

SYNAPSE: NETWORKS

Synapse:Networks GmbH – Theaterplatz 1 – 53177 Bonn – 0228-93458-0/99 fon/fax – www.synapse.de

Stand: Januar 2003



Synapse:Networks sind seit über 10 Jahren am Markt tätig und auf LAN-Analyse spezialisiert. Das LAN-Analyse Experten-System „TraceMagic“ sowie das Windows-Registry Experten-System „RegCheck“ wurden von Synapse:Networks entwickelt. Auch stammt die einschlägige Fach-Literatur von Synapse-Gründer Frank R. Walther: „Networker's Guide“ (2000,2003) und „Registry Guide“ (2001).

Netzwerk-Messungen / LAN-WAN-Analyse

VORBEREITUNGEN	2
EINRICHTUNG DER MESSPUNKTE.....	2
AUSWAHL DER MESSPUNKTE.....	2
BEGRIFFE / FESTSETZUNGEN.....	5
ABLAUF DER MESSUNG	6
ZAHL DER MESSRECHNER.....	6
ZIEL DER AUFZEICHNUNGEN.....	6
WAHL UND WECHSEL DER MESSPUNKTE.....	6
AUSWERTUNG DER AUFZEICHNUNGEN	7
VORGEHENSWEISE / TRACEMAGIC.....	7
ECKPUNKTE DER ANALYSE.....	7
BERICHT / DOKUMENTATION	12
KURZ-BERICHT (VORAB-BERICHT).....	12
ABSCHLUSS-BERICHT.....	12
BERICHT: CD-ROM / EMPFÄNGER / FREISTELLUNG VON RECHTSFOLGEN.....	12
BERICHT: TECHNISCHE DOKUMENTATION.....	12
BERICHT: BEWERTUNG / EMPFEHLUNGEN.....	13
NACHFRAGEN / NACHSORGE.....	13
ARCHIVIERUNG: ERGEBNIS-DATEN / MESS-DATEN / DATENSCHUTZ.....	13
ANALYSE-PREISE	14

Die folgenden Darlegungen stellen einerseits eine allgemeine Einführung in die Vertrags-Gestaltung dar sowie in den Ablauf der Arbeiten, stellen aber andererseits auch die Vertrags-Grundlagen dar und werden vom Kunden bei Auftragserteilung anerkannt.

Vorbereitungen

Einrichtung der MessPunkte

Der Kunde stellt die MessPunkte zur Verfügung.

Im Wesentlichen handelt es sich hierbei um das Einrichten von Mirror Ports an den Switches und Routern.

Ersatzweise können Fast-Ethernet-Hubs (100 Mbps Repeater) verwendet werden, wo Mirror Ports nicht zu schalten sind. Dann jedoch muss darauf geachtet werden, dass ggf. Server-Anbindungen von Full-Duplex-Ethernet auf Half-Duplex-Ethernet zurück zu stellen sind, was im Tagesbetrieb nicht möglich ist und daher am Abend zuvor eingerichtet werden muss.

Die aktuellen Beschreibungen zu diesem Thema sind zu finden unter:

http://www.synapse.de/2003/htm/ger/analysis_services_terms_of_trade.htm

Auswahl der MessPunkte

A. "Messpunkte = Config- und Domain-Server"

Es wird grundsätzlich angestrebt, früh morgens das LOGIN bzw. die Netzwerk-Anmeldung der Clients mitzulesen.

Hierzu sollte der LAN-Verkehr der folgenden Server (sofern vorhanden) mitgelesen werden:

- BOOT / DHCP Server
- WINS Server
- DNS Server
- Windows PDC / BDC Server
- NetWare NDS Server
- ggf. weitere, bei LOGIN beteiligte Server.

Da das LOGIN erfahrungsgemäß wenig Datenverkehr umfasst, können insbesondere die Name Server / Config Server (DHCP, DNS, WINS) über den selben Messpunkt abgegriffen werden, sofern dies anlagentechnisch möglich ist, etwa: über den selben Fast-Ethernet-Hub (sofern mit Half-Duplex Fast-Ethernet angebunden), oder über das Spiegeln mehrerer Server-Ports auf einen gemeinsamen Switch-Mirror-Port.

Es können auch mehrere Server auf einen gemeinsamen Fast-Ethernet-Hub (half-duplex Repeater) gelegt werden, sofern die zu erwartenden Datenraten dies zulassen.

B. "Messpunkte = Datenserver"

Den Applikationen entsprechen in aller Regel bestimmte Applikations-Server bzw. Daten-Server.

Je nach Aussagen der Anwender, bei welchen Anwendungen Probleme auftreten, sollte auch der LAN-Verkehr dieser Daten-Server mitgelesen werden.

Auch hier sind die Mirror-Ports an den Switches entsprechend zu schalten.

Es können auch mehrere Server auf einen gemeinsamen Fast-Ethernet-Hub (half-duplex Repeater) gelegt werden, sofern die zu erwartenden Datenraten dies zulassen.

C. "Messpunkte = Client-Workgroups"

Das Geschehen lässt sich nur verstehen, wenn es auch aus der Sicht der Client-PCs nachvollzogen wird.

Daher sollten zwei, drei Client-Workgroups (möglichst repräsentativ) gemessen werden.

Ideal ist es, den Uplink des jeweiligen Workgroup-Switches zum Core-Switch auf den Mirror-Port auszuspiegeln, da somit der gesamte LAN-Verkehr der Client-Workgroup aufgezeichnet werden kann.

Es können auch mehrere Clients auf einen gemeinsamen Fast-Ethernet-Hub (half-duplex Repeater) gelegt werden, da die Datenraten der Clients dem i.d.R. nicht entgegen stehen.

D. "Messpunkte / Mirror Ports: Frage der Bitraten"

-1-

"Rx/Tx"

Die einfachste und schnellste Vorgehensweise ist die Messung über Mirror-Ports.

Hierzu müssen die für Messung in Frage kommenden Verkehrspunkte (Router, Switches) in der Lage sein, aktive Ports auf Mirror-Ports auszuspiegeln.

Es ist **ungenügend**, wenn der Switch *nur Rx* oder *nur Tx* ausspiegeln kann.

Wichtig ist, dass der Mirror-Port sowohl *Rx wie auch Tx* gemeinsam ausgibt.

-2-

"Port Mirroring / Group Mirroring"

Einige Switch-Typen können nicht nur einzelne Ports auf den Mirror-Port spiegeln, sondern Port-Gruppen (also mehrere Ports auf Mirror-Port).

Dies ist für die Praxis oft hilfreich, da es die Messung beschleunigen und Zusammenhänge besser sichtbar machen kann.

Es ist nicht unbedingt erforderlich, dass die Switches über diese Fähigkeit verfügen, aber nützlich.

-3-

"Line Speed / Bitrate"

Es stehen maximal zur Verfügung:

1 x Gigabit Ethernet Analyzer
4 x Fast Ethernet Analyzer

Es kann im Gigabit-Bereich also wie folgt vorgegangen werden:

Entweder gibt es jeweils nur 1 Messpunkt im Gigabit-Bereich,

oder (a)

es werden Gigabit-Ports auf 100-Mbps-Mirror-Ports gespiegelt, was bei geringem Datendurchsatz ohne große Bedenken durchgeführt werden kann,

oder (b)

es müssen ggf. mehr Messpunkte an die Peripherie gelegt werden, wo wieder 100-Mbps bzw. Fast Ethernet vorliegt,

oder (c)

es werden am jeweiligen Gigabit-Switch mehrere Server-Ports auf den Mirror-Port gespiegelt; dies ist z.B. bei Cisco-6000er-Switches problemlos möglich.

E. "Zeitlicher Ablauf"

-1-

Die Messung morgens hängt hinsichtlich des Beginns wesentlich davon ab, wenn das LOGIN der Client-PCs erfolgt.

Zwei Stunden vor allgemeinem Arbeitsantritt sollte die Einrichtung der Messpunkte begonnen werden, um rechtzeitig fertig zu sein.

-2-

Um am Abend des ersten Tages die ersten Ergebnisse vorlegen zu können, und um die Entscheidung zu einer etwaigen Verlängerung in den nächsten Tag hinein möglichst qualifiziert treffen zu können,

ist immer wieder Zeit bis in den Abend notwendig, um die nötigen Auswertungen betreiben zu können.

Es ist daher wichtig, dass die zuständigen Mitarbeiter und Entscheider auf der Seite des Kunden auch am Abend anwesend sind (sofern die Entscheidung über einen Folgetag noch nicht getroffen wurde.)

F. "Personal / Begleitung"

Seitens des Kunden muss für die gesamte der Dauer der Messung ein Mitarbeiter abgestellt werden,

- um Synapse:Networks Zugang zu den LAN-technischen Anlagen zu verschaffen,
- um an den Switches und Routern die Mirror-Ports zu schalten,
- um Dokumentations-Anfragen zu beantworten bzw. um Dokumentation auf Bedarf zu beschaffen.

Sollte diese Begleitung nicht immer über die ganze Zeit möglich sein (was nahe liegt), so sollte die Begleit-Person über Mobil-Funk jederzeit erreichbar sein.

G. "Network Management / Port Statistics"

Es kann sehr hilfreich, ggf. nötig sein, von Switches und Routern die Statistiken und Geräte-Einstellungen abzufragen und zu dokumentieren.

Dies kann geschehen über TELNET oder HTTP, je nach Möglichkeiten am gegebenen Switch oder Router.

Es ist durch den Kunden sicher zu stellen, dass zum Zeitpunkt der Messung ein zur Abfrage der Statistiken und Einstellungen berechtigter Administrator anwesend ist. Dies gilt auch dann, wenn ein Switch oder Router nicht in der Hoheit des Kunden steht, sondern etwa unter der Hoheit eines externen Providers.

H. "Windows Registry"

Es kann zum Verständnis des Kommunikationsverhaltens wichtig bzw. zwingend sein, die System-Einstellungen von Windows-Rechnern nachzuvollziehen.

Hierzu ist jeweils die Windows-Registry über "REGEDIT" zu exportieren im Text-Format von REGEDIT-4.

Es ist hilfreich, wenn von den wichtigsten Windows-Servern und einigen repräsentativen Windows-Clients die Registry-Daten auf diese Weise zur Verfügung gestellt und Synapse:Networks ausgehändigt werden.

Begriffe / Festsetzungen

Im Falle eines Vertrages, der eine LAN-Analyse zum Gegenstand hat, gilt:

- Unter "**Messung**" im Sinne dieses Vertrages ist zu verstehen: Das Einlesen von Kommunikations-Daten an den Anlagen des lokalen Netzes (LAN) des Kunden mittels geeigneter Messgeräte; aufgezeichnet werden sog. LAN Frames. Die einzige technische Berührung von Synapse mit den Kommunikations-Anlagen des Kunden ist das Verbinden des Messgeräts mit dem vom Kunden eingerichteten und zur Verfügung gestellten Messpunkt mittels Datenkabel (etwa: Cat-5, IBM-Typ-1) und der Betrieb des solcher Art angeschlossenen Messgeräts. Synapse legt nicht selber Hand an die Anlagen des Kunden (nimmt z.B. keine Konfigurations-Arbeiten an den Anlagen vor). Etwaige Abfragen von Statistiken in Switches/Routern (etwa: Port-Statistiken) oder File-Servern (etwa: Registry-Exports) etc. werden auf Bitte bzw. Anregung seitens Synapse allein vom Kunden vorgenommen oder einem vom Kunden beauftragten Dritten.
- Unter "**Messgerät**" im Sinne dieses Vertrages ist zu verstehen: Üblicherweise sog. Protokoll-Analysatoren (LANdecoder32 / Triticom; Observer / Network Instruments; Surveyor / Shomiti; EtherPeek / Wildpackets).

Bei Messungen durch Synapse vor Ort gilt:

- Die Messung erfolgt jeweils an einem vom Kunden zur Verfügung gestellten und eingerichteten Messpunkt, das Messgerät wird im Regelfall von Synapse gestellt bzw. mitgebracht.
- Unter "**Messpunkt**" im Sinne dieses Vertrages ist zu verstehen: Ein Daten-Übergabe-Punkt, an dem Kommunikationsdaten des Daten-Netzes des Kunden zum angeschlossenen Messgerät hin zum Zwecke der Aufzeichnung und Auswertung ausgegeben werden. Messpunkte sind meistens in Form sog. Verteiler gegeben (Hubs, Repeater, Switches, Router) und können wie folgt beschaffen sein:
 1. Mirror-Ports, bei denen der Daten-Verkehr eines Verteilers auf die Anschlußbuchse des Analyzers in Kopie ausgegeben wird.
 2. Ethernet-Repeater (10/100 Mbps) oder Token-Ring Ringleitungsverteiler (4/16 Mbps) im Halb-Duplex-Modus, die den gewünschten Datenverkehr bedingt durch ihre Bauweise auf allen Buchsen ausgeben.
 3. Im Einzelfall (und nur nach Absprache) sog. Media-TAPs oder Media-Splitter, die eine Voll-Duplex-Leitung in Rx/Tx-Buchsen zwecks Datenausgabe auftrennt. Da hier erheblicher Zusatzaufwand nötig ist, um die so gewonnenen Messdaten auswerten zu können (was zudem nur mit starken Einschränkungen möglich ist), oder wegen des Erfordernisses zusätzlicher Hardware-Module, bedarf es der Absprache im Einzelfall.
 4. Der Zugriff auf RMON-Agenten via SNMP. Da diese Methode weniger zuverlässig ist und vor allem im Zeit- und Mengen-Verhältnis beschränkt ist, sollte sie nur nach Absprache bzw. ersatzweise bei Fehlen besser geeigneter Messpunkte angewendet werden.
- Bei Zusendung von Messdaten auf CD-ROM hat der Kunde für jede einzelne Messung den genauen Messpunkt gegenüber Synapse:Networks zu dokumentieren, da sonst die Auswertung eingeschränkt oder sogar unmöglich sein kann.

- Unter **"Messdaten"** im Sinne dieses Vertrags ist zu verstehen: Insofern Inhalte des Datenverkehrs am Messpunkt gespeichert werden, handelt es sich um "Messdaten". Diese können vorliegen in Form von Binär-Daten (Traces) oder Statistiken (z.B. CSV-Dateien).
- Unter **"Auswertung"** im Sinne dieses Vertrages ist zu verstehen: Die Durchsicht der Messdaten, das gezielte Suchen nach Auffälligkeiten / Fehlern, das Protokollieren der Ergebnisse in Form von Messberichten. Die Auswertung kann je nach Anlaß und Gegenstand voll- oder teil-automatisch bzw. voll- oder teil-manuell erfolgen, wobei es Synapse überlassen bleibt, die Vorgehensweise zu bestimmen.
- Unter **"Messbericht"** im Sinne dieses Vertrages ist zu verstehen: Die vorgelegten Auswertungen, ggf. mit weiteren Stellungnahmen / Zusammenfassungen.

Ablauf der Messung

Zahl der MessRechner

Es stehen zur Verfügung:

- 1 x Gigabit Ethernet LAN-MessRechner
- 4 x Fast Ethernet LAN-MessRechner

Je nach Größe des Netzwerkes und je nach Auftrag werden 2-5 MessRechner eingesetzt, um den Datenverkehr aufzuzeichnen.

Ziel der Aufzeichnungen

Ziel ist es, einen möglichst umfassenden und aussagekräftigen Querschnitt des Datenverkehrs aufzuzeichnen.

An den wichtigsten MessPunkten wird möglicherweise über einen ganzen Tag hinweg (12-24 Stunden) der Datenverkehr aufgezeichnet.

Hierzu werden leistungsfähige Systeme eingesetzt, um möglichst verlustfrei auch bei hohen Verkehrsspitzen eine zuverlässige Aufzeichnung zu erreichen.

Am Ende soll ein möglichst repräsentatives Bild des Datenverkehrs in den MessRechnern gespeichert sein.

Wahl und Wechsel der MessPunkte

In den meisten Fällen wird früh morgens mit der Messung begonnen, um die Boot- und Login-Phase mitlesen zu können, und zwar sowohl an der Server-Seite (DHCP, WINS, DNS, PDC, etc.), im Backbone (Core Switch), an der Client-Seite (Workgroup Switch).

Im Laufe des Tages werden dann zusätzlich verschiedene Client-Workgroups und Daten-Server in den Blick genommen.

Hierzu ist unbedingt erforderlich, dass die entsprechenden MessPunkte zuvor eingerichtet wurden, oder dass die Schaltung der nötigen Mirror Ports kurzfristig möglich ist.

Auswertung der Aufzeichnungen

Vorgehensweise / TraceMagic

Synapse:Networks arbeitet mit einem weltweit einmaligen Experten-System zur Auswertung der MessDaten (Aufzeichnungs-Dateien, Trace Files): TraceMagic.

<http://www.tracemagic.net/>

Die hierüber erzielbaren Ergebnisse sind der herkömmlichen Methodik marktüblicher LAN-Analyse weit überlegen.

Eckpunkte der Analyse

Ein paar der wesentlichen Highlights der TraceMagic-Analyse sind:

- Es können mehrere Gigabytes an Messdaten völlig automatisch ausgewertet werden. Damit können Messzeiträume von Stunden, wenn nicht Tagen, völlig automatisch analysiert werden. Diese Art von **Analysis Engine** ist weltweit zur Zeit ohne Konkurrenz.

TraceMagic verarbeitet die Capture-Files, die herkömmliche LAN-Analyser auf die Festplatte gebracht haben.

[TraceMagic liefert selbst über Gigabyte-Mengen den Total-Befund, voll-automatisch.](#)

- Alle LAN-Pakete, die zu Ereignis-Abläufen oder Fehlern im Sinne der Analyse gehören, werden aus den Original-Messdaten heraus gezogen und in neu erzeugte Trace-Dateien hinein kopiert. Auf diese Weise entsteht ein Subtrat, das genau die Ereignisse und Fehler abbildet, die gesucht werden. Ausführliche **Event-Logs** unterstützen das durch lesbare Text-Dateien.
- Die Analyse kann eingeschränkt bzw. gesteuert werden über die **Filter Engine** von TraceMagic. Über 500 Filter-Kriterien können maximal über die Filter-Datenbank aktiviert und kombiniert werden.

- TraceMagic verfügt über ein hoch leistungsfähige **Report Engine**. Denn Analyse geschieht zu dem Zweck, am Ende unanfechtbare, vollständige und revisionsfähige Ergebnisse zu haben.

Über ein breites Spektrum von Ereignissen und Fehlern werden automatisch Berichte erzeugt.

.TXT - lesbare Text-Dateien.

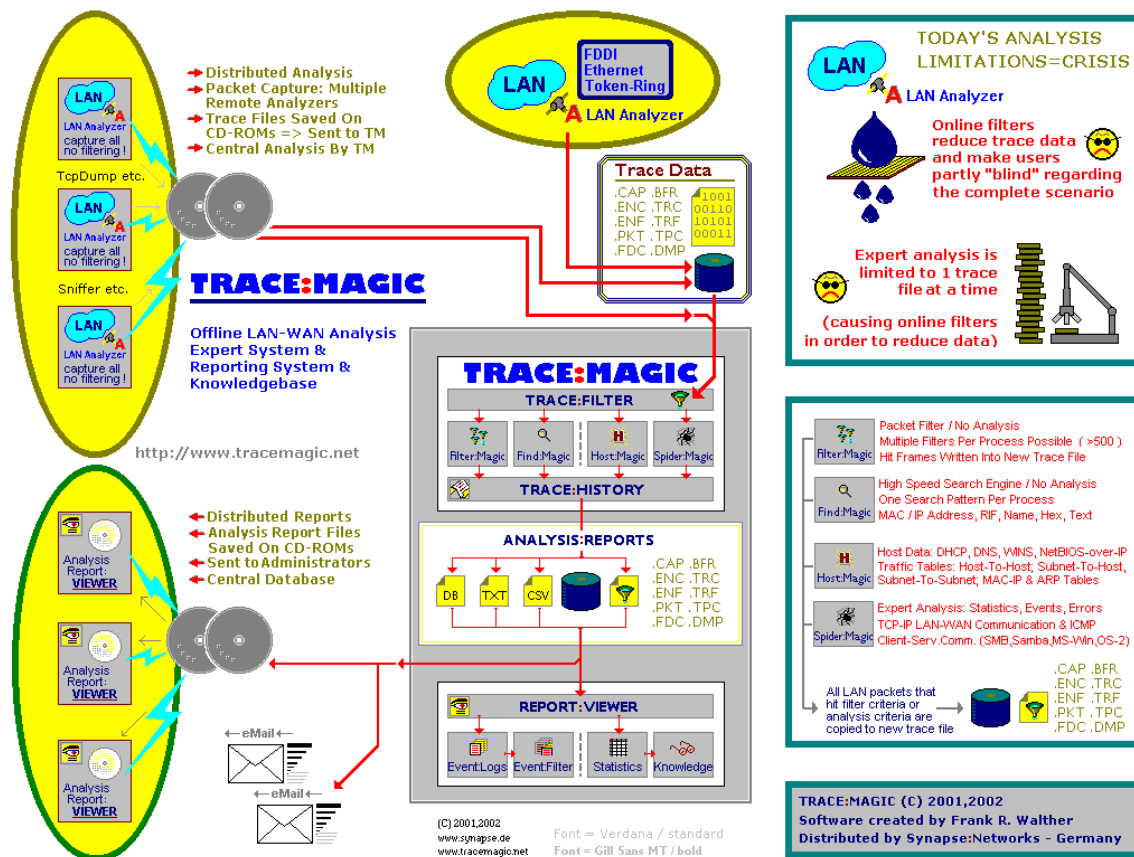
.CSV - Tabellen (gedacht für Excel)

.DB - Datenbanken mit komplexen Ergebnis-Darstellungen

- Die Report-Ergebnisse, insbesondere die Report-Datenbanken, können über ein **lizenz-freies REPORT-VIEWER-Modul** durch beliebige Dritte betrachtet und weiter verarbeitet werden.

Dies schafft eine **universelle Schnittstelle für die Berichts-Auswertung und -Weitergabe**, zumal jeder Empfänger der Ergebnis-Daten auf die Knowledgebase (Wissens-Datenbank) zugreifen kann.

- Das **Datenfluss-Modell von TraceMagic** ist daher ebenso einfach wie effizient und universell (volle Größe der Grafik: siehe unten, am Fuß des Dokuments):



- Wirkung: **Arbeitszeit wird gespart**, und **Reaktionszeiten werden verkürzt**.

An zentraler Stelle werden die Messdaten des ganzen Unternehmens ausgewertet (keine oder kaum Handarbeit mehr!) - und die Ergebnis-Reports (Text, CSV, Datenbanken) werden verteilt an alle, die es betrifft.

- TraceMagic verfügt über eine **Knowledgebase**, die sowohl im Analyse-Modul wie auch im Viewer-Modul arbeitet.

Auf diese Weise wird der Analyse-Techniker unterstützt, desgleichen aber auch sämtliche Empfänger der Ergebnis-Reports.

- TraceMagic erkennt Fehler auf folgenden OSI-Schichten bzw. in folgenden Protokoll-Stapeln:

OSI Layer 1-2:

Fehler in der Physik, insbesondere versteckte Switch-Fehler.

Beispiel (in 2002 mehrfach festgestellt): Das automatische Vervielfältigen von LAN-Paketen durch Switch-Ports wird von TraceMagic vollständig erkannt (von herkömmlichen LAN-Analysern nicht).

OSI Layer 2 + SNA:

Die LLC-Dialog-Kontrolle samt einem darüber laufenden SNA-Protokoll werden umfangreich und automatisch analysiert. Für Banken und Versicherungen heute noch interessant.

OSI Layer 3 (Network):

IP-Routing-Fehler insbesondere auf WAN-Strecken werden selbst dann erkannt, wenn es sich um höchst versteckte Ereignisse handelt, die von anderen Analyzern nicht erkannt werden. Der Nachweis mangelhaft arbeitender Provider-Strecken gelingt mittels TraceMagic (fast) nahtlos.

OSI Layer 4 (Transport):

Fehler in der Datenfluss-Kontrolle, im Dialog-Verhalten, im Sitzungs-Verhalten werden vollständig erkannt und in vielfacher Form ausgegeben (Text, CSV, Datenbank).

OSI Layer 5-7 (Name Services):

Mit hohem Anteil an Netzwerk-Fehlern sind die Microsoft Name-Services beteiligt (NetBIOS, WINS, DNS). TraceMagic ist die einzige Software, die hier gründlich aufräumt und die bislang versteckt ablaufenden Fehler sichtbar macht.

OSI Layer 7 (File Services, Application):

File Services:

Unterstützt werden die drei großen Client-Server-Protokolle:

- SMB (Windows, OS-2, Samba) (über LLC, NetBIOS, TCP/IP, Vines IP)
- NCP (Novell NetWare) (über IPX oder TCP/IP)
- HTTP (WWW, Internet)

Bislang war kaum bekannt, dass das Basis-Geschäft des lokalen Netzwerkes, die Datei-Dienste, ebenfalls bizarre Fehler aufweisen können, die bis zu Endlos-Schleifen und Programm-Abstürzen führen können. TraceMagic deckt diese Fehler auf und macht sie eingehender Untersuchung zugänglich.

File Reconstruction:

Neben der Analyse der Datei-Dienste ist TraceMagic in der Lage, den Inhalt der Dateien dokumentarisch zu rekonstruieren, die seitens der Clients auf den Servern gelesen werden. Dies ermöglicht Fehler-Erkennungen, die bislang nicht bekannt waren.

Script Follow-Up:

TraceMagic kann erkennen, ob der fehl geschlagene Zugriff eines Clients auf eine Server-Resource auf eine zuvor geladene Script-Datei zurück zu führen ist (.BAT, .CMD, etc.). Diese Fähigkeit ist weltweit bislang einmalig.

ORACLE:

Eine Spezial-Funktion für die Oracle-Analyse erlaubt es, spezielle Fehler, die im Zusammenhang mit TCP/IP-Ereignissen auftreten, nahtlos zu erkennen.

- TraceMagic verfügt vermutlich über **die ausgedehnteste TCP/IP-Analyse weltweit**, verglichen mit herkömmlichen LAN-Analysern. Über 200 Ereignis- und Fehler-Zähler werden je IP-Teilnehmer geführt und in den Berichten ausgegeben (Text, CSV, Datenbank) !

So wurden bereits im Dezember 2001 in einem der größten WANs Deutschland **die TCP/IP-Fehler von genau 22.661 IP-Teilnehmern automatisch erfasst und in Berichtsform ausgegeben!**

Diese Leistungskraft ist bisher völlig unerreicht und einmalig.

<http://www.synapse.de/tracemagic/tm.power.htm>

- TraceMagic verfügt als einziger Analyzer über **ausgedehnte Fähigkeiten, auf Layer 7 Applikations-Ereignisse und -Fehler zu erkennen**, auch in schwierigen Wechselwirkungen.

Die für MS-Windows typischen Fehler in den File Services, die kaum jemandem bislang bekannt waren (da sie von traditionellen Analyzern nur ungenügend sichtbar gemacht werden), werden weitgehend, wenn nicht gar vollständig aufgedeckt.

- Script Follow-Up: TraceMagic ist inzwischen in der Lage, Client-Zugriffe, die von Servern abgelehnt oder nicht bedient werden, auf zuvor geladene Script-Dateien zurück zu führen (etwa: .BAT, .CMD, .REG, Login Scripts).

- **TraceMagic automatisiert den Prozess der LAN-Analyse (fast) vollkommen.**

Sämtliche LAN-Pakete, die mit einem handelsüblichen Analyzer aufgenommen wurden (Sniffer, Observer, LANdecoder32, Ethereal, etc.) und in so genannten "Trace-Dateien" abgespeichert wurden, **werden vollkommen automatisch ausgewertet (mit Hinterlegung der Ergebnisse in abrufbaren Datenbanken).**

- Kunden aus Industrie und Regierung verlassen sich heute auf LAN-Analyse mit TraceMagic (Auswahl):
 - Bundesverteidigungsministerium (BMVg)
 - Krauss-Maffei-Wegmann (Rüstung)
 - T-Systems
 - Bayerischer Rundfunk
 - RBT - Rundfunk-Betriebs-Technik der öffentl.-rechtl. Sendeanstalten
 - Bosch-Rexrodt
 - Viessmann AG
 - Schering AG
 - ERGO-Versicherungen
 - Bayerische Sparkassen / IZB
 - Universitätsklinikum Düsseldorf
 - Fachhochschule Merseburg
 - ... und andere mehr

- Der erste veröffentlichte **Anwender-Bericht mit Erfahrungen zu TraceMagic** erschien in Oktober 2002 in der Zeitschrift "Network World" (Heft 19-2000):

"Netzwerk-Management und LAN-Analyse beim Bayerischen Rundfunk"

Network World (Germany), Heft 19-2002, 11. Okt. 2002

Artikel:

<http://www.networkworld.de/index.cfm?pageid=104&id=89291&type=detail>

Interview:

<http://www.networkworld.de/index.cfm?pageid=104&id=89259&type=detail>

Oder:

http://www.synapse.de/tracemagic/ger/htm/tracemagic_press_releases.htm

Zitat von Herrn Rennollet, dem Sachgebietsleiter beim Bayerischen Rundfunk:

"Dieses Expertensystem erleichtert unsere Arbeit erheblich. Es verkürzt den Zeitaufwand für die Fehlersuche und lässt sich sehr schnell produktiv einsetzen. Auch für nicht speziell geschulte Netzwerk-Administratoren ist es möglich, mit TraceMagic rasch gute Ergebnisse zu erzielen."

Bericht / Dokumentation

Kurz-Bericht (Vorab-Bericht)

Noch am Abend der Messung erhält der Kunde einen Kurz-Bericht. Dieser ist erfahrungsgemäß inhaltlich zu 60-80% identisch mit dem späteren Abschluss-Bericht.

Der Kurz-Bericht basiert auf den automatischen Auswertung des Experten-Systems „TraceMagic“ und wurde in den wesentlichen Punkten vor der Übergabe durch manuelle Durchsicht verifiziert.

Um dem Kunden derart schnell und punktgenau Befunde noch am Tage der Messung aushändigen zu können, ist es notwendig, dass bis in die Abendstunden hinein Personal des Kunden verfügbar bleibt.

Die Übergabe des Kurz-Berichts findet allgemein zwischen 16:00 und 22:00 Uhr statt.

Abschluss-Bericht

Der Abschluss-Bericht erfolgt gegenüber dem Kunden durchschnittlich 10-15 Kalendertage nach der Messung.

Die Bearbeitungsdauer hängt von der Menge der Messdaten ab sowie von Art und Umfang der darin festgestellten Ereignissen bzw. Fehler.

Ziehen sich die Arbeiten länger als 14 Kalendertage hin, wird der Kunde benachrichtigt und vorab mit den bislang gesicherten Teil-Ergebnissen versorgt, um Handlungsfähigkeit sicher zu stellen.

Bericht: CD-ROM / Empfänger / Freistellung von Rechtsfolgen

Die Übergabe des Abschluss-Berichts erfolgt per CD-ROM an die vom Kunden genannte Adresse.

Ist eine dritte Partei beteiligt (etwa: ein vom Kunden beauftragter Dienstleister), so muss der Kunde gegenüber Synapse:Networks GmbH schriftlich erklären, an welchen Empfänger die Berichts-CD-ROM gesendet werden soll, und dass der Empfänger befugt ist, die Inhalte einzusehen und zu verwenden. Im Ergebnis muss Synapse:Networks von allen Rechtsfolgen frei gestellt werden für den Fall, dass sich der vom Kunden angegebene Empfänger (z.B. aus datenschutzrechtlichen Gründen) doch nicht befugt war, die Daten zu empfangen, einzusehen und/oder zu verwenden.

Bericht: Technische Dokumentation

Die Dokumentation der Befunde im Sinne von Statistiken, Tabellen und Einzel-Nachweisen erfolgt in den folgenden Formaten:

.CSV	Statistiken im Tabellen-Format zur Weiterverarbeitung (etwa durch MS-Excel)
.TXT	Ausführliche Einzel-Nachweise und Event-Logs
.HTML	HTML-Projekt mit Einbindung (fast) aller Ergebnisse
.DB	Datenbank, für den Kunden frei verwendbar

Im Wesentlichen werden die Ergebnisse als in sich geschlossenes und indiziertes HTML-Projekt übergeben.

Im Einzelfall kann dieses HTML-Projekt mehrere Hundert Seiten umfassen.

Bericht: Bewertung / Empfehlungen

Es wird eine Übersicht und Zusammenfassung erstellt, in der auch Bewertungen und Empfehlungen abgegeben werden.

Für den Kunden stellt dies eine To-Do-Liste dar, die übersichtlich darstellt, was zu tun ist, und in welcher Reihenfolge vorgegangen werden sollte.

Die über TraceMagic erstellten Reports werden in vollem Umfang seitens Synapse:Networks durchgesehen, nachvollzogen und verifiziert. Dies ist im klassischen Sinne „Handarbeit“ und verlangt nicht unerheblichen Arbeitseinsatz. Insbesondere Fehler auf dem Application Layer werden auf diese Weise gründlich bearbeitet.

Nachfragen / Nachsorge

Synapse:Networks steht auch nach Abgabe bzw. Vorstellung des Berichts für Fragen zur Verfügung, um die möglichst effiziente Umsetzung der Befunde zu unterstützen.

Da Synapse:Networks den diagnostischen Teil einer Netzwerk-Entstörung liefert, der therapeutische Teil aber durch Dritte geleistet werden muss, diese Leistung durch Dritte aber vom Verständnis der Diagnose abhängt, begleitet Synapse:Networks die späteren Arbeiten im Sinne von Erläuterungen, Klärung von Detail-Fragen und dergleichen mehr.

Archivierung: Ergebnis-Daten / Mess-Daten / Datenschutz

Sofern nichts anderes vereinbart wurde, übergibt Synapse:Networks den Bericht samt dem dokumentarischen Werk an den Kunden, nicht aber die eigentlichen MessDaten, da dies bei den heutigen Mengen (schnell bis zu 50 GigaBytes pro Tag) wenig Sinn ergibt.

Da dem Auftraggeber jedoch die Daten als Eigentümer zustehen, kann gegen Aufpreis eine Kopie auf CD-ROM oder DVD erzeugt und dem Kunden ausgehändigt werden.

Die aufgezeichneten Daten werden im Hause von Synapse:Networks archiviert, unter Verschluss gehalten und Dritten nicht zugänglich gemacht.

Diese Archivierung ist notwendig, um Zweifelsfälle und Nachfragen anhand der originalen Daten nachvollziehen bzw. klären zu können; dies gilt zum Schutze des Kunden, aber auch zum Schutze von Synapse:Networks, insofern die Aussagen, die Synapse:Networks in seinen Berichten vornimmt, Anlass auch juristischer Auseinandersetzungen werden können.

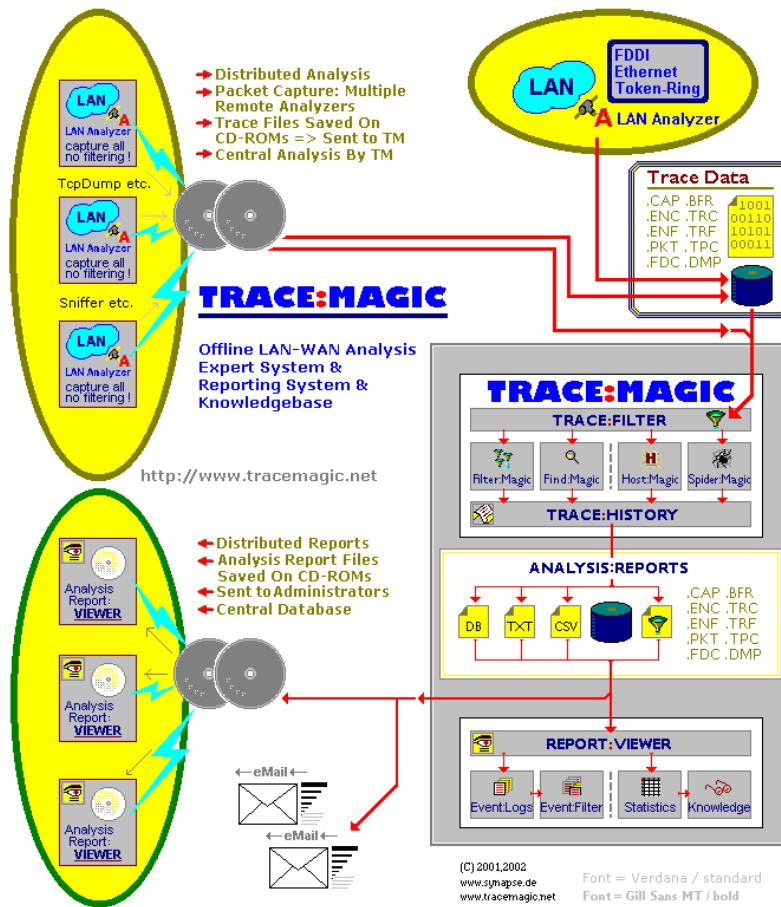
Wünscht der Kunde eine Vernichtung der Aufzeichnungen, so muss der Kunde im selben Schritt Synapse:Networks vollständig entlasten und von allen Rechtsfolgen des Vertrages frei stellen.

Analyse-Preise

Gegenstand	Dauer/ Umfang	Leistungsumfang	Preis je Tag (einschl.Report)
Netzwerk Wartung / Fest-Vertrag Suchen und Finden von LAN/WAN-Fehlern auf Basis fester Wartungs-Verträge.	1. Tag	inklusive Ergebnisbericht: <ul style="list-style-type: none"> • Kurz-Bericht am Abend der Messung auf CD-ROM. • Abschluss-Bericht in der Regel binnen 10 Werktagen, oder nach Absprache. 	2.000 EUR
	jeder weitere Tag		1.700 EUR
Netzwerk Analyse / Einzelfall Suchen und Finden von LAN/WAN-Fehlern nach terminlicher Vorabsprache Bis zu 3 MessRechner im Parallel-Einsatz.	1. Tag	inklusive Ergebnisbericht: <ul style="list-style-type: none"> • Kurz-Bericht am Abend der Messung auf CD-ROM. • <u>Keine</u> weitere Bearbeitung der Daten, kein weiterer Bericht. 	2.500 EUR
	jeder weitere Tag		2.000 EUR
Netzwerk Analyse / Einzelfall Suchen und Finden von LAN/WAN-Fehlern nach terminlicher Vorabsprache Bis zu 5 MessRechner im Parallel-Einsatz.	1. Tag	inklusive Ergebnisbericht: <ul style="list-style-type: none"> • Kurz-Bericht am Abend der Messung auf CD-ROM. • Abschluss-Bericht in der Regel binnen 10 Werktagen, oder nach Absprache. 	5.000 EUR
	jeder weitere Tag		4.000 EUR
Netzwerk Analyse = Notfall Einsatz / Troubleshooting Einsatz sofort nach Notfall-Meldung Zur "Notfall-Messung" wird ein Einsatz dann, wenn zwischen Auftrag und Einsatz max. 48 Stunden liegen. Bis zu 5 MessRechner im Parallel-Einsatz.	1. Tag	inklusive Ergebnisbericht: <ul style="list-style-type: none"> • Kurz-Bericht am Abend der Messung auf CD-ROM. • Abschluss-Bericht in der Regel binnen 10 Werktagen, oder nach Absprache. 	6.000 EUR
Datenanalyse & -auswertung Der Kunde stellt die Daten auf CD-ROM zur Verfügung; Austausch von MessDaten und Report-Daten per Post oder Kurier.	je Tag	Im Regelfall sind mit dem Honorar abgedeckt: bis zu 5 CD-ROMs mit unkomprimierten MessDaten der unterstützten Analyser-Formate.	1.700 EUR
Analyse zur Vorlage bei Gericht und in Gewährleistungsfällen Wir weisen darauf hin, daß wir keine staatlich geprüften Gutachter sind.		Messung vor Ort nach Aufwand & Absprache	
Netzwerkdokumentation Auf Basis von LAN-WAN-Messdaten (LAN Frames, LAN Packets).		Umfang & Kosten nach Absprache	

© 2002,2003

Synapse:Networks GmbH
Theaterplatz 1
53177 Bonn
+49. 228. 93458.0 - phone
+49. 228. 93458.99 - fax
+49. 171. 7421000 - mobile
<http://www.synapse.de/>
info@synapse.de



TODAY'S ANALYSIS LIMITATIONS=CRISIS

LAN
A LAN Analyzer

Online filters reduce trace data and make users partly "blind" regarding the complete scenario

Expert analysis is limited to 1 trace file at a time (causing online filters in order to reduce data)

Filter:Magic Packet Filter / No Analysis
Multiple Filters Per Process Possible (>500)
Hit Frames Written Into New Trace File

Find:Magic High Speed Search Engine / No Analysis
One Search Pattern Per Process
MAC / IP Address, RIF, Name, Hex, Text

Host:Magic Host Data: DHCP, DNS, WINS, NetBIOS-over-IP
Traffic Tables: Host-To-Host; Subnet-To-Host, Subnet-To-Subnet; MAC-IP & ARP Tables

Spider:Magic Expert Analysis: Statistics, Events, Errors
TCP-IP LAN-WAN Communication & ICMP
Client-Serv. Comm. (SMB, Samba, MS-Win_OS-2)

All LAN packets that hit filter criteria or analysis criteria are copied to new trace file

TRACE:MAGIC (C) 2001,2002
Software created by Frank R. Walther
Distributed by Synapse:Networks - Germany