Mobile Computing – Mobile Network Layer

- MNL provides **protocol enhancement** that allows transparent **routing of IP datagrams** to mobile nodes in the internet.
  - **Moves data** into and through other **networks**.
  - **Routes packets** from the source host to the destination host.
  - **Translates logical** network address into **physical** address
  - Provides network layer **flow control**, network layer **error control & packet sequence control**.
  - **Breaks larger packets** into smaller packets.

Motivation for Mobile IP

- **Routing**
  - Based on IP destination address, network prefix (e.g. 129.13.42) determines **physical subnet**
  - Change of **physical subnet** implies change of **IP address** to have a topological correct address (standard IP) or needs special entries in the routing tables
- **Specific routes to end-systems**
  - Change of all routing table entries to forward packets to the **right destination**
- **Changing the IP-address**
  - Adjust the **host IP address** depending on the **current location**

Requirements to Mobile IP

- **Transparency**
  - **Mobility** should remain invisible for many **higher layer protocols** and applications.
  - Higher layers should continue to work even if the mobile computer has changed its attachment to the network.
- **Compatibility**
  - Mobile IP has to be **integrated** into existing O.S.
  - Mobile IP has to remain **compatible** with all lower layers
  - End-systems should be able to **communicate** with fixed systems.
  - Mobile IP has to ensure that users can still **access** all other servers.
- **Security**
  - **Authentication** of all registration messages
  - IP layer should guarantee that the **IP address** of the receiver is **correct**.
- **Efficiency and scalability**
  - Enhancing IP for mobility must not generate too many new **messages flooding the network.**
  - **Mutiple devices**, vehicles etc have IP implementation and they require mobile IP.

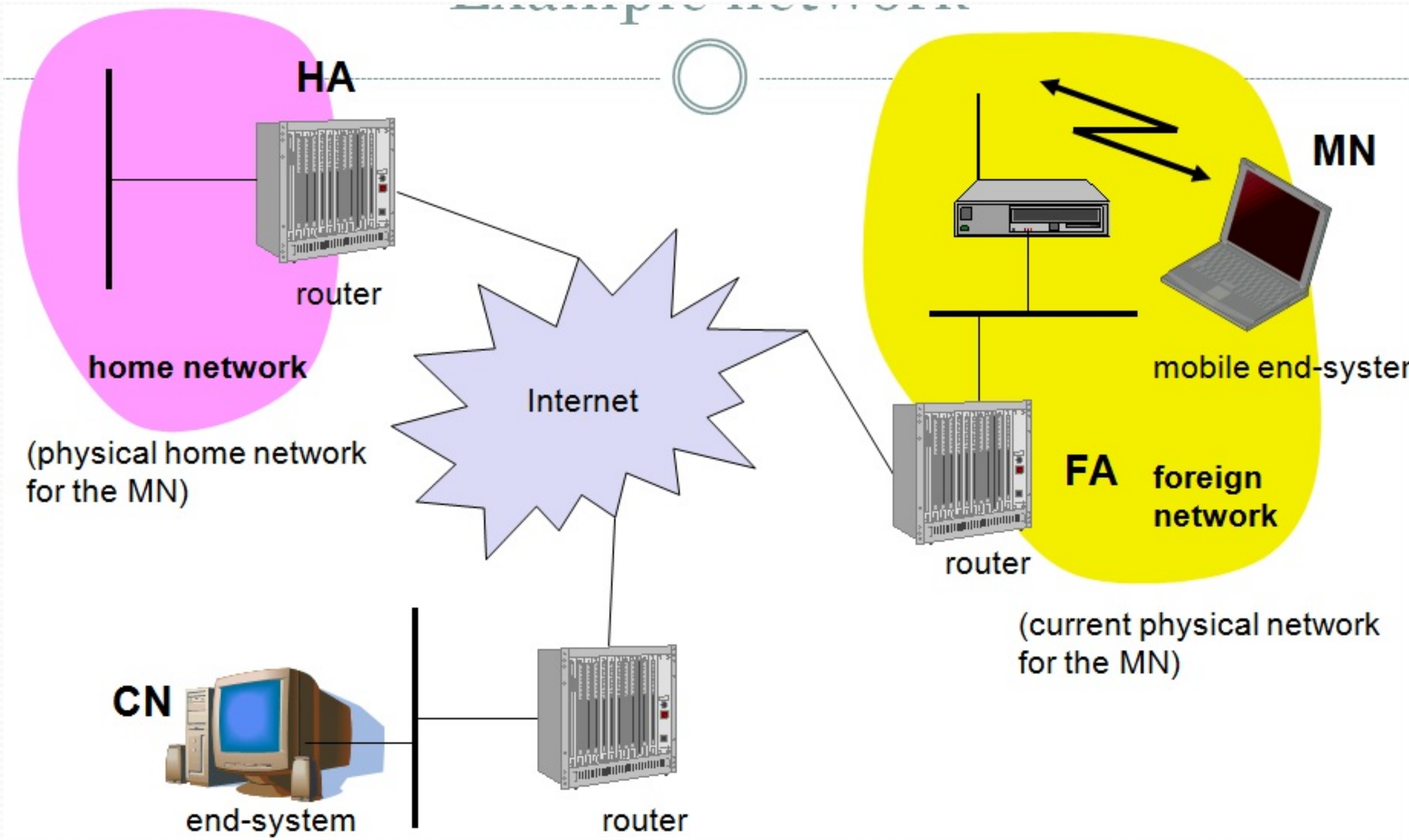
Entities & Terminology

- **Mobile Node** (MN) - System (node) that can change the point of connection to the network without **changing its IP address**
  - E.g laptop, mobile phone, router
- **Correspondent Node** (CN) – communication partner – fixed or mobile node
- **Home Network** (HN) – MN belongs to Home Network with respect to IP address.
- **Foreign Network** (FN) – visitor network for the MN
- **Foreign Agent** (FA)- acts as a **default router for the MN** when MN visits foreign network.
- **Care-of Address** (COA)- defines the **current location of the MN**.
  - IP packets sent to the MN are delivered to the COA
  - COA marks the **tunnel endpoint**

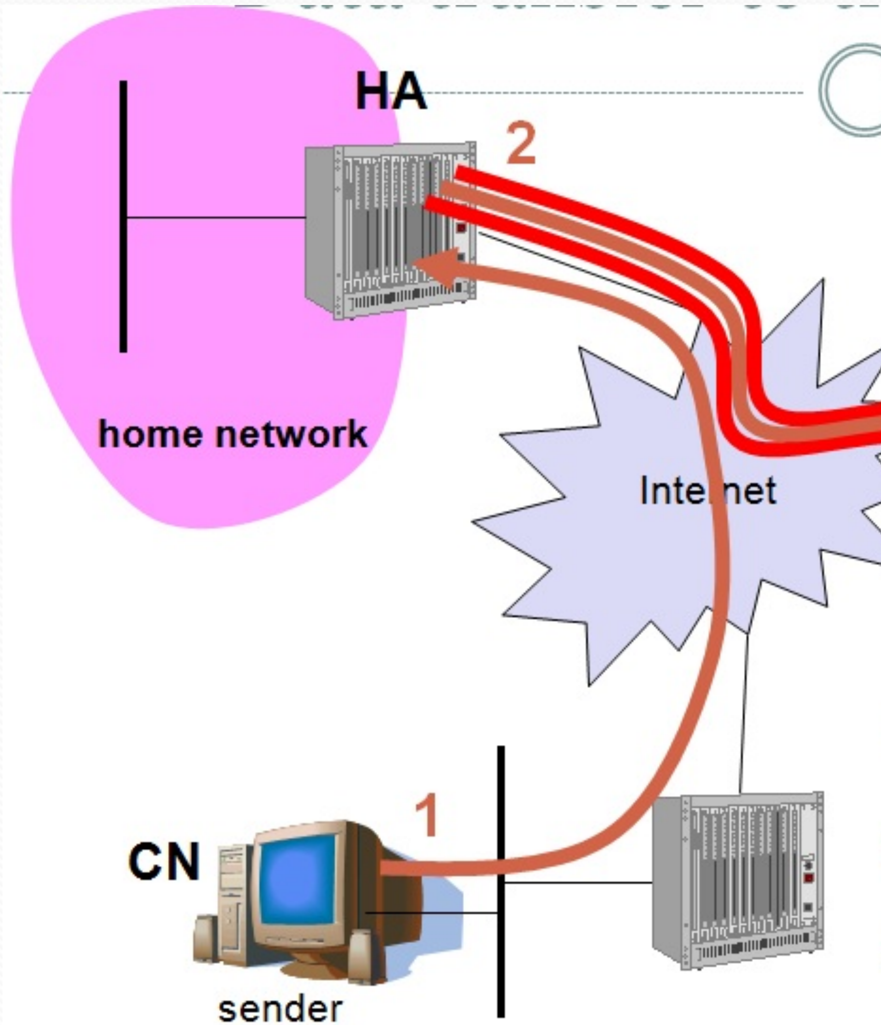
Entities & Terminology

- **Care-of Address** (COA)
  - Two possibilities:
    - **Foreign agent COA**:
      - COA is located at the FA , i.e COA is an IP address of the FA
      - The FA is the tunnel endpoint and forwards packets to the MN
    - **Co-located COA**:
      - COA is co-located if the MN temporarily acquired an additional IP address which acts as COA.
- **Home Agent** (HA)- provides services for the MN and it is located in the home network
  - Tunnel for packets toward the MN starts at the HA

Mobile IP Example Network

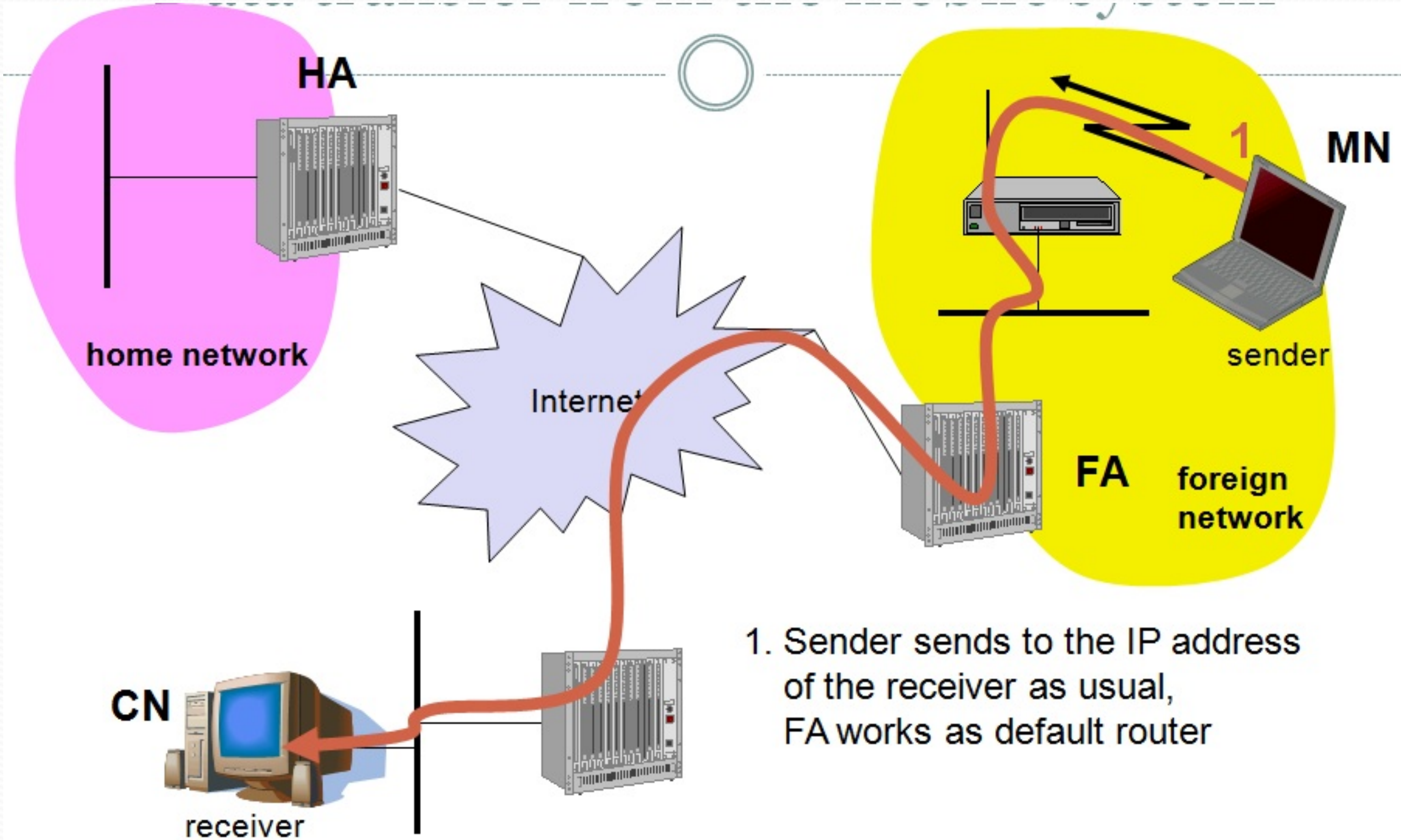


Data Transfer to the mobile system



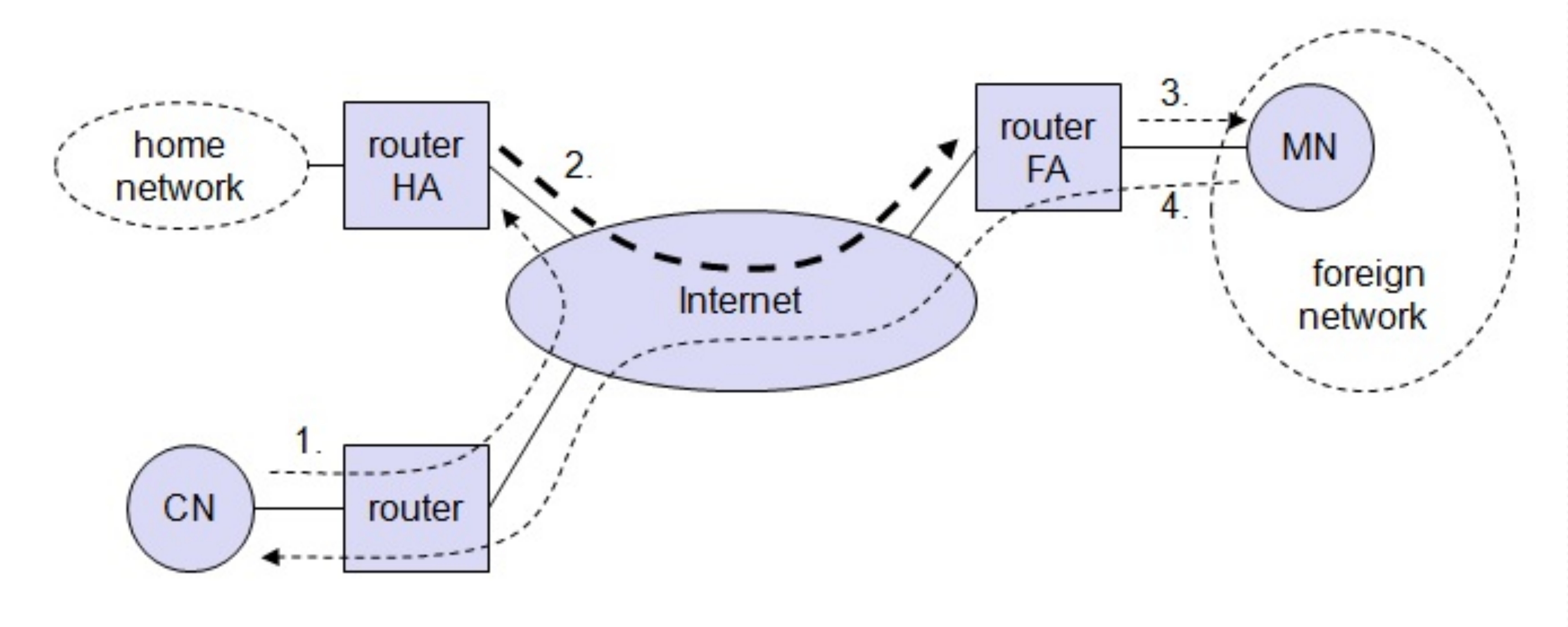
1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

Data Transfer from the mobile system



1. Sender sends to the IP address of the receiver as usual, FA works as default router

Packet Delivery to and from the mobile node



Network Integration

- **Agent Advertisement**
  - **HA and FA** periodically send **advertisement messages** into their physical subnets
  - **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
- **Registration**
  - **MN signals COA** to the HA, HA acknowledges to MN
  - These actions have to be secured by **authentication**
- **Advertisement**
  - **HA advertises the IP** address of the MN (as for fixed systems), i.e. standard routing information
  - **Routers adjust their entries**, these are stable for a longer time (HA responsible for a MN over a longer period of time)
  - **Packets to the MN are sent** to the HA,
  - Independent of changes in COA/FA

Agent Discovery

- **Mobile Node (MN)** needs to discover where it has moved
  - i.e it has to find its **foreign agent**
- Two methods used
  - **Agent advertisement**
    - In this foreign agents and home agents advertise their presence periodically using special **agent advertisement** messages.
    - **Internet Control Message Protocol (ICMP)** messages are used
    - **Routers advertise** their routing service periodically to the attached links.
  - **Agent solicitation**
    - In this MN tries to search for FA by sending **solicitation (**pinging/polling) messages

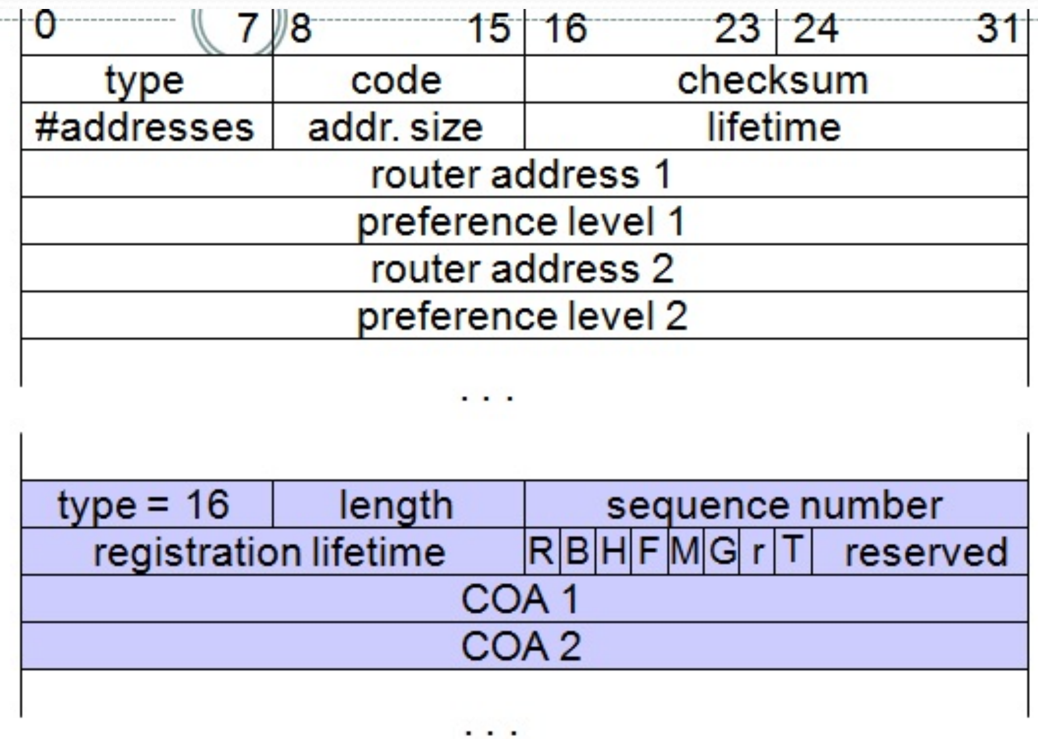
Agent Advertisement

- Agent advertisement packet
- Upper part represent the ICMP packet
  - Type – set to 9, code – set to 0, if agent routes traffic other than mobile traffic. Code- set to 16 if agent does not route anything else other than mobile traffic.
  - #addresses – denoted number of addresses advertised with the packet
  - Lifetime – denoted the length of time the advertisement is valid
    - Preference – helps a node to choose the router
- lower part is the extension needed for mobility.

Agent Advertisement

- Lower part of the packet – takes care of mobility
  - Type – set to 16
  - Length – depends on the number of COAs provided with the message
  - Sequence number – shows total number of advertisements sent since initialization.
  - Registration lifetime – agent specifies the maximum lifetime in seconds a node can request during registration.
  - R – shows if registration with agent is needed or not, B – shows if the agent is busy , H & F – indicates if its home or foreign agent, M & G – specify method of encapsulation M- minimal encapsulation, G – generic routing encapsulation. r-to specify header compression (0), T – reverse tunnel

Agent advertisement



type = 16
length = 6 + 4 * #COAs
R: registration required
B: busy, no more registrations
H: home agent
F: foreign agent
M: minimal encapsulation
G: GRE encapsulation
r: =0, ignored (former Van Jacobson compression)
T: FA supports reverse tunneling
reserved: =0, ignored

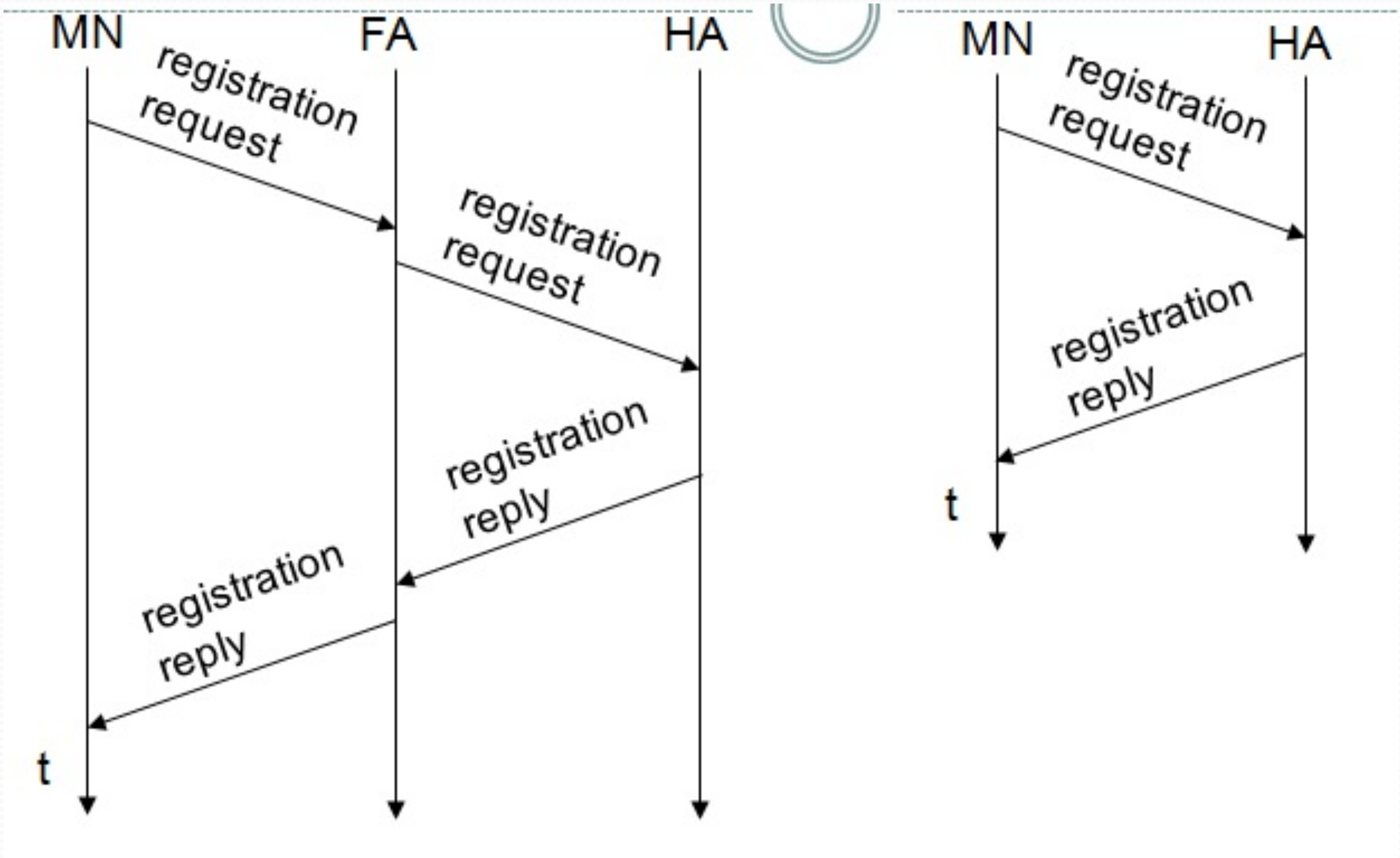
Agent Solicitation

- If no agent advertisements are available, the MN sends agent solicitations.
- MN sends three solicitations, one per second, as soon as it enters a new network
- **Challenge**
  - Dynamic nature of wireless networks and mobility of MNs one second delay could also lead to delay.
  - Multiple solicitation messages may flood the network

Registration

- Having received COA, MN has to register with the HA
- Registration is required to inform the HA of the current location for correct forwarding of packets.
- Two ways of registration
  - COA at FA
    - FA forwards the request to HA
  - COA at HA
    - MN directly contacts HA
- **Mobility Binding – Registration**
  - Lifetime of the registration negotiated during the registration process
  - MN should register before expiration

Registration



Mobile IP 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
B: broadcast datagrams
D: decapsulation by MN
M mininal encapsulation
G: GRE encapsulation
r: =0, ignored
T: reverse tunneling requested
x: =0, ignored

Registration Reply

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

Registration Reply Codes - Example

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

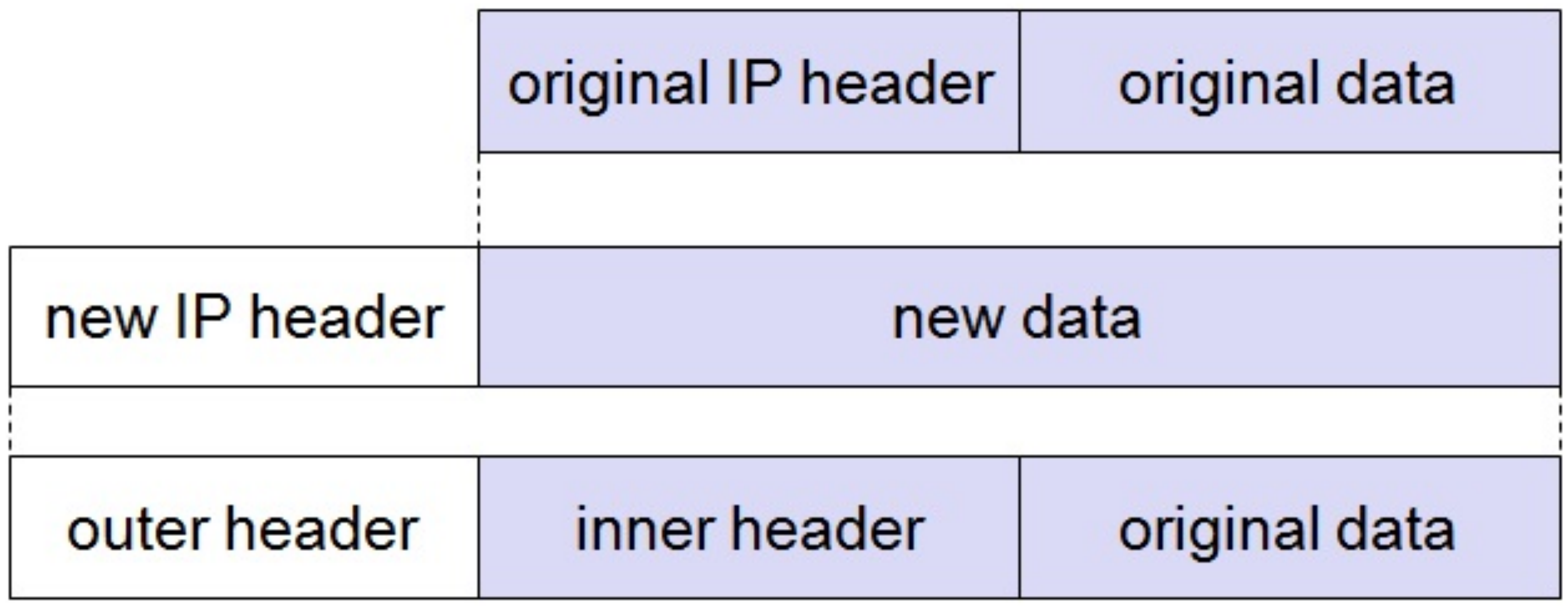
registration denied by HA

- 129 administratively prohibited
- 131 mobile node failed authentication
- 133 registration Identification mismatch
- 135 too many simultaneous mobility bindings

Tunneling & Encapsulation

- **Tunnel**: It establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint.
  - It is achieved by using encapsulation.
- **Encapsulation**: It is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet.
- **Decapsulation:** taking a packet out of the data part of another packet
  - Encapsulation & decapsulation is performed when a packet is transferred from a higher protocol layer to a lower layer.

IP Encapsulation



Encapsulation I (IP –in – IP encapsulation)

<table>
<tr><td>ver.</td><td>IHL</td><td>DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="3">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td>IP-in-IP</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="5">IP address of HA</td></tr>
<tr><td colspan="5">Care-of address COA</td></tr>
<tr><td>ver.</td><td>IHL</td><td>DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="3">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td>lay. 4 prot.</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="5">IP address of CN</td></tr>
<tr><td colspan="5">IP address of MN</td></tr>
<tr><td colspan="5">TCP/UDP/ ... payload</td></tr>
</table>

IP –in – IP encapsulation

- **Ver** – version 4, IPV4
  IHL – internet header length (length of outer header) – 32 bits
  DS(TOS) – differentiated services – type of service – copied from the inner header
  length – length of encapsulated packet
  TTL – time to leave (must be high for the packet to reach tunnel endpoint)
  IP-in-IP – type of protocol used in IP protocol
  checksum – for error correction
  IP address of HA – tunnel entry as source address
  COA – tunnel exit as destination address
- Inner Header – same fields as outer header
  IP address of CN- original sender
  IP address of MN – receiver MN of the packet

Encapsulation II (Minimal Encapsulation)

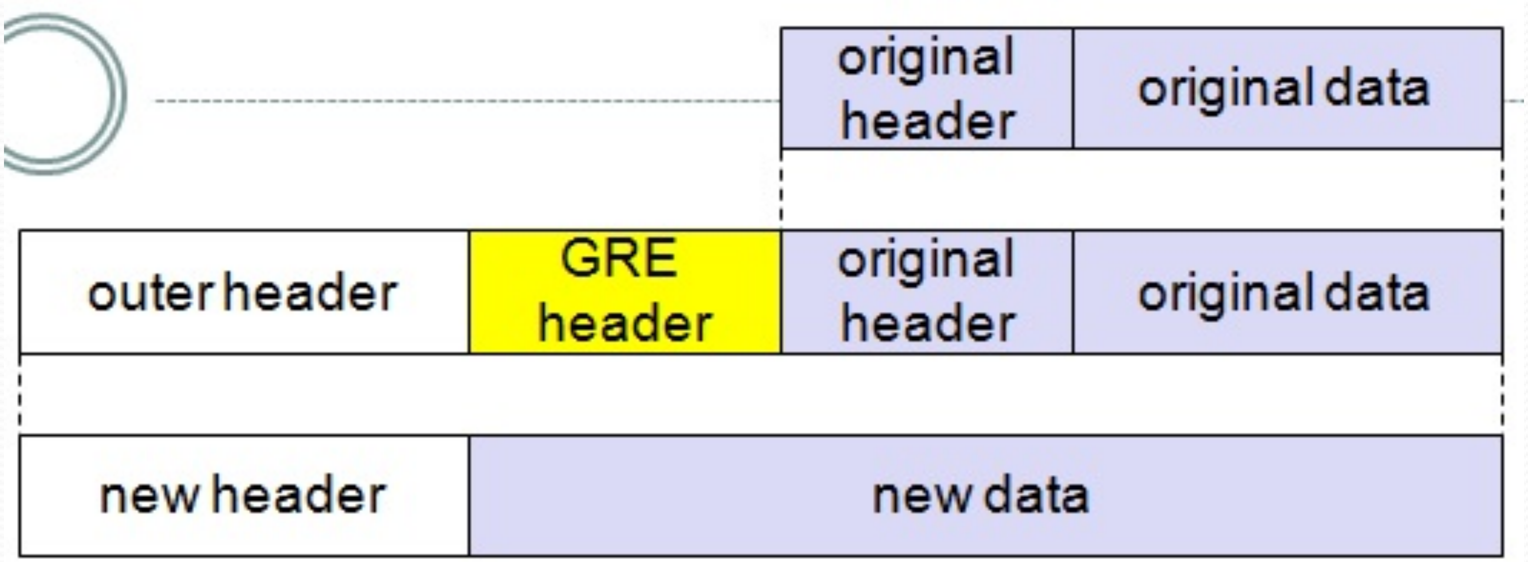
<table>
<tr><td>ver.</td><td>IHL</td><td colspan="2">DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="4">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td colspan="2">min. encap.</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="6">IP address of HA</td></tr>
<tr><td colspan="6">care-of address COA</td></tr>
<tr><td colspan="2">lay. 4 protoc.</td><td>S</td><td>reserved</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="6">IP address of MN</td></tr>
<tr><td colspan="6">original sender IP address (if S=1)</td></tr>
<tr><td colspan="6">TCP/UDP/ ... payload</td></tr>
</table>

Minimal Encapsulation

- Drawback of IP-in-IP encapsulation
  - Several fields are redundant
- Minimal Encapsulation
  - Address of the MN is needed
  - Only applicable for unfragmented packets
    S – if it is set, the original sender address of the CN is included
  - No field for fragmentation offset is left in the inner header

Generic Routing Encapsulation

- **Drawback of IP-in-IP & Minimal Encapsulation**
  - Both work only for IP
- GRE supports other network protocols also
  - It allows encapsulation of packets of one protocol suite into the payload portion of a packet of another suite.



Generic Routing Encapsulation

RFC 1701

<table>
<tr><td colspan="4">ver.</td><td colspan="2">IHL</td><td colspan="2">DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="8">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="6">TTL</td><td colspan="2">GRE</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="10">IP address of HA</td></tr>
<tr><td colspan="10">Care-of address COA</td></tr>
<tr><td>C</td><td>R</td><td>K</td><td>S</td><td>s</td><td>rec.</td><td>rsv.</td><td>ver.</td><td colspan="2">protocol</td></tr>
<tr><td colspan="8">checksum (optional)</td><td colspan="2">offset (optional)</td></tr>
<tr><td colspan="10">key (optional)</td></tr>
<tr><td colspan="10">sequence number (optional)</td></tr>
<tr><td colspan="10">routing (optional)</td></tr>
<tr><td colspan="4">ver.</td><td colspan="2">IHL</td><td colspan="2">DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="8">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="6">TTL</td><td colspan="2">lay. 4 prot.</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="10">IP address of CN</td></tr>
<tr><td colspan="10">IP address of MN</td></tr>
<tr><td colspan="10">TCP/UDP/ ... payload</td></tr>
</table>

Generic Routing Encapsulation

- Outer header
  standard IP header with HA as source address & COA as destination address.
- GRE header
  C- indicates checksum, if C is set – checksum field contains a valid IP checksum
  R – indicates if routing fields are present, if R is set – contains fields for source routing.
  Key – used for authentication
  S- sequence number field – used for decapsulator to restore packet order. **s** – indicates strict source routing is used.
  rec- recursion control – distinguishes GRE from IP-in-IP & minimal encapsulation.
  rsv- fields are 0 and ignored
  ver-version field contains 0 for GRE version.
- Inner header

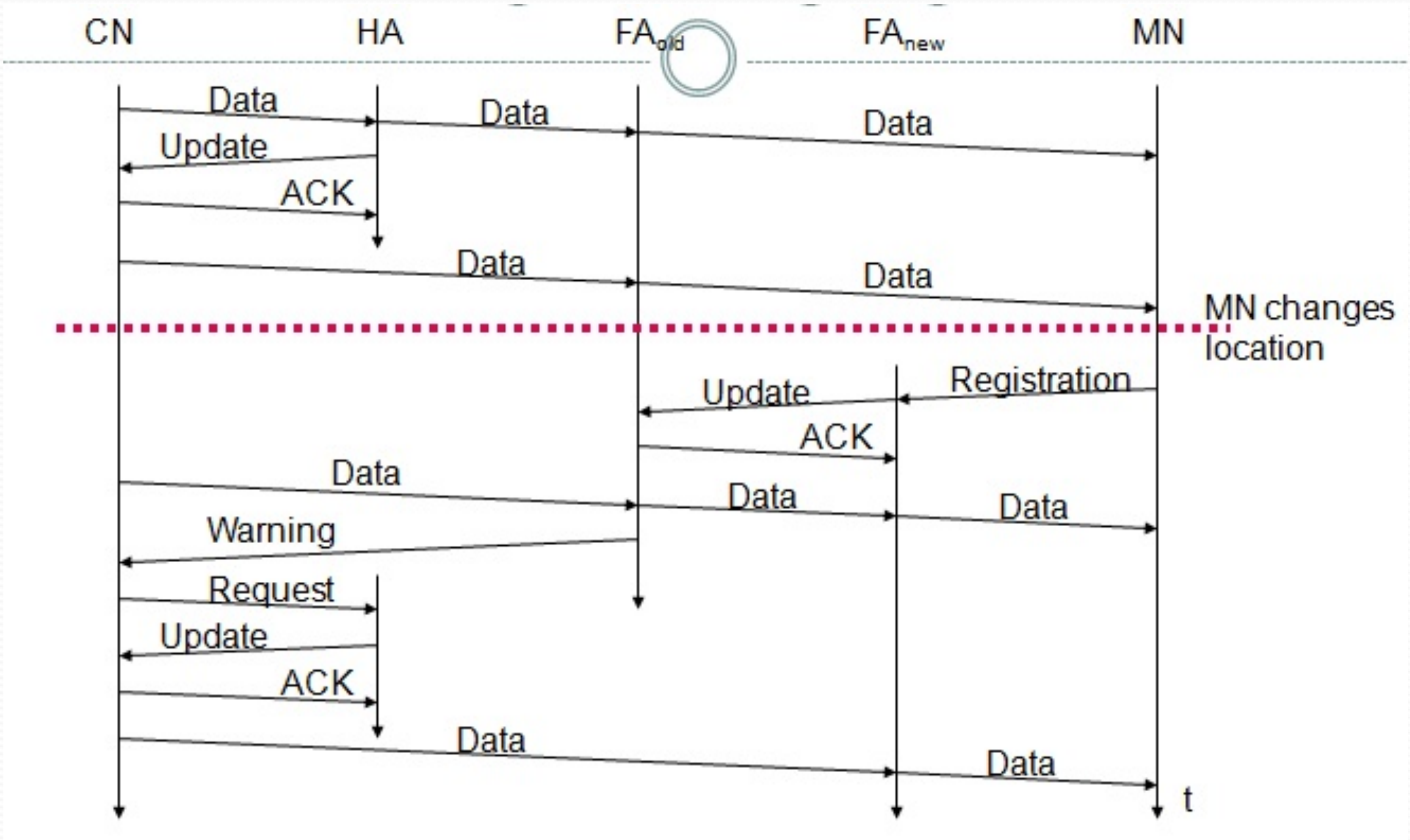
Optimization of Packet Forwarding

- **Drawback of normal routing (Triangular Routing)**
  - Sender (CN) sends all packets via HA to MN
    - E.g 2 nodes belonging to different country trying to send data
  - higher **latency & network load**
- **Solution**
  - Inform CN of the current location of the MN
    - CN stores information in its **binding cache –** in its routing table
  - HA informs CN of the location of MN

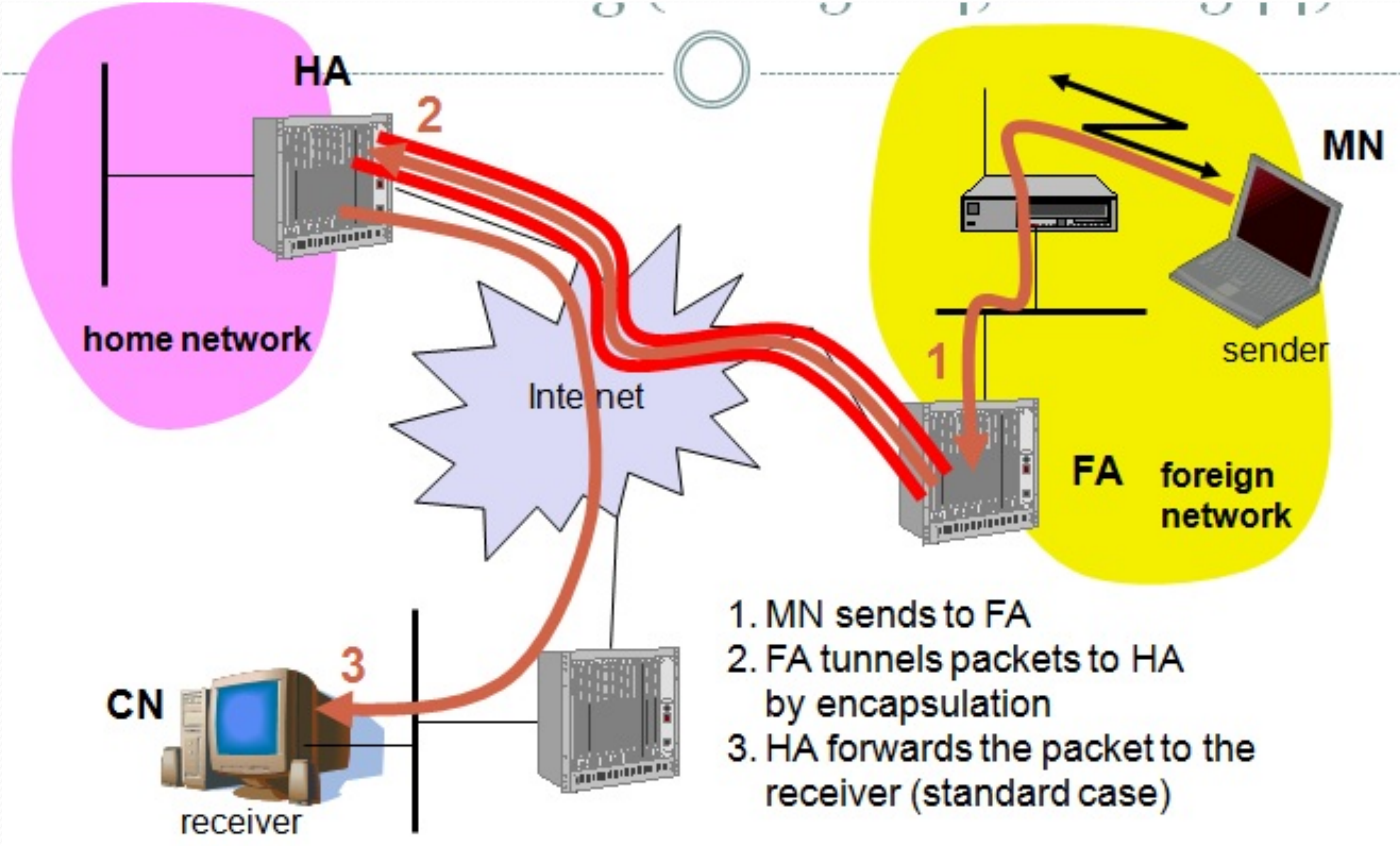
Optimization messages

- **Binding request:**
  - CN sends binding request to HA
  - HA reveals the binding update back to CN
- **Binding update:**
  - Message from HA to CN contains the fixed IP address of the MN/COA
  - Binding update requests for acknowledgement
- **Binding acknowledgement:**
  - CN sends a acknowledgement after receiving a binding update message
- **Binding warning:**
  - HA sends warning message to inform CN if the binding has become stale (i.e when communicating agent is not present)

Change of Foreign Agent



Reverse Tunneling



1. MN sends to FA
2. FA tunnels packets to HA by encapsulation
3. HA forwards the packet to the receiver (standard case)

Mobile IP with Reverse Tunneling

- Reverse Tunneling takes care of the following issues:
  - **Firewall:** Allows packets with topologically correct addresses to pass
    - Provides protection against misconfigured systems of unknown addresses.
  - **Multi-cast:** allows MN to participate in a multicast group
    - Well defined group of addresses (belonging to HA)
  - **TTL:** since TTL is short, packet received by HA will be delivered faster than packet getting sent directly from MN to CN

Mobile IP & IPv6

- Mobile IP was developed for IPv4, but IPv6 simplifies the protocols
  - **Security is integrated** and not an add-on, **Authentication of registration is included**
  - **COA** can be assigned via **auto-configuration**, every node has address auto-configuration
  - **No need for a special agent advertisement**, all routers perform router advertisement.
  - MN can signal directly to COA/CN, sending via HA not needed in this case (**Automatic Path Optimization**)
  - **Soft hand-over**, i.e. without packet loss, between two subnets is supported
    - MN sends the new COA to its old router
    - The old router encapsulates all incoming packets for the MN and forwards them to the new COA
    - **Authentication** is always granted

Challenges with mobile IP

- **Security**
  - **Authentication with FA problematic**, for the FA typically belongs to another organization
  - **Key management and key distribution** has been standardized in the Internet
- **Firewalls**
  - Typically mobile IP cannot be used together with firewalls, **special set-ups are needed** (such as reverse tunneling)
- **QoS**
  - **Tunneling-**takes time - encapsulation

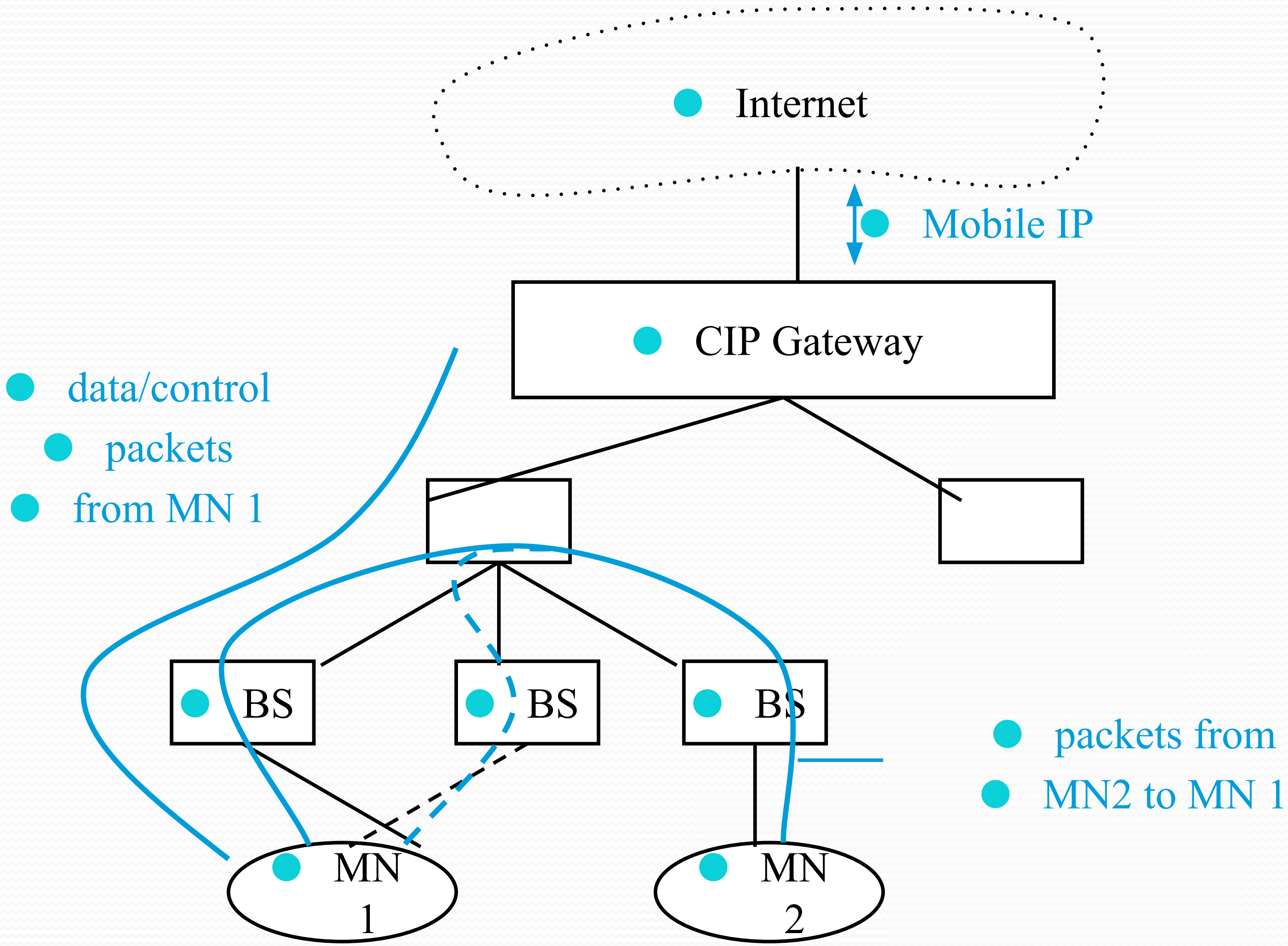
IP Micro-mobility support

- Micro-mobility support:
  - **Efficient local handover** inside a foreign domain **without involving a home agent**
  - **Reduces control traffic**
  - Especially needed in case of **route optimization**
- Example approaches:
  - **Cellular IP**
  - **HAWAII** (Handoff-Aware Wireless Access Internet Infrastructure
  - **Hierarchical Mobile IP** (HMIP)
- Important criteria:
  - **Security Efficiency, Scalability, Transparency, Manageability**

IP Micro-mobility support –Cellular IP

- **Cellular IP Gateway (CIPGW):** provides **local handovers without renewed registration** for each domain.
  - Inside the domain, **all nodes collect routing information** for accessing MNs based on the origin of packets sent by the MNs towards the CIPGW
  - **Handovers are achieved** by allowing **simultaneous forwarding** of packets destined for a mobile node along **multiple paths.**
  - **Mobile node moving between adjacent cells** is able to receive packets via both old and new base stations(BS)
  - CIPGW – handles mobile IP tunnel endpoint
  - CIPGW – handles initial registration processing

Architecture of Cellular IP

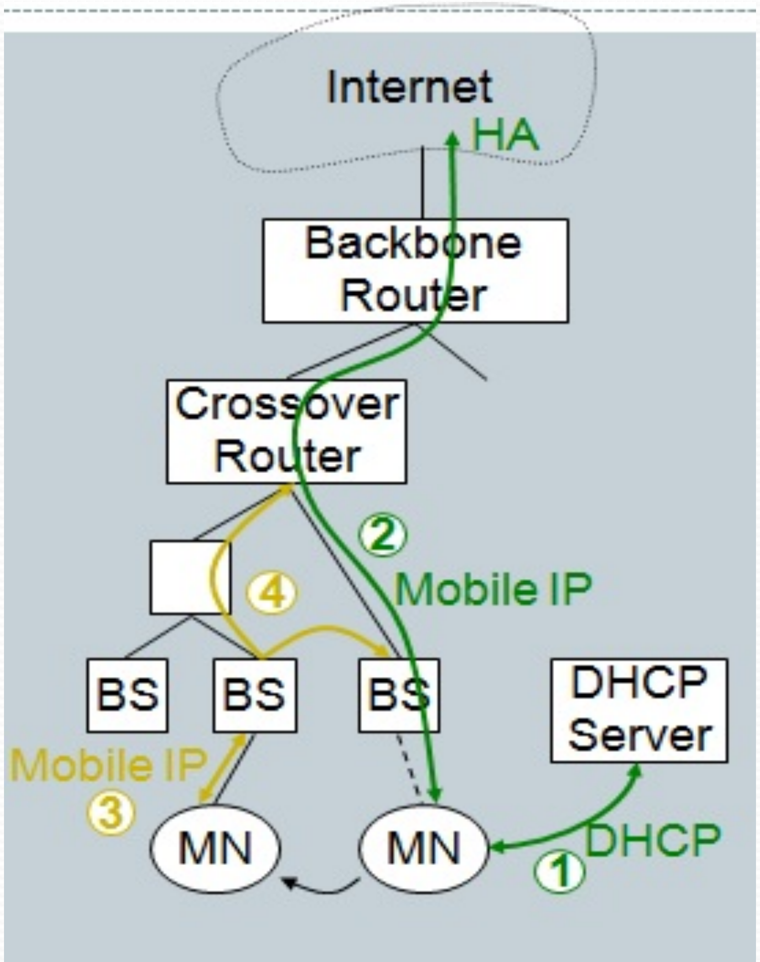


Cellular IP

- Advantages
  - **Manageability:**
    - Cellular IP is **self-configuring**
    - Integration of the CIPGW into firewall **facilitate administration of mobility-related functionality**.
- Disadvantages
  - **Efficiency:** additional network load is induced by forwarding packets on multiple paths.
  - **Transparency:** changes to MNs are required
  - **Security:** routing tables are changed based on messages sent by MNs.

IP Micro-mobility support –Hawaii

- Hawaii (Handoff-Aware Wireless Access Internet Infrastructure)
  - MN obtains co-located COA and registers with HA
  - **Handover**: MN keeps COA, new BS answers Registration request and updates routers
  - **Reconfiguration** of all routers on the path from old and new BS – **crossover router**

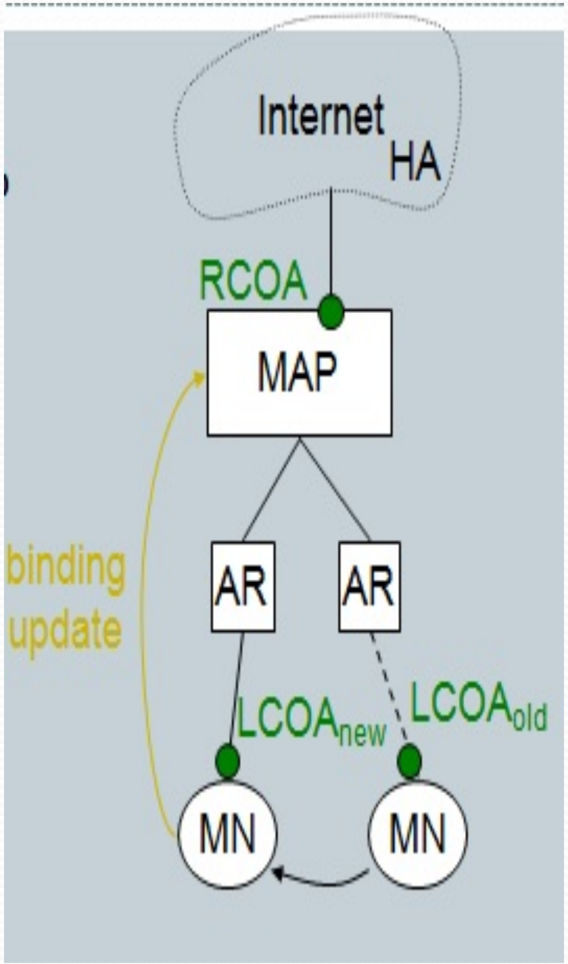


Hawaii

- Advantages:
  - **Security**: Challenge-response extensions are mandatory
  - **Transparency**: HAWAII is mostly transparent to mobile nodes
- Disadvantages:
  - **Security**: There are no provisions regarding the setup of IPSec tunnels.

–Hierarchical Mobile IPv6 (HMIPv6)

- Operation:
  - Network consists of Mobility Anchor Point (MAP)
    - Mapping of regional COA(RCOA) to link COA (LCOA)
  - Upon handover, MN informs MAP only
    - Gets new LCOA, keeps RCOA
  - HA is only contacted if MAP changes.



Hierarchical Mobile IPv6 (HMIPv6)

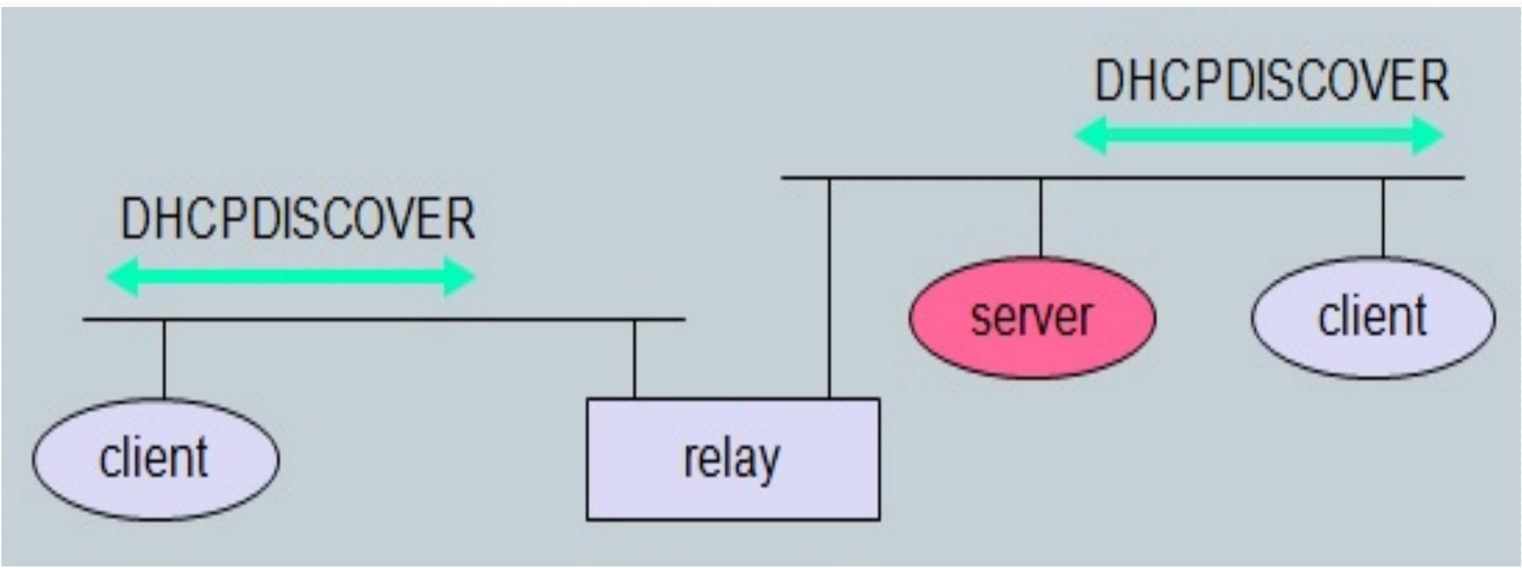
- Advantages:
  - **Security**: Local COAs can be hidden, which provides some location privacy
- Disadvantages:
  - **Transparency**: Additional infrastructure component (MAP)
  - **Security**: Routing tables are changed based on messages sent by MNs.
    - Demands for **strong authentication and protection**

DHCP: Dynamic Host Configuration Protocol

- Application
  - It simplifies **installation and maintenance** of networked computers
  - Supplies systems with all necessary information, such as **IP address, DNS server address, domain name, subnet mask, default router** etc.
  - **Enables automatic int**egration of systems into an Intranet or the Internet, can be used to acquire a COA for Mobile IP.
- **Client/Server-Model**
  - The client sends via a MAC broadcast a request to the DHCP server (DHCP relay)

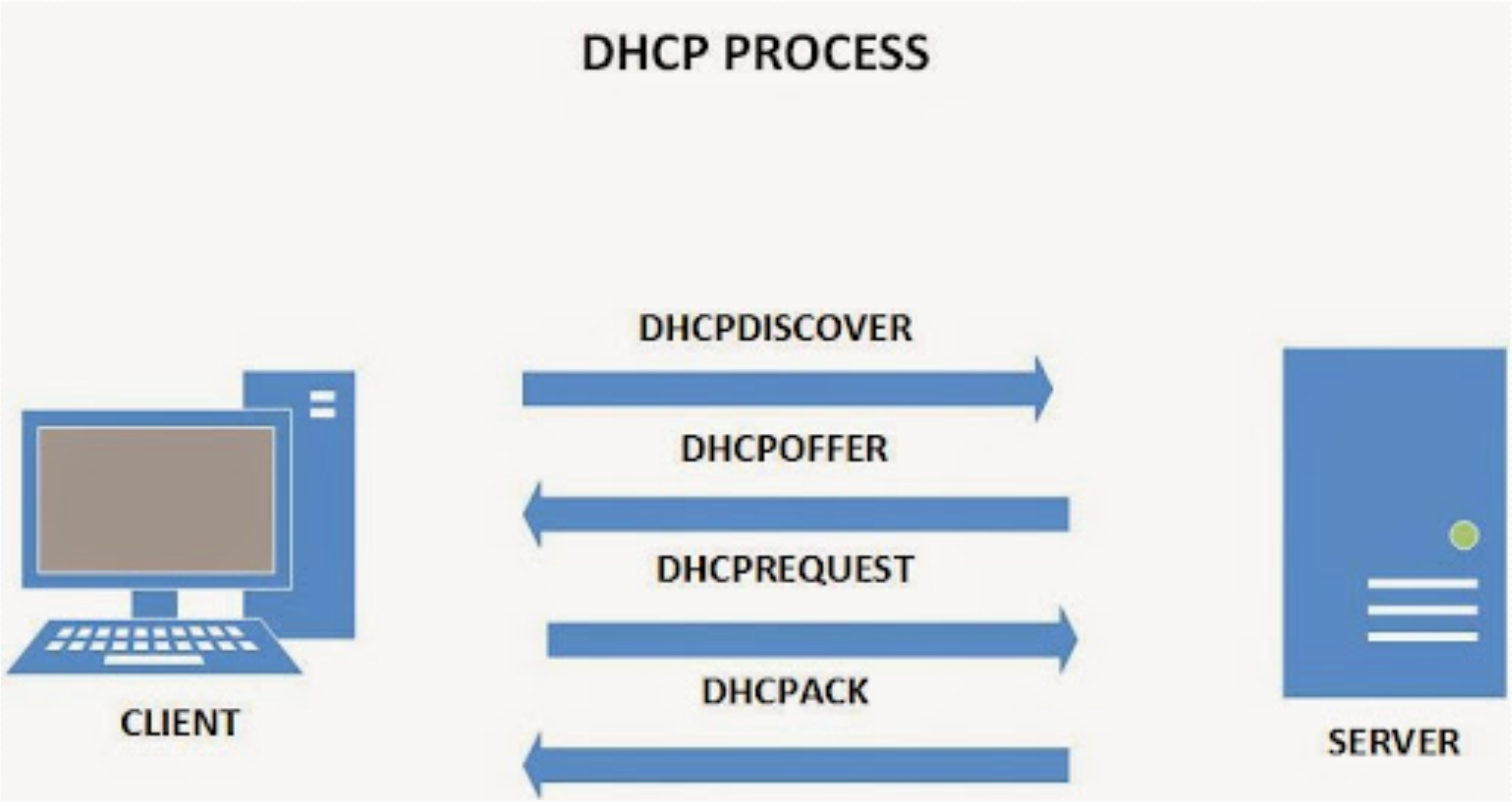
DHCP Configuration

- DHCP client send a request to a server (DHCPDISCOVER) to which the server responds
  - Client sends requests using **MAC broadcasts** to reach all devices in the LAN.
  - DHCP relay is used to forward requests across inter-working units to a DHCP server.

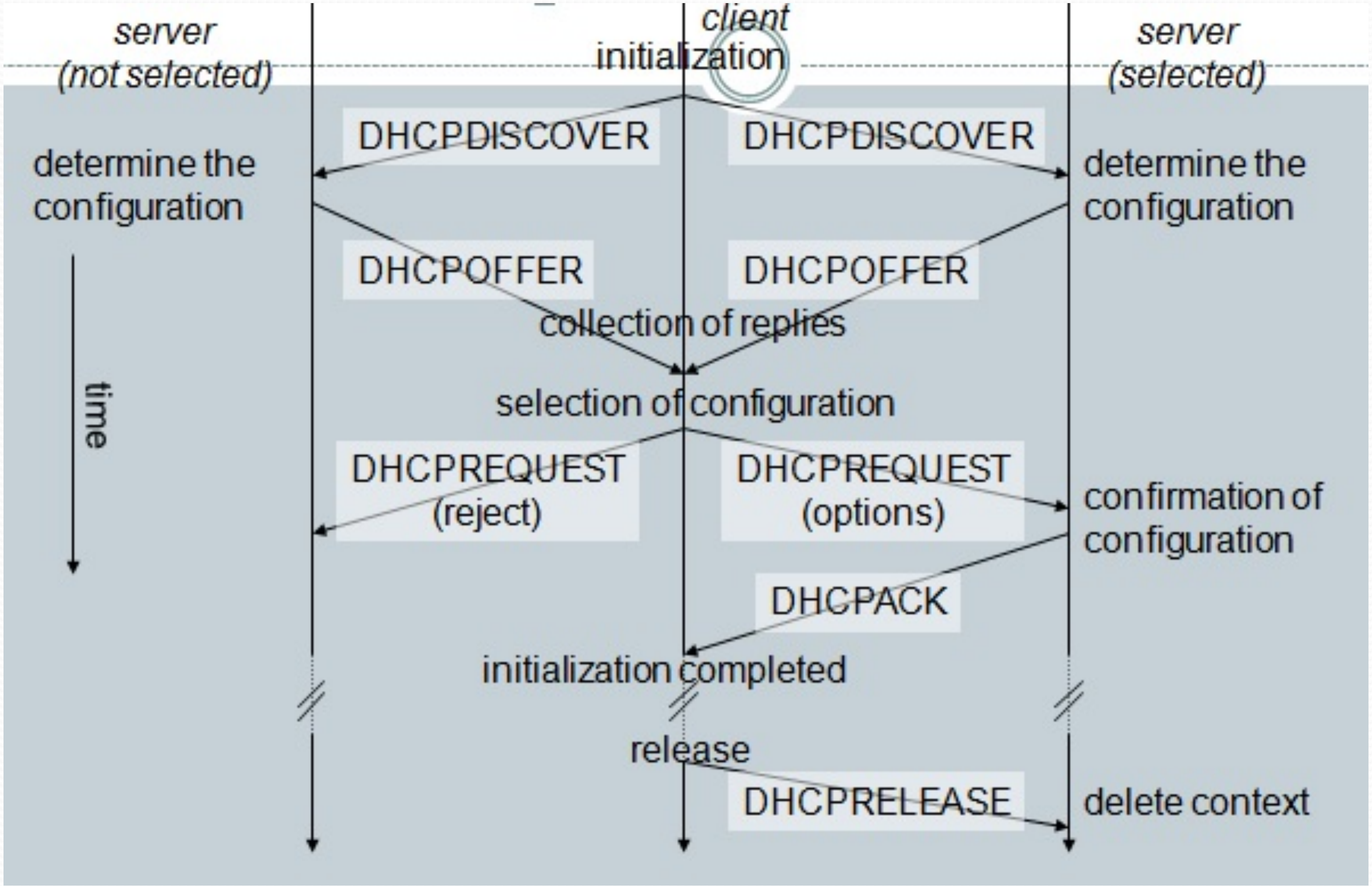


DHCP Server

DHCP Process



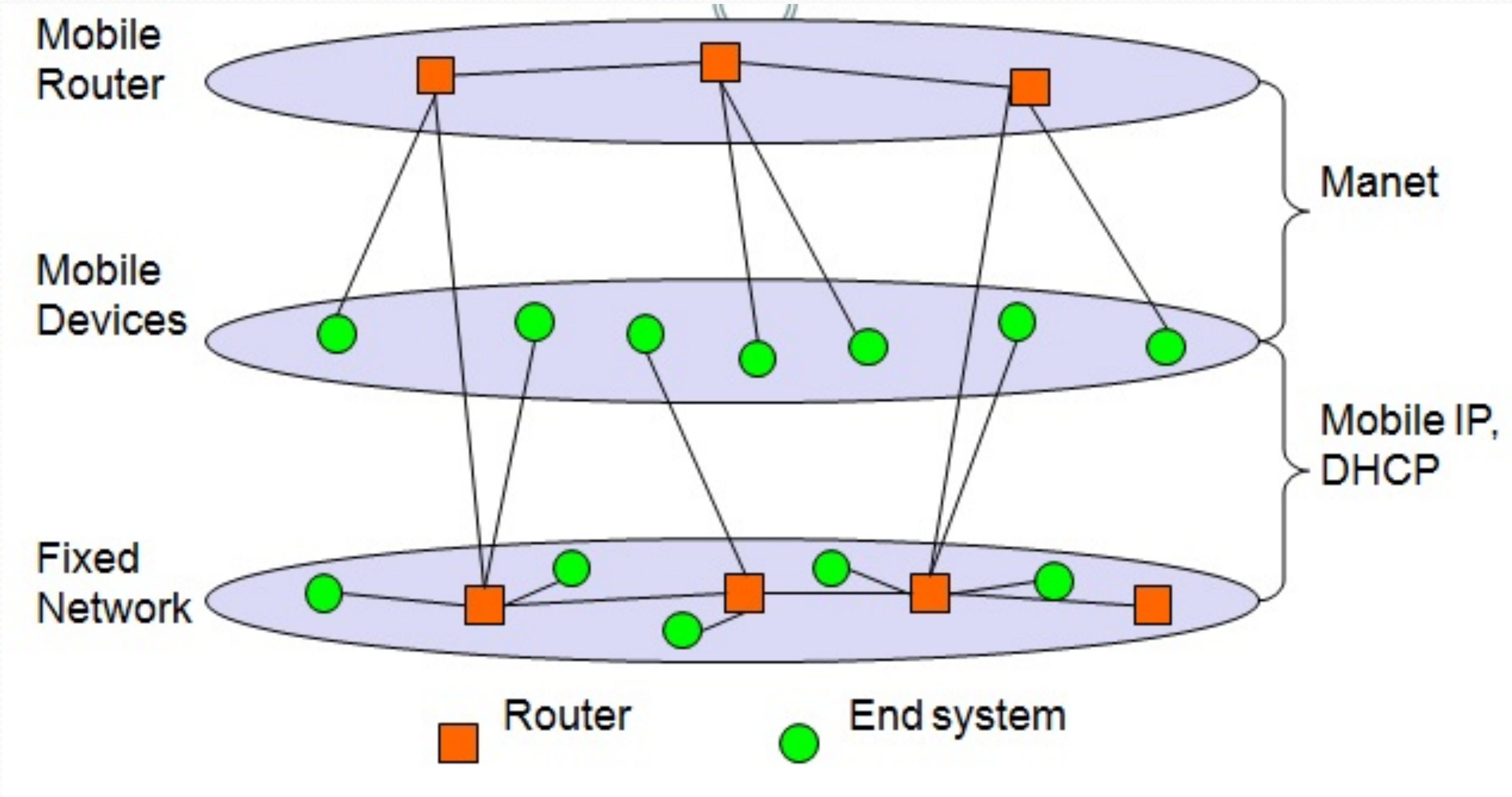
Client Initialization via DHCP



Mobile ad-hoc Networks

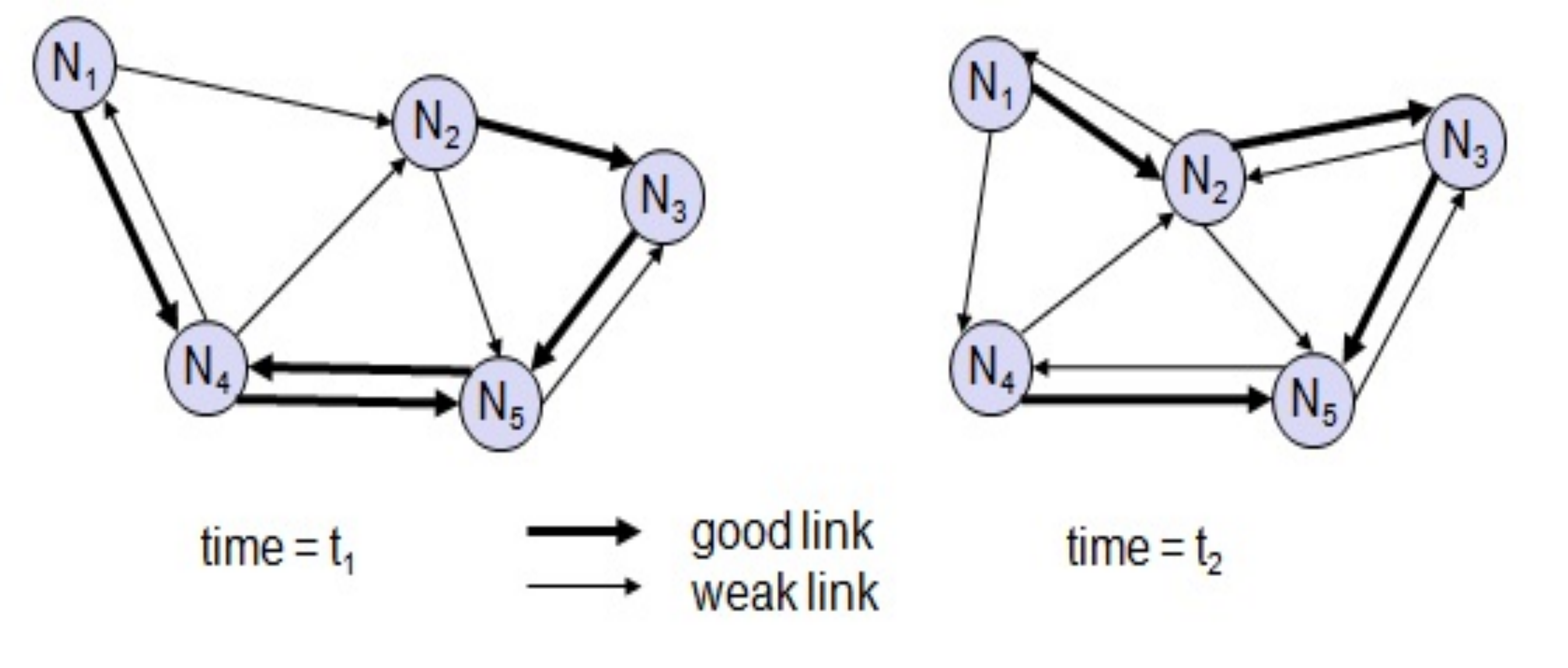
- Dynamic network which provides connectivity/access **when infrastructure is not available** or its too expensive.
  - **Mobile IP requires HA**, tunnels, default routers
  - **DHCP requires servers** and broadcast capabilities of the medium.
- Ad-hoc networks are needed under following situations
  - **Instant infrastructure:** unplanned meetings, spontaneous interpersonal communication
  - **Disaster relief:** emergency teams setting up network , military activities
  - **Remote areas:** setting up of infrastructure difficult
  - **Effectiveness:** ad-hoc set up faster and less expensive

MANETS & Mobile IP



Ad-hoc Network – Routing mechanism

- In wireless networks with infrastructure support , BS always reaches all mobile nodes, but **in ad-hoc network may drop go out of range**



Difference between wired & ad-hoc Networks

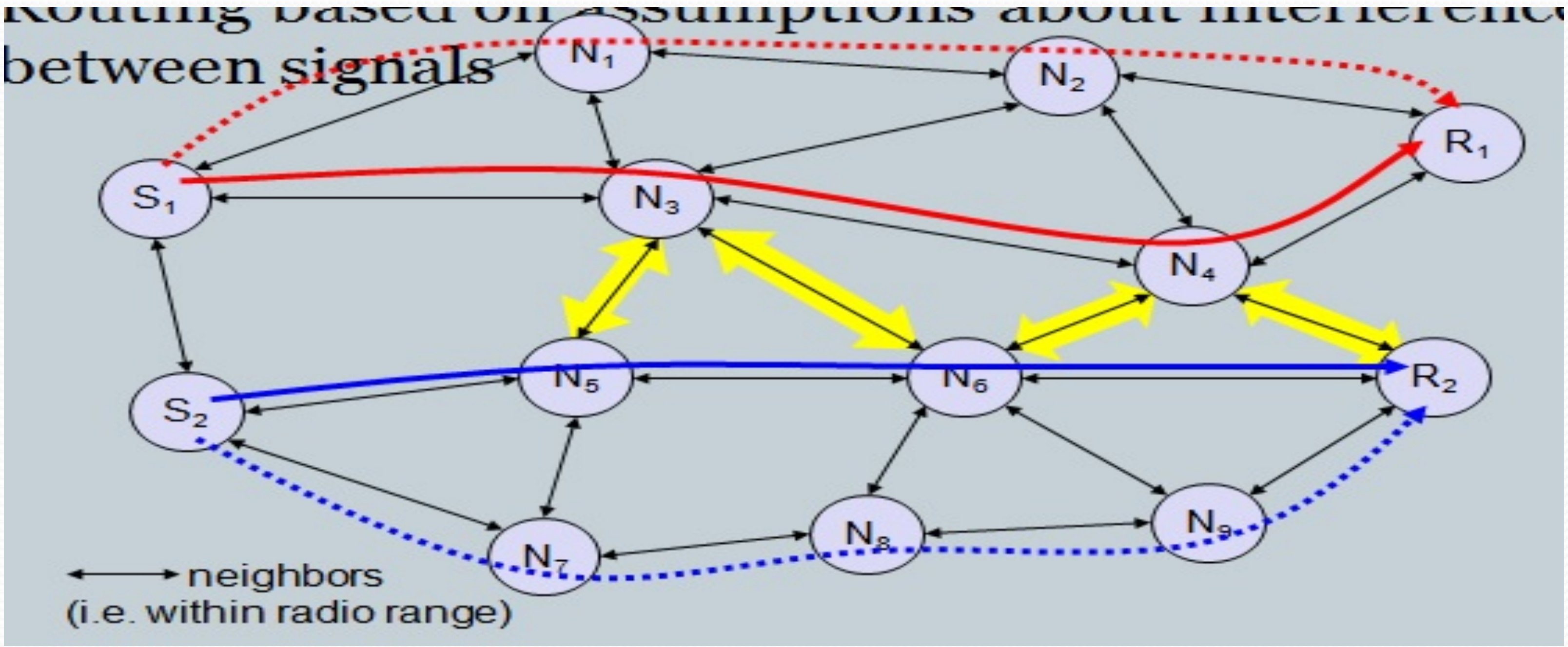
- **Asymmetric links**: bidirectional links
  - Wired Network
    - mostly consists of **symmetric links**
  - Ad-hoc Network
    - **asymmetric links**
- **Redundant links:** to survive link failures
  - Wired network
    - Consists of few **RL**, handled by infrastructure
  - Ad-hoc Network
    - **No infrastructure** to control redundancy, overhead
- **Interference:**
  - Wired network
    - Links exist only where wire exists, connections are planned/handled by network admin, less interference
  - Ad-hoc network
    - **Unplanned links** creates interference
- **Dynamic topology:**
  - Wired network
    - Can be **managed** since network can handle
  - Ad-hoc network
    - Becomes **complex** to handle

Ad-hoc Networks – Routing Concerns

- **Traditional Routing Algorithms:** ad-hoc networks have highly dynamic topology , asymmetric links, interference
- **Information from lower layers:** helps ad-hoc networks routing algorithms to find a good path.
- **Limited battery power:** ad-hoc network nodes has battery limitation
- **Wireless changing environment:** not possible to maintain a connection for a longer time.
- **Flooding of network:** forwarding of packet across unknown topology creates inefficiency.

Interference-based Routing

- Interference is taken into account in finding the best routing path.
  - Example network if S1 wants to send packet to R1 & if S2 wants to send packet to R2
  - Least Interference Routing (LIR):- calculate the cost of path based on successful transmissions & interference



Least Interference Routing (LIR)-Example

- For S1 to R1

C1 = cost(S1,N3,N4,R1)=16
C2=cost(S1,N3,N2,R1)=15
C3=cost(S1,N1,N2,R1)=12----path is chosen since less interference (all three paths have same number of hops)

For S2 to R2
C4= cost (S2,N5,N6,R2)=16
C5=cost(S2,N7,N8,N9,R2)=15---- path is chosen since less interference (though this path has one extra hop)

Overview of Ad-hoc Routing Protocols

- Ad-hoc routing protocols – new routing algorithms
  - **Flat ad-hoc routing**
    - All nodes in this approach play and equal role in routing
      - Two categories
        - Proactive protocols
        - Reactive protocols
  - **Hierarchical ad-hoc routing**
    - Used for larger networks – tree structure to manage the nodes/network
  - **Geographic position-assisted ad-hoc routing**
    - Routing is done based on geographical position of the node

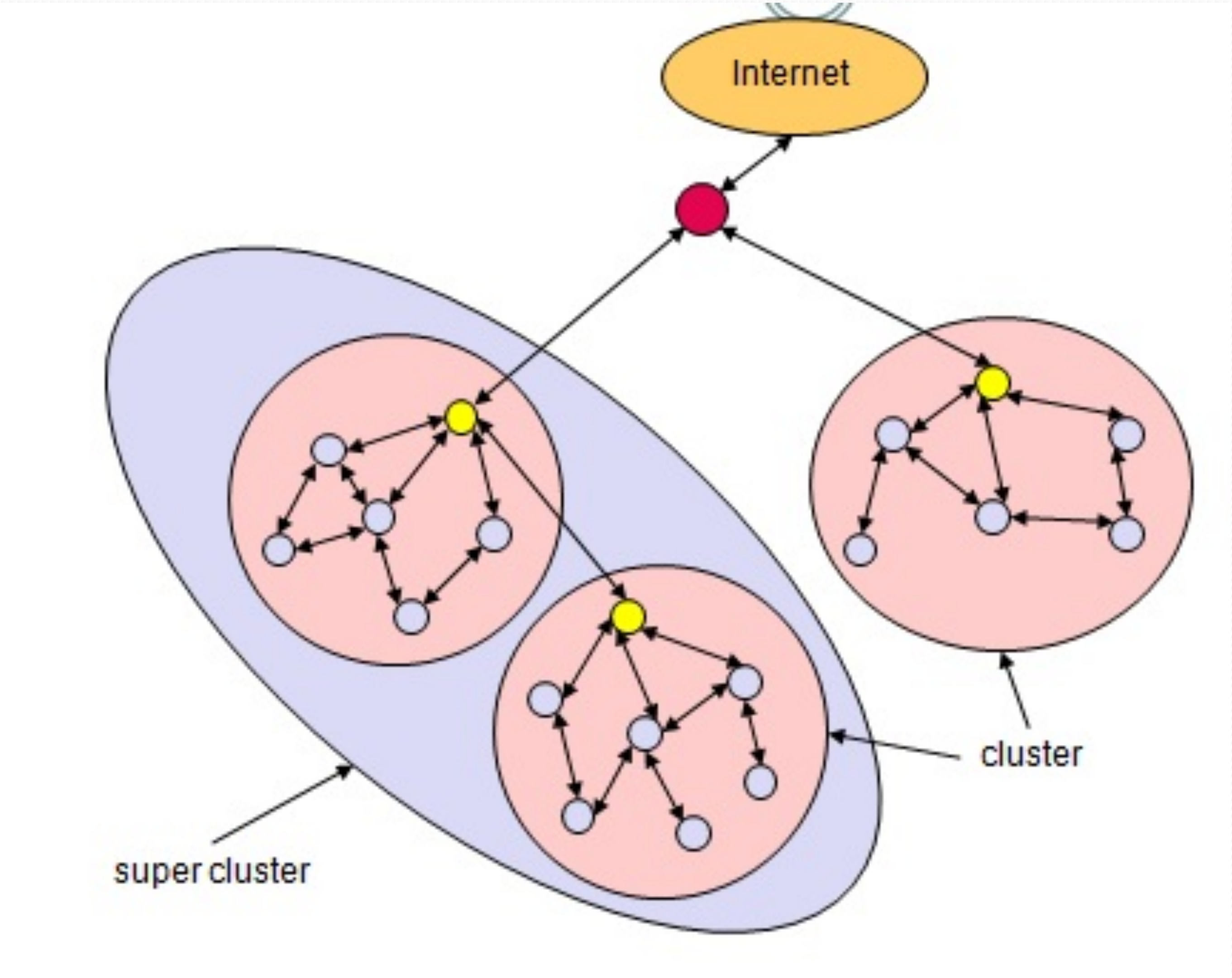
Flat Ad-hoc Routing

- **Proactive protocols:** they set up tables for routing
  - E.g **link-state algorithm:** - it floods their information about neighbors periodically
    - **Drawback:** it may take time and extra load
    - **Solution**
      - **Fuzzy sighted link-state:** routing entries corresponding to **faraway destination** are propagated **with lower frequency**
    - **Advantage:** as long as the topology does not change often, routing tables reflect the current topology with certain precision.
- **Reactive protocols:** avoids the problems of proactive by **setting up a path between sender and receiver only if a communication is waiting**.
  - **Disadvantage:** initial search latency may degrade the performance .

Hierarchical Ad-hoc Routing

- **Cluster based routing**
  - Nodes within the cluster needs to be managed
  - Cluster head acts as gateway for the cluster
    - **Advantages:** helps to reduce routing tables
    - **Disadvantages:** multiple levels of clusters within clusters
    - **Solution: Zone Routing** protocol
      - **Proactive routing** applied within the zone,
      - **Reactive routing** applied outside the zone

Hierarchical Ad-hoc Routing - Example



Geographic-position-assisted ad-hoc Routing

- **Global positioning system (GPS)**
  - Message may be sent to nodes using addresses based on **geographical routers**
- **Greedy perimeter stateless routing:**
  - Uses the location information of neighbors that are exchanged via periodic beacon messages
    - **Technique used**
      - Packets are forwarded to the neighbor that is geographically closest to the destination