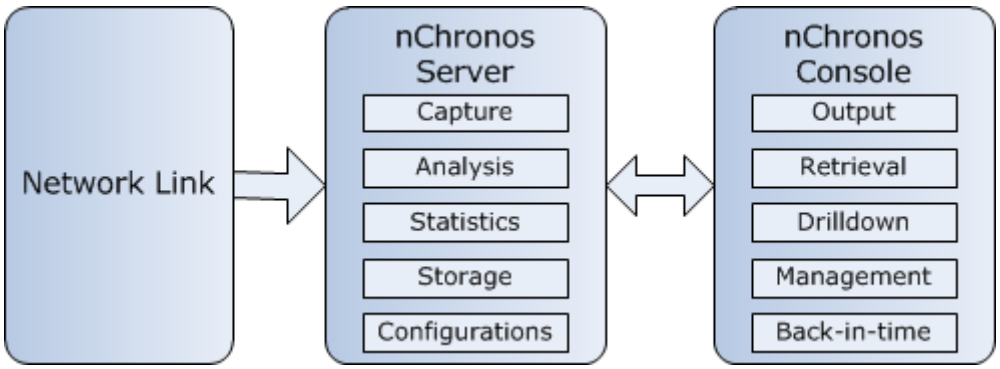
Architecture

Colasoft nChronos Consoles communicate with nChronos Servers using C/S (Client/Server) technology. nChronos Servers respond the commands from nChronos Console in real-time and return relating data. When users need to monitor or analyze the traffic of target network, just connect nChronos Console to the nChronos Server on target network to obtain statistics and other analysis data.

nChronos Consoles and nChronos Servers communicate using TCP/IP protocols over the Internet, nChronos Consoles can connect more than one nChronos Server, and the configurations for an nChronos Server can be done on a webpage browser via a dedicated access port. Therefore, all nChronos Servers can be managed remotely all over the world, and an nChronos Console can access any nChronos Server just with the IP address, access port number, and valid user name and password.

The functional architecture of nChronos Consoles and nChronos Servers is described as Figure 1.

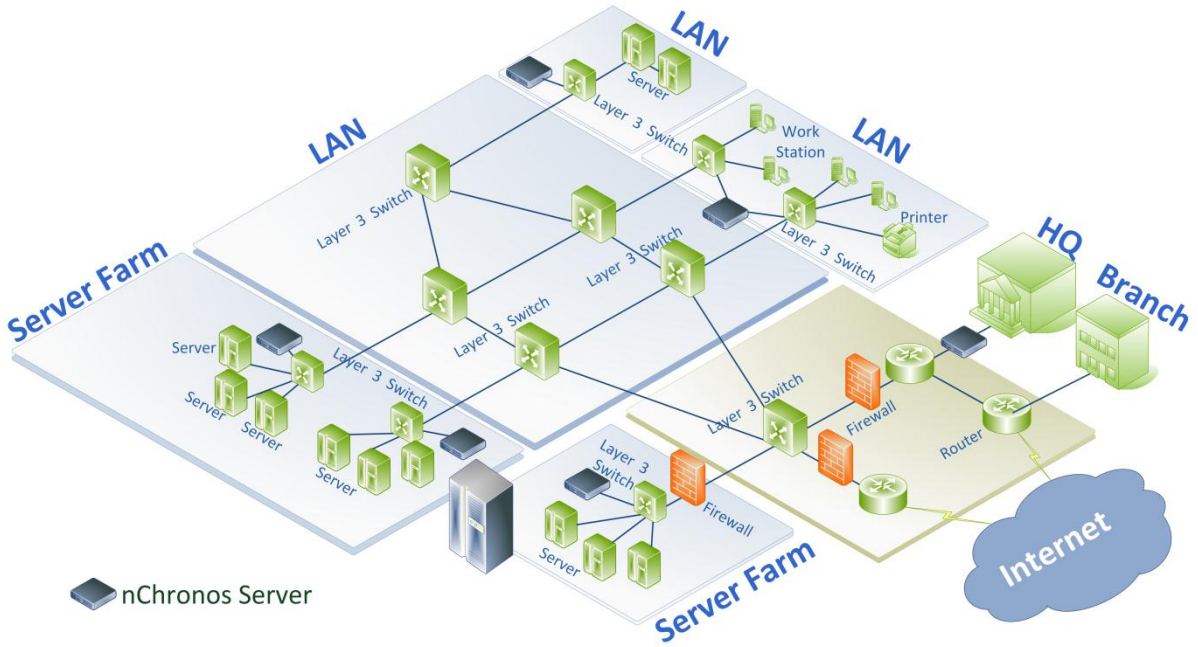
Figure 1 Functional Architecture of nChronos



Deployment

For the networks of different scales and with multiple network links, nChronos can not only capture and store the network data of local networks but support distributive deployment and remote monitoring. For the critical network links, multiple nChronos Servers can be deployed and users can connect to remote nChronos Servers at any place any time for data analysis and network management. Furthermore, using nChronos Consoles, the traffic of critical network links can be monitored in real-time and can be reported once there are anomalies. The deployment of nChronos is visualized as Figure **2**.

Figure 2 nChronos Deployment



Technical characteristics

Colasoft nChronos is capable of processing 10,000 Mbps traffic on a single network adapter, realizing linear speed analysis of the high traffic in bone link. It supports capturing traffic on multiple network adapters at the same time, so as to analyze the aggregated traffic from multiple paths.

Retrospective Analysis

Long-term Data Storage

nChronos is capable of long-term and high capacity data storage, capturing various statistics data such as original packets, data flows, network conversations and application logs in real-time and storing them in a long term and rate-limiting analysis and processing of important network traffic.

Retrospective Forensics Capacity

nChronos is capable of rapid retrospective analysis of large amounts of data stored. If the storage capacity is enough, nChronos is capable of retrospective analysis of network behaviors, application data and host communication data happened in the last 240 days, providing users with tracking and evidence of network problems, and supporting download of related original packets.

Big Data Mining Capacity

nChronos is capable of rapid retrieving and mining large amounts of data in any time period, helping users analyze big data in complicated and large amounts of data through data association, filtering and mining. There are powerful filter conditions in nChronos, which can greatly help users detect problems and get related information, provide more comprehensive analysis method for locating the problem reason rapidly.

7-layer Protocol Decoding

nChronos is capable of analyzing various common network communication protocols in Internet, which helps users master the communication status of every layer of the network.

Intelligent Analysis

With the powerful intelligent analysis module, nChronos is capable of intelligent analysis of network faults in 7 layers, restructuring application data flow and providing graphic views for data flow interaction, which helps users rapidly diagnose network and application faults.

Security Analysis

nChronos is capable of intelligent diagnosis of security events such as worm, DoS attack, ARP attack, TCP port scan, suspicious conversation, etc., rapidly locating the host with problem.

Application Visit Record

nChronos is capable of recording detailed user visit logs of common Internet applications such as DNS, Email, FTP, HTTP, which helps users exactly analyze network behaviors.

Application Monitoring

Exact Customized Application

Users can customize application according to the conditions such as IP address, communication port, IP conversation, communication signature, URL, etc. to realize exact application communication recognition and statistics. nChronos is capable of helping users review application traffic, exactly analyze the traffic changing trend of various application systems, and master the traffic distribution of various application systems.

Powerful Application Monitoring

nChronos is capable of analyzing visit quality of application communication in real-time, including the network transmission quality parameters of application visit and response time indexes of application system, which helps users master the key indexes of application visit quality at any time, and quickly find the key elements effecting the performance of the application.

Application Transaction Processing Analysis

nChronos is capable of monitoring and analyzing the transaction processing time and transaction status, transaction quantity of key applications, realizing real-time analysis of application performance, finding application performance processing anomaly in time and providing scientific evidence for optimizing application system performance.

Traffic Statistics

Comprehensive Traffic Statistics

nChronos provides statistics analysis of communication traffic of network links, hosts, applications, segments, conversations, etc., and graphically displays the changing trend of various key traffic parameters of monitored link at any time, so as to help users master the traffic situation and changing trend of the network.

Abundant Traffic Statistics Parameters

nChronos provides 140+ traffic statistics parameters for different objects such as packets sent, packets received, packets, response time, average packet size and TCP status to meet various traffic analysis requirements.

Support Third-party Data Analysis

All traffic statistics data can be easily exported, and they can be exported according to time period for secondary processing of statistics data.

Intelligent Alarm

Real-time Intelligent Alarm

Users can set alarms according to traffic, application quality index, data flow signature, email content, domain name to realize comprehensive warning of network behavior anomaly.

Support Customized Alarm

nChronos supports combination alarms of multiple traffic parameters. Users can flexibly adjust alarm parameters according to the situation of their network, so as to find abnormal network behavior more exactly.

Alarm Tracing

nChronos is capable of further intelligent analysis of the communication data triggering alarms, providing related data evidence, helping user trace the objects triggering alarms and further master the communication behaviors of abnormal hosts.

Intelligent Report Management

Support Customized Report

nChronos provides 10+ analysis reports of traffic, IP address application distribution, alarm statistics, application quality analysis, etc. by default to help decision-makers comprehensively master historical network communication situation from different respects. Users can customize reports, including specifying report object and setting the fields displayed in various report modules.

Scheduled Report and Auto-sending

nChronos supports generating scheduled reports such as hourly report, daily report, weekly report and monthly report, and automatically sending them to specified email box.

Report Data Comparison

Report supports data comparison. Users can select a time period to make data comparison, which directly displays the historical changing trend of the data.

Application Advantages

Colasoft nChronos is a high-performance platform integrated 7-layer network protocol analysis technology, high capacity of data storage, intelligent data-mining technology and distributive data processing technology. It provides users irreplaceable values comparing with other network security products.

Security Analysis

nChronos can deeply detect network communication through packet-level network behavior analysis, rapidly find the abnormal behaviors threatening network safety such as network attack, worm, Trojan, etc.

Fault Diagnosis

nChronos is capable of exactly locating the fault point and deeply analyzing the root of the fault through rapid retrieval and intelligent analysis of the communication data when the fault happened.

Network Alarm

nChronos is capable of detecting various anomalies timely and sending alarms through real-time intelligent network communication analysis, preventing potential network problem from becoming emergent event to cause unnecessary loss.

Decision Basis

nChronos is capable of providing analysis data of network behavior rules and running trend, providing scientific evidence for performance improvement, new application deployment, bandwidth planning, security strategy, etc.

Responsibility delimitation

nChronos is capable of exactly analyzing the root reasons of application anomalies, providing evidence for delimitating the responsibility and responsible person, enhancing the cooperation efficiency among operation and maintenance departments.

Application Review

nChronos is capable of sorting and analyzing network communication by application type, helping network managers effectively master application communication status, providing management strategy basis.

Application Monitoring

nChronos is capable of monitoring and analyzing application communication traffic, network transmission quality, application performance in real-time, finding abnormal running status in time, guaranteeing high network service quality for key applications.

Digital Forensics

nChronos is capable of rapid and exact location of the fault point, finding the evidence of network crime, completing the authentication and forensics work of security event, helping users make better security strategy.