

# Mobile IP

Roman Dunaytsev

The Bonch-Bruевич Saint-Petersburg  
State University of Telecommunications

[roman.dunaytsev@spbgut.ru](mailto:roman.dunaytsev@spbgut.ru)

Lecture № 9

# Outline

- 1 Introduction
- 2 Mobile IP operation
- 3 Agent discovery
- 4 Movement detection
- 5 Leaving the home network
- 6 Entering and staying in a visited network
- 7 Returning to the home network
- 8 Summary
- 9 Bibliography

# Outline

- 1 Introduction
- 2 Mobile IP operation
- 3 Agent discovery
- 4 Movement detection
- 5 Leaving the home network
- 6 Entering and staying in a visited network
- 7 Returning to the home network
- 8 Summary
- 9 Bibliography

# Introduction

- Why Mobile IP?
- IP was not designed with mobile networking in mind
  - At the time IP was developed, computers were large and rarely moved
  - Today, we have billions of mobile devices (laptops, smartphones, etc.)
- To support IP in a mobile environment, a new protocol called **Mobile IP** was developed
  - RFC 5944 'IP Mobility Support for IPv4', 2010 (aka **MIPv4**)
  - RFC 6275 'Mobility Support in IPv6', 2011 (aka **MIPv6**)

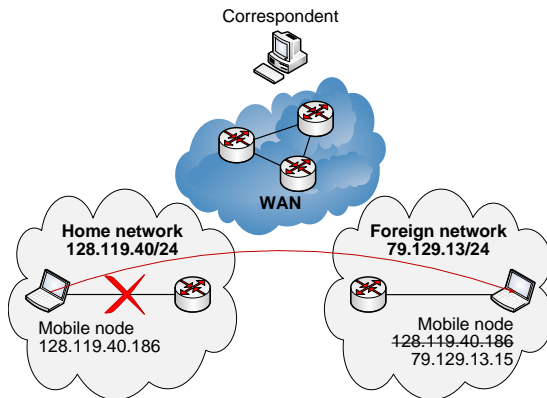


# Introduction (cont'd)

- The basic problem with supporting mobile nodes is that routing is performed using the IP address, while the IP address of a node is tied to the network where that node is located
- If a node changes networks, data sent to its old address cannot be delivered by conventional means
- Issues related to changing the IP address each time a node moves:
  - Break any existing connections
  - How to communicate the change of address to other nodes on the Internet?
  - Routing based on the entire IP address is not scalable

# Introduction (cont'd)

- With regular IP, when a mobile node moves to a foreign (visited) network, it will have to use an IP address from the IP address space of the foreign network



- **Goals and requirements :**
  - Seamless device mobility using existing device address
  - No new addressing or routing requirements
  - Limited hardware changes
  - Layer transparency
  - Interoperability
  - Scalability
  - Security

# Introduction (cont'd)

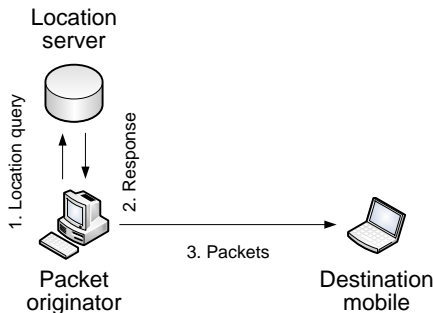
- Mobile IP accomplishes these goals and requirements by implementing a **forwarding** system for mobile nodes
  - When a mobile node is on its home network, it uses regular IP
  - When it moves to a different (aka foreign or visited) network, packets addressed to the mobile's home address are forwarded from its home network to its new location
- **Packet delivery to mobile destinations** – a process whereby a packet originator and the network use location information to deliver packets to a mobile destination
- **Packet delivery strategies** :
  - Direct delivery
  - Indirect (relayed) delivery



# Introduction (cont'd)

- **Direct delivery :**

- A packet originator first obtains the destination mobile's current location from a **location server**
- Then, it sends packets directly to the current location of the destination mobile



- **Benefits** of direct delivery:

- Ability to route packets along the most direct paths to their destinations

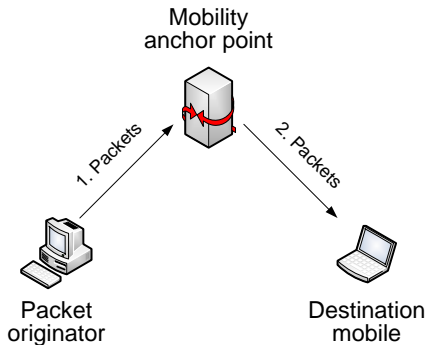
- **Shortcomings** of direct delivery:

- It requires a packet originator to determine whether the destination of a packet is a mobile or fixed host in order to decide whether a location query should be performed (performing location query for every destination could incur heavy overheads)
- It requires every packet originator to implement protocols for querying location servers
- Packet originators need to be able to discover the IP addresses of the location servers

# Introduction (cont'd)

- **Relayed delivery :**

- A packet will be sent first to a **mobility anchor point**, which then relays the packet toward its final destination
- The packet originator may not necessarily need to be aware of the existence of any mobility anchor point, nor the fact that it is sending packets to a mobility anchor point



- **Benefits** of relayed delivery:
  - It does not require changes to the packet originators; instead, mobility anchor points are responsible for determining the mobiles' locations and relaying packets to these mobile nodes
- **Shortcomings** of relayed delivery:
  - **Triangle routing problem** – packets must be routed first to the mobility anchor point and then to the final destination, even when a much more efficient route exists between the originator and the mobile node
  - Mobility anchor points could become performance bottlenecks
- **MIPv4 and MIPv6 use relayed delivery as their basic packet delivery strategy**

# Outline

- 1 Introduction
- 2 Mobile IP operation**
- 3 Agent discovery
- 4 Movement detection
- 5 Leaving the home network
- 6 Entering and staying in a visited network
- 7 Returning to the home network
- 8 Summary
- 9 Bibliography

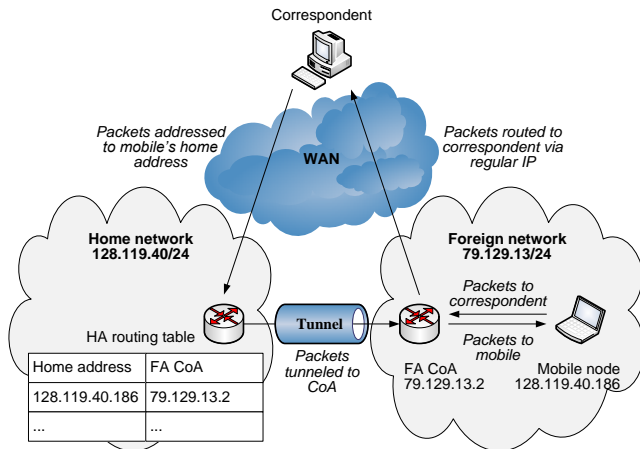
- Each mobile node has a **home network**
  - I.e., the network whose network address prefix matches that of the mobile's home address
- Packets addressed to a mobile's home address will be routed by regular IP routing to the mobile's home network
- When a mobile node is inside its home network, it receives and sends packets as a regular host without using Mobile IP
- When a mobile node is in a **foreign network**, a router on the mobile's home network will act as a **home agent** for the mobile node
  - The home agent will maintain up-to-date location information for the mobile node, intercept packets addressed to the mobile's home address, and tunnel these packets to the mobile's current location
  - **Tunneling** – the technology used to encapsulate one network protocol inside another for delivery

# Mobile IP Operation (cont'd)

- A mobile's location in a foreign network is identified by a temporary **Care-of Address (CoA)** assigned to the mobile node by the foreign network
- The mobile node uses this CoA to receive IP packets in the foreign network
- Each time the mobile node obtains a new CoA, it will register the new CoA with its home agent
- Each foreign network may have a **foreign agent** which:
  - Provides CoAs and other necessary configuration information
  - De-tunnels packets arriving from the visiting mobile's home agent and then delivers the packets to the visiting mobile node
  - Acts as the IP default router for packets sent by visiting mobile nodes
  - Helps visiting mobile nodes to determine whether they have moved into a different network

# Mobile IP Operation (cont'd)

- Packet flows between a correspondent host and a mobile node
  - The foreign agent is also the default router in the foreign network





# Mobile IP Operation (cont'd)

- **2 types of CoAs :**
- **Foreign agent (FA) CoA** – an IP address of a foreign agent
  - Each foreign agent is responsible for providing FA CoAs to visiting mobile nodes
  - When a FA CoA is used, the mobile's home agent tunnels the packets addressed to the mobile's home address to the mobile's current foreign agent
  - The foreign agent will then de-tunnel the packets and deliver them to the mobile node
- **Co-located CoA** – a CoA acquired by a mobile node through any method external to Mobile IP
  - E.g., by using the Dynamic Host Configuration Protocol (DHCP)
  - When a co-located CoA is used, the mobile's home agent tunnels the packets addressed to the mobile's home address directly to the mobile node itself

# Mobile IP Operation (cont'd)

- **Main phases of MIPv4 operation :**
  - Agent discovery
  - Movement detection
  - Leaving the home network
  - Entering and staying in a visited network
  - Returning to the home network

# Outline

- 1 Introduction
- 2 Mobile IP operation
- 3 Agent discovery**
- 4 Movement detection
- 5 Leaving the home network
- 6 Entering and staying in a visited network
- 7 Returning to the home network
- 8 Summary
- 9 Bibliography

- In order for a mobile node to communicate with a **mobility agent** (home or foreign), the mobile node will first need to know the agent's IP address
- Typically, each mobile node is configured with the IP address of its home agent
  - This is because a mobile's home agent usually does not change
  - However, to allow a mobile's home agent to change while the mobile node is away from home, a mobile node may also discover a home agent dynamically
- Mobile nodes always have to dynamically discover the existence and the IP addresses of foreign agents
  - Since it is impossible for a mobile node to be preconfigured with the addresses of all the foreign agents it may use

# Agent Discovery (cont'd)

- **Agent discovery** – the process for a mobile node to discover the mobility agents and receive information from these agents
- Agent discovery is achieved by the mobility agents advertising their services and system information to the mobile nodes via

## **Agent Advertisement messages**

- These messages may be periodically broadcast
- A mobile node does not have to wait passively for the Agent Advertisement messages to arrive
- It may solicit an Agent Advertisement message from the mobility agents by sending **Agent Solicitation messages** to the Mobile-Agents Multicast Group address 224.0.0.11
  - All mobility agents are required to respond to any received Agent Solicitation message

# Agent Discovery (cont'd)

- For Agent discovery, MIPv4 uses the Internet Control Message Protocol (ICMP) Router Discovery messages:
  - **ICMP Router Advertisement** – sent by a router to hosts to inform them of the IP addresses of the router
  - **ICMP Router Solicitation** – sent by a host to a router to ask the router to send an ICMP Router Advertisement message
- MIPv4 Agent Advertisement message uses the ICMP Router Advertisement format with 2 extensions to carry MIPv4-specific information
- MIPv4 Agent Solicitation message uses the ICMP Router Solicitation format, except that its IP Time-to-Live (TTL) field must be set to 1
  - Hence, Agent Solicitation messages will not propagate beyond the local IP subnet

- **2 extensions to the ICMP Router Advertisement message :**
- **Mobility Agent Advertisement**
  - Indicates that an ICMP Router Advertisement message is also a MIPv4 Agent Advertisement message
  - Carries information specific to a MIPv4 mobility agent
- **Prefix-Lengths**
  - An optional extension used to indicate the network prefix length, in bits, of each Router Address advertised in the ICMP Router Advertisement portion of the Agent Advertisement
  - The network prefix lengths may be used by a mobile node to determine whether it has moved into a new IP network

# Agent Discovery (cont'd)

- MIPv4 Agent Advertisement message

ICMP Router Advertisement (RFC 1256)
Mobility Agent Advertisement extension
Prefix-Lengths extension (if present)



# Agent Discovery (cont'd)

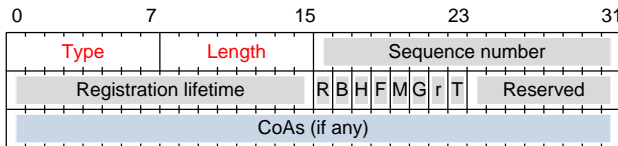
- **MIPv4 Mobility Agent Advertisement extension**

- **Type**, 8 bits

- Indicates the Agent Advertisement extension type
- For the Mobility Agent Advertisement extension, Type = 16

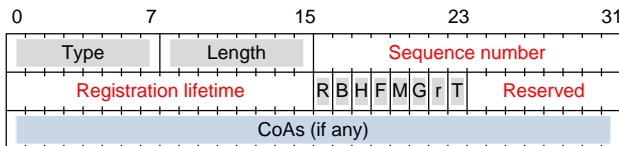
- **Length**, 8 bits

- Indicates the length of the extension, in bytes, excluding the Type and Length fields
- Thus, Length = 6 plus 4 for each CoA in the message



# Agent Discovery (cont'd)

- **Sequence number**, 16 bits
  - A sequential counter set to 0 when the router initializes and then incremented for each advertisement sent out
- **Registration lifetime**, 16 bits
  - Indicates the maximum length of time, in seconds, the agent is willing to accept for registration requests
  - A value of 65,535 (all '1's) means 'infinite'
- **Flags**, 8 bits (1 bit each)
- **Reserved**, 8 bits
  - Not used, must be all '0's



# Agent Discovery (cont'd)

- **R (Registration required)**

- Mobile nodes must register through the foreign agent, even when using a co-located CoA

- **B (Busy)**

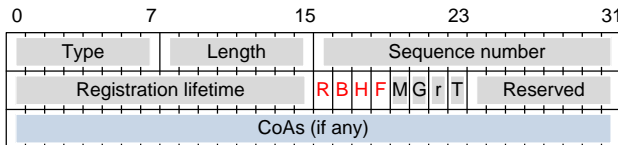
- The mobility agent is currently too busy to accept further registrations from mobile nodes

- **H (Home agent)**

- The mobility agent is willing to function as a home agent on this link
- Note that a router can offer services as both a home agent and a foreign agent

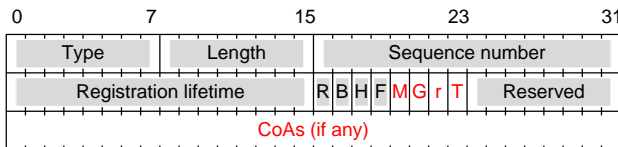
- **F (Foreign agent)**

- The mobility agent is willing to function as a foreign agent



# Agent Discovery (cont'd)

- **M (Minimal encapsulation)**
  - The agent can receive tunneled packets using minimal encapsulation
- **G (GRE encapsulation)**
  - The agent can receive tunneled packets using GRE encapsulation
- **r (Reserved)**
  - Not used, must be '0'
- **T (Reverse tunneling)**
  - The agent supports reverse tunneling
- **0 or more FA CoAs**
  - A foreign agent must always provide at least 1 address in its advertisement
  - A router that cannot act as a foreign agent will typically omit this field



# Agent Discovery (cont'd)

- **MIPv4 Prefix-Lengths extension**

- **Type**, 8 bits

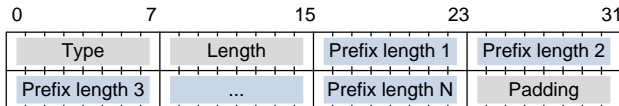
- Indicates the Agent Advertisement extension type
- For the Prefix-Lengths extension, Type = 19

- **Length**, 8 bits

- Indicates the length of the extension, in bytes, excluding the Type and Length fields
- Thus, Length = the number of prefix lengths (since each takes 1 byte)

- **Prefix lengths**, variable (1 byte each)

- Indicates the number of bits of network prefix that applies to each router address listed in the ICMP Router Advertisement portion



# Outline

- 1 Introduction
- 2 Mobile IP operation
- 3 Agent discovery
- 4 Movement detection**
- 5 Leaving the home network
- 6 Entering and staying in a visited network
- 7 Returning to the home network
- 8 Summary
- 9 Bibliography

# Movement Detection

- A mobile node needs to know when it enters a new IP subnet
  - I.e., when it may need to change its CoA
- **Movement detection** – the process for a mobile node to detect when it enters a new IP subnet
- Mobile nodes can use the following information in the received Agent Advertisement messages to detect movement:
- **Use the Lifetime field**
  - Each Agent Advertisement message has a Lifetime field (in the main body of the ICMP Router Advertisement portion) that indicates the length of time that this Agent Advertisement is valid
  - If the mobile node does not receive any new Agent Advertisement from the same mobility agent within the remaining Lifetime, it will assume that it has moved into a new network

# Movement Detection (cont'd)

- **Use the network prefixes**

- A foreign agent may advertise the network prefix length of the local subnet in the Agent Advertisement message with the Prefix-Lengths extension
- A mobile node may detect whether it has moved into a new IP subnet by comparing the network prefix of the old network with the network prefix of the new IP subnet
- If the 2 network prefixes differ, the mobile node has just entered a new IP subnet

- In addition, a mobile node may use any other method for movement detection
  - E.g., change of radio access points or radio channels

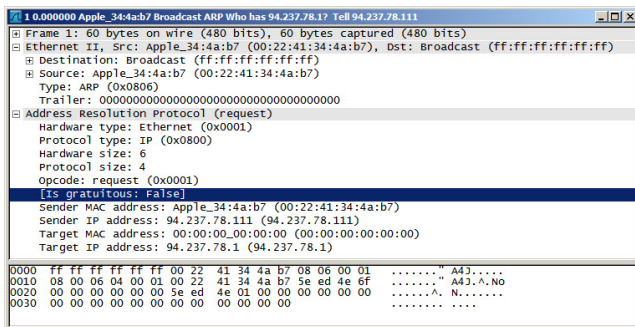


# Outline

- 1 Introduction
- 2 Mobile IP operation
- 3 Agent discovery
- 4 Movement detection
- 5 Leaving the home network**
- 6 Entering and staying in a visited network
- 7 Returning to the home network
- 8 Summary
- 9 Bibliography

# Leaving the Home Network

- Before a mobile node leaves its home network, it needs to ensure that, after it is outside its home network, the home agent will be able to capture the packets addressed to the mobile's home address
- This can be done by using the Address Resolution Protocol (ARP)
  - ARP is used to determine the hardware address associated with a target IP address



# Leaving the Home Network (cont'd)

- **2 issues need to be resolved** :
- Firstly, after a mobile node leaves its home network, other nodes on the home network may still have the mapping of the mobile's IP address to its hardware address cached in their **ARP caches**
  - As a result, they will continue to send packets to the mobile's hardware address rather than to the home agent
- MIPv4 uses **Gratuitous ARP** to solve this problem:
  - A Gratuitous ARP packet is sent by a node to trigger other nodes to update their ARP caches
  - Thus, before a mobile node leaves its home network, it broadcasts a Gratuitous ARP packet to all other nodes (including mobility agents) on the local IP subnet

## Leaving the Home Network (cont'd)

- Secondly, when the mobile node is away from the home network, it will not be able to reply to the ARP REQUESTs sent by other nodes on the home network
- MIPv4 uses **Proxy ARP** to solve this problem:
  - A Proxy ARP packet is sent by one node on behalf of another node in response to an ARP REQUEST
  - When the home agent receives an ARP REQUEST asking for the hardware address of the mobile node that is away from the home network, the home agent will reply to this ARP REQUEST providing its own hardware address
  - This will cause the nodes to forward packets addressed to the mobile's home address to the home agent

# Outline

- 1 Introduction
- 2 Mobile IP operation
- 3 Agent discovery
- 4 Movement detection
- 5 Leaving the home network
- 6 Entering and staying in a visited network**
- 7 Returning to the home network
- 8 Summary
- 9 Bibliography

# Entering and Staying in a Visited Network

- Upon entering a visited network, a mobile node will have to acquire a temporary CoA from the visited network
- Then, the mobile node will have to register this new CoA with its home agent
- This will cause the home agent to tunnel the packets addressed to the mobile's home address to this new CoA
- **2 messages for the registration operation :**
  - Registration Request
  - Registration Reply
- These messages are carried within UDP datagrams and sent to port 434

# Entering and Staying in a Visited Network (cont'd)

- A mobile node may register its current CoA with its home agent directly or through a foreign agent
  - **Directly** – sending Registration Request messages directly to the home agent without having to go through a foreign agent
  - **Through a foreign agent** – sending Registration Request messages first to a foreign agent, which will process the messages and then forward them to the mobile's home agent
- Registering through a foreign agent allows the visited network to **enforce policies on network access and accounting**
  - When a mobile node receives an Agent Advertisement with the 'R' flag, the mobile node is required to register through the foreign agent even if the mobile node can acquire its own co-located CoA without the assistance of the foreign agent

# Entering and Staying in a Visited Network (cont'd)

- MIPv4 registration message flows

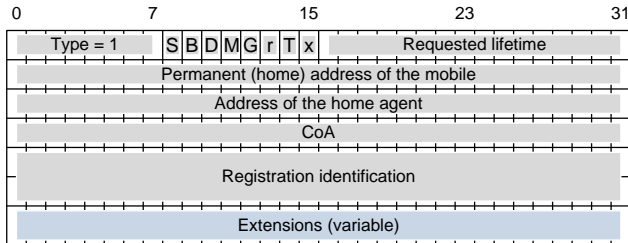




# Entering and Staying in a Visited Network (cont'd)

## • Registration Request

- S (Simultaneous bindings)
- B (Broadcast packets)
- D (Decapsulation by mobile)
- M (Minimal encapsulation)
- G (GRE encapsulation)
- r (Reserved, must be '0')
- T (Reverse tunneling requested)
- x (Reserved, must be '0')

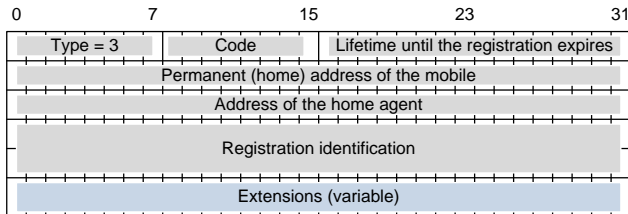


# Entering and Staying in a Visited Network (cont'd)

- **Registration Reply**

- **Code**, 8 bits

- Indicates the result of the registration request
- Code = 0 if the registration was accepted
- Code = 1 if the registration was accepted but simultaneous bindings were requested and are not supported
- If the registration was denied, a different value is provided that indicates the reason for the rejection, as well as whether it was the home or foreign agent that denied it



# Entering and Staying in a Visited Network (cont'd)

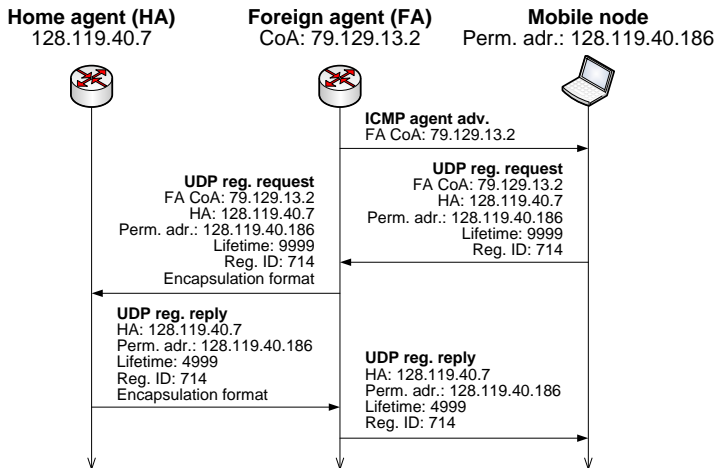
- **Registration through a foreign agent :**
- Following the receipt of a FA Agent Advertisement message, a mobile node sends a Registration Request message to the foreign agent
- The foreign agent receives the Registration Request message and records the mobile's permanent IP address
  - It now knows that it should be looking for tunneled packets containing an encapsulated packet whose destination address matches the permanent address of the mobile node
- Then, the foreign agent sends a Registration Request message to the home agent

## Entering and Staying in a Visited Network (cont'd)

- The home agent receives the Registration Request message and checks for authenticity and correctness
- Then, the home agent binds the mobile's permanent IP address with the CoA
  - In the future, packets arriving at the home agent and addressed to the mobile node will now be encapsulated and tunneled to the CoA
- The home agent sends a Registration Reply message to the foreign agent
- The foreign agent receives the Registration Reply and then forwards it to the mobile node

# Entering and Staying in a Visited Network (cont'd)

- Note that the home agent specifies a lifetime that is smaller than the lifetime requested by the mobile node



# Outline

- 1 Introduction
- 2 Mobile IP operation
- 3 Agent discovery
- 4 Movement detection
- 5 Leaving the home network
- 6 Entering and staying in a visited network
- 7 Returning to the home network**
- 8 Summary
- 9 Bibliography

# Returning to the Home Network

- When a mobile node returns to its home network, it needs to ensure that the packets addressed to its home address will now be forwarded to itself directly, rather than to its home agent
- Firstly, the IP-to-hardware address binding cached by nodes on the home network should be updated
  - The returning mobile node needs to broadcast **Gratuitous ARP** packets over the home network
- Secondly, the home agent should be informed that the mobile node is back
  - The returning mobile node needs to send a **MIPv4 Deregistration Request** to the home agent
  - It is simply a Registration Request message with its Lifetime field set to all '0'

# Outline

- 1 Introduction
- 2 Mobile IP operation
- 3 Agent discovery
- 4 Movement detection
- 5 Leaving the home network
- 6 Entering and staying in a visited network
- 7 Returning to the home network
- 8 Summary**
- 9 Bibliography



- Mobile IP accomplishes its goals as follows:
  - **Seamless device mobility using existing device address** – mobile devices can change their location while continuing to use their existing IP address
  - **No new addressing or routing requirements** – the overall scheme for addressing and routing as in regular IP is maintained
  - **Limited hardware changes** – changes are only required to the software in mobile devices and routers used directly by the mobile devices
  - **Layer transparency** – the changes made by Mobile IP are confined to the network layer
  - **Interoperability** – Mobile IP devices can still send to and receive from regular IP devices and vice versa
  - **Scalability** – Mobile IP allows a mobile device to change from one network to another, and supports this for an arbitrary number of devices
  - **Security** – Mobile IP works by redirecting messages, and includes authentication procedures to prevent an unauthorized device from causing problems

# Summary (cont'd)

- **Limitations of Mobile IP :**

- Triangular routing
- Mobility agents may become a performance bottleneck
- Potential long handover delays, not suitable for real-time applications
- Mobile nodes do not explicitly deregister with a foreign agent in a visited network, so it does not know when to release resources



- **Examples of use :**

- Roaming between overlapping wireless systems (DVB, WLAN, BWA)
- Currently, Mobile IP is not required within cellular systems such as 3G

# Outline

- 1 Introduction
- 2 Mobile IP operation
- 3 Agent discovery
- 4 Movement detection
- 5 Leaving the home network
- 6 Entering and staying in a visited network
- 7 Returning to the home network
- 8 Summary
- 9 Bibliography**

# Bibliography

-  Jyh-Cheng Chen, Tao Zhang, 'IP-Based Next-Generation Wireless Networks: Systems, Architectures, and Protocols', John Wiley & Sons, 2004
-  Charles M. Kozierok, 'The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference', No Starch Press, 2005

