BBBaden IT-School

Netzwerk betreiben und erweitern

Modul 145

Version 1.1 Haller

Angaben zum Dokument

Dateiname:	Modul_145
Vorlage:	LaTeX 2_ε
Verantwortliche(r):	Jürg Haller <juerg.haller@bbbaden.ch>
Builddatum:	22. August 2006
Copyright:	© BerufsBildungBaden, 2006

Änderungsnachweis

Datum	Version	Autor	Bemerkungen
Juli 2004	0.1	JH	init Dokument
Oktober 2004	1.0	JH	erster Release abgeschlossen
August 2006	1.1	JH	Anpassung MBK R3

Zusammenfassung

Inhaltsverzeichnis

Teil I

Netzwerkmanagement

Kapitel 1

Übersicht

Dieses Kapitel basiert vor allem auf den folgenden Quellen [5], [4]

Ein Netzwerk mit nur wenigen PCs und einem Server zu verwalten ist eigentlich kein Problem. Anders sieht die Sache aus, wenn das Netzwerk aus sehr vielen unterschiedlichen Workstations (Unix, Linux, Macintosh, Win 98/2000/XP) und einer Vielzahl von Servern, Gateways, Bridges, Routern und Hub-Systemen besteht.
Erschwerend kommt oft noch hinzu, dass das Netzwerk nicht nur aus einer Topologie besteht, sondern aus Ethernet, Token-Ring, FDDI oder ATM aufgebaut ist. Unterschiedliche Topologien, Server, Host-Systeme etc. bedeuten auch, dass im Netzwerk nicht nur ein Protokoll zum Einsatz kommt, sondern eine Vielzahl unterschiedlicher Protokolle genutzt werden muss, um eine Kommunikation untereinander zu ermöglichen. Wenn es sich um heterogene Netzwerke der oben beschriebenen Form handelt, ist es oft schwierig, auftretende Fehler überhaupt zu lokalisieren, bevor man sich an ihre Behebung machen kann.

Um Netzwerkadministratoren das Leben zu erleichtern, wird eine Vielzahl unterschiedlicher Netzwerkmanagement-Systeme angeboten. Der Fortschritt auf dem Gebiet der Netzwerktechnik und Netzwerkmanagement-Technik hat uns in den letzten Jahren eine fast unüberschaubare Vielfalt an Techniken und Komponenten (Hard- und Software) beschert. Die richtige Auswahl zu treffen ist nicht leicht, da die "eierlegende Wollmilchsau" bis heute noch nicht erfunden worden ist. Es wird also kein System zu finden sein, mit dem alle Anforderungen erfüllt werden können. Daher wird man immer gezwungen sein, mehr als eine Lösung zu implementieren.
Die zwei wichtigsten Fragen, die sich bei der Auswahl von Netzwerkmanagement-Systemen stellen, lauten:

- Welche Anforderungen werden an das gesuchte System gestellt ?
- Was soll damit erreicht werden?

Es macht einen Unterschied, ob man klassische Systeme zur Überwachung der installierten aktiven und passiven Komponenten sucht (Hub-Systeme und Verkabelung) oder ob mit dem System auch Endgeräte wie Server, Workstations, Router oder Bridges überwacht werden sollen. Von diesen Anforderungen hängt es ab, welche Systeme in Frage kommen werden.

Sie müssen sich dabei zwischen herstellereigenen und herstellerunabhängigen Systemen entscheiden. Ein genauer Vergleich ist durchaus sinnvoll, da in der Regel die herstellereigenen Systeme in der Lage sind, alle Funktionen vollständig zu unterstützen. Bei herstellerunabhängigen Systemen kann es durchaus vorkommen, dass nicht alle Funktionen vollständig zur Verfügung stehen. Wenn das Netzwerkmanagement-System zudem noch Lizenzüberwachung, SoftwareMetering, Remote Control und dergleichen mehr zur Verfügung stellen soll, so können diese Anforderungen unter keinen Umständen von nur einer Hard- und Software erfüllt werden, da sich die einzelnen Hersteller auf einzelne Aspekte konzentrieren. So liegt das Hauptaugenmerk für Cisco oder Cabletron vor allem darauf, die Hardware-Komponenten im Hub zu überwachen und zu steuern. Das Software-Metering oder die Lizenzüberwachung hängt in dieser Situation vom jeweiligen Netzwerk ab, sodass hier auf zusätzliche Produkte zurückgegriffen werden muss.

1.1 Bereiche des System- und Netzwerkmanagements

Das System- und Netzwerkmanagement kann grob in die folgenden Bereiche eingeteilt werden.

1.1.1 Netzwerk-Management

Eine zentral installierte, herstellerübergreifende Netzwerk-Management-Software wie HP OpenView sammelt alle einlaufenden SNMP-Daten in einer Datenbank. Diese Angaben bereitet das Überwachungssystem grafisch auf, so dass der Netzwerkadministrator einen guten Überblick über den Zustand seines Netzwerks erhält. Zudem wertet die Netzwerk-Software alle relevanten Informationen aus, wie Auslastung, Betriebsstatus oder Performance, um bei Überschreitung definierter Schwellwerte den Administrator zu alarmieren. Die folgende Übersicht fasst alle wichtigen Funktionen des Netzwerk-Managements zusammen:

Konfigurationsverwaltung: Beinhaltet die Bereitstellung und Steuerung von Netzwerk-Komponenten. Hilft zudem bei der Regelung der Planung, Erweiterung, Änderung und Wartung der Netzwerkkonfiguration und der Konfigurationsdaten.

Fehlermanagement: Hilft, drohende Engpässe eines Netzwerks rechtzeitig festzustellen. Netzwerkprobleme können somit im Vorfeld durch entsprechende Lösungsvorschläge verhindert werden.

Performance-Management: Erfasst und überwacht alle Performance-relevanten Vorgänge im Netzwerk. Dient zur Kontrolle und Steigerung der Netzwerk-Effizienz.

User-Administration: Vereinfacht die Einrichtung und Pflege von Benutzerkonten. Regelt die Verteilung der Netzwerk-Ressourcen.

1.1.2 Remote-Server-Management

Eine wesentliche Funktion jedes Server-Management-Systems ist der Zugriff auf den Server aus der Ferne. Man unterscheidet hier zwischen In-Band- und Out-of-Band-Verbindungen.

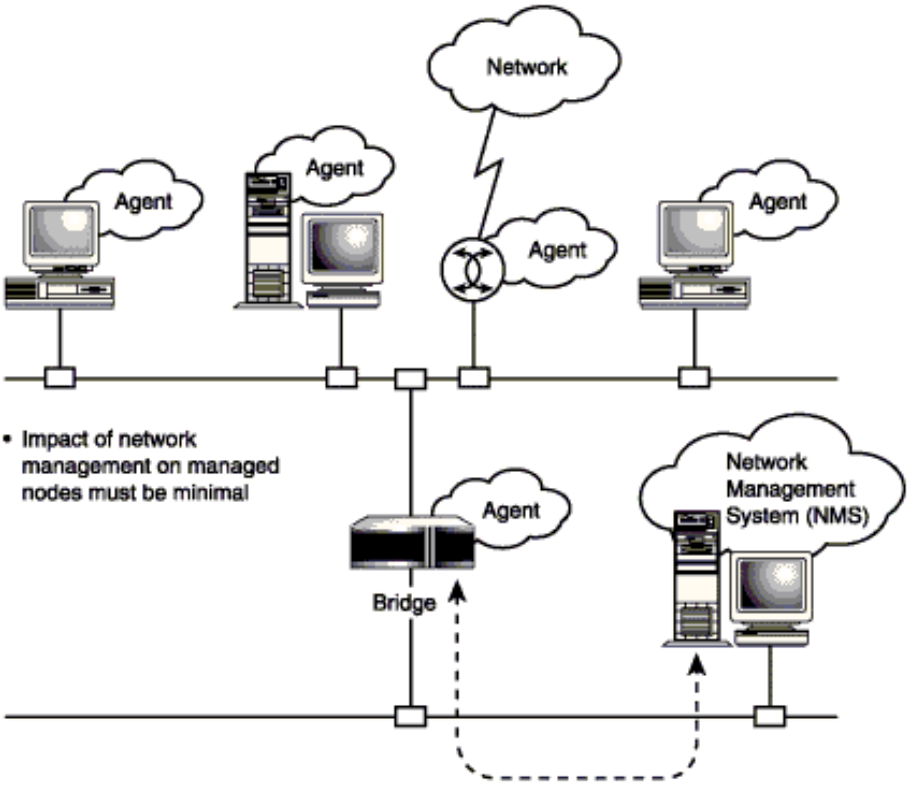

Abbildung 1.1: Netzwerk-Management Modell

Die In-Band-Kommunikation erfolgt über das Netzwerk-Interface der Maschine. Dagegen benutzt eine Out-of-Verbindung die USB-Schnittstelle, den seriellen Port oder ein Modem zur Datenübermittlung. Entscheidend für die Funktionalität ist, dass die Kommunikation nicht nur lokal, sondern auch remote möglich sein muss.

In der Regel werden auf der Serverseite Controller-Karten eingesetzt, die sich über ein eigenes unabhängiges Stromnetz mit Energie versorgen. Diese Lösungen verfügen über ein eigenes Betriebssystem und integrierte SNMP-Agenten sowie über ein User- und Alarm-Management. Mit Hilfe dieser Funktionen ist eine Systemanalyse bei einem Betriebssystemausfall oder aufgetretenen Hardware-Fehler möglich. Ein Neustart via remote kann ebenfalls eigenständig erfolgen. So erstellt zum Beispiel die Zusatz-Hardware bei einem Serverabsturz einen Statusbericht. Anhand dieser Informationen kann der Administrator die Ursache der Fehlfunktion im Remote-Modus analysieren und gegebenenfalls beheben. Umfangreiche Schutzmechanismen verhindern den Missbrauch des Remote-Zugangs durch Unbefugte. Dazu zählen Passwortschutz und Protokollierung des Remote-Datenverkehrs sowie eine automatische Verschlüsselung der Daten bei der Übertragung.

1.1.3 Inventory-Management

Das Inventory-Management dient der Bestandserfassung aller im Unternehmensnetzwerk verfügbaren Komponenten. Dazu fragt die Management-Software in regelmässigen Zeitabstän-

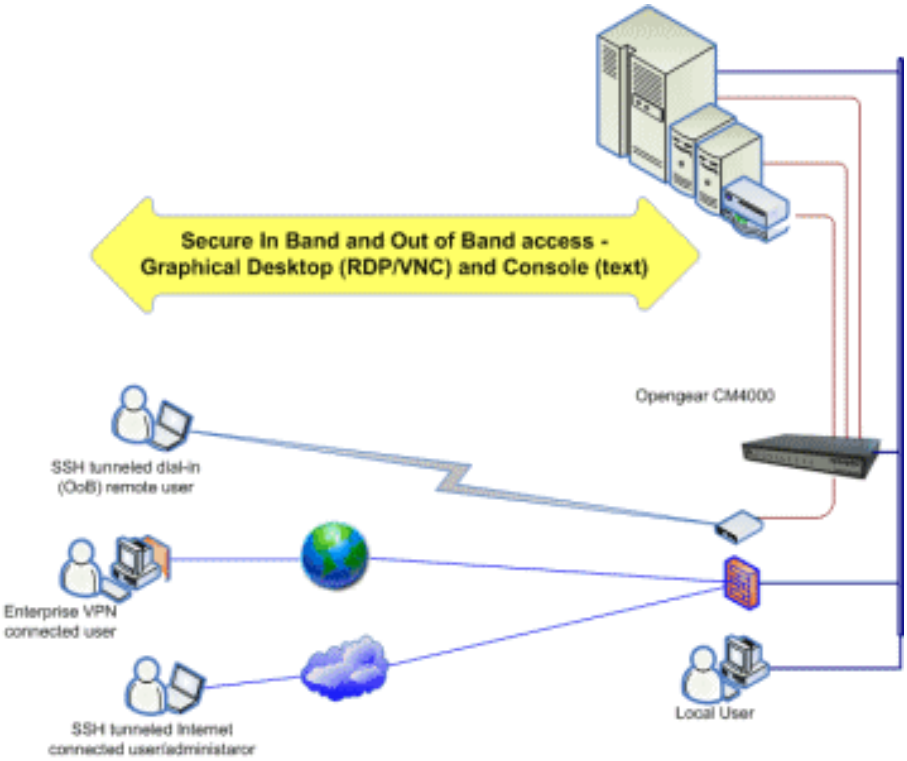

Abbildung 1.2: Remote-Administration

den die Konfigurationsdaten aller Geräte im Netz ab. Sie umfassen je nach verwendeter Management-Software mehr oder weniger detaillierte Informationen über das Mainboard (Bezeichnung, Hersteller, Seriennummer), BIOS-Version, Prozessor, Speicherausbau, Steckkarten oder Laufwerke sowie die Hard- und Software-seitige Ermittlung der Netzwerkkonfiguration. Die Inventory-Verwaltung erfasst auch die Herstellerdaten der angeschlossenen Peripheriegeräte wie Monitore oder Drucker.

Darüber hinaus liefern viele Management-Tools auch Daten über die installierte Software. Diese Informationen wie Programmnamen, Versionsnummer oder Installationsdatum sind unter anderem wichtig für die Verwaltung von Software-Updates und Lizenzrechten. Eine rechnergestützte automatisierte und zentrale Verwaltung der Hard- und Software-Konfigurationsdaten zählt zu den wesentlichen Vorteilen des Inventory-Managements. Auf der Basis der erfassten Daten lassen sich Funktionen wie Soll/Ist-Abgleich, geplante und rechnergestützte Upgrades oder Lizenzmanagement realisieren.

1.1.4 Applikations-Management

Das Applikations-Management besteht aus mehreren unterschiedlichen Funktionen. Die wichtigsten davon fasst man unter dem Oberbegriff Software Deployment zusammen. Es beschäftigt sich mit der Aufgabenstellung, die Software an den entsprechenden Empfänger zu verteilen. Daraus entstehen Probleme, denn der Verteilungsprozess muss in der Regel zu unterschiedlichen Systemplattformen und Konfigurationen sowie zu einer grossen Anzahl von

Komponenten erfolgen. Zusätzlich ist jede installierte Anwendung speziell an die Rechnersysteme wie Server oder Client angepasst.

Konfigurations-Management

In der ersten Phase des Software Deployment kommt das Konfigurations-Management zum Einsatz. Es befasst sich mit der planerischen Umsetzung der Software-Verteilung:

- Erfassen der bestehenden Software-Konfigurationen.
- Ermitteln, welche Veränderungen durch die Software-Verteilung im System entstehen.
- Erstellen eines Tools in Form eines Installations-Scripts zur Vereinfachung der Installation.
- Erstellen einer Paket-Datei zur schnellen und problemlosen Verteilung der Software. Um eine kostengünstige und problemlose Verwaltung der Software-Verteilung zu gewährleisten, sollte sie eine zentrale Stelle durchführen. Eine genaue Dokumentation der Software-Updates und -Veränderungen ist dabei unverzichtbar.

Software-Distribution und -Installation

Der zweite Schritt des Software-Deployment besteht aus der Software-Distribution und -Installation. Es beinhaltet die automatische Verteilung und Installation der Applikation beziehungsweise deren Updates. Ein optimales Software-Management-System sollte folgende wichtige Eigenschaften haben:

- Alle Installationen erfolgen von einer zentralen Stelle und werden von dieser protokolliert.
- Die Verteilung der Software ist individuell für verschiedene Zielsysteme konfigurierbar.
- Der Verteilungsprozess verursacht keine Performance-Engpässe im Netzwerk oder auf den Zielsystemen.
- Eine Lizenzverwaltung der installierten Software ist im Management-System implementiert.

1.1.5 Performance-Management und Monitoring

Das System-Performance-Management arbeitet eng mit dem Hardware- und Software-Monitoring zusammen. Denn zur Analyse der entsprechenden System-Performance ist eine Überwachung (Monitoring) und Meldung bei Grenzwertverletzungen dieser Komponenten erforderlich. Zu den grundlegenden Funktionen eines Performance-Managements gehören die Überwachung der Auslastung der Netzwerk-Verbindungen zu den Servern, die Kontrolle der Basisprozesse auf den Servern und die Erfassung der verfügbaren Massenspeicherkapazität. Zusätzlich sollte man die CPU-Auslastung und das Antwortzeitverhalten von Applikationen für eine optimale Performance-Analyse berücksichtigen.

Welche Performance-Optimierungen und Überwachungsfunktionen die meisten Vorteile bringen, hängt in erster Linie von der Grösse und Komplexität sowie von den festgelegten Vorgaben für die Verfügbarkeit des Client-/Server-Systems ab. Darüber hinaus müssen wirtschaftliche Aspekte für die Realisierung der verschiedenen Funktionen berücksichtigt werden.

1.1.6 Einschränkungen für dieses Modul

Wir werden uns im folgenden soweit möglich auf das Netzwerk-Management beschränken.

1.2 OSI und TCP/IP

Für eine heterogene Netzwerklandschaft ist nicht nur der Einsatz der unterschiedlichsten Hardware-Komponenten kennzeichnend, sondern meist auch eine heterogene Protokolllandschaft. Wenn es nur ein Protokoll zur Kommunikation in Netzwerken geben würde, wäre das zwar wünschenswert das wird aber für die nächsten Jahre Wunschdenken bleiben. Man wird sich damit abfinden müssen, dass unterschiedliche Rechnerwelten auch unterschiedliche Protokolle einsetzen. Die Idee von OSI als Einheitsprotokoll hat sich inzwischen als Traum erwiesen, da die etablierten Protokolle bereits so weit verbreitet sind, dass eine Umstellung auf OSI mit enormen Kosten und enormem Aufwand verbunden wäre.

Die eingesetzten Protokolle sind stark vom jeweiligen Hersteller des Systems abhängig. So wird man in der IBM-Grossrechnerwelt immer noch auf SNA stossen, obwohl es inzwischen auch möglich ist, Terminal-Emulationen über TCP/IP zu realisieren. IBM ist inzwischen, wie andere Hersteller auch, in der Lage, TCP/IP als Protokoll zu unterstützen. In einem Netzwerk mit NetWare als Serversystem kommen die Protokolle IPX/SPX zum Einsatz. Auch hier ist man inzwischen in der Lage, durch NetWare IP und Native-IP im Netzwerk TCP/IP als Transportprotokoll einzusetzen. Betrachtet man jetzt noch Windows NT, so verwendet auch Microsoft sein eigenes Protokoll, lässt einem jedoch bei der Installation die Wahl, TCP/IP als Transportprotokoll einzusetzen. Bei Windows 2000 und allen späteren Versionen, setzt auch Microsoft auf eine Native IP Umgebung, wobei immer noch NetBIOS unterstützt wird, wenn dies die Netzwerkumgebung fordert. TCP/IP, das ursprünglich aus der Unix-Welt kommt, erweist sich immer mehr als das universelle Protokoll, das von so ziemlich allen führenden Herstellern unterstützt wird.

Auch wenn TCP/IP vor Jahren noch keine Chancen auf dem Markt zugebillgt wurden, wird dieses Protokoll gerade in den letzten Jahren in grosser Zahl installiert, vor allem wenn es um den Aufbau von heterogenen Netzwerken geht. Dies ist auch der Grund, warum TCP/IP zum De-facto-Standard geworden ist. TCP/IP bietet auf den Schichten 3 und 4 einfache, anwendungsorientierte Grunddienste wie Dateitransfer, E-Mail und Virtual-Terminal-Emulation. Da auch Unix in den letzten Jahren immer mehr an Bedeutung gewonnen hat und TCP/IP sehr stark mit Unix verbunden ist, wurde und wird der zukünftige Einsatz von TCP/IP noch gefördert; der verstärkte Einsatz von Internet und Intranet-Anwendungen trägt wesentlich zum erhöhten Einsatz von TCP/IP bei. Mit TCP/IP kann man in einfacher Weise heute das

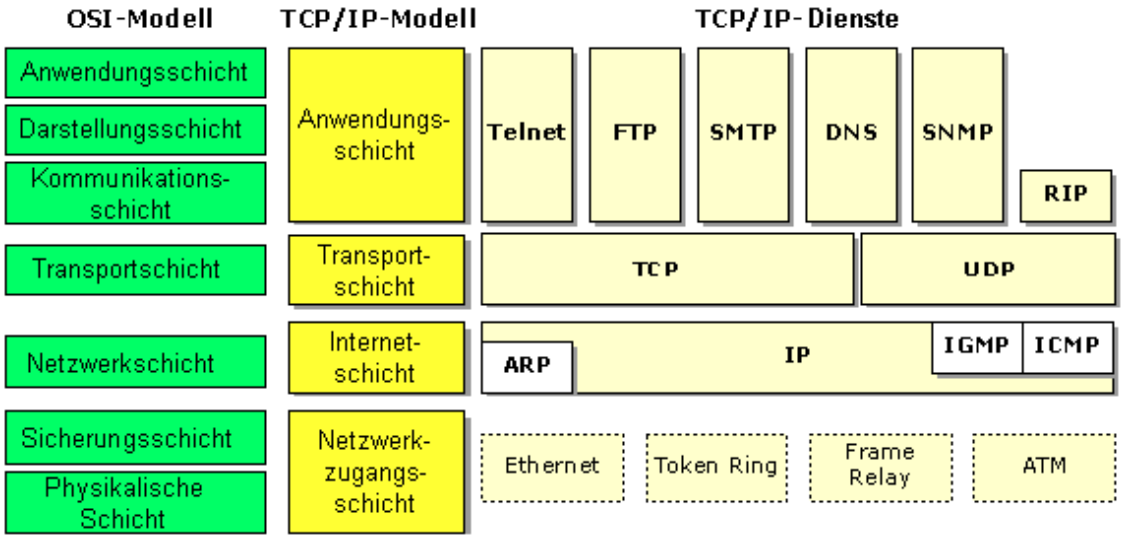

Abbildung 1.3: Vergleich TCP/IP und OSI

tun, was man eigentlich mit den Protokollen und Standards nach OSI machen wollte.

Das hat auch Auswirkungen auf den Bereich Netzwerkmanagement, wenn es um die Entscheidung geht: Netzwerkmanagement auf Grundlage von SNMP (kommt aus der TCP/IP-Welt) oder auf Grundlage von OSI. Im Zuge der TCP/IP-Entwicklung wurde auch SNMP (Simple Network Management Protocol) als einfaches und leicht zu implementierendes Netzwerkmanagement-Protokoll entwickelt. Wegen seiner Einfachheit und leichten Implementierung unterstützt SNMP auch die Netzwerkkomponenten fast jedes Herstellers und erfreut sich bei Netzwerkadministratoren grosser Beliebtheit. Das OSI-Netzwerkmanagement ist dagegen ins Hintertreffen geraten, auch wenn führende Hersteller versucht haben, ein OSI-Netzwerkmanagement auf dem Markt zu etablieren. Im Gegenteil: Um den gestiegenen Anforderungen gerecht zu werden, hat man SNMP weiterentwickelt und SNMPv2 veröffentlicht.

Kapitel 2

Anforderungen an das Netzwerkmanagement

Alle Anforderungen an ein Netzwerkmanagement lassen sich mit Sicherheit nicht erfüllen. Von daher ist es sehr angenehm, dass im Zuge der OSI-Standardisierung für das Netzwerkmanagement fünf wichtige Aspekte definiert worden sind, die von einem Netzwerkmanagement-System erfüllt werden müssen (oder besser gesagt: erfüllt werden sollten). Auch wenn es sich dabei um eine Spezifikation der OSI-Umgebung handelt, orientieren sich doch fast alle Hersteller daran. Um einen generellen Überblick über Netzwerkmanagement-Aufgaben zu erhalten, sollen diese Aspekte anschliessend näher betrachtet werden. OSI hat die folgenden fünf Bereiche definiert, die von einem Netzwerkmanagement-System erfüllt werden müssen:

Fault-Management Darunter sind Aufgaben zu verstehen, die es ermöglichen, Fehler zu erkennen, zu finden und zu beheben.

Configuration-Management Darunter versteht man Aufgaben, die es ermöglichen, Konfigurationsdaten zu sammeln, auszuwerten und zu ändern, also die zu überwachenden Systeme nicht nur überwachen, sondern auch steuern zu können.

Performance-Management Ist auch dieser Bereich abgedeckt, so dient das Netzwerkmanagement-System dazu, den Zustand der zu überwachenden Systeme bezüglich Durchsatz, Effizienz und Effektivität (d.h. die Leistung aller einzelnen Systeme) zu kontrollieren.

Accounting-Management Wenn es darum geht, die Nutzung bestimmter Komponenten zu verrechnen, weil diese gleichzeitig von mehreren Abteilungen genutzt, aber von einer zentralen EDV-Abteilung bereitgestellt werden, muss es die Möglichkeit geben, Einzelauswertungen durchzuführen. Auf diese Weise kann ermittelt werden, welche Komponenten wie stark "belastet" worden sind. Nur so kann eine interne Kostenverrechnung effektiv gestaltet werden.

Security-Management Damit nicht jeder die oben aufgeführten Management-Bereiche (Fault-Management etc.) ändern und manipulieren kann, müssen bestimmte Sicherheitsvorkehrungen vorhanden sein, um nur berechtigten Personen deren Möglichkeiten verfügbar zu machen.

Bei dieser Aufzählung handelt es sich um Standards, die von der OSI-Arbeitsgruppe definiert worden sind. Nicht jedes Managementsystem wird alle diese Punkte vollständig abdecken können. Andere Systeme werden auch noch andere Funktionen enthalten, die nicht exakt in diese Bereiche eingestuft werden können. Hierbei geht es um Zusätze, die vor allem im LAN-Bereich durch den Einsatz von Servern notwendig werden. Erwähnt seien nur die Notwendigkeit der Lizenzkontrolle, das Software-Metering, die Remote Control, die Software-Distribution oder auch die Virenschutzproblematik. Je nach Hersteller werden solche Möglichkeiten auch noch zusätzlich angeboten.

2.1 Fault-Management

Ab einer bestimmten Netzwerkgrösse wird es immer schwieriger, das System im Ganzen zu überwachen und zu kontrollieren, vor allem wenn es darum geht, nicht mehr funktionierende Komponenten nicht nur schnell zu erkennen, sondern auch auszuwechseln. Für den Fall, dass Fehler auftreten, geht es vor allem darum, so schnell wie möglich festzustellen, wo genau der Defekt aufgetreten ist, den Rest des Netzwerks von der fehlerhaften Komponente abzuschotten, sodass es immer noch funktionsfähig zur Verfügung steht, das Netzwerk so zu rekonfigurieren oder anzupassen, dass der Einfluss der fehlerhaften Komponente auf das Netzwerk so gering wie möglich ist, und die fehlerhafte Komponente auszutauschen oder zu reparieren, um das Netzwerk in den ursprünglichen Zustand versetzen zu können. Ausschlaggebend hierbei ist, welche Komponenten in einem Netzwerk ausfallen. So bewirkt der physikalische Ausfall einer Verkabelung, dass keine Signale mehr transportiert werden können und somit die Kommunikation zwischen Workstation und Server gestört ist. Zu ähnlichen Effekten kann ein schlecht montiertes Kabel führen. Treten bei einer Netzwerkadapterkarte Fehlfunktionen auf, kann das ebenso zu Störungen im Netzwerk führen. Diese Probleme müssen erkannt und behoben werden, um anschliessend wieder ein funktionsfähiges Netzwerk zu haben.

In der Regel erwartet jeder Anwender eine schnelle und zuverlässige Lösung seiner Probleme. Die Praxis zeigt, dass das kaum zu erfüllen ist, wenn den Verantwortlichen solche kleinen Hilfsmittel wie Cable Scanner (zum Prüfen der physikalischen Kabel im Netzwerk) verwehrt werden, mit deren Hilfe es möglich ist, einfache Kabelfehler zu erkennen bzw. zu finden. Nur die geeigneten Werkzeuge können dabei helfen, schnell zu reagieren und auftretende Fehlfunktionen zu finden und zu beheben. Nur vage Vermutungen, warum ein Kabel oder das Netzwerk (oder ein Teil davon) nicht funktioniert, sind hier nicht angebracht, da ein Fehler im Netzwerk unter Umständen durch eine Vielzahl von Randbedingungen beeinflusst werden kann. Allein durch geeignete Fehlererkennungs- und Diagnose-Managementfunktionen kann dem Netzwerkverwalter Unterstützung und Hilfestellung gegeben werden. Als Netzwerkverwalter will man aber nicht immer nur reagieren, sondern auch agieren können. Das Netzwerkmanagement soll eine Unterstützung bieten, um die sich anbahnenden Ausfälle frühzeitig erkennen zu können, sodass bereits im Vorfeld entsprechende Massnahmen eingeleitet werden können. Daher müssen auch Möglichkeiten zur Verfügung stehen, den aktuellen Zustand des Netzwerks ständig überwachen und kontrollieren zu können. Dazu zählen unter anderem auch Tests, die für bestimmte Komponenten durchgeführt werden können, Fehlermeldungen in entsprechenden Alert-Dateien oder auch Statistiken, die ausgewertet werden

können. Nach einer erfolgreichen Behebung des oder der Ausfälle ist zu prüfen, ob nicht auch noch an anderer Stelle Fehlfunktionen zu erwarten sind. Dieser Vorgang wird auch als Problem Tracking und Control bezeichnet.

2.2 Configuration-Management

Heutige Netzwerke bestehen aus einer Vielzahl von Einzelkomponenten und logischen Subsystemen (Device Driver, Protocol Stacks etc.), die zur Erfüllung der einzelnen Aufgaben konfiguriert und modifiziert werden können. Da ein Netzwerk nicht statisch ist, sondern sich durch seine Dynamik auszeichnet, ist die ständige Anpassung von bestehenden Konfigurationen gefordert. So kann es durchaus notwendig werden, einen seit langem in Betrieb befindlichen Router bezüglich der zu übertragenden Protokolle zu erweitern oder einzuschränken; die Konfiguration des Routers muss also geändert werden. Es könnte auch sein, dass interne Kommunikationsmechanismen des Routers (Timer, Pufferbereiche, Routing-Tabellen etc.) im Router anzupassen sind. Das Konfigurationsmanagement umfasst die Möglichkeiten, ein Netzwerk neu zu initialisieren oder teilweise abzuschalten, ohne dass davon andere wesentliche Teile des restlichen Netzwerks in Mitleidenschaft gezogen werden. Damit verbunden sind auch die Mechanismen, um Teile des Netzwerks zu pflegen, neue Komponenten hinzuzufügen, anzupassen oder gar zu entfernen und dies alles im laufenden Betrieb , um anschliessend allen davon betroffenen Stellen im Netzwerk die neuen Funktionen verfügbar zu machen. Bei der Durchführung solcher Anpassungen kommt es nicht selten vor, dass eine neu konfigurierte Komponente regulär beendet (Shutdown) und anschliessend neu gestartet werden muss. Es wäre wünschenswert, solche Operationen "unbeaufsichtigt" durchführen zu können. Dies bedeutet zum Beispiel, dass man einen Router in Berlin von München aus konfiguriert und anschliessend neu hochfährt. Nach einer gewissen Zeit müsste der neu konfigurierte Router in Berlin im Managementsystem wieder erscheinen und mit den neuen Werten im Netzwerk arbeiten. Der Netzwerkverwalter muss die Möglichkeit haben, alle Komponenten im Netzwerk automatisch zu erkennen und deren aktuellen Zustand und deren Konfiguration abzubilden. Wenn bestimmte Komponenten öfter installiert werden oder ähnlich konfiguriert werden, wäre es gut, bestehende Konfigurationen für andere, ähnliche Komponenten nutzen zu können, d.h. diese Einstellungen und Attribute per Download auf die Komponenten zu übertragen. Es geht in diesen Fällen aber nicht nur um die Rekonfiguration der einzelnen Komponenten, sondern auch um die Möglichkeit, über aktuelle Änderungen sofort informiert zu werden, Konfigurationslisten zu erzeugen oder auch bestehende Konfigurationen abzuspeichern, um diese später an anderer Stelle nutzen zu können. Netzwerkverwalter wollen zudem die Sicherheit haben, dass nur berechtigte Personen die Komponenten ändern und anpassen dürfen (Software-Distribution und Software-Updates).

2.3 Performance-Management

Ein Netzwerk grösseren Ausmasses besteht aus einer Vielzahl von Komponenten: aus der physikalischen Verkabelung, Netzwerkadaptern in den Workstations und Servern, aus Routern, Bridges, Broutern, Gateways, Fax-Servern und vielem mehr. Alle Komponenten stehen dabei in einer bestimmten Wechselwirkung, die unter anderem auch für die Leistungsfähigkeit und

den Durchsatz im Netzwerk verantwortlich ist. So kann es durchaus sein, dass in einem Netzwerksegment viele Stationen mit wenig Durchsatz angeschlossen sind, wohingegen in einem anderen Segment Stationen eingebunden sind, die eine Menge Datenverkehr im Netzwerk verursachen. Durch eine einfache Verteilung der Workstations auf die einzelnen Segmente könnte zum Beispiel der Gesamtdurchsatz im Netzwerk gesteigert werden. Ähnlich sieht die Situation aus, wenn ein Server im Netzwerk falsch platziert ist und dadurch die Koppelelemente (Bridge, Router oder Brouter) ständig mit Datenpaketen belastet werden, die in das andere Segment transportiert werden müssen. Die Aufgabe des Performance-Managements ist im Wesentlichen das Monitoring und Controlling im Netzwerk. Unter Monitoring versteht man die Aufgabe, den Datenverkehr im Netzwerk sichtbar zu machen, um zum Beispiel eine Situation wie die oben aufgeführte zu erkennen und eventuell Konfigurationsänderungen durchführen zu können. Unter die Kategorie Controlling fallen Aktivitäten, die es ermöglichen, Anpassungen durchzuführen, um die Leistungsfähigkeit im Netzwerk zu verbessern. Für den Netzwerkverwalter sind dabei die folgenden Fragen von Bedeutung: Wie gross ist die Auslastung im Netzwerk? Kann intensiver Datenverkehr einzelner Stationen festgestellt werden? Ist der Gesamtdurchsatz auf ein nicht akzeptables Mass gesunken? Sind generelle Engpässe festzustellen? Hat sich die Antwortzeit verschlechtert?

Diese Werte können vom Netzwerkverwalter nur dann vernünftig überwacht und kontrolliert werden, wenn Mechanismen zur Verfügung stehen, die es ermöglichen, entsprechend aussagekräftige Informationen zu erhalten. Hierzu zählen unter anderem Mechanismen, um Schwellenwerte zu definieren. Beim Erreichen dieser Schwellenwerte werden Meldungen erzeugt, die den Netzwerkverwalter darüber informieren, dass Leistungsengpässe aufgetreten sind. So ist es zum Beispiel ausschlaggebend, wie oft im Netzwerk Retransmissions (Wiederholung der Übertragung von Datenpaketen durch eine Fehlersituation) auftreten, bis ein Datenpaket korrekt vom Sender zum Empfänger transportiert ist. Das PerformanceManagement muss daher in der Lage sein, eine Vielzahl von Ressourcen im Netzwerk zu überwachen und entsprechend aussagefähige Werte zu liefern. Auf diese Weise kann genau kontrolliert werden, wie sich die Leistungsfähigkeit mit einer zunehmenden Anzahl von Endgeräten im Netzwerk verschlechtert bzw. durch Ergreifen von Gegenmassnahmen wieder verbessert. Damit der Netzwerkverwalter auf die Beschwerden der Anwender über ein zu langsames Netzwerk angemessen reagieren kann, müssen genaue Informationen über die aktuellen Zustände bezüglich Durchsatz und Leistungsfähigkeit der Einzelkomponenten vorliegen. Ohne solche Informationen wäre es nicht mehr als ein "Stochern im Heuhaufen", wenn der Netzwerkverwalter nach Gefühl an der einen oder anderen Stelle Anpassungen durchführte. Erst wenn ein Gesamtüberblick über alle Komponenten vorliegt, kann am Router, an der Workstation oder an der physikalischen Verteilung der einzelnen Stationen etwas geändert werden, um gezielt mehr Leistung zu erhalten. Zu beachten ist auf jeden Fall, dass Aussagen über das Antwortzeitverhalten im Netzwerk auch auf subjektiven Eindrücken der Anwender beruhen.

2.4 Accounting-Management

In einem flächendeckenden Netzwerk müssen oft einzelne Abteilungen oder Profit-Center, teilweise sogar vielleicht einzelne Projektgruppen, für die Inanspruchnahme von Netzwerkleistungen Gebühren zahlen. Hier geht es vor allem um die interne Kostenverrechnung. Dies gilt insbesondere, wenn das Netzwerk im Zuge von Outsourcing durch externe Firmen betrie-

ben wird und die Kosten nach den benötigten Leistungen abgerechnet werden. Auch wenn keine interne Kostenverrechnung durchgeführt wird, ist es für den Netzwerkverwalter aus folgenden Gründen von Vorteil, sich über die einzelnen verursachten Kosten einen Überblick zu verschaffen:

- Benutzer geben Berechtigungen an andere Benutzer weiter, ohne dafür die Erlaubnis zu haben. Somit arbeiten einige Teilnehmer auf Kosten anderer im Netzwerk.
- Die Anwender nutzen das Netzwerk auf ineffiziente Weise, und der Netzwerkverwalter kann in geeigneter Form den Anwender unterstützen, um eine effizientere Nutzung zu erreichen.
- Für den Netzwerkverwalter ist es einfacher, den zukünftigen Ausbau des Netzwerks zu planen, wenn die einzelnen Aktivitäten der Anwender genau bekannt sind (eine Aufgabe, bei der auch das Performance-Management von Bedeutung ist).

Für den Netzwerkverwalter bedeutet das Accounting-Management die Möglichkeit, die Accounting-Informationen festzulegen, die überwacht werden sollen und für die Gebühren verrechnet werden müssen. Zudem sind die Zeitintervalle zu definieren, in denen entsprechende Accounting-Daten generiert werden müssen. Das Erstellen von Accounting-Auswertungen ist zudem nur von entsprechend autorisierten Personen durchzuführen, da es sich hierbei um sehr sensible Daten handelt. Das Accounting-Management ist mit äusserster Vorsicht einzusetzen, da es durchaus sein kann, dass die damit erzeugten Daten und Auswertungen in die Kategorie der Mitarbeiterkontrolle gehören. Gegebenenfalls ist in grösseren Unternehmen die Zustimmung des Betriebsrats erforderlich. Das Netzwerkmanagement-System muss die Möglichkeit besitzen, notwendige Kennungen für Benutzer einzurichten, die das Accounting nicht nur konfigurieren, sondern auch auswerten dürfen.

2.5 Security-Management

Zum Security-Management zählen unter anderem die Erzeugung, die Verteilung und das Speichern von Verschlüsselungsinformationen. Passwörter, andere Autorisierungen und Zugangskontrollinformationen müssen gewartet werden. Das Security-Management betrifft aber auch die Überwachung und das Monitoring für den Zugang zum Netzwerk bzw. für alle Informationen, die über das Netzwerkmanagement-System erhalten werden. Dies bezieht sich auf sämtliche Komponenten im Netzwerk. Log-Files sind ausschlaggebend für die damit verbundenen Sicherheits-Tools. Daher ist das Security-Management sowohl mit dem Sammeln und Speichern von Auditing-Informationen und Sicherheitsmechanismen als auch mit dem Aktivieren und Deaktivieren dieser Mechanismen befasst.

Durch das Security-Management wird die Nutzung einzelner Ressourcen im Netzwerk sicherer gemacht. Dies betrifft auch das Sammeln und Auswerten spezieller benutzerspezifischer Informationen (s. Accounting-Management). Von daher sollten die Möglichkeiten auch nur für autorisierte Benutzer verfügbar sein, also nur von solchen Benutzern aktiviert und deaktiviert werden können. Dabei ist zu beachten, dass alle Netzwerkbetriebssysteme in der Regel eigene Sicherheitsmechanismen implementiert haben, sodass das Security-Management nur für ausgewählte Funktionsbereiche eingesetzt werden muss (bzw. kann). So kann man hierüber zum Beispiel definieren, dass ein bestimmter Port im Hub nur dann freigeschaltet wird,

wenn die Workstation mit der richtigen Node-Adresse angeschlossen ist. Andererseits kann man jeden nicht belegten Port im Hub generell abschalten, sodass es nicht vorkommen kann, dass plötzlich jemand einen weiteren Rechner im Netzwerk in Betrieb nimmt, weil gerade noch eine Anschlussdose im Büro frei ist (d. h., der Netzzugang wird dann also verhindert). Andere Sicherheitsfunktionen betreffen aber auch das Netzwerkmanagement-System selbst, um nur berechtigten Personen die Konfiguration und das Auswerten von Managementinformationen zu ermöglichen. Auf diese Weise kann keine unberechtigte Person einfach an der Hub-Einstellung oder am Router Änderungen vornehmen und so das gesamte Netzwerk in Unordnung bringen.

Kapitel 3

Dokumentation

Die Wartbarkeit eines Netzwerks hängt stark von der Qualität seiner Dokumentation ab. Eine exakte, vollständige und aktuelle Dokumentation ist unverzichtbar.

So besteht eine Netzwerkdokumentation aus folgenden Unterlagen:

Gruppe	Dokumente
Netzwerkkomponenten	Verkabelung (Lage der Kabeltrassen, Patch-Panel etc.) Belegung der aktiven Komponenten, Patch-Panel Netzplan (physikalisch, logisch) Externe Anbindungen
Handbücher	Arbeitsplatzsysteme, Serversysteme Akt. Komponenten Software
Bestandslisten	Hardware (Server, aktive Komponenten, Arbeitsplatzsysteme) Software (Server, akt. Komponenten, Arbeitsplatzsysteme)
Betrieb	Betriebshandbuch Schichtprotokoll
Datenschutz	Bestimmungen, Richtlinien
Konzepte	Datensicherung Notfallkonzept, Notfallhandbuch Benutzerrechte Sicherheitskonzept Netzwerk Management IT-Strategie
Räumlichkeiten	Zugangsrechte Lage der IT-Komponenten
Administration	Admin-Journal
Support	Supportstatistik

Wir beschränken uns im folgenden auf die Dokumentation der Netzwerkkomponenten und der Verkabelung, da die anderen Punkte den Rahmen des Moduls sprengen.

3.1 Netzwerkkomponenten

3.1.1 Verkabelung

Kabel sollten an allen Endpunkten beschriftet werden, ebenso wie in bestimmten Abständen, damit sie einfach identifiziert werden können, wenn sie sich in einer Decke oder einer Wand befinden (Einige Hersteller bieten an, ganze Kabelrollen entsprechend zu beschriften.). Es ist sinnvoll, Kopien lokaler Kabelführungen in den Kommunikationsschränker aufzuhängen, damit sie sofort aktualisiert werden können, wenn Änderungen durchgeführt werden. Alle paar Wochen sollte jemand die Änderungen sammeln und in eine elektronische Datenbank eintragen.

3.1.2 Belegung der aktiven Komponenten, Patch-Panel

Wenn in einem Kommunikationsschrank hunerte von Kabeln auf ein Patchpanel geführt werden und dort verschiedene physikalische Segmente verbinden, ist es unabdingbar die Belegung direkt am Panel (oder den aktiven Komponenten) oder direkt nebenan auf einem Belegungsschema beschriftet zu haben.

3.1.3 Netzwerkplan

Der logische Netzwerkplan (oder auch Netzplan) zeigt die Beziehungen zwischen Komponenten und den Informationsfluss durch das Netzwerk. Ein physikalischer Netzplan versucht möglichst genau zu zeigen wie jede Komponente physikalisch ans Netzwerk angeschlossen ist. Zum Beispiel könnte ein logischer Netzplan eines Windows-Netzwerks die Computer zu Domänen gruppiert zeigen, obschon diese sich physikalisch nicht im selben Abschnitt des Netzwerks befinden.Ein physikalischer Netzplan würde hingegen den Ort jedes Computers zeigen und an welchen Switch diese angeschlossen sind und so weiter. Allgemein helfen logische Netzpläne beim Auffinden von Konfigurations und Applikationsproblemen und physikalische Netzpläne um Probleme zu isolieren welche nur Teile eines Netzwerks betreffen (zum Beispiel ein fehlerhafter Switch).

Netzwerkpläne können entweder mit Zeichentools wie Visio oder Dia erstellt werden, oder automatisch mittels einer Managementsoftware.

Anforderungen

Ein Netzwerkplan muss mindestens folgende Anforderungen erfüllen, damit er sinnvoll eingestzt werden kann:

- Standardisierte Symbole aus Visio oder Dia
- logische Bezeichnungen der Komponenten
- Genaue Typ-Bezeichnung bei Geräten wie Router, Switch, Firewall usw.
- IP-Adressen der Komponenten

- Subnetzmaske

Es sind je nach Detaillierungsgrad aber auch noch mehr Informationen eintragbar, wie Kabeltyp/-länge und Stromversorgung. Netzwerkpläne welche automatisiert mittels Managementsoftware erstellt werden, können zusätzlich auch Status, Konfigurationseinstellungen, Traffic usw. anzeigen lassen.

Im folgenden Bild ist ein einfacher Netzwerkplan abgebildet.

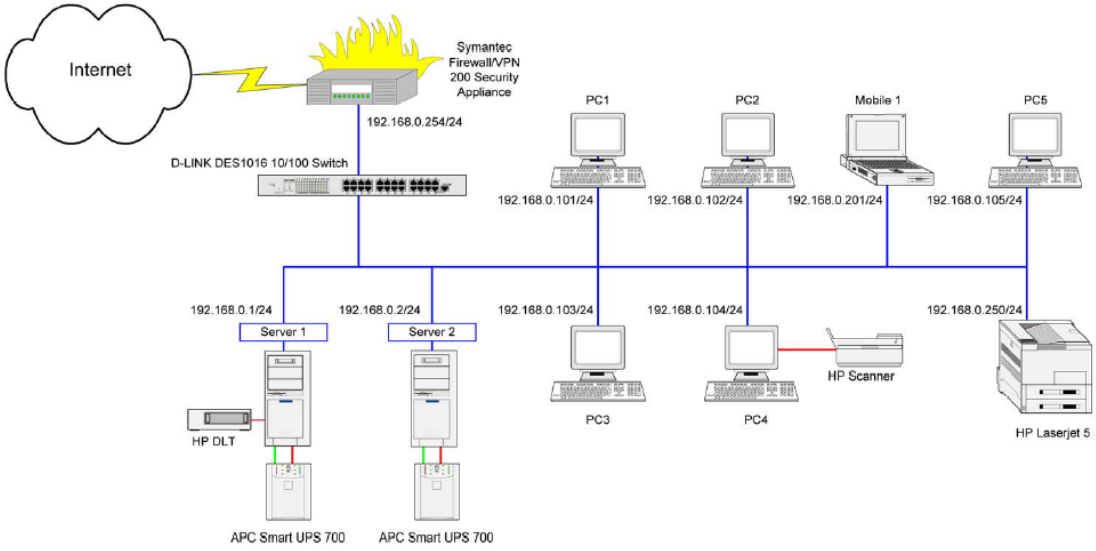

Abbildung 3.1: einfacher Netzwerkplan

Kapitel 4

Netzwerkverwaltung mit SNMP

Dieses Kapitel ist von [2] übernommen.

4.1 Überblick über SNMP

SNMP ist ein weitverbreitetes Protokoll für die Netzwerkverwaltung in TCP/IP- Netzwerken. Mit SNMP können die mit dem Netzwerk verbundenen Geräte überwacht und verwaltet werden.

4.1.1 Die Netzwerkverwaltung

Der Begriff Netzwerkverwaltung beschreibt spezielle Verwaltungsfunktionen und die Möglichkeit diese Funktionen von einer zentralen Verwaltungskonsole aus anzuwenden. Damit die Netzwerkverwaltung zentral ausgeführt werden kann, müssen andere Computer im Netzwerk unter anderem folgende Daten zur Verfügung stellen:

- Identifizierung und Statistiken des Netzwerkprotokolls
- Dynamisches Erkennen der mit dem Netzwerk verbundenen Computer
- Konfigurationsdaten für Hardware und Software
- Statistiken über Leistung und Auslastung des Computers
- Ereignis- und Fehlermeldungen der Computer
- Statistiken über die Verwendungen von Programmen und Anwendungen

4.1.2 Entwicklungsgeschichte von SNMP

Bei der Entwicklung und Forschung der Internetfamilie wurde kein großer Gedanke an die Verwaltung der Netze verschwendet. Dies kam auch dadurch Zustande, daß die Gateways für die Netzwerke, die diese Protokolle benutzten, von einem einzigen Hersteller stammen

und somit dieser Hersteller für die Verwaltung der Gateways durch eigene Techniken verantwortlich war. Hier kümmerte sich niemand um herstellerunabhängige Verwaltungstechniken.

Ab Mitte der 80er Jahre begann die Zahl der Netze, die mit dem Internet verbunden waren, sich jährlich zu verdoppeln und somit gab es nun Organisationen die für die Verwaltung von einzelnen Netzwerkteilen in Regionen, Universitäten und Backbones verantwortlich waren. Da alle benutzten Geräte von verschiedenen Herstellern stammen, mußte schnellstmöglich ein Modell für die Netzwerkverwaltung entwickelt werden, um die Arbeit dieser Organisationen zu erleichtern.

Im März 87 beschloß eine Gruppe von Netzwerkspezialisten aus Industrie und Forschung, daß etwas dagegen getan werden müßte. Es bestanden drei Entwicklungen:

- Aus der ersten Entwicklung entstand das Simple Gateway Monitoring Protocol (SGMP), welches im August außerhalb der Entwicklungsnetze eingesetzt wurde.
- Aus der zweiten Entwicklung entstand das High-level Entity Management System (HEMS), welches jedoch nie außerhalb der Entwicklungsnetze eingesetzt wurde und obwohl es einige interessante Konzepte enthielt, abgelehnt wurde.
- Aus der dritten Entwicklung entstand das OSI- Netzverwaltungsprotokoll für die Internet Familie: CMIP über TCP(Common Management Information Protocol über Transmission Control Protocol).

Da es zu keiner Einigung über diese drei Protokolle kam, wurde im Februar 1988 ein ad hoc Ausschuß aus interessierten Gruppen benannt, um dieses Problem zu lösen. Hierbei kam heraus das HEMS einen wesentlichen Nachteil nichttechnischer Natur hatte: es hatte nicht die Verbreitung von SGMP, welches in fast allen regionalen Netzen benutzt wurde, noch hatte es die Unausweichlichkeit von OSI. Der leitende Forscher von HEMS zog sich zurück.

Es wurde beschlossen eine langfristige und eine kurzfristige Lösung zu entwickeln:

- Kurzfristig: SGMP, jedoch sollte dieses Protokoll noch erweitert werden => SNMP
- Langfristig: OSI- Ansatz (CMIP über TCP)

Dank der Unterstützung durch die Hersteller und durch die große Verbreitung des Protokolls, wurde im April 1989 SNMP zum ëmpfohlenenŠtandard erhoben. Im Mai 1990 wurde SNMP vom IAB(Internet Activities Board = Vereinigung die sich mit der technischen Entwicklung der Internet Protokollfamilie befaßt) zum offiziellen Standard ernannt.

4.2 Wichtige Begriffe der Netzwerkverwaltung kurz erklärt

Host Bezeichnung für eine beliebige mit dem Netzwerk verbundene Hardwarekomponente inklusive Workstations oder Server

Verwaltete Objekte sowohl Host- Hardware wie auch Ressourcen Hardware, die von einem anderen Rechner im Netzwerk verwaltet werden können.

MIB (Management Information Base) Datendatei in der die Daten der verwalteten Objekte eines Host gespeichert sind. Jeder Host kann über mehrere MIBs verfügen.

Manager Softwareprogramm , welches Daten von einem Agenten im Netzwerk fordern kann. Der Manager verfügt üblicherweise über ein User- Interface, über den der Status und die abgerufenen Daten eines Host angezeigt werden können

Agent Softwareprogramm, welches die Bearbeitung der Datenanforderung eines Managers übernimmt. Nach der Datenaufforderung eines Managers, kann der Agent die Daten eines verwalteten Objektes abrufen

Nodes Werden unterteilt in:

- Gemanagte Nodes: Netzwerkknoten, die ständig Informationen zum Status des Netzwerks sammeln und senden.
- Management Nodes: Netzwerkknoten, die Informationen von einem gemanagten Node anfordern.
- Ungemanagte Nodes: Hierzu zählen alle Komponenten, die Netzwerk-Management nicht unterstützen oder nicht über ein kompatibles Protokoll verfügen.

Jeder gemanagte Knoten muss einen SNMP-Agenten zur Verfügung stellen. Dieser ermittelt Informationen und überträgt sie auf Anforderung an den Management Node. Der Datenaustausch beginnt stets mit einem Request des Management Node an den Agenten des Empfängers. Der prüft die Berechtigung der Anfrage, ermittelt die angeforderten Informationen und schickt sie an die Administrations-Konsole. Als Management Node kommt in der Regel eine Workstation mit installierter Netzwerk-Management-Software zum Einsatz. Das System sammelt in definierten Zeitabständen die Daten der gemanagten Nodes ein. Da dieses System ebenfalls überwacht werden muss, kann aber auch hier durchaus ein lokaler SNMP-Agent laufen.

4.2.1 Verfügbare Operationen von Manager und Agenten

Die Hauptfunktion eines SNMP Managers besteht darin, Informationen von einem SNMP-Agenten zu fordern. Ein Manager kann nur folgende Funktionen einleiten:

- get Anforderung eines bestimmten Wertes wie z.B. verfügbarer Festplattenspeicher
- get-next nforderung für den nächsten Wert
- set Ändern eines Wertes(da die meisten Werte schreibgeschützt sind, wird diese Funktion nicht oft benutzt)

Die Hauptfunktion des Agenten besteht darin, die vom Manager erhaltenen Operationen (get, get-next und set) auszuführen. Die einzige Operation, die vom Agenten eingeleitet wird, ist ein Trap. Mit Hilfe von Traps werden Manager über spezielle Ereignisse, Fehler oder Veränderungen von Objekten benachrichtigt, wie z.B. "verfügbarer Speicherplatz nur noch 10MB".

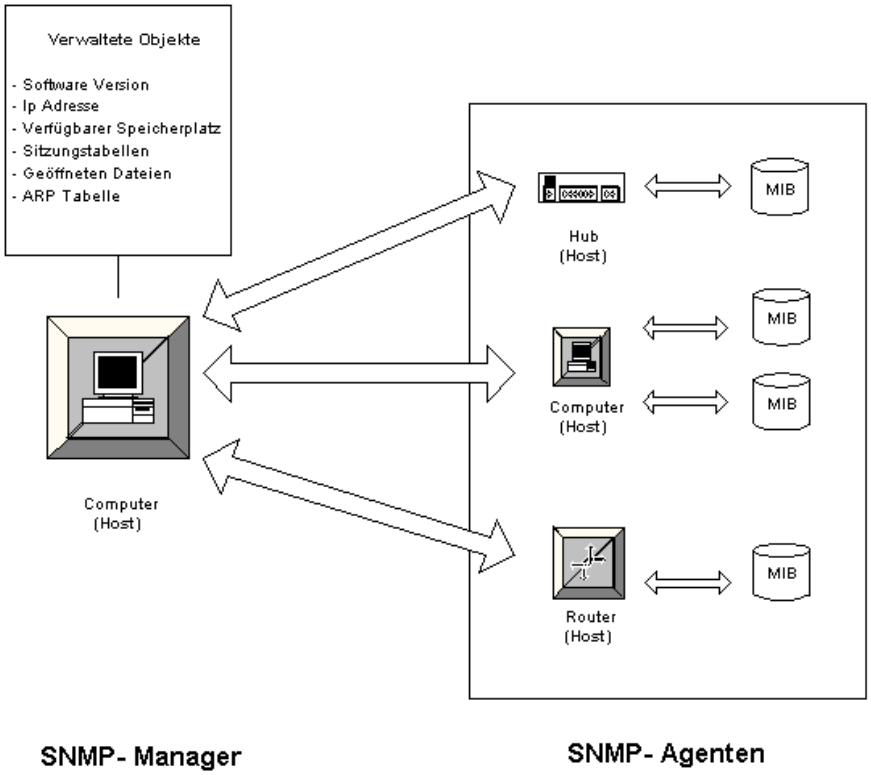

Abbildung 4.1: SNMP Begriffe

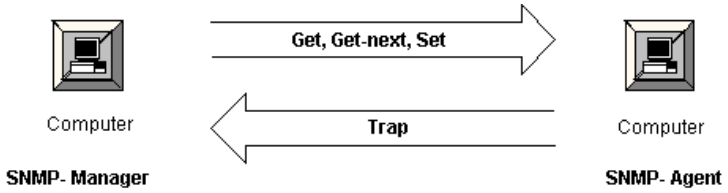

Abbildung 4.2: Funktion SNMP-Manager und Agent

4.3 Bestandteile von SNMP

4.3.1 Die Management Information Database (MIB)

Die MIB ist eine Datenbank, in der die Beschreibung der zu verwaltenden Objekte gespeichert werden. Jeder Host, der durch SNMP verwaltet wird, muß über eine MIB verfügen.

Jedes Objekt das in einer MIB verwaltet wird, wird folgendermassen definiert:

- Beziehung zwischen einem Objekt(Hardware oder Softwarekomponente eines Hosts) , Objektname und Objektbezeichner
- Beschreibung des Datentyps, durch den das Objekt definiert wird
- Beschreibung des Objekts in Textform

- Indexierungsverfahren für Objekte komplexer Dateitypen
- Lese- oder Schreibzugriff für dieses Objekt

In der Request for Comment 1213 (RFC 1213) wird die MIB-II gemäß Industriestandard definiert. Andere Hersteller wie z.B. Microsoft und Compaq haben jedoch auch die Möglichkeit Ihre Hardware und Software durch selbsterstellte MIBs zu überwachen.

4.3.2 Objektbezeichner (OID)

Jedes Objekt einer MIB wird einem eindeutigen Objektbezeichner zugewiesen. Das OID-Namenschema wird hierarchisch aufgebaut und wird wie ein auf den Kopf stehenden Baum dargestellt. So ist es Herstellern erlaubt eigene Zweige in diesem Baum einzufügen und somit Ihre Produkte mit eigenen OIDs zu verwalten. Die IETF (Internet Engineering Task Force) verwaltet das OID- Namensschema und erteilt Unternehmen das Recht ein Ast des Baumes für sich einzunehmen. Microsoft z.B. kann unter 1.3.6.1.4.1.311 ihre eigene OIDs bestimmen.

D.h., der Objektbezeichner , wird als eine hierarchische Folge von Bezeichnungen dargestellt, welche am Stamm beginnen und am Objekt enden:

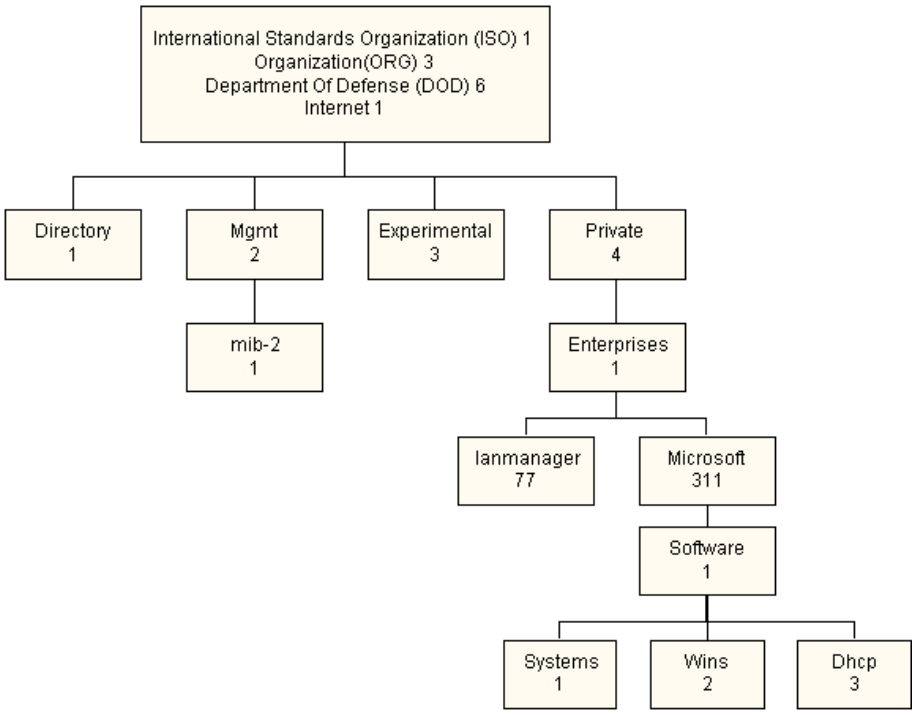

Abbildung 4.3: OID-Namensschema

Beispiel: MIB-2

Objektname Objektnummer Iso.org.dod.internet.Management.Mib2 1.3.6.1.2.1

4.3.3 Agenten

Auf jeden Host im Netzwerk, welches durch SNMP verwaltet werden soll, muß ein SNMP Agent installiert werden. Mit Hilfe einer Benutzeroberfläche werden die MIB´s verwaltet, die auf dem Host installiert sind. Hauptsächlich befindet sich ein SNMP- Agent in Wartestellung. Sobald eine Anforderung (get, getnext oder set)durch ein SNMP- Manager den Agenten erreicht, ruft dieser aus der zugehörigen MIB die Beschreibung der geforderten Daten ab. Die Anforderung wird im Falle von Windows NT an die zugehörige DLL weitergeleitet und dort der geeignete API- Aufruf durchgeführt. Die DLL gibt nun die Informationen an den Agenten zurück und dieser leitet diese Informationen an den zugehörigen Manager weiter. Die einzige Operation, die ein Agent ohne Anforderung eines Managers ausführen kann ist ein Trap. Hierdurch wird der Manager über Fehler oder Veränderungen von OIDs benachrichtigt.

4.3.4 Manager

Der Administrator, der den Manager verwaltet, sendet durch die Benutzeroberfläche eine Operation an dem Agenten und reagiert auf die erhaltenen Daten. Diese Daten werden direkt in der Benutzeroberfläche des Managers angezeigt oder für Statistiken und Auswertungen in einer Datenbank gespeichert.

4.3.5 Ports / Transportprotokoll

Bei der Standardinstallation eines Computers unter Windows werden folgende Ports für SNMP bereitgestellt:

- Port 161 - SNMP Meldungen
- Port 162 - SNMP Traps

Das benutze Transportprotokoll ist UDP.

4.3.6 SNMP Sicherheit

Die SNMP Sicherheit wird als Echtheitsbestätigungs- Dienst bezeichnet, d.h. vom Agent werden nur die SNMP- Meldungen bearbeitet, die auch Echtheitsbestätigt worden sind. Erfolgt keine Echtheitsbestätigung, dann werden die Anforderungen vom sendenden Manager nicht bearbeitet.

Diese Echtheitsbestätigung wird durch sogenannte Community-Namen abgewickelt. Damit ein SNMP Agent eine Anfrage von einem Manager bearbeiten kann, müssen beide denselben Community- Namen haben. Ist der Community- Name nicht identisch, gibt es hierbei noch die Möglichkeit den Manager einen Trap zu schicken. Im Normalfall wird die Anfrage ohne Rückmeldung fallengelassen.

Hat der Agent keinen Community Namen, so werden alle Anfragen bearbeitet, egal welchen Community-Namen der Manager hat. SNMP Agenten können gleichzeitig Mitglieder mehrerer Communities sein.

Das SNMPv3-Protokoll implementiert eine verschlüsselte Datenübertragung.

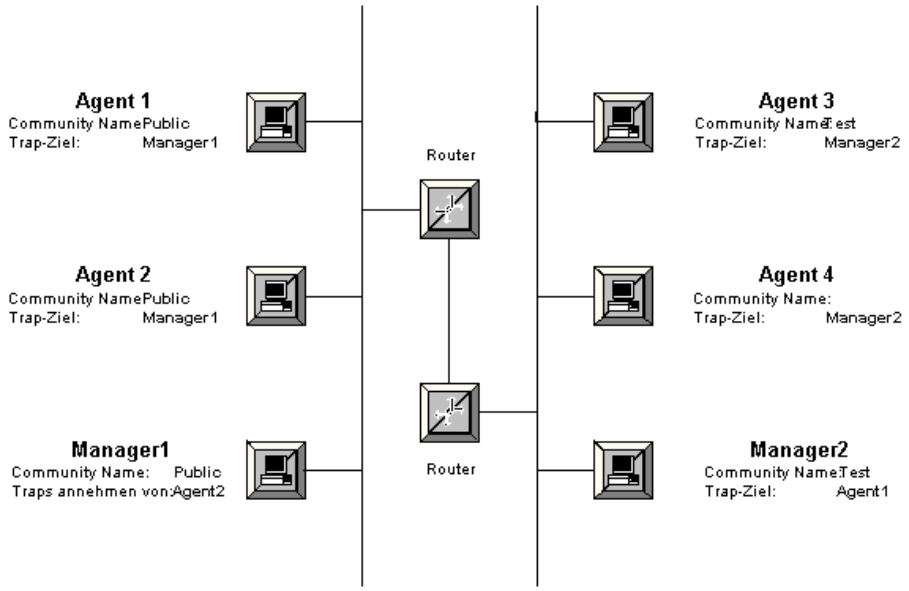

Abbildung 4.4: SNMP Netzwerk

4.4 Integration unterschiedlicher Management-Systeme

In einer heterogenen Netzwerk-Topologie arbeiten nicht nur Server eines Herstellers, sondern unterschiedliche Systeme müssen miteinander kommunizieren und verwaltet werden. Sie erzeugen durch Management-Agenten und -Systeme verschiedener Hersteller eine Vielzahl von proprietären Datensätzen.
Für ein zentrales System-Management (Single Point of Administration) stellt das auf Grund des damit verbundenen Analyse-Aufwands ein nahezu unlösbares Problem dar.

Daher bieten viele Hersteller so genannte Integrationsmodule für ein bereits vorhandenes standardisiertes Management-Framework an. Zu den wichtigsten Verwaltungsplattformen zählen derzeit HP OpenView (http://www.openview.hp.com/) , IBM Tivoli (http://www.tivoli.com/) und CA Unicenter (http://ca.com/) . Durch Integrationsmodule für diese Schaltzentralen können Funktionen wie Netzwerk- und Software-Management herstellerübergreifend genutzt werden.

Die Nutzung von Modulen zur Anpassung an ein zentrales Management-System bringt auch Nachteile. Der Administrator muss je nach vorhandener Systemumgebung verschiedene herstellerspezifische Integrationsmodule installieren und pflegen. Darüber hinaus können oft be-

sondere Zusatz-Features des Herstellers nicht genutzt werden, da sie nicht in das vorhandene Management-System integrierbar sind.

Kapitel 5

Systematische Fehlersuche

Netzwerkadministrationsaufgaben fallen in zwei sehr unterschiedliche Kategorien: Konfiguration und Fehlerbehebung. Konfiguartionsaufgaben bereiten auf das Erwartete vor. Sie erfordern detailliertes Wissen, sind normalerweise aber einfach auszuführen und berechenbar. Wenn ein System einmal richtig konfiguriert ist, gibt es kaum einen Grund diese Konfiguration wieder zu ändern. Der Konfigurationsprozess wird jedes mal, mit jedoch nur kleinen Änderungen, durchlaufen, wenn Patches oder Updates installiert werden.

Fehlerbehebung im Netzwerk dagegen, muss mit dem Unerwarteten umgehen. Häufig braucht diese Arbeit mehr konzeptuelles, als detailliertes Wissen. Netzwerkprobleme sind normalerweise, durch die Kombination von Topologie, Konfiguration und verschiedenen Komponenten einzigartig und manchmal auch schwierig zu lösen. Fehlerbehebung ist jedoch ein wichtiger Teil, um ein stabiles, zuverlässiges Netzwerk betreiben zu können. In diesem Kapitel werden einige Tools zur Überprüfung eines TCP/IP Netzwerks vorgestellt. Diese Tools sind jedoch nur effektiv, wenn sie auch richtig eingesetzt werden. Dazu ist eine systematische Vorgehensweise und ein grundlegendes Verständnis der Funktion eines Netzwerks erforderlich.

5.1 Vorgehensweise

Nicht alle Probleme in einem TCP/IP-Netzwerk gleichen sich und ebenso können nicht alle Probleme gleich angegangen werden. Der Schlüssel zur Lösung eines Problems ist das Verstehen was das Problem überhaupt ist. Dies ist nicht ganz so einfach wie es auf den ersten Blick aussieht. Das oberflächliche Problem ist manchmal irreführend und das echte Problem versteckt durch mehrere Schichten von Software. Häufig ist, wenn das richtige Problem einmal gefunden ist, die Lösung offensichtlich und einfach.

Grundsätzlich gibt es zur systematischen Fehlersuche in Netzwerken zwei Vorgehensweisen:

1. Der Auschluss fehlerloser Teilsysteme
2. Das Absuchen der OSI-Schichten

Die zwei Methoden werden häufig in der obgenannten Reihenfolge kombiniert. Der Ausschluss fehlerloser Teilsysteme erlaubt die örtliche Eingrenzung des Fehlers und reduziert so die Anzahl der möglichen Komponenten und eventuell auch Diensten. Das systematische Durchgehen der einzelnen Schichten des OSI-Modells ermöglicht es das betroffene Protokoll zu eruieren. Daraus können wiederum Rückschlüsse auf mögliche, den Fehler verursachende Komponenten und Software gezogen werden.

5.1.1 Erfassen des Fehlers

Wenn ein Fehler auftritt wird er als erstes erfasst. Finden Sie an diesem Punkt möglichst exakt heraus was passiert und notieren Sie die Angaben. In grösseren Betrieben sollten Formulare (auch in elektronischer Form), oder Software zur Unterstützung der Helpdesk vorhanden sein. Auch hier kann eine gute Dokumentation sehr hilfreich sein. Mögliche Fragen welche man stellen kann:

- Welche Applikation funktioniert nicht ?
- Welches ist der betroffene Remote-Hostname und dessen IP ?
- Welches sind Hostname und IP des Benutzers ?
- Welche Fehlermeldung wurde angezeigt ?
- Wie häufig taucht der Fehler auf ?

Wenn ein Benutzer anruft, überprüfen Sie falls möglich das Problem, indem Sie ihn durch den Vorgang führen. Ebenso sollten Sie versuchen das Problem auf dem eigenen System zu reproduzieren.

5.1.2 Testen

Durch das Testen vom System des Benutzers und anderen Systemen kann folgendes herausgefunden werden:

- Tritt das Problem in anderen Applikationen auf der Maschine des Users auf, oder ist es nur eine Applikation welche nicht funktioniert ? Wenn nur eine Applikation involviert ist, ist es möglich dass sie falsch konfiguriert ist oder auf dem Server nicht läuft. Aus Sicherheitsgründen sind auf vielen Systemen diverse Dienste nicht aktiviert.
- Tritt das Problem nur mit einem, allen, oder nur einer bestimmten "Gruppe" von remote Rechnern auf ? Wenn nur ein remote Rechner betroffen ist, so könnte das Problem sehr wohl bei diesem Server liegen. Falls alle übers Netzwerk erreichbaren Rechner betroffen sind, liegt das Problem sehr wahrscheinlich am System des Benutzers.(Speziell, wenn niemand anderes das selbe Problem hat.) Wenn nur Rechner eines bestimmten Subnetzes oder externer Netze betroffen sind, könnte das Problem im Zusammenhang mit Routing stehen.
- Tritt das Problem auf anderen lokalen Systemen auf ? Es sollten unbedingt andere Systeme im gleichen Subnetz überprüft werden. Falls das Problem nur auf dem Rech-

ner des betroffenen Benutzers auftritt, kann man sich auf dieses System konzentrieren. Andernfalls liegt das Problem eher beim Routing im Subnetz.

Nachdem die Symptome des Fehlers bekannt sind, kann überlegt werden, auf welcher Schicht des OSI-Modells Probleme auftreten.

5.2 Werkzeuge für die Fehlersuche

Für die Fehlersuche sind auf dem Markt eine grosse Zahl von Diagnosewerkzeugen vorhanden, vom mitgelieferten Betriebssystem-Utility über kostenlose und kommerzielle Paketanalyse-Software bis hin zu professionellen, Hardware-basierten Diagnoselösungen.

Nebst Software ist jedoch für die Fehlersuche häufig auch gewisse Hardware, wie Kabeltester und Testnotebook nötig. Wir beschränken uns im folgenden auf frei verfügbare oder im Betriebssystem mitgelieferte Tools, welche zahlreiche grundlegende Arbeiten bei der LAN-Diagnose und dem Troubleshooting im Netzwerk durchführen lassen. Um komplexen Problemen auf der Protokollebene auf die Spur zu kommen, reichen die Bordmittel des Betriebssystems allerdings meist nicht mehr aus. Dann gilt es, schwerere Geschütze, sprich: professionelle Paketanalyse-Software, aufzufahren. Dabei besteht auch hier die Wahl zwischen Freeware-Tools, kommerziellen Software-Lösungen und hochgezüchteten Hardware-Analyzern.

5.2.1 LAN-Analyse mit Windows

Um Problemen im Netzwerk auf die Spur zu kommen, hat Microsoft seinen Betriebssystemen eine ganze Reihe Kommandozeilentools mit auf den Weg gegeben. Diese werden zum Teil beim Standard- Setup mitinstalliert, zum Teil sind sie separat aufzuspielen.

ping

Ein ebenso einfaches wie wirkungsvolles Tool ist der Befehl ping. Mit ihm können Sie schnell feststellen, ob die TCP/IP-Verbindungen in Ihrem Netz funktionieren. Ein Ping auf die Loopback-Adresse 127.0.0.1 überprüft, ob TCP/IP auf dem lokalen Rechner korrekt installiert ist. Wenn Sie den Computer anschließend mit seiner eigenen IP-Adresse anpingen, sehen Sie auch gleich, ob die Netzwerkkarte vorschriftsmäßig arbeitet.

Beispielausgabe:

```
E:\>ping www.google.ch

Ping www.google.akadns.net [66.102.9.104] mit 32 Bytes Daten:

Antwort von 66.102.9.104: Bytes=32 Zeit=64ms TTL=240
Antwort von 66.102.9.104: Bytes=32 Zeit=64ms TTL=240
Antwort von 66.102.9.104: Bytes=32 Zeit=63ms TTL=240
Antwort von 66.102.9.104: Bytes=32 Zeit=76ms TTL=240
```

```
Ping-Statistik für 66.102.9.104:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 63ms, Maximum = 76ms, Mittelwert = 66ms
```

Antworten das Gateway und die anderen Subnetzstationen ohne größere Verzögerung, sollte auf dieser Ebene ebenfalls alles in Ordnung sein. Mit dem Ping-Befehl können Sie zudem schnell herausfinden, ob es Probleme mit der Namensauflösung gibt: Funktioniert der Ping auf die IP-Adresse eines Rechners, der Ping auf seinen Host-Namen aber nicht, ist sehr wahrscheinlich die Namensauflösung fehlerhaft.

Zeigen die von Ihnen durchgeführten Pings Paketverluste im LAN oder liegen die Antwortzeiten dauerhaft im zweistelligen Millisekundenbereich, dürfte ein Hardware- Fehler an einem Kabel, einer Netzwerkkarte oder einem Switch vorliegen.

route

Der Befehl route print zeigt die IP-Routing-Tabelle des jeweiligen Hosts an. Sie können sie mit Hilfe von route add und route delete verändern. Die Option -p speichert neue Routen dauerhaft, -f löscht alle Gateway-Einträge aus der Tabelle. Vorhandene Routen verändern Sie mit change.

Beispielausgabe:

```
E:\>route print
===========================================================================
Schnittstellenliste
0x1 ........................... MS TCP Loopback interface
0x2 ...00 0d 60 78 29 31 ...... Intel(R) PRO/1000 MT Mobile Connection -
Paketplaner-Miniport
===========================================================================
===========================================================================
Aktive Routen:
     Netzwerkziel    Netzwerkmaske          Gateway   Schnittstelle  Anzahl
          0.0.0.0          0.0.0.0      192.168.0.1     192.168.0.2      20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      192.168.0.0    255.255.255.0      192.168.0.2     192.168.0.2      20
      192.168.0.2  255.255.255.255        127.0.0.1       127.0.0.1      20
    192.168.0.255  255.255.255.255      192.168.0.2     192.168.0.2      20
        224.0.0.0        240.0.0.0      192.168.0.2     192.168.0.2      20
  255.255.255.255  255.255.255.255      192.168.0.2     192.168.0.2       1
Standardgateway:       192.168.0.1
===========================================================================
Ständige Routen:
  Keine
```

tracert

Mit tracert erhalten Sie eine Liste aller Router, die auf dem Weg zwischen Ihrem Computer und der angegebenen Zieladresse liegen. Dabei werden allerdings nur die Router gelistet, die Pakete mit abgelaufenen TTL-Werten nicht verwerfen. Zudem funktioniert tracert nur, wenn auf den beteiligten Routern und Firewalls die ICMP-Filter deaktiviert sind.

Beispielausgabe:

```
E:\>tracert www.google.ch

Routenverfolgung zu www.google.akadns.net [66.102.9.104]  über maximal 30
Abschnitte:

  1    13 ms    38 ms    16 ms  10.225.64.1
  2    37 ms    41 ms    12 ms  gig-10-0.blxOTF001.bb.cablecom.net
   [62.2.10.21]
  3    11 ms    37 ms    11 ms  gig-6-1-2.blxZHZ002.bb.cablecom.net
   [62.2.4.205]
  4    41 ms    44 ms    41 ms  195.66.224.185
  5    36 ms    71 ms    33 ms  p14-0.core01.lon02.atlas.cogentco.com
   [130.117.1.101]
  6    36 ms    33 ms    34 ms  p4-0.core01.bru01.atlas.cogentco.com
   [130.117.1.157]
  7    53 ms    38 ms    59 ms  p6-0.core01.ams03.atlas.cogentco.com
   [130.117.1.133]
  8    34 ms    51 ms    63 ms  p5-0.core01.dus01.atlas.cogentco.com
   [130.117.1.126]
  9    38 ms    84 ms    44 ms  p14-0.core01.fra03.atlas.cogentco.com
   [130.117.1.130]
 10    56 ms    53 ms    64 ms  217.71.111.38
 11    81 ms    77 ms    86 ms  64.233.175.249
 12    96 ms    96 ms    66 ms  216.239.49.9
 13    99 ms     *       63 ms  64.233.175.185
 14    90 ms    76 ms   127 ms  64.233.174.18
 15    67 ms    76 ms    93 ms  66.102.9.104

Ablaufverfolgung beendet.
```

pathping

Das interessante Route-Tracing-Tool pathping kombiniert quasi die Funktionen von ping und tracert miteinander und liefert dazu zusätzliche Informationen. Das Tool schickt über einen definierten Zeitraum hinweg Testpakete zu jedem Router, der auf dem Weg zu der angegebenen Endstation liegt. Diese Pakete werden vom jeweiligen Router wieder zurückgeschickt, wodurch pathping feststellen kann, an welcher Stelle im Übertragungspfad Pakete verloren gegangen sind. Damit ist es zum Beispiel möglich, einen überlasteten Router zu erkennen.

```
E:\WINDOWS\System32\cmd.exe

E:\>pathping www.google.ch

Routenverfolgung zu www.google.akadns.net [66.102.9.104]
über maximal 30 Abschnitte:
  0  xan-yae.bbbaden.ch [192.168.0.2]
  1  10.225.64.1
  2  gig-10-0.blxOTF001.bb.cablecom.net [62.2.10.21]
  3  gig-6-1-2.blxZHZ002.bb.cablecom.net [62.2.4.205]
  4  195.66.224.185
  5  p14-0.core01.lon02.atlas.cogentco.com [130.117.1.101]
  6  p4-0.core01.bru01.atlas.cogentco.com [130.117.1.157]
  7  p6-0.core01.ams03.atlas.cogentco.com [130.117.1.133]
  8  p5-0.core01.dus01.atlas.cogentco.com [130.117.1.126]
  9  p14-0.core01.fra03.atlas.cogentco.com [130.117.1.130]
 10  217.71.111.38
 11  64.233.175.249
 12  216.239.49.9
 13  64.233.175.185
 14  216.239.46.173
 15  66.102.9.104

Berechnung der Statistiken dauert ca. 375 Sekunden...
            Quelle zum Abs.  Knoten/Verbindung
Abs. Zeit   Verl./Ges.=   %  Verl./Ges.=   %  Adresse
  0                                           xan-yae.bbbaden.ch [192.168.0.2]
                                 1/ 100 =  1%   |
  1   25ms     1/ 100 =  1%      0/ 100 =  0%  10.225.64.1
                                 0/ 100 =  0%   |
  2   27ms     1/ 100 =  1%      0/ 100 =  0%  gig-10-0.blxOTF001.bb.cablecom.net
 [62.2.10.21]
                                 0/ 100 =  0%   |
  3   26ms     1/ 100 =  1%      0/ 100 =  0%  gig-6-1-2.blxZHZ002.bb.cablecom.ne
t [62.2.4.205]
                                 0/ 100 =  0%   |
  4   47ms     2/ 100 =  2%      1/ 100 =  1%  195.66.224.185
                                 0/ 100 =  0%   |
  5   50ms     1/ 100 =  1%      0/ 100 =  0%  p14-0.core01.lon02.atlas.cogentco.
com [130.117.1.101]
                                 0/ 100 =  0%   |
  6   49ms     2/ 100 =  2%      1/ 100 =  1%  p4-0.core01.bru01.atlas.cogentco.c
om [130.117.1.157]
                                 0/ 100 =  0%   |
  7   52ms     1/ 100 =  1%      0/ 100 =  0%  p6-0.core01.ams03.atlas.cogentco.c
om [130.117.1.133]
                                 0/ 100 =  0%   |
  8   49ms     1/ 100 =  1%      0/ 100 =  0%  p5-0.core01.dus01.atlas.cogentco.c
om [130.117.1.126]
                                 0/ 100 =  0%   |
  9   48ms     1/ 100 =  1%      0/ 100 =  0%  p14-0.core01.fra03.atlas.cogentco.
com [130.117.1.130]
                                48/ 100 = 48%   |
 10  ---     100/ 100 =100%    51/ 100 = 51%  217.71.111.38
                                 0/ 100 =  0%   |
 11  ---     100/ 100 =100%    51/ 100 = 51%  64.233.175.249
                                 0/ 100 =  0%   |
 12  ---     100/ 100 =100%    51/ 100 = 51%  216.239.49.9
                                 0/ 100 =  0%   |
 13  ---     100/ 100 =100%    51/ 100 = 51%  64.233.175.185
                                 0/ 100 =  0%   |
 14  ---     100/ 100 =100%    51/ 100 = 51%  216.239.46.173
                                 0/ 100 =  0%   |
 15   80ms    49/ 100 = 49%     0/ 100 =  0%  66.102.9.104

Ablaufverfolgung beendet.

E:\>
```

Abbildung 5.1: Beispielausgabe von pathping

arp

Um Fehler bei der Namensauflösung zwischen MAC- und IP-Adressen aufzuspüren, ist der Befehl arp hilfreich. Er zeigt die Einträge des arp-Cache an und ermöglicht es Ihnen, sie anzupassen. Mit arp -a erhalten Sie die MAC-Adressen der zuletzt angesprochenen Netzwerkressourcen. Die eigene MAC-Adresse lässt sich über getmac oder durch Eingabe von ipconfig /all feststellen.

Beispielausgabe:

```
E:\>arp -a
```

```
Schnittstelle: 192.168.0.2 --- 0x2
  Internetadresse       Physikal. Adresse     Typ
  192.168.0.1           00-09-5b-cc-3e-00     dynamisch
```

ipconfig

Das Tool ipconfig bietet neben der Ausgabe der Netzwerkkonfigurations-Parameter einige weitere nützliche Optionen, um Netzprobleme zu beseitigen: /flushdns löscht den DNS-Namens-Cache; /registerdns erneuert alle DHCP-Leases und registriert die DNS-Namen neu; /displaydns zeigt alle Einträge an, die im DNS-Resolver-Cache vorhanden sind.

Beispielausgabe:

```
E:\>ipconfig -all

Windows-IP-Konfiguration

        Hostname. . . . . . . . . . . . : xan-yae
        Primäres DNS-Suffix . . . . . . . : bbbaden.ch
        Knotentyp . . . . . . . . . . . . : Hybrid
        IP-Routing aktiviert. . . . . . . : Nein
        WINS-Proxy aktiviert. . . . . . . : Nein
        DNS-Suffixsuchliste . . . . . . . : bbbaden.ch

Ethernetadapter LAN-Verbindung:

        Verbindungsspezifisches DNS-Suffix:
        Beschreibung. . . . . . . . . . . : Intel(R) PRO/1000 MT
Mobile Connection
        Physikalische Adresse . . . . . . : 00-0D-60-78-29-31
        DHCP aktiviert. . . . . . . . . . : Ja
        Autokonfiguration aktiviert . . . : Ja
        IP-Adresse. . . . . . . . . . . . : 192.168.0.2
        Subnetzmaske. . . . . . . . . . . : 255.255.255.0
        Standardgateway . . . . . . . . . : 192.168.0.1
        DHCP-Server . . . . . . . . . . . : 192.168.0.1
        DNS-Server. . . . . . . . . . . . : 62.2.17.61
                                            62.2.24.158
                                            62.2.17.60
        Lease erhalten. . . . . . . . . . : Freitag, 8. Oktober 2004 22:03:16
        Lease läuft ab. . . . . . . . . . : Montag, 11. Oktober 2004 22:03:16
```

netdiag

Wenn ein von Ihnen betreuter Computer Netzwerkprobleme hat, sollten Sie als Erstes netdiag einsetzen. Dieses Tool benötigt keine zusätzlichen Parameter. Es führt automatisch

verschiedene Verbindungstests durch, markiert die Problembereiche und kann mit der Option /fix sogar einfache DNS-Probleme beheben. Das Netzwerkdiagnosetool lässt sich auch direkt von der Kommandozeile aus bedienen. Der Befehl hierfür lautet netsh -c diag. Daraufhin erscheint ein Prompt, an dem Sie die gewünschten Diagnosebefehle eingeben. Dabei greift netdiag auf andere Werkzeuge wie ipconfig oder netstat zurück, untersucht DLL-Dateien und prüft die Registry. Die Ergebnisse von netdiag liefern Hinweise, um die Ursache von Netzwerkproblemen herauszufinden.

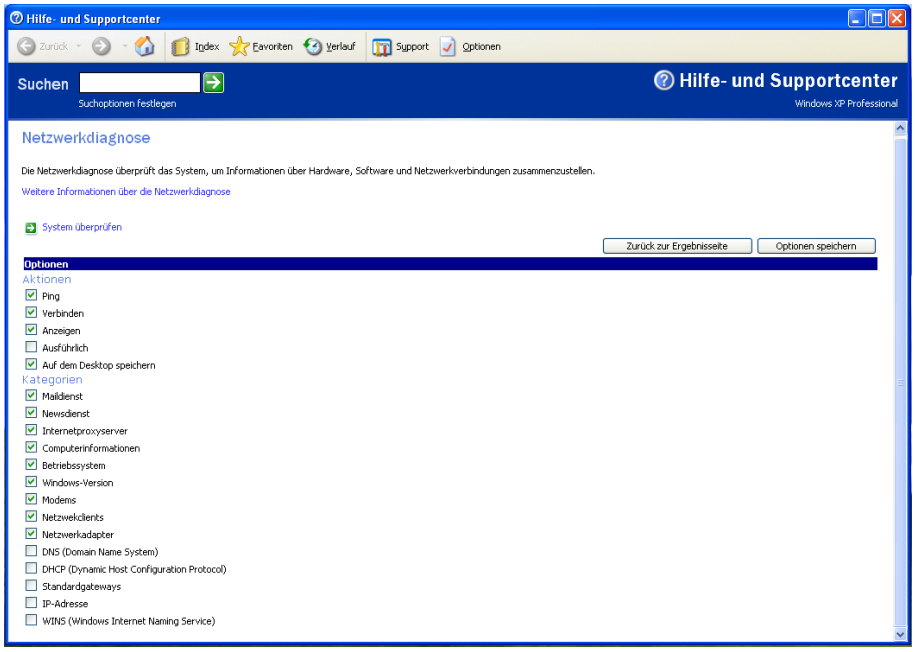

Abbildung 5.2: Analyse mittels netdiag

netstat

Das Tool netstat liefert Protokollstatistiken und listet die aktuellen TCP/IP-Verbindungen. netstat -a zeigt alle Verbindungen und die dazugehörigen Ports an. Den Inhalt der Routing-Tabelle erhalten Sie mit netstat -r, die Protokollstatistiken mit netstat -s.

nslookup

Für das Troubleshooting von DNS-Problemen, zum Beispiel bei der Namensauflösung von Hosts, ist nslookup das richtige Werkzeug. Es liefert unter anderem die zum jeweiligen Host gehörige IP-Adresse. Um die DNS-Konfiguration zu überprüfen, stehen zahlreiche weitere Befehlsoptionen zur Verfügung. Den Debug-Modus aktivieren Sie durch set debug oder durch set d2, womit Sie eine noch detailliertere Analyse erhalten.

Beispielausgabe:

```
E:\>nslookup www.google.ch
```

```
E:\WINDOWS\System32\cmd.exe

E:\>netstat -aes
Schnittstellenstatistik

                           Empfangen           Gesendet

Bytes                        961663           266701
Unicastpakete                  2349             2358
Nicht-Unicastpakete             114              115
Verworfen                         0                0
Fehler                            0                0
Unbekannte Protok.                0

IPv4-Statistik

  Empfangene Pakete                      = 2448
  Empfangene Vorspannfehler              = 0
  Empfangene Adressfehler                = 7
  Weitergeleitete Datagramme             = 0
  Empfangene unbekannte Protokolle       = 0
  Empfangene verworfene Pakete           = 114
  Empfangene übermittelte Pakete         = 2334
  Ausgabeanforderungen                   = 2466
  Verworfene Routingpakete               = 0
  Verworfene Ausgabepakete               = 0
  Ausgabepakete ohne Routing             = 0
  Reassemblierung erforderlich           = 0
  Reassemblierung erfolgreich            = 0
  Reassemblierung erfolglos              = 0
  Erfolgreiche Datagrammfragmentierung   = 0
  Erfolglose Datagrammfragmentierung     = 0
  Erzeugte Fragmente                     = 0

ICMPv4-Statistik

                             Empfangen Gesendet
  Meldungen                  44        51
  Fehler                     0         0
  Ziel nicht erreichbar      2         4
  Zeitüberschreitung         36        0
  Parameterprobleme          0         0
  Quelldrosselung            0         0
  Umleitungen                0         0
  Echos                      0         47
  Echoantworten              6         0
  Zeiteinträge               0         0
  Zeiteintragantworten       0         0
  Adressmasken               0         0
  Adressmaskenantworten      0         0

TCP-Statistik für IPv4

  Aktiv geöffnet                       = 200
  Passiv geöffnet                      = 0
  Erfolglose Verbindungsversuche       = 0
  Zurückgesetzte Verbindungen          = 47
  Aktuelle Verbindungen                = 0
  Empfangene Segmente                  = 1424
  Gesendete Segmente                   = 1453
  Erneut übertragene Segmente          = 3

UDP-Statistik für IPv4

  Empfangene Datagramme = 861
  Keine Anschlüsse      = 49
  Empfangsfehler        = 0
  Gesendete Datagramme  = 955

E:\>_
```

Abbildung 5.3: Analyse mittels netstat

```
Server:  ns11.cablecom.net
Address:  62.2.17.61

Nicht autorisierte Antwort:
Name:    www.google.akadns.net
Addresses:  66.102.9.99, 66.102.9.104
Aliases:  www.google.ch, www.google.com
```

nbtstat

Das Werkzeug nbtstat dagegen eignet sich für das Troubleshooting bei Problemen mit der Auflösung von NetBIOS-Namen in IP-Adressen. Mit diesem Tool können Sie fehlerhafte Einträge entfernen oder korrigieren. nbtstat -c zeigt das im Namens-Cache gespeicherte Mapping von NetBIOSNamen zu IP-Adressen. nbtstat -R entleert den Namens-Cache und lädt alle #PRE-Einträge aus der LMHOSTS-Datei neu.

5.2.2 Netzwerkanalyse mit Windows XP

Windows XP bringt für die Diagnose von Netzwerkverbindungen gleich mehrere neue Werkzeuge mit. Hierzu zählen eine einfach zu bedienende grafisch aufbereitete HTML-Oberfläche sowie neue Analysetools. Sie basieren auf dem Framework der Windows Management Instrumentation (WMI). Um die Weboberfläche für die Netzwerkdiagnose zu starten, rufen Sie über Start die Webseite Hilfe und Support auf. Hier klicken Sie auf Beheben eines Problems , anschließend auf Netzwerkproblem und dann auf Diagnostizieren von Netzwerkverbindungen . Damit sind Sie auf der Netzwerkdiagnoseseite angekommen und können hier die Überprüfungsoptionen festlegen und den Systemcheck starten. Dieses Tool stellt System- und Adapterinformationen bereit und führt verschiedene Ping- und Verbindungstests sowie zahlreiche weitere Diagnoseschritte aus. Um die Weboberfläche von der Kommandozeile aus zu starten, geben Sie in einem DOS-Fenster netsh diag gui ein. Alternativ können Sie auch über Start/ Ausführen die folgende Syntax verwenden: hcp://system/netdiag/dglogs.htm. Das Netzwerkdiagnosetool lässt sich auch direkt von der Kommandozeile aus bedienen. Der Befehl hierfür lautet netsh -c diag. Daraufhin erscheint ein Prompt, an dem Sie die gewünschten Diagnosebefehle eingeben. Diese Funktionen stehen auch mit Windows Server 2003 zur Verfügung.

Verbindungsstatus und Reparaturfunktion

Eine weitere Neuerung von Windows XP und 2003 ist die Ergänzung der Netzwerkverbindungsanzeige um Statusinformationen. Damit können Sie die aktuelle Konfiguration der Netzwerkparameter schnell überprüfen. Hier finden Sie auch die Reparaturfunktion für LAN-Verbindungen, die eine Reihe von Einstellungen überprüft und bei Bedarf automatisch korrigiert. Im Einzelnen führt dieses Tool folgende Schritte durch:

- Broadcast DHCP Lease Renew
- Flush ARP Cache
- nbtstat -R
- nbtstat -RR
- Flush DNS Cache
- Register DNS Name

Damit können Anwender versehentliche Fehlkonfigurationen per Mausklick wieder korrigieren. Die Reparaturfunktion lässt sich auch über das Netzwerkverbindungssymbol per rechter Maustaste starten.

Task-Manager

Den Task-Manager von Windows XP und Windows Server 2003 hat Microsoft um eine ganze Reihe von Netzwerkdiagnose-Funktionen erweitert.

Er verfügt jetzt über einen eigenen Reiter für die Netzwerküberwachung und listet alle installierten Netzwerkadapter. Endanwender können damit sehr schnell feststellen, ob eine überlastete Netzwerkverbindung für zu lange Antwortzeiten verantwortlich ist. Über den Menüeintrag Ansicht/Spalten auswählen definieren Sie, welche Parameter der Task-Manager im unteren Tabellenfenster anzeigt.

Systemmonitor

Von Windows 2000 bekannt ist der Systemmonitor, der bei Windows XP und Windows Server 2003 im Menü Verwaltung nun auf den Namen Leistung hört. Über Start/Ausführen rufen Sie das Tool durch Eingabe von perfmon auf. Im Systemmonitor können Sie per rechter Maustaste oder durch einen Klick auf den Menü-Button Hinzufügen gezielt auswählen, welche System- und TCP/IPNetzwerkparameter das Tool überwacht und aufzeichnet. Hier definieren Sie auch die Einstellungen für das Logging sowie die Alarmierungsfunktionen, die für die Netzüberwachung und die Fehlersuche eine wichtige Hilfe sind.

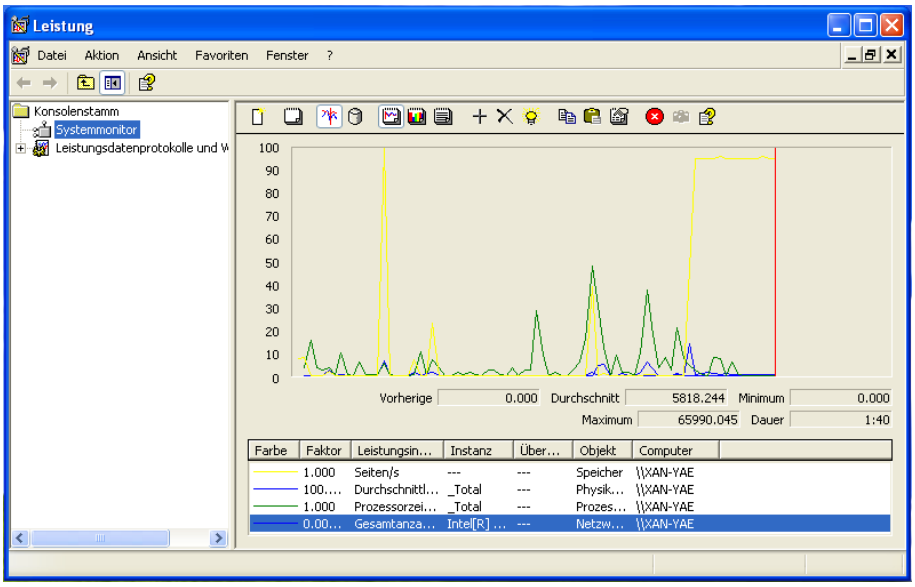

Abbildung 5.4: Analyse des lokalen Netzwerktraffics mit dem Systemmonitor

Diagnose mit dem Systemmonitor Der Systemmonitor ist ein mächtiges Werkzeug, mit dem Sie Fehlfunktionen auf die Spur kommen. So kann ein starker Anstieg der vom Arbeitsspeicher pro Sekunde verarbeiteten Seiten bei gleichzeitigem Rückgang der insgesamt verarbeiteten Bytes darauf hinweisen, dass der Computer zu wenig physikalischen Speicher für das Ausführen von Netzwerkaufgaben zur Verfügung hat. Viele Netzwerkkomponenten, wie zum Beispiel NICs oder Protokoll-Software, verwenden Nonpaged Memory. Verarbeitet ein Server sehr viele Seiten pro Sekunde, kann dies darauf zurückzuführen sein, dass der größte Teil seines Speichers von Netzwerkressourcen belegt ist und für andere Aufgaben nur noch sehr wenig physikalischer Speicher zur Verfügung steht. Auch zur Performance-Überwachung des Systems bieten Windows XP und Windows Server 2003 zwei neue Tools an. pmon.exe listet in einem DOS-Fenster die derzeitige CPU- und Speichertätigkeit und aktualisiert die Daten fortlaufend. pviewer.exe zeigt die laufenden Prozesse sowie die Arbeitsspeicherbelastung an. Wie beim Task-Manager können Sie einzelne Prozesse gezielt beenden.

Netzwerkmonitor

Windows XP und Windows Server 2003 verfügen ebenfalls über den von Windows 2000 bekannten Netzwerkmonitor für die LAN-Analyse. Falls Sie ihn nicht schon beim Betriebssystem-Setup installiert haben, richten Sie ihn über Systemsteuerung/Software/Windows-Komponenten hinzufügen ein. Sie finden den Netzwerkmonitor unter dem Eintrag Verwaltungs- und Überwachungsprogramme. Für die Installation benötigen Sie die Betriebssystem-CD. Falls Sie zusätzlich eine Netzüberwachung per SNMP-Konsole planen, können Sie hier auch gleich den SNMP-Agenten auswählen. Anschließend müssen Sie noch den Netzwerkkartentreiber für den Netzwerkmonitor installieren. Wechseln Sie hierfür zu den Eigenschaften der Netzwerkverbindung , wählen Sie die Schaltfläche Installieren und unter Protokolle den Treiber für den Netzwerkmonitor.

Diagnose mit dem Netzwerkmonitor Der Netzwerkmonitor kann Daten auf verschiedenen Layern aufzeichnen. Er erfasst die von der Netzwerkkarte auf Layer 2 übertragenen Frames ebenso wie TCP/IP-Pakete auf Layer 3 und 4 (TCP/IP, UDP, ICMP). Für die Analyse der Kommunikation auf der Anwendungsschicht verfügt das Tool unter anderem über Zähler für die Redirector-Objekte. Diese zeichnen die vom Workstation- und Server-Service übertragenen Anfragen auf. Die Datensammlung für die Paketanalyse starten Sie über das Hauptmenü mit Sammeln/Starten . Beim Beenden können Sie sich die erfassten Daten gleich anzeigen lassen oder sie in einer Trace-Datei speichern. Die Funktion Sammeln/ Filter ermöglicht es Ihnen, Daten gezielt mitzuschneiden, zum Beispiel nur die Pakete einer Kommunikation zwischen zwei bestimmten Stationen. Sie können Filter zudem für die Protokollart oder für spezielle Datenmuster setzen. Mit Display-Filtern wählen Sie aus bereits erfassten Daten genau diejenigen Pakete oder Frames aus, die Sie besonders interessieren. Eine Übersicht über die Protokolle, die Sie mit dem Netzwerkmonitor analysieren können, finden Sie auf der Microsoft-Technet-Webseite (http://www.micro soft.com/technet/). Bei dem von Microsoft mit Windows 2000, XP und Windows Server 2003 mitgelieferten Netzwerkmonitor handelt es sich um eine eingeschränkte Version, die nur den Datenverkehr auf der lokalen Station auswerten kann. Um ein gesamtes Netzwerk über mehrere Segmente hinweg zu überwachen und zu analysieren, benötigen Sie die Vollversion, die im Systems Management Server von

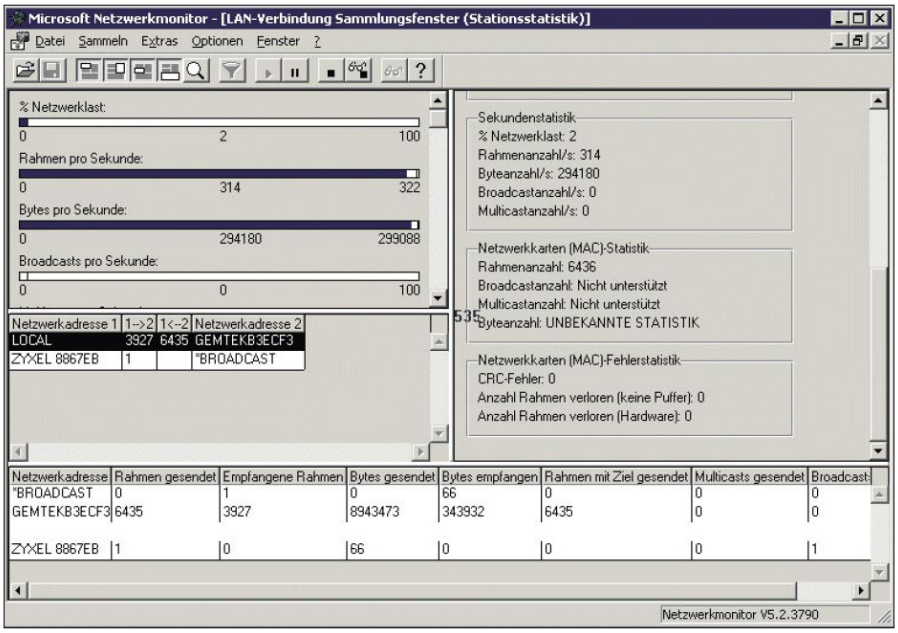

Abbildung 5.5: Analyse des lokalen Netzwerktraffics mit dem Netzwerkmonitor

Microsoft enthalten ist.

Auswertung von Trace-Dateien

Für die Auswertung von Trace-Dateien hat Microsoft Windows XP und Windows Server 2003 ein neues Tool spendiert: tracerpt kann unter anderem eine CSVDatei mit einer Berichtzusammenfassung erstellen sowie eine TXT-Berichtdatei. Die entsprechenden Befehlsoptionen lauten -summary [Dateiname] beziehungsweise -report [Dateiname]. Bei dem von Microsoft mit Windows 2000, XP und Windows Server 2003 mitgelieferten Netzwerkmonitor handelt

5.2.3 Unix/Linux-Tools

Die im folgenden genannten Tools sind in jeder Unix/Linux-Distribution zu finden und sind ausführlich in der RFC 1470 [7]und deren NOC-Tools Liste [8] beschrieben. Obschon diese RFC aus dem Jahr 1993 datiert und die aktualisierte NOC-Tools Liste aus dem 1998 sind dort nach wie vor nützliche Ressourcen zu finden.

ifconfig bietet Informationen zur Konfiguration der Netzwerkinterfaces. Nützlich um falsche IP-Adressen, Subnetzmasken und Broadcast-Adressen festzustellen. Das passende Windows-Tool heisst ipconfig 5.2.1

arp bietet Informationen zur Ethernet/IP-Übersetzung. Nützlich um falsch konfigurierte IP-Adressen in einem LAN festzustellen. Das passende Windows-Tool heisst ebenfalls arp 5.2.1

netstat bietet eine Vielzahl von Informationen zu Netzwerk-Sockets, Routing-Tabellen und detaillierte Statistiken von jedem Netzwerkinterface. Das passende Windows-Tool heisst ebenfalls netstat 5.2.1

ping zeigt an ob ein entfernter Rechner erreicht werden kann, liefert aber auch Informationen über Paketverluste und Zustellungszeiten. Das passende Windows-Tool heisst ebenfalls ping 5.2.1

nslookup bietet Informationen zur Namensauflösung. Das passende Windows-Tool heisst ebenfalls nslookup 5.2.1

dig bietet wie nslookup Informationen zur Namensauflösung.

traceroute verfolgt die Route welche ein Paket auf dem Weg zum Zielrechner nimmt und zeigt alle Zwischenziele an. Das passende Windows-Tool heisst tracert 5.2.1

route zeigt und ändert die Routingtabelle. Das passende Windows-Tool heisst ebenfalls route **??**

tcpdump ist ein TCP/IP Protokoll-Analyzer und untersucht Header und Inhalt von Paketen auf dem Netzwerk. Dieses Tool ist sehr nützlich falls Probleme mit einem bestimmten Protokoll auftreten.

Obschon einige Tools vom Namen und der Funktion denjenigen unter Windows gleichen, können sie sich dennoch in möglichen Optionen und Details unterscheiden.

Kapitel 6

WAN-Technologien

Fernbereichsnetze stützen in der Regel auf öffentlichen Übertragungskanälen ab, die heute noch oft auf dem letzten Teilstück für die Sprachübertragung ausgelegt und entsprechend schmalbandig sind. Durch die laufende Einführung der digitalen Übertragung können breitbandigere Kanäle (z.B. 64 kbps, 2 Mbps, 8Mbps, 34 Mbps, 140 Mbps in PDH, sowie 155Mbps, 622Mbps, 2.4Gbps und höher in SDH) eingesetzt werden. Wir unterscheiden zwischen verschiedene Nutzungsformen dieser Übertragungskanäle:

Punkt zu Punkt

Standleitung Der Übertragungskanal wird ausschliesslich durch eine Anwendung genutzt. Dieser Anwendung steht die gesamte Bandbreite exklusiv zur Verfügung. Bei Leitungsvermittlung wird vor dem Datenaustausch wird mit Hilfe eines Wählverfahrens zwischen Sender und Empfänger ein Übertragungskanal aufgebaut.

Zeitmultiplex Durch den Einsatz von Zeitmultiplexern (TDM - Time Division Multiplexer) lässt sich ein Übertragungskanal in n Subkanäle mit jeweils fixen Bandbreiten aufteilen.

Statistisches Multiplexieren Mehrere Datenströme mit sporadischem Verkehrsaufkommen werden bedarfsorientiert zusammengefasst (multiplexiert) und gemeinsam über einen Übertragungskanal transportiert. Am Ziel werden die einzelnen Datenströme wieder voneinander getrennt (demultiplexiert).

Netz

Paketvermittlung Damit ein vorhandener Übertragungskanal durch mehrere Benutzer gleichzeitig genutzt werden kann, führte man in den 70-er Jahren das Prinzip der Paketvermittlung ein. Pro Benutzer wird ein virtueller Übertragungskanal aufgebaut. Die vorhandene Bandbreite wird unter den Benutzern statistisch, d.h., bedarfsorientiert zugeteilt.

Rahmenvermittlung Um den Bedürfnissen nach höheren Bandbreiten gerecht zu werden, wurde anfangs der 90-er Jahre das Prinzip der Rahmenvermittlung (Frame Relay) ent-

wickelt. Dabei werden nicht Ebene 3-Pakete, sondern bloss Ebene 2-Rahmen vermittelt. Durch weglassen der Ebene 3-Funktionen in den Netzknoten erreicht man dadurch höhere Datendurchsatzraten.

Zellenvermittlung Schon lange besteht aus wirtschaftlichen Gründen der Wunsch, sowohl Daten, wie Bild-, Sprach- und Videoinformationen bedarfsorientiert über ein und dasselbe Netz zu transportieren. Zu diesem Zweck entwickelte man das Prinzip der Zellenvermittlung. Hierbei werden Datenrahmen mit fixer Länge (Zellen) vermittelt. Dadurch erreicht man ein garantiertes Antwortzeitverhalten bei der Übertragung von Sprach- und Viedosignalen, falls die Knoten in der Lage sind, den anfallenden Verkehr blockierungsfrei (d.h. ohne Zwischenspeicherung) zu übertragen. Die Zellenvermittlung setzt Übertragungskanäle von mindestens 2 Mbps voraus. Künftige zellenvermittelnde Netze sollen Bandbreiten bis mehrere Gbps bewältigen können, so dass man im Fernbereich dieselben Datenraten erreichen wird, wie sie in den heutigen LAN's anzutreffen sind.

Normen

Da die Fernbereichsnetze in der Regel auf den öffentlichen Telecomm-Netzen aufsetzen, wurden viele einschlägige Empfehlungen für die Datenvermittlungsnetze von der ITU geschaffen. Die ITU-TSS (International Telecommunication Union, Telecommunications Standards Section) ist für die Schaffung der Telekommunikationsnormen zuständigund. ITU ist der heutige Name für die ehemalige CCITT. Aktuelle Empfehlungen können direkt vom Internet unter http://www.itu.int heruntergeladen werden. Diese sind jedoch gebührenpflichtig.

6.1 Internetworking

Damit lokale Netze (LAN) oder Rechenzentren auch über grössere Distanzen miteinander verbunden werden können, müssen spezielle Techniken eingesetzt werden, die Techniken des Internetworking. Diese Techniken unterscheiden sich gegenüber den LAN-Techniken vor allem in der Leistungsfähigkeit. Mit LAN Komponenten können Netze von etwa 1 km Ausdehnung gebaut werden (in Ausnahmefällen, auch grössere Distanzen). Distanzen ab 1 km bedingen den Einsatz von MAN- oder WAN-Technologien. Für die Überbrückung noch grösserer Distanzen, z.B. interkontinentale Kommunikation, werden die GAN-Technologien eingesetzt. Die Betreiber von WANs bedienen sich immer häufiger der LAN Technologien (z.B. Ethernet) und die LAN-Betreiber machen sich mehr und mehr auch WAN-Technologien zu Nutze (z.B. ATM). Die Leistungsfähigkeit, und somit der Anschaffungspreis und die Unterhaltskosten der eingesetzten Geräte, sind jedoch nach wie vor entscheidende Unterscheidungsmerkmale.

Grundsätzlich unterscheidet man zwischen Internetworking im Nahbereich (bis ca. 10 km) und im Fernbereich (über 10 km). Im Nahbereich gelangen Standleitungen zum Einsatz und im Fernbereich Satellitenverbindungen und Wählnetze oder WAN-Dienst-Netze. Die Unterschiede und Einsatzgebiete dieser Möglichkeiten sind im folgenden beschrieben.

6.1.1 Die Wählnetz-Verbindung

Für Verbindungen, die nur zeitweise betrieben werden sollen, eignen sich Wählnetze. Die einfachste und wohl immer noch die verbreitetste Art solcher Wählnetze sind die analoge Telefonie oder das ISDN (Integrated Services Digital Network), die beiden Vertreter des öffentlichen telefon-Netzwerks. Mit diesen Netzen können einzelne PCs, LANs oder Rechenzentren zeitweise miteinander verbunden werden.

Der Nachteil dieser Lösung liegt in der kleinen Bandbreite dieser Netze (56 kBit/s bei analoger Telefonie, zwischen 128 kBit/s und 2 MBit/s bei ISDN), was gerade für den Filetransfer oder allenfalls für die Replikation von Servern ausreicht (schmalbandige WAN-Dienste).

Vorteile sind, dass diese Technologie, weltweit auch in abgelegenen Gebieten genutzt werden kann, da fast überall Telefonie-Dienste verfügbar sind und für die Verbindung nur ein Standard-Modem oder ein ISDN-Terminal-Adapter notwendig ist. Werden Daten nur während kurzer Zeit pro Tag übertragen, so ist diese Variante sehr kostengünstig.

6.1.2 Die Standleitung

Standleitungen sind Einrichtungen, die Kupferdrähte oder Lichtwellenleiter eines lokalen Netzbetreibers verwenden (diese werden gemietet), um darauf dauernde (stehende) Punkt-Punkt-Übertragungen zu realisieren. Standleitungen eignen sich für Verbindungen, mit Kupferkabeln über weniger als ca. 10 km Länge und mit LWL über eine deutlich längere Strecke. Bild [!!!] zeigt den Aufbau einer solchen Standleitung am Beispiel einer LAN Verbindung mit einem ISP (Internet Service Provider). Es gelangen in diesem Beispiel xDSL-Geräte zum Einsatz (Digital Subscriber Line, das x steht für eine beliebige Variante dieser Technologie). Im Prinzip müssen die Kommunikationspartner bei einem llast mileAnbieter die Drähte oder LWL mieten. (llast-mileAnbieter = ein Anbieter, der das Ortsnetz, d.h. die Kabel auf den letzten Metern zwischen den Zentralen der WAN-Netze und den einzelnen Häusern besitzt und betreibt).

Der llast-mileAnbieter wird die Leiter von den Nahzentralen bis in die Gebäude der beiden Kommunikationsteilnehmer führen. Es ist nun Sache der Kommunikationsteilnehmer, sich die xDSL-Geräte und die notwendigen Router zu beschaffen, an die gemieteten Leitungen zu installieren und zu betreiben. Die gesamte Betriebs- und Funktionsverantwortung liegt somit bei diesen beiden Partnern.

6.1.3 Die Mietleitung

Für das Internetworking über grössere Distanzen, z.B. weltweite Verbindungen von einzelnen LANs, benutzt man vorteilhafterweise die WAN-Dienste der WAN-Anbieter. Mietleitungen können für Punkt-Punkt-Verbindungen, aber auch für Punkt-Multipunkt-Verbindungen von mehreren Kunden des LANs eingesetzt werden. Die Kunden können mit Hilfe solcher Mietleitungen Virtuelle Private Netzwerke (VPN) realisieren, so dass keine unternehmensfremde Benutzer in den Datenverkehr eingreifen können.

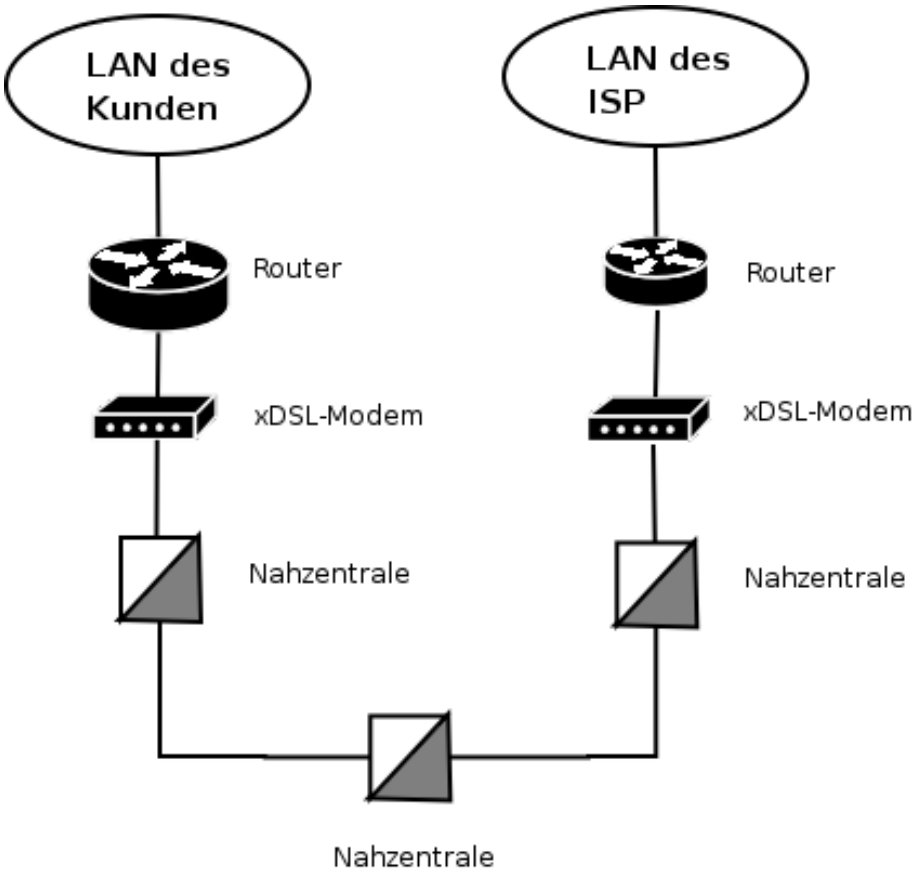

Abbildung 6.1: Beispiel einer Standleitung

Grundsätzlich muss ein LAN-Betreiber sein LAN mit Hilfe einer Standleitung am nächstgelegenen Point of Presence (POP, Netzanschluss des Anbieters) des WAN-Dienst-Anbieters anschliessen. In diesen POPs befinden sich die entsprechenden Netzabschlussgeräte für die jeweilige im Einsatz stehende WAN-Technologie. Z.B. braucht ein ATM-Netz einen ATM-Switch mit LAN-Einschüben für den Anschluss der Kunden-LANs. Bei grösseren Kunden sind die WAN-Betreiber daran interessiert, das WAN bis zum Kunden zu erweitern, so dass der POP im Gebäude des Kunden zu liegen kommt und die Verbindung zwischen dem LAN des Kunden mit dem Netz des Anbieters mit einfachen LAN-Technologien erreicht werden kann. Selbstverständlich haben dadurch diese grossen Kunden das Netzabschlussgerät (in unserem Beispiel den ATM-Switch) auch im eigenen Haus.

Die Vorteile dieser Lösung sind:

- Der Kunde kann sich auf den Aufbau und den Unterhalt von LANs beschränken und muss keine eigenes Know-How über WAN-Netze erwerben.
- Es ist möglich, eine beliebige Bandbreite und verschiedene Dienstqualitäten einzukaufen.
- Die Dienste können auf verschiedene Arten abgerechnet werden: nach angeschlossener Bandbreite, nach Mengen (z.B. Anzahl IP-Pakete) oder auf Grund der gewünschten

Dienst-Qualität (QoS, Quality of Service)

- Falls die Dienste von einem einzigen Anbieter (oder von Anbietern, die untereinander transparente Netze betreiben) bezogen werden, so sind die LANs miteinander verbunden und der Kunde hat den Eindruck, dass seine LANs direkt angeschlossen sind, weil die reinen Transport-Dienste des WAN im LAN nicht sichtbar sind.

Nachteile entstehen vor allem dann, wenn das Service Level Agreement (eine Abmachung über die Qualität und die Art der einzelnen Dienste) nicht fachgerecht erstellt wurde und der Anbieter somit nicht die gewünschte Qualität oder den gewünschten Service liefert.

6.1.4 Sateliten-, Funk-, Laser- und Radio-Verbindungen

LANs lassen sich auch über Satelliten, Funkstrecken, Laserstrecken und radio-Übertragungen realisieren. Bei den Satelliten ist vor allem das Problem der Signal-Laufzeit zu beachten. Diese Art der Verbindung geht doch immerhin über einige 10-tausend km und somit dauert es eine ganze Weile, bis z.B. ein IP-Paket von Punkt zu Punkt übertragen wurde. Für Broadcastdienste wie TV oder Multimedia spielt das nicht unbedingt eine Rolle. Bei Echtzeit-Anwendungen ist dies jedoch unbrauchbar. Satelliten-netze werden vorwiegend von grossen GAN-Betreibern gebaut und betrieben. Kunden dieser Anbieter mieten einen Kanal und betreiben eine eigene kleine Bodenstation (Satellitenschüssel), die es erlaubt, die LAN Signale in diesen Kanal zu verpacken, zu übertragen und an der Gegenstelle wieder auszupacken.

Richtfunk-, Laser- und Radio-Übertragung haben die Einschränkung, dass die beiden Kommmunikationsteilnehmer mehr oder weniger eine Sichtverbindung haben müssen. Besteht keine Sichtverbindung, müssen die Signale in Relais-Stationen (Zwischenstationen z.B. auf einem Berg) umgesetzt werden, was das Netz im Unterhalt und in der Beschaffung verteuert. Solche Techniken werden vorwiegend im lokalen Bereich eingetzt, wo die Chance einer guten Sichtverbindung bestehen (z.B. WLL, Wireless Local Loop).

Weitere Netze, die auf diesen Technologien beruhen, werden von grösseren, regional operierenden Unternehmen für den internen Datenverkehr oder als Backup-Übertragungstrecken für Rechenzentren aufgebaut (alternatives Routing im Falle einer Störung der Hauptverbindungen).

6.2 WAN-Dienste-Netze

In diesem Abschnitt werden einige WAN-Dienste-Netze und die dazugehörigen Dienste genauer erklärt. Ein Dienst ist eine Anwendung, die durch den Netzbetreiber zur Verfügung gestellt wird.

Es gibt z.B. folgende Dienst-Klassen:

- Sprache (voice)

- Text (zeichenorientiert)
- Daten (File-Transfer)
- Bilder (Fax, Video, MPEG-2, Fotos)

Was unterscheidet ein WAN von einem LAN, einmal abgesehen von der unterschiedlichen Technologie und somit von der möglichen Ausdehnung ?
LAN Betreiber kennen ihre "Kunden" am Netz genau. LANs sind somit überschaubar und die vorwiegend anwendungsorientierten Dienste auf den LANs werden durch die Server bereitgestellt. Im WAN werden schwergewichtig die oben aufgelisteten Übertragungsdienste bereitgestellt, die von allen Kunden der WAN Betreiber genutzt werden können, ohne dass der WAN Betreiber den Standort oder die Identität des Kuinden kennen muss. Der Kunde braucht nicht einmal einen persönlichen, ausführlichen Nutzungsvertrag mit dem Anbieter zu haben. telefondienste könnenz.B. mit prepaid services genutzt werden. Für die Jursiten ist dieser Umstand oft Anlass zur Kritik, da gerade diese Produkte von den Kriminellen gerne genutzt werden. Der Kunde braucht lediglich ein entsprechendes Endgerät, das ihm die Nutzung der WAN-Dienste erlaubt.
Diese Situation wird im folgenden Bild durch eine Wolke dargestellt. Was sich hinter der Wolke versteckt, ist für den Endkunden nicht interessant. Er ist nur and den Diensten interessiert. Den Fachmann interessieren die verschiedenen Topologien (wie Ringe, Maschen), Protokoll-Familien (wie ISDN, ATM, IP) und Dienste (z.B. Telefonie, Daten) in dieser WAN-Wolke sehr wohl. Im folgenden werden diese WAN-Netze beschrieben, wobei eine grundsätzliche Unterscheidung in Schmalband-Netze und Breitband-Netze gemacht wird.

6.2.1 Schmalband-Netze

Schmalband-Netze arbeiten mit Übertragungsraten von bis zu 2 MBit/s.
Zu den Schmalband-Netzen gehören:

- das PSTN (Public Switched Telephone Network), mit seinen beiden Ausprägungen POTS (Plain Old Telephone System), einem analogen Netz
- das ISDN (Integrated Digital Services Network), der digitale Nachfolger des analogen Netzes.
- das Fax-Netz
- das X.25 und das Frame-Relay-Netz
- das ADSL-Netz

6.2.2 Breitband-Netze

Zu den Breitband-Netzen zählt man Technologien wie z.B. ATM (Asynchroner Transfer Modus) und SDH (Synchrone Digitale Hierarchie), welche Übertragungsraten grösser als 2 MBit/s zulassen. Das SDH ist in den USA als SONET mit leicht unterschiedlichen Definitionen im Aufbau bekannt.

Ebenfalls in den WAN-Bereich gehören digitale (IP-) Dienste auf Kabel-TV-Netzen und Ëthernetmmit der Norm IEEE 802.3ae, welche 10GBit/s Bandbreite erlaubt. Bei dieser 10GBit-Norm wird nur noch der Full-Duplex Mode unterstützt, es gibt also kein CSMA/CD mehr, d.h. es gibt kein Ethernet mehr, auch wenn diese Variante noch Ethernet heisst.

SDH-Netze

SDH-Netze werden vor allem von grossen Daten- und Telefonie-Netz-Betreibern eingesetzt. Diese betreiben aber über SDH ein ATM (ATM/SDH) oder direkt ein IP-Netz (IP/SDH), da die Dienste des SDH nur rudimentär sind. Selbstverständlich kann jeder Endkunde bei den SDH-Betreibern einen Anschluss an das SDH-Netz mieten, um seine Kommunikationsbedürfnisse zu decken, dies ist aber nur bei Bedarf an hohen Datenraten sinnvoll (z.B. bei der Übermittlung von Röntgen-Bildern für Spitäler oder für Videokonferenzen).

Vor- und Nachteile von SDH

SDH hat folgende Vorteile:

- Mit den SDH-Protokollen ermöglichen Interkonnektionen mit den verschiedensten Netzen unterschiedlicher Betreiber.
- Das SDH-Netz wird auf Grund seiner typischen Schicht 1 Funktionalität vorwiegend zur Datenübertragung in Hochleistungsnetzen eingesetzt.
- Das SDH kann eine grosse Bandbreite bereitstellen (je nach Hierarchiestufe zwischen 155 MBit/s und 39.8 GBit/s)
- Das SDH wird heute vorwiegend auf LWL-Netzen eingesetzt.
- Über SDH können alle Protokolle ab Schicht 2 des OSI-Modells betrieben werden (z.B. ATM, IP, IPX).

SDH hat aber auch Nachteile:

- SDH bedingt ein grosses Know-How beim Betreiber.
- Der Anschluss an ein SDH-Netz kann in der Anschaffung der notwendigen Geräte und im Betrieb sehr teuer werden.

ATM

ATM wird heute als WAN-Dienst von verschiedenen Anbietern betrieben und eignet sich für die Übertragung der gesamten firmeninternen Kommunikationsdienste. So ist ATM ideal für Firmen, die rund um die Welt Niederlassungen betreiben und Videokonferenzen, Telefondienste und Datendienste mit einem einzigen WAN-Dienst übertragen wollen. ATM hat auch einige Verbreitung in regionalen Netzen gefunden, die als ATM/SDH-Netze auf Lichtwellenleitern aufgebaut wurden. Die Service Access Points für die Kunden der WAN-Dienste stellen

ATM-Dienste bereit oder neuerdings sogar IP/ATM. In LANs wird ATM für Backbones eingesetzt.

Vor- und Nachteile von ATM

Der Hauptvorteil des ATM ist, dass dieses Netz jede Art von Diensten übertragen kann. Der Nachteil liegt darin, dass auf Grund der fehlenden Standards (es existieren nur RFCs, Request For Comments) die Interkonnektion der verschiedenen Geräte der diversen Hersteller schwierig ist. Die Konfiguration der Geräte und die Planung der ATM-Netze bedingt grosses spezifisches Know-How.

6.3 Übersicht über die verschiedenen WAN-Dienste

Die folgenden Tabellen sollen einen Überblick über die verschiedenen Arten von WAN-Dienstnetzen und deren Hauptmerkmale geben:

Merkmal	**X.25**	**Frame Relay**
Typ	Paketvermittlung	Paketvermittlung Punkt-Punkt
Bandbreiten	64 KBit/s	64 bis 2048 kBit/s
Dienst	Datenübertragung, speziell für Host-Terminal Anwendungen (Bankomaten)	Optimiert für Datenübertragung, Punkt-Punkt-Verbindungen
Anzahl notwendiger Anschlüsse für gutes Kosten/Nutzen-Verhältnis	Unlimitiert	Wenige Anschlüsse, für den Ersatz von firmeneigenen Punkt-Punkt Leitungen geeignet.
Stärken	Grosse Verbreitung, Hohe IT-Sicherheit möglich	Hohe Bandbreite, Bandbreite nach Bedarf erhältlich, einfach skalierbar, Punkt-Punkt-Verbindungen, einfach realisierbar
Schwächen	Limitierte Bandbreite Nur wenig geeignet für LAN/LAN-Verbindungen	Teuer im Vergleich zu ISDN Benötigt Standleitungsanschluss Nicht weit verbreitet Änderungen an den breeits im Einsatz stehenden Anschlüssen sind teuer zu realisieren
Kostenstrukturen	Installationskosten Distanz- oder/und Mengenabhängige Kosten	Installationskosten Monatliche Kosten auf Grund der Bandbreite

Merkmal	**ISDN**	**xDSL**
Typ	Paket- oder Leitungsvermittlung	Punkt-Punkt Leitungsvermittlung
Bandbreiten	64 und 128 kBit,BRI 2048 bis 45 MBit/s PRI	64 KBit/s bis 51 MBit/s
Dienst	Optimiert für Sprache, Daten, Video	Daten, Internet-Zugang, LAN/LAN-Verbindungen, Videokonferenz
Anzahl notwendiger Anschlüsse für gutes Kosten / Nutzen-Verhältnis	Unlimitiert Nur für lokale Anschlüsse geeignet	Unlimitiert
Stärken	Hohe Bandbreiten möglich Parallelbetrieb von Daten und telefonie möglich Unterstützt Multimedia-Services	Kann unterschiedliche Dienste übertragen einfache Setup Benutzt standartisierte Protokolle
Schwächen	Kann aufgrund fehlenden Know-Hows der Installateure immer noch zu Installationsproblemen führen	Dienstnetzanschlüsse noch nicht weit verbreitet Ist in Entwicklung Nur für kleine Distanzen möglich

Merkmal	**Kabel-TV**	**ATM**
Typ	Punkt-Punkt	Switching von Zellen
Bandbreiten	500 kBit/s bis 30 MBit/s	2.048 - 622 MBit/s
Dienst	Internet-Zugang Datenübertragung LAN-LAN-Verbindungen	Optimiert für Sprachvermittlung Video Bilder Daten
Anzahl notwendiger Anschlüsse für gutes Kosten/Nutzen-Verhältnis	Begrenzung durch gemeinsame Nutzung der Kanäle durch die Benutzer unlimitiert	Nur für grosse Leistungen und wenige Anschlüsse geeignet
Stärken	hohe Bandbreite nutzt bestehende Infrastruktur einfacher Setup	sehr hohe Bandbreite kann diverse Dienste simultan nutzen sicher, stabil, zuverlässig
Schwächen	Relativ neue, unerprobte Technologie Bandbreite muss mit allen Teilnehmern geteilt werden historisch bedingt schlechtes Marketing der Netzbetreiber	Nicht weit verbreitet Keine Standards Teure Produkte proprietäre Produkte Inkompatible Produkte unter den Anbietern
Kostenstrukturen	Installationskosten und monatliche laufende Kosten	Nur nach Offerte (gewünschte Bandbreite und QoS)

Merkmal	**IP-Netze**
Typ	Paketvermittlung (Routing von Datagrammen)
Bandbreiten	abhängig vom Transportdienst: • ISDN bis 128 kBit/s • ATM bis 622 MBit/s • IP/DWDM mehr als 622 MBit/s möglich
Dienst	Optimiert für die Dienste der IP-Protokoll-Familie (IP-Stack)
Anzahl notwendiger Anschlüsse für gutes Kosten/Nutzen-Verhältnis	Unlimitiert, je mehr Anschlüsse desto rentabler
Stärken	Grosse Verbreitung Integriert alle möglichen Dienste auf der gleichen Plattform
Schwächen	Informationssicherheit Zuverlässigkeit, für gute QoS können hohe Kosten entstehen Das Netzwerkmanagement ist in vielen verschiedenen Händen
Kostenstrukturen	Abrechnung nach "Flat-Rate" (monatliche Anschlusskosten für eine bestimmte Bandbreite und bestimmte Dienste) Mengenabrechnung nach Anzahl bezogener Pakete, Bandbreiten- und Qualitätsabhängige Kostenstrukturen

Kapitel 7

Firewall Grundlagen

[10] Die Sicherheit steht an erster Stelle, wenn das private Netzwerk eines Unternehmens (LAN) mit dem Internet verbunden ist. Eine zunehmende Anzahl von Mitarbeitern braucht Zugang zu Internet-Diensten wie dem WWW, E-Mail, FTP und Remote-Verbindungen (Telnet, SSH). Unternehmen wollen zudem für ihre Webseiten und FTP-Server den öffentlichen Zugang über das Internet ermöglichen. Dabei muss die Sicherheit der privaten Netze gegenüber unautorisierten Zugriffen von außen gewährleistet sein. Der Administrator muss das lokale Netzwerk gegen das große Chaos "Internet" abschirmen, damit Daten nicht in unbefugte Hände geraten oder gar verändert werden. Für Firmen, die vom Internetzugang abhängig sind, stellen auch die sogenannten DoS-Attacken eine große Gefahr dar.
Mit Firewalls lassen sich Netzwerke gegen unbefugte Zugriffe von außen absichern. Die verfügbaren Lösungen reichen von der Zusatzsoftware bis hin zu speziellen Geräten, die ausschließlich auf diese Aufgabe ausgelegt sind. In ihrer grundlegenden Funktionsweise unterscheiden sich die Systeme allerdings nur wenig.

7.1 Definition einer Firewall

Eine Firewall besteht aus einer Gruppe von Netzwerkkomponenten (Hard- und Software) an der Schnittstelle zweier Netze. Sie gewährleistet die Einhaltung von Sicherheitsrichtlinien zwischen einem privaten und einem öffentlichen (nicht sicheren) Netz, wie zum Beispiel dem Internet. An dieser "Brandschutzmauer" entscheidet sich, auf welche Dienste innerhalb des privaten Netzes zugegriffen werden kann und welche Dienste des nicht sicheren Netzes aus dem privaten Netz heraus nutzbar sind.
Damit eine Firewall effektiv arbeiten kann muss entsprechend der gesamte Datenverkehr zwischen dem privaten Netz und dem Internet über diese Station laufen. Die Firewall untersucht alle Pakete und lässt nur die unverdächtigen passieren. Dabei muss die Firewall ihrerseits immun gegen Eindringlinge sein. Was würde eine Firewall nutzen, wenn Hacker sie nach Belieben anpassen könnten?
Daraus lässt sich eine "Schwäche" von Firewalls ableiten: Diese Systeme bieten leider keinen Schutz, sobald es einem Angreifer gelungen ist, sie zu überwinden. Daher ist auf die eigene Sicherheit der Firewall ebenso viel Augenmerk zu legen wie auf die Sicherheit des privaten Netzes selbst, die durch die Firewall gewährleistet werden soll. Eine Firewall ist nicht wie

ein Router, ein Bastion-Host oder ein anderes Gerät Teil des Netzes. Sie ist lediglich eine logische Komponente, die ein privates Netz vor einem öffentlichen Netz schützt. Ohne eine Firewall wäre jeder Host im privaten Netz den Attacken von außen schutzlos ausgeliefert. Das bedeutet: Die Sicherheit in einem privaten Netz wäre von der Unverwundbarkeit der einzelnen Rechner abhängig und somit nur so gut wie das schwächste Glied im Netz.

7.2 Zentraler Sicherheitsknoten

Der Vorteil einer zentralen Firewall ist, dass sie das Sicherheitsmanagement vereinfacht. Damit gilt die von ihr hergestellte Sicherheit für das gesamte Netz und muss nicht für jeden Rechner einzeln definiert werden. Die Überwachung geschieht ebenfalls zentral über die Firewall. So kann sie gegebenenfalls auch einen Alarm auslösen, da Angriffe von außen nur über diese definierte Schnittstelle zwischen den Netzen erfolgen können. Das Erkennen eines Angriffs ist der erste Schritt zur Abwehr des Angreifers. Als in den letzten Jahren die Internet-Adressen knapp wurden, trat auch in Unternehmen eine Verknappung von IP-Adressen ein. Eine Internet-Firewall ist in diesem Zusammenhang die geeignete Stelle zur Installation eines Network Address Translators (NAT), der die Adressenknappheit lindern kann. Und schließlich eignen sich Firewalls auch, um den gesamten Datenverkehr von und zum Internet zu überwachen. Hier kann ein Netzwerk-Administrator auch Schwachstellen und Flaschenhälse erkennen.

7.3 Nachteile und Begrenzung

Eine Firewall kann keine Angriffe abwehren, wenn die Pakete nicht durch sie hindurch geleitet werden. Wenn zum Beispiel eine Einwählverbindung via Modem oder ISDN aus dem geschützten Netzwerk besteht, können interne Benutzer eine direkte PPP-Verbindung zum Internet aufbauen. Benutzer, welche die zusätzliche Authentifizierung am Proxy-Server scheuen, werden schnell diesen Weg nehmen. Durch die Umgehung der Firewall erzeugen sie jedoch ein großes Risiko für eine Backdoor-Attacke. Firewalls nützen nichts bei Angriffen aus den eigenen Reihen. Sie hindern niemanden daran, sensitive Daten auf eine Diskette zu kopieren und sie außer Haus zu schaffen. Erst recht nicht, wenn diese Person weit reichende Rechte hat oder durch Diebstahl an Passwörter gelangt ist. Firewalls schützen auch nicht vor Computerviren oder Trojanern, da sie nicht jedes Datenpaket nach potenziellen Viren durchsuchen können. Auch sogenannte Data-driven Attacks können Firewalls nicht verhindern. Dabei handelt es sich um scheinbar harmlose Daten mit verstecktem Code zur Änderung von Sicherheitseinstellungen. Zudem muss die Firewall leistungsfähig genug sein, um den Datenstrom analysieren zu können. Je schneller die Internetanbindung, desto mehr Pakete fließen pro Sekunde in und aus dem Netzwerk. Soll die Firewall zudem noch die Datenströme - also nicht nur die einzelnen Pakete, sondern auch den logischen Datenfluss - überwachen, ist ein umso leistungsfähigeres System erforderlich.

7.4 Komponenten einer Firewall

Ein Firewall-System kann aus ein bis drei Komponenten bestehen:

- Paketfilterungs-Router
- Proxy-Server (Application Level Gateway)
- Verbindungs-Gateway (Circuit Level Gateway)

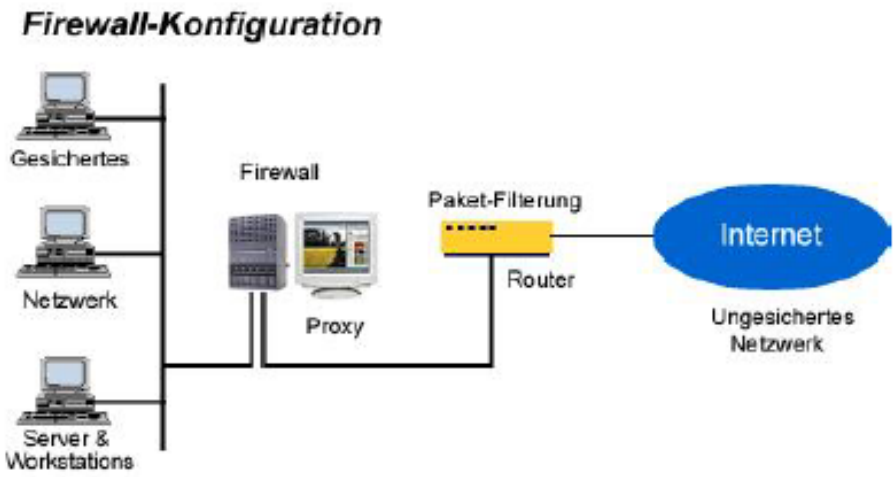

Abbildung 7.1: Firewall Konfiguration mit Paketfilterungs-Router und einem Proxy-Server

Grundsätzlich konkurrieren zwei Firewall-Konzepte: die "passive" Paketfiltertechnologie und die "aktiven" Application Level Gateways. Alle anderen Firewall-Systeme sind Varianten und Weiterentwicklungen dieser beiden Konzepte oder werden damit kombiniert. Dazu gehören etwa das Stateful Packet Filtering, Circuit Level Gateways oder sogenannte Hybrid-Firewalls. Diese neueste Variante stellt eine Kombination aus Paketfilter und Application Level Gateway dar.

7.4.1 Paketfilterungs-Router

Ein Paketfilterungs-Router entscheidet bei jedem Datenpaket anhand festgelegter Filterregeln, ob er es weiterleitet oder nicht. Überprüft werden Header-Informationen wie:

- IP-Ursprungsadresse
- IP-Zieladresse
- das eingebettete Protokoll (TCP, UDP, ICMP, oder IP Tunnel)
- TCP/UDP-Absender-Port
- TCP/UDP-Ziel-Port
- ICMP message type

- Eingangsnetzwerkschnittstelle (Ethernetkarte, Modem, etc.)
- Ausgangsnetzwerkschnittstelle

Falls das Datenpaket die Filter passiert sorgt der Router für die Weiterleitung des Pakets, andernfalls verwirft er es. Wenn keine Regel greift, verfährt der Paketfilterungs-Router nach den Default-Einstellungen.

Man unterscheidet hierbei drei Varianten:

allow Paket wird durchgelassen

deny / drop Paket wird verworfen (Sender bekommt einen "Time Out" bzw. keine Meldung)

reject Paket wird zurückgewiesen (Sender bekommt eine Fehlermeldung)

Default Einstellungen können zum Beispiel deny-all oder allow-all sein.

Anhand der Filterregeln kann ein Router auch eine reine Service-Filterung durchführen. Auch hier muss der Systemadministrator die Filterregeln vorher definieren. Service-Prozesse benutzen bestimmte Ports (Well Known Ports), wie zum Beispiel FTP den Port 21 oder SMTP den Port 25. Um beispielsweise den SMTP-Service abzublocken, sondert der Router alle Pakete aus, die im Header den Ziel-Port 25 eingetragen haben oder die nicht die Ziel-IP-Adresse eines zugelassenen Hosts besitzen. Einige typische Filterrestriktionen sind:

- Nach außen gehende Telnet-Verbindungen sind nicht erlaubt.
- Telnet-Verbindungen sind nur zu einem bestimmten internen Host erlaubt.
- Nach außen gehende FTP-Verbindungen sind nicht erlaubt.
- Pakete von bestimmten externen Netzwerken sind nicht erlaubt.

7.4.2 Abwehr von Angriffen

Bestimmte Angriffstypen verlangen eine vom Service unabhängige Filterung. Diese ist jedoch schwierig umzusetzen, da die dazu erforderlichen Header-Informationen Service-unabhängig sind. Die Konfiguration von Paketfilterungs-Routern kann auch gegen diese Art von Angriffen erfolgen, für die Filterregeln sind jedoch zusätzliche Informationen notwendig. Beispiele für diese Angriffe sind:

Source IP Address Spoofing Attacke Bei einer Spoofing-Attacke fälscht der Angreifer die IP-Absenderadresse eines Datenpakets und verwendet stattdessen die Adresse eines Rechners im internen Netz. Die Firewall kann einen solchen Angriff erkennen, indem sie überprüft, ob ein von außen kommendes Paket eine interne Adresse nutzt. Um den Angriff abzuwehren, sind solche Pakete entsprechend herauszufiltern.

Source Routing Attacke Bei einer Source Routing Attacke gibt der Angreifer die konkrete Route vor, die ein Datenpaket nehmen soll, um Sicherheitsmaßnahmen zu umgehen. Das Verfahren zum Source Routing ist zwar im TCP/IP-Standard vorgesehen, kommt jedoch kaum noch zum Einsatz. Deshalb kann die Firewall die Pakete mit diesem Flag bedenkenlos verwerfen.

Tiny Fragment Attacke Bei dieser Angriffsform erzeugt der Hacker extrem kleine Datenpakete, von denen nur das erste den TCP-Header enthält. Das soll den Router veranlassen, nur das erste Fragment zu prüfen und die restlichen ungeprüft durchzulassen. Dies erlaubt dem Hacker, die gewünschten Befehle ins Netz zu schmuggeln. Als Abwehr kann die Firewall alle Pakete verwerfen, bei denen das Feld Fragment-Offset auf eins gesetzt ist.

7.4.3 Vorteile von Paketfilterungsroutern

Die Mehrzahl der Firewall-Systeme setzen nur einen Paketfilterungs-Router ein. Außer der Zeit, die für die Planung der Konfiguration des Routers erforderlich ist, entstehen keine weiteren Kosten, denn die Filtersoftware ist Bestandteil der Router-Software. Um den Datenverkehr zwischen privatem und öffentlichem Netz nicht zu stark einzuschränken, sind von Haus aus nur sehr moderate und wenige Filter definiert. Die Paketfilterung ist im Allgemeinen durchlässig für Benutzer und Applikationen. Sie erfordert zudem kein spezielles Training und keine zusätzliche, auf den einzelnen Rechnern installierte Software.

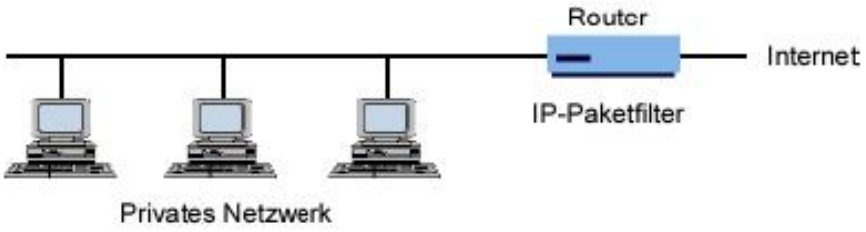

Abbildung 7.2: Einfache Sicherung: Hier schützt nur ein Paketfilterungs-Router das Netzwerk.

7.4.4 Nachteile von Paketfilterungsroutern

Doch die Paketfilterung hat auch Nachteile. So ist neben detaillierten Protokollkenntnissen für eine komplexe Filterung auch eine lange Regelliste notwendig. Derartige Listen sind sehr aufwändig und daher schwer zu verwalten. Es ist zudem schwierig, die Filter auf Wirksamkeit zu testen. Auch sinkt der Router-Durchsatz, wenn zu viele Filter definiert sind. Daneben können Hacker die Firewall durch Tunneln der Pakete überwinden, wobei ein Paket vorübergehend in einem anderen gekapselt wird. Und schließlich: Data-driven-Attacken kann der Router nicht erkennen, da keine Content-Filterung möglich ist.

7.5 Application Level Gateway / Proxy-Server

Ein Proxy-Server (engl. Proxy: Stellvertreter, Bevollmächtigter), auch Application Level Gateway genannt, erlaubt dem Netzwerk-Administrator die Installation von strengeren Sicherheitsregeln als dies bei einem Paketfilterungs-Router möglich ist. Der Server dient als sicheres Gateway zwischen einem privaten und einem öffentlichen (ungesicherten) Netz. Als

Gateway bezeichnet man entweder die Software, die eine Verbindung zwischen zwei Netzwerken herstellt, oder den Computer, auf dem diese Software ausgeführt wird.
Ein Proxy-Server dient nebenbei zur Zwischenspeicherung von Web-Inhalten und kann als erweiterbare Firewall verwendet werden. Das ermöglicht gleichzeitig Datensicherheit und einen schnelleren Zugriff auf Internetinhalte. Der Proxy hat dabei zwei Gesichter: Für den lokalen Client operiert er beim Abruf eines Web-Dokuments wie ein Webserver. Gegenüber dem entfernten Internet-Server tritt er wie ein Webclient auf. Proxy-Server sprechen aber nicht nur HTTP, sondern beherrschen auch Dienste wie FTP, POP3 oder IRC - allerdings abhängig vom jeweiligen Produkt. Da sie als einziger Knotenpunkt zwischen lokalem und globalem Netz geschaltet sind, schützen sie zudem die lokalen Clients. Denn nur der Proxy-Server ist Angriffen von außen ausgesetzt. Die Clients liegen "unsichtbar" hinter ihm.

7.5.1 Vorteile eines Proxy-Servers

Das Betriebssystem auf Client-Seite spielt prinzipiell keine Rolle. Nur spezielle Funktionen wie beispielsweise eine automatische Konfiguration der Clients oder das Trennen einer Internet-Verbindung vom Client funktionieren lediglich von Windows-Clients aus. Daneben lässt sich für jeden Dienst wie FTP oder HTTP ein separater Proxy einrichten. Unerwünschte Dienste filtert der Proxy heraus. Zudem findet kein direkter Paketfluss zwischen internen und externen Rechnern statt.

7.5.2 Nachteile eines Proxy-Servers

Aufgrund der Bearbeitung auf OSI-Layer 7 erreicht ein Proxy eine geringere Performance als z.B. Paketfilterungsrouter. Des weiteren gibt es nicht für alle Firewalls und Applikationen Proxies (Abhilfe ggf. "Generic Proxy").

7.6 Bastion-Host

Unter einem Bastion-Host versteht man einen besonders gesicherten Rechner, der wie eine Festung wirken soll. Er schützt die Rechner im privaten Netz vor Angriffen von Außen. Wie bei einer Festung gibt es nur einen Ein- und Ausgang, der ständig bewacht ist und bei Bedarf sofort geschlossen werden kann. Die Überwachung des Aus- und Eingangs übernimmt meist ein Router als Paketfilter. Bastion-Hosts sind von ihrer Art her damit die gefährdetsten Rechner in einer Firewall. Auch wenn sie in der Regel mit allen Mitteln geschützt sind, sind sie häufigstes Ziel eines Angriffs, da ein Bastion-Host als einziges System Kontakt zur Außenwelt unterhält.
Die Rechner im privaten Netz sind aus dem Internet nicht direkt erreichbar und dadurch unsichtbar. Andersherum ist auch das Internet nur über den Bastion-Host zugänglich. Deshalb ergibt sich für diesen Rechner die logische Grundhaltung: je einfacher der Bastion-Host aufgebaut ist, desto leichter ist er zu schützen. Denn jeder auf dem Bastion-Host angebotene Dienst kann Software- oder Konfigurationsfehler enthalten. Bei minimalen Zugriffsrechten sollte der Bastion-Host gerade so viele Dienste anbieten, wie er für die Rolle als Firewall unbedingt braucht.

Bastion-Hosts werden in unterschiedlichen Architekturen installiert, wie zum Beispiel als Dual-Homed-Host, in Kombination mit einem Überwachungs-Router.

7.6.1 Vorteile eines Bastion-Hosts

Ein Bastion-Host lässt sich so einrichten, dass Dienste nur über eine Authentifizierung abrufbar sind. Zudem kann der Administrator spezielle Bestandteile dieser Dienste komplett abschalten, etwa den PUT-Befehl für FTP-Server. Die voneinander unabhängigen Proxy-Dienste laufen unter einer unprivilegierten Benutzerkennung in separaten, gesicherten Verzeichnissen, so dass ein Angriff über diese Dienste nur schwer möglich ist. Alle anderen Dienste wie SMTP oder HTTP sind auf diesem Rechner komplett abgeschaltet und stellen somit keine Sicherheitslücke dar. Im Bedarfsfall kann der Administrator auch den kompletten Datenverkehr überwachen, um Angreifer zu erkennen.

7.6.2 Nachteile von Bastion-Hosts

Bei bestimmten Diensten, wie etwa Telnet oder FTP müssen sich die Benutzer zweimal einloggen: Einmal auf dem Proxy des Bastion-Hosts und danach auf dem eigentlichen Server. Zudem muss die Client-Software speziell an den Proxy angepasst werden.

7.7 Verbindungs-Gateways

Verbindungs-Gateways (Circuit Level Gateways) sind Proxy-Server mit Zusatzfunktionen. Sie beschränken sich, ähnlich wie Application Level Gateways, nicht nur auf die Kontrolle der IP- und Transportschicht-Header. Statt dessen bauen Sie die Datagramme der Transportschicht aus den IP-Paketen, die unter Umständen fragmentiert sind, zusammen. Wie bei Application Level Gateways gibt es auch hier keine direkten Verbindungen zwischen der Innen- und Außenwelt. Vielmehr findet automatisch eine Adressübersetzung statt. So lässt sich eine Benutzerauthentifizierung erzwingen. Auf der anderen Seite verstehen die Circuit Level Gateways das Anwendungsprotokoll nicht und können deshalb keine Inhaltskontrolle durchführen. Beide Gateway-Varianten verfügen zwar über gemeinsame Merkmale; aber die Fähigkeit, das Anwendungsprotokoll zu verstehen, besitzt nur das Application Level Gateway.

Verbindungs-Gateways vertrauen den internen Benutzern. In der Praxis werden Proxy-Server daher für die Verbindungen nach innen benutzt, während man Verbindungs-Gateways für den Datenverkehr von innen nach außen einsetzt.

7.8 Hybrid-Firewalls

Hybrid-Firewalls bestehen aus Paketfilter und Application Level Gateway, wobei das Gateway die Filterregeln des Paketfilters dynamisch ändern kann. Als "Stateful Inspection" bezeichnet man einen Paketfilter "mit Gedächtnis". Dieser speichert allerdings nur die Informationen aus den Paket-Headern.

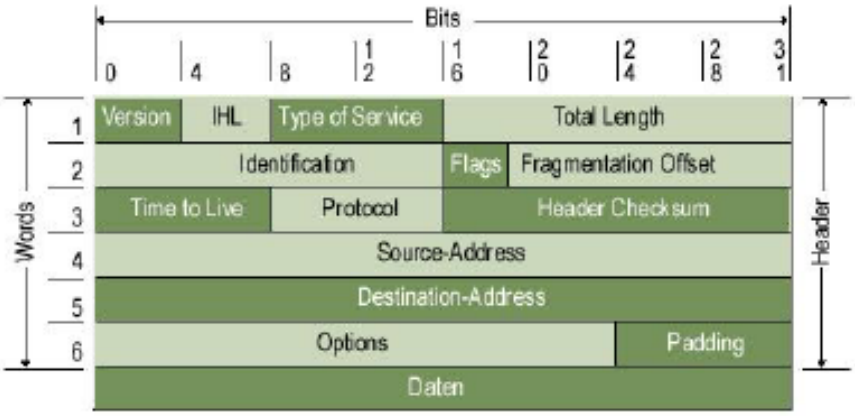

Abbildung 7.3: IP-Pakete: Ein Verbindungs-Gateway muss aus den Daten im IP-Header ersehen, welche Pakete zu einem Datenstrom gehören.

Der Vorteil einer Hybrid-Firewall gegenüber einem alleinigen Application Level Gateway liegt in der höheren Performance. Allerdings bedingt dies auch einen gewissen Sicherheitsverlust. Der Grund liegt darin, dass bei den meisten Protokollen der Proxy keinerlei Kontrolle mehr über die Verbindung besitzt, nachdem er den Paketfilter geöffnet hat. Deshalb muss ein Angreifer den Proxy nur eine Zeit lang in Sicherheit wiegen, um anschließend durch den (für ihn geöffneten) Paketfilter freies Spiel zu haben.
Grundlage des Paketfilters mit Stateful Inspection ist die sogenannte "Stateful Inspection Engine". Diese analysiert die Datenpakete während der Übertragung auf Netzwerkebene. Im gleichen Arbeitsgang erstellt die Engine dynamische Zustandstabellen, welche die Betrachtung mehrerer Pakete erlauben. Die Korrelationen zwischen zusammengehörenden ein- und ausgehenden Paketen ermöglichen ausgefeilte Analysen.

7.9 Hochsicherheits-Firewalls

Hochsicherheits-Firewalls können aus einem Firewall-Subnetz mit zwei Paketfilterungs-Routern und einem Proxy (Bastion Host) bestehen. Ein solches Firewall-System sichert auf der Netzwerk- und Applikationsebene durch die Definition einer "entmilitarisierten Zone" (Englisch: demilitarized zone, kurz DMZ). Dabei befinden sich Bastion-Host, Informationsserver, Modem-Pools und andere Server im DMZ-Netz. Das DMZ-Netz agiert so als kleines isoliertes Netzwerk zwischen dem privaten Netz und dem Internet.
Dabei ist das DMZ so konfiguriert, dass Zugriffe aus dem privaten Netz und dem Internet nur auf Server im DMZ erfolgen können. Direkter Verkehr durch das DMZ-Netz hindurch ist nicht möglich - egal in welcher Richtung.
Bei den hereinkommenden Datenpaketen schützt der äußere Router gegen Standard-Angriffe wie IP-Address-Spoofing oder Routing-Attacken und überwacht gleichzeitig den Zugriff auf das DMZ-Netz. Dadurch können externe Rechner nur auf den Bastion-Host und eventuell den Information-Server zugreifen. Durch den internen Router wird eine zweite Verteidigungs-

linie aufgebaut. Dieses Gerät überwacht den Zugriff vom DMZ zum privaten Netz indem es nur Pakete akzeptiert, die vom Bastion Host kommen. Damit kommen nur Benutzer in das interne Netz, die sich vorher am Bastion-Host authentifiziert haben.

Kapitel 8

Kryptographie Grundlagen

[9] Die Kryptographie hat längst die Grauzone des Spionagebereichs überschritten und soll für sichere Transaktionen im Internet sorgen. Als Grundlage dienen verschiedenste Verschlüsselungsverfahren.

Verschlüsselungsverfahren kommt im Rahmen der Datenübertragung eine besondere Bedeutung zu. Die Kryptographie soll die Geheimhaltung von Daten ermöglichen. Schließlich hat jede Person und jede Organisation ein legitimes Interesse an dem Schutz seiner Daten vor Ausspähung, sei es im Bereich von vertraulichen Bank- und Börsengeschäften oder sei es die E-Mail mit der Einladung zu einem Bewerbungsgespräch, die der bisherige Arbeitgeber nicht zu Gesicht bekommen soll. Insbesondere Firmen sind darauf angewiesen, ihre Einkaufskonditionen oder ihre Forschungsergebnisse vor den Augen der Konkurrenz zu schützen. Neben dem offensichtlichen Zweck der Geheimhaltung muss die Kryptographie andere, grundlegende Kriterien erfüllen. Die Authentifizierung, die Integrität und die Verbindlichkeit beim Austausch von empfindlichen Daten sind vor allem für Geschäftsabschlüsse im Internet zwingend erforderlich.

8.1 (Un-)Sicherheitsfaktoren

Die Authentifizierung spielt bei Internettransaktionen eine gewichtige Rolle: Erst der sichere Beweis, dass eine Person auch wirklich die ist, die sie zu sein vorgibt, führt Kunde und Verkäufer zu befriedigenden Geschäftsabschlüssen. Ein kritisches Gebiet findet sich außerdem im Bankgewerbe: Bank und Kunde müssen darauf vertrauen können, dass nur der Kontoinhaber Auskunft über seinen Kontostand bekommt und sich kein Unbefugter unter falschem Namen anmelden kann. Ein weiterer Unsicherheitsfaktor ist die Integrität der ausgetauschten Daten: Bei abgeschlossenen Transaktionen muss der Empfänger einer Nachricht davon ausgehen können, dass die Nachricht auf dem Weg zu ihm nicht manipuliert wurde. Es wäre fatal, wenn sich bei einer elektronischen Überweisung der Empfänger des Geldes nachträglich verändern ließe. Erst die Verbindlichkeit sichert einen gelungenen Geschäftsabschluss. Der Absender einer Nachricht darf später nicht leugnen können, dass die Nachricht, zum Beispiel eine Bestellung, tatsächlich von ihm stammt. Damit das Internet als Umschlagplatz für Waren und

Dienstleistungen in großem Umfang genutzt werden kann, braucht es deshalb die verbindliche, elektronische Unterschrift. Sie wird in Zukunft der wohl wichtigste Anwendungsfall für starke Kryptographie sein.

8.2 Starke Kryptographie

Vorneweg gilt es, ein mögliches Missverständnis zu klären. Kryptographie, wie sie hier verstanden wird, hat nichts mit dem Verstecken von Daten ("Security by obscurity") zu tun, wie es zum Beispiel im Bereich der Steganographie angewandt wird. Die berechnungssichere, so genannte starke Kryptographie zeichnet sich im Wesentlichen dadurch aus, dass ihre Algorithmen publiziert und allgemein bekannt sind. Die Entschlüsselung der verschlüsselten Nachricht ist dabei in vertretbarer Zeit ohne Kenntnis des Schlüssels nicht möglich. Die Publikation der Ver- und Entschlüsselungsalgorithmen ermöglicht es den Kryptoanalytikern in aller Welt, das Verfahren auf Herz und Nieren zu überprüfen. Nur ein Algorithmus, der seit einigen Jahren publiziert ist und untersucht wurde, kann als sicher gelten, sofern keine Schwachstellen gefunden wurden. Grundsätzlich sind alle gängigen Kryptoalgorithmen durch Ausprobieren zu überwinden. Ob ein Kryptoalgorithmus sicher ist, hängt in der Praxis davon ab, ob der zum Knacken des Algorithmus notwendige Aufwand in Relation gesehen höher ist als der Wert der verschlüsselten Nachricht. Wenn das Ausprobieren selbst mit den schnellsten Computer weitaus länger dauert als die zu lesende Nachricht bedeutsam ist, kann von einem sicheren Algorithmus gesprochen werden. So ist zum Beispiel die Geheimhaltung der Konstruktionspläne eines neuen Autos spätestens nach dessen Markteinführung bedeutungslos. Ein Kryptoalgorithmus, bei dem das Entschlüsseln durch Ausprobieren mehr als zehn Jahre dauert, wäre in diesem Falle also sicher.

8.3 Informationstheorie

Die hohe Redundanz menschlicher Sprache ist eine wichtige Voraussetzung für problemlose Verständigung, weshalb wir unseren Gesprächspartner auch verstehen, wenn es um uns herum sehr laut ist und die Hälfte des Satzes im Lärm untergeht. Wird eine Nachricht per Computer übertragen, ist diese hohe Redundanz unnötig. Den Unterschied macht folgendes Beispiel deutlich, das den Informationsgehalt eines Satzes hinterfragt. Der Satz: "Ich lese gerade diesen tecChannel-Artikel" besteht (einschließlich Leerzeichen) aus 41 Buchstaben. In der üblichen ASCII-Kodierung würde er 41 Byte, das entspricht 328 Bit, belegen. Tatsächlich beträgt der Informationsgehalt eines Buchstabens gewöhnlicher Sprache statt 8 Bit aber nur 1,0 bis 1,5 Bit, da nicht alle Buchstaben des ASCII-Zeichensatzes vorkommen beziehungsweise gleich häufig sind. Der Informationsgehalt dieses Satzes liegt somit bei etwa 60 Bit. Der Rest, zirka 270 Bit, ist Redundanz, also überflüssige Information. Die Redundanz macht die zu übertragende Datenmenge nicht nur größer als sie sein müsste. Sie bietet vor allem Kryptoanalytikern einen hervorragenden Ansatz für das Brechen der Verschlüsselung. Denn in jeder Sprache kommen verschiedene Buchstaben unterschiedlich häufig vor. Vor allem bei langen Chiffretexten ist es daher oft möglich, durch ausgefeilte statistische Analysen die Verschlüsselung zu knacken. Um dies unmöglich zu machen, komprimieren moderne Verschlüsselungsverfahren den Text, bevor sie ihn chiffrieren. Die Kompression entfernt einen großen

Teil der Redundanz des Textes und macht so statistische Kryptoanalyseverfahren weitgehend sinnlos.

8.4 Knackpunkt Rechenpower

Kryptoalgorithmen, bei denen der Aufwand zum Knacken der Verschlüsselung exponenziell mit der Schlüssellänge ansteigt, bieten einen ausreichenden Schutz vor dem wissenschaftlichen und technischen Fortschritt. Denn dieser ist, so paradox dies auf den ersten Blick klingen mag, der größte Feind der Kryptographie. Alle Aussagen über die Sicherheit von kryptographischen Verfahren beruhen auf Abschätzungen zum Rechenaufwand, der erforderlich ist, die Verschlüsselung zu brechen. Diese Abschätzungen basieren auf der Geschwindigkeit heutiger Rechner und den bekannten mathematischen Verfahren. Die Entwicklung der Verarbeitungsgeschwindigkeit neuer Prozessoren und Rechner lässt sich noch halbwegs vorhersagen. Hier ist mit einer Verzehnfachung der Rechenleistung alle fünf Jahre zu rechnen. Dies gilt aber nur für die heute bekannten, siliziumbasierten Computer. Optische oder biologische Rechner der Zukunft ermöglichen durch massive Parallelverarbeitung eventuell um Zehnerpotenzen höhere Rechengeschwindigkeiten. Ein ebenso großer Unsicherheitsfaktor ist die künftige Entwicklung der Mathematik. So glaubte man lange Zeit, dass das quadratische Sieb (QS) asymptotisch genauso schnell ist wie jede andere Faktorisierungsmethode. Mit NFS (Number Filed Sieve) wurde eine Faktorisierungsmethode entdeckt, die potenziell bis zu zehn Mal schneller ist als das quadratische Sieb.

8.5 Schlüssellängen

Die Frage nach der richtigen Schlüssellänge lässt sich nicht allgemein beantworten. Es kommt darauf an, wie wertvoll die Daten sind und wie lange sie geheim bleiben müssen. Eine Sensationsmeldung im Journalismus steht am nächsten Tag in der Zeitung, sie muss also nur bis zur Auslieferung der Zeitung geschützt werden. Dagegen soll die Identität eines Spions auch nach 50 Jahren geheim bleiben. Eine kleine Zusammenstellung minimaler symmetrischer Schlüssellängen findet sich bei Schneier (http://www.schneier.com/paper-keylength.html).

Die angegebenen Schlüssellängen gelten für Schlüssel zu symmetrischen Verfahren. Die für Public-Key-Verfahren verwendeten Schlüssel müssen deutlich länger sein, um die gleiche Sicherheit zu gewährleisten.

Sicherheitsgewährleistung

Längere Schlüssel erhöhen zwar die für das Ver- beziehungsweise Entschlüsseln benötigte Rechenzeit, doch diese Zeiten sind in der Regel so kurz, dass sie nicht ins Gewicht fallen. Es spricht daher wenig dagegen, lange bis sehr lange Schlüssel zu wählen. Es ist niemals sicher auszuschließen, dass die mathematische Wissenschaft oder die Entwicklung neuer, hochspezialisierter Chips zur Kryptoanalyse vermeintlich sichere Schlüssellängen in Zukunft als zu unsicher erscheinen lassen.

Empfohlene Schlüssellängen

Informationsart	Lebensdauer	Minimale symmetrische Schlüssellänge
Militärtaktische Informationen	Minuten/Stunden	56-64 Bit
Produktankündigungen, Firmenzusammenschlüsse, Zinssätze	Tage/Wochen	64 Bit
Langfristige Geschäftsplanungen	Jahre	64 Bit
Wirtschaftsgeheimnisse (z.B. Coca-Cola-Rezept)	Jahrzehnte	112 Bit
Geheime Daten zur Wasserstoffbombe	Über 40 Jahre	128 Bit
Personenbezogene Daten	Über 50 Jahre	128 Bit
Geheimdiplomatie	Über 65 Jahre	Mindestens 128 Bit
Daten der US-Volkszählung	100 Jahre	Mindestens 128 Bit

Abbildung 8.1: Empfohlene Schlüssellängen

Sicherheitsgewährleistung

Symmetrische Schlüssellänge	Asymmetrische Schlüssellänge
56 Bit	384 Bit
64 Bit	512 Bit
80 Bit	768 Bit
112 Bit	1792 Bit
128 Bit	2304 Bit

Abbildung 8.2: Sicherheitsgewährleistung

8.6 Kryptoalgorithmen

Es gibt zwei Arten von Kryptoalgorithmen mit Schlüsseln: symmetrische Algorithmen und Algorithmen mit öffentlichen Schlüsseln (Public-Key-Algorithmen). Bei symmetrischen Algorithmen sind Chiffrierschlüssel und Dechiffrierschlüssel entweder identisch, oder der Dechiffrierschlüssel lässt sich aus dem Chiffrierschlüssel berechnen und umgekehrt.
Bei symmetrischen Algorithmen benutzen Sender (oft als Alice bezeichnet) und Empfänger (namentlich Bob) einen gemeinsamen (geheimen) Schlüssel. Dieser geheime Schlüssel muss vor Beginn der verschlüsselten Kommunikation auf eine sichere Weise vereinbart und ausgetauscht worden sein. Zum Beispiel, indem sich Alice und Bob getroffen haben.

8.6.1 DES

Das bekannteste und am weitesten verbreitete symmetrische Verschlüsselungsverfahren ist der Data Encryption Standard (DES). Es wurde 1976 in den Vereinigten Staaten als Bundesstandard anerkannt und benutzt eine Schlüssellänge von 56 Bit.

DES ist auf Standardrechnern in Wochen bis Monaten zu knacken. Anfang 1999 war es möglich, durch die Nutzung der Leerlaufzeit vieler per Internet verbundener Computer, eine per DES verschlüsselte Nachricht innerhalb von 23 Stunden zu dechiffrieren. Erreicht wurde

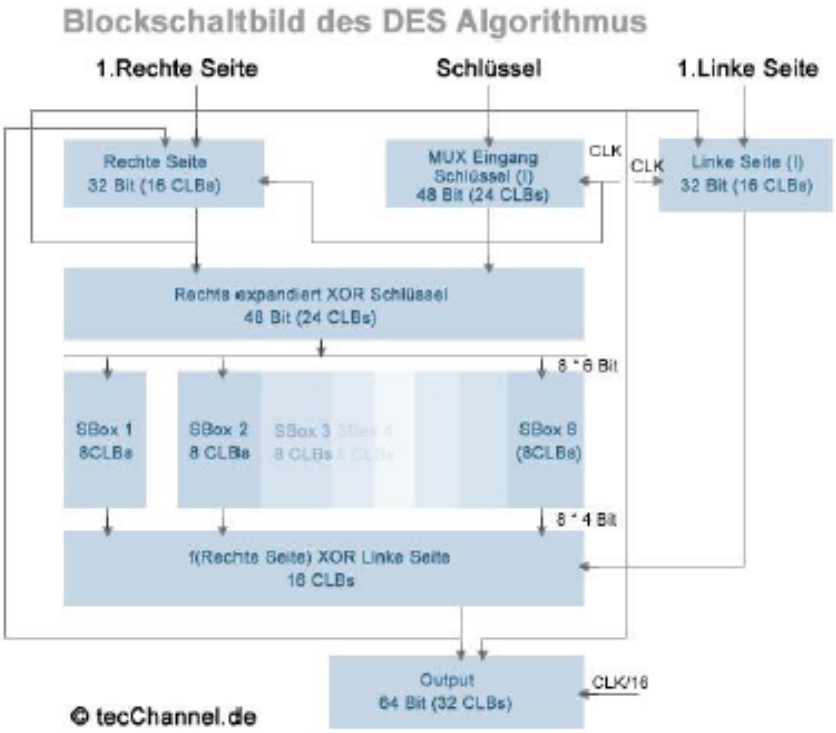

Abbildung 8.3: Blockschaltbild des DES-Algorithmus

dies einfach durch das Ausprobieren aller möglichen Schlüssel. Spezialrechner brauchen für die gleiche Aufgabe nur einen Bruchteil dieser Zeit. Eine auch heute noch sichere Variante von DES ist Triple-DES, das heißt, die dreimalige, hintereinander geschaltete Anwendung von DES. Die Schlüssellänge steigt dadurch auf 168 Bit.

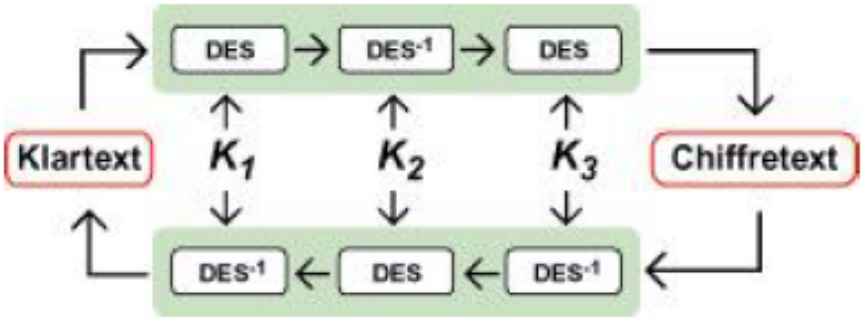

Abbildung 8.4: Beim Triple-DES wird gleich drei Mal verschlüsselt

8.6.2 Public-Key-Algorithmen

Algorithmen mit öffentlichem Schlüssel beruhen auf der Tatsache, dass manche Dinge im Leben einfach auszuführen, aber nur schwer rückgängig zu machen sind. Eine Vase aus zehn Metern Höhe fallen zu lassen, bereitet keine große Mühe; aus den Scherben die Vase wieder zusammenzukleben, ist jedoch fast unmöglich. Bei den Zahlen gibt es ähnliche Phänomene: Zahlen miteinander zu multiplizieren - selbst sehr große - ist leicht. Aber ein Produkt in seine (unbekannten) Faktoren zu zerlegen, ist vergleichsweise schwer. Bei dem Public-Key-Verfahren wird jeweils vom Sender ein Schlüssel zur Chiffrierung und vom Empfänger ein anderer, zugehöriger Schlüssel für die Dechiffrierung verwendet. Sender und Empfänger verwenden Schlüsselpaare. Bei einem guten asymmetrischen Verfahren kann trotz der Kenntnis eines Schlüssels der andere nicht abgeleitet werden.

Zusammengefasst haben Public-Key-Verfahren folgende Merkmale:

- Jeder potenzielle Kommunikationsteilnehmer besitzt einen öffentlichen Schlüssel (Public Key) und einen persönlichen Schlüssel (Private Key).
- Der Public Key darf öffentlich bekannt sein, der Private Key muss geheim gehalten werden.
- Es ist (praktisch) unmöglich, aus dem Public Key den Private Key zu berechnen.
- Der Sender einer vertraulichen Nachricht muss den Public Key des Empfängers kennen.

8.6.3 Funktionsweise Public Key

Will Alice eine geheime Nachricht an Bob schicken, verschlüsselt sie die Nachricht mit Bobs öffentlichem Schlüssel. So kann nur Bob diese Nachricht mit seinem privaten Schlüssel (Private Key) wieder entschlüsseln. Es ist dadurch möglich, dass Alice an Bob verschlüsselte Nachrichten schickt, ohne dass die beiden zuvor über einen sicheren Kanal einen gemeinsamen Schlüssel vereinbaren mussten. Das ist der große Vorteil gegenüber den symmetrischen Verfahren.

Bei diesem Verfahren spielt es keine Rolle, wer sonst noch Bobs öffentlichen Schlüssel kennt. Eine einmal mit diesem Schlüssel verschlüsselte Nachricht kann nur noch mit Bobs privatem Schlüssel wieder gelesen werden.

8.6.4 Primfaktorzerlegung

Die Zerlegung einer (großen) Zahl in ihre Primfaktoren ist eines der ältesten Probleme der Zahlentheorie. Neben der versuchsweisen Division, die einfach, aber bei großen Zahlen sehr zeitaufwendig ist, existieren einige effizientere Faktorisierungsalgorithmen, von denen an dieser Stelle nur der neueste und vermutlich bald auch schnellste, das so genannte Zahlenkörpersieb (Number Field Sieve, NFS) genannt werden soll. Im Moment ist man in der Lage, Zahlen mit etwa 130 Dezimalstellen (entspricht zirka 440 Bit) zu faktorisieren. 1993 benötigte man dazu etwa 5000 MIPS-Jahre (eine theoretische Größe für den Rechenaufwand). Vor einiger Zeit schaltete man über das Internet 1600 Rechner zusammen, die gemeinsam etwa acht

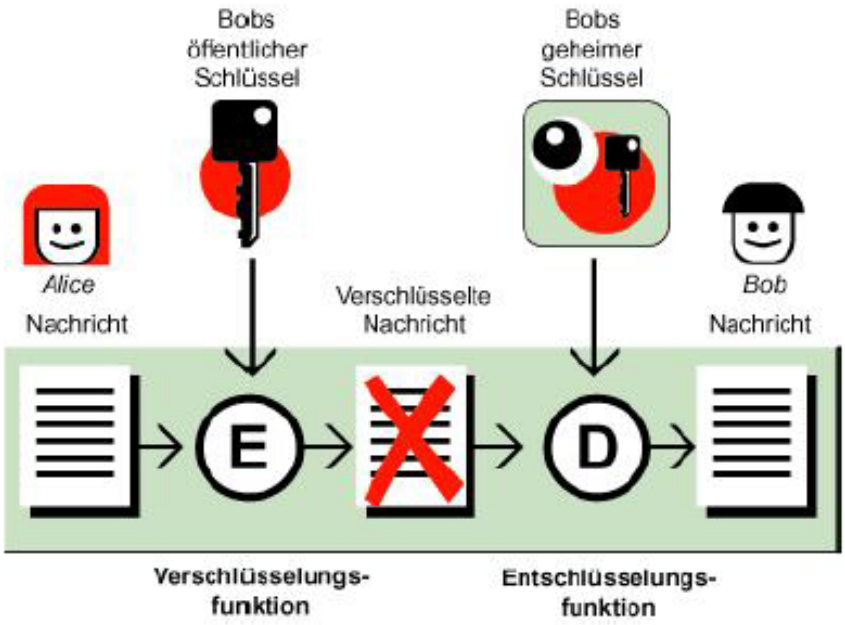

Abbildung 8.5: Beim Verfahren mit Public Keys kommen zwei verschiedene Schlüssel zum Einsatz

Monate brauchten. Nach Aussage der beteiligten Wissenschaftler wäre der Aufwand unter Verwendung des neuen NFS nur ein Zehntel dieser Zeit gewesen. Der Rechenaufwand steigt mit der Länge der zu faktorisierenden Zahl exponenziell an. Die Primfaktorzerlegung großer Zahlen ist ein seit langem sehr intensiv untersuchtes Problem. Große Fortschritte in Form neuer, wesentlich schnellerer Algorithmen sind daher in diesem Bereich unwahrscheinlich. Dies macht Kryptoalgorithmen, die auf der Primfaktorzerlegung beruhen, zu guten Kandidaten für sichere Kryptoalgorithmen.

8.6.5 Das BSI empfiehlt

Bei asymmetrischen Verschlüsselungsverfahren haben sich inzwischen eine Reihe unterschiedlicher Methoden etabliert. Vor allem zwei gelten derzeit als sicher und werden unter anderem vom Bundesamt für Sicherheit in der Informationstechnik (BSI (http://www.bsi.bund.de/aufgaben/projekte/pbdigsig/index.htm)) empfohlen:

1. ElGamal, 1985 Das Prinzip des Algorithmus von ElGamal zur asymmetrischen Verschlüsselung beruht auf der Schwierigkeit "diskrete Logarithmen modulo einer Primzahl" zu berechnen. In praktischen Anwendungen variiert die Primzahl zwischen 512 Bits (geringe Sicherheit) und 1024 Bits (sehr hohe Sicherheit). Eine Variante des ElGamal-Verfahrens ist der 1991 vom National Institute of Standards and Technology publizierte Digital Signature Standard (DSS), der den Digital Signature Algorithm (DSA) spezifiziert. Der ElGamal-Algorithmus ist nicht patentiert.

2. RSA (Rivest, Shamir, Adleman), 1977 RSA, benannt nach den Entwicklern Rivest,

Shamir, Adleman, ist das bekannteste Public-Key-Verfahren, die am weitesten verbreitete asymmetrische Verschlüsselungsmethode und ein Quasi-Standard im Internet. Das Prinzip beruht auf der Schwierigkeit, große natürliche Zahlen in der Größenordnung 10 hoch 150 (beispielsweise 200 Dezimalstellen oder 665 Bits) in ihre Primfaktoren zu zerlegen. In praktischen Anwendungen variieren die Zahlen zwischen 512 Bits (geringe Sicherheit) und 2048 Bits (sehr hohe Sicherheit). RSA ist weltweit seit Ende 2000 frei von Patenten.

8.6.6 RSA

Bei RSA beruhen öffentlicher und privater Schlüssel auf einem Paar sehr großer Primzahlen (100 bis 200 Stellen und mehr). Es wird allgemein angenommen, dass der Aufwand zur Wiederherstellung des Klartextes aus dem Chiffretext und dem öffentlichen Schlüssel äquivalent zur Faktorisierung des Produktes der beiden Primzahlen ist. (Dies ist allerdings streng genommen nur eine qualifizierte Vermutung, es wurde nie bewiesen, dass es wirklich so ist.) RSA ist um den Faktor 100 bis 1000 langsamer als DES. Dies mag im ersten Moment wie ein Nachteil von RSA aussehen, ist aber tatsächlich eher von Vorteil. Denn für die Ver- und Entschlüsselung von normalen Mitteilungen fällt diese Zeit praktisch nicht ins Gewicht. Wer aber RSA mittels einem Brute-Force-Angriff, also dem Ausprobieren aller möglichen Schlüssel, brechen möchte, tut sich umso schwerer, je langsamer der Algorithmus ist. Es ist zurzeit möglich, einen 512-Bit-langen RSA-Schlüssel zu knacken. Der Aufwand hierfür beträgt im Moment etwa 8000 MIPS-Jahre. Schlüssellängen von 1024 Bit oder gar 2048 Bit sind bei RSA nach menschlichem Ermessen in nicht absehbarer Zukunft absolut sicher.

8.6.7 Sicherheit von RSA

Wesentlich für die Sicherheit von RSA ist die Auswahl geeigneter Primzahlen. Sie müssen erstens zufällig gewählt werden und zweitens groß genug sein, um bei steigender Rechenleistung auch in zehn oder 20 Jahren noch einer Primfaktorzerlegung standhalten zu können. Sehr leistungsfähige Rechner könnten in den nächsten Jahren die den Einwegfunktionen zu Grunde liegenden Gleichungen umkehren. Man sollte deshalb im Zweifelsfall eine große Schlüssellänge wählen. Das BSI verlangt in einem Papier (http://www.bsi.bund.de/aufgaben/projekte/pbdigsig/index.htm) für den Modulus n = p * q eine Bitlänge von mindestens 2048. Für den Zeitraum bis Ende 2004 genügen noch 1024 Bit.

8.6.8 Hybride Verschlüsselung

Da asymmetrische Verschlüsselungssysteme in der Regel sehr viel langsamer arbeiten als symmetrische Algorithmen, werden bei den im Internet gebräuchlichen Verschlüsselungsprogrammen häufig beide Verfahren eingesetzt. Bei einem Verbindungsaufbau wird zunächst mit Hilfe einer asymmetrischen Verschlüsselung ein Sitzungsschlüssel (Session Key) gesichert übertragen. Dieser wird anschließend für eine symmetrische Verschlüsselung genutzt. Durch diese Kombination - man spricht von hybrider Verschlüsselung - vereinigt man einen gesicherten, aber langsamen Schlüsseltausch mit einer schnellen, aber weniger sicheren Verschlüsselung.

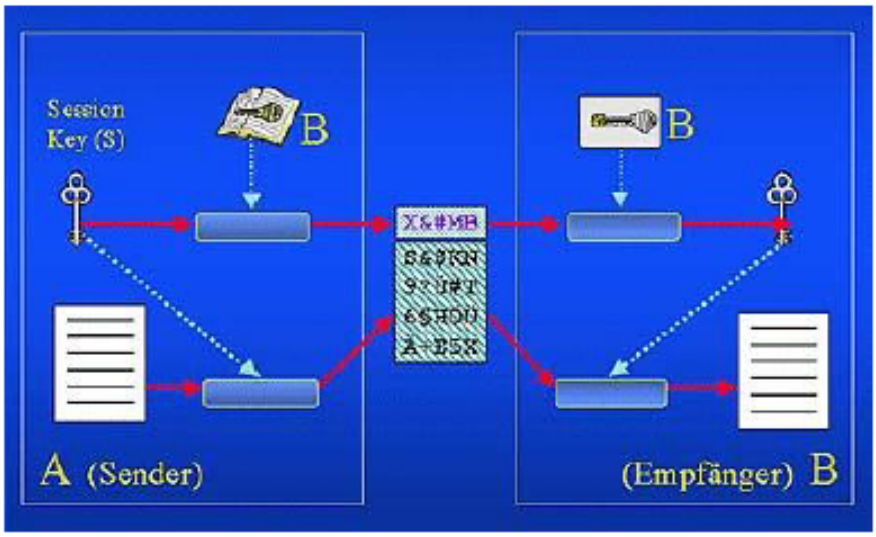

Abbildung 8.6: Hybridverfahren mit asymmetrischer/symmetrischer Verschlüsselung [?]

Das Hybridverfahren läuft wie folgt ab: Der Sender A erzeugt in seiner vertrauenswürdigen Umgebung einen möglichst zufälligen symmetrischen Schlüssel S, den so genannten Session Key und kodiert mit diesem seine Nachricht. Diesen Schlüssel selbst chiffriert der Sender mit dem öffentlichen (asymmetrischen) Schlüssel des Empfängers B. Beides, die mit S verschlüsselte Nachricht und der mit dem öffentlichem Schlüssel von B kodierte Sitzungsschlüssel, werden nun an den Empfänger übermittelt. Da der Empfänger B den Sitzungsschlüssel nicht kennt, muss er zunächst den chiffrierten (symmetrischen) Sitzungsschlüssel entschlüsseln. Dies erfolgt mit seinem geheimen (asymmetrischen) Schlüssel. Den so gewonnenen Sitzungsschlüssel S kann er nun dazu verwenden, die chiffriert übermittelte Nachricht wieder zu dechiffrieren und somit Kenntnis des Nachrichteninhalts zu erlangen.

8.7 Kryptoanalytische und andere Angriffe

Es gibt verschiedene Möglichkeiten zum Angriff gegen kryptographische Protokolle. Am offensichtlichsten ist der Weg des Brute-Force-Angriffs. Bei ihm werden einfach so lange alle möglichen Schlüssel auf den chiffrierten Text angewandt, bis der lesbare Klartext vorliegt. Daneben gibt es, je nach Algorithmus, mathematisch oft sehr anspruchsvolle Analysemöglichkeiten, die auf bestimmten Eigenheiten des verwendeten Kryptoalgorithmus aufsetzen. Gute Kryptoalgorithmen zeichnen sich dadurch aus, dass der Aufwand für derartige Angriffe genauso groß oder größer als der Aufwand eines Brute-Force-Angriffs ist. In der Praxis ist jedoch das Risiko, das aus der Ausspähung eines Schlüssels oder dessen Gewinnung durch Bestechung, Erpressung oder Drohung mit Gewalt erwächst, um Größenordnungen höher, als das Risiko, das aus kryptoanalytischen Angriffen resultiert. Die Frage des sicheren Austausches und der absolut sicheren Aufbewahrung von Schlüsseln hat daher eine besondere Bedeutung. Der sicheren Kommunikation droht noch aus einer anderen Richtung Gefahr. Staatliche Institutionen tun sich noch immer sehr schwer mit der Möglichkeit des Bürgers, unbelauscht zu

kommunizieren. Zu sehr haben sich NSA, FBI, die Bundes- und Landeskriminalämter und der Verfassungsschutz daran gewöhnt, jederzeit Zugriff auf alle sie interessierenden Daten der Bürger zu bekommen. Ein Mensch, der Wert darauf legt, seine alltägliche Kommunikation unbelauscht von nationalen und internationalen Organisationen zu praktizieren, gerät leicht in den Verdacht, etwas Verbotenes zu tun. Einschlägige Politiker und Sicherheitsexperten sind dann schnell mit dem Argument zur Hand, wer nichts zu verbergen habe, brauche auch keine Angst vor staatlicher Überwachung zu haben.

8.8 Hash-Funktionen für Signaturen

Verschlüsselungsverfahren wie RSA erreichen nur den Schutz der Vertraulichkeit einer Nachricht. Neben den eigentlichen Signaturverfahren zum Schutz der Vertraulichkeit benötigt man noch eine Methode, den Urheber einer Nachricht beweisbar zu dokumentieren. In der Regel erfolgt dies mit kryptographischen Prüfsummen, so genannten Hash-Funktionen . Das sind mathematische Methoden, die aus einem beliebigen Klartext nach einem vorbestimmten Verfahren eine Prüfziffer (Komprimat) generieren. Die Funktion verwandelt einen Klartext so in ein entsprechendes Komprimat um, dass auch die kleinste Veränderung des ursprünglichen Texts zu einer gänzlich anderen Prüfziffer führt.

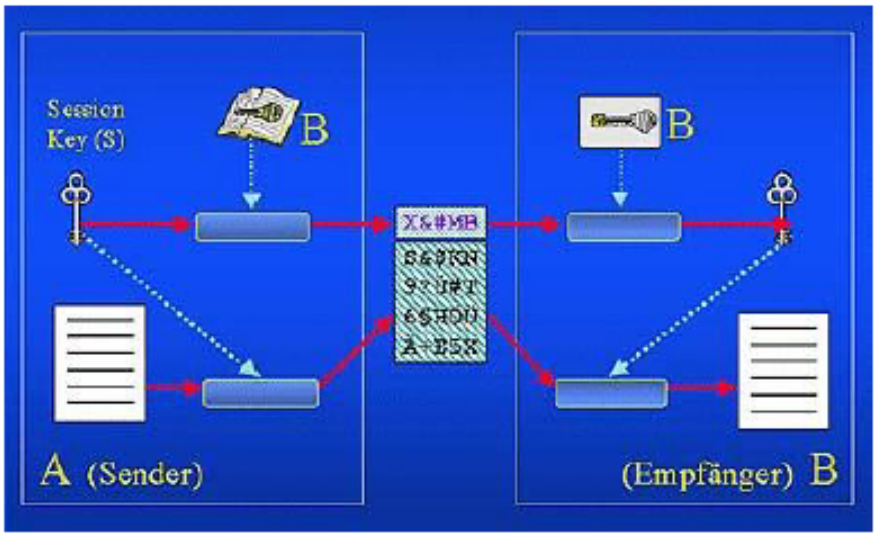

Abbildung 8.7: Nicht umkehrbar: das Ergebnis der Hash-Funktion [?]

Es gehört zu den Forderungen an diese mathematische Funktion, dass aus dem einmal erzeugten Komprimat der ursprüngliche Text nicht wieder rekonstruiert werden kann. Eine solche Hash-Funktion ist nicht umkehrbar und gilt somit als Einwegfunktion. Anders als beim Chiffrieren, ist also eine Wiederherstellung des ursprünglichen Textes nicht möglich. Außerdem muss die Hash-Funktion möglichst kollisionsfrei sein. Verschiedene Nachrichten mit gleichem Hashwert sollen möglichst selten vorkommen. So ist mit einer praktisch vernachlässigbaren Unsicherheit ein bestimmter Hashwert das Ergebnis eines und nur eines ursprünglichen Klartextes. Der Vorteil dieses Verfahrens liegt in der Tatsache, dass anstatt des gesamten Textes

lediglich ein kurzer Hashwert besonders geschützt werden muss.

8.8.1 Hash-Funktionen in der Praxis

Für digitale Signatur-Verfahren ist die Festlegung auf eine Hash-Funktion notwendig. Verfügbare Einweg-Hash-Funktionen sind:

SHA/SHA-1 (Secure Hash Algorithm One) SHA wurde von der NSA entwickelt und als US-Standard angenommen. Eine leicht modifizierte Form hat als SHA-1 den Algorithmus inzwischen ersetzt. Der mit SHA-1 erzeugte Hashwert wird für den DSA (Digital Signature Algorithm), der im DSS (Digital Signature Standard) spezifiziert wird, benötigt. Der Hashwert hat eine Länge von 160 Bit.

MD2, MD4, MD5 (Message Digest) MD4 und MD5 sind Hash-Funktionen, die von R. Rivest (RSA Laboratories) entwickelt und im Zusammenhang mit dem PEM-Standard (Privacy Enhanced Mail) vorgestellt wurden. MD5 ist eine Weiterentwicklung von MD4. Die Algorithmen erzeugen einen Message Digest (Hashwert) von 128 Bit Länge.

RIPEMD-128, RIPEMD-160 (RIPE-Message Digest) RIPEMD wurde im Rahmen des EU-Projektes RIPE (RACE Integrity Primitives Evaluation, 1988-1992) ins Leben gerufen. (RIPE-Message Digest). Wegen kryptographischer Schwächen von MD4 und MD5 wurde RIPEMD von Hans Dobbertin, Antoon Bosselaers und Bart Preneel entwickelt. Der Hashwert ist entweder 128 Bit (RIPEMD-128) oder 160 Bit (RIPEMD-160) lang. RSA Data Security hat auf Grund der Schwächen verfügt, dass MD4 und MD5 für zukünftige Hash-Funktionen nicht implementiert werden sollte. Generell bieten Hash-Funktionen mit längeren Prüfziffern höhere Sicherheit. Daher sollten zukünftig SHA-1 oder RIPEMD-160 verwendet werden. RIPEMD-160 scheint sich in Europa und SHA-1 in den USA als de facto Standard durchzusetzen. Erst die Kombination aus asymmetrischen Verschlüsselungsverfahren und Hashwerten bietet die Möglichkeit, ein Analogon zur menschlichen Unterschrift zu erzeugen.

Teil II

Anhang

Literaturverzeichnis

[1] Andreas Zenk: *Lokale Netze*, ISBN 3-8273-1829-7
Addison-Wesley, 7.Auflage, 2003

[2] Manuel Angel Santos Tarrío, *Die Netzwerkverwaltung und das Simple Network Management Protocol (SNMP)*
http://parallel.fh-bielefeld.de/pv/studien/snmp/

[3] Gerhard Glaser: *Internet und Sicherheit*
http://www.internet-und-sicherheit.de/

[4] Bernhard Haluschak: *Grundlagen: System- und Netzwerk-Management*
http://www.tecchannel.de/

[5] Terry William Ogletree: *Upgrading and Repairing Networks*, ISBN 0-7897-2817-6
Que, 4th Edition, August 2003

[6] Craig Hunt: *TCP/IP Network Administration*, ISBN 0-596-00297-1
O'Reilly, 3.Auflage, 2002

[7] Internet Engineering Task Force: *FYI on a Network Management Tool Catalog*
http://www.ietf.org/rfc/rfc1470.txt?number=1470

[8] NOC-Tools Working Group: *NOC-Tool Catalogue Revisions (noctool2)*
http://mirror.switch.ch/ftp/doc/ietf/noctool2/noctool2-charter.txt

[9] tecCHANNEL: *Kryptographie Grundlagen*
http://www.tecchannel.de/internet/416/index.html

[10] tecCHANNEL: *Firewall Grundlagen*
http://www.tecchannel.de/internet/682/index.html