# Topics in Wireless and Mobile Networking

David A. Maltz

*Carnegie Mellon University*

*dmaltz@cs.cmu.edu*

15-441 11/3/04

# Why Wireless is Different

Wireless and mobile networks break many assumptions

Media access control is a solved problem

- Distributed coordination is hard ***(802.11 MAC)***

Wired links have low ***bit error rate (BER)*** ($10^{-9}$ or less)

- Wireless links range from $10^{-4}$ to $10^{-7}$ ***(802.11 MAC)***

IP subnets have well defined borders

- Radio cells overlap ***(802.11 MAC, Mobile IP)***

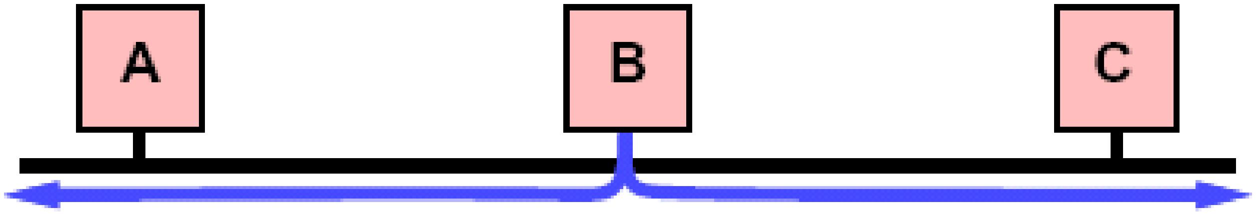
All machines on a subnet have a common prefix

- What about mobile machines visiting the subnet? ***(Mobile IP)***

# Wired Carrier Sense Multiple Access (CSMA)

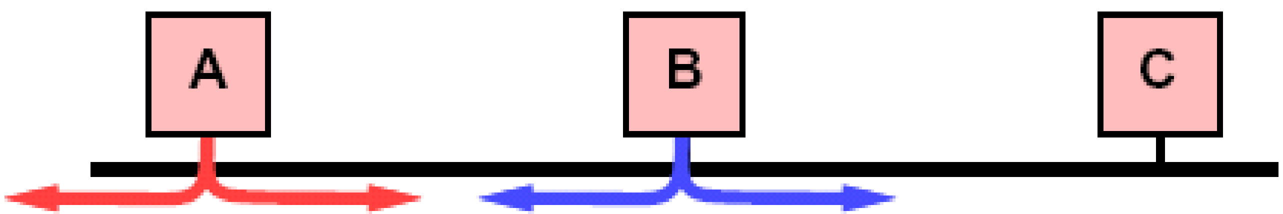
How to share a common channel?

- Listen for ***carrier*** before transmitting
- Carrier is just energy from another transmission
- While you hear carrier, wait before transmitting



# Wired Collision Detect (CD)

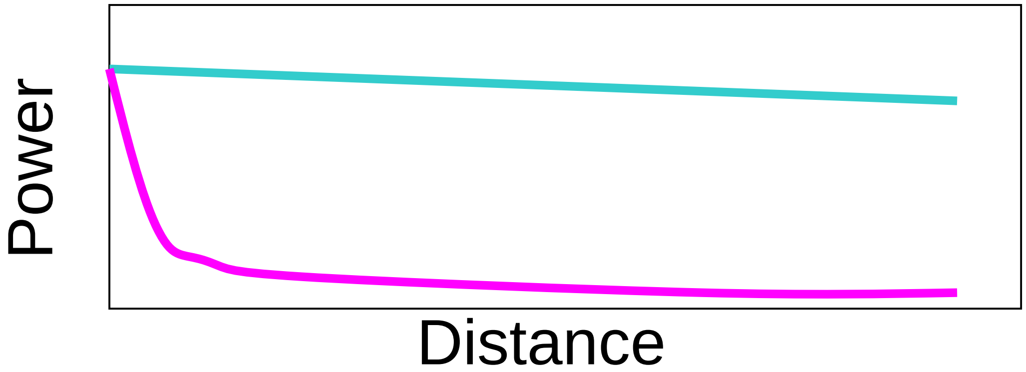
- Listen while transmitting
- If what you hear isn't what you're sending, then ***collision***:
  - Abort transmission of current packet
  - Try again after a random delay
  - Each collision for same packet doubles average delay



# Wireless CSMA

CSMA can be used in wireless, but has problems

- ***wired*** network: signal strength at sender and receiver are essentially the same
- ***wireless*** network: ***inverse square law*** (or worse) applies ($P_{recv} = P_{xmit}/D^k$, $k > 2$)




CSMA does not give the right information in wireless:

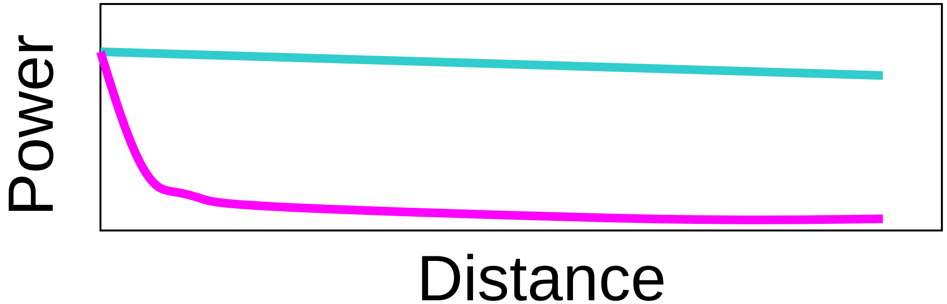
- Carrier sense detects signals at the ***transmitter***
- But collisions occur ***at the receiver***

# Issue 1: Wireless Collision Detect

Wireless can’t do collision detect like Ethernet

Can’t effectively listen while you send:

- In some systems, the hardware isn’t flexible enough:
  - Transmit and receive are on different frequencies
  - Transceiver might be half-duplex

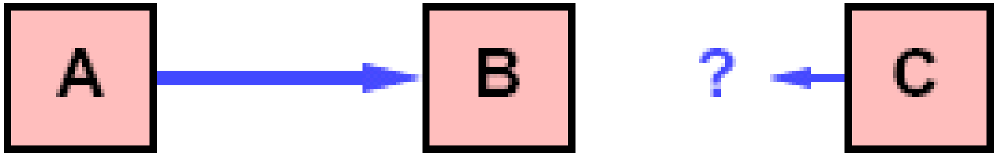



- In any case, all you could hear is yourself any way:
  - The inverse square law
  - Your own signal strength at your own antenna is ***much*** stronger than anybody else’s signal

# Issue 2: The Hidden Terminal Problem

Consider the following situation:

- A is sending to B
- C is ***out of range*** of A's transmissions to B
- C wants to send (to anybody)



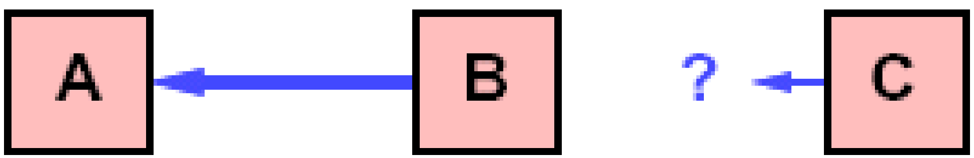

CSMA doesn't work well for wireless here:

- C can't know to wait since it can't hear carrier from A
- B can hear both A and C, thus collision at B
- A is "hidden" to C

# Issue 3: The Exposed Terminal Problem

Consider the following situation:

- B is sending to A
- C is ***in range*** of B's transmissions to A
- C wants to send to anybody but B




CSMA doesn't work well for wireless here either:

- C thinks it should wait since it can hear carrier from B
- If A is out of range of C, then C waits needlessly
- C is "exposed" to B

# Partial Solution: Virtual Carrier Sense

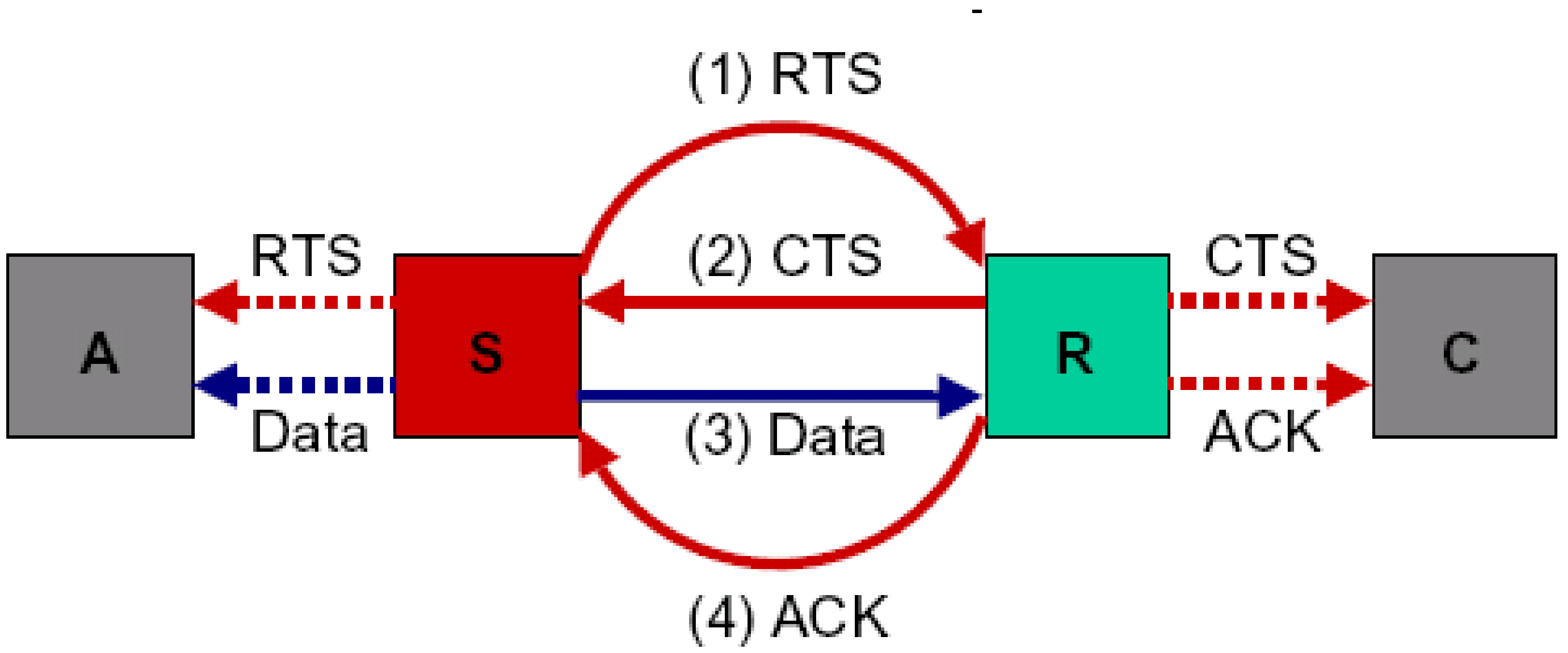
Packet types:

- ***Request-to-Send*** (RTS): Sender sends to receiver before sending a data packet
- ***Clear-to-Send*** (CTS): Receiver replies if ready for data packet to be sent
- ***Acknowledgment*** (ACK): receiver sends if data is received successfully

All packets contain:

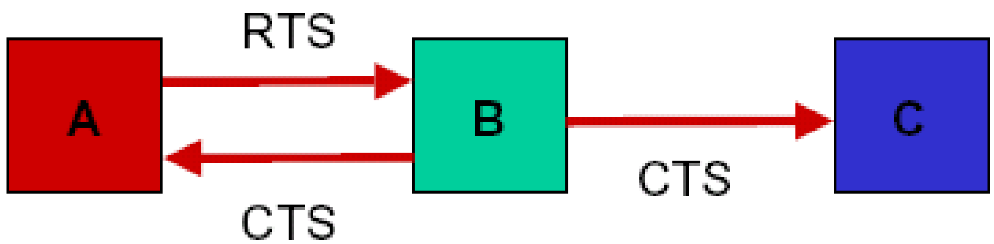
- Address of the ***sender*** of the intended data packet
- Address of the ***receiver*** of the intended data packet
- ***Duration*** of the remainder of the transmission

# Virtual Carrier Sense – 2



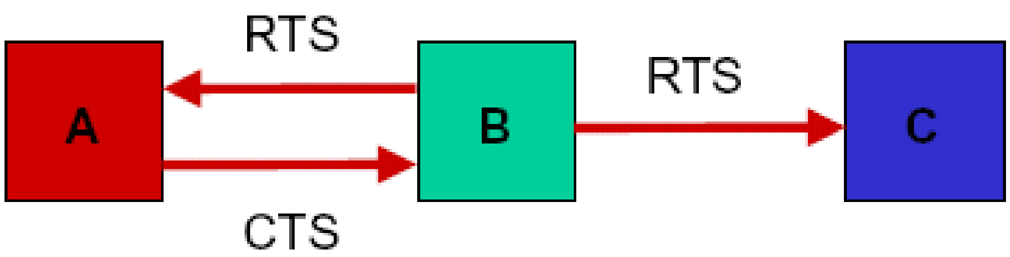
# Virtual Carrier Sense - 3

- Hidden terminal problem is avoided:




C waits to send since it hears B's CTS

- Exposed terminal problem is avoided:




C does not wait to send since it does not hear A's CTS

Does (and cannot) ***not*** prevent all collisions!

# IEEE 802.11 Usage Model

Host computer sees an "ethernet interface"

- Just like a wired LAN
- Uses 48-bit 802.3 MAC addresses
- All hosts "in range" of each other see common shared channel
- Supports ARP, broadcast, LAN multicast
- Can directly communicate with neighbors

# 802.11 Carrier Sensing

802.11 uses both ***physical*** and ***virtual*** carrier sensing:

- Physical carrier sense provided by PHY
- Virtual carrier sense provided by MAC

Virtual carrier sensing:

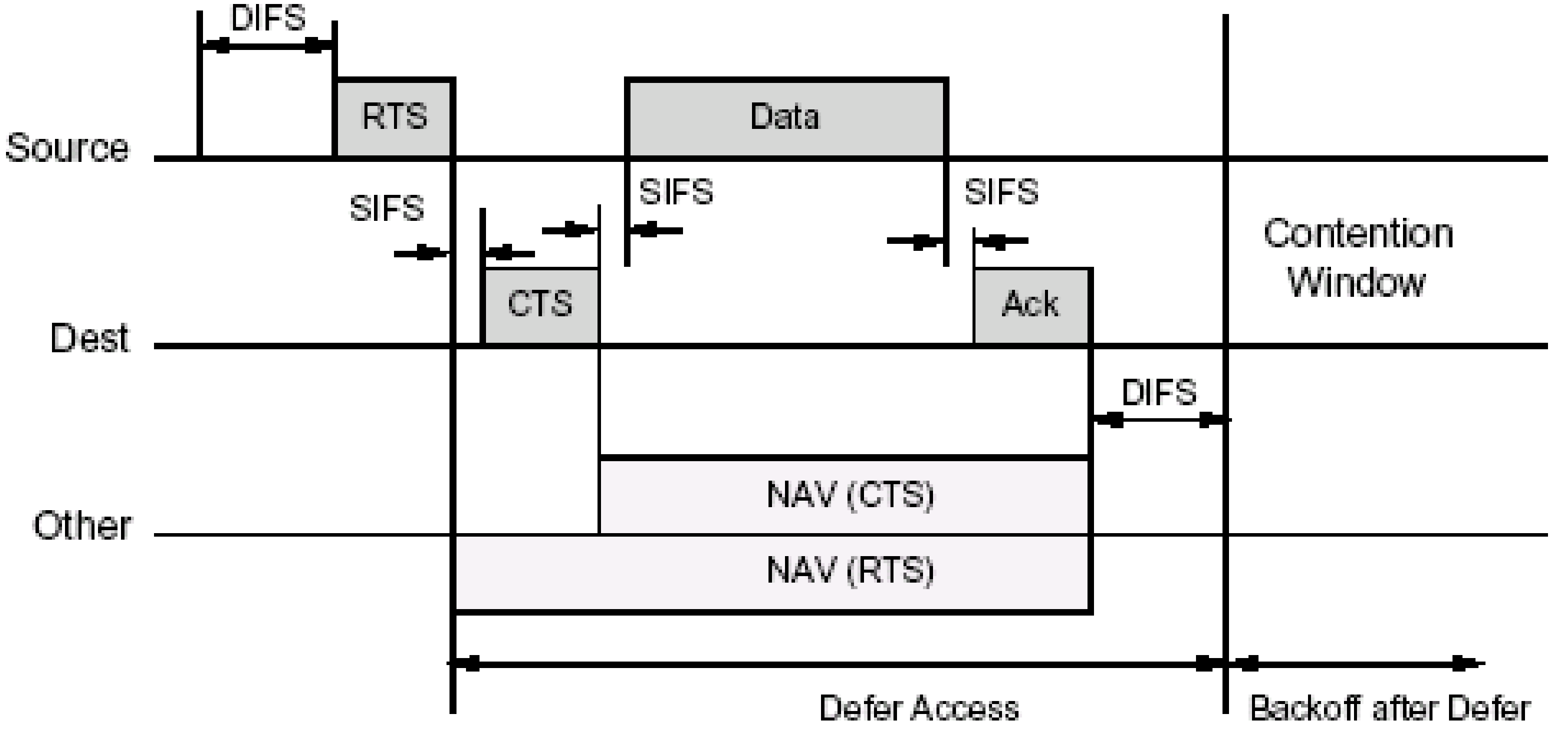
- Maintained by station through ***Network Allocation Vector (NAV)***
- NAV records prediction of future traffic on medium
- Counter that counts down busy time at uniform rate
- Set based on Duration field in received packets (e.g., RTS, CTS)
- When nonzero, virtual carrier sense thinks medium is busy

Carrier sense mechanism combines both mechanisms:

- Medium considered busy whenever either indicates carrier
- Medium also considered busy whenever our own transmitter is on

# Use of RTS and CTS

Other data senders must wait until entire RTS/CTS/Data/ACK finished




RTS/CTS only used for data packets larger than some threshold --- You can tune this!

# Multirate Support in 802.11

| 144 bits | 48 bits | | |
|---|---|---|---|
| PLCP preamble | PLCP hdr | MAC PDU | Data |

To enable sharing the media among many nodes:

- All control information must be transmitted at rate understood by all stations
- After control information, transceivers change to rate agreed on by sender and receiver
- Preamble and header sent at lowest coding rate
  - 1 Mbps in .11b/g
  - 6 Mbps in .11a

# 802.11 “Standards”

802.11b

- In theory: 1,2,5.5,11 Mbps
- Reality: 5-6 Mbps

802.11a

- In theory: 54 Mbps
- Reality: 20-24 Mbps

802.11g

- Specification: 54Mbps, Claims: 108 Mbps
- Reality: 20-70Mbps

1 in 4 new devices fails compliance testing – they’re probably marketed anyway

http://news.com.com/2100-7351-5139499.html

# Check Your Understanding

A B C D

You are node B running the 802.11 MAC protocol

You received RTS from node A indicating a 1KB pkt waiting for you

What do you do now?

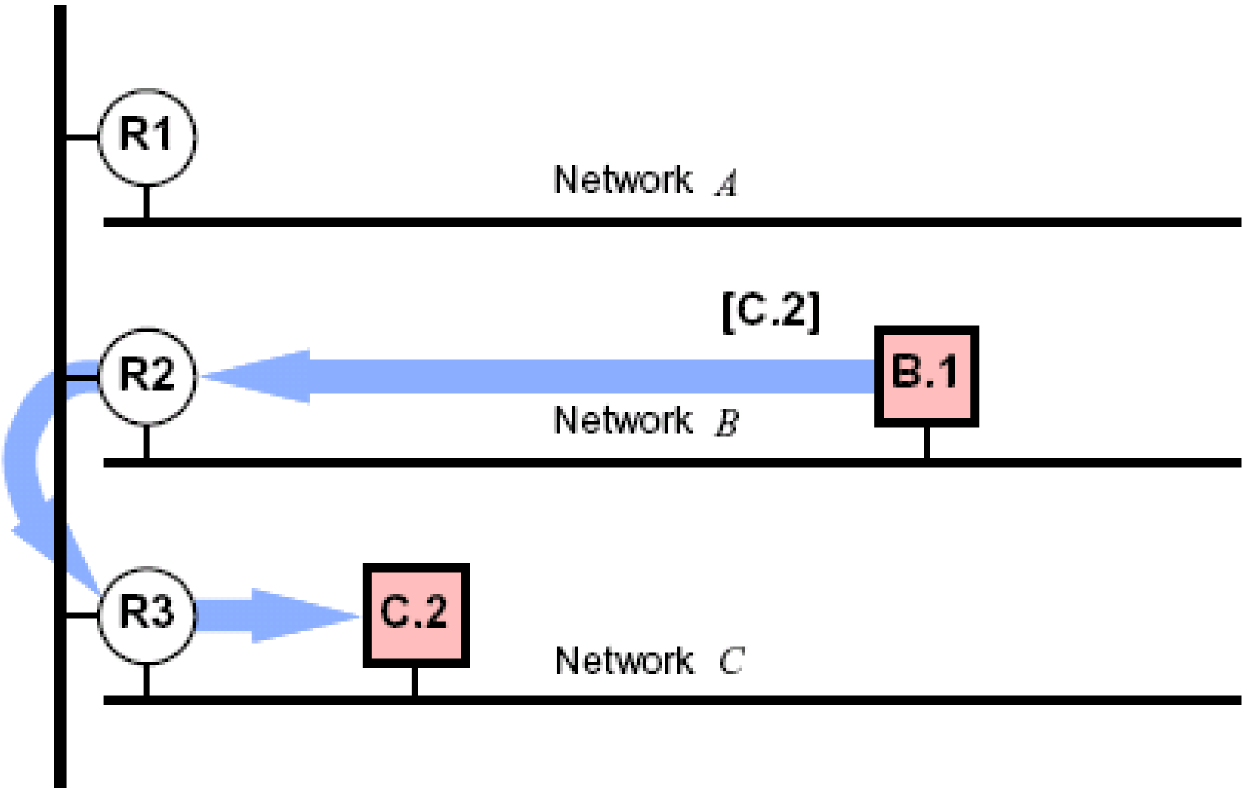
1. Immediately transmit CTS, so exchange completes before neighbor's timers run out
2. Virtually sense carrier, transmit CTS if clear
3. Physically sense carrier, transmit CTS if clear
4. Physically and virtually sense carrier, transmit CTS if clear
5. Sense for collision, retransmit if needed

802.11 solves the hidden terminal problem, even if D has a more powerful transmitter than B? (True or False? Explanation?)

# Mobility Support in the Network Layer

Routers only know the way to each network

If a host moves, its packets will still go to its home!



# Why Not Change Addresses?

- Must notify all hosts with open connections
  - Used to identify endpoints of connections
  - Used within some transport protocols
- Must also notify all ***hosts*** using connectionless protocols
- Cannot change hosts with “well known” addresses
- Name server must be updated:
  - Caching of addresses used for scalabilty
  - Too expensive to update quickly

# Location Registry

Mobile nodes away from home must record their current location ***somewhere***

- A database that is explicitly queried:
  - Can be stored anywhere, use special lookup protocol
  - Problem: non-mobile-aware nodes cannot use it?
  - Problem: must look up all addresses, whether or not destination is away from home?
- Send packet normally to the home network:
  - Internetwork routing already knows how to get there
  - Intercept packet there and tunnel to mobile node
  - Problem: Long trip to home for every packet?
  - Problem: Location is unavailable if home is down?

# IETF Mobile IP Requirements

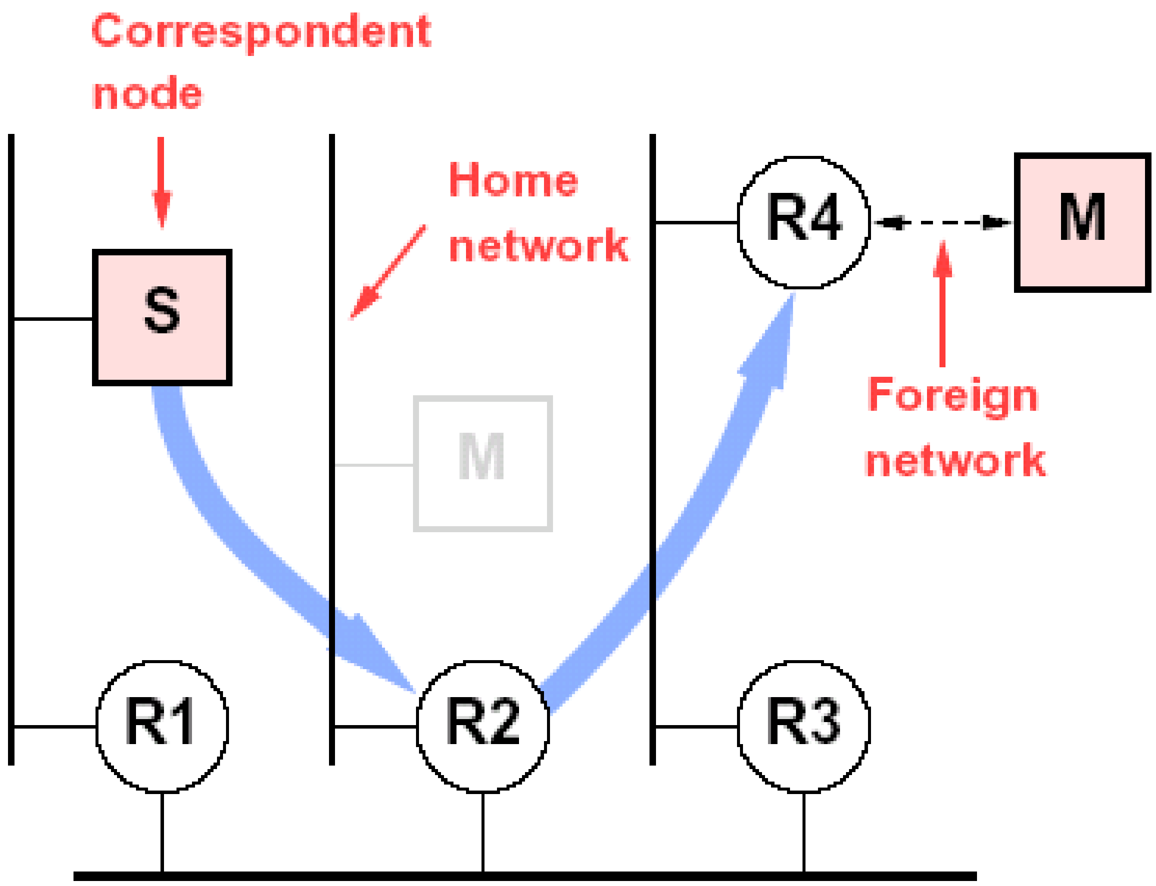
RFC 3344

- *Transparency*:
  - A mobile node continues to use its home address
  - Can still communicate after disconnect and reconnect
  - Can change its point of attachment
- *Compatibility*:
  - Supports any lower layer that IP runs on
  - No changes required to ordinary hosts and routers
  - Mobile node can communicate with unaware nodes
- *Security*:
  - All registration messages must be authenticated

# The Mobile Node

Each mobile node has a ***home network***

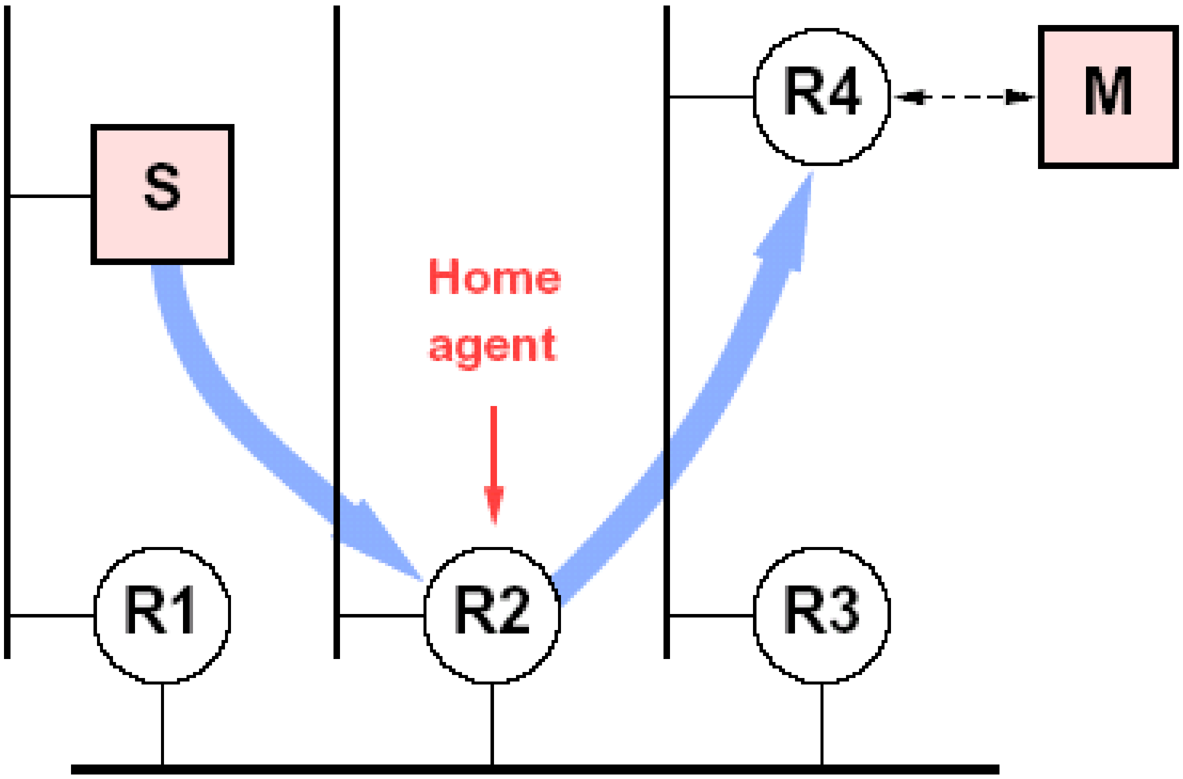
May move and connect to a ***foreign network***



# The Home Agent

Home agent keeps track of mobile node's care-of address

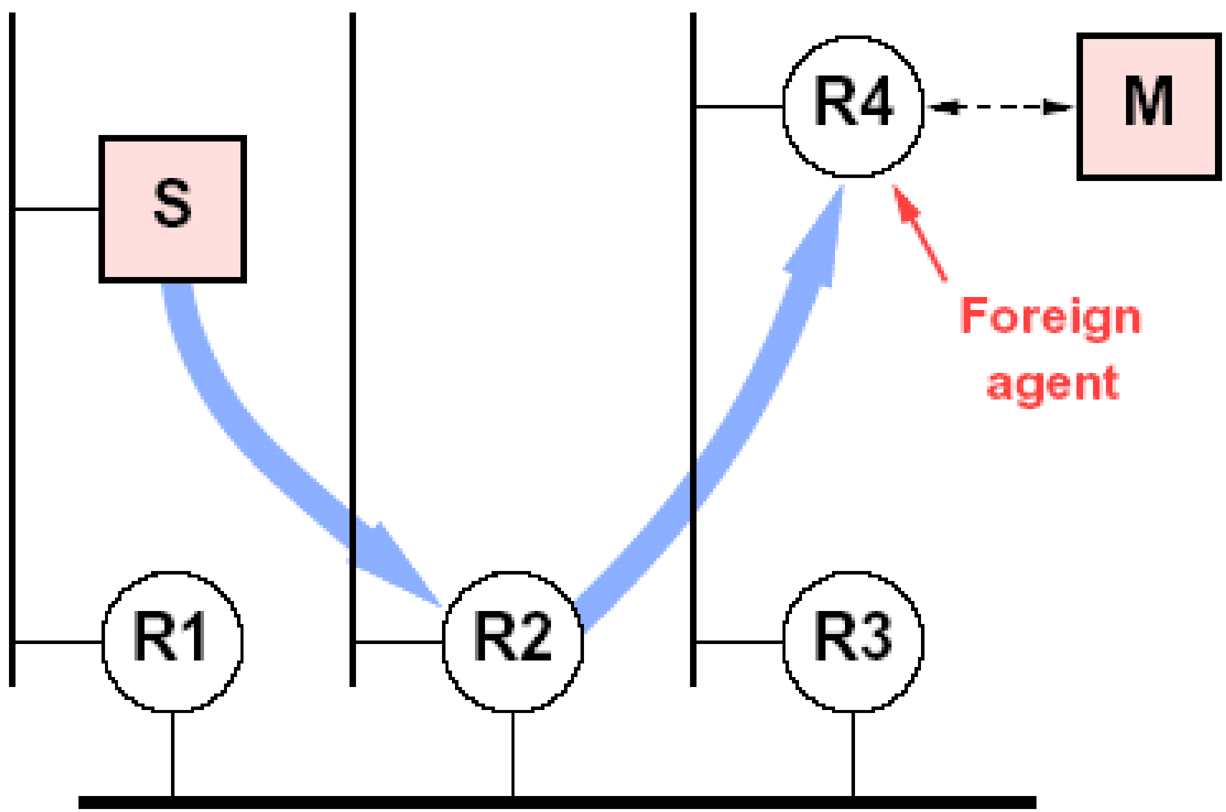
Intercepts and forwards packets to that address



# The Foreign Agent

Foreign agent assists with mobile node's registration

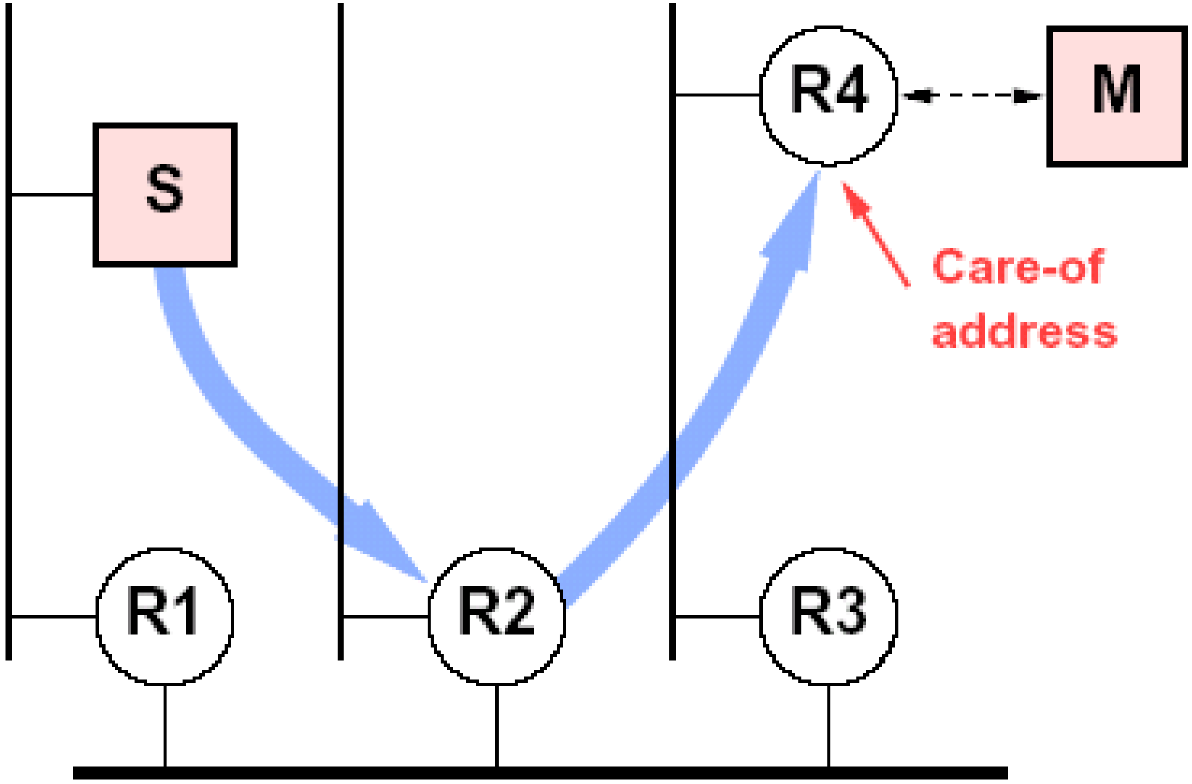
Delivers forwarded packets locally to the mobile node



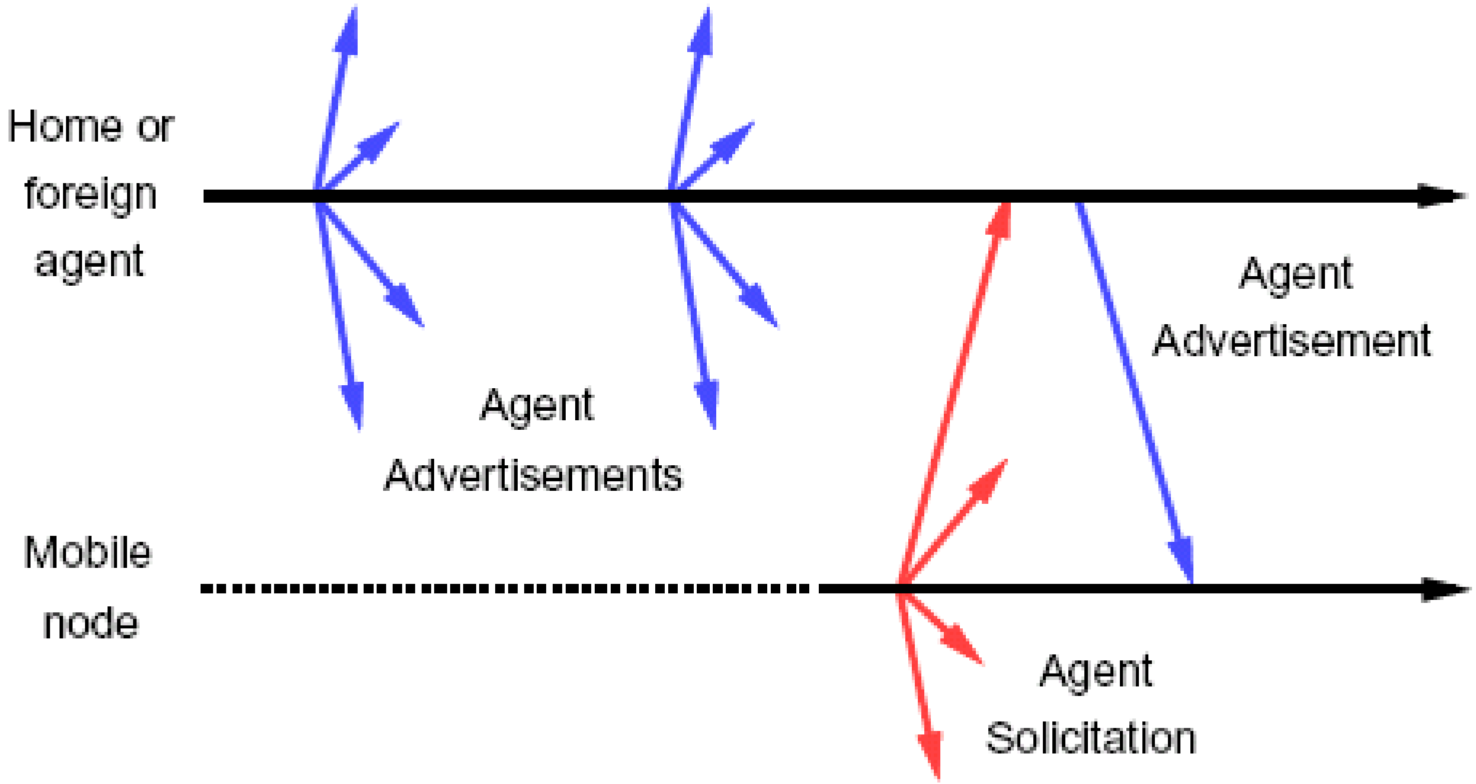
# The Care-of Address

May be foreign agent's own IP address

May be local address for mobile node (e.g., through DHCP)



# Agent Discovery Protocol




A mobile node recognizes that it has returned home when it discovers its own home agent

# Registration

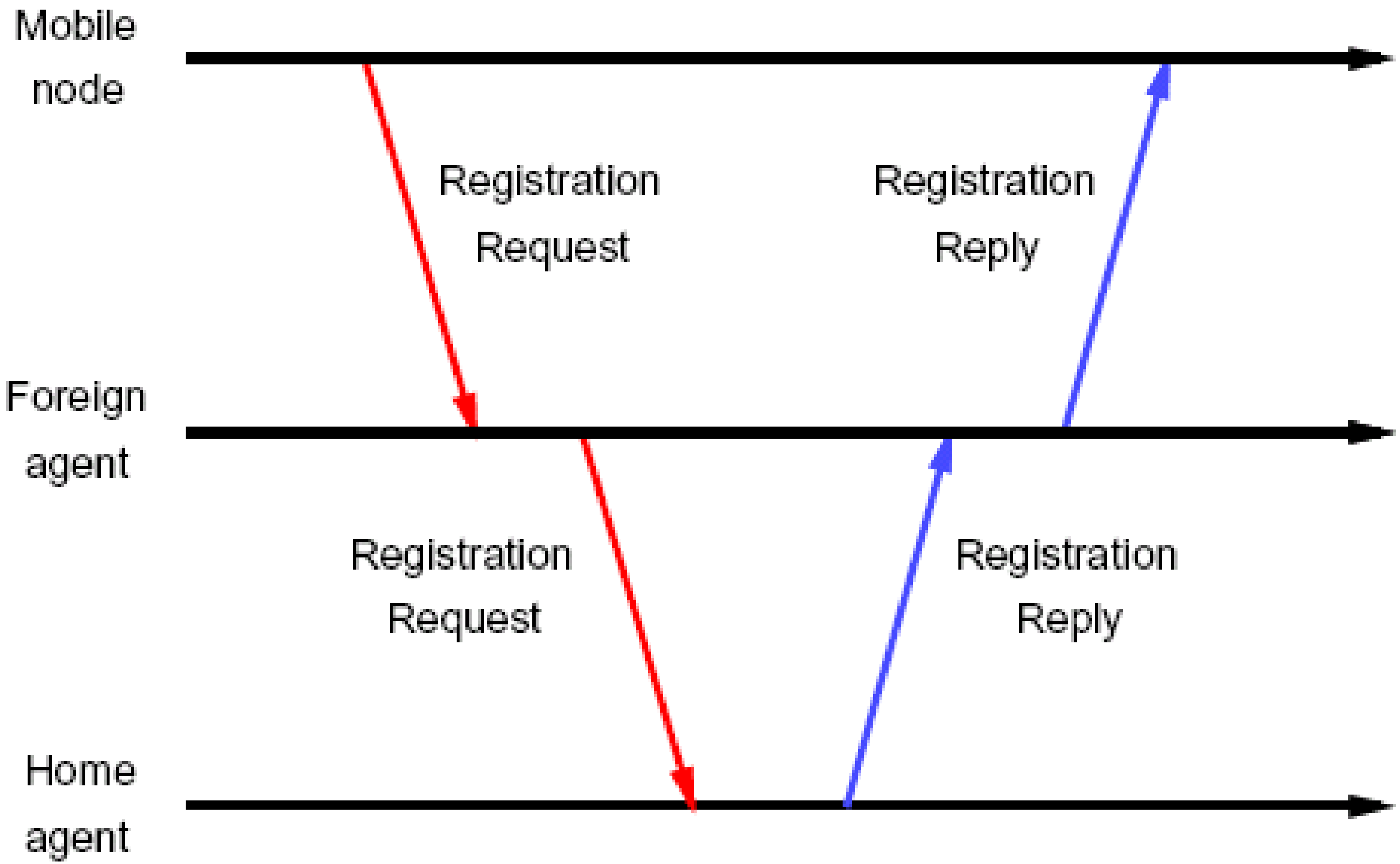
## Registration is used:

- To inform home agent of mobile node's care-of address, and
- To inform foreign agent that the mobile node is visiting

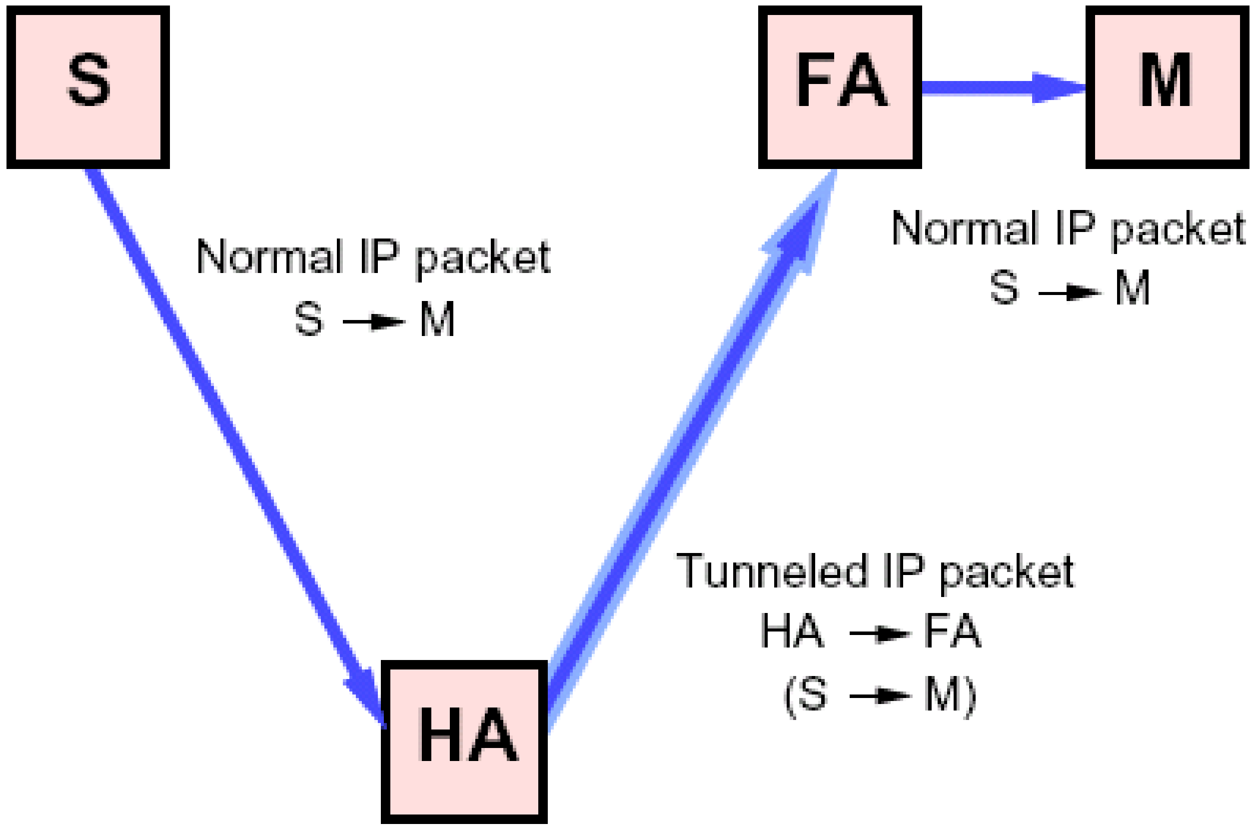
## Registration establishes a ***mobility binding***:

- Mobile node's ***home address*** and current ***care-of address***
- Remaining ***lifetime*** of this registration:
  - Period after which registration expires and is deleted
  - Negotiated during registration
  - Mobile node should reregister before expiration

# Registration Through a Foreign Agent



# Tunneling




This use of encapsulation known as ***tunneling***

Path from encapsulator to decapsulator known as tunnel

Intermediate routers ***need not know*** about Mobile IP!

# The Need for Authenication

Must authenticate new location information for mobile node

Otherwise, ***anybody*** could reroute packets ***anywhere***:

- ***Passive eavesdropping***:
  - Update registry to route somebody's packets to yourself
  - Simply look at them before forwarding to real destination
- ***Altering messages***:
  - Same, but alter them before forwarding them on
- ***Denial of service***:
  - Reroute them to yourself, but don't forward them on
  - Or just reroute them to a bogus address

# Check Your Understanding

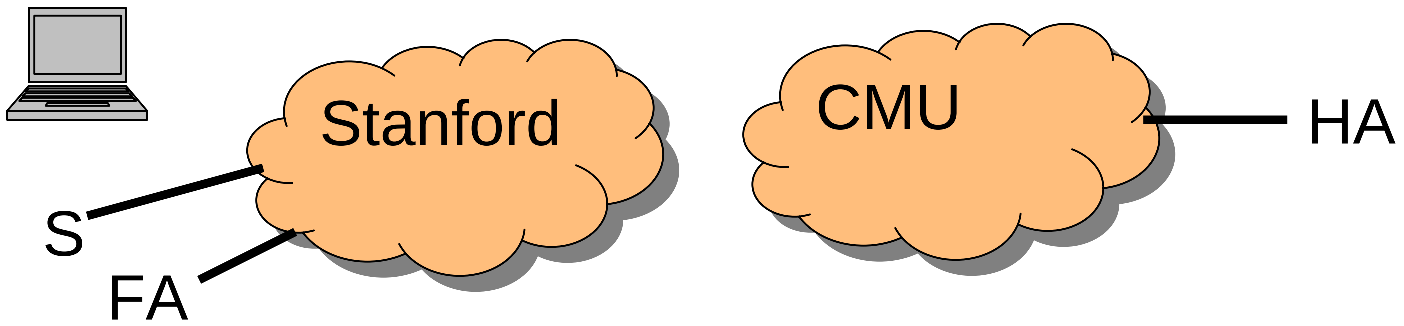
When a Mobile Node sends packets, what source IP address should it use? Why?

1. Its own home-address
2. Its care-of address

# Check Your Understanding

My laptop is a visiting mobile node (MN) at Stanford. A Stanford node (S) is communicating with my laptop. What path do the packets take?

1. S to laptop to S
2. S to CMU to CMU HA to Stanford FA to laptop to S
3. S to FA to laptop to S
4. S to CMU to CMU HA to Stanford FA to laptop to Stanford HA to Stanford FA to S



# Mobile IP and Cellular Telephony

The requirements for Mobile IP and mobile telephones are similar!

Can we sketch a protocol for cell phones using our Mobile IP knowledge?

| ***Mobile IP*** | ***Telephony*** | |
|---|---|---|
| Mobile Host | cell phone | |
| Internet | PSTN | public switched telephone net |
| Home Agent | MSC | mobile switching center |
| Foreign Agent | MSC | |
| HA binding table | HLR | home location registry |
| FA binding table | VLR | visitor location registry |
| care-of addr | TLDN | temp local directory number |

# IS-41 Protocol (GSM)