
Mobile Networking

Jim Binkley- jrb@cs.pdx.edu

outline

- ◆ introduction
 - problem space
- ◆ Mobile-IP - RFC 2002
- ◆ problems/solutions &&
- ◆ PSU solutions for some problems
 - security/redundancy
- ◆ one whacky idea
- ◆ research areas

but 1st - a commercial

- ◆ PSU/DARPA project
 “Secure Mobile Networks”
- ◆ try to combine Mobile-IP/IPSEC network security/Wavelan wireless LAN
- ◆ focus on **security** and **survivability**
- ◆ e.g., MIP has single point of failure in Home Agent, therefore developed
- ◆ HARP - Home Agent Redundancy Protocol

project home page

- ◆ <http://www.cs.pdx.edu/research/SMN>
- ◆ includes FreeBSD based
 - FA-oriented Mobile-IP
 - IPSEC integrated with Mobile-IP
 - » HA/MN 2-way ESP tunnels
 - Wavelan drivers: ISA/PCCARD
 - » old and IEEE 802.11
 - simple less insecure ad hoc routing protocol
 - » replacement for ARP

problem space

- ◆ mobile systems as opposed to fixed systems
- ◆ wireless or multi-interface as opposed to wired infrastructure
- ◆ current systems designed to stay put from OS up/down
- ◆ applications/transport/network/link layer
 - assumptions favor wired/fixed systems

some problems - net stack POV

app layer: dns* works at boot/rich bandwidth

transport layer: TCP disconnect=congestion

network layer: IP address -> subnet locality,
network design

link: wireless metrics/bandwidth/reachability

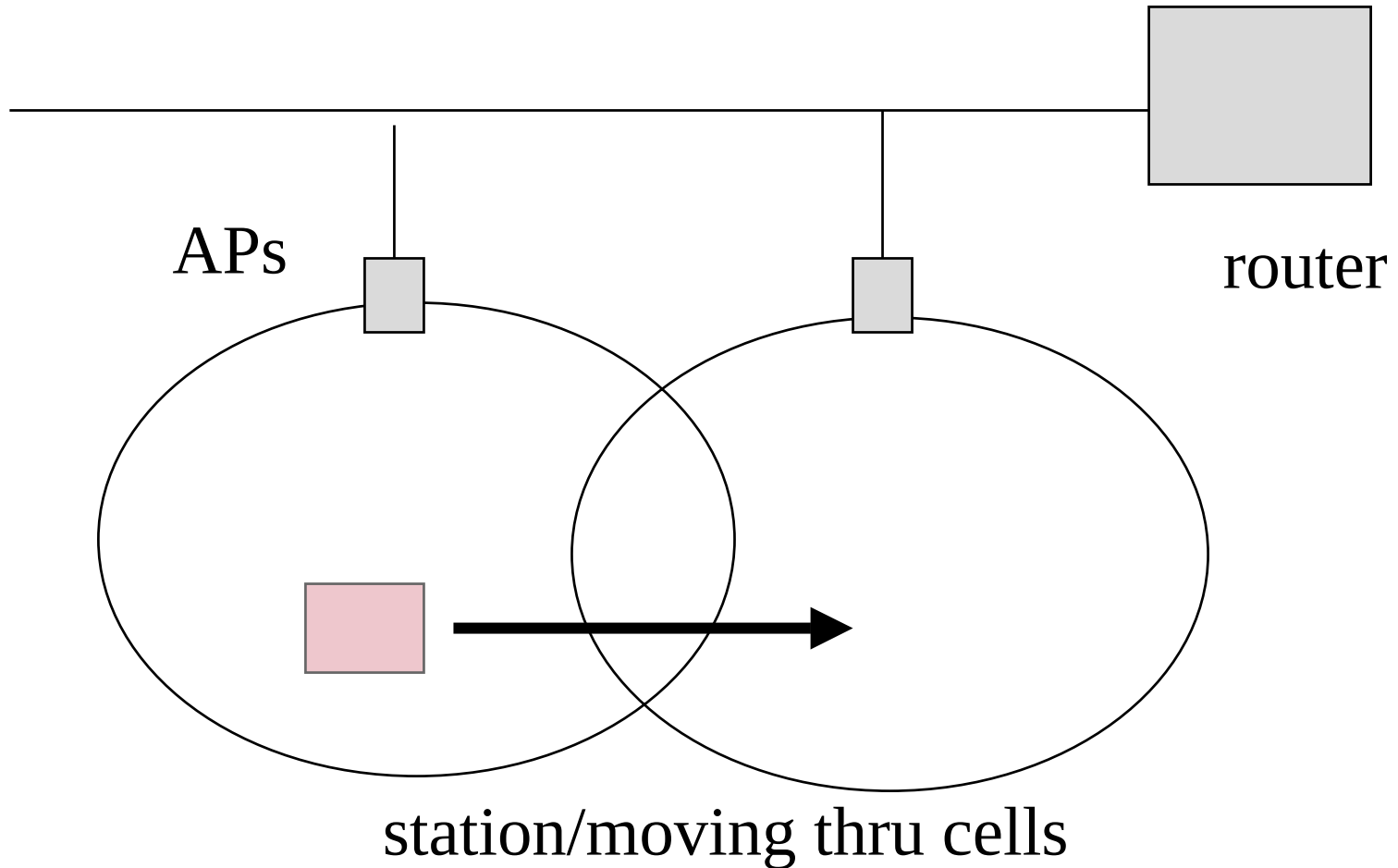
certain high-level problems

- ◆ multiple interfaces and networking, where again you have an assumption that you don't change i/fs (or IP addresses)
 - o.s. objects bound to immutable lower objects
 - Novell server knows your mac -- change cards?
- ◆ security - dumb end station no longer sheltered by firewall (still a problem)
- ◆ finding information on the road that applies only to travelers

3 mobile net design prototypes

- ◆ roaming; e.g., IEEE 802.11 wireless,
 - beacons from Access Points
 - STations login to A.Ps
 - IP subnet/connection problems ignored
- ◆ DHCP per subnet
 - can give you DNS (pro)
- ◆ Mobile-IP
- ◆ your idea here ...

IEEE 802.11 - roaming



pros/cons

◆ pros

- claimed interoperability

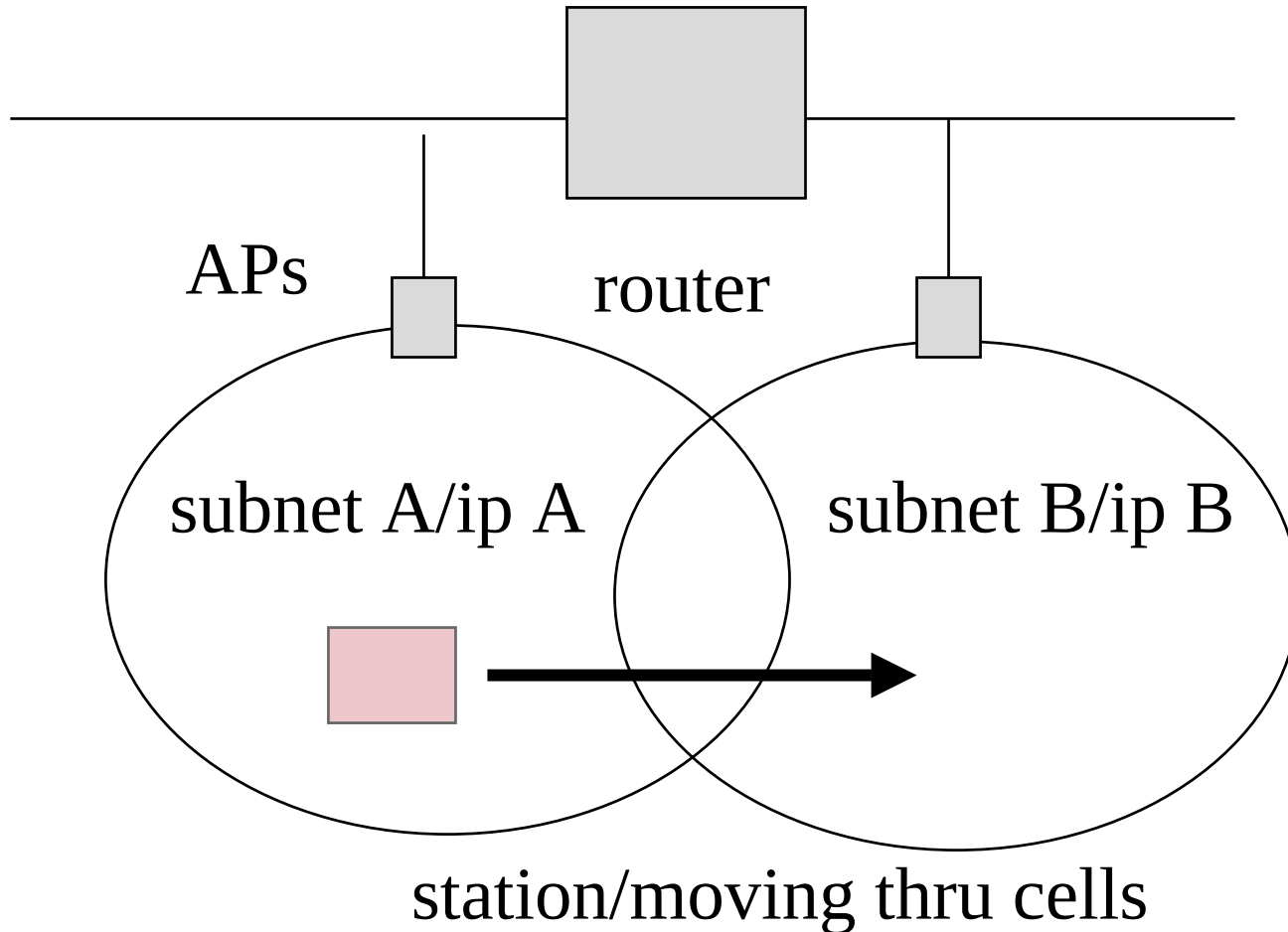
◆ cons

- can't span IP subnets
- one security model: mac addresses known a-priori
 - » mac addresses are spoofable
- bridge-centric (bridges leak)
- loading factor of wireless devices low

virtual lans

- ◆ vlans might save it
 - campus-wide external (outside) vlan model
 - must be top-down switch infrastructure
- ◆ more cons of wireless devices
 - too expensive
 - APs really too expensive

DHCP-model (sitzkreisig mobility)



DHCP model

- ◆ everytime you go to new subnet - you must replug (per subnet IP address)
- ◆ can co-exist with roaming model
- ◆ (may exist but) no well-known way to dynamically do this other than user-initiated
- ◆ can work with ethernet as well as wireless
- ◆ con: loss of connections on move
- ◆ security model: overall same as mobile-ip
 - however DHCP exchanges are unauthenticated

understand

- ◆ DHCP is an auto-discovery protocol
- ◆ not a routing protocol
 - can give you local default router
- ◆ gives you router/DNS/subnet mask/IP address
 - IP address is leased
 - perhaps time here should be shorter than 1 day
 - » 1 hour?

Mobile-IP

- ◆ rfc2002 - way too long to produce, standards trk
- ◆ basic goal: defeat the IP address fixed at a link problem; i.e.,
- ◆ invariant: **the Mobile Node may retain a “home” IP address that does not change from link to link**

pros for MIP

- ◆ easily change same-domain links - no bureaucracy
- ◆ IP address hides link-layer details; e.g., beaconing (or link discovery) is now MIP property
 - **FA beaconing makes for faster handoffs (mcast doable)**
- ◆ DNS name binding fixed
 - keep same name, change IP hard due to caching
- ◆ TCP connection may be retained across links - can't change peer state easily

pros (but worthy of argument)

- ◆ NO A.P. (wireless bridges) need apply
 - **do it with routers** to minimize flat universe + broadcast/security/multicast flooding problems
- ◆ extends IP address space
 - (IP away, IP at home) == 64 bits
 - **you need never go home**
 - (or 256 in the case of Ipng) - JOKE!
- ◆ meta-pro: IP address as name is useful

cons

- ◆ IGP or EGP (cross domain)?
 - if latter then huge security problems
- ◆ isn't DHCP way more cool?
 - slightly different problems
 - DHCP doesn't preserve an IP address
 - make case that **both are needed for adaptable MN**
 - FA or DHCP admin easier?
- ◆ fundamental attack on IP subnet model (pro?)?
- ◆ surprise: didn't solve all possible mobility problems

protocol

- ◆ MIP is a routing protocol that consists of:
 - 1. **link discovery** via advertisements or solicitations (ICMP router advert + MIP part)
 - 2. **forwarding via tunnels** (IPIP) from Home Agent to Foreign Agent/Mobile Node
 - 3. **MIP UDP registration protocol**
 - » UDP request/UDP reply
 - » MN (to FA) to HA and back again
- ◆ network layer - but app daemons

jargon/entities

- ◆ **MN - Mobile Node** (say, a laptop or peripatetic toaster)
- ◆ **HA - Home Agent** (router at “home” IP subnet)
 - when at home, normal IP
 - when away, HA forwards packets to your remote site
- ◆ **FA - Foreign Agent** (aka base station, router at “foreign” link/subnet, where you wandered to)
 - ids link, and serves as tunnel endpoint
- ◆ **CH - Correspondent Host**, any peer end system
- ◆ **COA - care of address**, where you wandered to

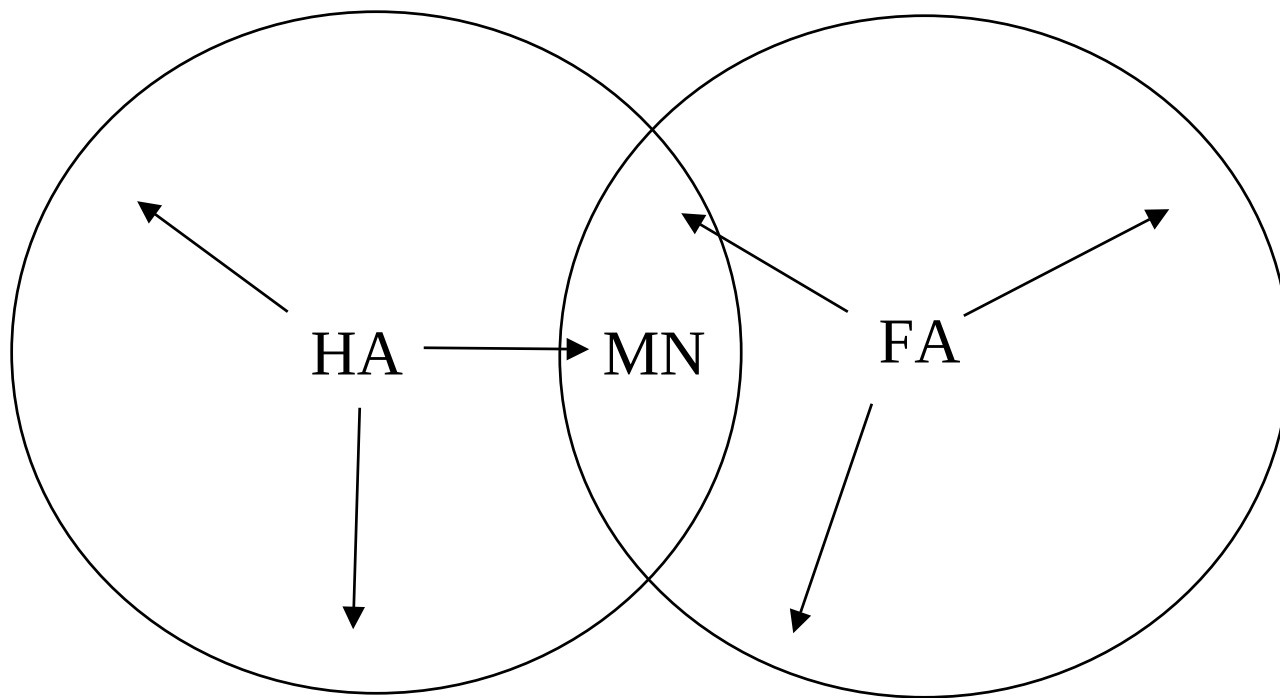
2 basic MIP topologies

- ◆ #1: FA-MIP: MN assumes FAs exist at subnets that are “elsewhere”
- ◆ #2: COA-MIP: MN acts as own FA, must be able to acquire local IP address on foreign FA-less link,
 - say via DHCP
 - or PPP dynamic IP allocation
 - or manually (ethernet config, SLIP)
- ◆ local net admin will determine which is available MN should adapt to link
- ◆ **MN could use DHCP for opt. info in all cases**

link discovery

- ◆ agents (HA/FA) may send ICMP router advertisements with MIP extension
- ◆ MNs can hear and make decisions about who to use
- ◆ MN may send solitication, but agent beacons enable faster handoff
- ◆ **FA beacon provides FA COA + local link IP address (may/may not be same)**

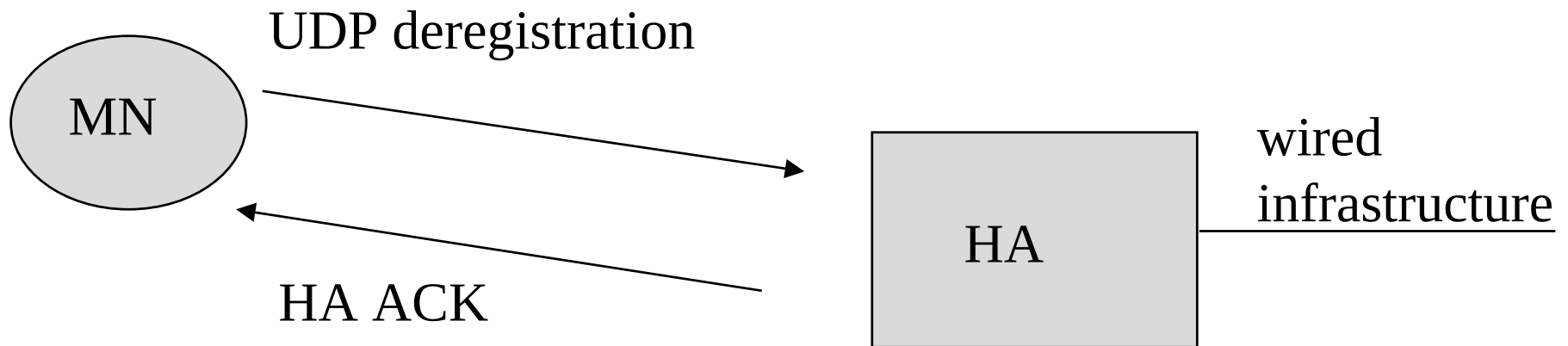
beaconing - radio POV



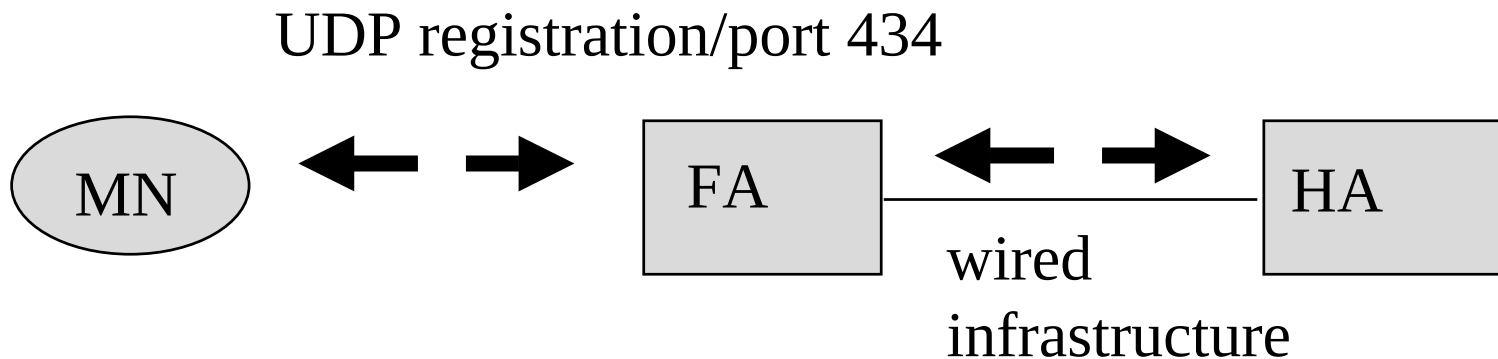
MIP registration

- ◆ MIP protocol consists of UDP registration/ack message on port 434
- ◆ at home MN tells HA it is home - HA cancels any “AWAY” tunnels/state
- ◆ treated as normal IP
- ◆ at FA, MN sends FA UDP registration (includes FA COA + HA address)
- ◆ FA proxy forwards to HA, and back to MN

MN - HA registration at home

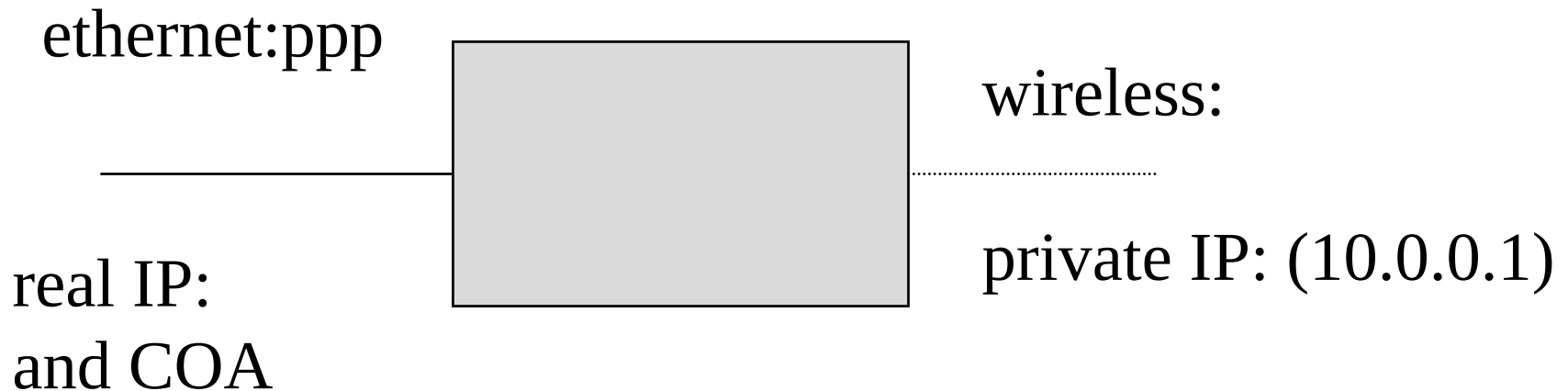


at FA



FA acts as application gateway to forward UDP registration to HA, MN tells HA that it is at FA

possible FA architecture/wireless

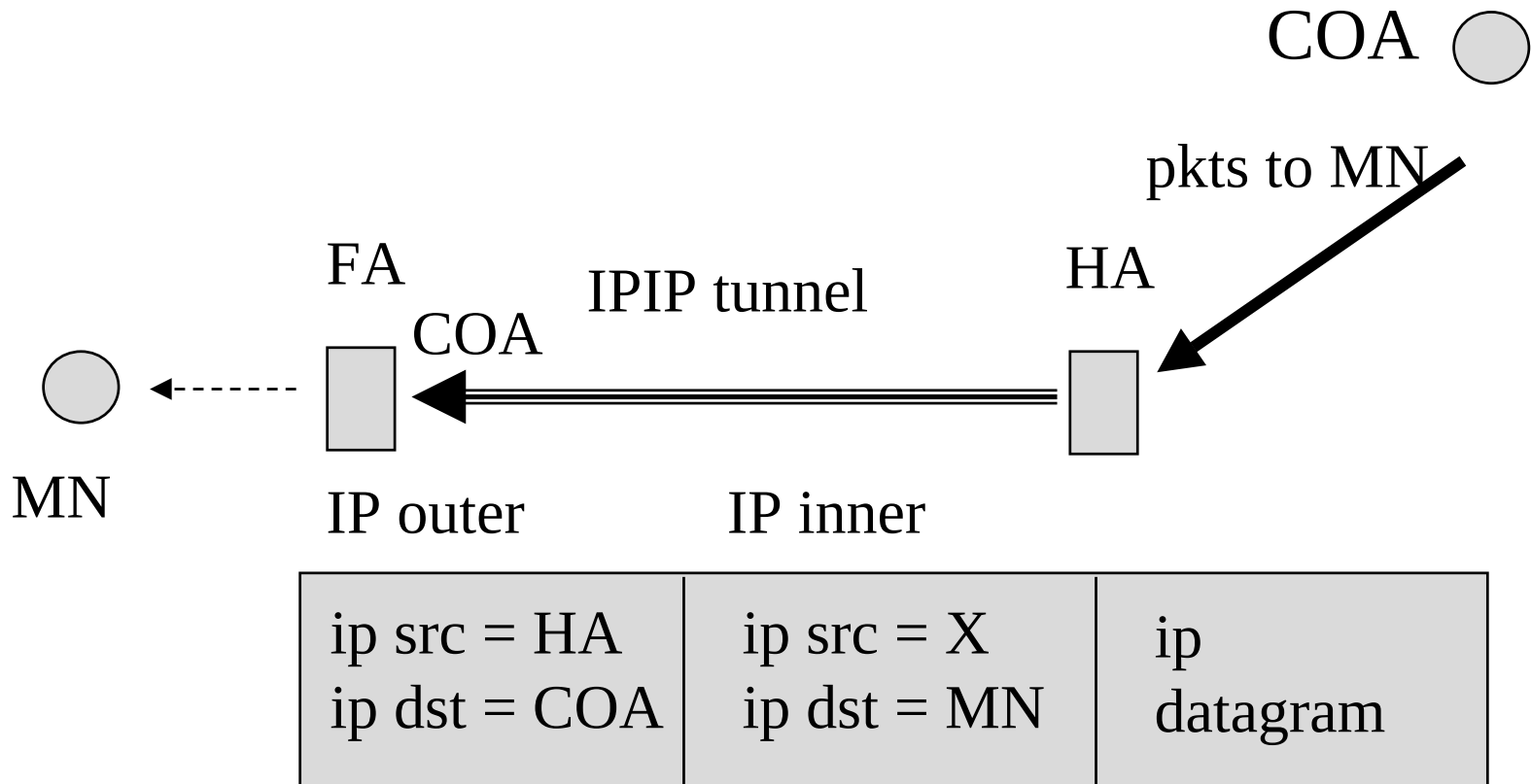


non MIP systems can only attack FA
don't waste IP address on FA side

registration result: MN/HA

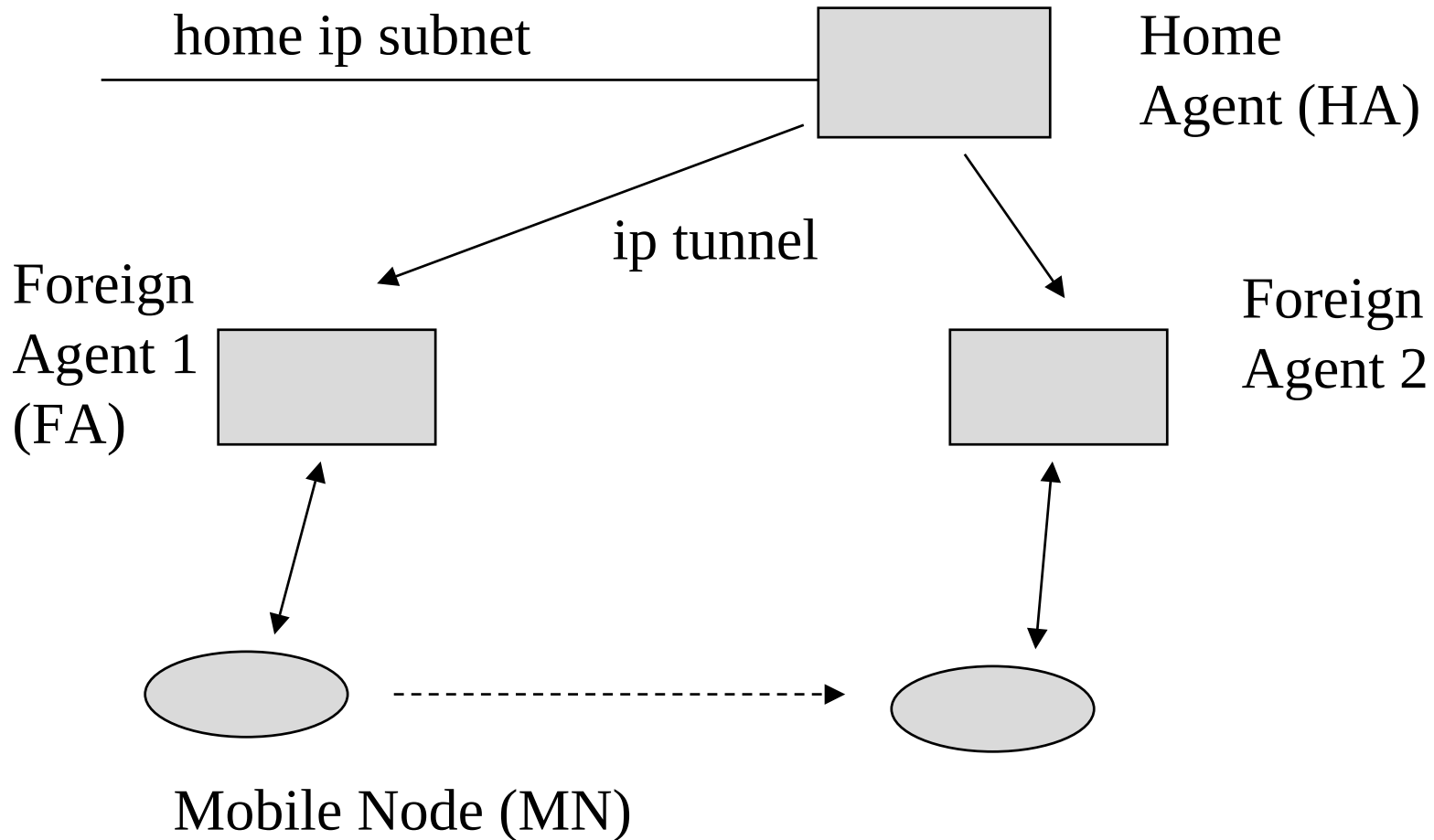
- ◆ HA knows that MN is at (COA IP, MN IP)
- ◆ uses IPIP(4) tunnel (or GRE etc...) to forward packets send to MN at home to FA
- ◆ FA is tunnel endpoint
- ◆ FA strips outer IP header and delivers inner IP datagram to local MN
- ◆ if no-FA case, MN acts as own tunnel sink

IPIP tunnel, HA to MN



note: IPIP is unicast, not multicast MBONE/DVMRP

MIP TOPO Overview



routing note

- ◆ packets to MN when AWAY are forwarded by HA to COA; i.e., local link surrogate
- ◆ MN must keep HA appraised of that COA, when it moves, tell HA about change
- ◆ fundamental MIP only deals with packets “to” the MN
- ◆ packets from the MN are routed normally; i.e., MIP need not apply

MIP UDP packet authentication

- ◆ shared symmetric MD5 128 bit key
- ◆ MN/HA, MN/FA, FA/HA authentication all may exist
- ◆ not dynamic, but manual key
- ◆ implemented with TLV at end of registration/reply packet
- ◆ IP address, SPI as indices
- ◆ 2 kinds of replay protection, TS, nonce

3 MIP security/net topos?

- ◆ **interior:** FA based for quick handoff, DHCP optional for local info (DNS server, printer)
- ◆ **exterior:** (for guests), DHCP a requirement so that MNs can get local address?
 - net admins must consider local security
- ◆ **on the road:** must be FA based for quick handoff and cell discovery.

problems ...

- ◆ MIP is IP-layer, a step up but not silver bullet for all known mobility problems
- ◆ triangle routing may be considered a problem (or an advantage ...)
- ◆ subnet && mobility a problem
 - wireless link and subnet != reachability
 - MN from subnet X/Y can't talk directly
- ◆ security security security

problems

- ◆ o.s. flexibility for MIP support may be put to test - implementation issues
 - bind i/f X (IP address) to subnet Y (FA)
 - change default route dynamically (MN)
 - arp issues
 - do tunnel out and tunnel in (HA/FA/MN)
- ◆ HA is possible single point of failure (fate-share)

security

◆ within-enterprise

- wireless links may be deemed less secure
- have you heard of TEMPEST?

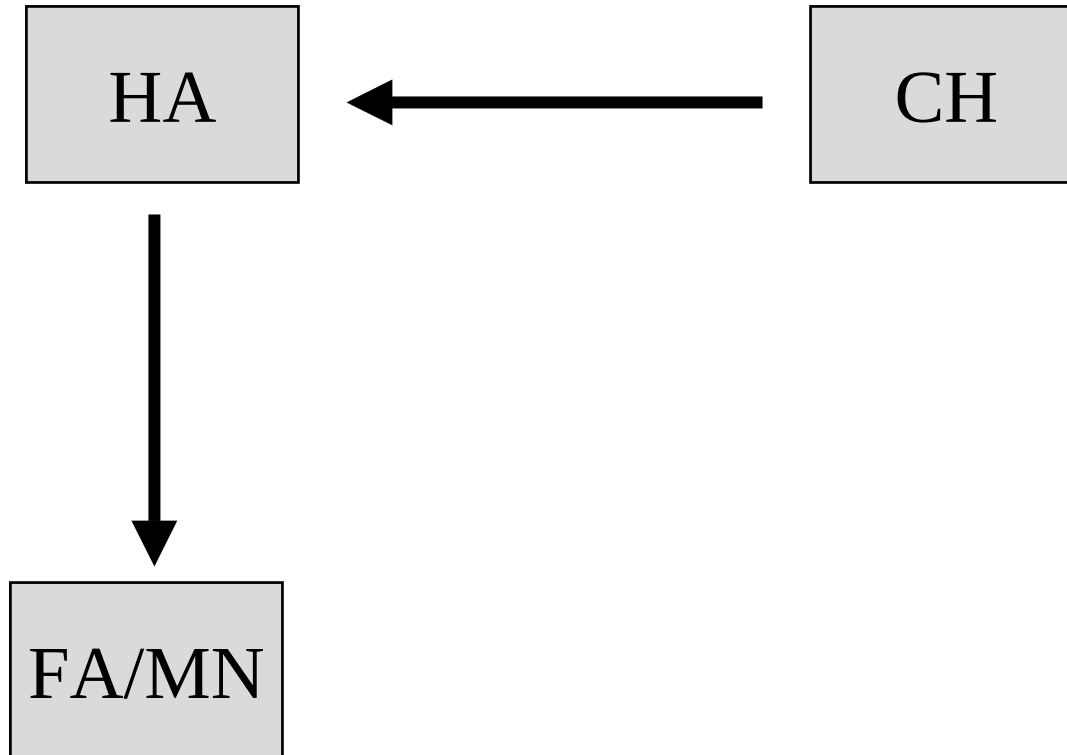
◆ without-enterprise

- laptop && owner abroad have shed home firewall - need own protection
- enterprise must have insecure subnet for visitors; i.e., visitors can't attack internal nets
- policy must evolve ... from no visitors allowed

security (more ...)

- ◆ MN/HA shared manual keys are scalable but
 - FA/HA (especially > 1 HA at a site)
 - FA/MN are not
- ◆ need dynamic lookup say via DNS or Kerberos like system
 - BBN MOIPS/PSU digsig both DNS based
- ◆ need security for all MN packets

triangle routing



triangle routing, cont.

- ◆ IPv6 to fix - CHs need to be told about MN move and tolerate (COA, MN) tuple
- ◆ on the other hand, from security POV
- ◆ may not want to fix it
- ◆ make the MN always appear to be at home
 - don't tell strangers where you are going ...
 - MN might always tunnel*back* home
 - **2T routing** :->

problem: subnet/reachability

- ◆ problems that MIP does not address
- ◆ call it the “subnet != link problem”
- ◆ if B can hear A/C, B can’t assume A can hear C (radio) (it’s not ethernet)
 - ICMP redirects are hazardous ...
- ◆ two MNs with different IP and radio sitting on top of each cannot talk with traditional IP/subnet/ARP (need router/FA)

PSU - simple Ad Hoc #1

- ◆ everybody beacons - MNs and agents
- ◆ overload ICMP router discovery with extra info
- ◆ authenticate (MAC src, IP src) with shared MD5 symmetric key (optional but we do it)
- ◆ if you hear a beacon, and you can authenticate it, then and only then install link-layer route
- ◆ if you don't install route, X can send you packets but you won't send X any
- ◆ note: **you don't speak ARP any more (IP/enet)**

2 MNs at a FA - problem #1

MN2
ip subnet=Y

MN1
ip subnet=X



MNs have DIFFERENT IP subnets, but could hear
each other and talk direct

note: impossible with conventional IP subnetting, what
if no FA? (with our ad hoc can still talk...)

problem #2

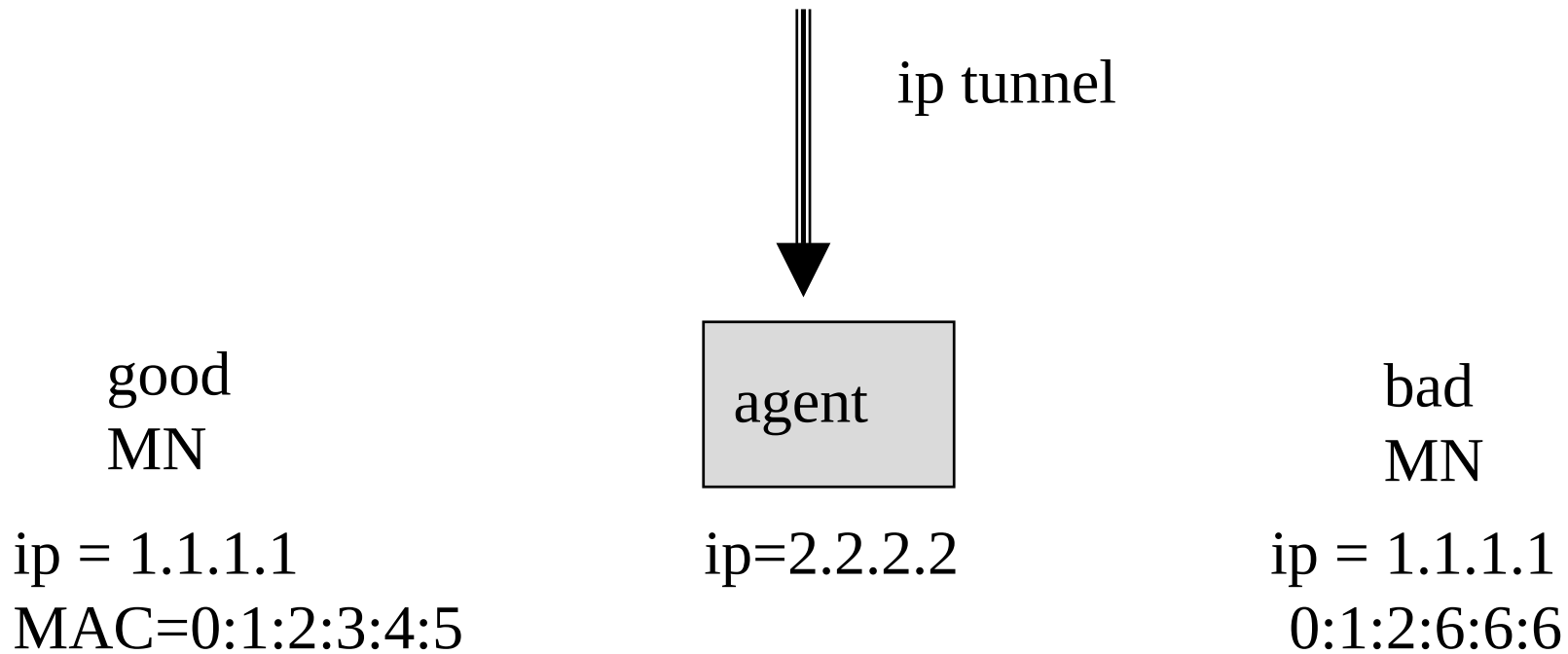
- ◆ 2 MNs with SAME subnet, one at HOME and one AWAY
- ◆ can't talk to each other with ARP/subnetting because obviously aren't on same link && not even close

MN1
subnet=X



MN2
subnet=X

problem #3: ARP spoof



arp spoof, cont.

- ◆ bad MN can send out promiscuous ARP overwrite that only FA can hear
- ◆ FA will overwrite ARP cache for good MN, with bad MN's MAC address
- ◆ bad MN can steal MIP tunnel and thus evade MIP UDP registration authentication even when MN-FA registration required
- ◆ good MN may not be able to hear bad MN promiscuous ARP overwrite ...
- ◆ upshot is now need to do MAC spoofing

arp spoof, cont

- ◆ spoofing now only possible if MAC the same,
- ◆ call it “**MAC spoof**”
- ◆ *party attacked will get attackers packets since they share a unicast link address ...*
- ◆ **increases odds that attacked party can learn about attack**

problems: beacon scalability

- ◆ MN conference == scalability problem?
- ◆ **I live for that day ...**
- ◆ solution/s:
 - 1. scale back MN/MN beaconing
 - » might answer solicitation (tricky problem)
 - 2. MN pushes beacons (or combines with)MIP
FA registration, ignores other MNs when in crowd, so MN/FA only. FA could tell loading

mobile security

- ◆ large problem area
- ◆ MN when going away must take site security/policies with it
- ◆ traditional firewall measures now have TWO new considerations
 - 1. our side abroad (home MN away)
 - 2. friendly visitors here (visitor MN here)

mobisec issues (more than this)

- ◆ 1. MN may choose to secure its own data to/from HA or to/from CHs, not just MIP registration security (all data)
- ◆ 2. site security must somehow setup visitor quarantine network - net design issues
 - can include internal wireless of course
- ◆ 3. scalability of MIP authentication itself an issue; especially FA/(HA,MN)

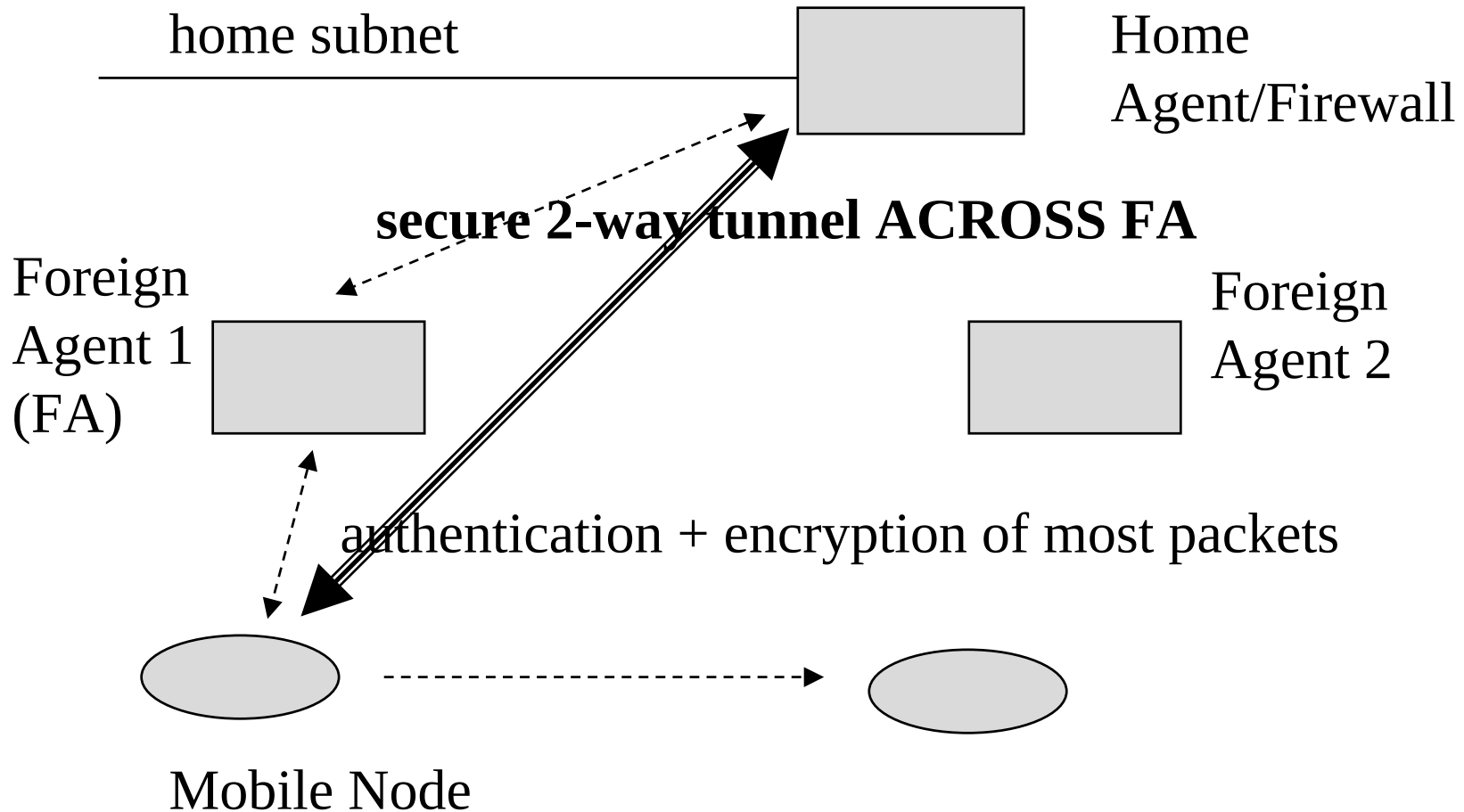
security/routing chicken/egg problem

- ◆ assume you want to do a 3-way handshake to setup a dynamic 1-way security association
- ◆ you need secure routing to do that; i.e., how to setup security if routing is unsecured?
- ◆ arp attack is trivial example of problem
- ◆ makes obtaining public keys or 3-way security handshakes hard(er)

data security via IPSEC

- ◆ 1st-cut policy && implementation
 - MN/HA 2-way IPSEC tunnels over FA
 - “don’t talk to strangers” FA is man in the middle
 - when at home, MN/HA == link-layer security
- ◆ IPSEC (RFCs 1825-), not just IPng
 - AH, authentication header (md5/sha)
 - ESP, confidentiality (DES, ...)

over FA (a long long way to run)



over FA: MN to HA with ESP

outer IP

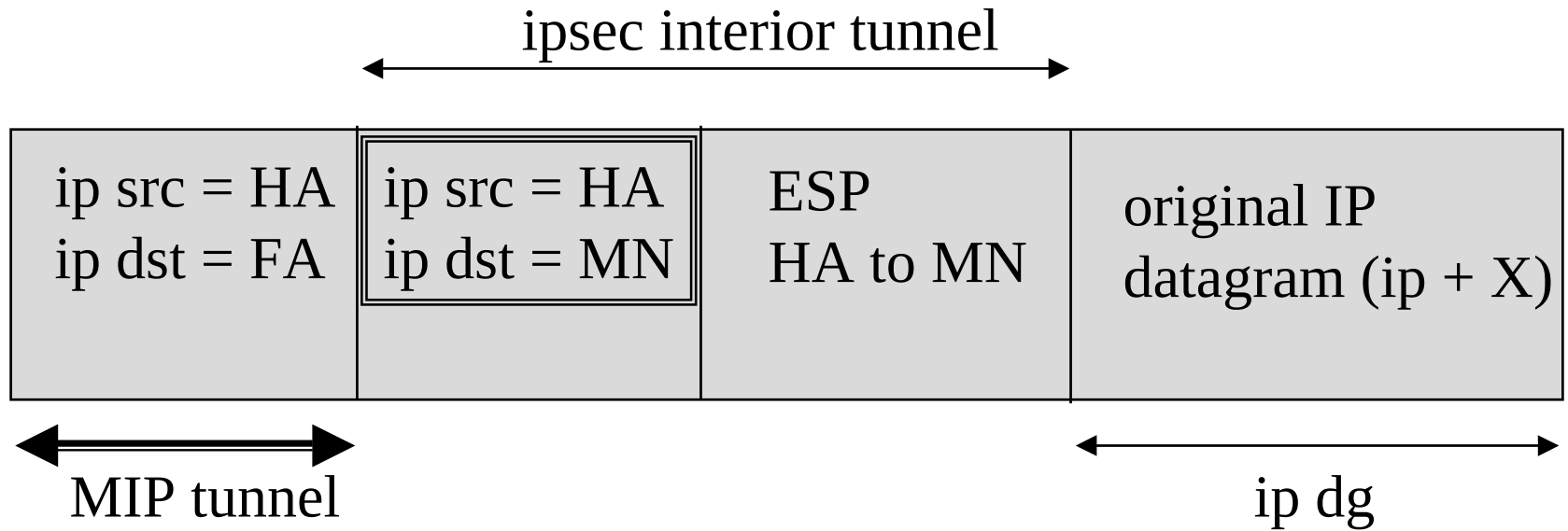
ESP

IP datagram

ip src=MN ip dst=HA	ESP spi for MN to HA	ip src=MN ip dst=X	TCP/UDP, etc.
------------------------	-------------------------------	-----------------------	---------------

default route to FA (next hop router), has itdst to HA
ip_output adds **IPSEC tunnel/ESP**

HA to MN



1. need IP | ESP insertion for IPSEC tunnel from HA to MN
 2. need outer MIP IP header for HA to FA
- note: could have AH or ESP between two headers for HA/FA relationship

IPSEC manual key

- ◆ **scalability** is of course an issue and key lifetime
- ◆ ISAKMP/Oakley are IPSEC answers for using public key technology to
 - dynamically generate security bindings
 - create session keys
- ◆ have demonstrated use of ISAKMP between MN/HA for 2-way tunnel

redundancy outline

- ◆ ad hoc

- # 1 (done), link layer (no router needed)
- # 2 - multi-hop protocol, call it **MADrp**

- ◆ HA redundancy (have > 1 at a time) -
HARP (HA Redundancy Protocol)

- ◆ FA redundancy

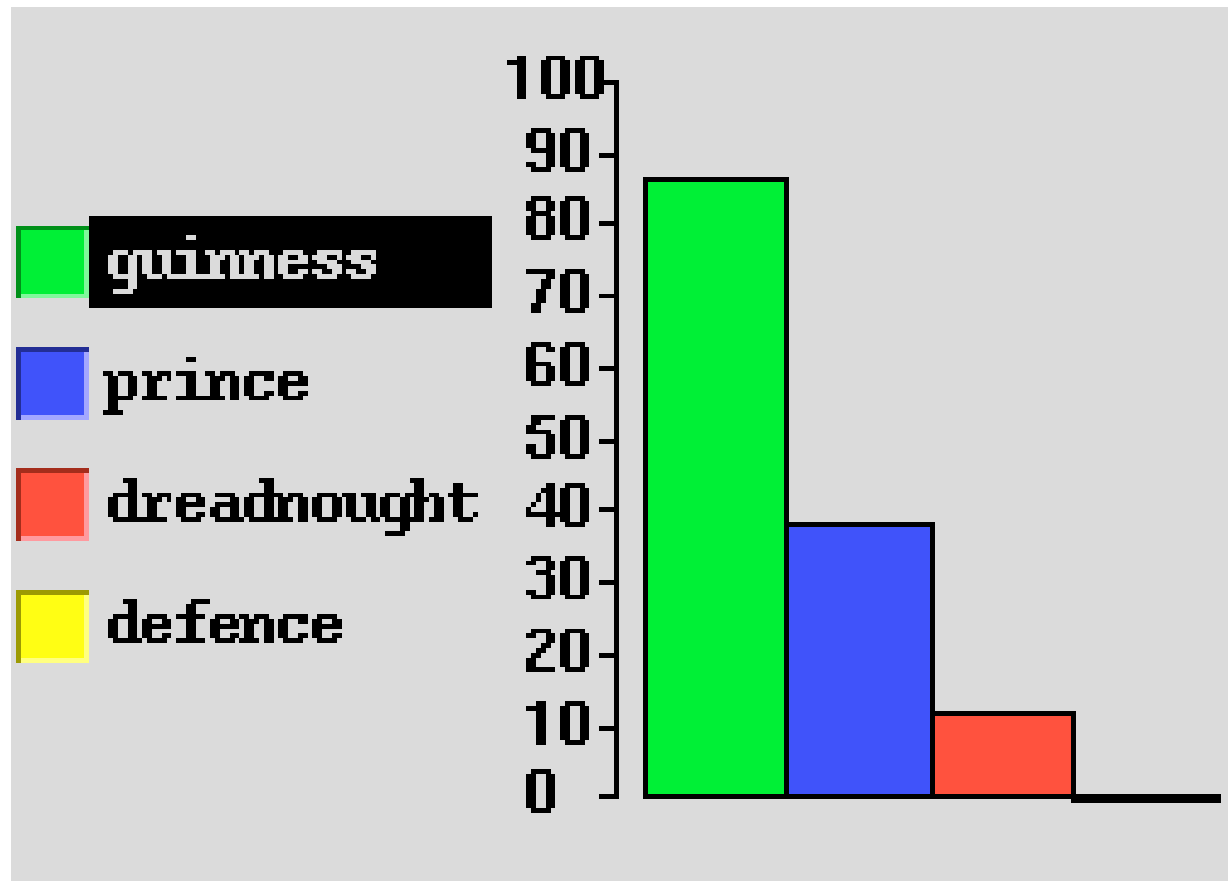
- improved wireless handoff (done)
 - » tolerate overlapping Fas ... avoid FA spoof

- use > 1 router at a time (not released yet)

wireless handoff + redundancy

- ◆ use wavelan signal strength + heuristics
- ◆ go for best agent over period X (say ten seconds)
- ◆ stick with him and don't bounce around
- ◆ agents at MN sorted by SN
- ◆ mark Foreign Agent as bad if we don't get HA ack from it, try another

agent signal strength



ad hoc #2 - MADrp

- ◆ multi-hop ad hoc routing protocol
- ◆ MNs as routers
- ◆ MADrp - *Multicast Ad hoc Demand routing protocol* (MAD for short, or MAD-DRIP)
- ◆ works with Mobile-IP so that MN can talk to Internet
- ◆ can setup IPSEC tunnels MN/MN if keys installed a priori due to auth. madrp pkts

HA redundancy

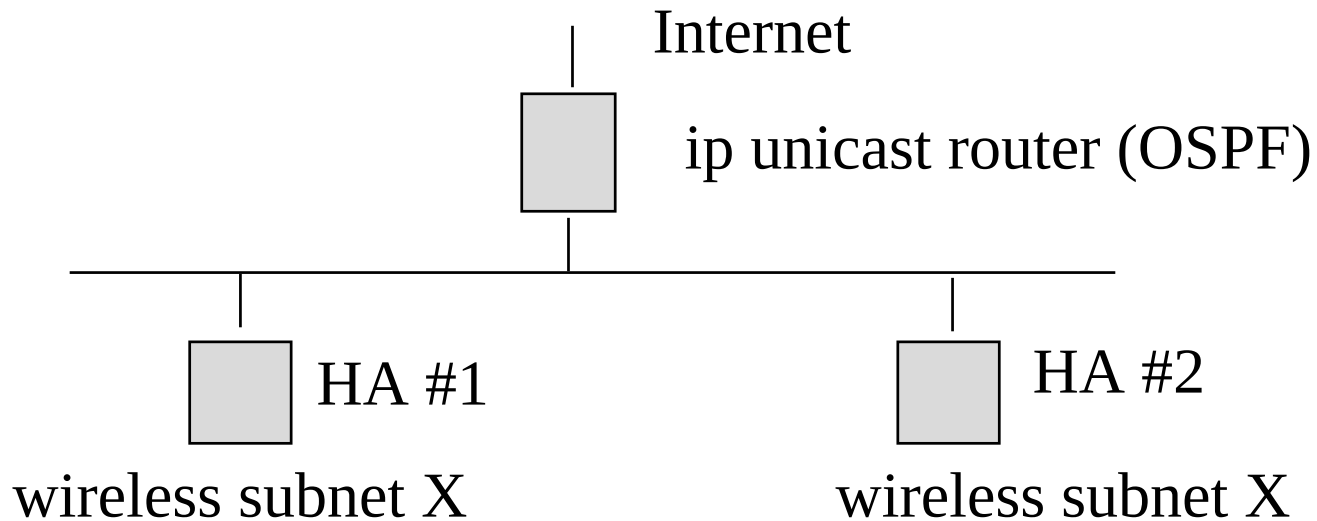
- ◆ view as critical for MIP, one HA is **single point of failure**
- ◆ if current HA goes down, your MIP net is lost
- ◆ FATE SHARING ALL OVER AGAIN

assertions:

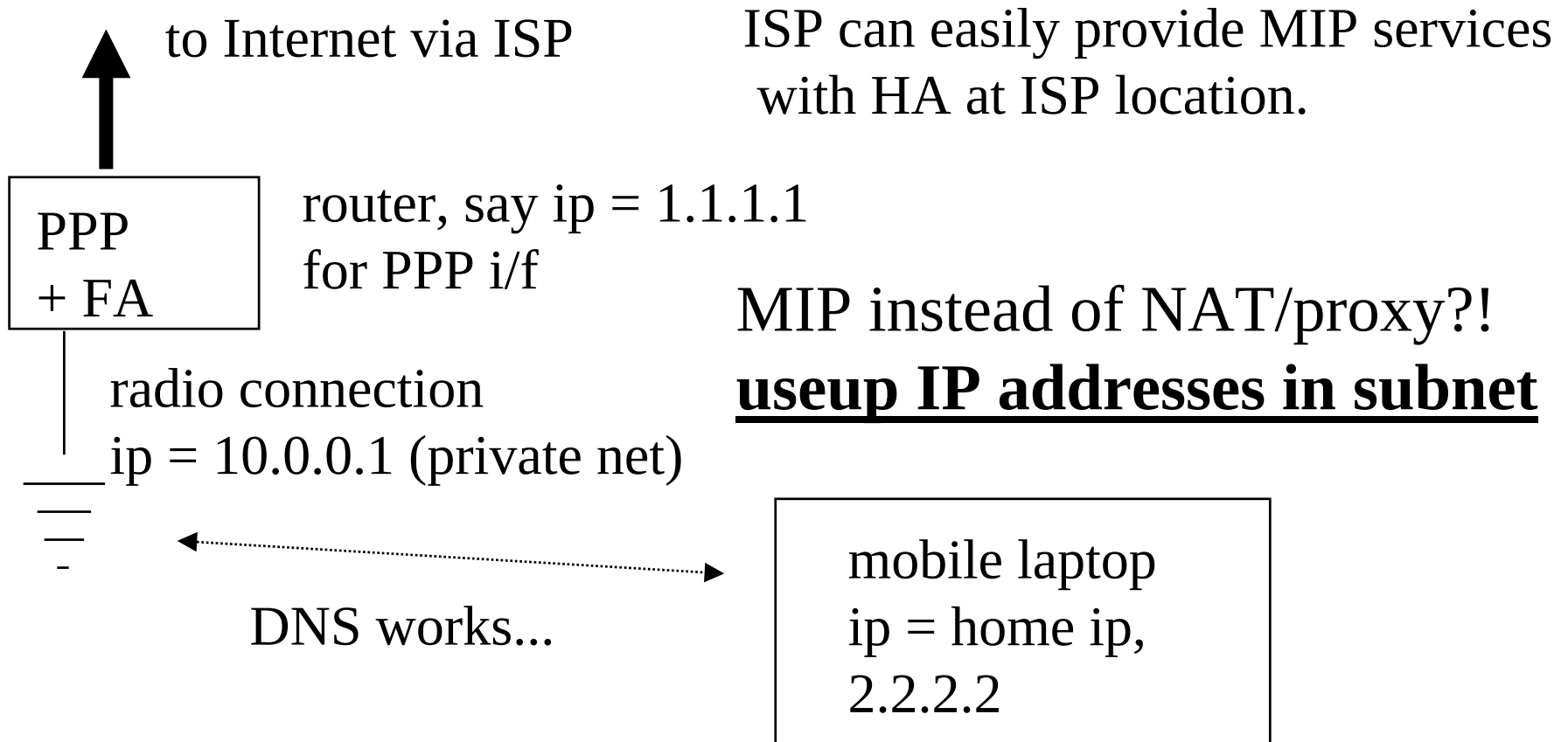
- ◆ HAs may be on same link but ideally are not
 - probably not too far apart though, but would like to shield against 2 HAs lost due to 1 router (or 1 enet card) failure
 - shared subnet, so can't be on OPPOSITE sides of Inet (barring a bridge technology)
- ◆ HAs should keep each other up to date with simple relatively stateless protocol
- ◆ ***no MODS to MIP (MNs/FAs won't know)***

plan:

- ◆ assume two HAs, each of which is a router and routes to the same (partitioned) mobile-IP subnet
- ◆ normal dynamic IP unicast routing can deal with this



whacky idea: HOME MIP



at HOME MIP

- ◆ MNs need never go home
- ◆ can allocate ALL of IP addresses in subnet
- ◆ simply use nearby tunnels from ISP term mux to “settop/ppp/FA” and in-house MNs
- ◆ MN is 2nd/3rd laptop/telephone/toaster
- ◆ this is because MIP addresses are (IP,IP)
- ◆ 2nd enhancement: PSU simple ad hoc enables MN/MN communication where subnet doesn't matter

research areas

- ◆ security
 - MNs dynamically take policy with them on the road
 - scalability of keys and policy negotiation
- ◆ richer data environments for on the road types
- ◆ MN flexibility in terms of multihomed, multi-device, multi-address
- ◆ wireless flexibility/**loading**/thruput
- ◆ multicast (not as done by MIP) routing AND apps
- ◆ ad hoc routing, MNs find a way to get there