Das kleine LAN-Howto

1. Grundlagen des TCP/IP-Netz (LAN, WAN, WLAN)

1.1 LAN

LAN bedeutet Local Area Network. Es ist ein lokal beschränktes Netzwerk mit mehreren Rechnern, die alle über ein Netzwerkprotokoll kommunizieren können. Das am meisten benutzte Protokoll ist mittlerweile TCP/IP, da es als verbindungsorientiertes Protokoll gegenüber IPX und NetBEUI Vorteile mit sich bringt und die selben Dienste wie im Internet nutzbar sind, da auch dieses auf TCP/IP beruht.

1.1.1 Die IP-Adressbereiche

Jeder Rechner in einem TCP/IP-Netz muß eindeutig identifiziert sein. Die dazu notwendige Adressierung, zu der eine IP-Adresse notwendig ist, darf innerhalb eines Netzes deshalb nur einmal existieren. Sie besteht aus vier Zahlen von 0 bis 255, die durch einen Punkt getrennt sind.
Die Adresse 80.131.214.85 wäre eine solche gültige IP-Adresse. Hört sich einfach an, wenn es nicht einige Ausnahmen gäbe: Die letzte Zahl darf nicht „255“ betragen. Dies ist die sog. Broadcast-Adresse und bezieht sich auf alle Rechner in einem Netz. Ebenso darf die letzte Zahl keine „0“ sein, da diese das Netz selbst benennt. Die Netzwerkadresse unseres Rechners mit der IP-Adresse 80.131.214.85 ist demnach 80.131.214.0. Die erste Zahl scheidet ebenfalls für die „0“ aus, ebenso die 127.0.0.1, da diese immer den lokalen Rechner kennzeichnet, auf dem der entsprechende Server läuft. Da die Anzahl der IP-Adressen durch diese Art der Adressvergabe eher beschränkt ist, hat man für Rechner ein einem LAN drei Adressbereiche reserviert, die man als private Netzwerke bezeichnet.
Folgende Bereiche werden für private Netzwerke verwendet:

10.0.0.0 bis 10.255.255.255
172.16.0.0 bis 172.31.255.255
192.168.0.0 bis 192.168.255.255

1.1.2 DHCP

Gibt man einem Rechner im LAN eine IP-Adresse, die er beibehalten sollte, bis man sie manuell wieder ändert, spricht man von einer statischen IP-Adresse. Durch diese ist der Rechner immer erreichbar. Startet man einen Windows-Rechner mit einer Netzwerkkarte, greift Windows beim Start auf die eingetragene IP-Adresse zurück. Hat er keine, sucht er einen Rechner im LAN, der in der Lage ist, ihm eine gültige IP-Adresse zu vergeben. Einen solchen Rechner nennt man DHCP-Server (Dynamic Host Configuration Protokoll). Er besitzt einen Pool von IP-Adressen aus einem privaten Adressbereich (z. B. 192.168.0.10 bis 192.168.0.20), die er an Rechner vergibt, die eine anfordern. Es stellt sich jetzt die Frage, wie ein Rechner mit einem anderen Kontakt aufnimmt um eine IP-Adresse zu bekommen, wenn er zu diesem Zeitpunkt noch gar keine hat? Das TCP/IP-Protokoll besteht aus mehreren Schichten, die in einzelne Protokolle aufgeteilt sind. Jedes dieser Protokolle nutzt einen speziellen Port, der es von den anderen unterscheidet. DHCP reagiert auf Anfragen, die unter dieser Protokollschicht liegen, in diesem Fall also auf eine bestimmte Art von Datenpaketen, die zum Zeitpunkt der Verbindungsaufnahme keine IP-Adresse benötigen.

1.2 WAN

Ein WAN (Wide Area Network) besteht dann, wenn mehrere Rechner an verschiedenen Standorten z. B. über Telefonleitungen miteinander verbunden werden. Dazu sind an den verschiedenen Rechnern Serverdienste notwendig, die die Verbindungsanfragen bearbeiten. Die Netzwerktopografie unterscheidet sich mit Ausnahme dieser Tatsache kaum vom LAN.

1.3 WLAN (Wireless LAN)

Was sich wie eine Kombination aus LAN und WAN anhört, bedeutet lediglich, daß man an Stelle von Kabeln, mit denen beim konventionellen LAN die Rechner miteinander verbindet, drahtlose Verbindungen nutzt. Dazu werden die Rechner mit WLAN-Netzwerkkarten ausgerüstet und über einen Access-Point miteinander verbunden.

2. Das Internet

2.1 Adressbereiche

Für das Internet gelten die in 1.1.1 beschriebenen Adressbereiche mit Ausnahme der privaten Netze und der 127.0.0.1. Ein Rechner mit einer privaten IP-Adresse ist vom Internet aus nicht erreichbar und kann auch die dort angebotenen Dienste nicht nutzen. Durch die Beschränkung der herkömmlichen Adressierung mit vier Zahlen (IPv4) nutzt man zunehmend das neue System IPv6, eine Kombination aus Zahlen und Buchstaben, aufgeteilt in sechs „Pakete“.

2.2 Router und Gateway

Ein Router ist ein Gerät, das Netze miteinander verbindet. Dies kann ein Rechner mit entsprechender Software sein oder, falls außer Routingdiensten nichts gewünscht wird, ein Stand-alone-Gerät, das irgendwo brav unterm Tisch seinen Dienst verrichtet. Will man mit mehreren Rechner ins Internet, verbindet man also ein TCP/IP-Netz (LAN) mit einem anderen (Internet), so kann diese Arbeit ein Router verrichten. Eine andere Lösung ist ein Proxy-Server. Dieser stellt jedoch nur bestimmte Dienste zur Verfügung, nicht jedoch den vollen Umfang des TCP/IP-Protokolls. Dafür ist er zum Teil in der Lage, Internetinhalte in einem Zwischenspeicher abzulegen, so daß kürzlich besuchte Internetseiten, die von einem anderen Teilnehmer im LAN aufgerufen werden, nicht immer neu angefordert werden müssen. Ein Gateway funktioniert ähnlich wie ein Router, ist jedoch nicht an eine Netzwerktopogafie gebunden und verbindet auch Netze, die nicht auf TCP/IP basieren.

2.3 Domain Name Service

Da man sich IP-Adressen nur schwer merken kann, hat man den Domain Name Service (DNS) eingeführt. Ein DNS-Server setzt IP-Adressen in Domainnamen um, die er in einer Art Liste gespeichert hat. Ruft man z. B. die Webseite www.wetter.de auf, kontaktiert der Rechner zuerst einen DNS-Server, bekommt von ihm die IP-Adresse vom Wetterrechner zurück und spricht diesen dann direkt über die IP-Adresse an.

2.4 NAT

Angenommen, es existiert ein LAN mit vier Rechnern (192.168.0.1 bis 192.168.0.4), das über einen Router mit dem Internet verbunden ist. Ruft Rechner 3 (192.168.0.3) eine Internetseite vom Wetterrechner auf, können seine Datenpakete aufgrund seiner privaten IP-Adresse nicht ins Internet geroutet werden. Mittlerweile sind aber alle Router in der Lage, die privaten Adressen von Rechnern im LAN durch ihre eigene öffentliche zu ersetzen (Network Adress Translation). Der Wetterrechner kommuniziert in diesem Fall nur mit dem Router, der aus seiner Sicht einfach nur ein normaler PC ist. Der Router jedoch merkt sich jedoch, welcher LAN-Rechner die Datenpakete angefordert hat und leitet sie an diesen weiter. Für den Wetterrechner erscheint der LAN-Rechner daher völlig transparent. Auch Hacker kommen in diesem Fall nur bis zum Router, nicht jedoch ins LAN. Die Rechner im LAN sind durch die meisten Angriffe aus dem Internet also geschützt, zudem die meisten Router eine Firewall mitbringen, mit der sich auch spezielle Protokolle und Ports sperren lassen.

3. Der Windows-PC im TCP/IP-Netz

3.1 Der Windows-PC im Internet

3.1.1 Konfiguration

Will man seinem Rechner Internettauglich machen, installiert man in den meisten Fällen ein Modem, eine ISDN-Karte oder eine Netzwerkkarte, teilt Windows seine persönlichen Zugangsdatem mit und wählt sich über das DFÜ-Netzwerk oder eine alternative Software beim Provider ein. Von ihm erhält der Rechner die notwendigen IP-Adressen (seine eigene, die des Gateways und des DNS). Auch dann, wenn man einen DSL-Zugang hat und eine Netzwerkkarte schon mit einer Adresse versehen im Rechner steckt. Eine Netzwerkkomponente wie eine Netzwerkkarte kann also mehrere IP-Adressen bwsitzten.

3.1.2 Kontrolle (was will mir mein Rechner sagen)

Hat sich eine Rechner ist Internet eingewählt, erhält er vom Einwahlserver des Providers eine dynamische IP-Adresse (sie ändert sich bei jedem Einwählvorgang), die des Gateways und eine oder zwei DNS-Adressen. Diese kann man bei Windows 2000 und XP mit dem Programm ifconfig, mit Windows 98 und Me mit WinIPConfig abrufen. Kann man keine Internetseite durch Eingabe einer Domain aufrufen, aber über die IP-Adresse, wurde entweder keine DNS-Adresse mitgeteilt oder der DNS ist nicht erreichbar. Nachprüfen kann man dies, indem man den DNS direkt anpingt (siehe 3.2.2).

3.2 Der Windows-PC im LAN

3.2.1 Konfiguration

Nach Einbau und Installation der Netzwerkkarte braucht jeder Rechner im LAN seine IP-Adresse. Je nach Windows-Version unterscheidet sich die Vorgehensweise, das Netzwerk einzurichten. Im Allgemeinen befindet sich auf dem Desktop ein Symbol für die Netzwerkumgebung. Nach einem Rechtsklick darauf öffnet sich ein Menü, in dem man die Eigenschaften anwählt. Es erscheint ein Fenster, in dem sich die Protokolle und sämtliche Netzwerkkomponenten befinden (Win98) bzw. eine LAN-Verbindung (WinXP).

Win 98: klicken auf:
TCP/IP->Netzwerkkarte - (IPX und NetBEUI kann man bedenkenlos löschen)
Eigenschaften
IP-Adresse festlegen
IP-Adresse: 192.168.0.1
Subnetz-Maske: 255.255.255.0
Falls man im Netz Dateien freigeben möchte, kann man alternativ im „Netzwerk"-Fenster unter Datei- und Druckfreigabe eine oder beide Optionen aktivieren.
Alles mit *Ok* bestätigen – danach obligatorischer Neustart
Zur Kontrolle das Programm WinIPConfig starten *Start->Ausführen->winipcfg->ok*
Im erscheinenden Fenster die Netzwerkkarte auswählen; die aktuelle IP-Adresse wird angezeigt.

WinXP: klicken auf:
LAN-Verbindung (Rechtsklick)
Internetprotokoll (TCP/IP)
Eigenschaften
Folgende IP-Adressen verwenden
IP-Adresse: 192.168.0.1
Subnetz-Maske: 255.255.255.0
Alles andere kann man leer lassen. Dann alles mit *Ok* bestätigen. Ein Neustart dürfte nicht erforderlich sein! Das Programm winipcfg kennt Windows XP nicht. Hier startet man die Eingabeaufforderung: *Start->Alle Programme->Zubehör->Eingabeaufforderung*. Nach der Eingabe des Befehls *ipconfig /all* erscheinen alle IP-Adressen.

3.2.2 Kontakt mit anderen Rechnern

Möchte man prüfen, ob zwei Rechner miteinander kommunizieren können, startet man bei einem (oder beiden) Rechner die Eigabeaufforderung und bedient sich des Programms „ping". Ping sendet viermal hintereinander ein Datenpaket an einen bestimmten Rechner und wartet darauf, daß es zurückkommt. Man tätigt foldende Eingabe: *ping IP-Adresse.* Es ist sinnvoll, zuerst den eigenen Rechner anzupingen, um zu testen, ob das Netzwerk überhaupt funktioniert. Hat der eigene Rechner die Adresse 192.168.0.1 ist die Eigabe demnach: *ping 192.168.0.1.* Nach erfolgreichem Test (Antwort von...) pingt man den anderen Rechner an. Schreibt ping so etwas wie „Ziel-Host nicht erreichbar" oder „no reply...", ist irgendwas faul (manchmal schaltet Windows einfach auf „stur", doch dazu später).

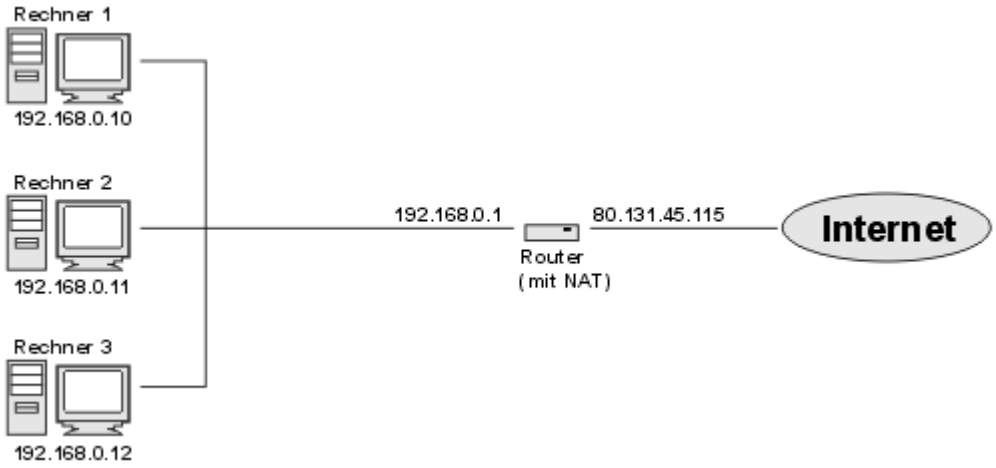

Bild1: Die Rechner im LAN sind über einen Router mit dem Internet verbunden. Zum LAN hin hat der Router die Adresse 192.168.0.1 und ist somit für die LAN-Rechner erreichbar. Bei der Einwahl beim Provider hat der Router, sofern er keine statische Adresse besitzt, die Adresse 80.131.45.115 erhalten. Damit die Datenpakete der Rechner hinausgeroutet werden können, unterstützt der Router NAT.

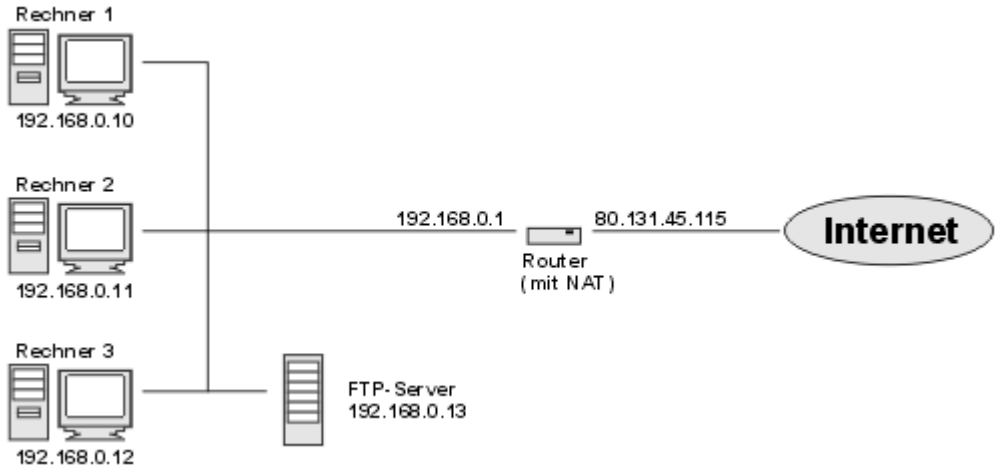

Bild2: Um den einzelnen Benutzern eine manuelle Datensicherung zu ermöglichen, wurde das LAN um einen FTP-Server ergänzt. Möchte jemand von einem entfernten Rechner aus dem Internet oder einem anderen LAN, das ebenfalls einen Internetzugang besitzt, auf diesen Rechner zugreifen, hat er ein Problem: Da sich der Server in einem Netz mit einem privaten IP-Adressbereich befindet, können seine Datenpakete nicht durchgeroutet werden. Da auf dem Router selbst kein FTP-Server installiert ist, werden seine Verbindungsanforderungen von diesem zurückgewiesen. Eine Lösung wäre ein VPN (virtuelles privates Netzwerk). Dabei werden zwei entfernte LAN's über das Internet zu einem LAN gekoppelt (sehr vereinfacht ausgedrückt!).

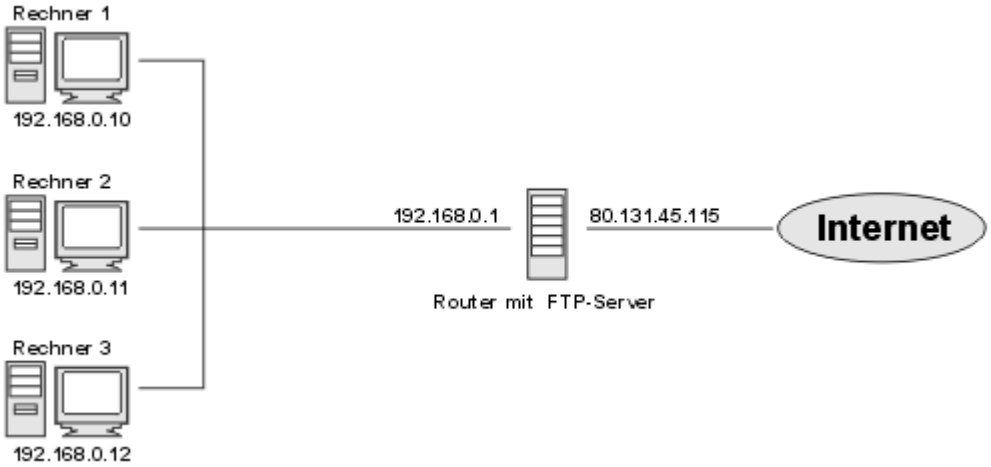

Bild 3: Eine andere Lösung: Der Router wude durch den Server ersetzt. Nun ist auch dieser vom Internet sowie vom LAN aus direkt erreichbar. Der Server übernimmt dabei die Routingdienste inklusive NAT.

3.2.3 Die TCP-Dienste (HTTP, E-Mail, FTP)

Kurze Zusammenfassung: Das TCP/IP-Protokoll teilt sich in verschiedene Schichten und Protokolle auf, die jeweils einem bestimmten Dienst entsprechen. Jeder Dienst besitzt einen zugehörigen Standartport, über den die Datenpakete verschickt werden.

Auf einem Rechner können also mehrere Dienste aktiv sein. Jeder Dienst wird duch einen Server angeboten, der ihn im Netz anderen Rechnern (Clients) zur Verfügung stellt. Ein Server ist in erster Linie eine Software, die den Rechner auf dem sie läuft, erst damit zum Server macht. Genauso verhält es sich mit den Clients. Da ein Webbrowser wie der Internet Explorer primär zum Anzeigen von Internetseiten dient und zu diesem Zweck den HTTP-Dienst nutzt, bezeichnet man ihn auch als HTTP-Client. Zu den am häufigsten genutzten Diensten im Netzt gehören HTTP, E-Mail und FTP.

3.2.3.1 HTTP

Das Hypertext Transfer Protokoll dient zur Übertragung von Webseiten. Webseiten bestehen im Allgemeinen aus einem Code, der durch den Webbrowser entweder direkt oder durch ein externes Programm übersetzt wird. In dem Code können Links und Grafiken eingebunden werden.

3.2.3.2 E-Mail

Der E-Mail-Dienst benötigt zwei Protokolle. Zum einen müssen geschriebene E-Mails verschickt, zum anderen an einem Empfänger gerichtete E-Mails abgeholt werden. Das entspricht in etwa einem Postbriefkasten, in den jeder seine Briefe hinein wirft und einem persönlichen Briefkasten an der Haustür. Für den persönlichen Briefkasten ist ein besonderes Authentifizierungsverfahren notwendig. Schließlich soll jeder nur Zugriff auf seine eigene Post haben. Mit E-Mail kann nicht nur Text und Grafik verschickt werden, sondern auch Dateien, die an den Brief angehängt werden (Attachments).

3.2.3.3 FTP

FTP (File Transfer Protokoll) dient ausschließlich zum Versenden von Dateien. Man benutzt es, um Dateien aus einem Verzeichnis auf dem lokalen PC in eines auf einem anderen PC in Netz zu kopieren. Es können ahnlich wie im Windows Explorer Dateien kopiert, verschoben, umbenannt oder gelöscht werden. FTP kann auch mit Verzeichnissen umgehen. Ein Nachteil des FTP ist, daß Login-Name und Paßwort im Klartext übertragen werden. Hacker können diese mit den entsprechenden Kenntnissen und wenn sie im selben Netz arbeiten, mitlesen und mißbrauchen. Da es allerdings nur um reinen Dateiaustausch geht, ist dies für Hacker nur dann interessant, wenn sie es explizit auf abgespeicherte Dokumente abgesehen haben. Wer also im Büro nebenan einen Werksspion vermutet, sollte zu Alternativen greifen. Im Internet wird FTP sehr häufig als Alternative zu HTTP genutzt, wenn Downloads von Programmen oder Treibern auf Herstellerseiten angeboten werden.

Einige wenige Protokolle:

Dienst/Protokoll	Anwendung	Server	Client	Port
HTTP (Hypertext Transfer Protokoll)	Übertragen von Webseiten	Apache*, Sambar, IIS	Internet Explorer, Netscape Navigator, Opera	80
SMTP (Simple Mail Transfer Protokoll)	Senden von E-Mail	Sendmail*, Exim*, MS Exchange Server	MS Outlook (Express), Netscape Mail, AK-Mail, Eudora, Pegasus, KMail*	25
POP3 (Post Office Protocol)	Abholen von E-Mail	Qpopper*, Quamm*, MS Exchange Server	MS Outlook (Express), Netscape Mail, AK-Mail, Eudora, Pegasus, KMail*	110
FTP (File Transfer Protokoll)	Übertragung von Dateien	ProFTP*, WuFTP*, IIS, Sambar	WS FTP, LeechFTP, alle Webbrowser (Download)	21
SSH (Secure Shell)	Fernwartung von Servern	ssh*	Putty, ssh*	22

* Programm läuft unter Linux

3.2.4 Dateiübertragung zwischen Windows-PC's (Das „it's not a bug, it's a new feature"-Phänomen")

Lösung 1:

Sind alle PC's im Netz konfiguriert, haben also zumindest eine IP-Adresse, bietet sich zum Datenaustausch die Windows-Dateifreigabe an. Bei FTP müßte auf jedem Rechner, der Daten empfangen will, ein FTP-Server installiert sein, damit ein anderer PC Daten aufspielen kann. Ein zentraler Server, auf dem jeder sein persönliches Verzeichnis hat, ist in diesem Fall sinnvoll. Dieser kann auch auf einem einzigen Rechner im LAN installiert sein, vorzugsweise der, der am meisten läuft. Windows selbst bringt allerdings schon ein Bordmittel mit, das die Sache sehr veinfacht – wenn's funktioniert! Gemeint ist das Netbios-Protokoll und ein dazugehöriger Name-Service. So findet man auch Rechner über ihren Namen, den man sich im allgemeinen leichter merken kann als eine IP-Adresse. Um ein Verzeichnis für andere im Netz freizugeben, klickt man mit rechts im Explorer auf ein Verzeichnis, dann auf Freigabe; noch einen Freigabenamen angeben und ein eventuelles Paßwort, und schon ist das Verzeichnis für die anderen LAN-Teilnehmer sichtbar. Um selbst zu sehen, ob im Netz andere Rechner schon Freigaben eigerichtet haben, klickt man im Explorer auf die Netzwerkumgebung und wartet, was passiert. Es sollten (!) jetzt alle Freigaben im Netz erscheinen. Tatsächlich erscheint in vielen Fällen erst einmal überhaupt nichts. Mit etwas Glück springt einem die Fehlermeldung (Das Netzwerk kann nicht durchsucht werden...) an. Dann läßt man es am besten gleich ganz sein und versucht Lösung 2. Bleibt die Fehlermeldung aus, doch die erhoffte Freigabe erscheint nicht, trifft wahrscheinlich folgender Fall zu: Windows sucht beim Start nach Freigaben im Netz und merkt sich diese. Wird erst nach dem Start irgendwo im LAN ein Rechner gestartet, der eine Freigabe zur Verfügung stellt, muß Windows erst über die neue Situation informiert werden. Man klickt im Explorer einmal mit links auf die Netzwerkumgebung, so daß diese markiert ist und drückt „F5". Dadurch sucht Windows erneut nach Freigaben in Netz und zeigt diese an. Im Optimalfall reicht eine einmalige Betätigung von F5. Es kann jedoch sein, das sich Windows erst durch extatisches Permanent-Hämmern auf F5 und erst nach Minuten dazu überreden läßt, die Liste zu aktualisieren. Erscheint dann plötzlich die Freigabe von dem Rechner, der bereits seit fünf Minuten läuft, hört der Spaß damit noch lange nicht auf: Jedes Windows scheint mit dem Netbios-Protokoll etwas anders und völlig willkürlich umzugehen. So kann es sein, daß in einem Netz vier Freigaben existieren, jeder Rechner aber eine andere anzeigt. Dieser Effekt verstärkt sich auf fast schon unterhaltsame Weise, wenn dazu noch verschiedene Windows-Versionen im Spiel (LAN) sind. Was hier wie Tom & Jerry in Binärform aussieht, nennt der Hersteller eine „optimale Netzwerkintegration".

Lösung 2: Es empfiehlt sich, manuell nach einem Rechner zu suchen, von dem man weiß, daß er eine gewünschte Freigabe bereitstellt. Man öffnet hierzu über *Start->suchen->Computer* das entsprechende Fenster. In der Zeile kann man wahlweise den Computernamen oder die IP-Adresse eingeben. Gibt man den Namen ein, kommt das Netbios-Protokoll wieder zur vollen Entfaltung (oder das, was Windows daraus macht). Einen Versuch sollte man jedoch wagen. Schlägt dieser fehl, empfehle ich die Eingabe der IP-Adresse, da man hier weniger auf Windows-Launen angewiesen ist.

In einem LAN mit DHCP kann dies allerdings zu Komplikationen führen. Einen zentralen Server (evtl. Samba unter Linux) mit fester IP sollte man daher in Erwägung ziehen.

Windows-Freigaben sollte man wie Fehlprägungen behandeln. Hat man einmal eine gefunden, sollte man sie nie wieder hergeben. Wenn die Freigabe beim nächsten Windows-Start automatisch erscheinen soll, klickt man das freigegebene Verzeichnis auf dem fremden Rechner (nicht den Rechner selbst) mit rechts an und meldet es als Netzlaufwerk an. Windows behandelt es dann ungefähr so, als wäre es ein lokales Laufwerk (z. B. eingebaute Festplatte). Bitte beachten: Windows versucht nun bei jedem Start, eine Verbindung mit diesem Netzlaufwerk herzustellen. Ist der betreffende Rechner allerdings ausgeschaltet, fragt Windows nach, ob es im Zukunft weiter versuchen soll, auf das Verzeichnis zuzugreifen. Dies sollte man auf jeden Fall bejahen. Auf Windows 2000 oder XP Home Rechnern muß der zugreifende Rechner als lokaler Benutzer registriert sein. Schlägt hier ein Verbindungsaufbau fehl, weil die Benutzer/Paßwort-Kombination in der Benutzerkennung einen Fehler enthält, kann dies ernsthafte Folgen haben, da Windows 98 immer wieder den selben Benutzer verwendet; eine Auswahlmöglichkeit, Benutzer und Paßwort getrennt einzugeben, bietet Windows 98 nicht an. Um das Anlegen eines neuen Benutzers führt dann kein Weg vorbei, es sei denn, man hackt sich geschickt durch die Registry. Aber damit wollen wir uns hier nicht herumschlagen.

Hallo, ich bin's – Das Winpopup

Ein kleines Tool, um übers LAN Nachrichten zu verschicken, bringt Windows 98 von Haus aus mit: Winpopup. Der gleichnamige Befehl startet das Tool im *Ausführen*-Fenster. Um Nachrichten zu empfangen, muß das Tool allerdings permanent laufen.

Fazit

Alles in allem beinhaltet das optimale LAN mit Internetzugang einen kleinen Server, der die wichtigsten Dienste verrichtet. Routing mit NAT, E-Mail, Windows-Fileserver, FTP, Firewall, automatisiertes Backup und DHCP können allesamt in einem einzigen Rechner untergebracht sein. Ein Standart-Bürorechner ab 500 MHz reicht völlig aus, ausgestattet mit dem kostenlosen bis günstigen Open-Source-Betriebssystem Linux ein hochintegriertes und ausreichend skalierbares System in einem Büro-LAN zur Verfügung zu stellen.

Dieses Howto gibt's auch im Internet bei www.it-maid.de *->it-maid->Leistungen->kleines LAN-Howto*