# Drahtlose Netzwerke
## Grundlagen und Einsatzfelder

## Mobile Vermittlungsschicht

# Adressvergabe

- **Problem: Mobilität der Stationen**
  - IP-Adressen sind ortsgebunden
- **Anforderungen:**
  - IP-Connectivity trotz Roaming
  - Keine Verbindungsunterbrechung
  - Minimaler Konfigurationsaufwand
- **Möglichkeiten**
  - Verzicht auf IP-Teilnetze
  - Dynamische Adressvergabe
  - Mobile IP

# Verzicht auf IP-Teilnetze

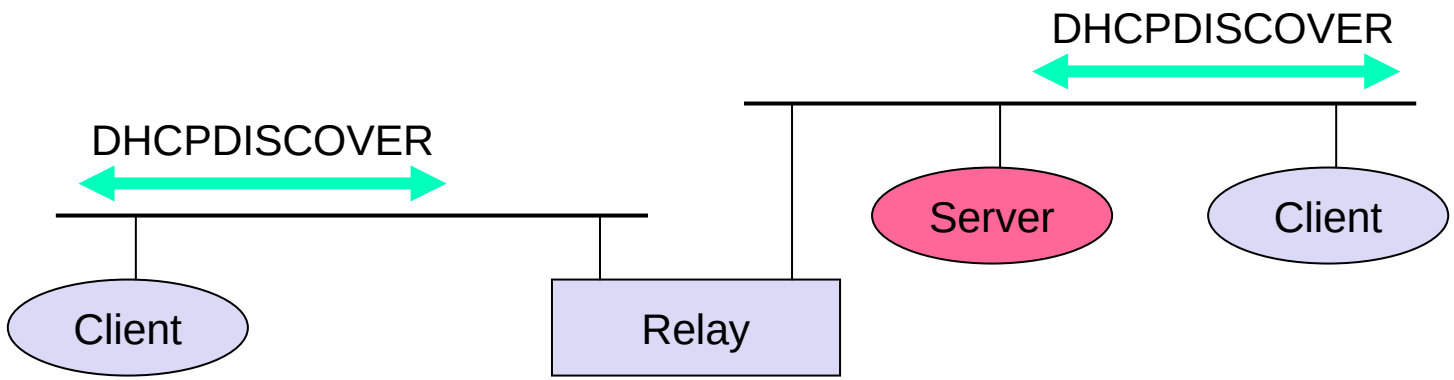
- **Alle APs zwischen denen Roaming stattfinden kann, gehören zu einem IP-Teilnetz**
- **Pros:**
  - Roaming ohne Probleme möglich
  - Keine Verbindungsunterbrechung
- **Cons:**
  - Schlechte Wartbarkeit
  - Hohe Last durch Broadcasts
- **Geeignet für:**
  - Weiträumige Netze mit wenigen Stationen

# Dynamische Adreßvergabe

- **Adresse werden in den verschiedenen IP-Teilnetzen dynamisch vergeben**
- **Pros:**
  - Skalierbar
  - Von allen Betriebssystemen unterstützt
- **Cons:**
  - Verbindungsunterbrechung beim Roaming
  - Variable Adresse (ungeeignet für Server)
- **Geeignet für:**
  - Netze mit Stationen, die den Ort nur zwischen den Sessions wechseln

# DHCP

- **Dynamic Host Configuration Protocol**
- **Anwendung**
  - vereinfacht Verwaltung großer Installationen
  - Liefert wichtige Daten
- **Client/Server-Modell**
  - Client erfragt via MAC-Broadcast seine Daten
  - evtl. DHCP-Relay



# DHCP Charakteristika

- **Server**
  - mehrere Server können konfiguriert werden
  - Koordination z. Zt. (noch) nicht standardisiert
  - ➔ manuelles Aufsetzen notwendig
- **Erneuerung der Konfiguration**
  - IP-Adressen regelmäßig neu angefordert
- **Optionale Angaben**
  - IP-Adresse
  - (Sub-)Netzmaske
  - Router
  - DNS (Domain Name System)-Server
  - DNS-Name
  - NTP (Network Time Protocol)-Timeserver
  - ...

# Mobile IP

- **Mobile Stationen behalten ihre IP-Adressen und IP-Nachrichten werden „umgeleitet“**
- **Pros:**
  - Keine Verbindungsunterbrechung
  - Keine Änderungen an den anderen Protokollen erforderlich
- **Cons:**
  - Erfordert Unterstützung durch die Netzinfrastruktur und das Betriebssystem
  - Overhead
  - Sicherheits-kritisch
- **Geeignet für:**
  - Stationen, die weiträumig mobil sind

# Mobile IP – Problemexposition

- **Wegwahl in IP-Netzen**
  - Netzwerk-Präfix definiert physikalisches Subnetz
  - Subnetz gewechselt ➔ IP-Adresse passend wechseln
- **Spezifische Routen zum Endgerät?**
  - anpassen aller Routing-Einträge
    - Umleitung entsprechender Pakete
  - Skaliert schlecht: Anzahl und Ort der mobilen Geräte
  - Sicherheitsprobleme
- **Wechseln der IP-Adresse?**
  - IP-Adresse je nach Lokation
  - DNS-Aktualisierung dauert lange
  - Abbruch von TCP!
  - Sicherheitsprobleme!

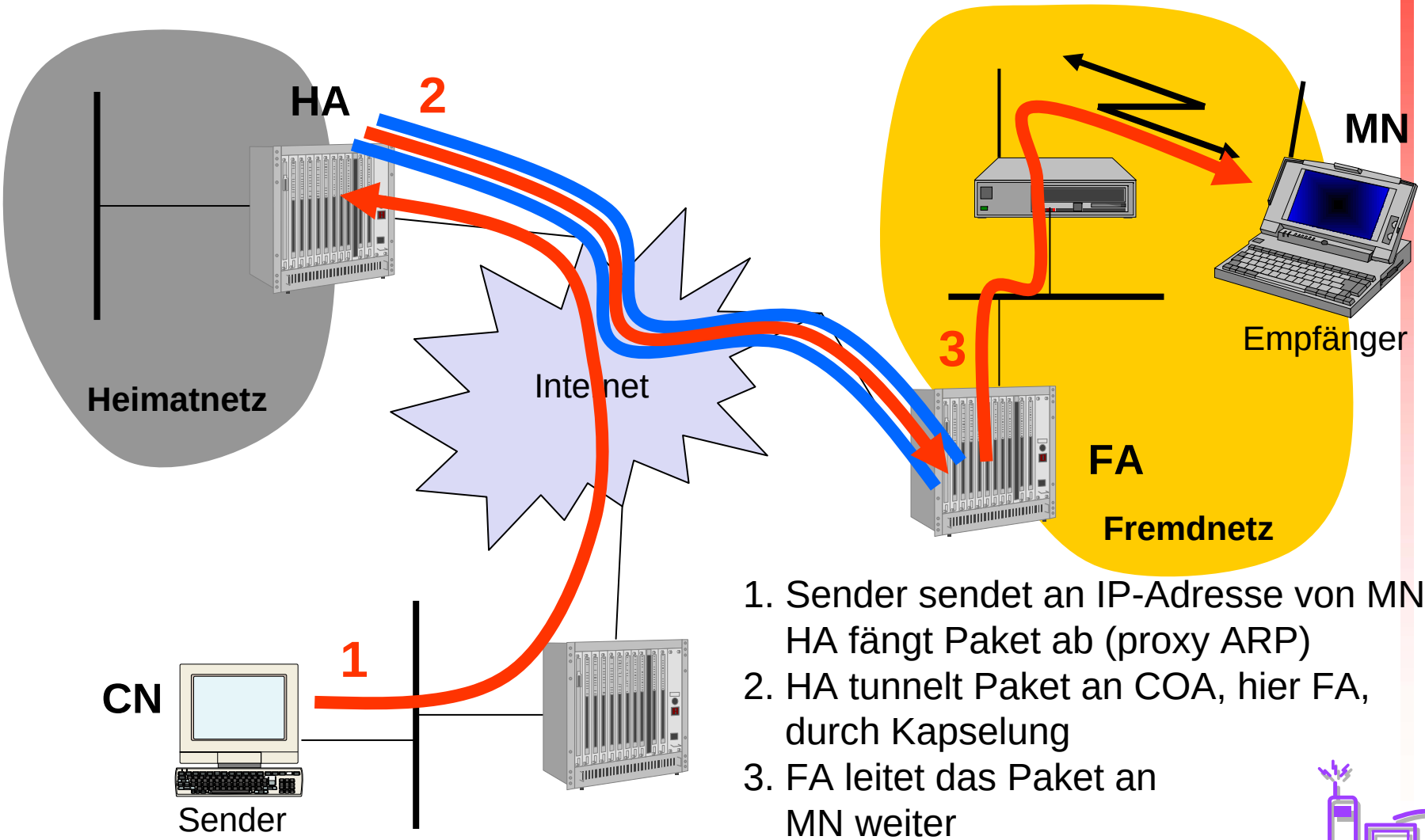
# Anforderungen an Mobile IP

- **Transparenz**
  - mobile Endgeräte behalten IP-Adresse
  - Wiederaufnahme der Kommunikation nach Abtrennung
  - Wechsel des Anschlusspunkt an das Netz möglich
- **Kompatibilität**
  - gleiche Schicht 2 und 4-Protokolle wie IP
  - keine Änderungen an bisherigen Rechnern und Router
  - mobile Endgeräte können mit festen kommunizieren
- **Sicherheit**
  - alle Registrierungsnachrichten authentifiziert
- **Effizienz und Skalierbarkeit**
  - wenige zusätzliche Daten zum mobilen Endgerät
    - evtl. über eine schmalbandige Funkstrecke angebunden
  - große Anzahl mobiler Endgeräte internet-weit unterstützt

# Terminologie

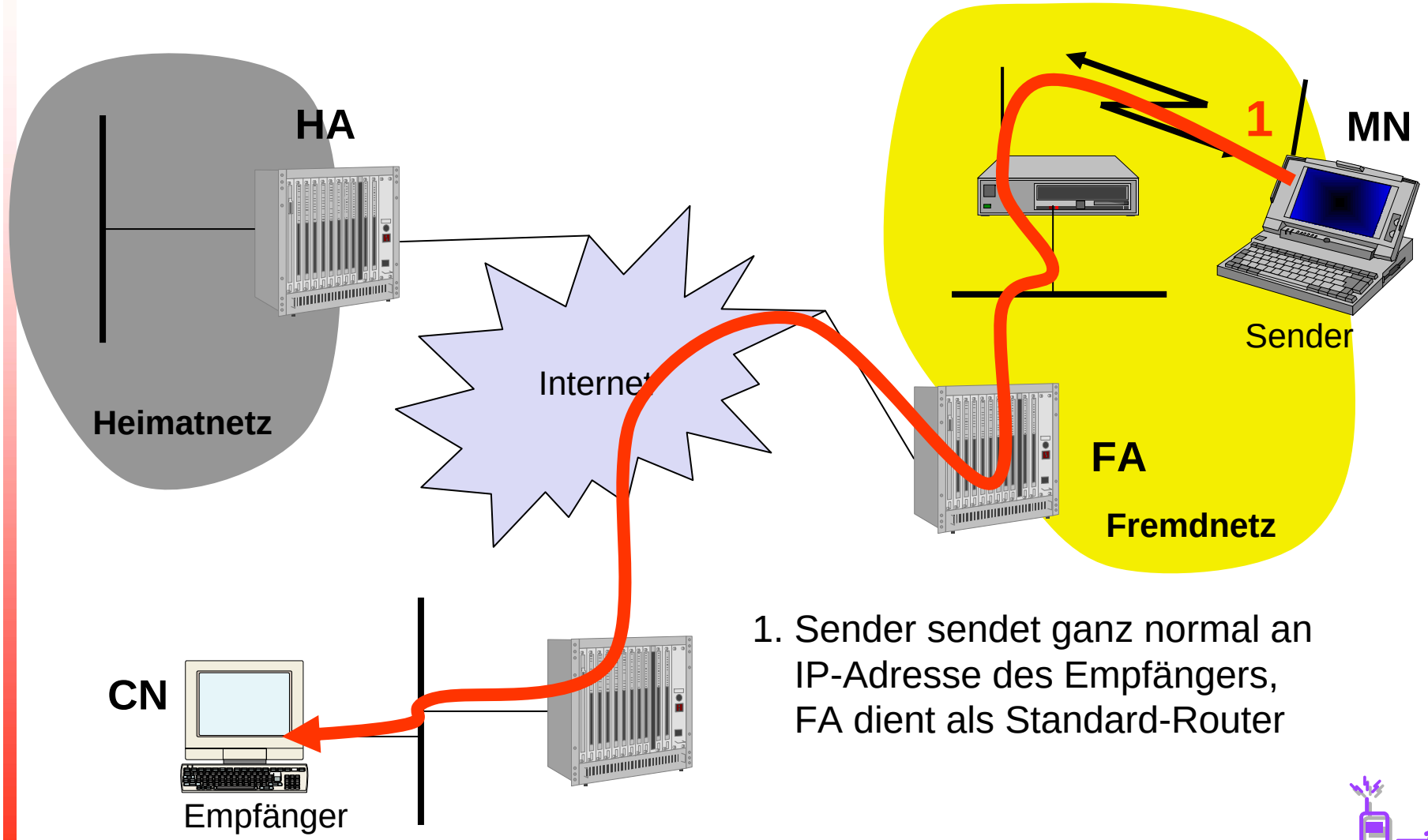
- **Mobile Node (MN)**
  - Knoten, der den Ort des Netzanschlusses wechseln kann, ohne seine IP-Adresse ändern zu müssen
- **Home Agent (HA)**
  - Einheit im „Heimatnetz“ des MN, typischerweise Router
  - verwaltet Aufenthaltsort des MN, tunnelt IP-Datagramme zur COA
- **Foreign Agent (FA)**
  - Einheit im momentanen „Fremdnetz“ des MN, typ. Router
  - weiterleiten der getunnelten Datagramme zum MN, stellt meist auch default-Router für den MN dar, stellt COA zur Verfügung
- **Care-of Address (COA)**
  - Adresse des für den MN aktuell gültigen Tunnelendpunkt
  - stellt aus Sicht von IP aktuelle Lokation des MN dar
  - kann z.B. via DHCP gewählt werden
- **Correspondent Node (CN)**
  - Kommunikationspartner

# Datentransfer zum Mobilrechner




1. Sender sendet an IP-Adresse von MN, HA fängt Paket ab (proxy ARP)
2. HA tunnelt Paket an COA, hier FA, durch Kapselung
3. FA leitet das Paket an MN weiter

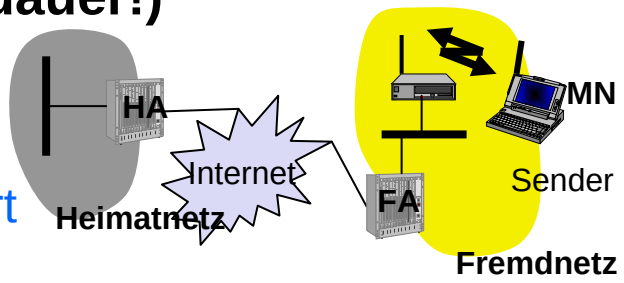
# Datentransfer vom Mobilrechner




1. Sender sendet ganz normal an IP-Adresse des Empfängers, FA dient als Standard-Router

# Netzintegration

- **Agent Advertisement**
  - HA und FA senden periodisch spezielle „Hello-“Nachrichten (lokal)
  - MN erkannt anhand „Hello“, ob im Heimat- oder Fremdnetz
  - MN erhält COA aus Nachrichten des FA
- **Registrierung (stets begrenzte Lebensdauer!)**
  - Adresse des MN (COA) via FA zu HA
  - HA bestätigt via FA an MN
  - Aktionen durch Authentifikation abgesichert




- **Bekanntmachung**
  - HA macht IP-Adresse des MN bekannt → gibt sich als MN aus
  - Router setzen ihre Einträge
    - relativ stabil, da HA nun für längere Zeit für MN zuständig ist
  - Pakete an MN nun an HA gesendet
    - Änderungen an COA und FA nun belanglos

# Kapselung

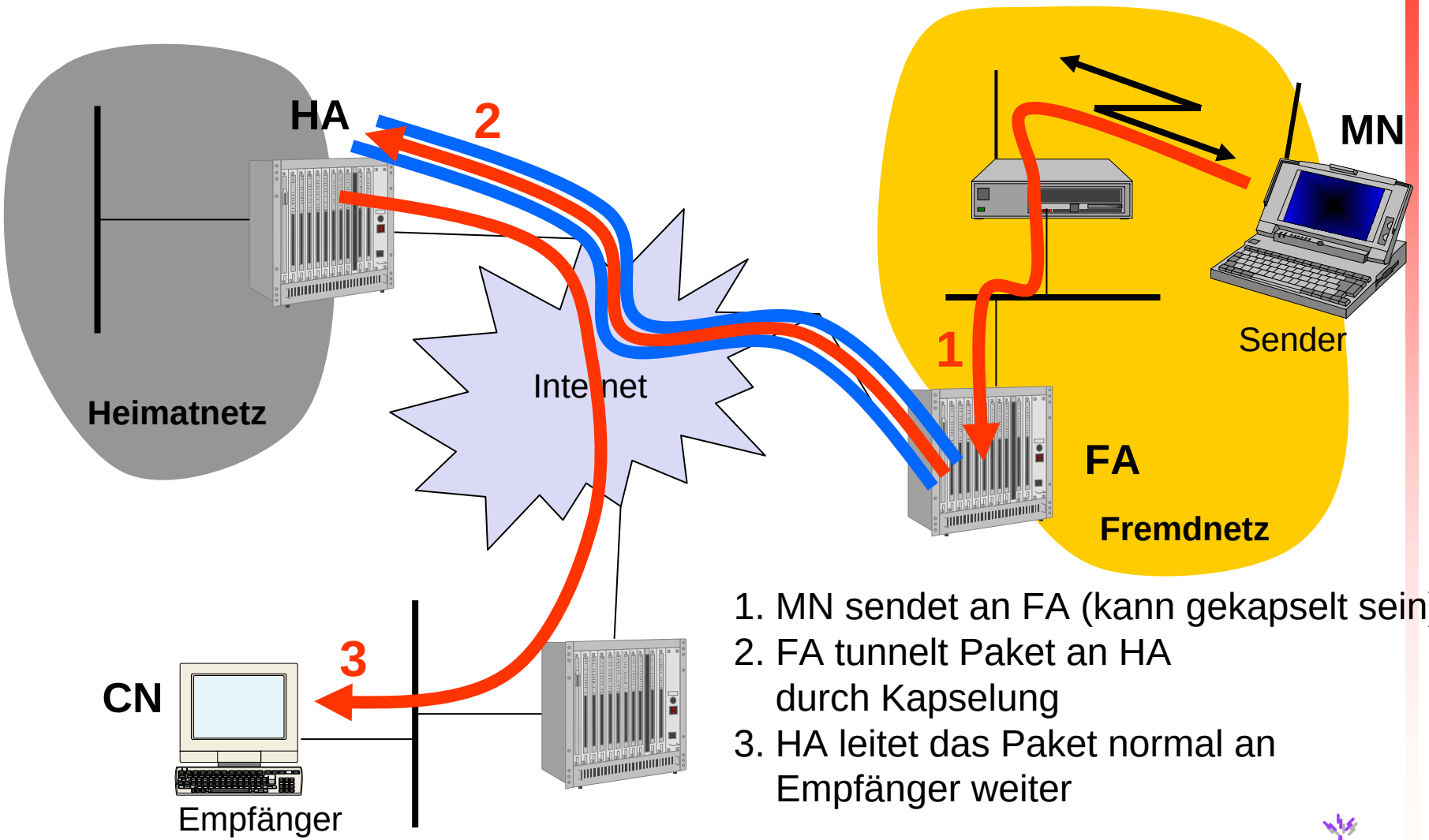
- **IP-in-IP-Kapselung**
  - Einkapseln eines Paketes in ein anderes als Nutzlast
- **Tunnel zwischen HA und COA**

| | | | | |
|---|---|---|---|---|
| Ver. | IHL | TOS | Gesamtlänge | |
| IP-Identifikation | | | Flags | Fragment Offset |
| TTL | | *IP-in-IP* | IP-Prüfsumme | |
| **IP-Adresse des HAs** | | | | |
| **Care-of Adresse COA** | | | | |
| Ver. | IHL | TOS | Gesamtlänge | |
| IP-Identifikation | | | Flags | Fragment Offset |
| TTL | | Schicht 4-Protokoll | IP-Prüfsumme | |
| **Originale Sender IP-Adresse des CNs** | | | | |
| **IP-Adresse des MNs** | | | | |
| TCP/UDP/ ... Nutzlast | | | | |

# Optimierung des Datenpfades

- **Triangular Routing**
  - Sender sendet alle Pakete via HA zum MN
  - unnötige Verzögerung und Netzlast
- **Lösungsansätze**
  - Lernen des aktuellen Aufenthaltsorts von MN durch einen Sender
  - direktes Tunneln zu diesem Ort
  - HA kann einen Sender über den Ort von MN benachrichtigen
  - große Sicherheitsprobleme
- **Wechsel des FA**
  - Pakete „on the fly“ während Wechsels gehen verloren
  - neuer FA kann alten FA benachrichtigen
    - Alter FA leitet noch ankommende Pakete an den neuen FA weiterl
    - FA kann Ressourcen für den MN wieder freigegen

# Reverse Tunneling




1. MN sendet an FA (kann gekapselt sein)
2. FA tunnelt Paket an HA durch Kapselung
3. HA leitet das Paket normal an Empfänger weiter

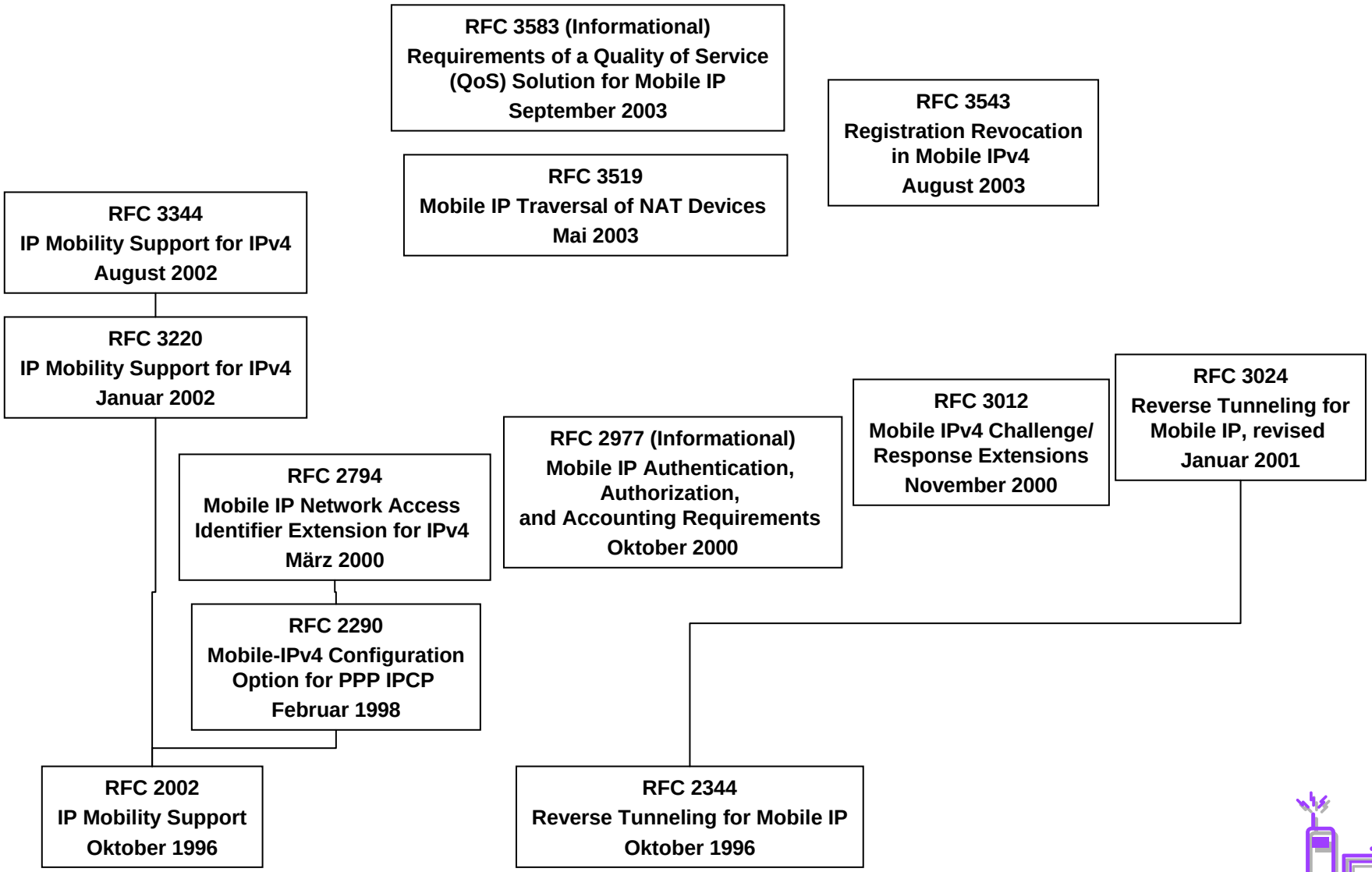
# Mobile IP mit Reverse Tunneling

- **Router akzeptieren oft nur „topologisch korrekte“ Adressen**
  - durch FA gekapseltes Paket des MN nun topologisch korrekt
  - Multicast und TTL-Problematik gelöst
    - TTL im Heimatnetz richtig, aber im fremden Netz zu klein
- **Reverse Tunneling löst nicht**
  - Problematik der *firewalls*
    - Nutzung des umgekehrte Tunnel (tunnel hijacking)
  - Optimierung der Wege
    - doppeltes Triangular-Routing
- **Neuer Standard ist rückwärtskompatibel**
  - Erweiterungen einfach integriert
  - Kooperation mit Implementierungen ohne die Erweiterung

# Probleme mit Mobile IP

- **Sicherheit**
  - Authentifikation mit FA problematisch
    - u.U. nicht unter eigener Kontrolle (fremde Organisation)
  - kein Standard für Schlüsselverwaltung und -verteilung
- **Firewalls**
  - verhindern typischerweise den Einsatz von Mobile IP
  - spezielle Konfigurationen sind nötig (z.B. reverse tunneling)
- **QoS**
  - häufige erneute Reservierungen im Fall von RSVP
  - Kein hineinsehen in den Tunnel
- **Sicherheit, Firewalls, QoS etc. sind aktueller Gegenstand vieler Arbeiten und Diskussionen!**

# Mobile IP: Standards



# Drahtlose Netzwerke
## Grundlagen und Einsatzfelder

## Mobile Transportschicht

# Traditionelles TCP

- **Staukontrolle**
  - Frameverlust
    - Annahme eines Staus
    - Datenrate massiv heruntergefahren
- **Slow-Start**
  - Herantasten an maximale Datenrate („congestion window“)
  - Verdoppeln des cw bis threshold erreicht, danach linear
  - Frameverlust oder doppelte Bestätigung
    → cw halbieren und von vorne beginnen
- **Fast Retransmit/Fast Recovery (optional)**
  - Bei doppelter Bestätigung *nicht* in Slow-Start gehen
    - Bestätigung → Paket empfangen, also wohl doch kein Stau
  - Nur bei ausbleibender Bestätigung Slow-Start

# TCP: Probleme im WLAN

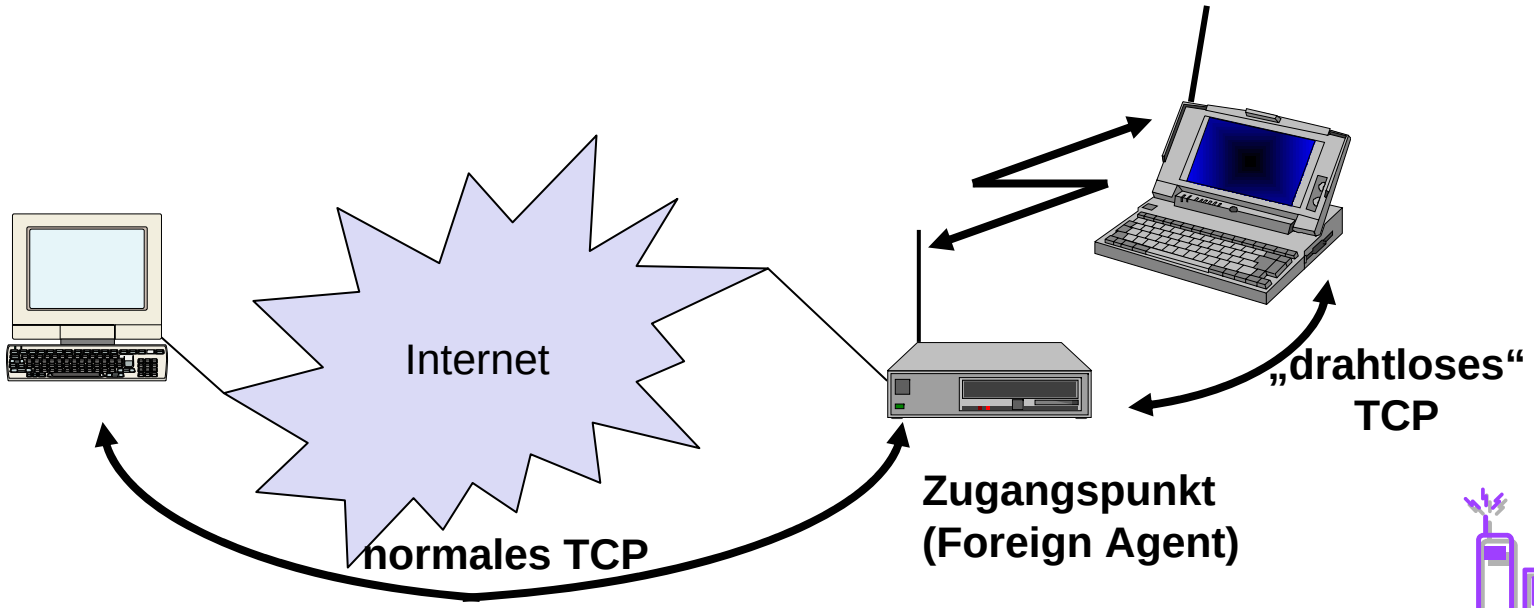
- **Fehlende Bestätigung = Stau?**
  - Verlustrate im WLAN wesentlich höher als im Festnetz
  - Retransmission auf MAC-Ebene
    - → größerer Jitter bei Empfang
    - → Wiederholung auf TCP-Ebene und MAC-Ebene gleichzeitig!
      - → Duplikate häufig nicht erkennbar (Verschlüsselung)
  - Mobilität führt zu Paketverlusten
    - Roaming, Mobile IP, ...
- **TCP erkennt Frameverluste durch Timer**
  - zieht falsche Schlüsse
  - Slow-Start kontraproduktiv bei einzelnen Frameverlusten

**→ „neues“ TCP notwendig**

**→ Aber: TCP kann nicht komplett geändert werden!**

# I-TCP

- **Indirektes TCP**
  - Aufteilung Verbindung in Festnetz- und WLAN-Teil
  - Zugangspunkt ist Proxy („Stellvertreter“)
  - Verbindung Festnetz ←→ Proxy
  - Verbindung Proxy ←→ drahtloses Netz

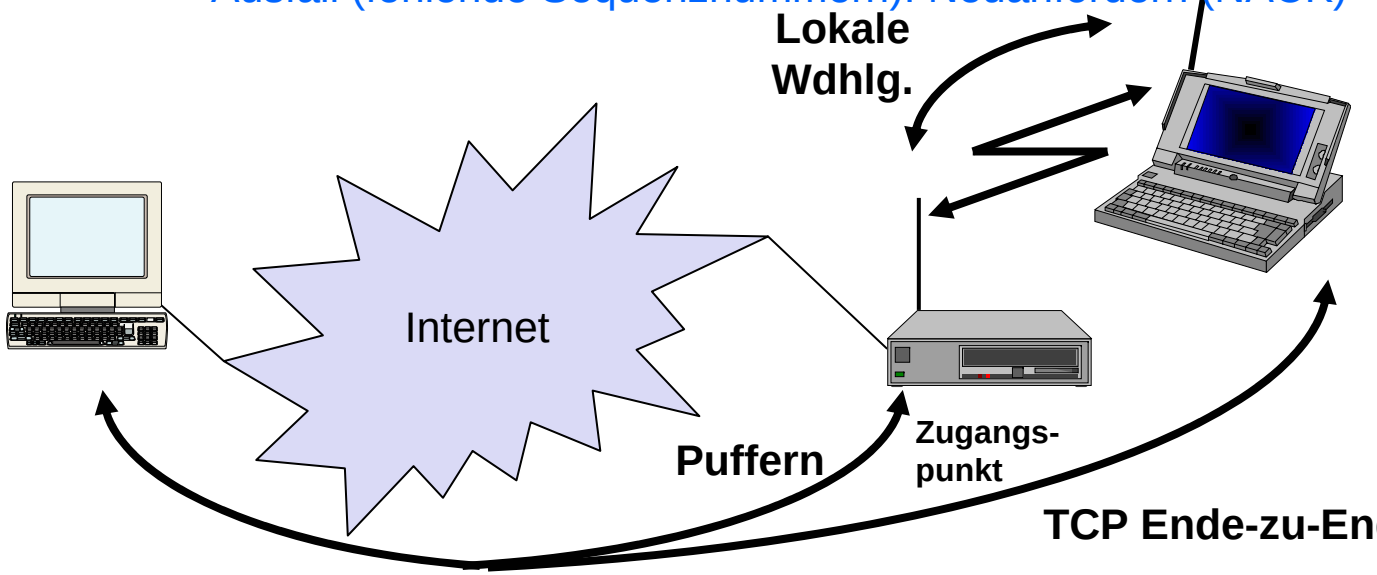


# I-TCP: Eigenschaften

- **Vorteile:**
  - Keine Änderungen an TCP notwendig
  - Übertragungsfehler pflanzen sich nicht in Festnetz fort
  - Drahtlos anderes Transportprotokoll als TCP möglich
    - Änderungen betreffen nur Proxy und MN
- **Nachteile:**
  - Ende-zu-Ende Semantik
    - Was, falls Proxy abstürzt?
    - Datenbank?
    - Transaktionen?
  - Stellvertreter vertrauenswürdig?
  - Wechsel der Stellvertreter?
    - Übertragung von Zustand notwendig

# Snooping TCP

- **„schnüffelndes“ TCP**
  - Kein Proxy, nur Zwischenspeicher
    - Verbindung Richtung Drahtlos:
      - Zugangspunkt speichert Frames zwischen
      - Bei fehlender Bestätigung: Lokale Wiederholungen
      - Doppelte Bestätigungen herausfiltern
    - Verbindung Richtung Festnetz:
      - Zugangspunkt liest Frames mit
      - Ausfall (fehlende Sequenznummern): Neuanfordern (NACK)



# Snooping TCP: Eigenschaften

- **Vorteile:**
  - Ende-zu-Ende Semantik
    - Für Kommunikationspartner transparent
  - Keine Zustandsübergabe bei Standortwechsel nötig
    - Neuer FA kann kein Snooping TCP → Rückfall auf „Standard“
- **Nachteile:**
  - Keine so gute Isolierung des Verhaltens des drahtlosen Netzes
  - NACK muss implementiert sein
  - Funktioniert nicht mit Verschlüsselung
    - IPSEC verschlüsselt TCP-Kopf, damit Sequenznummer
    - Sicherheitsmechanismen gegen Reply-Attacken