Mobile IP

Lecture Overview

- IP Mobility
  - Significance of mobility in IP networks
  - Peculiarities of IP addressing
  - Quasi-mobility vs. Full IP mobility
- Mobile IP
  - conceptual framework
  - basic operation
  - latency problem and route optimisation
  - ingress filtering and reverse tunneling
  - handoff delay
  - improvements in IP Version 6
- Network Mobility
- Proxy Mobile IP

Prerequisite knowledge

- IP Addressing
- DHCP
- ICMP
- PPP
- Reference textbooks
  - any introductory text on networking

Significance of TCP/IP Mobility

why move in TCP/IP networks?

Data means IP

- Internet is based on IP
- IP is ubiquitous
- IP is the *de facto* standard for data
- You want data, you must connect to IP network

Mobile data ➔ IP mobility

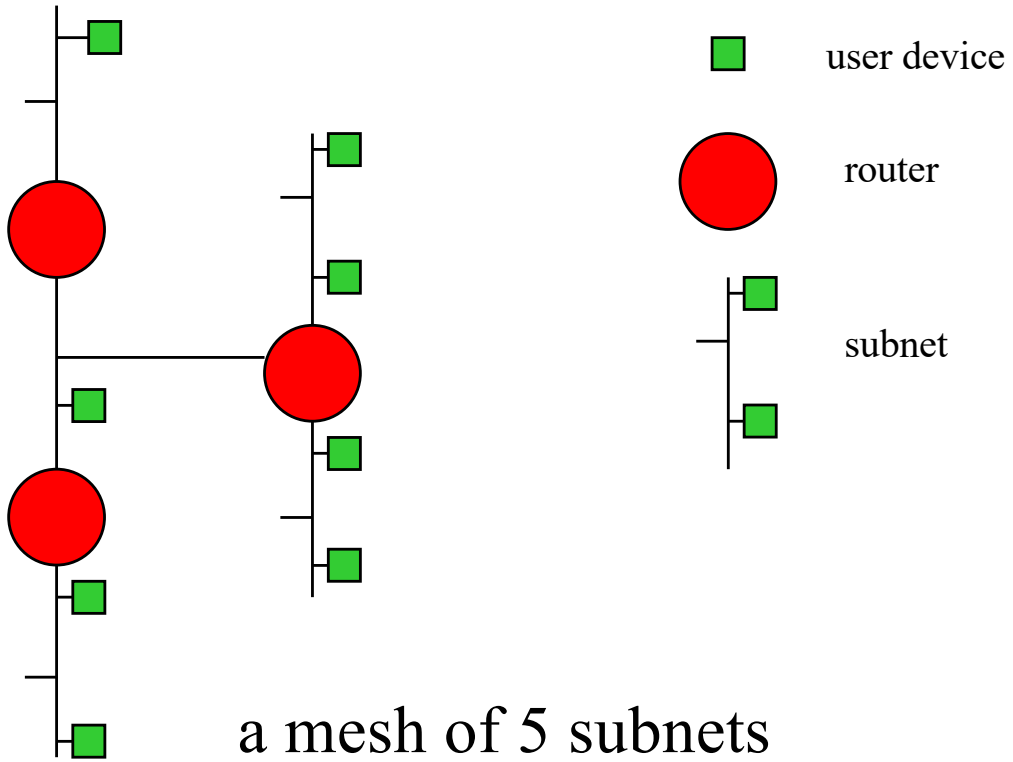
- Mobile data requires mobile connectivity to IP networks (or the Internet)
- Mobile data (wireless Internet access) increasingly desired
- Phone calls can be made over IP (VOIP)
  - (next to) free phone calls!

Peculiarities of IP addressing

what IP addressing has got to do with mobility

The world of IP

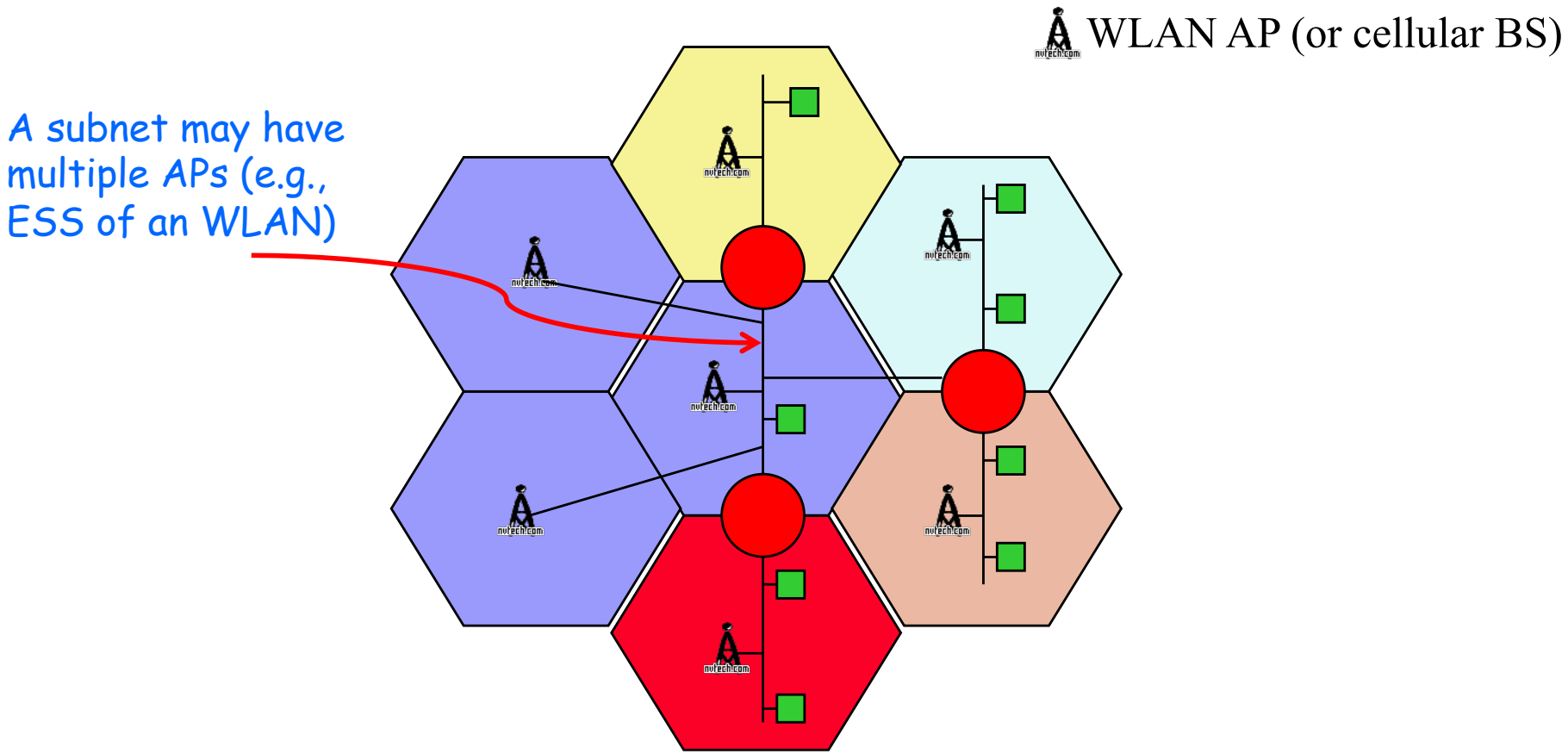
- A mesh of subnets interconnected by routers
- User device must be connected to one of the subnets



a mesh of 5 subnets

The world of IP
going wireless

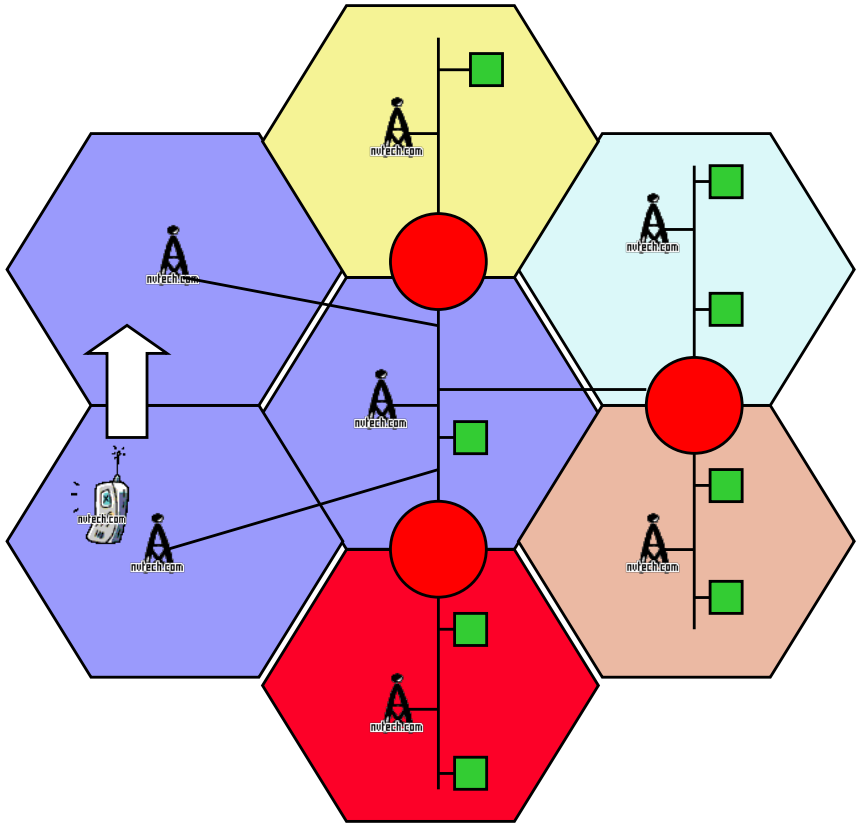
- Wireless makes it easy to connect to a subnet



Peculiarities of IP addressing

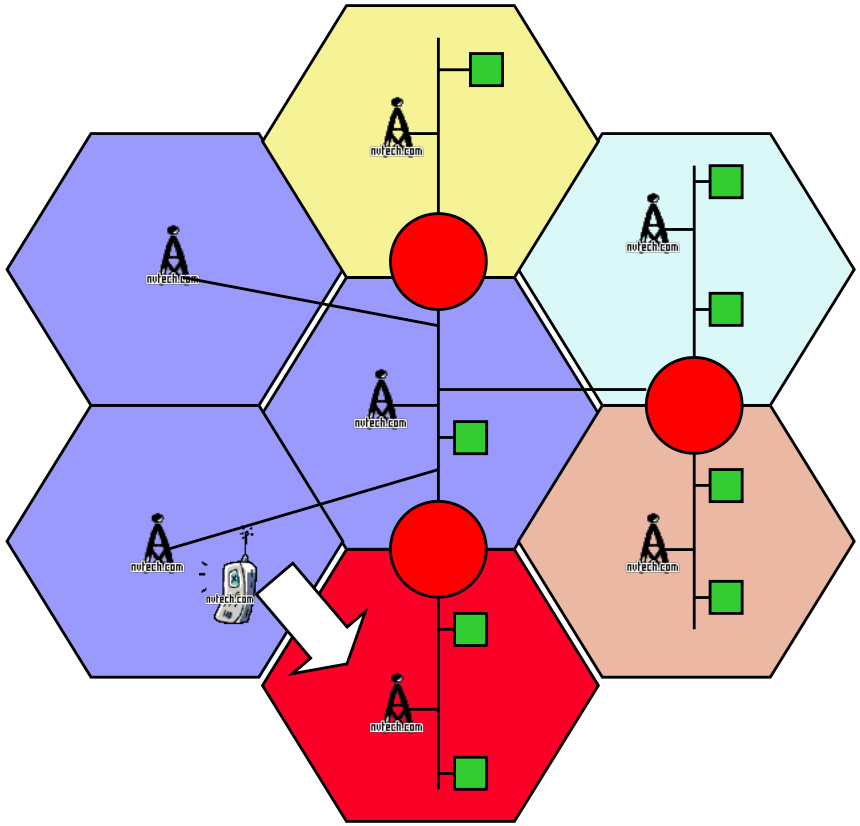
- A device must use a unique IP address to connect
- An IP address must carry the subnet prefix
  - eg 10.3.4.24/8 defines a host attached to subnet 10.0.0.0/8, and
  - 10.3.4.24/8 cannot be used to connect to subnet 12.0.0.0/8
- Subnet prefix is unique (makes IP address unique)
  - Used for routing
- Result ➔ inter-subnet movement requires change of IP address for the mobile device (intra-subnet movement does not)

Intra-subnet movement



this movement *does not* require change of IP address

Inter-subnet movement



this movement *does* require change of IP address

Quasi-mobility vs Full Mobility

Grades of mobility

- Quasi-mobility
  - YES: connect to Internet from any subnet
  - NO: move across subnet boundary within session
- Full mobility
  - YES: connect to Internet from any subnet
  - YES: move across subnet boundary within session

Quasi-mobility using DHCP-WLAN

- DHCP enables automatic IP address acquisition
  - get a new IP address valid for the new subnet
- WLAN makes connectivity even more effortless
  - Laptops and smartphones have built-in 802.11 capability (no WLAN cards required)
- Enables wireless/mobile Internet access
  - web browsing, e-mails, on-line chat, VPN, download, …
  - from cafes, airports, hotels, train stations, …
  - proved very useful and popular

Challenges of Full IP Mobility

Difficult to avoid address change (at subnet border crossing)

- Change of IP address at subnet border crossing is a key mobility problem
- No address change ➔ host-based routing
- Host-based routing does not scale
  - billions of hosts ➔ routing table explosion
  - routing table update required for every move
- Must find solutions that work with change of IP address

Mobile IP
enabling full mobility in IP networks

Conceptual framework

- Location = subnet
  - change of subnet = change of location
- Update location at subnet border crossing
- Location server always knows the current location of the mobile

Mobile IP Solution

- An IETF standard
  - (originally RFC 3344, now obsoleted by RFC5944)
- Most vendors support Mobile IP in their products, such as CISCO Routers

Dual IP Address

- With MIP, A mobile host has TWO IP addresses
  - a permanent address (or home address)
  - a temporary care of address (CoA)

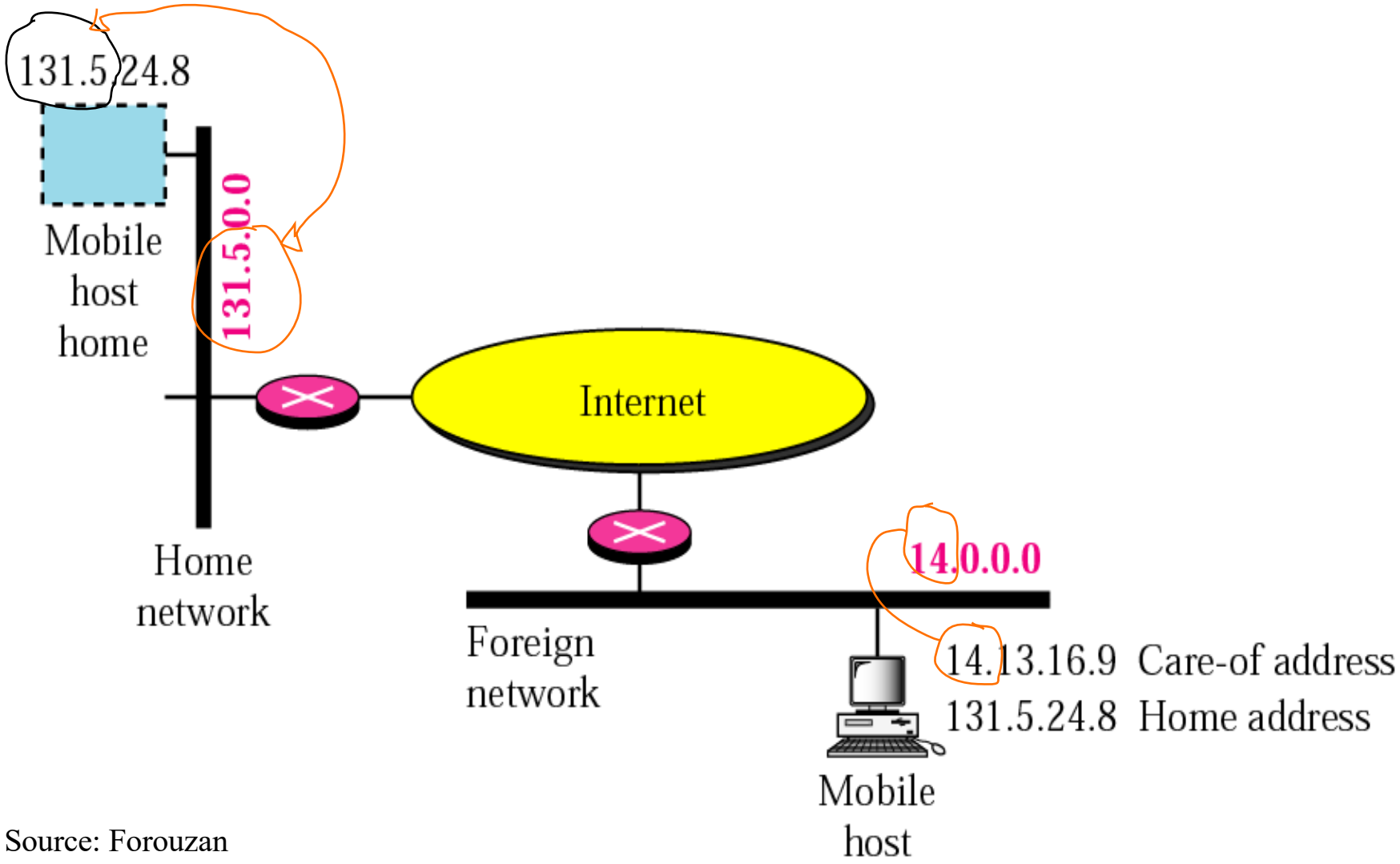
Home Address

- Home address = permanent IP address of the mobile host assigned during subscription
  - prefix of home address defines mobile's home subnet
- Mobile is always known by its home address
  - like the cellular phone number
- Anyone can reach the mobile anytime using home address
  - Home address does not change due to mobility
- DNS tables store home address
  - not updated during mobility
  - *mobility remains transparent to the rest of the world*

Care of Address

- A mobile host attached to a foreign network can be reached using a CoA
- CoA of a mobile host changes as it attaches to different subnets over time
  - mobile would require to update its CoA as it moves through different subnets

Illustration of Home Address and CoA address



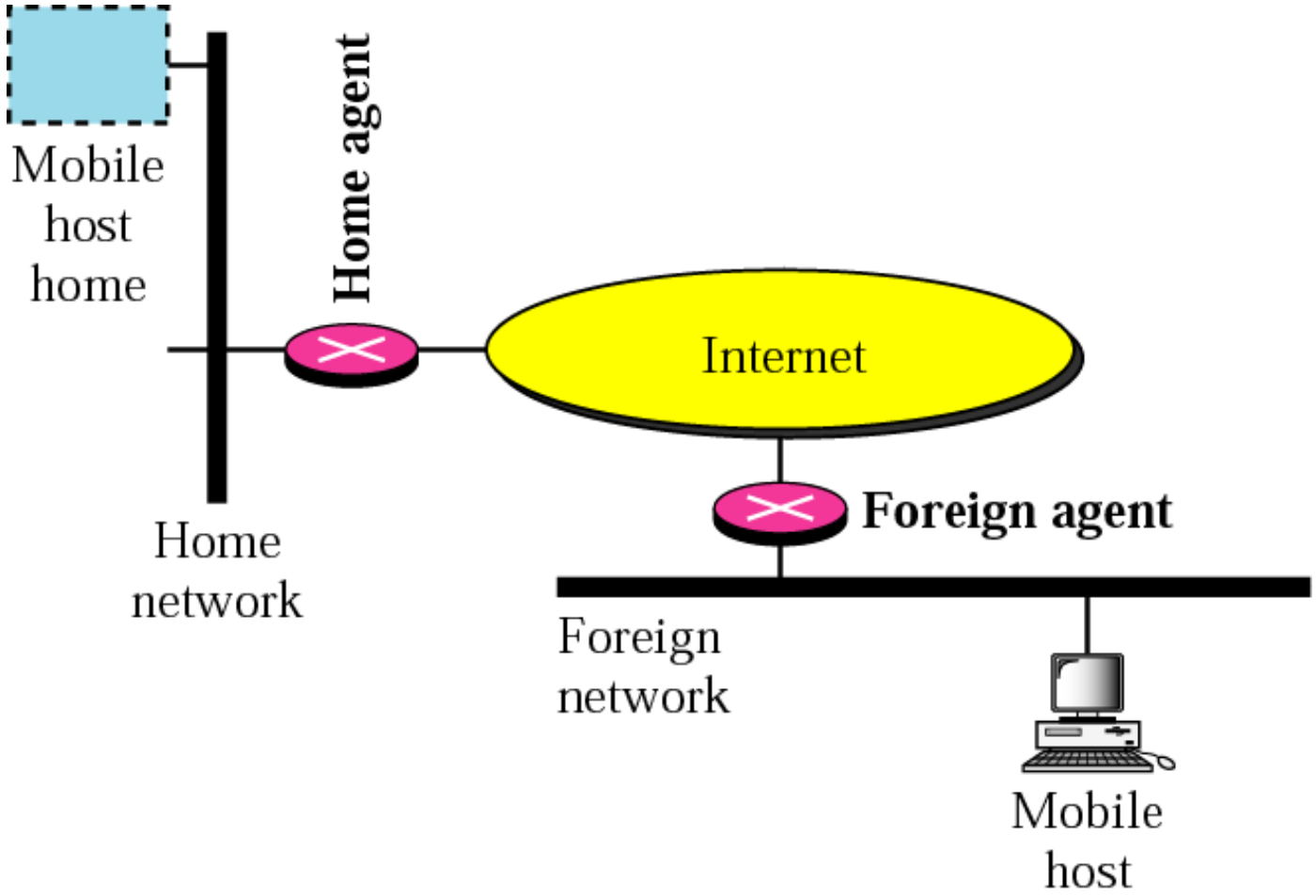
Source: Forouzan

Mobile IP agents

- Mobile IP requires two agents for its operation
- Home agent (HA) resides at home network
- Foreign agent (FA) resides at foreign network
- A network has both home agent & foreign agent
  - A network is home to some and foreign to others

Illustration of HA and FA

Agents are usually implemented in the routers



Home agent functions

- Typically implemented in a router
- Maintains up-to-date whereabouts (CoA) of mobile (home) hosts
  - acts as a location server for home hosts
- Receives packets on behalf of "out of town" mobile hosts and sends them to foreign agents

Foreign agent functions

- Accepts packets from home agents and delivers them to visiting mobile hosts
- Typically implemented in a router attached to the foreign subnet (or domain)
- Alternatively, FA can be located at mobile
  - called co-located CoA
  - mobile host does not need services of FA from the foreign network, but needs a new IP address to connect to foreign subnet

A Note on CoA

this CoA address is an IP address exclusively for the mobile device

- Co-located CoA
  - mobile needs unique IP address (consumes IP address)
  - unique address is obtained using DHCP etc.
- Foreign agent CoA
  - typically FA is a router known by several IP addresses
  - mobile uses one of FA IP addresses as CoA
  - several mobiles can use the same CoA
  - no new IP address is consumed (*DHCP not used!*)
  - Mobile connects using its permanent address

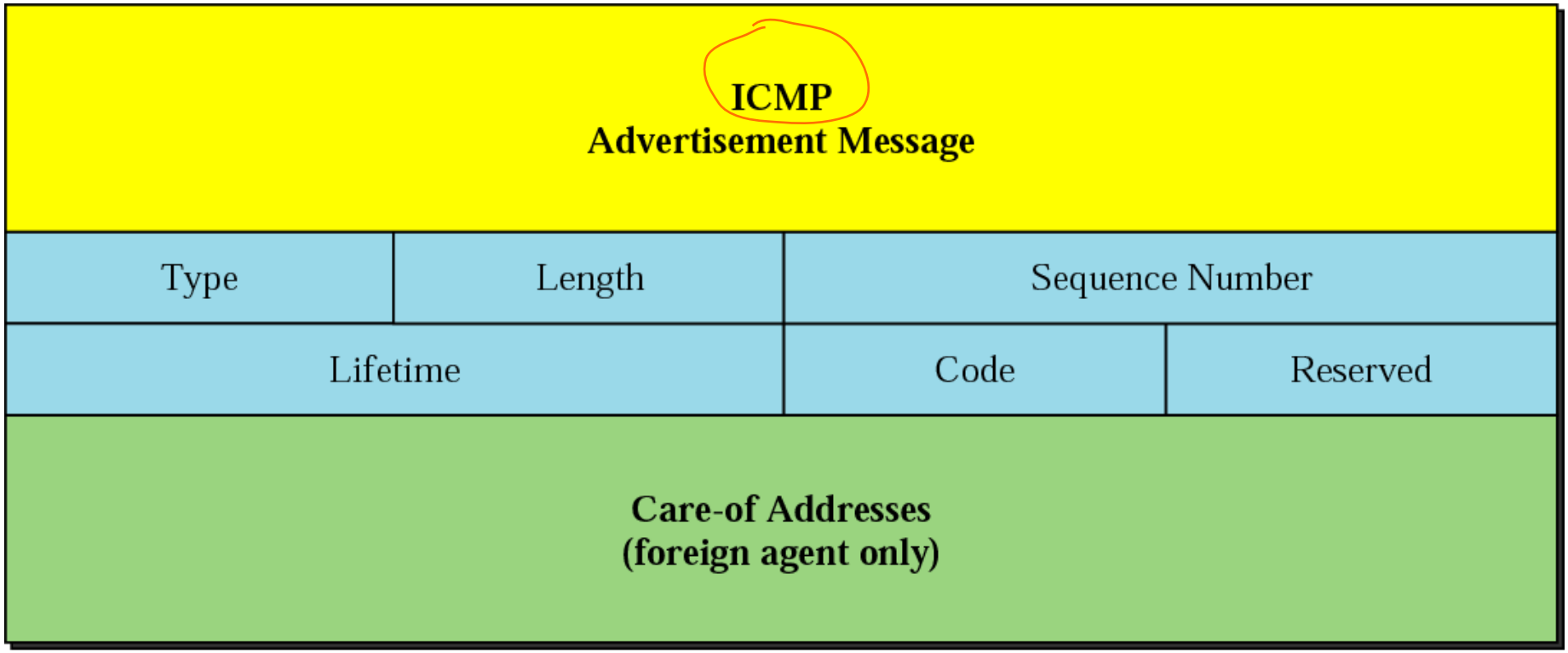
Phases of Mobile IP
FA located in router

Agent discovery is replaced by DHCP for colocated CoA

Agent discovery

- *This phase is needed if FA is located in router*
  - *Skip this phase if FA is colocated in the mobile*
- Mobile waits for periodic advertisement from FA
  - advertisement contains CoAs
- Mobile could solicit for CoA
  - If it didn't want to wait for periodic advertisement

Agent advertisement
FA located in router



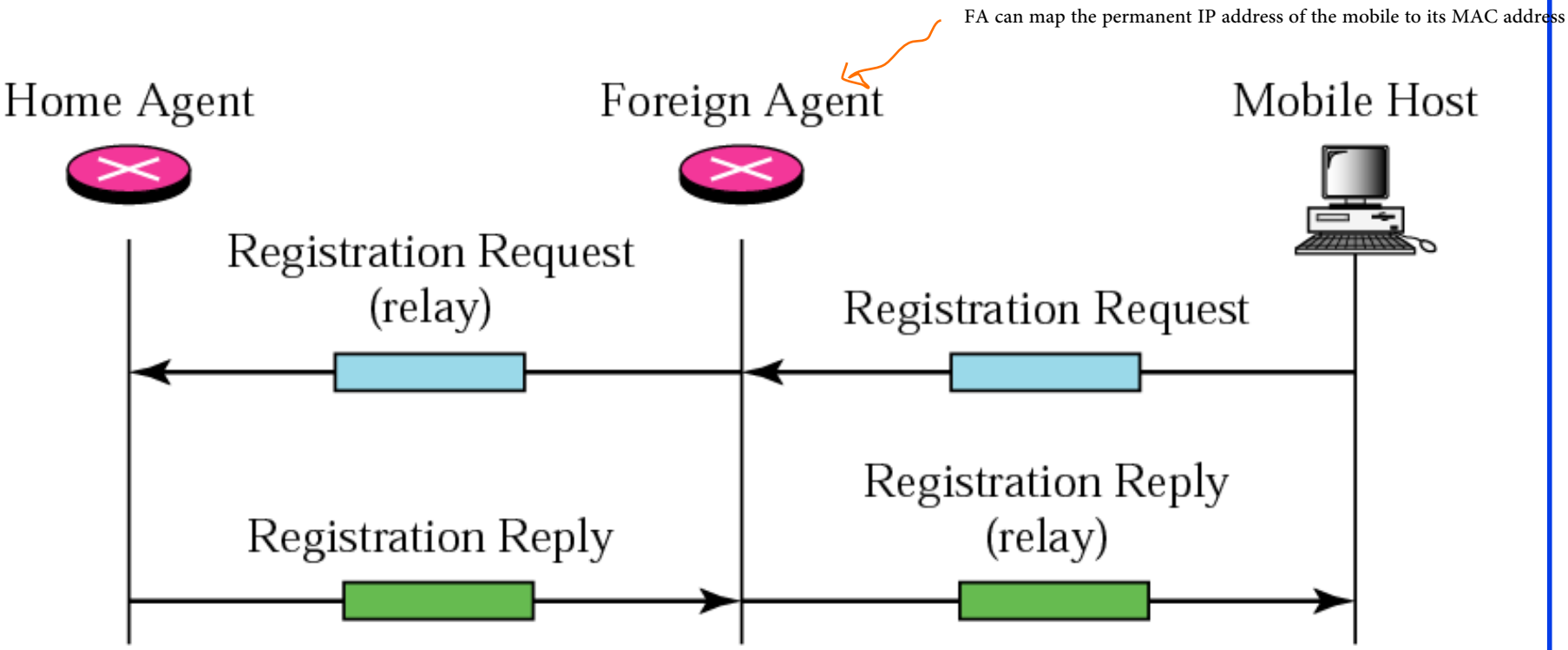
FA advertises router addresses as CoAs

Agent advertisement
Reuse of ICMP

Mobile IP does not use a new packet type for agent advertisement; it uses the router advertisement packet of ICMP, and appends an agent advertisement message.

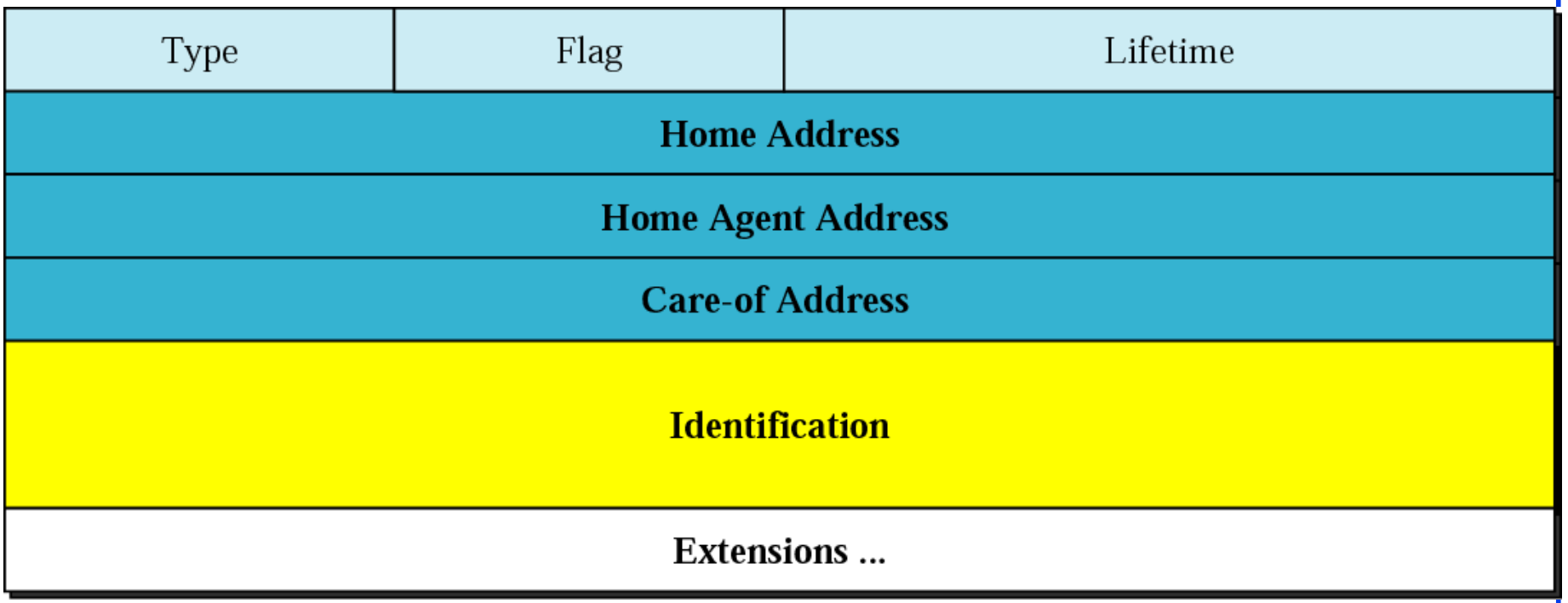
Mobile IP does not use a new packet type for agent solicitation; it uses the router solicitation packet of ICMP.

Registration request and reply
FA is located in a router

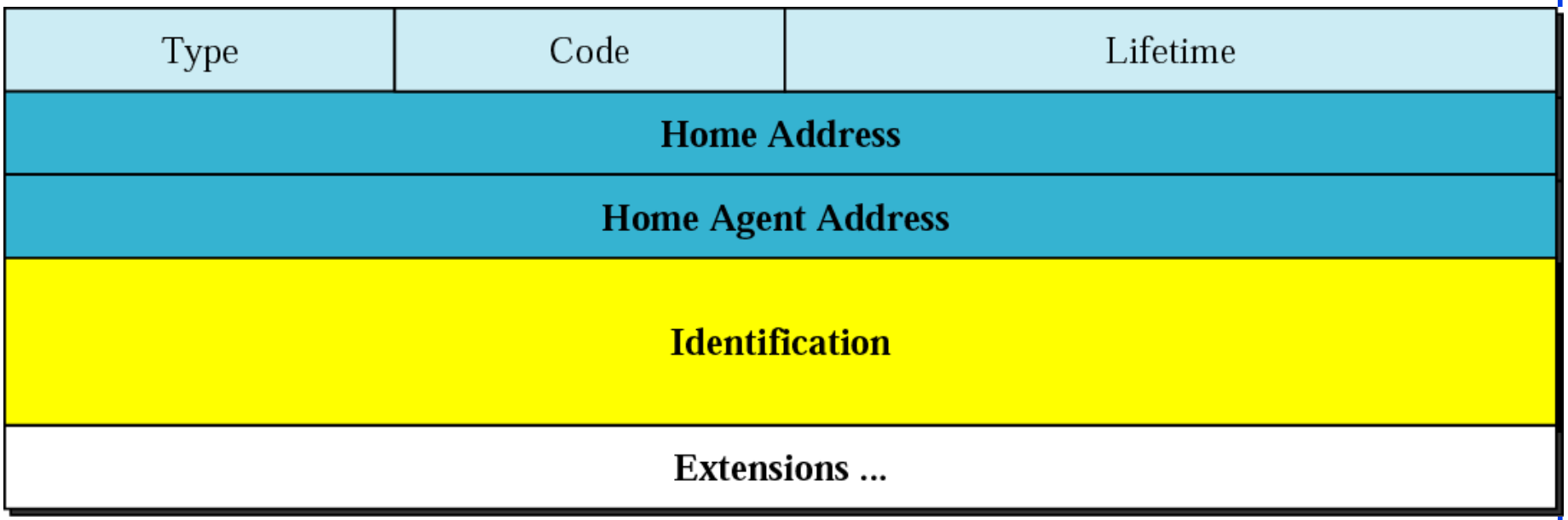


mobile talks directly to HA for colocated CoA

Registration request format



Registration reply format



Transport protocol for registration

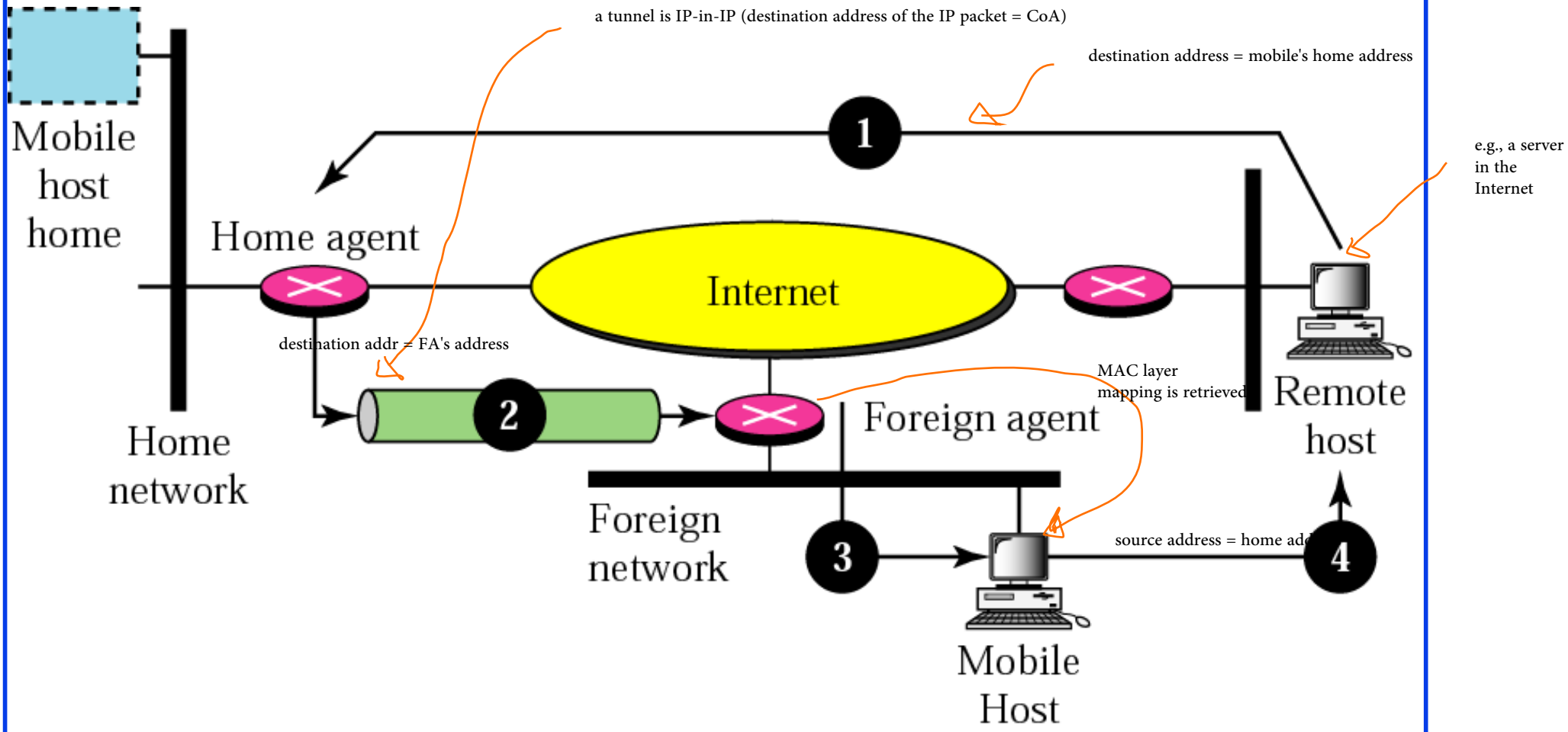
A registration request or reply is sent by UDP using the well-known port 434.

CN-MN Data Exchange

CoA is not co-located

- Step1: CN sends a packet to MN using home address
  - mobility remains transparent to CN
- Step2: HA intercepts it, encapsulates it in another packet with destination address as CoA and retransmits it (tunneling to FA)
- Step3: FA decapsulates, looks up MAC address of MN in registry, and sends the packet in LAN frame to MN
- Step4: MN sends packets directly to CN with source address as home address
  - mobility remains transparent to CH

CH-MH Data transfer (Remote host = CH)

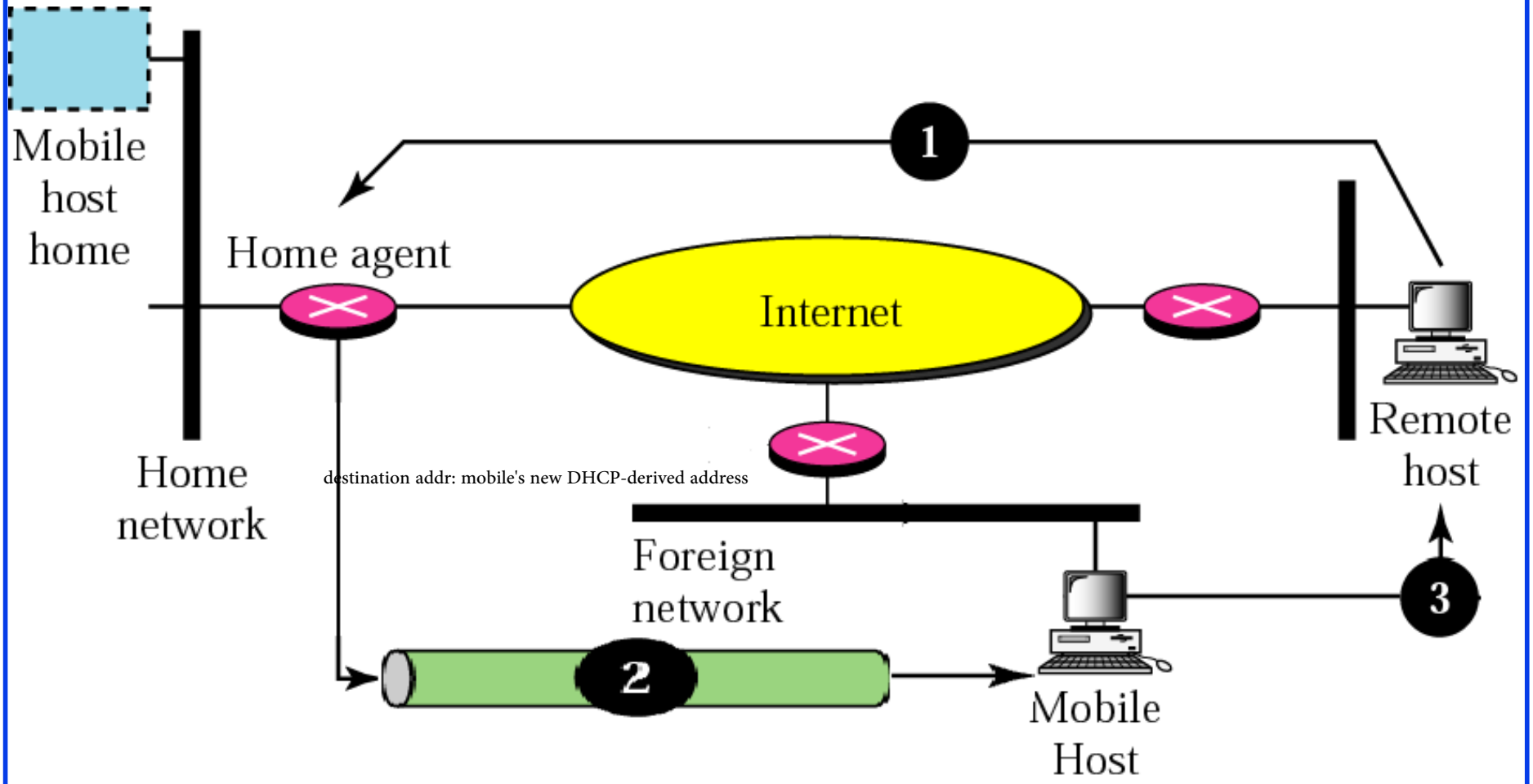


CH-MH Data Exchange

CoA is co-located

- Step1: CH sends packet to MH using home address
  - mobility remains transparent to CH
- Step2: HA intercepts it, encapsulates it in another packet with destination address as CoA and retransmits it (tunneling to MH), MH decapsulates and delivers to upper layers
- Step3: MH sends packets directly to CH with source address as home address
  - mobility remains transparent to CH

Data transfer Co-located CoA (Remote host = CH)



Headers of a Tunneled Packet

Using IP-in-IP Encapsulation

Inner Header: From CN to MN

Outer Header: From HA → FA/CoA

Outer IP Header	Inner IP Header	Transport Layer Header	User Data (if any)
Src Addr = HA Dest Addr =CoA Proto = IP	Src Addr = CN Dest Addr = MN Proto = TCP/UDP		

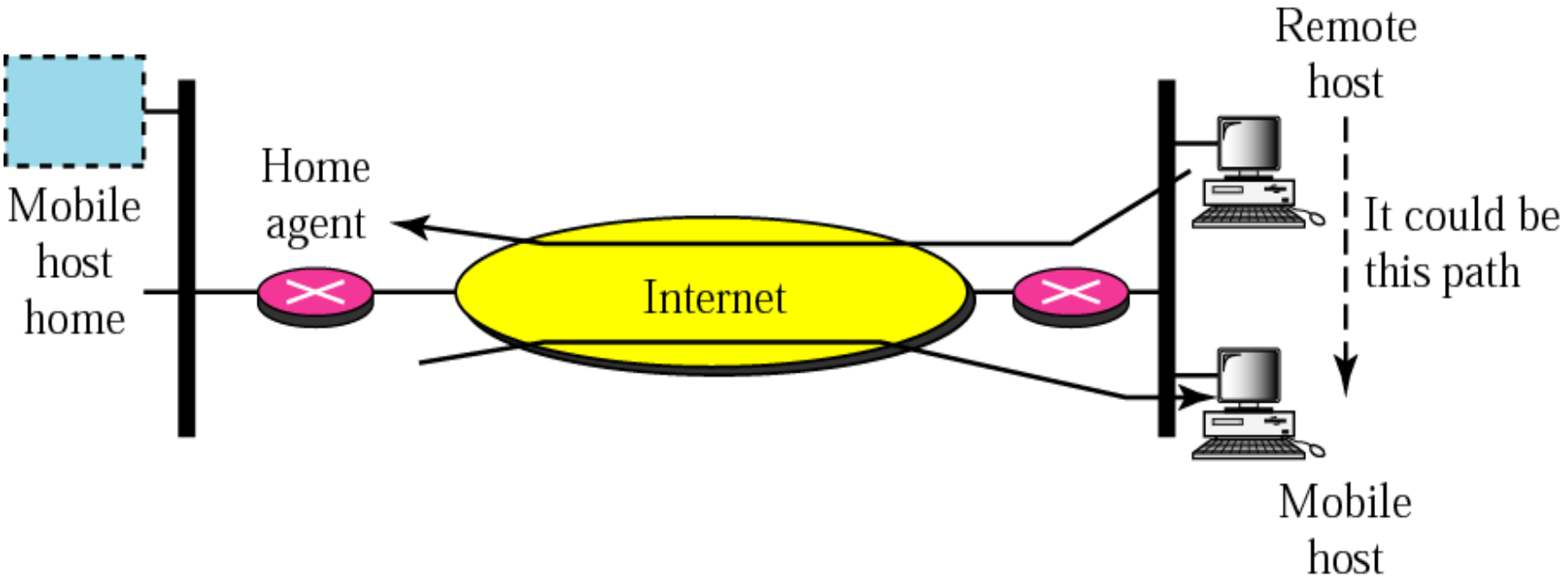
IP handoff

- Registration may take ‘long’ time
- Registration delay can cause problems
  - packets may got lost during IP handoff
- Solution A: previous FA buffer data and forward to new FA
  - works for data services, but not for voice
- Solution B: predict mobility and complete registration before moving to new subnet
  - Requires overlapping wireless coverage
  - Handoff delay reduced (good for voice)

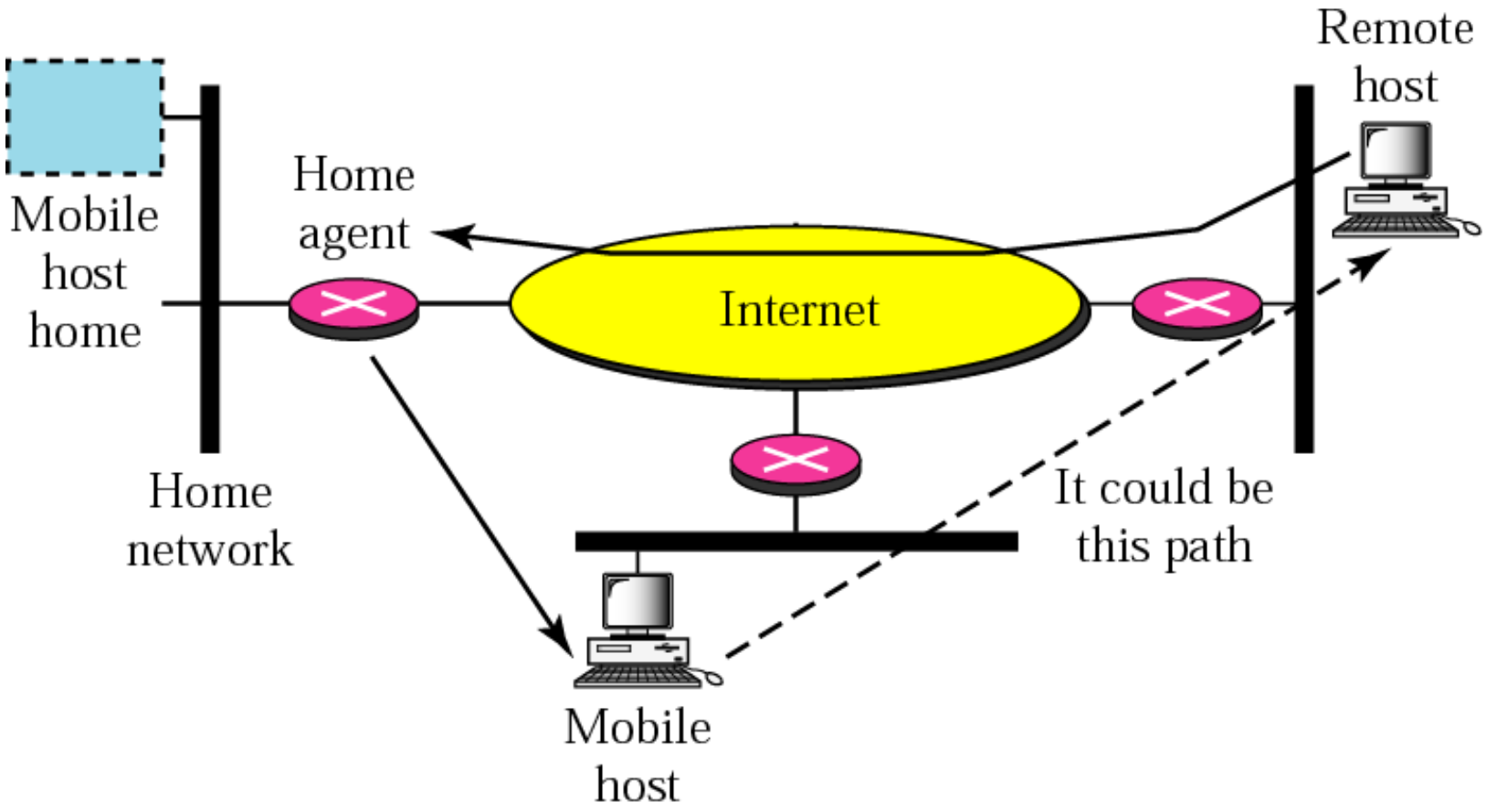
Latency problem

- Mobile IP stretches communication routes
  - more hops increases packet transit time
  - Not good for voice over IP
- Route stretch
  - Double crossing
  - Triangular routing

Double crossing

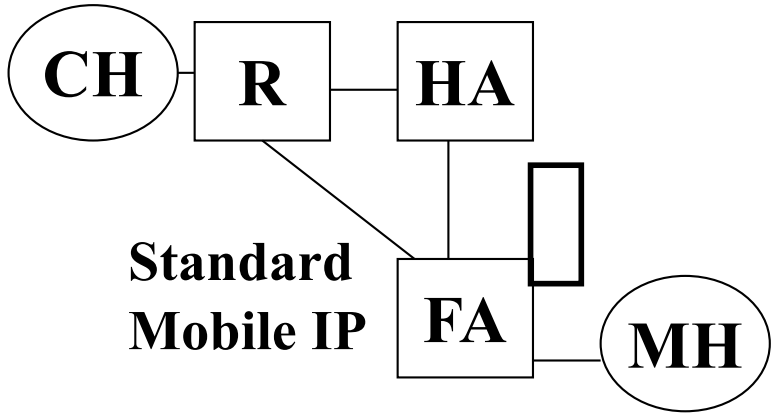


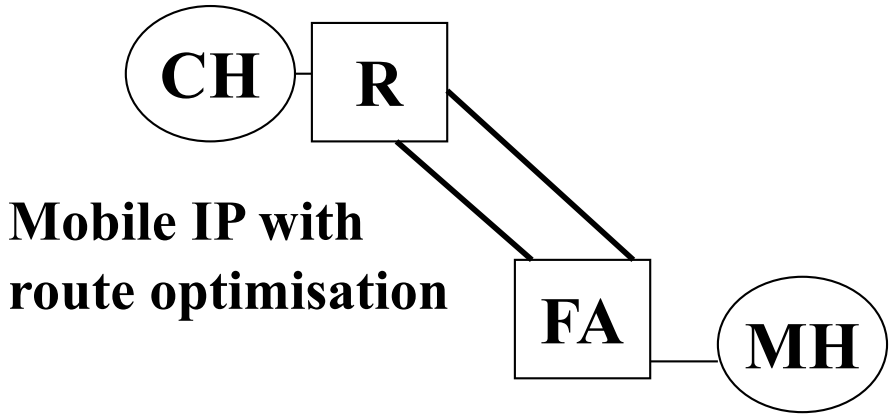
Triangular routing



Route optimisation
Principle

- CH directly tunnels to CoA
  - bypassing HA
- Triangular routing avoided





Route Optimisation

How does CH know CoA?

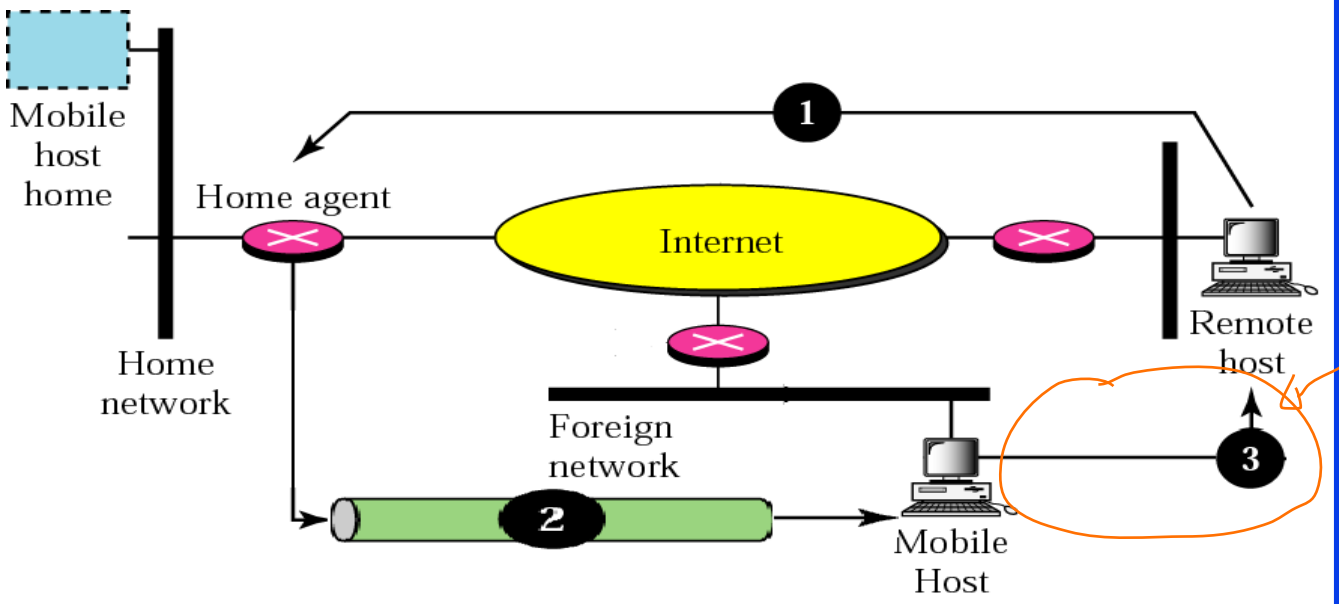
- Initially it does not know
- It sends packets to HA
- HA tunnels to FA, *but also sends CoA to CH*
- CH sends all subsequent packets directly to CoA (route optimisation)

Route Optimisation
problems

- CH learns the CoA
  - mobility is *not* transparent (privacy issue)
- Existing IP software at CH will not work
  - needs to be mobile IP capable
- Stored CoA may be invalid

Reverse tunneling (1)

- Original version of MIPv4 allows MH to send replies directly to CH
  - MH always uses Home Address as the source address



not work with ingress Filtering

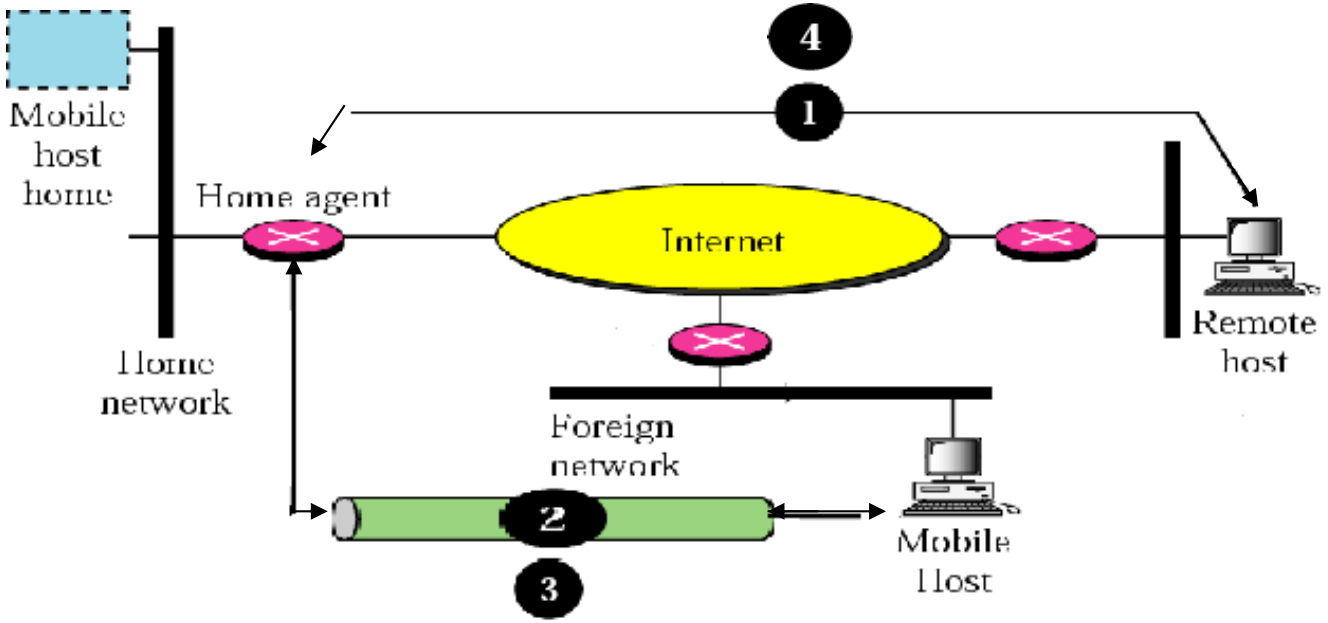
Reverse tunneling (2)

- To overcome Denial of Service(DoS) attacks, Internet routers began filtering packets passing through them.
  - Routers would allow a packet to pass through it only if the source address matched the origin of the packet
  - Called Ingress filtering
- Reverse tunneling was introduced to enable MIP to work with ingress filtering mechanism.

Reverse tunneling (3)

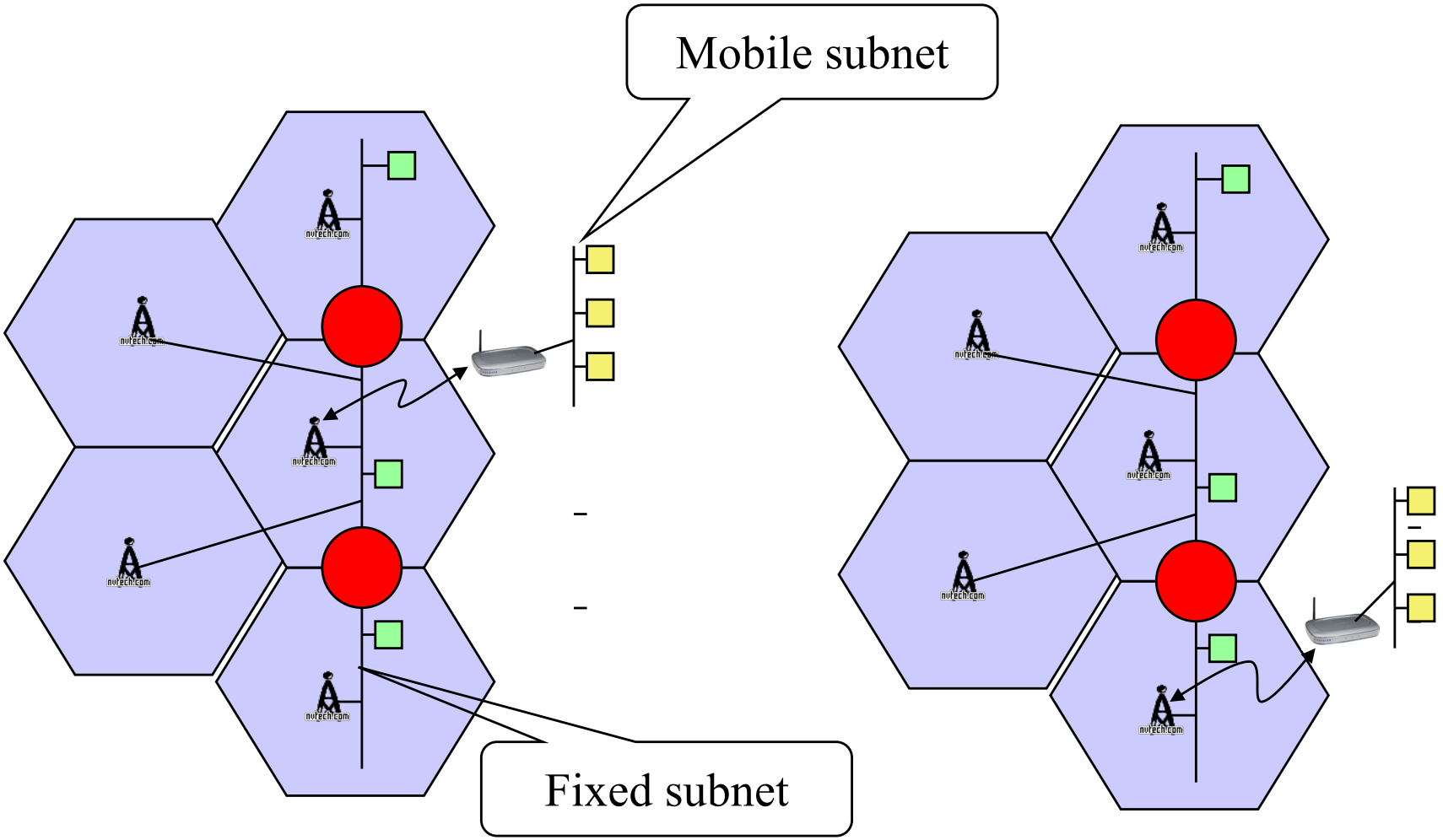
(Remote host = CH)

- MH-CH data exchange also takes place through a reverse tunnel between the MH/FA and HA
- Double Triangular routing ?



Network Mobility

What is network mobility?



Consider a *stub* subnet

Mobile subnet has moved

Motivation for supporting network mobility

- Commuters in trains and buses may wish to connect their devices to an onboard LAN
  - similar to connecting to the LAN at work
- If the onboard LAN could remain connected to the Internet, mobility could be hidden from the commuters
  - no *individual* mobility management
  - battery power saving by not connecting to a distant outdoor radio tower (low power)

Implications

- The onboard IP subnet will change its point of attachment to the Internet
- Reachability and session continuity must be preserved despite these changes
- IETF has set up a working group to standardise protocols that can support *subnet mobility* in the TCP/IP infrastructure

Solutions

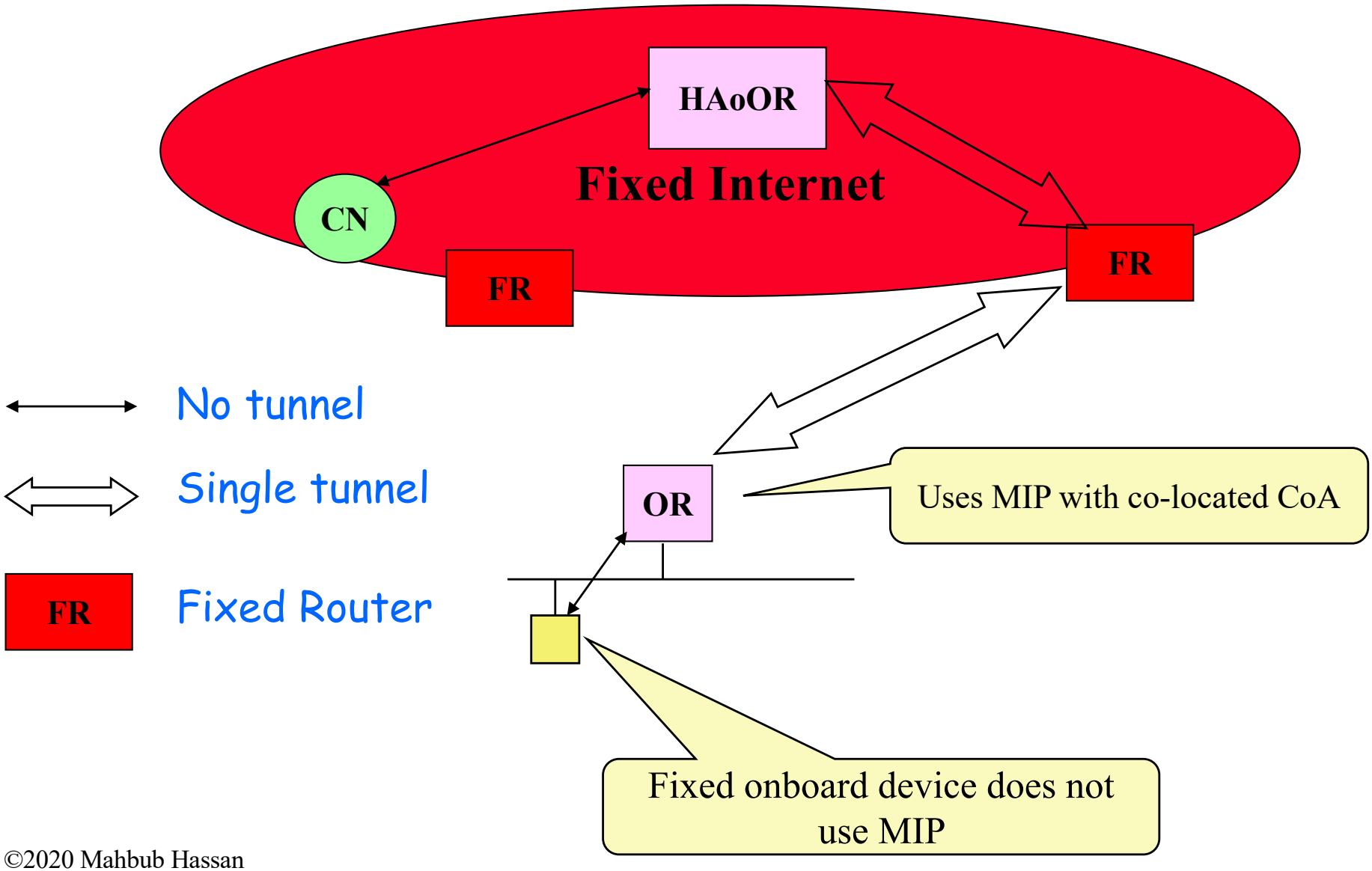
- Let us study a standard from IETF called NEMO
- NEMO is based on MIP
- IN NEMO, there is an *onboard central entity* that manages the mobility of the onboard IP subnet
  - onboard user devices require no action when the subnet changes point of attachment
  - movement of the subnet remains transparent to the onboard devices

NEMO overview

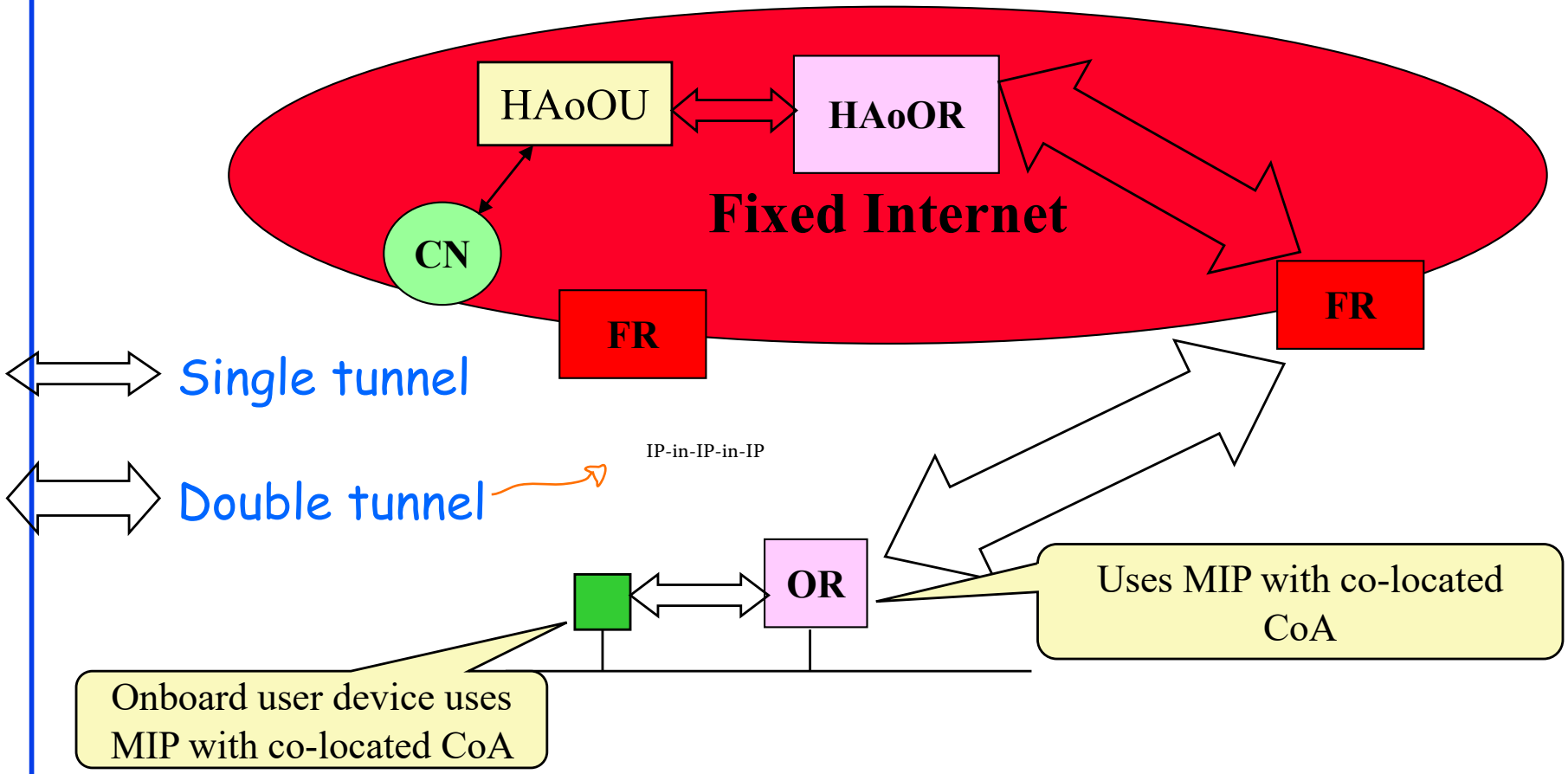
- RFC3963 released in 2005
- Onboard router (OR) uses MIP to manage the mobility of the moving subnet
- Bidirectional tunnel between OR and router home agent (RHA)
- If onboard mobile device uses MIP as well, we have a *recursive* MIP
  - fixed onboard devices may not need to use MIP
  - onboard user devices may need to use MIP

NEMO

Communication with fixed onboard device



NEMO
Communication with onboard user device



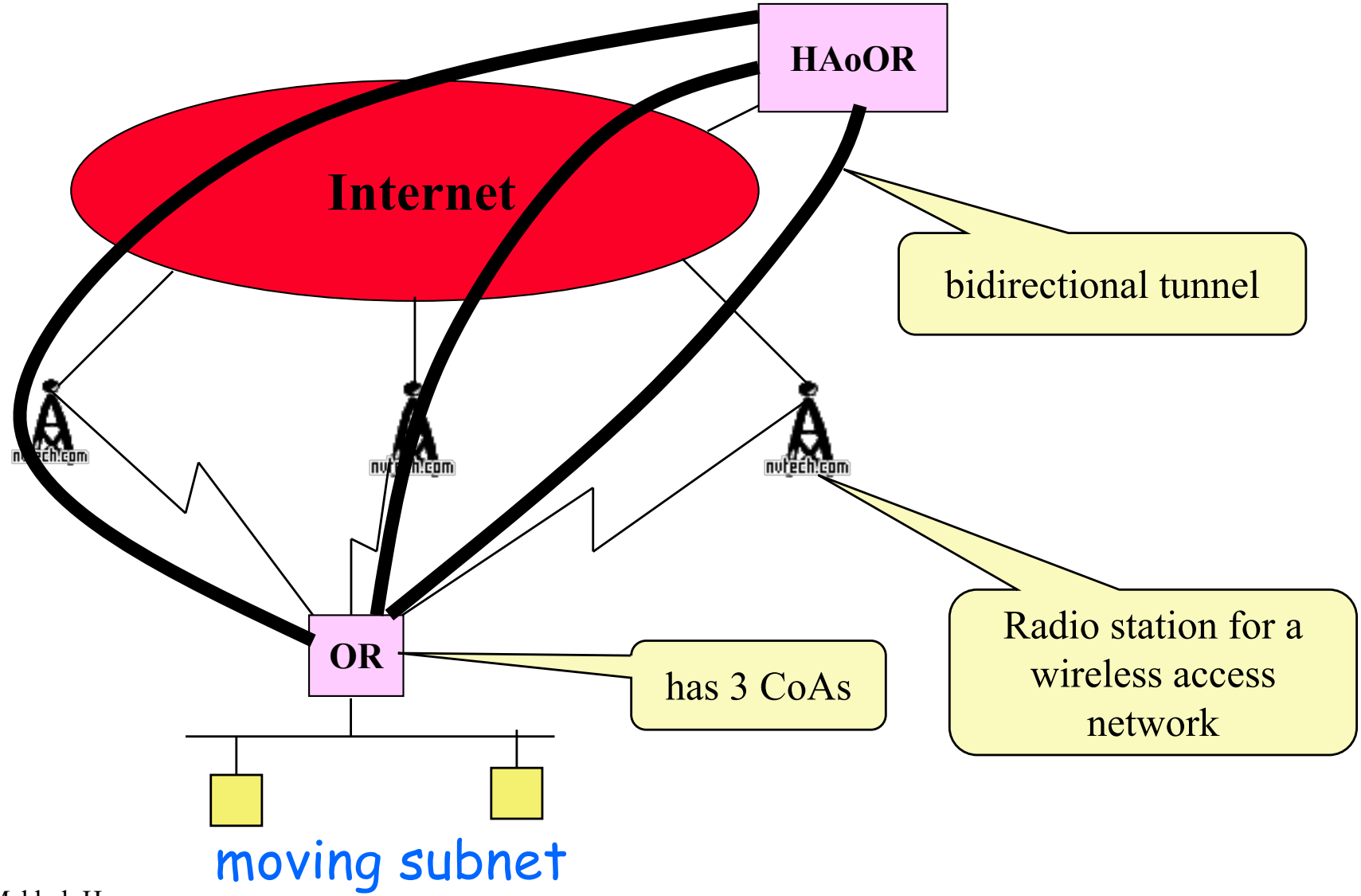
HAoOU: HA of onboard user device

Multihoming with NEMO

- (RFC4980, Oct 2007)
- Connect the mobile subnet to the Internet via multiple wireless access networks
  - Example of wireless access networks: cellular networks, WiFi, etc.
- All wireless interfaces can be used simultaneously
  - Registering multiple CoA with the HA is allowed
- Improves reliability and robustness of the Internet connectivity

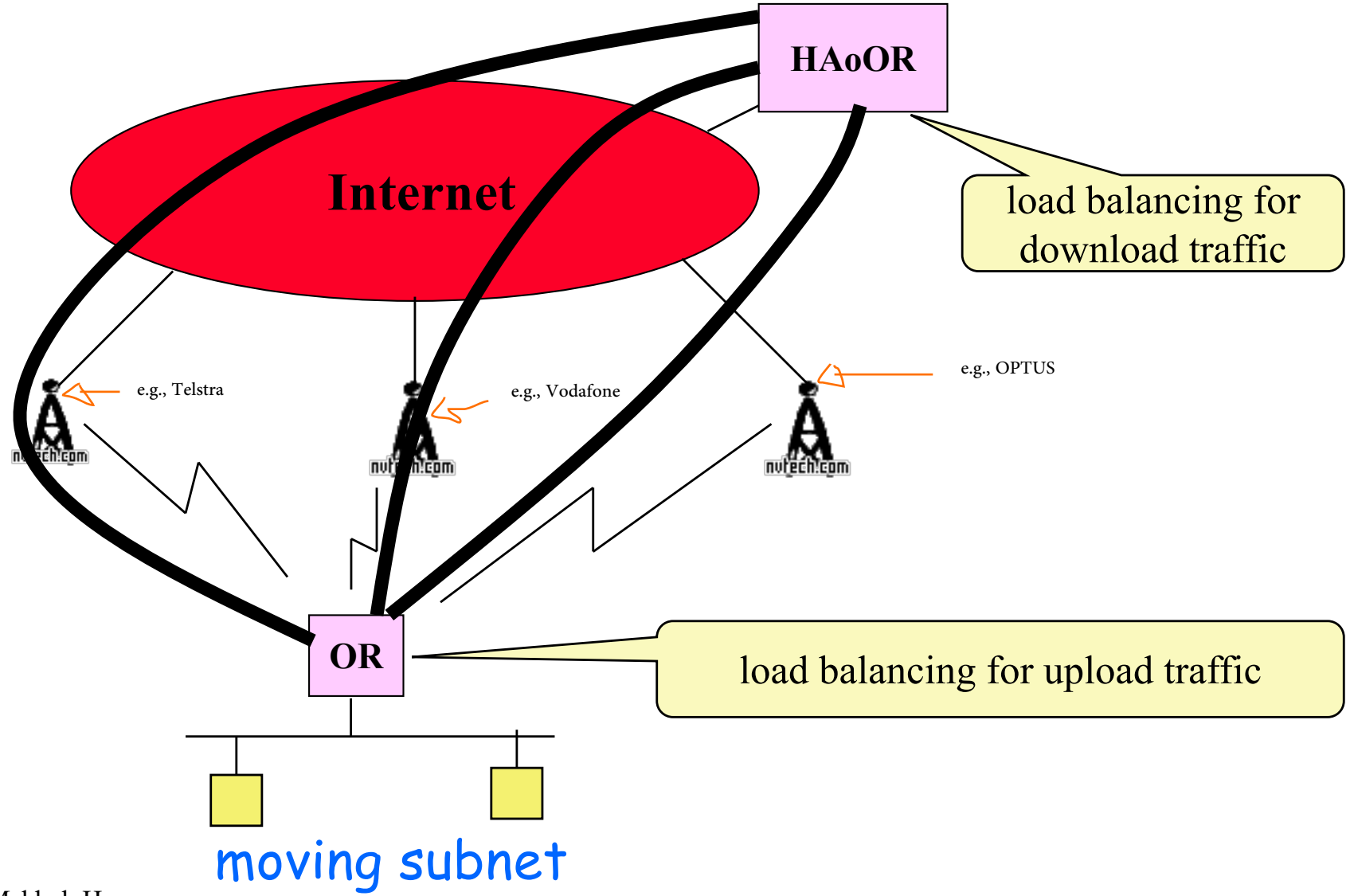
Multihoming with MIP-NEMO

graphical illustration



Multihoming with MIP-NEMO

load balancing



Mobile IPv6 (RFC 3775)

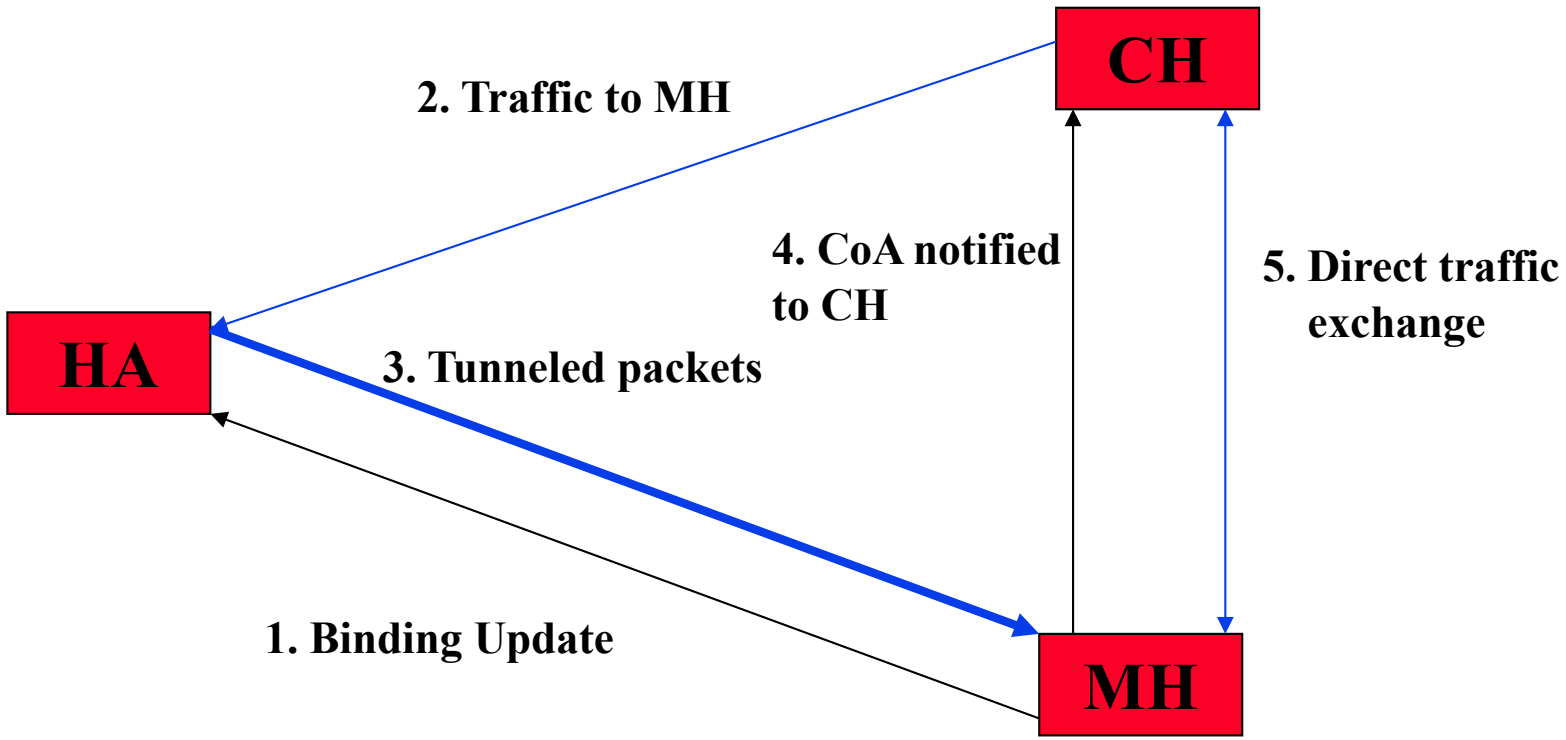
- IPv6 simplifies MIP
- CoA can be achieved through address auto-configuration mechanism of IPv6
  - No need for DHCP
  - There is no need for FA, mobile hosts can operate without any special support
- MIPv6 tries to avoid tunneling as much as possible

implementing Mobile IP in the IPv6 platform is more efficient than it is on the existing IPv4 platforms

Mobile IPv6

- Supports two different modes of operation
- Bidirectional tunneling mode
  - Same as IPv4 with reverse tunneling
  - No support from CH
- Route optimisation mode
  - Binding updates are sent to CHs from MHs
  - From CH→MH, new type of IPv6 routing header(Type 2) is used instead of IP-in-IP encapsulation
  - From MH→CH, new Home address option carries the Home address of MH
  - Each packet now contain both CoA and Home address, ingress filtering routers are now satisfied

Mobile IPv6
illustration



Proxy Mobile IP

Disadvantages of Mobile IP

- User device requires software upgrade
  - Cost
  - Admin overhead (MIP requires kernel support)
  - Population of mobile device may be dynamic (for a large organisation, it may be difficult to keep track which devices need MIP)
  - Security hole: MIP is in the kernel, opening new threats for security for the organisation

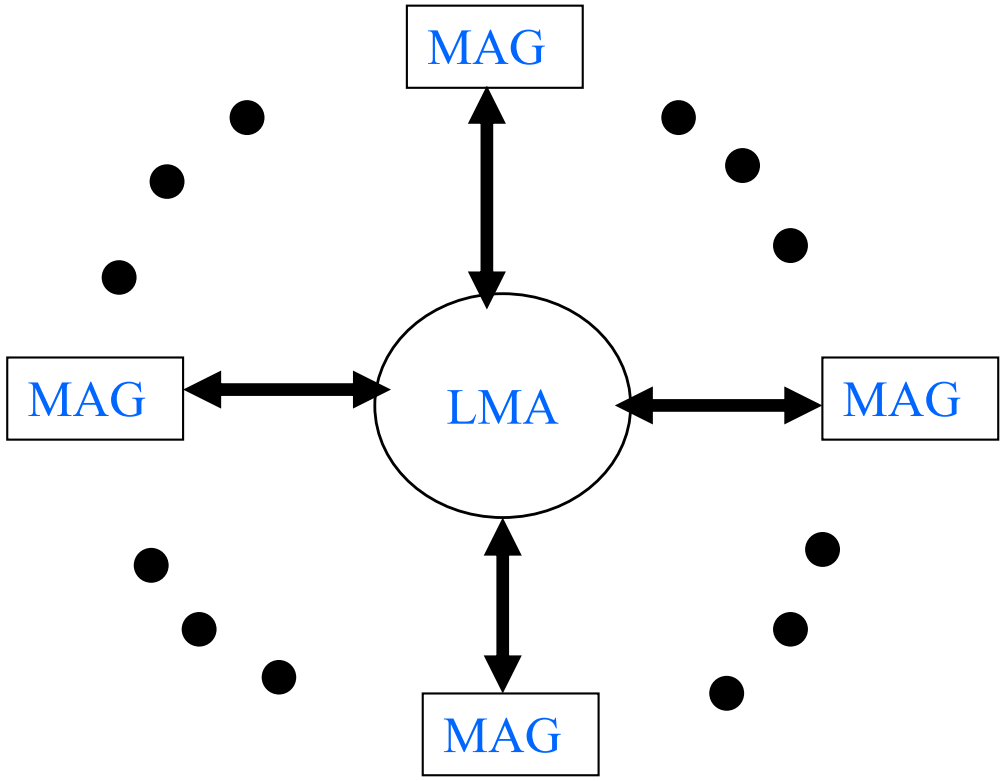
Key features of PMIP

- Seamless mobility across IP subnets within a *local area (campus)*
- No client software needed (totally transparent to the mobile devices)
- Network edge (access point) installs MIP client-proxy to relieve the client
- Support from both Internet and 3GPP:
  - IETF RFC5213 2008 “Proxy Mobile IPv6”
  - Adopted in 3GPP (3G/4G/5G) architectures, such as LTE (mobility management in IP-based mobile core)

PMIP Entities

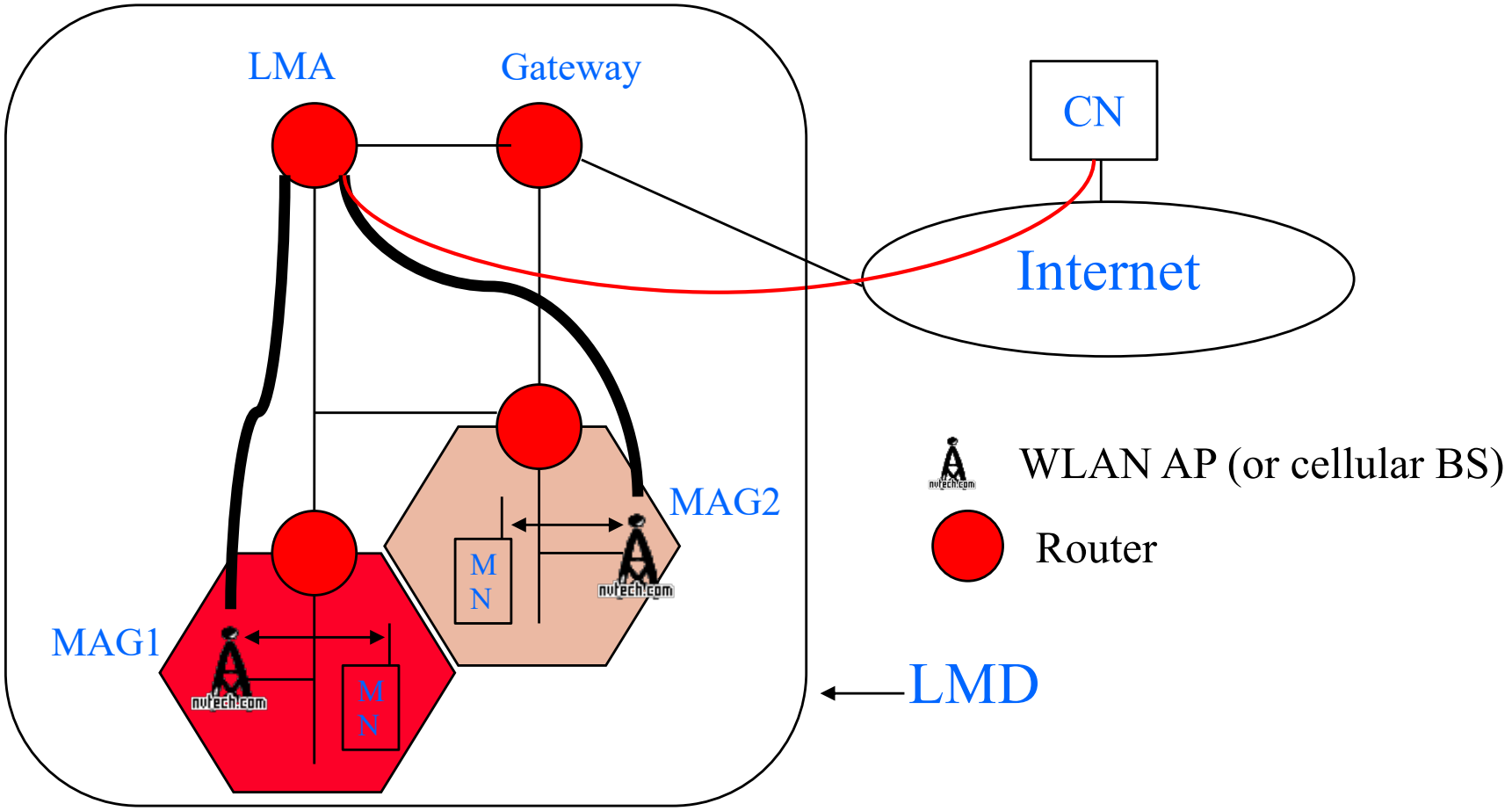
- LMA (local mobility anchor)
  - Only one LMA per local mobility domain (LMD)
  - LMA usually hosted in a router
  - all traffic to and from CN go via LMA
  - Traffic between two MNs in different MAGs go via LMA
  - Two MNs in the *same* MAG *do not* have to via LMA
- MAG (mobile access gateway)
  - Works as a *MIP client proxy* and does the registration with LMA etc.
  - Many MAGs per LMD
  - APs (wireless routers) must be configured to act as MAGs

LMA and MAGs



One LMA opens bi-directional tunnels with many MAGs

PMIP Topology



An example of PMIP operation

1. AP1, connected to subnet1, is configured as MAG1. AP2, connected to subnet2, is configured as MAG2.
2. MN associates with AP1 and obtains an IP address valid for subnet1. MAG1 registers MN's MAC address, IP address, and MAG number with LMA and establishes a bidirectional tunnel between LMA and MAG1. All traffic to and from CN now go via this tunnel.
3. MN moves closer to AP2 and based on signal strength, associates to AP2.
4. After associating with AP2, it starts to send traffic to AP2 with the IP address obtained earlier from subnet1. MAG2 detects that the IP address is from another subnet. MAG2 registers the new MAG (MAG2) for this MN with LMA and establishes a bidirectional tunnel between LMA and MAG2.
5. All traffic to and from CN now follow the new tunnel between LMA and MAG2. The MN is oblivious of the fact that it has moved to a new subnet. Any TCP connections between CN and MN remain intact. The mobility was handled completely by the network without any special actions from the MN.

Summary

1. In the beginning, the Internet was designed for fixed devices. This means that existing TCP sessions will break if the devices moves across subnet boundaries.
2. MIP was designed to support device mobility.
3. MIP is a network layer function, which hides mobility from transport and application layer protocols.
4. MIP requires software upgrades for mobile devices.
5. PMIP was designed later to manage mobility without requiring any software for the mobile devices. With PMIP, all existing mobile devices can enjoy the benefits of MIP without requiring any update.