



Windows Vista™



Windows Server® 2008

Einrichtung einer VPN Verbindung zum KMS des bm:ukk über Linux

Autor: Franz Furtschegger, Thomas Hauser

Version: 2.0

Veröffentlicht: Juni 2008

Feedback oder Anregungen: ffurtsch@hotmail.com, i-thhaus@microsoft.com

Abstract

Ziel dieses Dokuments ist die Einrichtung einer VPN Verbindung unter Linux zum zentralen Key Management Service des bm:ukk, um die Aktivierung von Windows Server 2008 sowie Windows Vista Clients im Rahmen des MS-ACH Agreements zu ermöglichen.

Voraussetzungen:

- Internetverbindung
- Softwarerouter basierend auf einer aktuellen Linuxdistribution (aktuellem Kernel mit MPPE Support)
- Server mit Windows Server 2008 bzw. Clients mit Windows Vista

Inhalt

1	Übersicht	3
2	Einrichtung der VPN-Verbindung unter Linux auf Basis PPTP	4
2.1	Installation der PPTP-Clientsoftware.....	4
2.2	Konfiguration der PPTP-Clientsoftware	5
2.3	Konfiguration der Routen.....	6
2.4	Adaptierung der Firewallregeln.....	6
2.5	Aktivierung der Einstellungen	6
2.6	Testen der Konfiguration.....	6
3	Konfiguration für den Aktivierungsclient	8
3.1	Konfiguration von Windows Server DNS.....	8
3.2	Konfiguration von BIND.....	11
3.3	Konfiguration unter Windows Server 2008 sowie unter Windows Vista.....	11
4	Testen der Verbindung, und Problembehebung.....	16
4.1	Anpingen des KMS Servers.....	16
4.1.1	Problembehebung:.....	17
4.2	Direktes Ansprechen des KMS Dienstes mittels Telnet	17
4.2.1	Problembehebung:.....	18
5	Aktivierung des Clients	19
6	Appendix A (Einrichten des Clients für ein Separates Gateway).....	24

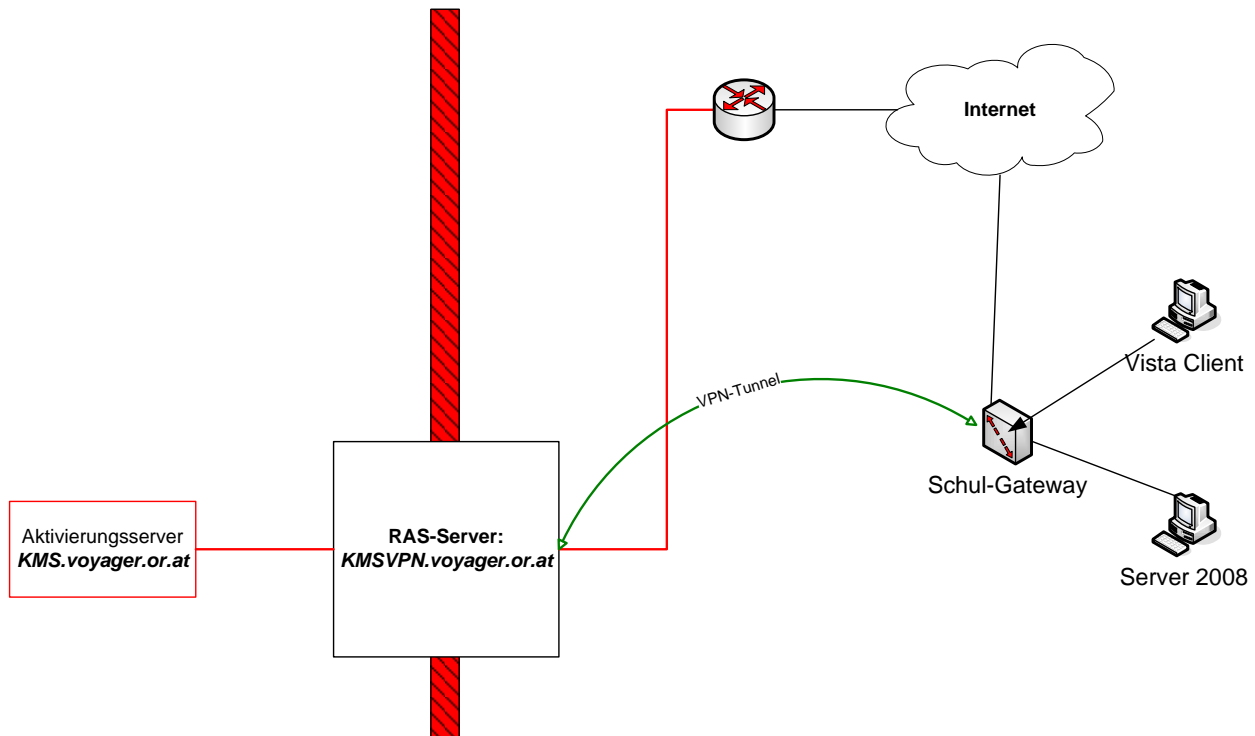
1 Übersicht

Der Key Management Service (KMS) dient zur zentralen Aktivierung von Windows, und wird für alle Schulen, die Server 2008 oder Vista im Rahmen des MS-ACH Agreement lizenziert haben, zentral im BM:UKK gehostet.

Damit sich Windows erfolgreich aktivieren kann, ist eine VPN Verbindung mit dem KMS notwendig. Diese wird von einem Gateway in der Schule permanent aufgebaut. Weiters muss der Aktivierungsclient die Information erhalten welcher KMS für die Aktivierung zuständig ist.

Der KMS hat die Vorteile, dass man zur Installation von Windows keinen Product-Key benötigt, nach einem Hardwaretausch oder Neuaufsetzen des Clients erfolgt die Aktivierung automatisch, und es werden beliebig viele Rechner aktiviert.

Graphische Übersicht der VPN Verbindung und des Aktivierungsvorganges:



2 Einrichtung der VPN-Verbindung unter Linux auf Basis PPTP

Hinweis: In dieser Anleitung kann nicht auf die Eigenheiten der jeweiligen Linux-Distributionen eingegangen werden da sich die einzelnen Distributionen in der Verwendung anderer Verzeichnisstrukturen, anderer Interfacebezeichnungen, etc. auszeichnen. Hier wird die Vorgangsweise anhand einer aktuellen OpenSuSE-Distribution erklärt. Sollten Sie darüber hinaus weitere Informationen benötigen, ziehen Sie bitte die Webseiten des Herstellers Ihrer Linux-Distribution oder die HOWTO-Anleitungen auf Ihren Linux-Installations-CDs bzw. aus dem Internet zu Rate.
Alle hier angegebenen Installations- und Konfigurationsarbeiten sind als User *root* durchzuführen.

Bezeichnungen:

eth0..... Interface mit der öffentlichen IP-Adresse der Schule

eth1..... Interface mit der privaten IP-Adresse (Intranet der Schule)

dsl0..... VPN-Interface (in anderen Distributionen mit ppp0 bezeichnet)

2.1 Installation der PPTP-Clientsoftware

Damit Sie das PPTP (Point to Point Tunneling Protocol) Protokoll unter Linux verwenden können, muss der PPTP-Client installiert werden. Installieren Sie dazu von Ihren Installations-CDs folgende Pakete:

- PPTP Client 1.7.0 (oder höher)
- PPP 2.4.2 (oder höher)

Bemerkung: Sollten Sie den PPTP-Client nicht auf Ihren Installations-CDs auffinden können, so können Sie ihn unter

http://sourceforge.net/project/showfiles.php?group_id=33063

herunterladen. Kann Ihre Linuxdistribution mit PRM-Installationpakete umgehen, so können Sie durch Eingabe von `rpm -i pptp-x.x.x-x.yyy.rpm` (statt `x.x.x-x` setzen Sie bitte die richtige Versionsnummer ein, statt `yyy` den Prozessortyp; so lautet die Datei z.B. `pptp-1.7.0-2.i386.rpm`) den entsprechenden PPTP-Client installieren.

2.2 Konfiguration der PPTP-Clientsoftware

Erstellen Sie im Verzeichnis `/etc/sysconfig/network` die Datei `ifcfg-dsl0` mit folgendem Inhalt:

```
BOOTPROTO='none'  
DEVICE='eth-id-xx:xx:xx:xx:xx:xx'  
MODEM_IP='144.65.14.10'  
NAME='DSL-Verbindung'  
PPPD_OPTIONS='require-mppe-128'  
PPPMODE='pptp'  
PROVIDER='bmuuk'  
STARTMODE='auto'  
UNIQUE=''  
USERCONTROL='no'  
VPIVCI=''
```

Bemerkung: Die Zeile `DEVICE='eth-id-xx:xx:xx:xx:xx:xx'` muss entsprechend Ihrer öffentlichen Netzwerkkarte adaptiert werden. Ersetzen Sie `xx:xx:xx:xx:xx:xx` durch die MAC-Adresse Ihres öffentlichen Interfaces (geben Sie dazu das Kommando `ifconfig eth0` ein und lesen Sie die MAC-Adresse unter `HWaddr=` aus)

Beispiel: `DEVICE='eth-id-00:04:75:85:c8:55'`

Erstellen Sie im Verzeichnis `/etc/sysconfig/network/providers` die Datei `bmuuk` mit folgendem Inhalt:

```
ASKPASSWORD='no'  
AUTODNS='yes'  
DEFAULTROUTE='no'  
DEMAND='no'  
DSLSUPPORTED='yes'  
IDLETIME='0'  
IPADDR=''  
ISDNSUPPORTED='no'  
MODEMSUPPORTED='no'  
MODIFYDNS='yes'  
MODIFYIP='yes'  
PASSWORD='xxxxxxx'  
PHONE=''  
PROVIDER='bmbwk'  
REMOTE_IPADDR=''  
USERNAME='yyyyyy'
```

Bemerkung: Dabei ist `xxxxxxx` durch Ihr Passwort und `yyyyyy` durch Ihre Schulnummer zu ersetzen.

Beispiel: `PASSWORD='azl;wk8u'`
`USERNAME='202099'`

2.3 Konfiguration der Routen

Erstellen Sie dazu im Verzeichnis `/etc/ppp/ip-up.d` die Datei `route_to_kms` mit folgendem Inhalt:

```
#!/bin/sh
VPNSERVER="144.65.14.10"
KMSHOST="144.65.19.33"
PUBLIC_INT="eth0"
VPN_INT="dsl0"
/sbin/route add -host $VPNSERVER $PUBLIC_INT 2> /dev/null
/sbin/route add -host $KMSHOST $VPN_INT 2> /dev/null
```

Ändern Sie die Berechtigung dieser Datei mit folgendem Kommando:

```
chmod 755 /etc/ppp/ip-up.d/route_to_kms
```

2.4 Adaptierung der Firewallregeln

Da üblicherweise auf einem derartigen Linuxrechner eine Firewall installiert und konfiguriert ist, sind noch die dortigen Firewallregeln um folgende Regeln zu ergänzen:

```
iptables -A INPUT -i dsl0 -p icmp -j ACCEPT
iptables -A OUTPUT -o dsl0 -p icmp -j ACCEPT
iptables -A FORWARD -p tcp --dport 1688 -i eth1 -o dsl0 -j ACCEPT
iptables -A FORWARD -p tcp --sport 1688 -o eth1 -i dsl0 -j ACCEPT
iptables -A FORWARD -p icmp -i eth1 -o dsl0 -j ACCEPT
iptables -A FORWARD -p icmp -o eth1 -i dsl0 -j ACCEPT
iptables -t nat -A POSTROUTING -o dsl0 -j MASQUERADE
```

2.5 Aktivierung der Einstellungen

Damit alle getätigten Einstellungen aktiviert werden, führen Sie einen Reboot Ihres Linux-Rechners durch.

2.6 Testen der Konfiguration

- a) Ist die PPTP-Verbindung aktiviert?

Geben Sie folgendes Kommando ein: `ifstat dsl0`

Interface	RX Pkts/Rate	TX Pkts/Rate	RX Data/Rate	TX Data/Rate
	RX Errs/Drop	TX Errs/Drop	RX Over/Rate	TX Coll/Rate
dsl0	21 0	56 0	1004 0	2916 0
	0 0	0 0	0 0	0 0

Sollte unter Interface kein Eintrag (hier `dsl0`) aufscheinen, so ist Ihre PPTP-Verbindung noch nicht aufgebaut worden. Bauen Sie diese Verbindung manuell mit dem Kommando `ifup dsl0` auf.

Überprüfen Sie

- i. die Ausgabe des Kommandos `ifup dsl0`
- ii. warum die PPTP-Verbindung nicht automatisch aufgebaut wurde

b) Ist die Route korrekt gesetzt?

Geben Sie folgendes Kommando ein: `route`

```
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
144.65.19.33 * 255.255.255.255 UH 0 0 0 dsl0
144.65.200.1 * 255.255.255.255 UH 0 0 0 dsl0
0.0.0.0 * 255.255.255.240 U 0 0 0 eth0
0.0.0.0 * 255.255.255.0 U 0 0 0 eth1
link-local * 255.255.0.0 U 0 0 0 eth0
loopback * 255.0.0.0 U 0 0 0 lo
default 0.0.0.0 0.0.0.0 UG 0 0 0 eth0
```

Sollten die beiden Routen unter Iface (hier beide Zeilen mit dsl0) nicht aufscheinen, so führen Sie das Kommando

```
/etc/ppp/ip-up.d/route_to_kms
```

manuell aus. Hat sich danach in Ihrer Routingtabelle immer noch nichts geändert, so ist vermutlich die VPN-Verbindung nicht korrekt aufgebaut worden (siehe Punkt a)

c) Überprüfen Sie, ob Sie vom Vistarechner aus den KMS-Server des bm:uuk anpingen können

```
C:\>ping kms.voyager.or.at

Ping wird ausgeführt für kms.voyager.or.at [144.65.19.33] mit 32 Bytes Daten:

Antwort von 144.65.19.33: Bytes=32 Zeit=24ms TTL=124
Antwort von 144.65.19.33: Bytes=32 Zeit=11ms TTL=124
Antwort von 144.65.19.33: Bytes=32 Zeit=10ms TTL=124
Antwort von 144.65.19.33: Bytes=32 Zeit=10ms TTL=124

Ping-Statistik für 144.65.19.33:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
    Minimum = 10ms, Maximum = 24ms, Mittelwert = 13ms
```

```
C:\>tracert kms.voyager.or.at

Routenverfolgung zu kms.voyager.or.at [144.65.19.33] über maximal 30 Abschnitte:

 1 <1 ms <1 ms <1 ms 10.1.1.1254
 2 <1 ms <1 ms <1 ms 10.1.1.1254
 3 <1 ms 1 ms <1 ms 10.1.1.1254
 4 12 ms 11 ms 10 ms 144.65.200.1
 5 12 ms 12 ms 10 ms kms.voyager.or.at [144.65.19.33]

Ablaufverfolgung beendet.
```

d) Überprüfen Sie die Eintragungen am Ende der Datei `/var/log/messages`, wenn Sie manuell die PPTP-Verbindung stoppen und erneut starten:

```
ifdown dsl0
ifup dsl0
tail -n 50 /var/log/messages
```

3 Konfiguration für den Aktivierungsclient

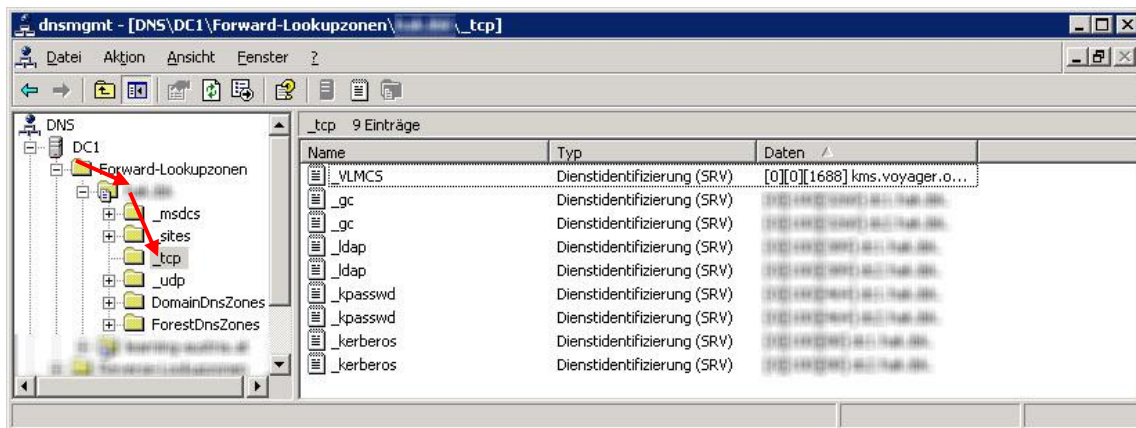
Damit Windows sich erfolgreich Aktivieren kann, muss es die Information erhalten, mit welchem KMS es Kontakt aufnehmen soll.

Es gibt 2 unterschiedliche Vorgehensweisen um diese Information zu verbreiten:

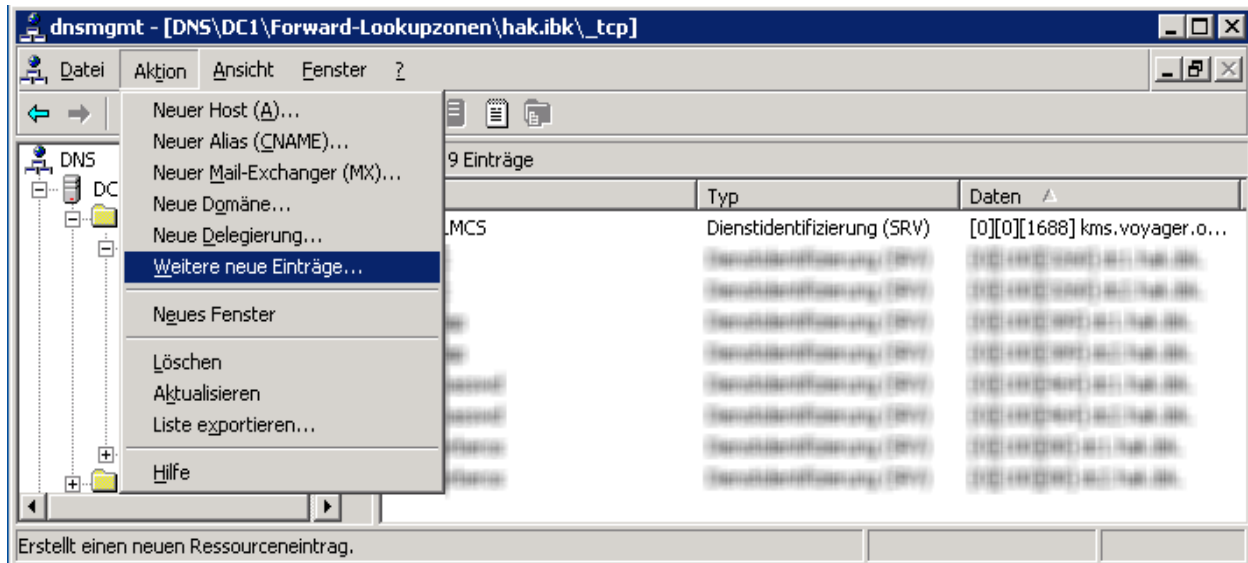
- Über einen Service Record (SRV) am DNS-Server.
- Direkt am Client.

3.1 Konfiguration von Windows Server DNS

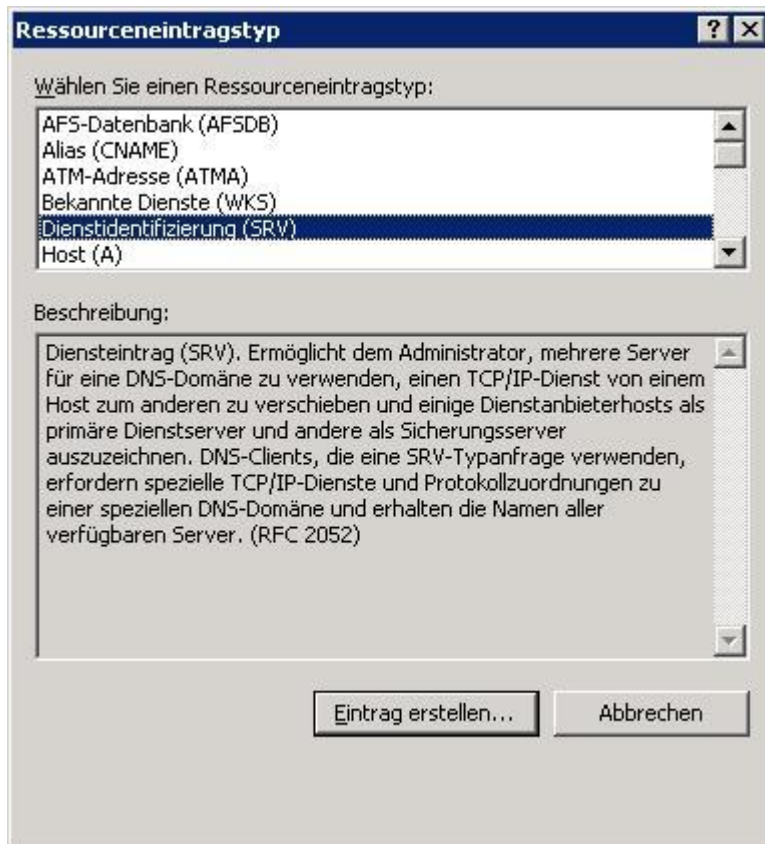
- Starten Sie die DNS-Verwaltungskonzole.
Start > Verwaltung > DNS



- Wechseln Sie zu FORWARD-LOOKUPZONEN > „IHRE DNS ZONE“ > _TCP.



- Wählen Sie AKTION > WEITERE NEUE EINTRÄGE.



- Wählen Sie den Eintrag DIENSTIDENTIFIZIERUNG (SRV) und klicken Sie auf EINTRAG ERSTELLEN...

- Schreiben Sie bei „Dienst:“ `_VLMCS` in das Feld, und bei „Portnummer:“ `1688`. Unter „Host der diesen Dienst anbietet:“ füllen Sie `kms.voyager.or.at` ein.
- Klicken Sie auf OK.

Damit ist die Konfiguration des DNS beendet, und ihre Clients können sich aktivieren.

Hinweis:

Falls Sie die Verbindung testen wollen, folgen Sie den Schritten unter Testen der Verbindung, und Problembehebung (S. 16). Um den ersten Client zur Probe manuell zu aktivieren folgen Sie den Schritten unter Aktivierung des Clients (S. 19).

3.2 Konfiguration von BIND

BIND unterstützt ab der Version 4.9.7 die benötigten SRV Records.

- Öffnen Sie ihre Zonendatei (z.B. ../etc/named/zones/db.test.local).

```
$TTL 86400
$TTL 1440m
$TTL 24h
$TTL 1d
test.local.                IN      SOA      hauser-e1k8f3zw.test.local (
    admin.test.local
    2007030803
    1h
    15m
    4w
    1h)
test.local.                IN      NS       hauser-e1k8f3zw.test.local.
hauser-e1k8f3zw.test.local. IN      A        200.0.0.50
_VLMCS._tcp.test.local.   IN      SRV      0       0       1688    kms.voyager.or.at.
```

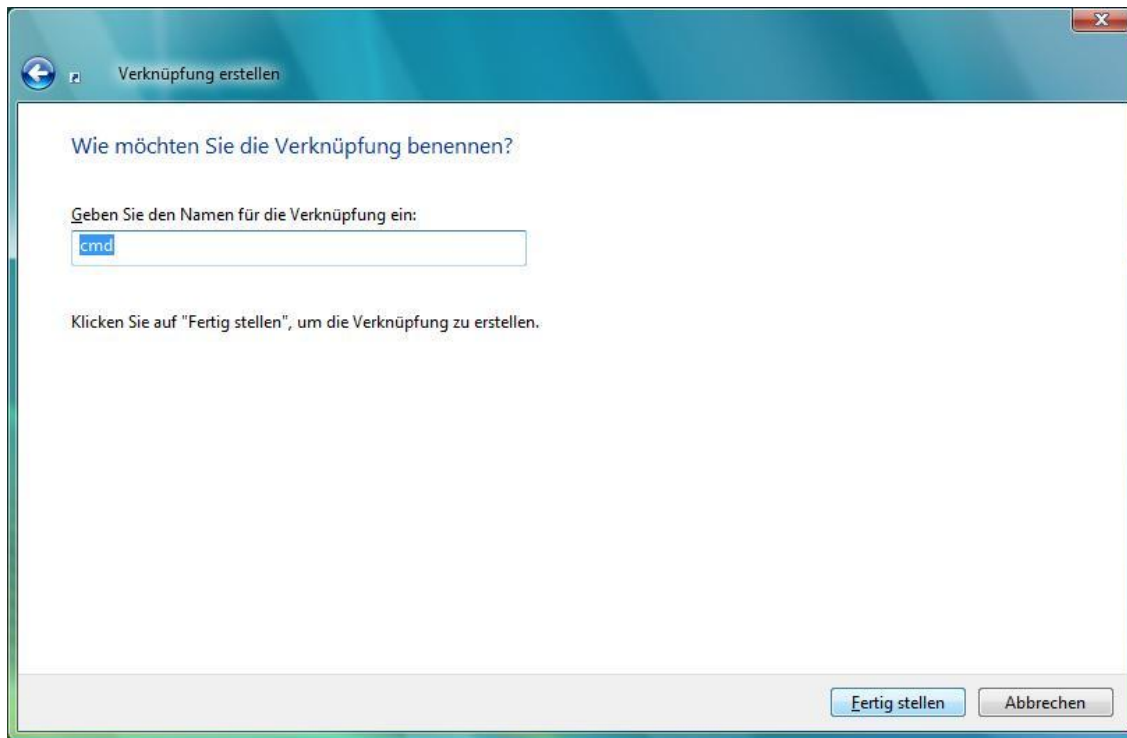
- Fügen Sie den Record
_VLMCS._tcp.IHRE.DOMAIN. IN SRV 0 0 1688 kms.voyager.or.at
(ROT) ein.
Vergessen Sie nicht, dass die Datei mit einer Zeilenschaltung enden muss!
- Ändern Sie die Seriennummer des SOA Records (BLAU), da ansonsten die Zonendatei nicht neu geladen wird.
- Speichern Sie die Datei ab.
- Starten Sie BIND neu.

Hinweis:

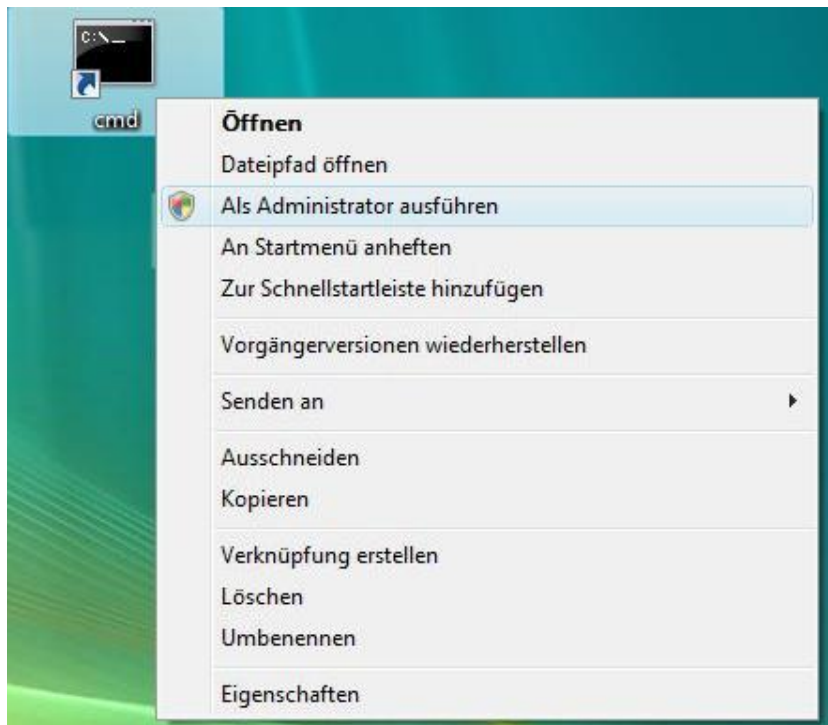
Falls Sie die Verbindung testen wollen, folgen Sie den Schritten unter Testen der Verbindung, und Problembehebung (S. 16). Um den ersten Client zur Probe manuell zu aktivieren folgen Sie den Schritten unter Aktivierung des Clients (S. 19).

3.3 Konfiguration unter Windows Server 2008 sowie unter Windows Vista

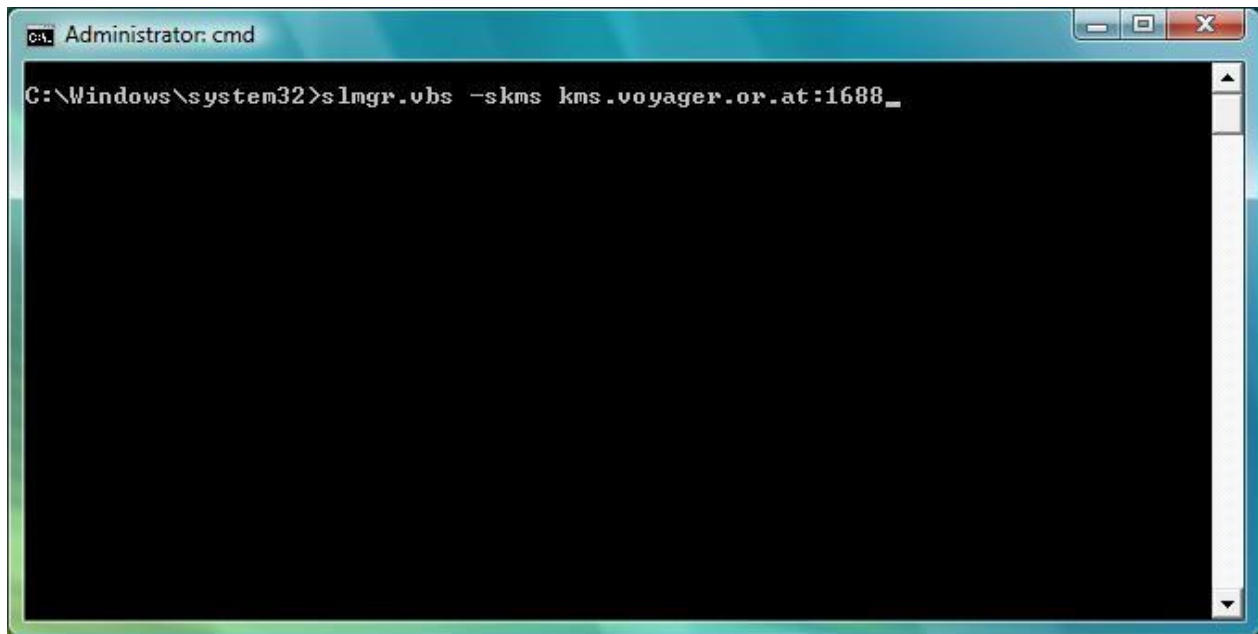
Falls Sie keinen DNS zur Verfügung haben, können Sie am Rechner direkt eintragen, welcher KMS zu kontaktieren ist. Dazu benötigen Sie lokale Administratorrechte.



- Klicken Sie auf FERTIGSTELLEN.

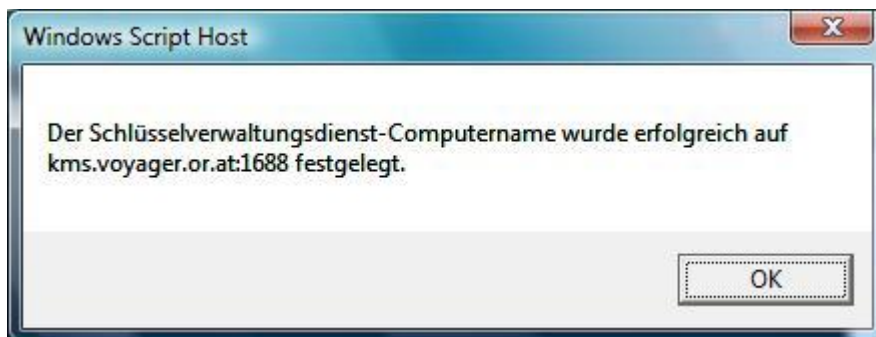


- Öffnen Sie das Kontextmenü der Verknüpfung, indem Sie darauf rechtsklicken, und wählen Sie ALS ADMINISTRATOR AUSFÜHREN. Bestätigen Sie die folgende Sicherheitswarnung mit FORTSETZEN.

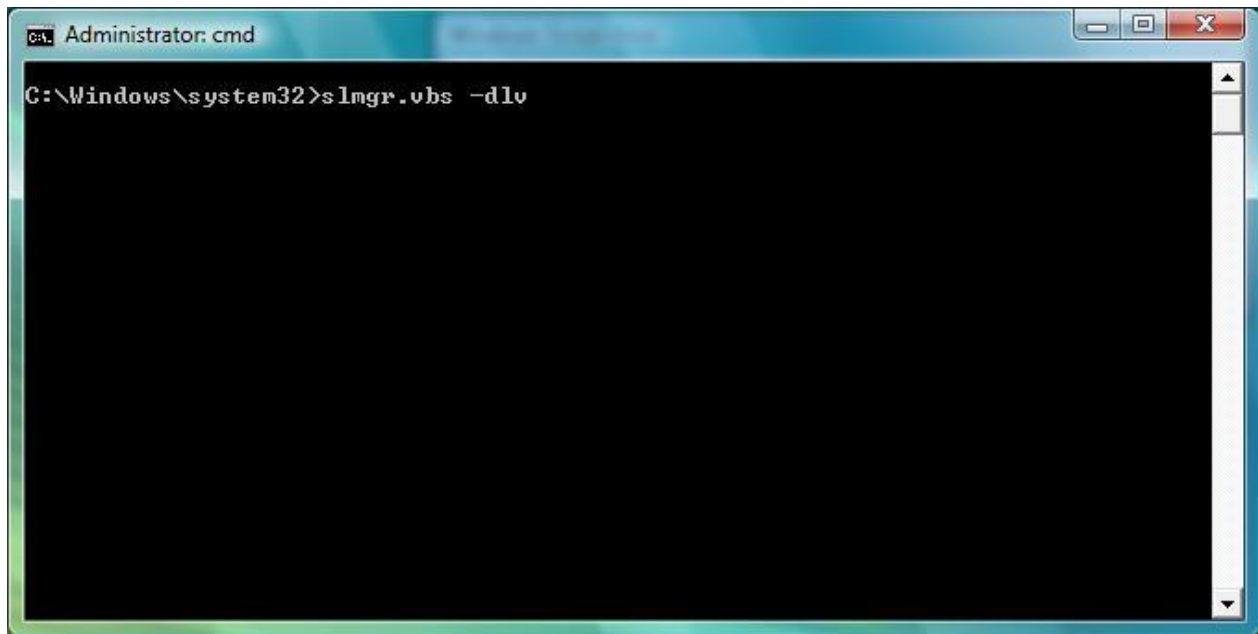


```
Administrator: cmd
C:\Windows\system32>slmgr.vbs -skms kms.voyager.or.at:1688_
```

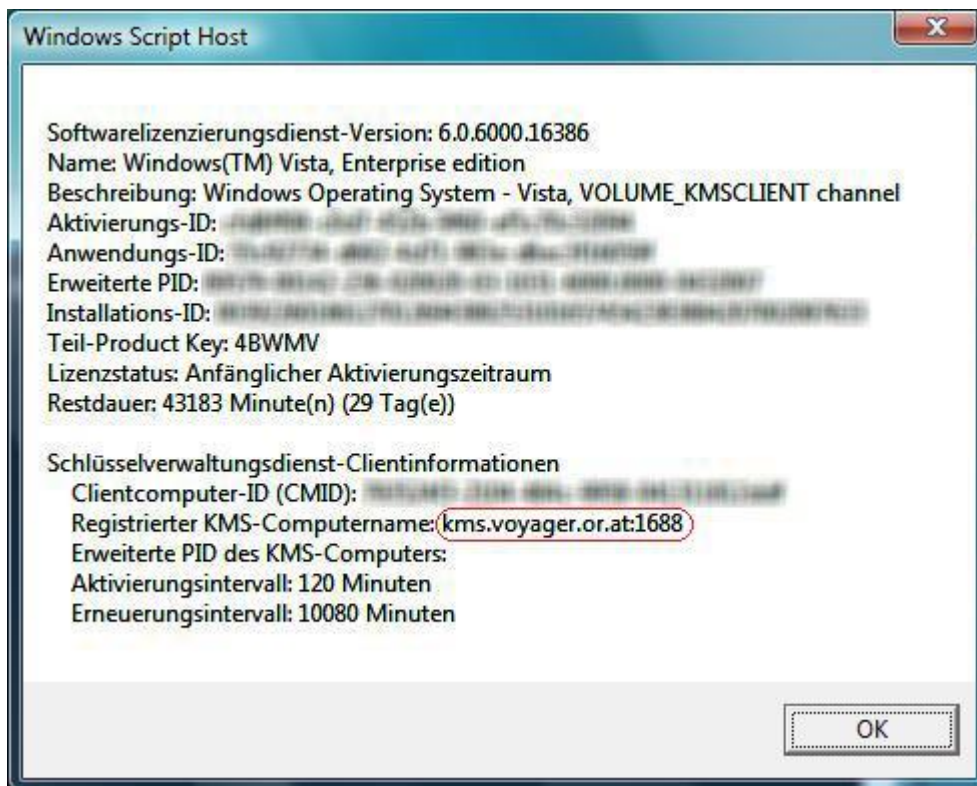
- Schreiben Sie `slmgr.vbs -skms kms.voyager.or.at:1688` und führen Sie den Befehl mit der Taste ENTER aus.



- Nach kurzer Wartezeit (<1 min) erhalten Sie zur Bestätigung obige Meldung. Klicken Sie auf OK.



- Um den Eintrag zu verifizieren, schreiben Sie `slmgr.vbs -dlv` in die Eingabeaufforderung und drücken ENTER.



- Jetzt sollte bei „Registrierter KMS-Computername:“ `kms.voyager.or.at:1688` aufscheinen.

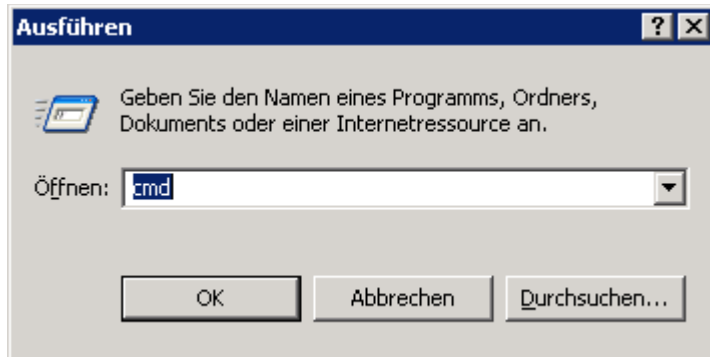
Damit ist die Einrichtung des KMS am Client abgeschlossen.

4 Testen der Verbindung, und Problembehebung

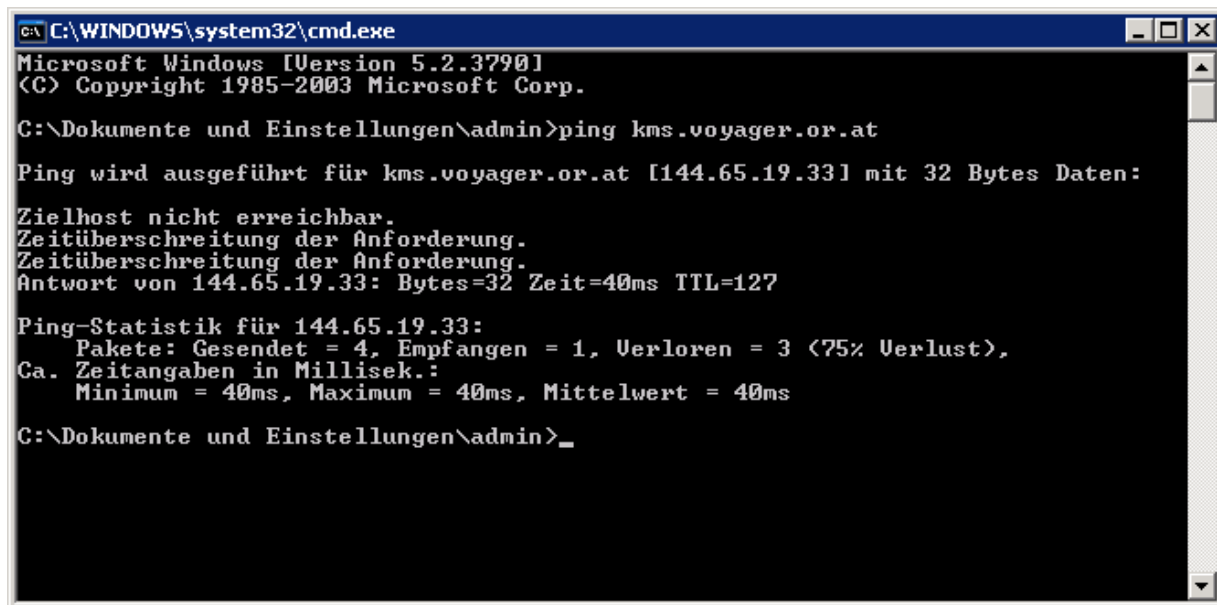
Um sicherzustellen, dass sich Ihre Clients nun aktivieren können, müssen einige Tests durchgeführt werden.

4.1 Anpingen des KMS Servers

Wechseln Sie zu einem Client der Ihr Gateway eingerichtet hat.



- Klicken Sie auf START > AUSFÜHREN, oder drücken Sie auf der Tastatur WINDOWSTASTE + R. Tragen Sie CMD ein, und bestätigen mit OK.



- Schreiben Sie ping kms.voyager.or.at und drücken Sie die ENTER Taste. Sie sollten nun nach eventuell fehlerhaften Versuchen (bis das Gateway die Verbindung aufgebaut hat) einen erfolgreichen Ping erhalten.

4.1.1 Problembehebung:

Sollten Sie die Meldung,

Ping-Anforderung konnte Host "kms.voyager.or.at" nicht finden. Überprüfen Sie den Namen, und versuchen Sie es erneut.

erhalten, verwenden Sie den Befehl `ping 144.65.19.33`.

Wenn Sie darauf Ping Antworten erhalten, müssen Sie bei den Schritten 3.1, 3.2 und 3.3 anstatt des DNS Namens `kms.voyager.or.at` die IP Adresse `144.65.19.33` verwenden.

Hinweis zu Schritt 3.3:

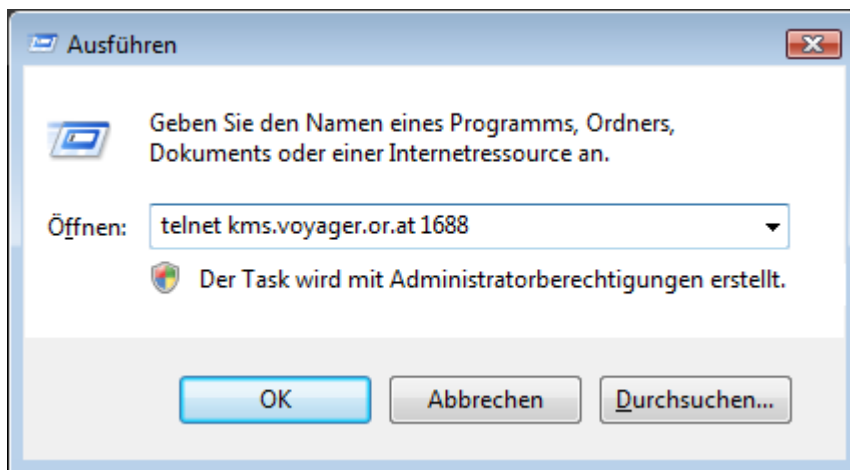
Um einen bereits eigetragenen KMS Server aus der Konfiguration von Windows Vista wieder zu löschen, verwenden Sie den Befehl `s1mgr.vbs -ckms`.

4.2 Direktes Ansprechen des KMS Dienstes mittels Telnet

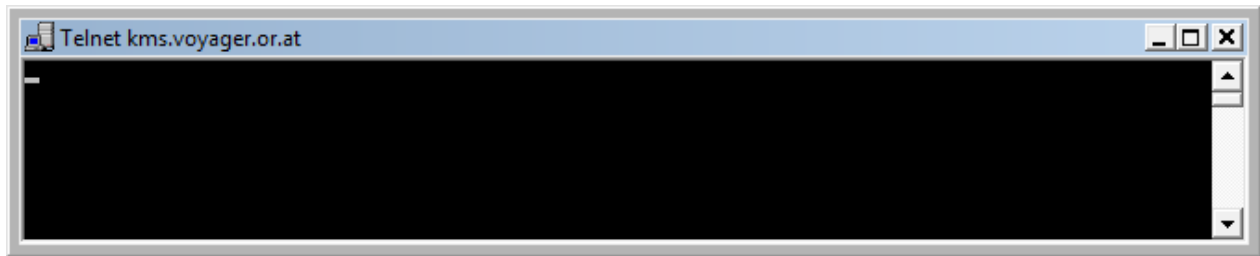
Wenn Sie erfolgreich einen Ping zum KMS Server senden konnten, überprüfen Sie nun, ob Sie eine Verbindung zum Aktivierungsdienst erhalten.

Dazu wird das Programm Telnet benötigt, das unter Windows Vista separat unter „Windows Funktionen ein- oder ausschalten“ in der Systemsteuerung aktiviert werden muss.

- Klicken Sie auf Start > Systemsteuerung > Programme > Windows Funktionen ein- oder ausschalten, und suchen Sie das Programm Telnet-Client. Aktivieren Sie das Häkchen, und bestätigen Sie mit OK.



- Klicken Sie auf START > AUSFÜHREN, oder drücken Sie auf der Tastatur WINDOWSTASTE + R.
- Tragen Sie `telnet kms.voyager.or.at 1688` bzw. `telnet 144.65.19.33 1688` ein, und bestätigen mit OK.



- Als Erfolgsmeldung erhalten Sie ein schwarzes Fenster mit blinkendem Cursor.

4.2.1 Problembehebung:

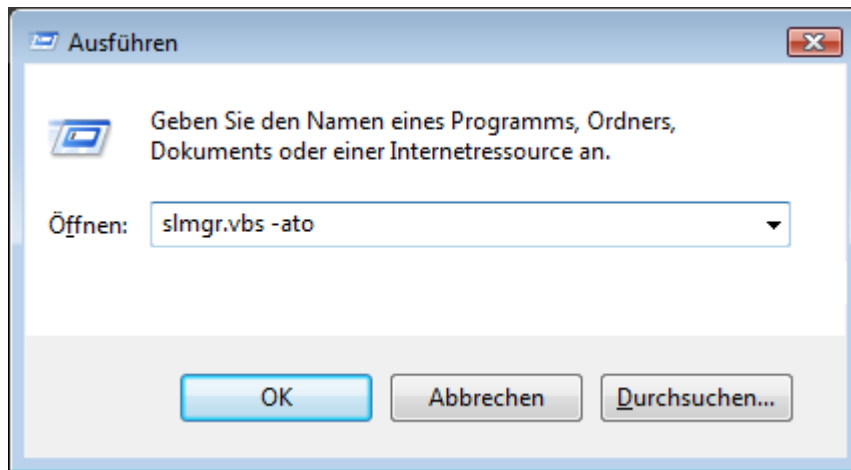
Sollten Sie hier eine Fehlermeldung erhalten, überprüfen Sie alle Firewalls bis zum VPN Tunnel (lokale Firewall, IPTables, usw.). Sie müssen keine Firewallinstellungen nach dem VPN Tunnel überprüfen (ISP, Router, usw.), da sich die Pakete ab diesem Punkt im Tunnel befinden, und für die Firewall nicht mehr sichtbar sind. Sollten Sie ein separates Gateway verwenden, überprüfen Sie, ob Sie auch die Route am Client wie unter Appendix A (Einrichten des Clients für ein Separates Gateway) (S. 24) korrekt eingerichtet haben.

5 Aktivierung des Clients

Nachdem alle Konfigurationsschritte abgeschlossen sind, und die Verbindung zum KMS Server erfolgreich getestet wurde, können Sie nun den ersten Client manuell zur Aktivierung anregen. Generell aktivieren sich alle Windows Vista bzw. Server 2008 Rechner automatisch, sobald die Konfiguration erfolgreich abgeschlossen ist.

Führen Sie die folgenden Schritte am Client aus.

- Klicken Sie auf **START > AUSFÜHREN**, oder drücken Sie auf der Tastatur **WINDOWSTASTE + R**.



- Tragen Sie `slmgr.vbs -ato` ein, und bestätigen mit **OK**.

Nach einer kurzen Wartezeit (<1 Minute) erhalten Sie eine Rückmeldung über den Aktivierungsversuch.

Wenn Sie zu Testzwecken den Lizenzierungsstatus zurücksetzen wollen, geben Sie `slmgr.vbs -rearm` ein.

Auf den folgenden Seiten finden Sie eine Aufstellung der möglichen Fehlercodes, mit der dazugehörigen Beschreibung auf Englisch.

Error Code	Error Message	Possible Cause	Troubleshooting Steps
0xC004F00F	The Software Licensing Server reported that the hardware ID binding is beyond level of tolerance.	The hardware has changed or the drivers were updated on the system.	MAK - Reactivate the system during the Out of Tolerance grace period using either online or phone activation. ¹ KMS - Reboot or run <code>slmgr.vbs -ato</code> ²
0xC004F014	The Software Licensing Service reported that the product key is not available	No product keys are installed on the system.	Install MAK product key.
0xC004F02C	The software Licensing Service reported that the format for the offline activation data is incorrect.	The system has detected that the data entered during phone activation is not valid.	Verify Confirmation ID is correctly entered.
0xC004F035	The software Licensing Service reported that the computer could not be activated with a Volume license product key. Volume licensed systems require upgrading from a qualified operating system. Please contact your system administrator or use a different type of key.	Volume editions are licensed for upgrade only. Installing a Volume OS on a computer that does not have a qualifying OS installed is not supported.	Install a qualifying version of a Microsoft OS, and then reinstall the Volume OS.
0xC004F038	The software Licensing Service reported that the computer could not be activated. The count reported by your Key Management Service (KMS) is insufficient. Please contact your system administrator.	Count on KMS host is not high enough. KMS count must be 25 or greater.	More machines are needed in the KMS pool (minimum of 25) for KMS clients to activate. Run <code>Slmgr.vbs -dli</code> to get current count on the KMS host.
0xC004F039	The software Licensing Service reported that the computer could not be activated. The Key Management Service (KMS) is not enabled.	KMS host is installed but the KMS host is not activated.	Activate the KMS host with either online or phone activation.

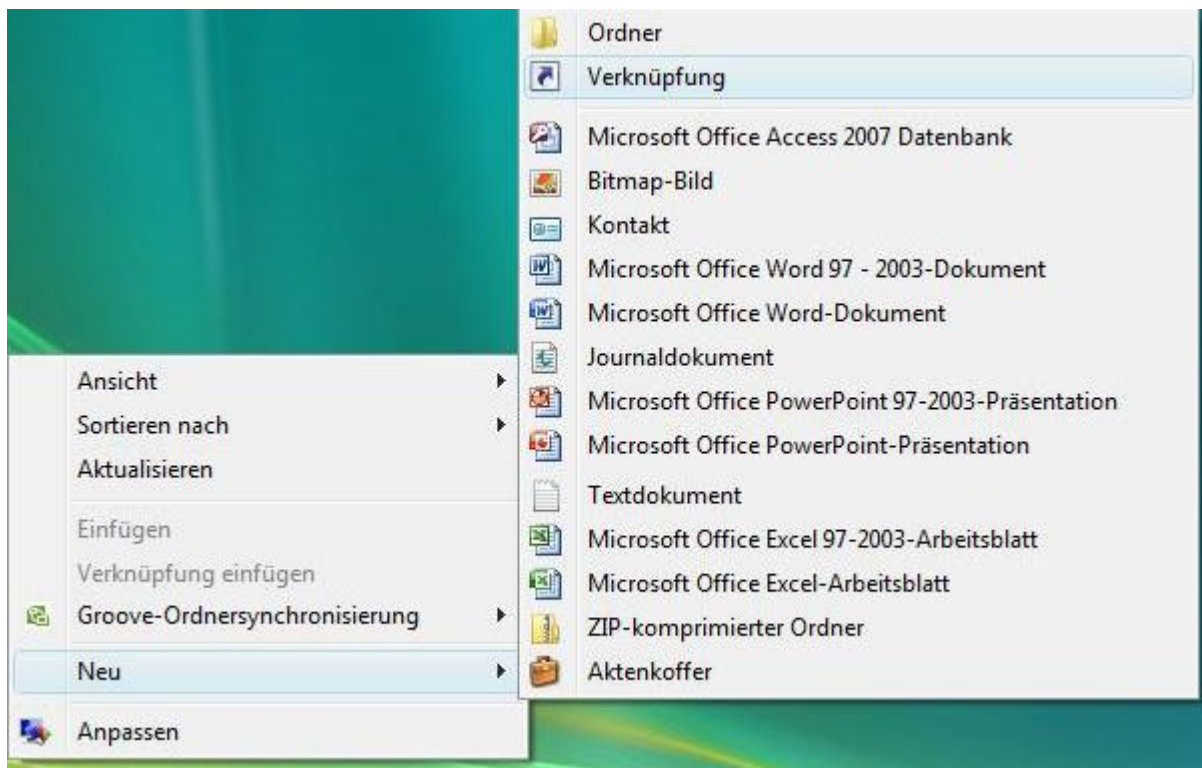
0xC004F041	The software Licensing Service determined that the Key Management Server (KMS) is not activated. KMS needs to be activated.	KMS host is not activated.	Activate the KMS host with either online or phone activation.
0xC004F042	The software Licensing Service determined that the specified Key Management Service (KMS) cannot be used.	Mismatch between KMS client and KMS host.	Check that a Beta client is not activating against a Released KMS host, or a Released client against a Beta KMS host.
0xC004F050	The Software Licensing Service reported that the product key is invalid.	This can be caused by a typo in the KMS key, or by typing in a Beta Key on a Released version of the OS.	Install the appropriate KMS key on the corresponding version of Windows. Check the spelling. If the key is being copied and pasted, make sure that em-dashes have not been substituted for the dashes in the key.
0xC004F065	The software Licensing Service reported that the application is running within the valid non-genuine period.	Windows Genuine Advantage has determined the system is not Genuine. The system will continue to run during the non-Genuine grace period.	Obtain and install a Genuine product key and activate the system during the grace period. At the end of the grace period, the system will go into non-Genuine RFM mode.

0xC004F066	The Software Licensing Service reported that the product SKU is not found.	Volume media has been used with a non-Volume key.	Match the product key to the OS edition. Contact the PA Call Center for assistance.
0xC004F069	The Software Licensing Service reported that the computer could not be activated. The Key Management Service (KMS) determined that the request timestamp is invalid.	The system time on the client computer is too different from the time on the KMS host.	Time sync is important to system and network security for a variety of reasons. Fix this issue by changing the system time on the client to sync with the KMS. Use of an NTP time source or AD for time synchronization is recommended. This issue uses UTP time, and is independent of Time Zone selection.
0x80070005	Access denied the requested action requires elevated privileges.	UAC (User Access Control) prohibits activation processes from running in a non-elevated command prompt.	Run <i>slmgr.vbs</i> from an elevated command prompt. Right click cmd.exe and choose "Run as Administrator".
0x8007232B	DNS name does not exist.	The KMS client cannot find KMS SRV resource records in DNS.	<ul style="list-style-type: none"> . Point the KMS client to KMS host using <i>slmgr.vbs -skms <kmshostname></i> . Install KMS host. . Obtain a MAK and change the product . Troubleshoot DNS.

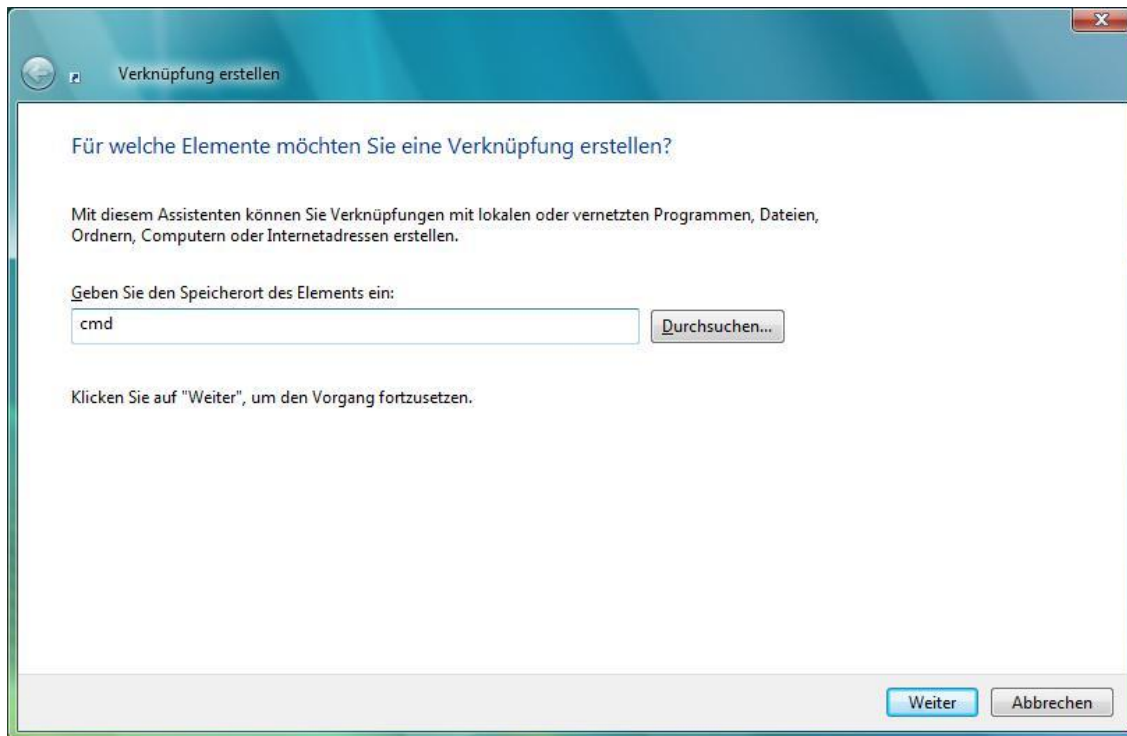
0x800706BA	The RPC server is unavailable.	Firewall settings are not configured on the KMS host or DNS SRV records are stale.	Ensure the KMS port is allowed access through the firewall on the KMS host or ensure SRV records point to a valid KMS host. Troubleshoot network connections.
0x8007251D	No records found for DNS query.	The KMS client cannot find KMS SRV resource records in DNS.	Troubleshoot network connections and DNS.

6 Appendix A (Einrichten des Clients für ein Separates Gateway)

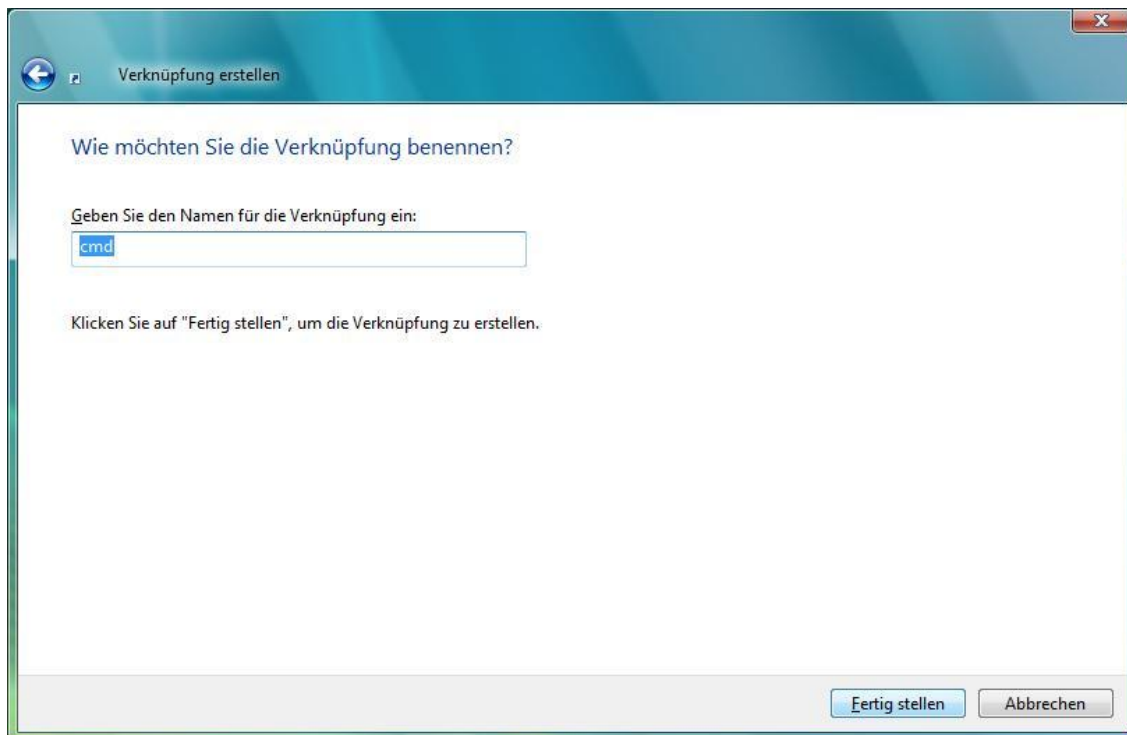
Falls Sie für die VPN Standort zu Standort Verbindung nicht das Standardgateway verwenden, müssen Sie am Client eine permanente Route eintragen.



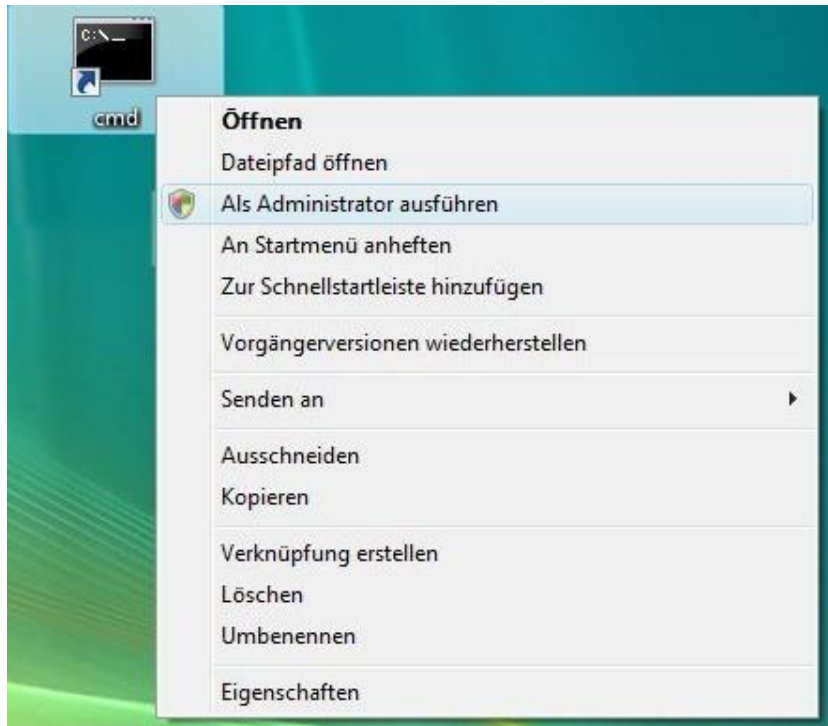
- Erstellen Sie eine neue Verknüpfung auf dem Desktop. Rechtsklicken Sie dazu auf den Desktop, und wählen Sie NEU > VERKNÜPFUNG.



- Tragen Sie nun cmd ein, und klicken Sie auf WEITER.



- Klicken Sie auf FERTIGSTELLEN.



- Öffnen Sie das Kontextmenü der Verknüpfung, indem Sie darauf rechtsklicken, und wählen Sie ALS ADMINISTRATOR AUSFÜHREN. Bestätigen Sie die folgende Sicherheitswarnung mit FORTSETZEN.

```
C:\Windows\system32>route -p add 144.65.19.33 10.1.1.254_
```

- Schreiben Sie `route -p add 144.65.19.33 xxx.xxx.xxx.xxx`. Wobei die zweite IP-Adresse durch die Ihres VPN-Gateways ersetzt werden muss. Führen Sie nun den Befehl mit der Taste ENTER aus.
- Sie erhalten die Rückmeldung „Ok!“, und die Konfiguration ist abgeschlossen.