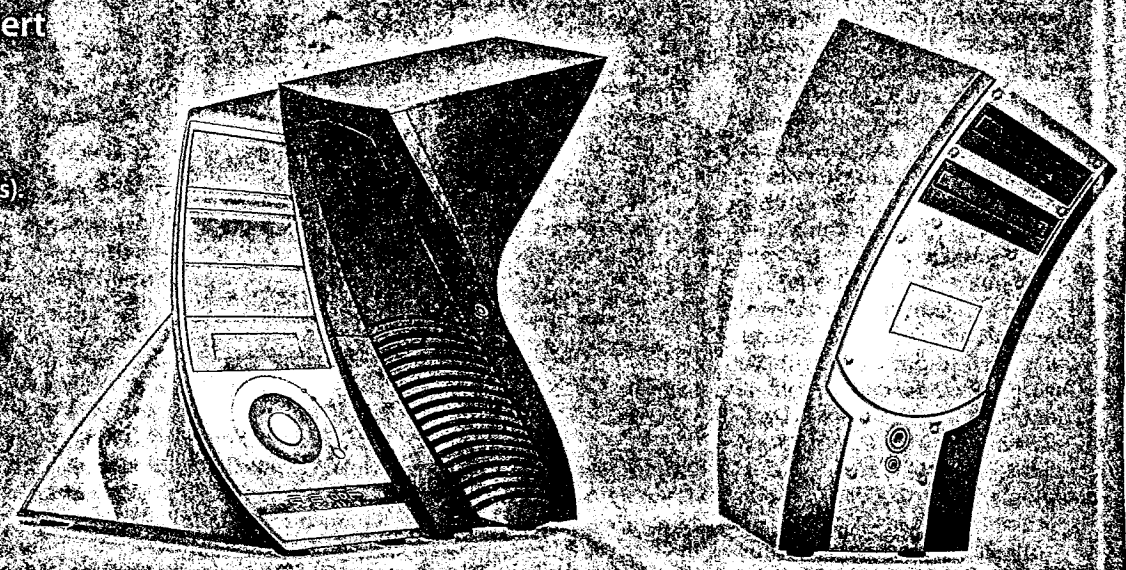
Reiko Kaps

LAN-Automatik zähmen

Wie Windows 7 Netze erkennt und einsortiert

Windows ab Vista sortiert einmal erkannte Netzwerke automatisch in Gruppen ein (Network Location Awareness). Anhand dieser Kriterien gewährt das Betriebssystem Zugriff auf Dienste und Anwendungen. Arbeitet der Windows-PC jedoch in einem Netz ohne Router, läuft die Automatik ins Leere – und blockiert unbelehrbar alle Zugriffe.



Eigentlich will Microsoft den Anwendern mit der Network Location Awareness (NLA) bei der Wahl der richtigen Einstellungen unter die Arme greifen: Vista und sein Nachfolger erkennen angeschlossene Netzwerke und sortieren sie in Kategorien, die das Betriebssystem beispielsweise zum Einstellen der Firewall auswertet.

Der wohl gut gemeinte Mechanismus hilft zwar Notebook-Nomaden, die häufig das Funknetz wechseln. Er stolpert aber bereits, wenn man zwei oder mehr Windows-7-Rechner nur über einen einfachen Switch vernetzt, was sich im Netzwerk- und Freigabecenter an der lapidaren Bemerkung „Nicht identifiziertes Netzwerk" bemerkbar macht. Obwohl dieses Netz nicht einmal einen Internetzugang besitzt, schottet sich Windows vollständig von anderen Rechnern im LAN ab. Die sonst gebotene Möglichkeit per Mausklick auf Heim- oder Arbeitsplatznetzwerk zu wechseln, verweigert das Betriebssystem dann beharrlich.

Andere PCs erreichen die Freigaben eines so abgeschotteten Rechners nicht, obwohl sie alle im gleichen Netzwerksegment liegen und am gleichen Switch hängen. Man könnte nun von Hand alle nötigen Ports in der Firewall freigeben. Doch scheidet diese Lösung spätestens dann aus, wenn der Rechner tatsächlich in einem öffentlichen Netzwerk etwa in einem Café, am Bahnhof oder in einem Rechenzentrum hängt. Die Folge wären unkontrollierte Zugriffe auf Windows-Dateifreigaben oder andere Dienste. Und die Firewall ganz auszuschalten, ist schlicht zu riskant.

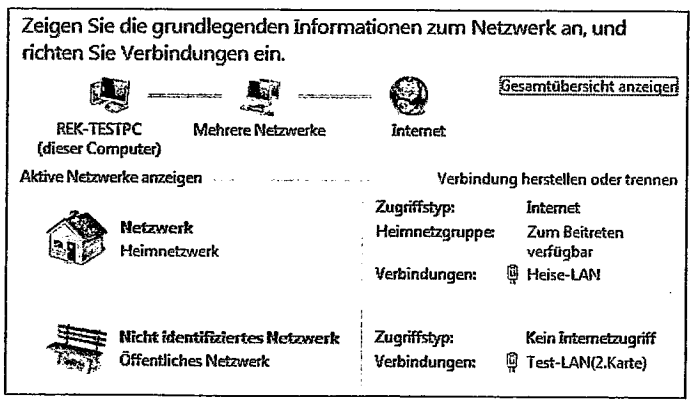
Netzwerk-Casting

Bereits seit Windows XP versucht Microsoft über den Dienst Network Location Awareness (NLA) die vorhandenen Netzwerke eines Rechners zu erkennen und einzuordnen. Unter XP überprüften diese Tests nur, ob ein oder mehrere Netzwerke momentan überhaupt aktiv sind, was Windows an angesteckten LAN-Kabeln oder den Kennungen von WLAN-Basisstationen abliest.

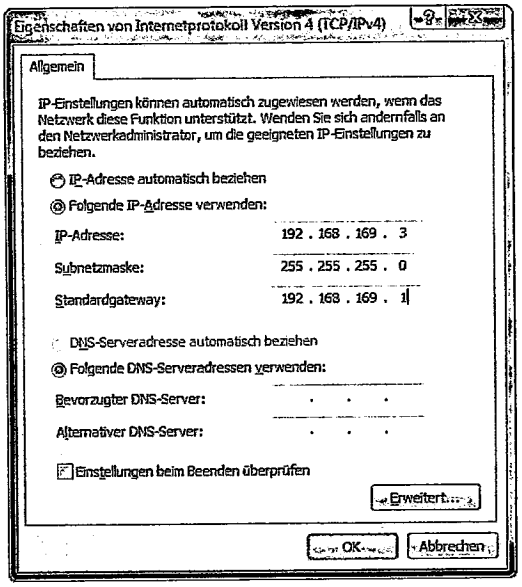
Seit Vista stellt Windows über die Erkenntnisse der Network Location Awareness jedoch die Firewall ein. Vista und Windows 7 unterscheiden dabei die vier Netztypen Öffentliches Netzwerk, Domänen-, Arbeitsplatz- sowie Heimnetzwerk

Gehört der PC zu einer Windows-Domäne, erkennen Vista und Windows 7 das verwaltete Netzwerk über die Erreichbarkeit des Domänen-Controllers und setzen die damit verbundenen Vorgaben automatisch. Macht die NLA ein nicht verwaltetes Netz aus, schlägt das Betriebssystem per Popup zunächst den Netzwerktyp „Öffentliches Netzwerk" vor. Per Mausklick wechselt man anschließend zum Heim- oder Arbeitsplatznetzwerk-Typ. Scheitert hingegen die Erkennung des LANs, lassen sich Vista und Windows 7 offenbar nicht davon abbringen, das Netzwerk als „Öffentliches Netzwerk" einzustufen.

Hängt der Rechner an einem Netz, das Windows oder der Benutzer als öffentliches Netz erkannt oder eingestuft hat, akti-



Einige Netzwerke behandelt Windows 7 immer wie öffentliche Netze – erst ein vermeintliches Gateway hilft dem Betriebssystem auf die Sprünge.



Eine per Ping erreichbare IP-Adresse im Feld Gateway überredet Vista und Windows 7 dazu, das angeschlossene Netzwerk als nicht öffentliches zu akzeptieren.

viert das Betriebssystem in der Firewall die Regeln für öffentliche Netzwerke, die fast jeglichen unverlangten Datenverkehr zum Rechner unterbinden.

Vista und Windows 7 nutzen das private Firewall-Profil bei Heim- und Arbeitsplatznetzwerken: Der Regelsatz lässt Verbindungen aus dem lokalen Netz zum Computer zu, sodass man den Rechner per ICMP (ping) erreichen, auf seine Freigaben zugreifen kann und er in der Netzwerkumgebung anderer Windows-Rechner auftaucht.

Erst Windows 7 trifft tatsächlich eine Unterscheidung zwischen Heim- und Arbeitsplatznetzwerk. Die schnelle und sehr einfache Vernetzung über eine Heimnetzgruppe funktioniert nur mit Rechnern, deren Netzwerkverbindung als Heimnetzwerk eingestuft wurde.

Netzwerk-Biometrie

Ein Domänennetzwerk erkennen Vista und sein Nachfolger am aktiven Domänen-Controller – also in der Regel an einem Windows Server. Er authentifiziert zentral Benutzer und Computer. Die Windows-Firewall besitzt für solche Netze ein eigenes Profil, das allerdings nur wenige Regeln umfasst.

Netze ohne Domänen-Controller (unmanaged) identifiziert das Betriebssystem hingegen über die Gateway-Adresse der jeweiligen Netzwerk-Schnittstelle: Das Gateway transportiert Netzwerkpakete weiter, deren Ziel nicht im eigenen lokalen Netz liegt. Zu Hause übernimmt meistens der eigene Router diese Aufgabe.

Die NLA erkennt das Gerät hinter der Gateway-Adresse anhand seiner Hardware-Kennung (MAC-Adresse), die es per ICMP und ARP herausfindet. Sofern sich die MAC-Adresse des Standard-Gatways nicht ändert, erkennt Windows 7 das Netzwerk sofort wieder, selbst wenn der verwendete Adressbereich im LAN (etwa von 192.168.111.x zu 192.168.169.x) wechselt.

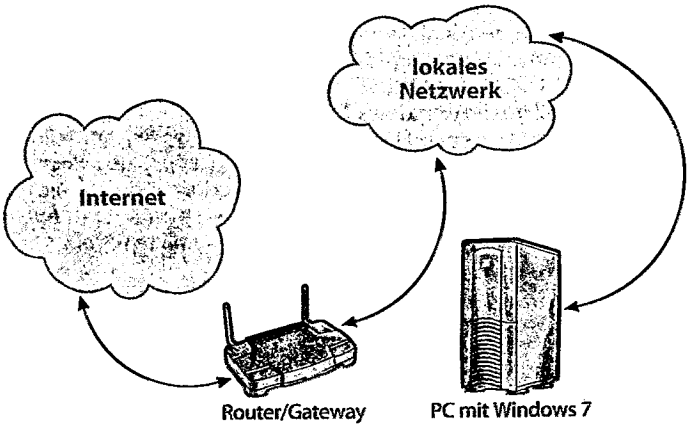
Vergibt man die IP-Adressen im LAN per Hand, lässt sich dieser Mechanismus auf einem Testrechner schnell nachprüfen. Dazu trägt man unter Gateway eine nicht aktive Adresse aus dem LAN-Bereich ein, schließt die Einstellungsdialoge und beobachtet das gleichzeitig geöffnete Netzwerk- und Freigabecenter. Nach einiger Zeit, in der Windows 7 das Netzwerk erneut identifiziert, wandelt sich die Verbindung vom Arbeitsplatz- oder Heimnetzwerk in ein öffentliches Netz, weil das Betriebssystem das Netz nicht identifizieren konnte. Gleichzeitig verschwinden die Möglichkeiten, Heim- und Arbeitsplatznetzwerk von Hand zu wählen.

Der Windows-7-Rechner in dem anfangs beschriebenen Netz aus einem Switch und zwei oder mehreren PCs benötigt also nur einen Gateway-Eintrag, der allerdings im Netzwerk tatsächlich erreichbar sein muss. Die eigene IP-Adresse akzeptieren die Vista- oder Windows-7-PCs nicht als Gateway-Eintrag. Bei zwei PCs nimmt man die Adresse des jeweils anderen Computers. Läuft in diesem LAN ständig ein Drucker oder Netzwerkspeicher, sollte man besser deren Adresse dafür nutzen – sie sind schließlich immer erreichbar.

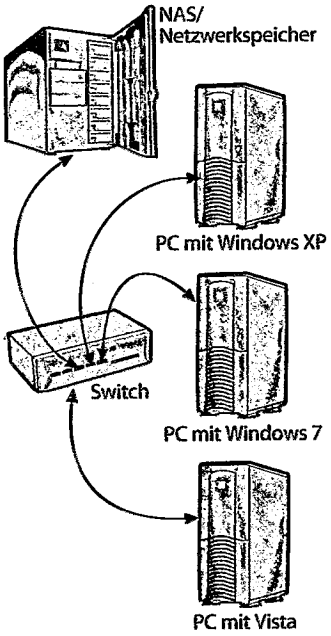
Öffnen Sie dazu den Punkt „Adaptereinstellungen ändern" im Netzwerk- und Freigabecenter. Ein Rechtsklick auf das Icon der betreffenden Netzwerkverbindung führt zu dessen Eigenschaften. Dort fördert ein Doppelklick auf „Internetprotokoll Version 4 (TCP/IPv4)" die nötigen Eingabefelder für die manuelle Vergabe der IP-Adresse und des Standard-Gateways zu Tage. Hat man einen alten oder einen Billig-Router übrig, kann auch er die IP-Adressen und das „vorgetäuschte" Gateway automatisch per DHCP verteilen.

Scharade

Setzt man den Gateway-Trick auf Rechnern ein, die über zwei Schnittstellen in zwei Netzen



Die Network Location Awareness unter Windows 7 braucht zwingend einen Router (Gateway), um das Netzwerk einzuordnen und wiederzuerkennen.



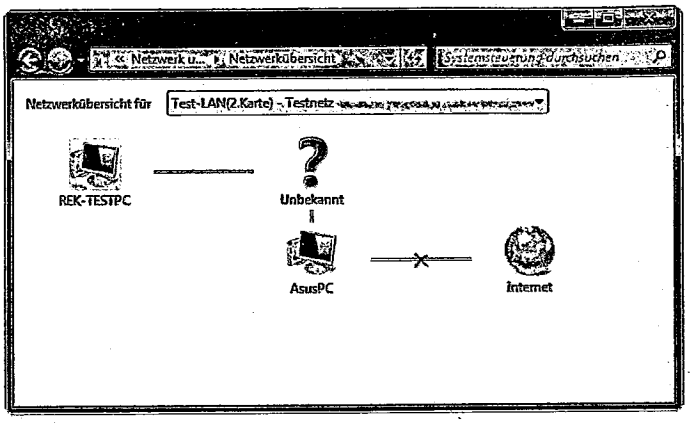
Fehlt ein Router im Netz, behandeln Vista und Windows 7 das LAN immer als öffentliches Netz und blockieren automatisch eingehende Verbindungen.

hängen (dual-homed), können jedoch Probleme auftauchen. Solche Konstruktionen setzen Profis gerne ein, wenn der Rechner über die zweite Karte etwa auf Netzwerkspeicher oder Datenbanken zugreift, die aber aus Sicherheitsgründen in einem separaten Netz arbeiten sollen.

Über seine erste Netzwerkkarte kennt der Rechner bereits ein Standard-Gateway. Trägt man für das Netz an der zweiten Schnittstelle eine Gateway-Adresse ein, landet diese anschließend ebenfalls in der Routing-Tabelle.

Diese Gateway-Einträge lassen sich über das Kommando `route print -4` für das IPv4-Netzwerk herausfinden. Windows wertet Einträge als Standard-Routen, deren Netzwerkziel und Netzmaske die Werte 0.0.0.0 sowie in der Spalte Gateway eine IP-Adresse besitzen.

Zwei gleichwertige Standard-Routen könnten bei der Auslieferung von Netzwerkpaketen Verwirrung stiften. Der zusätzliche Eintrag unterscheidet sich jedoch von der echten Standard-Route in einem Punkt: Der Metrik-Wert ist deutlich höher (siehe Bild auf S. 98). Die Metrik einer Netzwerk-Route beschreibt die Kosten respektive den Aufwand, den dieser Netzwerkweg verursacht: Liegt die Metrik der Route niedriger als bei anderen,



Ein vorgetäuschtes Gateway verwirrt die Netzwerkübersicht unter Vista und Windows 7 etwas.

bevorzugt das Betriebssystem diesen Weg.

Den Metrik-Wert für die Standard-Route (Gateway) legt Windows per Vorgabe automatisch fest. Die Standard-Route für die erste Netzwerkverbindung hat Windows als sehr günstig (10) eingestuft, offensichtlich eine Folge der erkannten Internetverbindung. Die Metrik der „vorgetäuschten" Standard-Route über die zweite Netzwerkkarte bewertet das Betriebssystem als extrem hoch (276), schließlich findet das Betriebssystem hier keinen Weg ins Internet. Andere Betriebssysteme können daher auf diese Route verzichten. Ohne sie erkennen Vista und Windows 7 jedoch nicht das angeschlossene Netz, was einige Anwender als Fehler ansehen.

Zusätzlich lässt sich über den Einrichtungsdialog „Erweiterte TCP-Einstellungen" in den Adaptereinstellungen auch ein Basiswert für die Metrik vorgeben. Zu dieser Zahl addiert Windows allerdings immer etwas hinzu, sodass der tatsächliche Metrik-Wert in der Routing-Tabelle etwas höher ausfällt. Durch die Bewertung der Routen erreichen die Netzwerkpakete immer auf dem schnellsten, also günstigsten Weg ihr Ziel. Es sei denn, die Internetverbindung über diese Route streikt oder stockt.

Aktenlage

Einmal erkannte Netze speichert Windows und benennt sie mit dem wenig aufschlussreichen Namen „Netzwerk" und einer fortlaufenden Nummer, den es gemeinsam mit einem Icon im Netzwerk- und Freigabecenter anzeigt. Bei WLANs übernimmt Windows die ausgestrahlte Funkzellen-Kennung (SSID), arbeitet es als Domänen-Mitglied, setzt die NLA hier den DNS-Suffix ein.

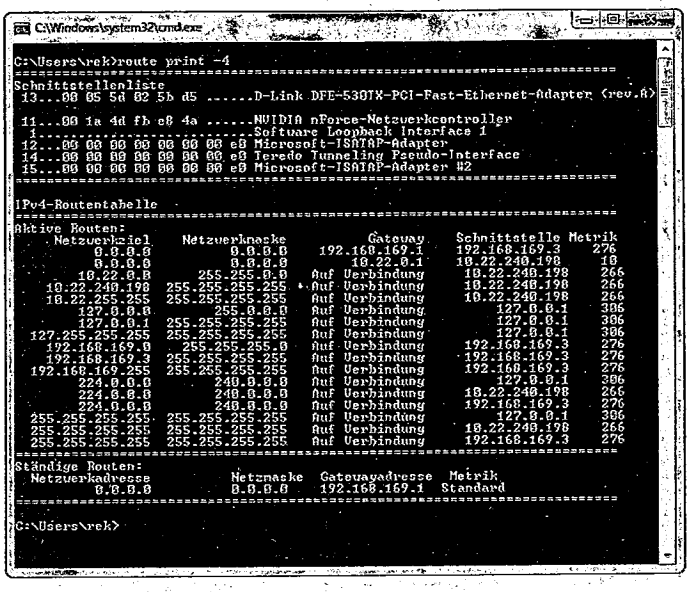
Name und Icon des aktiven Netzwerk-Profils lassen sich jedoch auch ändern. Den Dialog für das gerade aktive NLA-Profil erreicht man über einen Mausklick auf das Netzwerk-Icon im Netzwerk- und Freigabecenter. Die in diesem Fenster aufgelistete Funktion „Netzwerk zusammenführen und löschen" führt entweder ein aktives Profil mit einem anderen, derzeit nicht verwendeten zusammen oder löscht letztere aus der Liste. Die Namen der momentan nicht genutzten Profile verändert das c't-Hilfsmittel „Netzwerk umbenennen.exe" (siehe c't-Link).

Will man sich die Zuordnung zwischen Gateway-MAC und Profil genauer ansehen, ruft man im Programm regedit den Zweig „HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" in der Windows-Registry auf. Die passenden Signaturen respektive die MAC-Adressen lagert Windows in den Schlüsseln „Managed" und „Unmanaged" unter „HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures". Dort verweist der Wert ProfileGuid auf das passende NLA-Profil, dessen Details Windows auf der gleichen Registry-Ebene im Schlüssel Profiles sichert. (rek)

Literatur

[1] Ernst Ahlers, Trennschärfe, Lokale Netze mit einer Router-Kaskade trennen, c't 6/10, S. 148

www.ct.de/1009096



Wenn zwei Standard-Routen vorhanden sind, gibt das Betriebssystem der Route mit der niedrigeren Metrik den Vorrang.

Windows-Schutzwall

Die Regeln in der Windows-7-Firewall können den drei Profilen Privat, Domäne und Öffentlich angehören. Das passende Firewall-Profil wählt Windows über den von der NLA erkannten Netzwerktyp und bereitet damit den Rechner beispielsweise auf den Einsatz in einer Heimnetzgruppe vor.

Das öffentliche Firewall-Profil blockiert den Zugang zu den eigenen Datei- und Druckerfreigaben und die Freigabe über Homegroups – und schottet damit den Rechner sicher vor fremden Zugriffen beispielsweise an einem WLAN-Hotspot ab. Das Profil Privat erlaubt hingegen die allermeisten Zugriffe aus dem lokalen Netzwerk, sodass Windows-Rechner in Heim- und Arbeitsplatznetzwerken untereinander Freigaben erreichen und auf Pings (ICMP) antworten können. Gehört der Rechner einer Windows-Domäne an, aktiviert die Firewall die Regeln aus dem Domänen-Profil.

Eigene Profile lassen sich in der Windows-Firewall nicht einrichten, jedoch eigene Regeln, die sich den genannten Profilen zuordnen lassen. So fragt Windows nach dem Start eines Netzwerkprogramms per Popup-Fenster nach, ob das Programm von außerhalb erreichbar sein soll und auf welchen Netzwerktyp sich diese Vorgabe bezieht. Hat man den Zugriff erlaubt, erweitert das Betriebssystem die Firewall um zwei Regeln, die Zugriffe über alle TCP- und UDP-Ports von außerhalb auf das jeweilige Programm gestatten. Die Einstellungen lassen sich jedoch weiter eingrenzen – etwa auf Adressbereiche, Netzwerkgeräte-Typ und Port-Nummern. Wer beispielsweise den Zugriff auf einen Webserver nur im Büro und zu Hause von ganz bestimmten IP-Adressen erlauben will, kann das in der erweiterten Windows-Firewall sehr genau vorgeben.

In der „Windows-Firewall mit erweiterter Sicherheit" lassen sich die Vorgaben für ein- und ausgehende Verbindungen überprüfen und anpassen. Die gerade aktiven Regeln zeigt das Programm unter dem Punkt „Überwachung, Firewall" recht übersichtlich an, bearbeiten lassen sie sich über diese Ansicht allerdings nicht. Dazu wechselt man zu den ein- oder ausgehenden Regeln, markiert den entsprechenden Eintrag und aktiviert über das rechte Menü oder einen Rechtsklick dessen Eigenschaften.

c't