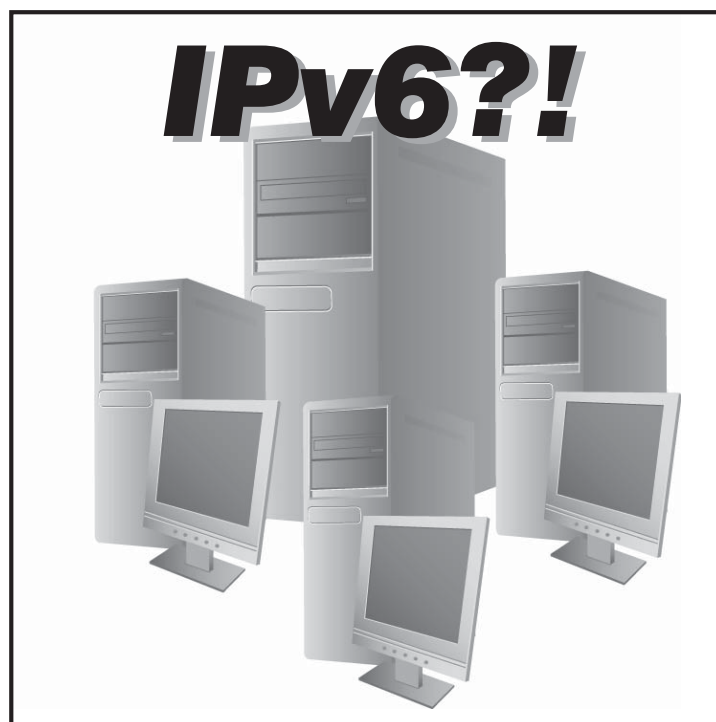


# Vorbereitung auf IPv6 - Erfolgsfaktoren und (erste) Praxiseinblicke

von Dipl.-Inform. Oliver Flüs



„Gestern noch“ wurde IPv6 gerne im Rahmen der Systemhärtung gezielt deaktiviert. Mittlerweile hört und liest man z.B. von Überlegungen, ob man nicht mit einem ohnehin anstehenden Wechsel auf Windows 7 „Nägel mit Köpfen“ machen und auch gleich auf IPv6 übergehen soll. Geht das so einfach, gar nebenbei?

Warnende Geleitworte, überblicksartige Artikel zu IPv6, zur Theorie der damit einhergehenden Neuerungen und zu grundsätzlichen Erwägungen, warum man wechseln sollte, hat es schon zahlreiche gegeben. Warum dann also „noch 'nen IPv6-Beitrag“? Es ist der Versuch, aus Diskussionen mit ComConsult-Kunden (z.B. auf Sonderveranstaltungen), sowie aus eigener Praxis aus dem ComConsult-Testla-

bor (siehe z.B. Windows 7), den eher abstrakten Einführungen erste Eindrücke aus dem praktischen Umgang mit IPv6 hinzuzufügen. Welche Fragen treiben erfahrenes, aber zu IPv6 noch unkundiges IT-Personal um? Worüber diskutiert man nach erster Berührung mit dem Thema, was für „Überraschungen“ erwarten einen?

weiter auf nächster Seite

## Schwerpunktthema

# Vorbereitung auf IPv6 - Erfolgsfaktoren und (erste) Praxis-einblicke

Fortsetzung von Seite 1



Dipl.-Inform. Oliver Flüs verfügt über langjährige Kenntnisse im Betrieb von IT-Infrastrukturen. Als Leiter des Competence Center IT-Service der ComConsult Beratung und Planung GmbH bearbeitet er seit Jahren Projekte in den Bereichen Services im IT-Bereich. Zu diesen Themengebieten ist er regelmäßig als Referent bei der ComConsult Akademie tätig, unter anderem als Schwerpunktreferent zu TCP/IP-Aspekten, in der Trouble Shooter-Seminarreihe sowie im Rahmen der Sicherheitsseminare

## Bereit für IPv6?

Oder Neudeutsch: bin ich, ist meine Umgebung „IPv6-ready“?

Hier gibt es Verschiedenes zu prüfen bzw. zu beachten, etwa:

- „Stimmt“ die Produktunterstützung für IPv6 bei Produktlinien, die man selbst einsetzt?

Um dies vorwegzunehmen, da kein Schwerpunkt des Artikels: gezielte Rechercheversuche im Frühjahr 2010 zeigten ein Bild, das auch bei Herstellern mit IPv6-Aktivität die Produktunterstützung Modell- bzw. Versions-abhängig war. Beispiel: neueste als Virtualisierungsbasis gedachte Produkte im Bereich von Appliances mussten bei IPv6 vorerst noch passen.

- Ist der IT-Betrieb „IPv6-ready“, d.h. ist das im Zeitalter von SLAs notwendiges Wissen für Planung und Betrieb von IPv6-Installationen gegeben?
- Insbesondere: Wie sieht bewusster Umgang mit IPv6 unter Sicherheitsgesichtspunkten aus?
- Wie müssen Adress- und Infrastruktur-Konzepte aussehen, um IPv6-Vorteile auszuschöpfen?

## Einarbeitung: auch das „Kleingedruckte“ lesen und nutzen ...

Der Aspekt der Adress- und Infrastrukturplanung wird in Artikeln naturgemäß häufig ausführlicher behandelt - eigentlich scheint alles gesagt?! Trotzdem ein Blick hierauf, konzentriert auf offenkundige Unterschiede zwischen dem Blickwinkel von Fachliteratur und den Eindrücken aus Gesprächen mit Planern und IT-Administratoren.

So wird über Nutzung und Nutzen registrierter IPv6-Adressen ausführlich geschrieben. Auf die (theoretische) Möglichkeit, selbst einen globalen Präfix zu beantragen, wird dabei auch hingewiesen, seltener jedoch darauf, dass die präferierte Praxis durchaus sein kann, dass der globale Präfix vom Internet-Provider „geleast“ wird. Warum denn das?

Nichts ist für die Ewigkeit, auch nicht der Providervertrag. Wechselt man den Internet-Zugang, taucht das eigene Netz an anderer Stelle im Verbund des Internet-Routing auf. Nähme man typisch den bislang genutzten Präfix mit, so risse dies jeweils ein Loch in den vom bisherigen Provider verwalteten Adressblock, der mitgenommene Teil seines Adressraums würde Routing-technisch zum neuen Provider wandern. Die Folge: durch jeden Providerwechsel neue „Einzelrouten“ - nichts wird es mit dem Ziel, lange IPv6-Präfixe für eine saubere Routing-Hierarchie, schlanke Routing-Tabellen zu nutzen und damit aus den Betriebserfahrungen mit IPv4 gelernt zu haben.

Natürlich wird man beim Provider-Wechsel seinen Präfix mitnehmen können, wenn man bereit ist, dafür zu zahlen. Es wäre aber keine Überraschung, wenn die interessanteren Preise mit dem Akzeptieren einer Adressmigration zu einem neuen Präfix, gestellt vom neuen Provider, angeboten werden sollten. Autsch - bei jedem Providerwechsel eine Adressmigration? Hier gibt es verschiedene Gesichtspunkte:

- Wie aufwändig ist eine Adressumstellung im Endgerätebereich?

Sofern man nichts an der internen Netzstruktur und dem Adresskonzept ändert, sondern nur die „elektronische Postleitzahl“ Präfix wechselt, hat man hier sowohl DHCP als auch - bei entsprechen-

der Entscheidung - Autoconfiguration als Helfer auf seiner Seite.

- Wie aufwändig ist die Umstellung der Routing-Punkte im eigenen Netz?

Hier spielt natürlich die Umgebungsgröße und Vermaschung des Netzes / Wegeredundanz eine Rolle, vor allem aber der Umfang eines Einsatzes von Sicherheits-motivierten Eingriffen (ACLs etc.). Ist die Router-Umstellung geschafft, geht in Autoconfiguration-Bereichen vieles „von selbst“ weiter.

- Adressumstellung im Bereich interner Dienste und Server?

Eigentlich dürfte man hier angesichts von Tendenzen in Richtung SOA gar nicht zucken - das Zusammensetzen von IT-Angeboten aus (wechselnden) Bausteinen in einem losen Verbund von Diensteservern muss entsprechende Mechanismen hergeben.

Das ist aber für viele noch Zukunftsmusik, viele arbeiten intern erfolgreich nach der Methode „ein Dienst - ein Server - mein Server!“ und finden die Aussicht auf häufigere Adresswechsel im Serverbereich wenig angenehm.

Aha - mit IPv6 wird es schwieriger, den Internet-Provider zu wechseln? Gegenfrage: Wieso war das bisher unter IPv4 denn einfacher? Wegen der Strategie zum Umgang mit (der Knappheit von) registrierten Adressen: vielfach wurde interne Kommunikation gar nicht mit registrierten Adressen realisiert, sondern mit „privaten“ IPv4-Adressen, bei Übergang zum Internet über Proxies etc. Natürlich soll an dieser Stelle kein Loblied auf NAT gesungen werden, die damit verbundene Problematik ist hinlänglich bekannt. Allerdings: es ist erstaunlich, wie überrascht häufig auf die In-

## Vorbereitung auf IPv6 - Erfolgsfaktoren und (erste) Praxiseinblicke

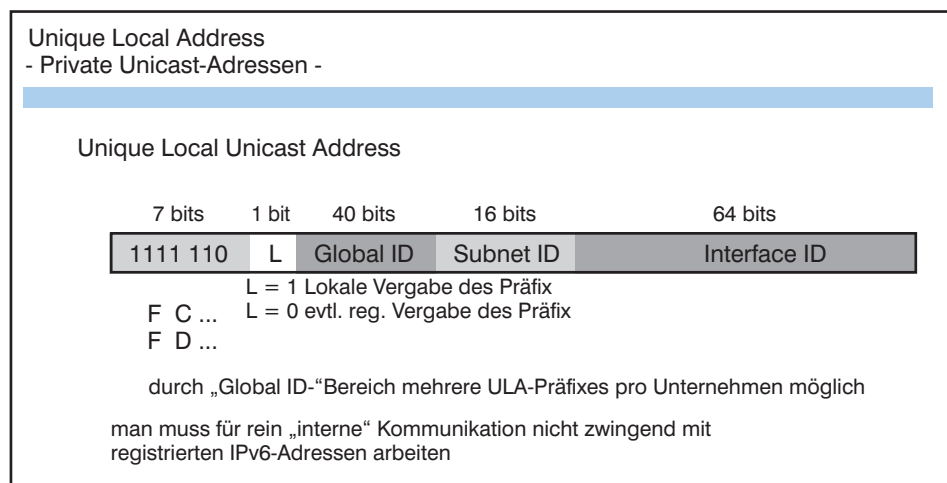


Abbildung 1: Option: Verwendung „privater“ Unique Local Adressen (ULAs)

formation reagiert wird, dass es auch unter IPv6 mit den Unique Local Adresses (ULA) Adressen „rein für den internen Gebrauch“ gibt, dabei (kurze „Standard-Präfixes“) mit geringerem Korsett-Effekt für die interne Netzstrukturierung. (siehe Abbildung 1)

Noch einmal, um nicht falsch verstanden zu werden: dies ist kein Plädoyer für den Einsatz „privater“ (ULA)-Adressen und NAT, aber: Wenn andere Möglichkeiten in der konkreten Situation zu unangenehm erscheinen, ohne dass man sich aus solchen Gründen fest an den „ersten“ Provider binden will, sollte man auch die Beibehaltung bislang aufgebauter und beherrschter Architekturen in die Überlegungen einbeziehen. Entsprechend als erster Tipp für die Vorbereitung auf IPv6: Beim Einarbeiten „gründlich lesen“, auch das Kleingedruckte, d.h. in Übersichtsartikeln nicht so oft Erwähnte - dann erst mit der Planung beginnen.

#### Adressverwaltung und betriebliche Erwägungen

Ein ähnliches Beispiel, wie man bei „klassischen“ IPv6-Diskussionsthemen die eigene Praxis berücksichtigen sollte, liefert die Betrachtung von Autoconfiguration und DHCP. Veröffentlichungen stellen hier die Varianten „IP-Adresse per Autoconfiguration“, DHCP zur Lieferung von Ergänzungsparametern“ und „DHCP im unter IPv4 etablierten vollen Umfang“ gegenüber.

Bei der (völlig richtigen) Diskussion wird dabei aber ein wichtiges Praxisargument kaum genannt: die Fehlerquelle „Mensch“ bei der Eingabe von Adressen/Adresspräfixes. Wer sich die Hexadezimalschreibweise von IPv6-Adressen das erste Mal anschaut, muss hier zwangsläufig zusam-

menzucken - die Möglichkeit, einen Tippfehler zu begehen und auch nicht sofort zu bemerken ist deutlich größer als unter IPv4. Das gilt sicher nicht nur für die komplette manuelle Festlegung der Zuteilung von IP-Adressen in einer Liste, die dann über DHCP verwaltet wird (unter IPv6 kaum diskutiert!), sondern auch für die Verwaltung von DHCP-Scopes. Auch hier ist wieder keine einseitige Empfehlung zugunsten einer bestimmten Strategie beabsichtigt, jedoch: völlig vergessen sollte man solche Überlegungen bei der Wahl zur Adressverwaltung auch nicht. Am besten bewertet man dies in Verbindung mit der konkreten Arbeits- und Trainings-Situation des zuständigen IT-Personals.

#### Eindrücke für Migrationsvorbereitung/ Administrator- und Fehlersuchealltag

Lesen bildet - aber reicht für die erfolgreiche Wahrnehmung von Administrations- und Betriebsaufgaben nicht aus. Zum Verstehen ist Literatur (auch die oft ungeliebten Handbücher, White Papers und RFCs) wichtig, bei Auswahl der zu vertiefenden Themen sowie zur sicheren Beherrschung hilft aber nur die Beschäftigung mit konkreten Produkten.

Dies beherzigend versucht ComConsult, sich bei entsprechender Produktverfügbarkeit möglichst bald eigene Einblicke zu verschaffen und eine eigene Meinung zu bilden, beginnend im Testlabor. Ein paar Beispiele werden im Folgenden zusammengestellt, ohne Anspruch auf Vollständigkeit, aber hoffentlich nicht nur für den Autor mit Aha-Wert.

#### Aspekt Ressourcenbedarf bei Netzkomponenten

Mit der Migrationsdiskussion zu IPv6 ist meist auch eine Diskussion der Auswir-

kung auf Ressourcenbedarf und Performance bei der Bearbeitung der neu organisierten Header verbunden. Das Thema ist wichtig, aber man muss die Kirche im Dorf lassen: Hier darf man zunächst keine Wunder erwarten, ehe nicht wie bei IPv4 das Grundgeschäft der Paketverarbeitung im Layer 3-Switch oder Router optimiert abläuft, sondern voll über die CPU der Komponente abgewickelt werden muss. Andererseits lohnt sich ein Blick auf die aktuelle Situation der eigenen Routing-Hops: Ein zentraler Layer 3-Switch, der zur Zeit mit IPv4 im Regelfall bei geringer CPU-Auslastung vor sich hindümpelt, wird auch den Übergang auf IPv6 im Parallelbetrieb mit IPv4 verkraften.

Allerdings: man darf nicht versäumen, das dünne Ende des Seils vorsorglich zu prüfen, bevor man sich darauf verlässt. Wie sieht es mit kleinen, für Nebenstandorte oder gar Heimarbeitsplätze verwendeten Routern aus? Hier kann schnell Handlungsbedarf bestehen - oder sogar eine Bremswirkung beim Start in IPv6. Ursprünglich mit Blick auf das Thema „Durchsatz“ sollte im ComConsult-Labor gezielt ein kleineres Router-Modell unter IPv6 verwendet werden, wie es unter IP4 gerne in kleinen Standorten als kombinierter LAN- und WAN-Übergang Verwendung findet. Erster Schritt: die IPv6-fähige Firmware besorgen und aufspielen. Hier warteten gleich zwei Überraschungen:

- Speicherbedarf für IPv6-fähige Firmware

Nach Sichtung der Hersteller-Veröffentlichungen zum Thema „welche Firmware-Version kann IPv6“ wurde das Basispaket der entsprechenden Firmware-Version für das fragliche Modell besorgt - und vorsorglich die Ressourcenausstattung des Routers mit den Angaben zur Firmware verglichen. Resultat: schade, zu wenig RAM!

Das mit der durchaus nicht uralten Firmware-Version unter IPv4 gut lauffähige Modell musste erst einmal mit zum Glück im Reparaturfundus vorhandenen RAM-Bausteinen aufgerüstet werden, dann konnte die neue Firmware überhaupt aufgespielt werden.

Nicht jeder hat aber für „ältere Schätzchen“ noch passendes RAM auf Lager liegen!

- Benötigte Firmware-Variante

RAM-Erweiterung vorgenommen, neue Firmware aufgespielt, stolz das Gerät in Betrieb genommen: nun konnte es losgehen!?! Als erstes also eine IPv6-

Vorbereitung auf IPv6 - Erfolgsfaktoren und (erste) Praxiseinblicke

Grundkonfiguration der Interfaces vornehmen, zumindest war das die Absicht - aber: Bei dem Versuch, eines der den Handbuchunterlagen entlockten Kommandos einzugeben, gab es nur Fehlermeldungen. Der Grund war ebenso einfach wie ärgerlich: die zur Bestimmung der benötigten Firmware zu Rate gezogene Unterlage war zwar vom Hersteller selbst, die Übersichtstabelle „welche Firmware kann was“ war zum Thema IPv6-Unterstützung auch korrekt gewesen. Was als kleine Detailinformation aber fehlte: Nicht das Basispaket dieser Firmware-Version bietet IPv6. Man muss vielmehr entweder ein speziell für Provider-Router gedachtes Paket verwenden, oder aber ein umfangreiches spezielles „Sicherheitspaket“. (Wie war das noch mit dem gründlichen Lesen und Recherchieren?!)

Die letztlich installierte erweiterte Version der Firmware funktionierte dann wie gewünscht. Allerdings war der Speicherplatz für Firmware mit diesem Paket vollständig ausgefüllt, d.h.: auf diesem Gerät mit dieser Speicherausstattung (alle Slots für Speicher voll besetzt!) waren typische Fall-back-Vorkerhungen wie das Vorhalten der aktuellen und der letzten zuvor verwendeten Firmware-Version nicht möglich!

Also: gerade die kleineren Geräte nicht vergessen, und deren Ressourcenbedarf für IPv6-Einführung auch im Sinne der etablierten Betriebsansätze (!) prüfen. Eventuell muss vor einer Migration erst investiert werden. (Wie es mit von Heim-arbeitsplatzanwendern selbst gestellten DSL-Routern und IPv6 zur Zeit aussieht, steht dann noch auf einem eigenen Blatt.)

**Aspekt Testen und Messen: Windows 7 und Adressen**

Nach Aufbau einer mit IPv6-fähigem Equipment (Router, Server, verschiedene Endgeräte) ausgestatteten Testumgebung erfolgten die ersten Tests. Erster Kandidat war Windows 7 als IPv6-Teilnehmer, z.B. zur messtechnischen Analyse, was bei Autoconfiguration im Detail konkret abläuft und in den Paketen zu sehen ist.

Erster positiver Eindruck: Anders als bei früheren Versuchen mit Windows Vista ist es zur Grundeinrichtung nicht mehr nötig, die Netsh-Kommandoumgebung („DOS“-Eingabefenster) zu bemühen (siehe Abbildung 2).

Eine der Stationen wurde unter Windows 7 für Autoconfiguration eingerichtet, die andere (eine Linux-Station) erhielt eine feste IPv6-Adresse „von Hand“ (siehe Abbildung 3).

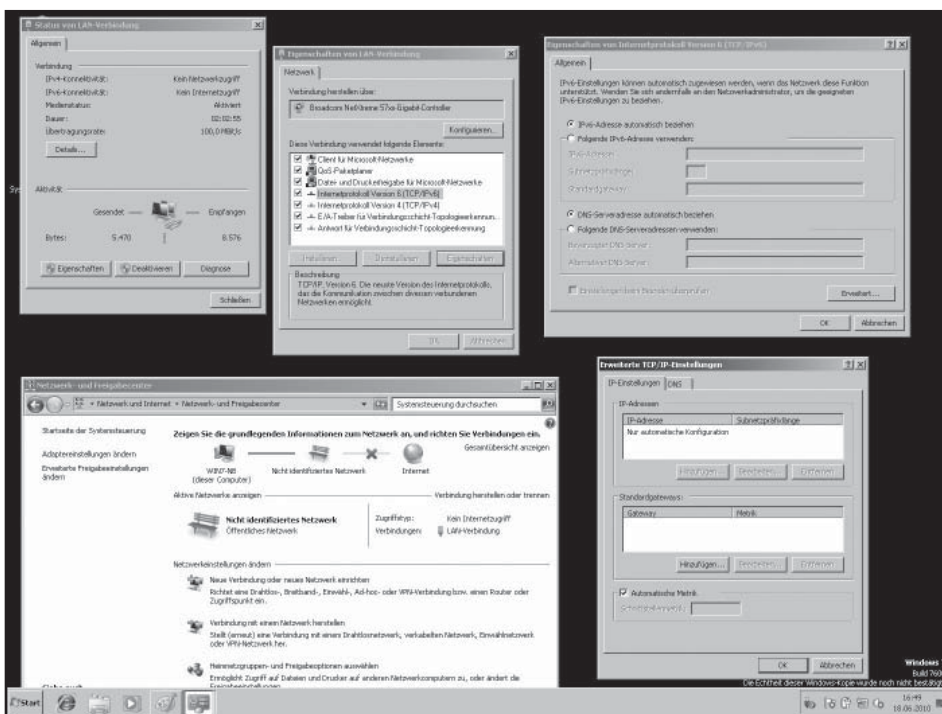


Abbildung 2: Windows 7: Einrichtung von IPv6-Grundkonfiguration über bekannt wirkende

Durchführen eines Pings zwischen den Stationen und Kontrolle des Ergebnisses wie in der Fehlersuche-Praxis gelernt stand als Nächstes auf dem Programm. Hier ist für viele ein erster Punkt des Um-

gewöhnens gegeben. Die altbekannten „Tools“ wie ipconfig, arp, route, netstat müssen erst probiert werden, um zu entdecken, welche Zustandsinformationen man auf welche Weise kontrollieren

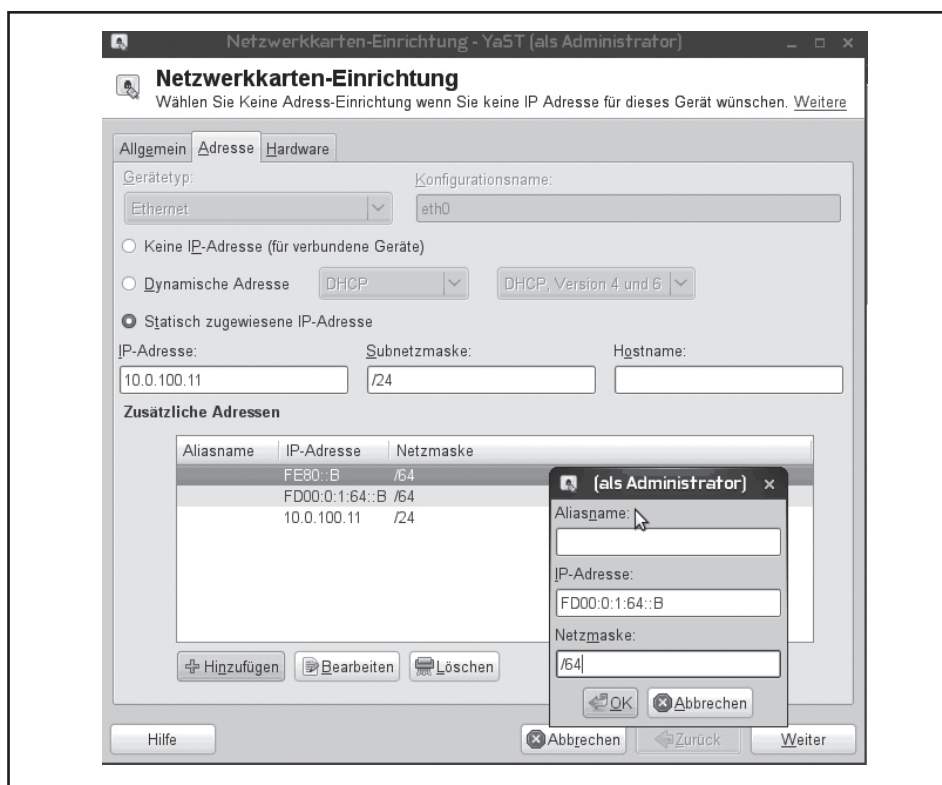


Abbildung 3: Einrichten einer festen IPv6-Adresse unter Linux

Vorbereitung auf IPv6 – Erfolgsfaktoren und (erste) Praxiseinblicke

kann. Hierbei rückt die zwar schon länger unter Windows verfügbare, aber bislang von vielen selten oder gar nicht verwendete „netsh“ mit IPv6 in den Vordergrund. Dies gilt insbesondere für das Abfragen der für volle IPv6-Funktionsfähigkeit, insbesondere den Sendevorgang unter IPv6 notwendigen, dynamisch gelernten Informationen. Statt langer Beschreibungen im Weiteren ein paar Eindrücke über Bildschirmanzeigen, die über das einfache „ipconfig /all“ hinausgehen.

Die auf einem Windows 7-Client wie von IPv4 bereits gewohnt geführte „Routing-Information“ (z.B. zur Verwaltung von Redirect-Informationen) lässt sich wie bei IPv4 z.B. über das route-Kommando abrufen (natürlich auch für parallel eingerichtete IPv4) (siehe Abbildung 4).

Als Quelle wird man richtig den mittels Neighbor Discovery-Mechanismus aufgebauten destination cache vermuten. Dieser umfasst allerdings noch mehr Detailinformationen. An diese kommt man dann typisch mittels netsh (siehe Abbildung 5).

Gleiches gilt für den neighbor cache (als Nachfolger der ARP-Tabelle), zum Beispiel zur Kontrolle der Sicht des Rechners auf die Erreichbarkeit der unmittelbaren Nachbarschaft (oder auch zur Entlarvung von Angreifern, die sich unberechtigt in dieser Umgebung eingenistet haben) (siehe Abbildung 6).

Nimmt man sich jetzt eine IPv6-fähige Analysatorsoftware zur Hand (im Beispiel: Wireshark), so kann man auch Paketabfolgen und -inhalte beim Ping betrachten und daran sein Wissen abklopfen und vertiefen (siehe Abbildung 7).

Im gezeigten Ablauf neu ist für einen IPv4-Kundigen neben den IPv6-Adressen im Wesentlichen die „Ablösung“ des ARP-Protokolls durch Neighbor solicitation und Neighbor advertisement, als spezielle ICMPv6-Nachrichten. Diese Pakete wurden im Beispiel „provziert“, indem der destination cache des Rechners zuvor mittels netsh (!) gelöscht wurde. Kleine Randnotiz: während reine Kontrollbefehle der netsh auch dem einfachen Anwender zur Verfügung stehen, benötigt man für das aktive Ändern (Löschen, Setzen von Einträgen) Administratorrechte – und muss diese auch bewusst nutzen. Ruft man, angemeldet als Administrator, die Eingabeaufforderung einfach wie unter Windows XP gewohnt auf, hat man im erscheinenden Fenster nur die für den Durchschnittsanwender verfügbaren Rechte und Möglichkeiten. Nur nach Aufruf des Eingabeaufforderungs-Fensters mit „Ausführen als

Administrator“ wird das Token des Administrators wirksam. (siehe Abbildung 8)

Dies ist kein IPv6-spezifisches Feature, sondern hat mit der User Account Cont-

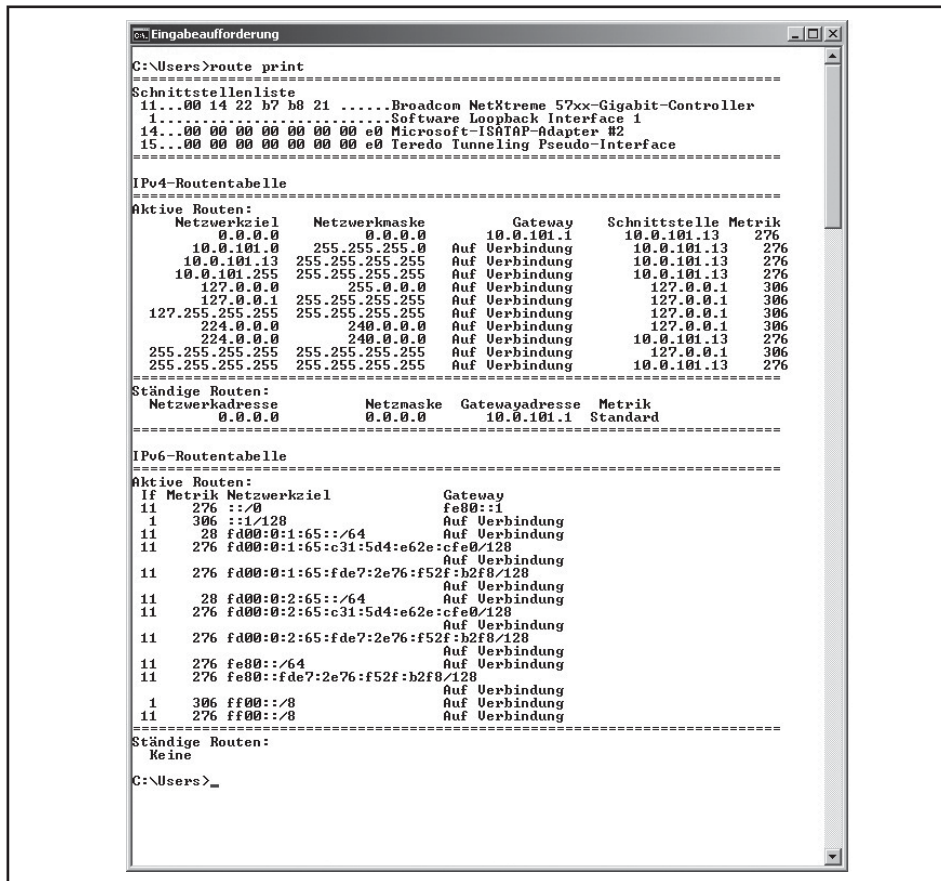


Abbildung 4: Abfrage von Windows 7-„next hop“-Informationen mittels route-Kommando

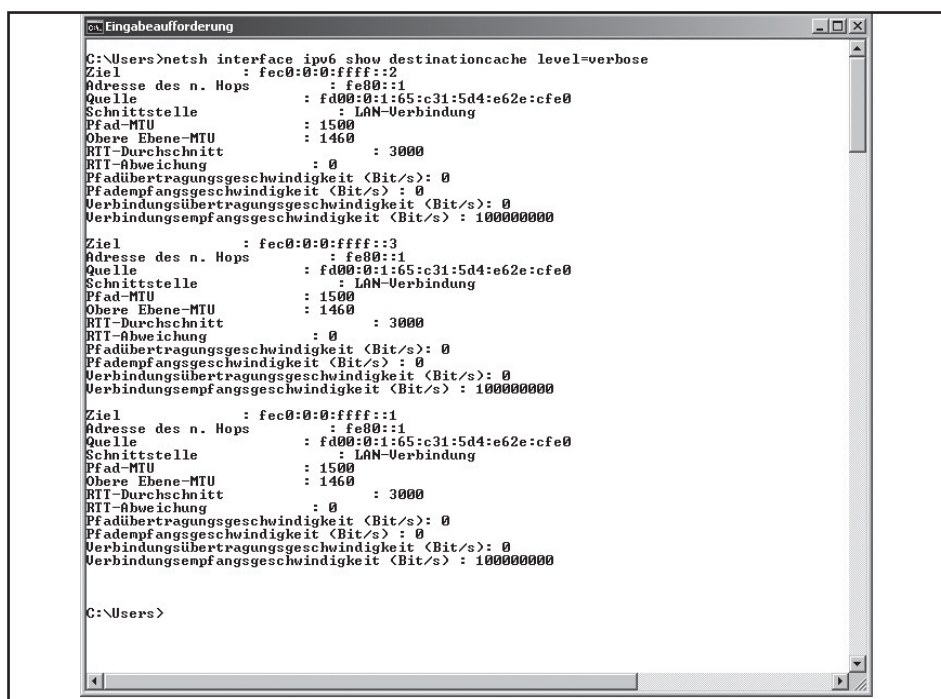


Abbildung 5: Auslesen des destination cache unter Windows 7 mittels netsh

Vorbereitung auf IPv6 – Erfolgsfaktoren und (erste) Praxiseinblicke

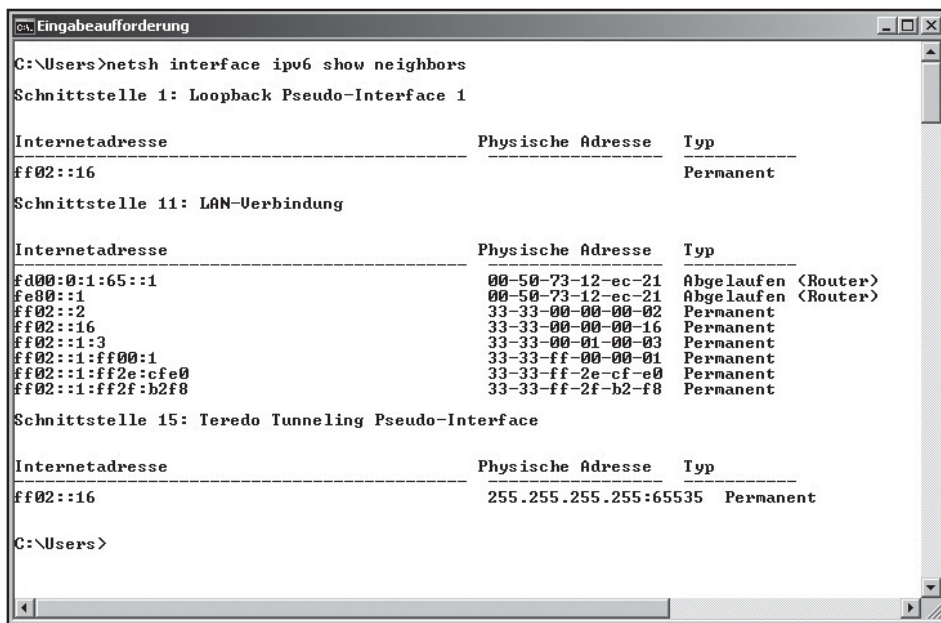


Abbildung 6: Auslesen des neighbor cache unter Windows 7 mittels netsh

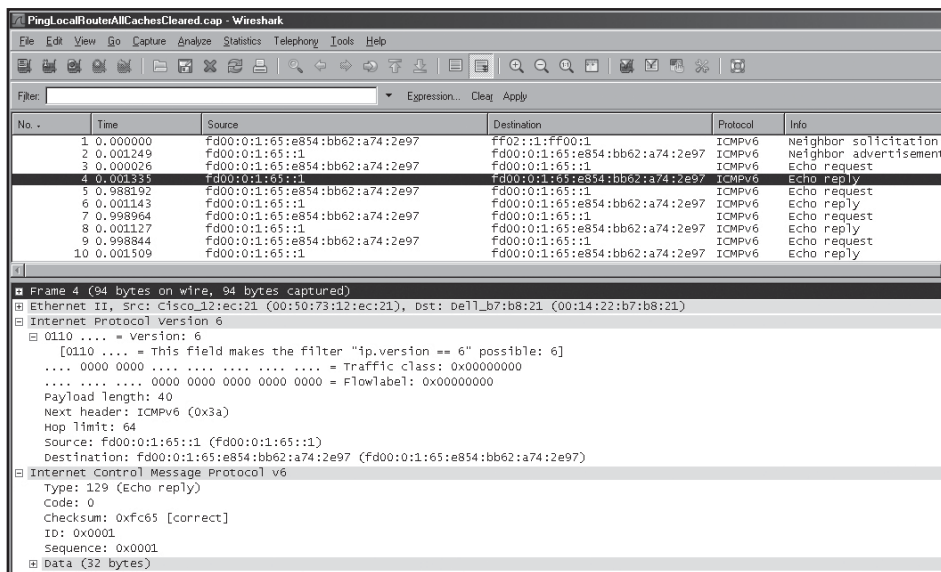


Abbildung 7: Beispiel: Paketabfolge bei ping unter IPv6

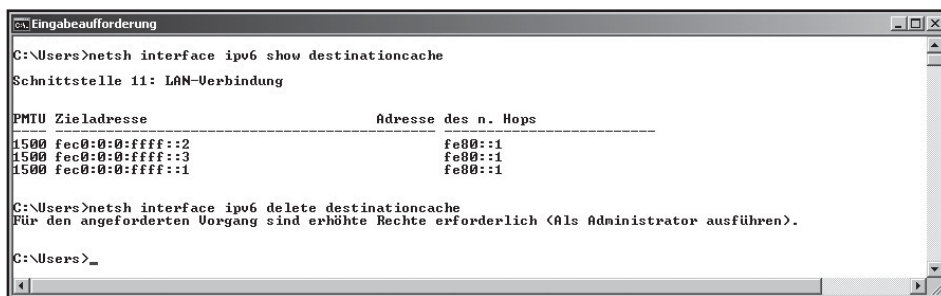


Abbildung 8: Fehlermeldung nach „Änderungsversuch“ mittels netsh ohne Administrator-Token

Na schön, man muss also seine Hausaufgaben machen und sich mit Einstell- und Kontrollmöglichkeiten vertraut machen. Das ist eine Fleißaufgabe, aber keine der angekündigten Überraschungen im Sinne von „Aha“-Effekten. Wo bleiben diese?

Nun, wer die Hausaufgaben macht, wird zumindest als gelernter Fehlersucher üben, typische Adressen und Adressaufbauten zu „lesen“. Erste einfache Fingerübung wäre hier z.B. das Wiedererkennen des EUI-64-Adressaufbaus beim Client mit Autoconfiguration-Adresse. Liest man hierzu noch mal nach, wie diese aussehen müsste, und schaut sich die oben angegebenen Beispiele genauer an, wird man feststellen: es ist nichts mit dem erwarteten Aufbau zu sehen. Wie kommt denn das?

Nun, Sicherheitsbeflissene haben in der häufig als Vorteil von IPv6 herausgestellten Möglichkeit zum Wiedererkennen des Teilnehmers (seiner Netzwerk-Karte) in der IPv6-Adresse eine Gefahr erspürt: Unabhängig vom Präfix der Umgebung, in der ein Gerät per Autoconfiguration arbeitsfähig wird, kann man auf die Identität des Geräts schließen. Bei mobilen Endgeräten heißt dies: hat man Zugriff auf die Information, welche Adressen wo aktiv genutzt werden/wurden (z.B. über DNS), kann man Bewegungsprofile für ein bestimmtes Gerät erstellen. Solche und ähnliche Überlegungen haben dazu geführt, die Option des Arbeitens mit „temporären Adressen“ zu entwickeln (siehe z.B. RFC4941). Windows 7 und Windows Server 2008 unterstützen bei Verwendung von Autoconfiguration solche temporären Adressen unter dem Parameter „privacy“, wobei dies im Default bei Windows Server 2008 deaktiviert ist, bei Windows 7 jedoch per Default aktiviert.

Was den Sicherheitsbeflissenen freuen mag, ist für den Betreiber einer Umgebung evtl. hinderlich. Wie der Name schon suggeriert, sind temporäre Adressen zeitlich begrenzt gültig, danach wird eine neue „Zufallsadresse“ errechnet. Bei wichtigen Stationen (z.B. Appliances auf Windows-Basis oder Geräte mit angeschlossener Sonderperipherie, die im Netz bereit gestellt werden soll), deren Verfügbarkeit man überwachen will, ist es wenig hilfreich, wenn diese regelmäßig die Identität wechseln. Auch der Sicherheitsplaner kann beim zweiten Hinsehen betroffen sein: wie will man mit wechselnden IP-Adressen eines Teilnehmers ACLs so gestalten, dass dieser Rechner Sonderbefugnisse erhält bzw. nur von bestimmten Partnern angesprochen werden darf?

rol unter Windows 7 zu tun. Hierauf sollte man allerdings grundsätzlich gefasst sein,

wenn man Kommandos / „Tools“ zu Administration und Fehlersuche startet.

Vorbereitung auf IPv6 - Erfolgsfaktoren und (erste) Praxiseinblicke

Man lernt: Detailfeatures und Defaults Kennen ist eine wichtige Hausaufgabe, und man muss sich a) eine eigene Meinung zum Nutzen in der eigenen Umgebung bilden und b) nötigenfalls wissen, wie man Einstellungen kontrolliert / den default abändert (temporäre Adressen unter Windows: auch hier ist wieder die netsh das Mittel)! (siehe Abbildung 9)

**(unerwünschte?) Tunnel funktionalitäten unter Windows**

Nächste Überraschung: Das Ping-Beispiel war mit den gezeigten Messungsinhalten noch nicht fertig. Das Messbild nach Anstoßen des ping stellt sich ausführlicher dar (siehe Abbildung 10).

Man sieht, dass nach erfolgreichem (!) Ausführen des ping der Windows-Cli-ent mit irgendwelchen Teredo-Aktivitäten beginnt. (Vor dem Ping war der Rechner minutenlang stumm, und weitere Kommandos/Aktivitäten wurden auf dem Gerät nicht durchgeführt.) Dieser Versuch, irgendwelche Anstalten zum Aufbau eines Teredo-Tunnels zu machen, ist gleich mehrfach seltsam:

1. Das Ping war doch erfolgreich!

Was soll also die Zusatzaktivität, als wäre ein Hilfstunnel nötig?

2. Microsoft selbst hat in der Vergangenheit Teredo als „Notangebot“ bezeichnet für Umgebungen und Fälle, in denen direkte IPv6-Kommunikation scheitert oder andere standardisierte Mechanismen wie 6to4/ ISATAP nicht verfügbar sind oder an Grenzen stoßen.

„Die Teredo-Technologie wurde lediglich als Ersatzlösung für IPv6-Konnektivität entwickelt. Wenn eine native IPv6, 6to4- oder ISATAP-Konnektivität zur Verfügung steht, arbeitet der Host nicht als Teredo-Client. Sobald mehr IPv4-NATS 6to4 unterstützen und IPv6-Netzwerke breitflächig verwendet werden, wird Teredo früher oder später nicht mehr benötigt werden.“

(aus: Microsoft-Artikel „Überblick zu Teredo“, veröffentlicht 05. März 2004)

Offenbar ist Teredo unter Windows 7 aber per Default aktiviert.

Im Testlaborbeispiel gab es keinen Server, der als Teredo-Tunnelträger hätte herhalten können, und die DNS-Auflösung in Richtung „microsoft.com“ ging auch ins Leere. In einer Produktivumgebung wären womöglich im Hintergrund ungewollt Teredo-Tunnel entstanden. Rückmeldungen

```
netsh interface ipv6>set privacy ?
Syntax: set privacy [[state=]enabled|disabled] [[maxdadattempts=]K<Ganze Zahl>]
[[maxvalidlifetime=]K<Ganze Zahl>]
[[maxpreferredlifetime=]K<Ganze Zahl>]
[[regeneratetime=]K<Ganze Zahl>]
[[maxrandotime=]K<Ganze Zahl>]
[[store=]active|persistent]

Parameter:
Tag      Wert
state    - Gibt an, ob temporäre Adressen aktiviert sind.
maxdadattempts - Mehrere Versuche zur Adressermittlung.
Der Standardwert ist 5.
maxvalidlifetime - Maximale Gültigkeitsdauer für
temporäre Adressen. Der Standardwert ist 7d
(sieben Tage).
maxpreferredlifetime - Maximal Gültigkeitsdauer in Sekunden, während
der temporäre Adressen bevorzugt werden. Der
Standardwert ist id (kein Tag).
regeneratetime - Zeit in Sekunden, bevor eine temporäre Adresse
verworfen und eine neue Adresse erstellt wird.
Der Standardwert ist 5s (fünf Sekunden).
maxrandotime - Obere Grenze, die zur Berechnung
eines Zufallswertes für die Verzögerungszeit
beim Starten verwendet wird. Der Standardwert
ist 10m (zehn Minuten).
store     - Einer der folgenden Werte:
active: Die Änderung besteht nur bis zum
nächsten Neustart.
persistent: Die Änderung ist beständig
(Standardwert).
```

Abbildung 9: Netsh-Optionen zum Umgang mit „privacy“ = temporären Adressen

aus Kundenumgebungen, wo man zufällig bei Tests auf solche Tunnel gestoßen ist, bestätigen diesen Verdacht. Wer Teredo nicht braucht, wird solche Tunnelautomatismen abschalten wollen (als Teil der Systemhärtung).

**IPv6 und Sicherheit - ein paar Streiflichter**

Wer die letzten Beispiele genauer liest, wird bemerken, dass wir mittendrin sind im Thema Security: temporäre Adressen zur Abwehr von Bewegungsprofil-Versuchen bzw. als Störenfriede bei ACL-Konfiguration, gezielte Systemhärtung, ...

Damit ist das Thema Sicherheit natürlich nur angekratzt. Weitere, bei Produktsichtung und Migrationsvorbereitung betrachtenwerte Aspekte kommen hinzu. Auch hier können an dieser Stelle nur Beispiele gegeben werden. Diese sollen ebenfalls zeigen, dass es wichtig ist, sich produktspezifisch vorzubereiten bzw. im Weiteren

auf dem Laufenden zu halten, sowie sich selbst ein Bild zu machen, wobei man wichtige Betriebsaspekte nicht übersehen darf.

• IPv6 und „ping sweep“

Mit ping sweep wird gerne der Vorgang bezeichnet, mittels ping Adressbereiche durchzuprobieren, um aktive vernetzte Geräte zu finden. Dies kann z.B. als erster Schritt eines Angreifers erfolgen, der zunächst aktive Ziele sucht, um diese dann mit Scanner-Software näher abzutasten, auf der Suche nach interessanten und mangelhaft geschützten Opfern.

Im Zusammenhang mit IPv6 wird nun darauf hingewiesen, dass wegen der erhöhten Adresslänge die Adressbereiche eigentlich zu groß werden, um ein solches Durchprobieren noch effizient erscheinen zu lassen. Es gibt sogar einen informational-RFC mit Tipps zur Gestaltung der Adresskonzeption derart, dass solches Durchtesten völlig uninteressant wird.

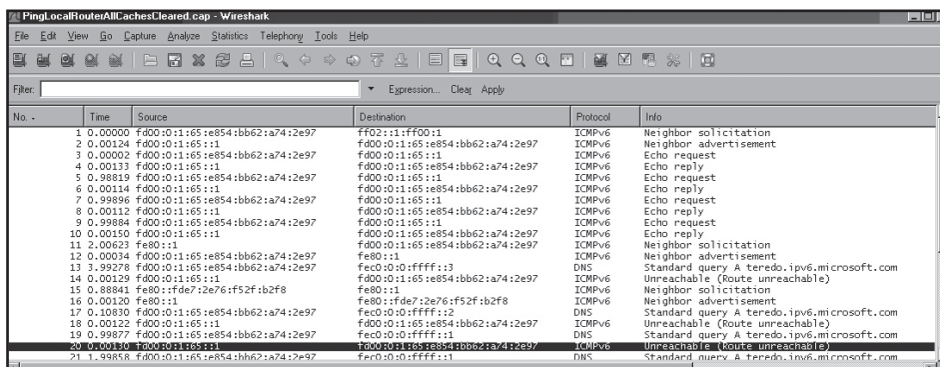


Abbildung 10: ping-Beispiel „ausführlich“

## Vorbereitung auf IPv6 - Erfolgsfaktoren und (erste) Praxiseinblicke

Also eigentlich eine schöne Änderung. Aber leider hat auch diese Rose Dornen: Management-Lösungen mit Autodiscovery-Funktion stützen sich ebenfalls mindestens als ein Standbein auf einen solchen ping sweep und werden somit wie ein Angreifer an dieser Stelle mit Einführung von IPv6 bei der Umgebungsdurchsuchung behindert.

Interessanterweise gibt es Tools, die gezielt im Zusammenhang mit IPv6-Unterstützung den ping sweep noch als Feature auflisten. Vorsicht: hier droht im schlimmsten Fall eine ungewollte DoS-Attacke auf das eigene Netz. Wird eine solche, in der Regel ressourcenstarke Netzmanagement-Lösung in diesem Sinne aktiv und probiert einen riesigen Adressvorrat durch, so wird sich dies für die Nutzkommunikation störend bemerkbar machen. ACLs oder Firewalls, die die entsprechenden ICMP-Pakete blocken, sind da nur bedingt ein Gegenmittel: Schon mit IPv4-basiertem ping sweep, der versehentlich über Standortgrenzen erfolgte und als work-around zunächst via Firewall geblockt werden sollte, ist es in Kundenumgebungen „gelingen“, die Firewall lahm zu legen.

- Auslesen von IPv6-caches statt ping sweep

Die Antwort auf den Wegfall des Nutzens von ping sweeps wird das konsequentere Auslesen dynamischer Informationen über den Umgebungszustand sein. Hier kommen die Caches unter IPv6 (neighbor und destination cache) natürlich „wie gerufen“ – dem Netzmanagement-Tool leider genauso wie einem Angreifer. Beide werden versuchen, z.B. über SNMP auf solche Cache-Informationen der Routing-Komponenten zuzugreifen. Was beim Netzmanagement gewollt ist, muss dem Angreifer verwehrt bleiben. Wer dies bis jetzt noch nicht getan hat, sollte daher intensiver über Maßnahmen wie SNMPv3 mit Authentication, zumindest aber „gute“ und häufig gewechselte SNMP-communities sowie die Beschränkung von Management-Agents und -zugriffen auf diese auf separate Management-Interfaces nachdenken.

- Angriffe auf Neighbor Discovery

Dynamisches Lernen durch vernetzte Geräte bedeutet immer auch Anfälligkeit gegen Täuschung durch manipulierte Informationen und Abfragen (Spoofing). Dies gilt unter IPv6 z.B. für den Neighbor Discovery-Ansatz. Die Tatsache, auf Authentication Header und ESP bei jeder IPv6-Implementierung zurückgreifen

zu können, hilft hier aus verschiedenen technischen Gründen leider nicht ideal.

Entsprechend wurde Secure Neighbor Discovery (RFC 3971) spezifiziert. Auch könnte das Pendel wieder zu DHCPv6 ausschlagen, das eine Authentication-Option mitbringt. Als Alternative zu SEND wurde in einem März 2010 erschienenen Draft (draft-jiang-v6ops-nc-protection-01.txt) außerdem ein Vorschlag gemacht, den Neighbor cache gegen Angriffe zu schützen, indem man ähnlich wie bei „Reverse DNS Lookups“ den Spieß herumdreht und die Neighbor-Discovery-Mechanismen benutzt, um die Authentizität von Informationen oder Zugriffen vorzuprüfen.

Hier wird man beobachten müssen, welche Produkte welche Idee umsetzen – und wann. Bis dahin kann man nur dazu raten, mit bereits ins Auge gefassten Aktivitäten zur Kontrolle des berechtigten Netzzugangs „am Port“ konsequent fortzufahren und diese nicht etwa mit Blick auf mögliche IPv6-Sicherheitsbeiträge erstmal einzufrieren.

Alle Beiträge in diesem Artikel waren nur Puzzle-Steinchen zu einem Gesamtbild, mit dem man sich vor und nach der Einführung von IPv6 beschäftigen muss. Sie haben aber hoffentlich dazu beitragen können, folgende Erkenntnisse zur Lage und zum Thema zu vermitteln:

- Man kann nicht früh genug anfangen, sich mit IPv6 zu beschäftigen: Die Einschätzung „Das bedeutet weit mehr als einfach die IP-Konfiguration austauschen“ stimmt.

- Man sollte sich bei der Einarbeitung nicht auf typisch diskutierte strategische Fragen / theoretische Grundlagen beschränken.

Gerade in der Anfangsphase sind Umfang und Details der Unterstützung stark produktspezifisch. Zum Teil muss man pro Gerätetyp / pro Software-Paket detailliert nachfragen oder testen. Wichtige Betriebsfragen wie manuelle Beherrschbarkeit, Sinn- oder Unsinn von Defaults in der eigenen Umgebung und der Nutzen von bekannten oder neuen Kommandos/Werkzeugen müssen mit geklärt werden.

- Zum Kennenlernen ist es diesmal besonders sinnvoll, über den Tellerrand hinauszuschauen.

Auch wer sonst nicht wie ein „Trouble Shooting-Profi“ arbeiten muss, hat über das Probieren mit Kommandos zur Zustandsprüfung sowie das Hineinschauen in einfache Analysatoraufzeichnungen (z.B. für ping) eine wertvolle Möglichkeit, sich Schritt für Schritt einzuarbeiten. Womöglich stößt man nur so auf Details, die einem sonst zunächst nicht ausdrücklich vorgestellt würden und an denen man entsprechend unfreiwillig erste Negativerfahrungen sammeln würde, die zu vermeiden gewesen wären.

- Bangemachen vor IPv6 gilt nicht, andere Migrationen vergleichbarer Komplexität waren auch erfolgreich - aber „mal eben nebenbei Migrieren“ bringt ziemlich sicher empfindliche Schrammen mit sich.

## Jetzt Leser werden

### Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.



Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:  
<http://www.comconsult-akademie.de/de/Registrierung.php>