Karlsruher Institut für Technologie

Kapitel 11 – Mobiles Internet mit Mobile IP

Vorlesung Mobilkommunikation Wintersemester 2016/17
Prof. Dr. Oliver Waldhorst (HS Karlsruhe), Markus Jung

INSTITUT FÜR TELEMATIK

Gliederung


Mobiles TCP
Mobile Ad Hoc Netze
Mobile IP
WLAN, Bluetooth
GSM, UMTS, LTE
Mobilitätsmanagement
Medienzugriff
Drahtlose Übertragung

Motivation

- Nutzer wünschen sich ubiquitären Internetzugang
  - zu jeder Zeit
  - an jedem Ort
  - über beliebige Technologie
- Erfordert Mobilitätsunterstützung → mobile Stationen
  - Wechsel zwischen Subnetzen der gleichen Technologie (horizontale Handover)
    - Bessere Verfügbarkeit/Signalstärke (geographische Bewegung der mobilen Station)
  - Wechsel zwischen Subnetzen unterschiedlicher Technologie (vertikale Handover)
    - Bessere Verfügbarkeit/Signalstärke (geographische Bewegung der mobilen Station)
    - Höherer Bandbreite
    - Kürzere Latenz
    - Geringere Zugangskosten
- Mobilfunknetze (GSM, UMTS) bieten Mobilitätsunterstützung, aber (noch) nicht IP-basiert
  - Umstellung auf IP
    - Besser geeignet für heterogene Dienste
    - Ermöglicht Integration anderer Technologien, bspw. WLAN (so genannte "4G-Netze")

[11.5]

Problematik

- Doppelfunktion von IP-Adressen
  - Wegewahl im Internet basiert auf IP-Zieladresse von Dateneinheiten
    - Adresspräfix (z.B. 129.13.42/8) legt physikalisches Subnetz fest
    - IP-Adresse ist Lokator
  - Gleichzeitig werden IP-Adressen in Transportprotokollen und Anwendungen zur Identifikation von Stationen genutzt
    - IP-Adresse ist Identifikator
- Konsequenz für mobile Stationen
  - Wechsel des Subnetzes erfordert Wechsel der IP-Adresse
    - Wechsel der IP-Adresse wiederum terminiert bestehende Kommunikationsverbindungen
  - Transparente Mobilität nicht möglich

Lösungsmöglichkeiten

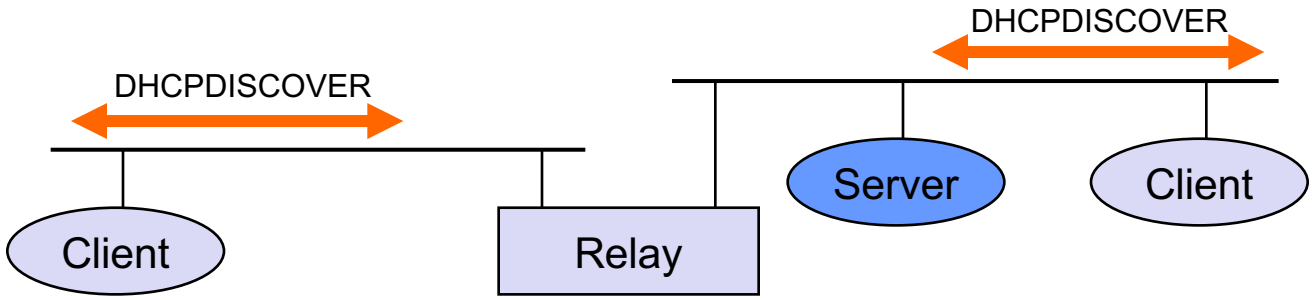
- Host-spezifische Routen zur mobilen Station
  - Anpassen der Routing-Einträge aller Router auf dem Kommunikationspfad → Skaliert nicht Internet-weit!
- Separate IP-Adressen für Wegewahl u. Identifikation
  - Je nach Lokation andere IP-Adresse für Wegewahl
  - Konstante IP-Adresse für Transportprotokolle und Anwendungen → Skaliert, aber…
    - Wie sollen mobile Stationen gefunden werden, wenn sich IP-Adresse ändert?
    - DNS-Aktualisierung für schnelle Handover zu träge

Portabilität	Mobilität
Mobile Stationen in versch. Subnetzen betrieben (Subnetz-Wechsel selten) Erhalt aktiver Komm.verbindungen nicht notwendig Lösung durch DHCP Mobile Stationen erhalten bei Subnetz-Wechsel neue IP-Adresse über DHCP	Häufige Subnetz-Wechsel Aktive Komm.verbindungen sollen erhalten werden Lösung durch Mobile IP

Dynamic Host Configuration Protocol (DHCP)

[11.7]
[11.8]

- Anwendung
  - Automatische Konfiguration vernetzter Stationen
  - Zuweisung einer IP-Adresse für begrenzte Zeitspanne
  - Zusätzliche Konfigurationsparameter, bspw.
    - IP-Adresse(n) von DNS-Server(n), Time-Server(n)
    - Subnetz-Maske, Zugangsrouter, Domain Name für Station
- Client-Server-Modell
  - Station (Client) sendet Anfrage per MAC-Broadcast an DHCP-Server, u.U. über DHCP-Relay
- Eigenschaften
  - Mehrere Server möglich (Koordination zurzeit noch nicht standardisiert)
  - Erneuerung der Konfiguration (IP-Addr müssen regelm. erneuert werden)
  - Modularer Aufbau (DHCP-Nachrichten, insbes. DHCPOFFER, enthalten IP-Adressen und andere Konfigurationsparameter in separaten Optionen)



Mobile IPv4

- Ziel: Mobile Stationen können bei Wechsel des Subnetzes aktive Kommunikationsverbindungen fortführen
  - IP-Adresse ändert sich nur für Zustellung von Dateneinheiten
  - Transparenz an den Endpunkten der Kommunikation gegenüber Transportprotokollen und Anwendungen

[11.9]

- Anforderungen
  - Kompatibilität
    - Keine Änderung an Schicht-2-Protokollen, Routern oder Festnetzstationen
    - Kommunikation zwischen mobilen Stationen und Festnetz-Stationen
  - Sicherheit
    - Authentifizierung von Registrierungsnachrichten
    - Privatsphäre soll geschützt werden
  - Effizienz und Skalierbarkeit
    - Mobile Stationen evtl. über eine schmalbandige Funkstrecke angebunden
      - Möglichst wenig Signalisierung auf Luftschnittstelle
    - Große Anzahl mobiler Stationen soll Internet-weit unterstützt werden

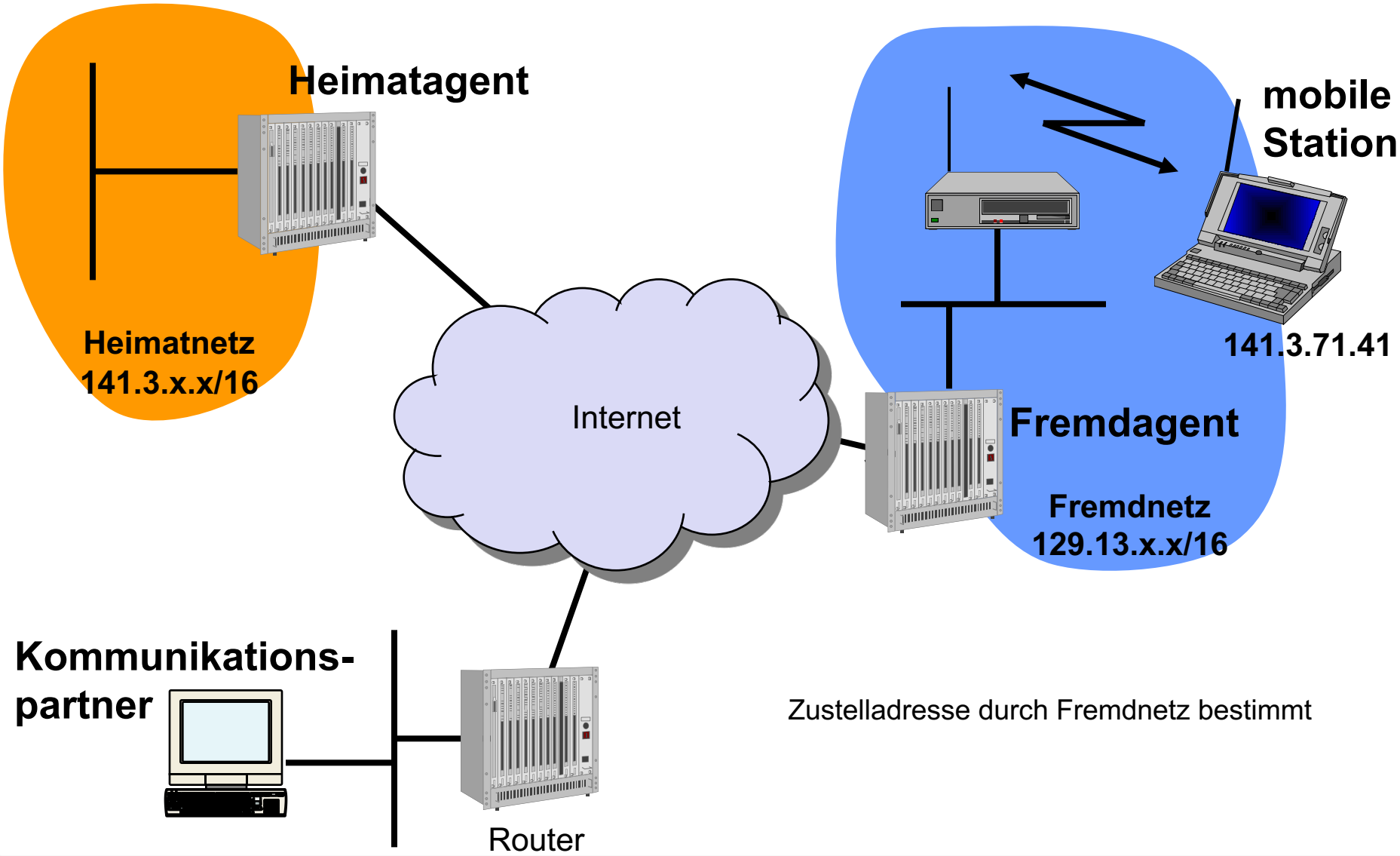
Terminologie

- Mobile Station
  - Station, die das Subnetz wechseln kann, ohne bestehende Kommunikationsverbindungen zu verlieren
- Kommunikationspartner (der mobilen Station) (Corresponding Node)
  - Kann ebenfalls mobil sein oder Festnetz-Station
- Heimatnetz (Home Network)
  - Mobiler Station zugewiesenes, eindeutiges Subnetz
  - Mobile Station kommuniziert im Heimatnetz ohne Mobile IP
- Fremdnetz (Foreign Network)
  - Jedes Subnetz außer dem Heimatnetz
- Heimatadresse (Home Address)
  - IP-Adresse der mobilen Station im Heimatnetz
  - Transportprotokolle und Anwendungen benutzen Heimatadresse auch dann, wenn sich mobile Station im Fremdnetz aufhält
- Zustelladresse (Care-of Address)
  - IP-Adresse, unter der mobile Station im Fremdnetz erreichbar ist
  - Z.B. über DHCP zugewiesen

Terminologie

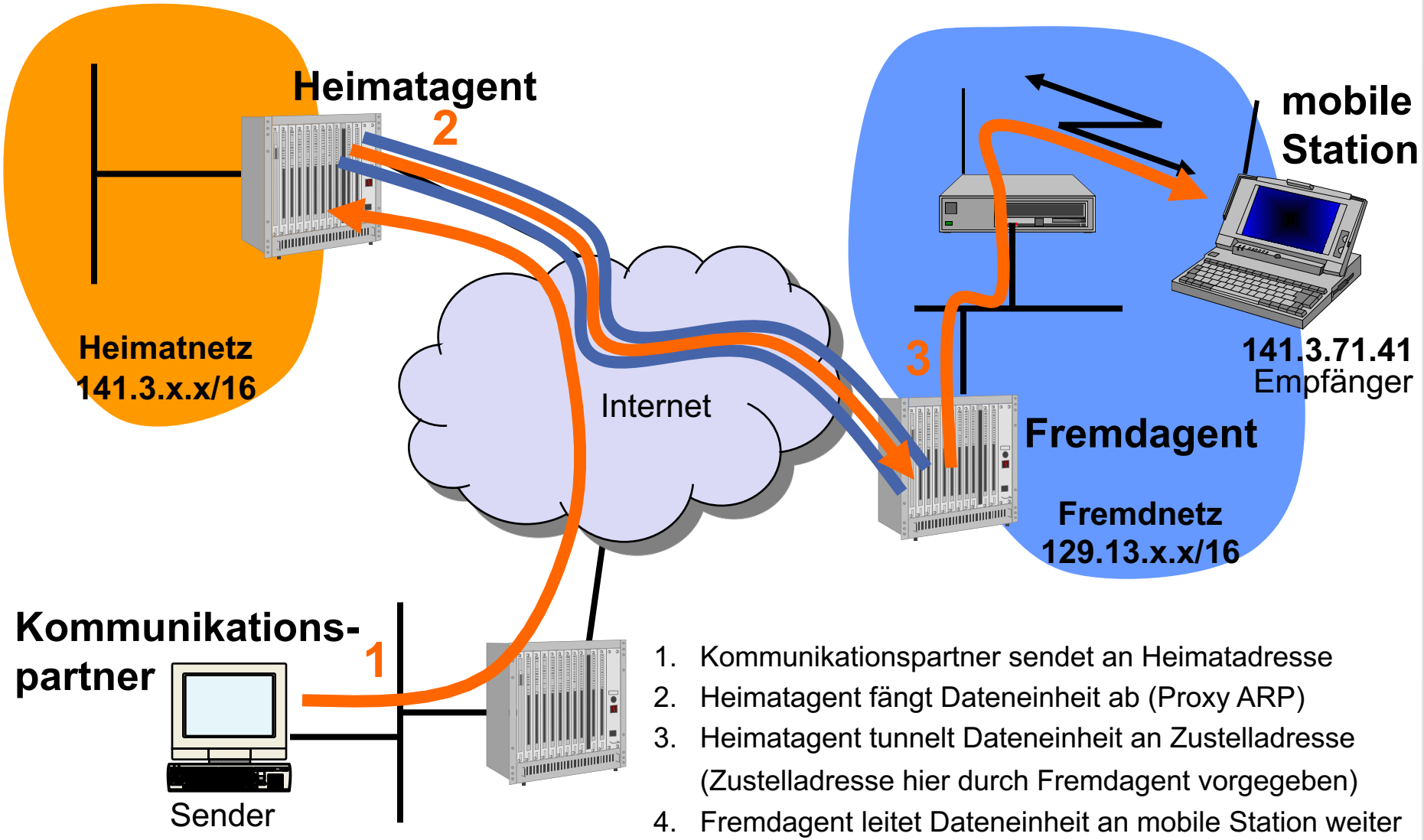
- Heimatagent (Home Agent)
  - Einheit im Heimatnetz, typischerweise Router
  - Stellvertreter der mobilen Station im Heimatnetz
  - Kennt aktuelles Fremdnetz (Aufenthaltsort) der mobilen Station
  - Endpunkt eines Tunnels zum Fremdnetz
    - Tunnelt vom Kommunikationspartner empfangene Dateneinheiten zum Fremdnetz
    - Leitet aus dem Fremdnetz getunnelte Dateneinheiten zum Kommunikationspartner weiter
- Fremdagent (Foreign Agent)
  - Einheit im Fremdnetz, typischerweise Zugangsrouter
  - Endpunkt des Tunnels zum Heimatagenten
    - Tunnelt von mobiler Station empfangene Dateneinheiten zum Heimatagenten
    - Leitet vom Heimatagenten getunnelte Dateneinheiten zur mobilen Station weiter
  - Kann Zustelladresse vorgeben

Beispielnetz



Zustelladresse durch Fremdnetz bestimmt

Datentransfer zur mobilen Station

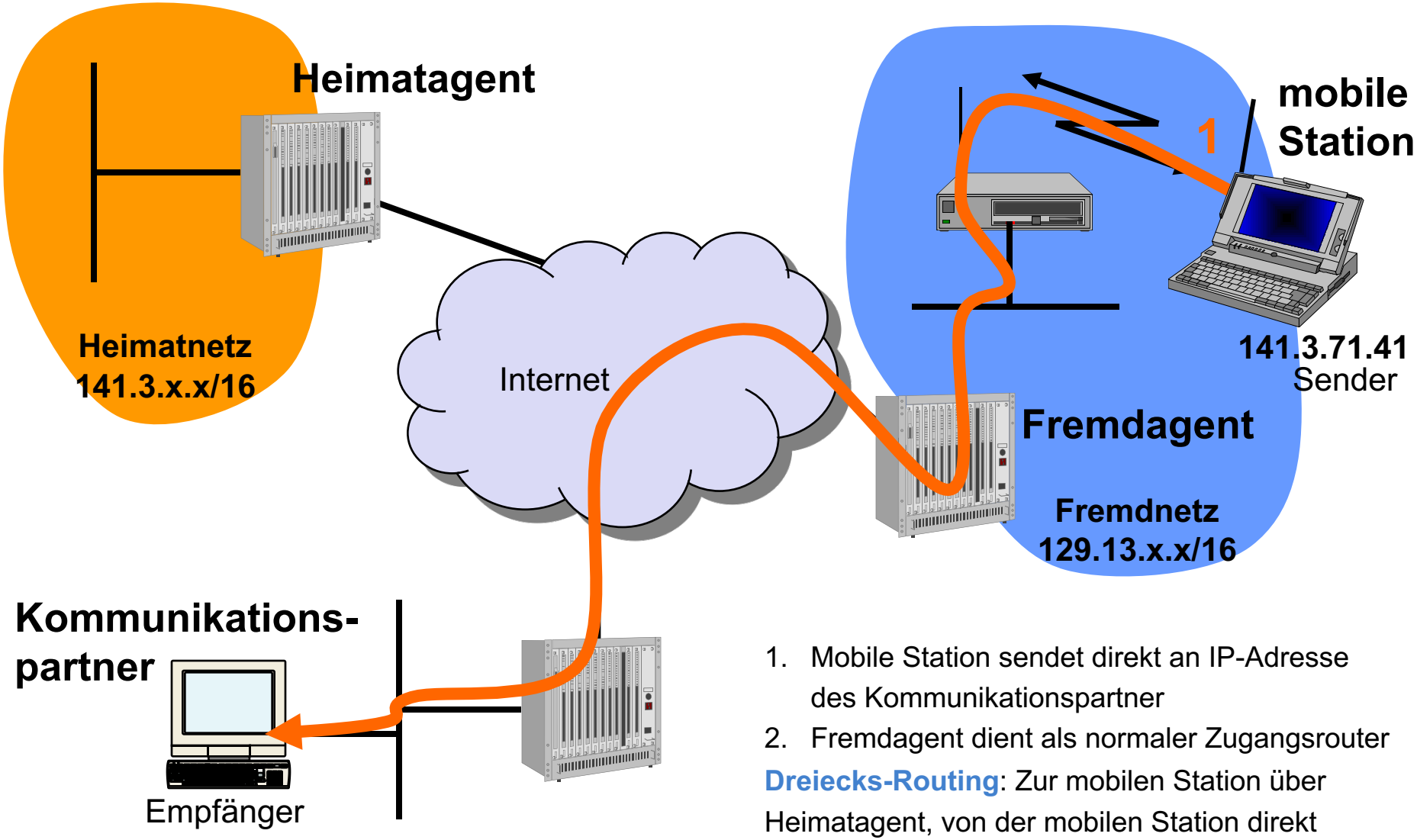


1. Kommunikationspartner sendet an Heimatadresse
2. Heimatagent fängt Dateneinheit ab (Proxy ARP)
3. Heimatagent tunnelt Dateneinheit an Zustelladresse (Zustelladresse hier durch Fremdagent vorgegeben)
4. Fremdagent leitet Dateneinheit an mobile Station weiter

Arten von Zustelladressen

- Zustelladresse des Fremdagenten
  - Zustelladresse gehört dem Fremdagenten
  - Mobile Station registriert sich über Fremdagent beim Heimatagenten
  - Fremdagent ist Endpunkt des Tunnels zum Heimatagenten
  - Vorteil: Sparsamer Umgang mit IP-Adressen, da eine Zustelladresse von mehreren mobilen Stationen verwendet werden kann
- Eigene Zustelladresse
  - Mobile Station konfiguriert eigene Zustelladresse
  - Mobile Station registriert sich direkt beim Heimatagenten
  - Mobile Station ist Endpunkt des Tunnels zum Heimatagenten
  - Vorteil: Kein Fremdagent erforderlich

Datentransfer von der mobilen Station



1. Mobile Station sendet direkt an IP-Adresse des Kommunikationspartner
2. Fremdagent dient als normaler Zugangsrouter

Dreiecks-Routing: Zur mobilen Station über Heimatagent, von der mobilen Station direkt

Probleme beim Dreiecks-Routing

- Quelladress-Filter
  - Viele Router und Firewalls verwerfen Dateneinheiten mit topologisch inkorrekten Quelladressen
  - Quelladresse der mobilen Station muss Heimatadresse sein
  - Daher nicht topologisch korrekt
- Lebensdauer der Dateneinheit (TTL)
  - Hin- und Rückrichtung sind evt. unterschiedlich lang
    - TTL mag für eine Richtung genügen, für andere aber nicht
  - Mobile Station muss TTL für ausgehende Dateneinheiten nach Subnetz-Wechsel ggf. anpassen

Reverse Tunneling

- Von mobiler Station gesendete Dateneinheiten werden
  - durch den Fremdagenten gekapselt
  - über Heimatagent getunnelt
- Lösung der Probleme von Dreiecks-Routing
  - Dateneinheiten topologisch korrekt
  - Lösung der TTL-Problematik (Tunnel hat Länge 1)
- Nachteile
  - Geringere Effizienz durch (potentiell) längere Wege
  - Sicherheitsproblematik bei Firewalls
    - Umgekehrter Tunnel kann zur Umgehung von Schutzmechanismen missbraucht werden
      - Böswillige Station im Fremdnetz kann Tunnel ihres Opfers zu ebenfalls böswilligen Heimatagent umleiten (Tunnel Hijacking)
    - Zusätzliche Authentifizierung löst dieses Problem
      - Zwischen mobiler Station und Fremdagent
      - Zwischen Fremdagent und Heimatagent

Netzintegration und Mobilitätsmanagement

- Netzintegration im Festnetz
  - Zugangsrouter versenden periodisch Router-Advertisement-Nachrichten
    - Explizite Anforderung durch Router-Solicitation-Nachricht möglich
    - Enthalten IP-Adressen der Zugangsrouter
    - Erweiterung von ICMP (RFC 1256)
    - Durch „Preference Level“ können bestimmte Zugangsrouter im Subnetz priorisiert werden
- Probleme bei Mobilität
  - Mobile Stationen können nicht erkennen, ob ein Zugangsrouter als Heimat- bzw. Fremdagent fungiert
  - Zustelladressen eines Fremdagenten können nicht bekannt gegeben werden
- Lösung
  - Zugangsrouter versenden periodisch Agent-Advertisement-Nachrichten (RFC 3344)
  - Dies sind Router-Advertisement-Nachrichten mitt zusätzlicher Option
  - Beinhalten Informationen für mobile Stationen

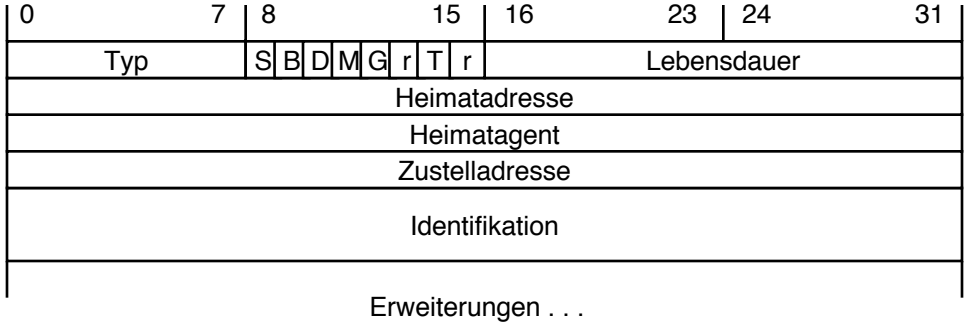
0 7	8 15	16 23	24 31
Typ = 9	Code = 0	Prüfsumme	
#Adressen	Adresslänge	Lebensdauer	
Router Adresse 1			
Preference Level 1			
Router Adresse 2			
Preference Level 2			
. . .			
Router Adresse *#Adressen*			
Preference Level *#Adressen*			

Registrierung

- Mobile Station erhält Zustelladresse (von Fremdagent oder über DHCP)
- Danach: Registrierung beim Heimatagent
  - Heimatagent erfährt damit aktuellen Aufenthaltsort der mobilen Station
- Registrierung besitzt stets begrenzte Lebensdauer
  - Danach automatisch gelöscht (Soft State)
  - Registrierung muss periodisch aufgefrischt werden
- Registrierung durch Authentifikation abgesichert

- Registrierungsanforderung:
  - Kapselung in UDP-Dateneinheiten (schneller als TCP, da kein Verb.aufbau)
  - Eigener Mechanismus für Übertragungswiederholungen
  - Ziel der UDP-Dateneinheit ist je nach Art der Zustelladresse der Heimatagent oder der Fremdagent

  - Aufbau des Nutzdatenteils einer Registrierungs-anforderung:



Sicherheit bei Mobile IPv4

- Sicherheitsprobleme
  - Authentizität nicht gewährleistet (unberechtigte Registrierungen)
    - Angreifer kann sich gegenüber Heimat- und Fremdagent als mobile Station ausgeben
    - Angreifer kann sich gegenüber mobiler Station als Heimat- oder Fremdagent ausgeben
  - Angreifer kann Dateneinheiten seines Opfers an falsche Zustelladresse umlenken
  - Wiedereinspiel-Angriffe (Replay-Attacken)

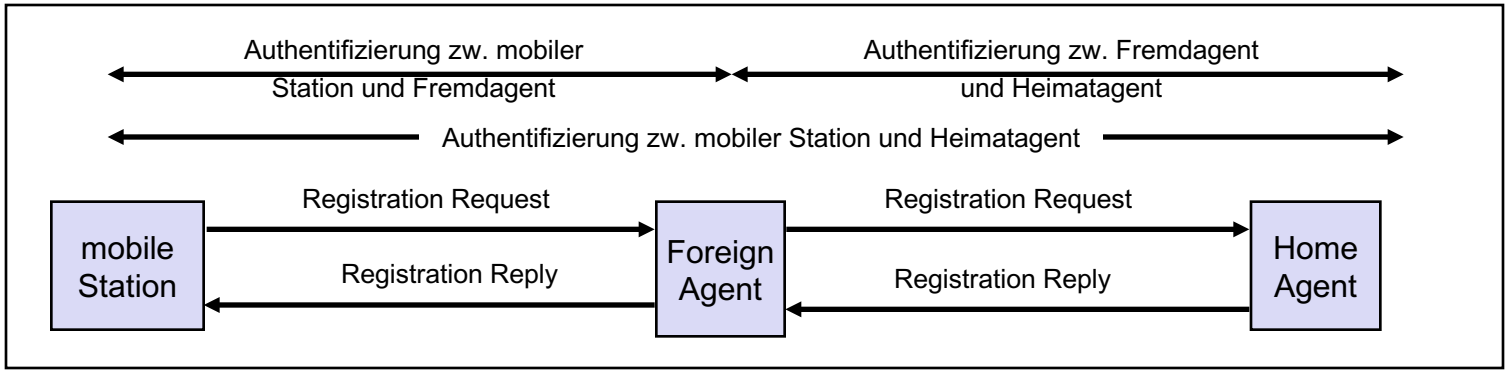
- Lösung
  - Authentifizierung der Registrierungsnachrichten
  - Schutz vor Wiedereinspiel-Angriffen

- Verschlüsselung nicht enthalten; erfordert zusätzliche Mechanismen

- Sicherheitsbeziehungen
  - Zwischen mobiler Station, Heimatagent und evtl. auch Fremdagent
  - Sicherheitsbeziehung (für ein bestimmtes Stationspaar) enthält
    - Authentifizierungsalgorithmus (Voreinstellung: HMAC-MD5)
    - Schlüssel (symmetrisch oder asymmetrisch)
    - Methode zur Verhinderung von Wiedereinspiel-Angriffen
  - Aushandlung der Sicherheitsbeziehung und Schlüsselaustausch durch externen Mechanismus

Sicherheit bei Mobile IPv4

- Authentifizierung der Registrierung
  - Vorgeschrieben zwischen mobiler Station und Heimatagent
  - Optional zwischen [mobiler Station ←→ Fremdagent ←→ Heimatagent]
  - Authentifizierungserweiterung für Registrierungsnachrichten



- Verhindern von Wiedereinspiel-Angriffen
  - Identifikationsfeld ist für jede Nachricht verschieden
  - 2 Verfahren: Zeitstempel (erfordert synchronisierte Uhren), Einmalwerte („Nonces“), optional
  - Identifikationsfeld geht in Authentifizierungsdaten ein
- Probleme
  - Authentifikation mit Fremdagent
    - Fremdagent gehört u.U. zu anderer Organisation als mobile Station und Heimatagent
  - Kein Protokoll für die Schlüsselverwaltung und Schlüsselverteilung im Internet standardisiert

Probleme mit Mobile IPv4

- Firewalls
  - Verhindern typischerweise den Einsatz von Mobile IP
  - Spezielle Konfigurationen sind nötig, z.B. Reverse Tunneling
- QoS
  - Erneute Reservierungen nach jedem Handoff
  - Tunneln verhindert das Erkennen gesondert zu behandelnder Datenströme
- Dreiecks-Routing
  - Hohe Verzögerungszeiten
  - Höhere Netzlast

Mobile IPv6

[11.11]

- Mobilitätsunterstützung für IPv6
  - Pendant zu Mobile IPv4
- Hohe Zahl von IPv6-Adressen erlaubt eigene Zustelladresse für jede mobile Station
  - IPv6-Konfiguration: Mobile Station wählt zufällige Zustelladresse und überprüft diese auf Eindeutigkeit
  - Mobile Station ist stets Endpunkt des Tunnels zum Heimatagenten
  - Fremdagent wird nicht mehr benötigt
- Netzintegration
  - Ähnlich wie in Mobile IPv4 über ICMPv6 und DHCPv6
- Geänderte Terminologie
  - Binding Update = Registration Request in Mobile IPv4
  - Binding Acknowledgement = Registration Reply in Mobile IPv4

Modi und Eigenschaften von Mobile IPv6


[11.11]

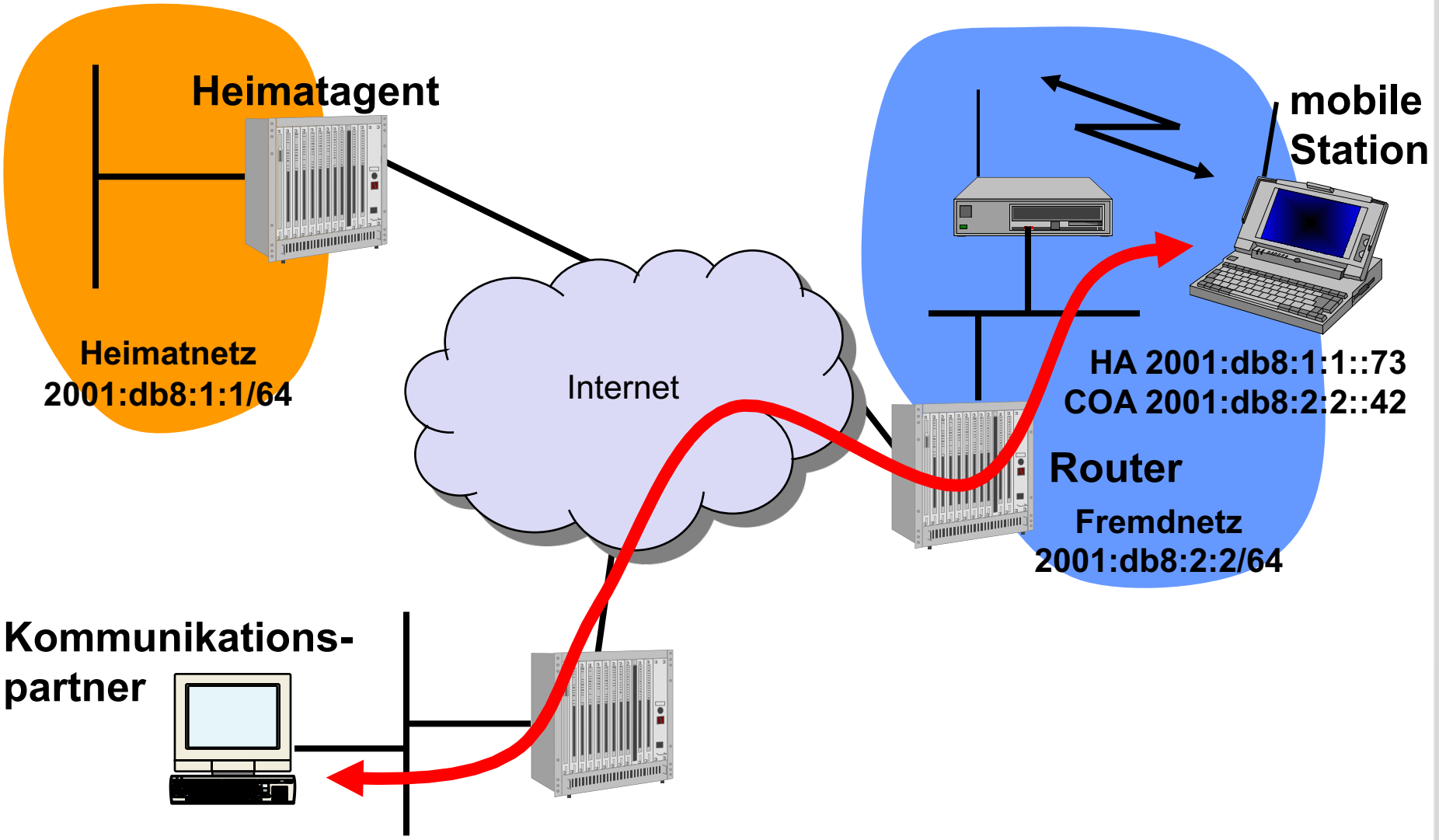
- Bidirektionales Tunneln (wie bei Mobile IPv4)
  - Vorteil: Mobilitätsunterstützung vom Kommunikationspartner nicht nötig
  - Nachteil: Erhöhte Zustelllatenz für Dateneinheiten
- Routenoptimierung (Ziel: Reduktion der Latenz für interaktive Echtzeit-Anwendungen)
  - Direktes Routing zwischen mobiler Station und Kommunikationspartner
    - Kein Umweg über Heimatagent, kein Dreiecks-Routing
  - Dateneinheiten im Netz
    - IPv6-Köpfe enthalten Zustelladresse (als Quelle oder Ziel)
    - Erweiterungen der IPv6-Köpfe enthalten Heimatadresse
  - Nachteil: Erfordert Mobilitätsunterstützung vom Kommunikationspartner

- Weitere Eigenschaften
  - Authentifizierung und Sicherheit von vorneherein integriert
  - IPsec für bidirektionales Tunneln
  - Return-Routability-Prozedur für Routenoptimierung
  - Falls Adresse des Heimatagenten unbekannt ist, kann diese erkundet werden (Dynamic Home Agent Discovery)
  - Heimatadresse der mobilen Station kann dynamisch angepasst werden, wenn z.B. Heimatnetz neues Präfix erhält (Mobile Prefix Discovery)

IPv6-Autokonfiguration

- Zustandsbehaftete Adress-Konfiguration
  - Zustelladresse wird einer mobilen Station auf Anfrage von DHCPv6-Server zugewiesen
  - DHCPv6-Server merkt sich vergebene Adressen
- Zustandslose Adress-Konfiguration
  - Mobile Station erhält Subnetz-Präfix durch Router Advertisement
  - Durch Kombination des Subnetz-Präfixes mit Link-abhängigen Identifikator (z.B. aufbauend auf 48-bittiger Ethernetadresse) bildet mobile Station Zustelladresse
- Duplicate Address Detection
  - Wird benötigt, um doppelte Adressen zu erkennen
  - Für zustandslose wie für zustandsbehaftete Adress-Konfiguration
  - Protokollablauf
    - Station sendet Neighbor-Solicitation-Nachricht mit zu prüfender Adresse an alle Nachbarn
    - Falls Adresse schon vergeben…
      - Station, der die Adresse gehört, sendet Neighbor-Advertisement-Nachricht
      - Anfragende Station muss andere Adresse wählen

Routenoptimierung



Routenoptimierung

- Idee: Direkter Austausch zwischen mobiler Station und Kommunikationspartner
  - Tunnel zwischen mobiler Station und Kommunikationspartner ineffizient
    - Echtzeit-Anwendungen wie Internet-Telefonie senden viele kleine Pakete
    - Zusätzlicher IPv6-Header fällt mit 40 Byte stark ins Gewicht
  - Daher alternativer Mechanismus über IPv6-Erweiterungsköpfe
  - Erfordert Mobilitätsunterstützung beim Kommunikationspartner
  - Initiiert von mobiler Station, wenn über den Heimatagenten getunnelte Dateneinheit empfangen wird

- Datentransfer
  - Transportprotokolle und Anwendungen senden an/von Heimatadresse
  - Sender ersetzt Heimatadresse (HA) durch Zustelladresse (COA) bei Verarbeitung der Dateneinheit auf Vermittlungsschicht
  - Heimatadresse wird in Erweiterung des IPv6-Kopfs untergebracht
    - IPv6 Destination Options Extension Header beim Transfer von mobiler Station zum Kommunikationspartner
    - IPv6 Routing Extension Header beim Transfer vom Kommunikationspartner zur mobilen Station
  - Dateneinheit wird direkt an/von Zustelladresse gesendet
  - Empfänger der Dateneinheit tauscht Heimatadresse und Zustelladresse vor Auslieferung an Transportprotokolle und Anwendungen

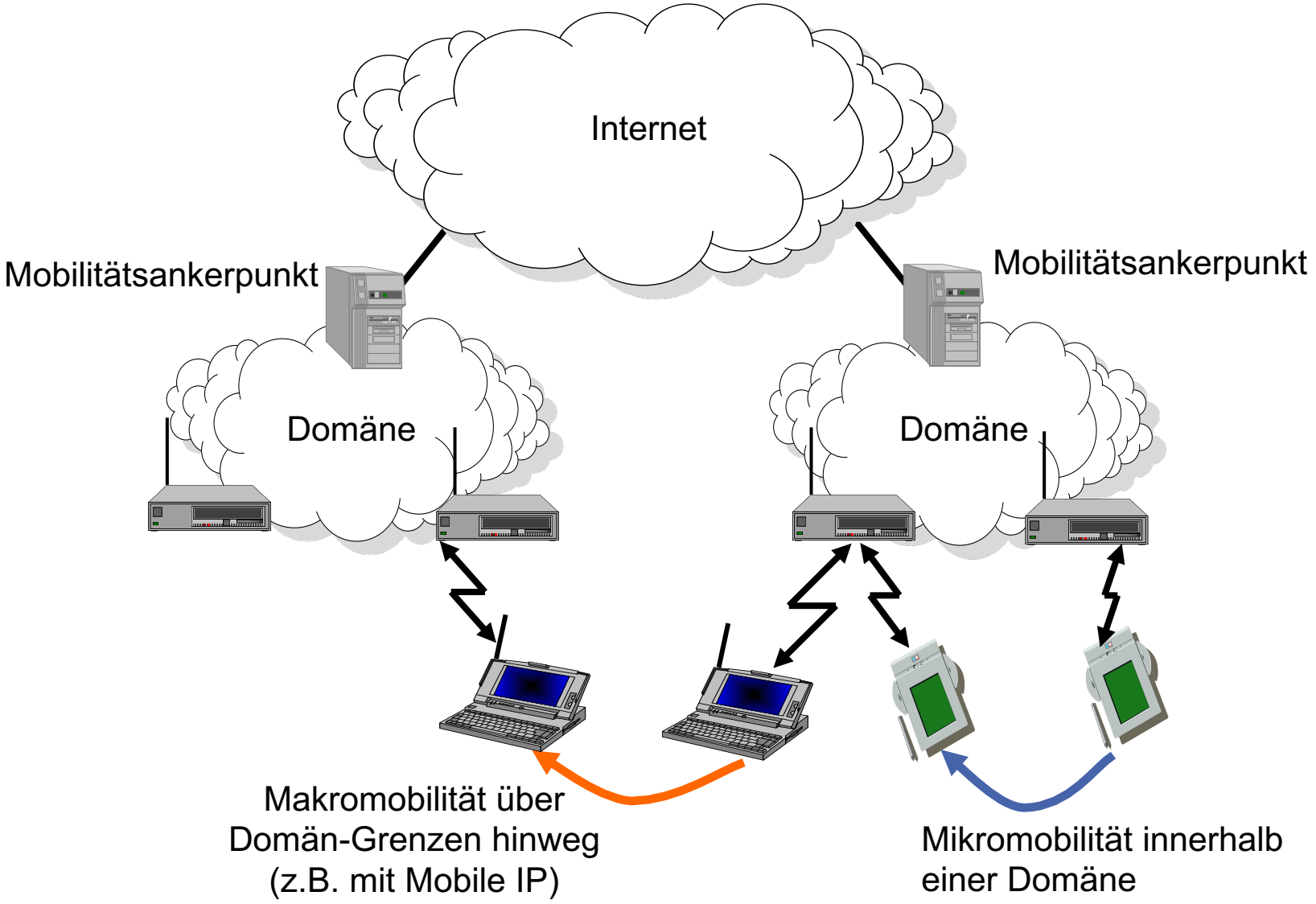
Routenoptimierung

- Effizienz
  - Geringere Zustelllatenzen für Dateneinheiten als bei bidirektionalem Tunneln
  - Datentransfer funktioniert auch bei Ausfall des Heimatagenten
  - Heimatagent wird entlastet
  - Quelladresse topologisch korrekt
    - Keine Probleme mit Quelladress-Filtern in Routern und Firewalls
- Sicherheit
  - Authentifizierung schwierig
    - I.A. kein Vertrauensverhältnis zwischen mobiler Station und Kommunikationspartner
    - Vorkonfiguration nicht möglich
  - Keine Privatsphäre
    - Kommunikationspartner kann aktuellen Aufenthaltsort der mobilen Station von Zustelladresse ableiten

Registrierung

- Registrierung beim Heimatagenten
  - Ermöglicht bidirektionales Tunneln
  - Ist auch für Routenoptimierung erforderlich
  - Protokollablauf
    - Mobile Station schickt Binding-Update-Nachricht mit Heimat- und Zustelladresse zum Heimatagent
    - Heimatagent bestätigt mit Binding-Acknowledgement-Nachricht
  - IPsec für Integrität und Authentizität der Nachrichten
- Registrierung beim Kommunikationspartner
  - Erfordert vorherige Registrierung mit Heimatagent
  - Prozedur wird mit Keyed-Hash-Algorithmus gesichert
    - Keine IPsec Security Association notwendig
  - Schlüssel K_{bm} wird aus „Keygen Tokens“ in Home-Test- und Care-of-Test-Nachrichten generiert
    - Ein Angreifer muss auf beiden Pfaden sein, um K_{bm} zu erlangen

Mikromobilität

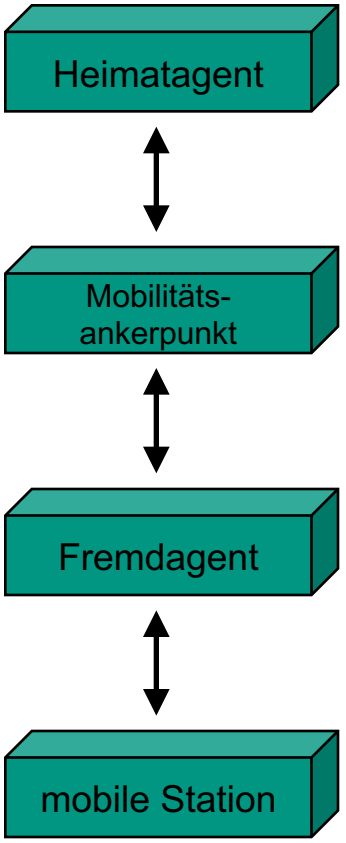


Makromobilität vs. Mikromobilität

- Makromobilität
  - Kann mit Mobile IP realisiert werden
  - Registrierungen erfordern globalen Nachrichtenaustausch
    - hoher Signalisierungsaufwand
    - lange Signalisierungszeiten
    - hoher Datenverlust
    - nahtlose Handovers nicht möglich
- Mikromobilität
  - Effizientere Mobilitätsunterstützung innerhalb einer Domäne
    - Ermöglicht Ansätze, die Internet-weit nicht skalieren würden
    - Bspw. Host-spezifische Routen
  - Mobile Station registriert sich mit einem lokalen **Mobilitätsankerpunkt**
    - Signalisierung nur innerhalb der Domäne
    - Mobile Station erhält IP-Adresse vom Mobilitätsankerpunkt
    - Diese kann als Zustelladresse bei Heimatagent und Kommunikationspartnern registriert werden
  - Mobilität innerhalb der Domäne transparent nach außen
    - Keine erneute Registrierung bei Heimatagent und Kommunikationspartnern
  - Ansätze aus der IETF
    - Regionale Registrierungen in Mobile IPv4
    - Hierarchisches Mobile IPv6
    - *Cellular IP*
    - *Handoff-Aware Wireless Access Internet Infrastructure (Hawaii)*

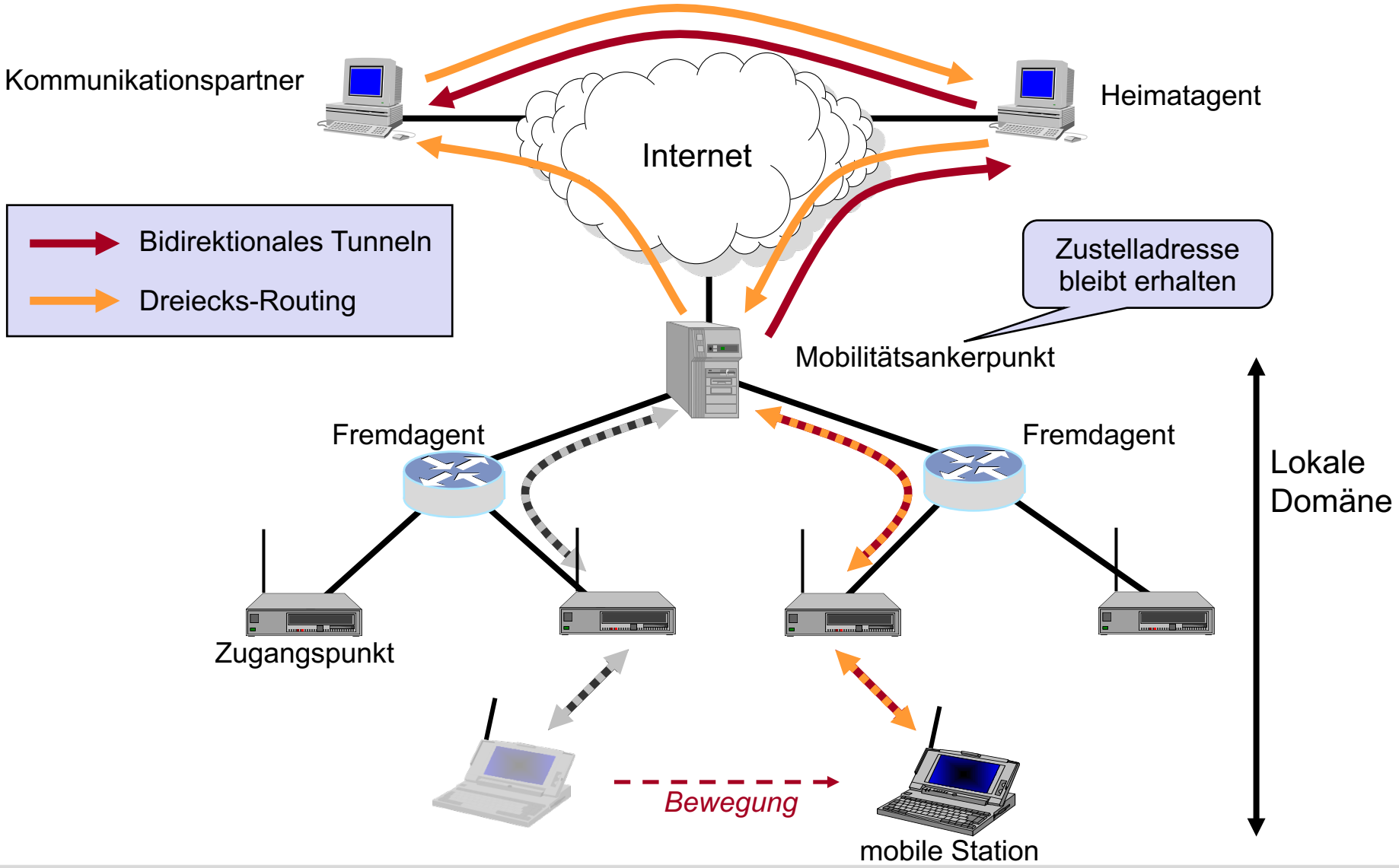
Regionale Registrierungen in Mobile IPv4

- Zwei (oder mehr) Level von Fremdagenten
  - Mobilitätsankerpunkt
  - Regionale Fremdagenten (optional)
  - Fremdagenten
- Mobilitätsankerpunkt liefert Zustelladresse, die für Heimatagent und Kommunikationspartner sichtbar ist
  - Tunnel zwischen mobiler Station und Mobilitätsankerpunkt
- Mobile Station behält Zustelladresse bei Wechsel des Fremdnetzes
- Regionale Registrierung bei Subnetz-Wechsel
- Reguläres Mobile IP (Makromobilität) bei Wechsel des Mobilitätsankerpunkts



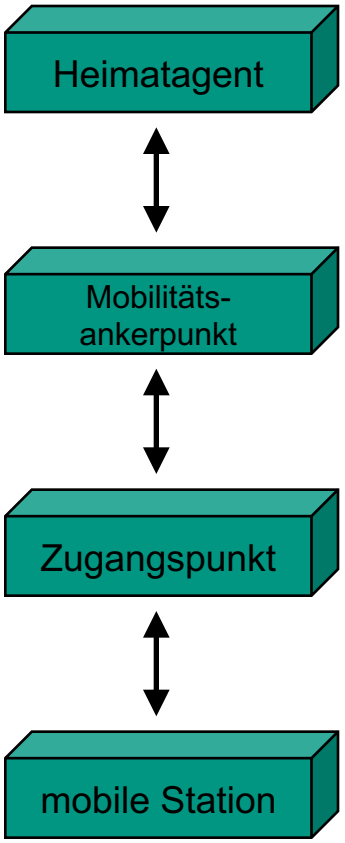
[11.17]

Regionale Registrierungen in Mobile IPv4



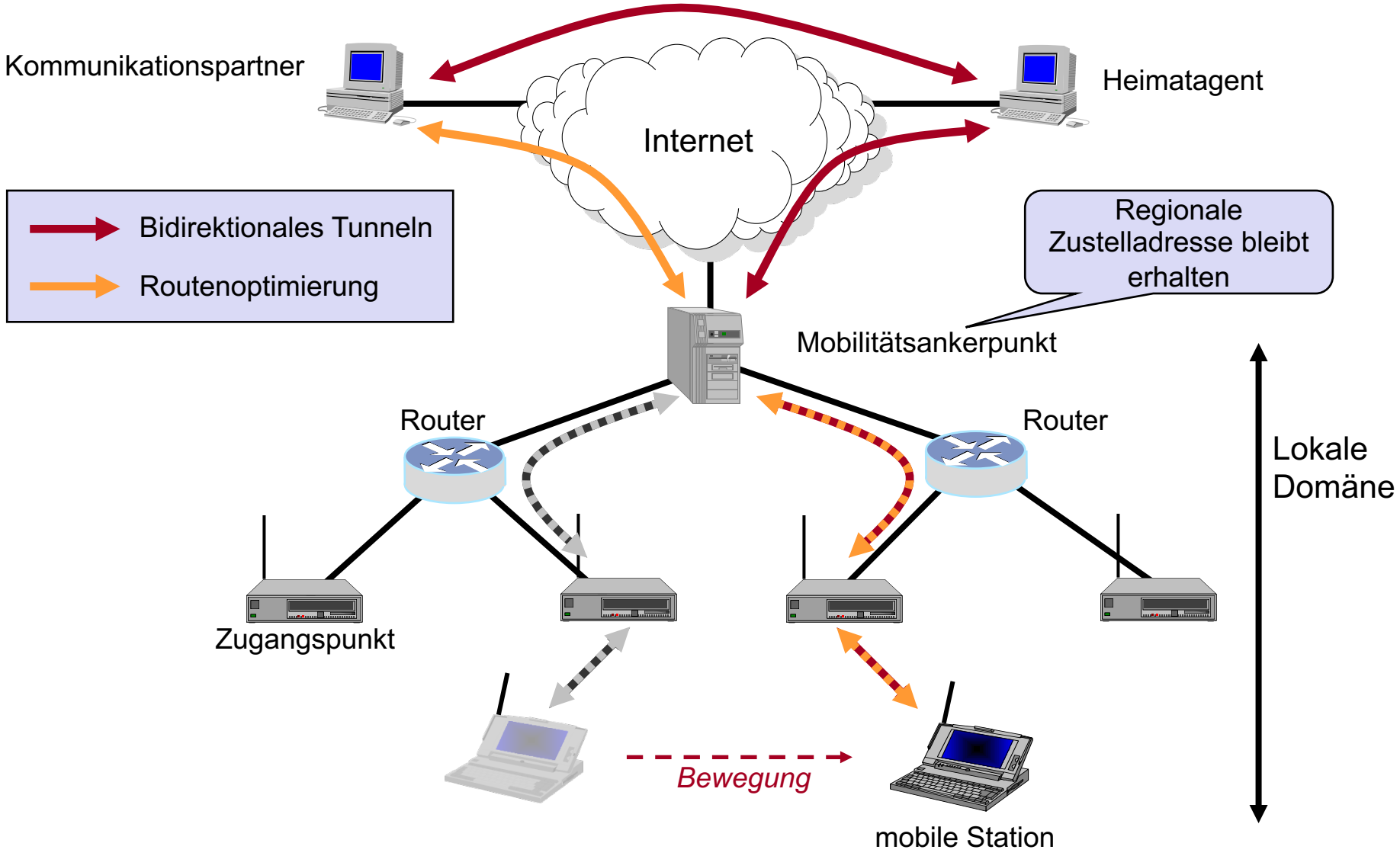
Hierarchisches Mobile IPv6

- Zwei Levels von Heimatagenten
  - Regulärer Heimatagent
  - Mobilitätsankerpunkt
- Mobilitätsankerpunkt liefert **regionale Zustelladresse**
  - Regionale Zustelladresse für Heimatagent und Kommunikationspartner sichtbar
  - Tunnel zwischen mobiler Station und Mobilitätsankerpunkt
- Mobile Station konfiguriert **On-Link-Zustelladresse**
- Mobile Station behält regionale Zustelladresse bei Wechsel des Fremdnetzes
- Regionale Registrierung bei Subnetz-Wechsel
- Reguläres Mobile IP (Makromobilität) bei Wechsel des Mobilitätsankerpunkts



[11.18]

Hierarchisches Mobile IPv6



Zusammenfassung

- Mobilitätsunterstützung auf Vermittlungsschicht erfordert speziellen Umgang mit IP-Adressen
  - Portabilität: Zuweisung einer „passenden“ IP-Adresse am jeweiligen Aufenthaltsort
  - Mobilität: Routing zum entsprechenden Gerät anhand der jeweils gültigen IP-Adresse
- MobileIP unterstützt Routing transparent für Kommunikationspartner und Netz
  - Heimatagent als Mobiliätsanker
  - Fremdagent als Endpunkt eines IP-Tunnels
- Besser verankert in IPv6
  - Direktes Routing zwischen Kommunikationspartner und mobilem Gerät

Übungen

11.1 Welche Probleme ergeben sich mit IP in Zusammenhang mit mobilen Stationen? Wie lassen sich diese lösen?

11.2 Welche Funktionalität stellt DHCP bereit? Welche Probleme lassen sich damit nicht lösen?

11.3 Skizzieren Sie die Funktionsweise von Mobile IP.

11.4 Was versteht man unter Dreiecks-Routing?

11.5 Wie lässt sich der Datenpfad bei Mobile IP optimieren?

11.6 Was geschieht bei einem Wechsel in ein anderes Fremdnetz? Wie lässt sich hier ein Datenverlust vermeiden?

11.7 Welche Probleme werden durch Reverse Tunneling gelöst? Welche nicht?

11.8 Wie unterscheiden sich Mobile IPv4 und Mobile IPv6?

11.9 Wie erkennt eine mobile Station den Wechsel in ein anderes Fremdnetz? Vergleichen Sie die Mechanismen bei IPv4 und IPv6.

11.10 Welche Sicherheitsprobleme treten beim Einsatz von Mobile IP auf? Was lässt sich dagegen tun?

Referenzen, weiterführende Literatur

[11.1] Jochen Schiller; Mobilkommunikation, Pearson Studium, 2. Auflage 2003

[11.2] James D. Solomon; Mobile IP: The Internet Unplugged, Prentice Hall, 1997

[11.3] Charles E. Perkins; Mobile IP: Design Principles and Practices, Addison-Wesley, 1997

[11.4] Andrew T. Campbell et. al.; Design, Implementation, and Evaluation of Cellular IP, IEEE Personal Communications, August 2000

[11.5] S. Keshav; Why Cell Phones Will Dominate the Future Internet, ACM Computer Communications Review, April 2005

[11.6] Andrew T. Campbell et al.; Comparison of IP Micromobility Protocols, IEEE Wireless Communications, Vol. 9 Nr. 1, Februar 2002

[11.7] R. Droms; Dynamic Host Configuration Protocol, RFC 2131, März 1997

[11.8] R. Droms et al.; Dynamic Host Configuration Protocol for IPv6, RFC 3315, Juli 2003

[11.9] C. Perkins; IP Mobility Support, RFC 3344, 2002

[11.10] C. Perkins; IP Encapsulation within IP, RFC 2003, 1996

[11.11] Hesham Soliman; Mobile IPv6, Addison-Wesley, 2004