FORSCHUNGSZENTRUM JÜLICH GmbH

Jülich Supercomputing Centre
52425 Jülich, ☎ (02461) 61-6402

JuNet-Helpdesk, ☎ (02461) 61-6440

Technische Kurzinformation

FZJ-JSC-TKI-0412
W.Anrath, S.Werner, E.Grünter
17.01.2023

IPv6 im JuNet
Information für Systemadministratoren

1. Einleitung

IPv6 ist ein neues Netzwerkprotokoll, das die stetig wachsende Nachfrage nach IP-Adressen im weltweiten Internet durch Erweiterung der Adresslänge von 32 Bit auf 128 Bit löst. Die 128 Bit lange Adresse besteht aus einem 64 Bit langen Netzwerk-Prefix (Subnetz) und einem 64 Bit langen Interface Identifier und wird hexadezimal dargestellt.

Auf Wunsch kann im JuNet in benannten physikalischen Subnetzen IPv6 Konnektivität angeboten werden. Beispiele für mögliche Netzwerk-Prefixe wären

2001:638:404:1200::/64 (gleichwertig: 2001:0638:0404:1200::/64)
2001:638:404:9999::/64 (gleichwertig: 2001:0638:0404:9999::/64)

Dabei entspricht der FZJ IPv6-Prefix **2001:638:404**::/48 funktional dem IPv4-Netz 134.94.0.0/16.

IPv6 wird dabei als Zusatz angeboten, d.h. IPv6-fähige Systeme im JuNet erhalten zusätzlich zur gewohnten IPv4-Adresse eine global gültige IPv6-Adresse:

2001:0638:0404:nnnn:iiii:iiii:iiii:iiii

Konkret könnte also eine solche IPv6-Adresse den Wert

2001:638:404:9999:0a:00:2b:ff:fe:21:32:43

haben. (Dabei ist *nnnn* die Subnetz-Nummer und *iiii* der Interface Identifier.)

Diese Betriebsart wird Dual Stack genannt. Dual Stack Hosts können sowohl mit IPv4-Systemen als auch mit IPv6-Systemen im Internet kommunizieren. Die **Host-Konfiguration** der IPv6-Adresse und der Routing-Einträge erfolgt in der Regel automatisch durch die sogenannte Stateless Address Autoconfiguration (SLAAC). Die manuelle statische Adressierung ist nur in speziellen Server-Netzen oder DMZs möglich; die erforderlichen IPv6-Konfigurationsparameter werden in diesem Fall vom Systemadministrator manuell konfiguriert.

Falls im physikalischen Subnetz einer Organisationseinheit IPv6 genutzt werden soll, kann durch eine Hausmitteilung (IT-Beauftragter) der Bedarf angemeldet werden. Das JSC bietet den jeweiligen IT-Verantwortlichen zur Unterstützung der Einführung ein technisches Briefing an.

Für alle Hosts mit IPv6-Unterstützung in einem solchen physikalischen Subnetz wird die globale IPv6-Adresse nicht explizit beantragt (Ausnahme: spezielle Server). Die nötigen Interface Identifier (IID) werden bei der IPv6 Autoconfiguration (SLAAC) durch eine Transformation der MAC-Adresse (modified-EUI-64 Interface ID) oder ‚Pseudorandom Functions' (Stable-Privacy oder Privacy Extensions) erzeugt und ergeben verknüpft mit dem Subnetz-Prefix eine global gültige IPv6-Adresse. Option: Für bestimmte Anwendung (z.B. optionaler DNS- oder Firewall Eintrag) müssen Hosts, die im Auslieferungszustand Pseudozufallszahlen (Stable Privacy oder Privacy Extensions) als Interface Identifier generieren, einmalig so konfiguriert werden, dass der Interface Identifier nach dem sogenannten EUI-64 Verfahren (IEEE-Standard) bestimmt wird.

2. IPv6 Grundeinstellungen der Dual Stack Hosts

Neben den Microsoft Betriebssystemen unterstützen auch die bekannten LINUX-Varianten und macOS (Apple) das IPv6-Protokoll parallel zum etablierten IPv4-Protokoll. Entscheidend ist dabei, dass das IPv6 Protokoll in den unterschiedlichen Betriebssystemen installiert und standardmäßig aktiviert ist, so dass die Systeme im Dual-Stack-Betrieb am Netzwerk kommunizieren. Dem IPv6-Standard entsprechend, führen alle Systeme nach der Initialisierung eine IPv6-Autokonfiguration (SLAAC) durch und erhalten so automatisch eine globale feste eindeutige IPv6-Adresse. Die Erzeugung dieser Interface Identifier folgt offiziell definierten und vorgegebenen Internet-Standards. Die Bezeichnung ‚Stable-Privacy' weist auf einen Interface-Identifier nach dem neueren Standard RFC 7217 hin, der als Nachfolger der EUI-64 Methode, beschrieben in RFC 4291, mittlerweile in fast allen Betriebssystemen favorisiert wird. Zusätzlich generieren die meisten Betriebssysteme für ausgehende Verbindung zyklisch temporäre IPv6 Adressen (Stichwort: Privacy Extensions) nach vorgegebenen Standardverfahren (RFC 4941 u. RFC8981).

Optional: Die Adressen der IPv6 Autokonfiguration müssen mit den bekannten Hardware-Adressen der JuNet-Datenbank für ausgewählte Szenarien wie die Erstellung optionaler DNS-Einträge (AAAA-Records) oder für Firewall-Freischaltungen derzeit noch synchron sein (modified-EUI-64 Interface Identifier) - dazu sind je nach Betriebssystem verschiedene Anpassungen nötig. Für die gängigen Betriebssysteme kann die geforderte modified-EUI-64 Interface Identifier Einstellung durch den System-Administrator konfiguriert werden.

Als **Windows 10 Administrator** sind im Bedarfsfall folgende Befehle ausführen:

```
netsh interface ipv6 set privacy state=disabled  store=persistent
netsh interface ipv6 set global  randomizeidentifiers=disabled  store=persistent
- danach bitte die  Hinweise  -IPv6 Sicherheit-  beachten  und einen Neustart initiieren -
```

In aktuellen **macOS (Apple)** sind sogenannte Opaque Interface Identifiers (IETF RFC 7217) aktiv. Diese Voreinstellung kann aktuell und zukünftig auf ARM64-Archtekturen im installierten macOS Betriebssystem nicht rekonfiguriert werden.

Bei den diversen **LINUX** sind im Bedarfsfall die Voreinstellungen anzupassen.

SUSE Linux Enterprise 15 wird mit aktiven Privacy Extensions ausgeliefert. Diese können durch folgende Einträge in /etc/sysctl.conf abgeschaltet werden:

```
net.ipv6.conf.all.use_tempaddr = 0
net.ipv6.conf.default.use_tempaddr = 0
```

Die ab **Ubuntu 16.04 LTS (-> 18.04 - 20.04 LTS / CentOS 8.1)** eingesetzte NetworkManager-Version generiert sogenannte Opaque Interface Identifiers (IETF RFC 7217). Daher sind bei Bedarf zum Wechsel auf EUI-64 Interface Identifier folgende Schritte auszuführen - Beispiel:

```
nmcli   conn    show                !! zeigt den Namen , hier im Bsp.:  'Wired connection 1'
nmcli   conn    edit    'Wired connection 1'
nmcli>  save
nmcli>  set  ipv6.addr-gen-mode eui64
nmcli>  set  ipv6.ip6-privacy    0
nmcli>  save
```

3. IPv6 Sicherheit

Diese Empfehlungen gelten unabhängig von der Teilnahme am IPv6-Betrieb im JuNet.

macOS

Aktivieren Sie bitte die Application Firewall:

Systemeinstellungen -> Persönlich -> Sicherheit -> Firewall

Linux

Eine ausführliche Anleitung zur Konfiguration eines Firewall-Regelwerks mittels *IP6TABLES* enthält die TKI-0402. (Bitte beachten Sie, dass *IPTABLES-Regeln* nicht für die IPv6-Kommunikation gelten.)

Zur ersten Illustration werden hier einige Beispiele zur Kontrolle des SSH-Zugriff gezeigt:

```
# Allow SSH Clients / list REMOTE LANs (Syntax:  PREFIX::/64)
#
ip6tables -A INPUT -p tcp -s 2001:638:404:1000::/64 --dport 22 -j ACCEPT
ip6tables -A INPUT -p tcp -s 2001:638:404:2000::/64 --dport 22 -j ACCEPT
ip6tables -A INPUT -p tcp -s 2001:638:404:3000::/64 --dport 22 -j ACCEPT
#
ip6tables -A INPUT -p tcp --dport 22 -j REJECT
```

Windows 10

Die Betriebssysteme Windows 8 / 10 versuchen automatisch IPv6-Tunnel zu starten. Dieser Mechanismus ist unabhängig von den IPv6 LAN-Einstellungen. Also: Auch bei deaktiviertem IPv6 für die LAN Anbindung sind die Tunnel aktiv!

Generell gilt, dass dies keine Besonderheit der Netzkonfiguration im FZJ ist. Wird ein derartiger Tunnel aktiv, ist das System als IPv6 Ziel erreichbar. Es wird daher empfohlen, diese Tunnel abzuschalten - insbesondere auf Laptops.

Der **System-Administrator** führt dazu 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
```

- danach REBOOT -

Zur weiteren Absicherung ist die Windows Firewall zu empfehlen.

4. IPv6 Betrieb – Status und Diagnose

Nachfolgend die wichtigsten hilfreichen Befehle zur Kontrolle und Diagnose der IPv6-Umgebung:

Windows 10

ipconfig /all	alle Interface Details anzeigen
ping ::1	IPv6 Protokoll Host intern testen (localhost)
netsh interface ipv6 show interface	Interface Status (alle) und IPv6-Adressen
netsh interface ipv6 show address	IPv6 Adressen inklusive Gültigkeitsdauer anzeigen
netsh interface ipv6 show privavy netsh interface ipv6 show global	Konfigurationseinstellung Privacy Extensions
netsh interface ipv6 show route route print -6	IPv6 Routing-Tabelle auflisten
netsh interface ipv6 show neighbors	Zuordnung IPv6-Adressen zu MAC-Adressen
netsh interface ipv6 show destination	Destination Cache inkl. PMTU-Werte
netsh interface ipv6 dump	alle Änderungen aufzeigen
netsh interface ipv6 reset	alle Änderungen zurücksetzen

Linux

ifconfig -a	alle Interface Details anzeigen
ifconfig eth0 | grep inet6	ETH0 - nur IPv6 Adressen
ping6 ::1	IPv6 Protokoll Host intern testen (localhost)
ip -6 address show	IPv6 Adressen inklusive Gültigkeitsdauer anzeigen
ip -6 maddr show	Multicast-Gruppen anzeigen
ip -6 route show route -A inet6 -n	IPv6 Routing-Tabelle auflisten
ip -6 neighb show	Zuordnung IPv6-Adressen zu MAC-Adressen
ip -6 route get to {ipv6_addr}	Route Cache inkl. PMTU-Wert

test -f /proc/net/if_inet6 && echo IPv6 Module aktiv

macOS

ifconfig -a	alle Interface Details anzeigen
ifconfig -L	zeigt die Gültigkeitsdauer der Adressen
ping6 ::1	IPv6 Protokoll Host intern testen (Loopback)
traceroute6 *ipv6-host*	
netstat -rnf inet6	Routing Einträge anzeigen
netstat -f inet	aktive IPv6 Verbindungen anzeigen
netstat -g	Multicast-Gruppen anzeigen
ndp -a	Zuordnung IPv6-Adressen zu MAC-Adressen
dscacheutil -flushcache	DNS Cache leeren

Ab Version 10.7 stehen folgende Befehle zur Verfügung:

nettop -n -m route	Routing Statistics in Echtzeit anzeigen
nettop -n	TCP & UDP Sockets in Echtzeit anzeigen

5. IPv6 Server-Dienste im JuNet

Nach der Stateless Address Autoconfiguration oder gegebenenfalls der manuellen IPv6-Konfiguration kann ein Host IPv6 als Kommunikationsprotokoll nutzen. Sind beide Kommunikationspartner IPv6-fähig, wird dieses Protokoll anstelle von IPv4 bevorzugt. Da jedoch in der Regel Dienste immer über vollqualifizierte Host-Namen und nicht direkt über die numerischen Adressen angesprochen werden, ist dazu ein entsprechender Eintrag im DNS nötig. Dieser Eintrag, der sogenannte AAAA-Record, verbindet den vollqualifizierten Hostnamen mit der 128 Bit langen IPv6 Adresse des Host. Solche Einträge müssen vom jeweiligen Systemadministrator explizit beantragt werden (JuNet-Portal).
Dabei ist folgende Vorgehensweise zu empfehlen:

- Betriebssystem: IPv6 aktiv ?
  - Loopback Adresse: ping ::1
- Netzwerk Interface: IPv6 aktiv?
  - Link Local Address fe80::*eui-64* vorhanden?
  - FZJ Global Unicast Address: 2001:638:404:*subnet:eui-64* vorhanden?
- Lokale IPv6 Firewall Regeln prüfen und gegebenenfalls anpassen?
- Applikationen (sshd/rdp..) – IPv6 Socket aktiv?
  - netstat -an
- Applikations Access Controls prüfen
- Teste Dienste/Services über die IPv6-Adresse (2001:638:404…..)
- IPv6 Adresse im DNS registrieren: **JuNet-Portal-Änderungsformular: AAAA-Record registrieren** (Folge: AAAA- und PTR-Record werden aktiv)
- Teste Dienste/Services über IPv6 (Hostname AAAA-Record)

6. IPv6 – Manuelle Konfiguration in DMZs und Server-Subnetzen

Durch die folgenden Maßnahmen verliert ein Host die Fähigkeit zur Stateless Address Autoconfiguration (SLAAC). Mögliche Anwendungsbeispiele sind FZJ-weite Server, deren IPv6-Adresse im DNS registriert werden soll und die Bindung des Hostnamens an die IPv6-Adresse über die Lebensdauer einer Ethernet-MAC-Adresse hinaus gelten soll (z.B. MS Active Directory Domain Controller).

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 Routes‘ übernimmt der Host 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. Im Anhang ist ein Beispiel (Ubuntu 18.04 LTS Server) zu finden.

Die für die Konfiguration erforderliche feste IPv6-Adresse kann im JuNet-Portal per Änderungsformular für das jeweilige Host-System beantragt werden. Das Freitextfeld ist mit der Bemerkung ‚IPv6-Antrag‘ auszufüllen. Zum Ende der Bearbeitung (vgl. ‚Kapitel 5‘) kann der IPv6 DNS Eintrag beauftragt werden; im Änderungsformular bitte dazu im Freitextfeld die Bemerkung ‚AAAA-Record registrieren‘ eintragen (-> AAAA- und PTR-Record werden erzeugt).

Anhang A: Ablauf der Stateless Address Autoconfiguration

Die Implementierung dieser Technik ist für jeden IPv6 Host verpflichtend und ist hier als Hintergrundinformation für die Systemadministratoren in Kurzform dargestellt. 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‘ (Internet Standard) folgende Stufen:

- Link-Local Address (Interface Identifier) generieren
    - Kommunikation im lokalen Subnetz ist möglich

- Prüfung: Duplicate Address Detection (DAD)
- Autoconfiguration abbrechen, falls Prüfung scheitert
- IPv6 Konfiguration für das Subnetz anfragen (Router Solicitation)
- FZJ Global Unicast Address generieren : verknüpfen von Subnetz-Information (Prefix) mit dem Interface Identifier
    - Kommunikation möglich : JuNet und Internet

Anhang B: Manuelle Konfiguration – Ubuntu 18.04 LTS Server (Beispiel)

Einträge in /etc/sysctl.conf:

```
net.ipv6.conf.eth0.autoconf = 0
net.ipv6.conf.all.use_tempaddr = 0
net.ipv6.conf.default.use_tempaddr = 0
```

Konfiguration in /etc/netplan/50-cloud-init.yaml:

```
# This file is generated from information provided by
# the datasource.  Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    ethernets:
        ens160:
            addresses:
            - 134.94.105.106/24
            - 2001:0638:0404:6900::6900:006a/64
            gateway4: 134.94.105.1
            gateway6: 2001:0638:0404:6900::6900:30
            nameservers:
                addresses:
                - 2001:0638:0404:6900::6900:00cb
                - 2001:0638:0404:6900::6900:00cc
                - 2001:0638:0404:6900::6900:00cd
                - 134.94.105.203
                - 134.94.105.204
                - 134.94.105.205
                search: []
```

Aktivieren mit: netplan apply

Anhang C: IPv6 Deaktivierung

Falls erforderlich, kann für ausgewählte Hosts das IPv6-Protokoll deaktiviert werden. Die Deaktivierung gilt je nach Betriebssystem systemweit (z.B. openSuse) für alle Netzwerk-Schnittstellen oder dediziert für einzelne Anschlüsse (z.B. Windows).

SuSe Enterprise Linux 15 YAST - System - Network Settings - Global Options
‚Enable IPv6'

abwählen und danach REBOOT

Windows 8 / 10 Systemsteuerung -> Netzwerk- und Freigabecenter
->LAN-Verbindung
-> Internet Protokoll Version 6 (TCP/IPv6)
abwählen

Wichtig: Bitte beachten Sie die besonderen Sicherheitshinweise bezüglich der IPv6-Tunnel.

MAC OS X (ältere Versionen)

sudo ip6 –x

MAC OS X 10.7.x / 10.8.x / 10.9

networksetup -setv6off ethernet

und/oder

networksetup -setv6off Wi-Fi

Kontrolle:
- Auswahl ‚Apple Menu'
- Auswahl ‚System Preferences'
- Auswahl ‚Network', dann ‚*Netzwerkname'*
- Auswahl ‚Advanced', dann ‚TCP/IP'
- Pop-Menu ‚Configure IPv6', Einstellung zeigt ‚Off'

(Stand: 17.01.2023 / Letzte Kontrolle: 17.01.2023)