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:

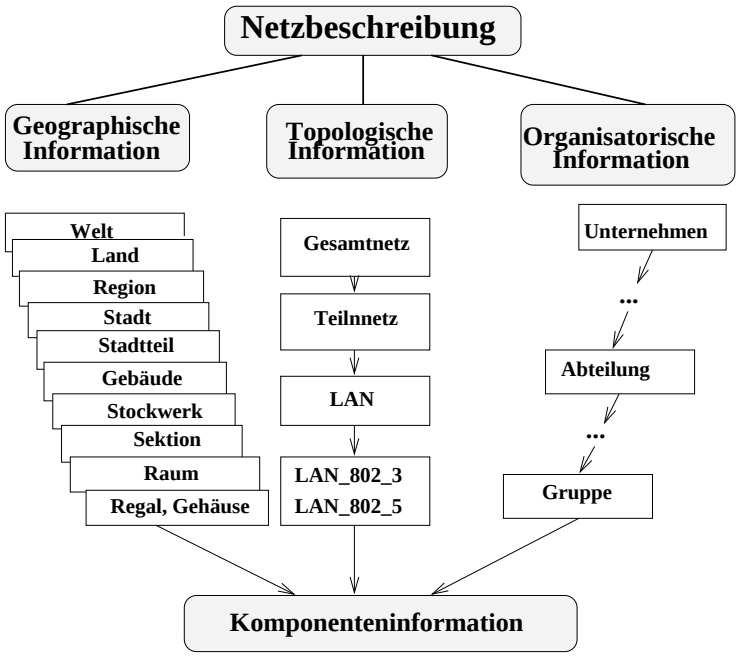

Abbildung 1.1: Inhalt einer Netzbeschreibung

- 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).

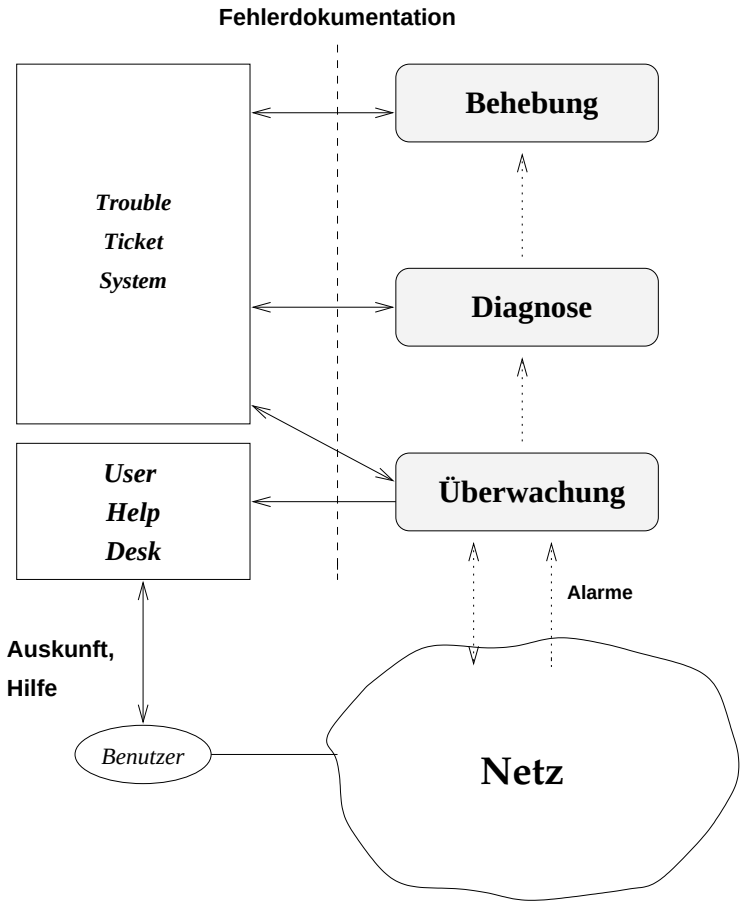

Abbildung 1.2: Teilaufgaben des Fehlermanagements

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

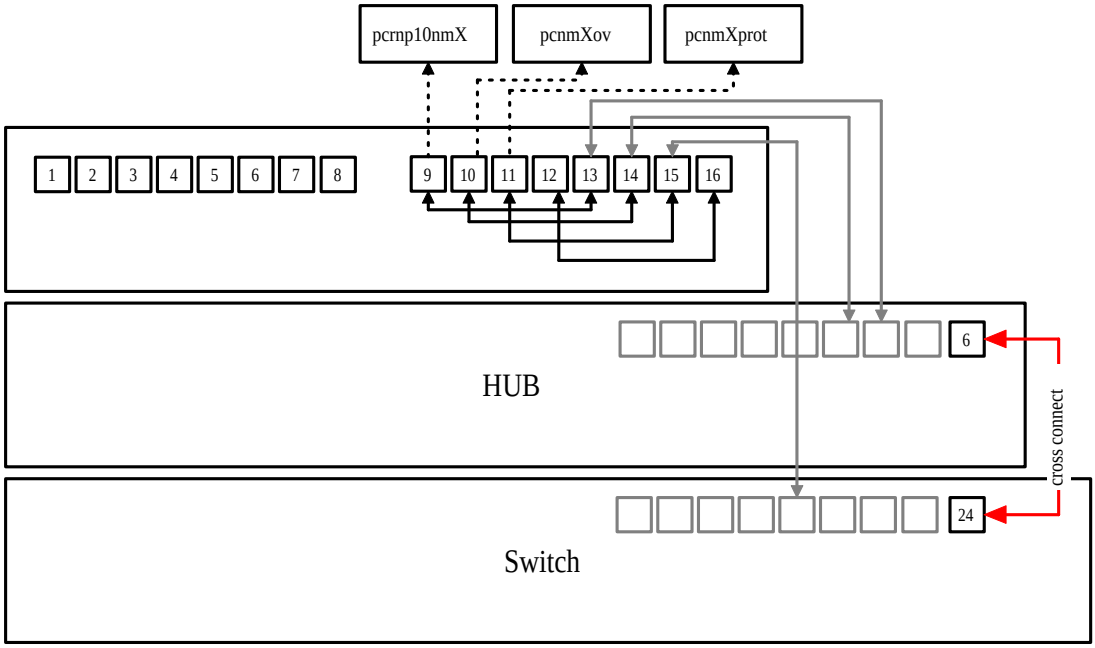

Abbildung 1.3: Patchfeld, Hub und Switch

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.

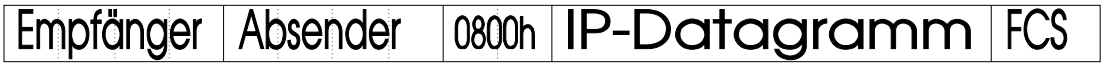

Abbildung 1.4: Ethernet Frame

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?

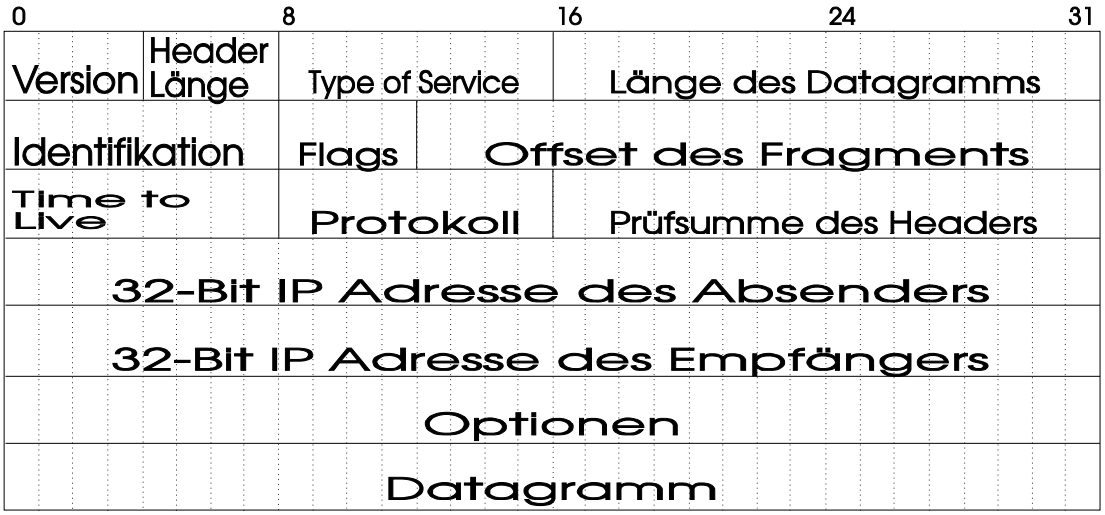

Abbildung 1.5: IP-Paket

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

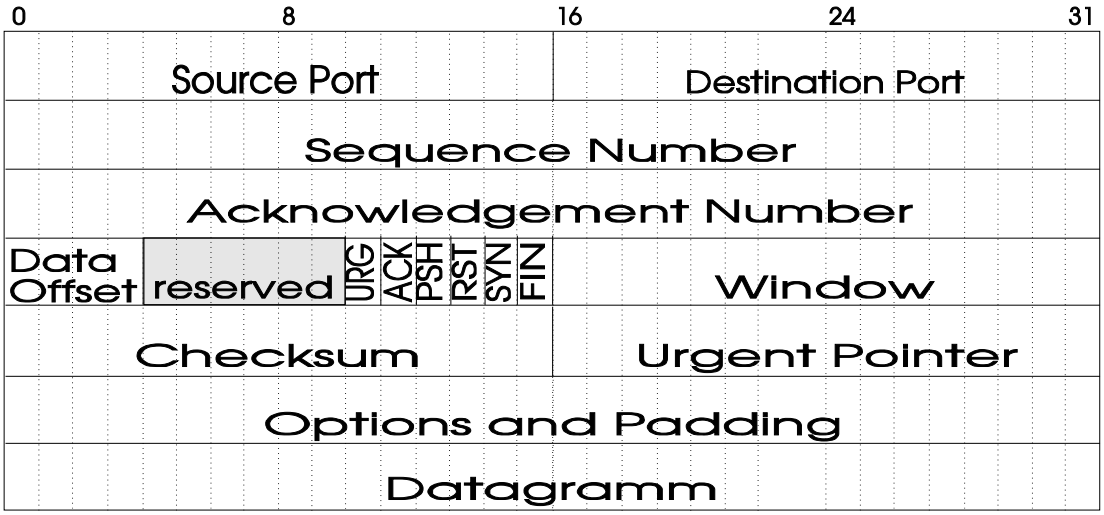

Abbildung 1.6: TCP-Paket

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