INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Fortgeschrittenenpraktikum

Anpassung der Versuche des Rechnernetzepraktikums an die neue Version von HP OpenView

Akos Regi

Aufgabensteller:	Prof. Dr. Heinz-Gerd Hegering
Betreuer:	Michael Brenner Vitalian Danciu
Abgabetermin:	15. Sept 2005

Zusammenfassung

Das Ziel dieses Fortgeschrittenenpraktikums war die Anpassung der Versuche des Rechnenetzepraktikums in dem Bereich des Netzmanagements an die neue Version des Managamenttools HP OpenView Network Node Manager. In diesem Dokument wird diese Anpassung beschrieben. Die Konfigurationen und vorgehensweise werden detailliert dargestellt, was alles und wie geändert werden musste. Die neue Version von HP OV NNM wurde auch auf einer neuen Plattform Micosoft Windows 2003 Server installiert. Dies musste zuerst aktualisiert und konfiguriert werden. Dann mussten die Netzwerkeinstellungen überprüft und gegebenenfalls auch angepasst werden. Es wurde auch der Zugriffsart von SSH mit der X Option auf Remote Terminal Session umgestellt, weshalb zwei neue Benutzerkonten mit speziellen Berechtigungen eingerichtet wurden. Die Klientrechner mussten ebenfalls auf Netzwerkeinstellungen und Softwaremäßig angepasst werden. Wenn die all diese Einstellungen bewerkstelligt wurden, erfolgte das Durchspielen der Praktikumsversuche und eventuell erforderliche Änderung der Konfiguration. Zuletzt wurde die Praktikumsanleitung mit Tutoranleitung überarbeitet und dieses Dokument erstellt.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kapitel 1

Einordnung und Ziel dieses FoPras

Dieses FoPra wurde in dem Bereich des Rechnernetzepraktikums an dem Lehrstuhl für Systemnahe Programmierung an der an der Ludwig Maximilians Universität München[1] durchgeführt. In den nächsten Abschnitten, werden aus diesem Grund kleine Erläuterungen zu diesem Praktikum gemacht.

1.1 Das Rechnernetze-Praktikum

Das Rechnernetze-Praktikum (im Weiteren Praktikum genannt) ist ein optionales Praktikum im Hauptstudium der Informatik. Das Praktikum baut auf die Vorlesungen Rechnernetze und Netzmanagement. Diese beiden Vorlesungen werden als Voraussetzung erwartet, da das Praktikum durch die beiden Vorlesungen vermitteltes Wissen zu vertiefen versucht. Solange in den Vorlesungen die Theorie behandelt wird, wird das theoretische Wissen in den Versuchen von den Studenten in der Praxis erprobt und validiert. Dies ist sehr wichtig, da in der Praxis nicht alles auf Anhieb gelingt. Diese nützliche Erfahrung sollte natürlich auch vermittelt werden.

Das Praktikum besteht aus drei Einheiten. Im ersten Teil werden die Grundlagen und die Themen zu ATM (**A**synchrounus **T**ransfer **M**ode) behandelt. In dem mittleren Teil wird das IP (**I**nternet **P**rotocol) Stack behandelt. Im letzten und für uns hier relevanten Teil werden die Themen zu Netzmanagement erörtert. In diesem Teil kommt auch das Netzmanagementtool von HP (HP steht für die Firma Hewlett Packard) ins Spiel. Die Aufgaben zu Netzmanagement werden mit Hilfe von HP OpenView (wird als OV abgekürzt) Network Node Manager (wird als NNM abgekürzt) durchgeführt. Der Schwerpunkt liegt bei der Verwaltung von Netz(Segmenten) und Netzwerkknoten (mehr dazu im Kapitel 2) inklusive Problematik und Möglichkeiten von Netzmanagement (FCAPS – **F**ault **C**onfiguration **A**ccounting **P**erfomance **S**ecurity).

1.2 Motivation

Das Praktikumsnetz wurde bisher mit HP OV NNM V05.01 untersucht und verwaltet. Diese bisherige Version von HP OV lief auf einem alten HP Rechner, deren Konfiguration bzw. die von HP OV NNM mit der Zeit in Leidenschaft gezogen wurden, weshalb die Überlegung entstand, ob die Konfiguration bereinigt werden soll, oder komplett auf eine neue Version umgestiegen werden soll. In wie weit die alte Version noch verwendbar war, beschreibt der nächste Absatz.
Der Existenz dieses FoPras beweist, dass nicht nur für eine Neuinstallation, sondern gleich für eine neue Version entschieden wurde. Die neue Version wurde nicht nur auf einem neuen Rechner, sondern auch

[1] **L**udwig **M**aximilians **U**niversität wird als LMU abgekürzt

gleich auf eine neue Plattform aufgesetzt. Die neue Plattform, hier Microsoft Windows 2003 Server, brachte einige Probleme mit sich. Dieses FoPra beschäftigt sich mit der Anpassung von HP OV NNM 6.41 an das Praktikumsnetz.

1.2.1 Der vorhandene Zustand

Die bisherige Version von HP OV NNM läuft auf einem alten HP Rechner unter HP-UX (ein Unix Derivat von HP). Der alte HP Rechner arbeitet nicht nur langsam, sondern läuft auch nicht mehr stabil. Eine der Gründe war bereits erwähnt, nämlich die nicht mehr ganz reine Konfiguration des Systems. Die bisherige Version von HP OV NNM arbeitete auch nicht immer ganz zuverlässig. Dieses beweist das Bild unten, das nach der Anmeldung am HP Rechner und nach dem Starten von HP OV NNM entstand. Nach dem diverse Meldungen weggeklickt wurden, konnte man mit dem System relativ gut aber langsam arbeiten. Die Abbildung veranschaulicht diesen Zustand.

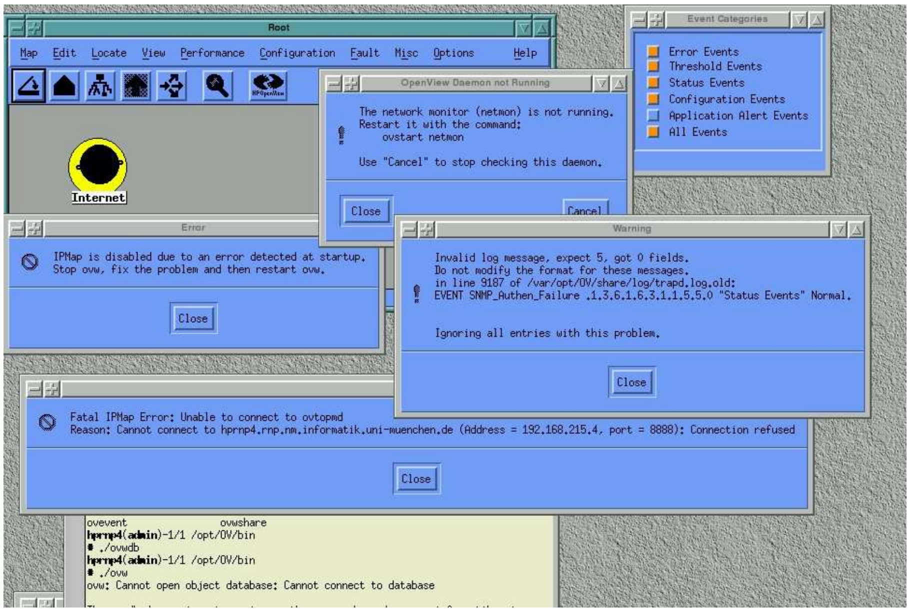

Abbildung 1.1: Startbild von HP OV NNM V5.02

1.2.2 Was bietet die neue Version?

Die neue Version bietet eine gute und relativ frei konfigurierbares Reporting mit optionaler Emailbenachrichtigung. Es bietet auch die Möglichkeit der Führung eines laufenden Inventars Über die im Netz befindlichen Geräte mit Angabe der on- bzw. offline Zeiten. Die Managementsoftware bietet außerdem ein Webinterface, das viele der Funktionen von HP OV NNM auch ohne Anmeldung an der Managementkonsole erreichbar macht. Der wichtigste Punkt ist die schnellere und bessere automatische Node-Discovery, das nicht nur IP, sondern auch OSI Schicht 2 unterstützt. Der Hersteller HP macht wenig Aussagen darüber, wie diese automatische Node-Discovery, von dem bereits eine neue weiterentwickelte Version gibt, funktioniert. Allerdings konnte aber in dem HP Forum einiges in Erfahrung gebracht werden. ([HPOVNNM 03], Seiten 56-61)
Die Schicht 2 Discovery funktioniert Über die Benutzung von ARP (**A**ddress **R**esolution **P**rotocol) Cache des Systems (in unserem Fall der Managementkonsole WINRNP7) und von dem default Gateway (Router). Es kommt noch die Benutzung von dem Seed Datei hinzu. Mit Hilfe der Seed Datei kann Netmon (Network Monitoring Process) mitgeteilt werden, von welchen Hosts und IPs aus er die MAPs erstellen

soll. ([HPOVNNM 03], Seiten 119-122) Netmon ist einer der für das Discovery zuständiger Prozesse. Das ARP Cache des Routers wird über den SNMP Agenten abgefragt. Als Quelle kann ich mich dazu nur auf die Angaben im HP IT Ressource Center Forums stützen. Suchen Sie dort nach einem Thread mit “how autodiscovery of NNM OV works? “ .

1.2.3 Ziel

Das Ziel war natürlich, dass die Versuche auch auf dem neuen System nachgestellt werden können. Da nicht nur die neue Version von HP OV NNM sondern auch das Betriebssystem Microsoft Windows 2003 Server konfiguriert werden musste, waren einige Änderungen erforderlich. So funktionierte keine SSH Verbindung mit der X-Session Weiterleitung, da Windows 2003 Server keinen SSH Server mitbringt, weshalb nach neuer Möglichkeit gesucht werden musste, wie man die Management Software von den Linux Clients aus erreichen und bedienen kann. (Mehr dazu im Abschnitt 2.2.4)
Diese beiden Teilaufgaben brachten unvorhersehbare Probleme mit sich, die zuerst Schrittweise abgearbeitet werden mussten. Diese Schritte und die vorgenommenen Änderungen am Betriebsystem, HP OV NNM und an den Clientrechner werden in den einzelnen Teilen des nächsten Kapitels beschrieben.

1.2.4 Aufteilung des Praktikums

Das ganze FoPra kann zweigeteilt werden, in einen praktischen Teil und in einem dokumentarischen Teil. In dem praktischen Teil wurden die Konfigurationen angepasst. Die erforderlichen Einstellungen waren nicht immer einfach und auf dem ersten Blick erkennbar. Die Informationen mussten oft zuerst besorgt werden, was nicht immer schnell und problemlos erfolgen konnte. Auch wenn die Informationen vorlagen, mussten diese auf das Praktikumsnetz angewendet werden. Die HP OV Support Seiten mit den zugehörigen Foren erwiesen sich als eine sehr nützliche Anlaufstellen.
Sie finden die HP Support Seiten inklusive Foren unter:

http://support.openview.hp.com/support.jsp?fromOV=false

In dem praktischen Teil wurden das Betriebsystem (Microsoft Windows 2003 Server), der Webserver (Microsoft Internet Information Server), die Managementsoftware (HP OpenView Network Node Manager), das Netzwerk und die Clientrechner konfiguriert. Diese vorgenommenen Änderungen werden in dem nächsten Kapitel detailliert beschrieben.
Der dokumentarische Teil beinhaltet natürlich auch zwei weitere Teilaufgaben, die Erfassung dieses Dokuments und die Anpassung der Tutoranleitungen.

Kapitel 2

Die Konfiguration der einzelnen Komponenten

Wie in der Einführung bereits erwähnt wurde, werden die Aufgaben dieses Praktikums in dem Bereich des Netzmanagement gestellt. Das Praktikumsnetz soll auch mittels Managementsoftware kennen gelernt werden. Die neue Version der Managementsoftware wurde auf eine neue Plattform gesetzt. Dies wirkte sich nicht nur auf die Managementkonsole, Managementsoftware sondern auch auf die Clientrechner aus. Diese Komponenten des Praktikumsnetzes und die durchgeführten Änderungen werden in diesem Kapitel die Reihe nach in den einzelnen Abschnitten beschrieben. Da das Praktikumsnetz die Grundlage bietet, wird das in den folgenden Abschnitten zuerst vorgestellt. Als nächstes wird der `PCRNP10` Rechner, der wichtige Aufgaben in diesem Netz verrichtet, kurz vorgestellt. Wenn das Netz soweit vorgestellt wurde, wird auf die Problematik und Komplexität der Konfiguration der Managementkonsole `WINRNP7` eingegangen. Im ersten Schritt wurden nicht nur die Netzwerkeinstellungen, sondern auch das Betriebssystem und dessen Aktualität und Konfiguration der Managementkonsole validiert und bei Bedarf angepasst. Diese bilden die Grundlagen für ein erfolgreiches Arbeiten der Managementsoftware. Wie all das bewerkstelligt wurde, können Sie hier in den einzelnen Abschnitten erfahren.

2.1 Beschreibung des Praktikumsnetzes

Das Praktikumsnetz besteht aus mehreren Netzsegmenten (Abbildung 2.1), was sich anhand der Ausgabe des `ovtopodump` Befehls leicht überprüfen lässt. Sie finden die Ausgabe des Befehls im Anhang. Weitere Details zu diesem Befehl finden Sie in diesem Kapitel später bei der Beschreibung der Konfiguration der Managementsoftware (Abschnitt 2.3.1). Von den Netzsegmenten werden verschiedene je nach Aufgabe des Praktikums benutzt. In dem Netzmanagementbereich werden zwei Segmente benutzt.
Während des Praktikums arbeiten die Studenten in Gruppen. Eine Gruppe besteht aus mindestens zwei Studenten. Dies ist nötig, um die Aufgaben im Netzmanagementbereich machen zu können, da sich die Rechner für diese Aufgaben komplementär im Netz befinden.

2.1.1 Das Praktikumsnetz allgemein

Der wichtigste zentrale Rechner ist `PCRNP10`. Die Rolle dieses Rechners wird in dem nächsten Abschnitt beschrieben. Andere für die Netzmanagement wichtige Komponenten befinden sich in zwei Subnetzen. Diese für die Managementaufgaben wichtigen Netzsegmente sind 1er und 2er Subnetze, die in den Abbildungen mit Gelb hinterlegt sind. Beide bestehen aus 2 Rechnern und aus einem managebaren HP Switch.

Die Managementsoftware (HP OV NNM) läuft auf einem Windows Rechner (WINRNP7). Es gibt außerdem noch ein ATM Subnetz bestehend aus 4 HP Rechnern, einem HP Protokollanalysator und aus zwei PCs (mit Microsoft Windows 98 Betriebssystem). Man muss noch die Firewall und Routernetze erwähnen, die die Firewall- und Routingsaufgaben übernehmen. Weitere zentrale Komponenten sind die zwei VLAN (**V**irtual **L**ocal **N**etwork **A**rea) Switches mit denen die Netzsegmente (VLANs) aufgebaut werden. Als letztes müssen noch die Forte Switches erwähnt werden, die als Koppelelement der ATM Geräte dient. Die Netztopologie wird in der Abbildung 2.1 gezeigt.

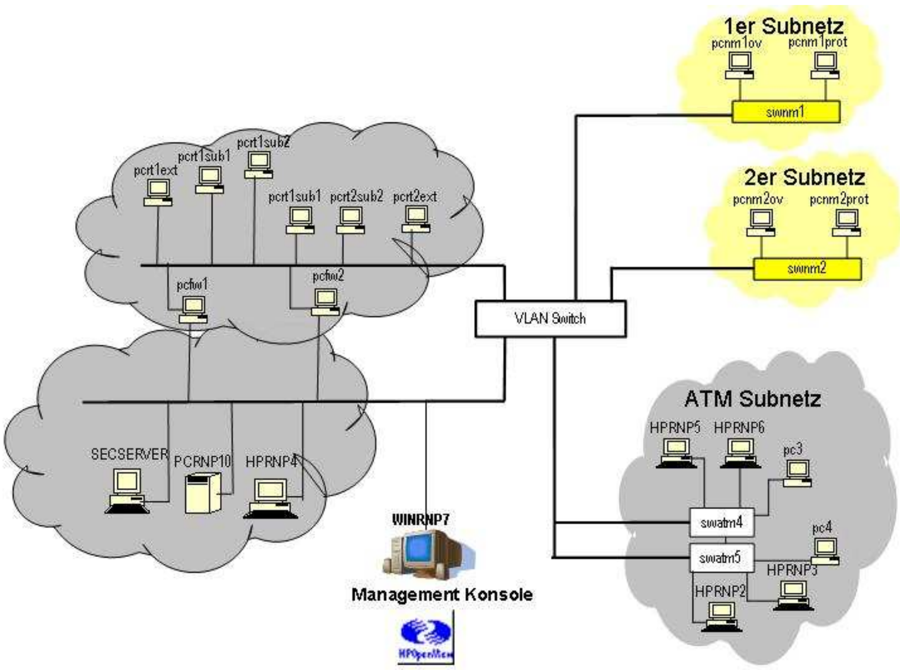

Abbildung 2.1: Netzwerktopologie des Praktikumsnetzes

2.1.2 Das Managementsubnetz

Es gibt zwei Netzsegmente für die Netzmanagementaufgaben, die aber weitestgehend analog aufgebaut sind. Die Geräte sind ähnlich benannt, der Name der Geräte unterscheidet sich nur in einer Ziffer in den Namen (1 oder 2). Im Weiteren werden die zutreffenden Ziffern mit X ersetzt.

Die Abbildung 2.2 zeigt das Netzsegment des Praktikumsnetzes, das während der Managementaufgaben benutzt wird. Die zwei Teilnetze sind hier ebenfalls Gelb hinterlegt. Zu sehen ist die Managementkonsole `WINRNP7`, der Routerrechner `PCRNP10` und das VLAN Switch. Wie es aus den Abbildungen entnommen werden kann, besteht jedes der Subnetze aus zwei Clientrechner, pcnmXov und pcnmXprot. X steht hier in dem Rechnernamen für 1 oder 2 je nachdem in welchem Netz der Rechner sich befindet. Die Namen der Rechner im 1er Netz sind also: `pcnm1ov` und `pcnm1prot`.

Jeder Gruppe der Studenten wird nochmals zweigeteilt. Einige arbeiten an dem Rechner pcnmXov, andere auf dem Rechner pcnmXprot. Diese ist nötig, da die Aufgaben komplementär aufgebaut sind.

Diese Rechner werden Clientrechner genannt, da die Managementsoftware auf einem Windows 2003 Server `WINRNP7` läuft und wird mit diesem mittels Remote Terminal Session verbunden. In jedem der Managementnetze befindet sich noch ein managbares HP Switch (swnmX) von Typ HP J3177A Switch 224T. Sie finden weitere Dokumentation zu diesem Switch unter:

http://www.hp.com/rnd/support/manuals/sw_208_224.htm

Die Aufgaben beziehen sich auf diese Switches. Die Studenten sollen diese Switches verwalten. Der Rest des Praktikumsnetzes soll nur angeschaut aber nicht verwaltet werden. (Abbildung 2.1 und Abbildung 2.2)

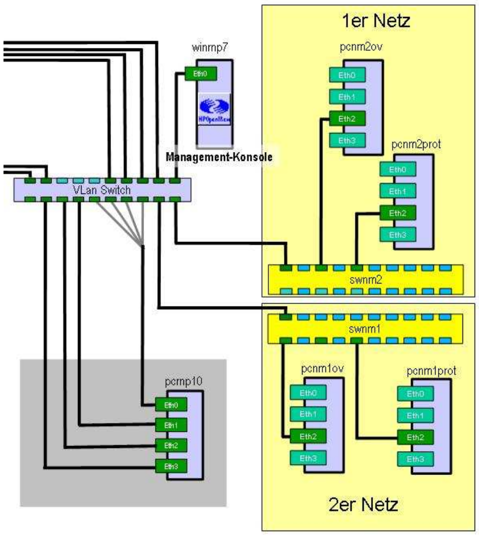

Abbildung 2.2: Ausschnitt des Managementsubnetzes vom Praktikumsnetz

2.1.3 Beschreibung des Routerrechners PCRNP10

Der Rechner `PCRNP10` ist der wichtigste Rechner im Praktikumsnetz. Dieser Rechner ist ein Routerrechner mit 4 Ethernet Interfaces und 3 zusätzlichen virtuellen Interfaces. Die Liste der Interfaces finden Sie im Anhang. Die Liste wurde mit dem Befehl `ifconfig -a` erstellt. Dieser Befehl erwies sich als sehr nützlich während des FoPras. Dieser Rechner ist für das Routing zwischen den Subnetzen und für die DNS (**D**omain **N**ame **S**erver) Auflösung zuständig.

2.2 Konfiguration der Managementkonsole

Die Managementsoftware läuft auf dem Rechner `WINRP7`. Wie schon der Rechnername verrät, handelt es sich dabei um einen Windows Rechner, in unserem Fall um einen Rechner mit Microsoft Windows 2003 Server. In den folgenden Absätzen werden die notwendigen Konfigurationsänderungen beschrieben.

2.2.1 Konfiguration der Netzwerkeinstellungen von WINRNP7

Als erster Schritt mussten die Netzwerkeinstellungen überprüft werden. Dies macht man am besten in dem Eingabeaufforderungsfenster mit dem Befehl `ipconfig /a` Als Ergebnis erhält man alle in das Betriebssystem eingehängten Netzwerkkarten. Gemeint sind die Netzwerkkarten, die in dem gerade aktiven Hardwareprofil aktiv und ohne Konflikt vorhanden sind. Diese kann man in dem Gerätemanager unter Netzwerkkarten überprüfen Diese Ergebnisliste liefert nicht nur die Netzwerkkarten sondern auch deren Hardwareadresse und die zugewiesene IP Adressen. Diese Adresse wird auch MAC Adresse (**M**edia **A**ccess **C**ontrol) genannt. Mehr Information dazu finden Sie unter:

http://de.wikipedia.org/wiki/MAC-Adresse

Anhand dieser Informationen kann man die Netzintegrität des Rechners überprüfen. Diese war soweit in Ordnung. Als nächster Schritt sollten die Gateway, Routing und DNS Informationen validiert werden. Man soll dazu den Routerrechner und einen anderen Rechner in einem anderen Subnetz zuerst mit der IP Adresse, dann mit Hostnamen anpingen. Dies macht man mit dem Befehl `ping [IP]` bzw. `ping [Hostname]`. Die Voraussetzung dafür ist, dass im Netz das ICMP Protokoll (**I**nternet **C**ontrol **M**essage

Protocol) nicht ausgefiltert und von dem Zielgerät nicht geblockt wird, ansonsten erhält man keine Antwort. In so einem Fall muss man sich andersweitig helfen. In dem Praktikumsnetz war das ICMP Protokoll weder geblockt noch gefiltert. Falls der Ping Befehl mit der IP Adresse ein Ergebnis und kein Timeout liefert, sollte man dasselbe mit Hostnamen versuchen. Falls dies zu einem Timeout führt sollten die Eigenschaften von TCPIP in dem Konfigurationsfenster der Netzwerkkarte überprüft werden. Der DNS Server ist in unserem Fall der `PCRNP10`. Dieser Fehler deutet auf DNS Auflösungsproblem hin.

2.2.2 Aktualisierung des Betriebssystems von WINRNP7

Wie schon in der Einführung erwähnt wurde, läuft die alte Version von HP OV NNM auf einem alten HP Rechner unter HP-UX. Die Konfiguration des Betriebssystems und der Managementsoftware wurde mit der Zeit entstellt, die eine Bereinigung erfordert hätte. Statt der Bereinigung und Neuinstallation wurde nicht nur für eine einfache Neuinstallation sondern gleich für eine neue Version von HP OV NNM auf einer neuen Basis, nämlich Microsoft Windows 2003 Server entschieden. So wurde die neue Version von HP OV 6.41 von HP UX auf Microsoft Windows 2003 Server umgestellt. Als offizielle Voraussetzung werden an das Betriebssystem keine besonderen Anforderungen gestellt. Auf dem Rechner wurde Windows 2003 Server mit Microsoft Internet Information Server (IIS) installiert.
Als erster Schritt musste natürlich die Aktualität des Betriebssystems geprüft werden. Diese Prüfung hat ergeben, dass noch einige Updates und Hotfixies für das Betriebssystem installiert werden mussten. (s.S Abbildung 2.3)

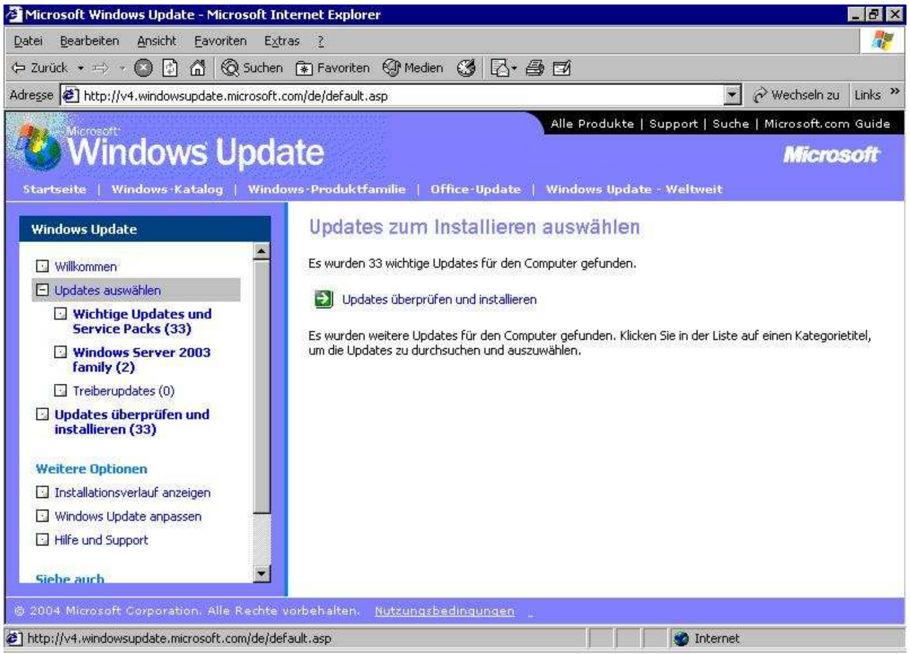

Abbildung 2.3: Installation der benötigten Updates und Hotfixies

Dieser Schritt musste während des Fopras öfters wiederholt werden, um die Aktualität, Stabilität und Sicherheit des Betriebssystems gewährleisten zu können.
Da die Managementsoftware teilweise auch mit Java arbeitet, musste Java JRE (**J**ava **R**untime **E**nvironment) nachinstalliert werden. Diese wurde von der JAVA Seite (http://java.sun.com/) von SUN geholt und eingespielt. Als das Betriebssystem aktualisiert worden ist, wurde die Managementsoftware Test weise gestartet und überprüft wie viel die Managementsoftware von dem Praktikumsnetz erkennt. Wie das Bild 2.4 zeigt, wurde eigentlich nur das Netzsegment, in dem sich die Managementkonsole selber befindet – erkannt sonst nichts. Um dies zu verbessern waren noch einige Einstellungen am Betriebssystem und an der Managementsoftware nötig. Die Änderungen am Betriebssystem werden in den anschließenden

Absätzen beschrieben, die von der Managementsoftware in den Absätzen danach.
Die Managementsoftware selber zeigt nicht die Geräte, sondern deren Interfaces. Diese werden in dem Netzmanagementbereich Nodes (Knoten) genannt. Wenn in dem Netzmanagementbereich von Geräten gesprochen wird, dann wird in der Regel ein Gerät mit mehreren Interfaces gemeint. Im Rechnernetze-Praktikum ist der Rechner `PCRNP10` ein sehr gutes Beispiel dafür. Dies ist empfehlenswert vor Augen zu halten, denn Geräte mit mehreren Interfaces in diesem Bereich verwaltet, überwacht und konfiguriert werden. Das heißt, dass alle Ports eines managbaren Switches bzw. Rechners in der Managementkonsole\ Managementsoftware erkannt und angezeigt werden müssen. Die Abbildung 2.4 zeigt, wie das Praktikumsnetzwerk mit Defaultwerten von der Managementsoftware angezeigt wurde, was der Topologie in der obigen Abbildung entsprechen sollte. Was nicht der Fall war.

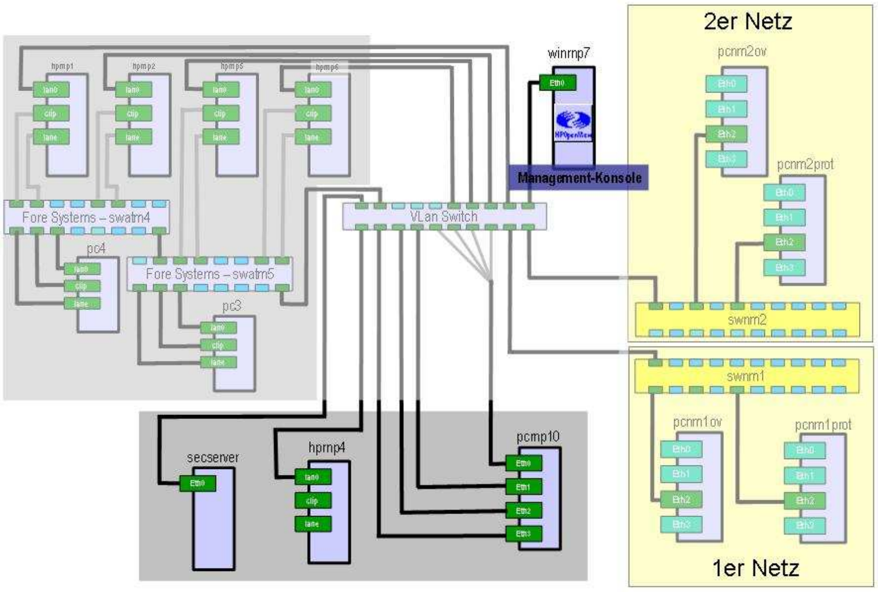

Abbildung 2.4: Das erkannte Praktikumsnetzwerk mit Defaultwerten

2.2.3 SNMP Konfiguration der Managementkonsole

Nachdem die Netzwerkeinstellungen von `WINRNP7` überprüft wurden, konnte man die anderen Rechner anpingen. Um einen Knoten mittels SNMP Abfragen zu können, muss dieser Knoten SNMP mäßig konfiguriert werden. Dies bedeutet einerseits, dass ein SNMP Dienst laufen muss, anderseits sollten paar MIBs (**M**anamegement **I**nformation **B**ase) konfiguriert werden.
Als erstes sollte der sog. Community String gesetzt werden. Dies dient zur Autorisierung. Dadurch wird erst eine Abfrage eines Knotens möglich. Der Community String wird in dem Knoten von dem Administrator gesetzt, und horcht nur auf diesen. Falls man einen Knoten mit falschem Community String abfragen will, wird dieser nicht antworten. Meistes kann man Informationen mit Angabe des Community Strings `public` gewisse Informationen abfragen. Darauf soll man sich aber nicht verlassen. Diese ist nicht mehr eine zeitgemäße Autorisierung, es hat sich aber so entwickelt. Dieser Community String wird als Plaintext verschickt, kann also abgehört werden. Das SNMP Protokoll ist ein Klartext Protokoll, und kann ohne meistens ohne große Aufwand abgehört werden. Es gibt bereits Ansätze in die Richtung sicherer SNMP Kommunikation, diese hat sich bisher aber nicht durchgesetzt.
Der Community String heißt im Praktikumsnetz, wie das Praktikum selber: **R**echner**N**etze**P**raktikum. In userem Fall heißt es, dass dieser String und die Kontaktdaten anpasst werden mussten. Der SNMP Dienst war installiert, bloß nicht an das Praktikumsnetz angepasst. Die Einstellungen wurden unter Verwaltung, Dienste über das Eigenschaftsfenster des SNMP Dienstes vorgenommen.

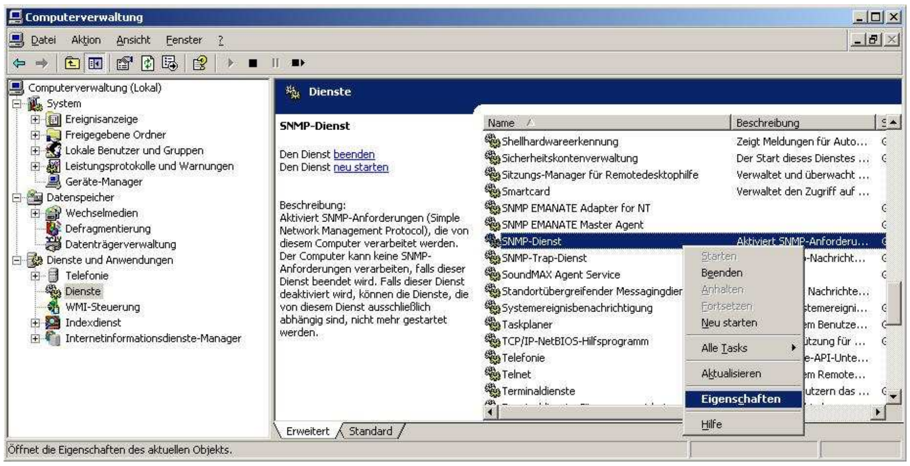

Abbildung 2.5: Diensteverwaltung von Microsoft Windows 2003 Server

Mit einem rechten Mausklick auf den SNMP Dienst, kann Eigenschaften aus dem Kontextmenü gewählt werden, um zu dem Eigenschaftenfenster von SNMP Dienst zu gelangen (siehe Abbildung 2.6). In diesem Fenster kann der SNMP Dienst konfiguriert werden. Die Tabelle 2.1 listet die notwendige Einstellungen.

Register	Beschreibung	Wert bzw. Einstellung
Agent	Kontakt Standort Dienst: Physisch Dienst: Anwendungen Dienst: Datenverbindung Subnetz Dienst: Internet Dienst: End-to-End	rnp@ifi.lmu.de LMU Muenchen, Oettingenstr. 67 Raum D7 deaktivieren aktivieren deaktivieren aktivieren aktivieren
Allgemein	keine Einstellung vornehmen	-
Traps	Communityname: Trapziele hinzufügen	rnp, public
Sicherheit	Authentifiezierungstrap senden Akzeptierte Communitynamen: hinzufügen SNMP-Pakete von jedem Host annehmen	aktivieren rnp: nur lesen aktivieren
Abhängigkeiten	keine Einstellung vornehmen	-

Tabelle 2.1: Einstellungen des SNMP Dienstes auf `WINRNP7`

Ob diese SNMP Einstellung erfolgreich war, lässt sich mit folgendem Befehl auf `WINRNP7` prüfen:
`snmpget -c rnp 127.0.0.1 system`

2.2.4 Einrichtung der Praktikumskennungen auf der Managementkonsole

Als letzte Einstellung des Betriebssystems sollten noch zwei Kennungen eingerichtet werden, damit ein entferntes Einloggen überhaupt möglich wird. Damit wird gleich das Problem angesprochen, das sich aus dem Unterschied der zwei Betriebssysteme ergibt.
Solange unter Unix die Möglichkeit des sicheren Verbindungsaufbaus (über SSH – **S**ecure **SH**ell) mit der Weiterleitung einer X Server Session (über die Option X) besteht, hat man diese Möglichkeit bei Windows 2003 Server nicht. Diese Möglichkeit wurde bisher genutzt um von einem Linux Rechner mit einem laufenden X-Server auf die HP Rechner zugreifen zu können. (Der X Server dient zur Darstellung der graphischen Oberfläche.) Nach der Anmeldung über SSH konnte HP OV NNM gestartet werden. Die graphische

Oberfläche von HP OV NNM, dank der Weiterleitung der X Sitzung, erscheint auf dem Clientrechner, in unserem Fall auf dem Linux Rechner.
Der Zugriff auf die Netzmanagementsoftware wurde ebenfalls auf Remote Terminal Session umgestellt, da es nicht nur komfortable Benutzung bietet, sondern weil die Einrichtung eines SSH und X Servers auf Windows nur über Umwegen realisierbar ist, das heißt, dass es durchaus möglich ist, diese beiden Server mit Hilfe von CygWin zu installieren. Diese hätte aber eine nicht einschätzbare Konfigurationsaufwand bedeutet. Um eine Remote Terminal Sitzung eröffnen zu können, war die Einrichtung zweier Benutzerkennungen (`praktiku` und `praktiku1`) mit speziellen Berechtigungen, die das Eröffnen einer Terminal Client Sitzung erlauben, erforderlich. Zwei Kennungen werden hierzu benötigt, da es nicht möglich ist, von zwei Clients aus mit der selben Kennung eine Remote Terminal Session zu eröffnen. Technisch ist es zwar möglich, die andere Remote Terminal Sitzung wird aber getrennt. Um diese Remote Terminal Sitzung benutzen zu können, musste auch an den Client Rechner ein Softwarepaket installiert werden. Dies wird aber später in Abschnitt 2.5.2 behandelt. Um die Benutzer mit entsprechenden Berechtigungen anzulegen, muss unter Computer-Verwaltung den Knoten Benutzer und Gruppen markieren, dann den Knoten Benutzer markieren und mit der rechten Maustaste in die rechte Fensterhälfte klicken und aus dem Kontextmenü „neuen Benutzer“ erstellen auswählen. In dem Eigenschaftenfenster des neuen Benutzers können die Berechtigungen gesetzt werden. Die Einstellungen der Benutzer wurden, wie in der Tabelle 2.2 zeigt, gesetzt.

Register	Beschreibung	Wert bzw. Einstellung
Allgemein	Benutzer kann Kennwort nicht ändern Kennwort läuft nie ab	aktivieren aktivieren
Mitgliedschaft	folgende Gruppen hinzufügen	Benutzer, Hauptbenutzer, Remotedesktopbenutzer, rnp
Profil	keine Einstellung vornehmen	-
Umgebung	Beim Anmelden Verbindung zu Clientlaufwerken herstellen Beim Anmelden Verbindung zu Clientdruckern herstellen Standardmäßig den Hauptdrucker des Clients verwenden	aktivieren aktivieren aktivieren
Sitzungen	Getrennte Sitzungen beenden Zeitlimit für aktive Sitzungen Wenn das Sitzungslimit erreicht oder die Verbindung getrennt wurde Erneuerte Sitzung zulassen	nie nie Sitzung beenden von einem beliebigen Client
Remoteüberwachung	keine Einstellung vornehmen	-
Terminaldienstprofile	Eröffnen einer Remote Terminal Sitzung erlauben keine andere Einstellung vornehmen	aktivieren -
Einwählen	RAS Berechtigung (Einwählen oder VPN) Anruferkennung verifizieren Rückrufoptionen Statische IP Adresse zuweisen Statische Routen anwenden	Zugriff verweigern deaktivieren kein Rückruf deaktivieren deaktivieren

Tabelle 2.2: Einstellungen der Remotebenutzerkennungen auf `WNRNP7`

Damit wären die grundlegenden Einstellungen an der Managementkonsole gemacht. Als nächstes müssen die Einstellungen der Managementsoftware geprüft und angepasst werden. Der nächste Abschnitt behandelt also diese Einstellungen. Die Änderungen sind zwar nicht alle an dem Managementtool direkt vorgenommen, werden aber der Managementsoftware zugeordnet, obwohl diese z.B. an dem Betriebsystem vorgenommen wurden, da diese Einstellungen eher mit der Managementsoftware zusammenhängen.

2.3 Konfiguration der Managementsoftware HP OV NNM

Diejenigen, die gerne die Managementsoftware von HP gerne ausprobieren würden, gibt es eine Testversion von HP OV NNM unter:

http://www.managementsoftware.hp.com/downloads/evals.html

Nach dem das Betriebssystem konfiguriert war, konnte man die Managementsoftware starten und anschauen, was die Software alles erkannte. Dieser Zustand war nicht der, der als Ziel gesetzt worden ist. Dies hatte mehrere Gründe, zum einem die Software benötigt einige Zeit um das Netz zu entdecken, zum anderen musste natürlich auch die Managementsoftware noch konfiguriert werden. Die zum Netzdiscovery benötigte Zeit ist nicht zu vernachlässigen, da die Software nicht nur die Nodes entdecken soll, sondern diese in eine Datenbank schreibt. Die Daten werden von der Managementsoftware ständig aktualisiert und die Topologie anhand der mitgeführten Topologiedatenbank erstellt und ebenfalls aktualisiert wird. Man kann zwar die Pollingslimit herunter setzen, damit die Nodediscovery schneller vorangeht, diese verursacht aber eine dementsprechende Netzlast.

Bevor man aber an der Konfiguration was ändert, sollte auf jedem Fall die Aktualität der Managementsoftware überprüft werden. Diese Überprüfung hat ergeben, dass einige fehlenden Updates noch installiert werden müssen. Die Updates sind über folgende Seite erreichbar:

http://www.managementsoftware.hp.com/downloads/index.html

Es wird dazu ein „HP Passport sign-in“ Account benötigt. Man kann sich frei anmelden. Man muss nur einige Daten angeben. Die HP OV Support Seite:

http://support.openview.hp.com/support.jsp?fromOV=false

mit dem zugehörigen Forum erwies sich als eine sehr nützliche Anlaufstelle.

Nach der Installation der Updates zeigte sich vom Praktikumsnetz erfasste Topologie immer noch nicht als zufrieden stellend, weshalb in den Foren nach Hinweisen gesucht wurde. Dort wurde erwähnt, dass man gewisse Änderungen auch an der Hosts Datei vornehmen muss.

2.3.1 Einrichtung der Hosts Datei auf WINRNP7

Da nicht alle Geräte in dem Praktikumsnetz gefunden wurden, wusste ich nicht weiter. Da habe ich mich in den Foren von HP erkundigt und gefragt, woran es liegen könnte. Dort habe ich erfahren, dass bei dieser Version von HP OV NNM einige Änderungen an der Hosts Datei vorgenommen werden soll. Diese Einstellung ist besonders bei VLAN (**V**irtual **L**ocal **A**rea **N**etwork) erforderlich, da diese oft denselben Adressraum für verschiedene Netzsegmente nutzen. (Ich möchte hier auf den erhaltenen Antworten in dem Forum von HP IT Resource Center hinweisen. Suchen Sie dort bitte nach „how to get NNM 6.4 to show VLAN?“)

In diese Datei sollen die IP Adressen der Routerrechner eingetragen werden, damit die Managementsoftware den weiteren Weg in die anderen Subnetze findet. Diese Datei befindet sich bei Windows unter:

```
[SystemDrive]:\Windows\system32\drivers\etc\
```

Diese Datei musste um alle IP Adressen des Routerrechners `PCRNP10` erweitert werden. Folgende Einträge mussten also gemacht werden. Die vollständige Datei finden Sie im Anhang A.

```
192.168.215.10   pcrnp10
192.168.215.33   pcrnp10
192.168.215.129  pcrnp10
192.168.215.225  pcrnp10
192.168.215.17   pcrnp10
192.168.215.209  pcrnp10
```

```
192.168.215.193 pcrnp10
```

Mit einer neueren Version von HP OV hat HP die sog. Extended Node Discovery eingeführt, die diese Änderung der Hosts Datei nicht mehr benötigt. Nach dieser Änderung sollte man der Software noch einige Zeit geben, damit sie sich an die neue Situation anpassen und die Nodes pollen kann. Nach dem Warten kann man die Liste der erkannten Geräte auch listen lassen. Diese lässt sich mit dem folgenden Befehl ausgeben oder in eine Datei umleiten. So eine Liste finden Sie im Anhang B. Diese Liste kann sehr lang sein und sollte eigentlich zur Überprüfung dienen, ob ein Node im Netzwerk gefunden wurde.

```
ovtopodump –L > C:\ovotopodump.txt
```

oder allgemein:

```
ovtopodump –L > [driveLetter]:\[filePath]\[fileName].txt
```

Diese Liste enthält nicht nur die Hardwareadressen sondern auch die IP Adressen und gegebenenfalls auch die Hostnamen.
Wie schon oben erwähnt wurde, wird die Erkennung der Nodes der anderen VLANS durch die Änderung der Host-Datei erreicht. Dies bedeutet, dass wir in unserem Fall alle Interfaces von `PCRNP10` (Routerrechner mit 4 Ethernet Interfaces und 3 zusätzlichen virtuellen Interfaces). Sie finden alle Interfaces von `PCRNP10` als Ausgabe des Befehls `ifconfig -a` im Anhang D. in die Hosts Datei aufgenommen werden mussten, und nicht nur jenes, das sich in demselben Subnetz, in welchem selbst die Managementstation ist befindet. Die Änderung der Hosts Datei ist eine Änderung der Einstellungen des Betriebssystems, was in diesem Fall eher eine benötigte Änderung der Managementsoftware zugeschrieben werden soll, da ohne diese Änderung funktionierte das Betriebssystem zwar einwandfrei, nicht aber die Managementsoftware. Sie finden die geänderte Datei im Anhang.
Damit war für die Managementsoftware alles bekannt. Bloß die Darstellung entsprach nicht der Zielsetzung, weshalb wieder Informationen besorgen werden musste. Es wurde nicht alles angezeigt, obwohl alles erkannt zu sein schien. Hilfe zu diesem Problem wurde in Foren Foren und in dem Handbuch ([HPOVNNM 03], Seite 184-194) gefunden. Die dazu benötigten Änderungen werden durch die Änderung der `netmon.lrf` Datei ereicht. Sie finden die gesamte Listing dieser Datei im Anhang C.

2.3.2 Änderung des LRF - Local Registration File auf WINRNP7

Eine Änderung der `netmon.lrf` Datei (**L**ocal **R**egistration **F**ile) war erforderlich, damit alle Interfaces eines Geräts schön aufgefächert dargestellt werden. Durch diese Datei werden gewisse Startoptionen an HP OV NNM beim Start mitgegeben. Diese wichtige Datei befindet sich auf dem `WINRNP7` unter

```
[systemdrive]:\[Program Files]\HP OpenView\lrf\netmon.lrf
```

Damit alle Subnetze in die Topologie eingetragen werden, muss die Reduktion ausgeschaltet werden, was man mit der Option „-k segRedux=false“ erreicht. Damit alle nicht IP Knoten auch angezeigt werden wurde zusätzlich die Option „-k discoverLevel2Nets=true“ eingefügt. Weitergehende Informationen finden Sie im Handbuch ([HPOVNNM 03], Seiten 184-194).
Die ganze angepasste Datei finden Sie als Listing im Anhang. Mit diesem Schritt ist die grundlegende Einstellung der Managementsoftware fertig. In den nächsten Abschnitten wird die Konfiguration des Webinterfaces und das Reporting vorgestellt. Diese gehören zwar zu der Managementsoftware, bilden aber keine Einheit damit. Man könnte diese als eine Art Zusatzmodule betrachten, die man zusätzlich konfigurieren kann, ist aber nicht zwingend notwendig. Diese Module greifen auf den Datenbestand von HP OV NNM bzw. auf die im Hintergrund laufenden Dienste zu.

2.3.3 Einstellungen des Webinterfaces von NNM

Um die Funktionalität von HP OV NNM übers Webinterface nutzen zu können, müssen einige Einstellungen vorgenommen und paar Sachen beachtet werden.

Bemerkung:
Der Zugriff übers Webinterface auf die Maps und auf die Daten kann nur erfolgen, wenn am Managementkonsole selber HP OV NNM läuft[1].

Die einfache Lösung um HP OV NNM laufend zu halten ist, dass man sich mit einer Kennung an der Konsole einloggt und HP OV NNM startet, dann die Konsole sperrt (Windowstaste und die Taste „L“).

Es gibt auch eine eingebaute Zugriffsteuerung in der Managementsoftware. Diese ist auch Gruppen bzw. Benutzer basiert. Als erstes muss natürlich für jeden Benutzer das Passwort gesetzt werden. Dies wird mit dem Befehl:

```
[systemdrive]:\[Program Files]\HP OpenView\www\bin\ovhtpasswd [Benutzername]
```

erledigt. Man erhält ein Prompt, bei dem Passwort eingegeben werden soll. Die Passwörter sind in der Datei `htpasswd` gespeichert. Diese Datei befindet sich in:

```
[systemdrive]:\[Program Files]\HP OpenView\www\etc\htpasswd
```

Es muss unbedingt ein Passwort angegeben werden. Leeres Passwort wird nicht akzeptiert, da die Mindestlänge eines Passwortes auf 4 Zeichen beschränkt ist.
Die Benutzer können verschiedenen Gruppen zugewiesen werden. Die Benutzer werden in der Datei `htgroup` in Gruppen aufgenommen werden. Diese Datei befindet sich unter:

```
[systemdrive]:\[Program Files]\HP OpenView\www\etc\htgroup
```

Der Einfachkeit halber wurde die `praktiku` Kennung in die Gruppen `NetworkAdmin` und `NetworkOper` aufgenommen. Sie finden weitere Details dazu in dem NNM Handbuch ([HPOVNNM 03], Chapter 14-NNM on the Web, S.488). Sie finden die Listing der Datei im Anhang E.
Es gibt die Möglichkeit, dass nur gewisse Benutzer auf das Webinterface zugreifen dürfen. Diese wird mit einer sog. „Session Configuration File“ gesteuert. Diese befindet sich unter:

```
[systemdrive]:\[Program Files]\HP OpenView\NNM\conf\session.conf
```

Um die Konformität etwas zu erhöhen wurde diese Option „UserLogin: off“ abgeschaltet. Die Listing der Datei befindet sich im Anhang F.
Wenn all diese Einstellungen vorgenommen wurden, konnte man sich der detaillierten Konfiguration des Webservers widmen. Diese wird in dem nächsten Abschnitt als Abschluss der Konfiguration des Webinterfaces behandelt.

2.4 Konfiguration des Webservers auf WINRNP7

Um die Funktionen der Managementsoftware übers Webinterface erreichen zu können, musste auch der Webserver eingerichtet werden. Als Webserver kommt Microsofts hauseigener Webserver IIS (Internet Information Server) zum Einsatz. Die nächsten Abschnitte beschreiben die Anpassung der Konfiguration. Zuerst musste der Perl Interpeter eingebunden werden.

[1] Vergleiche mit dem NNM Handbuch ([HPOVNNM 03], Chapter 14-NNM on the Web, S.486)

HP OV bringt ein Perl Interpreter mit sich. Dieser musste natürlich auch im IIS eingestellt werden. Der Perl Interpreter befindet sich in unserem Fall unter:

```
C:\Program Files\HP OpenView\NNM\Perl\bin
```

Dieser Pfad muss in der IIS Konfiguration unter Konfiguration des virtuellen Verzeichnisses von OvCgi eingetragen werden. Dort müssen „Skriptzugriff“ und „Lesen“ Berechtigungen gesetzt werden. Unter Anwendungseinstellungen befindet sich der Knopf Konfiguration, der ein weiteres Fenster „Anwendungskonfiguration“ öffnet. In diesem Fenster können die vorhandenen Erweiterungen bearbeitet bzw. eine neue angelegt werden. Mit dem Knopf „Hinzufügen“ öffnet sich ein neues Fenster, worin eine neue Erweiterung `.ovpl` hinzugefügt werden konnte. Hier wurde auch der Pfad zu dem Perl Interpreter eingestellt. Da ein Bild meistens mehr als tausend Worte sagt, möchte ich hier auf die Abbildung 2.6 verweisen.

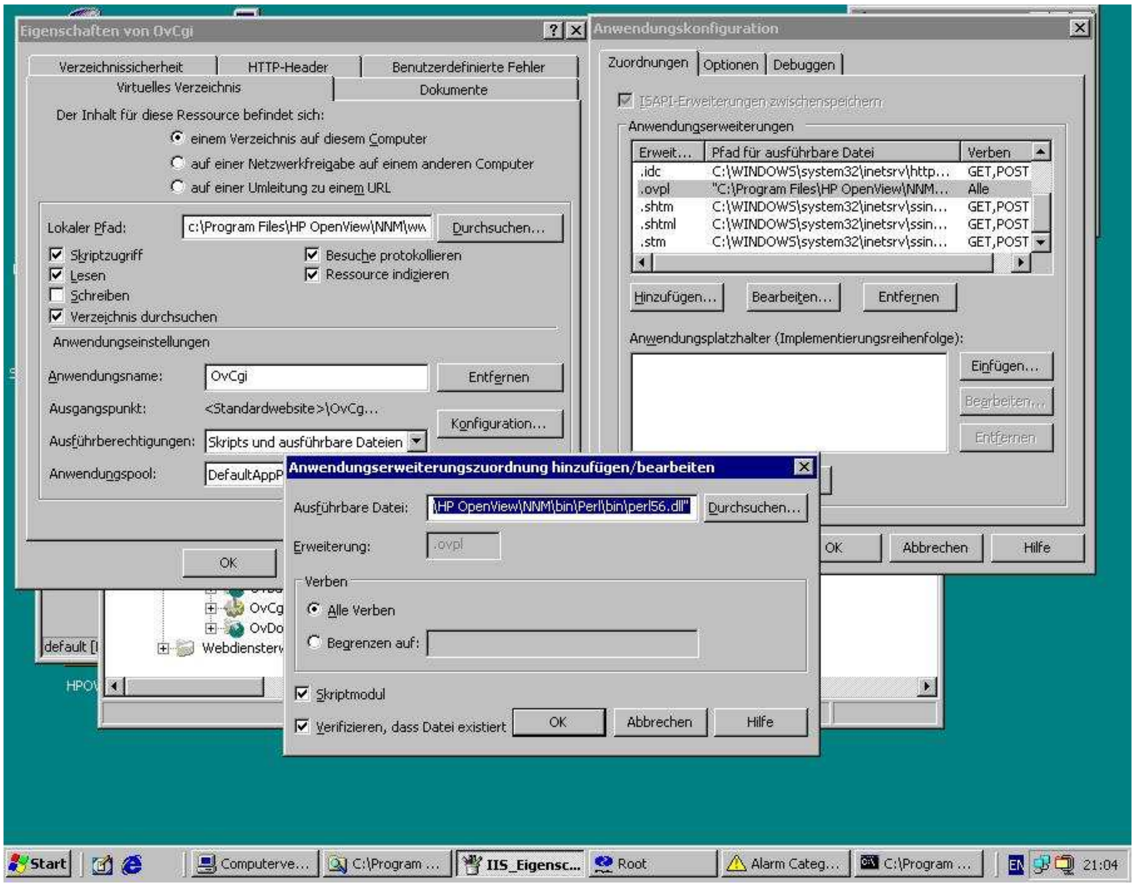

Abbildung 2.6: Die Perl Einstellungen von IIS

Damit ist noch nicht alles gemacht. Die Perl Skripte können jetzt zwar ausgeführt werden, der anonyme Zugriff auf das Webinterface sollte aber auch noch eingerichtet werden. Die ist besonders wichtig, da die Clientrechner mit Linux laufen und der Zugriff auf das Webinterface mit dem Browser Mozilla erfolgt, der die integrierte Benutzerüberprüfung à la Microsoft nicht unterstützt.

Der anonyme Zugriff auf die Webseiten von HP OV musste ebenfalls für den anonymen Zugriff eingerichtet werden. Um eine erneute Anmeldung zu vermeiden. Dieser anonyme Zugriff basiert auf einer Kennung, die bei der Installation von IIS automatisch eingerichtet wird. Der Webserver wird standardmäßig unter dieser Benutzerkennung laufen. IIS richtet bei der Installation ein Benutzerkonto IUSR_[ComputerName] ein. Siehe dazu [MS 03].

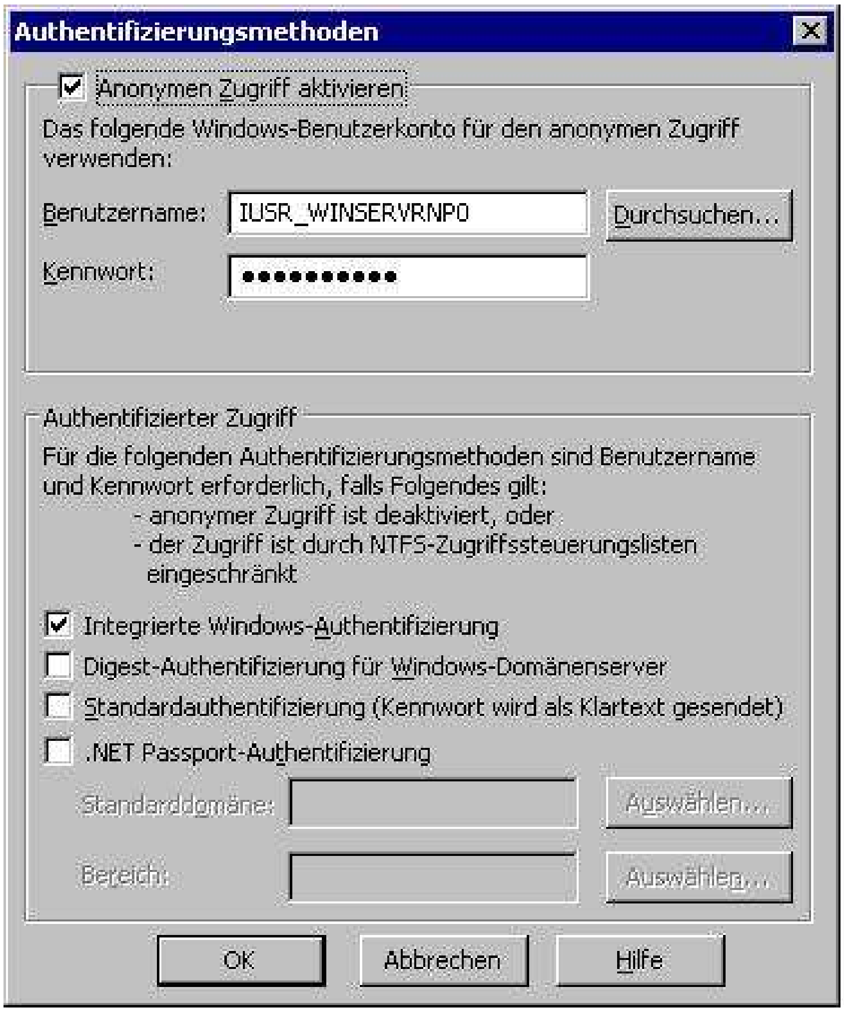

Abbildung 2.7: Einrichtung des anonymen Zugriffs

Wenn alle diese Einstellungen erfolgreich durchgeführt worden sind, dann kann die Konfiguration getestet werden, in dem das Webinterface über folgende Adresse aufgerufen wird:

http://winrnp7.rnp.nm.informatik.uni-muenchen.de:3443/OvCgi/ovlaunch.exe

Diese URL ist die Startseite des Webfrontends von HP OV. Man kann alle Funktionen über diese Seite erreichen.

2.5 Installation und Konfiguration der Clientrechner

Nachdem serverseitig alles (Betriebsystem, HP OV NNM, IIS etc.) konfiguriert wurde, mussten die Clientrechner unter die Lupe genommen werden. Dies erforderte fast soviel Zeit und Einsatz wie die bisherigen Konfigurationen, da die Konfiguration von 4 Rechnern überprüft werden musste und eine gleiche Softwarebasis geschaffen werden musste.
Auf den Client Rechner wurde SuSE Linux 9 Professional installiert. Als grafische Oberfläche (Fenstermanager) wurde FVWM installiert, da dieser wenig Ressourcen benötigt. Als zusätzliche Software mussten noch Rdekstop (Clientanwendung für die Remote Terminal Sitzung), Mozilla (Webbrowser), XV (zum Erstellen von Screenshots), MC (textbasierter Filemanager) und UCD-SNMPD (SNMP Dienst). Dieser Schritt durfte für alle 4 Rechner: `PCNM1OV, PCNM1PROT, PCNM2OV und PCNM2PROT` wiederholt werden. Nachdem alle 4 Rechner softwaremäßig gleich aussahen, mussten die Netzwerkeinstellungen geprüft werden.
Obwohl die Netzwerkeinstellungen der Clientrechner mittels DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) gesetzt wird, wurden diese aber mit:

```
ifconfig -a
```

bzw.

```
dhcpcd-test eth0
```

überprüft. Mit dem Befehl „ifconfig“ konnte überprüft werden, ob die Netzwerkkarte eine IP Adresse von dem DHCP Server erhalten hat. Mit dem Befehl „dhcpd-test eth0“ kann der DHCP IP Request- Response geprüft werden. Nach einigen Versuchen waren diese Einstellungen richtig, deshalb man sein Glück mit Ping versuchen konnte. (Siehe dazu den Abschnitt 2.2.1.) Wenn die anderen Clientrechner, `WINRNP7, PCRNP10` antworten, dann kann davon ausgegangen werden, dass die Netzkonfiguration in Ordnung ist. Diese Überprüfungen haben natürlich einige Zeit in Anspruch genommen, da auch eine gegenseitige Überprüfung erfolgte. Wenn das Netzwerk soweit konfiguriert wurde, stand nichts mehr im Wege die SNMP Einstellungen anzuschauen.

2.5.1 SNMP Konfiguration der Clientrechner

Der SNMP Dienst musste zuerst auf jedem Clientrechner installiert, dann an das Praktikumsnetz angepasst werden. Dazu musste die SNMP Konfigurationsdatei `Snmpd.conf`[2] geändert werden. Die Datei befindet sich unter:

```
/etc/snmpd.conf
```

In der SNMP Konfigurationsdatei mussten folgende Zeilen geändert werden:

```
syslocation Rechnernetze-Praktikum LMU Raum D9
syscontact Annette Kostelezky, Phone ++49-89-2178-2166
rocommunity rnp
```

Sie finden die Listing dieser Datei im Anhang G. Eine Sicherung dieser Datei wurde unter:

```
/root/sicherung/
```

angelegt. Nachdem der SNMP Dämon gestartet wurde:

[2] Nähere Informationen finden Sie in den Man-Pages. snmpd.comnf (5)

```
/etc/init.d/snmpd -start
```

kann die Richtigkeit der Einstellungen, wie folgt überprüft werden:

```
snmpwalk [RechnerName] rnp system
```

z.B.

```
snmpwalk pcnm1prot rnp system
```

Wenn die SNMP Einstellungen korrekt waren, musste der SNMP Dienst in die Liste der automatisch startenden Dienste hinzugefügt werden. Dies wurde mit einem einfachen Link (ln) Befehl erledigt. Der SNMP Dienst wurde dem Runlevel 5 hinzugefügt. Der SNMPD Startskript befindet sich bei SuSE 9 unter:

```
/etc/init.d/
```

Dieses muss in das entsprechende Verzeichnis (/etc/init.d/rc5.d) verlinkt werden. Es musste beachtet werden, dass dort zwei Verlinkungen erforderlich sind, eine für das Starten und eine für das Stoppen des Dienstes.

```
ln -s /etc/init.d/snmpd /etc/init.d/rc5.d/S08snmpd
ln -s /etc/init.d/snmpd /etc/init.d/rc5.d/K08snmpd
```

Die zwei Verknüpfungen unterscheiden sich nur in dem Anfangsbuchstaben: S steht für Start und K für Kill (Stop). Mehr Informationen finden Sie dazu unter:
http://www.linuxfibel.de/booten.htm .
Siehe dazu [Ermer 04]. Bei der Überprüfung von SNMP musste mehrmals erfolgen, da es von jedem Clientrechner aus erfolgte.

2.5.2 Einrichtung von Remotedesktop auf den Clientrechner

Nachdem Rdesktop installiert wurde, konnte man eine Terminalsitzung mit dem folgenden Befehl eröffnen:

```
rdesktop -g1000x760 winrnp7
```

Nähere Informationen und zusätzliche Optionen finden Sie in den Man-Pages „man rdesktop“. In dem Fenster erhält man eine Terminalsitzung auf dem winrnp7 Rechner. Nach der Anmeldung mit der Praktikumskennung, kann die Managementsoftware und der Rechner, wie gewohnt benutzt werden.

2.5.3 Konfiguration der Switches SWNM1 und SWNM2

Im Praktikumsnetz befinden sich zwei managebare HP Switches. Auf diesen Switches werden die eigentlichen Managementaufgaben durchgeführt. In dem alten Zustand durften die Switches nur von der alten Managementkonsole `HPRNP4` aus verwaltet werden. Dies musste natürlich auch geändert werden. Dazu musste man sich mit der Administrator Kennung (HP nennt die zwei Modi des Switches Operator und Managermode) über Telnet in die Managementsoftware des jeweiligen Switches einloggen und dort unter „Configuration“ über die Wahl des Menüpunktes „Internet (IP) Service“ unter dem Punkt „IP Config manual“ gewählt werden. Dann kann man die IP Adresse und die Netzmaske eintragen. Damit war gewährleistet, dass diese Switsches auch von `WINRNP7` verwaltet werden dürfen. Sie finden nähere Informationen zur Schwitchkonfiguration in dem Handbuch: HP AdvanceStack Switch 208/224 Management Module Installation and Reference Guide HP J3178A. ([hpj3177], Seiten 4-8)

Kapitel 3

Zusammenfassung und Ausblick

Zusammenfassend lässt sich feststellen, dass das gesetzte Ziel von diesem FoPra erreicht worden ist, wobei die Aufwand für die Umstellung auf die neue Version von HP OV NNM nicht reibungslos, wie man es vielleicht annehmen würde, verlaufen ist. Dies lässt sich auf die Komplexität des Produktes zurückführen. Dabei muss auch erwähnt werden, dass HP OV NNM nicht ein einfaches Werkzeug für Netzwerkmonitoring ist, sondern vielmehr eine Plattform, die für Erweiterungen offen ist. Wenn man alle diese Parameter vor Augen hält, kann man sich ungefähr vorstellen, wie mächtig diese Tool ist, was einerseits dessen Vorteil ist, andererseits eine Konfigurationskomplexität verursacht.
Nach all diesen Beobachtungen möchte ich zuerst die Konfigurationsänderungen zusammenfassen und anschließend für eventuelle Verbesserungen Anregungen geben.

3.1 Zusammenfassung

Die Umstellung der Versuche auf die neue Version von HP OV NNM konnte nicht ohne weiteres gemacht werden, obwohl es bei dem Produkt um dasselbe handelt, bloß in neuerer Version.
Im ersten Schritt mussten die vorhandenen Netzwerkeinstellungen von `WINRNP7, PCRNP10` und Clients (`pcnmXov, pcnmXprot, swnmX`) überprüft und ggf. angepasst werden. Obwohl die Netzwerkeinstellungen der Clientrechner mittels DHCP konfiguriert werden, wurden die Einstellungen trotzdem überprüft. An dieser Stelle muss der zentraler Rechner `PCRNP10` erwähnt werden, da dieser Rechner für das Routing zuständig und die IP Adressen mittels DHCP verteilt.
Im nächsten Schritt mussten die SNMP Einstellungen auf allen Rechnern konfiguriert und getestet werden. Nach all dem konnte ich mich dem neuen Terminalserver `WINRNP7` widmen. Mit dem neuen Rechner kam nicht nur ein neuer Rechner dem Praktikumsnetz hinzu, sondern auf gleich ein neue Plattform (Windows 2003 Server). Auf diese neue Maschine wurde die neue Version von HP OV installiert, die samt Betriebssystem an das Praktikumsnetz angepasst werden musste. Nach der Installation mussten zuerst die Netzwerkeinstellungen überprüft werden. Nachdem sowohl das Praktikumsnetz als auch das Internet erreichbar war, konnte das Betriebssystem und die Managementsoftware aktualisiert werden.

Als nächstes musste die Managementsoftware angepasst werden. An der Managementkonsole musste die Hosts Datei um einige Einträge erweitert werden, damit die Managamentsoftware auch in VLANs hinüberschauen kann. Damit das automatisch entdeckte Netzwerk „schön“ angezeigt wird, musste noch eine weitere Datei `netmon.lrf` modifiziert werden. Diese Datei beinhaltet die Startoptionen für HP OV. Damit

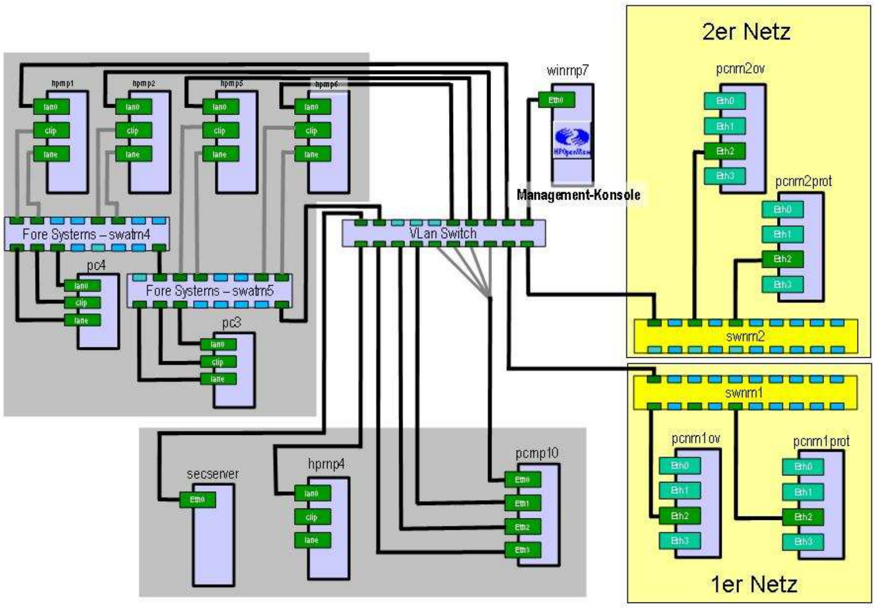

Abbildung 3.1: Das erkannte Praktikumsnetzwerk nach den Anpassungen

die Studenten das ganze benutzen können, wurden zwei Benutzeraccounts eingerichtet, die als notwendige Voraussetzung für eine Anmeldung über Remote Terminal Session dienen. Dementsprechend wurde auf die Clients Xdesktop installiert.
Jetzt musste nur noch die Verwaltungsberechtigung an den managbaren HP Switches für die Managementkonsole gesetzt werden. Die HP Switches haben zwei Zugangsarten für Benutzer und für Administratoren. Nur im sog. Admin Modus kann die Managementberechtigung für Rechner über das Netzwerk gesetzt werden. Die HP Switches habe einen IP Filter, der manuell gepflegt werden muss. Dieser Filter beinhaltet die IP Adressen der Rechner, die im Admin Modus den Switch über das Netzwerk verwalten dürfen.
Schließlich wurden die IIS Einstellungen für das Webinterface gesetzt und getestet werden.
Nachdem das Praktikumsnetz samt Subnetzen entdeckt wurde, konnten die Praktikumsaufgaben anhand der Anleitung nachgespielt werden.
Die Abbildung 3.1 zeigt das erkannte und angezeigte Praktikumsnetzwerk nach den gemachten Einstellungen.

3.2 Ausblick: Erweiterung der Rdesktop Anmeldung

Die Anmeldung mittels rdesktop könnte auch etwas komfortabler gestaltet werden. Dazu könnte man Tsclient installieren. Tsclient ist eine Remote Terminal Session Client Anwendung mit grafischem Benutzerinterface.
Eine andere ebenfalls interessante Sache, die gewisse Erleichterung bedeuten würde, betrifft den Datenaustausch zwischen dem Clientrechner und dem Managementrechner. Bei der Anmeldung über Remote Terminal Session hat man die Möglichkeit lokale Laufwerke einzubinden. Dazu würde man unter Linux auf dem Clientrechner einen installierten Samba Server benötigen. Über den Samba Server könnte man das Home Verzeichnis des angemeldeten Benutzers in die Remote Terminal Session als Laufwerk einbinden.

Diese beiden Erweiterungen würden eine komfortable Benutzung ermöglichen.

Anhang A

Die Hosts Datei

In Windows befindet sich die Hosts Datei unter:

```
[SystemDrive]:\ Windows\system32\drivers\etc\hosts
```

In diese Datei sollen die IP Adressen der Routerrechner (PCRNP10) eingetragen werden, damit die Managementsoftware den weiteren Weg in die anderen Subnetze findet. Diese Datei musste also um alle IP Adressen des Routerrechners PCRNP10 erweitert werden. Diese Einstellung ist besonders bei VLAN (**V**irtual **L**ocal **A**rea **N**etwork) erforderlich, da diese oft denselben Adressraum für verschiedene Netzsegmente nutzen. (Ich möchte hier auf die erhaltenen Antworten in dem Forum von HP IT Resource Center hinweisen. Suchen Sie dort bitte nach “how to get NNM 6.4 to show VLAN? “)

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Dies ist eine HOSTS-Beispieldatei, die von Microsoft TCP/IP
# üfr Windows 2000 verwendet wird.
#
# Diese Datei äenthlt die Zuordnungen der IP-Adressen zu Hostnamen.
# Jeder Eintrag muss in einer eigenen Zeile stehen. Die IP-
# Adresse sollte in der ersten Spalte gefolgt vom özugehrigen
# Hostnamen stehen.
# Die IP-Adresse und der Hostname ümssen durch mindestens ein
# Leerzeichen getrennt sein.
#
# äZustzliche Kommentare (so wie in dieser Datei) öknnen in
# einzelnen Zeilen oder hinter dem Computernamen üeingefgt werden,
# aber ümssen mit dem Zeichen '#' eingegeben werden.
#
# Zum Beispiel:
#
#       102.54.94.97     rhino.acme.com          # Quellserver
#        38.25.63.10     x.acme.com              # x-Clienthost

#06.12.2004, Akos, Regi
127.0.0.1        localhost
192.168.215.7    winrnp7
192.168.215.10   pcrnp10
192.168.215.33   pcrnp10
```

```
192.168.215.129  pcrnp10
192.168.215.225  pcrnp10
192.168.215.17   pcrnp10
192.168.215.209  pcrnp10
192.168.215.193  pcrnp10
```

Anhang B

Die mit dem Befehl *ovtopodump -L* erzeugte Liste

Mit Hilfe des Befehls *ovtopodump -L* lässt sich eine Liste aller von HP OV NNM erkannten Netzwerkknoten im Netzwerk listen. Man kann anhand dieser Liste überprüfen ob ein Gerät in Netzwerk befindet und wie es von HP OV NNM erkannt wurde. Diese Liste beinhaltet die MAC Adressen, die IP Adressen (falls vorhanden) und eventuell die Hostnamen. Die folgende Listig zeigt die leicht gekürzte Liste der Geräte.

```
OBJECT ID(S)          OBJECT                     STATUS
IP ADDRESS        LINK ADDRESS
   158        -       IP Internet                              -

STATIONS:
   159        -       winrnp7                    Normal        -
  1518        -       hprnp4.rnp.nm.informatik.uni-muenchen.de  Unmanaged
-

NETWORKS:
   160        IP      192.168.215                Normal        192.168.215.0
  1534        IP      192.168.215.32             Normal        192.168.215.32
  1537        IP      192.168.215.128            Normal        192.168.215.128
  1540        IP      192.168.215.224            Normal        192.168.215.224
  1543        IP      192.168.215.16             Normal        192.168.215.16
  1546        IP      192.168.215.208            Normal        192.168.215.208
  1549        IP      192.168.215.192            Normal        192.168.215.192
  1689        IP      192.168.215.144            Normal        192.168.215.144

SEGMENTS:
   163        -       192.168.215.Segment1       Normal        -
  1535        -       192.168.215.32.Segment1  Normal        -
  1538        -       192.168.215.128.Segment1  Normal        -
  1541        -       192.168.215.224.Segment1  Normal        -
  1544        -       192.168.215.16.Segment1  Normal        -
  1547        -       192.168.215.208.Segment1  Normal        -
  1550        -       192.168.215.192.Segment1  Normal        -
  1656        -       192.168.215.Segment2       Normal        -
  1660        -       192.168.215.Segment3       Normal        -
```

```
  1690        –     192.168.215.144.Segment1  Normal      –
  1699        –     192.168.215.Segment5      Normal      –

NODES:
   162        IP    winrnp7.rnp.nm.informatik.uni–muenchen.de  Normal
192.168.215.7
   162/161    IP    winrnp7.rnp.nm.informatik.uni–muenchen.de  Normal
192.168.215.7    0x000BCDA0A959
   534        IP    hprnp4.rnp.nm.informatik.uni–muenchen.de  Normal
192.168.215.4
   534/533    IP    hprnp4.rnp.nm.informatik.uni–muenchen.de  Normal
192.168.215.4    0x080009C2D6C8
   534/1516   –     hprnp4.rnp.nm.informatik.uni–muenchen.de  Unknown
–                <none>
   534/1517   –     hprnp4.rnp.nm.informatik.uni–muenchen.de  Unknown
–                <none>
   ...


  ...
  1520        IP    vlanswitch1.rnp.nm.informatik.uni–muenchen.de  Normal
192.168.215.1
  1520/1519   IP    vlanswitch1.rnp.nm.informatik.uni–muenchen.de  Normal
192.168.215.1    0x00509969FC38
  1520/1558   IP    vlanswitch1.rnp.nm.informatik.uni–muenchen.de  Normal
192.168.215.2    0x08004ED2FEF8
  1520/1560   –     vlanswitch1.rnp.nm.informatik.uni–muenchen.de  Unknown
–                0x0001
  1520/1698   –     vlanswitch1.rnp.nm.informatik.uni–muenchen.de  Normal
–                <none>
  1520/1700   –     vlanswitch1.rnp.nm.informatik.uni–muenchen.de  Normal
–                <none>
  1522        IP    secserv.rnp.nm.informatik.uni–muenchen.de  Normal
192.168.215.5
  1522/1521   IP    secserv.rnp.nm.informatik.uni–muenchen.de  Normal
192.168.215.5    0x000476DBFA31
  1530        IP    pcrnp10                   Normal      192.168.215.10
  1530/1529   IP    pcrnp10                   Normal
192.168.215.10   0x00105A313914
  1530/1551   IP    pcrnp10                   Normal
192.168.215.33   <none>
  1530/1552   IP    pcrnp10                   Normal
192.168.215.129  <none>
  1530/1553   IP    pcrnp10                   Normal
192.168.215.225  <none>
  1530/1554   IP    pcrnp10                   Normal
192.168.215.17   <none>
  1530/1555   IP    pcrnp10                   Normal
192.168.215.209  0x001022FD4AF0
  1530/1556   IP    pcrnp10                   Normal
192.168.215.193  0x000476D1B75B
  1659        –     HP–07049D                 Normal      –
  1659/1658   –     HP–07049D                 Normal
–                0x0060B007049D
  1662        –     HP–5FC294                 Normal      –
```

```
  1662/1661    –     HP–5FC294                  Normal
–                  0x0800095FC294
  1664         –     HP–7AACEC                  Normal        –
  1664/1663    –     HP–7AACEC                  Normal
–                  0x0800097AACEC
  1666         –     HP–C279AC                  Normal        –
  1666/1665    –     HP–C279AC                  Normal
–                  0x080009C279AC
  1668         –     ForeSystem–1F13F1          Normal        –
  1668/1667    –     ForeSystem–1F13F1          Normal
–                  0x0020481F13F1
  1670         –     ForeSystem–1F14FB          Normal        –
  1670/1669    –     ForeSystem–1F14FB          Normal
–                  0x0020481F14FB
  1673         IP    pcnm2ov                    Normal        192.168.215.211
  1673/1674    IP    pcnm2ov                    Normal
192.168.215.211 0x0002B3D76330
  1673/1693    –     pcnm2ov                    Unknown
–                  <none>
  1675         IP    pcnm2prot                  Normal        192.168.215.210
  1675/1676    IP    pcnm2prot                  Normal
192.168.215.210 0x0002B3D76449
  1675/1694    –     pcnm2prot                  Unknown
–                  <none>
  1677         IP    swnm2                      Normal        192.168.215.212
  1677/1678    IP    swnm2                      Normal
192.168.215.212 <none>
  1679         IP    pcnm1ov                    Normal        192.168.215.195
  1679/1680    IP    pcnm1ov                    Normal
192.168.215.195 <none>
  1681         IP    pcnm1prot                  Normal        192.168.215.194
  1681/1682    IP    pcnm1prot                  Normal
192.168.215.194 0x0002B3D75D0D
  1681/1695    –     pcnm1prot                  Unknown
–                  <none>
  1683         IP    swnm1                      Normal        192.168.215.201
  1683/1684    IP    swnm1                      Normal
192.168.215.201 <none>
  1685         IP    pcfw2ext                   Normal        192.168.215.132
  1685/1686    IP    pcfw2ext                   Normal
192.168.215.132 <none>
  1687         IP    pcfw2int                   Normal        192.168.215.158
  1687/1688    IP    pcfw2int                   Normal
192.168.215.158 <none>
  1692         IP    hprnp5.rnp.nm.informatik.uni–muenchen.de Normal
192.168.215.45
  1692/1691    IP    hprnp5.rnp.nm.informatik.uni–muenchen.de Normal
192.168.215.45  <none>
  1697         –     0x000476A1CFAD             Normal        –
  1697/1696    –     0x000476A1CFAD             Normal
–                  0x000476A1CFAD
```

Anhang C

Die netmon.lrf Datei

Der Pfad dieser Datei ist:

```
[systemdrive]:\[Program Files]\HP OpenView\lrf\netmon.lrf
```

Durch diese Datei werden gewisse Startoptionen an HP OV NNM beim Start mitgegeben. Sie finden weitere Informationen zu dieser Datei im Handbuch ([HPOVNNM 03], ab Seite 217).

```
#
# @(#)netmon.lrf
# @(#)HP OpenView NNM Release B.06.41  Feb 23 2003
# @(#)Copyright (c) 1990-2003 Hewlett-Packard Company
# $Revision: /main/7 $  $Date: 2000/03/24 18:36 UTC $
#
# Local Registration File for Network Node Manager network monitor daemon
#
# Arguments can be placed between the second and third colons
# of the second line.  See lrf(4) and netmon(1m)
#
# Run ovaddobj(1m), ovstop(1m) and ovstart(1m) after modifying this file:
#   ovaddobj $OV_LRF/netmon.lrf
#   ovstop netmon
#   ovstart netmon
#

#06.12.2004, Akos Regi
#netmon:netmon:
#OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true:OVs_WELL_BEHAVED:15:PAUSE

netmon:netmon:
OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=false
-k discoverLevel2Nets=true
-k bridgeMIB=true:OVs_WELL_BEHAVED:15:PAUSE
```

Anhang D

Die Liste der Interfaces des Rechners pcrnp10

Der Rechner PCRNP10 ist der wichtigste Rechner im Praktikumsnetz. Dieser Rechner ist ein Routerrechner mit 4 Ethernet Interfaces und 3 zusätzlichen virtuellen Interfaces. Die Liste der Interfaces finden Sie hier. Die Liste wurde mit dem Befehl “ifconfigf -a“ erstellt.

```
pcrnp10:~ # ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:10:5A:31:39:14
          inet addr:192.168.215.10  Bcast:192.168.215.15
Mask:255.255.255.240
          inet6 addr: fe80::210:5aff:fe31:3914/10 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1547354451 errors:2070 dropped:0 overruns:4 frame:2070
          TX packets:751498485 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:2871932809 (2738.8 Mb)  TX bytes:1918958664 (1830.0 Mb)
          Interrupt:9 Base address:0xa400

eth0:0    Link encap:Ethernet  HWaddr 00:10:5A:31:39:14
          inet addr:192.168.215.33  Bcast:192.168.215.47
Mask:255.255.255.240
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:9 Base address:0xa400

eth0:1    Link encap:Ethernet  HWaddr 00:10:5A:31:39:14
          inet addr:192.168.215.129  Bcast:192.168.215.143
Mask:255.255.255.240
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:9 Base address:0xa400

eth0:4    Link encap:Ethernet  HWaddr 00:10:5A:31:39:14
          inet addr:192.168.215.225  Bcast:192.168.215.239
Mask:255.255.255.240
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:9 Base address:0xa400

eth1      Link encap:Ethernet  HWaddr 00:04:75:75:10:90
```

```
          inet addr:192.168.215.17  Bcast:192.168.215.31
Mask:255.255.255.240
          inet6 addr: fe80::204:75ff:fe75:1090/10 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2520302126 errors:0 dropped:0 overruns:6 frame:0
          TX packets:193689492 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:3403133277 (3245.4 Mb)  TX bytes:2942891137 (2806.5 Mb)
          Interrupt:5 Base address:0xa000

eth2      Link encap:Ethernet  HWaddr 00:10:22:FD:4A:F0
          inet addr:192.168.215.209  Bcast:192.168.215.223
Mask:255.255.255.240
          inet6 addr: fe80::210:22ff:fefd:4af0/10 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:51387974 errors:2 dropped:0 overruns:0 frame:2
          TX packets:20117278 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1711297021 (1632.0 Mb)  TX bytes:3552484553 (3387.9 Mb)
          Interrupt:10 Base address:0x9800

eth3      Link encap:Ethernet  HWaddr 00:04:76:D1:B7:5B
          inet addr:192.168.215.193  Bcast:192.168.215.207
Mask:255.255.255.240
          inet6 addr: fe80::204:76ff:fed1:b75b/10 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5912277 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8250416 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:885409968 (844.3 Mb)  TX bytes:4059748481 (3871.6 Mb)
          Interrupt:9 Base address:0x9400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1778209 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1778209 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:265131421 (252.8 Mb)  TX bytes:265131421 (252.8 Mb)

sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

pcrnp10:~ #
```

Anhang E

Die htgroup Datei

Die Benutzer können verschiedenen Gruppen zugewiesen werden. Die Benutzer werden in der Datei htgroup in Gruppen aufgenommen werden. Diese Datei befindet sich unter:

```
[systemdrive]:\[Program Files]\HP OpenView\www\etc\htgroup
```

Der Einfachkeit halber wurde die Praktiku Kennung in die Gruppen NetworkAdmin und NetworkOper aufgenommen. Sie finden weitere Details dazu in dem NNM Handbuch ([HPOVNNM 03], Chapter 14-NNM on the Web, ab Seite 488).

```
# NetworkAdmin
# The role of NetworkAdmin is intended for individuals who have a
# higher level of knowledge of networks.  Capabilities for configuration
# of the network, configuration of connecting devices and advanced trouble
# shooting should be associated with this user role.
#
# NetworkOper
# The role of NetworkOper is intended for individuals who do routine
# trouble shooting and maintenance tasks associated with the network.
# Capabilities for monitoring the network, routine trouble shooting and
# maintenance of the network and network devices should be associated
# with this user role.
#
# NTAdmin
# The role of NTAdmin is intended for individuals who have a higher
# level of knowledge of NT systems.  Capabilities for configuration
# of NT systems and advanced trouble shooting should be associated
# with this user role.
#
# NTOper
# The role of NTOper is intended for individuals who do routine
# trouble shooting and maintenance tasks associated with NT systems.
# Capabilities for monitoring the system, routine trouble shooting and
# maintenance of the NT system should be associated with this user role.
#
# UNIXAdmin
# The role of UNIXAdmin is intended for individuals who have a higher
# level of knowledge of UNIX systems.  Capabilities for configuration
# of UNIX systems and advanced trouble shooting should be associated
```

```
# with this user role.
#
# UNIXOper
# The role of UNIXOper is intended for individuals who do routine
# trouble shooting and maintenance tasks associated with UNIX systems.
# Capabilities for monitoring the system, routine trouble shooting and
# maintenance of the UNIX system should be associated with this user role.
#
# OVAdmin
# The role of OVAdmin is intended for individuals who do configuration and
# customization of the HP OpenView environment and management applications.
# Capabilities for configuring and customizing management applications
# should be associated with this user role.

NetworkAdmin: +
NetworkOper: +
NTAdmin: +
NTOper: +
UNIXAdmin: +
UNIXOper: +
OVAdmin: +
```

Anhang F

Die session.conf Datei

Es gibt die Möglichkeit, dass nur gewisse Benutzer auf das Webinterface zugreifen dürfen. Diese wird mit einer sog. “Session Configuration File“ gesteuert. Diese befindet sich unter:

```
[systemdrive]:\[Program Files]\HP OpenView\NNM\conf\session.conf
```

Um die Konformität etwas zu erhöhen wurde diese Option “UserLogin: off“ abgeschaltet.

```
# This value determines whether or not the user must log in.
UserLogin: off
# This value enables or disables the logging of what user is logging in.
# original value = off
LoginLogging: on
# This value enables or disables the logging of what URLs are accessed.
# original value = off
AccessLogging: on
# Integer value determining how many hours a session will exist if the
# browser is running. A value of zero turns off session timeouts.
SessionTimeout: 9
```

Anhang G

Die snmpd.conf Datei

Der SNMP Dienst musste zuerst auf jedem Clientrechner installiert, dann an das Praktikumsnetz angepasst werden. Dazu musste die SNMP Konfigurationsdatei Snmpd.conf geändert werden. Die Datei befindet sich unter:

```
/etc/snmpd.conf

# Please see /usr/share/doc/packages/ucdsnmp/EXAMPLE.conf for a
# more complete example and snmpd.conf(5).
#
# Writing is disabled by default for security reasons.  If you'd like
# to enable it uncomment the rwcommunity line and change the community
# name to something nominally secure (keeping in mind that this is
# transmitted in clear text).

# don't use ' < > in strings for syslocation or syscontact
# Note that if you define the following here you won't be able to change
# them with snmpset

syslocation Rechnernetze-Praktikum LMU Raum D9
syscontact Anette Kostelezky, Phone:+49-89-2178-2166
sysname pcnm2prot

# These really aren't meant for production use.  They include all MIBS
# and can use considerable resources.  See snmpd.conf(5) for information
# on setting up groups and limiting MIBS.
#rocommunity public 127.0.0.1
# rwcommunity mysecret 127.0.0.1
#rocommunity rnp 127.0.0.1

rocommunity rnp default
```

Literaturverzeichnis

[Ermer 04] THOMAS ERMER, MICHAEL MEYER: *Die Linuxfibel*. Saxonia Systems AG, 2004, http://www.linuxfibel.de/ .

[HAN 99] HEGERING, H.-G., S. ABECK und B. NEUMAIR: *Integrated Management of Networked Systems – Concepts, Architectures and their Operational Application*. Morgan Kaufmann Publishers, ISBN 1-55860-571-1, 1999. 651 p.

[hpj3177] HP: *HP AdvanceStack Switch 208/224 Management Module Installation and Reference Guide HP J3178A*, 1997, ftp://ftp.hp.com/pub/networking/software/59665228.pdf .

[HPOVNNM 03] HEWLETTPACKARD: *Hewlett Packard OpenView Network Node Manager, Managing your Network with HP OpenView Network Node Manager*, 2003. HP Manual.

[MS 03] MICROSOFT: *SO WIRD'S GEMACHT: Die IIS-Webauthentifizierung in Windows Server 2003 konfigurieren*. Microsoft, 2003, http://support.microsoft.com/default.aspx?scid=kb;de;324276 .