Mobile IP

Motivazioni

- Routing
  - basato su indirizzo di destinazione IP, network prefix determina la subnet fisica
  - cambio della subnet fisica implica cambio di indirizzo IP per avere un indirizzo *topologicamente corretto* (standard IP) o c'è bisogno di entries speciali nelle tabelle di routing

- Routes specifiche agli end-system?
  - cambio di tutte le entries delle tabelle di routing per inoltrare pacchetti alla giusta destinazione
  - non scala con numero di host mobili e frequenti cambi di locazione, problemi di sicurezza
- Cambiare gli indirizzi IP?
  - aggiustare l'indirizzo IP di un host dipende dalla locazione corrente
  - è quasi impossibile trovare un sistema mobile, aggiornamenti DNS prendono un tempo troppo lungo
  - le connessioni TCP cadono, problemi di sicurezza

Requisiti

- Trasparenza
  - end system mobili mantengono il loro indirizzo IP
  - è possibile la continuazione della comunicazione dopo l'interruzione del link
  - punto di connessione alla rete fissa può essere cambiato
- Compatibilità
  - supporto degli stessi protocolli di livello 2 di IP
  - non sono richiesti cambiamenti agli end-systems e router correnti
  - end-system mobili possono comunicare con sistemi fissi

- Sicurezza
  - autenticazione di tutti i messaggi di registrazione
- Efficienza e scalabilità
  - richiesti solo piccoli messaggi aggiuntivi al sistema mobile (connessione tipicamente attraverso un link radio a bassa larghezza di banda)
  - supporto world-wide di un gran numero di sistemi mobili nell'intera Internet

Protocolli per la mobilità

- Necessità di un protocollo che permetta connettività di rete da un lato all'altro del movimento di un host
- Un protocollo per la mobilità non deve richiedere cambiamenti massicci al software dei router
- Deve essere compatibile con la grande base installata di networks/hosts IPv4
- Confinare i cambiamenti agli host mobili e a pochi host di supporto

Indirizzi topologicamente corretti

- Per progetto, l'indirizzo IP di un host è legato all'indirizzo di una home network
  - Si assume che gli host siano wired, immobili
  - Router intermedi guardano soltanto all'indirizzo di rete
  - Mobilità senza un cambiamento in indirizzo IP resulta in pacchetti *un-route-able*
- L'indirizzo IP è topologicamente significativo
- Situazione simile a quella telefonica

Perdita delle connessioni

Ogni router inoltra datagrammi confrontando il loro indirizzo IP di destinazione con i subnet prefix nella routing table.

Lo spostamento di un host su un nuovo punto di attacco in una differente subnet non può mantenere le connessioni TCP esistenti.

- Una connessione è identificata da due endpoint di comunicazione, ognuno identificato a sua volta da una coppia <IP, port>.
- Cambiare IP causa la perdita della connessione durante il cambiamento dei punti di attacco.

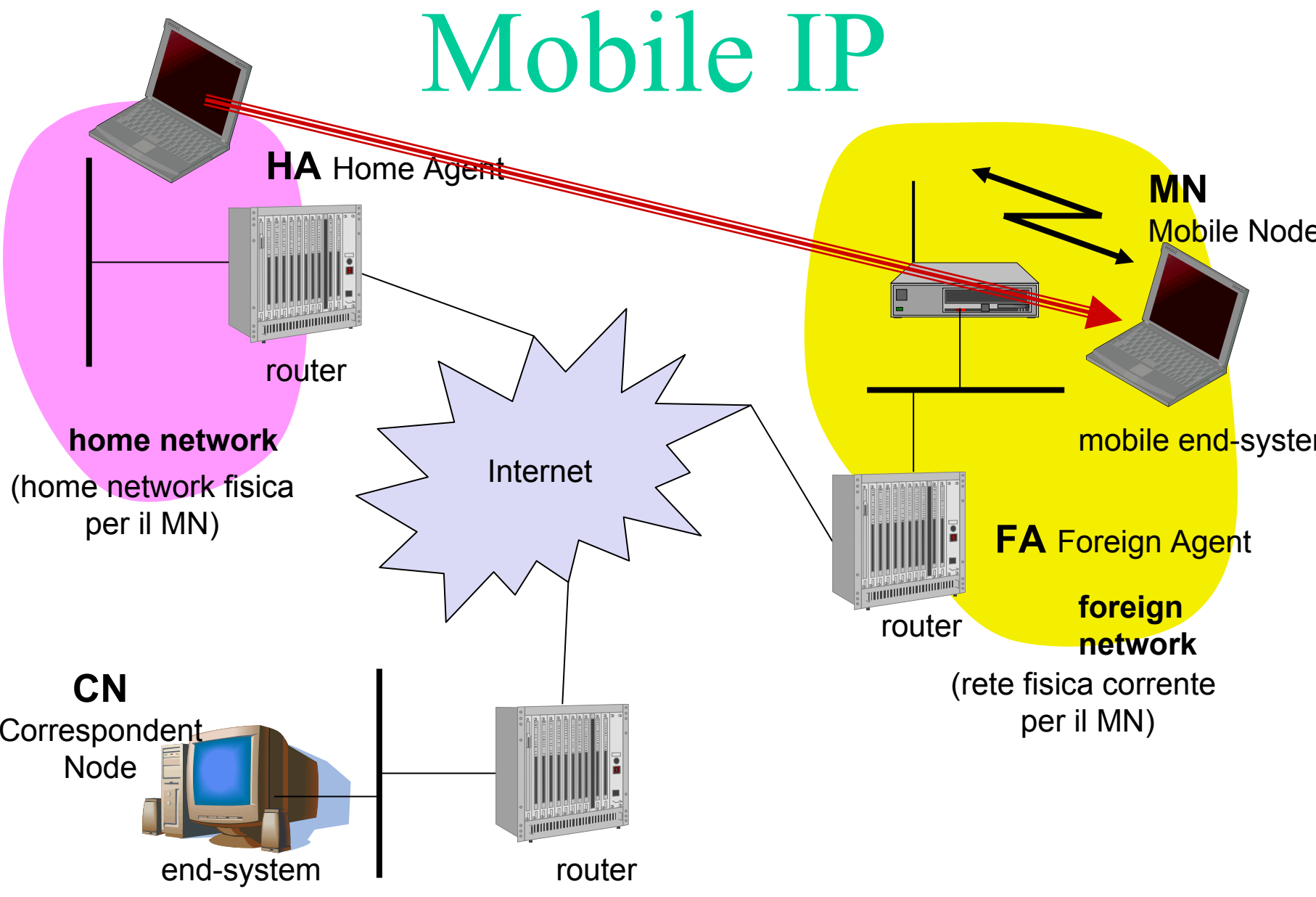
Connettività continua

Mobile IP permette che un host sia raggiungibile sempre allo stesso indirizzo, anche se cambia la sua locazione

- gli fa sembrare una rete come se questa si estendesse sulla intera Internet
- connettività continua, seamless roaming

  anche mentre stanno funzionando le applicazioni
- completamente trasparente all'utente

Mobile IP

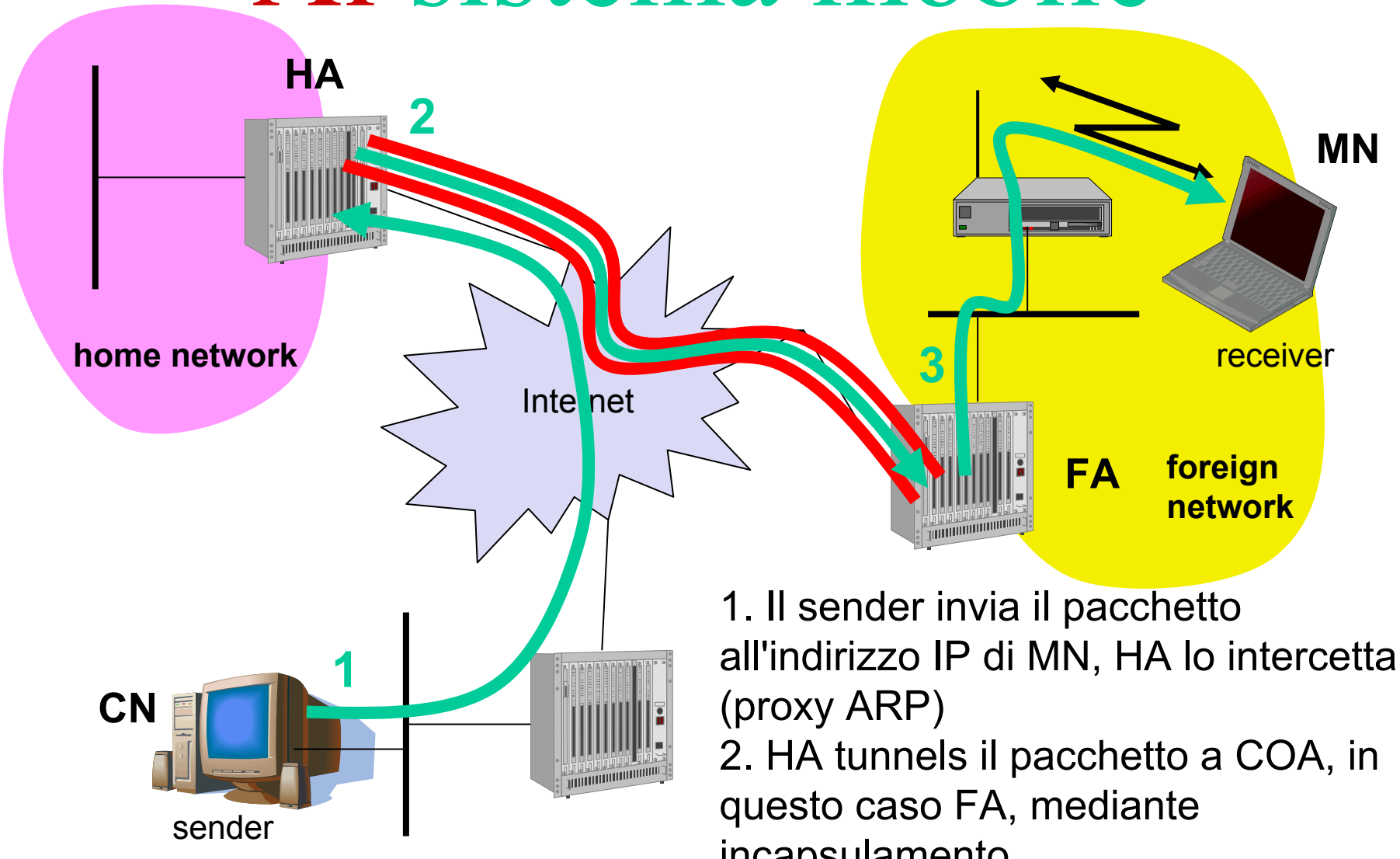

HA Home Agent
router
home network
(home network fisica
per il MN)
Internet
MN
Mobile Node
mobile end-syster
FA Foreign Agent
router
foreign
network
(rete fisica corrente
per il MN)
CN
Correspondent
Node
end-system
router

- Mobile Node (MN)
  - sistema (nodo) che può cambiare il punto di connessione alla rete senza cambiare il suo indirizzo IP
- Home Agent (HA)
  - sistema nella home network del MN, tipicamente un router
  - registra la locazione del MN, tunnels datagrammi IP al COA

- Foreign Agent (FA)
  - sistema nella foreign network corrente del MN, tipicamente un router
  - inoltra i datagrammi tunneled al MN, tipicamente anche il default router per il MN
- Care-of Address (COA)
  - indirizzo del punto di terminazione del tunnel corrente per il MN (al FA o MN)
  - locazione attuale del MN da un punto di vista IP
  - può essere scelto, per es., mediante DHCP, per essere co-locato con MN
- Correspondent Node (CN)
  - communication partner

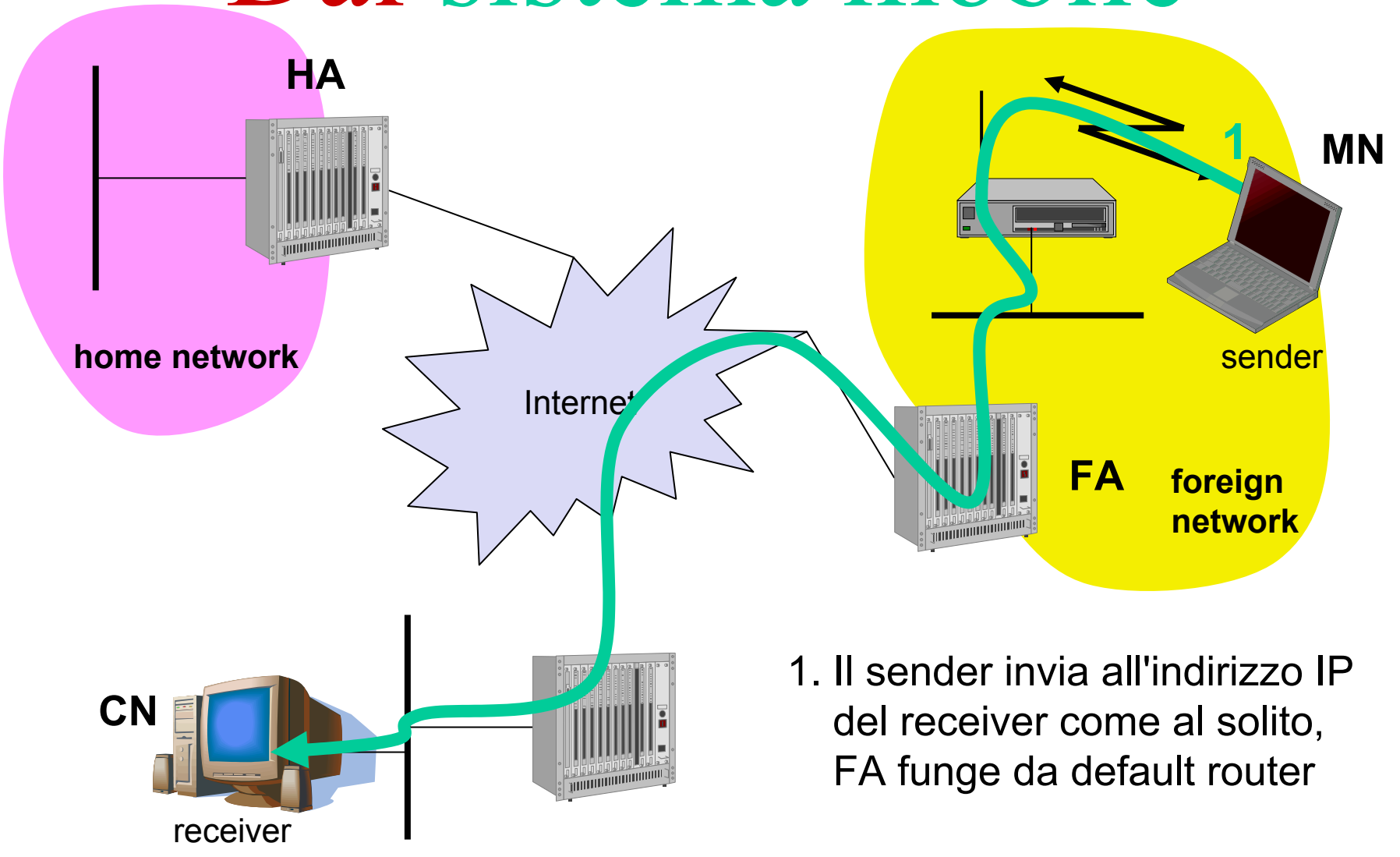
Tunneling

Al sistema mobile

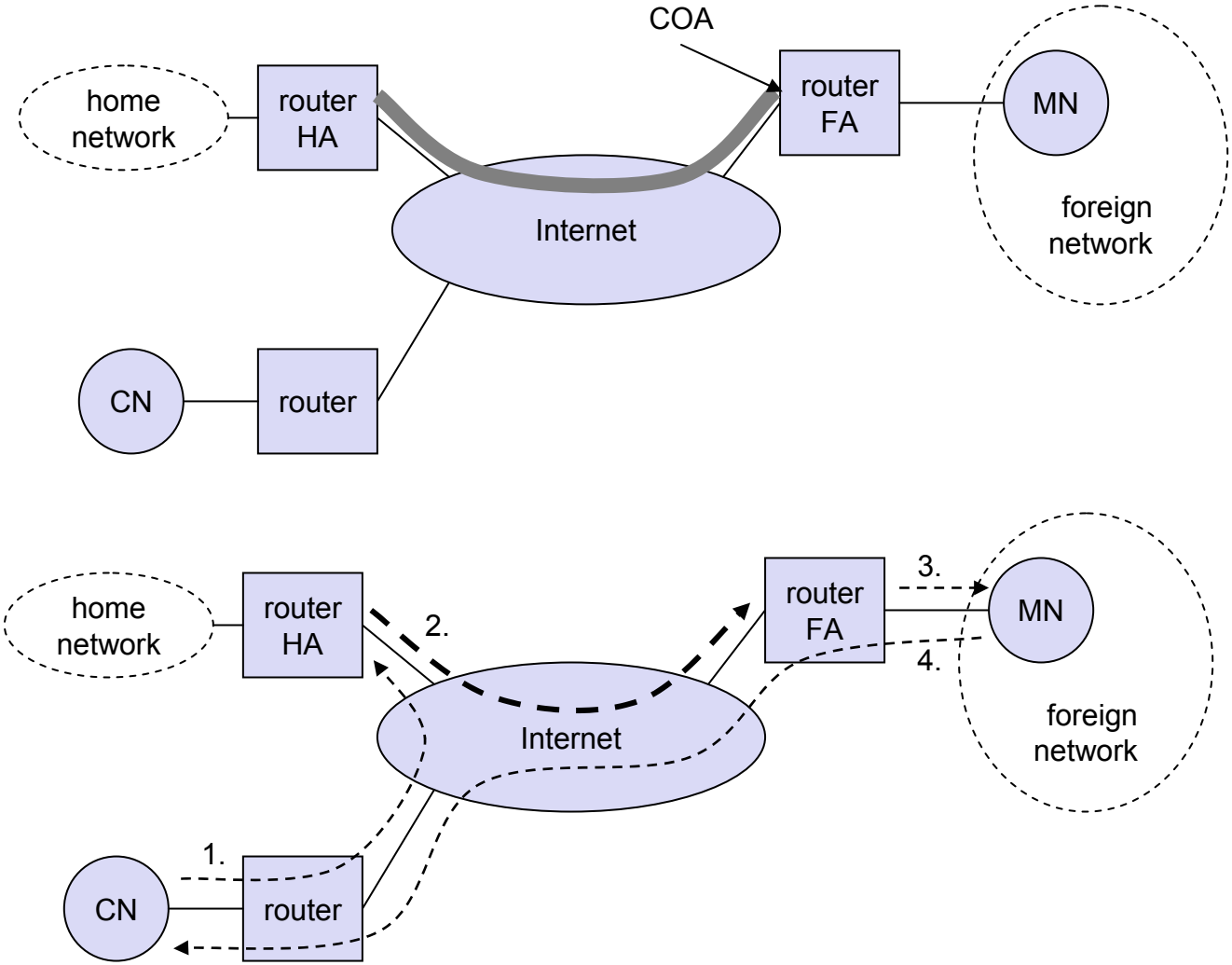


1. Il sender invia il pacchetto all'indirizzo IP di MN, HA lo intercetta (proxy ARP)
2. HA tunnels il pacchetto a COA, in questo caso FA, mediante incapsulamento
3. FA inoltra il pacchetto al MN

Dal sistema mobile



1. Il sender invia all'indirizzo IP del receiver come al solito, FA funge da default router

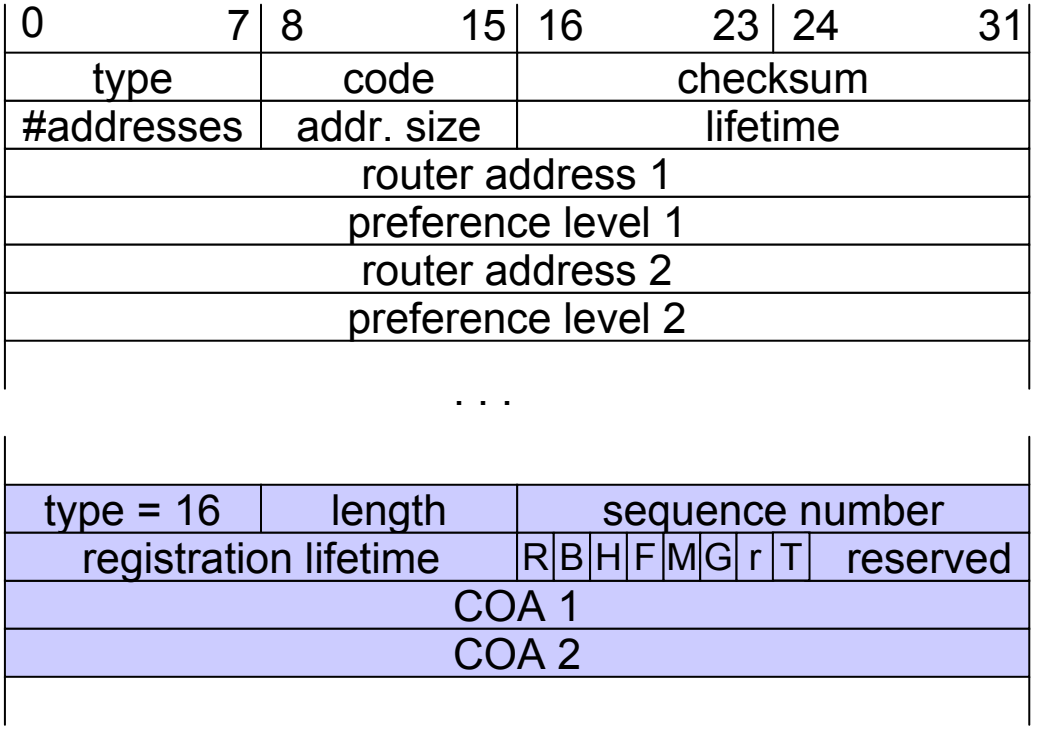

COA
home network
router HA
router FA
MN
Internet
foreign network
CN
router
home network
router HA
2.
router FA
3.
MN
4.
Internet
foreign network
1.
CN
router

Agent Advertisement

- Agent Advertisement
  - HA ed FA (mobility agents) periodicamente inviano messaggi di advertisement nelle loro subnet fisiche
  - MN ascolta questi messaggi e rileva dal network prefix se è nella home o in una foreign network (il caso standard è home network)
  - MN legge un COA dai messaggi di advertisement di FA
  - sono usati messaggi ICMP con alcune estensioni per mobilità

- HA annuncia l'indirizzo IP del MN (come per i sistemi fissi), cioè informazione standard di routing
- i router modificano le loro entries, queste sono stabili per un tempo più lungo del lifetime della registrazione (HA responsabile di un MN per un periodo di tempo più lungo)
- i pacchetti al MN sono mandati al HA,
- indipendente da cambiamenti in COA/FA

type = 9
code = 0 anche traffico non mobile
=16 solo traffico mobile



type = 16
length = 6 + 4 * #COA
sequence number = #advertisements inviati dopo l'inizializzazione
R: è richiesto che la registrazione sia tramite il FA
B: busy, non può accettare registrazioni
H: home agent
F: foreign agent
M: minimal encapsulation
G: GRE encapsulation
r: =0, ignorato
T: FA supporta reverse tunneling
reserved: =0, ignorato

Agent Solicitation

- Se un MN non riceve agent advertisement e non riesce procurarsi un COA con altri mezzi (vedi DHCP), deve mandare degli agent solicitation
- gli MN hanno fretta perchè possono perdere pacchetti
- per evitare flooding della rete, viene ridotta la frequenza di invio
- agent discovery può essere fatta in qualsiasi momento, non solo quando si connette ad una nuova rete, per cercare una migliore connessione

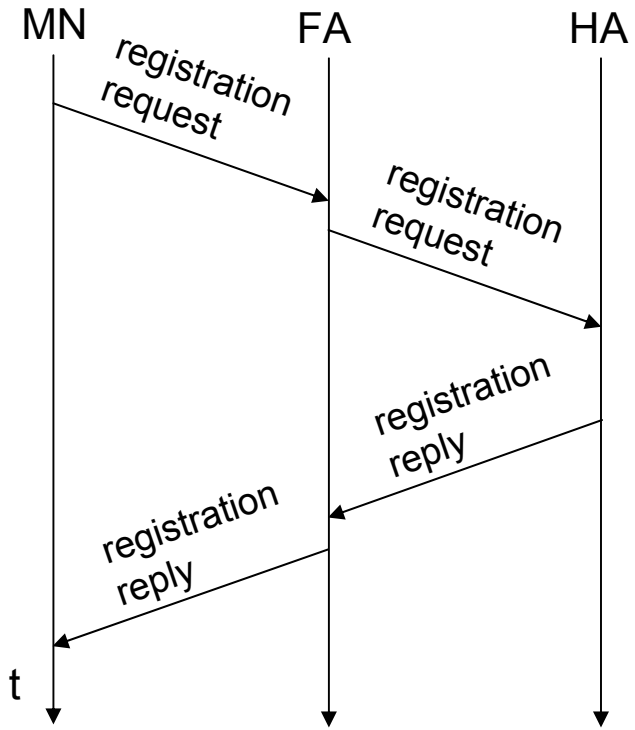
Registration

- Registrazione

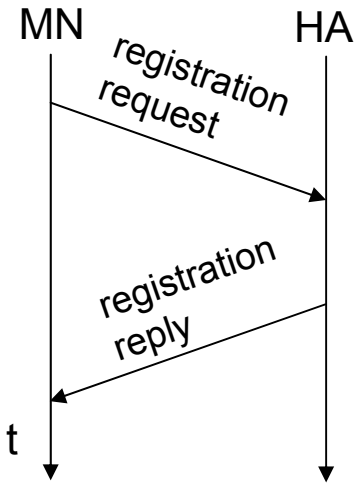
mobility binding : (home address, COA, lifetime)

  - sempre di durata limitata (campo lifetime)
  - MN segnala il COA al HA mediante il FA, HA acknowledges tramite FA al MN
  - queste azioni debbono essere rese sicure mediante autenticazione
  - può registrarsi anche direttamente al HA, se il COA è co-locato ed il bit R in un FA agent advertisement non è impostato ad 1
  - Viene usato UDP (porta 434) per il basso overhead e per le migliori prestazioni rispetto a TCP in ambienti wireless

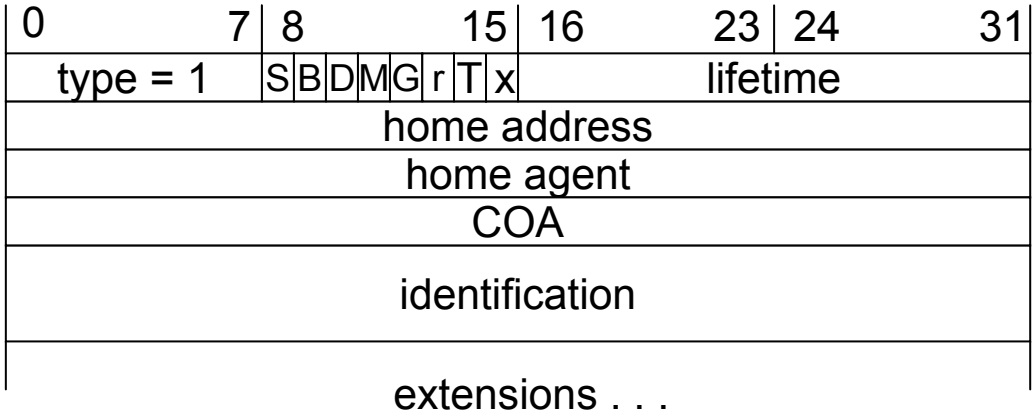
COA al FA:



COA co-locato:

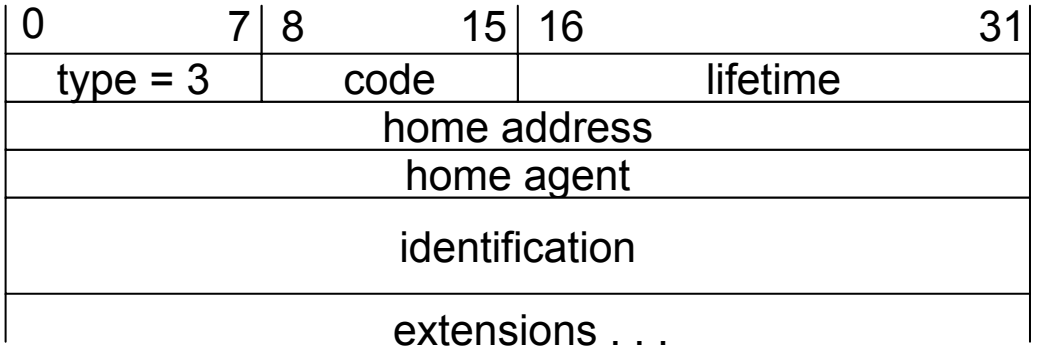


Registration Request



S: simultaneous bindings (mantenga i binding precedenti)
B: vuole ricevere datagrammi broadcast
D: decapsulation da MN (COA co-locato a MN)
M mininal encapsulation
G: GRE encapsulation
r: =0, ignorato
T: reverse tunneling
x: =0, ignorato
lifetime: validità della registrazione in secondi
= 0: deregistrazione
= tutti 1: infinito
identification: per evitare attacchi di replay (lo stesso numero dovrà essere usato da reg reply)
extensions: almeno parametri per autenticazione

Registration Reply



Esempi di ‘code’:

registrazione con successo

0 registrazione accettata

1 registrazione accettata, ma non è supportato bindings simultanei

registrazione negata da FA

65 proibita amministrativamente

66 risorse insufficienti

67 fallita autenticazione di MN

68 fallita autenticazione di HA

69 Lifetime richiesta troppo lunga

registrazione negata da HA

129 proibita amministrativamente

131 fallita autenticazione di MN

133 disaccordo sul valore di Identification di reg req

135 troppi bindings simultanei

Bindings simultanei

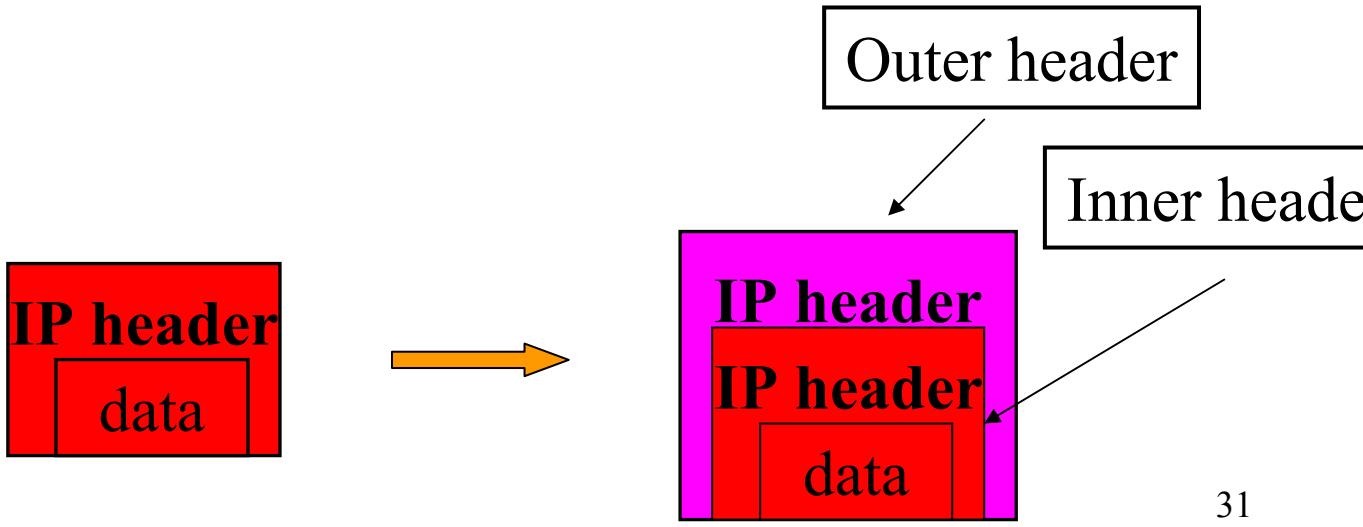
- Un Mobile Node può registrare multipli bindings simultaneamente
- Home Agent fa copie multiple dei pacchetti destinati al mobile host, e ne invia una copia tramite tunnel a ciascun care-of address
- Bindings simultanei possono essere usati per
  - facilitare seamless hand-off
  - evitare registrazioni troppo frequenti

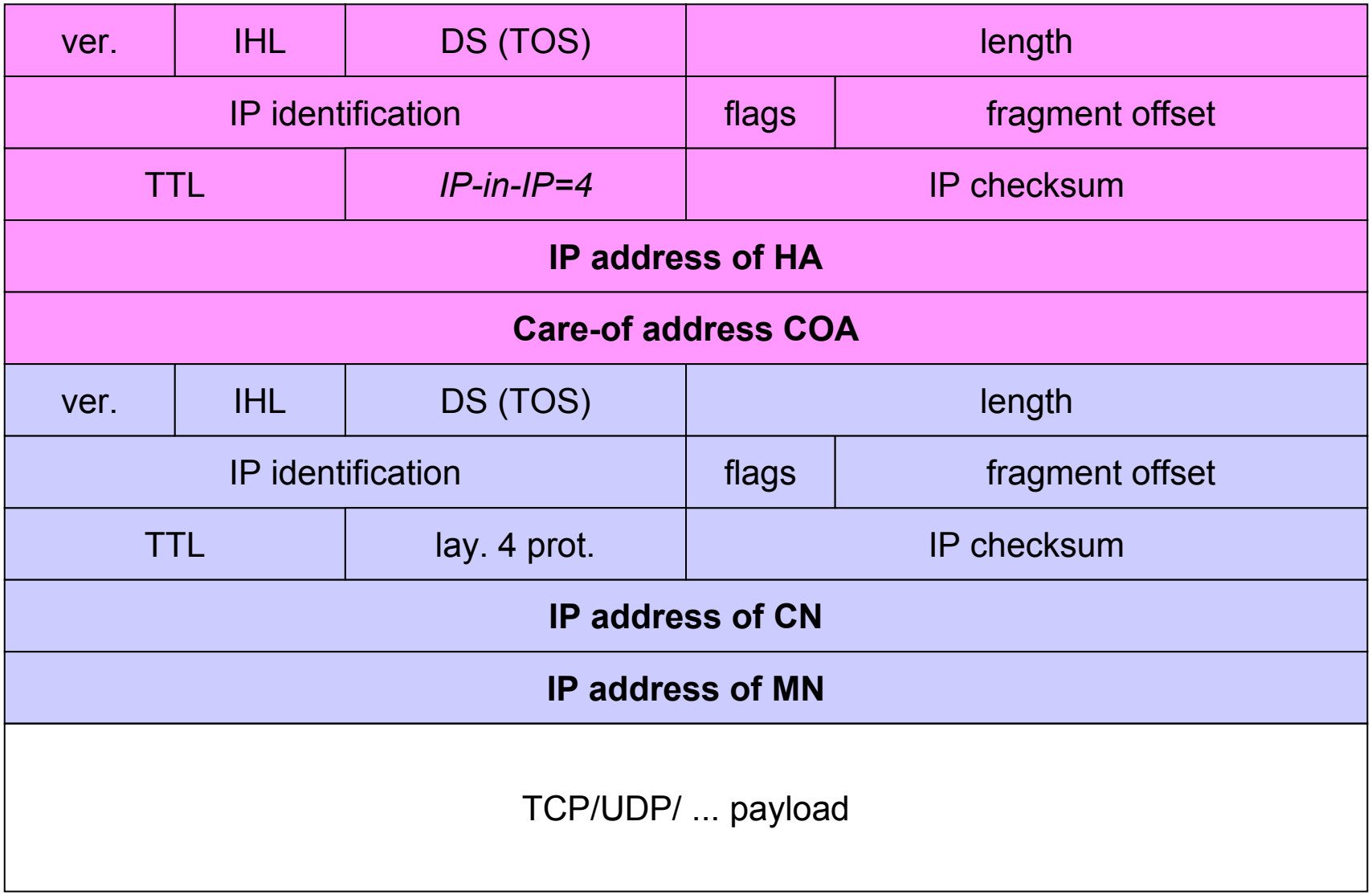
IP-in-IP Encapsulation

IP-in-IP-Encapsulation

- Incapsulamento di un pacchetto in un altro come payload
  - per es. IPv6 in IPv4 (6Bone), Multicast in Unicast (Mbone)
  - qui: IP-in-IP-encapsulation, minimal encapsulation
- IP-in-IP-encapsulation
  - tunnel tra HA e COA

- Nel nuovo header:
  - Destination = care-of-address
  - Source = indirizzo del home agent
  - Protocol number = IP-in-IP = 4
  - TTL abbastanza alto da poter raggiungere la fine del tunnel



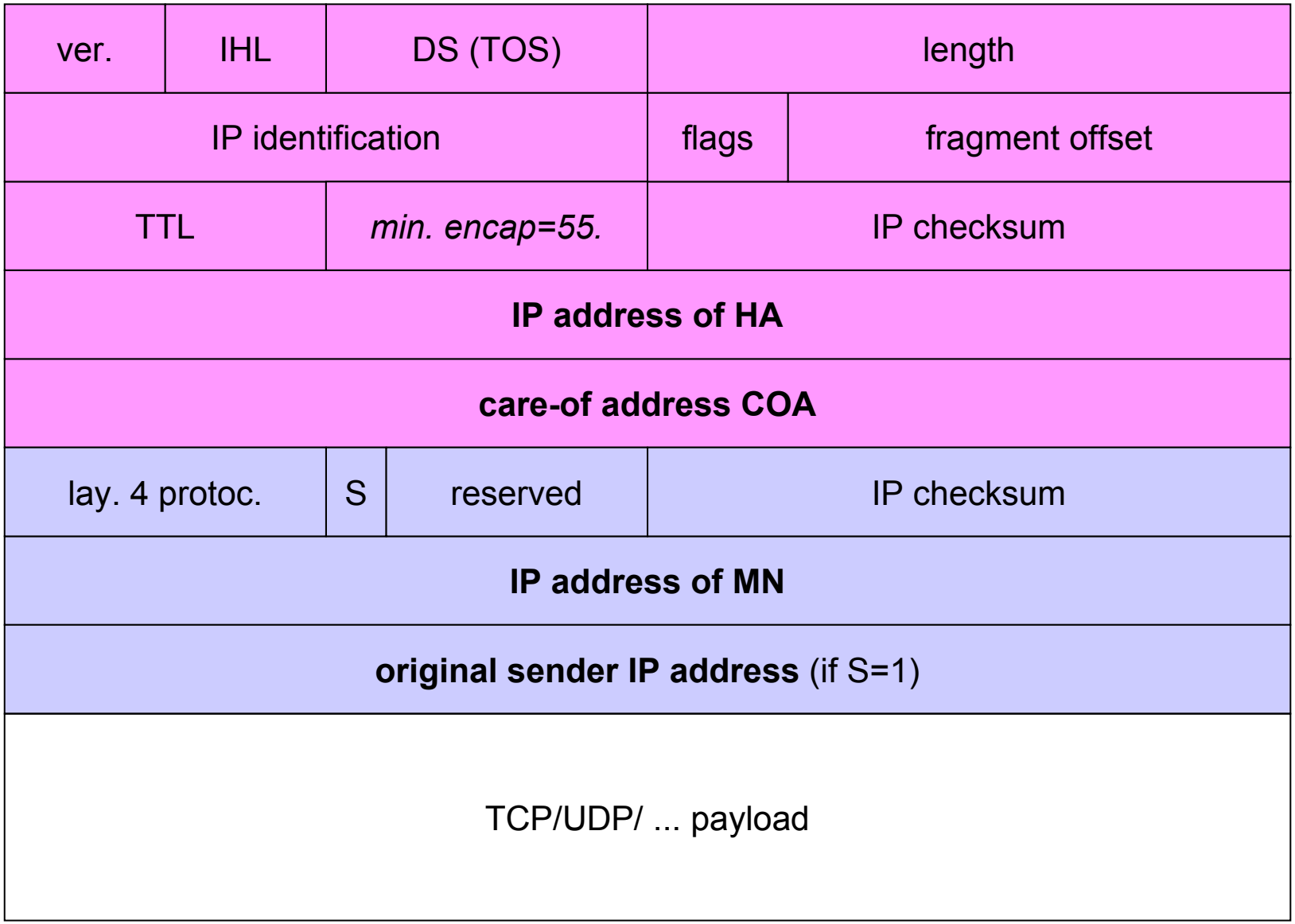


TTL, nel inner header, è posto uguale al TTL prima di entrare nel tunnel, decrementato di 1, poichè il tunnel visto come un singolo hop dal pacchetto (MN si comporta come se fosse attaccato alla home network)

Minimal Encapsulation

Minimal Encapsulation

- Minimal encapsulation (opzionale)
  - evita la ripetizione di campi identici
  - per es. IHL, version, DS (il vecchio TOS)
  - è applicabile soltanto a pacchetti non frammentati, non è lasciato spazio per identificazione dei frammenti


ver.
IHL
DS (TOS)
length
IP identification
flags
fragment offset
TTL
min. encap=55.
IP checksum
IP address of HA
care-of address COA
lay. 4 protoc.
S
reserved
IP checksum
IP address of MN
original sender IP address (if S=1)
TCP/UDP/ ... payload

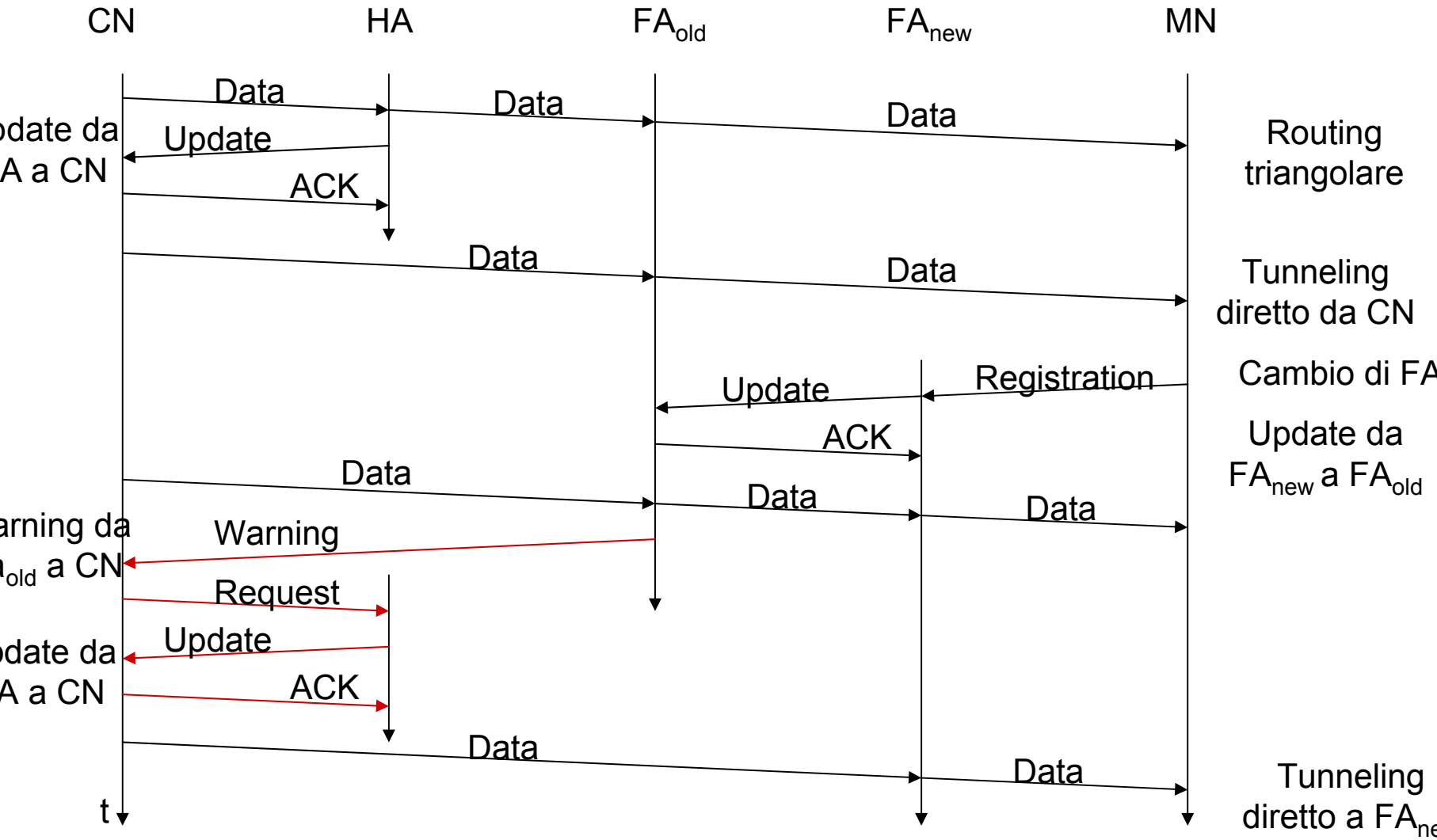
Ottimizzazioni

Tunneling Diretto

- Routing triangolare
  - il CN invia tutti i pacchetti ad MN tramite HA
  - carico della rete e latenza maggiori
- “Soluzioni”
  - il CN impara la locazione corrente di MN e la memorizza in una binding cache che è parte della routing table locale del CN
  - tunneling diretto a questa locazione
  - HA informa un sender circa la locazione di MN
  - grossi problemi di sicurezza!

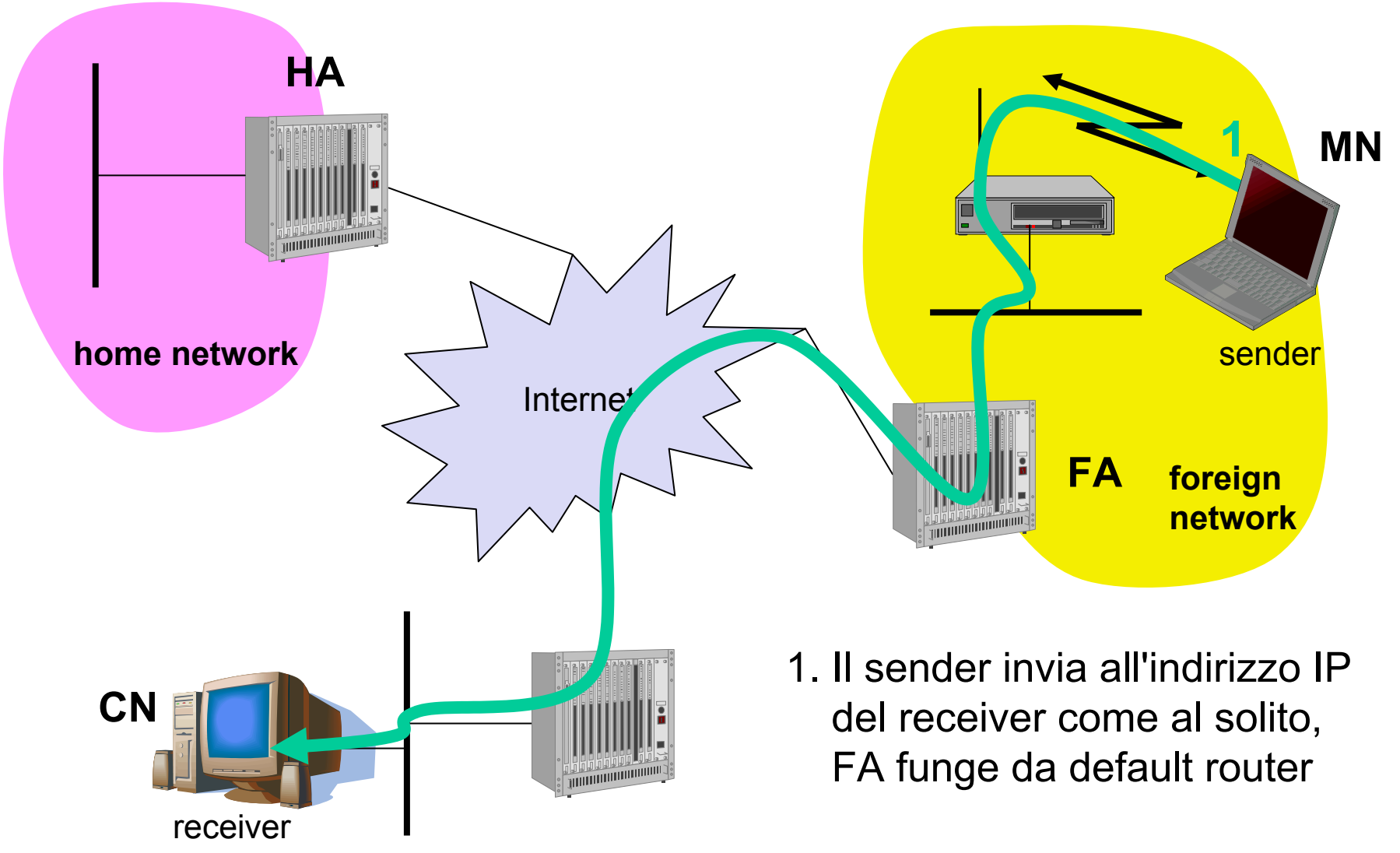
Cambio di FA
Smooth Handover

- Cambio di FA
  - pacchetti in volo durante il cambiamento possono essere persi
  - il nuovo FA informa il vecchio FA per evitare perdite di pacchetti, il vecchio FA ora inoltra i rimanenti pacchetti al nuovo FA (smooth handover)
  - questa informazione consente anche al vecchio FA di rilasciare le risorse per il MN


CN
HA
FA_old
FA_new
MN
Data
Data
Data
odate da
A a CN
Update
ACK
Routing
triangolare
Data
Data
Tunneling
diretto da CN
Update
Registration
Cambio di FA
ACK
Update da
FA_new a FA_old
Data
Data
Data
arning da
a_old a CN
Warning
Request
Update
odate da
A a CN
ACK
Data
Data
Tunneling
diretto a FA_ne
t

Reverse Tunneling

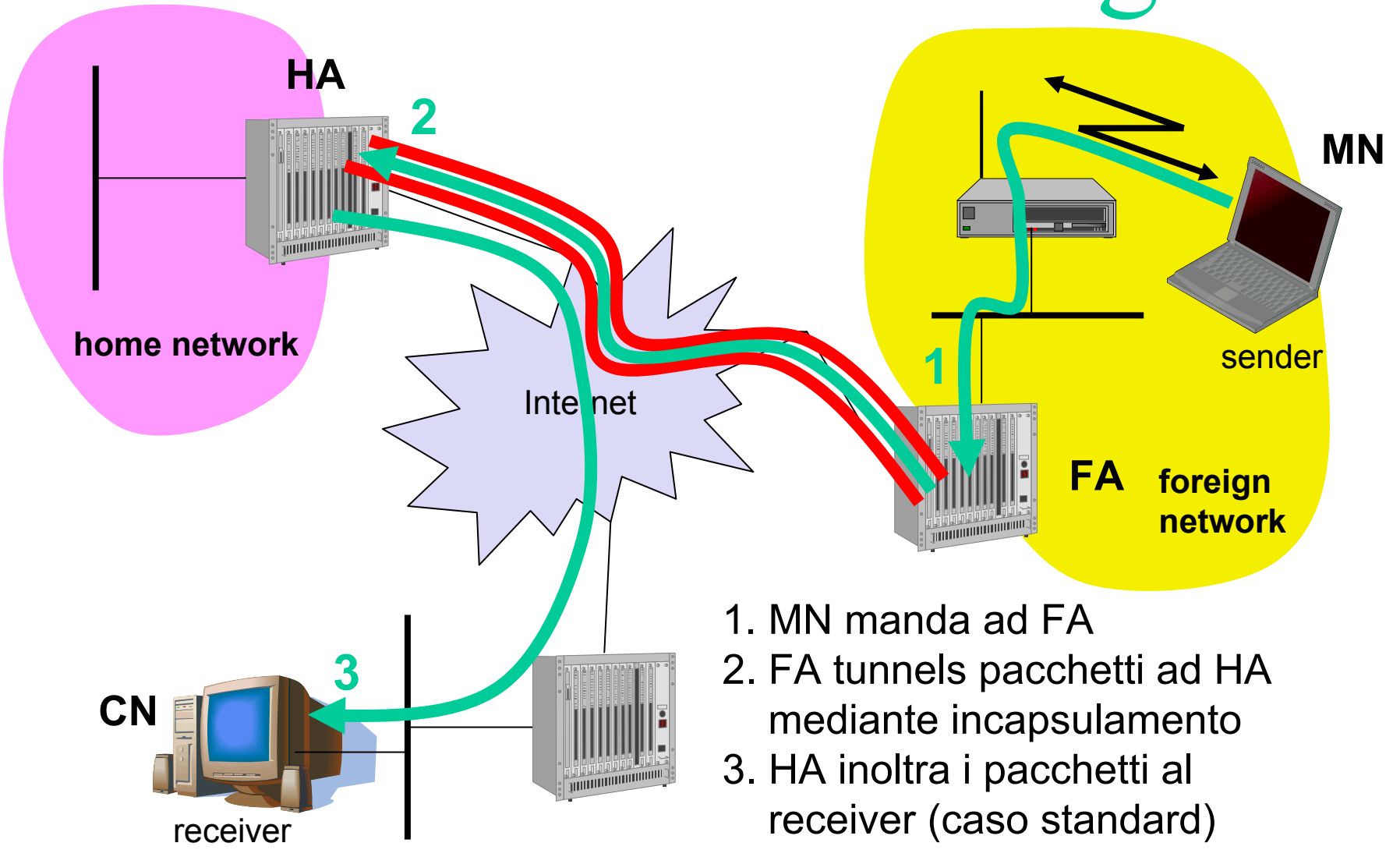
Dal sistema mobile



1. Il sender invia all'indirizzo IP del receiver come al solito, FA funge da default router

- I router spesso accettano soltanto indirizzi “topologicamente corretti“ (firewall!)
  - un MN non ha un indirizzo topologicamente corretto se è in una foreign network: un firewall non lascerà passare pacchetti in uscita generati da MN
  - se un MN, residente in una foreign network, invia un pacchetto alla sua home network, ed essa ha un firewall, questo lo filtrerà poichè un pacchetto proveniente dall’esterno ha un indirizzo sorgente che appartiene alla rete interna
  - un pacchetto da MN incapsulato da FA è topologicamente corretto
  - il reverse tunneling risolve, inoltre, problemi di multicast (la foreign network può non avere l’infrastruttura per effettuare multicasting) e di TTL (TTL nella home network è corretto, ma se MN si sposta può non essere sufficiente, mentre un tunnel conta solo un hop)

Reverse tunneling



1. MN manda ad FA
2. FA tunnels pacchetti ad HA mediante incapsulamento
3. HA inoltra i pacchetti al receiver (caso standard)

- Reverse tunneling
  - crea ora problemi di routing triangolare nella direzione inversa (CN potrebbe essere un nodo tradizionale, non mobile nè in grado di decapsulare: vedi compatibilità)
  - non risolve problemi con i *firewall*, il reverse tunnel può essere usato per aggirare meccanismi di sicurezza (tunnel hijacking)
- Lo standard è compatibile backwards
  - le estensioni possono essere implementate facilmente e cooperano con le implementazioni correnti che non hanno di queste estensioni