Ansätze zum automatischen Fehlermanagement in Netzwerken

Jörg Benze
Controlware GmbH, Technical Operations
Waldstraße 92, D-63128 Dietzenbach
joerg.benze@controlware.de

Abstract. Mit dem starken Wachstum der Telekommunikationsnetzwerke nimmt auch die Bedeutung des Netzwerkmanagements zu. Traditionelle Netzwerkmanagementaktivitäten, zu denen auch das Netzwerkfehlermanagement gehört, werden gegenwärtig unter Einbeziehung der menschlichen Arbeitskraft ausgeführt. Jedoch werden diese Aktivitäten zunehmend mehr nachgefragt und von ihrer Charakteristik her komplexer, so daß die Idee der Automation bzw. Teilautomation von Netzwerkmanagementaktivitäten zunehmend an Attraktivität gewinnt. In diesem Zusammenhang ist es angebracht, den Ablauf des Fehlermanagements in einem *Network Control Center* zu analysieren, um Ansatzpunkte für eine Automatisierung bzw. Teilautomatisierung des Netzwerkfehlermanagements zu finden.

1 Abgrenzung und Einordnung in das Themengebiet des Netzwerkmanagements

Nach dem ISO Modell unterteilt sich das Netzwerkmanagement in fünf funktionale Teilbereiche, auf die nachfolgend kurz eingegangen wird:
Das *Konfigurationsmanagement* beinhaltet das Nachvollziehen der Konfiguration einer Komponenten, so daß bei Problemen die Konfiguration wiederhergestellt werden kann und die Konfiguration neu hinzukommender Geräte entsprechend anpaßbar ist. Mittels des *Leistungsmanagements* können durch regelmäßige Beobachtung des Datenverkehrs und des Datendurchsatzes Fehler abgefangen werden, die duch Überlast entstehen. Ferner ist es hierdurch möglich, Überlastsituationen proaktiv zu verhindern. Das *Fehlermanagement* hat zum Ziel, aufgetretene Fehler (bzw. deren Ursache) schnellstmöglich zu erkennen und zu lokalisieren. Hierzu gehört auch die Möglichkeit, Fehler herauszufiltern und Fehlermeldungen gezielt weiterzuleiten. Der Bereich des *Sicherheitsmanagements* umfaßt die Kontrolle der Zugangsberechtigung und der Authentisierung. Alle Zugriffe auf die Netzwerkkomponente sollten mitgeschrieben werden und bei unberechtigtem Zugriff eine Alarmmeldung geschickt werden, dies aber schon beim Versuch

des Zugriffs. Durch das *Abrechnungsmanagement* bzw. durch das Mitprotokollieren, wer wann wie lange welche Ressource nutzt, können Kosten gerechter auf die Nutzer verteilt werden. Auch Kosten für Neuinvestitionen können hierdurch besser zugeordnet werden.

2 Praktische Erfahrungen hinsichtlich des Auftretens von Fehlern im Tagesgeschäft des Netzwerkmanagements

Betrachtet man die Störungen, die in einem *Network Control Center* eingehen bzw. zur Bearbeitung durch die Mitarbeiter anstehen nach der Art und Weise ihrer Häufigkeit, so wird man im Gespräch mit den Operators an der Konsole des Network Control Centers folgendes feststellen:



Fig 1. Network-Control-Center

Die größte Anzahl der aufgelaufenen Störungen sind Leitungsstörungen, die ein Umschalten auf eine Ersatzleitung erfordern und die Einleitung des Entstörungsmanagements der ausgefallenen Leitung. Neben dem Leitungsausfall treten im Bereich der Leitungsstörungen noch Datenübertragungsfehler bzw. Bitratenfehler und Delay-Fehler auf. Fehler dieser Art stellen den Löwenanteil der im Tagesgeschäft zu bearbeitenden Störungen dar.

Neben Leitungsstörungen werden die Operators auch häufig von Performance-Problemen in Anspruch genommen. Bei einem Performance-Problem kann aber in den meisten Fällen keine schnelle Abhilfe geschaffen werden (die Bandbreite der Leitung ist halt begrenzt), sondern es erfolgt eine Analyse des Performance-Problems und die hieraus resultierenden Hinweise zur Änderung des Netzwerkaufbaus dienen als Grundlage für die weitere Netzentwicklung.

Fehlerhafte Gerätekonfigurationen sind im Normalbetrieb nur selten der Grund für Störungen. Fehler dieser Art steigen nur in Zeiträumen größerer Netzumbauten an, wobei die Fehler dann überwiegend einem direkten Zusammenhang zu den laufenden Umbaumaßnahmen haben.

Störungen im Betrieb des Netzwerks aufgrund von Hardware-Defekten an den eingesetzten Netzwerkkomponenten sind in der Relation zu den o.g. Störungen relativ selten.

Als Fazit ist aufgrund der praktischen Erfahrungen festzustellen, daß sich die überwiegende Tätigkeit der Operators im Rahmen des Fehlermanagements auf des Bearbeiten von Leitungsstörungen bezieht. Hieraus folgt, daß Anstrengungen zur Automatisierung des Fehlermanagements in Netzwerken primär in diesem Bereich erfolgen sollte, da hier der größte Bedarf ist.

3 Ablauf des Fehlermanagements

Definition: Ein Fehler ist ein Ereignis, das zu einem nicht gewünschten Verhalten des Netzwerks führt. Unter einem Fehler versteht man die Ursache, die zur festgestellten Auswirkung führt. Ein Fehler wird überwiegend nicht direkt festgestellt, sondern es muß aufgrund von einer oder mehrerer festgestellten Auswirkungen über eine Eingrenzung die Ursache gefunden werden.

Abbildung 2 gibt eine Übersicht hinsichtlich der Prozeßkette des Fehlermanagements, auf dessen einzelne Schritte nachfolgend eingegangen wird:

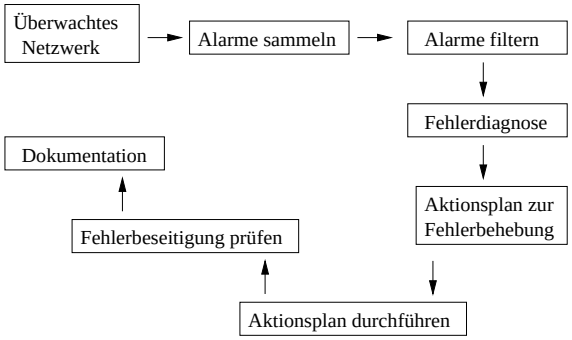


Fig 2. Prozeßkette des Fehlermanagements

Der erste Schritt beim Fehlermanagement ist das *Sammeln von Alarmmeldungen*, die die Netzwerkkomponenten auf unterschiedliche Weise ermitteln bzw. versenden. Die Alarmmeldungen sind an einem zentralen Punkt zu sammeln.
Hierbei unterscheidet man zwei Arten von Alarmen. Die eine Art sind Meldungen, die vom Gerät versendet bzw. vom Netzwerkmanagement erzeugt werden, wenn ein Gerät nicht mehr erreichbar ist. Die zweite Art sind Monitoring-Alarme. Hier werden Größen ständig überwacht und die Alarmmeldung wird erzeugt, wenn der Absolutwert oder der Trend einer Größe eine vorher bestimmte Grenze überschreitet. Alarmmeldungen können in zwei Kategorien eingeteilt werden, diese sind: Physikalische Alarme (z.B. Link down) und logische Alarme bzw. statistische Alarme (z.B. Leitungsauslastung > oberer Grenzwert).
Der zweite Schritt besteht darin, die *Alarmmeldungen zu filtern und zu bewerten*. Hierzu werden in der Regel vier verschiedene Techniken eingesetzt. Mittels

der *Verdichtung* erfolgt die Unterdrückung gleichlautender Alarme bzw. die Darstellung nur eines Alarms. Durch *zählen* wird eine quantitative Erfassung von Alarmen bzw. Klasse von Alarmen realisiert. Die *Unterdrückung* basiert auf einer Priorisierung der Alarmmeldungen, wobei die unterhalb eines definierten Levels unterdrückt werden. Mittels der *Generalisierung* wird ein Zusammenhang zwischen dem Alarm und einer vorher definierten Superklasse von Alarmen hergestellt.
In dritten Schritt, der *Fehlerdiagnose*, wird aufgrund der klassifiziert vorliegenden Sachlage der Alarmmeldungen eine Hypothese bzgl. der Fehlerursache erstellt, die u.U. durch Tests im Netzwerk erhärtet oder verworfen wird, wobei letztes eine neue Hypothese erfordert. Der Vorgang kann iterativ erfolgen. bis die Fehlerursache hinreichend sicher festgestellt ist.
Im vierten Schritt erfolgt die *Erstellung eines Plans zur Fehlerbeseitigung bzw. Fehlerüberbrückung*. Hierzu ist mehrheitlich eine Kette von Aktionen erforderlich, wobei die Einzelaktionen voneinander abhängig sind bzw. aufeinander aufbauen. Der Aktionsplan wird ausgehend von den Ergebnissen der Fehlerdiagnose und einer Strategie, die überwiegend auf der Erfahrung des Operators beruht, erstellt.
Die *Durchführung des Plans* erfolgt im Schritt fünf, wobei der Aktionsplan Schritt für Schritt abgearbeitet wird. Nach jeder Aktion wird der Erfolg dieser kontrolliert bzw. verifiziert, weshalb die für die Aktion postulierte Veränderung nicht eingetreten ist.
An sechster Stelle erfolgt die *Überprüfung des Erfolgs der Fehlerbearbeitung*, wobei dies u.U. durch Tests im Netzwerk erfolgt und durch eine Befragung der an diesem Vorgang beteiligten Stellen sichergestellt wird, daß der Fehler beseitigt ist.
Zum Schluß erfolgt der Abschluß der *Dokumentation des Vorgangs*, die schon während der Fehlerbearbeitung begleitend mitgeführt wurde, um die Änderungen am Netzwerk nachvollziehen zu können, falls durch Seiteneffekte neue Alarme hervorgerufen werden.

4 Ansatzpunkte für eine Automatisierung des Netzwerkmanagements

Im Bereich des Sammelns und Filterns von Alarmen bieten die heute verfügbaren Systems (z.B. Micromuse Netcool) eine für Zwecke des Netzwerkoperating ausreichende Leistungsfähigkeit.
Für den Bereich der Fehlerdiagnose und Fehlererkennung ist die heute mögliche Rechnerunterstützung sehr gering im Vergleich zu dem, was ein Operator mit entsprechender Berufserfahrung zu leisten vermag. Eine Automatisierung wird z.B. dadurch erschwert, daß die Fehlerbezeichnungen in den Traps sehr herstellerabhängig sind und teilweise sich auch von Softwarerelease zu Softwarerelease der Betriebssoftware eines Geräts ändern. Abhilfe würde hier eine standardisierte Fehlerbeschreibungssprache (wie z.B. das SNMP-Protokoll und die MIP ein einheitliches Beschreibungssystem für die Konfiguration von Netzwerkgeräten

ist) schaffen, wobei alle Hersteller sich auf eine gleiche texttuelle Beschreibung eines Ereignisses (z.B. Link down) einigen müßten und hierfür einen einheitlichen Fehlercode melden sollten. Um dies zu realisieren, sind Änderungen in der Betriebssoftware der Netzwerkkomponenten notwendig, die in der Regel nur der Hersteller vornehmen kann. Fehlerdiagnosesysteme, die auf Basis der Alarmmeldungen eine qualifizierte Fehlerdiagnose erstellen können, wären mit einer Vereinheitlichung in dem Bereich der Fehlermeldungen leichter realisierbar.
Im Bereich der Vorgehensplanung zur Fehlerbehebung, Durchführung des Vorgehensplans, Erfolgskontrolle der Fehlerbeseitigung und Dokumentation sind heute nur Anstrengungen hinsichtlich einer Teilautomatisierung bzw. der Aufbau von Unterstützungssystemen für die Operators sinnvoll, da die Kommunikation und Abstimmung der an einer Fehlerbeseitigung beteiligten Stellen heute überwiegend formlos per Telefon, E-Mail oder aus juristischen Gründen per Fax erfolgt. Die hier entstehenden Teilautomatisierungslösungen können dann in einem zweiten Schritt durch Integration den Weg zu einem vollautomatischen Fehlermanagement ebnen.

5 Ansatzpunkte für die Entwicklung eines Prototypen zur Automatisierung der Fehlerdiagnose bei Leitungsstörungen

Da Leitungsstörungen mit Abstand die Mehrzahl der von den Operators zu bearbeitenden Störungen darstellen, ist dies ein guter Ansatz, um einen Prototypen zur Fehlerdiagnose von Leitungsstörungen zu entwickeln. Das Fehlerdiagnosetool sollte in der Lage sein, die Art einer Leitungsstörung zu ermitteln und dem Operator anzuzeigen, ebenso alle zur Entstörung der Leitung notwendigen Informationen (z.B. Leitungsnummer, Faxvorlage zur Störungsmeldung beim Carrier, Rufnummern der Stellen, die bei Ausfall der Leitung zu informieren sind, usw.) Gegenwärtige Netzwerkmanagementsysteme liefern zwar bei Leitungsstörungen die Information, daß die Datenübertragung zwischen zwei Netzwerkkomponenten nicht mehr funktioniert, aber den genauen Grund hierfür zu finden, ist heute noch Aufgabe des Operators. Einen möglichen Realisierungsweg zeigt Abbildung 3. Die zu überwachenden Netzwerkkomponenten lassen sich heute mehrheitlich via SNMP über die Public MIB managen und abfragen. Das Leitungsfehlerdiagnose-system fragt nun zyklisch auf den Netzwerkkomponenten die Daten der Ports ab, die an den zu überwachenden Leitungen hängen oder gewinnt diese Information aus einem Netzwerkmanagement-System. Diese Art der Rohdatengewinnung ermöglicht den Einsatz eines Leitungsfehlerdiagnosetools über Hersteller- und Softwarereleasegrenzen hinweg.
Für jede Leitung wird aus den Daten der Leitungs-Ports ein aktuelles Zustandsprofil der Leitung gebildet und mit Daten einer Fehlerprofildatenbank verglichen. Bei einer hinreichenden Übereinstimmung des Leitungsprofils mit einem Fehlerprofil wird die zum Fehlerprofil gehörende Fehlermeldung dem Operator angezeigt. Ebenfalls werden die Daten der betroffenen Leitung aus der Leitungsdatenbank gelesen und ebenfalls für den Operator zur Anzeige gebracht, damit

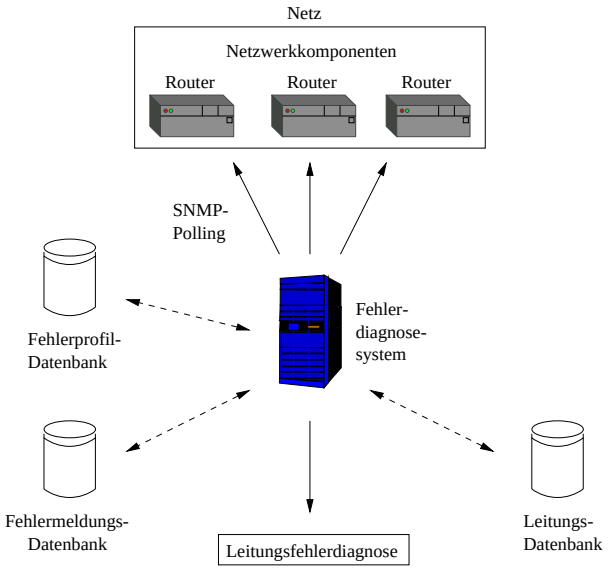


Fig 3. Aufbau eines Fehlerdiagnosetools zum Aufbau einer Fehlererkennung bei Leitungsstörungen

dieser schnell an alle Informationen kommt, die zum Einleiten der Entstörung benötigt werden.

6 Fazit

Die Realisierung eines vollständig automatisch ablaufenden Fehlernetzwerkmanagementsystems in einer mittelfristigen Zeitspanne scheitert derzeit an der Komplexität der Systeme und an der formlosen Kommunikation (Telefon, Fax, E-Mail) der an der Entstörung beteiligten Stellen.
Denkbar sind jedoch die Implementierung von Unterstützungssystem, die den Operators bei der Fehlerdiagnose helfen, indem die Fehlerdiagnose bzw. Teilschritte der Fehlerdiagnose automatisch erfolgt und Informationen, die zur Einleitung der Entstörung erforderlich sind, schnell und passend vom System zur Verfügung gestellt werden.

[1] Automated Network Fault Management, P. Viswanathan, http://www.isr.umd.edu/TechReports/ISR/1996/MS_96-14/MS_96-14.phtml (27.06.2002), Center for Satellite and Hybrid Communication Networks 1996 (http://www.isr.umd.edu/CSHCN)

[2] Intelligent Distributed Fault and Performance Management for Communication Networks, Hongjun Li, http://www.isr.umd.edu/TechReports/CSHCN/2002/CSHCN_PhD_2002-2/CSHCN_PhD_2002-2.phtml, (27.06.2002), Center for Satellite and Hybrid Communication Networks 2002 (http://www.isr.umd.edu/CSHCN)

[3] An Artifical Intelligence Approach to Network Faul Management, http://www.sce.carleton.ca/netmanage/docs/An_AI_Approach.pdf (27.06.2002), Denise W. Gürer, Irfan Khan, Richard Ogier, SRI International, 333 Ravenswood Ave., Menlo Park, CA 94025 USA, http://www.sri.com, Renee Keffer, Sprint, 9300 Matcalf, Overland Park, KS 66212 USA (http://www.sprint.com)