



synapse:
NETWORKS

Netzwerk-Analyse

Trace:Magic
Offline LAN Analysis
Expert System

10.2004

synapse:
NETWORKS

Telefon: 02228 - 9138 - 0 .

Telefax: 02228 - 9138 - 10

Internet Mail: info@synapse.de

WWW: <http://www.synapse.de>



Produkt: Trace:Magic ... LAN-WAN Offline Analysis Expert System & Database

Das von Synapse:Networks GmbH vertriebene Experten-System TraceMagic ist in der Lage, weit mehr zu leisten, als gemeinhin unter "LAN Analyse" verstanden wird:

Strategischer Ansatz

oder: Ein Vergleich zwischen Offline- und Online-Analyse

Warum TraceMagic, wenn das Unternehmen schon Capture+Co im Einsatz hat?

Herkömmliche LAN-Analyser wie Ethereal, EtherPeek, LANdecoder, Observer, Sniffer, Surveyor etc. (hier im Folgenden kurz genannt: "**Capture+Co**") sind in ihren Experten-Systemen teilweise beachtlich leistungsfähig und bieten z.T. Funktionen, die auch TraceMagic nicht hat (Capture Engine, RMON-Abfragen, Echtzeit-Messungen etc.).

Aber:

Offline-Analyse ist mit herkömmlichen LAN-Analysern nicht sinnvoll möglich, weil immer nur 1 Aufzeichnungs-Datei (Trace File, Capture File) zur selben Zeit untersucht werden kann. Also können lange Zeiträume nur mit Online-Analyse "gepackt" werden. Das aber läuft in den meisten Fällen auf folgende Nachteile hinaus:

- Schmerzliche Bindung von Personal für die Anwesenheit bei der Messung
- Kaum Möglichkeiten der Verifikation, wenn Zweifel am Ergebnis auftauchen
- Daher volle Anfechtbarkeit der Ergebnisse, wenn sie jemandem nicht passen
- Daher zu geringer Nutzen bei Gewährleistungs-Fällen (z.B. Hersteller/Lieferant leugnet Fehler)
- Mehrpunkt-Messungen sind schwer bezahlbar (2 x Analyzer-Lizenz, 2 x ausgebildeter Messtechniker, 2 x Reisekosten)

Dem würde von überzeugten Anwendern von **Capture+Co** entgegen gehalten:

- TraceMagic brauche doch noch 1-2 Tage, um den Traffic eines Tages auszuwerten
- Das sei nicht zeitnah genug in der Reaktion, wenn ein Netzwerk-Crash vorliege.

Dem wäre aus der Sicht von TraceMagic wieder entgegen zu halten:

- Erstens:

- Das ist manchmal so - viel zu oft aber genau anders herum.
- Komplizierte Fehler-Bilder mit über den Tag verteilten Abläufen sind online kaum zu fassen.
- Die gründlichen Auswertungen offline ermöglichen erst pro-aktive Analyse (Vorbeugung!).
- Das wiederum verhindert viele Crashes, in denen **Capture+Co** überhaupt erst eingesetzt würden.

- Zweitens:

- TraceMagic hilft sehr wohl, in "Fast-Echtzeit" die laufende Messung zu unterstützen.
- Auf leistungsstarken Rechnern kann das Capturing weiter laufen, während parallel schon TraceMagic mit der Auswertung beginnt.
- So sind zeitnah gute Ergebnisse möglich, und bereits am Abend des Tages ("at the end of the day") kann dem Kunden bereits ein Analyse-Bericht ausgehändigt werden, der nicht nur auf summarischen Online-Ergebnissen, sondern auch bereits auf der tiefer gehenden auf Offline-Verarbeitung beruht, in Datenbanken abgespeichert und in leserlicher Form ausgegeben ist (.TXT, .CSV, .HTML, .DB).
- Daher sind Einwände, TraceMagic wäre zu langsam, geradezu absurd. Das Gegenteil ist richtig. Ohne den Einsatz von TraceMagic wäre schnelle Erkenntnis nur ein Glücksspiel, da die Online-Analyse auf Grund der begrenzten Prozessor-Zeit online manche Effekte nicht erkennen bzw. nicht hinreichend dokumentieren kann.

- Drittens:

- Da **Capture+Co** in der Offline-Analyse an den großen Daten-Mengen scheitern, wird oft wie folgt vorgegangen:
- Es werden Online-Filter gesetzt, und die LAN-Frames werden nur teilweise aufgezeichnet ("Packet Slice", etwa nur die Aufzeichnung der ersten 100-200 Octets).
- Dies führt zu schwer wiegenden Mängeln (methodisch wie praktisch):
- Online-Filter führen dazu, dass der Analyst blind ist gegenüber allen Neben- und Wechselwirkungen bzw. Dritt-Einflüssen, die wegen des Filters nun nicht mehr sichtbar sind.
- Packet-Slice führt ebenfalls zu partieller Blindheit, erschwert in jedem Falle die Applikations-Analyse und verhindert den Nachweis spezifischer Fehler auf dem Physical Layer (Fehler, die in modernen LAN-Switches nicht selten vorkommen).
- Somit sind Vorgehensweisen, bei denen nicht der gesamte LAN-Traffic aufgezeichnet wird, nicht praktikabel und auch nicht akzeptabel.
- Somit können alle Messungen, bei denen nicht alles aufgezeichnet und ausgewertet wurde, von beliebigen Dritten in jeglicher Form - zu Recht! - angezweifelt und abgelehnt werden.
- Über TraceMagic können auch große DatenMengen im GigaByte-Bereich ausgewertet werden. Es gibt also keinen Grund mehr, nicht alles aufzuzeichnen.
- Somit ist die Anwendung von TraceMagic ein Muss.

Etwas sanfter, fairer ausgedrückt, ergibt ein System-Vergleich das folgende Ergebnis:

- Beide Produkt-Klassen haben ihre volle Berechtigung.
- Wer durch TraceMagic bestimmte Hinweise erhält, muss sie in schwerwiegenden Fällen manuell verifizieren.
- Hierzu ist ein klassischer LAN-Analyzer sehr wohl geeignet (einige davon sogar sehr gut).
- Gerade die Fähigkeit von TraceMagic, aus Millionen von LAN-Frames die paar Hundert oder Tausend heraus zu ziehen, auf die es ankommt, hilft im Umgang mit herkömmlichen LAN-Analysern:
- Jeder LAN-Analyzer wie **Capture+Co** freut sich, dieses Substrat der Fehler-Essenz quasi "vorgekaut+vorverdaut" geliefert zu bekommen.

In letzter Konsequenz zeichnen sich klare Trennungen in der Bewertung aus:

- Gerichtsfeste Nachweise sind ohne TraceMagic praktisch nicht gültig erbringbar, ...
- ..., weil dies die wissenschaftlich-methodische Unangreifbarkeit des Ergebnisses verlangt:
- Unangreifbarkeit der Ergebnisse verlangt volle Reproduzierbarkeit durch beliebige Dritte zu beliebiger Zeit.

Einen Schritt weiter gedacht, bedeutet dies:

- Online ließen sich LAN-Traffic-Daten beliebig und vorsorglich mitlesen, um sie in Störfällen sodann zur Analyse heran zu ziehen.
- In diesem Zusammenhang gibt es das Produkt NetVCR (NikSun) für permanentes Archivieren des Datenstroms auf Festplatte oder Tapes (sehr teuer, nur für große Unternehmen geeignet).
- Der Nutzen solche Archiv-Systeme ist jedoch auf den Placebo-Effekt vermindert, so lange nur mit herkömmlichen LAN-Analysen zur Auswertung der Archive gearbeitet wird. Denn:
- Die nachträgliche Auswertung solcher Archive ist nur (!!) mit TraceMagic möglich (Stand: Anfang 2003).
- Jeder herkömmliche LAN-Analyzer scheitert total an der nachträglichen Auswertung.

Daraus folgt:

- Im Grunde müsste neben TraceMagic bei großen Unternehmen auch NetVCR angeboten werden.
- Vorteil NetVCR: Indizierung über Tage, schneller Zugriff auf kleinere Zeit-Einheiten.
- Mittelfristig soll TraceMagic auch eine solche Funktion erhalten.

Bis dahin gilt:

- Für Messungen im Bereich von 12-48 Stunden reicht z.B. EtherPeek_NX aus.
- Die Übersicht in diesen Datenmengen ist auch mit TraceMagic heute möglich.
- DVD statt CD-ROM für die Archivierung (STACCer-MessRechner kommt daher mit DVD).

Zurück zum Ausgang: Der Vergleich zwischen den Analyse-Produkten bzw. die Abgrenzung gegen einander. Hier lässt sich wie folgt zusammen fassen:

- Sicher sind **Capture+Co** auf ihre Weise taugliche Produkte. Dies kann kaum sinnvoll angezweifelt werden.
- Das, worüber die Kunden sich oft täuschen (lassen), sind die Zusammenhänge zwischen Vorbeugung, Arbeitsteilung, Personalknappheit, Personalkosten, Reaktionszeit und Revisionsfähigkeit der Analyse.

Diese Zusammenhänge sind wie folgt zu sehen:

Arbeitsteilung:

- Heute unternimmt ein Messtechniker die Analyse, alle anderen müssen sich blind auf die Aussagen verlassen.
- Daher werden oft mehrere Messtechniker parallel eingesetzt. Sind mehrere Parteien an einem Störfall beteiligt, setzte jede Partei einen eigenen Messtechniker ein, um zu eigenen Ergebnissen zu kommen. Dies ist methodisch absurd, und dies ist wirtschaftlich gesehen völlig abwegig.

Revisionsfähigkeit:

- Dritte können daher (erst einmal offline gegangen) die Ergebnisse nicht mehr nachvollziehen.

Personalknappheit, Personalkosten:

- Wer **Capture+Co** wirklich nutzen will, muss das Personal teuer ausbilden.
- Ist der Techniker erst mal teuer ausgebildet, wird er abgeworben.
- Somit ist der Unternehmens-Prozess "Analyse" nicht mehr verfügbar; - trotz Analyzer-Lizenz.
- Somit ist "Analyse" ein Zufalls-Spiel, abhängig von der Personal-Verfügbarkeit und -Fluktuation.
- Das ist ein unannehmbare Zustand.

Reaktionszeit:

- Somit sind die Reaktionszeiten bei Crashes nicht mehr klar vorhersagbar.
- Reaktionszeiten hängen vom Zufall der Personal-Entwicklung ab.

Die Argumentation gegen **Capture+Co** ist also nur in einem Punkt technisch bedingt:

Die Unfähigkeit, offline die Daten auszuwerten (und das in beliebiger Wiederholung zwecks Verifikation bzw. Reproduktion -> methodisch/wissenschaftlich unabdingbar für die Gültigkeit=Anerkennung der Ergebnisse durch beliebige Dritte).

Ansonsten ist die Argumentation gegen **Capture+Co** betriebswirtschaftlich bedingt:

- Zu teuer, da zu personal-intensiv.
- Zu ungewiss, da von teuer ausgebildetem Personal abhängig.
- Zu unwirtschaftlich auch, weil die Ergebnisse anfechtbar sind (da nicht beliebig reproduzierbar)
- Zu heikel, da pro-aktiv nicht weit genug einsetzbar (zu sehr auf re-aktives Handeln bezogen).

Dass diese Argumentation stimmt und für die betriebliche Praxis von unmittelbarer Wirkung ist, zeigt sich in einem Anwender-Bericht des Bayerischen Rundfunks (BR) in der Zeitschrift Network World, Ausgabe 19/2002 (11.Nov.2003). Dort trifft der Abteilungsleiter, Michael Renollet, die zentrale Feststellung:

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

NetworkWorld:

Wie sind die bisherigen Erfahrungen mit der Analysesoftware »Trace:Magic« von Synapse Networks?

Renollet:

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 Netzwerkadministratoren ist es möglich, mit Trace:Magic rasch gute Ergebnisse zu erzielen.

NetworkWorld:

Welchen wirtschaftlichen Nutzen bringt der Einsatz dieser Netzmanagement- und Analyse-Tools?

Renollet:

Sehr wichtig ist für uns die Rationalisierung: Ich habe insgesamt neun interne und externe Mitarbeiter, die ein Netz mit rund 5000 Nodes betreuen. Deshalb brauchen wir möglichst einfache aber dennoch aussagekräftige Analysen auf Knopfdruck.

Die betriebliche Praxis gerade in Zeiten knappen Geldes und dünner Personaldecke läuft zwingend darauf hinaus,

- Unternehmens-Prozesse zu automatisieren,
- vom Personal weitgehend unabhängig zu machen,
- sie genau dadurch (und nur dadurch) verfügbar zu machen.

Viele Unternehmen haben das erkannt und haben die LAN-Analyse in weiten Teilen auf TraceMagic umgestellt. Eine Auswahl der größten TraceMagic-Kunden ist hier zu finden.

Somit lautet das Fazit:

FAZIT:

Herkömmliche LAN-Analyser sind ohne Ergänzung durch Offline-Analyser bzw. TraceMagic oft zu wenig wirkungsvoll, zu wenig kalkulierbar in Einsatz und Ergebnis. Umgekehrt wäre es ein Trugschluss, nur mit TraceMagic ohne LAN-Analyser wären alle Fehler zu finden.

Das eine zu tun, ohne das andere zu lassen: "L'unité fait la force" - in der Einigkeit (Gemeinsamkeit) liegt die Stärke.

Leistungsumfang

Daten-Aufnahme (Capturing)

Alles wird mitgelesen

Basierend auf der Fähigkeit, auch Gigabytes von Messdaten vollständig auswerten zu können, werden bei unseren Messungen **alle** LAN-Pakete am Messpunkt mitgelesen und abgespeichert, auch bei Gigabit-Ethernet.

Keine Online-Filter

Es werden **keine** Filter gesetzt: Somit kann **nichts** verloren gehen; die Wahrscheinlichkeit, dass während einer Messung Fehler auftreten, die wegen falsch gesetzter Aufnahme-Filter nicht aufgezeichnet werden, ist praktisch nahe oder gleich Null.

Revisionsfeste Nachweise

Somit sind unsere Ergebnisse auch **revisionsfest**, da sie wegen ihrer Lückenlosigkeit nicht mehr angezweifelt werden können.

Auswertung & Bericht

Die Auswertung von Messdaten erfolgt ganz überwiegend über das Experten-System TraceMagic.

Vorteile:

- Es können enorme Mengen von Messdaten automatisch verarbeitet werden.
- Es können Fehler in allen Netzwerk-Schichten (OSI Layer 1-7) automatisch erkannt werden.
- Es kann auf automatisch erzeugte Ergebnis-Berichte und -Datenbanken zurück gegriffen werden.
- Die automatisch erzeugten Reports liegen vor in folgenden Formaten:

.TXT	-> Event Log -> chronologischer Ereignis-Ablauf mit Fehler-Darstellung
.TXT	-> Statistiken in lesbarer, formatierter Aufmachung
.CSV	-> Statistiken in Tabellen-Format (etwa zur weiteren Verarbeitung in Excel)
.DB	-> Datenbanken mit äußerst umfangreichen Statistiken zu TCP/IP und Layer7
.HTML	-> Ergebnis-Ausgabe der Datenbanken in HTML-Projekten (voll indiziert).

Diese Reports können mit dem TraceMagic-VIEWER-Modul nachbearbeitet werden. Auch erlaubt das **lizenzfreie!** VIEWER-Modul den vollen Zugriff auf die Ergebnis-Datenbanken (.DB). Hierdurch können die Ergebnisse objektiv, neutral und umfassend durch beliebige Dritte vollständig nachvollzogen werden.

Nachweis-Umfang

Die Nachweise zum Kommunikations-Geschehen decken alle Netzwerk-Schichten ab:

Schicht	Name	Funktionen / Fehler
Layer 7	Application	Fehler in Client-Server-Dialogen, Logins, etc.
Layer 6	Presentation	(veraltet)
Layer 5	Session	Fehler in Namens-Diensten: NetBIOS, DNS, ...
Layer 4	Transport	Fehler in der Datenfluss-Steuerung (TCP)
Layer 3	Network	Fehler im Routing: WAN, Layer-3-Switching (IP)
Layer 2b	Data-Link / DLC Layer	Fehler rund um die Protokoll-Zuordnungen
Layer 2a	Data-Link / MAC Layer	Fehler rund um MAC-Adressen, Broadcasts, Multicasts
Layer 1	Physical	Fehler in der Bitübertragungsschicht, u.a. in LAN-Switches

Highlights dieser Nachweisfähigkeit von TraceMagic sind (Auswahl der wichtigsten bzw. auffälligsten Funktionen):

Schicht	Funktionen / Fehler
Layer 7	<p><u>Script Reconstruction / Script Follow-Up</u></p> <p>Fehler bei LOGIN-Vorgängen können automatisch Befehlen in Login-Scripts (.DAT, .BAT, .CMD, .INI, u.a.m.) zugeordnet werden.</p> <p>TraceMagic rekonstruiert aus den Messdaten die von Clients eingelesenen Scripts, die vom Sever geladen werden, und vergleicht die nachfolgenden Aktionen mit den Script-Befehlen. Fehler und Auffälligkeiten werden im Event-Log ausgegeben bzw. angezeigt.</p>
Layer 7	<p><u>File Services: Access Failure / Zugriffs-Fehler</u></p> <p>Was bisherige Analyzer in seinem wahren Ausmaß nie sichtbar gemacht haben, sind die teilweise bizarr falsch ablaufenden Datei-Zugriffe der Windows-Clients.</p> <p>TraceMagic erfasst alle Zugriffe, die seitens der Server (OS-2, Windows, Samba, Novell NetWare, HTTP-WWW) mit einer Fehler-Kennung abgelehnt werden. Im Bereich der Windows-Server werden zudem alle Ressourcen, die Clients erfolglos anfordern, zusätzlich in einer Datenbank erfasst und nachträglicher Bearbeitung zugänglich gemacht.</p> <p>TraceMagic erfasst weiterhin alle Datei-Zugriffe, die erfolgreich verlaufen, und weist in separaten Tabellen alle Zugriffe nach unter Nennung von Ressourcen-Name (Datei-Name) und File-Handle (vom Server heraus gegebener Zugriffs-Schlüssel). Auf diese Weise können einerseits reguläre Vorgänge nachvollzogen werden - aber es können auch Fehler nachgewiesen werden wie z.B. Endlos-Schleifen, bei denen ein Client in steter Wiederkehr die selbe Datei öffnet-liest-schließt.</p> <p>TraceMagic macht auch alle Teil-Schritte von Datei-Zugriffen sichtbar. Auf diese Weise kann beispielsweise nachvollzogen werden, wenn ein Client beim Lesen einer Datei ständig an der selben Daten-Position (Offset) fest hängt und nicht weiter kommt.</p>
Layer 5/7	<p><u>Name Services: Fehler in der Adress- und Namens-Auflösung</u></p> <p>Fehler in der Adress- und Namens-Auflösung können ganze Arbeitsabläufe nicht nur behindern, sondern vollständig lahm legen.</p> <p>Das häufigste Szenario jedoch ist, dass Fehler in den Namensdiensten Arbeitsabläufe verzögern - mit der Folge, dass Anwender auf Grund der Verzögerungen zum Schluss kommen:</p> <p>"Das Netzwerk ist langsam!"</p> <p>TraceMagic erfasst alle Client-Anfragen, Namen in Adressen aufzulösen, in folgenden Protokollen:</p>

	<ul style="list-style-type: none"> - DNS (besonders, falls mit Active Directory / ADS verbunden) - NetBIOS over LLC (NetBEUI) - NetBIOS over IP-UDP / Port 137 = NetBIOS Name Service / WINS - NetBIOS over IP-UDP / Port 138 = NetBIOS Datagram - NetBIOS over IP-TCP / Port 139 = NetBIOS Session (SMB) <p>In etwas weniger umfassender Form werden außerdem berücksichtigt:</p> <ul style="list-style-type: none"> - NetWare Client Requests, gerichtet an die Bindery - NetWare Client Requests, gerichtet an die NDS - Windows Client Requests, vorgenommen via Kerberos <p>Im Bereich von WINS, UDP-138 und DNS werden die Ergebnisse in ausführlichen Tabellen ausgegeben, um schnelle Erfolgs-Übersicht zu haben bezüglich der gesamten Tätigkeit der Namensdienste. Es wird schnell erkannt:</p> <ul style="list-style-type: none"> - Welche NetBIOS-WINS-DNS Namen nicht auflösbar sind - Welche Namen falsch notiert / formatiert sind - Welche Namen im lokalen Netz überhaupt nicht existieren - Welche Phantom-Namen im Windows-Bereich vorhanden sind - Welche Namen von den Name Servern nicht richtig behandelt werden
Layer 5/7	<p><u>Host Configuration: DHCP-Dialoge</u></p> <p>Fehler jeglicher Art können darauf zurück zu führen sein, dass Clients nicht wie gewünscht per DHCP konfiguriert werden.</p> <p>Dies kann auf verschiedene Weise geschehen:</p> <ul style="list-style-type: none"> - Clients nehmen erwartungswidrig nicht an DHCP teil. - Clients übergehen DHCP-Werte auf Grund lokaler Registry-Werte - Clients sind verwirrt wegen verschiedener DHCP-Server/Relay-Agents <p>TraceMagic wertet alle DHCP-Requests/Replies aus und stellt das Ergebnis in den Report-Dateien tabellarisch dar; außerdem werden die Vorgänge im Event-Log festgehalten.</p> <p>Zu den wichtigsten Informationen, die auf diese Weise zugänglich werden, gehören:</p> <ul style="list-style-type: none"> - Wie viele Requests sender der DHCP Client - Welcher DHCP-Server antwortet welchem DHCP-Client - IP Subnet Address - IP Subnet Mask - IP Subnet Broadcast Address - DNS Server -> IP Address - WINS Server -> IP Address - Time Server -> IP Address <p>Bei mehr als nur einem Kunden kam auf diese Weise heraus, dass die DHCP-Landschaft durchaus *nicht* so aussah, wie behauptet bzw. gewollt.</p>
Layer 4	<p><u>Data Flow Control / Datenfluss-Steuerung (TCP)</u></p> <p>TCP-Analyse ist bei den bisherigen Analyse-Methoden in vielen, entscheidenden Bereichen stark unterentwickelt, weil Online-Analyzer nicht die System-Ressourcen zur Verfügung stellen können, um komplexe Auswertungen zu ermöglichen.</p> <p><u>TCP Retransmissions / Packet Loss</u></p> <p>Der Nachweis von Wiederholungs-Übertragungen ist etwas komplizierter, als es herkömmliche LAN-Analyzer vermuten lassen. Nur über große Tabellen, in denen für jeden einzelnen von bis zu 65.000 IP-Teilnehmern Kommunikations-Daten für ein lange nachhängendes Zeitfenster präsent gehalten werden, können auch seltene Fehler zuverlässig erkannt werden.</p>

	<p>Herkömmliche Analyser können immer nur online mit knappen Statistiken arbeiten oder offline mit der Beschränkung, jeweils nur die LAN-Packets aus einer einzigen Aufzeichnungs-Datei bearbeiten zu können. Somit ist online zwar die Betrachtung langer Zeiträume, aber komplizierter Fehler nicht möglich, während offline zwar die Gelegenheit zu eingehenderer Betrachtung da ist, dafür aber die Datenmenge auf die wenigen LAN-Packets beschränkt ist, die in jeweils nur einer Aufzeichnungs-Datei abgespeichert sind. Diese Einschränkungen sind nicht hinnehmbar, und sie werden durch TraceMagic ganz oder vollständig aufgehoben.</p> <p><u>TCP Disordered Sequences / Routing Errors</u></p> <p>Nicht selten kommt vor, dass TCP-Pakete in ihrer Reihenfolge verdreht beim Empfänger ankommen. Dies geht in der Regel auf Ereignisse im IP-Routing zurück, wobei in Frage kommen: (a) Ereignisse wie Leitungs-Abbruch oder Router-Ausfall, (b) Ereignisse wie Load-Balancing.</p> <p>TCP-Fehler auf solche Layer-3-Ereignisse zurück führen zu können, ist von großer Bedeutung in der Analyse, um die richtigen Zusammenhänge erkennen zu können. Herkömmliche Analyser tun sich hier schwer oder bieten schlicht gar keine Möglichkeit, diese Zusammenhänge zu sehen.</p> <p><u>TCP Session Denied / Service Unavailable</u></p> <p>Immer wieder kommt es vor, dass TCP-Sitzungen, die von einzelnen Teilnehmern begehrt werden, von der Gegenstelle nicht akzeptiert werden.</p> <p>Die beiden hauptsächlichen Gründe können sein:</p> <ul style="list-style-type: none"> - Überlastung der Gegenstelle (des Servers) - Keine Unterstützung des TCP-Ports bzw. des Services/Dienstes <p>Diese Szenarien können harmlos sein (z.B., wenn eine Server kein SNMP unterstützt), aber sie können auch dramatisch sein (z.B. wenn ein Server unter steter Überlast leidet).</p> <p>Hier schnell die Abläufe zu erkennen, sie Servern und Applikationen zuzuordnen, gehört zu den Stärken der TraceMagic-Auswertung, da die entsprechenden Daten über eine Ergebnis-Datenbank beliebig abfragbar und sortierbar sind.</p> <p><u>TCP Port Statistics</u></p> <p>Alle diese Fehler und Ereignisse (und noch viele andere mehr) lassen sich über den TCP-Port einzelnen Applikationen zuordnen.</p> <p>Anders gesagt: Umfassende Tabellen können Aufschluss darüber geben, welche Applikationen von Transport- bzw. Übermittlungs-Fehlern betroffen sind. Herkömmliche Analyser haben nicht die nötigen Ressourcen, solch umfangreiche Tabellen aufzubauen und zuverlässig zu führen. TraceMagic kann dies, da die System-Architektur gerade zum Führen solcher Tabellen ausgelegt wurde.</p> <p>Die entsprechende Ergebnis-Datenbank kann über das Report-VIEWER-Modul *lizenzfrei* von Dritten bearbeitet und abgefragt werden. Somit sind die Ergebnisse beliebig vermittelbar.</p>
Layer 3	<p><u>Routing Errors / Internet & WAN</u></p> <p>IP-Analyse ist alles andere als trivial. Was von gängigen Analysern aus dem IP-Bereich sichtbar gemacht wird, ist oft weit unterhalb dessen, was tatsächlich "zu holen ist".</p> <p><u>Router melden sich per ICMP</u></p> <p>Wenn Router IP-Pakete verwerfen (warum auch immer), geben sie für gewöhnlich ICMP-Meldungen von sich, die an den Absender des verworfenen Paketes gerichtet sind.</p> <p>Eine vollständige Erfassung aller dieser Szenarien versteht sich von selbst und wird auf geliefert.</p>

	<p><u>Router melden sich *nicht* per ICMP</u></p> <p>WAN-Provider sorgen mit Vorliebe dafür, dass ICMP-Meldungen ihrer Router nicht bei den Kunden im Campus-LAN ankommen - damit der Kunde nicht alle Fehler und Instabilitäten nachvollziehen kann, die sich da ereignen.</p> <p>TraceMagic ist in weitem Umfang in der Lage, WAN-Fehler und Weiterverkehrs-Instabilitäten nachzuweisen *auch dann, wenn* die ICMP-Meldungen nicht bis zum Campus-LAN des Kunden durchgelassen werden.</p> <p>Die hierzu nötigen Techniken sind bei sehr vielen der am Markt gängigen Analyser nicht gegeben - und also können die Nachweise nicht geführt werden.</p> <p>Hierzu gehört, dass Merkmale der Protokolle IP (Layer 3) und TCP (Layer 4) gründlich über lange Zeiträume betrachtet, erfasst und ausgewertet werden.</p> <p>TraceMagic kann das, andere Analyser nicht.</p>
Layer 2	<p><u>MAC Errors</u></p> <p>Verschiedenste, LAN-typische Fehler werden von TraceMagic berücksichtigt - und, wie so oft, zusätzlich Ereignisse und Fehler, die von den üblichen Analysern *nicht* erkannt werden.</p> <p>Ein Beispiel: In 2002 wurden mehrfach Switches eines großen Herstellers dabei "erwischt", eingehende LAN-Pakete vervielfältigt auf der Ausgangsseite auf die Leitung zu geben.</p> <p>Die am Markt gängigen Analyser (auch von Weltmarktführern) waren/sind *nicht* in der Lage, dieses Szenario zu erkennen - TraceMagic schon.</p> <p>(Zur Erklärung: Andere Analyser weisen das als "TCP Retransmission" aus, oder ähnlich - jedenfalls als Wiederholungs-Übertragung.)</p> <p>Spanning Tree, Ethernet, Token-Ring, FDDI - für jede Topologie gibt es spezielle Analyse-Funktionen.</p>

FAZIT:

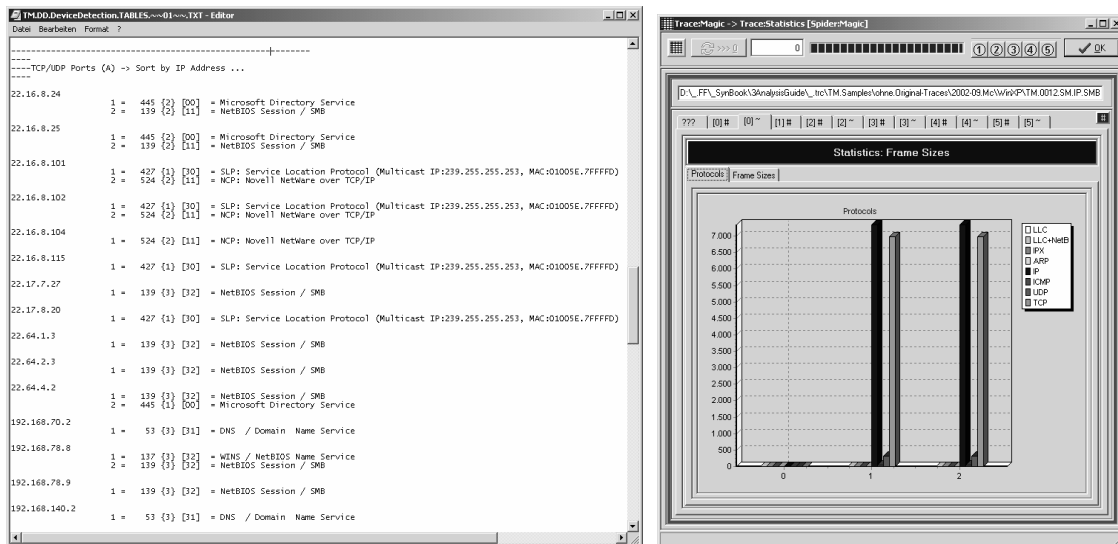
TraceMagic ist den in vielen Funktionen herkömmlichen LAN-Analyse-Systemen weit voraus. Für vorbeugende (pro-aktive) Qualitätssicherung im IT-Umfeld ist TraceMagic daher vollkommen unverzichtbar.

Beispiele für Event-Logs von TraceMagic

Diese Beispiele beschreiben nur einen winzigen Teil der Ergebnis-Ausgabe. Die TraceStatistics-Datenbank, das HTML-Report-Projekt sowie die CSV-Tabellen samt der zugehörigen Text-Berichte sind im beschränkten Umfang dieses Katalogs kaum darstellbar.

Nachweis von Auffälligkeiten und Fehlern in der Voice-over-IP Kommunikation. Hierzu werden die Sprach-Pakete, das Steuerungs-Protokoll sowie das Verhalten von TCP und IP gleichzeitig betrachtet.

Darstellung aus dem Event-Log mit dem Nachweis spezieller Fehler auf Layer 1-2-3: Pakete sind verfälscht, und gleichzeitig sind Paket-Inhalte mehrfach auf der Leitung. (Ein zur Zeit häufig zu beobachtender Fehler von LAN-Switches.)



OBFEN: Nachweis der aktiven Komponenten: IP-Adressen, TCP-Ports, Services; Protokoll-Statistik.

The screenshot shows the Trace-Magic web interface with the following sections:

- HostMagic**
 - [Device Detection: Switches, Router, Server](#)
 - [Single Hosts: DHCP & Name Services](#)
- SpiderMagic**
 - [Trace Statistics: Protocols, Frame Sizes](#)
 - [TCP/IP: Events & Errors](#)
 - [TCP/IP: Top Talkers](#)
 - [TCP/IP: TCP-UDP Port Statistics - Application Errors](#)
 - [TCP/IP: IP Hosts - Events & Errors \(IP - ICMP - TCP - UDP\)](#)
 - [TCP/IP: IP Hosts - Events & Errors \(IP\)](#)
 - [TCP/IP: IP Hosts - Events & Errors \(ICMP\)](#)
 - [TCP/IP: IP Hosts - Events & Errors \(TCP\)](#)
 - [SMB \(Windows, OS/2, Samba\): Denied Resources](#)
- Knowledgebase - TraceEvents**
 - [TraceEvents / KnowledgeBase](#)
- Event Log**
 - [tm_hit.frames.00~000.log_\(192.168.111.151\)_.htm](#)
 - [tm_hit.frames.00~000.log_\(192.168.111.152\)_.htm](#)
 - [tm_hit.frames.00~000.log_\(192.168.111.151\)_.htm](#)

Die Ergebnis-Ausgabe erfolgt im SpiderMagic-Modul auch im HTML-Format. Mit wenigen Ausnahmen werden sämtliche Teil-Reports in einem übergreifenden, voll indizierten HTML-Projekt zusammen gefasst bzw. zugänglich gemacht.

Leichte Navigation, gute Übersicht, klare Struktur erlauben auch unerfahrenen Dritten, problemlos Zugang zu den Ergebnissen zu finden.

Auf diese Weise können die Ergebnisse schnell gegenüber anderen Abteilungen, Lieferanten, Dienstleistern kommuniziert und in Handlung umgesetzt werden.

INDEX: C:\Trace\Seminar\Netlogon_ENF_und_DOC\TM.0006.SM.IP.SMB.NCP.HTTP.RC.PS\html\ - Netscape

TRACE:MAGIC syn Synapse:Networks LAN WAN Analysis Expert System & Knowledgebase Trace Reports & Statistics

TCP - UDP Port Statistics

c:\trace\seminar\netlogon_enf_und_doc\tm.0006.sm.ip.smb.ncp.http.rc.ps\html\tm.sm.spidermagic.tables.~03.00~.htm

[0] #	[1] Port (dec.)	[2] Port (hex.)	[3] all UDP Pkts [Rc]+ [Tx]	[4] all TCP Pkts [Rc]+ [Tx]	[5] UDP+TCP Pkts [Tx]	[6] UDP+TCP Pkts [Rc]	[7] UDP+TCP Octs [Tx]	[8] UDP+TCP Octs [Rc]	[9] TCP/SYN [Tx]	[10] TCP/SYN [Rc]	[11] SYN/ACK [Tx]	[12] SYN/ACK [Rc]	[13] SYN/RST [Tx]	[14] SYN/RST [Rc]
1	Trace:Magic	Port:Statistics	0	0	0	0	0	0	0	0	0	0	0	0
2	53	0x 0035	10	0	4	6	1510	369	0	0	0	0	0	0
3	67	0x 0043	46	0	23	23	7544	7544	0	0	0	0	0	0
4	68	0x 0044	46	0	23	23	7544	7544	0	0	0	0	0	0
5	80	0x 0050	0	334	163	171	143868	18967	0	11	11	0	0	0
6	137	0x 0089	332	0	166	166	16622	16622	0	0	0	0	0	0
7	138	0x 008A	48	0	24	24	5804	5804	0	0	0	0	0	0
8	139	0x 008B	0	95	41	54	5639	6472	0	4	4	0	0	0
9	520	0x 0208	22	0	11	11	792	792	0	0	0	0	0	0
10	1025	0x 0401	0	53	30	23	3882	2754	2	0	0	0	2	0
11	1026	0x 0402	0	28	16	12	1586	2091	1	0	0	0	1	0
12	1028	0x 0404	4	0	3	1	189	461	0	0	0	0	0	0
13	1029	0x 0405	0	66	34	32	4942	37882	1	0	0	0	1	0
14	1030	0x 0406	0	43	22	21	2998	25833	1	0	0	0	1	0
15	1031	0x 0407	2	14	9	7	1065	1314	1	0	0	0	1	0
16	1032	0x 0408	0	7	4	3	495	466	1	0	0	0	1	0
17	1033	0x 0409	2	0	1	1	57	339	0	0	0	0	0	0
18	1034	0x 040A	0	7	4	3	164	124	1	0	0	0	1	0

Dokument: Übermittelt

TRACE:MAGIC syn Synapse:Networks LAN WAN Analysis Expert System & Knowledgebase Trace Reports & Statistics

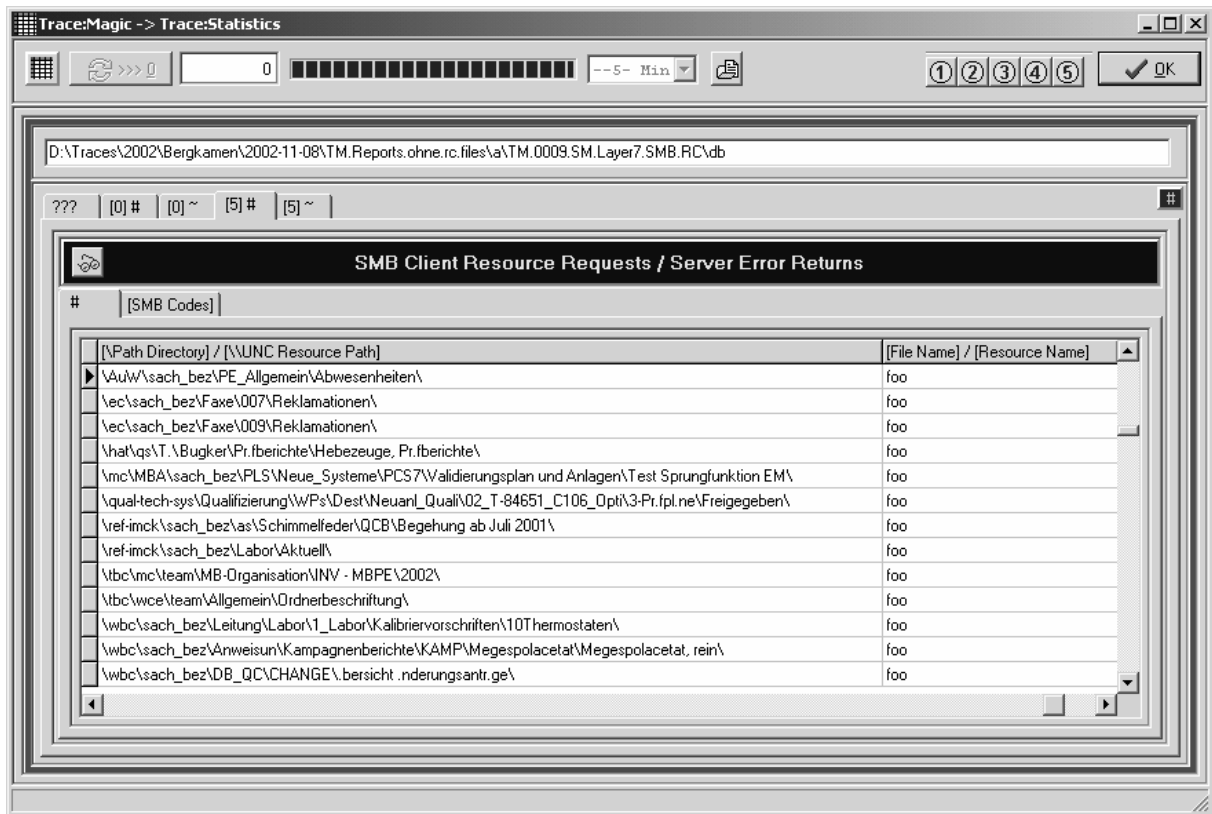
IP Host Statistics: IP - ICMP - TCP # Hosts

c:\trace\seminar\netlogon_enf_und_doc\tm.0006.sm.ip.smb.ncp.http.rc.ps\html\tm.sm.spidermagic.tables.~04.00~.htm

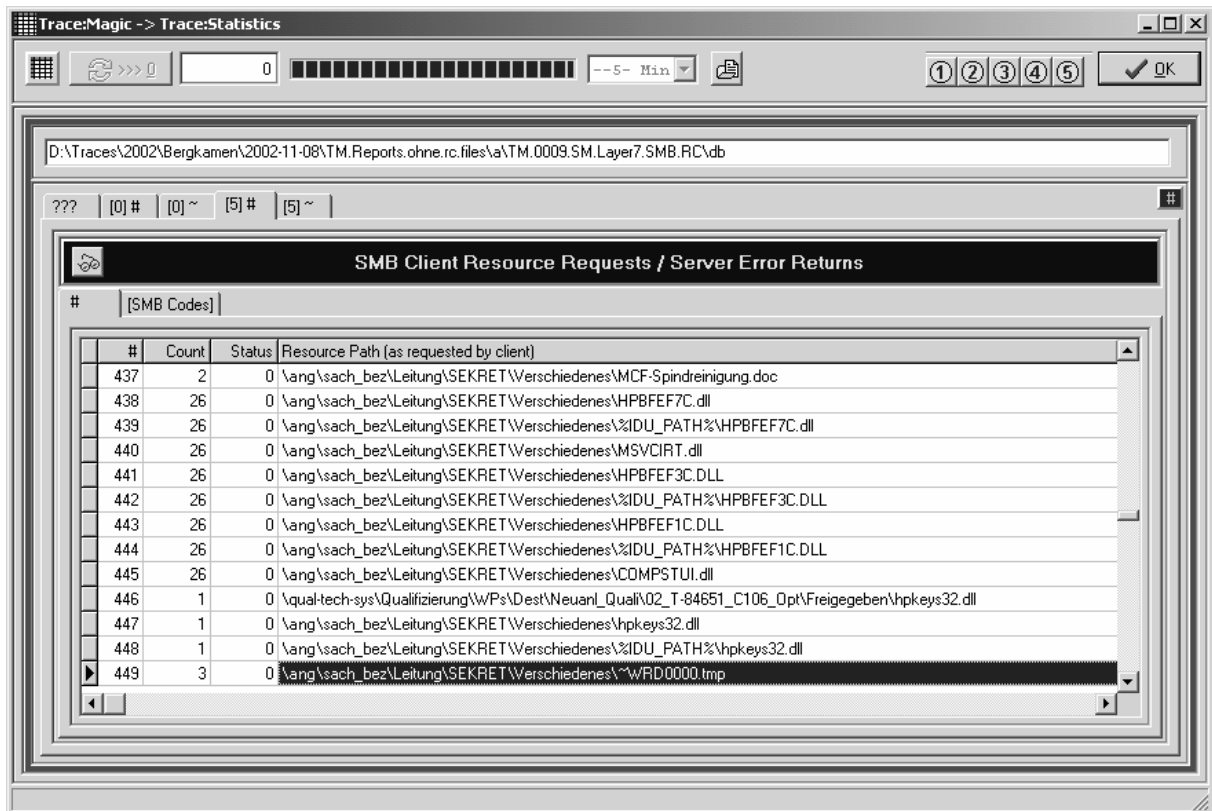
[0] #	[1] IP Address (dec.)	[2] IP Address (hex.)	[3] MAC Address(es)	[4] IP Packets	[5] TCP Packets	[6] UDP Packets	[7] ICMP Packets	[8] *	[9] Event Packets
1	Trace:Magic	TCP/IP Analysis		0	0	0	0	0	0
2	[1] 0.0.0.0	0x 00000000		1	4	0	4	0	0
3	[1] 129.42.18.99	0x 812A1263		1	105	105	0	**	16
4	[1] 192.76.144.66	0x C04C9042		1	4	0	4	0	0
5	[1] 192.168.111.1	0x C0A86F01		1	159	41	117	1	0
6	[1] 192.168.111.5	0x C0A86F05		1	231	198	33	0	4
7	[1] 192.168.111.151	0x C0A86F97		1	20	0	20	0	0
8	[1] 192.168.111.152	0x C0A86F98		1	108	27	80	1	0
9	[1] 207.46.130.149	0x CF2E8295		1	3	3	0	0	1
10	[1] 207.46.230.229	0x CF2EE6E5		1	53	53	0	0	6
11	[1] 216.39.104.49	0x D8276831		1	2	2	0	0	0

TRACE:MAGIC syn Synapse:Networks

Dokument: Übermittelt



OBEN/UNTEN: Nachweis von Ressourcen, die Clients vergeblich auf Servern per Netzwerk-Zugriff gesucht haben. Die Datenbank-Tabellen erlauben das Sortieren nach verschiedensten Gesichtspunkten; die Event-Log-Filter erlauben das schnelle Herunterbrechen auf die beteiligten Clients bzw. erlauben das Isolieren der jeweiligen Einzel-Vorgänge.



OBEN: Hier haben Clients lokale Umgebungs-Variablen nicht in die Klartext-Werte umgesetzt; folglich stimmen die Pfad-Angaben nicht, da statt Unterverzeichnis-Namen die Variablen-Namen auftreten.

Trace:Magic -> Trace:Statistics

D:\Traces\2002\Bergkamen\2002-11-08\TM.Reports.ohne.rc.files\b\TM.0007.SM.Layer7.SMB.RC\db

??? [0] # [0] ~ [5] # [5] ~

SMB Client Resource Requests / Server Error Returns

[SMB Codes]

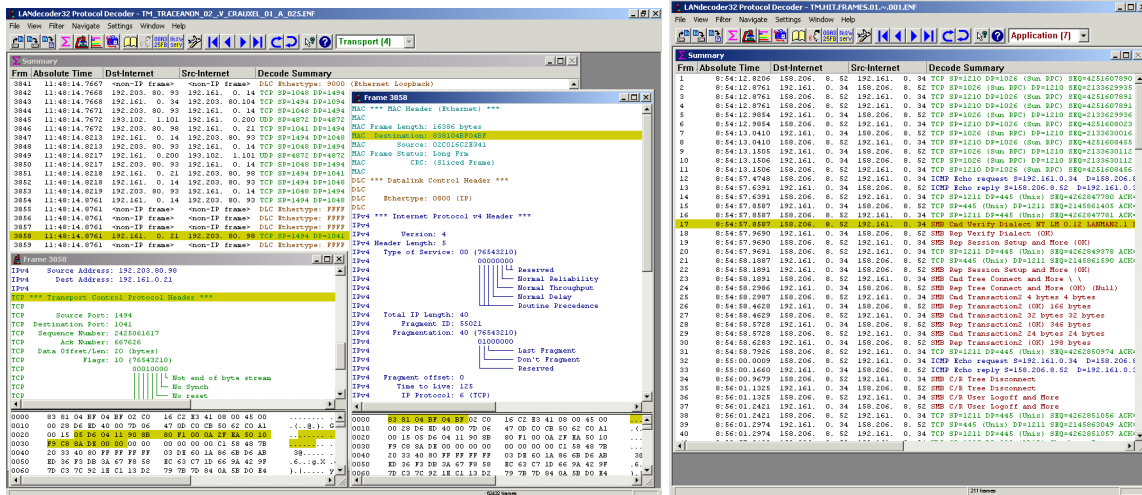
#	Count	Status	Resource Path (as requested by client)
1342	1	0	\de\ccmail.de\602.s\ccmail\SAPLogin 66218.exe
1345	1	0	\de\ccmail.de\602.s\ccmail\SAPLogin 66218 SAP_AUTOLOGIN.exe
1348	1	0	\de\ccmail.de\602.s\ccmail\SAPLogin 66218 SAP_AUTOLOGIN P60.exe
1351	1	0	\de\ccmail.de\602.s\ccmail\SAPLogin 66218 SAP_AUTOLOGIN P60 001.exe
1354	1	3	\de\ccmail.de\602.s\ccmail\SAPLogin 66218 SAP_AUTOLOGIN P60 001 .exe
1357	1	3	\de\ccmail.de\602.s\ccmail\SAPLogin 66218 SAP_AUTOLOGIN P60 001 .exe
1360	1	3	\de\ccmail.de\602.s\ccmail\SAPLogin 66218 SAP_AUTOLOGIN P60 001 .exe
1363	1	3	\de\ccmail.de\602.s\ccmail\SAPLogin 66218 SAP_AUTOLOGIN P60 001 .exe
1366	1	3	\de\ccmail.de\602.s\ccmail\SAPLogin 66218 SAP_AUTOLOGIN P60 001 .exe
1369	1	3	\de\ccmail.de\602.s\ccmail\SAPLogin 66218 SAP_AUTOLOGIN P60 001 .exe
1372	1	3	\de\ccmail.de\602.s\ccmail\SAPLogin 66218 SAP_AUTOLOGIN P60 001 .exe
1375	1	3	\de\ccmail.de\602.s\ccmail\SAPLogin 66218 SAP_AUTOLOGIN P60 001 .exe
1378	1	3	\de\ccmail.de\602.s\ccmail\SAPLogin 66218 SAP_AUTOLOGIN P60 001 .exe
1381	1	3	\de\ccmail.de\602.s\ccmail\SAPLogin 66218 SAP_AUTOLOGIN P60 001 .exe
1384	1	3	\de\ccmail.de\602.s\ccmail\SAPLogin 66218 SAP_AUTOLOGIN P60 001 .exe
1387	1	3	\de\ccmail.de\602.s\ccmail\SAPLogin 66218 SAP_AUTOLOGIN P60 001 .exe

OBEN: Der Nachweis von Fehlbildungen in der Datei-Anfrage seitens eines SAP-R3-Clients.

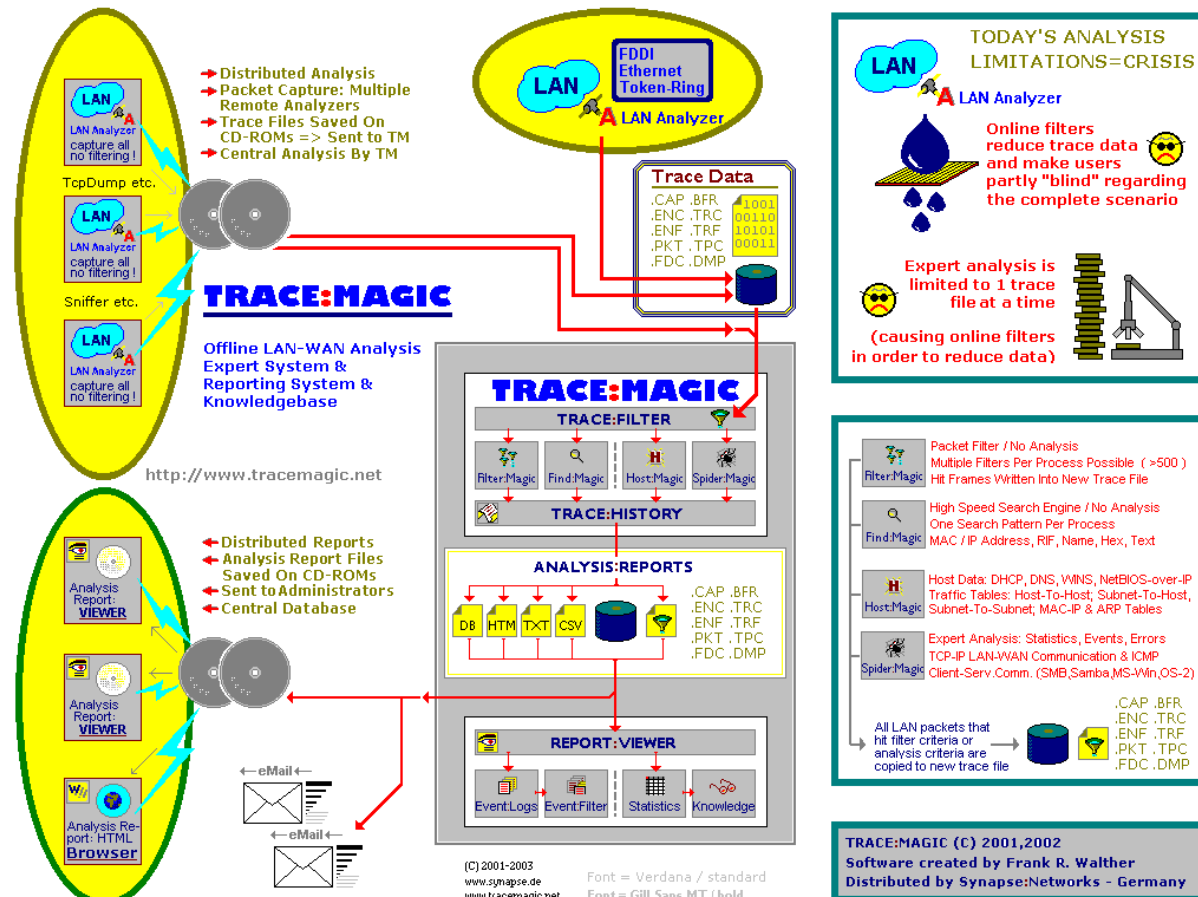
UNTEN: Nachweis von Fehlbildungen in der Datei-Anfrage eines NetInstall-Clients.

TM.HIT.FRAMES.01...001.LOG.TXT - Editor

1]	(I)	#	2013 :: 22.16.8.24	<<	192.168.2.195	::	SMB:	[0x A2]	ACCESS_FAILURE = "\\NiAgnt32.exe,Manifest"
1]	(I)	#	2014 :: 192.168.2.195	<<	22.16.8.24	::	SMB:	[0x A2]	SRVR_ERRORCODE = 0x 340000C0
1]	(I)	#	2015 :: 22.16.8.24	<<	192.168.2.195	::	SMB:	[0x 2E]	(Read And More.) "0xC00B (FileHandle
1]	(I)	#	2035 :: 22.16.8.24	<<	192.168.2.195	::	SMB:	[0x 32]	ACCESS_FAILURE = "\\NiAgnt32.exe,Local"
1]	(I)	#	2036 :: 192.168.2.195	<<	22.16.8.24	::	SMB:	[0x 32]	SRVR_ERRORCODE = 0x 340000C0
1]	(I)	#	2015 :: 22.16.8.24	<<	192.168.2.195	::	SMB:	[0x 2E]	(Read And More.) "0xC00B (FileHandle
1]	(I)	#	2037 :: 22.16.8.24	<<	192.168.2.195	::	SMB:	[0x 2E]	(Read And More.) "0xC00B (FileHandle
1]	(I)	#	2060 :: 22.16.8.24	<<	192.168.2.195	::	SMB:	[0x A2]	(NT Transaction Create And More.) "\\NiClnt32.dll"
1]	(I)	#	2061 :: 192.168.2.195	<<	22.16.8.24	::	SMB:	[0x A2]	0x00000000 SERVER_RETURN (-OK-)
1]	(I)	#	2066 :: 22.16.8.24	<<	192.168.2.195	::	SMB:	[0x 2E]	(Read And More.) "0xC008 (FileHandle
1]	(I)	#	2071 :: 22.16.8.24	<<	192.168.2.195	::	SMB:	[0x 2E]	(Read And More.) "0xC008 (FileHandle
1]	(I)	#	2071 :: 22.16.8.24	<<	192.168.2.195	::	SMB:	[0x 2E]	(Read And More.) "0xC008 (FileHandle
1]	(I)	#	2076 :: 22.16.8.24	<<	192.168.2.195	::	SMB:	[0x 2E]	(Read And More.) "0xC008 (FileHandle
1]	(I)	#	2096 :: 22.16.8.24	<<	192.168.2.195	::	SMB:	[0x 32]	ACCESS_FAILURE = "\\NiAgnt32.exe,Local"



Klassisches Packet-Decoding (im Bild oben: LANdecoder32, Triticom) wird von TraceMagic nicht geleistet; dies muss auch nicht sein, da der fürs Capturing zuständige Analyzer zugleich auch die Paket-Darstellung übernimmt. TraceMagic leistet die Massen-Verarbeitung und die Erzeugung der Ergebnis-Reports.



Datenfluss-Diagramm der TraceMagic-Analyse:

- Woher die MessDaten stammen, ist (fast) unwichtig.
- Lizenzpflichtig ist allein das Analyse-Modul (hier gezeigt mit FilterMagic, FindMagic, HostMagic, SpiderMagic).
- Lizenzfrei ist der Report-Viewer, der beliebigen Empfängern erlaubt, die Ergebnisse zu sichten und nachzubearbeiten.

Details zu den Analyse-Themen

Hinweise zum Spektrum der LAN-Analyse und Erklärungen zu einzelnen Begriffen.

Layer: Physical / Data Link / MAC

Der Physical Layer ist in heutigen Ethernet-LANs überwiegend zuverlässig. Trotzdem können Fehler auftreten. Diese Fehler sind eher selten den LAN-Adaptern zuzuordnen, sondern eher bei LAN-Switches angesiedelt.

Zu den Fehlern, die in den letzten Jahren (2000-2003) häufiger beobachtet werden konnten, gehören die folgenden:

- LAN-Switches vervielfältigen durchlaufende Unicast-Pakete: 1 Paket wird vom Switch empfangen, aber mehr als 1 Paket wird auf dem Ausgangs-Port gesendet (MAC Multiple Tx). Da dieses Ereignis irrtümlich vermutet werden kann, wenn der Mirror Port nicht korrekt gelegt wurde, ist bei der Diagnose eines solchen Szenarios äußerste Vorsicht geboten, bevor die Schlussfolgerungen endgültig gezogen werden.
- LAN-Switches verfälschen bisweilen durchlaufende Pakete, stattdessen sie aber dennoch mit einer korrekten MAC-Prüfsumme aus. Diese Fehler sind mit herkömmlichen LAN-Analysen bzw. deren Experten-Systemen nicht automatisch erkennbar, eben weil die MAC-Prüfsummen stimmen. Die Nachweise hierzu laufen über die Software "TraceMagic". Charakteristika und mögliche Ursachen sind erst durch nähere Kenntnisse der Umgebung sicher bestimmbar.
- LAN-Switches wurden schon mehrfach dabei beobachtet, die MAC-Adressen nicht korrekt zu behandeln; bisweilen wird die Absender-MAC-Adresse auf 0x000000000000 gesetzt. Die Eingrenzung auf den ursächlichen Switch ist messtechnisch ggf. mit Aufwand verbunden, da mit mehreren Messpunkten gearbeitet werden muss.
- LAN-Switches sind nach IEEE-Definition "LAN Bridges" einschließlich der Spanning-Tree-Topologie. Der Datenaustausch der Bridges/Switches läuft über BPDUs (Bridge Protocol Data Units). Falsche Konfigurationen im Spanning-Tree können katastrophale Folgen haben. Die (weitgehend) automatische Analyse dieses Umfelds gehört zum unerlässlichen Analyse-Umfang.
- LAN-Switches, die im WLAN-Bereich mit Roaming-Logik arbeiten, können ebenfalls schlimme Crashes bewirken, wenn diese Logik nicht einwandfrei arbeitet. Die zunehmende Verbreitung von WLANs verlangt hier besondere Aufmerksamkeit.

Layer: Network / IP Routing

Der Network Layer ist für sich genommen leicht zu analysieren, was die Struktur des IP-Protokoll-Headers in den Daten-Paketen anbetrifft.

Im Gegenteil jedoch ist die Analyse von WAN- bzw. Routing-Fehlern alles andere als einfach. Herkömmliche Analyse-Methoden verlassen sich auf die ggf. von Routern gesendeten ICMP-Meldungen (etwa: "Network Unreachable" oder "Fragmentation Needed").

WAN-Provider neigen jedoch dazu, die ICMP-Meldungen beim Übertritt zum Campus-LAN des Kunden heraus zu filtern (abzublenden), eben damit dort keine Hinweise auf etwaige Fehler greifbar werden, die auf den WAN-Provider zurück zu führen wären.

Nachweise auf Fehler im Provider-WAN verlangen daher spezielle Nachweis-Methoden, die zwar theoretisch nicht allzu kompliziert, praktisch aber alles andere als trivial sind.

- Router können Pakete verwerfen, wenn eine Teilstrecke zwischen zwei Routern die Paket-Größe nicht unterstützen (MTU-Problem). Router senden hierzu die Meldung "ICMP: Fragmentation Needed", wenn der Absender des IP-Pakets das Fragmentieren verboten hat (NF-Bit: "No Fragmentation"). Mit der ICMP-Meldung wird dem IP-Absender mitgeteilt, welche MTU-Größe (Maximum Transmission Unit) eben noch unterstützt wird. In der Folge sollte der IP-Absender entweder seine Paket-Größe anpassen (also vermindern) oder aber das Fragmentieren erlauben (die Aufteilung der IP-Pakete in verschiedene, kleinere Teile=Fragmente).
- Gehen einzelne Fragmente verloren, kann das ursprüngliche IP-Paket nicht wieder hergestellt werden (Reassembly). Der hierfür zuständige Router meldet in einem solchen Fall: "ICMP: Time Exceeded: Reassembly Timer Expired".
- Kommen diese ICMP-Meldungen beim IP-Absender nicht an, weil der WAN-Provider sie abblockt, entsteht ein so genanntes "Black Hole Szenario": Wie bei einem kosmischen Schwarzen Loch, das Licht anzieht, nicht aber wieder hergibt, verschlucken die WAN-Router die IP-Pakete, ohne dass davon irgend etwas sichtbar würde. Das selbe gilt, wenn die beteiligten Router erst gar keine ICMP-Meldungen abgeben.
- Bleibt die Frage: Wie ist dieses Szenario nachzuweisen, wenn die ICMP-Meldungen auf dem Campus-LAN nicht nachweisbar sind?
- Antwort: Es müssen die Paket-Größen sämtlicher IP-Hosts nachvollzogen werden, die hinter dem "Black Hole" siedeln und mit lokalen IP-Hosts sprechen. Insbesondere muss das TCP-Verhalten nachvollzogen werden, da über die Parameter "TCP Window Size" und "TCP Maximum Segment Size (MSS)" einschlägige Hinweise zwischen den IP-Teilnehmern ausgetauscht werden. Es sind längere Beobachtungs-Zeiträume nötig, um die entsprechenden Nachweise zu führen (ggf. mehrere Tage Messdauer).
- Router arbeiten für gewöhnlich redundant, um Ausfallsicherheit zu gewährleisten. Wenn Teilstrecken oder Nachbar-Router ausfallen, wird auf Ersatz-Leitungen umgeschaltet. Auch bei dieser Gelegenheit können Meldungen auftreten wie "ICMP: Network Unreachable", wenn die Umleitung auf den Ersatz-Weg nicht sofort greift.

- Sind keine ICMP-Meldungen nachweisbar, müssen indirekte Nachweise geführt werden; auch dies verlangt ggf. lange Beobachtungs-Zeiträume, wenn die Fehler nur sporadisch auftreten.
- Die Nachweise laufen wesentlich über eine Erfassung sämtlicher Paket-Verluste (IP Packet Loss, TCP Missing Sequence), Wiederholungs-Übertragungen (TCP Retransmissions) und Router-Hops (IP TTL) sowie über das Erfassen von IP-Paket-Drehern (IP Packets out of Sequence / IP Sort Error), die dann entstehen, wenn sich IP-Pakete gegenseitig im WAN überholen, wenn sie im schnellen Wechsel unterschiedliche Wege durchlaufen.
- Router im Campus-LAN sind heute als Layer-3-Switches bekannt. Sie können einerseits LAN-Frames verfälschen (zwischen Rx-Port und Tx-Port) und dies gleichzeitig verschleiern, indem verfälschte Pakete mit korrekten MAC-Prüfsummen ausgestattet werden. Dies ist kein Zauber oder Wunder, sondern zwingend, da beim IP-Routing (zwischen zwei IP-Subnetzen) der MAC-Frame immer vollständig neu aufgebaut wird.
- Herkömmliche LAN-Analyser können dieses Szenario regelmäßig nicht mit ihren Experten-Systemen erkennen, weil die Prüfsummen der verschiedenen Protokolle getrennt ausgewertet und in diesem Fall für korrekt bewertet werden.
- Die Erkennung solcher Szenarien verlangt also andere Nachweis-Methoden. Hierzu müssen die Protokoll-Ebenen verknüpft betrachtet werden, und es müssen andere Merkmale als die Prüfsummen heran gezogen werden.
- Der Nachweise dieser "IP-MAC Size Errors" verlangt längere Beobachtungs-Zeiträume, da sie erfahrungsgemäß nur sporadisch auftreten. Die Ursachen können in fehlerhafter Logik liegen, Memory-Fehler oder elektrischen Stör-Einflüssen.
- IP-Clients können Probleme erleiden (oder verursachen), wenn sie nicht korrekt über die IP-Umgebung informiert sind. Normalerweise sollten die Clients über DHCP korrekt informiert sein.
- Werden Clients über Jahre in Migrationen mitgezogen, können sich unerwartet versteckte Abweichungen von den DHCP-Profilen ergeben. Ursachen können hierzu sein: Alte LMHOSTS-Dateien; Registry-Einstellungen (über .REG, .INI, NTUSER.DAT, NTUSER.MAN etc.); konkurrierende bzw. wechselnde DHCP-Server; ICMP-basierende Konfigurationen.
- Fehler wie falsche IP-Subnetz-Masken oder etwa das stete Verweigern, den richtigen Router anzusprechen, können erhebliche Auswirkungen haben.
- Entsprechend muss LAN-Analyse darauf gerichtet sein, auch solche Umfeld-Fehler zu erkennen und zu dokumentieren.
- Das Fragmentieren von IP-Paketen (siehe oben: "Black Hole Scenario") soll eigentlich nur zwischen WAN-Routern stattfinden (sofern nötig und nicht vermeidbar).
- Gleichwohl kann IP-Fragmentation auch in LANs nachgewiesen werden - aber nicht als Folge von Inter-Routing-Connections, sondern als Folge falsch arbeitender Applikationen.
- Dieses Geschehen kann die Geschwindigkeit der Client-Server-Dialoge erheblich herunter drücken. Außerdem sind derlei Dialoge verstärkt dem Risiko von Paket-Verlusten ausgesetzt, da der Verlust nur eines Fragments den Verlust aller anderen zugehörigen Fragmente nach sich zieht und somit die entsprechende Anzahl von Retransmissions.

Diese Liste erhebt nicht den Anspruch auf Vollständigkeit. Sie gibt einen Eindruck, welche Herausforderungen die IP-Analyse an Menschen und Maschinen stellt.

Layer: Transport / TCP Data Flow Control

Der Transport Layer ist für die Herstellung, Sicherung und Beendigung der Host-zu-Host-Dialoge zuständig, wobei die Datenfluss-Steuerung (Data Flow Control) das zentrale Element darstellt.

TCP-Analyse ist höchst anspruchsvoll und wird von herkömmlichen LAN-Analysern bzw. deren Experten-Systemen in wichtigen Belangen nur unvollkommen (teilweise sogar fehlerhaft) geleistet.

- TCP Missing Sequence: Das Fehlen von TCP-Paketen, in denen Nutzdaten übertragen werden (die Teilmenge der zu übertragenden Nutzdaten wird als "TCP Sequence" bezeichnet), wird von vielen LAN-Analysern gar nicht angezeigt; lediglich die Wiederholungs-Übertragungen, TCP Retransmissions (TCP ReTx), werden angezeigt, und das noch nicht einmal vollständig. Die Charakteristik von Paket-Verlusten ist jedoch wichtig zur Erkennung spezifischer Fehler-Zustände (und nicht nur die Charakteristik der Retransmissions). (Nachweise: via TraceMagic.)
- TCP Retransmission (TCP ReTx): Die erneute Übertragung von TCP-Sequences, die entweder verloren gingen oder von der Gegenstelle nicht bestätigt wurden, gehört zu den Hauptaufgaben der TCP-Dialog-Sicherung. Hier ist es nicht nur interessant, die einzelnen Vorkommnisse zu sehen, sondern wichtig, die große Masse der Vorkommnisse zu erfassen und sowohl den jeweiligen Applikationen/Services zuzuordnen (Layer 7) wie auch den jeweiligen IP-Hosts bzw. IP-Subnets (Layer 3). Entsprechend lassen sich erhebliche Erkenntnisse gewinnen über die Zuverlässigkeit von Applikationen (identifiziert durch ihre TCP-Ports) sowie über die Charakteristik der IP-Kommunikation von und zu einzelnen IP-Hosts und IP-Subnets. (Nachweise: via TraceMagic.)
- TCP Window Size: Jeder TCP-Teilnehmer annonciert seiner Gegenstelle die Größe des verfügbaren Eingangs-Puffers; dies ist einerseits eine Einladung, die entsprechende Datenmenge zu senden, sowie andererseits ein Überlast-Schutz (Vermeidung von Buffer Overflow). Geht die annoncierte TCP Window Size langsam zurück, kann dies ein Zeichen von Überlastung des jeweiligen IP-Hosts sein. Fällt die TCP Window Size auf Null, kann dies einerseits ein Zeichen großen Desasters sein, kann aber auch Zeichen regulären Applikations-Verhaltens sein (Network Printing; Database Queries). Entsprechend ist es von zentraler Bedeutung, bei einem "WinSize-Zero"-Szenario den Vorlauf zu sehen: Springt die TCP Window Size schlagartig auf Null (vermutlich korrektes Applikations-Verhalten), oder sinkt sie langsam herab auf Null ("Sterbender-Schwan"-Szenario). Herkömmliche TCP-Analyser bieten hierzu nicht genügend Ansatz. - Der Nachweis spezifischer WAN-Fehler findet wesentlich auch über die vollständige Erfassung aller TCP-Window-Size-Angaben statt. Hierzu ist die Betrachtung langer Zeiträume notwendig, und es geht zur Zeit nur mit Offline-Analyse, da derlei Untersuchungen über PC-Ressourcen verfügen müssen, die während der Online-Analyse nicht (oder nur kaum) zur Verfügung stehen.
- TCP Maximum Segment Size (MSS): Beim Handshake zu Beginn einer TCP-Sitzung teilen sich die TCP-Teilnehmer mit, welche maximale Paket-Größe im jeweiligen LAN-Segment unterstützt wird; dies bezieht sich auf die sog. Maximum Transmission Unit (MTU) als Bezeichnung der physikalischen Nutzdaten-Menge, die von der LAN-Topologie unterstützt wird (Ethernet, Token-Ring, FDDI). - Der Nachweis spezifischer WAN-Fehler findet wesentlich auch über die vollständige

Erfassung aller TCP-Window-Size-Angaben statt. Hierzu ist die Betrachtung langer Zeiträume notwendig (siehe. TCP Window Size).

- TCP Flags (Session Commands): Sitzungs-Aufbau, Datenfluss-Steuerung und Sitzungs-Abbau werden von einigen, wenigen Befehlen bzw. Signalen gesteuert, die in Verbindung mit TCP-Sequence/Acknowledge-Number (Sende- bzw. Empfangs-Offset) sowie TCP Window Size ein umfassendes Regelungs-Werk der TCP-Kommunikation darstellen. LAN-Analyse bzw. Applikations-Analyse muss diese Vorgänge vollständig, umfassend und in ihren jeweiligen Zusammenhängen sichtbar machen und auf Fehler hin überprüfen.

Diese Liste erhebt nicht den Anspruch auf Vollständigkeit. Sie gibt einen Eindruck, welche Herausforderungen die IP-Analyse an Menschen und Maschinen stellt.

Layer: Configuration Services / File Services / Name Services / Application

Auf Layer 5-7 sind die Name Services, File Services, Configuration Services und Anwendungs-Prozesse angesiedelt. Hier siedelt sich ein reiches Panoptikum bizarrer Fehler an, deren Crash-Potenzial vor allem in unglücklichen Verkettungen und Wechselwirkungen liegt, die selten vorhersehbar sind und daher regelmäßige, vorbeugende LAN-Analyse zwingend notwendig machen.

- Configuration Services: Protokolle wie DHCP, ICMP, ADS bzw. LDAP, NDS, WINS, DNS etc. vermitteln dem Client die logische Kommunikations-Struktur, in der er sich bewegt. Schon geringe Fehler können in diesem Zusammenhang katastrophale Wirkungen haben. Nur schon ein einziger falsch gesetzter (oder unauffällig fehlender) DHCP-Parameter kann zum Resultat "das Netzwerk ist langsam" führen, wenn es die Adress- und Namens-Auflösungen lahm legt. LAN-Analyse muss daher auch Konfigurations-Analyse sein.
- Name Services: Insbesondere die NetBIOS-Dienste sind kaum in den Griff zu bekommen. Mit dem Wechsel von WinNT4 zu Win2000 bzw. WinXP hat hier eine gewisse Entspannung eingesetzt, aber immer noch sind Wirkungen im Umfeld von NetBIOS und WINS nachweisbar. Weiterhin ist die DNS-Praxis auch bei Win2000 bzw. WinXP alles andere als unbedenklich. Spätestens, wenn Datei-Anfragen als DNS-Request enden (etwa: Suche nach "JAHRESBILANZ.XLS", als ginge es um eine neue Top-Level-Domain), oder dann, wenn Script-Befehle als DNS-Request enden (etwa: Suche nach "www.ifmember.localdomain.com") ... dann stellen sich Fragen ein, die dringend geklärt werden müssen.
- File Services: Teils können Applikations-Fehler zu massiven Fehlern in den Datei-Zugriffen führen, teils können Treiber-Fehler die Datei-Zugriffe behindern bzw. in die Irre führen. Sei es, dass beim Lesen in Dateien Endlos-Schleifen gedreht werden, sei es, dass die Initialisierung eines Share-Zugriffs als Datei-Zugriff missverstanden und somit verpatzt wird - alles das kann erhebliche Störungen verursachen, bis hin zu verlängerten Antwortzeiten, Sitzungs-Abbrüchen und Datei-Verlusten.

Herkömmliche LAN-Analyser bieten in diesem Zusammenhang kaum sinnvolle Ansätze zur Analyse. Das von Synapse:Networks entwickelte Experten-System TraceMagic jedoch erlaubt weitgehende und voll-automatische Nachweise von erheblicher Reichweite und Deutungskraft.





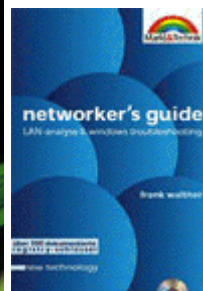
Frank R. Walther

Networker's Guide

2000:
LAN Analysis & Windows
Troubleshooting.

2003:
LAN/WAN-Analyse in
Hochleistungsnetzwerken

Verlag Markt+Technik
München



Mit der Ausgabe aus April 2000 werden die Grundlagen der LAN-Analyse vermittelt. Alle Kapitel dieser Ausgabe sind als PDF-Dateien auf der Beilage-CD-ROM der aktuellen Ausgabe enthalten.

Mit der Ausgabe aus März 2003 werden fortgeschrittene Funktionen der LAN-Analyse und vor allem der Client-Server-Analyse sowie TCP/IP-Analyse dargelegt. Eine zentrale Rolle spielen dabei die Befunde des Experten-Systems "Trace:Magic".

synapse: NETWORKS

	Synapse:Networks GmbH		Frank R. Walther Unternehmensberatung			
	Bonner Str. 10		53424 Rolandseck bei Bonn		+49.228.9138.0/.99 .phone/.fax	
	www.synapse.de		info@synapse.de			