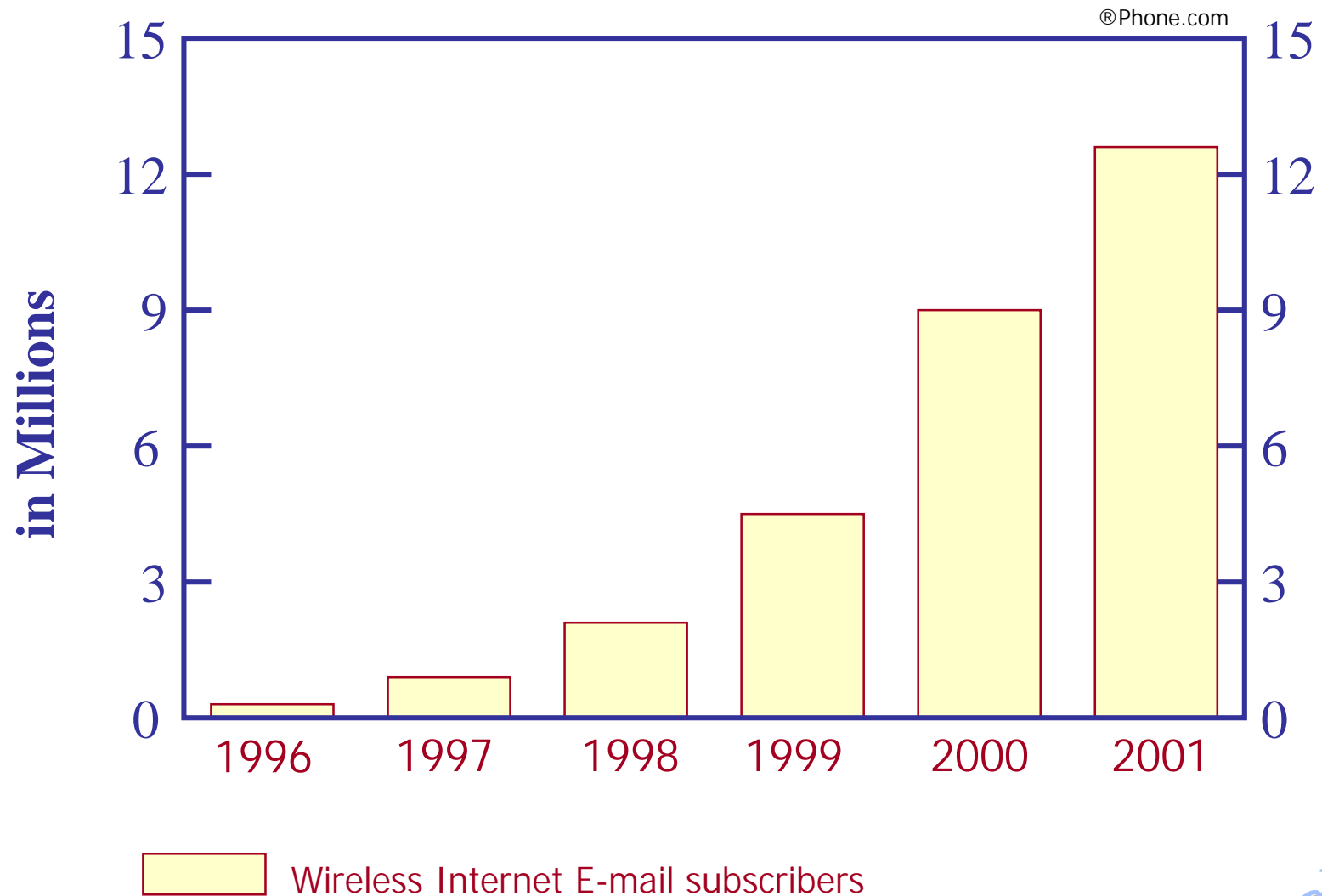


---

# Mobile IPv6

Tomás P. de Miguel  
DIT-UPM

# Internet Mobile Market



# Mobility

---

The ability to change locations, while connected to the network, accessing information services, anytime, anywhere.

- ◆ Access applications anywhere
  - ▶ Low bandwidth
  - ▶ Reduced battery life
- ◆ Maintain connections during movement
  - ▶ All messages sent to the mobile node are redirected to its real location
- ◆ More than portability
  - ▶ Operate at any point of attachment
  - ▶ Connections have to be shut down when node is moved

# Requirements

---

- ◆ Without geographical limitations
  - ▶ Portable computer work anywhere
- ◆ Network technology independent
  - ▶ Detect a local router and connect automatically
- ◆ Must able to communicate with other nodes that do not implement mobility
  - ▶ Communicate with any network node
  - ▶ Transparent to transport and application levels
- ◆ Without modification in the standard routing procedures or address formats
- ◆ Secure
  - ▶ Mobile node identification
  - ▶ Exchanged information protected

# IP connectivity

- ◆ Connections are identified by a data set

protocol	Source A.	Dest. A.	Source P.	Dest. P.
----------	-----------	----------	-----------	----------

- ◆ There are two attached points in each connection

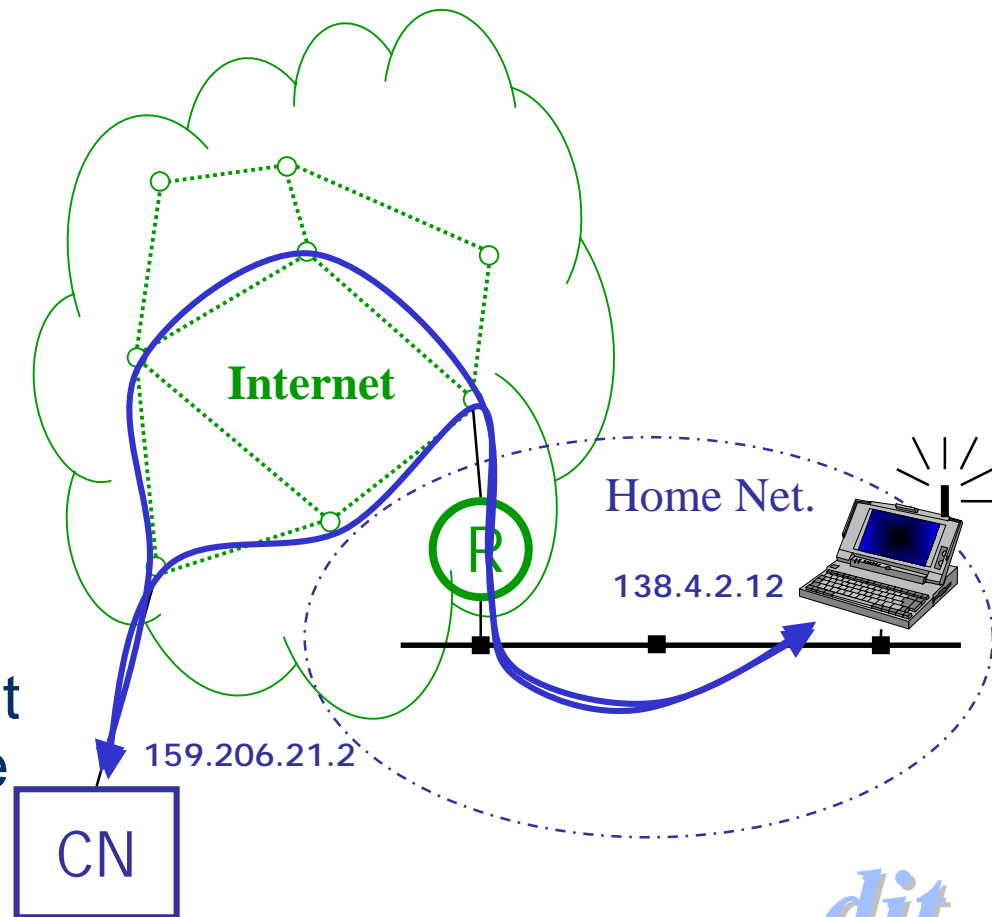
- ◆ The mobile node

- ◆ 138.4.2.12

- ◆ The correspondent node

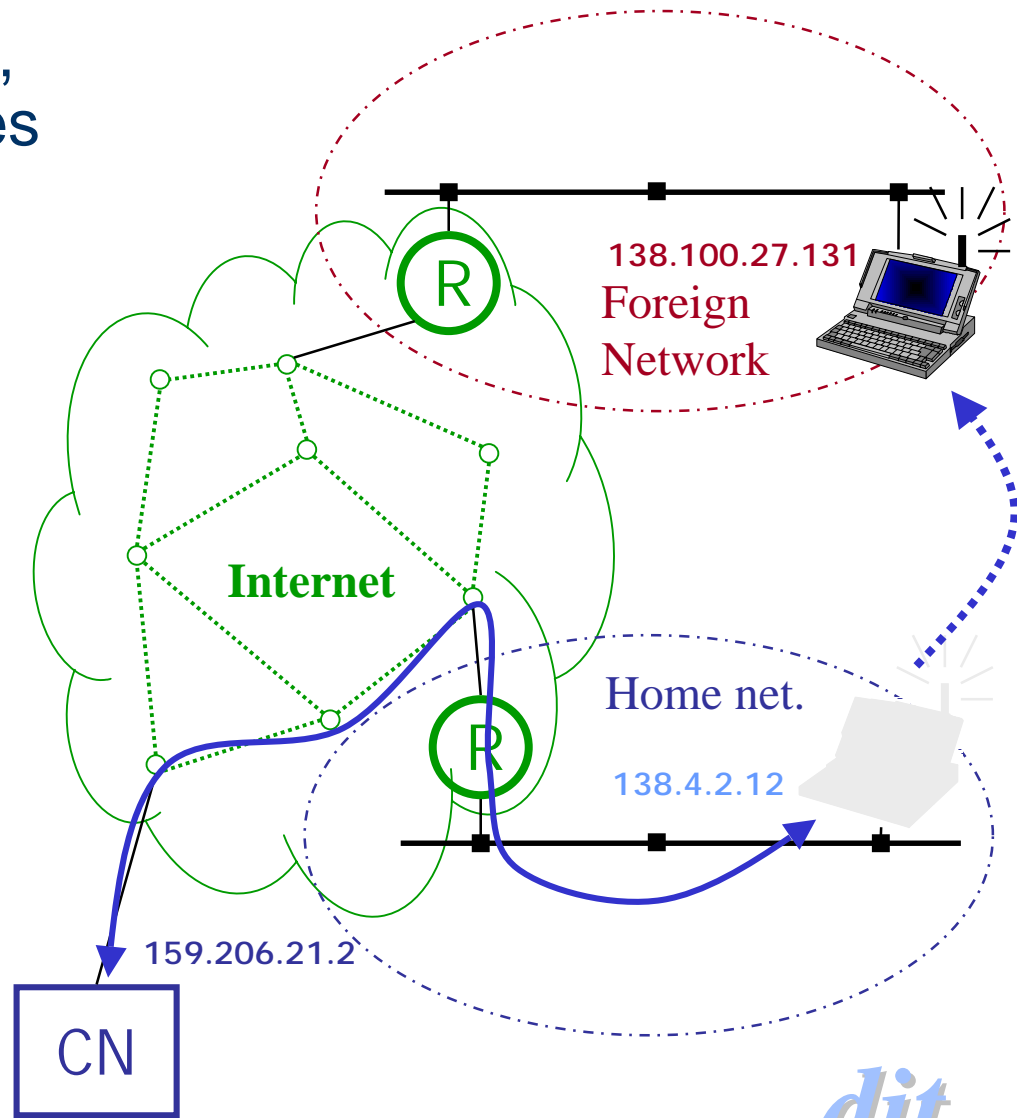
- ◆ 159.206.21.2

- ◆ Packets can be routed using different ways, but attached points must be always the same.



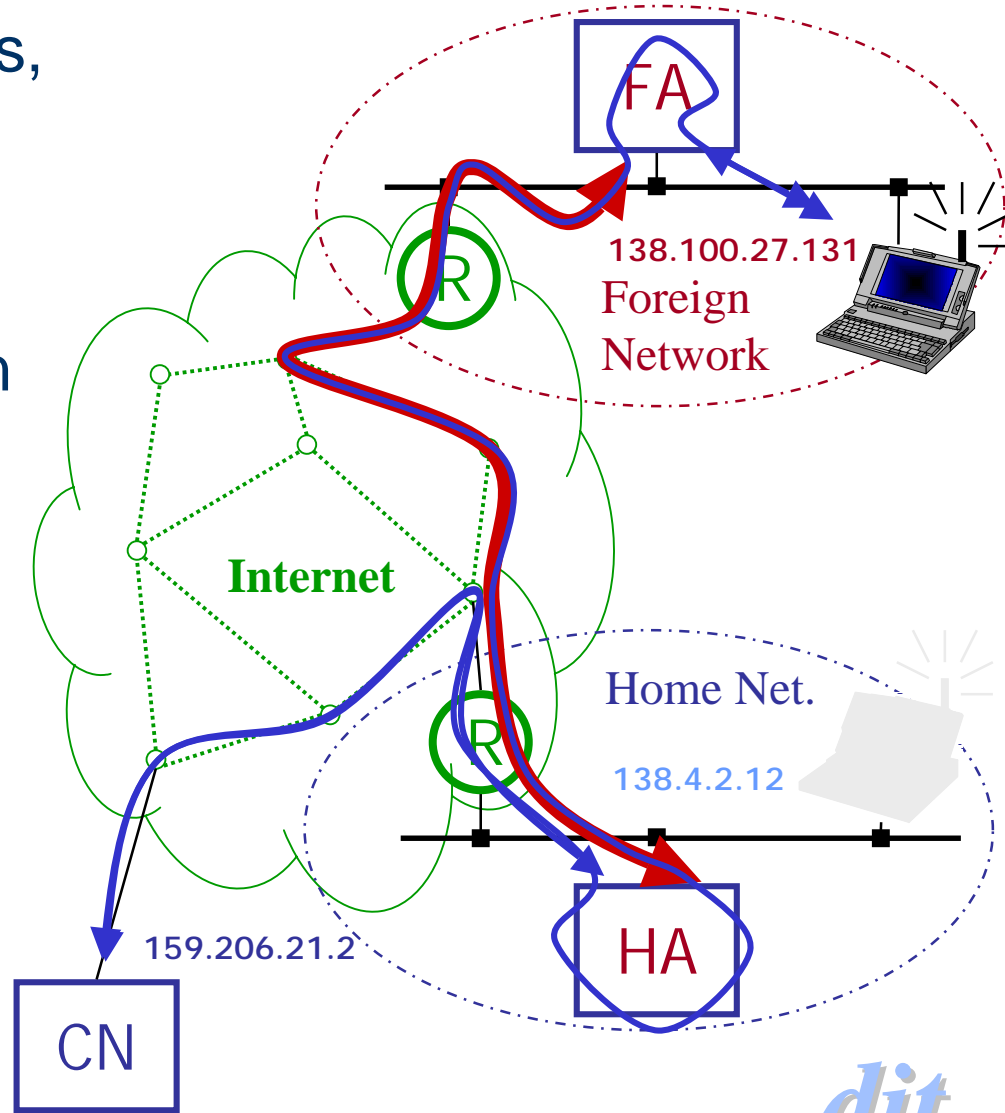
# IP mobility

- ◆ When location changes, then IP address changes
- ◆ All packets should be routed to the new address
- ◆ However, application should maintain original defined addresses
- ◆ Otherwise, established connections are lost



# IP mobility service

- ◆ To maintain connections, the traffic must be redirected to the new location
- ◆ All the traffic connection between home and foreign network is encapsulated with the help of two agents
  - ◆ Home Agent
  - ◆ Foreign Agent
- ◆ Such encapsulation is also called tunneling



# Mobility architecture

---

- ◆ Binding in the Foreign network
  - ▶ Connection to the Foreign Network
  - ▶ Home Network registration
- ◆ Information exchange
  - ▶ From Correspondent Node to Mobile Node
    - Routing using tunneling
  - ▶ From Mobile Node to Correspondent Node
    - Through Home Network using tunneling (strict routes)
    - Directly to Correspondent Node
- ◆ Remove Registration
  - ▶ Return to the Home Base
  - ▶ Move to a new Foreign Network



# Service Phase

---

- ◆ Correspondent nodes establishes connections using Mobile Node's Home Address
- ◆ Traffic from Correspondent Node
  - ▶ Correspondent Node → Home Agent
  - ▶ Home Agent – tunnel → Foreign Network
    - Foreign Agent → Mobile Node
    - Directly to the Mobile Node
- ◆ Traffic from the Mobile Node
  - ▶ Strict routing
    - Mobile Node → Correspondent Node
    - The source address is the Home Address
  - ▶ Direct routing
    - Foreign Network → Home Network
      - Mobile Node → Foreign Agent – tunnel → Home Agent
      - Mobile Node – tunnel → Home Agent
    - Home Agent → Foreign Node

# Remove registration

---

- ◆ The Mobile node leaves the Foreign Network
- ◆ Ways to know it
  - ▶ Stop the Foreign Agent Advertisement Messages reception during a long time
    - Ask for a explicit advertisement
  - ▶ Receive a message from another Foreign Agent
    - Maybe, we are in the same network, but the register should be updated
- ◆ Register a new address in the new network
  - ▶ Access a new Foreign Network
    - The Home Agent removes old register and register the new one
  - ▶ Return to the Home Network
    - The Home Agent removes the redirection

---

# Mobile IPv6

# Facilities with IPv6

---

- ◆ Stateless Address Autoconfiguration
  - ▶ to configure the Care-of Address
  - ▶ there is no need of Foreign Agent
- ◆ Neighbor Discovery
  - ▶ to detect movement
- ◆ Route optimization
  - ▶ IPv6 Routing Headers
- ◆ IP security
  - ▶ implement strong authentication and encryption features
- ◆ Additional facilities
  - ▶ Coexistence with Internet Ingress Filtering
  - ▶ Smooth Handoffs as part of route optimization
  - ▶ Renumbering of home networks
  - ▶ Automatic home agent discovery

# Mobile Node operation

---

1. The Mobile Node moves to a new point of attachment
2. Configure a new Care-of Address
  - ◆ Use Stateless Address Autoconfiguration
  - ◆ Stateful Address Autoconfiguration (DHCPv6)
3. Builds a new binding
  - ◆ Update the local Binding Cache List
  - ◆ Register the binding in the home subnet
  - ◆ Update binding cache in Correspondent Nodes
4. Delivering packets to and from Mobile Node

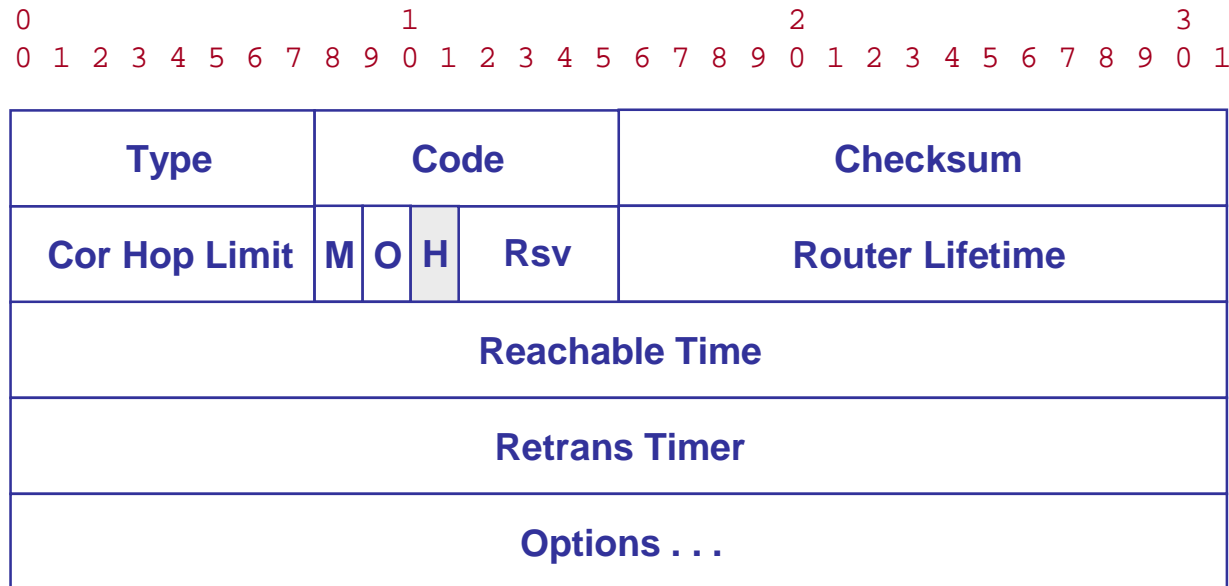
# Movement detection

---

- ◆ Based on IPv6 Neighbor Discovery
  - ▶ Router Discovery
    - Based on-link network prefixes
  - ▶ Neighbor Unreachability Detection
    - Supplement with lower protocol layers information
    - Setting the interface into promiscuous receive mode
- ◆ Router discovery
  1. Send Router Solicitation Message
  2. Wait periodic Router Advertisement messages
- ◆ Mobile Node maintains
  - ▶ Default Routers List (with lifetime)
  - ▶ Prefix Network List (with lifetime)
- ◆ It is important to quick detect when the router becomes unreachable
  - ▶ Use Neighbor Unreachability Detection

# Router advertisement Message

- ◆ It is a modification of Neighbor Discovery message



- ◆ H : the router is also the Home Agent

# Micro mobility

---

- ◆ In wireless networks mobile node has to report every movement to his home network
- ◆ This cause huge amount of signaling traffic and disturbing latency during handoffs.
- ◆ To solve it, the Home Network does not have to know the exact location of the Mobile Node
- ◆ Home Agent will allow mobile nodes to acquire new addresses while still using previously allocated addresses.
- ◆ Smooth Handoffs
  - ▶ Accept packets at previous care-of address even after reporting the new Care-of Address to its Home Agent



# Binding

---

- ◆ Binding
  - ▶ Association
    - (Mobile Node's Home Address - Care-of Address)
  - ▶ Lifetime of the association
- ◆ The Node Bindings Cache List is the central data structure of Mobile IPv6
- ◆ A Mobile Node may have more than one Care-of Address at a time
- ◆ Primary Care-of Address
  - ▶ Is the address of the most recent Mobile Node's binding
- ◆ Binding could be a source of security problems
  - ▶ Binding packets must include IPv6 Authentication Header

# Binding update

---

- ◆ Register the new Care-of Address
  - ▶ Request the home subnet router to function as the Home Agent for the Mobile Node.
  - ▶ Home Agent register only one mobile binding
    - The Primary Care-of Address
- ◆ Binding is also use with Correspondent Nodes
  - ▶ It can be included in any normal packet
- ◆ Binding is also send alone whenever
  - ▶ Mobile suspects that its Home Agent is not operational
  - ▶ Correspondent is not sending packets to the proper Care-of Address
- ◆ Mobile must not send Binding Updates to often
- ◆ Mobile may choose its location private
- ◆ When Mobile Node returns to its home subnet use Home Address as the Care-of Address
  - ▶ It must also send IPv6 Neighbor Advertisement

# Correspondent Node binding update

---

- ◆ Correspondent Node maintains a Binding Cache List to learn the actual mobile address (the Primary Care-of Address)
- ◆ Binding Update
  - ▶ After configuring a new Care-of Address
  - ▶ When binding is out of date
- ◆ Binding Update must be acknowledged
  - ▶ using Binding Acknowledgement
- ◆ Destination options can appear in any IPv6 packet

# Binding and acknowledgement

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

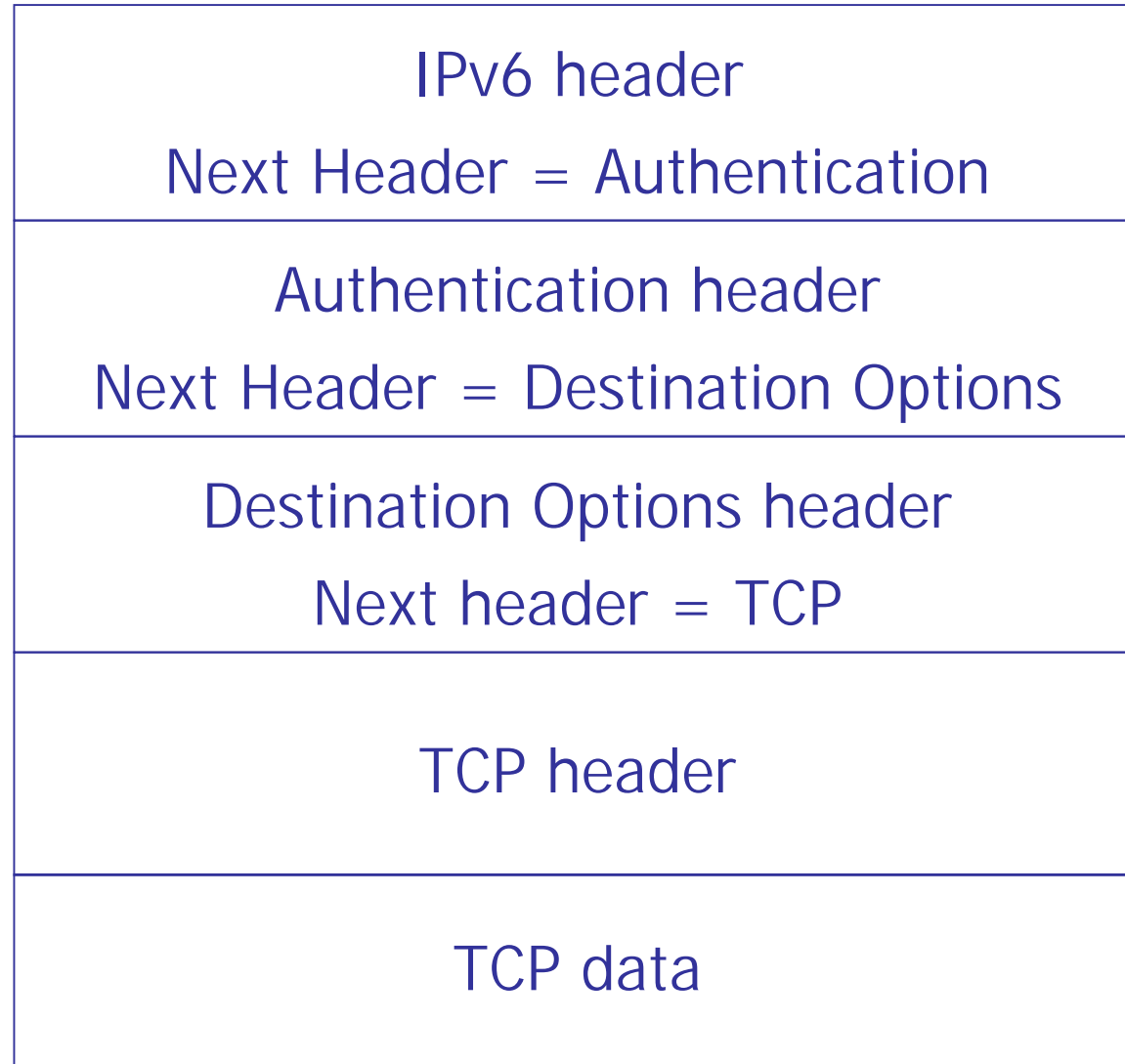
						Option Type	Option Length
A	H	R	D	Rsv	Prefix Length	Sequence Number	
Lifetime							
Sub-Options							

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

										Option Type		
Option Length			Status			Sequence Number						
Lifetime												
Refresh												
Sub-Options												

# Destination Options

---



# Route optimization

---

- ◆ IPv6 allows to send and receive packets directly to or from Correspondent Nodes.
- ◆ Packets are routed using IPv6 Routing Headers
- ◆ IPv6 encapsulation is used only when the Correspondent Node does not know the actual location of the Mobile Node
  - ▶ Packets are sent to the Home Address
  - ▶ Home Agent redirect received packets to the Mobile Node
    - The Home Agent can not use Routing Headers
- ◆ Home Agent use IPv6 Neighbor Discovery to intercept mobile packets received in the Home Network.

# Home Agent discovery

---

- ◆ Not always is possible or convenient for a Mobile Node to know the exact address of its Home Agent
- ◆ Mobile can dynamically discover it
  - ▶ Sending a Binding Update to the IPv6 anycast address
- ◆ The anycast address is received by exactly one router on the home subnet.
- ◆ Any router must reject the Binding Update
  - ▶ Send a Binding Acknowledgement with its unicast address
- ◆ The mobile will then repeat its Binding Update directly to the router that returned the rejection

# Handling errors

---

- ◆ Packets from Correspondent to Mobile Node can generate ICMP error messages.
- ◆ It is important to correctly return to the original sender the generated error.
- ◆ If Correspondent Node use Routing Header, the source address will be that of the Correspondent Node.
  - ▶ Then ICMP messages will be returned directly to the Correspondent Node.
- ◆ If Correspondent Node has no Binding Cache entry the packet will be intercepted by the Home Agent, encapsulated and tunneled to the Care-of Address
  - ▶ The source address in the tunnel is the Home Agent address
  - ▶ But ICMP errors must be received in the Correspondent Node
  - ▶ IPv6 use encapsulation with relay ICMP errors to the original sender
  - ▶ ICMP contain a portion of a packet generating the error



# Renumbering the Home Subnet

---

- ◆ All nodes on a subnet can gracefully autoconfigure new addresses.
  - ▶ Router issuing *multicast* Router Advertisement packets
- ◆ Mobile nodes outside its Home Network must receive Router Advertisement Packets
  - ▶ Home Agent tunnel *multicast* Router Advertisement packets
- ◆ Protocol rules
  - ▶ The mobile assumes that home network prefix has not changed until the reception of a Router Advertisement
  - ▶ Router Advertisement must be authenticated
  - ▶ Mobile must perform the standard autoconfiguration operation
  - ▶ Mobile may send a Router Solicitation message to its home Agent at any time

# Security

---

- ◆ Isec protection mechanisms must be included in all
  - ▶ Binding updates
  - ▶ Binding Acknowledgements
- ◆ It is not required for Binding Requests
- ◆ The great deal is the coexistence between
  - ▶ Mobility
  - ▶ Internet security features (Firewalls)
- ◆ Ingress Filtering
  - ▶ Many border routers discard packets coming from within the enterprise if the packets do not contain a source IP address configured for one of the enterprise's internal networks
  - ▶ The solution of this problem involves tunneling outgoing packets from the care-of address
    - The destination is the Home Agent
  - ▶ Encapsulate the packet to the Firewall

# Open Issues

---

## ◆ Link Layer

- ▶ Medium access control, channels reservation, security

## ◆ Network Layer

- ▶ Mobility management, admission control, resource reservation, point-to-point routing, quality of service

## ◆ Transport Layer

- ▶ High data loss, variable delays

## ◆ Applications

- ▶ Mobile computing, replication, emulation, synchronization, resource location, multimedia.

# Applications

---

- ◆ Mobility is not only a network issue
- ◆ Many applications have problems if they don't recognize mobility
  - ▶ different access points
  - ▶ low reliable links
  - ▶ variable bandwidth
- ◆ Replication, emulation and synchronization
- ◆ Resource location
- ◆ Multimedia and real time applications