smekal.at :: IT Consulting

"Take the long way home"

Grundlagen und Praxis von Mobile IPv6 unter Linux

smekal.at :: Goesta Smekal

- 15+ Jahre als IT Professional
- unterschiedliche Umgebungen:
  - 24x7 Operating im medizinischen Bereich
  - Support, Training, Implementierung
  - IT Leiter bei einer NPO
  - Senior Consultant Systemmanagement
- 15+ Jahre Open Source Erfahrung
- enger Kontakt zur Community
  (Vorstandsmitglied der Linux User Group Austria)

Erfahrungen kann man nicht lernen, man muss sie machen

Mobilität :: Erreichbarkeit

- Post - Meldewesen
  - Wohnsitz → Adresse
    eindeutige Ortszuweisung
  - Urlaub/Zweitwohnsitz → Meldepflicht → c/o
    Nachsendung
- Telefonnetz
  - Festnetz → Rufweiterleitung
    Rufnummer ist an Ort gebunden ≙ Adresse
  - Mobiltelefon → Handover / Roaming
    Mobilität wird vom Netzbetreiber sichergestellt

Mobilität :: Datennetze

- IP Adresse
  - bei Drahtnetzwerken ortsgebunden (Ausnahme: RFC 1918, also 192.168.0.0/24 & Co)
  - WLAN in Reichweite begrenzt
  - GPRS/UMTS gilt nicht ;-) (siehe Mobiltelefonie)
- VPN „Roadwarrior“
  - Daten werden ins Heimnetz getunnelt
  - Aufenthaltsort verschleiert

IPv4 Mobility

- RFC 3344 definiert „IP Mobility Support for IPv4“ (15 Jahre nach IPv4!)
- IPv4 Adressraum zu klein für verbreitete Nutzung
- Clients erhalten meist RFC 1918 Adressen
- NAT
- kein standardisiertes Verfahren um Routen zu optimieren
- kaum verbreitet

Mobile IPv6 :: Begriffe

- **Mobile-Node (MN)**
  ein Host, der (gelegentlich) auf Reisen geht

  - **Home-Link**
    das Netzwerksegment in dem ein Host „zu Hause“ ist
  - **Home-Address**
    die IPv6 Adresse eines Hosts an seinem Home-Link
  - **Home-Subnet-Prefix**
    das im Home-Link gültige IPv6 Präfix

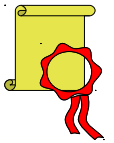
Mobile IPv6 :: Begriffe

- **Care-of-Address (CoA)**
  global-unicast Adresse einer MN in einem „fremden“ Netz
- **Correspondend-Node (CN)**
  ein Host, der eine MN kontaktieren möchte (kann auch selbst eine MN sein)

Mobile IPv6 :: Begriffe

- **Home-Agent (HA)**
  Router am Home-Link, der die CoA der MN verwaltet

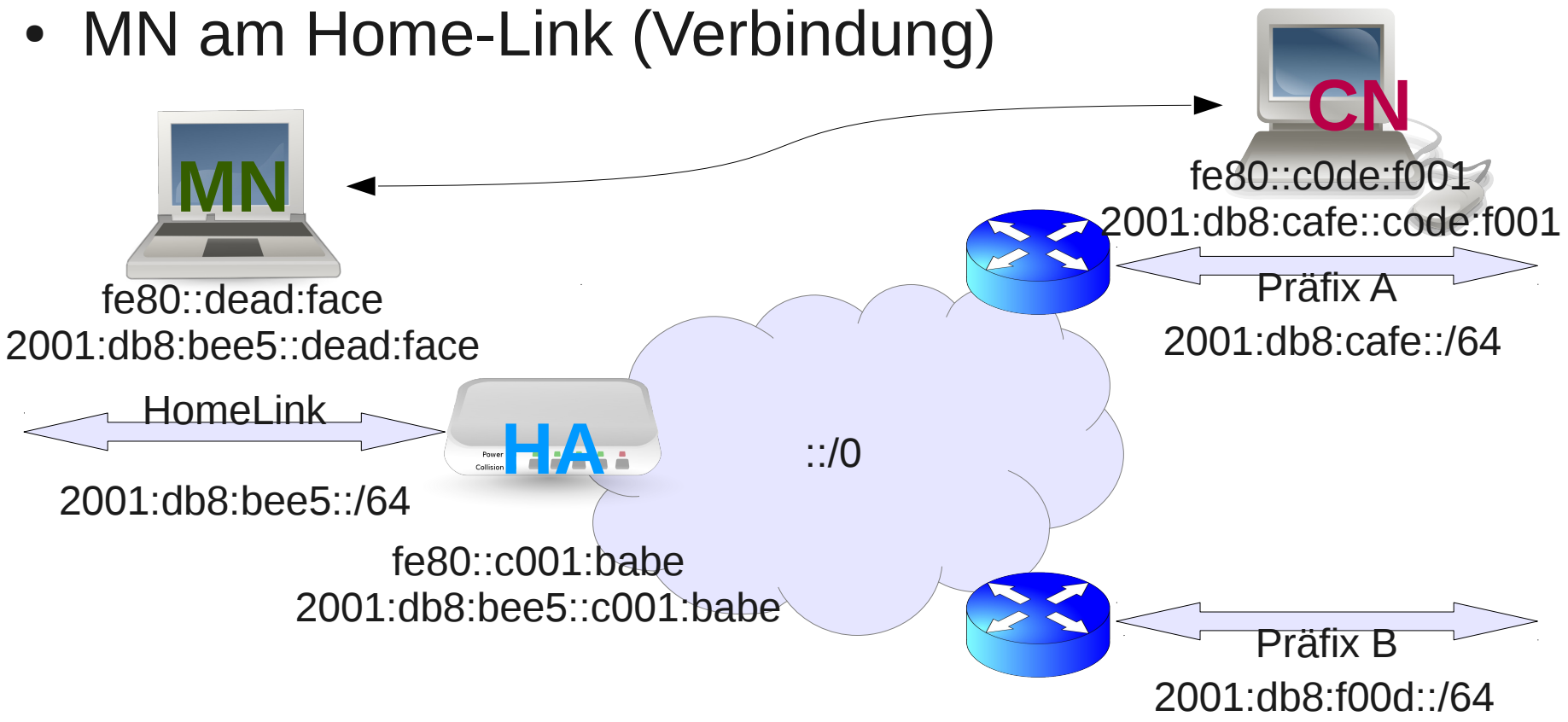
- **Binding:**
  „Meldung“ der MN beim HA



- **Binding Update (BU)**
  Nachricht mit der ein MN seinen HA von der (neuen) CoA informiert

Mobile IPv6 :: Funktionsweise

- MN am Home-Link (Verbindung)

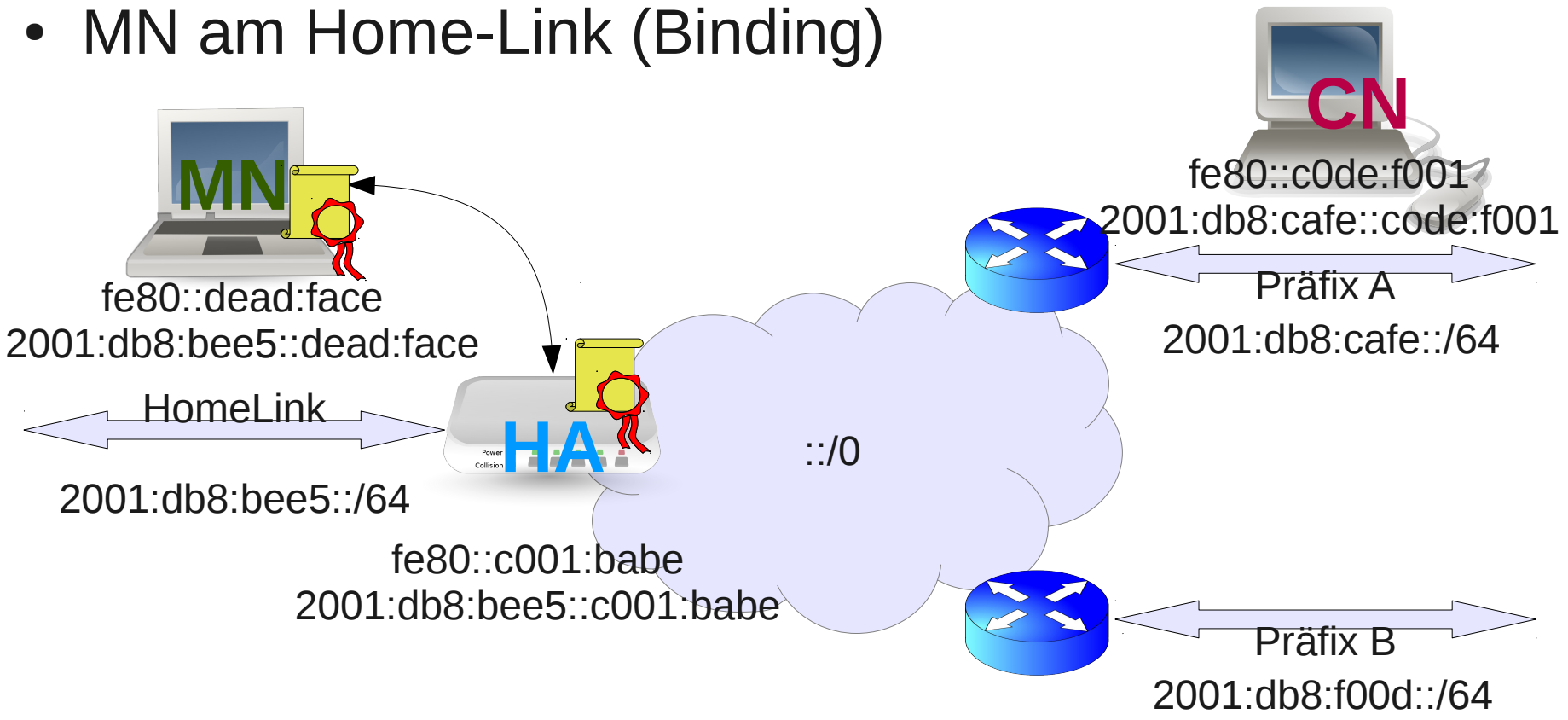


Mobile IPv6 :: Binding

- **Binding**: MN und HA tauschen Identität aus - kann (sollte!) kryptographisch gesichert erfolgen
- **Binding Cache**: CN, MN, HA speichern Informationen über CoA von bekannten MN
  - HomeAddress
  - CareOfAddress
  - Lifetime
- **Binding Update**: MN in einem fremden Netz sendet CoA an HA

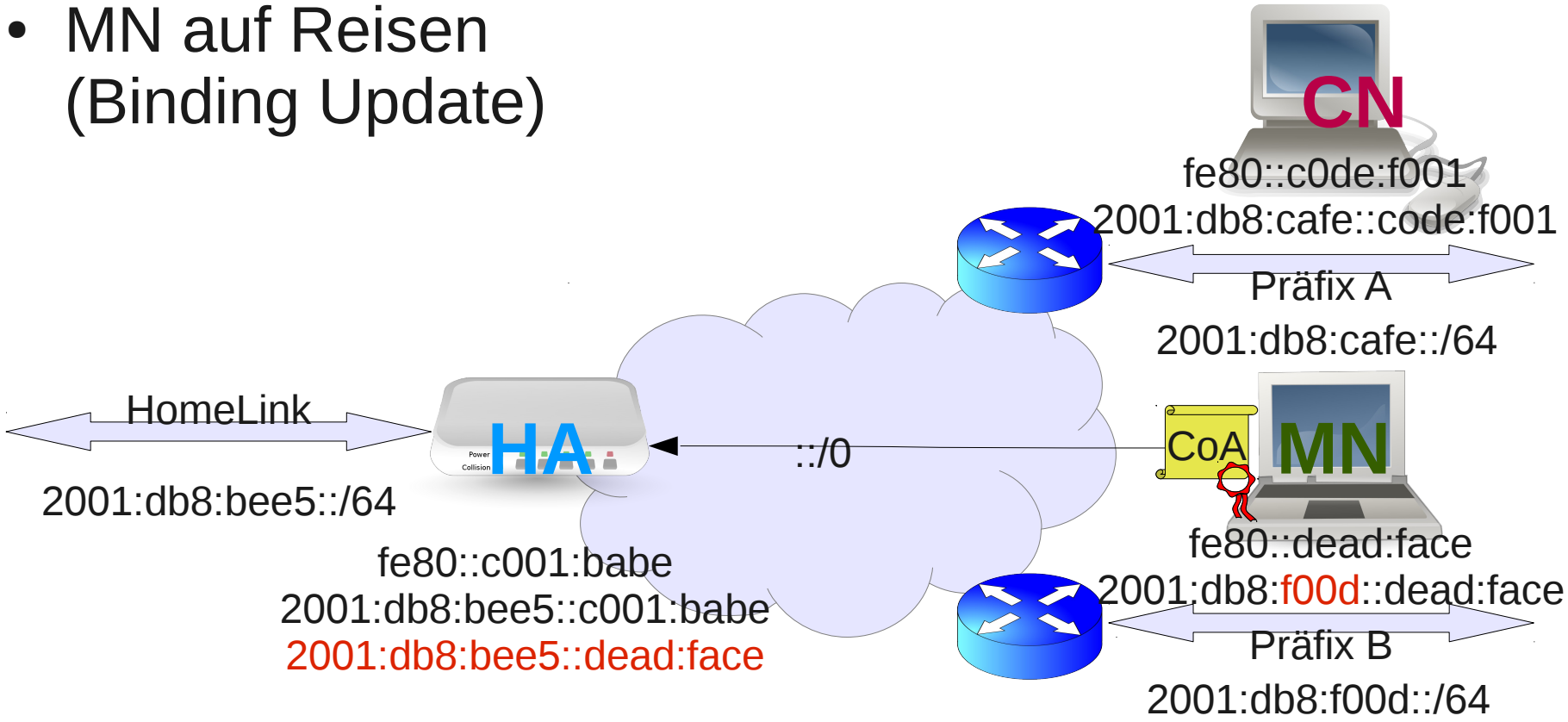
Mobile IPv6 :: Funktionsweise

- MN am Home-Link (Binding)



Mobile IPv6 :: Funktionsweise

- MN auf Reisen
  (Binding Update)



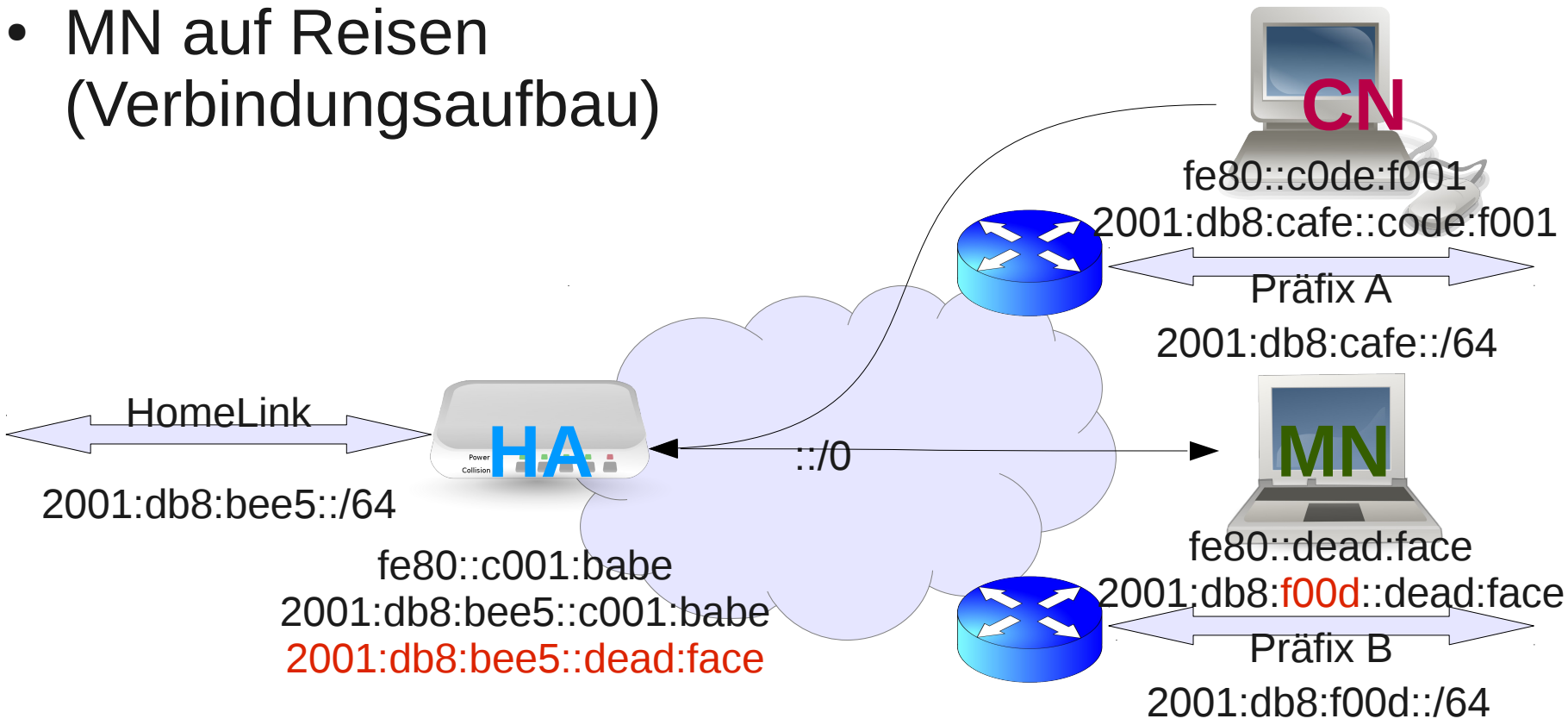
Mobile IPv6 :: MN ↔ CN

- Bidirectional Tunneling
  - CN und MN kommunizieren über HA
  - Routing wie in klassischem VPN
  - unelegant, ineffizient

- Route Optimization
  - CN und MN kommunizieren direkt
  - verringert Last am HA und HomeLink
  - erfordert Vertrauen (Kryptographie)

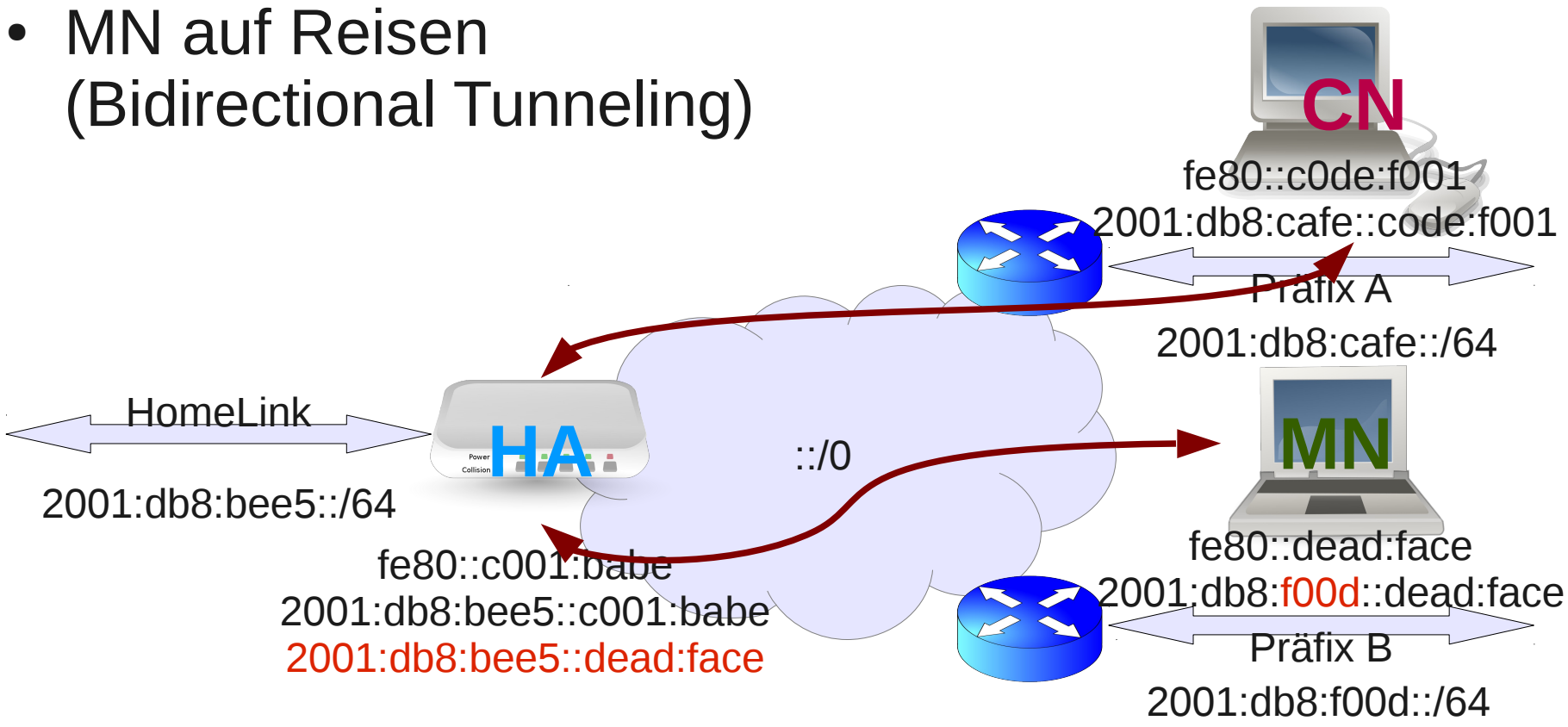
Mobile IPv6 :: Funktionsweise

- MN auf Reisen (Verbindungsaufbau)



Mobile IPv6 :: Funktionsweise

- MN auf Reisen
  (Bidirectional Tunneling)

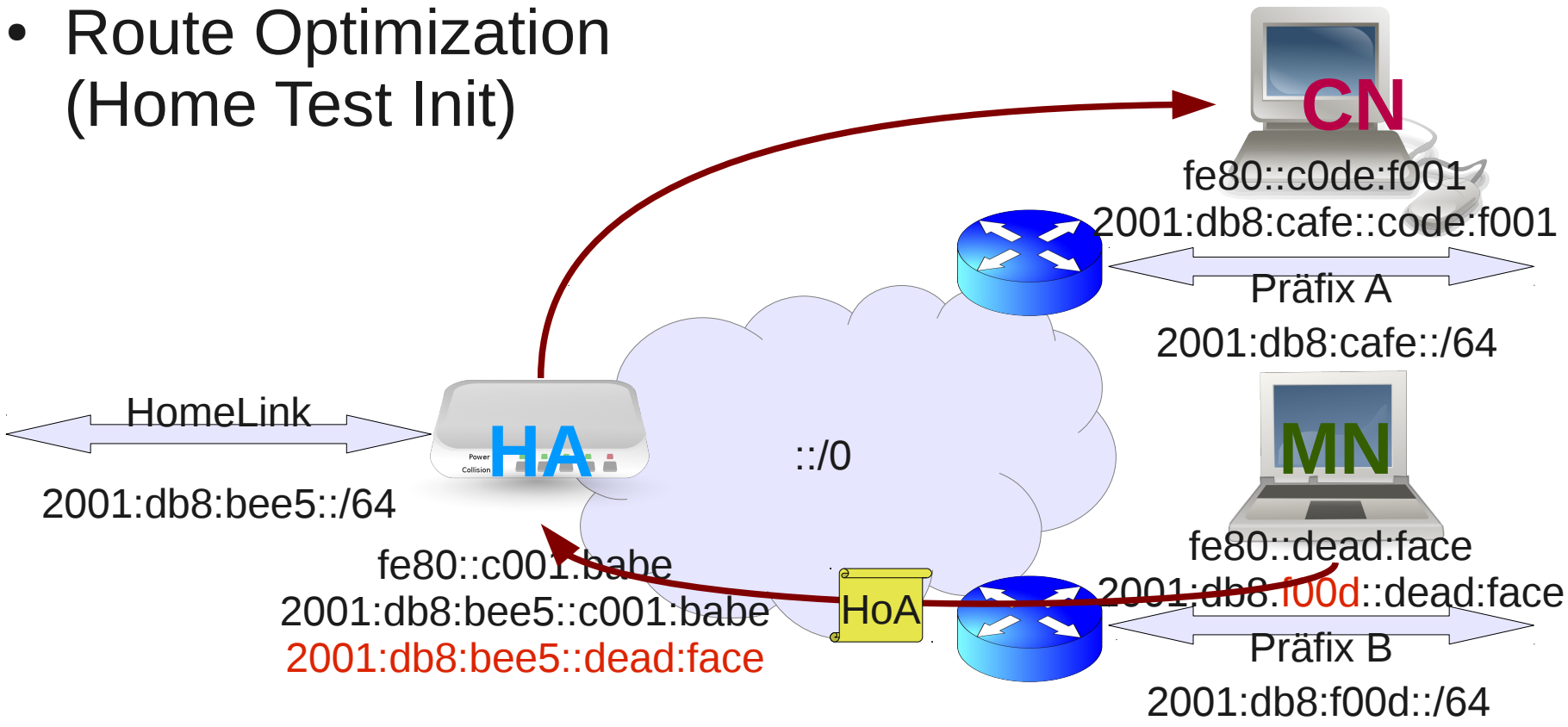


Mobile IPv6 :: Route Optimization

- Return Routability Procedure (RFC 4225):
  - Verbindung zu MN unter CoA möglich?
  - Verbindung zu MN unter HomeAddress möglich?
  - nur dann direkte Kommunikation
- Ablauf:
  1. MN sendet „Home Test Init“ via HA an CN (enthält „Home Init Cookie“)
  2. MN sendet „Care-of Test Init“ direkt an CN („Care-of Init Cookie“)
  3. CN antwortet auf „Home Test Init“ via HA („Home Init Cookie“, „Home Keygen Token“)
  4. CN antwortet auf „Care-of Test Init“ direkt („Care-of Init Cookie“, „Care-of Keygen Token“)

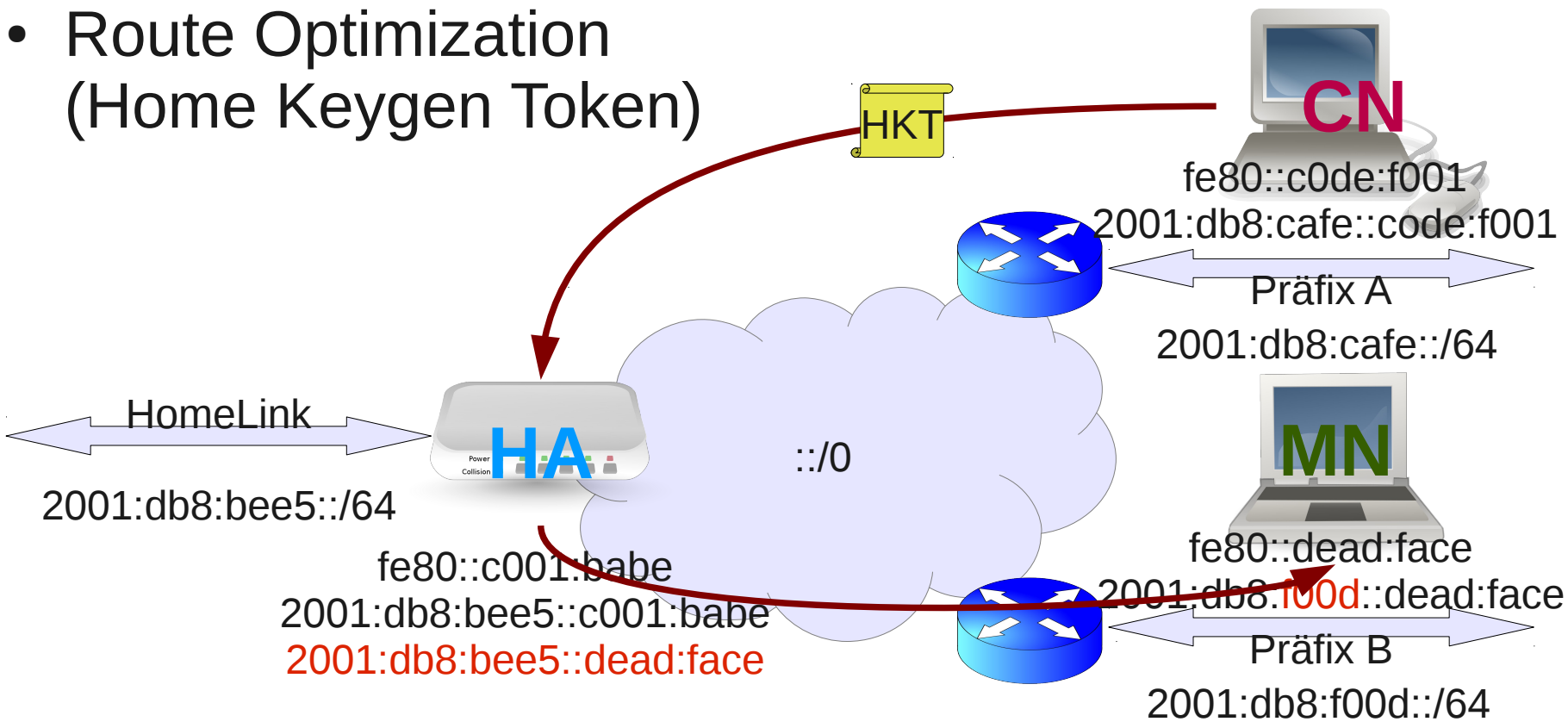
Mobile IPv6 :: Funktionsweise

- Route Optimization (Home Test Init)



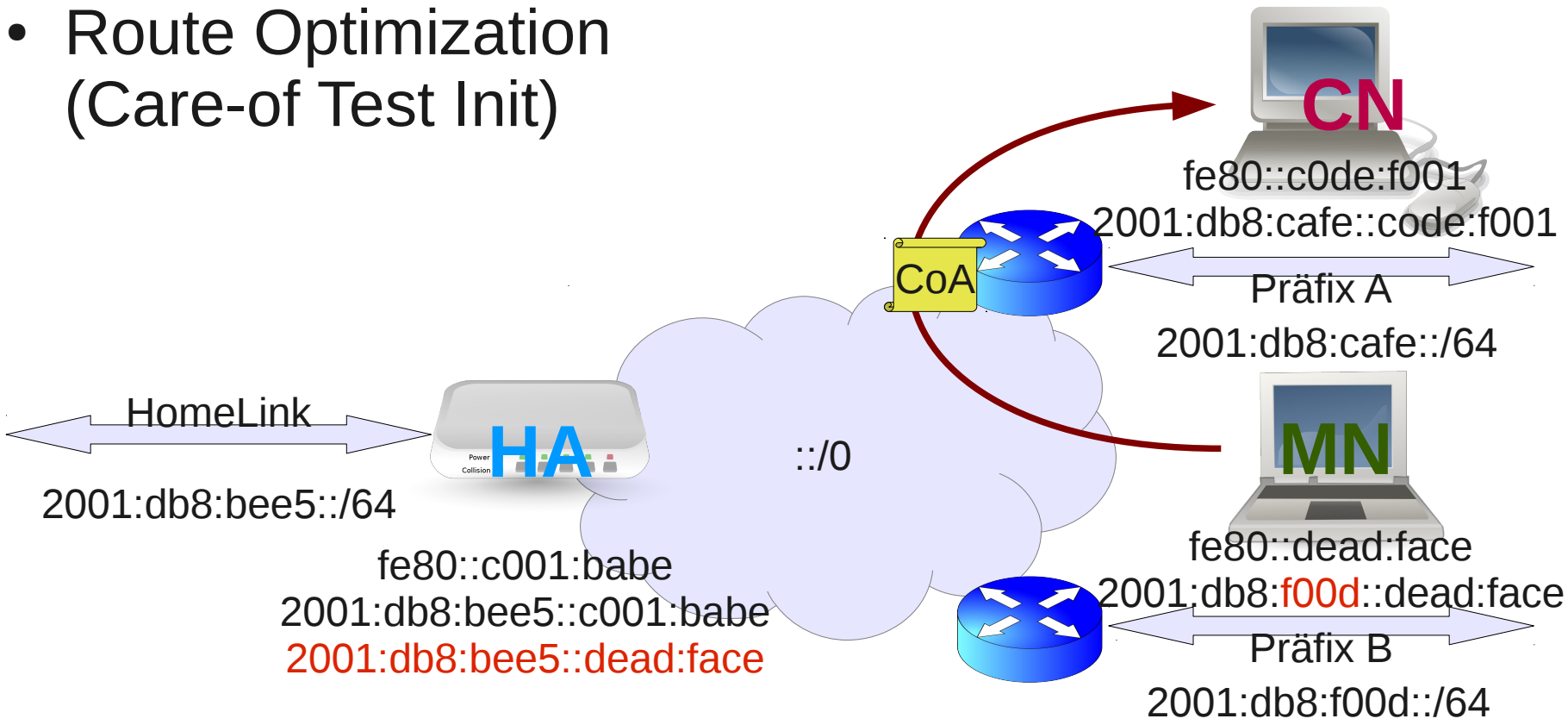
Mobile IPv6 :: Funktionsweise

- Route Optimization (Home Keygen Token)



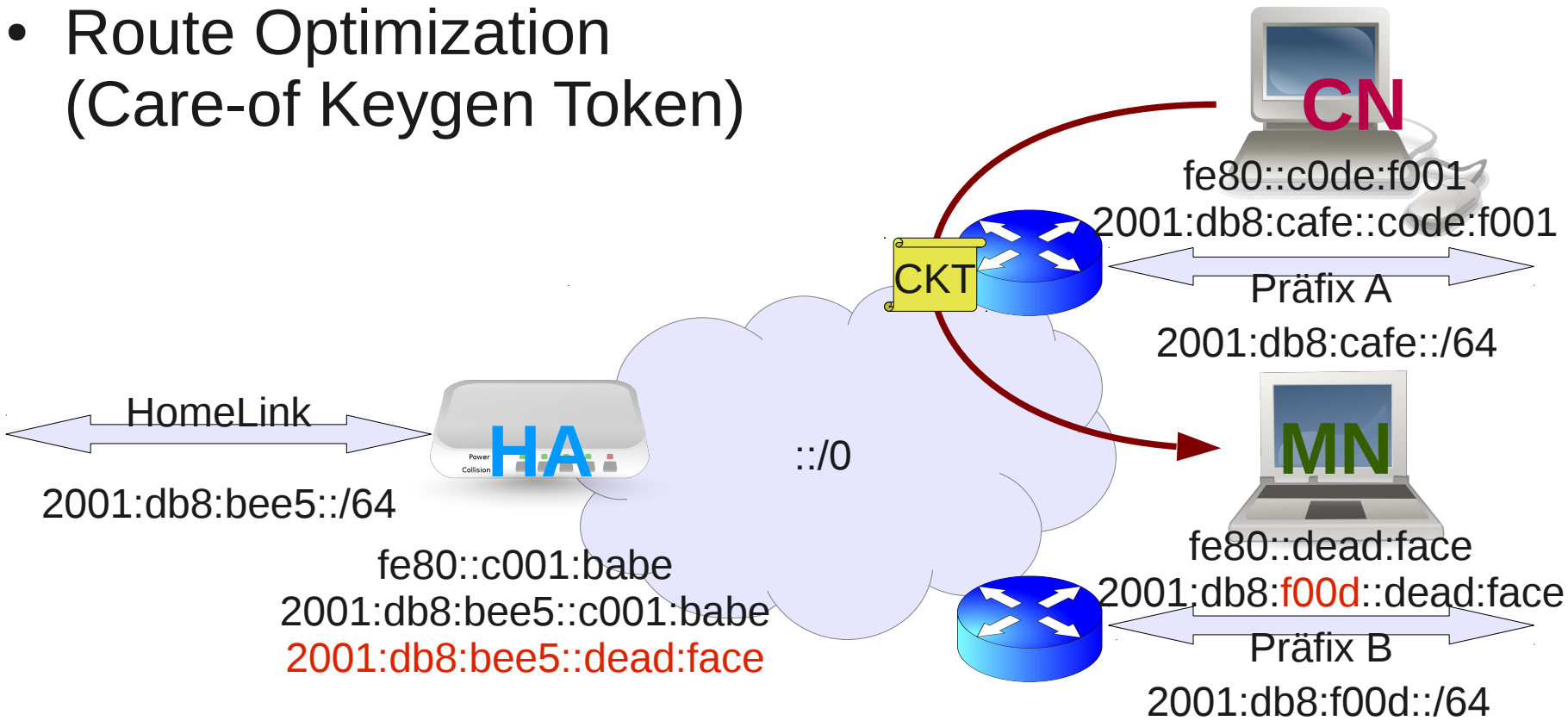
Mobile IPv6 :: Funktionsweise

- Route Optimization (Care-of Test Init)



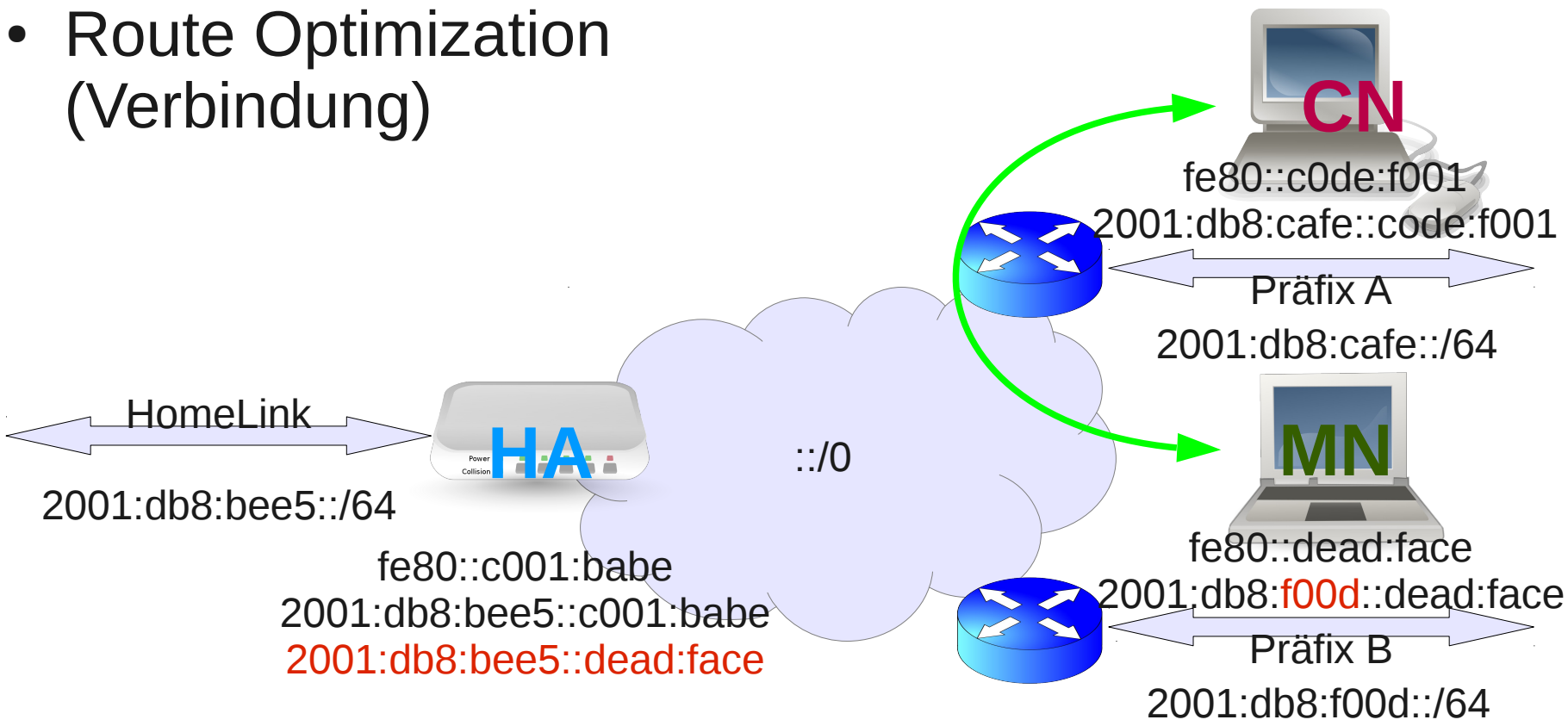
Mobile IPv6 :: Funktionsweise

- Route Optimization
  (Care-of Keygen Token)



Mobile IPv6 :: Funktionsweise

- Route Optimization (Verbindung)



Mobile IPv6 :: Security

- Identität und Integrität der Peers muss gewährleistet sein
- IPSec ist Bestandteil von IPv6
  - Authentication Header (AH)
    stellt Identität sicher
  - Encapsulated Security Payload (ESP)
    verschlüsselt übermittelte Daten
- Binding und Binding Update nutzen IPSec
  (theoretisch optional, in der Praxis unbedingt verwenden!)
- verschlüsselte Kommunikation kann am Perimeter nicht nach Inhalt gefiltert werden – weder Protokoll noch Daten sind erkennbar
- Paketfilter am HomeAgent eingeschränkt möglich (im Bidirectional Tunneling Mode)
- MN muss gut abgesichert werden

Mobile IPv6 :: Linux

- Implementierung historisch sehr verworren
- offizielle Kernel-Version bis 2.6.26 immer wieder fehlerhaft
- Kernel Patches von verschiedenen Projekten
- historisch mehrere Userspace Tools
- keine konsistente Timeline
- Howtos verwaist, viele Links ins Leere
- … :-P

Mobile IPv6 :: Linux Kernel

- aktueller Kernel unterstützt IPv6 Mobility
- historisch:
  - UMIP (ab 2009)
  - USAGI (bis 2008, Kernel 2.6.17)

```
CONFIG_SYSVIPC=y
CONFIG_PROC_FS=y
CONFIG_NET=y
CONFIG_INET=y
CONFIG_IPV6=y
CONFIG_IPV6_MIP6=y
CONFIG_XFRM=y
CONFIG_XFRM_USER=y
CONFIG_XFRM_ENHANCEMENT=y
CONFIG_IPV6_TUNNEL=y
CONFIG_IPV6_ADVANCED_ROUTER=y
CONFIG_IPV6_MULTIPLE_TABLES=y
```

Mobile IPv6 :: Userspace

- **mip6d:** Userspace Daemon für HA und MN
- Nautilus, NEMO und andere 2009 in **UMIP.org** zusammengeführt
- **MIPL**
  IPv6 Mobility für Hosts
  (historisch, letzter Patch 2.6.13?)
- **Nautilus**
  … für ganze Subnetze (zB WLAN im Zug, Sensornetze)
  (letzter „annual Report“ 2008)

Mobile IPv6 :: Installation

- Fertige Pakete für Debian:
  1. Repository-Key importieren
  2. Apt-Quelle hinzufügen
     (`deb http://umip.org/debian/ unstable main contrib`)
  3. Paket installieren
     (`apt-get update && apt-get install umip`)
- Aus Quellen kompilieren:
  `./configure && make && make install`

Konfiguration :: HomeAgent

- **mip6d.conf:**

```
NodeConfig HA;
DebugLevel 10;
# interface on the home link
Interface "eth0";
# only accept binding from known hosts (no PKI)
BindAclPolicy 2001:db8:bee5::dead:face allow;
DefaultBindPolicy deny;
# encryption parameters
UseMnHaIPsec enabled;
KeyMngMobCapability disabled;
IPsecPolicySet {
  HomeAgentAddress 2001:db8:bee5::coo1:babe;
  HomeAddress 2001:db8:bee5::dead:face/64;
  IPSecPolicy Mn UseESP 10;
  IPSecPolicy TunnelPayload UseESP 11;
}
```

Konfiguration :: HomeAgent

- **radvd.conf:**

```
interface eth0
{
  AdvSendAdvert on;
  # home agent parameter
  AdvHomeAgentFlag on;
  AdvHomeAgentInfo on;
  HomeAgentLifetime 1800;
  HomeAgentPreference 10;
   # local IPv6 prefix
  prefix 2001:db8:bee5::/64
  {
    AdvRouterAddr on;
    AdvOnLink on;
    AdvAutonomous on;
  };
};
```

Konfiguration :: MobileNode

- **mip6d.conf:**

```
NodeConfig MN;
DebugLevel 10;
Interface "eth0"{
  MnIfPreference 1;
}
MnHomeLink „eth0“ {
  HomeAgentAddress 2001:db8:bee5::coo1:babe;
  HomeAddress 2001:db8:bee5::dead:face/64;
}
UseMnHaIPsec enabled;
KeyMngMobCapability disabled;
IPsecPolicySet {
  HomeAgentAddress 2001:db8:bee5::coo1:babe;
  HomeAddress 2001:db8:bee5::dead:face/64;
  IPSecPolicy Mn UseESP 10;
  IPSecPolicy TunnelPayload UseESP 11;
}
```

Konfiguration :: IPSec

- **setkey.conf:**

```
#!/usr/sbin/setkey -f
flush;
spdflush;
# MN > HA transport SA for BindingUpdate
add 2001:db8:bee5::dead:face 2001:db8:bee5::coo1:babe esp 1000
  -u 10 -m transport
  -E 3dse-cbc 0x<your shared secret here>
  -A hmac-sha1 0x<your shared secret here> ;
# HA > MN transport SA for BindingAck
add 2001:db8:bee5::coo1:babe 2001:db8:bee5::dead:face esp 1001
  -u 10 -m transport
  -E 3dse-cbc 0x<your shared secret here>
  -A hmac-sha1 0x<your shared secret here> ;
# MN > HA transport SA for Traffic
add 2001:db8:bee5::dead:face 2001:db8:bee5::coo1:babe esp 1002
  -u 11 -m transport
  -E 3dse-cbc 0x<your shared secret here>
  -A hmac-sha1 0x<your shared secret here> ;
# HA > MN transport SA for Traffic
add 2001:db8:bee5::coo1:babe 2001:db8:bee5::dead:face esp 1003
  -u 11 -m transport
  -E 3dse-cbc 0x<your shared secret here>
  -A hmac-sha1 0x<your shared secret here> ;
```

Mobile IPv6 :: Literatur

- Mobile IPv6 HOWTO
  `http://tldp.org/HOWTO/Mobile-IPv6-HOWTO/index.html`
  (wird derzeit überarbeitet)
- UMIP.org
  `http://www.umip.org/`
- Aktueller Stand der Standards
  `https://tools.ietf.org/wg/mip6/index.pyht?sort=3&reverse=1`
- `http://natisbad.org/MIPv6/`

Nicht vergessen!

Am 6. Juni 2012 ist
„World IPv6 Launch Day“
http://www.worldipv6launch.org/