

SYNAPSE: NETWORKS

TRACE:MAGIC



Protocol Reference

Stand: 2004-09-16

Trace:Magic

Offline LAN-WAN Analysis Expert System - Reporting System - Knowledgebase

Diese Kurz-Beschreibung gibt eine Übersicht hinsichtlich der unterstützten bzw. untersuchten LAN-WAN-Protokolle.

Es muss an dieser Stelle betont werden, dass TraceMagic nicht, wie herkömmliche LAN-Analyzer, ein vollständiges Decoding eines jeden Protokolles betreibt (oder auch nur anstrebt), sondern gezielt automatisch nach Fehler-Szenarien sucht.

Protokoll-Parameter, die im Sinne automatischer Analyse von MessDaten keinen Erkenntnis-Gewinn versprechen, werden übergangen.

Statt dessen wird wesentlich Wert gelegt auf die Analyse von Ablauf-Szenarien und Vergleichen verschiedener Vorgänge über die Zeit hinweg.

Hierdurch werden Fehler nachgewiesen bzw. sichtbar gemacht, die zum Teil bis dahin noch gar nicht hatten nachgewiesen werden können.

Die Stärke von TraceMagic besteht wesentlich darin, nicht allein jedes LAN-Paket für sich zu betrachten, sondern - wie gesagt - massiv Vergleiche anzustellen - etwa wie folgt:

- Wie viele Router-Hops ist das aktuelle IP-Paket eines bestimmten Absenders hinter sich - und wie viele Router-Hops waren es in der Vergangenheit (bezogen auf den selben Absender) (bis hierhin: reine Betrachtung von Layer_3 bzw. dem IP-TTL Parameter), und welche Schlussfolgerungen lassen sich daraus ziehen, wenn bei einem Wechsel des IP-TTL-Wertes auch ein Wechsel des sendenden Router-Interfaces erfolgt (was Layer_1 bzw. Layer_2 mit der MAC-Adresse des jeweiligen Routers betrifft)?
- Welche Meldungen "ICMP: Port Unavailable" kommen jeweils aus einem IP-Subnetz, das sich von dem IP-Subnetz des ICMP-Empfängers unterscheidet (bis hierhin: Layer_3) - verbunden mit der Bedingung, dass der beim ICMP-Absender nicht erreichbare TCP/UDP Port (jetzt: Layer_4) über einem lokalen IP-Subnet-Multicast angesprochen wurde (wiederum Layer_3), was nicht hätte sein dürfen angesichts des Umstandes, das Absender und Empfänger in verschiedenen IP-Subnetzen liegen, die also nicht über lokale IP-Multicasts erreichbar sind? Welche Bedeutung hat das wiederum (a) hinsichtlich der Möglichkeit, dass möglicherweise die Remote-Router fälschlicherweise LAN-Broadcasts über WAN-Leitungen weiter leiten - was ein verbotenes/unerwünschtes Remote-Bridging wäre - , (Layer_2) sowie (b) hinsichtlich der Möglichkeit, dass IP-Helper falsch konfiguriert sein könnten (Layer_3)? Und welche Bedeutung hat es in diesem Zusammenhang, wenn bzw. dass eine bestimmte Applikation via TCP/UDP-Port durch Multicast angesprochen bzw. gesucht wird (Layer_4)?
- Was geschieht, wenn ein Client Server-Scripts lädt und abarbeitet (.BAT,.CMD,.REG etc) und hierbei Fehler macht bzw. erleidet, etwa in der Form, dass ein Script-Befehl zu einem Zugriff des Clients auf einen Server führt, der Server diesen Zugriff aber ablehnt? Kann die Server-Ablehnung ("Access Denied / Access Failure") mit dem Script und der zutreffenden Script-Zeile automatisch in Verbindung gebracht werden?

Klassische LAN-Analyser können Szenarien derartiger Komplexität nicht annähernd erfassen und analysieren. TraceMagic kann dies, und TraceMagic wurde eigens für solche Szenarien entwickelt.

Die Verknüpfungen zwischen verschiedensten OSI-Layern bzw. Protokoll-Schichten nehmen bisweilen einen solchen Umfang ein, dass selbst erfahrensten Netzwerk-Administratoren nicht mehr möglich wäre, allen Verbindungen und jedem Verdacht in manueller Arbeit nachzugehen - eben deswegen, weil die in Frage kommenden Quer-Beziehungen kaum noch nachvollziehbar sind - und schon gar nicht bei Millionen und Abermillionen von LAN-Packets.

Eine solche Leistungsfähigkeit setzt andere Arbeitsweisen voraus, als sie von klassischen Protocol-Decodern bekannt sind.

Mit diesem Verständnis gelesen, ist die nachfolgende Protokoll-Referenz allenfalls ein erster Ansatz zum Nachweis der TraceMagic-Fähigkeiten.

OSI Layer	Protocol	Simple Decoding => Event Log	Intelligent Analysis => Event Log	Statistics => Tables / Database
Layer 1+2a	Ethernet	[x]	[x]	[x]
Layer 1+2a	Token-Ring	[x]	--	--
Layer 1+2a	FDDI	[x]	--	--
Layer 2b	BPDU / Spanning Tree	[x]	[x]	[x]
Layer 2b	GVRP (GARP VLAN Registration Protocol)	[x]	--	--
Layer 2b	LLC (Logical Link Control) I+II	[x]	[x]	[x]
Layer 2b+7	SNA over LLC / Session Control	[x]	[x]	[x]
Layer 2b	SNAP / Cisco Discovery Protocol	[x]	--	--
Layer 2b	SNAP / Lucent WLAN	[x]	--	--
Layer 2+3	ARP / R-ARP	[x]	[x]	--
Layer 3	IP	[x]	[x]	[x]
Layer 3	IPX	[x]	--	--
Layer 3	IP-RIP (Routing Information Protocol)	[x]	--	--
Layer 3	OSPF (Open Shortest Path First)	[x]	--	--
Layer 3	VRRP (Virtual Router Redundancy Protocol)	[x]	--	--
Layer 2b	Cisco Discovery Protocol	[x]	--	--
Layer 3	Cisco E-IGRP	[x]	--	--
Layer 3	Cisco HSRP	[x]	--	--
Layer 3-7	ICMP	[x]	[x]	[x]
Layer 3-7	DHCP	[x]	[x]	[x]
Layer 4	UDP	[x]	--	[x]
Layer 4	TCP	[x]	[x]	[x]
Layer 5-7	UDP(53) - DNS	[x]	[x]	[x]
Layer 5-7	UDP(137) - WINS	[x]	[x]	[x]
Layer 5-7	UDP(138) - NetBIOS	[x]	[x]	[x]
Layer 7	HTTP (HyperText Transfer Protocol)	[x]	[x]	[x]
Layer 7	NCP (NetWare Core Protocol)	[x]	[x]	[x]
Layer 7	SMB (Server Message Block)	[x]	[x]	[x]
Layer 7	SMB - MAILSLLOT / BROWSE	[x]	[x]	[x]
Layer 7	ACCESS FAILURE (HTTP,NCP,SMB)	[x]	[x]	[x]
Layer 7	FILE RECONSTRUCTION (NCP,SMB)	[x]	[x]	[x]
Layer 7	KERBEROS	[x]	--	--
Layer 7	SNMP	[x]	[x]	--
Layer 7	VoIP - RTP / RTCP	[x]	[x]	--
Layer 7	Unix: FTP	[x]	--	--
Layer 7	Unix: TELNET	[x]	--	--
Layer 7	Unix: SMTP	[x]	--	--
Layer 7	Unix: POP3	[x]	--	--
Layer 7	Oracle TNS / Ports 1521 etc. (Listener)	[x]	--	--
Layer 7	ADS - Advanced Database Service	[x]	--	--
Layer 7	ProSytec Client/Server Exchange	[x]	--	--

Diskussion: Was bedeutet diese Protokoll-Referenz?

Es fällt auf, dass das Experten-System sich intensiv mit TCP und IP beschäftigt, dagegen (scheinbar?, offenkundig?) weniger tief mit Router-Exchange-Protokollen (RIP, OSPF, E-IGRP etc).

Es fällt auf, dass die Protokoll-Referenz neben Protokollen auch Analyse-Funktionen bzw. Fehler-Szenarien aufführt wie "Access Failure" oder "rc.files" bzw. "Reconstructed Files".

Was hat das zu bedeuten?

Routing-Fehler:

TraceMagic decodiert diese Protokolle zwar, führt aber - von Ausnahmen abgesehen - keine weiteren Untersuchungen durch.

Warum? Wären die Router Exchange Protocols denn nicht wichtig? Die Begründung lautet:

Im lokalen Campus-LAN spielen diese Protokolle kaum eine Rolle (mit Ausnahme von HSRP oder VRRP); vielmehr haben sie ihr Wirkungsfeld im WAN bzw. in Provider-Transit-Netzen. Die dortigen E-IGRP-, OSPF- und RIP-Pakete bekommt der LAN-Analyser bei der Aufzeichnung der MessDaten gar nicht zu sehen.

Was nützt also, umgekehrt gefragt, das beste Protocol Decoding, wenn die Pakete dieser Protokolle gar nicht am MessPunkt vorbei kommen?

Aus diesem Grunde legt TraceMagic großen Wert darauf, die Wirkungen etwaiger Routing-Fehler nachzuweisen - und das mit Methoden, die bislang weltweit einmalig und höchst effizient sind. Es ist wichtiger, etwaige Fehler-Szenarien nachzuweisen. Wer immer Provider-WANs nutzt, wird schnell verstehen, welchen Wert die TraceMagic-Reports haben.

Reconstructed Files:

Eine weitere Schwierigkeit, nur in Protokoll-Referenzen zu denken, ergibt sich bei der "rc.files"-Funktion - der Fähigkeit von TraceMagic, Dateien zu rekonstruieren, die Clients von Servern lesen (z.B. .BAT, .CMD, .REG, .VBS).

Die "rc.files"-Funktion unterteilt sich in die beiden Unter-Funktionen "file reconstruction" und "script follow-up":

Einerseits werden Script-Files dokumentarisch wieder hergestellt, um sie dem LAN-Analysten sichtbar zu machen; so können Batch-Files etc im Klartext gesichtet und die Client-Zugriffe nachvollzogen werden.

Andererseits können weitreichend die nachfolgenden Client-Aktionen auf einzelne Script-Befehle zurück geführt werden. Dies spielt insbesondere dann eine wesentliche Rolle, wenn der Client in der Abarbeitung von Script-Befehlen entweder selber Fehler begeht oder Fehler erleidet.

Oder, anders herum betrachtet: Ausgehend von Client-Server-Fehlzugriffen, kann TraceMagic prüfen und ggf. automatisch feststellen, ob bzw. dass die Aktion auf ein bestimmtes Script und auf eine bestimmte Zeile darin zurück zu führen ist. Diese Fähigkeiten sind bisher weltweit einmalig und erlauben Einblicke, die der LAN-Analyst bis dato nicht hatte.

TraceMagic ermöglicht vernetztes bzw. ganzheitliches Denken, verlangt es aber auch.

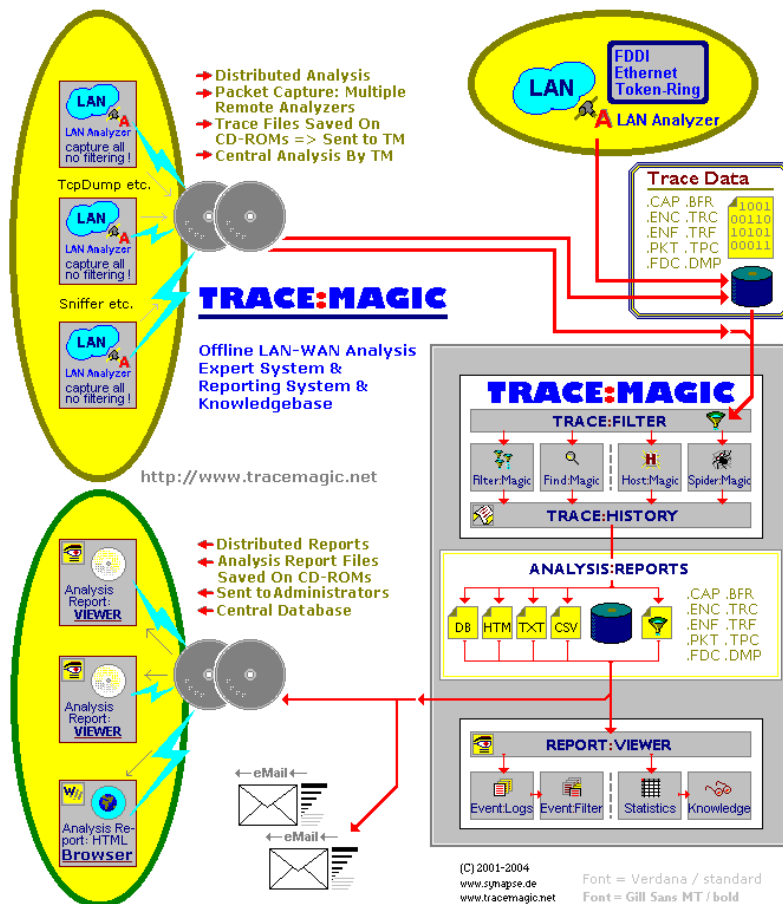
Waren noch zu "alten Novell-Zeiten" die Verhältnisse übersichtlich, da sich die Clients nur einzelnen Servern gegenüber per Login zu nähern hatten, so haben wir es heute mit komplexen Domain-Strukturen zu tun, deren Verständnis Zeit und Übersicht erfordern.

Einzelnes *Packet Decoding* kann dem nicht gerecht werden. Entsprechend "denkt" TraceMagic nicht in einzelnen LAN-Paketen, sondern in Szenarien, zeitlichen Abläufen und wechselseitigen Abhängigkeiten zwischen Client und Server.

TraceMagic im Internet:

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

Synapse:Networks GmbH
 Bonner Str. 10
 53424 Rolandseck bei Bonn
 +49. 2228. 9138.0 - phone
 +49. 2228. 9138.99 - fax
 +49. 170. 7334608 - mobile
 +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, NCP, HTTP, VoIP, etc.)
 Access Failure, File Reconstruction "rc.files"

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

.CAP, .BFR, .ENC, .TRC, .ENF, .TRF, .PKT, .TPC, .FDC, .DMP

TRACE:MAGIC (C) 2001-2004
 Software created by Frank R. Walther
 Distributed by Synapse:Networks - Germany