



**La Sapienza**

Università degli Studi di Roma

Dipartimento di Informatica e Sistemistica

# RETI DI CALCOLATORI II

## Mobile IP

**Emiliano Trevisani**

**[trevisani@dis.uniroma1.it](mailto:trevisani@dis.uniroma1.it)**

**A.A. 2008/2009**

# Host mobili

- Dispositivi wireless o wired mobili
- Connessione alla rete attraverso:
  - Wireless LAN
  - Reti cellulari
  - Reti Satellitari
  - LAN
  - ....
- Una rete di riferimento fornisce connettività IP
- IP mobility considera la mobilità tra reti diverse

# Alternative ovvie

## 1. Modificare l'indirizzo IP dell'host:

- Implica il reboot e la perdita delle connessioni a livello di trasporto

## 2. Propagare informazioni di instradamento basate sull'host

- Richiede tabelle di instradamento di dimensione pari al numero degli host

# Requisiti

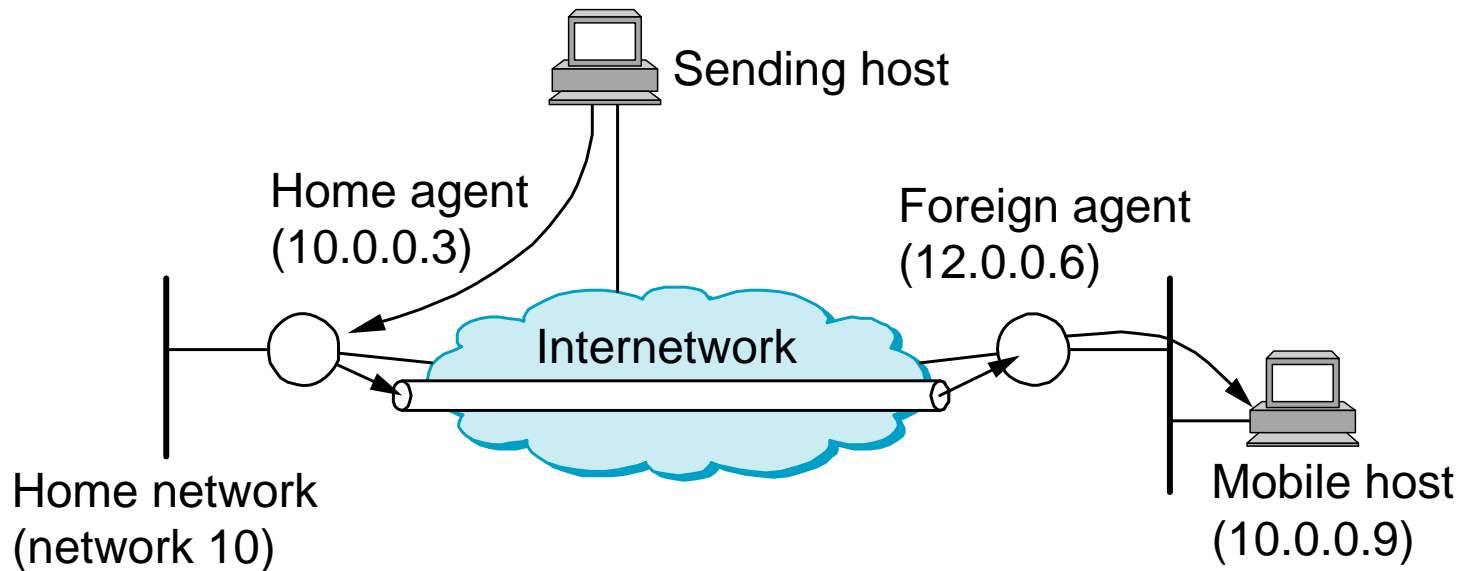
- “Connectivity anytime anywhere...”
- Nessuna modifica al SW dei sistemi fissi
- Movimento dell’host mobile trasparente rispetto all’applicazione remota
  - Es. le connessioni TCP persistono
  - Conseguenza: indirizzo IP fisso o soluzione equivalente

# Caratteristiche di Mobile IP

- Trasparente alle applicazioni ed ai protocolli di trasporto
  - Assunzione: host mobile ha un indirizzo permanente
  - Host mantiene indirizzo quando in movimento
- Interoperabilità con lo standard IPv4
- Scalabilità
- Sicurezza, autenticazione di host mobili al di fuori della rete di riferimento
- Macro mobilità (possibilità di lavorare al di fuori della propria rete di riferimento)

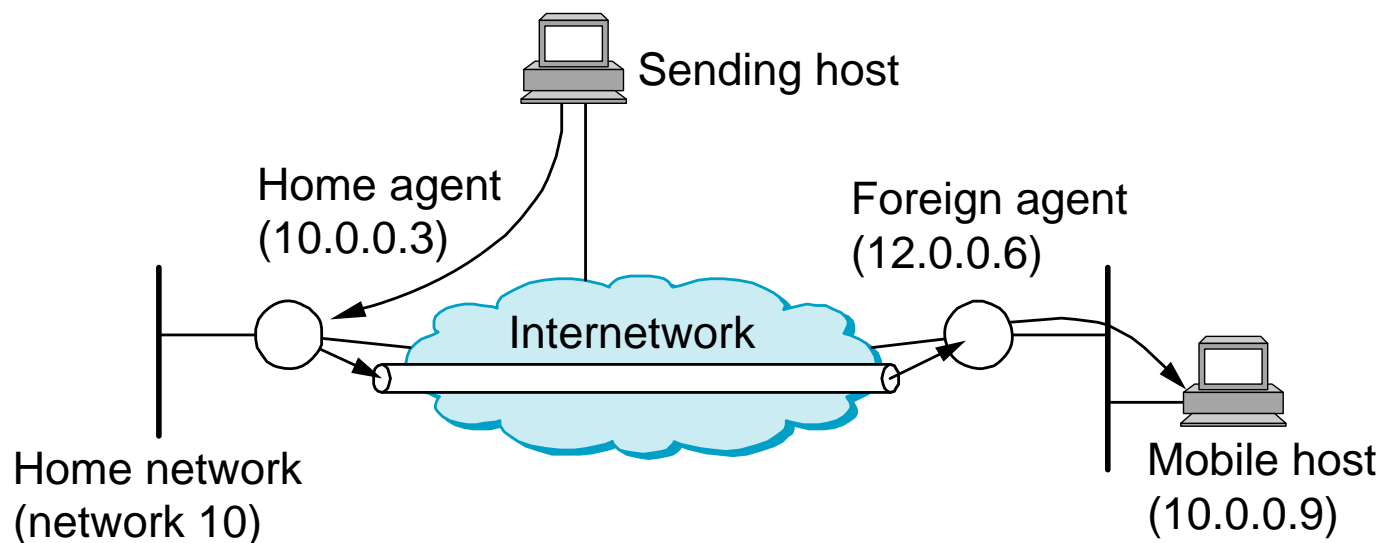
# Approccio generale

- Host mobile ha un *home address*
  - Home network
  - Home agent -> deve implementare nuove funzionalità
- Altri host inviano pacchetti all'home address
  - L'host mobile appare conservare il proprio indirizzo



# Approccio generale/cont.

- Spesso presente un *foreign agent*
  - Router della rete nella quale si trova temporaneamente l'host mobile
- Home e foreign agent inviano periodicamente messaggi che annunciano la loro presenza
  - Tali messaggi possono essere spediti su richiesta esplicita dell' host mobile



# Resto della lezione

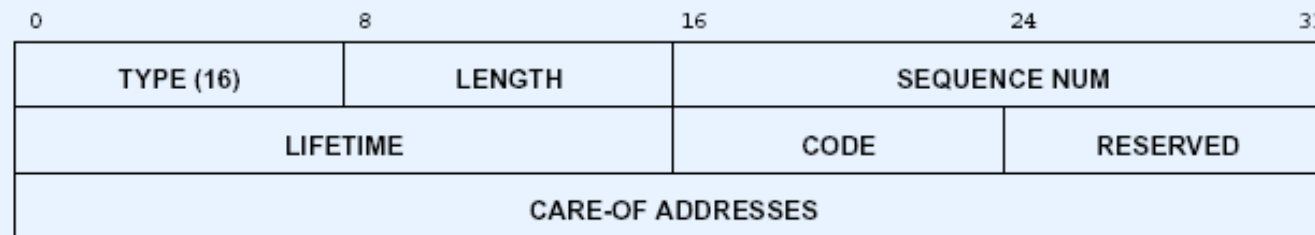
- Move detection
- Mobility agent advertisements
- Indirizzo dell'host mobile
- Registrazione
  - Foreign agent
  - Home agent
- Spedizione/ricezione pacchetti
  - Tunneling

# Move detection

- Riconoscimento ingresso in una nuova rete (o ritorno nella propria)
- Tecniche simili a quelle usate nella telefonia cellulare
- Nodi opportuni della rete (es. i foreign agent stessi o nodi equivalenti) annunciano periodicamente la propria presenza agli utenti mobili in transito
- Ogni nodo mobile che riceve un annuncio dal suo foreign agent inizializza un timer
- Scaduto il timer assume di aver perso contatto con la rete
- Se nel frattempo ha ricevuto annunci da un altro agente può tentare di registrarsi presso di esso

# Mobility agent advertisement

- Usa ICMP *router discovery*
  - Inviato periodicamente da foreign o home agent
  - Può essere sollecitato con ICMP *router solicitation*
- Extension mobility a ICMP router discovery
- Identificato dalla maggiore lunghezza del messaggio ICMP



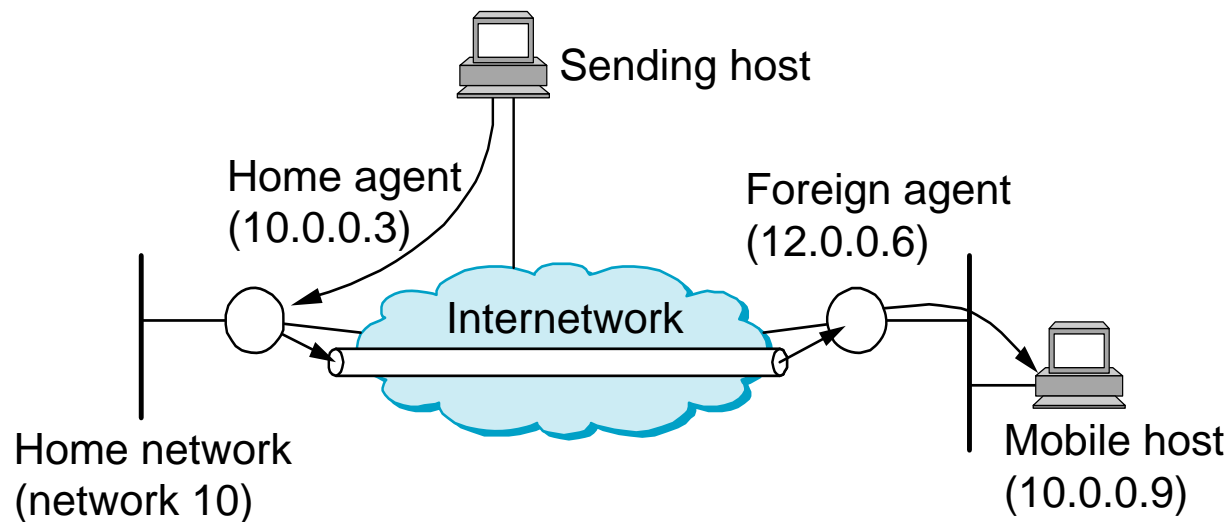
# Mobility agent advertisement

- Lifetime: tempo massimo di attesa per accettare richieste di registrazione
- Sequence number: permette di associare richieste e risposte
- Code:

Bit	Meaning
0	Registration with an agent is required; co-located care-of addressing is not permitted
1	The agent is busy and is not accepting registrations
2	Agent functions as a home agent
3	Agent functions as a foreign agent
4	Agent uses minimal encapsulation
5	Agent uses GRE-style encapsulation†
6	Agent supports header compression when communicating with mobile
7	Unused (must be zero)

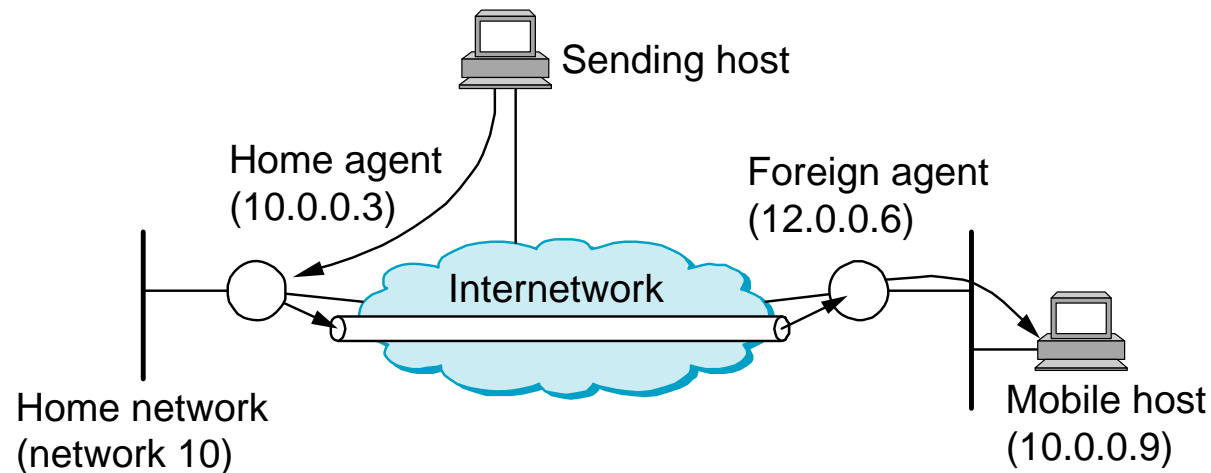
# Indirizzo/Care-of-Address

- Presenza di un *foreign agent*
- Host mobile si registra presso il foreign agent
- Host mobile ottiene un care-of-address



# Indirizzo/Co-located Address

- Rete foreign non prevede un *foreign agent*
- Host usa DHCP per ottenere un co-located address temporaneo
  - Pool di indirizzi riservati agli host mobili
- Host si registra direttamente presso l'home agent
  - Host gestisce la mobilità direttamente

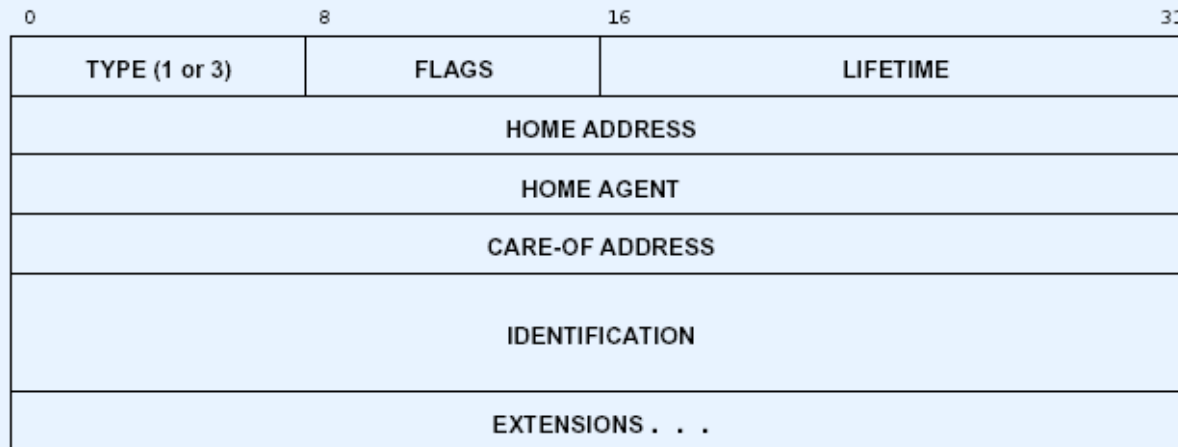


# Registrazione

- Host usa un care-of-address:
  - Registrazione presso il foreign agent
  - Foreign agent inoltra registrazione a home agent
  - Host conosce indirizzo del proprio home agent
  - Comunicazione tra host e foreign agent a livello link
- Host usa co-located address
  - Registrazione diretta presso l'home agent a meno che
    - Foreign agent presente e bit R a 1 (registration required) in mobility agent advertisement
    - Opzione usata per motivi di controllo e contabilita'
    - In tal caso c'e' un foreign agent ma esso e' usato per i motivi sopra citati e non per assegnare un care-of-address

# Registrazione

- Inviati attraverso UDP (porta 434)
- Type: request o reply
- LIFETIME: care-of address mantenuto nella binding-cache finché il LIFETIME scade.



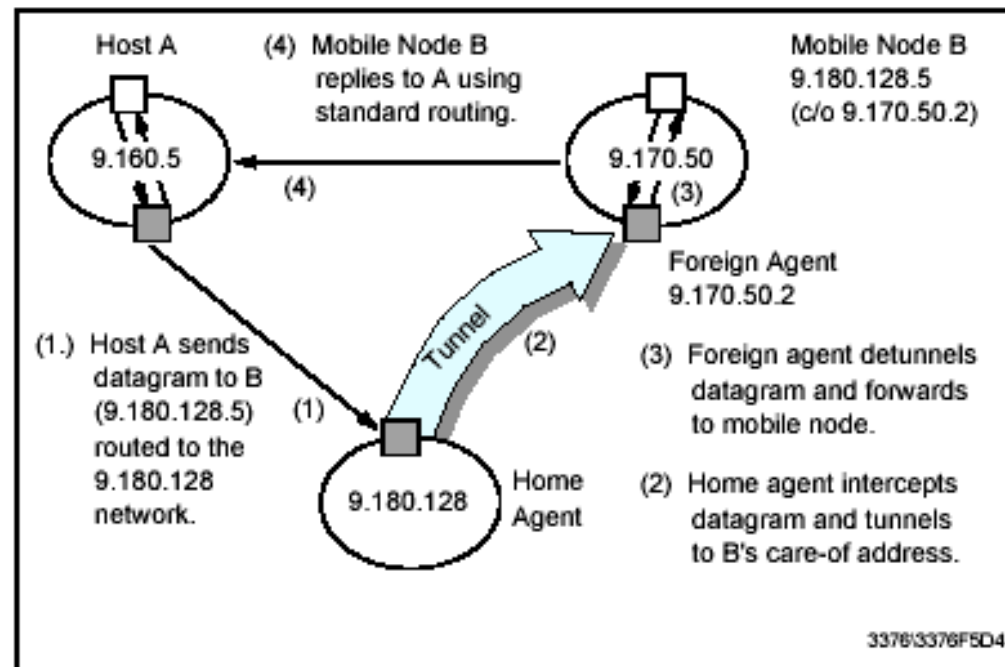
# Registrazione

- HOME ADDRESS, HOME AGENT, CARE-OF-ADDRESS: indirizzi e home agent dell'host mobile, indirizzo da usare per il tunneling
- IDENTIFICATION: corrispondenza tra richieste e risposte
- FLAGS: specifiche dell'inoltro da parte dell'HOME AGENT

Bit	Meaning
0	This is a simultaneous (additional) address rather than a replacement.
1	Mobile requests home agent to tunnel a copy of each broadcast datagram
2	Mobile is using a co-located care-of address and will decapsulate datagrams itself
3	Mobile requests agent to use minimal encapsulation
4	Mobile requests agent to use GRE encapsulation
5	Mobile requests header compression
6-7	Reserved (must be zero)

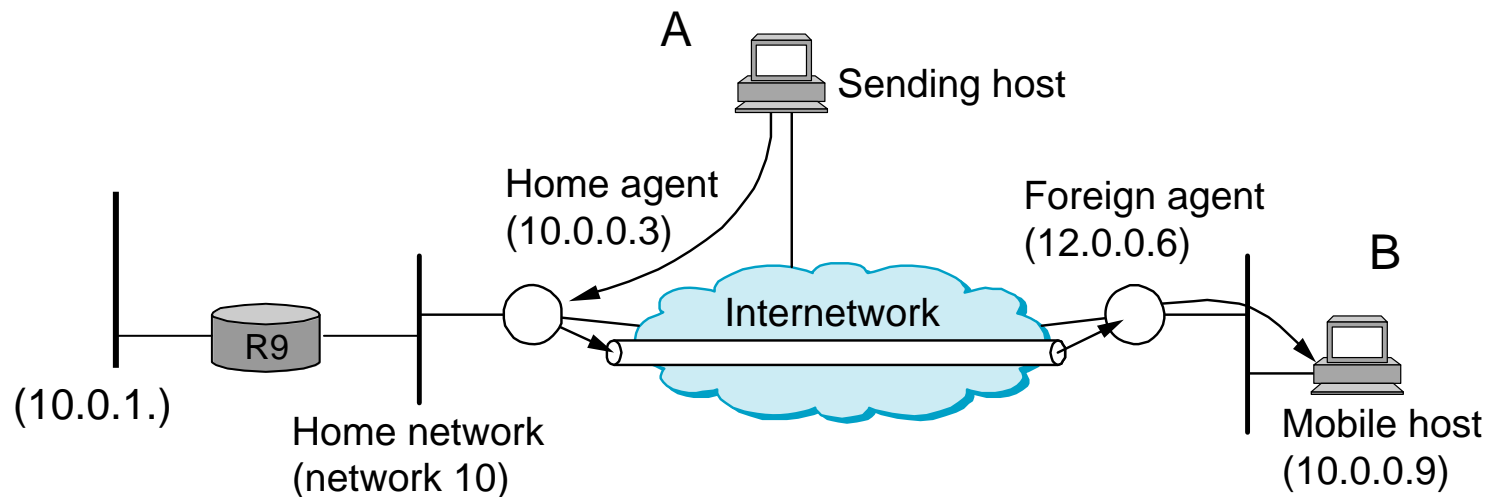
# Ricezione pacchetti

- Host A invia pacchetto a host mobile B su foreign network
- A spedisce pacchetto a home agent di B
- Tunnel tra home agent e foreign agent



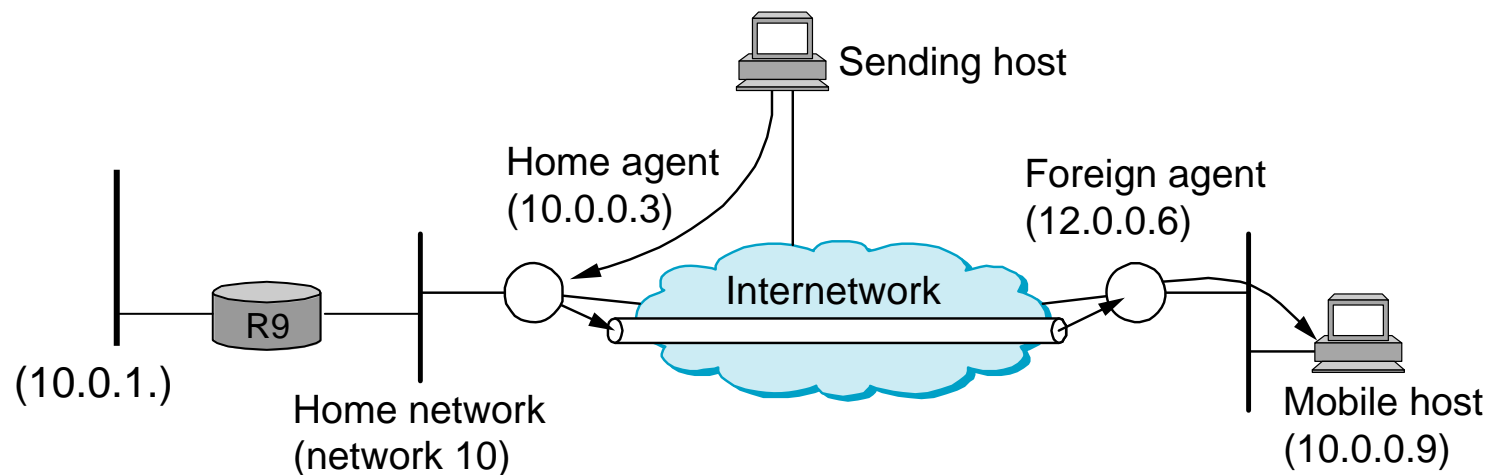
# Ricezione pacchetti/cont.

- Problemi:
  - Host A appartiene alla home network su cui si trova B
    - In tal caso il pacchetto normalmente non attraversa router
  - La home network di B contiene altri router oltre all'home agent
    - B appartiene alla sottorete 10.0.1/ mentre l'home agent della rete 10.0/ appartiene alla sottorete 10.0.0/
    - R9 potrebbe tentare di instradare i pacchetti diretti a B



# Ricezione pacchetti/cont.

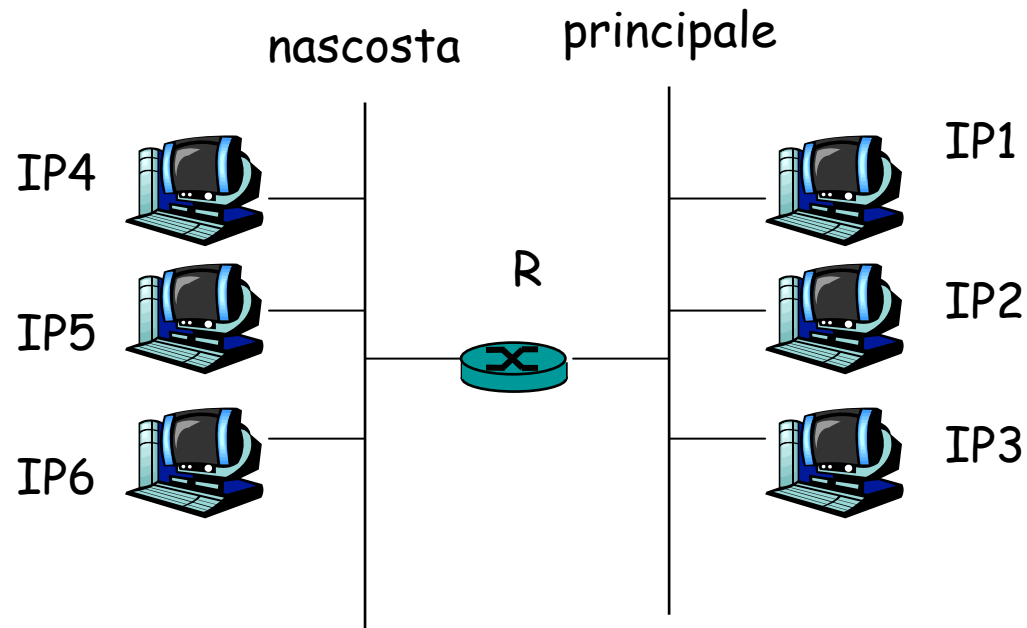
- Soluzione: ARP proxy
  - Home agent associa indirizzo IP di B alla propria interfaccia fisica verso la rete interna
  - Home agent invia un messaggio ARP (gratuitous ARP) con l'associazione appena B si registra attraverso il foreign agent
    - In tal modo vengono aggiornate le cache contenenti eventuali associazioni per l'indirizzo di B



# ARP proxy (promiscuo, hack)

- Permette di definire più reti locali
  - Rete principale nota all'esterno
  - Reti locali aggiunte successivamente nascoste
- Router speciale che:
  - Funziona da switch tra le diverse reti locali
  - Funziona da router da/verso l'esterno
- I router ignorano la presenza di subnet fisicamente distinte

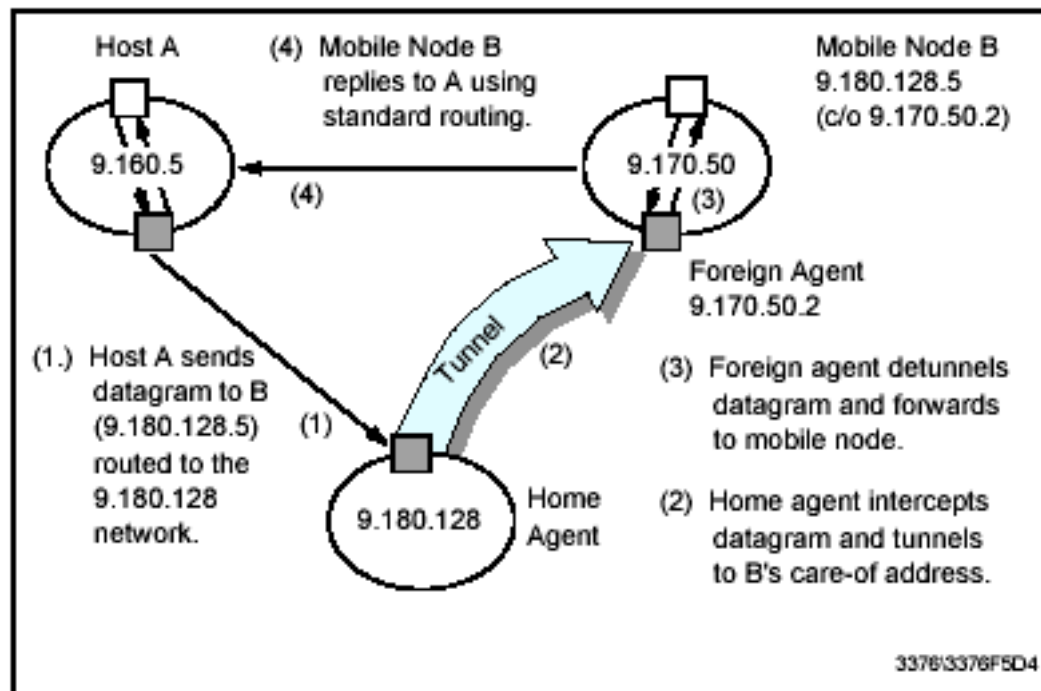
# ARP proxy - cont.



- Datagram  $IP1 \Rightarrow IP4$ 
  - R cattura richiesta ARP bcast di H1 e restituisce proprio MAC address
  - Datagrammi da IP1 a IP4 sono spediti a R che li inoltra a IP4

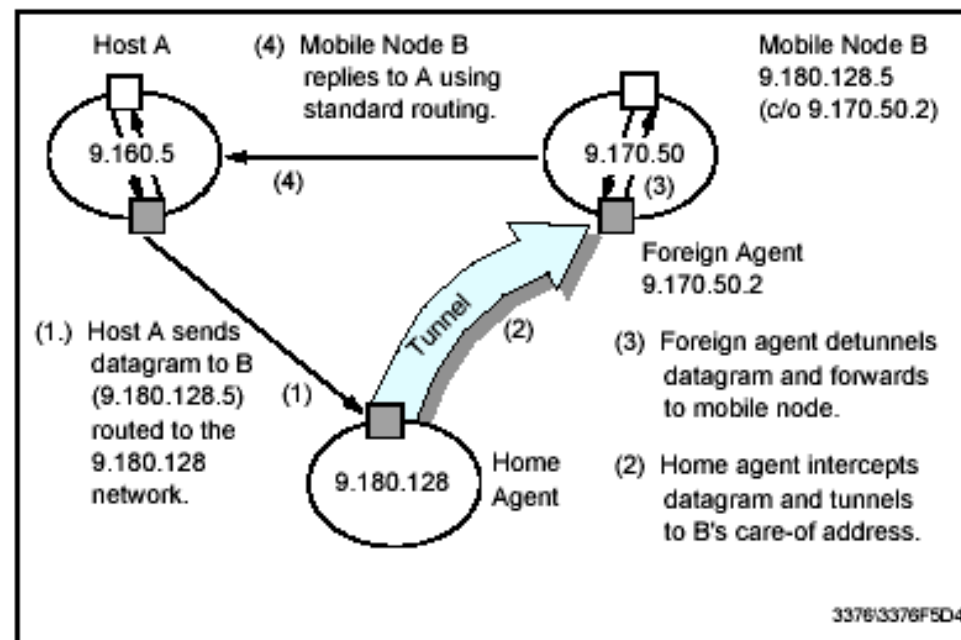
# Spedizione pacchetti

- Host B replica ad A usando instradamento standard



# Instradamento

- Instradamento verso l'host mobile deve necessariamente passare attraverso home agent
- Particolarmente inefficiente se l'host destinazione è vicino all'host mobile (*triangle routing problem*)



# Instradamento

- E' possibile propagare informazioni di instradamento specifiche dell'host
- Viene realizzato solo per reti che interagiscono significativamente con l'host mobile
- Occorre rimuovere queste informazioni quando l'host si sposta su un'altra rete.

# Sicurezza in IP mobility

- Chiave di sessione con il router locale
  - Centro di distribuzione delle chiavi
  - Diffie-Hellman per cambiare la chiave
- Autenticazione richiesta tra l'home agent e l'host mobile
  - Algoritmo di default è MD5
  - Chiavi di 128 bit
  - Foreign agent deve supportare autenticazione attraverso questo metodo
- Altri algoritmi possono essere applicati

# Altre questioni riguardanti la sicurezza

- Tunneling del traffico verso l'host mobile dall'home agent al rispettivo care-of-address
- ARP non è autenticato
- La comunicazione tra foreign e home agent deve essere assicurata per evitare uso illegale

# Problematiche

- Inefficienza nell'instradamento
- Sicurezza: Esigenza di rendere IP mobile deve convivere con le esigenze di sicurezza
- Firewall: provocano difficoltà poiché bloccano i pacchetti in entrata che non soddisfano determinati criteri
  - Messaggi di registrazione usano UDP
- Trasparenza: Opinioni discordi sulla necessità della sopravvivenza delle connessioni TCP agli spostamenti dell'host

# Riferimenti

- Rif. 1, cap. 4
- Rif. 4, cap. 19
- White paper CISCO:
  - [http://www.cisco.com/en/US/tech/tk827/tk369/technologies\\_white\\_paper09186a00800c9906.shtml](http://www.cisco.com/en/US/tech/tk827/tk369/technologies_white_paper09186a00800c9906.shtml)
- Nota: tutti i riferimenti dati costituiscono materiale integrante del corso