CS6504

Mobile Computing

Dr. Ayman Abdel-Hamid

Computer Science Department

Virginia Tech

Mobile IPv4

Outline

- Host Mobility problem and solutions
- IETF Mobile IPv4

Host Mobility Problem 1/2

An ***IP address*** reflects a host's point of attachment to the network

Example: TCP connection identified by a 4-tuple
< ***source IP address, source TCP port,***
destination IP address, destination TCP port >

if either host move, and acquire a new IP address, the **TCP connection breaks**

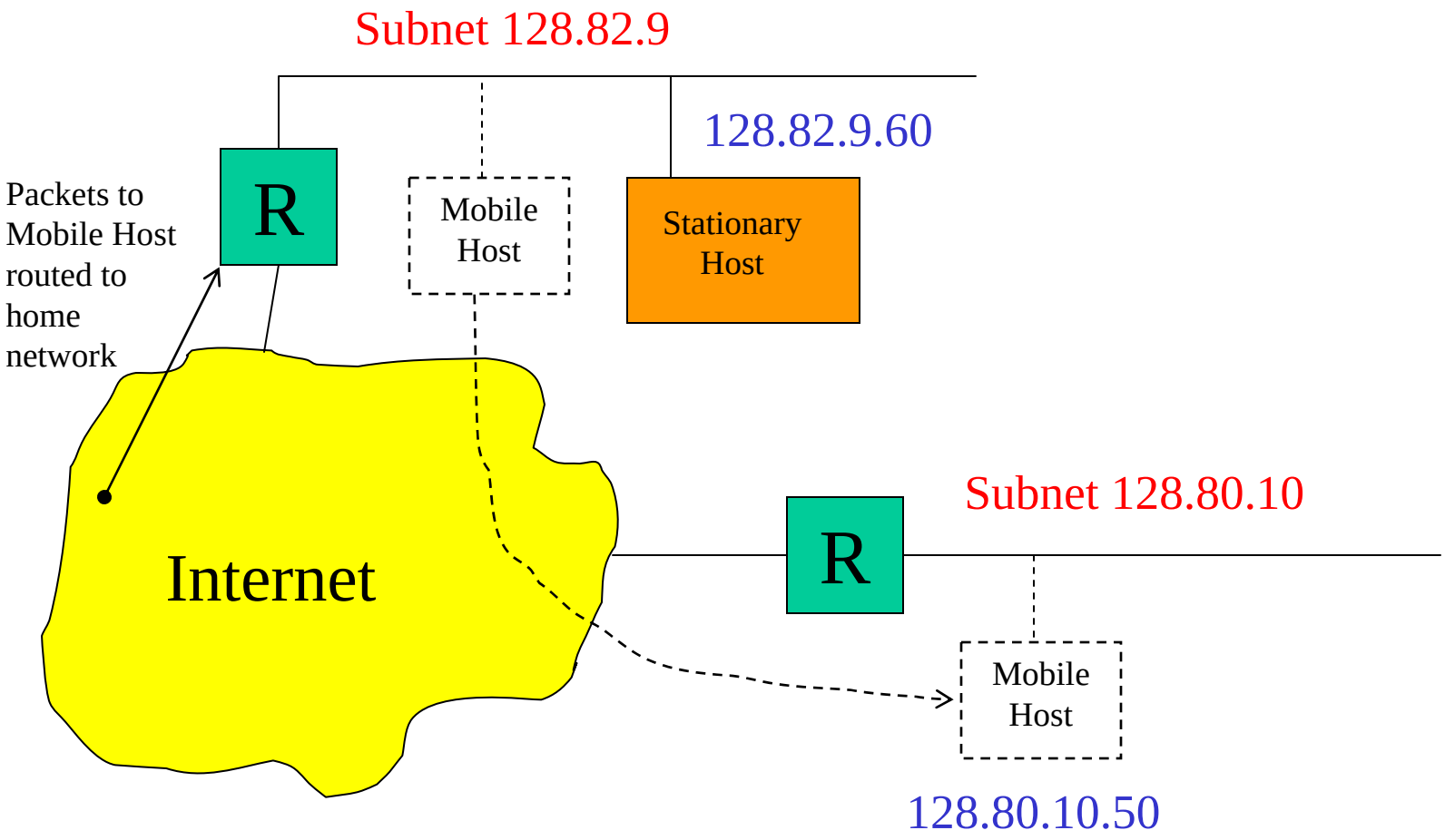
Fundamental Problem

an IP address serves dual purpose

Transport and application layer perspective: **end-point identifier**

Network Layer: **routing directive**

Host Mobility Problem 2/2



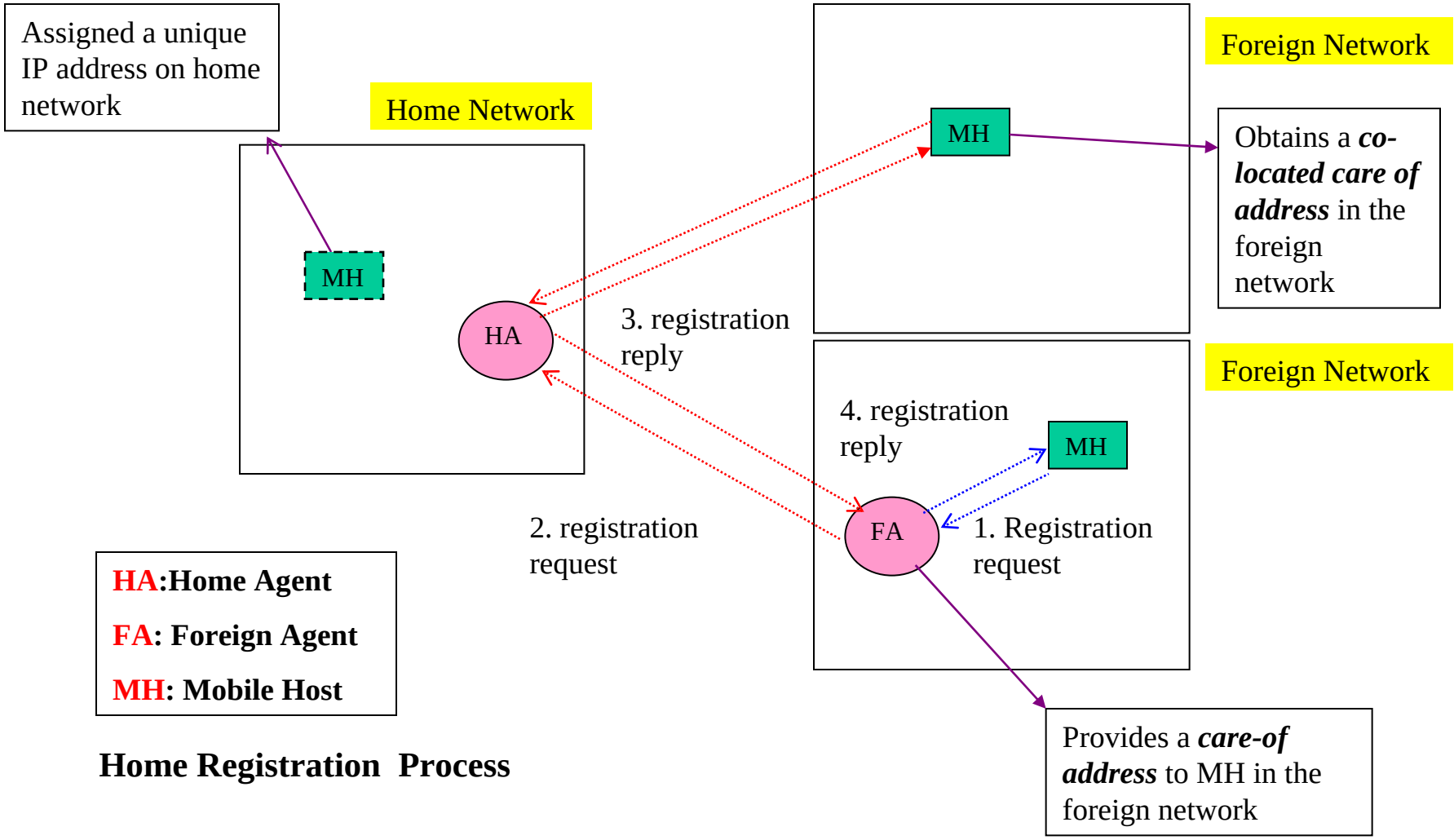
Host Mobility Problem Solutions

- **Network layer solutions**
  - -IETF Mobile IP (MIPv4 and MIPv6)
    - •uses “Mobility agents”
    - •hides a change of IP address, when a mobile host is moving between IP networks.
- **Application layer solutions**
  - -Mobility support using “Session Initiation Protocol”
    - •used for real-time mobile communications
    - •problem with TCP connections, suggests using mobile IP for TCP connections
- **End-to-End Host Mobility support**
    - •Relies on DNS secure dynamic updates
    - •TCP option for connection migration (suspend TCP connection and reactivate it from another IP address)

Network Layer Solutions Model

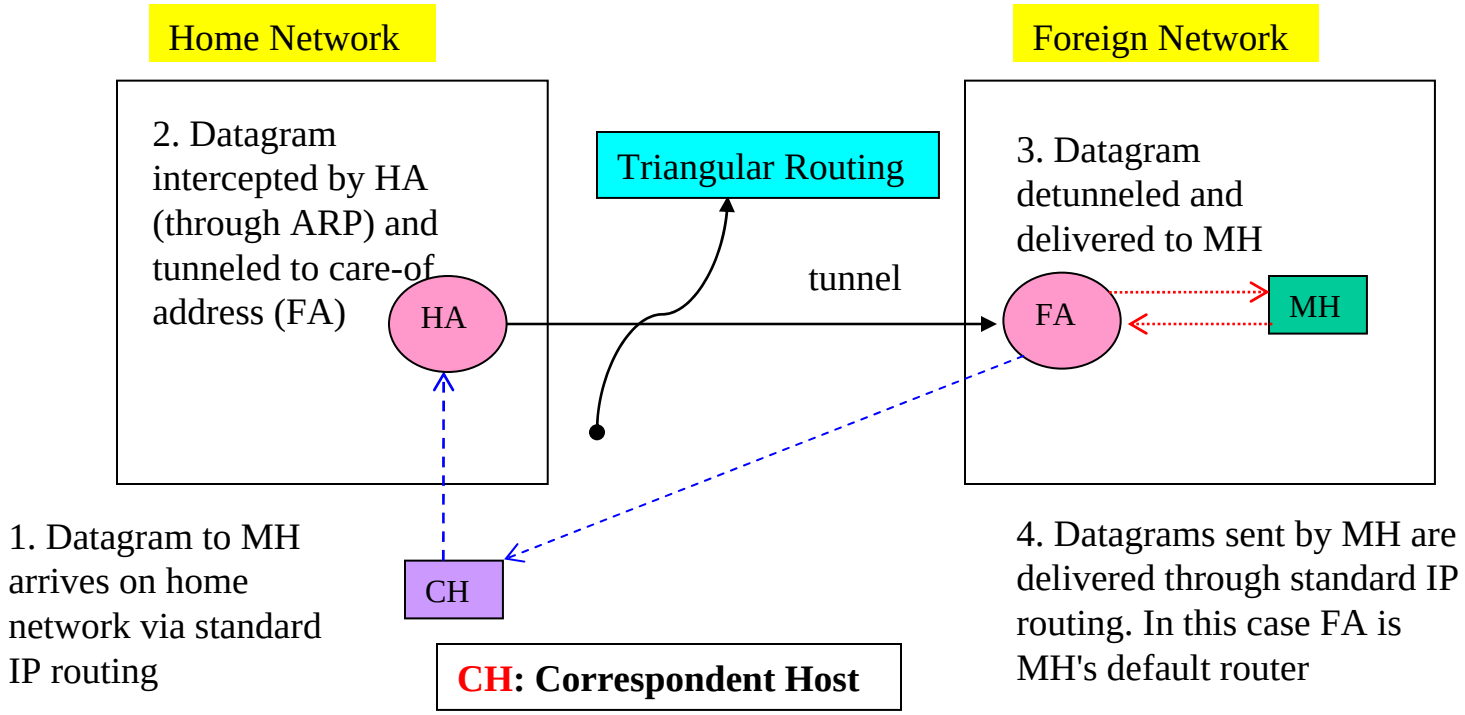
- two-level addressing architecture
  - home address & care-of address
- key mechanisms
  - address translation
    - map home address to care-of address
  - packet forwarding
    - tunnel packets to care-of address
  - location management
    - update mobile host's location

IETF Mobile IPv4 1/4



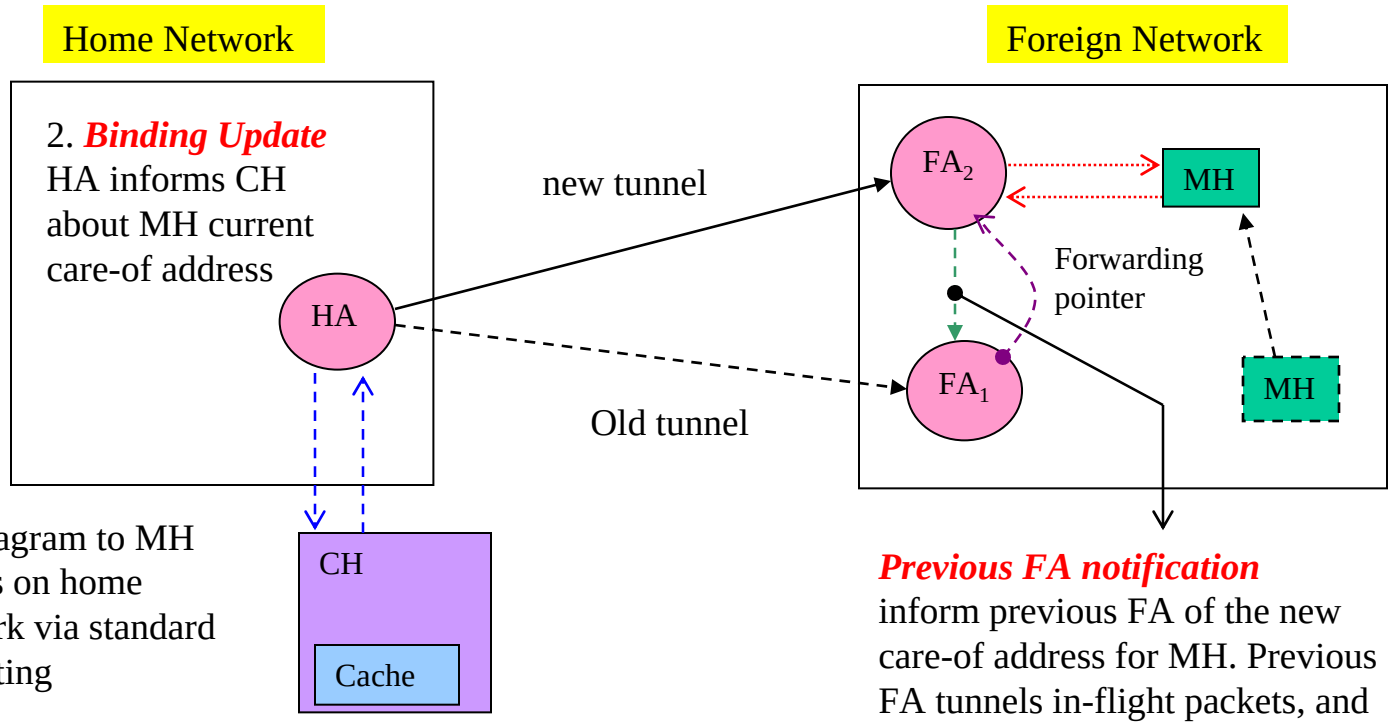
Home Registration Process

IETF Mobile IPv4 2/4



Unicast datagram routing to the MH's care-of address

IETF Mobile IPv4 3/4



Previous FA notification
inform previous FA of the new care-of address for MH. Previous FA tunnels in-flight packets, and packets from CH with out-of-date location cache entries to new FA. (Handoff)

Route optimization

3. CH caches MH care-of address and uses it for any subsequent datagrams destined to MH

IETF Mobile IPv4 4/4

Problems

- triangular routing (sub-optimal routing)
- tunneling overhead
- use of route optimization solves the triangular routing problem, BUT requires change in the IP stack of CH
- large signaling overhead (registration) , if movement within the same domain (local-area mobility). MH has to inform the HA whenever it changes its point of attachment.

Outline

- A more detailed look to Mobile IPv4
  - Architectural Entities
  - Operation Outline
  - Agent Discovery
  - Registration
  - Datagram Routing
  - Reverse Tunneling
  - Replay Protection

Architectural Entities

- Mobile Node
  - A host or router that changes its point of attachment from one network or subnetwork to another

Home Agent

- A router on a mobile node's home network which tunnels datagrams for delivery to the mobile node when it is away from home
- maintains current location information for the mobile node

Foreign Agent

- A router on a mobile node's visited network which provides routing services to the mobile node while registered
- detunnels and delivers datagrams to the mobile node that were tunneled by the mobile node's home agent.

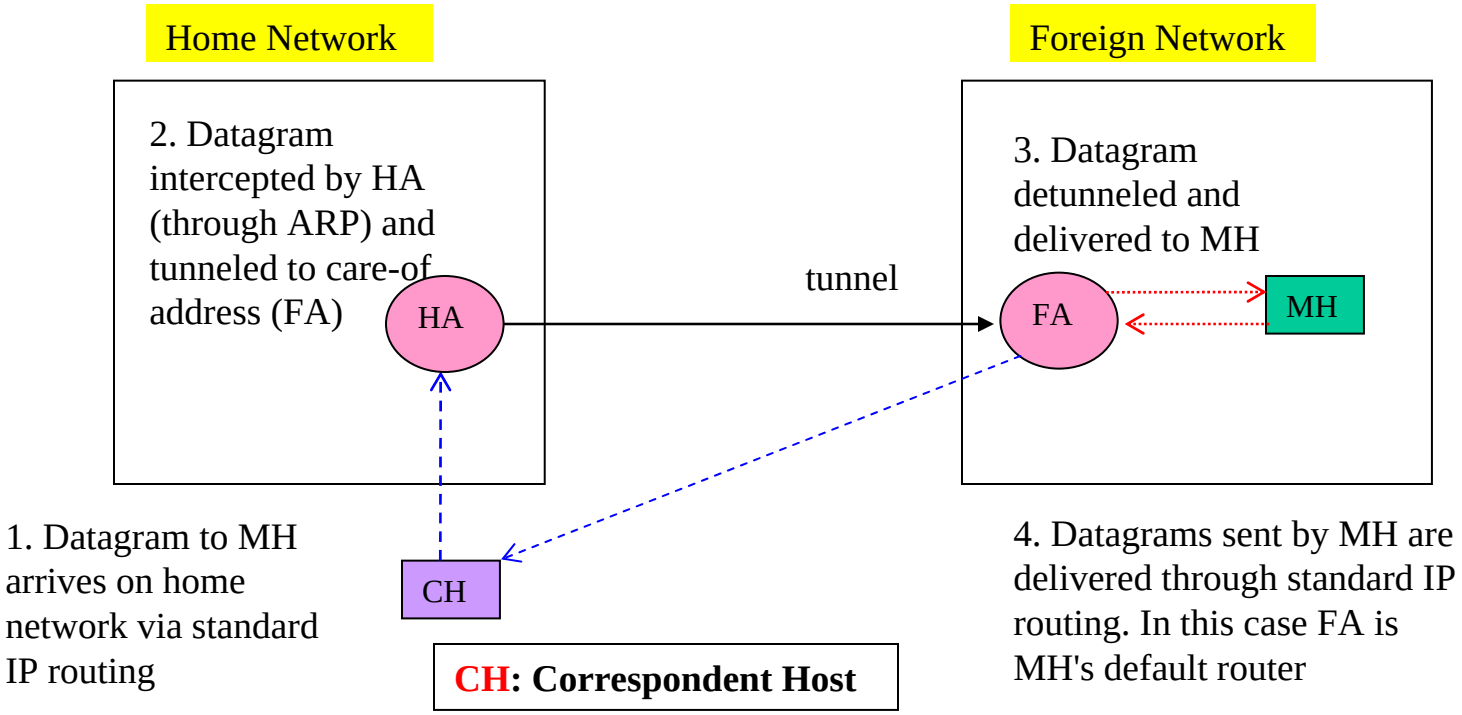
Operation Outline 1/3

- Mobility agents advertise presence via *Agent Advertisement messages*
- A mobile node may optionally solicit such message through an *Agent Solicitation message*
- A mobile node determines whether in a home or foreign network
- In home network → operates without mobility services
- If returning to its home network, the mobile node *deregisters* with its home agent
- In a foreign network, it obtains a *care-of address*
  - from a foreign agent's advertisements (a foreign agent care-of address)
  - by some external assignment mechanism such as DHCP (a co-located care-of address)

Operation Outline 2/3

- The mobile node operating away from home
  - registers its new care-of address with its home agent through exchange (possibly via a foreign agent)
- Datagrams sent to the mobile node's home address
  - intercepted by its home agent
  - tunneled by the home agent to the mobile node's care-of address
  - received at the tunnel endpoint, and finally delivered to the mobile node
- In the reverse direction, datagrams sent by the mobile node
  - are generally delivered to their destination using standard IP routing mechanisms

Operation Outline 3/3

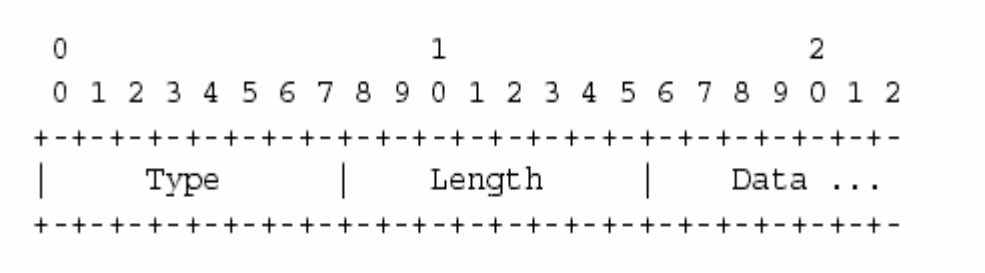


Unicast datagram routing to the MH's care-of address

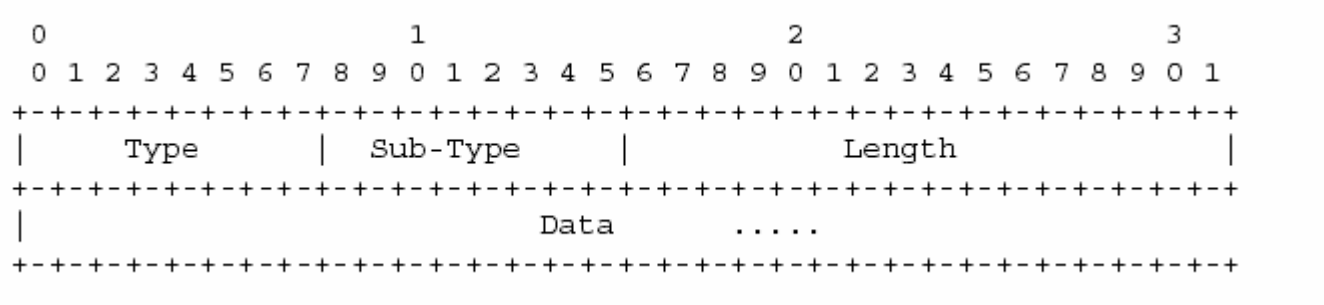
Message Format and Protocol Extensibility 1/2

- Mobile IP defines a set of new control messages, sent with UDP using well-known port number 434 (Registration request and reply)
- For Agent Discovery: use of the existing Router Advertisement and Router Solicitation messages defined for ICMP Router Discovery
- Mobile IP defines a *general Extension mechanism* to allow optional information to be carried by Mobile IP control messages or by ICMP Router Discovery messages
- Extensions format
  - Type-Length-Value Extension Format (Type-Length(8 bits)-Data)
  - Long Extension Format (Type–SubType– Length (16 bits)-Data)
  - Short Extension Format (Type-SubType-length(8 bits)-Data)

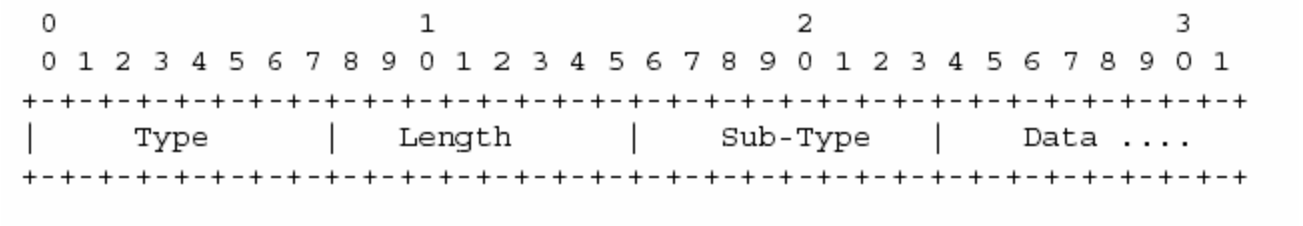
Message Format and Protocol Extensibility 2/2



Type-Length-Value Extension Format



Long Extension Format



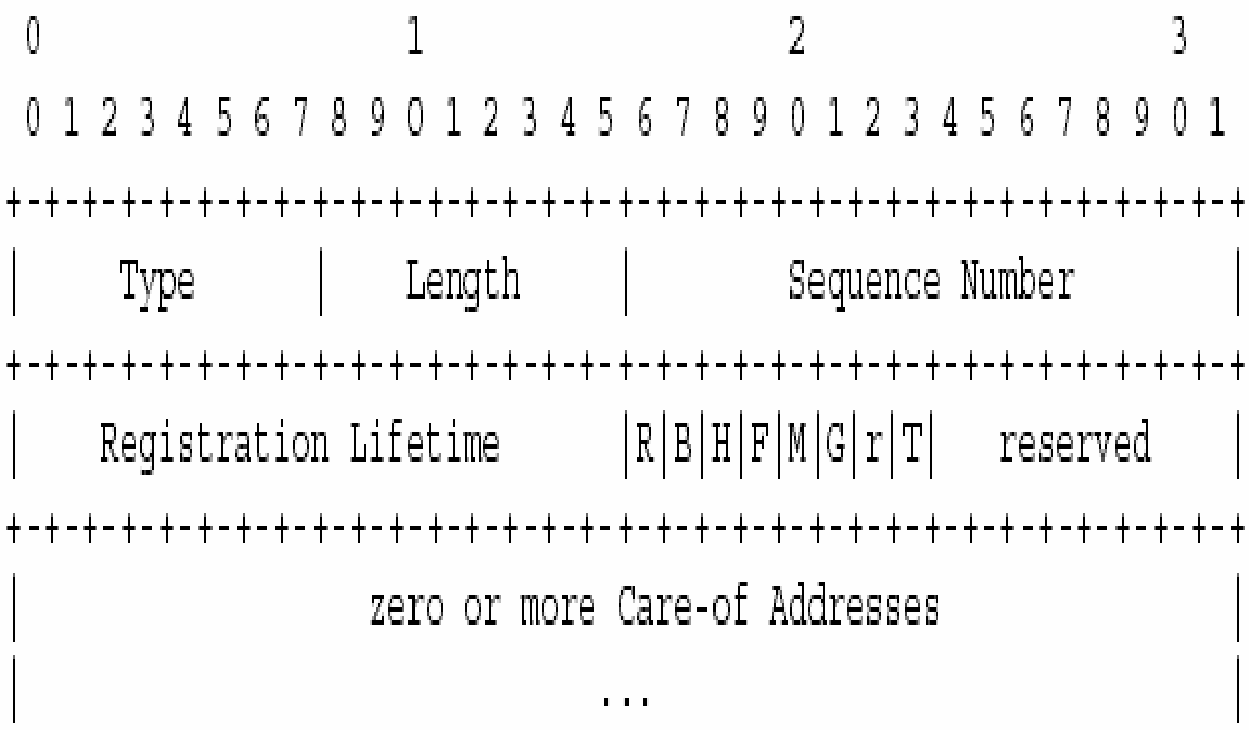
Short Extension Format

Agent Discovery 1/2

- An *Agent Advertisement* is formed by including a *Mobility Agent Advertisement Extension* in an ICMP Router Advertisement message
- An Agent Solicitation is identical to an ICMP Router Solicitation with the further restriction that the IP TTL Field MUST be set to 1
- IP Fields in ICMP router advertisement message (Mobile agents multicast group is 224.0.0.11)
  - TTL: set to 1
  - Destination address:
    - "all systems on this link" multicast address (224.0.0.1)
    - the "limited broadcast" address (255.255.255.255).
    - When unicast to a mobile node, the IP home address of the mobile node

Agent Discovery 2/2

•Mobility Agent Advertisement Extension



R Registration required

B Busy

H Home Agent

F Foreign Agent

M Minimal Encapsulation

G GRE Encapsulation

r sent as Zero

T Reverse tunneling

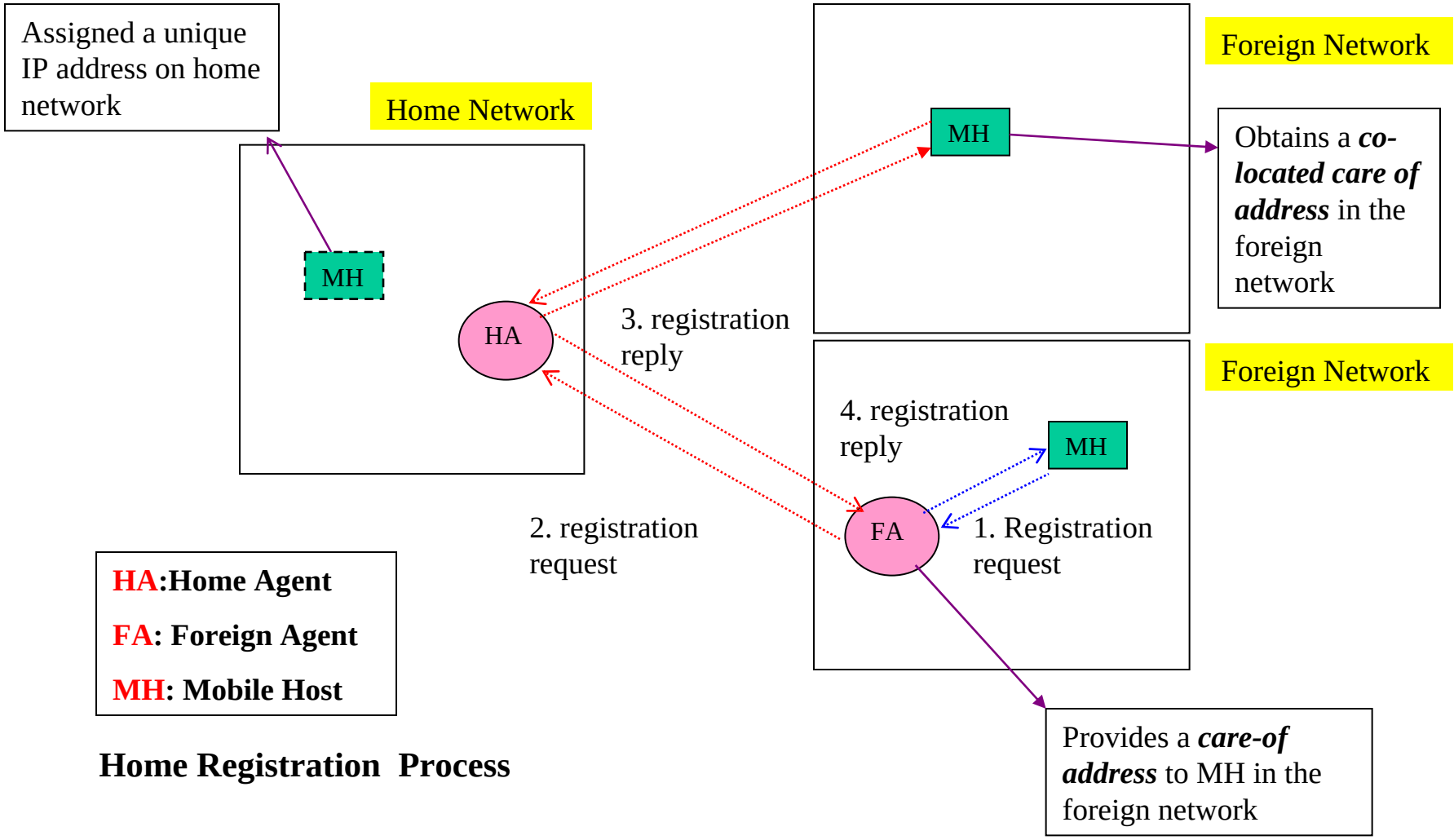
•Length is 6 + 4 * number of care-of addresses

•Sequence number is the count of Agent Advertisement messages sent since the agent was initialized. Initially 0. Upon rollover, start from 256 (why?)

Registration 1/2

- request forwarding services when visiting a foreign network
- inform home agent of current care-of address
- *renew* a registration which is due to expire
- *deregister* when they return home
- Optionally
  - maintain *multiple simultaneous registrations*, so that a copy of each datagram will be tunneled to each active care-of address
  - deregister specific care-of addresses while retaining other mobility bindings
  - discover the address of a home agent, if not already configured with such information

Registration 2/2



Home Registration Process

Registration Authentication

•Each mobile node, foreign agent, and home agent MUST be able to support a *mobility security association* for mobile entities, indexed by their SPI and IP address. In the case of the mobile node, this must be its Home Address

•Mobility Security Association (MSA)

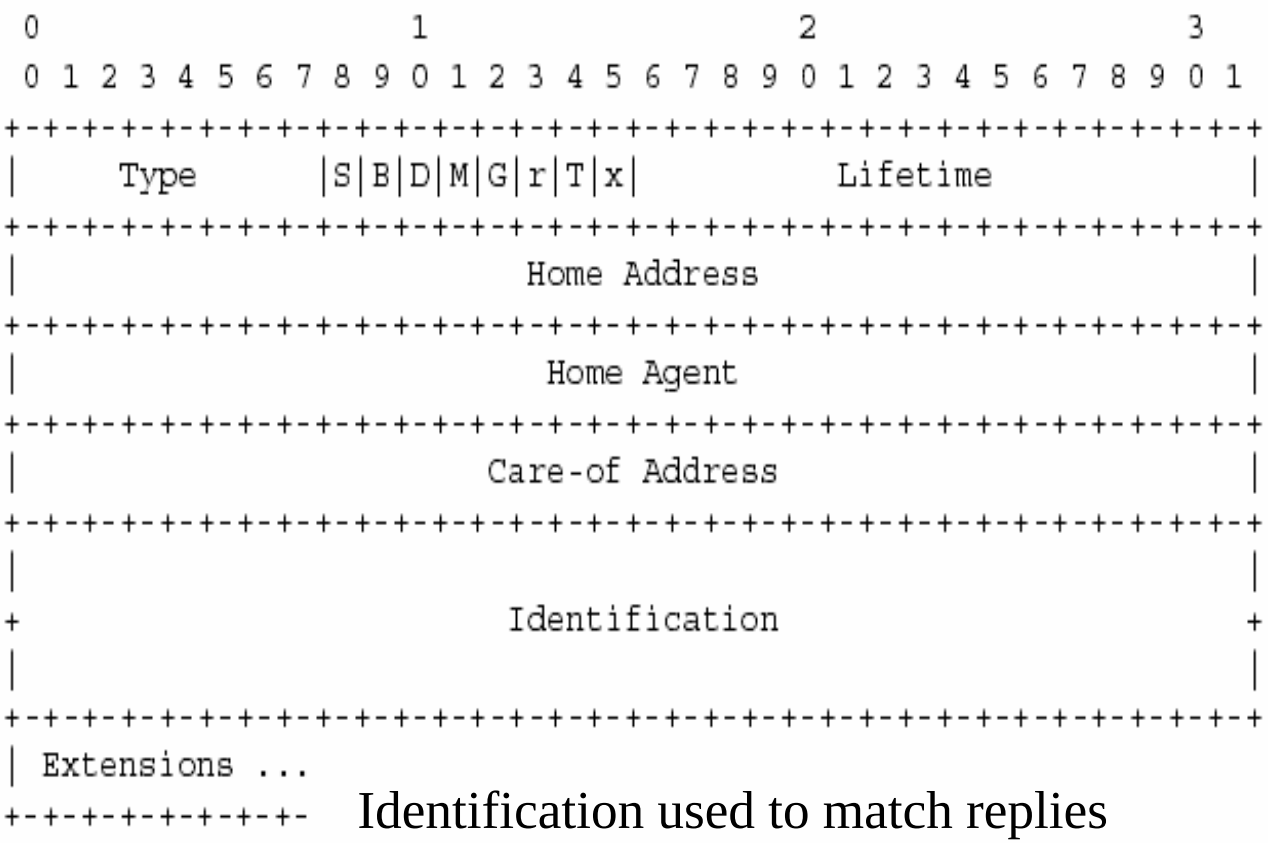
A collection of mobile IP security contexts, between a pair of nodes. Each context indicates an authentication algorithm and mode, a secret (a shared key, or appropriate public/private key pair), and a style of replay protection

•Security Parameter Index (SPI)

An index identifying a security context between a pair of nodes among the contexts available in the MSA.

Registration Request

Mobile IP Fields in registration request



Identification used to match replies versus requests and for replay protection

S Simultaneous binding

B Broadcast datagrams

D Decapsulation by MH

M Minimal Encapsulation

G GRE Encapsulation

r sent as Zero

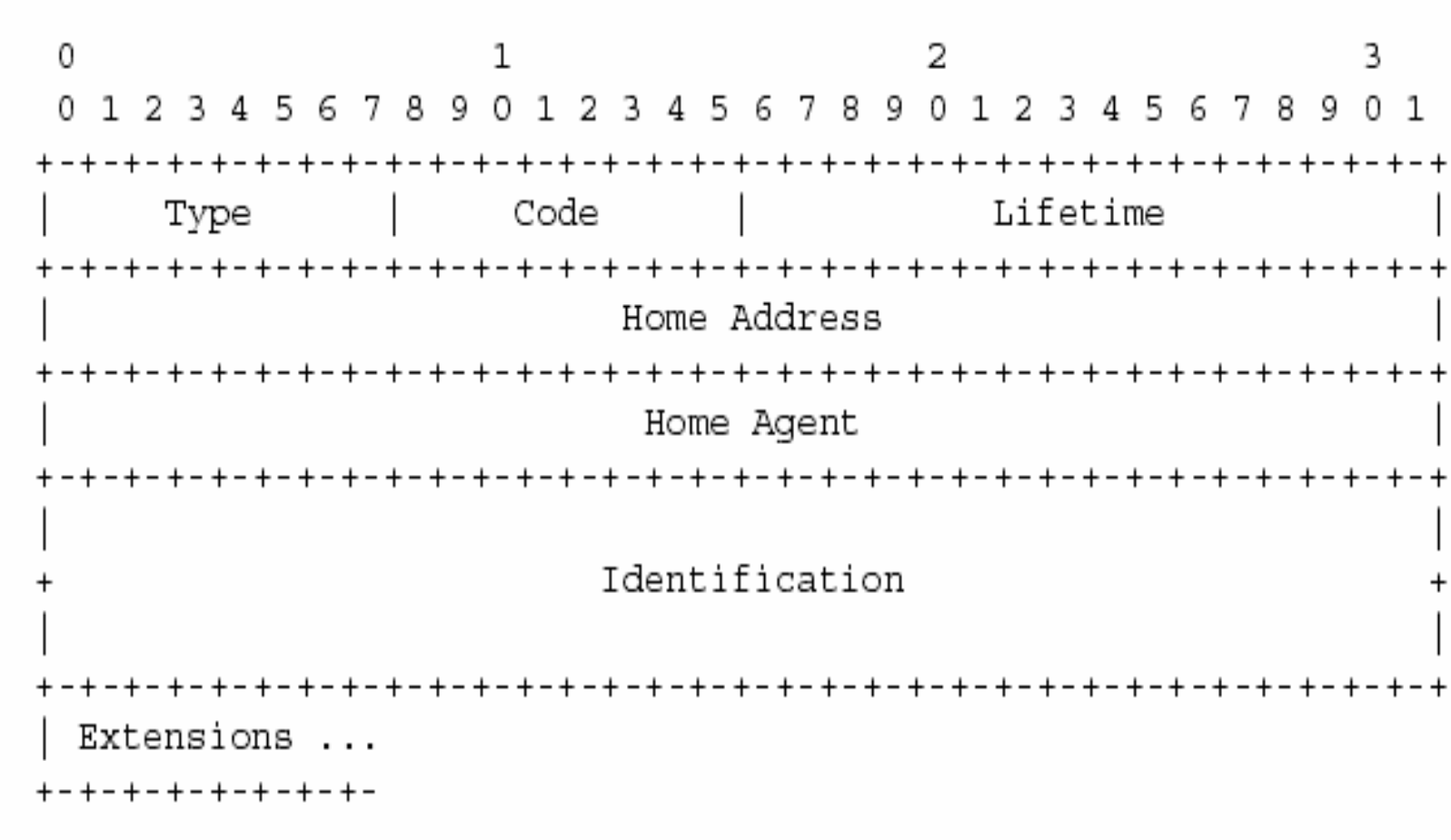
T Reverse tunneling

x sent as Zero

A value of zero in lifetime indicates request for deregistration

Registration Reply

Mobile IP Fields in registration reply



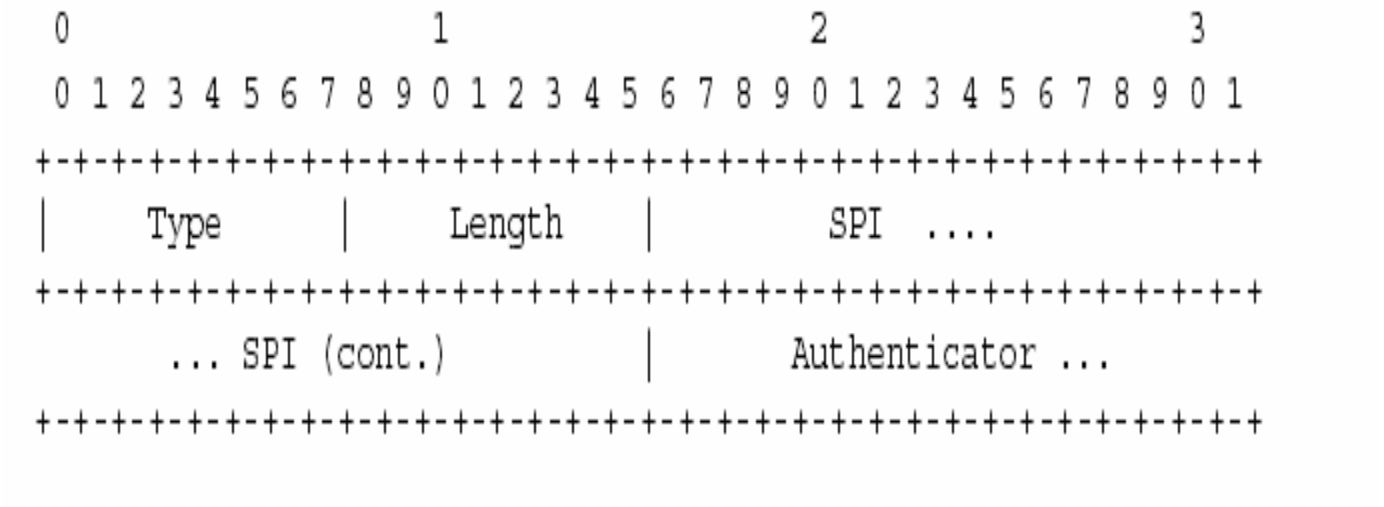
Registration extensions

Computing authentication extension values

- The default authentication algorithm compute a 128-bit "message digest" of the registration message
- The data over which the digest is computed is defined as
  - the UDP payload (Registration Request or Registration Reply data)
  - all prior Extensions in their entirety
  - the Type, Length, and SPI of this Extension

Mobile-Home Authentication Extension

Must be present in registration requests and in registration replies generated by HA



The same format is used for *Mobile-Foreign* and *Foreign-Home* authentication extensions

Extensions order 1/2

The following order must be adhered to in registration requests

- The IP header, followed by the UDP header, followed by the fixed-length portion of the Registration Request
- If present, any non-authentication Extensions expected to be used by the home agent (which may or may not also be useful to the foreign agent)
- An authorization-enabling extension
- If present, any non-authentication Extensions used only by the foreign agent
- The Mobile-Foreign Authentication Extension, if present.

Extensions order 2/2

The following order must be adhered to in registration replies

- The IP header, followed by the UDP header, followed by the fixed-length portion of the Registration
- If present, any non-authentication Extensions used by the mobile node (which may or may not also be used by the foreign agent)
- The Mobile-Home Authentication Extension
- If present, any non-authentication Extensions used only by the foreign agent
- The Foreign-Home Authentication Extension, if present.

Data Structures at HA and FA

Mobility binding entry at HA

- the mobile node's home address
- the mobile node's care-of address
- the Identification field from the Registration Reply
- the remaining Lifetime of the registration

Visitor list entry at FA (for each pending or current registration)

- the link-layer source address of the mobile node
- the IP Source Address
- the IP Destination Address (FA IP address might be unknown to MH)
- the UDP Source Port
- the Home Agent address
- the Identification field
- the requested registration Lifetime
- the remaining Lifetime of the pending or current registration.

Datagram routing 1/5

- Broadcast datagrams
  - MH must have requested forwarding of broadcast datagrams
  - Tunnel to co-located care-of address
  - If FA care-of address, encapsulate into unicast datagram destined to MH home address, then encapsulate into a unicast datagram to FA address (MH must be able to decapsulate received datagram)
- Multicast datagram routing
  - To receive
    - Join via a local multicast router in foreign network
    - Join via a bi-directionnal tunnel to its HA (assuming HA is a multicast router)
  - To send
    - Send directly on visited network (must use a co-located care-of addr)
    - Send via a tunnel to its home agent (use home IP address)

Datagram routing 2/5

•A *Proxy ARP* is an ARP Reply sent by one node on behalf of another node which is

- ➢unable or,
- ➢unwilling to answer its own ARP Requests (provide link-layer address)
- ➢The node receiving the Reply will then associate this link-layer address with the IP address of the original target node
- ➢Will transmit future datagrams for this target node to the node with that link-layer address

•A *Gratuitous ARP* is an ARP packet sent by a node in order to spontaneously cause other nodes to update an entry in their ARP cache

Datagram routing 3/5

- While a mobile node is registered on a foreign network
  - its home agent uses proxy ARP to reply to ARP Requests it receives that seek the mobile node's link-layer address
  - provide its own link-layer address
- When a mobile node leaves its home network and registers a binding on a foreign network
  - its home agent uses *gratuitous ARP* to update the ARP caches of nodes on the home network
  - such nodes will associate the link-layer address of the home agent with the mobile node's home (IP) address

Datagram routing 4/5

- ARP Processing rules when MH leaves home network
  - ➢The mobile node disables its own future processing of any ARP Requests relating to its home address (unless request is by FA)
  - ➢When the mobile node's home agent receives and accepts the Registration Request
    - ✓performs a *gratuitous ARP* on behalf of the mobile node, and
    - ✓begins using *proxy ARP* to reply to ARP Requests that it receives requesting the mobile node's link- layer address

Datagram routing 5/5

- ARP Processing rules when MH returns to home network
  - Before transmitting the Registration Request, the MH re-enables its own future processing of any ARP Requests relating to its home address
  - The MH performs a gratuitous ARP for itself
  - When the mobile node's HA receives and accepts the Registration Request
    - it stops using proxy ARP to reply to ARP Requests, and
    - then performs a gratuitous ARP on behalf of the mobile node

Reverse Tunneling 1/5

- MIP uses tunneling from the home agent to the mobile node's care-of address, but rarely in the *reverse direction*
- Usually, a mobile node sends its packets through a router on the foreign network, and assumes that routing is independent of source address
- When this assumption is not true, it is convenient to establish a topologically correct reverse tunnel from the care-of address to the home agent
- *Use of MH's home address makes the reverse tunnel topologically incorrect*

Reverse Tunneling 2/5

- Two packet delivery styles from MH to FA
  - Direct Delivery Style
    - ✓the mobile node designates the foreign agent as its default router
    - ✓proceeds to send packets directly to the foreign agent, that is, without encapsulation
    - ✓The foreign agent intercepts them, and tunnels them to the home agent
  - Encapsulating Delivery Style
    - ✓the mobile node encapsulates all its outgoing packets to the foreign agent
    - ✓The foreign agent decapsulates and re-tunnels them to the home agent, using the foreign agent's care-of address as the entry-point of this new tunnel

Reverse Tunneling 3/5

Direct Delivery Style (MH must designate FA as default router)

- *Packet format received by the foreign agent*
  - IP fields
    - Source Address = mobile node's home address
    - Destination Address = correspondent host's address
- *Packet format forwarded by the FA*
  - IP fields (encapsulating header)
    - Source Address = foreign agent's care-of address
    - Destination Address = home agent's address
    - Protocol field: 4 (IP in IP)
  - IP fields (original header)
    - Source Address = mobile node's home address
    - Destination Address = correspondent host's address

Reverse Tunneling 4/5

Encapsulating Delivery Style (MH must perform encapsulation)

- *Packet format received by the foreign agent (Encapsulating Delivery Style)*
  - IP fields (encapsulating header)
    - Source Address = mobile node's home address
    - Destination Address = foreign agent's address
    - Protocol field: 4 (IP in IP)
  - IP fields (original header)
    - Source Address = mobile node's home address
    - Destination Address = correspondent host's address

Reverse Tunneling 5/5

Encapsulating Delivery Style (MH must perform encapsulation)

- *Packet format forwarded by the foreign agent*
  - IP fields (encapsulating header)
    - Source Address = foreign agent's care-of address
    - Destination Address = home agent's address
    - Protocol field: 4 (IP in IP)
  - IP fields (original header)
    - Source Address = mobile node's home address
    - Destination Address = correspondent host's address

Replay Protection 1/4

•The *Identification* field is used to let the HA verify that a registration message has been freshly generated by the mobile node

•Style of replay protection part of MSA

- ➢Timestamp-based replay protection
- ➢Nonce-based replay protection

•In either approach, low-order 32 bits of the *Identification* MUST be copied unchanged from the Registration Request to the Reply

- ➢The FA uses those bits (and the mobile node's home address) to match Registration Requests with corresponding replies
- ➢The mobile node MUST verify that the low-order 32 bits of any Registration Reply are identical to the bits it sent in the Registration Request.

Replay Protection 2/4

Timestamp-based replay protection

- The node generating a message inserts the current time of day, and the node receiving the message checks that this timestamp is sufficiently close to its own time of day (Implication?)
- A timestamp is valid if it is close to HA time and greater than all previously accepted timestamps
- If the timestamp is valid, the HA copies the entire Identification field into the Registration Reply
- If the timestamp is not valid, the HA copies only the low-order 32 bits into the Registration Reply, and supplies the high-order 32 bits from its own time of day

Replay Protection 3/4

Nonce-based replay protection

- The basic principle of nonce replay protection is that
  - node A includes a new random number in every message to node B, and checks that node B returns that same number in its next message to node A.
  - Both messages use an authentication code to protect against alteration by an attacker.
  - At the same time node B can send its own nonces in all messages to node A (to be echoed by node A), so that it too can verify that it is receiving fresh messages.

Replay Protection 4/4

Nonce-based replay protection

- The HA inserts a new nonce as the high-order 32 bits of the identification field of every Registration Reply.
- The HA copies the low-order 32 bits of the Identification from the Registration Request message into the low-order 32 bits of the Identification in the Registration Reply.
- When the mobile node receives an authenticated Registration Reply from the home agent, it saves the high-order 32 bits of the identification for use as the high-order 32 bits of its next Registration Request.
- If a registration message is rejected because of an invalid nonce, the Reply always provides the mobile node with a new nonce to be used in the next registration.