Konfiguration von Netzen in virtualisierten Umgebungen

# Fein gestrickt

Sven Ahnert

In Laborumgebungen sind virtuelle Maschinen und im produktiven Umfeld längst etabliert. Wer komplexere Testszenarien möchte oder im Rechenzentrum virtuelle Server ins LAN integrieren will, muss sich mit der speziellen Vernetzung auseinandersetzen.

Virtuelle Netze bieten mehr Varianten bei der Konfiguration als die physische Verkabelung, werfen aber umso mehr Fragen auf: Produktive virtuelle Server müssen als Plattform auf allen Ebenen im LAN ansprechbar sein, möglichst mit redundanter Anbindung. Für Testumgebungen steht dagegen das Abschotten eines Netzsegments im Vordergrund, idealerweise hinter einer Firewall. Ein Entwickler will auch unterwegs auf seinen virtuellen SQL-Server zugreifen, und seine virtuelle Maschine (VM) wiederum soll die UMTS- oder ISDN-Verbindung des Host ins Internet nutzen können. Für solche Anforderungen existieren mehrere Lösungen.

In diesem Beitrag geht es um die Konzepte virtueller Netze, vom virtuellen Switch bis zur MAC-Adresse, und Tipps zum praktischen Einsatz. Als Beispiel dient VMwares Server, weil er umfangreiche Netzwerkoptionen bietet und für jedermann kostenlos verfügbar ist. Alle Aussagen gelten ebenso für VMwares Workstation. Wenn nötig, geht der Beitrag auf die Besonderheiten des kommerziellen ESX Server von VMware und Microsofts kostenlosen Virtual Server/PC ein.

Alle Virtualisierungsprodukte ähneln sich im grundsätzlichen Aufbau und fast sämtliche Elemente eines physischen Netzes tauchen in der virtuellen Welt auf (siehe Abb. 1).

## Mit Netz und ohne Kabel

Eine VM besitzt emulierte Netzwerkadapter, die an virtuellen Switches (vSwitch) angeschlossen sind. Alle VMs mit Adaptern am gleichen vSwitch bilden ein Subnetz und kommunizieren darüber untereinander. Die Subnetze sind voneinander isoliert, lassen sich aber mit einer VM als Router koppeln.

Ein virtueller Switch (vSwitch) existiert nur als Software auf dem Host und trennt das virtuelle Netz vom physischen. Als Uplink zum LAN dient ein Bridge-Protokoll, das den Verkehr des vSwitches bei Bedarf über eine physische Netzwerkkarte tunnelt. Ob ein Gastsystem isoliert bleibt oder mit physischen Maschinen kommunizieren kann, hängt in erster Linie von der Konfiguration des vSwitches ab.

VMwares Server stellt jeder VM bis zu vier virtuelle Netzkarten zur Verfügung, die der Anwender über „VM -> Settings -> Hardware“ zuweisen oder entfernen kann. Die Software emuliert jeden NIC vollständig, unabhängig von der tatsächlich eingebauten Hardware. VMs können für Testzwecke sogar völlig ohne physische Adapter in virtuellen Netzen Daten austauschen.

Standardmäßig emuliert VMware einen PCNet Adapter von AMD, für den fast jedes OS Treiber mitbringt. Dank Plug & Play installiert das Gastsystem den Treiber automatisch, ohne einen Unterschied zu realer Hardware festzustellen. Alle Protokolle, etwa TCP/IP oder IPX/SPX, funktionieren wie gewohnt. Sind VMwares Tools im Gast installiert, ersetzen sie den Standardtreiber mit einem optimierten „VMware Accelerated AMD PCNet Adapter“. Er bietet eine bessere Leistung bei Gigabit-Ethernet und entlastet die Host-CPU. Daneben emuliert VMware in 64-Bit-Gästen einen Intel PRO/1000 Adapter, für den viele Gast-OS einen 64-Bit-Treiber liefern.

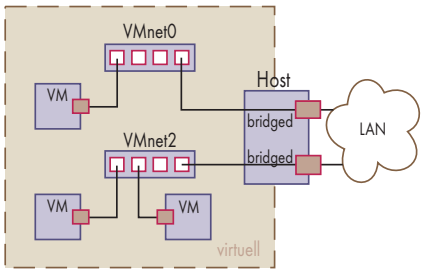



**Abbildung: Die meisten Komponenten von physischen Netzen haben ihre Pendants im Virtuellen (Abb. 1).**

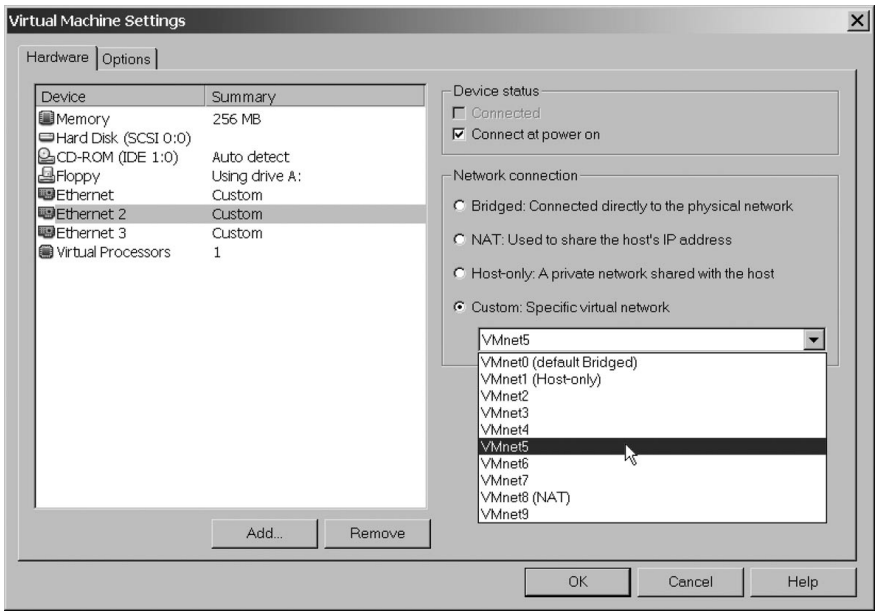
Die Anzeige der LAN-Geschwindigkeit im Gast ist übrigens rein kosmetisch. Beim Standard-Treiber beträgt sie immer nur 10 MBit/s, obwohl das System die verfügbare Geschwindigkeit der physischen Verbindung ausnutzt. Der optimierte Treiber zeigt dagegen immer 1 GBit/s an, selbst wenn der physische Link maximal 100 MBit/s schnell ist.

Um die Adapter der VMs untereinander zu verbinden, liefert VMware insgesamt zehn virtuelle Switches, die es VMnet0 bis VMnet9 nennt. Der Anschluss eines virtuellen Adapters geschieht entweder über das Menü „VM -> Settings -> Hardware“ (Abb. 2) oder einfacher über das kleine Netzwerksymbol in der Statusleiste einer laufenden VM (Abb. 3). Änderungen der VMnet-Zuordnung sowie das Trennen und Verbinden des Adapters können im laufenden Betrieb erfolgen, für das Gastsystem entspricht das dem Umstecken eines Patchkabels.

VMware bietet drei Voreinstellungen für jeden Adapter: „Bridged“, „Host-only“ und „NAT“. Sie dienen der intuitiveren Bedienung, verbergen aber die dahinterliegenden Funktionen vor dem Anwender. Zum tieferen Verständnis eignet sich die Custom-Einstellung, die letztendlich alle Modi abbildet. Eine Listenauswahl unter Custom schließt den Adapter an einen virtuellen Switch (VMnet) an, wodurch er sofort mit anderen VMs am gleichen VMnet kommunizieren kann (Abb. 1).

Ob Pakete das virtuelle Netz verlassen, entscheidet die Konfiguration unter „Host -> Virtual Network Settings -> Host Virtual Network Mapping“ (Abb. 4). Auf einem Linux-Host fehlt das Menü, die Konfiguration erfolgt dort über das Skript *vmware-config.pl*.

VMnets stehen meist standardmäßig auf „Not bridged“ und bilden isolierte Netzwerke. Sobald jedoch einem ein physischer Adapter des Host zugewiesen ist, hält es mitsamt seiner VMs eine Verbindung zum LAN.

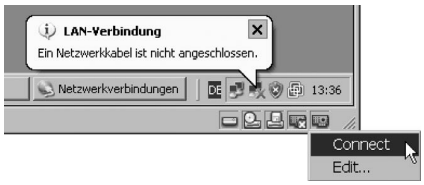



**Netzwahl: Über die VM-Settings kann der Admin die virtuellen Netzwerkkarten „Ethernet“ mit den virtuellen Netzen „VMnet“ verbinden (Abb. 2)...**

VMnet0 hat standardmäßig eine Verbindung mit dem ersten verfügbaren physischen Adapter des Host, zu sehen am Eintrag „Bridged to an automatically chosen adapter“. Anstelle der Automatik kann der Anwender aus der Liste zum VMnet eine physische Netzwerkkarte explizit wählen. Mehrere physische Adapter lassen sich unterschiedlichen VMnets zuweisen (in Abb. 4, VMnet2 und -3), etwa zur Lastverteilung oder zum Anschluss separater LAN-Segmente.

## Die Brücke zur Matrix

Das sogenannte „VMware Bridge Protocol“ regelt den Transport der Pakete von der virtuellen in die physische Welt. In der Netzwerkkonfiguration auf dem Host bedient es alle physischen Adapter (Abb. 5) und in deren Einstellungen ist das zugewiesene VMnet ersichtlich. Das Bridge-Protokoll versetzt




**... oder per einfachem Klick auf das Symbol für die LAN-Verbindung unter Windows einrichten (Abb. 3).**

die physische Netzwerkkarte in den Promiscuous Mode, sodass sie auch Pakete annimmt, die nicht für die eigene MAC-Adresse bestimmt sind. VMware kann somit den LAN-Verkehr abhören und ins VMnet weiterleiten. Umgekehrt tunnelt das Bridge-Protokoll den Verkehr des VMnets auf die physische Netzwerkkarte. Alle VMs treten dadurch im LAN als unabhängige Clients mit eigener MAC-Adresse auf, parallel und unabhängig vom Host.

Eine Besonderheit bieten die beiden virtuellen Switches VMnet1 und VMnet8. Ihnen sind zwei logische Netzwerkkartentreiber zugewiesen, die VMware während der Installation auf dem Host einrichtet. Sie erscheinen in der Netzwerkkonfiguration des Host als „VMware Network Adapter VMnet1 (Host-only)“ und „VMware Network Adapter VMnet8 (NAT)“. Aus Sicht des Host handelt es sich um normale Netzwerkadapter, allerdings sind sie nicht an einen physischen Switch, sondern an ein VMnet angeschlossen. Damit kommuniziert der Host direkt mit den virtuellen Netzen, auch ohne physischen Link.

### iX-TRACT

- Virtuelle Netze, die Verbindungen zwischen Virtual Servern herstellen, bieten mehr Flexibilität als physische.
- Auf einem System lassen sich von der Außenwelt abgeschottete Subnetze konfigurieren, was unter anderem für Testumgebungen gefragt ist.
- Mit virtuellen Maschinen und Netzen können Anwender Techniken wie Lastverteilung und Hochverfügbarkeit implementieren.
- Wer will, kann seine virtuelle Server-Frames auf seinem Laptop mit auf die Reise nehmen und an beliebigen Orten in Betrieb nehmen.

Beispielsweise deaktiviert Windows XP bei abgezogenem Patchkabel die Netzwerkkarte auf dem Host, wodurch eine Bridged-Verbindung ihren Kontakt zu den VMs verlieren würde. Mit einer Host-only Verbindung gelingt der Zugriff auf die VMs auf dem Laptop immer, auch unterwegs.

Der Verkehr über die logischen Adapter ist nicht grundsätzlich isoliert. Mit den richtigen Routing-Einträgen könnte ein LAN-Client über den Host das interne Test-Netzwerk erreichen. Unter „Host -> Virtual Network Settings -> Host Virtual Adapters“ lassen sich weitere logische Adapter definieren, was aber in der Praxis selten notwendig sein dürfte.

Zusätzlich läuft im VMnet1 und VMnet8 ein virtueller DHCP-Server für die Gäste. VMware konfiguriert die beiden logischen Host-Adapter mit der ersten IP-Adresse aus dem DHCP-Bereich. Holt ein Gast im VMnet1 oder VMnet8 seine IP-Konfiguration per DHCP, funktioniert die Kommunikation mit dem Host auf Anhieb. Den internen IP-Bereich kann der Anwender bei Bedarf über den kleinen Pfeil rechts neben jedem VMnet anpassen (siehe Abb. 5).

Über den Reiter „DHCP“ der Virtual Network Settings lässt sich bei Bedarf für jedes VMnet ein DHCP-Server einschalten, aber Vorsicht: Ein virtueller DHCP-Server in einem bridged VMnet liefert Adressen auch ins physische LAN. Da das nicht sein muss, sollte man virtuelle Server mit unveränderlichen festen IP-Adressen konfigurieren.

Im VMnet8 läuft als weiterer Dienst ein Software-Router, der die „Network Address Translation“ (NAT) beherrscht. Damit kommunizieren die Gäste unter der Identität des Host, ähnlich wie hinter einem DSL-Router, der für mehrere PCs die gleiche öffentliche IP nutzt. Damit die VMs den virtuellen NAT-Router als Default-Gateway verwenden, verteilt der DHCP-Server im VMnet8 diese Einstellung gleich mit.

## Im praktischen Einsatz

Gäste im VMnet8 benötigen deshalb nur eine interne IP. So kann ein Gast etwa den aktiven UMTS- oder ISDN-Zugang eines Laptops ohne Weiteres mitverwenden. Genauso greift eine Test-VM auf das LAN zu, ohne selbst sichtbar zu sein. Ein Nachteil von NAT ist, dass beispielsweise ein virtueller SQL-Server vom LAN aus unerreichbar bleibt. Dazu kann man zwar unter „Virtual Network Settings -> NAT -> Edit- > Portforwarding“ für bestimmte Ports eine Weiterleitung (PortForwarding) konfigurieren, sinnvoller ist für solche Fälle aber eine Bridged-Verbindung.

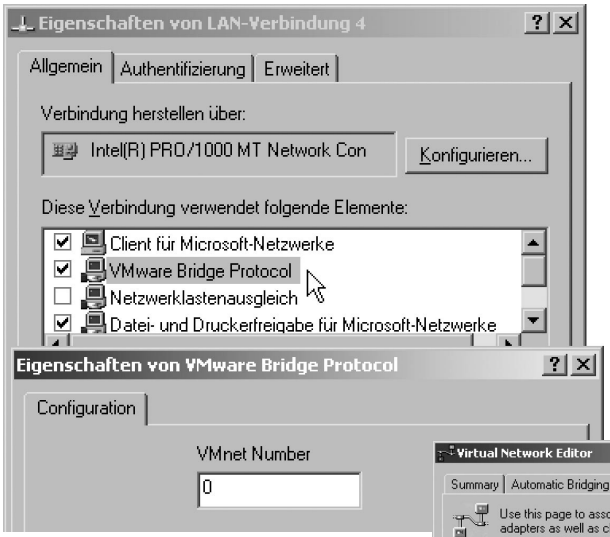
Die detaillierte NAT-Konfiguration erfolgt über den Reiter „NAT“ der Virtual Network Settings. Der interne NAT-Router funktioniert übrigens völlig unabhängig vom logischen Host-Adapter „VMware Network Adapter VMnet8 (NAT)“ und könnte genauso in jedem anderen VMnet laufen.

Die eingangs erwähnten vordefinierten Optionen Bridged, Host-only und NAT zu jedem virtuellen Adapters erschließen einem Gast nur das originäre VMnet: bridged an VMnet0, host-only an VMnet1 und per NAT an VMnet8. Die dahinterliegenden Zusammenhänge erkennt man erst mit dem eben beschriebenen Blick auf die „Virtual Network Settings“. Ein paar praktische Einsatzbeispiele fassen die Funktionen zusammen:

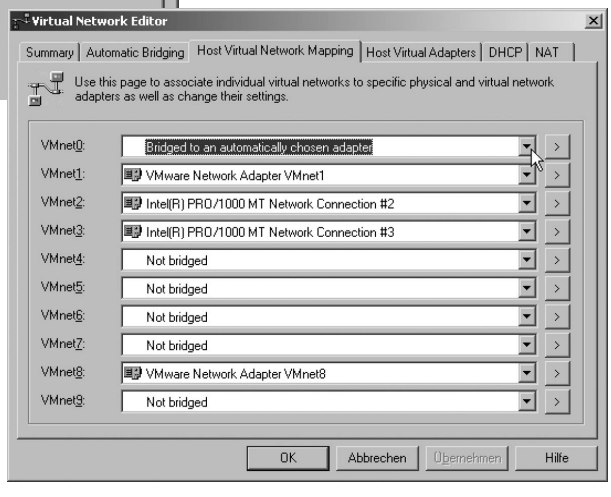
Sollen physische Server uneingeschränkt im LAN erreichbar sein und gleichzeitig ihre Last auf mehrere physische Netzwerkkarten verteilen, kommt ein Anschluss in Gruppen an bestimmte VMnets in Betracht. Jedes VMnet bekommt eine physische Netzwerkkarte zugewiesen (Abb. 6).

Für eine Testumgebung in einem abgeschotteten LAN-Segment koppelt man alle VMs an ein VMnet ohne physischen Adapter (not bridged). Soll dieses Segment kontrollierten Zugriff auf das LAN oder das Internet haben, empfiehlt sich eine VM mit Software-Firewall, die einen virtuellen Adapter im Testnetzwerk und einen im Bridged-VMnet hat (Abb. 7). Alternativ können alle VMs den NAT-Router von VMnet8 verwenden. Diese Funktion bieten aber nicht alle Produkte, sie fehlt zum Beispiel beim ESX Server.

Wenn ein Entwickler unterwegs vom Laptop auf seinen virtuellen Testserver zugreifen will, kann er das über eine direkte Host-only Verbindung tun, etwa im VMNet1 oder VMnet8. Soll eine VM über eine ISDN- oder UMTS-Verbindung des Laptops im Internet surfen, funktioniert das am einfachsten über eine NAT-Verbindung im VMnet8 (Abb. 8).



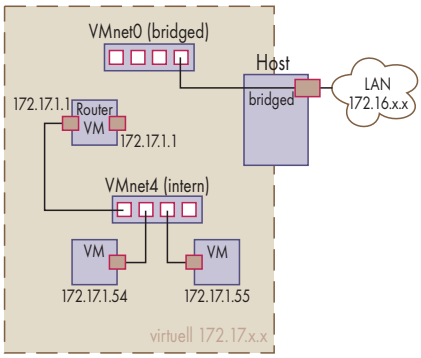

**Brückenschlag: Für das VMnet 0 fiel hier die Wahl auf die Bridge-Funktion für den Netzwerkadapter, VMnet2 und -3 nutzen die „Pseudo“-Ethernetkarte (Abb. 5).**



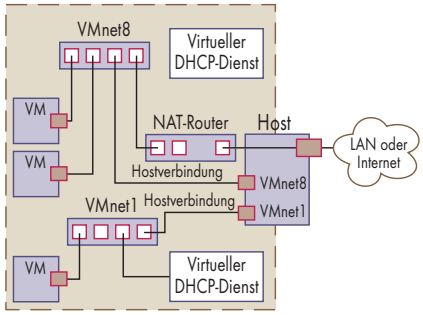

**Kartenlegen: Über diese Zuordnung entscheidet der Administrator, welche VMnets eine Verbindung nach draußen erhalten (Abb. 4)**

## Besonderheiten

Im produktiven Umfeld stellt sich die Frage nach Lastverteilung und Ausfallsicherheit, nach LoadBalancing und Failover. VMwares Server bietet hier wenig, nur wenn der Host das Adapter-Teaming der physischen Netzwerkkarten unterstützt, kann er sie den VMnets zuweisen. Failover und Load Balancing regelt allein der




**Zugeteilt: Zur Lastverteilung empfiehlt es sich, VMs in Gruppen zusammenzufassen und jede mit einer physischen Netzwerkkarte zu verbinden (Abb. 6).**




**Grenzkontrolle: Soll eine Umgebung abgeschottet sein, fasst man die zugehörigen VMs in einem VMnet zusammen. Für den kontrollierten Weg nach außen kann eine VM mit Firewall mit einer VMnet-Bridge dienen (Abb. 7).**

Host, meist mit herstellerspezifischen Treibern.

Ähnliche Einschränkungen gelten für VLANs nach 802.1Q. Um bestimmte VMs unterschiedlichen VLANs des physischen Netzes zuzuordnen, kann das über eine Gruppierung der Gäste in VMnets geschehen. Jedes VMnet erhält einen physischen Adapter, der am passenden VLAN-Port des physischen Switches angeschlossen ist. Alternativ könnte man 802.1Q-Treiber auf dem Gastsystem einrichten.

Für solche Aufgaben hat VMwares ESX Server wesentlich mehr zu bieten, da er direkt die Hardware anspricht und eigene optimierte Treiber verwendet. So kann der Admin jedem vSwitch mehrere physische Netzwerkkarten zuweisen und sie über Regeln als Load-Balancing- oder Standby-Adapter definieren (Abb. 9). Fällt ein Adapter oder der Link aus, bleibt das gesamte virtuelle Netz über einen anderen erreichbar.

Lastverteilung für den nach außen fließenden Datenverkehr beherrscht der ESX Server ebenfalls. Um den eingehenden muss sich immer der physische Switch kümmern, da nur er den Verkehr auf die richtigen Ports verteilen kann.

Zu jedem vSwitch des ESX Servers kann der Admin zusätzlich eine oder mehrere Portgruppen definieren, denen er VLAN-IDs zuweisen kann. Sind die physischen Adapter des vSwitches mit VLAN-Trunk-Ports eines physischen Switches verbunden, wertet der ESX Server die VLAN-IDs aus, verteilt den Verkehr auf die virtuellen Portgruppen und versieht ausgehenden Verkehr der virtuellen Portgruppen mit den richtigen VLAN-Tags. Über das Traffic-Shaping kann er zusätzlich die Leistung einzelner Portgruppen drosseln. Er verfügt über keine NAT-Funktion. Im typischen produktiven ESX-Umfeld dient für solche Einsatzzwecke eher eine Software-Firewall, etwa der ISA-Server oder ein Linux-Router (Abb. 7).

## MAC-Adressen und Klonen von VMs

Ein wichtiges Thema sind die MAC-Adressen der virtuellen Adapter. Sie hängen von einer internen ID ab, die VMware für jede VM eindeutig vergibt, vom „Universally Unique Identifier“ (UUID). Nach dem Kopieren von VMs fragt VMwares Server, ob er eine neue UUID erstellen oder die alte beibehalten soll. Beim Klonen muss es immer eine neue ID sein, weil sonst mehrere VMs die gleichen MAC-Adressen hätten.

Sollen Adapter unveränderliche MAC-Adressen erhalten, beispielsweise weil der Lizenzschlüssel einer Anwendung davon abhängt, kann der Zuständige das direkt in der Konfigurationsdatei der VM festlegen, aber nur in den recht engen Grenzen des für VMware reservierten MAC-Adress-Bereiches (siehe auch http://www.vmware.com/support/esx21/doc/esx21admin_MACaddress.html).

MAC-Adressen vorhandener physischer Karten lassen sich nur innerhalb des Gastes zuweisen. Unter Windows über die Netzkonfiguration des virtuellen Adapters und unter Linux mit dem Befehl *ifconfig ethX up hw ether 00:xx:xx:xx:xx:xx*. Das kann beispielsweise nach der Übernahme einer physischen Maschine (P2V) erforderlich sein, wenn Lizenzschlüssel oder Authentifizierungen von der alten MAC-Adresse abhängig sind.

## Netze unter Microsofts Windows

Bei Microsofts Virtual Server und PC unterscheiden sich die Komponenten etwas:

**Emulierter Adapter:** Den DEC 21140 erkennen Gastsysteme häufig als baugleichen Ethernet Adapter von Intel.

**Bridge Protcol:** An eine Host-Netzkarte muss das Protokoll „Virtual Machine Network Services“ gebunden sein. Diese Karte kann der Anwender dann aus der Liste beim virtuellen Adapter auswählen.

**HostOnly:** Microsofts Loopback-Adapter gehören zum Lieferumfang von Windows. Über „Systemsteuerung -> Hardware -> neues Gerät hinzufügen“ kann man sie auf dem Host als Netzwerkadapter installieren, das Protokoll „Virtual Machine Network Services“ manuell binden und beim virtuellen Adapter als Netzwerkkarte auswählen.

**NAT:** Der Modus „Shared Networking (NAT)“ existiert nur beim Virtual PC. Beim Virtual Server lässt er sich nur über „Microsoft Loopback-Adapter“ und die „Internet-Verbindungsfreigabe“ (ICS) auf dem Host nachbilden.

**Isolierte Netze:** Beim Virtual PC gibt es nur eins mit der Auswahl „nur lokal“. Beim Virtual Server kann man mehrere über die Auswahl „internes Netzwerk“ erstellen.

Virtuelle Netze bieten flexible Konfigurationen auf wenige Mausklicks hin, ohne ein Kabel umstecken oder einen Switch einbauen zu müssen. Wer die Konzepte verstanden hat, kann individuelle Konfiguration erstellen, was nicht nur in Testumgebungen dienlich sein kann. (rh)

SVEN AHNERT

betreut als Mitarbeiter eines Systemhauses mittelständische Firmen in den Bereichen Netzwerke und Serversysteme.

### Literatur

[1] Michael Ziegler; Virtualisierung; Desktop zentral; VMwares Konzept der Virtual Desktop Infrastructure; *iX* 8/2006, S. 110

[2] Sven Ahnert; Server-Virtualisierung; Virtuelle Piloten; VMwares GSX-Server in der Praxis; *iX* 2/2006, S. 137