



# Mini-Howto Domain-übergreifendes DNS Version 1.3

Thorsten Gehrig 3.6.2003

- 1. Inhaltsverzeichnis
- 2. Einleitung.
- 3. Voraussetzungen.
- 4. Testszenario.
- 5. mögliche Lösungswege.
- 6. CIPE-Konfiguration.
- 7. Lösungsweg 1: Abfrage-Lösung (Query)
  - 7.1. Nameserver-Konfiguration in Base.txt
  - 7.2. BIND8.TXT-Konfiguration.
- 8. Lösungsweg 2: Slave-Zonen-Lösung (Transfer)
  - 8.1. Nameserver-Konfiguration in Base.txt
  - 8.2. BIND8.TXT-Konfiguration.
- 9. CIPE-Konfiguration – patchen von rc.cipe (für beide Lösungswege notwendig)
- 10. Beispielskonfiguration für 3 Netze.
- 11. Schlusswort

## 2. Einleitung

Dieses Howto soll beschreiben, wie man ein DNS-Service einrichtet mit 2 oder mehr LAN's an verschiedenen Standorten.

## 3. Voraussetzungen

Es wird dabei vorausgesetzt dass die LAN's mit den opt\_cipe verbunden sind. Theoretisch sind auch andere VPN oder bridge-Netzwerkverbindungen denkbar – man muss dann aber nach erfolgreicher Aktivierung der Verbindung den Bind8-Daemon manuell/selbst neu initialisieren (siehe Kapitel 9 / Befehl: killall -HUP named).

Als Nameserver wird der Bind8 Version 0.7.3 (opt\_bind8-0.7.3) auf FLI 2.0.7 / 2.0.8 vorausgesetzt.

## 4. Beispielszenario

In dieser Howto wird von 2 Lokalen Netzen mit folgenden Parametern ausgegangen:

Name: Domäne: Netzwerk/Maske: Cipe-Adresse:

Netz1 domain1.lan 192.168.0.0/255.255.255.0 10.0.1.1

Netz2 domain2.lan 192.168.1.0/255.255.255.0 10.0.1.2

## 5. mögliche Lösungswege

Es gibt 2 Möglichkeiten eine entsprechende DNS-Auflösung zu erreichen.

Möglichkeit: man erlaubt jedem Namensserver im VPN eine Namensauflösung einzeln anzufragen.

Vorteil: man hat immer wirklich aktuelle Daten vorliegen

Nachteil: man erzeugt für die DNS-Auflösungen zusätzlichen Verkehr im VPN

Jeder lokale Domainserver ist nicht nur „Masterserver“ für seine eigene Zone, sondern hat noch für jedes andere VPN-Netz eine Slave-Zone.

Vorteil: Man spart sich viel Netzwerkverkehr und hat schnellere Namensauflösungen.

Nachteil: Man hat z.T. nicht die aktuellsten Daten (je nach Aktualisierungsintervall).

Da in den meisten Fällen die IP's „halbwegs“ statisch sind, sollte für die meisten Anwendungsfälle der 2. Lösungsweg der richtige sein. In diesem Howto wird auf beide Lösungen eingegangen.

## 6. CIPE-Konfiguration

Bevor der Nameservice eingerichtet wird sollte das Cipe-Netzwerk funktionsfähig installiert sein – d.h. es muss möglich sein von jedem Rechner im jedem Netzwerk einen beliebigen Rechner im anderen Netzwerk zu Pinggen.

## 7. Lösungsweg 1: Abfrage-Lösung (Query)

### 7.1. Nameserver-Konfiguration in Base.txt

Zuerst konfigurieren wir in der /config/base.txt den (oder die) zuständigen Nameserver für die anderen VPN-Netze. Dazu wird in der Sektion „Special DNS“ folgendes eingetragen:

(in Base.txt von domain1.lan)

```
#-----  
-----  
# Special DNS configuration  
#-----  
-----  
DNS_N=' 2'  
DNS_1='domain2.lan 192.168.1.1' # IP des FLI41 mit BIND8 von domain2  
DND_2='1.168.192.in-addr.arpa 192.168.1.1' # für die  
Rückwärtsnamensauflösung
```

(in Base.txt von domain2.lan)

```
#-----  
-----  
# Special DNS configuration  
#-----  
-----  
DNS_N=' 2'  
DNS_1='domain1.lan 192.168.0.1' # IP des FLI41 mit BIND8 von domain1  
DND_2='0.168.192.in-addr.arpa 192.168.1.1' # für die  
Rückwärtsnamensauflösung
```

Es ist darauf zu Achten das der Parameter „startdns='no'“ gesetzt ist. Die restlichen DNS-Parameter aus base.txt müssen richtig gesetzt sein und werden automatisch von BIND8 verwendet.

## 7.2. BIND8.TXT-Konfiguration

Die ‚OPT\_BIND8\_SLAVEZONE‘ ist auf NO zu setzen. Dieser Parameter spezifiziert den Einsatz von Slavezonen (die wir ja nicht einsetzen).

In dem Parameter BIND8\_ADDITIONAL\_LISTEN\_ADDR wird die LOKALE Cipe-IP eingetragen. Diese Eintrag ermöglicht es dem Namensserver anfragen (Query und Transfer) auf dieser Netzwerkkarte entgegenzunehmen.

In den Parameter BIND8\_ALLOW\_QUERY wird definiert wer DNS-Anfragen durchführen darf. Dies ist erstmal der Namensserver auf der anderen Seite. Mann kann aber auch (wenn man den Bedarf hat) dem kompletten Netz erlauben direkt Querys durchzuführen (ist zum Teil für die Fehlersuche Hilfreich). Im folgenden Beispiel wird beides frei geschaltet.

auf fli4l.domain1.lan sieht das ganze dann so aus:

```
BIND8_ADDITIONAL_LISTEN_ADDR='10.0.1.1'  
BIND8_ALLOW_QUERY=' 10.0.1.2 192.168.1.0/24'
```

und auf fli4l.domain2.lan sieht das ganze dann so aus:

```
BIND8_ADDITIONAL_LISTEN_ADDR='10.0.1.2'  
BIND8_ALLOW_QUERY=' 10.0.1.1 192.168.0.0/24'
```

## 8. Lösungsweg 2: Slave-Zonen-Lösung (Transfer)

### 8.1. Nameserver-Konfiguration in Base.txt

Es ist darauf zu Achten das der Parameter „startdns='no'“ gesetzt ist. Die restlichen DNS-Parameter aus base.txt müssen richtig gesetzt sein und werden automatisch von BIND8 verwendet. Im Bereich „Special DNS configuration“ muss nichts eingetragen werden (also Parameter auf DNS-N='0' lassen).

### 8.2. BIND8.TXT-Konfiguration

Die ‚OPT\_BIND8\_SLAVEZONE‘ ist auf YES zu setzen. Dieser Parameter spezifiziert den Einsatz von Slavezonen (die wir ja bei dieser Variante einsetzen).

In dem Parameter BIND8\_ADDITIONAL\_LISTEN\_ADDR wird die LOKALE Cipe-IP eingetragen. Diese Eintrag ermöglicht es dem Namensserver anfragen (Query und Transfer) auf dieser Netzwerkkarte entgegenzunehmen.

BIND8\_ALLOW\_QUERY='10.0.1.2' erlaubt dem entsprechenden DNS-Server die Abfragen, das Kopieren wird mit der Variable BIND8\_ALLOW\_TRANSFER='10.0.1.2' erlaubt. Beide Parameter müssen gesetzt sein, da ein Transfer nicht ohne Query möglich ist!

Mehrere Namensserver (bei einem VPN aus mehr als 2 Netzen) sind dort mit Leerzeichen zu trennen.

Der Parameter `OPT_BIND8_SLAVEZONE='yes'` aktiviert die Erstellung und Nutzung der Lokalen DNS-Kopien (Slavezonen), die in den Variablen

```
BIND8_SLAVEZONE_1_DOMAIN='...' # Name der Domäne die kopiert werden soll
BIND8_SLAVEZONE_1_DIALUP='yes' # Markiert eine entfernte Domäne
BIND8_SLAVEZONE_1_MASTERS='...' # IP-Adresse des zuständigen DNS
```

definiert werden.

Jede Domäne hat immer ZWEI Zonen, eine für die Umwandlung von Name in IP, eine für die Umwandlung von IP in den Namen (Ein `NSLOOKUP 192.168.0.1` ergibt `fli4l.domain1.lan`, ein `NSLOOKUP fli4l.domain1.lan` ergibt die IP-Adresse `192.168.0.1`). Die erste Zone ist immer der Domainnamen wie er in der `Base.txt` unter `DOMAIN_NAME=` eingetragen ist, die Zone für die Rückwärtsauflösung ist

und auf `fli4l.domain1.lan` sieht das ganze dann so aus:

```
BIND8_ADDITIONAL_LISTEN_ADDR='10.0.1.1' # Lokale Cipe-IP
BIND8_ALLOW_TRANSFER='10.0.1.2' # Entferne Cipe-IP
BIND8_ALLOW_QUERY='10.0.1.2' # Entferne Cipe-IP
BIND8_SLAVEZONE_N='2' # Anzahl der Slave Zonen
```

```
BIND8_SLAVEZONE_1_DOMAIN='domain2.lan' # Name der Zone
BIND8_SLAVEZONE_1_DIALUP='yes'
BIND8_SLAVEZONE_1_MASTERS='192.168.1.1' # Master DNS für Zone
```

```
BIND8_SLAVEZONE_2_DOMAIN='1.168.192.in-addr.arpa' # Name der Zone
BIND8_SLAVEZONE_2_DIALUP='yes'
BIND8_SLAVEZONE_2_MASTERS='192.168.1.1' # Master DNS für Zone
```

und auf `fli4l.domain2.lan` sieht das ganze dann so aus:

```
BIND8_ADDITIONAL_LISTEN_ADDR='10.0.1.2' # Lokale Cipe-IP
BIND8_ALLOW_TRANSFER='10.0.1.1' # Entferne Cipe-IP
BIND8_ALLOW_QUERY='10.0.1.1' # Entferne Cipe-IP
BIND8_SLAVEZONE_N='2' # Anzahl der Slave Zonen
```

```
BIND8_SLAVEZONE_1_DOMAIN='domain1.lan' # Name der Zone
BIND8_SLAVEZONE_1_DIALUP='yes'
BIND8_SLAVEZONE_1_MASTERS='192.168.0.1' # Master DNS für Zone
```

```
BIND8_SLAVEZONE_2_DOMAIN='0.168.192.in-addr.arpa' # Name der Zone
BIND8_SLAVEZONE_2_DIALUP='yes'
```

```
BIND8_SLAVEZONE_2_MASTERS='192.168.0.1' # Master DNS für Zone
```

### **9. CIPE-Konfiguration – patchen von rc.cipe (für beide Lösungswege notwendig)**

Leider wird der BIND8-Daemon (named) schon gestartet bevor die CIPE-Netzwerkkarte installiert und verbunden ist. Daher wird bei der Initialisierung des „named“ nicht die entsprechende ciped-Netzwerkkarte (die wir als BIND8\_ADDITIONAL\_LISTEN\_ADDR eingetragen haben) mit eingebunden.

Durch eine Neuinitialisierung des BIND8-Daemons „named“ nachdem die CIPE-Verbindung steht wird dieses Problem gelöst. Dazu ist ein Patchen der Datei

```
\fli41-2.0.x\opt\etc\rc.d\rc.cipe
```

notwendig.

In dieser Datei wird (u.a.) von CIPE eine Batch-Datei erzeugt die nach Herstellung einer CIPE-Verbindung die entsprechenden ROUTE-Befehle ausführt.

Durch ein anfügen des Befehls „killall –HUP named“ wird der BIND8-Daemon neu initialisiert und dabei die CIPE-Netzwerkkarte entsprechend eingebunden.

Ein angepasstes rc.cipe liegt diesem Howto bei (oder ist unter <http://www.gehrig.info/rc.cipe> zu bekommen).

### **10. Beispielskonfiguration für 3 Netze**

In diesem Beispiel gehen wir von 3 LAN's aus. Diese 3 LAN's sind mit zwei CIPE-Tunneln verbunden

```
Name: Domaine: Netzwek/Maske: Cipe1-Adr*: Cipe2-Adr*:  
Netz1 domain1.lan 192.168.0.0/255.255.255.0 10.0.1.1 10.0.2.1  
Netz2 domain2.lan 192.168.1.0/255.255.255.0 10.0.1.2  
Netz3 domain3.lan 192.168.2.0/255.255.255.0 10.0.2.2
```

Wie man hier erkennen kann, wird vom Netz1 aus sternförmig zu Netz2 und zu Netz3 „verkabelt“. Bei diesem Beispiel ist eine Kommunikation zwischen Netz2 und Netz3 \*nicht\* möglich! Um dies zu erreichen kann man

a) zwischen Netz2 und Netz3 noch ein Cipe-Netz aufbauen (z.b. 10.0.3.1 und 10.0.3.2)

b) das Routing über Netz 1 leiten - was allerdings bei geringen Bandbreiten (DSL) nicht zu empfehlen ist.

\*Ich habe die Tunnel 1 und 2 jeweils über eigene Ports aufgebaut (Port 2000 für Tunnel 1 von 10.0.1.1 nach 10.0.1.2 und Port 2001 für Tunnel 2 von 10.0.2.1 nach 10.0.2.2).

cipe.txt auf Netz1:

```
OPT_CPIPE='yes'  
CIPE_DEBUG='no'  
CIPE_N='2'
```

#Verbindung nach Netz2

```
CIPE_1_REMOTE_INTERFACE_ADDR='10.0.1.2'  
CIPE_1_REMOTE_ADDR='domain2.dyndns.org'  
CIPE_1_REMOTE_PORT='2000'  
CIPE_1_LOCAL_INTERFACE_ADDR='10.0.1.1'  
CIPE_1_LOCAL_ADDR='0.0.0.0'  
CIPE_1_LOCAL_PORT='2000'  
CIPE_1_LOCAL_DIALUP='yes'  
CIPE_1_KEY=' 0123456789ABCDEF0123456789ABCDEF'  
CIPE_1_ROUTE='192.168.1.0/255.255.255.0'
```

#Verbindung nach Netz3

```
CIPE_2_REMOTE_INTERFACE_ADDR='10.0.2.2'  
CIPE_2_REMOTE_ADDR='domain3.dyndns.org'  
CIPE_2_REMOTE_PORT='2001'  
CIPE_2_LOCAL_INTERFACE_ADDR='10.0.2.1'  
CIPE_2_LOCAL_ADDR='0.0.0.0'  
CIPE_2_LOCAL_PORT='2001'  
CIPE_2_LOCAL_DIALUP='yes'  
CIPE_2_KEY='FEDCDBA9876543210FEDCBA987654321'  
CIPE_2_ROUTE='192.168.2.0/255.255.255.0'
```

cipe.txt auf Netz2:

```
OPT_CPIPE='yes'  
CIPE_DEBUG='no'  
CIPE_N='1'
```

#Verbindung nach Netz1

```
CIPE_1_REMOTE_INTERFACE_ADDR='10.0.1.1'  
CIPE_1_REMOTE_ADDR='domain1.dyndns.org'  
CIPE_1_REMOTE_PORT='2000'  
CIPE_1_LOCAL_INTERFACE_ADDR='10.0.1.2'  
CIPE_1_LOCAL_ADDR='0.0.0.0'  
CIPE_1_LOCAL_PORT='2000'  
CIPE_1_LOCAL_DIALUP='yes'
```

```
CIPE_1_KEY=' 0123456789ABCDEF0123456789ABCDEF'  
CIPE_1_ROUTE='192.168.0.0/255.255.255.0'
```

cipe.txt auf Netz3:

```
OPT_CIPE='yes'  
CIPE_DEBUG='no'  
CIPE_N='1'
```

#Verbindung nach Netz1

```
CIPE_1_REMOTE_INTERFACE_ADDR='10.0.2.1'  
CIPE_1_REMOTE_ADDR='domain1.dyndns.org'  
CIPE_1_REMOTE_PORT='2001'  
CIPE_1_LOCAL_INTERFACE_ADDR='10.0.2.2'  
CIPE_1_LOCAL_ADDR='0.0.0.0'  
CIPE_1_LOCAL_PORT='2001'  
CIPE_1_LOCAL_DIALUP='yes'  
CIPE_1_KEY='FEDCDBA9876543210FEDCBA987654321'  
CIPE_1_ROUTE='192.168.0.0/255.255.255.0'
```

bind8.txt auf Netz1:

```
OPT_BIND8='yes'
```

```
BIND8_SAVEDIR='/data/conf'  
BIND8_ADDITIONAL_LISTEN_ADDR='10.0.1.1 10.0.2.1'  
BIND8_HEARTBEAT_INTERVAL='120'  
BIND8_CLEAN_INTERVAL='60'  
BIND8_DEBUGLEVEL='0'  
BIND8_USEUNPRIVILEGEDPORTS='no'  
BIND8_NCACHE_TTL='1000'  
BIND8_ALLOW_QUERY='10.0.1.2 10.0.2.2'  
BIND8_ALLOW_TRANSFER='10.0.1.2 10.0.2.2'  
BIND8_DDNS_SUPPORT='yes'
```

```
OPT_BIND8_SLAVEZONE='yes'
```

```
BIND8_SLAVEZONE_ONLY='no'  
BIND8_SLAVEZONE_N='4'  
BIND8_SLAVEZONE_1_DOMAIN='1.168.192.in-addr.arpa'  
BIND8_SLAVEZONE_1_DIALUP='yes'  
BIND8_SLAVEZONE_1_MASTERS='192.168.1.1'  
BIND8_SLAVEZONE_2_DOMAIN='domain2.lan'  
BIND8_SLAVEZONE_2_DIALUP='yes'  
BIND8_SLAVEZONE_2_MASTERS='192.168.1.1'
```

```
BIND8_SLAVEZONE_3_DOMAIN='2.168.192.in-addr.arpa'  
BIND8_SLAVEZONE_3_DIALUP='yes'  
BIND8_SLAVEZONE_3_MASTERS='192.168.2.1'  
BIND8_SLAVEZONE_4_DOMAIN='domain3.lan'  
BIND8_SLAVEZONE_4_DIALUP='yes'  
BIND8_SLAVEZONE_4_MASTERS='192.168.2.1'
```

bind8.txt auf Netz2:

```
OPT_BIND8='yes'
```

```
BIND8_SAVEDIR='/data/conf'  
BIND8_ADDITIONAL_LISTEN_ADDR='10.0.1.2'  
BIND8_HEARTBEAT_INTERVAL='120'  
BIND8_CLEAN_INTERVAL='60'  
BIND8_DEBUGLEVEL='0'  
BIND8_USEUNPRIVILEGEDPORTS='no'  
BIND8_NCACHE_TTL='1000'  
BIND8_ALLOW_QUERY='10.0.1.1'  
BIND8_ALLOW_TRANSFER='10.0.1.1'  
BIND8_DDNS_SUPPORT='yes'
```

```
OPT_BIND8_SLAVEZONE='yes'
```

```
BIND8_SLAVEZONE_ONLY='no'  
BIND8_SLAVEZONE_N='2'  
BIND8_SLAVEZONE_1_DOMAIN='0.168.192.in-addr.arpa'  
BIND8_SLAVEZONE_1_DIALUP='yes'  
BIND8_SLAVEZONE_1_MASTERS='192.168.0.1'  
BIND8_SLAVEZONE_2_DOMAIN='domain1.lan'  
BIND8_SLAVEZONE_2_DIALUP='yes'  
BIND8_SLAVEZONE_2_MASTERS='192.168.0.1'
```

bind8.txt auf Netz3:

```
OPT_BIND8='yes'
```

```
BIND8_SAVEDIR='/data/conf'  
BIND8_ADDITIONAL_LISTEN_ADDR='10.0.2.2'  
BIND8_HEARTBEAT_INTERVAL='120'  
BIND8_CLEAN_INTERVAL='60'  
BIND8_DEBUGLEVEL='0'  
BIND8_USEUNPRIVILEGEDPORTS='no'  
BIND8_NCACHE_TTL='1000'  
BIND8_ALLOW_QUERY='10.0.2.1'  
BIND8_ALLOW_TRANSFER='10.0.2.1'
```

```
BIND8_DDNS_SUPPORT='yes'
```

```
OPT_BIND8_SLAVEZONE='yes'
```

```
BIND8_SLAVEZONE_ONLY='no'
```

```
BIND8_SLAVEZONE_N='2'
```

```
BIND8_SLAVEZONE_1_DOMAIN='0.168.192.in-addr.arpa'
```

```
BIND8_SLAVEZONE_1_DIALUP='yes'
```

```
BIND8_SLAVEZONE_1_MASTERS='192.168.0.1'
```

```
BIND8_SLAVEZONE_2_DOMAIN='domain1.lan'
```

```
BIND8_SLAVEZONE_2_DIALUP='yes'
```

```
BIND8_SLAVEZONE_2_MASTERS='192.168.0.1'
```

Nach diesem Muster kann man die Vermaschung beliebiger weiterer Netze aufbauen. Man sollte hier allerdings eine saubere IP-Planung im Vorfeld vornehmen um IP-Chaos zu vermeiden. Es darf dabei **KEINE** Überschneidung der IP-Adressen geben. Eine klare Trennung von „reellen LAN´s“ und CIPE-LAN´s in die IP-Bereiche 192.168.x.y und 10.0.x.y halte ich dabei für sehr empfehlenswert.

## **11. Schlusswort**

Für Fragen/Anregungen/Kritik bin ich per eMail unter [Thorsten@Gehrig.de](mailto:Thorsten@Gehrig.de) zu erreichen.

Klicken Sie hier, um die Seite auszudrucken.