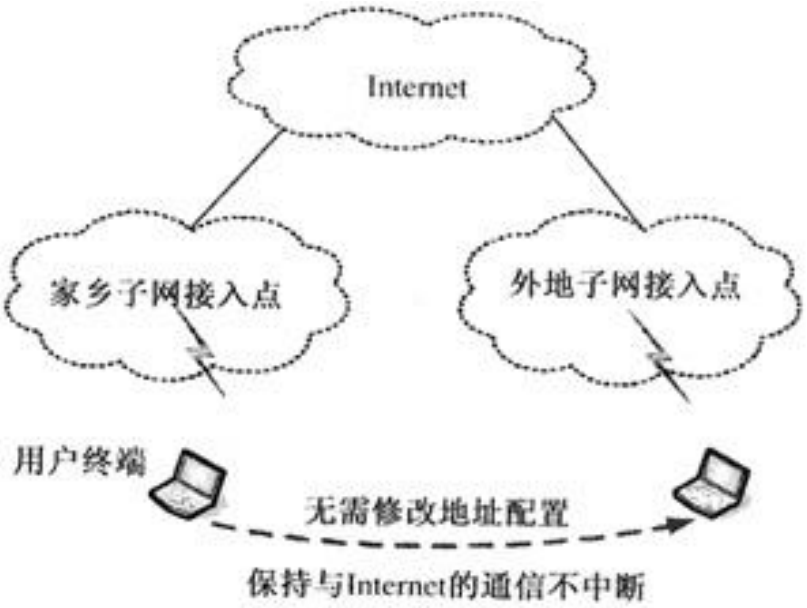
移动IP技术与协议

MIP

- 概述
- MIPv4协议
- MIPv6协议
- 快速切换技术
- 安全技术

网络层移动性管理概述

- **目标**：在Internet上提供移动功能的网络层方案，它可以使移动节点用一个永久的地址与互联网中的任何主机通信，并且在切换子网时不中断正在进行的通信。



网络层移动性管理概述

- **功能**：Internet上移动节点位置变化时，不改变其原有地址，也不必采用特定主机路由，仍然能够保持和其他节点之间的连续通信。

- 移动IP需要满足的要求
  - MN应能与不具备移动IP功能的计算机通信
  - 无论MN连接在哪个数据链路层接入点，它仍能用原来IP地址通信
  - MN改变链路层接入点后，高层连接不中断
  - MN具有较好的安全性

网络层移动性管理协议

- 协议分类
  - 基于主机的移动性管理协议
    - 原理：终端支持相应的协议栈，对终端要求高，终端设计复杂、成本高
    - 典型协议：MIPv4、MIPv6
  - 基于网络的移动性管理协议
    - 原理：移动终端不需要有特殊功能，全部移动性管理功能，如：MN的移动性检测、注册、路由等功能全部由网络完成。
    - 典型协议：PMIPv6

网络层移动性管理相关技术

- 代理ARP技术
- 隧道技术

代理ARP技术

- 代理ARP(Proxy ARP): ARP协议的一个变种
- 功能：通过使用一个主机(通常为路由器)，来作为指定的设备对另一个设备的ARP请求进行应答。
- 优点：子网的变化对主机是透明的
- 缺点
  - 增加了ARP流量
  - 安全问题：ARP欺骗

无偿ARP

- 无偿ARP
  - 无偿发送 ARP 响应,实际上是向网络上的每台主机/设备广播其 IP 到 MAC 的转换。
  - 作用
    - 检查地址重复
    - 更新ARP缓存

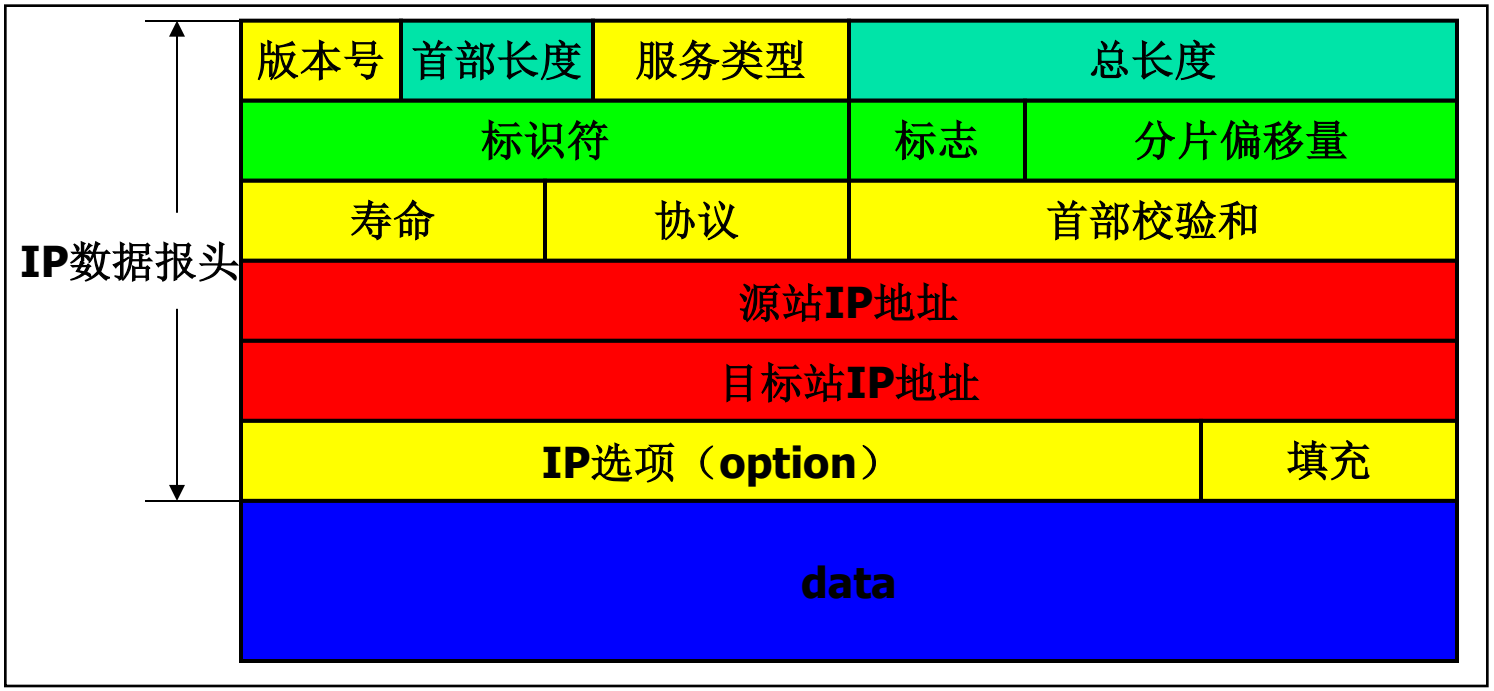
隧道技术

- IP in IP
- 最小封装
- GRE封装

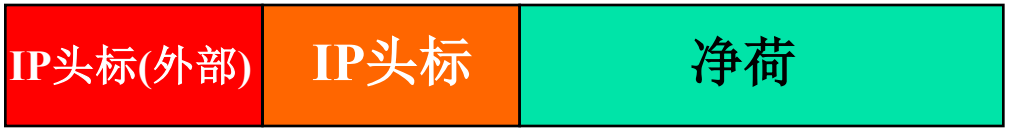
隧道技术-IP in IP

- 是支持Mobile IP的移动节点必须支持的IP协议隧道封装技术
- IETF的RFC2003定义
- 内容
  - 将一个IP数据包做为另一个IP数据包的净荷，形成具有两个IP报头的新的数据包，作为净荷的原始IP包不做任何改动

隧道技术-IP in IP


IP数据报头
版本号
首部长度
服务类型
总长度
标识符
标志
分片偏移量
寿命
协议
首部校验和
源站IP地址
目标站IP地址
IP选项（option）
填充
data


IP头标
净荷


IP头标(外部)
IP头标
净荷

MIP概念

- 产生背景
  - 随着网络技术的不断发展和手提电脑、掌上电脑和各种移动数字设备的广泛应用，在IP网络中实现对移动性的支持变得很重要
  - 蜂窝移动电话的漫游
- 作用

  Mobile IP是一种在全球Internet上提供移动功能的方案，可使移动主机在切换链路时仍保持正在进行的通信

MIP概念

- MIP提供的服务
  - 移动节点在移动时不需要改变IP地址就能收发分组
  - 移动节点在移动时不需要改变相关路由器的路由表信息
  - 移动节点在移动时保持其所正在进行的通信
- MIP目标
  - 操作透明性
  - 性能透明性

MIPv4协议机制

- 相关实体和术语
- MIPv4工作原理与过程

相关实体和术语(1/2)

- 相关实体
  - Mobile IP引入的新功能实体
    - Mobile Node（host or router）移动节点
    - Home Agent（router）本地代理
    - Foreign Agent（router）外地代理
  - Mobile IP涉及的其他功能实体
    - Correspondent Node 通信节点

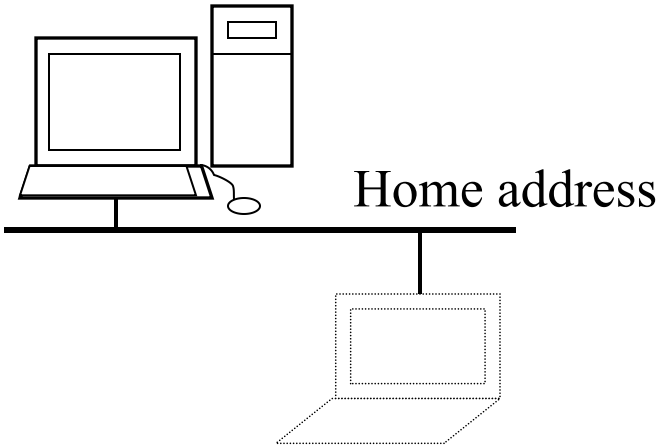
相关实体和术语(2/2)

- 相关术语
  - 本地地址（Home Address）
  - 转交地址（Care-Of-Address）
  - 位置注册（Registration）
  - 代理发现（Agent Discovery）
  - 隧道（tunnel）

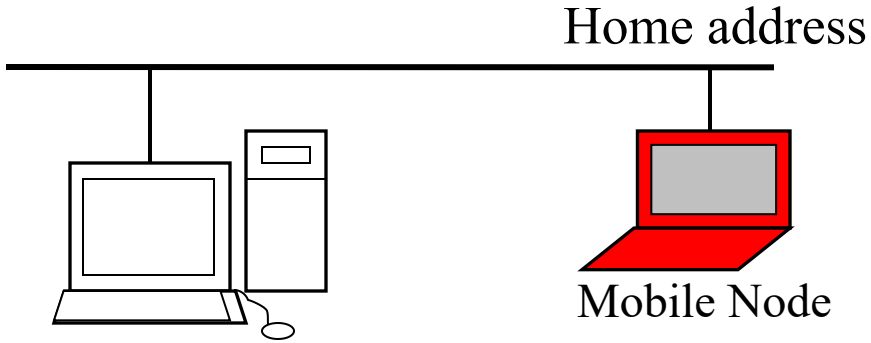
MIPv4工作原理与过程

- Mobile IP协议的内容包括
  - 移动性管理
  - 移动节点的数据传输

MIPv4工作原理与过程

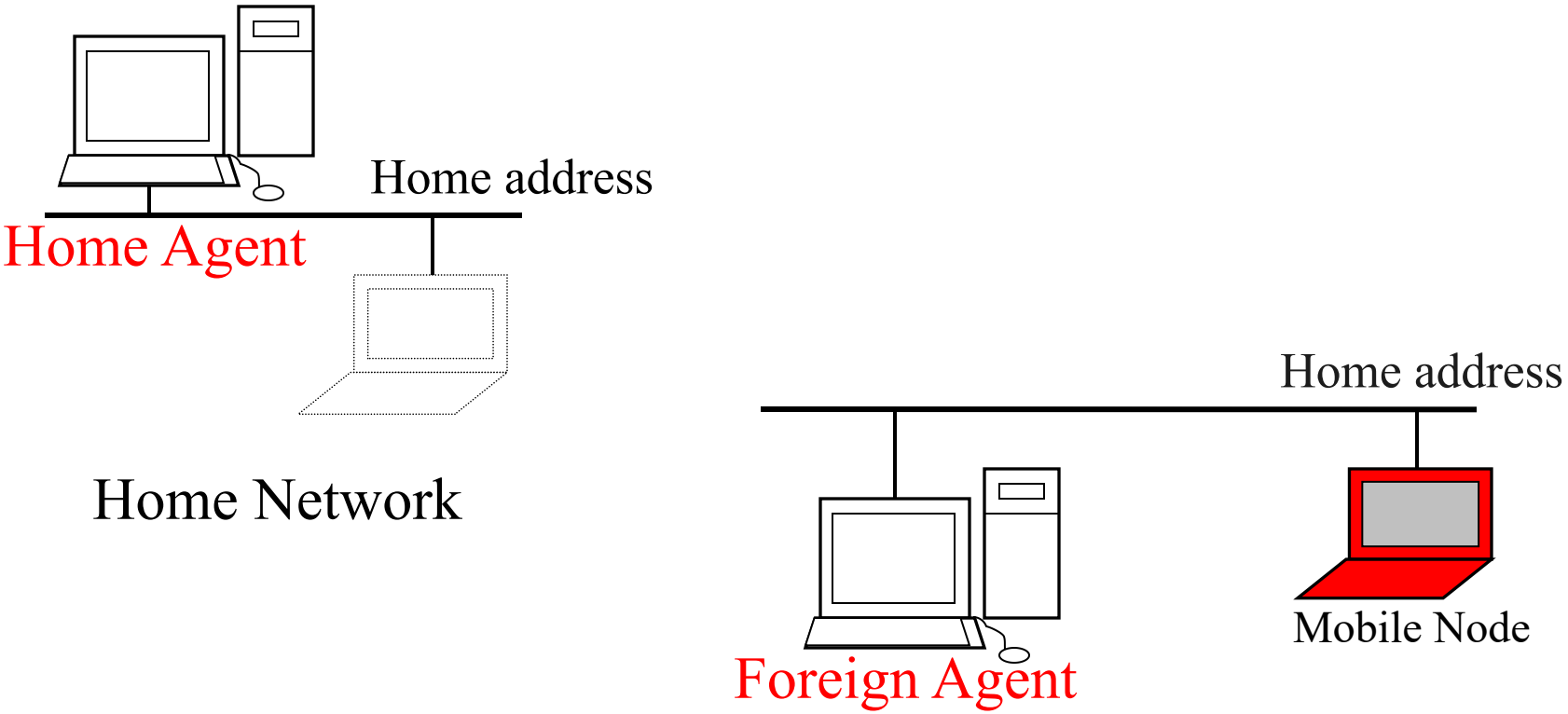


Home Network

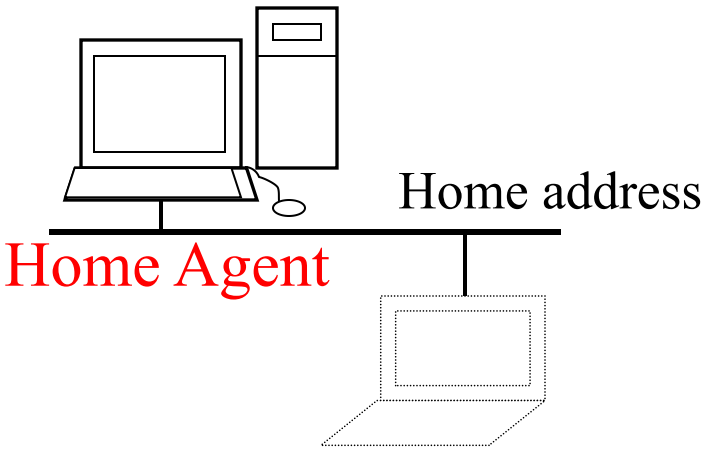


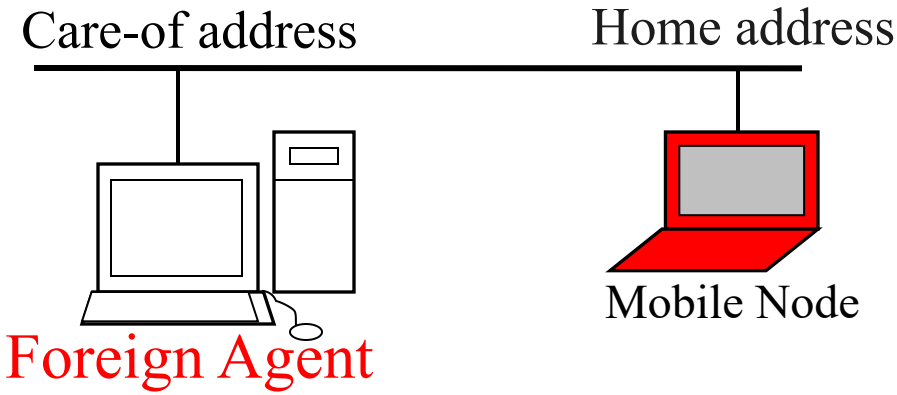
Foreign Network

MIPv4工作原理与过程

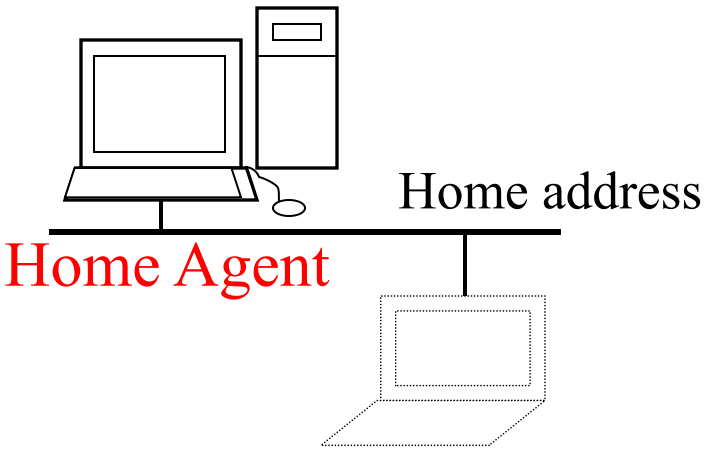


MIPv4工作原理与过程

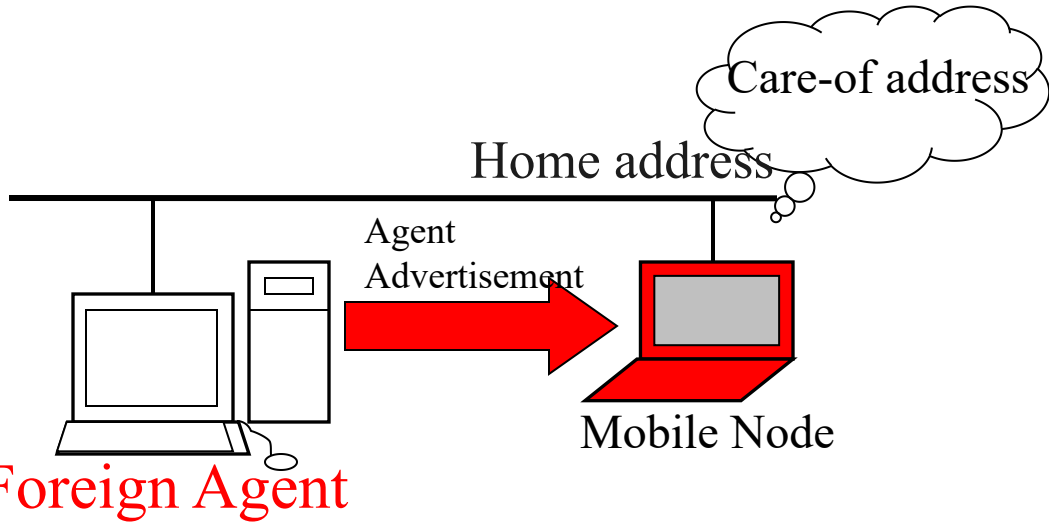




MIPv4工作原理与过程

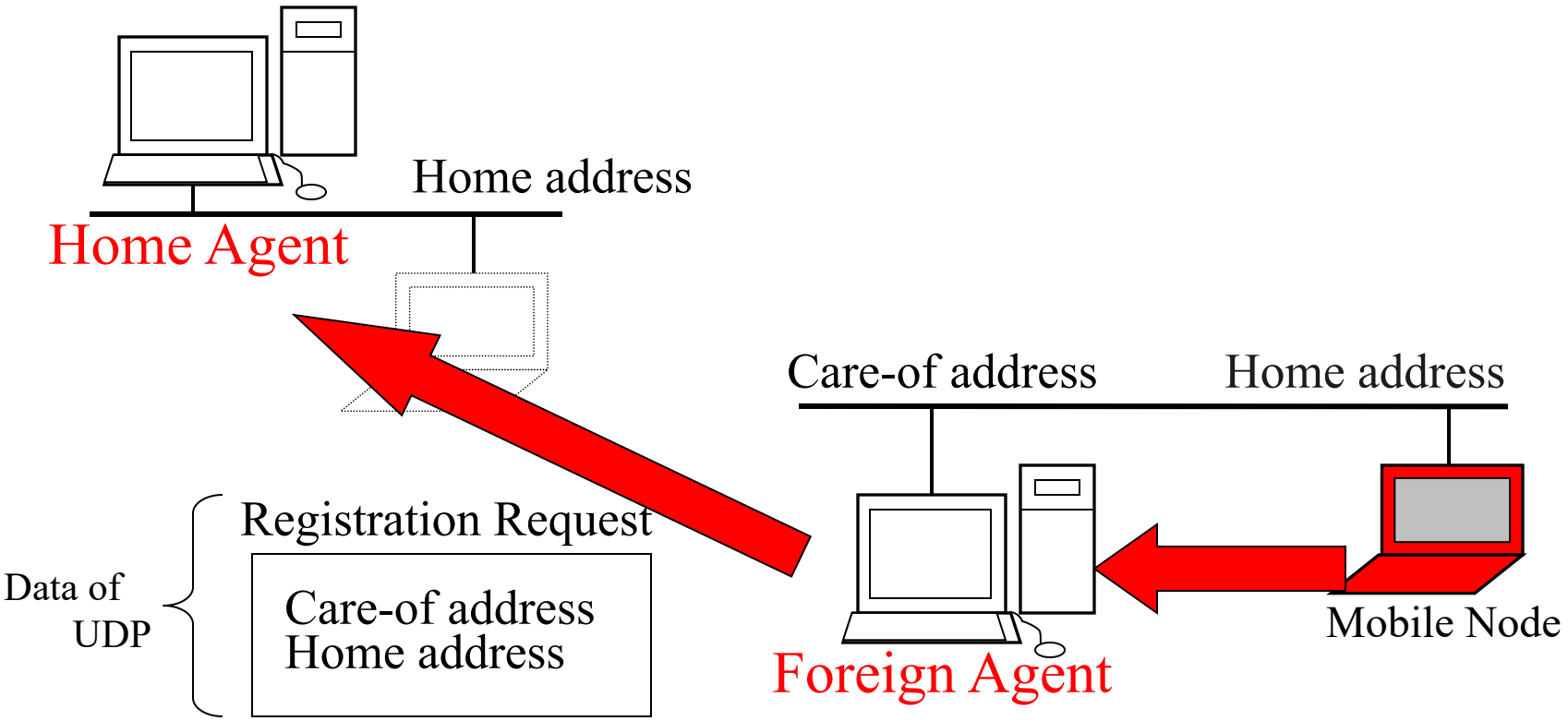


Home Network

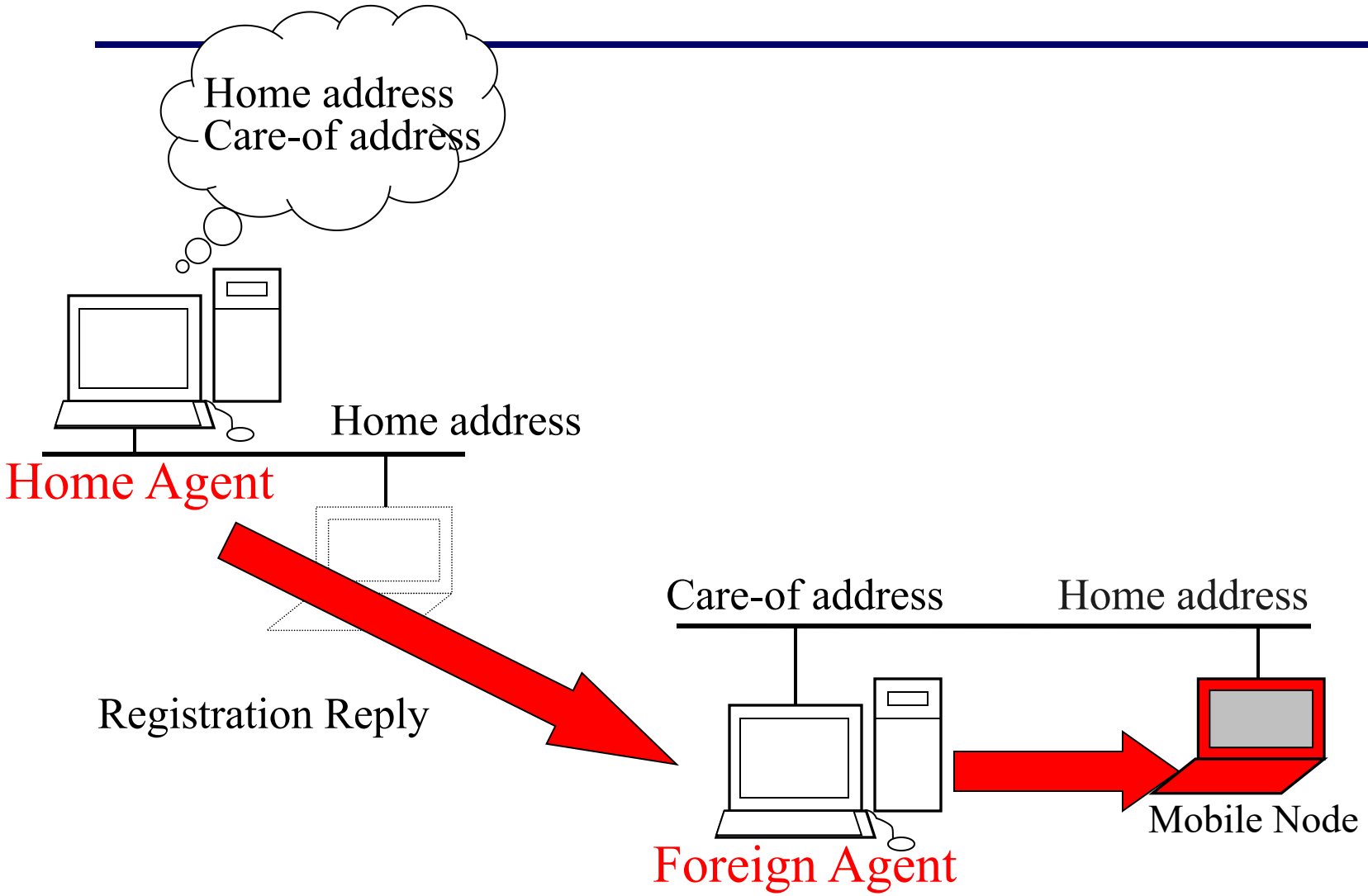


Foreign Network

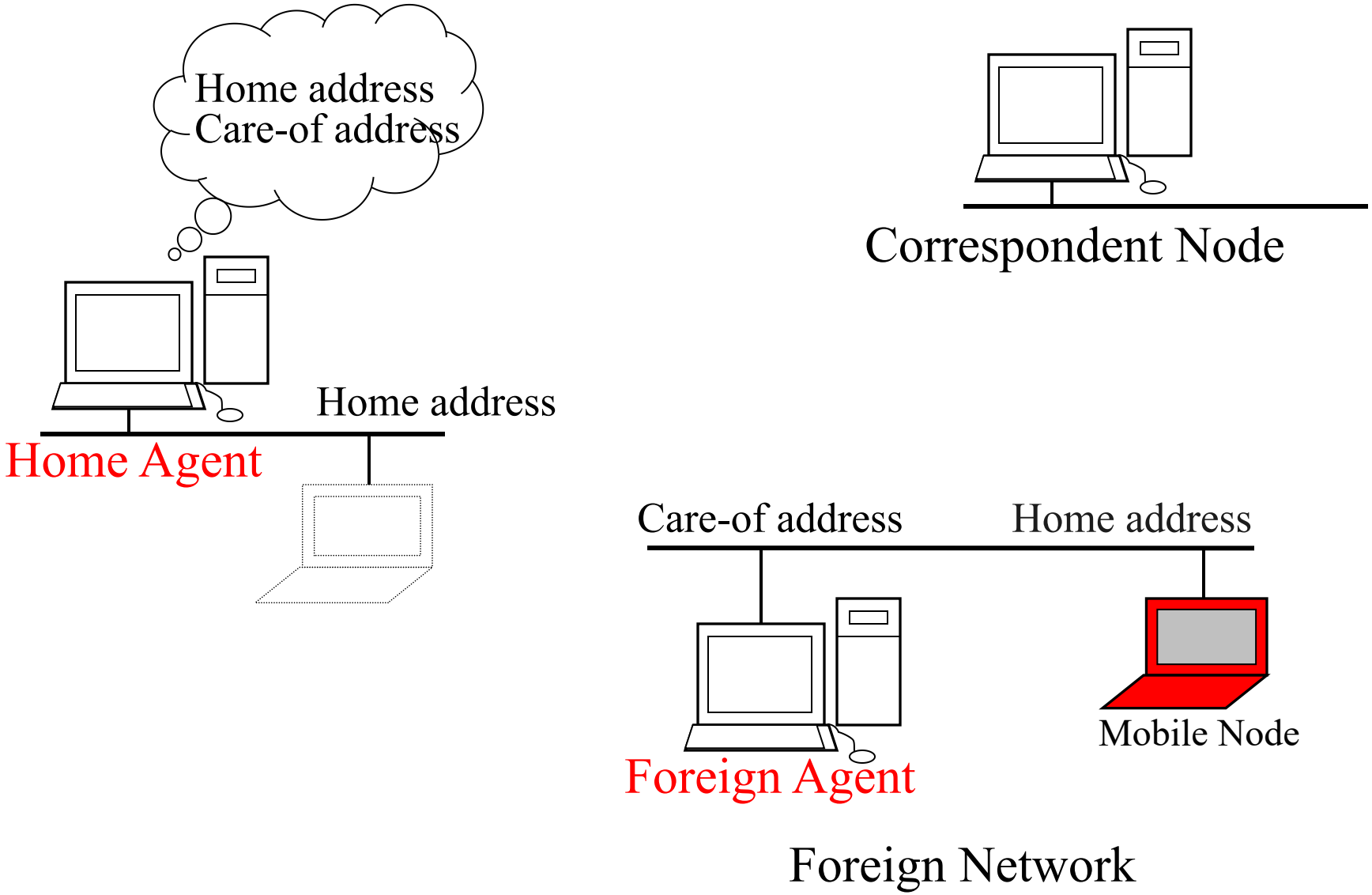
MIPv4工作原理与过程



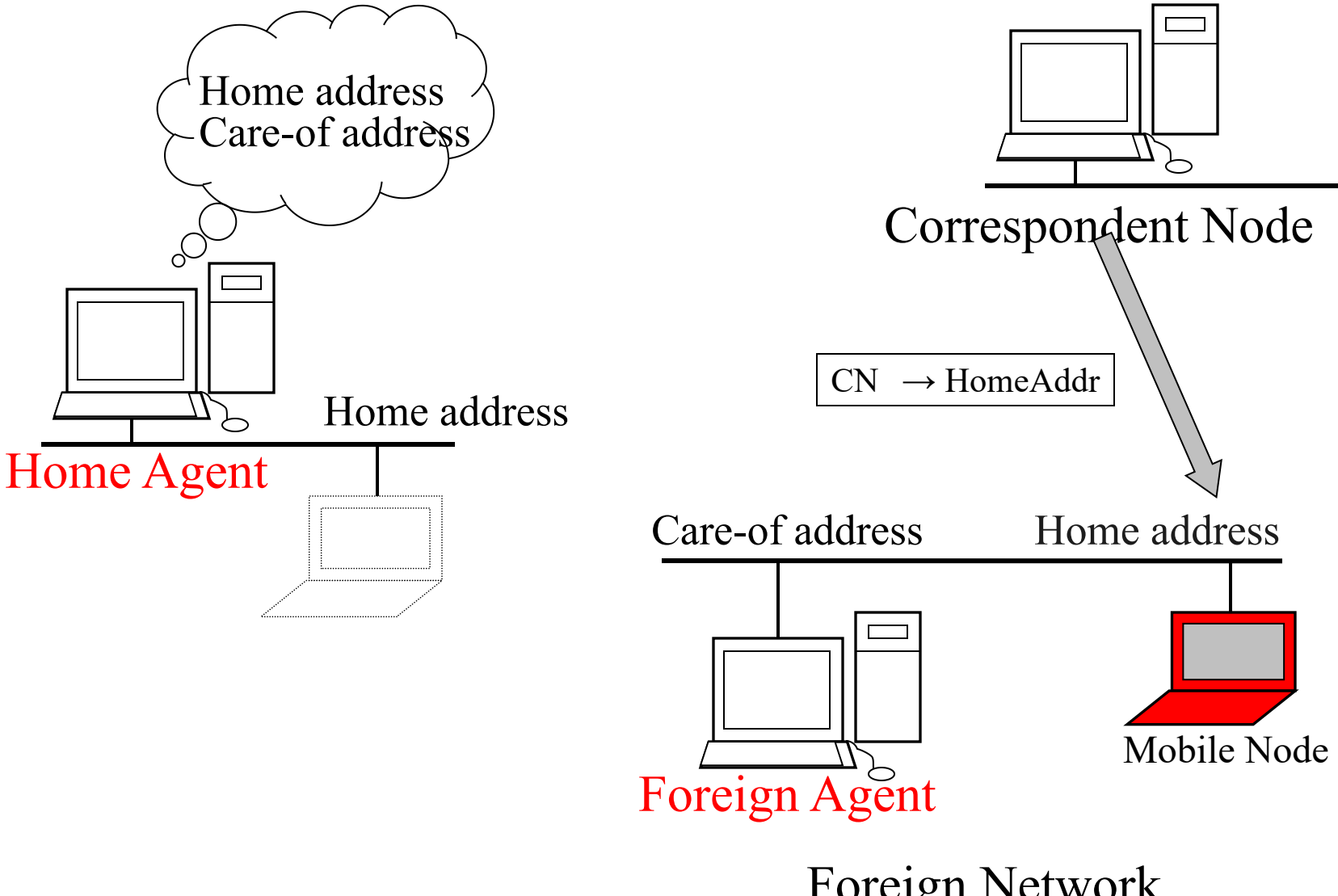
MIPv4工作原理与过程



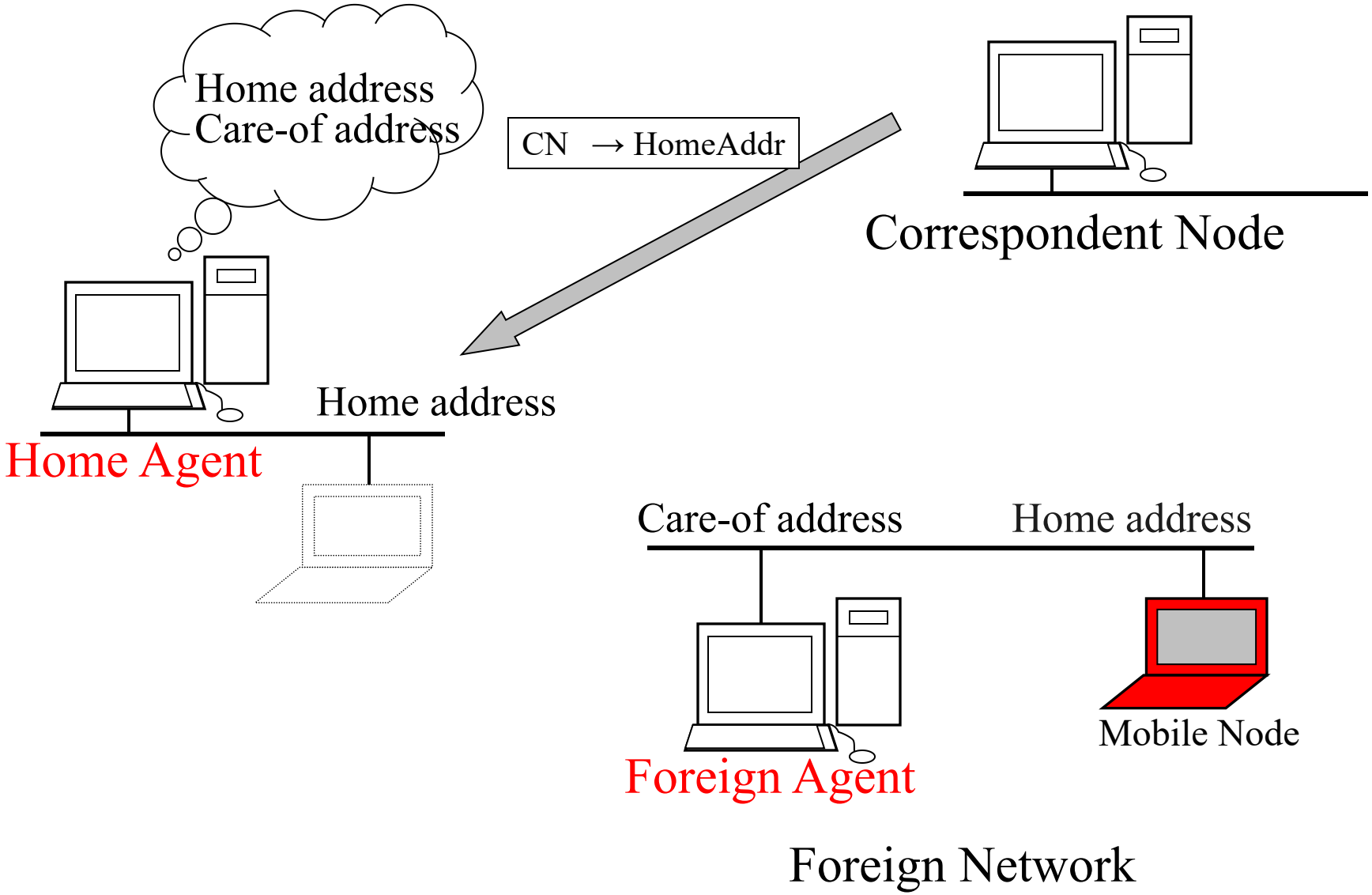
MIPv4工作原理与过程



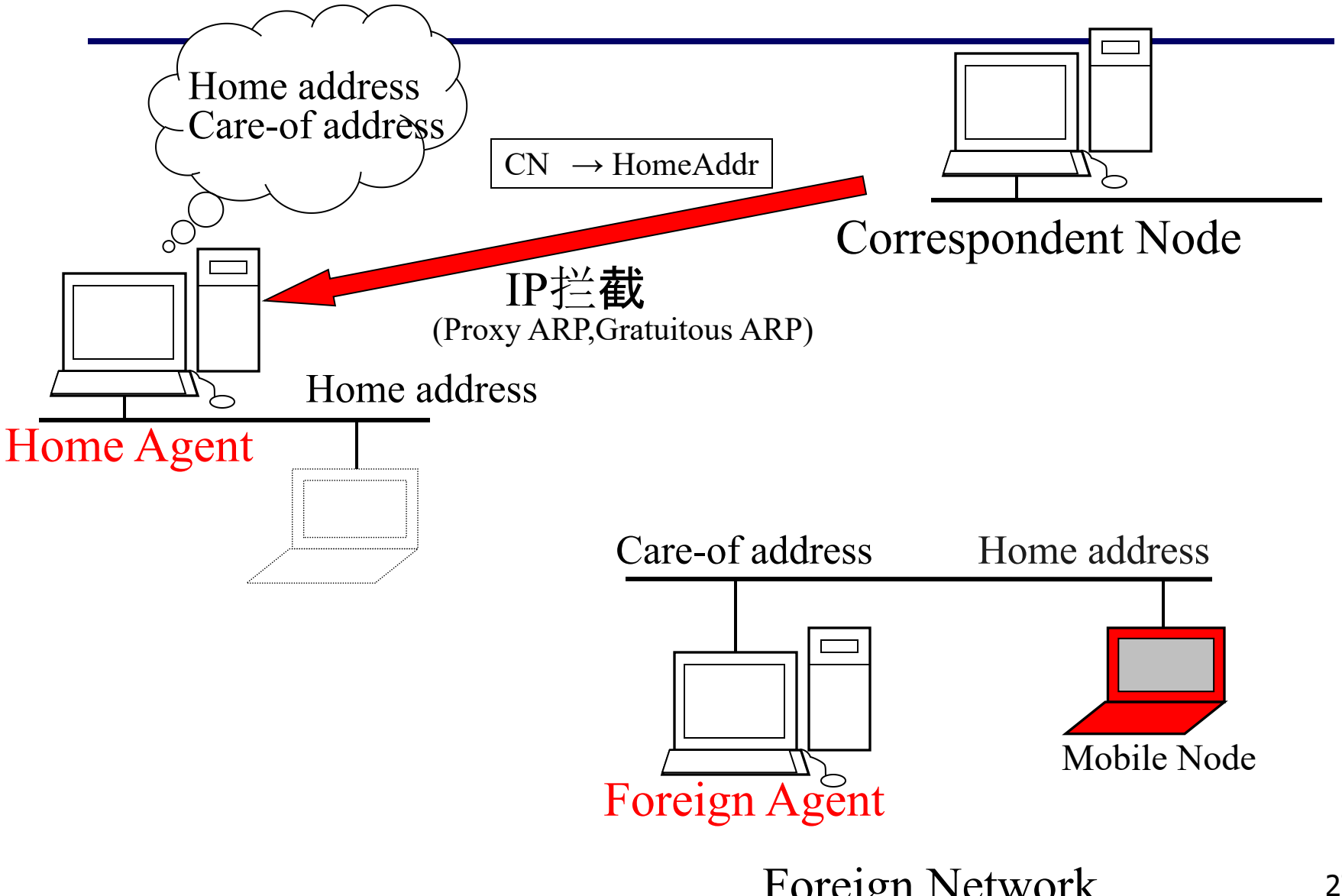
MIPv4工作原理与过程



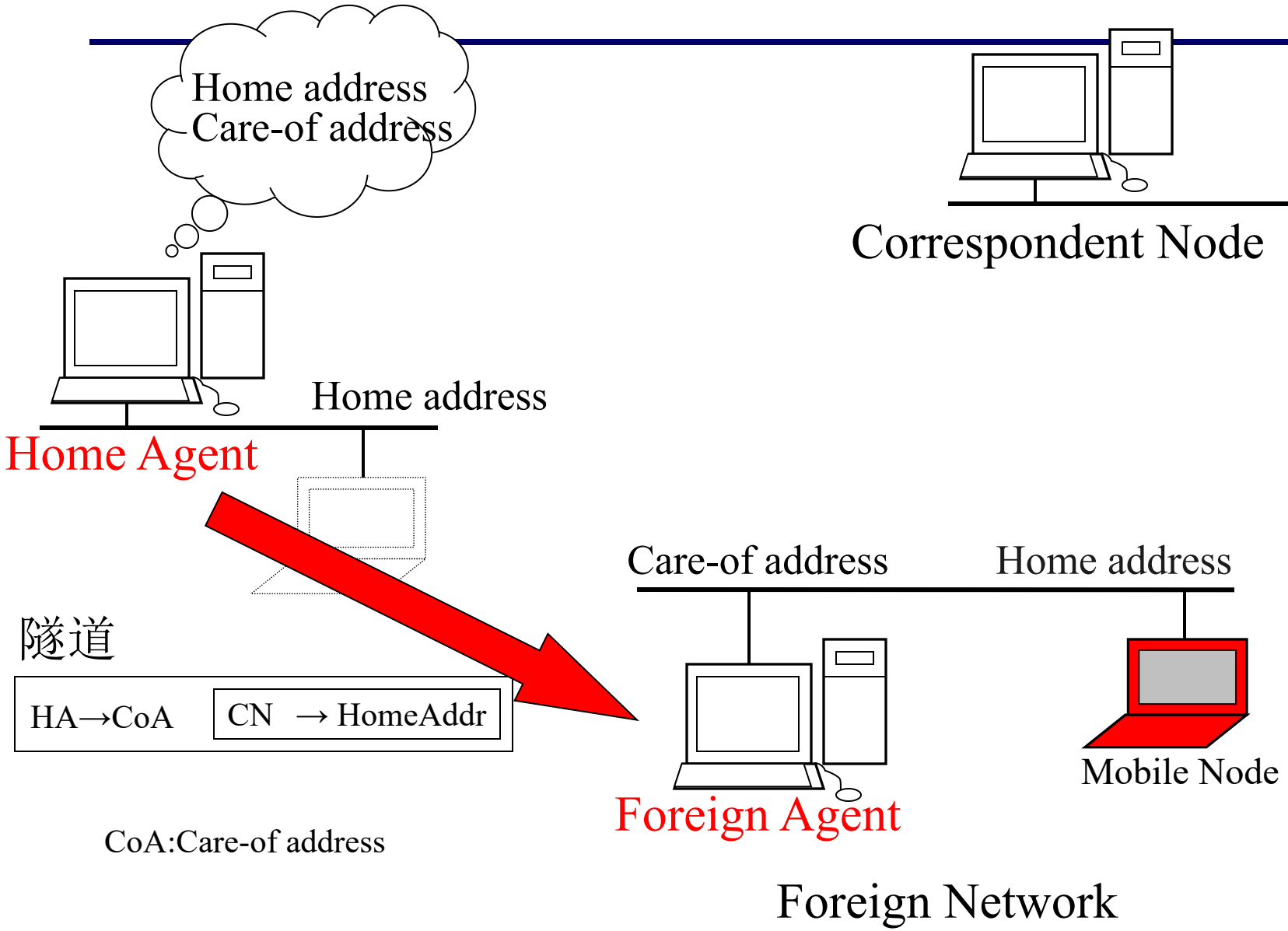
MIPv4工作原理与过程



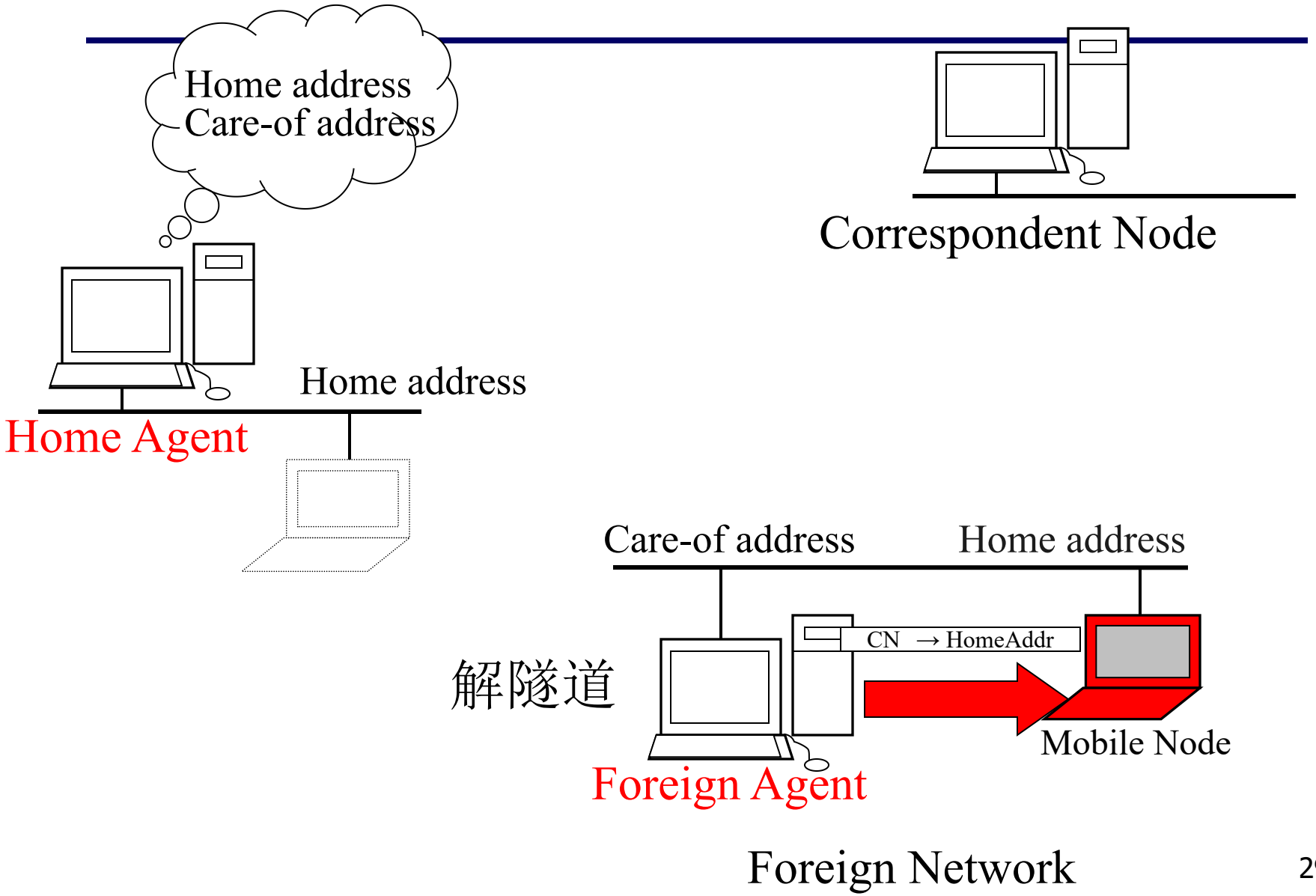
MIPv4工作原理与过程



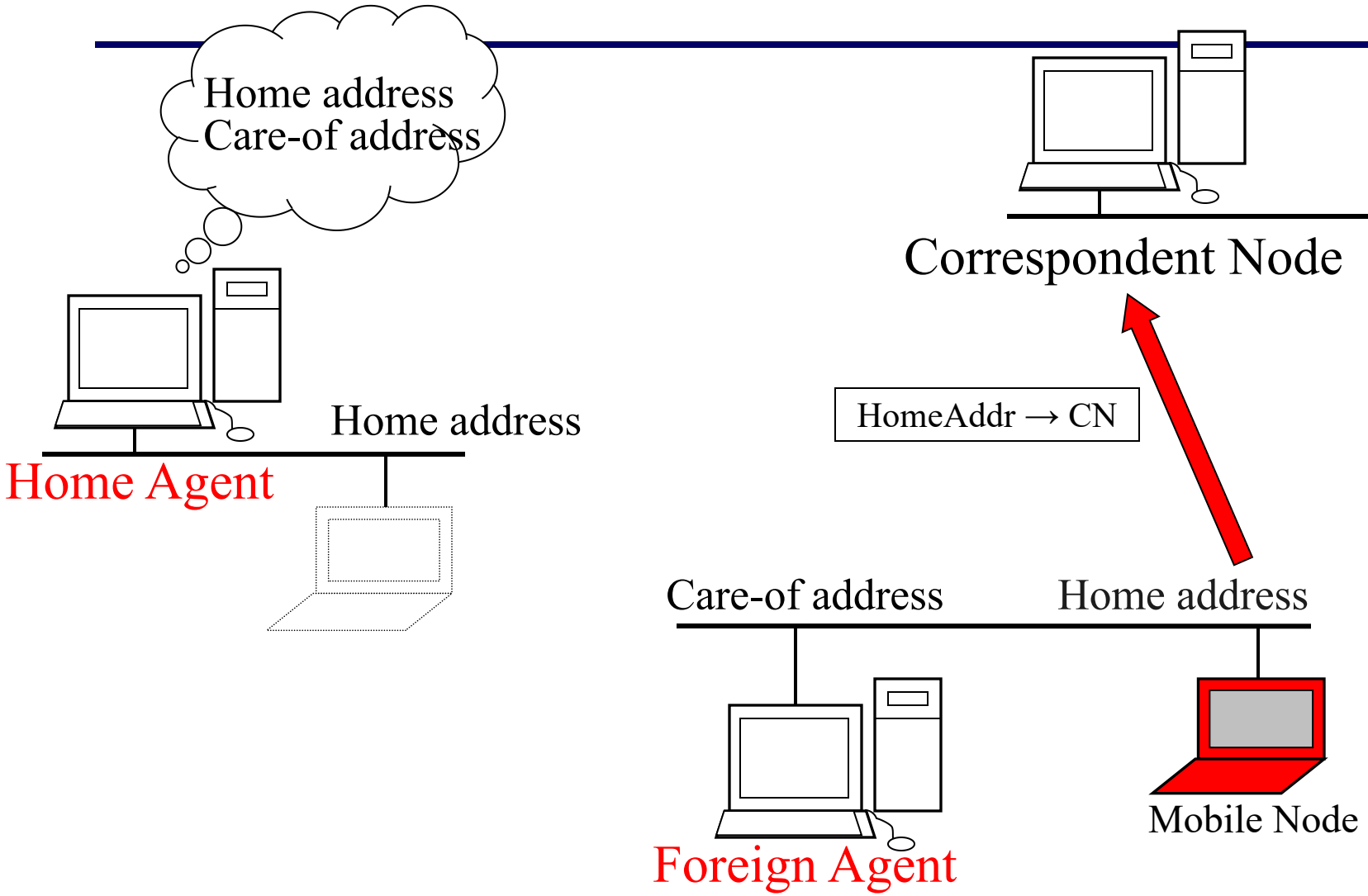
MIPv4工作原理与过程



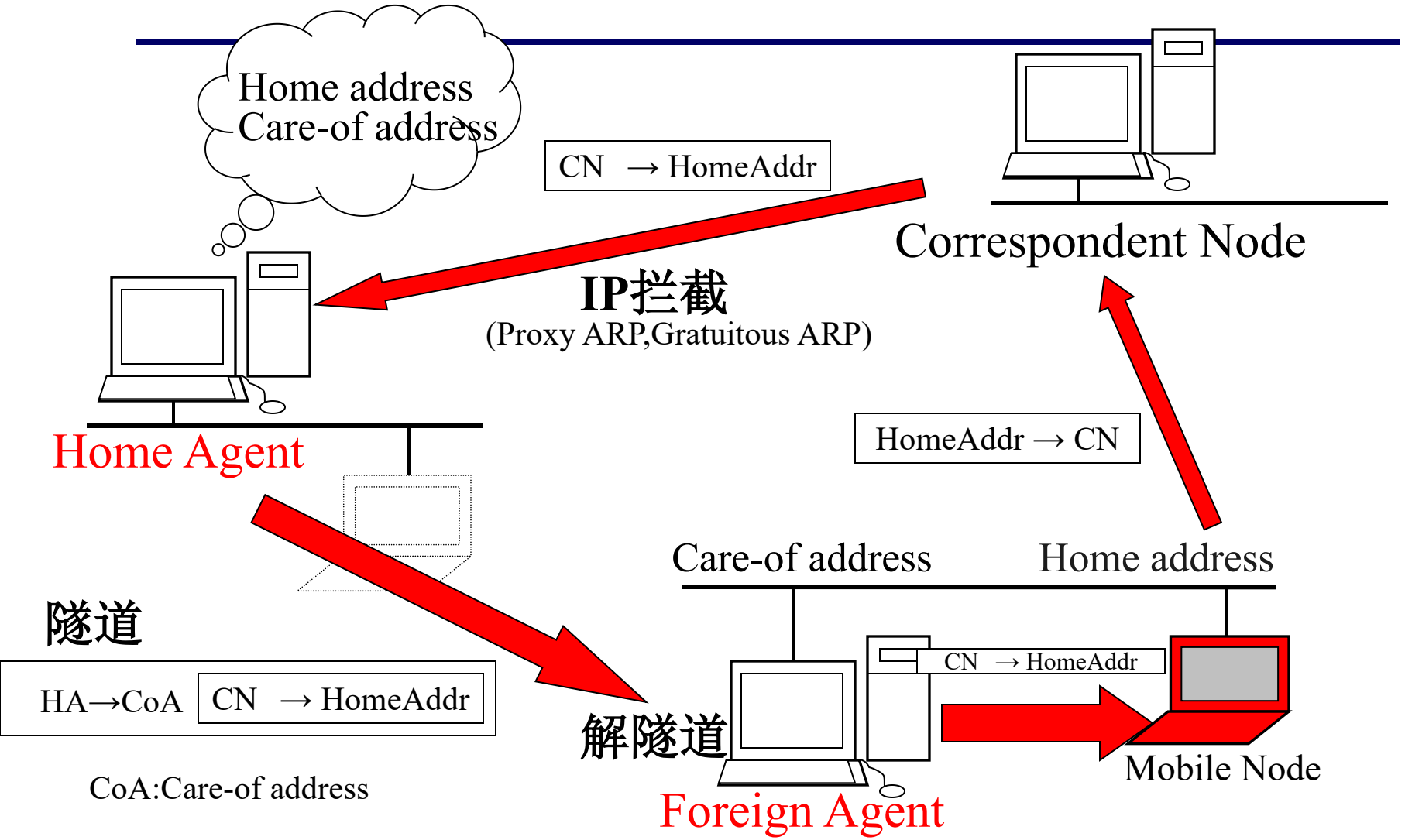
MIPv4工作原理与过程



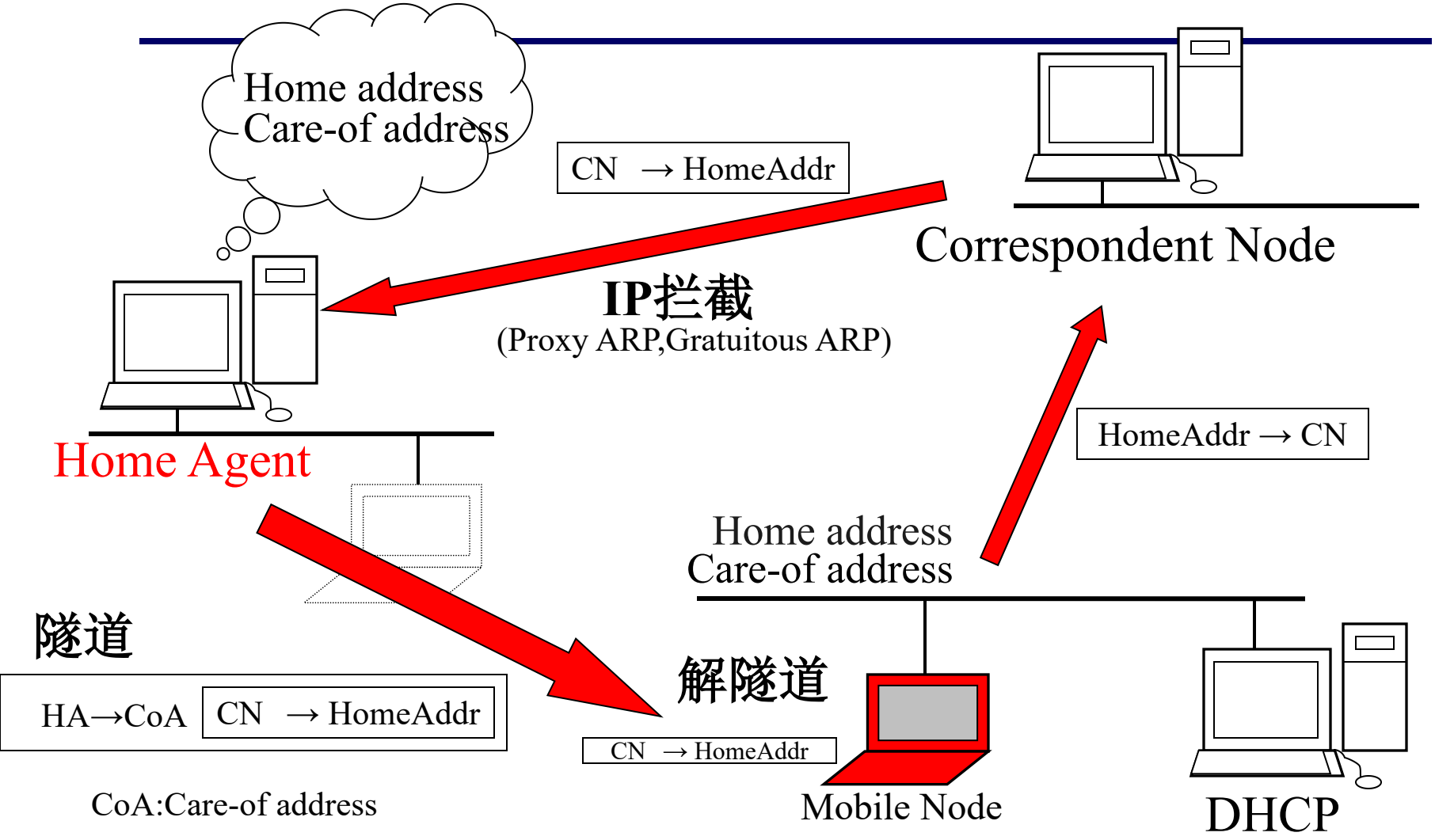
MIPv4工作原理与过程



MIPv4工作原理与过程



MIPv4工作原理与过程



MIPv4的基本工作过程

- 移动代理通过代理公告报文通告它的存在，一个移动节点可选择地通过发送代理请求报文获取代理公告报文
- 移动节点根据获取的代理公告报文判断出自己是在本地网络还是在外地网络
- 当移动节点检测到它在本地网络时，则不需要移动服务，如果它从外地漫游回来，则应该向本地代理注销以前的漫游注册信息

MIPv4的基本工作过程

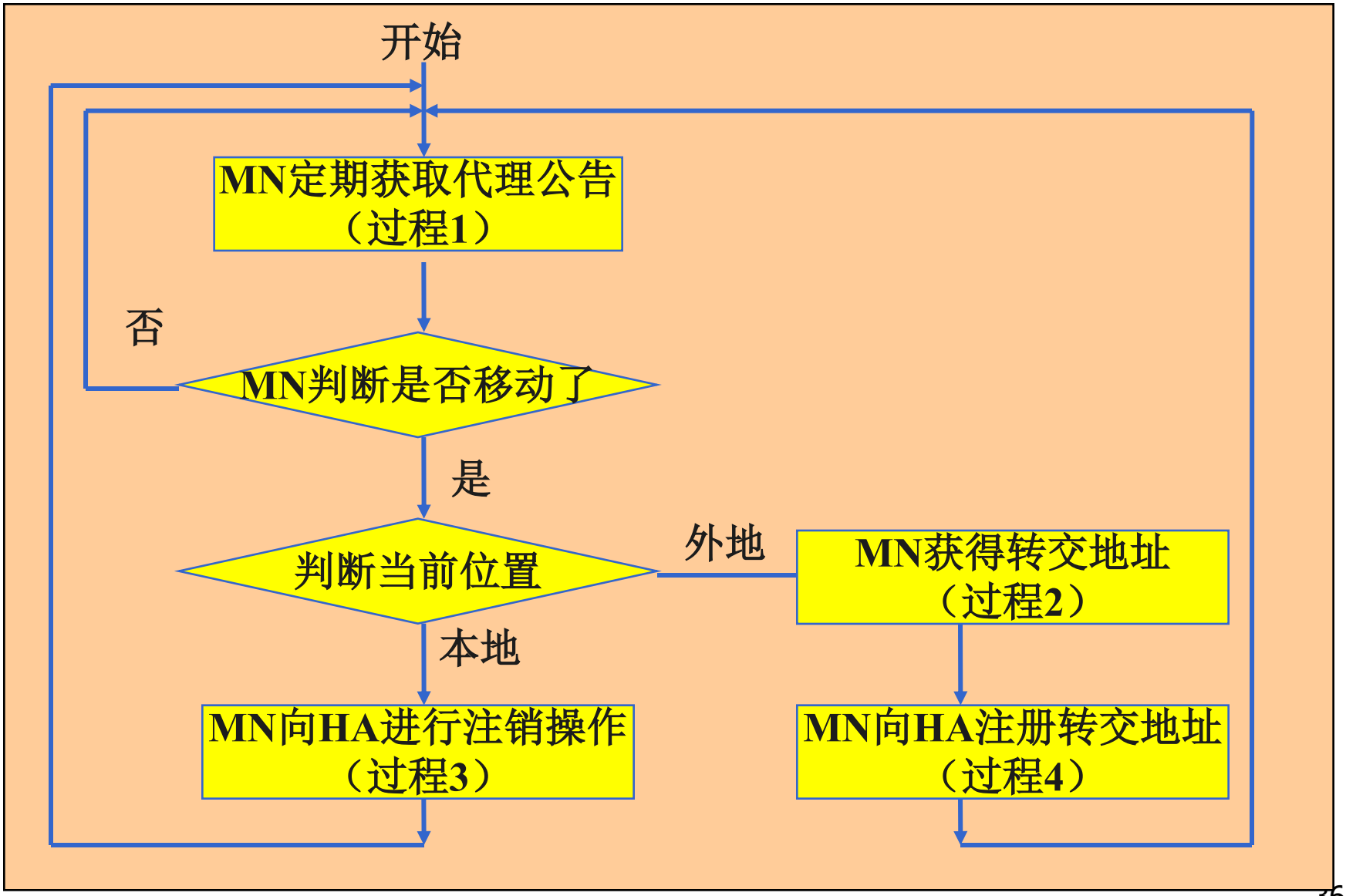
- MN检测到自己已经漫游到外地网络，则在外地网络上获得一个转交地址

- MN离开本地网络后，通过发送注册请求和接收注册响应报文，向它的本地代理注册它的转交地址（可通过它的外地代理完成，也可由移动节点直接完成）

MIPv4的基本工作过程

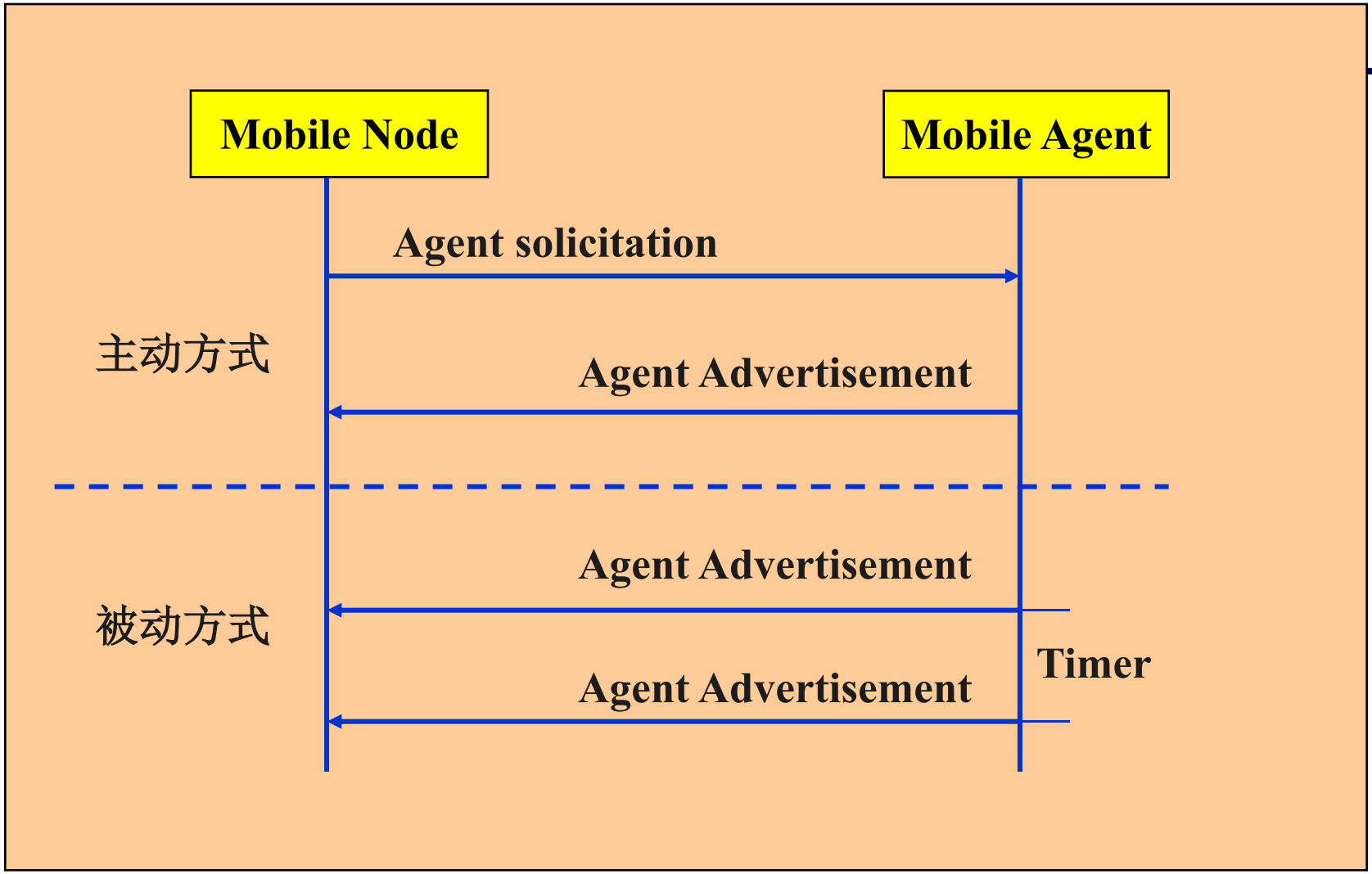
- 发往MN本地地址的分组被它的本地代理拦截，经隧道技术封装后发往 MN的转交地址，在隧道尽头拆封后转交给MN

- 在相反方向，当MN发送分组时，它使用标准的IP路由机制，无须本地代理的介入


开始
MN定期获取代理公告
（过程1）
否
MN判断是否移动了
是
判断当前位置
外地
MN获得转交地址
（过程2）
本地
MN向HA进行注销操作
（过程3）
MN向HA注册转交地址
（过程4）

过程1：MN获取代理公告

- MN可以通过两种方法获取移动代理公告
  - 被动获得方式：周期性地接收移动代理主动发送的代理公告
  - 主动获得方式：主动发送移动代理请求消息来立即获得代理公告

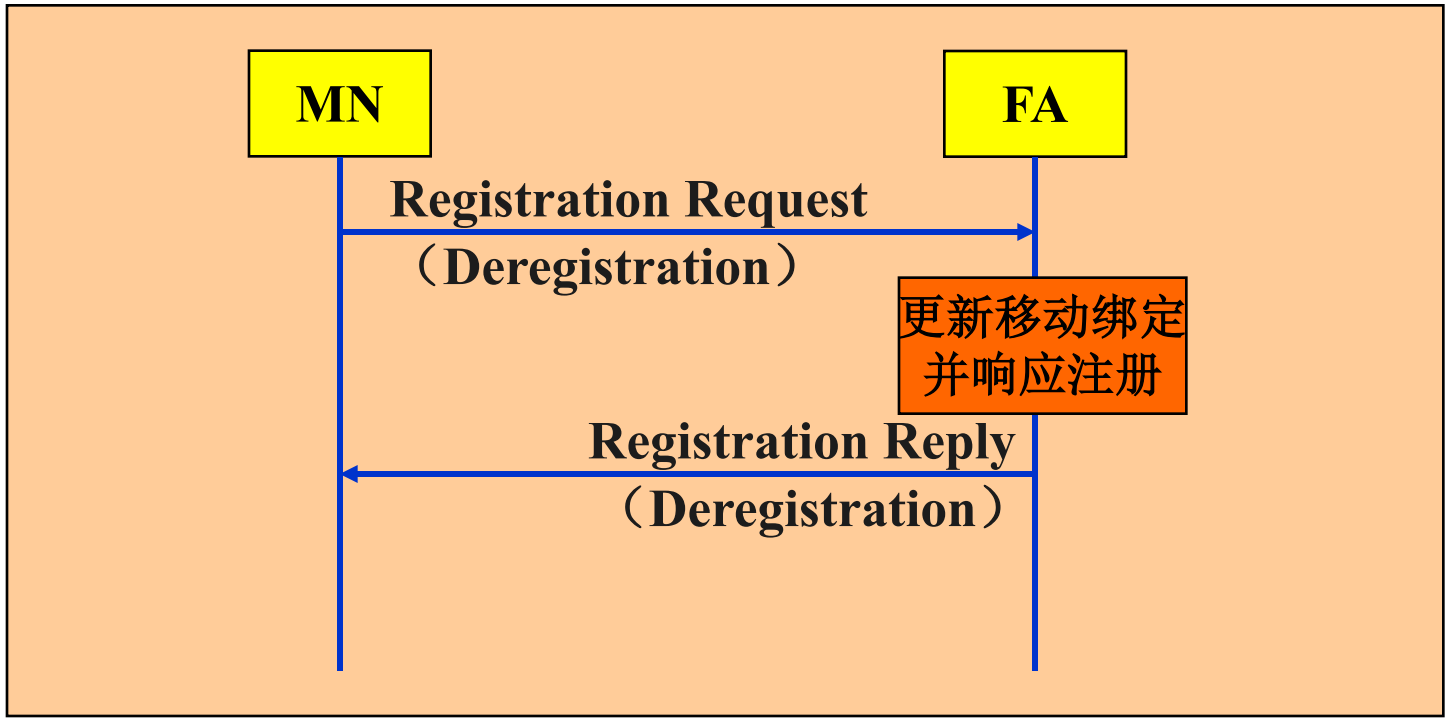

Mobile Node
Mobile Agent
Agent solicitation
主动方式
Agent Advertisement
Agent Advertisement
被动方式
Timer
Agent Advertisement

过程2：MN获得转交地址

- Mobile IP定义了两种模式获得转交地址
  - “外地代理转交地址”是由外地代理通过代理公告报文提供的一个转交地址（该转交地址就是外地代理的IP地址）
  - “配置转交地址”是MN通过其他方法获得的转交地址（该模式不需要外地代理）

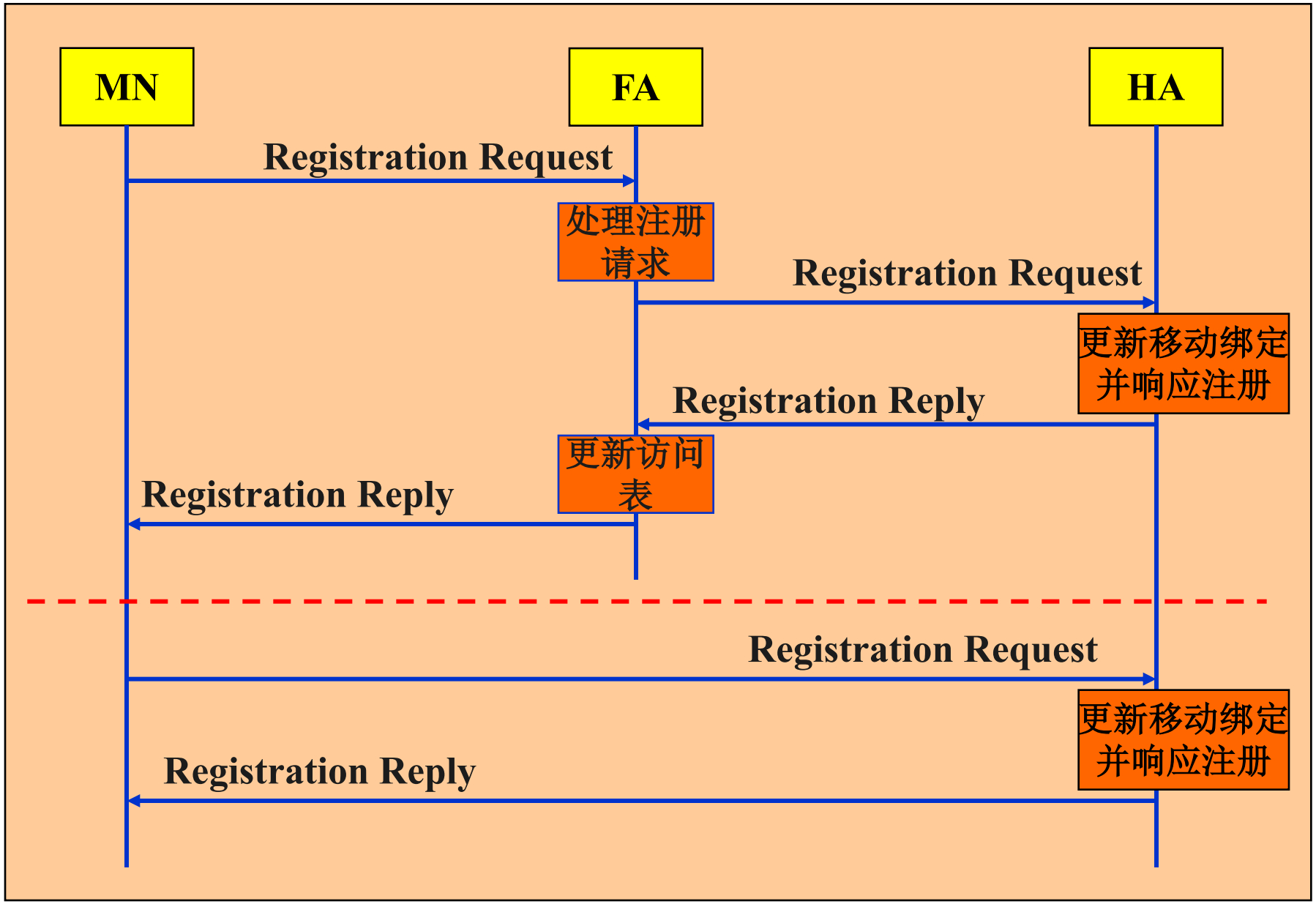
过程3：MN向HA进行注销

- 当MN返回到本地后，需要向本地代理进行注销，操作如下：



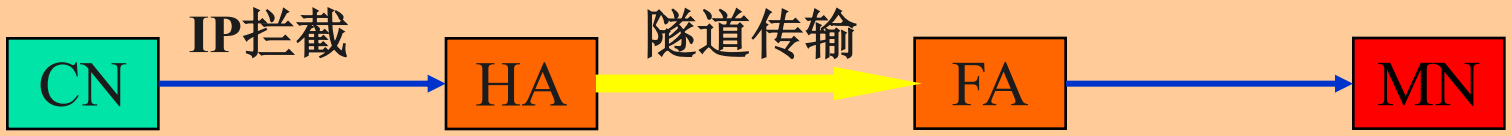
过程4：MN向HA注册转交地址

- Mobile IP定义了两种注册过程
  - MN通过外地代理向MN的本地代理注册
    （适用条件：使用外地代理转交地址）
  - MN直接向MN的本地代理注册
    （适用条件：使用配置转交地址）


MN
FA
HA
Registration Request
处理注册请求
Registration Request
更新移动绑定并响应注册
Registration Reply
更新访问表
Registration Reply
Registration Request
更新移动绑定并响应注册
Registration Reply

移动节点接收IP数据报过程

- 使用外地代理转交地址

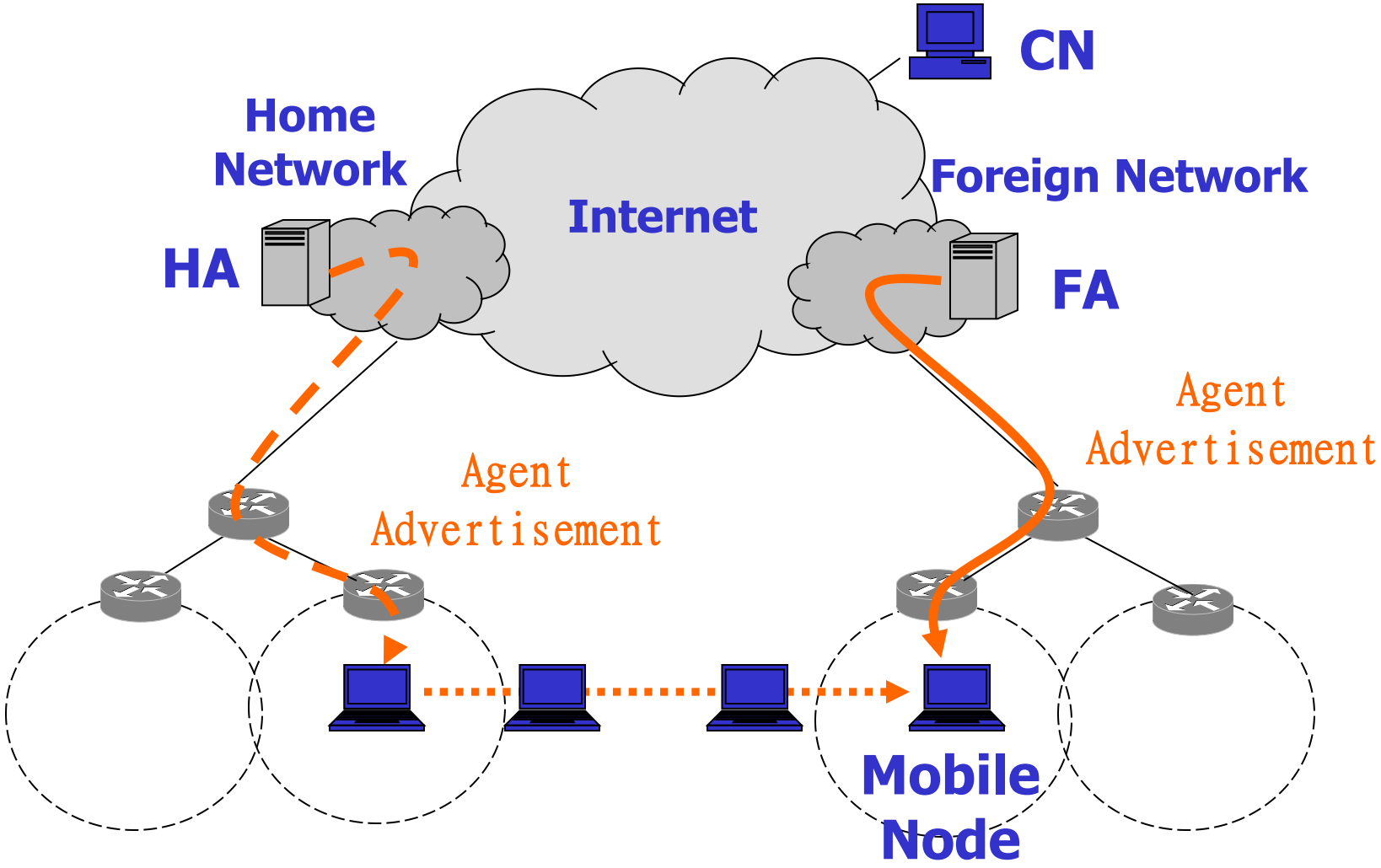


- 使用配置转交地址

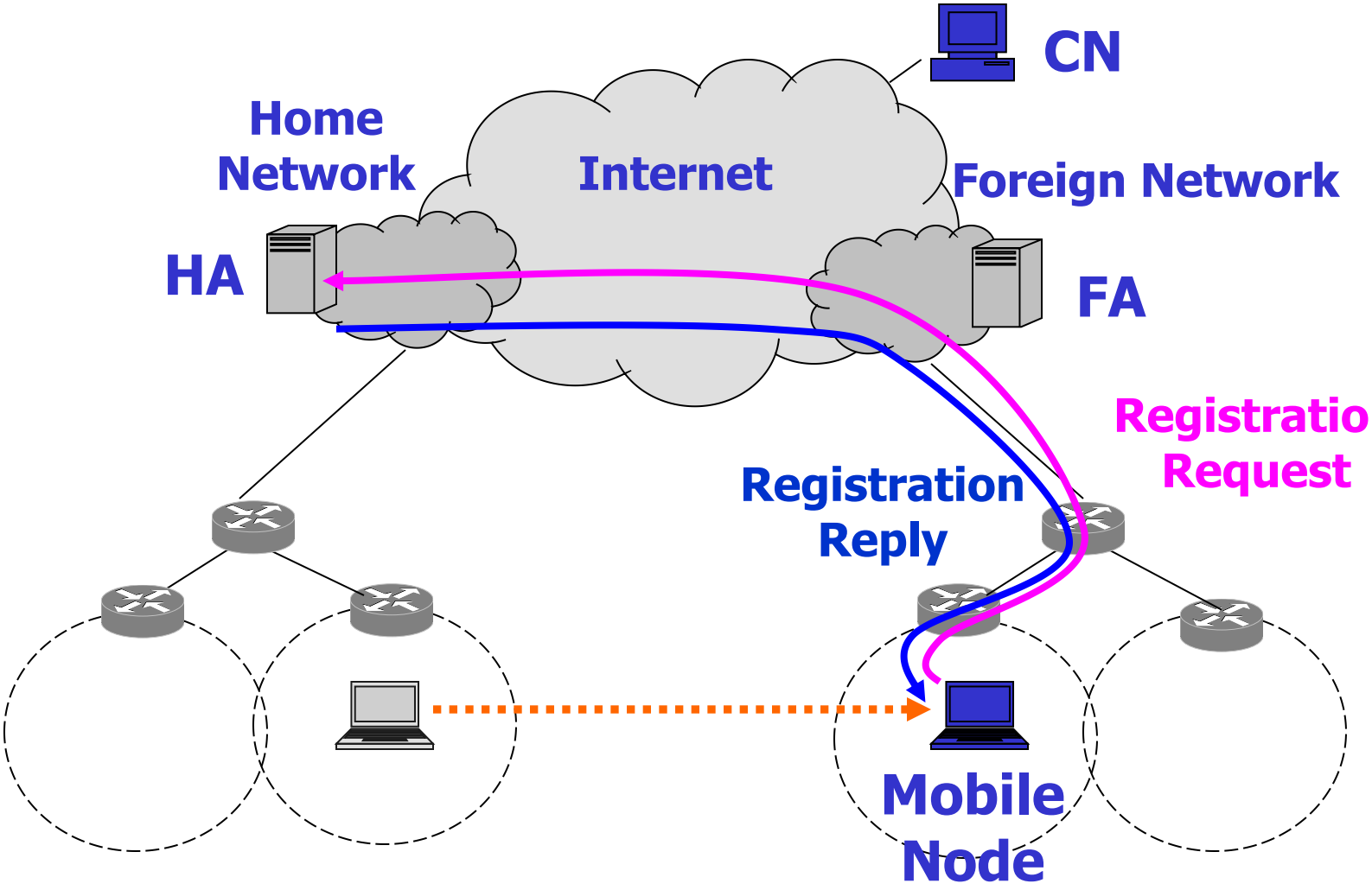
- 移动节点发送IP数据报过程

  移动节点采用标准的IP协议发送IP数据报

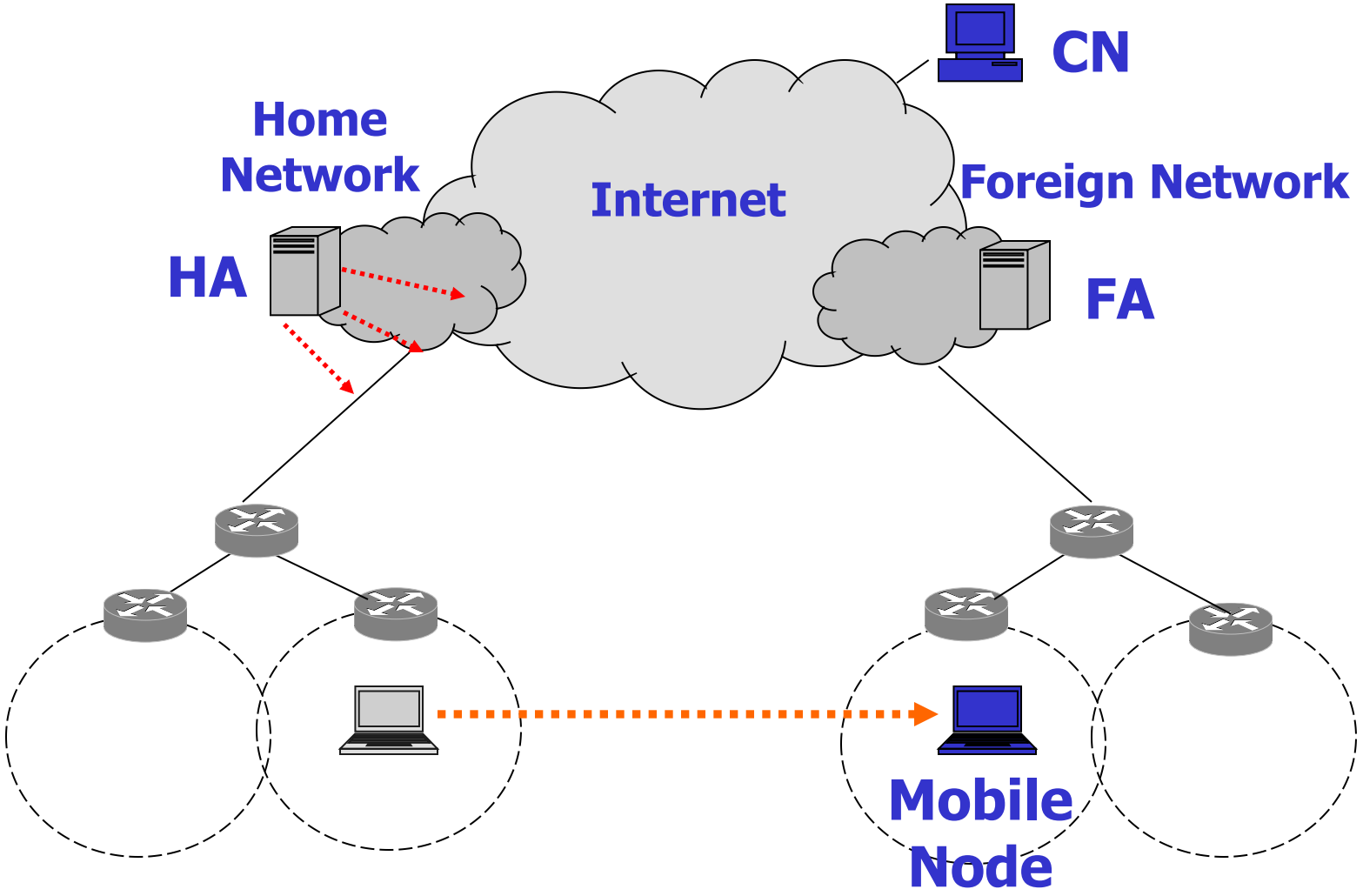
MIPv4 : Concepts



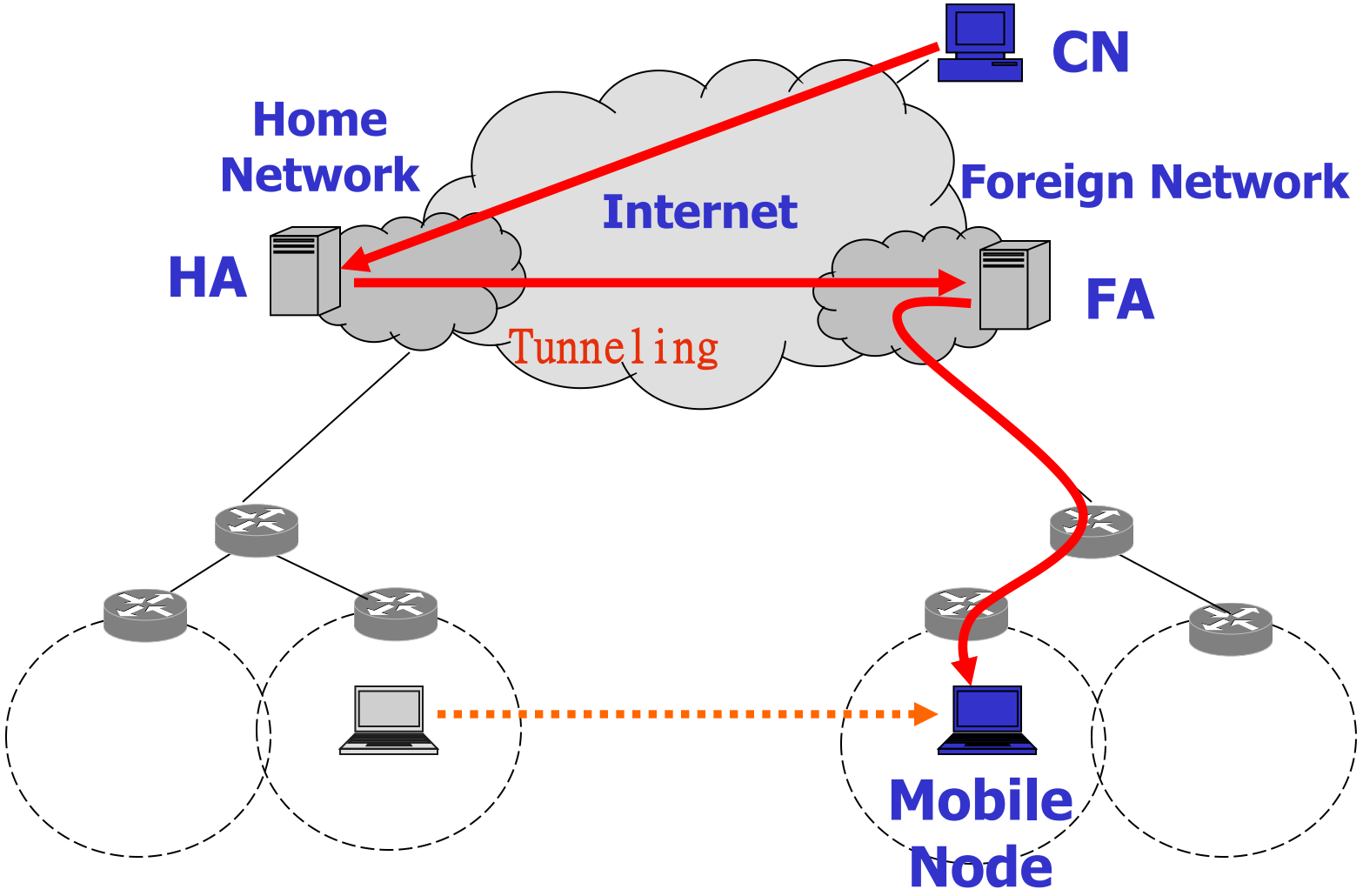
MIPv4 : Concepts



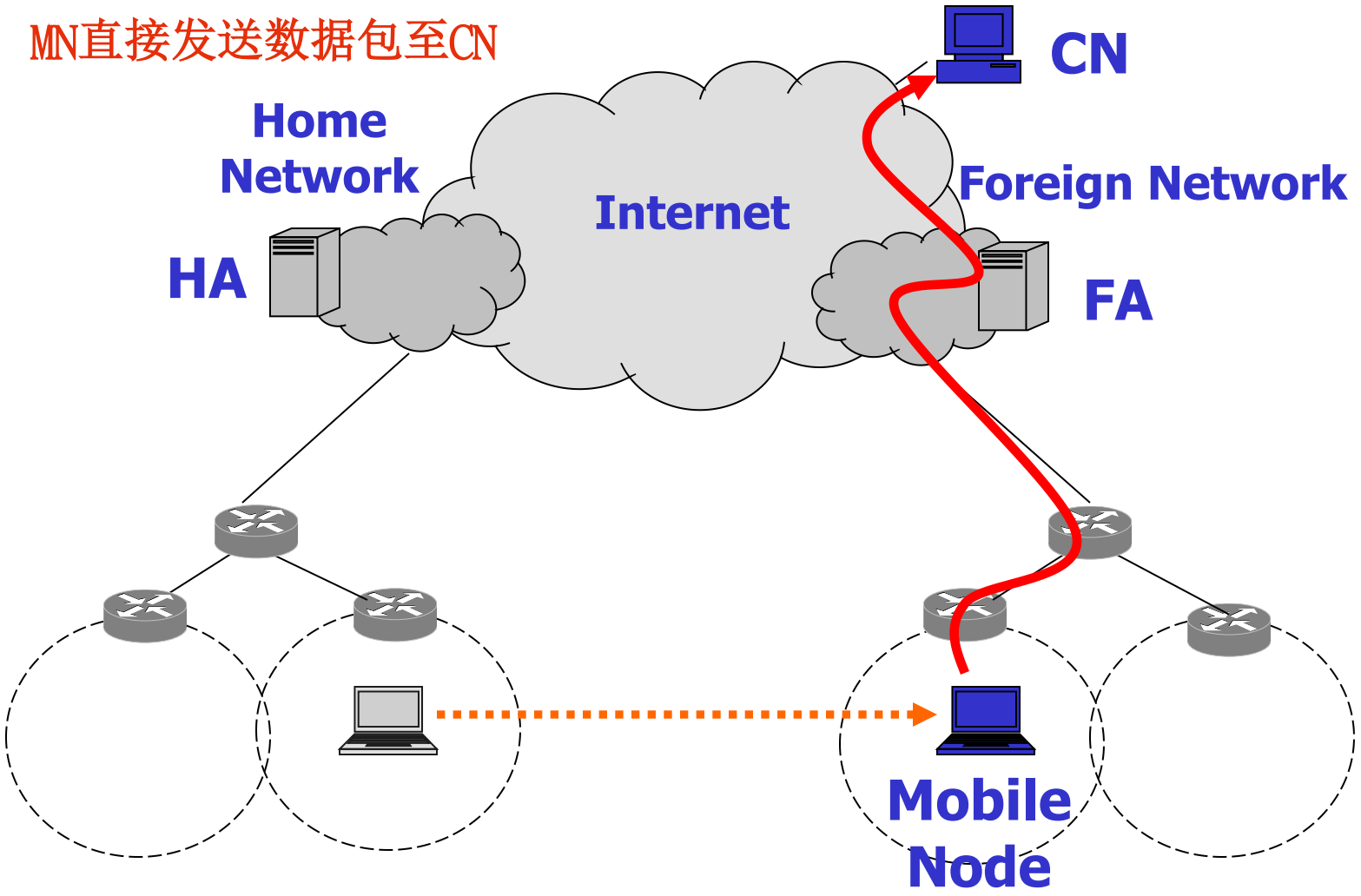
MIPv4 : Concepts



MIPv4 : Concepts

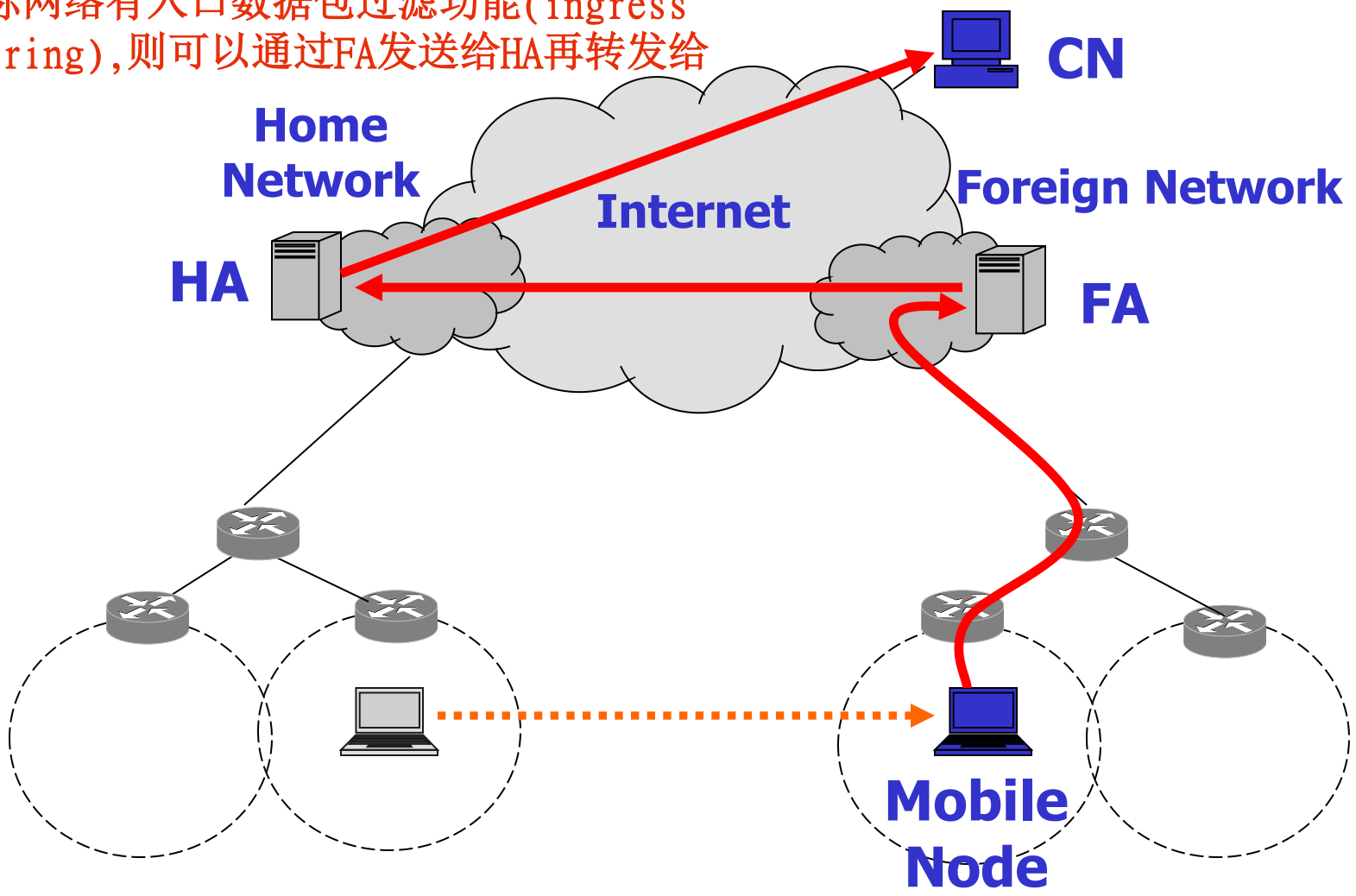


MIPv4 : Concepts



MIPv4 : Concepts

若目标网络有入口数据包过滤功能(ingress filtering),则可以通过FA发送给HA再转发给CN



MIPv6协议地址

- IP地址的作用
  - 节点的标识:两个节点之间的连接关系通过源地址和目的地址配对维持
  - 节点的位置信息:路由器寻址
- MIPv6主机拥有两个地址
  - 来自接入网络的地址(转交地址)作为定位符
  - 来自归属网络的地址(归属地址)作为标识符

MIPv6涉及的功能实体

- 移动节点
  - 两个地址:转交地址和归属地址
- 本地代理
  - 建立与移动节点之间的双向隧道
- 通信节点
  - 可以支持路由优化机制
  - 转交地址作为源地址, 归属地址信息由选项首部携带
  - 转交地址作为目的地址, 归属地址信息由“路由首部”携带

MIPv6基本工作原理(1/2)

- MN通过ICMPv6邻居发现机制中的无状态或状态地址自动配置机制获得一个或多个转交地址

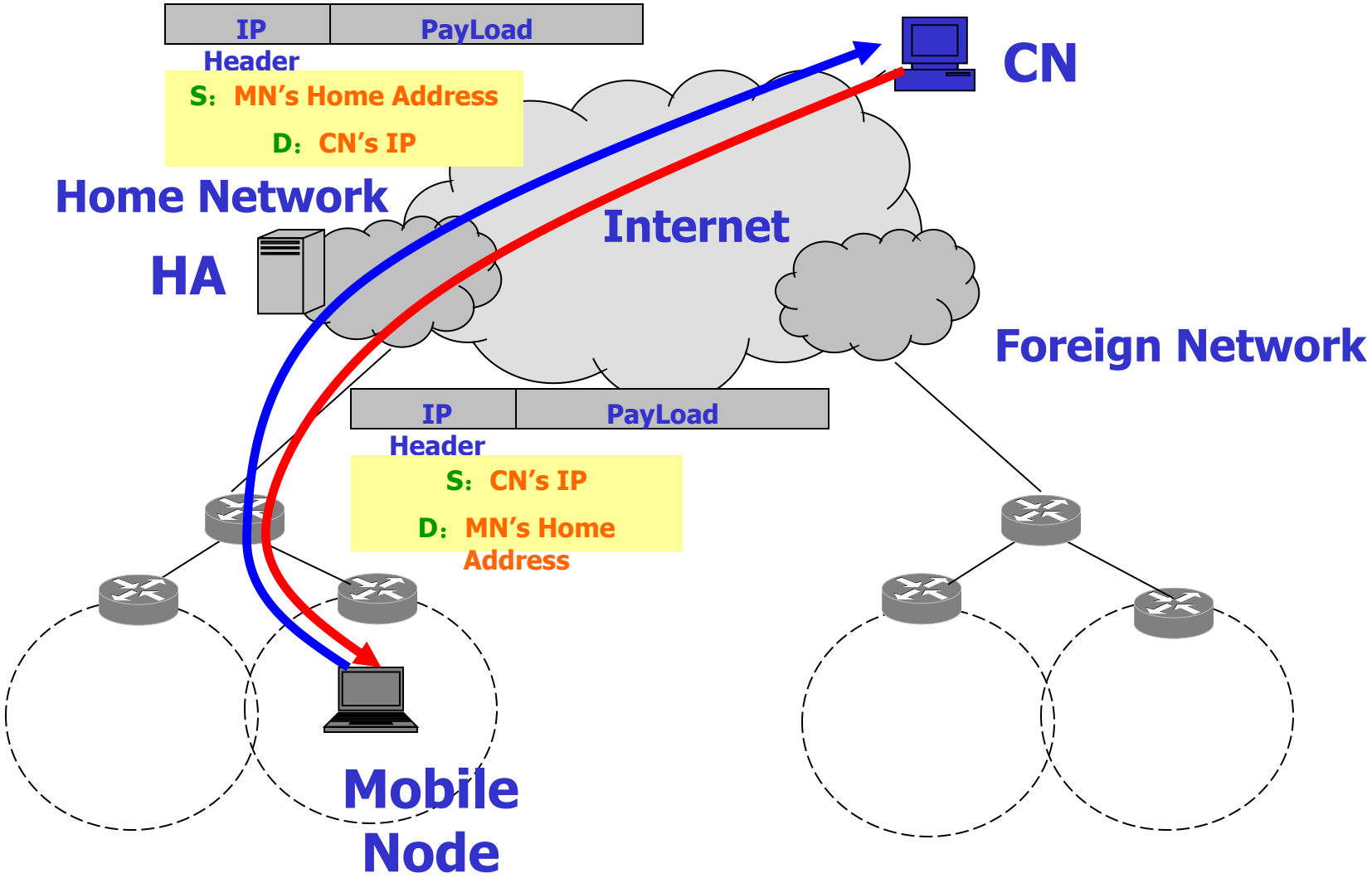
- MN获得转交地址，向家乡代理申请注册，为MN的家乡地址和转交地址在家乡代理上建立绑定

MIPv6基本工作原理(2/2)

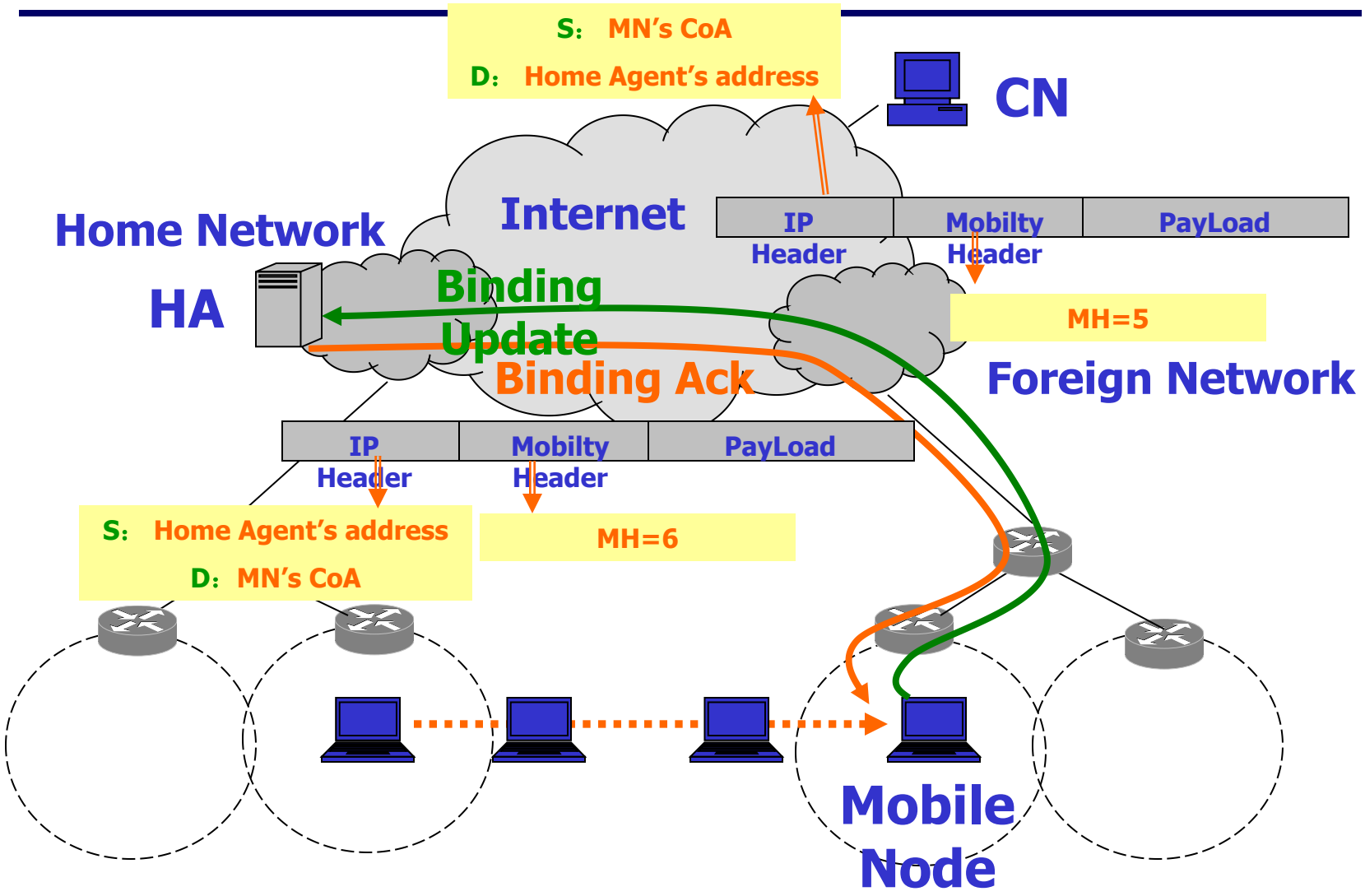
- CN发送分组至MN时,发送分组给家乡地址，经家乡代理的隧道发送给MN

- MN发送分组给CN
  - 源地址：MN的当前转交地址
  - 家乡地址选项：MN的家乡地址

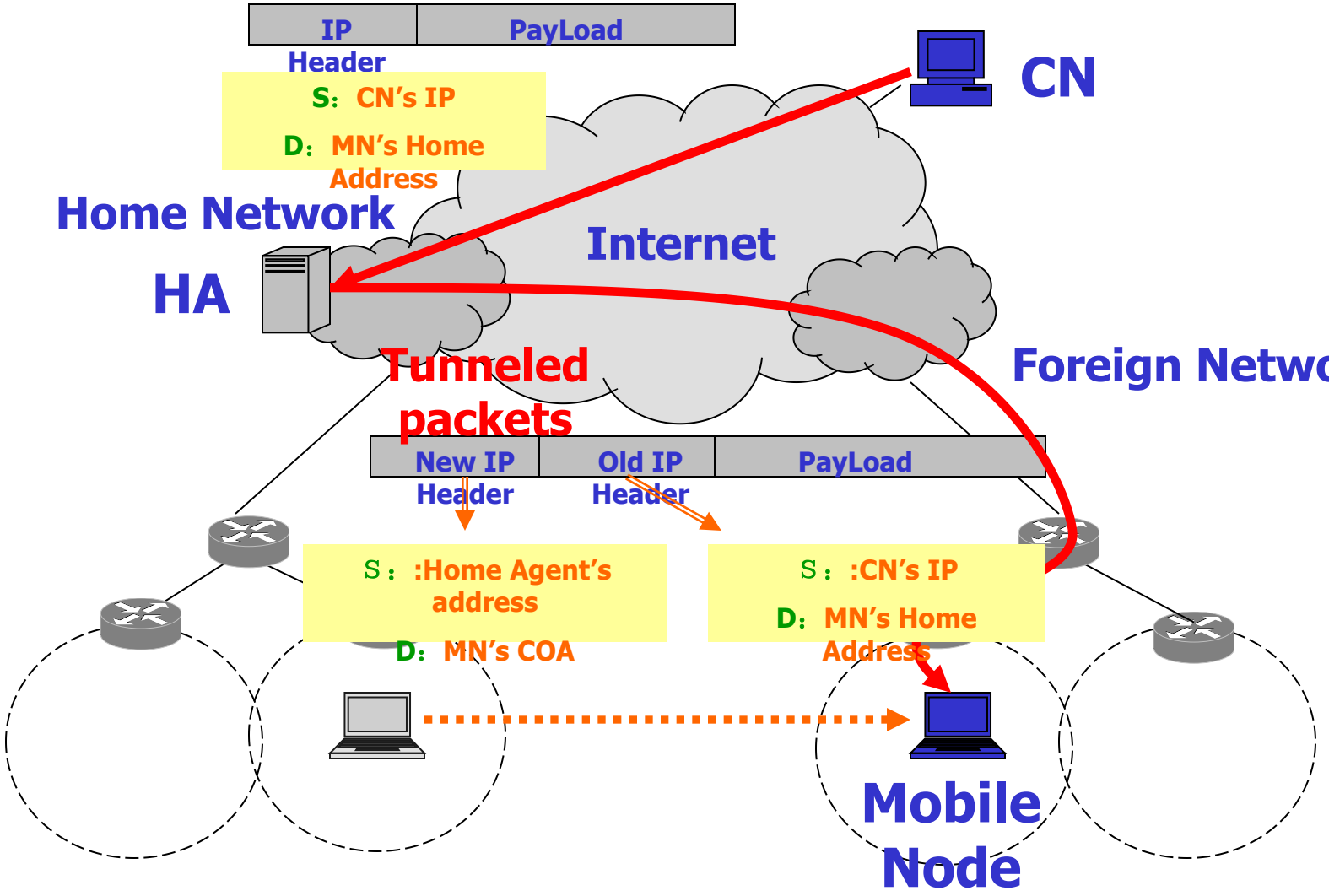
MIPv6协议


IP
PayLoad
Header
S：MN's Home Address
D：CN's IP
CN
Home Network
HA
Internet
Foreign Network
IP
PayLoad
Header
S：CN's IP
D：MN's Home Address
Mobile Node

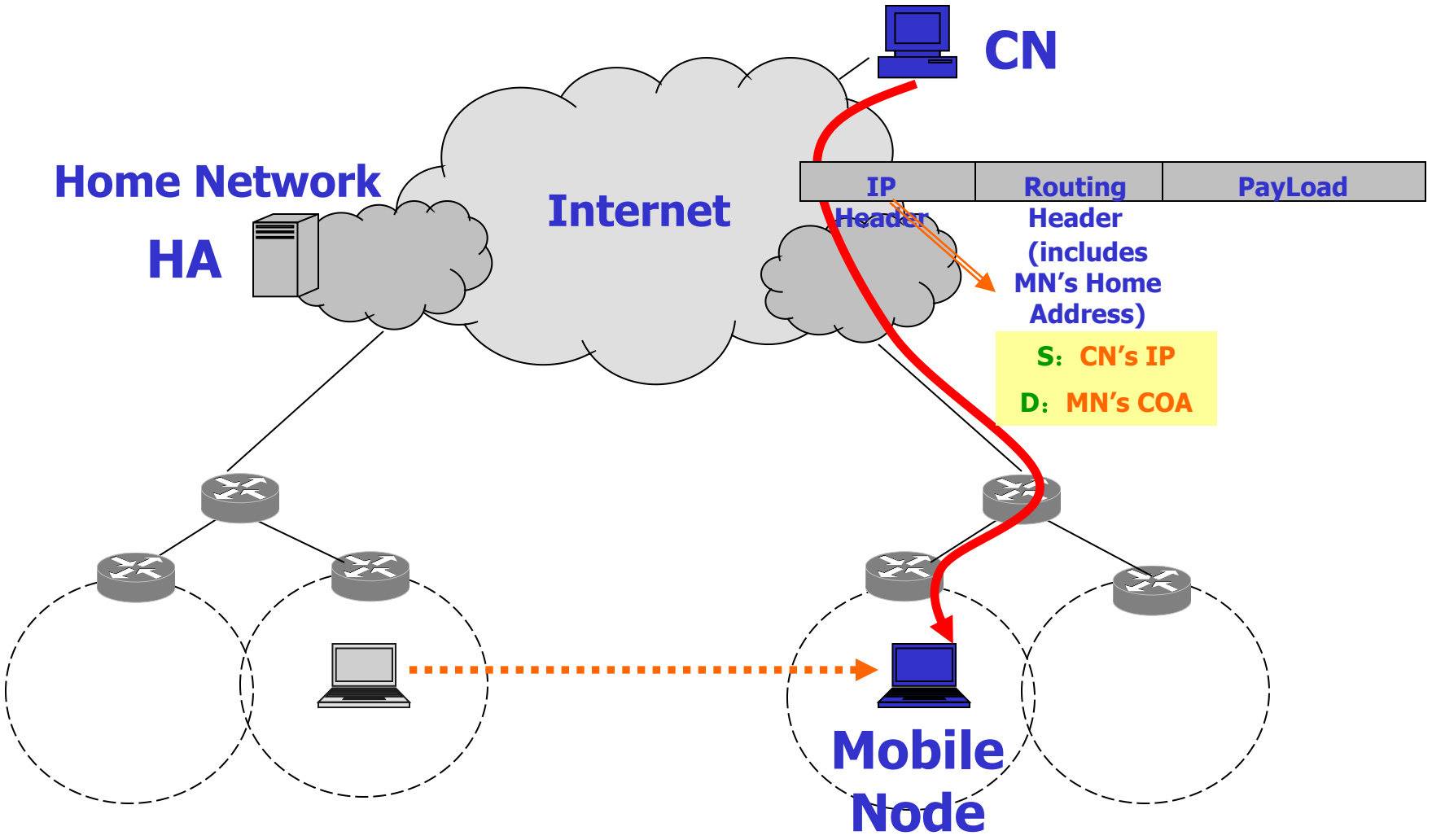
MIPv6协议


S: MN's CoA
D: Home Agent's address
CN
Internet
Home Network
HA
IP Header
Mobilty Header
PayLoad
Binding Update
Binding Ack
MH=5
Foreign Network
IP Header
Mobilty Header
PayLoad
S: Home Agent's address
D: MN's CoA
MH=6
Mobile Node

MIPv6协议


IP Header
PayLoad
S：CN's IP
D：MN's Home Address
CN
Home Network
HA
Internet
Tunneled packets
Foreign Network
New IP Header
Old IP Header
PayLoad
S：:Home Agent's address
D：MN's COA
S：:CN's IP
D：MN's Home Address
Mobile Node

Mobile IPv6 : Concepts



路由优化(1/3)

- 优化问题的提出：场景描述

  MN与CN在同一个网络上,虽然两个节点可以通过本地网络直接访问,但其之间的分组仍然都要发送到移动节点的归属网络中

- 解决方法
  - 对等节点支持路由优化机制

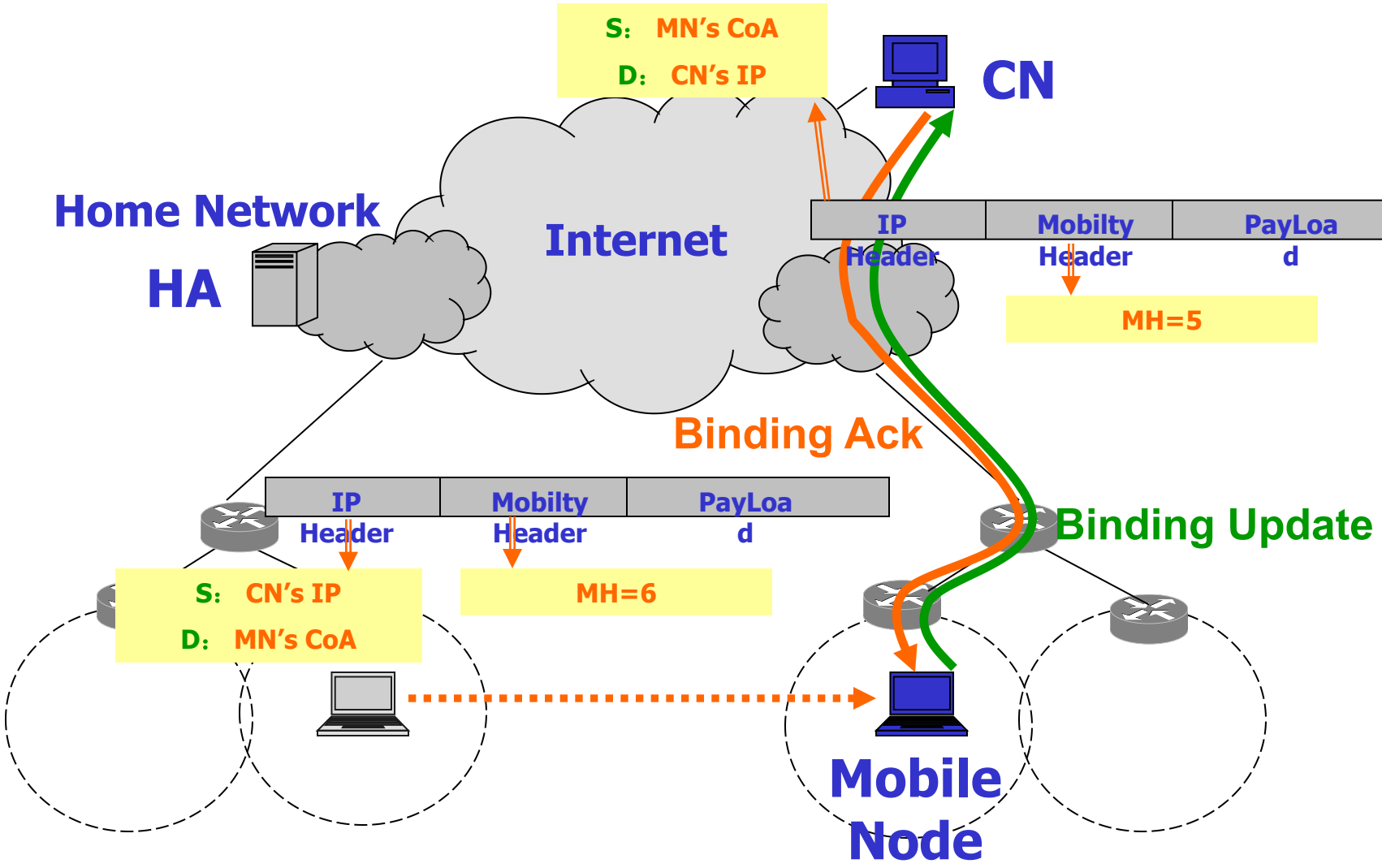
路由优化(2/3)

- 最佳路由
  - 通信主机直接将数据隧道传输至移动主机
- 工作原理
  - 移动节点转交地址的获取
  - 移动节点本地地址与转交地址的邦定

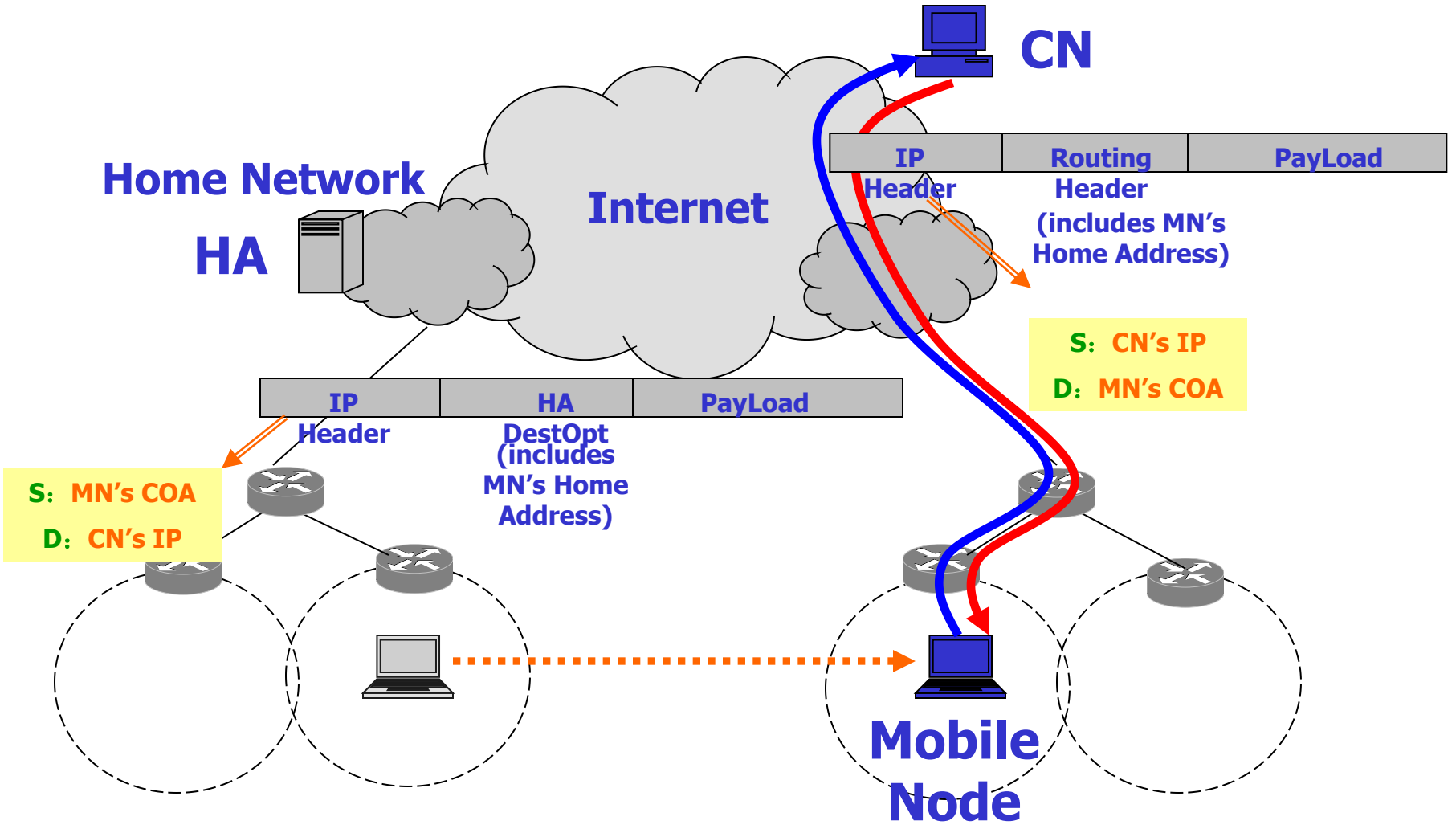
路由优化(3/3)

- MIPv6的路由优化
  - CN发送分组至MN时：
    - 根据目的IP查询绑定缓存，如果存在匹配，直接发送到转交地址；
    - 如果不存在匹配，发送分组给家乡地址，经家乡代理的隧道发送给MN
  - MN收到经家乡代理转发的分组后，向CN发送绑定更新消息

Mobile IPv6


S: MN's CoA
D: CN's IP
CN
Home Network
HA
Internet
IP Header
Mobilty Header
PayLoad
MH=5
Binding Ack
IP Header
Mobilty Header
PayLoad
Binding Update
S: CN's IP
D: MN's CoA
MH=6
Mobile Node

Mobile IPv6 : Concepts

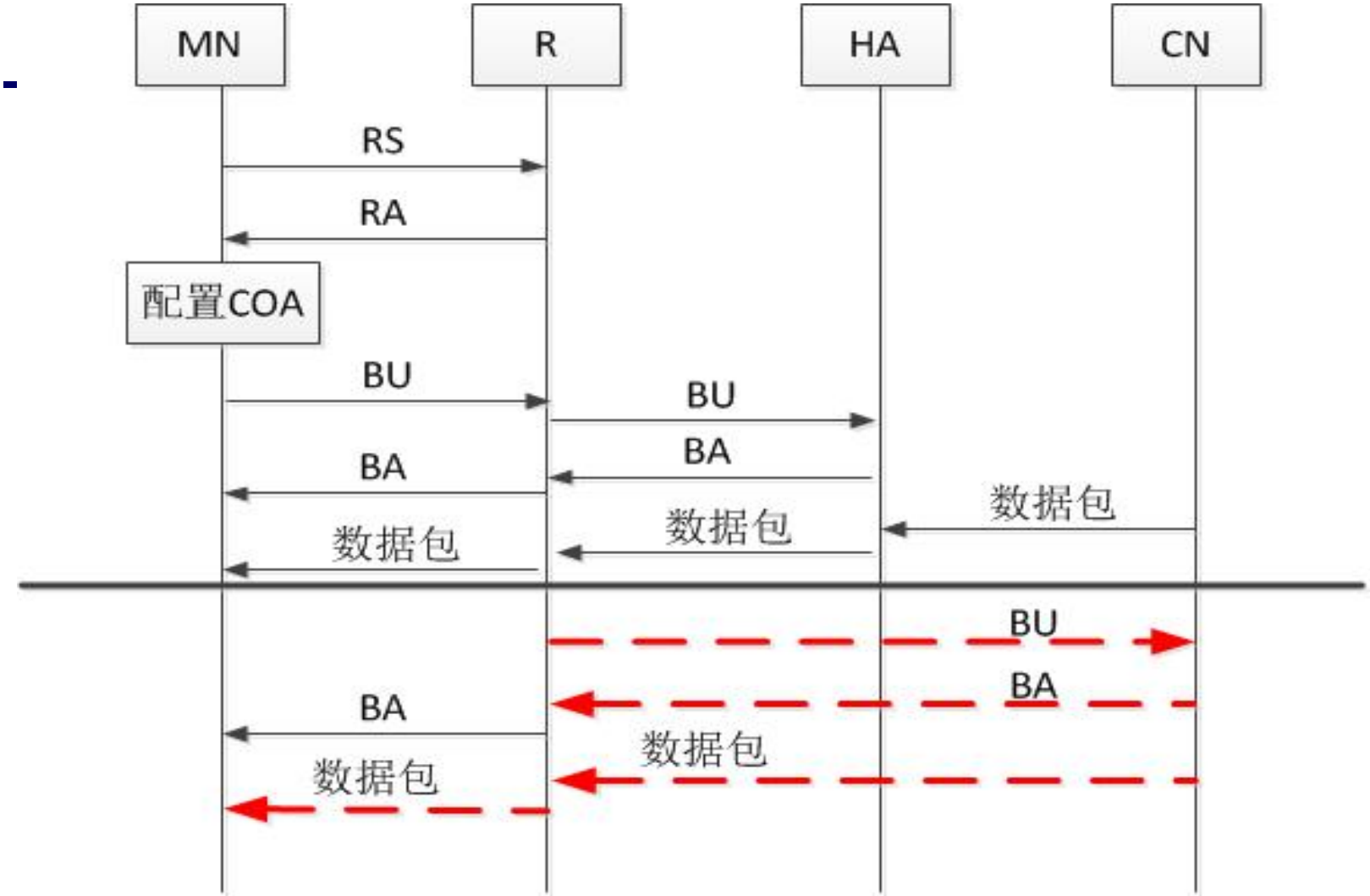


类型2路由选项头标

- 数据包到达转交地址后，MN从扩展头标中得到家乡地址，并作为数据包最终的目的地址
- 类型2路由选项头跟在其他路由选项头的后面

- 目的地址选项头标

  - 选项类型：201(表明该选项为家乡地址选项)
  - MN使用该选项通知CN自己的家乡地址
  - 位置
    - 若有路由头，放在路由头后
    - 若有分片头，放在分片头前
    - 若有AH头，放在AH头前


MN
R
HA
CN
RS
RA
配置COA
BU
BU
BA
BA
数据包
数据包
数据包
BU
BA
BA
数据包
数据包

- 移动IPv4与IPv6的区别
  - 涉及的功能实体: MN,HA,FA；MN,HA
  - 转交地址:配置转交地址/外地代理转交地址；配置转交地址
  - 转交地址的获取方法：DHCP; DHCP或无状态地址自动配置
  - IP数据包拦截：代理ARP; ICMPv6
  - 移动性检测：代理公告；路由器公告
  - 登录过程：注册；绑定更新
  - CN到MN 的数据包：利用隧道传输；利用隧道或者类型2的路由选项头标传输
  - 路由器入口过滤问题：反向隧道；目的选项扩展头标

- IPv6与IPv4比具有更好的移动性
  - 解决了Mobile IPv4的三角路由问题
  - 地址数量多
  - 灵活的地址自动配置
  - 解决了Mobile IPv4防火墙/路由器的入口过滤问题
  - 路由优化，结构简单：取消了外地代理概念
  - 解决了Mobile IPv4隧道软状态问题

移动互联网的快速切换机制

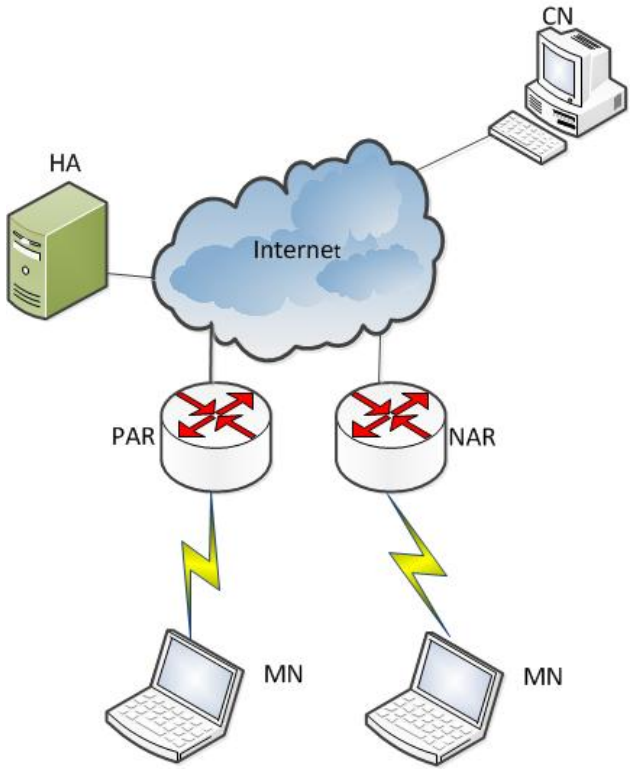
- 切换管理是在MN运动过程中，通过控制接入点的改变来保持通信的连续性
- 过程
  - 切换触发
  - 路由重建
  - 分组转发
- 切换管理的目标：提高切换的性能和速度

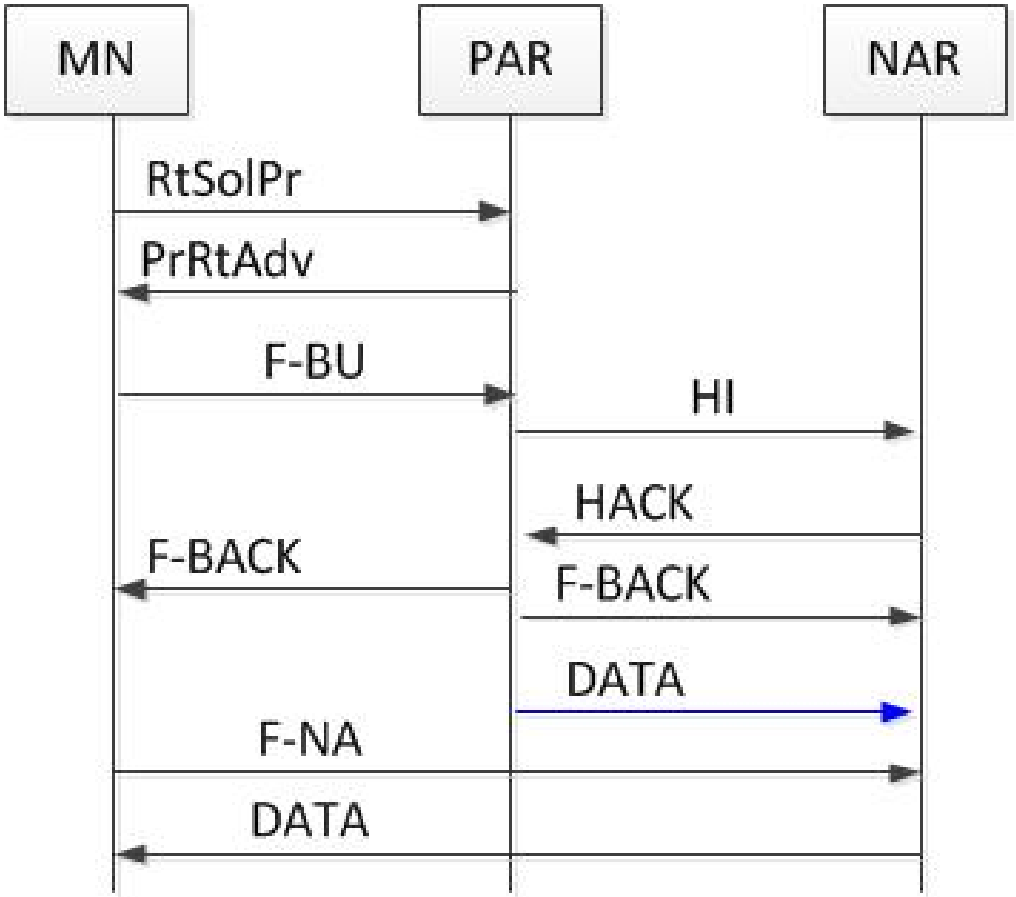
MIPv4扩展协议

- 快速移动IPv4
  - 新实体：PAR(原FA)、NAR(新FA)
  - 通过在PAR和NAR之间建立绑定关系来提高移动切换的性能
- 层次移动IPv4
  - **思路**：当MN在外地的一个访问域内移动时，只要没有移出这个域的范围，就不需要向家乡代理注册，只需要向当地代理注册，进而降低MN向HA注册的次数，提高切换性能。

MIPv6扩展协议

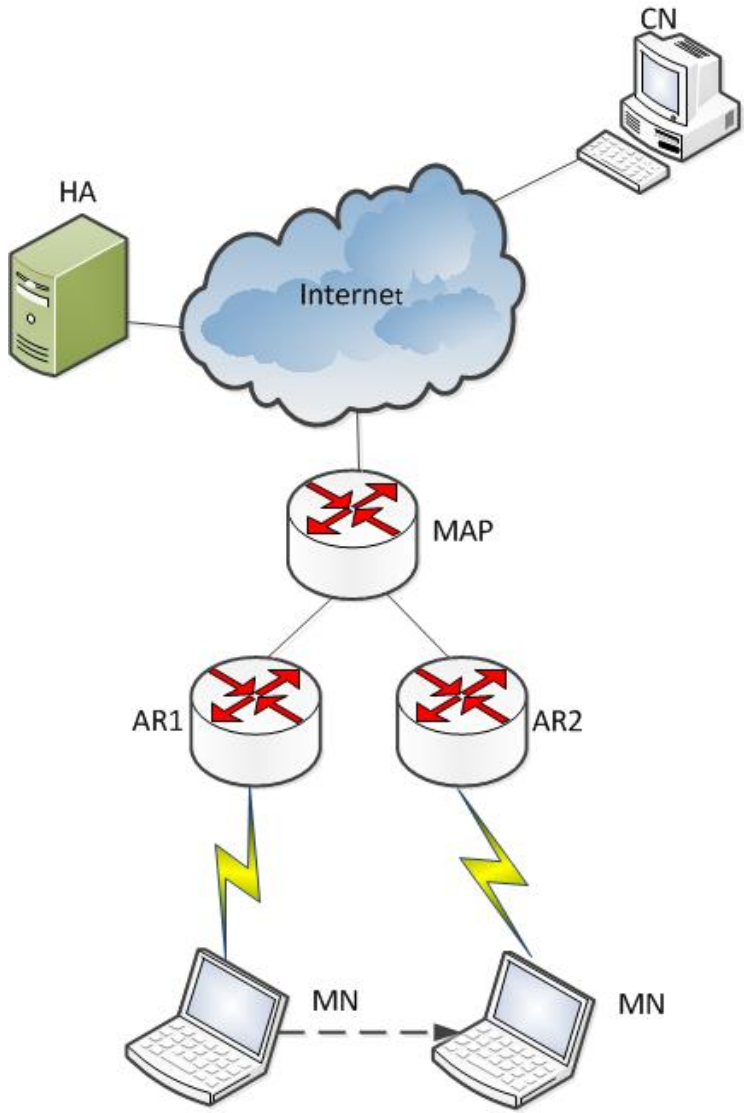
- 快速移动IPv6(FMIPv6)
  - **思路**：允许MN在进入新的子网前就配置完成转交地址，在新的接入点处尽快恢复IP连接。
  - PAR(MN原接入路由器)
  - NAR(MN新接入路由器)
  - 路由器请求代理消息MN->PAR
  - 代理路由通告消息PAR->MN
  - 切换发起(HI)、确认消息(HACK)
  - 快速绑定更新(F-BU)、确认消息(F-BACK)
  - 快速邻居通告消息(F-NA)

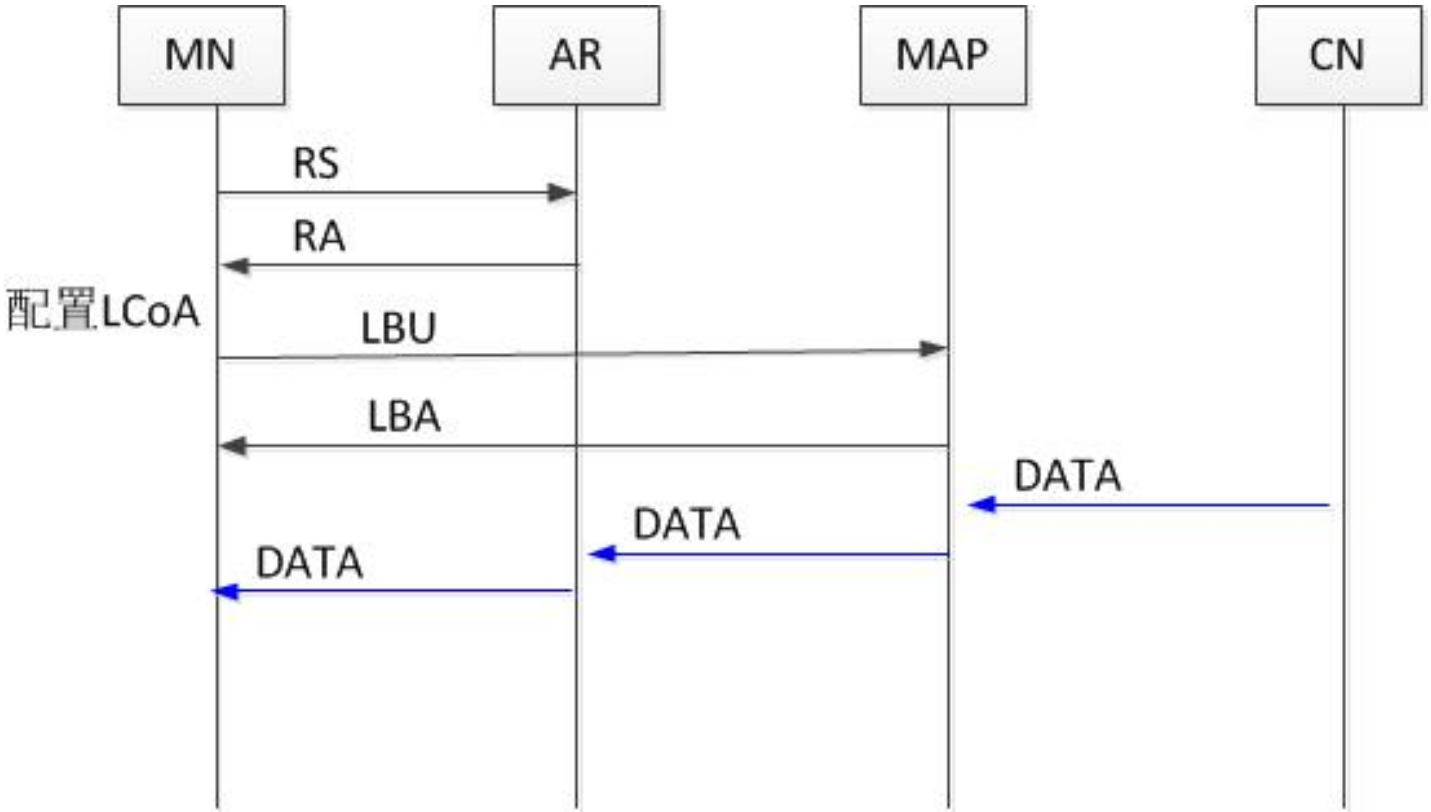



MN
PAR
NAR
RtSolPr
PrRtAdv
F-BU
HI
HACK
F-BACK
F-BACK
DATA
F-NA
DATA

MIPv6扩展协议

- 层次移动IPv6(HMIPv6)
  - **思路**：通过使用层次网络管理结构来减少注册时间。
  - 新实体：
    - 移动锚点MAP
    - 区域转交地址RCoA、
    - 链路转交地址LCoA、
    - 本地绑定更新消息LBU

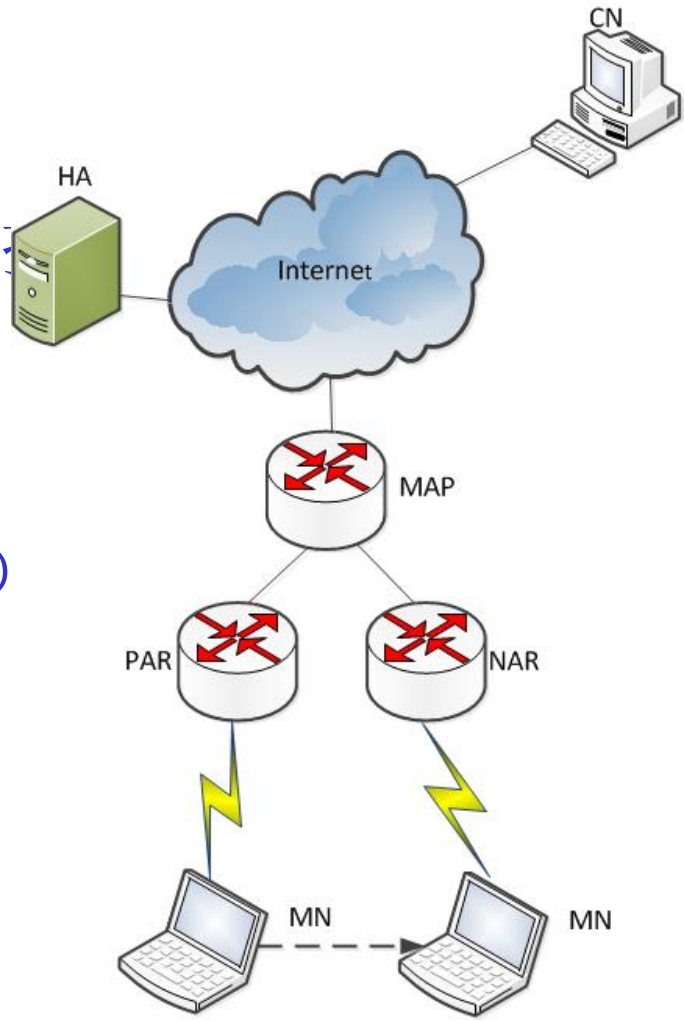



MN
AR
MAP
CN
RS
RA
配置LCoA
LBU
LBA
DATA
DATA
DATA

快速分层移动IPv6

- 快速分层移动IPv6(F-HMIPv6)
  - **思路**：HMIPv6与HMIPv6相结合

在层次移动管理模型中实施快速切
  - **新实体**：
    - PLCoA（PAR子网中的CoA）
    - NLCoA （NAR子网中的CoA）



MIP的安全机制

- 背景: 移动环境下的计算机大都采用无线接入技术,这种链路容易受到恶意攻击和窃听.
- 方法
  - 安全认证
  - 登录报文重发保护

安全认证

- 代理公告和代理请求的认证可采用IP认证头标
- 本地代理、外地代理和移动节点必须支持认证功能，缺省算法是128比特秘钥的MD5

登录报文的重发保护

- 登录报文的重发保护原理

  在登录请求和响应中设置一个识别域，使用该识别域可以让本地代理查证收到的登录报文是MN发出的，还是由攻击者先前窃取的登录报文作出的重发。

- 方法
  - 现时重发保护（可选）
  - 时戳重发保护（支持）

登录报文的重发保护

- 时戳重发保护（支持）
  - 原理：节点需要生成一个插入当时时间的报文，当其他节点收到这个报文时就检测这个时戳是否接近当时的时间。
  - 条件：两个节点时间需要同步
  - 步骤
    - MN发送登录请求消息
    - HA验证识别域中的时戳
    - 如果时戳有效，则返回接受响应（拷贝识别域）
    - 如果时戳无效，则返回拒绝响应—识别域不匹配（自己的时戳+拷贝低32位）
    - MN核实后使用高位时钟重新同步