Vorwort

Aufgrund des stetig steigenden Bedarfs an Informationsfluss, proportional dazu wachsende, hochverfügbare Kommunikationsnetze und der Vermischung von Sprach- und Datennetzen durch VOIP (Voice over IP) Technologie steigen auch die Anforderungen an die mittlerweile unverzichtbaren Netzwerkmanagementsysteme, die hinzukommenden Komponenten entsprechend ihrer Art zu erkennen, anzuzeigen und zu überwachen.

Dieses Dokument soll dem geneigten Leser einen Überblick über Netzwerkmanagement, dessen Hauptaufgabengebiete und die Abdeckung durch die derzeit am Markt befindlichen Netzwerkmanagement-Tools geben. Desweiteren wird kurz auf die Umsetzung des Layer 2 Managements eingegangen.

Abschliessend erfolgt eine Darstellung der Funktionalitätsabdeckung durch derzeit auf dem Markt etablierte Netzwerkmanagementprodukte.

Netzwerkmanagement

Nach wie vor lassen sich die Hauptaufgabengebiete von Netzwerkmanagementsystemen mit den von der ISO (International Standardizing Organisation) aufgestellten fünf „Specific Management Functional Area`s“ (SMFA) wie folgt aufteilen:

Fehlermanagement

Aufgabe des Faultmanagement ist es, die Vefügbarkeit des Netzwerks zu erhöhen und autretende Fehler anzuzeigen. Fehlermanagement beinhaltet drei wesentliche Aufgabengebiete:

Fehlererkennung

Hierbei werden die zu managenden Objekte regelmaessigen Tests (Polling) unterzogen, oder von der Komponente wird ein Störungsfall an das Managementsystem gemeldet (Trapping).

Fehlerdiagnose

Zur Erforschung der Fehlerursache werden Diagnosetools (Test Connectivity, Abfrage von MIB-Variablen) eingesetzt. Ausserdem können bisher gesammelte Daten über das zu verwaltende Objekt (Ereignisstatistiken, Fehler-Reports) zur Fehlerdiagnose herangezogen werden.

Fehlerbehebung

Zur Fehlerbehebung werden im Managementsystem hinterlegte Fehlerbehebungsprozeduren gestartet oder eine entsprechende Fehlereskalation in Form von externer Benachrichtigung o.ä. betrieben.

Konfigurationsmanagement

Das Konfigurationsmanagement soll die im Netzwerk vorhandenen Komponenten überwachen, deren Bestandteile und Einstellungen kontrollieren und bei Bedarf auch verändern. Das Konfiguration Management deckt alle Funktionen, die im Zusammenhang mit folgenden Aspekten stehen:

- Existenz und Namen von Netzkomponenten
- Technische Daten von Netzkomponenten
- Beziehung zwischen Netzkomponenten
- Addressierungen
- Routing-Informationen

Abrechnungsmanagement

Das klassische Abrechnungsmanagement (Accounting) will die Nutzung von Netzwerkressourcen benutzerbezogen quantifizieren und abrechnen.

Leistungsmanagement

Der Bereich des Performancemanagements beinhaltet Möglichkeiten zur Analyse und / oder Bewertung relevanter Kommunikationsprozesse. Durch permanente Datensammlung und Archivierung lassen sich spezifische Auswertungen anzeigen.

Typischerweise werden die Ergebnisse in Echtzeitstatistiken oder auch speicher- und druckbaren Reports zur Verfügung gestellt.

Sicherheitsmanagement

Die Funktionen des Securitymanagements umfassen die Sicherheit von Diensten und Protokollmechanismen der sieben OSI-Ebenen vor unberechtigtem Zugriff auf Datennetze und Ressourcen.

Da der Begriff „Security“ gerade im IT – Umfeld viele Gesichtspunkte hat, können diese nicht allein von einer Systemmanagement-Lösung abgedeckt werden.

Managementprotokoll

Als Managementprotokoll findet nach wie vor SNMP Einsatz im Systemmanagementbereich. Mittlerweilen wird seitens der Managementsysteme auch eine Unterstützung des „neuen“ SNMP v3 geboten, jedoch der Einsatz auf Komponentenseite (Router, Switches) lässt noch auf sich warten. Der Marktführer CISCO bietet die SNMP v3 Funktionalität in seinem IOS ab Version 12.0(3). Alle Systeme bringen bereits eine Vielzahl unterschiedlicher MIB`s gängiger Komponenten mit, die aber auch erweitert werden kann.

Ausserdem wird von den gängigen Tools das CDP (Cisco Discovery Protocol) auf Komponenten angewandt, die während des Discoveryprozesses als „Cisco Devices“ erkannt werden.

Layer 2 Management

Mittlerweilen findet sich, auch aufgrund der derzeit etablierten „geswitchten“ Netzwerke, volle Layer 2 Unterstützung in den derzeit am Markt positionierten Netzwerkmanagementsystemen wieder, oder kann durch den Erwerb von Zusatzprodukten realisiert werden (IBM Tivoli Switch Analyzer).

Die Umsetzung erfolgt in den Bereichen Discovery und Root-Cause Analyse.

Im Rahmen der Netzwerkdiscovery kann mit entsprechender Layer 2 Unterstützung die physikalische Konnektivität zwischen zwei zu verwaltenden Netzwerkobjekten ermittelt werden. Dadurch laesst sich auch der genaue Netzwerkpfad zwischen Objekten ermitteln und kann zu Diagnosezwecken herangezogen werden.

Die sogenannte Root-Cause Analyse unterstützt den Netzwerkoperator bei der Suche der Hauptursache nach einem im Netzwerk aufgetretenen Fehler und den daraus resultierenden Fehlerbenachrichtigungen, die am Managementsystem eintreffen. Sollte ein Switch ausfallen, werden normalerweise bei der nächsten Statusabfrage alle an diesem Switch hängenden Komponenten als Fehlerhaft diagnostiziert. Durch die vorhandenen Layer 2 Informationen im Managementsystem, lassen sich die an dem Switch angeschlossenen Komponenten identifizieren und den defekten Switch als „Root-Cause“ (Hauptursache) des Fehlers diagnostizieren. Dadurch wird entsprechend das Polling (Statusabfrage) auf die nicht zu erreichenden Komponenten solange unterdrückt, bis der Fehler behoben wurde, und das Netzwerk in den normalen Betriebsstatus überwechselt.

Funktionsabdeckung durch Produkte

Die derzeit auf dem Markt im Einsatz befindlichen Netzwerkmanagementsysteme (HP OV Network Node Manager, IBM Tivoli Netview, Aprisma Spectrum, Micromuse Precision -das auf den RiverSoft NMOS Techniken basiert - decken mit den vorhandenen Funktionalitäten hauptsächlich den Bereich des klassischen Fehlermanagements ab.

In den Einzelbereichen Fehlererkennung, -diagnose und Fehlerbehebung unterscheiden sich die Ausstattungen und Funktionalitäten der Produkte nur minimal.

Im Bereich Konfigurationsmanagement bieten die meisten Netzwerkmanagementsysteme zwar Basisfunktionen, der Einsatz eines produktspezifischen Elementmanagers wie CiscoWorks oder 3Com Transcend bleibt aber unerläßlich.

Ausserdem wird in keinem Netzwerkmanagement Tool die Möglichkeit geboten, Standortinformationen zu einem gemanagten Gerät zu hinterlegen. Da dies aber ein entscheidendes Kriterium zur Bewältigung der Netzwerkmanagementaufgaben ist, muss ein separates Assetmanagement geführt werden. Zusätzlich bietet ein konsequent gepflegtes Assetmanagement auch die Möglichkeit, Daten zwischen Netzwerkmanagementsystem und Assetmanagement abzugleichen. Eventuell kann auch die Konfiguration des Netzwerkmanagementwerkzeugs durch ein führendes Assetmanagement erstellt werden. Die Teilaufgaben Accounting und Performancemanagement finden zwar teilweise in den Netzwerkamangement-Tools Anwendung, müssen aber vor dem Hintergrund der Umsetzung von SLA`s (Service Level Agreements) mit dafür vorgesehenen Tools (Vital Suite, e-Health) veranstaltet werden. Der Bereich Sicherheitsmanagement bezieht sich bei Netzwerkmanagementsystemen lediglich auf die Absicherung der Managementumgebung gegen unbefugten Zugriff und die Ausfallsicherheit des Systems (Backup der Datenbanken, Übernahme von Diensten).

Sollten Sie Fragen zu den hier behandelten Themen haben, zögern Sie nicht, uns anzusprechen. Gerne stehen wir zu einem persönlichen Gespräch zur Verfügung.

Thomas Wollner
IT Beratung und Integration
Akazienstr. 46
52353 Düren
tw@wollner-net.de
www.wollner-net.de