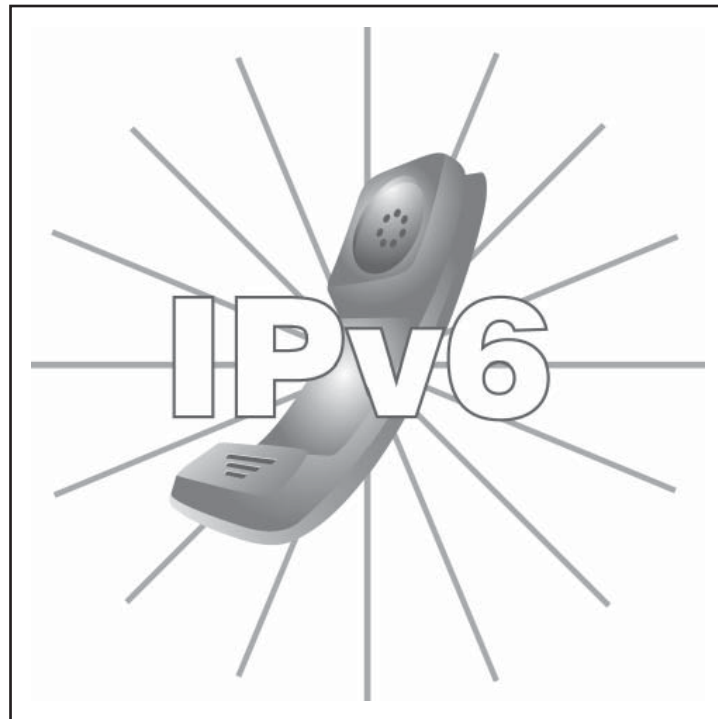


# Einstieg in IPv6 - (nicht nur) am Beispiel Adressplanung und „Direct Access“

von Dipl.-Inform. Dietlind Hübner, Dipl.-Inform. Oliver Flüs



Verschiedene Beiträge im Netzwerk Insider haben bereits darauf hingewiesen, dass es an der Zeit sei, sich mit IPv6 so bald wie möglich zu beschäftigen, um nicht plötzlich überrollt zu werden. Wieso auf einmal die Eile, mag der eine fragen. Sollen das erst mal die anderen Kollegen im IT-Bereich machen, ich habe dieses Jahr genug anderes zu tun, mag der andere denken.

So wird das im Falle von IPv6 nicht funkti-

onieren: Diesmal ist (noch mehr als sonst) koordiniertes und abgestimmtes Planen und Einführen angesagt, und dies auf Basis eines rechtzeitig aufgebauten Detailwissens mindestens für grundsätzliche Entscheidungen. Die Alternative: Der Einstieg wird eine Stolper-Tour, erste Versuche werden deutlich mühsamer als nötig, erste Schnellschüsse gehen deutlich am angestrebten Ziel vorbei oder beinhalten Fehler, die nur mühsam zu korrigieren

sind. Insbesondere geht bei IPv6 (fast) nichts ohne Einbindung der Betreiber von Netzinfrastruktur und Firewalls und zugehöriger Entscheidungen. Dies soll an zwei akuten Beispielen vorgeführt werden, der Adressplanung einerseits und der möglichen Einführung von Direct Access, einem Microsoft-Lösungsangebot, das völlig ohne IPv6 nicht nutzbar ist.

weiter auf nächster Seite

## Schwerpunktthema

# Einstieg in IPv6 - (nicht nur) am Beispiel Adressplanung und „Direct Access“

Fortsetzung von Seite 1



Dipl.-Inform. Dietlind Hübner ist seit mehr als 20 Jahren als Spezialistin für Netzwerk-Strukturierung, Netzwerk-Protokolle, Konnektivität und Netzwerk-Anwendungen tätig. Als Senior Consultant arbeitet sie regelmäßig in Projekten zu diesen Themenschwerpunkten mit und hat hierbei wesentliche Standard-Konzepte für Büro- und Industrieumgebungen erarbeitet sowie deren Umsetzung begleitet. Darüber hinaus gehören die Konzeption und Einsatzplanung von IT-Sicherheit und Neuerungen bei Netzwerkprotokollen, insbesondere IPv6, zu ihren thematischen Schwerpunkten.



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.

## Der IPv6-Router als Lotse auf dem Weg zur funktionierenden Konfiguration

Beschäftigt man sich mit der Einführung von IPv6, kommt man zumindest für den Endgerätebereich am Stichwort „auto-configuration“ kaum vorbei. Eine typische Entscheidungsmöglichkeit besteht hier darin,

- Adressen von Endgeräten, Druckern u.ä. im Access-Bereich angeschlossenen Geräten automatisch erzeugen zu lassen

(wer dies in früheren Insider-Artikeln oder anderer Literatur zu IPv6 genauer nachlesen will, kann über die Suche nach eben dem Begriff „autoconfiguration“ einsteigen)

und

- sich die übrigen zur vollen Arbeitsfähigkeit notwendigen Parameter (z.B. Name Server, NTP-Server, ...) wie unter IPv4 gewohnt mittels DHCP abzuholen.

Das Stichwort ist hier natürlich allgemein DHCP, in RFCs oder eng am RFC-Vokabular formulierter Literatur genauer „stateless DHCP“.

Na schön, dann entscheidet man sich

vielleicht genau für diesen Weg.

Wo ist das Problem, wieso ist da Teamarbeit, also abgestimmte Vorgehensweise und übergreifende Planung angesagt?

Die Konfigurationsverwaltung für den Endgerätebereich ist doch klar geregelt, Punkt - sobald im Netz überhaupt IPv6 transportiert wird, entscheidet der Endgerätebetreiber und der DHCP-Server-Betreiber, was er wie einstellt!? O.K., Autoconfiguration benötigt eine „Präfixliste“, d.h. eine Liste von „vorderen Teilen“ der IPv6-Adresse, die zu einem betrachteten IP-Subnetz gehört: die automatisch generierte Adresse wird dann dadurch erzeugt, dass an diesen „Netzvorspann“ ein für die Netzchnittstelle des Endgeräts eindeutiger „Interface Identifier“ angehängt wird. Der Präfix einer weltweit eindeutigen Adresse wird sich dabei aufteilen in einen weltweit eindeutigen Teil und den Teil, der das „Subnetz“ im eigenen Netzwerk identifiziert (Subnet Identifier), man kann also wie gewohnt sein Netz selbst flexibel strukturieren.

Der Interface Identifier andererseits kann z.B. nach fester Vorschrift aus der Ethernet-Adresse eines Geräts abgeleitet sein (Stichwort: modified EUI-64-Darstellung), oder man folgt den Sicherheits-Ideen von RFC 4941 („privacy extensions“) und lässt

den Identifier so erzeugen, dass das Endgerät weniger leicht an der IPv6-Adresse erkannt werden kann. Solange man die Konvention einhält, hierfür die IPv6-Adresse halbe-halbe aufzuteilen (64 Bit Präfix, 64 Bit Interface Identifier), kann jede RFC-konforme Variante der ID-Erzeugung verwendet werden. Die Wahl der Identifier-Form wird man sicherlich auf dem Endgerät als Teil der IPv6-Einrichtung festlegen. (siehe Abbildung 1)

Wer sich schon ein wenig in IPv6 eingelesen hat, wird denken „das habe ich auch schon genauer erläutert gesehen“. Alle werden denken: Und wo ist die Besonderheit/ Stolperfalle?

Die erste Besonderheit im Vergleich zu IPv4 ergibt sich bei der Frage, wo man bei Entscheidung zum Pärchen „automatisch konfigurierte Adresse + stateless DHCP“ diese Entscheidung konfiguriert.

Antwort: auf dem Subnetz-Router

- typische Quelle für eine Liste der in einem Subnetz funktionierenden Präfixes ist der Subnetz-Router
- typische Quelle für die Festlegung „DHCP liefert zusätzliche (andere) Parameter, außer der IP-Adresse“ ist ebenfalls der Subnetz-Router.

Einstieg in IPv6 - (nicht nur) am Beispiel Adressplanung und „Direct Access“

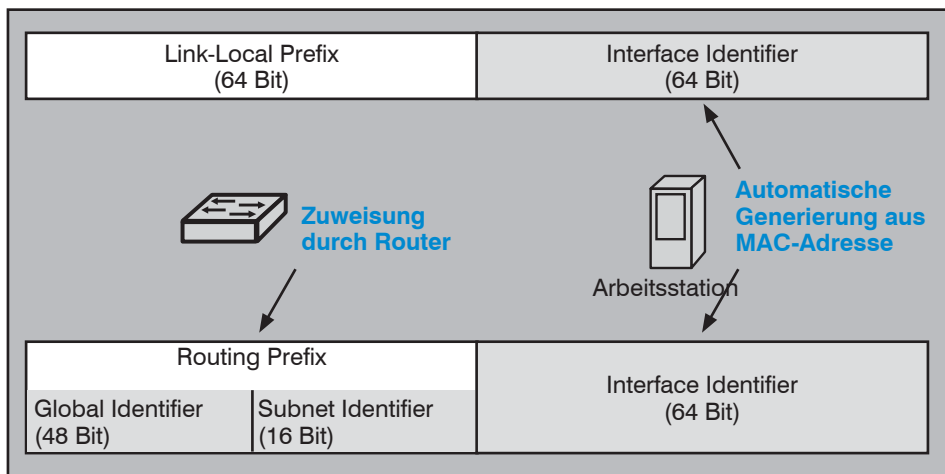


Abbildung 1: Zusammensetzung von IPv6-Adressen aus Präfix und Interface Identifier

Ist dieser entsprechend konfiguriert, so verteilt er (regelmäßig oder auf gezielte Anfrage, Suchwort zum Nachlesen: „router solicitation“) die entsprechenden Vorgaben in Form spezieller Pakete, so genannter Router Advertisements. (siehe Abbildung 2)

Auf dem Endgerät stellt man lediglich ein, dass dieses auch auf solchen Input vom

Router lauschen soll - der Rest wird auf dem Router konfiguriert (siehe Bild-Beispiel für den „testrouterbp“). Für die Routerkonfiguration ist aber der Netzbetreiber zuständig, d.h. die vom Endgerätebetreiber getroffene Betriebsentscheidung muss der Netzbetreiber umsetzen - Teamwork Punkt 1.

So ganz „nebenbei“ lässt sich im Router

Advertisement auch gleich über optionale Elemente („Prefix Information“) mitteilen, welche Präfixes für die automatische Adresserzeugung benutzt werden können. Hat man sich wegen der im Bild gezeigten Flags für Lauschen auf Advertisements entschieden, liegt es nur nahe, die Präfix-Information auch vom Router liefern zu lassen - zumal die Präfixes auf diesem ja ohnehin eingetragen werden müssen, damit er das Subnetz korrekt anbinden kann (warum also die Arbeit unnötig zweimal machen?). (siehe Abbildung 3)

Je nach Betriebssystem ist es auch möglich, solche Router-Funktionalität als „Dienst“ auf einem anderen Gerät zu simulieren. So kennt Linux z.B. einen Router-Advertisement-Daemon radvd, den man hierfür nutzen könnte. Hiermit könnte man sogar die im Advertisement zu schickenden Parameter auf dem zu vernetzenden Gerät selbst setzen, und dieses versorgt sich dann über die IPv6-Loopback-Schnittstelle selbst. Aber mal ehrlich - sich statt lokaler Hinterlegung einer funktionierenden, fertigen Konfiguration auf dem Gerät für automatische Konfiguration inkl. DHCP-Nutzung entscheiden, und dann mühselig solche Krückenlösungen bauen, die dann auch noch für jeden Gerätetyp anders aussehen können: das klingt doch nicht nur widersinnig ... Sollte man also auf die Mitwirkung des Routers und damit des Netzbetreibers an der Endgerätekonfiguration für IPv6 verzichten, dann nur ausnahmsweise, weil man dazu gezwungen ist.

Wer sich schon genauer zu IPv6 belesen hat, wird es wissen, die anderen werden es vielleicht ahnen: Der Subnetz-Router kann noch weitere Details mitteilen und so wichtige Mechanismen steuern. Dies birgt natürlich die Gefahr von neuen Angriffsformen durch „Vorgaukeln der Router-Rolle“ durch einen Angreifer. Entsprechend müssen auch die für IT-Sicherheit und die für ein funktionierendes Netz Zuständigen auf Grundlage eines gemeinsamen Kenntnisstands zusammenarbeiten. (Die Überraschung wird aber nicht ganz so groß sein!)

**Adressverschwendung auf reinen Transport-Strecken wegen Autoconfiguration?**

Natürlich muss und wird man bei Einführung von IPv6 auch ein IPv6-Adresskonzept festlegen müssen. Die Zuständigkeit hierfür wird vermutlich dort bleiben, wo sie in einer betrachteten Umgebung auch für IPv4 schon lag. Grundsätzliches hierzu wurde im Insider schon in früheren Artikeln gesagt,

```

4 0.000459 fe80::1 ff02::1 ICMPV
Frame 4: 150 bytes on wire (1200 bits), 150 bytes captured (1200 b
Ethernet II, Src: Cisco_12:ec:21 (00:50:73:12:ec:21), Dst: IPv6mca
Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1
Internet Control Message Protocol v6
  Type: 134 (Router advertisement)
  Code: 0
  Checksum: 0x77c0 [correct]
  Cur hop limit: 64
  Flags: 0x40
    0... .. = Not managed
    .1... .. = Other
    ..0... .. = Not Home Agent
    ...0 0... = Router preference: Medium
    .... .0.. = Not Proxied

testrouterbp(config-if)#ipv6 nd ?
dad                Duplicat Address Detection
managed-config-flag Hosts should use DHCP for address config
ns-interval        Set advertised NS retransmission interval
other-config-flag  Hosts should use DHCP for non-address config
prefix             Configure IPv6 Routing Prefix Advertisement
ra-interval        Set IPv6 Router Advertisement Interval
ra-lifetime        Set IPv6 Router Advertisement Lifetime
reachable-time     Set advertised reachability time
suppress-ra        Suppress IPv6 Router Advertisements

testrouterbp(config-if)#ipv6 nd other-config-flag
testrouterbp(config-if)#_
    
```

Abbildung 2: Anweisung zur autom. Konfiguration von Endgeräten o.Ä. über Router-Advertisement

Einstieg in IPv6 - (nicht nur) am Beispiel Adressplanung und „Direct Access“

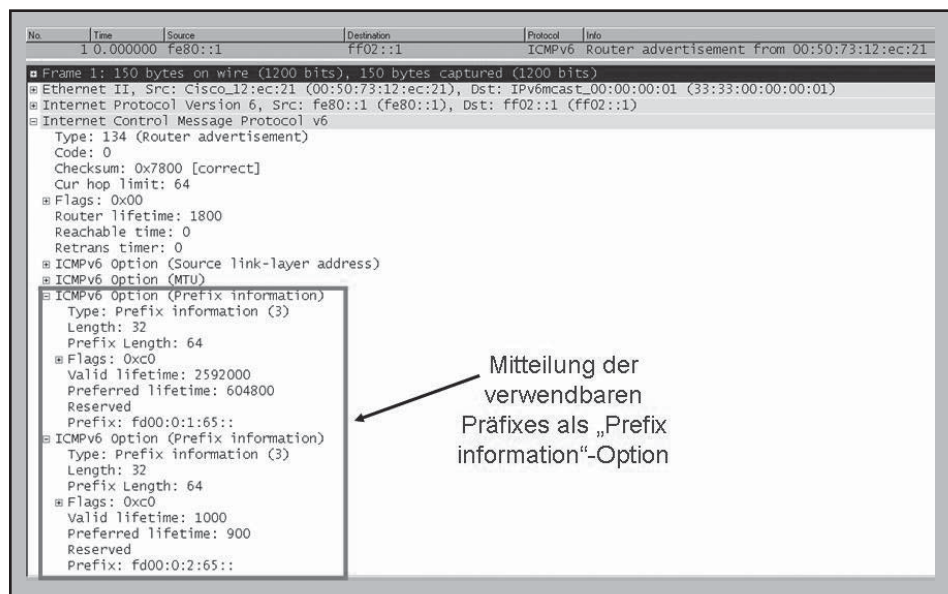


Abbildung 3: Beispiel Präfix-Information via Router-Advertisement

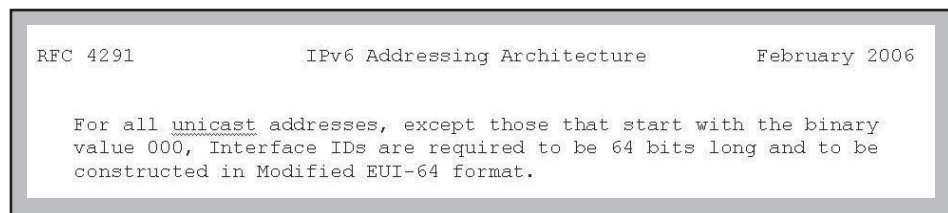


Abbildung 4: RFC 4291 bzgl. (Länge des) Interface Identifier

- im Zusammenhang mit der Vorstellung mit den unter IPv6 zur Verfügung stehenden Adresstypen (Stichworte zum Suchen/ Nachlesen z.B.: Globale Adressen, Unique Local Adressen/ ULA) und
- mit Hinweis auf mögliche Vorteile durch den deutlich größeren Adressvorrat.

Keine Sorge für die regelmäßigen Insider-Leser, der oben gelieferte grobe Kurzaussatz zu Konfigurationsautomatismen musste als Hintergrund für neue Mitglieder der Leserschaft sein, aber die grundsätzlichen Aussagen zur Adresskonzeption werden nicht auch noch wiederholt.

Allerdings zeigen Fragen und Diskussionen zur IPv6-Adresskonzeption, in Kundenprojekten genauso wie in Veranstaltungen der ComConsult Akademie, dass die im Kurzaussatz aufgeführten Punkte der Autoconfiguration-Idee auch Auswirkungen auf die Adresskonzeption haben. Die erste Idee des „EUI 64“-artigen Interface Identifier hat dazu geführt, dass alle per RFC für automatische Adresskonfiguration dargelegten Varianten stets die hinteren 64 Bit der IPv6-Adresse für den Identifier beanspruchen. Wer pannenfrei auch nachträglich auf automatische Konfiguration zurückgreifen können möchte, muss

sich bei der Netzstrukturierung im Adresskonzept via Präfix-Gestaltung auf die ersten 64 Bit beschränken. Im Prinzip macht das nichts, vergleicht man diese Manövriermasse mit der heutigen Lage unter IPv4. Gängige Subnetzgrößen wie 256 Adressen (4. Oktett für die Host-ID) oder 64 Adressen (für 48 Port-Switches mit der Idee „ein Switch = ein Subnetz“) führen unter IPv4 etwa bei der Verwendung einer Class A-Adresse zu einer Anzahl möglicher Subnetze, die man unter IPv6 mit 64 Bit-Präfixes auch erreicht, selbst wenn man einen größeren Teil des Präfix für einen weltweit eindeutigen „Global Identifier“ hernimmt.

Allerdings wird es in der Praxis Fälle geben, in denen man dennoch aus Prinzip zusammenschluckt, wenn man wegen einer pauschalen Festlegung „die hinteren 64 Bit sind für das Adresskonzept tabu“ massiv Adressen verschwenden muss. Das wohl typischste Beispiel dieser Art sind „Transport-Netze“, zum Beispiel zur direkten Verbindung zweier Standorte oder direkte Verbindungen von Layer 3-Switches verschiedener Strukturierungsebenen (z.B. „Core- und Distribution-Switch“ oder ähnliche begriffliche Rollenunterscheidungen in Netzkonzepten mit stärkerer Layer 3-Strukturierung).

Soll man bei solchen Transportnetzen, gar bei reinen Punkt-zu-Punkt-Verbindungen von Routern/ Layer 3-Switches, tatsächlich den Präfix bei Bit 64 enden lassen? Folgt man sklavisch dem RFC 4291 „IP Version 6 Addressing Architecture“, so muss man das tun, was in Abbildung 4 beschrieben ist.

RFC 4291 ist nicht „informational“, sondern gehört zum „standards track“, und Spielregeln der Standardisierung sollte man einhalten, wenn man Ärger vermeiden will, schon zur Vermeidung von Kompatibilitätsproblemen zwischen im Netz eingesetzten Produkten. Oder eben zur Wahlmöglichkeit zwischen verschiedenen Optionen, die ein Minimum an Gemeinsamkeiten aufweisen, hier eben die EUI 64-artigen Interface IDs und scheinbar willkürlich aussehende Alternativen gemäß der oben erwähnten „privacy extensions“ bei automatisch konfigurierten Adressen – alle solchen Adressformen haben sämtlich eine Präfixlänge von nicht mehr als 64 Bit, eben als einheitliche Basis für automatische Adresskonfiguration.

Also Fazit: Die Möglichkeit zur Betriebserleichterung für den Endgerätebetrieb über automatische Adresskonfiguration führt zu Verschwendungspflicht beim RFC-konform arbeitenden Adressplaner, und der Endgeräte-Verantwortliche muss dies auch stur so einfordern?!

Zum Glück nicht, aber das merkt nur, wer sehr genau liest:

- Würde man die zitierte Stelle aus RFC 4291 als Muss wörtlich nehmen, wäre auch der RFC zu „privacy extensions“ damit sinnlos.

Wer etwas genauer nachliest, wird feststellen, dass „modified EUI-64 format“ und die Umsetzung von Ideen aus dem privacy extensions-RFC sich widersprechen können. Microsoft führt z.B. mit den unter Windows 7 verfügbaren „temporären Adressen“ vor, wie man unter Umsetzung von privacy-extensions-Ideen zu einem Adressformat kommt, das mit modified EUI 64 aber auch gar nichts gemeinsam hat.

- In einem weiteren (informational) RFC 5375 „IPv6 Unicast Address Assignment Considerations“ wird für Transportverbindungen eine Präfixlänge von > 64 diskutiert und die Verwendung einer Präfixlänge von /112 für solche Fälle vorgeschlagen.

Das ist immer noch „Verschwendung“, aber zumindest nicht mehr ganz so schlimm wie /64 gemäß RFC 4291.

## Einstieg in IPv6 - (nicht nur) am Beispiel Adressplanung und „Direct Access“

Voraussetzung für ein Abweichen von der halbe-halbe-Aufteilung der IPv6-Adresse in Präfix und Identifier ist natürlich, dass man in entsprechenden Teilnetzen auf alle Mechanismen im Zusammenhang mit der Autoconfiguration verzichten kann. Folge: Während für dauerhaft reine Transportnetze eine solche Ausnahme möglich ist, wäre es bei Subnetzen, in denen nachträglich nicht vom Netzbetreiber administrierte Geräte angeschlossen werden könnten (z.B. zwecks Monitoring, als Proxies o.Ä.), eine mögliche Stolperfalle. Ehe ein Gerätebetreiber also ein erstes Gerät in ein Teilnetz einbringt, das er mit Autoconfiguration (egal welches Adressformat) betreiben will, sollte er sich nötigenfalls beim Netzbetreiber bzgl. der Präfixlänge(n) in diesem Teilnetz erkundigen.

Das wäre ja noch einfach, aber liest man RFC 5375 genauer und auch den darin referenzierten RFC 3627, so stellt man fest, dass der /112-Vorschlag eigentlich nicht wirklich begründet wird. Es werden nur aus der IPv4-Praxis naheliegendere Größen wie /127 als problematisch erläutert und die Hoffnung geäußert, dass mit /112-Präfixen keine Pannen passieren werden.

Was kann man aus diesem Ausflug in die Details zur IPv6-Adressverwaltung und IPv6-Adressplanung lernen?

1. Der Betrieb von Endgeräten und Netzkomponenten hängen in der IPv6-Praxis enger zusammen als unter IPv4.
2. Eine unabgestimmte Planung verschiedener IT-Spezialisten ist nachteiliger als unter IPv4, kann sogar zu Fehlschlägen oder vermeidbaren Pannen führen.
3. Eine Abstimmung zwischen den verschiedenen Spezialisten setzt zum Abstimmungszeitpunkt eine geeignete Schnittmenge des IPv6-Wissens voraus, und man muss für geeignete Kompromisse mehr „über den eigenen Tellerrand hinaus“ denken und wissen.
4. Mit einem kurzen „Schnellkurs IPv6“ in Form eines einführenden Artikels o.ä. ist es nicht getan. Will man erfolgreich sein und insbesondere unnötige Ungeschicklichkeiten vermeiden, muss auch das „Kleingedruckte“ und weiterführende Information berücksichtigt werden (produktspezifische Varianten kommen natürlich noch zusätzlich hinzu).

### Abgestimmtes Vorgehen heißt auch: eine sinnvolle Einstiegsreihenfolge finden

Bislang ging es mehr um Grundsätzlichkeiten, z.B. dem Zusammenwirken von Netzkomponenten und Endgerätekongfiguration zur Herstellung eines IPv6-fähigen Gerätezustands.

Die in der Betriebspraxis auch unter IPv4 bereits vielfach vorgekommene „Pannensituation“ ist aber doch: Es soll ein neues netzbasiertes Serviceangebot eingeführt werden und Netzbetreiber und „IT-Sicherheit“ erfahren als Letzte davon. Auf den Einstieg in IPv6 übertragen bedeutet dies: Es gibt konkrete Planungen zur Einführung einer IPv6-basierten Lösung, am besten schon mit festen Terminvorstellungen und der Betreiber einer noch nicht (durchgängig) auf IPv6-Unterstützung vorbereiteten Infrastruktur aus Netz- und Sicherheitskomponenten wird kurzfristig damit konfrontiert.

Das Resultat: eine Infrastrukturumstellung auf parallelen IPv4-/ IPv6-Betrieb im Wettkampftempo und

- Pannen sind wahrscheinlich,
- der Aufwand ist gegenüber einer abgestimmten Einführungsreihenfolge (ideal: zumindest im internen Netz inklusive Sicherheitsübergängen durchgängig konfigurierter Unterstützung von IPv6) unnötig erhöht,
- das neue Service-Angebot kann seinen vollen Wert womöglich zunächst nicht

entfalten und

- das Sicherheitsniveau kann vorübergehend sinken.

### Einstieg in IPv6 und Direct Access - wie am besten?

Ein erstes, akutes Beispiel ist Direct Access von Microsoft.

#### Motivation: Direct Access, IPv6 als notwendige Voraussetzung

Direct Access ist ein Lösungsangebot von Microsoft, verfügbar mit Windows 7/ Windows Server 2008 R2. Es ermöglicht für mobile Clients einen automatischen Verbindungsaufbau mit dem Unternehmensnetz, sobald Internet-Verbindung für einen Client besteht. Diesem werden auf diese Weise ohne Zutun des Anwenders interne IT-Ressourcen der Zielumgebung zugänglich gemacht.

Anders als bei herkömmlichen VPN- oder RAS-Lösungen ist die Berechtigung an den damit verbundenen Zugang zum internen Netz nicht an die Authentisierung des Anwenders (z.B. Login) geknüpft, sondern an eine Geräteauthentisierung. So besteht die Möglichkeit, zunächst die Kommunikation des mobilen Geräts auf bestimmte interne Ziele zu beschränken, von denen aus der sicherheitstechnisch angemessene Zustand (z.B. Aktualität von Sicherheitsupdates) automatisiert abgeprüft und nötigenfalls hergestellt werden kann, bevor der Anwender Zugriff zu den eigentlichen IT-Services erhält.

- Direct Access kann den Komfort für den

## 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>

## Einstieg in IPv6 - (nicht nur) am Beispiel Adressplanung und „Direct Access“

Anwender beim mobilen Endgeräte-Einsatz erhöhen (Wegfall manueller Initiierung des Verbindungsaufbaus zum internen Netz).

- Direct Access kann dazu genutzt werden, dass Gefährdungsrisiko durch mobile Clients für die internen IT-Installationen zu reduzieren.

Insofern kann Direct Access sowohl als verbessertes Service-Angebot an den Anwender genutzt werden, als auch als Basis zur Restrisiko-Reduzierung aus Security-Sicht. Dies sind gleich zwei schlagkräftige Argumente, die eine Einführung von Direct Access interessant und es damit verständlich machen, wenn eine zeitnahe Einführung erzwungen wird.

Was hat Direct Access nun mit der IPv6-Einführung zu tun?

**Direct Access setzt IPv6 als Kommunikationsbasis voraus, was einen Mindestanstieg in IPv6 als Voraussetzung zur Nutzung von Direct Access nötig macht.**

- Der Direct Access-Clients sendet ausschließlich IPv6-Traffic zum Direct Access-Server.
- Direct Access ist nur durch IPv6-fähige Client-Anwendungen nutzbar.
- Clients müssen zwecks Nutzung von Direct Access für IPv6 aktiviert und mit einer entsprechenden Konfiguration versehen werden.
- Direct Access-Server müssen für IPv6 aktiviert und konfiguriert werden.

Entsprechend ist beim Betreiber von Direct Access IPv6-Know-How gefordert.

Dieses muss sicherstellen, dass ein Direct Access-Client in unterschiedlichsten Gastumgebungen eine geeignete IPv6-Konfiguration erhält.

- Interne Dienste / Services, die über Direct Access (DA) genutzt werden sollen, müssen mindestens mittelbar über IPv6 erreichbar sein.

- Entweder ist die entsprechende Lösung IPv6-fähig, oder es wird z.B. ein Tunnelmechanismus benötigt, etwa ISATAP.

Es sollte in der Einsatzumgebung Know-How bzgl. Konfiguration und Betrieb (Entstörung) eines solchen Tunnelmechanismus gegeben sein, z.B. beim Betreiber des DA-Servers (dieser kann bei der Installation als

ISATAP-Router konfiguriert werden).

oder

- Die genutzten internen Services sind bereits IPv6-basiert installiert und direkt mittels IPv6 erreichbar.

Hier muss insbesondere auch zwingend beim Server- / Dienst- / Applikationsbetreiber IPv6-Know-How gegeben sein.

(Alternativen zur Realisierung der IPv4/IPv6-Konnektivität mittels NAT sind wegen derzeit mangelhafter Standardisierungsbasis von NAT für IPv6 bzgl. Zukunftssicherheit bedenklich.)

**Ein optimaler Nutzen von Direct Access hängt auch von Performance-Aspekten ab.**

**Optimum: IPv6 „Ende zu Ende“, zumindest ab dem DA-Server**

Optimale Performance wird erreicht, wenn auf IPv4-IPv6-Kopplungsmechanismen verzichtet werden kann, so dass die Paketbearbeitung an Tunnelenden oder ähnlichen Übergangspunkten entfällt. Soll zumindest ab Erreichen der eigenen Infrastruktur das Performance-Optimum angeboten werden, so setzt dies voraus:

- durchgängige IPv6-Unterstützung im eigenen Netz vom DA-Server zu den internen Servern
- IPv6-Fähigkeit der internen Server und der darauf zu nutzenden Dienste und Applikationen

Zur Schaffung dieser Voraussetzungen müssen

- Hard- und Software der Netzkomponenten und Server ausreichend sein sowie geeignete Software- bzw. Firmware-Versionen vorhanden sein,
- die betroffenen Netzkomponenten für IPv6 konfiguriert werden, geeignetes Adresskonzept und Betriebs-Know-How vorausgesetzt, und

- Server und Dienste/Applikationen mit IPv6-Unterstützung installiert und konfiguriert werden, geeignetes Betriebs-Know-How vorausgesetzt.

**Vermeidbare Hilfsmechanismen zum Transport von IPv6 über eine IPv4-(Teil-)Strecke sind für die Performance nicht förderlich.**

Wie bedeutsam ist aber dieser Punkt?

Man muss hier bedenken, dass die Lösung auf die Anbindung mobiler Rechner abzielt, die „von außerhalb“ mit internen Servern und Diensten kommunizieren. Die aus bisherigen VPN- und RAS-Angeboten bekannten Laufzeitaspekte sind also Erfahrungswerte, die anzuwenden sind.

Für den Kommunikationsweg vom mobilen Client zum Eintrittspunkt in das interne Netzwerk (DMZ mit Direct-Access-Server) kann dies nur bedingt vorausgesetzt werden, hier ist die IPv6-Unterstützung fremdbetriebener Strecken nicht erzwingbar.

Kann auch in der eigenen Umgebung eine durchgängige IPv6-Unterstützung durch die für Direct Access relevanten Geräte und Dienste/ Anwendungen und die Kommunikationswege zu diesen zunächst nicht gewährleistet werden, geht dies zu Lasten der Performance.

Zu den ohnehin bei Zugriffen von mobilen Clients zwangsläufig anfallenden Verzögerungen durch

- zu überwindende Entfernung,
- Zeitaufwand für Verschlüsselung / Entschlüsselung der Übertragung,
- Zeitaufwand für Prüfung auf Paketfiltern und Firewalls sowie
- evtl. nicht vermeidbare Engpass-Phänomene an WAN-Zugängen mit Bandbreitengefälle LAN-WAN

kommen

- Zeitaufwand für Einpacken/Auspacken der IPv6-Pakete an den Endpunkten des „Tunnels“ zur Übertragung von IPv6-Paketen im IPv4-Netz über einen neuen Tunnelmechanismus
- Zeitaufwand für Sicherheitsüberprüfungen durch Firewalls auf der „getunnelten“ Strecke.

Bei Antwortzeit-empfindlichen Applikationen und Diensten kann dies bis zu Abbrüchen führen, bei ungünstigem, nicht vermeidbarem Streckenverlauf im WAN-Bereich werden für den mobilen Anwender zumindest spürbare Leistungseinbußen möglich sein.

Hier ist insbesondere abzuwägen, inwieweit remote-Aktualisierung von Sicherheitsupdates u.Ä. unter solchen Gesichtspunkten stets zu einem geeigneten Ergebnis führt. Eventuell sind Vorkehrungen zu treffen, um nach Abbrüchen solcher Vorgänge den mobilen Client

## Einstieg in IPv6 - (nicht nur) am Beispiel Adressplanung und „Direct Access“

wieder in einen kontrollierten Zustand zurückführen zu können. Mindestens aber wird der betroffene mobile Anwender über besonders langes Warten bis zur Zugangsgewährung zu den für ihn interessanten Diensten und Daten nicht eben erfreut sein. Für ihn ist die Phase, in der sein Endgerät via Direct Access zunächst geprüft und nötigenfalls in einen Soll-Zustand gebracht wird, reine Wartezeit.

Es muss betont werden: Laufzeitbedingten Negativ-Effekte der beschriebenen Art für Applikations- und Dienstzugang via Direct Access und der mögliche Bumerang-Effekt bei der Nutzung von Direct Access aus Sicherheitserwägungen wären dabei nicht auf die Qualität der Implementierung von Direct Access zurückzuführen, sondern auf eine ungünstige Reihenfolge bei der Einführung des Pakets „IPv6 und Direct Access“ in der Zielumgebung.

Zumindest Direct-Access-Interessenten, die in der Vergangenheit bzgl. bestehender RAS- oder VPN-Zugangsmöglichkeiten zu Fine Tuning zwecks Behebung von Laufzeitproblemen gezwungen waren, sollten solche Überlegungen ernst nehmen und in ihre (Reihenfolge- und Test-)Planung einfließen lassen.

### Notwendige Mindestvorbereitungen im Firewall-Bereich bei Direct Access-Einführung

Wie dargestellt kann ein Einstieg auf IPv6 wegen Einführung von Direct Access über verschiedene Szenarien (mit oder ohne Tunnelnotwendigkeit in der Zielumgebungs-internen Infrastruktur) erfolgen.

In allen Fällen sind jedoch auf den eingesetzten Übergängen mit Sicherheitsfunktionalität (Paketfilter oder weitergehende Firewall-Funktionalität) notwendige Voraussetzungen zu schaffen:

#### 1. Firewall/Paketfilter zur Außenanbindung

Hier sind gezielte Freischaltungen für Kommunikation zwischen mobilen Clients mit Direct Access und dem in einer DMZ angebotenen Direct Access-Server notwendig, entweder direkt auf Basis von IPv6-Adressen auf Server und Client oder zur Unterstützung gemäß Sicherheitskonzept zulässiger Tunnel oder sonstiger Kopplungstechnik (z.B. auch IP-HTTPs). Je nach Tunnelvariante muss dieser Sicherheitsübergang insbesondere für bestimmte ICMPv6-Pakete „von außen nach innen“ durchlässig gemacht werden. Soll dies

ohne vermeidbare Sicherheitslücken erfolgen, sind entsprechende detaillierte Kenntnisse erforderlich.

#### 2. Firewall/ Paketfilter zwischen Direct-Access-Server und internen Servern

Hier sind gezielt Freischaltungen für Kommunikation zwischen Direct-Access-Server und internen Zielen notwendig, entweder für direkte IPv6-Kommunikation oder für Verwendung des Direct Access-Servers als Tunnel-Router. Im letzten Fall ist auch zu klären, inwieweit eine Prüfung der getunnelten Pakete vor Durchlassen zum internen Netz erfolgen kann und soll.

(Zu Details vergleiche man z.B. das Herstellerdokument „DirectAccess for Windows Server 2008 R2 - Design, Deployment, and Troubleshooting Guides“, Dezember 2009 / September 2010.) Beide Sicherheitsübergänge benötigen für die beschriebenen Einstellmöglichkeiten mindestens grundlegende IPv6-Unterstützung, die vorbereitend herbeizuführen ist.

Die insgesamt beschriebenen Details im Umfeld einer Direct Access-Einführung beleuchten, dass eine erfolgreiche Direct-Access-Nutzung bestimmte Mindestvoraussetzungen in der Kommunikationsinfrastruktur der Zielumgebung benötigt.

Mindestens für die Sicherheitsübergänge muss frühzeitig IPv6-Unterstützung hergestellt werden.

Sollen Performance-Nachteile wegen Tunnel- oder vergleichbaren Kopplungslösungen zwischen IPv4- und IPv6-Installationen vermieden werden, ist eine durchgängige Aktivierung von IPv6 parallel zu IPv4 auf allen Netzkomponenten zu empfehlen, sowie die IPv6-Aktivierung auf den für Direct Access-Clients zugänglich zu machenden internen Servern.

Die entsprechenden Vorarbeiten umfassen Aktivitäten der folgenden Art, die sich aus dem vorliegenden Artikel sowie im Detail auch aus früheren Insider-Beiträgen zu IPv6 begründen lassen:

- Bestandsaufnahme der Produktstände (Hard- und Software)
- Informationseinholung bei Herstellern bzgl. notwendiger Auf- bzw. Umrüstung betroffener Komponenten
- Know-How-Aufbau (produktspezifische Anteile z.B. über Proof-of-Concept-Tests)

- Weiterentwicklung aller IP-bezogenen Konzepte

- Durchführung notwendiger Auf- bzw. Umrüstungsarbeiten an der produktiven Infrastruktur im notwendigen Umfang

- Durchführung der notwendigen Konfigurationsarbeiten, auf Basis entsprechend aktualisierter Konzepte (Adresskonzept, Sicherheitskonzept, ...).

Auch dieser Artikel kann nur einen kleinen Beitrag auf dem Weg zu einer erfolgreichen Migration zu IPv6 leisten. Die beispielhaft diskutierten Planungs- und Betriebsaspekte stellen aber Themen dar, die in aktuellen Projekten und Kundenanfragen bei ComConsult eine wichtige Rolle spielen. Sie zeigen:

- Die Zeit der Beschäftigung mit IPv6 nur in der Theorie ist vorbei. Neben dem vielzitierten Ende des Vorrats an IPv4-Adressen und den hieraus resultierenden Forderungen nach Einführung von IPv6 im Internet klopfen erste Produktlösungen an die Tür, die IPv6 benötigen oder zumindest mit Hilfe von IPv6 eleganter und nützlicher verwendet werden können.

- Schon beim punktuellen Einstieg in IPv6 ist es wichtig, die Planung für IPv6 zur Infrastruktur (Netz, Sicherheitsfunktionalitäten, Verwaltung von Adressen und erweiterter IP-Konfiguration) nicht zu spät anzugehen und umzusetzen.

Eine IPv6-Einführung ist umso weniger schmerzhaft, je mehr sie im IT-Bereich als „Team-Aufgabe“ begriffen wird. Wer nicht über Service-Level oder Sicherheitsmanagement-Auflagen entsprechend zu arbeiten gewöhnt ist, den sollten unter IPv6 gegebene technische Wechselwirkungen und zu präferierende Betriebsformen dazu „motivieren“.

- Die Auswirkung eines Einstiegs in IPv6 ist nicht-trivial und eine Vorbereitung in Projektform ist empfehlenswert. Mindestens in komplexen Fällen ist ein übergreifendes Zusammenarbeiten erforderlich, um die notwendige Ressourcenkonzentration und koordinierte Vorgehensweise für die Zielumgebung zu gewährleisten.