CS 480: MOBILE NETWORKS

Mobile Network Layer

1st February 2017

Topics Covered

- Mobile IP
- Dynamic host configuration protocol (DHCP)
- Mobile ad-hoc networks
- Routing
- Destination sequence distance vector (DSDV)

Mobile IP

Mobile IP

- One of the protocols developed for the network layer to support mobility

Goals, Assumptions and Requirements (1)

- Mobile computing is clearly the paradigm of the future.
- The internet is the network for global data communication with hundreds of million users.
- Why not simply use a mobile computer in the internet?
- The reason is simple:
  - you will not receive a single packet as soon as you leave your home network (the network your computer is configured for) and reconnect your computer (wireless or wired) at another place (if no additional mechanisms are available).
- The reason for this is quite simple if you consider routing mechanisms on the internet.
- A host sends an IP packet with the header containing a destination address with other fields.

Goals, Assumptions and Requirements (2)

- The destination address not only determines the receiver of the packet but also the physical subnet of the receiver.
- As long as the receiver can be reached within the physical subnet, the receiver gets the packets
- As soon as the receiver moves outside the subnet, a packet will not reach it.
- A host needs a topologically correct address.

Quick “Solutions” (1)

- A quick solution to this problem would be to assign to the new computer a new, topologically correct IP address.
  - This can be achieved with the help of DHCP.
  - So moving to a new location would mean assigning a new IP address.
- The problem is that nobody knows this new address.
  - It is almost impossible to find a (mobile) host on the Internet which has just changed its address.
- One could argue that with the help of dynamic DNS an update of the mapping logical name-IP address is possible
  - This is what many computer users do if they have a dynamic IP address and still want to be permanently reachable using the same logical computer name.

Quick “Solutions” (2)

- Most of mobile IP’s motivations are important if a user wants to offer services from a mobile node (acting as a server).
  - Here the IP address is of no special interest for service usage implying that DHCP is sufficient.
- Another motivation for permanent IP addresses is emergency communication with permanent and quick reachability via the same IP address
- What about dynamically adapting the IP address with regard to current location?
  - The problem is that the domain name system (DNS) needs some time before updating the internal tables necessary to map a logical name to an IP address.

Quick “Solutions” (3)

- This approach does not work if a mobile node moves quite often.
  - The internet and DNS have not been built for frequent updates.
- There is a severe problem with higher layer protocols like TCP which rely on IP addresses.
  - Changing the IP address while still having a TCP connection (identified by source IP address, source port, destination IP address and destination port) open means breaking the connection.
- Thus a TCP connection cannot survive any address change.

Quick “Solutions” (4)

- Another approach is the creation of specific routes to the mobile node
- Routers choose the best-fitting prefix for the routing decision.
- While it is theoretically possible to change routing tables worldwide to create specific routes to a mobile node,
  - this does not scale at all with the number of nodes in the internet.
- Routers are not built for fast updates of routing tables.

Requirements (1)

- Since “quick solutions” did not work, a more general architecture had to be designed.
- Mobile IP was established as a standard to enable mobility in the internet.
- Several requirements accompanied the development of the standard:
- *Compatibility*: due to the huge installed base of internet computers (running TCP/IP)
  - Mobile IP has to be integrated into existing operating systems or work with them
  - Routers within the internet should not necessarily require other software
  - Mobile IP has to be compatible with all lower layers used for the non mobile standard IP

Requirements (2)

  - End systems enhanced with a mobile IP implementation should be able to communicate with fixed systems without mobile IP.
  - Same address format and routing methods required
- *Transparency*: mobility should remain “invisible” for many higher layer protocols and applications
  - mobile end-systems must keep their IP address
  - continuation of communication after interruption of link should be possible
  - point of connection to the fixed network can be changed
- *Scalability and efficiency*: introducing a new mechanism must not affect the efficiency and scalability
  - only little additional messages to the mobile system required (connection typically via a low bandwidth radio link)
  - Mobile IP to be scalable over a large number of participants in the internet, world-wide

Requirements (3)

- *Security*: mobility poses many security problems
  - All messages related to the management of Mobile IP should be authenticated
- The goal of a mobile IP can be summarized as:
  - “supporting end-system mobility while maintaining scalability, efficiency, and compatibility in all respects with existing applications and Internet protocols”

Entities and Terminology (1)

- Several entities and terms are needed to understand mobile IP.
- Figure 1 illustrates an example scenario.
- *Mobile Node (MN)*: system (node) that can change the point of connection to the network without changing its IP address.
  - E.g., laptops, mobile phones, a router onboard an aircraft
- *Home Agent (HA)*: system in the home network of the MN, typically a router.
  - This registers the location of the MN, tunnels IP datagrams to the COA
- *Foreign Agent (FA)*: system in the current foreign network of the MN, typically a router.
  - This forwards the tunneled datagrams to the MN, typically also the default router for the MN

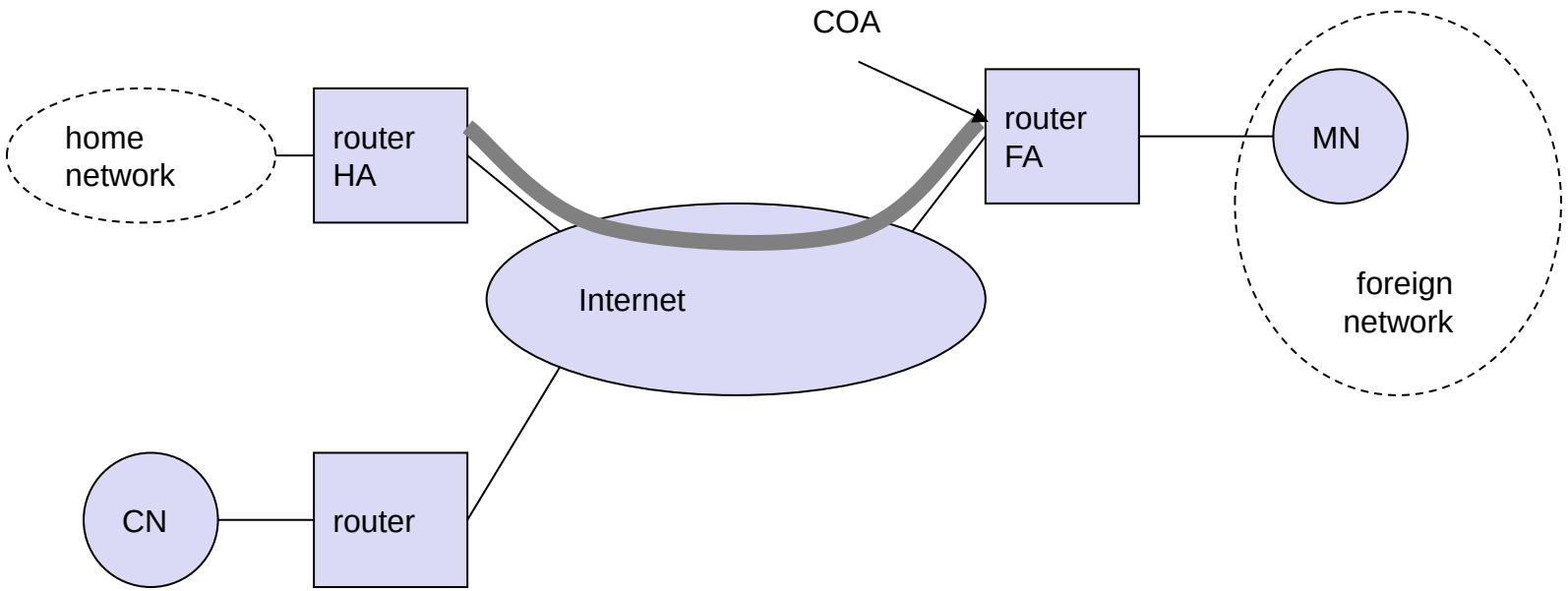

Figure 1: Entities and Terminology

Entities and Terminology (2)

- *Care-of Address (COA)*: address of the current tunnel end-point for the MN (at FA or MN).
  - This is the actual location of the MN from an IP point of view. This can be chosen, e.g., via DHCP
- *Correspondent Node (CN)*: communication partner
- The example scenario in Figure 1 shows the following situation:
  - A CN is connected via a router to the internet, as are the home network and the foreign network.
  - The HA is implemented on the router connecting the home network with the internet, an FA is implemented on the router to the foreign network.
  - The MN is currently in the foreign network. The tunnel for packets toward the MN starts at the HA and ends at the FA, since the FA has the COA in this example.

IP Packet Delivery (1)

- Figure 2 illustrates packet delivery to and from the MN using the example network of Figure 1
- A CN wants to send an IP packet to the MN.
- A CN does not need to know anything about MN's current location and sends the packet as usual to the IP address of MN (step 1).
- CN sends an IP packet with MN as a destination address and CN as a source address.
  - The internet not having information on the current location of MN, routes the packet to the router responsible for the home network of MN using standard routing mechanisms of the internet
- The HA now intercepts the packet, knowing that MN is currently not in its home network.

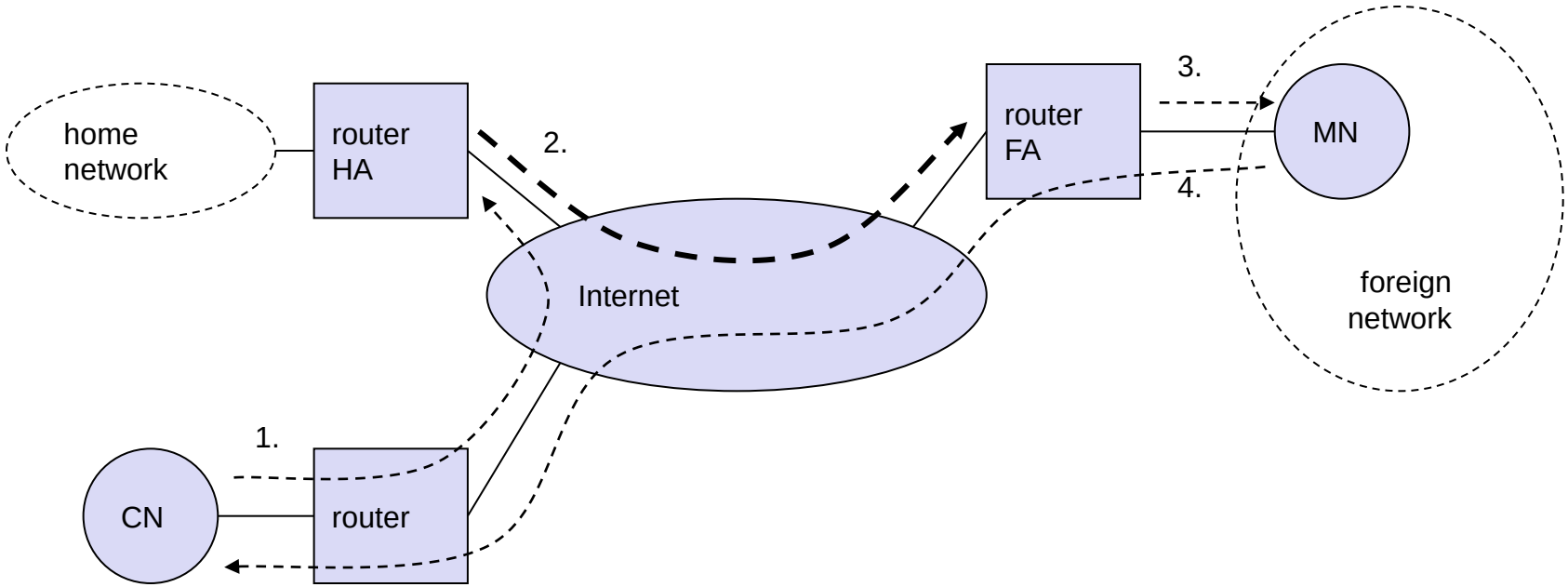

Figure 2: Packet Delivery to and from the Mobile Node

IP Packet Delivery (2)

- The packet is not forwarded into the subnet, but encapsulated and tunneled to the COA.
- A new header is put in front of the old IP header showing the COA as new destination and HA as source of the encapsulated packet (step 2).
- The foreign agent now decapsulates the packet, i.e., removes the additional header, and forwards the original packet with CN as source and MN as destination of the MN (step 3).
- Sending packets from the MN to the CN appears simpler.
  - The MN sends the packet with its own fixed IP address as source and CN's address as destination (step 4).

Agent Discovery (1)

- One initial problem of an MN after moving is how to find a foreign agent.
- How does the MN discover that it has moved?
- Mobile IP uses two methods as solutions: agent advertisement and agent solicitation
  - *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
  - *Agent solicitation*:
    - if no agent advertisements are present and an MN has not received a COA by other means, e.g., DHCP, the mobile node must send agent solicitations

Agent Discovery (2)

- A mobile node typically sends out three solicitations, one per second, as soon as it enters a new network.

- After these steps of advertisement or solicitations the MN can now receive a COA, either one for an FA or a co-located COA.

Registration (1)

- Having received a COA, the MN has to register with HA.
- The main purpose of registration is to inform the HA of the current location for correct forwarding of packets.
- Registration can be done in two different ways depending on the location of the COA
  - If the COA is at the FA, registration is done as illustrated in Figure 3 (left).
    - The MN sends its registration request containing the COA to the FA which forwards the request to the HA
    - The HA sets up a mobility binding containing the mobile node's home IP address and the current COA.
    - The mobility binding also contains the lifetime of the registration. Registration expires after the lifetime.
    - After setting up the mobility binding, the HA sends a reply message back to the FA which forwards it to the MN

Registration (2)

- If the COA is co-located, registration can be simpler and is shown in Figure 3 (right)
  - The MN may send the request directly to the HA and vice versa.
  - This also the procedure for MNs returning to their home network.

- UDP packets are used for registration requests.
  - UDP is used due to its low overheads and better performance compared to TCP in wireless environments

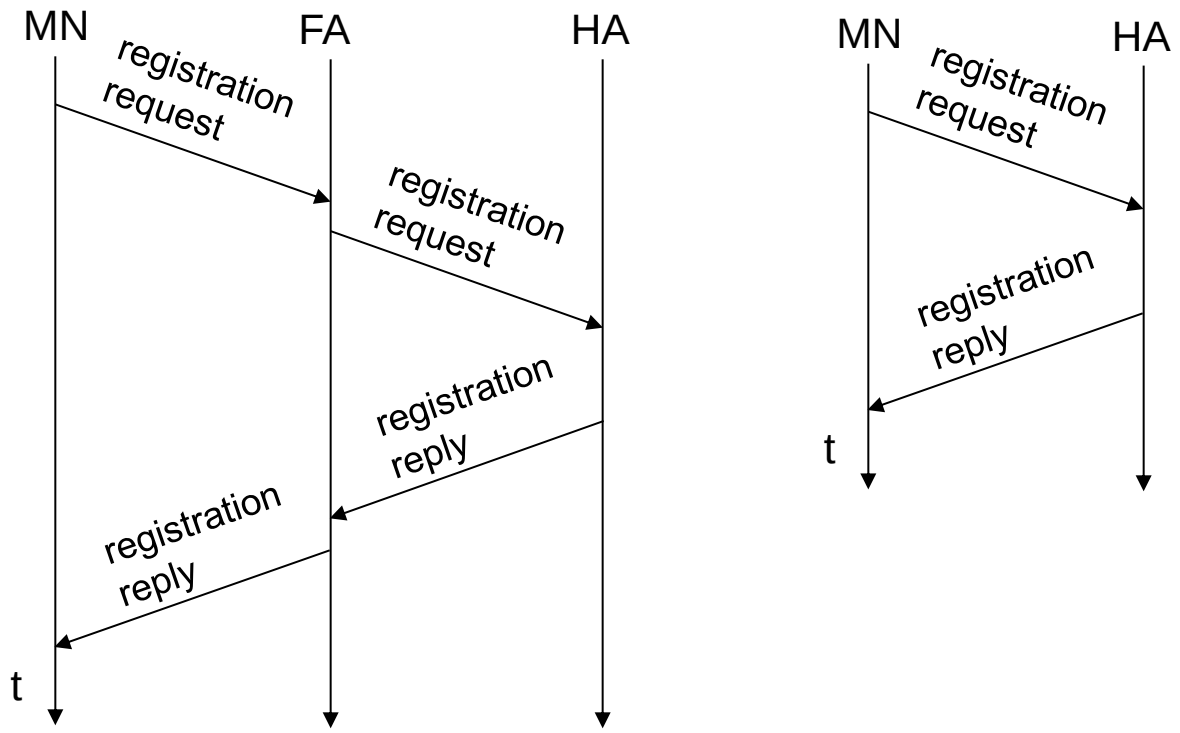

Figure 3: Registration of a Mobile Node via the FA or Directly with the HA

Tunneling and encapsulation

- Here, the mechanisms used for forwarding packets between the HA and the COA, as shown in Figure 2, step 2 are discussed
- A *tunnel* establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint
  - Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged.
- Tunneling is achieved by using encapsulation
- *Encapsulation* 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* is taking a packet out of the data part of another packet
- This mechanism is shown in Figure 4.

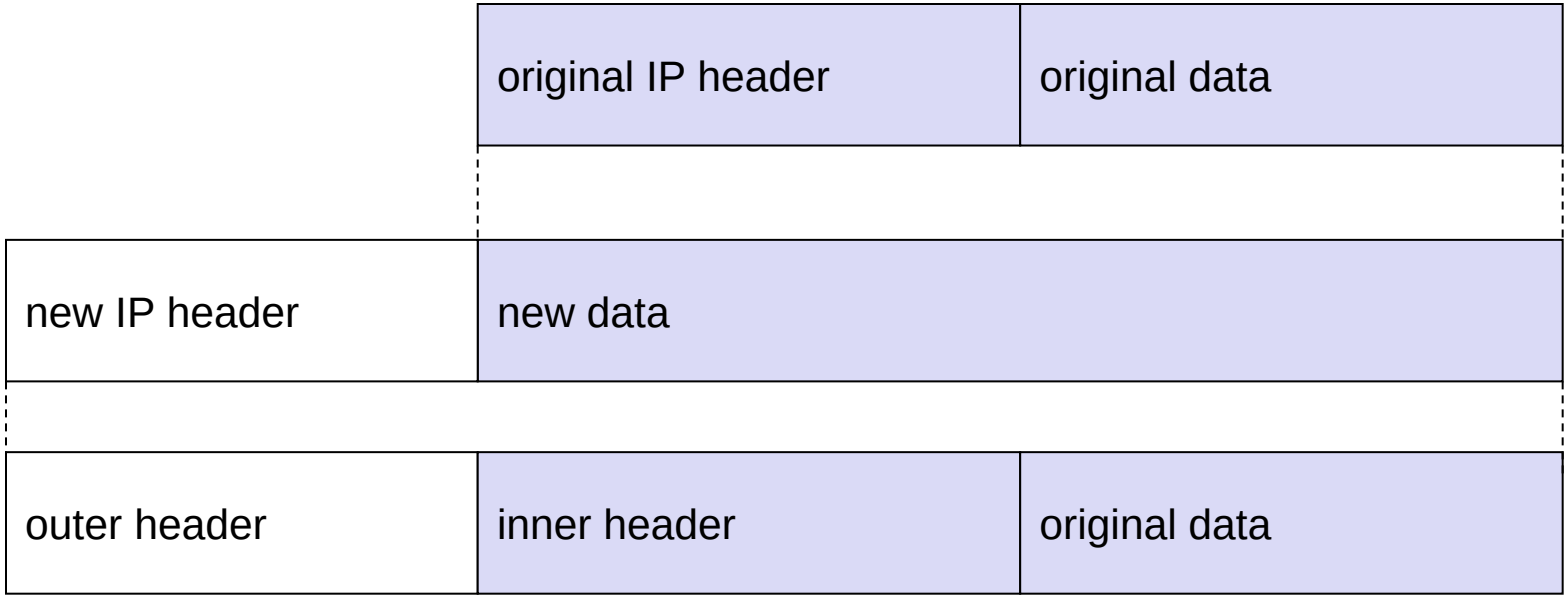

Figure 4: IP Encapsulation

Reverse Tunneling (1)

- At first glance, the return path from the MN to the CN shown in Figure 2 looks quite simple.
- The MN can directly send its packets to the CN as in any other standard IP situation.
- The destination address in the packets is that of CN.
- There are several severe problems associated with this simple solution
  - *Firewalls*: often firewalls only allow packets with topologically correct addresses to pass
    - However MN still sends packets with its fixed IP address as source which is not topologically correct in a foreign network

Reverse Tunneling (2)

- *Multi*-cast: reverse tunnels are needed for the MN to participate in a multi-cast group.
  - While nodes in a home network might participate in a multi-cast group, an MN in a foreign network cannot transmit multi-cast packets in a way that they emanate from its home network without a reverse tunnel.
- *TTL (time to live)*: consider an MN sending packets with a certain TTL while still in its home network.
  - The TTL might be low enough so that no packet is transmitted outside a certain region.
  - If the MN moves to foreign network, this TTL might be too low for the packets to reach the same nodes as before
  - Mobile IP is no longer transparent if a user has to adjust the TTL while moving

Reverse Tunneling (3)

- A reverse tunnel is needed that represents only one hop, no matter how many hops are really needed from a foreign network to the home network
- All these considerations led to the RFC 2344 defining reverse tunneling as an extension to mobile IP.
- The RFC was designed to be backward-compatible to mobile IP and defines topologically correct reverse tunneling as necessary to handle the above problems

IPv6 (1)

- While mobile IP was originally designed for IP version 4, IP version 6 makes life much easier.
- Security is integrated and not an add-on, authentication of registration is included
- COA can be assigned via auto-configuration (DHCPv6 is one candidate), every node has address auto-configuration
- No need for a separate FA, all routers perform router advertisement which can be used instead of the special agent advertisement; addresses are always co-located
- MN can signal a sender directly the COA, sending via HA not needed in this case (automatic path optimization)

IPv6 (2)

- “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

Dynamic Host Configuration Protocol (DHCP)

Dynamic host configuration protocol (DHCP) (1)

- DHCP is mainly used to simplify the installation and maintenance of networked computers.
- If a new computer is connected to a network,
  - DHCP can provide it with all the necessary information for full system integration into the network such as IP address, DNS server address, domain name, subnet mask, default router etc.
- Providing an IP address makes DHCP very attractive for mobile IP as a source of COA
- DHCP is based on a client/server model as shown in Figure 5
- DHCP clients send a request (DHCPDISCOVER) to a server to which the server responds
- A client sends requests using MAC broadcasts to reach all devices in the LAN.

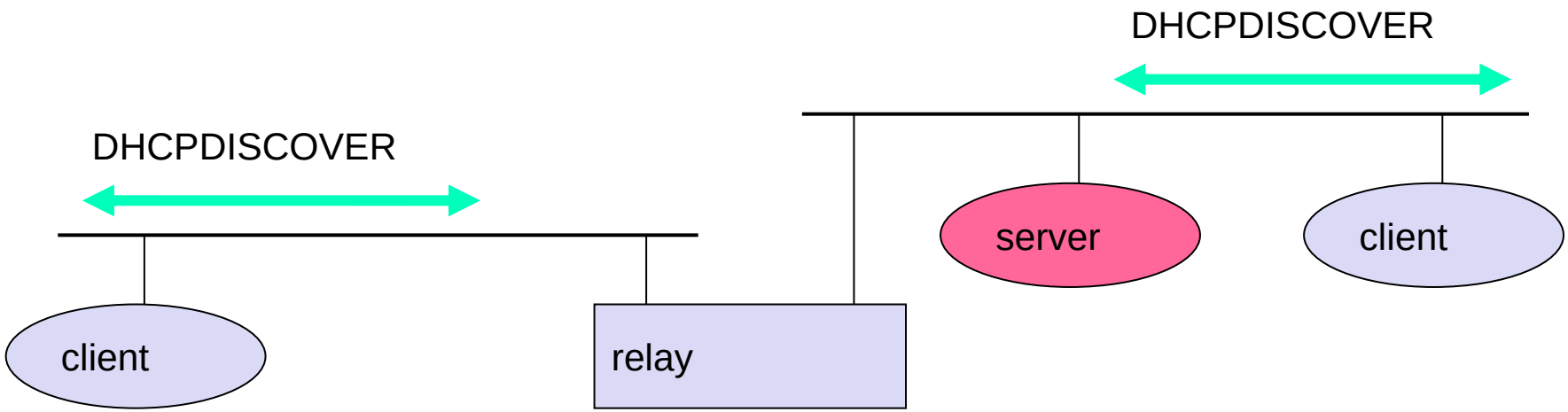

Figure 5: Basic DHCP configuration

Dynamic host configuration protocol (DHCP) (2)

- A DHCP relay might be needed to forward requests across inter-working units to a DHCP server
- A typical initialization of a DHCP client is shown in Figure 6 (one client and two servers).
- The client broadcasts DHCPDISCOVER into the subnet.
- Two servers receive this broadcast and determine the configuration to offer to the client.
  - One example of this could be checking for available IP addresses and choosing one for the client.
- Servers reply to the client's request with DHCPOFFER and offer a list of configuration parameters.
  - The client can choose one of the configurations offered

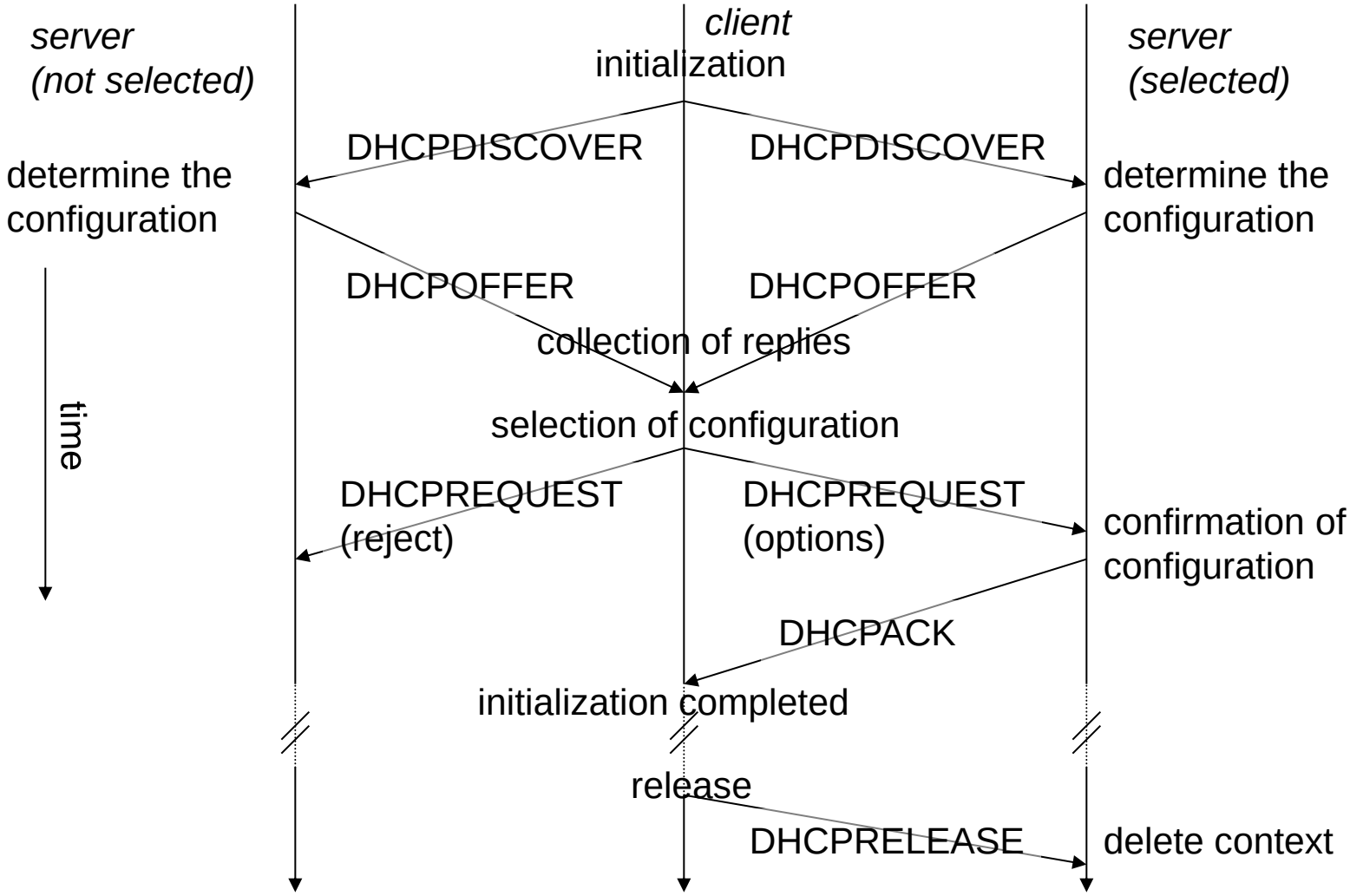

Figure 6: Client initialization via DHCP

Dynamic host configuration protocol (DHCP) (3)

- The client replies to the servers, accepting one of the configurations and rejecting others using DHCPREQUEST.
- If a server receives a DHCPREQUEST with a rejection, it can free the reserved configuration for other possible clients
- The server with the configuration accepted by the client confirms the configuration with DHCPACK.
  - This completes the initialization phase.
- If a client leaves a subnet, it should release the configuration received to a server using DHCPRELEASE

Mobile ad-hoc networks

Mobile ad-hoc networks (1)

- Mobility support described under mobile IP and DHCP relies on the existence of some infrastructure
  - Mobile IP requires, e.g., home agent, tunnels and default routers
  - DHCP requires servers and broadcast capabilities of the medium reaching all participants to servers
- There may be several situations where users of a network cannot rely on an infrastructure, may be too expensive, or there is none at all.
- In these situations mobile ad-hoc networks are the only choice
- These networks should be mobile and use wireless communications.

Mobile ad-hoc networks (2)

- Examples for the use of such mobile, wireless, multi-hop ad-hoc networks, are:
  - *Instant infrastructure*: unplanned meetings, spontaneous interpersonal communications etc cannot rely on any infrastructure.
    - Infrastructures need planning and administration. It takes too long to set up infrastructure; thus ad-hoc connectivity has to be set up
  - *Disaster relief*: infrastructures do break down in disaster areas.
    - Hurricanes cut phone and power lines, floods destroy base stations, fires burn servers.
    - Emergency teams rely on infrastructure they can set up themselves
    - No forward planning can be done and the setup must be extremely fast and reliable.
  - *Remote areas*: even if infrastructures could be planned ahead, it is sometimes too expensive to set up an infrastructure in sparsely populated areas.
    - Depending on the communication pattern, ad-hoc networks or satellite infrastructures can be a solution.

Mobile ad-hoc networks (3)

  - *Effectiveness*: services provided by existing infrastructures might be too expensive for certain applications.
    - If, for example, only connection oriented cellular networks exist, but an application sends only a small status information every other minute, a cheaper ad-hoc packet-oriented network might be a better solution

- Ad-hoc networking has led to creation of a working group at the IETF that is focusing on mobile ad-hoc networking called MANET.
- Figure 7 shows the relation of MANET to mobile IP and DHCP.
- While mobile IP and DHCP handle the connection of mobile devices to a fixed infrastructure, MANET comprises mobile routers, too.

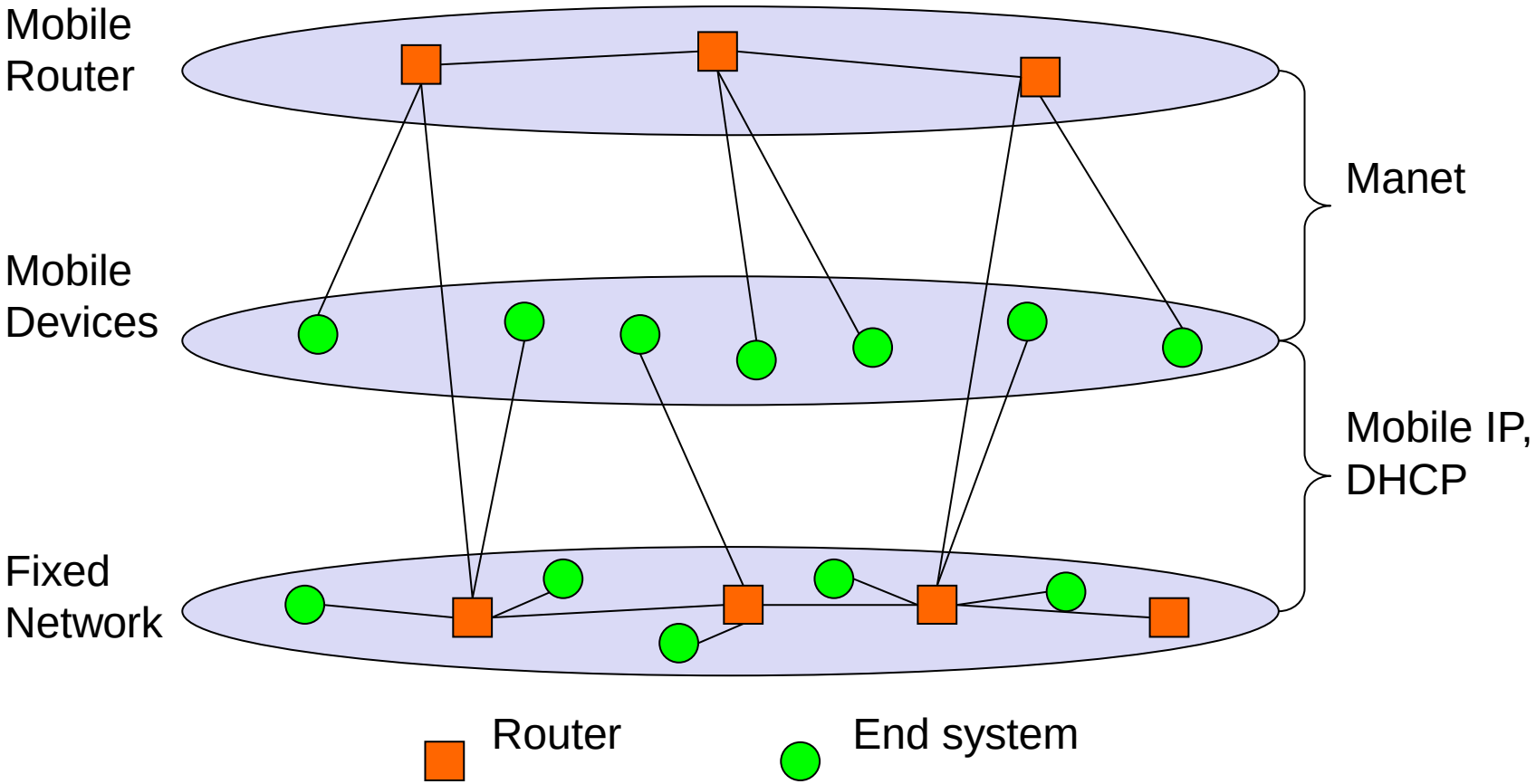

Figure 7: MANETs and mobile IP

Mobile ad-hoc networks (4)

- Mobile devices can be connected either directly with an infrastructure using mobile IP for mobility support and DHCP as a source of many parameters, such as an IP address.
- MANET research is responsible for developing protocols and components to enable ad-hoc networking between mobile devices.

Routing

Routing (1)

- While in wireless networks with infrastructure support, a base station always reaches all mobile nodes, this is not always the case in an ad-hoc network.
- A destination node might be out of range of a source node transmitting packets.
- Routing is needed to find a path between source and destination and to forward the packets appropriately.
- In wireless networks using an infrastructure, cells have been defined.
- Within each cell, the base station can reach all mobile nodes without routing via a broadcast
- In ad-hoc networks, each node must be able to forward data to other nodes.

Routing (2)

- This creates many additional problems
- Figure 8 gives a simple example of an ad-hoc network.
- At a certain time t_1, the network topology might look as illustrated on the left side of the figure.
- Five nodes, N_1 to N_5, are connected depending on the current transmission characteristics between them.
- N_4 can receive N_1 over a good link, but N_1 receives N_4 via a weak link.
- Links do not necessarily have the same characteristics in both directions.
  - The reasons for this are, e.g., different antenna characteristics or transmit power.
- N_1 cannot receive N_2, but N_2 receives a signal from N_1.

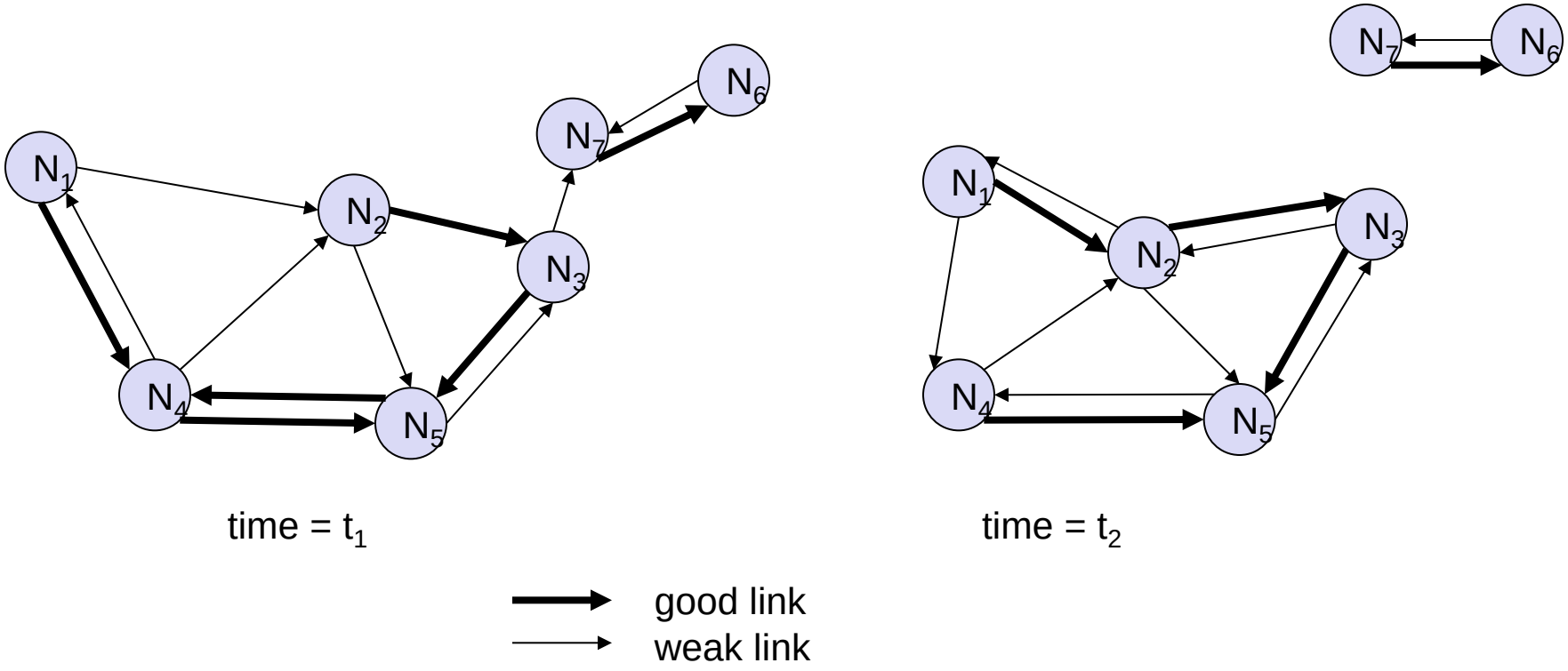

Figure 8: Example ad-hoc network

Routing (3)

- The situation can change quite fast as the snapshot at t_2 shows.
- N_1 cannot receive N_4 any longer, N_4 receives N_1 only via a weak link.
- But now N_1 has an asymmetric but bi-directional link to N_2 that did not exist before.
- This very simple example shows some fundamental differences between wired networks and ad-hoc wireless networks related to routing.
  - *Asymmetric links*: Node A receives a signal from node B. Node B might receive nothing, have a weak link, or even a better link than the reverse direction.
    - Routing information collected for one direction is of almost no use for the other direction. Many routing algorithms for wired networks rely on symmetric scenario.

Routing (4)

- *Redundant links*: In ad-hoc networks nobody controls redundancy, so there might be many redundant links up to the extreme of a completely meshed topology.
  - Routing algorithms for wired networks can handle some redundancy, but high redundancy can cause a large computational overhead for routing table updates.
- *Interference*: In wired networks links exist only where a wire exists, and connections are planned by network administrators.
  - In ad-hoc networks links come and go depending on transmission characteristics, one transmission might interfere with another, and nodes might overhear the transmission of other nodes.
  - Interference creates new problems by unplanned links between nodes.
- *Dynamic topology*: The greatest problem for routing arises from the highly dynamic topology.
  - The mobile nodes might move as shown in Figure 8 or medium characteristics might change.
  - This results in frequent changes in topology. In ad-hoc networks, routing tables must somehow reflect these frequent changes in topology and routing algorithms have to be adapted.

Destination sequence distance vector (DSDV)

DSDV (1)

- DSDV routing is an enhancement to the distance vector routing for ad-hoc networks
- Distance vector routing is used as routing information protocol (RIP) in wired networks.
- It performs extremely poorly with certain network changes due to count to infinity problem
- Each node exchanges its neighbor table periodically with its neighbors.
- Changes at one node in the network propagate slowly through the network.
- The strategies to avoid this problem which are used in fixed networks do not help in wireless ad-hoc networks due to rapidly changing topology.

DSDV (2)

- DSDV adds two things to the distance vector algorithm:
  - *Sequence numbers*: each routing advertisement comes with a sequence number.
    - Within ad-hoc networks, advertisements may propagate along many paths.
    - Sequence numbers help to apply advertisements in correct order
    - This avoids loops that are likely with unchanged distance vector algorithm.
  - *Damping*: transient changes in topology that are of short duration should not destabilize the routing mechanisms.
    - Advertisements containing changes in the topology currently stored are thus not disseminated further.
    - A node waits with dissemination if these changes are probably unstable.
    - Waiting time depends on the time between the first and the best announcement of a path to a certain destination.