Chapter 8

Virtual Networks

The highlight of virtualization

Virtual networks are certainly the highlight of the virtual environment, because of their flexibility offering a wide variety of possibilities. They can provide a network infrastructure offering almost everything one needs and at much lower costs. You also always have a test space or "play area" available, where you can safely try out new ideas, and easily throw out the bad ones with just a few clicks.

No wiring or switch configuration

Within the virtual environment there is no inconvenient wiring or configuration of switch ports needed. You still need to do a little work to configure the network of the host system, but there is less effort compared with alternative systems.

All protocols supported by guest can be used

Through emulation of the entire hardware in the virtual machine, all networking protocols supported by the guest operating system can be used. The only exception is the NAT Adapter which, by its very nature, can only work with the TCP/IP protocol.

8.1 VMware Server and VMware Player

Ten virtual networks are possible

Both products, VMware Server and VMware Player offer ten virtual networks on Microsoft Windows (on Linux there are about 100), three of which have already been preconfigured during the installation:

Host-only, **Bridged** and **NAT**. Yet: via the GUI, VMnet0 can only be used for a bridged network; VMnet1 can only be used for Host-only; and VMnet8 only for a NAT network.

Virtual networks are isolated from each other like physical networks

These networks can be compared with physically separate networks, as only the virtual machines within the same virtual network can see each other. If a virtual machine must be available in multiple virtual networks, you must install multiple network cards into the relevant virtual networks or alternatively configure one virtual machine (or the host system) as a router between the networks.

If the virtual network cannot be accessed by the host system and/or the physical network it is called Guest-only

The seven remaining networks are defined as Guest-only by default, which means that only the virtual machines are connected over the network. The host, by comparison, remains on the Host-only network, and has no connection to the Guest-only network.

If you install a further virtual network adapter on the host and allocate this to a Guest-only network, then this network will become a Host-only network, because then the host and all VMs can see each other. On Windows and on most Linux derivatives these Guest-only networks are directly available. However on systems with UDEV devices, such as newer SuSE and Ubuntu versions, device nodes for VMnet must be created.

As you will have certainly noticed, the assignment of the virtual networks to the virtual machines works through adding a network card to the virtual machine, which is configured for the respective network.

Guest-Only networks can only be created with the Custom option

In Figure 8.1 you can see this process: Under the **Custom** radio button all the available virtual networks are listed. The radio buttons above show the three networks installed by VMware Server itself. All virtual networks which you install yourself must be chosen through the Custom button.

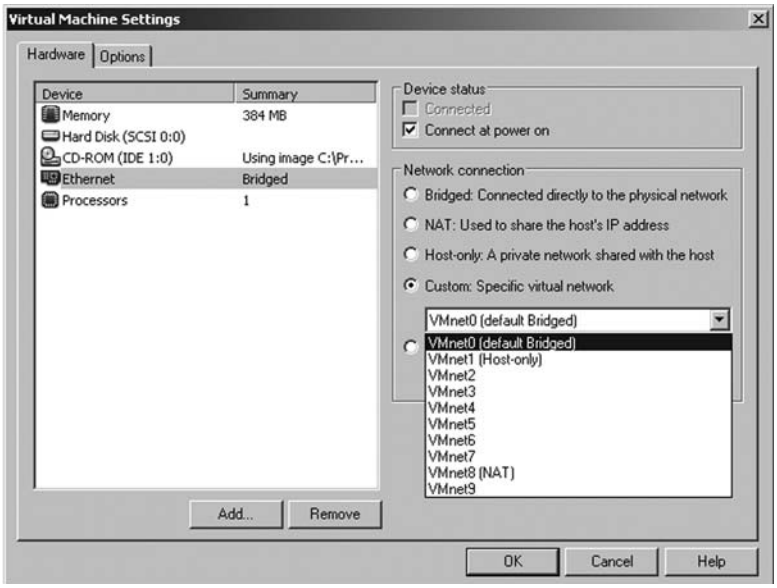

Figure 8.1 – Assignment of the virtual machine to a virtual network

As there are no physical devices involved here, you can at any time and even during operation of the server, change or deactivate the assigned network for the virtual network card. This is done by unticking the **Connected** checkbox.

You can unplug the "wire" by unchecking the Connected box

By default VMware Player can only use the three preconfigured networks whose assignment is handled through the Ethernet GUI. If you are looking for full functionality, in terms of being able to use custom networks, then manual changes are required to the configuration file. These changes automatically disable the Ethernet GUI.

Custom networks require manual changes to configuration files

8.1.1 How are the VMnets used?

As you can see in Figure 8.2, ten virtual networks exist which offer various functions and are differently assigned. VMnet0 is the only network which is directly connected to the physical network via bridging.

VMnet0

VMnet1 and VMnet8

In VMnet1 and VMnet8 the host system has a virtual network card and so can communicate with the virtual machines, and also provide a gateway function in the NAT network.

All remaining networks are completely virtual - they have no contact with the outside world or with the host system. Further on you can recognize the assignment of the virtual machines to the networks. The number of network connections in the virtual machine is identical to the number of built-in virtual network cards.

Figure 8.2 shows the layout of the virtual networks on VMware Player and VMware Server.

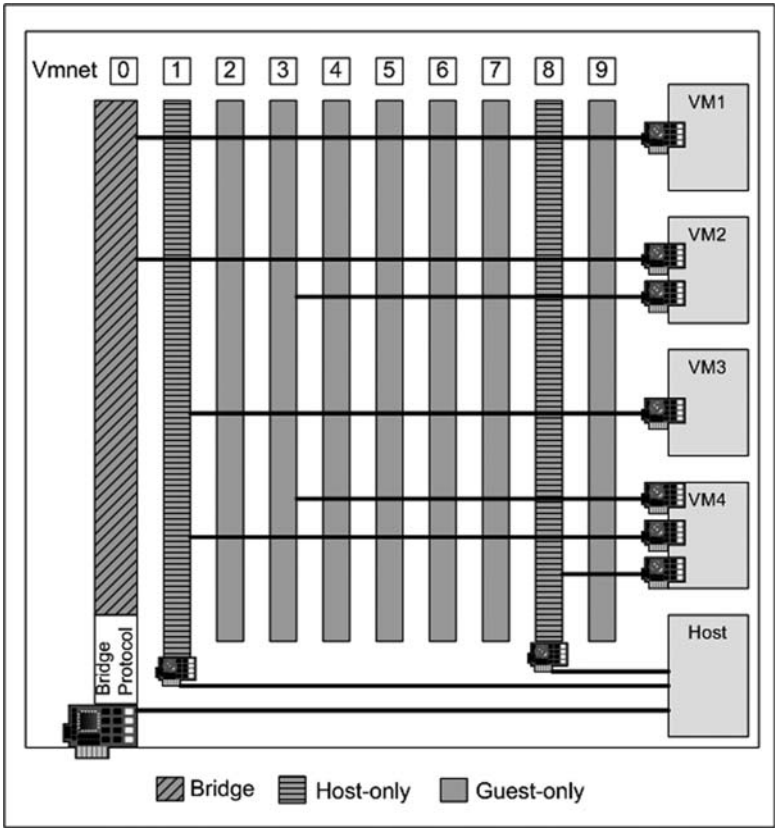

Figure 8.2 – Default network configuration on VMware

The host system has a physical adapter, which functions as a bridge to the physical network on VMnet0, and also two virtual adapters which provide the connectivity between the host and the guest on VMnet1 (Host-only) and VMnet8 (NAT).

The virtual machines VM1 to VM4 are equipped with different numbers of virtual network cards, which are in turn assigned to the different VMnet networks:

- **VM1** is an internal server system, which should be reachable from every member of the network. So, it only has an adapter to VMnet0.
- **VM2** should likewise be reachable in the network, but additionally have a connection to VM4 over the separate Guest-only network VMnet3.
- **VM3** needs connection to VM4 and to the host system, as these three systems exchange data with one another. Therefore only a Host-only network connection (VMnet1) is required.
- **VM4** is a system with various different applications and must therefore have a dedicated connection to VM2 (VMnet3), a separate connection to the host and VM3 (VMnet1), as well as an Internet connection. As there is no reason for a connection from the physical network to VM4, a NAT network (VMnet8) is ideal for this purpose.

Table 8.1 helps you determine the correct VMnet settings to choose and configure the virtual network for a new guest system.

Table 8.1 – Virtual networks and their connections to other systems

Connection to:	**Host System**	**Guest Systems in the network**	**Outside World**
VMnet6	No	VMnet6	No
VMnet7	No	VMnet7	No
VMnet8 (NAT)	Yes	VMnet8	Outgoing yes, if there is an active NAT service. Incoming traffic restricted by the NAT service.
VMnet9	No	VMnet9	No

Use this list as a matri

For example, if you would like to create a guest system which will only provide an Internet connection, either VMnet0 or VMnet8 can be chosen. If you are not interested in incoming network traffic, then VMnet8 would be the better choice.

If you want a network which is completely isolated from the rest of the environment in order, for example, to create your own test domain, you will need a Guest-only network (VMnet 2 to 7 or VMnet 9).

8.1.2 Changing the Network Adapter in the Configuration File

These changes to the network installation are possible through the VMware Server Console, but also by manual changes to the configuration file of the virtual machine. With VMware Player this is the only way to change the network configuration and use custom networks.

Automatic assignment of the bridge network is not recommended

The following procedure is recommended to avoid problems with the automatic assignment of the network cards of the host system. This is especially important on host systems with multiple network cards, otherwise you never know which adapter will be assigned to the bridged network and it can happen that the wrong adapter is chosen.

Therefore you should first disable this automatic assignment using **vmnetcfg** and then in the tab **Host Virtual Network Mapping** manually assign each physical card the required VMnet.

Figure 8.3 shows the Virtual Network Editor on VMware Player.

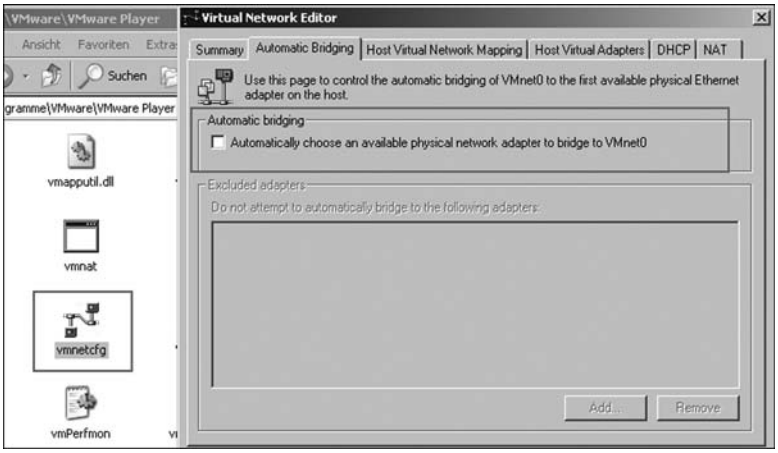

Figure 8.3 – Virtual Network Editor on VMware Player

To configure which network the virtual network card should be connected to, the **Custom** setting works better than Bridged, Host-only or NAT. It is clearly more flexible in case additional networks are required. With VMware Player these entries must be made with a text editor in the configuration file of the virtual machine.

Note
For information about how to make manual changes to the network configuration refer to Chapter 14.

8.1.3 Internal DHCP Server

DHCP service automatically available for IP address assignment

After the installation of VMware Server a virtual DHCP Server is available which assigns dynamic IP addresses to the virtual machines when using Host-only and NAT networks. The address ranges to be used can be modified in the option **Virtual Network Settings** on the VMware Server. With VMware Player use *vmnetcfg* on Windows and *vmware-config.pl* on Linux.

To get there, use *Start menu, VMware, VMware Server, Manage Virtual Networks* (this selection runs *vmnetcfg.exe*) or via the Virtual Machine Console in the Host section on the DHCP tag shown in Figure 8.4.

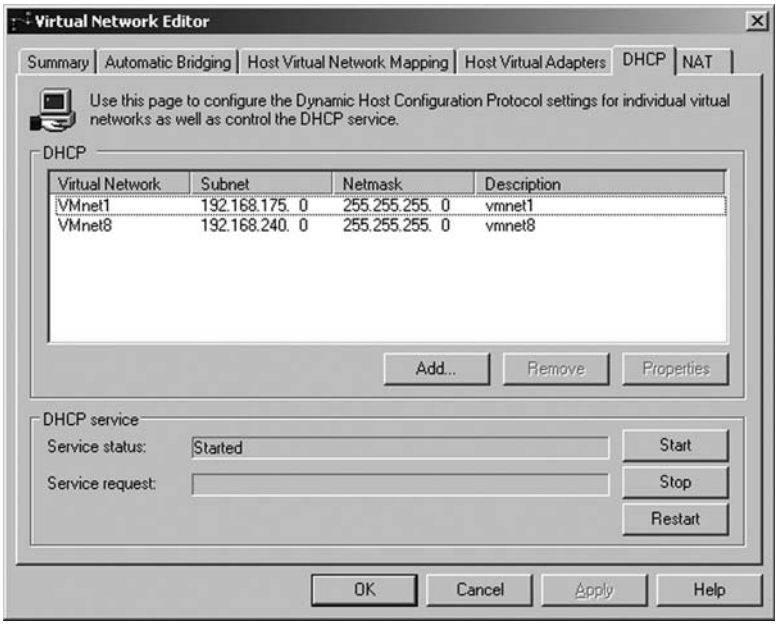

Figure 8.4 – Configuration of the DHCP server on VMware Server

Configure the networks that should use VMware DHCP and the address ranges

Here you can customize the available virtual networks with **Properties**, or delete them with **Remove**. You should remember to make the changes immediately so the current state is displayed correctly. If you have created new networks for which you want to provide DHCP, you can use **Add** and choose the relevant network then use **Properties** to allocate the IP range.

If the DHCP server creates problems or if you want to switch it off, you can control the DHCP service from this management display. By the way you can also control this DHCP service using the conventional Microsoft Windows Services management. The VMware DHCP service can be found under the name **VMware DHCP Service**.

The DHCP configuration is stored in files

The configuration of the DHCP server is also stored on the hard disk in the following files:

1. **vmnetdhcp.conf**: complete configuration of the DHCP server.
2. **vmnetdhcp.leases**: the validity of the DHCP client addresses.

On Windows these files can be found in the VMware Server configuration directory *C:\Documents and Settings\All Users\Application Data\VMware*.

On Linux you can find the configuration files in the directory */etc/vmware/vmnet#*.

8.1.4 Guest-only

This network provides a pure virtual network connection, in which the virtual machines can communicate with each other exclusively within the same VMnet.

This network is also frequently used for the heartbeat network between clustered virtual machines. The hearbeat network is used by cluster members for cluster management communication.

Frequently used for the heartbeat network between cluster members

Note
For information about clustering refer to Chapter 15.

Basically the Guest-only network is ideal for isolated environments, from which no packets should pass to the host system, or to the connected network environment. The VMware DHCP service cannot be used on such a network

Ideal for isolated environments

8.1.5 Host-only

If you install a virtual network card for the host system, the Guest-only network turns into a host-only network. Communication is then possible between the virtual machines and the host system.

By default VMware Server installs a virtual Host-only network adapter which appears as VMnet1 in the list of network cards on the host system. The VMnet8 adapter is also a Host-only network adapter, which additionally offers a NAT service. Within this network by default a DHCP service runs, which can be disabled if required.

VMnet1 is installed as a Host-only network

Routing can be configured between virtual networks

As the host system has a virtual network card, it is possible to route Host-only networks into the physical world by enabling the routing function on the host system and making the necessary routing table entries. Of course this offers some nice possibilities for creating your own virtual address range, with connection to the outside world. Such configurations are often used in test environments.

Create a new Host-only network

To create a new Host-only network, you must switch to the Virtual Network Editor and choose **Host Virtual Adapters** as shown in Figure 8.5 and click on **Add**.

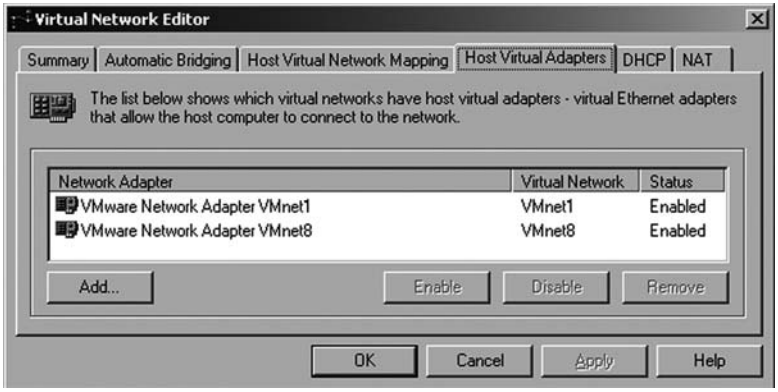

Figure 8.5 – Creating a new virtual network

Now a menu appears, shown in Figure 8.6, in which you can choose one of the available networks. This is then recorded in the list of network cards and is available to you. It is important that this network is in an **Enabled** state. In this case, you find this network in the tab **Host Virtual Network Mapping**, where you can adjust the network address range.

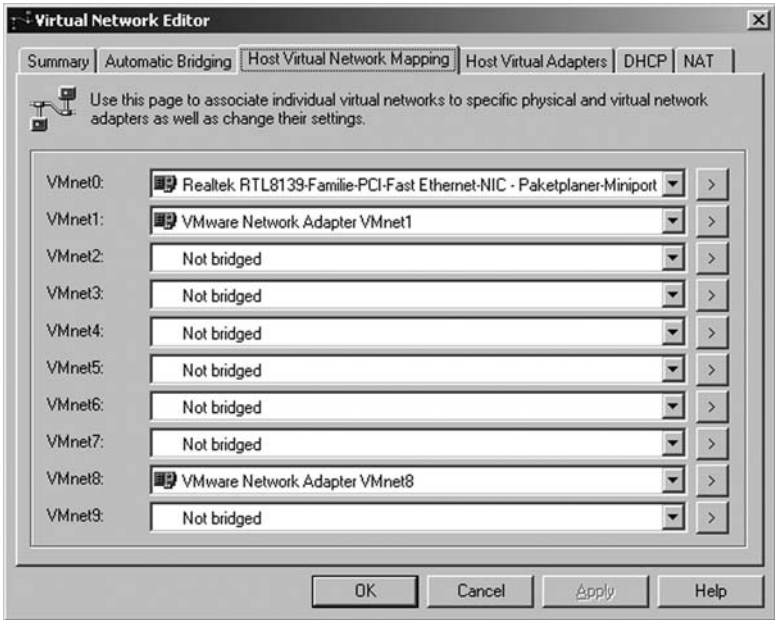

Figure 8.6 – Display and configuration of all virtual networks

You can select a physical adapter for the virtual networks

You can also see in Figure 8.6, that next to each virtual network name there is a field for the adapter being used, and to the far right there is a button with a large arrow. With this button you can jump into all currently available configurations for the virtual adapter. In the case of a Host-only adapter there would be one choice Subnet, allowing you to configure the network address and an option DHCP, if you have activated this service for the internal network.

All networks which are listed here can also be found as virtual network adapters on the host system. On Windows this would be in the start menu under *Settings, Network Connections* or with the command line command *ipconfig*. Under Linux you can view the network configuration with the command *ifconfig*.

8.1.6 Bridged Networks

When using bridged networks VMs are visible in the LAN with their own MAC and IP address

Now we come to the most frequently used type of virtual network, the Bridged network. In this type of network all packets from the guest system are forwarded directly to the physical network card of the host system. The virtual machine is visible in the LAN like any other device with its own MAC address and its own IP address.

Internal VMware DHCP service cannot be used with bridged networks

The internal VMware DHCP server can no longer service this kind of network. Therefore you must either use a fixed IP address or use a DHCP server from your physical network. A Bridged network is not different from a real network adapter. So the virtual machine is reachable in an unrestricted way from the real network. Through VMware Server's hardware emulation this virtual network is protocol independent and can therefore also be used for protocols such as IPX/SPX.

With VMware Server you can install as many Bridged networks as you have physical networks or until you have reached the maximum number of virtual networks. After the installation of the VMware product a Bridged network, named VMnet0 is already available.

To install new networks simply look for a free virtual network (as can be seen in Figure 8.7) and choose from the list of corresponding physical network cards.

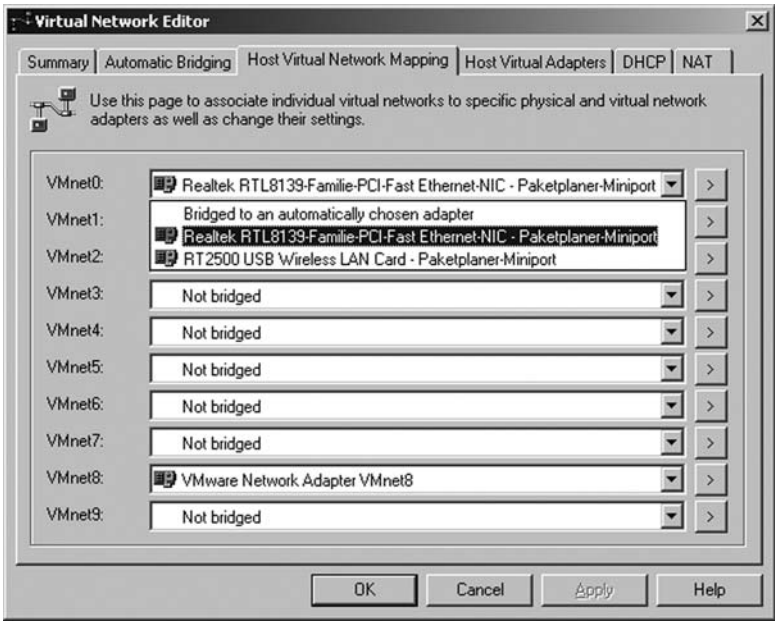

Figure 8.7 – Configuration of the bridged network

When choosing the network card over which the bridge protocol should be used, the option **Bridged to an automatically chosen adapter** is available. If you choose this, VMware Server will automatically look for a physical network card as a bridge. With one network card this is no problem and will by default be used for VMnet0. However, with multiple adapters you should make the assignment yourself, or otherwise you will not have proper control over the virtual network.

With multicple network adapters the option to automatically choose the adapter is not recommended

If you would like to use this function, you can restrict the physical network cards to be used, in that you can mark one or more as an **Excluded Adapter** However this function is unnecessary, as it is better to choose the adapter used for the bridge under **Host Virtual Network Mapping**. Therefore completely dispensing with automatic bridging is generally the most sensible thing to do.

Bridged networks use the VMware Bridge Protocol

When you look at the properties of the physical adapter on the host system after installing the bridge, you will find a protocol called **VMware Bridge Protocol.** This protocol contains, as a property, the name of the virtual network for which it is responsible – in this case the default-installed Bridged network VMnet0 (Figure 8.8).

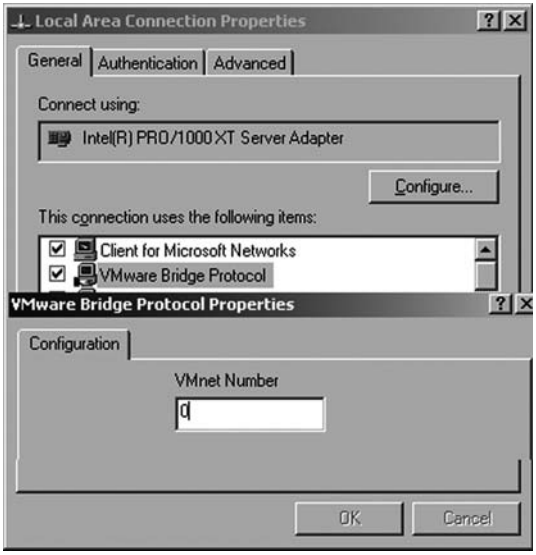

Figure 8.8 – Properties of the physical network card

You can find this property on every physical adapter of the host system which is used as a bridge. This property will show the assignment to the virtual network being used.

Load balancing and fault tolerance are available if the network driver on the host system supports it

If you have multiple network adapters available in your host system, and these can be configured as an "adapter team" using the manufacturer's utility, then this resulting logical network card can be used completely normally with VMware as a bridge adapter. There is no difference as far as your virtual machine is concerned.

8.1.7 NAT Networks

The NAT network (VMnet8) is not different from a Host-only network (such as VMnet1). However there is a NAT service on the host system assigned to this network.

NAT is interesting if you have only one public IP address in the LAN but want to run multiple systems behind it

NAT allows the shared use of the host's physical network - for example, for sharing an Internet connection. Due to the architecture of NAT there are a few restrictions which affect the reachability of the virtual machine from outside. The NAT service translates the internal IP addresses of the virtual machine to the IP addresses of the physical host system adapter. No other network protocol can be used in this case as NAT only works with TCP/IP.

With NAT you can restrict reachability from the network

Through translation of the source address it is only possible to reach the virtual machine over a connection to the physical network adapter, which means that only reply packets from outside can find their way back to the virtual machine. It is not possible to initiate a connection to a host in the private network from the outside world.

A VM behind a NAT cannot be reached from the Internet

For example, if you create a web server in the virtual machine (in VMnet8), it cannot be accessed from the Internet. The reason is that the private IP address range is not usable from the Internet. If you want to make this possible, then certain rules must be installed within the NAT service.

This type of virtual network is mostly used if the virtual machine will mainly remain in the virtual environment, but for example can be used to access the Internet via the physical connection in the real network. The advantage of this is that only the host system must be given an IP address in the real network: All virtual machines within the NAT network are then managed via that address. The reduced direct reachability of the virtual machine from the physical network, combined with a firewall offers improved security so that, for example, worms from the Internet are not able to reach the VM directly.

Note
VMware Server only offers a configurable NAT service on the host system. As the configuration of this service is complex, you should avoid changing the NAT network number (VMnet8).

Figure 8.9 shows the configuration screen for the NAT network.

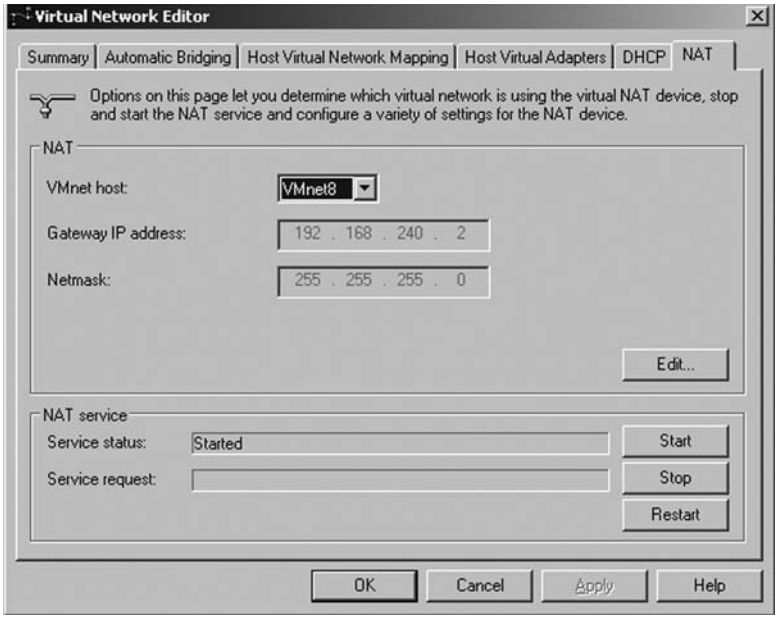

Figure 8.9 – Configuration of the NAT network

Only one NAT service is possible

As you can only operate one NAT service, the VMnet8 network created by the installation is recommended for its ease of use. This is already preconfigured and a DHCP server runs inside it. If you want to disable this DHCP service, you can do this in the same way as has already been explained.

To change the installation of this NAT service, you should go to the **Virtual Network Editor** (Figure 8.9), choose the **NAT** tab and click on **Edit**. Another tip: You can also stop or restart the NAT service from this window if there is any problem.

The NAT Service consists of several configuration files

This service is called **VMware NAT Service** and can also be found in the services management of the operating system. You can find the configuration files in the same directory as the DHCP configuration under the following names:

1. **vmnetnat.conf**: Configuration file for the gateway
2. **vmnetnat-mac.txt**: the MAC address of the gateway

Now back to the topic of changing the configuration via the **Virtual Network Editor**. After choosing **Edit** you will see the configuration of the NAT network shown in Figure 8.10 in which you can configure the IP address of the gateway and the various timeouts, port forwarding and DNS entries. The virtual machine will then use this gateway for all packets intended for the real network, so that the NAT gateway can translate them.

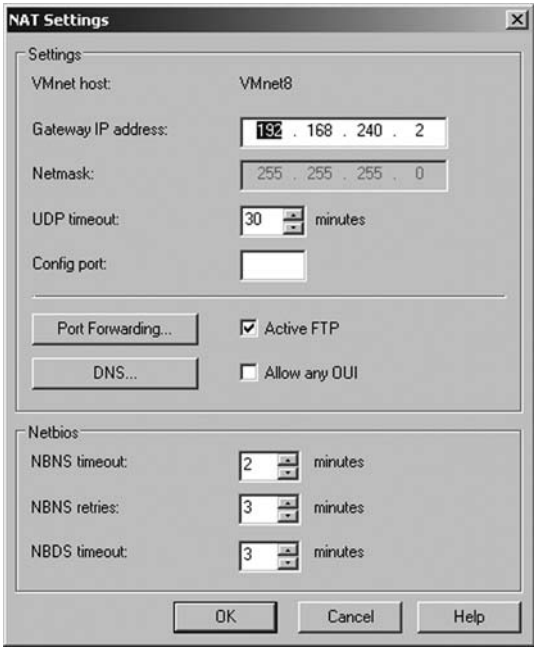

Figure 8.10 – Configuration of the NAT network

If there is a need to run an application in the virtual machine which should be reachable from the real world, you must first configure port forwarding on the host system. This means that you configure a specific port, on which the host system listens. As soon as a packet arrives on this port, the NAT gateway of the host system forwards the packet to the defined virtual machine. As a port can only be used once, each service can only be forwarded over NAT once on the same port.

Port forwarding can be configured if VMs behind the NAT need to be reachable from outside

Let's discuss an example:

How to configure port forwarding

Four virtual machines exist in the NAT network, and each offers a web server running on port 80. On the host system four different ports must now be configured. As on the host system itself there is also a web server, port 80 cannot be used.

A sample configuration is shown in Table 8.2.

Table 8.2 – Table 8.2: Example of NAT Port Forwarding

Port Forwarding Host System	Target System: Port number
1080	VM1 Port 80
1081	VM2 Port 80
1082	VM3 Port 80
1083	VM4 Port 80

Assign port numbers only above 1024

I have chosen the ports on the host system completely arbitrarily. However the port numbers chosen must be greater than 1024 as all lower-numbered ports are officially reserved for applications.

As can be seen in Table 8.2, all packets for port 1080 on the host system will be forwarded directly to the web server of virtual machine VM1 on port 80. For this to work you must enter the address *http://<hostsystem>:1080* in the browser.

This configuration can be created in the Virtual Network Editor in the following way:

Choose **Port Forwarding** In the NAT menu shown in Figure 8.10 which takes you to the next configuration window shown in Figure 8.11, where you can add entries with **Add**. If the network protocol to be used is not TCP, but rather the connectionless UDP protocol, you must enter the ports in the lower area of the window.

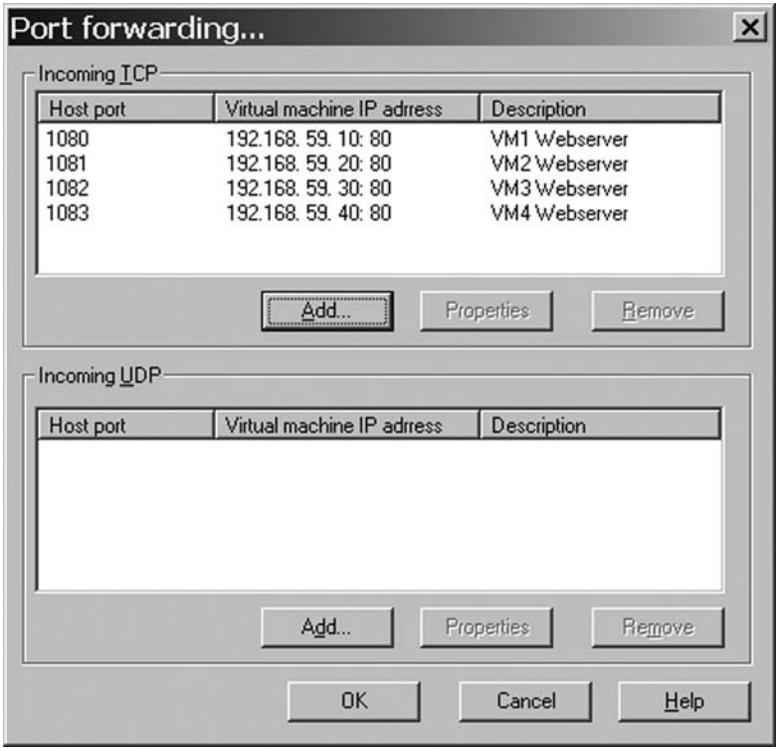

Figure 8.11 – Configuration of Port Forwarding

Forwarding of DNS requests

Another setting which can be configured in the NAT section is the forwarding of DNS requests over the NAT gateway. This means that the gateway can be used as a DNS server for the virtual machines.

To do this choose **NAT settings** (refer to Figure 8.10), **DNS** and in the dialog which follows (Figure 8.12), enter one or more DNS servers which exist in the real network. The timeout, number of retries and DNS entries can also be configured here.

Figure 8.12 – Configuration of DNS forwarding for the NAT gateway

DNS policies are available

There are three DNS policies to choose from and they have the following meaning:

- **order**: The DNS servers are contacted in the order they appear on the list.
- **rotate**: The given DNS servers will be rotated for each request, which means that no server will be contacted twice in a row.
- **burst**: asks the servers randomly and waits for the server which answers first.

The NAT technology is complex and is explained in more detail in Figure 8.13.

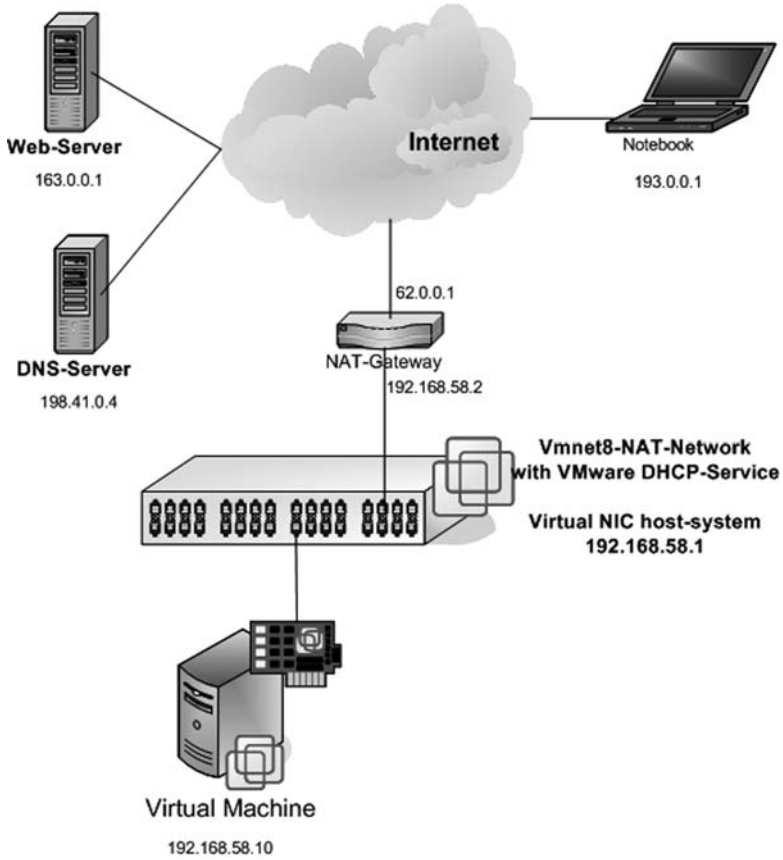

Figure 8.13 – Example environment for a NAT network

How NAT works

As you can see in Figure 8.13, in this environment there is a virtual machine, a Host-only network card on the host system, and a notebook. There is also a DHCP service and a NAT service on the host system. To ensure NAT functionality, an additional network address (Alias) is created on the host's VMnet8 network card which can be used as a gateway.

When a virtual machine is switched on it receives its own IP address from the DHCP service. This IP address comes out of the allocated private address range for VMnet8 (192.168.58.0). In the DHCP options, in contrast to a Host-only network, there are also options to enter a gateway and a DNS server. Both the gateway and the DNS server have the IP address of the alias of the host's VMnet8 network card (192.168.58.2). To access a

web server on the Internet from the virtual machine, the packet is sent to the gateway which replaces the source address with its own public address (62.0.0.1).

A packet sent over NAT

IP packet (Original):
Source: 192.168.58.10 - Destination: 163.0.0.1

IP packet (from NAT):
Source: 62.0.0.1 - Destination: 163.0.0.1

The NAT gateway maintains a list with address mappings

The gateway maintains all connections and address mappings in a list. The receiving web server replies conventionally to the packet to the address of the gateway (62.0.0.1), which is the source address of the packet it received. The NAT gateway then translates the destination address to the address of the virtual machine according to its list.

VMware has a DNS cache implemented

VMware has implemented a DNS cache in the NAT service, which caches all DNS replies. For example, when *www.google.com* is requested, the DNS server configured through the DHCP option is contacted. The reply from the DNS server is then cached at the NAT gateway. If the same request is made a second time, the NAT gateway responds from this cache.

How port forwarding works

It gets even more complex when port forwarding is used. In this case, not only the address but also the port must be modified by the NAT gateway. For example, let's say that you want a simple Internet surfer to access the web server on the virtual machine. We remember that the web server runs on port 80 on the virtual machine and the NAT gateway manages a port forwarding entry for this web server on its own port 1080 (Table 8.2).

A packet sent over NAT with port forwarding

When the Internet surfer enters the address *http://62.0.0.1:1080* in his browser the following happens:

- Packet from Source 62.0.0.5 to Destination 62.0.0.1:1080
- The packet header is translated by the gateway. The destination address and destination port are modified from 62.0.0.1:1080 to 192.168.58.10:80
- Reply packet from the virtual machine: Source 192.168.58.10 to Destination 62.0.0.5
- The packet header is translated by the gateway. The source address is modified from 192.168.58.10 to 62.0.0.1.

Through the central authority of the gateway a network member would notice nothing of this address translation. In this way the communication is not disrupted.

8.2 General Networking Technology

By now you should already have some rough overview of the possible network types for your future, or already existing, virtual environment. Certainly the next few pages will explain the detailed technology and the resulting possible options, but nevertheless the basic structure and configuration of the host system should be clear at this point.

Types of networks

What types of networks can we think of? These include adapter teaming, switched networks, dedicated LAN connections, and VLANs. If these terms mean something to you, but you don't know exactly what the function looks like, the following pages will help.

You could push the boundaries even further and create, for example, a complete intranet structure, including firewall, router and proxy in a small scale. Again, virtual networks offer you all the necessary functions.

8.2.1 Adapter Teaming, Fault Tolerance, Load Balancing

Adapter Teaming

By **Adapter Teaming** we mean the combination of multiple network adapters into one logical device. This means the logical network card is given only one network address. Depending on the support of the network card manufacturer multiple modes can be used, of which the most common are called **Fault Tolerance** and **Load Balancing**.

Fault Tolerance

Fault Tolerance offers pure fault tolerance, which means that I have a logical network interface, which consists of one primary and one or more secondary network cards. Only the primary network card maintains the network connection while the system is running and the secondary network cards only become active if the primary card stops working. The primary card will again take over the network connection if it becomes active again.

Fault tolerance can be implemented in two ways

There are two different ways to implement Fault Tolerance. **Adapter Fault Tolerance** can discover the malfunction of the network card. **Switch Fault Tolerance** can also accommodate the malfunction of the switch. When using Adapter Fault Tolerance, all network cards taking part must be connected to the same switch with Spanning Tree Protocol disabled. However with Switch Fault Tolerance the different switches must be connected together with Spanning Tree Protocol enabled.

Load Balancing

When using Fault Tolerance only one adapter is actively used while all other cards remain passive in their slots. With the technique called **Load Balancing**, also sometimes called **Smart Load Balancing**, all adapters are active at the same time and the speed of all grouped network cards is added up. In the case of a malfunction of one network card the system continues working with the other network cards. However the ports of the combined network cards must be grouped together on the switch using Link Aggregation.

8.2.2 Switched Network

Switches optimize traffic patterns

Switched network refers to a network on which all nodes are connected to one another via switches. In contrast, for example, to a network using a hub, each node does not see the traffic of all other nodes but instead only sees the traffic intended for itself. This also avoids network collisions, since the switch only passes the network packet to the intended node. Additionally, a switched network offers some basic protection against so-called sniffers, devices which can read and decode all the network traffic.

8.2.3 Dedicated LAN Connection

A dedicated LAN connection usually consists of two computers connected to each other over their own separate network. This kind of network is not created using active components such as switches or routers, but instead using a simple crossover cable. This type of dedicated LAN connection is mainly found with clustered servers, in order to establish the so-called heartbeat network.

8.2.4 VLAN (Virtual Local Area Network)

VLANs are virtual networks which are separated from one another on one switch, or divided over multiple physical switches. Therefore one does not necessarily need two switches to create two separate networks. The membership of a host in a VLAN is defined by the VLAN ID.

To connect from one VLAN to another, a router or a layer 3 switch (switch with integrated routing functionality) is required. In order to make a computer available to all VLANs, a so-called **Trunk port** has to be configured and the network card of the system must support this (802.1q-support).

Trunkports are the only ports receiving all packets

Now that you have learned about designing and configuring a virtual network, Chapter 9 introduces the tools, procedures and advanced configurations to manage VMware Server.