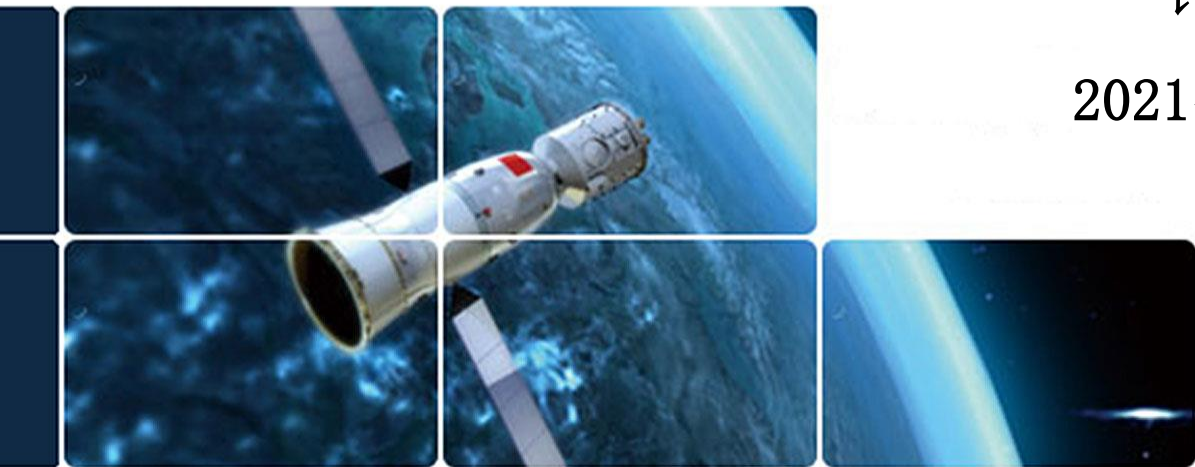


# 第5讲 移动IP技术

计算学部

2021年10月28日



- 为什么需要移动IP
- 移动IP的概念
- 移动IPV4

提出问题



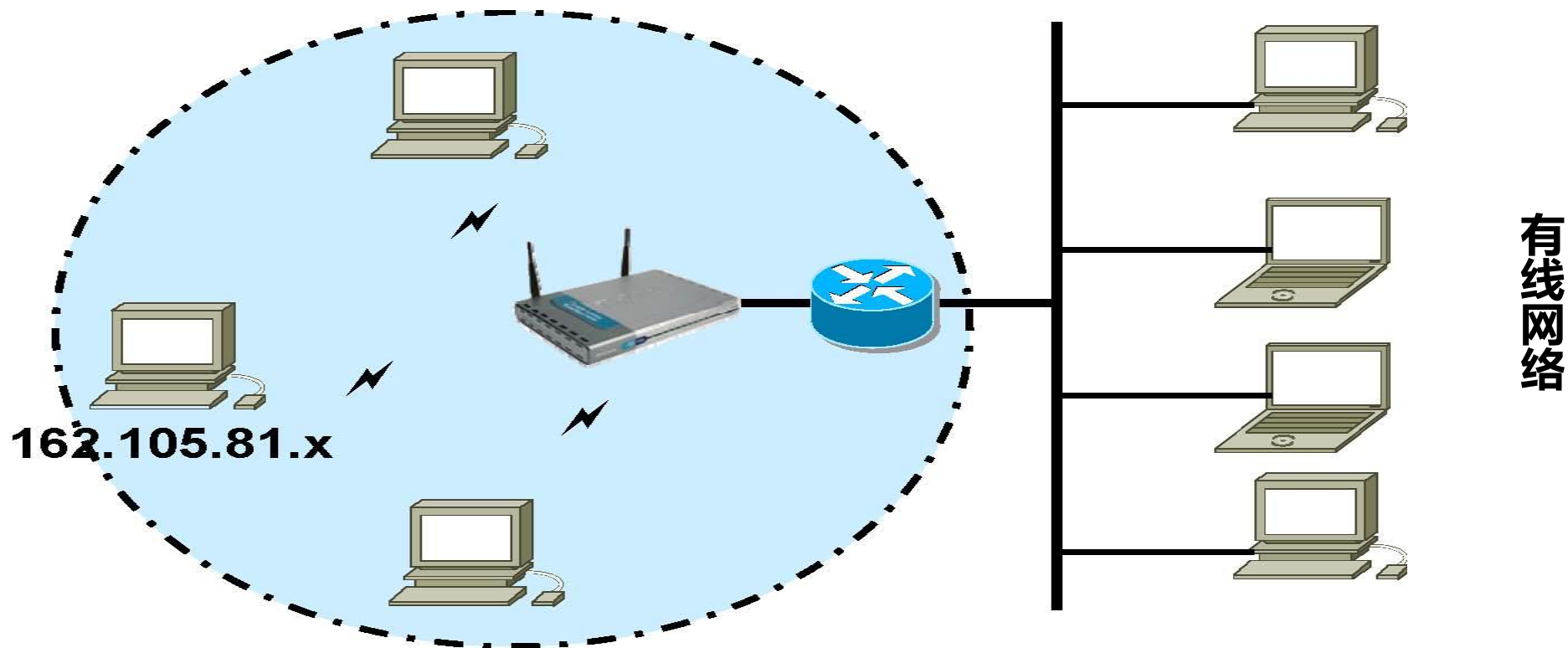
定义问题



解决问题

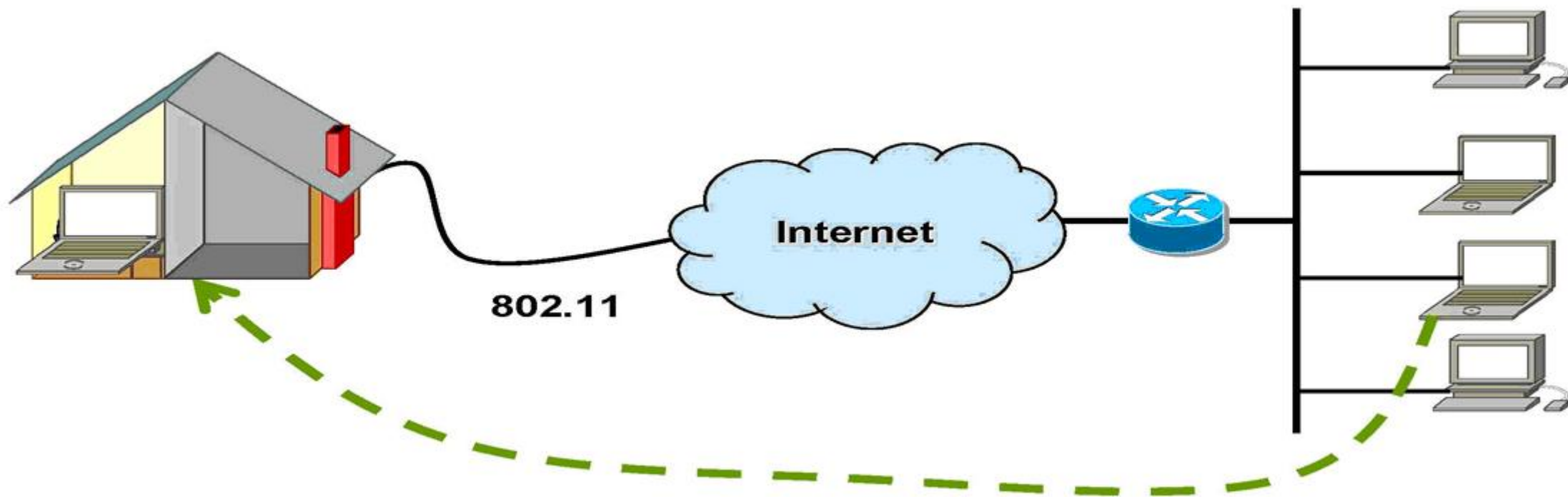
## 1. 计算机通过无线上网

实际上没有移动的概念!



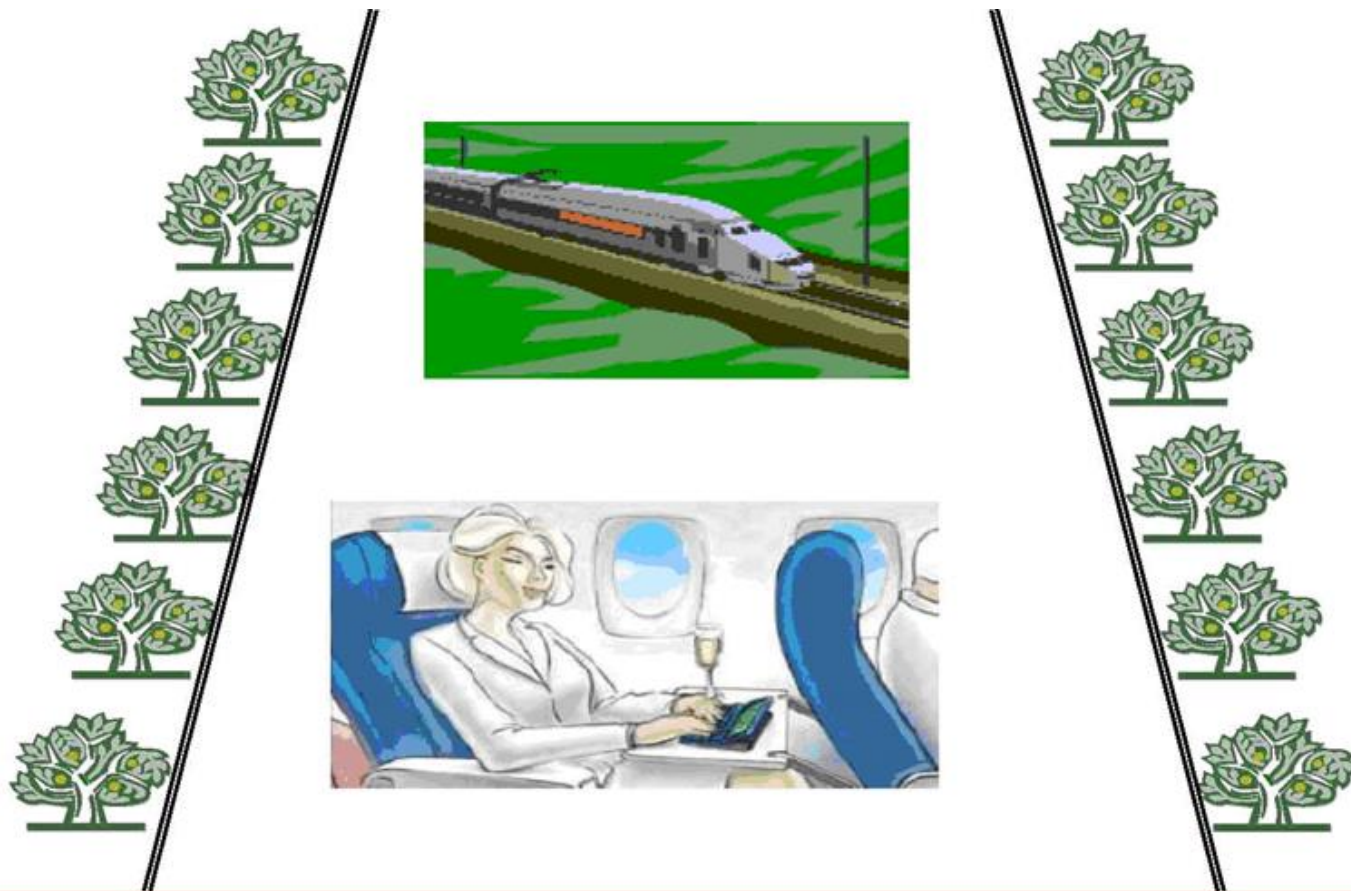
## 2. 将笔记本从办公室移动到宿舍、食堂、咖啡厅

用户是移动的，但在移动期间不需要保持连接！



### 3. 坐在移动火车或汽车上访问Internet

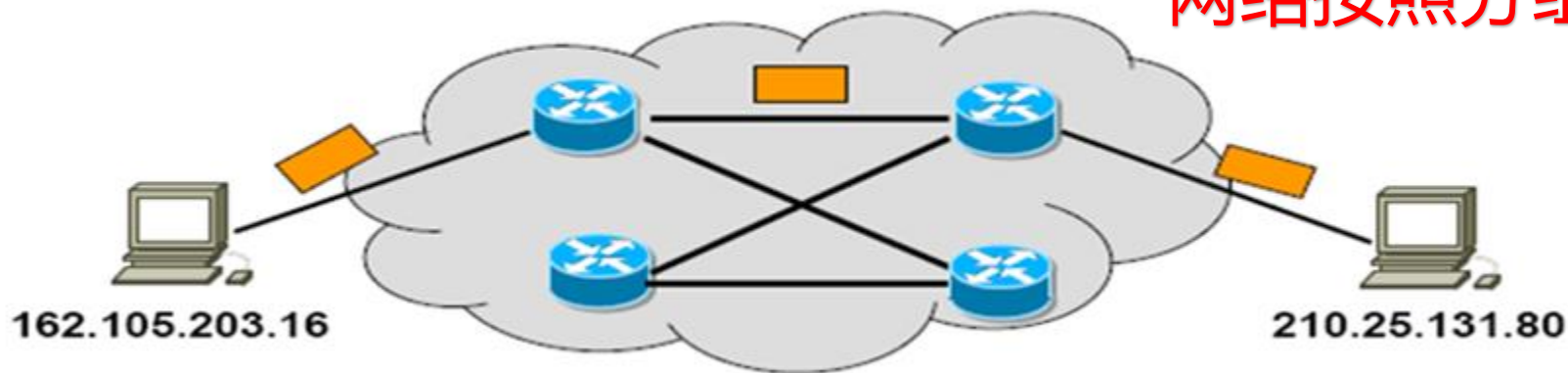
## 用户处于绝对移动的环境中!



- 以人为本（人的惰性） — 不用重配置
- 通信的持续 — 不能中断通信
- 无所不在 — 无论何时、何地、与任何人都可以无约束的通信



网络按照分组携带的IP地址进行路由



## □ Internet 地址级别

第一级：域名 (*DNS Address*)

主机位置无关标识： `www.hit.edu.cn`

第二级：IP 地址 (*IP Address*)

主机逻辑位置： `202.118.239.46`

第三级：MAC地址 (*MAC Address*)

网络接口硬件地址： `00 a4 24 4a 8f 00`

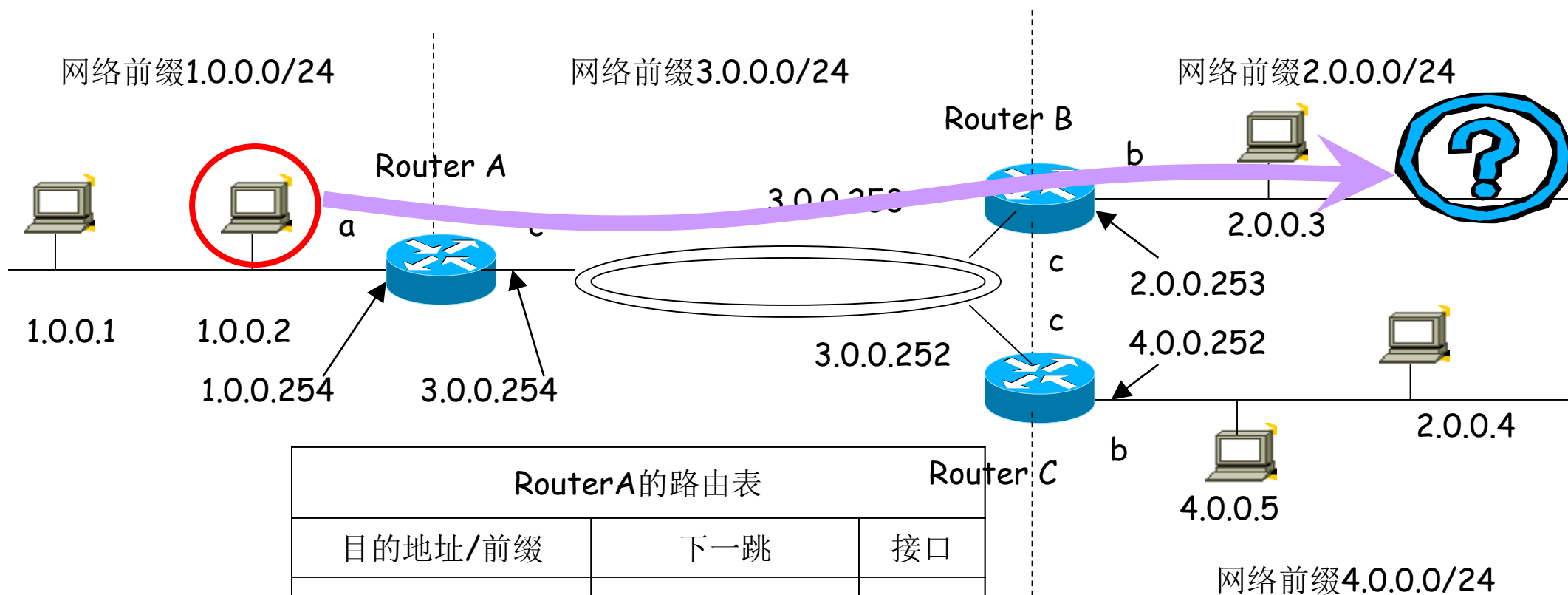
□ **Internet** 路由机制：到某一目的地的IP包，将被路由转发到宣告了该地址前缀可达性的路由器

□ 现有**Internet**路由规则

1. 路由器以**网络前缀形式的路由宣告**
2. 路由器**根据路由宣告构造路由表**
3. 单**IP**包的转发**基于目的地址与路由表项前缀的匹配**

一旦配有**固定IP**地址的移动主机移出原有接入路由器的作用范围，则该移动主机进入了**Internet 路由盲区**





Router A 的路由表		
目的地址/前缀	下一跳	接口
1.0.0.0/24	"direct"	a
3.0.0.0/24	"direct"	c
2.0.0.0/24	3.0.0.253	c
4.0.0.0/24	3.0.0.252	c



How to solve...?..?

□ **两个术语**：就移动节点而言，其所在网络分为两种类型

- **家乡链路（网络）（*Home Link*）**：具有与移动节点**固定IP地址子网前缀**一样的网络前缀的网络
- **外地链路（网络）（*Foreign Link*）**：任何不是家乡链路（网络）的网络，每一个外地链路（网络）有一个自己的网络前缀

□ **移动 IP 的问题领域**

- 在现有 *Internet* 路由机制下，移动节点在 *Internet* 上的移动过程中**不用更改 *IP* 地址**，能够与网络上另一对端节点进行持续通信

## □支持移动的网络

- 任何时候、任何地点都能提供可靠的*Internet*访问
- 移动对网络应用和高层协议是透明的

## □移动需求

- 移动性**：越来越多用户要求*Internet*能支持移动性
- 透明性**：移动对于*IP*上层协议来说都是透明的
- 易使用**：不需要用户的操作或仅需要简单操作
- 路由**：移动应该与所有路由协议兼容并能优化路由
- 安全**：移动不应该降低*Internet* 的安全性

无移动

移动性逐渐增加

高移动

1. 不移动的移动设备

使用不变AP接入

2. 低速移动的移动设备

使用DHCP与网络连接的移动用户

3. 高速移动的移动设备

穿越多个AP, 同时保持当前连接的移动用户

**RFC2131: DHCP** (动态主机配置协议: *Dynamic Host Configuration Protocol* )

*DHCP*允许自动配置, 但自动配置要受管理员的控制

- 主要用于简化联网计算机的安装和维护
- 允许计算机快速、动态获取*IP*地址
- 任何时候, 连到网络上的新计算机均与*DHCP*服务器联系, 并申请一个地址
- 服务器从管理员指定的地址中选择一个地址, 并将它分配给该计算机



□ *DHCP*能解决临时上网问题

□ *DHCP*能有效管理IP地址空间

□ *DHCP*不能进行移动管理

□ *IP*地址的每次改变不为人知

□ 当移动节点在两个子网之间漫游时，由于其*IP*地址变化，将导致移动节点无法与其他用户通信

□为什么不可以使移动节点在网络间移动时自动改变*IP* 地址?

听起来很有道理!

## □对传输层的影响

- TCP**是*Internet*上使用最多的传输层协议之一，移动解决方案必须能支持它

- TCP**是面向连接的协议。一个**TCP**连接由四元组标识：

(源IP地址，源端口，目的IP地址，目的端口)

在一个连接的生命周期中，四个元素不能改变，否则连接终止，通信中断

## □通信对端可以接收吗？

- 移动节点不断更换*IP*地址，通信对端如何找到它？

- DNS*行吗？

## □移动节点的*DNS*域名在移动过程中保持不变，而域名到*IP*地址的映射在移动过程中不断更新

- DNS*的查询与更新量将急剧上升

- DNS*更新存在安全问题

□采用**DDNS** (动态**DNS**) 技术行吗?

■动态更新**DNS**的资源记录 (**RR**)

□无法解决移动管理问题

■延迟大, 不适应频繁移动

■当移动的节点数目增多时可能造成域名系统的不一致



还是无法实现！



## □移动 (*Mobility*) 与漫游 (*Nomadcity*)

- 移动**: 移动节点占有一个固定*IP*地址, 在移动过程中, 已有通信不必中断
- 漫游**: 漫游节点不必有固定*IP*地址。当漫游节点改变接入点 (*point-of-attachment*) 时, 它必须中断已有所有的通信。在获得新的地址后, 漫游节点再以新地址发起连接

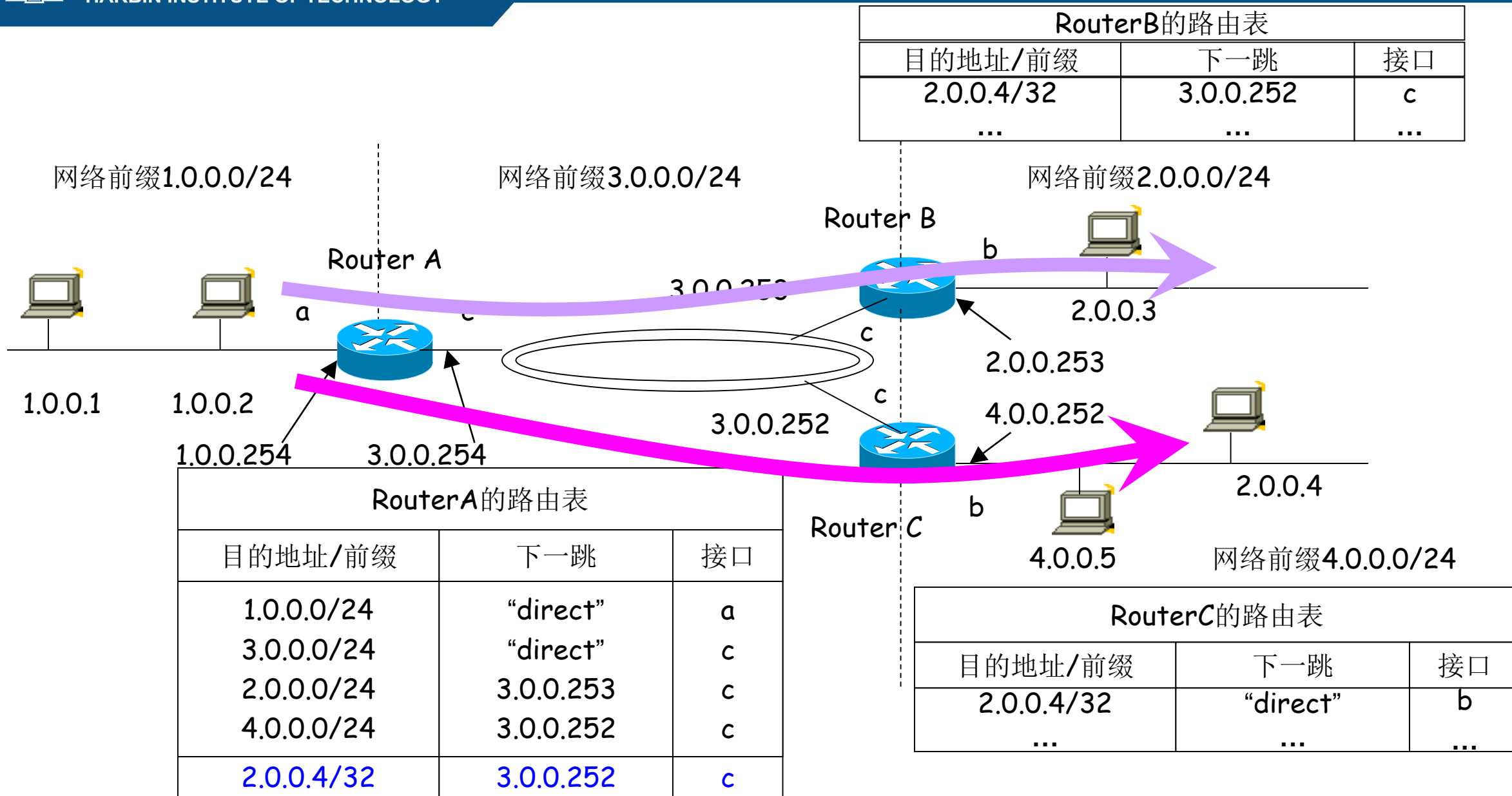
## □ 特定主机路由(*Host-Specific Routes*)?

### ■ 何谓特定主机路由?

特定主机路由是对特定的目的主机指明的一个路由

### ■ 如何解决问题?

当移动主机移动到另一接入点时, 网络其他部分到它的路由使用特定主机路由



□这个解决办法好吗？

■**评判标准1：**需要的额外的特定主机路由的数量多少！而这又取决于：

- (1) 移动节点的数量
- (2) 每一个移动节点移动之后，相应特定主机路由必须传播的最小节点集
- (3) 移动节点切换接入点的频率

■**评判标准2：**健壮性如何？

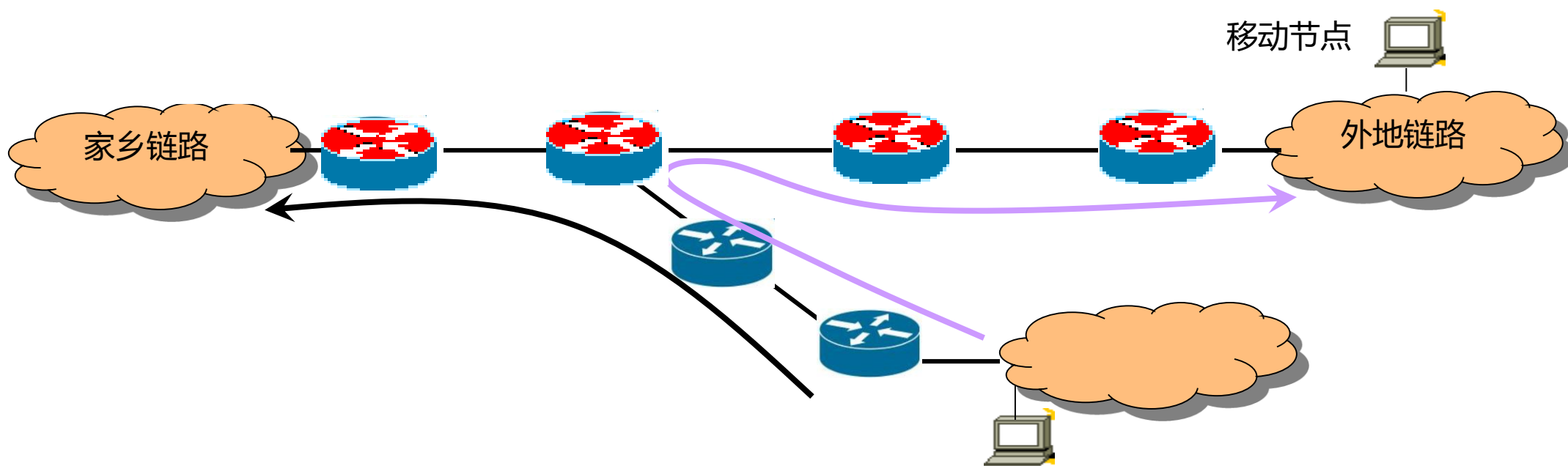
■**评判标准3：**安全吗？

## 1. 将来可能有无数的移动节点

- 笔记本电脑
- 移动电话
- 你还能想出什么来吗? .....

## 2. 需要非常多的特定主机路由

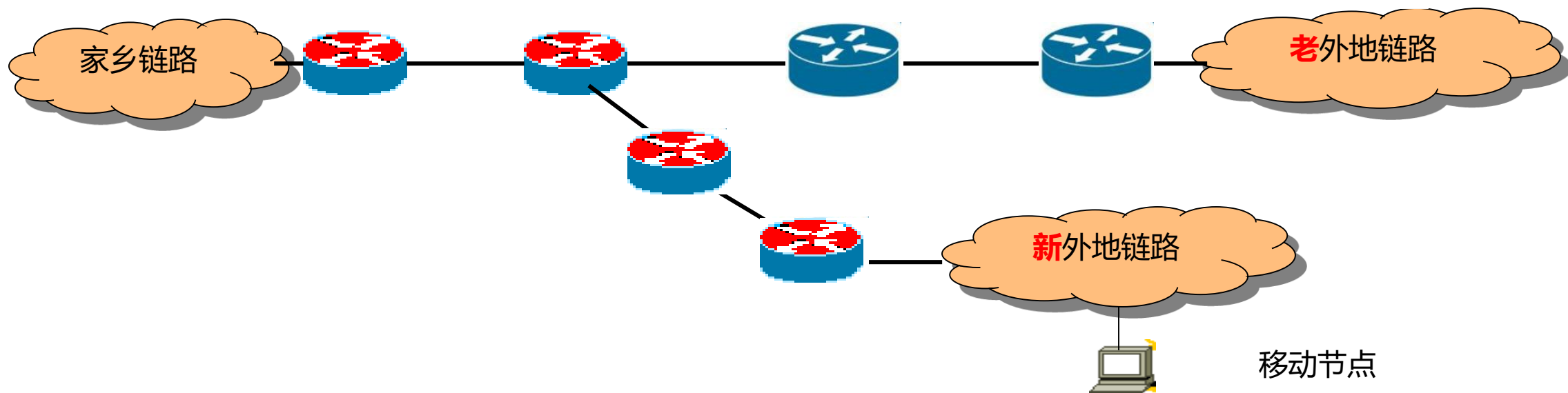
- 对每一个移动到外地链路的移动节点来说，至少需要在家乡链路到外地链路途经的所有路由器添加一条特定主机路由





## 3. 移动节点切换接入点的频率

- 移动节点切换接入点的频率是比较快的
- 移动节点切换接入点一次，需要大量路由节点增加或是删除相应特定主机路由



## 4. 健壮性

### ■ 最小路由器集合

- 从家乡链路到外地链路之间所有路由器

### ■ 单故障点：最小集合中的每一个路由器

- 一旦它们中的任何一个出现故障，去往该移动节点的通信将中断
- 这与Internet路由的健壮性不符

### ■ 巨大的移动节点群

- 移动节点切换接入点过程中增加或删除大量特定主机路由
- 网络不稳定

## 5. 安全?

- 特定主机路由的更新需要认证
- 这不是特定主机路由的错

特定主机路由方案不适合移动问题的解决!

蜂窝数据网、802.11？

## □链路层技术不足以解决移动问题

- 链路层技术只在单一介质类型中提供移动支持
- 每一种介质类型有一种特定的移动解决方案
- 移动节点在不同介质之间切换时，移动节点可能得不到移动服务
- 导致了移动服务的地域限制

- *Internet* 上的每个节点都有网络层
- 网络层负责将分组路由到合适的位置
- 移动性面向整个 *Internet*，改变物理介质应该对应用透明

因此，网络层解决方案对全部应用来说是全局解决方案！





# 移动IP-网络层的解决之道

- 为什么需要移动IP
- 移动IP的概念
- 移动IPV4

提出问题



定义问题



解决问题

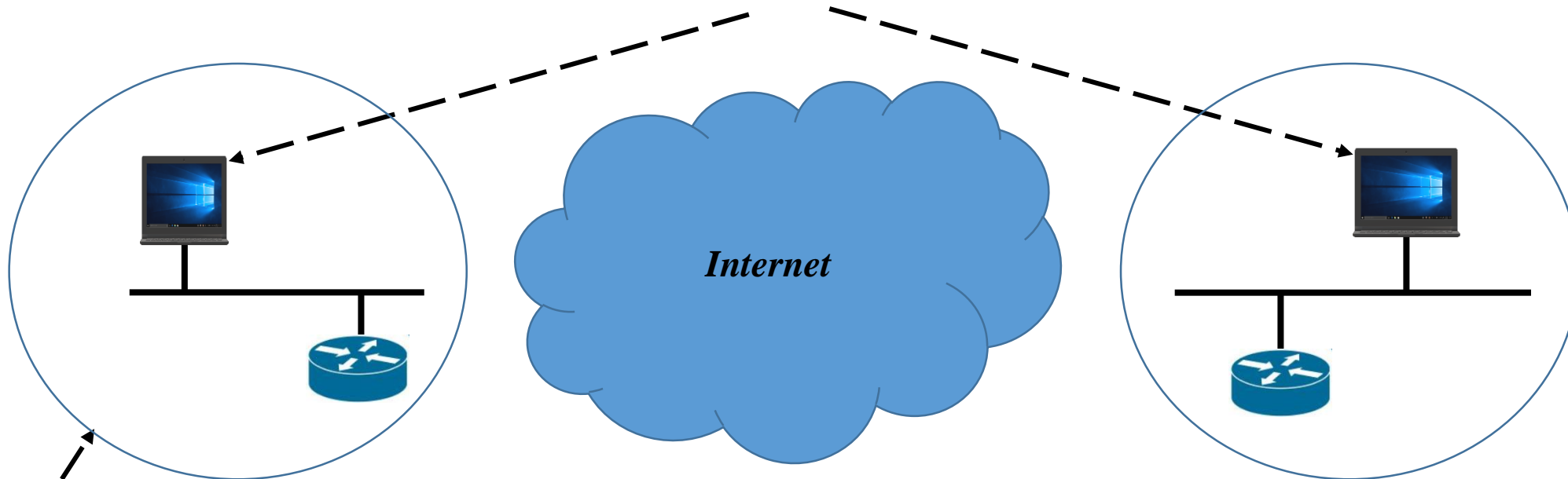
- 移动节点在改变接入点之后能继续与其他节点通信
- 移动节点只要与接入点连接就能用原来的IP地址通信
- 移动节点能与不具有移动IP功能的其他节点通信
- 移动节点不应该比其他节点的安全性差

- 移动IP具有扩展性、可靠性和安全性
- 移动IP与传输介质无关
- 移动IP与现有Internet 协议兼容，并能与不具有移动IP的主机进行正常通信

## 国际互联网工程任务组 (IETF) 草案:

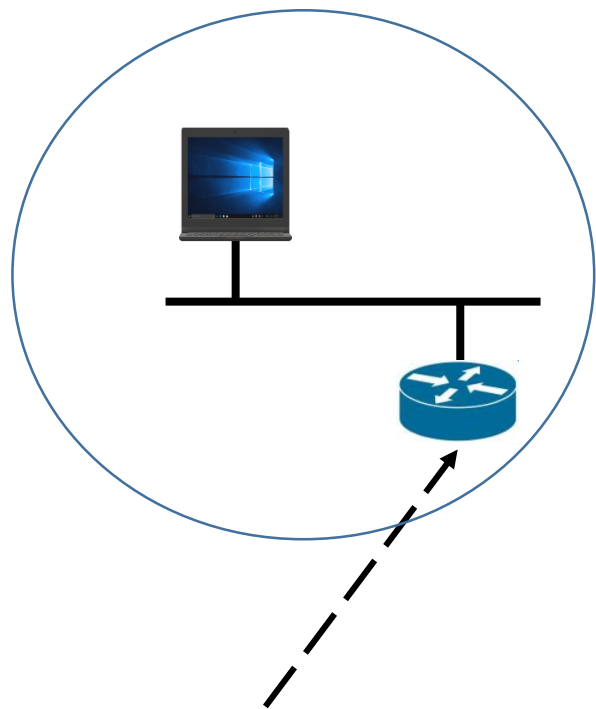
- **RFC2002**: 定义了移动**IP**协议
- **RFC2003/2004/1701**: 定义了移动**IP**的隧道技术
- **RFC2005**: 定义了移动**IP** 的应用
- **RFC2006**: 定义了移动 **IP** 的管理信息库**MIB**

**移动节点MN (Mobile Node)**  
从一个网络链路切换到另一个网络链路

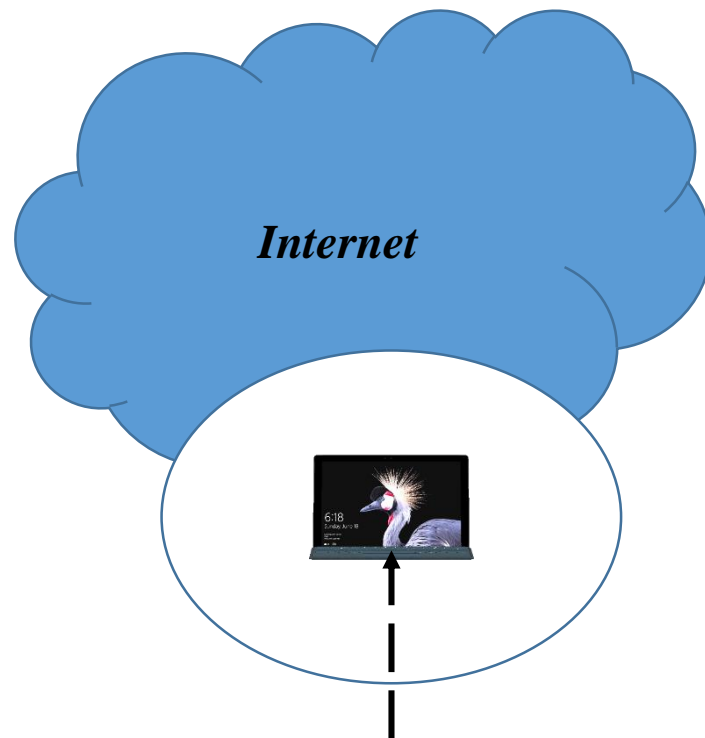


**家乡网络 (Home Network)**  
移动节点的“永久家乡”

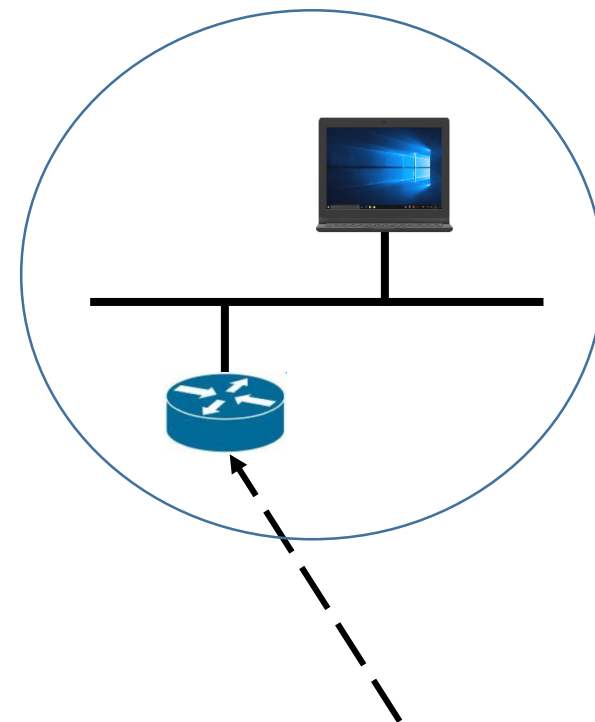
**外地网络 (Foreign Network)**  
移动节点当前驻留非家乡的网络



**家乡代理HA (Home Agent)**  
可代表MN (远程时)  
执行移动功能的实体

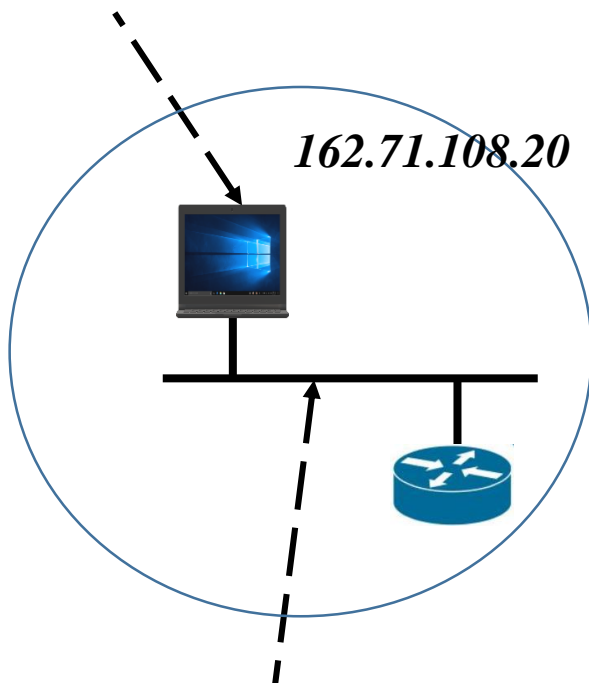


**CN: 与MN通信的  
对等节点**

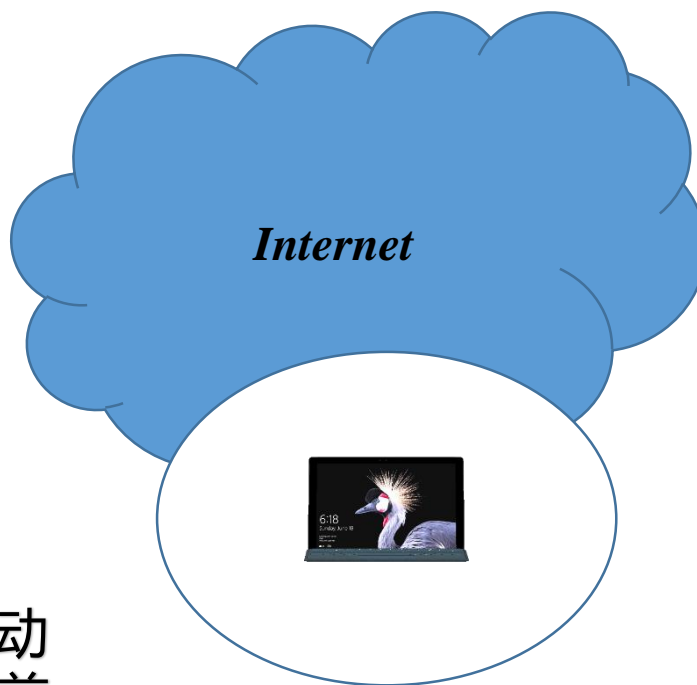


**外地代理FA (Foreign Agent)**  
MN访问网络中代表MN  
执行移动功能的实体

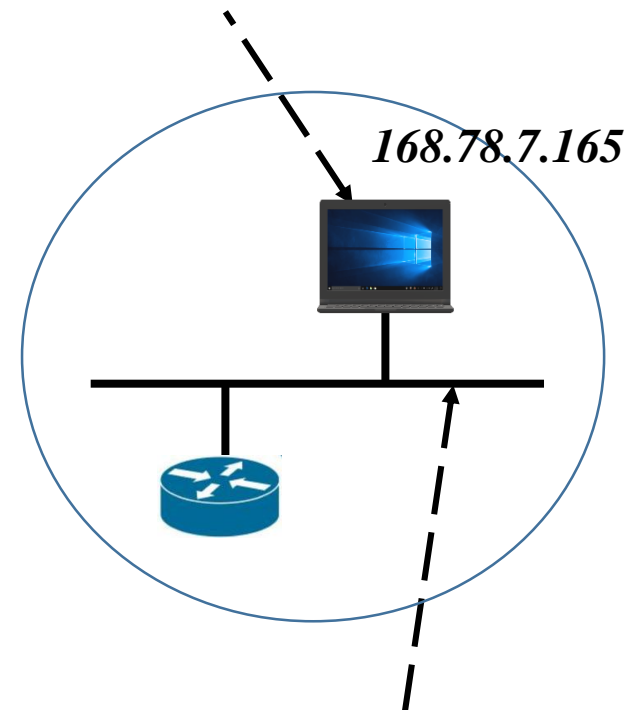
**永久地址 (Permanent Address) :**  
移动节点*MN*在家乡网络中的地址



**家乡链路 (Home Link) :** 与移动节点*MN*家乡地址具有相同网络前缀的链路，是移动节点*MN*在家乡网络时的链路



**转交地址 (Care-of-Address) :** 移动节点*MN*在外地网络中的地址



**外地链路 (Foreign Link) :** 与移动节点*MN*家乡地址网络前缀不同的链路



- 每个移动节点 (*MN*) 有两个 *IP* 地址
  - 一个固定的家乡地址 (用来标识该节点)
  - 一个可变的转交地址 (*CoA*) (用来转发数据报)

- 所有发送给移动节点*MN*的数据报通过隧道投递给*CoA*, *CoA*是隧道的出口

- 共享式*CoA*

  - 外地代理转交地址

  - 从外地代理获得的一个*IP*地址

  - 外地代理是隧道的出口

- 专用*CoA*

  - 配置转交地址(*Co-located CoA*)

  - 通过地址分配机制为移动节点分配的*IP*地址

  - 移动节点是隧道的出口

- ◆ 可节约IPV4地址

- ◆ 不再需要外地代理
- ◆ 增加了地址需求负担

- 为什么需要移动IP
- 移动IP的概念
- 移动IPV4

提出问题



定义问题



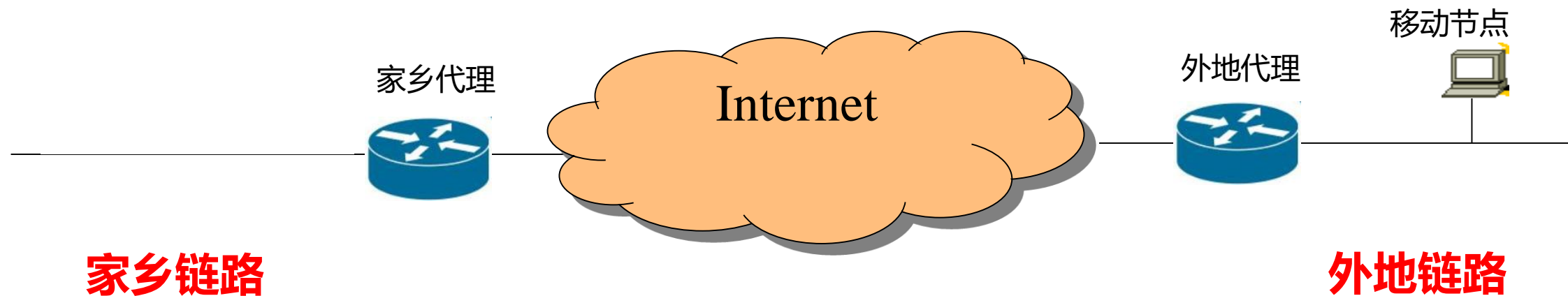
解决问题

- 1.代理发现 (*Agent Discovery*)
- 2.注册 (*Registration*)
- 3.分组路由
- 4.注销

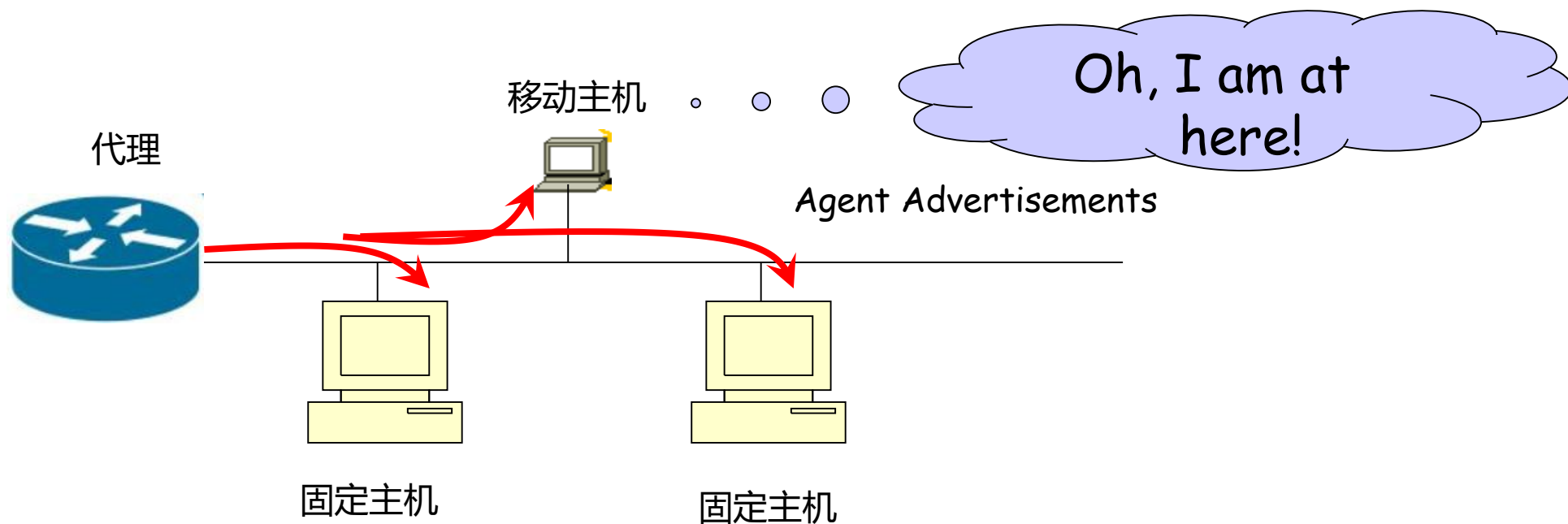
- (1) 移动代理 (*HA*或*FA*) 通过代理通告消息告诉*MN*移动代理的存在, *MN*也可以通过当前访问网络发送代理请求获得代理通告消息。*MN*接收到代理通告消息后, 可以确定它是在家乡网络还是外地网络上, 如果在家乡网络, 其操作与固定主机一样; 如果是从其它注册的网络回到家乡网络, 将通过和家乡代理交换 “注销请求” 和 “注销应答” 消息在家乡代理上进行注销
- (2) 如果*MN*发现它已经移动到了一个外地网络, 它将获得该外地网络上的一个转交地址 ( *CoA* ), 这个转交地址*CoA*或者来自*FA*的通告, 或者由*DHCP*确定, 前者称为外地代理转交地址 ( *Foreign Agent CoA* ), 后者称为配置转交地址 ( *Co-located CoA* )

- (3) 移动到外地网络上的**MN**随后与家乡代理交换**注册请求和注册应答消息**，注册它的转交地址**CoA**
- (4) **HA**截获发往**MN**家乡地址的数据分组
- (5) **HA**通过隧道把截获的数据分组发送到**MN**的转交地址**CoA**
- (6) 隧道的输出端点（**FA**或者**MN**本身）收到的报文进行拆封后，交给**MN**
- (7) **MN**发出的报文通过标准**IP**路由机制被路由到目标节点，不需要经过**HA**

□ *MN* 移动到外地链路后是如何通信的



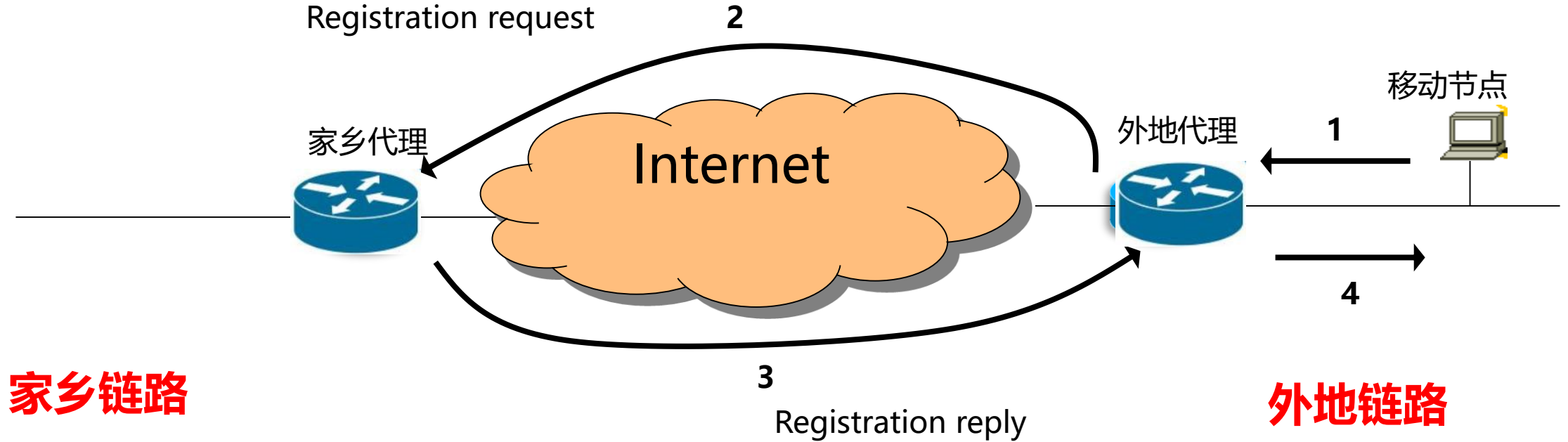
□ *HA*和*FA*均会周期性地广播代理通告消息 (*Agent Advertisements*)



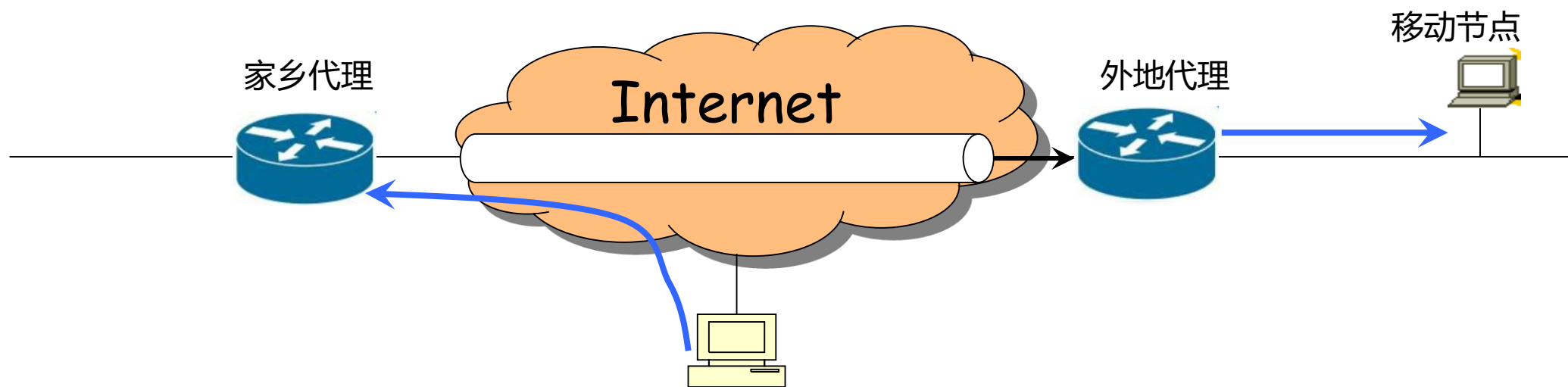


- *MN*检查代理通告*Agent Advertisement*消息，判断自己连接在家乡链路还是外地链路
- 如果*MN*从外地链路移回家乡链路，则必须通知*HA*取消先前的注册信息
- 连接在外地链路上的*MN*在*FA*的*Agent Advertisement*消息中得到*CoA*

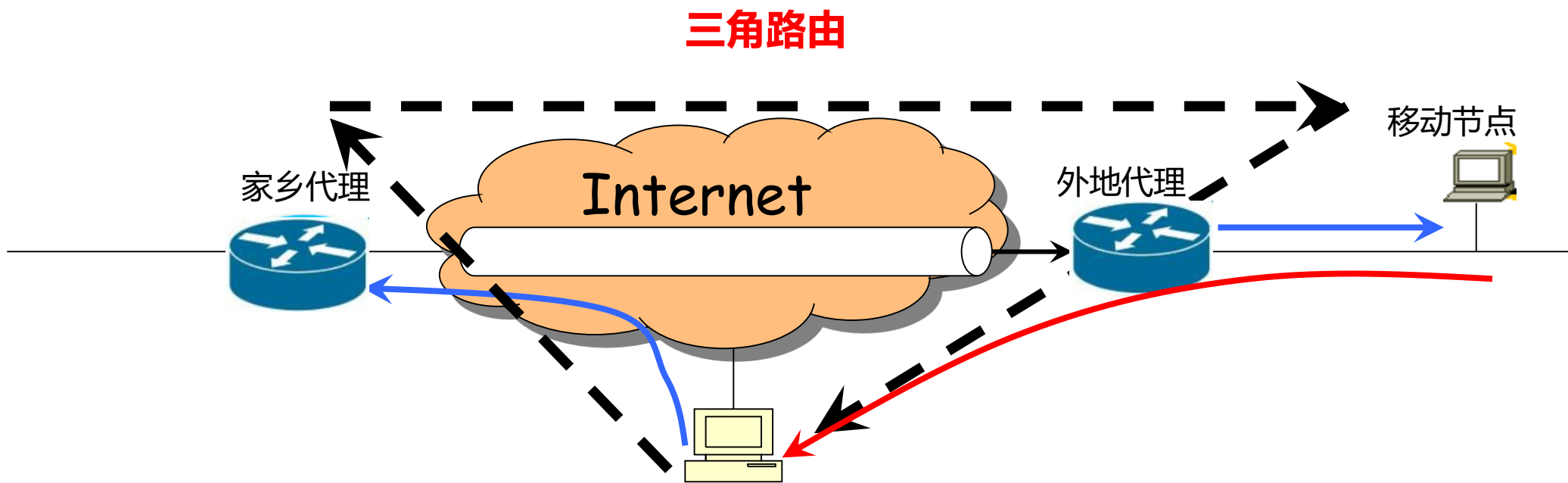
## □ *MN*向*HA*注册其*CoA*



- *Internet* 上其他主机向 *MN* 发送的数据报将被 *Internet* 路由到 *MN* 的 *HA*
- *HA* 将 *MN* 的数据包以隧道方式传送，隧道的出口地址为先前注册的 *MN* 的 *CoA*
- *FA* 抽取出隧道包中的原始数据报，并将其转发给 *MN*



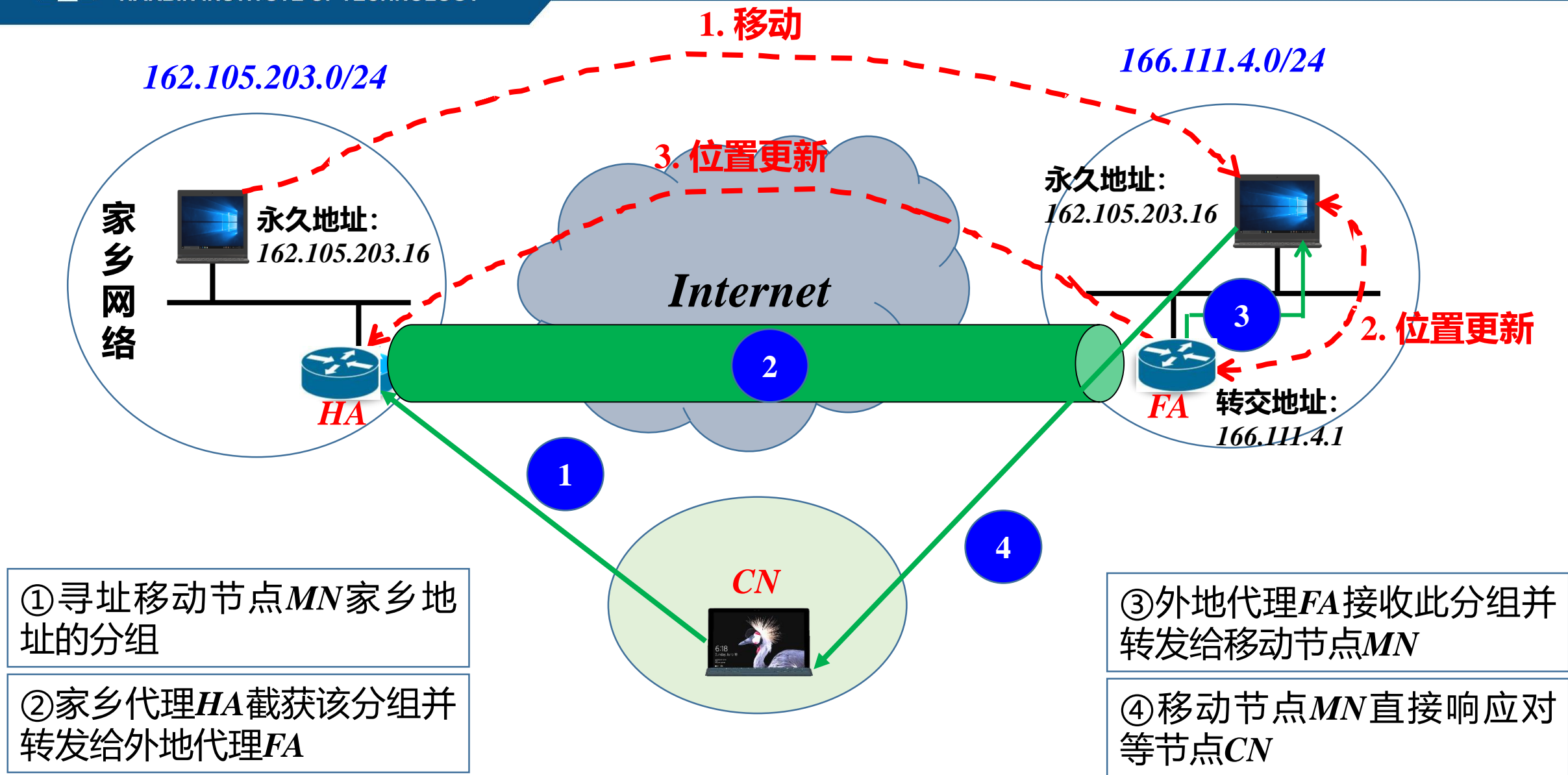
□ *MN* 发送给 *CN* 的数据报经由正常的 *Internet* 路由到达 *CN*



□ *MN* 移动到外地链路之后，除非使用特定主机路由等一些特别手段，现有的 *Internet* 路由机制不可能将发送到 *MN* 家乡地址的数据报转发给 *MN*

路由盲区！

□ 由前面讨论，特定主机路由方案不可行，于是，移动 *IP* 使用隧道技术！



## 第一步：通告/代理发现 (*Agent Discovery*)

□ *MN* 通过收到的代理通告消息确定其接入点或 *IP* 地址

- (1) 确定连接的链路
- (2) 检测是否改变了接入点
- (3) 如果连接到一个外地网络则获得一个 *CoA*
- (4) 允许向代理发送代理请求消息
- (5) *Agent discovery* 消息由 *ICMP (Internet Control Message Protocol)* 报文承载

## 第二步：注册转交地址 (*Registration*)

□ *MN* 请求 *FA* 为其服务，并向 *HA* 报告新 *CoA*

- (1) 用注册消息向 *HA* 注册和解除注册
- (2) 注册消息由 *UDP* 报文承载

注意： *CoA* 必须是通过常规 *IP* 路由可传递数据报的地址

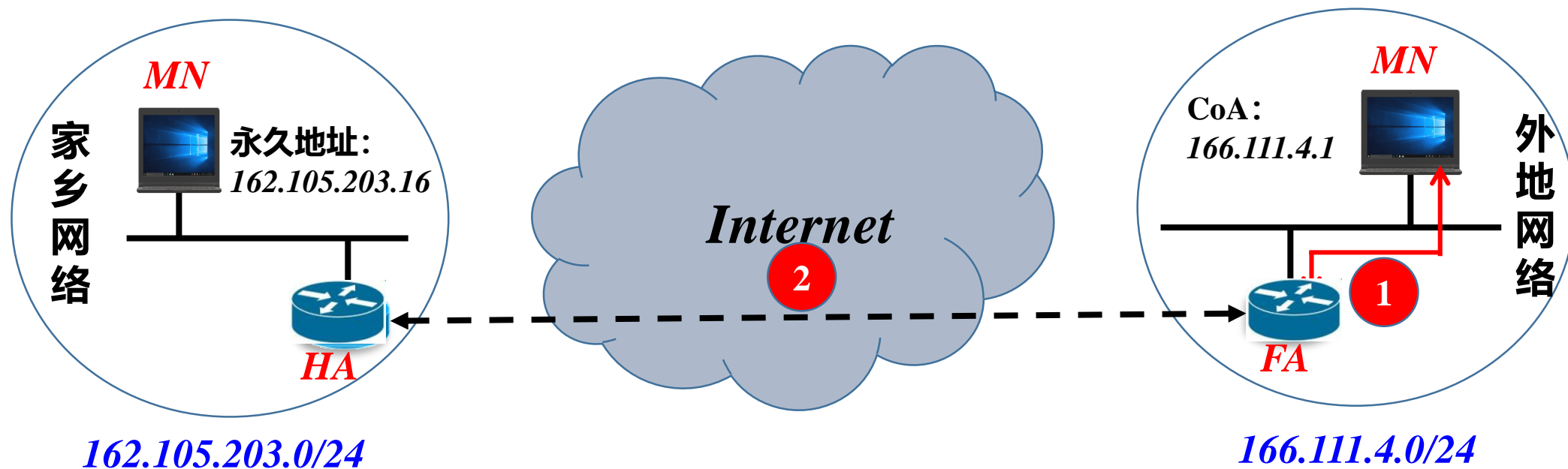


第三步：隧道（完成路由）转发数据报

- 移动IP把数据报隧道给离开家乡网络的MN
- 在隧道的入口点进行封装
- 在隧道的出口点进行拆封



使MN进行移动检测，判断其在家乡网络还是在外地网络，或者从一个外地网络移动到另一个外地网络



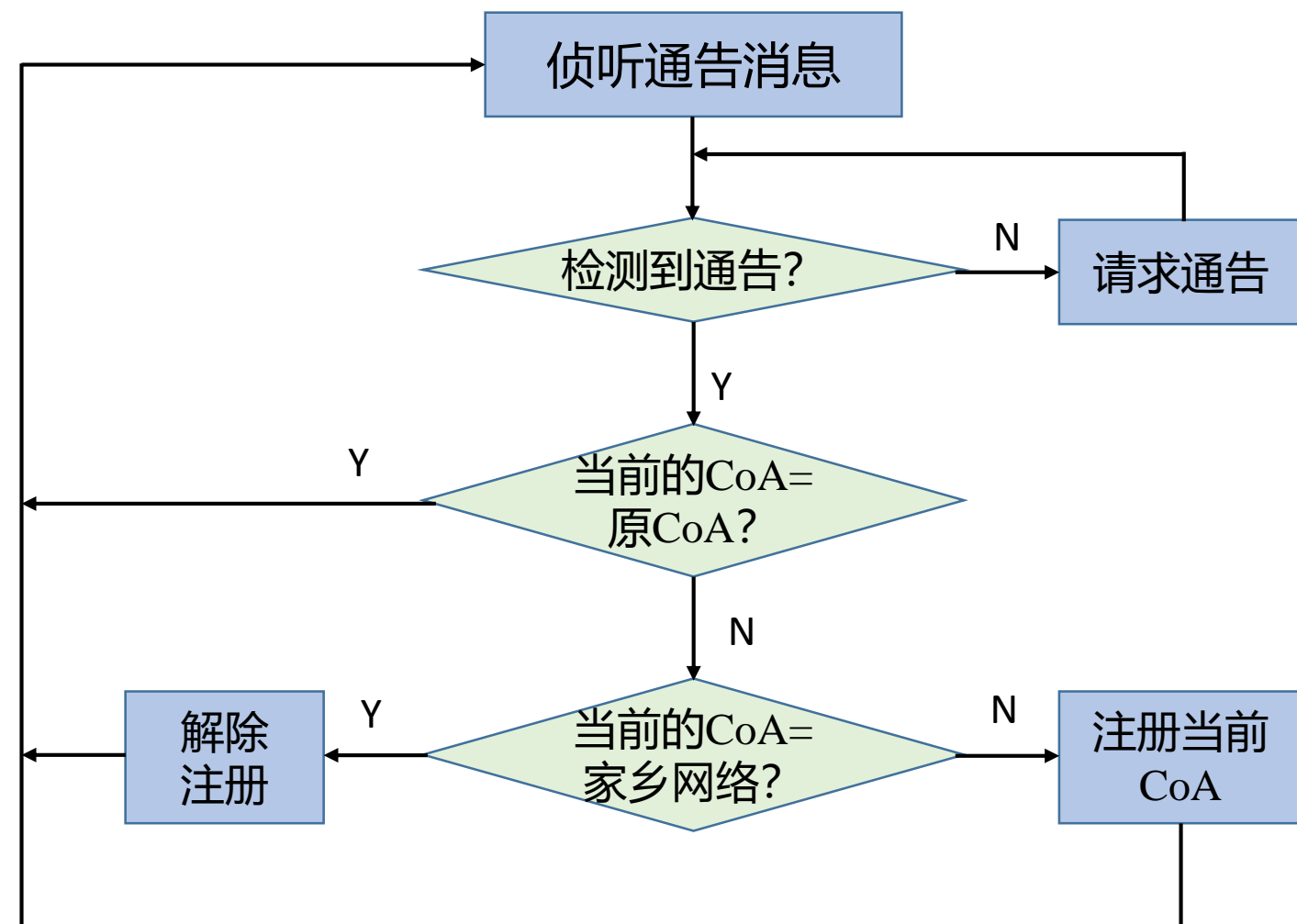
## □ FA的作用:

- 为MN生成CoA
- 通告其HA
- 可由MN自己担任

① MN进入外地网络后与FA取得联系

② FA与HA联系 “这个移动节点现在在我这里”

- 定义了代理通告和代理请求两个消息（基于ICMP路由发现机制）
- 移动代理（HA/FA）定期发送代理通告消息通告自己的存在
- MN通过代理请求消息请求代理
- 移动代理（HA/FA）用代理通告作为MN的代理请求响应消息



□当 $MN$ 从一个无线网段移动到另一个无线网段时，如何确定其新接入点或者 $IP$ 地址？

□通过代理发现， $MN$ 可以确定自己连接在家乡网络还是外地网络，可以确定是否已经改变了接入点

□一旦 $MN$ 获得一个新 $CoA$ 便立即进入注册过程

□ **ICMP**的**Code**字段明确指示移动代理的作用：

- (1) **Code=0**，作为常规路由器，不与**MN**关联
- (2) **Code=16**，作为**FA**，此时必须把**MN**发送的数据报路由给默认路由器

**RFC1256**：ICMP路由发现消息  
**RFC3220**：IPV4的移动支持

IP header(20 bytes)
ICMP Router Advertisement
Agent Advertisement

## *advertisement*

Type(9)	Code(0)	Checksum
#addr.	Addr.size	lifetime
Router addr1		
Preference level1		
Router addr2		
Preference level2		

## *solicitation*

Type (10)	Code(0)	Checksum
Reserved		

□广播代理通告消息的代理特性由标志位 (*Type*) 描述

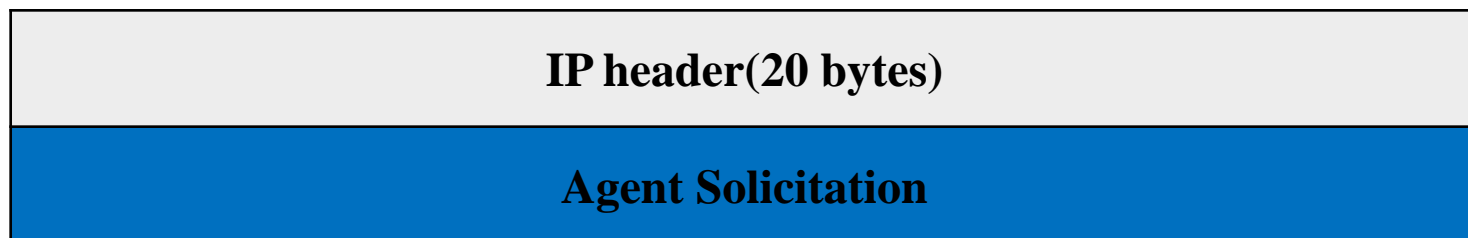
标志位Type	标志含义	标志位Type	标志含义
R	必须注册	M	允许最小封装
B	代理忙	G	允许GRE封装
H	家乡代理	r	接收时忽略
F	外地代理	T	支持逆向隧道

愿意接收注册请求的最长时间

初始化后发送的通告计数

Type (16)	length	Sequence number	
Registration lifetime		RBHFMGrT	reserved
CoA1			
CoA2			

- 与**ICMP** 路由器请求报文格式相同
- MN**通过该消息发现自己所处的位置和所在网络的移动代理
- 连续三次请求未获得代理反馈通告，则以**指数后退算法**延迟重发代理请求消息



- 任何不能被链路层协议发现的移动代理必须发送代理通告消息
- 所有移动代理都应该响应发送到224.0.0.1的代理请求消息
- 移动代理必须限制它广播或者组播通告消息的速度，连续3次没有获得响应必须后退再次发送的时间
- 代理可配置成只在响应代理请求消息时才发送代理通告消息



## □发送代理请求

- 在未收到代理通告及未通过其他方法获得 $CoA$ 时,  $MN$ 应发送代理请求
- $MN$ 必须限制发送代理请求的速度 (按二进制指数后退算法)

## □处理代理通告

- $MN$ 必须处理收到的代理通告, 区分出代理通告消息和 $ICMP$ 路由器通告消息
- 如果通告地址多于一个, 则取出第一个地址开始注册
- $MN$ 收到 $R$ 位 (表示必须注册) 的通告后, 即使已经获得可配置 $CoA$ , 也必须向 $FA$ 注册

## □移动检测

- 如果**MN**在生存期 (*lifetime*) 内没有收到来自同一个代理的通告, 则可假设自己已失去了和这个代理的连接
- 如果收到了另一个代理的通告, 则立即尝试连接该新代理, 否则**MN**应该去发现新的移动代理

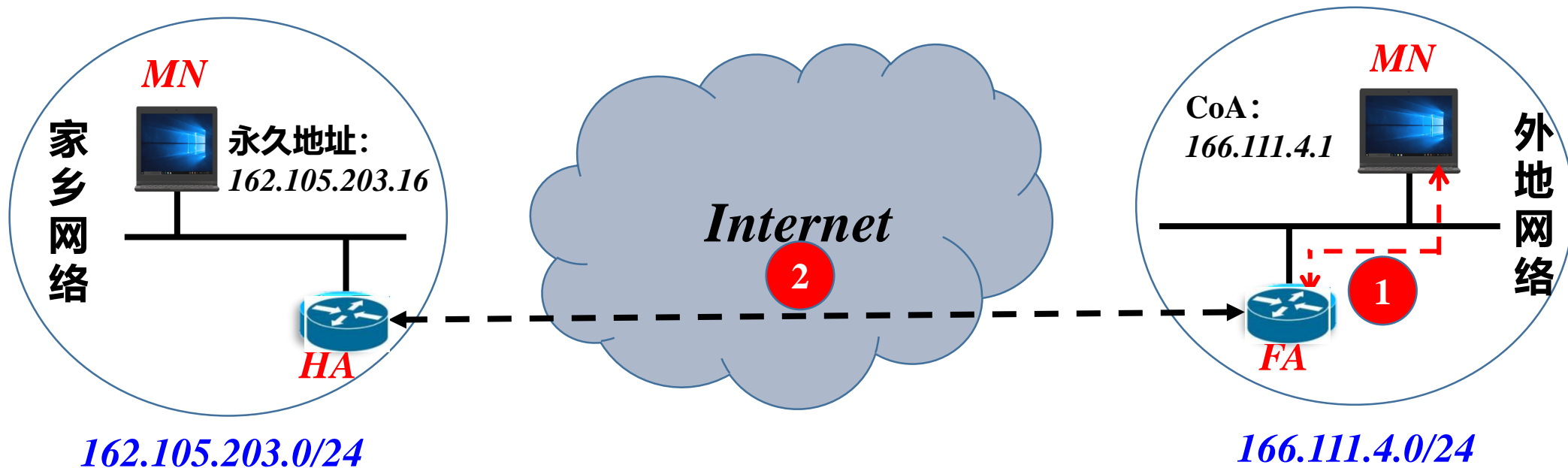
## □回到家乡

- 当**MN**收到来自其**HA**的通告时可确信自己返回家乡, 应该向**HA**注销

## □序号处理

- 如果**MN**从注册的**FA**相继收到两个“通告”, 其中第二个序号值小于第一个, 且在0~255之内, 则**MN**应该再次进行注册

- ***MN***到达新的网络后，通过注册过程将自己的可达信息通知***HA***，注册过程涉及***MN***、***FA***和***HA***，***MN***与***HA***交换注册报文，在***HA***上创建或修改“移动绑定”，使***HA***在规定的生存期内保持***MN***的家乡地址与***CoA***的关联性
- 通过注册可以达到以下目的
  - (1) 使***MN***获得***FA***的转交服务
  - (2) 使***HA***知道***MN***当前的转交地址
  - (3) ***HA***实时更新即将过期的***MN***的注册信息，或注销回到家乡的***MN***



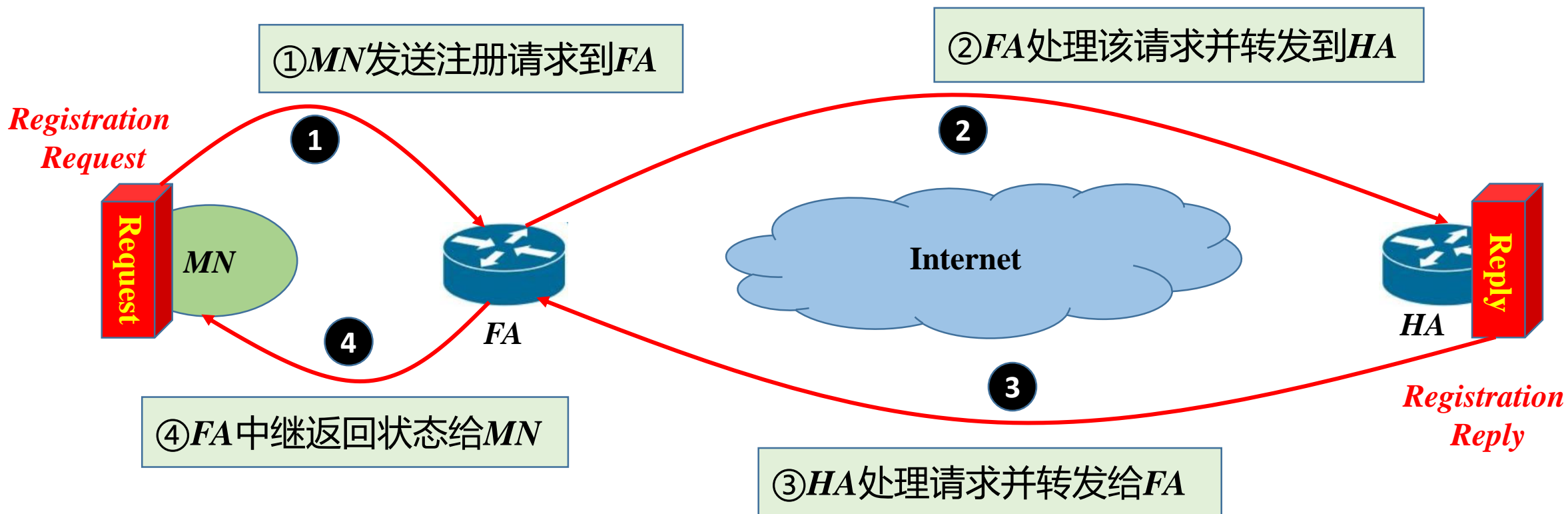
□ FA的作用:

- 为MN生成CoA
- 通告其HA
- 可由MN自己担任

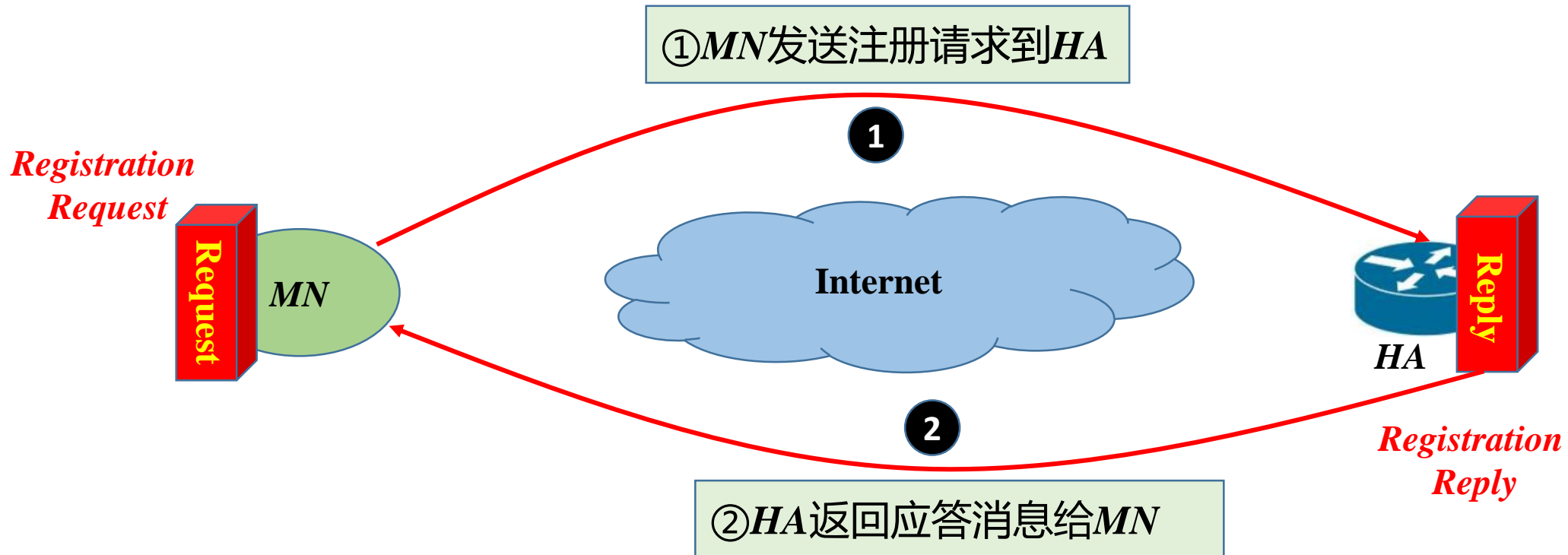
① MN进入外地网络后与FA取得联系

② FA与HA联系 “这个移动节点现在在我这里”

□如果移动节点使用外地代理CoA

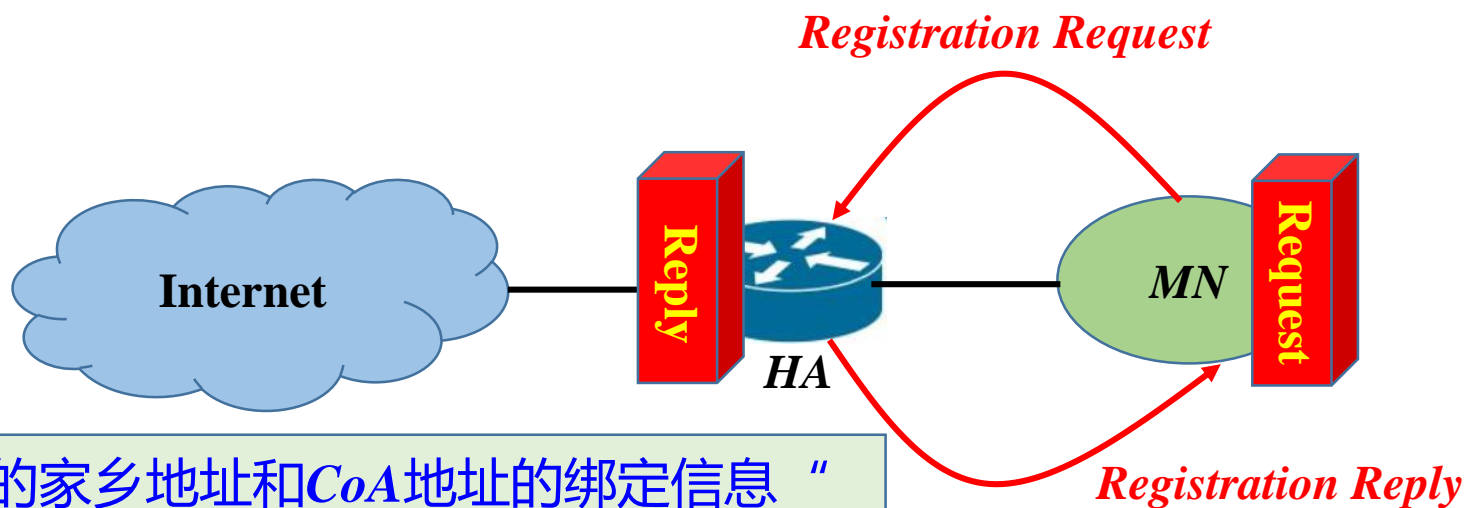


□如果移动节点使用配置CoA



□如果移动节点回到了家乡网络，则必须在家乡链路上进行注册（**注销其移动绑定信息**）

① MN向HA发送*Registration*消息（通过UDP报文）



② HA更新 "*MN*的家乡地址和*CoA*地址的绑定信息 "

- *Home address*
- *Care-of-Address*
- *Lifetime*

- **HA** 创建一个**移动绑定**，将**MN**的家乡地址和当前**CoA**绑定在一起，并设置生存期
- **MN**在此绑定信息超时之前必须续订

标志位Type	标志含义	标志位Type	标志含义
S	同时绑定	G	使用GRE封装
B	请求广播报文	r	保留
D	自己拆封	T	请求逆向隧道
M	使用最小封装	r	保留



Type (1)	SBDMGrTx	lifetime
Home address		
Home Agent		
COA		
identification		
Extensions.....		



- 如果**MN**不知道**HA**地址，就向家乡网络**广播注册消息**
- 每个有效**HA**均给予响应，**MN**采用某个有效**HA**的地址发起注册请求
- HA**和**FA**类似于**本地和外地**数据库
  - 一次有效的注册，**HA**为**MN**创建一个条目-**相当于本地数据库中的一条记录**
    - {**MN**的**CoA**、标识字段和此次注册的生存期}
  - 每个**FA**维护一个访问列表-**相当于外地数据库中的一条记录**
    - {**MN**链路层地址、**MN**的家乡地址、**UDP**注册源**port**、**HA**的**IP**地址、标识字段、注册生存期、当前或未处理注册的剩余生存期}

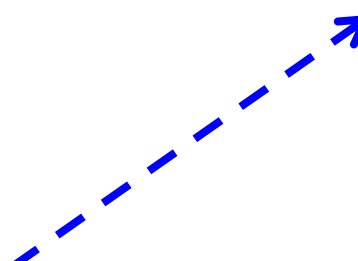
□ **HA** 返回**注册应答**表明注册是否成功

□ 如果**MN**通过**FA**注册，则该应答消息由**FA**转发

□ 注册请求可被拒绝

Code0: 注册成功  
Code1: 注册成功但不支持  
多个同时绑定

- 没有足够的资源
- HA不可达
- 太多的同时绑定
- 注册标识不匹配
- 认证失败等



Type (3)	Code	lifetime
Home address		
Home Agent		
identification		
Extensions.....		

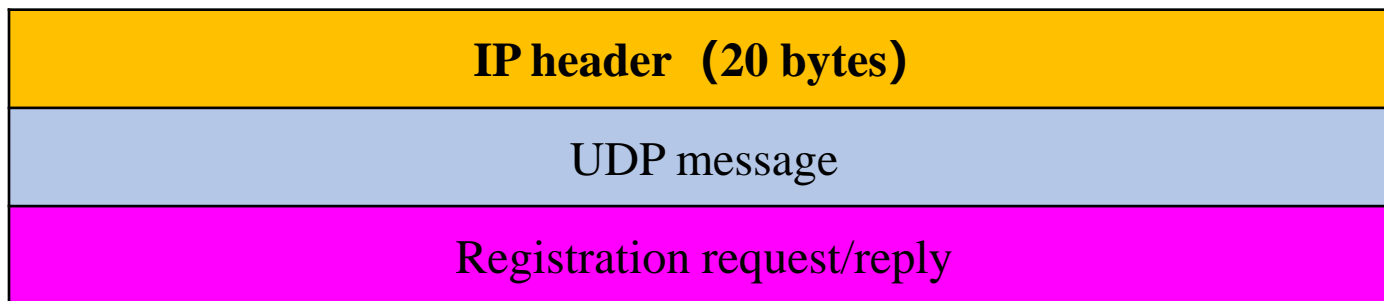
□注册请求和注册应答消息通过**UDP**报文传输

■**Port**: 434

■**Data**: 注册请求/应答

■**UDP** 开销小，在无线环境下性能优于**TCP**

**RFC768**: 用户数据报协议



- **MN**需要进行网络掩码的配置
- 只要检测到连接网络发生变化就发起注册
- 发送注册请求
  - **IP**源地址为**CoA**/家乡地址
  - **IP**目的地址
    - **FA**的地址/**224.0.0.1**
    - **HA**的地址/子网广播地址
- 处理注册应答
  - 接受（外地/家乡）/拒绝

□ **FA**在**MN**和**HA**之间中继注册请求，并且如果提供**CoA**，还要为**MN**拆封数据分组

□ **FA**的配置表和注册表

■ 维护**MN**的访问表

□ **FA**对注册请求的处理


■ 有效性检查

■ 转发请求到**HA**

□ 接收注册应答

■ 有效性检查

■ 转发应答到**MN**

- 
- MN的链路层地址
  - MN的家乡地址
  - UDP源端口号
  - HA地址
  - 标识字段
  - 请求的注册生存期
  - .....

- **HA**从**MN**接收注册请求，更新自己关于该**MN**的移动绑定记录，并为每个请求启动一个应答作为响应。
  - **HA**的配置表和注册表
  - **HA**对注册请求的处理
    - **HA**接受**MN**请求
    - 更新对于该**MN**的绑定信息
  - 发送注册应答

**The End !**