Netzwerküberwachung

Die Überwachung des firmeneigenen Netzes bewegt sich im Spannungsfeld zwischen dem Aufspüren von Performance Engpässen und Sicherheitslücken, der Kostenrechnung (Accounting), den Sofortanalysen im Problemfall und den Langzeitanalysen zur Trenderkennung. Visualisierung des gesamten Netzwerkes mit MS Visio und MS Access Datenbank, inkl. Fehlererkennung und Langzeitüberwachung.

Wegen dieses weiten Spektrums von Anforderungen an die Netzüberwachung sollte man sich ein Instrumentarium schaffen, das von den verwendeten Netzwerkkomponenten möglichst unabhängig arbeitet. Andererseits liefern die vorhandenen Netzwerkkomponenten häufig wertvolle Messwerte. Um Investitionen in zusätzliche sog. Messprobes zu vermeiden, ist es sinnvoll, diese −kostenlosen− Werte mit in die Netzüberwachung einzubeziehen.

Man sollte sich allerdings auch der Einschränkungen bewusst sein. So lassen sich z.B. über SNMP von allen an einen managebaren Switch angeschlossenen Segmenten die Zahl der Broadcasts, Multicasts, sowie versch. Fehler abfragen. Will man aber die Netzlast abfragen, so teilt der Switch bzw. Router in der Regel nur die über den jeweiligen Port geleitete Last mit, und nicht die innerhalb des Segmentes selbst herrschende Last.

Auch wird nicht mitgeteilt, welche Verbindungen gerade aktiv sind. Wer an der letzten Fragestellung interessiert ist, (d.h. *wer redet mit wem wieviel über welchen Port*) muss entweder doch zusätzliche Probes installieren, oder Switche bzw. Router einsetzen, die NetFlow* − Daten aussenden können.
Ausgefeilte, auf den Kunden und seine Anforderungen zugeschnittene Überwachungstools können natürlich Alarme per SMS verschicken und sogar Umkonfigurationen vornehmen, aber sie müssen bei jeder Netzänderung angepasst werden. Dies ist ein Dauerjob, der erhebliche Manpower kosten kann.

RzK hat bei vielen seiner Kunden gesehen, dass eine Langzeitüberwachung des Netzes sehr sinnvoll sein kann. Im Fehlerfall sollten möglichst viele Daten vorhanden sein. Zum Teil bekommen die Daten erst im Nachhinein Bedeutung. Automatisierte Tools, die möglichst viele Daten "vollautomatisch" sammeln kosten wenig Manpower. Eine Netzüberwachung sollte Ethernet bzw. IP Monitor und Recorder, SNMP−Abfrage, Flow Analyse, Station Detection, tägliche Statistiken, Intrusion und VLAN Detection, momentane und tägliche Hitlisten, Erreichbarkeitstests und das alles "Web"−gerecht bieten.

---

*NetFlow ist ein eingetragenes Warenzeichen von Cisco Inc

Aspekte der Netzüberwachung

- Performance
- Sicherheit
- Accounting
- Qualitäts − Sicherung