Internet Security – Auf dem Wege zur ganzheitlichen Sicherheit im CampusNetz

Dipl.-Ing. Thomas Wegner

Universität Rostock
Fachbereich Elektrotechnik und Informationstechnik
Institut für Angewandte Mikroelektronik und Datentechnik
Richard Wagner Str. 31
18119 Rostock
Tel.: (0381) 498 3533, Fax: (0381) 498 1126, Email: weg@e-technik.uni-rostock.de

Abstract. Mit wachsender Verbreitung des Internets sehen sich Einzelbenutzer und Institutionen zunehmend Angriffen auf ihre Systemintegrität und Datensicherheit ausgesetzt. Daher werden die Sicherheitsansprüche der angeschlossenen Einrichtungen ständig steigen. Dieser Beitrag beschreibt den Einsatz und die Performanceanalyse eines IP-Paketfilters als ein Baustein auf dem Wege zur Schaffung einer ganzheitlichen Sicherheitsarchitektur in einem bestehenden Intranet. Im wesentlichen können zwei Verfahren für die notwendige Abschottung der DV-Systeme im lokalen Netzwerk sorgen, Virtual Privat Networks (VPN) und Firewalls. Das Ziel einer Performanceanalyse soll die Ermittlung der über ein LINUX-Firewall-System erreichbaren Datenübertragungsrate sein. Die untersuchten Netzwerkstrukturen und die dabei ermittelten Messwerte werden unter praktischen Gesichtspunkten hinsichtlich erforderlicher zukünftiger Netzerweiterungen diskutiert.

1. Die Sicherheit des lokalen Institutsnetzes im universitären Umfeld

Da sich Einzelbenutzer und Institutionen zunehmend Angriffen auf ihre Systemintegrität und Datensicherheit aus dem Internet ausgesetzt sehen, steigen ständig die Sicherheitsansprüche der vernetzten, über das gesamte Stadtgebiet verteilten Einrichtungen der Universität Rostock.
Im wesentlichen können zwei Verfahren für die notwendige Abschottung der DV-Systeme im Campus-Netzwerk sorgen, Virtual Privat Networks (VPN) und Firewalls. Die damit möglichen Schutzmaßnahmen lassen sich wie folgt klassifizieren:

- Access Security: Schutz der lokalen Systeme vor unerlaubtem Zugriff von inner- und außerhalb des LANs,
- Content Security: Schutz der lokalen Anwendungen und Daten vor Veränderungen und schädlichen Inhalten,
- Authentication Security: Sichere Identifikation der Kommunikationspartner,
- Crypto Security: Schutz der Daten hinsichtlich Vertraulichkeit und Integrität durch Verschlüsselung

Hauptanforderung an die Sicherheit im universitären Umfeld des im Bild 1 dargestellten Institutsnetzes ist der Schutz der System- und Datenintegrität. Mögliche Angriffspunkte auf dieses lokale Netzwerk sind:

- interne Angriffe aus dem LAN durch authentifizierte Nutzer und Computer,
- interne Angriffe aus dem LAN durch Fremdsysteme,
- interne Angriffe aus dem WLAN durch Eigen- und Fremdsysteme,
- externe Angriffe aus dem WIN/Internet durch bekannte und nichtbekannte Nutzer und Computer,
- interne und externe Angriffe auf das LANE-System des ATM-Backbone.

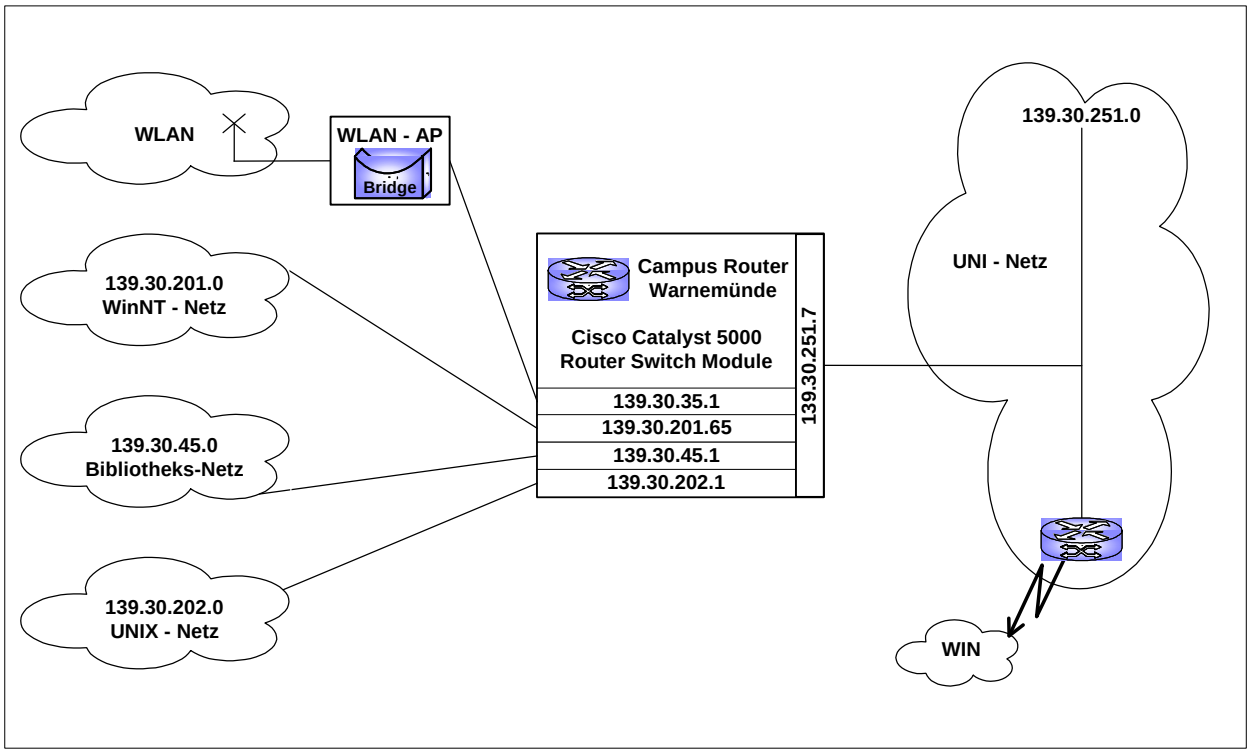

Bild 1: Die VLAN-Struktur des Campus-Netzes

Die steigende Anzahl und Komplexität der Computersysteme erhöhen laufend den Aufwand zur Absicherung des aktuellen Security-Patch-Levels der eingesetzten Betriebssysteme (SUN/SOLARIS, MS/WinNT, SuSE/LINUX).
Ein weiterer Ausweg ist hier neben dem Einsatz von Desktop-Firewall-Systemen, die Anzahl der möglichen Angriffspunkte im Netz durch den Einsatz von ThinClients (SUN RAY) zu verringern.
Mit Layer-3-Firewalls (IP-Paketfilter) und Application-Firewalls (Viren-Scanner, URL-Blocking, Java & ActiveX-Screening) erreicht man Access- und Content-Security.
Die Authentication- und Crypto-Security für Daten ermöglicht die Kryptographie (PGP) und die digitale Signatur. VPNs ermöglichen Authentication- und Crypto-Security natürlich nur zwischen Netzen mit ähnlichem Sicherheitsniveau. Man unterscheidet VPNs mit Layer-2-Tunneling (PPTP, L2F, L2TP) und mit Layer-3-Tunneling (IPSec).
Desktop-Firewalls können mit Hilfe von Protokollfiltern, Einbruchserkennung, Policy-Management, Paket- und Anwendungsmonitoring/Reporting den persönliche Datenschutz am Arbeitsplatzrechner erhöhen. Filterfunktionen für das IP-Protokoll zur Realisierung eines Personal-Firewalls sind mittlerweile integraler Bestandteil der Betriebssysteme MS/Win2k und SuSE/LINUX 7.x.

2. Der Einsatz eines LINUXbasierten Firewall-Routers

In der ersten Ausbaustufe wurde das UNIX-Netz mit den SUN-SOLARIS-Workstation für den VLSI-Entwurf durch einen LINUXbasierten IP-Paketfilter geschützt. Das virtuelle Subnetz im ATM-LANE-System bleibt erhalten, aber es wird nicht mehr direkt über das RSM-Modul des Cisco Catalyst 5000 geroutet, sondern über den als Firewall-Router konfigurierten LINUX-PC. Das hat weiterhin den Vorteil, daß damit auch ein IP-Paketmonitor zur Verfügung steht, um Konfigurationsfehler im LAN schneller zu erkennen.
Folgende Ausstattungsmerkmale kennzeichnen den Firewall-PC:

- Dual Pentium III Board, 550 MHz, 512 KByte Cache, SuSE/LINUX 6.4,
- 512 MByte Hauptspeicher,
- PCI-Netzwerkadapter Intel PRO/100 MBit/s,
- 20 GByte IDE Festplatte.

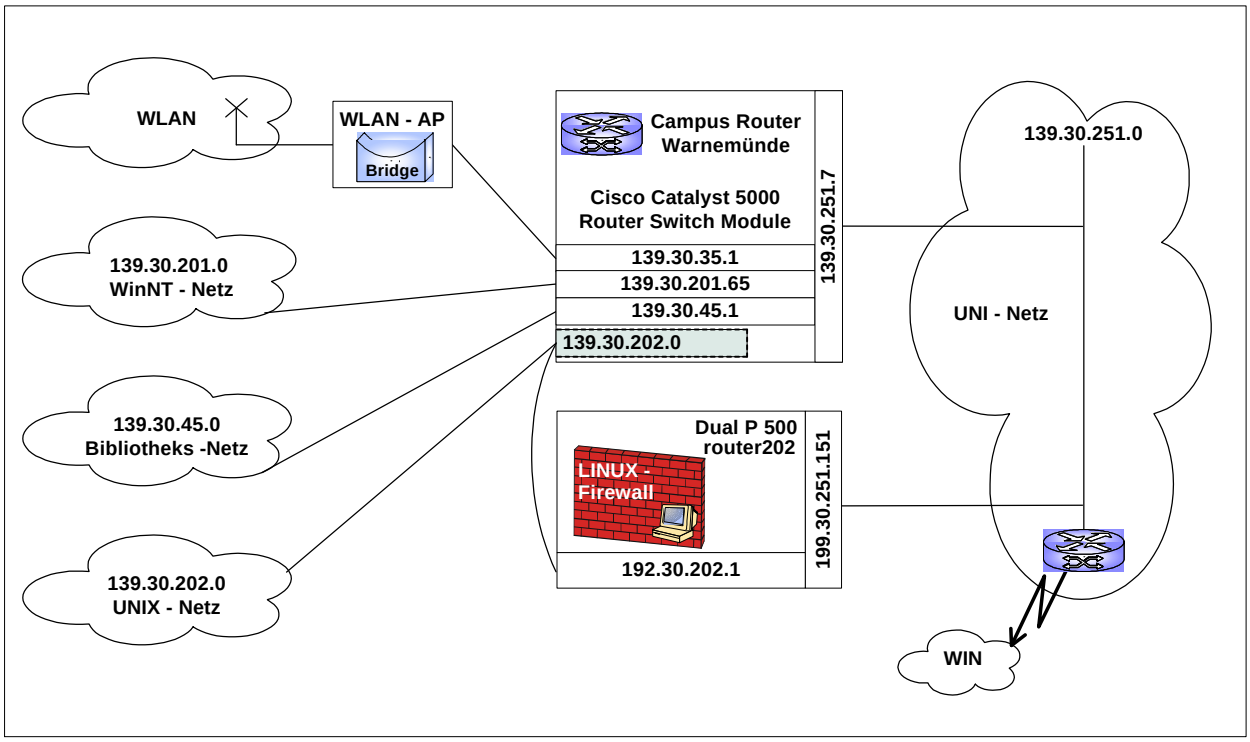

Bild 2: Der Einsatz eines LINUXbasierten Firewall-Routers

Als nichttrivial erwies sich die Aufstellung und Beschreibung der notwendigen Filterregeln für das Tool ipchain des LINUX-Kernels 2.3., da für eine Vielzahl von Diensten (NFS, NIS+, DNS, FTP, NTP, SSH, POP3, usw.) und Protokollen (IP/TCP/UDP, HTTP, NETBIOSoverTCP/IP) die Filtermasken zu setzen waren.

3. Performanceanalyse des Netzwerkes mit Firewall

Für die Analyse eines Datennetzwerkes sind die verschiedensten Monitoring- und Benchmarking-Tools in Hard- und Software realisiert. Die Software Netperf von HP [NET95] ist ein Benchmark, mit dem verschiedene Aspekte der Netzwerkperformance über das TCP/IP-Protokoll gemessen werden können. Entsprechend dem Client/Server-Modell wird beim Aufruf des Programms Netperf auf der Gegenstelle der Netserver-Prozeß durch den Inetd-Dämon gestartet.

#netperf -l test_time -H remotehost -m message_size -s local_send/receive_buffer -S remote_send/receive_buffer

Receive_buffer in Byte	Send_buffer in Byte	Message in Byte	Test_time in s
57344	57344	4096	60
57344	57344	8192	60
57344	57344	32768	60
32768	32768	4096	60
32768	32768	8192	60
32768	32768	32768	60
8192	8192	4096	60
8192	8192	8192	60
8192	8192	32768	60

Tabelle 1: Kommandozeilenparameter des netperf-script

Das in der freien Netperf-Distribution vorhandene tcp_stream_script variiert beim Test die Größen der Socket-Buffer auf Sender- und Empfängerseite mit verschiedenen Nachrichtenlängen, wie in der Tabellen 1 aufgeführt. Hauptanwendungsgebiet ist die Messung der Stream-Performance über TCP oder UDP zwischen zwei Systemen.

Die Datenpfade der durch Netperf erzeugten Last sind in der im Bild 3 dargestellten Meßanordnung zu erkennen.

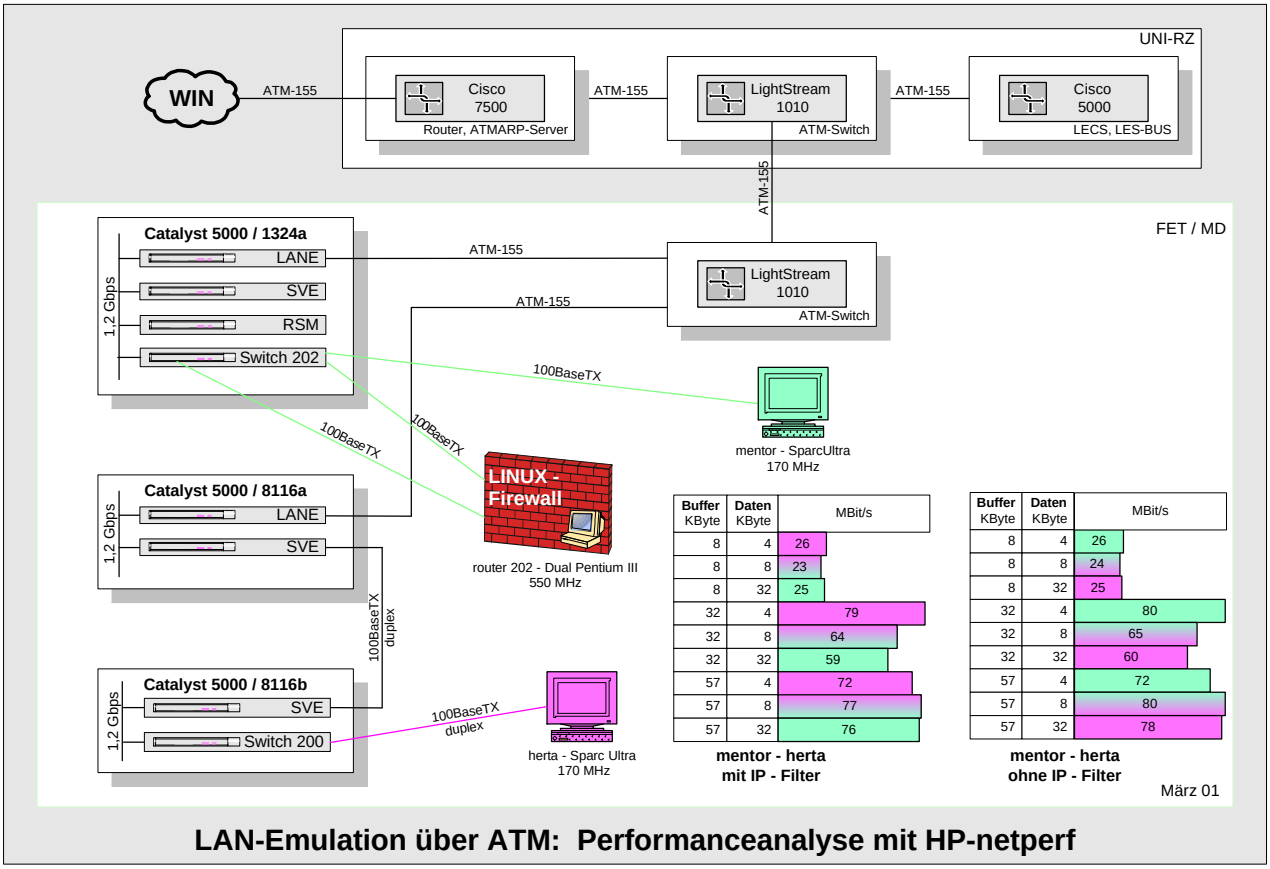

Bild 3: Die Struktur des mit HP-netperf untersuchten 100BaseT-ELANs

Es zeigt sich, daß bei Routerbetrieb die erreichbare Netzwerkgeschwindigkeit durch das LINUX-PC-System nicht beeinträchtigt wird. Sind die TCP/IP-Filterfunktionen über das Tool ipchain im LINUX-Kernel aktiviert, verschlechtert sich die Performance um ziemlich genau 1 MBit/s.

Anbieter	Produkt	Durchsatz in MBit/s
McAfee	Personal Firewall 2.06	9.0
Network Ice	Black Ice Defender	9.0
Conseal	PC Firewall 2.06	8,7
Sybergen Networks	Secure Desktop	8,6
Zone Labs	Zonealarm	7,8
Symantec	Norton Personal Firewall 200	6,5

Tabelle 2: Performancetest von PC-Personal-Firewalls [NWW00]

Die in Tabelle 2 aufgeführten Vergleichstests von PC-Firewalls der Zeitschrift NetworkWorld [NWW00] liefern ähnliche Ergebnisse. Interessant sind die doch recht deutlichen Performanceunterschiede der einzelnen Produkte unter MS/WinNT4.0 zu sehen. Als Referenzwert für die Netzwerkgeschwindigkeit ohne Desktop-Firewall zwischen Computer und Gateway des Routers wurde hier mit der Testsoftware WS_Ping-Propack 2.2 der Firma Ipswitch ein Wert von 9,7 MBit/s ermittelt.
Ziel muß sein, die TCP/IP-Filterfunktionen dem Cisco-RSM-Modul zu übertragen, aber für das Aufstellen und Testen der Filterregeln ist der standalone Firewall-Router hilfreich, damit bei Konfigurationsfehlern nicht immer gleich die gesamte LANemulation betroffen ist.

4. Performanceanalyse des Netzwerkes mit LINUX- und Win2k-Router

Weiterhin sollte im Rahmen dieser Performanceanalyse ermittelt werden, welchen Einfluß die Leistungsklasse der verwendeten Intel-PC-Plattform auf die erreichbare Datenübertragungsrate hat, um notwendige Ausstattungsrichtlinien für die PC-Router abschätzen zu können. Als Testumgebung standen zwei PC-Systeme mit den Betriebssystemen LINUX und MS/Win2kServer im LAN zur Verfügung. Die untersuchten Netzwerkstrukturen und ermittelten Meßwerte sind im Bild 4 dargestellt.

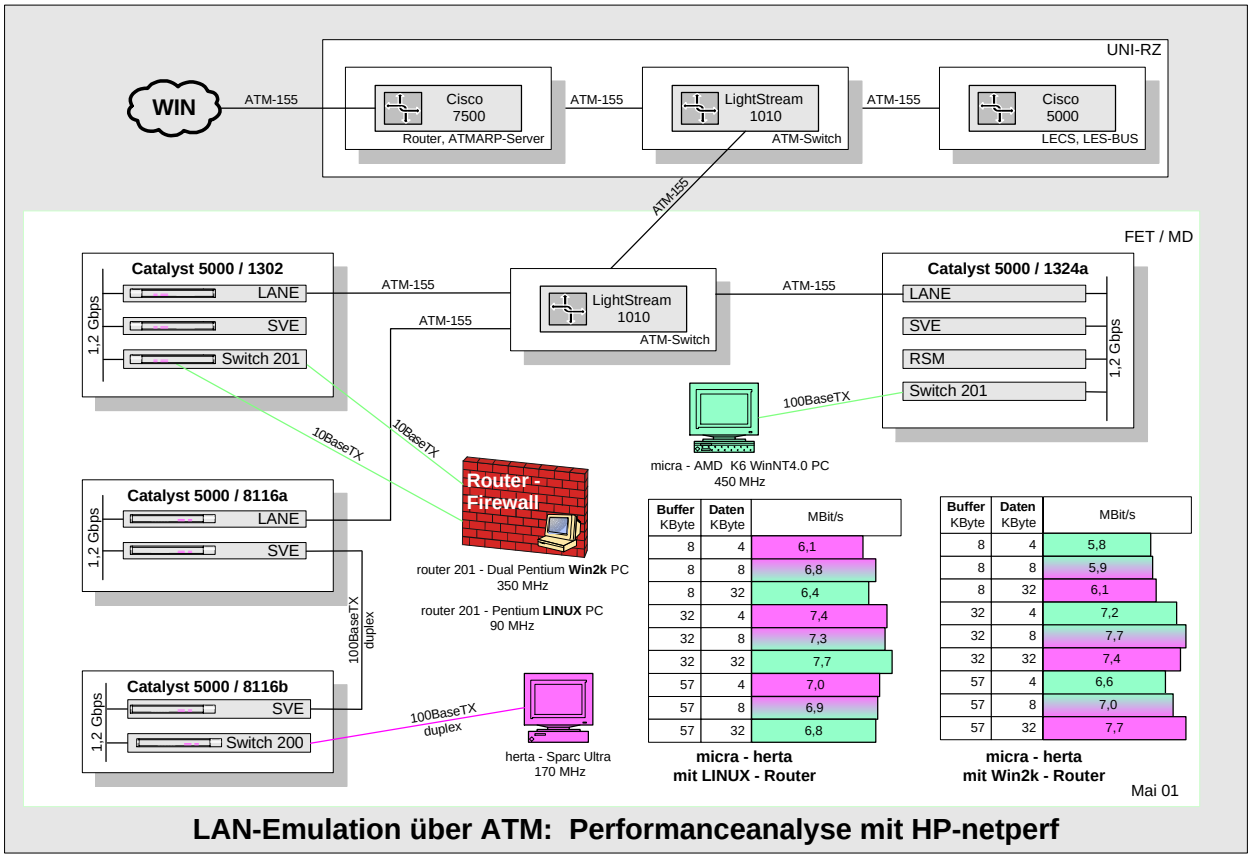

Bild 4: Die Struktur des mit HP-netperf untersuchten 10BaseT-ELANs

Die IP-Routing-Messwerte im Bereich 10BaseT vom LINUX- und Windowssystem unterscheiden sich nur unwesentlich. Es konnte nur bei laufendem Netzwerkbetrieb gemessen werden, bei weniger Netzwerkauslastung sind noch bessere Ergebnisse zu erwarten. Interessanterweise hat der Prozessortakt keinen wesentlichen Einfluß auf die Datengeschwindigkeit zwischen den Routerports. Der Durchsatz von Speicher- und PCI-Chipsatz reicht offensichtlich auch schon auf dem MotherBoard des P90-Systems aus, um ähnlich gute Ergebnisse wie mit dem Win2k-System zu erreichen.

Folgende Ausstattungsmerkmale kennzeichnen die PC-Router:

LINUX-System

- iPentium, 90 MHz, 256 KByte Cache, SuSE/LINUX 7.1,
- 48 MByte Hauptspeicher,
- PCI-Netzwerkadapter SMC EtherPower 10/100 MBit/s,
- 1 GByte SCSI Festplatte.

Win2kServer-System

- Dual iPentium III Board, 350 MHz, 512 KByte Cache, MS/Win2kServer,
- 512 MByte Hauptspeicher,
- PCI-Netzwerkadapter SMC EtherPower 10/100 MBit/s,
- 4 GByte SCSI Festplatte.

5. Zusammenfassung

Die Netzwerksicherheit in einem LAN kann durch den Einsatz eines Internet-Protokollfilters schon wesentlich verbessert werden. Um die Systemlast des LANE-Router-Switch-Moduls im IPoverATM-Netz nicht noch weiter zu erhöhen, wurde die Installation eines Standalone-Router-Firewalls auf PC/LINUX-Basis erwogen. Praktische Messungen der 100BaseT-Netzwerkperformance zeigen, dass sich die erreichbare Übertragungsgeschwindigkeit durch den IP-Filteraufwand beim Software-Routing nur um ca. 1Mbit/s verringert. Dieser praktikable Wert spricht für die Implementierung des IP-Protokollstacks im LINUX-System. Beim Betrieb der Firewall auf IP-Protokollebene können ältere Pentiumsysteme schon zu preiswerten Sicherheitslösungen führen. Bei der Bildung der virtuellen LANs ist hinsichtlich des maximalen Durchsatzes ebenfalls darauf zu achten, dass ein Server mit seinen Klienten möglichst auch über einen Ethernet-Switch verbunden ist, um die Routerbelastung des ATM-Systems zu minimieren.

Literatur

[NET95] http://www.netperf.org/netperf/NetperfPage.html

[SIEM97] Andreas Bonnard, Christian Wolff: Gesicherte Verbindung von Computernetzwerken mit Hilfe einer Firewall, Studie der SIEMENS AB Zentralabteilung Technik, München, 1997

[NWW00] Steve Janss: Sichere Desktops, Computerwoche Verlag GmbH NetworkWorld Germany 19/00, S. 88-90, München, September 2000

[THW98] Thomas Wegner: Performanceanalyse an einer bestehenden IP over ATM 10BaseT-Netzwerk-struktur, Tagungsband Symposium Maritime Elektronik, S. 79-82, Rostock, April 1998

[THW99] Thomas Wegner: Performanceanalyse an einer bestehenden IP over ATM 100BaseT-Netzwerk-struktur, Tagungsband 2. IuK-Tage MV, Rostock, Juni 1999

[WWW] http://www-md.e-technik.uni-rostock.de/ma/weg/weg.html