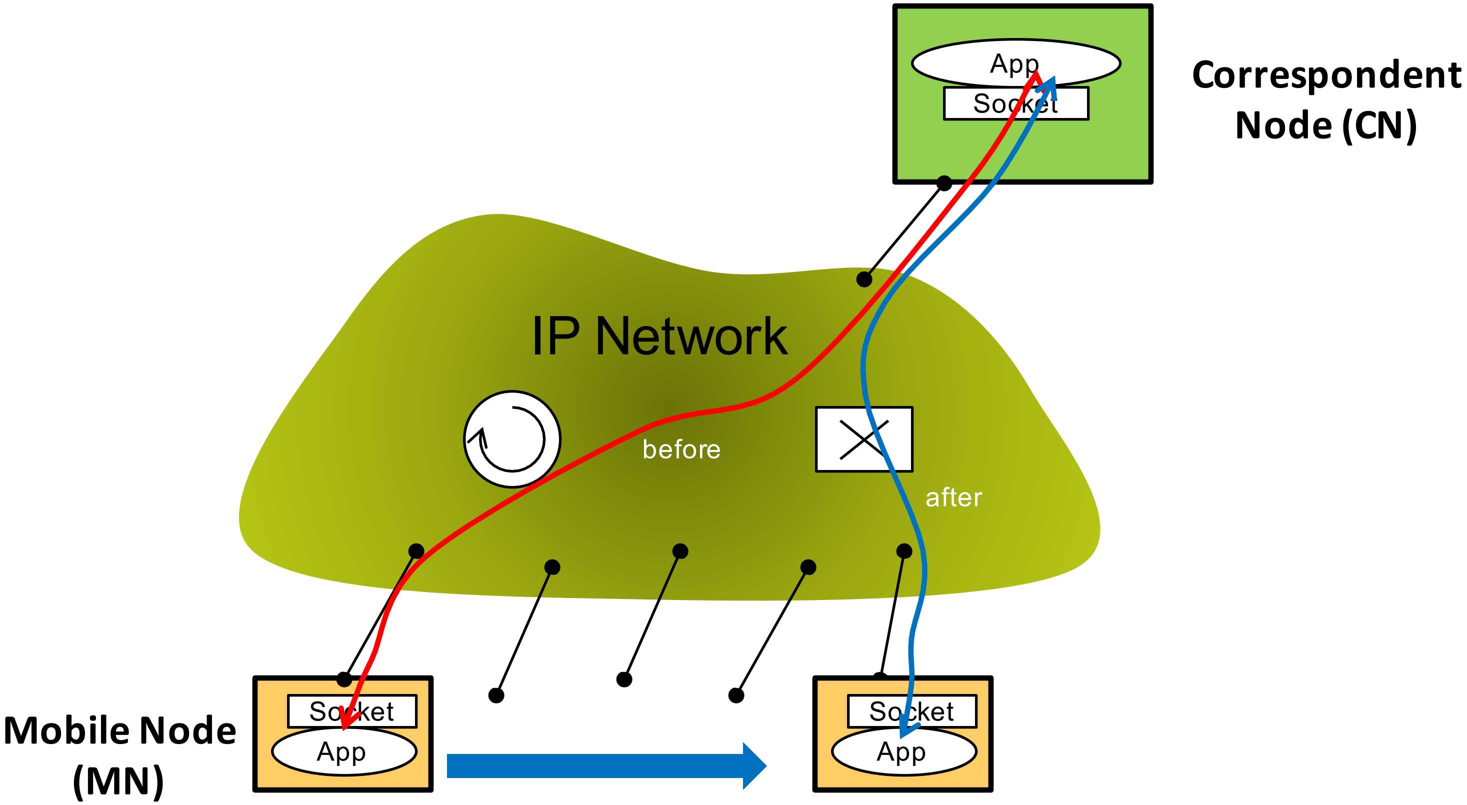
Support for IP Mobility

IP Mobility Problem Statement



- An application on a fixed correspondent node (CN)desired to maintain its <u>application session </u>(eg. voice) with a mobile node (MN) whose IP point of attachment to the network changes during the application session.

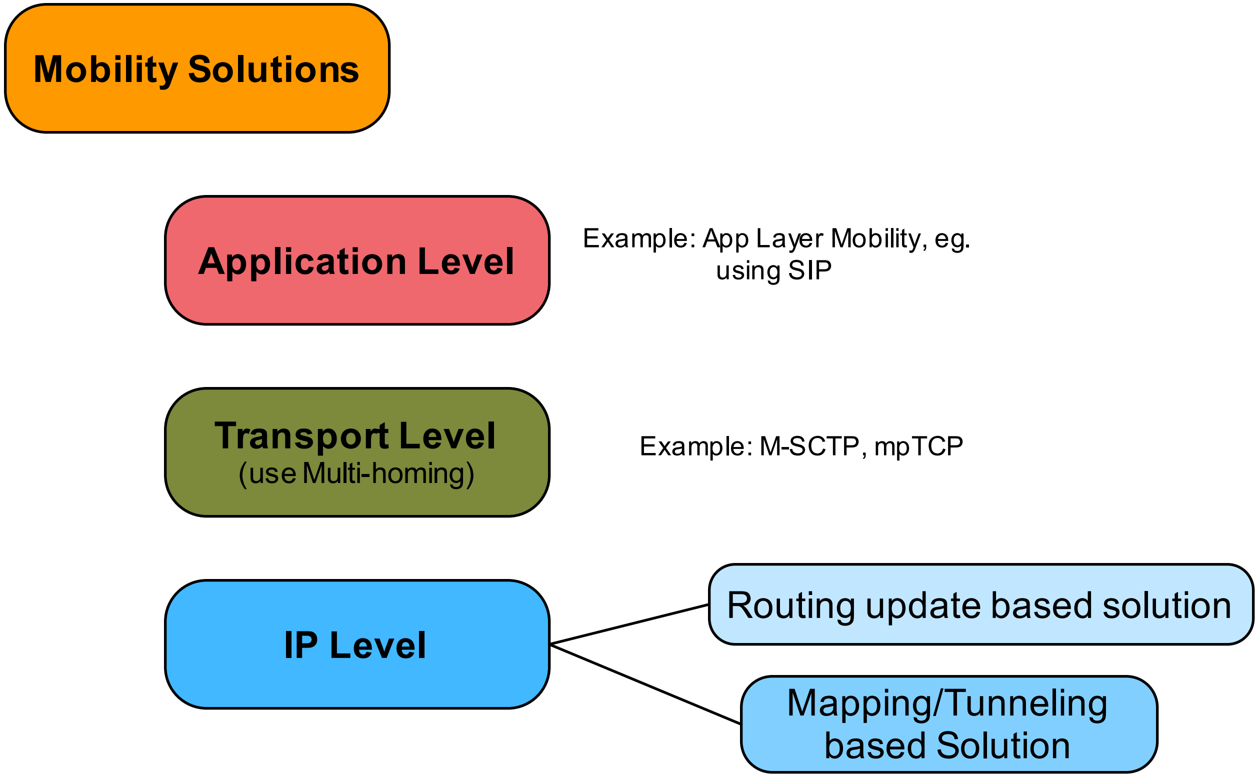
Definitions

- Identifier
  - A stable value used to identify a mobile node which does not change as the MN moves around
- Locator
  - The IP address of the MN’s current point of attachment to the network. It is the topologically correct subnetwork address of where the mobile is.
- Mapping
  - Between the identifier and the locator.

Axis for categorizing Mobility Solutions

1. Scale
    1. Local Mobility Management: manages mobility only within a limited scale, eg. operator’s network
    2. Global Mobility Management: manages mobility with a wider scale, i.e. identifier does not change on a global scale
2. Layer at which the solution works
    1. Application layer
    2. Transport layer
    3. Network layer
    4. L2 layer (Strictly not IP mobility problem)
3. Is CN’s protocol stack mobility aware
    1. Yes
    2. No
4. Is MN’s protocol stack mobility aware
    1. Yes
    2. No

Survey of Mobility support protocols for IP



Mobility Solutions

Application Level

Example: App Layer Mobility, eg. using SIP

Transport Level (use Multi-homing)

Example: M-SCTP, mpTCP

IP Level

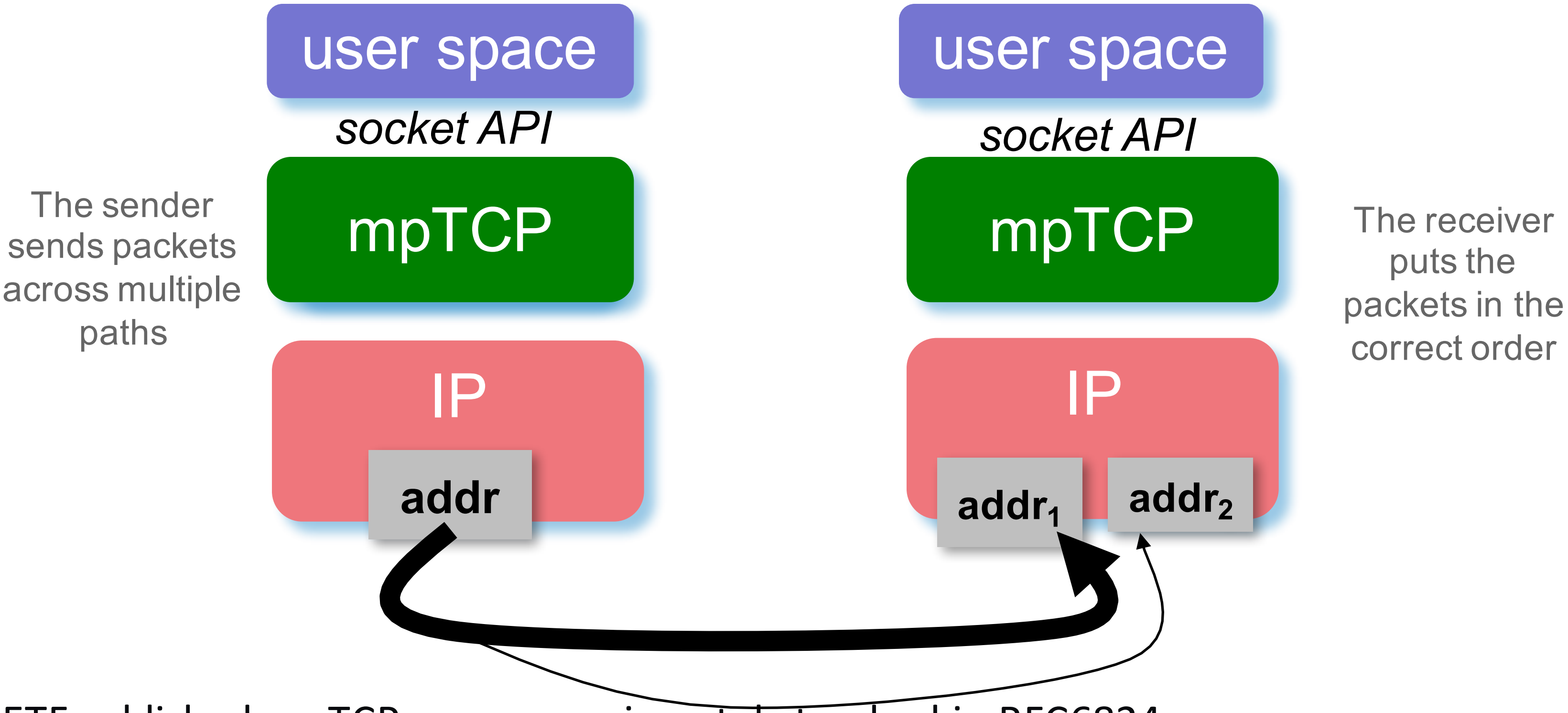
Routing update based solution

Mapping/Tunneling based Solution

- IP level mobility would provide a solution that can be used by all the upper layers and hence do not require support from the upper layers.

Transport Layer based Schemes

Multipath TCP (mpTCP)

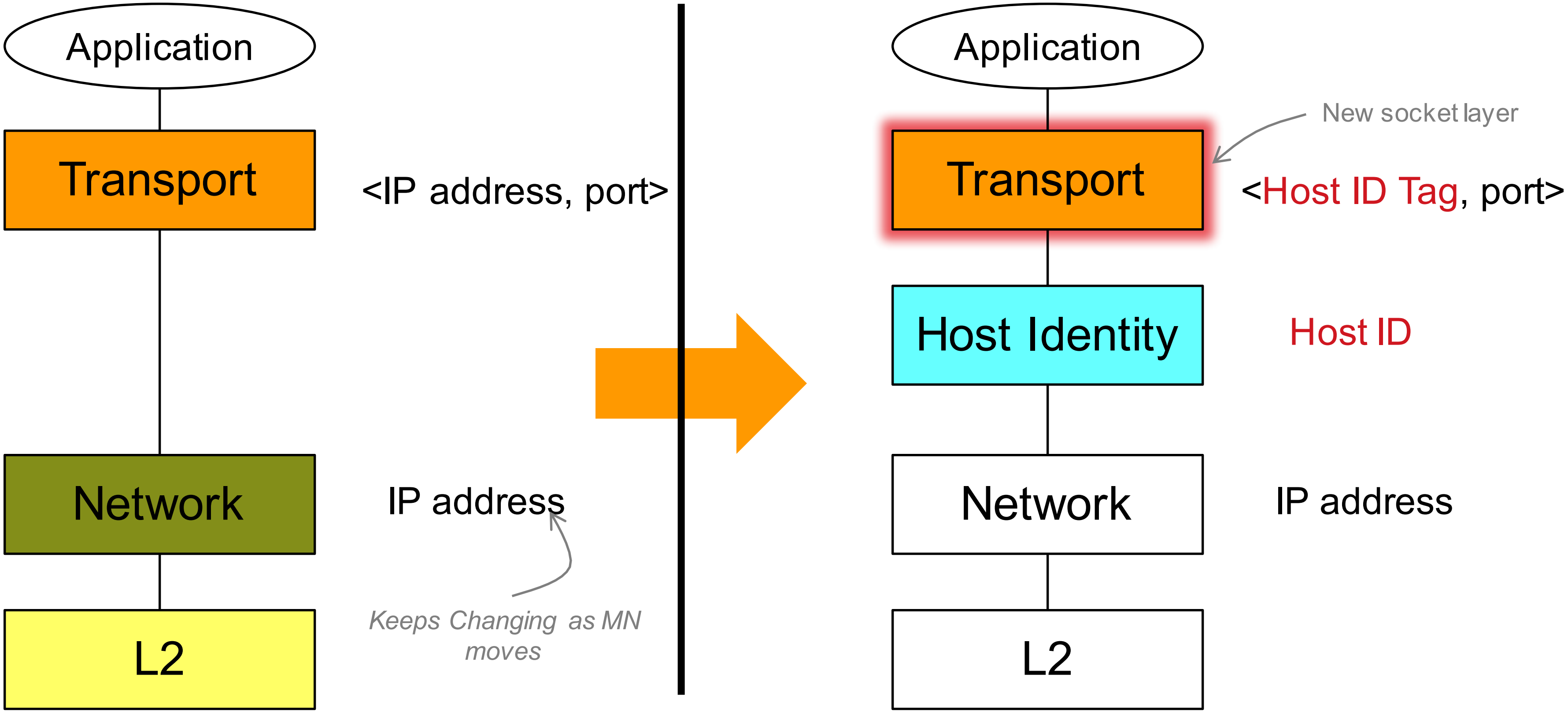


The sender sends packets across multiple paths

The receiver puts the packets in the correct order

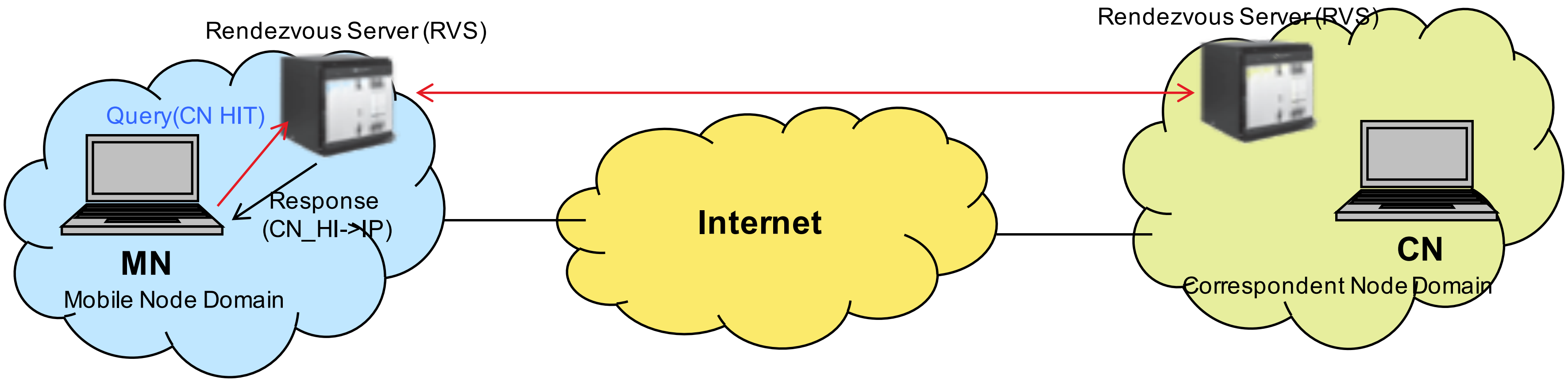
- IETF published mpTCP as an experimental standard in RFC6824
- Apple iOS7 released in September 2013 provides support for mpTCP for its Sirri application.
- mpTCP has been written to be backwards compatible with TCP
  - An mpTCP host can communicate with a TCP host
  - Socket API is written in such a way that an unmodified application can make use of the new socket API.

Host Identity Protocol (HIP): RFC 5201 (2008) Experimental



- The HIP protocol introduces a new permanent identifier for host, which is called the Host Identity. HI is tied to the public key of the host. The Host Identity Tag (HIT) is a 128 bit hash from the public key.
- The transport layer (new socket) binds to the HIT (and not the locator IP address).

HIP: Mapping from Host Identity to IP addresses



- HIP by default uses its own static infrastructure Rendezvous Servers.
- Each mobile node has a designated Rendezvous Server (RVS), which tracks the current location of the mobile node.
- When a CN wants to communicate with mobile node, it queries DNS with a mobile node's HIT to obtain the IP address of the mobile node's RVS.
- If the mobile node moves to a new address, it notifies the CN by sending HIP UPDATE with LOCATOR parameter indicating its new IP address (Locator). Meanwhile, it also updates the mapping in RVS.

IP Level Mobility Solution

Survey of Mobility support protocols for IP

- Informational RFC 6301, “A Survey of Mobility Support in the Internet”, July 2011 is a good survey of the various approaches till date.

- The main problem of mobility is how to send data to a moving receiver.
  - ➡ The sending node is called Correspondent Node (CN)
  - ➡ The moving node is called mobile node (MN)

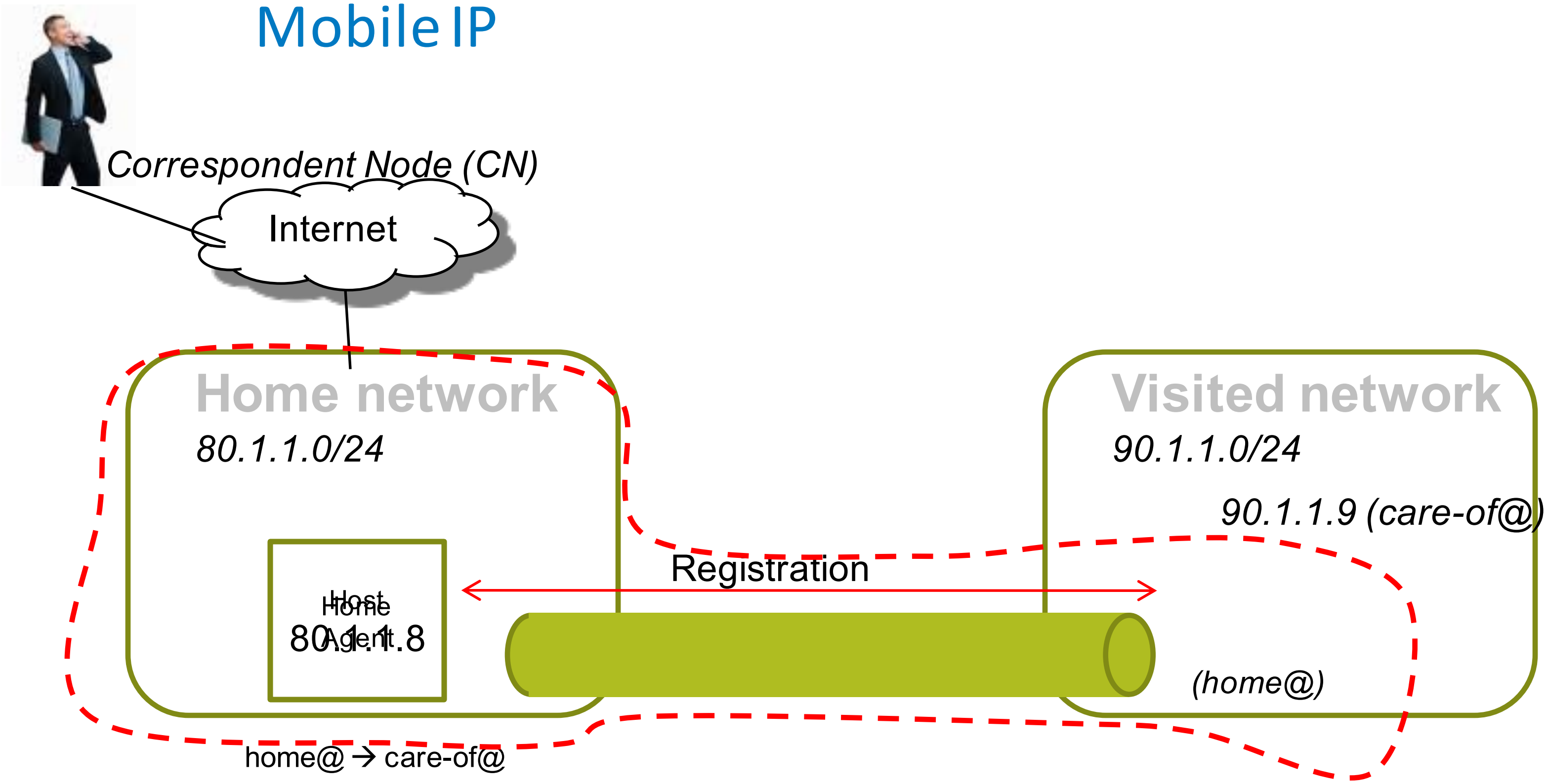
- One of the main goals of mobility solution is to provide “seamless” session continuity
  - ➡ “Seamless” term is used to imply that the user does not perceive any interruption in service. For voice this can equate to less than 200 msec of interruption. For streaming video, the interruption can be longer due to buffering. For web browsing, it could mean that the web page downloads completely.

IP Layer based Mobility Solution

1. Routing-update based solutions
   - MN keeps its IP address unchanged
   - As the MN moves, the routing information is updated so that packet arrives to the subnetwork where the mobile is currently located
   - Pros: CN is not impacted. No tunneling
   - Cons: Routing tables need to be updated at a fast rate.
   - Example: Cellular IP, HAWAII (not commercially implemented)

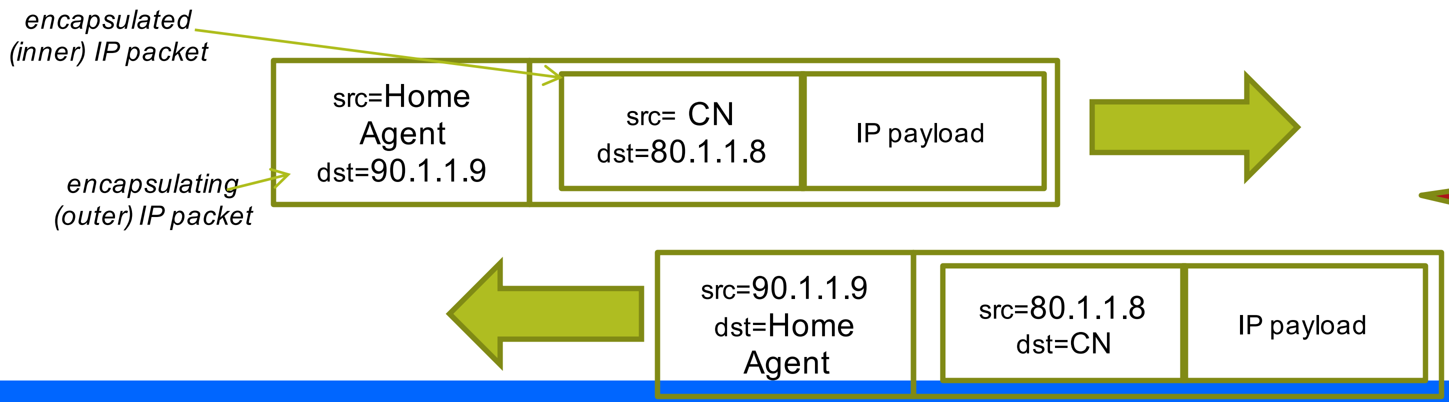
2. Tunneling/Mapping based solution
   - The MN node has one **identifier** that it keeps unchanged.
   - The MN node has a **locator** which is typically in the subnetwork where the UE is.
   - **Mapping system** maintain mapping between identifier and locator
   - Pros: CN is not impacted. Routing is not impacted.
   - Cons: Requires a node to maintain the mapping between identifier and locator. Tunneling is needed to get the packet to its destination.
   - Examples:
     - GTP, PMIP (MN not mobility aware),
     - MIP (MN is mobility aware)

Mobile IP



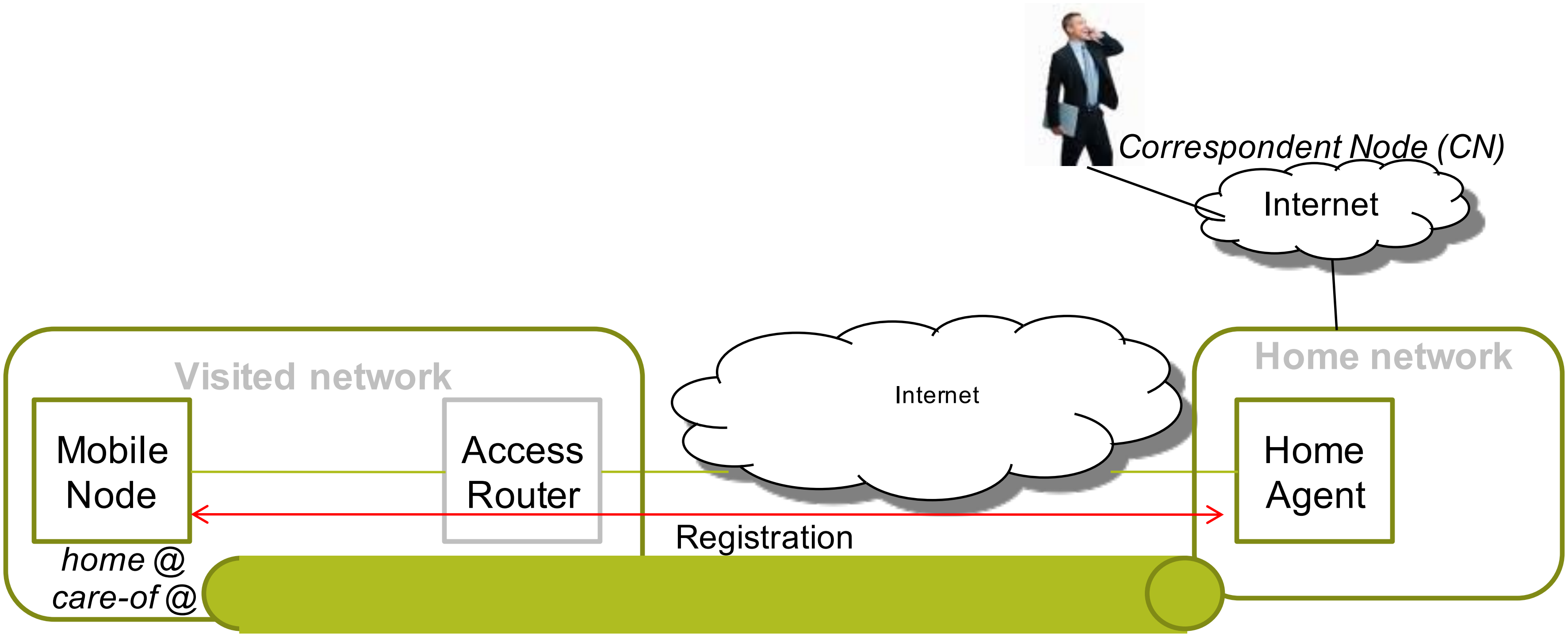
Origin authenticated, integrity/replay protected

Registration: "*Dear Home Agent, please intercept packets destined to 80.1.1.8 on my behalf and tunnel them to 90.1.1.9*"



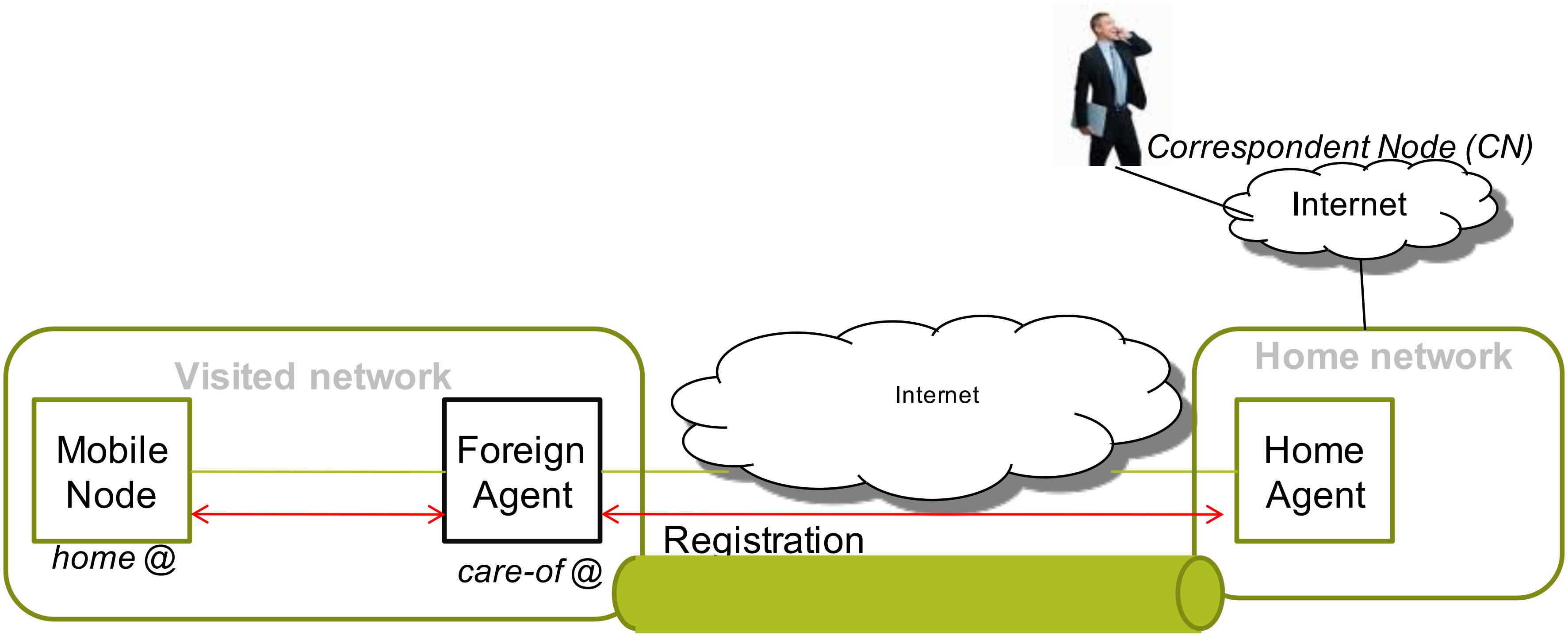
Tunnel extends the home network topology to the host@visited network

Mobile IP Variants



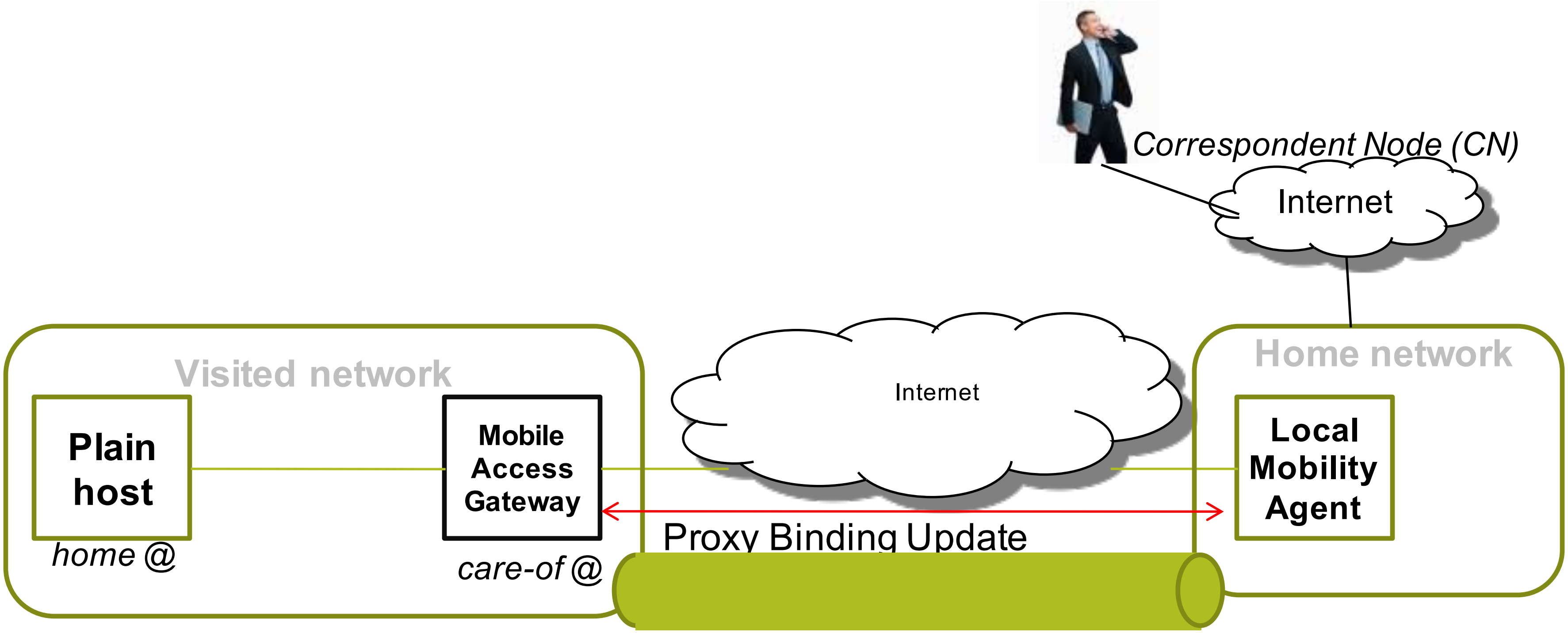
- Mobile IPv4, IETF RFC 3344
- Mobile IPv6, IETF RFC 3775/3776 (Registration is called Binding Update)
  - Several mobility support headers options allowed in IPv6 header. Also CN can directly tunnel packets to the MN without going via the HA.
- Co-located care-of address

Mobile IP Variants



- FA-located care-of address
  - ➡ No need to allocate dedicated CoAs to each Mobile Node
- Only applies to Mobile IPv4

Mobile IP Variants



- Proxy Mobile IPv6, IETF RFC 5213

Issues with Tunneling Mobility Protocols (MIP, GTP)

- Requires extensive network support, Home-agent, Foreign-agent.

- Tunneling is a “hack” to get packets to reach a home-address which is not topologically correct (i.e in a foreign network).

- Results in “two-hop” routing in both directions: CN <-> HA <-> MN.

  - In the MN-CN direction, MN can send traffic directly to CN, but due to presence of NAT at the CN’s domain (NATs will not have “hole” open for MN’s address) and firewall (not allowing traffic from source not initially contacted by the CN).

- Several optimizations for MIP have been proposed, but we will not go into them further, but focus on alternative schemes for supporting mobility in the next few slides.

Overview

- IP protocol was not designed with mobility in mind.
  - ➡ If the IP address changes, an IP session using TCP or UDP breaks. New session needs to be created.
- Mobility support on top of IP was added later as an add-on feature.
  - ➡ Mobile IPv4 (MIPv4) is IETF’s main approach for mobility support for IPv4.
  - ➡ IPv6 has been designed to enable faster deployment of Mobile IPv6 (MIPv6).
  - ➡ Neither of these schemes have been deployed widely.
- Cellular networks are the biggest commercially deployed IP networks supporting IP mobility.
  - ➡ GTP is by far the mostly widely deployed mobility protocol for IP
  - ➡ PMIPv6 is the second most widely deployed mobility protocol for IP (used in Japan by NTT DOCOMO and also in 3GPP2 network by KDDI).
- GTP/PMIP or MIPv4 and MIPv6 require expensive network equipment (PGW, SGW) and hence are not very extensible to the entire Internet.
- Creating a light-weight mobility support protocol that can be widely deployed in the internet is still an open problem.

Identifier-Locator Separation (ILS) Protocols

Identifier Locator Network Protocol (ILNP)

- ILNP has been recommended by the Internet Research Task Force (IRTF) to be standardized in IETF (RFC6115, 2011).

- The primary goal of ILNP is to reduce the size of routing tables in the internet, which is driven by ISPs multi-homing onto the internet and injecting duplicate (specific) routes on the multi-homed interfaces.
  - Specific (i.e routes with higher number of prefix bits) are injected to try to influence on which of the multi-homed interface traffic from the internet ingresses into the ISP.

- While solving the routing problem, ILNP also solves the mobility problem.

ILNP: Naming

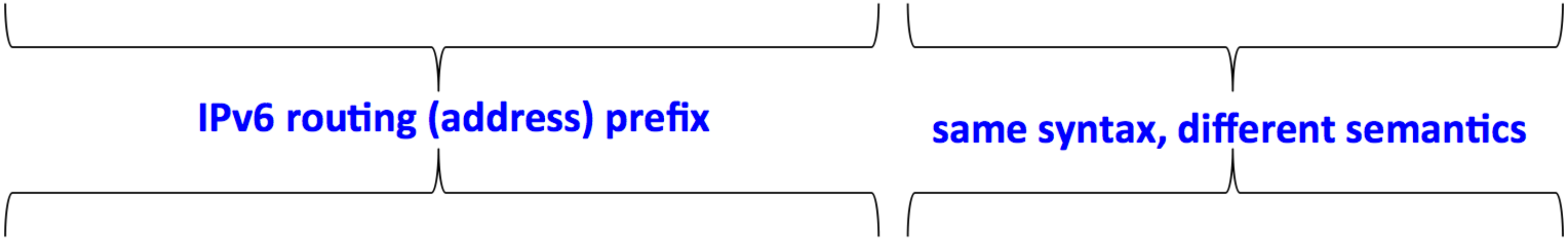
Protocol	IP	ILNP
Application	FQDN or **IP address**	FQDN
Transport	**IP address** (+ port number)	**Identifier** (+ port number)
Network	**IP address**	**Locator**
(interface)	**IP address**	(dynamic mapping)

Entanglement ☹ **Separation ☺**

IPv6 Addresses and ILNPv6

IPv6 (as in RFC3587):

```
| 3 |     45 bits         |   16 bits  |        64 bits              |
+---+---------------------+-----------+-----------------------------+
|001|global routing prefix| subnet ID |    Interface Identifier     |
+---+---------------------+-----------+-----------------------------+
```



IPv6 routing (address) prefix

same syntax, different semantics

ILNPv6:

```
|             64 bits                 |        64 bits              |
+---+---------------------+-----------+-----------------------------+
|             Locator                 |       Node Identifier       |
+---+---------------------+-----------+-----------------------------+
```

same syntax and semantics as
IPv6 routing (address) prefix
so IPv6 core routers work as today

these bits only examined and
acted upon by end systems

ILNPv6 Identifier and Locator [1]

- Locator, L:
  - ➡ Topologically significant.
  - ➡ **Names a (sub)network** (as today's network prefix).
  - ➡ •Used only for routing and forwarding in the core.
- Identifier, I:
  - ➡ Is not topologically significant.
  - ➡ Names a logical/virtual/physical node, **does not name an interface**
- Upper layer protocols bind only to Identifier.

Locator and Identifier [2]

- Locator, L:
  - ➡ Can change value during the lifetime of a transport session (mobility, site-controlled traffic engineering).
  - ➡ Multiple Locators can be used simultaneously (multi- homing, multi-path transport protocols).
- Identifier, I:
  - ➡ Remains constant during the lifetime of a transport session (localised addressing, IPsec.).
  - ➡ Multiple Identifiers can be used simultaneously by a node, but not for the same session.

Mapping FQDN to I/L Values

- DNS is used as today:
  - ➡ FQDN is used to map to I/L values instead of AAA
- Need new DNS Resource Records, e.g.:
  - ➡ I64 – 64-bit Identifier value,
  - ➡ L64 – 64-bit Locator value
  - ➡ LP – Locator Pointer (like CNAME for L64)
- DNS lookup will return:
  - ➡ 1 or more I64 records, 1 or more L64 records
  - ➡ For multiple I64 and L64 RRs, use preference bits

ILNP Mobility Support

- The two functions to be considered in mobility:
  - ➡ Rendezvous, to permit incoming connections to a mobile host
    - ➡ Rendezvous is provided by querying DNS to obtain the MN’s latest location.
  - ➡ Handoff to allow a mobile host to maintain communication sessions that are active during location changes.
    - ➡ Handoff is supported by each node sending a location update directly to the other host. The MN also updates the DNS record.