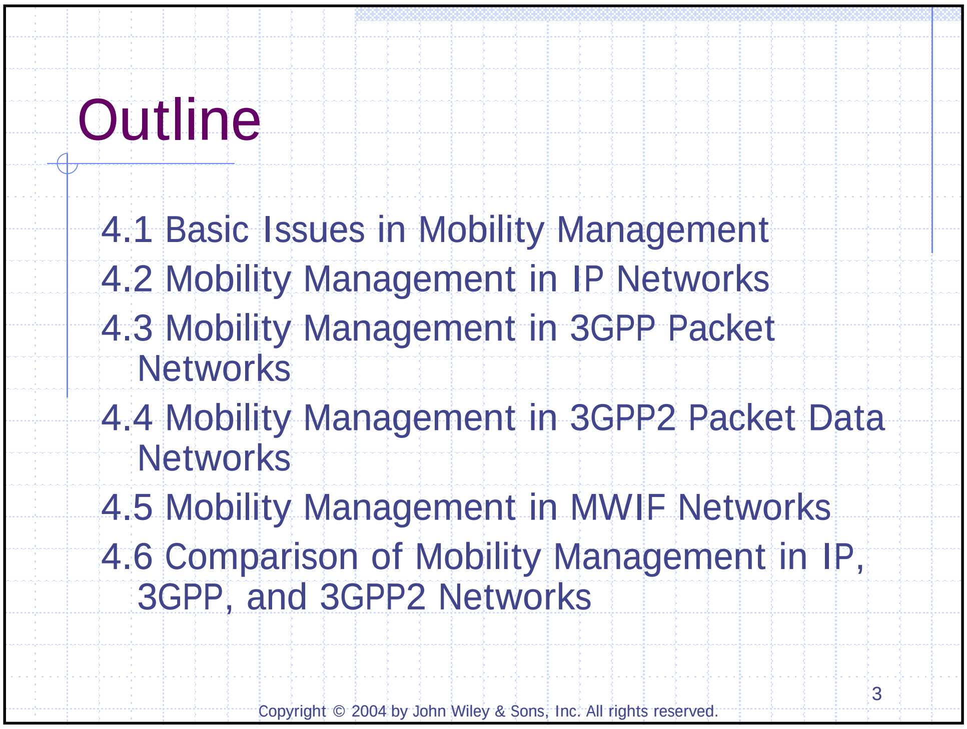
Chapter 4: Mobility Management

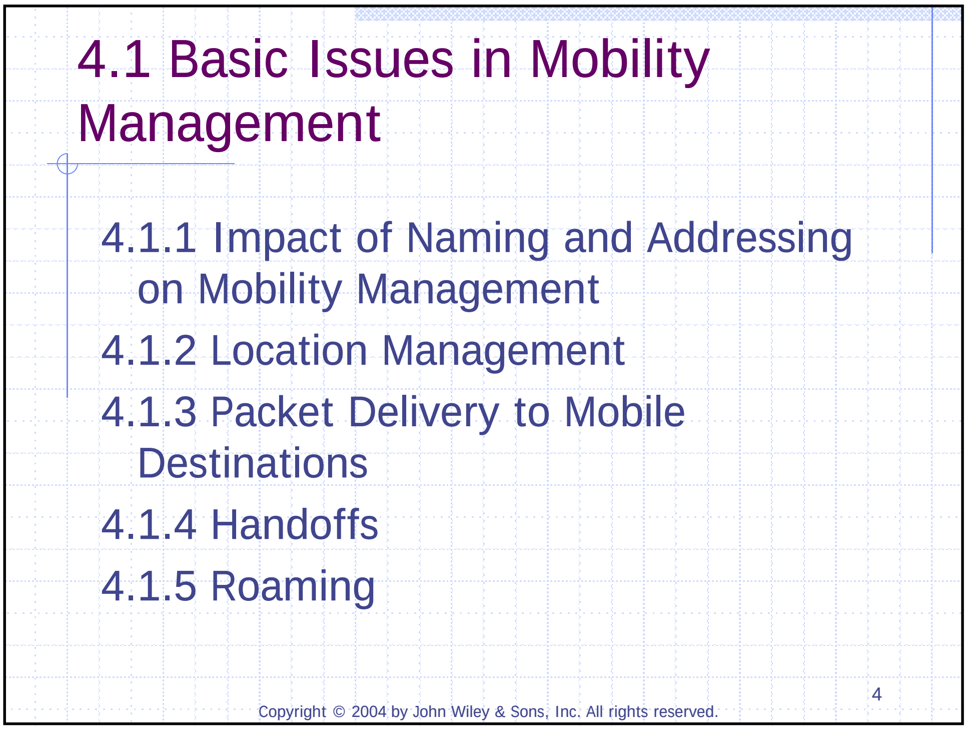
Jyh-Cheng Chen and Tao Zhang

IP-Based Next-Generation Wireless Networks
Published by John Wiley & Sons, Inc.
January 2004



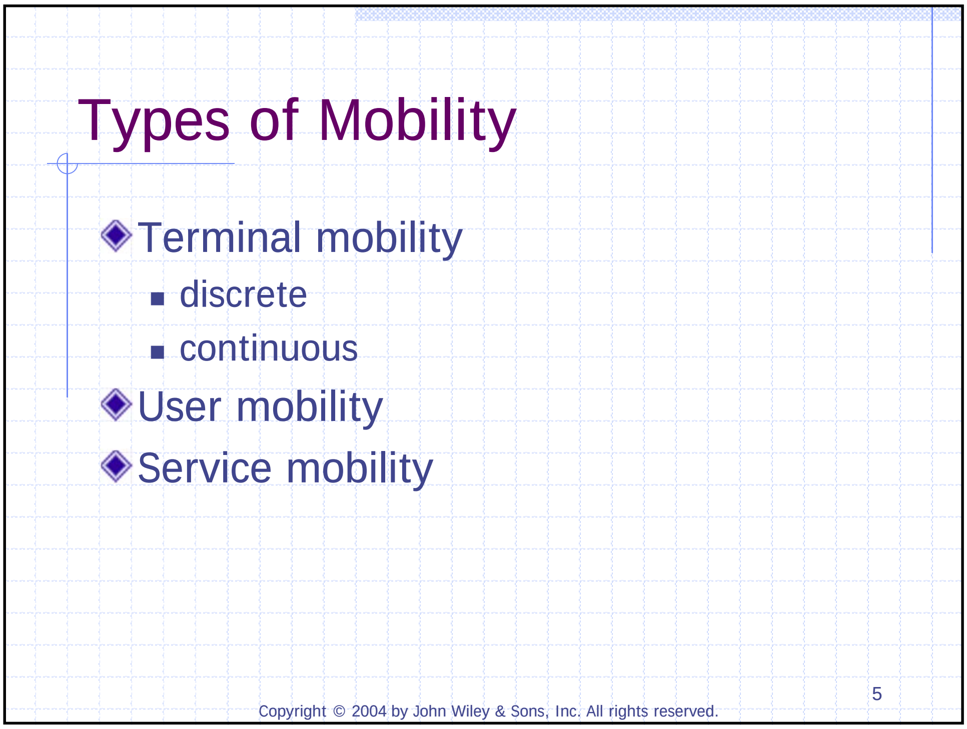
Outline

- 4.1 Basic Issues in Mobility Management
- 4.2 Mobility Management in IP Networks
- 4.3 Mobility Management in 3GPP Packet Networks
- 4.4 Mobility Management in 3GPP2 Packet Data Networks
- 4.5 Mobility Management in MWIF Networks
- 4.6 Comparison of Mobility Management in IP, 3GPP, and 3GPP2 Networks



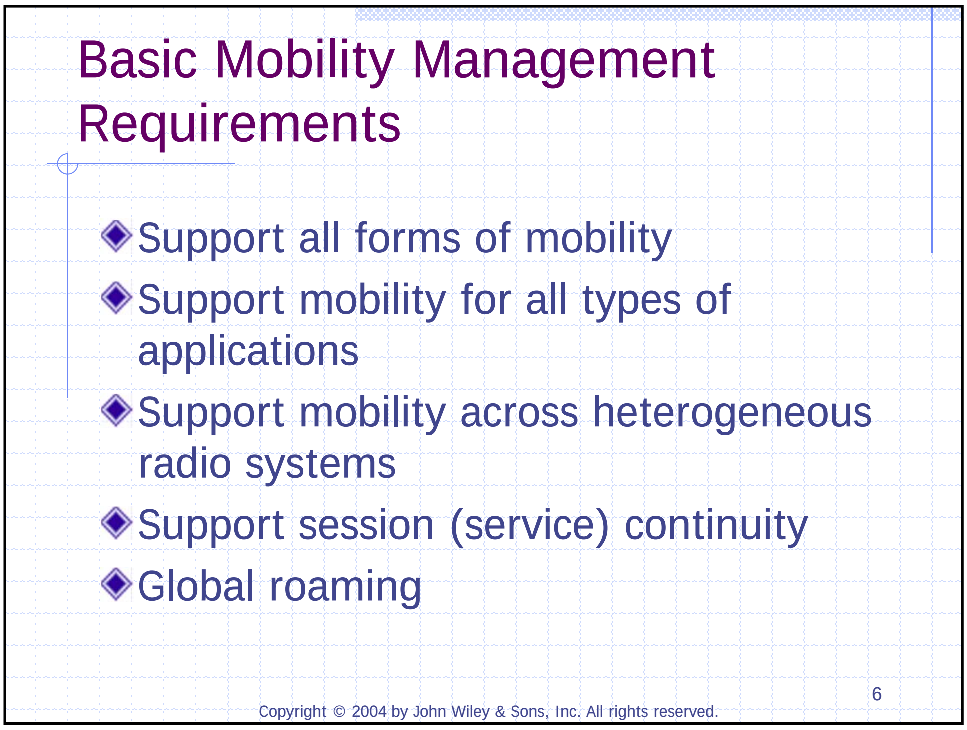
4.1 Basic Issues in Mobility Management

- 4.1.1 Impact of Naming and Addressing on Mobility Management
- 4.1.2 Location Management
- 4.1.3 Packet Delivery to Mobile Destinations
- 4.1.4 Handoffs
- 4.1.5 Roaming



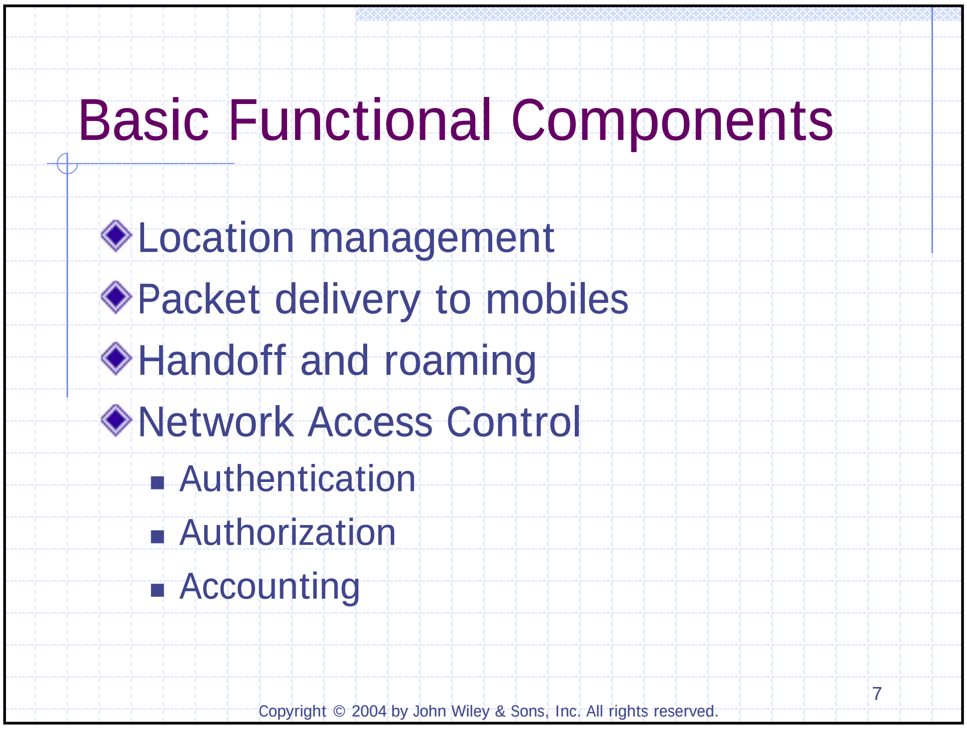
Types of Mobility

- Terminal mobility
  - discrete
  - continuous
- User mobility
- Service mobility



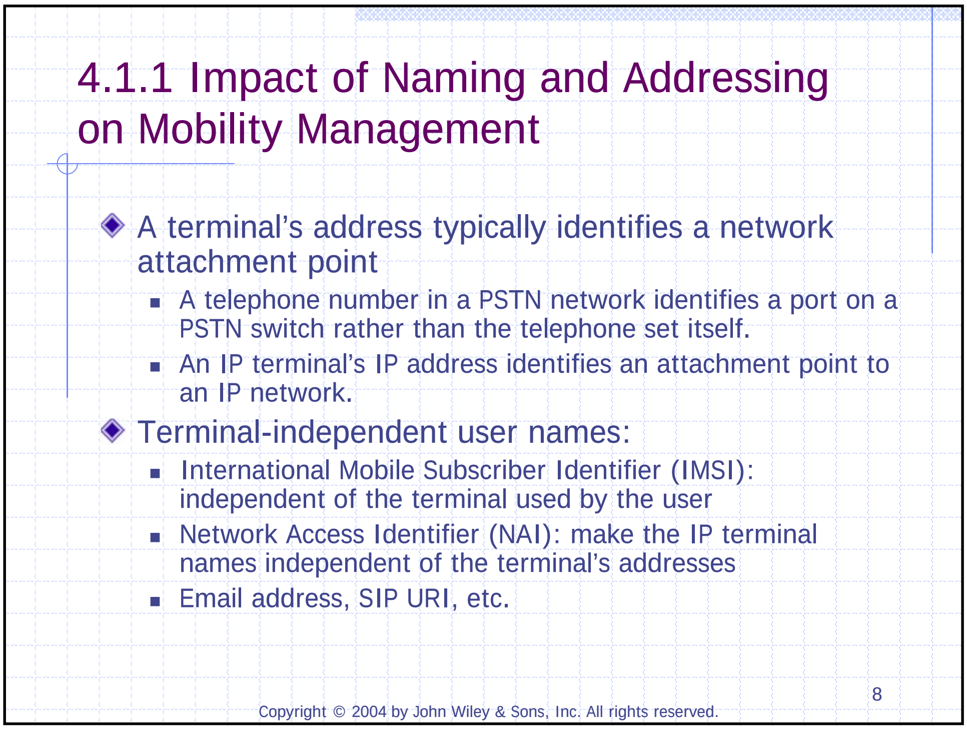
Basic Mobility Management Requirements

- Support all forms of mobility
- Support mobility for all types of applications
- Support mobility across heterogeneous radio systems
- Support session (service) continuity
- Global roaming



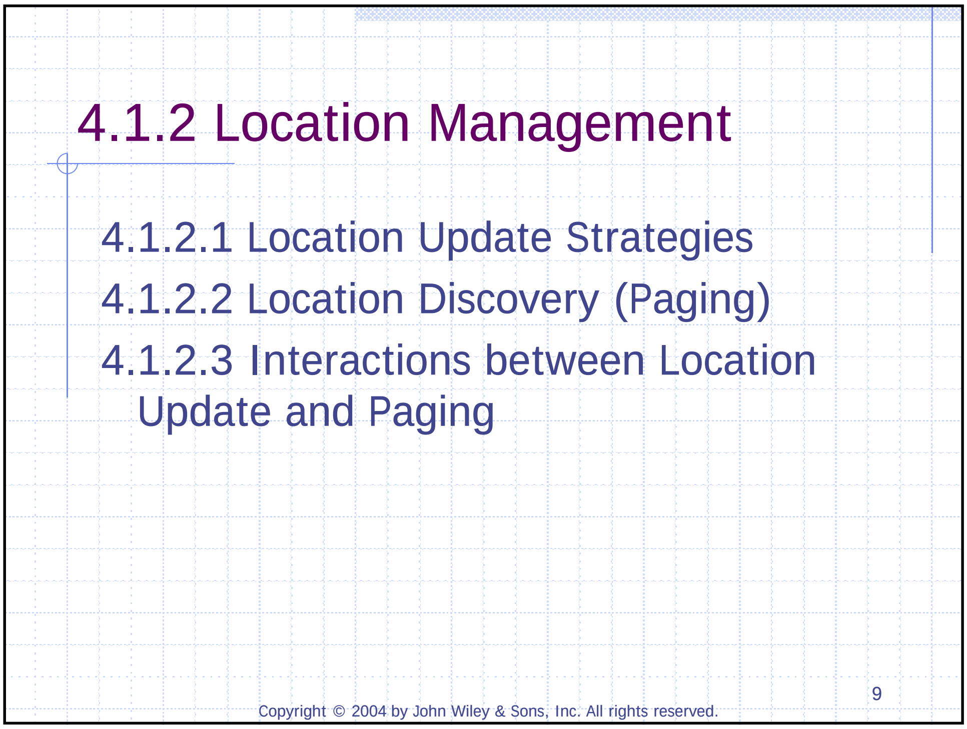
Basic Functional Components

- Location management
- Packet delivery to mobiles
- Handoff and roaming
- Network Access Control
  - Authentication
  - Authorization
  - Accounting



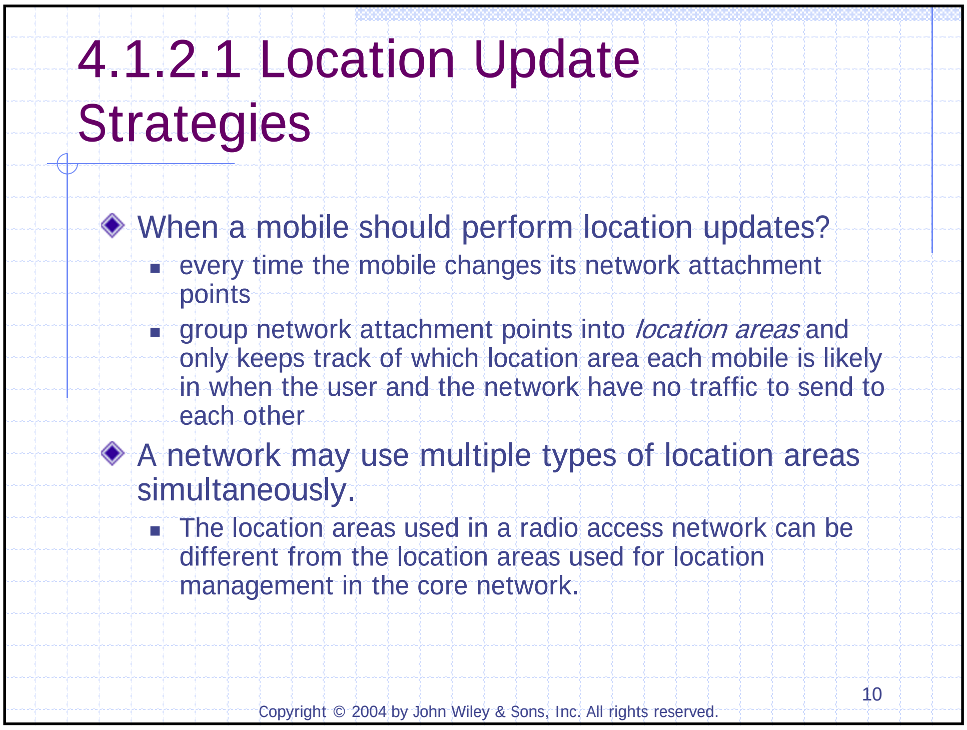
4.1.1 Impact of Naming and Addressing on Mobility Management

- A terminal's address typically identifies a network attachment point
  - A telephone number in a PSTN network identifies a port on a PSTN switch rather than the telephone set itself.
  - An IP terminal's IP address identifies an attachment point to an IP network.
- Terminal-independent user names:
  - International Mobile Subscriber Identifier (IMSI): independent of the terminal used by the user
  - Network Access Identifier (NAI): make the IP terminal names independent of the terminal's addresses
  - Email address, SIP URI, etc.



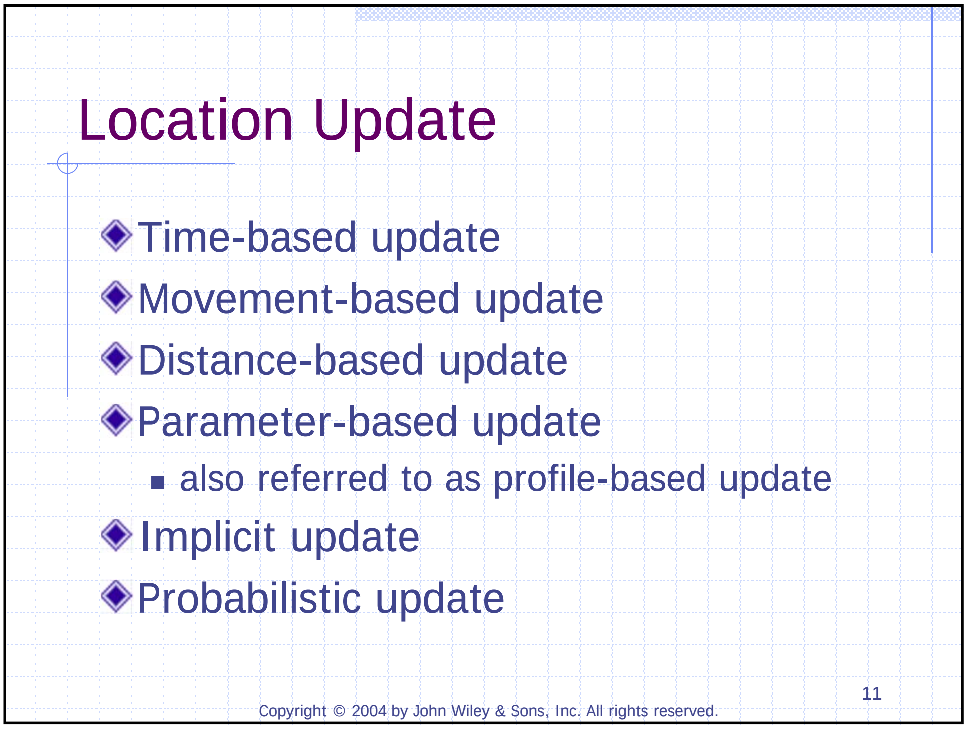
4.1.2 Location Management

- 4.1.2.1 Location Update Strategies
- 4.1.2.2 Location Discovery (Paging)
- 4.1.2.3 Interactions between Location Update and Paging



4.1.2.1 Location Update Strategies

- When a mobile should perform location updates?
  - every time the mobile changes its network attachment points
  - group network attachment points into *location areas* and only keeps track of which location area each mobile is likely in when the user and the network have no traffic to send to each other
- A network may use multiple types of location areas simultaneously.
  - The location areas used in a radio access network can be different from the location areas used for location management in the core network.



Location Update

- Time-based update
- Movement-based update
- Distance-based update
- Parameter-based update
  - also referred to as profile-based update
- Implicit update
- Probabilistic update

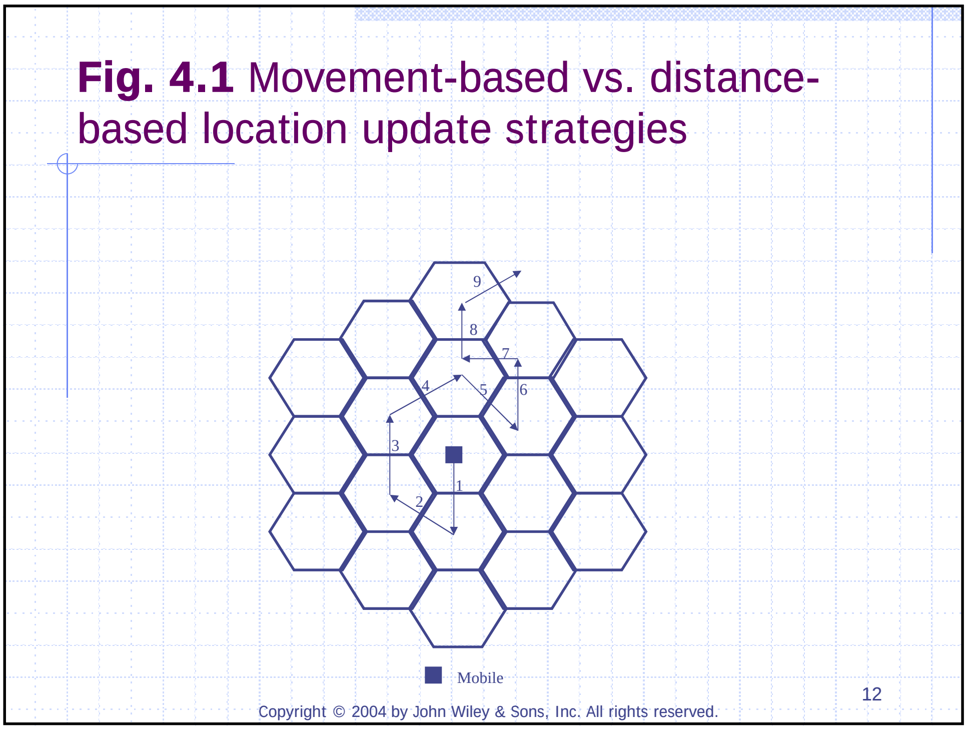
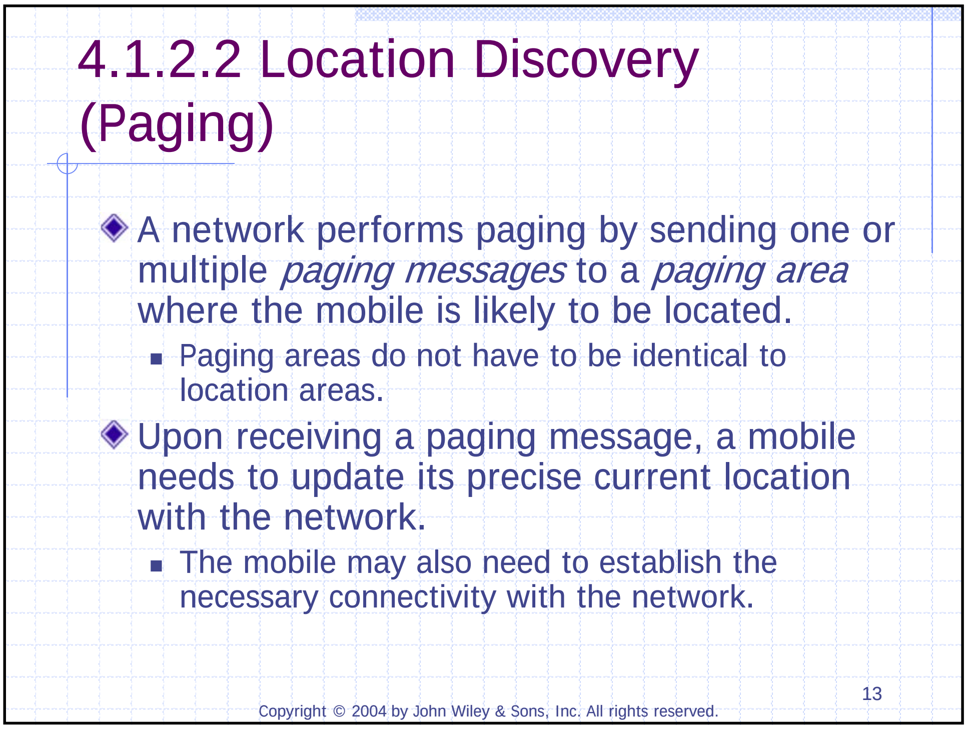
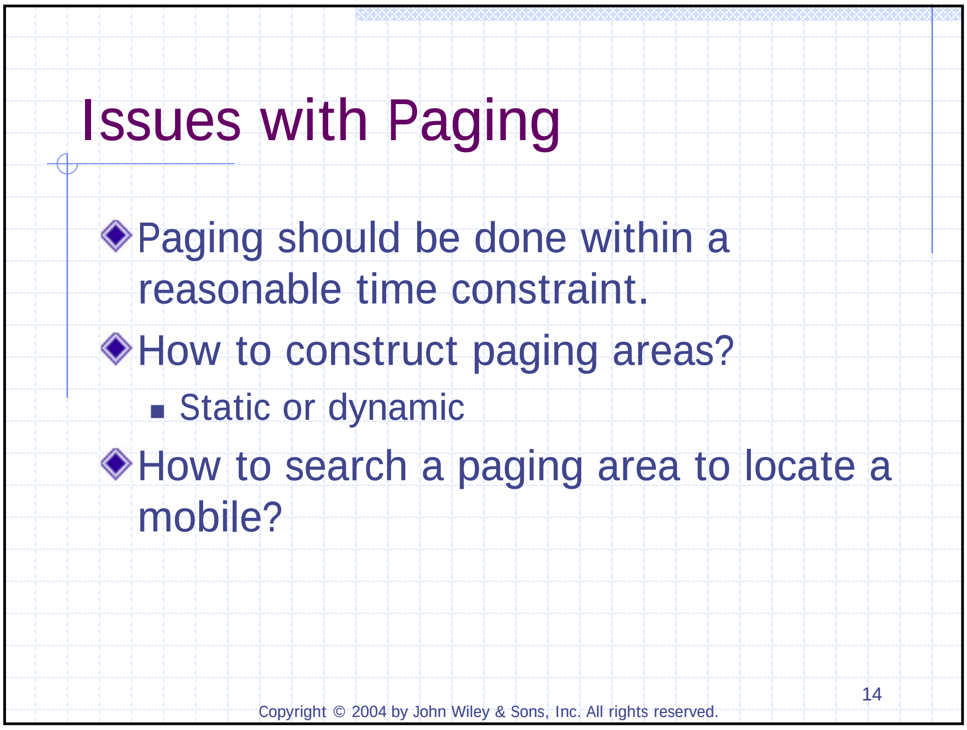


Fig. 4.1 Movement-based vs. distance-based location update strategies



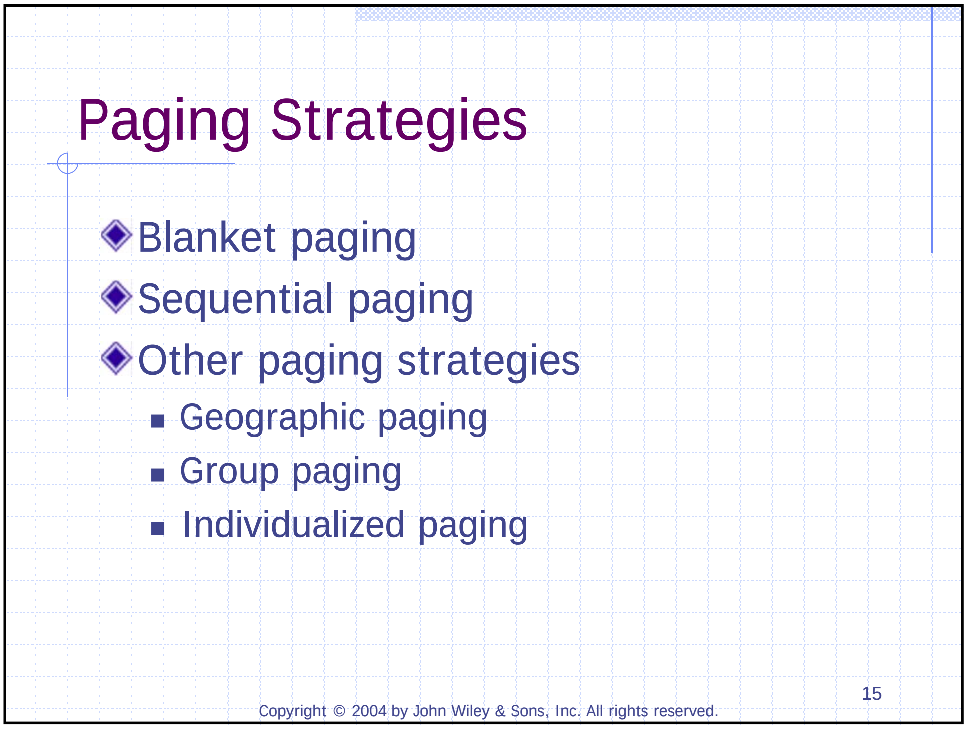
4.1.2.2 Location Discovery (Paging)

- A network performs paging by sending one or multiple *paging messages* to a *paging area* where the mobile is likely to be located.
  - Paging areas do not have to be identical to location areas.
- Upon receiving a paging message, a mobile needs to update its precise current location with the network.
  - The mobile may also need to establish the necessary connectivity with the network.



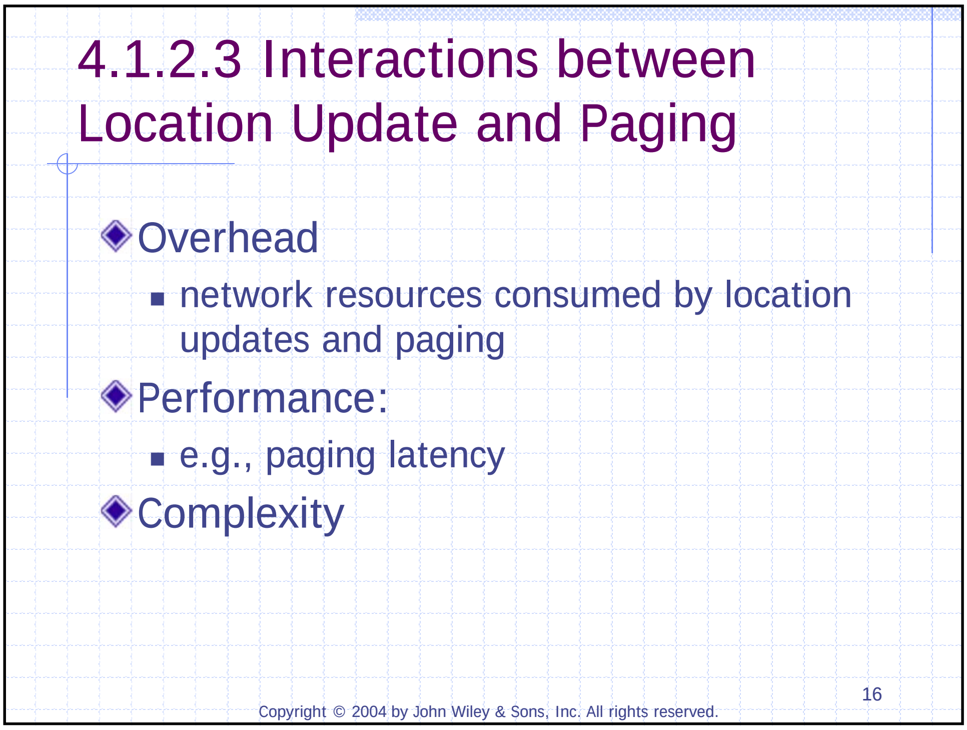
Issues with Paging

- Paging should be done within a reasonable time constraint.
- How to construct paging areas?
  - Static or dynamic
- How to search a paging area to locate a mobile?



Paging Strategies

- Blanket paging
- Sequential paging
- Other paging strategies
  - Geographic paging
  - Group paging
  - Individualized paging



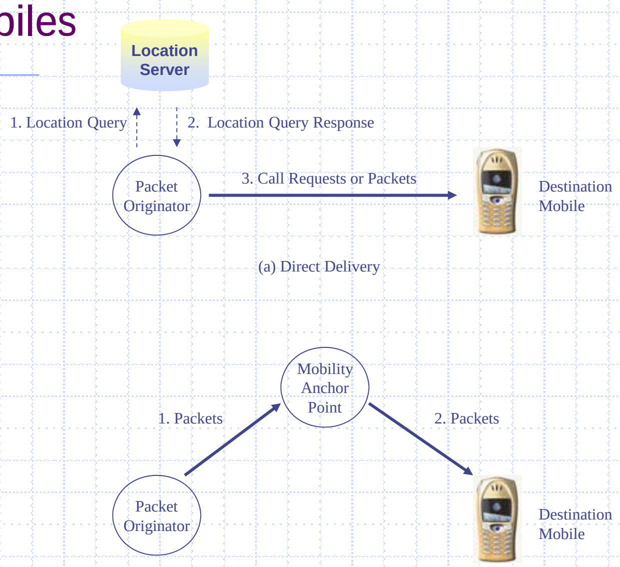
4.1.2.3 Interactions between Location Update and Paging

- Overhead
  - network resources consumed by location updates and paging
- Performance:
  - e.g., paging latency
- Complexity

4.1.3 Packet Delivery to Mobile Destinations

- Direct Delivery
  - may route packets along the most direct paths
  - need to know whether destination is a mobile or fixed host
  - require every originator to implement protocols for determining a destination’s location
- Relayed Delivery
  - mobility anchor points could become traffic and performance bottlenecks

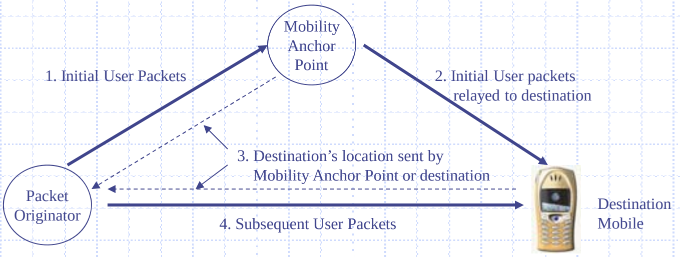
Fig. 4.2 Strategies for delivering packets to mobiles



(a) Direct Delivery

(b) Relayed Delivery

Fig. 4.3 Integrated Delayed Delivery and Direct Delivery strategies



Mobility Anchor Point

1. Initial User Packets

2. Initial User packets relayed to destination

3. Destination's location sent by Mobility Anchor Point or destination

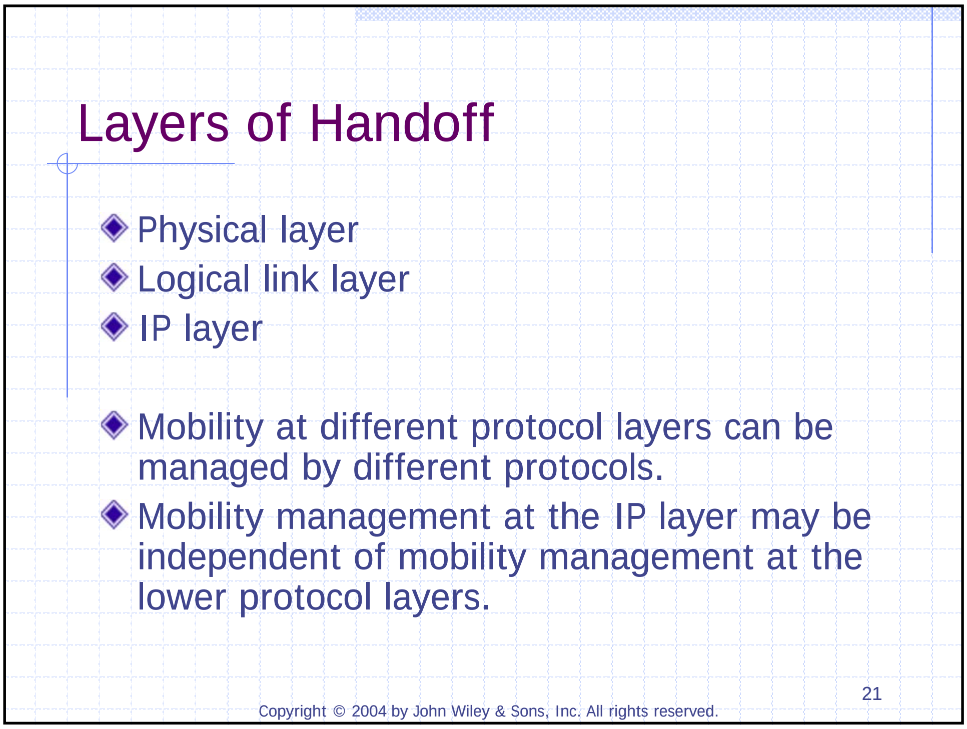
Packet Originator

4. Subsequent User Packets

Destination Mobile

4.1.4 Handoffs

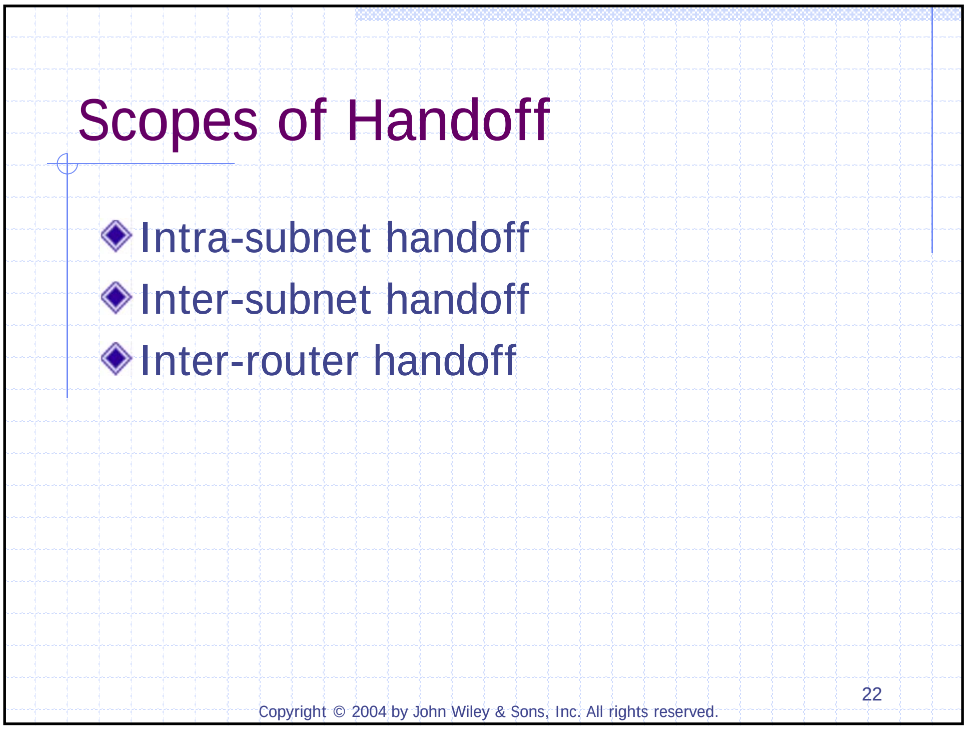
- Handoffs in an IP-based wireless network may occur at different protocol layers.
- Handoffs at each protocol layer may occur in different scopes.
- Handoffs can be hard or soft.



Layers of Handoff

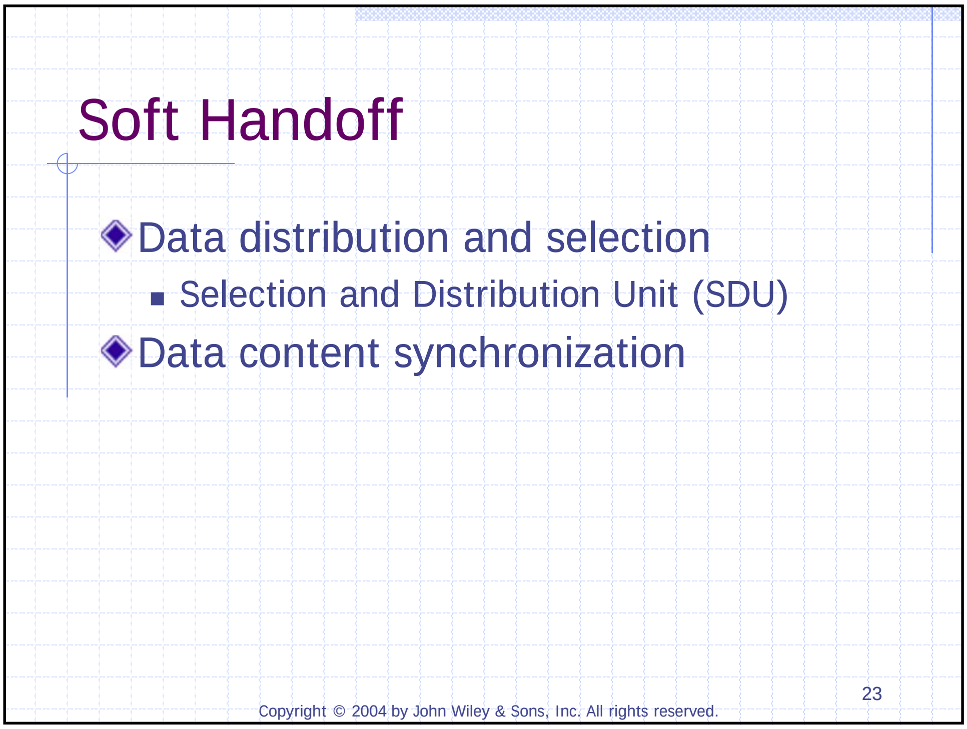
- Physical layer
- Logical link layer
- IP layer

- Mobility at different protocol layers can be managed by different protocols.
- Mobility management at the IP layer may be independent of mobility management at the lower protocol layers.



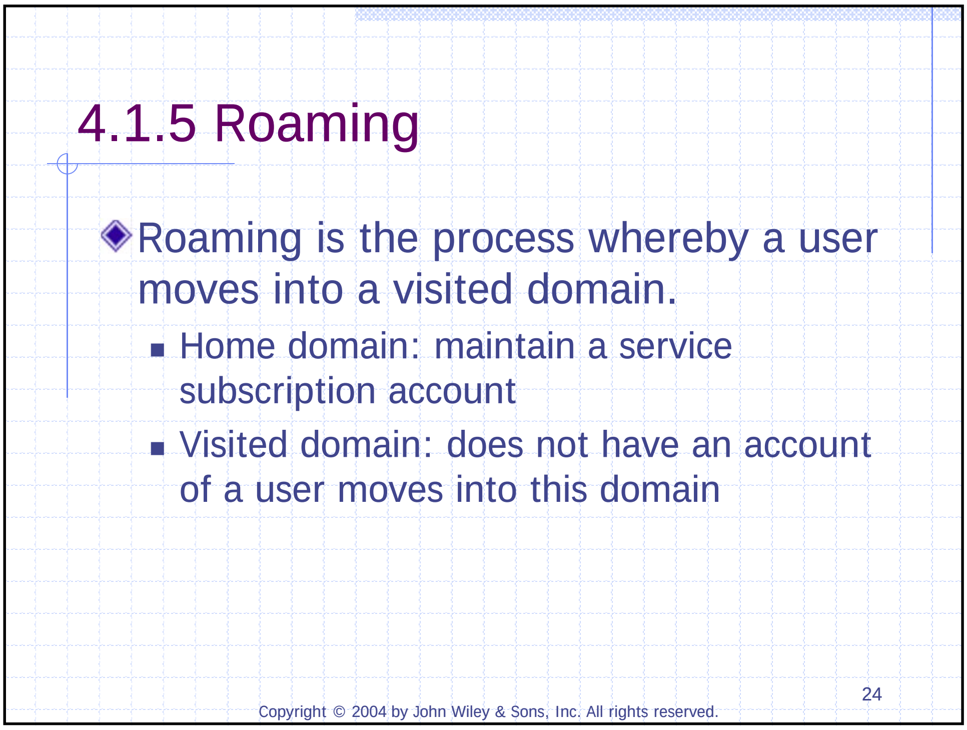
Scopes of Handoff

- Intra-subnet handoff
- Inter-subnet handoff
- Inter-router handoff



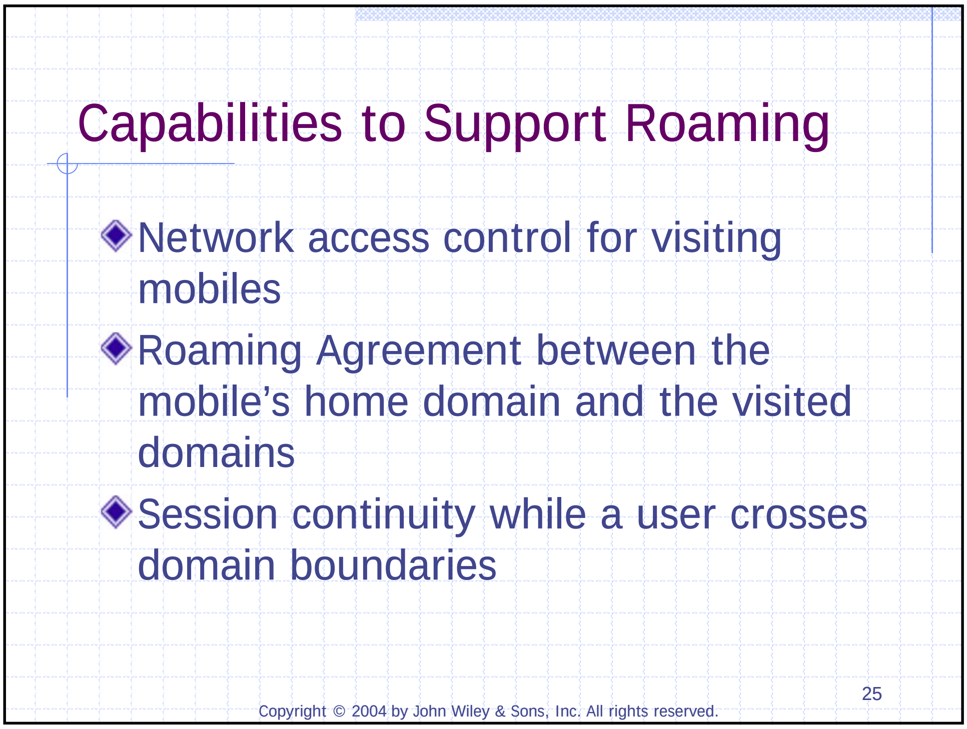
Soft Handoff

- Data distribution and selection
  - Selection and Distribution Unit (SDU)
- Data content synchronization



4.1.5 Roaming

- Roaming is the process whereby a user moves into a visited domain.
  - Home domain: maintain a service subscription account
  - Visited domain: does not have an account of a user moves into this domain



Capabilities to Support Roaming

- Network access control for visiting mobiles
- Roaming Agreement between the mobile’s home domain and the visited domains
- Session continuity while a user crosses domain boundaries

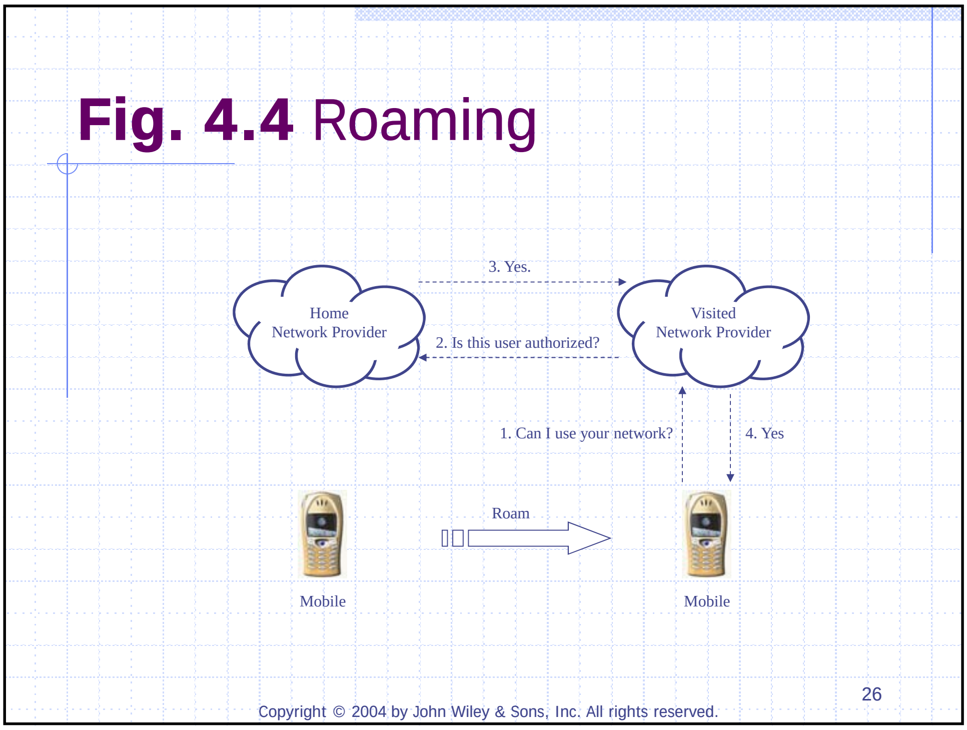


Fig. 4.4 Roaming

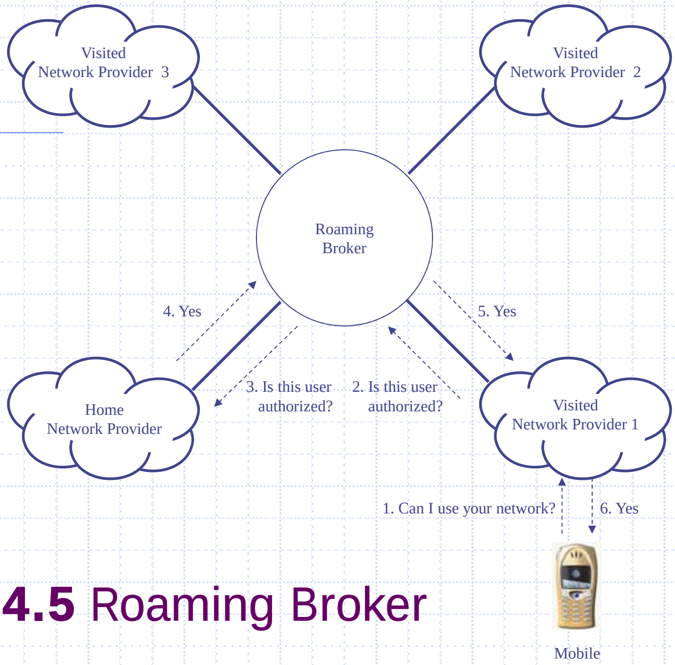
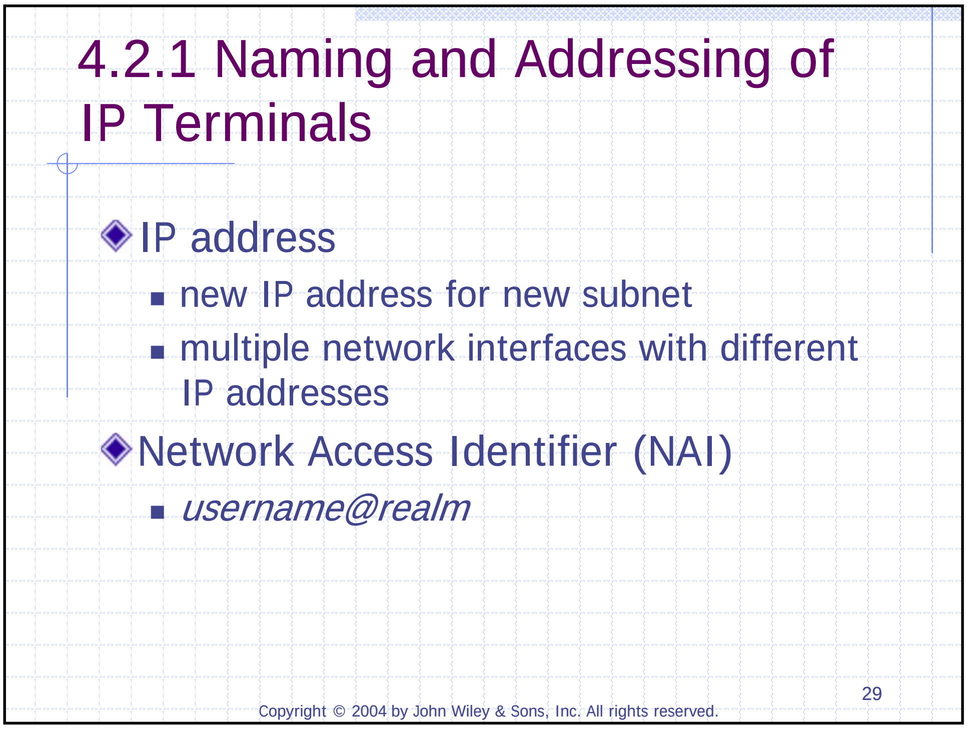


Fig. 4.5 Roaming Broker

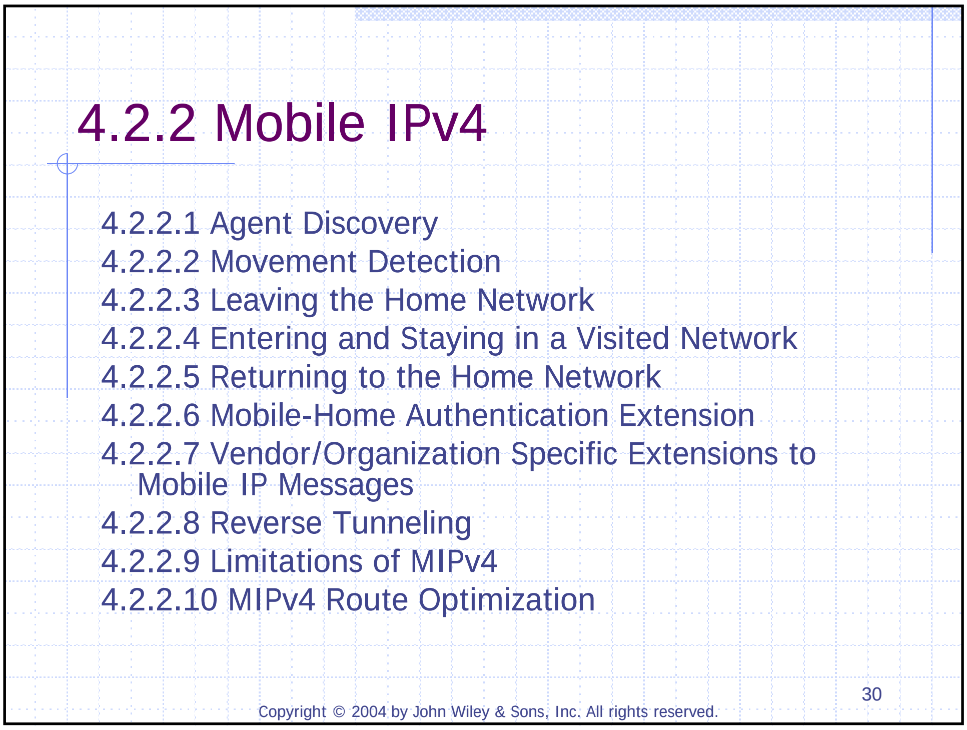
4.2 Mobility Management in IP Networks

- 4.2.1 Naming and Addressing of IP Terminals
- 4.2.2 Mobile IPv4
- 4.2.3 MIPv4 Regional Registration
- 4.2.4 Paging Extensions to Mobile IPv4
- 4.2.5 Mobile IPv6
- 4.2.6 SIP-based Mobility Management
- 4.2.7 Cellular IP
- 4.2.8 HAWAII



4.2.1 Naming and Addressing of IP Terminals

- IP address
  - new IP address for new subnet
  - multiple network interfaces with different IP addresses
- Network Access Identifier (NAI)
  - *username@realm*



4.2.2 Mobile IPv4

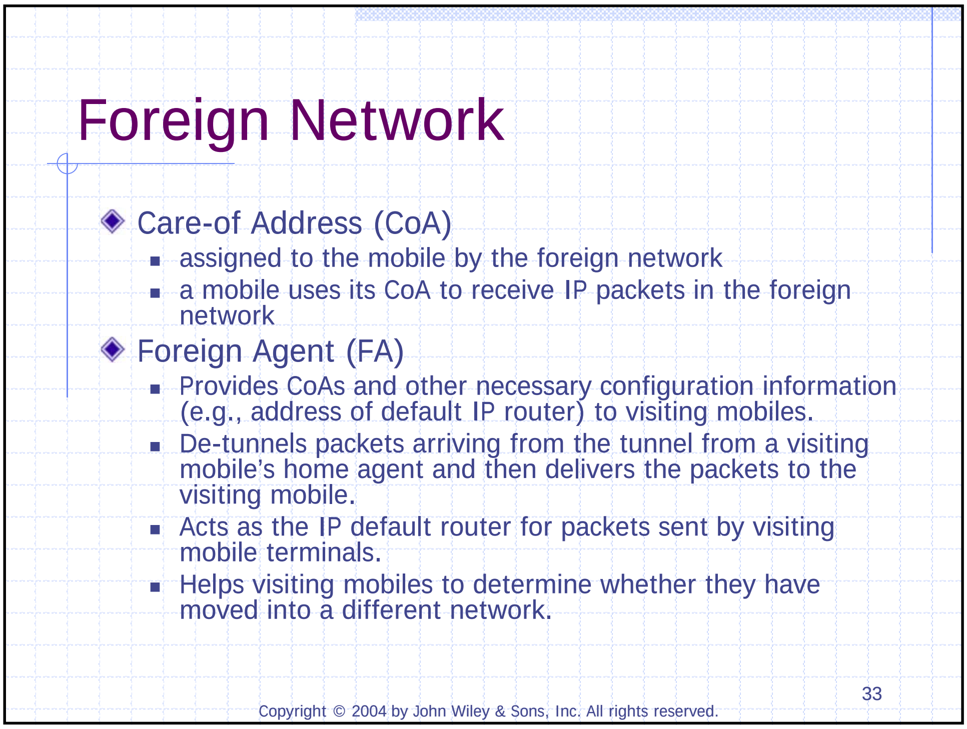
4.2.2.1 Agent Discovery
4.2.2.2 Movement Detection
4.2.2.3 Leaving the Home Network
4.2.2.4 Entering and Staying in a Visited Network
4.2.2.5 Returning to the Home Network
4.2.2.6 Mobile-Home Authentication Extension
4.2.2.7 Vendor/Organization Specific Extensions to Mobile IP Messages
4.2.2.8 Reverse Tunneling
4.2.2.9 Limitations of MIPv4
4.2.2.10 MIPv4 Route Optimization

Mobility Issues in IP Networks

- Once a mobile terminal moves to a new subnet
  - A correspondent node needs to use the mobile’s new IP address
    - It is difficult to force every possible correspondent node to keep track when a mobile terminal may change its IP address and what the mobile’s new address will be.
  - Changing IP address will cause on-going TCP sessions to break
    - Ensure on-going TCP connection does not break
    - Restore quickly if TCP connection breaks

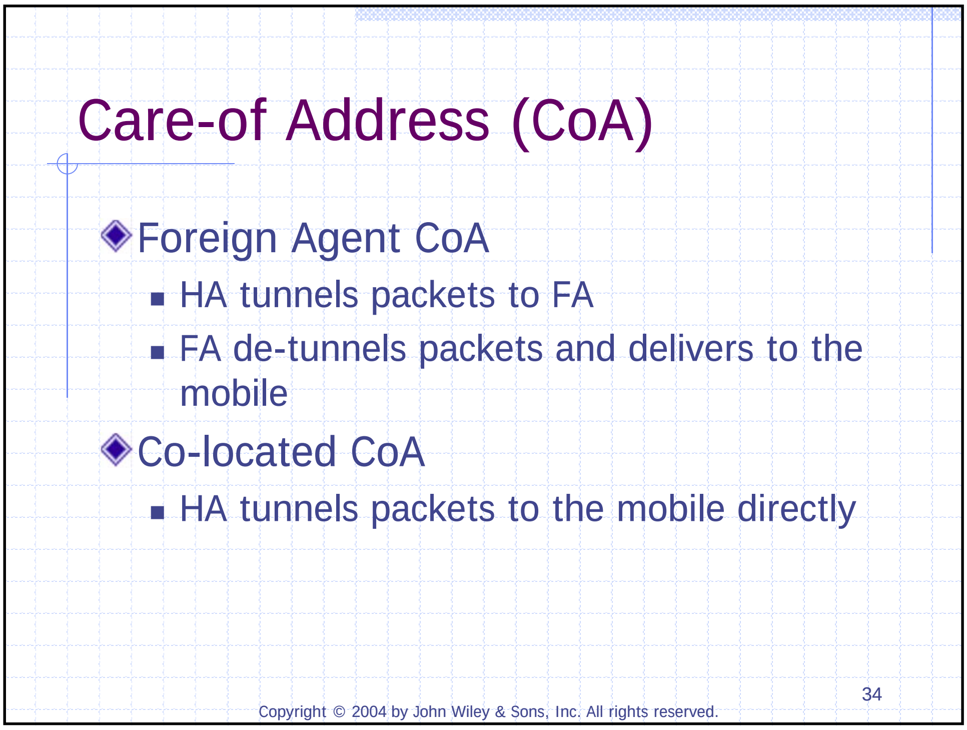
Home Network

- Home address: a globally unique and routable IP address
  - preconfigured or dynamically assigned
- Home network: the network whose network address prefix matches that of the mobile terminal’s home address
- Home agent (HA)
  - maintain up-to-date location information for the mobile
  - intercept packets addressed to the mobile’s home address
  - *tunnel* packets to the mobile’s current location



Foreign Network

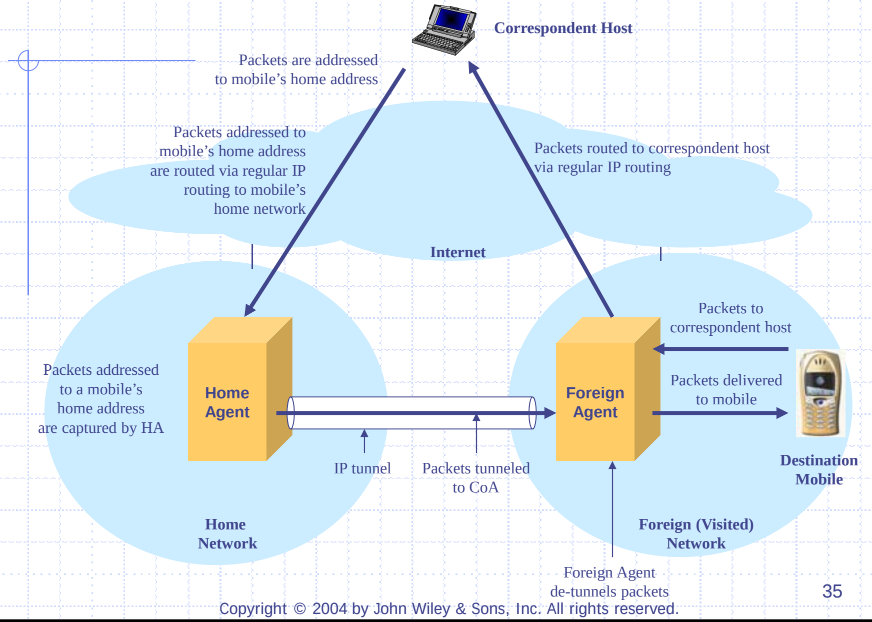
- Care-of Address (CoA)
  - assigned to the mobile by the foreign network
  - a mobile uses its CoA to receive IP packets in the foreign network
- Foreign Agent (FA)
  - Provides CoAs and other necessary configuration information (e.g., address of default IP router) to visiting mobiles.
  - De-tunnels packets arriving from the tunnel from a visiting mobile's home agent and then delivers the packets to the visiting mobile.
  - Acts as the IP default router for packets sent by visiting mobile terminals.
  - Helps visiting mobiles to determine whether they have moved into a different network.



Care-of Address (CoA)

- Foreign Agent CoA
  - HA tunnels packets to FA
  - FA de-tunnels packets and delivers to the mobile
- Co-located CoA
  - HA tunnels packets to the mobile directly

Fig. 4.6 Packet flows between a correspondent host and a mobile: mobile uses FA CoA



Correspondent Host

Packets are addressed to mobile's home address

Packets addressed to mobile's home address are routed via regular IP routing to mobile's home network

Packets routed to correspondent host via regular IP routing

Internet

Packets to correspondent host

Packets delivered to mobile

Packets addressed to a mobile's home address are captured by HA

IP tunnel

Packets tunneled to CoA

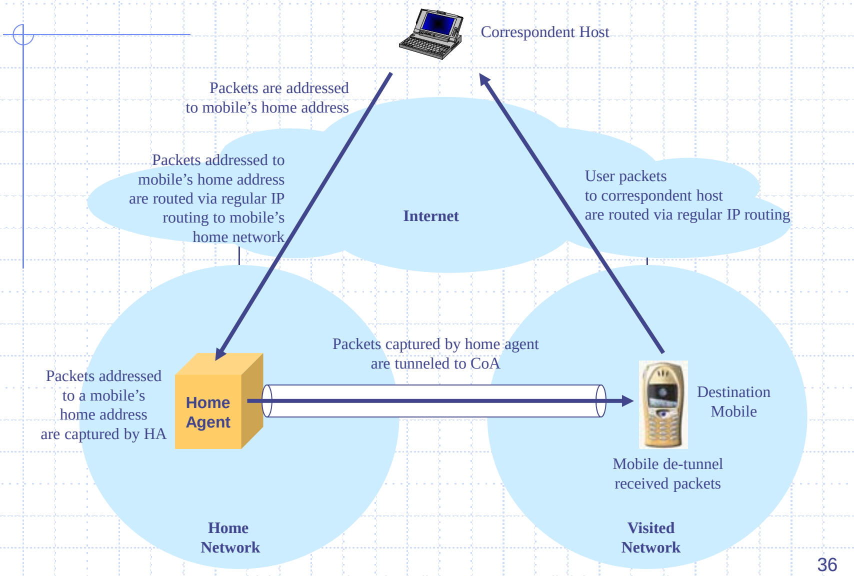
Destination Mobile

Home Network

Foreign (Visited) Network

Foreign Agent de-tunnels packets

Fig. 4.7 Packet flows between a correspondent host and a mobile: mobile uses co-located CoA



Correspondent Host

Packets are addressed to mobile's home address

Packets addressed to mobile's home address are routed via regular IP routing to mobile's home network

Internet

User packets to correspondent host are routed via regular IP routing

Packets captured by home agent are tunneled to CoA

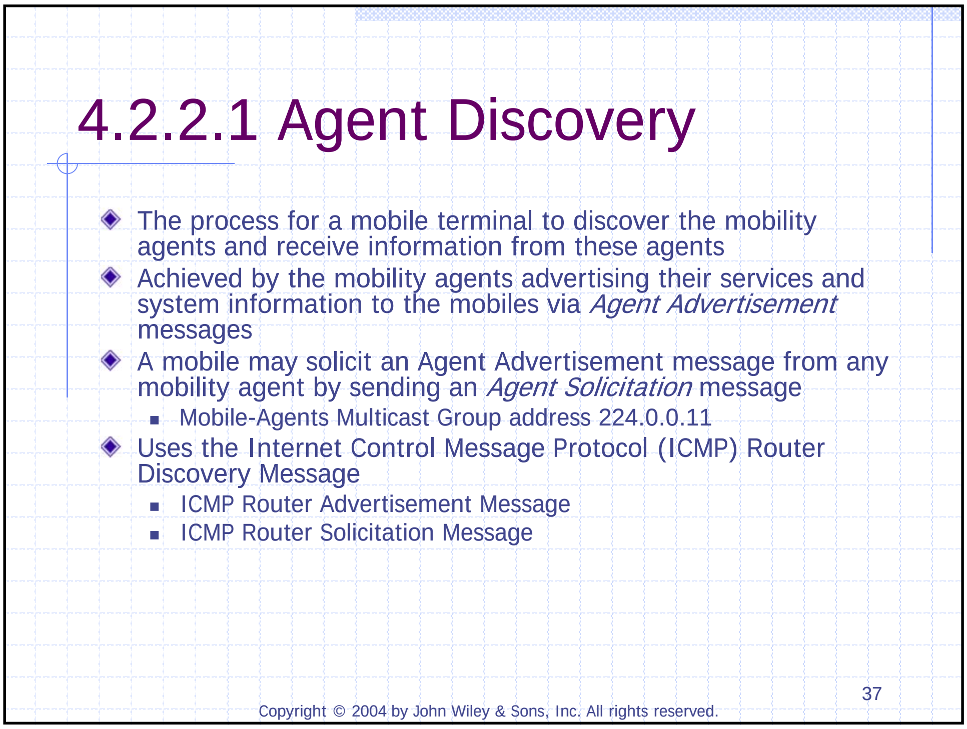
Packets addressed to a mobile's home address are captured by HA

Destination Mobile

Mobile de-tunnel received packets

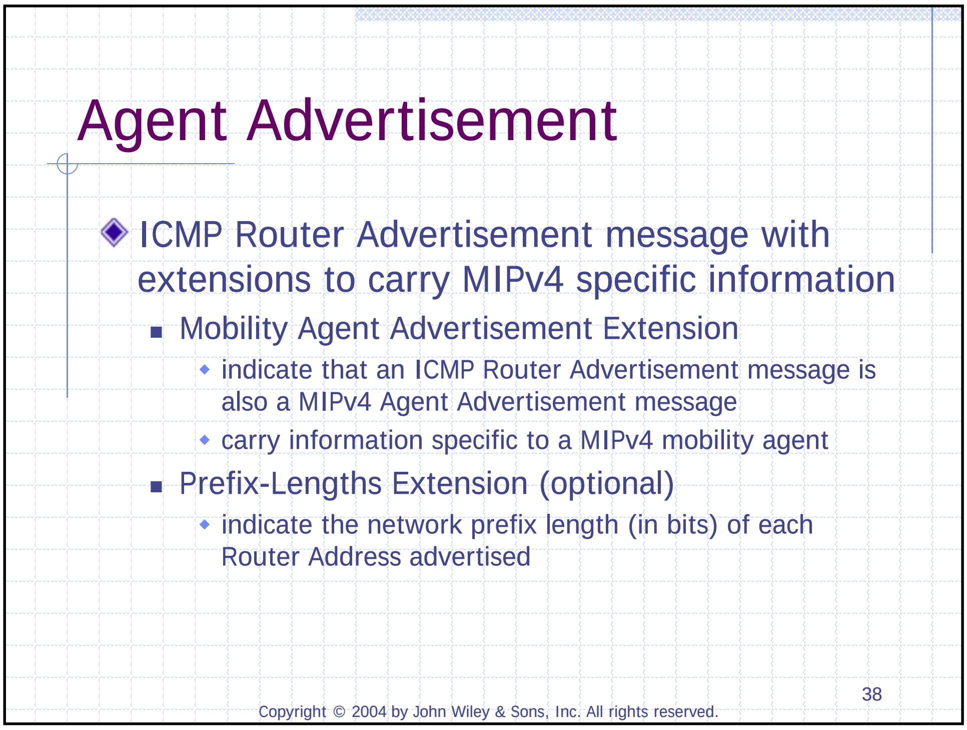
Home Network

Visited Network



4.2.2.1 Agent Discovery

- The process for a mobile terminal to discover the mobility agents and receive information from these agents
- Achieved by the mobility agents advertising their services and system information to the mobiles via *Agent Advertisement* messages
- A mobile may solicit an Agent Advertisement message from any mobility agent by sending an *Agent Solicitation* message
  - Mobile-Agents Multicast Group address 224.0.0.11
- Uses the Internet Control Message Protocol (ICMP) Router Discovery Message
  - ICMP Router Advertisement Message
  - ICMP Router Solicitation Message



Agent Advertisement

- ICMP Router Advertisement message with extensions to carry MIPv4 specific information
  - Mobility Agent Advertisement Extension
    - indicate that an ICMP Router Advertisement message is also a MIPv4 Agent Advertisement message
    - carry information specific to a MIPv4 mobility agent
  - Prefix-Lengths Extension (optional)
    - indicate the network prefix length (in bits) of each Router Address advertised

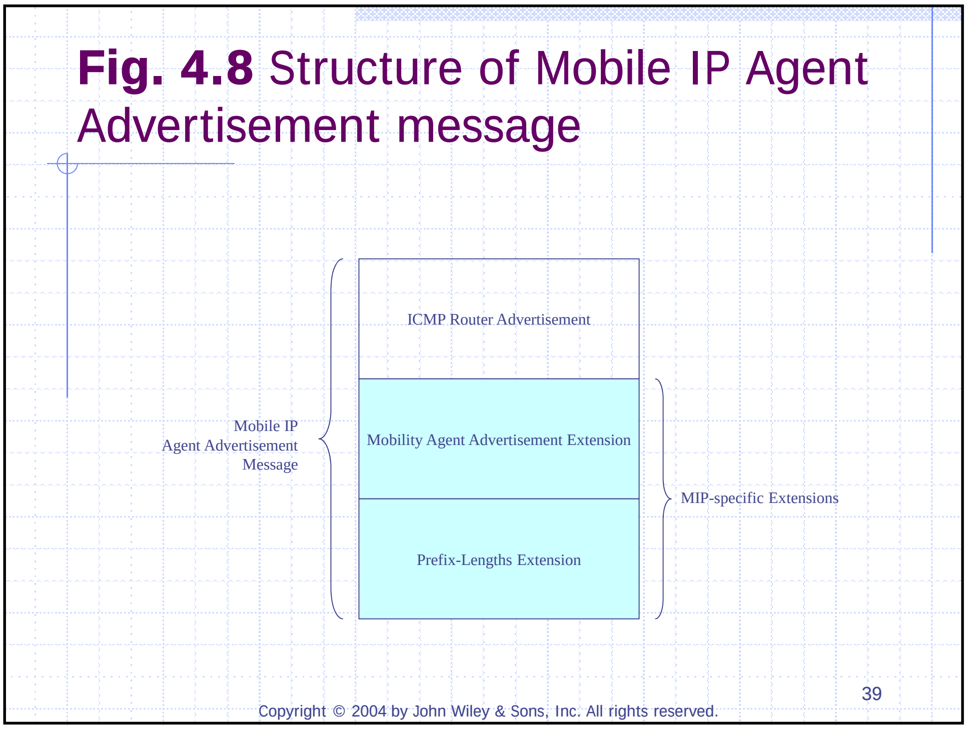
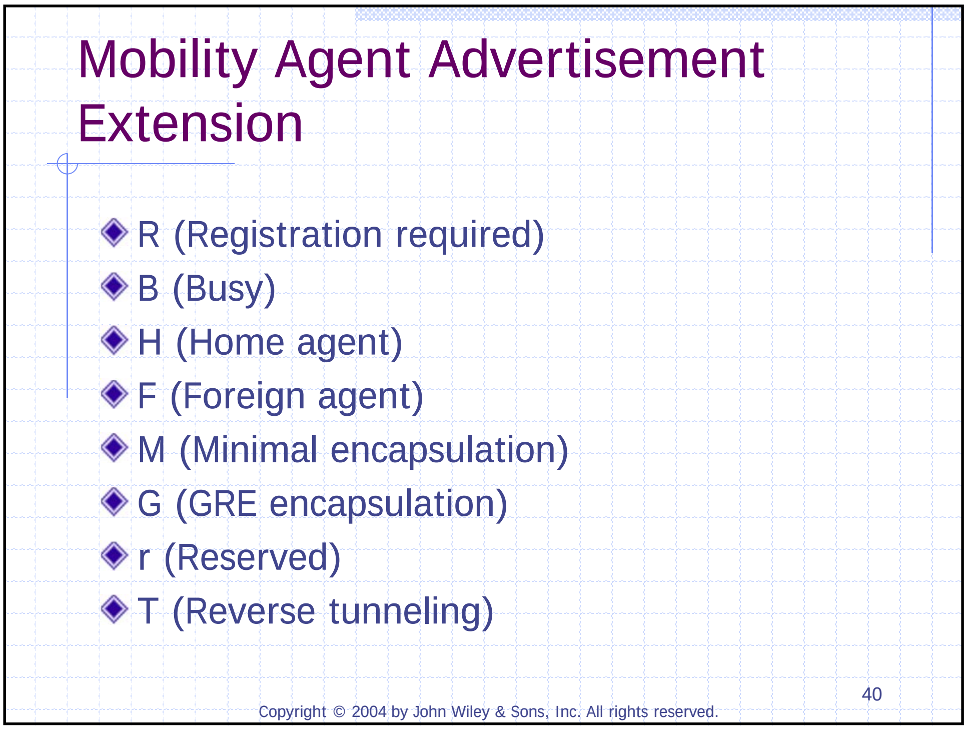


Fig. 4.8 Structure of Mobile IP Agent Advertisement message

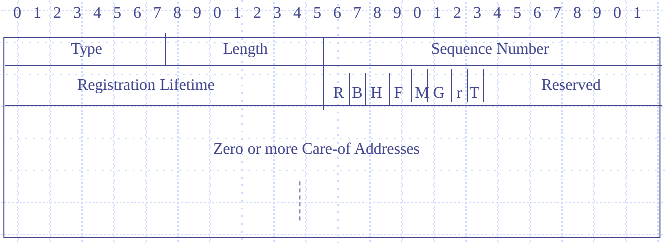
ICMP Router Advertisement
Mobility Agent Advertisement Extension
Prefix-Lengths Extension
Mobile IP Agent Advertisement Message
MIP-specific Extensions



Mobility Agent Advertisement Extension

- R (Registration required)
- B (Busy)
- H (Home agent)
- F (Foreign agent)
- M (Minimal encapsulation)
- G (GRE encapsulation)
- r (Reserved)
- T (Reverse tunneling)

Fig. 4.9 MIPv4 Mobility Agent Advertisement Extension to ICMP Router Advertisement message



0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type

Length

Sequence Number

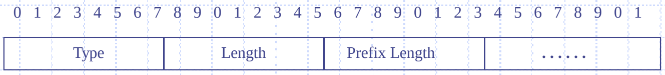
Registration Lifetime

R B H F M G r T

Reserved

Zero or more Care-of Addresses

Fig. 4.10 MIPv4 Prefix-Length Extension to ICMP Router Advertisement message



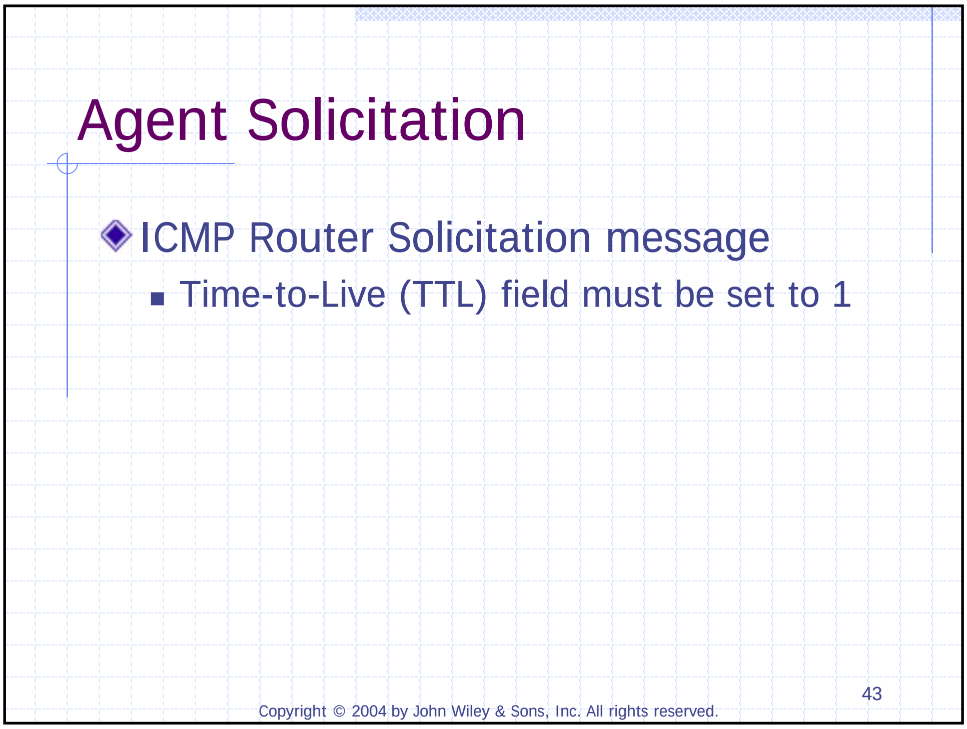
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type

Length

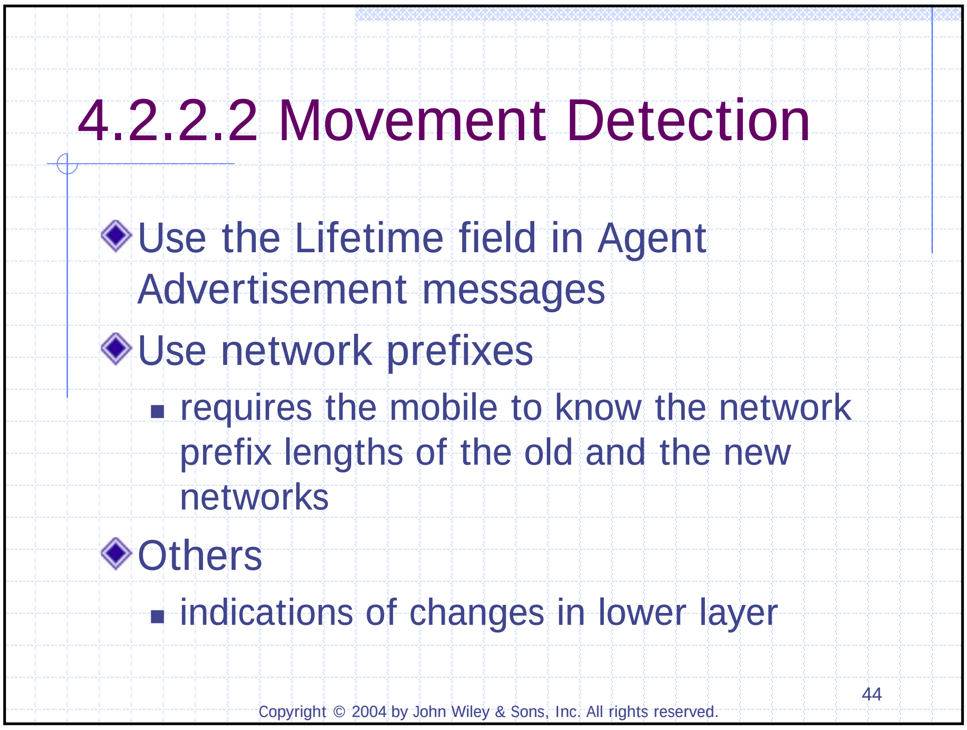
Prefix Length

……



Agent Solicitation

- ICMP Router Solicitation message
  - Time-to-Live (TTL) field must be set to 1



4.2.2.2 Movement Detection

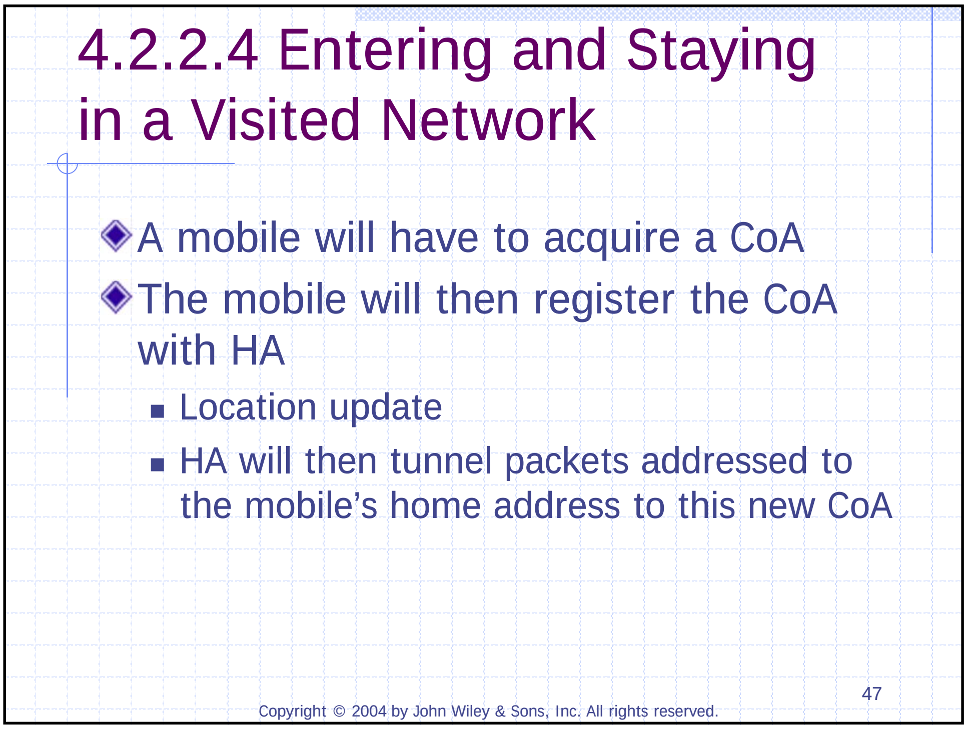
- Use the Lifetime field in Agent Advertisement messages
- Use network prefixes
  - requires the mobile to know the network prefix lengths of the old and the new networks
- Others
  - indications of changes in lower layer

4.2.2.3 Leaving the Home Network

- ARP (Address Resolution Protocol) REQUEST
  - Sender Protocol Address
  - Target Protocol Address
  - Sender Hardware Address
- ARP REPLY
- ARP Cache

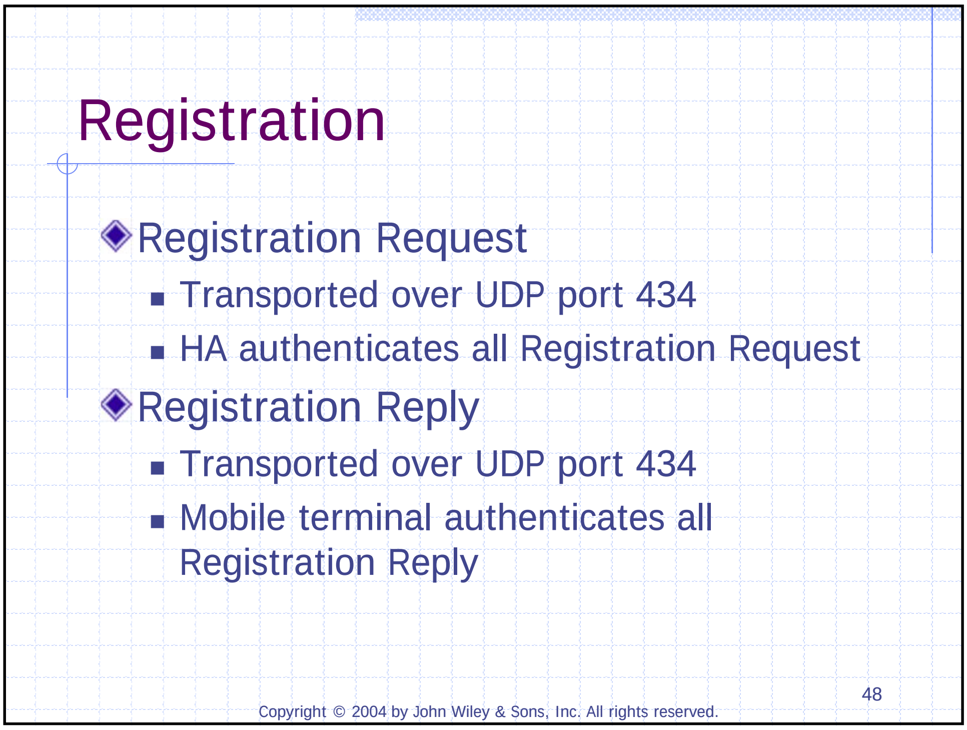
ARP in MIPv4

- Gratuitous ARP
  - A mobile broadcasts a Gratuitous APR before leaving home network.
  - Any node that receives such a Gratuitous ARP packet will update its ARP cache to map the sending mobile’s home address to the home agent’s hardware address.
- Proxy ARP
  - Mobile’s home agent will reply to ARP REQUEST on behalf of the mobile.



4.2.2.4 Entering and Staying in a Visited Network

- A mobile will have to acquire a CoA
- The mobile will then register the CoA with HA
  - Location update
  - HA will then tunnel packets addressed to the mobile’s home address to this new CoA



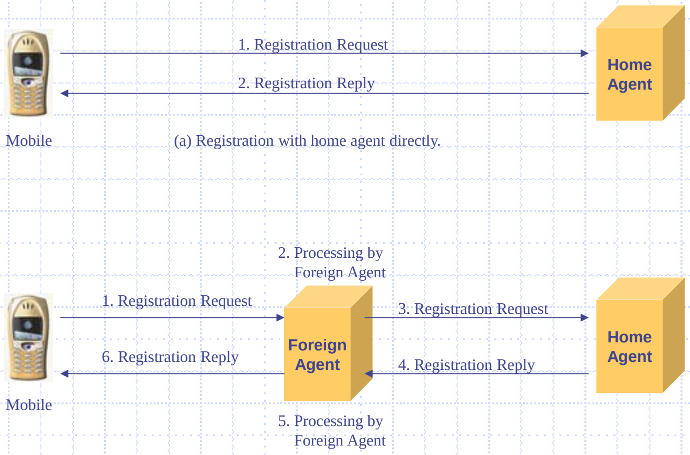
Registration

- Registration Request
  - Transported over UDP port 434
  - HA authenticates all Registration Request
- Registration Reply
  - Transported over UDP port 434
  - Mobile terminal authenticates all Registration Reply

FA CoA vs. Co-located CoA

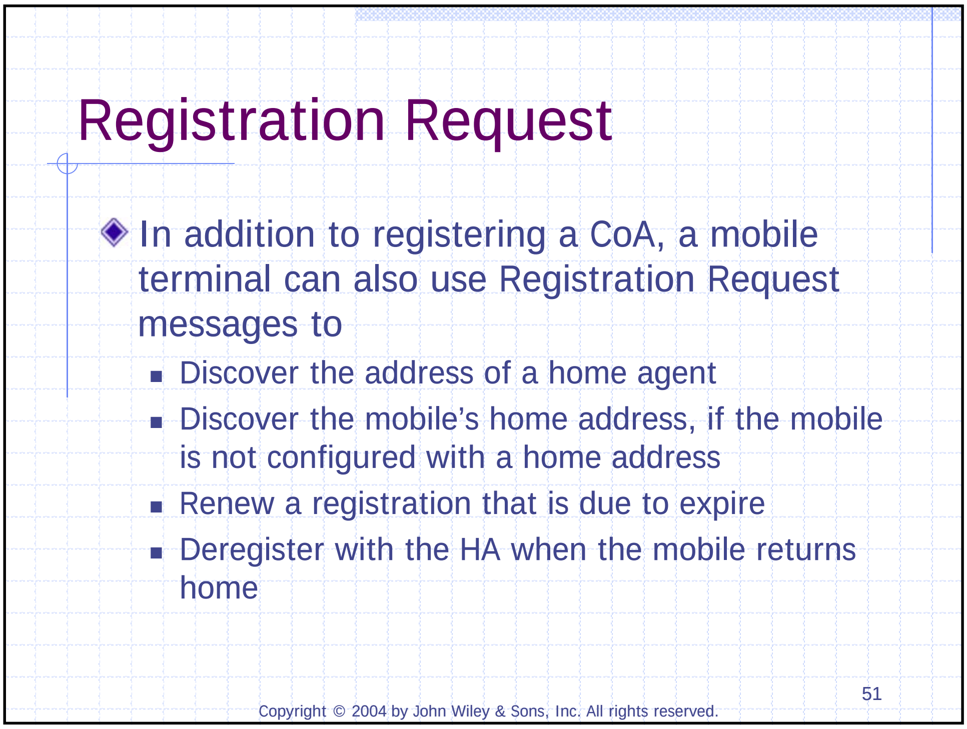
- FA CoA
  - Registration must be done via the FA
  - If FA wants to deny network access
    - discard the Registration Request
    - generate a Registration Reply to the mobile
- Co-located CoA
  - Registration may be done directly with the HA, unless the FA requires registration via the FA.
    - The FA can force a mobile to register through the FA by setting the ‘R’ flag in the Agent Advertisement it sends to the mobiles.

Fig. 4.11 MIPv4 registration message flows



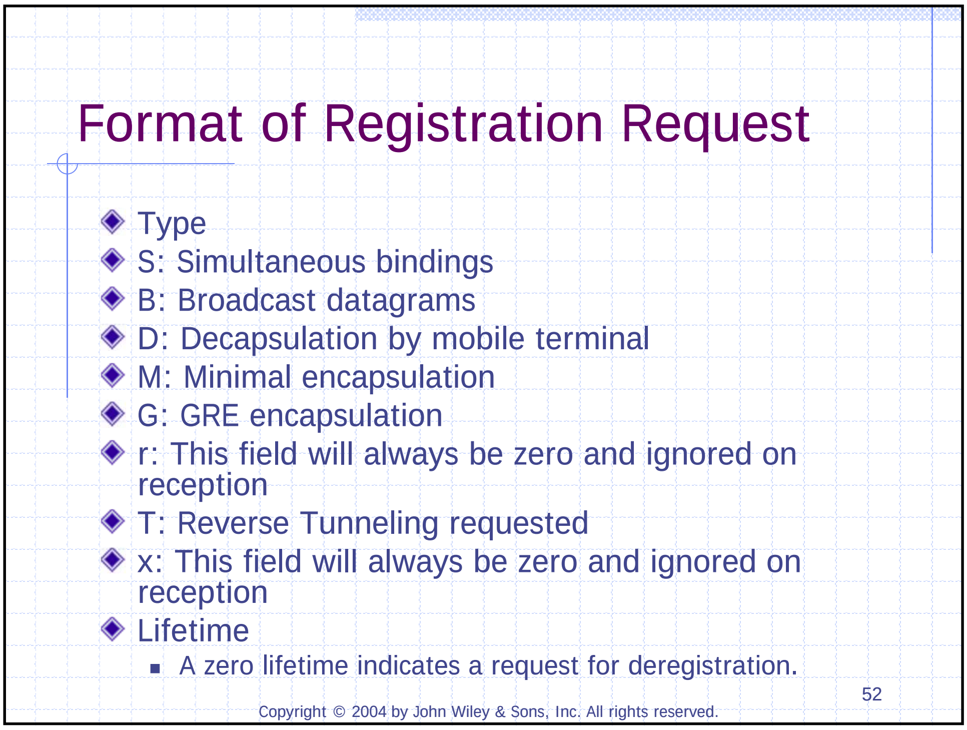
(a) Registration with home agent directly.

(b) Registration through foreign agent



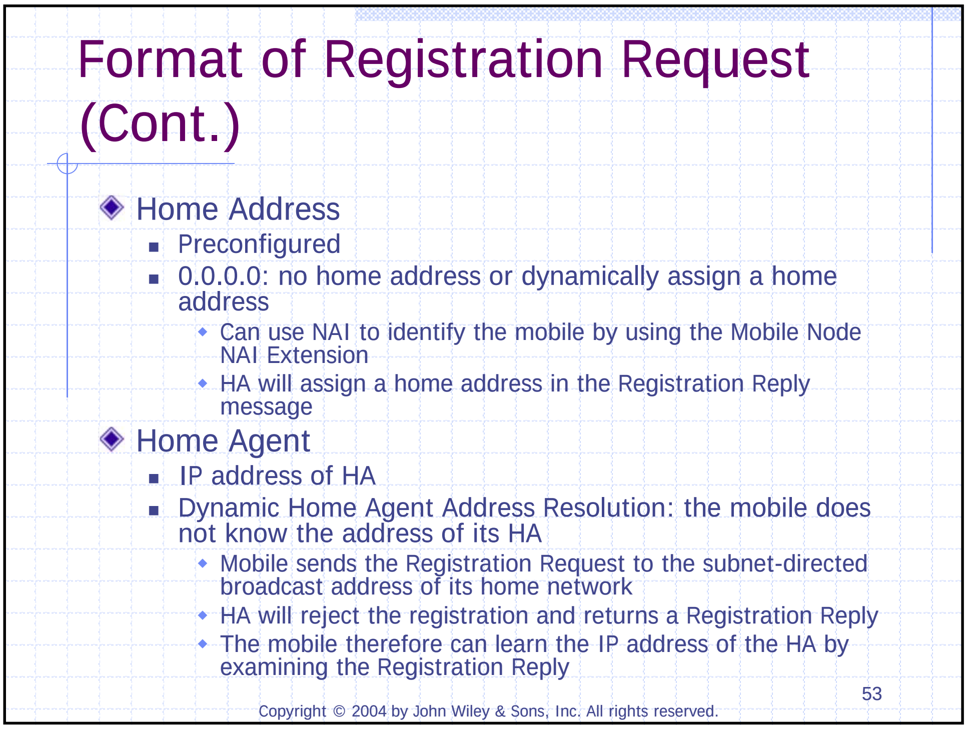
Registration Request

- In addition to registering a CoA, a mobile terminal can also use Registration Request messages to
  - Discover the address of a home agent
  - Discover the mobile's home address, if the mobile is not configured with a home address
  - Renew a registration that is due to expire
  - Deregister with the HA when the mobile returns home



Format of Registration Request

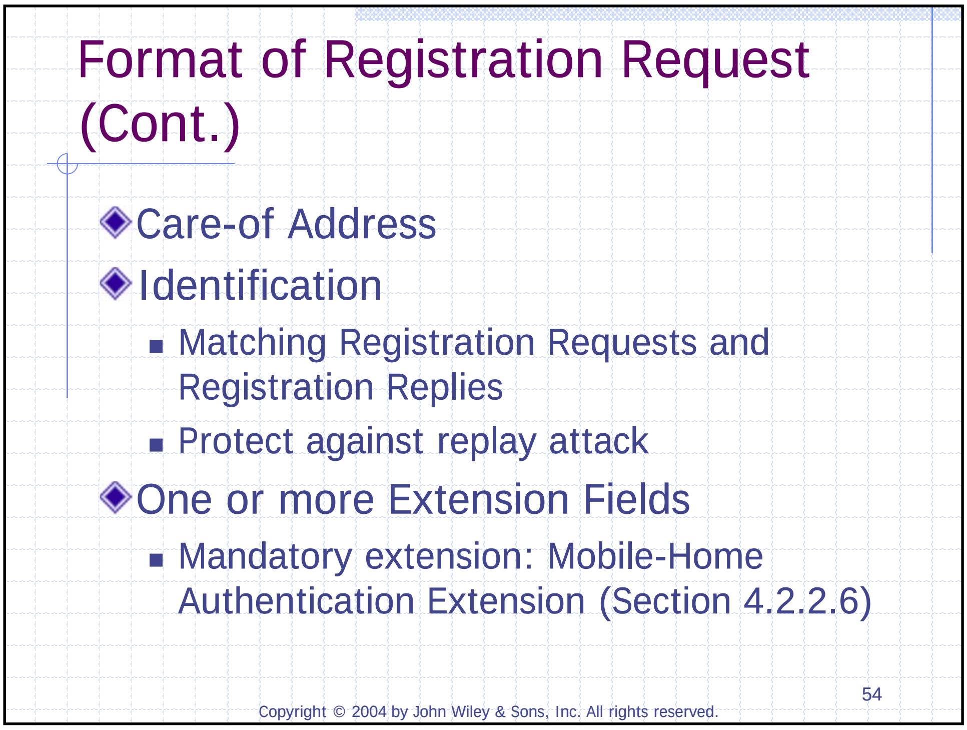
- Type
- S: Simultaneous bindings
- B: Broadcast datagrams
- D: Decapsulation by mobile terminal
- M: Minimal encapsulation
- G: GRE encapsulation
- r: This field will always be zero and ignored on reception
- T: Reverse Tunneling requested
- x: This field will always be zero and ignored on reception
- Lifetime
  - A zero lifetime indicates a request for deregistration.



Format of Registration Request (Cont.)

- Home Address
  - Preconfigured
  - 0.0.0.0: no home address or dynamically assign a home address
    - Can use NAI to identify the mobile by using the Mobile Node NAI Extension
    - HA will assign a home address in the Registration Reply message
- Home Agent
  - IP address of HA
  - Dynamic Home Agent Address Resolution: the mobile does not know the address of its HA
    - Mobile sends the Registration Request to the subnet-directed broadcast address of its home network
    - HA will reject the registration and returns a Registration Reply
    - The mobile therefore can learn the IP address of the HA by examining the Registration Reply

53



Format of Registration Request (Cont.)

- Care-of Address
- Identification
  - Matching Registration Requests and Registration Replies
  - Protect against replay attack
- One or more Extension Fields
  - Mandatory extension: Mobile-Home Authentication Extension (Section 4.2.2.6)

54

Fig. 4.12 MIPv4 Registration Request message format

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type	S	B	D	M	G	r	T	x	Life Time
Home Address									
Home Agent									
Care-of Address									
Identification									
Extension Field									
⋮									
Extension Field									

Registration Reply

- Code: a value indicating the result of the corresponding Registration Request
- Lifetime
  - Successful registration: the number of seconds remaining before the registration is considered expired
    - zero: indicate that the mobile terminal has been deregistered
  - Failed registration: this field should be ignored

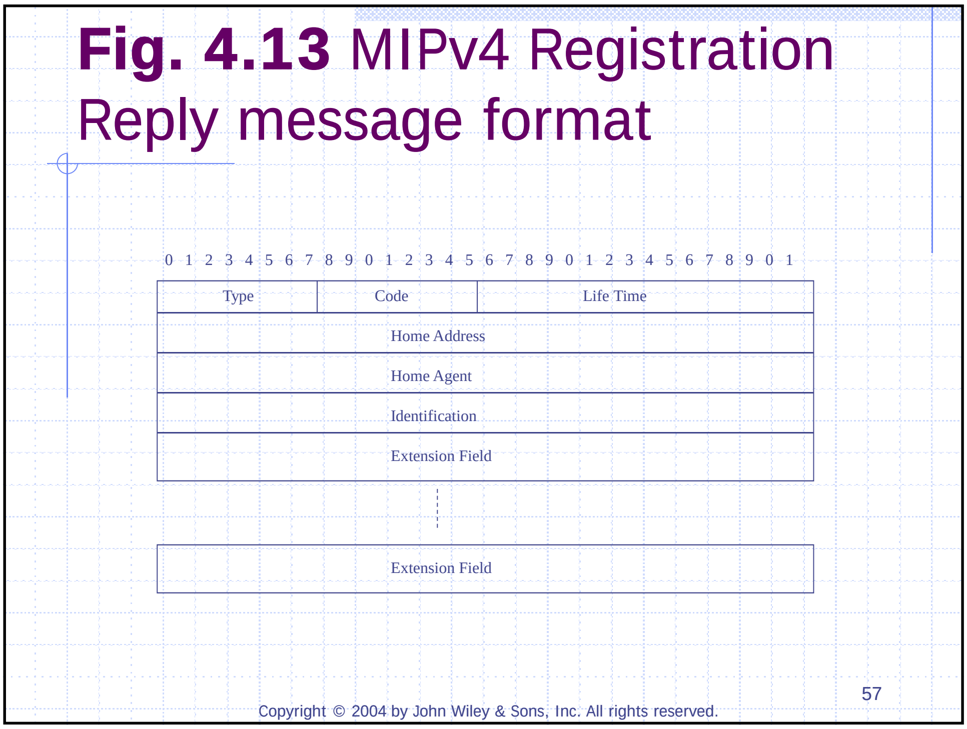
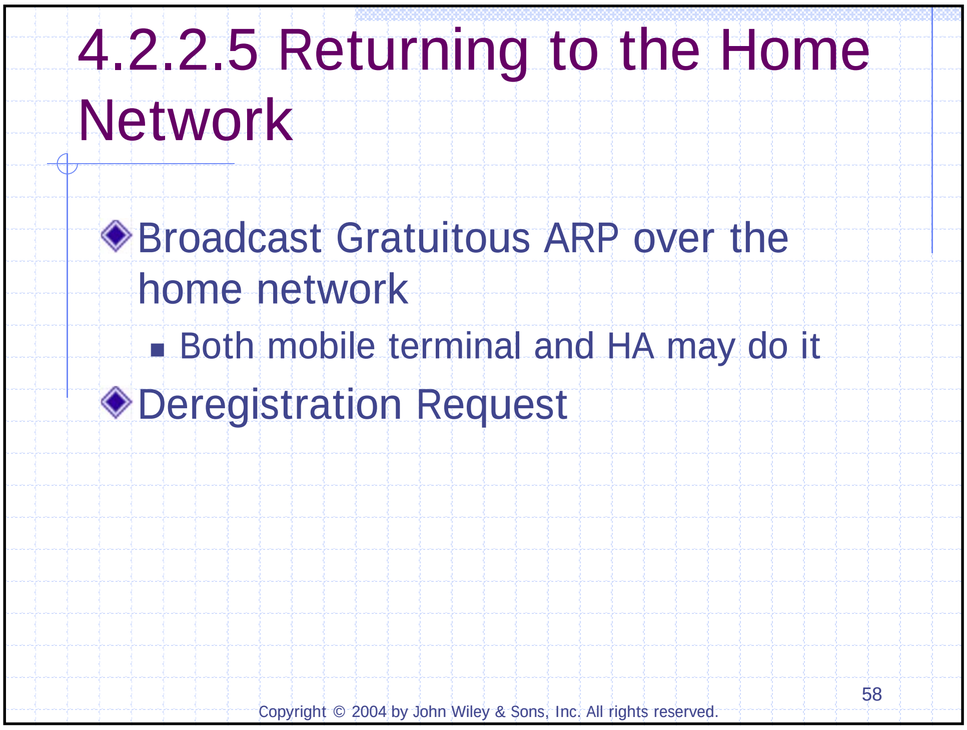


Fig. 4.13 MIPv4 Registration Reply message format

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type	Code	Life Time
Home Address		
Home Agent		
Identification		
Extension Field		
⋮		
Extension Field		



4.2.2.5 Returning to the Home Network

- Broadcast Gratuitous ARP over the home network
  - Both mobile terminal and HA may do it
- Deregistration Request

4.2.2.6 Mobile-Home Authentication Extension

- Security Parameter Index (SPI)
  - a 4-octet identifier used to identify a security context between a mobile and its home agent
- Authenticator
  - a number calculated by applying an authentication algorithm on the message that needs to be protected
  - HMAC-MD5: default authentication algorithm

Fig. 4.14 Mobile-Home Authentication Extensions to Mobile IP messages

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type	Length	Security Parameter Index (SPI)
SPI (continued)		Authenticator . . . . . .

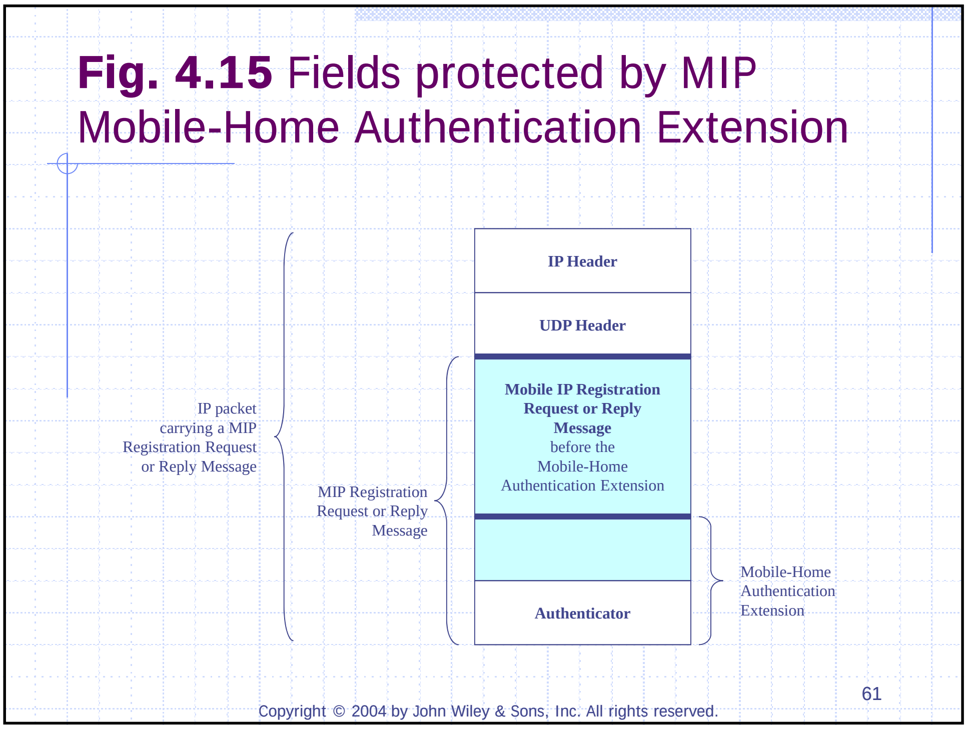


Fig. 4.15 Fields protected by MIP Mobile-Home Authentication Extension

IP Header

UDP Header

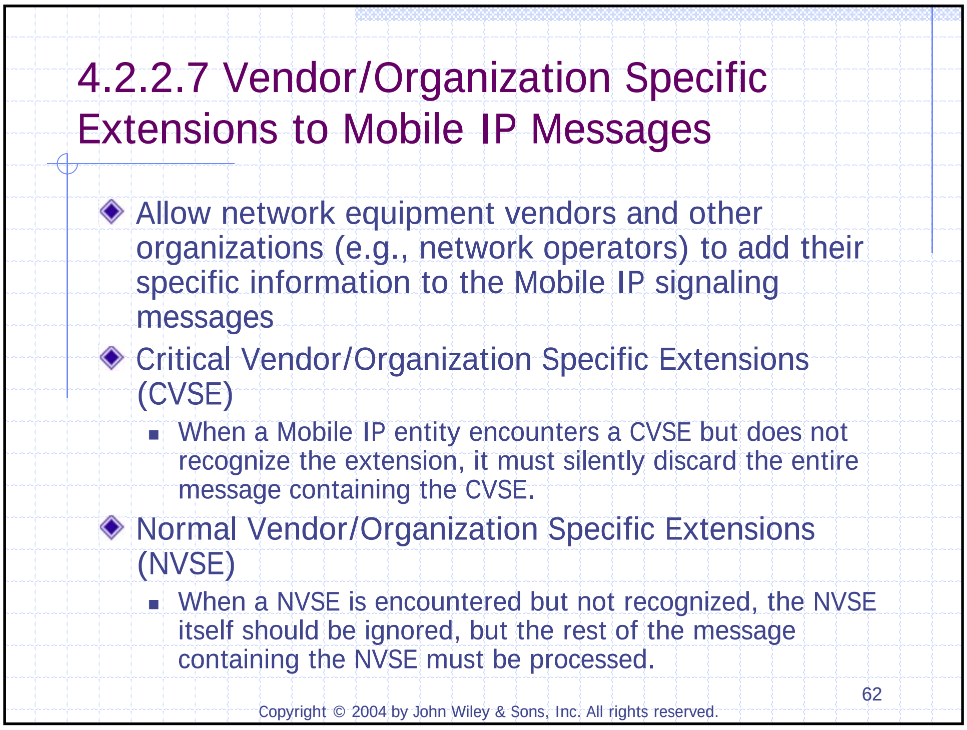
Mobile IP Registration Request or Reply Message before the Mobile-Home Authentication Extension

Authenticator

IP packet carrying a MIP Registration Request or Reply Message

MIP Registration Request or Reply Message

Mobile-Home Authentication Extension



4.2.2.7 Vendor/Organization Specific Extensions to Mobile IP Messages

- Allow network equipment vendors and other organizations (e.g., network operators) to add their specific information to the Mobile IP signaling messages
- Critical Vendor/Organization Specific Extensions (CVSE)
  - When a Mobile IP entity encounters a CVSE but does not recognize the extension, it must silently discard the entire message containing the CVSE.
- Normal Vendor/Organization Specific Extensions (NVSE)
  - When a NVSE is encountered but not recognized, the NVSE itself should be ignored, but the rest of the message containing the NVSE must be processed.

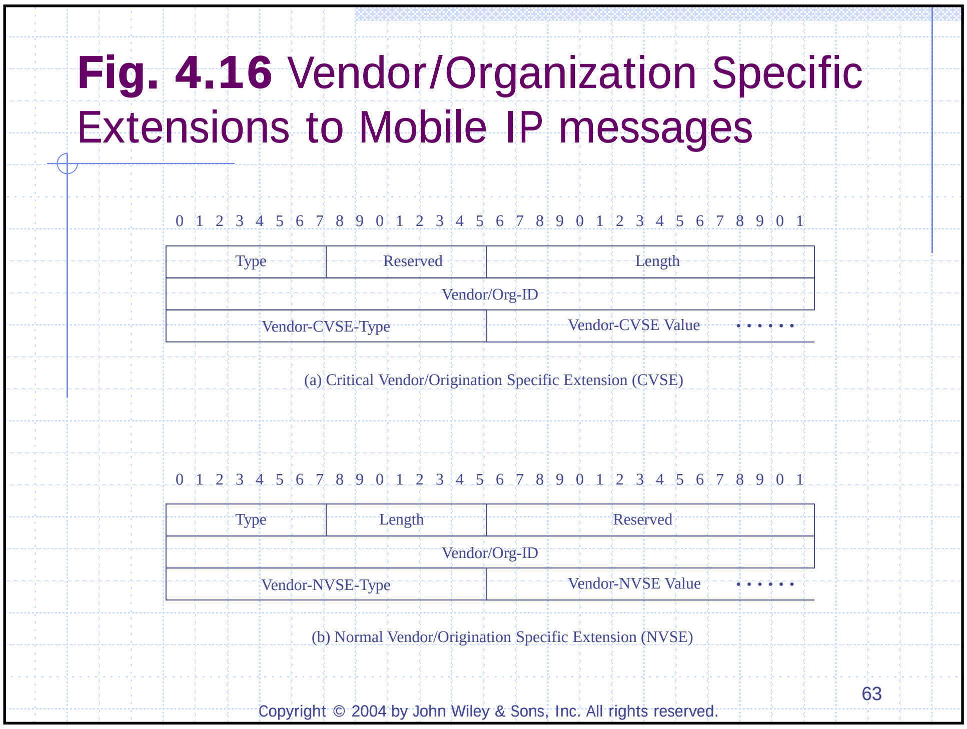


Fig. 4.16 Vendor/Organization Specific Extensions to Mobile IP messages

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

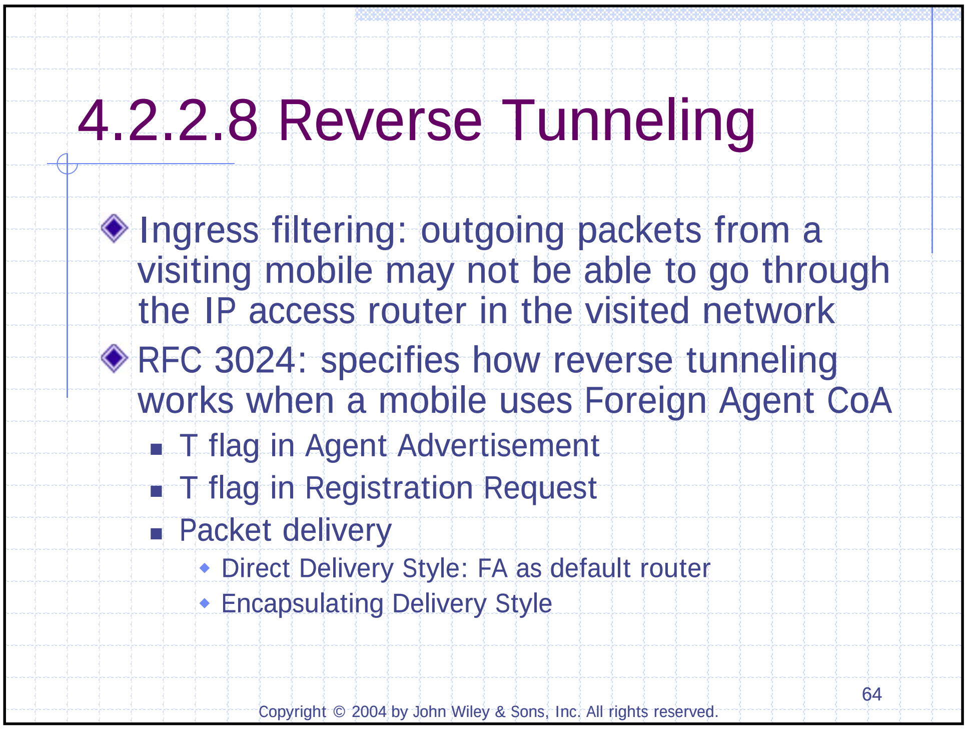
Type	Reserved	Length
Vendor/Org-ID		
Vendor-CVSE-Type		Vendor-CVSE Value · · · · · ·

(a) Critical Vendor/Origination Specific Extension (CVSE)

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type	Length	Reserved
Vendor/Org-ID		
Vendor-NVSE-Type		Vendor-NVSE Value · · · · · ·

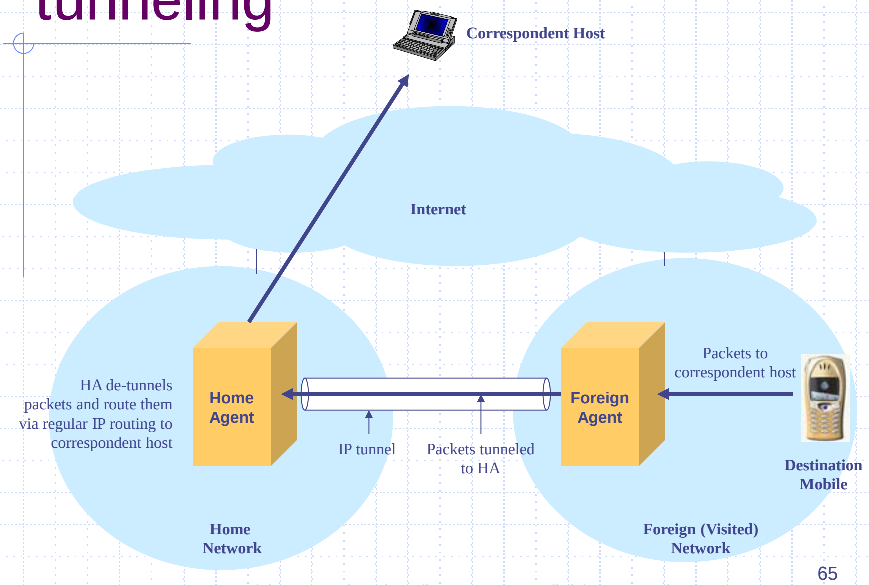
(b) Normal Vendor/Origination Specific Extension (NVSE)



4.2.2.8 Reverse Tunneling

- Ingress filtering: outgoing packets from a visiting mobile may not be able to go through the IP access router in the visited network
- RFC 3024: specifies how reverse tunneling works when a mobile uses Foreign Agent CoA
  - T flag in Agent Advertisement
  - T flag in Registration Request
  - Packet delivery
    - Direct Delivery Style: FA as default router
    - Encapsulating Delivery Style

Fig. 4.17 Mobile IPv4 reverse tunneling


Correspondent Host
Internet
HA de-tunnels packets and route them via regular IP routing to correspondent host
Home Agent
IP tunnel
Packets tunneled to HA
Foreign Agent
Packets to correspondent host
Destination Mobile
Home Network
Foreign (Visited) Network

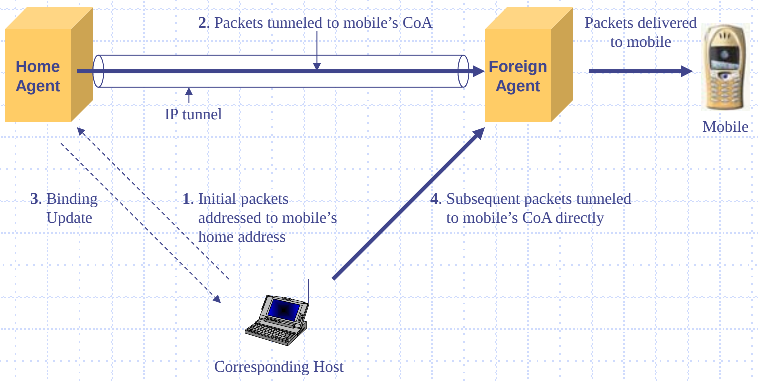
4.2.2.9 Limitations of MIPv4

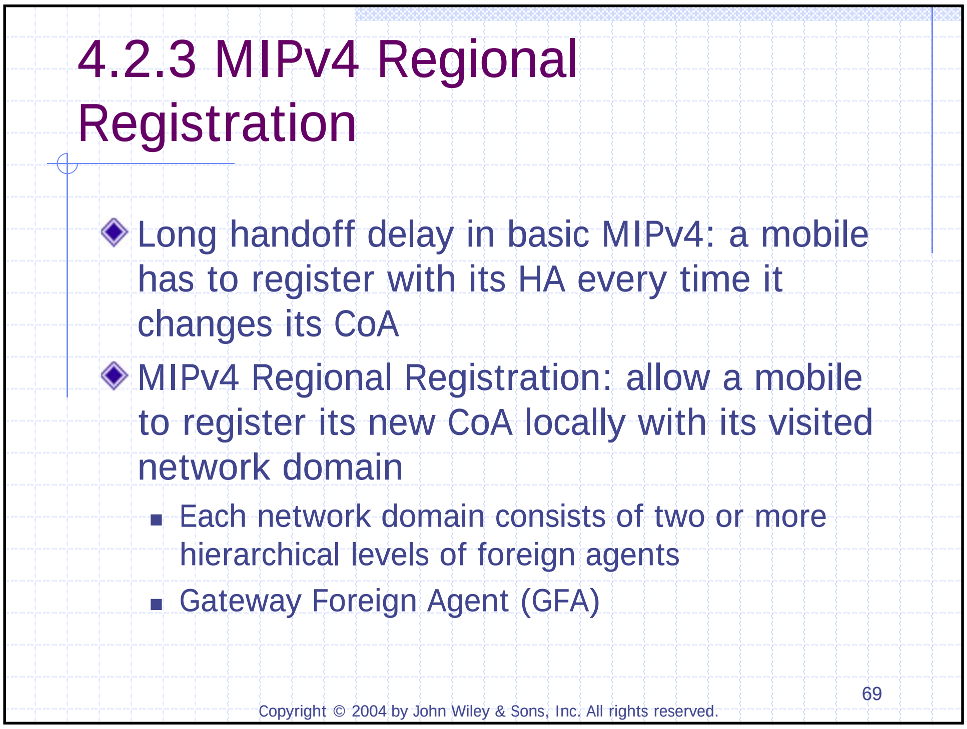
- Triangular routing
  - route optimization in Section 4.2.2.10
- A home agent may become a traffic and performance bottleneck
- Potential long handoff delay
  - micromobility management in Sections 4.2.3, 4.2.7 and 4.2.8
- Potential insufficient deregistration capability
  - registration with the old foreign agent expires only when the registration lifetime expires
- Insufficient capabilities to support other mobility management requirements
  - Paging in Section 4.2.4

4.2.2.10 MIPv4 Route Optimization

- Allow a correspondent node (CN) to be aware of a mobile's current CoA and then tunnel packets to the destination mobile's CoA directly
- Binding Cache: maintained by a CN to map the mobiles' home addresses to their CoAs
- Binding Update: HA informs CN the mobile's current CoA
- A security association between the CN and the HA needs to be established
  - scalability

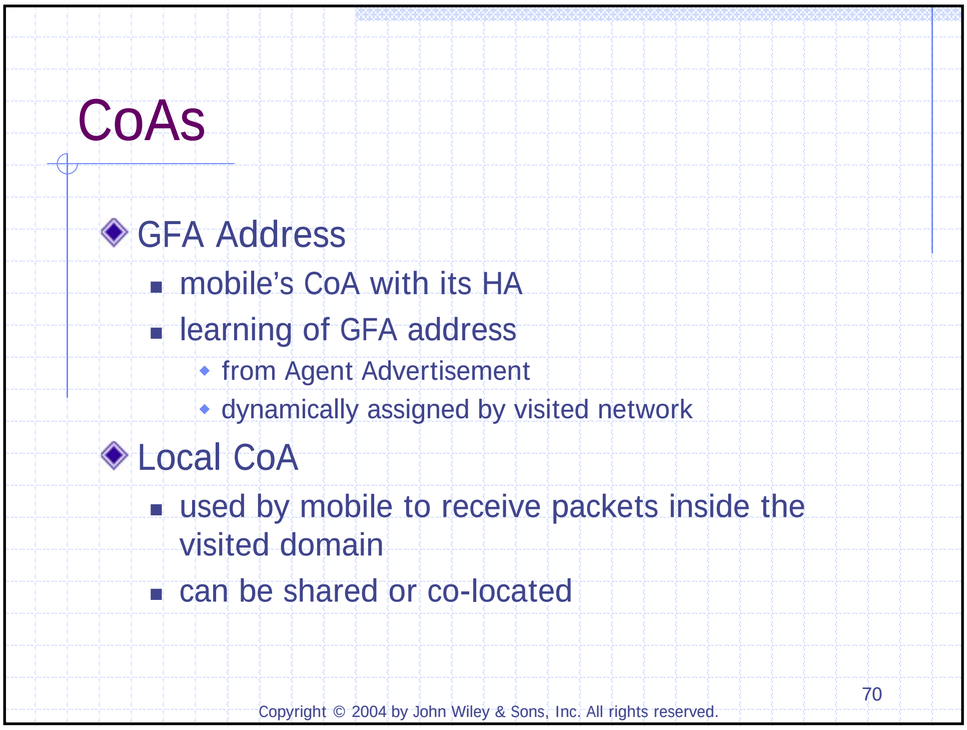
Fig. 4.18 MIPv4 route optimization


Home Agent
2. Packets tunneled to mobile's CoA
Foreign Agent
Packets delivered to mobile
IP tunnel
Mobile
3. Binding Update
1. Initial packets addressed to mobile's home address
4. Subsequent packets tunneled to mobile's CoA directly
Corresponding Host



4.2.3 MIPv4 Regional Registration

- Long handoff delay in basic MIPv4: a mobile has to register with its HA every time it changes its CoA
- MIPv4 Regional Registration: allow a mobile to register its new CoA locally with its visited network domain
  - Each network domain consists of two or more hierarchical levels of foreign agents
  - Gateway Foreign Agent (GFA)



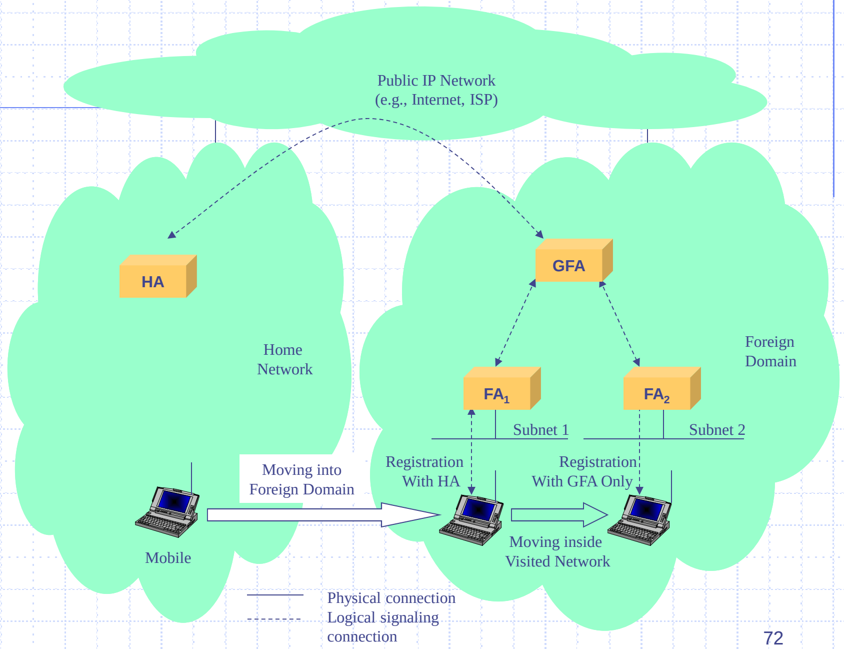
CoAs

- GFA Address
  - mobile's CoA with its HA
  - learning of GFA address
    - from Agent Advertisement
    - dynamically assigned by visited network
- Local CoA
  - used by mobile to receive packets inside the visited domain
  - can be shared or co-located

Registration

- MIP registration: move to a new GFA
- Regional registration: move between FAs connected to a same GFA
  - Regional Registration Request: sent by a mobile to a GFA via the FA to initiate regional registration.
  - Regional Registration Reply: sent by a GFA to a mobile in response to a Regional Registration Request.

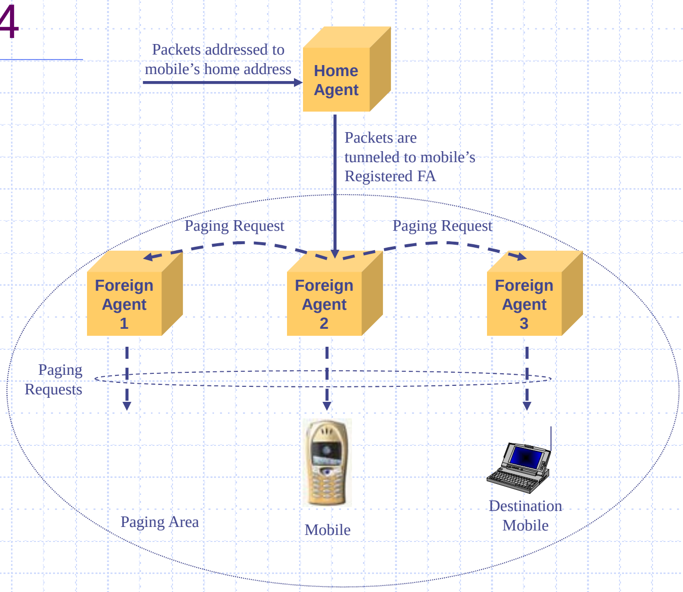
Fig. 4.19 MIPv4 Regional Registration

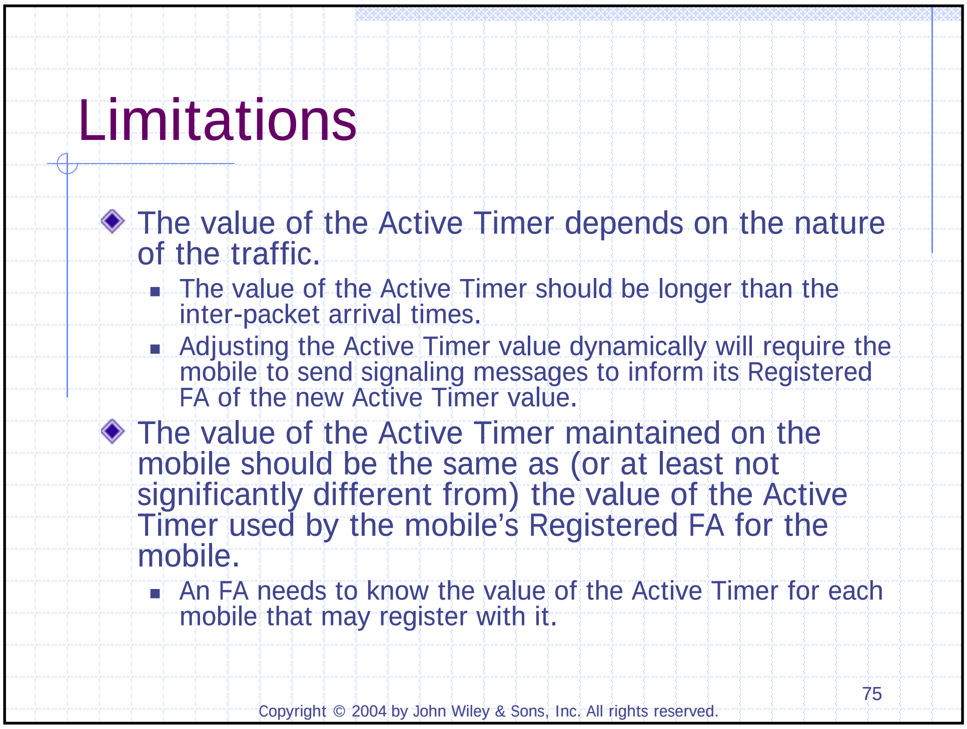


4.2.4 Paging Extensions to Mobile IPv4

- Paging in Mobile IP (P-MIP)
  - Active Timer: determine a mobile is in active or idle state
    - active state: standard MIP
    - idle state: may not perform MIP registration
    - no explicit signaling messages
  - Registered FA
    - the FA through which a mobile performed its last MIP registration
    - responsible for keeping track of whether the mobile is in active or idle state by using Active Timer
    - an FA is required on each IP subnet
  - Paging Area: an idle mobile does not have to perform MIP registration when moving inside the same paging area
    - Paging Area Identifier (PAI): carried by Agent Advertisement
    - A mobile compares the PAIs received from different FAs to determine whether it has moved into a new Paging Area.

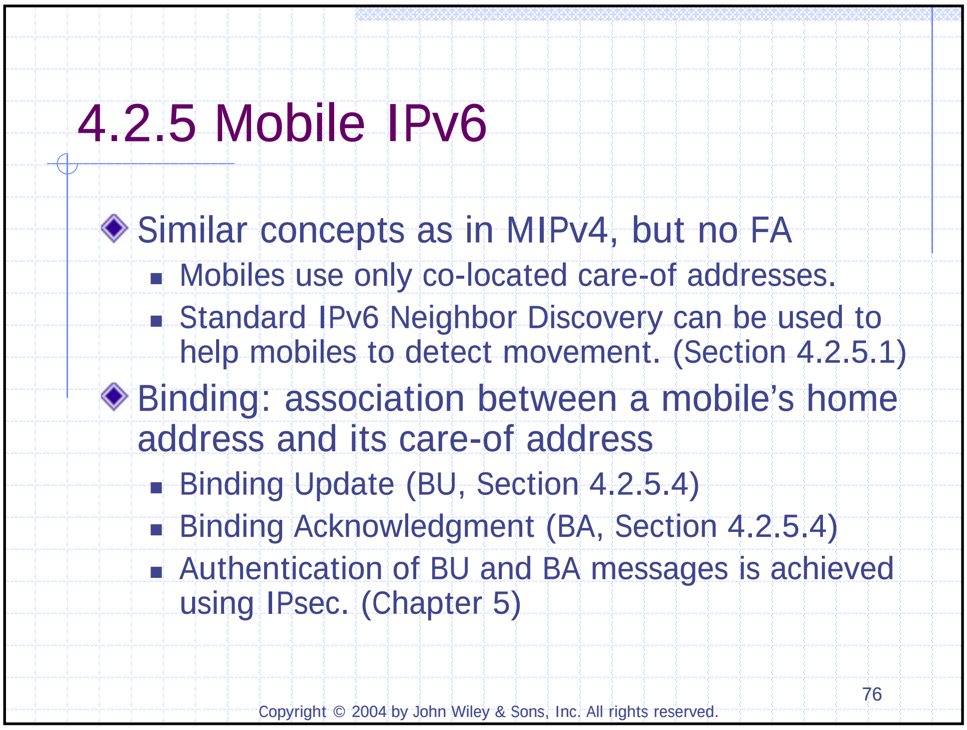
Fig. 4.20 Paging Extensions to Mobile IPv4





Limitations

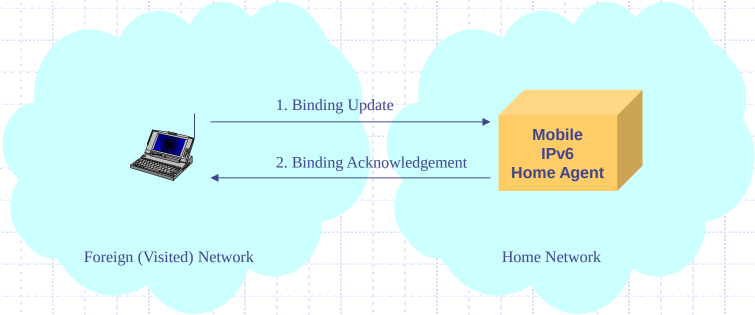
- The value of the Active Timer depends on the nature of the traffic.
  - The value of the Active Timer should be longer than the inter-packet arrival times.
  - Adjusting the Active Timer value dynamically will require the mobile to send signaling messages to inform its Registered FA of the new Active Timer value.
- The value of the Active Timer maintained on the mobile should be the same as (or at least not significantly different from) the value of the Active Timer used by the mobile's Registered FA for the mobile.
  - An FA needs to know the value of the Active Timer for each mobile that may register with it.



4.2.5 Mobile IPv6

- Similar concepts as in MIPv4, but no FA
  - Mobiles use only co-located care-of addresses.
  - Standard IPv6 Neighbor Discovery can be used to help mobiles to detect movement. (Section 4.2.5.1)
- Binding: association between a mobile's home address and its care-of address
  - Binding Update (BU, Section 4.2.5.4)
  - Binding Acknowledgment (BA, Section 4.2.5.4)
  - Authentication of BU and BA messages is achieved using IPsec. (Chapter 5)

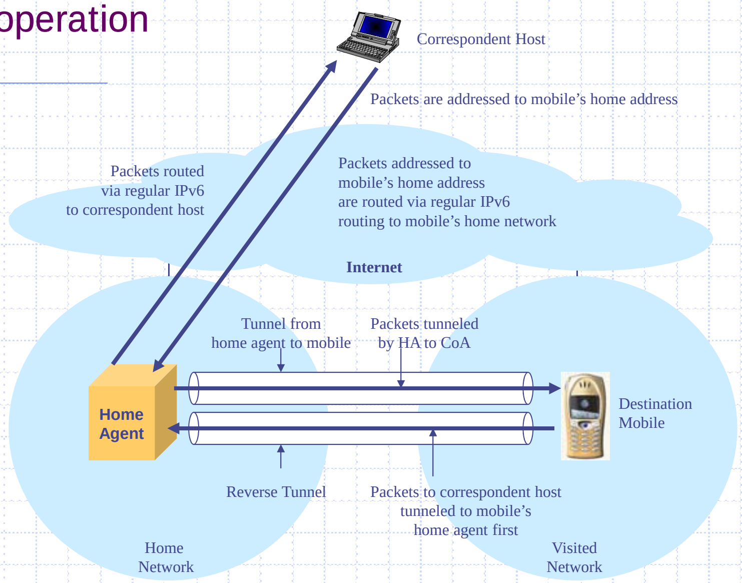
Fig. 4.21 MIPv6 address binding with home agent



Packet Delivery

- Bi-directional tunneling mode
  - A correspondent host does not have to use Mobile IPv6.
- Route optimization mode
  - Route optimization is designed to be an integral part of MIPv6.

Fig. 4.22 MIPv6 bi-directional tunneling mode of operation



Correspondent Host

Packets are addressed to mobile's home address

Packets routed via regular IPv6 to correspondent host

Packets addressed to mobile's home address are routed via regular IPv6 routing to mobile's home network

Internet

Tunnel from home agent to mobile

Packets tunneled by HA to CoA

Home Agent

Destination Mobile

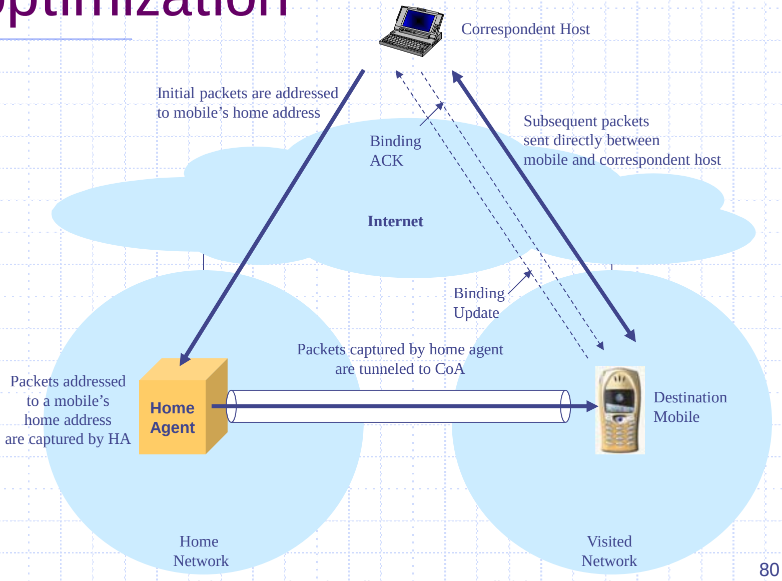
Reverse Tunnel

Packets to correspondent host tunneled to mobile's home agent first

Home Network

Visited Network

Fig. 4.23 MIPv6 route optimization



Correspondent Host

Initial packets are addressed to mobile's home address

Binding ACK

Subsequent packets sent directly between mobile and correspondent host

Internet

Binding Update

Packets captured by home agent are tunneled to CoA

Packets addressed to a mobile's home address are captured by HA

Home Agent

Destination Mobile

Home Network

Visited Network

Mobile IPv6

4.2.5.1 Movement Detection

4.2.5.2 Sending Packets Directly to Mobile’s Care-of Address

4.2.5.3 Sending Packets While Away From Home

4.2.5.4 Formats of Binding Update and Binding Acknowledgement Messages

4.2.5.5 Hierarchical Mobile IPv6 Registration

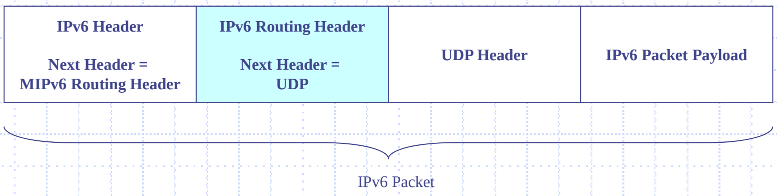
4.2.5.1 Movement Detection

- IPv6 Neighbor Discovery
  - Router Advertisement
    - carry, among other information, the IPv6 addresses of the router and network prefixes that can be used by mobiles to configure their care-of addresses
  - Neighbor Solicitation
- Any other means available to supplement the capabilities provided by IPv6 Neighbor Discovery

4.2.5.2 Sending Packets Directly to Mobile's Care-of Address

- MIPv6 routing header: used by an IPv6 source node to list one or more nodes that should process the IPv6 packet
- The change of CoA is transparent to the upper layer protocols and applications.
  - CN uses the mobile's CoA as the destination address.
  - Mobile's home address is carried in a routing header.
- When the mobile receives the packet:
  - replace the IPv6 destination address in the IPv6 header with the mobile's home address
  - decrement the Segments Left field in the routing header by one (i.e., the Segments Left will become 0, indicating that the mobile's home address is the final destination of the packet)

Fig. 4.24 IPv6 routing header



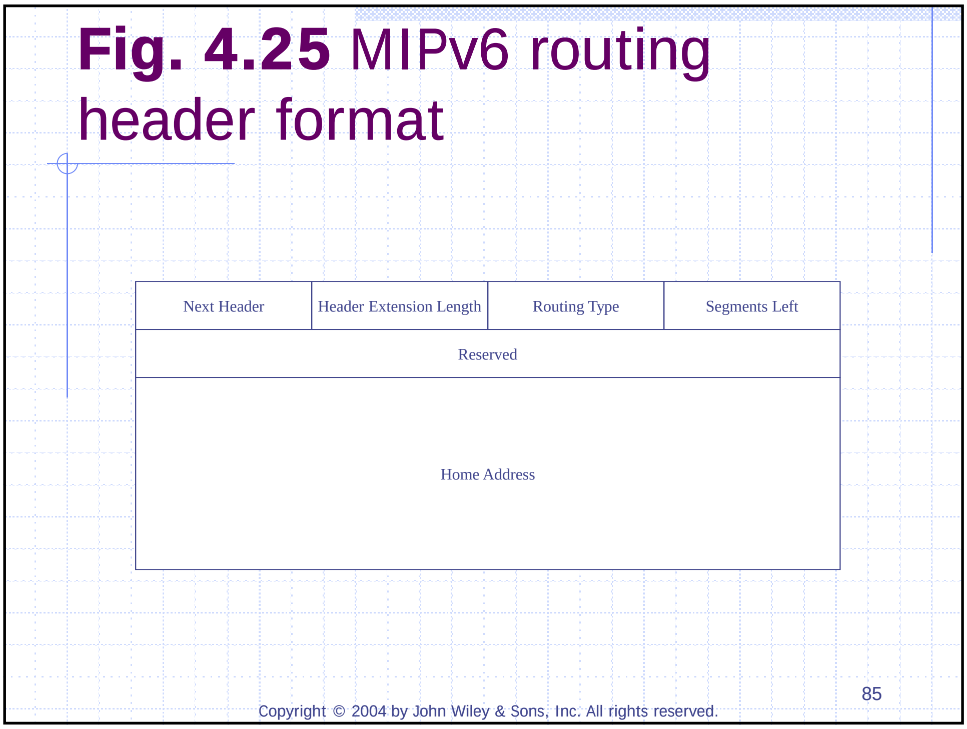
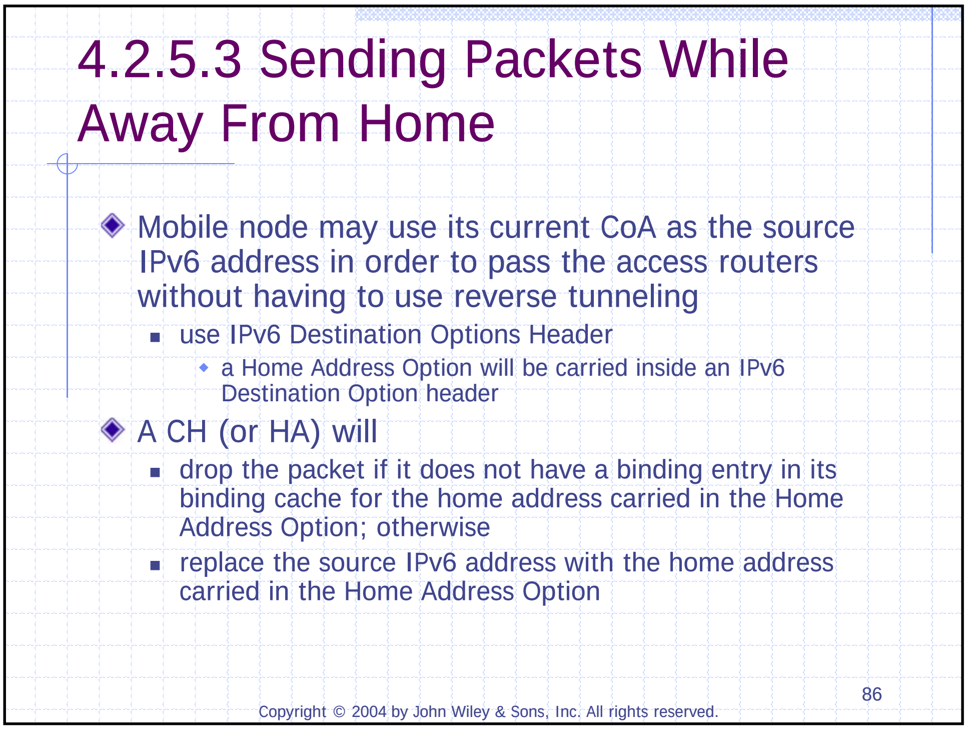


Fig. 4.25 MIPv6 routing header format

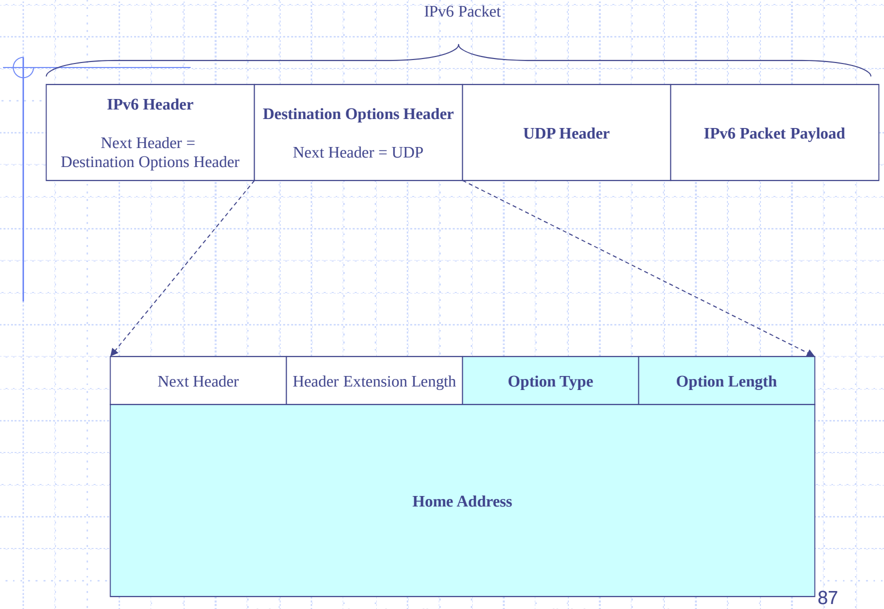
Next Header	Header Extension Length	Routing Type	Segments Left
Reserved			
Home Address			



4.2.5.3 Sending Packets While Away From Home

- Mobile node may use its current CoA as the source IPv6 address in order to pass the access routers without having to use reverse tunneling
  - use IPv6 Destination Options Header
    - a Home Address Option will be carried inside an IPv6 Destination Option header
- A CH (or HA) will
  - drop the packet if it does not have a binding entry in its binding cache for the home address carried in the Home Address Option; otherwise
  - replace the source IPv6 address with the home address carried in the Home Address Option

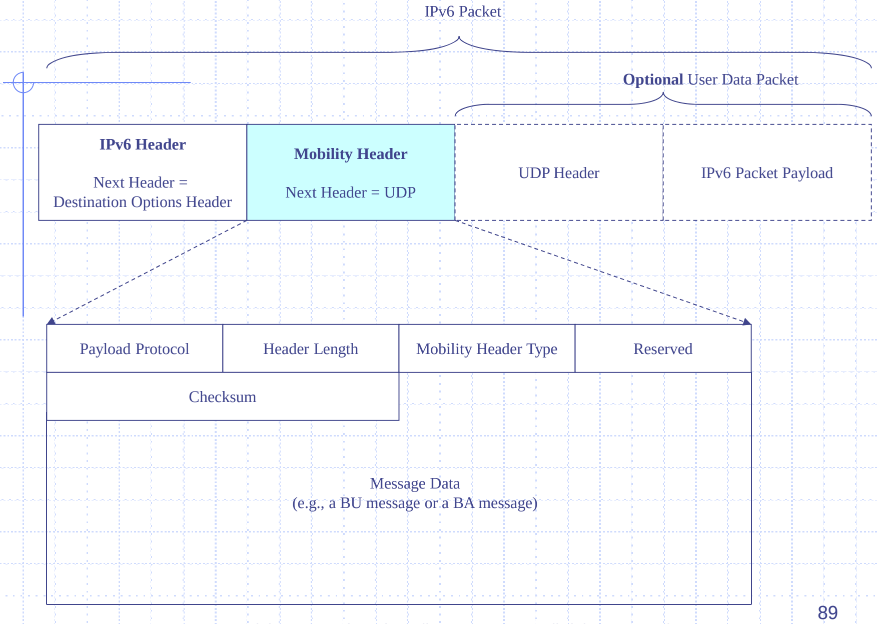
Fig. 4.26 Format of IPv6 Destination Options Header carrying a Mobile IPv6 Home Address Option



4.2.5.4 Formats of Binding Update and Binding Acknowledgement Messages

- Mobility Header: defined by MIPv6 to carry BU and BA
  - The BU or BA message is carried in the Message Data field of the Mobility Header.

Fig. 4.27 Mobile IPv6 Mobility Header



IPv6 Packet

Optional User Data Packet

IPv6 Header

Next Header = Destination Options Header

Mobility Header

Next Header = UDP

UDP Header

IPv6 Packet Payload

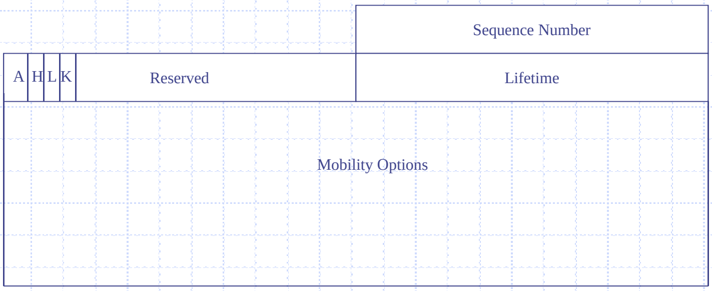
Payload Protocol	Header Length	Mobility Header Type	Reserved
Checksum			

Message Data
(e.g., a BU message or a BA message)

Binding Update

- Sequence Number
- A (Acknowledge): request a BA message be returned upon receipt of the BU message
- H (Home Registration): request that the receiving node act as the sending node's HA
- L (Link-Local Address Compatibility): set when the home address has the same interface identifier as the link-local address
- K (Key Management Mobility Capability): indicate whether the protocol used for establishing the IPsec security association can survive movement
  - only valid in a BU message sent to a HA
- Reserved
- Lifetime: the number of time units remaining before the binding expires
- Mobility Options: a variable-length field that contains one or more Mobility Options in a Type-Length-Value format

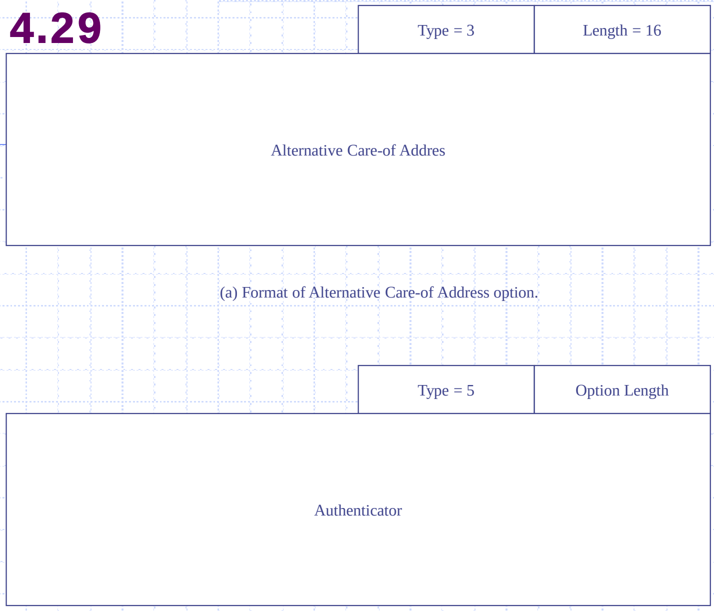
Fig. 4.28 Format of Mobile IPv6 Binding Update message



Mobility Options

- Options in BU
  - Alternative Care-of Address option: carry a mobile's CoA
  - Binding Authorization Data option: carry security-related information needed by the receiving node to authenticate and authorize the BU message
  - Nonce Indices option: used by CN to authenticate a BU from a mobile
    - only used when the BU message is sent to a CN

Fig. 4.29



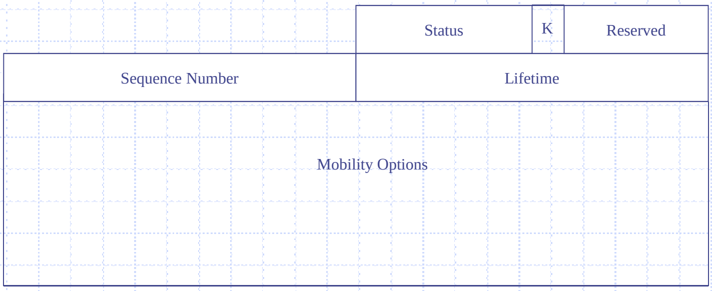
(a) Format of Alternative Care-of Address option.

(b) Format of Binding Authorization Data option.

Binding Acknowledgment

- Statue: indicate the status of how the corresponding BU message is processed
- K: indicate whether the protocol used by HA for establishing the IPsec security association can survive movement
- Reserved
- Sequence Number: copied from the corresponding BU
- Lifetime
- Mobility Options
  - Binding Authorization Data option
  - Binding Refresh Advice option: used by a home agent to inform a mobile how often the mobile should send a new BU message to the home agent.

Fig. 4.30 Format of Mobile IPv6 Binding Acknowledgement message



Status

K

Reserved

Sequence Number

Lifetime

Mobility Options

4.2.5.5 Hierarchical Mobile IPv6 Registration

- Forwarding from the previous care-of address
- Local home agent

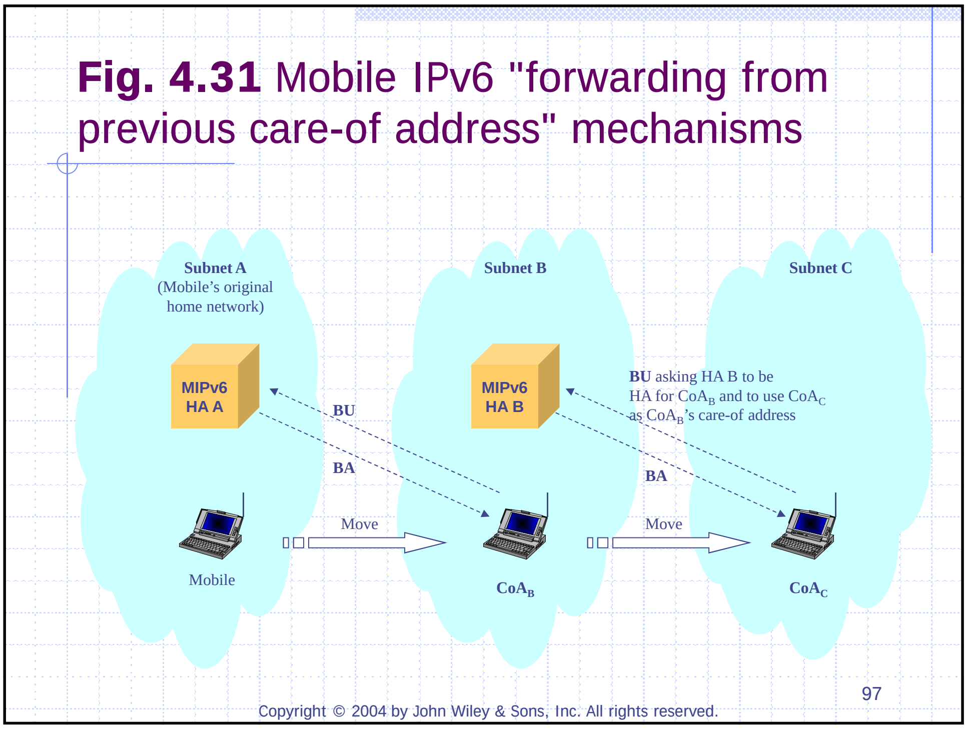


Fig. 4.31 Mobile IPv6 "forwarding from previous care-of address" mechanisms

Subnet A
(Mobile's original
home network)

Subnet B

Subnet C

MIPv6
HA A

MIPv6
HA B

BU

BA

BU asking HA B to be
HA for $\mathrm{CoA_B}$ and to use $\mathrm{CoA_C}$
as $\mathrm{CoA_B}$'s care-of address

BA

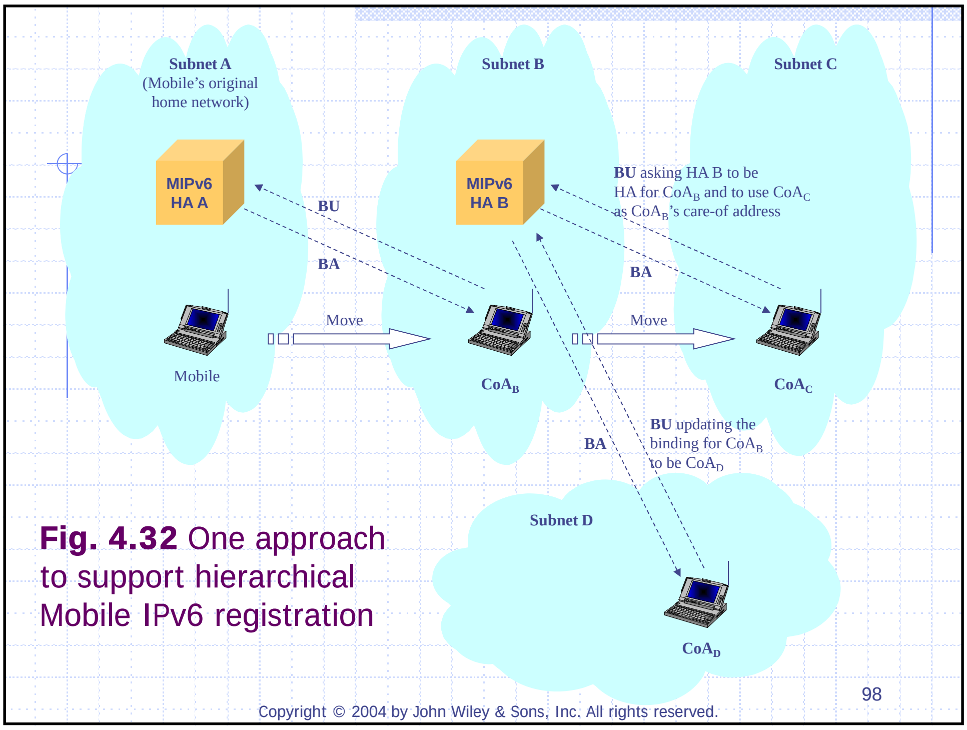
Move

Move

Mobile

$\mathrm{CoA_B}$

$\mathrm{CoA_C}$



Subnet A
(Mobile's original
home network)

Subnet B

Subnet C

MIPv6
HA A

MIPv6
HA B

BU

BA

BU asking HA B to be
HA for $\mathrm{CoA_B}$ and to use $\mathrm{CoA_C}$
as $\mathrm{CoA_B}$'s care-of address

BA

Move

Move

Mobile

$\mathrm{CoA_B}$

$\mathrm{CoA_C}$

BA

BU updating the
binding for $\mathrm{CoA_B}$
to be $\mathrm{CoA_D}$

Subnet D

$\mathrm{CoA_D}$

Fig. 4.32 One approach to support hierarchical Mobile IPv6 registration

4.2.6 SIP-based Mobility Management

- Main reasons for SIP-based mobility management
  - SIP is currently the protocol of choice for signaling and control of real-time voice and multimedia applications over IP networks.
  - Significant efforts in the research community and the industry have been devoted to supporting mobility using SIP.
  - SIP appears to be the only application-layer protocol that can be readily extended to support terminal mobility today.
- SIP already supports user mobility.
- Key difference between SIP-based mobility management and Mobile IP: SIP servers may only participate in setting up the application sessions between the end users
  - Solve the triangular routing problem
  - SIP servers will not likely become bottlenecks

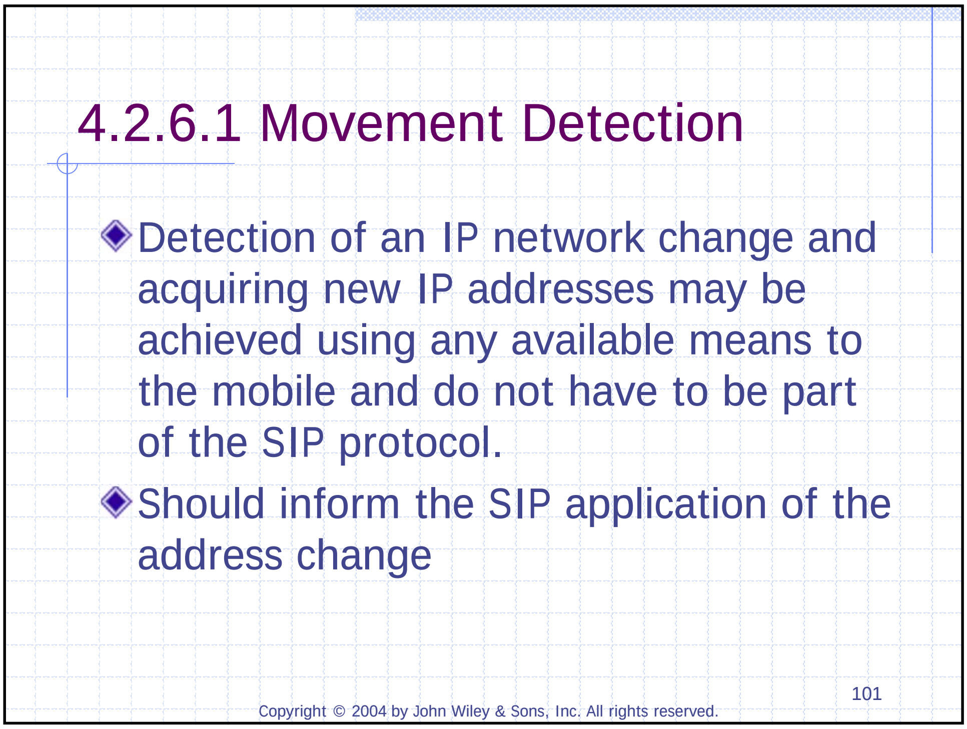
SIP-based Mobility Management

4.2.6.1 Movement Detection

4.2.6.2 Pre-Session Terminal Mobility

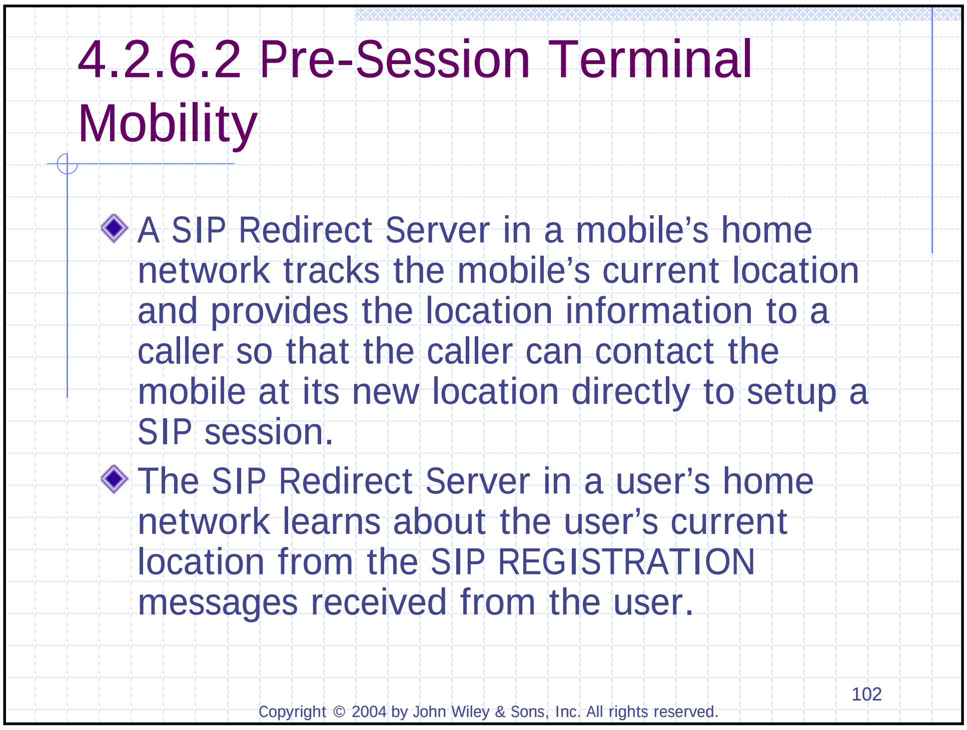
4.2.6.3 Mid-Session Terminal Mobility Support

4.2.6.4 Limitations of IP Mobility Using SIP



4.2.6.1 Movement Detection

- Detection of an IP network change and acquiring new IP addresses may be achieved using any available means to the mobile and do not have to be part of the SIP protocol.
- Should inform the SIP application of the address change



4.2.6.2 Pre-Session Terminal Mobility

- A SIP Redirect Server in a mobile’s home network tracks the mobile’s current location and provides the location information to a caller so that the caller can contact the mobile at its new location directly to setup a SIP session.
- The SIP Redirect Server in a user’s home network learns about the user’s current location from the SIP REGISTRATION messages received from the user.

Fig. 4.33 SIP-based pre-session terminal mobility management

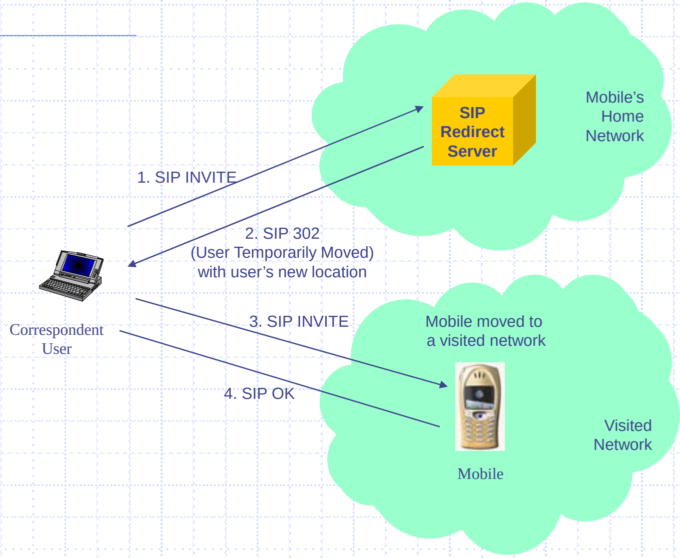
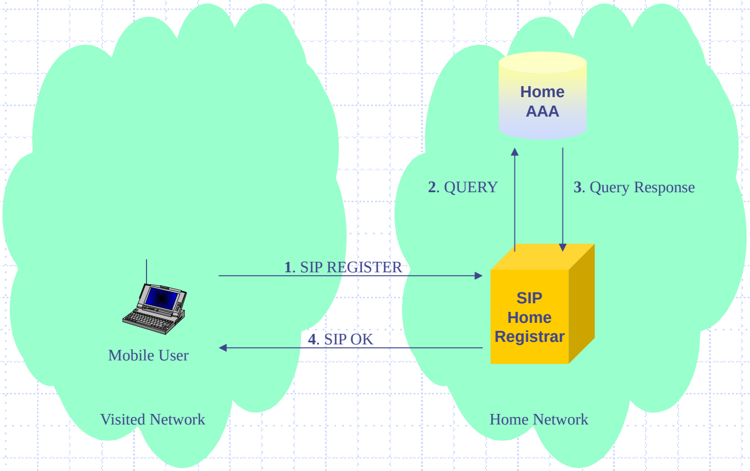


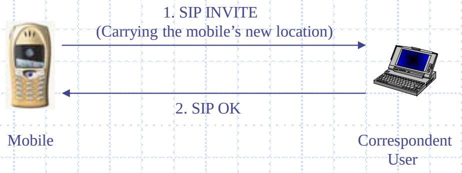
Fig. 4.34 Location update for supporting SIP-based terminal mobility

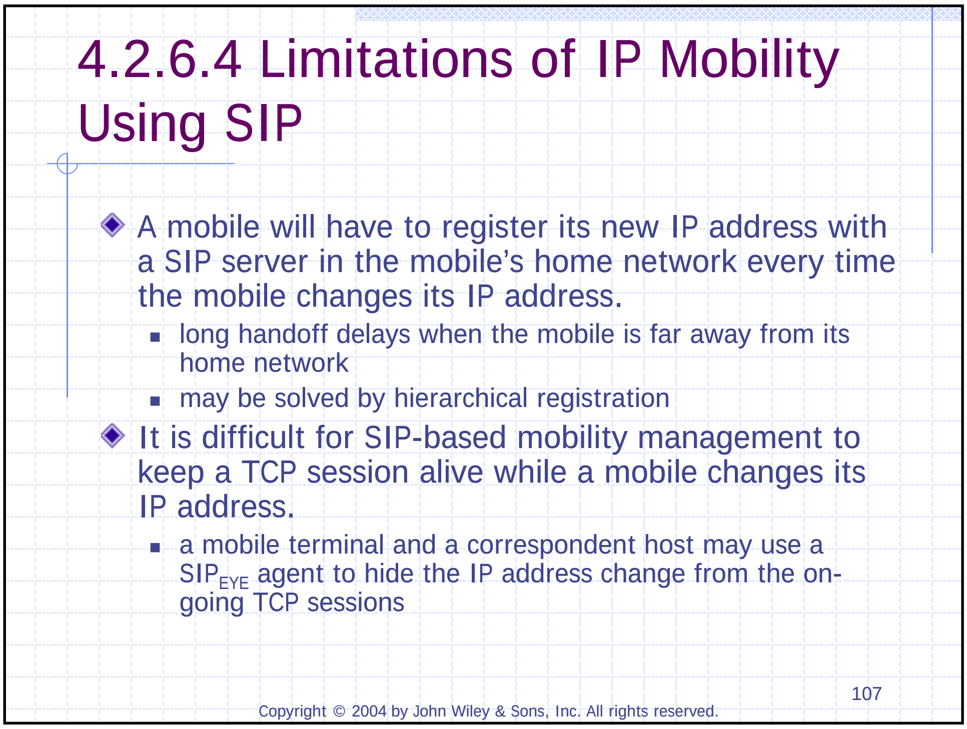


4.2.6.3 Mid-Session Terminal Mobility Support

- Mobile sends a new SIP INVITE message to invite the correspondent host to re-establish the SIP session to the mobile's new location.
- Mobile also updates its location with its home SIP Redirect Server.

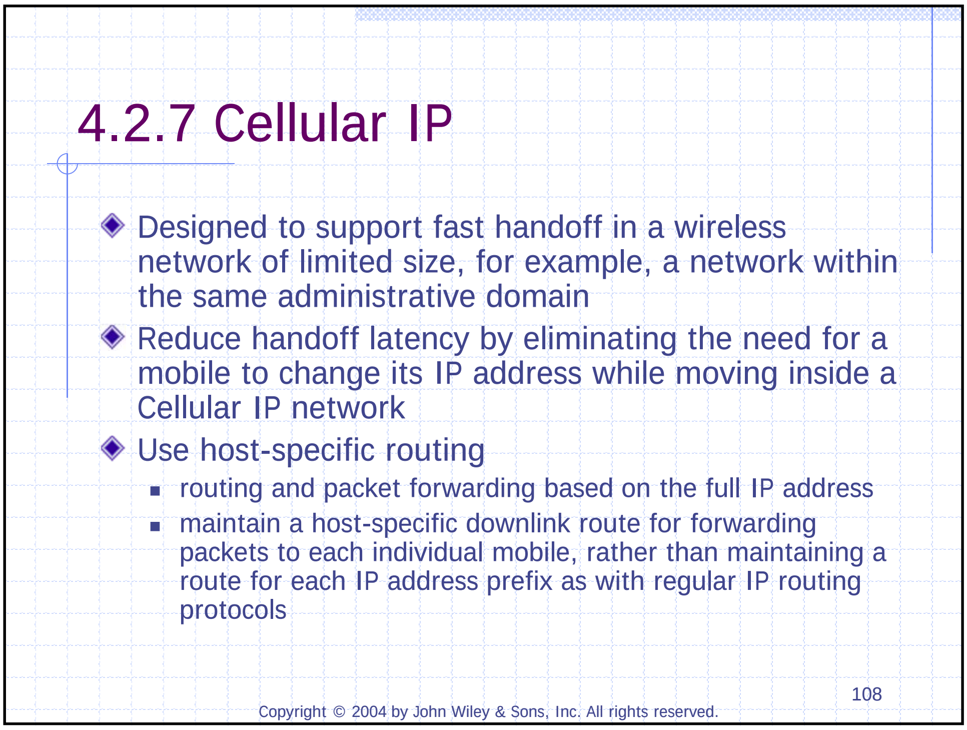
Fig. 4.35 SIP-based mid-session terminal mobility management





4.2.6.4 Limitations of IP Mobility Using SIP

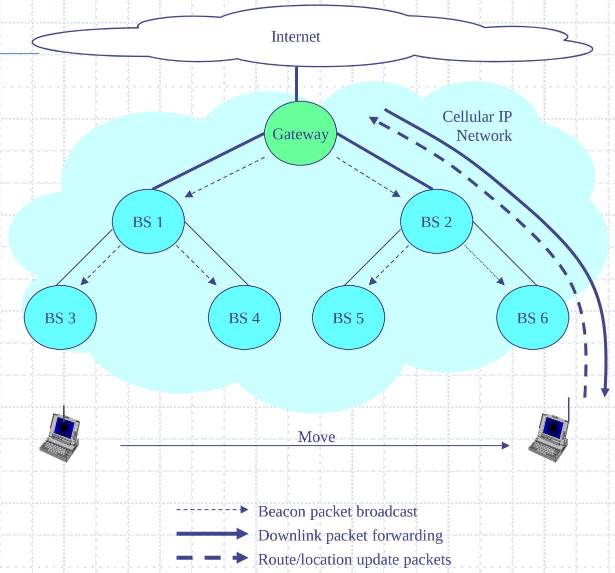
- A mobile will have to register its new IP address with a SIP server in the mobile’s home network every time the mobile changes its IP address.
  - long handoff delays when the mobile is far away from its home network
  - may be solved by hierarchical registration
- It is difficult for SIP-based mobility management to keep a TCP session alive while a mobile changes its IP address.
  - a mobile terminal and a correspondent host may use a SIP_{EYE} agent to hide the IP address change from the on-going TCP sessions



4.2.7 Cellular IP

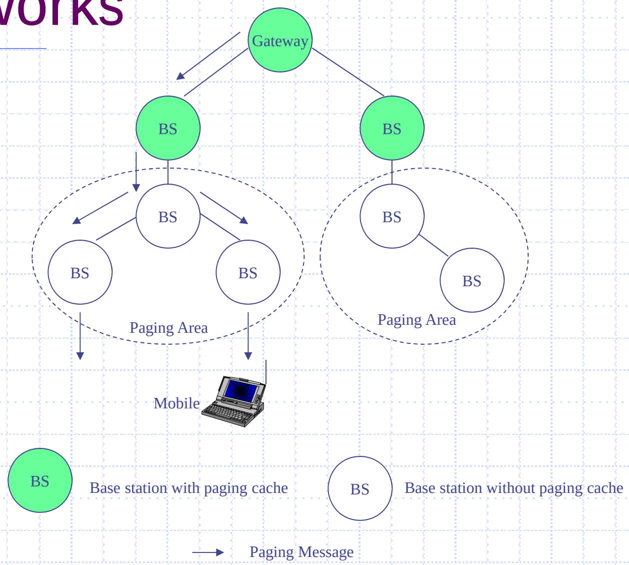
- Designed to support fast handoff in a wireless network of limited size, for example, a network within the same administrative domain
- Reduce handoff latency by eliminating the need for a mobile to change its IP address while moving inside a Cellular IP network
- Use host-specific routing
  - routing and packet forwarding based on the full IP address
  - maintain a host-specific downlink route for forwarding packets to each individual mobile, rather than maintaining a route for each IP address prefix as with regular IP routing protocols

Fig. 4.36 Cellular IP



Beacon packet broadcast
Downlink packet forwarding
Route/location update packets

Fig. 4.37 Paging in Cellular IP networks



🟩 BS Base station with paging cache
○ BS Base station without paging cache
→ Paging Message

4.2.8 HAWAII

- Similar to Cellular IP, HAWAII (Handoff-Aware Wireless Access Internet Infrastructure) is designed to support fast handoff and paging inside a wireless network under a single administrative domain.
  - reduce handoff latency
  - use host-specific routing
- HAWAII and Cellular IP differ in routing and mobility management implementations.

Fig. 4.38 HAWAII

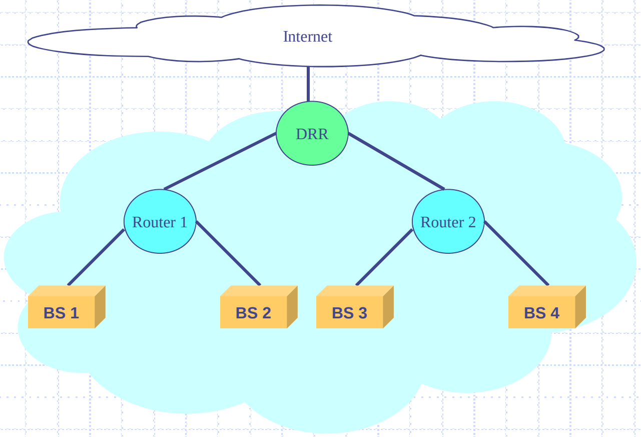


Fig. 4.39 HAWAII mobile power-up procedure

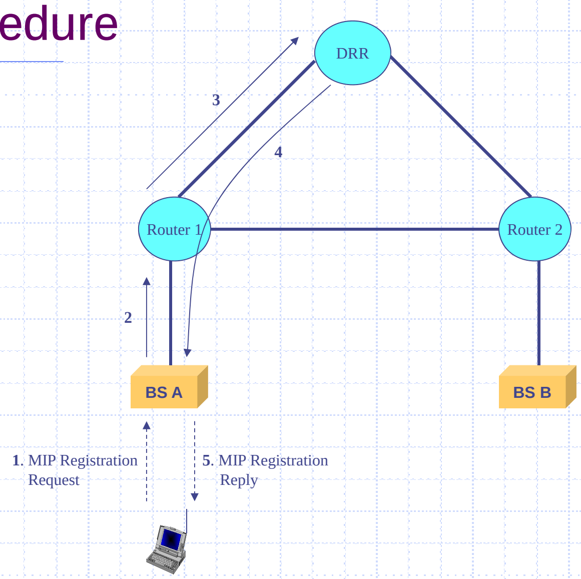
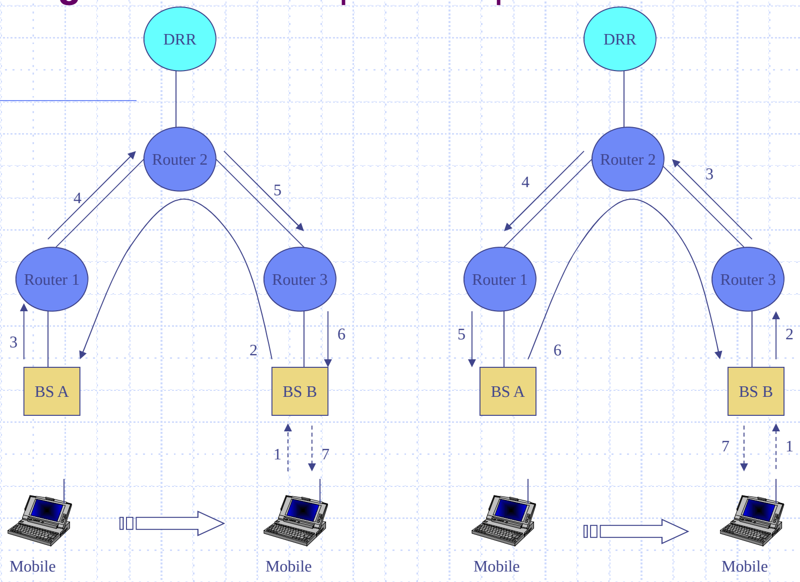


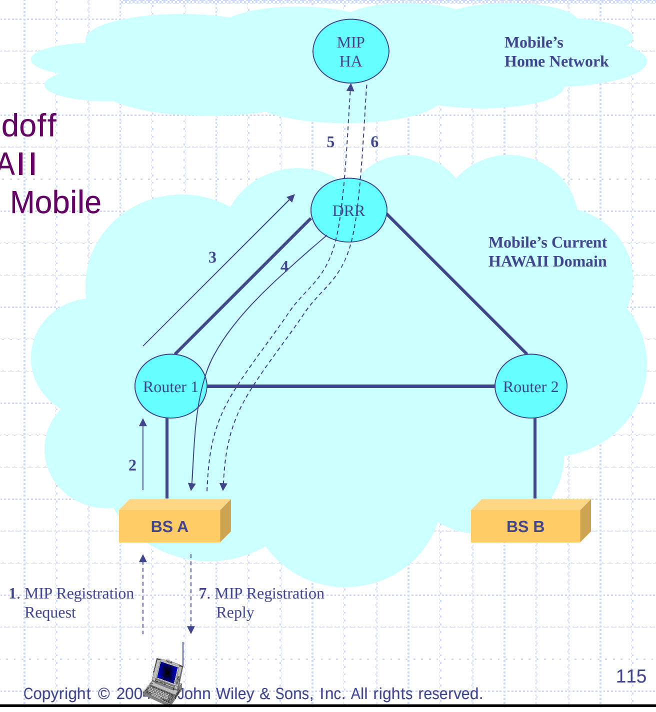
Fig. 4.40 HAWAII path setup schemes



(a) Forwarding Path Setup

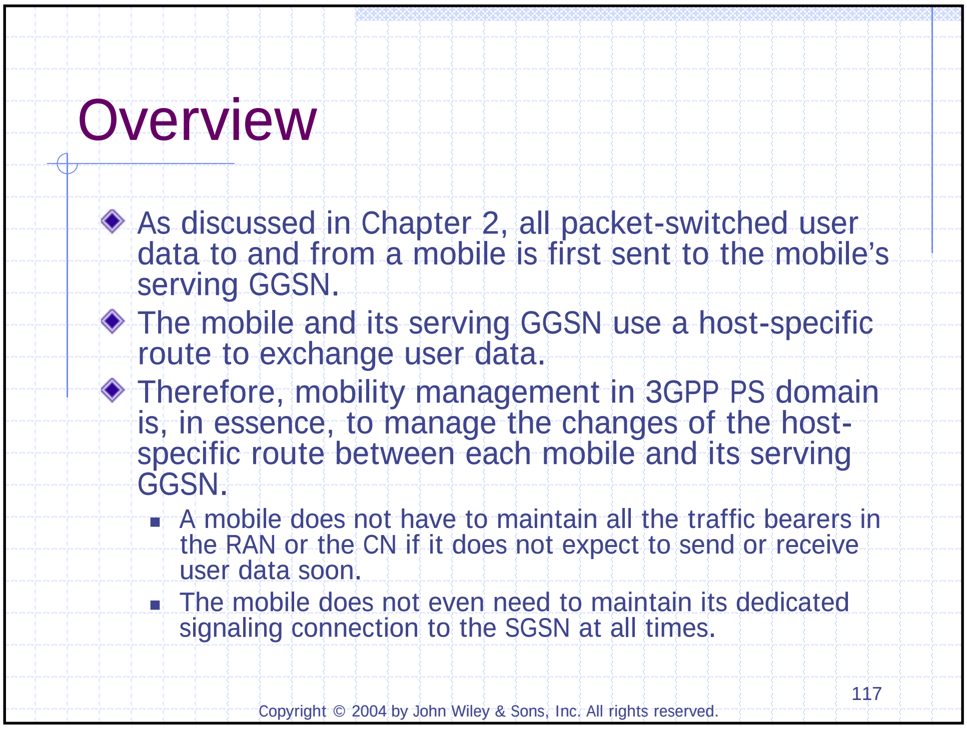
(b) Non-Forwarding Path Setup

Fig. 4.41 Handoff between HAWAII domains using Mobile IP



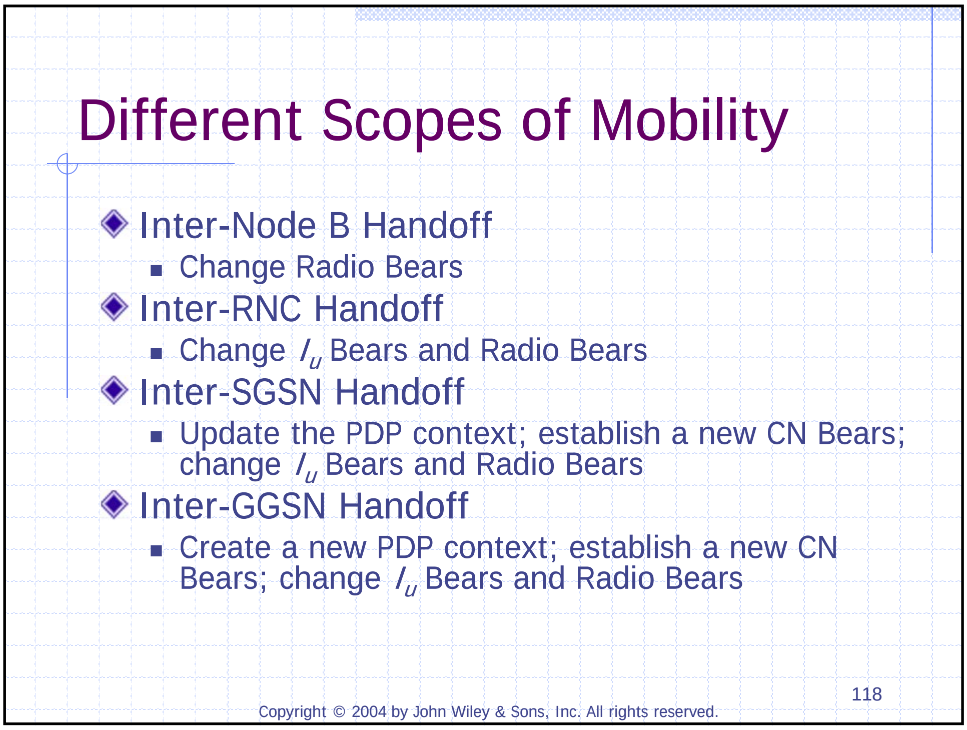
4.3 Mobility Management in 3GPP Packet Networks

- 4.3.1 Packet Mobility Management (PMM) Context and States
- 4.3.2 Location Management for Packet-Switched Services
- 4.3.3 Routing Area Update
- 4.3.4 Serving RNS Relocation
- 4.3.5 Hard Handoffs
- 4.3.6 Paging Initiated by Packet-Switched Core Network
- 4.3.7 Service Request Procedure
- 4.3.8 Handoff and Roaming Between 3GPP and Wireless LANs



Overview

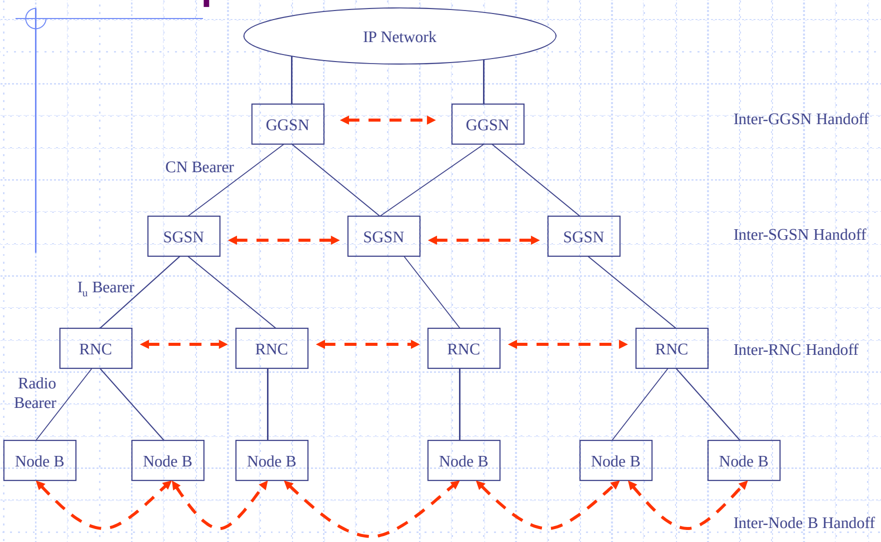
- As discussed in Chapter 2, all packet-switched user data to and from a mobile is first sent to the mobile's serving GGSN.
- The mobile and its serving GGSN use a host-specific route to exchange user data.
- Therefore, mobility management in 3GPP PS domain is, in essence, to manage the changes of the host-specific route between each mobile and its serving GGSN.
  - A mobile does not have to maintain all the traffic bearers in the RAN or the CN if it does not expect to send or receive user data soon.
  - The mobile does not even need to maintain its dedicated signaling connection to the SGSN at all times.



Different Scopes of Mobility

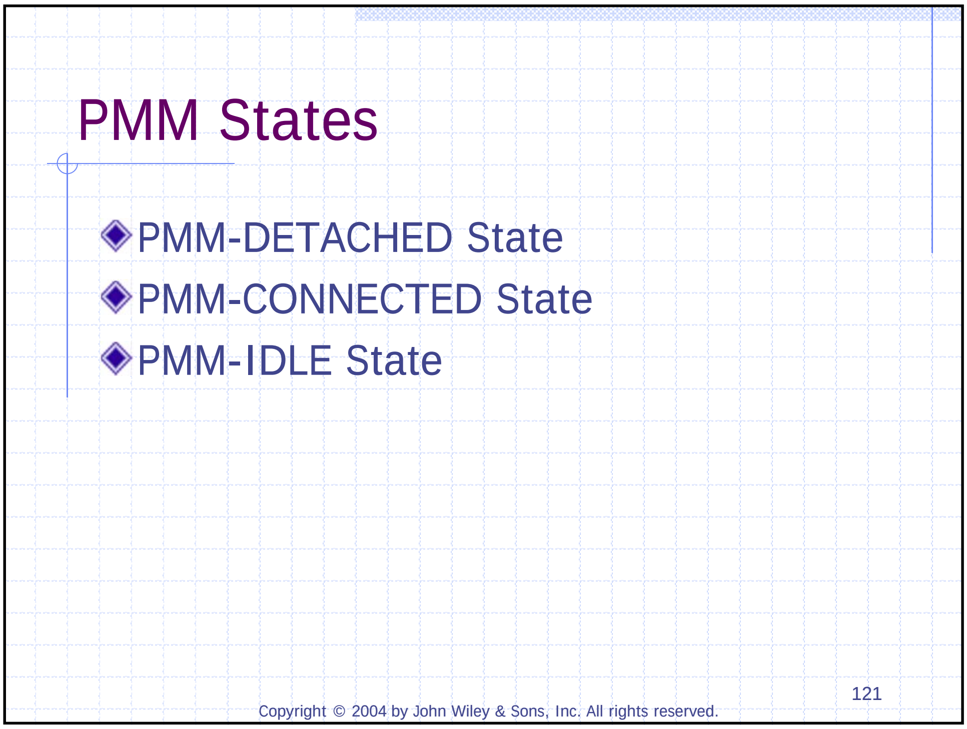
- Inter-Node B Handoff
  - Change Radio Bears
- Inter-RNC Handoff
  - Change I_u Bears and Radio Bears
- Inter-SGSN Handoff
  - Update the PDP context; establish a new CN Bears; change I_u Bears and Radio Bears
- Inter-GGSN Handoff
  - Create a new PDP context; establish a new CN Bears; change I_u Bears and Radio Bears

Fig. 4.42 Scope of mobility in 3GPP packet-switched domain



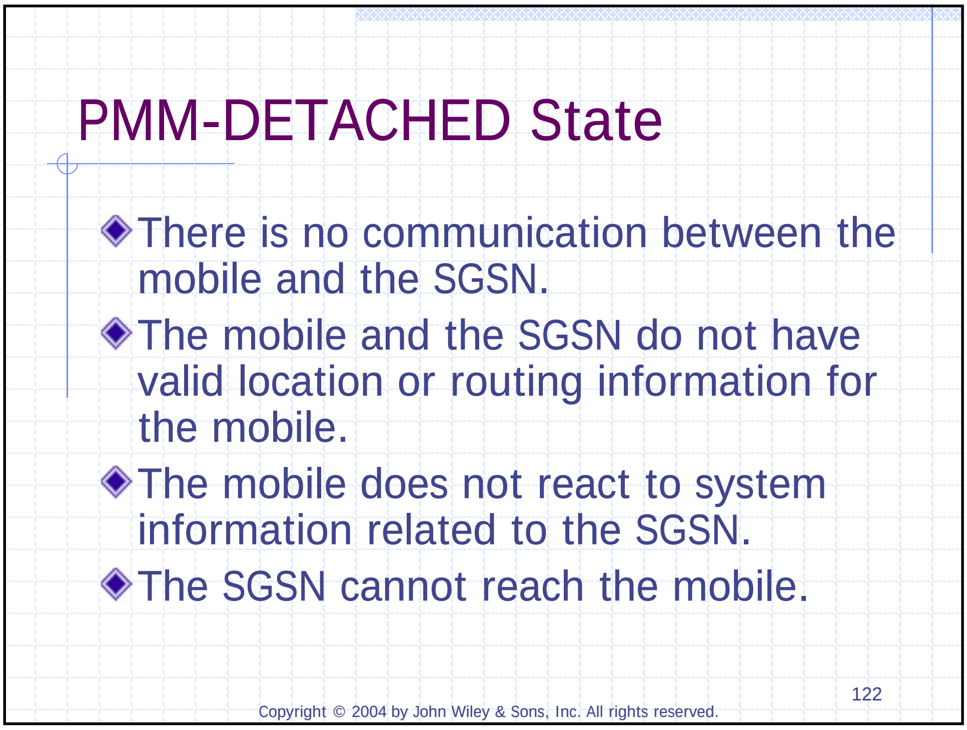
4.3.1 Packet Mobility Management (PMM) Context and States

- PMM context: a set of information used by the network to track the mobile’s location
- PMM state
  - Which network connections (bearers) between the mobile and the SGSN should be maintained for the mobile
  - How the mobile’s location should be tracked by the network
- Maintained by SGSN and mobile station



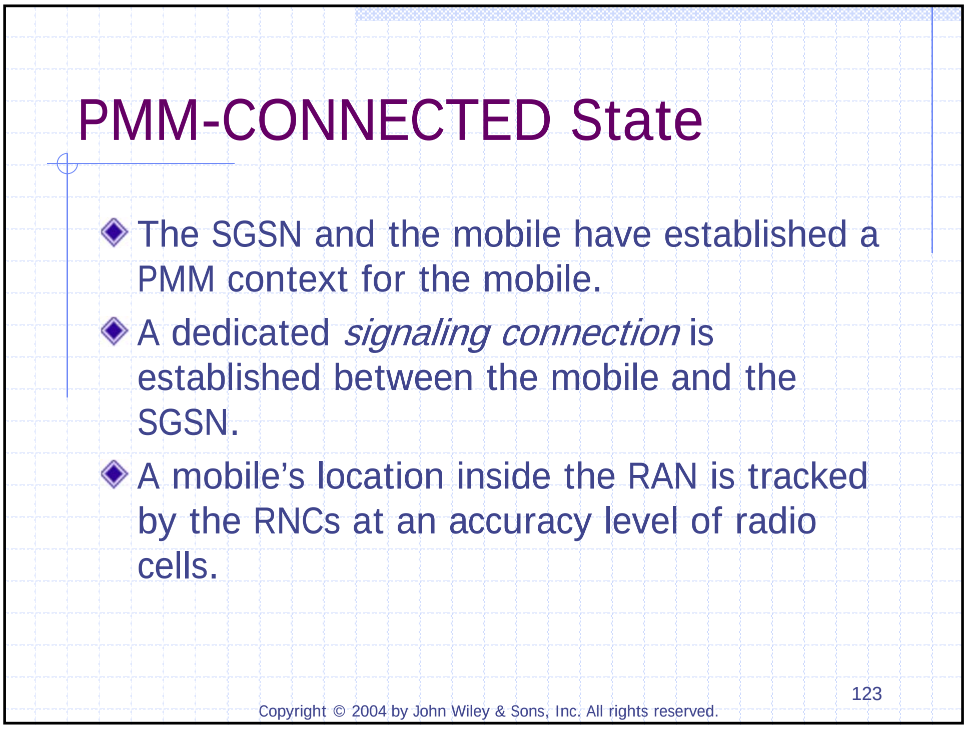
PMM States

- PMM-DETACHED State
- PMM-CONNECTED State
- PMM-IDLE State



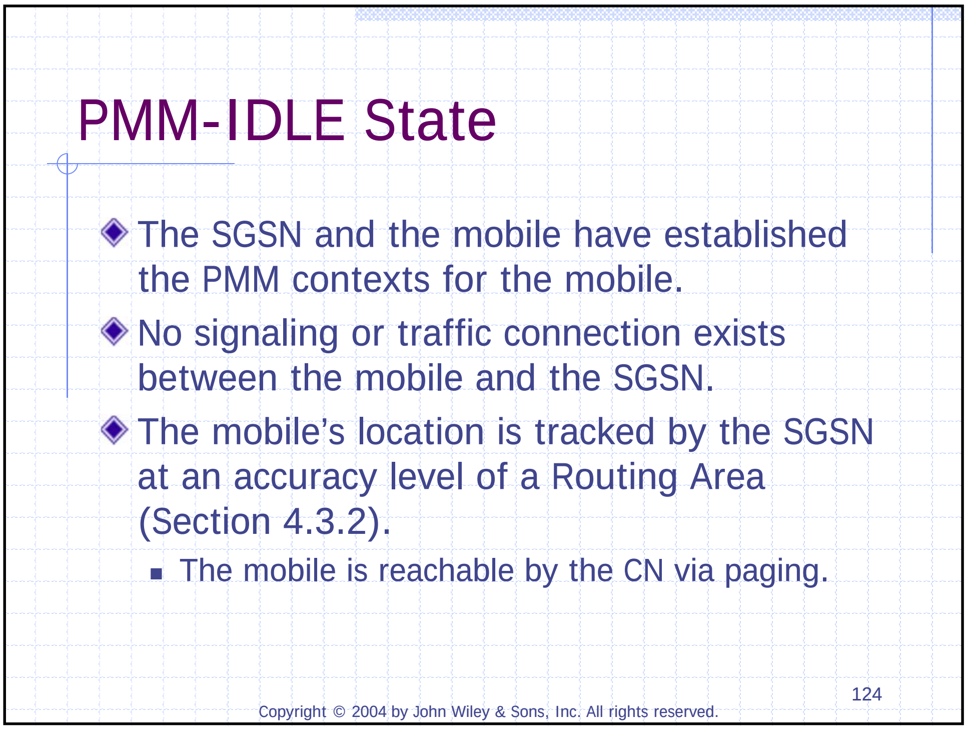
PMM-DETACHED State

- There is no communication between the mobile and the SGSN.
- The mobile and the SGSN do not have valid location or routing information for the mobile.
- The mobile does not react to system information related to the SGSN.
- The SGSN cannot reach the mobile.



PMM-CONNECTED State

- The SGSN and the mobile have established a PMM context for the mobile.
- A dedicated *signaling connection* is established between the mobile and the SGSN.
- A mobile’s location inside the RAN is tracked by the RNCs at an accuracy level of radio cells.



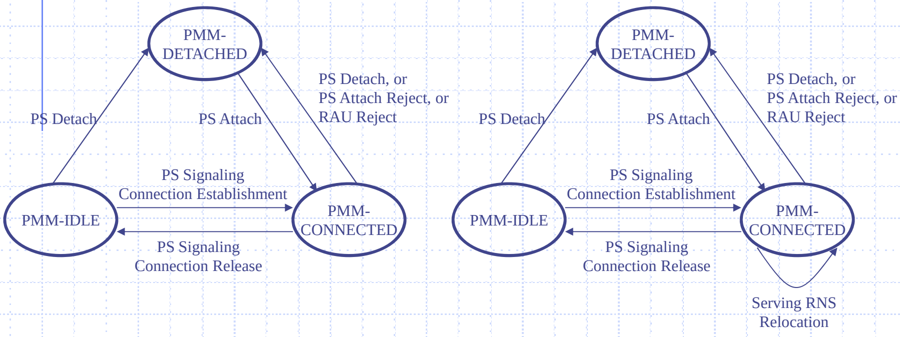
PMM-IDLE State

- The SGSN and the mobile have established the PMM contexts for the mobile.
- No signaling or traffic connection exists between the mobile and the SGSN.
- The mobile’s location is tracked by the SGSN at an accuracy level of a Routing Area (Section 4.3.2).
  - The mobile is reachable by the CN via paging.

PDP Context

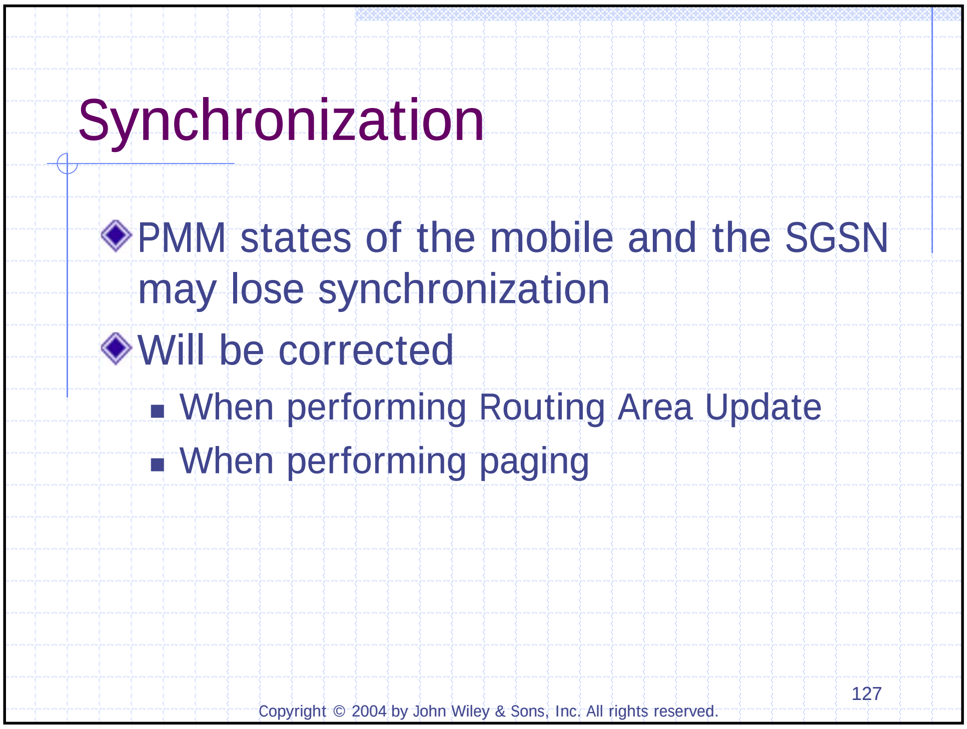
- When the mobile's PMM state transitions from PMM-CONNECTED to PMM-IDLE subsequently, the mobile's existing active PDP contexts will continue to remain in ACTIVE state on the GGSN and the SGSN.
  - Reduce the time for a mobile to change from PMM-IDLE state back to PMM-CONNECTED state
  - Make it easier for the PS CN domain to support paging
    - Allow the GGSN to always know a mobile's serving SGSN
    - GGSNs do not have to be aware of the paging operations

Fig. 4.43 3GPP PMM state transition machines



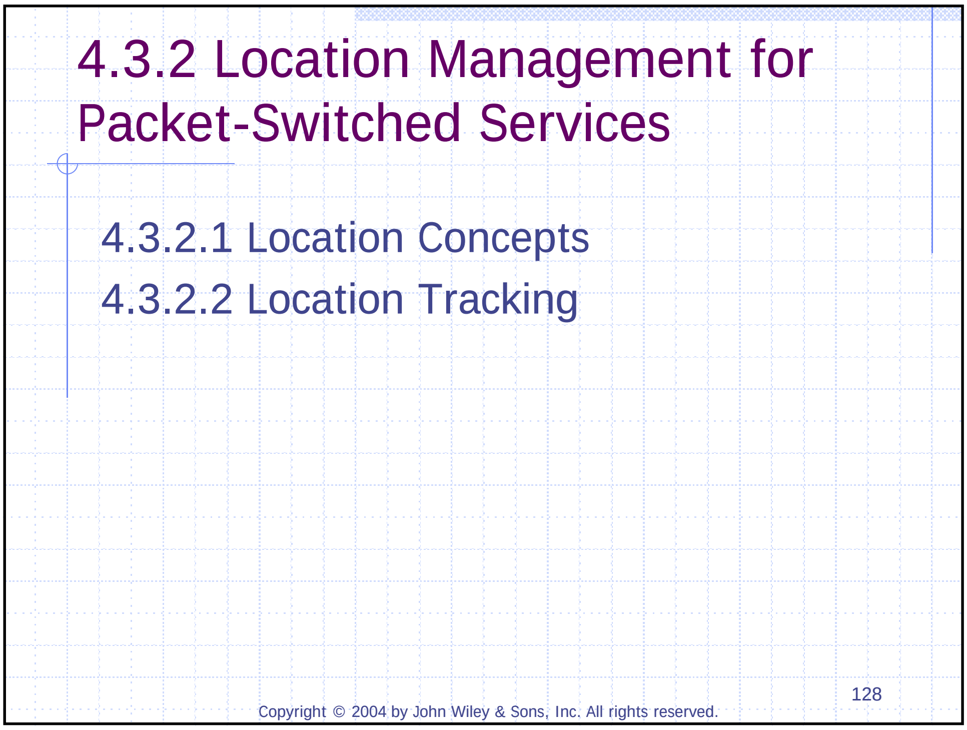
(a) PMM states on mobile

(b) PMM states on SGSN



Synchronization

- PMM states of the mobile and the SGSN may lose synchronization
- Will be corrected
  - When performing Routing Area Update
  - When performing paging



4.3.2 Location Management for Packet-Switched Services

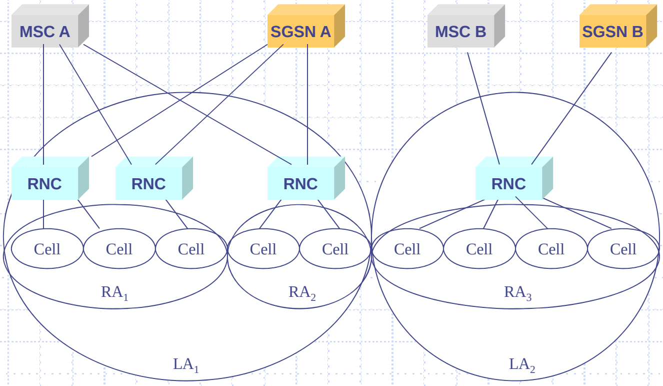
4.3.2.1 Location Concepts

4.3.2.2 Location Tracking

4.3.2.1 Location Concepts

- The RAN uses the following location concepts
  - Cell Area (or Cell)
  - UTRAN Registration Area (URA): an area covered by a set of cells
- The CN uses the following location concepts
  - Location Area (LA): a group of Cells used by the CS CN domain to track the locations of mobiles that are using CS services
  - Routing Area (RA): a group of Cells used by the PS CN domain to track the locations of mobiles that are using PS services

Fig. 4.44 3GPP location management for packet services

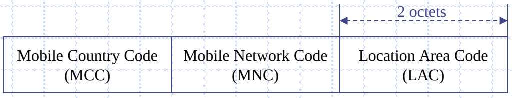


LA vs. RA

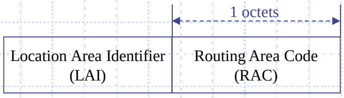
- LA
  - One LA is handled by *only one* MSC/VLR.
  - Each LA is identified by a globally unique Location Area Identifier (LAI).
  - When a mobile moves inside a LA, it does not have to perform location update with the CN CS domain.
- RA
  - One RA is handled by *only one* SGSN.
  - Each RA is identified by a globally unique Routing Area Identifier (RAI).
  - When a mobile moves inside a RA, it does not have to perform location update with the CN PS domain.
- One RA cannot belong to more than one LA while each LA may contain multiple RAs.

131

Fig. 4.45 Structures of 3GPP Location Area Identifier and Routing Area Identifier

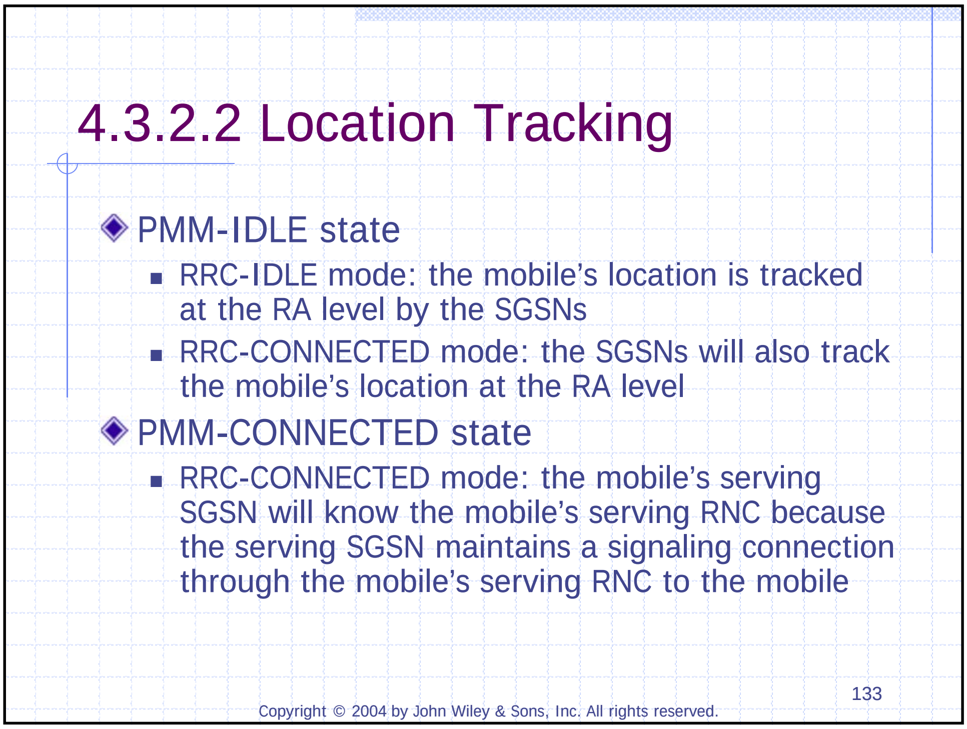


(a) Structure of Location Area Identifier (LAI)



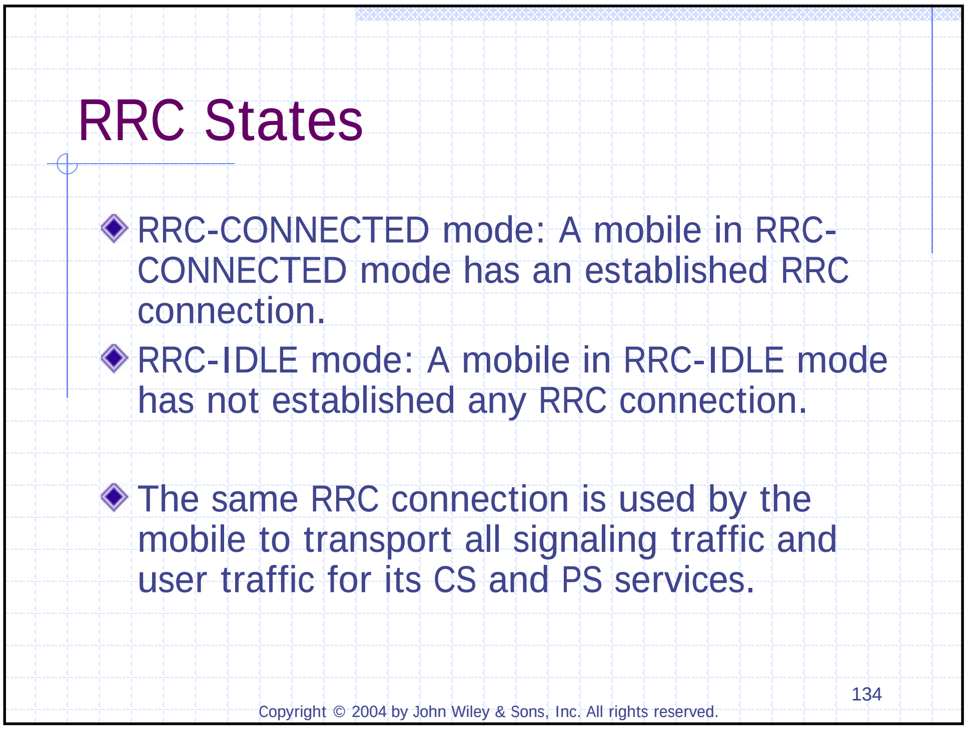
(a) Structure of Routing Area Identifier (RAI)

132



4.3.2.2 Location Tracking

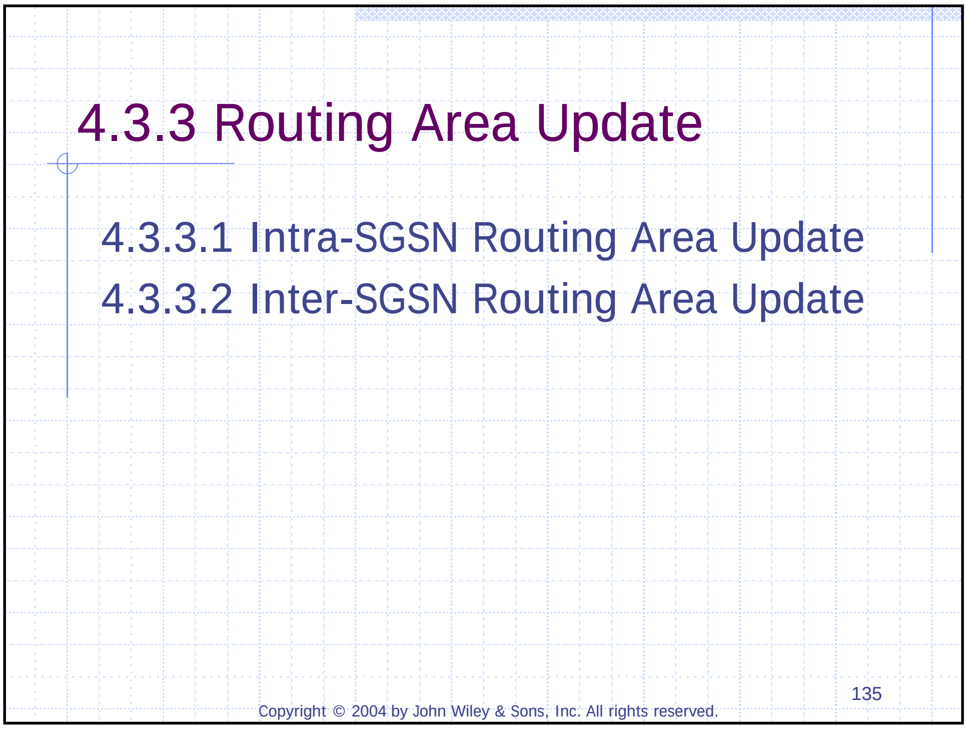
- PMM-IDLE state
  - RRC-IDLE mode: the mobile's location is tracked at the RA level by the SGSNs
  - RRC-CONNECTED mode: the SGSNs will also track the mobile's location at the RA level
- PMM-CONNECTED state
  - RRC-CONNECTED mode: the mobile's serving SGSN will know the mobile's serving RNC because the serving SGSN maintains a signaling connection through the mobile's serving RNC to the mobile



RRC States

- RRC-CONNECTED mode: A mobile in RRC-CONNECTED mode has an established RRC connection.
- RRC-IDLE mode: A mobile in RRC-IDLE mode has not established any RRC connection.

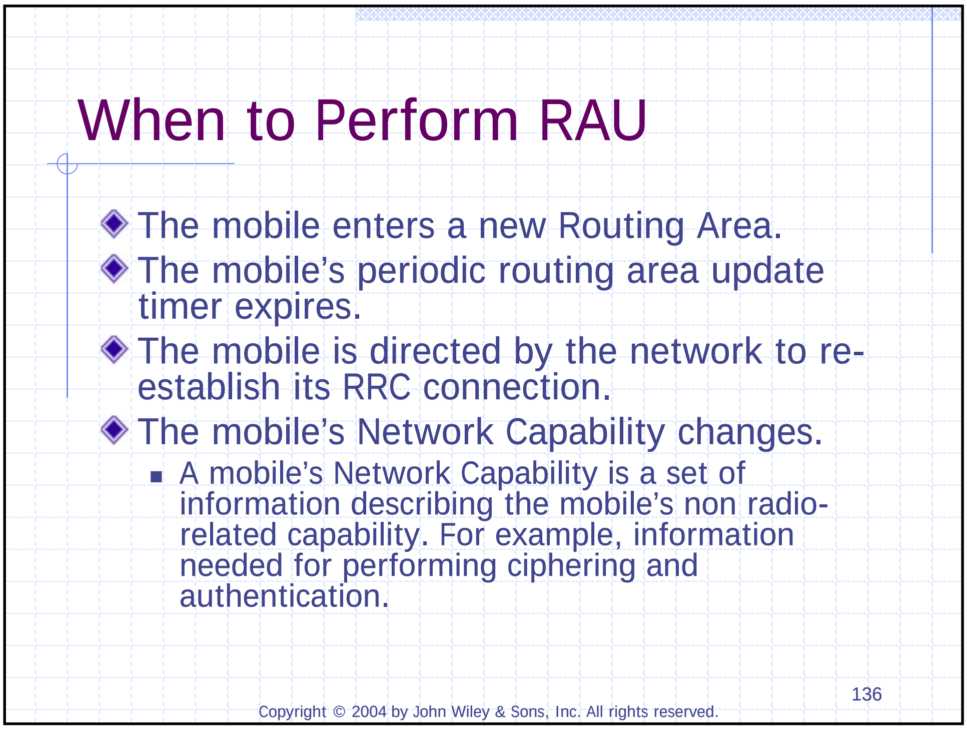
- The same RRC connection is used by the mobile to transport all signaling traffic and user traffic for its CS and PS services.



4.3.3 Routing Area Update

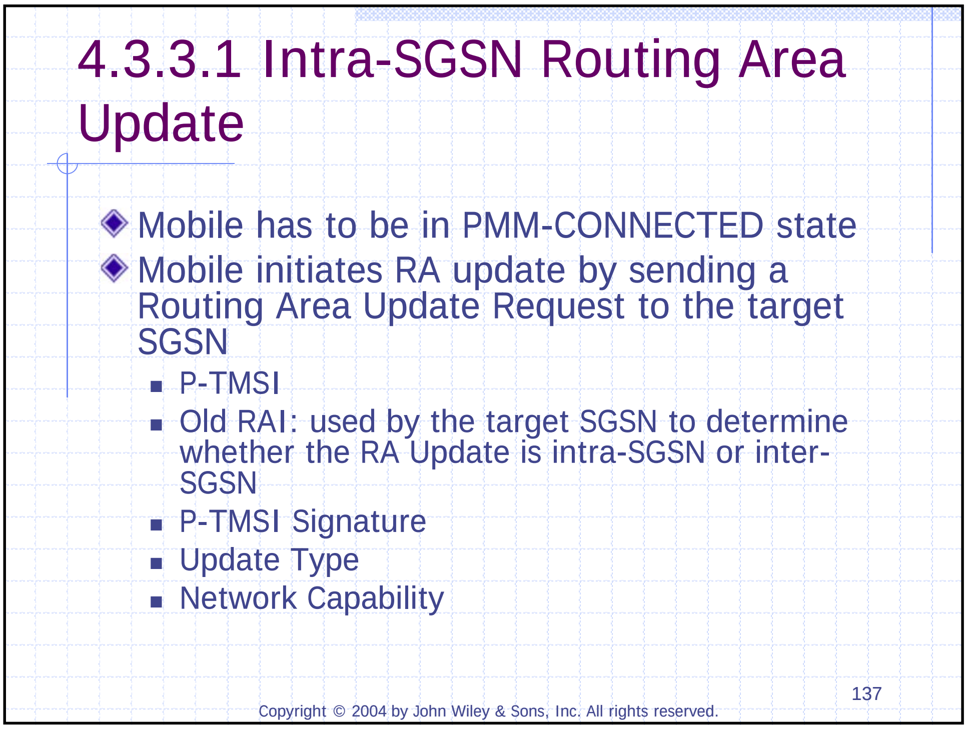
4.3.3.1 Intra-SGSN Routing Area Update

4.3.3.2 Inter-SGSN Routing Area Update



When to Perform RAU

- The mobile enters a new Routing Area.
- The mobile's periodic routing area update timer expires.
- The mobile is directed by the network to re-establish its RRC connection.
- The mobile's Network Capability changes.
  - A mobile's Network Capability is a set of information describing the mobile's non radio-related capability. For example, information needed for performing ciphering and authentication.



4.3.3.1 Intra-SGSN Routing Area Update

- Mobile has to be in PMM-CONNECTED state
- Mobile initiates RA update by sending a Routing Area Update Request to the target SGSN
  - P-TMSI
  - Old RAI: used by the target SGSN to determine whether the RA Update is intra-SGSN or inter-SGSN
  - P-TMSI Signature
  - Update Type
  - Network Capability

137

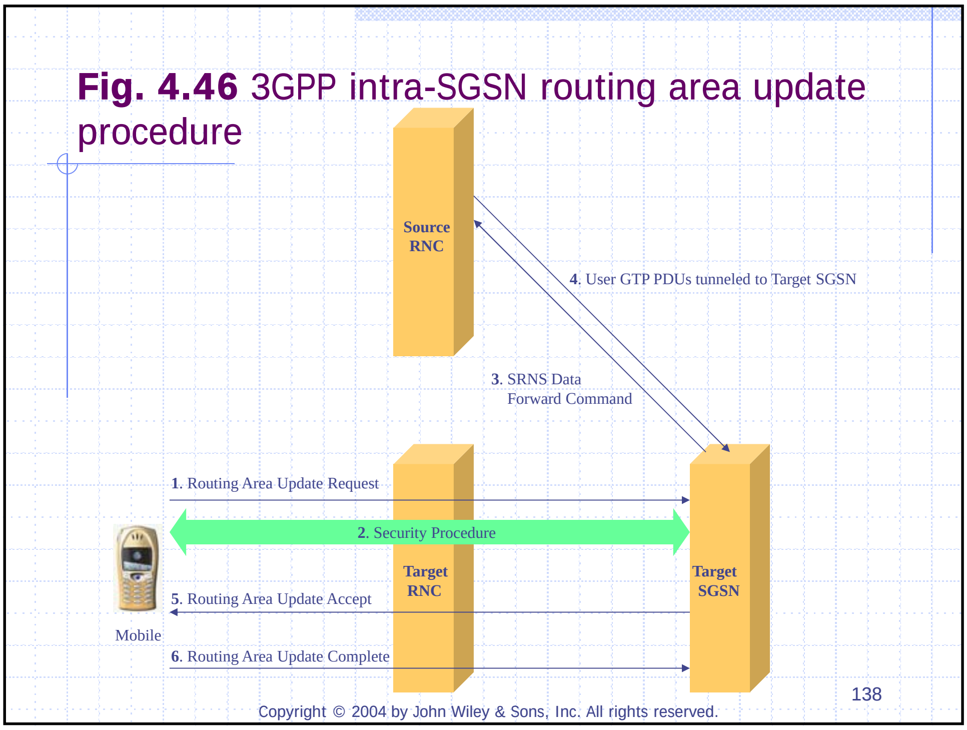


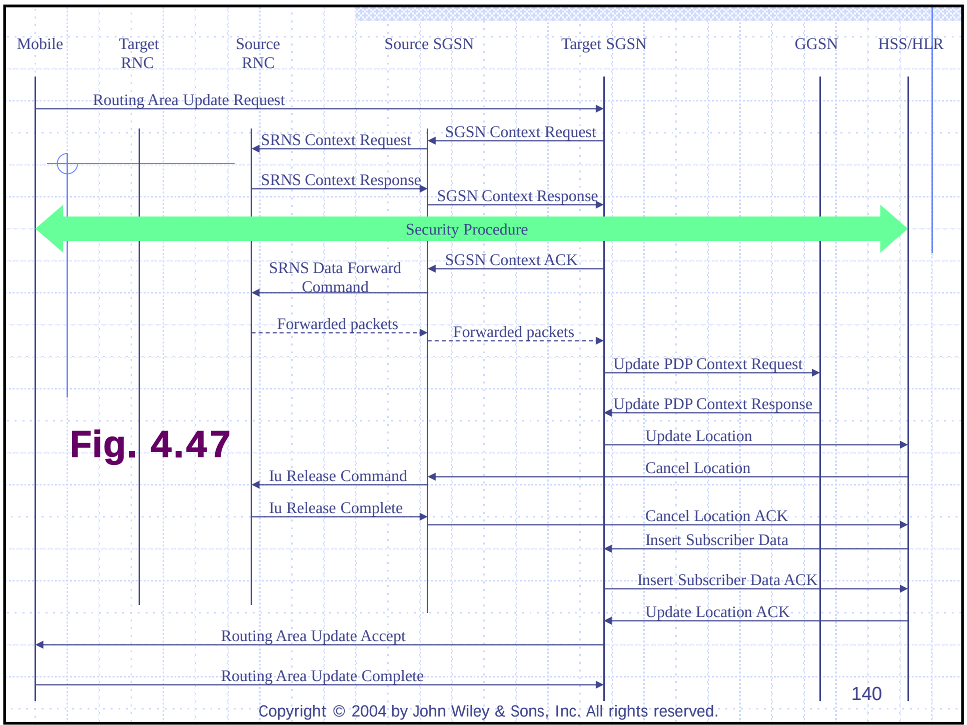
Fig. 4.46 3GPP intra-SGSN routing area update procedure

Source RNC
4. User GTP PDUs tunneled to Target SGSN
3. SRNS Data Forward Command
1. Routing Area Update Request
2. Security Procedure
Target RNC
Target SGSN
5. Routing Area Update Accept
Mobile
6. Routing Area Update Complete

138

4.3.3.2 Inter-SGSN Routing Area Update

- The target SGSN is different from the source SGSN
  - The target SGSN will send a SGSN Context Request message to the source SGSN to ask the source SGSN to validate the mobile's P-TMSI
- The source SGSN will
  - Upon positive validation of the P-TMSI
    - SGSN Context Response: carry PMM context and PDP context
    - SRNS Context Request
  - Upon negative validation of the P-TMSI
    - The source SGSN will send an appropriate error cause to the target SGSN, which will trigger the target SGSN to initiate the security procedures directly with the mobile to authenticate the mobile.
    - If this authentication is positive, the target SGSN will send another SGSN Context Request message to the source SGSN to retrieve the mobile's PMM context and PDP context.
- After RAU, the host-specific route is also updated.



Mobile
Target RNC
Source RNC
Source SGSN
Target SGSN
GGSN
HSS/HLR

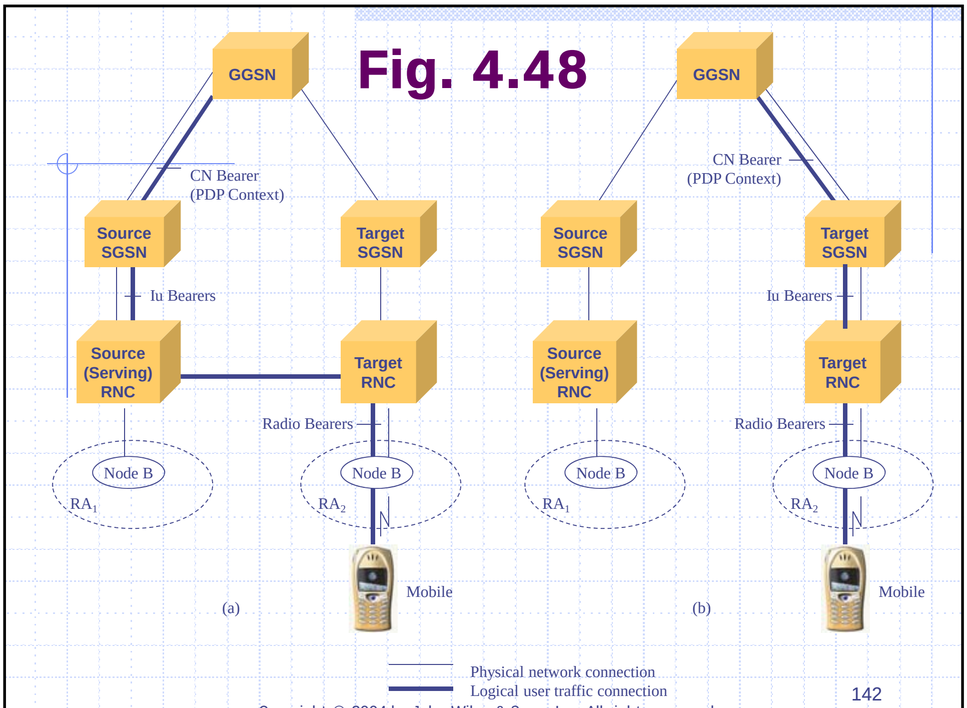
Routing Area Update Request
SGSN Context Request
SRNS Context Request
SRNS Context Response
SGSN Context Response
Security Procedure
SGSN Context ACK
SRNS Data Forward Command
Forwarded packets
Forwarded packets
Update PDP Context Request
Update PDP Context Response
Update Location
Cancel Location
Iu Release Command
Iu Release Complete
Cancel Location ACK
Insert Subscriber Data
Insert Subscriber Data ACK
Update Location ACK
Routing Area Update Accept
Routing Area Update Complete

Fig. 4.47

4.3.4 Serving RNS Relocation

- Relocate I_u connections from the old serving RNC to the new serving RNC
- This section assumes that before the relocation, the mobile's serving RNC is using the I_{ur} interface to forward signaling and user traffic to another RNC, which in turn delivers the user traffic to the mobile.

Fig. 4.48

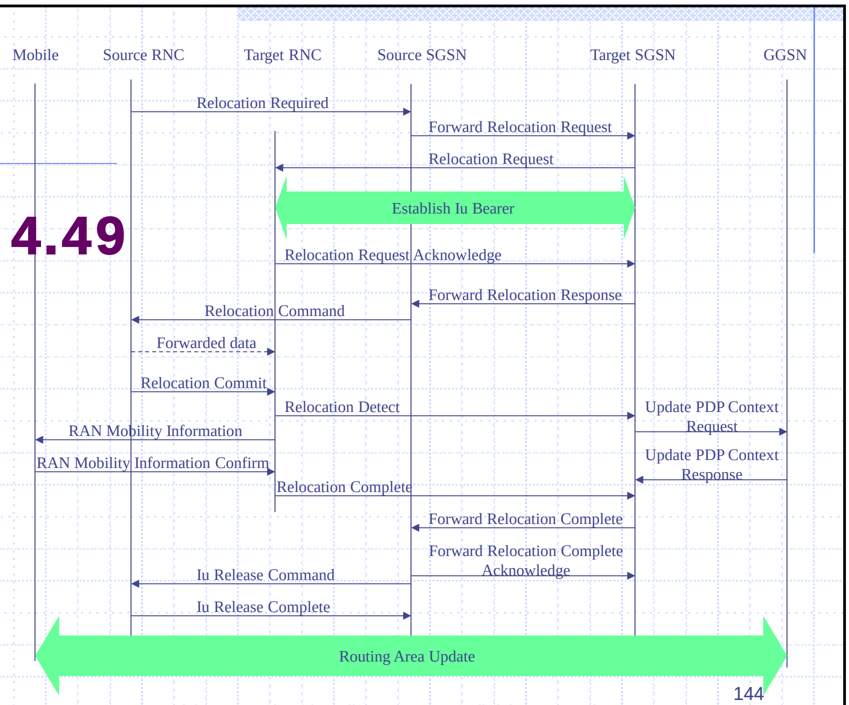


Procedure

- Only the source RNC can initiate Serving RNS Relocation.
  - Based on measurement results of the quality of the radio channels to the mobile and based on its knowledge of the RAN topology
  - Send a RANAP Relocation Required message to the source SGSN
    - Relocation Type: “UE not Involved” or “UE Involved”
    - Source ID: Identifier of the source RNC
    - Target ID: Identifier of the target RNC
    - Source RNC to target RNC transparent container: information needed by the target RNC to perform serving RNC relocation including security information, RRC context

143

Fig. 4.49



Mobile, Source RNC, Target RNC, Source SGSN, Target SGSN, GGSN

Relocation Required

Forward Relocation Request

Relocation Request

Establish Iu Bearer

Relocation Request Acknowledge

Forward Relocation Response

Relocation Command

Forwarded data

Relocation Commit

Relocation Detect

Update PDP Context Request

RAN Mobility Information

RAN Mobility Information Confirm

Update PDP Context Response

Relocation Complete

Forward Relocation Complete

Forward Relocation Complete Acknowledge

Iu Release Command

Iu Release Complete

Routing Area Update

144

4.3.5 Hard Handoffs

- Inter-RNC hard handoff without I_{ur} interface
- Only the source RNC can initiate the inter-RNC hard handoff process.
  - RANAP Relocation Required message to the source SGSN
  - Relocation Type: UE Involved
- Relocation Request Acknowledge: carry an extra information element - Target RNC to Source RNC Transparent Container
  - contain all the radio-related information that the mobile will need in order to tune its radio to the radio channels of the target RNS

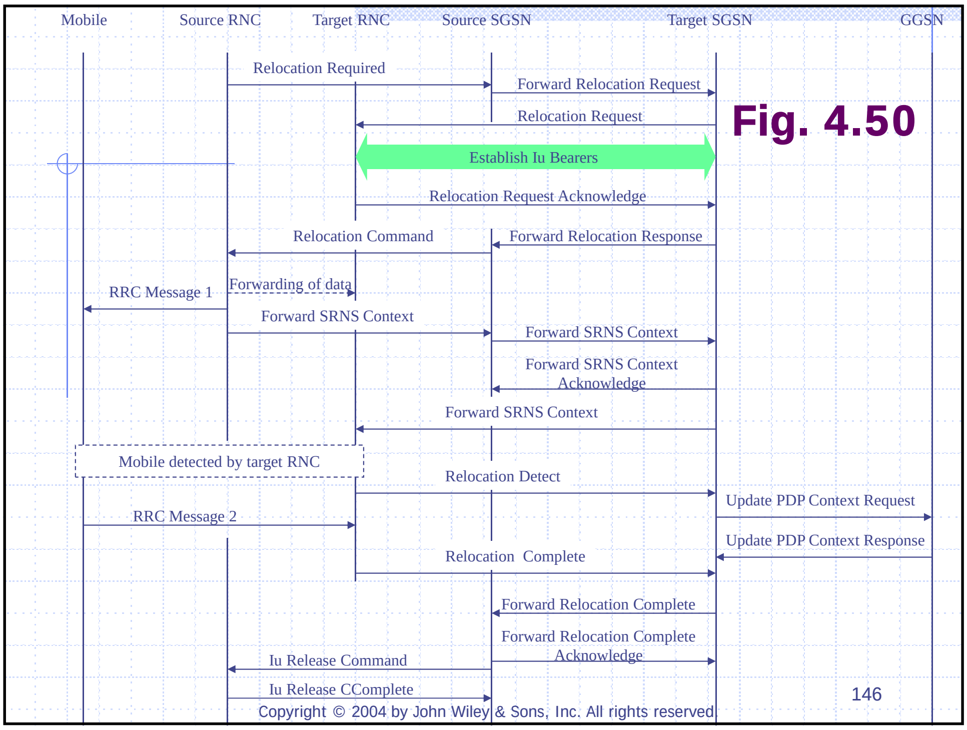
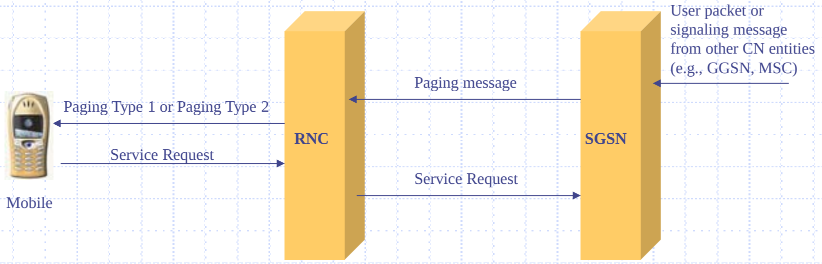


Fig. 4.50

4.3.6 Paging Initiated by Packet-Switched Core Network

- A mobile in PMM-IDLE state
- The SGSN initiates paging by sending a RANAP Paging message to every RNC in the Routing Area
  - Identities of the mobile to be paged
  - CN Domain Identifier
  - Area
- Two types inside RAN
  - Type 1 Paging
    - No dedicated RRC connection
    - Use Paging Channel
  - Type 2 Paging
    - Use dedicated RRC connection

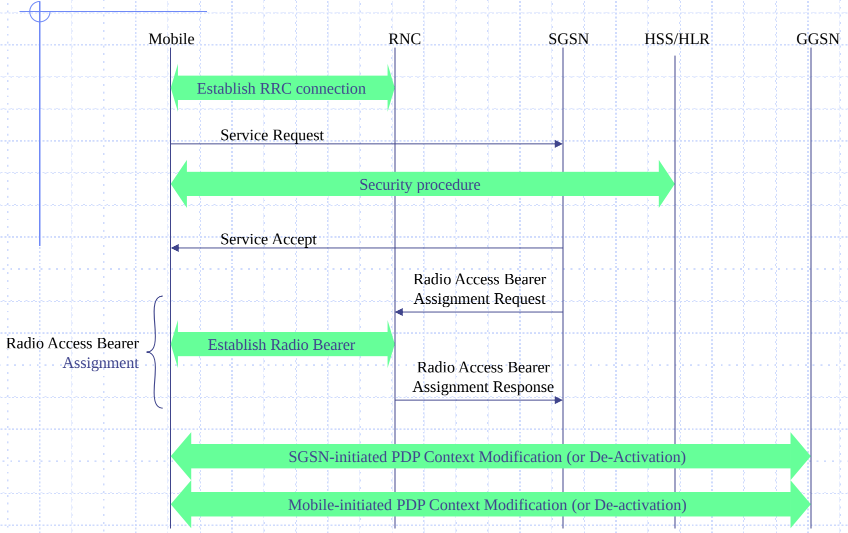
Fig. 4.51 3GPP paging in packet switched domain



4.3.7 Service Request Procedure

- Used by a mobile
  - in PMM-IDLE state: request the establishment of a signaling connection between the mobile and the SGSN
  - in PMM-CONNECTED state: request resource reservation for the mobile’s active PDP contexts
- SGSN takes actions based on the Service Type in the received Service Request
  - DATA
    - a signaling connection between the mobile and the SGSN will be established
    - the RABs will be allocated for the mobile’s active PDP contexts
  - SIGNALING
    - Only a signaling connection between the mobile and the SGSN will be established
- Service Request is acknowledged
  - Mobile in PMM-CONNECTED state and Service Type is DATA: SGSN will return a Service Accept
  - Mobile in PMM-IDLE state and Service Type is SIGNALING: SGSN does not send any explicit signaling message

Fig. 4.52 3GPP Mobile-initiated Service Request Procedure


Mobile
RNC
SGSN
HSS/HLR
GGSN
Establish RRC connection
Service Request
Security procedure
Service Accept
Radio Access Bearer Assignment Request
Radio Access Bearer Assignment
Establish Radio Bearer
Radio Access Bearer Assignment Response
SGSN-initiated PDP Context Modification (or De-Activation)
Mobile-initiated PDP Context Modification (or De-activation)

4.3.8 Handoff and Roaming Between 3GPP and Wireless LANs

- Handoff between 3GPP and IP networks using Mobile IP
- Sample signaling flow for handoff between 3GPP and IP networks using MIPv4
- Mobile terminals with dual home addresses

Fig. 4.53 Handoff between 3GPP and IP networks using Mobile IP

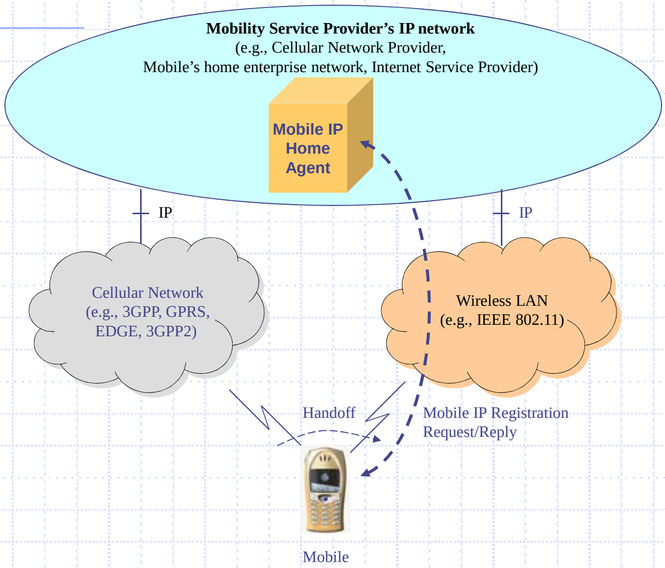
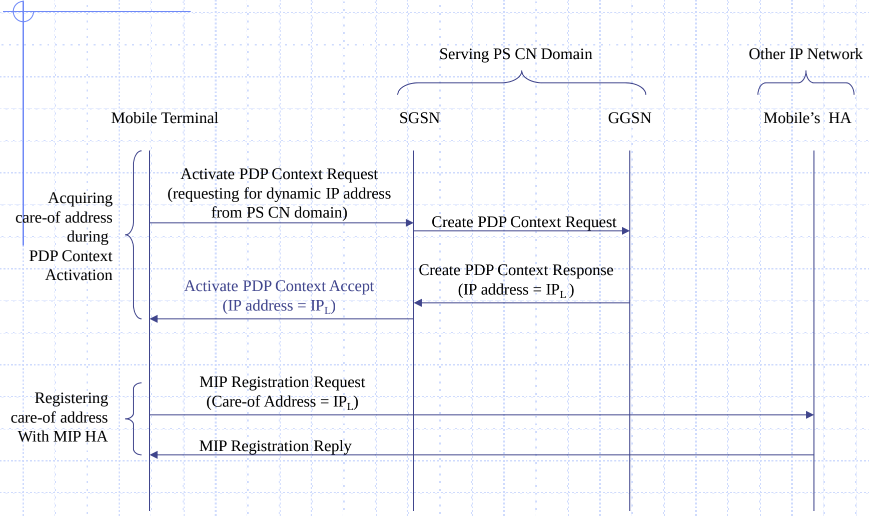

Mobility Service Provider's IP network
(e.g., Cellular Network Provider,
Mobile's home enterprise network, Internet Service Provider)
Mobile IP Home Agent
IP
IP
Cellular Network
(e.g., 3GPP, GPRS, EDGE, 3GPP2)
Wireless LAN
(e.g., IEEE 802.11)
Handoff
Mobile IP Registration Request/Reply
Mobile

Fig. 4.54 Sample signaling flow for handoff between 3GPP and IP networks using MIPv4



Serving PS CN Domain

Other IP Network

Mobile Terminal

SGSN

GGSN

Mobile's HA

Acquiring care-of address during PDP Context Activation

Activate PDP Context Request (requesting for dynamic IP address from PS CN domain)

Create PDP Context Request

Create PDP Context Response (IP address = IP_L)

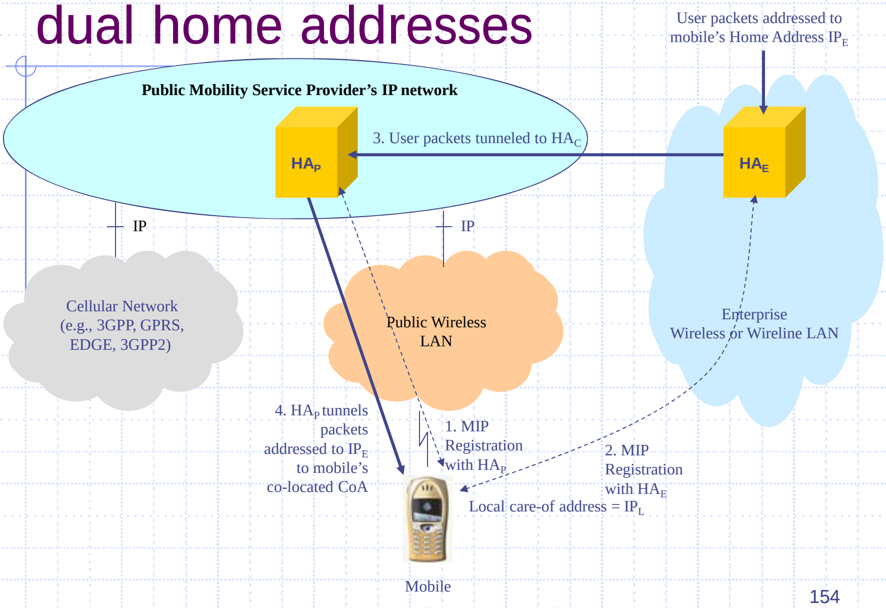
Activate PDP Context Accept (IP address = IP_L)

Registering care-of address With MIP HA

MIP Registration Request (Care-of Address = IP_L)

MIP Registration Reply

Fig. 4.55 Mobile terminals with dual home addresses



User packets addressed to mobile's Home Address IP_E

Public Mobility Service Provider's IP network

HA_P

3. User packets tunneled to HA_C

HA_E

IP

IP

Cellular Network (e.g., 3GPP, GPRS, EDGE, 3GPP2)

Public Wireless LAN

Enterprise Wireless or Wireline LAN

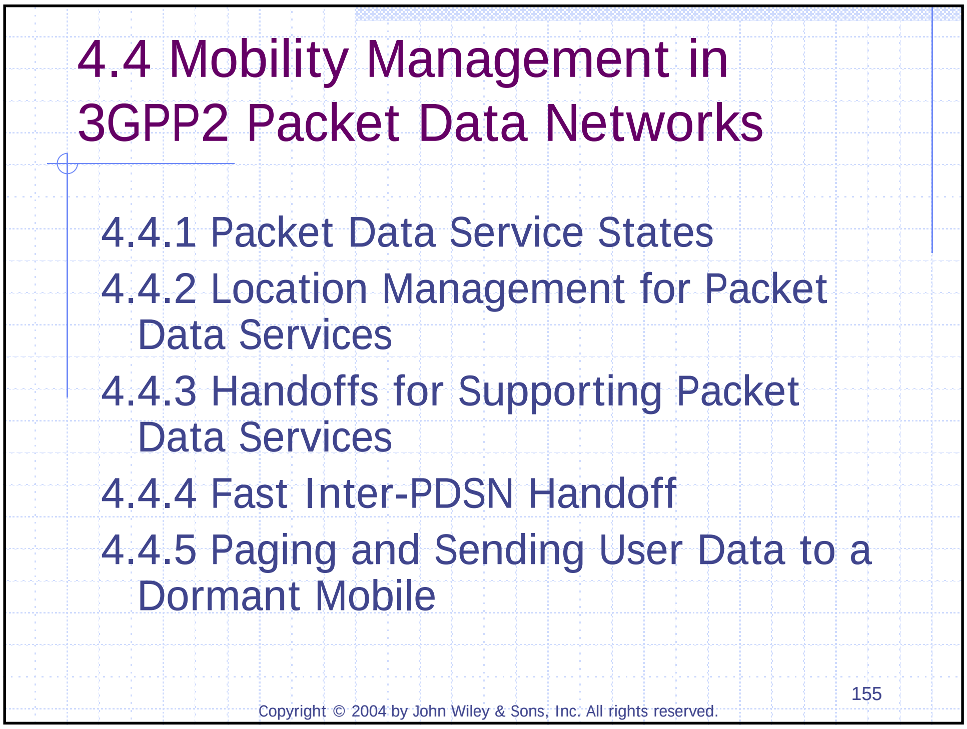
4. HA_P tunnels packets addressed to IP_E to mobile's co-located CoA

1. MIP Registration with HA_P

2. MIP Registration with HA_E

Local care-of address = IP_L

Mobile



4.4 Mobility Management in 3GPP2 Packet Data Networks

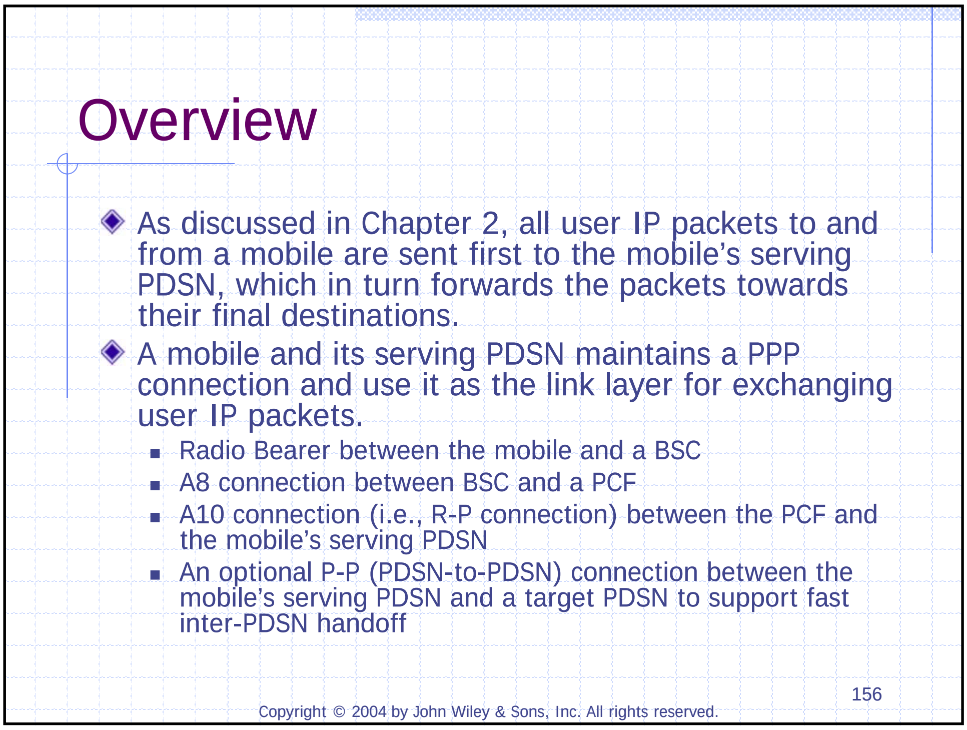
4.4.1 Packet Data Service States

4.4.2 Location Management for Packet Data Services

4.4.3 Handoffs for Supporting Packet Data Services

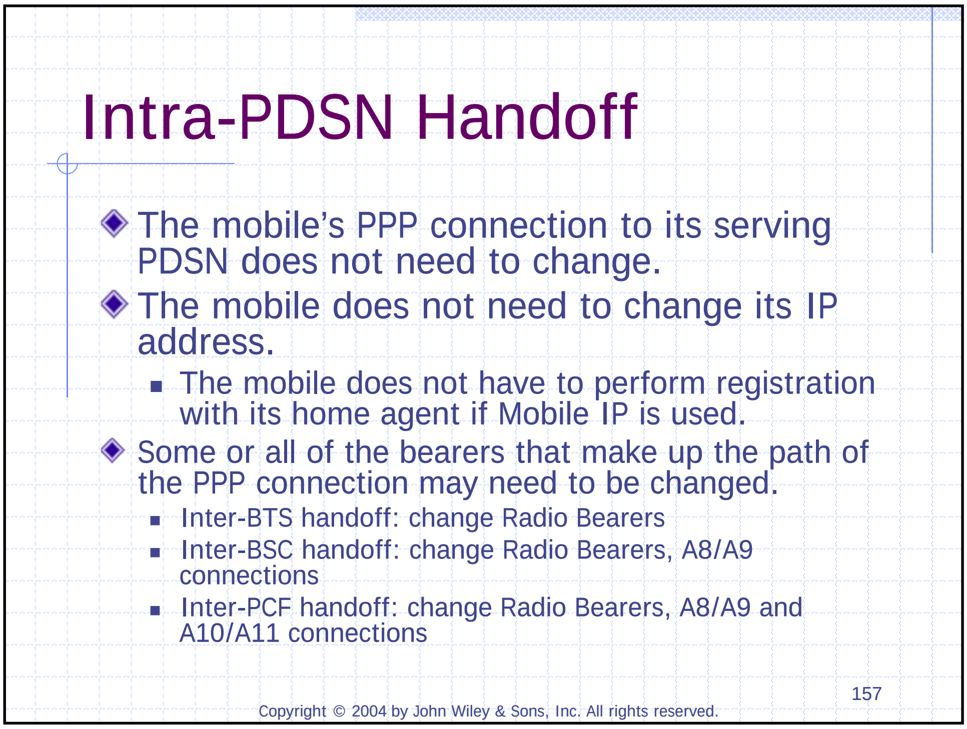
4.4.4 Fast Inter-PDSN Handoff

4.4.5 Paging and Sending User Data to a Dormant Mobile



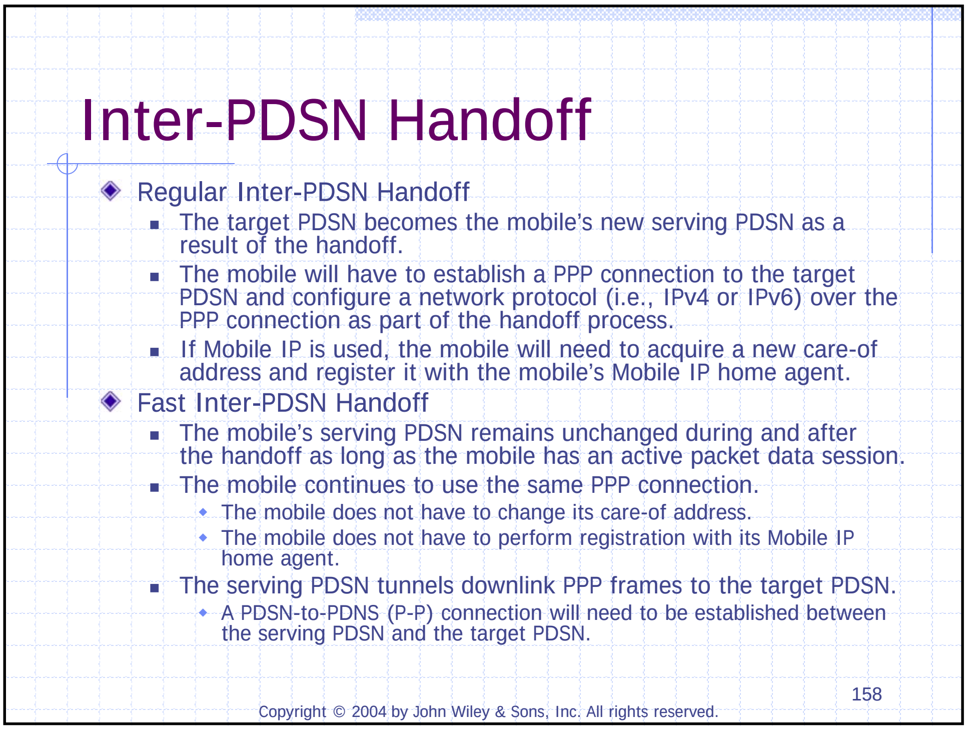
Overview

- As discussed in Chapter 2, all user IP packets to and from a mobile are sent first to the mobile's serving PDSN, which in turn forwards the packets towards their final destinations.
- A mobile and its serving PDSN maintains a PPP connection and use it as the link layer for exchanging user IP packets.
  - Radio Bearer between the mobile and a BSC
  - A8 connection between BSC and a PCF
  - A10 connection (i.e., R-P connection) between the PCF and the mobile's serving PDSN
  - An optional P-P (PDSN-to-PDSN) connection between the mobile's serving PDSN and a target PDSN to support fast inter-PDSN handoff



Intra-PDSN Handoff

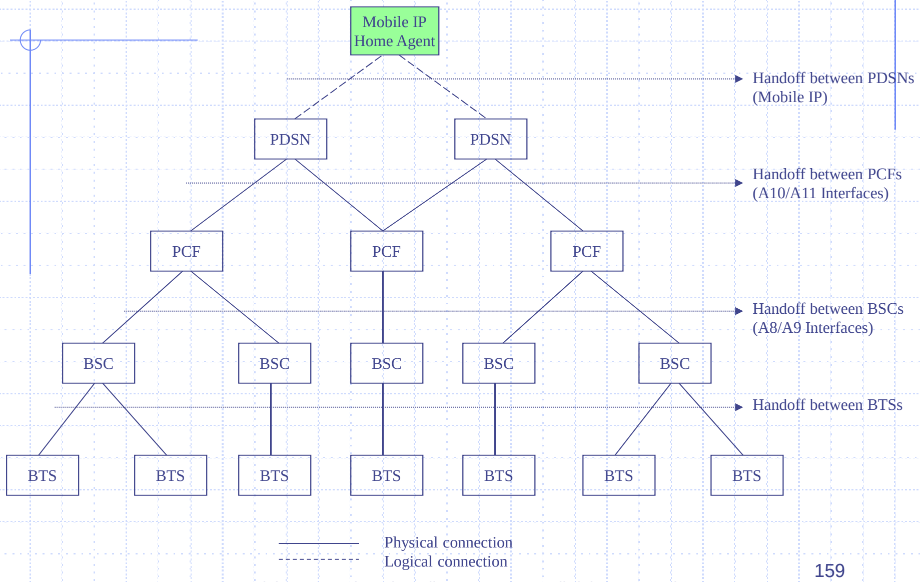
- The mobile's PPP connection to its serving PDSN does not need to change.
- The mobile does not need to change its IP address.
  - The mobile does not have to perform registration with its home agent if Mobile IP is used.
- Some or all of the bearers that make up the path of the PPP connection may need to be changed.
  - Inter-BTS handoff: change Radio Bearers
  - Inter-BSC handoff: change Radio Bearers, A8/A9 connections
  - Inter-PCF handoff: change Radio Bearers, A8/A9 and A10/A11 connections



Inter-PDSN Handoff

- Regular Inter-PDSN Handoff
  - The target PDSN becomes the mobile's new serving PDSN as a result of the handoff.
  - The mobile will have to establish a PPP connection to the target PDSN and configure a network protocol (i.e., IPv4 or IPv6) over the PPP connection as part of the handoff process.
  - If Mobile IP is used, the mobile will need to acquire a new care-of address and register it with the mobile's Mobile IP home agent.
- Fast Inter-PDSN Handoff
  - The mobile's serving PDSN remains unchanged during and after the handoff as long as the mobile has an active packet data session.
  - The mobile continues to use the same PPP connection.
    - The mobile does not have to change its care-of address.
    - The mobile does not have to perform registration with its Mobile IP home agent.
  - The serving PDSN tunnels downlink PPP frames to the target PDSN.
    - A PDSN-to-PDNS (P-P) connection will need to be established between the serving PDSN and the target PDSN.

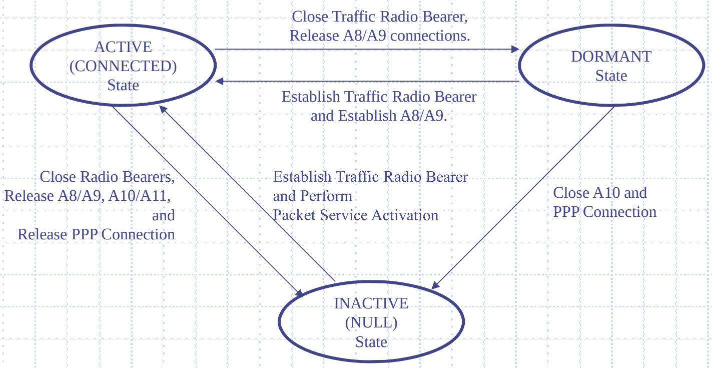
Fig. 5.56 Scopes of mobility in a 3GPP2 packet data network



4.4.1 Packet Data Service States

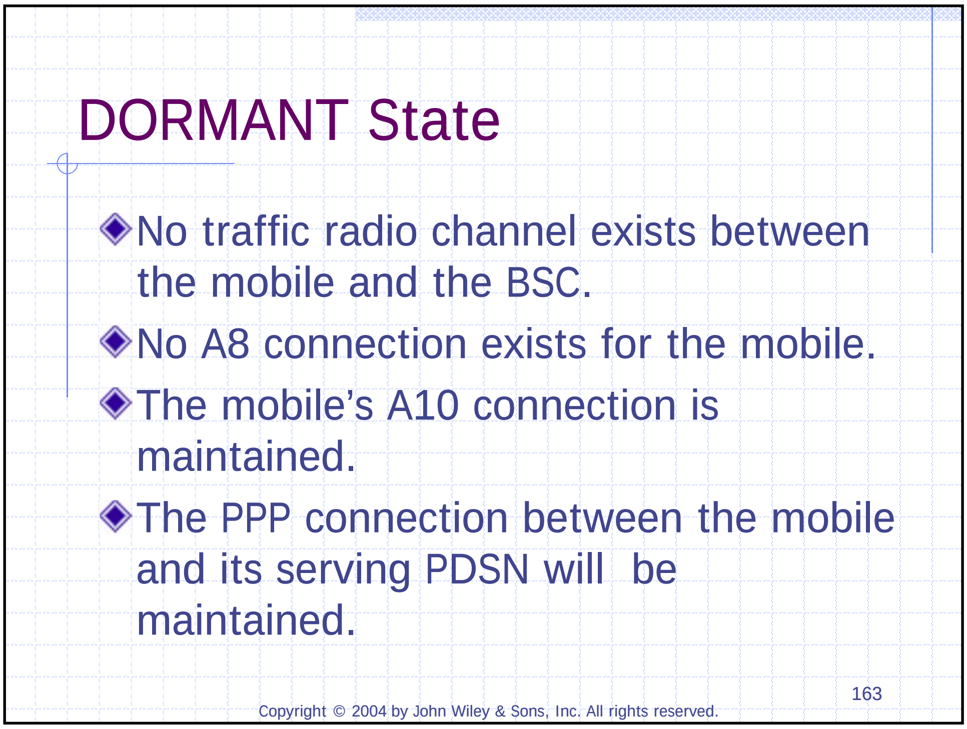
- ACTIVE/CONNECTED state
- DORMANT state
- NULL/INACTIVE state

Fig. 4.57 3GPP2 Packet Data Service State transitions


ACTIVE (CONNECTED) State
DORMANT State
INACTIVE (NULL) State
Close Traffic Radio Bearer, Release A8/A9 connections.
Establish Traffic Radio Bearer and Establish A8/A9.
Close Radio Bearers, Release A8/A9, A10/A11, and Release PPP Connection
Establish Traffic Radio Bearer and Perform Packet Service Activation
Close A10 and PPP Connection

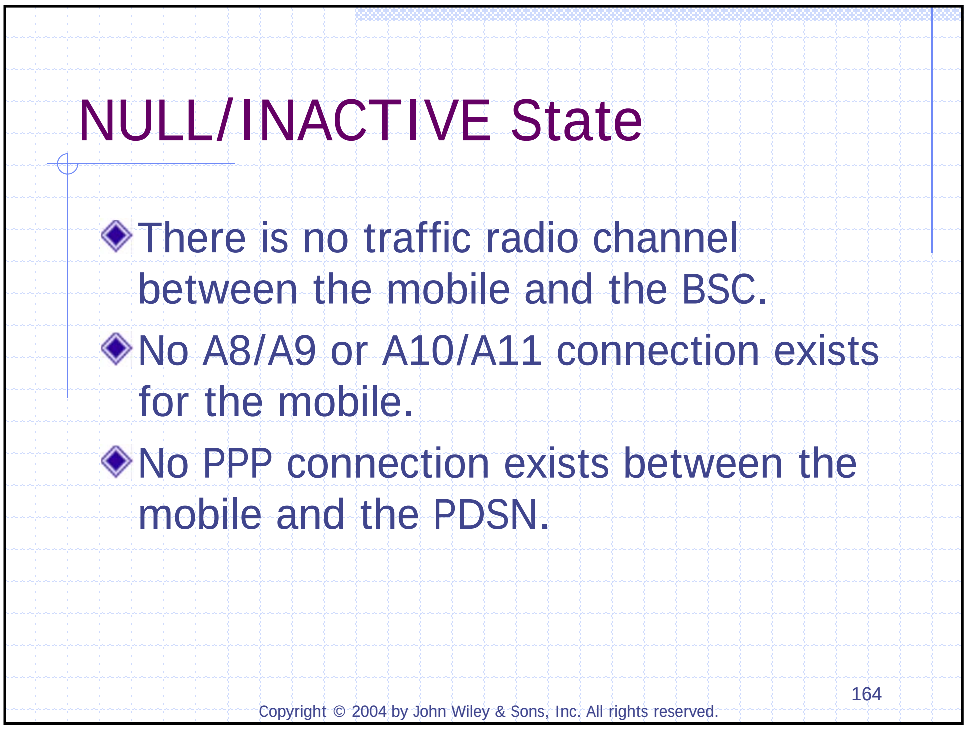
ACTIVE/CONNECTED State

- A bidirectional traffic radio channel is established between the mobile and the BSC.
- The A8/A9 and A10/A11 connections are established for the mobile.
- The mobile and its serving PDSN maintains a PPP connection.
- When Mobile IP is used for mobility management, the mobile will have already performed Mobile IP registration with its home agent.



DORMANT State

- No traffic radio channel exists between the mobile and the BSC.
- No A8 connection exists for the mobile.
- The mobile's A10 connection is maintained.
- The PPP connection between the mobile and its serving PDSN will be maintained.



NULL/INACTIVE State

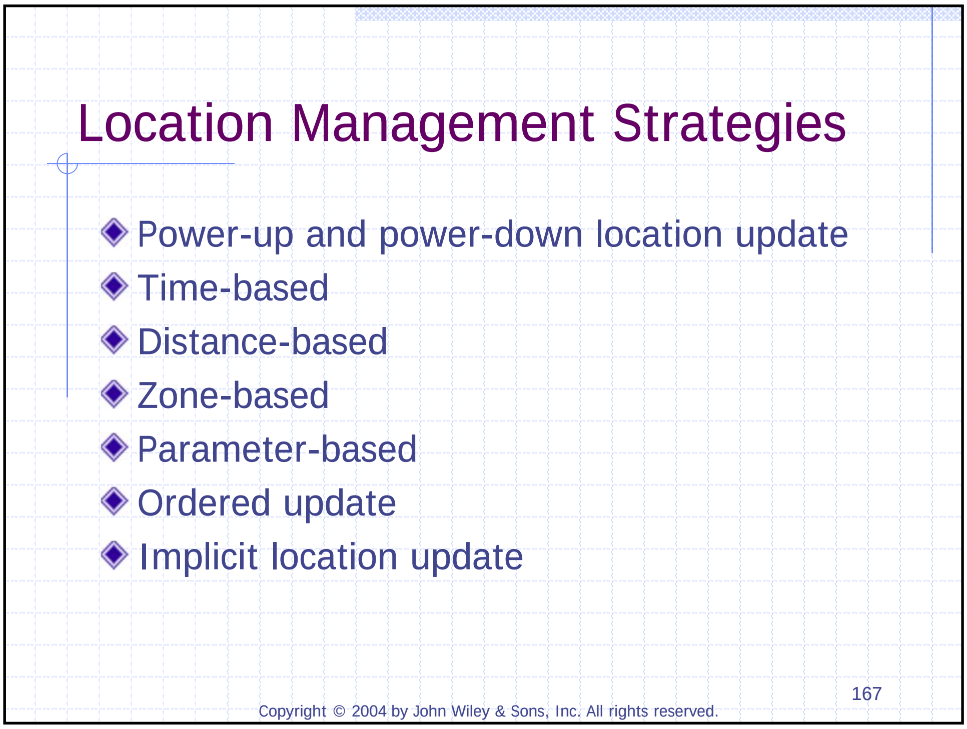
- There is no traffic radio channel between the mobile and the BSC.
- No A8/A9 or A10/A11 connection exists for the mobile.
- No PPP connection exists between the mobile and the PDSN.

State Maintenance

- The Packet Data Service States are maintained in both PCF and mobile terminal.
- The PDSN will not be aware whether a mobile is in Active or DORMANT state.

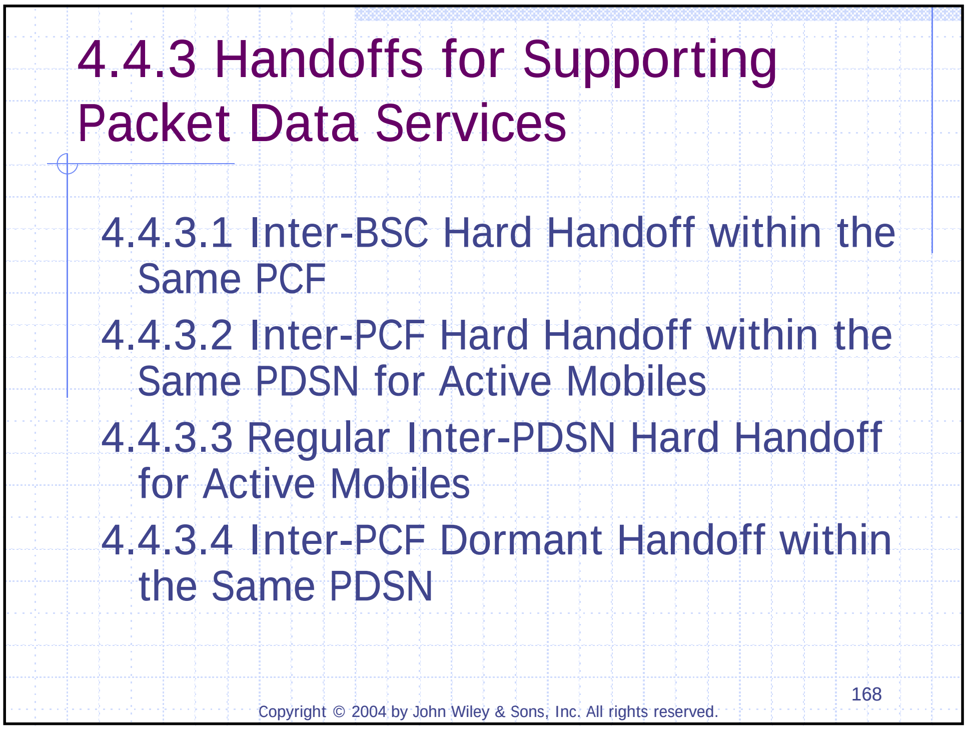
4.4.2 Location Management for Packet Data Services

- Packet Zone: geographical area served by a single PCF
  - uniquely identified by a Packet Zone ID (PZID)
- Each BS periodically broadcasts, over the broadcast radio channels, the PZID of the Packet Zone it serves.
- A dormant mobile will be able to receive such broadcast system information and use it to determine whether it has moved into a new Packet Zone.
  - 3GPP2 does not define any new protocol, message, or procedure uniquely for performing Packet Zone update.
  - The procedure for inter-PCF dormant handoff is used to serve the purpose of Packet Zone update.



Location Management Strategies

- Power-up and power-down location update
- Time-based
- Distance-based
- Zone-based
- Parameter-based
- Ordered update
- Implicit location update



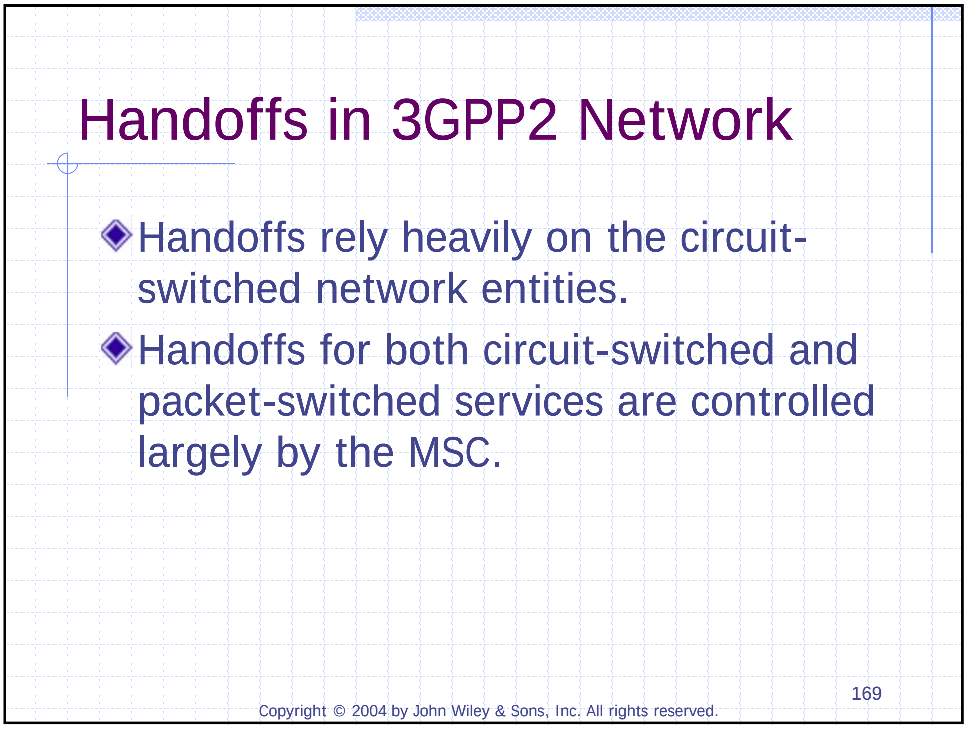
4.4.3 Handoffs for Supporting Packet Data Services

4.4.3.1 Inter-BSC Hard Handoff within the Same PCF

4.4.3.2 Inter-PCF Hard Handoff within the Same PDSN for Active Mobiles

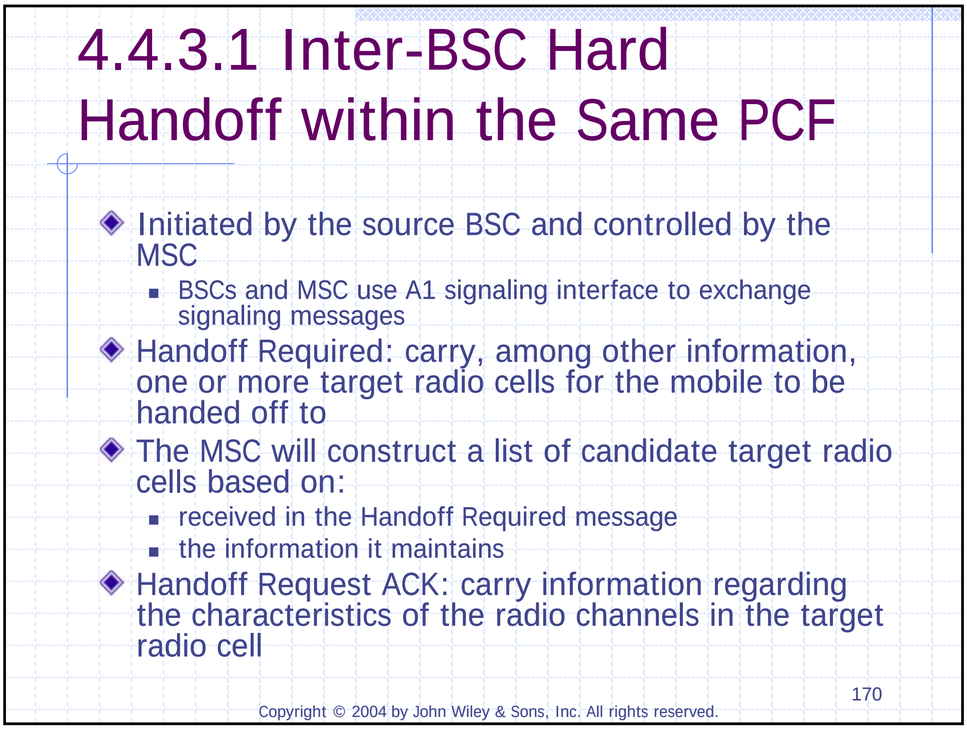
4.4.3.3 Regular Inter-PDSN Hard Handoff for Active Mobiles

4.4.3.4 Inter-PCF Dormant Handoff within the Same PDSN



Handoffs in 3GPP2 Network

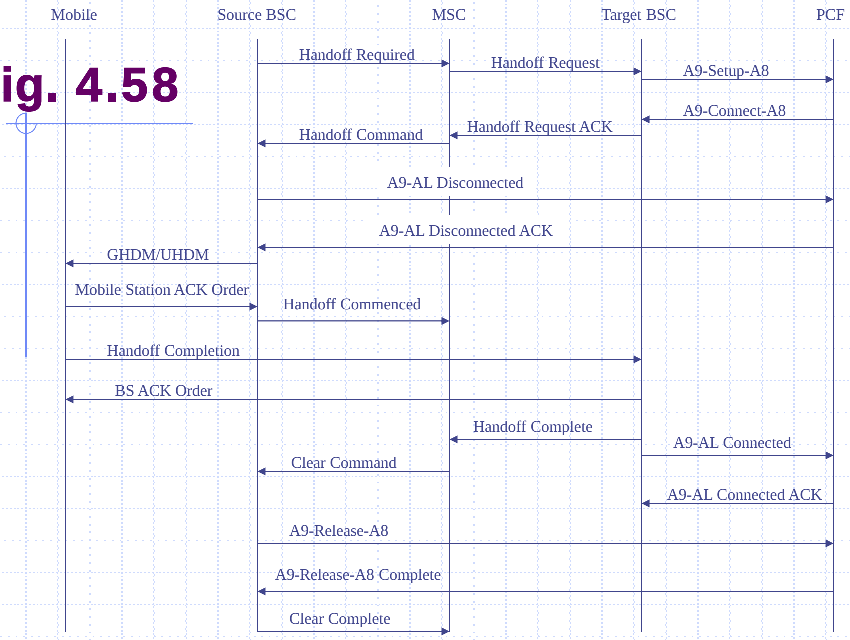
- Handoffs rely heavily on the circuit-switched network entities.
- Handoffs for both circuit-switched and packet-switched services are controlled largely by the MSC.



4.4.3.1 Inter-BSC Hard Handoff within the Same PCF

- Initiated by the source BSC and controlled by the MSC
  - BSCs and MSC use A1 signaling interface to exchange signaling messages
- Handoff Required: carry, among other information, one or more target radio cells for the mobile to be handed off to
- The MSC will construct a list of candidate target radio cells based on:
  - received in the Handoff Required message
  - the information it maintains
- Handoff Request ACK: carry information regarding the characteristics of the radio channels in the target radio cell

Fig. 4.58



Mobile | Source BSC | MSC | Target BSC | PCF

- Handoff Required
- Handoff Request
- A9-Setup-A8
- A9-Connect-A8
- Handoff Request ACK
- Handoff Command
- A9-AL Disconnected
- A9-AL Disconnected ACK
- GHDM/UHDM
- Mobile Station ACK Order
- Handoff Commenced
- Handoff Completion
- BS ACK Order
- Handoff Complete
- A9-AL Connected
- Clear Command
- A9-AL Connected ACK
- A9-Release-A8
- A9-Release-A8 Complete
- Clear Complete

4.4.3.2 Inter-PCF Hard Handoff within the Same PDSN for Active Mobiles

- Initiated by the source BSC
- Handoff Required: carry information to indicate that the requested handoff is for packet-switched services and is an inter-PCF hard handoff
  - PDSN IP Address
  - Protocol Type: identifies the Link-Layer protocol used at the mobile and its serving PDSN to exchange user IP packets
- A11 Registration Request
  - As discussed in Chapter 2, the A11 Registration Request uses the same format as the MIPv4 Registration Request (Figure 4.12).
    - Care-of Address field: set to the IP address of the target PCF
    - Home Agent field: set to the IP address of the PDSN
    - Home Address field: set to zero to indicate that the requested A10 connection is for supporting an intra-PDSN handoff

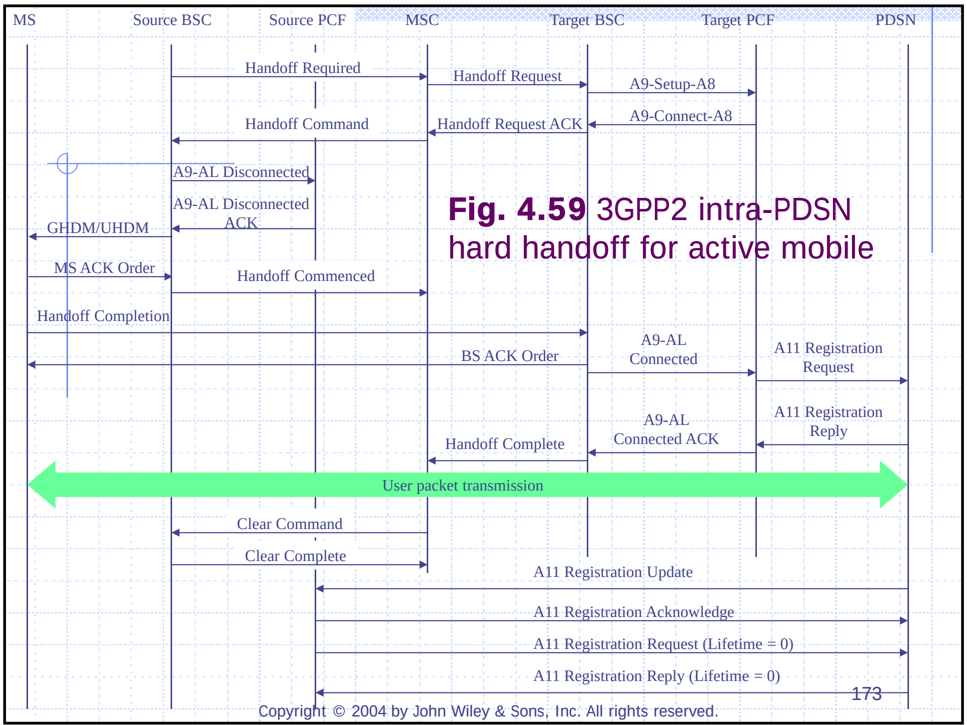


Fig. 4.59 3GPP2 intra-PDSN hard handoff for active mobile

4.4.3.3 Regular Inter-PDSN Hard Handoff for Active Mobiles

- No P-P interface is implemented between the mobile's serving PDSN and the target PDSN.
- The target PCF will have to select a target PDSN for each mobile that is performing inter-PDSN handoff.
  - How to determine which PDSN should be the target PDSN for a mobile is an implementation issue.
- The target PDSN becomes the mobile's new serving PDSN after the handoff.
  - The mobile needs to establish a new PPP connection to the target PDSN during the handoff process.
  - The mobile has to use a new care-of address after it is handed off to the target PDSN.
  - The mobile will need to perform Mobile IP registration.

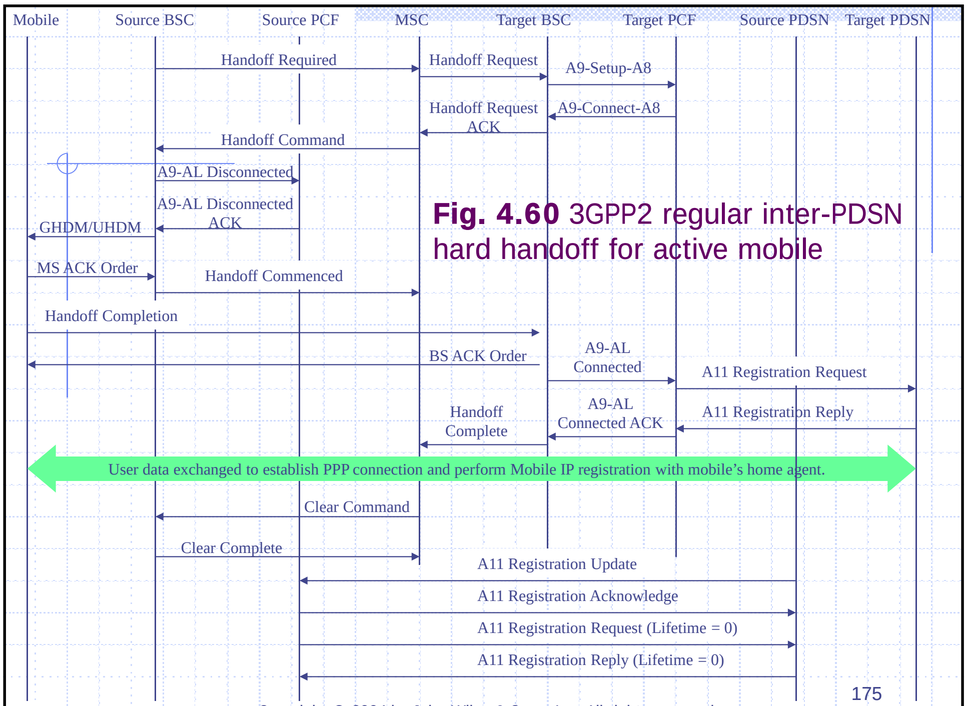
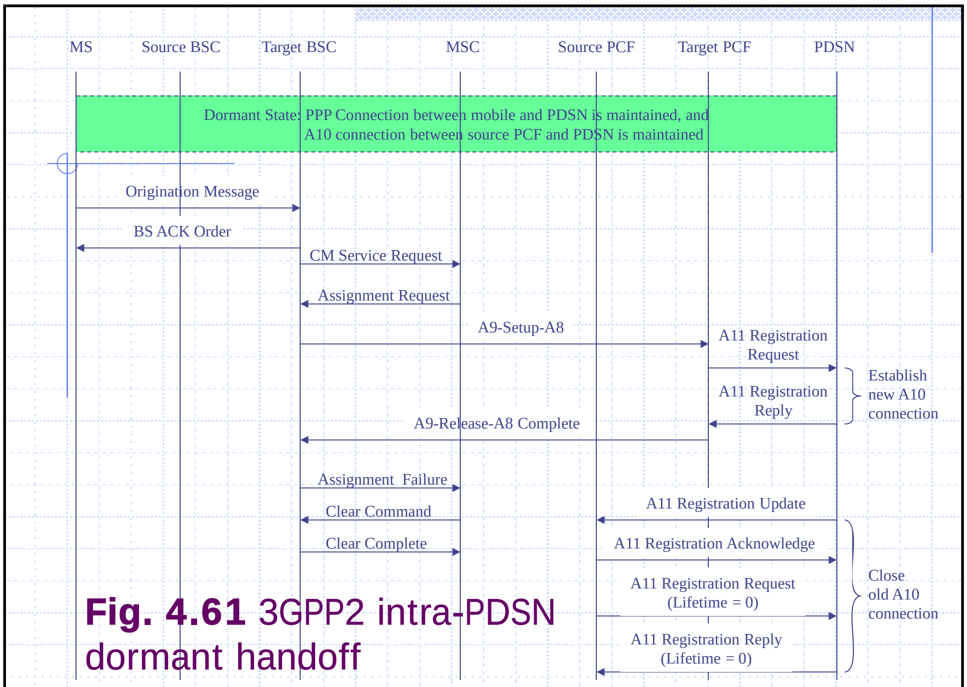


Fig. 4.60 3GPP2 regular inter-PDSN hard handoff for active mobile

4.4.3.4 Inter-PCF Dormant Handoff within the Same PDSN

- Initiated by a mobile
- May be performed when the mobile detects a change of the Packet Zone ID (PZID), Network ID (NID) or System ID (SID)
  - When triggered by a change of PZID, it also serves the purpose of Packet Zone update.
- The main task is to establish a new A10 connection between the target PCF and the PDSN.
- The A11 Registration Reply message to the target PCF carries an indication to inform the target PCF whether the PDSN has user data to send to the mobile at the moment.
  - If the PDSN has no user data to send to the mobile: The target PCF will reply to the target BSC with an A9-Release-A8 Complete message.
  - If the PDSN has user data to send to the mobile: The target PCF will reply to the target BSC with an A9-Connect-A8 message.
- Assignment Failure: carry a Failure Cause value indicating Packet Call Going Dormant rather than any real failure



MS
Source BSC
Target BSC
MSC
Source PCF
Target PCF
PDSN

Dormant State: PPP Connection between mobile and PDSN is maintained, and A10 connection between source PCF and PDSN is maintained

Origination Message
BS ACK Order
CM Service Request
Assignment Request
A9-Setup-A8
A11 Registration Request
A11 Registration Reply
Establish new A10 connection
A9-Release-A8 Complete
Assignment Failure
Clear Command
Clear Complete
A11 Registration Update
A11 Registration Acknowledge
A11 Registration Request (Lifetime = 0)
A11 Registration Reply (Lifetime = 0)
Close old A10 connection

Fig. 4.61 3GPP2 intra-PDSN dormant handoff

4.4.4 Fast Inter-PDSN Handoff

- Can only be supported when a mobile is in ACTIVE state
- The mobile's serving PDSN remains unchanged as long as the mobile's Packet Data Service State remains in ACTIVE state.
- The mobile does not renegotiate its PPP connection.

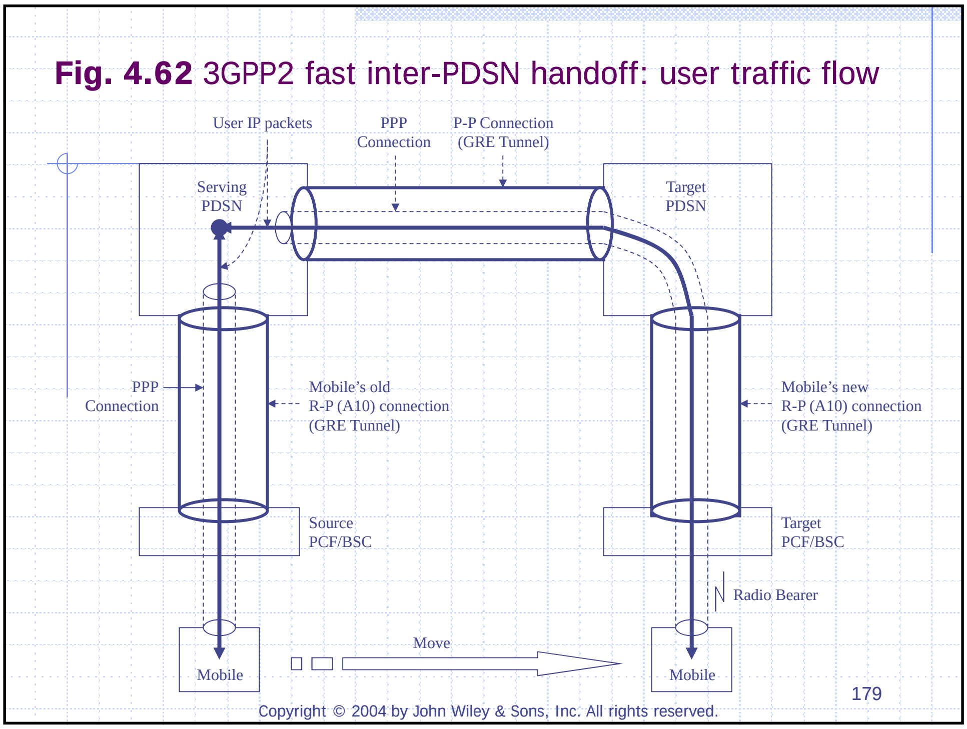
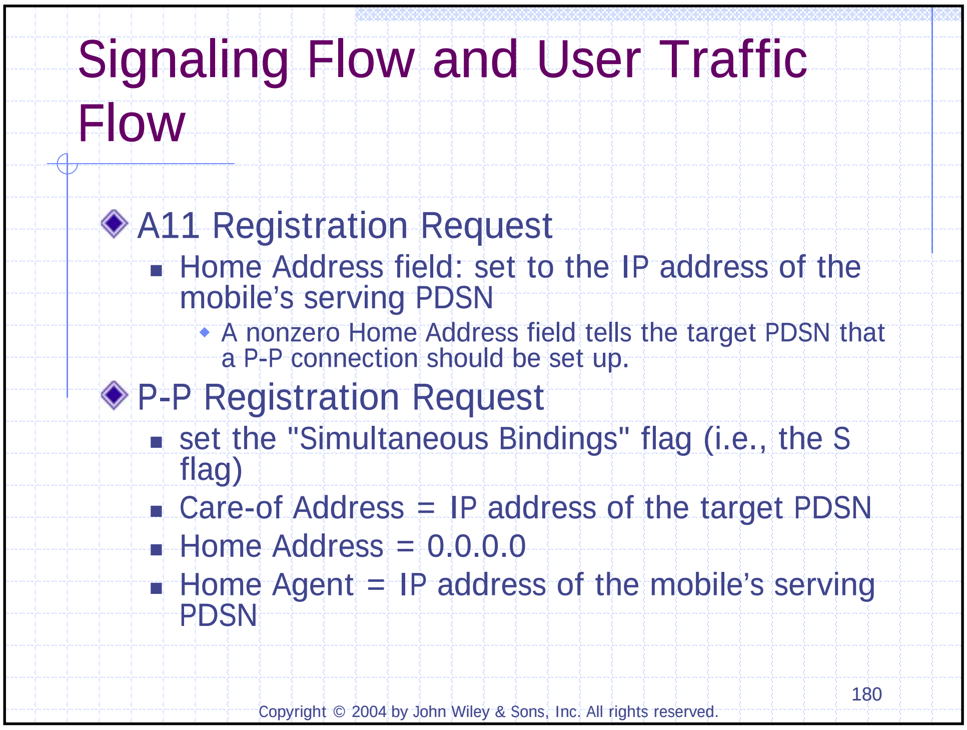


Fig. 4.62 3GPP2 fast inter-PDSN handoff: user traffic flow

179

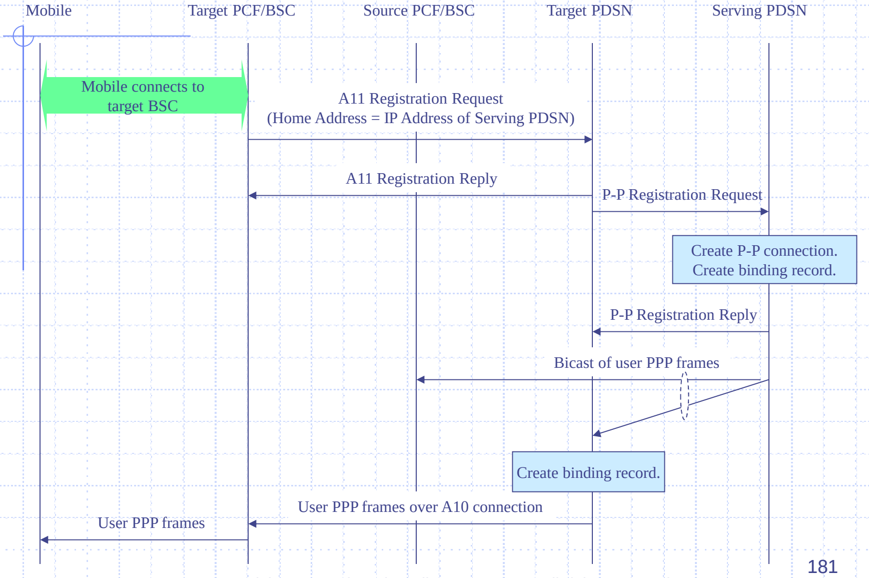


Signaling Flow and User Traffic Flow

- A11 Registration Request
  - Home Address field: set to the IP address of the mobile's serving PDSN
    - A nonzero Home Address field tells the target PDSN that a P-P connection should be set up.
- P-P Registration Request
  - set the "Simultaneous Bindings" flag (i.e., the S flag)
  - Care-of Address = IP address of the target PDSN
  - Home Address = 0.0.0.0
  - Home Agent = IP address of the mobile's serving PDSN

180

Fig. 4.63 3GPP2 fast inter-PDSN handoff: signaling flow and user traffic flow



Mobile

Target PCF/BSC

Source PCF/BSC

Target PDSN

Serving PDSN

Mobile connects to target BSC

A11 Registration Request
(Home Address = IP Address of Serving PDSN)

A11 Registration Reply

P-P Registration Request

Create P-P connection.
Create binding record.

P-P Registration Reply

Bicast of user PPP frames

Create binding record.

User PPP frames over A10 connection

User PPP frames

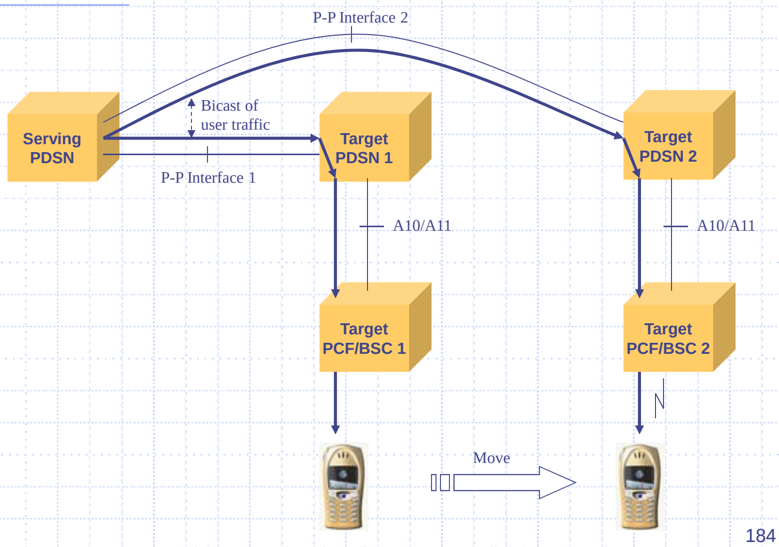
Enter DORMANT State

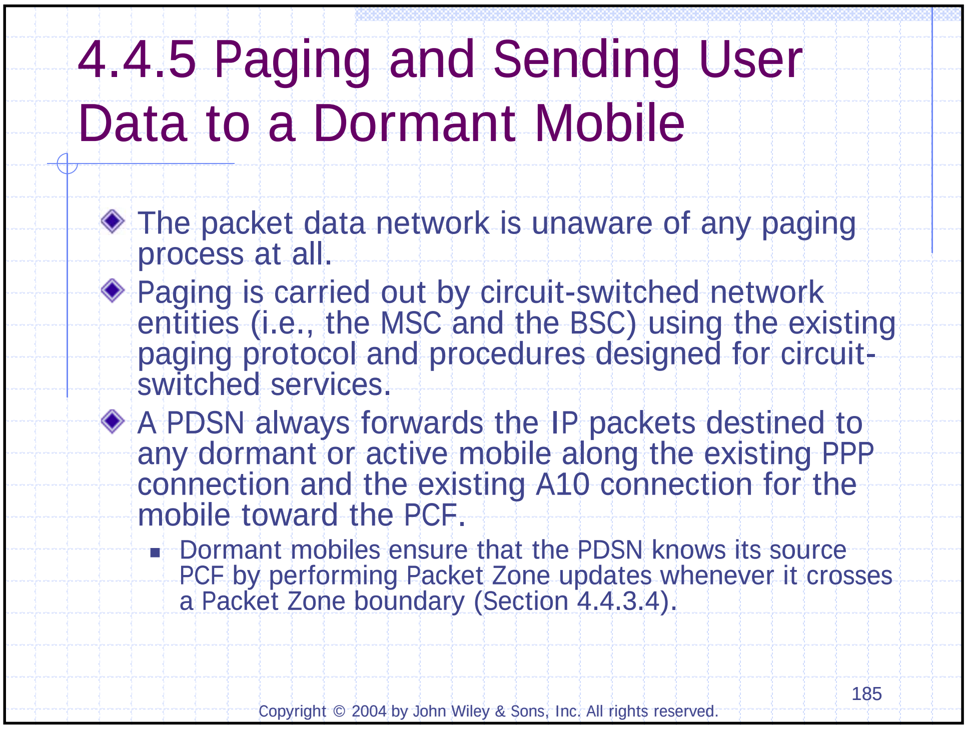
- When the mobile plans to transition into DORMANT state, its serving PDSN will have to be changed to the target PDSN first.
- As an A10 connection has already been established between the target PCF/BSC and the target PDSN during the fast inter-PDSN handoff process, the mobile will only need to establish a PPP connection to the target PDSN before the mobile changes into DORMANT state.

Change Target PDSN

- Target PDSN 2 can use the same procedure described above to establish a P-P connection to the mobile's serving PDSN.
- The mobile's serving PDSN can bicast user PPP frames to both target PDSN 1 and target PDSN 2.

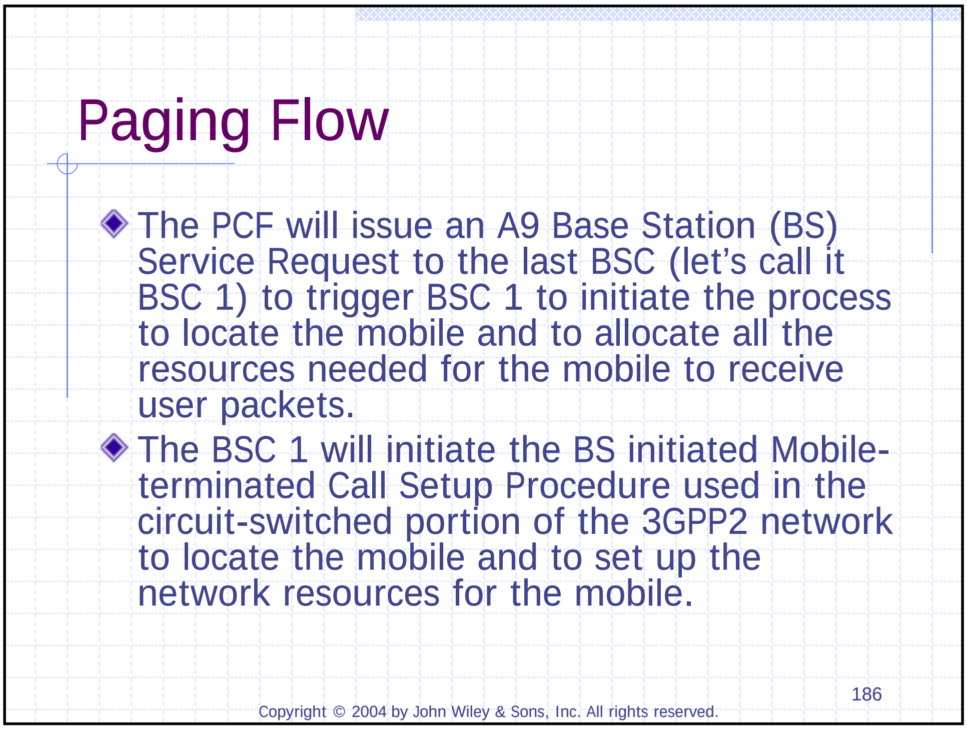
Fig. 4.64 3GPP2 fast inter-PDSN handoff from target PDSN 1 to target PDSN 2





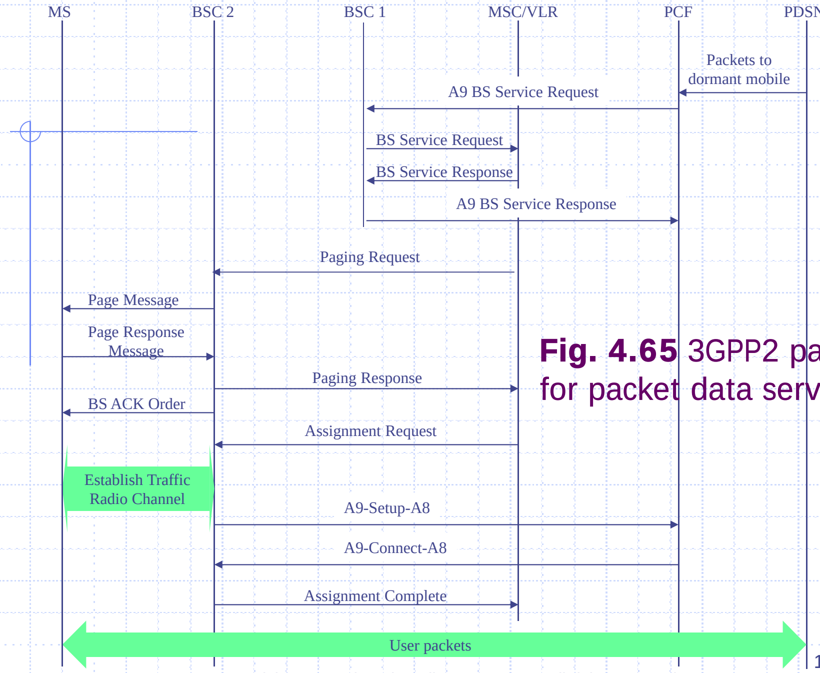
4.4.5 Paging and Sending User Data to a Dormant Mobile

- The packet data network is unaware of any paging process at all.
- Paging is carried out by circuit-switched network entities (i.e., the MSC and the BSC) using the existing paging protocol and procedures designed for circuit-switched services.
- A PDSN always forwards the IP packets destined to any dormant or active mobile along the existing PPP connection and the existing A10 connection for the mobile toward the PCF.
  - Dormant mobiles ensure that the PDSN knows its source PCF by performing Packet Zone updates whenever it crosses a Packet Zone boundary (Section 4.4.3.4).



Paging Flow

- The PCF will issue an A9 Base Station (BS) Service Request to the last BSC (let’s call it BSC 1) to trigger BSC 1 to initiate the process to locate the mobile and to allocate all the resources needed for the mobile to receive user packets.
- The BSC 1 will initiate the BS initiated Mobile-terminated Call Setup Procedure used in the circuit-switched portion of the 3GPP2 network to locate the mobile and to set up the network resources for the mobile.



MS

BSC 2

BSC 1

MSC/VLR

PCF

PDSN

Packets to dormant mobile

A9 BS Service Request

BS Service Request

BS Service Response

A9 BS Service Response

Paging Request

Page Message

Page Response Message

Paging Response

BS ACK Order

Assignment Request

Establish Traffic Radio Channel

A9-Setup-A8

A9-Connect-A8

Assignment Complete

User packets

Fig. 4.65 3GPP2 paging for packet data services

4.5 Mobility Management in MWIF Networks

- Use IP-based protocols defined or being developed by the IETF to support mobility
- Main functional entities for mobility management
  - Mobile Attendant (MA)
  - Home Mobility Manager (HMM)
  - Home IP Address Manager
  - IP Address Manager
  - Location Server
  - Geographical Location Manager (GLM)
  - Global Name Server (GNS)
  - Service Discovery Server
- MWIF recommended IETF protocols for the interface references point between the mobility management functional entities.

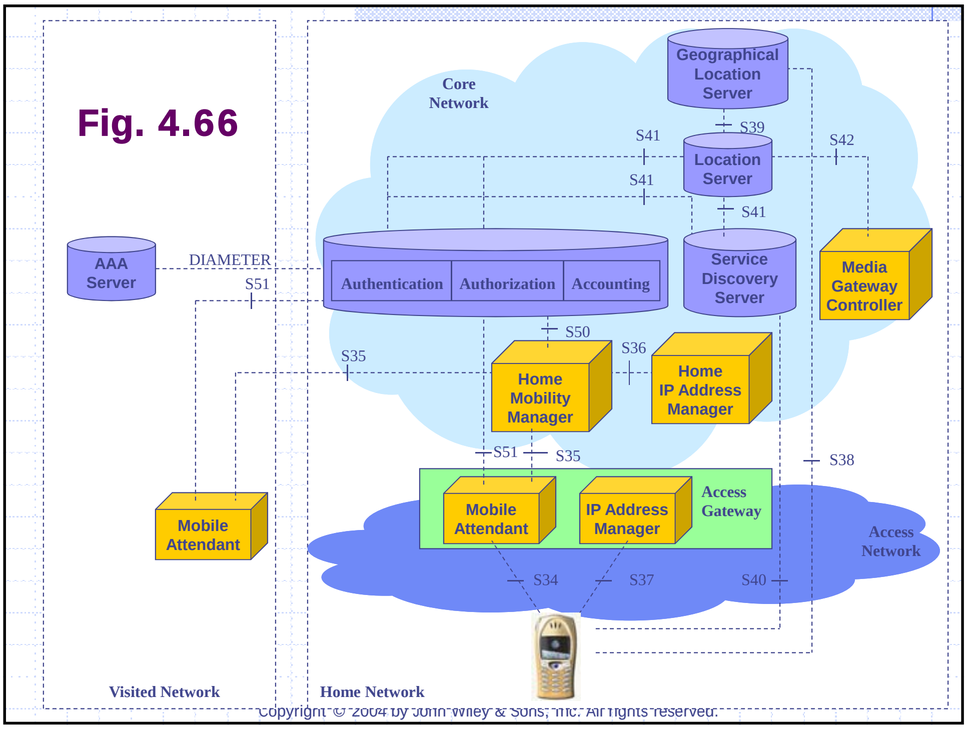
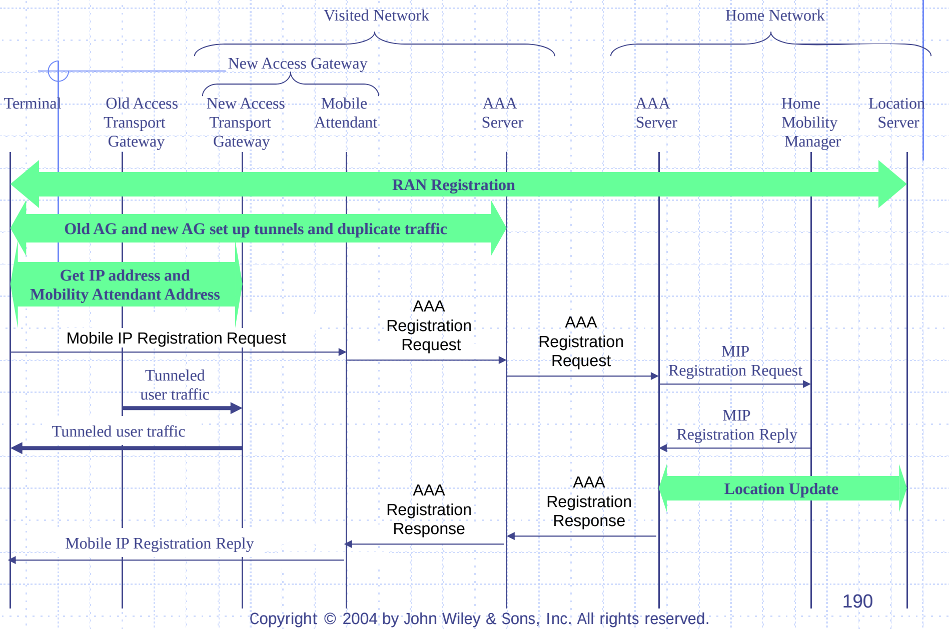


Fig. 4.66

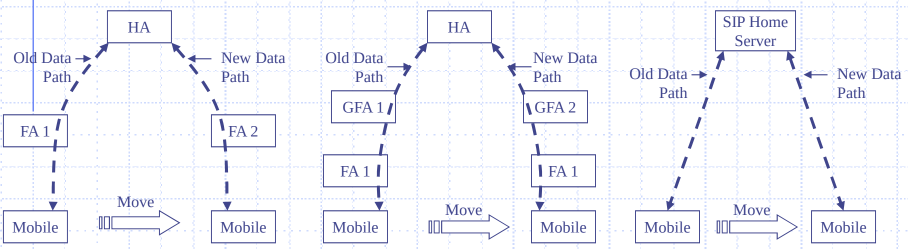
Fig. 4.67 MWIF handoff procedure



4.6 Comparison of Mobility Management in IP, 3GPP, and 3GPP2 Networks

- Similarity: They all use the *Relayed Delivery* strategy as the basic strategy for delivering packets to mobiles.
  - In particular, a *mobility anchor point* is used for tracking the mobile's locations and for relaying packets to mobiles.
- Differences
  - The ways packets are transported from one mobility protocol entity to another.
    - Regular IP, IP-in-IP tunnel, GTP, GRE, etc.
  - How location management is related to route management.
    - Regular IP routing, host-specific routing, etc.
  - Whether and how paging is supported.

Fig. 4.68 Simplified mobility management models used by Mobile IP, Mobile IP Regional Registration, and SIP mobility

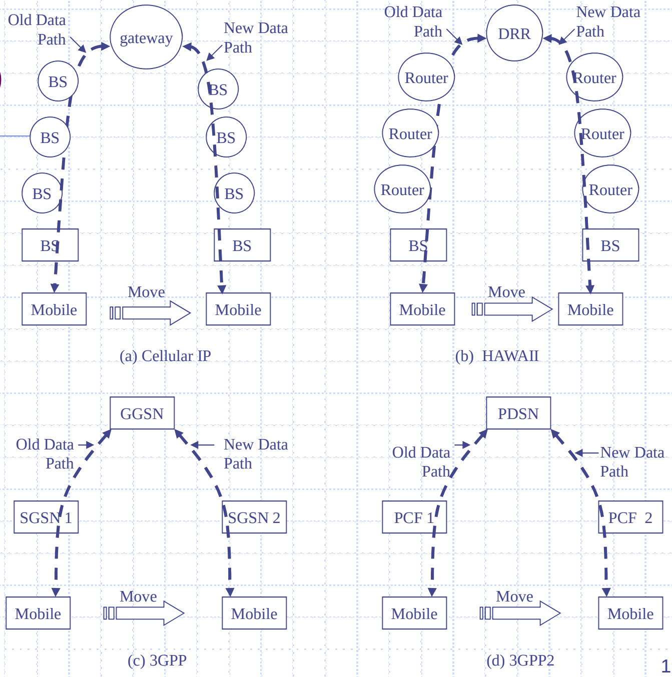


(a) Mobile IP

(b) Mobile IP Regional Registration

(c) SIP Mobility

Fig. 4.69



(a) Cellular IP

(b) HAWAII

(c) 3GPP

(d) 3GPP2

193