Mit System

Fehlern auf der Spur durch Netzmonitoring

Kai-Oliver Detken

Der reibungslose Betrieb heutiger komplexer Netzstrukturen kann nur sichergestellt werden, wenn alle Teile eines Netzes überwacht und gesteuert werden. Ein Netzmanagement oder Netzmonitoring ist demnach unverzichtbar.
Die Grundlage dafür bilden Managementapplikationen, die mit Hilfe eines eigenen Protokolls Systemkomponenten überwachen und durch Befehle zu Reaktionen veranlassen.

Die Aufgaben und Anforderungen, die ein Netzmanagementsystem zu bewältigen hat, können sehr unterschiedlich sein. Um den Anwendern die Auswahl eines Systems zu erleichtern, hat die ISO eine Unterteilung vorgenommen:

- Konfigurationsmanagement: wird für die Konfiguration von Systemkomponenten verwendet. Bestimmte Anwendungsbereiche werden gruppiert und in einer geografischen Aufteilung der Systeme dargestellt. Subnetze und Geräte werden in entsprechenden Tabellen bzw. grafisch mit Hilfe von Landkarten verwaltet. Zur problemlosen Bedienung ist meistens ein Graphical User Interface (GUI) vorhanden.
- Leistungsmanagement: wird für die Beobachtung und Bewertung der Netzdaten in bezug auf die Qualität von Übertragungsstrecken und Schnittstellen verwendet. Qualitätsmeßpunkte lassen sich grafisch anzeigen. Qualitätsdaten können gelesen, angezeigt, gedruckt und in einer Datei gespeichert werden.
- Fehlermanagement: unterstützt den Administrator, um auftretende Fehler erkennen, visualisieren, lokalisieren und protokollieren zu können. Spontane Ereignisse/Alarme werden asynchron von den angeschlossenen Systemen empfangen und registriert. Weiterhin sind Fehlererkennung bei Verbindungspfaden und Knoten sowie eine Fehlerbearbeitungsfunktion enthalten, so daß eine zentrale Bearbeitung aller Alarme des Netzes möglich ist. Alarme können bestätigt, gespeichert und archiviert werden (Alarmlog). Die Verfügbarkeit der Baugruppenträger wird durch ein automatisches Polling-Verfahren abgefragt.
- Benutzermanagement: wird für das Tracking von individuellen Auslastungen oder Gruppenverkehr eingesetzt. Dadurch lassen sich die Ressourcen des Netzes besser verplanen. Engpässe werden frühzeitig aufgezeigt, so daß man ihnen entgegenwirken kann. Statistiken lassen sich übersichtlich abrufen und zentral erfassen. Ein Inventarmanagement kann integriert sein.
- Sicherheitsmanagement: regelt den sicheren Zugang zum Netzmanagementsystem. Der Administrator vergibt für jeden Benutzer einen Namen und ein Paßwort mit der entsprechenden Zugangsberechtigung (Schreiben, Lesen).

Alle genannten Managementbereiche werden von heutigen Managementsystemen meistens nur teilweise abgedeckt. Sog. Framework-Tools haben den Anspruch, alle Disziplinen abzudecken. Diese Lösungen wie CA Unicenter, HP OpenView und IBM Tivoli sind allerdings sehr mächtig und inzwischen sogar in der Lage, Speichernetze mit zu verwalten. Allerdings sind sie auch sehr kostspielig und werden nur bruchstückhaft vom Anwender genutzt.
Der Markt bietet heute zahlreiche Alternativen, um Netze kontinuierlich zu überwachen. Dabei reicht die Palette von kostenlosen SNMP-Kommandozeilen-Tools bis hin zu erschwinglichen Monitoring-Produkten.

Das Thema in Kürze

Netzmanagementsysteme gibt es von jedem Hersteller in jedweder Ausrichtung. Allerdings sind nicht alle Systeme dafür geeignet, die unterschiedlichsten Anforderungen der Anwender zu erfüllen. Ausgehend von einer Erläuterung der Managementaufgaben und der für das Netzmonitoring eingesetzten Protokolle werden in diesem Beitrag verschiedene Netzmanagementsysteme einander gegenübergestellt.

Dr.-Ing. Kai-Olliver Detken ist Geschäftsführer der DECOIT GmbH sowie Dozent und freier Autor in Bremen

Protokolle und Standards

Aus einer Reihe unterschiedlicher Ansätze heraus hat sich das Simple Network Management Protocol (SNMP) in der Version 1 zum Defacto-Standard entwickelt. Es ist wesentlicher Bestandteil des Fehler- und Konfigurationsmanagement auf der Grundlage der TCP/IP-Protokolle. Ein SNMP-basiertes Managementsystem setzt sich aus einer Managementstation, den Agents mit ihren MIBs in den zu überwachenden Geräten und dem Managementprotokoll zusammen (*Bild 1*).
Die Management Information Base (MIB) enthält eine Ansammlung von Objekten, die über mehrere Attribute (Parameter) verfügen. Die Managementfunktion ist dann eine Folge von parametrisierten Operationen auf dem Objekt. Ausgehend von der Managementstation erfolgt die Kommunikation mit den Agents. Diese beantworten Anfragen oder setzen Befehle in Aktionen um. Darüber hinaus können sie auch unaufgefordert Alarmmeldungen an die Managementstation senden. Die mit der MIB (MIB I, MIB II)

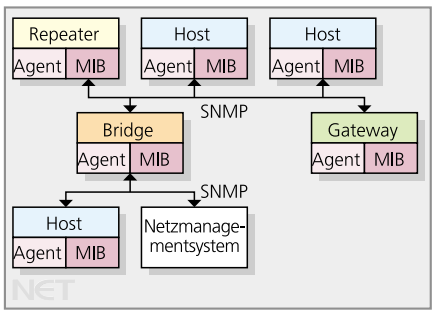

Bild 1: Zentrales SNMP-Management

zu ermittelnden statistischen Daten sind nur als Momentaufnahmen einiger, den Datenverkehr betreffender Parameter zu werten. Sie sind wenig geeignet, um langfristige Statistiken zu generieren und daraus Trends abzuleiten. Zwischen dem Fehler- und Konfigurationsmanagement und einem echten Netzreporting besteht also eine Lücke.
Das Werkzeug für ein echtes Netzreporting ist RMON (Remote Monitoring). Es erweitert das SNMP-Modell und liefert statistische Meßwerte, die auf einer längerfristigen Analyse des realen Datenverkehrs beruhen. Damit sind detaillierte Aussagen über den Status des Netzes und Rückschlüsse auf die Netzentwicklung möglich. Voraussetzung sind ein RMON-Manager (Applikation auf einer Managementstation) und die RMON-Agents (Software in den Netzkomponenten oder eigenständige Probe).
Die Management Information Base (MIB) der RMON1-Version enthält neun Gruppen für festgelegte Funktionsbereiche. Eine zehnte behandelt den Token Ring. Die damit ermittelten Statistiken werden aus den Adressen der Ebene 2 des OSI-Schichtenmodells abgeleitet. Sie lassen Aussagen über die Netzauslastung an den einzelnen Ports wie auch über die Kommunikationsbeziehungen zwischen einzelnen Teilnehmern zu. Somit können auch Teilnehmer, die eine besonders hohe Netzlast erzeugen, ermittelt werden.

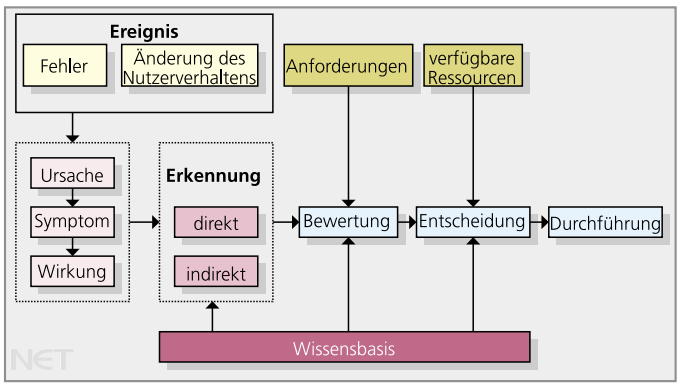

Bild 2: Strukturiertes Netzmanagement

Die RMON2-Version stellt eine Erweiterung der Version 1 dar und enthält zehn weitere Funktionsgruppen. Mit ihr lassen sich Protokolle der Ebenen drei bis sieben in die Analyse einbeziehen. Lastverteilungen einzelner Protokolle oder Applikationen können so ermittelt werden. RMON-Funktionen sind verstärkt in den aktiven Netzkomponenten anzutreffen. Als Folge beschränkter Ausstattungsmöglichkeiten (Prozessor, Speicher) sind aber meist nur wenige Gruppen implementiert. Eigenständige Geräte (externe Probe) dagegen, die auf sehr leistungsfähiger Hardware aufbauen, können über alle Funktionsgruppen verfügen. Für eine Leistungsbewertung von RMON-Funktionen sind daher immer die verfügbaren MIB-Gruppen heranzuziehen.
Der Einsatz von externen Probes ist in Netzen mit LAN-Switchen, besonders wenn deren einzelne Ports nur dediziert genutzt werden (Verbindungen immer nur zwischen einzelnen Geräten), wenig praktikabel. Hier müßte jeder Port mit einer Probe ausgestattet werden. Eine Alternative dazu stellen Lösungen dar, bei denen ein Monitorport konfiguriert wird, der den Verkehr anderer Ports spiegelt. Hierbei sind jedoch die Speicherkapazität für diesen Port und das gesamte Volumen der Statistikdaten zu beachten. Vielfach müssen erhebliche Einschränkungen in Kauf genommen werden. Die nicht zufriedenstellenden Möglichkeiten in einer Switch-Umgebung führten zum Switch Monitoring (SMON). Damit lassen sich physische Einheiten wie Switche oder deren Module, aber auch logische Gruppen wie VLANs als Datenquellen für die RMON-MIBs auswerten.

Kostengünstige Alternativen

Der ordnungsgemäße Betrieb eines Netzes, der eine definierte Bandbreite, Qualität und Verfügbarkeit einschließt, wird durch Ereignisse beeinflußt. Dabei muß man zwischen einmaligen und wiederkehrenden Ereignissen unterscheiden. Ein einmaliges Ereignis, das den regulären Netzbetrieb beeinträchtigt, ist ein Fehler. Ein häufig wiederkehrendes Ereignis zeigt hingegen eine tendenzielle Veränderung des Verhaltens der Nutzer an. Direkt (durch den Netzteilnehmer) oder indirekt (durch das Netzmanagement) können diese Ereignisse zum Administrator gelangen.
Ein Ereignis und seine Folgen können in drei Bereiche gegliedert werden:

- Ursache: z.B. Durchtrennen eines Ethernet-Kabels;
- Symptom: kein korrekter Zugriff auf das Übertragungsmedium möglich;
- Wirkung: Client-Server-Verbindung wird mit einem Time-out abgebrochen.

Bild 3: Netzkarte unter WhatsUp Gold

Im allgemeinen ist die Ursache nicht sofort erkennbar, sondern nur die Wirkung oder bestenfalls das Symptom. Die Zuordnung von der Ursache zum Symptom und weiter zur Wirkung ist eindeutig. Umgekehrt gibt es meist viele mögliche Ursachen, die eine Wirkung bedingen. Es hängt vom richtigen Einsatz von Monitoren und der Erstellung von Statistiken, aber auch wesentlich von der Erfahrung und dem Wissen des Netzmanagers ab, wie rasch eine Ursache erkannt wird. Eine strukturierte Vorgehensweise wie in *Bild 2* ist dabei unabdingbar. Das Anlegen einer Wissensdatenbank wird empfohlen.

Das Erkennen von Fehlern und die Netzdarstellung kann bereits durch günstige oder kostenlose Monitoring- und Netzlösungen erreicht werden. Das Tool WhatsUp Gold von Ipswitch zählt z.B. zu den bekanntesten der kostengünstigen Netzmonitorsysteme. Weitere Tools sind beispielsweise SNMPc v6.0 von Castlerock oder Network Probe 1.0 von Object Planet.

WhatsUp Gold bietet wie ähnliche Lösungen umfangreiche Funktionen, mit denen sich auch größere Netze über mehrere IP-Subnetze hinweg zentral überwachen lassen. Ein Event-Monitoring beobachtet kontinuierlich die vom Administrator definierten Bereiche und schlägt Alarm, sobald Fehlfunktionen auftreten oder Schwellwerte überschritten werden. Zahlreiche Standardreports ermöglichen eine schnelle Analyse von wichtigen Parametern wie Netzverfügbarkeit oder Bandbreitenauslastung. Die Reports sind individuell anpaßbar.

Das zentrale Werkzeug für die Verwaltung ist die sog. Network Map, die alle gefundenen Geräte grafisch darstellt (*Bild 3*). Hier muß eingestellt werden, welche Discovery-Methode das jeweilige Tool verwenden soll. Für größere Netze mit mehreren SNMP-fähigen Routern eignet sich z.B. SNMP Smart Scan. Damit generiert WhatsUp Gold eine sog. Parent Map des übergeordneten Netzes und für jedes IP-Subnetz eine eigene Ansicht. Dabei wird auch angegeben, nach welchen Diensten gesucht werden soll.

Normalerweise werden vorhandene Dienste und Geräte inkl. der nicht SNMP-fähigen anhand ihrer IP-Adresse und ihres Host-Namens erkannt. Alternativ kann auch ICMP verwendet werden, was aber nur bei kleinen, flachen Netzen zu empfehlen ist. Trotzdem funktioniert die Zuordnung der Symbole nur bei den Geräten korrekt, die entsprechende Informationen bereitstellen. Es ist daher bei allen Monitoring-Systemen fast immer einige Nacharbeit nötig, bis die Network Map das Testnetz richtig abbildet.

Einzelne Geräte lassen sich flexibel anordnen und per Maustaste schnell miteinander verbinden. Auf diese Weise können Darstellungen nach Belieben angepaßt werden, so daß sie mit der jeweiligen Netzstruktur über-

Bild 3: NetSight Element Manager in der Topologiedarstellung

einstimmen. Wie häufig die zu überwachenden Systeme per Polling abgefragt werden, muß generell oder separat für einzelne Geräte eingestellt werden. Außerdem wird meistens das Polling über unterschiedliche Protokolle ermöglicht bzw. festgelegt, ob nur die Dienste überwacht werden sollen.

Für eine kontinuierliche Netzüberwachung sind aussagekräftige Reports unverzichtbar. Hier stellen alle Tools eine ganze Reihe Standardreports bereit, die unterschiedliche Parameter auswerten. So lassen sich z.B. die Antwortzeiten, die Verfügbarkeit und die Performance des gesamten Netzes oder ausgewählter Systeme über längere Zeiträume hinweg darstellen. Es wird zudem auch meistens eine umfangreiche Event-Konfiguration ermöglicht, die automatisch Alarm auslösen kann.

Fazit

Neben vorhandenen Netztools kann man natürlich eine Anzahl von Werkzeugen für die Netzüberwachung und -analyse verwenden, die bereits in die Betriebssysteme integriert ist. Dies sind u.a. bei Linux- bzw. Unix-Systemen Ping, Traceroute, Lookup, Finger, Whois und SNMP-Abfragen. Hinzu kommen Open-Source-Lösungen wie Multi Router Traffic Grapher (MRTG), OpenNMS und Scotty, die ähnliche Funktionalitäten unter Linux anbieten wie eine Monitoring-Gesamtlösung, aber noch ergänzt bzw. angepaßt werden müssen, wenn man sie bedenkenlos einsetzen möchte. Eine Alternative bieten sie auf jeden Fall. Man sollte allerdings vorher seine Anforderungen kennen und die Monitorlösung anhand einer erstellten eigenen Leistungsbeschreibung aussuchen.

Ebenfalls nicht bedenkenlos einsetzbar sind Herstellerlösungen von aktiven Netzkomponenten, die nur die eigene Systemfamilie komplett verwalten können. Zu dieser Gruppe gehören Tools wie CiscoWorks2000 von Cisco Systems, NetSight Element Manager von Enterasys Networks (*Bild 4*) und EPICenter von Extreme Networks. Alle Netzhersteller bieten diese Tools für ihre Geräte an, die aber leider alle proprietär realisiert sind. Hinzu kommen sehr hohe Kosten, da ein Netzmanagement allein oft nicht ausreicht in einem heterogenen Netzverbund. Dafür lassen sich in Verbindung mit den Systemkomponenten des Herstellers alle Funktionen eines ISO-konformen Netzmanagements ausnutzen.

Preiswerte Tools in Kombination mit vorhandenen Netzzeugen können dagegen durchaus die Anforderungen an ein Unternehmen bis zu einer bestimmten Netzgröße abdecken. Das gilt insbesondere für das reine Monitoring. Will man aber das Management in seiner ganzen Vielfalt für ein großes Netz realisieren, sollten spezielle Herstellerlösungen bevorzugt oder auf übergreifende Framework-Tools für heterogene Netze zurückgegriffen werden. *(bk)*