

FORSCHUNGSZENTRUM JÜLICH GmbH

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

Beratung und Betrieb, ☎ (02461) 61-6400

Technische Kurzinformation

FZJ-JSC-TKI-0413

W. Anrath, E. Grünter

14.01.2020

macOS und Bonjour-Konfiguration im JuNet

Einleitung.....	1
Bonjour-Protokoll.....	1
Sleep Proxy Service.....	2
Konfiguration.....	2

Einleitung

Apples Betriebssystem macOS (früher OS X) bietet mit dem sog. Sleep-Proxy eine Funktionalität, die aktiv IP-Adressen anderer Apple-Systeme übernimmt, wenn diese sich im Ruhemodus befinden und zuvor per Bonjour-Protokoll zur Verfügung stehende Dienste annonciert haben. Diese Funktionalität führt zu unnötigen Alarmen im Netzwerk-Monitoring und –Management des JSC. Daher wird in dieser TKI empfohlen, Multicast-Advertisements auf Mac OS X zu deaktivieren.

Bonjour-Protokoll

Bonjour ist eine Implementierung des Zero Configuration Networking von Apple und hieß bis zur Mac OS X Version 10.4 Rendezvous. Wesentliche Bestandteile dieser Lösung sind:

- IPv4LL
- Multicast DNS (mDNS)
- DNS-basierte Service Discovery (dns-sd)

IPv4LL bezeichnet eine Link-lokale Adressierung, welche in den meisten Betriebssystemen unter IPv4 erst dann zum Zuge kommt, wenn per DHCP keine Adresse bezogen werden kann Die IP-Adresse

wird dabei aus dem Netz 169.254.0.0/16 zufällig gewählt. Unter IPv6 wird die im Rahmen der Stateless Address Auto Configuration (SLAAC) zwingend zu generierende Link-Local-Adresse mit dem Prefix FE80::/10 genutzt.

mDNS bezeichnet eine Technik zur Namensauflösung in Netzwerken, die – im Gegensatz zum klassischen DNS – ohne DNS-Server funktioniert. Zur Namensauflösung sendet der Client seine Anfrage an den UDP-Port 5353 einer definierten Multicast-Gruppe (IPv4: 224.0.0.251, IPv6: FF02::FB). Die zugehörige Top-Level-Domain ist „local.“.

Mit Hilfe der DNS-basierten Service Discovery lassen sich verfügbare Dienste, wie z.B. SSH-Zugang und Druckerfreigaben, finden und zur Verfügung stellen.

Sleep Proxy Service

Im Netzwerk-Monitoring und –Management des Campusnetzwerkes traten Alarmer auf, weil die Zuordnungen zwischen IP- und Hardware-Adressen nicht mit den Registrierungen in der JuNet-Datenbank übereinstimmten. Bei genauerer Analyse waren es immer nur Apple Systeme, die eine IP-Adresse vortäuschten bzw. deren Adresse vorgetäuscht wurde.

Ursache dafür ist Apples Bonjour Sleep Proxy Service, der mDNS-Anfragen im Auftrag von kompatiblen Geräten, die sich im Low-Power-Modus befinden beantwortet. Falls der Low-Power-Modus beendet werden muss, sendet der Sleep Proxy ein wake-up-Paket an den betreffenden Rechner.

Konfiguration

Multicast Advertisements können unter Mac OS X bis 10.10.x folgendermaßen deaktiviert werden. Dazu müssen die folgenden Befehle mit root-Rechten ausgeführt werden:

```
launchctl unload /System/Library/LaunchDaemons/com.apple.mDNSResponder.plist
```

```
defaults write /System/Library/LaunchDaemons/com.apple.mDNSResponder ProgramArguments -array-add "-NoMulticastAdvertisements"
```

```
launchctl load /System/Library/LaunchDaemons/com.apple.mDNSResponder.plist
```

Ab OS X 10.11.x führte Apple das Sicherheitskonzept System Integrity Protection (SIP), auch „Rootless“, ein. SIP sorgt dafür, dass Programme und Anwender selbst mit Root-Rechten keine System-Ordner von macOS mehr verändern können. Zu diesen Ordnern zählt auch /System.

Damit Anwender weiterhin Einstellungen ändern können, liest der mDNSResponder zusätzlich die Datei /Library/Preferences/com.apple.mDNSResponder.plist. Führen Sie folgenden Befehl mit root-Rechten aus:

```
defaults write /Library/Preferences/com.apple.mDNSResponder.plist NoMulticastAdvertisements -bool YES
```

Danach muss das System einmal neu gestartet werden.

Zudem ist die Internetfreigabe unter Systemeinstellungen > Freigaben > Internetfreigabe zu deaktivieren, da sich mit dieser Einstellung weitere Fehlersituationen ergeben.

Diese Empfehlung bedeutet keine Einschränkung für den Zugriff auf die im JuNet verfügbaren Dienste.