INSTITUT FÜR INFORMATIK
DER LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Praktikum Rechnernetze

Prof. Dr. H.–G. Hegering
M. Garschhammer, M. Brenner, V. Danciu

Sommersemester 2004

Netzmanagement

Inhaltsverzeichnis

Kapitel 1

NM 1 - Netzmanagement-Werkzeuge

Als ersten Schritt in die Welt des **integrierten Netzmanagements** wollen wir zunächst einen längeren Blick auf die vielzähligen kleinen Tools im alltäglichen „Werkzeugkasten des Netzadministrators“ werfen. Hierzu betrachten wir in diesem Versuch zwei sehr unterschiedliche Klassen von Werkzeugen: zum einen die SNMP-Tools und zum anderen die Protokollanalysatoren.

1.1 Einführung in die Netzmanagement-Problematik

Der folgende Einführungstext ist ein kurzer, geringfügig abgewandelter Ausschnitt aus dem Buch „Integriertes Management vernetzter Systeme - Konzepte, Architekturen und deren betrieblicher Einsatz“ von Hegering/Abeck/Neumair.

Die Beschreibung, wie sich die Management-Problematik einem Betreiber gegenüber darstellt, macht den Umfang und die Komplexität dieses Themengebiets deutlich. Im folgenden werden verschiedene Dimensionen des Managements herausgearbeitet, wodurch der Gesamtkomplex unter verschiedenen Aspekten in einzelne Teilbereiche systematischer gegliedert wird. In diesem Einführungstext geht es uns also nicht primär um eine erneute inhaltliche Darstellung von Managementaufgaben, sondern vorrangig um eine Klassifikation.

Es existiert sicherlich eine Vielzahl von Kriterien, durch die sich der Bereich des Managements in bestimmter Weise ordnen läßt. Die wohl wichtigsten Ordnungskriterien, die wir aufgrund ihrer besonderen Stellung in der Gesamtheit der Kriterien auch als **Dimensionen** bezeichnen, sind:

- Funktionale Dimension
  Diese Dimension betrifft die Zuordnung von Management-Aufgaben zu Funktionsbereichen. Durch das Management-Framework der ISO wird eine Unterteilung in die Bereiche Konfiguration, Fehler, Leistung, Abrechnung und Sicherheit vorgenommen.

- Zeitliche Dimension
  Die zeitliche Dimension teilt den Prozeß, durch den die Managementleistung erbracht wird, in verschiedene Lebenszyklusphasen auf. Es kann unterschieden werden zwischen einer Planungs-, einer Realisierungs- und einer Betriebsphase.

- Dimension der Szenarien
  Es haben sich in letzter Zeit neben dem klassischen Netzmanagement dessen zentrale Aufgabe das Komponentenmanagement ist, noch weitere „Management-Szenarien" wie Systemmanagement, Anwendungsmanagement und Enterprisemanagement herauskristallisiert. Diese Szenarien unterscheiden sich dadurch, dass sie unterschiedliche Zielobjekte als Gegenstand des Managements besitzen und dadurch zu charakteristisch anderen Managementanwendungen führen.

Wir gehen im Folgenden ausschließlich auf die funktionale Dimension näher ein.

Der Betrieb eines Kommunikationsnetzes oder eines verteilten Systems stellt verschiedenartige Aufgaben, die sich zu Aufgabengruppen zusammenfassen lassen. Da diese Gruppierung von Aufgaben offensichtlich ist, gibt es zumindest bzgl. der Definition der Management-Funktionsbereiche in den verschiedenen herstellerübergreifenden und herstellerspezifischen Managementansätzen kaum Differenzen. An dieser Stelle erfolgt nur ein kurzer Überblick; dabei orientieren wir uns an den Funktionsbereichen, die von der ISO vorgeschlagen wurden.

1.1.1 Konfigurationsmanagement

Ein Kommunikationsnetz oder ein verteiltes System besteht aus einer Vielzahl von Ressourcen, die in geeigneter Weise miteinander kooperieren müssen. Die Aufgabe des Konfigurationsmanagements besteht darin, diese Ressourcen so zu verknüpfen und anzupassen, dass die Kommunikationsleistung oder Systemfunktion auch in der erwünschten Form erbracht wird.

Voraussetzung für die Erfüllung dieser Aufgabe ist die Kenntnis der in dem Netz oder verteilten System vorkommenden Ressourcen. Diese Information ist in der **Netz-** bzw. **Systembeschreibung** enthalten. Die Entwicklung einer für die Managementbelange geeigneten Netzbeschreibung hat sich als eines der zentralen Themen in den letzten Jahren herausgestellt; die Netzbeschreibungsproblematik ist zumindestens zu einem überwiegenden Anteil dem Bereich des Konfigurationsmanagements zuzurechnen. Im folgenden wird ein Ausschnitt der in einer Netzbeschreibung zu berücksichtigenden Informationsmenge in hierarchischer Form dargestellt. Es zeigt sich, dass nicht die Quantität, sondern die Qualität der Managementinformation, die in der großen Informationsvielfalt besteht, das eigentliche Problem darstellt.

Die Netzbeschreibung ist für das Konfigurationsmanagement die Basis für die Erbringung folgender Teilaufgaben:

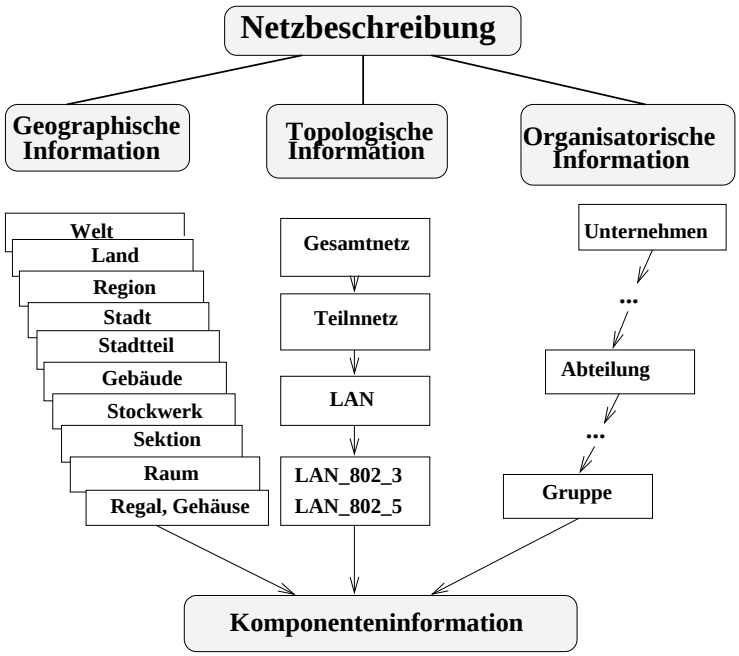

Abbildung 1.1: Inhalt einer Netzbeschreibung

- Automatisches Fortschreiben der Konfiguration.
- Umkonfigurieren von Ressourcen (z.B. im Fehlerfall).
- Konfigurieren aus der Ferne.
- Bereitstellen einer Verwaltung von Netzversionen.
- Initiierung von Aufträgen und Verfolgung von deren Abwicklung.

1.1.2 Fehlermanagement

Dieser Funktionsbereich läßt sich grob charakterisieren durch die beiden Merkmale „besonders wichtig“ und „besonders komplex“. Die Aufgabe des Fehlermanagements besteht darin die Verfügbarkeit des Netzes oder verteilten Systems möglichst hoch zu halten - ein Anliegen, das wohl jeder Netzbetreiber hat. Die aus dieser Zielvorgabe erwachsenden Teilaufgaben sind einfach abzuleiten:

- Überwachen des Netz- bzw. Systemzustandes.
- Entgegennehmen und Verarbeiten von Alarmen.
- Diagnostizieren von Fehlerursachen.

- Feststellen von Fehlerfortpflanzungen.
- Einleiten und Überprüfen von Fehlerbehebungsmaßnahmen
- Einführen eines Trouble-Ticket-Systems.
- Leisten von Hilfestellungen für den Benutzer (User Help Desk).

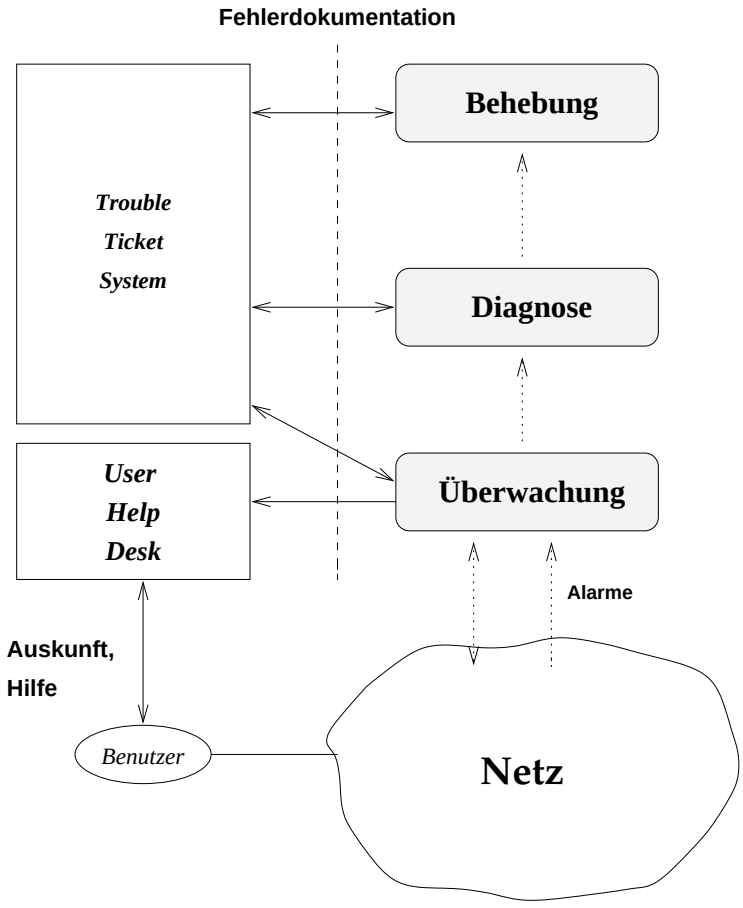

Abbildung 1.2: Teilaufgaben des Fehlermanagements

Die angedeuteten Schwierigkeiten bei der Lösung der Fehlermanagement-Aufgaben liegen im Bereich der Diagnose. Der Einsatz von Techniken der Künstlichen Intelligenz hat sich für diese Problemstellung als schwierig herausgestellt. Das liegt einerseits an der komplexen Materie der Kommunikationstechnik, was die Akquisition von Wissen erschwert; zum anderen haben Forschungsarbeiten gezeigt, dass Kommunikationsnetze aufgrund von ständigen Umkonfigurationen, Erweiterungsmaßnahmen oder dem kurzzeitigen Abschalten von Netzkomponenten einer hohen Änderungsdynamik unterworfen sind, was von den meisten der bestehenden Ansätze nicht adäquat behandelt werden kann.

1.1.3 Leistungsmanagement

Das Leistungsmanagement kann von seiner Zielsetzung her als eine konsequente Weiterführung des Fehlermanagements angesehen werden: während das Fehlermanagement dafür verantwortlich ist, dass das Kommunikationsnetz bzw. verteilte System überhaupt läuft, gibt sich das Leistungsmanagement damit nicht zufrieden und setzt sich zum Ziel, dass das Gesamtsystem „gut“ läuft. In dem Begriff „gut“ liegt bereits ein erstes Problem, das vom Leistungsmanagement gelöst werden muß, nämlich die Definition der **Dienstgüte**. Hierbei kann auf die Festlegungen, die im Zusammenhang mit dem Quality of Service in geschichteten Kommunikationssystemen getroffen wurden, zurückgegriffen werden.

Als Teilaufgaben des Leistungsmanagements sind zu nennen:

- Bestimmen von Dienstgüte-Parametern.
- Überwachen des Kommunikationsnetzes oder Systems im Hinblick auf Leistungs-Engpässe.
- Durchführen von Messungen.
- Aufbereiten von Meßdaten und Verfassen von Berichten.
- Durchführen von Leistungs- und Kapazitätsplanungen.

Die zur Lösung dieser Aufgaben einzusetzenden Grundlagentheorien sind dabei gefestigter als vergleichsweise im Fehlermanagement. Viele der aus dem Bereich der Leistungsbewertung von klassischen Rechensystemen entwickelten Theorien können in leicht abgewandelter Form auch für das Leistungsmanagement von Kommunikationsnetzen oder verteilten Systemen genutzt werden.

1.1.4 Abrechnungsmanagement

Die Bereitstellung von Kommunikations- oder Server-Diensten führt zu Kosten, die auf die Kostenverursacher verteilt werden müssen. Gemäß welcher Strategien und Verfahren diese Aufteilung erfolgt, kann und darf dabei von einem Abrechnungsmanagement nicht fest vorgeschrieben sein, sie ist Gegenstand der Abrechnungspolitik. Eine wichtige Anforderung an das Abrechnungsmanagement ist somit, dieses gemäß den Vorgaben der Abrechnungspolitik konfigurieren zu können.

Teilaufgaben des Abrechnungsmanagements sind:

- Erfassen von Verbrauchsdaten.
- Führen von Abrechnungskonten.
- Zuordnen von Kosten zu Konten.

- Verteilen und Überwachen von Kontingenten.
- Führen von Verbrauchsstatistiken.

Die grundsätzlichen Verfahren zur Abrechnung, die von den eingesetzten Algorithmen her als einfach einzuschätzen sind, können zum Teil aus der Großrechner-Welt übernommen werden. Schwieriger dagegen ist die Beschaffung der hierfür notwendigen Managementinformation; eine Vielzahl der im Leistungsmanagement durch Messung und Beobachtung ermittelten Daten kann hier allerdings den mit der Informationsbeschaffung verbundenen Aufwand erheblich reduzieren.

1.1.5 Sicherheitsmanagement

Für gewisse Branchen wie z.B. Banken hat der Funktionsbereich des Sicherheitsmanagement die höchste Priorität. Die noch nicht bewältigten Probleme auf diesem Bereich sind u.a. dafür verantwortlich, dass nach wie vor an vielen Stellen die Großrechner noch nicht von den dezentralen Workstation-Clusters abgelöst wurden.

Die folgenden Teilaufgaben fallen im Sicherheitsmanagement an:

- Überwachen des Systems bzw. Netzes im Hinblick auf Sicherheitsangriffe.
- Verschlüsseln von Information.
- Durchführen von Authentifizierungen.
- Verfolgen von Sicherheitsmaßnahmen.

Im Bereich des Sicherheitsmanagements kann man von einem weitestgehend stabilen Satz von anerkannten und vielfach bereits als Public Domain Software vorliegenden Sicherheitsverfahren ausgehen. Das zentrale Problem besteht darin, diese Verfahren geeignet in die Managementarchitektur einzubetten und im Sinne einer **Security Policy** zu steuern.

1.2 Theorie der Netzmanagement-Werkzeuge

Management-Werkzeuge sind ein wichtiges Mittel, um den Administrator bei seinen Aufgaben zu unterstützen, bzw. sie erst zu ermöglichen. Dazu betrachten wir in diesem Versuch zwei sehr unterschiedliche Vertreter: Zum einen die SNMP-Tools, zum anderen den Protokollanalysator.

Eine erste Einführung in das im Praktikum verwendete SNMP-Management wird vermittelt, indem der Aufbau von SNMP mit den Begriffen Managed Node und Agent dargelegt wird. Danach wird das Kommunikationsprotokoll SNMP, mit dessen Hilfe zwischen den

einzelnen Knoten kommuniziert wird, noch genauer unter den Aspekten seines Aufbaus betrachtet.

Die SNMP-Tools erlauben es mittels Kommandozeilen-Eingabe Managementinformation, die in sogenannten MIB-Variablen gespeichert ist, zu lesen oder auch zu setzen. Sie stellen somit den SNMP Manager dar, welcher mit dem Agenten der Komponente kommuniziert. Im praktischen Teil dieses Themas, werden wir von diesen SNMP-Tools Gebrauch machen und ihre Einsatzbereiche veranschaulichen.

Der zweite Vertreter der Management-Werkzeuge ist, wie bereits erwähnt, der Protokollanalysator. Ein Protokollanalysator hört praktisch den gesamten Netzverkehr an einer bestimmten Stelle des Netzes ab und kommt so auf die Struktur des vorhandenen Netzes und dessen Komponenten. Die Beobachtung und Analyse von Protokollabläufen auf allen sieben Schichten des Kommunikationsmodells ist eine wichtige Aufgabe, um den Betrieb eines Rechnernetzes gewährleisten zu können. Der hierzu notwendige Protokollanalysator ist somit eines der unverzichtbaren Werkzeuge für den Netzoperateur.

Im theoretischen Teil dieser Aufgabe soll u.a. geklärt werden, in welchen Teilbereichen des Netzmanagements ein Protokollanalysator sinnvoll eingesetzt werden kann. Dazu werden wir den funktionalen Aufbau eines solchen Gerätes näher betrachten und uns die Grenzen dieser Analysemethode verdeutlichen. Desweiteren soll ein weiteres Protokoll, das File Transfer Protocol FTP, eingehend betrachtet werden.

Im praktischen Teil lernen wir das Programm **Ethereal** kennen, welches uns als Ersatz für einen hardwarebasierten Protokollanalysator dient (das Rechnernetzepraktikum verfügt zwar auch über einen „echten“ Protokollanalysator, dieser wird jedoch für die ATM-Versuche benötigt). Wir werden den Software-Protokollanalysator im Rahmen der Netzmanagementversuche dazu benutzen, Messungen zur Netzauslastung, Fehlerrate und Netzstatistik durchzuführen. Ein weiterer Schwerpunkt der praktischen Aufgabe wird die Analyse des Ablaufs einer FTP-Verbindung zwischen zwei Praktikumsrechnern, sowie einer SNMP-Anfrage, wie sie im ersten Teil der Aufgabe erfolgte, sein.

Der verwendete Protokollanalysator zeichnet sich vor allem dadurch aus, dass eine Vielzahl gängiger Protokolle aus verschiedenen Schichten automatisch dekodiert und interpretiert werden kann. Zudem besteht u.a. die Möglichkeit, relevante Teile des Netzverkehrs auszufiltern, um die anfallenden Datenmengen einzuschränken.

1. Management-Werkzeuge

   (a) Zählen Sie Werkzeuge auf, die im Bereich Netzmanagement eingesetzt werden.

   (b) Nennen Sie einige Klassifizierungsmerkmale und ordnen Sie die Werkzeuge entsprechend zu.

2. Management mit Hilfe von SNMP

   Das Management-Modell der IAB basiert auf einer hierarchischen Manager-Agent Beziehung zwischen Manager und Managed-Node.

(a) Erklären Sie die Begriffe „Managed Node“ und „Agent“ und grenzen Sie die Begriffe voneinander ab. Legen Sie die Aufgaben eines Agenten fest. Gehen Sie dabei auch auf den Begriff „Proxy-Agent“ ein. Literatur:[rose91],[garb91],[hege92],[kern95]

(b) Die Kommunikation zwischen Manager und Agent wird in der TCP/IP-Welt über das Protokoll SNMP (Simple Network Management Protocol) abgewickelt. Geben Sie eine kurze zusammenfassende Beschreibung von SNMP. Literatur:[blac92],[hege92],[rose91]

(c) Erläutern Sie, welche Bedeutung der Begriff „community“ in SNMP hat. Erklären Sie dabei auch den Begriff „community name“. Literatur:[blac92],[rose91]

(d) Wie sind die Protocol Data Units (PDUs) von SNMPv1 bzw. SNMPv2 aufgebaut? Literatur:[blac92],[rose91]

(e) Welche Bedeutung und Vorteile hat bei SNMP „trap-directed Polling“? Literatur:[blac92],[hege92],[rose91]

3. Aufbau und Einsatz von Protokollanalysatoren

(a) Definieren Sie grob die Anforderungen an einen Protokollanalysator in einer Netzwerkumgebung.

(b) Entwerfen Sie aus Ihrem Anforderungsprofil heraus die funktionalen Einheiten eines Analysators und stellen Sie den Aufbau graphisch dar.

(c) Erläutern Sie das Zusammenspiel der funktionalen Einheiten. Zeigen Sie Schwachstellen und Engpässe auf.

(d) Inwieweit kann ein Analysegerät aktiv am Netzverkehr teilnehmen? Nennen Sie hierfür zwei Beispiele.

(e) Welche prinzipiellen Unterschiede ergeben sich beim Einsatz rein softwarebasierter Analysatoren?

(f) Welche Aufgaben aus dem Bereich des Netzmanagements kann ein Protokollanalysator übernehmen? Welche nicht? Begründen Sie Ihre Antwort.

4. FTP-Protokoll

(a) Erläutern Sie kurz den Sinn und die Aufgabe des FTP-Protokolls.

(b) Stellen Sie den Protokollstack eines FTP-Kontrollpaketes dar, das über das Institutsnetz übertragen wird (Ethernet 802.3, TCP/IP). Welcher Schicht ist dieses Protokoll zuzurechnen?

(c) Interpretieren Sie für alle Schichten des Stacks die Informationen der Header und erläutern Sie die Bedeutung der einzelnen Datenfelder.

(d) Stellen Sie einen Verbindungsaufbau zwischen zwei Rechnern auf TCP-Ebene dar.

(e) Modellieren Sie eine FTP-Verbindung mit allen beteiligten Prozessen der Clients und Server, und erläutern Sie deren Aufgaben.

(f) Beurteilen Sie das FTP-Konzept im Hinblick auf Effizienz, Kosten und Fehleranfälligkeit.

1.3 Versuch I: Lesen von MIB-Variablen

Um Netzmanagement durchführen zu können, ist es notwendig, Managementinformation von entfernten Komponenten auf der zentralen Managementstation zur Verfügung zu haben. Diese Informationen können über ein eigenes Managementprotokoll von entfernten Systemen ermittelt werden. Dazu wird auf die jeweilige MIB der Komponente über SNMP zugegriffen. In dieser Aufgabe sollen Informationen mit Hilfe der SNMP-Tools abgefragt werden.

1. Versuchen Sie mit Hilfe des SNMP Befehls `snmpget` auf `pcnmXov` die verantwortliche Kontaktperson, den Standort, die unterstützten Schicht-Dienste, das Betriebssystem, dessen Version und die Uptime der Komponente `swnmX` herauszubekommen. Ermitteln Sie nun den für das Auslesen von Variablen korrekten „community name“ und versuchen Sie es erneut.

2. Versuchen Sie nun selbiges mittels des Befehls `snmpwalk`.

Hinweis:
Die `system` Group finden Sie im Teilast `iso.org.dod.internet.mgmt.mib-2`. Mögliche Befehle erhalten Sie auf der `hprnp4` (loggen Sie sich per `ssh` ein) mit: `man snmpget`. Es gibt einen „get community name“ und einen „set community name“ für jeden Rechner, wobei mit dem „get community name“ nur Variablen ausgelesen werden können, während mit dem „set community name“ Variablen sowohl gelesen als auch geschrieben werden können. **Die beiden „community names“ können in der Konfigurationsdatei ermittelt werden (nur mit Admin Account).**

1.4 Versuch II: Verändern von MIB-Variablen

Jede einzelne Komponente eines Netzes ist durch die Werte ihrer MIB-Variablen für den Netzverkehr konfiguriert. Netzmanagement mit Hilfe der SNMP-Tools geschieht durch „Lesen“ und „Setzen“ von Variablen der SNMP-MIB. Um unbefugten Management-Zugriff auf Komponenten zu vermeiden, existiert ein Zugriffsschutz, mit dessen Hilfe Rechner in verschiedene Domänen eingeteilt werden können. Die Zugehörigkeit eines Rechners zu einer Domäne läßt sich über die Konfigurationsdatei `/etc/SnmpAgent.d/snmpd.conf` ermitteln.

In dieser Aufgabe soll nun versucht werden, einige Variablen des Rechners `hprnp4` zu lesen und zu verändern.

1. Ermitteln Sie den „community name“, den Sie brauchen, um eine Variable zu verändern. Belegen Sie über den Befehl `snmpset` den Namen der Kontaktperson mit Ihrem eigenen Namen.

2. Schauen Sie sich nun noch einmal das Konfigurationsfile an und notieren Sie das Ergebnis.

1.5 Versuch III: Netzverkehr und Fehlerquellen

1. Begreifen des Patchfeldes:

   - Vor Ihnen auf dem Tisch ist ein Switch („Hewlett Packard“), ein Hub und ein Patchfeld aufgebaut. Über diesen Switch erfolgt der Uplink der beiden Hosts `pcnmXov` und `pcnm1prot`.
   - Das Patchfeld dient dazu, die empfindlichen Portbuchsen des Switches vor Beschädigung und Abnutzung zu bewahren. Im Idealfall sollten Sie am Switch gar nichts umstecken müssen.
   - Werfen Sie nun einen Blick auf Abbildung 1.3, um das Patchfeld zu verstehen. Buchse Nr. 9 ist mit Buchse Nr. 13 verbunden, Buchse Nr. 10 mit Buchse Nr. 14 und so weiter...
   - Die Stecker der Kabel „pcrnp10nmX“ (gelb), „pcnmXov“ (grau) und „pcnmXprot“ (grau) sollten sich in den Patchbuchsen Nr. 9, 10 und 11 befinden. Sollte dem nicht so sein, dann stecken Sie sie bitte dort hin und belassen sie dort bis zum Ende aller Zeiten.
   - Buchse Nr. 13 des Patchfeldes muss über ein **Cross-Connect-Kabel** mit einem beliebigen Port des Switches verbunden sein (achten Sie auf die kreuzförmige Kabelbeschriftung). Die Buchsen Nr. 14 und 15 des Patchfeldes müssen ebenfalls mit irgendwelchen Ports des Switches verbunden sein, allerdings über normale Kabel (keine Cross-Connects).

2. Starten des Protokollanalyse-Programms:

   Loggen Sie sich mit der Praktikumskennung am `pcnmXprot` ein. Starten Sie das Prokotollanalyse-Programm `ethereal` (mittels `sudo ethereal`). Löschen Sie alle noch bestehenden Display-Filter (siehe Hinweis) und starten Sie eine Messung, die Ihnen einen Überblick über die Rechner des Praktikumsnetzes gibt und aus der Sie die Auslastung des Netzes ersehen können. Es ist hilfreich, einen Filter zum Ignorieren des NFS-Traffics zu setzen. Beachten Sie auch die unten angegebenen Hinweise.

3. Ermittlung des DNS-Servers:

   Ermitteln Sie den oder die Rechner im Netz, die als DNS-Server dienen. Erstellen Sie dazu einen Filter, der Nameserver-Anfragen filtert. Welchen Traffic beobachten Sie, und woraus können Sie die IP-Addresse des Nameservers ersehen? Falls Sie keine Nameserver-Anfragen im Netz beobachten, starten Sie mit `nslookup` selber eine.

4. Fehlerquellen im Netzwerk:

   Starten Sie eine Messung, und das Programm , welches fehlerbehafteten Netzverkehr simuliert (das Programm ist zur Zeit nicht installiert). Beobachten Sie die Auswirkungen im Netzwerk. Was für Fehler und Störungen können Sie beobachten? Beenden Sie nach der Messung das Programm und starten Sie das Aufräum-Skript .

5. Hub und Switch:

   Wir wollen den Uplink der Hosts `pcnmXov` und `pcnmXprot` nunmehr über den Hub führen (und nicht mehr über den Switch).

   - Ziehen Sie aus den Buchsen Nr. 14 und 15 des Patchfeldes die beiden Verbindungskabel heraus. Am Switch ändern Sie nichts.
   - Verbinden Sie nun mit **zwei anderen Kabeln** die Buchsen Nr. 14 und 15 des Patchfeldes mit zwei beliebigen Ports des Hubs.
   - Der Hub muss über das rote Cross-Connect-Kabel mit Port 24 des Switches verbunden sein.
   - Beobachten Sie nun mit dem Protokollanalysator die Änderungen im Netzverkehr. Welche Unterschiede im Traffic können Sie feststellen, wenn Sie den Uplink über den Switch mit dem Uplink über den Hub vergleichen? Ist aus Management-Sicht ein geswitchtes Netz von Vorteil? Was für Nachteile sind damit verbunden?
   - Sie können die beiden Hosts für den nächsten Versuch am Hub belassen.

Hinweis:

- Das Programmfenster des Protokollanalyse-Programms `ethereal` ist in drei Unterfenster aufgeteilt. Im oberen sehen Sie eine Zusammenfassung des mitgehörten Netzverkehrs. Im mittleren können Sie sich einzelne Pakete anzeigen und den Protokollstack dekodieren lassen. Im unteren sehen Sie eine hex-Darstellung der gesnifften

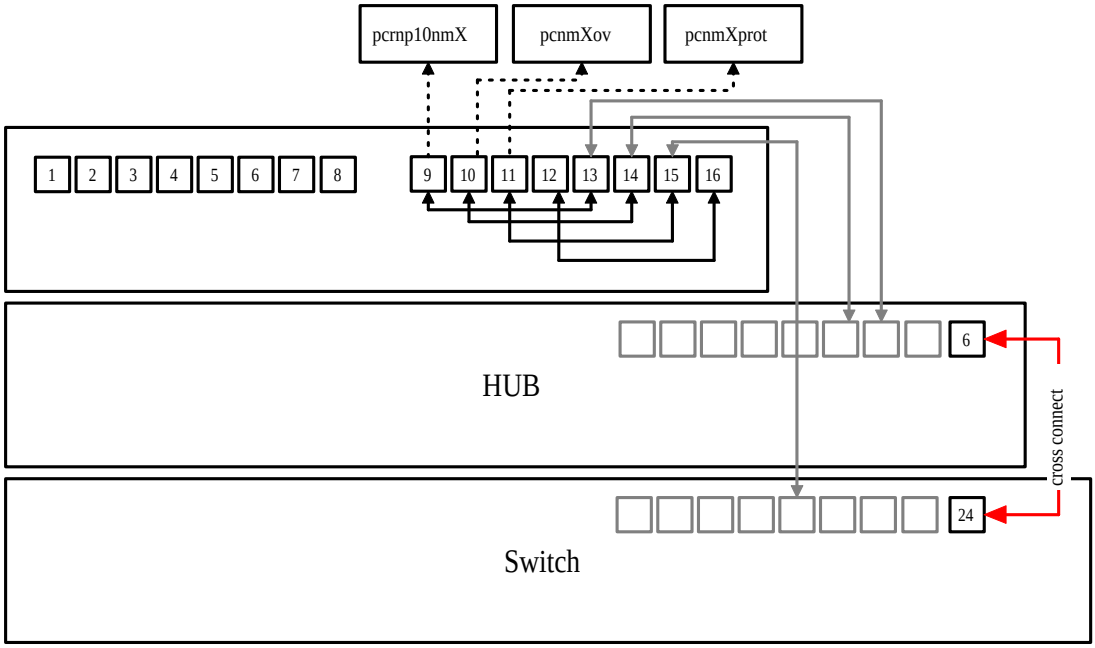

Abbildung 1.3: Patchfeld, Hub und Switch

Pakete. Wenn Sie im mittleren Fenster ein Feld im Protokollheader selektieren, so werden im unteren Fenster die zugehörigen Bytes markiert.

- Sie können jetzt im Menü „Capture“ mit Start eine Messung beginnen. Im daraufhin erscheinenden Auswahlfenster haben Sie die Möglichkeit, einen Filter auszuwählen. Als Interface sollte `eth0` eingestellt sein. Mit OK beginnen Sie die Messung, mit Stop beenden Sie diese wieder. Im Verlauf der Messung sehen Sie auch Statistiken über die Art der geloggten Pakete. Sie können die komplette Messung oder einzelne Pakete davon mittels des Menuepunktes Print im Menue File in eine Textdatei exportieren und für Ihre Ausarbeitungen verwenden.

- In Ethereal werden zwei Arten von Filtern bereitgestellt: Display-Filter und Capture-Filter. Capture-Filter ermöglichen es, vor Beginn einer Messung genau anzugeben, welche Art von Paketen mitgeloggt bez. ignoriert werden soll. Display-Filter ermöglichen nachträglich präzise Filterung der bereits dekodierten Pakete. Im RNP werden Capture-Filter eingesetzt.

- Für die Erstellung von Capture-Filtern wird die normale tcpdump-Filter-Syntax benutzt. Einige Filter sind schon voreingestellt. Eigene Filter können Sie folgendermassen erstellen: Im Menue Edit den Punkt „Capture Filters“ selektieren, im Feld „Filter name“ und „Filter string“ jeweils den Namen und den Filter eingeben, auf New klicken um den neuen Filter anzulegen und Save, um das Filterfile zu sichern.

Achtung: Filter, die Sie selber erstellen, werden nach dem Neustart von `ethereal` überschrieben. Die Syntax der Capture-Filter ist (vereinfacht) die folgende:

```
[not] primitive [ and|or [not] primitive ...]
```

Ein `primitive` ist dabei ein Identifier (zum Beispiel eine Ip-Addresse oder eine Port-Nummer) mit einem Qualifier davor, der angibt, worum es sich beim nachfolgenden Identifier handelt. Als Qualifier sind möglich: host, net und port für eine Host-Addresse, eine Netz-Addresse oder eine Portnummer; src bzw. dst, falls es sich um die Quell- bzw. Zieladdresse handelt und ether, ip, arp, icmp, tcp und upd zum Filtern nach Protokoll. Die genaue Syntax der Capture-Filter können Sie z.B. der Manpage zu `tcpdump(1)` entnehmen.

- Filterbeispiele:
  - tcp port 23
    ⇒ TCP-Verkehr auf Port 23, Telnet
  - not host 192.215.168.10 and tcp port 23
    ⇒TCP-Verkehr auf Port 23, aber nichts vom Rechner 192.215.168.10
  - src host 192.215.168.10 and dst host 192.215.168.11
    ⇒Verkehr zwischen diesen zwei Rechnern, nur eine Richtung.

  Die Portnummern finden Sie in der Datei `/etc/services`.

1.6 Versuch IV: Analyse des FTP/TCP/IP Protokollstapels

1. Aktivieren des Filters, Verbindungsaufbau:

   Stellen Sie sicher, dass beide Rechner des NM-Versuchs (`pcnm1ov` und `pcnmXprot`) an den Hub angeschlossen sind. Erstellen Sie einen Filter, um eine FTP-Verbindung zwischen den Rechnern `pcnm1ov` und `hprnp4` zu analysieren. Starten Sie eine Messung und einen ftp-Zugriff. Beobachten Sie den Verbindungsaufbau. Warum können Sie den Datenkanal nicht sehen?

2. Protokollanalyse:

   Analysieren Sie die einzelnen Protokollebenen der Pakete, die bei der FTP-Verbindung verschickt wurden. Wählen Sie hierfür die geeigneten Messungen aus.

3. Stellen Sie nun am Patchfeld die alte Verkabelung wieder her (Uplink des beiden Hosts `pcnm1ov` und `pcnm1prot` über den Switch).

Hinweis:

- Sie können sowohl nach Portnummern als auch nach Host filtern. Die Portnummern für ftp entnehmen Sie /etc/services.
- Sie können im Protokoll-Stack-Fenster Details zu den einzelnen Protokoll-Ebenen anzeigen lassen, indem Sie auf das + klicken.
- Der Aufbau eines Ethernet Frames, sowie der Aufbau von IP- und von TCP-Paketen ist in den Abbildungen 1.4, 1.5 und 1.6 dargestellt.
- Eine FTP-Kommandosequenz hat folgende Struktur:

  ```
  [Command (4 Chars)] [Option(s)]
  ```

  Bsp: USER **SPACE** [username] **CR LF**

  Für alle verfügbaren Befehle und Optionen siehe RFC 959.

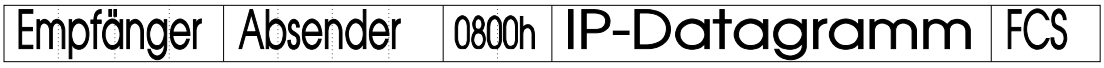

Abbildung 1.4: Ethernet Frame

1.7 Versuch V: Analyse des SNMP-Protokolls

Dieser Versuch verläuft analog zum vorherigen, allerdings mit dem Unterschied, dass jetzt SNMP analysiert wird.

1. Führen Sie einen `snmpget` von der `pcnmXov` auf die `swnmX` aus (sprich `snmpget swnmX rnp` ...) und zeichnen sie den dabei entstehenden Verkehr mit dem Protokollanalysator auf. Analysieren Sie den Protokollstack der Anfrage sowie der Antwort im Analysator.
2. Ermitteln Sie den Community-String.
3. Welchen Hauptunterschied auf Schicht 4 können Sie im Vergleich zur Analyse von FTP feststellen?

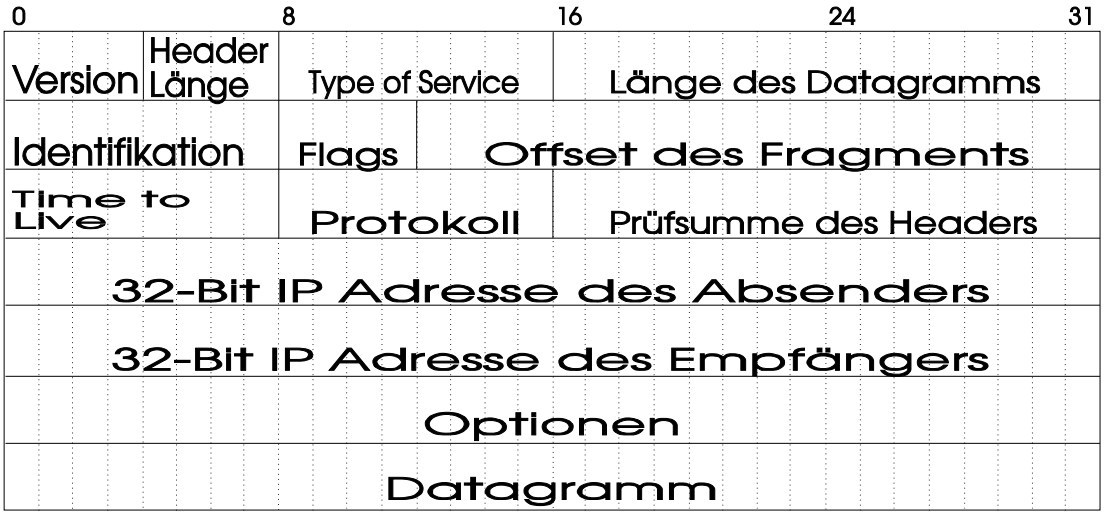

Abbildung 1.5: IP-Paket

1.8 Sicherheit im Netzmanagement

In diesem Versuch soll veranschaulicht werden, wie ungeschützt und greifbar sensible Daten sind, wenn sie unverschlüsselt über ein Netzwerk gehen.

1. telnet
   Starten Sie mit Capture->Start die Messung. Wählen Sie als Filter telnet. Loggen Sie sich per `telnet` auf `swnmX` ein (Passwort: nmn). Können Sie das Passwort aus dem mitgeschnittenen Netzwerkverkehr ermitteln?

2. http
   Starten Sie den zeichenorientierten Browser `lynx`. Starten Sie eine Messung und rufen Sie die Seite `http://pcrnp10/rnp/login.cgi` auf. Geben Sie einen beliebigen Usernamen und eine Kennung an und loggen Sie sich ein. Können Sie das Passwort aus dem mitgeschnittenen Netzwerkverkehr ermitteln?

3. ssh
   Starten Sie eine Messung. Loggen Sie sich mittels `ssh` auf einen beliebigen Praktikumsrechner ein. Können Sie das Passwort aus dem mitgeschnittenen Netzwerkverkehr ermitteln?

Vergleichen Sie die drei untersuchten Anwendungen in Hinblick auf die gebotene Sicherheit. Viele Netzwerkkomponenten lassen sich per `telnet` oder `http` konfigurieren, einige wenige bieten auch einen `ssh`-Zugang an. Wie schätzen Sie dieses Sicherheitskonzept ein? Kann immer davon ausgegangen werden, dass kritische Netzkomponenten sich hinter einer Firewall

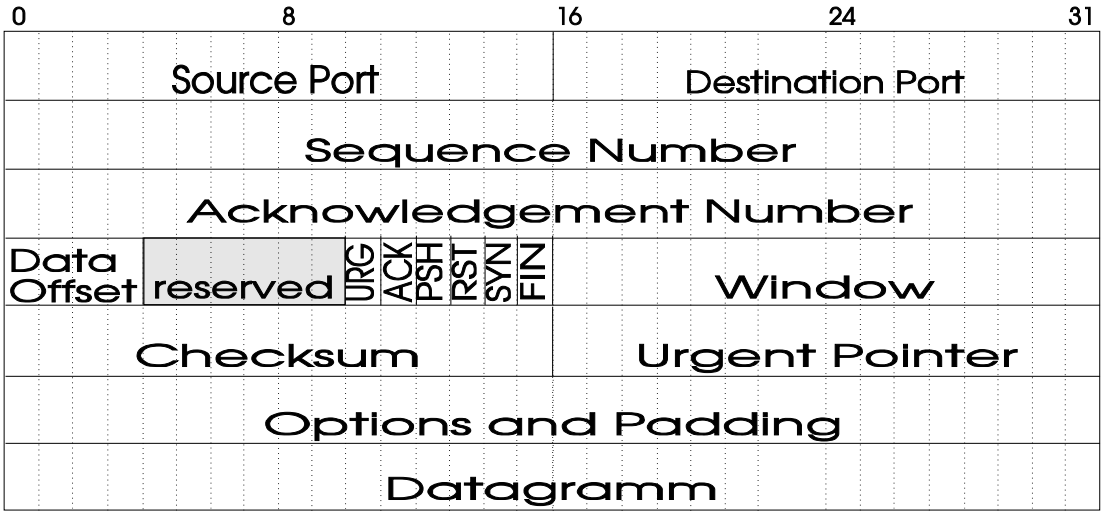

Abbildung 1.6: TCP-Paket

befinden oder sonstwie dem Zugriff böswilliger Individuen entzogen sind? Berücksichtigen Sie hierbei insbesondere die Bequemlichkeit von web-basierten Administrationsinterfaces.

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 OpenView Windows. Grenzen Sie die Aufgabenbereiche beider Produkte voneinander ab. Ordnen Sie beide Produkte in die vorige Skizze ein. Literatur: HP Handbücher (OpenView 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 Protokollanalysators?

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 herstellerspezifischen 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 Rechnernetzepraktikums 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 gestatet 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 Kostelezky, 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.

Kapitel 3

NM 3 - Komponentenmanagement

Damit ein Kommunikationsnetz ordnungsgemäß funktioniert, sind regelmäßig steuernde und kontrollierende Maßnahmen an den zentralen Ressourcen, den Netzkomponenten, vorzunehmen. Die Gesamtheit dieser Maßnahmen fassen wir unter dem Begriff **Komponentenmanagement** zusammen. Am Beispiel eines LAN Switches werden wir uns in Laufe dieses Versuches mit einfachen Formen des Komponentenmanagements vertraut machen.

3.1 Einführung

In der vorliegenden Praktikumsaufgabe soll ein Switch sowohl theoretisch als auch in praktischen Versuchen näher untersucht werden, wobei vor allem das Management des Switches über eine Managementplattform besonders berücksichtigt werden soll. Bei der theoretischen Betrachtung des Switches sind es in erster Linie zwei Aspekte, die für das Verständnis der Zusammenhänge und Konzepte von zentraler Bedeutung sind:

- Der eine Aspekt betrifft die Funktionalität des Switches und soll in den Theorie-Aufgaben 1 und 2 herausgearbeitet werden.
- Der andere Aspekt betrifft die Abstraktion von der tatsächlichen Hardware/Software-Ressource. Im zurückliegenden Praktikumsversuch haben Sie sich bereits etwas mit dem Informationsmodell des Internet-Managements auseinander gesetzt. In der Theorie-Aufgabe 3 haben Sie nun die Gelegenheit, Ihre Kenntnisse am Beispiel der MIB-Erweiterung für den Switch zu vertiefen.

Die gewonnenen theoretischen Kenntnisse sollen die Grundlage für die praktischen Versuche bilden. Zunächst soll die tatsächlich vorhandene Topologie des Praktikums-Switches ermittelt und mittels der graphischen Benutzeroberfläche von HP OpenView dargestellt werden. Die Überwachung des Switches kann nun entweder lokal mittels des VT 420-Terminals oder remote durch HP OpenView erfolgen. Verschiedene Management-Aufgaben sollen

einen Einblick in die Möglichkeiten beider Verfahren gewähren. Aufbau und Inhalte der Internet-MIB werden ebenso behandelt wie die Konfiguration der Agenten, durch die die MIB-Information der Komponenten dem Managementsystem bereitgestellt wird.

3.2 Theorie

3.2.1 Aufgabe 1: Ethernet-Switch

1. Grenzen Sie folgende Netzkomponenten voneinander ab und berücksichtigen Sie auch, welche Kommunikationsschichten diese jeweils berühren:

   - Bridge
   - Router
   - Brouter
   - Repeater
   - Multiport-Repeater, Hub, Sternenkoppler
   - Gateway

   Wie läßt sich ein Ethernet-Switch in dieses Schema einordnen?

   (Literatur: [tane96], [nemz88], [kern95])

2. Was sind die wichtigsten Kabeltypen, die im Bereich der Rechnervernetzung verwendet werden? Geben Sie die wichtigsten Merkmale, sowie deren Vor- und Nachteile an.

   (Literatur: [tane96], [nemz88], [kern95])

3. Welche grundlegenden logischen und physischen Topologien gibt es und wie unterscheiden sie sich? Welche dieser Topologien werden bei den jeweiligen Kabeltypen (siehe Teilaufgabe 2) bevorzugt verwendet und warum? Für welche Topologien wird der Switch eingesetzt?
   (Literatur: [tane96], [nemz88])

3.2.2 Aufgabe 2: Switch-Funktionalität

Geben Sie eine kurze Funktionsbeschreibung eines Ethernet-Switches an, und diskutieren Sie dabei auch die Verbesserungen einer sternförmigen Realisierung des Ethernet-Konzeptes gegenüber der klassischen busförmigen Realisierung.

(Literatur: [hege92])

3.2.3 Aufgabe 3: MIB-Erweiterung für den Switch

Es soll nun je ein Template für folgende Variablen der MIB-II des Switches erstellt werden:

- ifEntry
- SwitchPortEntry
- ifIndex

Folgende Zusatzinformationen sind vorhanden:

1. Der Status von ifEntry und SwitchPortEntry ist je „mandatory“.
2. SwitchPortEntry hat eine etwas abweichende Struktur:

   SwitchPortEntry ::= SEQUENCE {...}
3. Die ifEntry besitzt zusätzlich die Notation „INDEX {...}“; dort wird die Variable angegeben, die eindeutig den Port identifiziert, für den in der Tabelle die korrespondierenden Werte angegeben werden.

Hinweis:

- siehe Theorie-Aufgabe 4 des letzten Praktikumstages (NM 2)
- entsprechende Variablen in OpenView abfragen
- Literatur: [rose91], [blac92], [hege93]

3.3 Versuch 1: Erstellen einer Netzbeschreibung

1. Entwurf einer Skizze:

   Schließen Sie die beiden Rechner `pcnmXov` und `pcnmXprot` über den Switch an. Fertigen Sie dazu eine Skizze über die Topologie inklusive Patchfeld an. Beschriften Sie in Ihrer Skizze auch die Ports der Switches.

2. Erstellung einer Submap unter HP OpenView:

   Öffnen Sie zunächst die Submap „Raumübersicht“ und erzeugen Sie darin ein Location/Room Objekt mit dem Label „Raum D9 Gruppe X“. Im „Add Object“ Dialogfenster wählen Sie als Behavior „explode“ (beachten Sie dabei den kurzen Infotext, der Ihnen unmittelbar unter den Behavior-Buttons angezeigt wird). In der „OpenView Windows QUESTION“ klicken Sie „Modify“ und als Layout Manager wählen Sie „Point to Point“. Fügen Sie jetzt die Informationen aus Ihrer Skizze aus Teilaufgabe 1 in die leere Submap des Raumes D9 ein.

Hinweis:

- Mittels „Locate“ - „Object“ - „By Selection name“ können Sie Netzressourcen aus anderen Submaps selektieren.
- Mittels „Edit“ - „Copy Odject“ (und anschließendem „Paste“) können Sie Symbole von einer Submap in eine andere kopieren.
- Die Kopierfunktion kann man auch auf mehrere Symbole gleichzeitig anwenden (Selektion mehrerer Symbole z.B. mit Strg + Mausklick).
- Fügen Sie eventuell fehlende Verbindungen manuell hinzu.
- Erzwingen Sie schließlich ein „Redo Layout“.

3.4 Versuch 2: Konfiguration des Switches

Im Allgemeinen ermöglicht erst die vorherige Konfiguration von Komponenten einen angemessenen Betrieb. Dabei können die in ein Rechnernetz integrierten Komponenten auf zwei verschiedene Arten konfiguriert werden (remote und direkt, z.B. über eine Konsole). Im Rahmen dieser Aufgabe soll der Praktikums-Switch direkt über die RS232 Schnittstelle konfiguriert werden.

1. „Anschluss“ des Terminals:

   - Starten sie als Terminalemulation das Programm „minicom“ auf `pcnmXprot`. HINWEIS:
     - Ctrl+Alt+Z: Help
     - Ctrl+Alt+Q: Quit

  - Das Passwort für den Operator-Mode ist „rnp“
- Sie befinden sich jetzt im Hauptmenü des Management Modules. Machen Sie sich mit den Untermenüs vertraut und finden Sie dabei heraus, welches Protokoll zwischen Switch und Terminal verwendet wird.

2. IP-Adresse und Ethernet-Adresse:

   Zum Aufbau von Verbindungen und zur genauen Identifikation von Komponenten in Rechnernetzen werden Adressen benutzt. Die zentrale Adresse in der TCP/IP-Welt ist die IP-Adresse. Daneben existiert die Ethernet-Adresse (auch MAC-Adresse, physikalische Adresse oder Station Adresse genannt), die hardwareabhängig und weltweit für jedes Gerät eindeutig ist.

   (a) Ermitteln Sie mit Hilfe des Terminals die Ethernet-Adresse des Switches. Verifizieren Sie Ihr Ergebnis mit Hilfe der am Switch angebrachten Beschriftung am Management-Einschub.

   (b) Ermitteln Sie die IP-Adresse des Switches mit Hilfe des Terminals.

   HINWEIS: Hierzu reichen Ihre momentanen Rechte als „Operator“ nicht mehr aus. Loggen Sie sich daher wieder aus, und anschließend mit neuem Passwort (das Sie beim Betreuer erfragen) wieder ein.

   (c) Ermitteln Sie die Ethernet- und IP-Adresse des Switches mittels HP OpenView:
   - Anklicken des Icons mit rechter Maustaste
   - Auswahl von Menu-Punkt „Describe/Modify Object...“
   - Anklicken von IPMap in Dialogbox „Object Attributes“
   - Anklicken „View/Modify Object Attributes...“

3. Management-Funktionen:

   Da der Switch, im Gegensatz zum Hub, eine direkte Vermittlung zwischen Ports betreibt (Mikrosegmentierung), gestaltet sich die Überwachung einzelner Ports schwierig. Hierfür bietet das Management-Modul die Möglichkeit den Verkehr eines Ports an einem zweiten Port zu beobachten. Aktivieren Sie diese Funktion und geben Sie ein Beispiel einer Anwendung an.

3.5 Versuch 3: Switch Management

3.5.1 PING

Mit Hilfe des Ping-Kommandos kann die Erreichbarkeit zwischen zwei Systemen ermittlelt werden, wobei zusätzlich der Round-Trip-Delay gemessen wird:

- Führen Sie von der `hprnp4` aus den Ping-Befehl zum `swnmX` aus. Anzahl Pakete: ca. 100
- Starten Sie Open View und selektieren Sie den Switch `swnmX`. Wählen Sie das Menü „Performance“ aus und lassen Sie sich den „Interface Traffic“ grafisch anzeigen. Um eine sichtbare Veränderung herbeizuführen, besteht im Menü „Fault“ ebenfalls die Möglichkeit eines Pings.
- Um einen besseren Einblick in den ankommenden bzw. herausgehenden Datenverkehr der einzelnen Ports der Switches zu bekommen, lassen Sie sich diesen ebenfalls graphisch anzeigen.

Hinweis:

- Wählen Sie dazu im Menü „Options“ das Untermenü „Data Collection and Thresholds:SNMP“ aus.
- Definieren Sie jeweils ein MIB-Objekt für den gesamten eingehenden und eines für den gesamten hinausgehenden Datenverkehr.
- Konfigurieren Sie diese Objekte.
- Wählen Sie für „Collection Mode“: „Store, No Thresholds“
- Speichern Sie Ihre Konfigurationen ab, bevor Sie sich die Graphik ansehen.

3.5.2 Counter

Bei der Übertragung von Daten im Netz müssen Werkzeuge bereitstehen, die es erlauben, Ereignisse rasch zu lokalisieren. Ein solches Hilfsmittel stellt der Switch z.B. über das VT420-Terminal zur Verfügung: Im Menü des Management-Modules lassen sich Counter-Werte für die Anzahl der verschickten Pakete auslesen. Senden Sie mittels `ftp` eine Datei von der `pcnmXov` zur `pcnmXprot`. Lesen Sie am Terminal die Counter-Werte aus.

Hinweis:
Um einen besseren Überblick zu bekommen, setzen Sie die Zähler durch „Reset“ auf Null zurück.

3.5.3 Counter und MIB-Variablen

Die Zähler, welche Sie in Teilaufgabe 2 mittels VT420-Terminal ausgelesen haben, entsprechen bestimmten MIB-Variablen in der MIB-Erweiterung für den Switch. Somit können dieser Werte auch mit der Management-Plattform ausgelesen werden.

- Lesen Sie die entsprechenden MIB-Variablen an der Management-Station aus. Vergleichen Sie das Ergebnis mit dem aus Teilaufgabe 2.
- Verfolgen Sie den zeitlichen Werteverlauf verschiedener MIB-Variablen mittels der „Graph"-Funktion.
- Was passiert, wenn eine Query auf einen Knoten im MIB-Baum ausgeführt wird, der kein „Blatt" des Baumes ist? Erklären Sie Ihre Antwort.

Hinweis:

- Zähler an der Terminal-Console und entsprechende MIB-Werte.
- Vorgehensweise in OpenView:
  - Anklicken des Icons `swnmX`.
  - Pull-down Menü „Options", Menü-Punkt „Load/Unload MIBs: SNMP", „hp-icf" laden (falls noch nicht geladen).
  - Pull down Menu „Misc", Menu-Punkt „SNMP MIB Browser".
  - Community name: „rnp"

3.5.4 Deaktivieren eines Ports

An einer Management-Plattform sollte es auch möglich sein, Werte der MIB-Variablen zu verändern, ohne extra ein Terminal an den Switch anzuschließen. Führen Sie folgende Schritte zweimal durch:

- einmal mit Hilfe des VT420-Terminals
- das zweite Mal mit Hilfe der entsprechenden MIB-Variablen an der Management-Station

1. Eröffnen Sie eine Remote-Session auf der `pcnmXprot` von der `pcnmXov` aus mittels `ssh`.

2. Ermitteln Sie mit Hilfe der Skizze aus Aufgabe 1 denjenigen Port, an welchem die `pcnmXov` angeschlossen ist.

3. Deaktivieren Sie diesen Port und versuchen Sie Teilschritt (1) erneut. Was lässt sich demnach damit steuern?

4. Aktivieren Sie die deaktivierten Ports erneut. Überprüfen Sie den Status! Machen Sie zur Kontrolle einen erneuten login von der `pcnmXov` zur `pcnmXprot`.

Hinweis:

- Aktivieren/Deaktivieren der Ports am VT420-Terminal mittels Menüsteuerung.
- Aktivieren/Deaktivieren der Ports an der Management Station mittels der MIB-Variable „ifAdminStatus“.

3.5.5 HP OpenView Farbsemantik

Eine Netzmanagement-Plattform bietet u.a. die Möglichkeit, den Ausfall von Netzkomponenten festzustellen. Der Betriebsstatus der Komponenten wird i.a. durch unterschiedliche Farben dargestellt. Wiederholen Sie noch einmal die Bedeutung der unterschiedlichen Farben (Help-Menu).

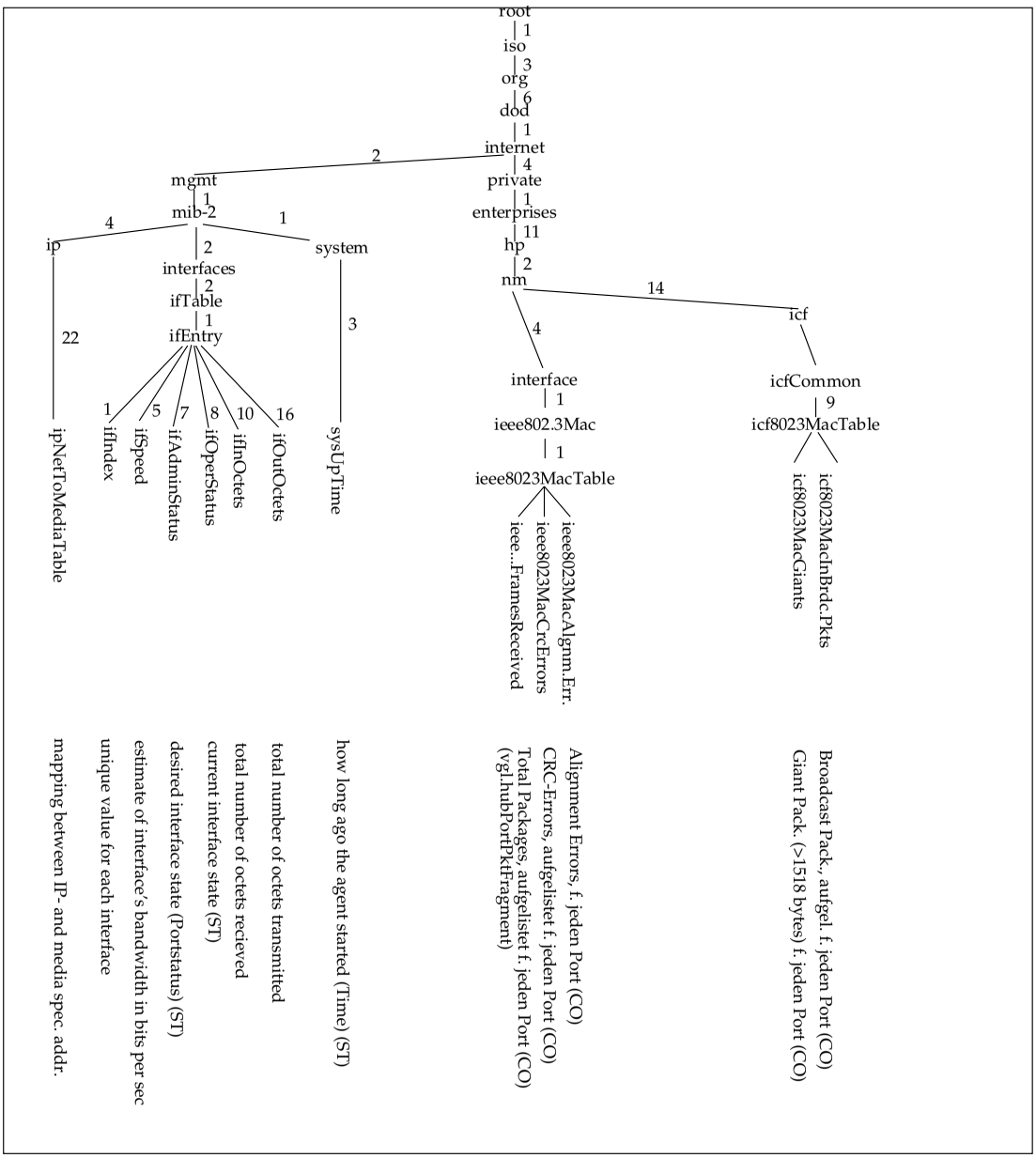

Abbildung 3.1: MIB für den HP Ethernet Switch