2G1305 Internetworking/Internetteknik
Spring 2005, Period 4

Module 11: Mobile IP

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with *TCP/IP Protocol Suite*, by Behrouz A. Forouzan, 3rd Edition, McGraw-Hill.

For this lecture: Chapter 24

Last modified: 2005.05.14:18:20

maguire@it.kth.se

Outline

- Mobile IP

Emerging Network Architecture

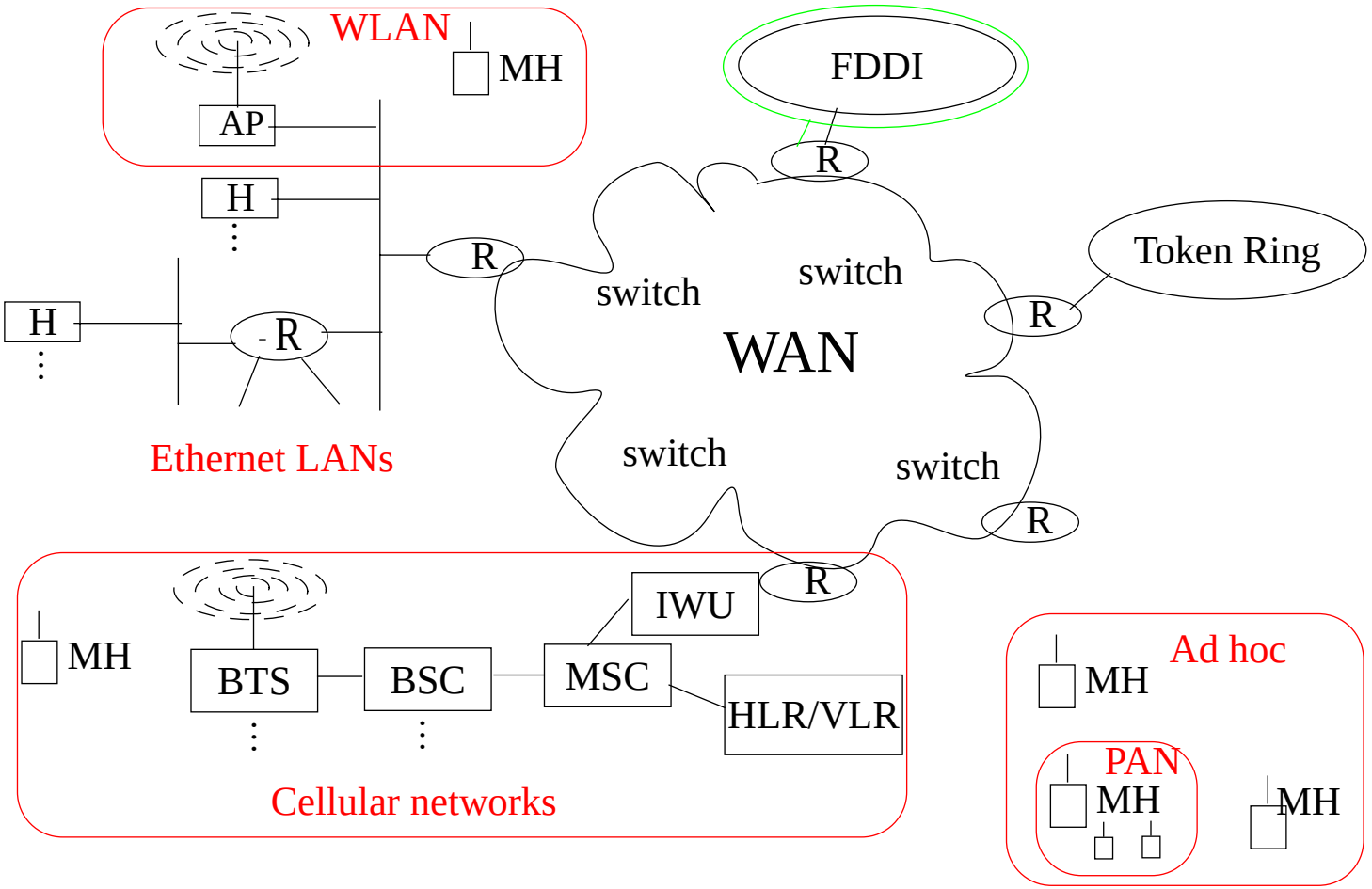


Figure 93: Mobility (WWAN, WLAN, PAN, …) driving us towards Mobile Internet

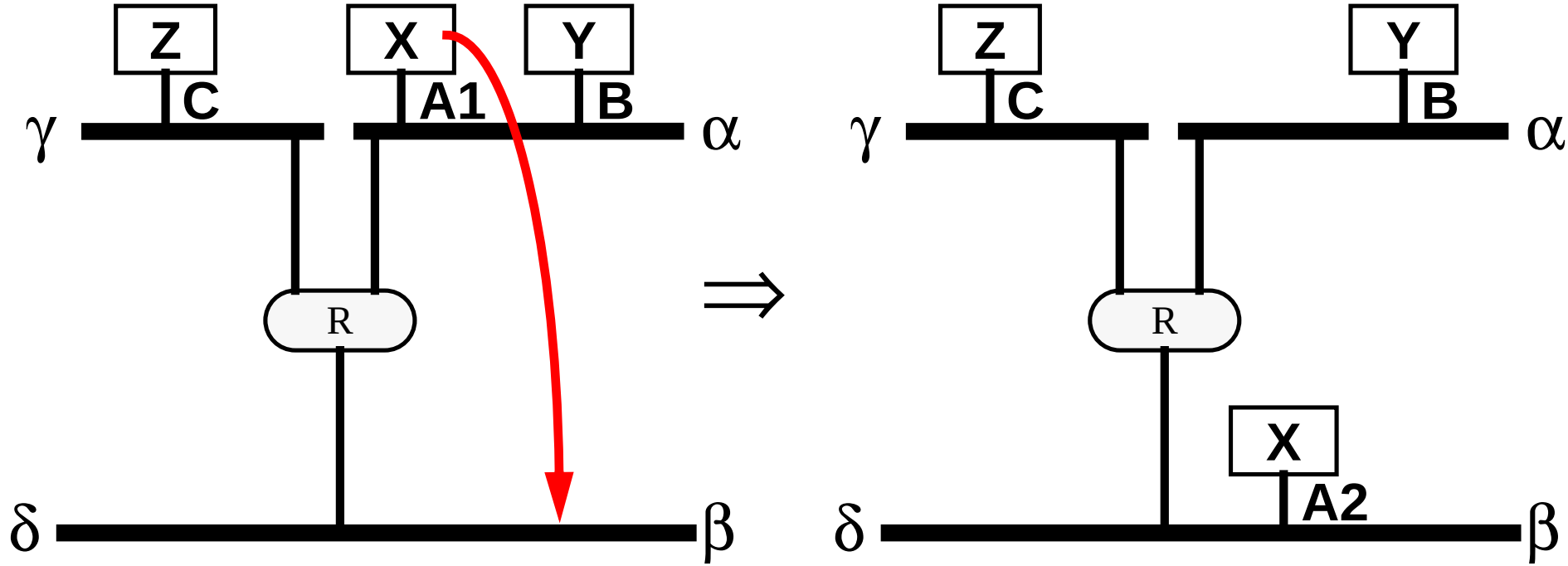


Figure 94. X disconnects from location A1 and reconnects at location A2

What is "X"? X represents the identity (ID) of the node[1]

- in an Ethernet it might be the MAC address, thus a node has a constant identity

While A1, A2, … represent the network addresses of node X.

- IP network address consists of {Network, Host}, i.e., A1={α | n}, where n is unique on network α.

1. Of course this really mixes the interface ID with the node ID - solution is a Network Access Identifier[104].

Updating after a move

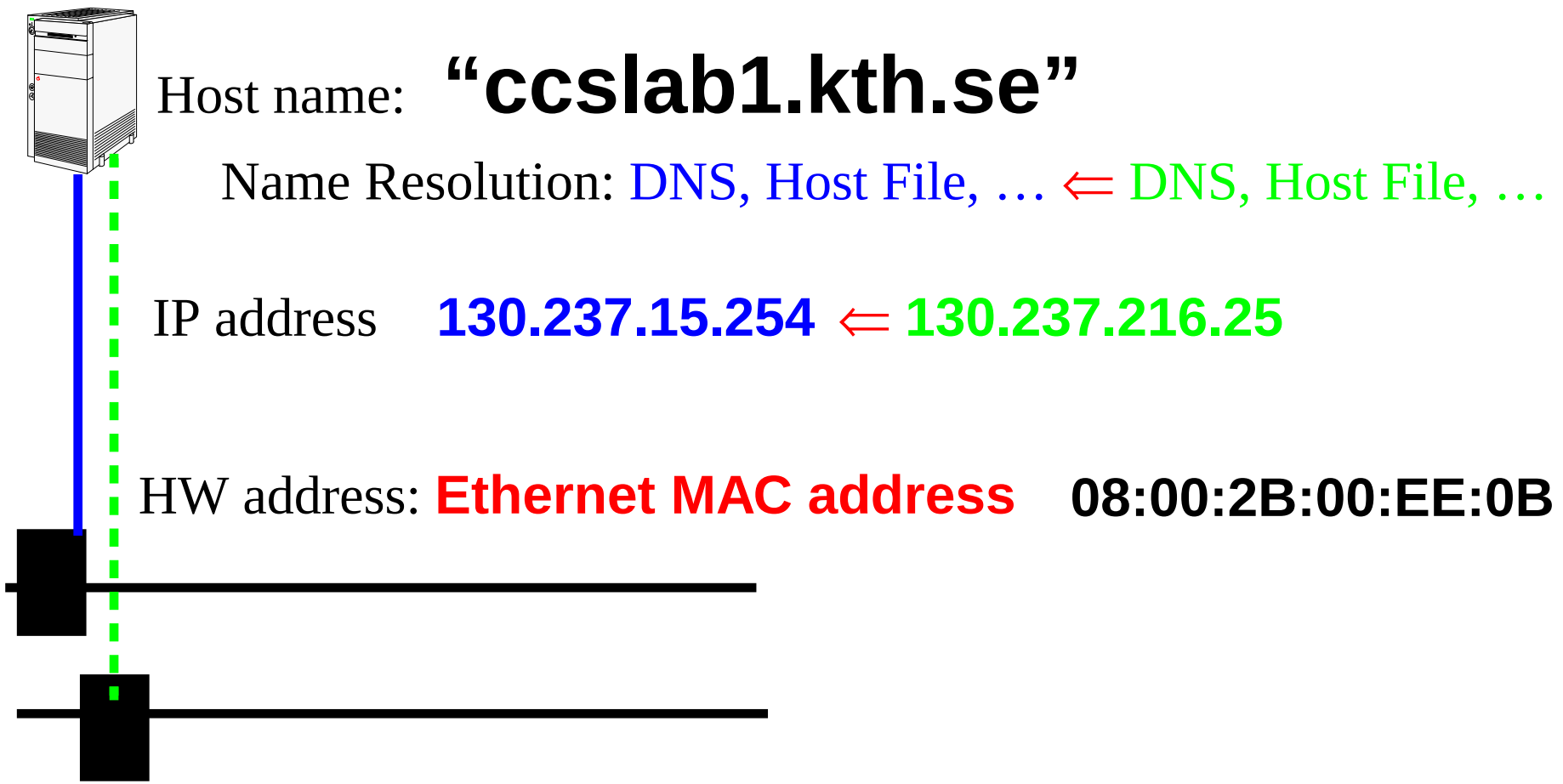


Figure 95: Must update IP address related mappings after a move ⇒ administrative nightmare

Objectives of Mobile IP

- To provide mobility support for the Internet
- To enable node mobility: across changes in IP subnet
- Allow change in location without change of IP address
- Communication should be possible (even) while moving (if the interface/link supports it)
- TCP/IP connections should survive movement
- Active TCP and UDP port bindings should be maintained

Communication from Z to X

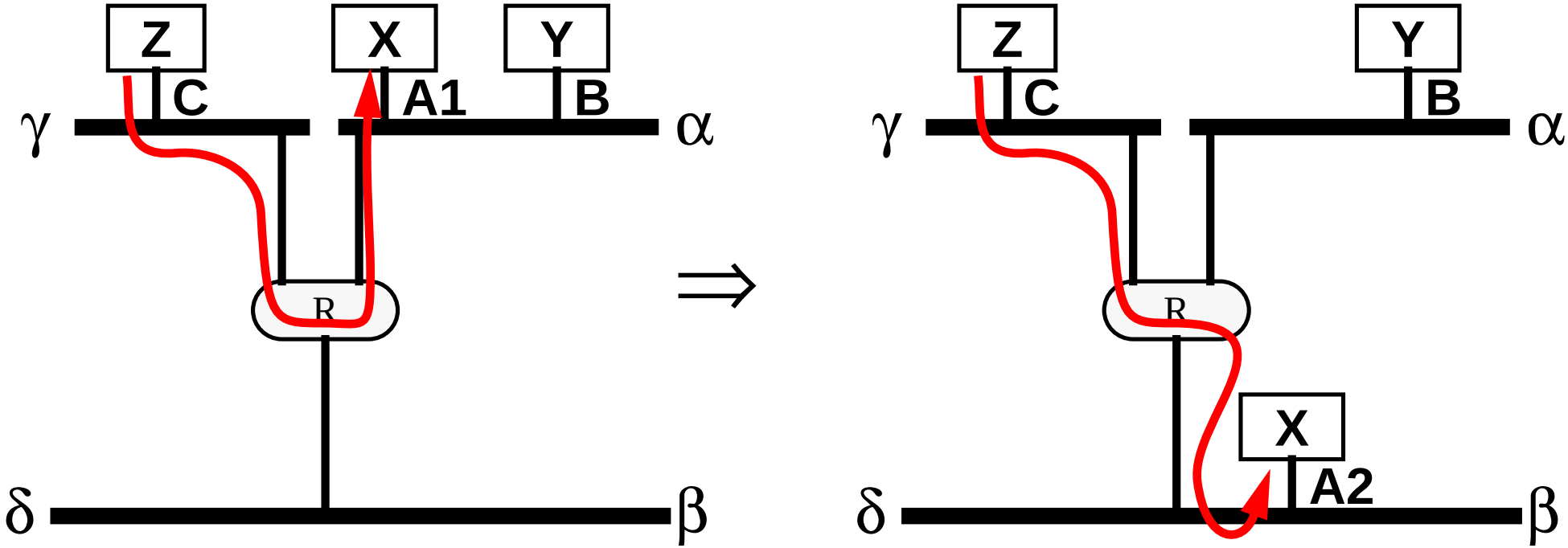


Figure 96. Z is communicating with X at A1 and wants to continue when X reconnects at location A2

- This would require that router R send packets from Z to X over a new path (route).
  - ✘ But X now has a new network address, since it is on a different network (β).

How can Z continue to communication to X?

1. Just use bridging and change the forwarding table in the bridge (since the bridge uses MAC addresses)
   - ✘ But bridging does **not** scale well
2. The application could stop, then restart with the new address for X
   - ✘ This is unpleasant for the user - since they might have to do this very frequently and/or the programs may not tolerate this change - since they have too much state.
3. We could hide this change with a new layer of software
   a. We could change the socket library
      - ✘ for example: we could do source routing - but, it turns out that this is not well supported by existing code in the OS[1] and in router (in addition, many the firewall routers at many sites filter out source routed packets!)
      - ✘ Would require changes in all systems (even the non-mobile systems - since both ends of the communication would have to change)

   b. We could remap the addresses in the router
      - ✘ This would means doing host specific routing, which does not scale well

   c. We could define a new Mobile-IP address
      - ✔ The implications of this will be described in the following material.

1. An informal experiment conduced by John Ioannidis as part of this Mobile*IP research (and documented in an appendix of his thesis) indicted that almost all operating systems, of the time, did not correctly support source routing!

Identification

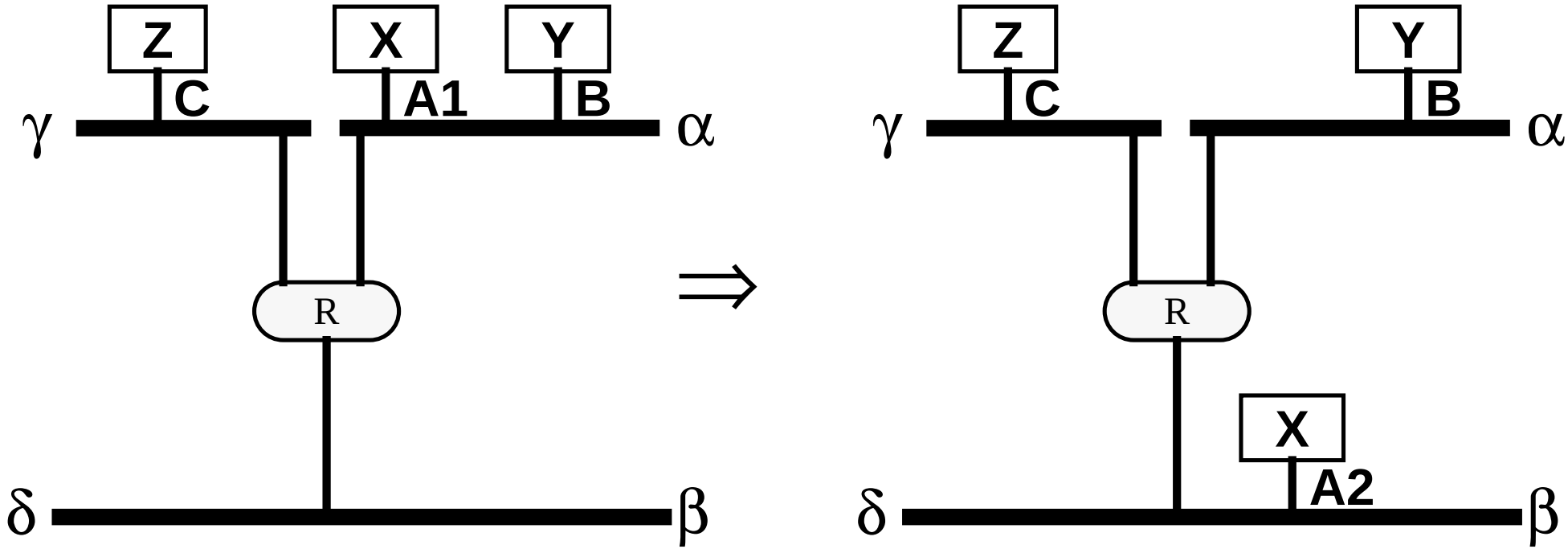


Figure 97. How do we know it is the same X?

When X moves to its new location (A2)

- Why should it get service?
- How do we know it is the same X? (Or even that it is X?)

Establishing Identity

When a node arrives on a network it must identify itself

- mechanism: typically via a challenge response protocol
- Who should it identify itself to? Answer: The MSR ≡ Mobility Support Router

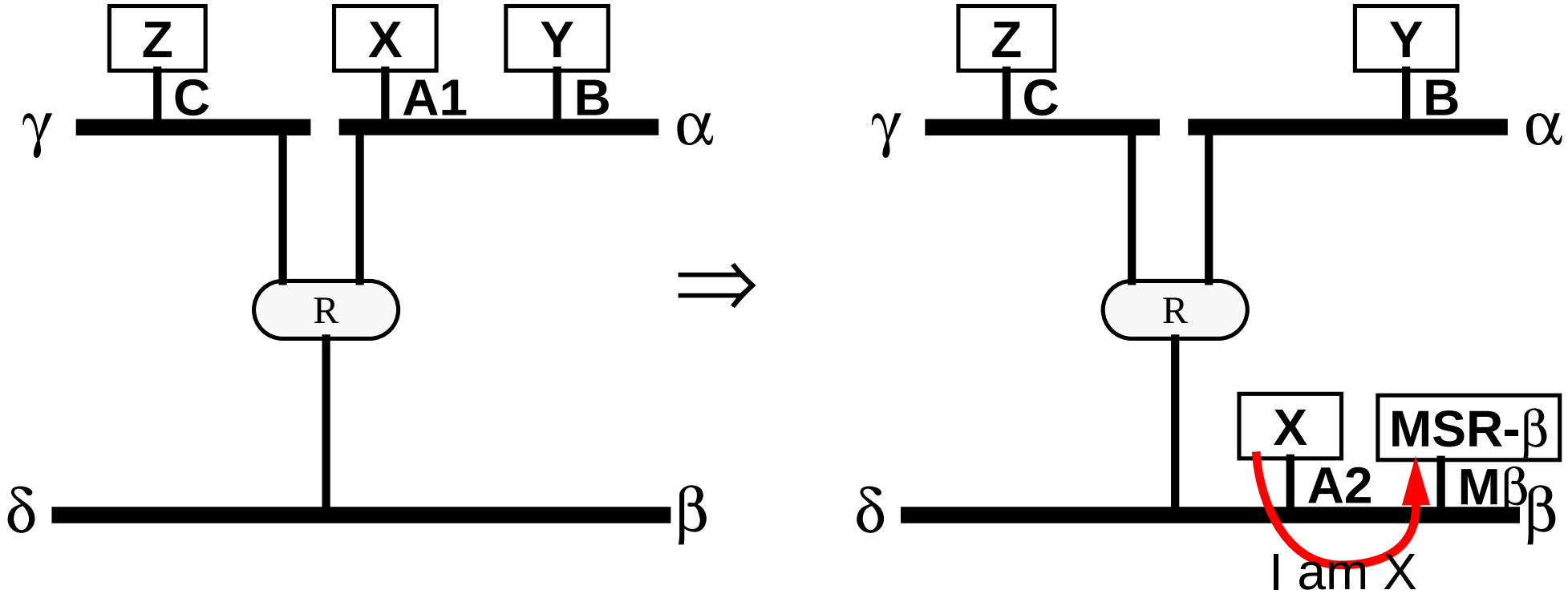


Figure 98. How do we know it is the same X?

How did it know to send the “I am” message to the MSR?

- **When a node arrives on a network it listens for broadcasts from MSRs**

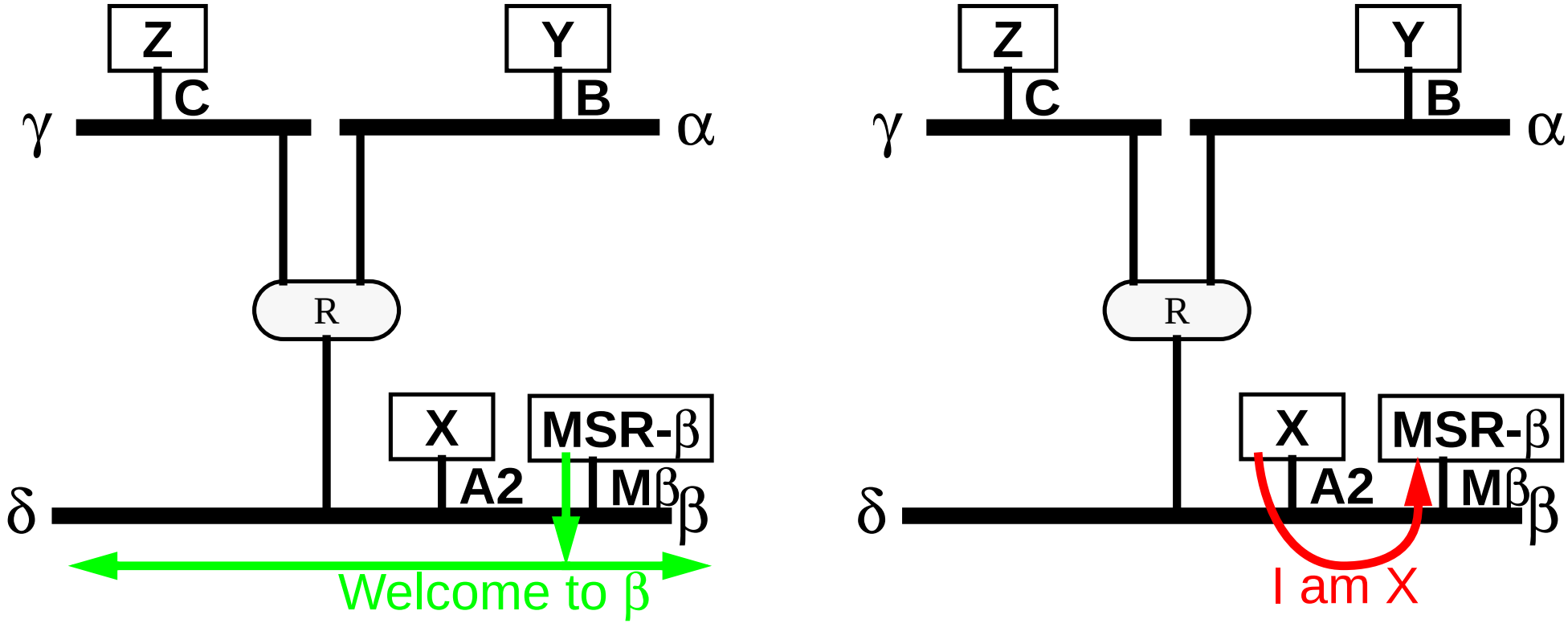


Figure 99. “Welcome (Greeting)” messages answered by “I am” messages

These broadcast “Welcome” messages advertise:

- the presence of an MSR (and its MAC address)
- advertise one or more networks it provides connectivity to

Could the MSR functionality be collocated with the router?

- **When a node arrives on a network it listens for broadcasts from MSRs**

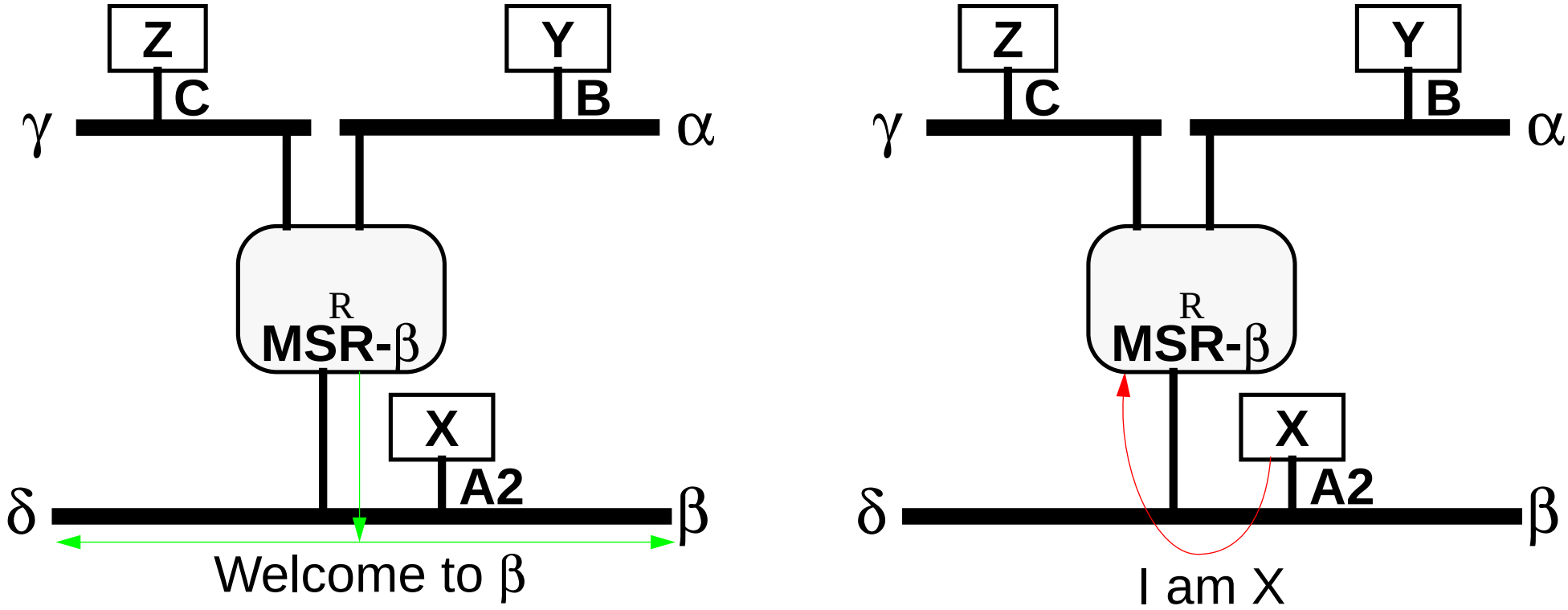


Figure 100. "Welcome (Greeting)" messages from router answered by "I am" messages

✘ Requires updating **all** of the routers on network segments which are going to support mobility to be updated.

Getting Service

Once it's identity is know, the policy question must be ask: Should X get service?

The policy question and its answer may involve:

- roaming agreements (generally reciprocal agreements),
- current traffic loads,
- anticipated traffic loads,
- mobile user's priority/class/… ,
- … .

The question of authentication, authorization, and accounting (AAA) for mobile users is addressed in [107].

See also IEEE 802.1x Port Based Network Access Control

http://www.ieee802.org/1/pages/802.1x.html

Back to the original problem: Z wants to send a message to X

Initially X is located at A1 then it moves to A2.

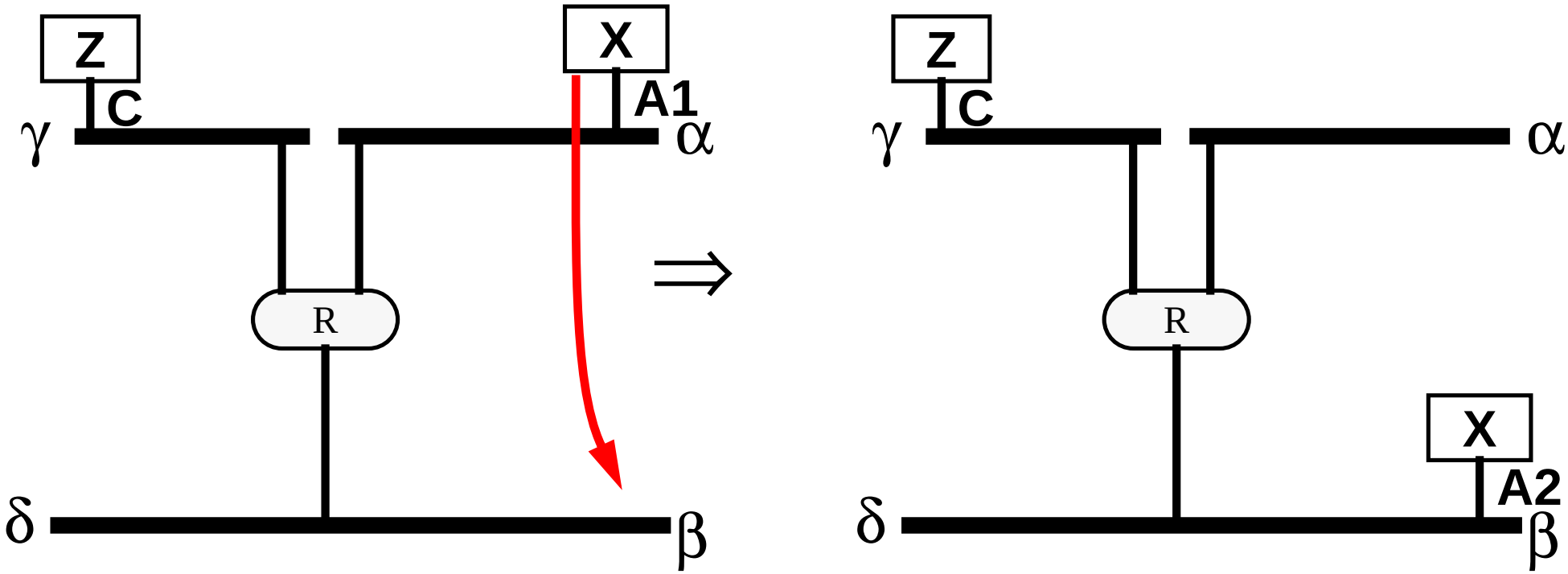


Figure 101. X moves from A1 to A2, Z not aware of Mobility

There are several alternatives.

Alternative 1

Initially X is located at A1 then it moves to A2.

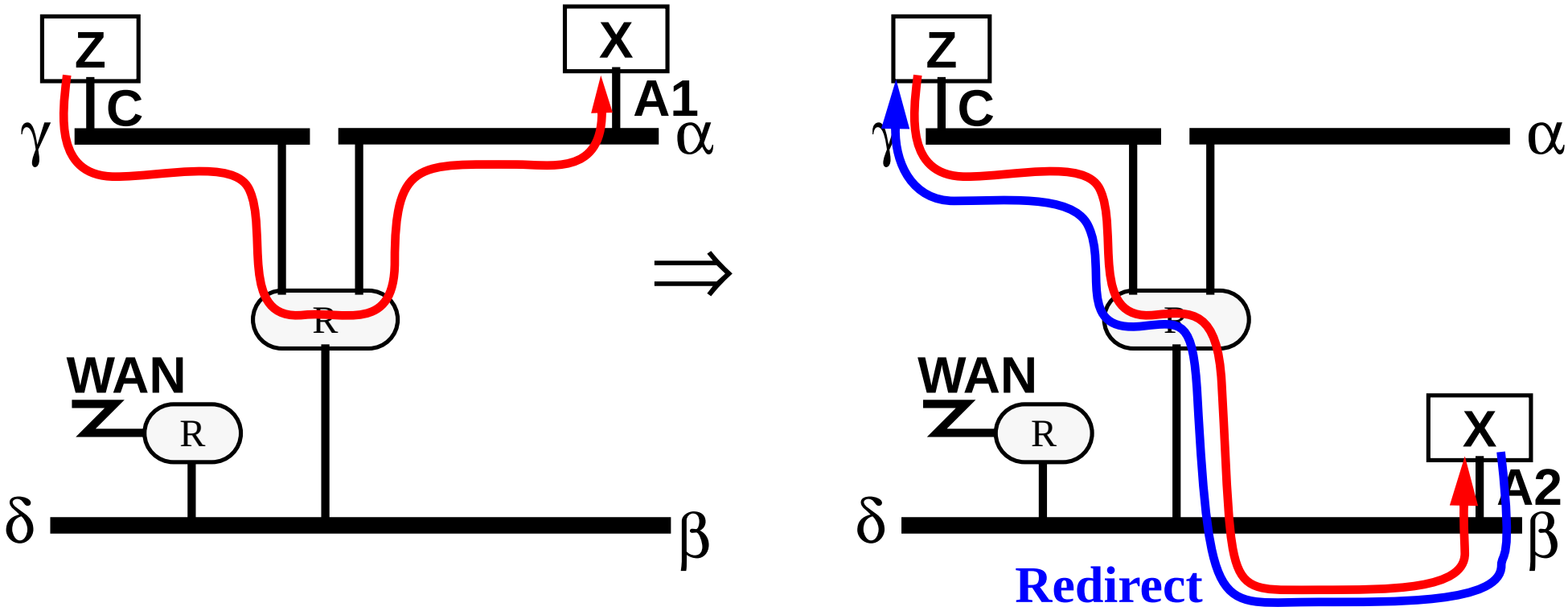


Figure 102. X must send a redirect message to Z, to tell it it's new address A2.

- ✘ Z must be aware of where X currently is.
- ✘ X must get a new local address A2 (How? perhaps DHCP)

Alternative 2

Initially X is located at A1 then it moves to A2.

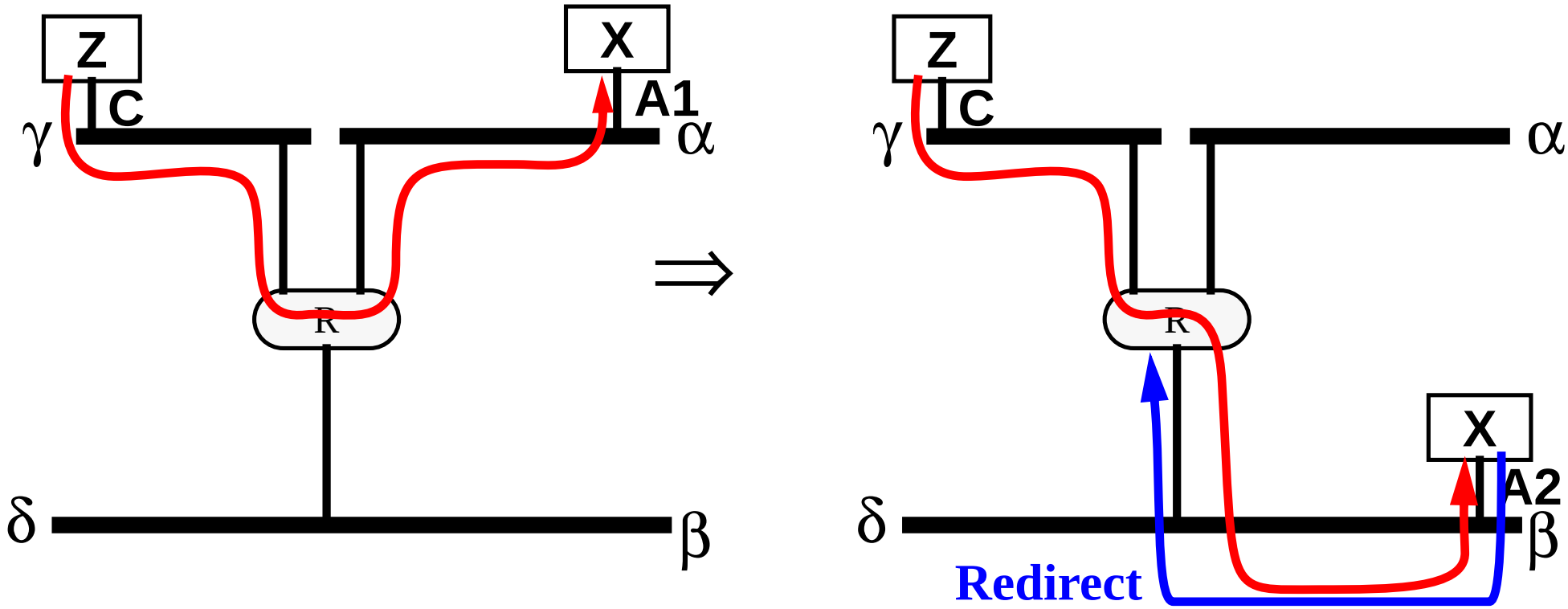


Figure 103. X must send a redirect message to the **Router**, to tell it it's new address A2 (rather than A1).

- ✘ Router must now perform host specific routing.
- ✘ X must get a new local address A2 (How? perhaps DHCP)

Alternative 3

Initially X is located at A1 then it moves to A2.

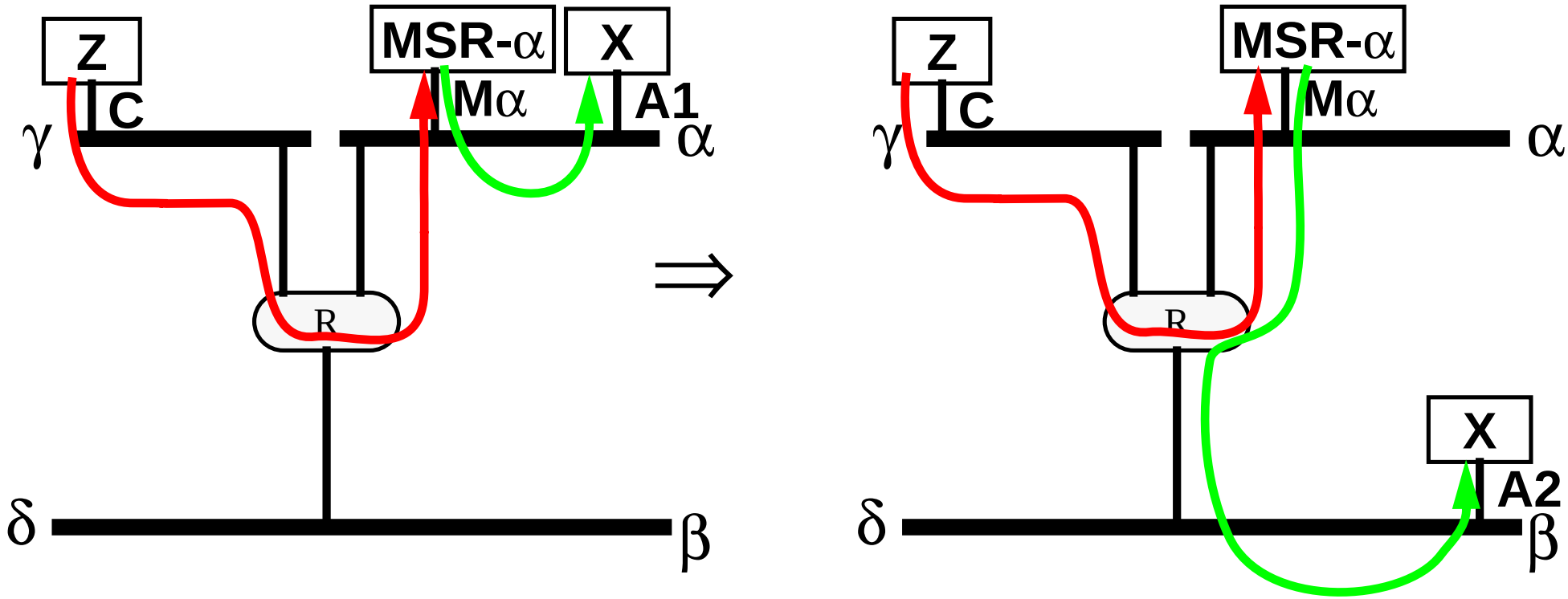


Figure 104. X must send a redirect message to a Mobility Support Router (**MSR-α**), to tell it it's new address A2 (rather than A1).

- ✘ **MSR-α** must now perform host specific routing.
- ✘ X must get a new local address A2 (How? perhaps DHCP)
- ✔ Z is now completely unaware of the move.
- ✔ Router R is now completely unaware of the move (except for twice the traffic over the link to/from α).

Alternative 4

Initially X is located at A1 then it moves to A2.

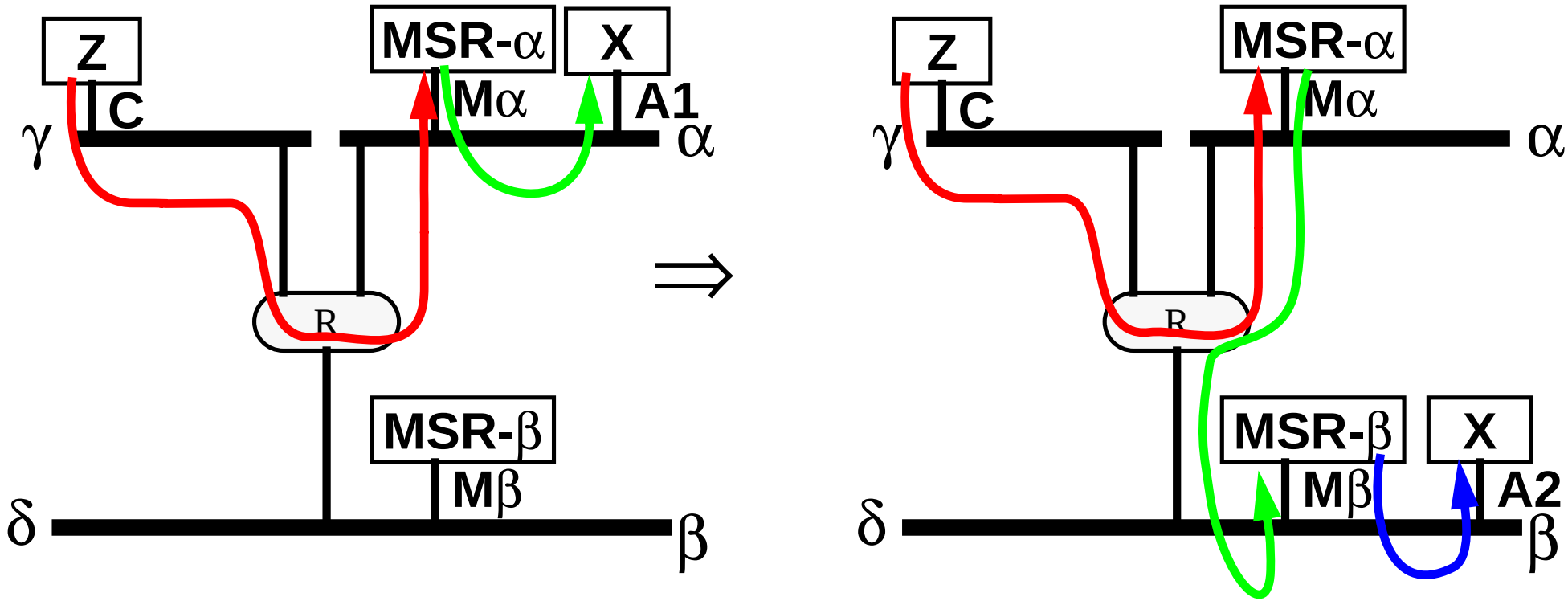


Figure 105. X sends a message to **MSR-β**, to get it's new address A2 and says it's old MSR was **MSR-α**.

- ✘ **MSR-α** must now perform host specific routing to **MSR-β** (which can provide the local address A2)
- ✔ Z is now completely unaware of the move - it always sends traffic to **MSR-α**.
- ✔ If X moves again, Z does not change where it sends traffic to & traffic need not go via **MSR-β** - it will go directly from **MSR-α** to the MSR responsible for the new segment.

Alternative 4 continued

Initially X is located at A1 then it moves to A2 and then moves to A3.

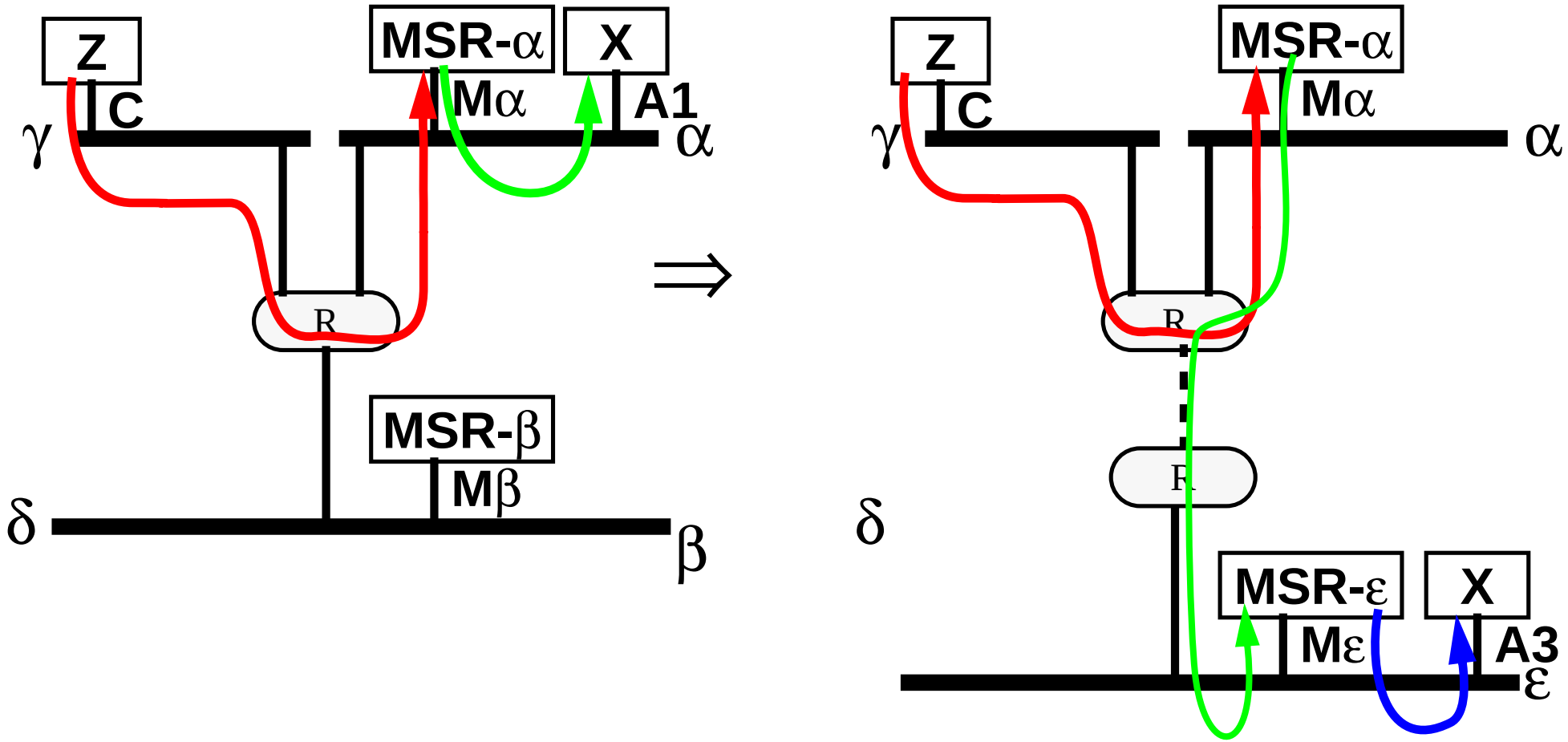


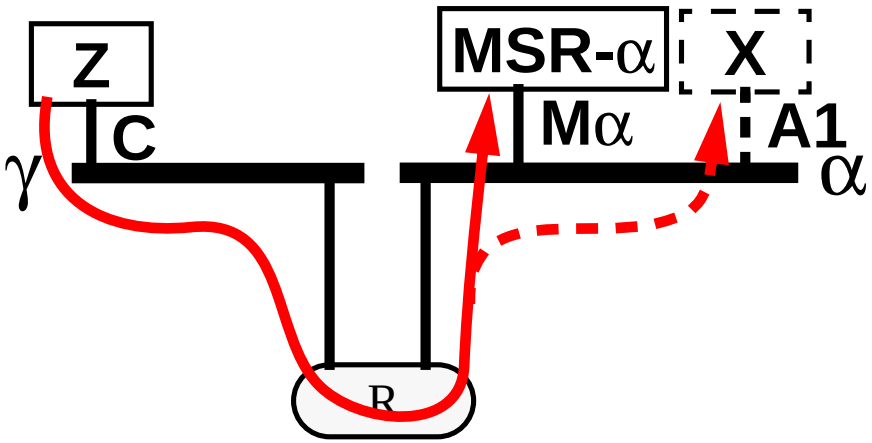
Figure 106. X sends a message to **MSR**-ε, to get it's new address A3 and says it's old MSR was **MSR**-α.

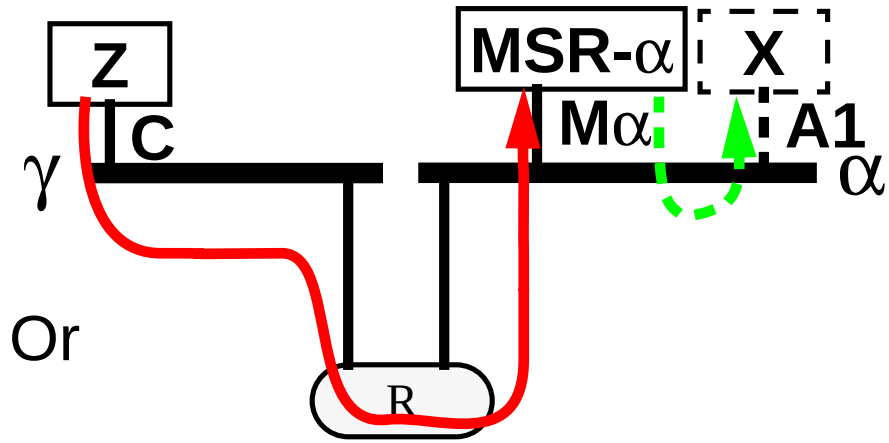
- ✔ The traffic from **MSR**-α to **MSR**-β or **MSR**-α to **MSR**-ε can be encapsulated, using for example IP in IP (written IP-IP) encapsulation. Thus none of the intervening routers needs know about mobility.

How does Z know to send things to MSR-α?

It does **not** know to do this! ⇒ Z simply sends the packet to the network address of X.

But what is the (real) network address of X?.





- X's address is A1
- A1 is an address on network α
- MSA-α intercepts packets addressed to A1 and forwards them if X is not currently present on the network α

- X's address is {Mobile-Network,X}
- A1 is a temporary address on network α
- MSA-α routes {Mobile-Network,X} packets to **A1**when X is **local** and to another **MSR** when it is **non-local**

Figure 107. X's address - either on either an actual network or on a virtual network

✔ In the first case ("actual" network addresses), either the hosts and routers have to be changed, or MSRs are necessary to intercept and reroute the packets.

✔ In the virtual network case, we use the MSRs to implement mobility for nodes on a virtual mobile network.

What happens in the case of wireless networks?

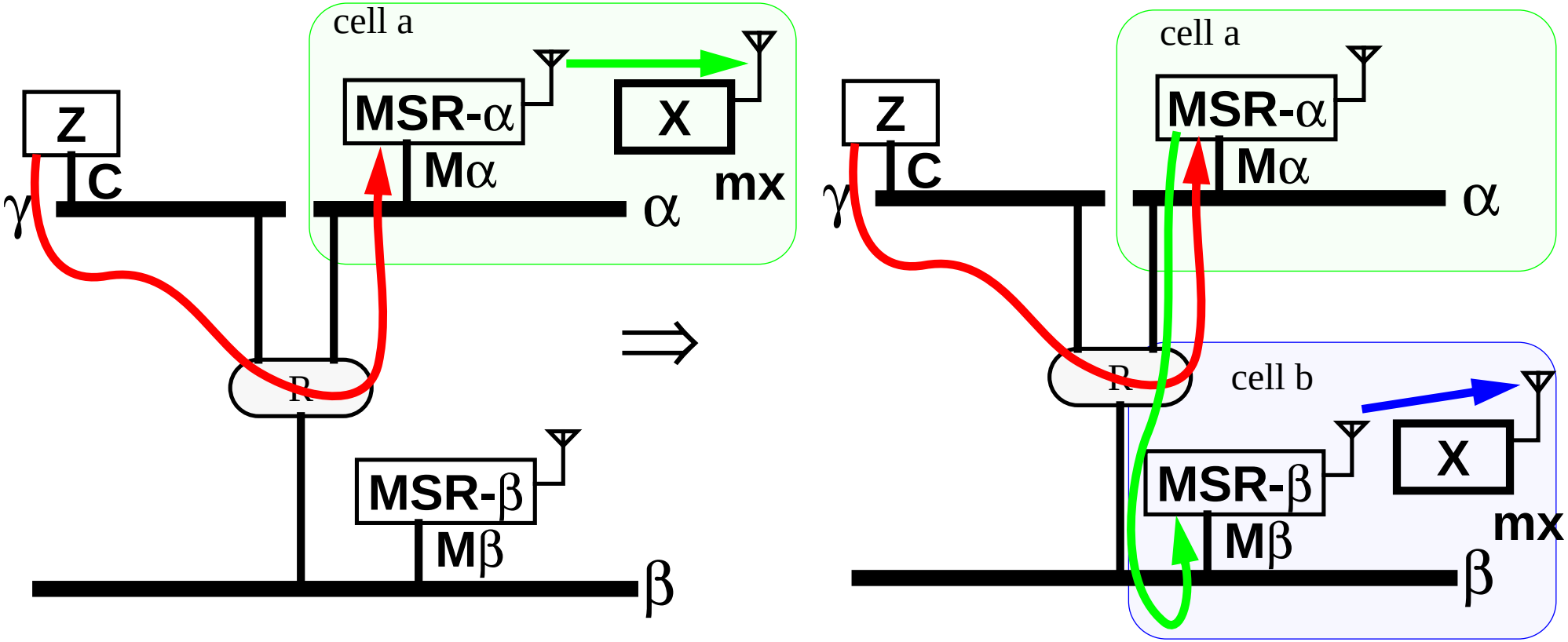


Figure 108. X moves from the cell a to the cell b

- The wireless cells are implemented by a basestation co-located with the MSR.
- Note that X retains it's mobile network address "mx".

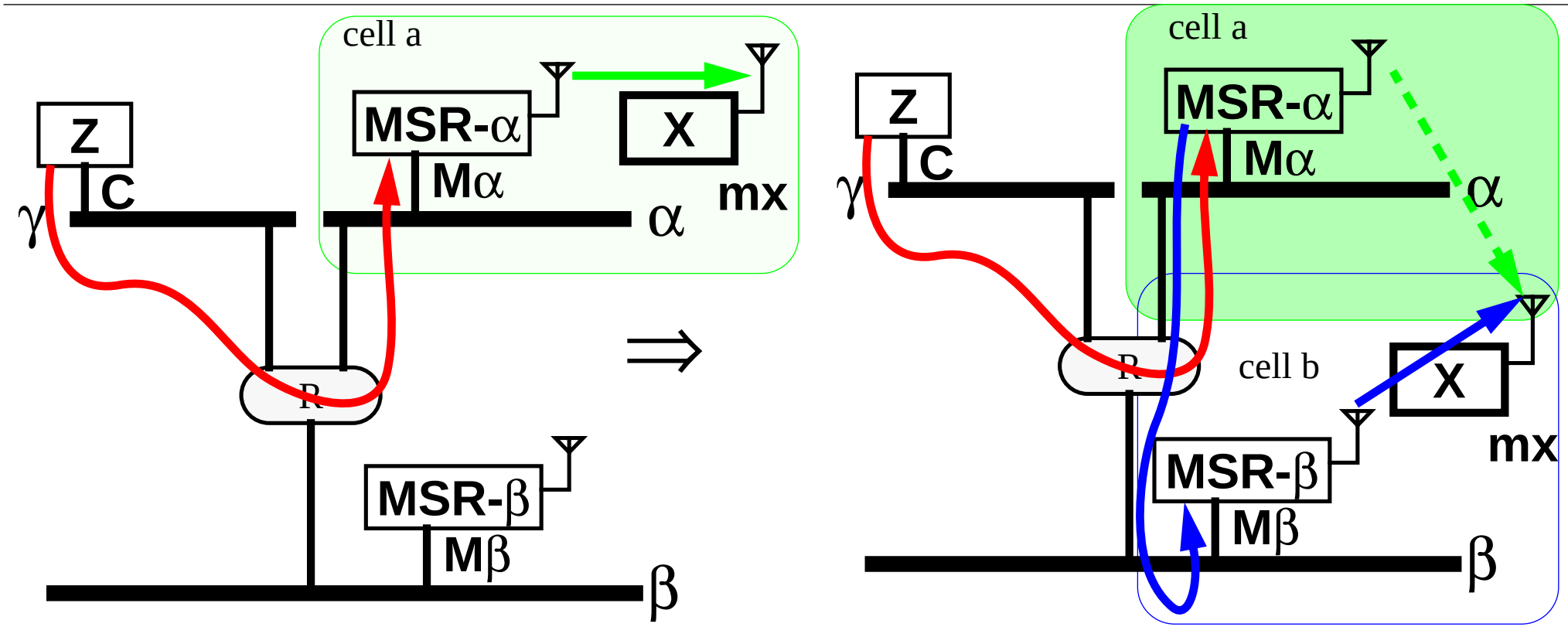


Figure 109. X moves from the cell a to the cell b, but is still reachable by cell a!

- Mobile network address "mx" is reachable from both MSR-α and MSR-β.
- This could not occur in the wired case (unless there were multiple interfaces), since X would have to disconnect from network α to connect to network β.
- If the cell size is small the movement between cells could be frequent (and caused by other events, such as a new user, a door moving, …).

Wireless WANs

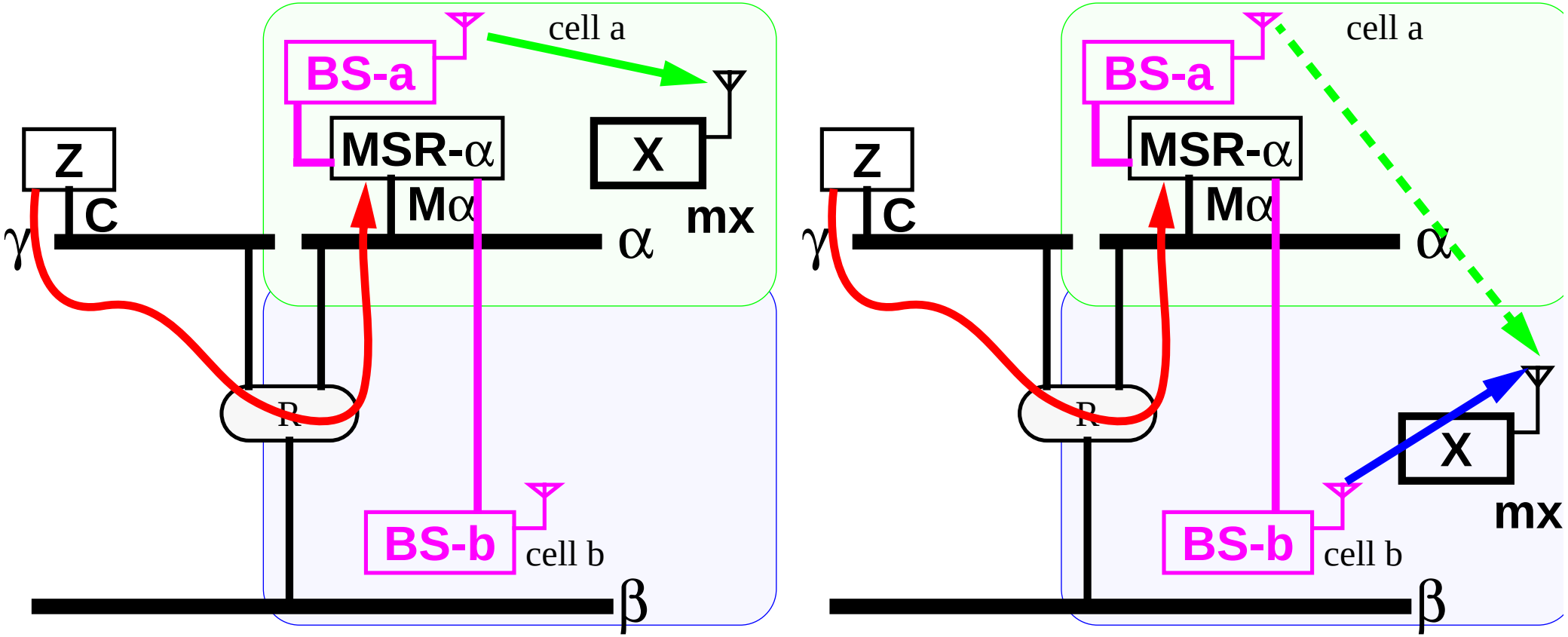


Figure 110. X moves from the cell a to the cell b, but may still reachable by cell a - but both cells are part of the same network

- Basestation-a, basestation-b, … are all part of the same network and it is up to this network to select which cell a mobile is in and which basestation will be used to communicate with it.

Simulcasting in Wireless Local Area Networks (WLANs)

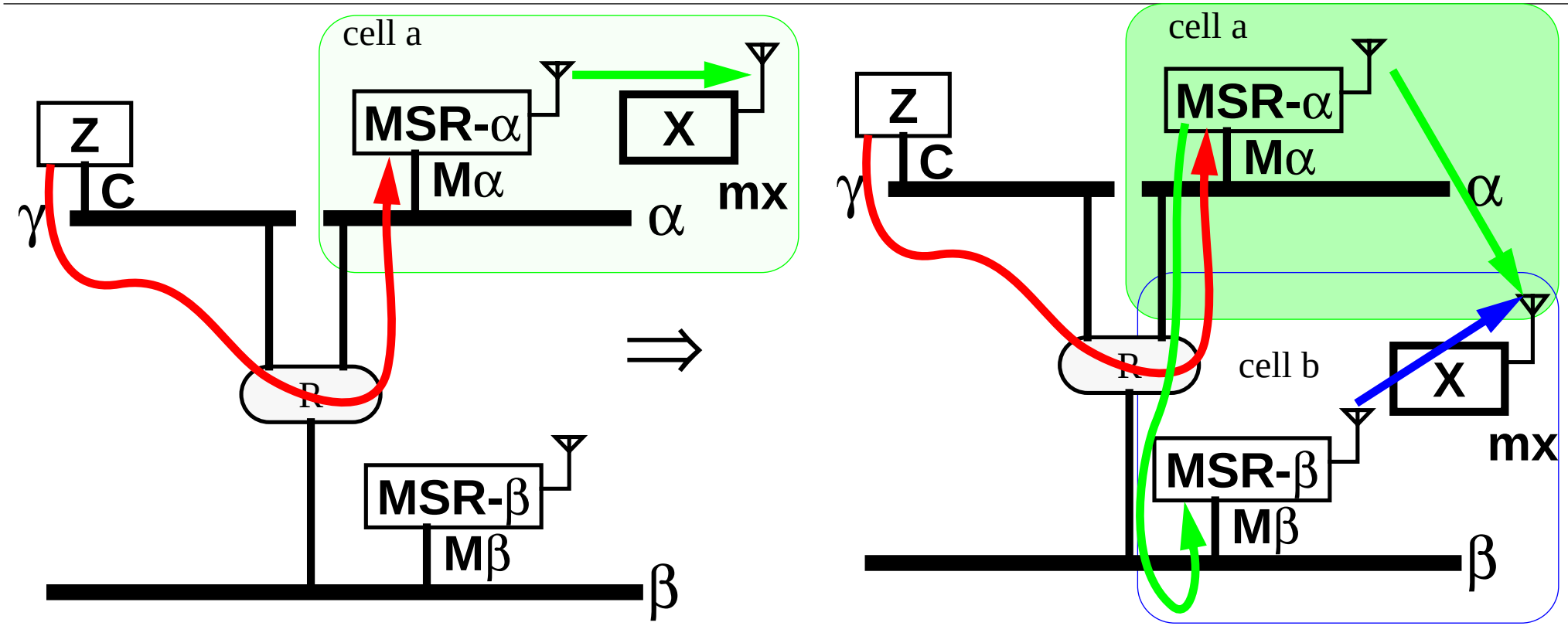


Figure 111. X is moving from the cell a to the cell b

- Mobile network address "mx" is partially reachable from both MSR-α and MSR-β - thus we will send packets via both MSR-α and MSR-β. This insures:
  - ✔ Lower probability of packet loss (important if we must provide low latency and high reliability - such as is needed for voice and some other services)
  - ✘ increases traffic in both cells

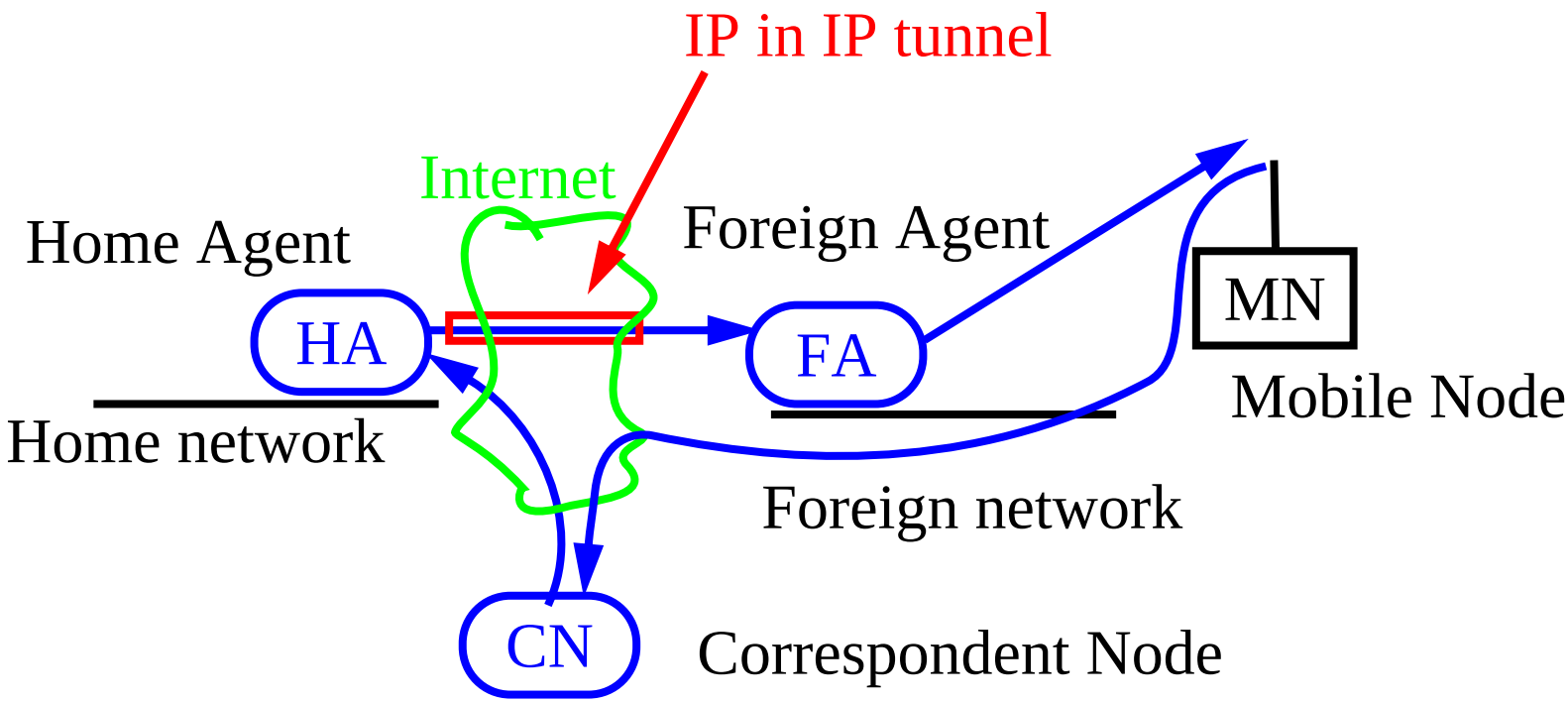
Mobile IP Standardization Effort

- Originally proposed by Columbia University, IBM, etc.
- Internet Engineering Task Force (IETF) Mobile-IP working group
  - *http://www.ietf.org/html.charters/mobileip-charter.html*

Mobile-IP standard status:

- RFCs:
  - Mobile-IPv4 (RFC 2002) IP Mobility Support; RFC 2003: IP Encapsulation within IP; RFC 2004, RFC 2005, RFC 2006, etc.
  - Mobile-IPv6
- Many Drafts related to v4 & v6:
  - Mobile IP NAI Extension, AAA Registration Keys for MIP, Registration Keys for Route Optimization, Mobile IP Challenge/Response Extensions, CDMA2000 Extension to MIP, Cellular IP, Regional Tunnel Management, Hierarchical MIP Handoffs, etc.

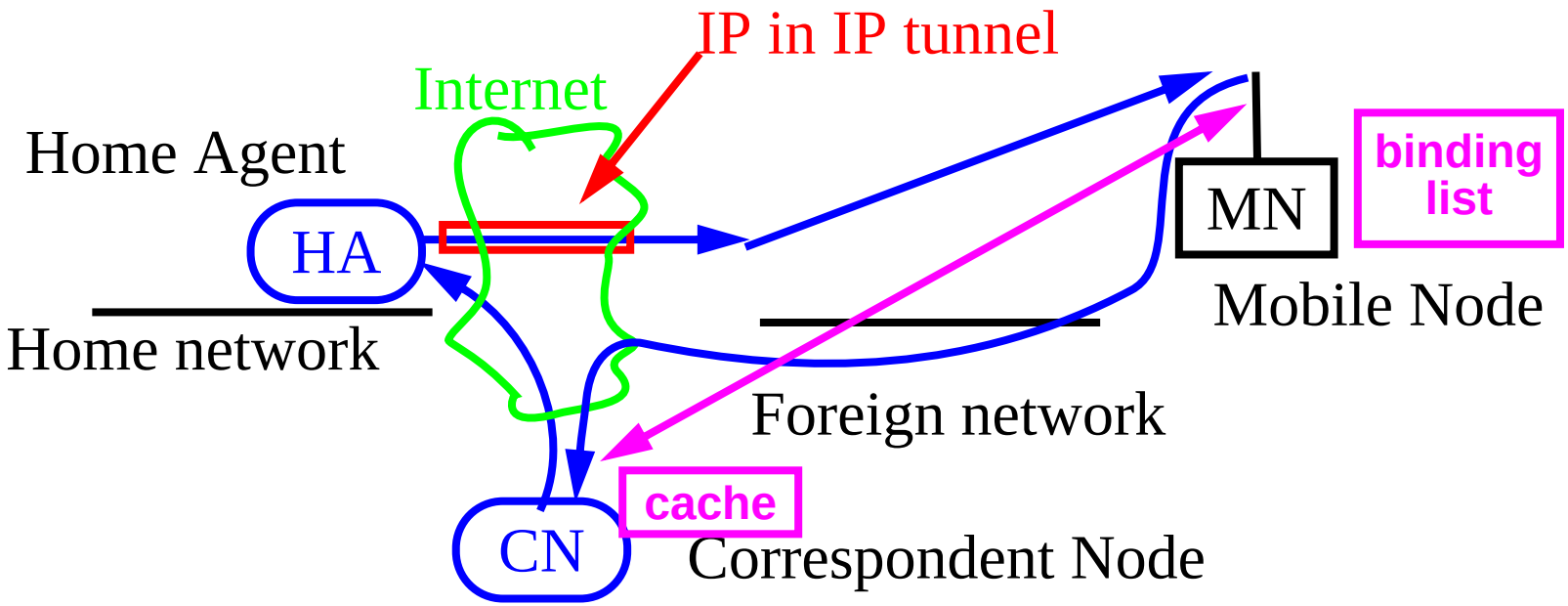
A Mobile-IP(V4) Scenario



CN sends packet to MN's home network (because that is where its IP address is logically located), HA intercepts them and forwards them inside an IP-in-IP tunnel to the Care of Address (CoA) where the FA forwards them to the MN.

Traffic from the MN can go directly to the CN (**unless** there is ingress filtering) ⇒ triangle routing

A Mobile-IP(V6) Scenario



CN sends packet to MN's home network (because that is where its IP address is logically located), HA intercepts them and forwards them inside an IP-in-IP tunnel to the Care of Address (CoA) which is the MN's address in the foreign network.

However, the MN can tell the CNabout its **current** address via a binding update (BU), now traffic can flow both ways directly between the CN and MN.

IP-in-IP Encapsulation

In-in-IP vs. Minimal encapsulation - the major difference is the first puts the whole IP packet inside another, while the later tries to only put a minimal header inside along with the original data portion of the IP packet.

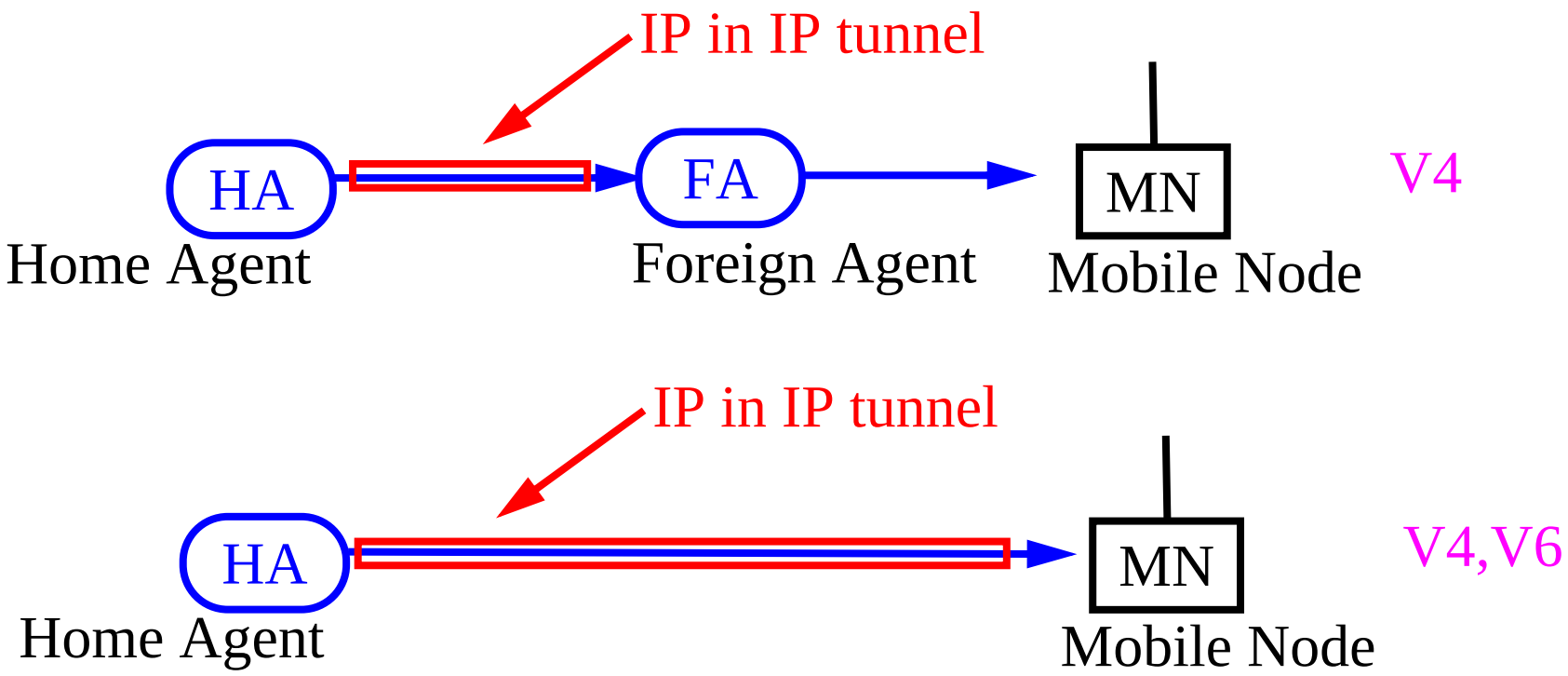
For details see

- IP Encapsulation within IP, RFC 2003 [105]
- Minimal Encapsulation within, IP RFC 2004 [106]

Tunneling IP Datagrams

Both home agents and foreign agents (v4) must support tunneling datagrams using IP-in-IP encapsulation and decapsulation.

MNs that use a co-located COA must also support decapsulation (v6).



Temporary Address Assignment

Two types of temporary Care-Of-Address:

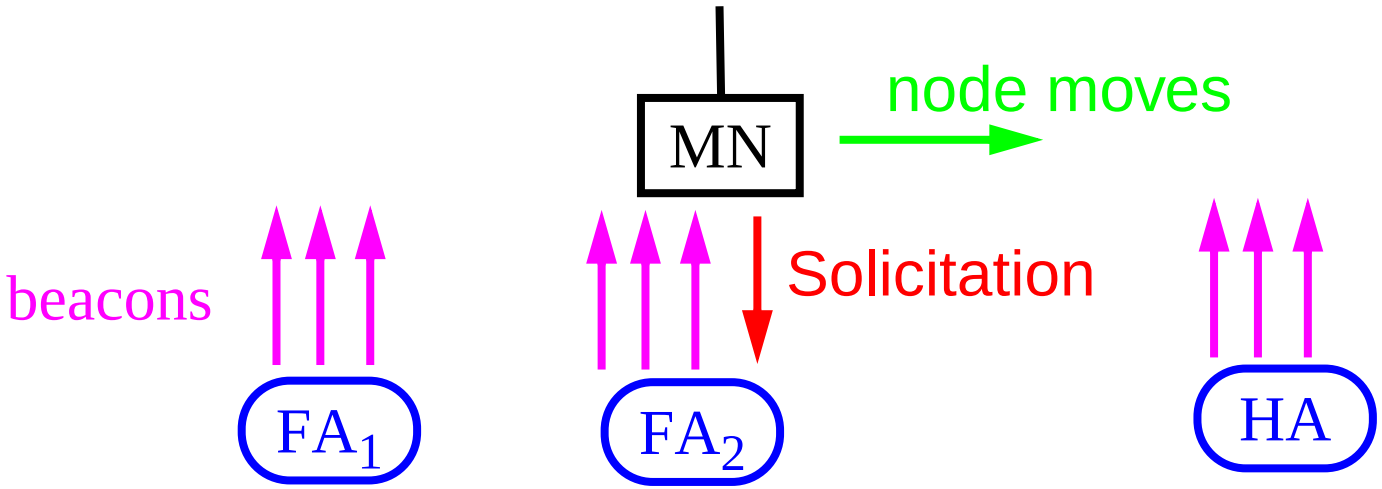
- Foreign agent care-of address (V4)
  - a care-of address provided by a foreign agent through its Agent Advertisement messages.
- Co-located care-of address (V4, V6)
  - a care-of address acquired by the mobile node as a local IP address through some external means, eg. dynamically acquired as a temporary address through dynamic host configuration protocol (DHCP) RFC 1541, or the address may be owned by the MN as a long-term address for its use while visiting this foreign network.

Agent Discovery

Why Agent Discovery?

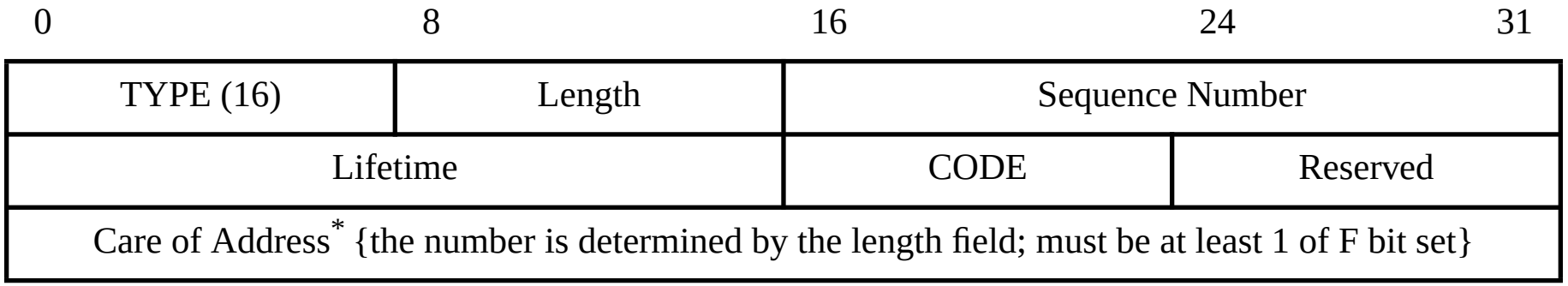
Methods an MN can use to determine whether it is currently at its home network or a foreign network. By:

- Agent Advertisement
  - periodic transmissions (beacons) sent by a mobility agent (rate limited to max. 1/s).
- Agent Solicitation
  - Send by an MN to discover agents.



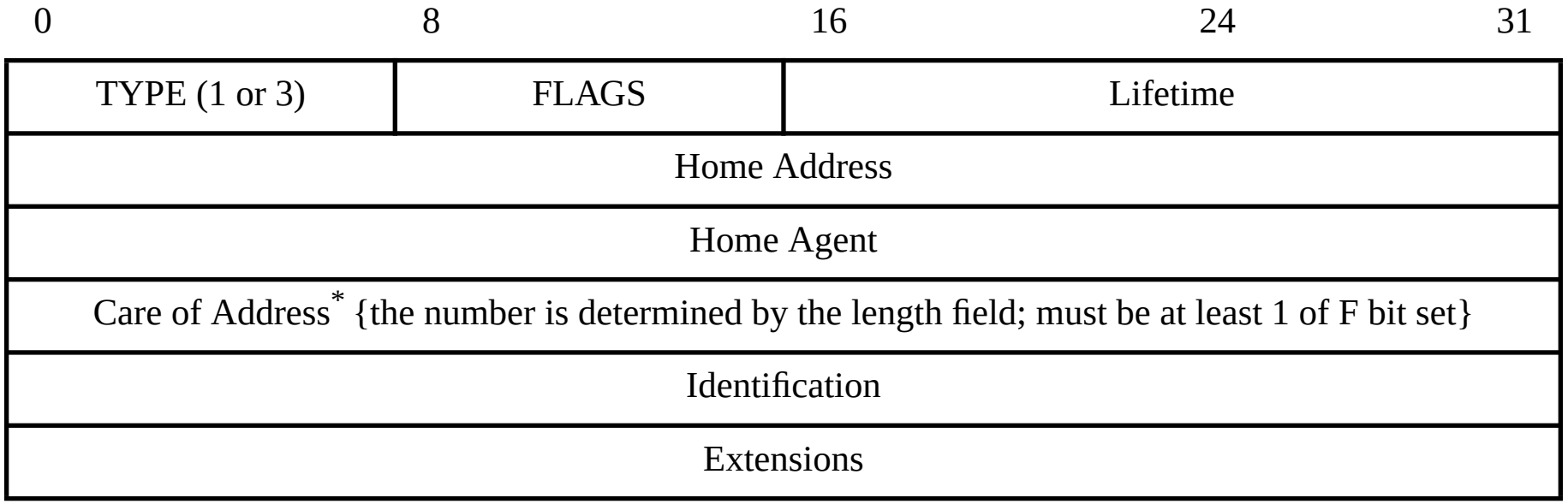
Agent Advertisement Message Format

Extension of an ICMP router advertisement



Bit	Name	Meaning
0	R	Registration with this foreign agent (or another foreign agent on this link) is required; using a co-located care-of address is not permitted.
1	B	Busy. Foreign agent not accepting registrations from additional mobile nodes.
2	H	Agent offers service as a home agent.
3	F	Agent offers service as a foreign agent.
4	M	Agent implements receiving tunneled datagrams that use minimal encapsulation
5	G	Agent implements receiving tunneled datagrams that use GRE encapsulation
6	V	Agent supports Van Jacobson header compression over the link with any registered mobile node.
7		reserved (must be zero)

Registration Message Format



Bit	Name	Meaning
0	S	Simultaneous bindings, this is an additional address for the mobile
1	B	Broadcast datagrams. Home agent to tunnel any broadcast packets it receives to the mobile.
2	D	Mobile using co-located care-of address and will decapsulation itself
3	M	Mobile requests home agent to use Minimal encapsulation.
4	G	Mobile requests home agent to use GRE encapsulation.
5	V	Mobile node requests that agent use Van Jacobson header compression.
6-7		reserved (must be zero)

MN Requirements

An MN must have:

- home address, netmask,
- mobility security association for each HA.

For each pending registration, MN maintains the following information:

- link-layer address of the FA to which the Registration Request was sent
- IP destination address of the Registration Request
- Care-of address used in the registration
- remaining lifetime of the registration

FA Requirements (v4)

- Each FA must be configured with a **care-of-address**.
- Must maintain a **visitor list** with following information:
  - Link-layer source address of the mobile node
  - IP Source Address (the MN's Home Address)
  - UDP Source Port
  - Home Agent address
  - Requested registration Lifetime
  - Identification field

This visitor list acts much like a Visitor Location Register (VLR) in a cellular system.

HA Requirements

Each HA must have:

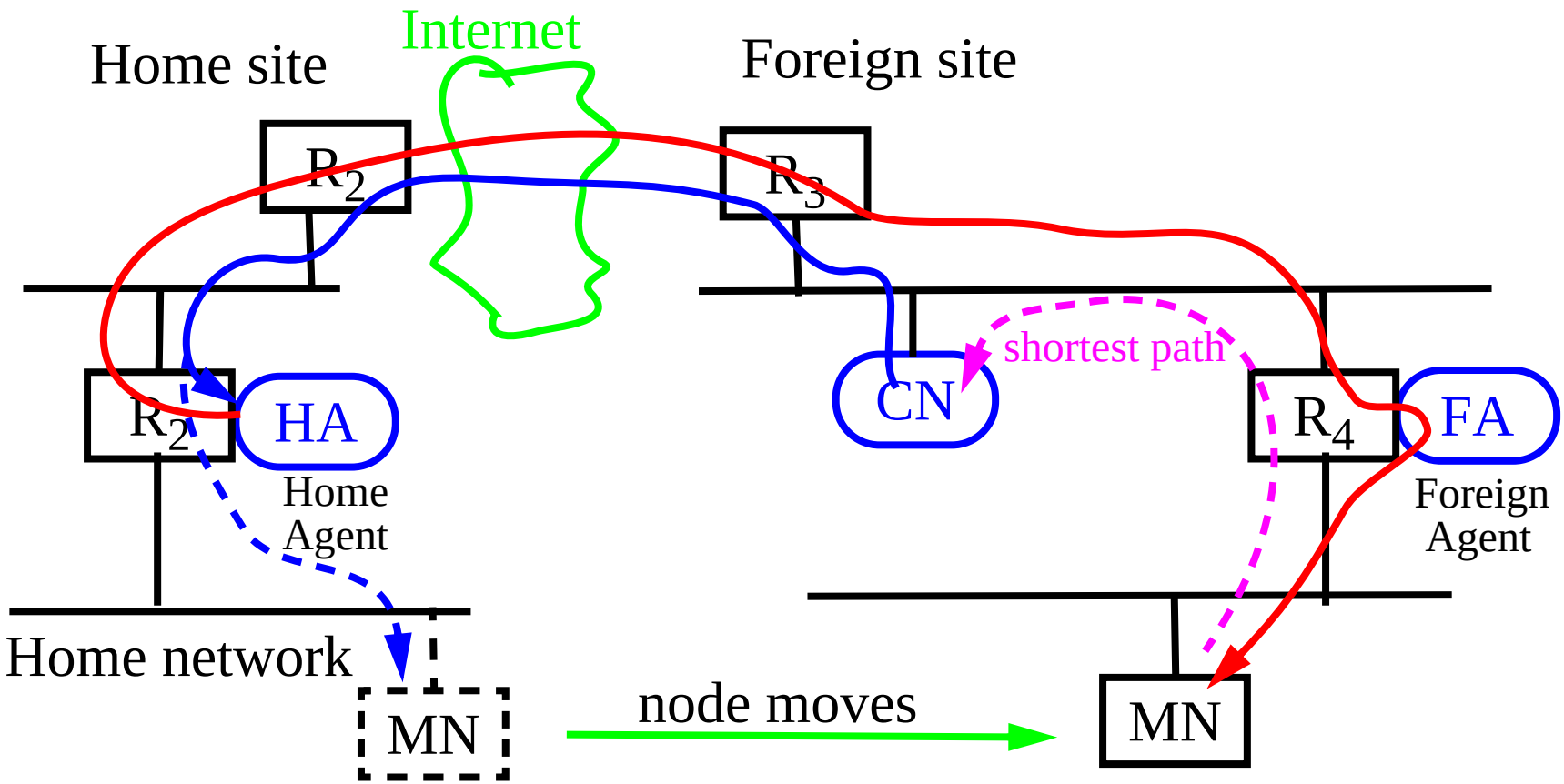
- the home address and mobility security association of each authorized MN that it is serving as a home agent.

Must create or modify its **mobility binding list** entry containing:

- Mobile node's CoA (or CoAs in the case of simultaneous bindings)
- Identification field from the Registration Request
- Remaining Lifetime of the registration

The mobility binding list acts much like a Home Location Register (HLR) in a cellular system.

Optimization Problem



We can **not** follow the shortest path in Mobile IPv4 because the CN will always send it via our home network. However, we may be able to use the shortest path from the MN to the CN.

Problems of Mobile IP (RFC2002)

- Only provides basic "macro mobility" support
- Not developed for cellular systems
- No interface defined between cellular systems
- (e.g. between Mobile-IP/HLR/VLR)
- No handover support

} ⇒ Cellular; Micro Mobility

- Weak in security
- No key distribution mechanism

} Security

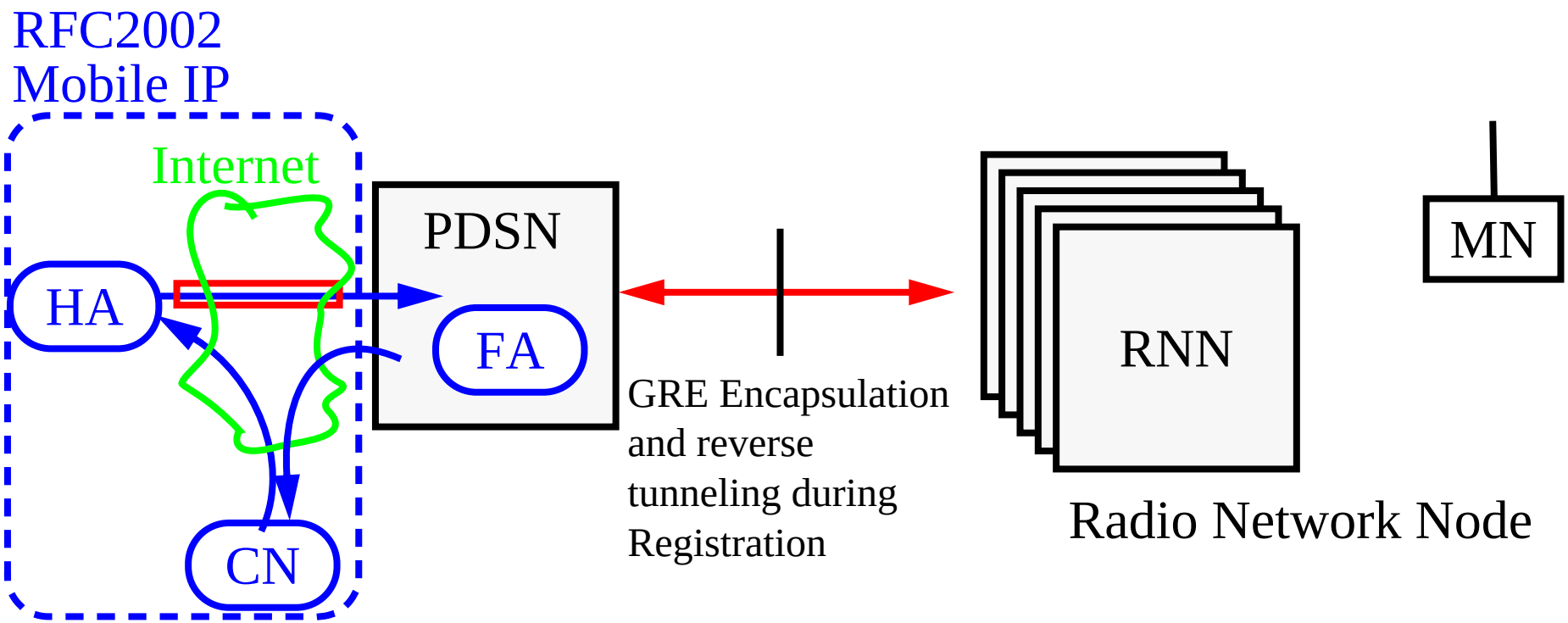
- Route optimization problems ⇒ Optimization
- No QoS, real-time support, (DiffServ, RSVP) ⇒ QoS and Real-time
- …

Mobile IP Problems and Development

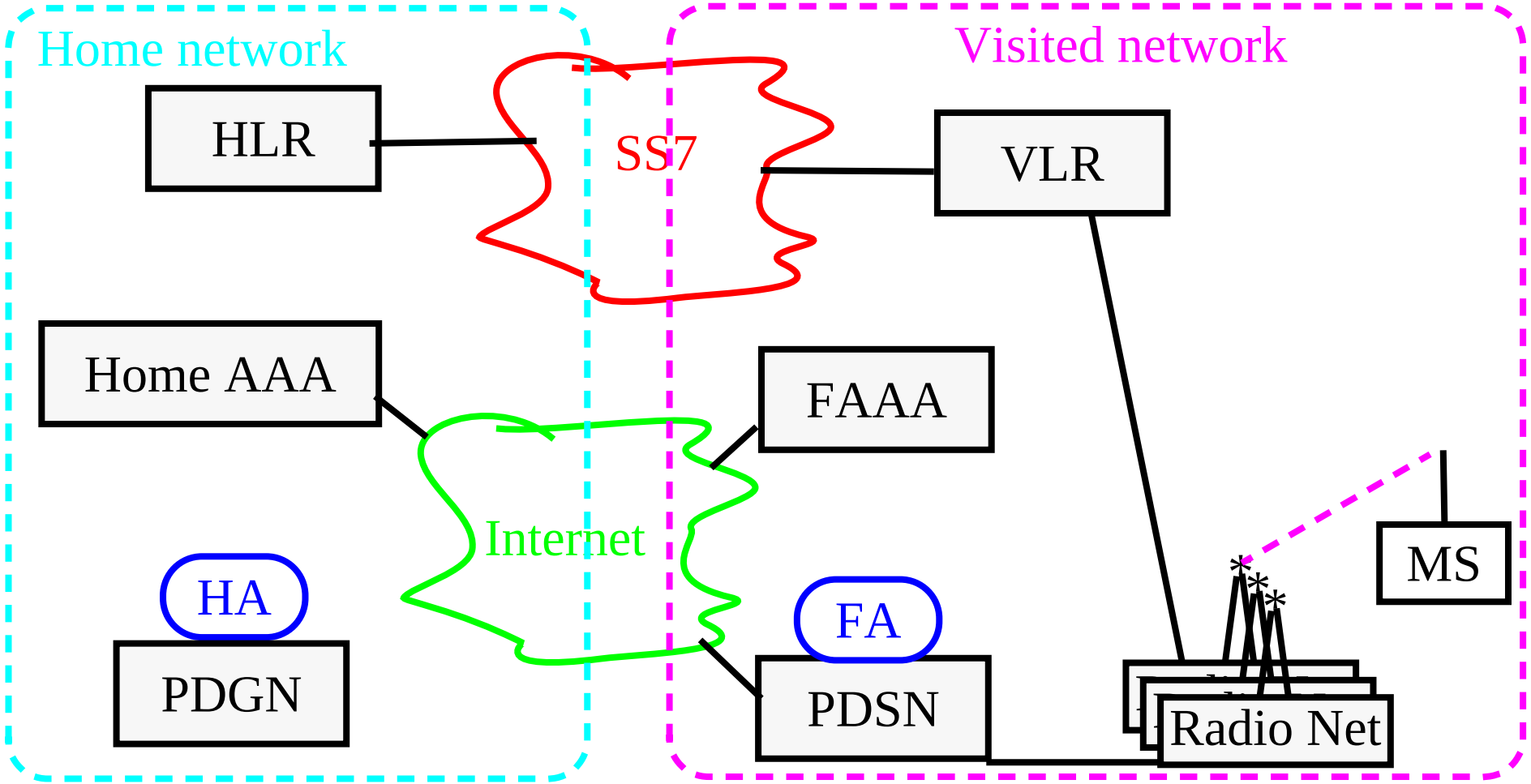
- Cellular Micro Mobility:
  - CDMA2000 Extension to MIP
  - Cellular IP
  - Regional Tunnel Management
  - Hierarchical MIPv6 Handoffs
  - MIP based Micro Mobility Mgt
- Security:
  - Mobile IP NAI Extension
  - AAA Registration Keys for MIP
  - Registration Keys for Route Optimization
  - Mobile IP Challenge/Response Extensions
- Route Optimization:
  - Route optimization for MIPv4, v6
- Real-time QoS:
  - No solution yet

CDMA2000 Extension to Mobile IP

A draft entitled: Mobile IP Based Micro Mobility Management Protocol in the Third Generation Wireless Network, by 3Com, Alcatel, Cisco, Ericsson, Lucent, Nortel, Motorola, Samsung, etc.

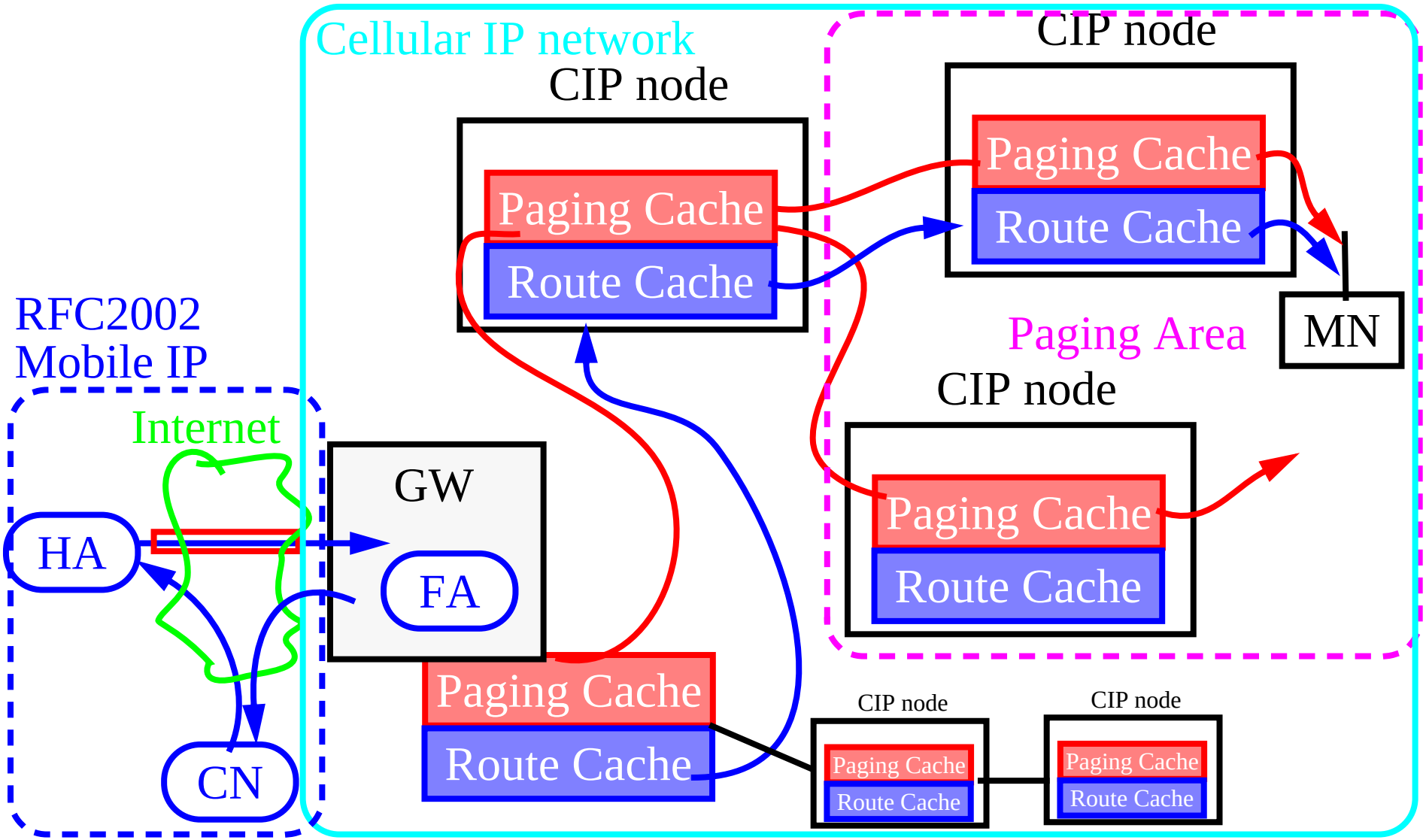


Wireless IP Network Architecture



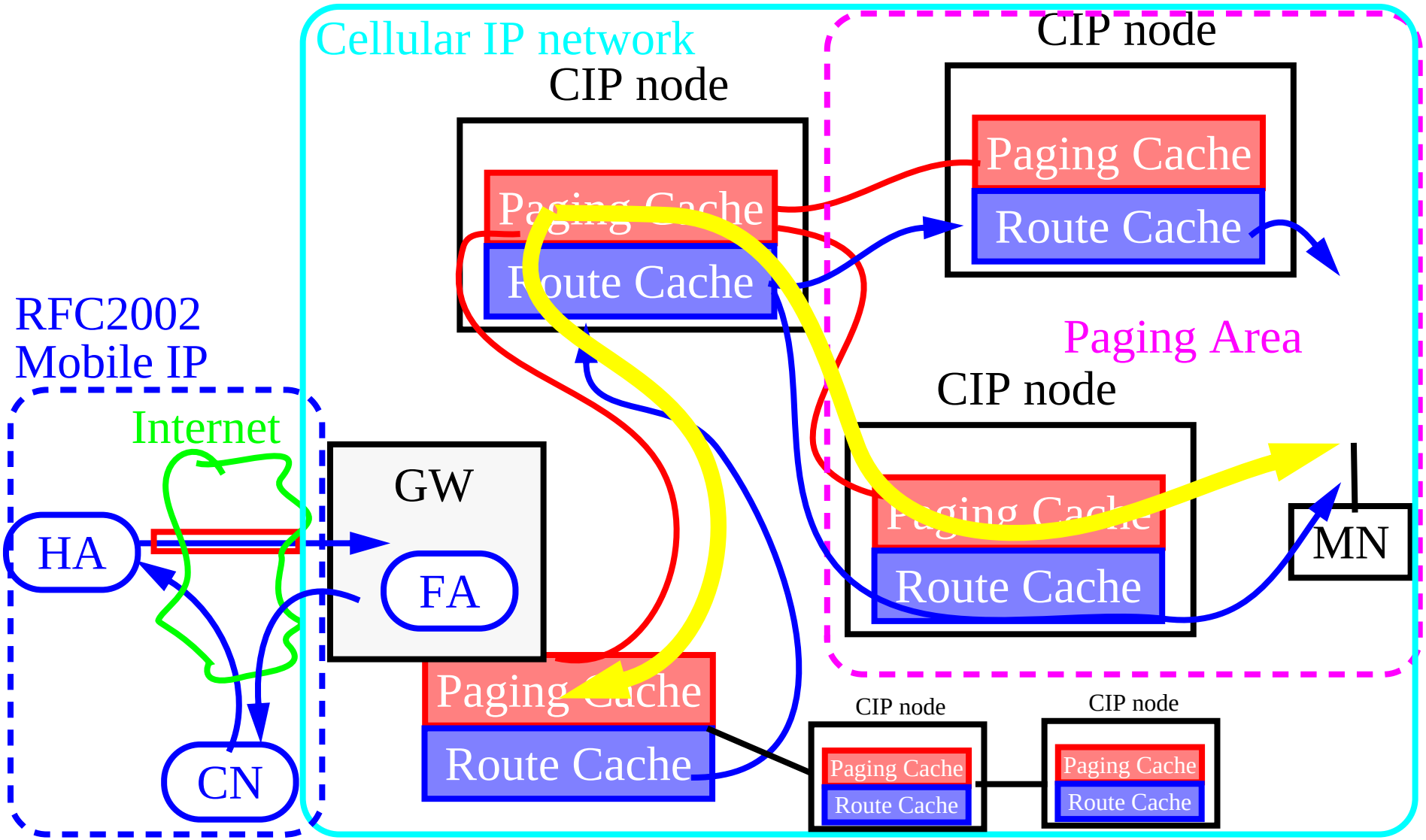
Cellular IP (CIP)

HAWAII extension is similar to Cellular IP.



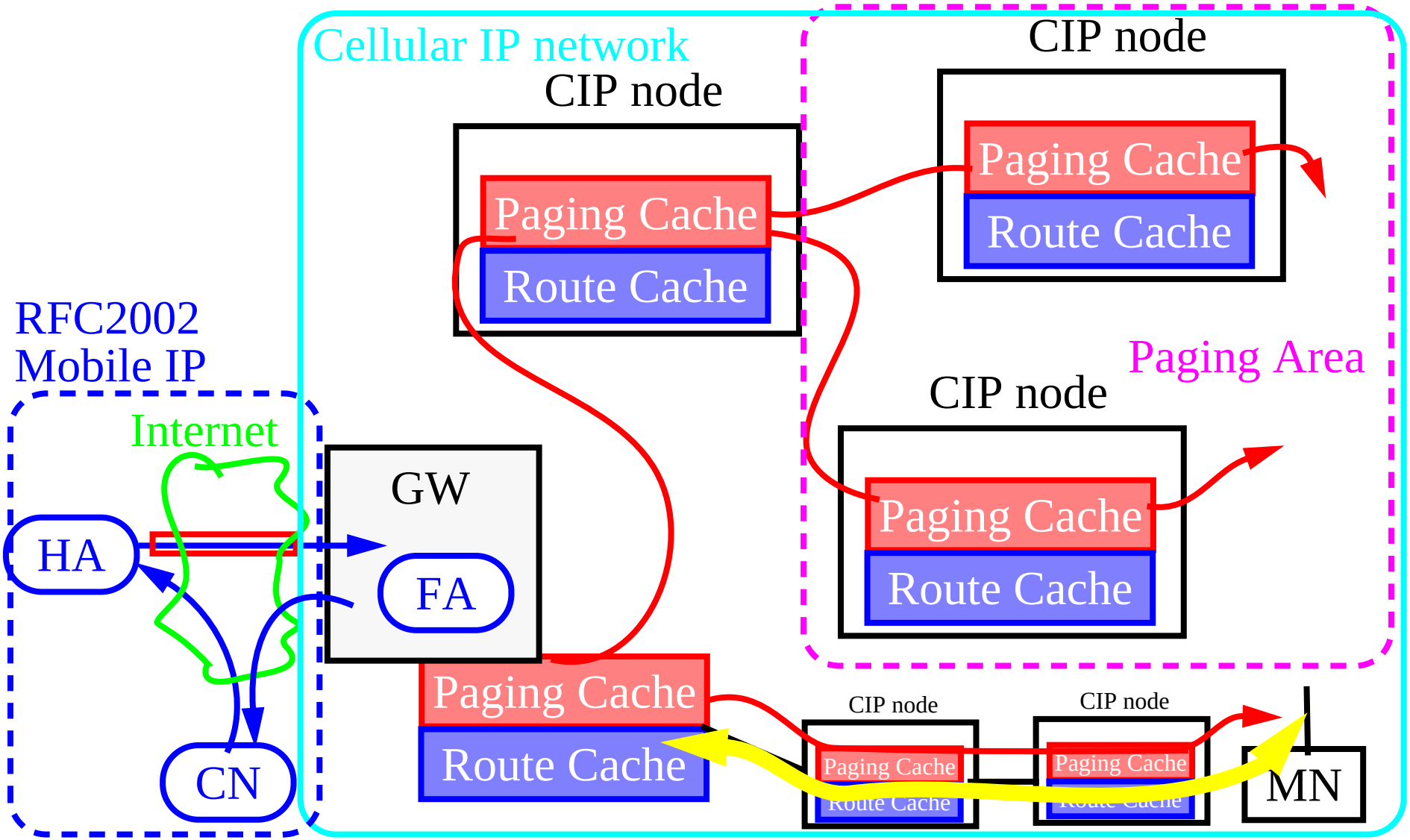
Cellular IP (CIP): Handover

HAWAII extension is similar to Cellular IP.

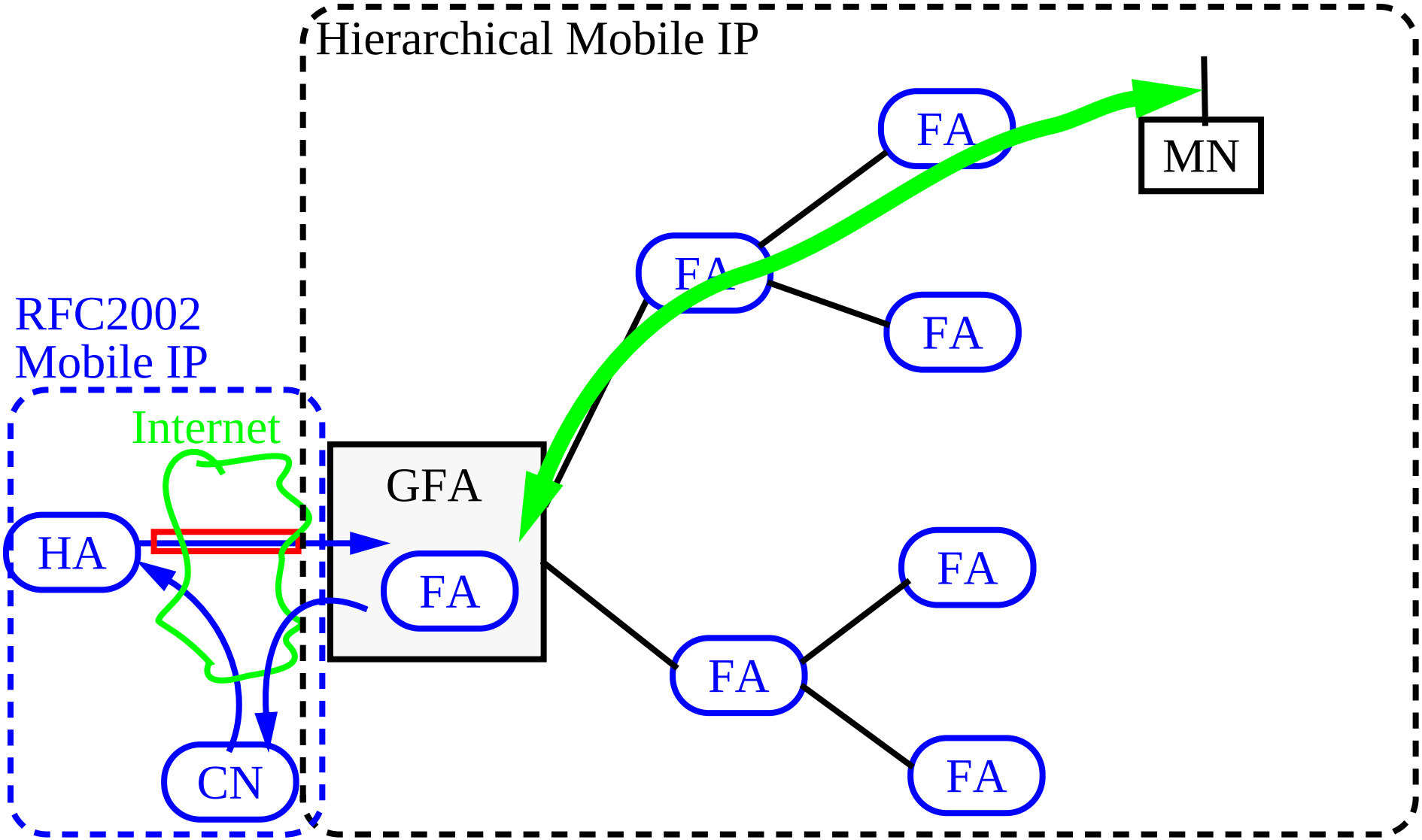


Cellular IP (CIP): Location Update

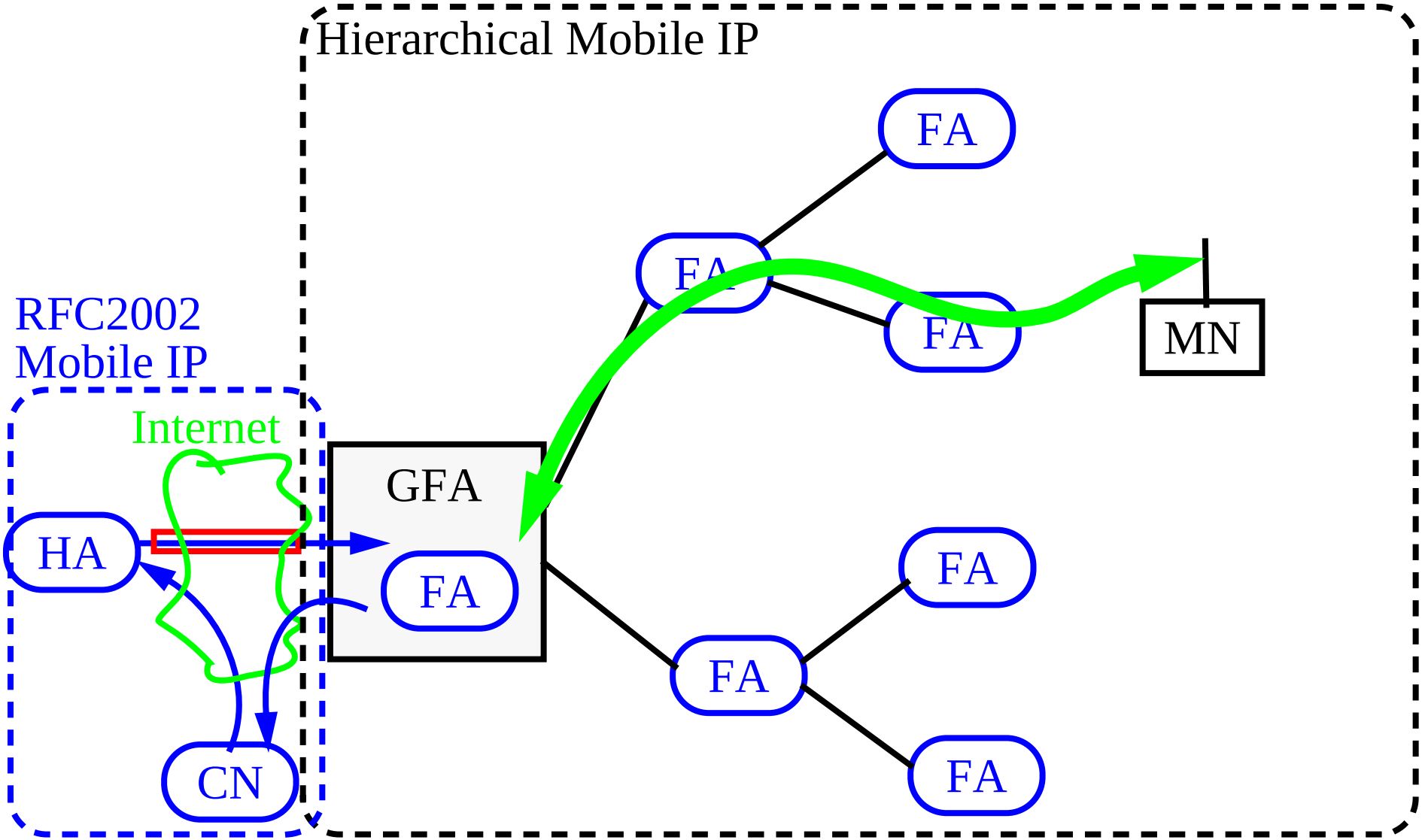
HAWAII extension is similar to Cellular IP.



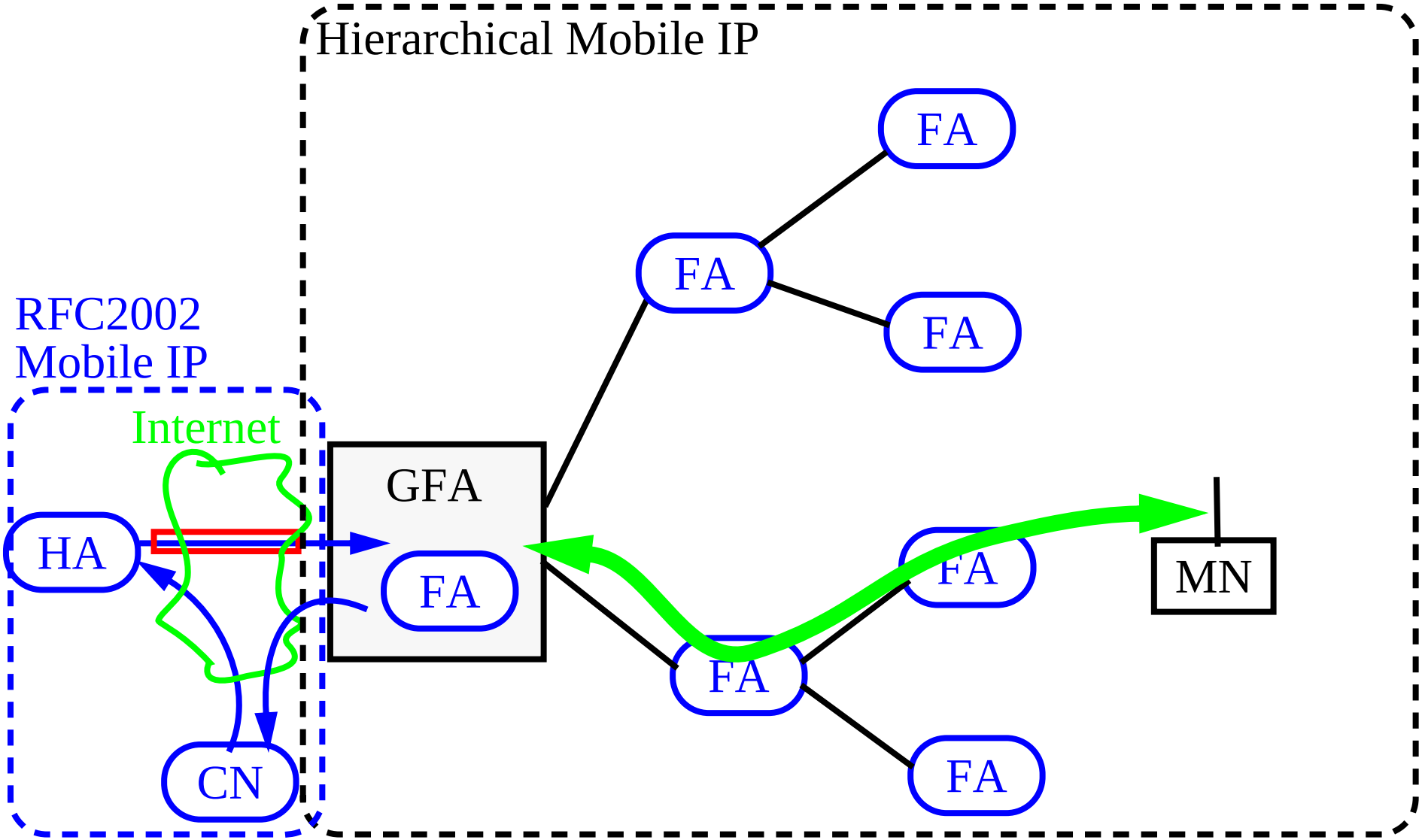
Hierarchical FA and Regional Tunneling



Hierarchical FA and Regional Tunneling



Hierarchical FA and Regional Tunneling



Why not simply use Dynamic DNS (DDNS)?

Problems of Dynamic DNS Mobility

- Only support inter-session mobility.
- TCP has to be disconnected when changing net.
- No inter-networking handover.
- Performance limitation problems.
- Security, Intranet firewall, etc.

	Mobile IP	Dynamic DNS
TCP survive the movement	Yes	No
Intra-session mobility	Yes	No
Handover Support	(Working on)	No
Performance Limitation	No	Yes

Thus DDNS does not really provide mobility, just connecting at different places.

Summary

This lecture we have discussed:

- Mobile IP

References

[104]. B. Aboba and M. Beadles, “The Network Access Identifier”, IETF RFC 2486, January 1999 http://www.ietf.org/rfc/rfc2486.txt

[105]C. Perkins, “IP Encapsulation within IP”, IETF RFC 2003, October 1996 http://www.ietf.org/rfc/rfc2003.txt

[106]C. Perkins, “‘Minimal Encapsulation within IP”, IETF RFC 2004, October 1996 http://www.ietf.org/rfc/rfc2004.txt

[107]Juan Caballero Bayerri and Daniel Malmkvist, Experimental Study of a Network Access Server for a public WLAN access network, M.S. Thesis, KTH/IMIT, Jan. 2002