

SWITCHING UND REMOTE-MONITORING

SNMP über den Mund gefahren

Switching hat das Monitoring und die Analyse von Netzwerken im Vergleich zu klassischen Ethernet-Netzen um ein Vielfaches komplexer und aufwändiger gemacht. Insbesondere beim Remote-Monitoring stört es daher ungemein, dass das fast in jedem Netz als Managementgrundlage dienende SNMP-Protokoll so "geschwätzig" ist. Schon ohne nennenswerte Nutzdaten sorgt oft allein der SNMP-Verkehr für eine hohe Auslastung des Netzes – im WAN natürlich verbunden mit entsprechenden Kosten. Obwohl niemand SNMP wirklich über Bord werfen will, gibt es dennoch Ansätze, der "heiligen Kuh" etwas auf den Pelz zu rücken.

Monitoring ist nach wie vor ein essenzieller, unverzichtbarer Job jedes Netzwerkmanagers – dienen die hierbei erfassten Daten doch oft als Grundlage für die Erweiterung oder Umstrukturierung des Netzes.

In vielen Fällen liefert Monitoring den richtigen Ansatz für Intervention in das Netzwerk zwecks Optimierung oder gar Fehlerbeseitigung.

Während man unter lokalem Monitoring traditionell die Auslotung eines lokalen, geschalteten LANs verstand, meinte man mit klassischem Remote-Monitoring beispielsweise die Messung in WAN-gebundenen Segmenten. Durch den Einsatz intelligenter Komponenten wie LAN-/WAN-Switches oder Router verändert sich für den Manager die Sichtweise seiner Netz-

werke erheblich: Während man früher wenige Segmente lokal wie remote verwalten musste, scheint die Zahl der LAN-Segmente in modernen Strukturen förmlich zu explodieren. Ein Switch mit bei-

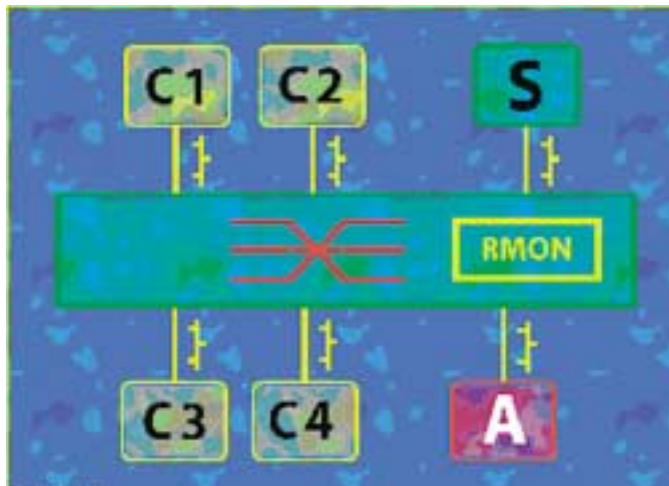


Bild 1. Embedded RMON basiert auf integrierten RMON-Agenten innerhalb der Switches
C=Client, S=Server, A=Analyse-Plattform, R=Router

spielsweise 24 Ports vergrößert die Anzahl der LANs um 24 Segmente (Collision-Domains), jedes mit einem Eigenleben hinsichtlich Last, Paketaufkommen,

Fehlerrate etc. Mit dem Einsatz der Full-Duplex-Technologie verdoppelt sich die Zahl der Segmente nochmals, da hierbei ein vollkommen separiertes Sende- und ein Empfangssegment pro Port realisiert sind.

Remote-Monitoring beginnt also bereits hinter dem ersten lokalen Switching-Port, auf dem man mit dem Messsystem angehängt ist. Für den Administrator einer komplexen geschalteten Netzumgebung stellen sich nun eine Reihe sehr unbequemer Fragen: Wie viele Segmente sollte oder müsste man überwachen? Wie viele Probes, also Messwertaufnehmer, benötigt man, beziehungsweise, kann man sich unter ökonomischen Gesichtspunkten leisten? Welche Details sollten von diesen nunmehr Mikrosegmenten aufgezeichnet und analysiert werden? Und – last not least – mit welcher Methode können die gewünschten Analysedaten am besten beschafft werden? Folgende Lösungsansätze bieten sich zur Überwachung in komplexen Strukturen an:

KLASSISCHES TROUBLESHOOTING "ON DEMAND"

Der Messkoffer, der dem Analysten von Zeit zu Zeit durch Umschalten in Segmenten dienlich ist, war früher nicht wegzudenken. Um bei Switching-LANs die Segment-(also: Port-) Informationen mitschneiden zu können, benötigt man einen Hub (Konzentrator), den man über ein Kreuzkabel an den Switch anbindet. An diesen Hub schaltet man nun wieder den Server an. Diese Methode ist jedoch bestenfalls für Notfälle geeignet, nicht für konstantes Monitoring und Management. Die Gründe liegen auf der Hand:

- Für jede Messung an einem anderen Port muss die Verbindung kurz unterbrochen werden.
- Die Duplex-Fähigkeit des Switch-Ports geht verloren.
- Messungen sind nicht an mehreren Ports gleichzeitig möglich.

MIRROR-PORT-ANALYSE Einen Ausweg bietet die Verwendung eines Analysators oder von Probes in Verbindung

mit einem Spiegel-Port (Mirror- oder auch Span-Port): Diese Methode ist ein probates Mittel zur Vermeidung von "Stöpselarbeit", das heißt, der zu analysierende Port wird permanent auf einen speziell als Mess-Port definierten Anschluss kopiert. Jedoch gibt es auch hier Probleme beziehungsweise Einschränkungen:

- a) Oftmals können nur ein oder wenige Ports als Spiegel-Port definiert werden.
- b) Wie spiegelt man einen Duplex-Port mit 2 mal 100 MBit/s auf einen "gewöhnlichen" Spiegel-Port, der ja an der Schnittstelle zum Analytiker nur einmal 100 MBit/s Sendekapazität hat?

- c) Roving-Mirror-Ports (ständig wechselnde Beobachtung der gesamten Ports) bringen oft mehr Verwirrung als Übersicht.

Außerdem – wer glaubt, alle Fehler (besonders die physikalischen und logischen auf Layer-2) eines Netzes via Mirror-Port analysieren zu können, der irrt. Die ASIC-Backplane eines Switches ist für den rasend schnellen Versand von

korrekten Paketen konzipiert, nicht für die Übertragung von defekten Datenströmen. Defekte Frames werden schlichtweg verworfen, sind daher für den Analytiker oder die Probe auch nicht sichtbar. Vorsicht ist auch in Verbindung mit

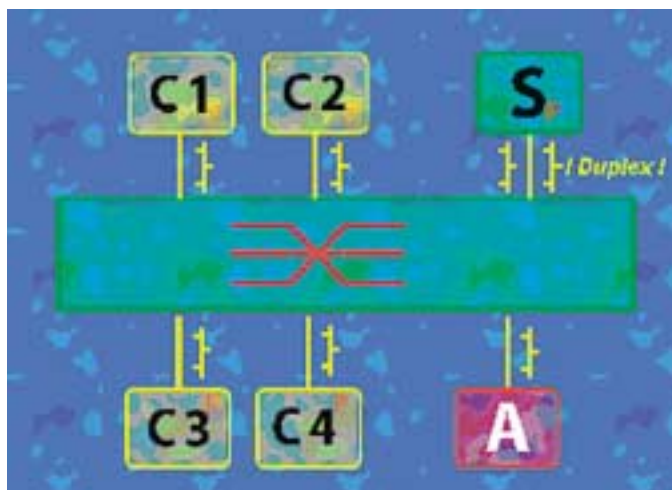


Bild 2. Durch Integration der Analyseagenten in die Zielsysteme erfolgt die Sammlung von Messwerten in praktisch allen LAN-Segmenten

VLANs geboten. Unsachgemäße Konfiguration kann zu heimtückischem Fehlverhalten der Komponenten führen.

RMON-ANALYSE MIT DEDIZIERTEN PROBES Eine weitere Methode ist die Verteilung von dedizierten RMON-Agenten im Netzwerk. Dies liefert reiche Details aus den LAN-Segmenten. Leider gibt es auch hier einige Fußangeln:

- a) Diese Methode ist sehr kostspielig und

aufgrund der heute enormen Port-(Segment-)Dichte nicht mehr praktikabel.

- b) Der Anschluss an das zu messende Medium ist problematisch: Man muss für jeden Port einen zusätzlichen Hub zwischenschalten.
- c) Auch hier geht die Duplex-Funktion des gemessenen Ports verloren, es sei denn, man verwendet spezielle Duplex-Probes inklusive der so genannten Century-Taps. Dies treibt die Kosten nochmals drastisch in die Höhe.

EMBEDDED-RMON-ANALYSE MIT INTEGRIERTEN PROBES

Einen vielversprechenden Ansatz bieten die modernen Switches selbst: Embedded RMON basiert auf integrierten RMON-Agenten innerhalb der Switches (Bild 1). Das ist allerdings nur dann hilfreich, wenn lediglich globale Statistiken und keine Details erforderlich sind. Die meisten Switching-Komponenten bieten nämlich nur Teilbereiche der RMON-Gruppen an, zum Beispiel 1, 2, 3 und 9. Wer mehr will, muss oft tief in die Tasche greifen. Oftmals wird außerdem unterschlagen, dass Switches erheblich unter der zusätzlichen Last der RMON-Funktion "leiden", womit sich erklärt, warum bei den meisten Herstellern diese Funktion per Default ausgeschaltet ist.

SNMP: DER "NATÜRLICHE FEIND" VON RMON

Sicher ist der Administrator gut beraten, zur Netzwerkverwaltung auf einen Standard zu setzen. SNMP (Simple



Network Management Protocol) hieß das Zauberwort, mit dem ursprünglich im Auftrag des amerikanischen Verteidigungsministeriums (DoD) Ende der 80er-Jahre eine Lösung für wirklich globales Networkmanagement auf den Weg gebracht wurde. Ein wenig aus einer Verlegenheit heraus nahm man seinerzeit ein bereits vorhandenes SGMP (Simple-Gateway-Management-Protocol) und formte hieraus flugs den neuen Dienst. Der Erfolg und die Verbreitung der ersten Generation des SNMP (Version 1) war atemberaubend. Heute sind praktisch vom kleinsten Router bis zum großen ATM-Carrier-Switch alle halbwegs intelligenten Komponenten mit SNMP-Support ausgestattet. SNMP ist einer der meistverbreiteten Dienste der Kommunikationswelt überhaupt und damit ein aus der Industrie heraus gewachsener De-facto-Standard. Über die durchaus gut gemeinte CMIP-Konkurrenz aus dem Hause ISO (CMIP war der offizielle Standard von der International Standards Organisation) spricht heute niemand mehr.

HP, Tivoli, Concord und viele weitere Unternehmen, die sich weitgehend auf die Nutzung des SNMP-Standards konzentrieren, bieten eine Fülle von sehr professionellen Werkzeugen zur Erreichung der idealen "Five-Nines", also einer Netzwerk-Uptime von 99,999 Prozent (was in etwa einer Ausfallzeit von rund fünf Minuten pro Jahr entspricht). Hier hat sich eindeutig SNMP als einfacher aber zweckmäßiger Standard bewährt. Kratzt man jedoch objek-

tiv am Lack des Protokoll-Stacks, so drängen sich eine Reihe von Merkwürdigkeiten ins Blickfeld. Die Entwickler des Standards SNMP haben wohlweislich niemanden im Unklaren darüber gelassen, dass es sich bei dem Produkt der Bemühungen um eine "simple" Lösung handelt und nicht etwa um ein "komplexes" oder gar "intelligentes" Network Management Protocol. Ohne die zweifelsfrei wertvollen Funktionen des Standards zu schmälern, hier einige Details aus der Problemecke:

- SNMP ist (in der verbreiteten Version 1) unsicher, da die Passwortvariablen (Community), die einen Schutz vor unerlaubtem Zugang zu den verwalteten Systemen geben sollten, in Klartext durch einfachste Capture-Werkzeuge sichtbar gemacht werden können.
- Auch die Transportbasis des SNMP ist nicht sicher. Traps, auch diejenigen, welche eine überaus wichtige Warnmeldung für den Netzwerkadministrator beinhalten, werden nach dem Prinzip Hoffnung per UDP als ungesicherte Datagramme übertragen.
- SNMP ist bandbreitentechnisch extrem ineffektiv – insbesondere über WAN-Verbindungen sind die SNMP-Daten (Management-Overhead) regelrechte Nutzdatenkiller. Das Netzwerk, das man mit dem Managementsystem zu optimieren gedenkt, wird durch die Massen an Statistik- und Messinformationen oft schon bis an seine Grenzen ausgereizt. Besonders drastisch wird das Phänomen, wenn man auf das vorhandene SNMP noch eine RMON-Applikation aufsetzt. Liest man beispielsweise die Konversa-

tionstabelle eines RMON-Agenten aus, so werden pro Konversation rund 4 etwa 250 Byte große Pakete benötigt. Dies bedeutet, dass in selbst mittleren LAN-Segmenten ein Retrieval von zum Beispiel 500 LAN-Konversationen eine Datenmenge von etwa einem halben Megabyte produziert. Dies ist das Datenvolumen einer RMON-Gruppe, insgesamt gibt es neun beziehungsweise zehn (inklusive Token Ring) solcher Gruppen. Man kann sich sehr leicht vorstellen, was dies für ein WAN bedeutet.

- Die vom SNMP zur Verfügung gestellten Statistik-Counter, also zum Beispiel die Zählregister für Received Packets, Bytes, Errors etc. sind mit einer Breite von 4 Byte versehen. Nach einer Anzahl von rund 4,3 Milliarden "Increments" werden die Registerinhalte ähnlich einem Stromzähler "über Null" gedreht und beginnen wieder von vorne. Vor zwölf Jahren galten derartig große Zahlen als vollkommen praxisgerecht, heute benötigt ein Gigabit-

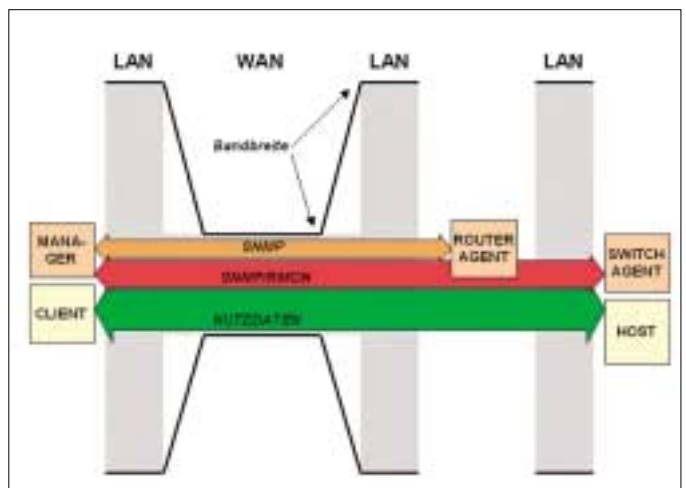


Bild 3. Klassischer SNMP-Ansatz

Uplink nur wenige Minuten unter "Dampf", um die Zählerwerte des SNMP-Registers zu überdrehen. Dies bedeutet, dass ohne ständigen Interventionskontakt zu den Agenten die Statistikdaten der SNMP-Systeme unbrauchbar werden können, sofern sie nicht in kurzen Abständen wiederholt

