FORSCHUNGSZENTRUM JÜLICH GmbH

Jülich Supercomputing Centre

D-52425 Jülich, Tel. (02461) 61-6402

Interner Bericht

IPv6 im lokalen Netz – Gefahren und Lösungen

Werner Anrath, Egon Grünter, Sabine Werner

FZJ-JSC-IB-2011-07

November 2011

(letzte Änderung: 04.11.2011)

Inhalt

IPv6 Status 2011 - Überblick 3

Dual Stack Implementierungen 4

Native IPv6 – Risiken und Gefahren 6

Stateless Address Autoconfiguration 6

Interface Identifier 7

Rogue Router Advertisements 10

DNS und LLMNR 12

Lösungen 15

IPv6 Transition Technologies – Risiken und Gefahren 19

ISATAP- Intra-Site Automatic Tunnel Addressing Protocol 20

6to4 - Connection of IPv6 Domains via IPv4 Clouds 21

Teredo 22

Tunnel Broker 24

Rogue Tunnel - Gefahren 25

Lösungen 25

Fazit 26

Literatur 27

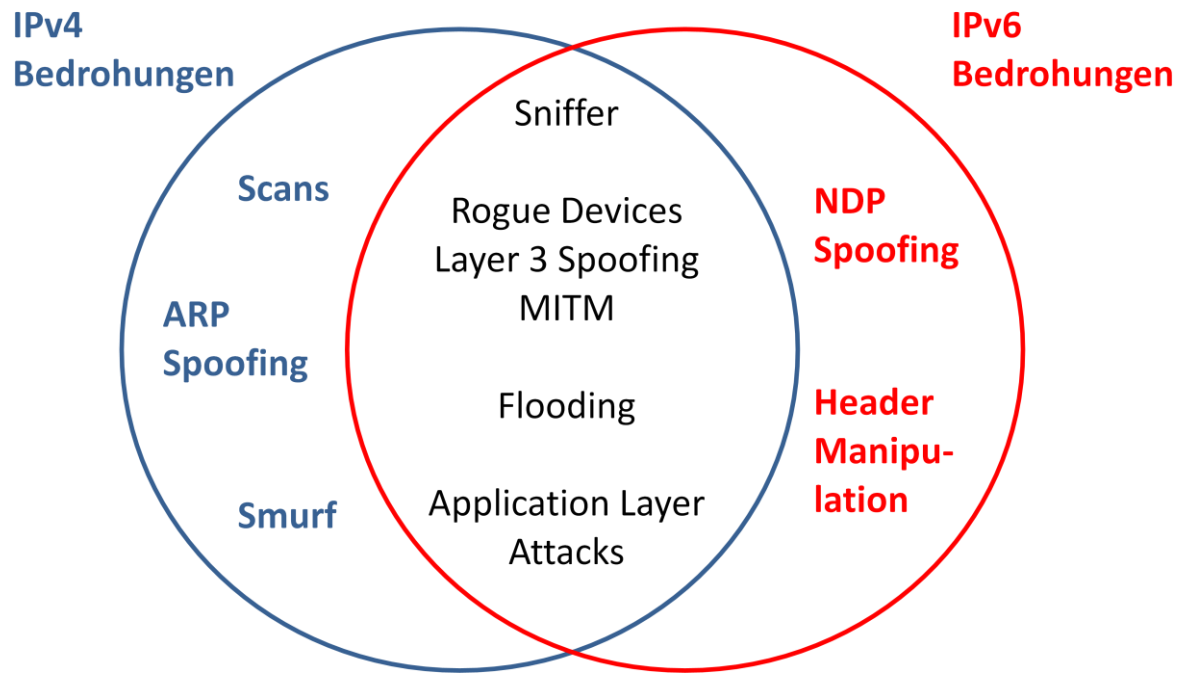
IPv6 Status 2011 - Überblick

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. Mit der Einführung von Windows Vista und den Windows-Server-Plattformen im Jahr 2007 ist das IPv6-Protokoll im LAN installiert und aktiv. Damit existiert in den lokalen Netzen eine latente Bedrohung bevor überhaupt der administrativ organisierte IPv6 Einsatz beginnt und IPv6 im Netzbetrieb integriert ist.

Weitere Aufmerksamkeit ist auf die Weiter- und Neuentwicklungen von Hackertools zu richten. Die im Internet zur Verfügung gestellten Werkzeuge können im lokalen Netz aggressiv Protokollschwächen und -eigenheiten ausnutzen. Dabei ist eine Konzentration auf ICMPv6 mit den Schwerpunkten Neighbor Discovery Protocol (NDP[1]) und Link-Local-Multicast Protokolle zu verzeichnen.

In den folgenden Darstellungen werden zur Illustration von Schwachstellen die Auswirkung von Fehlkonfigurationen und IPv6-Automatismen betrachtet. Schon dabei können annähernd Situationen im lokalen Netz auftreten, die dem Einsatz der oben genannten Werkzeuge ähneln. Letztlich sollen diese als Beispiele für den unabdingbaren Handlungsbedarf gesehen werden, IPv6 in die Netzwerkstrategie und Sicherheitsplanung aufnehmen zu müssen.

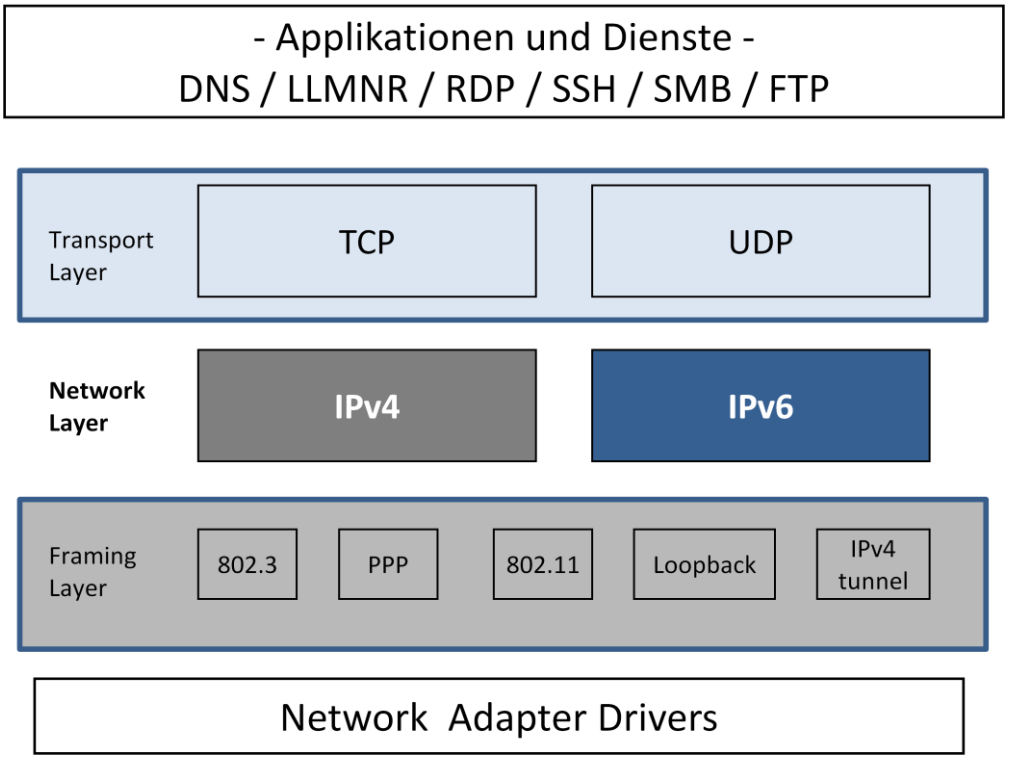


[1] Neighbor Discovery Protocol

Die hier vorgestellten Sachverhalte gelten nahezu für alle lokalen Netze, in denen gegenwärtig IPv4 genutzt wird, IPv6 bisher aber nicht administrativ betrachtet wird.

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 Grafik) am Netzwerk kommunizieren. Die Microsoft Betriebssysteme nutzen zudem sogenannte Transition Technologies, die den Zwang zur Planung und Organisation des IPv6-Betriebs im lokalen Netz erhöhen.



IPv6 – Dual Stack Implementierung

Windows Vista / 7 / 2008

- **IPv6 ist installiert und aktiv**
- Stateless Address Autoconfiguration aktiv (RFC[2] 2462 / RFC 4862)
- IPv6 Stack: zahlreiche Verbesserungen (Dual Layer)
- GUI, CLI and GPO[3] Konfiguration
- Integrated Internet Protocol security (IPsec) verfügbar
- Privacy Extensions[4] (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**

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 Apple-Betriebssysteme für iPhone und iPad haben im Auslieferungszustand das IPv6 Protokoll aktiviert. Die Android-Smartphones werden ebenfalls so ausgeliefert. Es existiert keine administrative Schnittstelle zum Deaktivieren bzw. Aktivieren dieser Funktionalität.

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

Native IPv6 – Risiken und Gefahren

Stateless Address Autoconfiguration

Der IPv6 Standard sieht für jeden Host nach RFC 2461 ‚Neighbor Discovery for IP Version 6 (IPv6)' die sogenannte Stateless Address Autoconfiguration (SLAAC) vor. Die Implementierung dieser Technik ist für jeden IPv6 Host verpflichtend. Weitere Methoden sind optional und können das jeweilige Host-Interface mit weiteren IPv6-Adressen konfigurieren. Die LAN-Interfaces durchlaufen bei der Initialisierung nach RFC 2462 ‚IPv6 Stateless Address Autoconfiguration' folgende Stufen:

- Link-Local Address (EUI-64[5] IID[6] oder Pseudozufallszahl) generieren
- Neighbor Solicitation (NS) für Duplicate Address Detection (DAD) senden
- Autoconfiguration abbrechen, falls ein Neighbor Advertisement (NA) einen Adresskonflikt anzeigt
- Router Solicitation (RS) senden
- Falls kein Router Advertisement (RA) empfangen wird, starte DHCPv6
- Falls ein Router Advertisement (RA) empfangen wird:
    - generiere Adressen für die enthaltenen Prefixe; danach DAD
- M Flag == 1 im Router Advertisement (RA):
    - starte DHCPv6 um weitere Adressen und Parameter zu erhalten
- M Flag == 0 und O Flag == 1 im Router Advertisement (RA):
    - starte DHCPv6 um weitere Konfigurationsparameter zu erhalten (z.B. DNS Server)

Aus der Übersicht ist ersichtlich, dass dieser Vorgang im lokalen Netz ohne zusätzliche Sicherung durch kryptografische Maßnahmen Angriffspunkte bietet. Diverse Tools aus bekannten Werkzeugsammlung im Internet nutzen diese Angriffspunkte aus – u.a.:

- dos-new-ip6 – Angriff auf Duplicate Address Detection
- fake_router6 – Rogue Router Advertisements (RA) verteilen
- fake_dhcps6 – Rogue DHCPv6 Server

Rogue Router sind durch Benutzer fehlkonfigurierte oder durch Angreifer absichtlich installierte Router, die schädliche Auswirkungen auf die Verfügbarkeit, Integrität und Vertraulichkeit der Kommunikation haben. Aber auch Fehlkonfigurationen im lokalen Netz, häufig durch benutzeradministrierte Hosts hervorgerufen, haben schädliche Auswirkungen.

In der Praxis zeigt sich, dass insbesondere Rogue Router Advertisements regelmäßig die Ursache von Störungen sind. Wird ein Rogue Router aktiv, kann er durch Flags im Router Advertisement die Hosts zur Stateless Address Autoconfiguration (SLAAC) veranlassen und danach auch neben der Adress- und Routingkonfiguration die DNS-Funktionen des Hosts kontrollieren.

Aufgrund der besonderen Bedeutung wird die Bearbeitung von Router Advertisements später in einem eigenen Abschnitt gesondert dargestellt.

[5] 64 Bit Extended Unique Identifier – IEEE-Standard
[6] Interface Identifier

Betrachtet man die IPv6-Adressen der Hosts nach der SLAAC-Phase, so werden die vielfältigen Varianten zur Bildung der IPv6 Interface Identifier (IID) sichtbar, die sowohl die Identifizierung von Rogue Routern als auch nachgeordnete Forensik-Arbeiten nachhaltig erschweren.

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 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-ID und Board-ID

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

und invertieren des **U/L-Bit** 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 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 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 [7]gelöscht wird. Diese Adressen werden Random Address oder Temporary Address genannt.

Ohne Anpassung der Voreinstellungen (Auslieferungszustand) der genannten Betriebssysteme zeigen sich abweichende Methoden zur Bestimmung der Interface-Identifier (IID) bei der Initialisierung der IPv6-Module im Kernel und der späteren Stateless Address Autoconfiguration (SLAAC):

[7] Universal/Local Bit

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	+	-	+	-	-
Mac OS 10.6	-	+	-	-	+
Mac OS 10.7	-	+	-	+	+
openSUSE 11.3	-	+	-	-	+
Debian 6.0	-	+	-	-	+

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 verschiedene Netzwerkmanagement-Aufgaben erschweren:

- DNS Betrieb
- Access Control List
- Forensik

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

Beispiel - IPv6 Address: 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

Im RFC 3041 werden die aus Pseudozufallszahlen gebildeten Interface Identifier technisch eingeführt. Aber auch die Vor- und Nachteile beim Einsatz von Privacy Extensions zur Generierung der Interface Identifier werden in diesem Dokument ausführlich diskutiert. Insbesondere der Vergleich mit den EUI-64 Interface Identifier und die Abwägung, welche Variante je nach Einsatz als suboptimal einzustufen ist, wird im Abschnitt 4 dieses Dokuments erörtert.

Zur Deaktivierung der Privacy Extensions Windows 7/Vista/2008 System sind dazu 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

Falls nötig, kann das EUI-64 Enforcement über eine Interface-spezifische Traffic-Filter-ACL[8] auf dem Router oder einer Layer 2 Port-ACL implementiert und durchgesetzt werden. Dabei werden nur Interface Identifier mit gesetztem U/L-Bit[9] erlaubt. Die Liste zeigt die möglichen Muster:

::x**2**:xx:xx:xx:xx:xx

::x**6**:xx:xx:xx:xx:xx

::x**A**:xx:xx:xx:xx:xx

::x**E**:xx:xx:xx:xx:xx

Eine entsprechende IPv6 Access Control List (ACL) muss pro Subnetz erstellt werden, um nur zulässige Kombinationen weiterzuleiten. Hier ein Beispiel für eine solche Interface-ACL, die auf einem Router Interface wirkt:

```
ipv6 access-list BLOCK-RFC3041
        remark Block randomized and temporary IPv6 addresses from routing core
        deny    any  fec0::/10
        deny    any  fd00::/7
        permit  2001:db8:4711:d800:0000::/80 any

        permit  2001:db8:4711:d800:02**2**00::/72 any
        permit  2001:db8:4711:d800:1**2**00::/72 any

        !!!  Alle möglichen Kombinationen auflisten
                ......................
        permit  2001:db8:4711:d800:0**6**00::/72 any
                ......................
        permit  2001:db8:4711:d800:0**A**00::/72 any
                ......................

        permit  2001: db8:4711:d800:f**E**00::/72 any

        deny    2001:db8:4711::/48  any  log
        permit  any any
        remark  NOW IMPLICIT DENY / icmpv6 ND allowed
        end
```

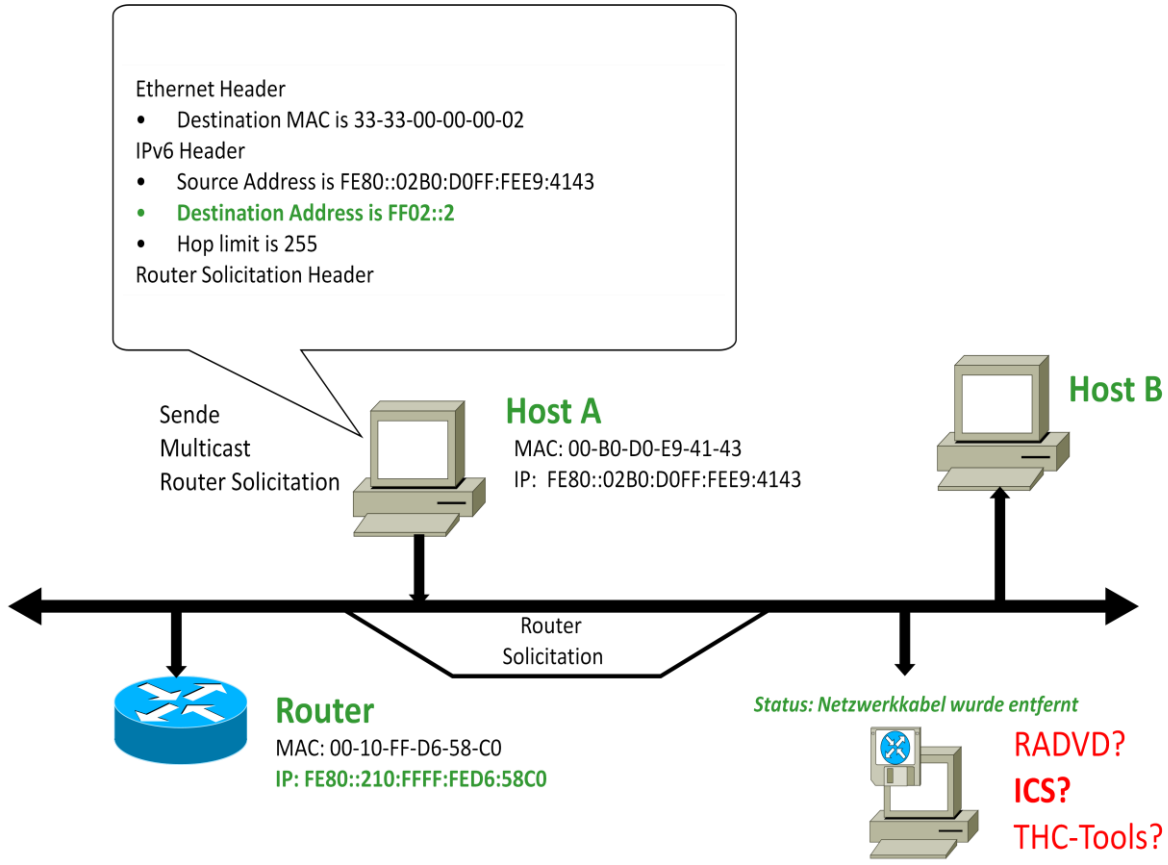
[8] Access Control List

[9] IEEE Universal/Local Bit

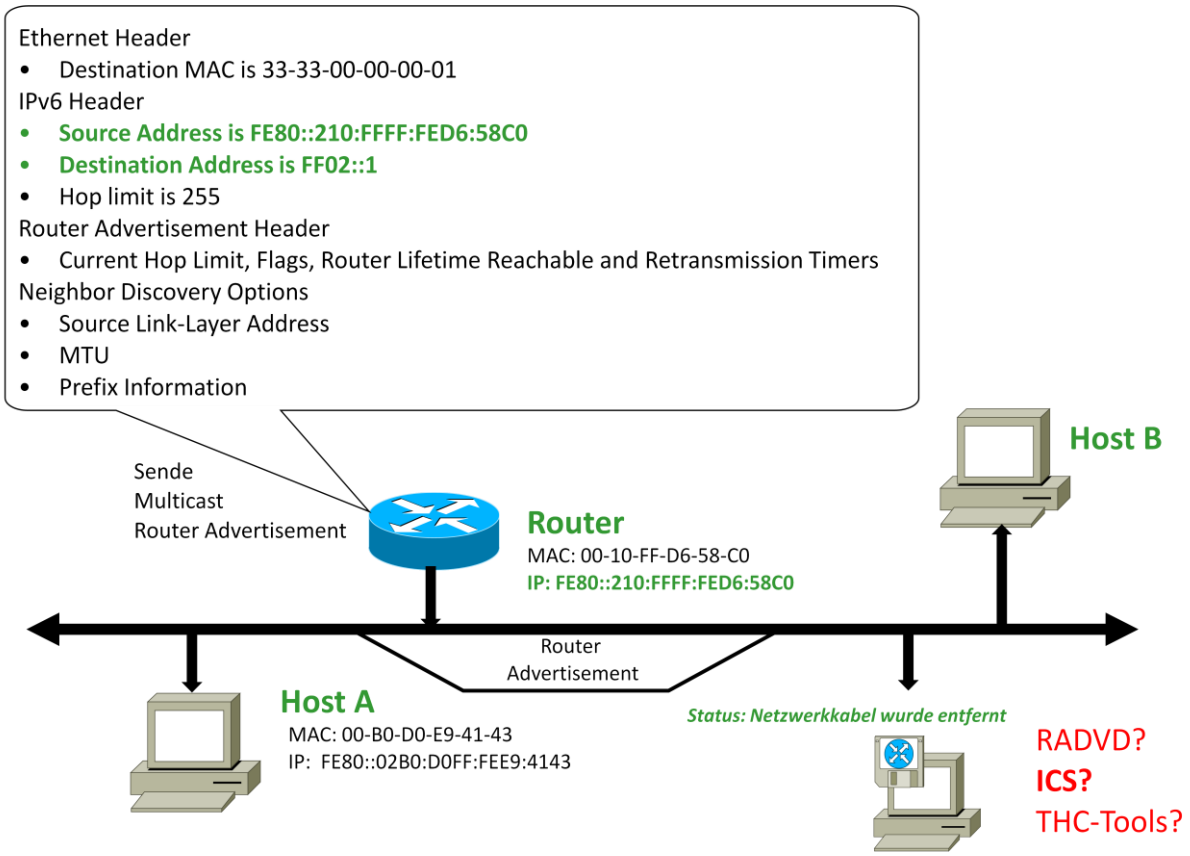
Rogue Router Advertisements

Betrachtet man den Autoconfiguration-Prozess nach RFC 2462 ergeben sich unmittelbar verschiedene Schwachstellen, welche sowohl in böswilliger als auch unbeabsichtigter Weise genutzt werden können und so eine erhebliche Gefährdung der lokalen Teilnehmer darstellen. Zu diesen Gefährdungspotenzialen zählen insbesondere Rogue Router, durch deren Konfiguration der Verkehrsfluss im Netz beliebig manipuliert werden kann. Dieses Szenario ist in der Praxis häufig vertreten, da durch Technologien wie Windows Internet Connection Sharing (ICS) oder Software Routern in Linux-Derivaten (radvd), die ohne großen Aufwand aktiviert und genutzt werden können, sogenannte Router Advertisements (RAs) an die lokalen Kommunikationspartner gesendet werden.

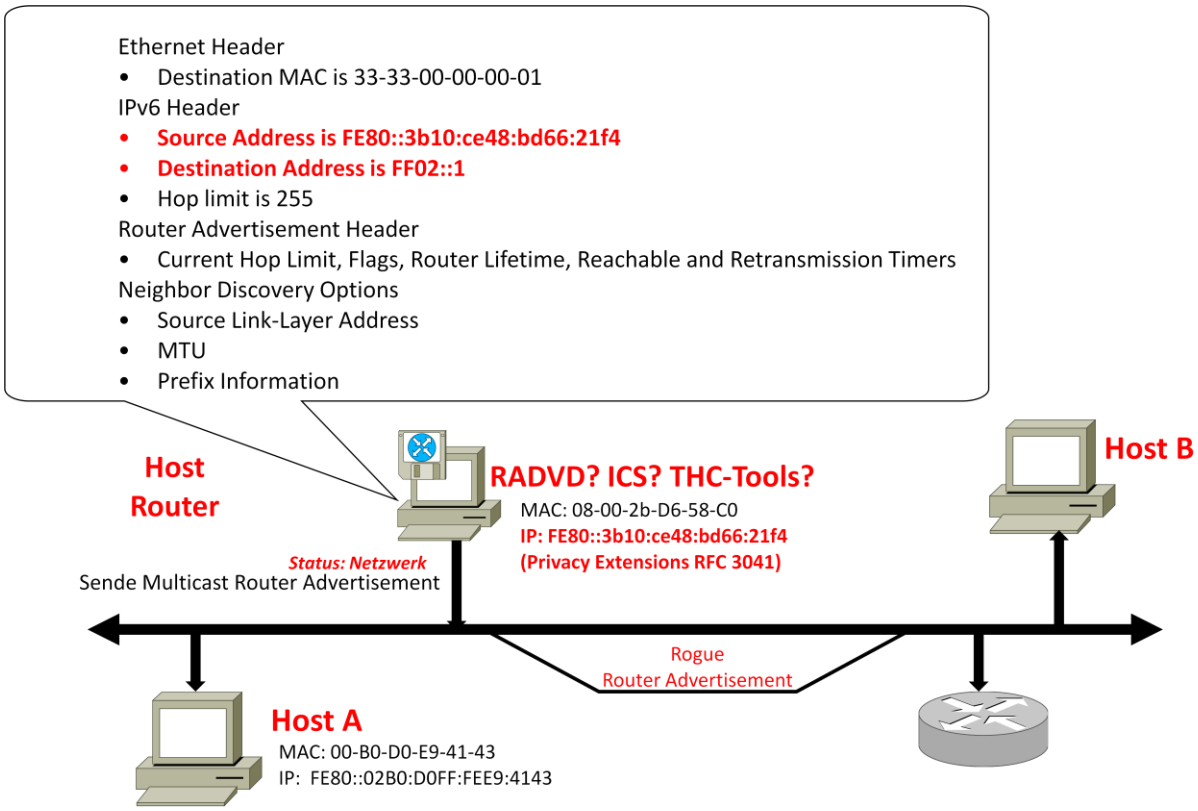
Durch Senden einer sogenannten initialen Router-Solicitation an die Link Local Multicast Address FF02::2 versuchen die Hosts durch Stateless Address Autoconfiguration unternehmensweit oder weltweit gültige IPv6-Prefixe zu erhalten, die mit einem Interface Identifier verknüpft eine vollständige 128 Bit IPv6-Adresse ergeben. Damit ist die Kommunikation über Subnetzgrenzen hinweg möglich.



Der reguläre IPv6-Router antwortet mit einem Router Advertisement (RA). Die Antwort wird an die Link-Local-Multicast-Address FF02::1 (All-Nodes) gesendet. Als Payload enthält diese Nachricht alle am Local Link (Subnetz) gültigen IPv6-Prefixe. Durch Flags erfolgt ferner eine Feinabstimmung der Konfiguration. Die Router Advertisement (RA) Nachricht wird außerdem periodisch wiederholt.



Wird nun ein Rogue Router an das Netzwerk angeschlossen und sendet dieser ebenfalls an die Multicast-Gruppe FF02::1 ein Router Advertisement (RA), ist die Netzwerk-Konfiguration der Hosts manipuliert. Routingtabelle und Adressen entsprechen nicht mehr den administrativen Vorgaben. In LANs, in denen IPv6 nicht überwacht wird, kann sich ein Rogue Router unbemerkt als Default-Gateway etablieren.

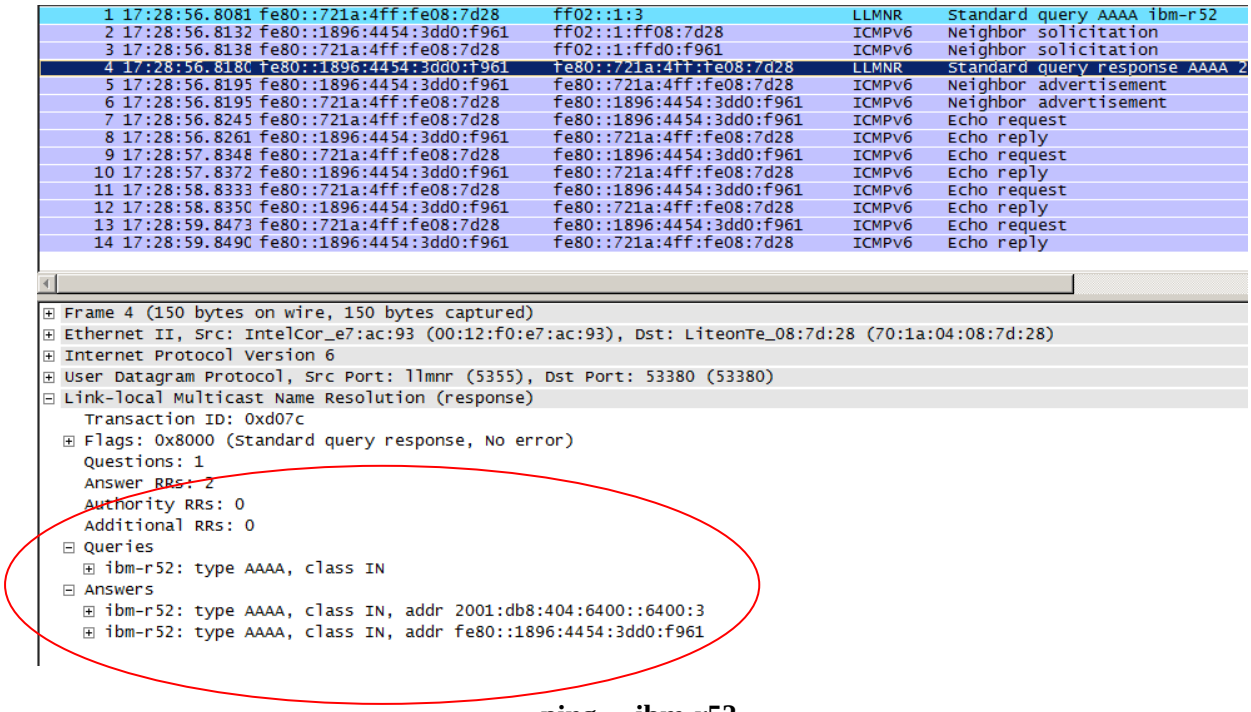


DNS und LLMNR

Eine weitere Gefährdung für die lokale Sicherheit ergibt sich aus der Tatsache, dass immer mehr Anwendungen durch Nutzung einer RFC 3484 konformen Resolver-Library in Richtung IPv6 migrieren. Aufgrund der selbstverständlichen Nutzung von IPv4 und der unbewussten IPv6-Nutzung ergeben sich Wechselwirkungen mit den Personal Firewalls auf den jeweiligen Endsystemen, sowie dem Netzwerkmonitoring, da zum heutigen Zeitpunkt diese Maßnahmen auf IPv4 fokussiert sind.

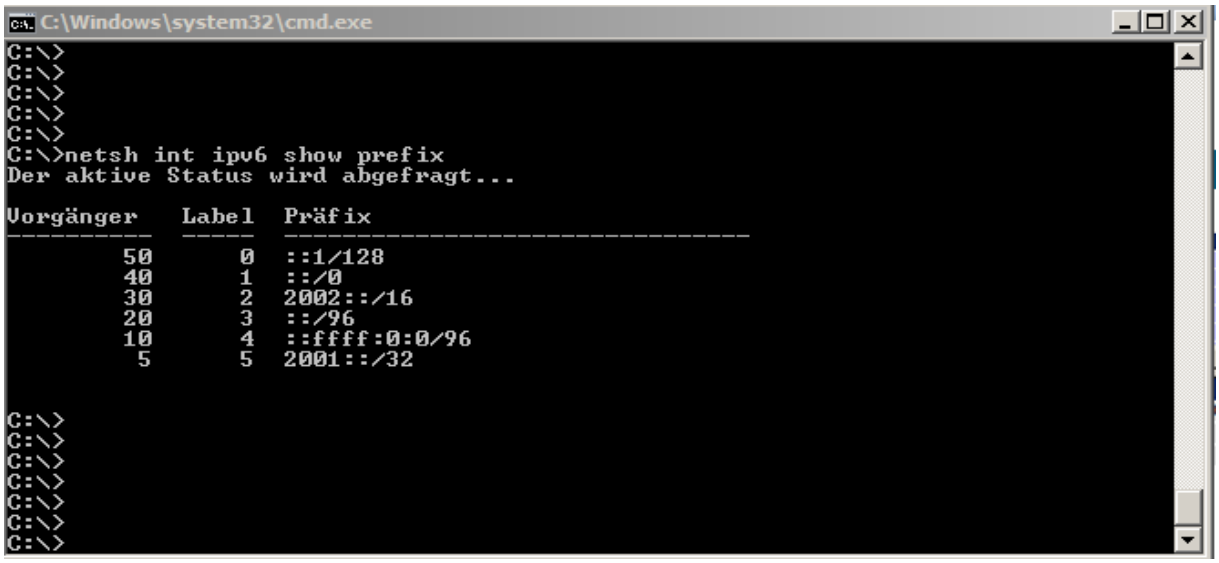
Der folgende Mitschnitt zeigt die Auflösung des Host-Names „ibm-r52“ durch das Link Local Multicast Name Resolution Protocol (LLMNR). Diese Funktion ist in allen neueren Microsoft Betriebssystemen implementiert und als Ergänzung bzw. Fallback zur DNS[10]-Auflösung gedacht, die hier vorab keine Zuordnung des Host-Namen zu einer Adresse lieferte. Wie aus der Aufzeichnung der Pakete zu sehen, wird nachfolgend IPv6 als Übertragungsprotokoll genutzt. Source Address und Destination Address sind aus dem Link-Local Scope (fe80::/10). Die Tatsache, dass IPv6 aktiviert ist und LLMNR eine Namensauflösung liefert, bedingt den Transport der Nachrichten über IPv6.

[10] Domain Name System



ping ibm-r52

Der RFC 3484 fordert die Implementierung einer administrativen Schnittstelle im jeweiligen Host-Betriebssystem zur Steuerung des bevorzugten Netzwerkprotokolls und der Adressauswahl. Die Microsoft Betriebssysteme erlauben eine Anpassung der Policy über die NETSH-Befehle. Linux-Administratoren können die Datei /etc/gai.conf anpassen. MAC OS X hat keine Schnittstelle dazu.

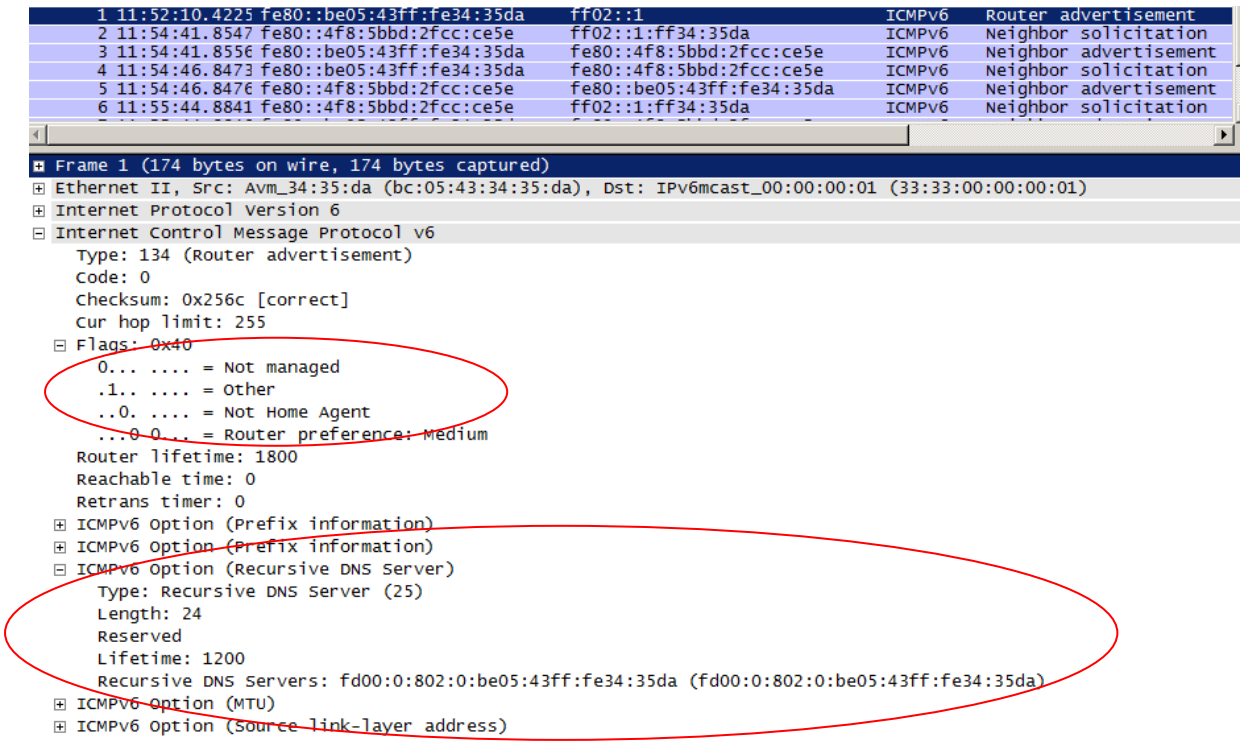


Den einzelnen Zeilen werden im Auswahlprozess nach RFC 3484 folgende Adresstypen zugeordnet, indem nach einer bestmöglichen Übereinstimmung gesucht wird:

- ::1/128 Loopback
- ::/0 IPv6 Adressen
- 2002::/16 6to4 Adressen
- ::/96 IPv4 kompatible Adressen (veraltet)
- ::ffff:0:0 IPv4 Adressen (mapped)
- 2001::/32 Teredo

Die Spalte Vorgänger (engl. Precedence) gibt einer IPv6 Global Unicast Adresse den Wert 40, der IPv6 Loopback Adresse den Wert 50. Platzhalter für mögliche IPv4-Adressen ist der Eintrag ::fffff:0:0/96 mit der Precedence 10. Aufgrund der höheren Precedence wird IPv6 bevorzugt. Dabei werden *Source Address* und *Destination Address* möglichst so ausgewählt, dass der Gültigkeitsbereich (Global oder Link Local) übereinstimmt. Die Spalte Label beeinflusst die Auswahl der Adressen, falls Tunnel oder *native* Transport genutzt werden könnten.

Die im Router Advertisement gesetzten Flags haben ebenfalls direkten Einfluss auf die DNS-Konfiguration der Hosts. Das unten gezeigte Router Advertisement signalisiert dem Host durch das gesetzte OTHER FLAG weitere Konfigurationsparameter mittels Stateless DHCPv6[11] zu suchen. So kann also die DNS-Konfiguration eines Hosts gesteuert bzw. manipuliert werden. Relativ neu ist die Möglichkeit, nach RFC 5006 direkt einen DNS-Server im Router-Advertisement (Option Recursive DNS Server) bekannt zu geben. Das hat zur Folge, dass die vorhandene reguläre DNS-Infrastruktur umgangen wird und ein potentieller Angreifer die Zuordnung von Namen und IP-Adressen bestimmt. Das gilt sowohl für die Abbildung der Host-Namen auf IPv4-Adressen als auch auf IPv6-Adressen.



[11] Dynamic Host Configuration Protocol Version 6

In der Microsoft Welt kann durch dynamische DNS Updates im Active Directory und der später in diesem Bericht dargestellten 6to4 Tunnel ungewollt die Kommunikation über IPv6 erfolgen.

Lösungen

Aufgrund der fehlenden Sicherungsmaßnahmen der Basiskonzepte des IPv6-Protokolls wie ICMPv6 und Link-Local-Multicast, existiert eine latente Gefährdung, die durch entsprechende Maßnahmen entschärft werden muss. Eine einfache Gegenmaßnahme listet das Dokument „Requirements for IPv6 in ICT Equipment“ (Ripe[12]501), in dem zwingend gefordert wird, dass Layer 2 Switches Router Advertisements filtern. Erste Erfahrungen zeigen allerdings, dass auch führende Hersteller diese Funktion nur in neuesten Modellen und Software-Versionen korrekt implementieren und vollständig unterstützen.

Auf Layer 2 Geräten wie z.B. den CISCO Catalyst 4500 Sup 7[13] Switches kann zur Erhöhung der Betriebssicherheit auf allen Access-Ports (Link-Layer) eine IPv6-Port-ACL geschaltet, die Rogue Router und Rogue DHCPv6 Advertisements sperrt:

```
IPv6 access-list BlockRA
        deny icmp any any router-advertisement log sequence 10
        deny udp any eq 547 any eq 546 log sequence 20
        permit ipv6 any any  sequence 30


interface FastEthernet1/11
        !! Beispiel Port – Layer 2
         switchport access vlan 13
         switchport mode access
                  ……
        ipv6 traffic-filter BlockRA in
        end
```

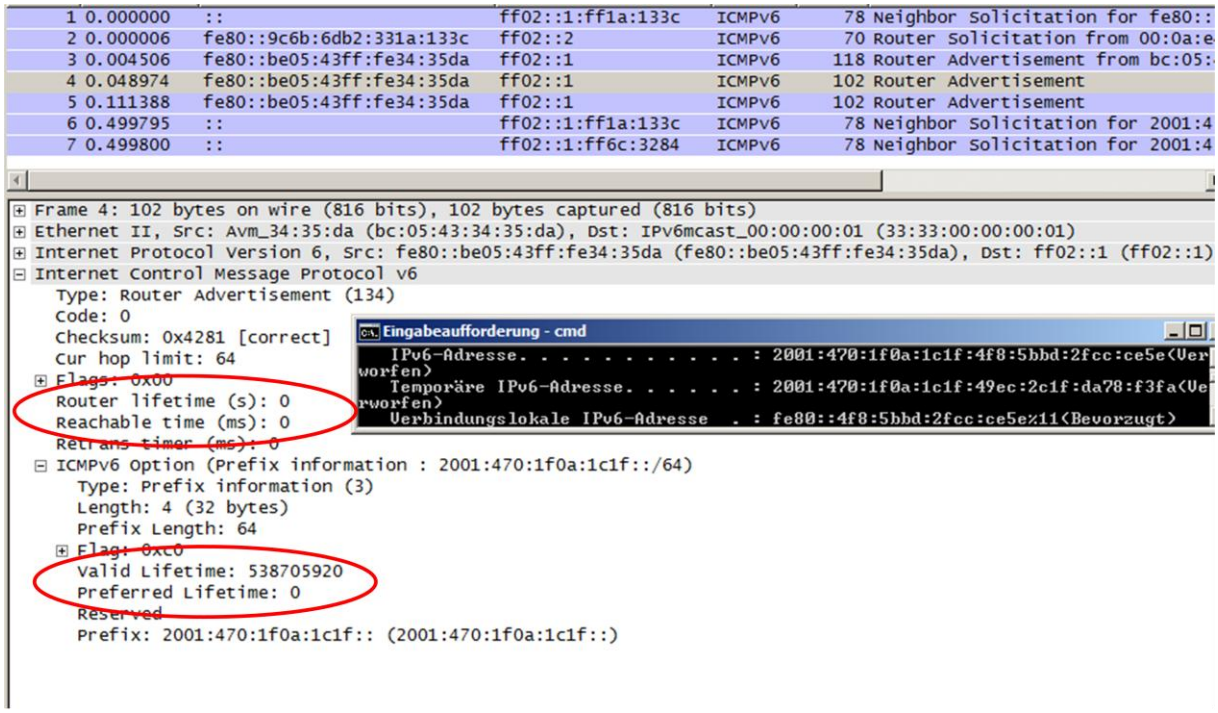
Der RFC 6104 ‚Rogue IPv6 RA Statement‘ liefert eine umfassende Zusammenstellung der Problematik.

Letztlich ergeben sich auch durch DHCPv6 weitere Angriffspunkte, die den aus der IPv4-Welt bekannten Szenarien ähneln. Bisher traten in der Praxis DHCPv6 Server für eine sogenannte Stateful Address Configuration nicht in Erscheinung. Günstig ist hier der Umstand, dass dieser Dienst nicht durch die Standardeinstellungen der gängigen Betriebssysteme aktiviert wird. Bekannte DHCPv6 Threats sind derzeit:

- Starvation (deplete Pool)
- DoS (spray Solicitation Messages)
- Scanning
- Missinformation (rogue Parameters)

[12] Réseaux IP Européens Network Coordination Centre (RIPE NCC)
[13] Catalyst 4500 Supervisor Engine 7

Das Tool RAMOMD kann Router Advertisements als Antwort auf Rogue Router Advertisements generieren, die die Konfigurationsparameter aus der Stateless Address Autoconfiguration (SLAAC) verwerfen. Dazu wird ein spezielles Router Advertisement gesendet. Die Router Lifetime und die Preferred Lifetime müssen die Werte Null haben, um die gewünschte Wirkung zu entfalten. Natürlich sind alle Adressen (Layer 2 und Layer 3) in diesem Advertisement vorgetäuscht (spoofed). Empfängt ein Host ein solches Router Advertisement, verwirft er die dazugehörigen IPv6-Adressen und Routing-Einträge. Das Tool kann auch vorsätzlich für DoS[14]-Attacken auf reguläre IPv6 Deployments in lokalen Netzen eingesetzt werden. Die beschriebenen IPv6-Port-ACLs schützen vor dem böswilligen Einsatz dieser Software.



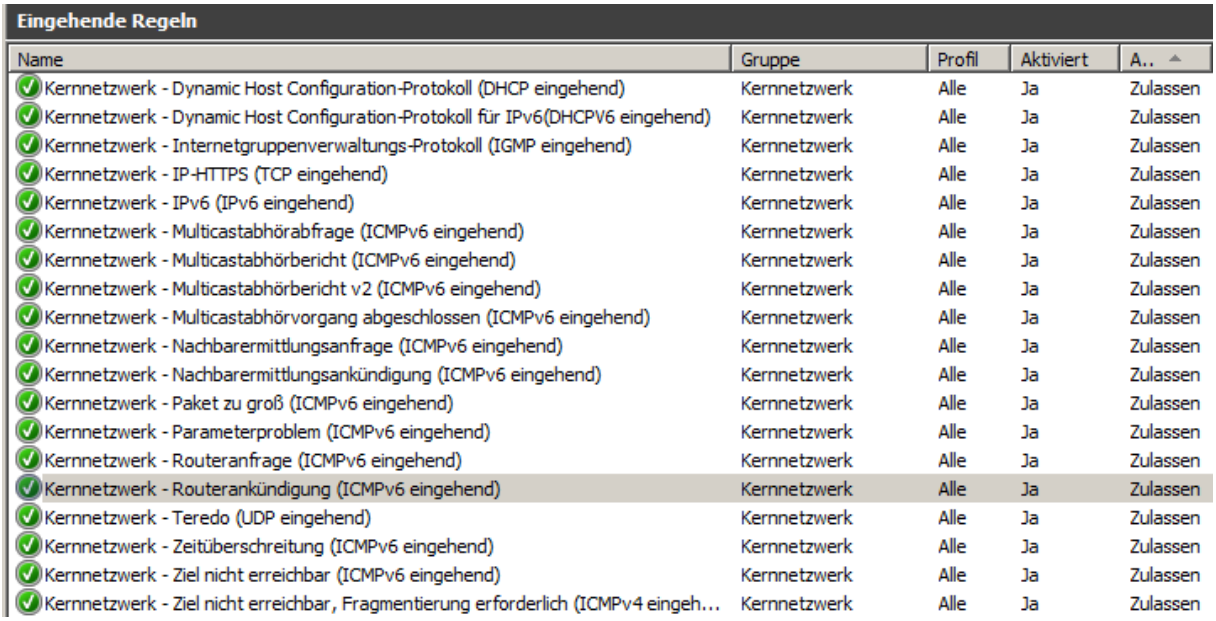
Personal Firewalls verschiedener Hersteller zeigen im Umgang mit IPv6 wenig Überzeugendes. Insbesondere die Behandlung von Tunnel-Protokollen zeigte sich bei Tests unzureichend. Soweit vom Protokoll-Design her überhaupt möglich, können die hier genannten Implementierungen Angriffe auf NDP, z.B. über ICMPv6 Redirects, mindern. Hier kann zur Konfiguration der RFC 4890 ‚Recommendations for Filtering ICMPv6 Messages in Firewalls' als Anleitung herangezogen werden.

Im Bereich der Personal Firewall ist die Microsoft-Firewall, die sowohl IPv4 als auch IPv6 Stateful Inspection bietet und die Transition Technologies korrekt behandelt, zu empfehlen. Bei Bedarf können hier für stationäre Host-Systeme ICMPv6-Pakete und damit Angriffe auf die NDP-Mechanismen gefiltert werden. Denkbar ist beispielsweise eine Regel, die den Empfang von Router Advertisements auf bekannte administrativ zugewiesene Link-Local-Adressen reduziert. Nachteilig ist allerdings der erhebliche Aufwand. Eine Verbesserung wäre allerdings in Form einer Weiterentwicklung der

[14] Denial of Service

bisherigen *Netzwerkerkennung* denkbar, um eine persistente Bindung zwischen den Adressen (Layer 2 und Layer3) eines regulären Routers und der Windows-Firewall einmalig pro Subnetz einzurichten.

Hier noch zur Illustration die Anzeige der in Windows 7 verfügbaren ICMPv6-Filter:



Eingehende Regeln

Name	Gruppe	Profil	Aktiviert	A..
Kernnetzwerk - Dynamic Host Configuration-Protokoll (DHCP eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Dynamic Host Configuration-Protokoll für IPv6(DHCPV6 eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Internetgruppenverwaltungs-Protokoll (IGMP eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - IP-HTTPS (TCP eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - IPv6 (IPv6 eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Multicastabhörabfrage (ICMPv6 eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Multicastabhörbericht (ICMPv6 eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Multicastabhörbericht v2 (ICMPv6 eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Multicastabhörvorgang abgeschlossen (ICMPv6 eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Nachbarermittlungsanfrage (ICMPv6 eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Nachbarermittlungsankündigung (ICMPv6 eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Paket zu groß (ICMPv6 eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Parameterproblem (ICMPv6 eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Routeranfrage (ICMPv6 eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Routerankündigung (ICMPv6 eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Teredo (UDP eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Zeitüberschreitung (ICMPv6 eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Ziel nicht erreichbar (ICMPv6 eingehend)	Kernnetzwerk	Alle	Ja	Zulassen
Kernnetzwerk - Ziel nicht erreichbar, Fragmentierung erforderlich (ICMPv4 eingeh...	Kernnetzwerk	Alle	Ja	Zulassen

Linux-Administratoren können ab Kernel 2.6.20 mit ip6tables ebenfalls eine Stateful Inspection konfigurieren und erhalten bei Aufruf von

```
ip6tables -p icmpv6 -h
```

eine Aufstellung, welche Möglichkeiten zur Filterung von ICMPv6 und insbesondere NDP vorhanden sind. Im folgenden Beispiel werden ICMPv6 Redirect Meldungen geblockt:

```
ip6tables -A INPUT -p icmpv6 --icmpv6-type redirect -j DROPs
```

Durch die folgenden Maßnahmen verliert ein IPv6 Host die Fähigkeit zur Stateless Address Autoconfiguration (SLAAC) – ein wesentlicher funktionaler Bestandteil des IPv6-Protokolls. Die Vorgehensweise sei daher auch nur der Vollständigkeit halber dargestellt und sollte nur in begründeten Ausnahmefällen als Schutzmaßnahme (z.B. Server-Betrieb in externen Standorten) angewendet werden.

Die Verarbeitung von Router Advertisements und damit insbesondere SLAAC kann in den Microsoft Windows Betriebssystemen pro Netzwerkadapter wie folgt deaktiviert werden:

```
netsh interface ipv6 set interface „IfIndex“ routerdiscovery=disabled
```

```
netsh interface ipv6 set interface „IfIndex“ routerdiscovery=disabled store=persistent
```

Linux-Administratoren können im Bedarfsfall die Autokonfiguration eines Netzwerkadapters, hier am Beispiel eth0, durch einen Eintrag in die Datei /etc/sysctl.conf deaktivieren:

```
net.ipv6.conf.eth0.autoconf = 0
```

Diese Zeile verhindert lediglich die Stateless Address Autoconfiguration. Mögliche Default Router übernimmt der Hosts weiterhin aus den Router Advertisements. Um die Verarbeitung von Router Advertisements komplett abzuschalten, kann in /etc/sysctl.conf die Zeile

```
net.ipv6.conf.eth0.accept_ra=0
```

eingetragen werden. Der Default Router muss in diesem Fall bekannt sein und bei der manuellen IPv6 Konfiguration eingetragen werden.

Zur Absicherung von Subnetzen, insbesondere solcher, die derzeit nur IPv4 Funktionalität haben, kann ein NDPMON[15]-Server installiert werden, der eine Historie über die Zuordnung von RFC3041 IPv6 Adressen und MAC-Adressen liefert sowie über Rogue Router Advertisements informiert. Als Rogue Router treten nach bisherigen Erfahrungen in der Regel Windows Rechner mit aktivem Internet Connection Sharing (ICS) in Erscheinung. Unverzichtbar sind in Zukunft auf neuen Layer 2 Switch-Komponenten Funktionen wie

- IPv6 RA Guard
- IPv6 ND Inspection
- Device Tracking

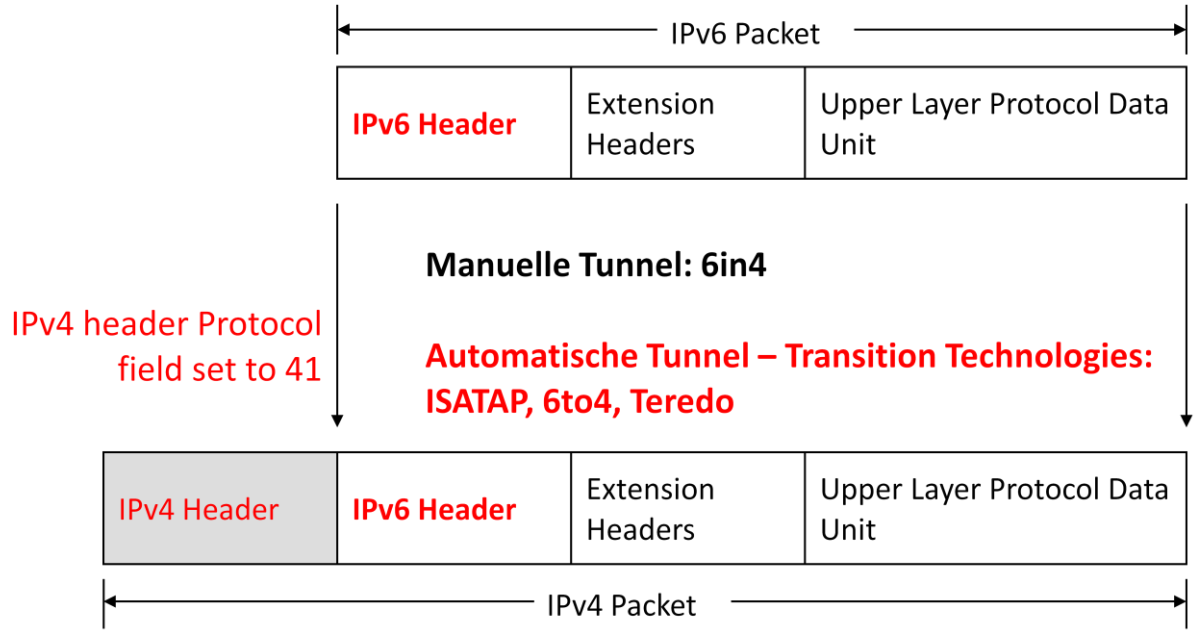
Welche Kombinationen aus ICMPv6 Header, Fragment Header, Destination Option Header und Hop by Hop Option überhaupt sinnvoll sind, ist seitens der IETF zu überdenken. Hier kann eine Vereinfachung des Standards die Situation entschärfen. Als Beispiel sei hier auf die erfolgreiche Vorgehensweise im Fall der Routing Type Header 0 Unterstützung (RFC 5095 ‚Deprecation of Type 0 Routing Headers in IPv6') hingewiesen.

Wichtig ist jedoch weiterhin eine angemessene Strukturierung im lokalen Netz, um eventuelle Störungen oder Angriffsversuche regional einzudämmen.

[15] Neighbor Discovery Protocol Monitor

IPv6 Transition Technologies – Risiken und Gefahren

Wurde *native* IPv6 bis zu dieser Stelle im Netzwerkmanagement und im IT-Sicherheitsprozess außer Acht gelassen, so werden durch die von Microsoft automatisch aktivierten Tunneltechnologien wie ISATAP[16], 6to4 oder Teredo neue latente Gefährdungen in die Kommunikationsnetze getragen. Dabei ist insbesondere eine intensive Wechselwirkung mit dem etablierten IPv4-Netz unübersehbar, da alle diese Technologien den IPv6-Datenverkehr in IPv4 tunneln und somit das alt hergebrachte IPv4 Netz als Link Layer Technologie betrachten.

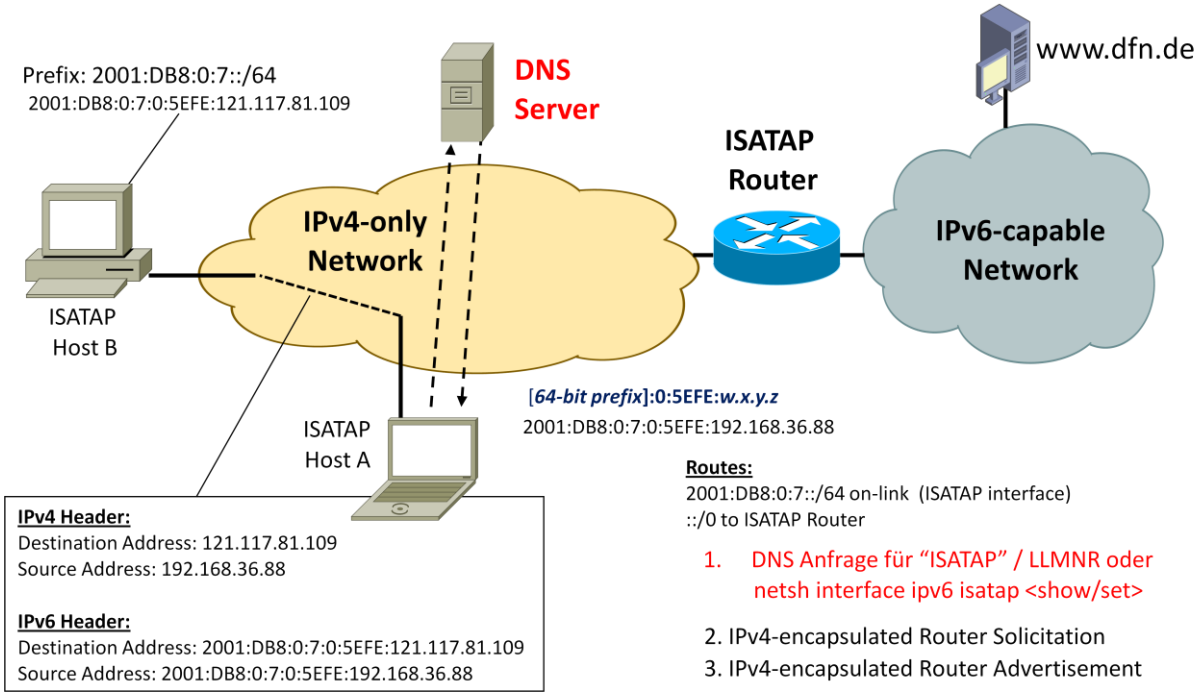


Es gibt aber auch Varianten mit GRE, IPSEC oder UDP Encapsulation

IPv6 Tunnel Encapsulation

[16] Intra-Site Automatic Tunnel Addressing Protocol

ISATAP- Intra-Site Automatic Tunnel Addressing Protocol



Wird keine *native* IPv6 Konfiguration nach dem Durchlaufen der Stateless Address Autoconfiguration ermittelt, versuchen die Microsoft Betriebssysteme einen ISATAP-Tunnel zu konfigurieren. Der sogenannte ISATAP-Router wird im IPv4-Netz (Intranet oder Internet) kontaktiert. Wesentlich ist dabei, dass im die Auflösung des Host-Namens ***isatap*** eine gültige IPv4 Router-Adresse liefert. Danach wird wie gewohnt, jedoch als IPv4 Unicast, über Router Solicitation (RS) und Router Advertisement (RA) ein Tunnel mit IPv6-Adresse konfiguriert. Wesentliche Merkmale sind

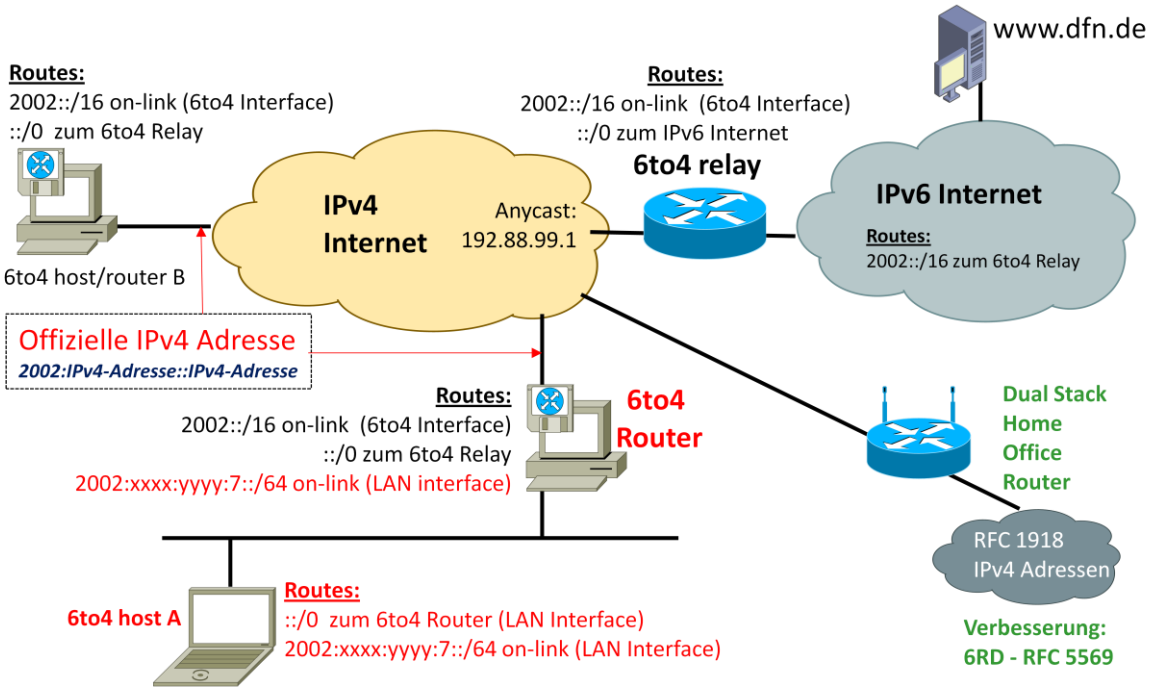
- das Intranet oder Internet arbeiten als Link-Layer für IPv6
- Tunnel Mode 6in4 – also Protocol 41
- Die ISATAP-Hosts sind adjazent zu *native* IPv6-Netzen (sogar weltweit)

Die Auflösung des Host-Names kann durch DNS-Server, LLMNR oder lokale Einträge (Hosts-Datei) erreicht werden. Es ergeben sich die schon skizzierten Angriffspunkte im Bereich DNS / LLMNR. Eine mögliche ISATAP Konfiguration für Cisco Router zeigt das folgende Beispiel:

```
interface Tunnel6
        description ISATAP Tunnel
        no ip address
        no ip redirects
        ipv6 address 2001:db8:4711:7500::/64 eui-64
        ipv6 enable
        no ipv6 nd suppress-ra
        ipv6 ospf cost 1
        ipv6 ospf 1 area 52425
        tunnel source FastEthernet0
        tunnel mode ipv6ip isatap
```

6to4 - Connection of IPv6 Domains via IPv4 Clouds

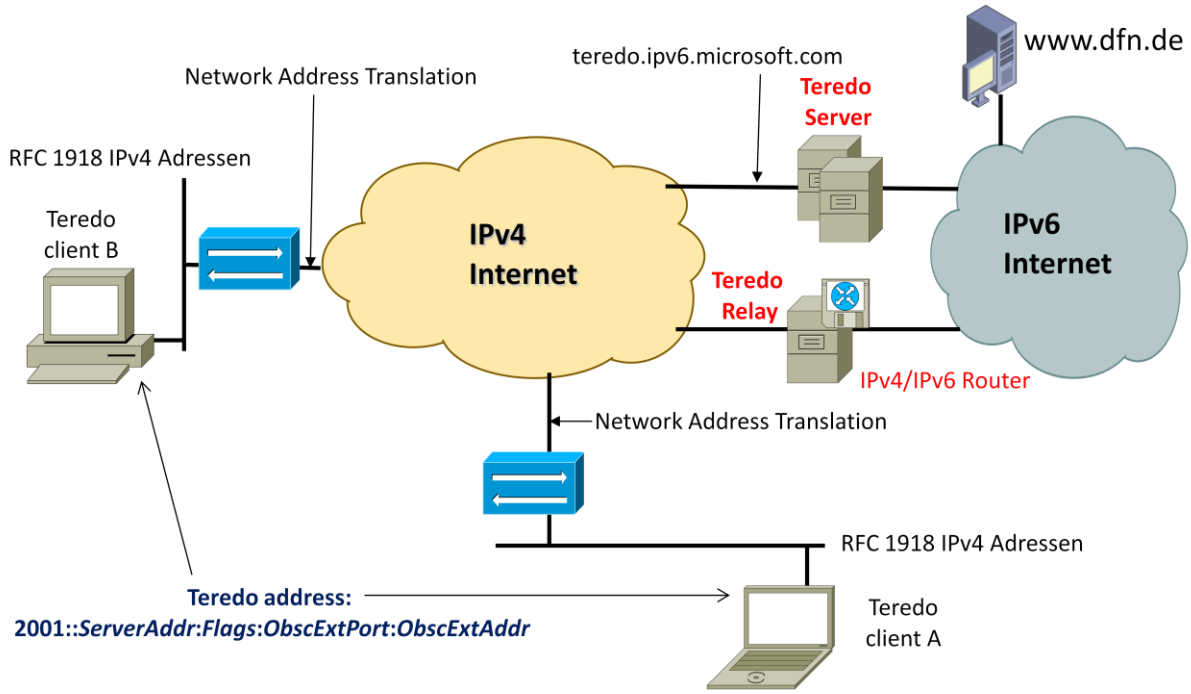
In jedem Intranet mit offiziellen IPv4-Adressen (Class A / Class B / Class C) können Hosts eine sogenannte 6to4-Adresse generieren, die aus dem IPv6-Prefix 2002::/16 und der offiziellen IPv4-Adresse besteht. Damit sind alle Hosts in einem Intranet lokal adjazent und haben zudem über das IPv4-Protokoll 41 (IPv6-in-IPv4) Zugriff in das weltweite IPv6-Netz. Diese Komponente wird automatisch aktiv (Microsoft Windows), falls weder die *native* Autoconfiguration noch ISATAP eine IPv6 Konnektivität herstellen konnten. Zentrale Sicherheitsmaßnahmen, wie z.B. Firewalls, die den Transport dieses Protokolls nicht unterbinden, sind somit auch nicht in der Lage, die Sicherheit des Netzes in einem ausreichenden Maße zu gewährleisten. Welches zusätzliche Potenzial in diesem Mechanismus steckt, zeigt die Kombination aus Internet Connection Sharing (ICS) und 6to4: Aktiviert ein Windows Benutzer ICS, wird das System zum 6to4-Host-Router und verteilt im lokalen Netz Router Advertisements, wodurch dieses System zum aktiven IPv6-Router im lokalen Netz wird, der eine Verbindungen zwischen Intranet und INTERNET herstellen kann.



Im Home Office Bereich kann mit Hilfe dieser Technik auf einfache Weise eine Anbindung an das weltweite IPv6-Netz erfolgen. Verschiedene Internet-Service-Provider bieten mit 6RD – IPv6 Rapid Deployment nach RFC 5569 eine optimierte Weiterentwicklung zur Nutzung an. Home Office Router wie die neueren AVM-Modelle unterstützen diese Zugangstechnik.

Teredo

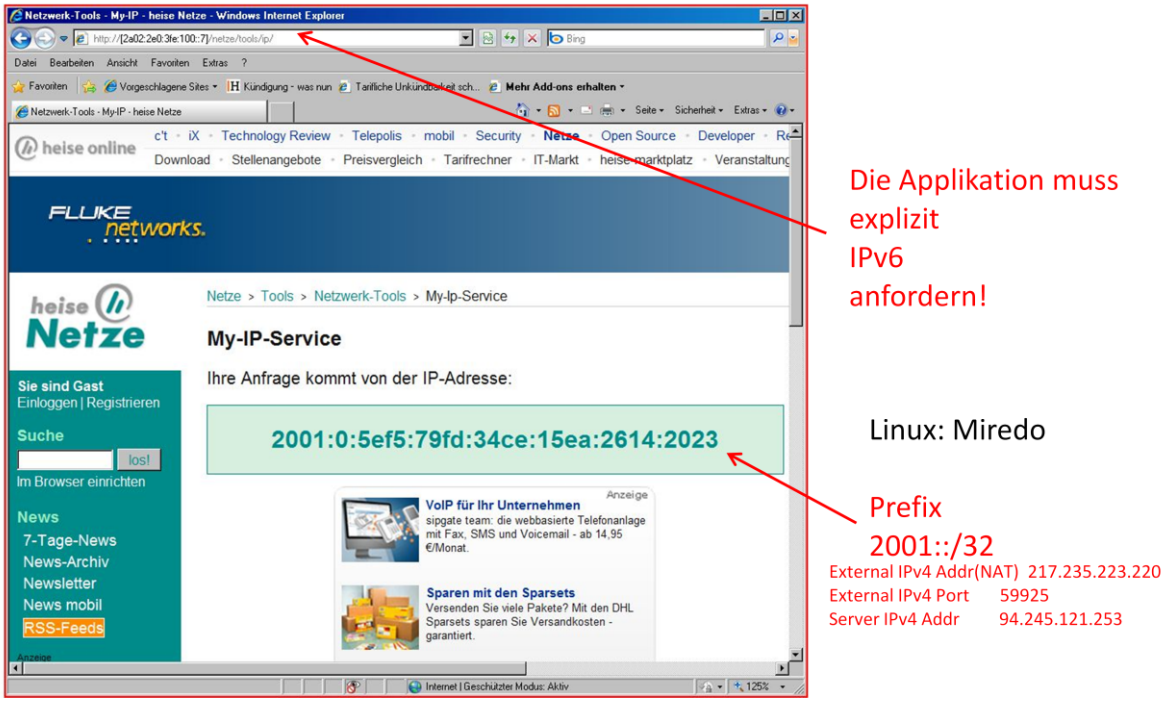
Um auch in NAT-Umgebungen im Bedarfsfall IPv6-Konnektivität bereitstellen zu können, ist als sogenannte Last Resort Transition Technologie nach RFC 4380 ‚Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)' in den Microsoft Betriebssystemen installiert. Als Open Source Lösung steht für die verschiedenen LINUX-Distributionen das Paket MIREDO zur Verfügung.



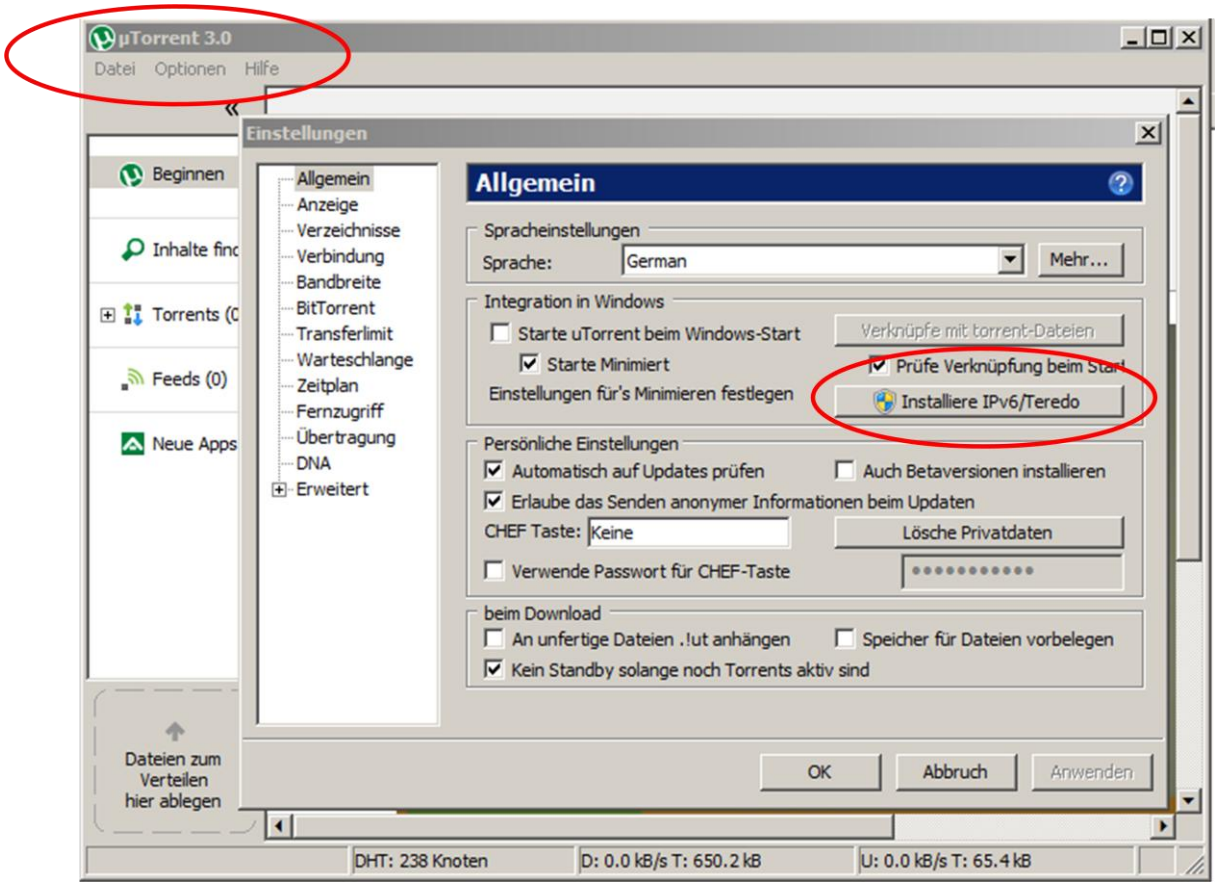
Durch Angabe einer **expliziten IPv6-Adresse als Ziel** wird die Teredo-Komponente aktiv und öffnet mit Unterstützung externer Server durch sogenannte Bubble-Packets die nötigen Ports in den NAT-Geräten (lokaler NAT-Router, Firewall). Damit sind die Hosts als IPv6-System weltweit erreichbar und NAT ist als Barriere zwischen Internet und lokalem Netz ausgehebelt. Die Teredo-Komponente wird nur auf explizite Anforderung hin aktiv, falls bis dahin keine IPv6-Konfiguration (SLAAC, ISATAP, 6to4) abgeschlossen werden konnte.

Der Verkehr erreicht über externe Teredo Relays das jeweilige Ziel. Hier ist im lokalen Netzwerk keine direkte IPv6-Kommunikation zu sehen, da die Übertragung in IPv4-UDP (Port 3544) gekapselt wird. Durch die in der IPv6-Adresse des Client kodierten IPv4-Informationen (IPv4-Adresse des Servers / NAT-Typ/Externer IPv4 Port / Externe IPv4-Adresse) kann der bidirektionale Verkehrsfluss mittels IPv4-UDP vom Client über ein Relay zum externen IPv6-Rechner ermöglicht werden.

Die folgende Abbildung zeigt einen Zugriff über IPv6 aus einem lokalen IPv4-Netz mit RFC 1918 Adressen auf ein externes Web-Angebot durch direkte Eingabe der Zieladresse:

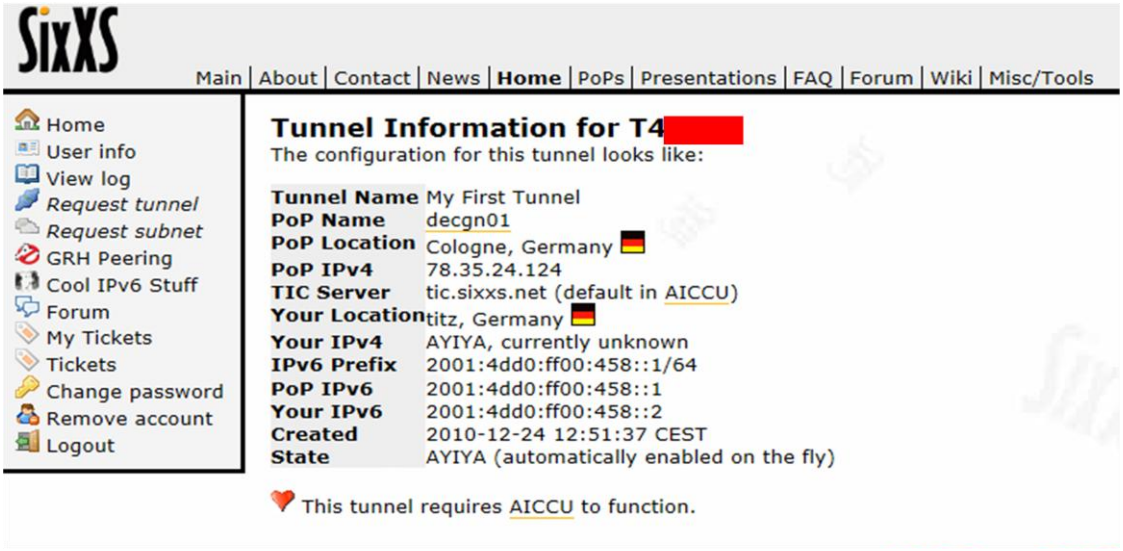


Auch bleibt festzuhalten, dass kollaborative Filesharing-Protokolle ebenfalls den Teredo-basierten Transfer nutzen können:



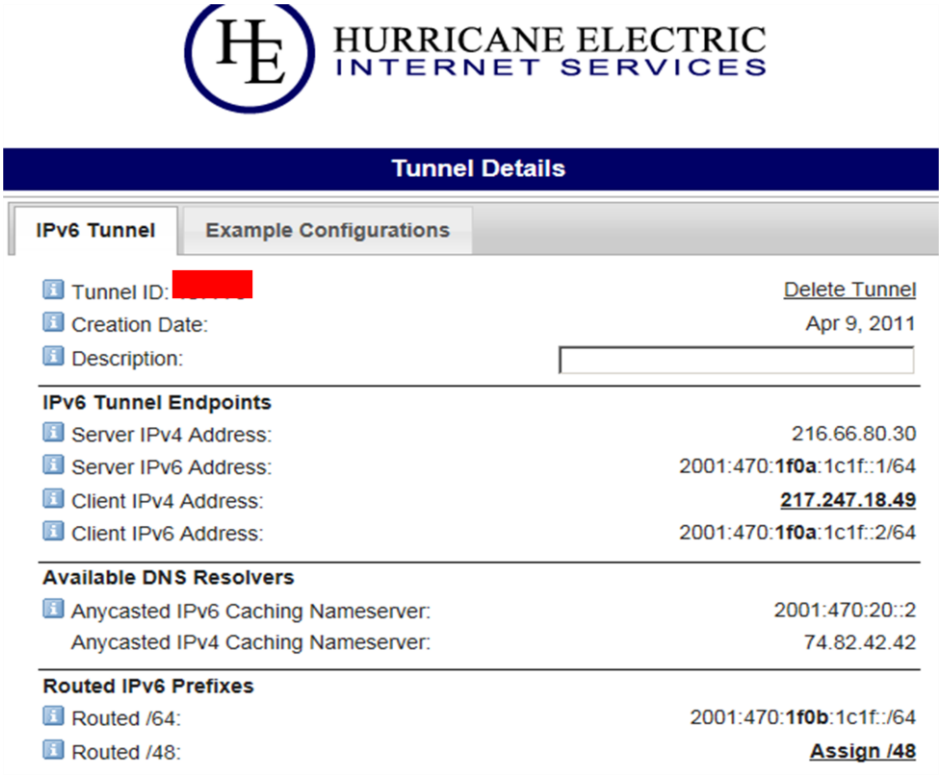
Tunnel Broker

Neben den bisher betrachteten Tunnel-Mechanismen bieten sogenannte Tunnel Broker weitere Möglichkeiten der IPv6-Anbindung.



... nutzt UDP Port 5072!

Die Übertragungsvarianten nutzen oftmals UDP oder 6in4 um einen Router oder ein Relay des jeweilgen Anbieters zu erreichen. Wiederum besteht die Gefahr, dass unbedarfte Anwender Verbindungen des lokalen Netzes im Unternehmen zum weltweiten IPv6-Internet herstellen. Die Tunnel-Broker weisen in der Regel nach einer Registrierung dem Kunden großzügig IPv6-Prefixe zu. Dieser kann wiederum durch einen Rogue Router diesen Adressraum im lokalen Netz verteilen und als illegaler Router zum weltweiten IPv6-Netz agieren.



Rogue Tunnel - Gefahren

Durch die Kapselung der Übertragung in IPv4 sind die Kommunikationsbeziehungen schwer aufzudecken und zu unterbinden. Firewall-Regeln, die augenscheinlich Punkt-zu-Punkt Verbindungen erlauben und Freischaltungen für bestimmte Ports regeln, sind vor diesem Hintergrund neu zu betrachten. Ungewollt und unbemerkt entstehen auf Netzwerkebene sogar weltweite Adjazenzen, welche die etablierte Sicherheitspolicy untergraben können.

Im Intranet kann es zu ungewollten Umleitungen von Datenströmen über weniger geeignete Teilstecken kommen, die letztlich natürlich auch in einer MITM[17]-Attacke gipfeln können.

Treffen verschiedene Bedingungen wie eine nicht administrierte Namensauflösung, fehlkonfigurierte Hosts mit Windows ICS und eine nur auf IPv4 ausgerichtete Firewall-Policiy aufeinander, können die Folgen gravierend sein.

Lösungen

Sind die Hosts in einem verwalteten IPv6-Subnetz, d.h. der IPv6 Betrieb ist organsiert und reguläre Router verteilen die Advertisements, werden die Microsoft-Tunnel nicht aktiv! Diese Tatsache ist ein gewichtiges Argument für ein natives IPv6 Deployment.

Ansonsten ist zu empfehlen, die Tunnel abzuschalten. Der **System-Administrator** führt zum Abschalten der Microsoft-Tunnel folgende Befehle aus:

```
netsh interface ipv6 6to4 set state disabled undoonstop=disabled

netsh interface ipv6 isatap set state disabled

netsh interface ipv6 set teredo disable
```

und Neustart

Falls die Windows Systeme Mitglied einer Domäne (Active Directory) sind, können die Einstellungen zentral verwaltet werden (AD GPO):

Computer Configuration > Policies

> Administrative Templates > Network > IPv6 Configuration

Mögliche Pv6 Einstellungen:

Enable all IPv6 components (Windows default)
Disable all IPv6 components
Disable 6to4
Disable ISATAP

[17] Man in the Middle (Angriffsform in Netzwerken)

Disable Teredo
Disable Teredo and 6to4
Disable all tunnel interfaces
Disable all LAN and PPP interfaces
Disable all LAN, PPP and tunnel interfaces
Prefer IPv4 over IPv6.

Weiterhin sollte das Protokoll 6in4 (Protokoll Number 41) sowie die Teredo Kommunikation (IPv4 UDP 3544) in Firewalls und Routern geblockt werden.

Fazit

Aufgrund der Erfahrungen aus dem lokalen Unternehmenswerk stellt sich IPv6 zunächst als eine Zusatzbelastung für die Netzadministration dar. Allerdings ergeben sich durch die latenten Gefährdungspotenziale und die de facto Nutzung des Protokolls Notwendigkeiten für Schulung und Training von Administratoren und Benutzern. Gleichermaßen ist eine zentral koordinierte Einführung des neuen Protokolls von großer Bedeutung für den weiteren störungsfreien Betrieb des Netzes. Wegen der Komplexität sollte der Zeitfaktor nicht unterschätzt werden und frühzeitig mit den Planungen begonnen werden. IPv6 zu ignorieren ist gefährlich für die Sicherheit des Unternehmensnetzwerks, da IPv6 Netzfunktionen auch auf Basis von IPv4 genutzt werden können.

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