FORSCHUNGSZENTRUM JÜLICH GmbH
Zentralinstitut für Angewandte Mathematik
D-52425 Jülich, Tel. (02461) 61-6402

Interner Bericht

RMON in Switch-basierten Umgebungen Beta-Test eines Network Analysis Moduls für Catalyst 6500 Switches der Firma Cisco Systems

Olaf Mextorf

FZJ-ZAM-IB-2001-15

Dezember 2001

(letzte Änderung: 20.12.2001)

Inhaltsverzeichnis

1 Einleitung

Mit der Markteinführung der Ethernet Switch Familie Catalyst 6500 hat die Fa. Cisco Systems im Jahre 1999 ein Produkt etabliert, das aufgrund seiner hohen Portdichte, seiner leistungsfähigen Backplane-Architektur und der Integration von Layer 2- und Layer 3/4-Forwarding-Funktionalität insbesondere im Backbone-Bereich moderner lokaler Netzwerke als wesentliche Netzwerkkomponente zum Einsatz kommt.

Der massive Einsatz von Switch-basierten Ethernetanschlüssen hat jedoch für das Netzwerk Monitoring zur Folge, daß die bisher auf Bus- bzw. Repeater-basierenden Ethernet-Topologien aufbauenden Analysewerkzeuge aufgrund der Verkehrsseparation durch einen Switch keinen Zugriff mehr auf den in einem Netz laufenden Verkehr haben.

Dieses Problem konnte durch den Einsatz externer Analysegeräte (Probes) in Kombination mit einer Verkehrsspiegelung zum Analysator innerhalb des Switches gemildert werden. Solche externen Probes sind neben reinen „Sniffer“-Systemen oftmals RMON-basierte Geräte, die auch über längere Zeit ein kontinuierliches Mitschreiben von Netzwerkparametern und –statistiken ermöglichen.

Der Gegenstand der Kooperation, das Network Analysis Modul (im folgenden kurz NAM genannt) für Switches der Catalyst 6000 Familie, bietet nun die Funktionalität eines externen Analysators plus zusätzliche Features in Form eines in den Switch integrierten Moduls.

Die Vorteile einer solchen integrierten Lösung liegen in dem durch den Backplane-Anschluß potentiell höheren Datendurchsatz zum Analysator, in der engeren Kopplung mit dem den zu analysierenden Verkehr bereitstellenden Switch, insbesondere unter Konfigurations- und Managementaspekten, sowie in der Unterstützung zusätzlicher Cisco-interner Analysemethoden, wie z.B. der Auswertung von im Switch generierten Informationen zu Packet-Flows (Switch-Port, Layer-2-, -3- und –4-basierenden Statistiken zu allen weitergeleiteten Paketen eines Switches).

Im Rahmen der Kooperation wurden Vorserienmodelle des NAM in verschiedenen Switches des ZAM unter unterschiedlichen Randbedingungen (weitere Module, unterschiedliche Netzwerklast und –protokolle, unterschiedliche Client-Software und Analysetechniken) getestet. Die Ergebnisse der Tests gingen in dem oben genannten Zeitraum in die Entwicklung und Fertigstellung der endgültigen Version des NAM ein, das im Juni 2000 von Cisco offiziell als Produkt angekündigt wurde.

2 Historie

2.1 Klassisches Ethernet in Bus-Topologie

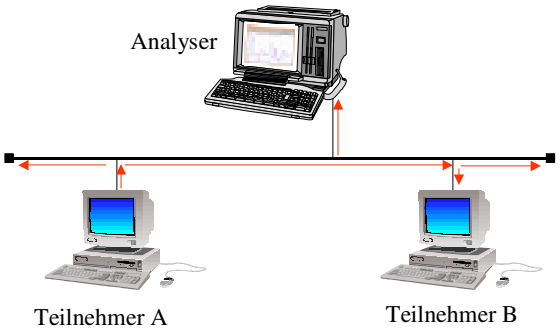

Abbildung 1: Verkehrsanalyse im Ethernet in Bus-Topologie

Beim klassischen Ethernet in Bus-Topologie, das unter Verzicht auf jegliches Bridging lediglich aus durch Repeatern verbundenen Thick- und Thinwire-Segmenten bestand, konnte durch den Einsatz eines Netzwerkanalyse-Tools an jeder beliebigen Stelle in einer Broadcast-Domain jeweils die gesamte in dieser Domain laufende Kommunikation analysiert werden. Was aus Netzwerkteilnehmersicht ein eindeutiger Nachteil war, nämlich das dynamische Aufteilen eines Netzwerkmediums mit fester Bandbreite (z.B. 10 Mbit/s) unter vielen Teilnehmern, war aus Sicht der Statistikerfassung und Analyse im Netz ein großer Vorteil. Zu diesen Zeiten wurden zur Analyse im wesentlichen dedizierte Analyse-Tools, wie z.B. Sniffer-Systeme, oder aber auch übliche Netzwerkteilnehmer mit einem im Promiscous-Mode arbeitenden Ethernetadapter und passender Software, wie z.B. tcpdump, eingesetzt.

2.2 Hubs

Im weiteren Verlauf der Ethernet-Entwicklung wurden verstärkt Hub-Systeme eingesetzt, die über verschiedene Schnittstellen (seriell, Telnet, SNMP) managebar waren und Repeater-Funktionalität für mehrere Broadcast-Domains („Ethernets“) mit hoher Portdichte flexibel zur Verfügung stellten. Gleichzeitig wurden die Bus-basierenden Übertragungstechniken, wie z.B. 10Base2, durch Punkt-zu-Punkt

Übertragungsstandards im Ethernet, wie z.B. 10BaseT und 10BaseFB/FL, ersetzt. Beides führte dazu, das in den Netzen zwar weiterhin die Broadcast- und die Collision-Domains deckungsgleich waren, aufgrund der Übertragungstechnik jedoch ein einfaches „Einschleifen“ von Analyse-Tools nicht mehr möglich war.

Gleichzeitig begannen die Hersteller von Hub-Systemen Analyse-Tools in ihre Systeme einzubauen. Als Beispiel sei hier das Corebuilder 5000 System von Chipcom bzw. 3Com genannt, das u.a. 8 getrennte Ethernets auf der Backplane und bis zu 4 zusätzliche lokale Ethernets auf einem Modul führt, denen beliebig Ports zugeordnet werden können. Auf einem beliebigen Modul aufgesteckte Management- bzw. Analyse-Tochter-Boards konnten dann, ebenso wie externe Analyser, diesen Ethernets (Broadcast- und Collision-Domain) zugeordnet werden und den Verkehr beobachten.

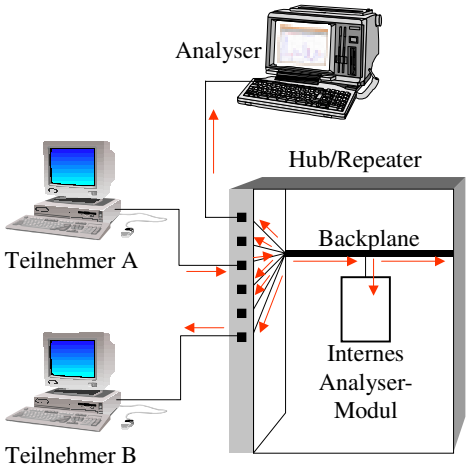

Abbildung 2: Verkehrsanalyse im Hub/Multiport-Repeater

Zur Verwendung kamen im Falle des Corebuilder 5000 Systems die Tochter-Boards 6100D-MGT und 6100D-AMGT, von denen das erste die RMON1-Gruppen Statistics, History, Host, Host Top N, Matrix, Event und Alarm unterstützte und das zweite zusätzlich Packet Filtering und Capturing sowie proprietäre RMON2-Funktionalität auf der Basis von zusätzlicher, u.a. mit der RMON-Client Software LANsentry ladbarer Software (ECAM, „Enterprise Communications Analysis Module“), bot. Die Möglichkeit des Packet Capturing, wenn auch mit lediglich 12 MB Speicher auf dem Board, bei geeigneter Filtersetzung sowie die zusätzlichen, durch das Laden der ECAM-Software auf das Management-Tochter-Board erhältlichen Layer-3 Statistiken zu einem Zeitpunkt, als RMON2 noch nicht standardisiert war, boten in Kombination mit der flexiblen Zuordnung der Tochter-Boards zu Broadcast-Domains (internen Ethernets) eine umfassende Möglichkeit der Verkehrserfassung und Fehlersuche in 10Mbit/s Ethernet-Segmenten. Übrigens boten Chipcom bzw. 3Com damals durch den Support der selbst entwickelten PACMIB („Port Address Correlation MIB“) bereits

bei den Repeater-Modulen die Möglichkeit, die MAC-Adressen der an einem Port angeschlossenen Teilnehmer auszulesen (unabhängig von der dot1dBridge-MIB).

Die später für den Corebuilder 5000 erhältlichen Switch-Module, wie z.B. die der 66xxM-Familie, die mit internem Zugriff auf die Switch-Backplane (2.4 GBit/s) ein Bridging zwischen den eigenen Ports und den Ports weiterer Switch-Module ermöglichten, wobei die Ports in VBridges, den Vorläufern der VLANs, organisiert waren, ermöglichten die Nutzung des jeweiligen Switch-Modul-Prozessors als RMON-Analyser. Wie in aktuellen Switches konnte ein beliebiger Port eines Switch-Moduls entweder zu einer externen Probe oder aber zu einem Modulprozessor (auch modulübergreifend) zwecks Analyse gespiegelt werden. Die Möglichkeiten bei der RMON-basierten Analyse auf einem Switch-Modul-Prozessor blieben jedoch in Bezug auf die unterstützten RMON-Gruppen hinter den Möglichkeiten der Tochter-Boards zurück (sowohl Capturing als auch die RMON2-Erweiterung mit ECAM konnten nicht genutzt werden).

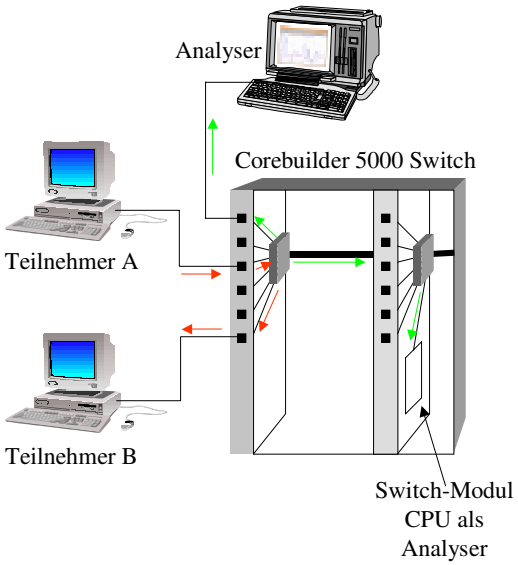

Abbildung 3: Verkehrsspiegelung zu einer Switch-Modul CPU und einem externen Analyser

2.3 Stackable Switches

Stackable Switches, wie z.B. die SuperStackII 3300 Serie von 3Com, bieten die standardmäßig aktivierten RMON-Gruppen Statistics, History, Alarm und Events für alle Ports (incl. der VLANs, die als „virtuelle“ Ports realisiert sind) an und erlauben, in Abhängigkeit von den verfügbaren Ressourcen CPU und Memory auf dem Switch, die Definition zusätzlicher Host, Host top N und auch Matrix Einträge für einzelne Ports.

3 Cisco Catalyst Layer 2/3 Switches

Die folgenden Angaben beziehen sich im wesentlichen auf die Switch Familien Catalyst 6000 und z.T. auch Catalyst 4000 der Fa. Cisco Systems.

3.1 Mini-RMON Implementierung

Auf den Switches kann eine Mini-RMON Implementierung genutzt werden, die für alle Ports bzw. Interfaces die RMON1-Gruppen 1-3 und 9 (Statistics, History, Alarm und Event) zur Verfügung stellt.

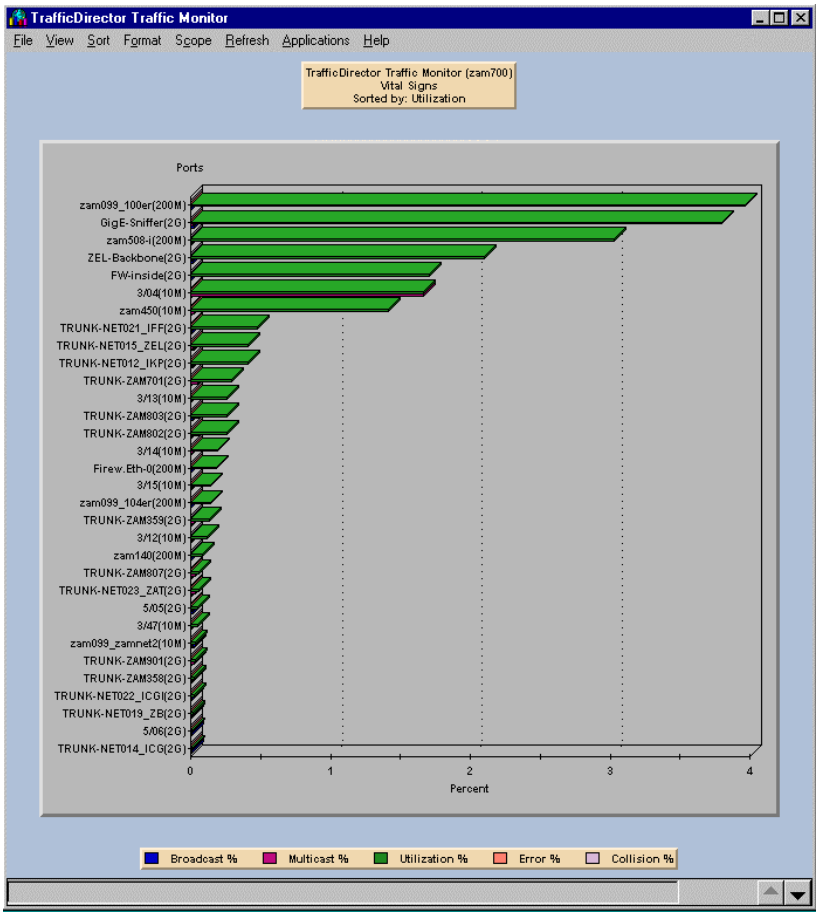

Abbildung 4: Mini-RMON zur "alltäglichen" Switch-Überwachung

Das Spiegeln des Verkehrs ist nur zu einem externen Analyser möglich; eine interne, über die oben erwähnten RMON-Gruppen hinausgehende Analyse, z.B. mit der CPU- und Memory-Leistung der Supervisor-Engine (wie z.B. beim 3Com Corebuilder 5000), die bei diesen Switches ohnehin für alle Ports die Forwarding-Engine ist und somit den gesamten Verkehr bearbeitet, ist nicht vorgesehen. Diese Lücke soll für die Catalyst 6000 Systeme durch das Network Analysis Modul geschlossen werden.

3.2 Port-Spiegelungen (SPAN und RSPAN)

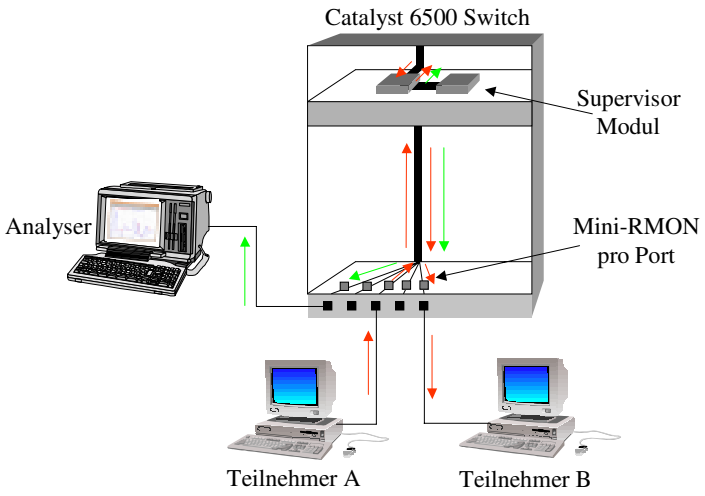

Abbildung 5: Verkehrs-Spiegelung (SPAN) zu einem externen Analyser

Um zu analysierenden Verkehr einem externen Analyser zuzuführen, ist bei den Catalyst Switches eine Spiegelung dieses Verkehrs mit Hilfe der SPAN-Funktion (Switch Port Analyser) möglich. Als Quelle des zu untersuchenden Verkehrs können sowohl ein einzelner Port (incl. Trunk Ports) als auch eine Gruppe von Ports (incl. Channels) oder auch ganze VLANs herangezogen werden. Die Anzahl gleichzeitig konfigurierbarer Verkehrsquellen und auch die Anzahl paralleler SPAN-Sessions ist abhängig von der Switch-Familie, der Version der Supervisor-Engine und auch der Betriebssystem-Version (CatOS-Version) des Switches. Beim Spiegeln des Verkehrs wird nach dem Treffen der Forwarding-Entscheidung durch die Supervisor-Engine neben dem tatsächlichen Ausgangsport des bearbeiteten Paketes auch dem SPAN-Destination-Port das Lesen des Paketes auf dem Datenbus angewiesen.

Nachteile der Verkehrs-Spiegelungs-Technik gegenüber dem klassischen Einschleifen eines Analysers liegen insbesondere in der nicht 100%ig erfolgenden Spiegelung allen Verkehrs. So werden z.B. Fehler auf den unteren Layern durch die MAC-Schicht des Source-Ports bereits korrigiert und nicht bis zum SPAN-Port weitergeleitet. Ebenso erfolgt eine Interpretation von MAC-Protokollen, wie z.B. SpanningTree und CDP, bereits vor der Verkehrsspiegelung; diese werden zumindest im Falle von RSPAN (s.u.) nicht weitergeleitet. Gleichzeitig bietet die Verkehrsspiegelung in der Realisierungsform der Catalyst Switches natürlich die Möglichkeit, mit einem Analyser zeitgleich den Verkehr mehrerer Quellen zu analysieren.

Eine Erweiterung der SPAN-Funktionalität stellt bei den Catalyst 6000 Switches die RSPAN-Funktion (Remote-SPAN, Abbildung 6) dar. Bei ihr können Quelle und Ziel des zu spiegelnden Verkehrs auf unterschiedlichen Switches liegen. Die Hardware- und Software-Anforderungen an die beteiligten Switches zur Nutzung dieses Features liegen allerdings etwas höher (der Source-Switch muss z.B. eine Supervisor-Engine mit Policy-Feature-Card (PFC) oder Multilayer-Switch-Feature-Card (MSFC) haben).

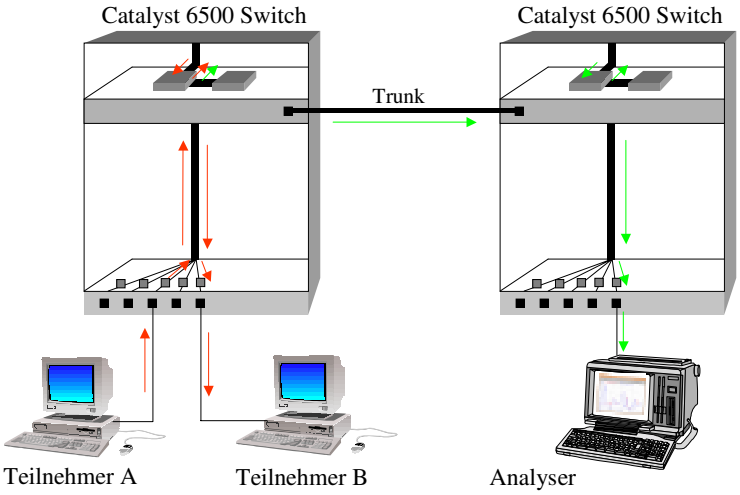

Abbildung 6: Verkehrs-Spiegelung zu einem Analyser an einem zweiten Switch (RSPAN)

4 NAM Beta-Test

4.1 Allgemeines / Testablauf

Das erste NAM wurde am 29.03.2000 geliefert. Die zugehörige Dokumentation war über einen FTP-Server bei Cisco abrufbar. Sie umfaßte folgende Dokumente:

- „Catalyst 6000 Command Reference“ für die Version 6.1
- „Catalyst 6000 Network Analysis Module Installation and Configuration Note“
- „Ft. Lauderdale 0.34 Release Notes“ mit bereits bekannten Bugs incl. Ids
- „Catalyst 6000 NAM Release 1.1(0.8a) Caveats“ mit prakt. Tips zur aktuellen Hardware-/Software-Version des NAM (was bereits bzw. noch nicht funktioniert, bekannte Probleme u.a. auch mit Ft. Lauderdale 0.34 und TrafDir 5.8a)
- „6KNAM Quick Start User’s Guide with TrafficDirector 5.8 ver 110“
- „Using the Traffic Director Application“

Auch die ebenfalls zu testende, zugehörige Beta-Software war über einen FTP-Server bei Cisco abrufbar. Dazu zählte die CatOS-Version 6.1(0.34)FTL für den Catalyst 6500 (gleichzeitig erste Voice-over-IP-Version) und eine Vorversion des Traffic Director V5.8.

Während der Tests (ca. 14 Wochen) wurde wöchentlich ein umfassender Report über durchgeführte Tests, deren Ergebnisse und auffällige Probleme an den Beta-Test Koordinator Mike Candalaria bei Cisco Systems gesandt. Bei erkannten Problemen wurden dann detailliert Testergebnisse und weitere Teststrategien mit dem Entwickler-Team besprochen und realisiert.

Nach 9 Testwochen mit der Test-Hardware 1 und der CatOS-Version 6.1(0.34)FTL wurde mit einer zweiten Test-Hardware (V1.1(0.17)) und der CatOS-Version 5.5(0.69) weitergearbeitet. Dieses zweite NAM wurde wiederum nach ca. 2 Wochen durch einen Software-Upgrade auf den Stand V1.1.1 gebracht und mit der CatOS-Version 5.5.1 betrieben.

Die Network Analysis Module wurden während der Testphase in mehreren unterschiedlich ausgestatteten und ausgelasteten Catalyst 6500 Switches betrieben.

4.2 Aufbau des NAM

Das Network Analysis Modul für den Catalyst 6000 Switch benötigt einen Slot im Switch und ist auf der Basis einer 533 MHz Pentium III CPU mit 256 MB RAM und Festplatte sowie eines UNIX- Betriebssystems, das für den Switch-Administrator nicht sichtbar ist, aufgebaut. Für die RMON-Tabellen stehen insgesamt 256 MB zur Verfügung; bis zu 70 MB davon für den Capture Buffer.

Es stellt in gewissem Sinne eine in Modulform gebrachte RMON-Probe dar, der jedoch, zumindest theoretisch, aufgrund der direkten Anbindung an den Switch-Bus

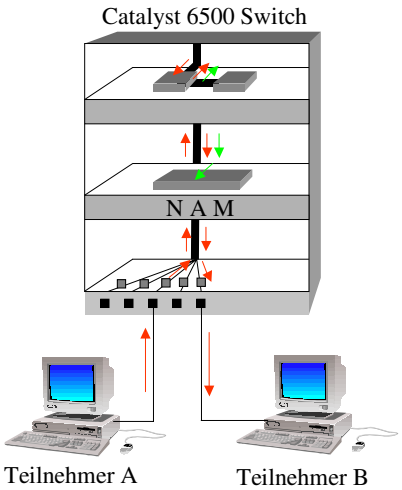

Abbildung 7: das NAM als interne Probe/Analyser im Catalyst 6500

eine Gesamtsicht auf den Verkehrsfluß im Switch möglich ist.

Konfiguriert werden kann das NAM über eine von der Switch-Konsole aus aufzubauende Konsol-Session oder über eine Telnet-Verbindung. Dabei arbeitet das NAM mit einer eigenen IP-Adresse, die automatisch dem VLAN zugeordnet ist, in dem sich auch das Management-Interface des Switches (sc0) befindet.

Die Konsolfunktionalität beschränkt sich auf die Konfiguration einiger weniger Parameter wie IP, SNMP und Autostart-RMON-Kontrolleinträge, das Verwalten der UserIDs/Passwörter und Rebooten des Moduls. Außerdem läßt sich auf dem NAM ein Coredump sowie ein detaillierter Report über die NAM-Konfiguration (incl. der RMON-Kontrolleinträge und –Ressourcen) und die das NAM betreffende Konfiguration des Switches erzeugen. Aufgrund des eigenständigen Betriebssystems mit Festplatten-basierendem Filesystem des NAM ist ein Herunterfahren des Moduls mittels „shutdown“-Befehl oder durch Drücken eines entsprechenden Knopfes an der Frontblende des Moduls vor jedem „Power Off“ (Herausziehen des Moduls, Ausschalten des Switches) unbedingt notwendig. Nachfolgend ist beispielhaft ein Login und Reboot auf dem NAM zu sehen:

```
zam700> (enable) sess 9
Trying NAM-9...
Connected to NAM-9.
Escape character is '^]'.

Cisco Network Analysis Module (WS-X6380-NAM)

login: root
Password:

Network Analysis Module (WS-X6380-NAM) Console, 1.1(1a)
Copyright (C) 1999, 2000, Cisco Systems, Inc.

root@zam702.zam.kfa-juelich.de# ?
show         - show system parameters
ip           - set ip parameters
snmp         - set snmp parameters
config       - set or clear config and config files
exsession    - disable outside logins
password     - set new password
shutdown     - shutdown the system
reboot       - reboot the system
coredump     - retrieve the coredump file
autostart    - enable/disable autostart collections
logout       - logout of system
exit         - logout of system
help         - display help screen
?            - display help screen

root@zam702.zam.kfa-juelich.de# show snmp

SNMP Agent:   zam702.zam.kfa-juelich.de   134.94.172.195

SNMPv1:  Enabled
SNMPv2C: Enabled
SNMPv3:  Disabled

community   write_comm_1  write
community   write_comm_2  write

sysDescr          "Catalyst 6000 Network Analysis Module (WS-X6380-NAM)"
sysObjectID       1.3.6.1.4.1.9.5.1.3.1.1.2.223
sysContact        "O. Mextorf, Tel. 2519 oder 74-502"
sysName           ZAM702
sysLocation       "ZAM, Geb.16.3, Raum 1"
```

```
root@zam702.zam.kfa-juelich.de# config clear
Reset the RMON configuration? (Y/N) [N]: y

root@zam702.zam.kfa-juelich.de# reboot
Reboot the NAM? (Y/N) [N]: y

System reboot in process...
root@zam702.zam.kfa-juelich.de#
Broadcast message from root Wed Nov 14 10:18:37 2001...

The system is going down for system halt NOW !!

root@zam702.zam.kfa-juelich.de# zam700> (enable)
zam700> (enable)
```

4.3 Durchgeführte Tests

Bei den Tests wurde die Zusammenarbeit des neu entwickelten NAM mit den das NAM beherbergenden Catalyst 6500 Switches und den jeweils dort vorhandenen Modulen untersucht. Weiterhin wurde die Interoperabilität mit der RMON-Software Traffic Director V5.8 (Frontier Netscout) und LANsentry Version 5.2.3 (aus der 3Com Transcend Management Suite) getestet. Es wurden verschiedenen Verkehrsquellen benutzt, darunter einzelne Ports (10, 100 und 1000 Mbit/s Ethernet), Port-Gruppen, Trunk-Ports und VLANs. Das Testen von VLAN-spaning war erst mit der zweiten Version der Testhardware möglich (siehe Problem 3 weiter unten). Weiterhin wurde in der Beta-Version des Traffic Directors das Port Roving (SMON), also das direkte Konfigurieren von SPAN-Sessions mit dem NAM als Ziel mittels Traffic Director unter Umgehung des Command Line Interfaces (CLI, „Konsole“) des Switches, noch nicht unterstützt.

4.4 Details zu den Tests

4.4.1 RMON1/2

Die Tests überstrichen alle RMON1-Gruppen incl. Capturing sowie die Protokoll- und Applikations-bezogenen Statistiken der RMON2-Gruppen.

Bei den Tests mit den RMON1-Gruppen Statistics, History (Short- und Long-Term), Hosts, TopN sowie Matrix traten keine großen Probleme auf. Das NAM arbeitete nach Konfiguration und Erzeugung entsprechender RMON-Kontrolleinträge über ein mitgeliefertes Property-File sowohl mit LANsentry als auch mit dem Traffic Director problemlos. Lediglich bei der Auswahl und der Konfiguration der Probe-Interfaces zeigte sich der Traffic Director etwas hakelig (s.u. „Sichtbarkeit der Interfaces“). Oftmals wurde z.B. bei der Konfiguration eines NAM-Interfaces als Agent im Configuration Manager des Traffic Director der Network-Typ (wie z.B. „FastET-FDX“) nicht korrekt erkannt und falsch besetzt.

Bei der Definition von Alarmeinträgen und auch der Filterdefinition und -allokation mittels LANsentry auf dem NAM kam es jedoch häufig zu einem Verlust der SNMP-Konnektivität zum NAM (siehe Problem 2). Ebenso ging die SNMP-Verbindung zum ersten Beta-Test-NAM oft bei dem Versuch, mit LANsentry RMON2 Protokoll- und Applikations-Statistiken („virtual interfaces“) zu erfassen, verloren.

Die gleichen Aufgaben erledigte das NAM in Verbindung mit dem Traffic Director grundsätzlich nahezu ohne Probleme. Am Ende der Tests konnte jedoch auch die zweite Beta-Hardware mit der wiederum aktualisierten Firmware die oben skizzierten Aufgaben wie Capturing und Alarming sowie einige RMON2-Statistiken in Zusammenarbeit mit der LANsentry Software ohne Probleme bewältigen.

Insgesamt verbesserte sich die Stabilität des NAM über die getesteten Hardware- und Software-Versionen hinweg deutlich. Am Ende der Tests, ca. 1 Monat vor Beginn der offiziellen Auslieferung des NAM, waren keine grundsätzlichen Einschränkungen im Bereich der dokumentierten Features mehr vorhanden. Lediglich eine Analyse eines bestimmten Bereiches des JuNet-Backbones mit einem weiten Spektrum an Protokollen bei mittlerer Auslastung führte weiterhin in einigen Fällen zu einem Verlust der SNMP-Konnektivität des NAM.

4.4.2 Sichtbarkeit der Interfaces

Bei der Beta-Hardware 1 waren beim Ansprechen des NAM als Switch mit dem Typ GENERIC alle im das NAM beherbergenden Catalyst-Switch verfügbaren Interfaces (physikalische Ports, jedoch ohne VLANs oder NDE), vergleichbar mit einer Mini-RMON-Implementierung, mit ihren Interface-Nummern sichtbar (siehe Abbildung 8).

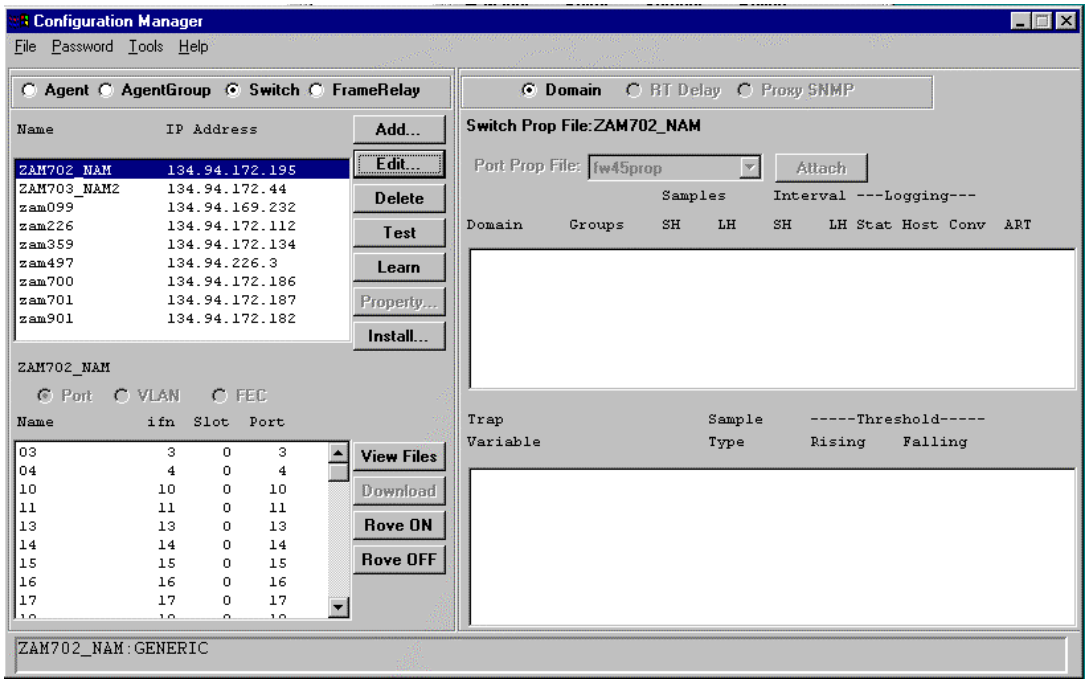

Abbildung 8: Interface-Sichtbarkeit der ersten Beta-Hardware

Diese Interfaces waren vom NAM bereits so initialisiert, daß keine weitere Domain-Installation notwendig war und sie im Mini-RMON Umfang direkt genutzt werden konnten. Eine Installation von weiteren, den Mini-RMON Umfang übersteigenden Domains und damit letztendlich die umfassende Nutzung des NAM als vollwertige RMON-Probe war dann lediglich auf dem Interface möglich, dessen Interface-Nummer der Interface-Nummer der Quelle einer SPAN-Session auf dem Switch entsprach.

Im Gegensatz dazu waren die Mini-RMON Versionen sämtlicher Switch-Ports bei der zweiten Beta-Hardware nicht mehr sichtbar und auch nicht nutzbar (siehe Abbildung 9). Lediglich der Port 1 des NAM, der bei der SPAN-Session des Switches als Ziel-Port konfiguriert wurde, war nun noch sichtbar und wurde für die umfassende Verkehrsanalyse genutzt.

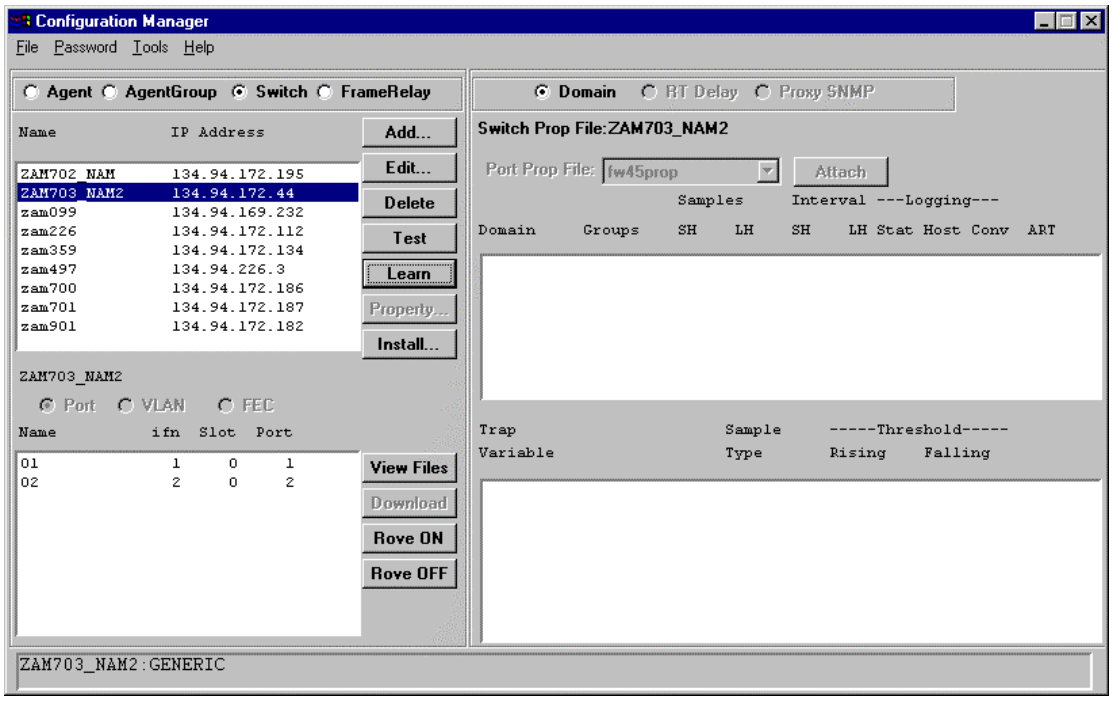

Abbildung 9: Interface-Sichtbarkeit der zweiten Beta-Hardware

Grundsätzlich läßt sich sagen, daß die Bezeichnung und Auflistung einzelner Interfaces bei der LANsentry RMON-Software von 3Com (Teil der Transcend Management Suite) deutlich übersichtlicher und informativer gelöst ist als beim Traffic Director. So werden nicht nur die Interface-Nummern aufgelistet sondern auch die Interface-Beschreibung. Außerdem werden auch die Interface-Nummern der VLANs eines Switches (Mini-RMON) sowie beim NAM das für Netflow Data Export (NDE, s.u. „Netflow Data Export“) fest benutzte Interface 3000 mit korrekter Beschreibung aufgelistet (siehe Abbildung 10).

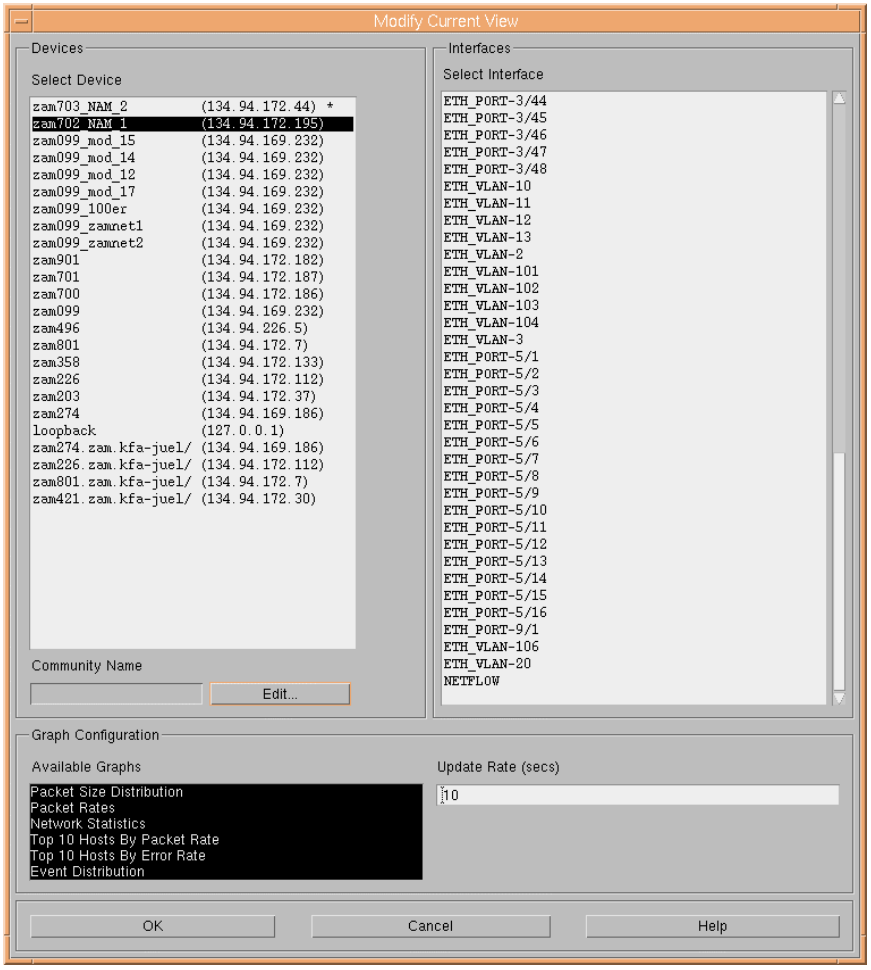

Abbildung 10: Interface-Sichtbarkeit bei Benutzung der LANsentry RMON-Software

4.4.3 Netflow Data Export

Neben der direkten Erfassung von RMON-Statistiken durch die Spiegelung von Verkehrsströmen zum NAM ist dieses auch in der Lage, Verkehrsfluß-Statistiken auf der Basis von NDE (Netflow Data Export) zu empfangen und aufzubereiten. NDE wird in Cisco-Switches und -Routern benutzt, um Verbindungsdaten, die bereits bei Ausnutzung des Multilayer Switching zu Forwarding-Zwecken existieren, einer weiteren Auswertung, u.a. zum Accounting, zuzuführen. Exportiert werden dabei die Verbindungsdaten in der jeweils für das Multilayer Switching konfigurierten Auflösung, also z.B. nur mit Angaben zum IP-Ziel einer Verbindung, mit Angaben zu Absender und Ziel oder auch bei einem komplett Flow-basierten Multilayer Switching mit zusätzlichen Angaben zu den benutzten Protokollen und Ports. Die Aufgabe des Flow Collectors, die das NAM hier übernimmt, muß ansonsten eine eigene, externe Hardware („PC“) mit einer entsprechenden Software („FlowCollector“) übernehmen. Die gesammelten Daten werden im NAM nach dem RMON2-Standard „aufbereitet“ und können entsprechend den Möglichkeiten z.B. des TrafficDirector bzw. Netscout oder auch anderer RMON-Software wie LANsentry dargestellt und ausgewertet

werden. Insgesamt kann man diese Form der Flow-basierten Datensammlung und Aufbereitung jedoch als NDE-light bezeichnen, da die von Cisco ebenfalls angebotenen dedizierten Lösungen zur Sammlung und weiteren Aufbereitung (Accounting, Billing, Profiling) die Auswertungs- und Report-Möglichkeiten z.B. des TrafficDirectors deutlich übersteigen und weitere beim NDE mitgelieferten Informationen wie z.B. Ein- und Ausgangs-Interface, Next Hop Router, TCP/UDP Port-Nummer, genaue Anfangs- und Endzeiten des Flows oder auch das Type of Service (TOS) Byte mit berücksichtigen.

Bei der Interpretation der auf NDE basierenden RMON/RMON2-Statistiken z.B. im Traffic Director sollte man beachten, daß der Datenexport zum NAM nur nach der Beendigung eines Flows oder aber nach dem Ablauf eines Timers beim Multilayer Switching (MLS-Flow-Aging, normalerweise einige Minuten) erfolgt. So kann z.B. durchaus ein Top-Talker einige Minuten aktiv sein, ohne aber in einer entsprechenden RMON-Statistik, selbst bei 30-sekündlichem Update, zu erscheinen. Es liegt also mit NDE keine Realtime-Statistik vor, sondern lediglich eine Zusammenfassung des Verkehrs eines bestimmten Zeitraumes zum Offline-Accounting.

Getestet wurden die Fähigkeiten des NAM, NDE-Daten zu empfangen und aufzubereiten. Dabei wurde NDE Version 1 als „Ausgabeformat“ auf dem Switch konfiguriert und zur Auswertung die für NDE reservierte Interfacenummer 3000 auf dem NAM benutzt. Das Ergebnis war durchaus zufriedenstellend, auch wenn, wie bereits erwähnt, der Traffic Director das NDE-Interface des NAM bei der Konfiguration der Probe nicht zur Auswahl anbietet (im Gegensatz zu LANsentry), sondern dieses „manuell“ konfiguriert werden muß.

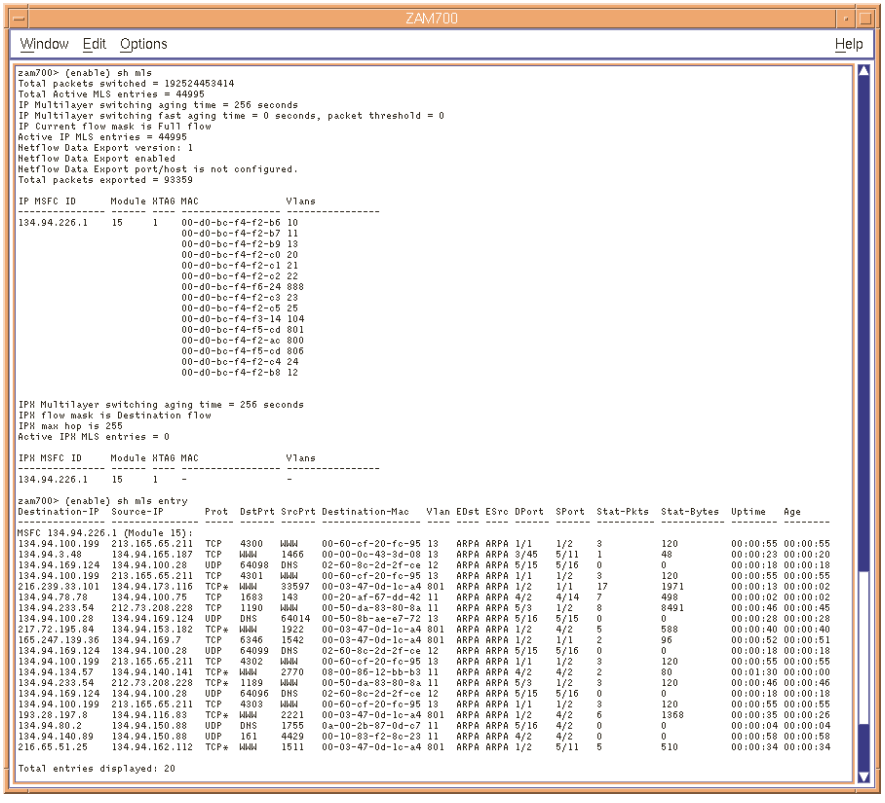

Abbildung 11: MLS-Einträge auf dem Switch, die Daten-Quelle für NDE

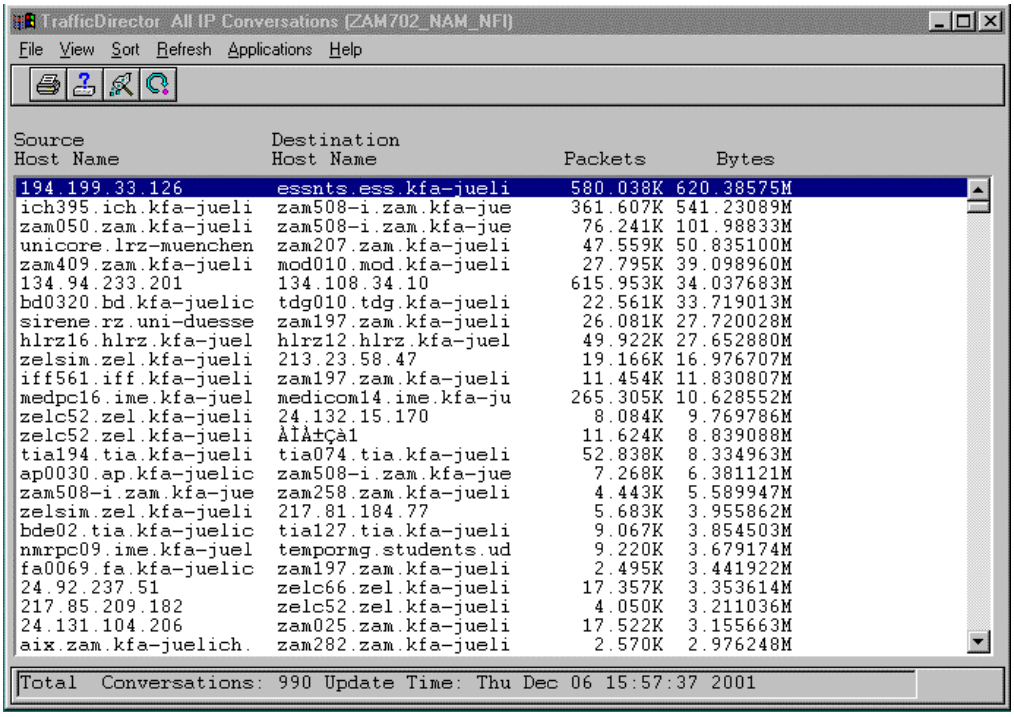

Abbildung 12: IP-Verkehrsstatistiken auf der Basis von NDE

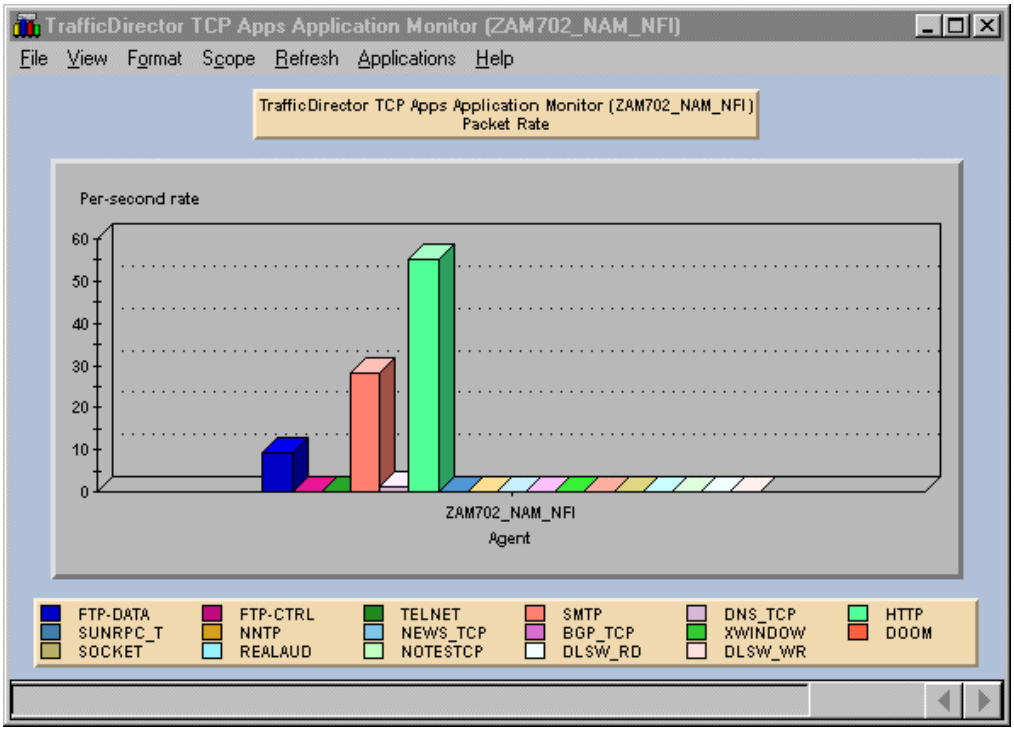

Abbildung 13: Protokollübersicht auf der Basis von NDE

4.4.4 Packet-Capturing

Beim RMON Packet-Capturing wurde ebenfalls mit LANsentry und dem Traffic Director getestet. Insbesondere die erste Beta-Hardware verhielt sich jedoch bei der Definition von Capture-Filtern und dem Allokieren von Capture-Buffer mit LANsentry äußerst instabil. Als Verkehrsquelle wurde u.a. ein über ein falsch angepaßtes Glasfaserkabel laufender Trunk zu einem Test-Switch (Catalyst 4006) genutzt, wobei defekte Pakete gespiegelt und im Trace korrekt als solche ausgewiesen wurden (CRC- und Alignment-Errors). Weiterhin wurde versucht, einen Eindruck von eventuellen Paketverlusten beim Mitschreiben von Paketen zu erhalten. Neben der Analyse einzelner Pakete eines Flows wurde u.a. auf einer Sun mit Hilfe des Tools netperf mit den Optionen „-m 5100 –s 5000 –S 5000“ bei üblicher Ethernet MTU-Size 1500 eine Folge bezüglich ihrer Größe regelmäßig verteilter Ethernet-Pakete erzeugt. Das korrekte und im Vergleich zur Überprüfung einer großen Zahl von Paketsequenznummern leicht zu verifizierende Auftreten dieser Folgen im Capture-Buffer wies keinen Hinweis auf einen eventuellen Paketverlust beim Mitschneiden des Verkehrs bis zu der mit den Teilnehmern realisierten Datenrate von ca. 350 Mbit/s auf.

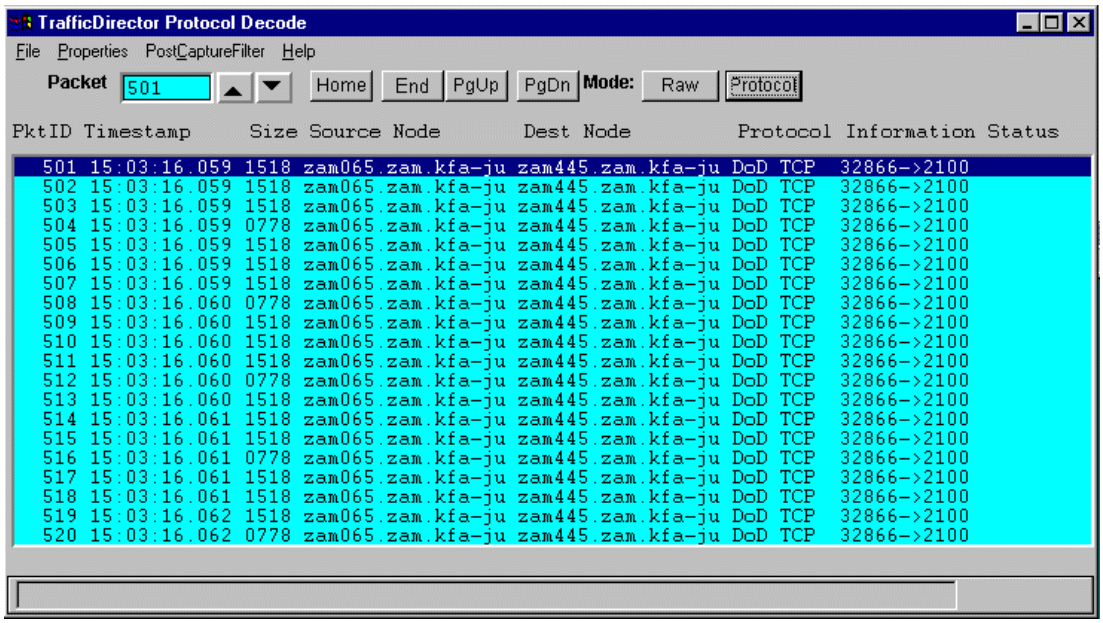

Abbildung 14: regelmäßige Paketgrößenabfolge im Capture-Buffer des NAM

4.4.5 Probleme / Bugs

Im folgenden werden beispielhaft einige der während der Testphase entdeckten und in den meisten Fällen auch von Cisco behobenen Probleme und Bugs vorgestellt.

4.4.5.1 Problem 1

Nach der ersten Installation des NAM in einen Catalyst 6500 Switch erreichte das Modul nicht den erwarteten Status „ok“, sondern fiel nach mehrminütigem Verweilen im Status „other“ in den Status „faulty“. Das Modul wurde daraufhin in einem anderen Slot desselben und anschließend auch in einen anderen Switch eingebaut und blieb in allen diesen Fällen im Status „faulty“.

Nach Rücksprache mit Cisco wurden alle Steckverbinder, insbesondere der Steckverbinder zu dem parallel zum eigentlichen Modulboard aufgesetzten PC-Mainboard, noch einmal, diesmal allerdings außergewöhnlich fest, angedrückt. Nach dieser Maßnahme konnte das Modul den Status „ok“ erreichen.

Laut Cisco war dieses Kontaktproblem bekannt und sollte in zukünftigen Releases behoben sein.

4.4.5.2 Problem 2

Beim Testen mit der RMON-Software LANsentry, V5.2.3, die Bestandteil der vom Autor eingesetzten Management Suite Transcend der Fa. 3Com ist, konnte reproduzierbar beim Löschen von allokiertem Capture Buffer auf dem NAM ein Verlust der SNMP-Konnektivität des NAM erreicht werden. Durch dieses Problem war das NAM als RMON-Probe nicht weiter nutzbar. Zur Auflösung dieses Zustandes mußte das NAM jeweils über die Konsole (CLI) rebootet werden. In einigen Fällen mußte das Modul sogar kurz aus dem Slot gezogen oder alternativ der gesamte Switch rebootet werden. Log-Einträge zu diesem Problem waren weder auf dem das NAM beherbergenden Switch noch im NAM selber zu finden. Das CLI des NAM und auch der Gesamtstatus des Moduls im Switch waren durch das Problem nicht betroffen.

4.4.5.3 Problem 3

Getestet wurde das NAM u.a. in einem Catalyst 6509 Switch mit einer MSFC und einem zum damaligen Zeitpunkt ebenfalls im Beta-Test befindlichen FlexWan Modul (dieses Modul dient zur Integration von Port-Adaptern der Router-Familien 7200 und 7500 von Cisco in die Catalyst 6000 Switch-Familie). Beim Versuch, ein VLAN mit dem NAM zu monitoren, in dem die MSFC ein IP-Interface hatte, war die MSFC nach einigen Minuten nicht mehr erreichbar und routete keine Pakete mehr. Gleichzeitig ging das FlexWan Modul in den Status „Power Down“. Log-Einträge der MSFC deuteten auf Probleme im Memory Management hin:

```
Apr 12 14:59:37 zam901-a 67: Apr 12 14:59:37: %SYS-2-MALLOCFAIL: Memory
  allocation of 1684 bytes failed from 0x601AA088, pool I/O, alignment 32
Apr 12 15:00:34 zam901-a 103: Apr 12 15:00:33: %FIB-3-FIBLC_OOSEQ: Slot 7
  disabled - Out of Sequence. Expected 1249, received 1253
Apr 12 15:01:28 zam901-a 142: Apr 12 15:01:27: %FIB-3-FIBLC_OOSEQ: Slot 23 disabled - Out
of Sequence. Expected 30, received 31
Apr 12 15:01:30 zam901-a 143: Apr 12 15:01:29: %ATM-3-FAILCREATEVC: ATM
  Failed to create VC(VCD=12, VPI=0, VCI=387) on Interface ATM7/0/0,(Cause of the failure:
Failed to have the driver to accept the VC)
```

Da bei diesem Test die MSFC mit der Beta-Software c6msfc-jsv-mz.Mar7 betrieben wurde, wurde der oben erläuterte Test mit der IOS-Version 12.1(1)E wiederholt. Diesmal gab es auf dem MSFC-CLI die Meldung „VLAN spaning not supported“ zu lesen, sobald auf der Switch-Konsole das Monitoren eines VLANs konfiguriert wurde. Die anschließend zu diesem VLAN im NAM gesammelten RMON-Statistiken entsprachen nicht den tatsächlichen Verkehrsflüssen und waren unbrauchbar. Interessanterweise schien die von der MSFC generierte Fehlermeldung über die fehlende Unterstützung des VLAN-Monitoring den Entwicklern des NAM unbekannt zu sein, wie entsprechende Rückfragen erkennen ließen.

Eine einige Wochen nach Auftreten dieses Problems auf der MSFC eingespielte Beta-IOS-Version c6msfc-jsv-mz.May1, die sich als V12.1(20000501:115110) zu erkennen gab, unterstützte dann erstmals VLAN-spaning.

4.4.5.4 Problem 4

Beim weiteren Testen mit dem NAM stellte sich ein gravierenderes Problem heraus; nämlich eine unterschiedliche Sichtbarkeit von Paketen in Abhängigkeit von der Analysequelle („span source“). In Kombination mit einer MSFC, die mit der IOS-Version V12.1(20000501:115110) und später mit der IOS-Version c6msfc-is-mz.121-1.E betrieben wurde, und einem FlexWan-Modul mit ATM OC3 Portadapter wurde folgendes Testszenario aufgebaut:

- In 3 IP-Subnets (192.168.88.0/255.255.255.0, 192.168.89.0/255.255.255.0 und 134.94.8.0/255.255.248.0) wurde jeweils eine Workstation angeschlossen (Teilnehmer A bis C in Abbildung 15).
- In allen 3 IP-Subnets hatte die MSFC eine IP-Adresse. Sie wurden geroutet.
- Die beiden Subnets aus dem privaten Adreßbereich waren als VLANs in dem Catalyst 6509 realisiert.
- Das dritte Subnet war ein ATM Classical IP Netz und wurde über das FlexWan Modul geführt.
- Die beiden Workstations in dem privaten Adreßbereich waren jeweils über Gigabit Ethernet an dem Catalyst 6509 angeschlossen.

- Es wurden auf den Workstations im 192.168.88er Netz und 134.94.8er Netz jeweils ein Ping (ICMP Echo request) zur Workstation im 192.168.89er Netz in sekündlichem Abstand abgesetzt.

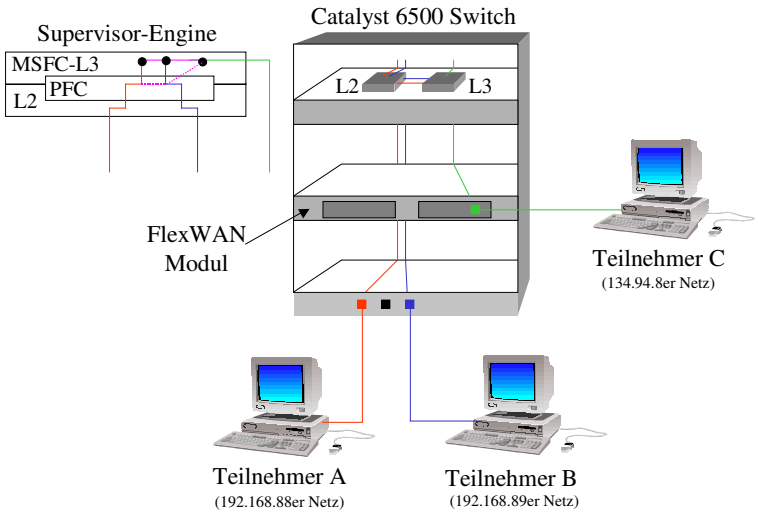

Abbildung 15: Testaufbau zu Problem 4

Der Verkehrsfluß wurde nun vom NAM nacheinander an 2 verschiedenen Meßpunkten analysiert:

- Der erste Meßpunkt war das VLAN der Ziel-Workstation (192.168.89); der Verkehr wurde durch VLAN-spaning zum NAM geführt.
- Der zweite Meßpunkt war der Anschlußport der Ziel-Workstation (1/2); der Verkehr wurde durch Port-spaning zum NAM geführt.

Weiterhin wurden die Tests mit und ohne Multilayer Switching (MLS) durchgeführt. Beim Multilayer Switching wird, zur Beschleunigung des Routing, die per Software in der MSFC ermittelte Routing-Entscheidung eines jeden Flows (fixe Kombination aus 2 Kommunikationspartnern (IP-Adressen) und TCP- bzw. UDP-Portnummern) an die PFC weitergeleitet, die in Kombination mit den Layer-2 Forwarding-Informationen dann auch für Subnet-übergreifenden Verkehr ein Hardware-basiertes und damit gegenüber dem klassischen Routing deutlich schnelleres Weiterleiten von Paketen ermöglicht. Wird ein Paket mittels MLS bzw. PFC weitergeleitet, so ergibt sich aufgrund der internen Realisierung der Paket-Spiegelung von VLANs eine veränderte Sichtbarkeit des Paketes am Analyser. Diese dem VLAN-spaning grundsätzlich anhaftende Eigenart wird bei Cisco u.a. im „Catalyst 6000 Family Configuration Guide“ erwähnt.

Als Besonderheit bei diesem Test wurde einer der 3 Teilnehmer über einen ATM-PA eines FlexWan-Moduls angeschlossen. Dieses Interface ist im Switch jedoch wie das Interface eines herkömmlichen Routers realisiert. Es ist direkt über das IOS der MSFC konfigurierbar und auf den ersten Blick nicht über das CatOS der Supervisor-Engine ansprechbar. Tatsächlich läuft jedoch auch der Weg von der MSFC zum ATM-PA als

„unsichtbares“ VLAN entsprechend dem Design des Catalyst 6500 über die Supervisor-Engine und die für das Ethernet-Switching optimierte Backplane.

Folgende Verkehrsflüsse (in Paketen pro Sekunde) wurden gesehen:

	Meßpunkt 1	Meßpunkt 2
MLS enabled	2 in, 2 out	0 in, 2 out
MLS disabled	4 in, 4 out	0 in, 2 out

Messungen mit V12.1(20000501:115110)

	Meßpunkt 1	Meßpunkt 2
MLS enabled	2 in, 2 out	0 in, 2 out
MLS disabled	2 in, 4 out	0 in, 2 out

Messungen mit c6msfc-is-mz.121-1.E

Die Messungen wurden sowohl mit Traffic Director (Domain History) als auch mit LANsentry durchgeführt. Außerdem wurde der Verkehr auf dem NAM mitgeschrieben (RMON1 Capture) und die Statistikwerte anhand der Timestamps des Traces verifiziert.

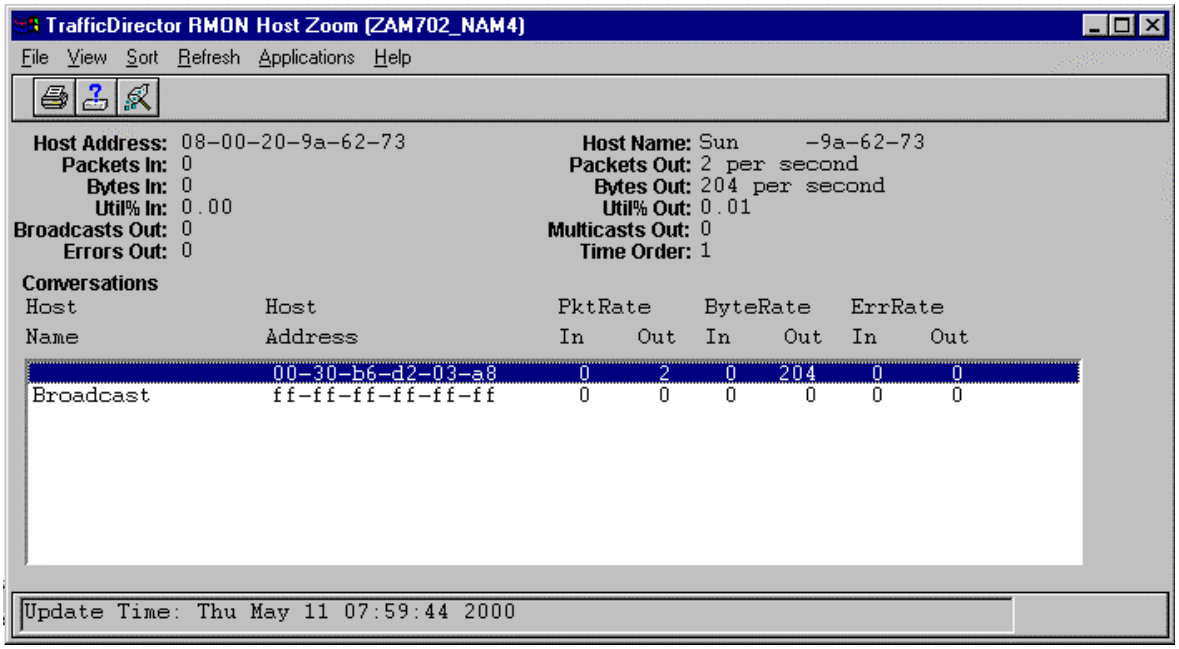

Abbildung 16: Paket-Statistik am Meßpunkt 2 für die Ziel-Workstation

Insgesamt ergaben sich bei diesem Test also 4 verschiedene Verkehrsstatistiken für ein- und denselben Datenfluß, die ihre Ursache in der Realisierung der Verkehrsspiegelung im Switch in Kombination mit dem Multilayer Switching haben.

Die aufgezeigten Probleme führten dann auch zu einem regen Austausch mit den Entwicklern und Beta-Test Betreuern der Fa. Cisco.

4.4.5.5 Problem 5

Bei den Tests, in diesem Fall mit Multicast-Verkehr (MBONE), wurde zufällig ein Port auf einem 10/100BaseTX-Modul entdeckt (Port 3/2), zu dem, wenn er als Source-Port für das Monitoring mit dem NAM benutzt wurde, Traffic Director bei der Konfiguration des korrespondierenden NAM-Interfaces (Interface 12) (siehe „Sichtbarkeit der Interfaces“) eine „Net Speed“ von „1 bits/sec“ angab. Die Installation der Traffic Director Property „nam6kprop“ war ohne Probleme möglich. Beim Auslesen und Darstellen der RMON-Statistik, die eine falsche Auslastung von 100% angab, verlor das NAM dann jedesmal die SNMP-Konnektivität.

Eine manuelle Festlegung des „network“-Eintrags des problematischen NAM-Interfaces auf „FastET-FDX“, „FastET-HDX“ und auch „Ethernet“ (der betreffende Switch-Port wurde mit 10 Mbit/s halbduplex autodetected betrieben) brachte keine Änderung des Verhaltens.

Nach Umschaltung des Teilnehmers auf den Switch-Port 3/4 konnte ohne Probleme mit dem entsprechenden NAM-Interface (Interface 14) gearbeitet werden. Die „Net Speed“ wurde dabei korrekt mit „10 Mbit/sec“ angegeben.

Die Benutzung des Ports 3/2 über die Mini-RMON Implementierung war jederzeit ohne Probleme und mit korrekt angegebener Portgeschwindigkeit möglich.

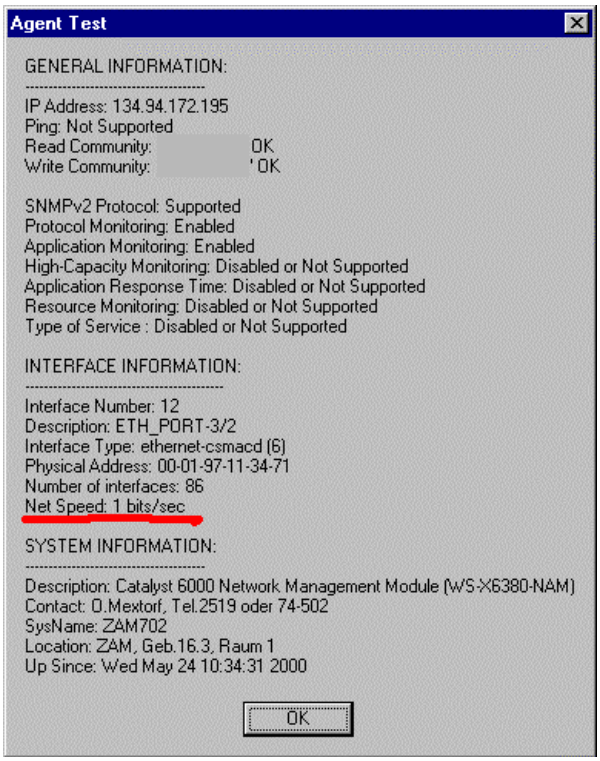

Abbildung 17: Falsche Interface-Geschwindigkeitsangaben des NAM

4.4.5.6 Problem 6

Während des Vorserientests konnten diverse Unzulänglichkeiten in der Dokumentation zum NAM erkannt und beseitigt werden.

Dazu zählten neben einigen Rechtschreib- und Syntaxfehlern sowie Bezügen auf falsche Hardware (Catalyst 5000 Familie) insbesondere fehlende Angaben zur VLAN-Zuordnung des Management-Interfaces des NAM und fehlende Angaben zum Löschen von Community-Einträgen, so daß z.B. die vorbesetzten Default- Read- und Write-Communities nur durch eigene Werte erweitert, nicht jedoch gelöscht werden konnten. Da gleichzeitig die Hilfefunktion innerhalb des Command Line Interfaces nur sehr spartanisch realisiert war, fehlten notwendige Informationen zum sicheren Betrieb des NAM.

5 Zusammenfassung

Das Network Analysis Modul für Switches der Catalyst 6000/6500 Familie der Fa. Cisco Systems stellt eine von mehreren Möglichkeiten dar, auf der Basis von RMON- und RMON2-Statistiken in einem Switch-basierten Datennetz zu sammeln. Es ist eine integrierte Monitoring-Lösung innerhalb einer Switch-Familie, läßt allerdings die durch den Einsatz von Multi-VLAN-Switches prinzipbedingten Einschränkungen beim Monitoring nicht verschwinden und bietet auch keine wesentlichen, über den RMON-Umfang hinausgehenden Möglichkeiten der Datenanalyse (wie z.B. ein Sniffer-System mit seinem Expert Analyser und ausgefeilten Möglichkeiten der Filterdefinition). Lediglich die Möglichkeit, NDE-Daten nach RMON-Standard aufzubereiten, geht über den Umfang einer „normalen“ RMON-Probe hinaus. Wer jedoch ernsthaft Accounting und Billing durchführen will, ist mit einer dedizierten Lösung zur Auswertung der NDE-Daten besser positioniert. Für die Zukunft sind für das NAM Features wie die Unterstützung von DSMON zur detaillierten Untersuchung Differentiated-Services-basierender Netze oder auch die Implementierung der ARTMIB zum Messen von Antwortzeiten auf Applikationsebene, wie es Frontier/Netscouts eigene Probes bereits können, in Aussicht gestellt.

Die Teilnahme am Vorserientest eröffnete für das ZAM des Forschungszentrums Jülich die Möglichkeit, sich frühzeitig mit einem interessanten Produkt zur Verkehrsanalyse und zum Monitoring im Umfeld der im FZJ eingesetzten Switches Catalyst 6500 auseinandersetzen zu können und ein klein wenig an der Fertigstellung eines „runden“ Produktes mitarbeiten zu können. Für die Fa. Cisco Systems war das Forschungszentrum Jülich mit seiner heterogenen Netzwerkumgebung und der im ZAM vorhandenen Erfahrung im Betrieb von Catalyst 6500 Switches ein interessanter Beta-Test Partner. Erfreulich war, die deutliche Konvergenz bezüglich Stabilität und Funktionalität des NAM im Verlauf der Beta-Test Phase mit mehreren Testgeräten und –versionen zu sehen. Auch ist der regelmäßige und fruchtbare Kontakt mit den Entwicklern des NAM sowie der CatOS-Software positiv zu erwähnen. Aus der Sicht eines Netzwerkbetreibers wäre dieser direkte Draht zu kompetenten Gesprächspartnern auch bei anderen Problemen oftmals wünschenswert.

6 Literatur

[1] Network Working Group, S. Waldbusser: Request for comment 1757 – RMON

[2] Network Working Group: Request for comment 2021 – RMON2

[3] Cisco Systems: Catalyst 6000 Command Reference Version 6.1

[4] Cisco Systems: Catalyst 6000 Network Analysis Module Installation and Configuration Note

[5] Cisco Systems: Ft. Lauderdale 0.34 Release Notes

[6] Cisco Systems: Catalyst 6000 NAM Release 1.1(0.8a) Caveats

[7] Cisco Systems, Danny Lee: 6KNAM Quick Start User's Guide with TrafficDirector 5.8 ver 110

[8] Cisco Systems: Catalyst 6000 Family Configuration Guide Version 6.1