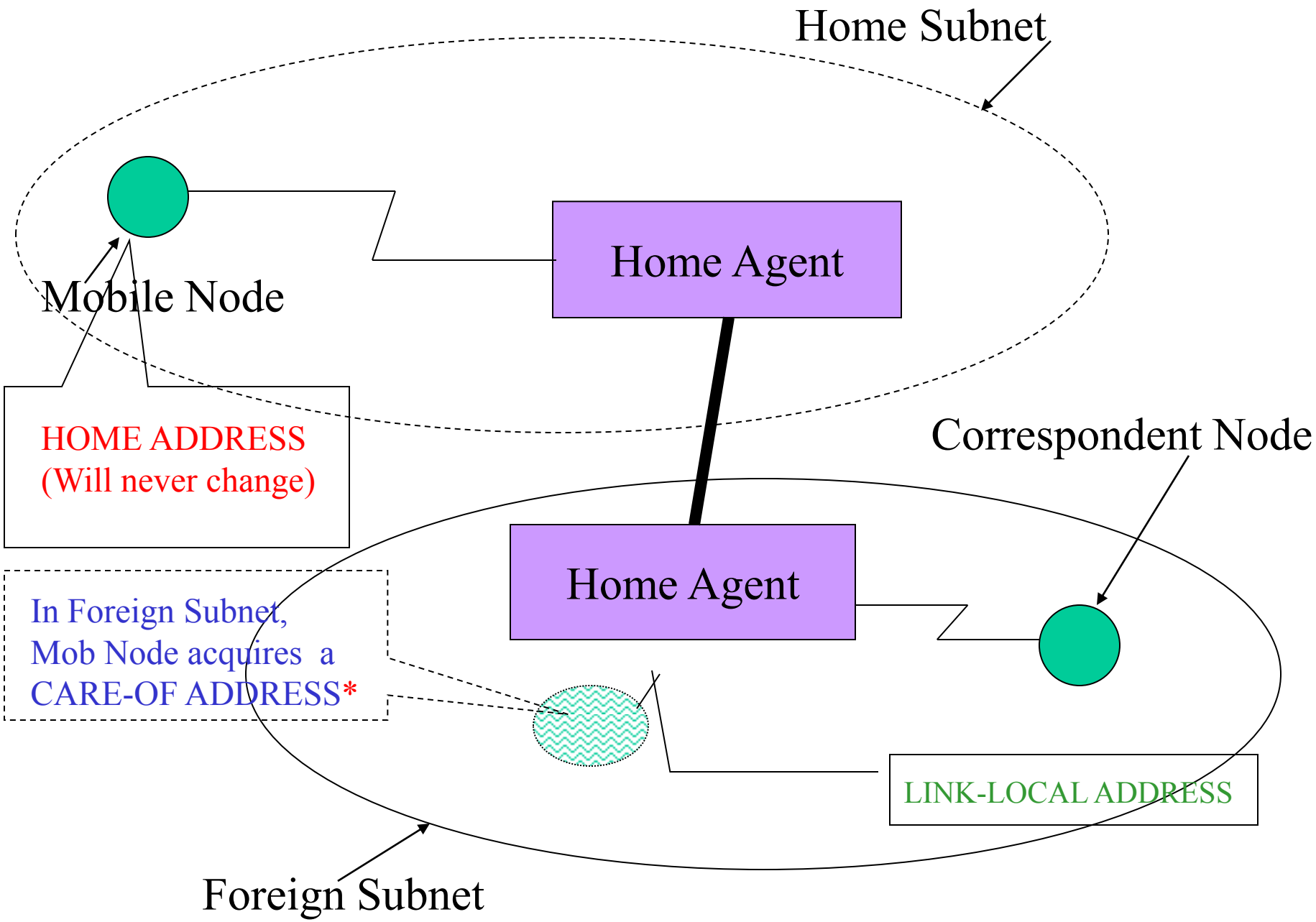
Mobile IP

Motivation

- Mobile IP is a proposed standard protocol that builds on the Internet Protocol for packet routing and delivery by making mobility transparent to applications and higher level protocols like TCP.
- Changed perceptions of the Internet due to large variety of wireless devices offering IP connectivity, such as PDAs, handhelds, and digital cellular phones.

Motivation

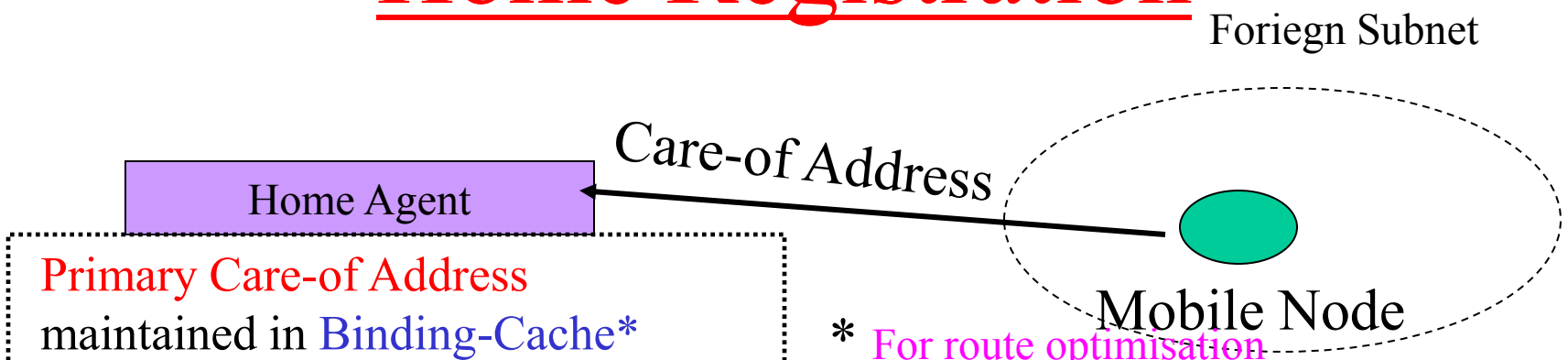
- Without specific support, delivery not possible for mobile nodes away from its home IP subnet (because routing based on the network prefix and destn IP addr).
- Cannot change IP address on moving to new IP-subnet (because cannot maintain tpt/higher level connections).


Home Subnet
Mobile Node
Home Agent
HOME ADDRESS
(Will never change)
Correspondent Node
Home Agent
In Foreign Subnet,
Mob Node acquires a
CARE-OF ADDRESS*
LINK-LOCAL ADDRESS
Foreign Subnet

Binding

Home Address ⟷ (association) Care-of Address

Home Registration



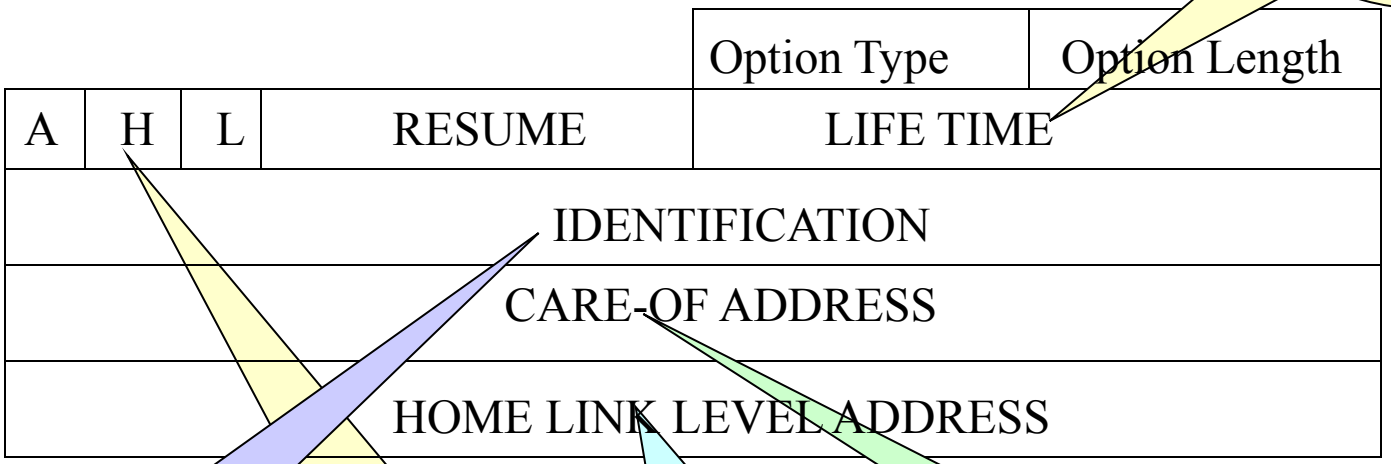
Primary Care-of Address
maintained in Binding-Cache*
till Life-Time expires.
Used for Tunneling by
employing Encapsulation

* For route optimisation
Avoid congestion at HA
Minimise N/W load
Reduction of impact of
failure of HA

Binding : Issues

- Registration. When node acquires a new care-of address.
- Intimation. Node must intimate to
  - HA
  - Correspondent node.
- Binding Ack. Node may expect an Ack
- Life-time. Node should know its likely time of association.
- Identification of Binding Updates.

Binding Update



Binding update survives for the time specified as Life Time

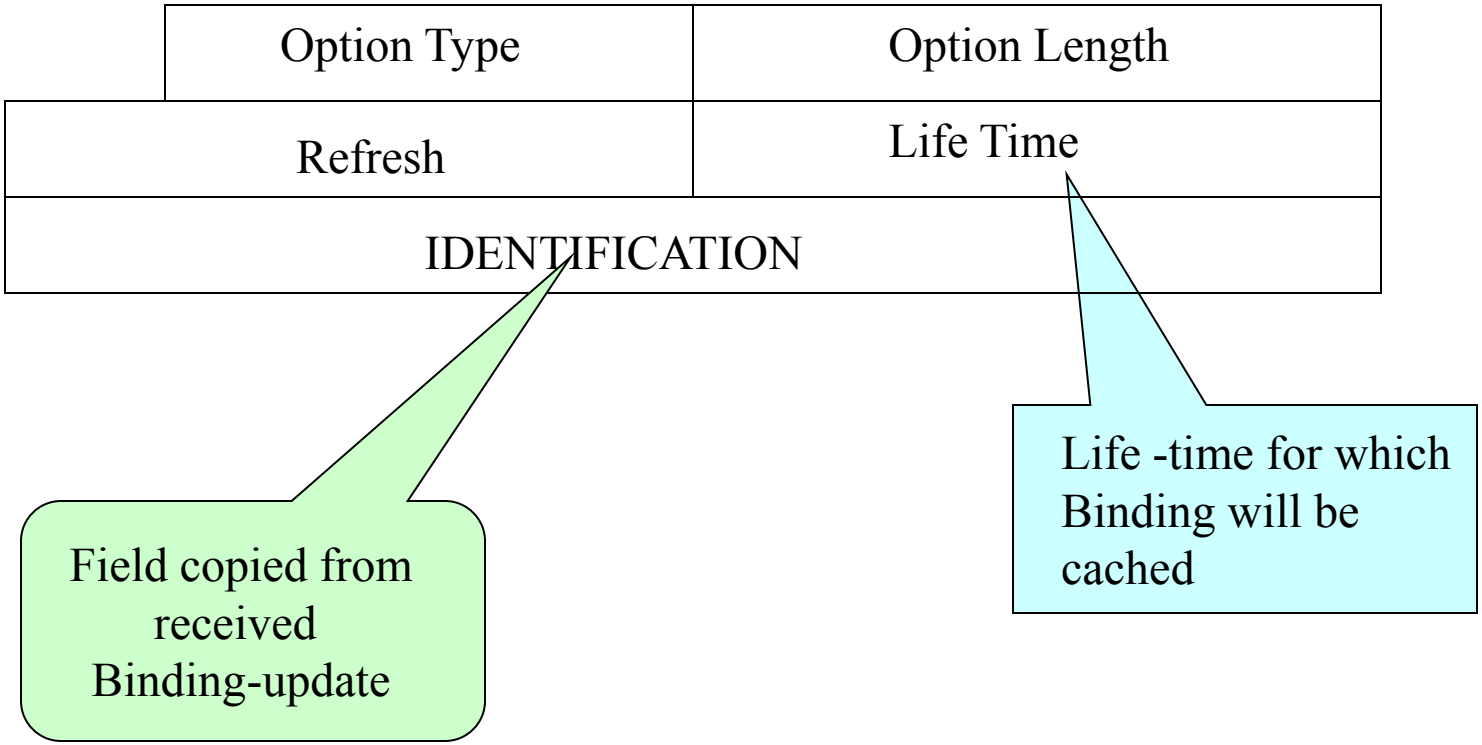
Node maintains a counter and increments it as and when it acquires a c/o addr Binding update is identified by this field.

H=1 : Request to serve as Home Agent
L=1 : Link-Local Address included
A=1 : Ack reqd.

Distinguishing Link-Local address

Care of address acquired by node is reflected in this field

Binding Ack


Option Type
Option Length
Refresh
Life Time
IDENTIFICATION
Field copied from received Binding-update
Life -time for which Binding will be cached

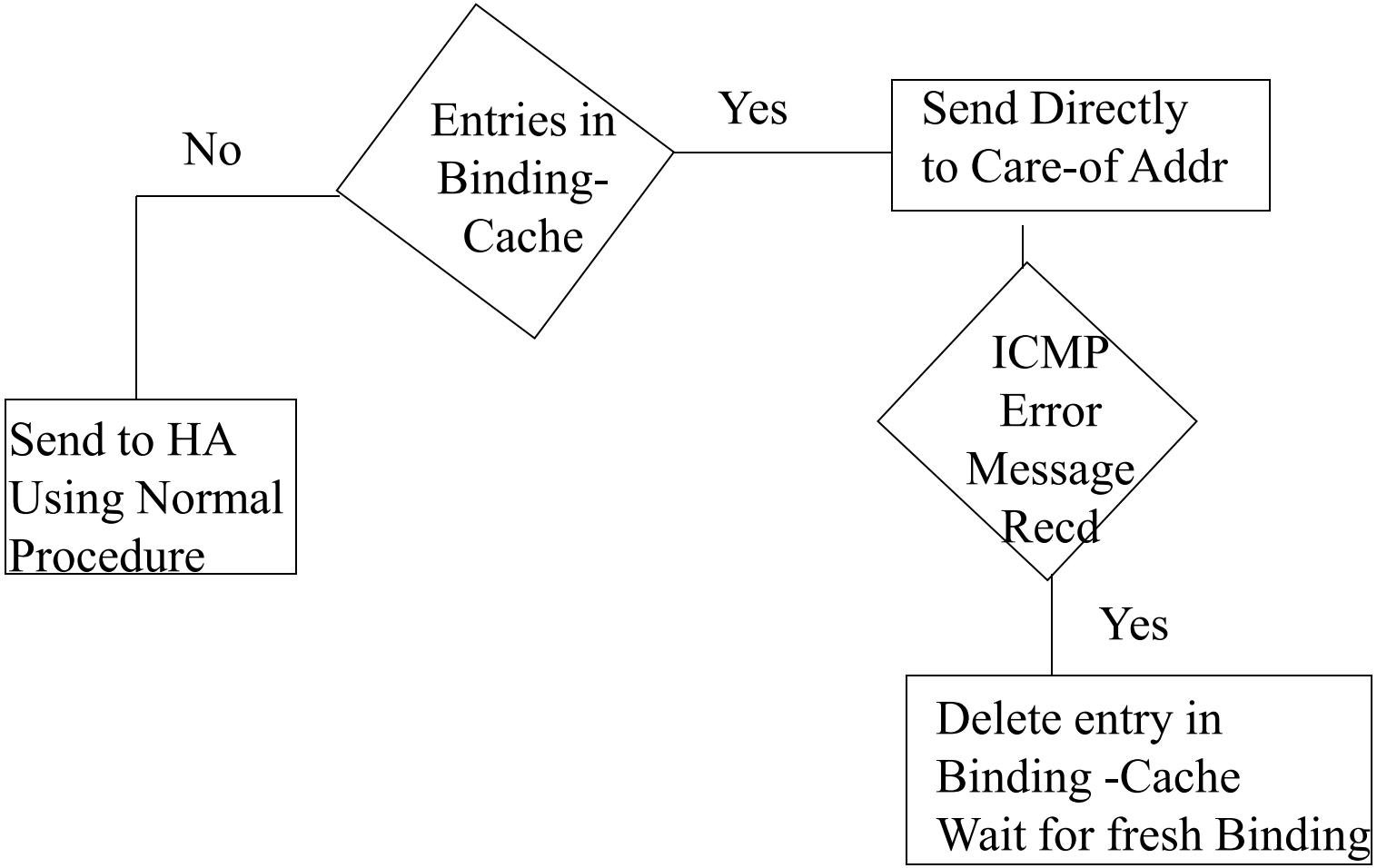
Mobile Node Operation

- IP decapsulation.
- Send Binding updates.
- Receive Binding Ack.
- Keep track of Nodes (because of Life-time).
- Send Binding Updates using Routing Header.

Correspondent Node Ops

- Process received Binding Updates.
- Send Binding-Ack.
- Maintain Binding-Cache.
- Maint Security Association.

Packet Delivery



Home Agent Ops

- Send Binding-Ack to Binding Updates.
- Encapsulate Pkts for tunneling.
- Neighbour Advertisement.
- Proxy Neighbour Advertisement.
- Home Agent Discovery.
- Handle Returned ICMP errors.

Issues

- Encapsulation.
- Movement Detection.
- Security.

IP Encapsulation within IP

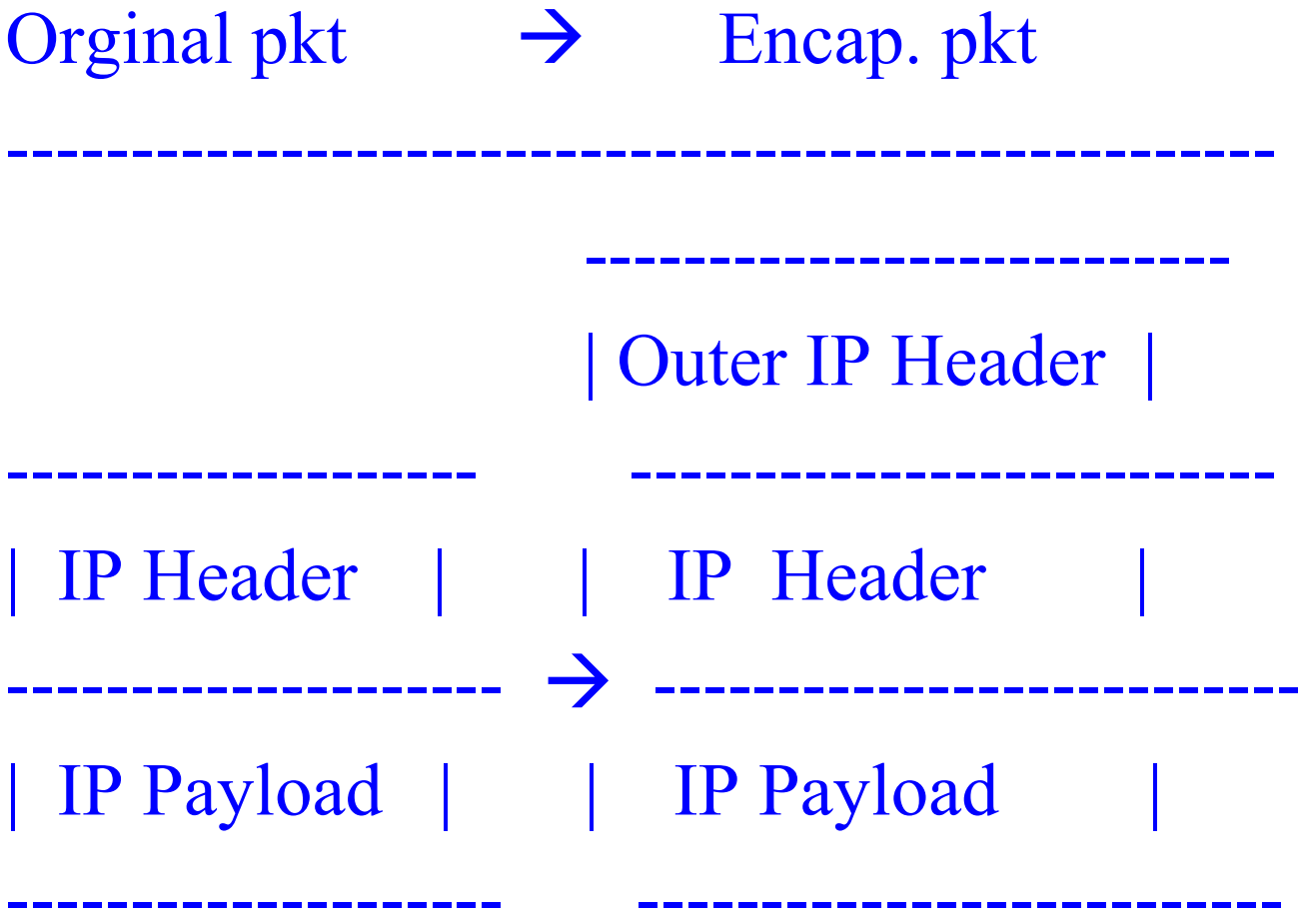
- Required when HA receives packet for a node which has moved outside home territory.

Tunneling

- This method of sending IP datagrams is called ‘tunneling’
- End-points of tunnel are called encapsulator & decapsulator
- Flow of packets :

  src → encapsulator →decapsulator →destn
- Mobile node is attached to a foreign network.
- Need to deliver packets addressed to mobile node, to an agent that can deliver datagrams to mobile node at current location
- The datagrams are sent over the tunnel
- Multiple src-dest pairs can share the same tunnel

Encapsulated Pkt



IP header fields

- Src. and dest. addresses are those of end points of tunnel
- Internet header length :
  - Length of outer header in 32 bit words
- Total length :
  - Measures length of entire encapsulated IP datagram
- Don’t fragment bit :
  - Copied from inner header if set
- Time to live TTL:
  - Appr time to deliver to tunnel exit

Routing failures

- If IP src addr of datagram matches that of the receiving router itself, then discard packet
- If IP src addr matches that of the tunnel exit point, then discard packet

ICMP messages from the tunnel

- Encapsulator may receive ICMP messages from any intermediate router in the tunnel other than exit
- Some typical messages received are shown
- Network unreachable:
  - Return dest unreachable message to org sender
- Host unreachable:
  - Return host unreachable message
- Datagram too big:
  - Relay ICMP datagram too big to org sender
- Source route failed:
  - Handled by encapsulator itself and MUST NOT relay message to org sender

ICMP error messages (contd.)

- Source quench
  - SHOULD NOT relay msg to org sender , SHOULD activate congestion control mechanism
- Time exceeded
  - MUST be reported to org sender as host unreachable message

Tunnel management

- ICMP requires routers to return 8 bytes of datagram beyond IP header
  - This may not contain the org datagram
- So not always possible for encap to relay ICMP messages from interior of tunnel to org sender
- Encap maintains "soft state" about tunnel
  - MTU of the tunnel
  - TTL (path length) of tunnel
  - Reachability of the tunnel
- Encap updates soft state based on ICMP msgs received

Tunnel management (contd.)

- For eg. If TTL of recvd packet is less than the TTL value in soft state, then return error message to sender

- If size of recvd datagram is bigger than MTU of tunnel and if “don’t fragment” bit set, then return datagram too big message to sender.

Disadvantages

- Encapsulated datagrams are larger than source routed datagrams, because of added header
- Encapsulation cannot be used unless it is known that the node at tunnel exit can decapsulate the datagram

Mobile Computing

Neighbor Discovery for IP Version 6 (IPv6)

Issues : Movement Detection

- Neighbour Discovery Protocol. How does a Node know its likely Link-Local address provider?
- Router Discovery. How to discover a HA?
  - Router Solicited Message.
  - Unsolicited Periodic Message.
- Neighbour Unreachability Detection. When is Node/HA unreachable and How to detect?

Issues : Movement Detection

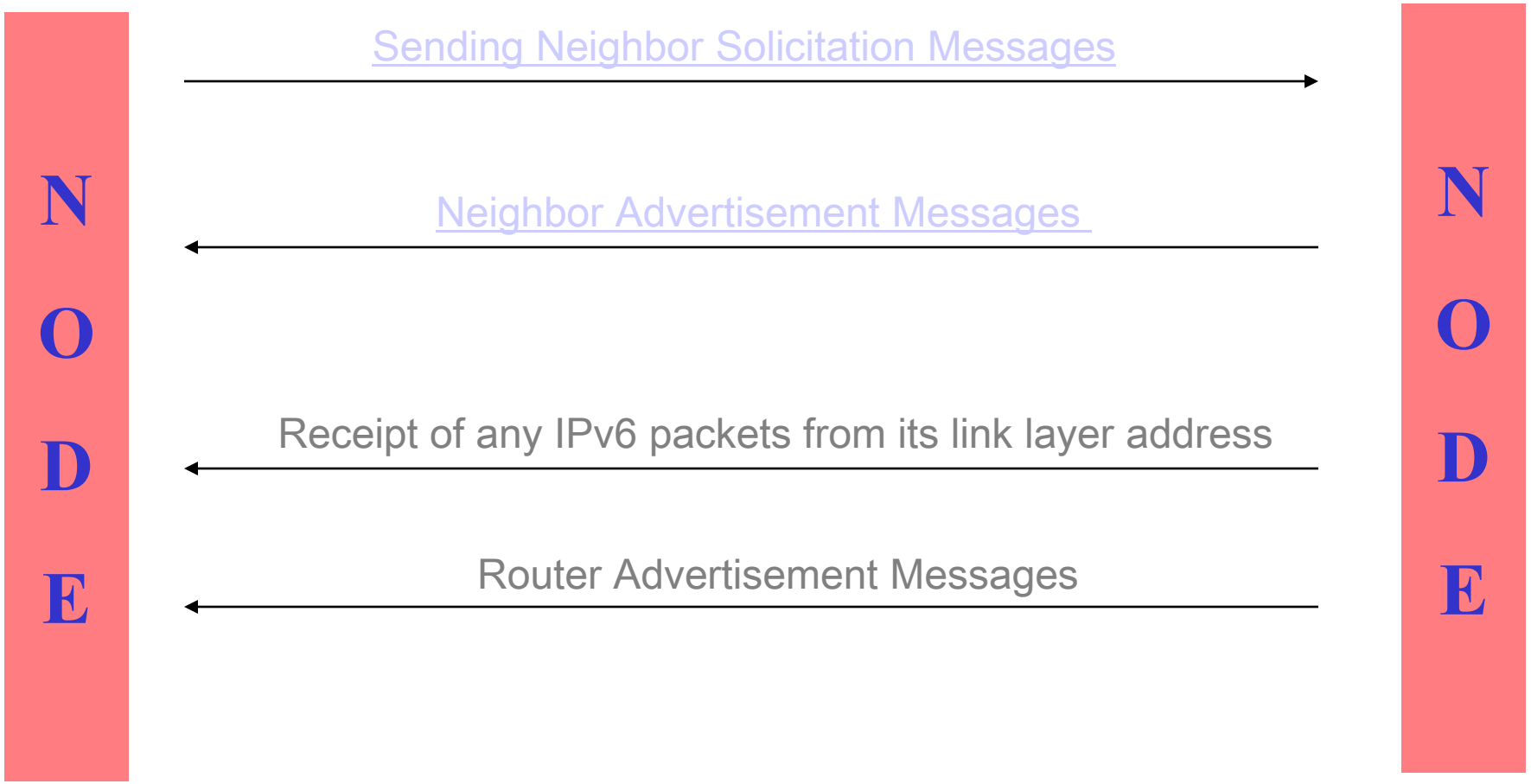
- Hand-off with overlapping cells. How does a hand-off with overlapping cells should be done?
- Router assisted Hand-off. How can a Router assist in Hand-off.
- Renumbering the Home Subnet. What if the Home Subnet itself gets changed?

Movement Detection

- Neighbor Discovery Protocol
  - Router Discovery
  - Neighbor Unreachability Detection

Router Discovery

Neighbor Unreachability Detection



ADDRESS RESOLUTION AND NEIGHBOR UNREACHABILITY DETECTION

- Message Validation
  - The IP Hop Limit field has a value of 255, i.e., the packet could not possibly have been forwarded by a router
  - If the message includes an IP Authentication Header, the message authenticates correctly
  - ICMP Checksum is valid
  - ICMP Code is 0
  - ICMP length (derived from the IP length) is 8 or more
  - All included options have a length that is greater than zero.

Back

Security Issues

- Session Keys with local routers.
  - Key Distribution
  - Diffie-Hellman Key exchange algorithm.
- Source Address filtering by firewalls.

Security Considerations

- Security considerations are important
- Wireless links are vulnerable to
  - passive eavesdropping
  - Active replay attacks
  - Other attacks

Message Authentication Codes

- Authentication required between home agent and mobile node
  - Default algorithm is keyed MD5
  - Key size 128 bits
  - Data should be hashed using this key
  - Foreign agents need to support authentication using this method
- Other algorithms also can be applied

Areas of security concern

- Tunneling mobile node's traffic to its care-of-address
- ARP is also not authenticated
- Communication between foreign and home agent need secured to avoid illegal users and for billing purposes

MD5 algorithm

- Input: message of arbitrary length
- Output: 128 bit ‘fingerprint’ or ‘Message Digest’
- Computationally infeasible to produce two messages with same message digest
- Reliable than checksum

Privacy issues

- Encryption required for sensitive data
- Absolute location policy
  - Mobile node can create tunnel to home agent
  - Datagram look like to be sent by home agent
  - Location tracking is difficult

Replay protection for registration requests

- Home agent need to verify message is from node, not replayed by an attacker from previous registration
- Two methods
  - Timestamps (mandatory)
  - Nonces (optional)

Protection using timestamps

- Two nodes must have adequately synchronized TOD clock
- Current time sent with request
- Default value 7 sec. time difference
- Time synchronization messages should be protected

Protection using nonces

- Node A includes new random number in every message to B
- A checks if B returns same number back in next message
- Authentication code is used to protect against alteration
- Self synchronizing: if registration fails, new nonce is sent in reply

Problem Areas

- Routing inefficiencies. Problem of Triangle Routing.
- Security issues. Requirement of making Mobile IP coexist with the security features coming into use within the Internet. **Firewalls**, in particular, cause difficulty for Mobile IP because they block all classes of incoming packets that do not meet specified criteria.

Problem Areas

- User perceptions of reliability. The design of Mobile IP is founded on the premise that connections based on TCP should survive cell changes. However, opinion is not unanimous on the need for this feature.
- Competition from other protocols. Mobile IP may well face competition from alternative tunneling protocols such as PPTP and L2TP.

References

URLs

- http://www.ietf.org/html.charters/mobileip-charter.html
- http://www.computer.org/internet/v2n1/perkins.htm

Drafts :

- Route Optimization in Mobile IP
- Mobility Support in IPv6
- IP Mobility Support for IPv4, revised