

Kurzfassung

Migration von IPv4 nach IPv6 und deren Auswirkungen auf Microsoft Windows Systeme in einem Unternehmen

Bei einer Umstellung der IT Infrastruktur von IPv4 auf die Version IPv6 müssen im Vorhinein viele Faktoren beachtet werden um ungeplante und unberücksichtigte negative Folgen zu minimieren.

Um alle Probleme und Auswirkungen solch einer Umstellung aufzuzeigen wurde eine KMU IPv4 IT Infrastruktur mit Hilfe von verschiedenen Virtualisierungstechnologien geschaffen und auf IPv6 umgestellt.

Diese Bachelorarbeit befasst sich mit den Auswirkungen auf die eingesetzten Microsoft Systeme. Anhand eines Microsoft Servers 2008 R2 wird gezeigt, welche Änderungen durchgeführt werden müssen, sodass alle Dienste sowohl IPv4 als auch IPv6 fähig sind. Zusätzlich sind ein Windows 7 Client und ein Windows XP Client IPv6 fähig gemacht worden. Es sind alle Schritte mit Screenshots und Erklärungen dokumentiert worden, um einem Dritten die ersten Schritte bei solch einer Migration zu erleichtern.

Die Auswirkungen auf unixoide Systeme werden in der Bachelorarbeit von Herrn Robert Huber mit dem Titel „Migration von IPv4 nach IPv6 und deren Auswirkungen auf unixoide Systeme in einem Unternehmen“ beschrieben.

Inhaltsverzeichnis

1	Einleitung.....	5
1.1	Problemstellung / Aufgabenstellung.....	5
1.2	Zielsetzung	5
2	Grundlagen zu dem Internet Protocol 6.....	6
2.1	Die IPv6 Adresse.....	6
2.2	Arten von IPv6 Adressen	7
2.2.1	Global-Unicast-Adressen	7
2.2.2	Unique-Local-Adressen	7
2.2.3	Link-Local-Unicast-Adressen	8
2.2.4	Multicast- Adressen	8
2.2.5	Loopback-Adresse	8
2.3	Subnetting	8
2.4	Adresskonfiguration	9
2.4.1	EUI-64 Format.....	9
2.4.2	Statische Konfiguration	9
2.4.3	Automatische Konfiguration	10
3	Migrationsstrategien	11
3.1	Übergangsmechanismen	11
3.2	Dual-Stack.....	12
3.3	Tunneling.....	13
3.4	Übersetzung	13
4	KMU IT Infrastruktur.....	14
4.1	Ausgangskonfiguration des lokalen Teils	14
4.2	Windows Server 2008 R2 Routingkonfiguration.....	15
4.2.1	IPv4 Konfiguration	15
4.2.2	Testen der IPv4 Konfiguration mittels Win7 Client.....	20
4.2.3	Öffentliche IPv6 Adressen wählen	22
4.2.4	Konfiguration von „gogoClient“ mit einem /56 Netz.....	24
4.2.5	Testen der IPv6 Erreichbarkeit des Servers von Extern	26
4.2.6	Routing Advertisement mit Windows 2008 Server	28
4.2.7	Testen der IPv6 Erreichbarkeit des Servers von Intern	31
4.2.8	Testen der Erreichbarkeit des Clients von Extern.....	32
4.3	DHCPv6 Server Installation am Windows Server.....	34
4.3.1	Stateless DHCPv6 Server	34
4.3.2	Statefull DHCPv6 Server	35
4.3.3	Testen des Statefull DHCPv6 Servers	37

4.4	IPv6 DNS Server Installation am Windows Server	38
4.4.1	DHCP Server auf DNS Server konfigurieren	40
4.4.2	Statischen DNS Record anlegen.....	43
4.5	Sicherheitsfunktionen unter Windows 7 deaktivieren	44
4.5.1	Randomized Identifiers deaktivieren	44
4.5.2	Privacy Extension deaktivieren	46
4.6	IPv6 Konfiguration auf Windows XP	47
5	Ergebnisse / Diskussion	50
6	Zusammenfassung.....	51
7	Verzeichnisse	52
7.1	Literaturverzeichnis	52
7.2	Abkürzungsverzeichnis.....	53
7.3	Abbildungen	54

1 Einleitung

1.1 Problemstellung / Aufgabenstellung

Da die Nachfrage nach öffentlichen IPv4 Adressen immer größer und größer wurde, begann man im Jahr 1998 mit der Entwicklung von IPv6. Der IPv6 Adressraum ist wesentlich größer und so sollte es in nächster Zukunft keine Engpässe mehr bei der Vergabe von öffentlichen IP Adressen geben.

Jedoch bringt die neue Technologie einige Veränderungen mit sich. Bereits verwendete Hard- und Software muss IPv6 tauglich sein und ganze Systeme müssen mit dem neuen Internet Protocol in der Version 6 kommunizieren können. Mit enormen Umstellungskosten ist bei größeren Netzwerken zu rechnen. Dies beginnt mit der Planung und endet mit der Umschulung der Benutzer.

Aufgabe ist es, alle Microsoft Systeme im lokalen KMU Netzwerk IPv4 und IPv6 fähig zu machen.

1.2 Zielsetzung

Ziel dieser Bachelorarbeit ist es, wichtige Erkenntnisse bei so einer Umstellung des Internet Protocols zu gewinnen. Dies betrifft jedoch nur die verwendeten Microsoft Systeme. Es wird besonders auf die Dienste DHCP und DNS eingegangen, da es hier womöglich die meisten Probleme geben könnte. Die Umstellung von unixoiden Systemen in einem KMU Unternehmen wird in der bereits erwähnten Bachelorarbeit von Robert Huber behandelt.

Weiters werden auch mehrere Migratisstrategien vorgestellt, um IT Technikern mehrere Möglichkeiten der Migration aufzuzeigen.

Im Rahmen dieser Bachelorarbeit werden alle gewonnen Erkenntnisse zusammengefasst und abschließend analysiert. Ziel ist es, anhand dieser Bachelorarbeit, anderen IT Technikern und IT Entscheidungspersonen Erfahrungen einer solchen Umstellung näherzubringen und Sie somit bei Ihrer eigenen Umstellung von IPv4 zu IPv6 zu unterstützen.

2 Grundlagen zu dem Internet Protocol 6

2.1 Die IPv6 Adresse¹

Da die weltweite Nachfrage nach IPv4 Adressen in den letzten Jahren rasant gestiegen ist, wurde das Internet Protocol in der Version 6 entwickelt. Im neuen Internet Protocol wurde ein größerer Adressbereich geschaffen und zusätzlich wurden einige interessante Erweiterungen integriert.

Die IPv6 Adresse besteht aus 32 hexadezimalen Ziffern, die in Blöcke (Quartetts) von jeweils vier Ziffern, durch einen Doppelpunkt getrennt, aufgeteilt sind.

Führende Nullen in einem Block dürfen entfallen. Wenn ein Block nur aus Nullen besteht können somit drei Nullen weggelassen werden, nicht vier.

Aufeinanderfolgende Blöcke mit ausschließlich Nullen können durch zwei Doppelpunkte dargestellt werden. Das kann jedoch nur einmal in einer Adresse erfolgen, da sonst die Eindeutigkeit der Adresse nicht mehr gegeben ist.

IPv6 Präfixe sind den IPv4 Präfixen sehr ähnlich, sie beschreiben ebenfalls die Größe und die Adresse eines Netzes und wird durch eine IPv6 Adresse mit anschließenden Schrägstrich und einer Zahl, die die Länge des Netzwerkteils in Bits beschreibt, gebildet. Bei IPv6 gibt es jedoch keine Unterscheidung zwischen klassenlos und klassenbezogen, die Adressierung in IPv6 ist immer klassenlos.

Das Netz wird bei IPv6 genau wie bei IPv4 durch die die Netzadresse im Adressteil und lauter Nullen im Hostteil mit anschließendem Präfix dargestellt.

Eine Adresse mit Präfix: 2001:c5:5:345::3:1/64

Ein (Sub-)Netz: 2001:c5:5:345::/64

¹ RFC2460-IP Version 6 Specification, <http://www.ietf.org/rfc/rfc2460.txt>

2.2 Arten von IPv6 Adressen²

Es gibt drei Arten von IPv6 Adressen:

- Unicast: Adressieren eine Schnittstelle an einem Host
- Multicast: Adressieren eine Gruppe von Hosts. Dienen zum Ansprechen von Hosts des gleichen Typs, wie z.B. Router, DHCP Server etc.
- Anycast: Hosts können eine einheitliche Unicast-Adresse beziehen, Pakete werden zum nächstgelegenen Host mit dieser Adresse geroutet, damit lässt sich z.B. Load Balancing realisieren.

Broadcast Adressen gibt es wie bei IPv4 nicht mehr, denn diese werden durch verschiedene Multicast Adressen abgelöst. Somit wird z.B. bei der Suche nach einem DHCP Server nicht mehr ein Broadcast Paket an alle Host gesendet, sondern ein Multicast Paket nur mehr an alle DHCP Server.

2.2.1 Global-Unicast-Adressen

Global-Unicast-Adressen sind vergleichbar mit den öffentlichen Adressen von IPv4. Sie sind öffentlich weltweit erreichbar (global) und sprechen eine Schnittstelle an einem einzelnen Host an (unicast).

Alle globalen Unicast Adressen stammen aus dem Bereich 2000::/3. Die Adressen lassen sich in diesem Bereich noch weiter unterteilen, jedoch wird das nicht weiter behandelt.

2.2.2 Unique-Local-Adressen

Diese Adressen sind vergleichbar mit den privaten Adressen in IPv4. Diese Adressen können lokal verwendet werden, erlauben aber keinen Zugriffs auf das Internet und werden dort auch nicht geroutet.

Der Adressbereich für die Unique-Local-Adressen ist FD00::/8. Die Aufteilung der Adressen sieht eine Globale-ID mit 40bit vor, sowie einen 16Bit Subnetzteil und einen 64 Bit Hostteil. Die Globale-ID wird dabei vom Netzwerkadministrator frei gewählt, somit ist die Eindeutigkeit des Netzes mehr oder weniger gegeben.

² RFC4291-IPv6 Addressing Architecture, <http://tools.ietf.org/html/rfc4291>

2.2.3 Link-Local-Unicast-Adressen

Link-Local Adressen sind nur innerhalb eines Links gültig, sie werden also von Routern nicht weitergeleitet. Jeder Host erzeugt sich eine Link-Local Adresse, um mit den Geräten in seinem Netz zu kommunizieren und anschließend mithilfe dieser Adresse, das Präfix des Netzes zu erfahren und eine Global-Unicast-Adresse zu generieren.

Oft werden die Link-Local Adressen statt den Global-Unicast Adressen verwendet, z.B. für die Adresse des default-Gateways oder der Next-Hop-Adresse bei Routern.

2.2.4 Multicast- Adressen

Multicast-Adressen sprechen immer eine Gruppe von Hosts an. Dabei gibt es verschiedene Multicast Adressbereiche, die eine unterschiedliche Reichweite haben.

Wichtige Multicast Adressen:

FF02::1	Alle Hosts eines Links
FF02::2	Alle Router eines Links
FF02::1:2	DHCP-Relay-Agenten

Multicast Adressen stammen alle aus dem Bereich FF00::/8. Darauf folgen 4 Bits für verschiedene Flags und 4 Bits für die Reichweite des Pakets.

2.2.5 Loopback-Adresse

Die Adresse ::1 ist die Loopback Adresse von IPv6.

2.3 Subnetting³

Wie auch schon bei IPv4 verwendet man bei Subnetting einen Teil der Hostadressen um in einem Netz mehrere Unternetze (Subnets) zu erzeugen. Unternehmen werden in der Regel von ihrem Internetprovider ein /48 oder ein /56 Netz zugeteilt bekommen. Dies bietet noch einigen Spielraum für Subnetting. Man sollte jedoch darauf achten, den Hostteil immer auf 64 Bit zu konfigurieren, da nur mit 64Bit die Autokonfiguration der IPv6 Client anstandslos funktioniert. Bei einem 56 Bit Netz bleiben uns also 8Bit um Subnetze zu bilden. Daraus können 256 Subnetze gebildet werden oder 16 Subnetze die wiederum jeweils 16 Subnetze enthalten können.

³ IPv6 Praxishandbuch von Jarzyna, Dirk, ab Seite 130

2.4 Adresskonfiguration⁴

Damit ein Host Ressourcen im Internet abrufen kann, benötigt er einiges an Informationen, seine IP-Adresse, einen Standardgateway und eine DNS-Server Adresse. Mit IPv4 können diese Informationen statisch eingestellt werden oder per DHCP zugeteilt werden.

Unter IPv6 gibt es mehrere Möglichkeiten, sowohl bei der statischen als auch bei der automatischen Konfiguration.

2.4.1 EUI-64 Format

Ein Verfahren, dass bei beiden Arten von Konfigurationen verwendet wird, ist die Erzeugung der Interface-ID (Hostteils der Adresse) durch das EUI-64 Verfahren. Dabei wird anhand MAC Adresse der Hostteil abgeleitet. Da die MAC Adresse eindeutig sein sollte, bekommt jeder Host eine eindeutige Adresse.

Das Verfahren generiert aus den 48bit der MAC Adresse den 64bit langen Hostteil der IP-Adresse. Dabei wird die MAC Adresse in der Hälfte geteilt und FFFE eingefügt. Zusätzlich wird noch das 7. Bit im ersten Byte auf 1 gesetzt.

Beispiel:

00-21-85-11-6E-57

0221:85FF:FE11:6E57

2.4.2 Statische Konfiguration

Bei der statischen Konfiguration wird dem Host die IPv6 Adresse mit dem Präfix, ein Standardgateway sowie ein oder mehrere DNS-Server eingestellt.

Bei der Konfiguration der IP-Adresse kann entweder die gesamte Adresse angegeben werden oder nur der 64bit Präfix. Soll nur der Präfix angegeben werden, muss dem Host mitgeteilt werden, wie er den Hostteil (Interface-ID) erzeugen soll. Dies kann automatisch mit der EUI-64-Interface-ID geschehen.

⁴ IPv6 Praxishandbuch von Jarzyna, Dirk, ab Seite 145

2.4.3 Automatische Konfiguration

Man unterscheidet zwischen der stateful und der stateless Adresskonfiguration.

Die stateful Adresskonfiguration funktioniert mit einem DHCPv6 Server, ähnlich wie bei IPv4. Dabei fragt der Host über einen Multicast den DHCPv6 Server nach einer Adresse und einem DNS Server. Der Name stateful kommt davon, dass sich der DHCPv6 Server die Adressen der Client und weitere Daten merkt. Der Server hat intern einen Status gespeichert.

Der DHCPv6 Server kann jedoch auch in einem stateless Modus betrieben werden. Dabei werden vom DHCPv6 Server keine Informationen gespeichert, sondern er dient nur als Informationsquelle für den Client, z.B. um Adressen von DNS-Server zu erfahren.

Die zweite Möglichkeit ist die stateless Autokonfiguration. Dazu ist im Netzwerk kein DHCPv6 Server nötig und der Client holt sich alle benötigten Informationen im einfachsten Fall beim Router. Dazu wird das Neighbor-Discovery-Protocol (NDP) verwendet. Mit Hilfe dieses Protokolls ist es dem Host möglich, dass im Netzwerk verwendete 64bit Präfix zu erfahren und sich mit dessen und dem EUI-64-Verfahren seine IPv6 Adresse zu generieren. Außerdem wird ihm vom Router mitgeteilt, wie die Adresse des Standardgateways lautet.

Dem Host wird außerdem mitgeteilt, ob er noch weitere Adressen oder Informationen von einem im Netzwerk vorhandenen DHCPv6 Server abfragen soll. Dazu gibt es zwei Flags in der Antwort des Routers. Sie teilen dem Client mit, ob er eine Anfrage an einen stateful DHCPv6 Server senden soll und sich von ihm eine IPv6 Adresse sowie weitere Informationen geben lassen soll oder ob er bei einem stateless DHCPv6 Server nur nach weiteren Informationen, wie dem DNS-Server fragen soll.

Bei Microsoft Windows (ab Windows Vista) Systemen wird standardmäßig ein Feature verwendet, welches für die stateless Autokonfiguration ein Verfahren verwendet, das eine zufällige und temporäre Adresse für das Interface erzeugt, die jedoch nur für kurze Zeit gültig ist.

Da es wegen des EUI-64 Verfahrens Sicherheitsbedenken gibt (jeder Host ist weltweit eindeutig identifizierbar), wurde das "Privacy Extension for Stateless Adresse Configuration in IPv6" Verfahren eingeführt, welches die Erzeugung einer sicheren Adresse ermöglicht.

3 Migationsstrategien⁵

In den meisten Unternehmen wird ein schneller Umstieg von IPv4 auf IPv6 nicht so ohne weiteres möglich sein. In Netzwerken die über die Zeit gewachsen sind, bleiben immer wieder ältere Geräte, deren Tausch nur schwer möglich ist oder mit hohen Kosten verbunden ist.

IPv6 wurde mit den Gedanken entwickelt, einen reibungslosen Umstieg zu ermöglichen und somit wurden schon früh Techniken geschaffen, die es ermöglichen IPv4 und IPv6 parallel betreiben zu können.

Es wird nicht wegen IPv6 migriert, sondern wegen den Diensten und Anwendungen die IPv6 vor raussetzen.

Änderungen:

- zustandslose Adresszuweisung (kein DHCP Server nötig)
- kein Bedarf für NAT und PAT
- zwingende IPSec Integration

3.1 Übergangsmechanismen

Welcher Übergangsmechanismus soll verwendet werden?

- Dual-Stack - wird von allen modernen Betriebssystemen unterstützt, IPv6 Netz beeinflusst das IPv4 Netz nicht und kann langsam eingeführt werden
- Tunneling - wenn IPv6 Inseln über IPv4 Netze erreicht werden müssen
- Übersetzung - wenn Geräte die nur ein Protokoll können auf Geräte zugreifen müssen, die nur das andere Protokoll verstehen

Einige Fragen, die am Anfang beantwortet werden müssen.

Welches Netz erhalten wir vom Internet Service Provider?

Muss neue Hardware oder neue Software angeschafft werden?

Müssen Sicherheitsregeln aktualisiert oder für IPv6 übernommen werden?

Wie sollen die Adressen an die Hosts verteilt werden (statisch, RA, DHCPv6)?

Müssen die Mitarbeiter geschult werden?

Kommt es zu Ausfallzeiten im Netzwerk?

⁵ IPv6 Praxishandbuch von Jarzyna, Dirk, ab Seite 169

Die Migration eines Netzwerks in eine Dual-Stack Umgebung ist eine sehr einfache Möglichkeit. Fast alle Betriebssysteme unterstützen Dual-Stack. Es ist unwahrscheinlich, dass in einem Unternehmen neue Geräte zum Netzwerk hinzukommen, die nur IPv6 unterstützen und gleichzeitig nur mit IPv4 Geräten kommunizieren müssen.

Wenn vorhandenes Netzwerkequipment, IPv6 nicht unterstützt, ist ein update/upgrade oder eine Neuanschaffung notwendig. Es kann aber auch Hardware durch Softwarelösungen ersetzt oder ergänzt werden, um einen günstigeren Umstieg zu ermöglichen. Außerdem sollte zuerst ein Testnetzwerk aufgebaut werden oder die Migration auf nur einen Teil des Firmennetzes angewendet werden, um Erfahrungen mit IPv6 zu sammeln und Probleme im Vorhinein erkennen zu können.

Mögliche Vorgehensweise:

- Analyse des vorhandenen Netzes
 - Kompatibilität der vorhandenen Netzwerkteilnehmer
 - Aufteilung in Subnetz, Größe von Subnetzen
- Zugang über IPv6 zum Internet (ISP, Tunnelbroker, ...)
- Planung des neuen IPv6 Netzes
 - Auswahl der Übergangsmechanismen
 - Verteilung der Adressen
- Anschaffung neuer Hard- und Software
- Einrichten des Routers mit Subnetzten und Adressverteilung
- Einrichten der Firewall / eines Tunnels / einer Übersetzung
- Einrichten des DHCPv6 Server
- Einrichten des DNS Servers
- Einrichten der Client-Systeme
- Einrichten von Management- Monitoring Systemen

3.2 Dual-Stack⁶

Dual-Stack ist die einfachste Migrationslösung. Moderne Geräte sind in der Lage sowohl IPv4 als auch IPv6 über ihre Netzwerkinterfaces zu sprechen, ohne dass die übrigen Layer den Unterschied merken (mit Ausnahmen).

⁶ Dual Stack Architecture - <http://technet.microsoft.com/library/bb878108>

In Dual-Stack kann Hybrid-Stack implementiert sein, sodass IPv4 und IPv6 über einen TCP/IP Stack verarbeitet wird. Dies ist z.B. bei Windows ab Vista und Server 2008 der Fall. Ist IPv4 und IPv6 getrennt voneinander implementiert (wie bei Windows Server 2003), müssen Programme um Pakete über beide Protokolle erhalten oder senden zu können, immer zwei Sockets öffnen.

3.3 Tunneling

Um den Übergang von IPv4 zu IPv6 zu erleichtern wurden verschiedene Tunnel-Mechanismen entwickelt, welche IPv6 Pakete durch IPv4 Netze tunneln können. Dazu werden die IPv6 Pakete in IPv4 Pakete gekapselt. Man unterscheidet zwischen statischem Tunnel, die meist dazu verwendet werden zwei Standorte in einem Firmennetz zu verbinden. Die Endpunkte des Tunnels müssen nur IPv4 und IPv6 fähig sein. Auch Tunnelbroker die Zugang über ihre Server in das IPv6 Internet anbieten (wie „gogo6“ mit „freenet6“) zählen zu den statischen Tunnels.

Dynamische Tunnel, wie 6to4 ISATAP und Teredo, ermöglichen den Clients den Aufbau von dynamische Tunneln durch IPv4 Netze zu anderen IPv6 Clients. 6to4 verwendet dazu eine Methode um aus speziellen IPv6 Adressen IPv4 Adressen abzuleiten und somit gekapselte IPv6 Pakete direkt an die IPv4 Adresse zu senden, die dort weitergeleitet werden. Damit können einzelne IPv6 Standorte durch wenig Konfiguration über ein IPv4 Netz miteinander verbunden werden.

ISATAP benötigt Router, zu denen sich der Host mit seinem ISATAP Client verbinden kann. Dazu gibt es ebenfalls eigene IPv6 Adressen, die der ISATAP Client generiert. ISATAP funktioniert nicht über NAT und ist also nicht für kleine Unternehmen mit z.B. einem DSL Anschluss geeignet.

Teredo dient dazu, Dual-Stack fähige Hosts miteinander zu verbinden. Dazu verpacken die beteiligten Hosts die Pakete selbst in IPv4. Teredo wird meist als letzte Möglichkeit verwendet, wenn z.B. keine der anderen Tunnelmethoden funktioniert oder der Host keine globale Unicast-Adresse hat.

3.4 Übersetzung

Für Hosts, die nur in der Lage sind ein Protokoll zu sprechen, egal ob IPv4 oder IPv6, gibt es Mechanismen, die IPv6 Pakete auf IPv4 Pakete übersetzen und umgekehrt. Dabei übersetzt meist ein Router oder ein Gateway die IPv4 Header auf IPv6 Header, ähnlich wie bei IPv4 NAT.

4 KMU IT Infrastruktur

Anhand einer KMU IT Infrastruktur wird gezeigt, wie man ein IPv4 Netzwerk in ein IPv6 Netzwerk migriert. Diese KMU IT Infrastruktur besteht aus einem gehosteten Teil und einem lokal selbst verwalteten Teil. In dieser Bachelorarbeit wird gezeigt, wie der lokal verwaltete Teil um konfiguriert werden muss, um einen Dualbetrieb zu ermöglichen. Dualbetrieb bedeutet, dass alle Komponenten sowohl über ein IPv4 Adresse als auch eine IPv6 Adresse besitzen und somit über beide IP Protokolle kommunizieren können. Es gibt mehrere Strategien bzw. Ansätze um ein Netzwerk auf IPv6 zu migrieren. Hier ist auf Dualbetrieb entschieden worden, da die Services IPv4 und zusätzlich IPv6 kompatibel sein müssen. Die Migration des gehosteten Teils wird in der bereits erwähnten Bachelorarbeit von Herrn Robert Huber behandelt.

4.1 Ausgangskonfiguration des lokalen Teils

Die Ausgangssituation für die Umstellung unseres Netzwerkes auf einen Dual-Stack Betrieb von IPv4 und IPv6 ist ein klassisches KMU – Windows Netzwerk mit einem Windows 2008 Server, der die Aufgabe des Routers und DHCP Servers übernimmt. Zusätzlich sind im Netzwerk Windows 7 und Windows XP Clients vorhanden.

Netzwerkkomponenten:

- Windows Server 2008 R2
- Windows 7 Client
- Windows XP Client

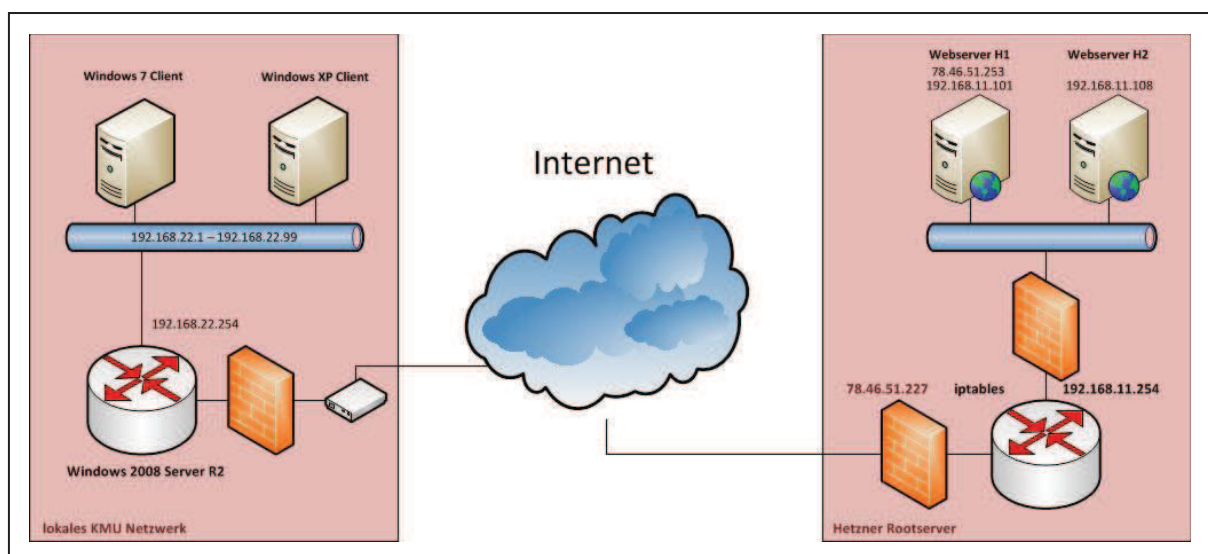


Abb. 1: Netzwerkstruktur

4.2 Windows Server 2008 R2 Routingkonfiguration

4.2.1 IPv4 Konfiguration

Es werden die Rollen für Dateidienste, DHCP, DNS, Drucker und Netzwerkrichtlinien und Zugriffsdienste hinzugefügt.

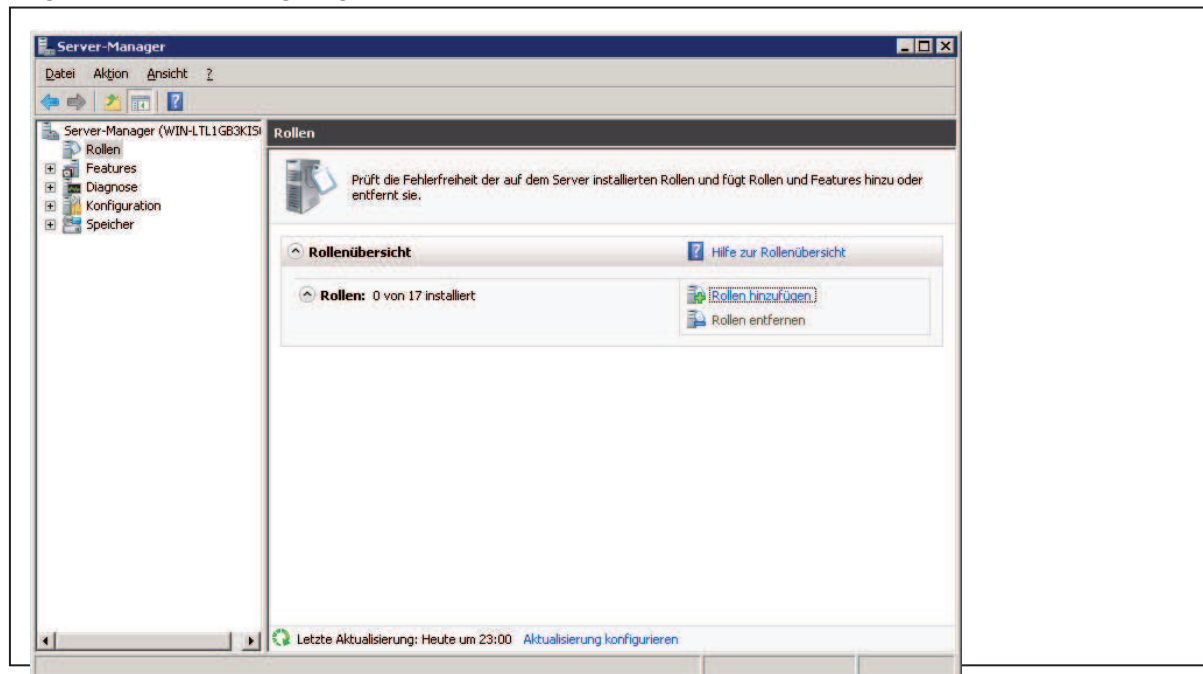
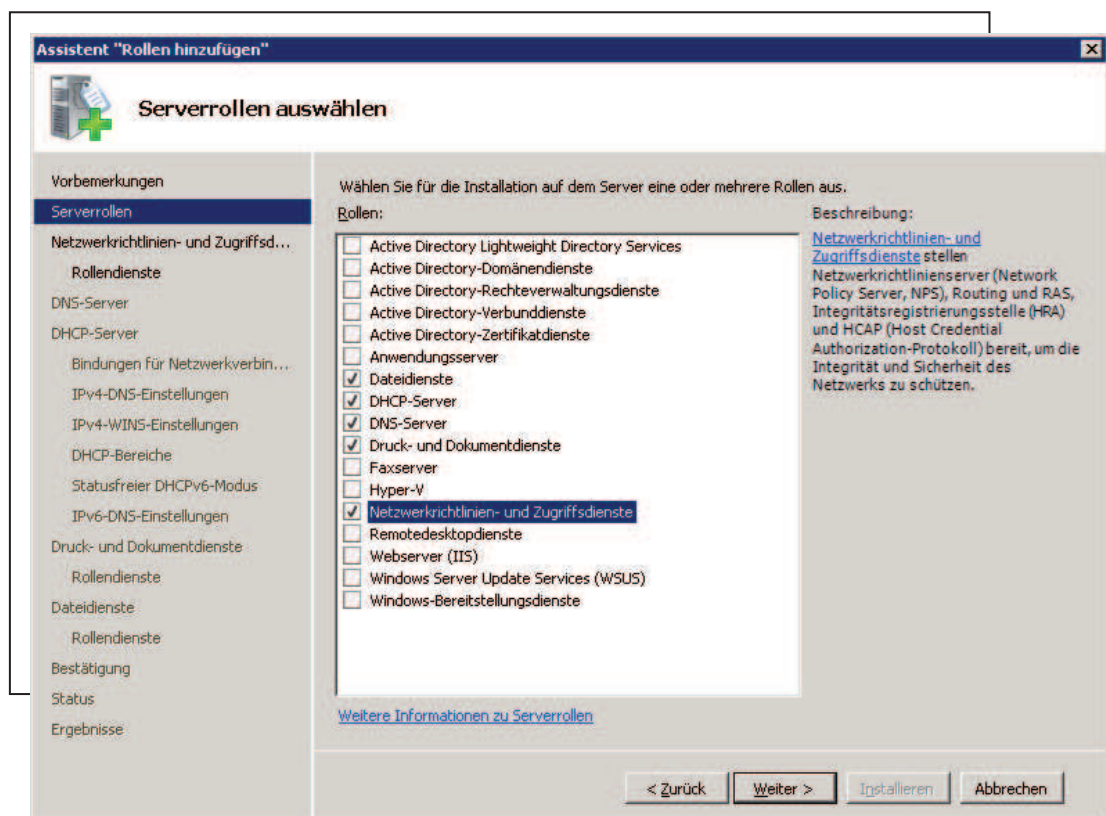
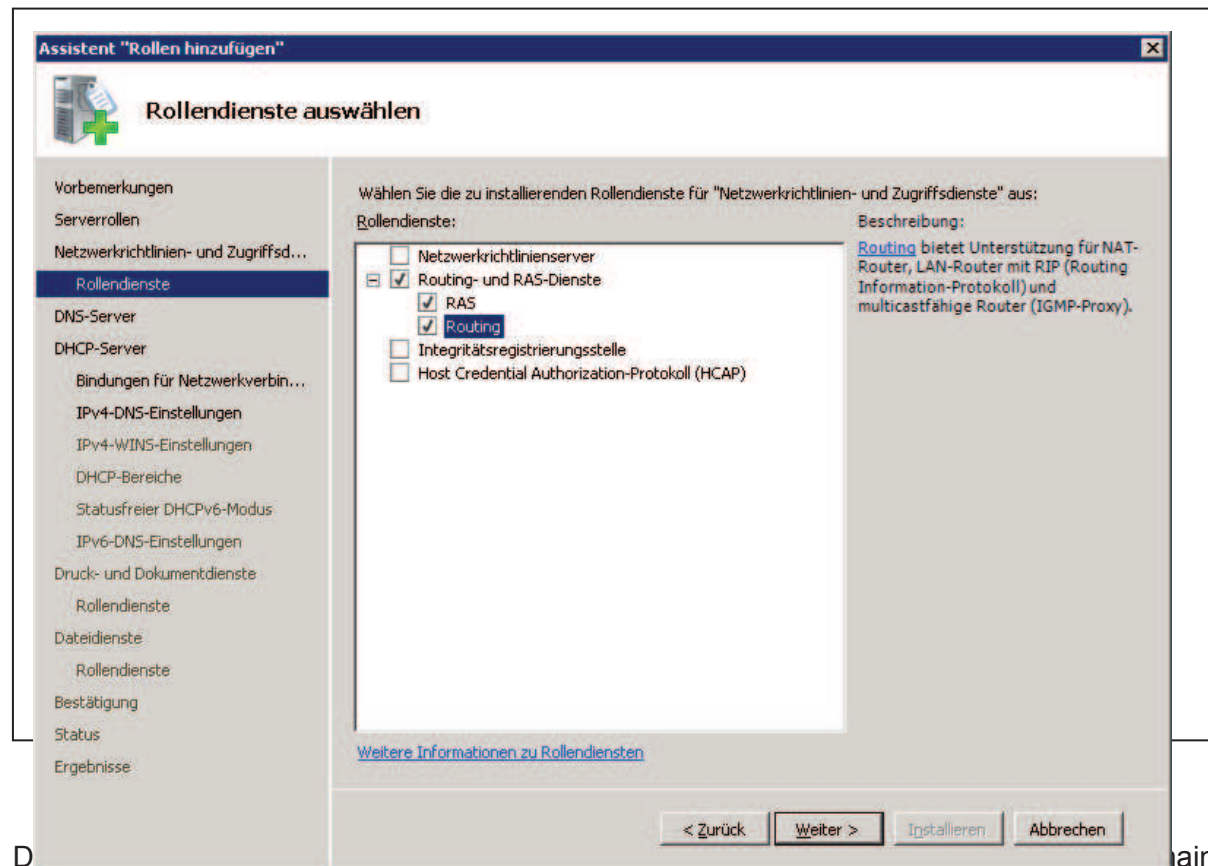


Abb. 2: Rollen am Windows Server 2008 hinzufügen

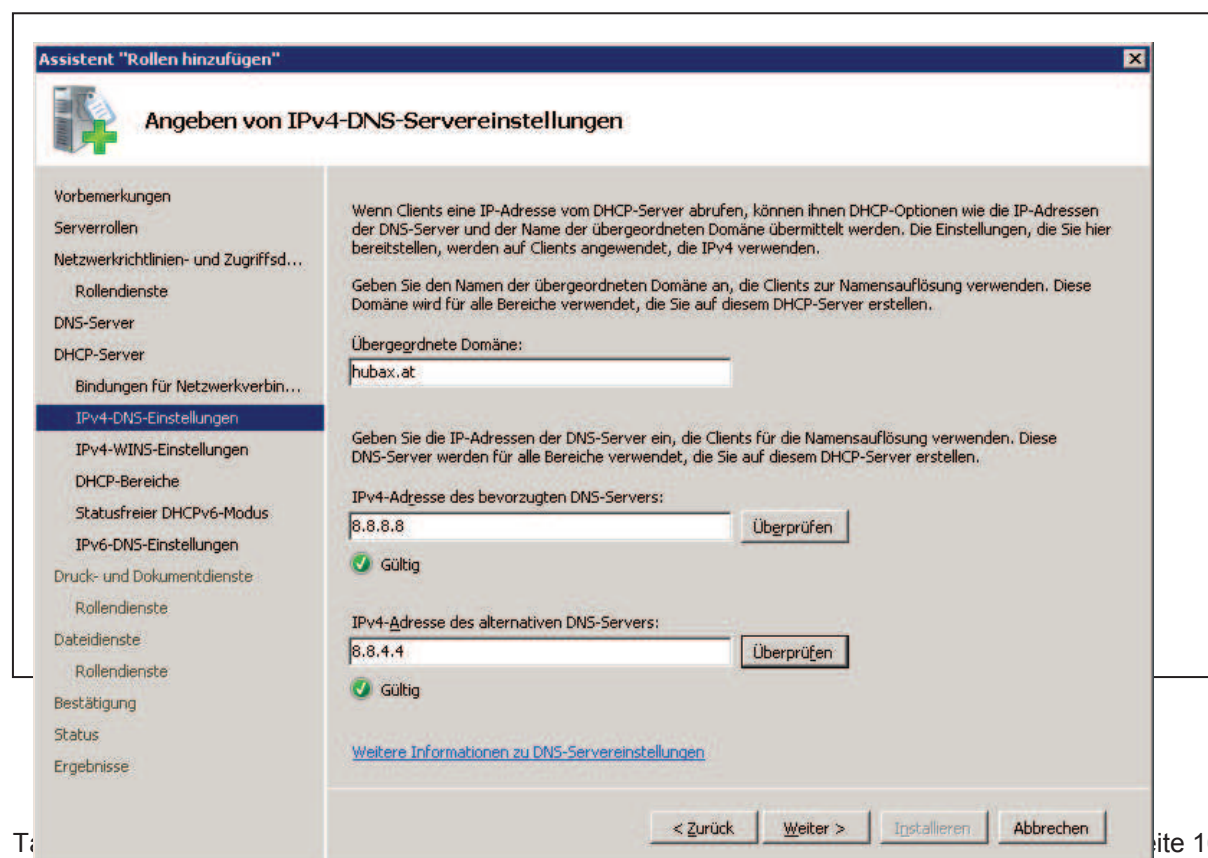
Dafür wird der „Rollen hinzufügen“ Assistent des Servers ausgeführt und dem Assistenten durch die einzelnen Schritten gefolgt.



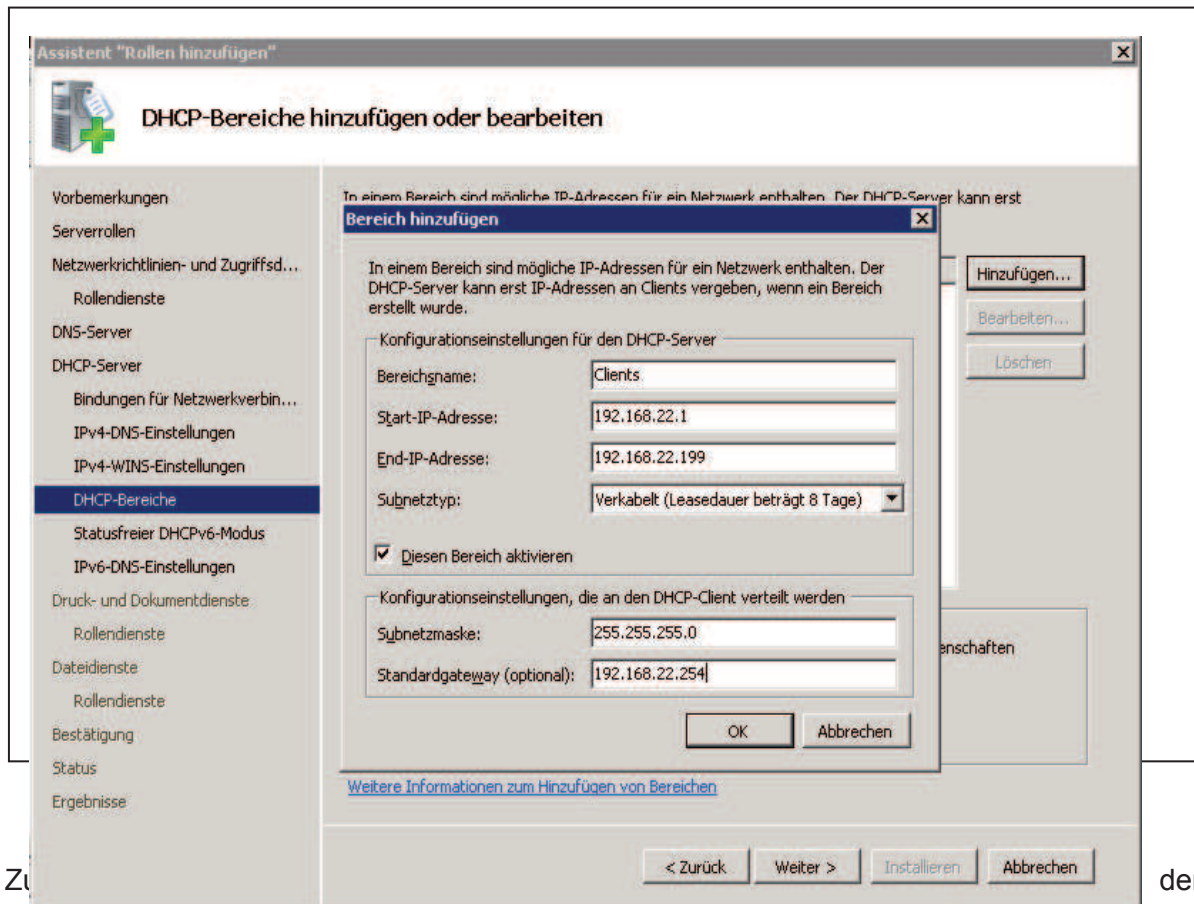
Routing und RAS Dienste bieten die Unterstützung für Routing (NAT, RIP, ...) und Remote Access Services sowie verschiedene VPN Dienste.



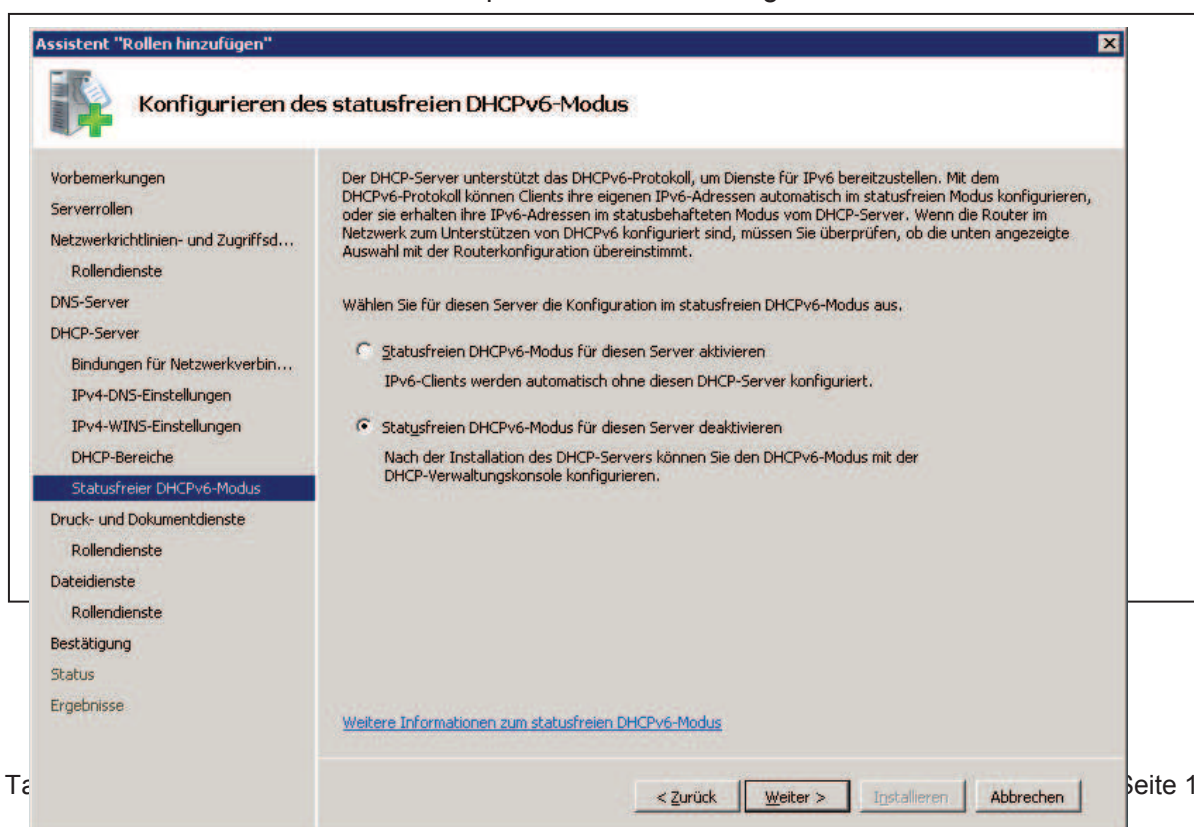
hubax.at als übergeordnete Domain verwendet. Als DNS Server werden öffentliche IPv4 DNS Server von Google verwendet.



Als DHCP Bereich für die Clients wird der Bereich von 192.168.22.1 – 192.168.22.199 vergeben. Als Standardgateway wird 192.168.22.254 vergeben. Der Server übernimmt mit dem DHCP Server die Vergabe der lokalen IPv4 Adressen.



Zu „Statusfreien DHCPv6-Modus“ auf deaktiviert setzt, verwendet man den „Statusbehafteten Modus“. Die Adressen werden somit per DHCP Server vergeben.



Um den Clients den Zugriff auf das Internet über diesen Server zu ermöglichen, wird Routing und RAS als NAT konfiguriert. Als erstes werden die Routing und RAS Services am Server aktiviert. Dies geschieht über den Servermanager unter dem Punkt „Rollen -> Netzwerkrichtlinien ... -> Routing und RAS“.



Abb. 8: Routing und RAS Konfiguration

Es öffnet sich ein Assistent, bei dem wir die Netzwerkadressübersetzung (NAT) auswählen und den Schritten des Assistenten weiter folgen.

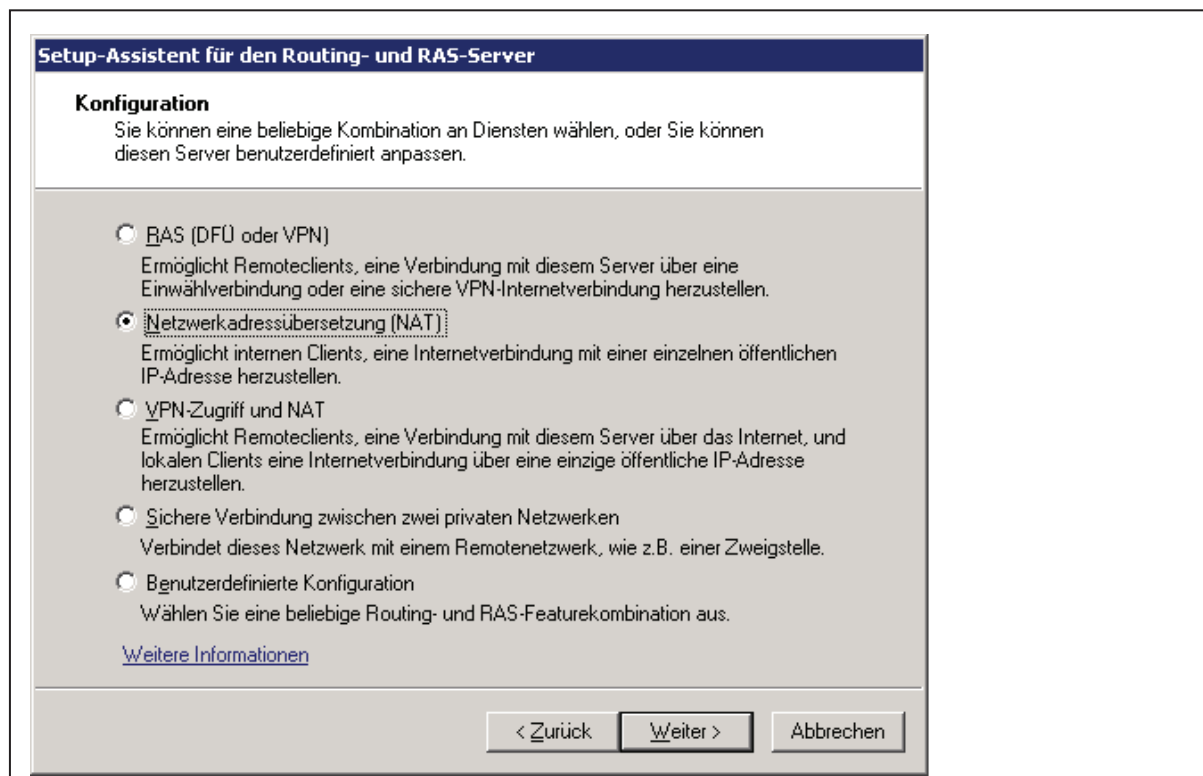


Abb. 9: NAT Konfiguration

Als öffentliche Schnittstelle wird das „WAN“ Interface verwendet, welches eine dynamische IPv4 Adresse von einem DHCP Server zugeordnet bekommt.

Setup-Assistent für den Routing- und RAS-Server

VPN-Verbindung
Mindestens eine Netzwerkschnittstelle muss über eine Internetverbindung verfügen, um VPN-Clients zu ermöglichen, auf diesen Server zuzugreifen.

Wählen Sie die Netzwerkschnittstelle aus, die eine Verbindung zwischen diesem Server und dem Internet herstellt.

Netzwerkschnittstellen:

Name	Beschreibung	IP-Adresse
LAN-Verbindung	Realtek RTL8139C+Fa...	192.168.1.4 (DHCP)
LAN-Verbindung 2	Realtek RTL8139C+Fa...	192.168.22.254

Setup-Assistent für den Routing- und RAS-Server

IP-Adresszuweisung
Sie können die Zuweisungsmethode für IP-Adressen für Remoteclients auswählen.

Wie sollen IP-Adressen den Remoteclients zugewiesen werden?

☒ **Automatisch**
Falls Sie einen DHCP-Server für die Adresszuweisung verwenden, müssen Sie bestätigen, dass dieser ordnungsgemäß konfiguriert wurde. Falls Sie keinen DHCP-Server verwenden, wird dieser Server die Adressen generieren.

☐ Aus einem angegebenen Adressbereich

Setup-Assistent für den Routing- und RAS-Server

Mehrere RAS-Server verwalten
Verbindungsanforderungen können lokal authentifiziert oder an einen RADIUS-Server zum Authentifizieren weitergeleitet werden.

Obwohl Verbindungsanforderungen mit Routing und RAS authentifiziert werden können, wird in großen Netzwerken mit mehreren RAS-Servern häufig ein RADIUS-Server für die zentrale Authentifizierung verwendet.

Falls Sie einen RADIUS-Server im Netzwerk verwenden, können Sie diesen Server zum Weiterleiten von Authentifizierungsanforderungen an den RADIUS-Server einrichten.

Soll dieser Server für die Verwendung eines RADIUS-Servers eingerichtet werden?

☒ **Nein, Routing und RAS zum Authentifizieren von Verbindungsanforderungen verwenden**

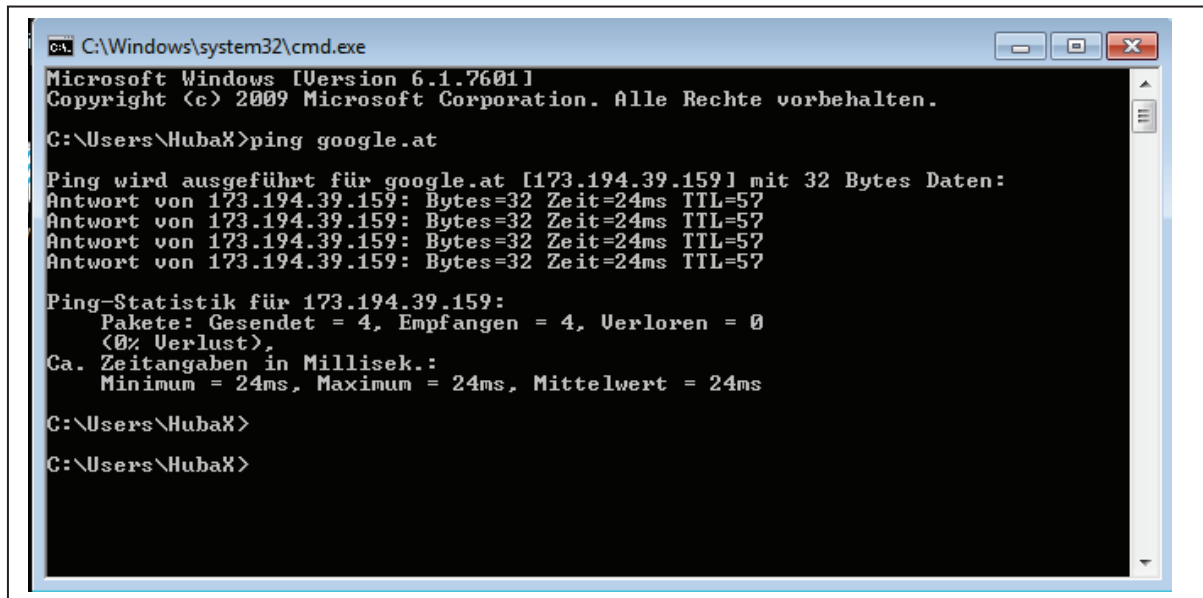
☐ Ja, diesen Server für die Verwendung eines RADIUS-Servers einrichten

[Weitere Informationen](#)

< Zurück Weiter > Abbrechen

4.2.2 Testen der IPv4 Konfiguration mittels Win7 Client

Der Windows 7 Client bekommt vom Windows 2008 Server automatisch eine IPv4 Adresse zugewiesen und kann mit dieser mit dem zuvor eingerichteten NAT über die öffentliche Adresse des Servers auf des Internet zugreifen.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

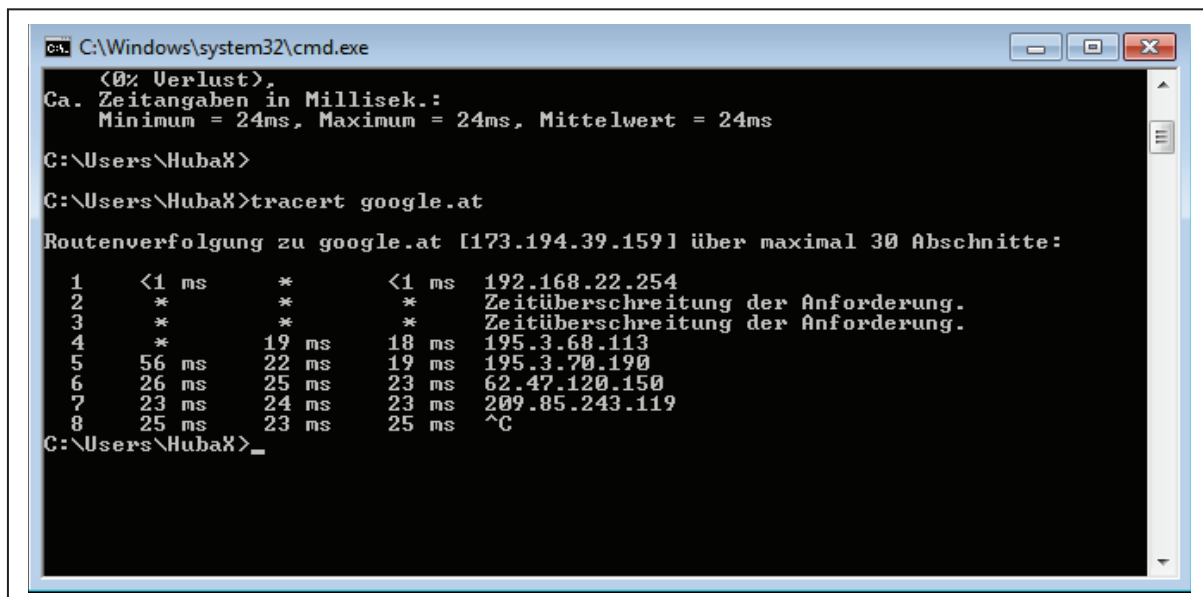
C:\Users\HubaX>ping google.at

Ping wird ausgeführt für google.at [173.194.39.159] mit 32 Bytes Daten:
Antwort von 173.194.39.159: Bytes=32 Zeit=24ms TTL=57
Antwort von 173.194.39.159: Bytes=32 Zeit=24ms TTL=57
Antwort von 173.194.39.159: Bytes=32 Zeit=24ms TTL=57
Antwort von 173.194.39.159: Bytes=32 Zeit=24ms TTL=57

Ping-Statistik für 173.194.39.159:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 24ms, Maximum = 24ms, Mittelwert = 24ms

C:\Users\HubaX>
C:\Users\HubaX>
```

Abb. 13: IPv4 Pingtest



```
C:\Windows\system32\cmd.exe
<0% Verlust>,
Ca. Zeitangaben in Millisek.:
    Minimum = 24ms, Maximum = 24ms, Mittelwert = 24ms

C:\Users\HubaX>
C:\Users\HubaX>tracert google.at

Routenverfolgung zu google.at [173.194.39.159] über maximal 30 Abschnitte:

 1  <1 ms    *      <1 ms    192.168.22.254
 2  *        *      *          Zeitüberschreitung der Anforderung.
 3  *        *      *          Zeitüberschreitung der Anforderung.
 4  *        19 ms   18 ms    195.3.68.113
 5  56 ms    22 ms   19 ms    195.3.70.190
 6  26 ms    25 ms   23 ms    62.47.120.150
 7  23 ms    24 ms   23 ms    209.85.243.119
 8  25 ms    23 ms   25 ms    ^C

C:\Users\HubaX>
```

Abb. 14: IPv4 Traceroutetest

Wie auf folgender Abbildung zu sehen ist, wird dem Client die Adresse 192.168.22.1 zugewiesen. Der Standardgateway und der DNS Server sind der Windows 2008 Server mit der Adresse 192.168.22.254 und als DNS Server werden die zwei öffentlichen Server 8.8.8.8 und 8.8.4.4 verwendet.

Es ist außerdem zu sehen, dass sich der Rechner automatisch eine IPv6 Adresse generiert hat. Adressen mit fe80:: beginnend, sind Link-Local Adressen und nur auf einem Netzwerklink erreichbar. Diese Adresse wurde von der MAC-Adresse der Netzwerkkarte automatisch abgeleitet. Ein IPv6 Standardgateway oder ein IPv6 DNS Server ist noch nicht vorhanden.

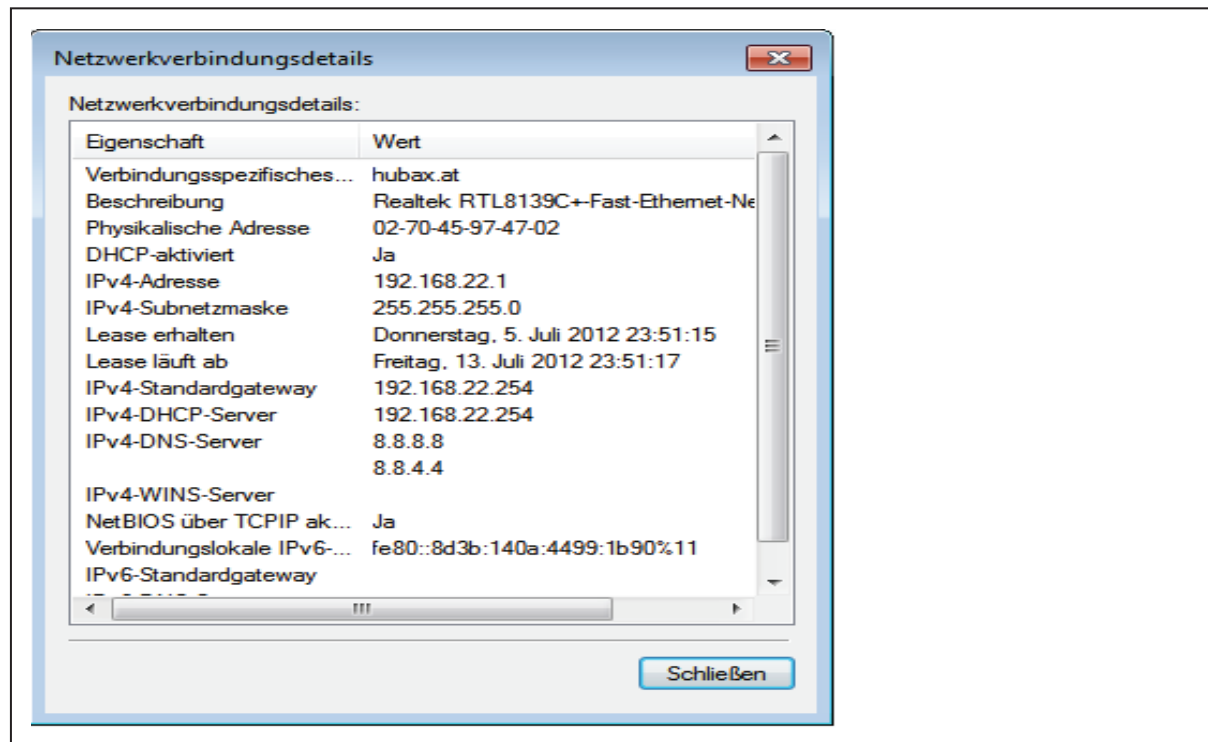


Abb. 15: Netzwerkverbindungsdetails

4.2.3 Öffentliche IPv6 Adressen wählen⁷

Wenn der Internet Provider (wie in vielen Fällen) für Privatkunden und Geschäftskunden noch keine IPv6 Verbindung ermöglicht, muss man entweder zu einem Provider wechseln, der dies ermöglicht oder die IPv6 Verbindung über einen IPv6 Tunnelbroker aufbauen.

Einer dieser Tunnelbroker ist „gogoNet“, der über seinen Dienst „freenet6“ kostenlose Zugänge zum Internet über einen IPv6-in-IPv4 Tunnel bietet. Die Registrierung ist einfach und der Client gut verständlich. Die kostenlosen Zugänge bieten zwar nicht die Performance von herkömmlichen Breitbandanschlüssen, reichen aber allemal zum Testen und Kennenlernen von IPv6. Mit einer Registrierung ist es außerdem möglich, nicht nur eine fixe IPv6 Adresse zu bekommen, sondern direkt ein ganzes /56 Netz zu bekommen. Dieses kann dann noch in Subnetze zerlegt werden.

Vorgehensweise:

- Anmelden und Registrieren auf der Website <http://www.gogo6.com>

Auf der „gogo6“ Website kann man sich mit einer gültigen E-Mail Adresse registrieren und man erhält einen eigenen Benutzernamen und ein Passwort für einen IPv6 Tunnel. Der Aufbau eines Tunnels mit dem „gogoClient“ ist auch anonym möglich, jedoch erhält man damit keine fixe IPv6 Adresse und kein IPv6 /56 Subnetz. Wenn man zusätzlich einen „freenet6“ Account erstellt, bekommt man fixe IPv6 Adressen aus einem /56 Netz zugewiesen.

Zugewiesenes IPv6 /56 Netz von „freenet6“: 2001:0:5ef4:97fb::

- Downloaden des „gogoClient“

Der Client ist ein Windowsprogramm, der bei der Installation eine virtuelle Netzwerkschnittstelle erstellt, über welche man anschließend eine öffentliche IPv6 Adresse erhält und über diese auf das Internet zugreifen kann.

- Starten des „gogoClients“

Nach dem Start des Clients muss zuerst die Server Adresse, sowie der Benutzername und das Passwort eingegeben werden. Mit einem Klick auf Connect verbindet sich der Client.

⁷ „gogo6“ Helpcenter - <http://www.gogo6.com/freenet6/help-center>

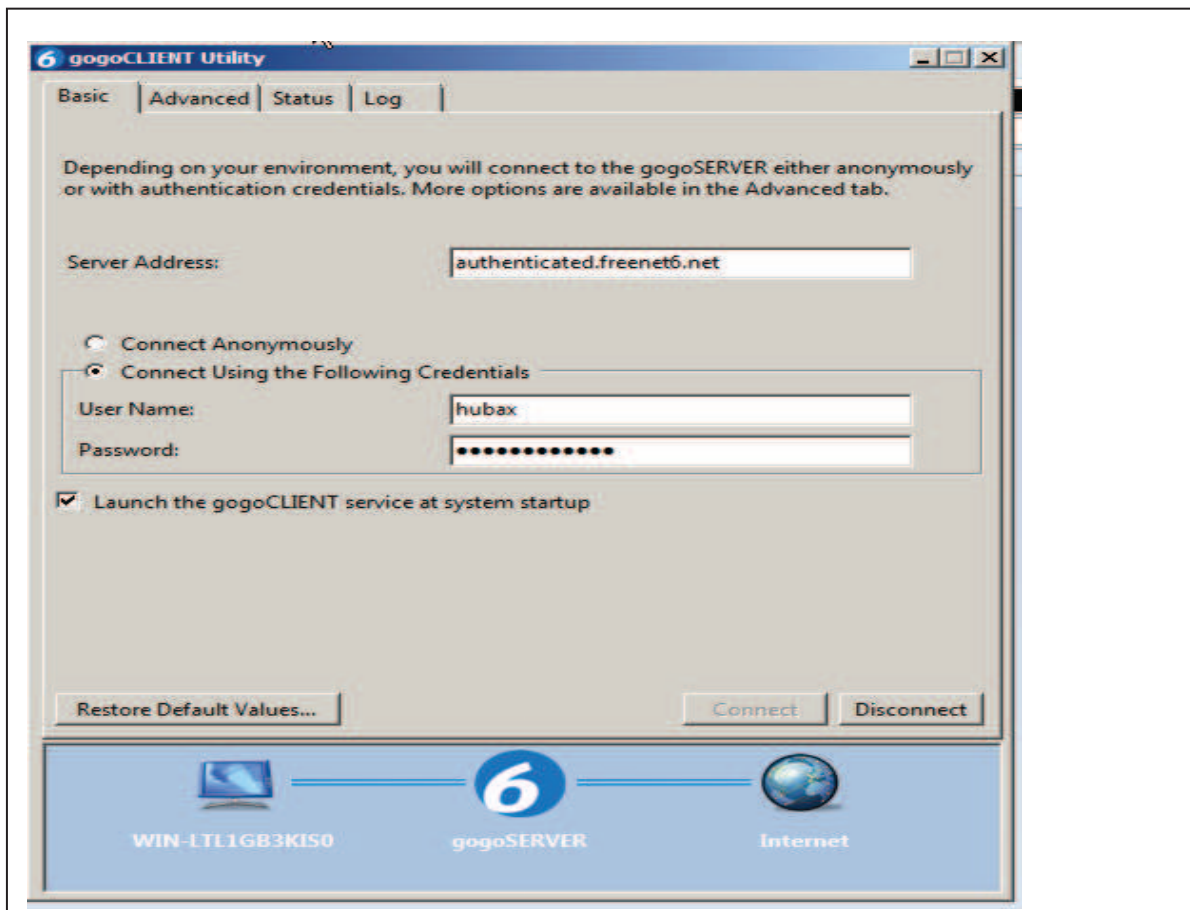


Abb. 16: gogoClient Anmeldung

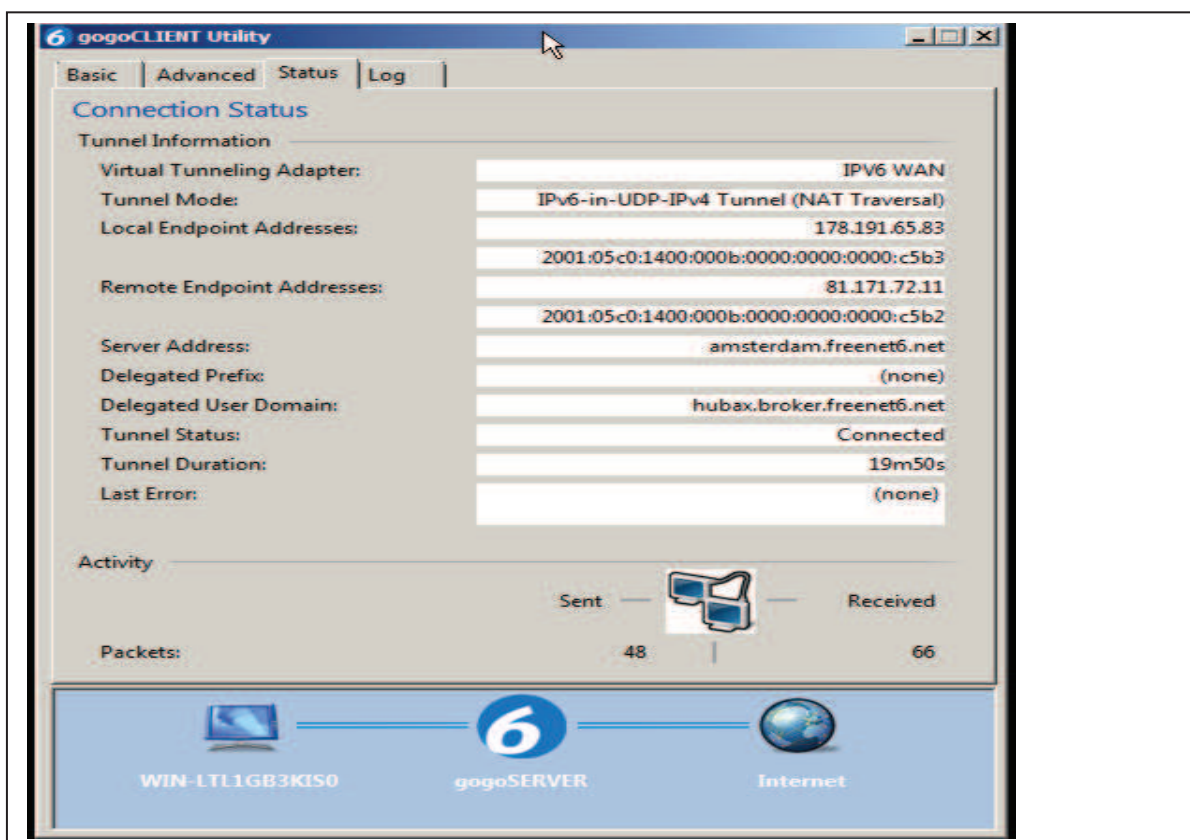


Abb. 17: gogoClient Verbindungsstatus

In der Standardkonfiguration wird dem Host eine IPv6 Adresse zugeordnet. In diesem Fall ist die Adresse 2001:5c0:1400:b::c5b2. Außerdem wird dem Host ein IPv6 DNS Server zugeordnet, um die Namensauflösung über IPv6 zu ermöglichen.

Der Server ist nun über eine IPv6 und eine IPv4 Adresse über das Internet erreichbar und umgekehrt. Das Netzwerk kann nur per NAT über die IPv4 Adresse in das Internet.

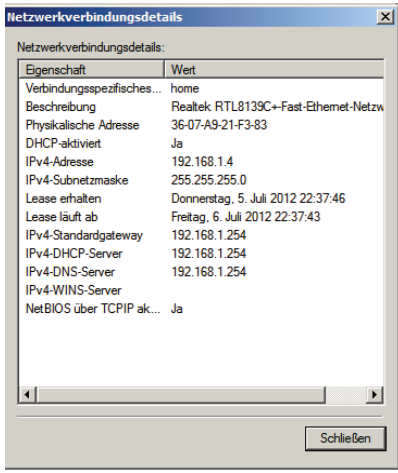
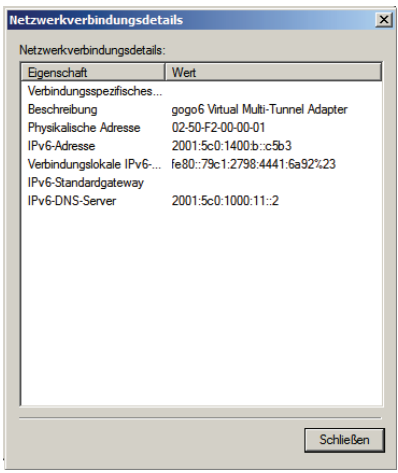
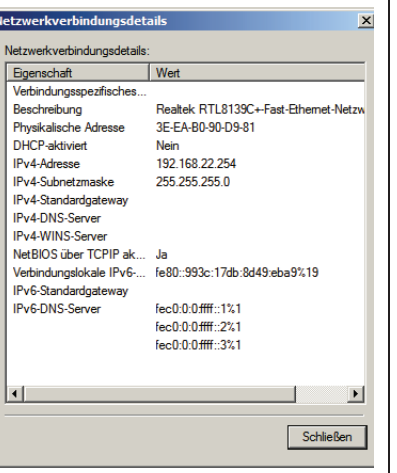
IPv4 WAN	IPv6 WAN	LAN Schnittstelle
		

Abb. 18: aktuelle Netzwerkkonfiguration am Windows Server 2008

4.2.4 Konfiguration von „gogoClient“ mit einem /56 Netz⁸

Um den LAN Clients den Internetzugriff über IPv6 zu ermöglichen, kann der „gogoClient“ so konfiguriert werden, dass der Tunnelbroker unserem Server ein IPv6 Netz zuordnet.

In den „Advanced Settings“ können die nötigen Änderungen gemacht werden. Um ein fixes IPv6 Netz zu erhalten, muss sich der Client immer mit demselben Server verbinden, in unserem Fall amsterdam.freenet6.net. Die Option „Enable Routing Advertisements“ versetzt unseren Client in den „Router“ Modus, indem er vom Server das /56 Netz zugeordnet bekommt. Gleichzeitig muss ein Interface gewählt werden, auf dem das IPv6 den einzelnen Clients bekannt gemacht wird.

⁸ RFC4861 - Neighbor Discovery for IPv6, <http://tools.ietf.org/html/rfc4861>

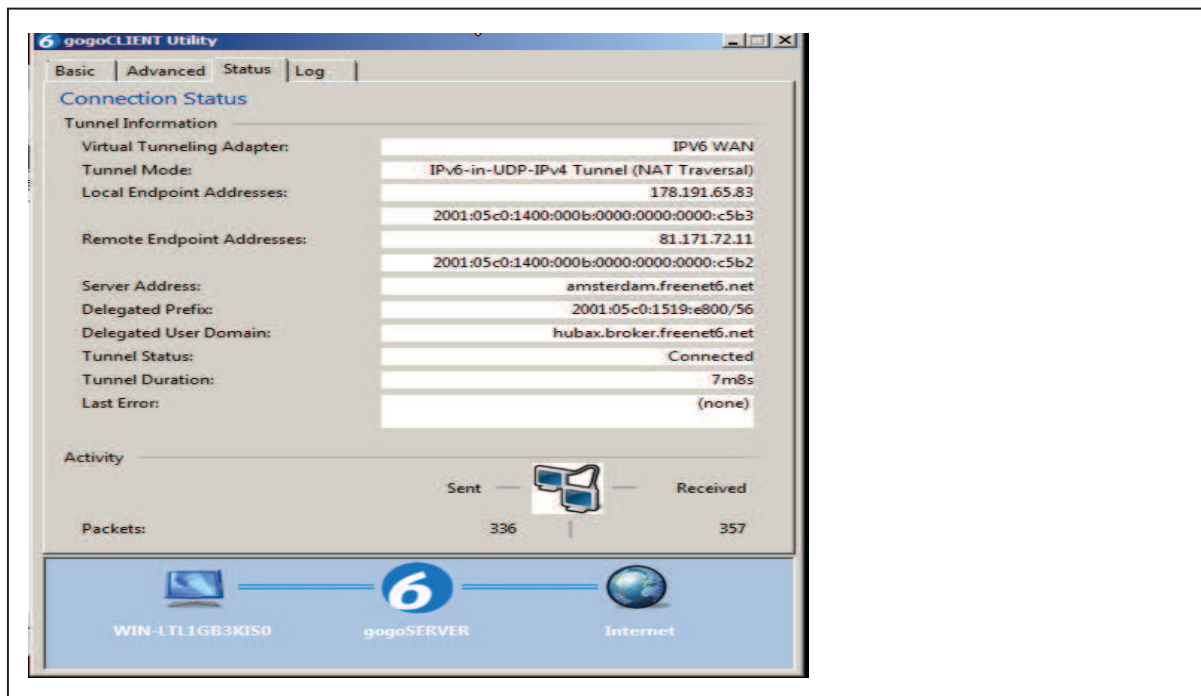


Abb. 19: „gogoClient“ Verbindungsstatus

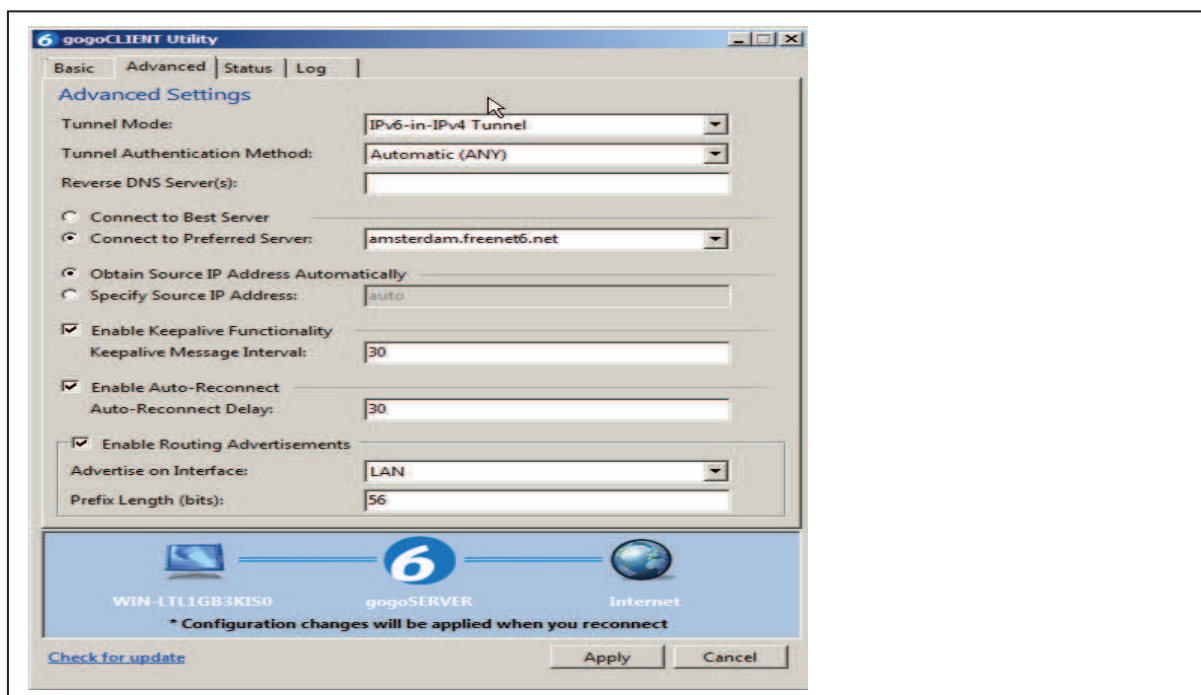


Abb. 20: „gogoClient Advanced Settings“

Der LAN Schnittstelle wird automatisch vom „gogoClient“ die erste IP Adresse im Netz zugewiesen. Die zweite Adresse wird vom Host automatisch durch die MAC-Adresse erzeugt.

4.2.5 Testen der IPv6 Erreichbarkeit des Servers von Extern

Pingversuch auf die öffentliche IPv6 Schnittstelle des Servers.

```
IPv6 Ping Output:
PING 2001:5c0:1400:b::c5b3(2001:5c0:1400:b::c5b3) 32 data bytes
40 bytes from 2001:5c0:1400:b::c5b3: icmp_seq=0 ttl=122 time=40.6 ms
40 bytes from 2001:5c0:1400:b::c5b3: icmp_seq=1 ttl=122 time=41.1 ms
40 bytes from 2001:5c0:1400:b::c5b3: icmp_seq=2 ttl=122 time=39.7 ms
40 bytes from 2001:5c0:1400:b::c5b3: icmp_seq=3 ttl=122 time=40.7 ms

--- 2001:5c0:1400:b::c5b3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3013ms
rtt min/avg/max/mdev = 39.753/40.578/41.120/0.524 ms, pipe 2

Finished!
```

Abb. 21: Pingtest auf öffentlich IPv6 Schnittstelle des Windows Servers 2008 R2

Pingversuch auf die interne IPv6 LAN Schnittstelle des Servers.

```
Pv6 Ping Output:
PING 2001:5c0:1519:e800::1(2001:5c0:1519:e800::1) 32 data bytes
40 bytes from 2001:5c0:1519:e800::1: icmp_seq=0 ttl=121 time=44.7 ms
40 bytes from 2001:5c0:1519:e800::1: icmp_seq=1 ttl=121 time=42.1 ms
40 bytes from 2001:5c0:1519:e800::1: icmp_seq=2 ttl=121 time=40.0 ms
40 bytes from 2001:5c0:1519:e800::1: icmp_seq=3 ttl=121 time=40.1 ms

--- 2001:5c0:1519:e800::1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 40.003/41.764/44.776/1.929 ms, pipe 2

Finished!
```

Abb. 22: Pingtest auf die interne IPv6 Schnittstelle des Windows Servers 2008 R2

```

Windows-IP-Konfiguration
Hostname . . . . . : WIN-LTL1GB3KISO
Prim„res DNS-Suffix . . . . . :
Knotentyp . . . . . : Hybrid
IP-Routing aktiviert . . . . . : Ja
WINS-Proxy aktiviert . . . . . : Nein
DNS-Suffixsuchliste . . . . . : home

Ethernet-Adapter LAN:
Verbindungsspezifisches DNS-Suffix:
Beschreibung. . . . . : Realtek RTL8139C+-Fast-Ethernet-Netzwerkkarte #2
Physikalische Adresse . . . . . : 3E-EA-B0-90-D9-81
DHCP aktiviert. . . . . : Nein
Autokonfiguration aktiviert . . . : Ja
IPv6-Adresse. . . . . : 2001:5c0:1519:e800::1 (Bevorzugt)
IPv6-Adresse. . . . . : 2001:5c0:1519:e800:993c:17db:8d49:eba9 (Bevorzugt)
Verbindungslokale IPv6-Adresse . : fe80::993c:17db:8d49:eba9%19 (Bevorzugt)
IPv4-Adresse . . . . . : 192.168.22.254 (Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.0
Standardgateway . . . . . :
DHCPv6-IAID . . . . . : 322890416
DHCPv6-Client-DUID. . . . . : 00-01-00-01-17-4D-99-83-36-07-A9-21-F3-83
DNS-Server . . . . . : fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
NetBIOS ☐ber TCP/IP . . . . . : Aktiviert

Ethernet-Adapter WAN:
Verbindungsspezifisches DNS-Suffix: home
Beschreibung. . . . . : Realtek RTL8139C+-Fast-Ethernet-Netzwerkkarte
Physikalische Adresse . . . . . : 36-07-A9-21-F3-83
DHCP aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . : Ja
IPv4-Adresse . . . . . : 192.168.1.9 (Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.0
Lease erhalten. . . . . : Donnerstag, 12. Juli 2012 10:38:37
Lease l„uft ab. . . . . : Dienstag, 24. Juli 2012 18:54:23
Standardgateway . . . . . : 192.168.1.254
DHCP-Server . . . . . : 192.168.1.254
DNS-Server . . . . . : 192.168.1.254
NetBIOS ☐ber TCP/IP . . . . . : Aktiviert

Ethernet-Adapter IPV6 WAN:
Verbindungsspezifisches DNS-Suffix:
Beschreibung. . . . . : gogo6 Virtual Multi-Tunnel Adapter
Physikalische Adresse . . . . . : 02-50-F2-00-00-01
DHCP aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . : Ja
IPv6-Adresse. . . . . : 2001:5c0:1400:b::c5b3 (Bevorzugt)
Verbindungslokale IPv6-Adresse . : fe80::79c1:2798:4441:6a92%23 (Bevorzugt)
Standardgateway . . . . . : ::
DHCPv6-IAID . . . . . : 386027762
DHCPv6-Client-DUID. . . . . : 00-01-00-01-17-4D-99-83-36-07-A9-21-F3-83
DNS-Server . . . . . : 2001:5c0:1000:11::2
NetBIOS ☐ber TCP/IP . . . . . : Deaktiviert

Tunneladapter LAN-Verbindung* 11:
Verbindungsspezifisches DNS-Suffix:
Beschreibung. . . . . : Microsoft-Teredo-Tunneling-Adapter
Physikalische Adresse . . . . . : 00-00-00-00-00-00-E0
DHCP aktiviert. . . . . : Nein
Autokonfiguration aktiviert . . . : Ja
IPv6-Adresse. . . . . : 2001:0:5ef5:79fb:3032:23f8:3d59:d4f1 (Bevorzugt)
Verbindungslokale IPv6-Adresse . : fe80::3032:23f8:3d59:d4f1%11 (Bevorzugt)
Standardgateway . . . . . :
NetBIOS ☐ber TCP/IP . . . . . : Deaktiviert

Tunneladapter isatap.{9C8C1A48-0A70-4496-9977-A054F32E8E1A}:
Medienstatus. . . . . : Medium getrennt
Verbindungsspezifisches DNS-Suffix:
Beschreibung. . . . . : Microsoft-ISATAP-Adapter #2
Physikalische Adresse . . . . . : 00-00-00-00-00-00-E0
DHCP aktiviert. . . . . : Nein
Autokonfiguration aktiviert . . . : Ja

Tunneladapter isatap.home:
Medienstatus. . . . . : Medium getrennt
Verbindungsspezifisches DNS-Suffix: home
Beschreibung. . . . . : Microsoft-ISATAP-Adapter #3
Physikalische Adresse . . . . . : 00-00-00-00-00-00-E0
DHCP aktiviert. . . . . : Nein
Autokonfiguration aktiviert . . . : Ja

```

Abb. 23: Windows Server 2008 R2 Netzwerkkonfiguration

4.2.6 Routing Advertisement mit Windows 2008 Server ⁹

Wenn der „gogoClient“ für die Verbindung per IPv6 zuständig ist, übernimmt dieser das Routing Advertisement. Wird eine IPv6 Verbindung über einen anderen Weg hergestellt, muss der Windows Server 2008 das Routing Advertisement übernehmen. Dies ist mit ein paar einfachen Schritten über einen Assistenten oder in der Konsole über netsh möglich.

```
Netsh interface IPv6 show interfaces  
  
Netsh interface IPv6 set interface 11 advertise=enable  
Netsh interface IPv6 route 2001:5c0:1519:e800::/64 interface=11 publish=yes  
Netsh interface IPv6 route ::/0 interface=23 publish=yes  
  
Netsh interface IPv6 set interface 11 otherstateful=Enabled
```

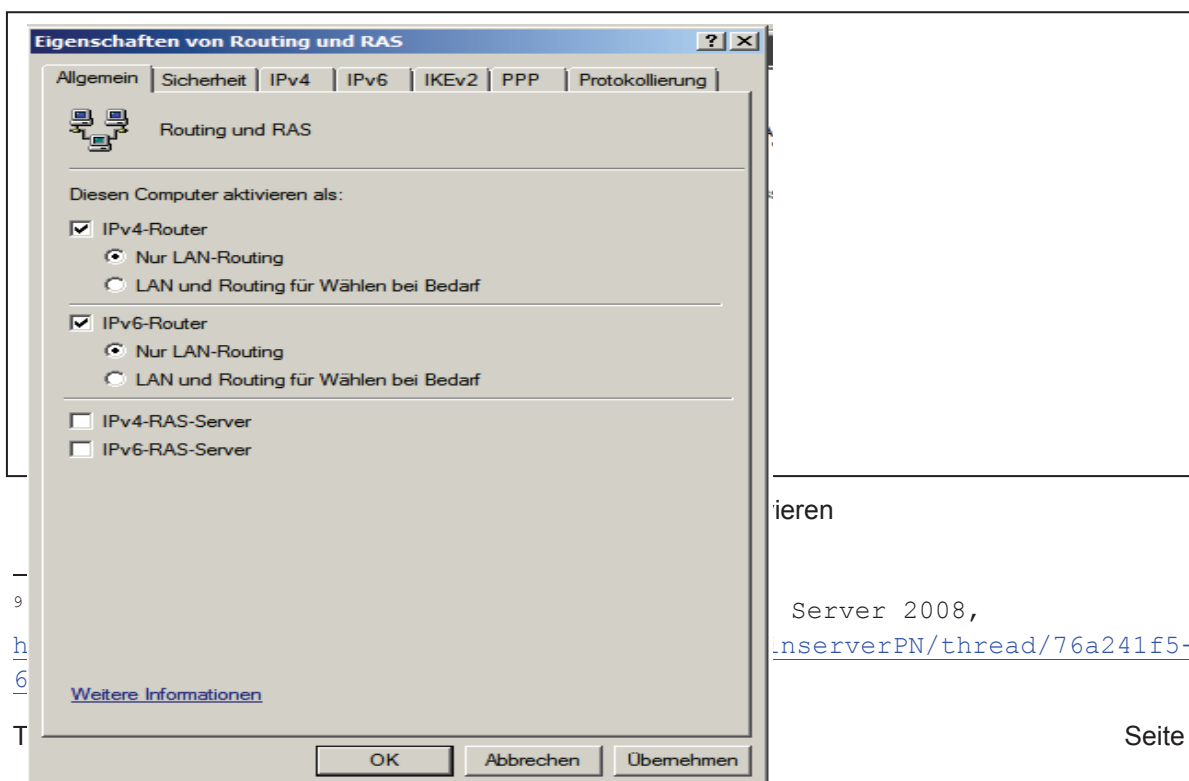
Abb. 24: netsh Konfiguration der LAN Schnittstelle

Der erste Befehl „show interfaces“ listet die Interfaces des Servers auf. Hier sieht man, dass die LAN Schnittstelle die Nummer 11 besitzt. Der zweite Befehl aktiviert das Router Advertising, mit dem der Router den Prefix an die Clients verteilt und somit wird gleichzeitig der Default Gateway bekannt gegeben. Die Adresse des Default Gateways am Client ist eine Link-Local Adresse. Diese bleibt gleich, wenn sich der globale Prefix oder die globale Adresse ändern sollte. Der dritte Befehl weist den Client daraufhin, dass es im Netzwerk noch einen statefull DHCPv6 Server gibt.

Alternative:

Alternativ kann das Routing auch ohne Konsole grafisch konfiguriert werden.

Die IPv6 Routingkonfiguration kann unter „Rollen -> Netzwerkrichtlinien- und Zugriffsdienste -> Routing und RAS -> Eigenschaften“ im Reiter „Allgemein“ aktiviert werden.



ieren

Server 2008,
[.nserverPN/thread/76a241f5-](http://serverPN/thread/76a241f5-)

Unter dem Reiter „IPv6“ kann dem Server ein IPv6 Präfix zugeordnet werden, dass in diesem Fall nicht nötig ist, da dies von dem verwendeten „gogoClient“ durchgeführt wird.

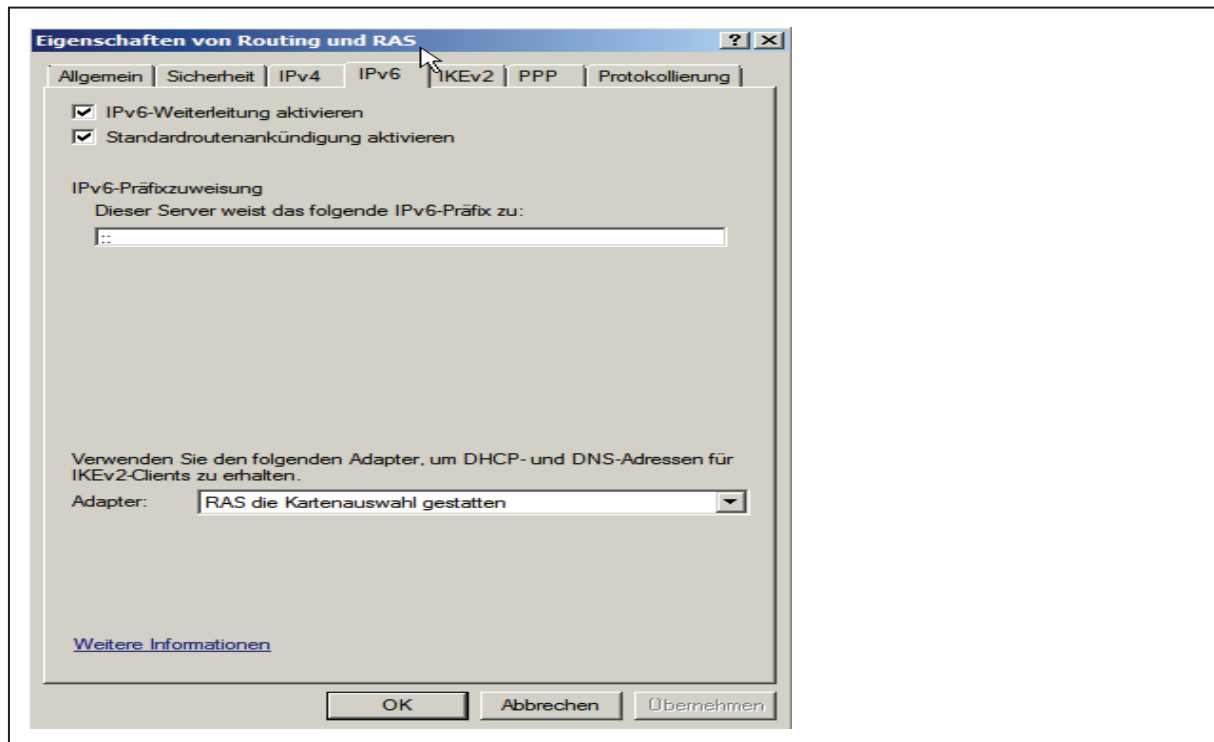


Abb. 26: IPv6 Einstellungen im IPv6 Reiter

Für dieses Netzwerk müssen keine weiteren Einstellungen vorgenommen werden. Es sind keine weiteren Router vorhanden und alle vorhandenen Netze sind direkt mit dem Windows Server verbunden.

```

=====
Schnittstellenliste
19...3e ea b0 90 d9 81 .....Realtek RTL8139C+-Fast-Ethernet-Netzwerkkarte #2
12...36 07 a9 21 f3 83 .....Realtek RTL8139C+-Fast-Ethernet-Netzwerkkarte
23...02 50 f2 00 00 01 .....gogo6 Virtual Multi-Tunnel Adapter
1.....Software Loopback Interface 1
11...00 00 00 00 00 00 e0 Microsoft-Teredo-Tunneling-Adapter
22...00 00 00 00 00 00 e0 Microsoft-ISATAP-Adapter #2
24...00 00 00 00 00 00 e0 Microsoft-ISATAP-Adapter #3
=====

IPv4-Routentabelle
=====
Aktive Routen:
Netzwerkziel      Netzwerkmaske      Gateway      Schnittstelle      Metrik
0.0.0.0           0.0.0.0           192.168.1.254  192.168.1.9        20
127.0.0.0         255.0.0.0         Auf Verbindung  127.0.0.1          306
127.0.0.1         255.255.255.255   Auf Verbindung  127.0.0.1          306
127.255.255.255   255.255.255.255   Auf Verbindung  127.0.0.1          306
192.168.1.0       255.255.255.0     Auf Verbindung  192.168.1.9        276
192.168.1.9       255.255.255.255   Auf Verbindung  192.168.1.9        276
192.168.1.255     255.255.255.255   Auf Verbindung  192.168.1.9        276
192.168.22.0      255.255.255.0     Auf Verbindung  192.168.22.254     276
192.168.22.254    255.255.255.255   Auf Verbindung  192.168.22.254     276
192.168.22.255    255.255.255.255   Auf Verbindung  192.168.22.254     276
224.0.0.0         240.0.0.0         Auf Verbindung  127.0.0.1          306
224.0.0.0         240.0.0.0         Auf Verbindung  192.168.1.9        276
224.0.0.0         240.0.0.0         Auf Verbindung  192.168.22.254     276
255.255.255.255   255.255.255.255   Auf Verbindung  127.0.0.1          306
255.255.255.255   255.255.255.255   Auf Verbindung  192.168.1.9        276
255.255.255.255   255.255.255.255   Auf Verbindung  192.168.22.254     276
=====
St.,ndige Routen:
Keine

IPv6-Routentabelle
=====
Aktive Routen:
If Metrik Netzwerkziel      Gateway
23 276 ::/0 Auf Verbindung
1 306 ::1/128 Auf Verbindung
11 58 2001::/32 Auf Verbindung
11 306 2001:0:5ef5:79fd:824:598:3f57:fef6/128 Auf Verbindung
19 276 2001:5c0:1115:1f00::/128 Auf Verbindung
23 276 2001:5c0:1400:b::/64 Auf Verbindung
23 276 2001:5c0:1400:b::c5b2/128 Auf Verbindung
23 276 2001:5c0:1400:b::c5b3/128 Auf Verbindung
19 276 2001:5c0:1519:e800::/64 Auf Verbindung
19 276 2001:5c0:1519:e800::/128 Auf Verbindung
19 276 2001:5c0:1519:e800::1/128 Auf Verbindung
19 276 2001:5c0:1519:e800:993c:17db:8d49:eba9/128 Auf Verbindung
19 276 fe80::/64 Auf Verbindung
23 276 fe80::/64 Auf Verbindung
11 306 fe80::/64 Auf Verbindung
11 306 fe80::824:598:3f57:fef6/128 Auf Verbindung
23 276 fe80::79c1:2798:4441:6a92/128 Auf Verbindung
19 276 fe80::993c:17db:8d49:eba9/128 Auf Verbindung
1 306 ff00::/8 Auf Verbindung
11 306 ff00::/8 Auf Verbindung
19 276 ff00::/8 Auf Verbindung
23 276 ff00::/8 Auf Verbindung
=====
St.,ndige Routen:
=====

```

Abb. 27: Routingtabelle des Windows Servers 2008 R2

4.2.7 Testen der IPv6 Erreichbarkeit des Servers von Intern

Dem Windows 7 Client im Netzwerk wurde das IPv6 Netzwerk über das Router Advertisement mitgeteilt und der Client hat sich daraus die IPv6 Adresse 2001:5c0:1519:e800:8d3b:140a:4499:1b90 berechnet. Zusätzlich ist ihm der Standard Gateway fe80::993c:17db:8d49:eba9%11 vom Windows Server 2008 R2 zugewiesen worden.

```
Ethernet-Adapter LAN-Verbindung:
  Verbindungsspezifisches DNS-Suffix: hubax.at
  Beschreibung. . . . . : Realtek RTL8139C+-Fast-Ethernet-Netzwerkkarte
  Physikalische Adresse . . . . . : 02-70-45-97-47-02
  DHCP aktiviert. . . . . : Ja
  Autokonfiguration aktiviert . . . : Ja
  IPv6-Adresse. . . . . : 2001:5c0:1519:e800:8d3b:140a:4499:1b90 (Bevorzugt)
  Temporäre IPv6-Adresse. . . . . : 2001:5c0:1519:e800:b1fe:9ada:9867:baa7 (Bevorzugt)
  Verbindungslokale IPv6-Adresse . : fe80::8d3b:140a:4499:1b90%11 (Bevorzugt)
  IPv4-Adresse . . . . . : 192.168.22.1 (Bevorzugt)
  Subnetzmaske . . . . . : 255.255.255.0
  Lease erhalten. . . . . : Dienstag, 24. Juli 2012 01:52:03
  Lease läuft ab. . . . . : Mittwoch, 1. August 2012 01:52:03
  Standardgateway . . . . . : fe80::993c:17db:8d49:eba9%11
                               192.168.22.254
  DHCP-Server . . . . . : 192.168.22.254
  DHCPv6-IAID . . . . . : 235040837
  DHCPv6-Client-DUID. . . . . : 00-01-00-01-17-4D-8F-94-02-70-45-97-47-02
  DNS-Server . . . . . : 8.8.8.8
                               8.8.4.4
  NetBIOS über TCP/IP . . . . . : Aktiviert
```

Abb. 28: Netzwerkkonfiguration der LAN Schnittstelle

Mit „ipconfig /all“ sieht man, dass dem Client noch kein IPv6 DNS Server zugeordnet wurde, ohne IPv4 könnte somit keine Adressauflösung gemacht werden. In der Abbildung 25 sieht man, dass die Namensauflösung über den IPv4 DNS Server geschieht und dass die IPv6 Adresse bevorzugt wird.

```
C:\Users\HubaX>ping google.at
Ping wird ausgeführt für google.at [2a00:1450:400d:805::1018] mit 32 Bytes Daten
:
Antwort von 2a00:1450:400d:805::1018: Zeit=64ms
Antwort von 2a00:1450:400d:805::1018: Zeit=64ms
Antwort von 2a00:1450:400d:805::1018: Zeit=64ms
Antwort von 2a00:1450:400d:805::1018: Zeit=65ms

Ping-Statistik für 2a00:1450:400d:805::1018:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 64ms, Maximum = 65ms, Mittelwert = 64ms

C:\Users\HubaX>nslookup ipv6.google.com.
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Nicht autorisierende Antwort:
Name:     ipv6.l.google.com
Address:  2a00:1450:400d:805::1014
Aliases:  ipv6.google.com

C:\Users\HubaX>_
```

Client

4.2.8 Testen der Erreichbarkeit des Clients von Extern

Der Ping auf einen lokalen Rechner wird durch die Firewall des Windows 7 Rechners blockiert. Der Windows 2008 Server lässt das ICMPv6 Protokoll passieren.

```
IPv6 Ping Output:  
PING 2001:5c0:1519:e800:94:8adf:aefb:7529(2001:5c0:1519:e800:94:8adf:aefb:7529) 32 data  
bytes  
  
--- 2001:5c0:1519:e800:94:8adf:aefb:7529 ping statistics ---  
4 packets transmitted, 0 received, 100% packet loss, time 2999ms  
Finished!
```

Abb. 30: Pingtest auf die LAN Schnittstelle des Windows 7 Clients

Um den Ping von einem externen Netzwerk zu erlauben, muss die Firewallregel „Datei- und Druckerfreigabe (Echoanforderungen – ICMPv6 eingehend)“ auf dem Windows 7 Client geändert werden. Somit werden Pakete aus allen Netzen akzeptiert.

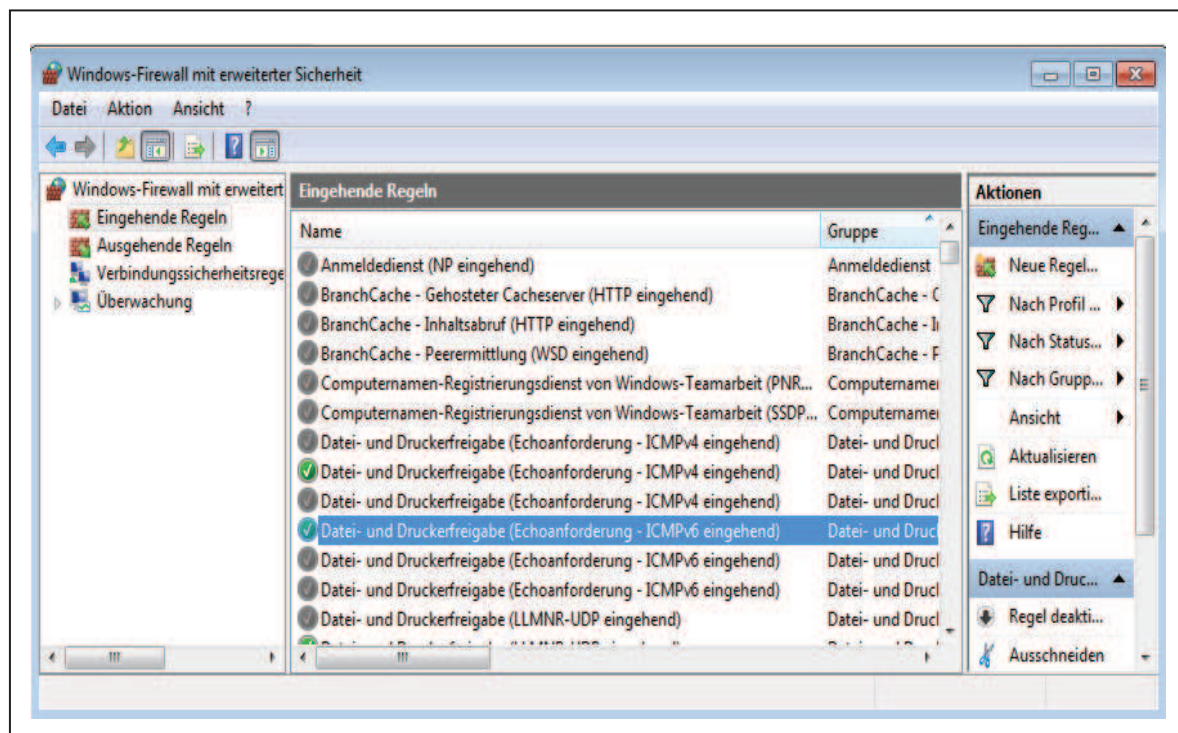


Abb. 31: Windows 7 Firewallregeln

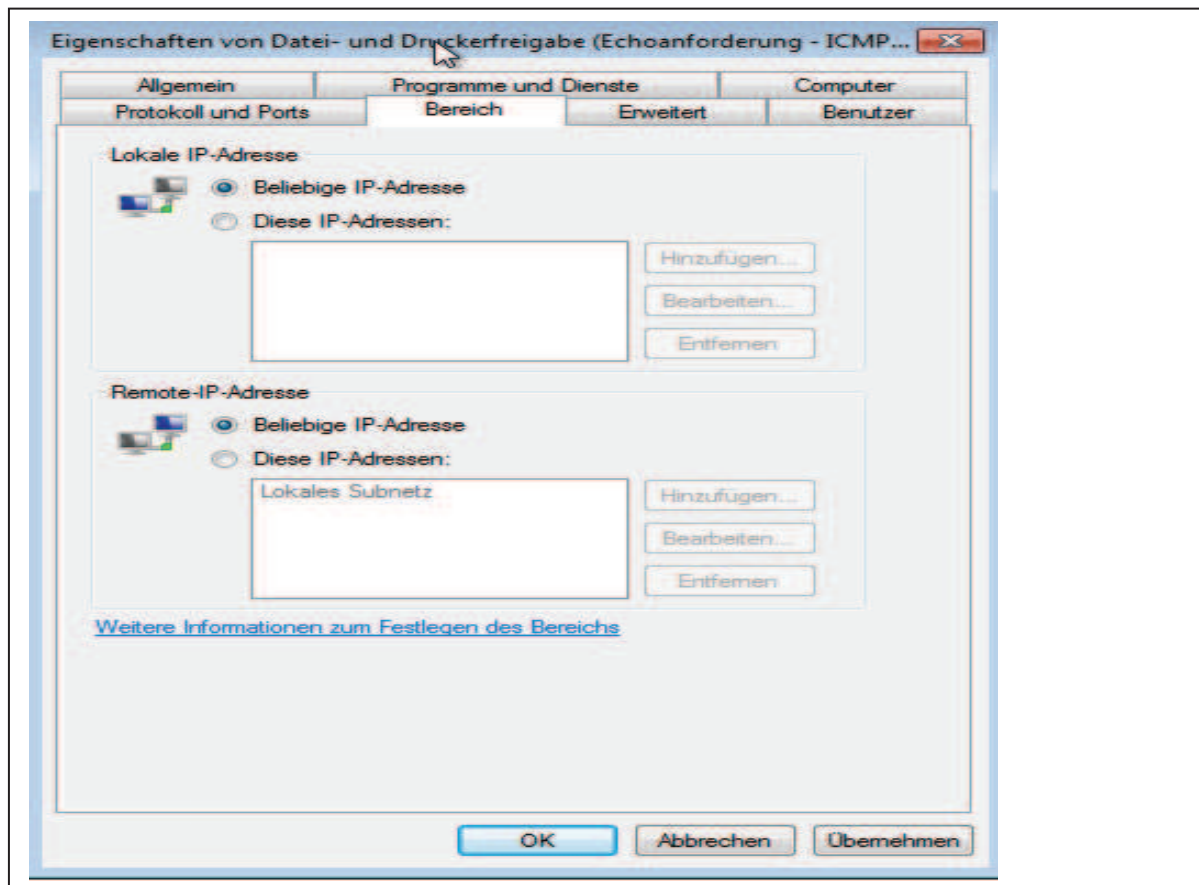


Abb. 32: Firewallregel für beliebige Netze konfigurieren

Mit den geänderten Firewallregeln lässt sich die LAN Schnittstelle des Windows 7 Clients außerhalb des Netzwerks pingen.

```
IPv6 Ping Output:

PING 2001:5c0:1519:e800:94:8adf:aefb:7529(2001:5c0:1519:e800:94:8adf:aefb:7529) 32 data bytes

40 bytes from 2001:5c0:1519:e800:94:8adf:aefb:7529: icmp_seq=0 ttl=121 time=52.0 ms
40 bytes from 2001:5c0:1519:e800:94:8adf:aefb:7529: icmp_seq=1 ttl=121 time=40.6 ms
40 bytes from 2001:5c0:1519:e800:94:8adf:aefb:7529: icmp_seq=2 ttl=121 time=40.4 ms
40 bytes from 2001:5c0:1519:e800:94:8adf:aefb:7529: icmp_seq=3 ttl=121 time=40.2 ms

--- 2001:5c0:1519:e800:94:8adf:aefb:7529 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 40.271/43.362/52.073/5.034 ms, pipe 2

Finished!
```

Abb. 33: erfolgreicher Ping auf die LAN Schnittstelle des Windows 7 Clients

4.3 DHCPv6 Server Installation am Windows Server¹⁰

4.3.1 Stateless DHCPv6 Server

Der DHCPv6 Server wurde bereits bei der Erstellung des DHCP Server erstellt, es wurde jedoch noch kein IPv6 Bereich definiert.

Im Moment läuft der Server in dem stateless Betrieb. Der Server merkt sich keinerlei Informationen der Clients, sondern liefert nur Informationen, wie DNS Server, an die Clients im Netzwerk. Jedoch sind noch keine Informationen am Server eingetragen. Dies geschieht unter „Rollen -> DHCP-Server -> IPv6 -> Serveroptionen -> Optionen konfigurieren ...“. Dort kann die Option 23 „IPv6-Adressliste für DNS-Server ...“ hinzugefügt werden und ein IPv6 DNS Server eingetragen werden.

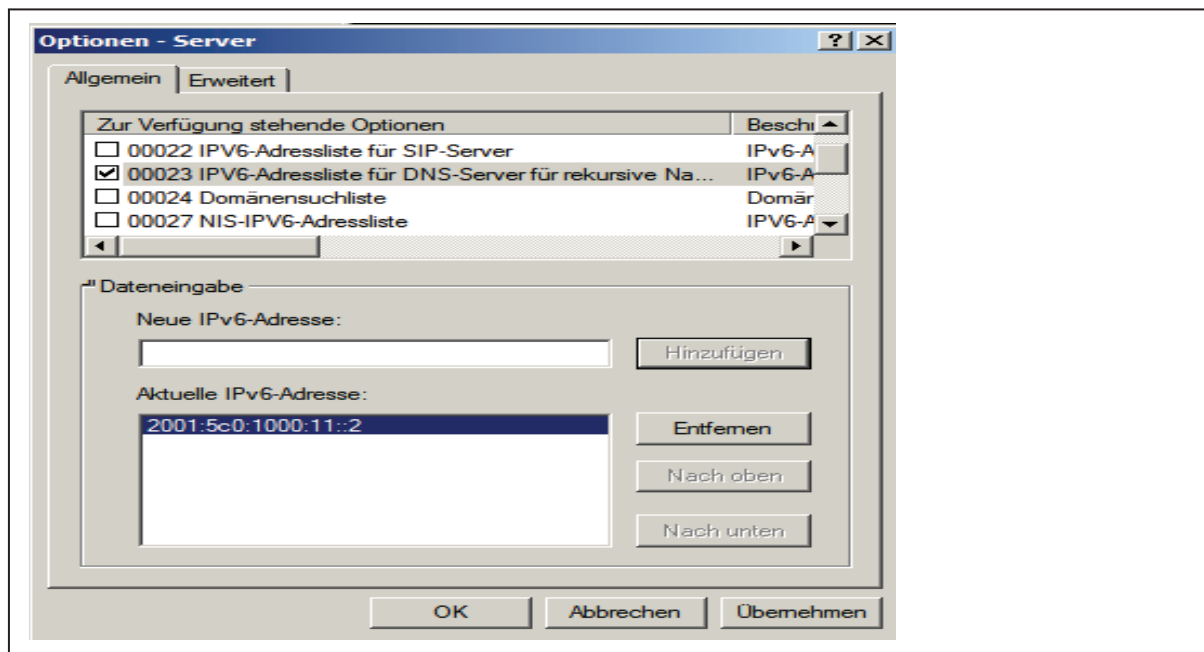


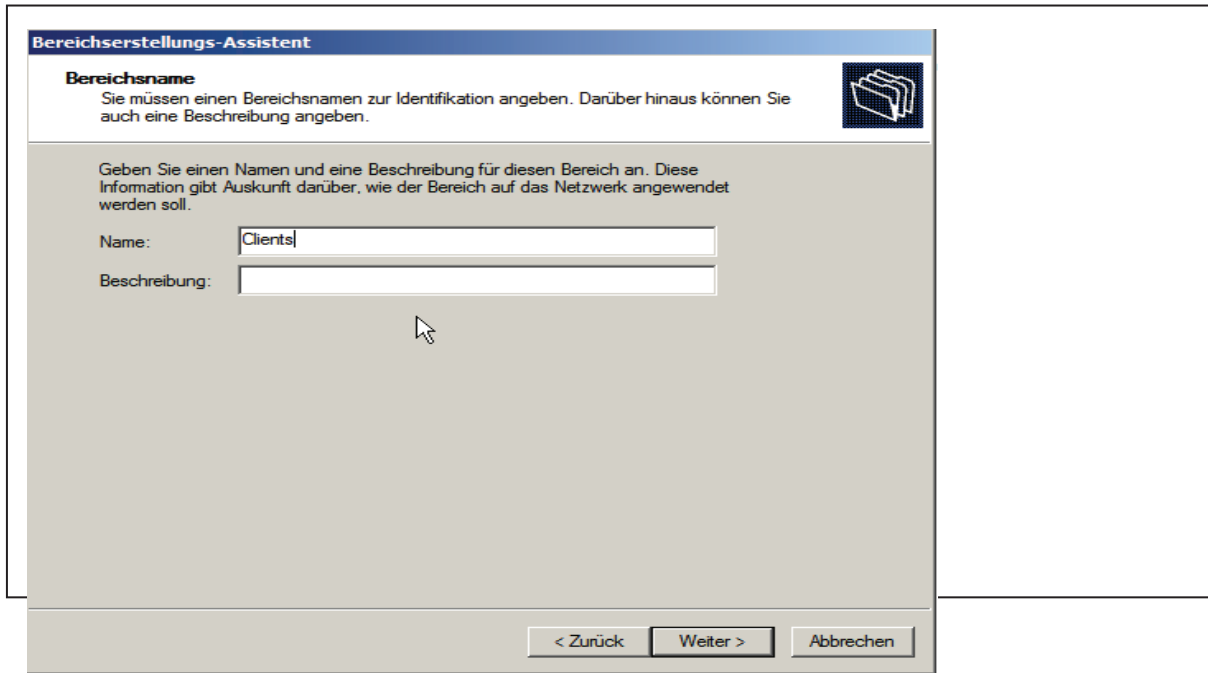
Abb. 34: IPv6 DNS Server hinzufügen

Nach dem Hinzufügen und Schließen des Fensters hat der Windows 7 Client diese Einstellungen übernommen und die DNS Auflösung kann über die IPv6 Verbindung getestet werden.

¹⁰ statefull & stateless DHCPv6 Configuration, <http://blogs.technet.com/b/teamdhcp/archive/2009/03/03/dhcpv6-understanding-of-address-configuration-in-automatic-mode-and-installation-of-dhcpv6-server.aspx>

4.3.2 Statefull DHCPv6 Server

Ein statefull DHCPv6 Server verteilt aktiv IP Adressen und merkt sich die Leases und kann fixe Adressen immer denselben Hosts zuordnen, wie schon bei IPv4. Um einen neuen Bereich anzulegen kann unter „Rollen -> DHCP-Server -> IPv6 -> Neuer Bereich“ ein Assistent geöffnet werden.



Wir folgen dem Assistenten und geben einen Namen für unseren Bereich ein. Auf der nächsten Seite bestimmen wir den Präfix (die Netzwerkmaske ist fix) und die Präferenz.

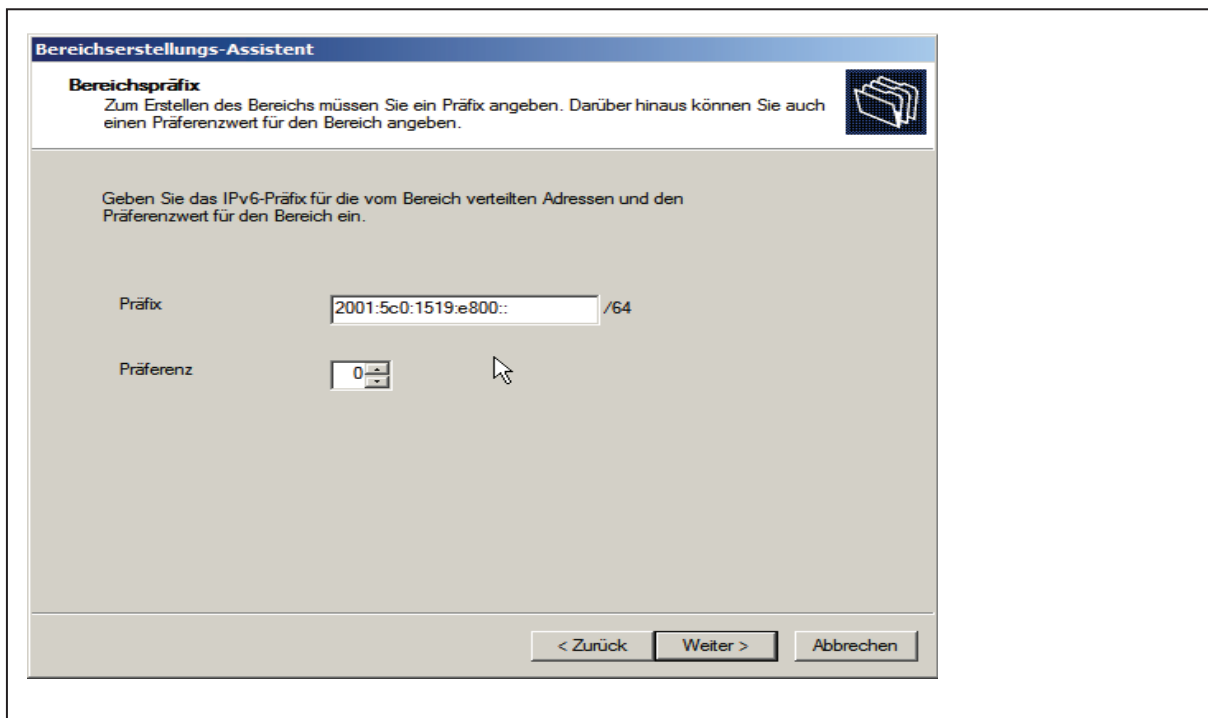


Abb. 36: Bereichspräfix einstellen

Bereichserstellungs-Assistent

Ausschlüsse hinzufügen
Ausschlüsse sind Adressen oder ein Adressbereich, die/der nicht vom Server verteilt werden/wird.

Geben Sie den IPv6-Adressbereich ein, den Sie für den angegebenen Bereich ausschließen möchten. Wenn Sie eine einzelne Adresse ausschließen möchten, geben Sie in "Start-IPv6-Adresse" nur eine ID ein.

Start-IPv6-Adresse: 2001:5c0:1519:e800:

End-IPv6-Adresse: 2001:5c0:1519:e800:

Ausgeschlossener Adressbereich:

2001:5c0:1519:e800::1:1 nach 2001:5c0:1519:e800:ffff:ffff

Abb. 37: Bereichsausschluss hinzufügen

Im nächsten Schritt kann man Adressbereiche ausnehmen. Die Adressen aus diesem Bereich werden nicht vergeben. Zum Beispiel können in diesem Bereich fixe Adressen für Server vergeben werden.

Bereichserstellungs-Assistent

Bereichslease
Die Leasedauer bestimmt, für wie lange ein Client eine IPv6-Adresse aus diesem Bereich verwenden kann.

Die Leasedauer sollte normalerweise mit der durchschnittlichen Zeit übereinstimmen, die der Computer mit dem gleichen physikalischen Netzwerk verbunden ist.

Nicht temporäre Adresse (IANA)

Bevorzugte Gültigkeitsdauer

Tage: Stunden: Minuten:

Gültigkeitsdauer

Tage: Stunden: Minuten:

Nach dem Fertigstellen des Assistenten und aktivieren des Bereichs ist in den Adressleases die Adresse des Windows 7 Clients zu sehen.

4.3.3 Testen des Statefull DHCPv6 Servers

Die Netzwerkkonfiguration des Clients zeigt die zugeteilte IPv6 Adresse.

```
Ethernet-Adapter LAN-Verbindung:

Verbindungsspezifisches DNS-Suffix: hubax.at
Beschreibung. . . . . : Realtek RTL8139C+-Fast-Ethernet-Netzwerkkarte
Physikalische Adresse . . . . . : 02-70-45-97-47-02
DHCP aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . : Ja
IPv6-Adresse. . . . . : 2001:5c0:1519:e800:5e76:d0b:f05f:9295 (Bevorzugt)
Lease erhalten. . . . . : Mittwoch, 25. Juli 2012 02:22:04
Lease l„uft ab. . . . . : Montag, 6. August 2012 02:22:04
IPv6-Adresse. . . . . : 2001:5c0:1519:e800:8d3b:140a:4499:1b90 (Bevorzugt)
Tempor„re IPv6-Adresse. . . . . : 2001:5c0:1519:e800:3174:c690:dd3a:555d (Bevorzugt)
Verbindungslokale IPv6-Adresse . : fe80::8d3b:140a:4499:1b90%11 (Bevorzugt)
IPv4-Adresse . . . . . : 192.168.22.1 (Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.0
Lease erhalten. . . . . : Mittwoch, 25. Juli 2012 02:22:02
Lease l„uft ab. . . . . : Donnerstag, 2. August 2012 02:22:02
Standardgateway . . . . . : fe80::993c:17db:8d49:eba9%11
                          192.168.22.254
DHCP-Server . . . . . : 192.168.22.254
DHCPv6-IAID . . . . . : 235040837
DHCPv6-Client-DUID. . . . . : 00-01-00-01-17-4D-8F-94-02-70-45-97-47-02
DNS-Server . . . . . : 2001:5c0:1000:11::2
                          8.8.8.8
                          8.8.4.4
NetBIOS „ber TCP/IP . . . . . : Aktiviert
Suchliste f„r verbindungsspezifische DNS-Suffixe:
                          hubax.at
```

Abb. 39: Netzwerkkonfiguration des Windows 7 Clients

Wie in der Abbildung 38 zu sehen ist, bekommt der Client nun eine IPv6 Adresse zugeordnet und auch ein DNS Server mit einer IPv6 Adresse. Es kann nun getestet werden, ob die Namensauflösung über den IPv6 Server geschieht. Dazu wird das Tool nslookup und die Adresse „ipv6.google.com.“ bzw. „google.com.“ verwendet.

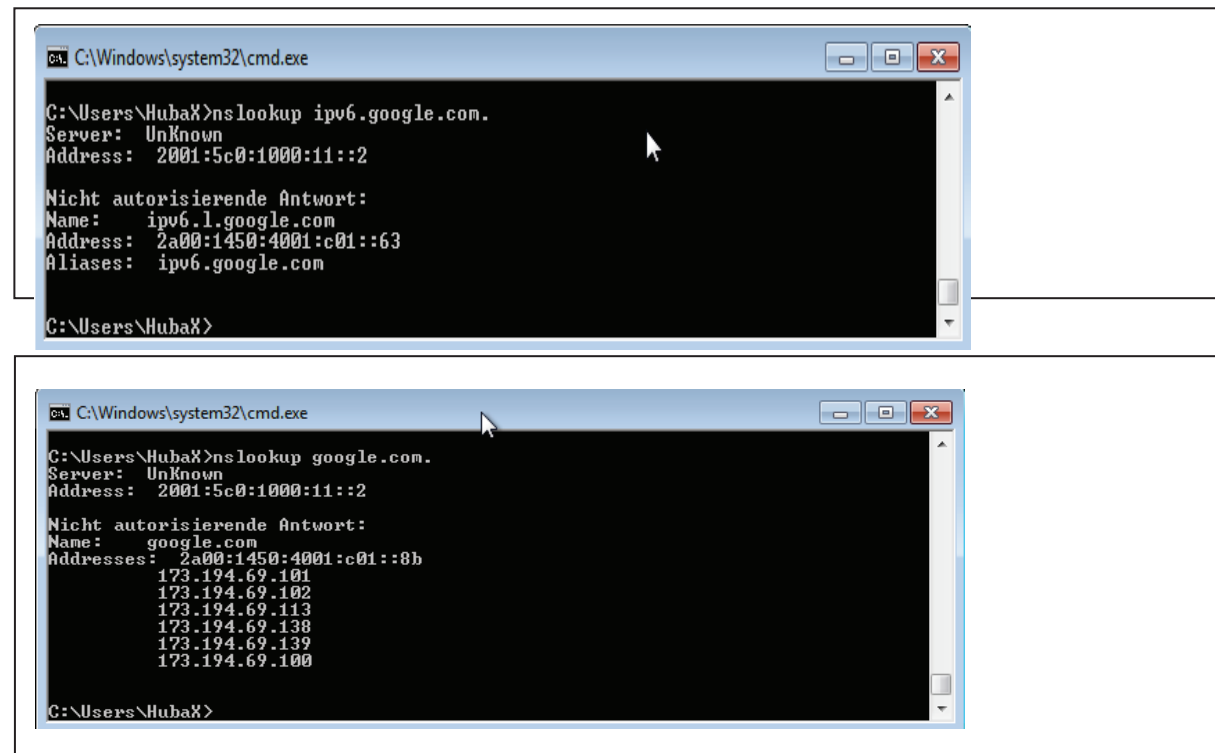


Abb. 41: "nslookup" Test google.com

4.4 IPv6 DNS Server Installation am Windows Server

Um eine DNS Auflösung unserer lokalen Domain „ip6test.hubax.at“ zu ermöglichen, wird auf dem Windows 2008 Server ein DNS Server installiert. Damit ist eine Auflösung auf IPv4 sowie auf IPv6 Adressen möglich. Damit kann der DHCP Server Adressen der Clients dynamisch auf dem DNS Server updaten. Der Server kann über den Servermanager installiert und konfiguriert werden.

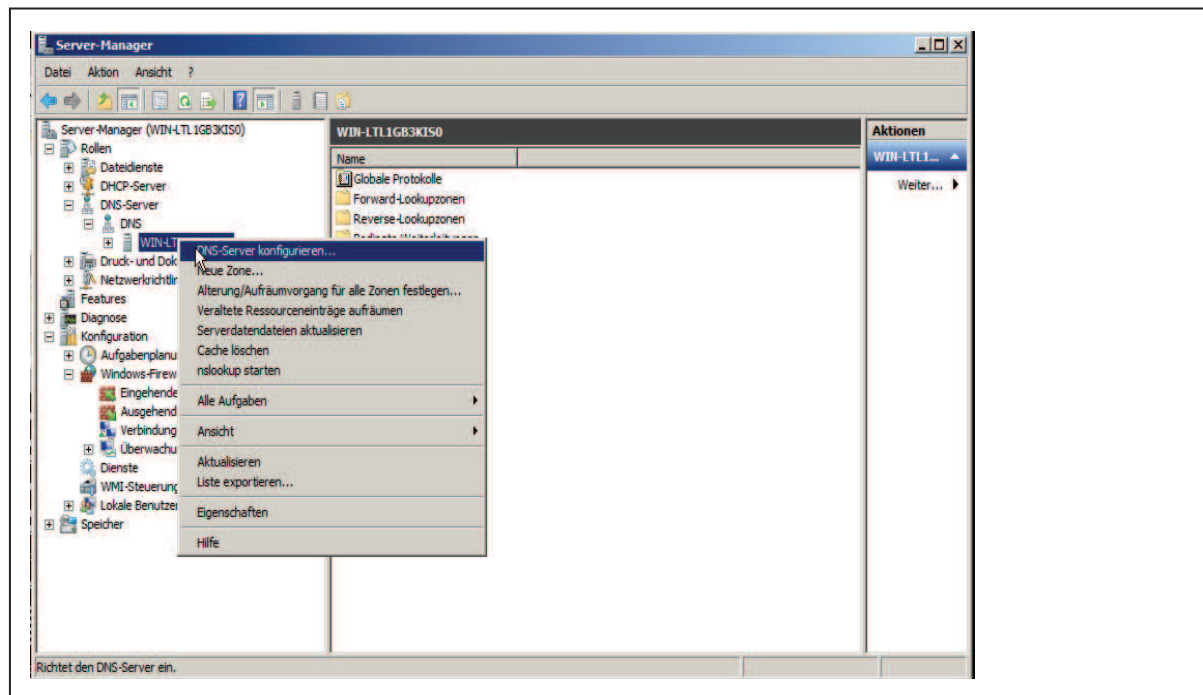


Abb. 42: DNS Server Konfiguration

Der Einfachheit halber erstellen wir eine Forward-Lookup Zone (ohne Reverse-Lookup Zone) für die Domain „ip6test.hubax.at“.

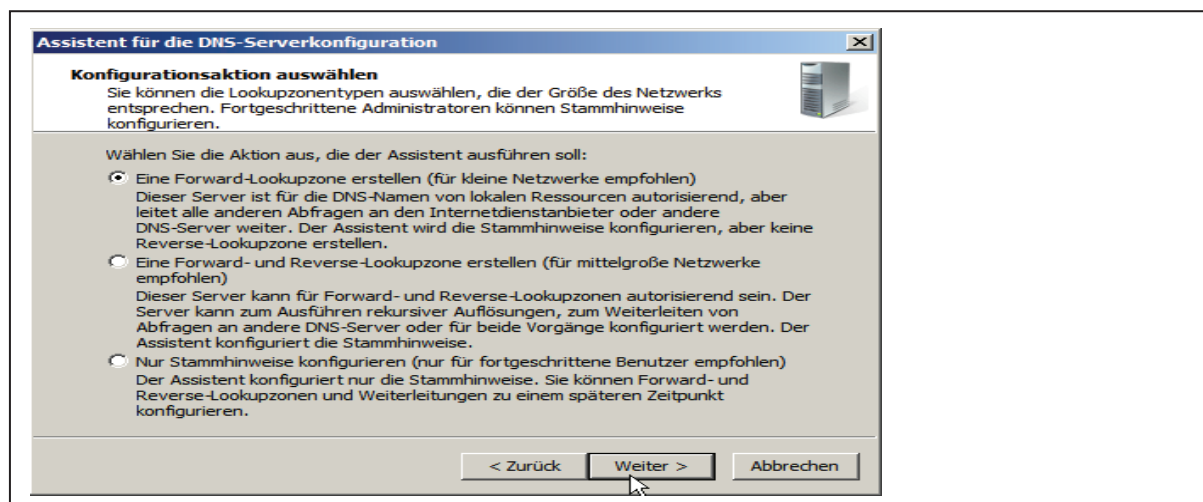


Abb. 43: Forward Lookupzone erstellen

Im nächsten Installationsschritt werden wir zunächst dynamische Updates nicht zulassen, jedoch später aktivieren, um eine DNS Auflösung für die wechselnden IP-Adressen der DHCP Clients zu ermöglichen.

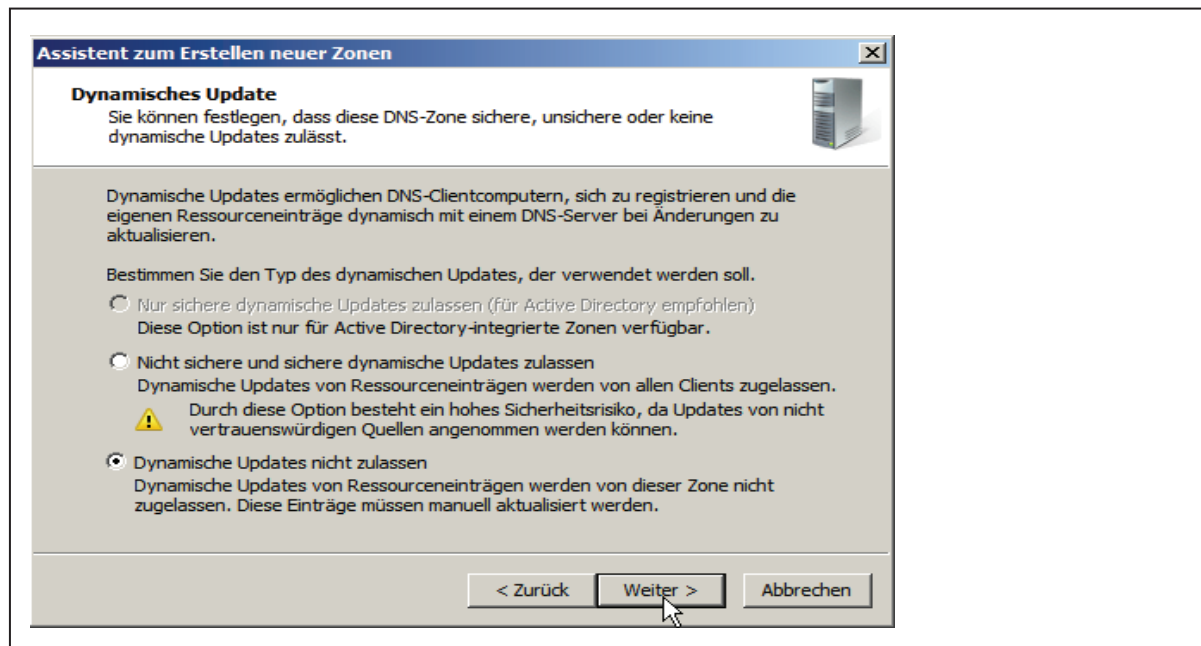


Abb. 44: Dynamische Updates nicht zulassen

Anschließend werden IPv6 und IPv4 DNS Server eingetragen, zu denen Anfragen weitergeleitet werden.

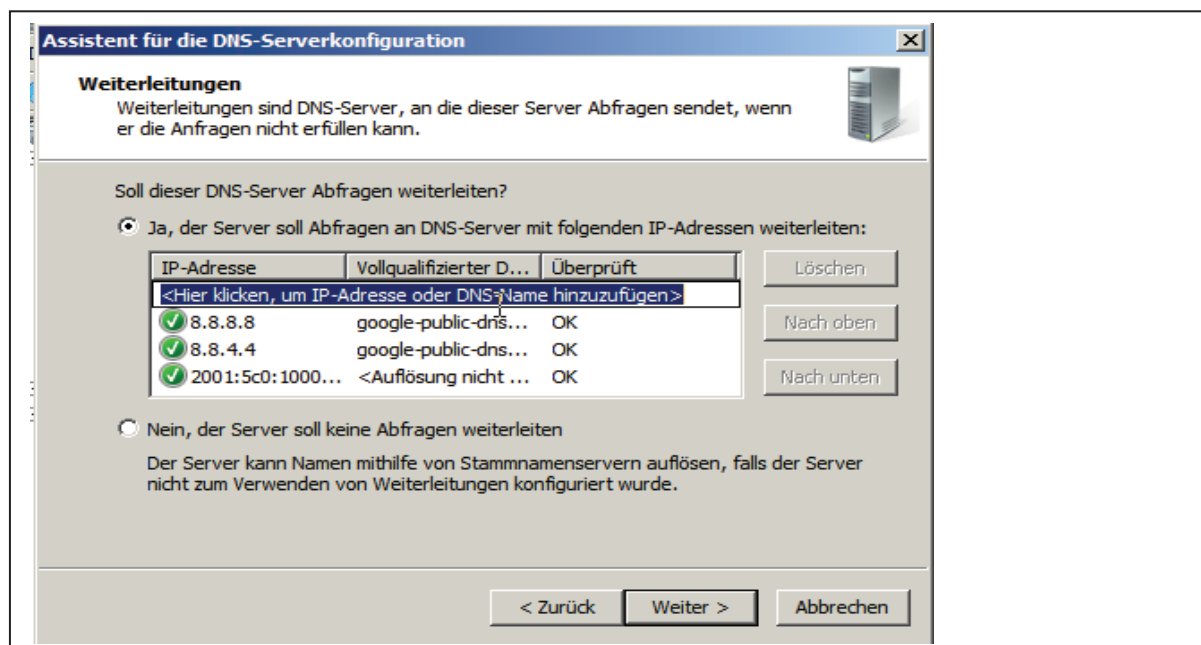


Abb. 45: DNS Weiterleitungen

4.4.1 DHCP Server auf DNS Server konfigurieren

Unter den Eigenschaften für den DHCPv6 Server kann die dynamische DNS-Aktualisierung aktiviert werden. Dabei können die Einträge immer aktualisiert werden oder nur bei Anfrage des Clients. Außerdem wird dem Client die Suchdomain und die Adresse des Windows 2008 Servers als Primärer DNS-Server mitgeteilt.

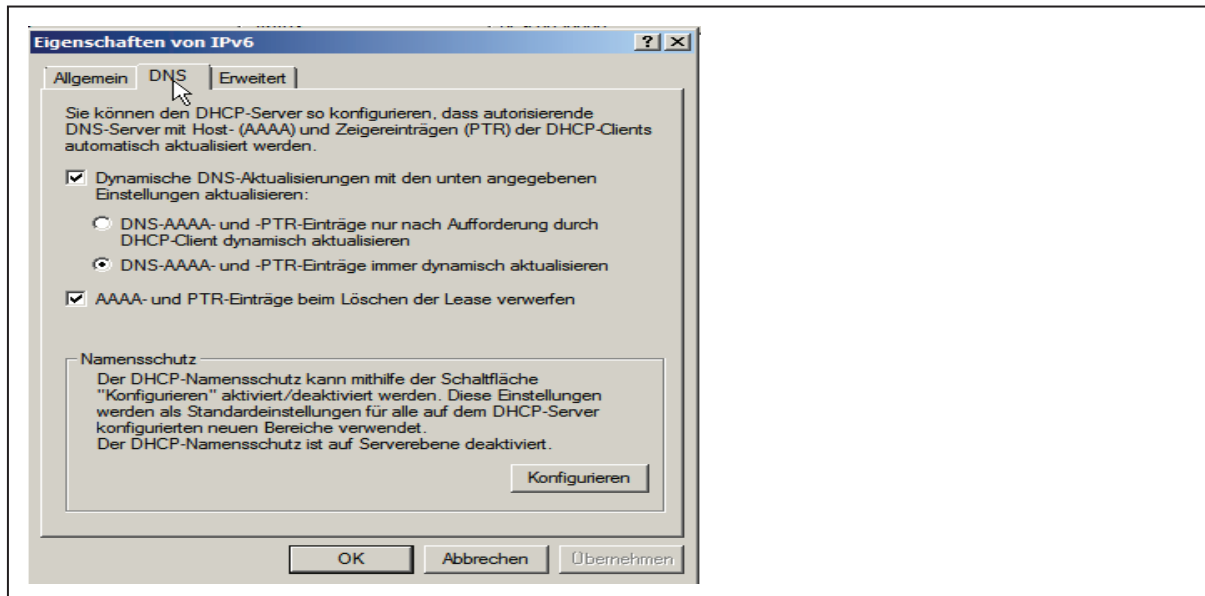


Abb. 46: DNS Einstellungen am DHCPv6 Server

Unter „Rollen -> DHCP-Server -> IPv6 -> Serveroptionen -> Optionen konfigurieren ...“ wird der Eintrag „ip6test.hubax.at“ für die Domänensuchliste hinzugefügt.

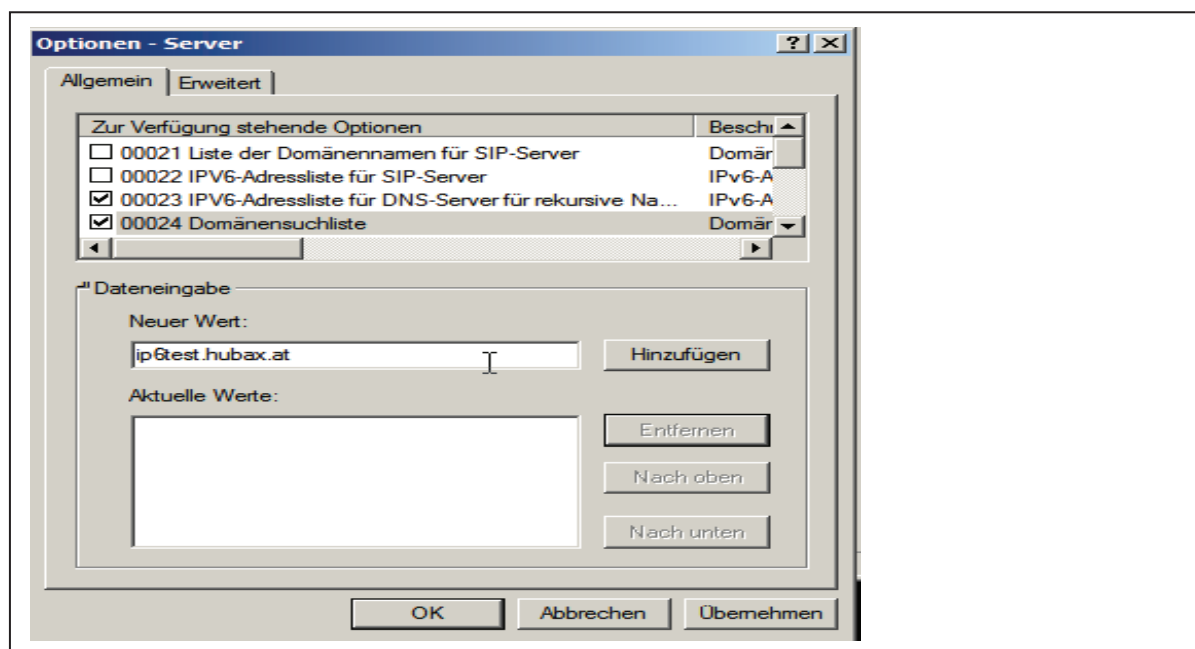


Abb. 47: neuer Eintrag in der Domänensuchliste

Als Adresse für den DNS Server wird die Link-Local Adresse verwendet.

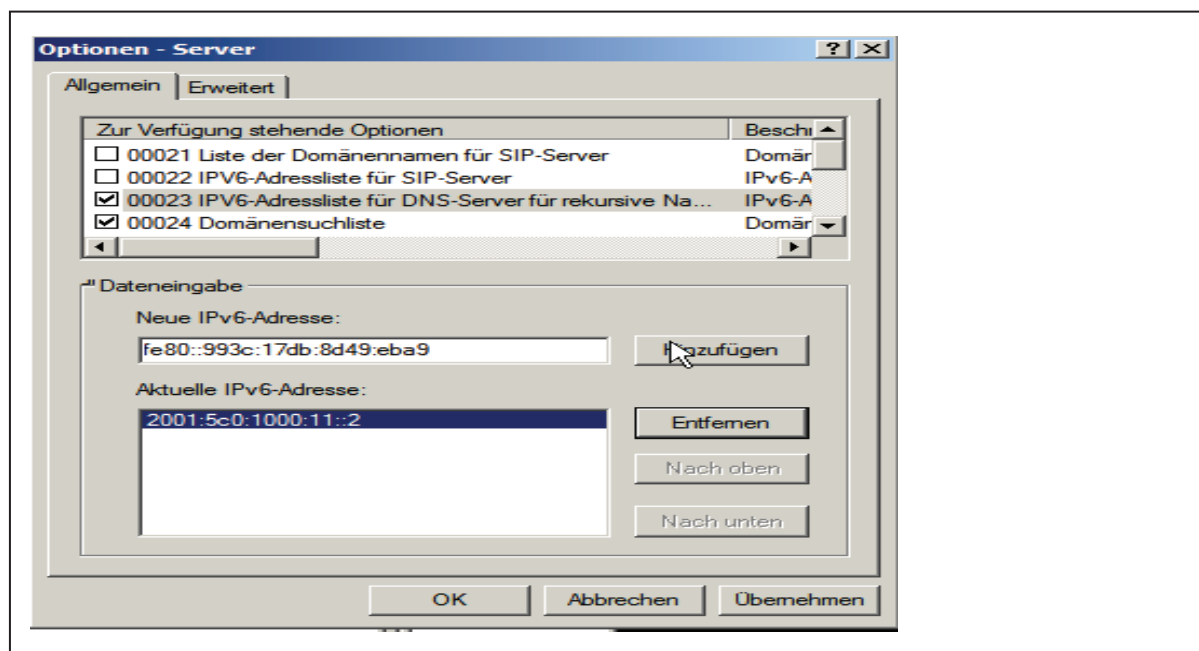


Abb. 48: IPv6 Adresse für DNS Server Namensauflösung

Dieselben Einstellungen werden dann auch für den DHCPv4 Server getroffen.

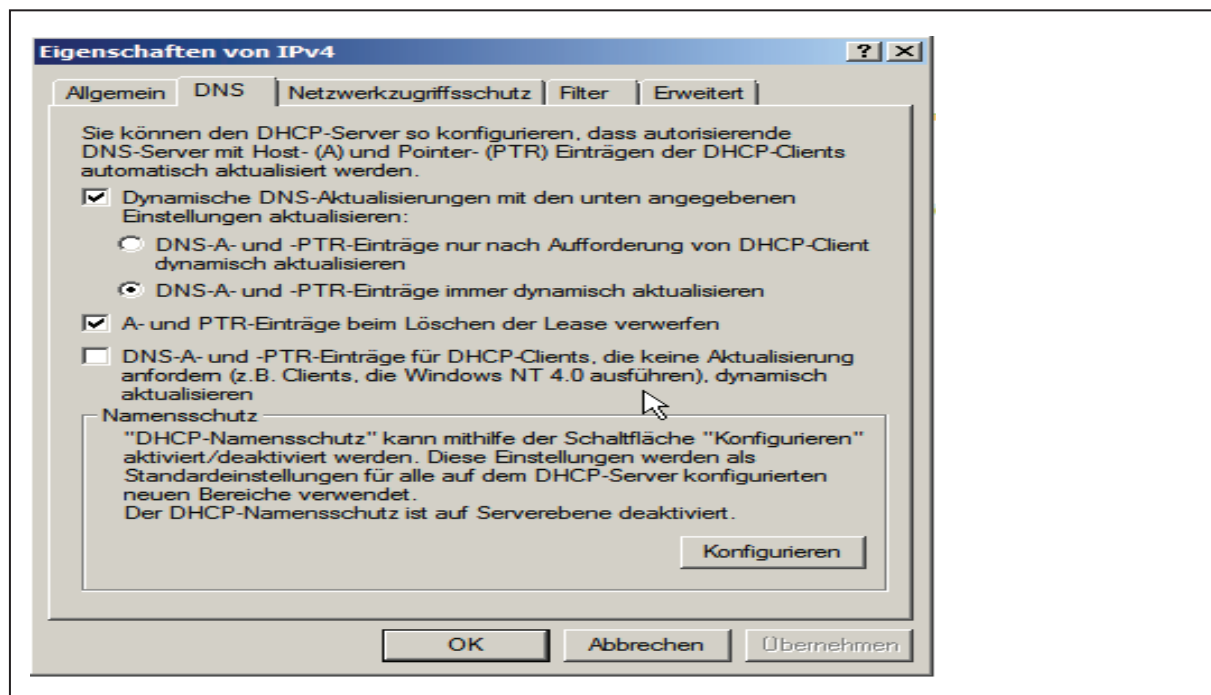


Abb. 49: DNS Einstellungen am DHCPv4 Server

Unter „Rollen -> DHCP-Server -> IPv4 -> Serveroptionen -> Optionen konfigurieren ...“ wird der Eintrag „ip6test.hubax.at“ für die Domänensuchliste hinzugefügt.

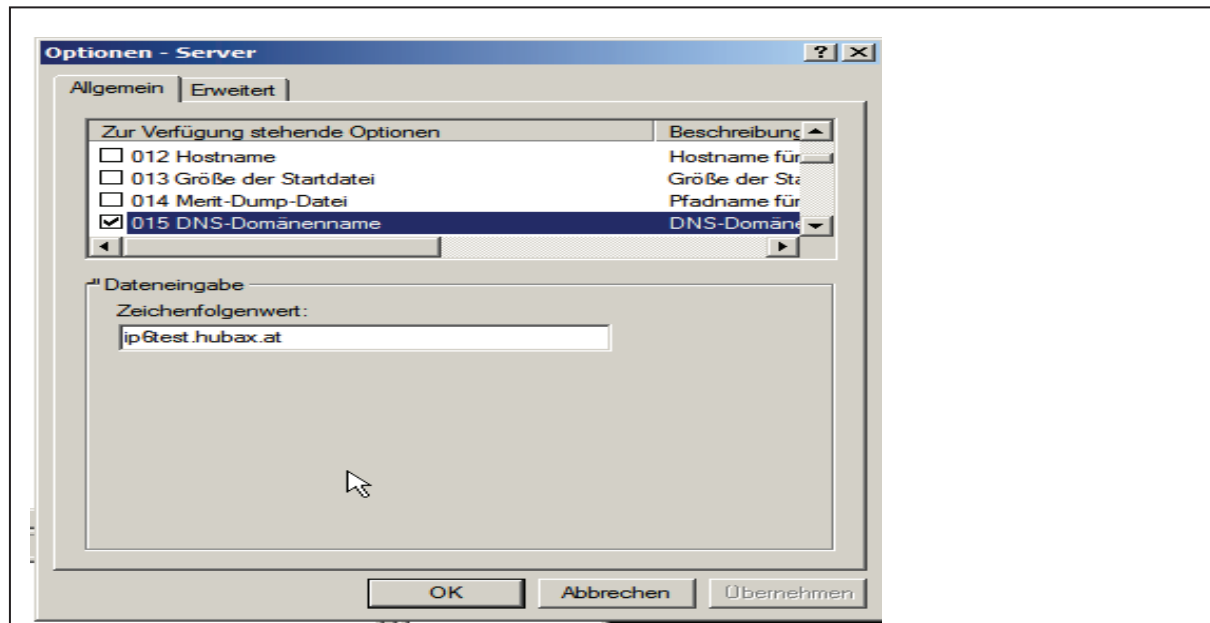


Abb. 50: neuer Eintrag in der Domänensuchliste

Als Adresse für den DNS Server wird die Adresse der LAN Schnittstelle des Servers verwendet.

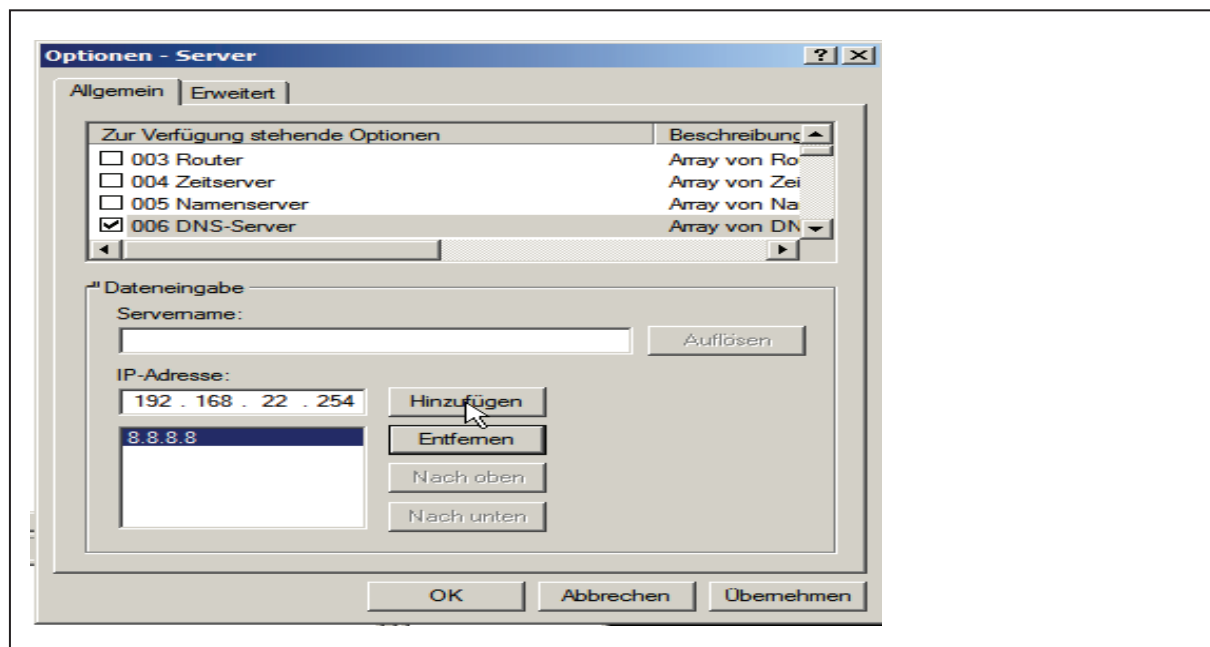


Abb. 51: IPv4 Adresse für DNS Server

4.4.2 Statischen DNS Record anlegen

Ein DNS Record für eine IPv6 oder IPv4 Adresse, die sich nicht ändert, kann über einen einfachen Eintrag erzeugt werden. Es wird der DNS Name und die IP Adresse eingetragen und der Assistent entscheidet über die Art der IP Adresse, ob es sich um einen AAAA (für IPv6) oder einen A (für IPv4) Eintrag handelt.

Unter Forward Lookupzonen am DNS Server einen neuen Host mit einer IPv6 Adresse anlegen.

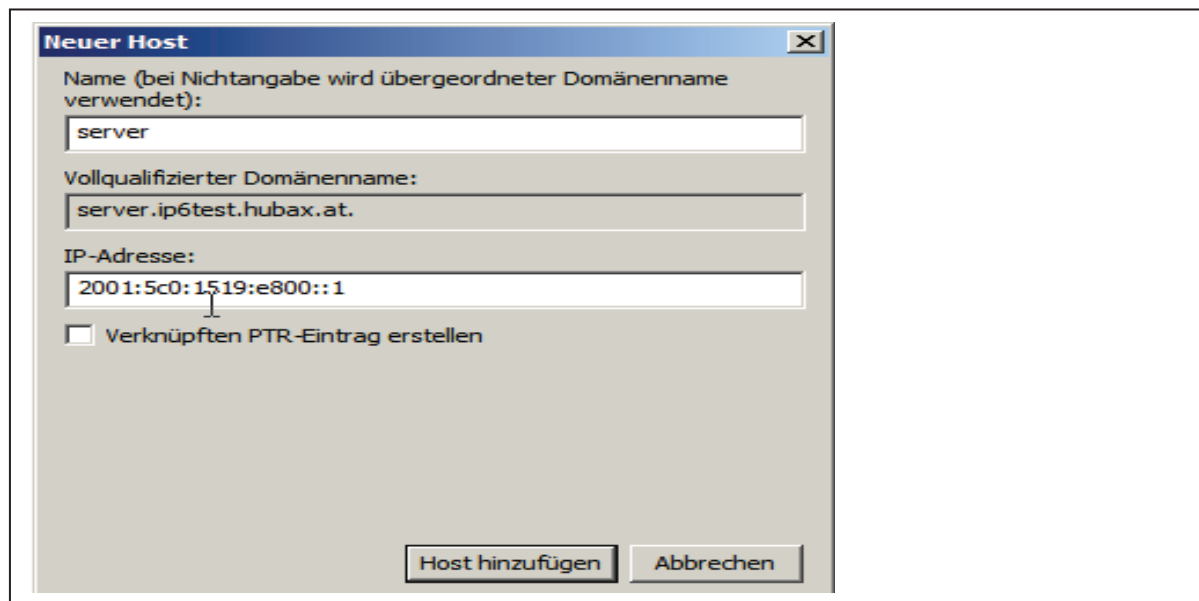


Abb. 52: neuen Host am DNS Server anlegen

Nun erfolgt der Erreichbarkeitstest mittels Pingtest am Windows 7 Client.

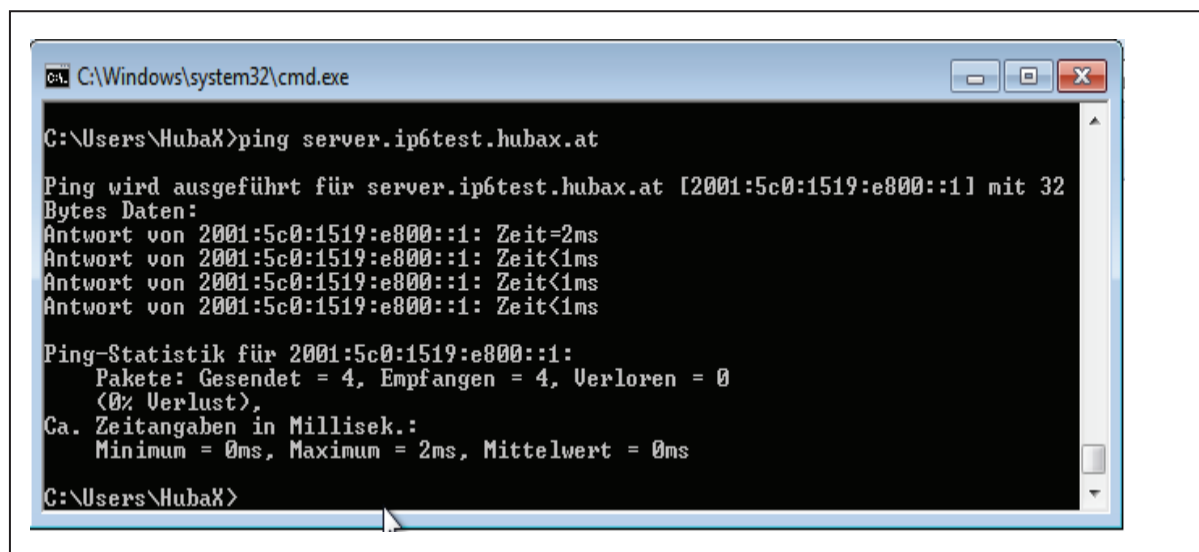
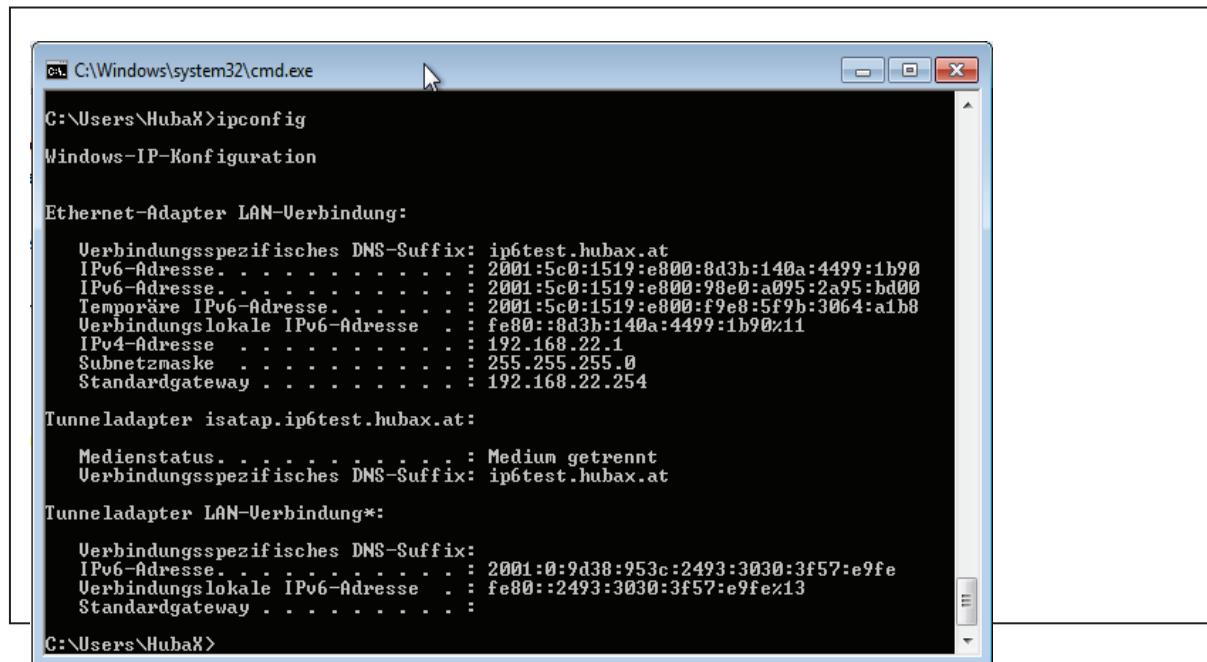


Abb. 53: Pingtest am Windows 7 Client

4.5 Sicherheitsfunktionen unter Windows 7 deaktivieren

4.5.1 Randomized Identifiers deaktivieren¹¹

Standardmäßig erzeugt Windows 7 und Vista die IPv6 Adresse aus der MAC Adresse. Jedoch nicht nach dem EUI64 Verfahren, sondern mit sogenannten „Randomized Identifiers“.



Mit dem Befehl „Netsh interface ipv6 set global randomizedidentifiers=disabled“ wird die Randomize Funktion deaktiviert. Dies muss mit Administratorrechten geschehen.

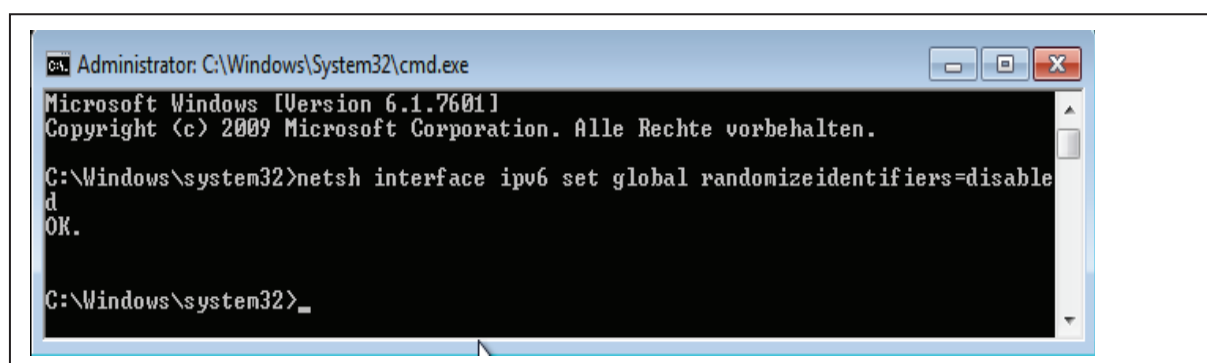


Abb. 55: deaktivieren der Randomize Funktion

¹¹ Randomized Identifiers deaktivieren,

<http://www.heise.de/netze/artikel/IPv6-Privacy-Extensions-einschalten-1204783.html?artikelseite=2>

Wie man sieht, hat sich die selbst erzeugte globale Adresse sowie die Link Lokale Adresse geändert und man erkennt bereits den Zusammenhang zwischen IPv6 Adresse und MAC Adresse.

MAC: 02-70-45-97-47-02
Globale IPv6 Adresse: 2001:5c0:1519:e800:70:45ff:fe97:4702
Link-Local IPv6 Adresse: fe80::70:45ff:fe97:4702

```
C:\Windows\system32\cmd.exe
C:\Users\HubaX>ipconfig

Windows-IP-Konfiguration

Ethernet-Adapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix: ip6test.hubax.at
    IPv6-Adresse. . . . . : 2001:5c0:1519:e800:70:45ff:fe97:4702
    IPv6-Adresse. . . . . : 2001:5c0:1519:e800:98e0:a095:2a95:bd00
    Temporäre IPv6-Adresse. . . . . : 2001:5c0:1519:e800:7542:840a:2eb7:6de5
    Temporäre IPv6-Adresse. . . . . : 2001:5c0:1519:e800:f9e8:5f9b:3064:a1b8
    Verbindungslokale IPv6-Adresse . . : fe80::70:45ff:fe97:4702%11
    IPv4-Adresse . . . . . : 192.168.22.1
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : fe80::993c:17db:8d49:eba9%11
                               192.168.22.254

Tunneladapter isatap.ip6test.hubax.at:

    Medienstatus. . . . . : Medium getrennt
    Verbindungsspezifisches DNS-Suffix: ip6test.hubax.at

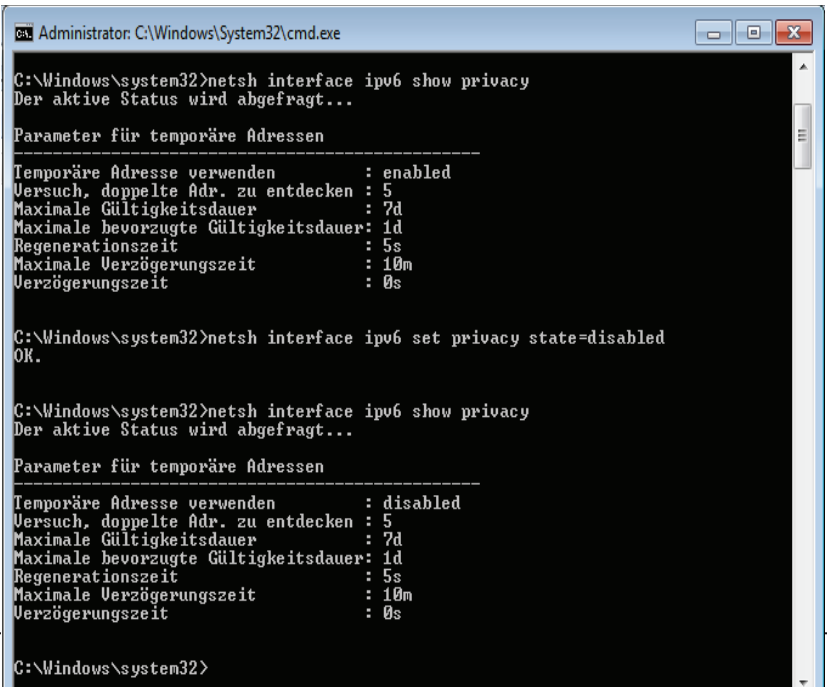
Tunneladapter LAN-Verbindung*:

    Verbindungsspezifisches DNS-Suffix:
    IPv6-Adresse. . . . . : 2001:0:9d38:953c:3c18:20a3:3f57:e9fe
    Verbindungslokale IPv6-Adresse . . : fe80::3c18:20a3:3f57:e9fe%13
    Standardgateway . . . . . :
```

Abb. 56: aktuelle Netzwerkkonfiguration am Windows 7 Client

4.5.2 Privacy Extension deaktivieren¹²

Die Privacy Extension veranlasst Windows in regelmäßigen Abständen eine temporäre IPv6 Adresse zu wählen und diese immer wieder zu ändern. Dies kann mit dem Befehl „Netsh interface ipv6 set privacy state=disabled“ abgeschaltet werden. Bei Windows Server Versionen ist diese Feature standardmäßig deaktiviert, da dort eine ständig wechselnde Adresse nicht von Vorteil ist.



```
Administrator: C:\Windows\System32\cmd.exe

C:\Windows\system32>netsh interface ipv6 show privacy
Der aktive Status wird abgefragt...

Parameter für temporäre Adressen
-----
Temporäre Adresse verwenden           : enabled
Versuch, doppelte Adr. zu entdecken  : 5
Maximale Gültigkeitsdauer             : 7d
Maximale bevorzugte Gültigkeitsdauer : 1d
Regenerationszeit                     : 5s
Maximale Verzögerungszeit             : 10m
Verzögerungszeit                      : 0s

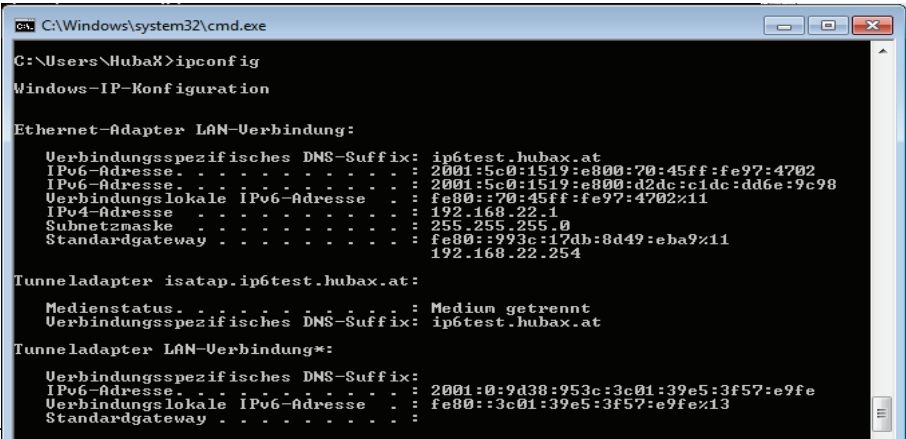
C:\Windows\system32>netsh interface ipv6 set privacy state=disabled
OK.

C:\Windows\system32>netsh interface ipv6 show privacy
Der aktive Status wird abgefragt...

Parameter für temporäre Adressen
-----
Temporäre Adresse verwenden           : disabled
Versuch, doppelte Adr. zu entdecken  : 5
Maximale Gültigkeitsdauer             : 7d
Maximale bevorzugte Gültigkeitsdauer : 1d
Regenerationszeit                     : 5s
Maximale Verzögerungszeit             : 10m
Verzögerungszeit                      : 0s

C:\Windows\system32>
```

Die temporären Adressen werden nach der Gültigkeitsdauer oder nach einem Neustart des Interfaces fallen gelassen.



```
C:\Windows\system32\cmd.exe

C:\Users\HubaX>ipconfig

Windows-IP-Konfiguration

Ethernet-Adapter LAN-Verbindung:

    Verbindungsspezifisches DNS-Suffix: ip6test.hubax.at
    IPv6-Adresse. . . . . : 2001:5c0:1519:e800:70:45ff:fe97:4702
    IPv6-Adresse. . . . . : 2001:5c0:1519:e800:d2dc:c1dc:dd6e:9c98
    Verbindungslokale IPv6-Adresse . . : fe80::70:45ff:fe97:4702%11
    IPv4-Adresse . . . . . : 192.168.22.1
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : fe80::993c:17db:8d49:eba9%11
                               192.168.22.254

Tunneladapter isatap.ip6test.hubax.at:

    Medienstatus. . . . . : Medium getrennt
    Verbindungsspezifisches DNS-Suffix: ip6test.hubax.at
    Tunneladapter LAN-Verbindung*:

    Verbindungsspezifisches DNS-Suffix:
    IPv6-Adresse. . . . . : 2001:0:9d38:953c:3c01:39e5:3f57:e9fe
    Verbindungslokale IPv6-Adresse . . : fe80::3c01:39e5:3f57:e9fe%13
    Standardgateway . . . . . :

C:\Users\HubaX>
```

Abb. 58: temporäre IPv6 Adresse nicht mehr vorhanden

¹² Privacy Extension deaktivieren, <http://www.heise.de/netze/artikel/IPv6-Privacy-Extensions-einschalten-1204783.html?artikelseite=2>

4.6 IPv6 Konfiguration auf Windows XP¹³

Nach der Installation von Windows XP SP3 ist die Unterstützung für IPv6 deaktiviert.

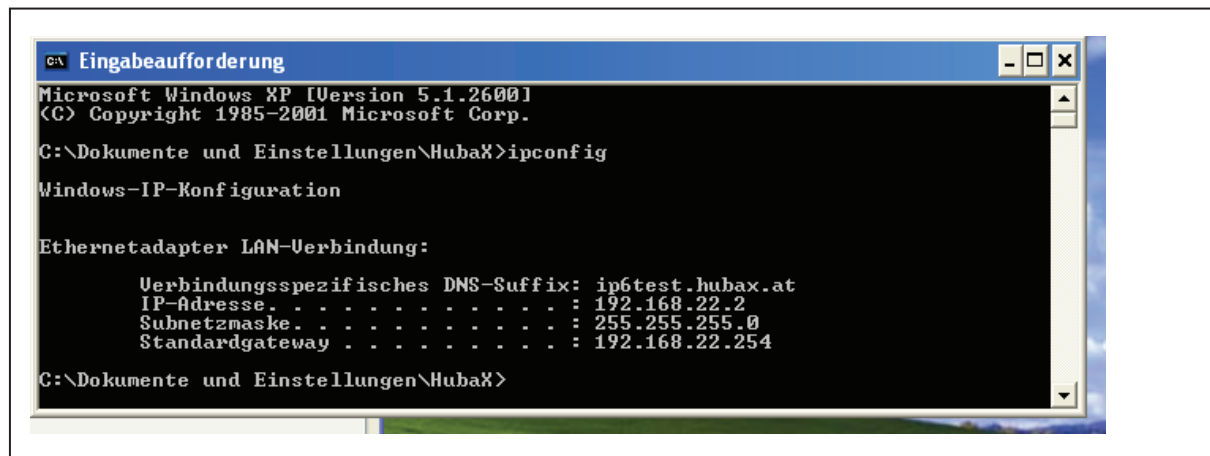


Abb. 59: Windows XP Netzwerkkonfiguration

Nach der Aktivierung mittels „netsh interface ipv6 install“ ist Windows XP IPv6 fähig. Windows XP kann per Autokonfiguration eine IPv6 Adresse wählen und einen Standardgateway erhalten.

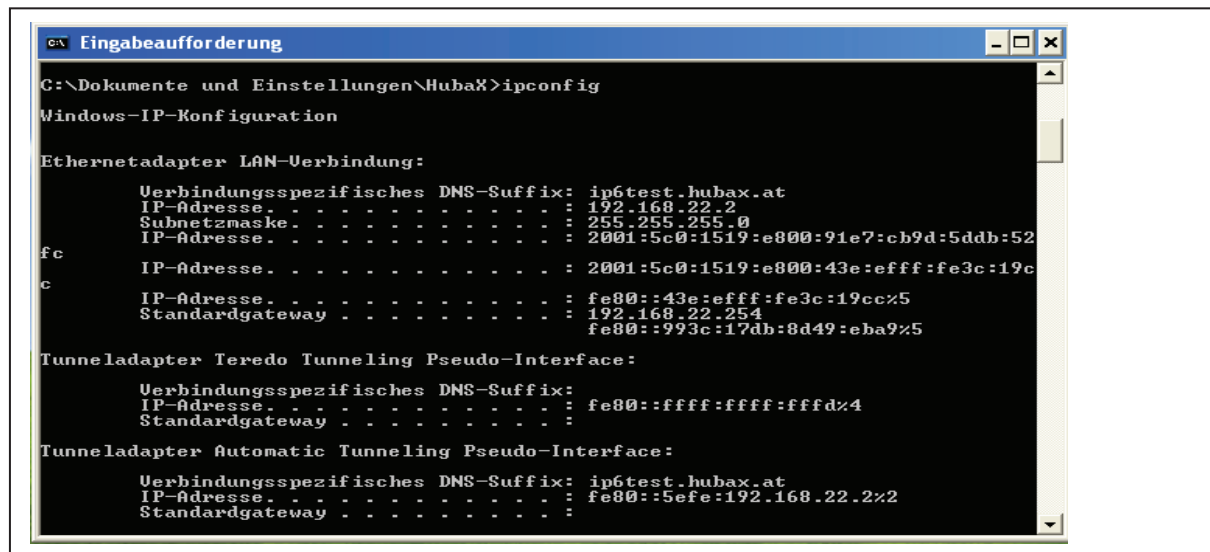


Abb. 60: Windows XP IPv6 Netzwerkkonfiguration

¹³ Windows XP IPv6 Konfiguration, <http://www.easy-network.de/ipv6-installieren.html>

Mittels Ping wird getestet, ob der Windows XP Client IPv6 fähig ist.

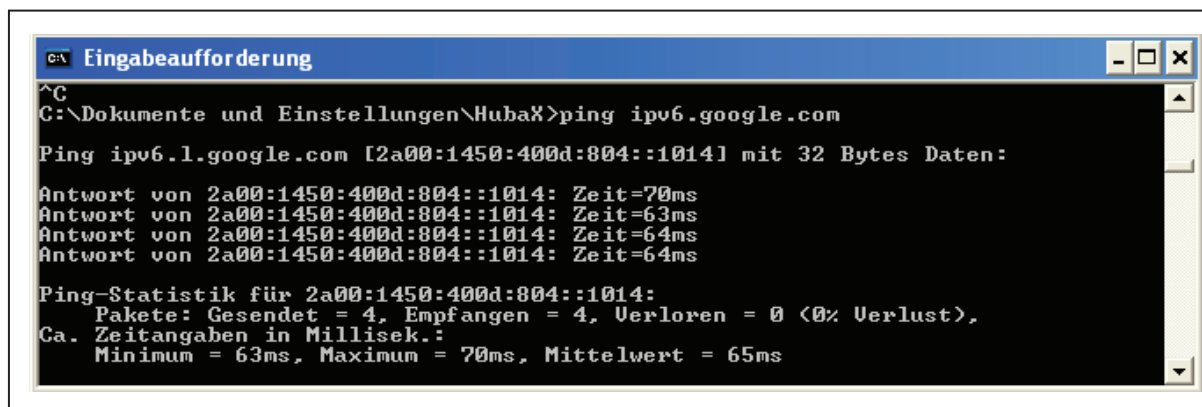


Abb. 61: IPv6 Fähigkeit testen

Windows XP hat keinen DHCPv6 Client, daher muss dieses Feature mittels externer Software nachgereicht werden. Hier wird die frei Software Dibbler¹⁴, die für Windows und Linux verfügbar ist, verwendet. Dibbler beinhaltet einen DHCPv6 Server, einen Client und ein Relais, welche zusammen oder einzeln installiert werden können.

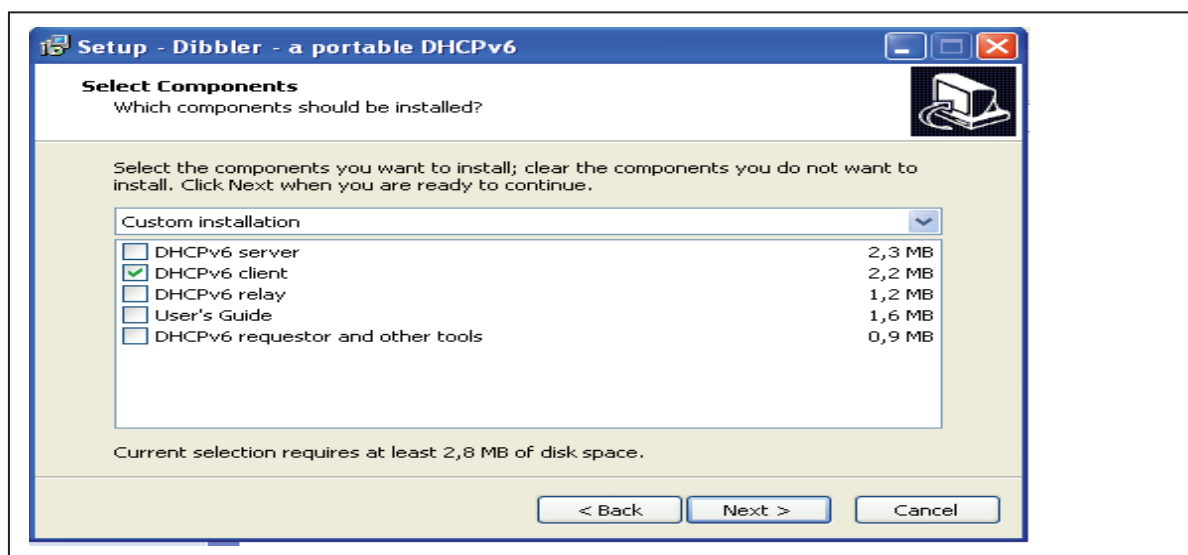


Abb. 62: Dibbler Installation

Die Konfigurationsdatei „client.conf“ im Installationsverzeichnis (Standardmäßig: C:\dibbler) beinhaltet die Konfiguration des Clients. In dieser Datei muss das Interface sowie die Optionen konfiguriert werden. Wir verwenden eine statefull Client Konfiguration auf dem Interface „LAN-Verbindung“ und fragen vom DHCPv6 Server die Optionen „dns-server“ und „domain“ ab.

¹⁴ Dibbler, <http://klub.com.pl/dhcpv6/>

Mit dem Befehl „dibber-client install“ wird ein Dienst für den DHCPv6 Client installiert, der mit dem Befehl „dibbler-client start“ gestartet werden kann. Wie aus dem Log zu sehen ist, hat der Client eine IPv6 Adresse, die DNS-Server und den Domainnamen vom Server erhalten. Diese sind nun auch in der Netzwerkkonfiguration über „ipconfig /all“ einzusehen.

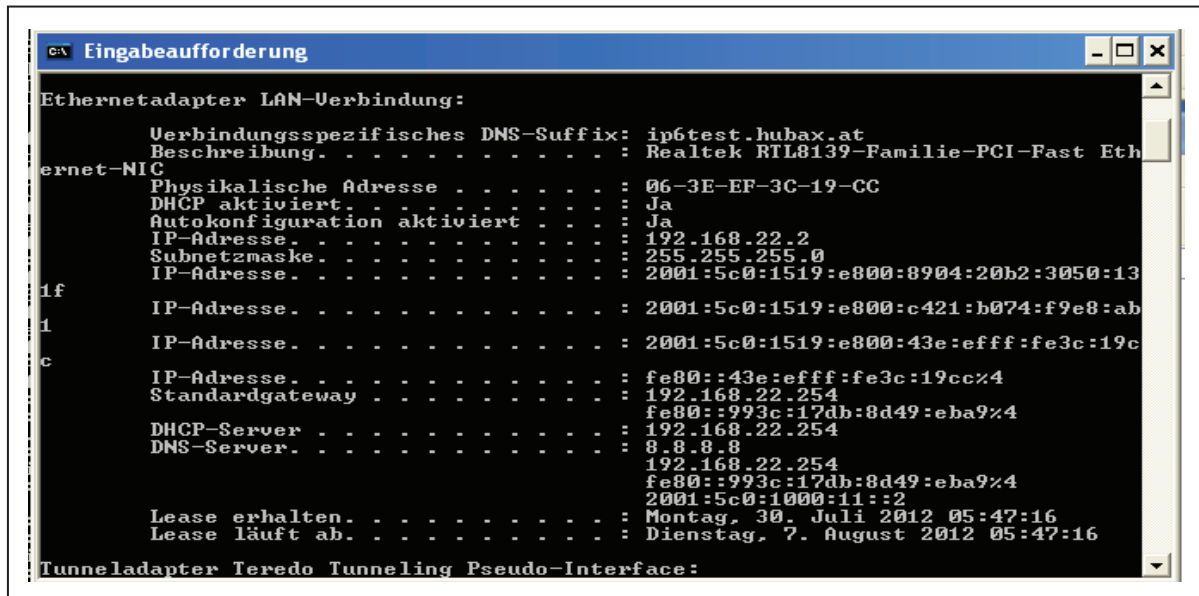


Abb. 65: aktuelle Netzwerkkonfiguration vom Windows XP Client

5 Ergebnisse / Diskussion

Die Umstellung eines Windows KMU Netzwerks auf IPv6 kann im Idealfall sehr schnell von statten gehen. Aktuelle Windows Version haben IPv6 implementiert und standardmäßig aktiviert.

Der Windows 2008 R2 Server bietet alle Funktionen, die in einem Netzwerk benötigt werden, sowohl für IPv4 als auch für IPv6. Hat man jedoch ältere Windows Versionen im Einsatz, wie Windows XP und Server 2003, kann die Umstellung komplizierter und kostenaufwändiger werden, da IPv6 Funktionen entweder durch zusätzliche Programme nachinstalliert werden müssen oder es muss sogar auf eine neue Version von Windows gewechselt werden.

In einem Netzwerk, das über Jahre gewachsen ist, kommen meist allerlei Versionen von Software und Hardware zum Einsatz. Es wird in realen Umgebungen Software und Hardware geben, die nicht mit IPv6 kompatibel sind und ausgetauscht werden müssen. Jedoch muss das nicht über sofort passieren. IPv6 bietet die Möglichkeit, IPv4 und IPv6 parallel zu betreiben und somit kann der Umstieg langsam vollzogen werden.

Sollten Teile des Netzwerkes nicht um IPv6 erweitert werden können und nicht ausgetauscht werden können, gibt es Tunnel und Gateways, die zwischen IPv4 und IPv6 vermitteln. Es sollte somit für jeden erdenklichen Fall eine Lösung zu finden sein.

6 Zusammenfassung

Die Einrichtung eines dualen Netzwerkes mit IPv4 und IPv6 ist mit dem Windows Server 2008 R2 kein Problem. Der Server kann dabei die Funktion des Routers, des DHCP Servers, des DNS Server und vieler weiterer Dienste übernehmen. Es ist jedoch auch möglich diese Services auf verschiedene Instanzen zu verteilen und mit Hardwarelösungen zu mischen.

Windows Clients ab Windows Vista werden standardmäßig mit IPv6 ausgeliefert und es sind praktisch keine Einstellungen auf ihnen nötig. Bei älteren Windows Clients kann es mit manchen Funktionen von IPv6 zu Problemen kommen. Jedoch können diese Funktionen durch externe Programme nachgerüstet werden und es ist nur ein kleiner Installationsaufwand zu beachten.

Der Dualbetrieb von IPv6 und IPv4 funktioniert ohne Probleme. Der Client wählt wenn möglich eine IPv6 Verbindung und verwendet, wenn diese nicht möglich ist eine IPv4 Verbindung. Serverseitig müssen einige Einstellungen doppelt gemacht werden. Andere Dienste ermöglichen eine gemeinsame Konfiguration von IPv6 und IPv4. Mit modernen Clients und Servern ist ein Dualbetrieb von IPv6 und IPv4 ohne großen Aufwand und Problemen möglich. Auch die Umstellung aus dem Dual Betrieb zu einem IPv6 Betrieb ist anschließend mit einigen Einstellungen vollbracht.

7 Verzeichnisse

7.1 Literaturverzeichnis

Boddenberg, Ulrich. *Windows Server 2008 R2: Das umfassende Handbuch. Inkl. Hyper-V*. Galileo Computing, 2009.

Microsoft. *Microsoft TechNet - Routing und RAS*. [http://technet.microsoft.com/de-de/library/cc731671\(v=ws.10\).aspx](http://technet.microsoft.com/de-de/library/cc731671(v=ws.10).aspx) (Zugriff am August 2012).

Jarzyna, Dirk. *IPv6 - Das Praxisbuch*. mitp, 2011.

Hagen, Silvia. *Planning for IPv6*. O'Reilly Media, 2011.

Freenet6. *Freenet6 Help Center*. <http://www.gogo6.com/freenet6/help-center> (Zugriff am August 2012).

Mrugalski, Tomasz. *Dibbler - a portable DHCPv6*. <http://klub.com.pl/dhcpv6/> (Zugriff am August 2012).

7.2 Abkürzungsverzeichnis

IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
KMU	Kleine und mittlere Unternehmen
IP	Internet Protocol
IT	Informationstechnik
NAT	Network Address Translation
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
MAC	Media-Access-Control
NDP	Neighbor Discovery Protocol
VM	Virtuelle Maschine

7.3 Abbildungen

Abb. 1: Netzwerkstruktur	14
Abb. 2: Rollen am Windows Server 2008 hinzufügen	15
Abb. 3: Serverrollen auswählen	15
Abb. 4: Routing und RAS aktivieren	16
Abb. 5: IPv4 DNS Einstellungen	16
Abb. 6: DHCP Konfiguration	17
Abb. 7: DHCPv6 Modus Konfiguration	17
Abb. 8: Routing und RAS Konfiguration	18
Abb. 9: NAT Konfiguration	18
Abb. 10: Öffentliche Schnittstelle wählen	19
Abb. 11: DHCP Konfiguration	19
Abb. 12: Radius Server Konfiguration	19
Abb. 13: IPv4 Pingtest	20
Abb. 14: IPv4 Traceroutetest	20
Abb. 15: Netzwerkverbindungsdetails	21
Abb. 16: gogoClient Anmeldung	23
Abb. 17: gogoClient Verbindungsstatus	23
Abb. 18: aktuelle Netzwerkkonfiguration am Windows Server 2008	24
Abb. 19: „gogoClient“ Verbindungsstatus	25
Abb. 20: „gogoClient Advanced Settings“	25
Abb. 21: Pingtest auf öffentlich IPv6 Schnittstelle des Windows Servers 2008 R2 ..	26
Abb. 22: Pingtest auf die interne IPv6 Schnittstelle des Windows Servers 2008 R2	26
Abb. 23: Windows Server 2008 R2 Netzwerkkonfiguration	27
Abb. 24: netsh Konfiguration der LAN Schnittstelle	28
Abb. 25: IPv6 LAN Routing aktivieren	28
Abb. 26: IPv6 Einstellungen im IPv6 Reiter	29
Abb. 27: Routingtabelle des Windows Servers 2008 R2	30
Abb. 28: Netzwerkkonfiguration der LAN Schniststelle	31
Abb. 29: Ping und nslookup vom Windows 7 Client	31
Abb. 30: Pingtest auf die LAN Schnittstelle des Windows 7 Clients	32
Abb. 31: Windows 7 Firewallregeln	32
Abb. 32: Firewallregel für beliebige Netze konfigurieren	33
Abb. 33: erfolgreicher Ping auf die LAN Schnittstelle des Windows 7 Clients	33
Abb. 34: IPv6 DNS Server hinzufügen	34
Abb. 35: DHCP Bereichsnamen vergeben	35
Abb. 36: Bereichspräfix einstellen	35
Abb. 37: Bereichsausschluss hinzufügen	36

Abb. 38: Leasedauer einstellen.....	36
Abb. 39: Netzwerkkonfiguration des Windows 7 Clients	37
Abb. 40: "nslookup" Test ipv6.google.com	37
Abb. 41: "nslookup" Test google.com.....	37
Abb. 42: DNS Server Konfiguration.....	38
Abb. 43: Forward Lookupzone erstellen.....	38
Abb. 44: Dynamische Updates nicht zulassen	39
Abb. 45: DNS Weiterleitungen	39
Abb. 46: DNS Einstellungen am DHCPv6 Server	40
Abb. 47: neuer Eintrag in der Domänensuchliste	40
Abb. 48: IPv6 Adresse für DNS Server Namensauflösung.....	41
Abb. 49: DNS Einstellungen am DHCPv4 Server	41
Abb. 50: neuer Eintrag in der Domänensuchliste	42
Abb. 51: IPv4 Adresse für DNS Server	42
Abb. 52: neuen Host am DNS Server anlegen.....	43
Abb. 53: Pingtest am Windows 7 Client	43
Abb. 54: IPv6 Adresse mit aktivierten "Randomized Identifiers"	44
Abb. 55: deaktivieren der Randomize Funktion.....	44
Abb. 56: aktuelle Netzwerkkonfiguration am Windows 7 Client.....	45
Abb. 57: Privacy Extension deaktivieren	46
Abb. 58: temporäre IPv6 Adresse nicht mehr vorhanden.....	46
Abb. 59: Windows XP Netzwerkkonfiguration	47
Abb. 60: Windows XP IPv6 Netzwerkkonfiguration	47
Abb. 61: IPv6 Fähigkeit testen	48
Abb. 62: Dibbler Installation	48
Abb. 63: Dibbler Konfigurationsdatei.....	49
Abb. 64: Dibbler Debugmeldungen	49
Abb. 65: aktuelle Netzwerkkonfiguration vom Windows XP Client	50