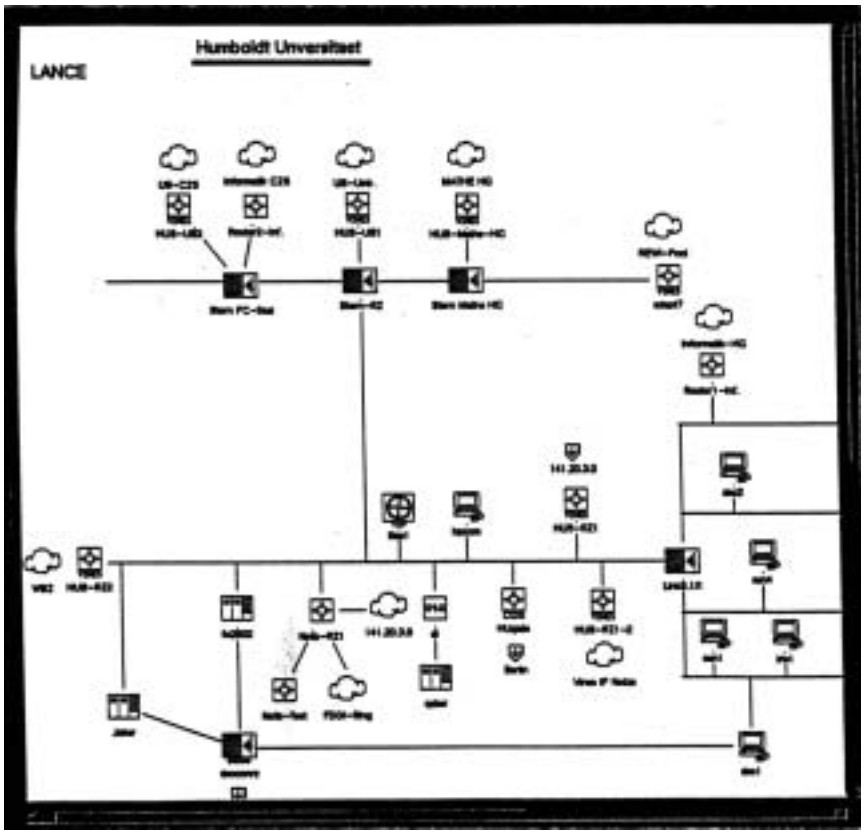
Netzwerk Management auf SNMP-Basis

In den letzten zwei Jahren hat sich die Nutzung von Netzwerkdiensten in der Humboldt-Universität sprunghaft entwickelt. Das ist vor allem eine Folge der raschen Verbreitung von Arbeitsplatzrechnern in fast allen Bereichen der Universität. Diese Rechner sind in den meisten Fällen in Netzwerke eingebunden. Das sind z.B. lokale PC-Netze wie Banyan VINES, die auch weltweit verbunden werden können, X.25 basierte Dienste wie z.B. X.400-Mail oder das weltweite Internet von UNIX-Rechnern.
Für den Anwender von Netzdiensten bleibt meist die dahinterliegende Infrastruktur verborgen. Das sind z.B. unterschiedliche Übertragungsmedien wie Telefonleitungen, Koaxkabel, Glasfaserkabel, Laser-Links u.a.

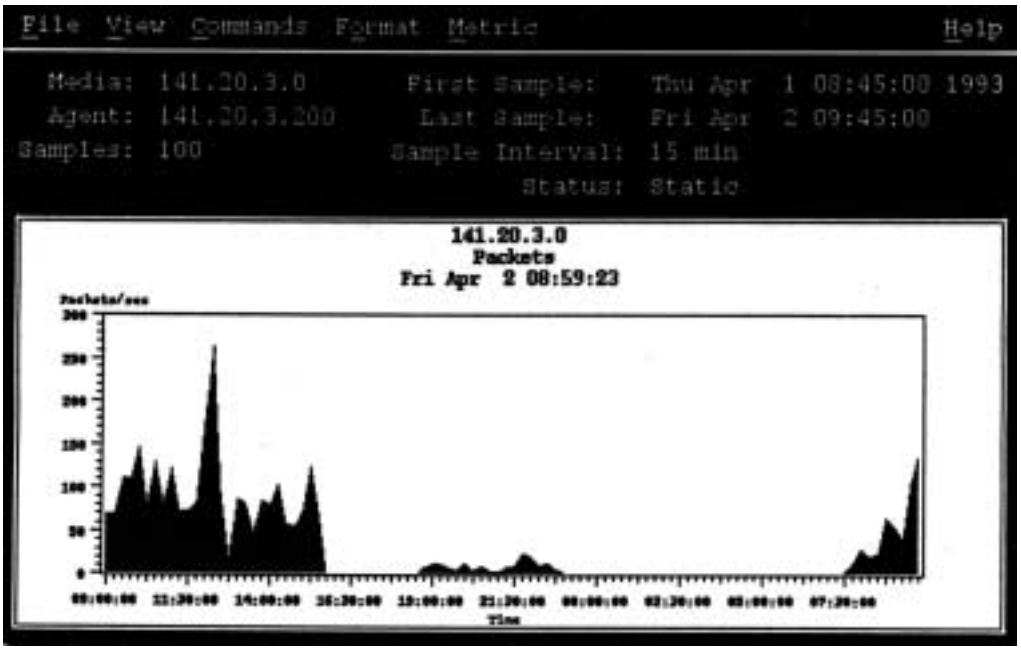
IP-Adressen sind ziemlich willkürlich in der Welt verteilt. Ein UNIX-Rechner kennt meist nur die Ethernetadressen der IP-Partner, die an das gleiche Ethernetsegment angeschlossen sind. Für alle anderen Partner wendet er sich an den in seinem Segment angeschlossenen Router. Das kann auch ein UNIX-Rechner mit mehreren Netzanschlüssen sein. Dieser sucht dann einen geeigneten Übertragungsweg und sendet die Daten weiter. Die Router tauschen zu diesem Zweck untereinander über spezielle Routing-Protokolle Informationen aus und müssen auch entsprechend programmiert werden. In der Humboldt-Universität gibt es z.Z. nur für IP etwa 60 Subnetze mit ca. 20 Routern. Dazu kommen ungefähr 30 VINES-Server, die untereinander verbunden sind. An



Die Medien können gleichzeitig oder abwechselnd mit unterschiedlichen Protokollen betrieben werden. So ist z.B. IP-Verkehr u.a. über Ethernet, X.25 oder FDDI möglich.
Für die Verbindung der verschiedenen Medien und Teilnetze ist ein Vielzahl unterschiedlicher Geräte wie Modems, Repeater, Bridges und Router notwendig. Diese Geräte können hier unmöglich alle beschrieben werden. Es soll nur kurz auf die Funktion von Routern eingegangen werden.

einer IP-Verbindung in die USA sind ca. 20 Router beteiligt.
Die Überwachung und Steuerung dieser vielen, dem Benutzer verborgenen Geräte obliegt einigen wenigen Netzwerkverantwortlichen. Es liegt auf der Hand, daß diese auf die Nutzung moderner Rechentechnik angewiesen sind.
Neben einigen Lösungen großer Firmen, die vor allem Managementsysteme für eigene Produkte anbieten, gibt es einen Ansatz, der aus der UNIX-Welt

stammt und eine Lösung für heterogene Netze bietet. Basierend auf dem Internet-Protokoll wurden **SNMP** (Simple Network Management Protokoll) und **MIB** (Management Information Base), eine Sprache zum Austausch von Betriebsdaten der Netzkomponenten, definiert.
Nach diesem Standard können nun wichtige Netzkomponenten, wie Router, Server o.ä. mit SNMP-Agenten ausgerüstet werden. Das sind zusätzliche Softwarekomponenten bzw. Spezialprozessoren, die Daten aus ihrer unmittelbaren Netzumgebung sammeln. Diese Agenten senden über IP-Verbindungen Daten oder Alarmmeldungen an eine oder mehrere Netzwerkmanagementstationen (**NMS**). Das sind Workstations, die mit spezieller Software ausgerüstet sind. Diese Software enthält eine Datenbasis für die Netzstruktur, eingehende Daten und Alarmmeldungen und deren Aufbereitung bzw. Bearbeitung. Dazu kommen Werkzeuge zur Visualisierung von Netzwerkdaten und Betriebszuständen.
Außer den reinen Überwachungs- und Analysefunktionen bietet SNMP auch begrenzte Möglichkeiten zur Steuerung von Gerätefunktionen.
Im Rechenzentrum ist seit Anfang des Jahres das Managementsystem **LANCE+** der Firma LEXEL im Einsatz.
Zu dem System gehören eine Datenbasis (Ingres) und ein Monitor, der die Betriebszustände der Netzkomponenten grafisch, z.B. durch unterschiedliche Färbung, anzeigt (siehe Abb.1).
Im Hintergrund laufen ständig Prozesse, die die Erreichbarkeit der überwachten Geräte kontrollieren und an den Monitor melden. Spezielle Werkzeuge gestatten es, Analysen (siehe Abb.2) und Berichte über Datenraten, Fehlerhäufigkeiten u.ä. anzufertigen. Besondere Agenten (sogenannte Probes) sammeln in wichtigen Netzsegmenten Betriebsdaten und können diese auch speichern. So ist auch bei unterbrochener Verbindung eine Fehleranalyse vor Ort oder nachträglich möglich.
Das Netzwerkmanagementsystem ermöglicht es uns, Störungen zu erkennen und diese zu lokalisieren, bevor sich die Betroffenen im Rechenzentrum melden. Außerdem können Engpässe analysiert werden. Bei dem zu erwartenden stürmischen Ausbau des Universitäts-Rechnernetzes, z.B. im Rahmen des SERVUZ-Projektes, ist der anfallende Arbeitsaufwand ohne solche Hilfsmittel nicht zu bewältigen.
Wie auch in anderen Bereichen der Netzwerkentwicklung ist auch hier die UNIX-Welt anderen Bemühungen einer Standardisierung einer heterogenen Umgebung weit voraus. Netzwerkmanagementsysteme auf Basis des OSI-Standards werden sich praktisch erst in einigen Jahren verbreiten.



Klemens Müller