Mobility support for control signaling with the IETF NSIS protocol suite

Cornelia Kappler, Siemens AG / ITG Workshop Bremen, January 2006

Outline

- Introduction
- NSIS
  - NSIS Basics
  - NSIS lower layer (GIST)
  - NSIS Signaling Applications
  - NSIS Extension: off-path
- NSIS & Mobility
  - Problems for NSIS caused by mobility
  - General NSIS approach to mobility
  - QoS NSLP & MIP, HMIP, FMIP
  - QoS NSLP & Mobility in B3G
- Conclusion

Introduction

- **IP networks originally designed to just robustly deliver data**
- **Telecommunication networks and Internet converge**
  - Cf. Beyond 3G
- **Telecommunication networks offer sophisticated operator-centric control**
- **Flexible IP-based control protocols necessary**
  - QoS
  - Mobility
  - Security
  - Charging
  - Monitoring
  - …

Introduction – NSIS history

- **NSIS Working Group of the IETF chartered November 2001**
  - NSIS: “Next Steps in Signaling”

- **NSIS Charter**
  - develop general-purpose, extensible signaling protocol suite for control of network nodes
    - Broadened from original goal (QoS signaling beyond RSVP)

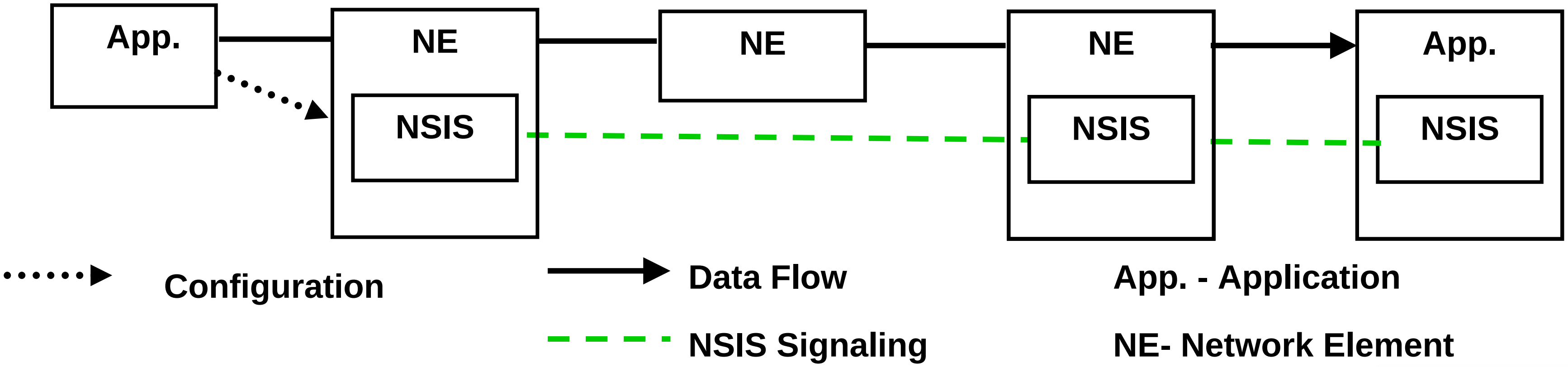
- **NSIS Timeline**
  - NSIS Requirements (RFC 3726) April 2004
  - NSIS Framework (RFC 4080) June 2005
  - First protocol specification (GIST) about to go into IESG review
  - Next protocol specifications (QoS NSLP, NATFW NSLP) expected to go into Working Group Last Call in spring

First set of protocols currently being finalized

SIEMENS

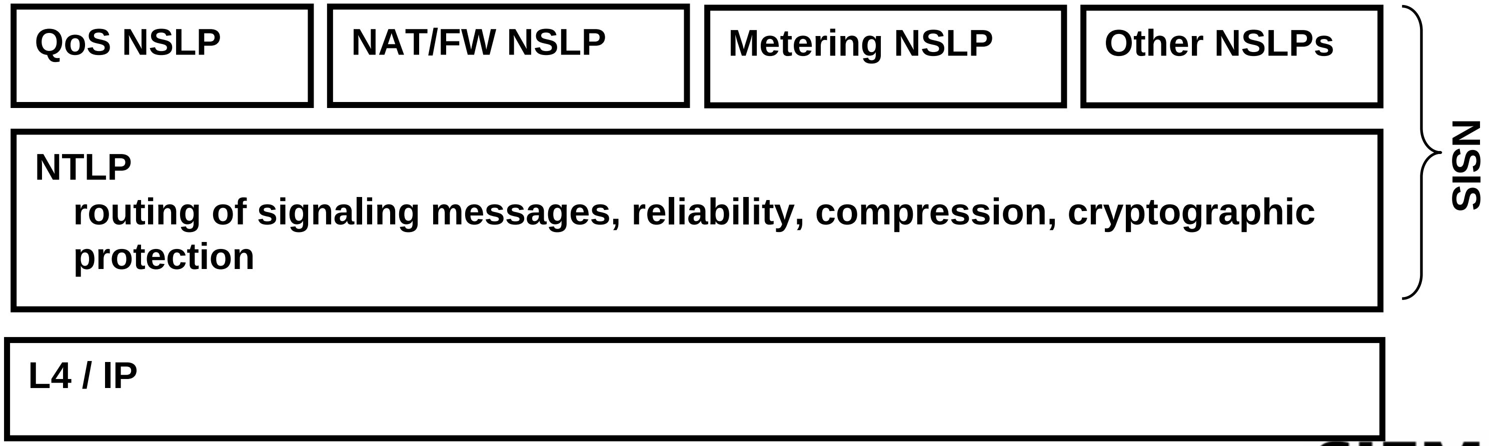
NSIS Basics

- **What is ‘Control Signaling’ in NSIS?**
  - Manipulation of flow-related control state held in network elements
    - setting up, modifying, monitoring and tearing down state
  - NSIS currently only covers ‘path-coupled signaling’
    - Signaling entities must be on the flow path
  - Not all routers on the data path need to take part in the signaling
  - Flow end-points may or may not be initiator / receiver of the signaling messages
    - Proxy operation build-in
  - Excludes network management, routing, e2e control (this would be SIP)



NSIS Basics

- NSIS protocol suite has two layers
  - Lower layer: “NSIS Transport Layer Protocol” (NTLP)
    - Provides functionality common to all control signaling applications
    - Establishment of secure signaling overlay
  - Upper layer: “NSIS Signaling Layer Protocols” (NSLPs)
    - Signaling applications, only contain signaling semantics
      - E.g. QoS signaling, NAT/Firewall configuration, (meter configuration) etc.
- New signaling applications (NSLPs) can easily be defined
  - Modular and extensible design
- All NSIS state is soft-state



QoS NSLP

NAT/FW NSLP

Metering NSLP

Other NSLPs

NTLP

routing of signaling messages, reliability, compression, cryptographic protection

L4 / IP

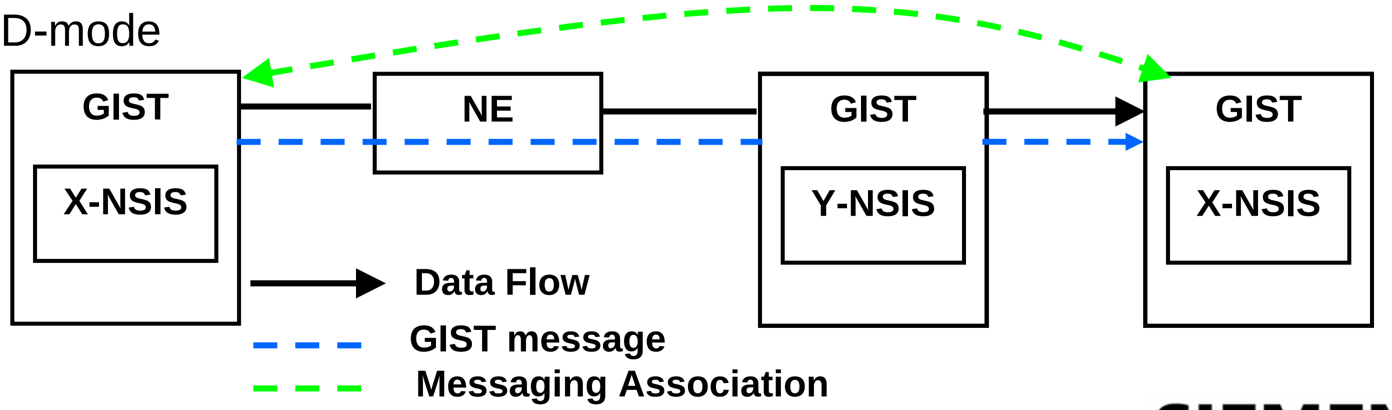
NSIS

GIST - Overview

- The current protocol specification for NTLP is GIST
- A NSIS-capable node implements GIST and typically one or more NSLPs
- Upon receiving a message from a local NSLP…
  - …GIST sends it to the next NSIS node on the flow path featuring the same NSLP
  - … where it is received by the local GIST, and delivered to NSLP
  - The message is now terminated - GIST signaling only hop-by-hop

GIST - Overview

- How does GIST know the next relevant NSIS hop?
  - First NSLP message for a new session
    - *“Datagram mode” (D-mode):*
      send packet to flow receiver with router-alert option / UDP
    - Next GIST node receives message and checks whether it locally has the right NSLP
    - If yes, it (usually) installs a “Messaging Association” with previous GIST node
      - Including Security Association building on existing protocols (IPSec, TLS,..)
      - Including „backwards routing state“
    - If it does not, it just sends the message on
  - Subsequent NSLP messages for a session
    - If Messaging Association exists: *“Connection Mode” (C-Mode)* over TCP
      - GIST directly addresses message to next GIST peer
    - Otherwise: D-mode



NSIS Signaling Applications: QoS NSLP

- **QoS NSLP is a QoS signaling protocol**
- **Reserves resources on a flow path**
- **Can be considered to be like RSVP, but more flexible**
  - Can provide sender/receiver/bidirectional reservation
  - No multicast support
  - Decouples resource description more fully from protocol
    - Can be used for multiple “QoS Models”
      - IntServ, DiffServ, 3GPP like description of QoS,…
  - Uses GIST for routing/transport
  - Mobility handling (as well as rerouting, etc)
  - Flexible location of sender / receiver (not just originator of flow)

NSIS Signaling Applications: NATFW NSLP

- NATFW NSLP is a protocol to configure Firewalls and NATs
- NAT /FWs can be obstacles to applications
  - => Desireable to enable the user to communiate with NAT / FWs
    - signal to open a “pinhole” in a firewall for his flow
    - User can inquire NAT about his address bindings
- Related to STUN / MIDCOM work but complementary

NSIS Signaling Applications: Metering NSLP

- Metering NSLP is a protocol for configuration of Metering Entities
  - Monitoring entities, accounting and charging entities
- Motivation
  - In future networks central configuration of metering entities unfeasible
- Metering NSLP follows data path and discovers and configures appropriate network nodes
- Metering entities usually are located on the data path
- Export of metering data by other means
- IPFIX, DIAMETER,…
- Configuration information distributed
- Select network elements doing the metering
- Description of Triggers to start / stop accounting
- Distribution of identifiers for Collector / flows / user

NSIS Extension: Off-path NSIS

- Some NSIS applications could benefit from including off-path entities
  - Bandwidth brokers in QoS NSLP, ….
  - Interworking with / Integration into 3GPP, ITU-T
  - Migrating from other QoS signaling solutions
- IETF is not fond of centralized control
  - NSIS is restricted to on-path signaling currently
- ID "A Problem Statement for Path-Decoupled Signalling in NSIS"
  - Describes scenarios and possible NSIS modifications
  - NSIS feature: do on-path and off-path signaling with one protocol
  - Only minor NSIS modifications necessary, e.g.
    - GIST QUERY is redirected to off-path node
    - Messaging Association is built with off-path node
  - http://www.ietf.org/internet-drafts/draft-hancock-nsis-pds-problem-01.txt
  - Some likelihood to become working group draft

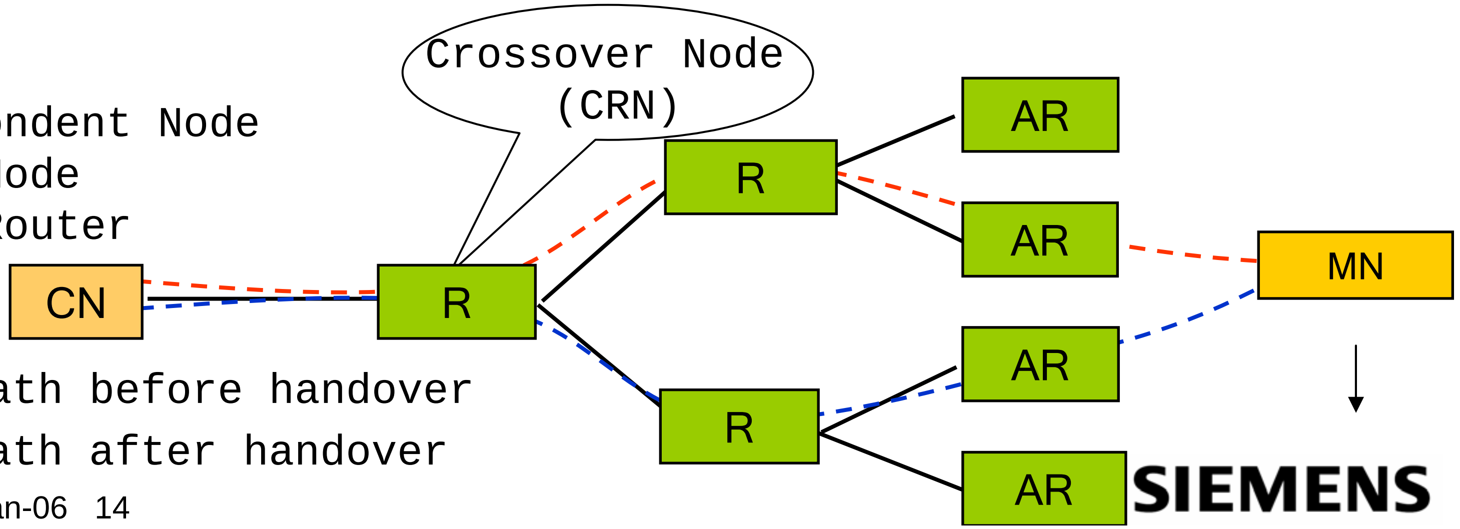
Outline

- Introduction
- NSIS
  - NSIS Basics
  - NSIS lower layer (GIST)
  - NSIS Signaling Applications
  - NSIS Extension: off-path
- NSIS & Mobility
  - Problems for NSIS caused by mobility
  - General NSIS approach to mobility
  - QoS NSLP & MIP, HMIP, FMIP
  - QoS NSLP & Mobility in B3G
- Conclusion

Problems for control signaling caused by mobility

- Due to handover, a part of the packet path is rerouted
  - Between CRN and MN
- Due to handover, the IP address of the MN may change
- On the new part of the path, new state must be installed
- On the old part of the path, the old state must be torn down
- On the unchanged part of the path between CN and CRN, the state must be maintained
  - NSIS signaling must recognize CRN
  - At CRN join new and old branch of the session
    - Recognize they are really „the same“ session
      - Identification of session must not be based on IP address

R – Router
CN – Correspondent Node
MN – Mobile Node
AR – Access Router

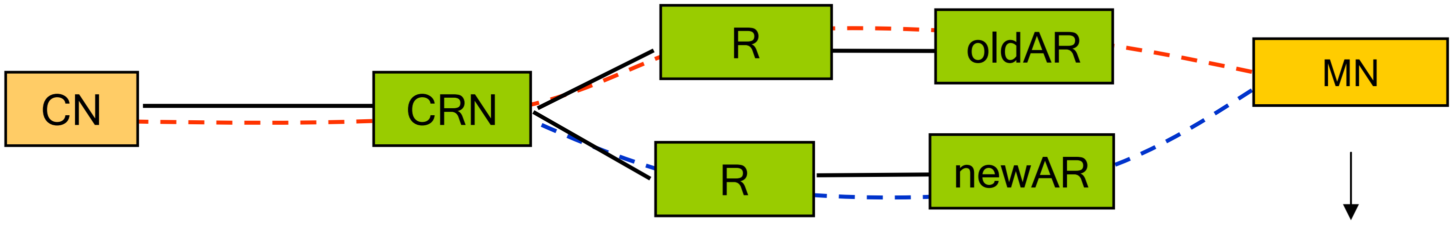


---- packet path before handover

---- packet path after handover

General NSIS approach to mobility

- NSLP sessions are identified by a randomly generated Session ID
  - Doesn‘t change due to mobility event
  - Allows joining of reservations on old and new path
- Packets belonging to a particular session are identified by a Flow ID (filter)
  - E.g. sender / receiver IP address, ports etc
  - Must be updated on entire path when IP address changes
- NSLPs may introduce additional mobility support
  - Mobility problems are thought to be NSLP specific



```
R  – Router
CN – Correspondent Node
MN – Mobile Node
AR – Access Router
```

---- „old“ session

---- „new“ session

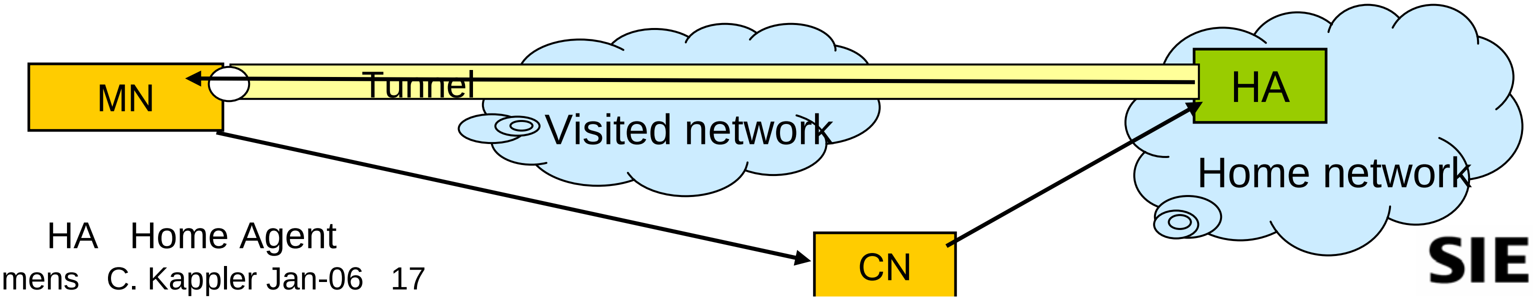
Overview of QoS NSLP approach to mobility cont‘

- Assumptions on this page
  - MN receives new IP address due to handover
  - CN learns new IP address (e.g. Binding Update)
  - Direct routing between MN and CN
- Note: Reserve and Refresh are identical messages in QoS NSLP
- **Update of QoS NSLP reservation MN -> CN**
  - When MN arrives at new Access Router, it issues a RESERVE
    - With old session ID and new flow ID (because IP address changed)
    - RESERVE causes „new“ reservation on new path between MN and CRN
  - When RESERVE arrives at CRN, CRN recognizes it as a known session arriving at a new interface
    - CRN sends RESERVE on, towards CN, in order to refresh reservation and update Flow ID
  - „old“ reservation between MN and CRN times out or can be town down actively by CRN
    - Possible authorization problem: is it important that a reservation can be torn down only by the node that originally initiated it?
- **Update of QoS NSLP reservation CN -> MN**
  - CN sends RESERVE towards MN‘s new IP address
  - Between CN and CRN, the existing reservation is refreshed and the Flow ID updated
  - At CRN the RESERVE leaves the „old path“ and automatically causes a new reservation
    - GIST determines it must use datagram mode because flow ID changed
    - CRN must have intelligence to tear down old reservation
- NOTE: upstream and downstream CRN are not necessarily the same node
  - Because of asymmetric routing

QoS NSLP and Mobile IPv6

- Mobile IPv6 summary
  - MN has both home address and Care of Address (CoA)
  - MN registers CoA with Home Agent (Binding Update)
  - 3 possible routing scenarios

1. Triangle routing (see Figure)
   - CN -> MN
     - CN addresses packets to home address
     - HA tunnels them to CoA
       -> for tunnel: source address HA, destination address CoA
     - Tunnel between HA and MN
   - MN -> CN
     - MN sends packets directly to CN (CoA as source address)
2. Reverse Tunnelling
   - CN -> MN as above
   - MN -> CN
     - MN tunnels packets via HA in order to hide its location
       -> for tunnel: source address CoA, destination address HA
3. Route Optimization
   - MN sends Binding Update to CN, too
   - All packets are sent directly between MN and CN



HA Home Agent

SIEMENS

QoS NSLP and Mobile IPv6 cont‘

- QoS NSLP signaling with MIPv6

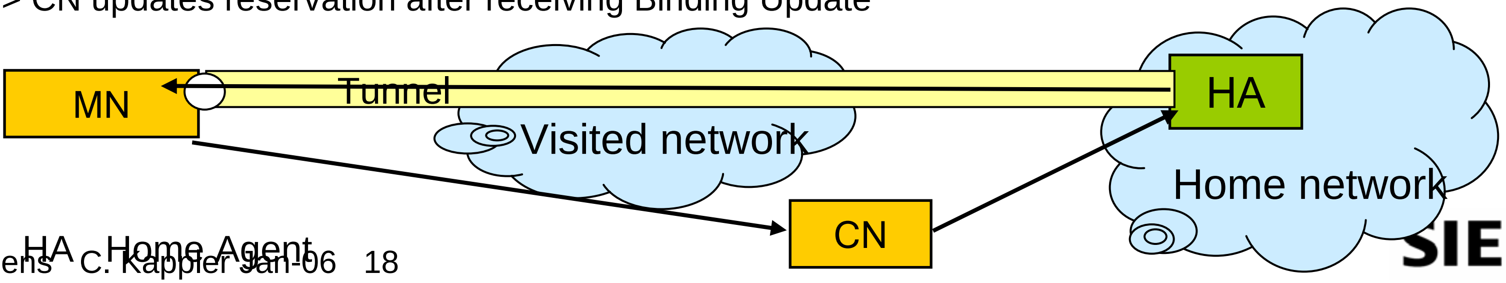
1. Triangle routing (see Figure)
   - CN -> MN
     - CN sends RESERVE to home address

     -> results in reservation between CN and HA

     -> RESERVE tunnelled between HA and MN (i.e. has no effect)
     - HA, upon receiving RESERVE, initiates independent RESERVE for the tunnel
     - When CoA changes due to handover, HA updates reservation for tunnel
   - MN -> CN
     - MN sends RESERVE directly to CN
     - When CoA changes due to handover, MN initiates new RESERVE (see above)
2. Reverse Tunnelling
   - CN -> MN as above
   - MN -> CN
     - MN sets up reservation for tunnel to HA
     - Additional RESERVE is tunnelled to HA and sets up reservation between HA and CN
3. Route Optimization
   - Both MN and CN set up normal reservations
   - When CoA changes due to handover

   -> MN immediately updates reservation

   -> CN updates reservation after receiving Binding Update



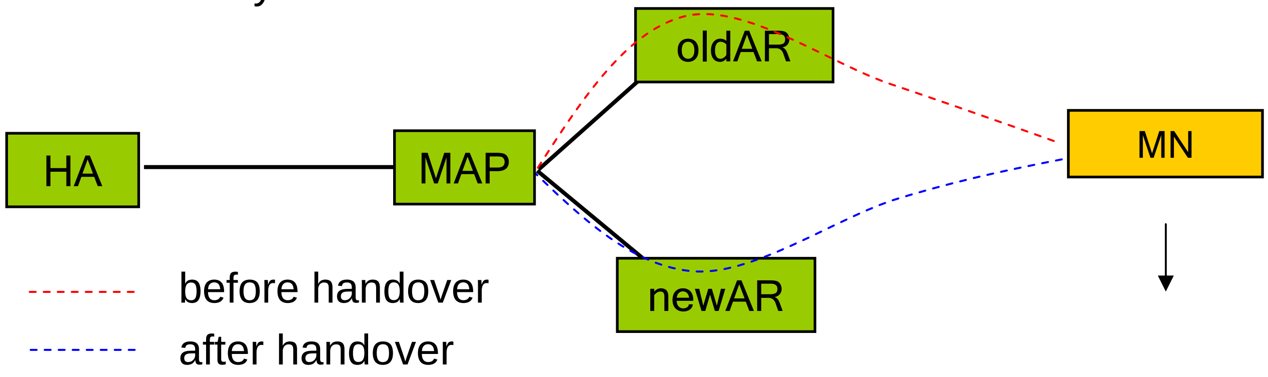
HA Home Agent

QoS NSLP & HMIP, FMIP

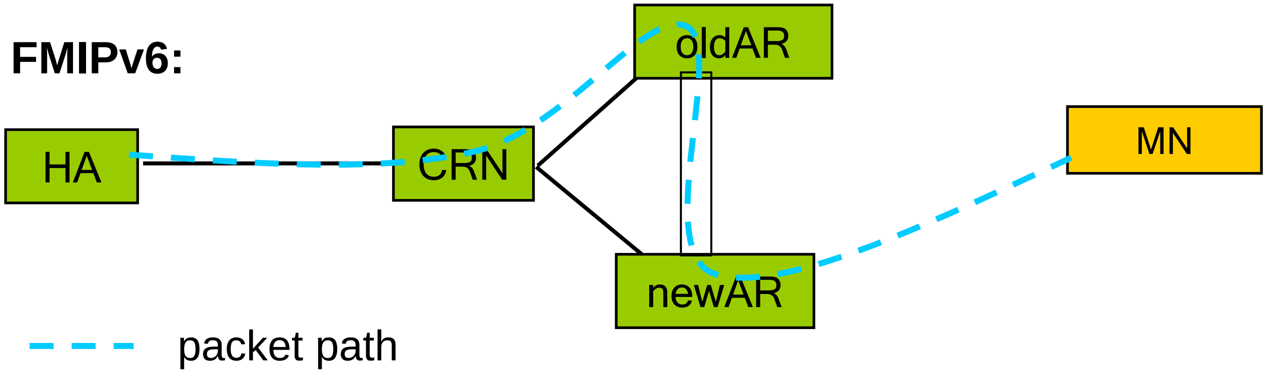
- HMIP and FMIP just introduce additional tunnels
  - must be set-up and maintained independently

HMIPv6:

MAP Mobility Anchor Point



FMIPv6:



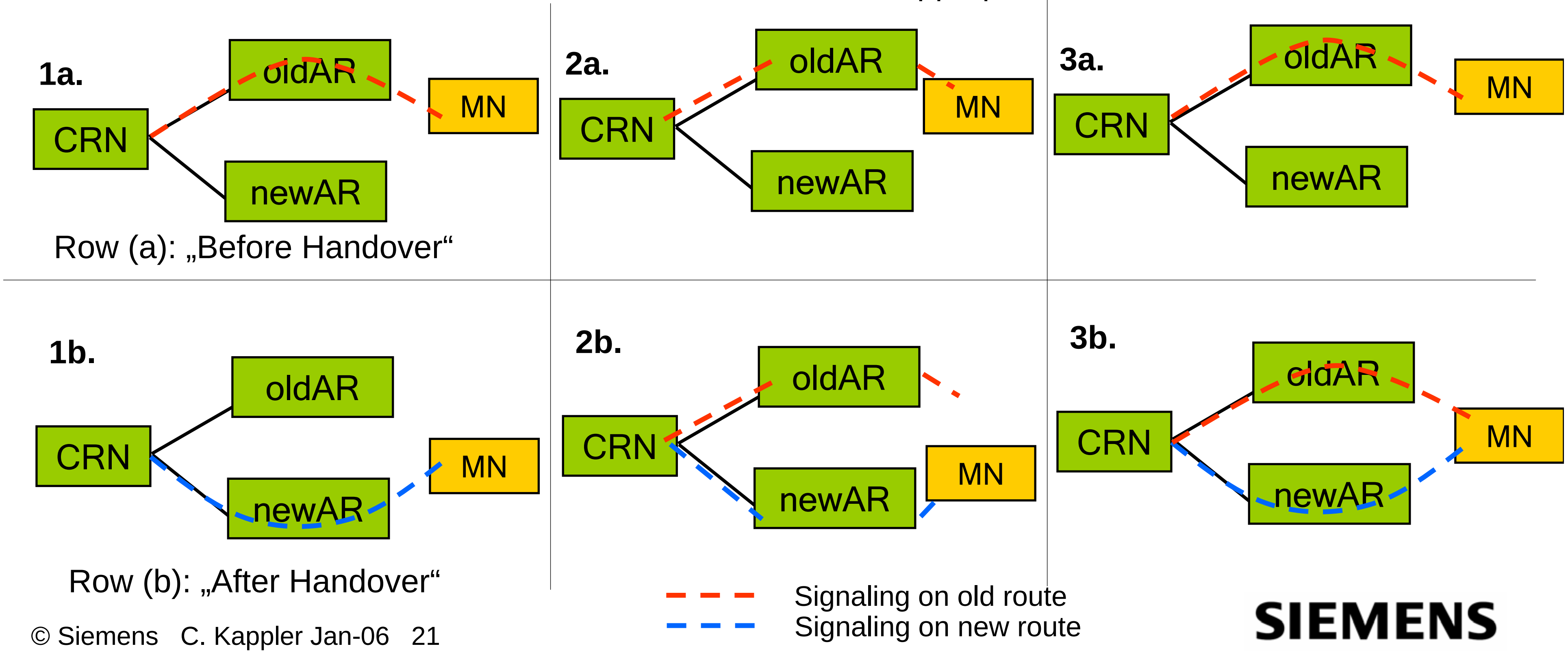
QoS NSLP & Mobility in B3G I

- NSIS signaling should be issued by a proxy in the network (e.g. AR) rather than by the MN
  - NSIS allows proxy operation
  - Collaboration of NSIS with „MIP“ in such a scenario depends on details of mobility handling
    - Presumably MN doesn‘t issue MIP messages in this scenario either
- make-before-break desireable
  - i.e. reserve on the new path before tearing down reservation on the old path
  - QoS NSLP has a „REPLACE“ flag
    - When not set, the reservation on the old section of the path will not be torn down immediately
    - This way, a „bifurcating“ reservation can be maintained
    - Who initiates tear-down when?

QoS NSLP & Mobility in B3G II

- Fast teardown of reservations, particularly on the air interface

1. In a „standard IP situation“ with MN initiating the signaling and „break-before-make“: impossible
2. When AR proxies the NSIS signaling for the MN, oldAR can tear down reservation on air interface as soon as it notices MN moved away
   - Cannot tear down yet towards CRN, because CRN is not determined yet (except in well defined environments)
3. In „make-before-break“, MN can initiate tear-down when appropriate



Conclusion

- NSIS is a general-purpose, extensible signaling protocol suite for control of network nodes
- NSIS protocol suite has two layers
  - Lower layer: “NSIS Transport Layer Protocol” (NTLP)
    - Provides functionality common to all control signaling applications
    - Establishment of secure signaling overlay
  - Upper layer: “NSIS Signaling Layer Protocols” (NSLPs)
    - Signaling applications, only contain signaling semantics
- Current NSLPs
  - QoS NSLP, NATFW NSLP, (Metering NSLP – not yet Working Group Item)
- NSIS design „mobility aware“
  - QoS NSLP can work with Mobile IP and its optimizations (HMIP, FMIP) “as-is”
    - No changes to the protocol necessary
  - Need extra logic in MN and HA
    - Must update reservation when IP address of MN changes
  - Need extra logic in CRN
    - If it is supposed to tear down reservation on old portion on the path
  - Mobility support in proxy operation requires further thought