

# Mobile IP

## Quick and Dirty

(C) Herbert Haas 2005/03/11

## A Very Quick Summary



1. **Where should the tunnel be terminated**
  - Co-located CoA
  - FA CoA
2. **Authenticated Messages**
  - MD5-HMAC or keyed-MD5 between MN and HA
  - Optionally also to FA
3. **Replay Protection**
  - Via synchronized timestamps in identification fields
4. **Reverse Tunneling**
  - To avoid ingress filtering,
  - allow multicast generation to home network
  - and support NAT (RFC 1918 addresses at MN, NAT at HA)
5. **Broadcast Packets**
  - HA replicates and tunnels them to MNs
  - Additional encapsulation needed in case of FA-CoA
6. **ARP Issues**
  - Gratuitous ARP by HA
  - MN also sends packets for nodes in home network to foreign router

(C) Herbert Haas 2005/03/11

2

## Introduction



- **Nomadic vs Cellular**
  - ◆ Cellular: IP Roaming (reachability) plus handoff (continuous TCP/UDP sessions)
- **Goal:**
  - ◆ Mobile Node (MN) wants to keep home IP address
- **Mobile IP**
  - ◆ IESG June 1996, latest RFC is RFC 3344
- **Alternative: host routes**
  - ◆ MN keeps own IP address and every router in the network installs a host route
  - ◆ Scalability problem: Lots of entries in routing tables and updates

## Applications



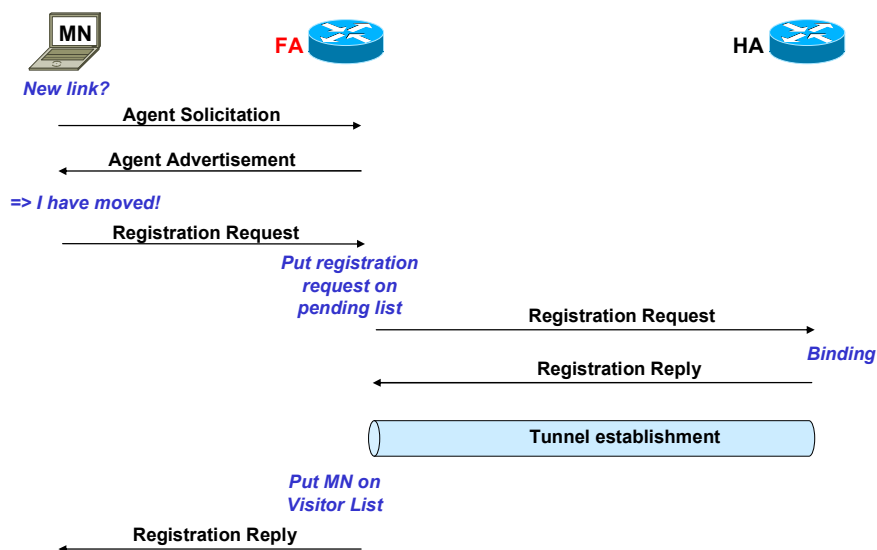
- **Enterprise networks**
  - ◆ When crossing VLANs with wireless VoIP devices
- **Wireless ISPs**
- **Mobile Networks**
  - ◆ Using mobile routers
  - ◆ No Mobile IP on nodes

## Basic Concepts



- Mobile IP must be enabled on HA but only optional on FA
- Use of FA recommended
  - ◆ IP address conservation: Single endpoint for HA
  - ◆ Local authentication
  - ◆ Statistics and billing
- Co-located COA
  - ◆ MN learns local IP address via DHCP
  - ◆ MN talks directly to HA
- FA COA
  - ◆ One COA for all MNs

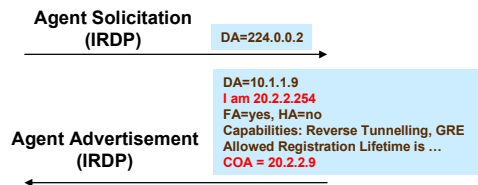
## Registration Procedure (FA CoA)



# Router Discovery Details



New link?



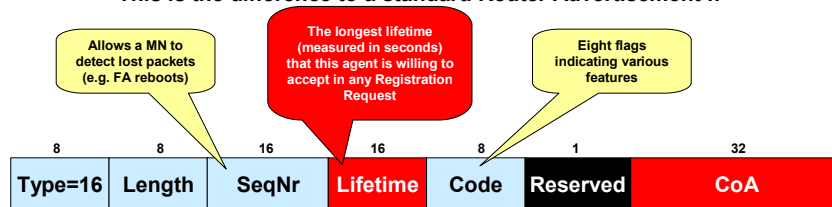
=> I have moved!

Either **FA detected** (HA lost),  
 or **COA changed** (new FA),  
 or **FA gone**  
 (no advertisement during previously  
 announced lifetime period;  
 FA is removed from list of valid  
 agents)

# IRDP Details

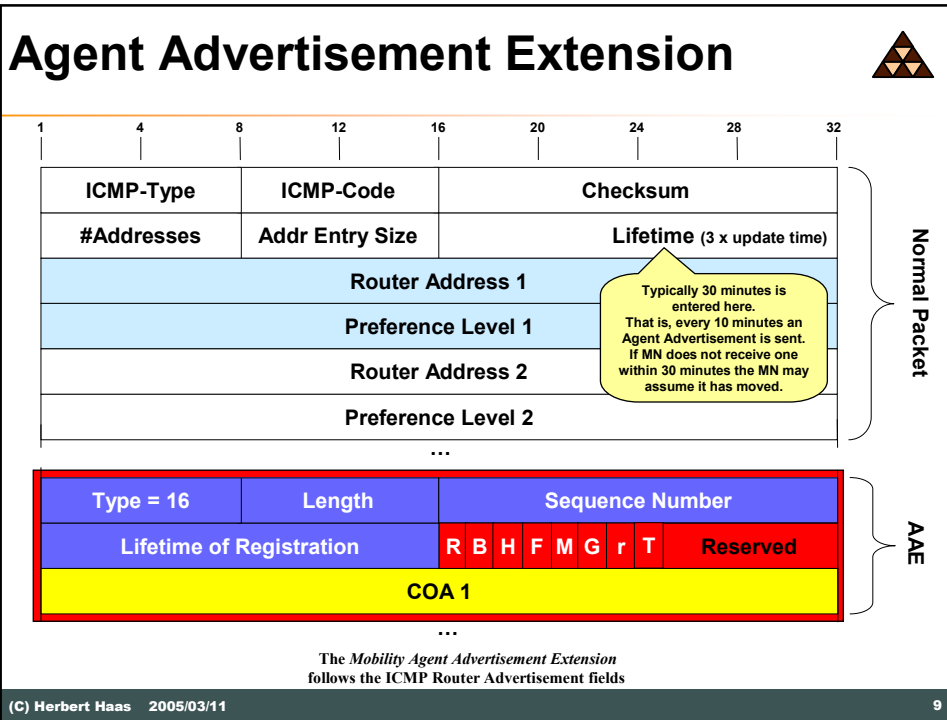


- **Agent Solicitation**
  - ◆ DA=224.0.0.2
  - ◆ ICMP Type 10 ("Router Solicitation")
  - ◆ **TTL=1**
- **Agent Advertisement**
  - ◆ Sent as response but also periodically (DA=224.0.0.1 or 255.255.255.255)
  - ◆ ICMP Type 9 ("Router Advertisement")
  - ◆ Additional "**Mobility Agent Extension**" after ICMP Data field
    - This is the difference to a standard Router Advertisement !!



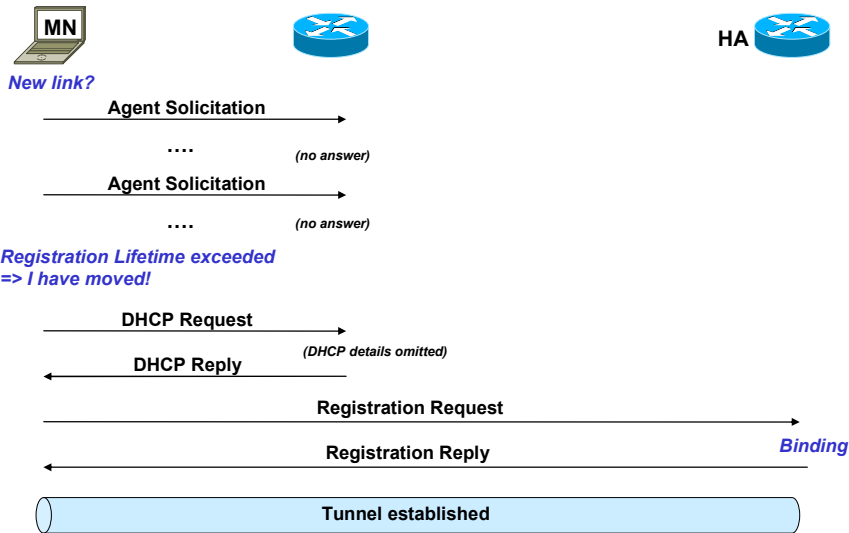
The Mobility Agent Extension

(Also multiple CoAs possible)

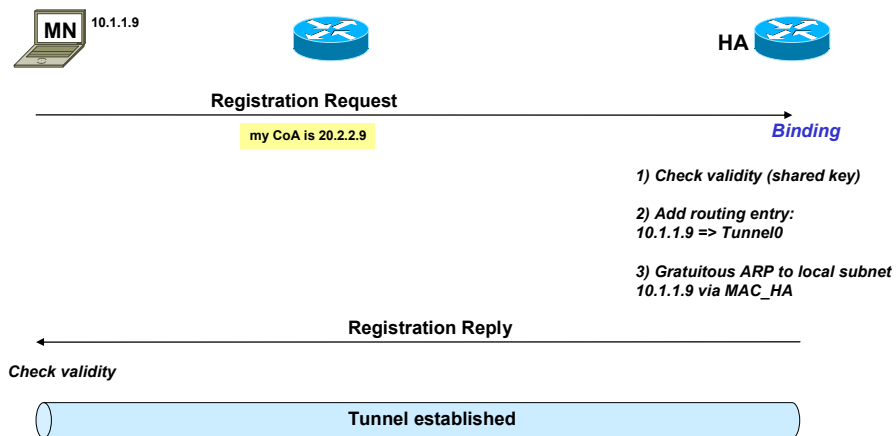


- # AAE Flags
- **R** – Registration required, *even when using a CCoA*
  - **B** – Busy The FA will not accept any registrations from additional MNs
  - **H** – Can act as HA
  - **F** – Can act as FA
  - **M** – Supports minimal encapsulation
  - **G** – Supports GRE encapsulation
  - **r** – reserved
  - **T** – Supports Reverse Tunneling
- (C) Herbert Haas 2005/03/11 10

# Registration Procedure (Co-located CoA)



# Details



# The Registration

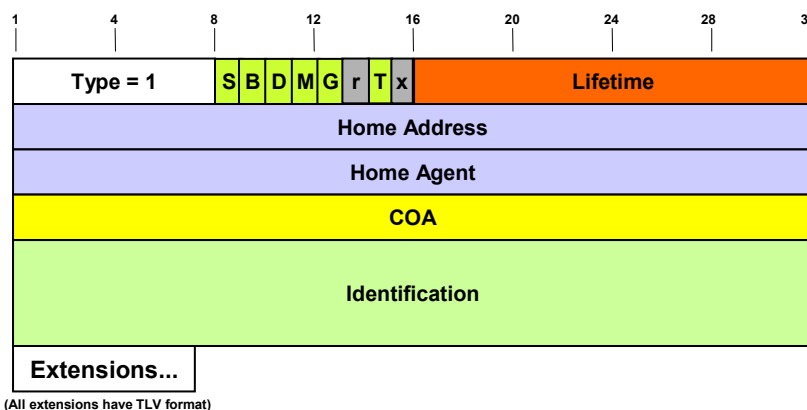


- **Reasons**
  - ◆ **Tell HA about current CoA**
  - ◆ Renew a registration
  - ◆ Deregister when home again
- **MN uses either**
  - ◆ FA CoA
  - ◆ Co-located CoA
    - Then MN might be not required to register through FA
- **MN configuration includes**
  - ◆ IP address of HA
  - ◆ **Mobility Security Association** (shared key) of HA

# Registration Request (1)



(Carried in UDP Payload, Port 434)



## Registration Request (2)



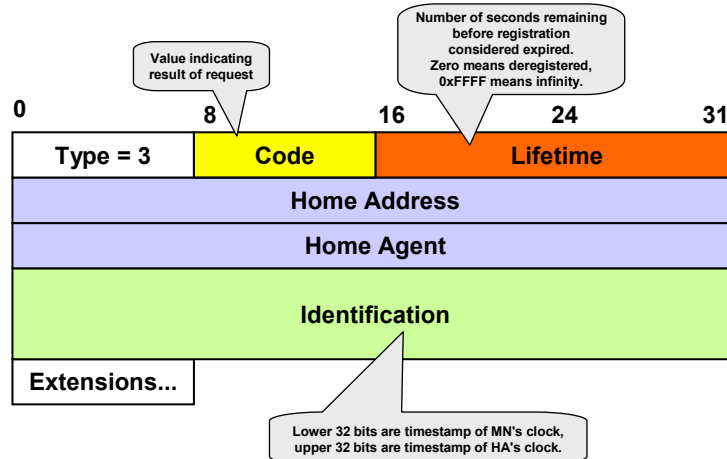
- **S – Simultaneous bindings**
  - ♦ "Mobile node requests HA to retain its prior mobility bindings"
  - ♦ If a wireless MN moves within transmission range of more than one FA, the HA keeps multiple tunnels open and replicates each packet in order to reach the MN
- **B – Broadcast datagrams**
  - ♦ HA should tunnel any broadcast datagrams that it receives on the home network
- **D – Decapsulation by mobile node**
  - ♦ MN decapsulates datagrams by itself (using a co-located COA)
- **M – Minimal Encapsulation**
- **G – GRE Encapsulation**
- **T – Reverse Tunnel Request**

## Registration Request (3)



- **Lifetime**
  - ♦ **Number of seconds before registration is considered expired**
  - ♦ zero = deregistration, 0xffff = infinity
- **Home Address**
  - ♦ IP address of the MN
- **Home Agent**
  - ♦ IP address of the MN's HA
- **Care-of Address**
  - ♦ IP address of tunnel endpoint
- **Identification**
  - ♦ 64-bit number used to match registration requests and replies
  - ♦ Mitigates replay attacks of registration messages
  - ♦ Lower 32 bits are timestamp from MN's clock
- **Extensions**
  - ♦ E. g. Mobile Home (MH) Authentication Extension (MHAE), which is generated from shared key

## Registration Reply (1)



## Registration Reply (2) – Code Values



- 0 registration accepted
- 1 registration accepted, but simultaneous mobility bindings unsupported
- 64 reason unspecified
- 65 administratively prohibited
- 66 insufficient resources
- 67 mobile node failed authentication
- 68 home agent failed authentication
- 69 requested Lifetime too long
- 70 poorly formed Request
- 71 poorly formed Reply
- 72 requested encapsulation unavailable
- 73 reserved and unavailable
- 77 invalid care-of address
- 78 registration timeout
- 80 home network unreachable (ICMP error received)
- 81 home agent host unreachable (ICMP error received)
- 82 home agent port unreachable (ICMP error received)
- 88 home agent unreachable (other ICMP error received)
- 128 reason unspecified
- 129 administratively prohibited
- 130 insufficient resources
- 131 mobile node failed authentication
- 132 foreign agent failed authentication
- 133 registration Identification mismatch
- 134 poorly formed Request
- 135 too many simultaneous mobility bindings
- 136 unknown home agent address

## Network Address Identifier (NAI)



- If MN adds the NAI extension, the NAI overrides the Home Address field
  - ♦ NAI is a character string in e-mail format
  - ♦ AAA servers at foreign networks can identify MNs
- Home Address field is typically 0.0.0.0, otherwise MN is requesting that address
  - ♦ FA scans registration reply for IP addresses assigned by HA and adds this address to its visitor table
- NAI extension field
  - ♦ Must be the first of all extension fields
  - ♦ Type 131
- RFC 2794

## Authentication Extension



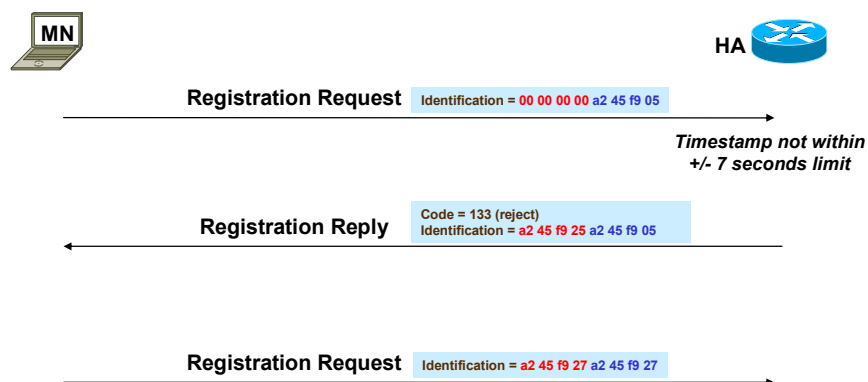
- **Mobile Home Authentication Extension (MHAE) field required** for all MN-HA messages !!!
  - ♦ To prevent unauthorized nodes from accessing the home network
  - ♦ HMAC-MD5 with pre-shared 128-bit key (RFC 3344)
  - ♦ Or keyed-MD5 in "prefix-suffix" mode with pre-shared 128-bit key (RFC 2002) using MD5("key, registration message, key")
    - Note: The "prefix+suffix" use of MD5 to protect data and a shared secret is considered vulnerable to attack by the cryptographic community. (RFC 3344)
- Optionally MN-FA or FA-HA messages can also be protected
  - ♦ Using the Mobile-Foreign Authentication Extension (MFAE)
  - ♦ or the Foreign-Home Authentication Extension (FHAE), respectively.
- Message details
  - ♦ Type fields: 32=MHAE, 33=MFAE, 34=FHAE
  - ♦ 4 byte SPI to support different devices with same NAI
  - ♦ 128 bit "Authenticator" field (longer fields also supported)

## Replay Protection



- 64 bit **Identification** field in RRQ
  - ◆ MN puts own clock value in low-32 bits
  - ◆ HA examines this field and rejects the RRQ if MN's clock is not within +/- 7 seconds of HA's clock
  - ◆ The rejection message uses code 133 and the high-32 bits of the identific

## Replay Protection



## Tunneling

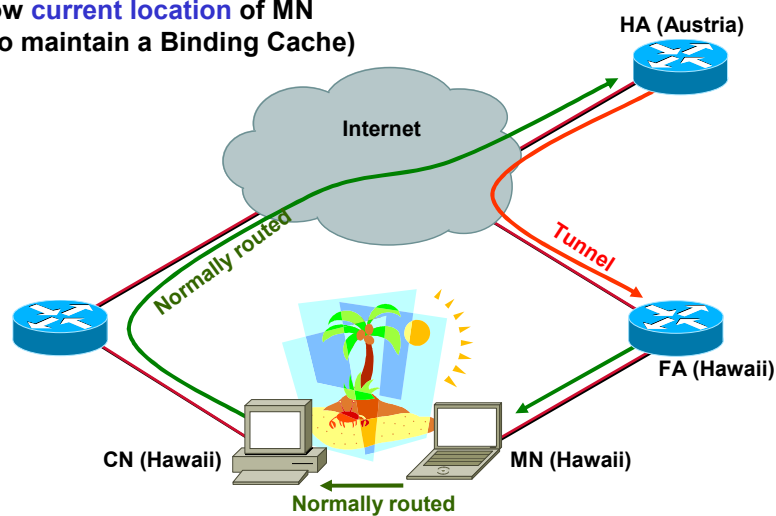


- IP in IP is default
- Minimal Encapsulation and GRE are optional
- Path MTU discovery can be used
  - ◆ However, firewalls might not allow that

## Triangle Routing



To optimize Mobile IP, CN needs to know **current location** of MN  
(=> also maintain a Binding Cache)



## Reverse Tunneling - Reasons



- **Ingress Filtering using RPF**
  - ◆ CN's router might perform RPF to detect SA spoofing attacks
  - ◆ If FA sends MN's packets into a reverse tunnel to the HA the router at the CN has no problems
- **Multicast**
  - ◆ Reverse tunnels allows a MN to send multicast packets to a multicast tree in its home network
- **NAT**
  - ◆ If the MN uses a RFC 1918 home address, then all packets must be sent back to the HA where the translation occurs

## Reverse Tunneling

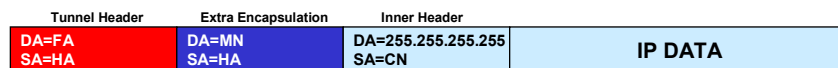


- **To create a reverse tunnel, the MN must set the "T" flag in registration requests**
  - ◆ Co-located CoA: HA will handle reverse tunnel requests by default
  - ◆ FA CoA: FA must be configured to support reverse tunnels
- **Can be IP-in-IP or GRE tunnels**

## Encapsulation of Broadcasts



- MN is logically still "at home"
  - ◆ And might want to receive all broadcasts
- HA can be configured for "broadcast encapsulation"
  - ◆ Disabled by default
  - ◆ If configured, a MN can request this service using the "B" bit
  - ◆ Each broadcast packet is sent as unicast to every client in the binding table (broadcast replication)
- Requires **extra encapsulation** if FA is used
  - ◆ Otherwise all other nodes at the FA's subnet will receive the broadcast
  - ◆ Only for co-located CoAs normal tunneling is sufficient



## ARP Issues



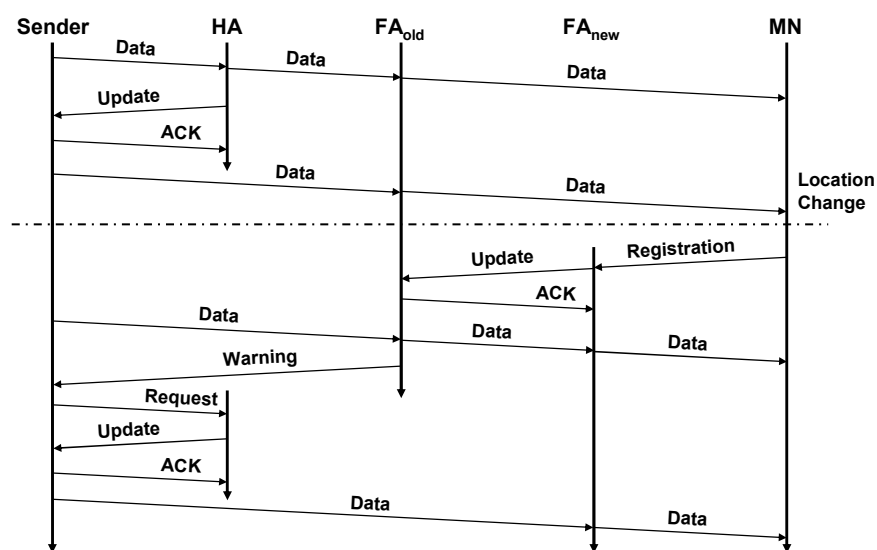
- After registration HA sends **Gratuitous ARP**
  - ◆ So all local nodes can update their ARP cache (IP\_MN => MAC\_HA)
  - ◆ That is, HA acts as *Proxy-ARP* agent for MN
- CN in same (foreign) subnet
  - ◆ MN cannot perform ARP at local (=foreign) network
  - ◆ Therefore also packets to nodes in local (=foreign) network are sent to foreign router
    - FA forwards them to CN
    - CN replies by sending to HA (=> tunnel => MN)

## Optimization (1)



- HA may inform CN – but 4 new messages necessary:
  - ♦ **Binding Request**
    - Every CN who wants to know MN's current location can send this message
    - If MN *allowed* publication of current location, HA can send a Binding Update
  - ♦ **Binding Update**
    - Includes home IP address of the MN and COA address
  - ♦ **Binding Acknowledgement**
    - Acknowledgement of Binding Update
  - ♦ **Binding Warning**
    - If a FA receives a packet but this FA isn't the current FA anymore, this FA can send a Binding Warning (smooth handover)
    - Send to HA

## Optimization (2)



## Client Software



- **Cisco Mobile IP Client (CMC)**
  - ◆ **Current (1Q2006) version 1.0(.12) is a bit buggy**
    - Identification via static IP address does not work – use NAI only!
  - ◆ **As “Default GW” use HA inside interface**
- **Birdstep Mobile IP Client**
  - ◆ **Free for personal use, but complicated registration procedure**

## Configuration: HA



```
(config)# router mobile
(config)# ip mobile home-agent lifetime 300

(config)# ip mobile host nai herbert@left.com
        address 10.20.2.100 interface fa0/1
(config)# ip mobile secure host
        nai herbert@left.com spi 100
        key hex 112233...

(config-if)# ip irdp !!! inside interface !!!
(config-if)# ip mobile prefix-length
```

## Configuration: HA Redundancy



```
interface FastEthernet0/0  !!! connected to other router
ip address 10.1.0.2 255.255.255.0
standby ip 10.1.0.1          !!! this will be MN's HA address
standby priority 102
standby name classlab
!
interface FastEthernet0/1  !!! connected with MN
ip address 10.20.2.1 255.255.255.0
ip irdp
!
router mobile
!
router eigrp 100
redistribute mobile  !!! to enter virtual networks in routing tables
network 10.0.0.0
!
ip mobile home-agent lifetime 300
ip mobile home-agent redundancy classlab virtual-network
ip mobile virtual-network 10.50.60.0 255.255.255.0
ip mobile host nai herbert@left.com address 10.50.60.100 virtual-network
                                     10.50.60.0 255.255.255.0
ip mobile secure host nai herbert@left.com spi 100 key hex
                                     11223344556677889900aabbccddeeff algorithm md5 mode prefix-suffix
ip mobile secure home-agent 10.1.0.3 spi 100 key hex
12345678901234567890123456789012 algorithm md5 mode prefix-suffix
```

## Configuration: HA Red. + FA



```
interface FastEthernet0/0
ip address 10.1.0.2 255.255.255.0
standby ip 10.1.0.1
standby priority 102
standby name classlab
interface FastEthernet0/1
ip address 10.20.2.1 255.255.255.0
ip irdp
ip mobile foreign-service
ip mobile prefix-length
!
router mobile
router eigrp 100
redistribute mobile
network 10.0.0.0
!
ip mobile home-agent lifetime 300
ip mobile home-agent redundancy classlab virtual-network
ip mobile virtual-network 10.50.60.0 255.255.255.0
ip mobile host nai herbert@left.com address 10.50.60.100 virtual-network
                                     10.50.60.0 255.255.255.0
ip mobile foreign-agent care-of FastEthernet0/1
ip mobile secure host nai herbert@left.com spi 100 key hex
                                     11223344556677889900aabbccddeeff algorithm md5 mode prefix-suffix
ip mobile secure home-agent 10.1.0.3 spi 100 key hex
                                     12345678901234567890123456789012 algorithm md5 mode prefix-suffix
```

## Important Verification Commands



- **show ip mobile binding | visitor**
  - ◆ MNs on HA | FA (see CoA | tunnel endpoints)
- **show ip route**
  - ◆ See “M” prefix and tunnel interface
- **debug ip mobile**
  - ◆ Shows nearly everything
- **show ip mobile global**
  - ◆ Important mobile-ip parameters (features, lifetime, etc)
- **show ip mobile host | tunnel | violations**

## Using an AAA



- **If thousands of MN-SAs are configured statically on the router**
  - ◆ Everything is stored in NVRAM (!)
  - ◆ Also CPU burden
- **Let HA download SAs from AAA server when needed**
  - ◆ Simplifies changes on redundant HAs
  - ◆ HA may **drop** or cache SAs after use
    - **# clear ip mobile secure**

## Configuration: HA for AAA



```
aaa new-model
aaa authorization ipmobile default group radius

radius-server host 10.1.0.42
radius-server retransmit 3  !!! try 3 times
radius-server key MyKey

ip mobile host nai herbert@left.com address
                        10.20.2.100 interface fa0/1 aaa
```

## ACS Configuration (1)



- **Interface Configuration**
  - ◆ Check “cisco-av-pair” (first item)
- **Network Configuration**
  - ◆ Enter HA in the “AAA Client IP address” field
  - ◆ Enter key which has been configured on HA (myKey)
- **Under “Authenticate Using” select**
  - ◆ “RADIUS (Cisco/PIX)”

## ACS Configuration (2)



- **User Setup**
  - ◆ Enter IP address as User-ID
  - ◆ Omit the password field (!!!)
- **Cisco IOS/PIX Radius Attributes**
  - ◆ (Scroll down a bit to see it)
  - ◆ Check “[009\001] cisco-av-pair” and enter:

mobileip:spi#0=spi 100 key hex  
11223344556677889900aabbccddeeff

mobileip:spi#1=spi 101 key hex  
123456789012345678901234567890ab

(optional additional  
entries)

## Proxy Mobile IP (PMIP)

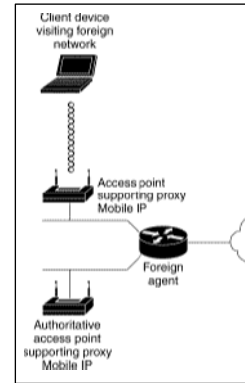


- **With PMIP, the Mobile Node does not need a Mobile IP stack**
- **The AP**
  - ◆ Cares for agent discovery
  - ◆ Generates registrations to the HA in behalf of the MN
- **Three steps to perform:**
  - ◆ **Agent discovery**
  - ◆ **Updating the subnet map table**
  - ◆ **Device registration**
- **Tunnel types: GRE or IPinIP**

## PMIP Phases (1)



- AP boots up or PMIP is enabled
  - ♦ Agent Discovery is performed
  - ♦ HA and FA advertise their services on the network via IRDP
  - ♦ AP learns
    - Whether an agent is a HA, a FA, or both
    - The COA
    - Capabilities (GRE and reverse tunneling, registration lifetime, roaming period)
  - ♦ AP can also enforce these advertisements by sending agent solicitation messages
  - ♦ Must have configured a **Subnet Map Table, containing a list of HA IP addresses and subnet masks**
- Subnet Map Table is sent to **Authoritative AP (AAP)**
  - ♦ AAP is responsible to keep the latest Subnet Map Table
  - ♦ AAP adds new (PMIP-) AP to a list
  - ♦ AAP also adds learned HA to the Subnet Map Table
  - ♦ Finally, the AAP informs all other APs
  - ♦ You can designate **up to three AAPs** on your wireless LAN



Source: Cisco Systems

## PMIP Phases (2)



- When AP detects that client is connected to a foreign network
  - ♦ The AP obtains a COA from the FA
  - ♦ This COA can be *shared* for multiple client devices
  - ♦ The AP notices that the client belongs to another network and begins the registration
  - ♦ The AP now determines the client's HA address from the subnet map table
- Registration
  - ♦ Each AP is configured with the **mobility security association** (shared key) of all potential visiting clients with their corresponding HA
    - Can be provided by a Radius server
  - ♦ AP sends registration request (mobile-SA shared key, client's IP) to the HA of the client
- Agents check this request
  - ♦ FA checks validity of the registration request (requested lifetime must not exceed its limitations and requested tunnel encapsulation must be available)
  - ♦ HA checks if authentication valid

## PMIP Phases (3)



- HA
  - ◆ Creates a mobility binding (client to COA association)
  - ◆ Creates a tunnel to the COA
  - ◆ Creates a routing entry to the client's home IP address through the tunnel
  - ◆ Sends a registration reply
- FA
  - ◆ Checks if registration reply is valid (is registration request still pending?)
  - ◆ Add visiting client to visitor list
  - ◆ Establishes a tunnel to the HA
  - ◆ Creates routing entry to HA
  - ◆ Relays registration reply to client
- AP
  - ◆ Checks validity of registration reply
  - ◆ Forwards client packets to FA
  - ◆ Re-registers on behalf of the visiting client before its registration lifetime expires

## Note



- Proxy Mobile IP does not support VLANs (currently?)
- Use NTP:
  - ◆ Registration requests may fail if the timestamps generated by the requestor are outside the window expected by the receiver
- Be sure to enable proxy Mobile IP on each SSID that requires it
  - ◆ None of the proxy Mobile IP configuration commands take effect until proxy Mobile IP is set on the SSID
- AP requires a default gateway entry
- No IP multicast support
- Make sure that UDP port 6500 is not blocked between the authoritative AP and other APs
  - ◆ Used for subnet table updates

## PMIP Configuration



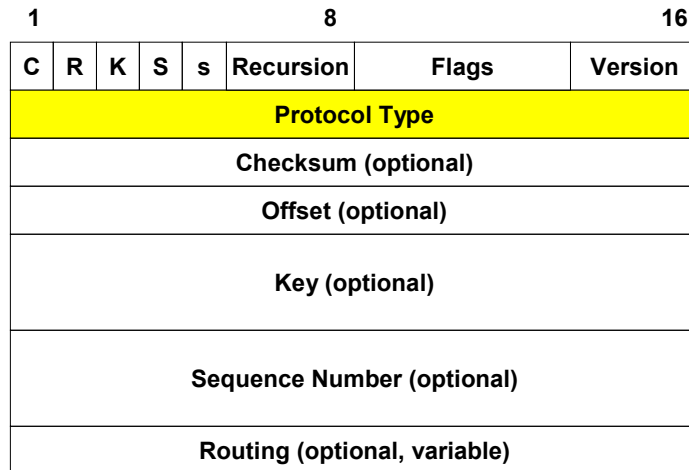
```
ap1200# configure terminal
ap1200(config)# ip proxy-mobile enable
ap1200(config)# ip proxy-mobile aap 192.168.15.22 192.168.15.24 192.168.15.28
ap1200(config)# ip proxy-mobile secure node 10.91.7.151 10.91.7.176 spi 102 key ascii 0987654
ap1200(config)# interface fastethernet 0
ap1200(config-if)# ip proxy-mobile
ap1200(config-if)# interface dot11radio 0
ap1200(config-if)# ip proxy-mobile
ap1200(config-if)# ssid tsunami
ap1200(config-if-ssid)# ip proxy-mobile
ap1200(config-if-ssid)# exit
ap1200(config-if)# exit
ap1200(config)# interface bvi1
ap1200(config-if)# ip proxy-mobile
ap1200(config-if-ssid)# end
```

## PMIP Security



- **Mobile IP**
  - ◆ **Uses a strong authentication scheme to protect communications to and from visiting clients**
  - ◆ **All registration messages between a visiting client and the home agent must contain the mobile-home authentication extension (MHAE).**
- **Proxy Mobile IP**
  - ◆ **Also implements this requirement in the registration messages sent by the AP on behalf of the visiting clients to the home agent**

## Old GRE Header Format (RFC 1701)



## Header Bits



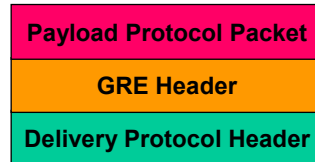
- **Protocol Type**
  - ◆ Ethernet protocol Type of the payload packet
- **Offset**
  - ◆ Present if the Routing or the Checksum field is/are present
- **Checksum**
  - ◆ Of the GRE Header and the Payload Packet
- **Key**
  - ◆ May be used to authenticate the source of the packet
- **Sequence Number**
  - ◆ May be used to check the order of the packets



## IPv4 and GRE



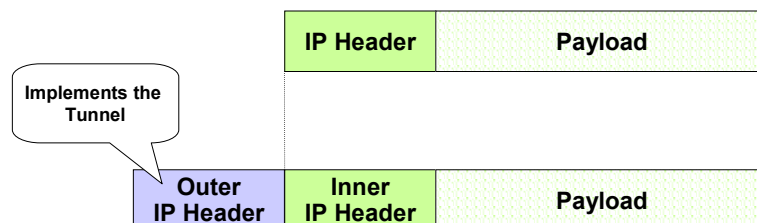
- IPv4 as a GRE Payload Protocol
  - ◆ GRE Protocol Type field is set to 0x800
- IPv4 as a GRE Delivery Protocol
  - ◆ IPv4 protocol field is set to 47

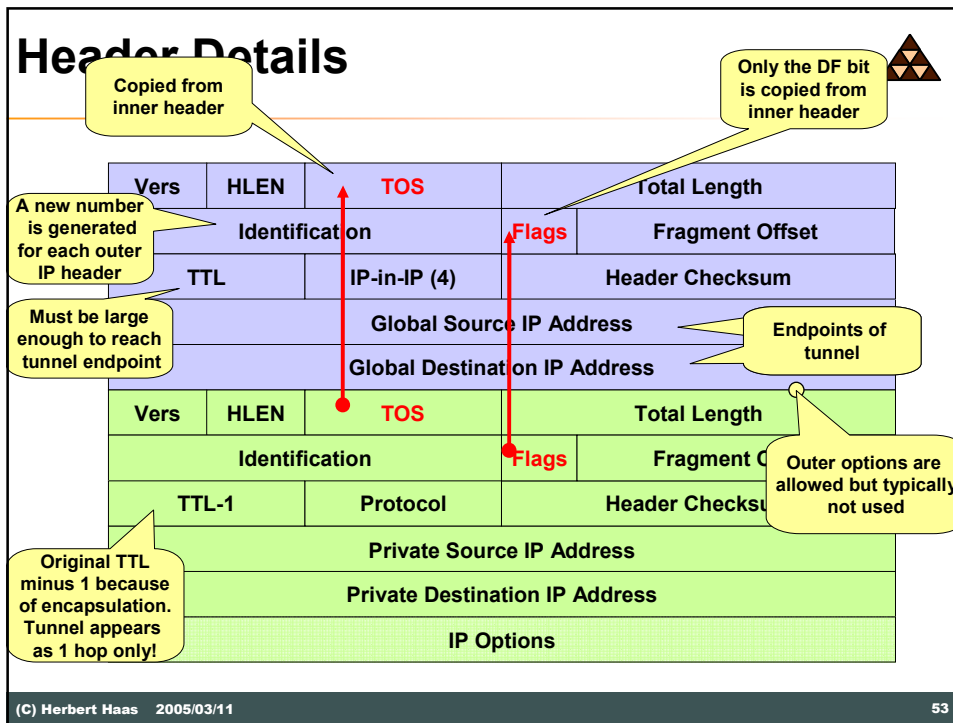


## IP in IP Encapsulation



- RFC 1853
- Used with Mobile IP per default
- Other headers might be used in between (e. g. security headers)





- ## ICMP Problems
- ICMP messages only return 8 bytes of the IP payload
    - ◆ Not enough information for originating host
  - Thus, encapsulating routers should maintain tunnel soft-states
    - ◆ Reachability of end-of-tunnel
    - ◆ MTU
    - ◆ Load
- (C) Herbert Haas 2005/03/11 54

## Minimal Encapsulation



- **IP-in-IP Encapsulation includes many redundant header fields**
  - ◆ ToS is only copied
  - ◆ Inner fragmentation often unnecessary

## IPv6 (1)



- **No FA needed, every MN has a CCoA**
  - ◆ Enough addresses available
- **Use IPsec(AH) for authentication of binding requests**
- **MN can send binding updates to CN**
  - ◆ To announce the current CoA and to avoid triangle routing
  - ◆ CN sends packets to MN using CCoA as DA and MN's home address in the routing extension header

## IPv6 (2)



- **MN addresses HA-Anycast address**
  - ◆ For ICMP HA Discovery Requests
  - ◆ Reply lists all active HAs
- **Return Routability Procedure**
  - ◆ CN and MN have secret keys and generate encrypted cookies every few minutes
  - ◆ These cookies are sent directly and indirectly (through the HA) between each other to test routability
  - ◆  $\text{hash}(\text{cookie\_CN}, \text{cookie\_MN}) = \text{session key}$

## IPv6 (3)



- **MN sends Home Test Init to CN**
  - ◆ via HA (reverse tunnel)
  - ◆ Including a Home Test Init Cookie (HOTI)
- **MN sends a Care-of Test Init to CN**
  - ◆ Directly
  - ◆ Including a COTI
- **CN creates a home cookie and sends a Home-Test (HOT) via HA to MN**
  - ◆ Also includes HOTI from MN again

## IPv6 (4)



- **CN creates CoA-cookie and sends CoA-Test to MN (directly)**
  - ◆ Also includes COTI from MN again
- **MN hashes home-cookie and CoA-cookie to create session key**
- **MN sends binding message (protected via session key) to CN**