Advanced Network Technologies

Wireless 2

Dr. Wei Bao | Lecturer
School of Computer Science

THE UNIVERSITY OF SYDNEY

IEEE 802.11 Wireless LANs WiFi

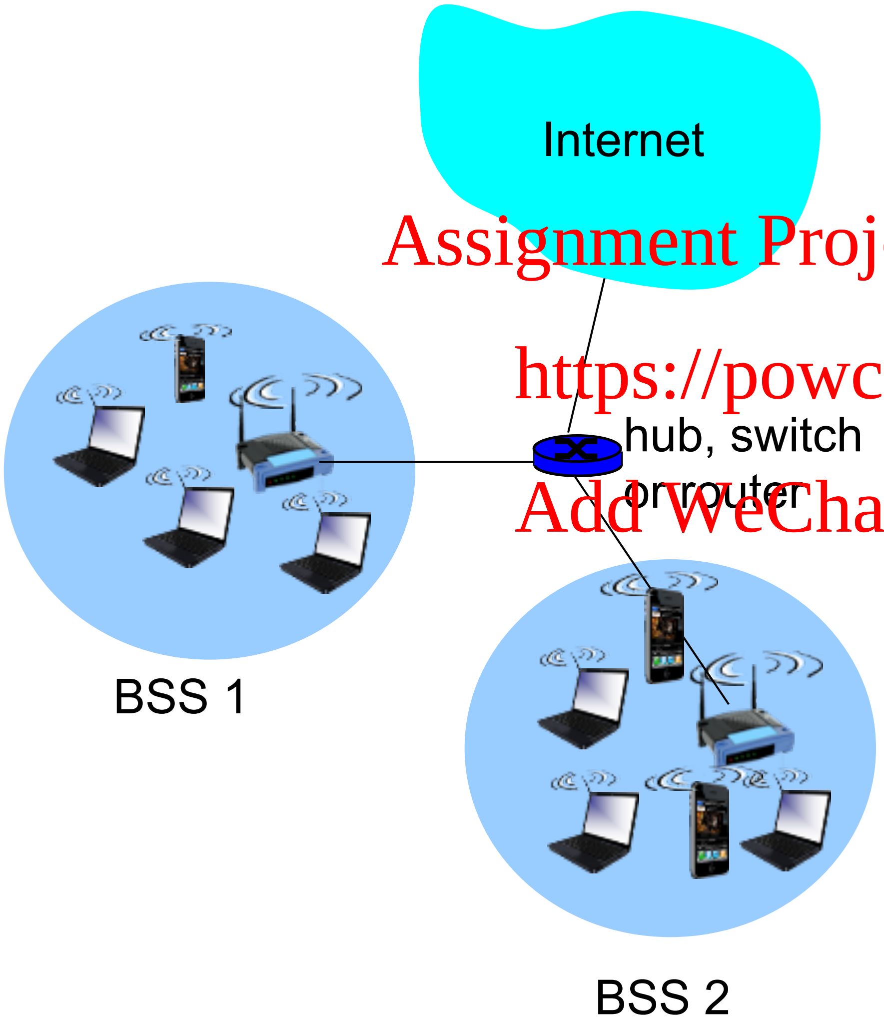
IEEE 802.11 WiFi

IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30m	2.4 Ghz
802.11a	1999	54 Mbps	30m	5 Ghz
802.11g	2003	54 Mbps	30m	2.4 Ghz
802.11n (WiFi 4)	2009	600 Mbps	70m	2.4, 5 Ghz
802.11ac (WiFi 5)	2013	3.47Gpbs	70m	5 Ghz
802.11ax (WiFi 6)	2020 (exp.)	14 Gbps	70m	2.4, 5 Ghz
802.11af	2014	35 – 560 Mbps	1 Km	unused TV bands (54-790 MHz)
802.11ah	2017	347Mbps	1 Km	900 Mhz

- all use CSMA/CA for multiple access, and have base-station and ad-hoc network versions

THE UNIVERSITY OF SYDNEY

802.11 LAN architecture



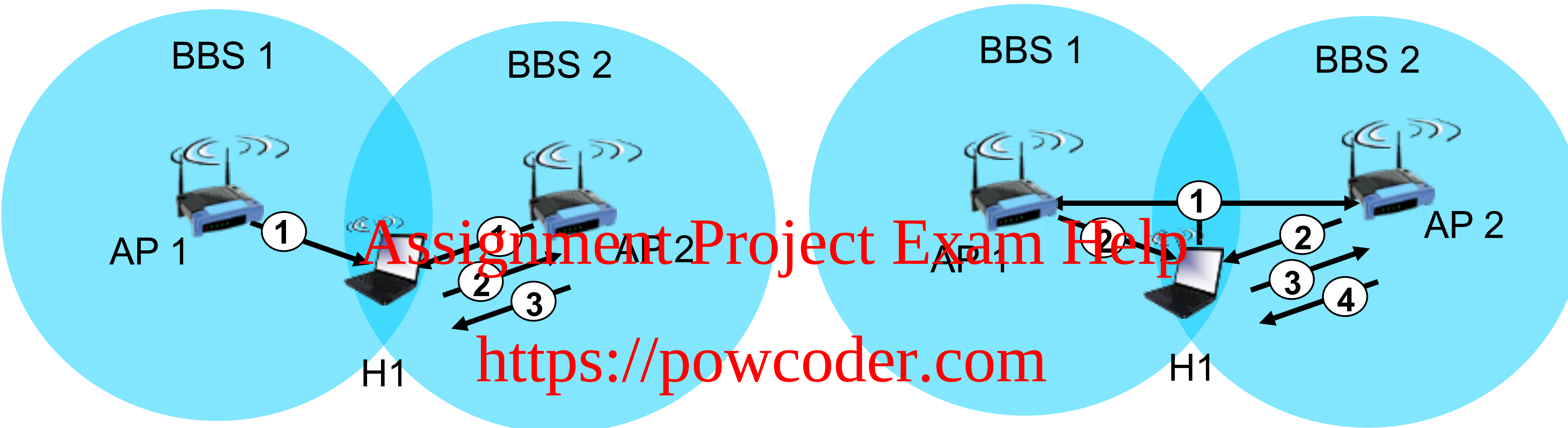
- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

802.11: Channels, association

› 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!

› host: must *associate* with an AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - may perform authentication
  - will typically run DHCP to get IP address in AP's subnet

802.11: passive/active scanning



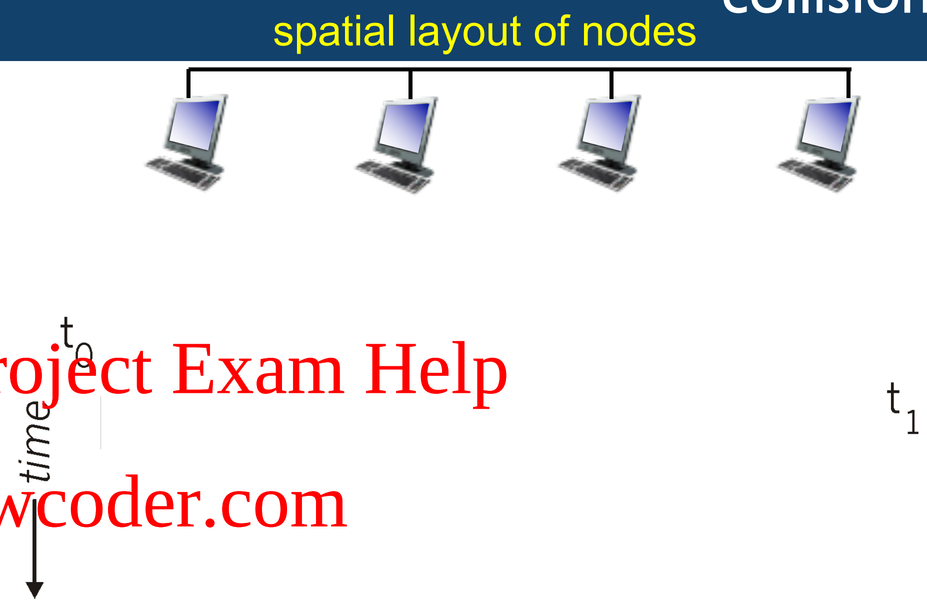
passive scanning:

(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1

active scanning:

(1) Probe Request frame broadcast from H1
(2) Probe Response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent from selected AP to H1

collisions



- collisions *can* occur: propagation delay means two nodes may not hear each other's transmission
- collision: frame transmission time wasted

Wired Networks: CSMA/CD (collision detection)

CSMA/CD:

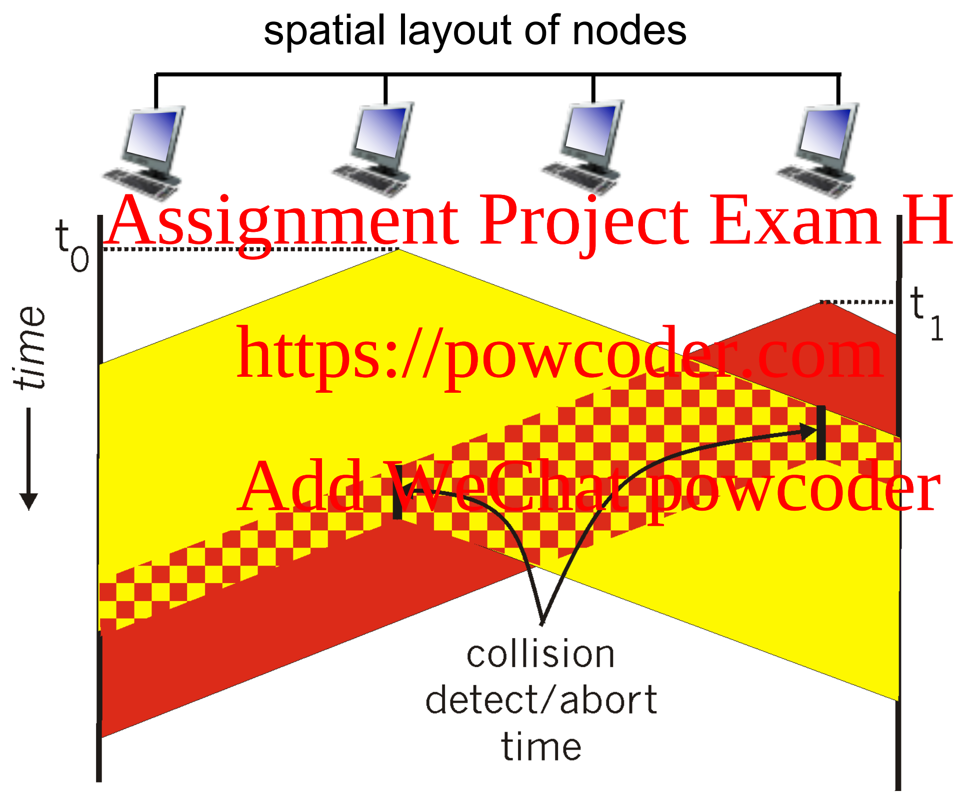
- collisions *detected* within short time
- colliding transmissions aborted, reducing channel wastage

› collision detection:

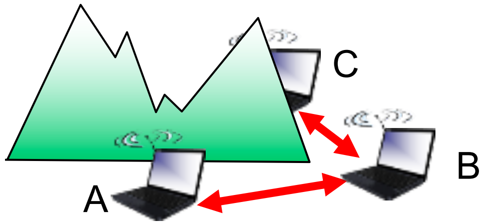
- wired LANs: measure signal strengths, compare transmitted, received signals
  - Can transmit and sense at the same time
- wireless LANs: received signal strength overwhelmed by local transmission strength
  - CSMA-CD cannot be used in wireless LAN

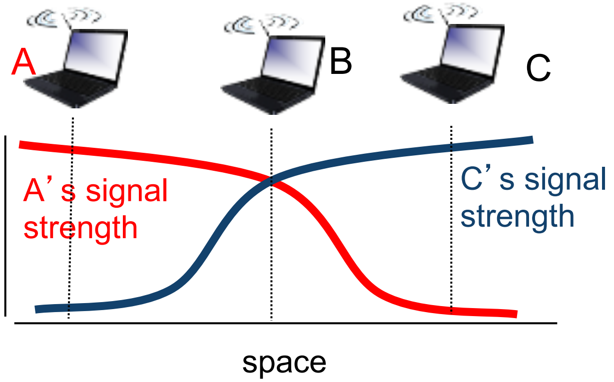
THE UNIVERSITY OF SYDNEY

CSMA/CD (collision detection)



- 802.11: *no* collision detection!
  - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - can not sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/C(ollision)A(voidance)





IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

1 if sense channel idle for **DIFS** (Distributed inter-frame space) then

transmit entire frame (no CD)

2 if sense channel busy then

start random backoff time

timer counts down while channel idle

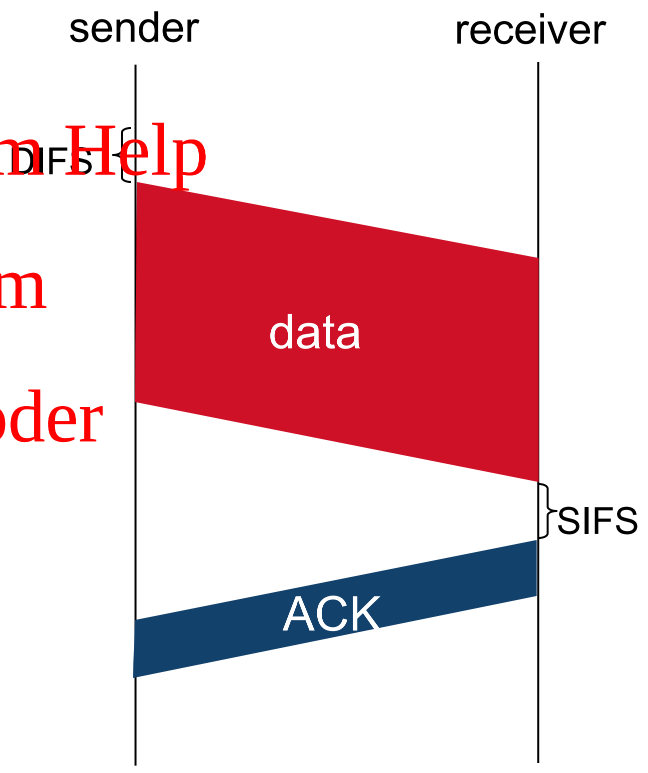
transmit when timer expires

802.11 receiver

- if frame received OK

return ACK after **SIFS** (Shorter inter-frame spacing)

Sender : if no ACK, increase random backoff interval, repeat 2



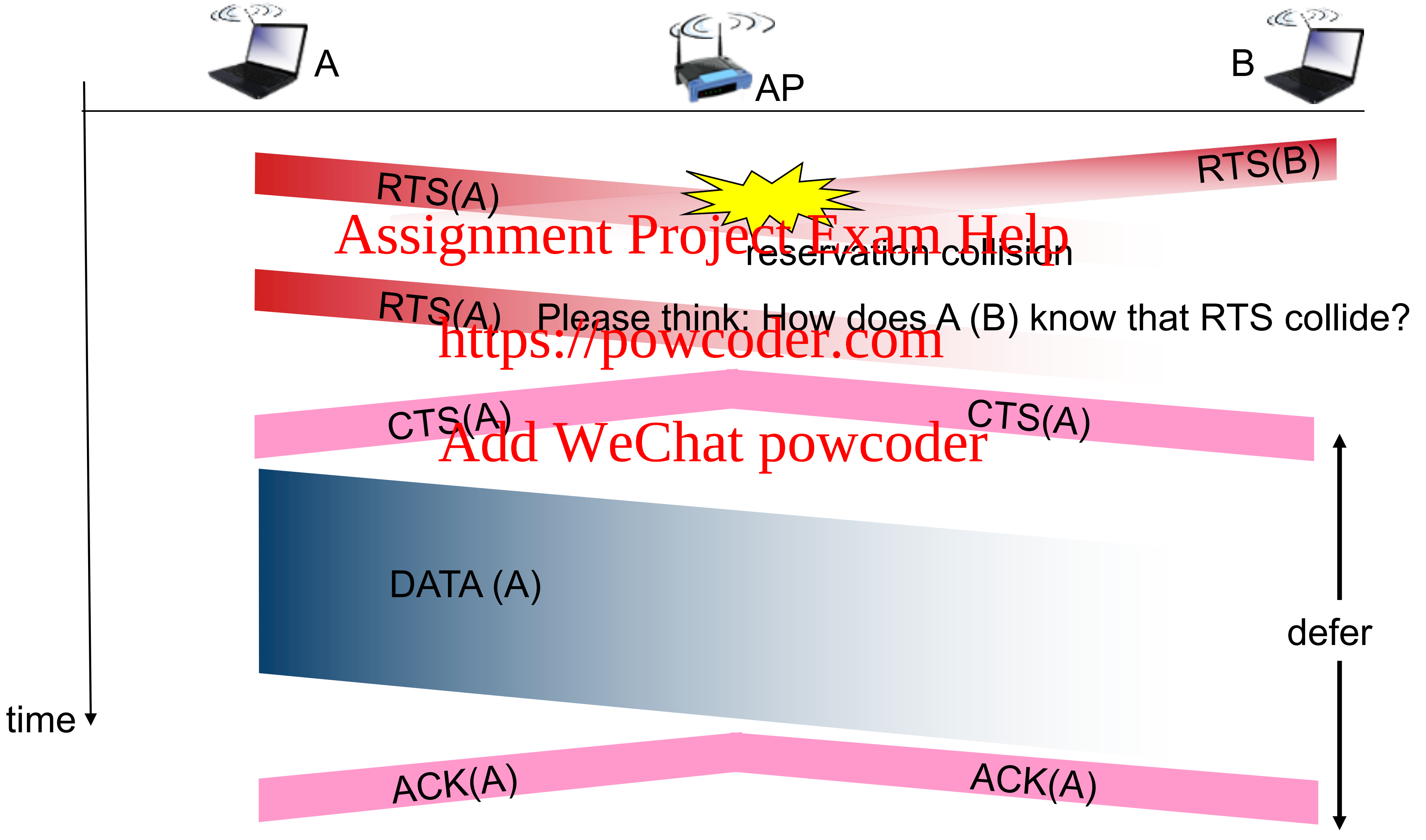
Avoiding collisions (more)

idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

avoid data frame collisions completely using small reservation packets!

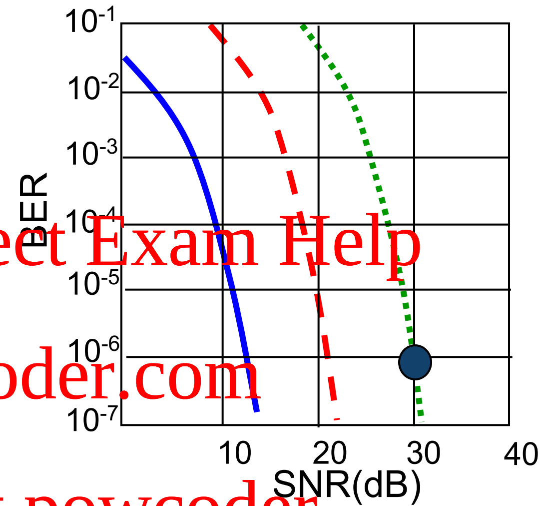
Collision Avoidance: RTS-CTS exchange



802.11: advanced capabilities

Rate adaptation

› base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies

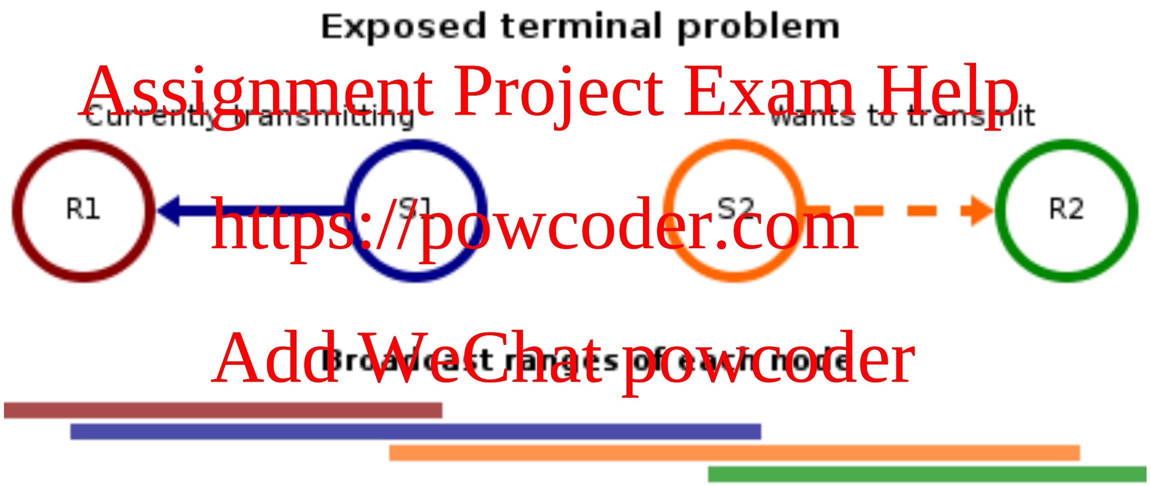


QAM256 (8 Mbps)
QAM16 (4 Mbps)
BPSK (1 Mbps)
operating point

1. SNR decreases, BER increase as node moves away from base station

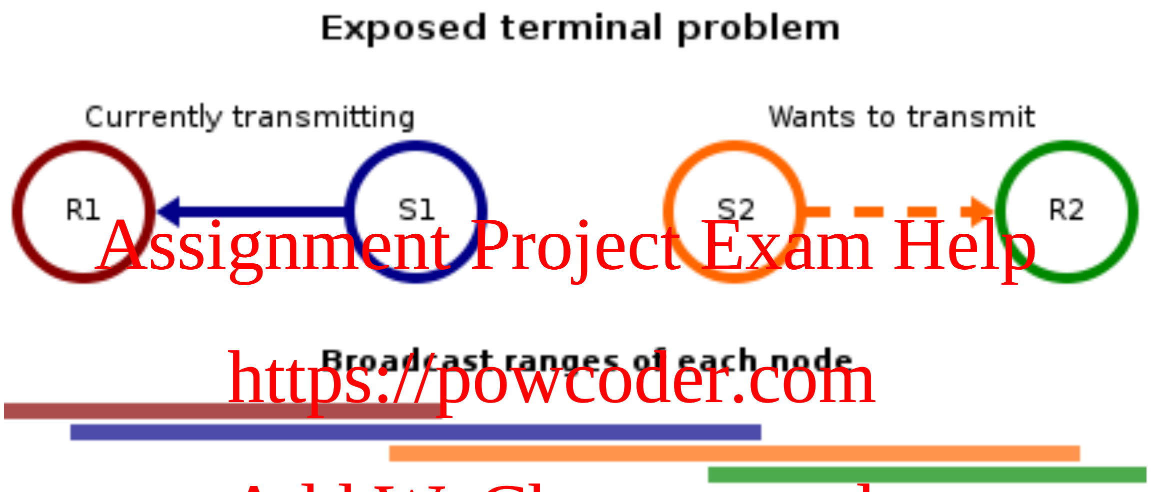
2. When BER becomes too high, switch to lower transmission rate but with lower BER

Exposed Terminal



Source: Wikipedia

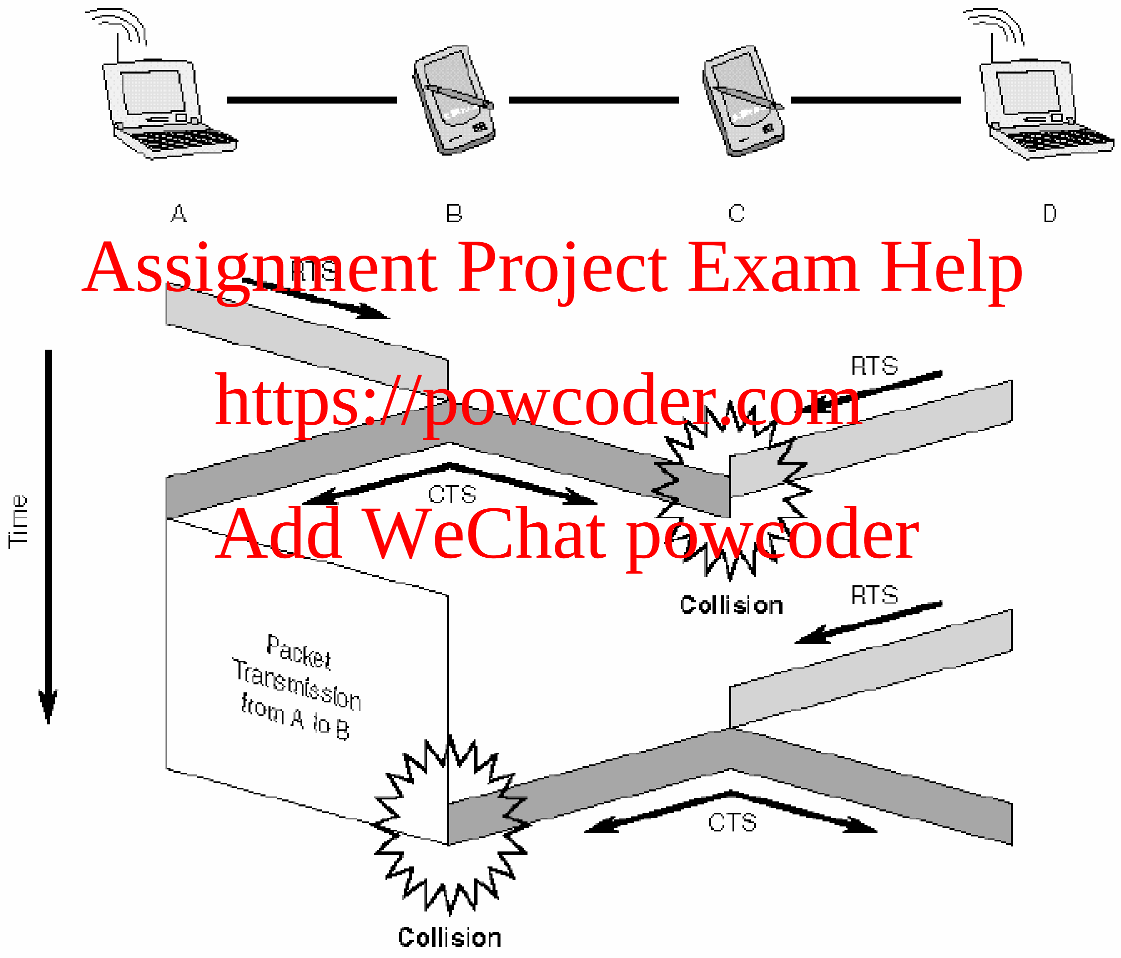
Exposed Terminal



Ideal: S1->R1 and S2->R2 simultaneously

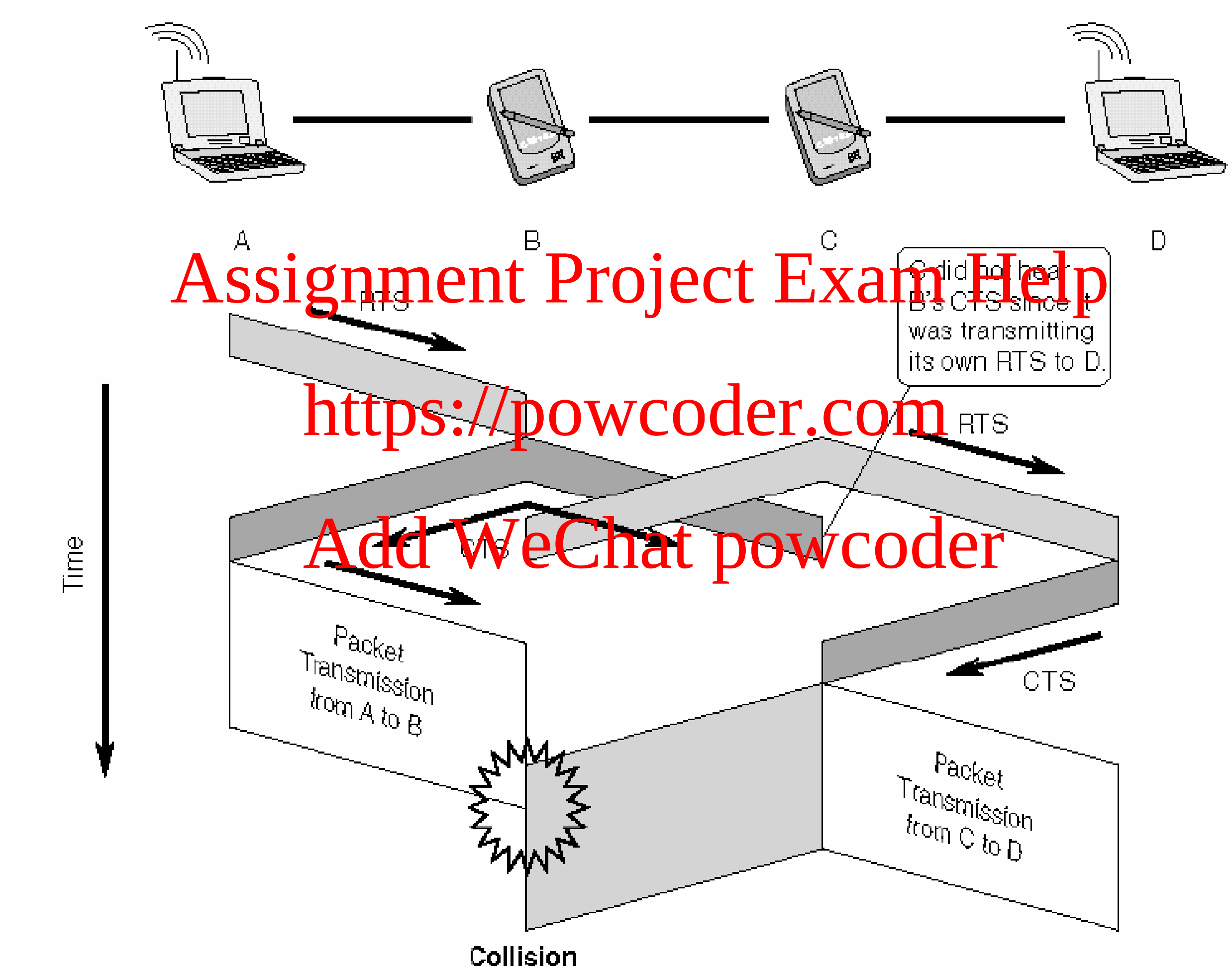
However: S2 can sense the carrier of S1 so that it keeps silence

Can RTS-CTS fail? Yes



Source: http://www.cs.jhu.edu/~cs647/mac_lecture_3.pdf

Can RTS-CTS fail? Yes



Source: http://www.cs.jhu.edu/~cs647/mac_lecture_3.pdf

Cellular Internet Access Architecture and standards

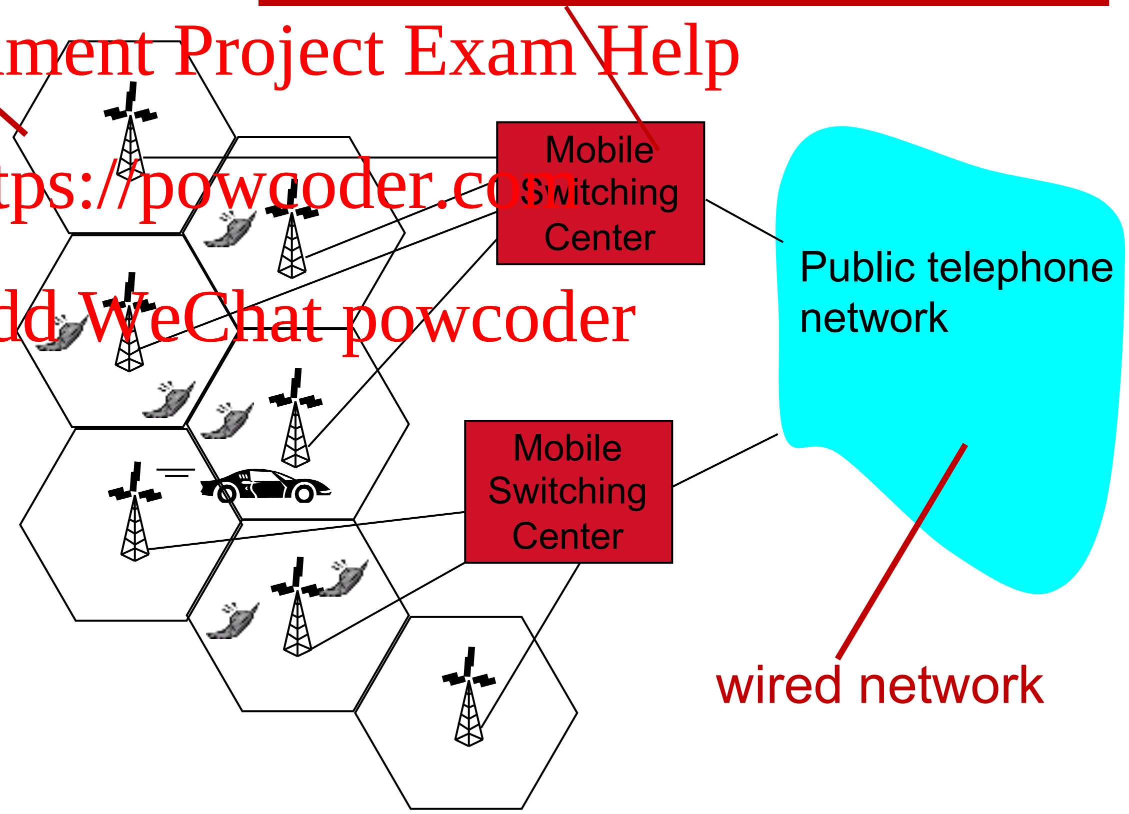
Components of cellular network architecture

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

MSC

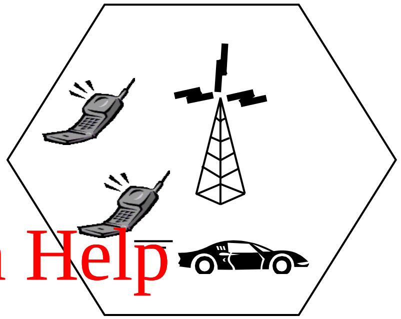
- connects cells to wired tel. net.
- manages call setup (more later!)
- handles mobility (more later!)

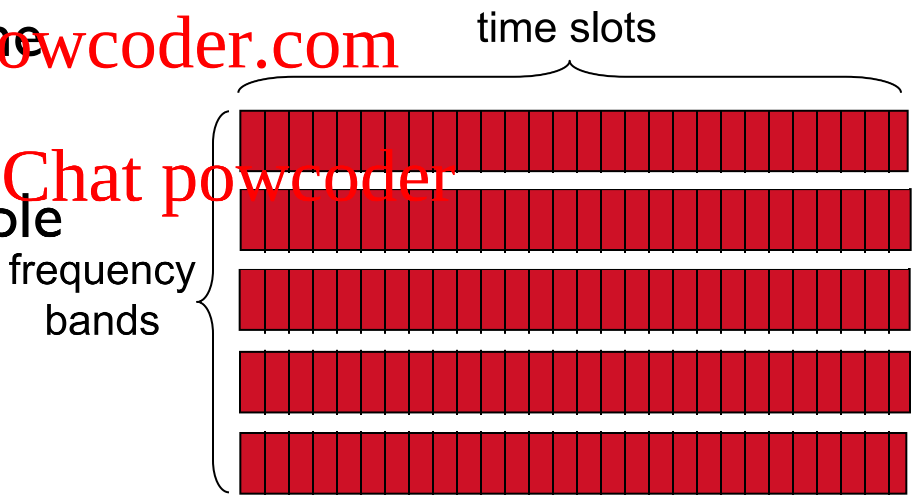


Cellular networks: the first hop

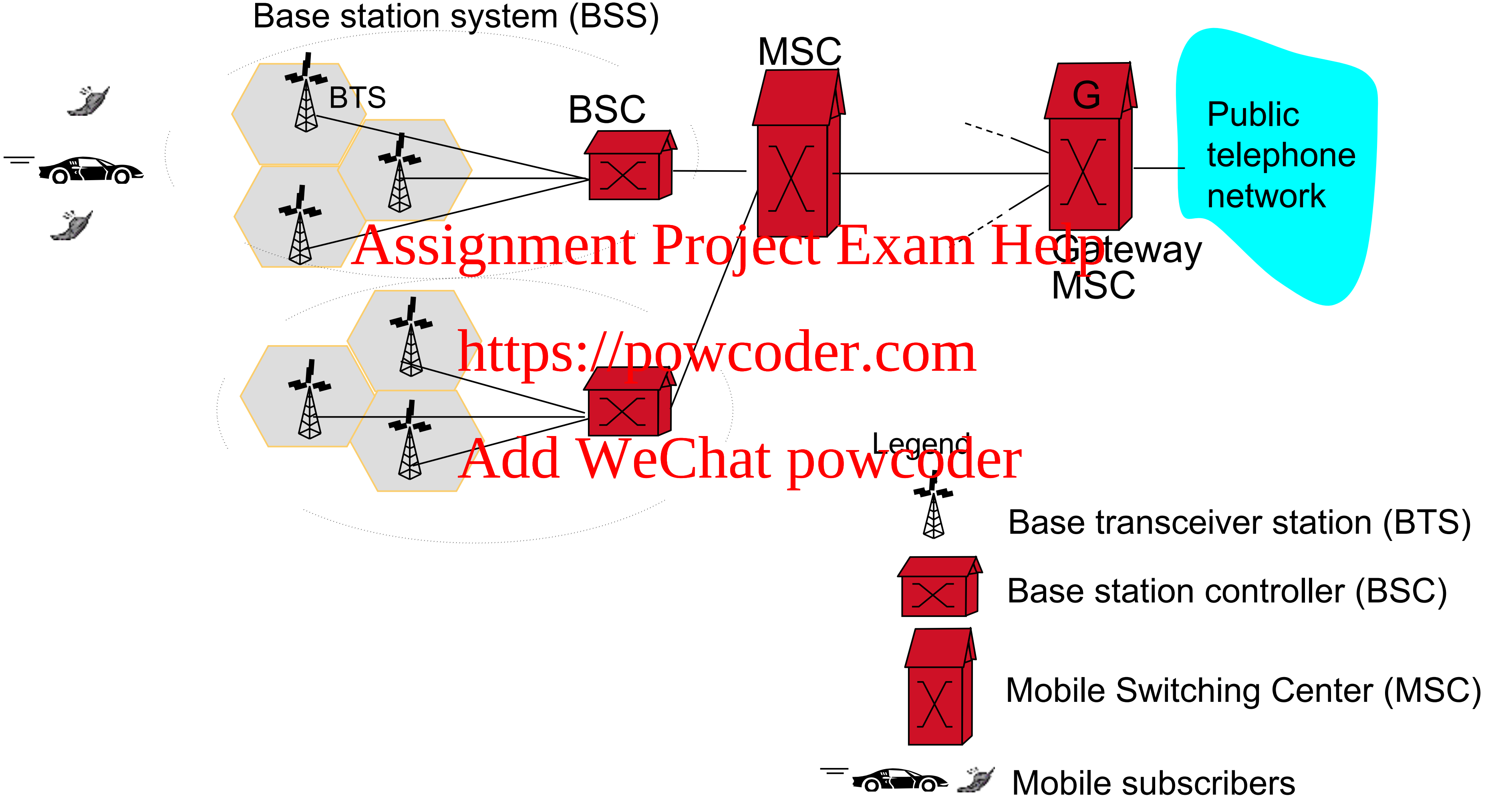
Two techniques for sharing mobile-to-BS radio spectrum

- combined FDMA/TDMA: divide spectrum in frequency channels, divide each channel into time slots
- CDMA: code division multiple access

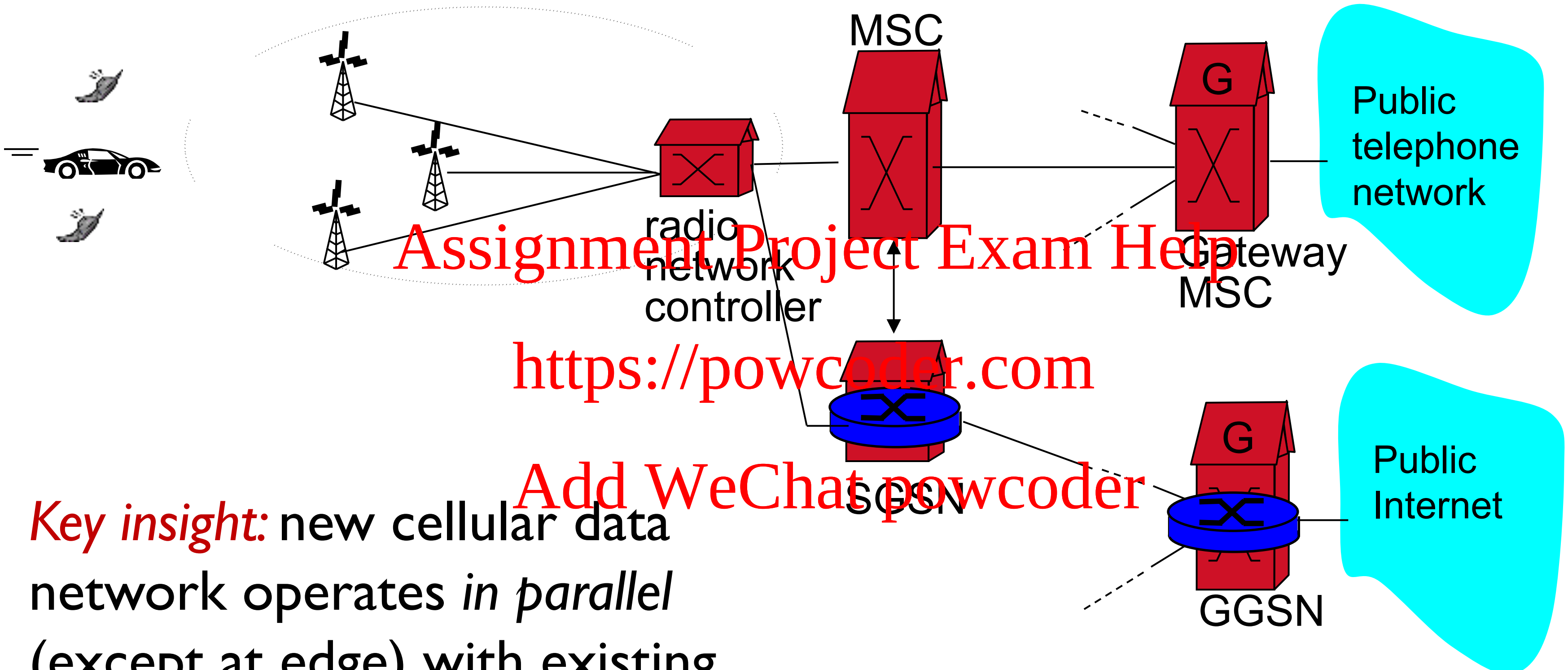




2G (voice) network architecture

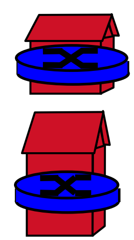


3G (voice+data) network architecture



Key insight: new cellular data network operates *in parallel* (except at edge) with existing cellular voice network

- voice network unchanged in core
- data network operates in parallel

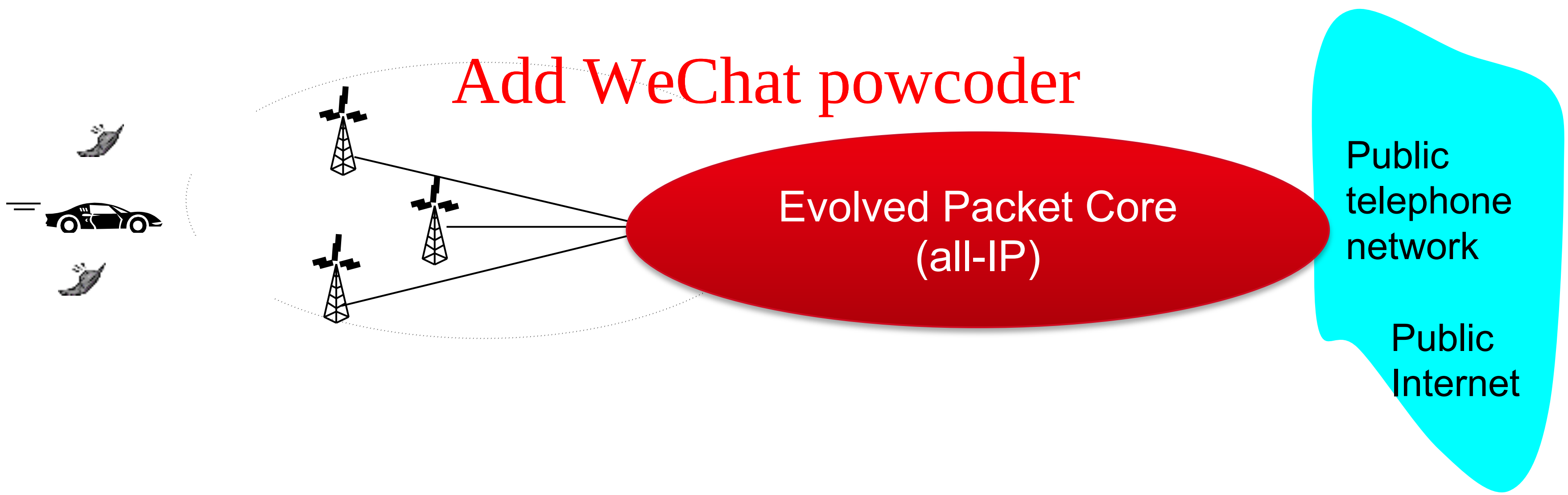


General Packet Radio Service

4G: Long-Term Evolution (LTE)

Two important innovations over 3G

1. Evolved packet core (EPC): simplified all-IP core network that unifies the cellular circuit-switched voice network and the packet switched cellular data network.

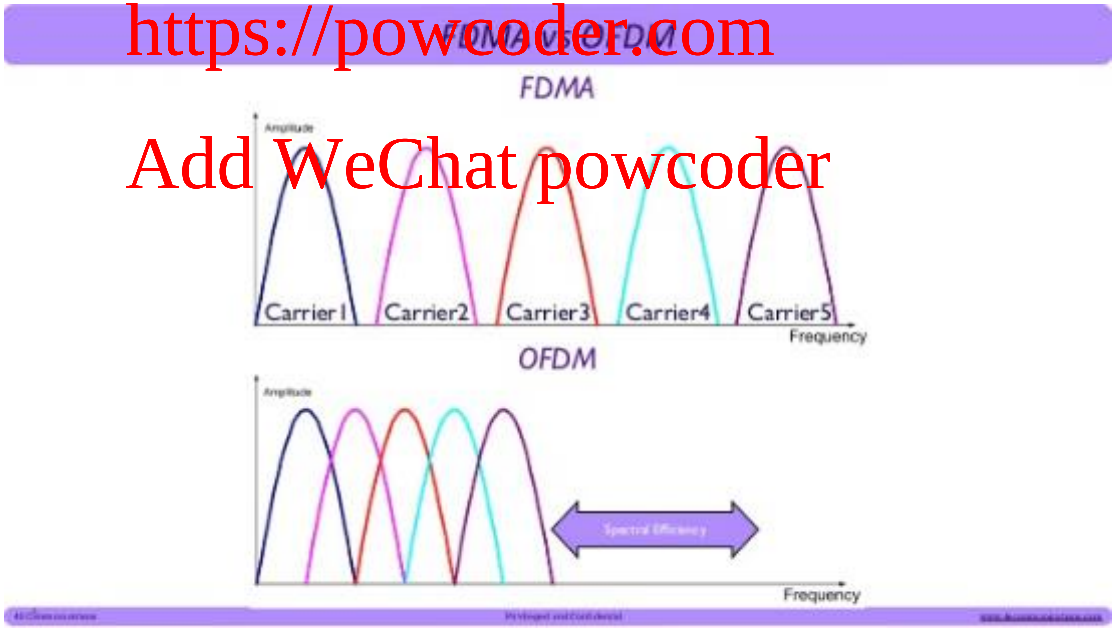


THE UNIVERSITY OF SYDNEY

4G: Long-Term Evolution (LTE)

Two important innovations over 3G

2. LTE Radio Access Networks: uses a combination of orthogonal frequency-division multiplexing (OFDM) and time division multiplexing.

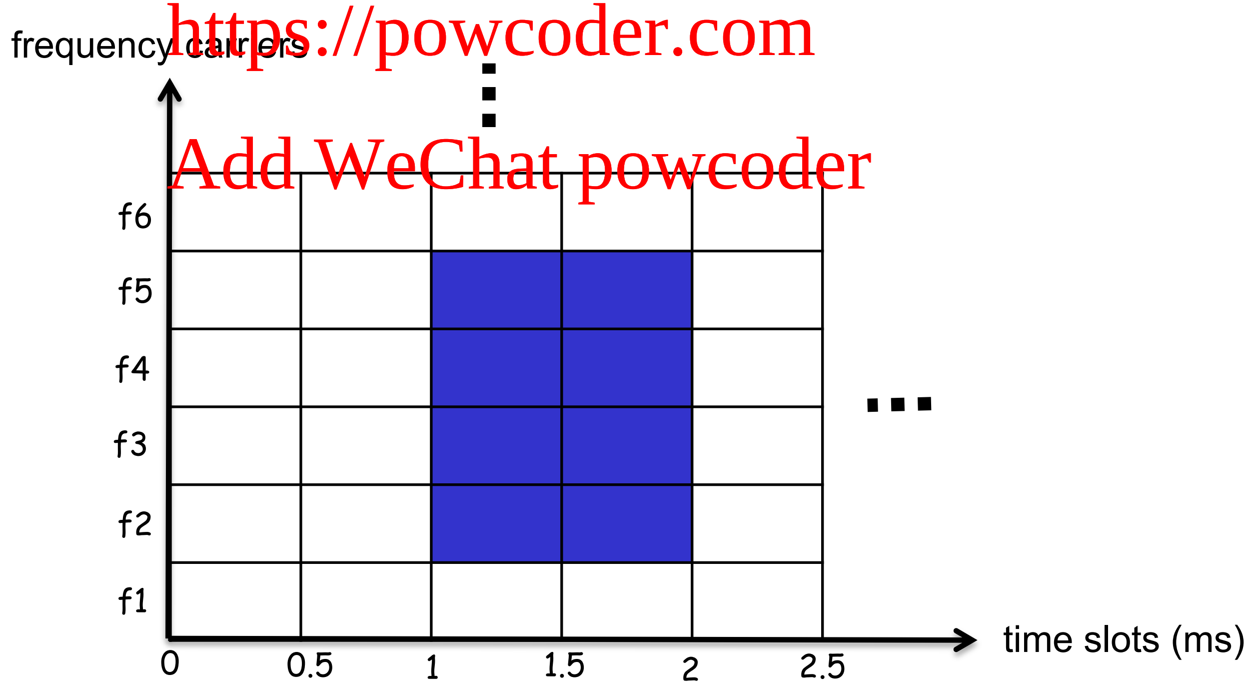


http://www.slideshare.net/ravi4s/modulation-multiple-acces-schemes

4G: Long-Term Evolution (LTE)

Two important innovations over 3G

2. **LTE Radio Access Networks:** uses a combination of orthogonal frequency-division multiplexing (OFDM) and time division multiplexing.



Mobility principles: Addressing and routing to mobile users

What is mobility?

› spectrum of mobility, from the *network* perspective:

mobile wireless user, using same access point

mobile user, disconnecting from network when moving.

mobile user, passing through multiple access point while maintaining ongoing connections (like cell phone)

Should Address always remain the same?

- Mobile phone: the phone number remains the same at all time when you travel

- How about IP Address?

Mobility: vocabulary

home network: permanent "home" of mobile
(e.g., 128.119.40/24)

home agent: entity that will perform mobility functions on behalf of mobile

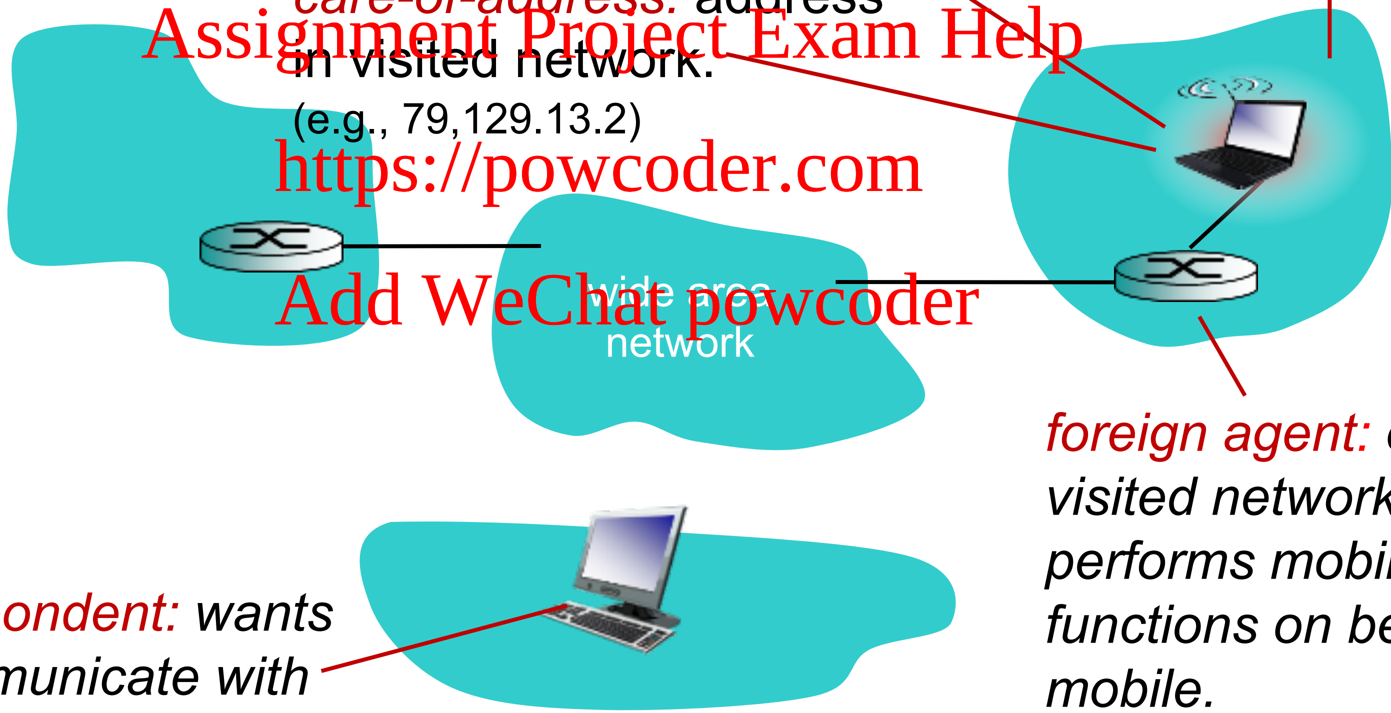
permanent address:
address in home network, *can always* be used to reach mobile
e.g., 128.119.40.186

Mobility: more vocabulary

permanent address: remains constant (e.g., 128.119.40.186)

Foreign (visited) network: network in which mobile currently resides (e.g., 79.129.13/24)

care-of-address: address in visited network. (e.g., 79,129.13.2)



foreign agent: entity in visited network that performs mobility functions on behalf of mobile.

correspondent: wants to communicate with mobile

How do *you* contact a mobile friend:

Consider friend frequently changing addresses, how do you find her?

- search all phone books?
- call her parents?
- expect her to let you know where he/she is?

Mobility: approaches

- *let routing handle it:* routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.
  - routing tables indicate where each mobile located
  - no changes to end-systems
- *let end-systems handle it:*
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

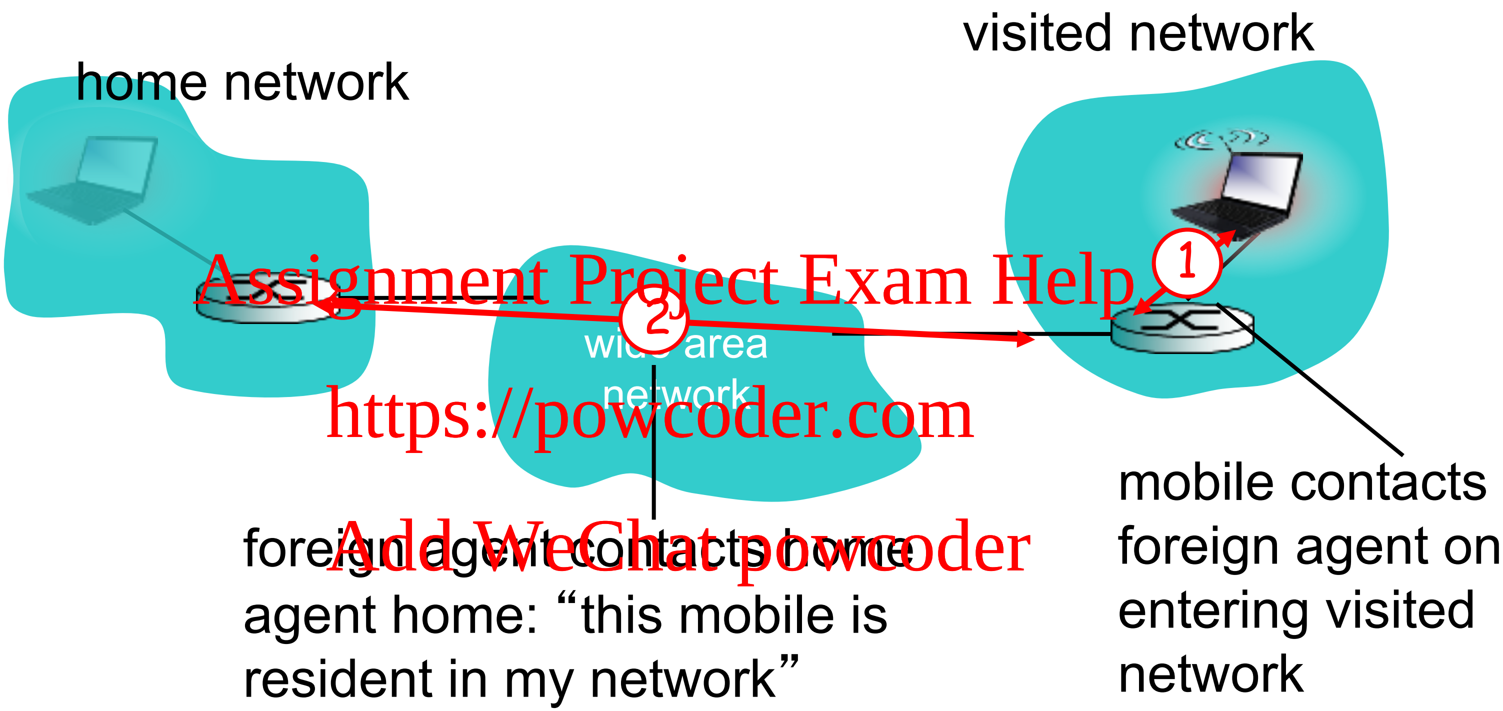
Mobility: approaches

- *let routing handle it:* rout[illegible]ertise permanent address of mobile-nodes-in-resi[illegible]al routing table exchange.
  - routing tables indicate w[illegible]ated
  - no changes to end-system[illegible]

not
scalable
to millions of
mobiles

- *let end-systems handle it:*
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

Mobility: registration

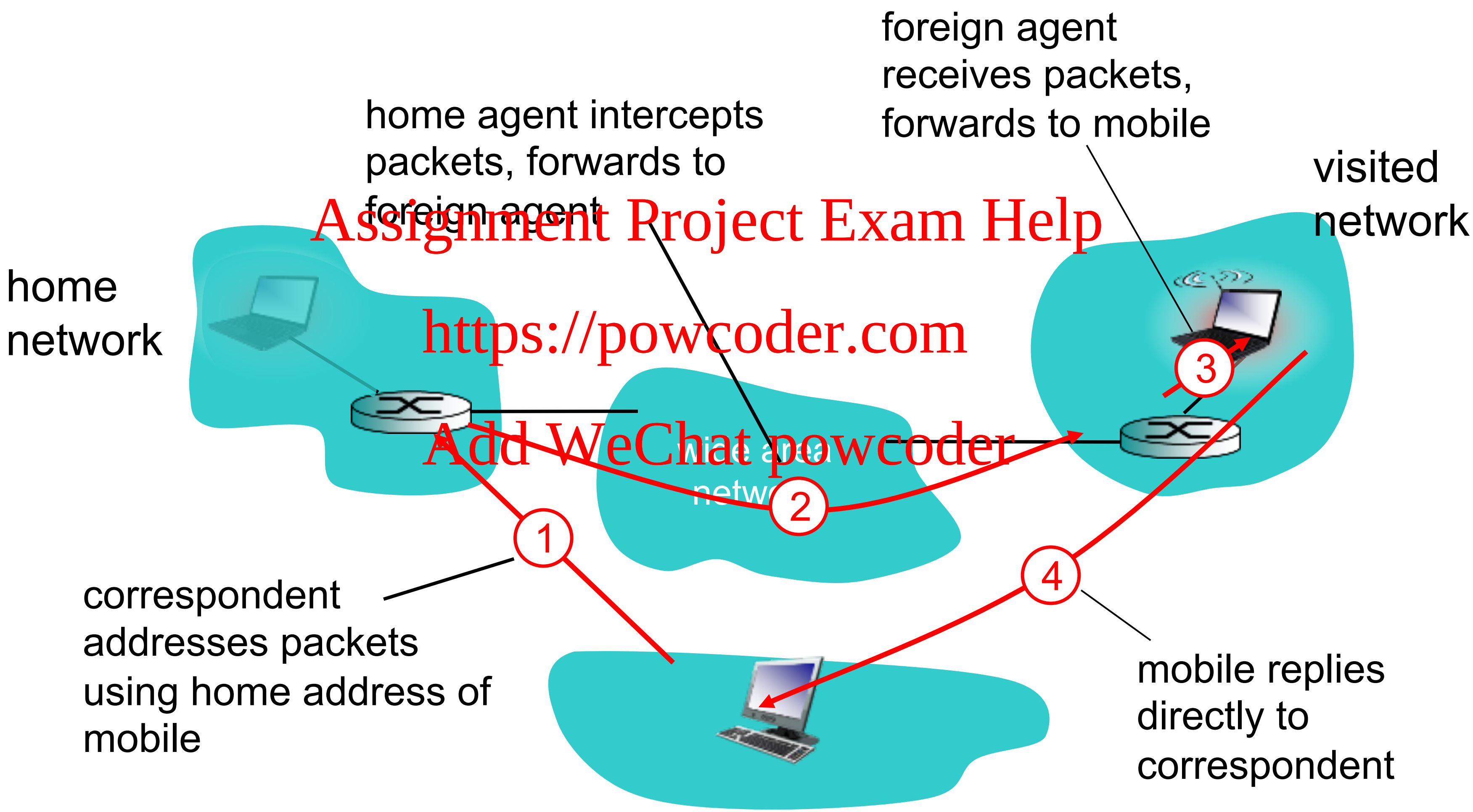


end result:

› foreign agent knows about mobile

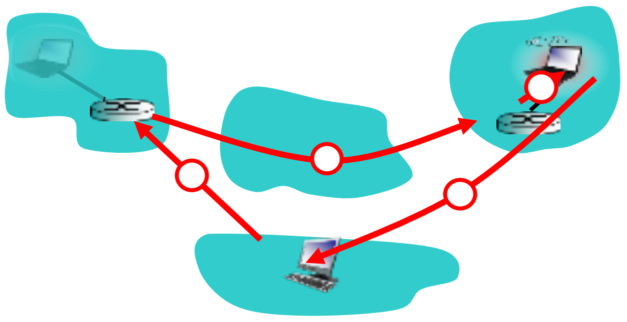
› home agent knows location of mobile

Mobility via indirect routing



Indirect Routing: comments

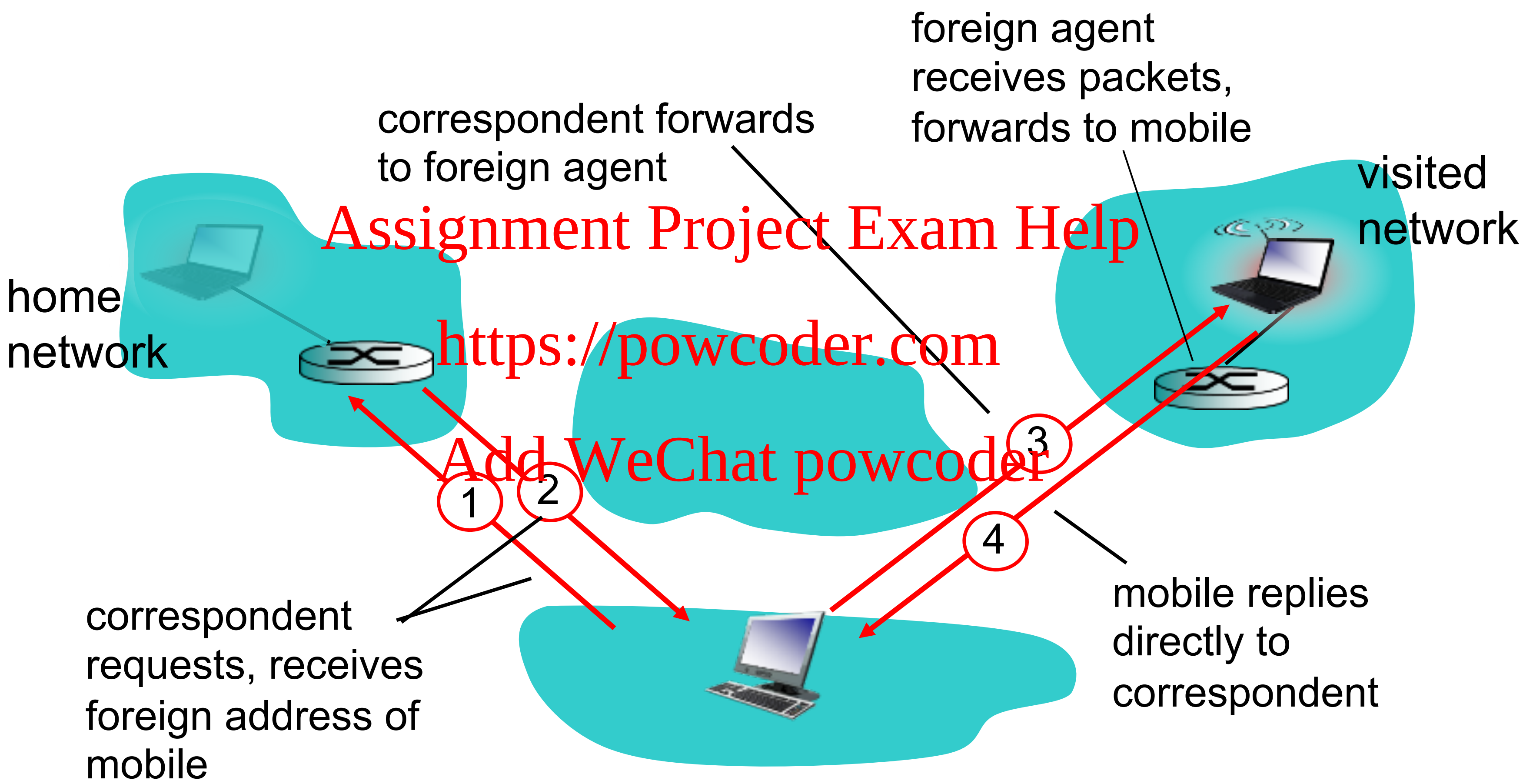
- mobile uses two addresses:
  - permanent address: used by correspondent (hence mobile location is *transparent* to correspondent)
  - care-of-address: used by home agent to forward datagrams to mobile
- triangle routing: correspondent-home-network-mobile
  - inefficient when correspondent, mobile are in same network



Indirect routing: moving between networks

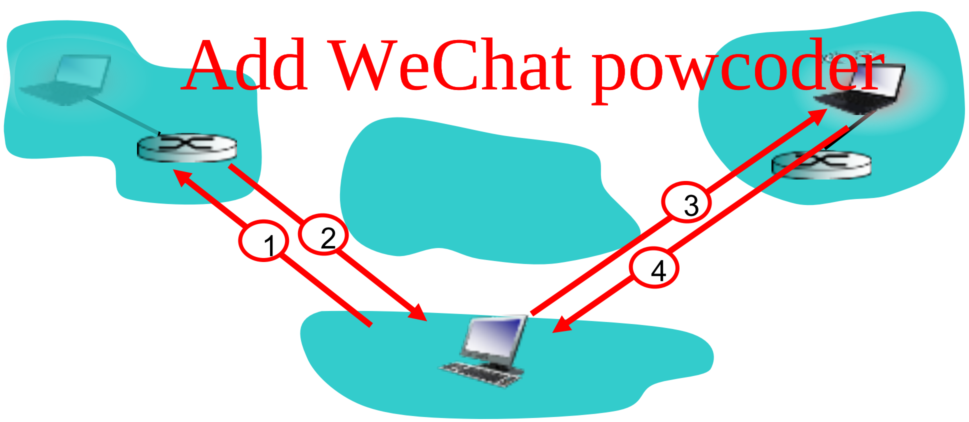
- suppose mobile user moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)
- changing foreign networks transparent: *on going connections can be maintained!*

Mobility via direct routing



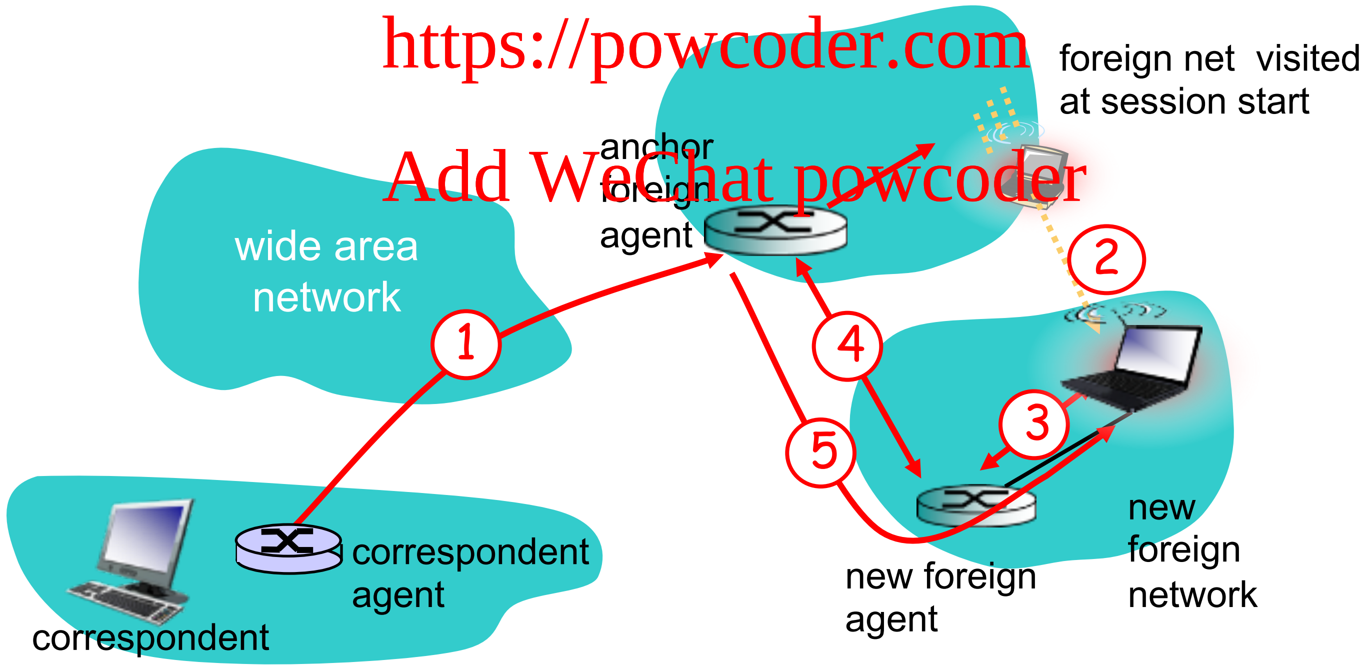
Mobility via direct routing: comments

- overcome triangle routing problem
- *non-transparent to correspondent:* correspondent must get care-of-address from home agent
  - what if mobile changes visited network?



Accommodating mobility with direct routing

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

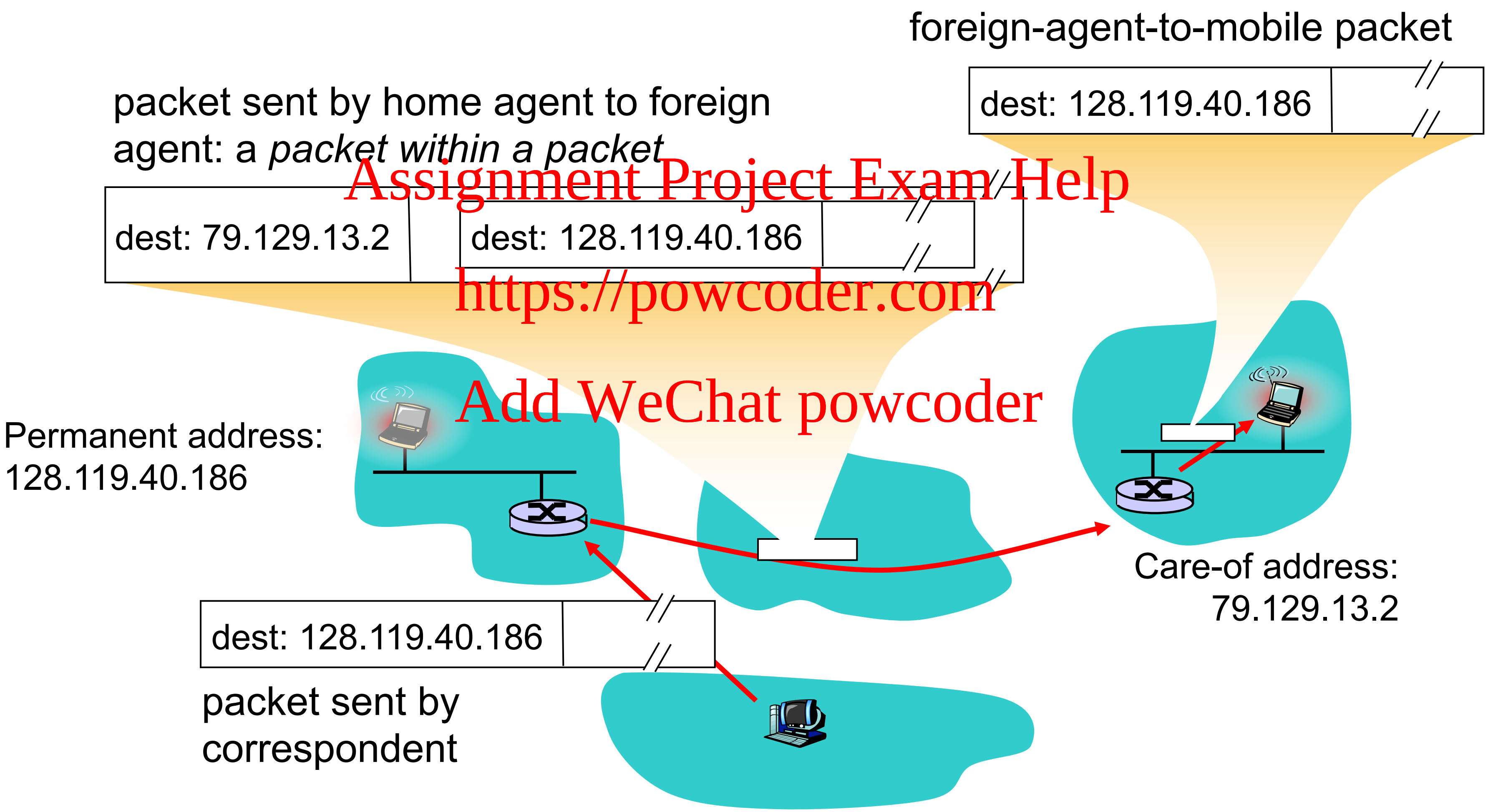


Mobile IP

Mobile IP

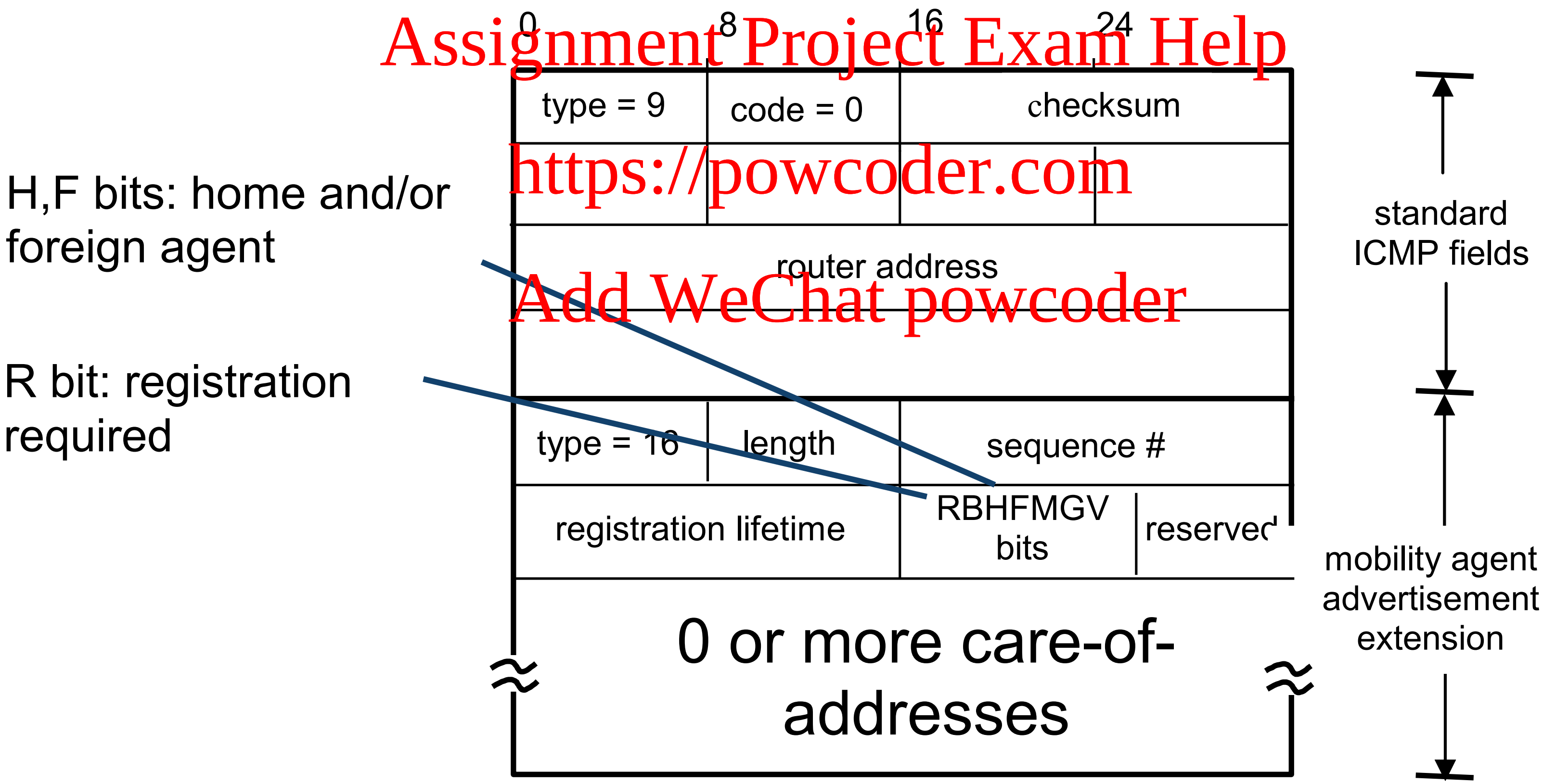
- RFC 3344
- has many features we have seen:
  - home agents, foreign agents, foreign-agent registration, care-of-addresses
- three components to standard:
  - indirect routing of datagrams
  - agent discovery
  - registration with home agent

Mobile IP: indirect routing

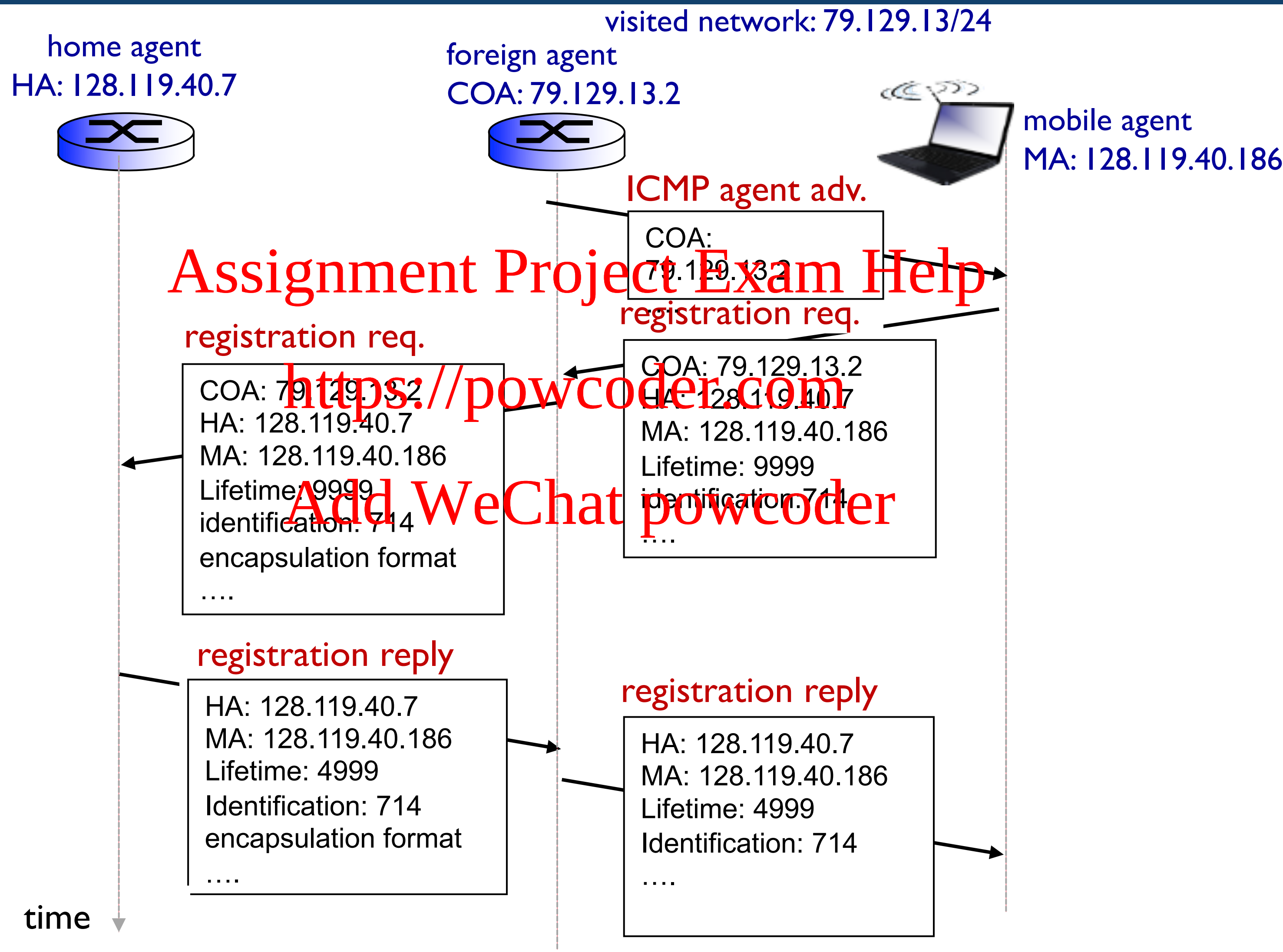


Mobile IP: agent discovery

› *agent advertisement:* foreign/home agents advertise service by broadcasting ICMP (Internet Control Message Protocol) messages (typefield = 9)



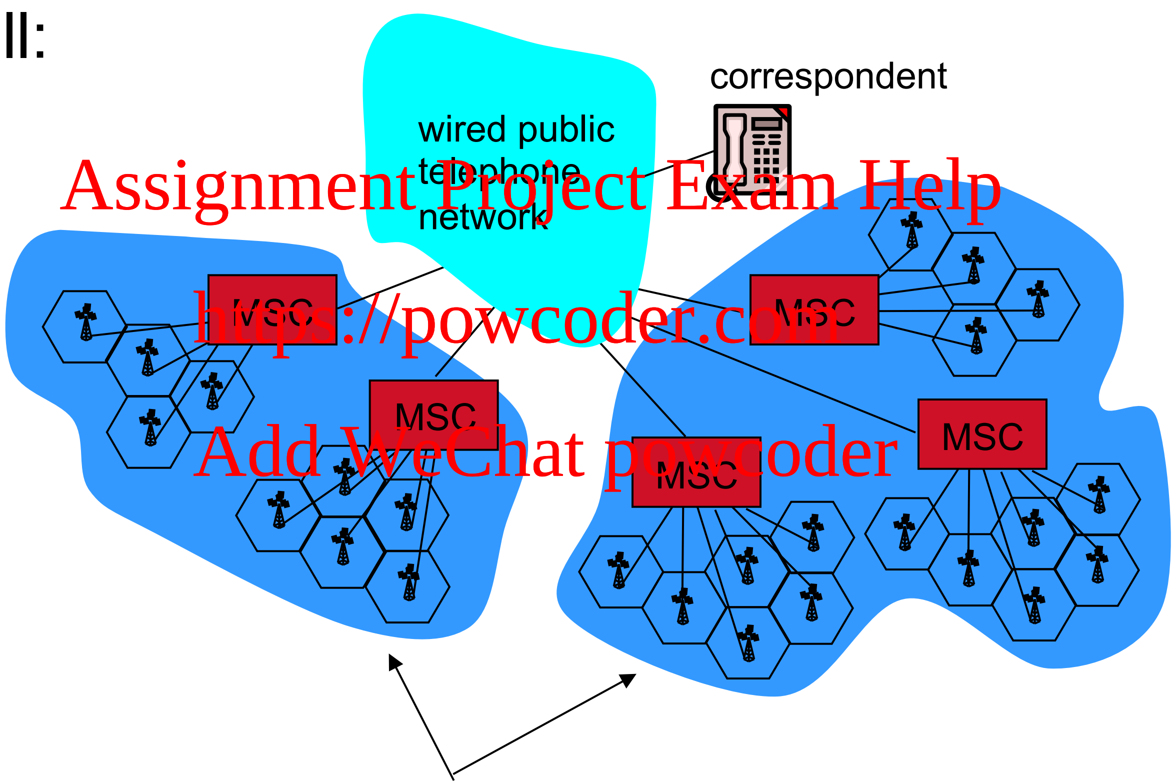
Mobile IP: registration example



Mobility in Cellular Networks

Components of cellular network architecture

recall:

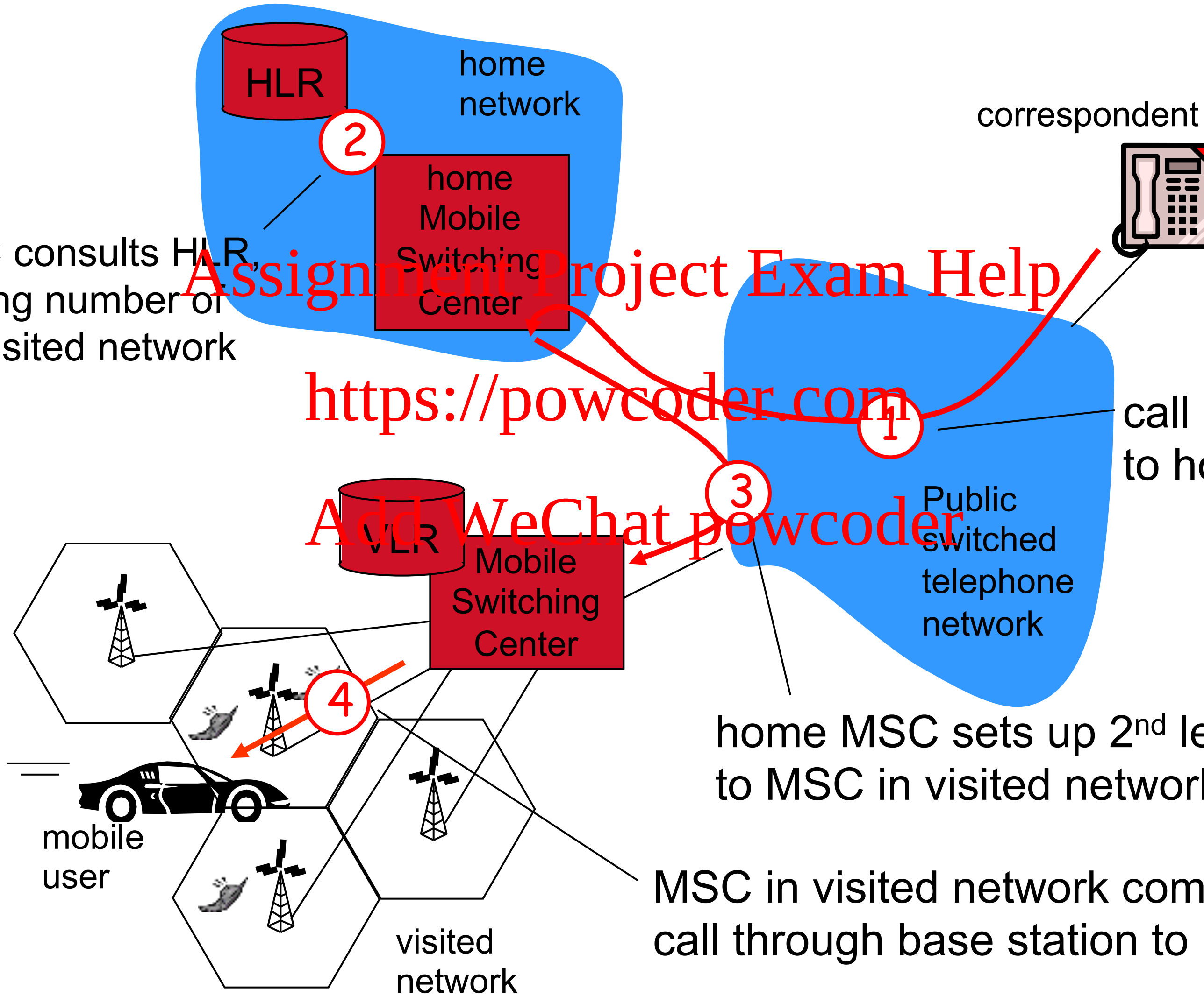


different cellular networks,
operated by different providers

Handling mobility in cellular networks

- *home network:* network of cellular provider you subscribe to (e.g., Vodafone)
  - *home location register (HLR):* database in home network containing permanent cell phone #, profile information (services, preferences, billing), information about 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
  - could be home network

GSM: indirect routing to mobile



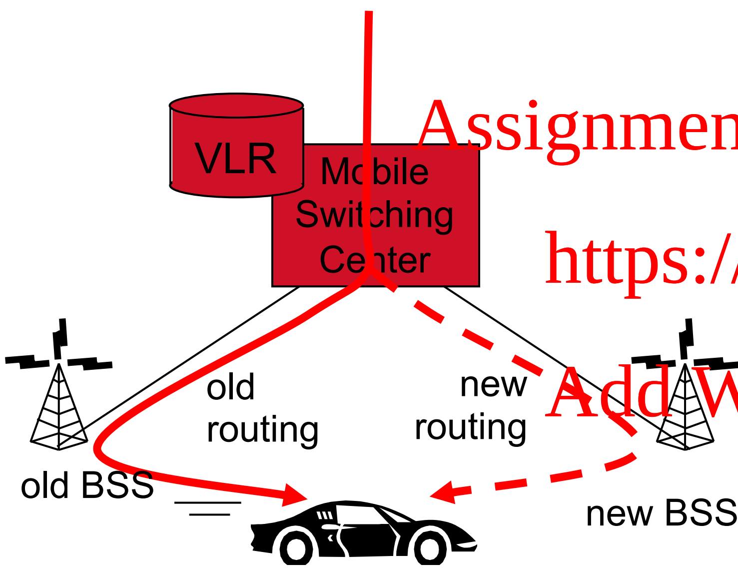
home MSC consults HLR, gets roaming number of mobile in visited network

call routed to home network

home MSC sets up 2nd leg of call to MSC in visited network

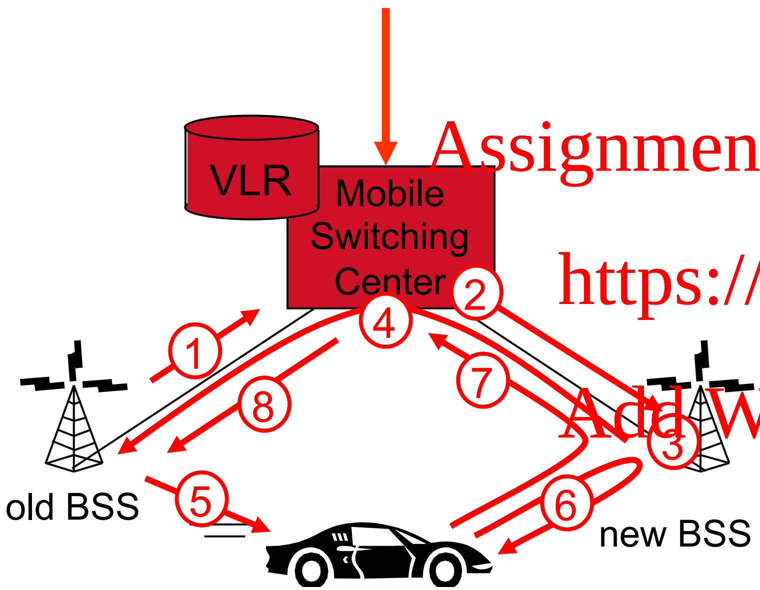
MSC in visited network completes call through base station to mobile

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
- handoff initiated by old BSS

GSM: handoff with common MSC

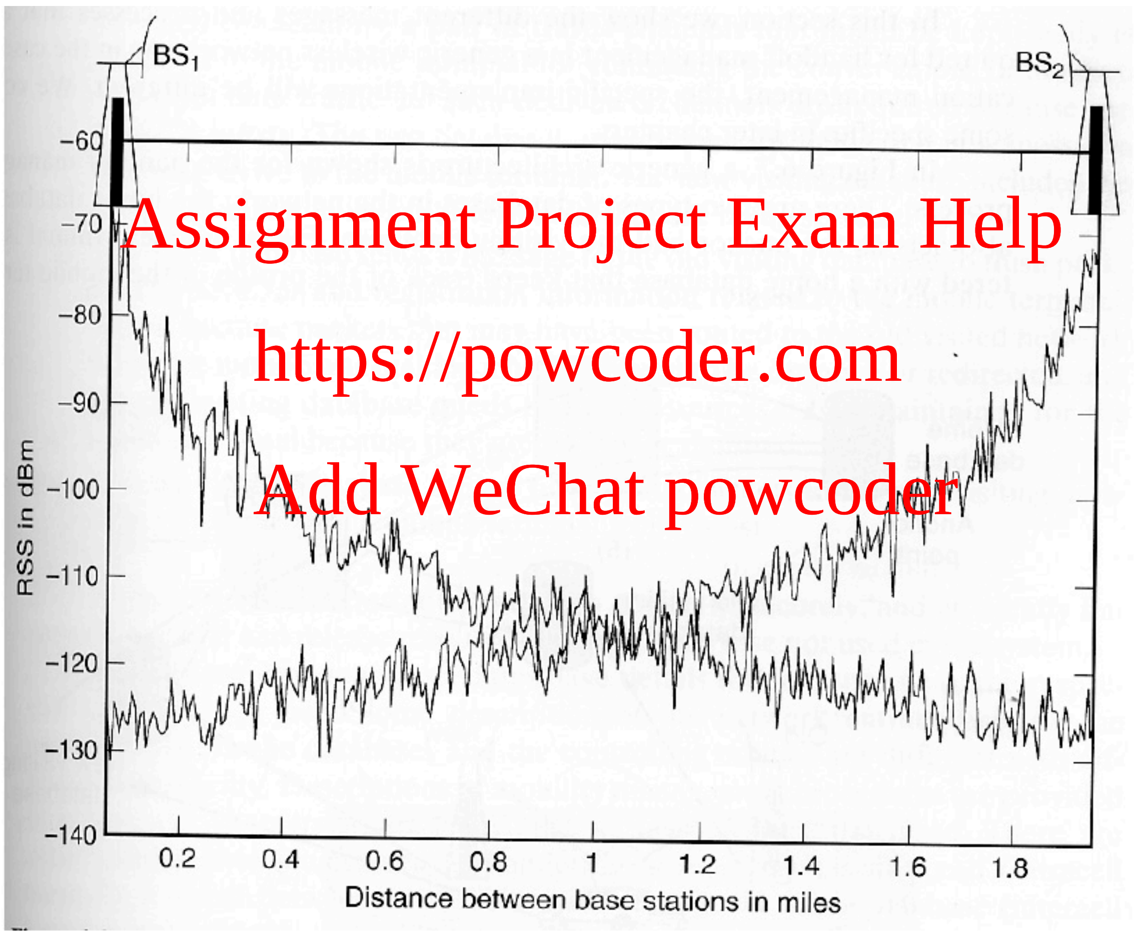


1. old BSS informs MSC of impending handoff, provides list of 1^+ new BSSs
2. MSC sets up path (allocates resources) to new BSS
3. new BSS allocates radio channel for use by mobile
4. new BSS signals MSC, old BSS: ready
5. old BSS tells mobile: perform handoff to new BSS
6. mobile, new BSS signal to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

8 MSC-old BSS resources released

THE UNIVERSITY OF SYDNEY

Handoff algorithm: a brief overview

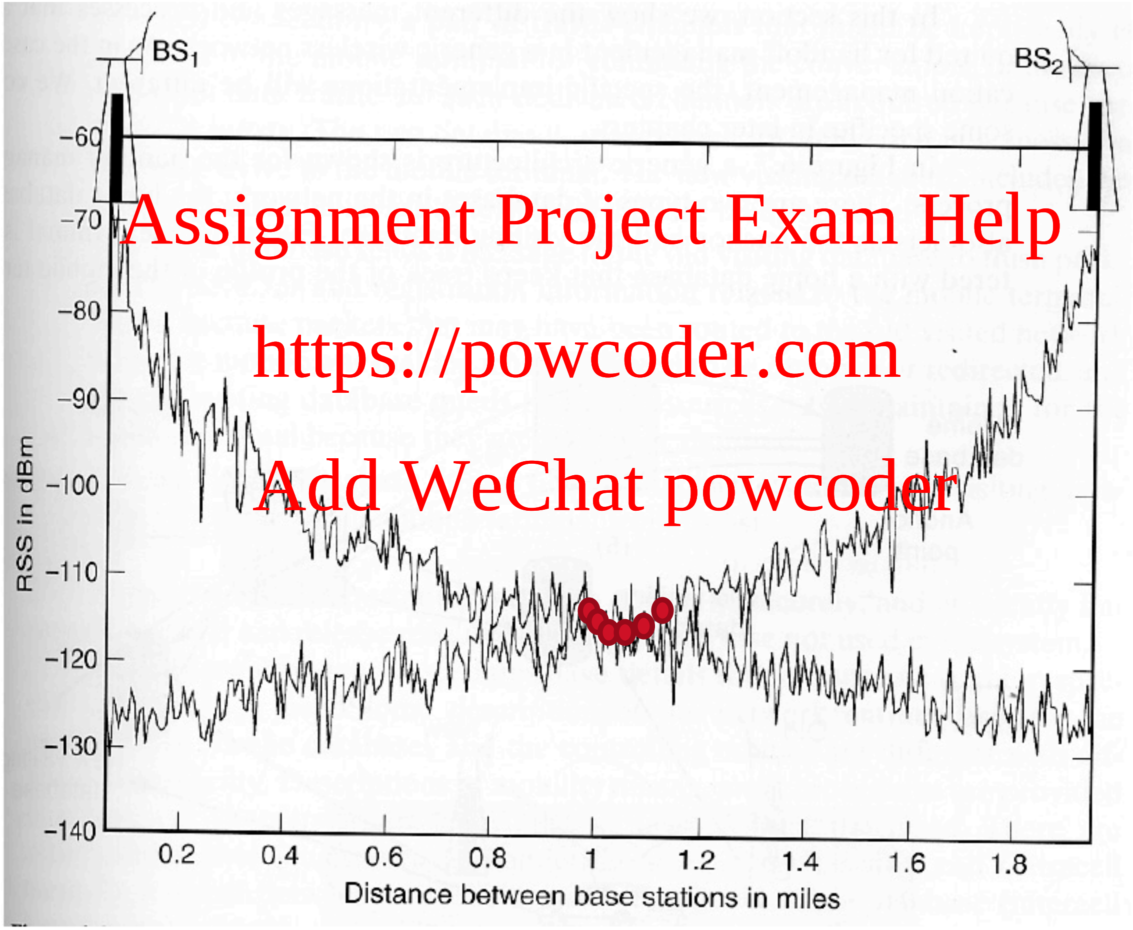


Signal Strength of Two Base Stations: when to handoff?

Handoff algorithm: a brief overview

- Naive way: Compare the RSSs (Received Signal Strength) of two BSs Handoff at
  - $P_{new} > P_{old}$

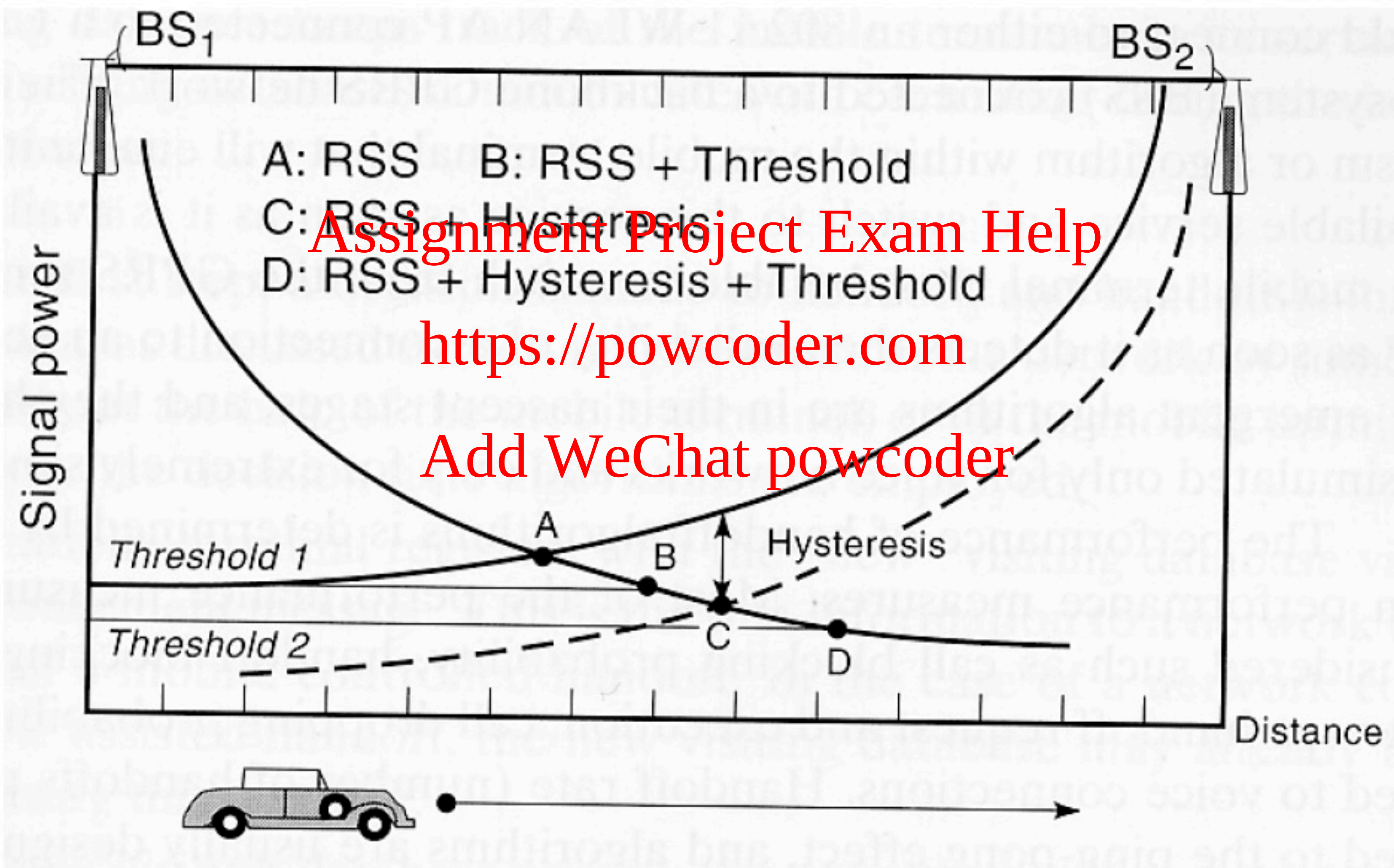
Ping-pong effect



Handoff back and forth.

Smarter ways

- RSS: initiate handoff to BS new if
  - $P_{new} > P_{old}$
- RSS with threshold(PT): choose BS new if
  - $P_{new} > P_{old}$ and $P_{old} < P_T$
- RSS with hysteresis(PH): choose BS new if
  - $P_{new} > P_{old} + P_H$
- RSS with threshold(PT) and hysteresis(PH): choose BS new if
  - $P_{new} > P_{old} + P_H$ and $P_{old} < P_T$
- Even better: Add a Dwell Timer to the above algorithms: start timer when above condition is met; initiate handoff if condition persists when timer expires



BS1
BS2
A: RSS
B: RSS + Threshold
C: RSS + Hysteresis
D: RSS + Hysteresis + Threshold
Signal power
Threshold 1
Threshold 2
A
B
C
D
Hysteresis
Distance

THE UNIVERSITY OF SYDNEY

Wireless, mobility: impact on higher layer protocols

- logically, impact *should* be minimal …
  - best effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile
- … but performance-wise:
  - packet loss/delay due to bit-errors (discarded packets, delays for link-layer retransmissions), and handoff
  - TCP interprets loss as congestion, will decrease congestion window un-necessarily
  - delay impairments for real-time traffic