

Mobilkommunikation

VII. Mobiles Internet




Kapitel 11 Mobile Vermittlungsschicht



Kapitelübersicht

- I. **Einleitung**
 - 1. Einführung und Grundlagen
- II. **Drahtlose Telekommunikationssysteme**
 - 2. GSM
 - 3. UMTS
- III. **Drahtlose lokale Netze**
 - 4. IEEE 802.11 / WiFi
 - 5. Mobile Ad Hoc Netze
- IV. **Drahtlose innerstädtische Netze**
 - 6. IEEE 802.11s
 - 7. IEEE 802.16 / WiMax
- V. **Drahtlose persönliche Netze**
 - 8. Bluetooth
 - 9. IEEE 802.15.4 / ZigBee
- VI. **Positionsbestimmung**
 - 10. Positionsbestimmung
- VII. **Mobiles Internet**
 - 11. Mobile Vermittlungsschicht
 - 12. Mobile Transportschicht

- 11.1 Motivation
- 11.2 DHCP
- 11.3 Mobile IPv4
- 11.4 Mobile IPv6
- 11.5 Mikromobilität
- 11.6 Nahtlose Handovers

- Neuartige Kommunikationsanwendungen mit Interaktivität und Echtzeit-Anforderungen
 - Internet-Telefonie (Voice over IP)
 - Video-Konferenzen
 - Audio- und Video-Streaming
 - etc.
- Nutzer wünschen sich ubiquitären Internetzugang  [VI.5]
 - 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 Services
 - ▶ Ermöglicht Integration anderer Technologien, bspw. WLAN (so genannte "4G-Netze")

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

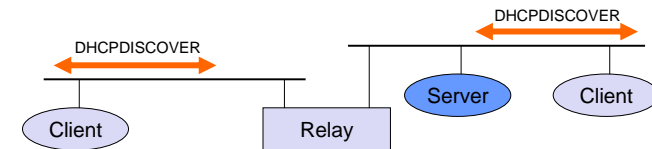
- **Host-spezifische Routen** zur mobilen Station
 - Anpassen der Routing-Einträge aller Router auf dem Kommunikationspfad
→ Skaliert nicht Internet-weit!
- **Separate IP-Adressen für Wegewahl u. Identifikation**
 - Je nach Lokation andere IP-Adresse für Wegewahl
 - Konstante IP-Adresse für Transportprotokolle 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 (nächste Folie) Mobile Stationen erhalten bei Subnetz-Wechsel neue IP-Adresse über DHCP	Häufige Subnetz-Wechsel Aktive Komm.verbindungen sollen erhalten werden Lösung durch Mobile IP (Kap 11.3 ff.)

5

- **Anwendung**
 - Automatische Konfiguration vernetzter Stationen
 - Zuweisung einer IP-Adresse für begrenzte Zeitspanne
 - Zusätzliche Konfigurationsparameter, bspw.
 - ▶ IP-Adresse(n) von DNS-Server(n), Name-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. DHCP OFFER, enthalten IP-Adressen und andere Konfigurationsparameter in separaten Optionen)

[Vl.7]
[Vl.8]



6

- Ziel: Mobile Stationen können bei Wechsel des Subnetzes aktive Kommunikationsverbindungen fortführen
 - IP-Adresse ändert sich nur für Zustellung von Dateneinheiten
 - Transparenz gegenüber Transportprotokollen und Anwendungen
- Anforderungen
 - Kompatibilität
 - ▶ Keine Änderung an Schicht-2-Protokollen, Routern oder Festnetzstationen
 - ▶ Kommunikation zwischen mobilen Stationen und Festnetz-Stationen
 - Sicherheit
 - ▶ Authentifizierung von Registrierungsrichten
 - ▶ 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



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

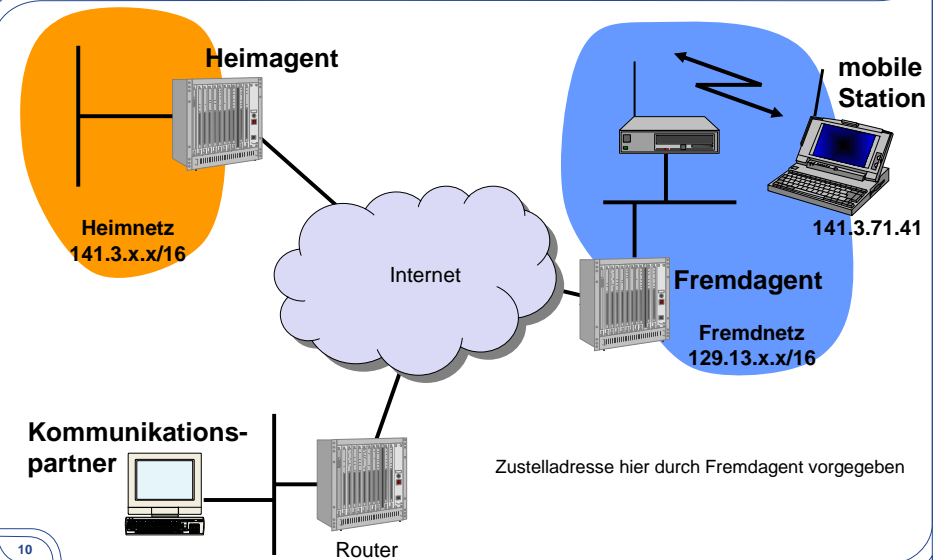


• Heimagent

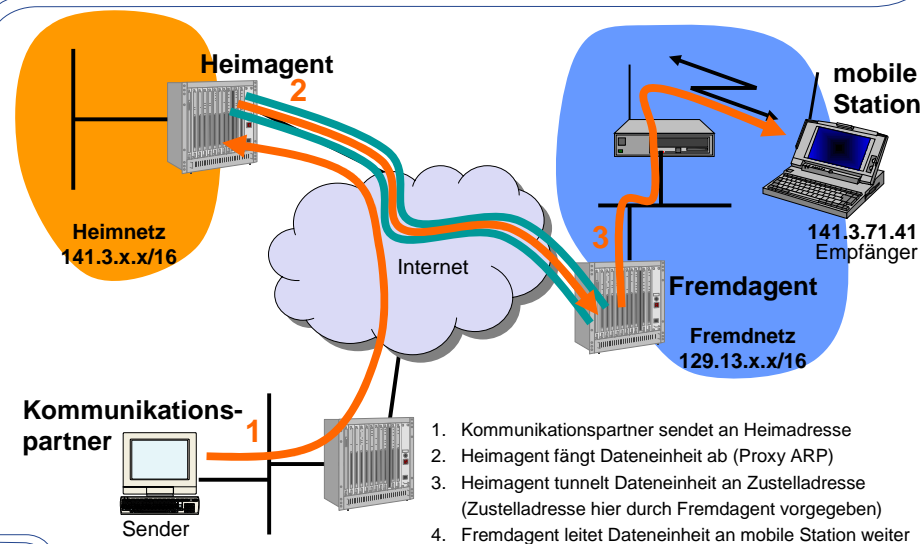
- Einheit im Heimnetz, typischerweise Router
- Stellvertreter der mobilen Station im Heimnetz
- Kennt aktuelles Fremdnetz (Aufenthaltort) der mobilen Station
- Endpunkt eines **Tunnels** zum Fremdnetz
 - ▶ Tunnelt vom Kommunikationspartner empfangene Dateneinheiten zum Fremdnetz
 - ▶ Leitet aus dem Fremdnetz getunnelte Dateneinheiten zum Kommunikationspartner weiter

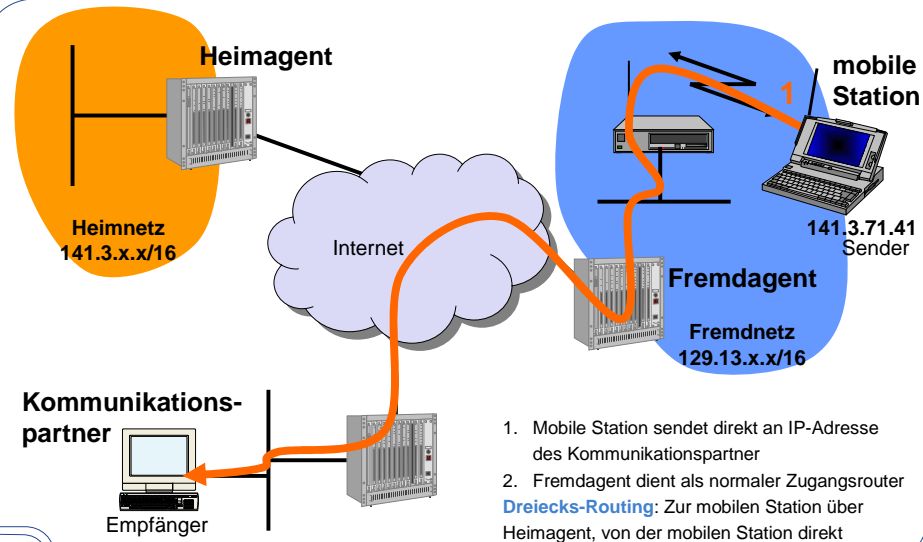
• Fremdagent

- Einheit im Fremdnetz, typischerweise Zugangsrouter
- Endpunkt des Tunnels zum Heimagenten
 - ▶ Tunnelt von mobiler Station empfangene Dateneinheiten zum Heimagenten
 - ▶ Leitet vom Heimagenten getunnelte Dateneinheiten zur mobilen Station weiter
- Kann Zustelladresse vorgeben



- **Zustelladresse des Fremdagenten**
 - Zustelladresse gehört dem Fremdagenten
 - Mobile Station registriert sich über Fremdagent beim Heimagenten
 - Fremdagent ist Endpunkt des Tunnels zum Heimagenten
 - 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 Heimagenten
 - Mobile Station ist Endpunkt des Tunnels zum Heimagenten
 - Vorteil: Kein Fremdagent erforderlich





13

• Quelladress-Filter

- Viele Router und Firewalls werfen Dateneinheiten mit topologisch inkorrekten Quelladressen
- Quelladresse der mobilen Station muss Heimadresse sein
- Daher nicht topologisch korrekt

• Multicast

- Möglicherweise keine Unterstützung für Multicast im Fremdnetz
- Teilnahme an Multicast-Gruppen im Heimnetz über Tunnel zwischen mobiler Station und Heimagent
- Quelladresse der mobilen Station beim Tunneln gemäß Mobile-IPv4-Standard gleich Heimadresse, daher topologisch inkorrekt

• 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

14

- Von mobiler Station gesendete Dateneinheiten werden
 - durch den Fremdagenten gekapselt
 - über Heimagent getunnelt
- Lösung der Probleme von Dreiecks-Routing
 - Dateneinheiten topologisch korrekt
 - Lösung der Multicast-Problematik
 - Lösung der TTL-Problematik (Tunnel hat Länge 1)
- Nachteile
 - Geringere Effizienz durch 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 Heimagent umleiten (Tunnel Hijacking)
 - ▶ Zusätzliche Authentifizierung löst dieses Problem
 - ▶ Zwischen mobiler Station und Fremdagent
 - ▶ Zwischen Fremdagent und Heimagent

15

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

16

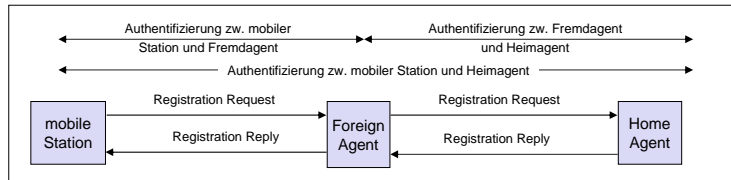
- Mobile Station erhält Zustelladresse (von Fremdagent oder über DHCP)
- Danach: Registrierung beim Heimagent
 - Heimagent erfährt damit aktuellen Aufenthaltsort der mobilen Station
- Registrierung besitzt stets begrenzte Lebensdauer
 - Danach automatisch gelöscht (Soft State)
 - Registrierung muss periodisch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

Aufbau des Nutzdatenteils einer Registrierungsanforderung:

0	7	8	15	16	23	24	31				
Typ		S	B	D	M	G	r	T	r	Lebensdauer	
Heimatadresse											
Heimagent											
Zustelladresse											
Identifikation											
Erweiterungen . . .											


- Sicherheitsprobleme
 - Authentizität nicht gewährleistet (unberechtigte Registrierungen)
 - ▶ Angreifer kann sich gegenüber Heim- und Fremdagent als mobile Station ausgeben
 - ▶ Angreifer kann sich gegenüber mobiler Station als Heim- oder Fremdagent ausgeben
 - Angreifer kann Dateneinheiten seines Opfers an falsche Zustelladresse umlenken
 - Wiedereinspiel-Angriffe (Replay-Attacken)
- Lösung
 - **Authentifizierung** der Registrierungsanrichten
 - Schutz vor Wiedereinspiel-Angriffen
- Verschlüsselung nicht enthalten; erfordert zusätzliche Mechanismen
- Sicherheitsbeziehungen
 - Zwischen mobiler Station, Heimagent und evtl. auch Fremdagent
 - Sicherheitsbeziehung (für ein bestimmtes Knotenpaar) enthält
 - ▶ Authentifizierungsalgorithmus (Voreinstellung: HMAC-MD5)
 - ▶ Schlüssel (symmetrisch oder asymmetrisch)
 - ▶ Methode zur Verhinderung von Wiedereinspiel-Angriffen
 - Aushandlung der Sicherheitsbeziehung und Schlüsselaustausch durch externen Mechanismus


- Authentifizierung der Registrierung
 - Vorgeschrieben zwischen mobiler Station und Heimagent
 - Optional zwischen [mobiler Station \leftrightarrow Fremdagent \leftrightarrow Heimagent]
 - Authentifizierungserweiterung für Registrierungsnachrichten



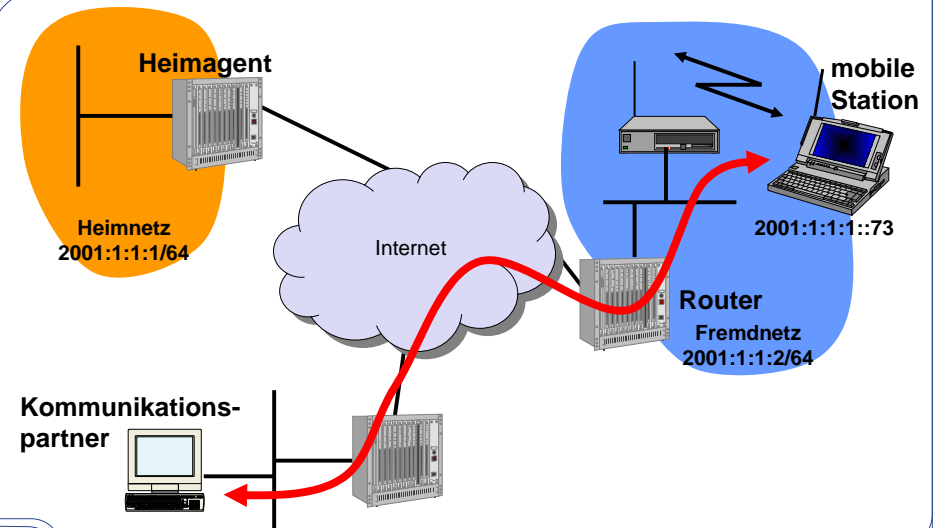
- Verhindern von Wiedereinspiel-Angriffen
 - Identifikationsfeld ist für jede Nachricht verschieden
 - 2 Verfahren: **Zeitstempel** (erfordert synchronisierte Uhren), **Einmalwerte** („Nonces“), optional
 - Identifikationsfeld geht in Authentifizierungsdaten ein
- Probleme
 - Authentifikation mit Fremdagent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

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

- Mobilitätsunterstützung für IPv6  [VI.11]
 - 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 Heimgenten
 - 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

- Bidirektionales Tunneln (wie bei Mobile IPv4)  [VI.11]
 - 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 Heimgent, kein Dreiecks-Routing
 - Dateneinheiten im Netz
 - ▶ IPv6-Köpfe enthalten Zustelladresse (als Quelle oder Ziel)
 - ▶ Erweiterungen der IPv6-Köpfe enthalten Heimadresse
 - Nachteil: Erfordert Mobilitätsunterstützung vom Kommunikationspartner
- Weitere Eigenschaften
 - Authentifizierung und Sicherheit von vornherein integriert
 - IPsec für bidirektionales Tunneln
 - **Return-Routability-Prozedur** für Routenoptimierung
 - Falls Adresse des Heimgenten unbekannt ist, kann diese erkundet werden (Dynamic Home Agent Discovery)
 - Heimatadresse der mobilen Station kann dynamisch angepasst werden, wenn z.B. Heimnetz neues Präfix erhält (Mobile Prefix Discovery)

- **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



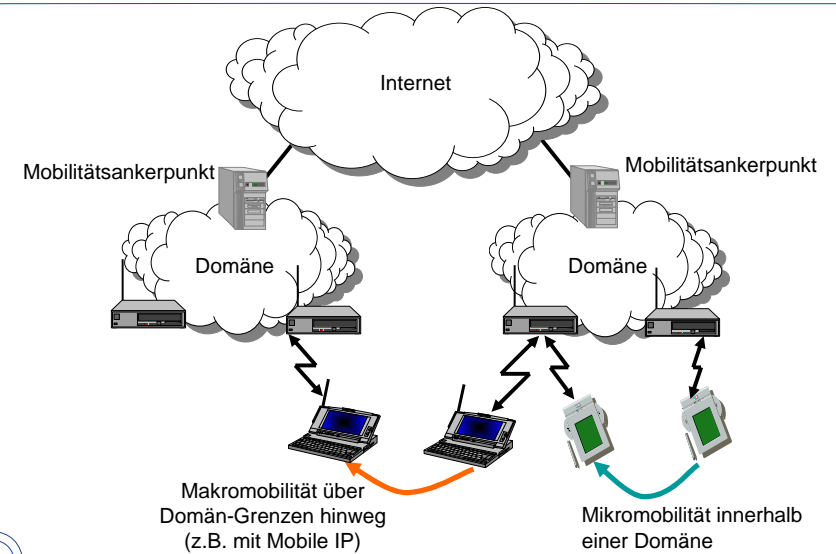
- **Idee:** Direkter Austausch zwischen mobiler Station und Kommunikationspartner
 - Initiiert von mobiler Station, wenn über den Heimagenten getunnelte Dateneinheit empfangen wird
 - Erfordert Mobilitätsunterstützung beim Kommunikationspartner
 - Tunnel zwischen mobiler Station und Kommunikationspartner 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
- **Datentransfer**
 - Transportprotokolle und Anwendungen senden an/von Heimadresse
 - Sender ersetzt Heimadresse durch Zustelladresse bei Verarbeitung der Dateneinheit auf Netzwerk-Schicht
 - Heimadresse 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 Heimadresse und Zustelladresse vor Auslieferung an Transportprotokolle und Anwendungen

25

- **Effizienz**
 - Geringere Zustelllatenzen für Dateneinheiten als bei bidirektionalem Tunneln
 - Datentransfer funktioniert auch bei Ausfall des Heimagenten
 - Heimagent 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

26

- Registrierung beim Heimagenten
 - Ermöglicht bidirektionales Tunneln
 - Ist auch für Routenoptimierung erforderlich
 - Protokollablauf
 - ▶ Mobile Station schickt Binding-Update-Nachricht mit Heim- und Zustelladresse zum Heimagent
 - ▶ Heimagent bestätigt mit Binding-Acknowledgement-Nachricht
 - IPsec für Integrität und Authentizität der Nachrichten
- Registrierung beim Kommunikationspartner
 - Erfordert vorherige Registrierung mit Heimagent
 - 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 dem entsprechenden Pfad sein, um ein „Keygen Token“ abzuhören



• 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 Heimagent und Kommunikationspartnern registriert werden
- Mobilität innerhalb der Domäne **transparent** nach außen
 - ▶ Keine erneute Registrierung bei Heimagent und Kommunikationspartnern
- Ansätze aus der IETF
 - ▶ Regionale Registrierungen in Mobile IPv4
 - ▶ Hierarchisches Mobile IPv6
 - ▶ Cellular IP
 - ▶ Handoff-Aware Wireless Access Internet Infrastructure (Hawaii)

• Zwei (oder mehr) Level von Fremdagenten

- Mobilitätsankerpunkt
- Regionale Fremdagenten (optional)
- Fremdagenten

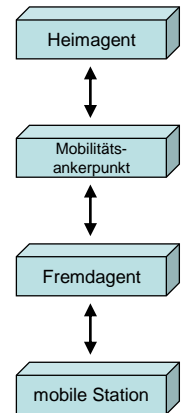
• Mobilitätsankerpunkt liefert Zustelladresse, die für Heimagent und Kommunikationspartner sichtbar ist

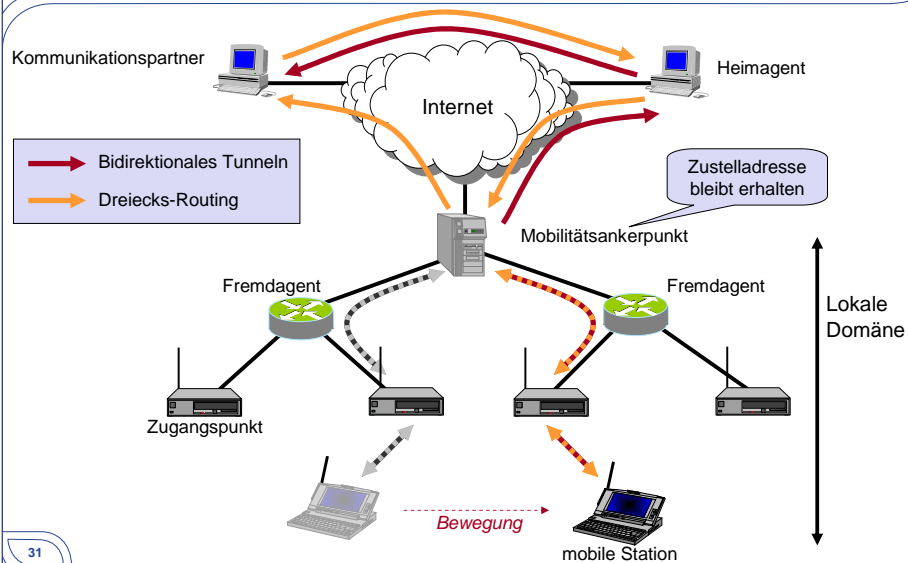
- Tunnel zwischen mobiler Station und Mobilitätsankerpunkt

• Mobile Station behält Zustelladresse bei Wechsel des Fremdnetzes

• Regionale Registrierung bei Subnetz-Wechsel

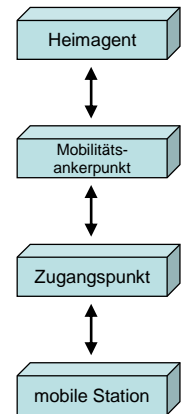
• Reguläres Mobile IP (Makromobilität) bei Wechsel des Mobilitätsankerpunkts





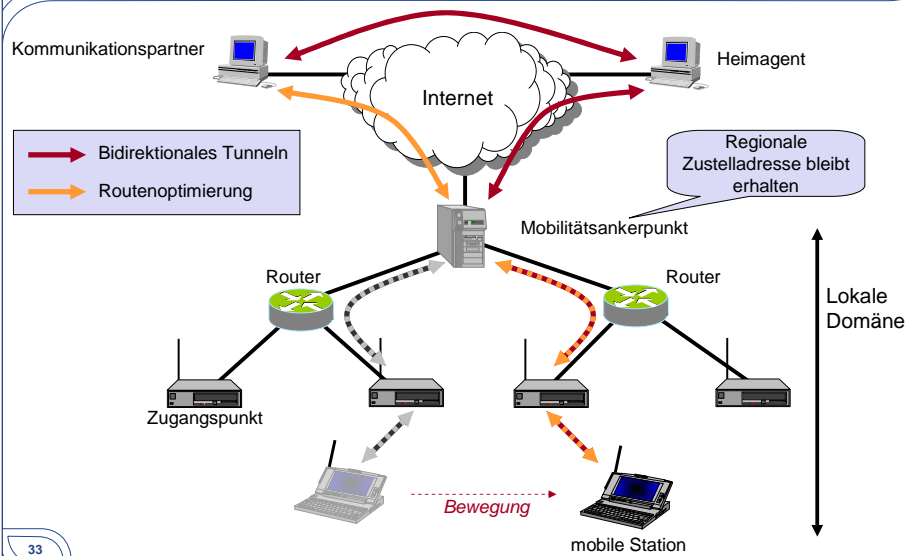
31

- Zwei Levels von Heimagenten
 - Regulärer Heimagent
 - Mobilitätsankerpunkt
- Mobilitätsankerpunkt liefert **regionale Zustelladresse**
 - Regionale Zustelladresse für Heimagent 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



[VI.18]

32



Mobilkommunikation VI. Mobiles Internet



Kapitel 11 Mobile Transportschicht und mobile Dienste



- I. **Einleitung**
 - 1. Einführung und Grundlagen
- II. **Drahtlose Telekommunikationssysteme**
 - 2. GSM
 - 3. UMTS
- III. **Drahtlose lokale Netze**
 - 4. IEEE 802.11 / WiFi
 - 5. Mobile Ad Hoc Netze
- IV. **Drahtlose innerstädtische Netze**
 - 6. IEEE 802.11s
 - 7. IEEE 802.16 / WiMax
- V. **Drahtlose persönliche Netze**
 - 8. Bluetooth
 - 9. IEEE 802.15.4 / ZigBee
- VI. **Positionsbestimmung**
 - 10. Positionsbestimmung
- VII. **Mobiles Internet**
 - 11. Mobile Vermittlungsschicht
 - 12. Mobile Transportschicht

- 12.1 Mobiles TCP
- 12.2 Service Location Protocol

- In Festnetzen entstehen Datenverluste i.A. durch Überlast
 - Router verwerfen Dateneinheiten, sobald Puffer voll sind
 - Übertragungswiederholungen würden Stausituation verschlimmern
- TCP wurde für **Festnetze** entwickelt
 - Slow Start zum Messen verfügbarer Ende-zu-Ende-Bandbreite
 - Bei Datenverlust wird Stau angenommen: TCP reduziert Datenrate
 - ▶ Fast Retransmit/Fast Recovery bei 4 gleichen Bestätigungen
 - ▶ Staufenster wird auf Hälfte der ausstehenden Daten gesetzt
 - ▶ Anschließend Congestion Avoidance
 - ▶ Slow Start bei Timeout
 - ▶ Staufenster wird auf 1 gesetzt
 - ▶ Verfügbare Ende-zu-Ende-Bandbreite wird neu bestimmt



Vorlesung "Telematik"
behandelt TCP im Detail



- Stauannahme von TCP im Festnetz i.A. richtig
- Allerdings falsch in drahtlosen mobilen Netzen
 - Drahtlose Netze: Datenverluste meist durch Übertragungsfehler
 - Mobilität: Dateneinheiten zu alter Zustelladresse unterwegs
 - ▶ Subnetz-Wechsel impliziert Timeout \Rightarrow Slow Start
 - ▶ Sinnvoll, da Ende-zu-Ende-Bandbreite auf neuem Pfad zunächst unbekannt
- Konsequenz für TCP bei Mobilität
 - Übertragungsfehler reduzieren Datenrate/Durchsatz unnötig
 - Slow Start nach jedem Subnetz-Wechsel ist zeitaufwändig
 - ▶ Insbes. für Pfade mit hohen Bandbreiten und hoher Latenz (z.B. Satellitenlinks)
 - ▶ Macht sich bei hoher Mobilität stark bemerkbar
- TCP kann aber nicht „grundsätzlich“ verändert werden
 - Interoperabilität mit Festnetzrechnern notwendig
 - Stau- und Flusskontrolle halten im Festnetz das Internet zusammen

- Ziel
 - Stau- und Flusskontrolle von TCP im Wesentlichen beibehalten
 - Zusätzliche Mechanismen
 - ▶ bei Übertragungsfehlern in drahtlosen Netzen
 - ▶ nach Subnetz-Wechsel bei Mobilität
- Lösungsansätze
 - Erzwungener Fast Retransmit
 - Indirektes TCP
 - Snooping TCP
 - Quick Start für TCP

• Problem

- Dateneinheiten werden nach Subnetz-Wechsel zunächst an falsche Zustelladresse gesendet
 - ▶ Dateneinheiten gehen verloren
 - ▶ Sender erhält keine Bestätigungen
 - ▷ Timeout und Slow Start
- Wiederholung der Dateneinheiten erst nach Timeout
 - ▶ Selbst bei zwischenzeitlicher Mobile-IP-Registrierung
 - ▶ Timeout kann lang sein, insbes. wegen Backoff bei "Mehrfach-Timeouts"



[VI.23]

• Lösungsmöglichkeit

- Erzwingen von **Fast Retransmit** durch mobile Station
 - ▶ Mobile Station sendet nach Subnetz-Wechsel 4 gleiche Bestätigungen
 - ▶ Kommunikationspartner führt Fast Retransmit durch
- Anschließend **Slow Start** anstatt Fast Recovery
 - ▶ Bandbreite auf neuem Datenpfad muss neu bestimmt werden
 - ▶ Slow Start automatisch, falls Timeout vor Eingang der Bestätigungen auftrat
 - ▶ Ansonsten muss Slow Start "erzwungen" werden

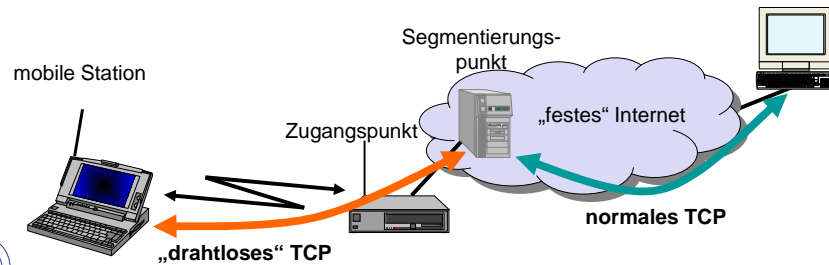
39

• Nachteile

- Wiederholte Dateneinheiten legen gesamten Weg durch das Netz zurück
 - ▶ Komplette Umlaufzeit für die 4 gleichen Bestätigungen und erste wiederholte Dateneinheit nötig
- Ermittlung der neuen Datenrate über Slow Start langwierig
- Berücksichtigt nur Datenverluste bei Subnetz-Wechsel
 - ▶ Durch Übertragungsfehler verursachte Verluste können aber durch reguläres Fast Retransmit/Fast Recovery behoben werden
- Erzwingen des Slow Starts erfordert Modifikation von TCP am Kommunikationspartner

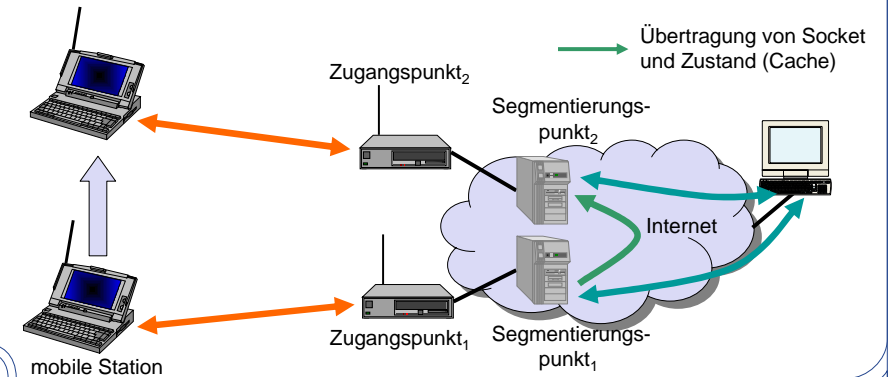
40

- Aufteilen der TCP-Verbindung in zwei Segmente
 - ▶ Aufteilung findet in der Nähe des Übergangs vom Festnetz ins drahtlose Netz statt
 - ▶ Zum Beispiel beim Fremdagenten bzw. Zugangsrouter
 - Keine Änderung am TCP-Protokoll für Festnetz-Stationen
 - ▶ Installierte Basis ist zu hoch
 - Optimiertes Transportprotokoll zwischen Segmentierungspunkt und mobilem Endgerät („drahtloses“ TCP)
 - ▶ Zum Beispiel Indirect TCP
 - Festnetz-Stationen bemerken Subnetz-Wechsel der mobilen Station nicht



41

- Optimierung der Mobilstrecke
 - Zwischenspeicherung von Dateneinheiten im Segmentierungspunkt
 - Schnelle Übertragungswiederholung, da Strecke zwischen Segmentierungspunkt und mobiler Station kurz
 - Übertragung des TCP-Zustands bei Subnetz-Wechsel zum neuen Segmentierungspunkt



42

• Vorteile

- Keine Änderungen im Festnetzbereich
 - ▶ Existierende Mechanismen hier weiterhin effektiv
- Fehler auf der drahtlosen Strecke pflanzen sich nicht ins Festnetz fort
- Relativ einfach administrierbar, da nur die kurze Strecke (wenige Hops) zwischen Segmentierungspunkt und mobiler Station

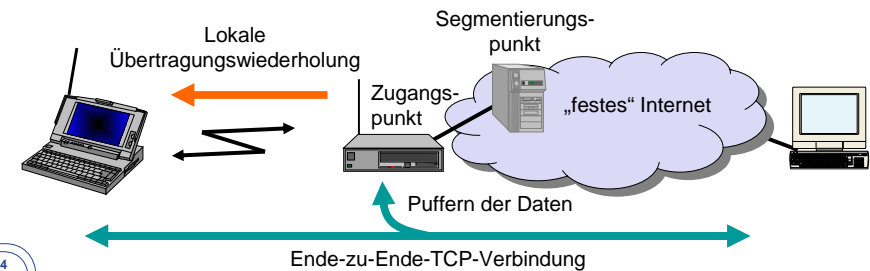
• Nachteile

- Verlust der Ende-zu-Ende-Semantik
 - ▶ Bestätigung an Sender heißt nun nicht mehr, dass Empfänger wirklich die Daten erhalten hat
 - ▶ Was passiert bei einem Absturz/Fehlfunktion des Segmentierungspunkts?
 - ▶ Konsistenz der Sichten?
- Vergrößerte Latenzzeiten durch Pufferung der Daten im Segmentierungspunkt und evtl. Übertragung an neuen Segmentierungspunkt
- Übertragung von Socket und Zustand (Cache) bei Wechsel des Zugangspunktes notwendig
 - ▶ Kurzzeitige Unterbrechung der Datenübertragung über Transportverbindung


43


• „Transparente“ Erweiterung von TCP im Segmentierungspunkt

- Puffern der zur mobilen Station gesendeten Daten
- Bei Datenverlust auf der Strecke zwischen Segmentierungspunkt und mobiler Station (beide Richtungen) direkte Übertragungswiederholung durch Segmentierungspunkt („lokale“ Übertragungswiederholung)
- Dazu hört der Segmentierungspunkt den Datenverkehr ab und erkennt Bestätigungen in beide Richtungen (Filtern der Bestätigungen)
- TCP bleibt in beiden Endsystemen unverändert



44

- Datentransfer zur mobilen Station  [VI.13]
[VI.14]
 - Segmentierungspunkt puffert Daten bis zur Bestätigung
 - Erkennt Datenverluste durch duplizierte Bestätigungen oder Timeouts
 - Schnelle Übertragungswiederholung; transparent gegenüber Festnetz
- Datentransfer von mobiler Station
 - Segmentierungspunkt erkennt Datenverluste auf dem Weg von mobiler Station anhand der Sequenznummern, sendet daraufhin negative Bestätigung zur mobilen Station
 - Mobile Station kann nun sehr schnell erneut übertragen
- Probleme
 - Snooping TCP isoliert die drahtlose Verbindung nicht komplett
 - ▶ Selbst bei einer lokalen Übertragungswiederholung kann beim Kommunikationspartner ein Timeout auftreten
 - Je nach Verschlüsselungsverfahren ist Snooping nutzlos
 - ▶ IPsec verschlüsselt bspw. den Inhalt von IP-Datagrammen und somit auch den TCP-Header. Segmentierungspunkt hat also keinen Zugriff darauf.

- Problem: Timeout und Slow Start nach jedem Subnetz-Wechsel ist  [VI.20]
zeitaufwändig
 - Kann bei hoher Mobilität und Datenpfaden mit großen Bandbreiten und langen Verzögerungszeiten Großteil der Kommunikationszeit ausmachen
- Quick Start für TCP hilft, verfügbare Bandbreite *schnell* zu bestimmen
 - Station fragt Router auf Datenpfad nach verfügbarer Bandbreite
 - ▶ IP-Option in TCP-Dateneinheit enthält gewünschte Bandbreite in Bit/s
 - ▶ Zweite IP-Option enthält „Quick Start TTL“
 - Router können Bandbreite in IP-Option reduzieren
 - ▶ Quick-Start-fähige Router dekrementieren Quick Start TTL
 - Kommunikationspartner sendet Ergebnis zurück
 - ▶ TCP-Option in erster TCP-Dateneinheit
 - Quick Start TTL zeigt, ob alle Router Quick-Start-fähig sind
 - ▶ Nur dann kann Quick Start angewendet werden
 - Station passt Staufenster an verfügbare Bandbreite an
 - ▶ Verfügbare Bandbreite * Einschätzung der Umlaufzeit = neues Staufenster
 - ▶ Schneller als Bandbreitenermittlung über Slow Start
 - Kommunikationspartner führt umgekehrt gleiche Prozedur durch
 - **Einsatz von Quick Start bei Mobilität zurzeit jedoch noch nicht standardisiert**

- Vorteile
 - Kein zeitaufwändiger Timeout und Slow Start
 - Trotzdem Ausnutzung verfügbarer Bandbreite
 - Quick Start auch für andere Transportprotokolle außer TCP geeignet
- Nachteile
 - Beide TCP-Partner müssen Quick-Start-fähig sein
 - Alle Router auf dem Pfad müssen Quick-Start-fähig sein
 - An ubiquitären Einsatz wird zurzeit nicht gedacht, insbes. nicht in Core-Routern
- Probleme bei Mobilität
 - Nach Subnetz-Wechsel sendet mobile Station i.A. zunächst keine TCP-Dateneinheit
 - ▶ Quick-Start-Option muss aber an TCP-Dateneinheit angehängt werden
 - 1 Roundtrip-Zeit erforderlich zum Ermitteln der verfügbaren Bandbreite
 - Mobile Station muss Umlaufzeit auf neuem Pfad kennen, um Staufenster anzupassen
 - ▶ Umlaufzeit ändert sich bei Subnetz-Wechsel möglicherweise stark
 - ▶ Lösungsansatz: Verwende für Bandbreitenbestimmung benötigte Umlaufzeit
 - ▶ Nachteil: Umlaufzeit kann schwanken; ermittelter Wert evt. sehr ungenau
 - Noch Forschungsbedarf

Verfahren	Mechanismus	Vorteile	Nachteile
Fast Retransmit/ Fast Recovery	Schnelles Erzwingen einer Übertragungswiederholung nach Verbindungswechsel	Einfach, effizient	Vermischung der Schichten, nicht transparent
Indirektes TCP	Auftrennen in zwei TCP-Verbindungen	Isolation der drahtlosen Strecke, einfach	Verlust der TCP-Semantik, erhöhte Latenz
Snooping TCP	Mithören von Daten und Quittungen, lokale Wiederholung	Transparent für Ende-zu-Ende	Problematisch bei Verschlüsselung, schlechtere Isolation
Quick Start für TCP	Explizite Auskunft über verfügbare Bandbreite von Routern	Bandbreiten-Bestimmung ohne Slow Start	Beide TCP-Partner und alle Router auf dem Datenpfad müssen Optimierung unterstützen

- Mobile Stationen greifen auf diverse Netzdienste zu
 - Drucker
 - Faxgeräte
 - DNS-Server
 - Web-Server
 - Proxy-Server
 - Timeserver
 - Dateisysteme
 - Datenbanken
- Station muss Namen des Hosts kennen, der Netzdienst anbietet
 - Vorkonfiguration für Heimnetz denkbar
 - Vorkonfiguration für Fremdnetze aufwändig oder unmöglich
- Ziel
 - Mobile Stationen sollen ohne Kenntnis von Hostnamen auch nach Subnetz-Wechsel auf benötigte Netzdienste zugreifen können
 - ▶ Interessant insbes. bei Wechsel der administrativen Domäne
 - ▶ Zuvor genutzte Netzdienste dann ggf. nicht mehr verfügbar
 - Automatische Ermittlung benötigter (und verfügbarer) Netzdienste



[VI.21]

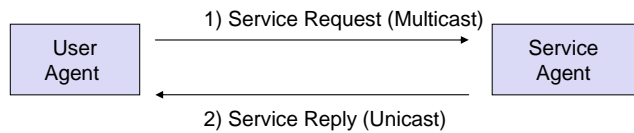
49



- Lösung bietet Service Location Protocol (SLP)
 - Ermittelt Existenz, Lokation und Konfiguration von Netzdiensten
 - Mobile Station kann nach Subnetz-Wechsel nach benötigten Netzdiensten suchen
- Terminologie
 - **User Agents** suchen und nutzen Netzdienste
 - **Service Agents** bieten Dienste an
 - **Directory Agents** speichern Beschreibungen verfügbarer Dienste
- Zwei Modi in SLP
 - Direkte Interaktion zwischen User Agents und Service Agents
 - Dienstlokalisierung über Directory Agent

50

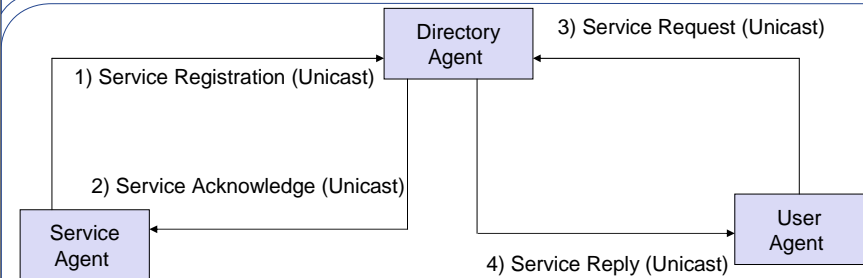




• Kein Directory Agent vorhanden

- User Agent sendet Service-Request-Nachricht per Multicast
 - ▶ z.B. Anfrage für Druckdienst
 - ▶ Multicast Adresse: 239.255.255.253
- Anfrage kann benötigte Dienstcharakteristika enthalten
 - ▶ z.B. Postscript-Fähigkeit
- Service Agents antworten, wenn sie einen entsprechenden Dienst anbieten

51



- Service Agents registrieren ihre Dienste beim Directory Agent
 - Attribute und Schlüsselwörter beschreiben Dienste des Service Agents
 - Directory Agent schickt Service-Acknowledge-Nachricht nach erfolgreicher Registrierung
- User Agent sendet Service-Request-Nachricht an Directory Agent
 - Anfrage kann benötigte Dienstcharakteristika enthalten, z.B. Postscript-Fähigkeit
- Directory Agent sucht in seiner Datenbank entsprechenden Dienst und antwortet

52

- Aktive Suche nach Directory Agent
 - User Agent oder Service Agent sendet Service-Request-Nachricht per Multicast
 - ▶ service-type = "directory-agent"
- Passive Suche nach Directory Agent
 - Directory Agent sendet periodisch Directory Agent Advertisement
 - ▶ Multicast oder Broadcast
- Andere Möglichkeiten
 - DHCP
 - ▶ SLP Directory Agent Option (Code 78)
 - Manuelle Konfiguration



- Service URL
 - Ermittlung der Lokation eines Dienstes
 - In einer Form wie „service:“<srvtype>“:“<addrspec>
 - ▶ <srvtype>: Typ des Dienstes
 - ▶ <addrspec>: Adresse des Dienstes
- Beispiele
 - Webseite des Instituts –
service:http://www.tm.uka.de
 - Netzdrucker –
service:lpr://lprserver.tm.uka.de/lj4100

•URL-Eintrag

0	7	8	15	16	23	24	31
Reserved		Lifetime		URL Länge			
URL Länge		URL (unterschiedliche Länge)					
# der Auth.		Auth. Block					

- Verwendet in Service-Reply- und Service-Registration-Nachrichten
- Angabe der Information über Service URL
 - Länge der Service URL
 - Gültige Zeit
 - Authentifizierungsinformation

55

• Registrierung eines Druckdienstes im Directory Agent

```
URL = service:lpr://lprserver.tm.uka.de/lj4100
scope-list = Development
Lang. Tag = de
Attributes = (Name=LaserJet 4100),(Description=For
              developers only),
              (Protocol=LPR),(location-description=3rd floor),
              (Operator=Frank Winter \3cwinter@tm.uka.de\3e),
              (media-size=na-letter),(resolution=res-600),x=OK
```

- URL: service URL
- scope-list: Druckdienste nur für Abteilung Development
- Lang. Tag: Beschreibungen auf Deutsch
- Attributes: einzelnen Paare vom (Attributname, Attributwert)

56

- **Authentifikation**
 - Authentisierung von Service URLs und Dienstattributen
 - Autorisierung der Service Agents
 - Gewährleistung durch digitale Signaturen
- **Mobilitätsbezogenes Problem**
 - Schlüsselaustausch im Fremdnetz nötig
 - Verifikation von Zertifikaten
 - Hoher Verwaltungsaufwand für PKI
- **Verschlüsselung**
 - Nicht unterstützt in SLP
 - ▶ Ziel ist lediglich Bekanntgabe vorhandener Netzdienste
 - Alternative: IPsec Encapsulating Security Payload (ESP) zur Verschlüsselung der SLP-Nachrichten

- 6.1 Welche Probleme ergeben sich mit IP in Zusammenhang mit mobilen Stationen? Wie lassen sich diese lösen?
- 6.2 Welche Funktionalität stellt DHCP bereit? Welche Probleme lassen sich damit nicht lösen?
- 6.3 Skizzieren Sie die Funktionsweise von Mobile IP.
- 6.4 Was versteht man unter Dreiecks-Routing?
- 6.5 Wie lässt sich der Datenpfad bei Mobile IP optimieren?
- 6.6 Was geschieht bei einem Wechsel in ein anderes Fremdnetz? Wie lässt sich hier ein Datenverlust vermeiden?
- 6.7 Welche Probleme werden durch Reverse Tunneling gelöst? Welche nicht?
- 6.8 Wie unterscheiden sich Mobile IPv4 und Mobile IPv6?
- 6.9 Wie erkennt eine mobile Station den Wechsel in ein anderes Fremdnetz? Vergleichen Sie die Mechanismen bei IPv4 und IPv6.
- 6.10 Welche Sicherheitsprobleme treten beim Einsatz von Mobile IP auf? Was lässt sich dagegen tun?

- 6.11 Weshalb ist Mobile IP nicht für häufige Handover geeignet?
- 6.12 Erklären Sie den Unterschied zwischen Mikro- und Makromobilität.
- 6.13 Welche Ansätze gibt es zur Unterstützung von Mikromobilität?
- 6.14 Welche Vorteile besitzt Cellular IP bei häufigen Verbindungsübergaben im Gegensatz zu Mobile IP?
- 6.15 Erklären sie die Funktionsweise von dynamischen Host-spezifischen Routen.
- 6.16 Wie wird eine Verbindungsübergabe bei Cellular IP durchgeführt?
- 6.17 Worin liegen die Probleme beim Einsatz von TCP über drahtlose Verbindungen?
Durch welche Ansätze lassen sich diese Probleme lösen?
Welche Vor- und Nachteile bieten die angesprochenen Ansätze?
- 6.18 Skizzieren Sie weitere Möglichkeiten für mobile Transportprotokolle.
- 6.19 Welches Problem wird durch SLP gelöst? Beschreiben Sie die Funktionsweise.

- [VI.1] Jochen Schiller; Mobilkommunikation, Pearson Studium, 2. Auflage 2003
- [VI.2] James D. Solomon; Mobile IP: The Internet Unplugged, Prentice Hall, 1997
- [VI.3] Charles E. Perkins; Mobile IP: Design Principles and Practices, Addison-Wesley, 1997
- [VI.4] Andrew T. Campbell et. al.; Design, Implementation, and Evaluation of Cellular IP, IEEE Personal Communications, August 2000
- [VI.5] S. Keshav; Why Cell Phones Will Dominate the Future Internet, ACM Computer Communications Review, April 2005
- [VI.6] Andrew T. Campbell et al.; Comparison of IP Micromobility Protocols, IEEE Wireless Communications, Vol. 9 Nr. 1, Februar 2002
- [VI.7] R. Droms; Dynamic Host Configuration Protocol, RFC 2131, März 1997
- [VI.8] R. Droms et al.; Dynamic Host Configuration Protocol for IPv6, RFC 3315, Juli 2003
- [VI.9] C. Perkins; IP Mobility Support, RFC 3344, 2002
- [VI.10] C. Perkins; IP Encapsulation within IP, RFC 2003, 1996
- [VI.11] Hesham Soliman; Mobile IPv6, Addison-Wesley, 2004
- [VI.12] Hala Elaarag; Improving TCP Performance over Mobile Networks, ACM Computing Surveys, September 2002

- [VI.13] H. Balakrishnan, S. Seshan, R. H. Katz; Improving reliable transport and handoff performance in cellular wireless networks, Wireless Networks, J.C. Baltzer, Band 1, 1995
- [VI.14] E. A. Brewer et al.; A Network Architecture for Heterogeneous Mobile Computing, IEEE Personal Communications, 5(5), 1998
- [VI.15] J. Roth; Mobile Computing: Grundlagen, Technik, Konzepte, dpunkt, 2002
- [VI.16] A. Fieger, M. Zitterbart; Zuverlässige Transportdienste für Mobile Computing, Informatik – Forschung und Entwicklung, 16(4), 2001
- [VI.17] IETF MIP4 Working Group, <http://www.ietf.org/html.charters/mip4-charter.html>
- [VI.18] H. Soliman et al.: Hierarchical Mobile IPv6 Mobility Management, RFC 4140, August 2005
- [VI.19] Rajeev Koodli: Fast Handovers for Mobile IPv6, RFC 4068, Juli 2005
- [VI.20] IETF Transport Area Working Group, <http://www.ietf.org/html.charters/tswwg-charter.html>
- [VI.21] RFC 2608 - Service Location Protocol, Version 2
- [VI.22] RFC 2610 - DHCP Options for Service Location Protocol
- [VI.23] S. Schütz et al.: Protocol Enhancements for Intermittently Connected Hosts, ACM Computer Communication Review, Juli 2005