IPv6 Kongress 2010

Mobile IPv6 ganz praktisch

Lutz Donnerhacke

IKS GmbH

http://www.iks-jena.de/

IKS

Ein neues Zeitalter des Internets

Techniken im Vergleich

Anforderung	IPv6	VPN	DirectAccess	Mobile IPv6
Zugriff Internet	Ja	Split-Tunnel	Ja	Ja
Zugriff Intranet	Firewall	Ja	Ja	Ja
Feste Client IP	Nein	Im LAN	Im LAN	Ja
Nutzer bekannt	Nein	Ja	Ja	Nein
Automatisch an	Ja	Nein	Ja	Ja
Effizienter Datenfluss	Ja	Nein	Nein	Ja
Unterbrechungsfrei	Nein	Nein	Nein	Ja
Moderner Server	Ja	Nein	Ja	Ja
Legacy Server	Nein	Ja	NAT64	Nein
Moderner Client	Ja	Nein	Ja	Ja
Public Legacy Client	6to4	Ja	6to4	6to4
Private Legacy Client	Teredo	NAT-Traversal	Teredo	Teredo

IKS

Mobile IPv6 – unterwegs daheim

- Sicherstellen der Erreichbarkeit
  - Anrufe auf die Firmennummer sollen immer den richtigen Mitarbeiter erreichen
- Netz stellt die Erreichbarkeit sicher
  - Nur noch Handys erlaubt
- Mitarbeiter meldet sich mit aktueller Nummer
  - Sekretariat stellt Anrufe durch
  - Mitarbeiter gibt aktuelle Nummer weiter

IKS

Mobile IPv6 – Annahmen

- Native IP-Adressen sind regional verschieden
  - Trotz Roaming sollen Verbindungen bleiben
- IP Routing ist sicher und geht nur nach Ziel
  - Sicherheit nicht besser als ohne Mobilität
  - Feste System-Adresse auch Mobil erreichbar
- Ende-zu-Ende statt Änderungen am Netz
- Mobiles Gerät nur daheim vorab bekannt
- Hauptgefahren: Mobiler MitM, Flooding

IKS

Mobile IPv6 – Meld‘ Dich An

- MN sucht HA: „Wer macht Sekretariat?“
  - Dynamic HA Discovery per ICMP Anycast
  - *Eine* Antwort mit Liste aller HA
  - Alternativ Autoconfig im LAN, H-Bit
- MN bereitet Weggang vor: Hinterläßt Kennung
  - Vereinbarung einer IPSec SA für ESP (manuell)
- MN am Ziel: Hinterlegt neue Nummer
  - BindungsUpdate per IPSec mit CoA

IKS

Mobile IPv6 – ineffizient arbeiten

- HA simuliert MN im Heimnetz
  - Nimmt alle Kommunikation von CN an
  - auch Link Local und Multicast!
- HA leitet abgefangene Daten an MN
  - Verschlüsselt und authenisiert mit ESP
- MN antwortet klassisch
  - Verschlüsselt und authenisiert per ESP
- HA sendet getunnelte Daten klassisch an CN

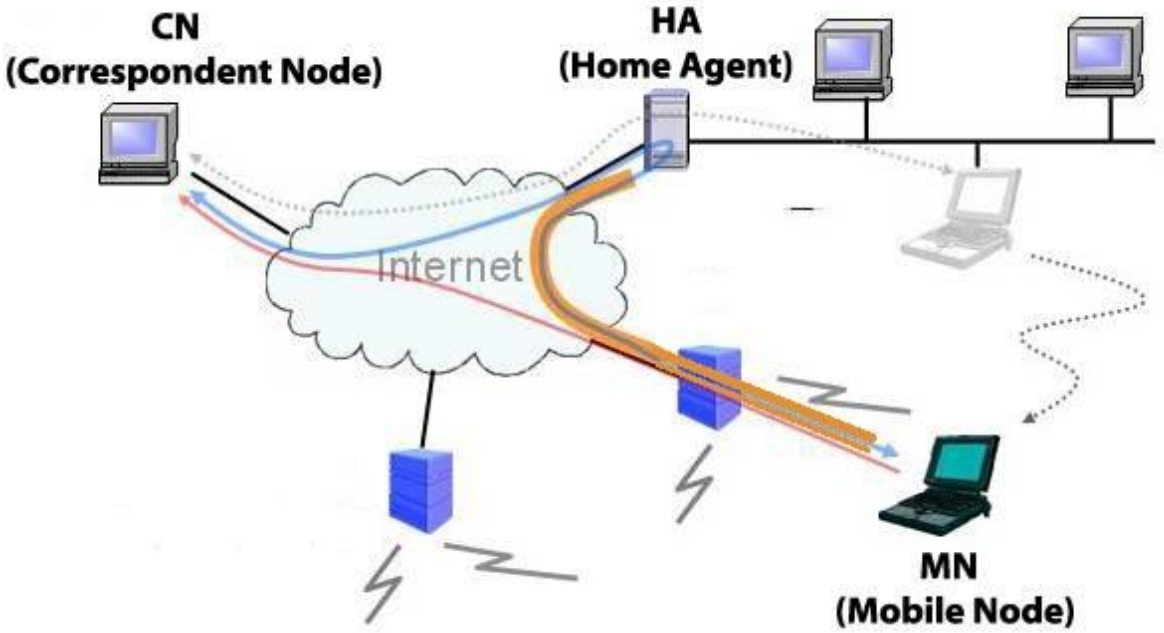
IKS

Mobile IPv6 – effizient arbeiten

- MN informiert CN über direkte Erreichbarkeit
  - CN würde die Information anzweifeln
- MN informiert CN auf beiden Wegen
  - Direkt mit CoA und via HA
- CN antwortet mit geteiltem Geheimnis
  - Direkt an CoA und via HA
- MN baut Geheimnis zusammen, sendet BU
  - Direkte Kommunikation zwischen MN und CN

IKS

Mobile IPv6 – Datenfluss



http://www.youtube.com/watch?v=N2kvPCwJkLU

IKS

Mobile IPv6 – Mit fremden Federn

- Routing Header (2)
  - Alle Applikationen sehen nur Heimatadresse
  - Nutzung von Ingress Filter da topologisch korrekt
  - Erlaubnis trotz Verbots von Source Routing (RH0)
- Alternative CoA bei Topologieproblemen
- Kaum State auf CN, da Indizes in Noncetabelle
- Aktualisierung der Bindung kurzfristig möglich
  - Kein Return Routability Test nötig, nur ein Paket
  - Häufige Updates, Bindung nur für Minuten

IKS

Mobile IPv6 – Veränderungen daheim

- Wechsel des HA: „Vertretung im Sekretariat“
  - Dynamic HA Discovery -> Neuer HA
- Renumber: „Wechsel des Dienstleisters“
  - Regelmäßiger BU beim HA enthält Umzugshinweis
  - Dynamic Prefix Discovery -> Neue Heimatadresse
  - Parallelbetrieb möglich
- Returning Home Konflikt: „Wer ist wer?“
  - Rückmeldung per Multicast, dann erst Übernahme

IKS

Mobile IPv6 – Standortwechsel

- Bei Wechsel der IP Anbindung (neuer Prefix)
  - Schnelle Umschaltung durch 1-Paket BU
  - Neuer Return Routability Test: sechs Zyklen
- Verbindungen reißen nicht ab
  - CoA nicht für Applikationen sichtbar
- Umschaltzeiten hängen von Layer 2 ab
  - Kein Netz, keine Daten
  - Neues Netz schnell detektieren, Altes lange halten
  - Router Announcements alle 50ms statt alle 2min?

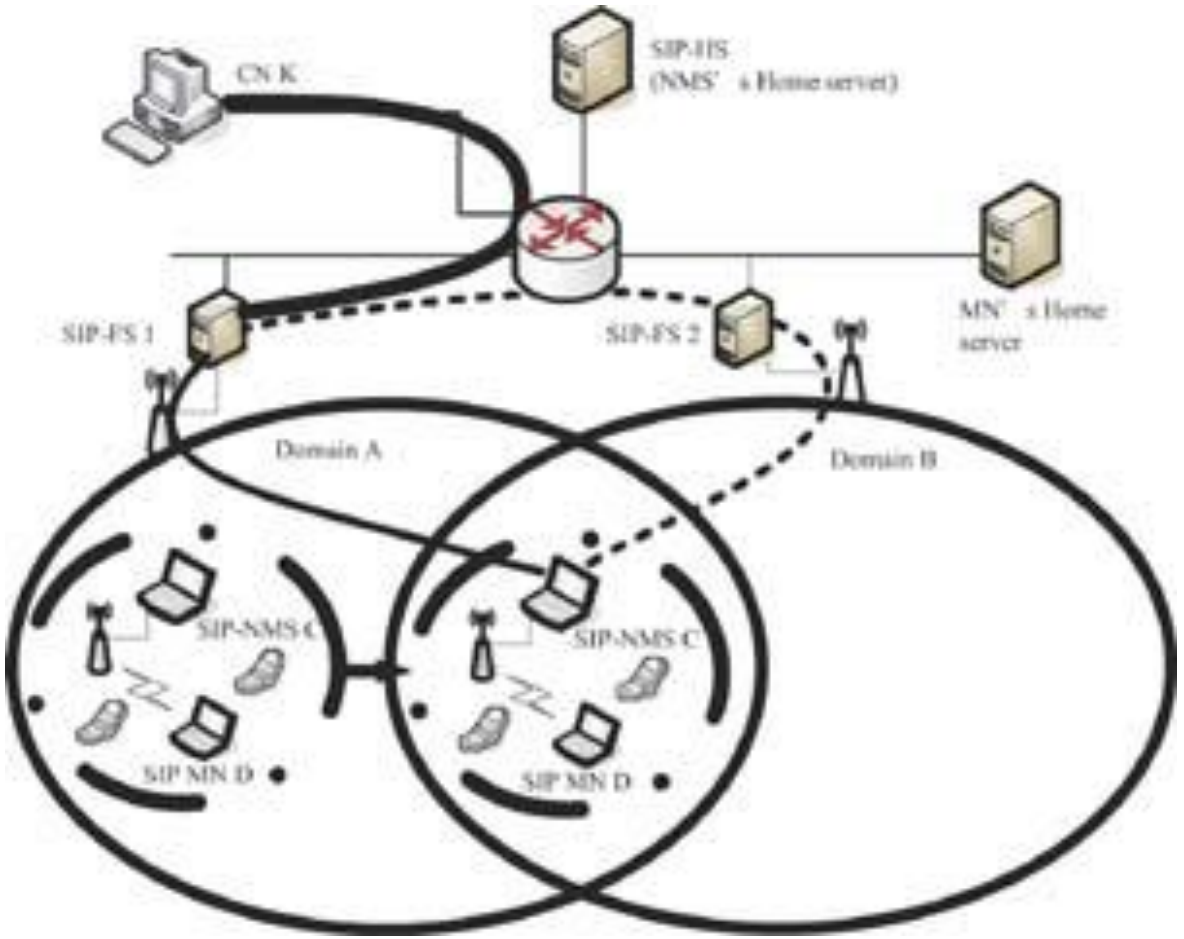
IKS

Fast Mobile IPv6 – Schnelle Wechsel

- MN fragt alten Router nach direkten Nachbarn
- MN wählt neuen Router, z.B. anhand Stärke
  - Fast BU an alten Router, authentisiert mit SEND (CGA)
- Router informieren sich über den Wechsel
  - Duplizieren Datenverkehr zum neuen Router
- MN wechselt die Netze
  - Neue L3 Adressen, BUs an HA und CNs
- MN informiert neuen Router über Abschluß
  - Quertraffic zwischen Routern erstirbt

IKS

Mobile IPv6 – Schnelle Wechsel



HMIPv6 – Türme im Netz

- Verstecken der Mikromobilität
  - MN lernt vom Router regionale Gateways (MAP)
  - MN bindet sich lokal und den MAP global
  - Roaming innerhalb des MAP-Bereichs sehr schnell
- MAP fungiert als Proxy für MN
  - CoA des MN nicht mehr extern sichtbar
- MN kann sich bei mehreren MAP melden
  - Topologie bzgl. CN bestimmt Nutzung

IKS

Mobile IPv6 – Firewall Nightmare

- MIPv6 Support praktisch vernachlässigbar
- Firewall vor MN
  - ESP Traffic eingehend verboten, HA evtl. möglich
  - Spontaner Verbindungsaufbau durch CN verboten
  - Route Optimization generiert stateless Traffic
  - Roaming zu anderer Firewall: MN stateless
- Übungsaufgabe: Firewall vor HA oder CN
- Lösungen?

IKS

Mobile IPv6 – praktische Probleme

- Replay Angriffe verhindern mit IKE
- Mobilität in vertrauenswürdigen Netzen
  - IPSec viel zu teuer: Einfache Authentifizierung
- HA Downtime, Überlast, Renumber
  - Proaktive Signalisierung vom HA an den MN
- Mobile IPv6 fähige Anwendungen: API
- Multicast: IPTV (restricted access)
- Datenschutz bzgl. MN: Lokation möglich
  - Heimadresse oder CoA verstecken (topologisch)

IKS

Mobile IPv6 – praktische Probleme

- FMIP pro 802.11, 802.16 (WIMAX), 3G, …
  - 802.21 – Media independet Handover
- Roaming zu langsam
  - Preshared Key zwischen MN und CN
  - CN und HA Ummeldungen gleichzeitig
  - Paralleler Netzzugriff und multiple CoA
  - Temporärer Fallback auf HA allein
  - Datenversand auf Kredit durch CN
  - Kryptographische Adressen mit Authentikator

IKS

Mobile IPv6 – praktische Probleme

- Standard zu starr für Entwicklungen
  - Proprietäre Vendor Options
  - Experimentelle Protokolle
- Einfacheres Bootstrapping: AAA statt Manuell
  - MN eindeutig identifizieren (ISMI, FQDN, …)
  - Support für multiple Provider, Zertifikate, …
- Betrieb mehrerer Mobilitätsprovider
  - Auswahl nach angebotenen Services: voip, im, …
- Ressoucenlast des MN im Fremdnetz
  - 802.1x Authentisierung durch ISPs zum Heimnetz

IKS

Mobile IPv6 – praktische Probleme

- NASA/Boeing: Nutzbarkeitsstudie (RFC 5522)
  - Untersuchungen in Flugzeugen mit VDL 2
    - In der Luft alle 30-60min Handover
    - „Up“-Bandbreite nur 1% der „Down“-Bandbreite
    - Anforderungen an Latenz, Verfügbarkeit, Overhead
    - Route Optimization zwingend nötig
  - Zukunft
    - 802.16: Boden, P34, LDL: Land, Satcom: Ozean
    - Internet und VoIP für Passagiere

IKS

NEMO – Netze auf Reisen

- MN wird Mobile Route mit (Sub)Netz
  - Systeme im mobilen Netz merken gar nichts
- Roaming durch mobile Netze
  - Beliebige Verschachtelung von MR
  - MN funktionieren auch hinter NEMO
- Bidirektionaler Tunnel zwischen HA und MR
  - Keine Route Optimization
- Multihoming und Location Privacy
- IPv4 und NAT-Traversal

IKS

Proxy Mobile IPv6

- Mobilität als Aufgabe des Netzwerkes
  - Endknoten haben trotz Roaming feste Anbindung
  - Netzwerk stellt mobiles Heimnetz bereit
  - Keine Unterstützung bei den Endknoten nötig
  - Mehrere Netzwerke pro Gerät möglich
  - Viele Features (ECN) durch homogene Technik
- Nur noch ein zentraler HA pro PMIPv6 Domain
- Kein Roaming zwischen PMIPv6 Domains
  - Separate Authentisierung und Provisionierung

IKS

Standards

- RFC 4225; Mobile IPv6 Design; 2001–2002
- RFC 3775; Mobility Support in IPv6; June 2004
- RFC 3776; Home Agent IPsec; June 2004
- RFC 3963; NEMO Basic Support; January 2005
- RFC 4260; 802.11 Fast Handover; November 2005
- RFC 4283; MN Identifier Option; November 2005
- RFC 4285; Authentication Protocol; January 2006
- RFC 4449; Shared Data for CN-BU; June 2006
- RFC 4487; MIPv6 and Firewalls; May 2006
- RFC 4584; Socket-API for MIPv6; July 2006

IKS

Standards

- RFC 4866; Enhanced Route Optimization; May 2007
- RFC 4877; Mobile IPv6 with IKEv2; April 2007
- RFC 4882; MIP6 Location Privacy; May 2007
- RFC 4885; NEMO Terminology; July 2007
- RFC 4886; NEMO Goals; July 2007
- RFC 4887; NEMO Home Network Models; July 2007
- RFC 4908; Multihoming with NEMO; June 2007
- RFC 5026; MIP6 Bootstrapping; October 2007
- RFC 5094; MIPv6 Vendor Specific Option; December 2007

IKS

Standards

- RFC 5096; Experimental Messages; December 2007
- RFC 5142; Home Agent Switch; January 2008
- RFC 5149; Service Selection; February 2008
- RFC 5213; Proxy Mobile IPv6; August 2008
- RFC 5269; FMIPv6 Security; June 2008
- RFC 5270; FMIPv6 over 802.16e; June 2008
- RFC 5271; FMIPv6 over 3G CDMA; June 2008
- RFC 5380; Hierarchical MIPv6; October 2008
- RFC 5447; Diameter MIPv6 NAS; February 2009

IKS

Standards

- RFC 5555; Dual Stack Mobility; June 2009
- RFC 5568; MIP6 Fast Handovers; July 2009
- RFC 5677; IEEE 802.21 Mobility; December 2009
- RFC 5678; DHCPv6 Mobility Service; December 2009
- RFC 5679; DNS Mobility Service; December 2009
- RFC 5726; MIP6 Location Privacy; February 2010
- RFC 5757; Mobile Multicast Problem; February 2010
- RFC 5778; Diameter MIPv6 HA; February 2010
- RFC 5779; Diameter PMIPv6; February 2010

IKS

Fragen?

Lutz Donnerhacke

dig NAPTR 1.6.5.3.7.5.1.4.6.3.9.4.e164.arpa. +dnssec

OpenPGP: DB089309 lutz@iks-jena.de
1C 1C 63 11 EF 09 D8 19 E0 29 65 BE BF B6 C9 CB

Wir beraten und liefern auch normal und kommerziell. ☺

IKS