Jülich Supercomputing Centre

IPv6 Privacy Extensions – Alptraum im Enterprise LAN

November 2011

Werner Anrath, Egon Grünter, Sabine Werner

Interner Bericht · FZJ-JSC-IB-2011-08

JÜLICH
FORSCHUNGSZENTRUM

FORSCHUNGSZENTRUM JÜLICH GmbH

Jülich Supercomputing Centre

D-52425 Jülich, Tel. (02461) 61-6402

Interner Bericht

IPv6 Privacy Extensions – Alptraum im Enterprise LAN

Werner Anrath, Egon Grünter, Sabine Werner

FZJ-JSC-IB-2011-08

November 2011

(letzte Änderung: 21.11.2011)

Inhalt

IPv6 Status 2011 - Überblick

Im Jahr 1995 wurde von der Internet Engineering Task Force (IETF) IPv6 als Nachfolgetechnik des allgegenwärtigen IPv4-Protokolls ausgewählt.

Durch die Knappheit der IPv4-Adressen und die Zuweisung der letzten freien IPv4 Adressblöcke durch die Internet Assigned Numbers Authority (IANA) im Frühjahr 2011 hat das IPv6-Protokoll an Bedeutung gewonnen. Seit 2006 bietet der Verein zur Förderung eines Deutschen Forschungsnetzes (DFN Verein) den angeschlossenen Einrichtungen im Wissenschaftsnetz (X-WiN) *native* IPv6-Regelbetrieb an. Verliefen diese Vorbereitungen seitens der Provider und die Einführung von IPv6 in den Transportnetzen eher unbemerkt, änderte sich die Situation in den lokalen Netzen zunehmend. Seit der Einführung von Windows Vista und den Windows-Server-Plattformen im Jahr 2007 ist das IPv6-Protokoll im LAN installiert und aktiv. Mit der stark anwachsenden Verbreitung von mobilen Geräten, die IPv6 fähig sind, begann in der Öffentlichkeit und unter Datenschutzexperten eine intensive Diskussion um die Methoden zur Bestimmung der IPv6 Interface Identifier. Die Bedenken der Datenschützer zielen auf die aus der weltweit eindeutigen 48 Bit Ethernet Hardware (IEEE) abgeleiteten EUI-64 Interface Identifiern. Hier wird bemängelt, dass damit eine weitere Möglichkeit besteht, diese Interface Kennung als Personal Identifier zum User Tracking einzusetzen.

Die Internet Engineering Task Force hat im Jahr 2003 mit dem RFC 3041 ‚Privacy Extensions for Stateless Address Autoconfiguration in IPv6' die Verwendung von Pseudozufallszahlen als Interface Identifier in den Standard aufgenommen. Die Windows-Betriebssysteme sowie die jüngste Generation der Apple-Betriebssysteme generieren solche Interface Identifier. Im RFC 4941 , Privacy Extensions for Stateless Address Autoconfiguration in IPv6' wurde der 2003 eingeführte Standard nochmals aufgearbeitet.

Bei der Abwägung, welche IPv6-Technik zur Erzeugung der Interface Identifier im Enterprise LAN eingesetzt werden soll, liefern die genannten RFCs eine ausführliche Erörterung. Die dort vorgestellten Argumente sollen in diesem Dokument technisch präzisiert werden. Die ausgewählten Beispiele in den folgenden Abschnitten sprechen für einen Einsatz der EUI-64 Interface Identifier. Diese werden im Dokument RFC 4291 ‚IP Version 6 Addressing Architecture' beschrieben.

Dual Stack Implementierungen

Mit der Ablösung der Windows XP Systeme durch Windows 7 wird aktuell die Verbreitung des IPv6-Protokolls gesteigert. Neben den Microsoft Betriebssystemen nutzen auch die bekannten LINUX-Varianten und Mac OS X das neue IPv6-Protokoll parallel zum etablierten IPv4-Protokoll. Wesentlich ist dabei, dass dieses neue Protokoll in den unterschiedlichen Betriebssystemen installiert und standardmäßig aktiviert ist, so dass die Systeme im Dual-Stack-Betrieb (siehe Abbildung 1) am Netzwerk kommunizieren.

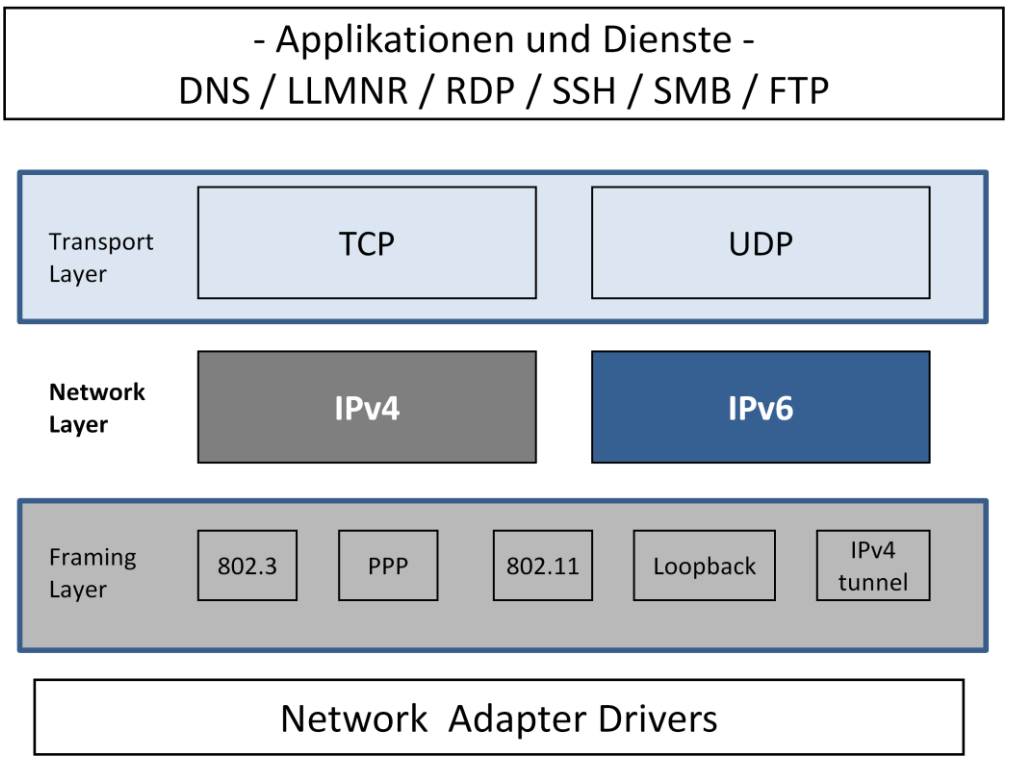

Abbildung 1: IPv6 - Dual Stack Implementierung

Die folgende Übersicht zeigt die Standardeinstellungen in aktuellen Betriebssystemen:

Windows Vista / 7 / 2008

- **IPv6 ist installiert und aktiv**
- Stateless Address Autoconfiguration aktiv (RFC[1] 2462 / RFC 4862)
- IPv6 Stack: zahlreiche Verbesserungen (Dual Layer)
- GUI, CLI and GPO[2] Konfiguration
- Integrated Internet Protocol security (IPsec) verfügbar
- Privacy Extensions[3] (RFC 3041 /RFC 4941) aktiv
- Domain Name System (DNS) Unterstützung
- Source and Destination Address Selection (RFC 3484)
- DHCPv6 Client aktiv
- Link-Local Multicast Name Resolution (LLMNR)
- Transition Technologies (Tunnel) aktiv
- **Windows Firewall ist IPv6 fähig, Stateful Inspection**

[1] Request for Comments
[2] Group Policy Object – Windows Active Directory
[3] Pseudozufallszahlen als IPv6 Interface Identifier

Linux

- **IPv6 ist installiert und aktiv**
- Stateless Address Autoconfiguration aktiv (RFC 2462 / RFC 4862)
- GUI und CLI Konfiguration möglich
- Privacy Extensions (RFC 3041 / RFC 4941) optional
- Domain Name System (DNS) Unterstützung
- Source and Destination Address Selection (RFC 3484)
- DHCPv6 Client optional
- Multicast DNS
- Transition Technologies (Miredo) optional
- **Firewall: ip6tables, Stateful Inspection ab Kernel 2.6.20**

Mac OS X

- **IPv6 installiert und aktiv**
- Stateless Address Autoconfiguration (RFC2462 / RFC 4862)
- GUI und CLI Konfiguration möglich
- Privacy Extensions (RFC 3041 / RFC 4941) optional
- ab 10.7 Privacy Extensions aktiv
- Source and Destination Address Selection (RFC3484)
    - Administrative Schnittstelle nicht vorhanden
- DHCPv6 ab 10.7
- Multicast DNS Unterstützung
- Transition Technology (6to4) optional
- **Firewall: ip6fw – kein Konfigurationsmenu - Standardeinstellung: *accept***

Die iOS-Versionen für das Apple iPhone und iPad haben im Auslieferungszustand das IPv6- Protokoll aktiviert. Die Android-Smartphones werden ebenfalls so vorkonfiguriert ausgeliefert. Es existieren keine administrativen Schnittstellen, mit der die IPv6-Konfiguration durch den Anwender verändert werden kann.

Interface Identifier

Um die nötigen Interface Identifier ohne administrativen Zusatzaufwand automatisch erzeugen zu können, sind im IPv6-Protokoll derzeit zwei Methoden vorgesehen. Im Fall der sogenannten EUI-64 Interface Identifier wird aus der 48 Bit MAC Adresse der Ethernet-Schnittstelle der entsprechende Wert generiert – dazu ein Beispiel: aus der MAC-Adresse (48 Bit)

00:15:77:96:74:bc

wird durch Einfügen von **ff:fe** zwischen Hersteller- und Board-ID

00:15:77:**ff:fe**:96:74:bc

und invertieren des **U/L-Bit**[4] entsprechend dem IEEE EUI-64 Standard

0**2**:15:77:ff:fe:96:74:bc

die IPv6 Link Local Address

fe80:: 215:77ff:fe96:74bc

und in Verbindung mit einem Netzwerk-Prefix wie z.B. 2001:db8:4711:2011::/64 ergibt sich die IPv6 Global Unicast Address

2001:db8:4711:2011:215:77ff:fe96:74bc

Das gesetzte U/L-Bit in einer EUI-64 konformen IPv6-Adresse zeigt an, dass der Interface Identifier aus einer schon global eindeutigen Kennung (nämlich der 48 Bit MAC-Adresse) abgeleitet wurde. Werden Pseudozufallszahlen als Interface Identifier verwendet, wird das U/L-Bit in der IPv6-Adresse nicht gesetzt. Letztlich erfolgt also eine Invertierung dieses Bits bei der Bildung des EUI-64 Interface-Identifiers aus der 48 Bit MAC-Adresse.

Im Fall der sogenannten Randomized Identifiers beschreibt erstmalig der RFC 3041 einen iterativen Algorithmus zur Erzeugung von Pseudozufallszahlen und deren Verwendung als 64 Bit Interface Identifier. Wichtig ist, dass das U/L-Bit gelöscht wird. Die Adressen, gebildet aus Prefix und Randomized Interface Identifier, werden Temporary Address oder Random Address genannt. Eine Random Address hat eine längere Lebensdauer und kann dynamisch im DNS registriert werden; das ist eine Besonderheit der Microsoft-Betriebssysteme.

Der Erzeugungsprozess ist wie folgt:

- ein vorhandener bisheriger Wert (IID Historie) und die EUI-64 Adresse werden verknüpft
- dann wird mit Hilfe des MD5-Algorithmus ein 128 Bit Wert erzeugt
- die niederwertigen 64 Bit werden als IID Historie gespeichert
- dann wird das U/L Bit in den höherwertigen 64 Bits auf 0 gesetzt
- der IPv6 Interface Identifier ist damit generiert

[4] Universal/Local Bit (IEEE Standard)

Die Gültigkeit einer IPv6-Adresse ist zeitlich begrenzt und die Nutzung erfolgt abhängig vom Status:

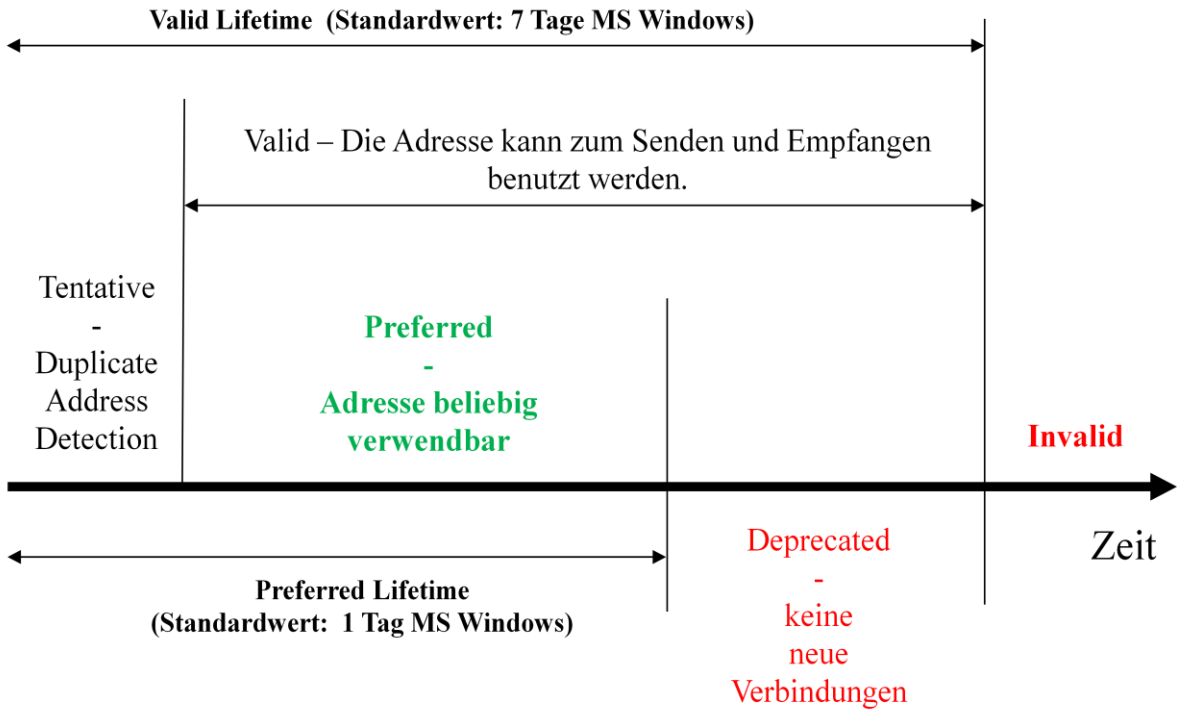

Abbildung 2: Address Lifetime

Die in der Abbildung genannten Werte sind Voreinstellungen. Eine Anpassung der Timer durch Prefix-Optionen im Router Advertisement ist möglich.

Für die nachfolgend in der Tabelle genannten Betriebssysteme zeigen sich im Auslieferungszustand unterschiedliche Methoden zur Bestimmung der Interface-Identifier (IID) bei der Initialisierung der IPv6-Module im Kernel und der späteren Stateless Address Autoconfiguration (SLAAC):

IPv6 Interface Identifier	Link-Local Random	Link-Local EUI-64	Global Unicast Addr Random	Global Unicast Addr Temporary	Global Unicast Addr EUI-64
Windows XP	-	+	-	+	+
Windows 7	+	-	+	+	-
Windows 2008	+	-	+	-	-
Windows 8 Beta	+	-	+	+	-
Mac OS 10.6	-	+	-	-	+
Mac OS 10.7	-	+	-	+	+
openSUSE 11.3	-	+	-	-	+
openSUSE 11.4	-	+	-	-	+
openSUSE 12.1	-	+	-	+	+
Debian 6.0	-	+	-	-	+
Android 2.3	-	+	-	-	+
iPad 4.3	-	+	-	+	-
iPhone 4.3	-	+	-	+	-
ubuntu 11.10	-	+	-	-	+

Eine Vereinheitlichung auf EUI-64 Interface IDs ist zu favorisieren, weil die aus Pseudozufallszahlen (RFC 3041 ‚Privacy Extensions for Stateless Address Autoconfiguration') gebildeten Interface Identifier Diagnosearbeiten behindern und verschiedene Netzwerkmanagement-Aufgaben erschweren:

- Verbindungsabbrüche
- DNS Betrieb
- Access Control List
- Forensik

Zur Deaktivierung der Privacy Extensions sind bei Windows 7/8 Preview/Vista/2008 als Administrator folgende Befehle auszuführen:

```
netsh interface ipv6 set privacy state=disabled  store=persistent
netsh interface ipv6 set global  randomizeidentifiers=disabled  store=persistent
```

und Neustart

Ab Mac OS X 10.7 sind Privacy Extensions aktiv und können wie folgt abgeschaltet werden. Die Datei /etc/sysctl.conf muss dazu folgende Zeile enthalten:

```
net.inet6.ip6.use_tempaddr=0
```

und Neustart

Ab openSUSE 12.1 sind Privacy Extensions ebenfalls aktiv und können durch einen Eintrag in Datei /etc/sysctl.conf abgeschaltet werden (Reboot nötig). Die Abbildung 3 zeigt den Eintrag in /etc/sysctl.conf und zur Kontrolle die Adressen:

```
linux-121:~ #
linux-121:~ # tail -1 /etc/sysctl.conf
net.ipv6.conf.eth0.use_tempaddr = 0
linux-121:~ #
linux-121:~ # ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0C:29:EB:BF:0C
          inet addr:192.168.178.38  Bcast:192.168.178.255  Mask:255.255.255.0
          inet6 addr: 2001:470:1f0a:1c1f:20c:29ff:feeb:bf0c/64 Scope:Global
          inet6 addr: fe80::20c:29ff:feeb:bf0c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1332 errors:0 dropped:0 overruns:0 frame:0
          TX packets:194 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:388104 (379.0 Kb)  TX bytes:22207 (21.6 Kb)
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:80 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4236 (4.1 Kb)  TX bytes:4236 (4.1 Kb)

linux-121:~ #
```

Abbildung 3 openSUSE 12.1 EUI-64 Enforcement

Verbindungsabbrüche

Im folgenden Beispiel wird gezeigt, wie eine bestehende SSH-Verbindung unterbrochen wird, weil der Verbindungsaufbau mit einer temporären IPv6 Source Address erfolgte. Die Microsoft Windows Systeme nutzen zum Verbindungsaufbau bevorzugt die kurzlebige Temporary Address.

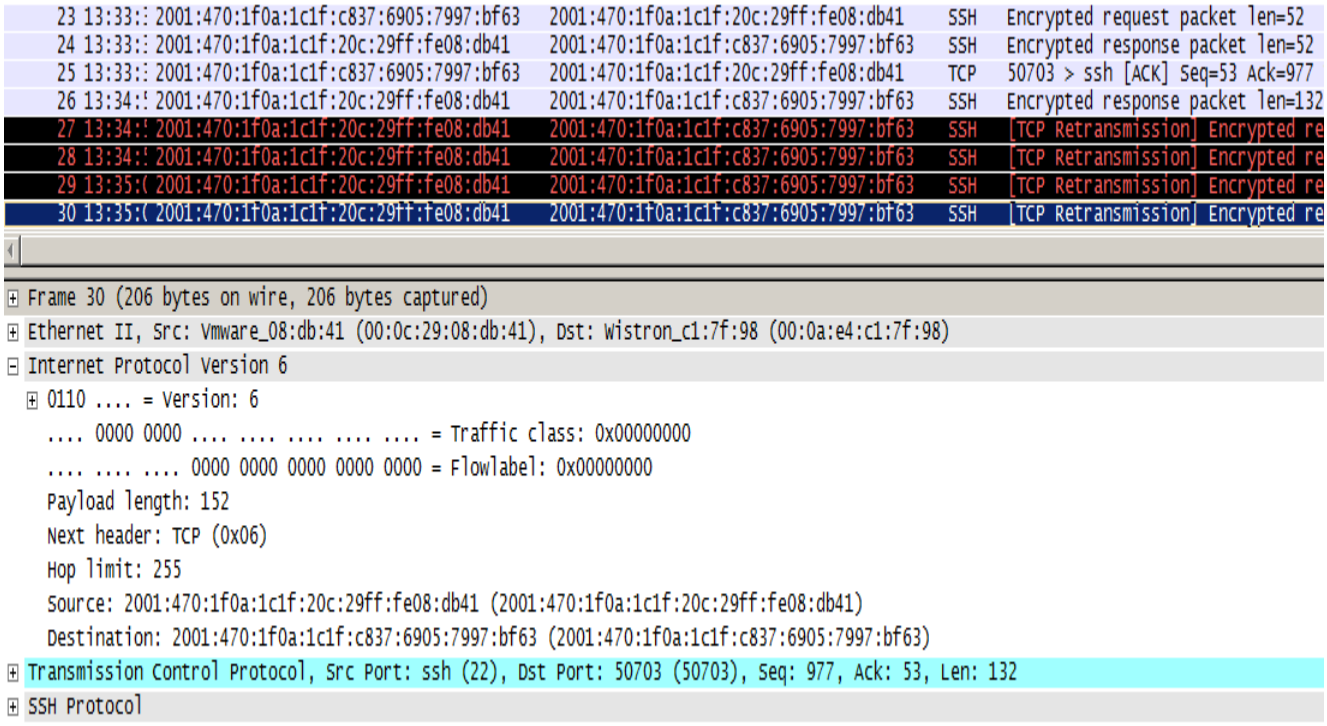

Abbildung 4: wireshark - TCP Unterbrechung

Nach Ablauf der Valid Time berechnet der Windows Client einen neuen zufälligen Interface Identifier. Ohne weitere Rücksicht auf die bestehende Verbindung wird die bisher genutzte Adresse verworfen und die damit bestehende TCP-Verbindung (siehe Abbildung 3 ‚TCP Retransmission') unterbrochen. Der Benutzer sieht letztlich nur ein SSH-Terminal-Fenster, das nicht mehr reagiert. Server-seitig sieht die Verbindung noch intakt aus. Erst nach Ablauf der TCP-Überwachungstimer im Kernel werden die Socket-Strukturen gelöscht. Solange sieht der Systemadministrator bei der Prüfung mittels *netstat* eine scheinbar funktionstüchtige Verbindung auf dem SSH-Server.

```
linux-hsrk:/var/log # date
Sun Nov  6 13:49:51 CET 2011
linux-hsrk:/var/log # who
root     :0           2011-11-06 12:39 (console)
root     pts/0        2011-11-06 12:39 (:0.0)
root     pts/2        2011-11-06 12:40 (:0.0)
root     pts/3        2011-11-06 12:45 (fe80::9c6b:6db2:331a:133c%eth0)
root     pts/4        2011-11-06 13:22 (2001:470:1f0a:1c1f:c837:6905:7997:bf63)
linux-hsrk:/var/log # ping6 2001:470:1f0a:1c1f:c837:6905:7997:bf63 -I eth0
PING 2001:470:1f0a:1c1f:c837:6905:7997:bf63(2001:470:1f0a:1c1f:c837:6905:7997:bf63) from 2001:470:1f0a:1c1f:20c:29ff:fe08:db41
6 data bytes
From 2001:470:1f0a:1c1f:20c:29ff:fe08:db41 icmp_seq=1 Destination unreachable: Address unreachable
From 2001:470:1f0a:1c1f:20c:29ff:fe08:db41 icmp_seq=2 Destination unreachable: Address unreachable
From 2001:470:1f0a:1c1f:20c:29ff:fe08:db41 icmp_seq=3 Destination unreachable: Address unreachable
^C
--- 2001:470:1f0a:1c1f:c837:6905:7997:bf63 ping statistics ---
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time 4003ms

linux-hsrk:/var/log #
linux-hsrk:/var/log # who
root     :0           2011-11-06 12:39 (console)
root     pts/0        2011-11-06 12:39 (:0.0)
root     pts/2        2011-11-06 12:40 (:0.0)
root     pts/3        2011-11-06 12:45 (fe80::9c6b:6db2:331a:133c%eth0)
root     pts/4        2011-11-06 13:22 (2001:470:1f0a:1c1f:c837:6905:7997:bf63)
linux-hsrk:/var/log # netstat -an | grep 2001:470:1f0a:1c1
tcp        0    792 2001:470:1f0a:1c1f:2:22 2001:470:1f0a:1c1:50703 ESTABLISHED
linux-hsrk:/var/log #
```

Abbildung 5: Linux SSH-Server - Inkonsistente Sockets

Diese Überlegungen sind auf alle anderen TCP-Verbindung übertragbar. Darunter fallen also auch Zugriffe auf Dateifreigaben, der NFS-Betrieb sowie Terminalsitzungen (RDP, VNC).

DNS-Betrieb

Die Microsoft Betriebssysteme Windows Vista, Windows 7 und die Windows 2008 Server Plattformen können in der jeweiligen DNS Forward Lookup Zone AAAA Records registrieren. Diese Registrierung beschränkt sich auf die langlebigen Random Interface Identifiers. Die kurzlebigen temporären Interface Identifier werden nicht registriert. Letztlich unterscheiden sich diese beiden Adressen in den Merkmalen DNS Registrierung und Lebensdauer. Ein weiteres Kriterium für die Registrierung ist der Scope. Global Unicast Adressen und ULA[5] Adressen erfüllen die Voraussetzung.

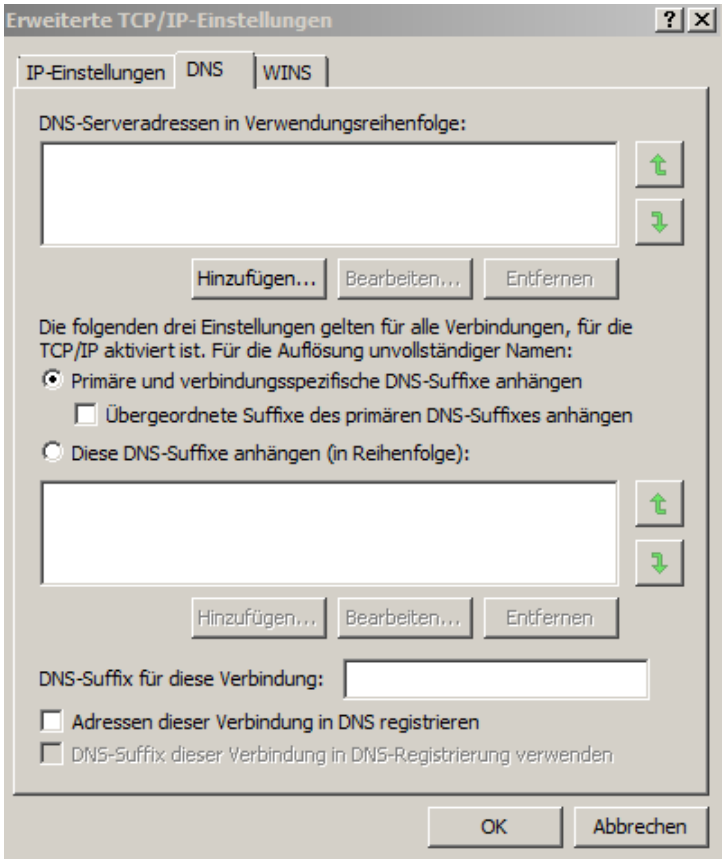

Abbildung 6: Windows 7 DNS Client

Temporäre IPv6-Adressen werden nicht beim dynamischen DNS Update berücksichtigt. Link Local Adressen ebenfalls nicht. Da die temporäre IPv6-Adresse aber nicht im DNS registriert wird, das gilt sowohl für die jeweilige Forward Lookup Zone als auch für das Reverse Lookup, können keine Zugriffsrichtlinien, beispielsweise SAMBA oder NFS, an den DNS-Namen des IPv6 Clients gebunden werden.

Die gängigen Linux-Derivate bieten derzeit im Auslieferungszustand keine administrative Schnittstelle zur Kontrolle der dynamischen Registrierung von IPv6-Adressen. Allen Apple-Betriebssystemen fehlt diese Funktionalität ebenfalls.

[5] Unique Local Address (RFC 4193)

Dieser Umstand zeigt, dass die konsistente und flächendeckende Erfassung der RFC 3041 Interface Identifier derzeit weder durch die Zulassung von dynamischen DNS Updates im Enterprise LAN noch durch eine mit immensen Aufwand einhergehende administrative Erfassung sinnvoll möglich ist.

Der Betrieb einer DNS Infrastruktur in Verbindung mit dynamischen Updates eröffnet zudem neue Angriffsmöglichkeiten. Stellvertretend sei hier Programm *fake_dnsupdate6* genannt.

Access Control

Die heute üblichen Filterregeln in Enterprise Firewalls und Personal Firewalls enthalten als Parameter üblicherweise Hostnamen oder IP-Adressen. Falls Hostnamen verwendet werden, sind die Prozesse zur Abbildung der Hostnamen auf IPv4- oder IPv6-Adressen plattformspezifisch im Detail zu analysieren. Erfolgt die Auflösung der Hostnamens nur einmalig bei der Aktivierung einer Filterregel, sind Fehler unvermeidbar, wenn die temporäre IPv6-Adresse nach Ablauf der Valid Time erneuert wird. Anderseits ist die Auflösung in Echtzeit für jedes übertragene IP-Paket nicht vertretbar. Die im Linux-Umfeld benutzte Firewall ip6tables weist in der Manual Page (Ausschnitt) darauf hin:

```
[!] -s, --source address[/mask]
       Source specification.  Address can be either be a hostname, a network IP address
       (with /mask), or a plain IP address.  Names will be resolved once  only,  before
       the rule is submitted to the kernel.  Please note that specifying any name to be
       resolved with a remote query such as DNS is a really bad idea.  (Resolving  netâ
       work names is not supported at this time.)  The mask is a plain number, specifyâ
       ing the number of 1's at the left side of the  network  mask.   A  "!"  argument
       before  the  address  specification  inverts  the sense of the address. The flag
       --src is an alias for this option.  Multiple addresses  can  be  specified,  but
       this will expand to multiple rules (when adding with -A), or will cause multiple
       rules to be deleted (with -D).
```

Abbildung 7: ip6tables Manual Page (Linux)

Zudem schränken die Konfigurationsoberflächen die Möglichkeiten oftmals unmittelbar ein – die Angabe einer IPv4- oder IPv6-Adresse ist dann zwingend:

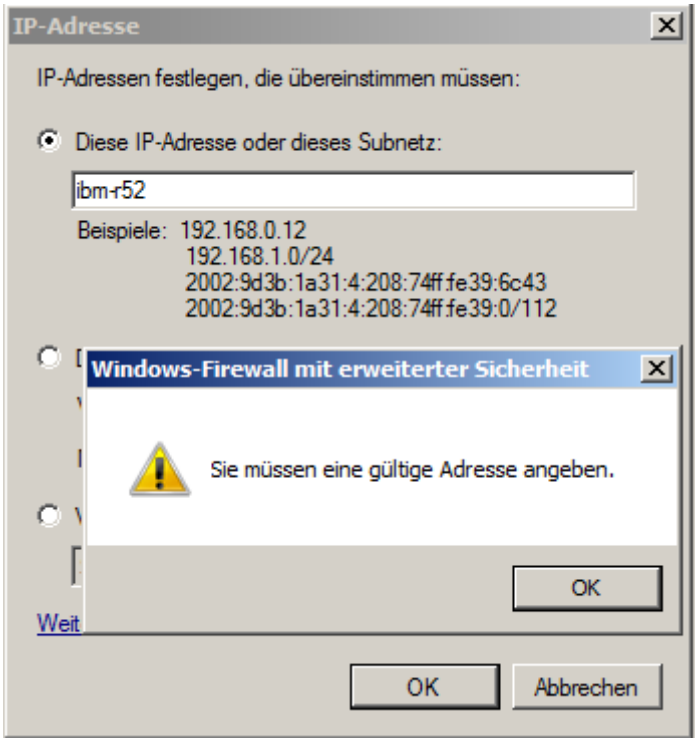

Abbildung 8: Windows 7 Firewall

Die Konfigurationsoberfläche der Windows Firewall lässt nur die Eingabe von IPv6-Adressen im Format RFC 5952 ‚A Recommendation for IPv6 Address Text Representation' zu. Hostnamen werden als Eingabeparameter nicht akzeptiert.

Die gleiche Situation zeigt sich bei der Definition einer IPv6 Access List auf einem CISCO IOS-Router. Hostnamen sind nicht zulässig:

```
CISCO(config)#ipv6 access-list SSH-SERVERLISTE
CISCO(config-ipv6-acl)#
CISCO(config-ipv6-acl)#permit ipv6 any host 2001:db8:4711::22
CISCO(config-ipv6-acl)#
CISCO(config-ipv6-acl)#permit ipv6 any host ssh-server.example.com
                                   ^
% Invalid input detected at '^' marker.

CISCO(config-ipv6-acl)#
CISCO(config-ipv6-acl)#end
```

Forensik

Neben der MAC-Adresse im Fall von EUI-64 Interface IDs lassen sich beispielsweise folgende Informationen aus einer Global Unicast Adresse ableiten und bei der Netzwerkdiagnose und Forensik nutzen:

2001:db8:4711:c800:0215:77ff:fe76:74b9

Prefix Info Global Unicast Address (RFC3587) - 2000::/3
Interface ID Info:
IEEE EUI-64 based Interface ID (RFC4291)
Hardware Address (IEEE - 48 bit MAC) 00-15-77-76-74-b9
IPv6 Solicited-Node Multicast Address ff02::1:ff76:74b9
Corresponding Ethernet Multicast Address 33-33-ff-76-74-b9
getaddrinfo Result: 2001:db8:4711:c800:215:77ff:fe76:74b9

Kommen Privacy Extensions bei der Erzeugung der IPv6-Adresse zum Einsatz, ist die Zuordnung zur MAC-Adresse nicht möglich:

2001:0db8:4711:c800:08f1:343a:2610:b3b3

Prefix Info Global Unicast Address (RFC3587) - 2000::/3
Interface ID Info:
Locally administered Bit not set (U/L Bit)
Randomized Interface Identifier (RFC3041/RFC4941)
IPv6 Solicited-Node Multicast Address ff02::1:ff10:b3b3
Corresponding Ethernet Multicast Address 33-33-ff-10-b3-b3
getaddrinfo Result: 2001:db8:4711:c800:8f1:343a:2610:b3b3

Insbesondere die Zuordnung von IPv6-Adresse zur 48 Bit Ethernet Hardwareadresse kann bei aktivierten Privacy Extensions nur durch Zusatzprogramme wie NDPMON[6] oder durch Auslesen von kurzlebigen Neighbor Cache Einträgen erfolgen. Betrachtet man die nachfolgend gezeigten SSH-Logins in der Syslog-Datei eines Linux-Rechners, wird nicht unmittelbar klar, welche Systeme als SSH-Clients in Frage kommen.

Nov 6 12:43:31 linux-hsrk sshd[9811]: Accepted keyboard-interactive/pam for root from fe80::9c6b:6db2:331a:133c%eth0 port 50699 ssh2

Nov 6 12:45:57 linux-hsrk sshd[9972]: Accepted keyboard-interactive/pam for root from fe80::9c6b:6db2:331a:133c%eth0 port 50700 ssh2

Nov 6 13:22:07 linux-hsrk sshd[11275]: Accepted keyboard-interactive/pam for root from 2001:470:1f0a:1c1f:c837:6905:7997:bf63 port 50703 ssh2

[6] Neighbor Discovery Protocol Monitor (MADYNES Project)

Alle drei erfolgreichen Login-Versuche wurden vom gleichen Client-Rechner aus initiiert. Dabei handelt es bei den beiden obersten Syslog-Einträgen um die Link Local Address eines Windows 7 Systems, aufgebaut aus dem länger gültigen Randomized Interface Identifier (Default Preferred Lifetime: 7 Tage).
Der gleiche Windows Rechner konnektiert danach über die Global Unicast Address den Linux-Server. Bestandteil der IPv6 Source Address ist diesmal der einen Tag lang (Default Preferred Lifetime) gültige temporäre Interface Identifier. Die Quelladresse wird dabei in Abhängigkeit von der Zieladresse entweder aus dem Link Local Scope (fe80::/10) oder Global Scope (2000::/3) gewählt (RFC 3484).

Im Gegensatz dazu ist bei Verwendung von EUI-64 Interface Identifiern unmittelbar das Client-System eindeutig erkennbar.

Nov 9 16:14:56 linux-hsrk sshd[12389]: Accepted keyboard-interactive/pam for root from 2001:470:1f0a:1c1f:221:6aff:fe0d:8cbe port 49246 ssh2

Nov 9 16:29:29 linux-hsrk sshd[12866]: Accepted keyboard-interactive/pam for root from fe80::221:6aff:fe0d:8cbe%eth0 port 49260 ssh2

Der nachfolgende Syslog-Eintrag stammt wiederum von einem Client-System mit aktiven Privacy Extensions.

Nov 9 16:34:46 linux-hsrk sshd[13101]: Accepted keyboard-interactive/pam for root from 2001:470:1f0a:1c1f:174:27ba:89a8:d973 port 1113 ssh2

Ohne weitere Maßnahmen kann nicht mehr geklärt werden, ob es sich um den oben beschriebenen Windows 7 Rechner (SSH-Client) handelt. Die kurzlebigen dynamischen Neighbor Cache Einträge enthalten keine Daten mehr vom 6. November.

Fazit

Im Enterprise LAN wird durch die Stateless Address Autoconfiguration in Verbindung mit EUI-64 Interface Identifiern jedem Host eine feste IPv6-Adresse zugewiesen. Insbesondere in Netzen, in denen bereits feste IPv4-Adressen konfiguriert und mit DHCP permanent zugewiesen werden, ist so ein vergleichbarer Status für IPv6 herstellbar. Die IPv6-Adressierung kann so ohne zusätzlichen administrativen Aufwand in die existierenden Abläufe übernommen werden. Von Vorteil ist an dieser Stelle, dass die Ethernet-Hardware-Adressen bereits zum Aufbau der DHCP-Datenbank (IPv4) erfasst sind.

In Netzen, wo keine DNS-Einträge und granulare Zugriffsregeln verwaltet werden müssen, können Privacy Extensions eingesetzt werden. Beispielhaft seien hier WiFi- und Access-VPN-Netze genannt, in denen die Anwender nur wenige Stunden *online* sind und persistente Verbindungen beim Zugriff auf Server-Dienste nur eine untergeordnete Bedeutung haben.

Falls die externen WEB-Zugriffe aus dem Enterprise LAN über einen WEB-Proxy erfolgen, bleiben unabhängig von der gewählten Strategie zur Bestimmung der Interface Identifier die wirklichen Adressen (IPv4 und IPv6) verborgen. Extern ist nur die IPv6-Adresse des WEB-Proxy sichtbar.

Die gezeigten Beispiele sind gewichtige Argumente für die Stateless Address Autoconfiguration in Verbindung mit EUI-64 Interface Identifiern. Seitens der IETF wäre zu überlegen, ob durch neue Optionen im Router Advertisement die Verfahren zu Generierung der Interface Identifier den Anforderungen im jeweiligen Netz angepasst werden könnten. Der Internet Draft ‚Managing the Use of Privacy Extensions for Stateless Address Autoconfiguration in IPv6‘ beschreibt eine mögliche Realisierung.

Literatur

[1] IPv6 Security – Protection measures for the next Internet Protocol; E. Vyncke; Cisco Press; ISBN-13 978-1-58705-594-2

[2] Understanding IPv6; J. Davies; Microsoft Press; ISBN-13 978-0-7356-2446-7

[3] IPv6 for Enterprise Networks; S. McFarlan et al.; Cisco Press; ISBN-13: 978-1-58714-227-7

[4] Requirements for IPv6 in ICT Equipment; J. Zorz, S. Steffann

[5] IPv6 Stateless Address Autoconfiguration; RFC2462 / RFC 4862

[6] Rogue IPv6 Router Advertisement Problem Statement; RFC 6104

[7] IP Version 6 Addressing Architecture; RFC 4291

[8] Connection of IPv6 Domains via IPv4 Clouds; RFC3056

[9] IPv6 Unicast Address Assignment Considerations; RFC 5375

[10] Address Allocation for Private Internets; RFC 1918

[11] Unique Local IPv6 Unicast Addresses; RFC 4193

[12] Dynamic Host Configuration Protocol for IPv6 (DHCPv6); RFC 3315

[13] Default Address Selection for Internet Protocol version 6 (IPv6); RFC 3484

[14] Privacy Extensions for Stateless Address Autoconfiguration in Ipv6; RFC 3041/RFC 4941

[15] Multiprotocol Extensions for BGP-4; RFC 4760

[16] IPv6 Global Unicast Address Format; RFC 3587

[17] Neighbor Discovery for IP version 6 (IPv6); RFC 4861