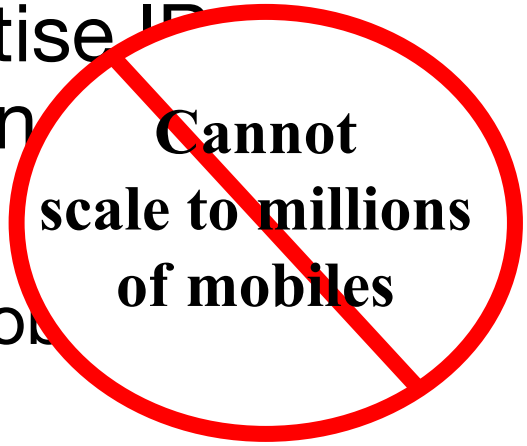
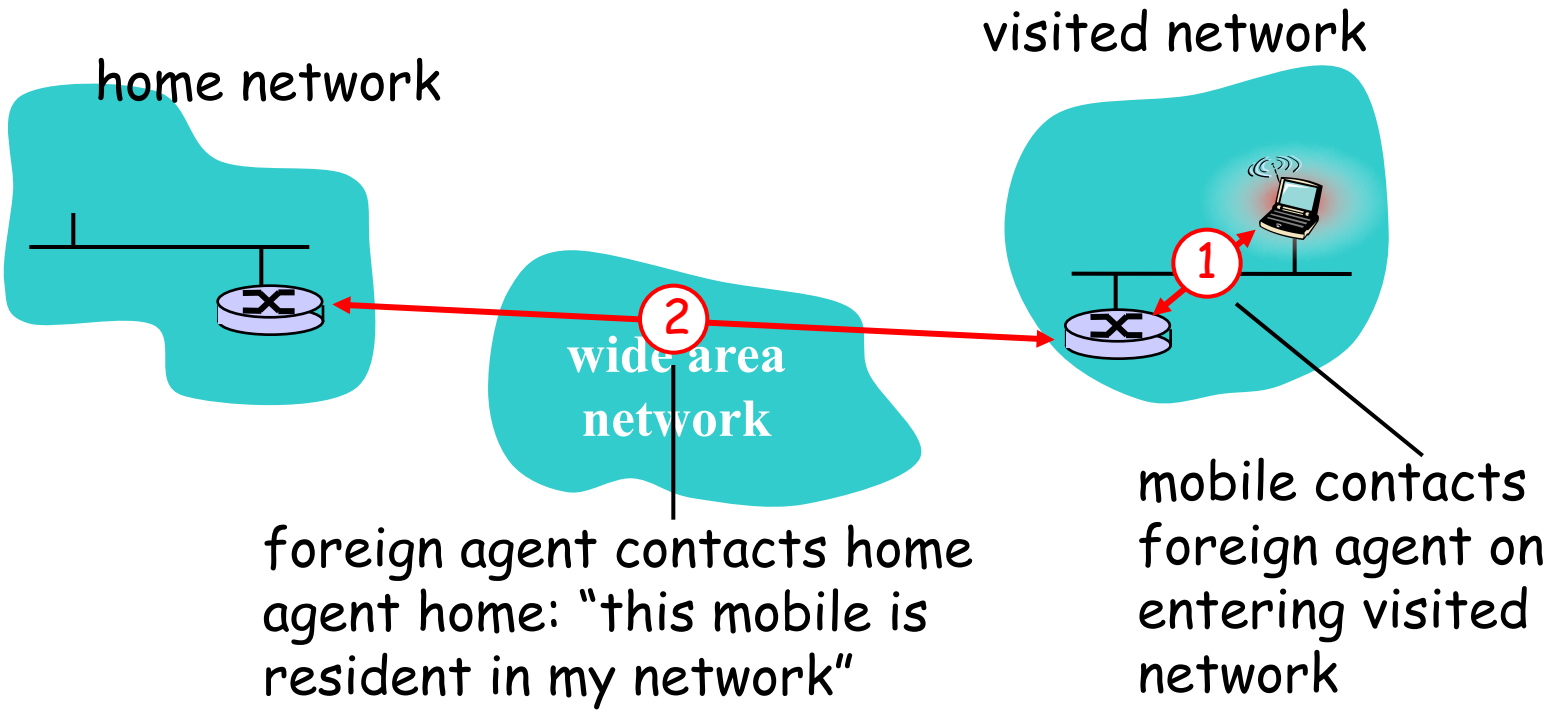
Mobility: approaches

- *Let routing handle it*: routers advertise IP address of mobile-nodes-in-residen routing table exchange.
  - routing tables indicate where each mo
  - no changes to end-systems



- *Let end-systems handle it*:
  - Mobile keeps home agent updated on its whereabouts
  - *indirect routing*: correspondent sends packets to mobile's home agent, which forwards to mobile
  - *direct routing*: correspondent gets mobile's foreign address, sends directly to mobile

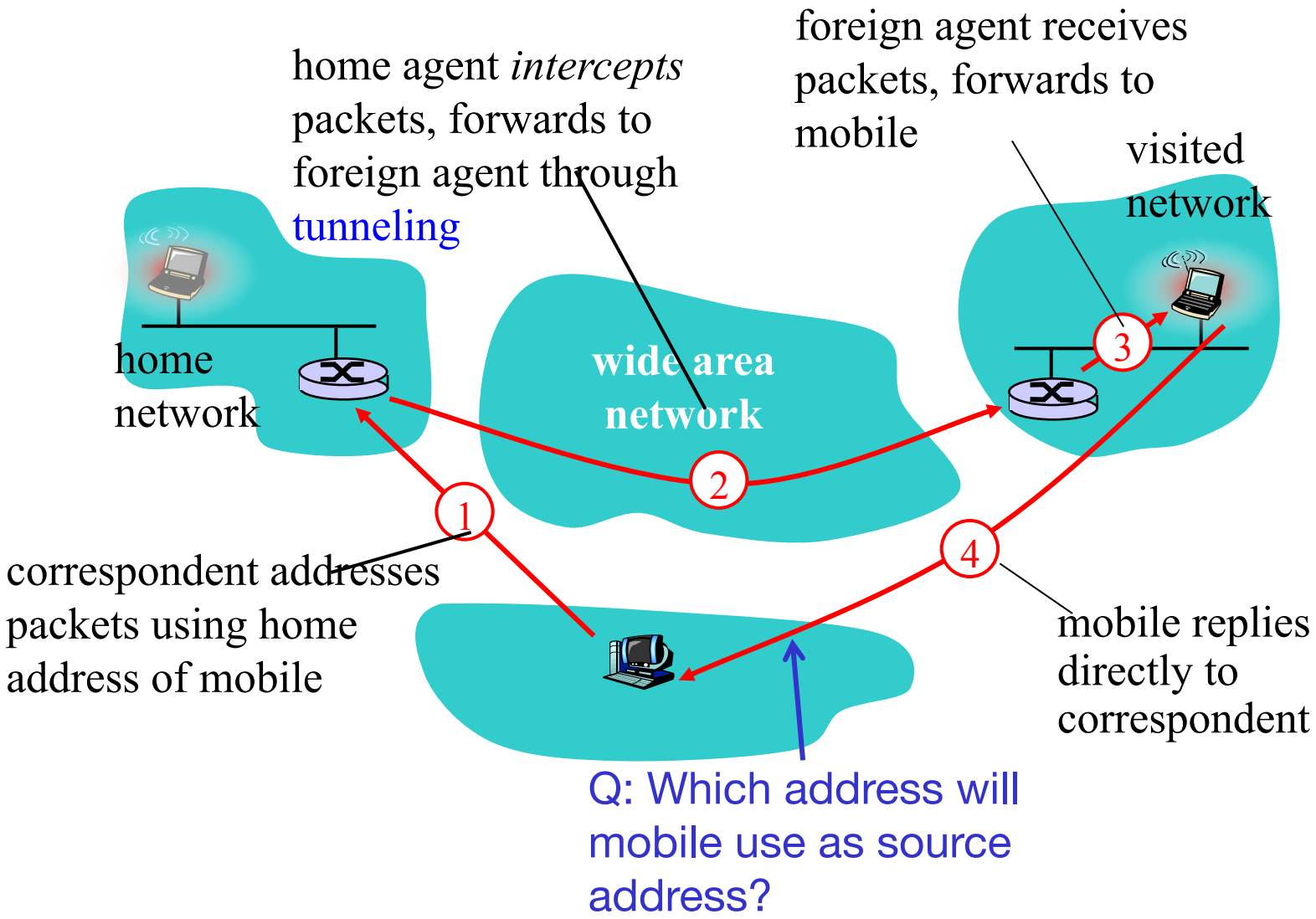
Mobility: registration



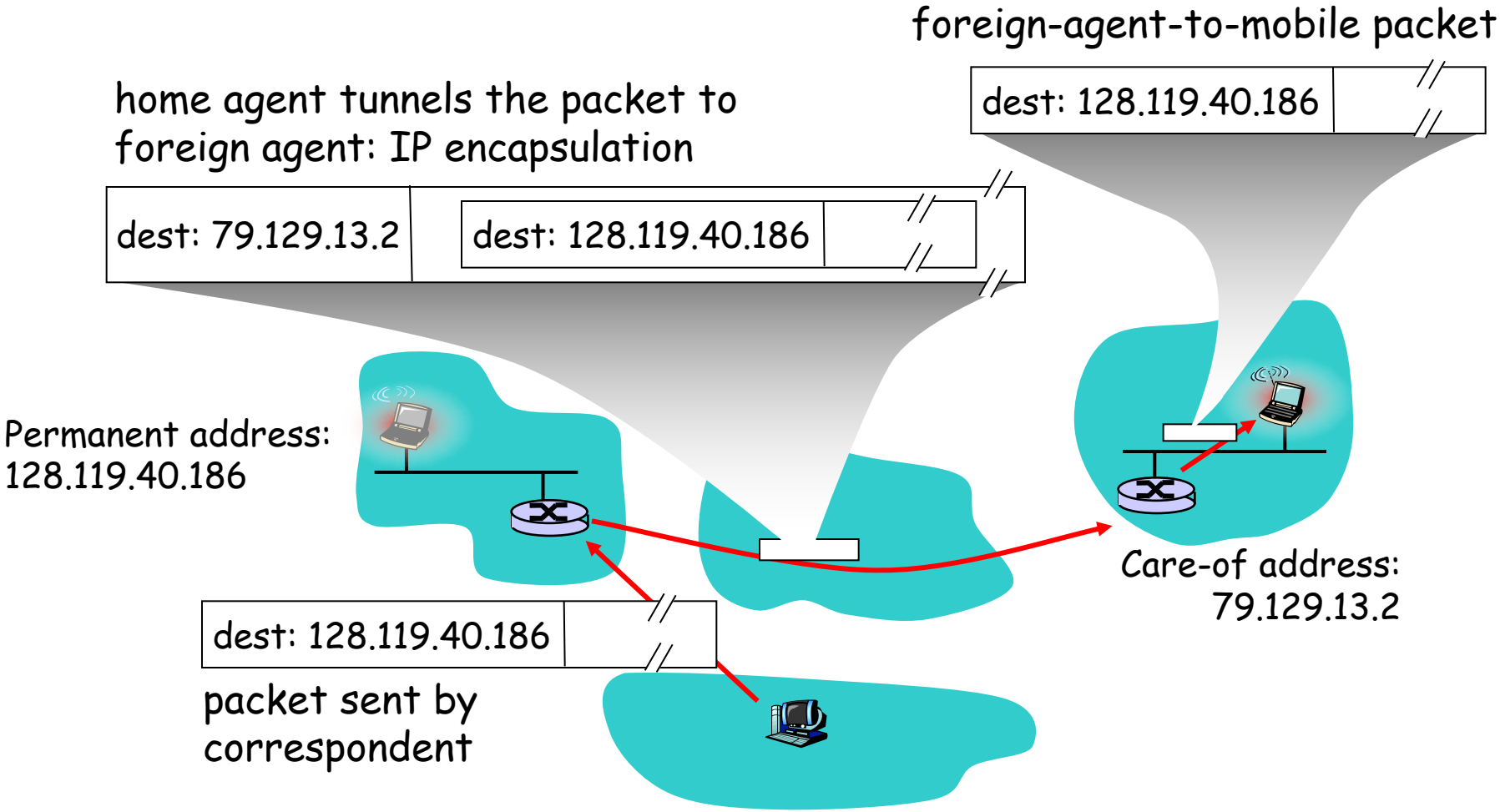
End result:

- Foreign agent knows about mobile
- Home agent knows location of mobile

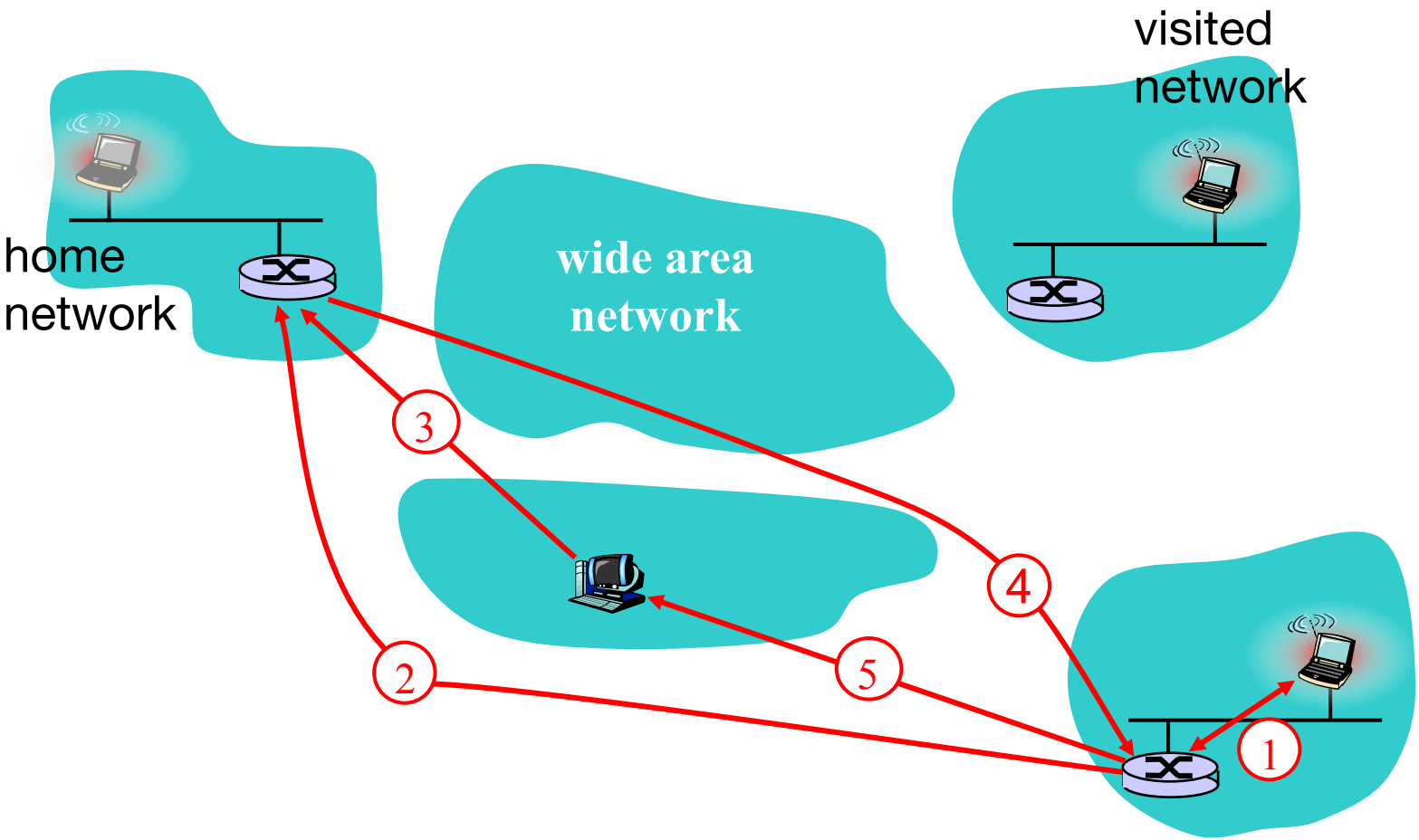
Supporting Mobility via Indirect Routing



Mobile IP: indirect routing



Indirect Routing: handling further movement



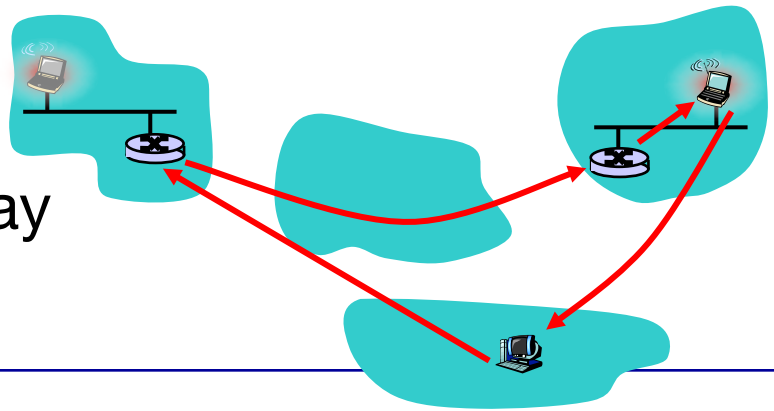
Q: Will the correspondence be aware of mobile's move?

Indirect Routing: moving between networks

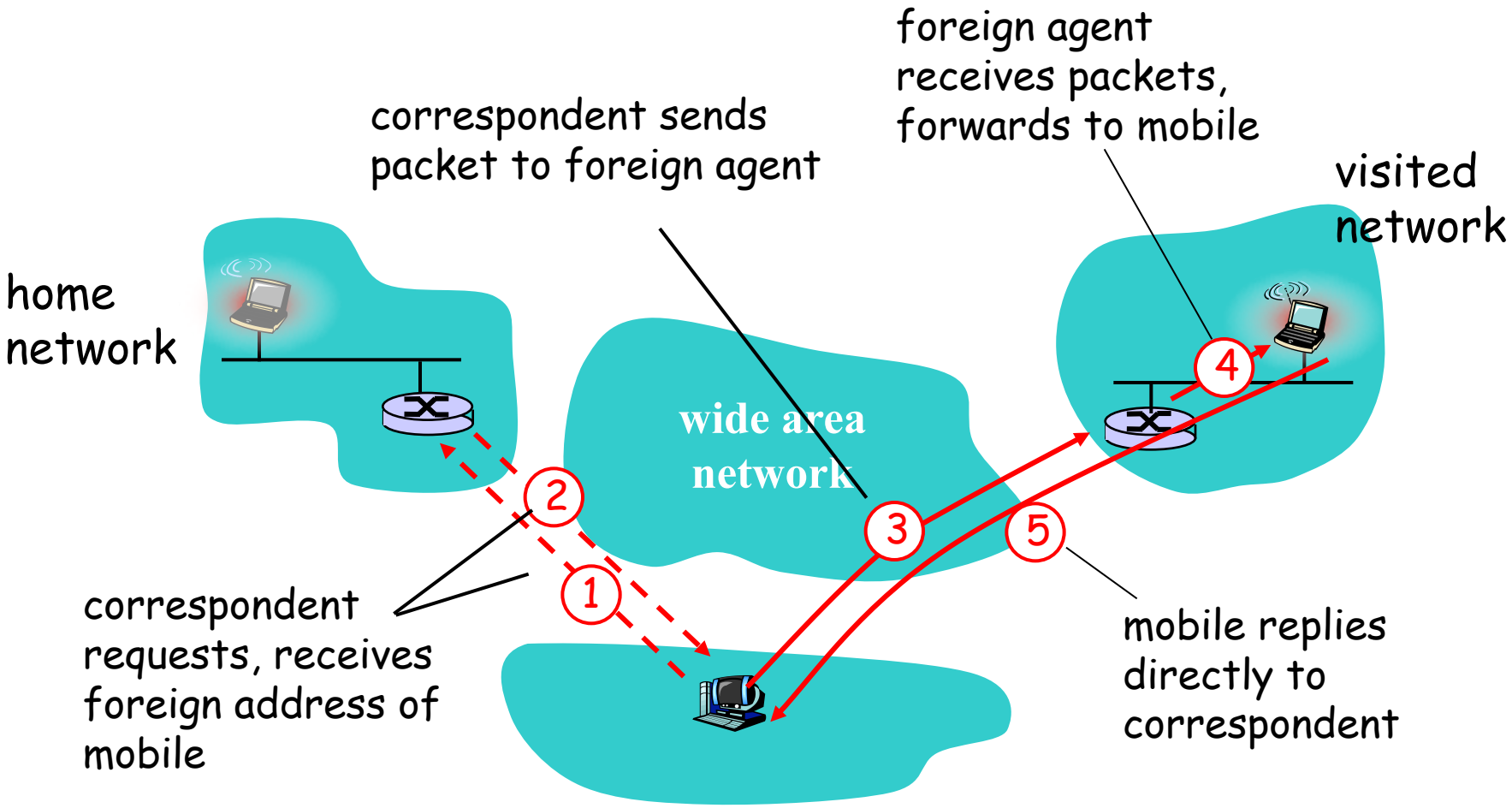
- When mobile moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - Home agent continue to forward packets to mobile through IP-in-IP tunnel (to the new care-of-address)
- Mobility is transparent to correspondent
- mobility is transparent to TCP (or any other transport protocol)
  - TCP connection uses mobile's home address, *ongoing connections can be maintained* while mobile moves

Summary of Indirect Routing

- Mobile uses two addresses:
  - permanent address: used by correspondent to send packet to mobile
  - care-of-address: used by home agent to forward packet to mobile
- Mobile can perform foreign agent function itself
  - Just get a care-of address from foreign DHCP server
- Mobility is transparent to correspondent
- May result in triangle routing: correspondent→home-network→mobile
  - Inefficient, especially when correspondent & mobile are close but home agent is far away

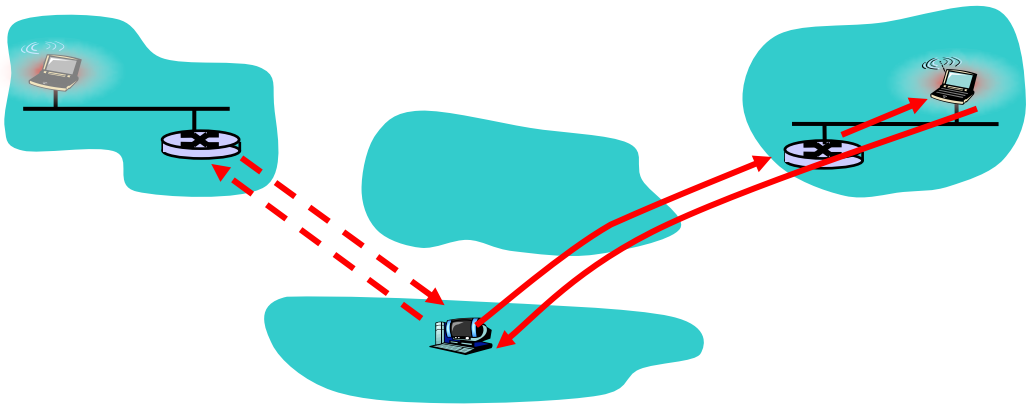


Mobility via Direct Routing



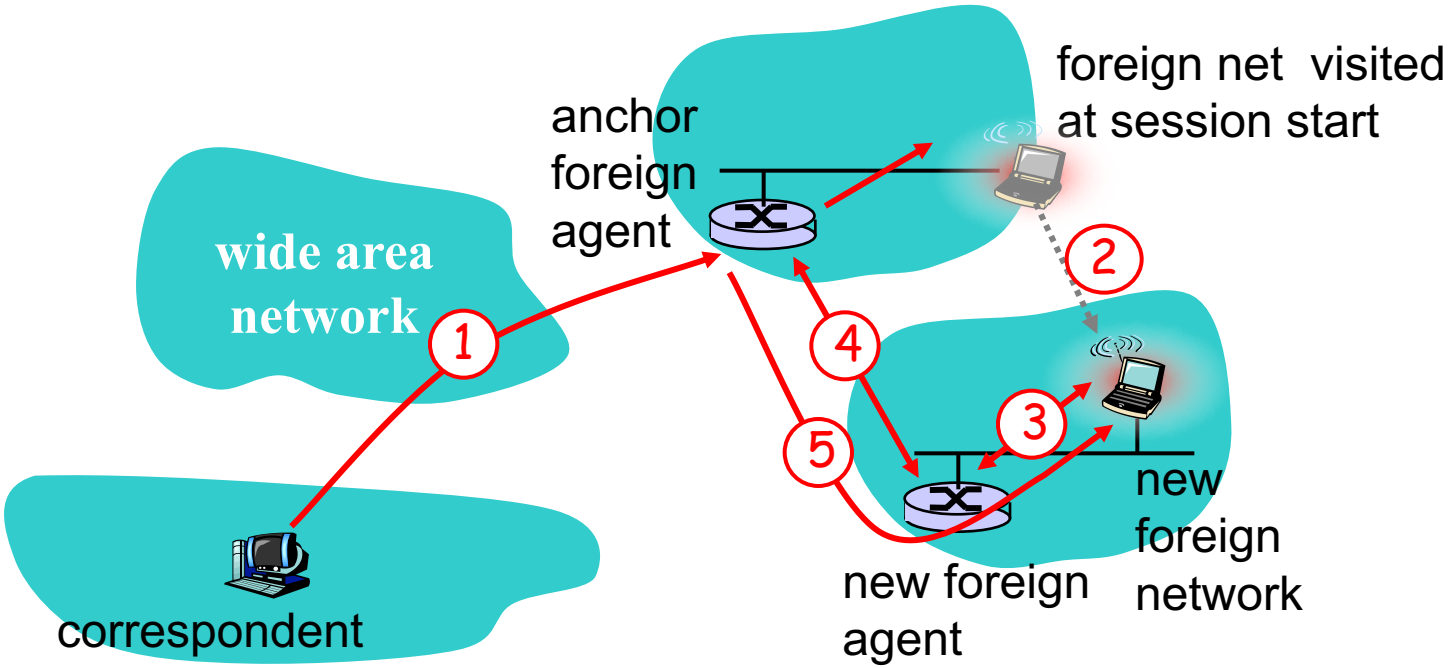
Mobility via Direct Routing: comments

- Good: Eliminate triangle routing problem
- bad:
  - Correspondent must be aware of mobility support
  - what if mobile moves from network to network?



Accommodating mobility with direct routing

- anchor foreign agent: FA in the first visited network
- data always routed first to anchor FA
- when mobile moves: new FA notifies the old FA to have data forwarded from old FA (chaining)



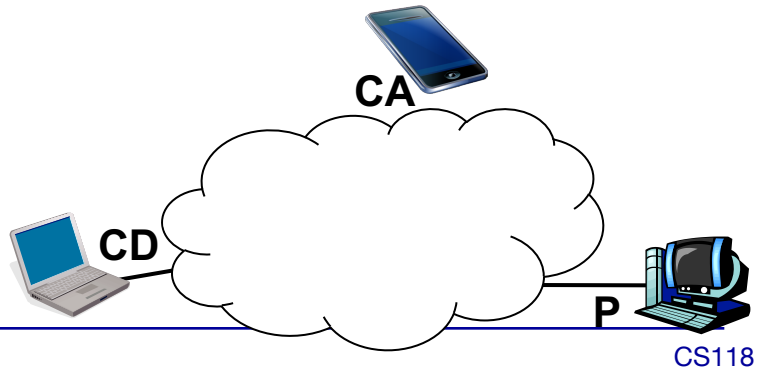
IP mobility: summary

- A mobile has
  - a home-agent, and
  - a permanent home IP address
- When a mobile moves to a new location,
  - Obtain a new care-of address
  - Informing its home agent of its new IP address
- Indirect routing: A correspondent sends data to a mobile's home address, the home-agent forward data to the mobile's care-of address
- Direct routing: correspondent obtains mobile's care-of address, sends packet to mobile directly

Mobility via indirect routing

- correspondent sends data to the mobile's home agent
  - Source = CD; destination = P (mobile's permanent address)
- Home agent tunnels data to mobile
  - Outer IP header: Source = P; destination = CA
  - Inner IP header: source = CD; destination = P
- Mobile tunnels data to correspondent
  - Outer header: Source = CA; destination = CD
  - Inner header: source = P; destination = CD
- Supports mobile movement transparently
  - No change to transport protocols
  - Cost: triangle routing

P = mobile's Permanent home address
CA = Care-of Address
CD = CorresponDent address

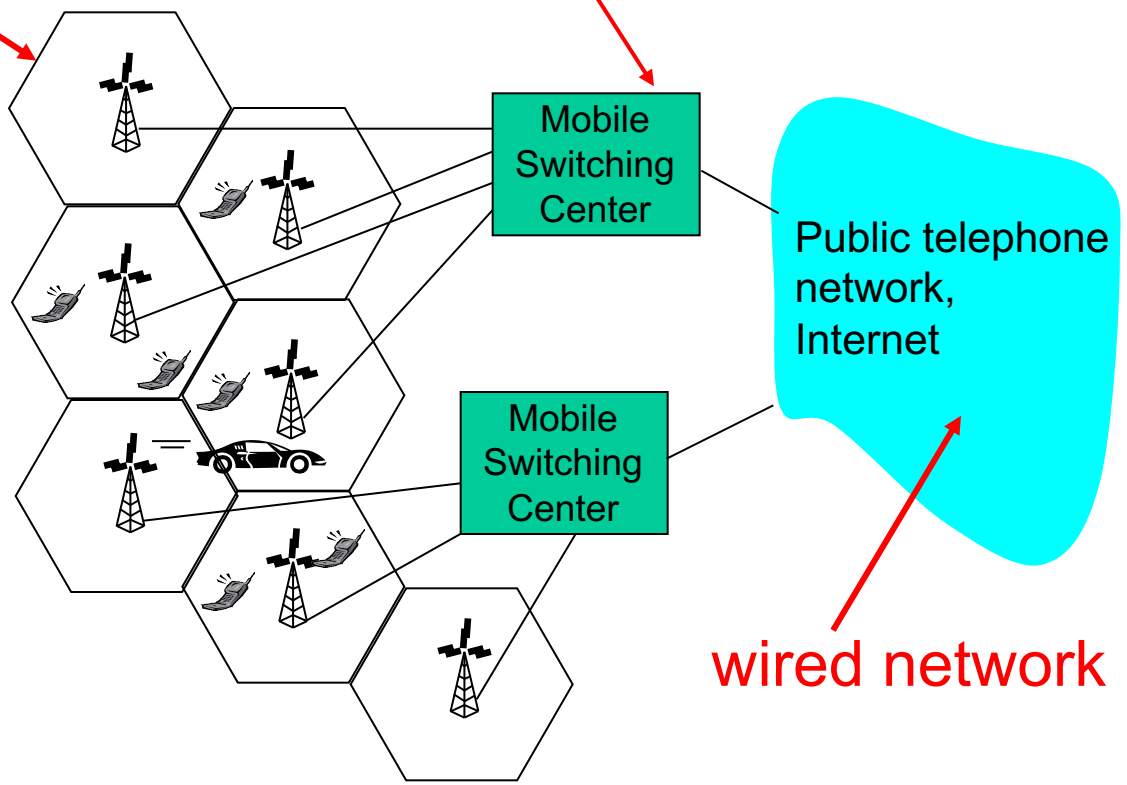


Cellular Networks

Components of cellular network architecture

MSC
- connects cells to wide area net
- manages call setup (more later!)
- handles mobility (more later!)

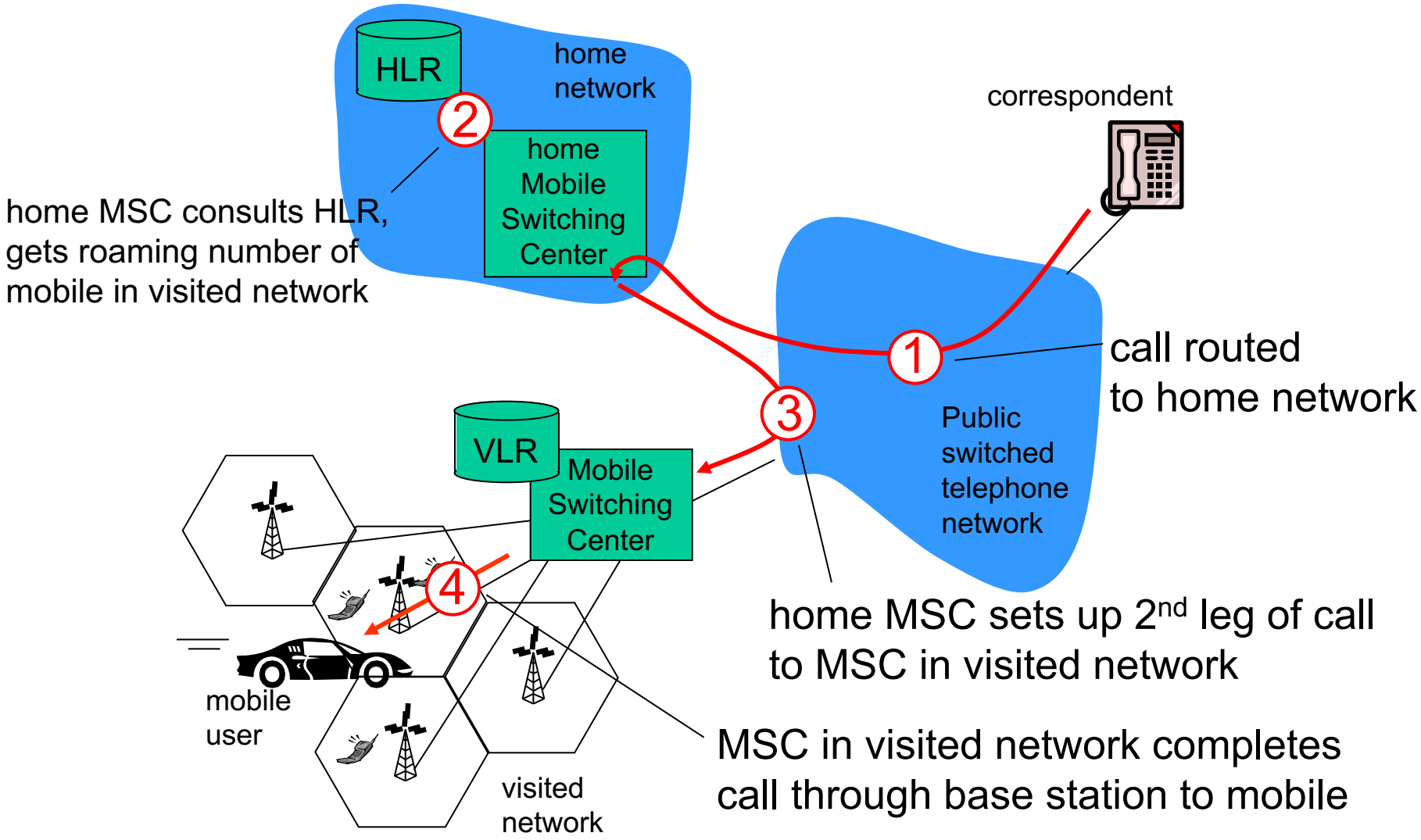
cell
- covers geographical region
- *base station* (BS) analogous to 802.11 AP
- *mobile users* attach to network through BS
- *air-interface:* physical and link layer protocol between mobile and BS



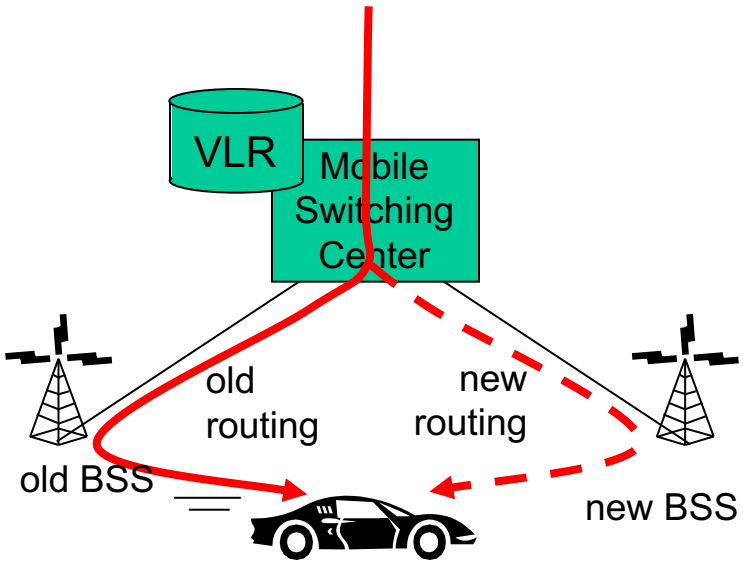
GSM: Global System for Mobile communications

- *home network:* network of cellular provider you subscribe to (e.g., ATT, Sprint PCS, Verizon)
  - *home location register (HLR):* database in home network containing permanent cell phone #, profile information (services, preferences, billing), information about the mobile's current location (could be in another network)
- *visited network:* network in which mobile currently resides
  - *visitor location register (VLR):* database with entry for each user currently in network

Indirect routing to reach mobile

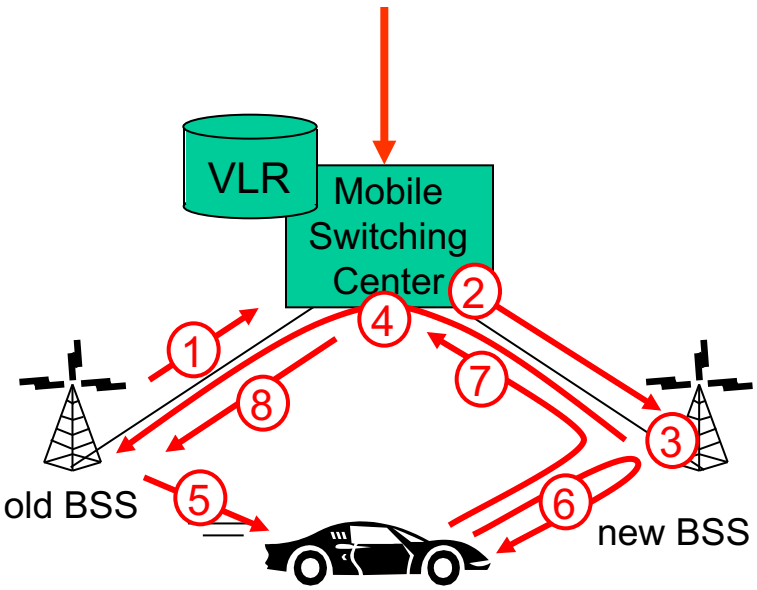


GSM: handoff with common MSC



- Handoff goal: route call via new base station (without interruption)
- reasons for handoff:
  - stronger signal to/from new BSS (continuing connectivity, less battery drain)
  - load balance: free up channel in current BSS
  - GSM doesn't mandate why to perform handoff (policy), only how (mechanism)
- handoff initiated by old BSS

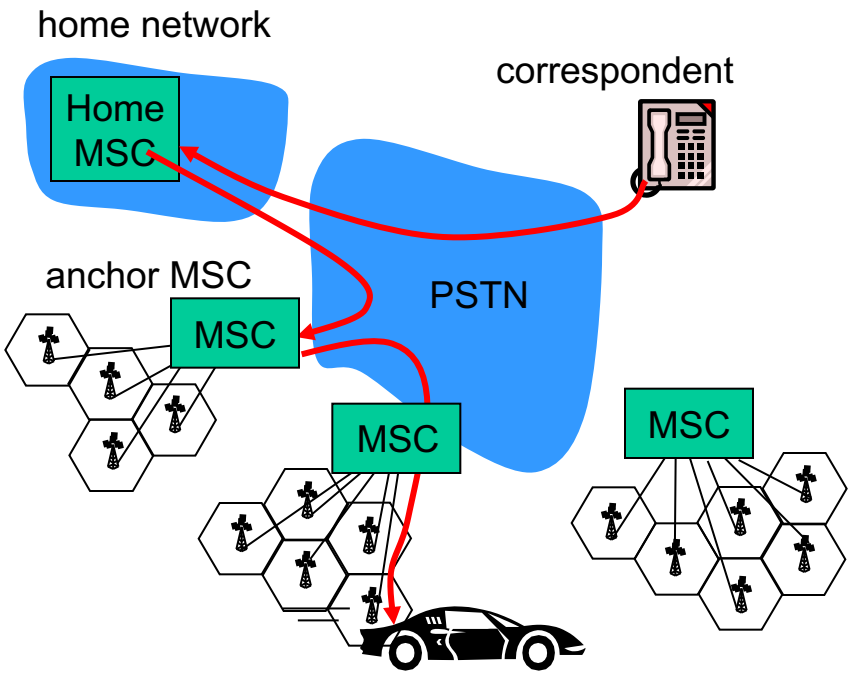
GSM: handoff with common MSC



1. old BSS informs MSC of impending handoff, provides list of 1^+ new BSSs
2. MSC sets up path (allocates resources) to new BSS
3. new BSS allocates radio channel for use by mobile
4. new BSS signals MSC, old BSS: ready
5. old BSS tells mobile: perform handoff to new BSS
6. mobile, new BSS signal to activate new channel
7. mobile signals via new BSS to MSC: handoff complete. MSC reroutes call

8 MSC-old-BSS resources released

GSM: handoff between MSCs



(a) before handoff

- *anchor MSC:* first MSC visited during the call
  - call remains routed through anchor MSC
- new MSCs add on to end of MSC chain as mobile moves to new MSC
- IS-41 allows optional path minimization step to shorten multi-MSC chain

VPNs

What is network-layer confidentiality ?

between two network entities:

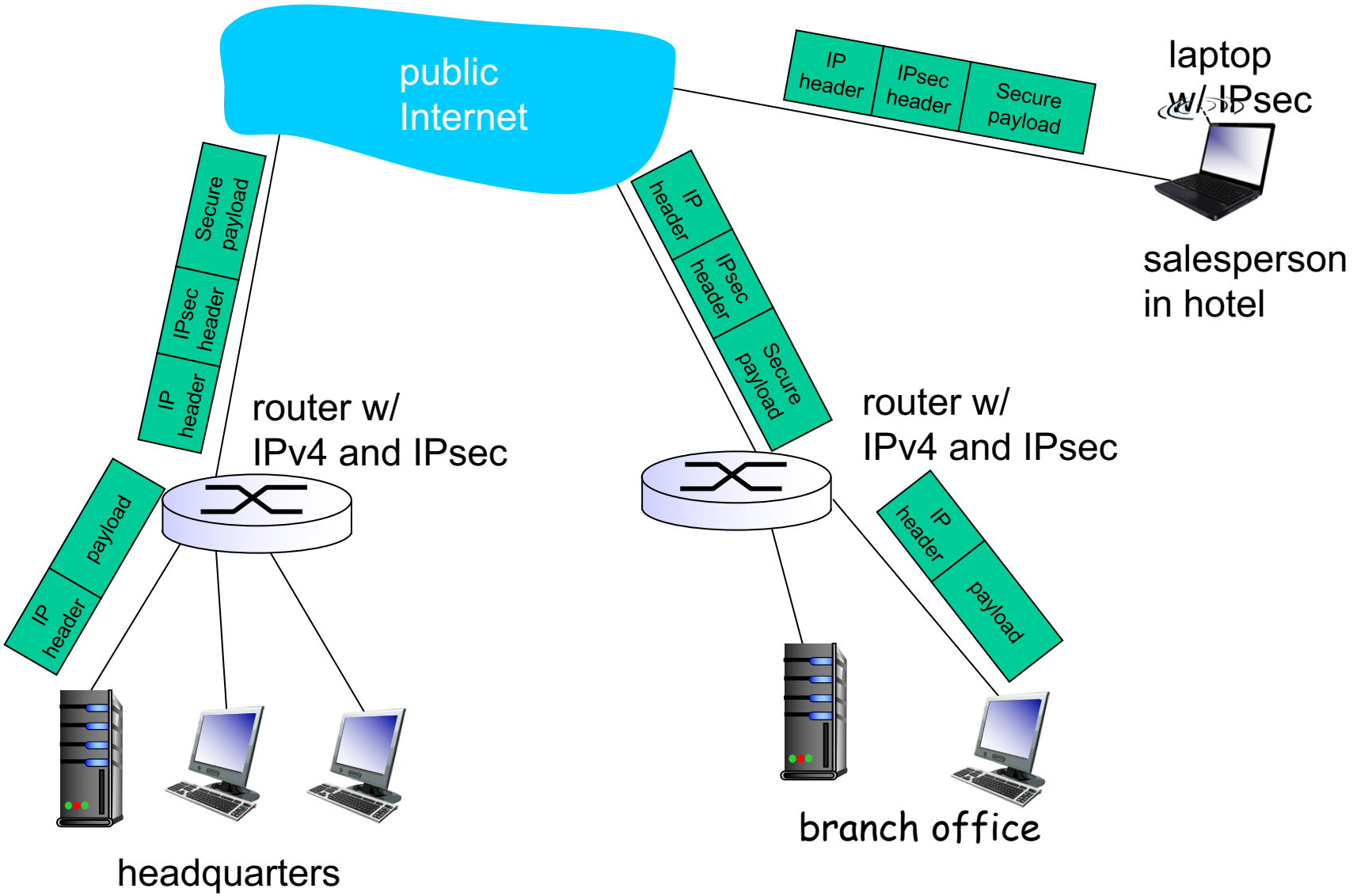
- sending entity encrypts datagram payload, payload could be:
  - TCP or UDP segment, ICMP message, OSPF message ….
- all data sent from one entity to other would be hidden:
  - web pages, e-mail, P2P file transfers, TCP SYN packets …
- "blanket coverage"

Virtual Private Networks (VPNs)

motivation:

- institutions often want private networks for security.
  - costly: separate routers, links, DNS infrastructure.
- VPN: institution's inter-office traffic is sent over public Internet instead
  - encrypted before entering public Internet
  - logically separate from other traffic

Virtual Private Networks (VPNs)

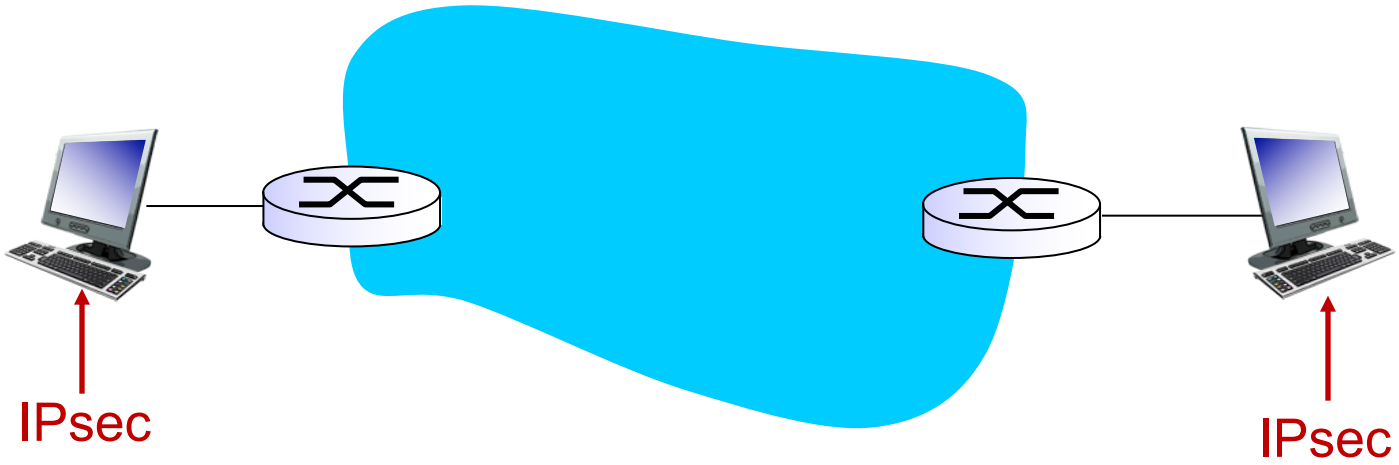


IPsec services

- data integrity
- origin authentication
- replay attack prevention
- confidentiality

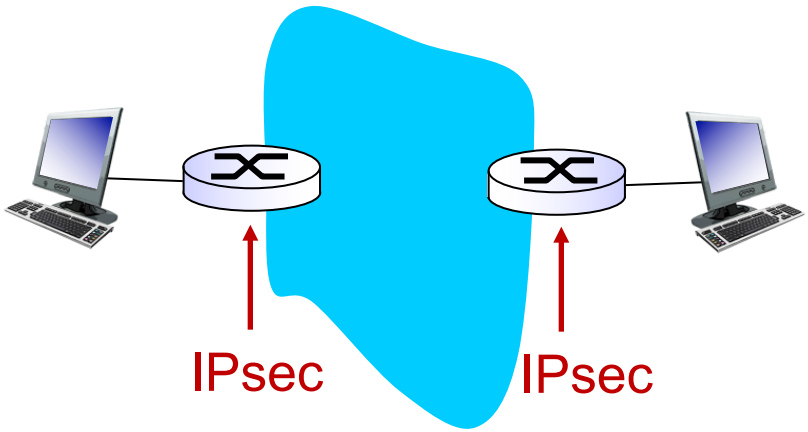
- two protocols providing different service models:
  - Authentication headers (AH)
  - Encapsulating security payload (ESP)

IPsec transport mode

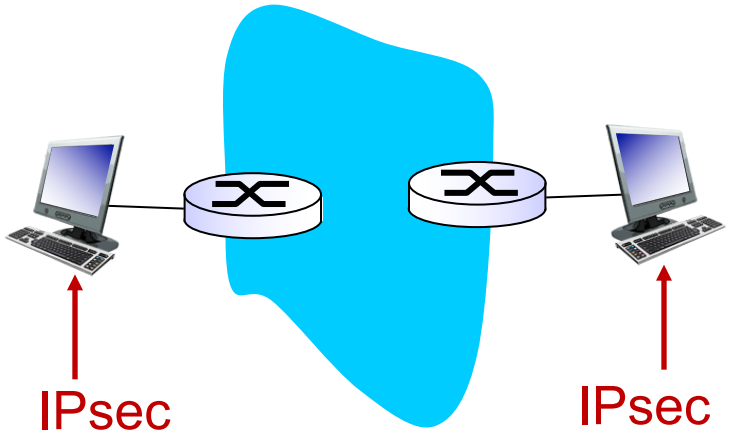


- IPsec datagram emitted and received by end-system
- protects upper level protocols

IPsec – tunneling mode



- edge routers IPsec-aware



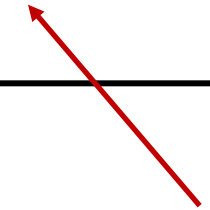
- hosts IPsec-aware

Two IPsec protocols

- Authentication Header (AH) protocol
  - provides source authentication & data integrity but *not* confidentiality
- Encapsulation Security Protocol (ESP)
  - provides source authentication, data integrity, *and confidentiality*
  - more widely used than AH

Four combinations are possible!

Host mode with AH	Host mode with ESP
Tunnel mode with AH	Tunnel mode with ESP

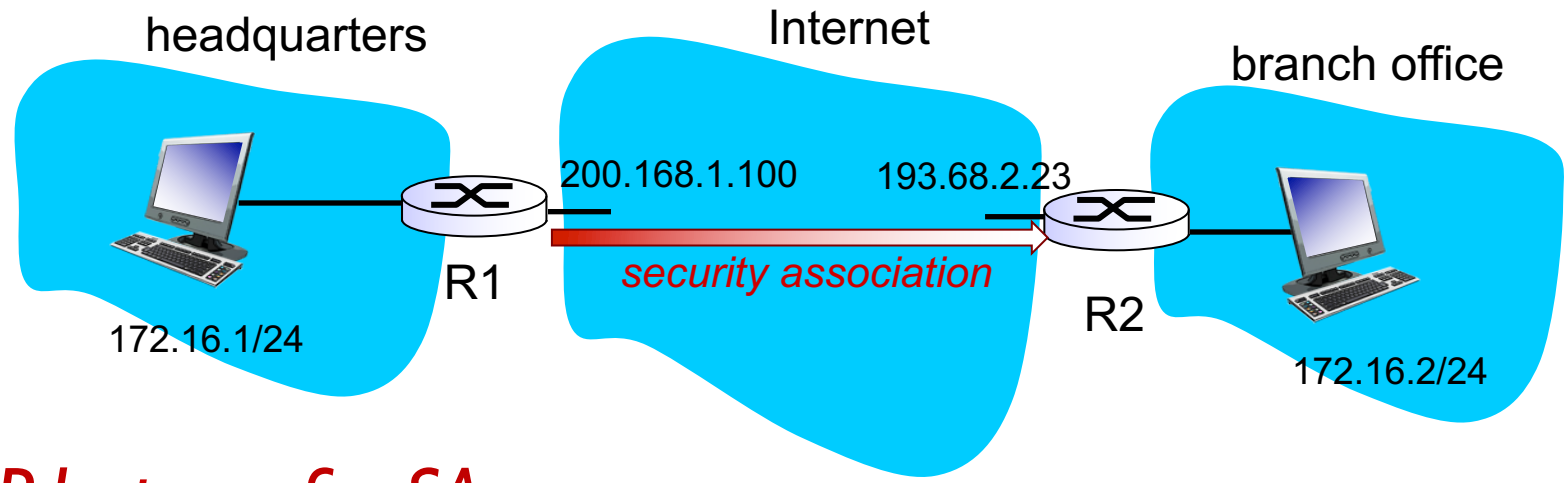


most common and most important

Security associations (SAs)

- before sending data, "security association (SA)" established from sending to receiving entity
  - SAs are simplex: for only one direction
- ending, receiving entitles maintain *state information* about SA
  - recall: TCP endpoints also maintain state info
  - IP is connectionless; IPsec is connection-oriented!
- how many SAs in VPN w/ headquarters, branch office, and n traveling salespeople?

Example SA from R1 to R2

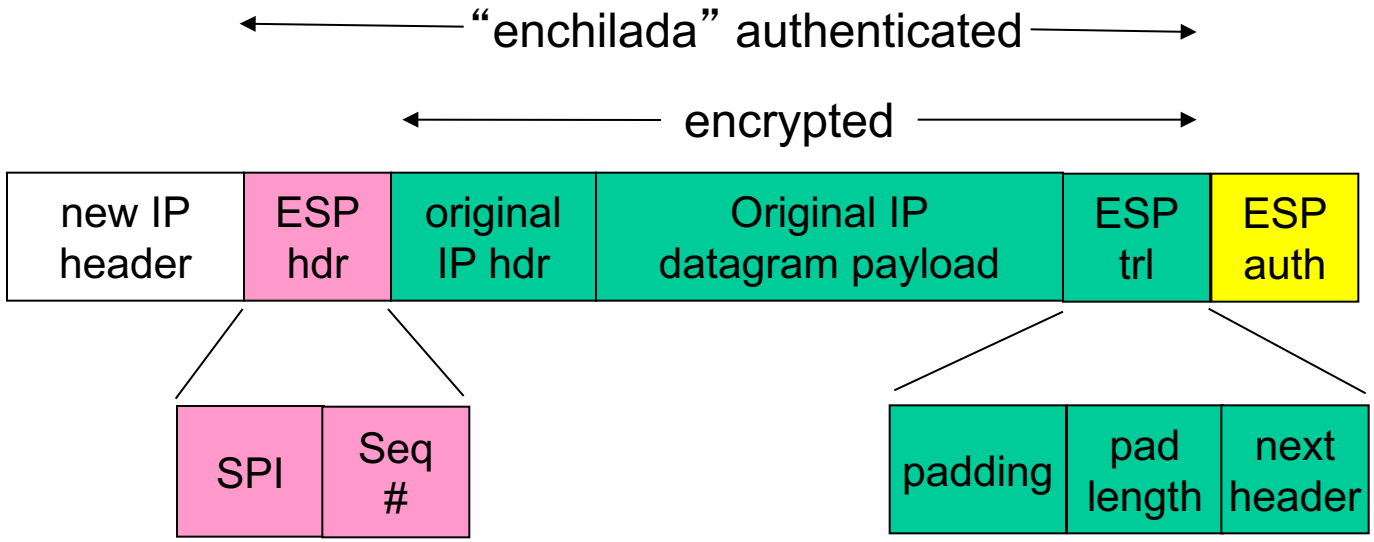


R1 stores for SA:

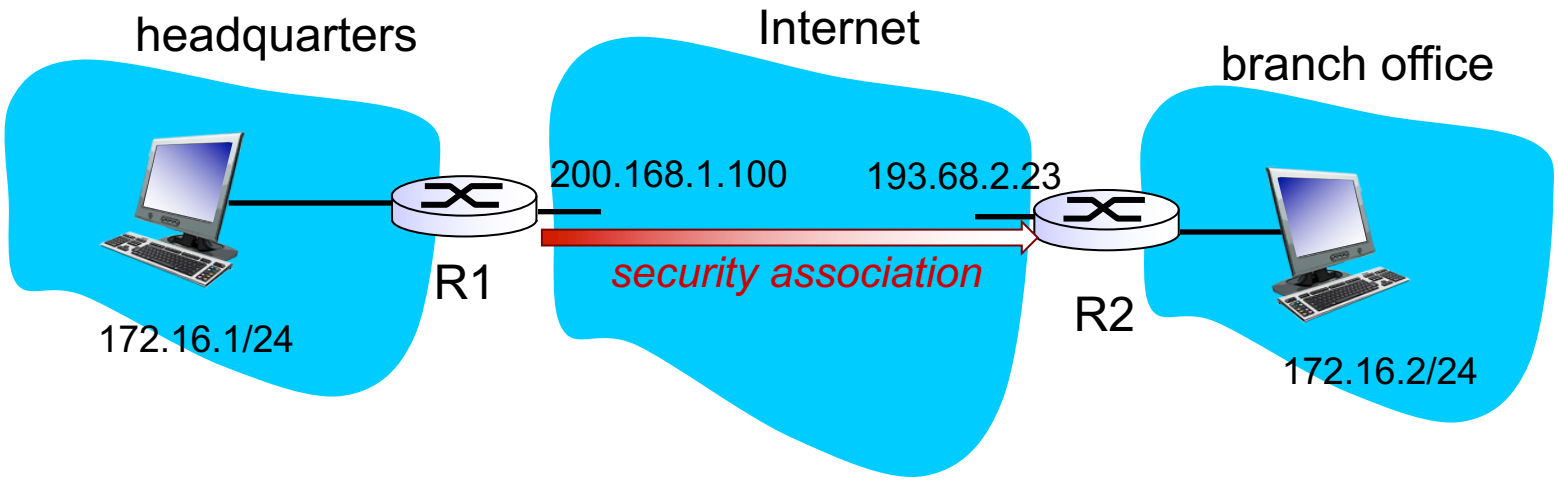
- 32-bit SA identifier: *Security Parameter Index (SPI)*
- origin SA interface (200.168.1.100)
- destination SA interface (193.68.2.23)
- type of encryption used (e.g., 3DES with CBC)
- encryption key
- type of integrity check used (e.g., HMAC with MD5)
- authentication key

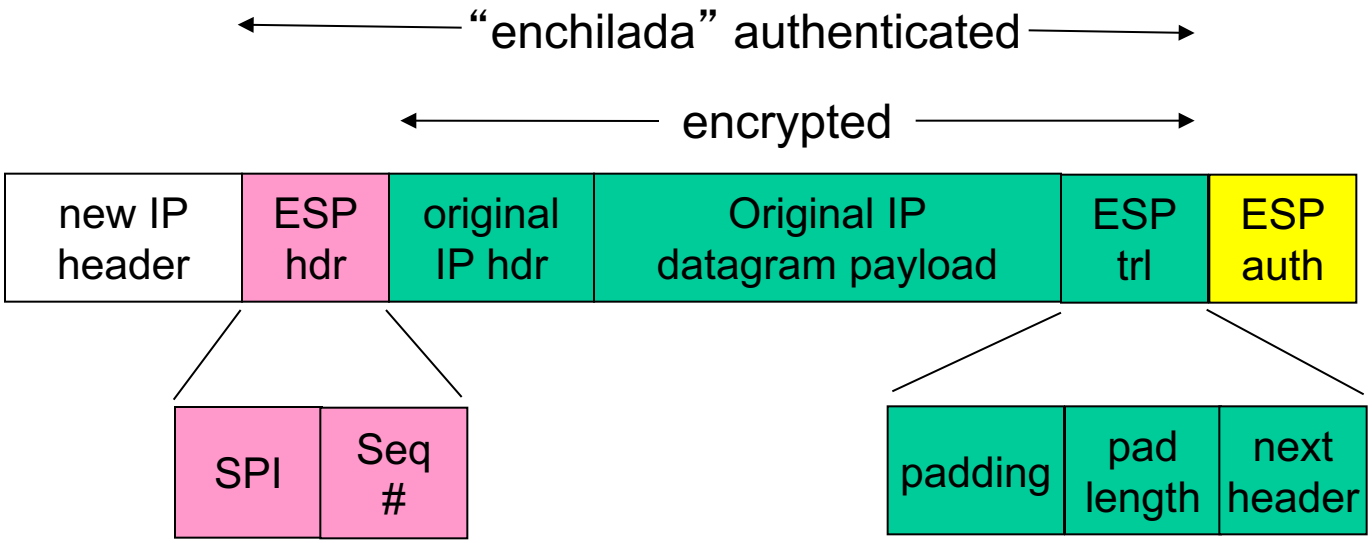
IPsec datagram

focus for now on tunnel mode with ESP



What happens?

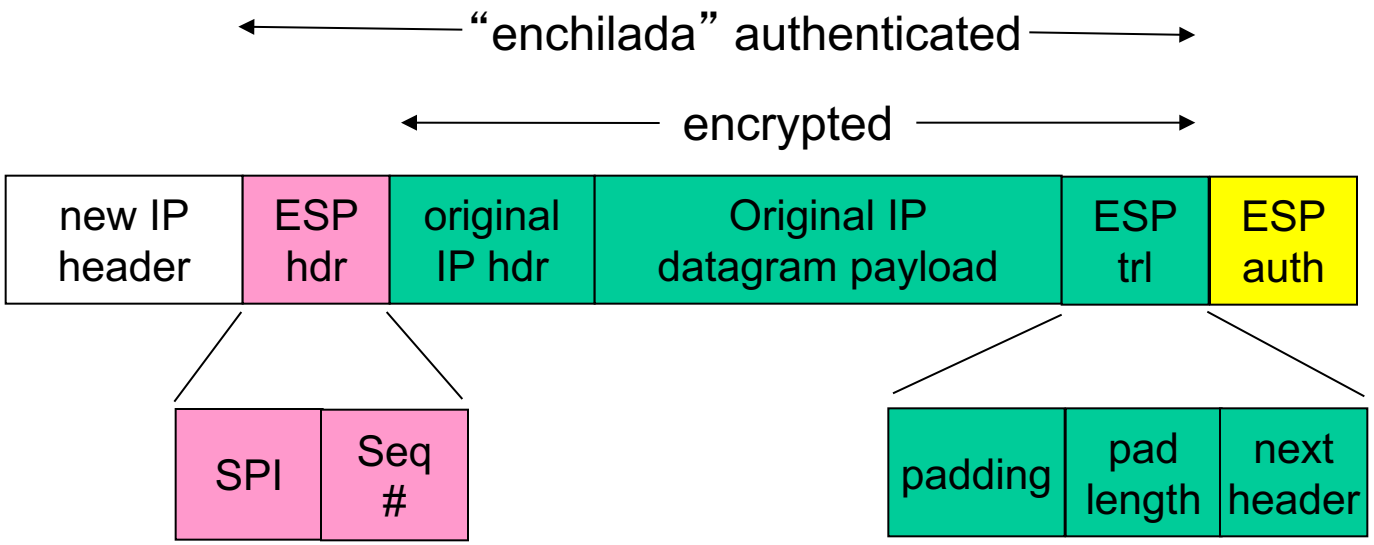




R1: convert original datagram to IPsec datagram

- appends to back of original datagram (which includes original header fields!) an "ESP trailer" field.
- encrypts result using algorithm & key specified by SA.
- appends to front of this encrypted quantity the "ESP header, creating "enchilada".
- creates authentication MAC over the *whole enchilada*, using algorithm and key specified in SA;
- appends MAC to back of enchilada, forming *payload*;
- creates brand new IP header, with all the classic IPv4 header fields, which it appends before payload.

Inside the enchilada:



- ESP trailer: Padding for block ciphers
- ESP header:
  - SPI, so receiving entity knows what to do
  - Sequence number, to thwart replay attacks
- MAC in ESP auth field is created with shared secret key

IPsec sequence numbers

- for new SA, sender initializes seq. # to 0
- each time datagram is sent on SA:
  - sender increments seq # counter
  - places value in seq # field
- goal:
  - prevent attacker from sniffing and replaying a packet
  - receipt of duplicate, authenticated IP packets may disrupt service
- method:
  - destination checks for duplicates
  - doesn't keep track of *all* received packets; instead uses a window

Summary: IPsec services

- suppose Covfefe sits somewhere between R1 and R2. she doesn't know the keys.
  - will Trudy be able to see original contents of datagram? How about source, dest IP address, transport protocol, application port?
  - flip bits without detection?
  - masquerade as R1 using R1's IP address?
  - replay a datagram?

IKE: Internet Key Exchange

- *previous examples:* manual establishment of IPsec SAs in IPsec endpoints:

  Example SA

  SPI: 12345
  Source IP: 200.168.1.100
  Dest IP: 193.68.2.23
  Protocol: ESP
  Encryption algorithm: 3DES-cbc
  HMAC algorithm: MD5
  Encryption key: 0x7aeaca…
  HMAC key:0xc0291f…

- manual keying is impractical for VPN with 100s of endpoints
- instead use *IPsec IKE (Internet Key Exchange)*

IKE: PSK and PKI

- authentication (prove who you are) with either
  - pre-shared secret (PSK) or
  - with PKI (pubic/private keys and certificates).
- PSK: both sides start with secret
  - run IKE to authenticate each other and to generate IPsec SAs (one in each direction), including encryption, authentication keys
- PKI: both sides start with public/private key pair, certificate
  - run IKE to authenticate each other, obtain IPsec SAs (one in each direction).
  - similar with handshake in SSL.

IKE phases

- IKE has two phases
  - *phase 1:* establish bi-directional IKE SA
    - note: IKE SA different from IPsec SA
    - aka ISAKMP security association
  - *phase 2:* ISAKMP is used to securely negotiate IPsec pair of SAs
- phase 1 has two modes: aggressive mode and main mode
  - aggressive mode uses fewer messages
  - main mode provides identity protection and is more flexible

IPsec summary

- IKE message exchange for algorithms, secret keys, SPI numbers
- either AH or ESP protocol (or both)
  - AH provides integrity, source authentication
  - ESP protocol (with AH) additionally provides encryption
- IPsec peers can be two end systems, two routers/firewalls, or a router/firewall and an end system