

Kapitel 2

NM 2 - Netzmanagement-Plattformen

Das Ideal eines vollständig integrierten Managements wäre das **Universal Management**, welches für alle denkbaren Ressourcen genau ein genormtes Informations- und Kommunikationsmodell festschreiben würde. Die Realität der käuflich zu erwerbenden Netzkomponenten, der Softwareprodukte und Schnittstellenspezifikationen weicht freilich von diesem Ideal ab. Als Zwischenschritt zum universellen Management haben sich **Management-Plattformen** etabliert. Als Beispiel einer Management-Plattform werden wir in diesem Versuch das professionelle Softwarepaket **HP OpenView** kennenlernen.

2.1 Theorie

Mit der zunehmenden Expansion der Rechnernetze haben sich zwangsläufig Probleme für die Verwaltung, Kontrolle und Planung dieser Netze ergeben. Dadurch kommt dem Netzmanagement, das sich mit der Überwachung und Steuerung größerer Netze beschäftigt, eine größer werdende Bedeutung zu.

Im Zuge der Praktikumsaufgabe soll eine Einführung in die Managementproblematik gegeben werden. Netzmanagement wird zuerst in Teilbereiche mit unterschiedlichen Aufgaben untergliedert, die Funktionen dieser Teilbereiche werden dann abgesteckt. Anschließend sollen die grundlegenden Kennzeichen von typischen Management-Architekturen vermittelt werden. Unter dem Stichwort des integrierten Netzmanagements werden die Stufen der Integration verdeutlicht, was auf den Begriff der Netzmanagement-Plattform hinführt.

Im Praxisteil wird zuerst ein Überblick der Funktionalität der verwendeten Plattform HP OpenView gegeben, und auf die allgemeine Problematik der Informationsflut eingegangen. Eine kurze Einführung in das Fehlermanagement zeigt einfache Möglichkeiten der Netzdiagnose zur Eingrenzung von Fehlern auf. Analog zum vorhergehenden Versuch wird aus OpenView heraus, mittels des SNMP-Protokolls, das Lesen und Setzen von Management-

Variablen entfernter Rechner durchgeführt. Zum Schluß wird zusätzlich auf die Erzeugung und Behandlung außergewöhnlicher Ereignisse (Traps) durch den SNMP-Agenten eingegangen.

2.1.1 Aufgabe 1: Netzmanagement: Begriffsklärung, Probleme, Lösungen

1. Was versteht man unter dem Begriff Netzmanagement und in welche Dimensionen läßt er sich zerlegen?
Literatur: [Gar91], [HL92], [Ker95]
2. Zeigen Sie anhand von Beispielen aus der LAN- und WAN-Welt, in welche (OSI-) Funktionsbereiche sich Netzmanagement zerlegen läßt!
Literatur: [Bla95], [Gar91], [Ker95], [Ros96]
3. Erläutern Sie, welche grundsätzlichen Probleme beim Netzmanagement auftreten können.
4. Die Lösung dieser Probleme besteht in der Bereitstellung einer gemeinsamen Architektur durch die Standardisierung. Durch welche Teilmodelle wird dabei eine Management-Architektur geprägt?
5. Es gibt mehrere Architekturen für Netzmanagement in heterogener Umgebung. Erläutern Sie die Teilmodelle von OSI und die des Internet-Managements. Vergleichen Sie beide Architekturen.
6. Gehen Sie speziell auf die Unterschiede der verwendeten Management-Protokolle (SNMP vs. CMIP, CMOT) ein.
Literatur: [Bla95], [Gar91], [HL92], [Ker95], [Ros96]

2.1.2 Aufgabe 2: Management-Plattform: Begriff und Architektur

1. Erklären Sie die verschiedenen Ansätze zur Integration von Management-Funktionalität, und gehen Sie dabei speziell auf den Begriff „Management-Plattform“ ein. Literatur: [hege92], [neum92]
2. Erklären Sie anhand einer Skizze die Architektur der HP OpenView Plattform. Literatur: [neum92]
3. Die Plattform verbindet zwei verschiedene Produkte, den Node-Manager und Open-View Windows. Grenzen Sie die Aufgabenbereiche beider Produkte voneinander ab. Ordnen Sie beide Produkte in die vorige Skizze ein. Literatur: HP Handbücher (Open-View Windows und Network Node Manager User's Guide)

4. Wie unterscheidet sich grundsätzlich die Ermittlung der im Netz vorhandenen Systeme (Hosts, etc.) einer Management-Plattform von der eines Protokollanalytors?

2.1.3 Aufgabe 3: Management-Architekturen

Auf dem Weg zu einem integrierten Netzmanagement ist es notwendig, von der Heterogenität der Netze durch Standardisierung zu abstrahieren.

1. Welche herstellereinspezifischen Management-Architekturen kennen Sie? Literatur: [hege92], [hege93]
2. Im Hinblick auf ein integriertes Netzmanagement in heterogener Umgebung gibt es u.a. folgende relevante Ansätze: OSI-Management und Internet-Management. Worin liegen die Vorteile und Nachteile des von IAB entwickelten Konzeptes? Literatur: [kern95], [hege92], hege93]

2.1.4 Aufgabe 4: Das Informationsmodell im Internet-Management

1. Die Internet-MIB
 - (a) Beschreiben Sie den prinzipiellen Aufbau der Internet-MIB und gehen Sie dabei auch auf die Begriffe „Structure of Management Information (SMI)“, „Internet-Registrierungsbaum“, „Objektidentifikator“, „Objekttyp“ und „Internet-MIB“ ein.
 - (b) Welche Quellen bestimmen die Inhalte der MIB bei Internet und OSI gleichermaßen? (siehe [kern95])
 - (c) Aus welchen drei Hauptzweigen setzt sich die Internet-MIB zusammen?

(Literatur: [hege92], [blac92], [kern95])

2. Beschreiben Sie das Schema für eine Objektdefinition (Managed Object) gemäß Internet SMI; gehen Sie in diesem Zusammenhang auf die Begriffe „consise MIB Definition“ und „Object-Type Makro“ genauer ein. (Literatur: hege92, blac92, rose91)

2.2 Versuch 1: Grundlagen und Überblick

Verschaffen Sie sich zunächst mit Hilfe der Manuale einen Überblick über die Funktionalitäten der einzelnen Menüs von HP OpenView Windows. Von den bereitliegenden Anleitungsbüchern sind vor allem die Bücher „HP OpenView - Using Network Node Manager“ und

„HP OpenView Window's User Guide“ für Sie relevant. Kopien einiger Manual-Ausschnitte sind ferner im Ordner „Rechnernetzpraktikum - Netzmanagement“ enthalten. Informationen über die einzelnen Menüs erhalten Sie aus dem Hilfetext des jeweiligen Menüs.

- Eröffnen Sie am Rechner `pcnmXov` (per `ssh`) auf `hprnp4` eine Sitzung als User „praktiku“. Das Paßwort ist vom Betreuer zu erfragen. Geben Sie `/opt/OV/bin/ovw` ein und HP OpenView Windows wird nun automatisch gestartet. Alternativ ins Verzeichnis `/opt/OV/bin` wechseln und dann mit `./ovw` starten.
- Gehen Sie nun auf „Map“, klicken Sie „Maps“ an und rufen „Open/List“ auf. Wählen Sie hier „nmX“ (die Map des Rechnernetzpraktikums für Gruppe X) und bestätigen Sie „Open Map“. Sie starten im View auf die „Internet Welt“ (gekennzeichnet mit „Internet“). Diese View wird nach dem Start von HP OpenView Windows automatisch angelegt. Als View bezeichnet man die logische Zusammenfassung von Netzkomponenten. Die erste kleine Übung besteht darin, durch alle vorhandenen Views zu navigieren. (In einen View wechselt man durch Doppelklick mit der linken Maustaste auf das entsprechende Icon).
- Beschreiben Sie kurz den Aufbau der ganzen Map und erklären Sie dabei die Views, die von den Submaps dargestellt werden. Die vorhandene Map wurde durch eine im Hintergrund laufende IP-Applikation automatisch erstellt, und erhält von dieser auch laufend Information über Ereignisse im Netz.
- Zählen Sie auf, welche Informationen durch diese Applikation gewonnen werden. Diese Informationen werden auch dem „Event Manager“, einer weiteren Applikation, gemeldet.
- Informieren Sie sich in den Manualen über Aufbau und Bedeutung des „Event Managers“, sehen Sie sich mit seiner Hilfe die vom Netz empfangenen Ereignisse an, und interpretieren Sie mindestens 3 unterschiedliche Ereignisse. Schätzen Sie ab, wieviele Ereignisse innerhalb der letzten 3 Stunden gemeldet wurden.

Warnung:

- Sollten während des Startup von HP OpenView Windows irgendwelche Fehlermeldungen auftreten (z.B. „... cannot connect to ...“), dann hat vermutlich einer der Hintergrundprozesse von HP OpenView seinen Geist aufgegeben. Diese Hintergrundprozesse laufen ständig, auch wenn die Benutzeroberfläche HP OpenView Windows nicht läuft. Verschaffen Sie sich Überblick über die laufenden Dämonen mittels `/opt/OV/bin/ovstatus`. Prozesse, die sich nicht im Zustand „RUNNING“ befinden, müssen neu gestartet werden. Das kann allerdings nur der Administrator.

- Die Symbole der Benutzeroberfläche HP OpenView Windows besitzen eine Farbsemantik, welche etwas über den Zustand der Managementobjekte ausdrückt:
 - weiß: Objekt wird nicht gemanaged (unmanaged)
 - dunkelblau: Objekt wird gemanaged, aber sein Zustand ist unbekannt (unknown)
 - grün: Objekt ist im Normalzustand
 - türkis: kleinere Probleme (warning)
 - gelb: kleinere Probleme (minor/marginal)
 - rot: Objekt funktioniert nicht (critical)
- Für alle folgenden Versuche zu HP OpenView Windows gilt: Die Symbole für IP-Netze, Router, Switches, LAN-Segmente, Interfaces und belegte Switch-Ports dürfen nur grün, türkis oder (schlimmstenfalls) gelb sein. Rote Symbole dürfen im Grunde nur bei unbelegten Switch-Ports auftreten (Port ist down). Ein dunkelblaues Symbol bedeutet, dass es der Managementplattform nicht möglich ist, den Betriebszustand des entsprechenden Objekts zu ermitteln. Falls Sie überwiegend dunkelblaue Symbole auf dem Monitor haben sollten, dann betreiben Sie in Wirklichkeit kein Netzmanagement, sondern bedienen nur ein aufwändiges Malprogramm.

2.3 Versuch 2: Viewbildung

Ein generelles Problem beim Netzmanagement die auftretende Informationsmenge. Eine Möglichkeit, durch eine Vorauswahl diese Informationsflut zu reduzieren, kann über sogenannte „Views“ realisiert werden.

2.3.1 Aufgabenstellung

- Ihre Aufgabe ist es, einen **eingegrenzten View** zu managen, d.h nur Information über die Komponenten dieses Views zu erhalten. Dabei soll die Gruppe X jeweils nur ihre **eigenen** Komponenten managen (also `pcnmXov`, `pcnmXprot`, `swnmX`). Außerdem sollen **beide** Gruppen den `vlanswitch1` managen, sowie `pcrnp10` und `hprnp4` (und natürlich auch die zugehörigen IP-Netze und LAN-Segmente). Auf den „Rest der Welt“ soll kein Managementzugriff erfolgen.
- Als Resultat erhält man eine Reduzierung der Menge der neu eingehenden Informationen. Dies wird in einer späteren Aufgabe noch verifiziert werden.

Hinweis:

- Für diesen Versuch sollen Sie in HP OpenView eine neue Map erstellen. Dies machen Sie über folgende Befehlskombination. Klicken Sie nacheinander „Map“ - „Maps“ - „New“ an. Nun geben Sie in das Feld Name „MapX“ ein, wobei „X“ als Platzhalter für Ihre Gruppennummer steht und bestätigen Sie mit „OK“. Anschließend erhalten Sie von HP OpenView die Mitteilung, dass Ihre Map erstellt wurde und Sie befinden sich sogleich in selbiger.
- Im Menü „Map“ finden Sie die Befehle zum Managen bzw. Unmanagen von Objekten. Durch Anklicken der Objekte mit der linken Maustaste werden diese selektiert. Wird gleichzeitig zur Maustaste auch die Ctrl-Taste gedrückt, können Sie mehrere Komponenten selektieren.
- Objekte, welche Sie durch Unmanagen aus der Administrationsdomäne entfernt haben, können durch „Edit“ - „Hide“ - „From This Submap“ überdies versteckt werden. Auf diese Weise reduzieren Sie ihren View auf das Netz.
- Nach Beendigung Ihrer Versuche, löschen Sie durch folgende Befehlskombination die von Ihnen erstellte Map wieder. „Map“ - „Maps“ - „Delete“, auswählen der „MapX“ (X ist Ihre Gruppennummer) und „Delete“. Bestätigen Sie mit „OK“.

2.4 Versuch 3: Untersuchen von Endsystem-Verbindungen

In großen LANs, die auf Ethernet basieren, kommt es zu einer Segmentierung in Teilnetze durch Bridges, Switches, etc. Um auftretende Fehler, z.B. „auf einem Rechner ist kein rlogin möglich“, lokalisieren zu können, ist es notwendig, dass eine Managementanwendung Diagnosemittel bereitstellt, mit denen der Zustand von Komponenten und Verbindungen festgestellt werden kann. Diese Diagnosemittel setzen auf verschiedenen Schichten auf. Ist ein Rechner nicht erreichbar, so gibt es mehrere Möglichkeiten, wie z.B.:

- der angesprochene Rechner ist nicht am Netz
- das Segment mit dem angesprochenen Rechner ist nicht erreichbar
- die physische Verbindung ist unterbrochen
- der an der Verbindung beteiligte Rechner ist außer Betrieb

2.4.1 Aufgabenstellung

1. Stellen Sie fest, ob eine Schicht-3-Verbindung von der hprnp4 zur pcrnp10 besteht und wenn ja, wie lange eine Nachricht an diesen Rechner momentan maximal benötigt.

2. Ermitteln Sie den Weg einer Nachricht von der `hprnp4` zur `pcrnp10` und erklären Sie das Ergebnis. Warum sieht man hier den VLAN-Switch nicht?

Hinweis:

In dem Menü „Fault“ finden Sie verschiedene Befehle, mit denen Verbindungsprobleme zwischen Rechnern analysiert werden können. Mit den Kommandos `ping` werden Schicht-3-Pakete versandt. Mit dem Kommando „Locate Route: via SNMP“ können Sie den Weg, den eine Nachricht geht, ermitteln.

2.5 Versuch 4: Lesen und Verändern von MIB-Variablen

Am ersten Praktikumstag zum Netzmanagement haben wir mittels den SNMP-Tools verschiedene MIB Variablen ausgelesen. Dies gilt es jetzt mit HP OpenView und seinem MIB-Browser zu tun.

2.5.1 Aufgabenstellung

1. Ermitteln Sie **mit Hilfe des MIB-Browsers** die verantwortliche Kontaktperson, den Standort, die unterstützten Schicht-Dienste, das Betriebssystem, dessen Version und die Uptime der Komponente `swnmX`. Warum gelingt das Auslesen der MIB-Variablen, obwohl Sie keinen Community String spezifiziert haben?
2. Machen Sie sich klar, woher HP OpenView die herstellerspezifischen Teilbäume der MIB kennt. Führen Sie dazu die folgenden Schritte aus:
 - Gehen Sie in den MIB-Browser und lesen Sie den Wert der folgenden Variablen auf der `hprnp4` aus:

```
iso.org.dod.internet.private.enterprises.hp.nm.system.  
general.computerSystem.computerSystemFreeMemory
```
 - Gehen Sie nun im HP OpenView Menu auf „Options“ und dann auf „Load/Unload MIBs SNMP“. Entfernen Sie nun die „hp-unix“ MIB mittels `unload`. Gehen Sie nun wieder in den MIB-Browser, den Sie vorher geschlossen haben sollten, und versuchen Sie erneut jenen Wert auszulesen. Was stellen Sie fest?

- Versuchen Sie nun den Wert der Variablen über eine numerische Pfadangabe zu bekommen. Die Pfadangabe bekommen Sie über die richtige MIB Definitionsdatei heraus, welche in `/var/opt/ov/share/snmp_mibs/` zu finden ist. Was stellen Sie fest?
 - Laden Sie die „hp-unix“ MIB wieder her.
3. Auch mit HP OpenView besteht natürlich die Möglichkeit MIB Variablen zu verändern. Ändern Sie den Namen der Kontaktperson auf der `hprnp4` auf Ihren Namen und setzen Sie ihn anschließend wieder zurück auf: „Annette Kosteletzky, Phone ++49-89-2178-2166, EMail:kostel@informatik.uni-muenchen.de“. Die Community Strings für die `hprnp4` finden Sie in der Datei `/etc/snmpd.conf`.

Hinweis:

- In dem Menü „Misc“ finden Sie unter dem Menüpunkt „SNMP MIB Browser“ den MIB-Browser. Durch die baumartig strukturierte MIB bewegen Sie sich, indem Sie einen Teilast anwählen und dann mittels des Buttons „Down Tree“ in diesen Teilast hinabsteigen. Mit dem Button „Up Tree“ kommen Sie jeweils eine Stufe höher im Baum. Die `system` Group finden Sie im Teilast `iso.org.dod.internet.mgmt.mib-2`.
- Es könnte hilfreich sein, einen Blick auf die Konfigurationen im Menü „Options“ - „SNMP Configuration“ zu werden.

2.6 Versuch 5: Konfiguration von Events

Management-Plattformen bieten die Möglichkeit, bestimmten Events (z.B. Erhalt eines Traps) eine zuvor definierte Aktion folgen zu lassen. In der vorangegangenen Aufgabe löste der Ausleseversuch von MIB-Variablen mit falschem Community String das Senden eines Traps aus, der von Ihnen bisher nicht wahrgenommen wurde. Um unerlaubte Zugriffsversuche bemerkbar zu machen, soll nun eine sichtbare Reaktion auf einen Event definiert werden.

2.6.1 Aufgabenstellung

1. Versuchen Sie zunächst irgendeine MIB-Variable der `hprnp4` auszulesen und benutzen Sie dabei einen falschen Community String.

2. Sehen Sie sich anschließend die „Error Events“ an, und ermitteln Sie die Meldung, welche vom SNMP Agenten (infolge des Ereignisses „Anfrage mit falschem Community String“) an die Management-Plattform geschickt worden ist. Anmerkung: SNMP Agent und Management-Plattform laufen in diesem Falle beide auf der `hprnp4`. Lassen Sie sich davon nicht verwirren.
3. Um das Ereignis nicht unbemerkt ablaufen zu lassen, ist es Ihre Aufgabe, die Management-Plattform so zu konfigurieren, dass sie eine kurze Meldung in einem Popup-Fenster anzeigt, sobald der betreffende Trap vom Agenten der `hprnp4` an die Management-Plattform geschickt wird. Die Management-Plattform soll aber nur dann reagieren, wenn der Trap vom Agenten der `hprnp4` stammt.
4. Benutzen Sie auf dem `pcnmXprot` das Kommando `snmptrap`, um einen Trap des betreffenden Typs an die Management-Plattform zu schicken.

Hinweis:

In dem Menü „Options“ finden Sie unter dem Menüpunkt „Event Configuration“ die Möglichkeit, Reaktionen auf bestimmte Ereignisse zu definieren. Den zugehörigen Trap zu diesem Ereignis finden Sie, indem Sie „snmpTraps“ anklicken und dann den Event „SNMP_Authen_Failure“ durch Doppelklick auswählen. Das Kommando `snmptrap`, aus der Kommandozeile abgesetzt, erzeugt einen Trap.