# Netzwerke mit VMware – Teil1

**VMware bietet ausgefeilte Möglichkeiten zur Vernetzung der virtuellen Maschinen. Diese Flexibilität wird leider erkauft mit einer unübersichtlichen Anzahl von Optionen. Zu keinem Themenbereich erreichen VMaschinen.de mehr Fragen. Dieser Artikel erklärt die Grundlagen virtueller Netzwerke und zeigt anhand praktischer Beispiele die Verwendung der verschiedenen Netzwerktypen auf. Zusätzlich gibt es Tipps und Tricks zum Thema.**

*Dieses PDF-Dokument enthält Lesezeichen als Inhaltsverzeichnis!*

## Wichtiger Hinweis:

Viele der Newsletter-Workshops finden Sie stark überarbeitet, erweitert und aktualisiert in meinem Buch **„Virtuelle Maschinen mit VMware und Microsoft“** vom Verlag Addison-Wesley. Eine ausführliche Buchvorstellung mit Inhaltsverzeichnis, Bildern und Leseproben finden Sie hier:
http://www.vmaschinen.de/cgi-bin/vmware.cgi?vmwarebuch

Jetzt aber zum Netzwerkartikel….

Jede VM muss früher oder später einmal ans Netz. Sei es nur, um den Internetanschluß des Host-Systems mitzunutzen, oder um aktiv am Netzwerkverkehr des Firmen-LANs teilzunehmen.

VMaschinen.de zeigt wie es funktioniert und was zu beachten ist. Im ersten Teil geht es vor allem um Grundlagen, Netzwerktypen und praktischen Nutzen. Der zweite Teil wird Tipps und Tricks sowie Besonderheiten behandeln.

***Hinweis:*** *Die Artikel setzen das entsprechende Basiswissen zum Protokoll TCP/IP und zu den Netzwerkeinstellungen im jeweiligen Betriebsystem voraus. Begriffe, wie Routingtabelle oder Netzwerkmaske sollten bekannt sein.*

## allgemeine Grundlagen

Grundsätzlich können jeder VM unter VMware bis zu vier virtuelle Netzkarten zugewiesen werden.

***Tip:*** *Die Workstation-Version unterstützt offiziell nur drei Adapter, aber ein Vierter kann durch direktes Editieren der VMX-Datei zugewiesen werden. (sh. Tips+Tricks in Teil2, bzw. auf www.vmaschinen.de)*

Jede virtuelle Netzkarte wird von VMware hardwaremäßig emuliert. Das OS in der VM denkt dabei, es ist ein echter Netzwerkadapter eingebaut. In der Netzwerkumgebung des virtuellen Systems erscheinen ein oder mehrere *AMD-PCNET-Adapter*, bzw. *VMware PCI Ethernet Adapter*. Auf den Unterschied gehe ich später ein. Dank funktionierender Plug&Play-Unterstützung erkennt das OS die Netzkarten meist automatisch und installiert den passenden Treiber.

An die erkannten Netzkarten können innerhalb der VM beliebige Protokolle gebunden und konfiguriert werden. Z.B. kann man feste IP-Adressen zuweisen und Routing zwischen mehreren virtuellen Netzkarten und Netzen einstellen.

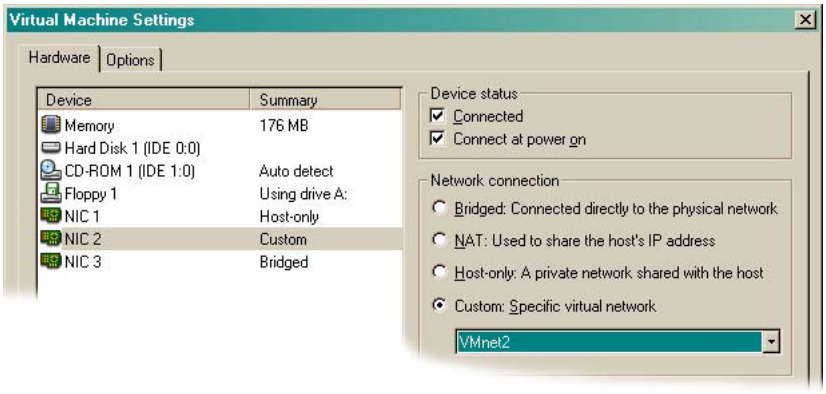
Wie gesagt: Nicht ein Protokoll oder eine höhere Schicht wird für das Betriebssystem in der virtuellen Maschine emuliert, sondern direkt die Hardware einer Netzkarte! Damit erübrigen sich die oft gestellten Fragen: „Wird auch IPX/SPX unterstützt?“ Oder „Welche Netzkarte im Host kann ich verwenden?“.

Antwort1: Es können alle Protokolle verwendet werden, welche im OS der VM (z.B. W2K, Linux oder Netware) unterstützt werden.

Antwort2: Die Netzwerkfunktionalität einer VM ist völlig unabhängig von der im Host eingebauten physischen Netzkarte. Das geht soweit, dass im Host überhaupt keine physische Netzkarte notwendig ist, wenn sich die Kommunikation der VMs auf die internen virtuellen Netzwerke, bzw. auf den Datenaustausch mit dem Host beschränkt.

## Typen der virtuellen Netzkarten

Ob die Pakete des erzeugten Netzverkehrs aus einer VM die wahre Welt draußen erreichen, oder ob diese Pakete nur im virtuellen Netz bleiben, hängt maßgeblich von der Art des emulierten Adapters ab. Vier Typen stehen zur Verfügung:




### Bridged

Ein Adapter vom Typ „Bridged“ leitet alle Pakete aus der VM direkt auf eine physische Netzkarte des Hosts weiter. Die VM erscheint damit im realen LAN als eigenständiger PC mit eigener MAC-Adresse. Sie benötigt eine eigene IP-Adresse, bzw. kann sich vom DHCP-Server im LAN eine Adresse abholen. Der gesamte Netzwerkverkehr, den die VM auf einem Bridged Adapter produziert, erscheint *protokollunabhängig(!)* komplett am physischen Anschluss der verbundenen Host-Netzkarte und die VM ist über diesen Adapter auch direkt von außen erreichbar.

### NAT

Auch die Pakete aus einer VM mit NAT-Adapter gelangen ins physische LAN. Allerdings „borgt“ sich die VM dafür die Identität (MAC-Adresse, IP-Adresse) des Hosts. Damit ist keine freie IP-Adresse im LAN für diese VM notwendig. Die VM ist dafür aber nicht direkt aus dem LAN heraus erreichbar. Z.B. funktioniert keine Fernsteuerung über VNC, bzw. Remote-Desktop und ein virtueller Server bleibt unansprechbar. Nur Antwortpakete auf Anfragen aus der VM gelangen zurück, etwa beim Surfen im Internet. Für einen Zugriff von außen gibt es allerdings noch die Möglichkeit zum sog. Portforwarding - doch dazu später.
***Hinweis**: NAT-Adapter unterstützen nur TCP/IP!*

### Host-only

Eine VM mit Host-only-Adapter ist vom physischen LAN getrennt. Nur mit dem Host selbst ist eine uneingeschränkte

Kommunikation in beiden Richtungen möglich. Dazu besteht zwischen Host und VMs ein virtuelles Netzwerk mit eigenem IP-Adressbereich und internem DHCP-Server für die VMs. Die Trennung des Netzes ist allerdings nicht absolut, man könnte mit manuell gesetzten Routing-Einträgen am Host und in der VM durchaus den Verkehr aus dem virtuellen Netz ins physische LAN leiten und umgekehrt.

**Custom**

Ein virtueller Adapter im Modus „Custom“ wird oft dazu verwendet, um VMs komplett von der realen Welt abzuschotten. Diese VMs können dann in einem virtuellen Netzwerk nur untereinander kommunizieren, kein Paket gelangt nach draußen, auch nicht zum Host! Dazu stellt VMware zehn virtuelle Switches (VMNet0-VMNet9) bereit. An einem solchen Switch können virtuelle Netzkarten „gesteckt“ werden. Alle Adapter am gleichen Switch befinden sich dann im gleichen virtuellen Netz und „sehen“ sich. Damit ist es möglich, eine Testumgebung mit Servern und Workstations, verschiedenen Netz-Segmenten und sogar mit Routing aufzubauen, ohne dass ein einziges Paket in die reale Welt und damit ins LAN gelangt. Wohlgemerkt: alles auf dem gleichen physischen Rechner!

***Hinweis:*** *Eigentlich ist der Modus „Custom“ der Urtyp aller Adaptertypen. Man könnte auf die drei Modi Bridged/NAT/Host-only verzichten, sie sollen nur den Umgang mit virtuellen Netzkarten vereinfachen. Einen Custom-Adapter ans VMNet0 anzuschließen, ist nämlich das Gleiche, wie diesen Adapter als Bridged zu konfigurieren. Gleiches gilt für VMNet1 (Host-only) und VMNet8 (NAT). Wir werden noch darauf zurückkommen, wenn es um die Verwendung mehrerer Netzkarten geht.*

***Tipp:*** *Zwischen den verschiedenen Netzkarten-Modi kann im laufenden Betrieb jederzeit umgeschaltet werden. Einer VM ist es völlig egal, welche Art Adapter emuliert wird. Für die VM sieht es aus, als würde nur das LAN-Kabel umgesteckt. So kann die Test-VM kurz ins reale LAN gestellt werden und bei Problemen sofort wieder isoliert werden. Doppelklicken Sie dazu am einfachsten unten rechts im Fenster der VM auf das kleine Netzkartensymbol.*

## Einsatz der Adaptertypen, Besonderheiten

Um die kurze Vorstellung der verschiedenen Netzkartentypen von VMware weiter zu vertiefen, werden wir nun für jeden Adaptertyp einen konkreten Einsatzzweck und weitere Besonderheiten kennenlernen.

### Einsatz von Bridged

Ein Adapter vom Typ Bridged wird immer dann verwendet, wenn eine VM uneingeschränkt direkt im physischen LAN erscheinen soll. Das ist am häufigsten in Produktionsumgebungen der Fall, wenn die VM im Netz eine konkrete Aufgabe zu erfüllen hat. Die Konfiguration mit einem Bridged-Adapter ist am einfachsten und liefert schnell volle Netzfunktionalität. Man muss allerdings das vorhandene physische LAN kennen.

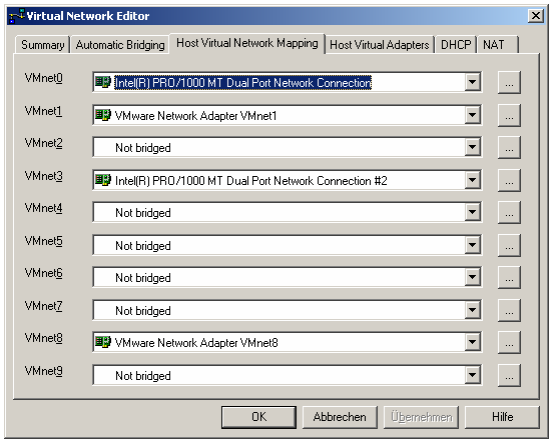
Voraussetzung ist eine freie IP-Adresse im LAN bzw. ein verfügbarer DHCP-Server. Die Netzkarte in der VM ist entsprechend zu konfigurieren. Die VM tritt mit eigener MAC-Adresse auf und nutzt über das sogenannte *„VMware Bridging Protokoll“* einen physischen Adapter des Hosts, als wäre es ihr eigener. So kann ein Webserver, ein Terminalserver, Netware (auch mit IPX) usw. direkt in das LAN gestellt werden.

Dabei können mehrere VMs und auch der Host gleichzeitig dieselbe physische Netzkarte verwenden.

***Achtung!*** *Eine versehentlich laufende Test-VM im Modus Bridged auf dem eigenen Laptop, kann im LAN eines Kunden schnell den Sicherheitsadmin auf den Plan rufen, wenn plötzlich doppelte oder fremde IP-Adressen, NetBios-Namen usw. im Firmen-LAN auftauchen. Denken Sie immer daran – eine VM mit Netzkarte im Modus Bridged verhält sich im LAN wie ein vollwertiger PC!*

Ein weiterer Einsatzzweck für Bridged-Adapter kann die direkte Anbindung eines DSL-Modems über PPPoE an eine VM sein. Mit einem Adapter im Modus „Bridged“ ist es möglich, völlig transparent auf angeschlossene Ethernet-Geräte zuzugreifen.

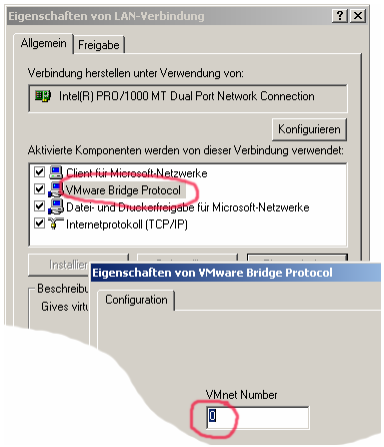
Wichtigste Komponente für das Tunneln des Netzverkehrs ist das erwähnte *„VMware Bridge Protocol“*. Es kann an jeden beliebigen Netzadapter im Host gebunden werden, auch an mehrere. Die Auswahl, welcher virtuelle Adapter mit welchem physischen Adapter verbunden ist, erfolgt über den Menüpunkt *Edit > virtual Network Settings > Host Virtual Network Mapping.*




Hier kann jedem virtuellen Netz ein physischer Adapter des Host-PC zugewiesen werden. Nur VMNet1 (Host-Only) und VMNet8 (NAT) sind bereits anderweitig reserviert. Standardmäßig wird VMNet0 ein automatisch ausgewählter Adapter zugewiesen.

***Tip:*** *Um nichts dem Zufall zu überlassen, sollte ein Adapter für VMNet0 explizit ausgewählt werden. Bei mehreren Adaptern im Host, ist dies dringend zu empfehlen!*

Anhand der getätigten Einstellungen, wird dann von VMware automatisch in der Netzwerkumgebung des Hosts das *„VMware Bridge Protocol“* an den entsprechenden Adapter gebunden und auf das gewählte virtuelle Netz (z.B. VMNet0) eingestellt.




***Hinweis:*** *Um andere Netze, als VMNet0 zum Bridgen zu verwenden, muss der Custom-Modus benutzt werden. Das kann bei mehreren Netzkarten im Host notwendig sein.*

**Einsatz von NAT**

Immer dann, wenn man entweder keine freie IP-Adresse aus dem LAN zur Verfügung hat, bzw. wenn die VM nur als heimlicher Zaungast am Netzwerkverkehr teilnehmen soll, ist ein Adapter im Modus NAT zu verwenden. NAT ist erste Wahl, wenn die VM nur mal eben schnell ins Internet will oder Daten aus dem Firmen-LAN abrufen muss. Vorausgesetzt der Host ist bereits vollwertig ins LAN integriert, hat man sich in der VM um nichts weiter zu kümmern. Auch den ISDN- oder Modem-Zugang des Hosts kann die VM auf diese Weise mit benutzen.

Die Netzkarte in der VM sollte so konfiguriert werden, dass sie Ihre IP-Konfiguration von einem DHCP-Server erhält. Das ist in den meisten Betriebsystemen die Standardeinstellung. Ein interner DHCP-Server von VMware liefert dem OS in der VM nämlich eine dynamische IP-Adresse samt Default-Gateway und DNS-Server.

Der NAT-Dienst leitet danach allen Verkehr automatisch über den Host. Für alle Beteiligten im LAN sieht es so aus, als würde der Host selbst die Pakete senden. Die Antworten schickt der NAT-Dienst zurück an die VM.

Nachteil: Die VM ist nur mittels Portforwarding von außen zu erreichen. Wenn dabei zur selben Zeit in der VM und auf dem Host Dienste wie VNC auf den gleichen Ports lauschen, kann nur eine Maschine den Dienst anbieten, oder es sind unterschiedliche Ports zu verwenden.

Für einen NAT-Adapter spielen mehrere Komponenten eine Rolle. Einmal der Dienst „*VMware NAT Service*“, welcher sozusagen als virtueller Router mit Adressumsetzung zwischen den VMs und dem Host fungiert. Weiterhin verteilt der *„VMware DHCP Service“* an alle virtuellen Maschinen dynamische IP-Adressen mit den richtigen Gateway und DNS-Einträgen. So muss man am virtuellen Adapter in der VM keinerlei Einstellungen vornehmen.

Als Schnittstelle zwischen den VMs und dem Host dient der logische Adapter *„VMware Network Adapter VMnet8“ (sh. auch Host-only-Netzwerk weiter unten)*

Detailierte Beschreibung aller Komponenten, sowie des Portforwarding sh. Komponenten weiter unten.

**Einsatz von Host-only**

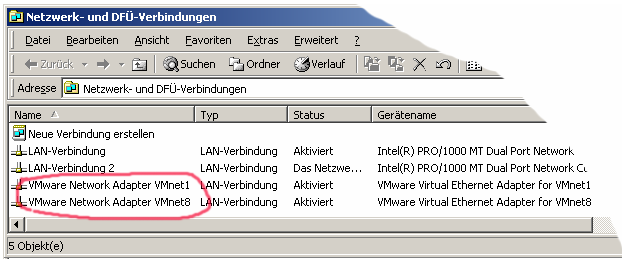
Das Host-only-Netz ist für eine Verbindung der VMs mit dem Host vorgesehen, etwa zum Datenaustausch, aber auch für Entwickler, die Ihren eigenen Web-Server oder SQL-Server usw.

gleich „im Bauch“ Ihres PC laufen lassen wollen und sich so einen zusätzlichen Rechner sparen.

***Tip:** Eine gute Alternative zum bloßen Datenaustausch mit dem (Windows-)Host bieten die sog. Shared Folder. Damit kann man komplett auf ein Netzwerk zwischen Host und VM verzichten und eine VM auch völlig ohne Netzkarte konfigurieren.*

Das Host-only-Netz bedient seine VMs, wie beim NAT-Adapter, ebenfalls mittels internem DHCP-Server mit dynamischen IP-Adressen. Man kann aber auch eine feste Zuordnung treffen.

Um das Host-only-Netz verwenden zu können, muss keine physische Netzkarte im PC eingebaut sein. Der Verkehr läuft über den logischen Adapter *„VMware Network Adapter VMnet1“*, welcher von VMware auf dem Host automatisch installiert wurde. Dieser Adapter wird vom Host-System als eine normale Netzkarte angesehen, nur eben mit einer virtuellen Buchse „nach innen“ zu den VMs.




Damit kann zwischen physischen Netzkarten im Host und dem *„VMware Network Adapter VMnet1“* auch geroutet werden. Man könnte z.B. für die VMs ein eigenes internes IP-Netz aufbauen und dieses ans physische LAN mittels Routing über den Host anbinden. So wäre eine logische Trennung vom physischem LAN und virtuellem LAN möglich.

### Einsatz von Custom

Wie schon erwähnt – der Custom-Modus erlaubt es eigentlich, alle Möglichkeiten virtueller Netzkarten auszuschöpfen. Vorerst wollen wir uns hier allerdings auf den Haupteinsatzzweck beschränken – den Aufbau völlig abgeschotteter Testumgebungen.

Wenn ein Netzwerk benötigt wird, in dem mehrere virtuelle Maschinen untereinander kommunizieren sollen, ohne Pakete ins reale LAN zu entlassen, dann sind Custom-Adapter zu verwenden. Durch die Möglichkeit, mehrere VMs an unterschiedliche virtuelle Switches (VMNet0-9) anzuschließen,

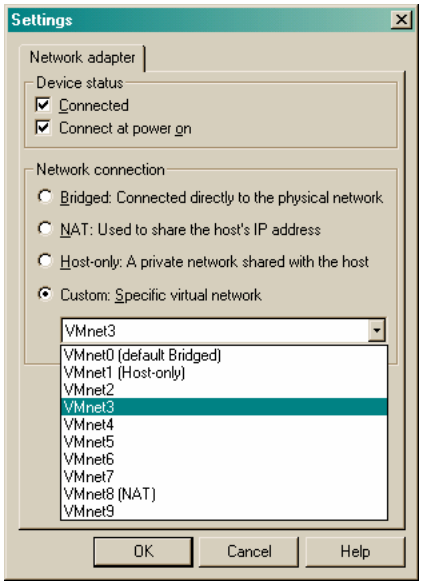
können komplexe Netze aufgebaut werden, ohne dass die Gefahr besteht, das reale LAN zu kompromittieren.

So können auf ein und der selben Hardware z.B. Test-Clients in verschiedenen Konfigurationen auf einen virtuellen Netware-Server oder W2K-Server zugreifen. Oder eine Migration mehrerer NT4-Server mit Domänen auf W2K mit ADS (sogar über verteilte Standorte) kann bequem getestet werden.

Auch für den Custom-Modus muss nicht unbedingt eine physische Netzkarte im Host eingebaut sein.

Weiterhin ist der Custom-Modus unentberlich, wenn im Host mehrere physische Netzkarten dediziert auf verschiedene VMs verteilt werden sollen. So kann in einer Produktionsumgebung jeder VM eine eigene physische Netzkarte und damit ein eigener Port am physischen LAN-Switch zugewiesen werden.

Wichtigste Komponente der Custom-Adapter sind die internen virtuellen Netze von VMware. Zehn Stück (VMNet0-VMNet9) stehen zur Verfügung, wobei VMNet0, VMNet1 und VMNet8 schon fest für bestimmte Aufgaben reserviert sind.




Alle anderen virtuellen Switches stehen zur freien Verfügung und können entweder intern verwendet werden oder mittels *„VMware Bridge Protocol“* mit beliebigen physische Netzkarten verbunden werden.

Ungebridgde virtuelle Switches sind völlig abgeschottet und kein Paket gelangt zum Host oder nach draußen (außer VMNet1+8).

## Komponenten des Netzwerkes

Zusammenfassend werden hier nochmals alle am Netzwerk beteiligten Komponenten genannt, welche auf dem Host installiert sind.

### logische Netzwerkadapter

Am Host existieren folgende logischen Netzwerkadapter:

***(Sichtbar unter Netzwerk- und DFÜ-Verbindungen)***

*VMware Network Adapter VMnet1 (Host-Only)*
*VMware Network Adapter VMnet8 (NAT)*

Theoretisch können weitere hinzugefügt werden (kaum sinnvoll):

***Menüpunkt: Edit > virtual Network Settings > Host Virtual Adapters.***

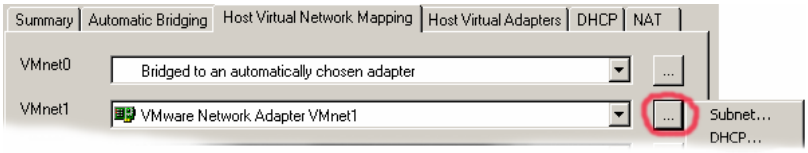
Alle logischen Adapter wirken für das OS auf dem Host als normale Netzkarten. Wo sie "angeschlossen" sind, wird über den virtuellen Switch bestimmt, dem sie zugeordnet werden:

***Menüpunkt: Edit > virtual Network Settings > Host Virtual Network Mapping.***
*(sh. auch Sreenshot bei "Einsatz von Bridged" weiter oben.)*

IP-Adressen dieser Adapter können direkt manuell im Host-OS gesetzt werden, oder besser über:

***Menüpunkt: Edit > virtual Network Settings > Host Virtual Network Mapping.***

Klicken sie hier auf die drei Punkte rechts neben jedem Adapter und wählen Sie dort das Kontextmenü *Subnet*.




### VMware Bridge Protocol

Diese Protokoll tunnelt den Verkehr eines virtuellen Adapters, ungesehen vom Host-OS, direkt auf einen physischen Adapter. Das kann parallel zur normalen Host-Kommunikation erfolgen (bei nur einer Netzkarte im Host) oder auch dediziert für eine bestimmte VM (alle Bindungen und Protokolle am physischen Adapter sind dann zu deaktivieren).

Mehrere VMs und der Host selbst können die gleiche physische Netzkarte verwenden.

**Dienste auf dem Host**

*VMware NAT Service*
Dient als virtueller Router mit NAT- und Portforwarding-funktionalität zwischen dem Host und VMs mit NAT-Adapter.

*VMware DHCP Service*
Liefert an virtuelle Netze aus definierten IP-Bereichen dynamische Adressen. Den VMs muss damit keine feste IP zugewiesen werden.

Die Konfiguration der Adressbereiche des DHCP-Servers, bzw. der Parameter für NAT/Portforwarding findet sich hier:

***Menüpunkt: Edit > virtual Network Settings > DHCP / NAT.***

Die aktuelle Konfiguration, vergebene Adress-Leases und weitere interessante Informationen, finden sich in folgenden Dateien auf dem Host:

vmnetdhcp.conf
vmnetdhcp.leases
vmnetnat.conf
vmnetnat-mac.txt

z.B. unter:
**C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware**

## Praxisbeispiel

Ein Praxisbeispiel erläutert nun die Verwendung der wichtigsten Adaptertypen noch einmal und verdeutlicht in einer einzigen Konfiguration ein mögliches Zusammenspiel.

### Mobiler Web- oder Datenbankserver für Entwickler

Dazu läuft in diesem Beispiel auf einer virtuellen Maschine „*VM1*“ ein Webserver. Das kann je nach Geschmack unter Linux oder W2K sein. Apache mit Perl, PHP und MySQL-Datenbank kommen genauso in Frage, wie IIS mit ASP und MS-SQL.

Mit dieser lauffähigen virtuellen Maschine hat der Entwickler auf dem Laptop ständig seinen eigenen vollwertigen Webserver mit am Mann, auch außerhalb der Firma, selbst ohne Internetanbindung, offline im Zug oder im Flugzeug.

### Zugriff auf die VM vom Host aus

Um nun vom Laptop Zugriff zum Webserver zu haben, wird eine *Host-Only-Verbindung* verwendet. Sie kann genutzt werden, um Daten auf dem Webserver zu aktualisieren, oder einfach per Browser Seiten abzurufen und zu testen. Dazu erhält VM1 eine feste IP aus dem Bereich 192.168.2.x (eine dynamische Zuordnung ist, wegen der Erreichbarkeit von außen, nicht sinnvoll). Der Verkehr vom Host läuft über den *„VMware Network Adapter VMnet1*“ durch das interne virtuelle Host-Only-Netz und gelangt schließlich zum virtuellen Adapter der VM1.

Eine Besonderheit ist die feste Einstellung der IP 192.168.2.1 für den *„VMware Network Adapter VMnet1*“ auf dem Host. Sh. dazu weiter oben bei „Komponenten des Netzwerkes“.

Im Browser auf dem Host kann jetzt die Zeile „*http://192.168.2.2/*" eingegeben werden und die Seiten des virtuellen Webservers sind zu sehen.

### weitere Test-VMs im virtuellen Netz

Für den Fall, dass die Darstellung dieser Seiten in verschiedenen Browserversionen und von verschiedene Betriebssystemen aus getestet werden soll, können mehrere VMs mit Linux oder Windows und verschiedenen Browserkonfigurationen installiert werden. Diese greifen dann über ein internes virtuelles *Custom-Netz* auf VM1 zu.

Dazu erhalten diese Test-VMs je einen Adapter im *Custom-Modus*. VM1 erhält ebenfalls eine zusätzliche virtuelle Netzkarte im *Custom-Modus*. Alle diese virtuellen Adapter werden intern mit dem virtuellen Netz *VMNet2* verbunden. Sie werden manuell mit IP-Adressen aus dem gleichen (frei wählbaren) Netz konfiguriert.

So kann dann im genannten Beispiel aus jeder dieser VMs mittels „*http://192.168.3.1/*“ auf den virtuellen Webserver zugegriffen werden.

***Tip:** Wird in den VMs als Default-Gateway 192.168.3.1 gesetzt, so kann auch direkt auf die 192.168.2.2 zugegriffen werden.*

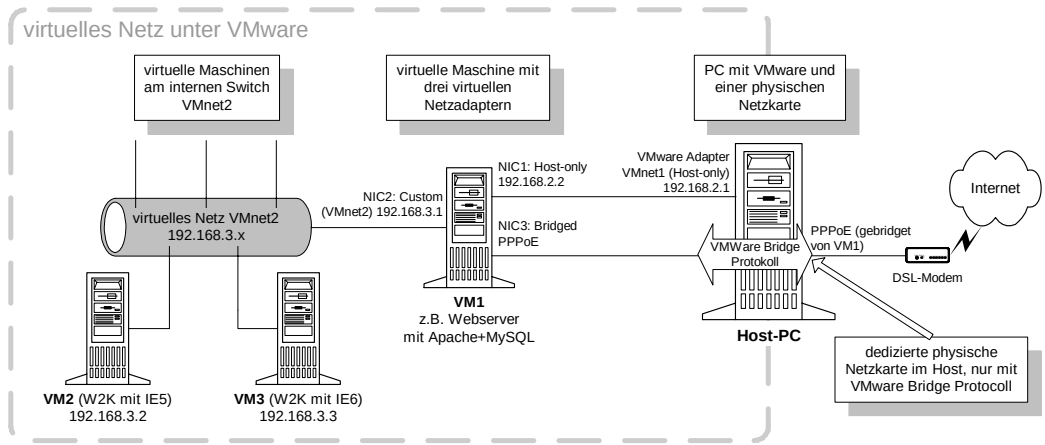
*Bis hierher ist keine physische Netzkarte im Host nötig!*

**Erreichbarkeit der VM vom externen LAN**

Soll aber VM1 auch von außen erreichbar sein, etwa für Kunden-Demos, oder sogar direkt aus dem Internet, dann ist die Anbindung über einen *Bridged-Adapter* möglich. Dabei kann die VM direkt in ein externes LAN eingebunden werden (mittels fester IP oder DHCP aus dem LAN), bzw. auch direkt mittels PPPoE ein DSL-Modem ansteuern (wie im Beispiel).

## Übersichtsplan der Beispielkonfiguration

**Praxisbeispiel für eine virtuelle Vernetzung**




Die Netzwerkkommunikation zwischen dem **Host** und **VM1** erfolgt über das virtuelle Host-Only-Netz *VMnet1*. An diesem Netz hängt der logische Adapter *"VMware Network Adapter VMnet1"* des Hosts sowie der Host-Only-Adapter von VM1. Beide Adapter wurden manuell mit festen IP-Adressen aus dem Netz 192.168.2.x konfiguriert.

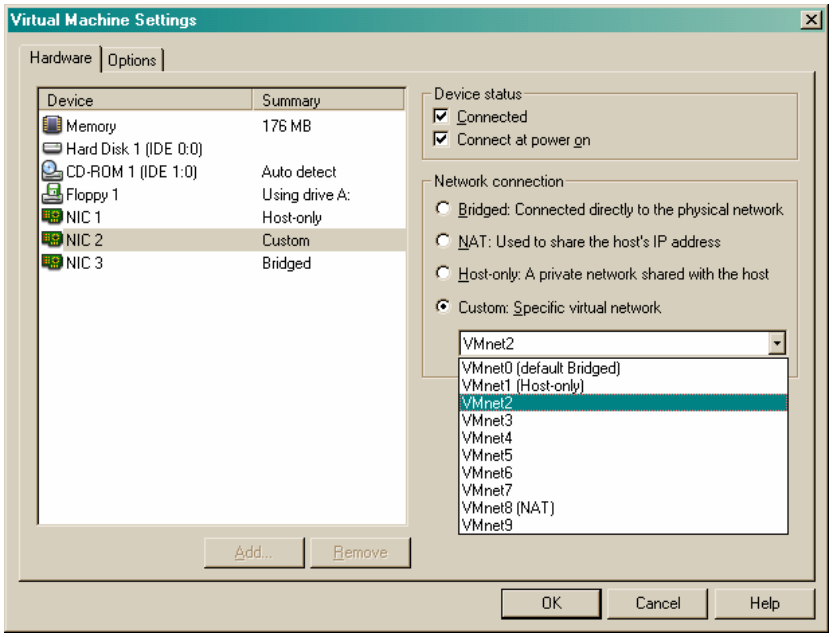
**VM2** und **VM3** im virtuellen Netz *VMnet2* können mit dem Custom-Adapter von **VM1** kommunizieren. Dazu sind alle VMs am virtuellen Switch *VMnet2* angeschlossen. Alle beteiligten VMs haben feste IP-Adressen aus dem gleichen (beliebig wählbaren) Netzbereich. Hier 192.168.3.x.

**VM1** spricht zusätzlich ein **DSL-Modem** mittels PPPoE über einen Bridged-Adapter. Dieser virtuelle Adapter ist mittels *"VMWare Bridge Protokoll"* mit einer physischen Netzkarte im Host verbunden. Der Verkehr wird, unsichtbar für das Host-OS, über dieses Protokoll direkt nach draussen getunnelt.

Netzverkehr aus einem **physischen LAN** 192.168.1.x (soweit vorhanden) könnte über zwei Wege zu **VM1** gelangen:
***Lösung1:*** Ein weiterer (vierter) Adapter in VM1 im Modus Custom wird an *VMnet4* angeschlossen. *VMnet4* wird dann gebridged auf eine zweite physische Netzkarte im Host.
*Oder noch einfacher:* Man schließt anstelle des DSL-Modems das LAN (Hub oder Switch) direkt an den schon vorhandenen physischen Adapter an und nutzt in VM1 weiterhin den Bridged-Modus.
***Lösung2:*** Mittels richtig gesetzter Routing-Einträge am Host, in den VMs und im externen LAN, kann direkt über die Host-Only-Verbindung zu VM1 geroutet werden. Dazu muß das interne Netz 192.168.2.x dem externen LAN bekannt sein (Routing-Tabelle) und das externe Netz 192.168.1.x muß wiederum der VM1 bekannt sein. Der Host selbst muß dazu natürlich ans LAN angebunden werden, eventl. über eine zusätzliche Netzkarte oder anstelle des DSL-Modems.

21.12.04 Sven Ahnert
www.vmaschinen.de

### Konfiguration der Adaptertypen im Beispiel




### Anbindung eines externen LAN

Das Beispiel kann beliebig erweitert werden. So könnte mit den richtigen Routing-Einträgen vom Host aus, über VM1, auch auf die VMs im virtuellen Netz Vmnet2 zugegriffen werden. Damit wäre eine Anbindung des separaten virtuellen Netzes an den Host und über diesen sogar an das physische LAN möglich. Der Phantasie sind hier keine Grenzen gesetzt!

Um ein externes Netzwerk *192.168.1.x* anzubinden, ist eine weitere Netzkarte notwendig, über die erst einmal der Host selbst ordentlich im LAN kommunizieren kann (IP-Adresse, Gateway DNS usw.).

Um Rechnern aus dem LAN dann Zugriff auf das interne virtuelle Netz *192.168.3.x* zu geben, sind zusätzlich folgende Routing-Einträge notwendig (hier in Linux-Syntax):

*in VM1:*
**route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.2.1**

*auf den externen PCs:*
**route add -net 192.168.3.0 netmask 255.255.255.0 gw 192.168.1.1**
***ODER:***
**route add -net 0.0.0.0 netmask 0.0.0.0 gw 192.168.1.1**

Auf dem Host müssten die notwendigen Routingeinträge automatisch vorhanden sein.

## konkrete Einsatzszenarien

Am Ende des ersten Teils soll eine kurze Übersicht die Entscheidung erleichtern, welche Art virtueller Netzkarte für einen bestimmten Einsatzzweck gewählt werden kann.

**Dienste-Server**

Sie möchten Dienste Ihrer Produktionsumgebung virtualisieren. z.B. Webserver, DNS/DHCP, Domänenkontroller, NDS-Replica, Lizenzierungsserver, Terminalserver usw.
Adaptertyp:
Bridged
Besonderheiten:
Sind im Host mehrere Netzkarten vorhanden, sollten Sie diese in Produktionsumgebungen explizit bestimmten VMs oder VM-Gruppen zuweisen. Damit lässt sich die Lastverteilung steuern.

**VM soll als Software-Firewall dienen**

Adaptertyp:
Bridged zum Internet, Host-only oder Bridged zum LAN.
Besonderheiten:
Es sollten zwei physische Netzkarten existieren. Am Adapter zum Internet sollte auf dem Host nur das *„VMware Bridge Protocol“* gebunden sein. Kein TCP/IP, kein Client! So ist der Internetverkehr optimal vom Hostsystem isoliert, bevor er die Firewall in der VM passiert.

**VM soll einfach nur zum Surfen ins Internet**

Adaptertyp:
NAT
Besonderheiten:
Nutzen Sie einfach Ihren funktionierenden Internetzugang vom Host. Internet auf dem Host muss natürlich konfiguriert sein.

**VM soll zusätzlich in Tauschbörsen agieren (Emule...)**

Adaptertyp:
NAT mit Portforwarding oder Bridged-Adapter
Besonderheiten:
Hier muss eine Erreichbarkeit auf bestimmten Ports von außen gegeben sein. Am einfachsten ist die Konfiguration mit einem Bridged-Adapter und Mitbenutzung eines vorhanden LAN (DSL-Router, Standleitung o.ä.), bzw. die direkte Anbindung eines DSL-Modems. Bei NAT-Adaptern ist für die erforderlichen Ports Portforwarding einzustellen.

**VM soll als Testmaschine im Testnetz kommunizieren**

Adaptertyp:
Custom
Besonderheiten:
VMs sollten am gleichen virtuellen Switch das gleiche IP-Subnet verwenden. Keine Pakete gelangen nach draußen.

**die VMs sollen nur Daten mit dem Host-PC austauschen, aber sonst unsichtbar bleiben.**

Adaptertyp:
Host-only
Besonderheiten:
Die Abschottung ist nicht absolut. Bei richtig gesetzten Routing-Einträgen, kann Netzverkehr nach draußen gelangen

**alle VMs ihrer Testumgebung sollen als separates Netz ins physische LAN angebunden werden.**

Adaptertyp:
Host-only
Besonderheiten:
Routing über den Host zum internen virtuellen Netz.
***ODER***
Adaptertyp:
Bridget + Custom
Besonderheiten:
Eine VM spielt den Router. Bridged ins LAN, Custom nach innen zum virtuellen Netz.

Die Anzahl von Beispielen ist unerschöpflich. Die oben genannten Konfigurationen können nur ein Gefühl für die Möglichkeiten der Adaptertypen vermitteln.

## Ausblick

Damit sollten die Grundlagen für die Arbeit mit virtuellen Netzkarten unter VMware gelegt sein. Wozu die verschiedenen Adapter dienen, welche Komponenten zusammenspielen und welche Aufgaben erfüllt werden ist geklärt.

Der zweite Artikel wird noch etwas ins Detail gehen und entschärft auch einige Stolperstricke.

Folgende Fragen werden u.a. angesprochen:

Wie arbeitet man sinnvoll mit mehreren Netzkarten?
Unterschied vlance, vmxnet.
Gigabit-Anbindung und Performance.
Was ist beim Clonen (Kopieren) einer VM zu beachten?
Wo lauern Fehlerquellen, wie verändernde MAC-Adressen usw.?
Portforwarding mit NAT-Adaptern.

Sven Ahnert