

Cisco Router mit T-Home VDSL

Daniel Demmler
CCIE #21033

Inhaltsverzeichnis

Voraussetzungen.....	2
Physikalisches Setup.....	2
Vorbereiten des Routers.....	2
1. Allgemeine nützliche Einstellungen.....	2
2. Konfiguration der Seriellen Konsole.....	2
3. Konfiguration der Virtual Terminal Lines.....	2
4. Aktivierung des Logging.....	3
5. Einstellen der Zeitzone und des NTP-Servers.....	3
Konfiguration externes Interface zum VDSL-Modem.....	3
Konfiguration eines Dialer-Interface zur Internetwahl.....	4
Setup des Dialer-Interface mit den T-Online Zugangsdaten.....	4
Konfiguration des Routings.....	4
Troubleshooting der Internetverbindung.....	5
Erstellen einer Access Control List (Firewallfunktion).....	6
Konfiguration der Filterregeln für die lokale Firewall.....	6
Aktivierung der Firewall.....	6
Troubleshooting der Firewall.....	6
Konfiguration internes LAN Interface.....	7
Anlegen eines DHCP-Pools.....	7
Anlegen eines einfachen DHCP-Pools im IOS.....	7
Troubleshooting des IOS DHCP-Servers:.....	8
Aktivierung von NAT/PAT.....	8
Konfiguration des NAT+PAT für ausgehenden Internet-Verkehr (inside-to-outside).....	8
Aktivierung des NAT+PAT.....	8
Troubleshooting des NAT/PAT.....	9
Einschalten des lokalen DNS-Servers.....	9
Impressum und rechtliche Hinweise.....	10

Voraussetzungen

Als Voraussetzung für die hier weiter unten beschriebenen Konfigurationen wird angenommen, dass ein T-Home VDSL-25 oder VDSL-50 Anschluss vorhanden ist sowie gültige Zugangsdaten vorliegen.

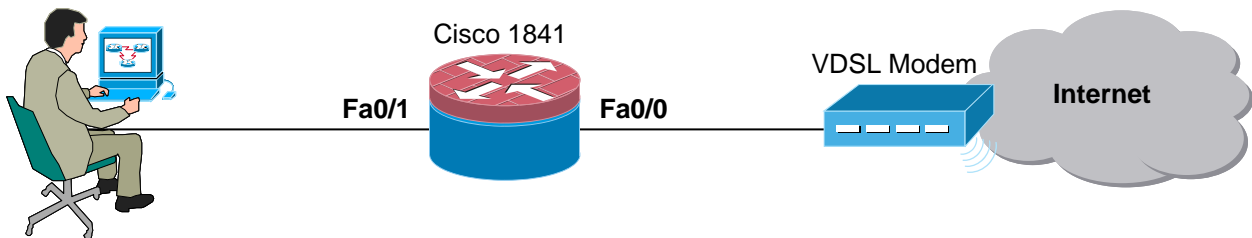
Die Einrichtung von IPTV und des T-Home Mediareceivers (Entertainment) und die dafür notwendige Multicast-Konfiguration wird in einem separaten Dokument beschrieben. Nachfolgend wird erläutert, welche IOS commands benötigt werden um den VDSL Internetzugang in Betrieb zu nehmen.

Auf folgenden Hardware-Plattformen wurde die nachfolgende Konfiguration getestet:
Cisco Router 871 / 1812 / 1841 / 2811 mit der IOS Version 12.4(15) und verschiedene Feature-Sets.

Physikalisches Setup

In unserem Testlabor haben wir die VDSL Config auf verschiedenen Hardware-Plattformen getestet, nachfolgende Kapitel beziehen sich konkret auf einen Cisco Router 1841 der wie folgt angeschlossen wurde:

Privates LAN
192.168.1.0 /24



Falls andere Router-Modelle verwendet werden, können einzelne Kommandos abweichen, insbesondere die Interfacebezeichnungen wie Fa0/0 könnten dann anders heißen, z.B. E0/0 oder Gi0/0. Falls ein Router mit eingebautem Switch verwendet wird, wie z.B. 876 oder 1812, dann heißt das interne LAN-Interface **Vlan1**.

Vorbereiten des Routers

1. Allgemeine nützliche Einstellungen

Zuerst bitte den lokalen DSN-lookup ausschalten, damit falsch eingegebene Befehle nicht jedes Mal als Hostname interpretiert werden. Der domain-name ist optional, wird aber benötigt falls ein SSH-Zertifikat generiert werden soll um später die Administration des Routers via SSH zu ermöglichen.

```
!  
no ip domain lookup  
ip domain name ditc.eu  
!
```

2. Konfiguration der Seriellen Konsole

Das Grundsetup der seriellen Konsole inkl. tuning der Logmeldungen (kein Zeilenumbruch).

```
!  
line con 0  
  exec-timeout 60 0  
  logging synchronous  
  password cisco  
  login  
!
```

3. Konfiguration der Virtual Terminal Lines

Die Virtuellen Terminal Lines regeln den remote Zugriff auf den Router (z.B. via Telnet oder SSH).

```

!
service linenumbers
!
line vty 0 4
  exec-timeout 60 0
  logging synchronous
  password cisco
  login
  transport input telnet ssh
!

```

4. Aktivierung des Logging

Ein vernünftiges Logging wird benötigt um sinnvolles Troubleshooting zu ermöglichen.

```

!
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service sequence-numbers
logging buffered 102400 debugging
!

```

5. Einstellen der Zeitzone und des NTP-Servers

Die aktuelle Uhrzeit kann im Internet abgefragt werden, der hier verwendete NTP-Server ist zuverlässig und kostenlos nutzbar. Nach Aktivierung enthalten auch alle Logmeldungen die genaue Uhrzeit.

```

!
clock timezone CET 1
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
ntp server 192.53.103.108
!

```

Konfiguration externes Interface zum VDSL-Modem

Zunächst ist die Konfiguration des FastEthernet Interface notwendig an welchem das externe VDSL-Modem steckt. Für VDSL ist im Gegensatz zum normalen T-DSL ein zusätzliches Subinterface notwendig um dem VDSL-Modem mit Vlan 7 getaggte Frames nach 802.1Q zu senden (VLAN-trunk). Alternativ könnte man das auch mit einem virtuellen „Interface Vlan 7“ machen, diese Variante wird jedoch nicht empfohlen. Weiterhin aktivieren wir das PPPoE Protokoll auf dem Subinterface und weisen dieses dann dem Dial-Pool 1 zu.

```

!
interface FastEthernet0/0
  no ip address
  duplex auto
  speed auto
  no shutdown
!
interface FastEthernet0/0.7
  description ### ext. Modem zum VDSL ###
  encapsulation dot1q 7
  pppoe enable group 1
  pppoe-client dial-pool-number 1
  no cdp enable
!

```

Sobald man das Interface mit „no shutdown“ aktiviert hat, erscheinen folgende Logmeldungen:

```

*Jul 21 13:41:16.047 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to up
*Jul 21 13:41:17.047 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
*Jul 21 13:42:05.387 CEST: %LINK-3-UPDOWN: Interface Virtual-Access1, changed
state to up
*Jul 21 13:42:06.387 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up

```

Zur Verifizierung ob der physikalische Link zum Modem funktioniert, kann der Interface-Status wie folgt abgefragt werden. Die grauen Markierungen zeigen den Soll-Zustand, der Status „up/up“ beweist die korrekte Funktion. Sollte der Status auf „up/down“ stehen, muss das Patchkabel zwischen Router und Modem geprüft werden.

```
Router#show ip interface brief
Any interface listed with OK? value "NO" does not have a valid configuration

Interface                IP-Address      OK? Method Status
Protocol
FastEthernet0/0          unassigned      YES manual up
FastEthernet0/0.7        unassigned      YES unset  up
...
Router#
```

Konfiguration eines Dialer-Interface zur Interneteinwahl

Die Einwahl ins Internet erfolgt im Cisco IOS über ein virtuelles Interface, den sog. Dialer. Im Folgenden wird beschrieben wie ein solches Dialer-Interface konfiguriert und mit den Zugangsdaten versehen wird. Dieses Dialer-Interface ist immer online (persistent), es erfolgt max. eine Zwangstrennung alle 24h durch die Telekom. Wichtig ist weiterhin die Anpassung der MTU size und der TCP segment-size. Der Parameter „bandwidth“ ist optional, hier bitte die korrekte Download-Bandbreite des Anschlusses in kbit/s eingeben.

Bei [abcxyz] bitte die Anschlusskennung gefolgt von der T-Online-Nummer eingeben, weiter hinten bei [1234567890] bitte das korrekte login Passwort eintragen.

Setup des Dialer-Interface mit den T-Online Zugangsdaten

```
!
interface Dialer1
  description ### Dialer VDSL ###
  bandwidth 50000
  ip address negotiated
  ip mtu 1492
  ip virtual-reassembly
  encapsulation ppp
  ip tcp adjust-mss 1452
  dialer pool 1
  dialer idle-timeout 0
  dialer persistent
  keepalive 20
  no cdp enable
  ppp authentication pap callin
  ppp pap sent-username [abcxyz]0001@t-online.de password [1234567890]
  ppp ipcp dns request
!
```

Sobald das Dialer-Interface erfolgreich angelegt wurde mit den richtigen Zugangsdaten, erscheinen folgende Logmeldungen auf der Konsole:

```
*Jul 21 13:43:52.971 CEST: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Jul 21 13:43:52.983 CEST: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
*Jul 21 13:43:54.195 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2,
changed state to up
```

Konfiguration des Routings

Für das Routing muss noch mind. eine statische Route (Default Route) eingetragen werden, diese konfiguriert man wie folgt:

```
!
ip route 0.0.0.0 0.0.0.0 Dialer 1
!
```

Troubleshooting der Internetverbindung

Falls der Router keine Internetverbindung herstellen kann, sollte folgende Einstellungen/Protokolle geprüft werden. Die grau markierten Bereiche zeigen die wichtigen Werte bei korrekter Funktion.

```
Router#show pppoe session all
```

```
Total PPPoE sessions 1
```

```
session id: 4805
```

```
local MAC address: 0013.c443.b7d0, remote MAC address: 0030.8813.25bd
```

```
virtual access interface: Vi2, outgoing interface: Fa0/0.7
```

```
14 packets sent, 16 received
```

```
232 bytes sent, 319 received
```

```
Router#
```

```
Router#show ip interface brief
```

```
Any interface listed with OK? value "NO" does not have a valid configuration
```

Interface	IP-Address	OK?	Method	Status
FastEthernet0/0	unassigned	YES	manual	up
FastEthernet0/0.7	unassigned	YES	unset	up
FastEthernet0/1	unassigned	YES	unset	administratively down
NVI0	unassigned	NO	unset	up
Virtual-Access1	unassigned	YES	unset	up
Virtual-Access2	unassigned	YES	unset	up
Dialer1	79.235.218.192	YES	IPCP	up

```
Router#
```

Die IP-Adresse des Dialer1 ist die vom ISP zugewiesene öffentliche IP-Adresse, welche im Internet sichtbar ist und später auch als Absenderadresse für ausgehenden Internet-Traffic genutzt wird. Die Default-Route (0.0.0.0) muss auf den Dialer1 zeigen.

Falls der Status des Interface Dialer1 ständig zwischen up/down/up/down usw. wechselt, dann stimmt höchstwahrscheinlich die Config der Zugangsdaten nicht, also des T-Online Benutzernamens und/oder des Passwortes. Genauere Auskunft gibt der Befehl „debug ppp nego“, der dadurch erzeugte Output zeigt die Aushandlung der PPP-Session, im Besonderen die Authentifizierungsparameter. Sollte auf einen CONF-REQUEST ein CONF-NACK folgen, so wurden die Zugangsdaten vom Login-Server abgelehnt. In diesem Fall bitte auf dem Dialer1 die entsprechende Zeile korrigieren.

Im nächsten Abschnitt wird geprüft, ob die Einstellungen des Routings korrekt arbeiten. Falls der Befehl „show ip route“ nichts anzeigt, muss evtl. das Routing noch global aktiviert werden mit „ip routing“.

```
Router#show ip route
```

```
.....  
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
```

```
87.0.0.0/32 is subnetted, 1 subnets
```

```
C 87.186.224.46 is directly connected, Dialer1
```

```
79.0.0.0/32 is subnetted, 1 subnets
```

```
C 79.235.218.192 is directly connected, Dialer1
```

```
S* 0.0.0.0/0 is directly connected, Dialer1
```

```
Router#
```

Im nächsten Abschnitt wird geprüft ob der Router eine IP-Adresse im Internet per PING erreichen kann (hier die IP des NTP-Servers), die 5 Ausrufezeichen symbolisieren 5 erfolgreiche Antwortpakete (icmp echo-reply)

```
Router#ping 192.53.103.108
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.53.103.108, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/44/48 ms
```

```
Router#
```

Erstellen einer Access Control List (Firewallfunktion)

Konfiguration der Filterregeln für die lokale Firewall

Nachfolgend wird eine beispielhafte Firewall-Konfiguration erstellt, die hier abgebildeten Regeln stellen den minimalen Regelsatz dar um im Internet surfen zu können, Hostnamen per DNS aufzulösen und diverse Hosts im Internet anzupingen. Diese Regeln können bei Bedarf jederzeit ergänzt werden, falls zusätzliche Services/Dienste frei geschaltet werden müssen.

```
!  
ip access-list extended PUBLIC-VDSL  
 10 permit tcp any any established  
 20 permit udp any eq domain any  
 30 permit udp host 192.53.103.108 eq ntp any  
 40 permit icmp any any echo-reply  
 999 deny ip any any log  
!
```

Fall der DSL-Anschluss eine feste IP-Adresse hat, kann statt des „any“ am Ende jeder Zeile auch diese feste IP-Adresse eingetragen werden. Das Beispiel hier geht davon aus, dass es keine feste IP gibt und der DSL-Router bei jeder Einwahl bzw. alle 24 Stunden eine wechselnde IP-Adresse hat.

Die Zeile 10 erlaubt alle bereits existierenden Traffic flows für TCP. Falls auch UDP Pakete erlaubt werden müssen, so kann folgender Eintrag ergänzt werden: „permit udp any any gt 1023“ Dadurch werden auch UDP Verbindungen von innen nach außen frei geschaltet, die Portrange >1023 ist die Standardrange für NAT (siehe Kapitel NAT/PAT weiter unten).

Die Zeile 20 erlaubt dem Router sowie allen den internen Clients DNS-Anfragen an Server im Internet zu stellen. (udp/53 = dns)

Die Zeile 30 erlaubt dem Router sowie allen internen Clients auf dem NTP-Server Ihre Uhrzeit zu synchronisieren.

Die Zeile 40 erlaubt dem Router sowie allen internen Clients ins Internet zu pinggen und die Ping-Antwort-Pakete zu empfangen (Ping = icmp echo).

Die Zeile 999 sorgt dafür, dass alle anderen verbotenen Pakete protokolliert werden, dies ist besonders während der Installation und Troubleshooting-Phase hilfreich. Für Pakete welche aufgrund der Firewall-Regeln verboten sind, wird eine Log-Meldung erzeugt und auf der Konsole ausgegeben.

Aktivierung der Firewall

Zum Aktivieren der Firewallfunktion muss die soeben erstellte ACL noch auf das Dialer Interface gebunden werden, dies geschieht wie folgt:

```
!  
interface dialer1  
 ip access-group PUBLIC-VDSL in  
!
```

Ab diesem Zeitpunkt ist die ACL aktiviert und filtert eingehenden Traffic aus dem Internet.

Troubleshooting der Firewall

Zur Prüfung ob die Firewall funktioniert und welche Regel IP-Pakete durchlässt bzw. verbietet, kann folgendes Kommando verwendet werden:

```
Router#show ip access-lists  
Extended IP access list PUBLIC-VDSL  
 10 permit tcp any any established  
 20 permit udp any eq domain any  
 30 permit udp host 192.53.103.108 eq ntp any (48 matches)  
 40 permit icmp any any echo-reply (15 matches)  
 999 deny ip any any log (78 matches)  
Router#
```

Die Klammer am Ende jeder Zeile zeigt an, ob der jeweilige Eintrag in der ACL auch Treffer hat, also ob aus dem Internet Pakete kommen, welche auf diesen Eintrag passen. Sollten Einträge erscheinen welche über längere Zeit keine „matches“ zeigen, so stimmt diese Zeile wahrscheinlich nicht und sollte daher korrigiert werden.

Falls der Router via Telnet oder SSH administriert wird und keinerlei Logmeldungen angezeigt werden, muss in der jeweiligen Sitzung noch der Befehl „terminal monitor“ eingegeben werden. Die Ausgabe von Logmeldungen auf der seriellen Konsole ist standardmäßig aktiviert und benötigt keine zusätzliche Konfiguration.

Konfiguration internes LAN Interface

In diesem Beispiel ist das interne LAN Interface Fa0/1, falls ein Router mit eingebautem Switch verwendet wird (z.B. 876 oder 1812) heißt das Interface Vlan1. Die Konfiguration ist dennoch immer gleich, nur der Interfacename muss angepasst werden.

```
!  
interface FastEthernet0/1  
  description ### inside LAN ###  
  ip address 192.168.1.1 255.255.255.0  
  duplex auto  
  speed auto  
  no shutdown  
!
```

Sobald man das Interface mit „no shutdown“ aktiviert hat, erscheinen folgende Logmeldungen:

```
Jul 21 13:58:32.476 CEST: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed  
state to up
```

```
Jul 21 13:58:33.476 CEST: %LINEPROTO-5-UPDOWN: Line protocol on Interface  
FastEthernet0/1, changed state to up
```

Zur Verifizierung ob der physikalische Link zum internen LAN-Switch funktioniert (nur 1841 bzw. 2811), kann der Interface-Status wie folgt abgefragt werden. Hat der Router ein Interface Vlan1 (z.B. 876 oder 1812) so wird dieses erst den Status UP zeigen sobald der erste Client am Switchport angeschlossen ist. Die grauen Markierungen zeigen den Soll-Zustand, der Status „up/up“ beweist die korrekte Funktion. Sollte der Status auf „up/down“ stehen, muss die physikalische Verbindung (das Patchkabel) zwischen Router und Switch bzw. zwischen Router und Endgerät geprüft werden.

```
Router#show ip interface brief
```

```
Any interface listed with OK? value "NO" does not have a valid configuration
```

Interface	IP-Address	OK?	Method	Status	
Protocol					
FastEthernet0/0	unassigned	YES	manual	up	up
FastEthernet0/0.7	unassigned	YES	unset	up	up
FastEthernet0/1	192.168.1.1	YES	manual	up	up
NV10	unassigned	NO	unset	up	up
...					

```
Router#
```

Anlegen eines DHCP-Pools

Anlegen eines einfachen DHCP-Pools im IOS

Der DSL-Router soll allen internen Clients wie PC, Notebook, Drucker usw. per DHCP eine IP-Adresse zuteilen. Falls bereits ein DHCP-Server existiert im internen LAN, kann dieser Abschnitt übersprungen werden. Im Folgenden wird zum Test ein Pool mit 253 Adressen angelegt. Das Netz 192.168.1.0 mit der Subnetzmaske von 255.255.255.0 sind 254 Adressen insgesamt - minus 1 Adresse des Routers (wird nicht an Clients vergeben). Bei Bedarf kann hier optional eine statische Reservierung anhand der MAC-Adresse(n) der Endgeräte erfolgen.

```

!
ip dhcp pool LAN
  network 192.168.1.0 255.255.255.0
  default-router 192.168.1.1
  dns-server 192.168.1.1
  lease 7
!

```

Der *default-router* sowie der *dns-server* ist die IP-Adresse vom internen LAN-interface des DSL-Routers. Falls das interne LAN in einem anderen Adressbereich liegt, wie z.B. 172.16.1.0, dann muss der DHCP Pool entsprechend angepasst werden.

Troubleshooting des IOS DHCP-Servers:

Die bereits an interne Clients vergebenen IP-Adressen des IOS-DHCP-Servers lassen sich wie folgt abfragen:

```

Router#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/          Lease expiration    Type
                   Hardware address/
                   User name
192.168.1.2         0100.15f2.ee2b.59  Jul 28 2009 02:16 PM Automatic
Router#

```

In meinem Fall hat der interne PC die IP-Adresse 192.168.1.2 bekommen, die IP sowie die MAC-Adresse sind farblich markiert. Wenn über längere Zeit keine Adressen vergeben werden, kann ggf. mittels „debug ip dhcp server events“ und „debug ip dhcp server packet“ auch die Aktivität des IOS-DHCP-Servers protokolliert werden, z.B. um zu prüfen ob die DHCP-Anfragen überhaupt am Router ankommen.

Aktivierung von NAT/PAT

Konfiguration des NAT+PAT für ausgehenden Internet-Verkehr (inside-to-outside)

Um den Clients im internen LAN den Internetzugriff zu ermöglichen, müssen die privaten IP-Adressen mittels Network Address Translation (NAT) übersetzt werden, private Adressbereiche werden im Internet nicht geroutet und spätestens am nächsten Telekom-Router verworfen.

Dazu muss NAT mit PAT aktiviert werden, was zur Folge hat, das der Router in allen Paketen die ins Internet geschickt werden die private Absenderadresse (z.B. 192.168.1.10) ersetzt durch die öffentliche IP-Adresse des externen VDSL-Interface. Die privaten LAN Adressen sind im Internet nicht sichtbar. Die Zuordnung der vielen internen Adressen zur einzigen öffentlichen Adresse macht der Router über verschiedene UDP/TCP Ports, also Port Address Translation (PAT).

Folgende Kommandos sind notwendig um NAT+PAT zu konfigurieren:

```

!
access-list 123 permit ip 192.168.1.0 0.255.255.255 any
!
route-map check->NAT permit 10
  match ip address 123
!
ip nat inside source route-map check->NAT interface Dialer1 overload
!
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 3600
!

```

Aktivierung des NAT+PAT

Solange es keine Interface gibt welche als „nat inside“ und „nat outside“ markiert wurden, bleibt die weiter oben beschriebene Config wirkungslos, folgende Kommandos werden zur Aktivierung benötigt.

```

!
interface Dialer 1

```

```
ip nat outside
interface FastEthernet0/1
ip nat inside
!
```

Troubleshooting des NAT/PAT

```
Router#ping 192.53.103.108 source FastEthernet 0/1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.53.103.108, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/44 ms
```

```
Router#show ip nat translations
```

```
Pro Inside global      Inside local      Outside local      Outside global
icmp 79.235.218.192:8  192.168.1.1:8    192.53.103.108:8  192.53.103.108:8
Router#
```

```
Router#show ip nat statistics
```

```
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  Virtual-Access2, Dialer1
Inside interfaces:
  FastEthernet0/1
Hits: 10 Misses: 0
CEF Translated packets: 5, CEF Punted packets: 0
...
Router#
```

Einschalten des lokalen DNS-Servers

Der lokale DNS-Server auf dem Cisco Router dient zur Namensauflösung der intern angeschlossenen Clients, alle DNS-Anfragen werden an den Telekom DNS-Server im Internet weitergeleitet (forwarding).

```
!
ip dns view default
  dns forwarding
  dns forwarding source-interface FastEthernet0/1
ip dns server
!
```

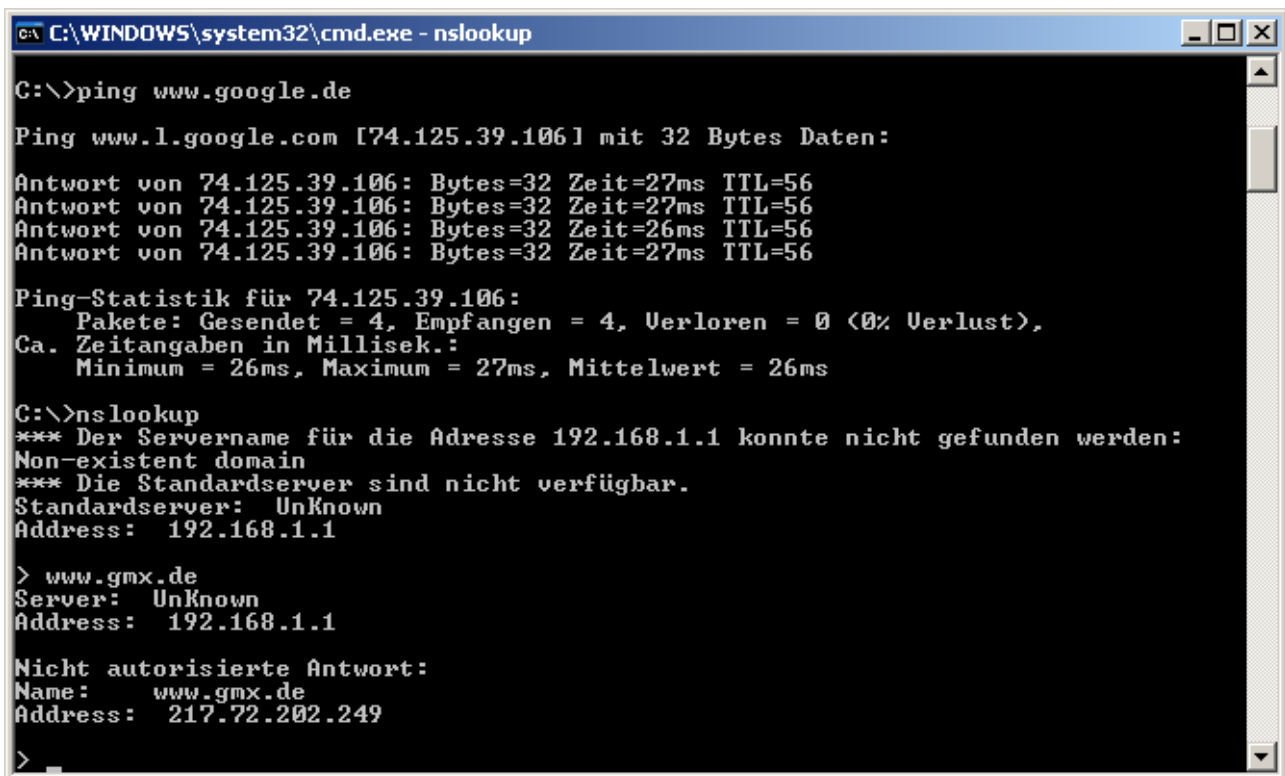
Zur Verifizierung des lokalen DNS-Dienstes dient folgender Befehl, die 2 IP-Adressen der DNS-Server hat der Router dynamisch gelernt während der PPP Sessionaushandlung (ppp ipcp dns request).

```
Router#show ip dns view
```

```
DNS View default parameters:
Logging is off
DNS Resolver settings:
  Domain lookup is disabled
  Default domain name: vdsl-domain.local
  Domain search list:
  Lookup timeout: 3 seconds
  Lookup retries: 2
  Domain name-servers:
    217.0.43.161
    217.0.43.177
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
  Forwarder source interface: FastEthernet0/1
```

```
Router#
```

Wenn die 2 DNS-Server der Telekom wie oben beschrieben zur Verfügung stehen, kann auf dem Client geprüft werden ob das Forwarding der DNS-Anfragen richtig arbeitet. Der folgende Screenshot zeigt die Vorgehensweise und das Ergebnis wenn alles korrekt funktioniert:



```
C:\WINDOWS\system32\cmd.exe - nslookup
C:\>ping www.google.de
Ping www.1.google.com [74.125.39.106] mit 32 Bytes Daten:
Antwort von 74.125.39.106: Bytes=32 Zeit=27ms TTL=56
Antwort von 74.125.39.106: Bytes=32 Zeit=27ms TTL=56
Antwort von 74.125.39.106: Bytes=32 Zeit=26ms TTL=56
Antwort von 74.125.39.106: Bytes=32 Zeit=27ms TTL=56
Ping-Statistik für 74.125.39.106:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 26ms, Maximum = 27ms, Mittelwert = 26ms
C:\>nslookup
*** Der Servername für die Adresse 192.168.1.1 konnte nicht gefunden werden:
Non-existent domain
*** Die Standardserver sind nicht verfügbar.
Standardserver: UnKnown
Address: 192.168.1.1
> www.gmx.de
Server: UnKnown
Address: 192.168.1.1
Nicht autorisierte Antwort:
Name: www.gmx.de
Address: 217.72.202.249
>
```

Das Ping-Kommando am PC kann den Hostnamen erfolgreich auflösen, weiter unten wird mit dem Befehl nslookup eine direkte Anfrage an den DNS-Server (unser Router) gestellt und von diesem beantwortet.

Impressum und rechtliche Hinweise

Der Autor stellt dieses Dokument der Öffentlichkeit unentgeltlich zur Verfügung. Die Nutzung und Verwendung geschieht auf eigene Gefahr, für Schäden die aus der Nutzung der hier beschriebenen Informationen resultieren wird keine Haftung übernommen.

Abdruck bzw. Vervielfältigung im Ganzen oder in Teilen ist mit einer Quellenangabe gestattet.

Konzept / Konfiguration / Test:

Daniel Demmler
Demmler IT-Consulting GmbH
Haarer Weg 3 B
85630 Grasbrunn
Deutschland

Email:

d.demmler@ditc.eu