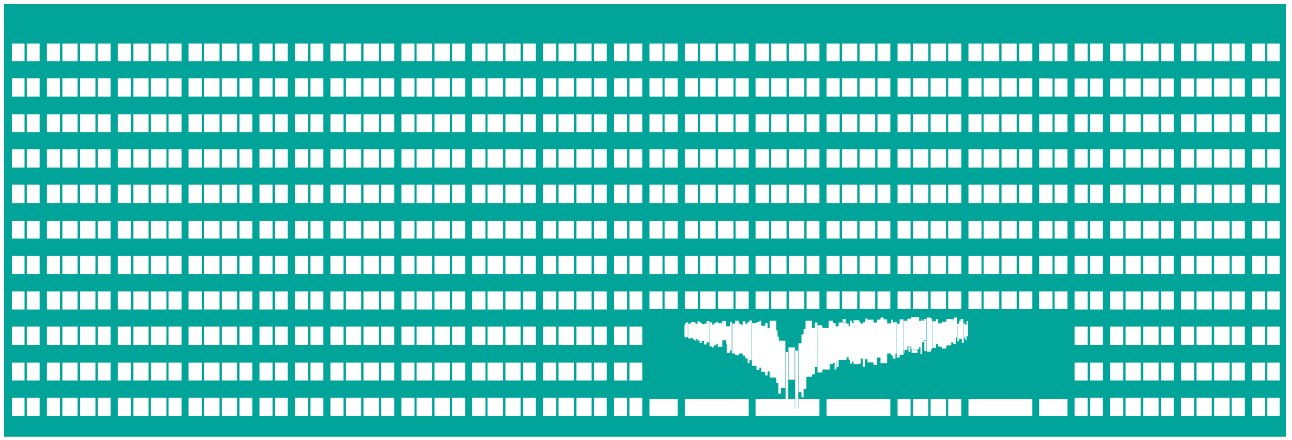
VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF COMPUTER SCIENCE

Mobility in IP networks



MS (Mobile Computing)
Lecture 8

Main ideas of IP mobility

- Keep the same IP address independently on the network the equipment is connected to:
  - Should be reachable from Internet/home network?
  - How to configure such address?
  - Is it possible to reach real mobility?
- Was not considered in IPv4 development, workarounds:
  - Tunneling
  - Mobility in IPv4 – RFC 3344 (2002) – hard to optimize, extended in RFC 4721 (2007) – challenge/response extensions
- IPv6 was built with IP mobility as one of its functions → MIPv6

Mobility in GPRS networks

- GPRS core network - integrated part of the GSM network switching subsystem, provided services:
  - mobility management
  - session management
  - transport of datagrams (IPv4, IPv6, PPP)
- GPRS tunneling protocol (GTP)
  - Connection of users to internetwork through Gateway GPRS Support Node (GGSN) from “single” location.
  - Carries subscriber's data from subscriber's current Serving GPRS Support Node (SGSN) to the GGSN
  - GTP-U – user data, GTP-C – control (setup & deletion, updates – e.g. move, verification of GSN reachability), GPT' – accounting, transfer of charging data from GSNs

Tunneling protocols

One network protocol (the delivery protocol) encapsulates a different payload protocol. Virtual circuit on shared infrast.

- Different approaches
  - static × dynamic
  - point-to-point × point-to-multipoint
  - single station × network segment(s)
- On different layers of ISO-OSI RM
  - L7 – Application-specific protocols – e.g. SSH tunnels
  - L4 – Lower-layer prot. over UDP (or TCP), e.g. L2TP
  - L3 – General route encapsulation – GRE – **XXX** over IP
  - L2 – 802.1q tunneling QinQ, …

Virtual private network (VPN)

- VPNs allow building of private WANs using public shared infrastructure with the same level of security and configuration options as with private infrastructure
  - Tunneling and encr. methods, authentication (AAA)
- VPN examples:
  - IPsec (Internet Protocol Security) – originally developed for IPv6 (core part), backported to IPv4 (frequent use)
  - Transport Layer Security, can be used even when L3 VPNs encounter NAT problems, e.g. OpenVPN. Problem – datagrams over stream connection → Datagram TLS (DTLS), e.g. Cisco AnyConnect VPN
  - Secure Shell (SSH) VPN in OpenSSH (limited), WWW
  - ...

VPN implementation

- Common approaches:
  - Router-to-router (firewall)
    - Site-to-site VPNs
    - Single router may terminate multiple tunnels
  - Remote User to VPN concentrator
    - Remote access VPNs
    - User has to have special encryption software installed (VPN client)
- Mobile VPN (mVPN)
  - Mobile devices can access network resources on their home network. Classic mobility issues (weak m., …)
  - Functions: persistence, roaming, application compatibility, security, acceleration, strong authentication

IPsec

- General architecture for implementation of dynamically negotiated VPN tunnels
- Provides authentication, data integrity and encryption
- General framework independent on utilized cryptographic algorithms
  - Algorithms are negotiated during tunnel establishment
  - Security Association with limited lifetime
- Only for IP (unicast) traffic
  - Other protocols and multicast traffic may be encapsulated into IP prior sending to the tunnel
- Current standards (2005): RFC 4301 & RFC 4309

Mobile IP

- New IP address associated with the new point of attachment (PoA) is required → two different IPs for one mobile node
  - Home address: static
  - Care-of address (CoA): topologically significant address, i.e. locally assigned address in foreign network
- *Home network* → *home agent* (*HA*)
- *Foreign network* → **MIPv4:** *foreign agent* (*FA*)

Mobile IPv4

- Foreign agent lends IP address (care-of address) to the mobile node to build an IP tunnel.
- Mobile IP mechanisms
    1. *Discovering* the care-of address (ICMP)
    2. *Registering* the care-of address (UDP)
    3. *Tunneling* to the care-of address (IP)

MIPv4 – Address discovery

- Extension of ICMP Router Advertisement
- Home agents and foreign agents periodically broadcast agent advertisement messages, which:
  - Enable detection of mobility agents
  - Informs the mobile node about special features
  - Lists one or more available care-of addresses → mobile node selects its care-of address
  - Information for mobile node, whether the agent is a home agent or foreign agent
- Mobile node issues ICMP router solicitation message

MIPv4 – Registration

Once a mobile node has obtained a care-of address, it must inform its home agent about it

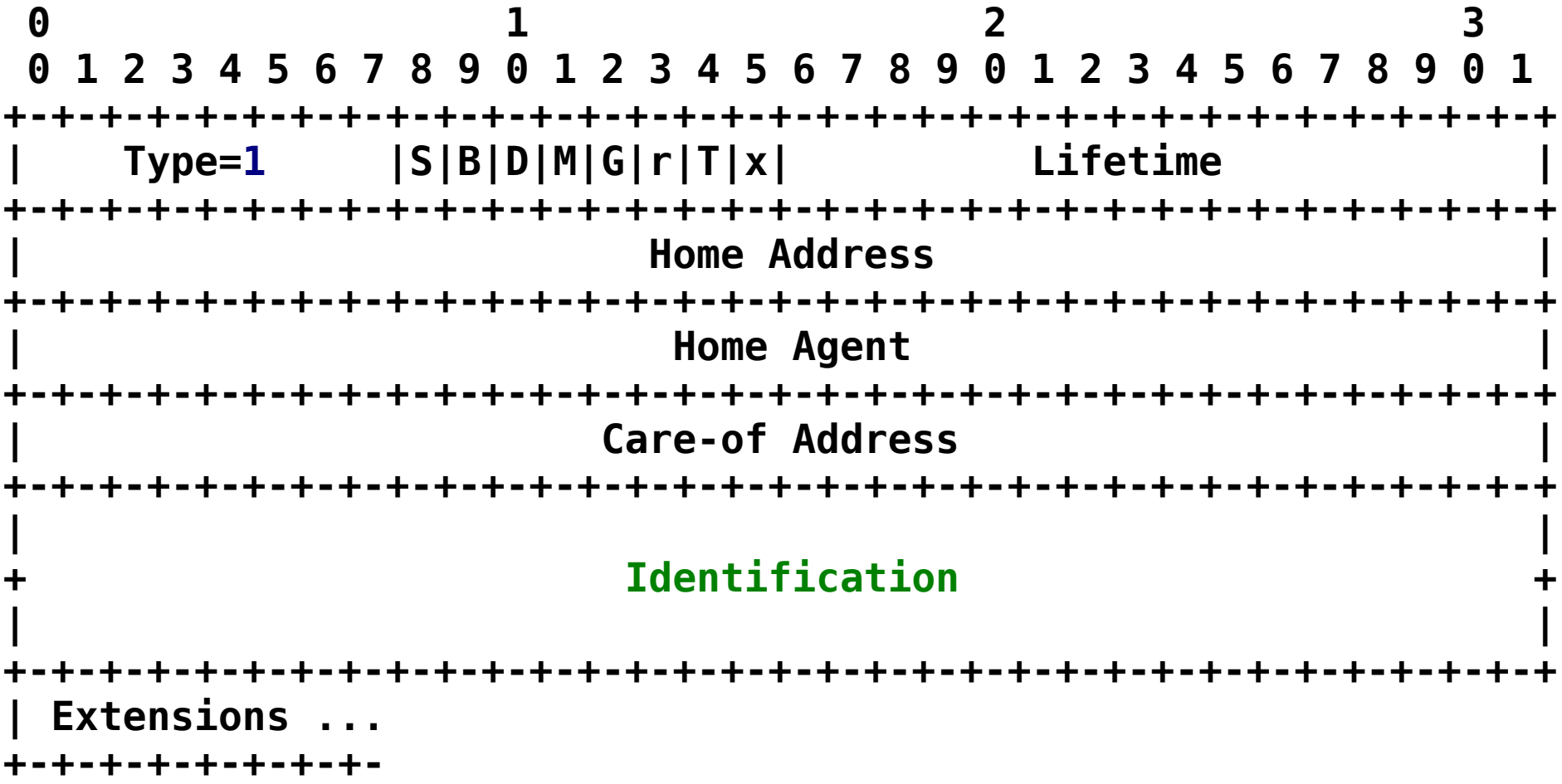
0. Foreign agent sends agent advertisements
1. Mobile node sends request to foreign agent
2. FA forwards request to node's home agent
3. HA accepts or denies the request
4. FA relays the status based on HA reaction to the mobile node

MIPv4 tunneling

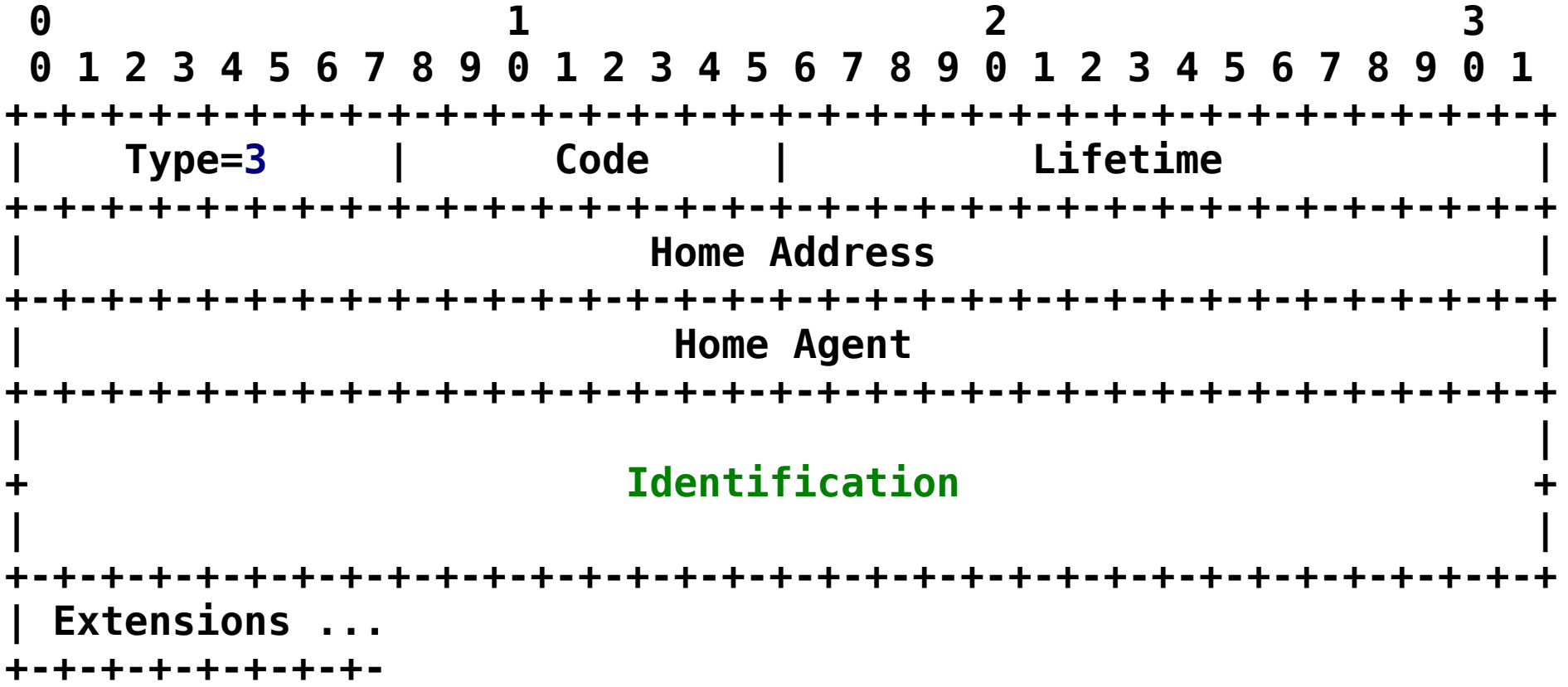
1. Datagram to mobile node arrives to home network via classic IP routing
2. Home agent intercepts datagram and tunnels it to the care-of address via foreign agent
3. Foreign agent detunnels the datagram and forwards it to the mobile node.
4. All datagrams from mobile node are delivered to destinations through classic IP routing (FA can act as mobile node's default router).

MN directly connected to HA does not use tunneling.

MIPv4 Registration request



MIPv4 Registration reply



- Extensions in request and reply:
  - Authentication: Mobile-Home, Mobile-Foreign, Foreign-Home

IPv6 Mobility (MIPv6)

- Based on core features of IPv6 (design from scratch)
  - Base IPv6 has been designed to support Mobility → Mobility is not an “Add-on” feature
    - All IPv6 routers, nodes, LANs & Subnets are IPv6-Mobile Ready
  - IPv6 Neighbor Discovery and Address Autoconfig. allow hosts to operate in any location without special support
- Goals
  - Offer direct communication with mobile node
  - Reduce the number of actors (no Foreign Agent unlike mobile IPv4 requires)
- Current specification (2004) : RFC 3775 + 3776 (IPSec)

MIPv6 basics

- No foreign agent is being used in MIPv6!
  - MN can get a new IPv6 address, which can be only used by the MN → the FA no longer exists
  - IPv6 Address auto-configuration possible: MN can obtain a CoA in foreign network without help of FA
- A globally unique IPv6 address is assigned to every Mobile Node (MN): Home Address (HoA)
  - HoA enables the MN identification by its Correspondent Nodes (CN)
  - MN must be able to communicate with non-mobile nodes
  - Communications (keep L4 connections) have to be maintained while the MN is moving and connecting to foreign networks.

MIPv6 basic features

- Corresponding node can:
  - Put/get a binding update (BU) in/from their binding cache
  - Learn the position of a mobile node by from BU options
  - Perform direct packet routing toward the MN (Routing Header)
- The MN's Home Agent must:
  - Be a router in the MN's home network
  - Do reverse tunneling (MN → CN)
  - Intercept packets which arrive at the MN's home network and whose destination address is its home address + tunnel (IPv6 encapsulation) intercepted packets directly to the MN

MIPv6 features

- More Scalable → Better Performance
  - Reduced traffic through Home Link
  - Less redirections/re-routing (due to traffic optimization)
- Bi-directional tunneling mode
  - Support of MIPv6 on correspondent nodes not required
  - Use of Reverse tunneling (RFC 2344) – to home agent
- New IPv6 Destination Option
  - Home Address destination option
- New ICMPv6 Messages:
  - Home Agent Address Discovery Request & Reply
  - Mobile Prefix Solicitation & Advertisement

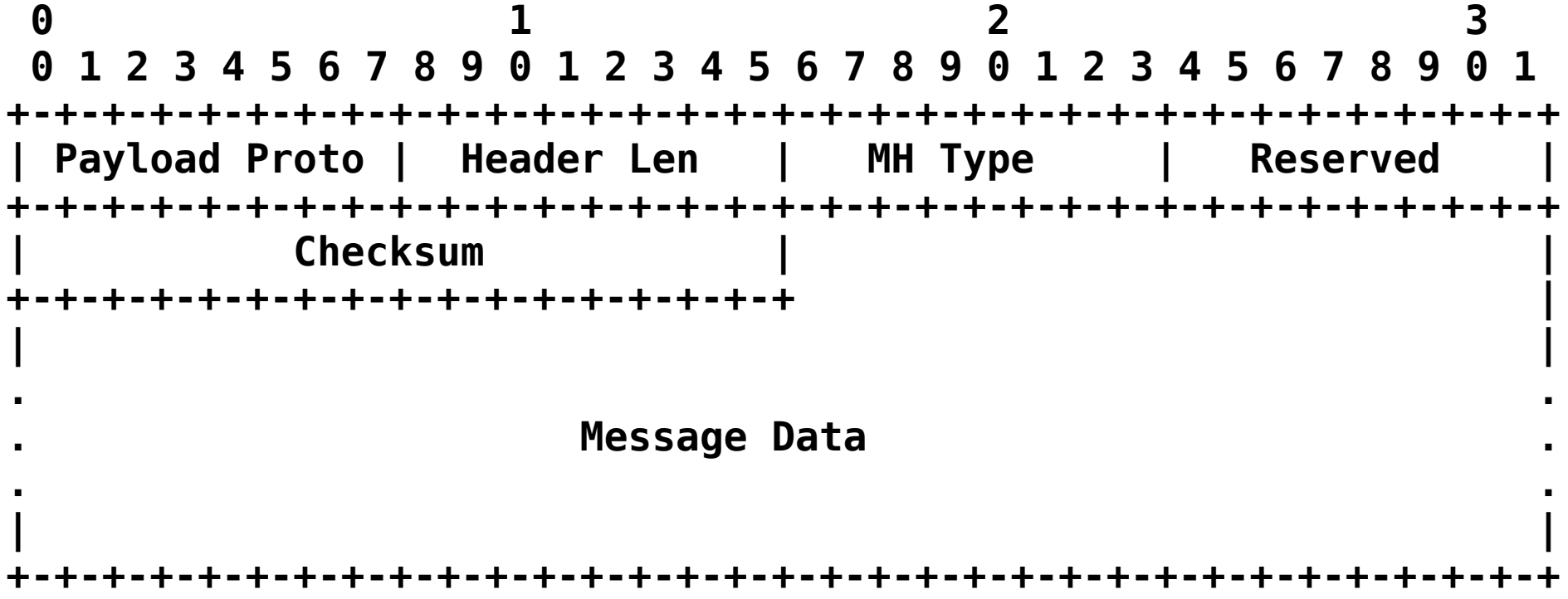
Route optimization (RO) mode

- Requires to register the MN's current binding at the CN
- Uses a new type of IPv6 routing header
  - Type-2 routing header = home address (Dest Addr = MN's CoA)
- Shortest communications path
- Eliminates congestion at the MN's HA and home link
- Reduced impact of any possible failure of the HA or networks on the path to or from HA.

Dynamic HA address discovery

- Allows MN to dynamically discover the IP address of the home agent on its home link
- ICMPv6 home agent address discovery request
  - Destination address: Home Agent anycast address for its own home subnet prefix
- Reply
  - HA list (with preferences) in the home link
  - Each HA maintains the home agent lists and can send the reply

Mobility header



- Identified by Next Header value 135 in previous hdr.
- MH Type – type of mobility message
- Message data – mobility message contents

Mobility messages

- Home Test Init & Home Test
  Care-of Test Init & Care-of Test
  - Return routability procedure from MN to CN to ensure authorization of subsequent binding updates
- Binding Update (**BU**) & Binding Acknowledgement (**BA**)
- Binding Refresh Request
- Binding Error (**BE**)

Some messages contain additional option fields (Alternate CoA, Binding refresh advice, Nonce indices, Binding authorization data)

Movement detection

A) Detect L3 handovers

B) Neighbor Unreachability Detection (NUD)

- Default router is no longer bi-directionally reachable

Follow-up steps:

1. Router Discovery: select a new default router
2. Prefix Discovery: form new care-of address
3. Home registration
4. Correspondent registration

Communication with MN

Two communication methods:

- Bi-directional Tunneling
  - No mobility requirements on CNs
  - No visibility of MNs for CNs
  - Network load increased
  - HA role much reinforced

- Direct Routing
  - Much more complex mechanism
  - HA role much alleviated
  - Route optimization mode (RO)

Correspondent node registration

- Allowing the CN to cache the MN's current CoA
- Return routability procedure + registration
- After home registration, the MN should initiate a correspondent registration for each node that already appears in the MN's Binding Update list
- The initiated procedures can be used to either update or delete binding information in the CN
- In addition, MN initiate the registration in response to receiving a packet tunneled using IPv6 encapsulation

Required mobility features (1)

- Mobile nodes:
  - IPv6 packet encapsulation/decapsulation
  - Send BUs and receive BAs (process the Mobility Header)
  - Keep track of sent BUs
- Corresponding nodes:
  - Process Mobility Header (BU, BA)
  - Use the Routing Header (type 2)
  - Maintain the binding cache

Required mobility features (2)

- Routers:
  - At least one IPv6 router on the Home Link of the MN must be able to act as a Home Agent
- Home agents:
  - Must maintain MN's binding information
  - HA intercepts packets for a MN in a Home Link it is responsible for
  - HA encapsulates/decapsulates (tunnel) these packets and forward them to the CoA of the MN

MIPv6 Security (1)

- Binding Updates to HA
  - **IPsec** and **ESP** between MN and HA
    - IPsec Security Association (SA) – between MN and HA. Provides integrity and autentication of BU and BA. One SA per home-address. Authentication-only service – authentication header (AH).
    - Encapsulating Security Payload (ESP) – authentication + encryption. After AH header
  - Key Distribution (IKE, Internet Key Exchange)

- Protection of mobile prefix discovery
  - Through the use of IPSec extension headers.

MIPv6 Security (2)

- Binding Updates to CN
  - Return routability procedure to assure that correct MN is sending the message. Node key – secret 160-bit key.
  - IPSec or Binding Authorization Data option
  - Binding management key (K_{bm}) – integrity and authenticity of the BU messages

- Protection of the mechanisms that MIPv6 uses for transporting data packets.
  - Mechanisms related to transporting payload packets – such as the Home Address destination option and type 2 routing header – have been specified in a manner which restricts their use in attacks

MIPv6 Security (3)

- Mobile Node and the Home Agent SHOULD use an IPSec security association to protect the integrity and authenticity of the Mobile Prefix Solicitations and Advertisements.
  - Both the MNs and the HAs MUST support and SHOULD use the Encapsulating Security Payload (ESP) header in transport mode with a non-NULL payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection

MIPv6 Enhancements

- Hierarchical MIPv6 (HMIPv6) – RFC 5380
  - New node: Mobility Anchor Point (MAP) limiting the amount of Mobile IPv6 signaling outside the local domain
  - MN only needs to perform one local BU to a MAP when changing attached point within the MAP domain.
- Fast Handovers for Mobile IPv6 (FMIPv6)
  - Anticipates Mobile IP messaging (before L2 movement)
  - Different RFCs for different (network) technologies, e.g. RFC 4260 for 802.11 networks

Additional Mobility Techniques

- Network Mobility (NEMO, RFC 3963)
  - Move a whole network segment/subnet
  - Accessible through mobile routers connected to HAs
- Proxy MIPv6 (proposed RFC 5213)
  - Mobile node does not participate in mobility signaling
  - Proxy detects the attachment of MN and communicates with home agent instead
  - Local mobility gateway (HA), local mobility anchor
  - Even for IPv4-only nodes
- Multipath TCP (draft of RFC 6824)
  - MP_capable TCP option (+subtypes)

Locator/ID Split Protocol (LISP)

- Split the localizator/identificator function of IP address to reduce global routing table size in default-free zone, non-aggregated block split, BGP-free multihoming, device **mobility** and identity. Address spaces:
  - Routing locators – where are the devices connected
  - Endpoint identifiers – unique device address
- Map-and-encap – map between address spaces, add new header. Tunneling (ingress/egress routers), Map server+resolver (RLOC)
- Mobility: mainly virtual machines
- Outer header (locators), L4 header, LISP header, inner header (EIDs)