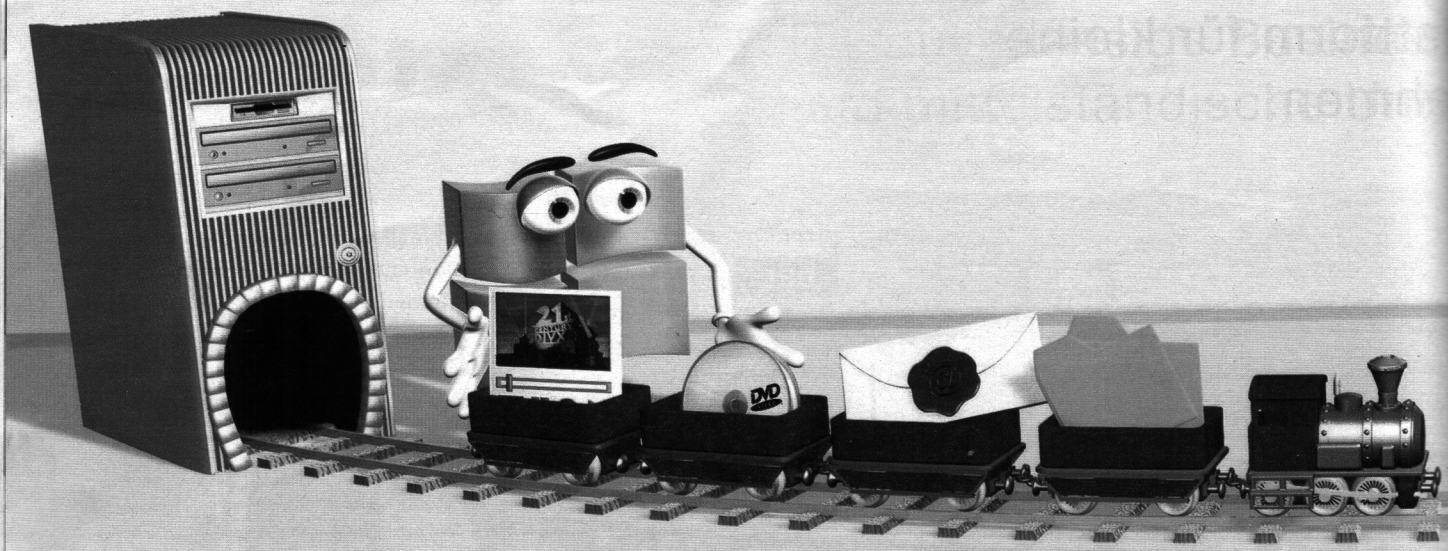


Peter Siering, Axel Vahldiek

Zug um Zug

Vernetzung mit Windows im Griff

Dank eingebauter Betriebssystemfunktionen sollte das Vernetzen von Windows-PCs sowie das gegenseitige Anbieten und Nutzen von Diensten leicht fallen – denkste: Subtile Unterschiede und Eigenarten der Versionen machen so manchem Strippenzieher einen dicken Strich durch die Rechnung. Hier gibt es das nötige Know-how und eine schrittweise Anleitung.

So selbstredend wie Netzwerkfunktionen seit Windows-Generationen zum Lieferumfang gehören, so wenig selbstverständlich funktionieren sie. Mitunter will schon die spontane Vernetzung zwischen zwei Notebooks mit gleicher Windows-Version nicht glücken, gar nicht zu reden vom viel gehegten Wunsch, alten und neuen PC via Netz Daten austauschen zu lassen, oder der Absicht, den Internet-Zugang mit mehreren Windows-PCs zu teilen. Patentrezepte gibt es weder für den einen noch den anderen Fall, sehr wohl aber kann man sich durch ein schrittweises Herangehen das Leben einfacher machen.

Dann steht auch anspruchsvolleren Wünschen nichts mehr entgegen, etwa zentraler E-Mail für alle oder einem gemeinsamen Musikarchiv. Mit den folgenden Artikeln bringen Sie Ihr Windows-basiertes Netz an den Start, bekommen Vorschläge für interessante Dienste im eigenen Netz, die auch auf der Heft-CD dabei sind, lernen alternative Techniken für den Datenaustausch kennen und können entscheiden, ob nicht vielleicht doch eine Serverversion besser geeignet wäre.

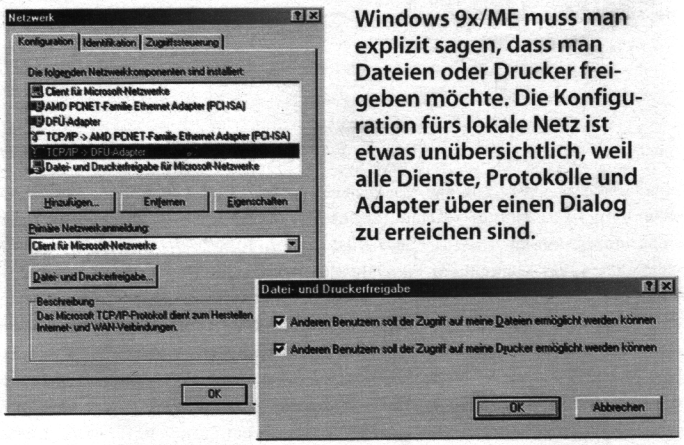
Vorspiele

Die wichtigste Grundlage, damit zwei oder mehr Windows-PCs überhaupt miteinander zu kommunizieren bereit sind, ist ein funktionierendes Netz an sich, egal ob Sie sich dabei für Funk, Powerline oder klassische Ethernet-Verkabelung entscheiden. Eine halbdefekte WLAN-Karte, ein marodes elektrisches Leitungsnetz, ein Wackelkontakt am Cat5-Stecker oder ein defekter Port am Hub oder Switch lassen sich mit Hausmitteln leider kaum erkennen, ohne dass man zumindest rudimentäre Konfigurationsarbeit unter Windows geleistet hat. Die steht deshalb zunächst im Mittelpunkt.

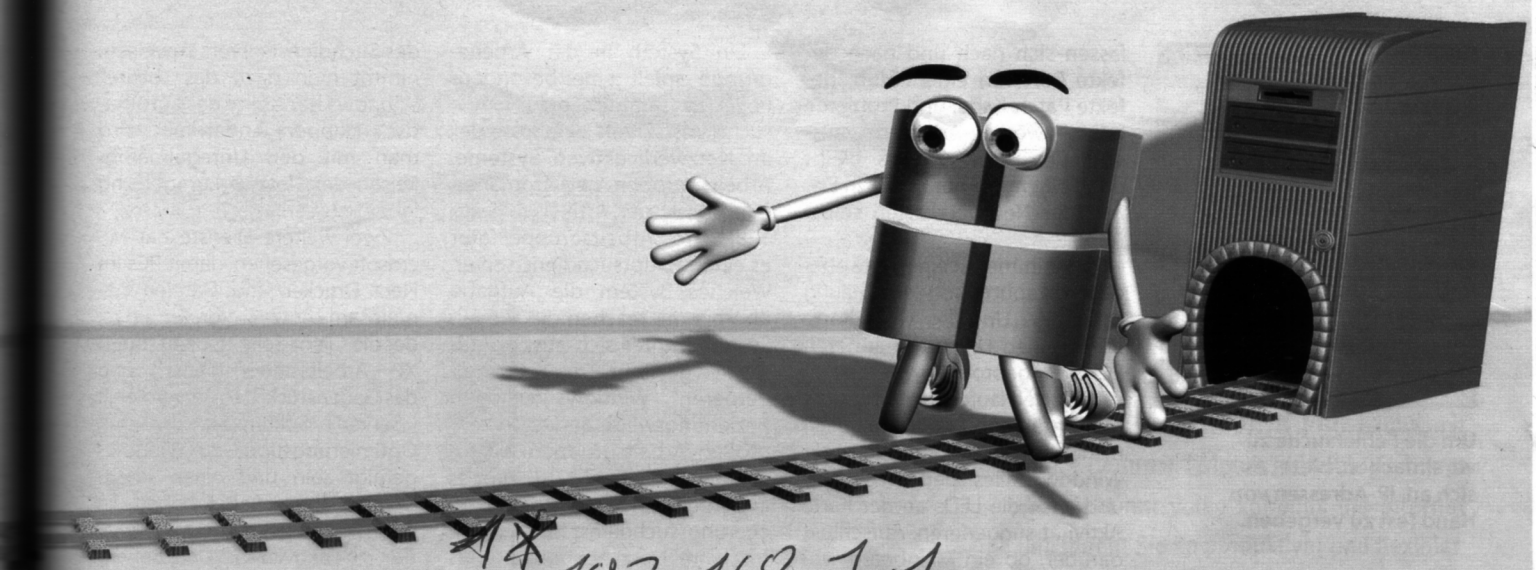
Die Grundlage aller über ein Netzwerk fließenden Daten stellen so genannte Protokolle dar, also Konventionen, die festlegen, wie die Informationen über Draht oder Funk ausgetauscht werden. Über die Details braucht sich bis zu einer gewissen Ebene niemand Gedanken zu machen, weil schon die Auswahl einer Technik hier entsprechende Vorgaben setzt. Erst bei der Sprache, in der sich die Systeme unterhalten, wird es interessant: Für Windows stehen hier neben TCP/IP, das heute die richtige Wahl ist, auch IPX und NetBEUI zur Wahl.

TCP/IP ist nicht nur deshalb die beste Option, weil es für den Datenaustausch mit dem Internet nötig ist, sondern auch, weil viele Anwendungen es voraussetzen und Diagnosewerkzeug verfügbar ist, das für andere Protokolle nicht so zum Greifen nahe liegt. Mit dem einfachen Befehl ping lässt sich etwa probieren, ob Systeme über ein Netz miteinander kommunizieren oder nicht. Die einzige Voraussetzung, die diese dafür zu erfüllen haben, besteht in der Vergabe einer eindeutigen IP-Adresse pro System.

Ähnlich, wie Sie in Ihrer Telefonanlage (mit einem definierten Übergabepunkt zum Anbieter) Durchwahlen beliebig vergeben können, so können Sie auch im eigenen Netz nahezu beliebige IP-Adressen nutzen, solange ein definierter Übergabepunkt ins Internet besteht, der Zugriffe nach außen auf die offizielle Adresse übersetzt, die der Provider vergibt. Ein solcher Übergabepunkt kann ein speziell konfigurierter PC sein oder eine separate Schachtel, Router genannt. Er übersetzt Anfragen ins Internet von den internen



Windows 9x/ME muss man explizit sagen, dass man Dateien oder Drucker freigeben möchte. Die Konfiguration fürs lokale Netz ist etwas unübersichtlich, weil alle Dienste, Protokolle und Adapter über einen Dialog zu erreichen sind.



auf offizielle Adressen und zurück (Network Address Translation, kurz NAT).

Zunächst geht es nur darum, die Adressen für das lokale Netz festzulegen, also die Detailkonfiguration der Netzwerkkarte und des daran gebundenen TCP/IP-Protokolls. Die Einstellungen von weiteren, in einer Windows-Installation anzutreffenden Adaptern können Sie dabei zunächst vernachlässigen, etwa ein 1394-Interface, das XP zusätzlich anzeigt, oder einen DFÜ-Adapter, der bei Windows 9x/ME in der Netzwerkkonfiguration herumspukt. Zu finden sind die Einstellungen unter Netzwerk in der Systemsteuerung (in der „klassischen Ansicht").

Für die Vergabe der Adressen in einem lokalen Netz gibt es mehrere Verfahren: Sie können diese fest eintragen, von einem zentralen System im Netz vergeben lassen (DHCP, Dynamic Host Configuration Protocol), etwa den Router, oder Windows automatisch die Adressen selbst aussuchen lassen (APIPA, Automatic Private IP Addressing). Die letzte Möglichkeit ist die schlechteste. Die erste Option kommt dann nicht in Frage, wenn Sie mit Windows XP den integrierten Dienst zur gemeinsamen Nutzung des Internet verwenden wollen – dann nämlich möchte dieser Windows-Zusatz die Adressen für Ihr Netzwerk selbst vergeben und lässt sich, anders als seine Vorläufer, dabei auch nicht reinreden.

Für einen ersten Funktionstest, ob die Hardware fürs Netz grundsätzlich arbeitet, können Sie aber in den Eigenschaften des TCP/IP-Protokolls feste Adressen vergeben. Es empfehlen sich dafür IP-Nummern aus einem für private Netze reservierten Bereich: Der erste PC bekommt die IP-Adresse 192.168.1.1, der zweite 192.168.1.2 und so weiter bis 254.

Zwei Adressen sind tabu: Die 192.168.0.0 beschreibt das gesamte Netzwerk (Netzwerkadresse) und die letzte Adresse im Netz 192.168.0.255 ist die Broadcast-Adresse, über die sich alle Systeme gleichzeitig ansprechen lassen. Als Netzmaske tragen Sie bei allen Systemen den Standard für dieses (Class-C-) Netz 255.255.255.0 ein. Die Felder für Gateway, Nameserver und WINS bleiben leer (Hintergründe, was sich hinter Akronymen wie WINS verbirgt, liefert der letzte Artikel dieser Serie ab Seite 128).

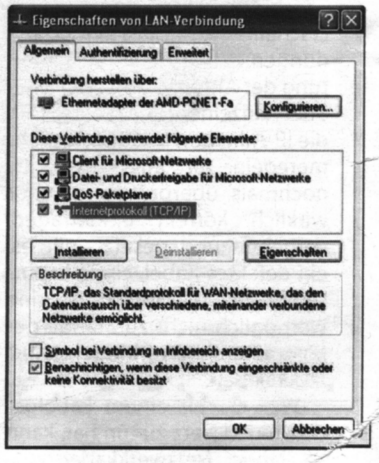
Bei älteren Windows-Versionen (9x und ME) müssen Sie nach dem Hinzufügen der Netzwerkkarte und dem Einrichten der Treiber gegebenenfalls das Microsoft-TCP/IP-Protokoll von Hand installieren. Das geht einfach, indem Sie über die Systemsteuerung „Netzwerk" aufrufen und den Hinzufügen-Knopf betätigen. Anschließend sollten Sie alle anderen Protokolle (IPX und NetBEUI) entfernen. Ebenso ist beim Einrichten der standardmäßig vorhandene DFÜ-Adapter allenfalls im Weg. Auch den können Sie gefahrlos löschen, solange der 9x/ME-PC nicht für den Zugang zum Internet nötig ist. 9x und ME gönnen sich anschließend einen Reboot.

2000 und XP fügen bei der Installation einer Netzwerkkarte von sich aus gleich TCP/IP als Protokoll hinzu und bieten weitere nur als Option. Beim Einrichten mittels WLAN müssen Sie Ihren Access Point oder Router geeignet konfigurieren und auch auf der Seite der Client-PCs die richtigen Schlüssel für WEP oder WPA eintragen. Das erledigt normalerweise die Software, die zu den Kartentreibern oder dem Access Point dazugehört.

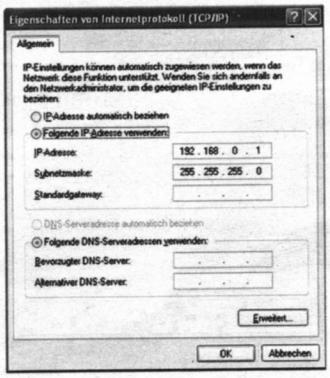
Haben alle beteiligten Systeme eine IP-Adresse, können Sie probieren, ob die Vernetzung grundsätzlich „passt". Rufen Sie einfach auf einem PC auf der Kommandozeile `ping` mit der Adresse eines anderen auf. Der sollte dann antworten. Wenn Sie die Adressen lieber automatisch verteilen lassen wollen, können Sie die zugewiesenen mit den Programmen ipconfig beziehungsweise winipcfg in Erfahrung bringen, um die grundsätzliche Kommunikationsbereitschaft zu erproben.

Klappt es nicht, sollten Sie sicherstellen, dass Ihnen keine Personal Firewall einen Strich durch die Rechnung macht. Der Einsatz einer solchen ist selbst hinter einem Router (oder einem System, das als solcher fungiert) sinnvoll. Deshalb gilt es, die Firewall nicht blind auszuschalten – auch wenn sich das für Tests immer anbietet –, sondern sie gleich geeignet anzupassen, also die Regeln so zu erweitern, dass lokale Zugriffe in Grenzen erlaubt sind.

Bei der zum XP Service Pack 2 gelieferten Firewall beschränkt sich das auf einige Klicks: Öffnen Sie in der Systemsteuerung „Netzwerkverbindungen". Rufen Sie dazu über einen Rechtsklick auf das Symbol der Netzwerkverbindungen die „Eigenschaften" auf. Dort wählen Sie unter „Erweitert" die Funktion „Einstellungen" für die Firewall aus. In dem sich daraufhin öffnenden Dialog sollte auf der ersten Seite („Allgemein") die Firewall „Aktiv" sein, aber das Feld „Keine



XP gibt sich aufgeräumter. Der QoS-Paketplaner stört nicht – auch wenn immer mal wieder die Rede davon ist, dass er Bandbreite „klaut".



Um die Fehlersuche zu vereinfachen, bietet es sich an, IP-Adressen von Hand fest zu vergeben.

Ausnahmen zulassen" sollte kein Häkchen zieren.

Auf der Dialogseite „Erweitert" erreichen Sie über „Einstellungen" unter „ICMP" die Optionen, mit denen Sie sicherstellen können, dass der PC auch auf Pakete reagiert, die das ping-Kommando verschickt. Setzen Sie dazu ein Häkchen vor „Eingehende Echoanforderung zulassen". Achten Sie dabei darauf, dass Sie die Option für die Netzwerkkarte setzen und nicht irgendeinen anderen Adapter, etwa die 1394-Schnittstelle. Abhängig von den übrigen Einstellungen für die Firewall ist diese Option unter Umständen schon gesetzt. Überprüfen sollten Sie sie aber allemal. Damit Sie die Erreichbarkeit der PCs in Ihrem Netz mit ping testen können, müssen die Einstellungen auf allen PCs so gesetzt sein.

Fehler im Netz

Erscheinen beim ping Fehlermeldungen, etwa „Zeitüberschreitung der Anforderung", bei allen oder einzelnen PCs, sollten Sie die IP-Adressen und die Ausnahmeregeln für Ihre Firewall(s) nochmals überprüfen. Ist alles wirklich korrekt eingetragen, vergeben und gesetzt, gilt es, ein defektes Kabel, einen kaputten Port am Hub oder eine womöglich nicht zu Stande gekommene Funkverbindung auszuschließen.

Wer es mit einem kabelgebundenen Netz zu tun hat, kann so lange Netzwerkkabel zwischen den PCs weglassen, die nicht mit einander kommunizieren wollen, bis er bei einer direkten Verbindung über ein gekreuztes Kabel angelangt ist. So lassen sich nach und nach defekte Ports an einem Hub, defekte Patch-Kabel und Probleme mit Powerline-Adaptern ausschließen. Zum Schluss bleibt dann eigentlich nur noch ein Defekt der Netzwerkkarten selbst übrig.

Nicht immer ist eine Karte aber gleich kaputt, sondern häufig kann der „Unwille" einer Karte durch einen Umzug in anderen PCI-Slot gebrochen werden – viele Karten laufen in einem nicht Master-fähigen PCI-Slot nämlich nicht, obwohl treiberseitig unter Windows alles perfekt scheint und auch die LEDs an der Karte Aktivität suggerieren. Aufschluss darüber, ob ein Mainboard womöglich solche Spar-PCI-Slots hat und welche es sind, sollte das Manual liefern.

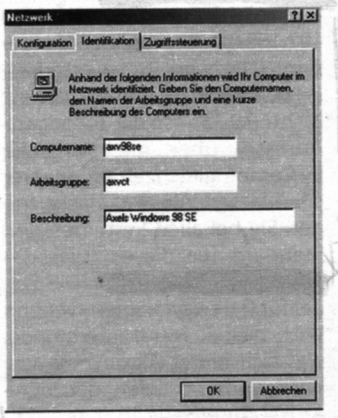
Sprechen alle PCs wie gewünscht via IP miteinander, so stehen die Zeichen gut, dass darauf aufbauende Dienste auch funktionieren werden. Meistens hat Windows sie schon automatisch mit der Installation der Netzwerkkarte installiert. Das Einrichten bleibt aber, wenn man den Assistenten links liegen lässt, am Benutzer hängen. Die Assistenten empfehlen sich nicht: Sie lassen Ihnen keine Wahl, was die verwendeten Adressen angeht, und erschweren dadurch die grundlegende Fehlersuche.

Für den Zugriff auf Drucker und Laufwerke, die übers Netz erreichbar sein sollen, verständigt man sich sinnvollerweise auf einen Namen für die Arbeitsgruppe. Der Name einer Arbeitsgruppe dient dazu, mehrere PCs in einem Netz zu einer logischen Einheit zusammenzufassen. Wenn man über die im Explorer integrierten Funktionen das Netzwerk durchsucht, tauchen alle Systeme in einer Arbeitsgruppe in einem gemeinsamen Ordner auf.

Der Arbeitsgruppenname sollte auf allen Systemen identisch eingetragen, maximal 15 Zeichen lang und frei von Sonderzeichen- sowie Umlautschmuck sein. Das vereinfacht die Netzerei. Die gleichen Regeln sind auch für den Namen zu beachten, den man jedem PC gibt. Anders als der Name der Arbeitsgruppe muss der freilich je PC individuell vergeben sein. Die Namen finden Sie in der Systemsteuerung unter Netzwerk/Identifikation (9x/ME) oder unter System/Computername (2000/XP).

Ein System in der Arbeitsgruppe spielt eine besondere Rolle: Es sammelt als „Hauptsuchdienstserver" eine Liste der im Netzwerk aktiven Systeme, Arbeitsgruppen und Domänen (die erklärt der Artikel ab Seite 128). Pro Arbeitsgruppe gibt es einen Hauptsuchdienstserver. Welches System die Aufgabe übernimmt, machen die aktiven Systeme unter sich aus; grundsätzlich gewinnen dabei die moderneren Windows-Versionen beziehungsweise Server. In sehr großen Arbeitsgruppen, Microsoft nennt die Zahl 32 [1], gibt es außerdem ein System, das als Sicherungssuchdienst fungiert. Ein frisch im Netz hochgefahrenes System taucht erst dann in der Netzwerkumgebung auf, wenn auch der Sicherungssuchdienst das System kennt. Das kann bis zu 15 Minuten dauern.

Nur wenn die Systeme sauber heruntergefahren, also nicht einfach abgeschaltet werden, aktualisiert Windows die Suchlisten. Ansonsten kann es bis zu einer Stunde dauern, bis Suchlisteneinträge automatisch verfallen. Hinter dem Dienst „Computerbrowser", den Windows XP automatisch startet, verbergen sich die Suchdienstfunktionen; die Dienste finden Sie in der Computerverwaltung.



Rechnernamen und Arbeitsgruppennamen helfen beim Auffinden von PCs im Netz. Die Namen sollten nicht allzu kunstvoll gewählt sein.

Es ist möglich, in die Auswahlprozesse für den Suchdienst einzugreifen und dadurch die Sichtbarkeit der Netzwerk-Ressourcen in der Netzwerkumgebung zu verbessern. Wenn ein System im Netz dauerhaft läuft, so sollte man ihm fest die Rolle des Suchdienstservers zuweisen; nimmt man dazu das „beste" Windows her, sollte das automatisch klappen. Andernfalls wird man mit den Unregelmäßigkeiten der Netzwerkumgebung leben müssen.

Zwei weitere Dienste hat Microsoft vorgesehen, damit PCs im Netz Drucker und Dateien gemeinsam nutzen können: den, der die Client-Seite bedient (unter XP „Arbeitsstationsdienst") und das Gegenstück, den Serverdienst („Server"). Sollten Sie absurden Optimierungstipps zu Windows gefolgt sein und einen dieser Dienste abgeschaltet haben, ist jetzt die Zeit gekommen, ihn wieder zu aktivieren. Der Serverdienst kann, wenn ein System nur auf die Ressourcen anderer zugreifen soll, allerdings deaktiviert bleiben.

Unterschiede

Bevor Sie sich daranmachen, mit diesen Diensten Verzeichnisse oder Drucker fürs Netz freizugeben und darauf andere PCs zugreifen zu lassen, müssen Sie sich einiger Unterschiede zwischen den verschiedenen Windows-Versionen bewusst werden: Im Netz ist Windows nicht gleich Windows. Manche Variante erwartet bei Zugriffen übers Netz, dass ein gültiger Benutzername mit übertragen wird, andere sperren sich, wenn ein Konto mit leerem Passwort übers Netz anfragt, und allen gemein ist die kleine Gemeinheit, dass ein Netz einige Minuten braucht, bis es „steht", sprich bis sich die Suchdienste etabliert habe.

Zuerst zu den Unterschieden: Windows 9x und ME kennen, jedenfalls in einfachen Netzen mit einigen PCs ohne dedizierten Server, nur die einfachste Form der gemeinsamen Ressourcen-Nutzung. Sie unterscheiden lediglich lesende und schreibende, auf Wunsch über ein Passwort geschützte Zugriffe. Wer auf den PC zugreift, also unter welchem Benutzernamen ein anderer PC verbinden will, interessiert sie nicht.

Sehr wohl übermitteln diese Windows-Versionen jedoch einen Benutzernamen beim Zugriff auf Ressourcen anderer PCs. Der Name lässt sich lediglich dadurch beeinflussen, dass Sie sich abmelden (im Startmenü findet sich normalerweise ein entsprechender Punkt, wenn zumindest der

XP Professional bietet die meisten Optionen beim Einrichten einer Freigabe auf. Die Zugriffsrechte lassen sich im Detail setzen. Mit einem Dollarzeichen versehene Freigaben tauchen in der Netzwerkumgebung nicht auf und sind nur für Benutzer mit Administratorrechten erreichbar; XP richtet sie automatisch ein.

Client-Dienst für Windows-Netze installiert ist) und wieder neu unter dem gewünschten Namen anmelden. Der Benutzername spielt keine Rolle, wenn Sie auf ein anderes System mit 9x oder ME zugreifen, sehr wohl aber, wenn es unter 2000 oder XP läuft.

Die Home Edition von Windows XP handelt ähnlich: Nur die Schreibzugriffe auf Freigaben kann man mit einem Passwort schützen, lesen darf jeder. Der Name eines Benutzers, der übers Netz zugreifen will, spielt erst gar keine Rolle: XP Home akzeptiert Namen beliebiger Benutzer für Netzwerkverbindungen, egal ob ihm ein Benutzer mit dem Namens bekannt ist oder nicht.

Sieht man sich die Dateien an, die ein „fremder" Benutzer auf einer Freigabe hinterlässt, so gehören Sie dem Konto „Gast" – und das unabhängig davon, ob das Konto aktiv ist oder nicht (Letzteres ist der Standardauslieferungszustand). Das heißt, bei der Home Edition lässt sich trotz mitgeliefertem NTFS, mit dem sich die Rechte einzelner Benutzer differenzieren ließen, im Netz nichts dergleichen ausrichten.

Die Professional-Variante von XP benimmt sich, wie man es eigentlich erwarten dürfte (und damit mit Windows 2000 weit gehend identisch). Auf Freigaben kann normalerweise nur ein Benutzer zugreifen, der auf dem freigebenden System bekannt ist, dort also normalerweise ein Konto hat (man könnte das Gast-Konto freischalten, was sich aber nicht empfiehlt). Für die Zugriffsmöglichkeiten gelten nicht nur die mit der Freigabe definierbaren Rechte, sondern auch die des eventuell darunter liegenden einer NTFS-Partition.

Anders als bei Windows 2000 gibt es aber Tücken: So verwehrt XP Professional Zugriffsversuche übers Netz, wenn für das verwendete Konto kein Passwort gesetzt ist, es also leer gelassen wurde. (Es ist zwar möglich, über das Ausführen von gpedit.msc die von Microsoft vorgegebenen Sicherheitsrichtlinien so zu verbiegen, dass auch ohne Passwort eine Anmeldung übers Netz möglich ist, aber auch das ist nicht zu empfehlen – schließlich hält das potenziellen Eindringlingen alle Türen, Tore und Fenster auf.)

Freigaben einrichten

Die Tatsache, dass XP Professional und Windows 2000 normalerweise ein Benutzerkonto und Passwort für den Zugriff von außen auf eine Freigabe voraussetzen, stellt die Ursache für die wohl häufigsten Netzwerkprobleme dar. Insbesondere, wenn Sie von Windows 9x/ME aus auf eine solche Freigabe zugreifen wollen, muss erstens sichergestellt sein, dass ein Konto auf dem „Server" existiert, und zweitens, dass Windows 9x/ME auch diesen Namen beim Anmeldeversuch übertragen – wie zuvor schon für 9x/ME beschrieben.

Hinter dem Einrichten einer Freigabe steckt nicht mehr, als einen Ordner (nicht, wie der Name sagt, Dateien) oder einen Drucker für die anderen im Netzwerk als zugänglich zu erklären. Ein Rechtsklick auf das jeweilige Objekt und die Auswahl von Freigabe genügt dafür gemeinhin. Je nach Version öffnet sich dann ein Dialog, in dem Sie über die Details bestimmen können. Im Fall von Dateifreigaben unterscheiden sich die Optionen erheblich. Windows 9x/ME und XP Home bieten wenig sicherheitsrelevante Einstellungen: Sie unterscheiden schreibende und lesende Zugriffe; 9x/ME schützen den Schreibzugriff auf Wunsch mit einem Passwort.

Auch XP Professional zeigt von sich aus nur eine vereinfachte Form der Dateifreigabe an: Erst wenn Sie im Explorer im Extras-Menü unter Ordneroptionen in Ansicht das Häkchen vor „Einfache Dateifreigabe aktivieren" entfernen, bekommen Sie die volle Pracht zu sehen. Ordner lassen sich gezielt für einzelne Benutzer und für eine Maximalzahl von Benutzern freigeben. Lesende, schreibende und einige weitere Operationen kann der Serverdienst unterscheiden. Außerdem gibt es Optionen, die über das Caching-Verhalten verbundener Clients bestimmen (siehe [2]).

Damit sind die Möglichkeiten nicht einmal ausgeschöpft. Bei Windows XP Professional kann unter einer Freigabe das NTFS-Dateisystem mit seinen zahlreichen Möglichkeiten zum Beeinflussen der Zugriffsrechte liegen. Wenn es Ihnen partout nicht glücken will, übers Netz eine Datei auf eine Freigabe eines Systems mit XP Professional zu schreiben, so müssen Sie nicht nur die Rechte der Freigabe selbst, sondern auch die des darunter liegenden Dateisystems untersuchen [3].

Mit der Freigabe eines Druckers unter XP, was die Professional-Version ebenfalls mit Optionen für die Rechte garniert, können Sie darüber bestimmen, ob und welche Treiber ein Client übers Netz automatisch für den Drucker zur Verfügung gestellt bekommt. Das ist recht praktisch, denn das lästige Installieren von Treibern auf dem Client entfällt damit. Entsprechend lässt sich draus auch eine Empfehlung ableiten: Der Drucker, der im Netz gemeinsam benutzt werden soll, sollte nach Möglichkeit am modernsten Windows hängen, damit die automatische Treiberinstallation möglichst viele Systeme bedenken kann – Windows 9x/ME könnten XP nicht mit Treibern beliefern.

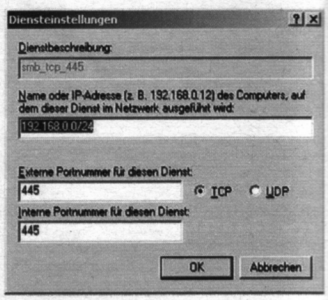
Den automatischen Treiberdownload beim Zugriff auf einen Netzwerkdrucker kann man sich sogar dann zu Nutze machen, wenn der Drucker physisch gar nicht an das XP-System angeklemmt ist. Hängt er etwa am Drucker-Port eines modernen Routers oder Access-Points, so kann ein XP-System im Netz diesen etwa als IP-Printer lokal eingerichteten Drucker übers Netz für andere wieder freigeben und ihnen gleich die Druckertreiber mit verabreichen.

Auch für die gemeinsame Drucker- und Ordnernutzung muss man an der seit XP Service Pack 2 mitgelieferten Firewall fummeln. Ähnlich wie eingangs für ICMP beziehungsweise das ping-Kommando erwähnt, bietet es sich für die Freigaben an, eine Ausnahmegenehmigung für die Dienste für das jeweils zuständige Interface einzurichten.

Die direkt im Konfigurationsdialog der Firewall erreichbare Seite „Ausnahmen" sollten Sie meiden: Sie setzt Ausnahmeregel für *alle* Schnittstellen – das ist gemeinhin nicht sinnvoll, sondern führt nur dazu, dass Sie Ihr System langfristig auch gleich ohne den Schutz der Firewall betreiben können. Einzige Ausnahme: Es ist ohnehin nur ein Netzadapter im System vorhanden, Sie bauen also keine Verbindung zum Internet mit dem System auf.

Sind mehrere Netzwerkschnittstellen vorhanden, etwa eine für den Zugang zum Internet, eine weitere für das lokale Netz, so sollten Sie Interface-spezifische Ausnahmen definieren. Ein Häkchen, wie es Microsoft in den globalen Ausnahmelisten für Datei- und Druckfreigaben vorgesehen hat, genügt dafür leider nicht. Stattdessen müssen Sie Ports und Protokolle im Detail angeben, welche die Freigabefunktionen benutzen: 139 und 445 für TCP sowie 137 und 138 für UDP (nicht wundern: UDP ist Bestandteil des installierten TCP/IP-Protokolls).

Obwohl Windows nach dem Namen oder der Adresse eines einzelnen Computers fragt, dessen Dienste weiterzuleiten sind, können Sie stattdessen – was sinnvoller ist – ein ganzes IP-



Um die Firewall gezielt für die Freigabe von Dateien oder Druckern zu öffen, sind vier einzelne Regeln nötig.

Netzwerk als Ausnahme definieren, etwa nach dem Muster 192.168.0.0/24; das heißt ausgeschrieben, dass alle Rechner mit einer IP-Adresse aus dem Netz 192.168.0.0 zugreifen dürfen (/24 ist die abgekürzte Schreibweise für die Maske 255.255.255.0). Für ein Netz brauchen Sie insgesamt also vier Regeln, für mehrere IP-Netze entsprechend mehr.

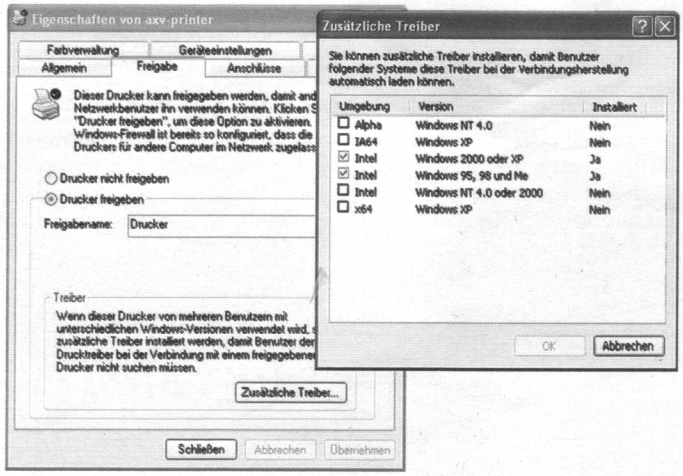
Protokollgemeinheiten

Zu den grundlegenden Unterschieden der Windows-Versionen gesellen sich noch einige Tücken der Microsoft-Netzwerkprotokolle: Beim Einsatz von TCP/IP gibt es zwei Varianten der Kommunikation. Die PCs können NetBIOS über TCP/IP benutzen (auch NBT genannt) oder direkt miteinander sprechen, ohne auf die Konventionen der DOS-Vernetzung zurückgreifen zu müssen. Alle älteren Windows-Varianten (vor Windows 2000), vor allem also die aus der DOS- und nicht NT-Familie, benutzen in einem einfachen Netz NetBIOS vor allem zur Namensauflösung. Damit XP und 2000 mit diesem System reden, muss dort NetBIOS über TCP/IP in den Einstellungen für TCP/IP aktiviert sein.

Weitere Protokolleigenschaften erfordern ein gerüttelt Maß an Geduld: Wenn mehrere Windows-PCs im Netz starten, dauert es einen Moment, bis sich die Suchlistenserver etabliert haben. Das aber heißt, wenn Sie Ihr Netz über das auf dem Desktop abgelegte Netzwerksymbol erkunden wollen, dass schon mal bis zu 15 Minuten vergehen, bis Sie etwas zu sehen bekommen. Deshalb: Geduld gehört dazu.

Ungeduldige Zeitgenossen können sich schneller der korrekten Funktion der Vernetzung vergewissern, indem sie die Kommandozeile bemühen – ein paar Tricks: `ping RECHNERNAME` bemüht die Windows-eigene Namensauflösung für den ping-Test. Wenn die Rechner korrekt eingerichtet sind, sollten die Antworten prompt folgen; wenn aber die Netzmasken zum Beispiel nicht einheitlich konfiguriert sind, dann klappt die Namensauflösung nicht.

Ebenso lassen sich direkt Freigaben auf einem PC erreichen: `net use * \\<RECHNERNAME>\<FREIGABENAME>` verbindet den nächsten freien Laufwerksbuchstaben (deshalb der „*“, der sich auch durch ein Laufwerk ersetzen lässt, etwa „f“) mit der Freigabe auf dem angegebenen Rechner. Um Probleme mit der Namensauflösung auszuschließen, können Sie statt des Rechnernamens auch die IP-Adresse des freigebenden PC einsetzen. Klappt all das nicht, dann stimmt definitiv etwas mit der Grundkonfiguration des Netzwerks nicht.



XP kann einen Drucker im Netz nicht nur freigeben, sondern andere Windows-Rechner auch gleich mit den passenden Treibern versorgen.

Mehrwertdienste

Auf die nahe liegende Frage, wie man das Netz denn ans Internet bringt, gibt es viele Antworten: Wenn ein Rechner stets läuft, bietet er sich als „Router“ an. Allerdings ist es nicht ganz ohne, einem System, auf dem gearbeitet wird oder das womöglich wichtige Dateien für andere bereitstellt, gleichzeitig direkt mit dem Internet zu verbinden. Sie sollten in jedem Fall sicherstellen, dass die Firewall auf dem System aktiv ist.

Als Router sollten Sie auf jeden Fall ein modernes Windows einsetzen. Sie tun sich damit erstens einen Gefallen, weil riskante Sicherheitslücken für XP eher als für Windows 9x geschlossen werden. Zweitens ist es einfacher, ein XP etwa mit DSL zusammenzubringen als 9x oder NT – die entsprechenden Funktionen gehören schließlich schon zum Lieferumfang.

Das Einrichten der Internet-Verbindungsfreigabe (durch einen Rechtsklick auf eine fertig konfigurierte Internet-Verbindung) bringt leider einen unvermeidlichen Assistenten hervor, der Ihr Netz umkrempelt: Windows richtet einen DCHP-Server ein, der feste, nicht manipulierbare IP-Adressen vergibt. Der macht allerdings die Umstellung des arbeitsfähigen Netzes für den gemeinsamen Internet-Zugriff einfach: Stellen Sie einfach alle Systeme in der TCP/IP-Konfiguration des LAN-Adapters so um, dass sie automatisch eine IP-Adresse beziehen; alle zusätzlich nötigen Daten, wie etwas das Default-Gateway und die Adresse des Nameservers erfahren diese dann automatisch.

Eine bessere, weil viel sichere Trennung zwischen Internet-Zugang und internem Netz verspricht ein separater Router. Die Baumarkt-Klasse genügt: Er bringt normalerweise einen DHCP-Server mit, bietet also den gleichen Komfort wie auch die Windows-eigene Internet-Verbindungsfreigabe.

Wer weder Router noch Internet-Verbindungsfreigabe benutzen, sondern mit wechselnden Rechnern direkt ins Netz gehen will, kann das natürlich trotz Heimnetz weiterhin tun. Empfehlenswert ist das aber nicht: Sie müssen dann mehrere Rechner akribisch gegenüber dem Internet abdichten, also mindestens mit Firewall und aktuellen Updates versorgen.

Auch ist die häufige Praxis, ein DSL-Modem für die wahlweise Nutzung durch mehrere PCs im Netz direkt an den gemeinsamen Hub oder Switch anzuschließen, nicht gerade klug: Man kann nicht wirklich ausschließen, dass jemand über das Modem – auch ohne dass eine Verbindung zum Internet besteht – im privaten Netz spazieren geht. Und vor allem: Die gleichzeitige Abwicklung von internem Netzwerkverkehr und DSL über eine Netzwerkkarte ist ein ziemliches Verwirrspiel bei der Konfiguration der Firewall. Besser ist es in solchen Fällen, zumindest eine zweite Netzwerkkarte lediglich für DSL in den PC zu stecken und nach Möglichkeit das DSL-Modem direkt anzuschließen.

Traumatisches

Bliebe noch eine Bemerkung zu den Merkwürdigkeiten, die es in Windows-Netzen immer wieder gibt: Rechner A redet mit B, aber B nicht mit A. In einer Richtung fließen die Daten mit erwartetem Tempo, aber beim Kopieren auch großer Dateien in anderer Richtung kleckern die Daten nur. Hier kann man nur versuchen, systematisch defekte Hub/Switch-Ports auszuschließen und Patch-Kabel auszutauschen sowie die eventuell aktive Firewall mal versuchsweise vorübergehend abzuschalten.

Bei Performance-Problemen könnte auch die Historie des PC eine Rolle spielen: Lief das System zunächst nur allein mit einer ISDN-Verbindung zum Provider? Falls ja, könnten sich Optimierungen am IP-Stack negativ auf den LAN-Betrieb auswirken. Der Einsatz von Software, die die Detailkonfiguration beeinflusst, mag sie auch generell nicht unbedingt empfehlenswert sein, könnte hier einfach Aufschluss liefern (etwa das über den Soft-Link erreichbare Dr. TCP). (ps)

Literatur

[1] englischsprachiger Artikel in der Microsoft-Knowledgebase mit Details zum Suchdienst: http://support.microsoft.com/default.aspx?scid=kb;en-us;188001

[2] Karlheinz Blank, Immer und überall, Offline-Dateien unter Windows 2000, c't 3/01, S. 202

[3] Axel Vahldiek, Selbstschutz, Das Sicherheitskonzept von Windows 2000 und XP, c't 15/04, S. 110

[4] Peter Siering, Der Pinguin serviert, Server-Selbstbau mit Linux, c't 23/02, S. 200 und diverse Folgeartikel

Soft-Link 0424112 c't

Peter Siering

Stellwerk fürs Netz

Die Windows-Server-Welt

Wer sich mit Windows-Vernetzung beschäftigt, stolpert früher oder später zumindest über Begriffe, die nur in der Welt der Windows Server eine Bedeutung haben. Hier erfahren Sie, was davon womöglich wichtig ist und was Ihnen ohne „echten" Windows Server entgeht …

Ein einfaches Windows-Netzwerk ist schnell aufgebaut, doch dabei bleiben Fragen offen: Welche IP-Adresse ist in das Feld WINS einzutragen? Was kann ich mit Gruppenrichtlinien im lokalen Netz erreichen? Woher erfährt die Workstation den Weg ins Internet? Ab wie vielen PCs lohnt sich ein Server? Reicht eine Arbeitsgruppe oder brauche ich eine Domäne?

Der Einsatz eines Servers im Netz bringt viele Vorteile mit sich, die sich erst erschließen, wenn man mehr über die einzelnen Funktionen weiß, die eine aktuelle Serverversion von Windows bietet. Ein Gutteil der Vorteile ist aber nicht an ein Produkt aus Redmond gebunden, sondern lässt sich gut auch mit den Alternativen umsetzen, etwa Samba.

Einer für alle

Der wohl grundlegendste Vorteil eines Servers im Netz besteht darin, dass er eine zentrale Datenbank führt, in der alle bekannten Benutzer eingetragen sind. Statt für den Benutzer Armin, der auf einem Rechner arbeiten, aber auf einen weiteren übers Netz zugreifen soll, auf beiden ein Konto einrichten zu müssen, genügt es, dieses Konto einmal auf dem Server einzurichten.

Der Server spielt dabei eine besondere Rolle, die in der Windows-Welt „Domänencontroller" (DC) heißt. Er stellt damit eine übergeordnete Verwaltungsinstanz für das Netzwerk dar: Ihm ist nicht nur jeder Benutzer bekannt, sondern auch jedes System im Netz, das zur Domäne gehört, also seiner Benutzerdatenbank vertraut – ein System muss, um sich zu einer Domäne zugehörig zu fühlen, dort explizit eingetragen werden.

Das Eintragen in eine Domäne geschieht ähnlich wie das Festlegen eines Namens für die Arbeitsgruppe. Man gibt den Namen der Domäne an und wird anschließend aufgefordert, sich gegenüber dem Domänencontroller mit einem Konto mit Domänenadministratorrechten nebst Passwort auszuweisen. Durch diesen Schritt vertrauen Server und Workstation einander (hinter den Kulissen wird ein unsichtbares Konto für die Workstation in der Domäne eingerichtet). Fürderhin können sich an die Workstation Benutzer anmelden, die kein lokales Konto dort haben, aber eines in der Domäne.

Wenn man anschließend Freigaben auf der Workstation einrichtet, so kann man bei der Vergabe von Rechten für den Zugriff darauf auf die Liste der Nutzerkonten aus der Domäne zurückgreifen. Automatisch erhalten Administratoren aus der Domäne volle Rechte auf der Workstation, so wie sie ein lokal an die Workstation angemeldeter Administrator genießt. Ein Administrator kann dadurch immer noch an lokal gehaltene Daten heran, wenn der Benutzer womöglich nicht erreichbar ist, ohne erst mühsam in das System einbrechen zu müssen.

Den Beitritt in eine Domäne unterstützt aber längst nicht jede Windows-Fassung: XP Home kann einer Domäne nicht wirklich beitreten. Das heißt, es kann zwar auf Freigaben einer Domäne zugreifen, so zur Anmeldung an diese Ressourcen ein gültiges Konto in der Domäne angegeben wird, aber an das System selbst können sich nur lokal bekannte Nutzer anmelden. Auch 9x/ME können auf Domänen-Ressourcen zugreifen, obwohl sie keine lokale Benutzerdatenbank unterhalten, beitreten können sie einer Domäne ebenso wenig.

Alle für einen

Mit dem Einrichten einer Domäne, meist also dem ersten Server im Netz, gehen eine ganze Reihe von weiteren Umstellungen einher: Während in einer Arbeitsgruppe die Rechner sich einigen, wer die verfügbaren Ressourcen verwaltet (Suchdienst), nimmt diese Rolle dann der Domänencontroller wahr. Wenn er das in einem größeren Netz auch nicht allein tut, so spielt er dabei doch die erste Geige und verwaltet die übergreifend gültigen Listen als „Master-Browser".

Besteht ein Netzwerk nur aus Arbeitsgruppen, so findet die Namensauflösung, also das Übersetzen von Namen in IP-Adressen, etwa beim Zugriff auf die Freigabe \\hannes\bilder mittels Rundrufen („Broadcasts") statt. Der anfragende Rechner ruft einfach ins Netz: Wie lautet die IP-Adresse von „hannes" und er-

hält – hoffentlich – die Antwort. Schnell wirken solche Rundrufe als Performance-Killer im Netz und sie haben auch Grenzen, wenn ein logisches Netzwerk nicht mehr aus nur einer Broadcast-Domain (sprich einem IP-Netz), sondern mehreren besteht.

Abhilfe für IP-basierte Netze vergangener Tage bestand darin, einen speziellen Namensdienst zu schaffen. Er sollte als NetBIOS-Nameserver von jedem System eine Registrierung entgegennehmen (ich heiße „faxserver" und habe die Adresse …) und auf Anfragen wieder ausspucken. Bei Microsoft heißt die Implementierung des Dienstes WINS (Windows Internet Name Service) und ist inzwischen überholt – gleich mehr dazu, warum das so ist.

WINS spielt in heutigen Netzen aber durchaus noch eine Rolle. Wenn man mit älteren Windows Servern – etwa NT4 – oder Alternativen wie Samba arbeitet, macht das Aufsetzen eines WINS-Servers Sinn. Er optimiert und beschleunigt nicht nur die Namensauflösung, sondern hilft auch der Suche nach Computern oder Arbeitsgruppen über die Netzwerkumgebung auf die Sprünge. Voraussetzung ist neben einem WINS-fähigen Server, dass die Clients die Adresse des WINS-Servers erfahren; sie registrieren sich dann dort und befragen den Server automatisch.

WINS++ = DDNS

Der Weisheit letzter Schluss ist WINS aber nicht: Es führt in bestehenden IP-Netzen einen zweiten Namensdienst neben dem für Zugriffe ins Internet üblichen DNS (Domain Name System) ein. DNS verwandelt Namen wie „www.heise.de" in IP-Adressen. Entsprechend ist Microsoft mit Windows 2000 Server dazu übergegangen, die Aufgaben von WINS an DNS zu übertragen. Wenn in einem Netz nur moderne Clients (2000 und XP) laufen, kann man sich WINS und die NetBIOS-Namensauflösung komplett sparen.

Mit der Umstellung gehen weitere Änderungen einher, die Microsoft mit Windows 2000 Server eingeführt hat: Der DNS-Dienst arbeitet nicht, wie im Internet üblich, nahezu statisch, sondern dynamisch. Das heißt, Namen und Adressen der Clients werden automatisch ein- und ausgetragen und sind nicht etwa vom Administrator von Hand zu pflegen. Entsprechend steht der Microsoft-Implementierung das D für „Dynamic DNS" zu.

Ist ein System Mitglied in einer Domäne, kann der Benutzer beim Anmelden auswählen, ob er sich lokal oder in der Domäne anmelden möchte.

Das perfekte Umfeld für einen Domänencontroller seit Windows 2000 besteht aus einer ganzen Familie von Diensten, die alle zwar das Wort Server ziert, die aber sehr wohl auf einem System laufen können: Der DDNS-Dienst ist unverzichtbar, da moderne Clients darüber unter anderem den Domänencontroller orten. Er ist von so zentraler Bedeutung, dass sich die meisten Fehlfunktionen des Active Directory auf Konfigurationsfehler im DDNS zurückführen lassen.

Ein DHCP-Server (Dynamic Host Configuration Protocol) ist nötig, damit die Clients überhaupt IP-Adressen erhalten und dabei auch gleich die Adressen des Gateways und des (D)DNS-Servers erfahren. Von Hand will heute niemand mehr diese Informationen an die Clients ausbringen. Auch findet eine Abstimmung zwischen DHCP und DDNS statt.

Bevor sich das Folgende aber den höheren Weihen der Windows-Vernetzung mit dem von Windows 2000 Server eingeführten Verzeichnisdienst „Active Directory" zuwendet, geht es noch kurz auf wichtige Aspekte beim Betrieb eines Domänencontrollers ein. Die betreffen zwar nur ältere Serverversionen, helfen aber einerseits beim Verstehen der Alternativen wie Samba und erklären andererseits viele Neuerungen des Active Directory.

Alt versus Neu

NT4 kannte für die Verwaltung eines Netzes eine Domäne. Wenn Netze sehr groß wurden, war ein Domänencontroller mitunter schon überfordert, die Benutzer zu authentifizieren, im Extremfall sogar die Anzahl überhaupt zu beherbergen. Als Ausweichmöglichkeit für ersteren Fall gab es so genannte Backupcontroller, die nur mit einer Kopie der Benutzerdatenbank arbeiten und bei den täglichen Aufgaben helfen, etwa der Authentifizierung.

Kapazitätsprobleme konnte man nur umgehen, indem man weitere Domänen (und damit Controller, also Server) in Betrieb nahm und mit so genannten Vertrauensstellungen untereinander dafür sorgte, dass Benutzer aus einer Domäne auch in einer anderen bekannt wurden. Es gab verschiedene Ansätze, diese Strukturen untereinander zu etablieren, aber das waren alles Krücken, mit denen Microsoft mit dem Active Directory gründlich aufgeräumt hat.

Selbst wer nicht an diese Grenzen stößt, ist trotzdem gut beraten, das Konzept zu kennen: Durch den Betrieb eines Backup-Domänencontrollers ist man nämlich in der glücklichen Lage, bei einem Ausfall des primären Controllers auf den Sicherungsserver umzuschalten und ihn vorübergehend alle Aufgaben übernehmen zu lassen. Ohne diese Absicherung würden womöglich alle Dienste im Netz brachliegen, bis der Controller wieder läuft.

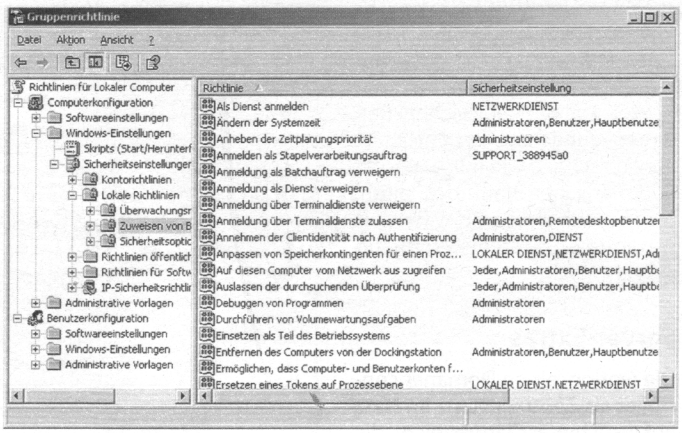
Die freie Software Samba [1], die als Windows Server unter GPL nicht unerheblich zum Erfolg von Linux auf Servern beiträgt, kann in der aktuellen Version 3 genauso arbeiten, wie es einst NT4 tat, kennt also das Konzept des primären und Sicherungscontrollers.

Schöne neue Welt

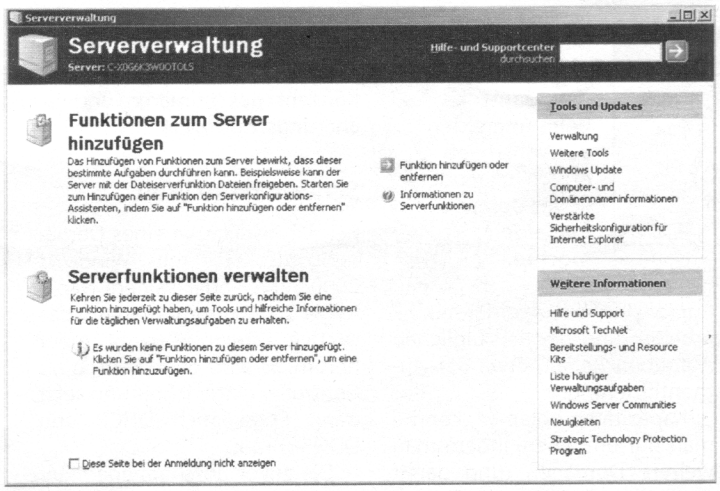
Bei der Installation eines Domänencontrollers mit Windows 2000 Server oder seinem Nachfolger 2003 kommt man um das „Active Directory" nicht mehr herum. Es wird beim Betrieb als Controller eingerichtet und setzt dann eben auch DHCP und DDNS voraus.

Die zuvor beschriebenen Einschränkungen, etwa was die Größe der Benutzerdatenbank angeht, sind damit gefallen. Es lassen sich mehrere Domänen auf mehrere Server verteilen – die relevanten Daten vervielfältigen die Server unter sich, ohne dass sich der Administrator darum kümmern müsste. Es gibt viele weitere erfreuliche Fortschritte, die im Detail zu beschreiben diesen Artikel sprengen würden. Ein älterer c't-Artikel zum Server 2000 hat sich damit im Detail auseinander gesetzt [2].

Es folgt aber noch ein Glanzlicht: Der Verzeichnisdienst dient nicht nur dazu, eine Liste von Benutzern und Gruppen aufzunehmen, sondern sie lassen sich in so genannte Organisationseinheiten (OUs) gliedern. Einer OU kann man dann über so genannte Gruppenrichtlinien bestimmte Rechte zuweisen oder absprechen, Windows-Einstellungen verordnen und sogar Software zuweisen [3]. Diese Art der Organisation eines Netzes ist mit NT4 oder Samba nicht so leicht möglich – allerdings will



In XP Professional verkümmert: Der Editor für die Gruppenrichtlinien läuft erst in einer Domäne mit Active Directory zur Hochform auf.



Die Konfigurationshelfer, die Microsoft seinen Servern beilegt, führen komfortabel und fast narrensicher durch wichtigste Konfigurationsschritte.

all der Umgang mit den Gruppenrichtlinie wohl überlegt und auch erst mal erlernt sein.

Wo Licht hinfällt, da ist auch Schatten: Anders als bei NT4 (oder Samba) mit der klaren Einteilung der Domänen-Controller in primäre und Sicherungsrolle, machen die neuen Server die Rollenverteilung unter sich aus. Das heißt, es ist nicht mehr so einfach, beim Ausfall des primären DC auf einen Sicherungs-DC umzuschalten – es geht, erfordert aber mehr Know-how.

All das klingt auf den ersten Blick mächtig kompliziert, aber wenn man von den Feinheiten der Konfiguration des Active Directory und den Details der Gruppenrichtlinien absieht, ist ein System mit Windows 2000 Server oder Server 2003 schnell am Start. Beim Einrichten der Domäne, sprich dem Active Directory, und den daran angeknüpften Diensten helfen Assistenten, die im Vergleich zu manchem Desktop-Helfer recht zielführend sind.

Wer auf die zahlreichen Beigaben zunächst verzichtet, ist ähnlich schnell wie mit NT4 – ein antiquarischer Kauf des alten, nicht mehr aktiv von Microsoft supporteten Systems empfiehlt sich also nicht.

Server-Extras

Die Option, einen Domänencontroller als Zentralinstanz im Netz aufzusetzen, ist längst nicht die einzige Funktion, die heutige Windows Server bieten. Microsoft hat sie mit vielen Extras angereichert: Recht bekannt ist noch der Internet Information Server, IIS, um Webserver aufzusetzen, um im Intra- oder Internet Webseiten anzubieten.

Weniger bekannt, aber sehr nützlich kann der Remote Access and Routing Service (RRAS) sein – ein stark aufgebohrtes DFÜ-Netz. Damit lernt Windows als Router zu agieren und bietet dafür eine ausgefeilte Bedienschnittstelle, um etwa Wählverbindungen einzurichten, die nur bei Bedarf geöffnet werden, oder aus dem Internet auf VPN-Verbindungen zu reagieren.

Ebenso spannend sind die Terminal-Services. Sie verwandeln das System in einen Applikationsserver: Office wird auf dem Server installiert und die Nutzer greifen über spezielle Terminal-Software darauf zu. Die Lösung hat verschiedene Vorteile: Der PC des Benutzers kann lahm sein, solange die Software zur Darstellung läuft, stört das nicht. Ein Benutzer kann aus der Ferne auch über eine ISDN-Leistung die Anwendungen benutzen.

Während für die Nutzung der Terminal-Services im beschriebenen Applikationsmodus zusätzliche Server-Lizenzen nötig sind, kann man sie für die Fernwartung eines Servers, zum Beispiel durch einen externen Dienstleister, kostenfrei einsetzen. Client-Software gibt es nicht nur für Windows, sondern auch für den Mac und für X11. Der Remote Desktop in XP Professional stammt von den Terminal-Services ab.

Servervarianten

Die Ausstattung der verschiedenen Serverversionen, die Microsoft im Angebot hat, weist viele Unterschiede auf. Je nach Preis nimmt die Anzahl der CPUs zu, die das Produkt unterstützt, kommen weitere Funktionen hinzu, etwa fürs Load Balancing, also die Lastverteilung von Diensten über mehrere Server. Ergänzende Produkte, die etwa Management- und Inventarisierungsfunktionen nachrüsten oder neue Anwendungswelten erschließen, bietet Microsoft extra an [4].

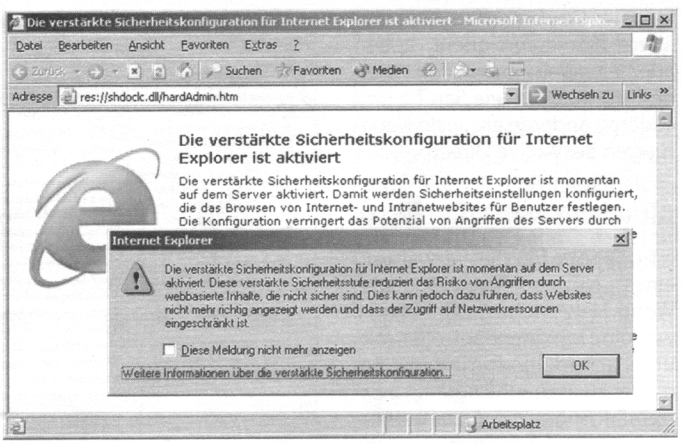
Für kleine Netze, die mit nur einem Server auskommen, scheinen all diese Angebote jedoch Overkill. Das weiß auch Microsoft und hat spezielle Schmankerl im Programm: Der Small Business Server 2003, den es auch in verschiedenen Versionen gibt. Die kleinste vereint in der Standardausgabe die Server Lizenz mit einer für Exchange. Außerdem fasst das Produkt die Assistenten zur Installation der Serverdienste zusammen, sodass der Käufer ein Rundumsorglos-Paket erhält, mit dem er ein kleines Netz fertig einrichten kann und sogar E-Mail, Terminplaner et cetera dazu bekommt.

E-Mail-Dienste gehören nur beim Small Business Server zum Lieferumfang. Der darin enthaltene Exchange-Server ist Microsofts Lösung für solche Aufgaben. Wer einen herkömmlichen Server erwirbt, muss das Paket also extra kaufen.

Der Small Business Server ist zwar preisgünstig, aber auch mit einigen Einschränkungen belegt: So gibt es eine Obergrenze für die maximale Anzahl der Benutzer, das Verzeichnis lässt sich nicht mit weiteren Servern erweitern und die Terminal-Dienste kennen keinen Applikationsmodus; wer mehr will, muss zur echten Serverversion greifen.

Der Preis für den Server allein macht es nicht: Microsoft legt allen Paketen nur ein bis zwei Hand voll so genannter „Client Access"-Lizenzen (CALs) bei. Wer mit mehr PCs Dienste des Servers nutzen will, muss nachordern. Die Bedingungen, was als Client gilt, bedarf einer genauen Betrachtung. Die Redmonder haben die Modelle immer mal wieder umgeworfen oder erweitert, etwa von einer Sicht auf Serververbindungen hin zu einer auf Benutzer; oft gibt es sogar mehrere Möglichkeiten, bis hin zu Versionsnummern für Lizenzen …

Der Gedanke, sich die Serverdienste mit Open Source ins Haus zu holen, liegt nahe, aber Microsoft argumentiert nicht zu unrecht mit dem zeitlichen Aufwand, der in einer solchen Lösung steckt. Wer mal einen Small Business Server installiert hat, dürfte einigermaßen verblüfft sein, wie schnell der Server eingerichtet ist. (ps)



Als Workstation eignet sich ein Windows Server kaum: Nur Domänenadministratoren können sich anmelden und haben wenig Freude mit dem auf sicher getrimmten Internet Explorer.

Literatur

[1] Home-Page des Samba-Projekts: www.samba.org

[2] Karlheinz Blank, Peter Siering, Eduard Zander, Server 2000, Windows 2000 Server, c't 10/00, S. 112

[3] Klaus Bierschenk, Gruppenzwang, Gruppenrichtlinien: Werkzeuge und Fehlersuche, c't 12/03, S. 226

[4] Webseiten von Microsoft zu der Server-Produktfamilie: www.microsoft.com/windowsserver c't