Mobile IP

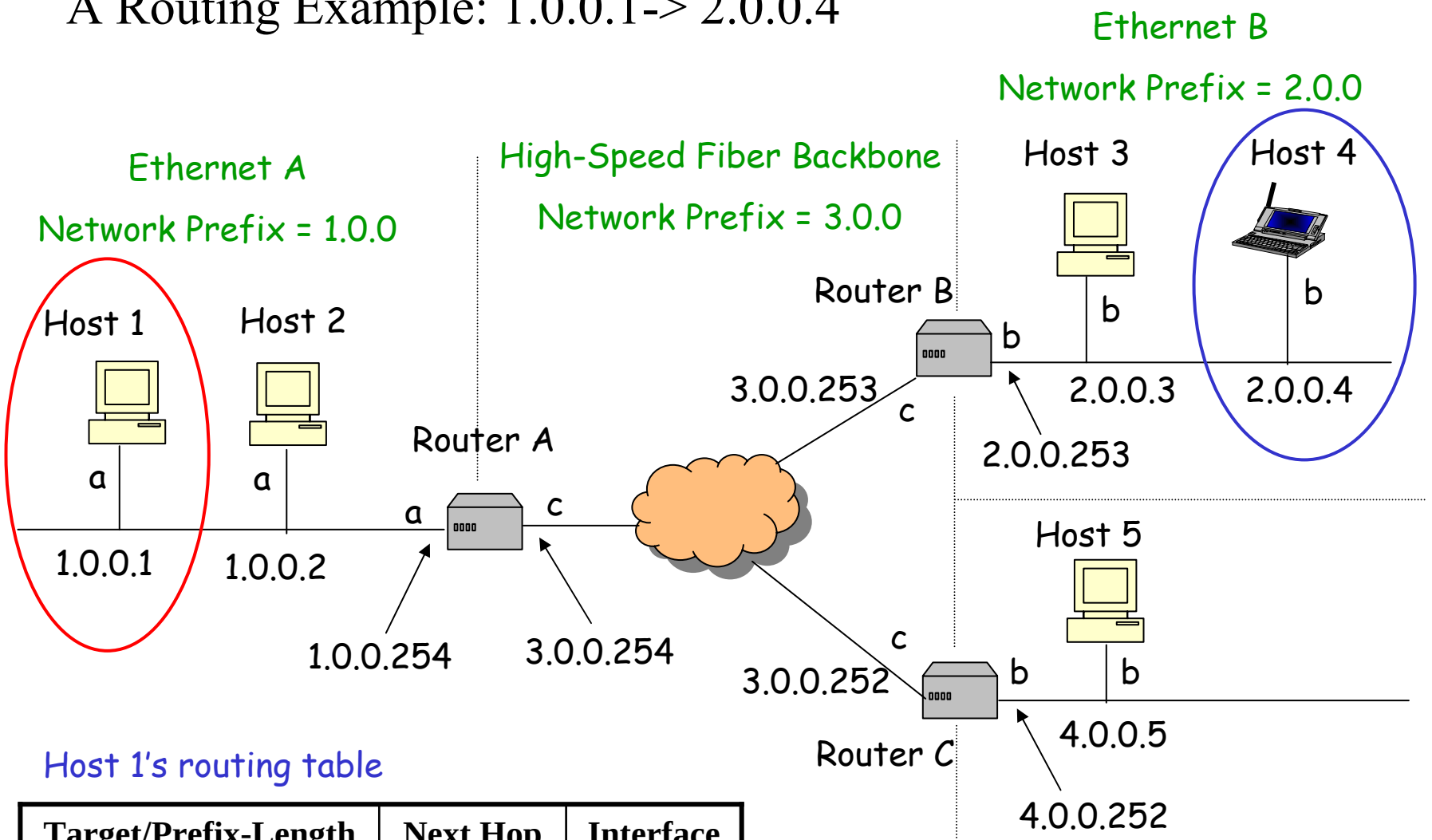
- Support for mobile hosts in the Internet
- Discussion based on IPv4
- Original work by John Ioannidis:

- Protocols for Mobile Internetworking, Ph.D. thesis, Columbia University, 1993
- First full implementation, Columbia University, 1991

- Many other implementations with slightly different approaches:

- Sony 1991
- IBM 1992
- Harvard 1994
- Linux Mobile IP 1996

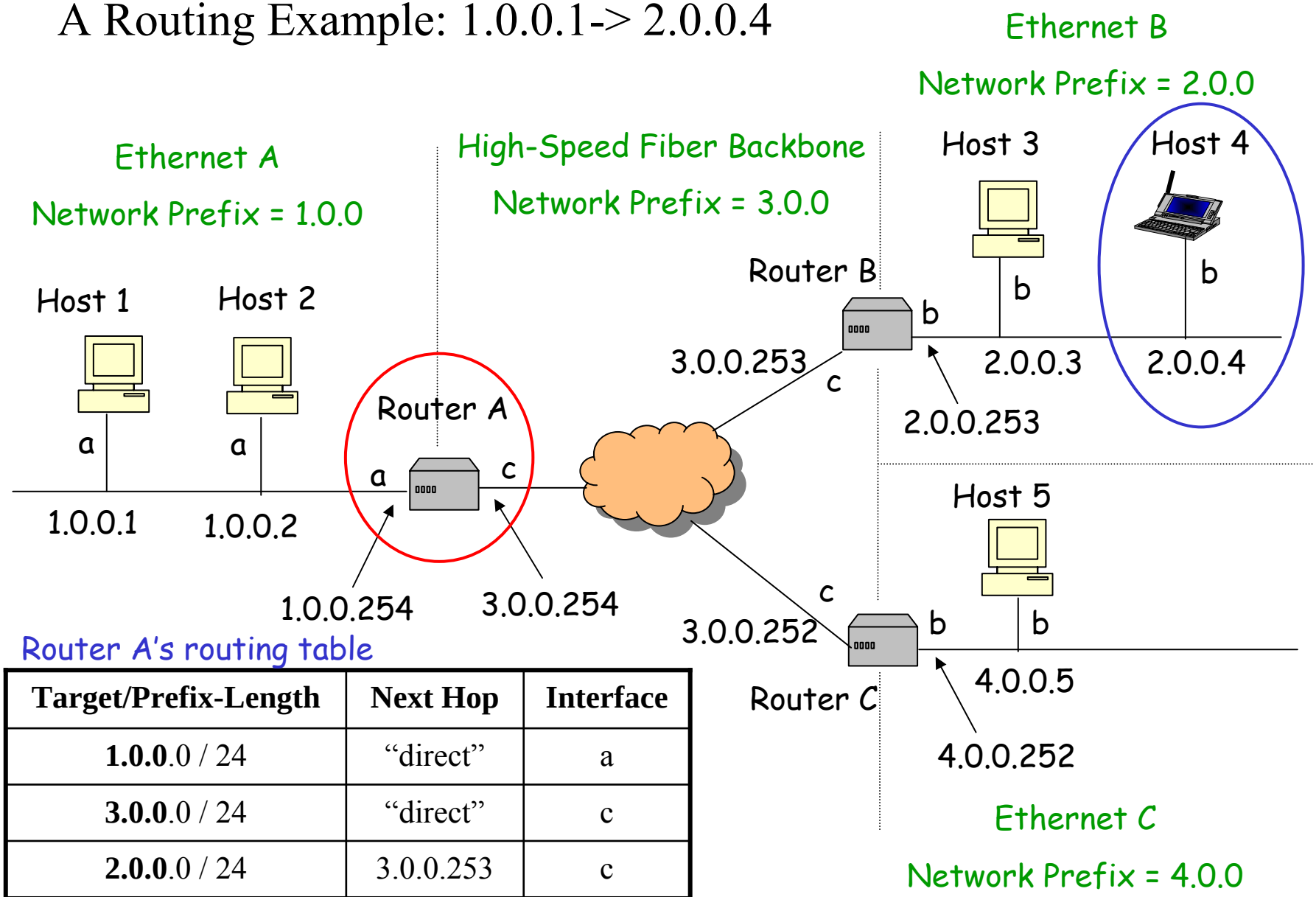
A Routing Example: 1.0.0.1-> 2.0.0.4



Host 1's routing table

Target/Prefix-Length	Next Hop	Interface
1.0.0.0 / 24	"direct"	a
0.0.0.0 / 0	1.0.0.254	a

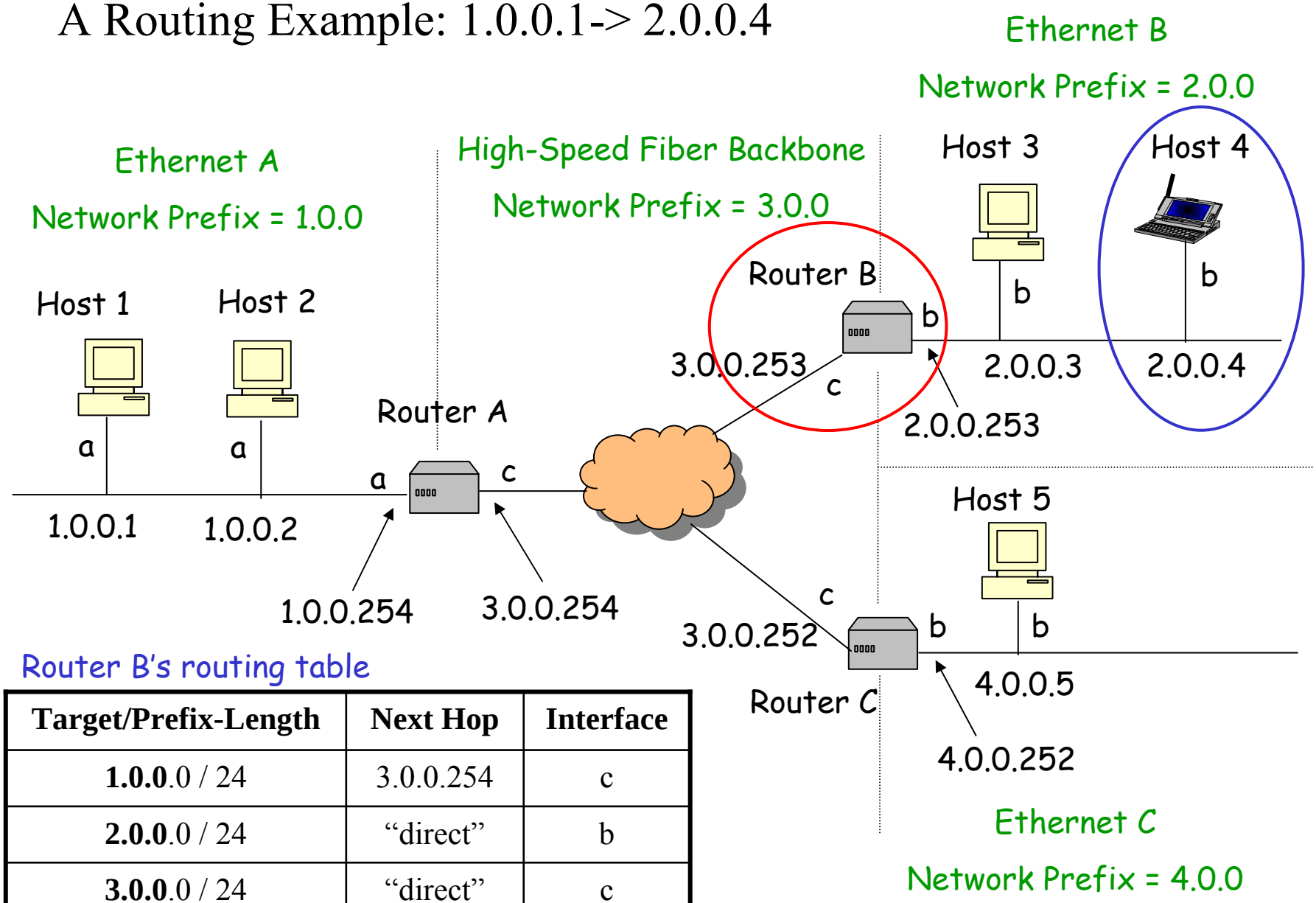
A Routing Example: 1.0.0.1-> 2.0.0.4



Router A's routing table

Target/Prefix-Length	Next Hop	Interface
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

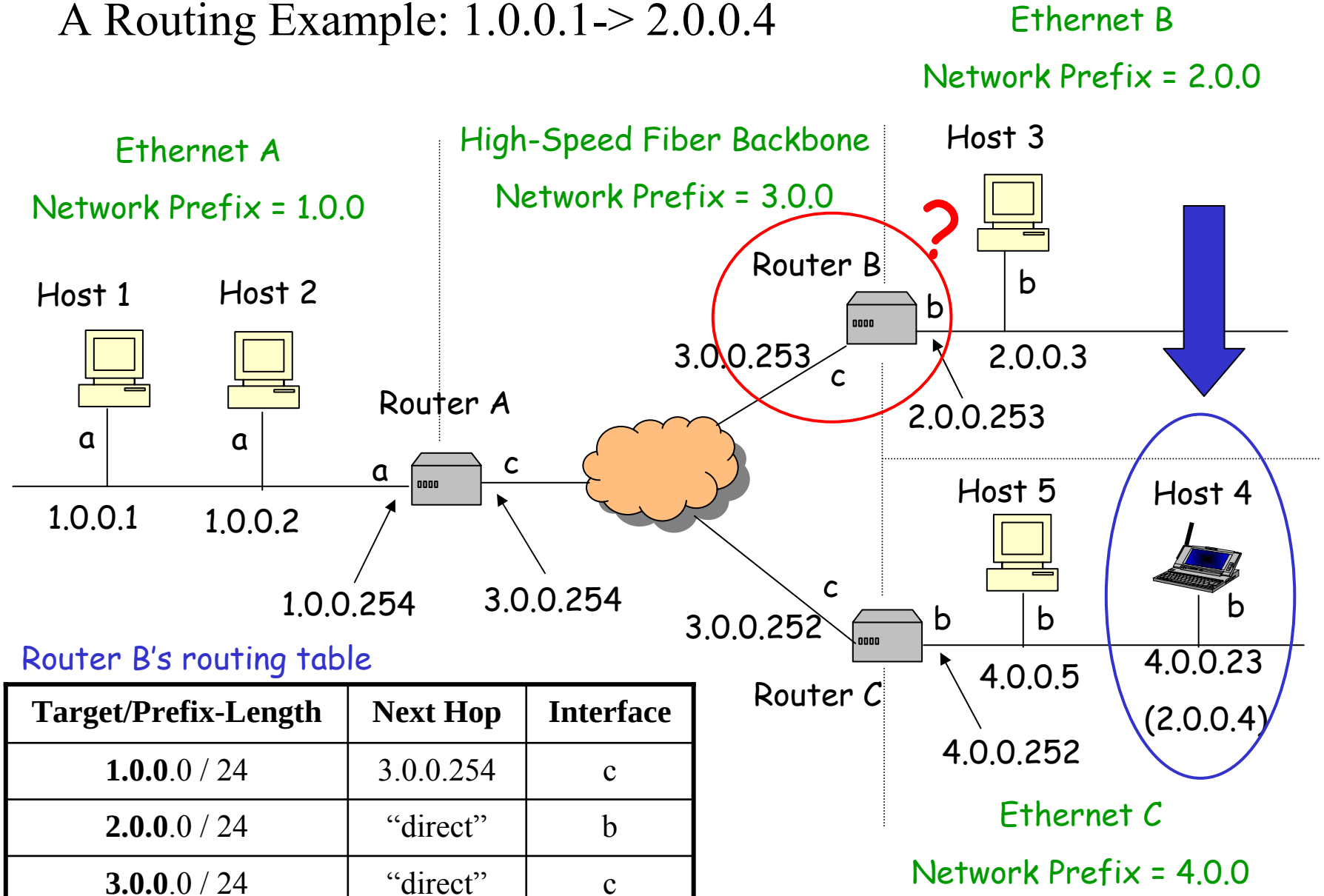
A Routing Example: 1.0.0.1-> 2.0.0.4



Router B's routing table

Target/Prefix-Length	Next Hop	Interface
1.0.0.0 / 24	3.0.0.254	c
2.0.0.0 / 24	"direct"	b
3.0.0.0 / 24	"direct"	c

A Routing Example: 1.0.0.1-> 2.0.0.4



Router B's routing table

Target/Prefix-Length	Next Hop	Interface
1.0.0.0 / 24	3.0.0.254	c
2.0.0.0 / 24	"direct"	b
3.0.0.0 / 24	"direct"	c

The Problem

- The packet cannot be delivered
  - Host 4 is no longer connected to Ethernet B
  - It has moved to Ethernet C
  - Keeps the same IP address (2.0.0.4), or
  - Is assigned (somehow) a new IP address (4.0.0.23)
- Router B will send:
  - An ICMP host unreachable message back to host 1
- Suggestions on how to solve this problem?

Solution 1: Host-specific Routes

- When host 4 keeps its old IP address (2.0.0.4)
- Enter host-specific routes into the routing tables of routers A, B and C:

Router A

Target/Prefix-Length	Next Hop	Interface
2.0.0.4 / 32	3.0.0.252	c

Router B

Target/Prefix-Length	Next Hop	Interface
2.0.0.4 / 32	3.0.0.252	c

Router C

Target/Prefix-Length	Next Hop	Interface
2.0.0.4 / 32	“direct”	b

Solution 2: Change IP Address

- Simply change the IP address of host 4, as it moves from Ethernet B to Ethernet C
  - New IP address: 4.0.0.23
  - Assignment via some automated way, DHCP
- Change the IP address of a host whenever it changes its point of attachment

Solution 3: Mobile IP

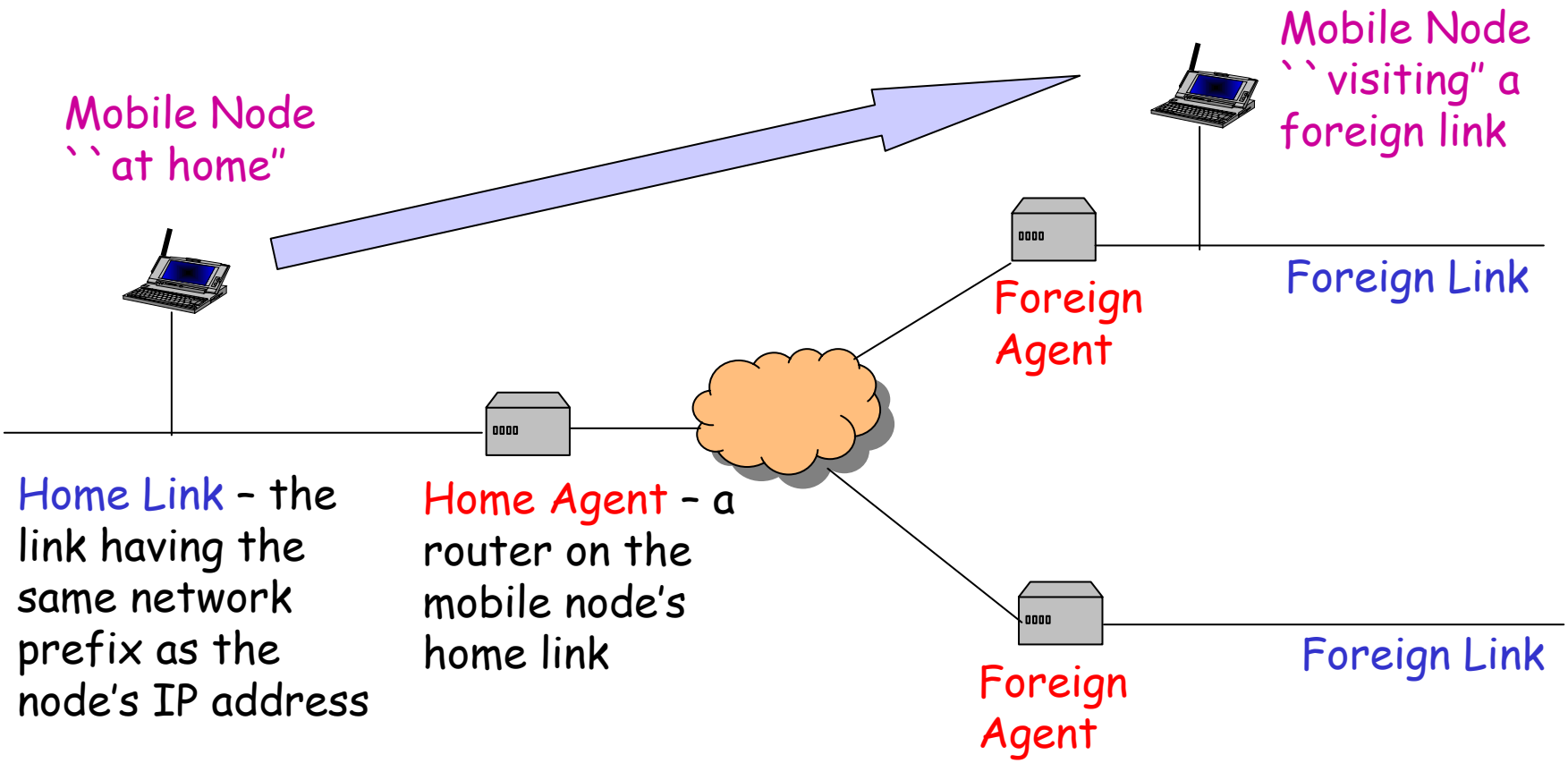
- A standard proposed to address the problem of mobile internetworking
- It allows a mobile node to use two IP addresses:

- A fixed IP address, called *home address*

- An IP address that changes at each new point of attachment, called *care-of address*

- Home address is a permanent IP address assigned by the node's home network
- Care-of address is a temporary address assigned by the foreign network (the network that the host visits)

Entities and Relationships



Home and Foreign Agent

- Home Agent:
  - A router on a mobile node's home network
  - Maintains current location information for the mobile node.
- Foreign Agent:
  - Serves as a default router for the registered mobile nodes

Care-of Address: Foreign Agent CoA

- Two different conceptual types:

- Foreign agent care-of address:

  * IP address of a foreign agent (FA) that has an interface on the foreign link

  * The FA may have more than one IP address; So, the network prefix need not be the same as the network prefix of the foreign link

  * The same FA CoA can be shared by many mobile nodes simultaneously

Care-of Address: Collocated CoA

- Collocated care-of address:
  * An IP address temporarily assigned to a mobile node
  * Can be used by only one mobile node at a time
  * The network prefix must be the same as the network prefix of the foreign link
  * It might be used by a mobile node in situations where no foreign agents are available

Mobile IP Operation

- Three main mechanisms:
  - Agent discovery
  - Registration
  - Routing

Mechanism 1: Agent Discovery

- Home Agents and Foreign Agents periodically broadcasts *Agent Advertisements*

  - E.g. once every few seconds

  - If the mobile node does not want to wait for the periodic advertisement, it can broadcast *Agent Solicitations* that will be answered by any foreign agent that receives it

- Mobile nodes determine whether they have moved from one link to another

Movement Detection

- *Agent Advertisement* has a *Lifetime* field
  - Specifies how soon a mobile node should expect to hear another advertisement from that same agent
- If the mobile node fails to hear an advertisement from that agent within the specified *Lifetime*, then it assumes that it has moved to a different link
- Also movement detection based on network prefixes

Care-of Address

- A mobile node connected to a foreign link acquires a foreign agent care-of address from the *Agent Advertisements*
  - If multiple care-of addresses are listed, any one of them can be used
- If a foreign agent is unavailable, the mobile node can obtain a collocated care-of address by DHCP
- Or a previously assigned collocated care-of address may be used

Agent Discovery Security

- No authentication is required by the Mobile IP specification
  - MAY be authenticated using IPsec mechanisms
- We can have malicious mobile nodes or malicious foreign agents
- You can come up with your own ways of exploiting this

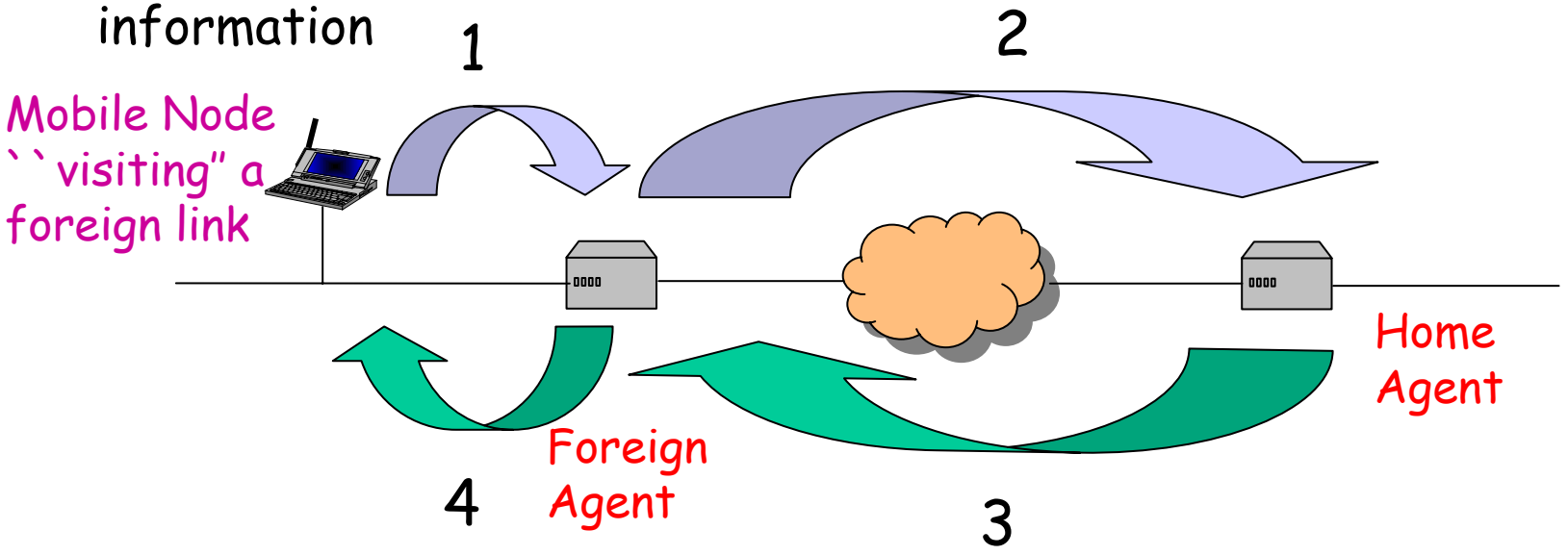
Mechanism 2: Registration

- Registration is the process by which a mobile node:

- Requests routing services from a foreign agent
- Informs its home agent of its current care-of address, which creates a *triple binding*:
  * Home address | Care-of address | Lifetime
- Renews a registration which is due to expire, *binding update*
- Multiple triple bindings may be kept for the same MN (*almost* seamless handoff)
- Deregisters when it returns to its home link

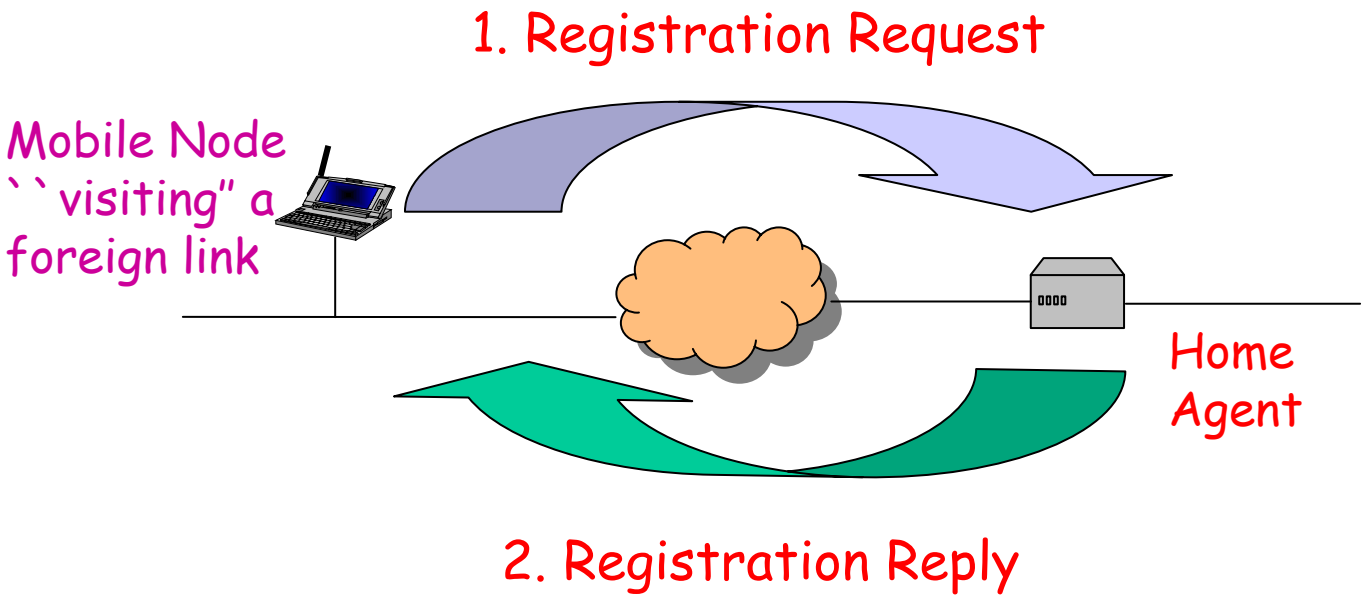
Registering Foreign Agent Care-of Address

• The mobile node, with the assistance of a foreign agent, sends a *Registration Request* with the care-of address information

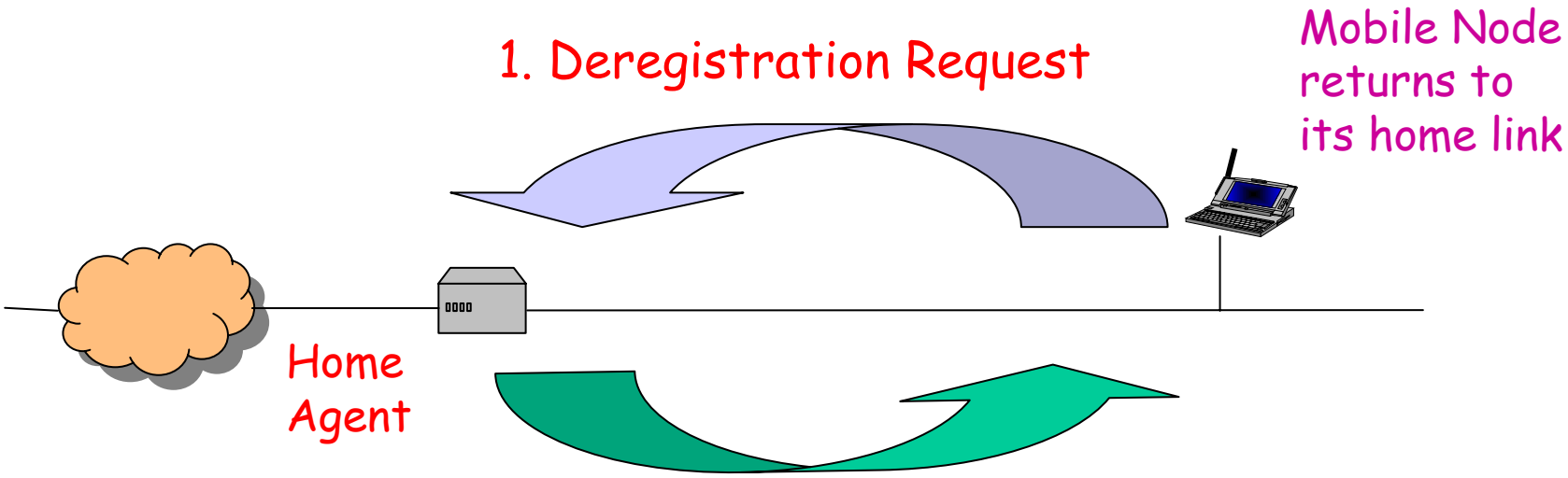


• When the home agent receives this request, it adds the necessary information to its routing table, and sends a *Registration Reply* back to the mobile node

Registering Collocated Care-of Address



Deregistration



Authentication

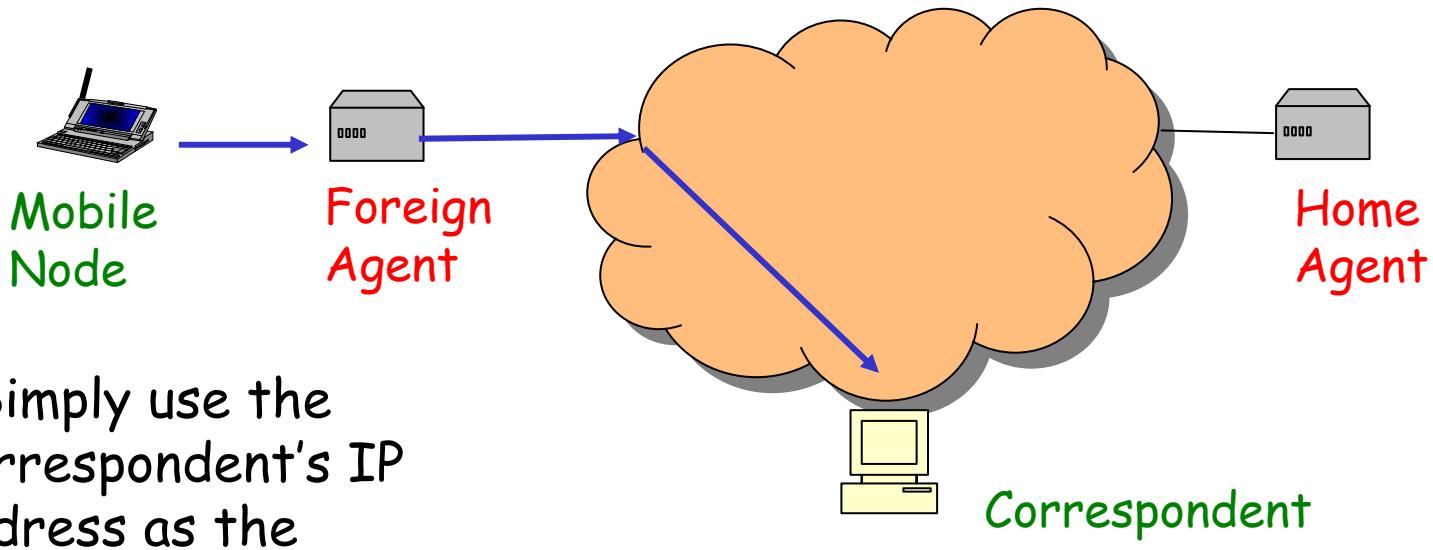
- The home agent must be certain that registration was originated by the mobile node and not by some other malicious node.
- Registration of the care-of address requires authentication

- The mobile node needs to prove its identity to its home agent
- It is done by making use of a secret key known only to the mobile node and its home agent
- Secret key is not sent as part of the communication
- Mobile IP standard requires keyed MD5

Mechanism 3: Routing

- Divided into different scenarios:
  - Mobile node→Correspondent node
  - Correspondent node→Mobile node
    * With a foreign agent
    * Without a foreign agent

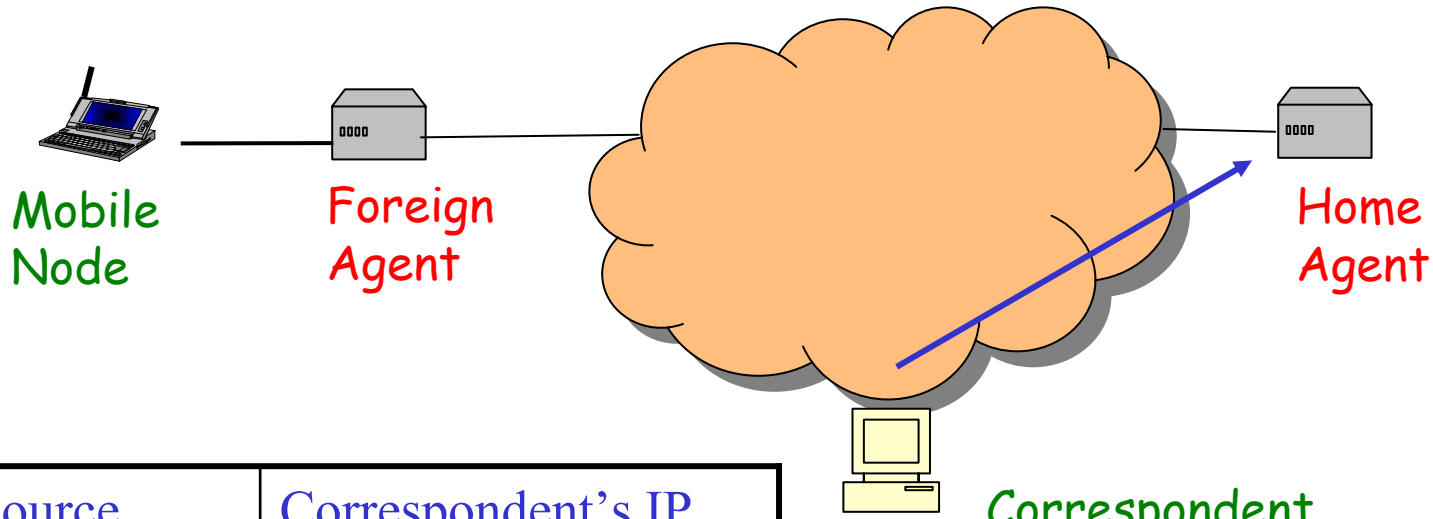
Mobile Node—Correspondent Node



- Simply use the Correspondent's IP address as the destination address

- How about the source address? Original IP address? Care-of Address?

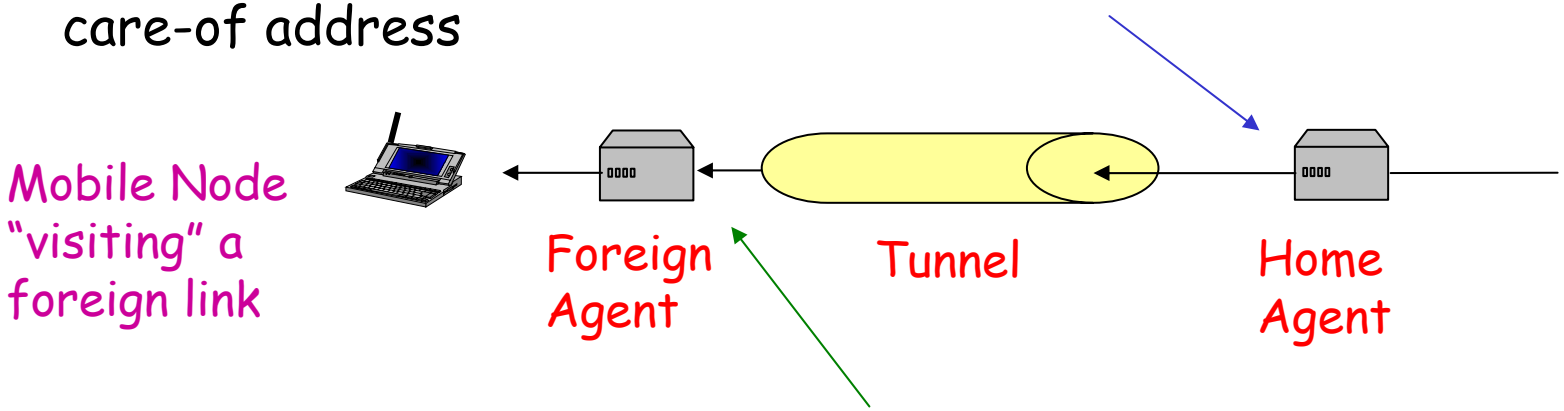
Correspondent Node→Mobile Node



Source address	Correspondent's IP address
Destination address	Mobile's IP address

Encapsulation is the Key

- The Home Agent intercepts packets destined to the mobile node's home address and tunnels them to the mobile node's care-of address



- The Foreign Agent removes original packet from the tunnel and delivers the original packet to the mobile node over the foreign link

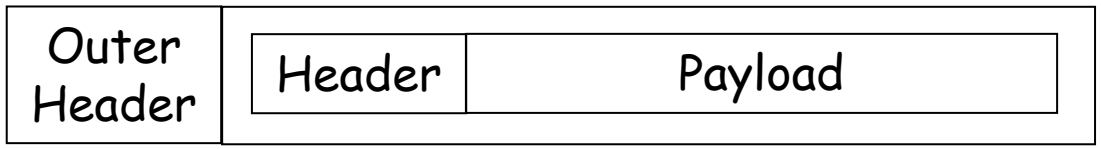
IP in IP Encapsulation

IPsrc: Original sender
IPdes: Destination's home address

Original IP packet

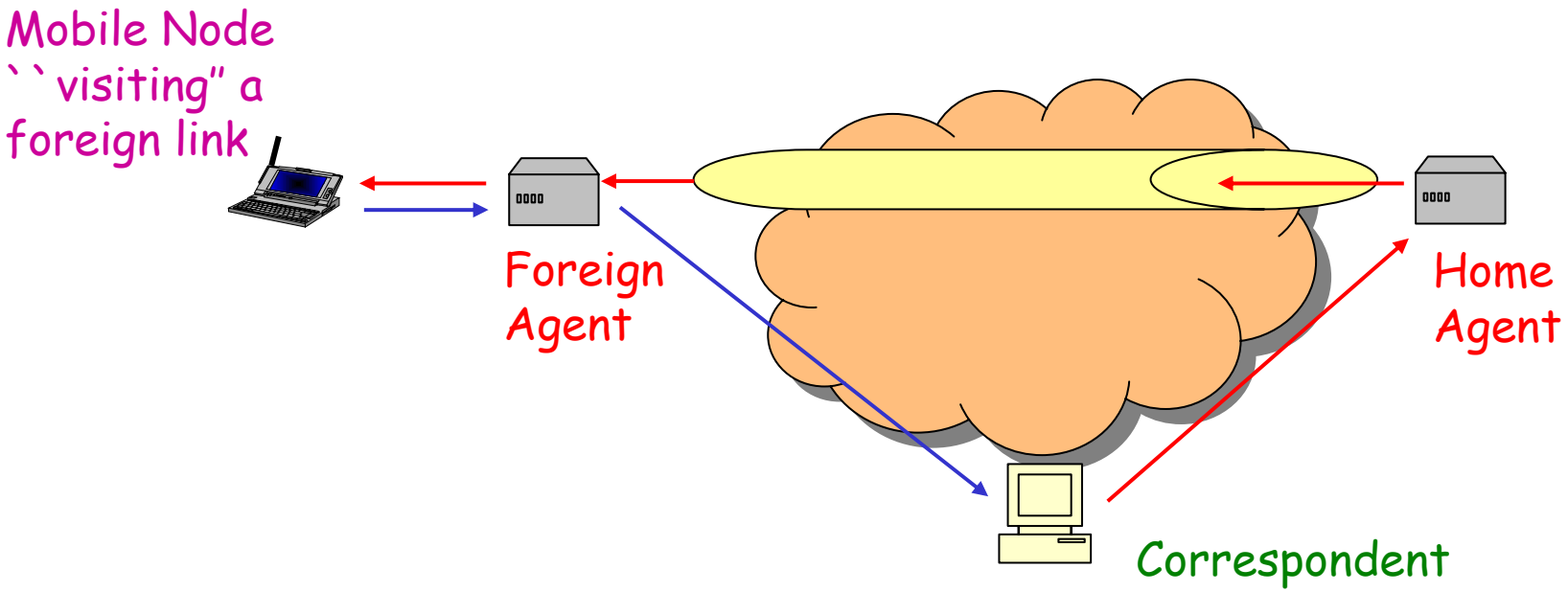
• The home agent inserts a new IP header, or tunnel header, in front of the IP header of any datagram addressed to the mobile node's home address

IPsrc: Home Agent
IPdes: Mobile node's Care-of Address



Encapsulated IP packet

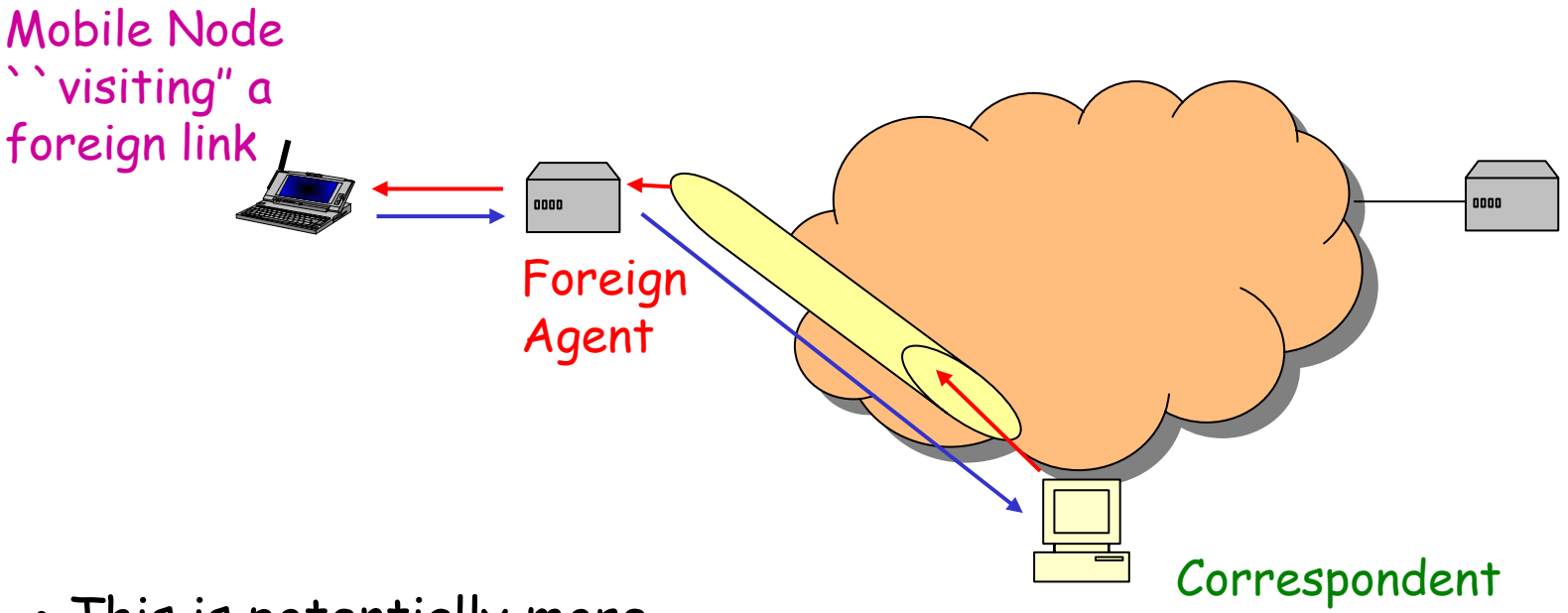
Triangle Routing (1/2)



Triangle Routing (2/2)

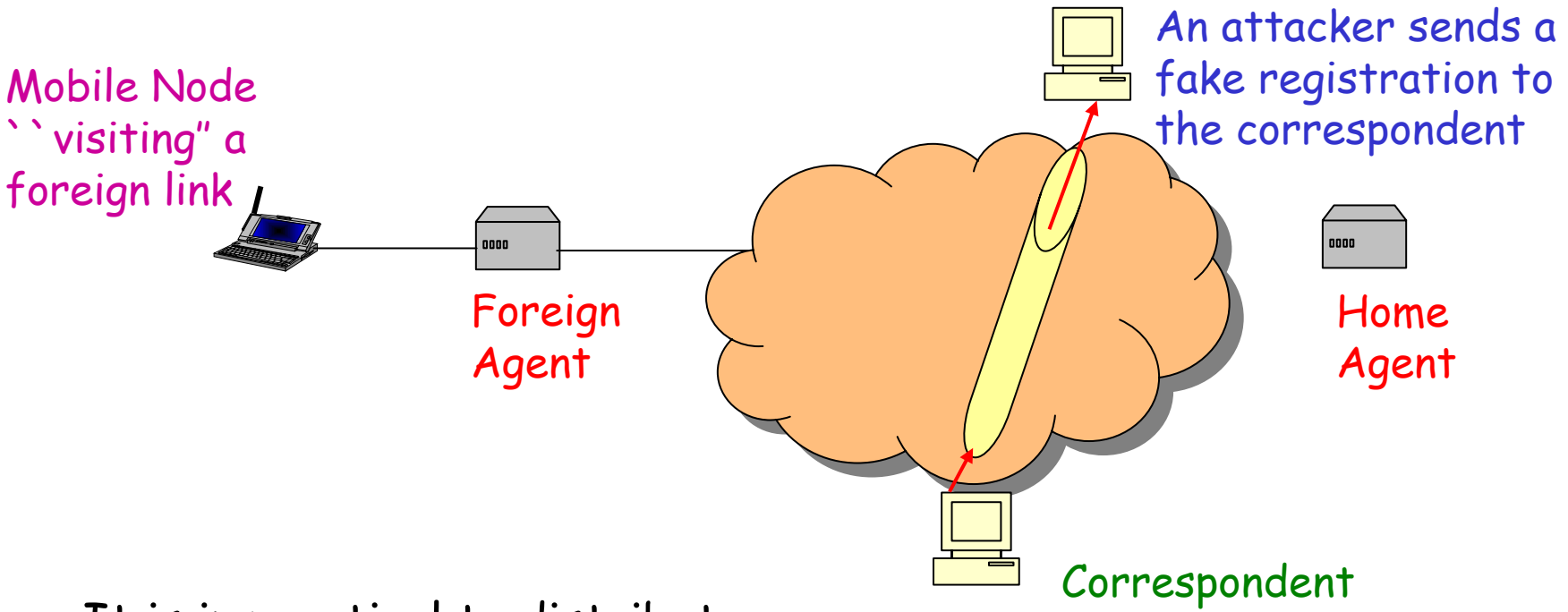
- Waste of network resources
- HA is a bottleneck
- What about network partitions?
- Why doesn’t the mobile node inform the correspondent of its care-of address and have it tunnel directly to the mobile node?

Optimized Routing



- This is potentially more efficient in terms of delay and resource consumption

Main Obstacle: Security



- It is impractical to distribute keys between a mobile node and every other node with which it might correspond

On the Home Network

- If the HA is the gateway host then picking up packets destined for the MH is trivial
- If the HA is **not** the gateway host then:

- The HA pretends to be MH and responds to requests for MH's physical address (e.g. Ethernet address) with its own physical address

- ARP caches on all hosts have to be updated upon registration of the MH (ARP replies)

On the Foreign Network

- The care-of address used for encapsulation may belong to the FA or may be a temporary address acquired by the mobile host (e.g. via DHCP)
- The MH must never send ARP frames on a foreign network
- The MH can obtain the FA's link-layer address from the *agent advertisement* messages

Mobile IPv6

- There is no need for Foreign Agents since the MH can use the *Address Autoconfiguration* protocol to obtain a dynamic care-of address

- No triangular routing

- Binding updates are supplied by encoding them as destination options in the IP header
- IPv6 provides security protocols hence simplifying the authentication process

Further Reading

- C. E. Perkins, “Mobile networking through mobile IP,” *IEEE Internet Computing*, pp. 58-69, Jan/Feb, 1998