

IT Netzwerkdiagnose



IT Netzwerkdiagnose

Networkers ist eines der in Deutschland führenden Unternehmen für die Planung, den Aufbau und den Betrieb von sicheren und leistungsfähigen Applikations- und Netzwerkinfrastrukturen.

Unternehmen und Organisationen bieten wir ein breites Spektrum an Services - zuverlässig, kompetent und herstellernerneutral.

IT-Netzwerkfehler

IT-Netzwerke stellen zweifelsohne eine der wesentlichen Triebfedern für das Informationszeitalter dar. In Unternehmen und Organisationen bilden sie die grundlegende Infrastruktur zur Ausführung von Arbeitstätigkeiten. Beeinträchtigungen innerhalb dieser Infrastrukturen bewirken meist mehr oder weniger hohe wirtschaftliche Schäden. Vor allem deshalb ist die Sicherstellung eines reibungslosen Netzwerkbetriebs von hoher Bedeutung.

Ausfälle und Verzögerungen lassen sich aber insbesondere in komplexeren IT-Infrastrukturen nicht immer ohne weiteres vermeiden. Und obwohl sie Nerven und in der Regel auch bares Geld kosten, gehören sie in vielen Unternehmen zum Alltag. Zweifelhafte Highlights sind etwa:

- nicht enden wollende Login-Prozesse
- plötzlich verschwundene Netzlaufwerke, Drucker oder Profile
- Datenverarbeitungen im Schneckentempo
- minutenlanges Warten auf Suchergebnisse
- Fehlermeldungen verschiedenster Art
- Systemabstürze
- und so weiter

Die Fehlerursachen stecken vielfach tief im Detail, so dass sie häufig nicht auf Anhieb ersichtlich sind. Sie können auf allen Netzwerkebenen und oft auch in Kombinationen auftreten, typischerweise in einem oder in mehreren der folgende Bereiche:

- Hardware-Defekte
- Konfigurationsfehler bei Treibern, Betriebssystemen oder Applikationen
- Fehler in der Adress- und Namensauflösung (DNS, DHCP, WINS)
- inkonsistente Netzwerkvermittlung bzw. im Routing
- und so weiter

Ziel dieser Broschüre ist es, einen allgemeinverständlichen Überblick über das Aufspüren, Analysieren und Lösen von Netzwerkproblemen zu geben. Im Mittelpunkt stehen dabei personelle und methodische sowie auch technische Aspekte rund um die Netzwerkdiagnose (oder neudeutsch: rund um das Troubleshooting).

OSI-Referenzmodell	TCP/IP Modell
Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data Link Layer	Network Layer
Physical Layer	

IT Netzwerkdiagnose

IT-Netzwerkanalysen

Das Maß tolerierbarer Netzwerkprobleme in Unternehmen wird häufig durch eine Kombination von Leidensfähigkeiten der IT-Anwender und den zur Verfügung stehenden Ressourcen, die die Probleme beseitigen können, bestimmt. Nähert man sich dem kritischen Punkt oder überschreitet ihn gar, stehen Netzwerkverantwortliche mit dem Rücken zur Wand. Dann erwartet man von ihnen, dass sie das bzw. die Problem(e) beheben - und zwar rasch!

In solchen Situationen wird dann üblicher Weise zunächst die *Hitliste* der bekannten Fehlerquellen abgearbeitet. Manchmal aber erfolglos, so dass daraufhin meist intuitiv *Plan B* zum Einsatz kommt: Die Suche nach der berühmten Stecknadel im Heuhaufen. Und zwar mit allen zur Verfügung stehenden Mitteln.

Einerseits verständlich, da der auf den Schultern lastende Druck mit zunehmender Störungsdauer zunimmt - andererseits eine wirtschaftlich fragwürdige Entscheidung. Denn das Ziehen der korrekten Rückschlüsse von vorliegenden Symptomen auf die eigentlichen Fehlerursachen ist alles andere als trivial. Im Gegenteil: Die Diagnose ist kompliziert und partiell vielfältig. Daher ist die Wahrscheinlichkeit, die Probleme innerhalb eines vertretbaren Zeitrahmens zu finden - wenn nicht gerade ein erfahrener Troubleshooter am Werk ist - relativ gering.

Beispiel: Fehlersuche und Netzwerkmesung

"In einem Unternehmen stürzte mehrmals täglich ein Server ab. Um den Fehler zu beseitigen, tauschten die Administratoren nach und nach fast alle infrage kommenden Bauteile aus; doch der Server stürzte nach wie vor ab. Messungen an einem Client im Netzwerk ergaben, dass dort deformierte Datenpakete empfangen wurden, die vom Server ausgingen. Daraufhin wurde selbst der LAN-Adapter des Servers getauscht, doch das Problem war nach wie vor existent.

Eine weitere Messung und die anschließende Analyse der aufgezeichneten Informationen durch einen Spezialisten auf diesem Gebiet lieferte letztendlich den Grund für die Serverausfälle: einer der Switches zerstörte Datenpakete, die daraufhin unleserlich waren und den Server regelmäßig zum Absturz brachten."

Dieses Beispiel verdeutlicht, dass ad hoc durchgeführte Try-and-Error-Methoden einerseits sehr zeit- und kostenintensiv sein können und andererseits nicht immer unmittelbar zum Erfolg führen. Das eigentliche Problem liegt nicht selten an einer ganz anderen Stelle.

Quelle: Frank R. Walther: Networker's Guide - LAN Analysis & Windows Troubleshooting

Der ideale Troubleshooter

Der ideale Troubleshooter ist ein Experte. Einer, der sich explizit auf die Netzwerktechnik spezialisiert hat und über profundes Fachwissen insbesondere in den Bereichen Topologien, Protokolle, Dienste und Anwendungen verfügt. Einer, der Netzwerkdiensttools und deren Funktionen nicht nur kennt, sondern deren Anwendungen auch aus dem Effeff beherrscht, der jahrelange Erfahrung vorweisen kann und zudem eine gute Portion analytischen Sachverstand mitbringt. Ein Kenner und Köhner, der Auffälligkeiten, Wirkungen und Abhängigkeiten in Netzwerken "sieht" - auch innerhalb komplexer IT-Infrastrukturen. Einer mit besonderer Auffassungsgabe und dem Talent eines Spürhundes. Einer, der Fehler nicht nur identifiziert, sondern auch gleich zweckmäßige Problemlösungen parat hat und zudem stets besonnen agiert und jederzeit die Übersicht behält - auch in hektischen Situationen.

Aus wirtschaftlicher Sicht ist es sicherlich nicht für jedes Unternehmen ratsam, einen solchen Experten dauerhaft zu beschäftigen. Fünf wesentliche Gründe sprechen jedoch dafür, rechtzeitig einen externen Spezialisten zu Rate zu ziehen, sofern Netzwerkprobleme vorherrschen und man über keinen Experten in den eigenen Reihen verfügt. Denn im Regelfall

- entdeckt der Spezialist vorherrschende Netzwerkanomalien schneller,
- diagnostiziert der Spezialist zuverlässiger, ob es sich bei entdeckten Anomalien um tatsächliche Fehlerursachen oder nur um Wirkungen einer oder mehrerer anderer Ursachen handelt,
- lokalisiert der Spezialist die eigentliche Fehlerursache schneller,
- deckt der Spezialist Optimierungspotenziale auf,
- erkennt der Spezialist, ob sich bereits weitere Probleme/Engpässe anbahnen.

Dies erreicht er einerseits durch die eingangs erwähnten Qualifikationen, andererseits aber auch durch sein konsequent methodisches Vorgehen, welches wir im nächsten Kapitel skizzieren.

IT Netzwerkdiagnose

Eckpunkte des methodischen Troubleshooting

Obwohl die Aufgabenstellung an einen Troubleshooter i.d.R. immer dieselbe ist - nämlich Netzwerkfehler schnellstens zu finden und abzustellen - besitzt jeder Netzwerkanalyst seine eigene Philosophie, wie er die "Nadel im Heuhaufen" am effizientesten zu finden gedenkt.

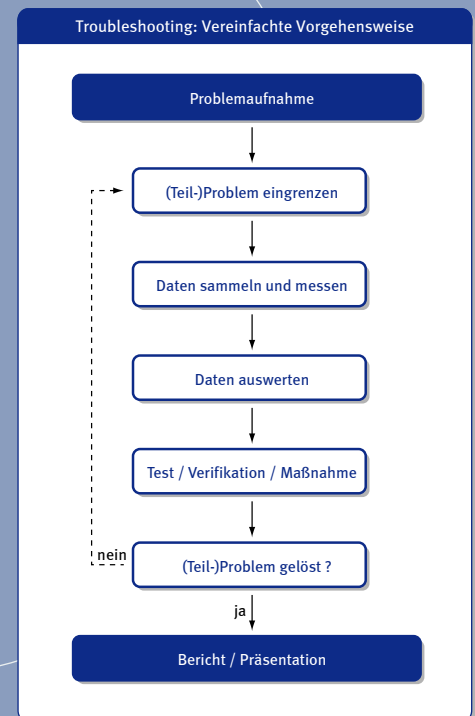
Auffällig ist jedoch, dass sich die Vorgehensweisen professionell agierender Troubleshooter in etwa angleichen, wenn ad hoc keine konkreten Verdachtsmomente über die jeweiligen Fehlerursachen vorliegen. Diese Methodik, die auf einer sukzessiven Eingrenzung potentiell vorhandener Fehlerherde beruht, wollen wir im Verlauf kurz beleuchten. Es sei allerdings bemerkt, dass sie den Anspruch auf eine Allgemeingültigkeit nicht erheben kann - dafür ist das Thema zu komplex. Vielmehr soll die Struktur eines praxisbewährten Troubleshooting allgemeinverständlich verdeutlicht werden.

Zum Kern der Methodik: Externe Troubleshooter stehen bei Ihrem Eintreffen beim Auftraggeber meist vor einem mehr oder weniger großen Scherbenhaufen. Konkrete Informationen über vorherrschende Problemsymptome sowie über Topologien, Komponenten, Systeme, Applikationen, etc. sind Ihnen in der Regel unbekannt. Sie müssen sich also notwendiger Weise zunächst ein grobes Bild erarbeiten - ähnlich wie Ärzte sich Informationen über Patientenzustände verschaffen müssen, bevor sie diagnostizieren und behandeln können.

So stellt der Troubleshooter gezielte Fragen zu z.B. Symptomen, Normalzuständen und Wunschzuständen und sieht z.B. vorhandene Dokumentationen und Topologiedaten (vorerst grob) ein, um sich mit den Gegebenheiten vertraut zu machen. Sofern es die Zeit und die Reproduzierbarkeit existenter Fehler erlauben, bieten sich darüber hinaus auch (kurze) Problemdemonstrationen an. Sie verbessern Quantität und Qualität der Datenerhebung erheblich und tragen daher auch meist zu einer schnelleren Problemlösung bei.

Im Rahmen der Vorerhebung stimmt der Troubleshooter last but not least wichtige organisatorische Eckpunkte ab. Im Wesentlichen geht es dabei

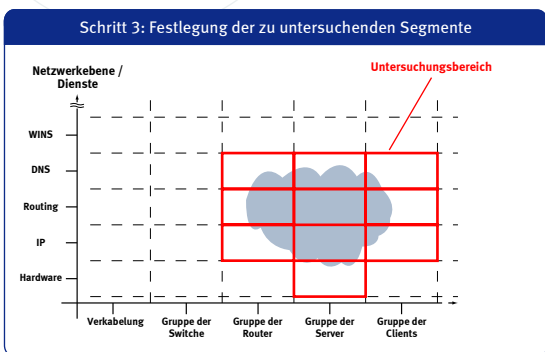
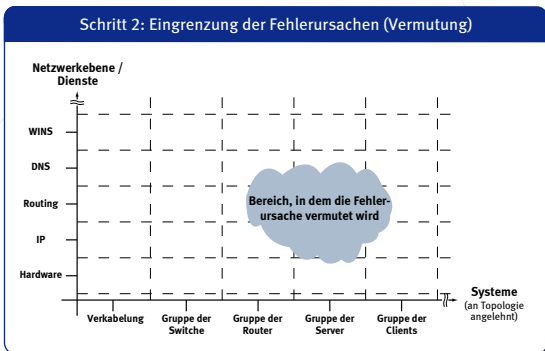
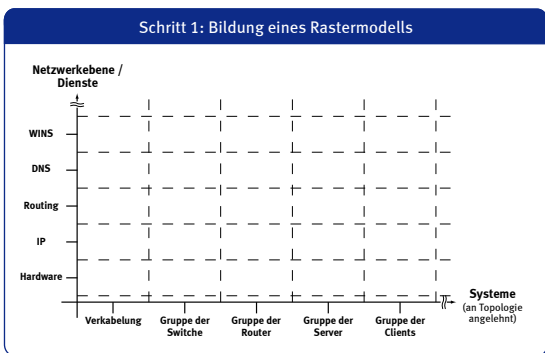
- um das Festlegen von Prioritäten,
- um das Bestimmen von Entscheidungsträgern und -befugnissen,
- um das Setzen von Terminen,
- um das Beachten von Besonderheiten,
- etc.



Sind auch diese Informationen erhoben, ist damit der oftmals als lästig und zäh wirkende, aber für den weiteren Verlauf unumgängliche Block der Bestandsaufnahme abgeschlossen - das Doing kann beginnen. Doch wer meint, dass der Troubleshooter nun die Ärmel hochkrempelt und sichtbaren Aktionismus an den Tag legt, irrt! Zumindest der erste Teil des Doings besteht nahezu ausschließlich aus Kopfarbeit.

Im Rahmen derer führt sich der Troubleshooter das zu untersuchende Netzwerk zunächst einmal bildlich als ein Koordinatensystem vor Augen. Während er auf der einen Achse das Netzwerk in *Layern* (in Anlehnung an die Ebenen des OSI-Referenzmodells) segmentiert, fasst er auf der anderen Achse die vorhandenen Netzwerkkomponenten, wie z.B. Kabel, Router, Clients, Server, etc., in Gruppen zusammen. Warum das Ganze? Nun, auch wenn es den Anschein haben mag, als läge dieses Vorgehen weit ab jeglichen realen Nutzens, so hat dieses Konstrukt den entscheidenden Vorteil, dass sich der Troubleshooter ein Raster - wenn auch *nur* ein gedankliches - mit Orientierungspunkten bilden kann. Und dieses Raster ist notwendig, um die Ursachen von Netzwerkfehlern - wie bereits oben kurz angerissen - auf Basis einer sukzessiven Eingrenzung auf potentiell vorhandene Fehlerherde vornehmen zu können.

Aber wie macht er das nun? Also: Er hat das mit den Netzeigenschaften gefüllte Koordinatensystem bildlich vor Augen und unterteilt dieses, so dass unterschiedliche Quadranten entstehen (siehe Grafik *Schritt 1*). Ein Quadrant stellt dabei jeweils eine Kombination einer Netzwerkebene und einer bestimmten Gruppe von Netzwerkkomponente dar. Auf Basis seiner bereits gewonnenen Informationen, aber auch auf Basis seiner Erfahrung, seines Know-hows und seines analytischen Potenzials kann er nun die vorherrschenden Anomalien einem oder einigen wenigen Quadranten zuordnen (siehe Grafik *Schritt 2*). So unterteilt er das Modell wiederum in zwei Bereiche: In die Summe der Quadranten, in denen die Fehlerursachen rein logisch stecken können und rein logisch eben nicht stecken können. Durch diese Vorgehensweise bestimmt der Troubleshooter sein *Zielgebiet* für die nachfolgenden Untersuchungen (siehe Grafik *Schritt 3*). Welche Untersuchungen idealtypischer Weise wie vorgenommen werden, schildern wir im nächsten Kapitel.



Die Netzwerküberprüfung

Ziel der Netzwerküberprüfung ist es, Fehlerursachen in den Bereichen aktive Komponenten, Topologie, Grundlagenprotokolle sowie -dienste innerhalb von LAN- und WAN-Verbindungen aufzudecken. Oder anders formuliert: Der Troubleshooter führt Netzwerküberprüfungen dann durch, wenn er Fehlerursachen im unteren Drittel des fiktiven Koordinatensystems (siehe Seite 7) vermutet. Dies führt der Troubleshooter aus, indem er

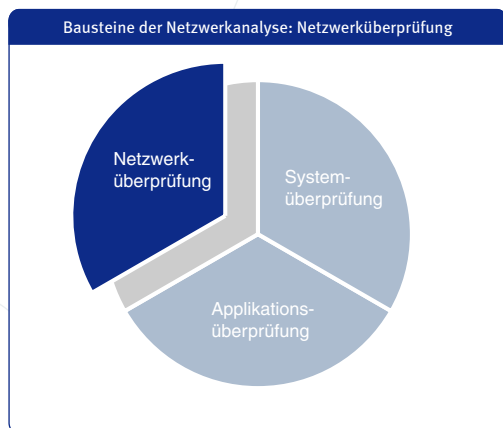
- ein oder mehrere geeignete Werkzeuge - Sniffer genannt - in das Netzwerk integriert, die in der Lage sind, Datenverkehr mitschneiden zu können. Unter anderem auch Daten der Grundlagenprotokolle IP, TCP, ARP, UDP, BOOTP, etc. sowie der Grundlagendienste DHCP, DNS, LDAP,

WINS, etc., die hier exemplarisch genannt seien. Die anschließende Auswertung des *gesniffen* Datenverkehrs mit gesonderten Analyzer-Tools kann dann Hinweise auf Fehlerursachen wie z. B. Broadcast-Stürme, nicht erreichbare Zielhosts, falsches Routing, mehrfach gesendete Datenpakete, etc. liefern. Obwohl es sich möglicher Weise recht simpel anhören mag, ist diese Analyse alles andere als einfach durchführbar. Allein schon die sinnvolle Auswahl und Bedienung der Tools stellt selbst gestandene Netzwerkprofis häufig vor große Probleme. Ganz zu

schweigen vom Finden *richtiger* Messpunkte und Messdauern. Zudem ist häufig festzustellen, dass Filterfunktionen falsch angewendet werden. Filter ermöglichen die Ansicht und Auswertung bestimmter Datenbereiche, was prinzipiell sehr sinnvoll ist. Wenn aber ausgerechnet die Datenbereiche ausgeklammert werden, in denen Fehlerursachen verborgen liegen, können selbst die besten Analyse-tools keine entscheidende Unterstützung bieten.

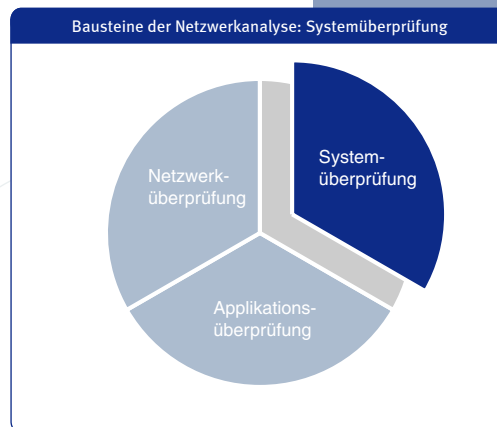
- vorhandene Netzwerpläne und Dokumentationen dahin gehend studiert, logischen Fehlern innerhalb der Netzwerktopologie (Bus, Stern, Ring) auf die Schliche zu kommen.
- zudem Ortsbegehungen durchführt. Diese sind insbesondere sinnvoll, wenn die ihm bereitgestellten Unterlagen nicht auf allerneuestem Stand sind oder aber Grund zur Annahme besteht, dass physikalische Fehler (die berühmten losen Stecker) vorliegen.

In der Praxis wird der professionelle Troubleshooter den oder die Fehler auf diese Weise sicherlich gefunden haben. Gesetzt den Fall aber, dass er die Fehlerursachen nicht lokalisieren konnte, fährt er mit der Systemüberprüfung und/oder Applikationsüberprüfung fort.



Die Systemüberprüfung

Innerhalb dieser Überprüfung werden die angeschlossenen Systeme (z. B. Clients und Server) analysiert. Oder, um noch einmal auf das Koordinatensystem (siehe Seite 7) zurückzukommen: Der Troubleshooter arbeitet sich waagrecht eine Ebene nach oben und untersucht nun in Anlehnung an die Ebenen des OSI-Referenzmodells das mittlere Drittel, den Bereich der Systeme. Dabei konzentriert sich der Troubleshooter im Wesentlichen auf die Inspektion der Installationen und Konfigurationen von Betriebssystemen (Microsoft Windows, Linux, Solaris, MacOS, etc.) sowie auf die fehlerfreie Einbindung von Gerätetreibern, Netzwerkdiensten und -protokollen auf Client-/ Serverebene.

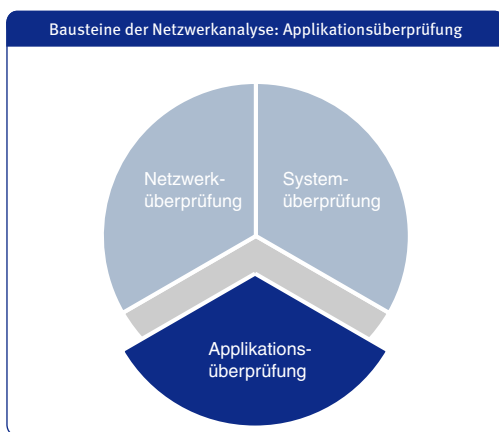


Dazu greift er erneut auf die mitgeschnittenen Daten der Netzwerküberprüfung zurück. Nur untersucht er diese hier mit einem anderen Fokus. Nämlich dahingehend, ob IP-Pakete einzelner Systeme korrekt gesendet, empfangen bzw. verfälscht oder gar verworfen werden. Das geschieht durch Einsicht in z.B. ICMP-Daten oder in IP-Daten einzelner Adressen, auf die er zuvor Filter setzt.

Wie auch bei der Netzwerküberprüfung darf man davon ausgehen, dass der professionelle Troubleshooter die gesuchten Fehlerursachen aufdeckt. Gesetzt den Fall aber, dass er die Fehlerursachen nicht lokalisieren konnte, so nimmt er nun anschließend die Applikationsüberprüfung vor.

Die Applikationsüberprüfung

Bei der Applikationsüberprüfung arbeitet sich der Troubleshooter in dem Koordinatensystem (siehe Seite 7) in die oberste waagerechte Ebene vor und untersucht in Anlehnung an die Ebenen des OSI-Referenzmodells nun den Bereich der Applikationen.



Die Applikationsüberprüfung zielt darauf ab, Kommunikationsprobleme zu lokalisieren, die von IT-Anwendungen verursacht werden. Zu diesen Anwendungen zählen beispielsweise Web-, Print-, Mail-, File-, Proxy- oder Authentisierungsserver sowie auch Firewalls oder Server innerhalb von Thin-Client-Strukturen. Applikationsfehler äußern sich häufig in Form von Anfragen an nicht vorhandene Hosts, in Form von Zugriffsversuchen auf nicht vorhandene IP-

Adressen oder aber in Form von fehlenden Zugriffsrechten auf bestimmte Dateien und/oder andere Ressourcen.

Zur Analyse bedient sich der Troubleshooter wieder des nunmehr bekannten Datenmitschnittes und überprüft diesen beispielsweise dahingehend, ob Anfragen von Clients oder anderen Systemen an Applikationen einerseits empfangen und andererseits korrekt beantwortet werden. Entdeckte Anomalien lassen dann auf fehlerhafte Implementierungen und/oder Konfigurationen von Applikationen schließen. In eher seltenen Fällen aber auch darauf, dass die eine oder andere Applikation eine unzureichende Leistungsfähigkeit besitzt und der Anzahl von Client-Anfragen nicht gewachsen ist.

Spätestens mit der Applikationsüberprüfung schließt der Troubleshooter den Bereich der Netzwerkanalyse ab und kann sich nun der Fehlerbehebung zuwenden - natürlich nur, sofern noch nicht geschehen.

Damit wollen wir den Bereich der Netzwerkanalysen verlassen. Einen wesentlichen Punkt können wir an dieser Stelle festhalten: Für zuverlässige und gute Ergebnisse im Rahmen Netzwerkanalysen muss die Kombination aus "Mensch und Technik" stimmen. Während wir hier und dort bereits die wichtigsten personellen Faktoren kennen gelernt haben, kommen wir im folgenden Kapitel zur Technik. Konkret zu der Vorstellung einiger praxisbewährter Werkzeuge und Tools.

IT Netzwerkdiagnose

Netzwerkmessungen: Tools und Werkzeuge

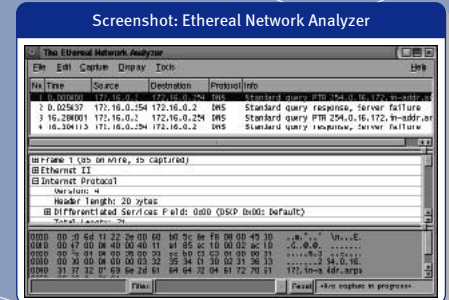
Zum Aufspüren von Netzwerkproblemen leisten so genannte LAN-Sniffer wertvolle Unterstützung. Nur durch deren Einsatz kann man die vollständigen Rohdaten erheben, die für die späteren Analysen benötigt werden. Obwohl es LAN-Sniffer als Freeware-Tools, als kommerzielle Software-Lösungen und auch als leistungsstarke Hardware-Versionen gibt, ist das prinzipielle Vorgehen bei der Fehlersuche mit diesen Werkzeugen ähnlich.

- Eine Capture Engine erfasst die über eine Netzwerkkarte übertragenen Datenpakete.
- Die Daten werden als Trace-Dateien abgespeichert.
- Mit einer gesonderten Analyzer-Software können die Trace-Daten dann anschließend z. B. Protokollanalysen und weiteren Untersuchungen unterzogen werden.

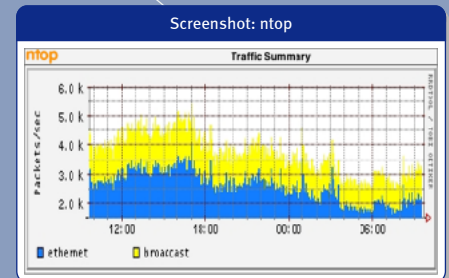
Über die Erzielung aussagekräftiger (Fehler-)Ergebnisse entscheiden vor allem die Qualität und die korrekte Bedienung der Sniffer. So ist die richtige topologische Platzierung des Sniffers im Netzwerk elementar, um sicher gehen zu können, dass tatsächlich auch der Datenverkehr *vorbeikommt*, der Aufschluss über die Fehlerursachen geben kann - insbesondere wichtig bei Mehr-Punkt-Messungen! Nicht minder elementar ist die Bandbreite an Daten, die der Sniffer mitschneiden kann, so dass tatsächlich auch die Verkehrsarten (Protokolle) berücksichtigt werden, die Aufschluss über die Fehlerursachen geben können. Auch hat die Dauer des Netzwerkmittschnittes Einfluss auf die Datenqualität. Sind Fehler reproduzierbar und/oder zeitlich eingrenzbar, reichen oftmals Kurzzeitmessungen. In manchen Fällen kann es jedoch erforderlich sein, den gesamten Datenverkehr einen Tag lang oder auch noch länger mitzusniffen, um eine zuverlässige und gültige Datenbasis für die anschließende Analyse zu erhalten.

Um die Messdaten kontinuierlich und vollständig auf Datenträgern speichern zu können, werden einerseits leistungsfähige Standard-Netzwerkkarten mit einer Capture Engine benötigt sowie andererseits auch Festplatten mit hoher Speicherkapazität. Manchmal reicht diese Ausstattung auch für Analysen in Gigabit Ethernets aus, wengleich der Einsatz spezieller Netzwerkkarten und/oder Hardware-Analyser sicherlich das Erzielen besserer Ergebnisse ermöglicht.

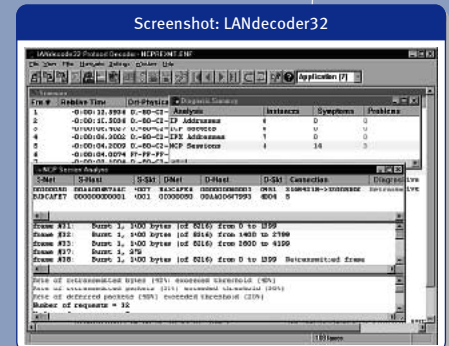
Screenshot: Ethereal Network Analyzer



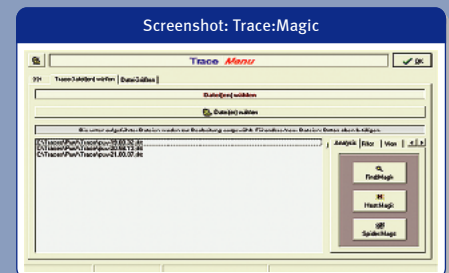
Screenshot: ntop



Screenshot: LANdecoder32



Screenshot: Trace:Magic





Screenshot: Observer

Mit dem Setzen von Filtern - etwa um nur die Kommunikation zwischen zwei bestimmten Stationen oder nur Frames eines bestimmten Protokolls angezeigt zu bekommen - lässt sich das Datenvolumen reduzieren. Doch Vorsicht: Denn damit ist unweigerlich verbunden, dass einige Daten gar nicht erst in die Analyse mit einfließen. Und möglicherweise handelt es sich dann dabei ausgerechnet um die Daten, die Rückschlüsse auf Fehlerursachen offenbaren (vergleiche dazu auch Seite 9).

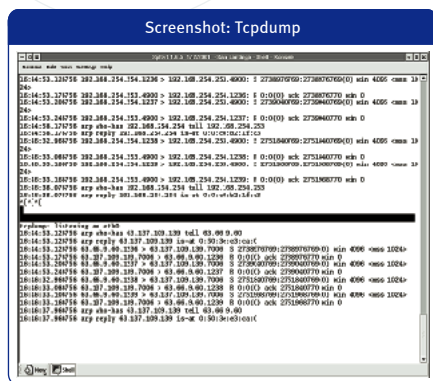
Vor dem Hintergrund massiv anfallender Trace-Daten sollte die zur Auswertung eingesetzte Analyzer-Software zudem in der Lage sein, mehrere Trace-Dateien gleichzeitig auszuwerten sowie diese korrelieren zu können. Das spart kostbare Zeit - insbesondere wenn es gilt, unter Druck die Ursachen größerer Netzwerkprobleme ausfindig zu machen und zu beheben.



Screenshot: Gigapeek NX

Freeware Tools

Neben den Werkzeugen Ntop, snoop und Tcpdump, die Trace-Dateien ebenfalls über normale Netzwerkkarten für die Analyse erzeugen, sei hier im Besonderen der Open-Source-Analyzer Ethereal erwähnt. Die Software ist sowohl unter Linux/Unix als auch unter Windows lauffähig. Mit der Ergänzung von Libpcap bzw. WinPcap erhält man eine recht leistungsfähige Capture Engine, welche auch mit Standard-Netzwerkkarten arbeitet. Annähernd 400 Protokolle können die Werkzeuge verarbeiten und dürften damit ein breites Spektrum an Anforderungen abdecken. Ethereal bietet diverse Filterfunktionen und erlaubt unter Einsatz eines weiteren Zusatzmoduls (Mergecap) das Zusammenfassen mehrerer Trace-Files zu einer Datei. Ein Expertensystem zur Auswertung der Trace-Daten bietet Ethereal jedoch nicht.



Screenshot: Tcpdump

Kommerzielle Tools

Das wohl bekannteste Tool zur LAN-Analyse ist die Software LANdecoder32 von Triticom. Zu den Klassikern zählen ebenso die Gigabit-Ethernet-Version Observer von Network Instruments und Gigapeek NX von Wildpackets. In jüngster Zeit macht jedoch immer mehr das Softwareprodukt Trace:Magic von sich reden. Es stammt von dem deutschen Anbieter Synapse Networks und nutzt Capture Engines von anderen Anbietern. Trace:Magic analysiert mehrere Trace-Dateien parallel und kann daher auch aus sehr umfangreichen Datenbeständen meist automatisch die für die Fehlersuche wichtigen Pakete selektieren.

IT Netzwerkdiagnose

Services von Networkers im Bereich Netzwerkanalysen

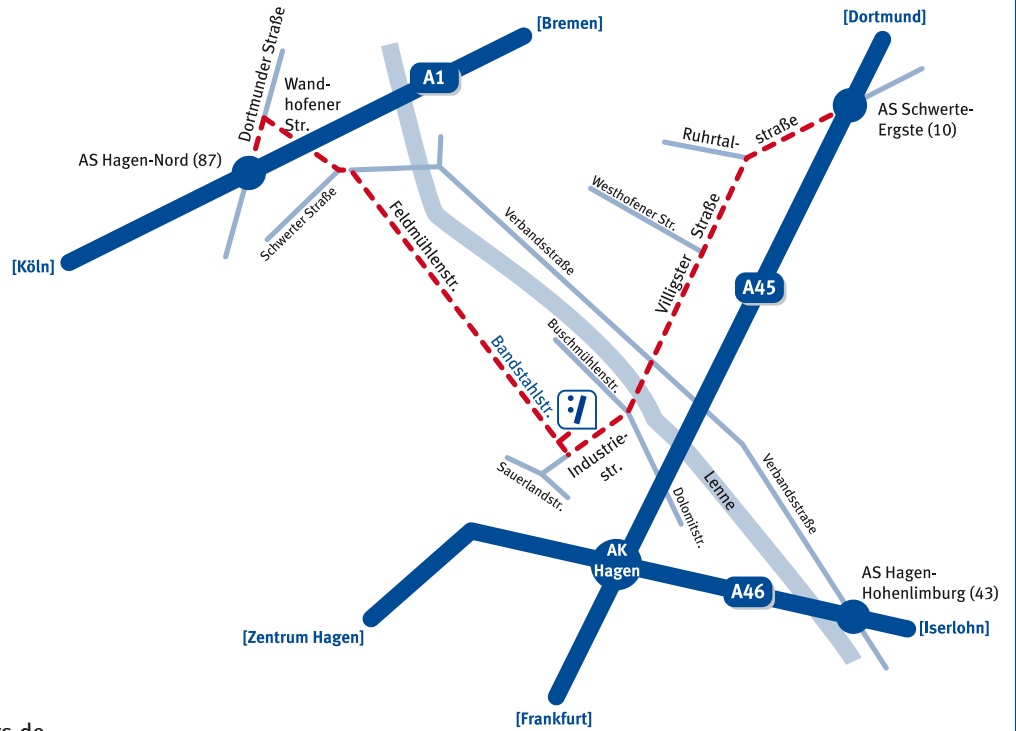
Im Bereich der Netzwerkdiagnosen (Ethernet / IP) besitzt Networkers fundiertes Know-how und Erfahrung. Unsere speziell ausgebildeten Experten spüren Kommunikationsprobleme schnell und effizient auf und beheben diese zuverlässig.

Zur Ermittlung von Daten und zur Auswertung setzen sie unter anderem Bündel speziell aufeinander abgestimmter Diagnosetools ein. Denn nur auf Basis zuverlässiger und gültiger Daten können anschließend exakt die Maßnahmen hergeleitet und umgesetzt werden, die die optimale Leistungsfähigkeit ihrer Netzwerkkumgebungen sicherstellen.

Sowohl in Breite als auch in Tiefe bieten wir umfassende Services, unter anderem:

- methodische Überprüfung Ihrer Netzwerk-Topologie sowie Überprüfung der Auswahl eingesetzter Komponenten hinsichtlich Einsatzzweck, Auslegung und Dimensionierung.
- Kontrolle der Komponentenplatzierung sowie deren Konfigurationseinstellungen.
- Durchführung von Struktur-, Datenverkehrs-, Kommunikations- und Bottle-Neck-Analysen.
- Durchführung genereller und/oder gezielter Messungen innerhalb der zu analysierenden Umgebungen.
- Lokalisierung von Anomalien, Fehlern und Engpässen.
- Ursachenbestimmung von Anomalien, Fehlern und Engpässen (z.B. nicht fachgerechte Konfiguration, Mängel in Soft- / Hardware).
- umfassende Aufbereitung der Messergebnisse.
- Dokumentation und Präsentation der Messergebnisse sowie der lokalisierten Anomalien und Fehler inklusive Empfehlungen von Lösungen / Maßnahmen zur Behebung und Optimierung.
- Entwicklung und Umsetzung technisch wie wirtschaftlich sinnvoller Lösungen / Maßnahmen.

Zentrale

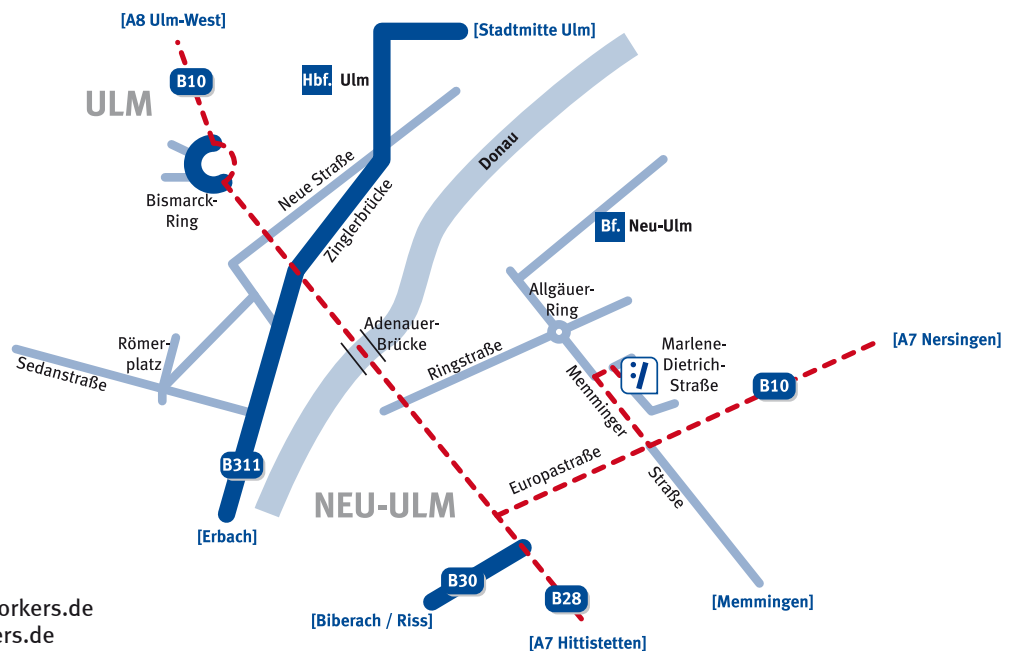


Networkers AG
Bandstahlstraße 2
58093 Hagen

fon: 0 23 31 . 80 95 0
fax: 0 23 31 . 80 95 499

email: info@networkers.de
web: <http://www.networkers.de>

Niederlassung Neu-Ulm



Networkers AG
Niederlassung Neu-Ulm
Marlene-Dietrich-Straße 5
89231 Neu-Ulm

fon: 07 31 . 98 58 88 70
fax: 07 31 . 98 58 88 74

email: info@neu-ulm.networkers.de
web: <http://www.networkers.de>



Networkers AG
Bandstahlstraße 2
58093 Hagen

fon: 0 23 31 . 80 95 0
fax: 0 23 31 . 80 95 499

email: info@networkers.de
web: www.networkers.de

Networkers AG Niederlassung Neu-Ulm
Marlene-Dietrich-Straße 5
89231 Neu-Ulm

fon: 07 31 . 98 58 88 70
fax: 07 31 . 98 58 88 74

email: info@neu-ulm.networkers.de
web: www.networkers.de