

Internet技术

张冬梅
北京邮电大学 计算机学院
zhangdm@bupt.edu.cn

移动互联网概述

□ 移动互联网定义

- 互联网技术、无线通信和移动技术相结合产生了移动互联网
- 百度百科：移动互联网，就是将移动通信和互联网二者结合起来，成为一体。

□ 互联网发展的三个阶段

- 固定/有线互联网络
- 无线互联网
- 移动互联网

□ 移动互联网络中存在的挑战

- 无线信道
- 用户移动性(移动互联网需要解决的关键问题)

□ 移动互联网需要解决的问题

- 如何保证终端和子网在移动过程中通信的连续性
- 如何解决终端和子网移动对网络各方面的影响
 - 路由协议、路由最佳化
 - 快速切换
 - 网络安全
 - 网络服务质量
 -

移动互联网

□ 移动互联网概述

□ 移动IP

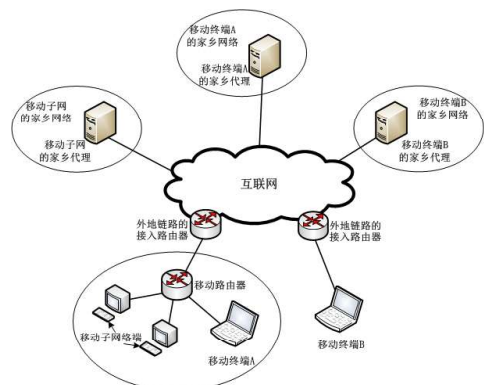
□ 移动互联网目标

- 无论移动终端还是移动子网，都可以在任意地方以任意方式接入到互联网，同时保持通信不间断。

□ 移动互联网移动性依次为：

- 终端或单机移动
- 子网移动
- 节点、子网等混合移动

简单
↓
复杂



移动性管理

- **移动性管理**指通信网中**用户或者终端的位置发生改变时能够继续通信，并实现位置信息的更新及管理**的能力，也即，用户的通信和对业务的访问**不受移动目标网络接入点变化的影响**。
- 移动网络中建立呼叫需要解决的问题
 - 用户所在的位置
 - 用户识别
 - 用户所提供的业务

2018/12/12

7

不同层的移动性管理

- 按工作的层次
 - 应用层移动性管理协议：SIP
 - 传输层移动性管理协议：MSCTP
 - 网络层移动性管理协议：**MIPv4, MIPv6**
 - 链路层移动性管理协议：WiMAX, WIFI, GSM等

8

移动互联网

- 移动互联网概述
- **网络层移动管理--- MIP**

9

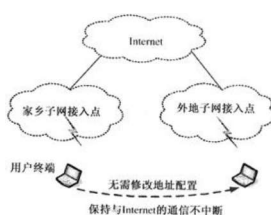
MIP

- 概述
- MIPv4协议
- MIPv6协议
- 安全技术

10

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。



网络层移动性管理效果示意图

11

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

12

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

13

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

14

MIPv4协议机制

□ 相关实体和术语

□ MIPv4工作原理与过程

□ 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

15

16

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

17

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)

18

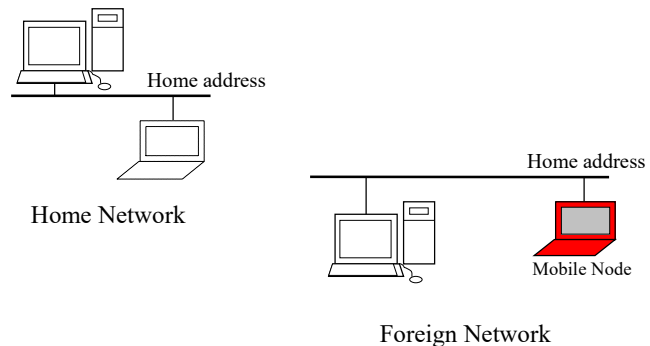
MIPv4工作原理与过程

□ Mobile IP协议的内容包括

- 移动性管理
- 移动节点的数据传输

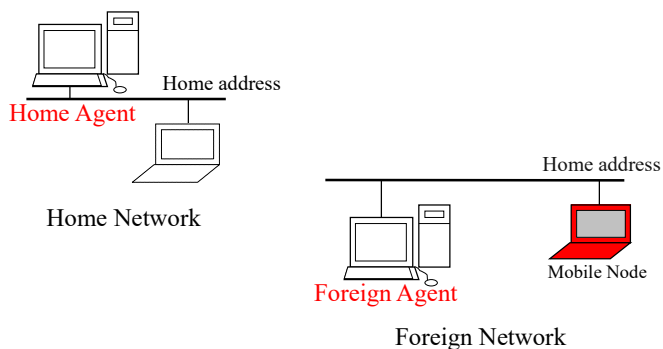
19

MIPv4工作原理与过程



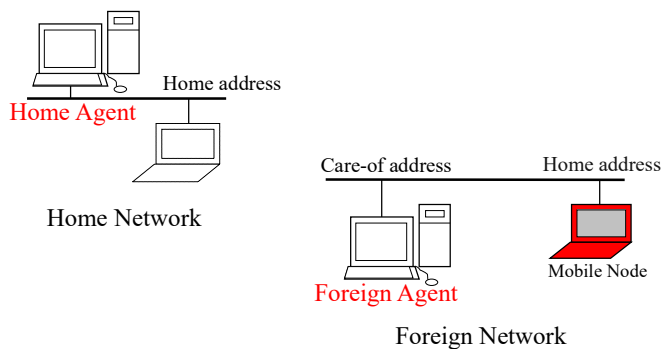
20

MIPv4工作原理与过程



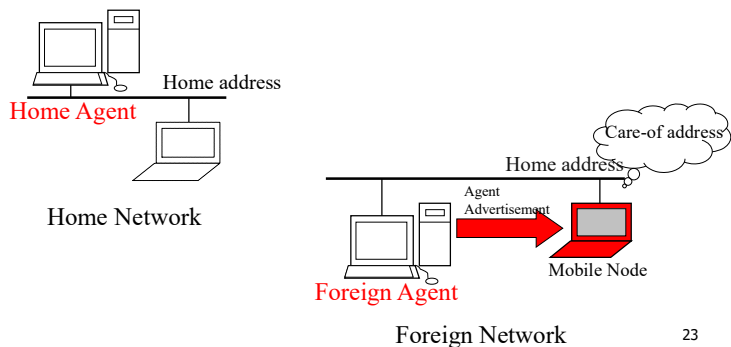
21

MIPv4工作原理与过程



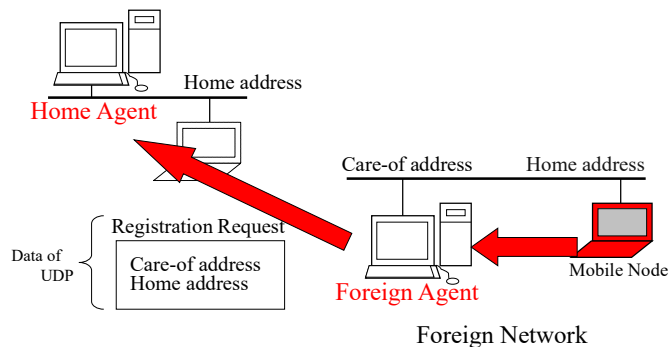
22

MIPv4工作原理与过程



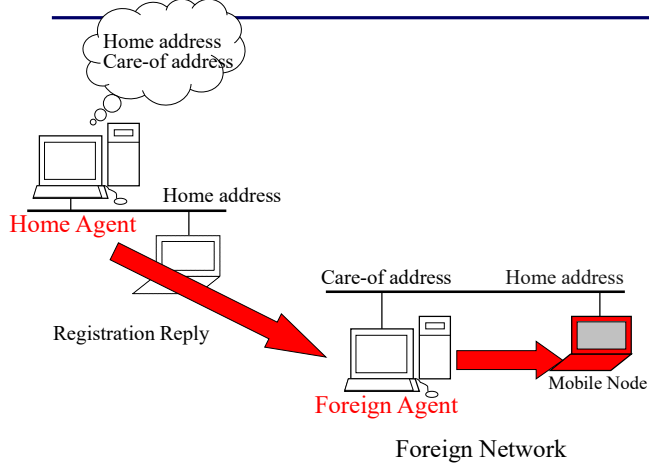
23

MIPv4工作原理与过程



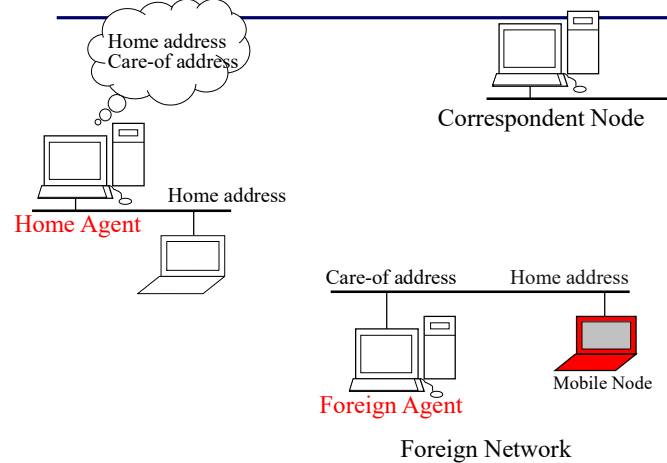
24

MIPv4工作原理与过程



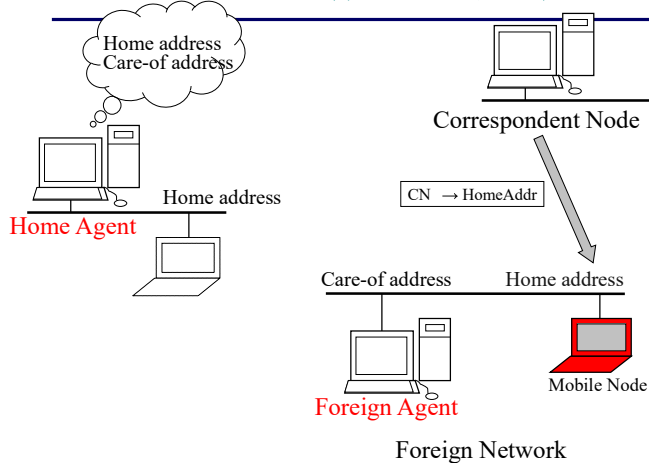
25

MIPv4工作原理与过程



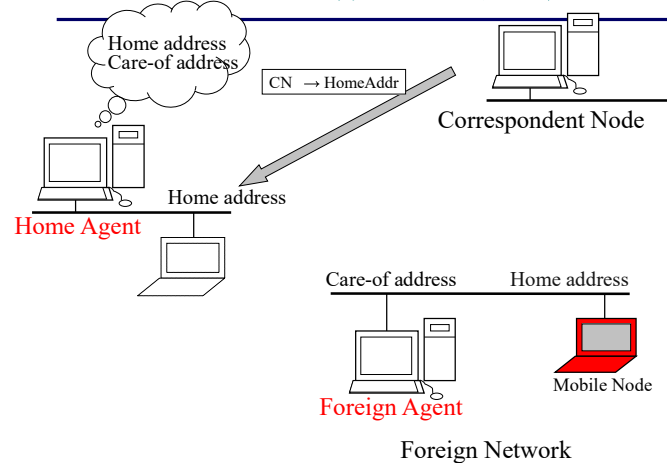
26

MIPv4工作原理与过程



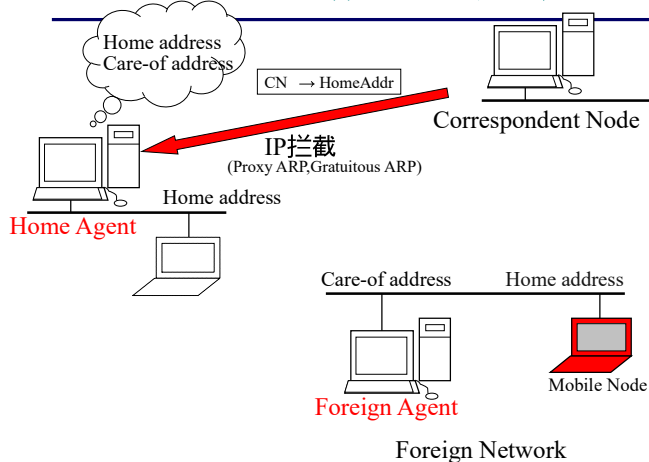
27

MIPv4工作原理与过程



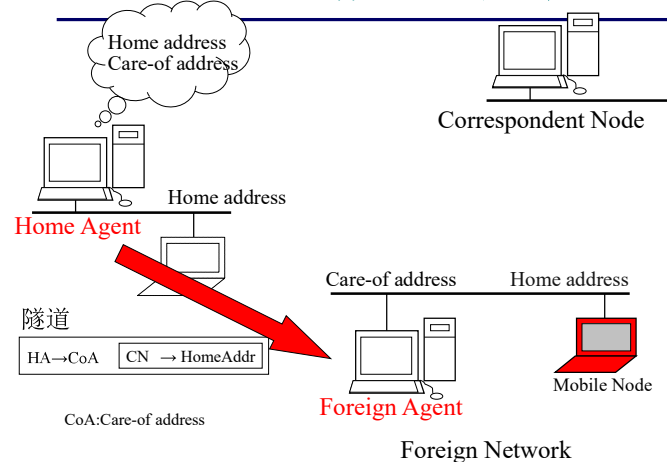
28

MIPv4工作原理与过程



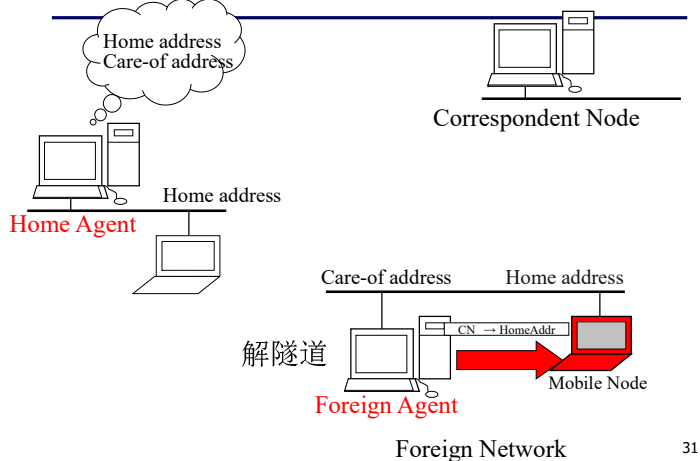
29

MIPv4工作原理与过程



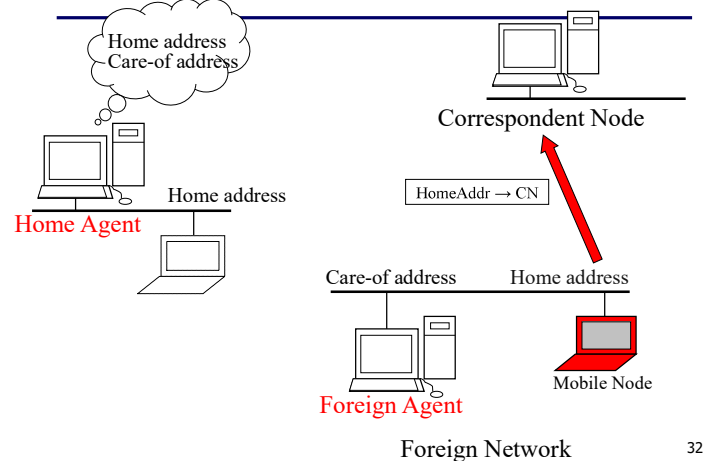
30

MIPv4工作原理与过程



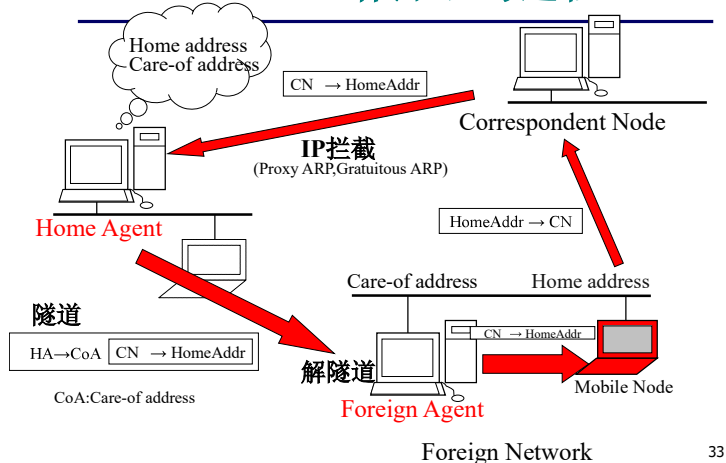
31

MIPv4工作原理与过程



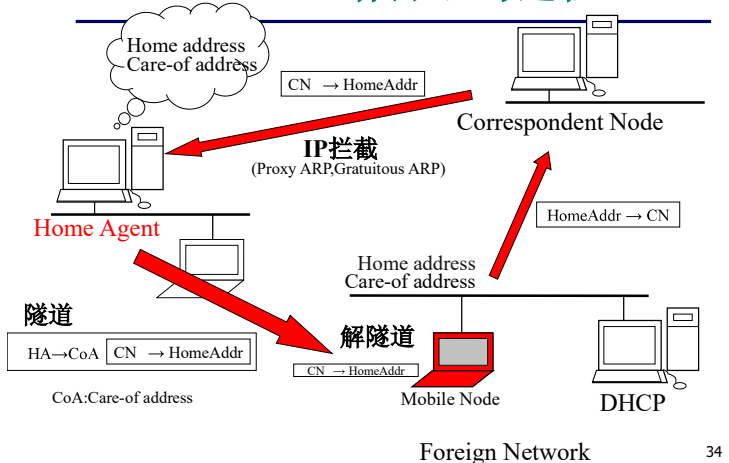
32

MIPv4工作原理与过程



33

MIPv4工作原理与过程



34

MIPv4的基本工作过程(文字描述)

- 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

35

MIPv4的基本工作过程(文字描述)

- 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）

36

MIPv4的基本工作过程(文字描述)

- 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

37

MIPv4协议

IP header										
ICMP Router Advertisement Message										
Type	Length			Sequence Number						
Registration Lifetime				R	B	H	F	M	G	V
Zero or more Care-of addresses										

R:Registration Required B:Busy
H:Home Agent F:Foreign Agent
M:Minimal Encapsulation G:GRE Encapsulation
V:Van Jacobson header compression

38

Registration

Request packet	IP header	UDP header	Registration request	Mobile-Home Auth. Ext.	Mobile-Foreign Auth.Ext.
----------------	-----------	------------	----------------------	------------------------	--------------------------

MN→FA→HA

Reply packet	IP header	UDP header	Registration reply	Mobile-Home Auth. Ext.	Mobile-Foreign Auth.Ext.
--------------	-----------	------------	--------------------	------------------------	--------------------------

HA→FA→MN

Authentication Extention	Type	Length	SPI
	Authenticator		

39

Registration Request/Reply

Type	Flag	Lifetime
Home Address		
Home Agent		
Care-of Address		
Identification		
Extensions		

<Registration Request>

S	B	D	M	G	C	rsv
---	---	---	---	---	---	-----

<Flag>

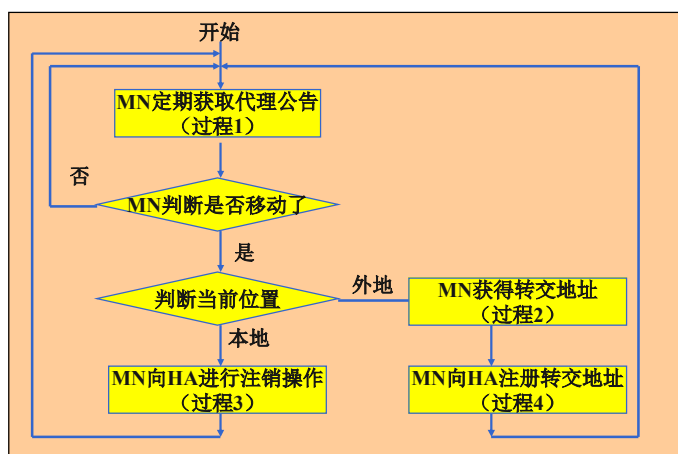
Type	Flag	Lifetime
Home Address		
Home Agent		
Care-of Address		
Identification		
Extensions		

<Registration Reply>

S:Simultaneous Binding
B:Broadcast Datagram
D:Decapsulation by Mobile Node
M:Minimal Encapsulation
G:GRE Encapsulation
V:V.Jacobson Header Compression

Code:
0,1=O.K.
64-88=NG by FA
128-=>Ng by HA

40



41

基本过程

- 代理搜索**：利用该过程，移动节点MN可以判断其当前的网络位置，并得到一个转交地址。
- 注册**：移动节点向外地代理请求服务，并通知家乡代理它的转交地址。
- 数据包转发**：当移动节点连接在外地网络是，对它发出的或者发往它的数据包进行路由的特殊机制。

42

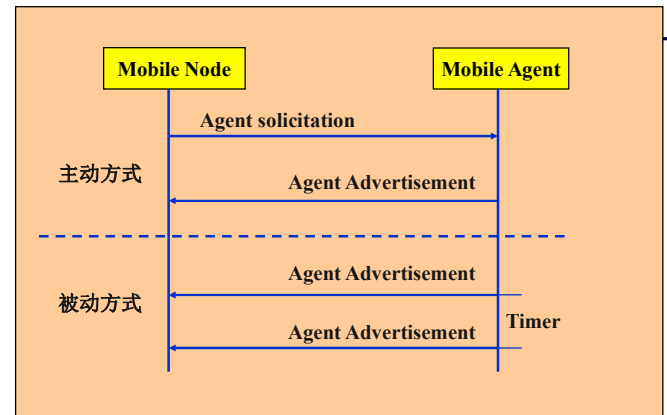
过程1：代理搜索

□ MN利用该过程

- 判断它当前连在家乡代理上还是外地链路上
- 检测它是否切换了链路
- 当连在外地链路上时，得到一个转交地址

□ 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(**Agent Advertisement**)
- 主动获得方式：主动发送移动代理请求(**Agent Solicitation**)消息来立即获得代理公告



43

44

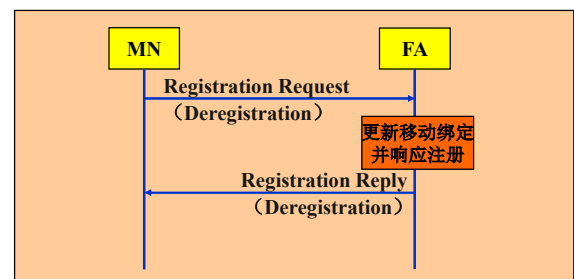
过程2：MN获得转交地址

□ 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：



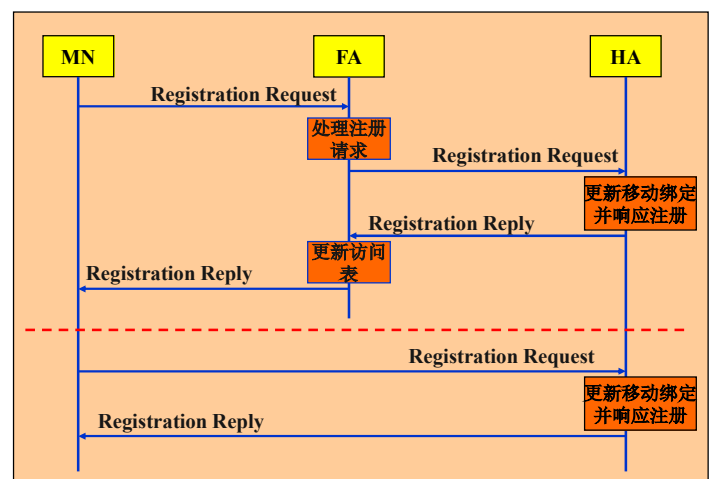
45

46

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）

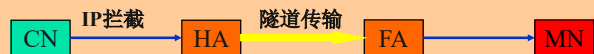


47

48

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

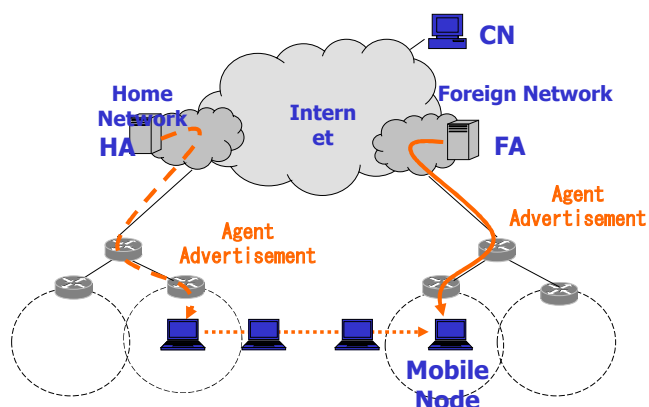


- 移动节点发送IP数据报过程

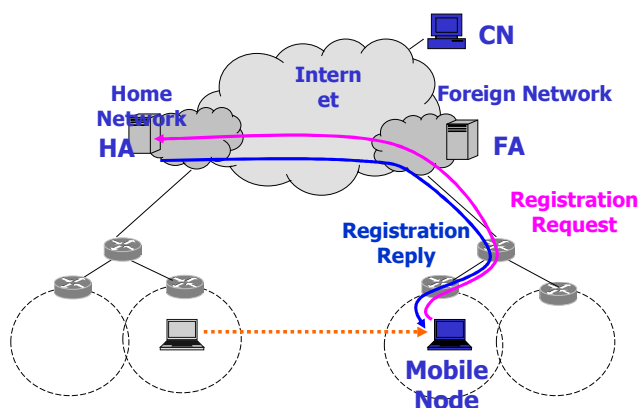
移动节点采用标准的IP协议发送IP数据报

49

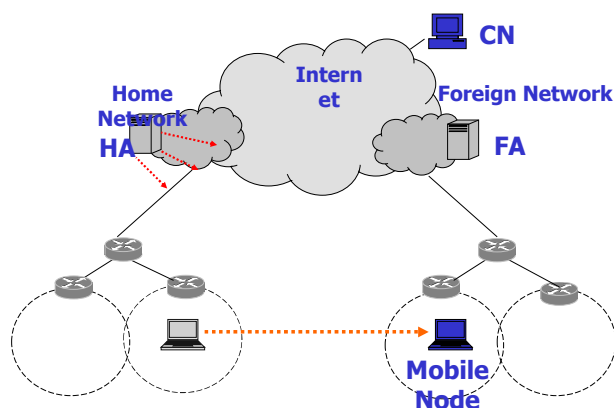
MIPv4 : Concepts



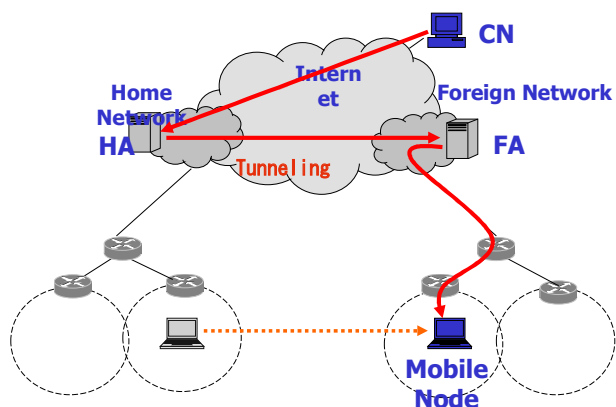
MIPv4 : Concepts



MIPv4 : Concepts

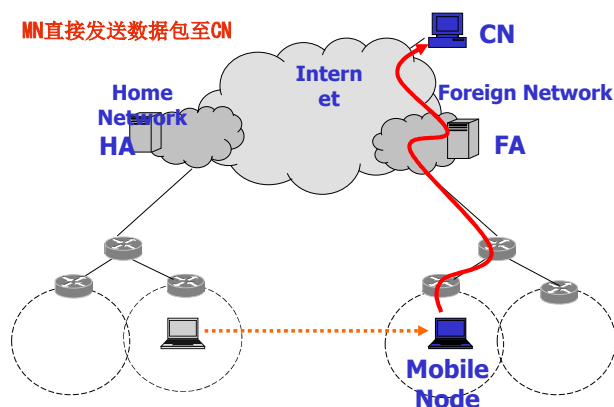


MIPv4 : Concepts



MIPv4 : Concepts

MN直接发送数据包至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,解决“拓扑错误分组”问题

□ 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“目的选项首部”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

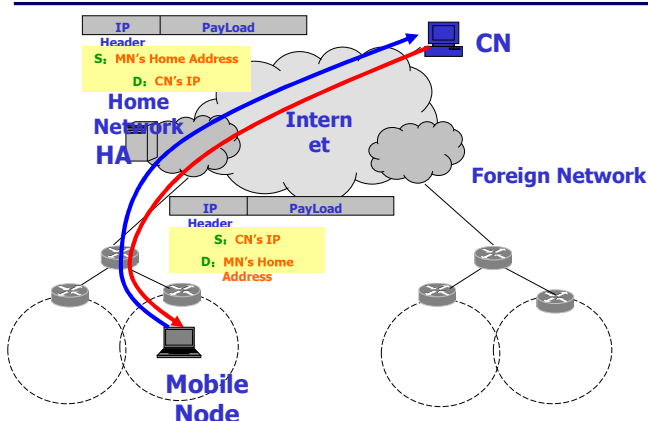
MIPv6基本工作原理(2/2)

- 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

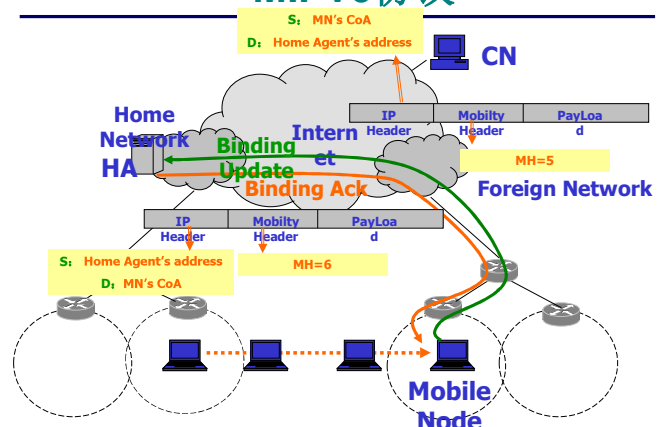
57

58

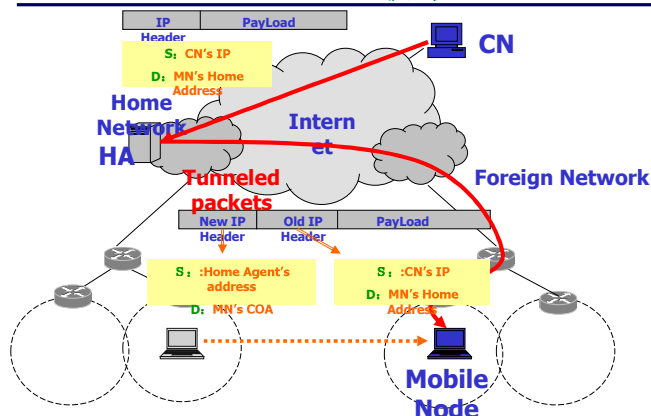
MIPv6协议



MIPv6协议



MIPv6协议



与移动IP相关的消息定义

□ RFC3775为移动IP修改了

- IPv6协议：定义了新的扩展头标，同时为现有头标定义了新的类型和选项
- ICMPv6协议：增加了新的消息类型，同时修改了已有的邻居发现消息的格式

□ IPv6

名称	功能	变化情况
移动头标	携带MIPv6协议的信令消息	新定义的扩展头标
家乡(归属)地址选项	当分组从移动节点发送时，该选项携带移动节点的家乡(归属)地址	信宿选项头标中新定义的一个首部类型
类型2路由头标	当分组从家乡代理或通信节点发送到移动节点时，该首部携带移动节点的归属地址	路由选项头标中新定义的一个首部类型

62

与移动IP相关的消息定义

□ ICMPv6

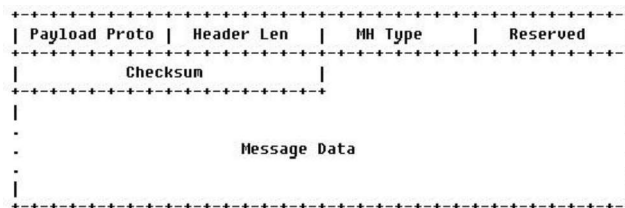
名称	功能	变化情况
家乡代理地址发现请求/公告	提供了在移动节点离开家乡网络时发现移动节点家乡代理地址的机制	新定义的ICMPv6报文类型144/145
移动前缀请求/公告	用于当移动节点离开家乡网络时向移动节点请求/告知家乡网络的前缀信息	新定义的ICMPv6报文类型146/147
路由器公告	增加一个标志用于指示路由器是否具有家乡代理功能	增加了一个标志参数
前缀信息选项	MIPv6中，家乡代理将其地址包含在该选项中作为前缀信息的一部分。同一个归属网络中的所有归属代理可以通过监听该选项获取网络中所有归属代理的地址	参数的含义变化了
归属代理信息选项	携带家乡(归属)代理的寿命和优先级	新定义的邻居发现选项
公告间隔选项	携带路由器两次发送的路由器请求报文之间的时间间隔	新定义的邻居发现选项

63

Mobility Header 选项

□ IPv6增加了Mobility Header选项

□ 格式



Mobility Header类型

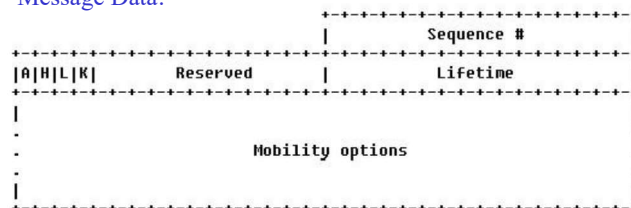
类型	名称	功能
0	BRR	绑定刷新请求：请求MN刷新其绑定
1	HoTI	家乡测试初始化
2	CoTI	转交测试初始化
3	HoT	家乡测试：用来响应HoTI
4	CoT	转交测试：用来响应CoTI
5	BU	绑定更新：MN向HA/CN注册，通告自己的当前CoA
6	BA	绑定确认：用来确认BU的接收
7	BE	绑定错误：标识与移动有关的错误

65

Binding Update Message

MH Type=5

Message Data:



A:Acknowledge

H:Home Registration

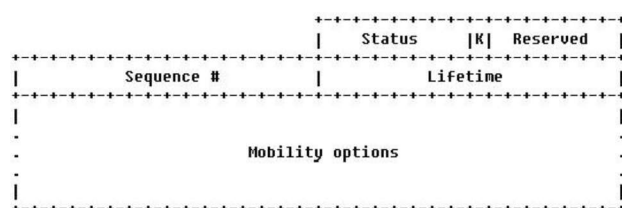
L:Link-Local Address Compatibility

K:Key Management Mobility Capability

Binding Acknowledgement Message

MH Type=6

Message Data:



K:Key Management Mobility Capability

家乡(归属)地址选项

□ 是新定义的**信宿(目的)选项头标**

下一头标	路由头长度	选项类型	选项长度
家乡地址			

- 选项类型: **0xC9**(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
- MN离开家乡网络时,一般不直接发送源地址为家乡地址的分组。为什么?
- 采用MN与家乡代理之间的双向隧道发送分组
 - 使用含有MN家乡地址的信宿选项头标,同时将MN的转交地址设为源地址

68

家乡(归属)地址选项

□ 使用情况

- MN发送绑定更新消息时
- MN与CN进行具有路由优化的通信时
- MN发送移动前缀请求报文时

□ 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

69

类型2路由选项头标

□ 是新定义的一种路由头标

下一头标	路由头长度	路由类型=2	分片剩余=1
预留			
家乡地址			

□ 三种使用情况

- 节点发送绑定确认消息时
 - 家乡代理或CN执行路由优化时
 - 家乡代理发送移动前缀公告报文时
- 如果一个节点需要向离开家乡网络的MN直接发送分组,则需要使用类型2路由首部。

70

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

71

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绑定

73

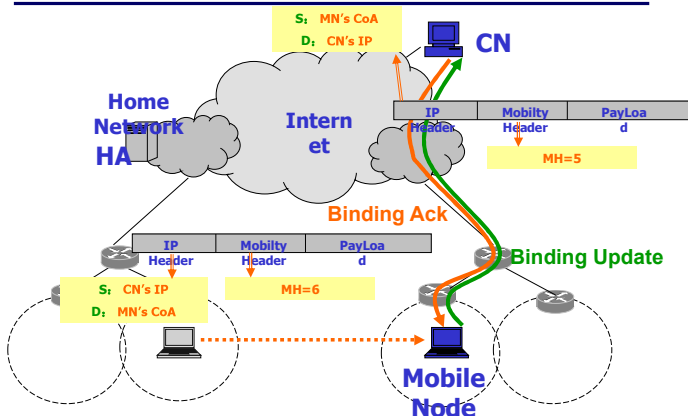
路由优化(3/3)

□ MIPv6的路由优化

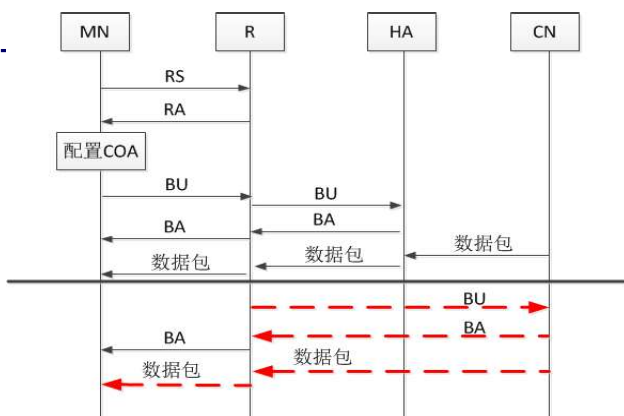
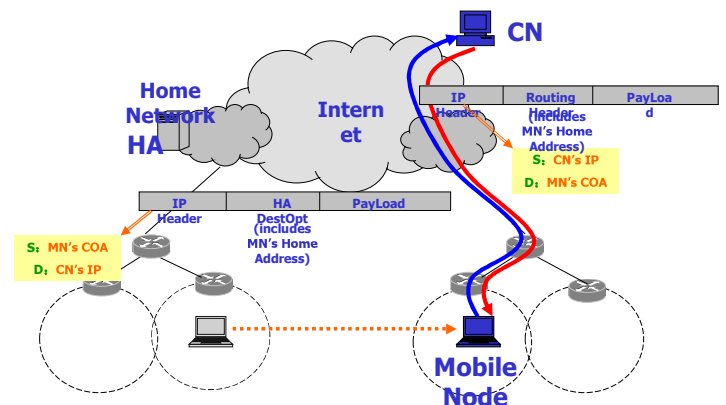
- CN发送分组至MN时：
 - 根据目的IP查询绑定缓存，如果存在匹配，直接发送到转交地址；
 - 如果不存在匹配，发送分组给家乡地址，经家乡代理的隧道发送给MN
- MN收到经家乡代理转发的分组后，向CN发送绑定更新消息

74

Mobile IPv6



Mobile IPv6 : Concepts



77

□ 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 (ICMP消息); 绑定更新 (扩展头标)
- 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

78

MIP的安全机制

- 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

79

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比特密钥的MD5

81

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

83

- 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

80

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）

82

补充：网络层移动性管理相关技术

- 代理ARP技术
- 隧道技术

84

代理ARP技术

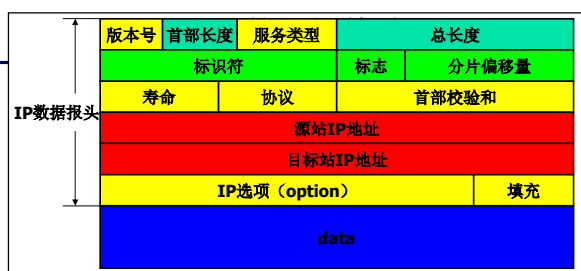
- 代理ARP(Proxy ARP): ARP协议的一个变种
- 功能: 通过使用一个主机(通常为路由器), 来作为指定的设备对另一个设备的ARP请求进行应答。
- 优点: 子网的变化对主机是透明的
- 缺点
 - 增加了ARP流量
 - 安全问题: ARP欺骗

85

IP in IP

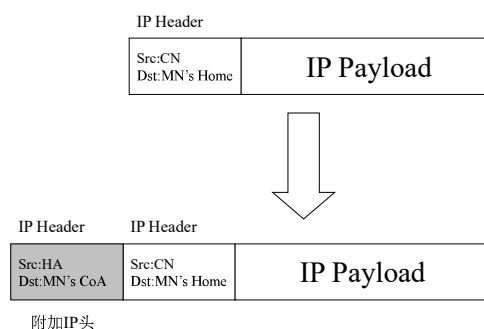
- 是支持Mobile IP的移动节点必须支持的IP协议隧道封装技术
- IETF的RFC2003定义
- 内容
 - 将一个IP数据包做为另一个IP数据包的净荷, 形成具有两个IP报头的新的数据包, 作为净荷的原始IP包不做任何改动

86



87

MIP中的隧道技术



88

谢谢!

89