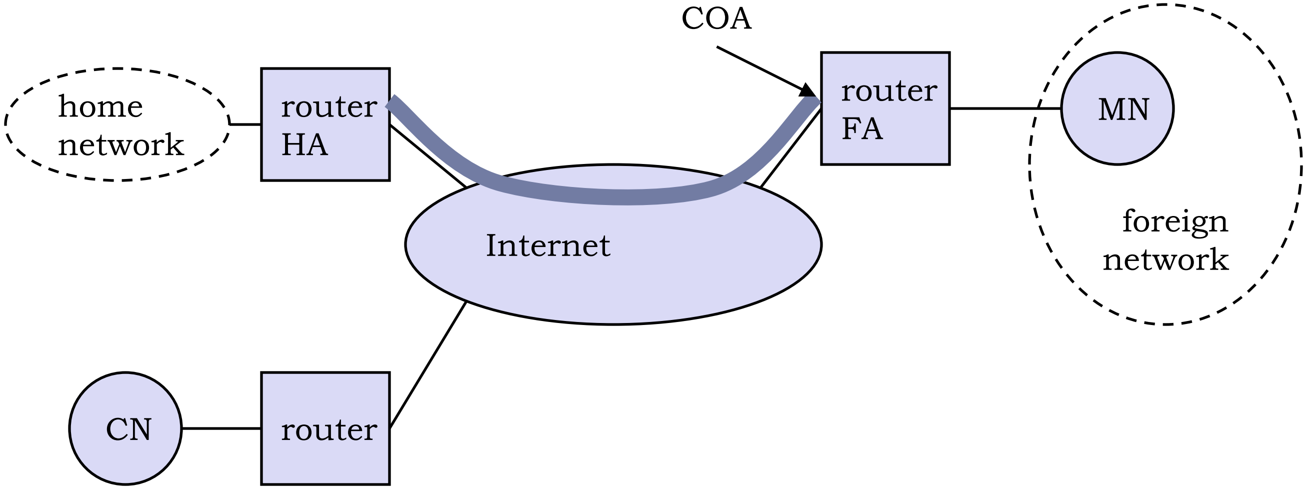
Key Mechanism used in Mobile IP

Beulah A.
AP/CSE

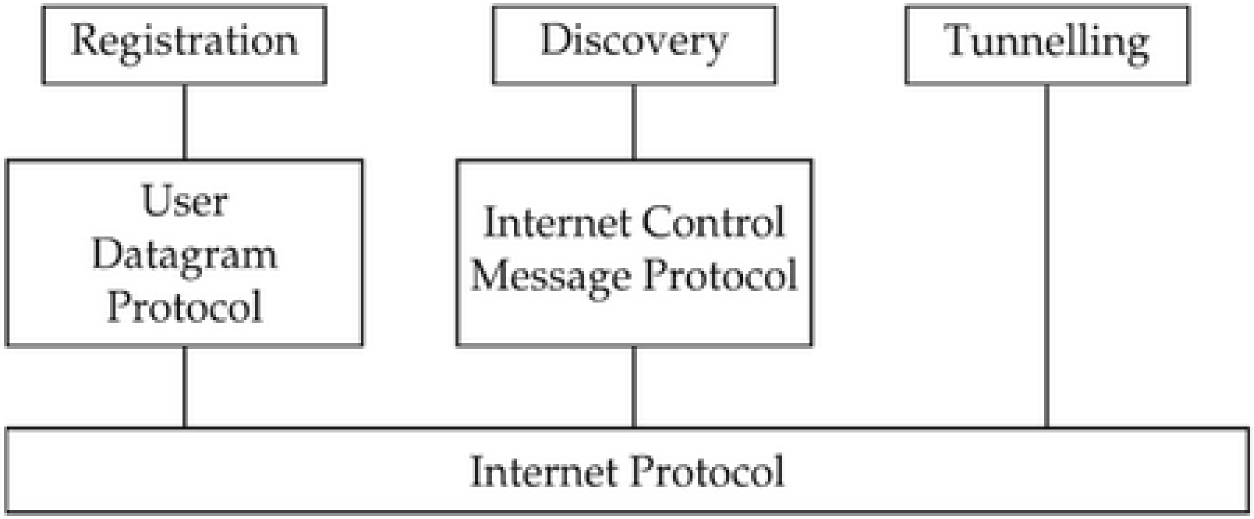
Scenario


COA
home network
router HA
router FA
MN
Internet
foreign network
CN
router

Key Mechanism used in Mobile IP

- 3 Basic Mechanism
  - Discovering the COA (Agent Discovery)
  - Registering the COA (Registration)
  - Tunneling to the COA (Tunneling)

Schematic Model of Mobile IP



Discovering the COA

- Each MN uses a discovery protocol to identify the respective home and foreign agent.
- Discovery of COA consists of following steps:
  1. Mobile Agent periodically broadcast "Agent Advertisement" msg
  2. On receiving "Agent Advertisement" msg, the MN can determine if it is in home network or foreign network.
  3. If the MN does not wish to wait, it transmits "Agent Solicitation" msg. A mobile agent will respond for this.

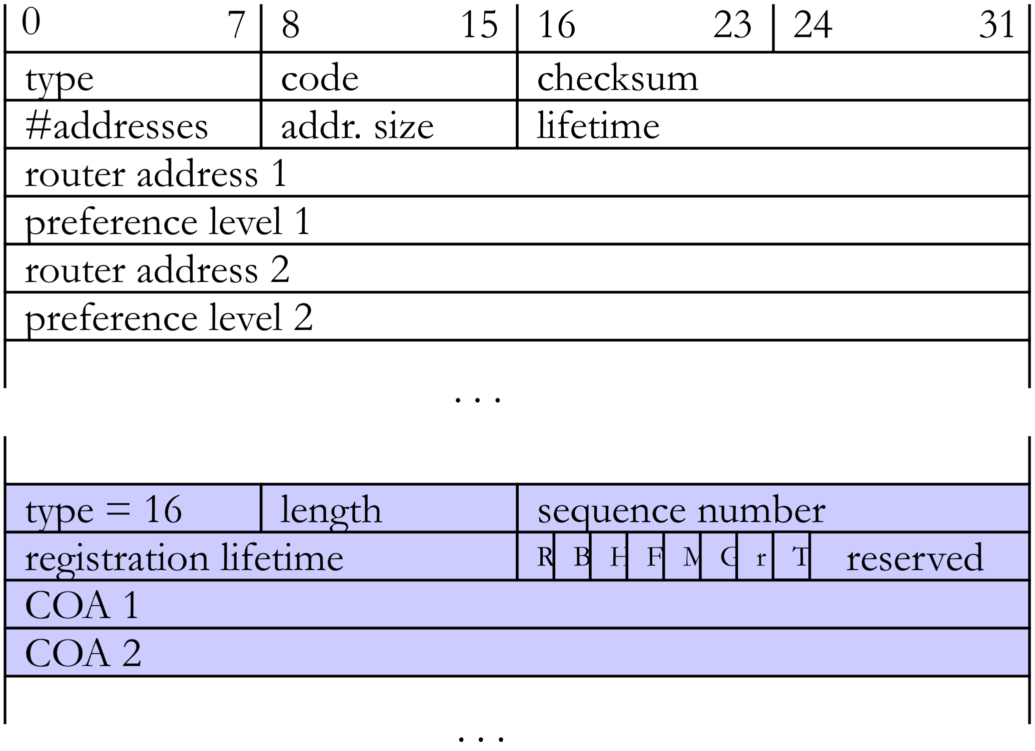
Agent Discovery

- How to find a foreign agent is the major problem.
- How does the MN discover that it has moved?
- 2 methods:
  - Agent advertisement
  - Agent solicitation

Agent Advertisement

- Home Agents and Foreign Agents periodically send **advertisement messages** into their physical subnets
- Advertisement is similar to Beacon Broadcast
- MN listens to these messages and detects, if it is in the home or a foreign network (standard case for home network)
- MN reads a COA from the FA advertisement messages

Agent Advertisement



0 7	8 15	16 23	24 31
type	code	checksum	
#addresses	addr. size	lifetime	
router address 1			
preference level 1			
router address 2			
preference level 2			
. . .			
type = 16	length	sequence number	
registration lifetime		R B H F M G r T	reserved
COA 1			
COA 2			
. . .			

RFC 1256 +mobility extension
(upper ICMP, lover mobility)
Type=9
Code 0 (normal)or 16(only mobile)

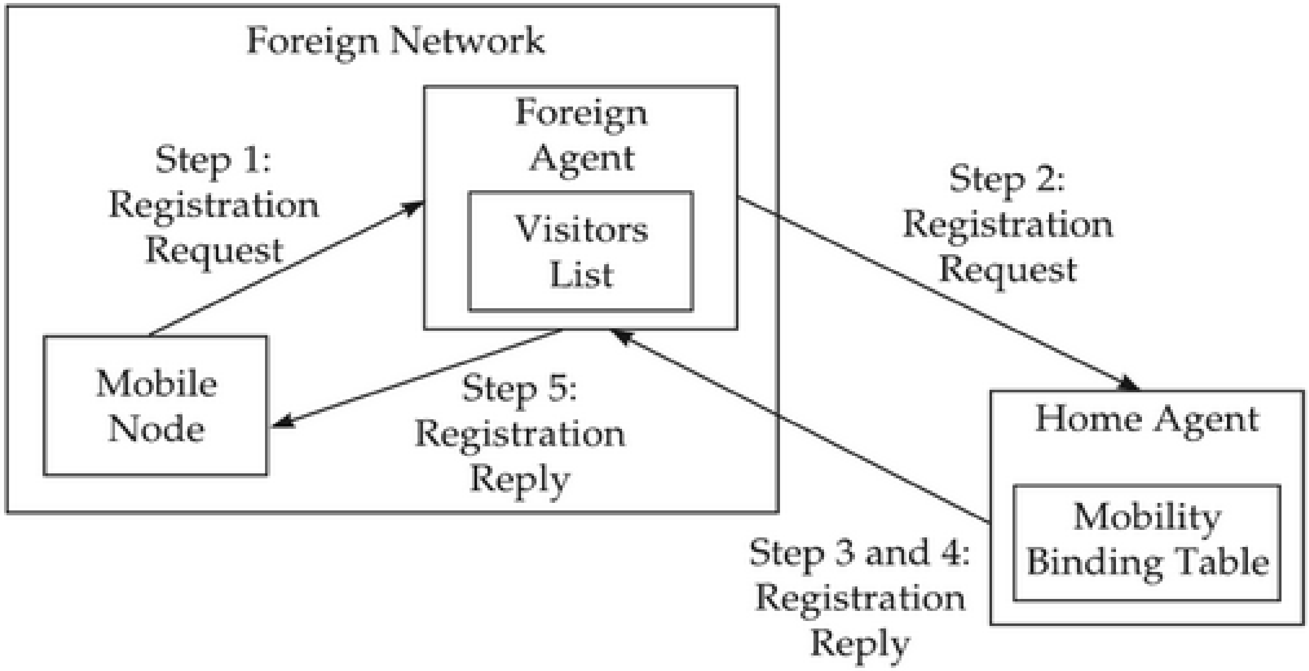
type = 16
length = 6 + 4 * #COAs
(6 = the number of bytes in the seq. no., Lifetime, Flags, and Reserved + another 4 bytes per each COA)
R: registration required
B: busy, no more registrations
H: home agent
F: foreign agent
M: minimal encapsulation
G: Generic Routing Encapsulation
r: =0, ignored (former Van Jacobson compression)
T: FA supports reverse tunneling
reserved: =0, ignored

Agent Solicitation

- The mobile node must send **agent solicitations** when it enters a foreign network.
- When a mobile node enters into a new network it can send out three solicitations, one per second
- If a MN does not get a new address, many packets will be lost
- If a MN does not receive an answer to its solicitations it must decrease the rate of solicitations exponentially to avoid flooding the network
- When the MN discovers a new agent it stops sending agent solicitation.
- A MN understands its FA by receiving an advertisement

Registering the COA

- MN Home network → No mobility services
- MN Foreign Network → Has COA
- Register the COA with HA.

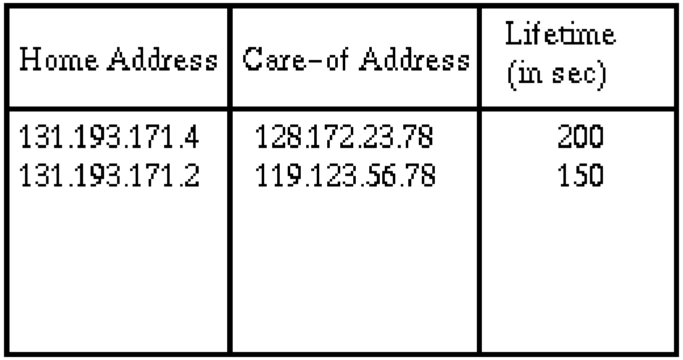

Foreign Network
Foreign Agent
Visitors List
Step 1: Registration Request
Mobile Node
Step 5: Registration Reply
Step 2: Registration Request
Home Agent
Mobility Binding Table
Step 3 and 4: Registration Reply

Registering the COA

- Step 1: Registration Request (MN → FA)
  - Registration request msg includes MN's IP Address (permanent), IP address of HA
- Step 2: Registration Request (FA→ HA)
  - Registration request msg includes MN's IP Address (permanent), IP address of FA
- Step 3: Updation of mobility binding table (HA)
  - Bind COA of MN with HA
- Step 4: Registration Reply (HA → FA)
  - Ack to FA
- Step 5: Registration Reply
  - Updates visitors list
  - Ack to MN

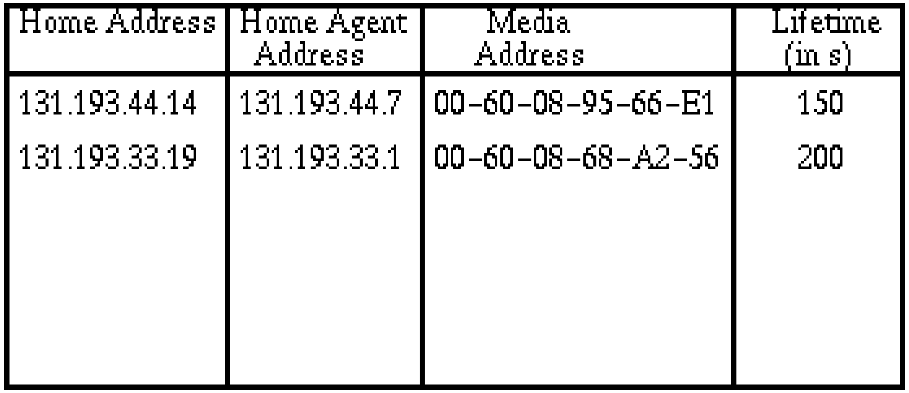
Tables maintained on routers

- Mobility Binding Table



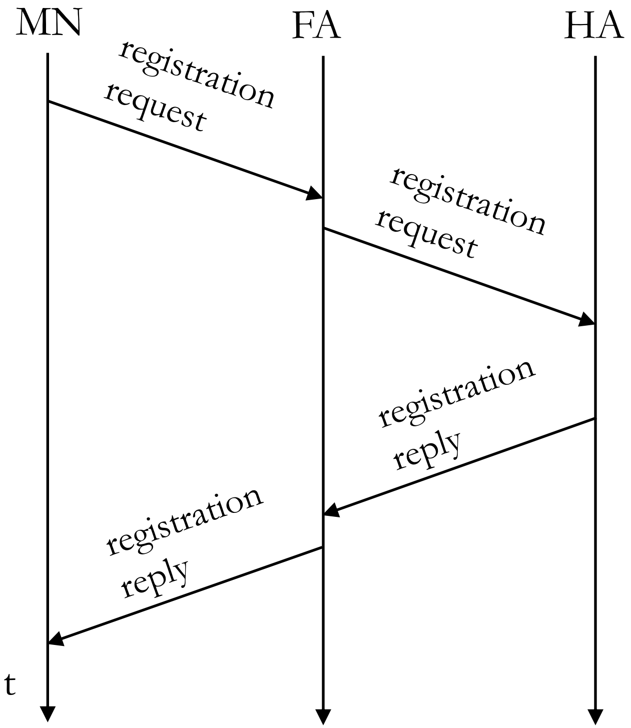
Home Address	Care-of Address	Lifetime (in sec)
131.193.171.4	128.172.23.78	200
131.193.171.2	119.123.56.78	150

- Visitor List

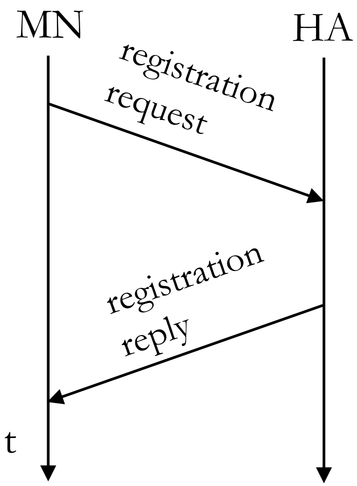


Home Address	Home Agent Address	Media Address	Lifetime (in s)
131.193.44.14	131.193.44.7	00-60-08-95-66-E1	150
131.193.33.19	131.193.33.1	00-60-08-68-A2-56	200

Registering the COA

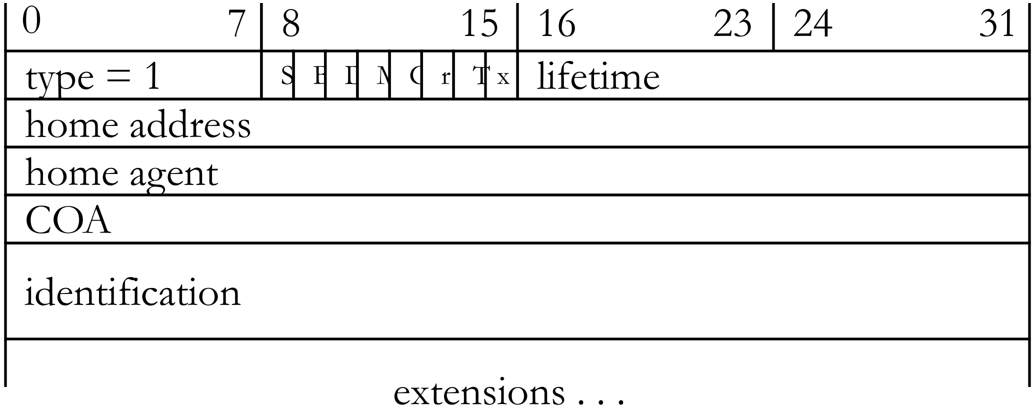


Foreign Agent COA



Co-located COA

Registration Request



0 7 | 8 15 | 16 23 | 24 31

type = 1 | S B D M G r T x | lifetime

home address

home agent

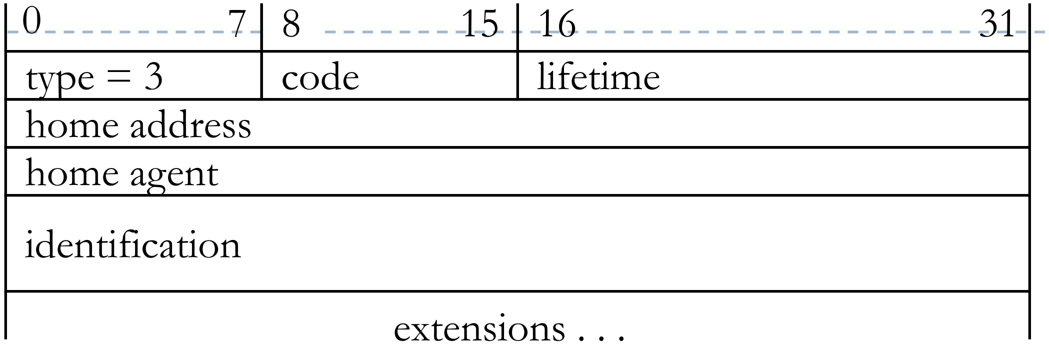
COA

identification

extensions . . .

S: simultaneous bindings (If MN wantsHA to retain prior mobility bindings)
B: broadcast datagrams (MN receives broadcast msgs which are broadcasted in Home network)
D: decapsulation by MN (Colocated COA→ Decapsulation at MN)
M: mininal encapsulation
G: GR Encapsulation
r: =0, ignored
T: reverse tunneling requested
x: =0, ignored
Identification : 64 bit id generated by MN to identify a request and match it with registration replies.

Registration Reply



0 ... 7	8 ... 15	16 ... 31
type = 3	code	lifetime
home address		
home agent		
identification		
extensions . . .		

Example codes:

registration successful

0 registration accepted

1 registration accepted, but simultaneous mobility bindings unsupported

registration denied by FA

65 administratively prohibited

66 insufficient resources

67 mobile node failed authentication

68 home agent failed authentication

69 requested Lifetime too long

registration denied by HA

129 administratively prohibited

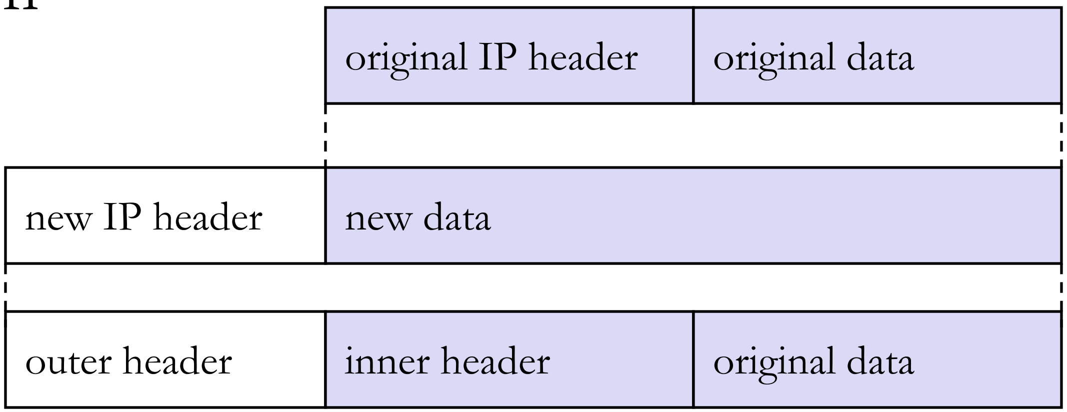
131 mobile node failed authentication

133 registration Identification mismatch

135 too many simultaneous mobility bindings

Tunneling to the COA

- Tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel end point.
- Tunneling→ sending a pkt through a tunnel is achieved by encapsulation
- Encapsulation → Taking a pkt (data + header), putting it into the data part of a new pkt.
- Decapsulation



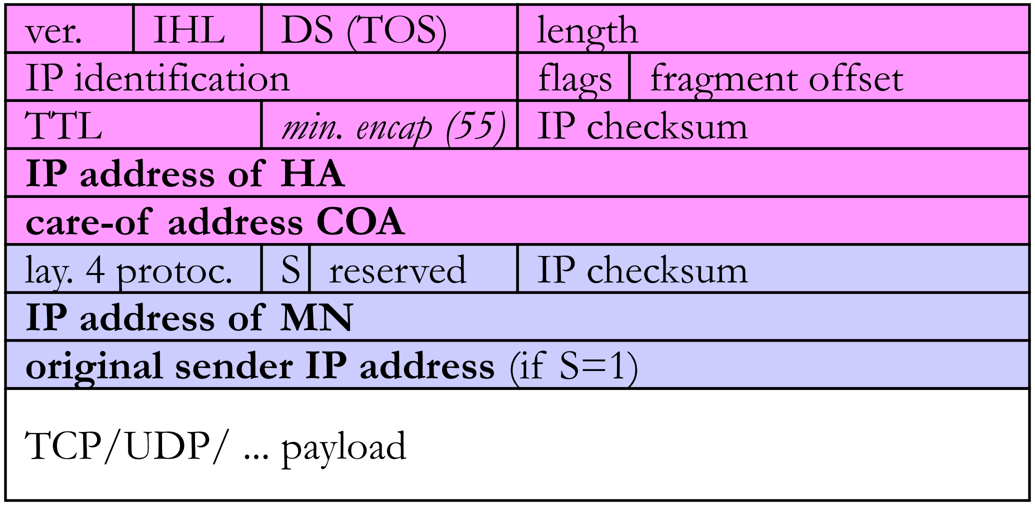
Encapsulation

- e.g. IPv6 in IPv4 (6Bone), Multicast in Unicast (Mbone)
- here: e.g. IP-in-IP-encapsulation, minimal encapsulation or GRE (Generic Record Encapsulation)
- IP-in-IP
  - Tunnel between HA and COA

ver.	IHL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL		*IP-in-IP (4)*	IP checksum	
IP address of HA				
Care-of address COA				
ver.	IHL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL		lay. 4 prot.	IP checksum	
IP address of CN				
IP address of MN				
TCP/UDP/ ... payload				

Encapsulation

- Minimal encapsulation (optional)
  - avoids repetition of identical fields
  - e.g. TTL, IHL, version, DS (RFC 2474, old: TOS)
  - only applicable for non fragmented packets, no space left for fragment identification



ver. | IHL | DS (TOS) | length

IP identification | flags | fragment offset

TTL | *min. encap (55)* | IP checksum

IP address of HA

care-of address COA

lay. 4 protoc. | S | reserved | IP checksum

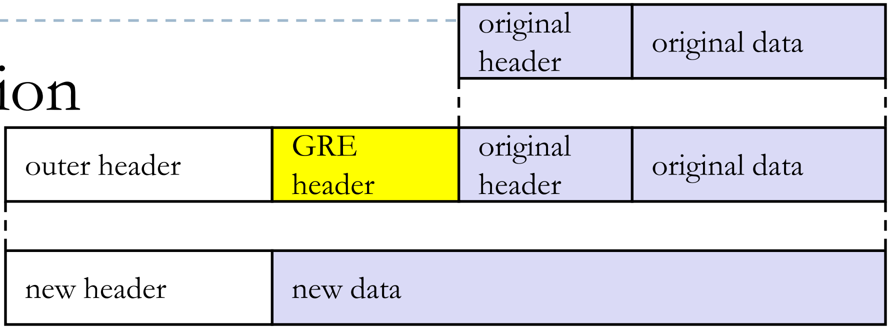
IP address of MN

original sender IP address (if S=1)

TCP/UDP/ ... payload

Encapsulation

- Generic Routing Encapsulation



RFC 1701

ver.	IHL	DS (TOS)		length	
IP identification				flags	fragment offset
TTL		*GRE(47)*		IP checksum	
IP address of HA					
Care-of address COA					
C R K S s	rec.	rsv.	ver.	protocol	
checksum (optional)				offset (optional)	
key (optional)					
sequence number (optional)					
routing (optional)					
ver.	IHL	DS (TOS)		length	
IP identification				flags	fragment offset
TTL		lay. 4 prot.		IP checksum	
IP address of CN					
IP address of MN					
TCP/UDP/ ... payload					

RFC 2784 (updated by 2890)

C	reserved0	ver.	protocol
checksum (optional)			reserved1 (=0)

C: Valid checksum

R:Routing fields are present

K: valid key for authentication

S:Sequence number is present

s: strict source routing

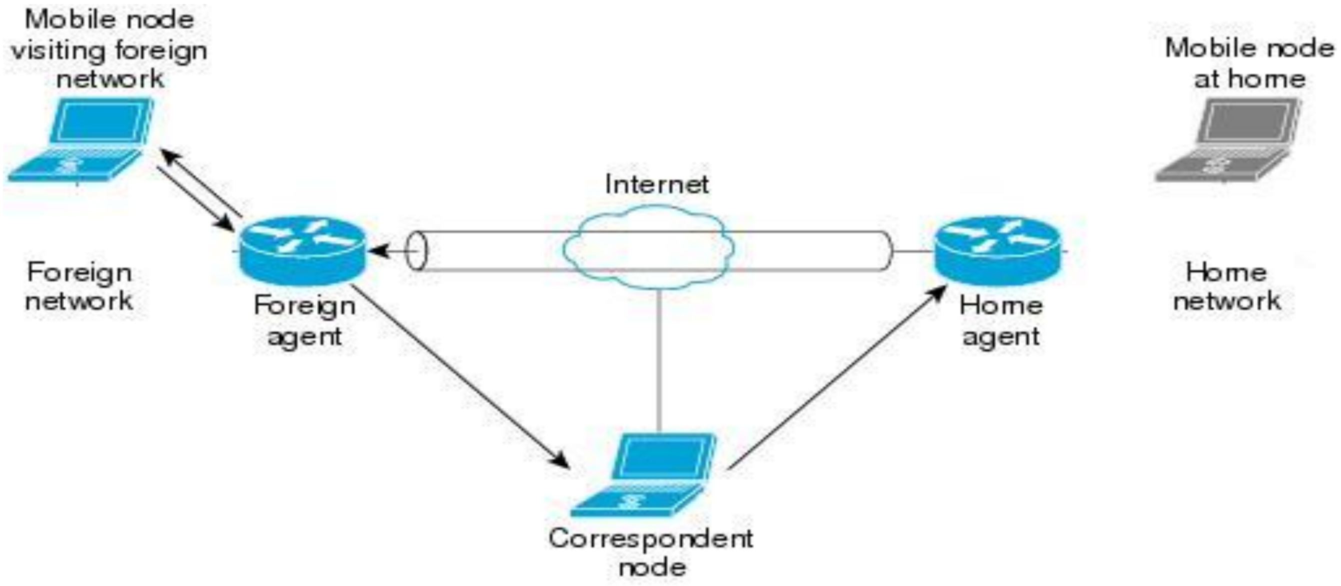
rec: recursion control (no. of recursive encapsulation allowed)

res: 0

ver: 0

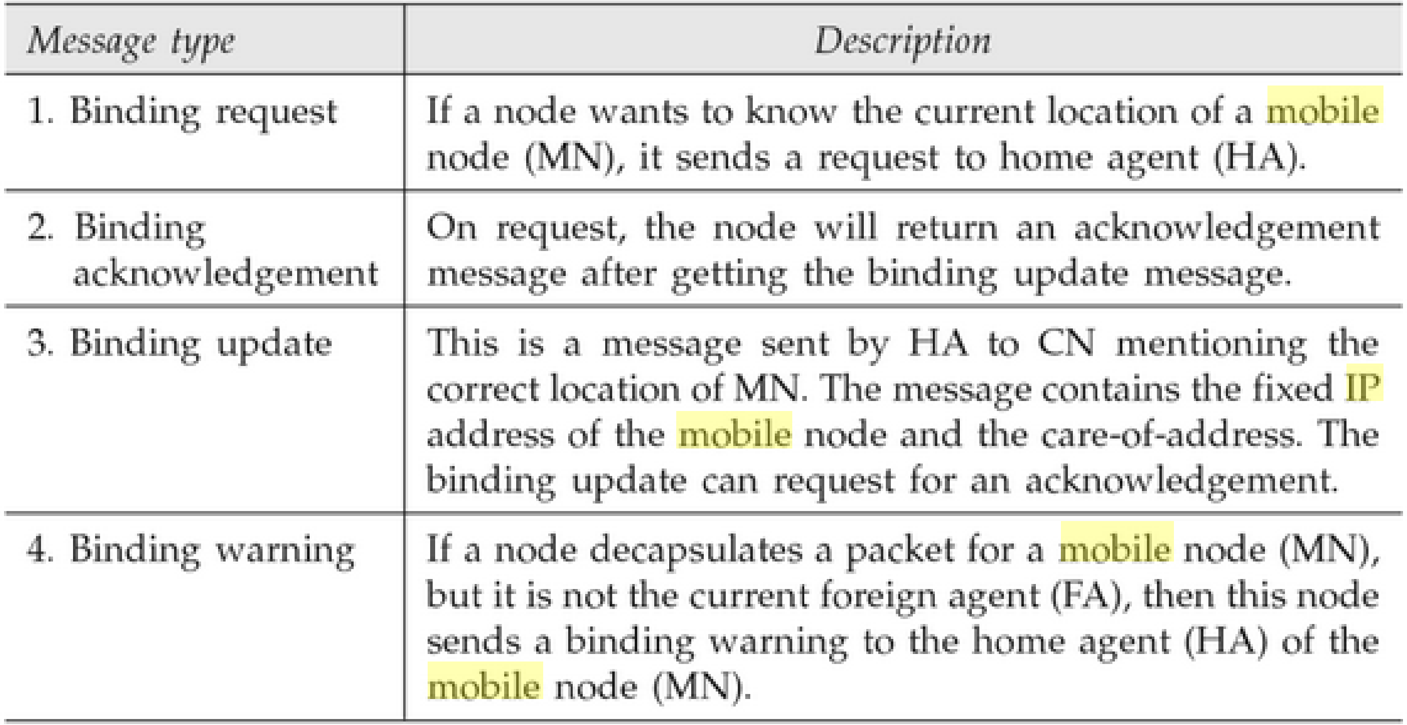
Route Optimization

- Triangular Routing (CN – HA, HA – COA/MN, MN – CN)
- 3 steps to optimize the route
  - Direct notification to CN
  - Direct tunnelling between CN and MN
  - Binding cache maintained at CN



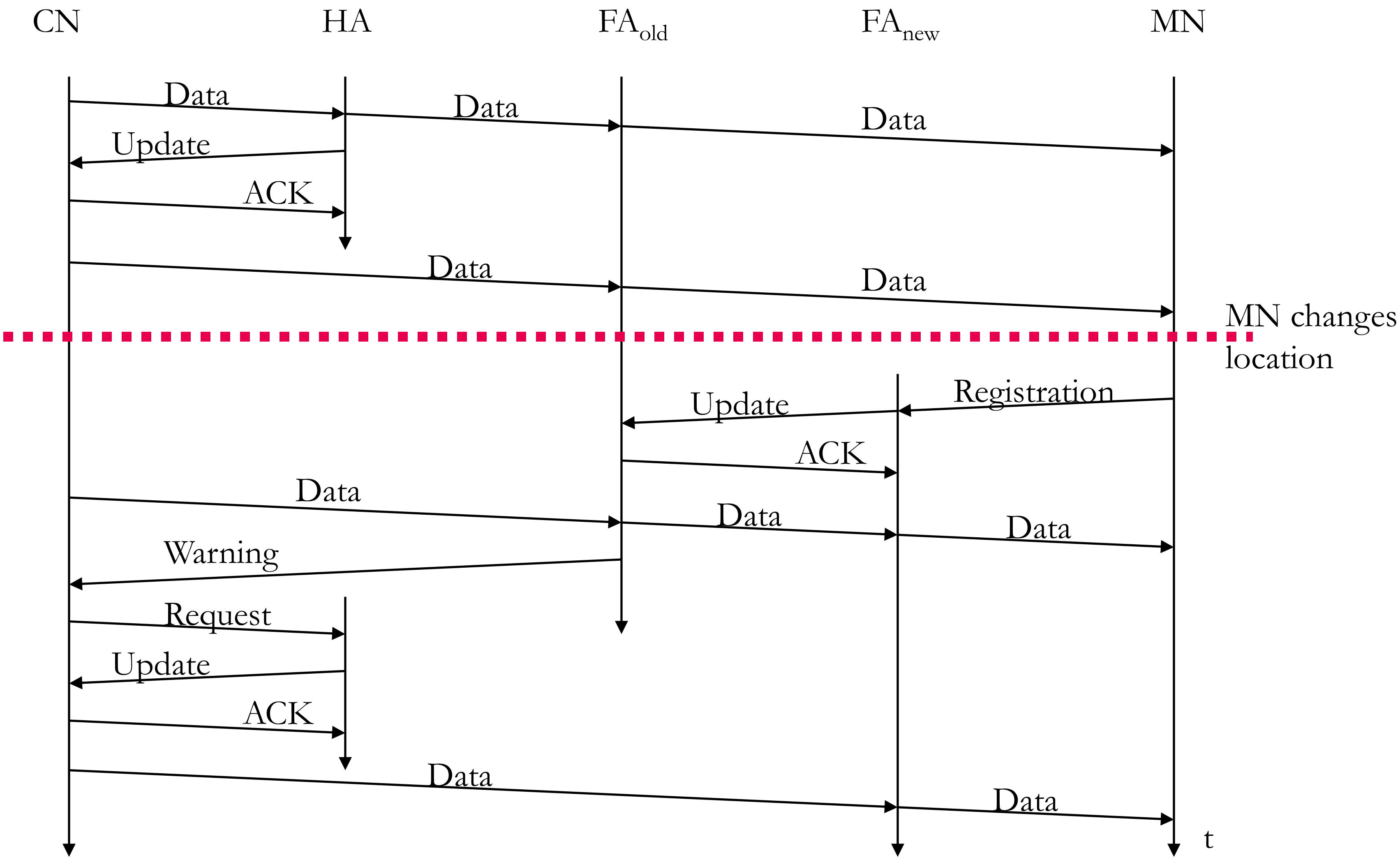
Route Optimization

- Binding → the association of Home address (IP of MN) with COA



Message type	*Description*
1. Binding request	If a node wants to know the current location of a mobile node (MN), it sends a request to home agent (HA).
2. Binding acknowledgement	On request, the node will return an acknowledgement message after getting the binding update message.
3. Binding update	This is a message sent by HA to CN mentioning the correct location of MN. The message contains the fixed IP address of the mobile node and the care-of-address. The binding update can request for an acknowledgement.
4. Binding warning	If a node decapsulates a packet for a mobile node (MN), but it is not the current foreign agent (FA), then this node sends a binding warning to the home agent (HA) of the mobile node (MN).

Route Optimization



DHCP

- Dynamic Host configuration Protocol
- DHCP automates the assignment of
  - Unique IP addresses
  - Subnet masks
  - Default gateways
  - Other IP parameters to individual computers and devices on the network.
- DHCP automatically assigns a new IP address when a node is moved into a different place in the network.
- BOOTP does not handle mobility

Preliminary

- (DHCP) Message → DHCP-PDU (A-PDU)
- Client → DHCP Client
- Server → DHCP Server
- Well-known port numbers
  - DHCP Server → UDP port 67
  - DHCP Client → UDP port 68
- Broadcast and Unicast used for PDU's in both directions

Phases of DHCP

- Discover Phase
- Offer Phase
- Request Phase
- Acknowledgement Phase
- Release Phase

Discover Phase

- When a DHCP configured devices connect to the network, the client sends a broadcast request (called a DISCOVER or DHCPDISCOVER) looking for a DHCP server to answer.

- The router directs the DHCPDISCOVER packet to the correct DHCP server.

- The DHCP server receives the DHCPDISCOVER packet.

- Based up on availability the server determines an appropriate IP address to give to the client.

Offer Phase

- The server temporarily reserves the IP address and response the client an Offer (DHCPOFFER) packet with the address information
- The server also configures the clients DNS servers, WINS servers, NTP servers, etc.

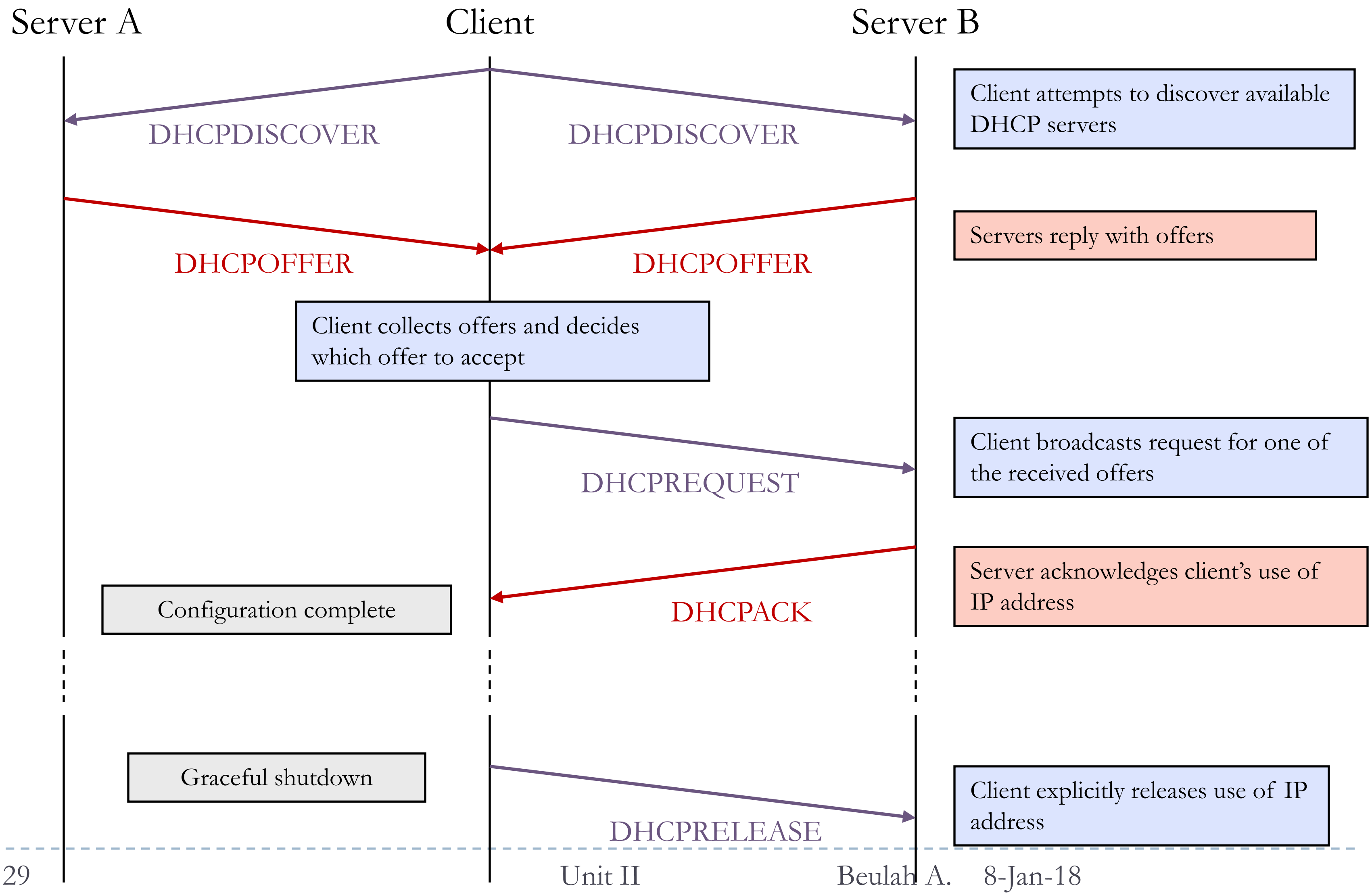
Request Phase

- The client sends a Request (DHCP REQUEST) packet, letting the DHCP server know that it intends to use that address.

Acknowledgement Phase

- The Server sends an Acknowledgement (DHCPACK) packet confirming client has been given a lease on the address
- A DHCP Lease is the amount of time a DHCP server grants the client permission to use a particular IP address.
- The Administrator of the DHCP server can set this.

DHCP - Protocol Mechanisms



Client attempts to discover available DHCP servers

Servers reply with offers

Client collects offers and decides which offer to accept

Client broadcasts request for one of the received offers

Server acknowledges client’s use of IP address

Configuration complete

Graceful shutdown

Client explicitly releases use of IP address

Ways of allocating IP Addresses

- **Manual allocation:** (static IP addresses): The server's administrator creates a configuration for the server that includes the MAC address and IP address of each DHCP client that will be able to get an address.
- **Automatic allocation:** The server's administrator creates a configuration for the server that includes only IP addresses, which it gives out to clients. An IP address, once associated with a MAC address, is permanently associated with it until the server's administrator intervenes.
- **Dynamic allocation**: Like automatic allocation except that the server will track leases and give IP addresses whose lease has expired to other DHCP clients.

Summary

- Key mechanisms in Mobile IP
  - Agent Discovery
  - Registration
  - Tunneling and Encapsulation
- Route Optimization
- DHCP
  - Different messages and steps in DHCP

Test Your Knowledge

- Which Internet Protocol (IP) number is used by a computer to send a message back to itself?
  - 0.0.0.0
  - 127.0.0.1
  - 255.255.255.255
- Which TCP/IP model layer does DHCP work at?

References

- Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.
- Prasant Kumar Pattnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi – 2012.