TOPIC 3
WIRELESS NETWORK

WANG ZHANQUAN

6 WIRELESS NETWORK

6.1 Introduction of wireless network

6.2 wireless network

6.3 wireless Ad hoc's network

Ch. 6: Wireless

Background:

- # wireless (mobile) phone subscribers now exceeds # wired phone subscribers (5-to-1)!
- # wireless Internet-connected devices equals # wireline Internet-connected devices
  - laptops, Internet-enabled phones promise anytime untethered Internet access
- two important (but different) challenges
  - *wireless:* communication over wireless link
  - *mobility:* handling the mobile user who changes point of attachment to network

Chapter 6 outline

6.1 Introduction

Wireless

6.2 Wireless links, characteristics

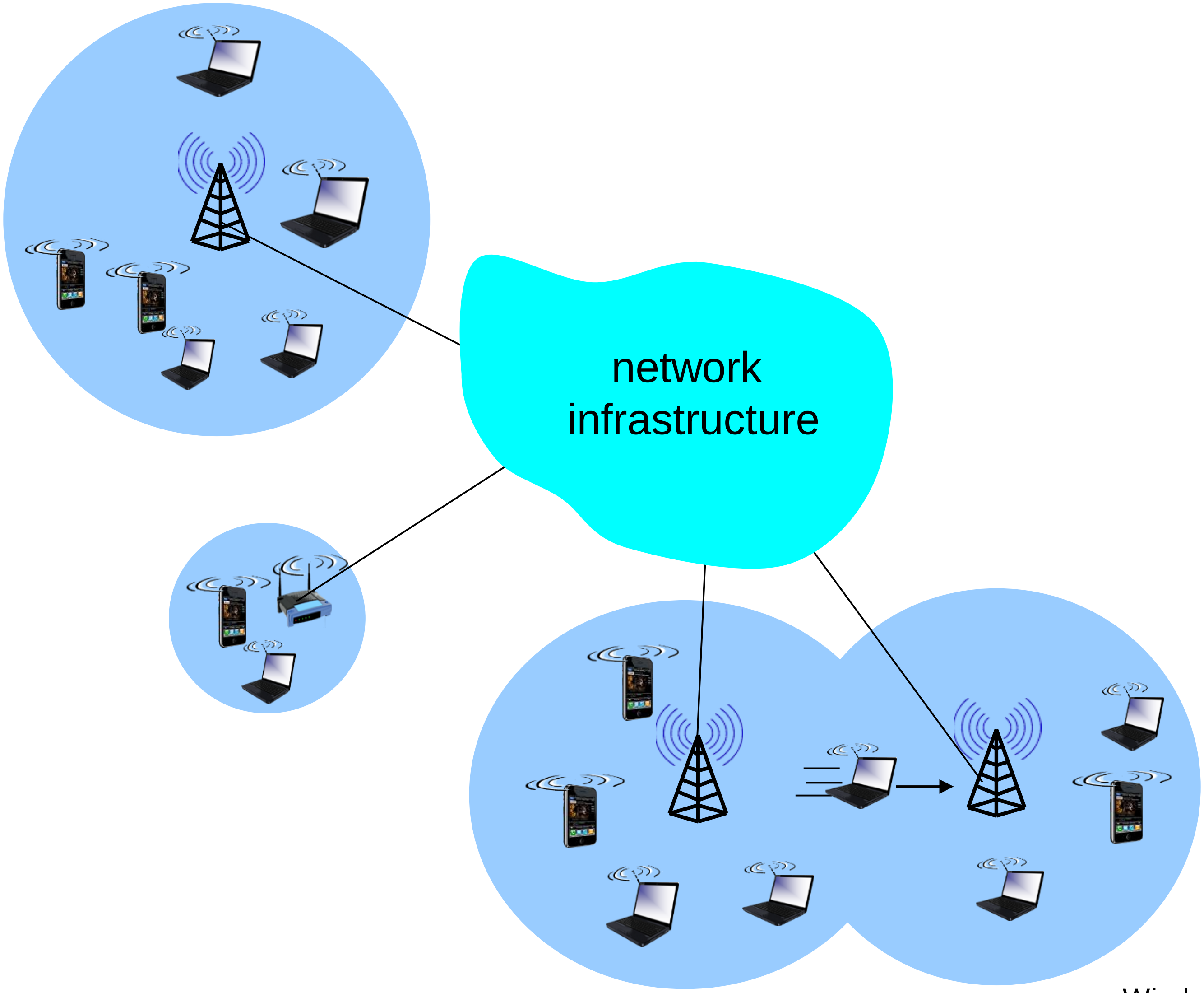
- CDMA

6.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

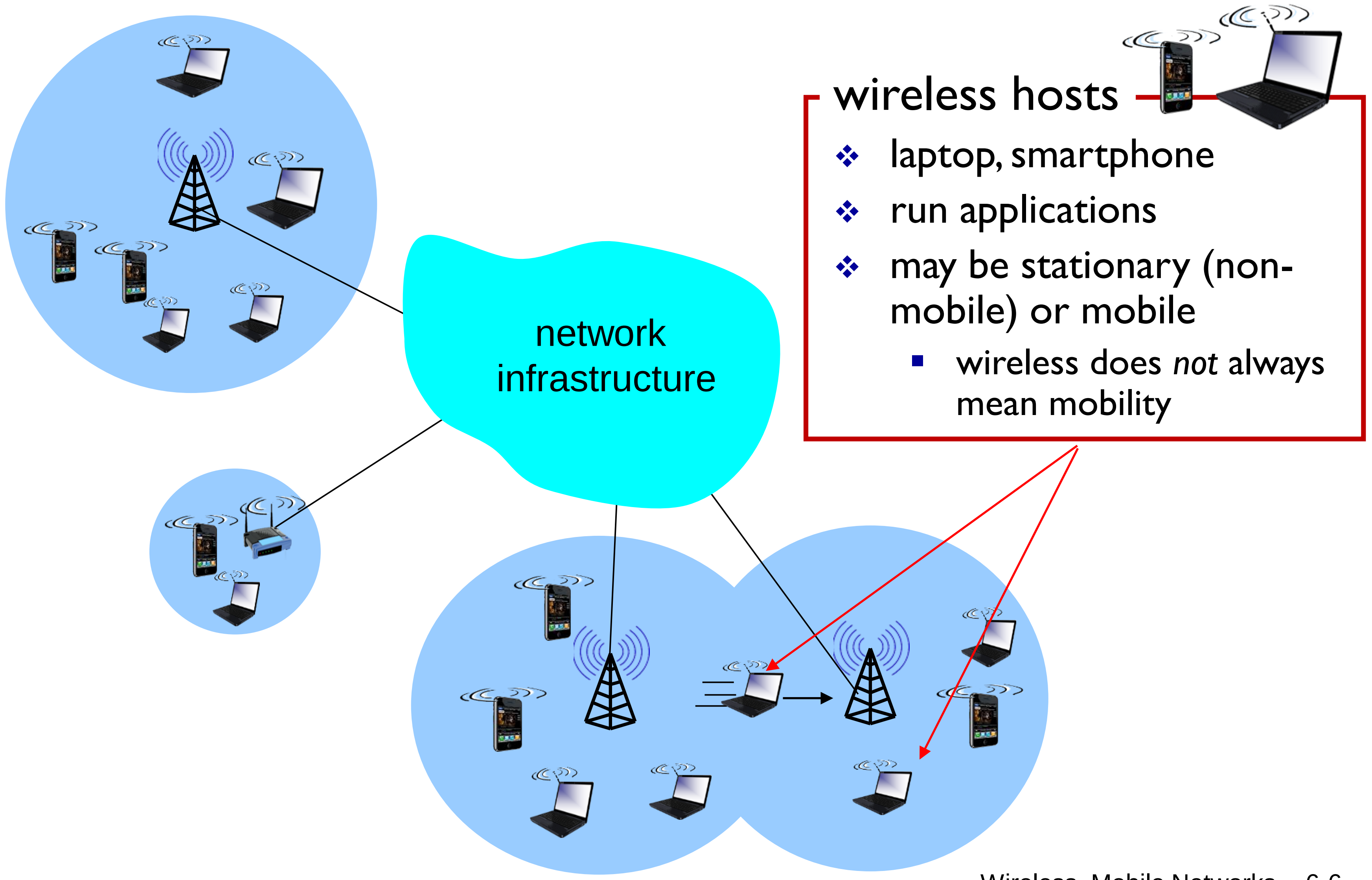
6.4 Cellular Internet Access

- architecture
- standards (e.g., GSM)

Elements of a wireless network



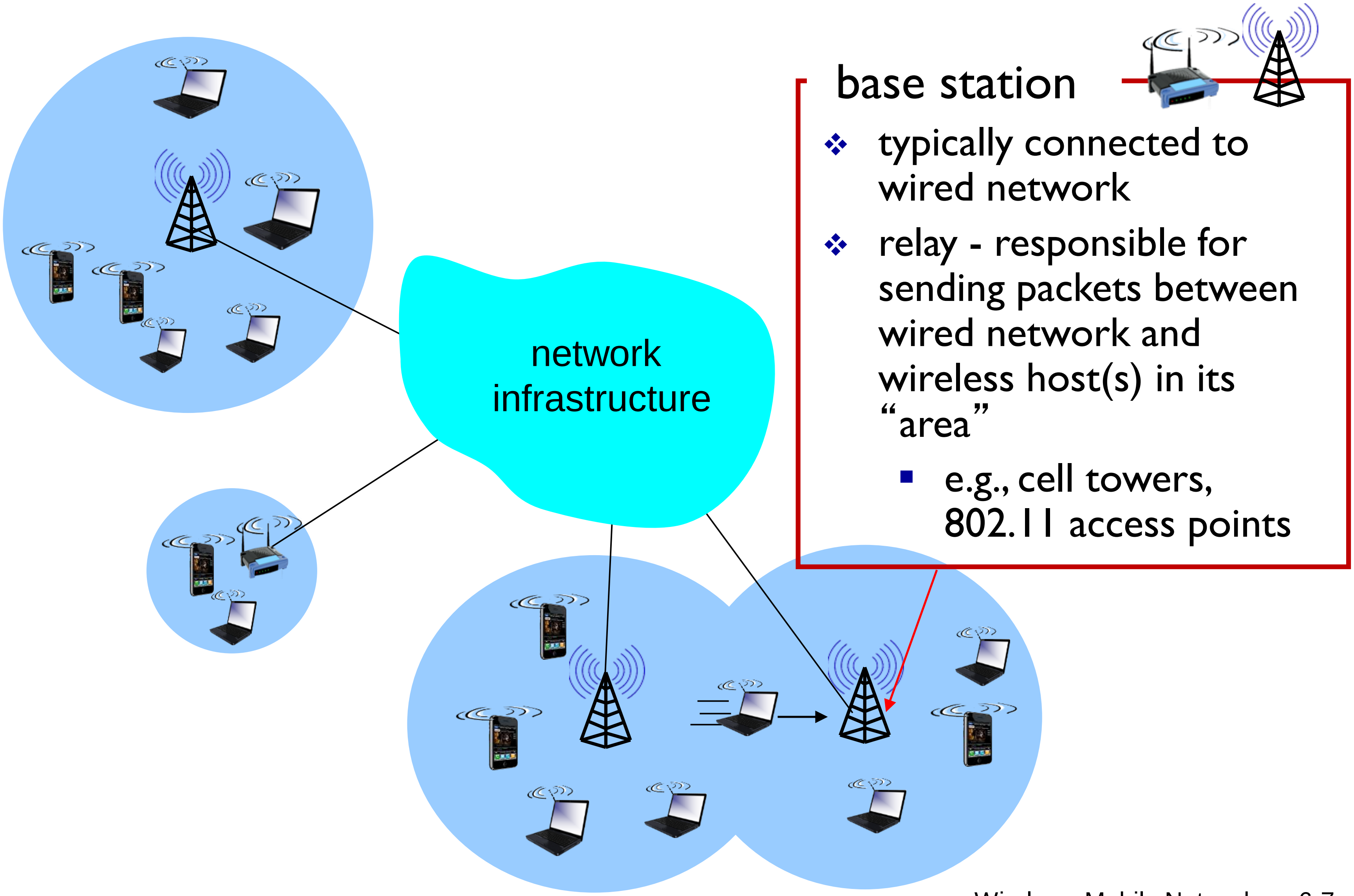
Elements of a wireless network



wireless hosts

- laptop, smartphone
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility

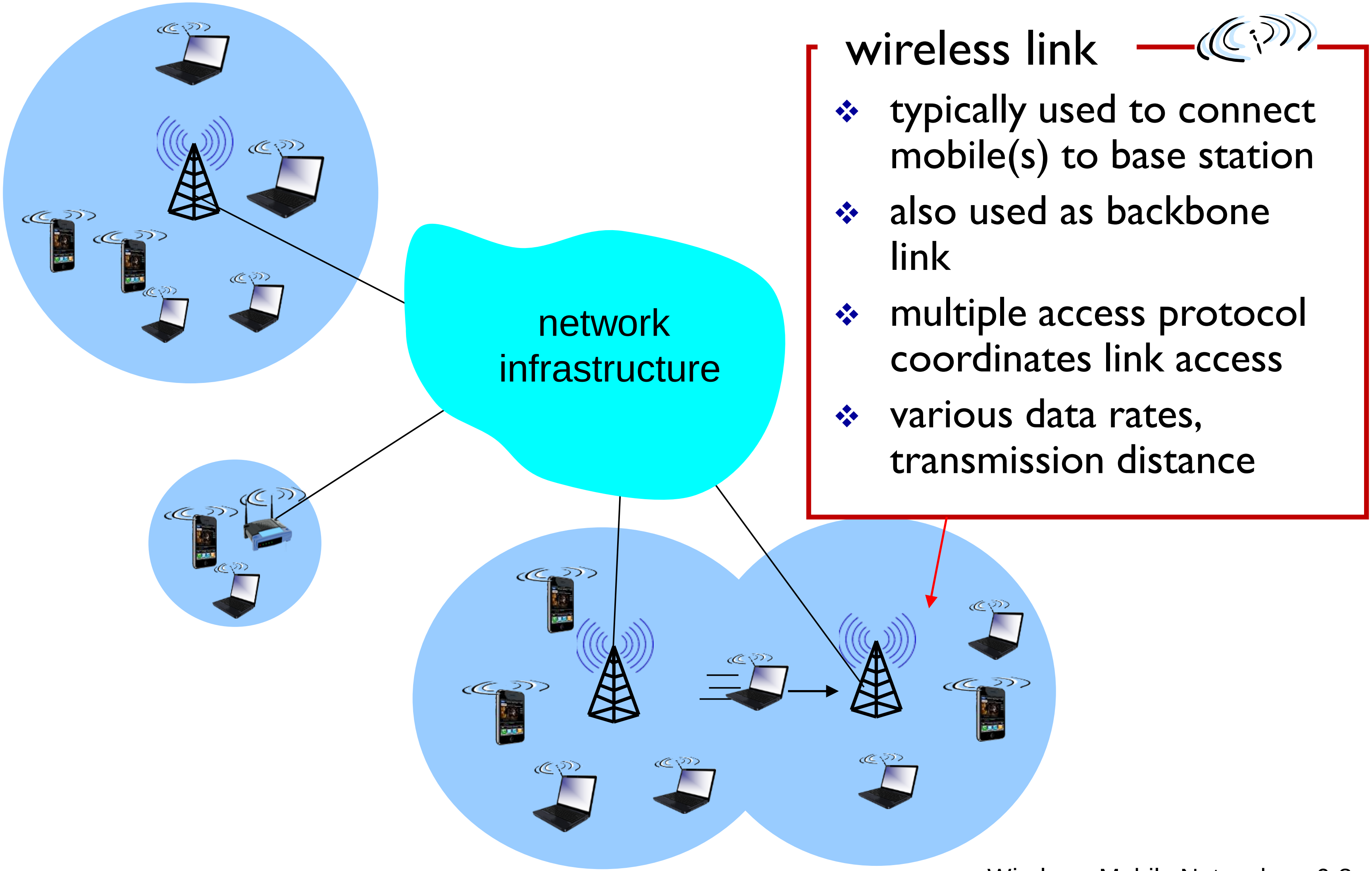
Elements of a wireless network



base station

- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless host(s) in its “area”
  - e.g., cell towers, 802.11 access points

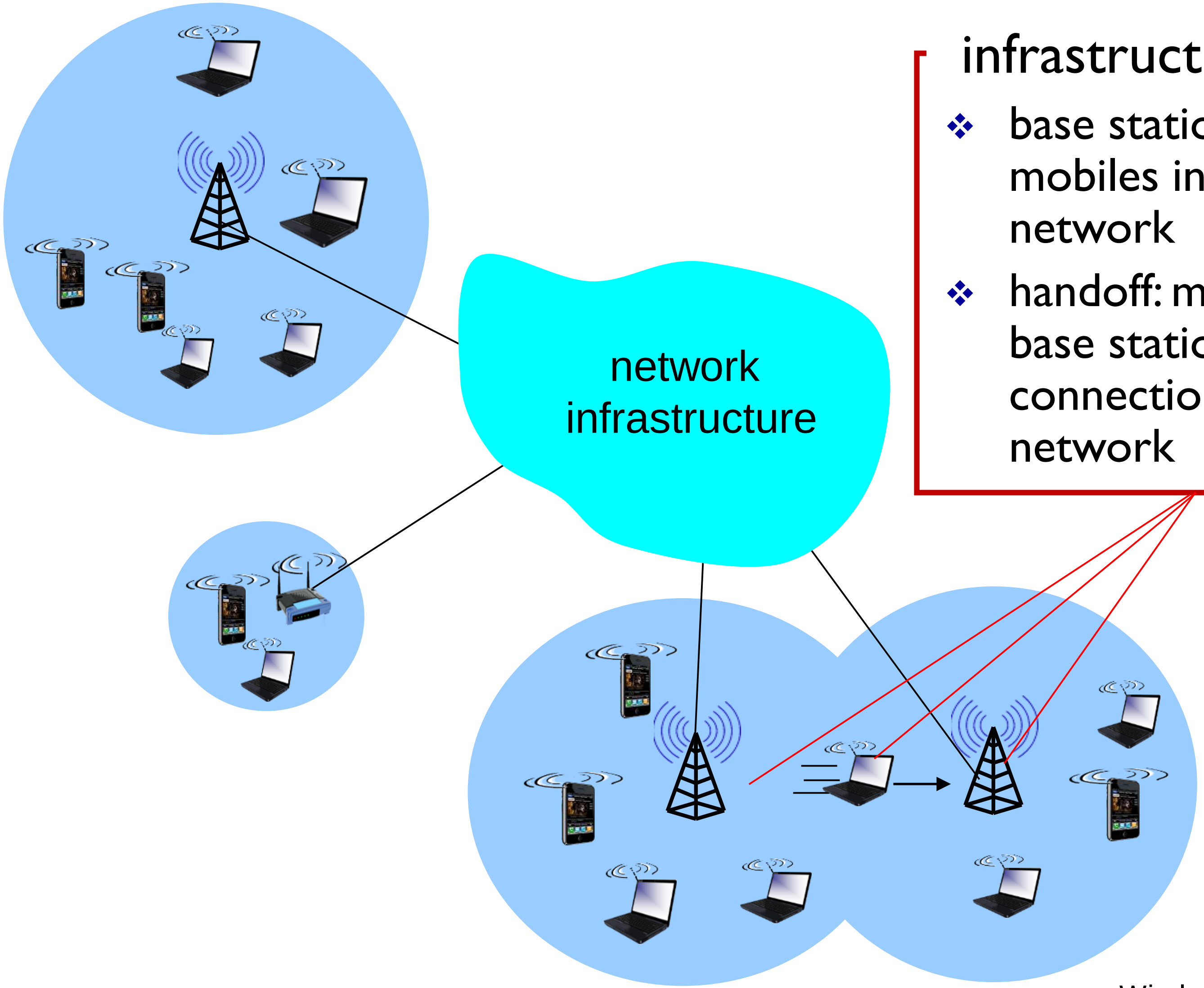
Elements of a wireless network



wireless link

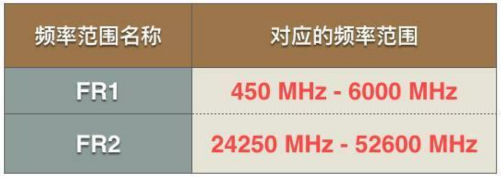
- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access protocol coordinates link access
- various data rates, transmission distance

Elements of a wireless network



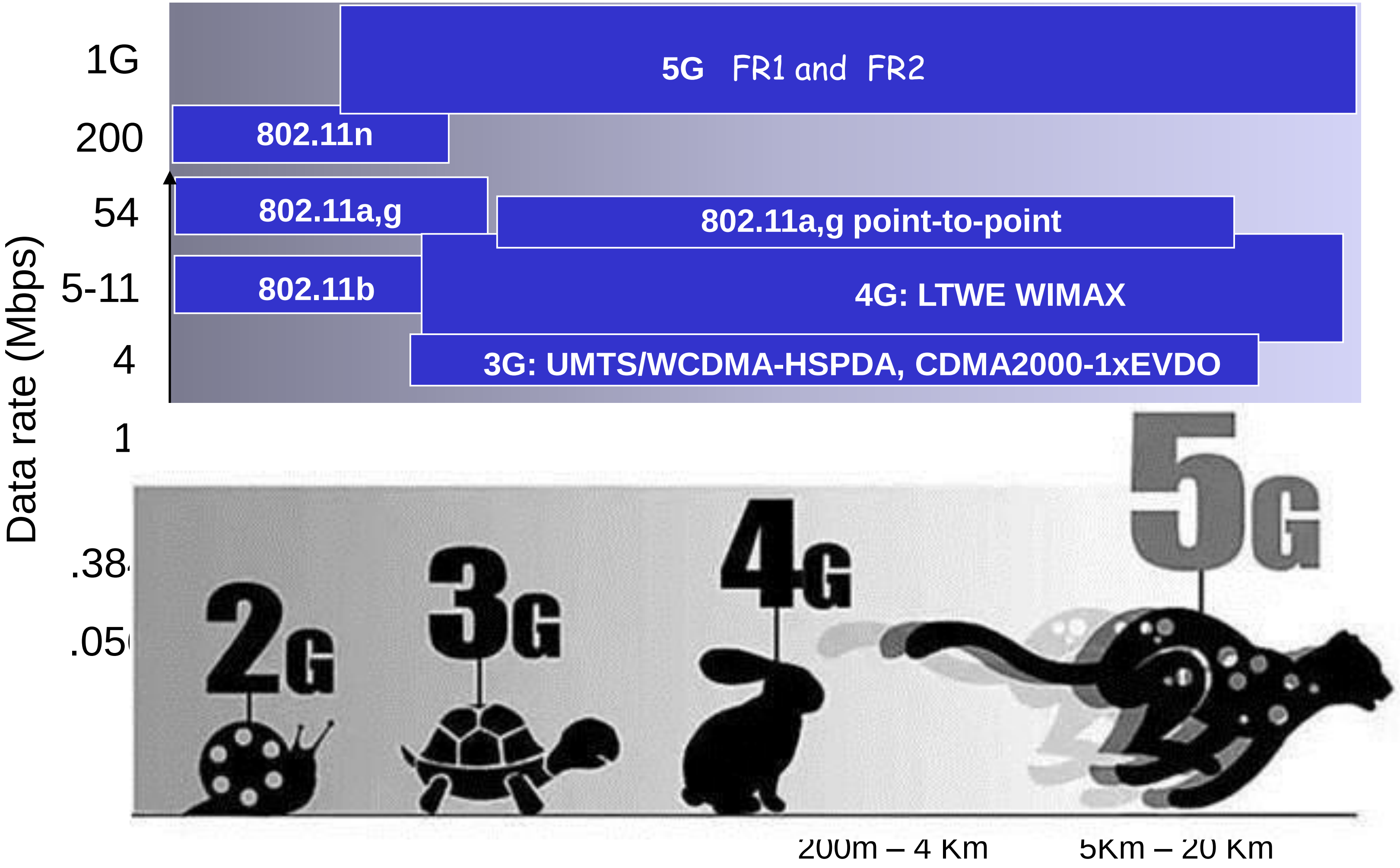
infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

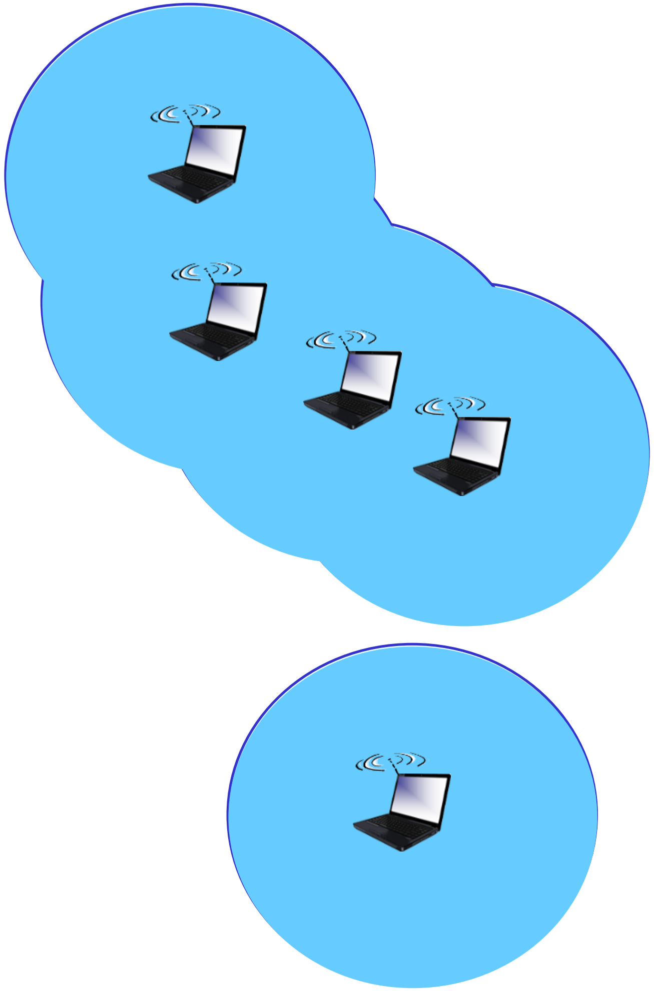


频率范围名称	对应的频率范围
FR1	450 MHz - 6000 MHz
FR2	24250 MHz - 52600 MHz

Characteristics of selected wireless links



Elements of a wireless network



ad hoc mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Wireless network taxonomy

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Chapter 6 outline

6.1 Introduction

Wireless

6.2 Wireless links, characteristics

- CDMA

6.3 IEEE 802.11 wireless LANs ("Wi-Fi")

6.4 Cellular Internet Access

- architecture
- standards (e.g., GSM)

1. Wireless Link Characteristics
2. Wireless network characteristics
3. Code Division Multiple Access (CDMA)

Wireless Link Characteristics (1)

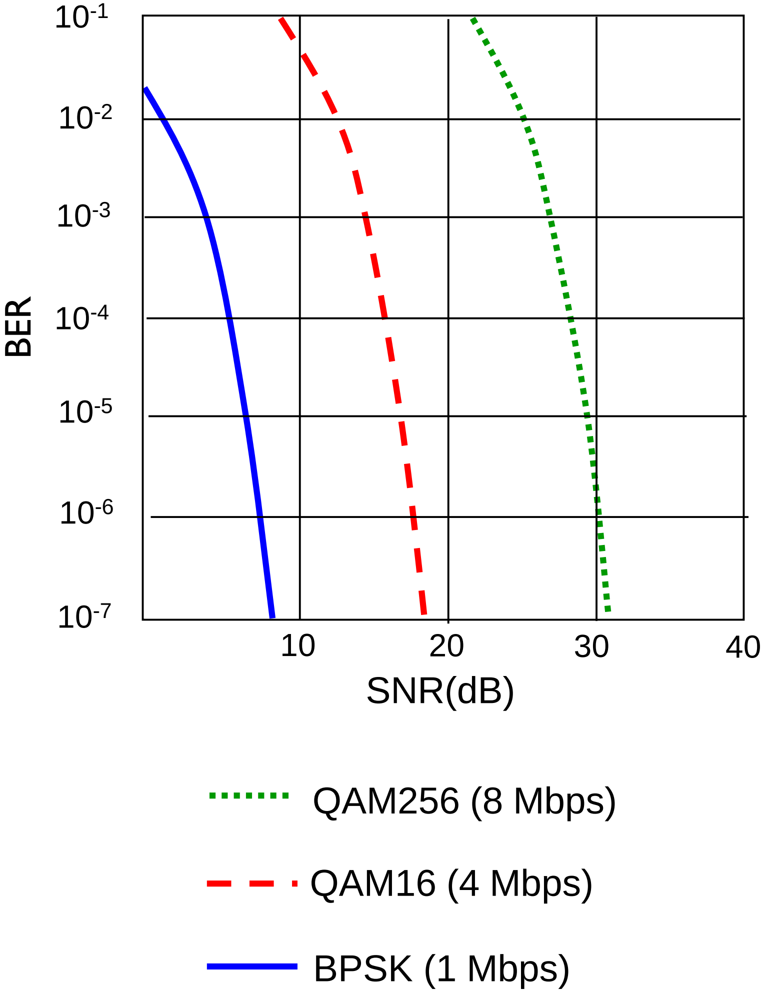
important differences from wired link ….

- *decreased signal strength:* radio signal attenuates as it propagates through matter (path loss)
- *interference from other sources:* standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- *multipath propagation:* radio signal reflects off objects ground, arriving ad destination at slightly different times

…. make communication across (even a point to point) wireless link much more "difficult"

Wireless Link Characteristics (2)

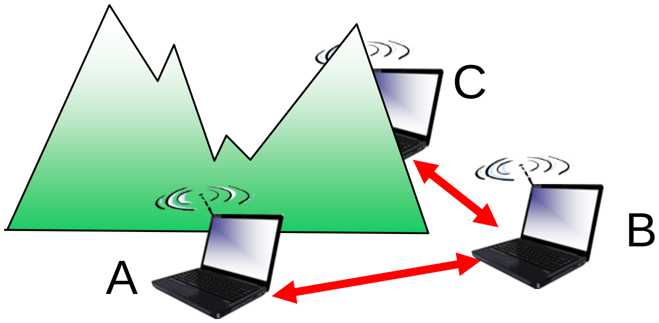
- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a "good thing")
- *SNR versus BER tradeoffs*
  - *given physical layer:* increase power -> increase SNR->decrease BER (Bit Error Rate)
  - *given SNR:* choose physical layer that meets BER requirement, giving highest thruput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



1. Wireless Link Characteristics
2. Wireless network characteristics
3. Code Division Multiple Access (CDMA)

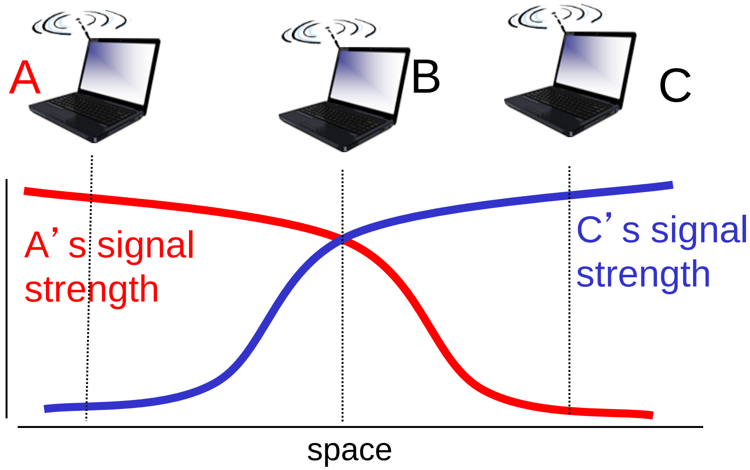
Wireless network characteristics

Multiple wireless senders and receivers create additional problems (beyond multiple access):



Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other means A, C unaware of their interference at B



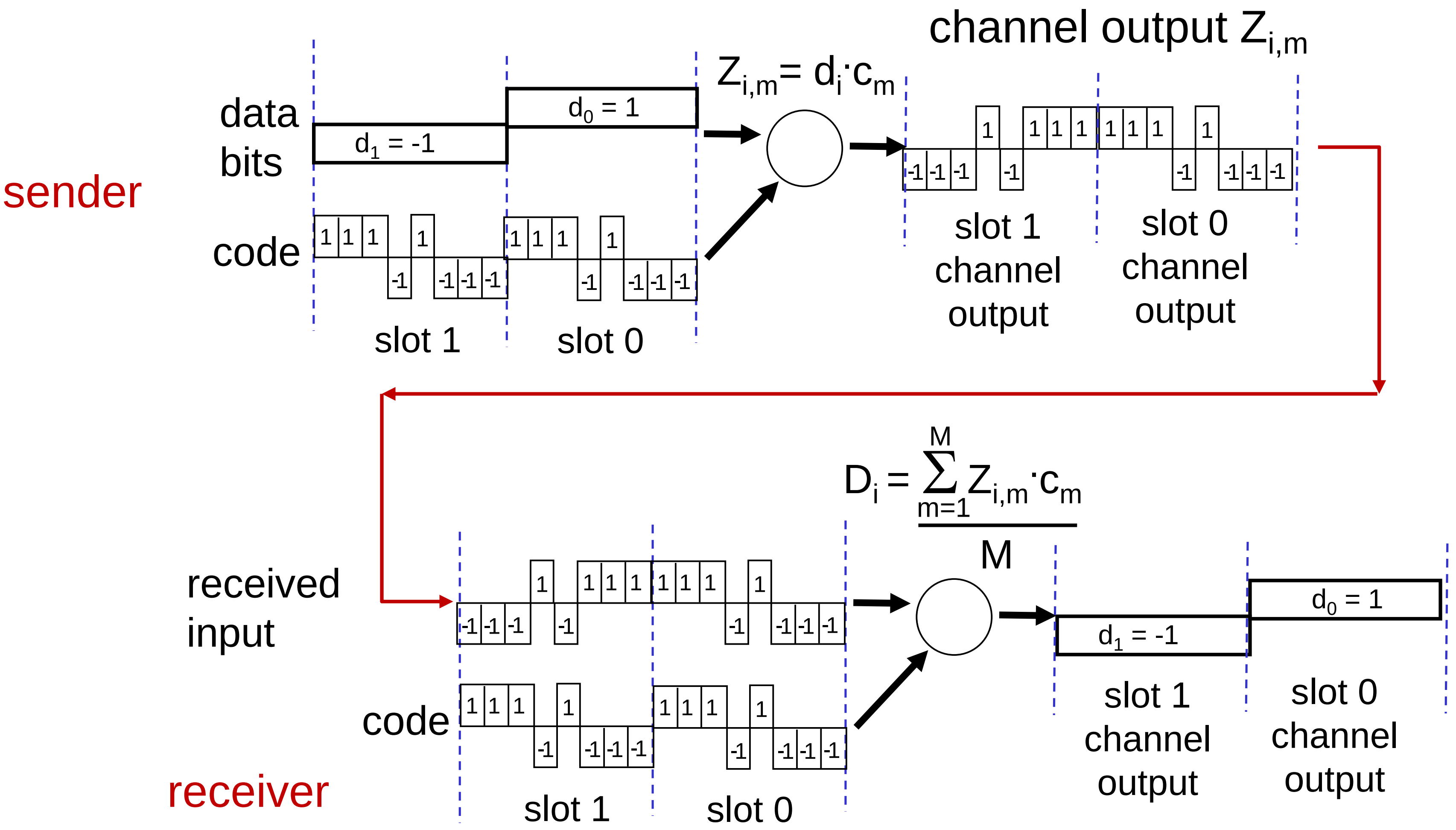
Signal attenuation:

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

Code Division Multiple Access (CDMA)

- unique "code" assigned to each user; i.e., code set partitioning
  - all users share same frequency, but each user has own "chipping" sequence (i.e., code) to encode data
  - allows multiple users to "coexist" and transmit simultaneously with minimal interference (if codes are "orthogonal")
- *encoded signal* = (original data) X (chipping sequence)
- *decoding:* inner-product of encoded signal and chipping sequence

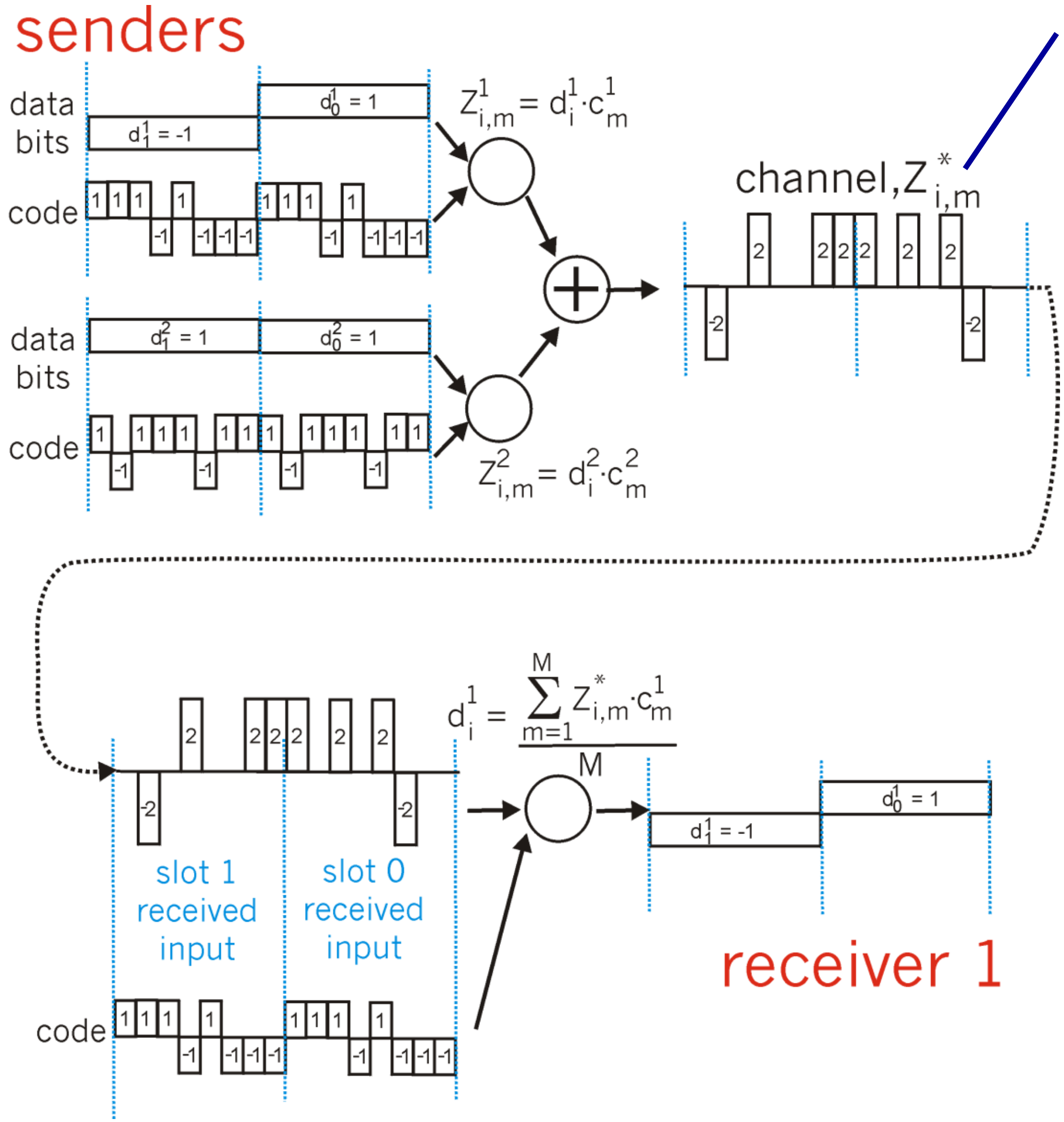
CDMA encode/decode



CDMA: two-sender interference

Sender 1

Sender 2



channel sums together transmissions by sender 1 and 2

using same code as sender 1, receiver recovers sender 1's original data from summed channel data!

6.2 Wireless links, characteristics - summary

1. Wireless Link Characteristics
2. Wireless network characteristics
3. Code Division Multiple Access (CDMA)

Chapter 6 outline

6.1 Introduction

Wireless

6.2 Wireless links, characteristics

- CDMA

6.3 IEEE 802.11 wireless LANs ("Wi-Fi")

6.4 Cellular Internet Access

- architecture
- standards (e.g., GSM)

1. IEEE 802.11 Wireless LAN
2. 802.11 LAN architecture
3. IEEE 802.11 MAC Protocol: CSMA/CA
4. 802.11 MAC FRAME
5. 802.11: advanced capabilities

I IEEE 802.11 Wireless LAN

802.11b

- 2.4-5 GHz unlicensed spectrum
- up to 11 Mbps
- direct sequence spread spectrum (DSSS) in physical layer
  - all hosts use same chipping code

802.11a

- 5-6 GHz range
- up to 54 Mbps

802.11g

- 2.4-5 GHz range
- up to 54 Mbps

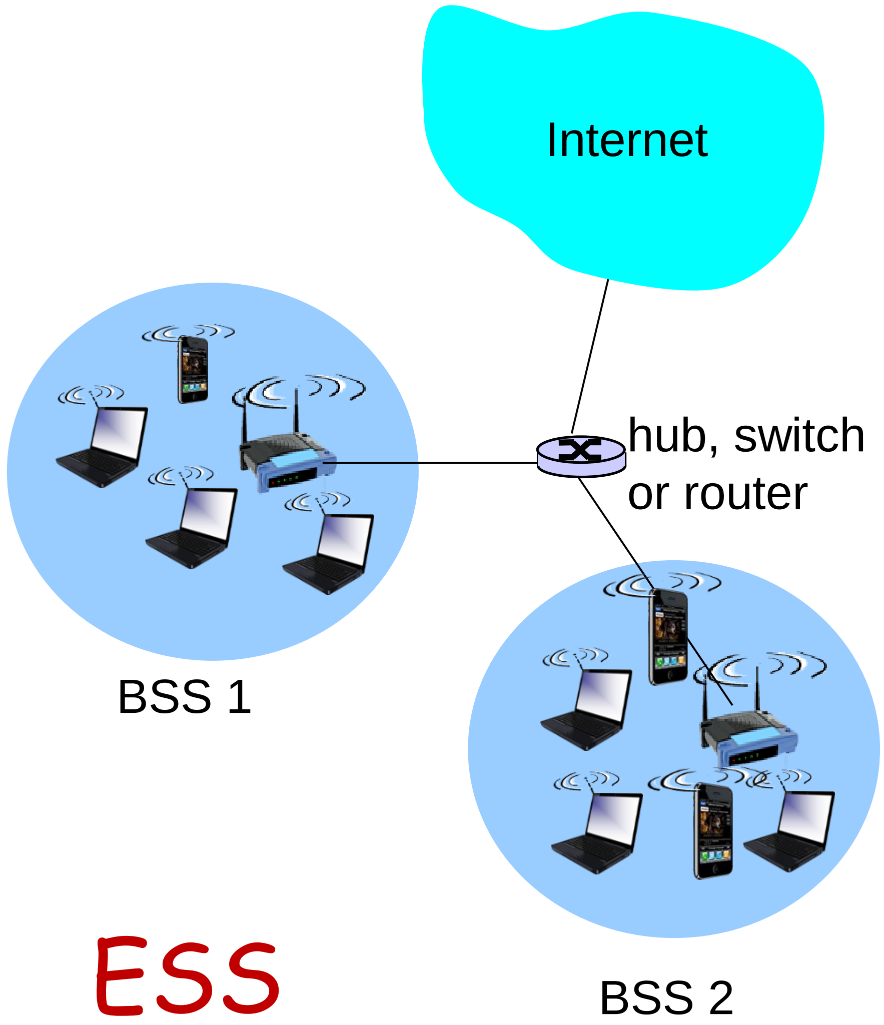
802.11n: multiple antennae

- 2.4-5 GHz range
- up to 200 Mbps

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

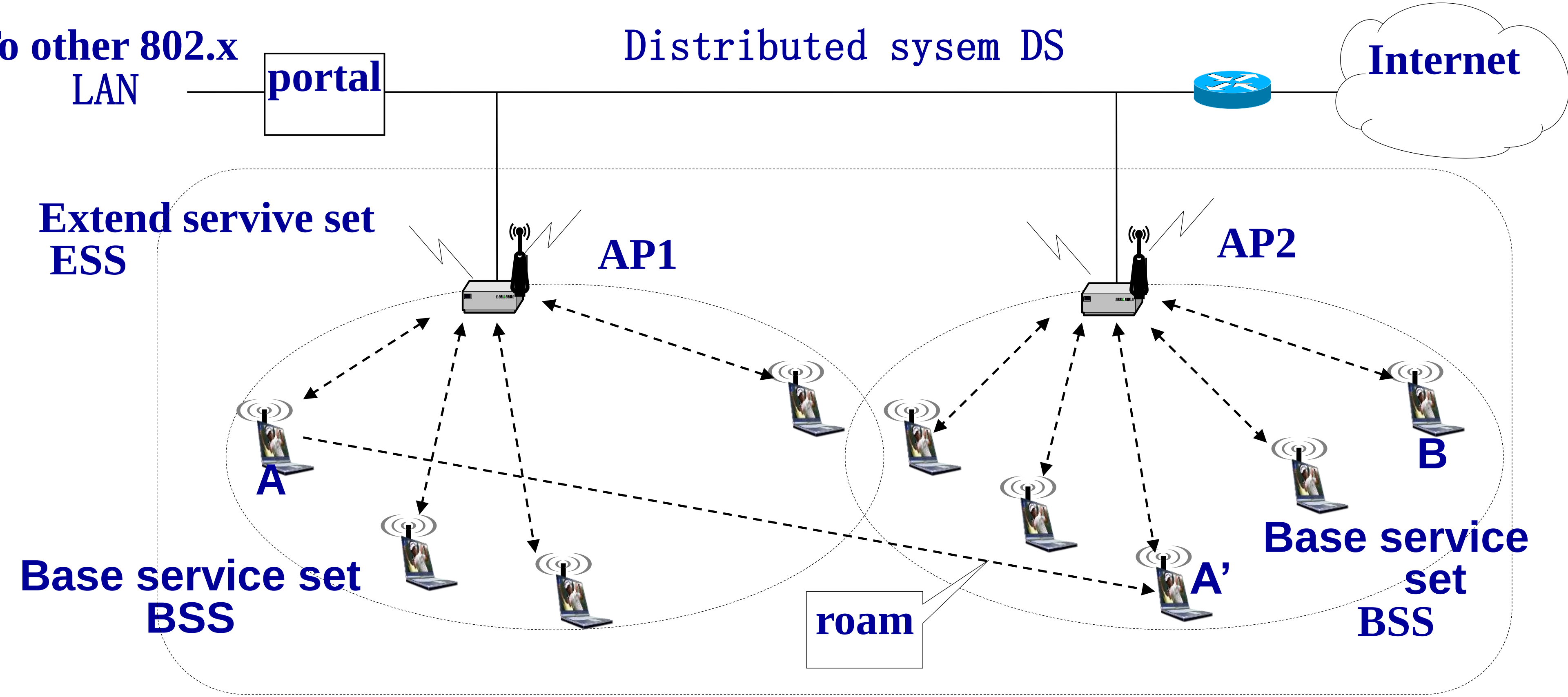
2 802.11 LAN architecture

1. IEEE 802.11 Wireless LAN
2. 802.11 LAN architecture
3. IEEE 802.11 MAC Protocol: CSMA/CA
4. 802.11 MAC FRAME
5. 802.11: advanced capabilities



- 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

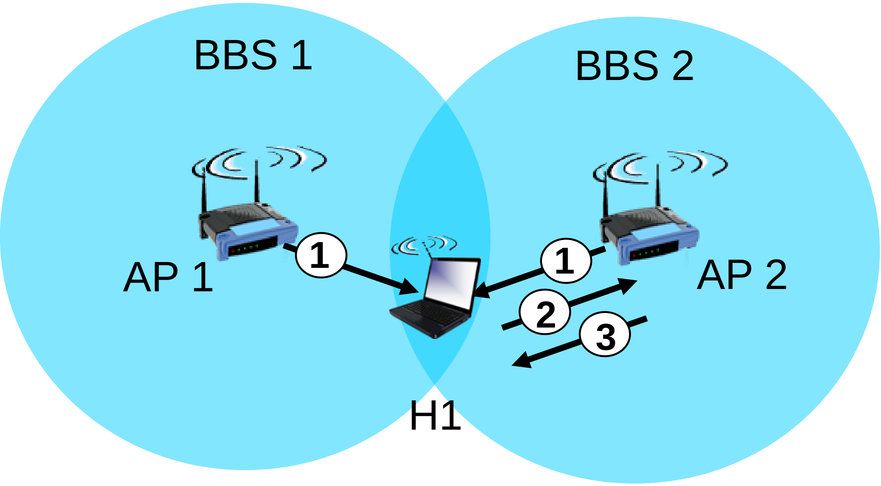
802.11's BSS and ESS

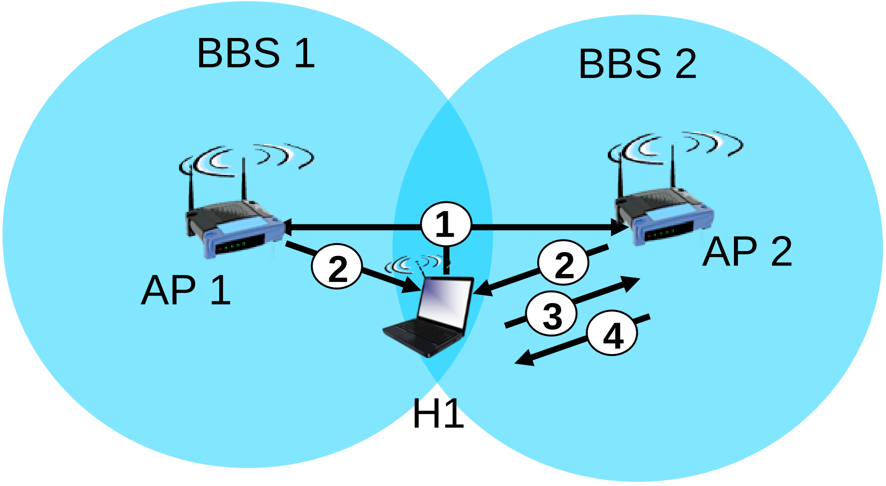


802.11: Channels, association

- 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: users and PWD
  - 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

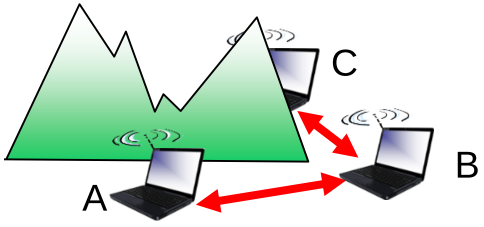
(2) Probe Response frames sent from APs

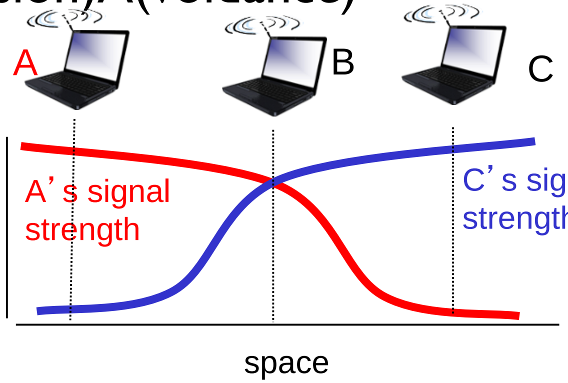
(3) Association Request frame sent: H1 to selected AP

(4) Association Response frame sent from selected AP to H1

IEEE 802.11: multiple access

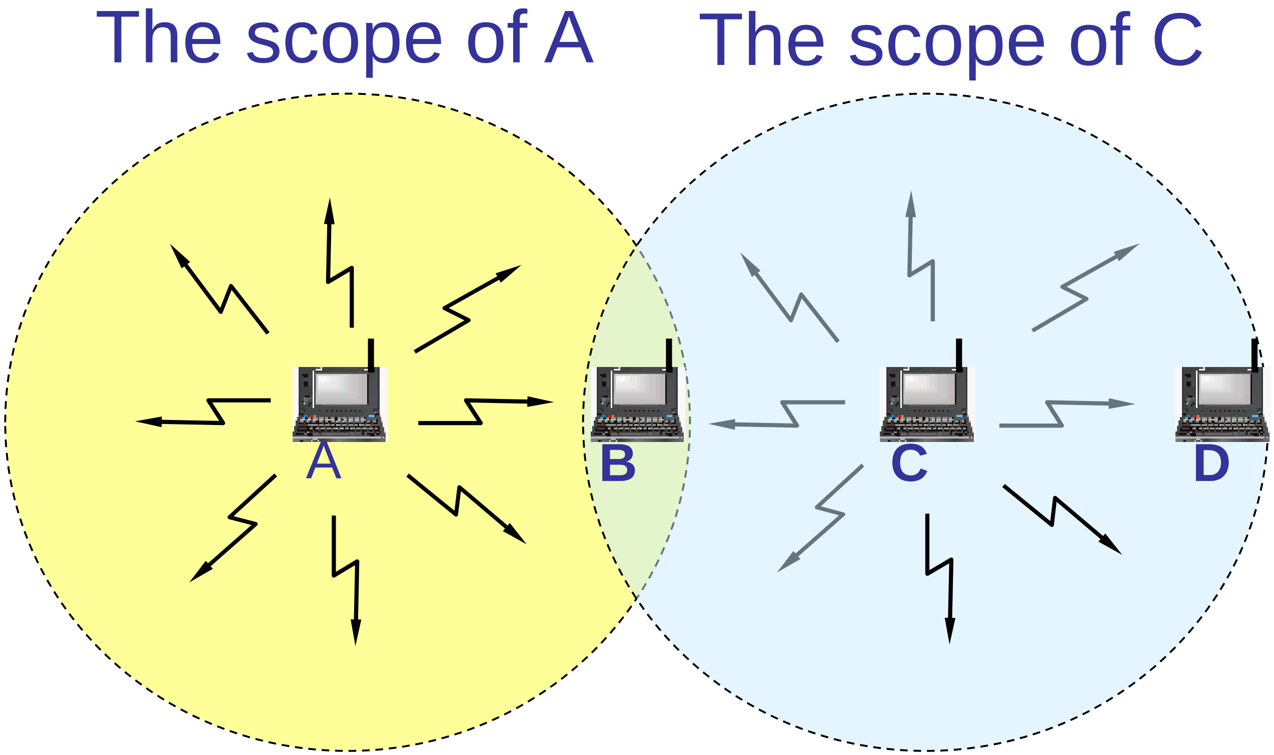
- avoid collisions: 2^{+} nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
  - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - can't sense all collisions in any case: hidden terminal, exposed terminal , fading
  - goal: *avoid collisions:* CSMA/C(ollision)A(voidance)





1. hidden terminal
2. exposed station

1. hidden terminal

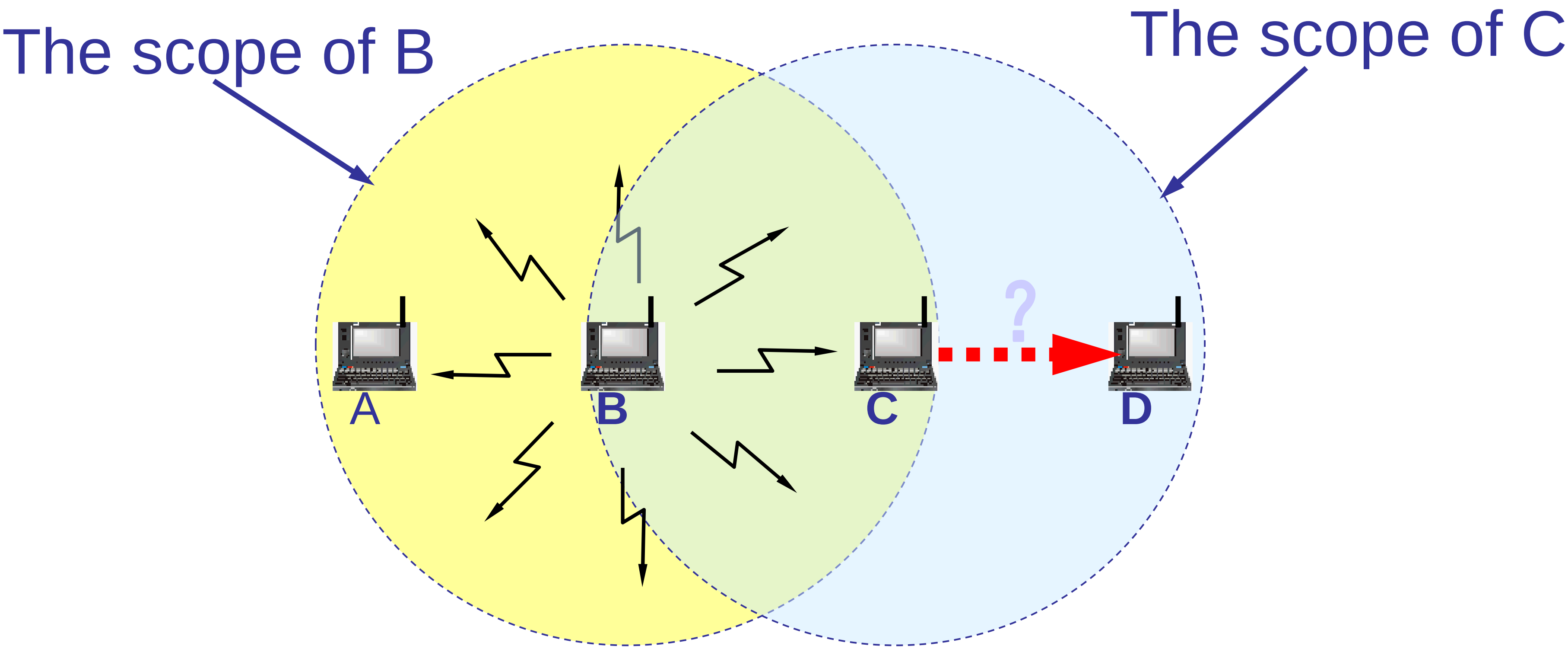


When A and C are far away from each other, because no wireless signal can be detected, both assume that B is idle, so they send data to B, and the results collide.

The problem of failing to detect signals that already exist in the media and not being able to detect potential media competitors is called **hidden station problem ,E.G. station C**

2 exposed station problem

B sends data to A, and C wants to communicate with D. C detects a signal on the media and can't send data to D



•In fact, B sending data to A doesn't affect C sending data to D , this is the exposed station problem

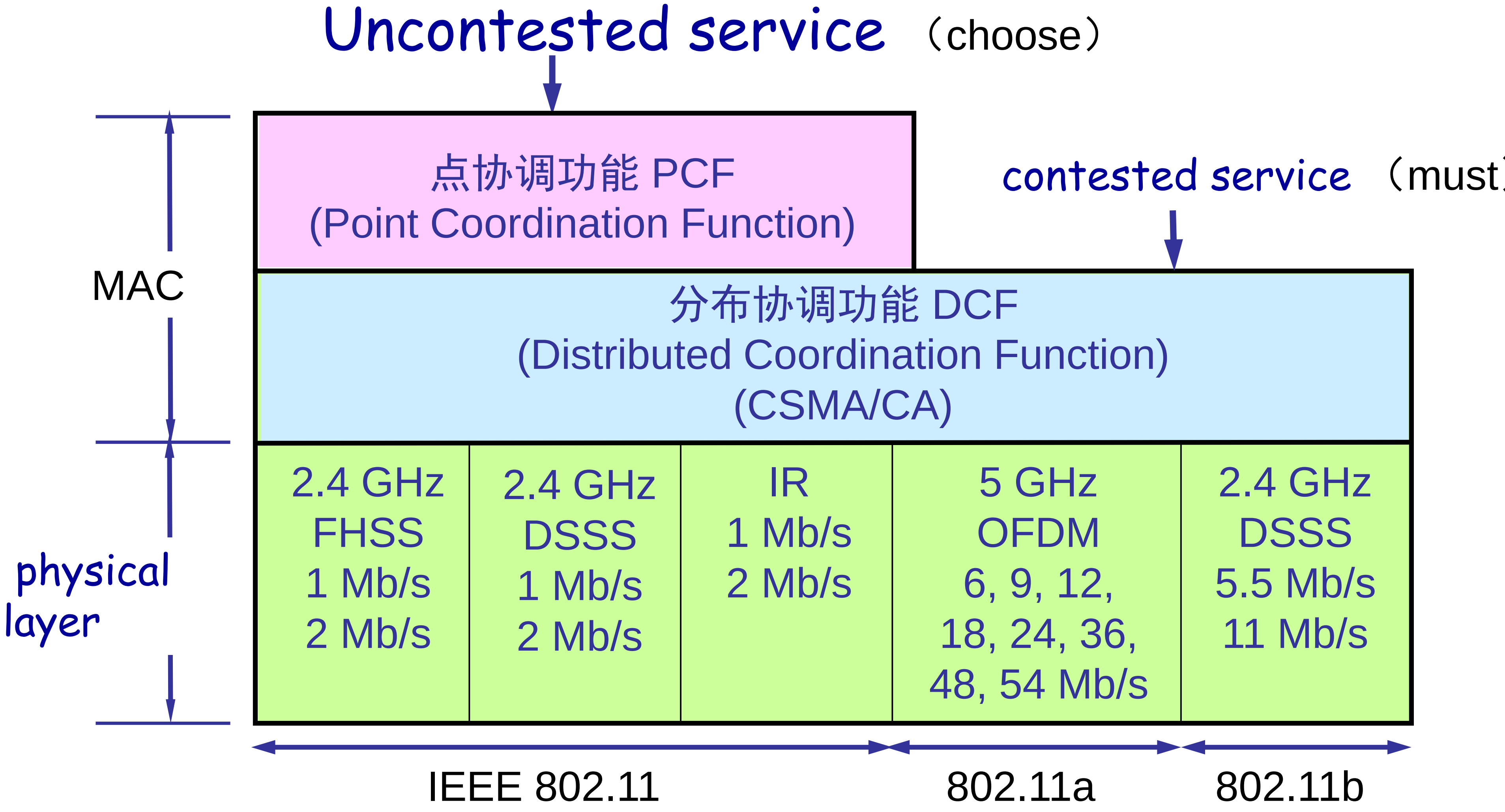
3 IEEE 802.11 MAC Protocol: CSMA/CA

802.11 MAC include tow sub-layer

- 802.11support two operation mode
  - Distributed coordination function DCF （ Must be implemented ）
  - Point coordination function PCF（ choose ）

1. IEEE 802.11 Wireless LAN
2. 802.11 LAN architecture
3. IEEE 802.11 MAC Protocol: CSMA/CA
4. 802.11 MAC FRAME
5. 802.11: advanced capabilities

802.11 MAC include tow sub-layer



Uncontested service （choose）

contested service （must

MAC

physical layer

点协调功能 PCF
(Point Coordination Function)

分布协调功能 DCF
(Distributed Coordination Function)
(CSMA/CA)

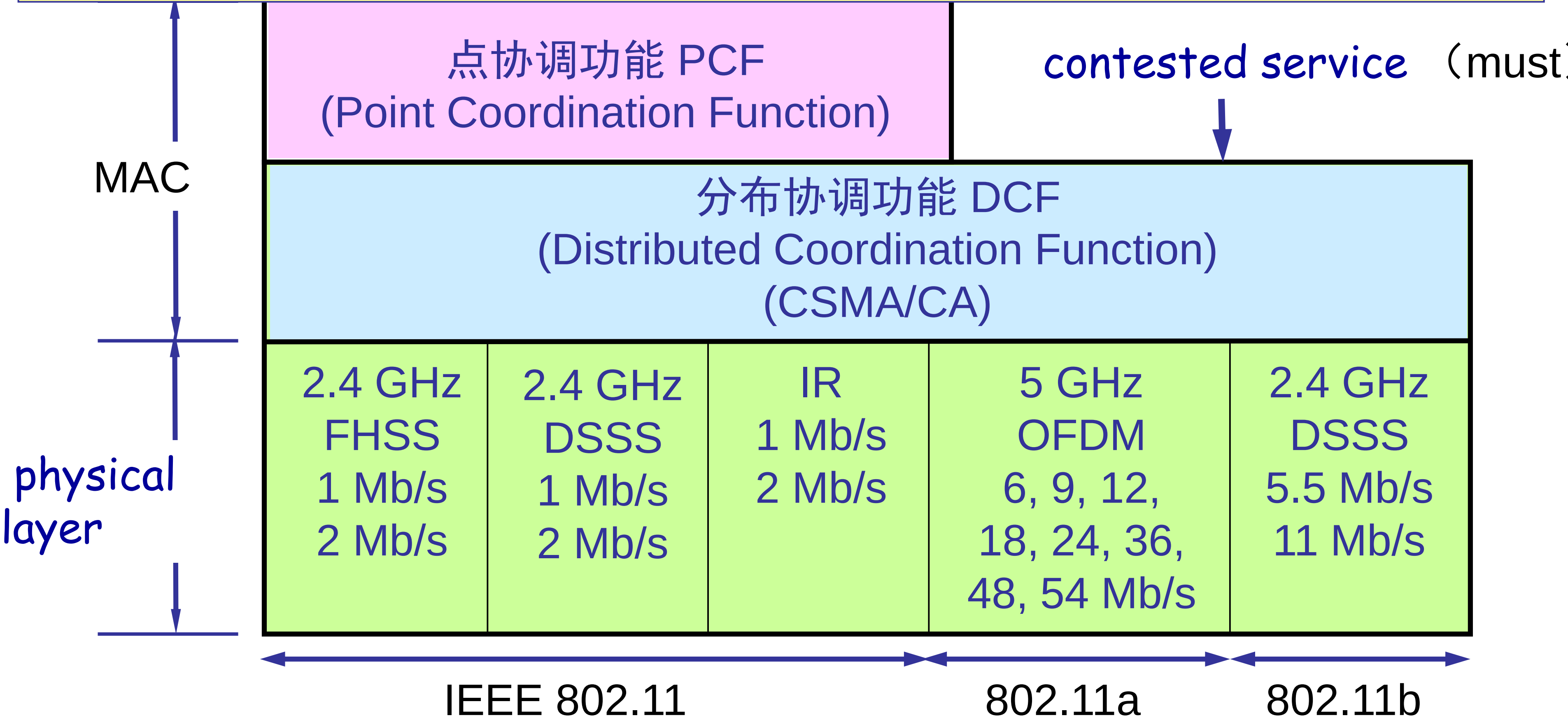
2.4 GHz FHSS 1 Mb/s 2 Mb/s	2.4 GHz DSSS 1 Mb/s 2 Mb/s	IR 1 Mb/s 2 Mb/s	5 GHz OFDM 6, 9, 12, 18, 24, 36, 48, 54 Mb/s	2.4 GHz DSSS 5.5 Mb/s 11 Mb/s

IEEE 802.11

802.11a

802.11b

The DCF sub-layer uses the distributed access algorithm of CSMA mechanism, so that each station can obtain the transmission right by competing channels.The DCF provides contention services.It is suitable for both the mode with infrastructure and the mode without infrastructure



MAC

physical layer

点协调功能 PCF
(Point Coordination Function)

contested service （must

分布协调功能 DCF
(Distributed Coordination Function)
(CSMA/CA)

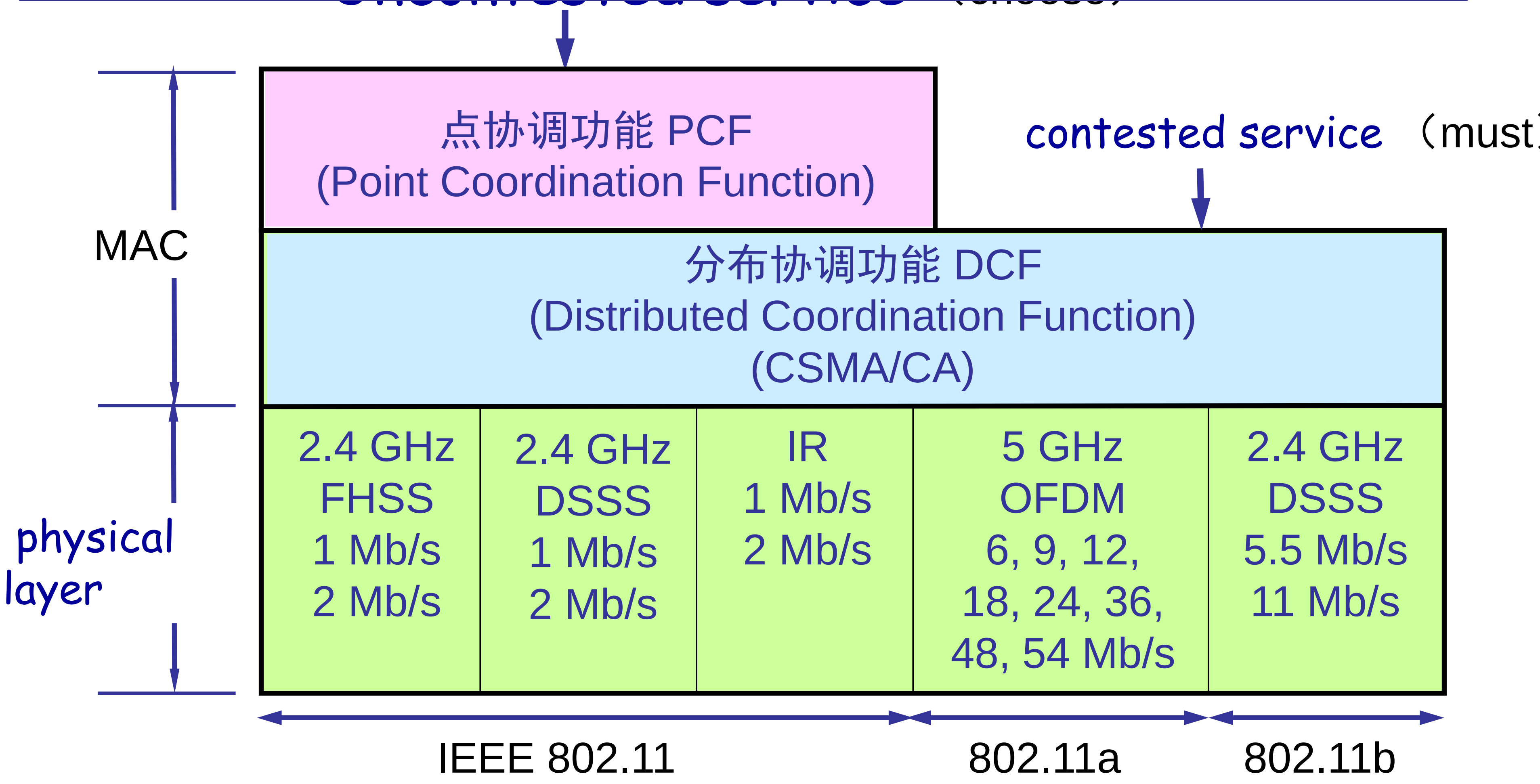
2.4 GHz FHSS 1 Mb/s 2 Mb/s	2.4 GHz DSSS 1 Mb/s 2 Mb/s	IR 1 Mb/s 2 Mb/s	5 GHz OFDM 6, 9, 12, 18, 24, 36, 48, 54 Mb/s	2.4 GHz DSSS 5.5 Mb/s 11 Mb/s

IEEE 802.11

802.11a

802.11b

The PCF sub-layer uses centrally controlled access algorithms (in AP) to rotate the right to send data to each station to avoid collisions. Only for infrastructure patterns.



contested service （must

点协调功能 PCF
(Point Coordination Function)

分布协调功能 DCF
(Distributed Coordination Function)
(CSMA/CA)

MAC

physical layer

2.4 GHz FHSS 1 Mb/s 2 Mb/s

2.4 GHz DSSS 1 Mb/s 2 Mb/s

IR 1 Mb/s 2 Mb/s

5 GHz OFDM 6, 9, 12, 18, 24, 36, 48, 54 Mb/s

2.4 GHz DSSS 5.5 Mb/s 11 Mb/s

IEEE 802.11

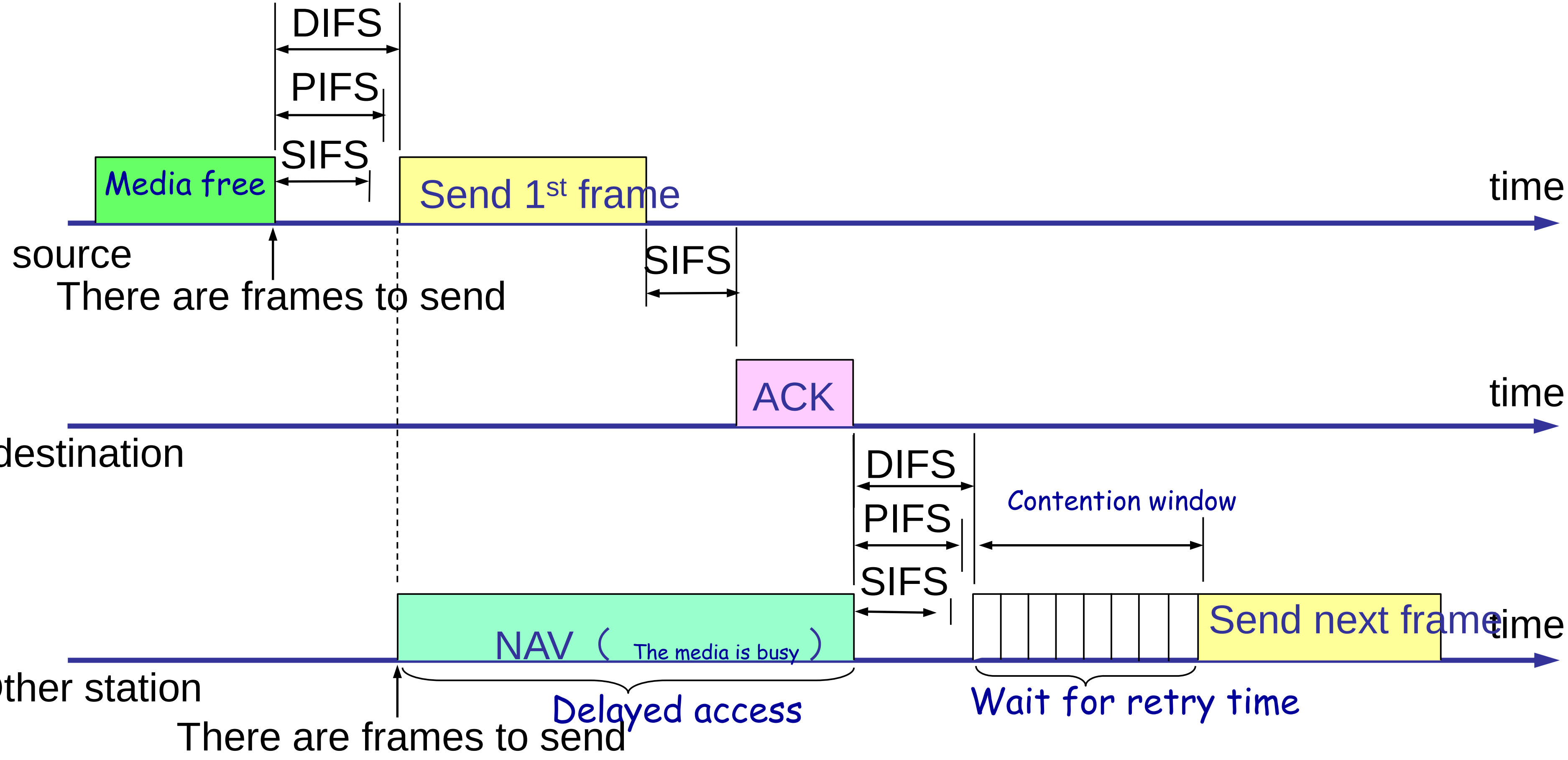
802.11a

802.11b

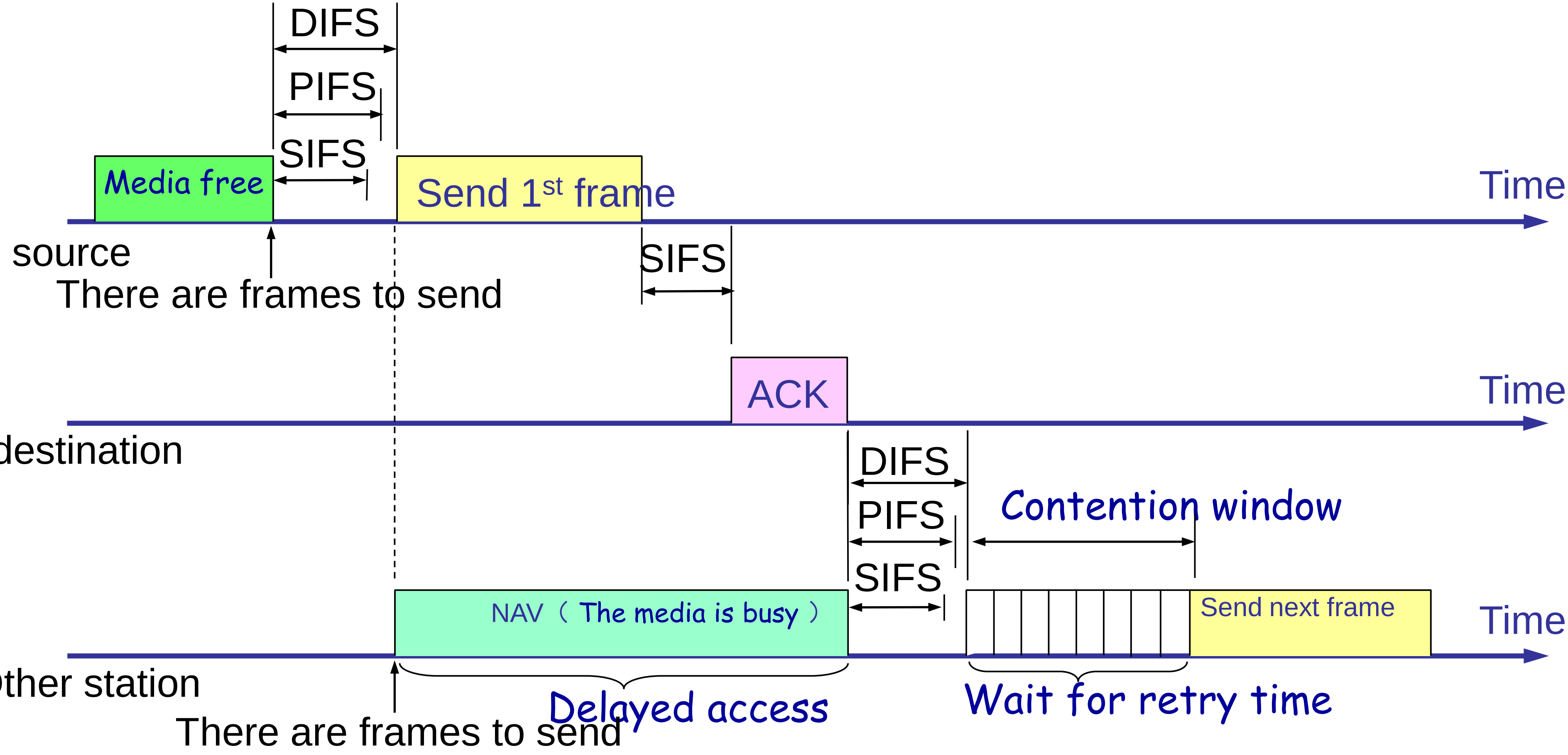
Inter-frame Spacing

- 802.11 specifies that all sites must wait a very short period of time (continue listening for channels) after sending to send the next frame. The general term for this period is interframe Inter-frame Spacing.
- There are three commonly used inter-frame intervals:
  - Short interframe Spacing SIFS
  - Point coordination function for inter-frame Spacing PIFS
  - Distributed coordination function inter-frame Spacing DIFS

SIFS， time length is 28 μs， is the shortest IFS. The types of frames that use SIFS are ACK frames, CTS frames, and any frames that answer AP queries and are sent by AP in PCF mode.

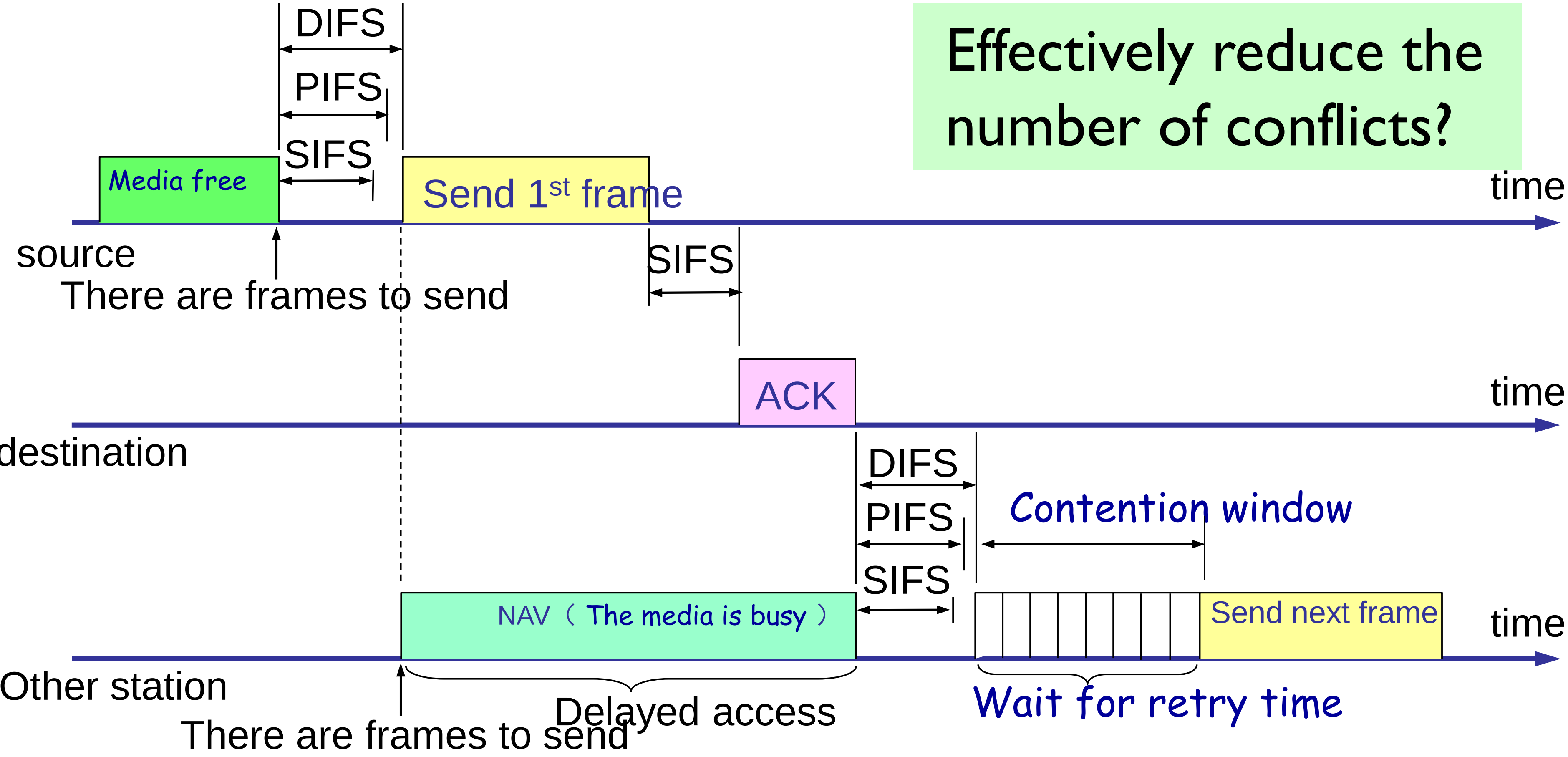


PIFS, which is the point coordination function's inter-frame spacing(longer than SIFS), is designed to prioritize access to media when PCF mode is used (without contention).The length of PIFS is SIFS plus a slot length (with a length of 50 ms), which is 78 ms.



DIFS, that is, the space between frames of distributed coordination function (the longest IFS),Used in DCF mode to send data frames and manage frames.DIFS length =PIFS +1 slot length, so the length of DIFS is 128 ms.。

Effectively reduce the number of conflicts?



IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

1 if sense channel idle for **DIFS** then

transmit entire frame (no CD)

2 if sense channel busy then

start random backoff time

timer counts down while channel idle

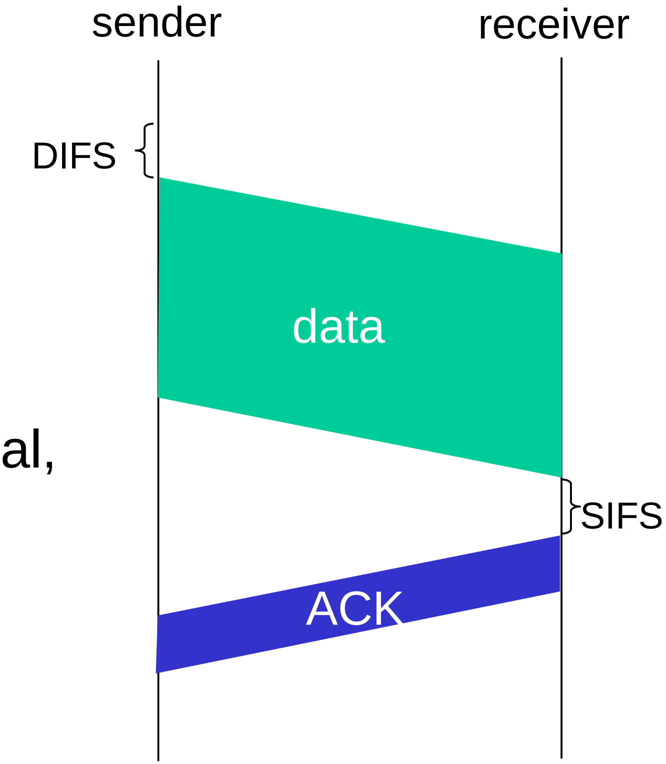
transmit when timer expires

if no ACK, increase random backoff interval, repeat 2

802.11 receiver

- if frame received OK

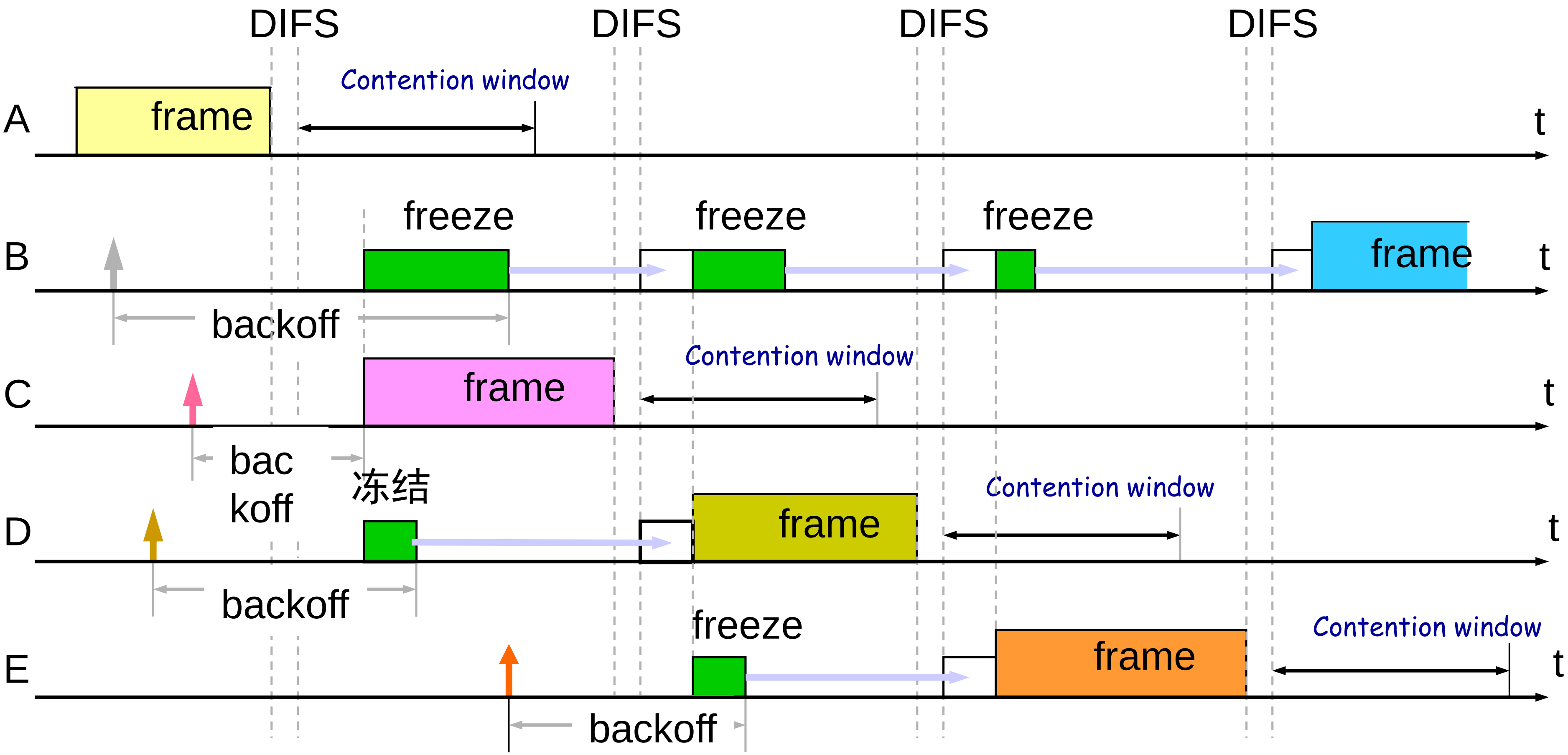
return ACK after **SIFS** (ACK needed due to hidden terminal problem)



802.11random backoff time

- The i^th^ retreat is $\{0,1...,2^{2+i}-1\}$ randomly choose one of the time slots, which further reduces the probability that different sites choose the same retreat time.
  - The first retreat is in 8 slots (instead of 2) {0,1...,7} choose one randomly;
  - The second retreat is in 16 slots (instead of 4) {0,1...,15}, choose one at random.
  - ......
  - The gap no longer increases when it reaches 255 (corresponding to the 6th retreat).

802.11 backoff examples



legend 🟩 —— Freezed remaining backoff time

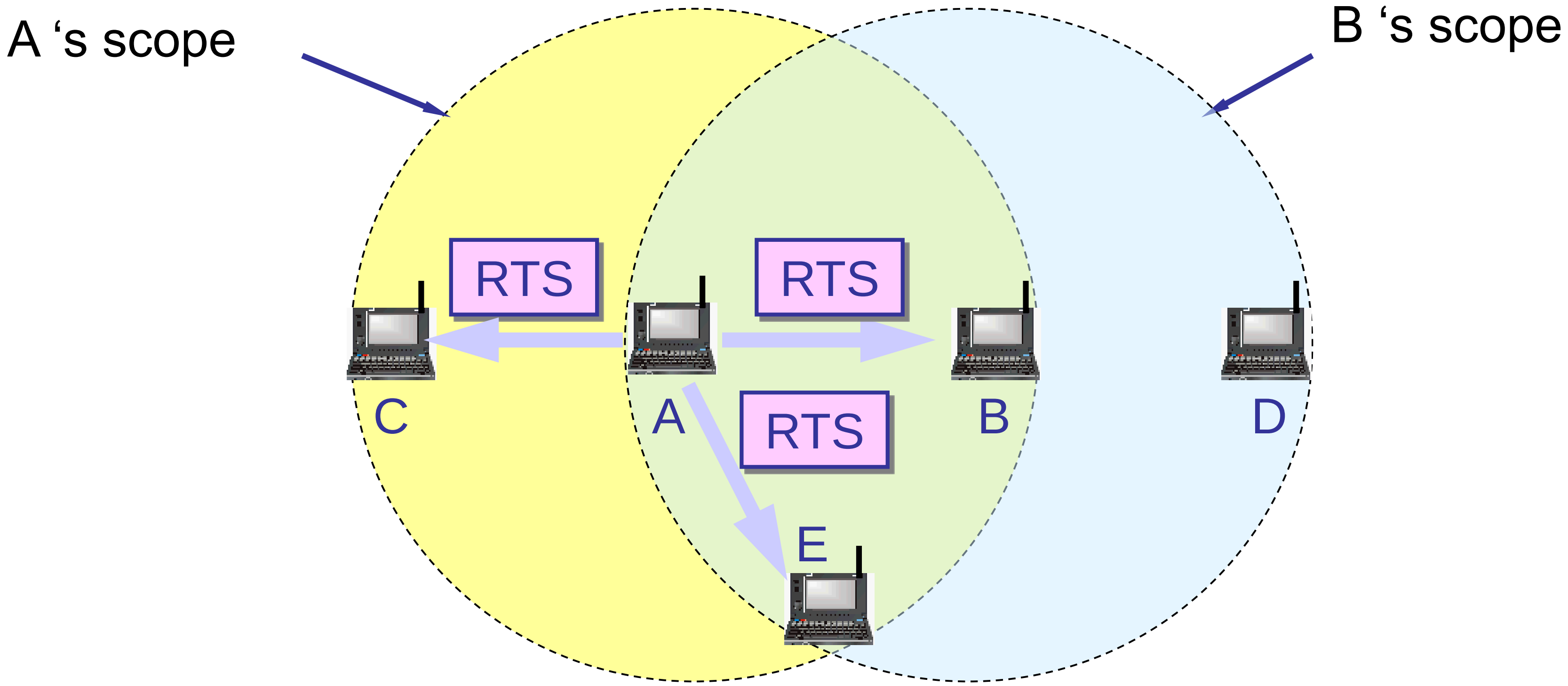
Avoiding collisions (more)

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

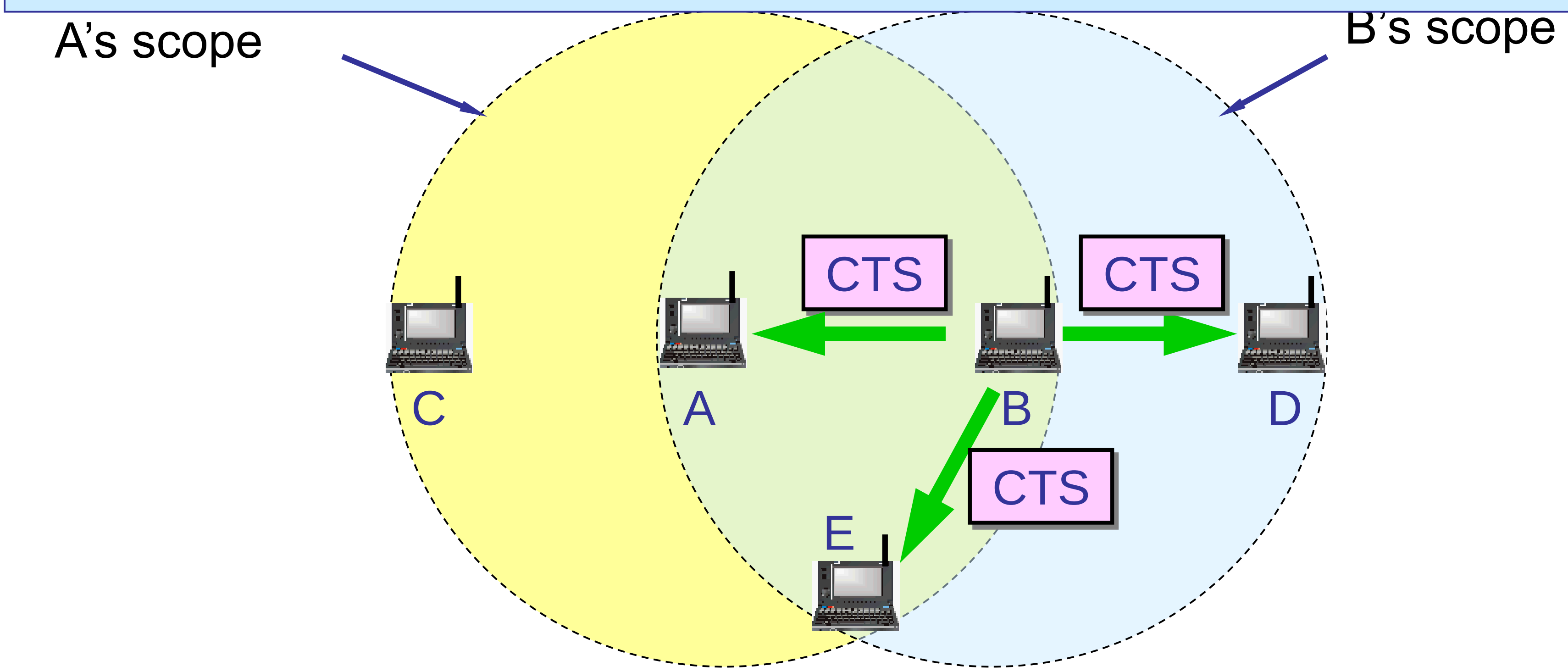
avoid data frame collisions completely using small reservation packets!

Source station A sends short control frame, called Request To Send, before sending the data frame, including the source address, destination address and duration (including the confirmation frame time of this communication).



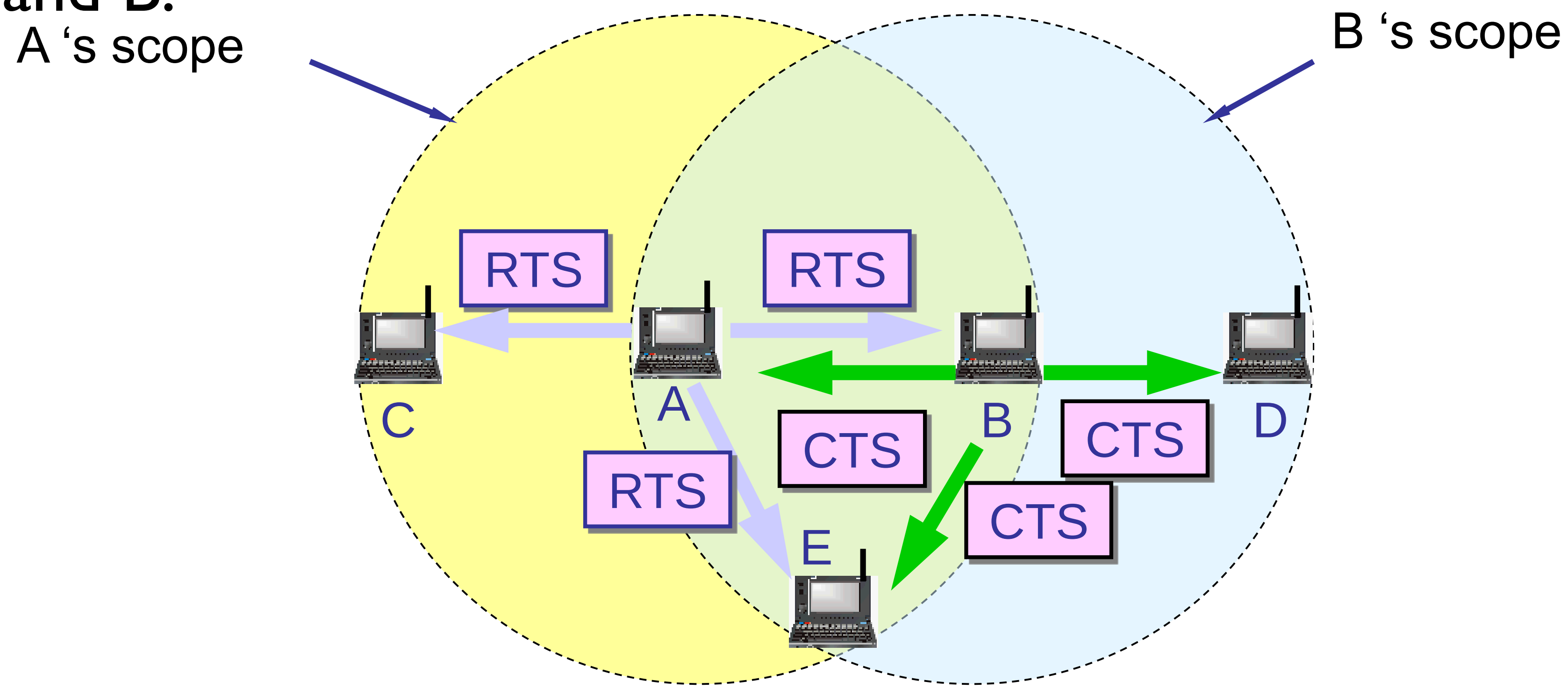
If the media is idle, destination B sends a response control frame. It's called allow CTS (Clear To Send), and it includes this Duration required for communication (this duration is taken from the RTS frame) Copy to CTS frame).

A receives the CTS frame and sends its data frame.

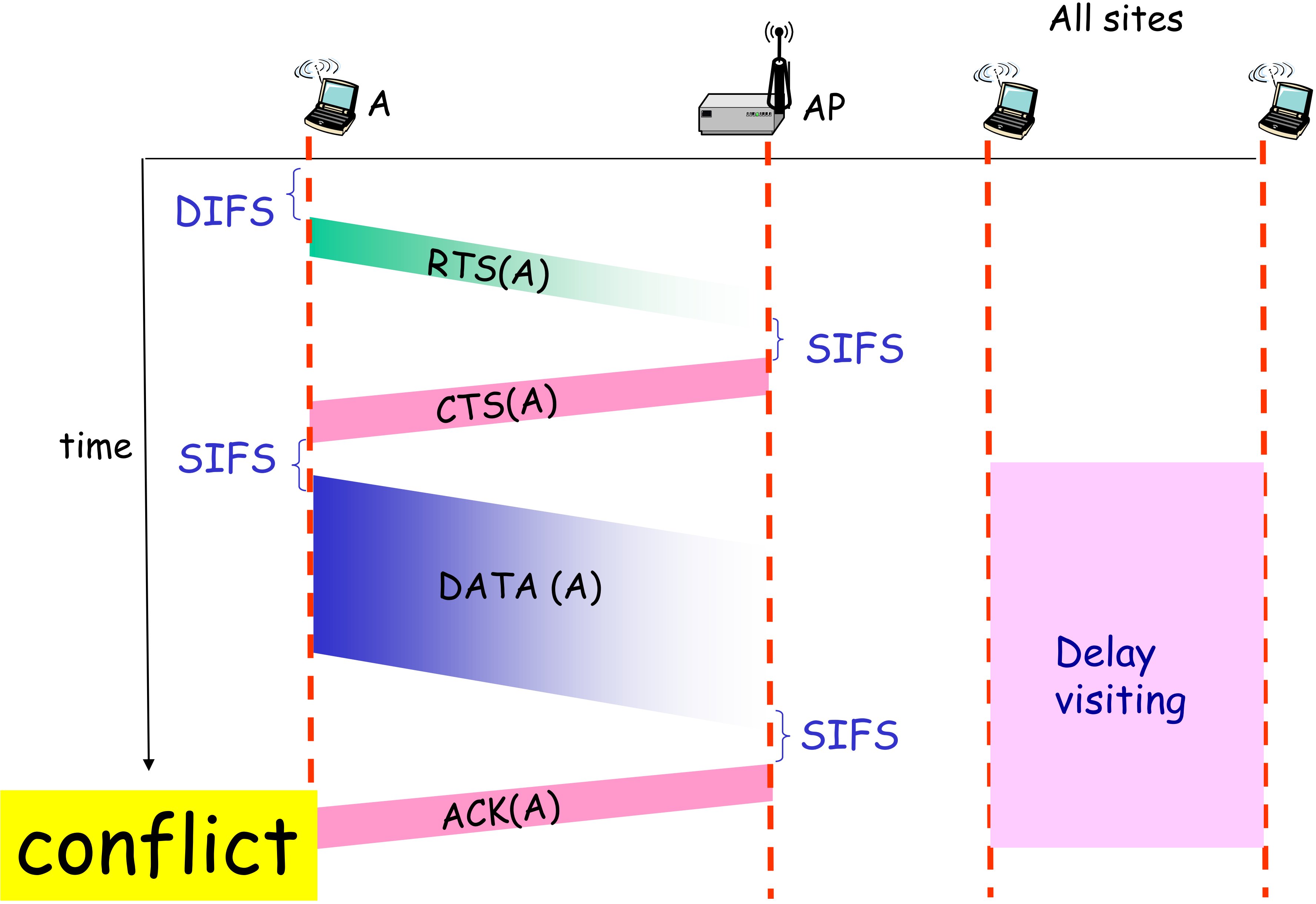


Influence of A and B on nearby stations C, D and E when communicating

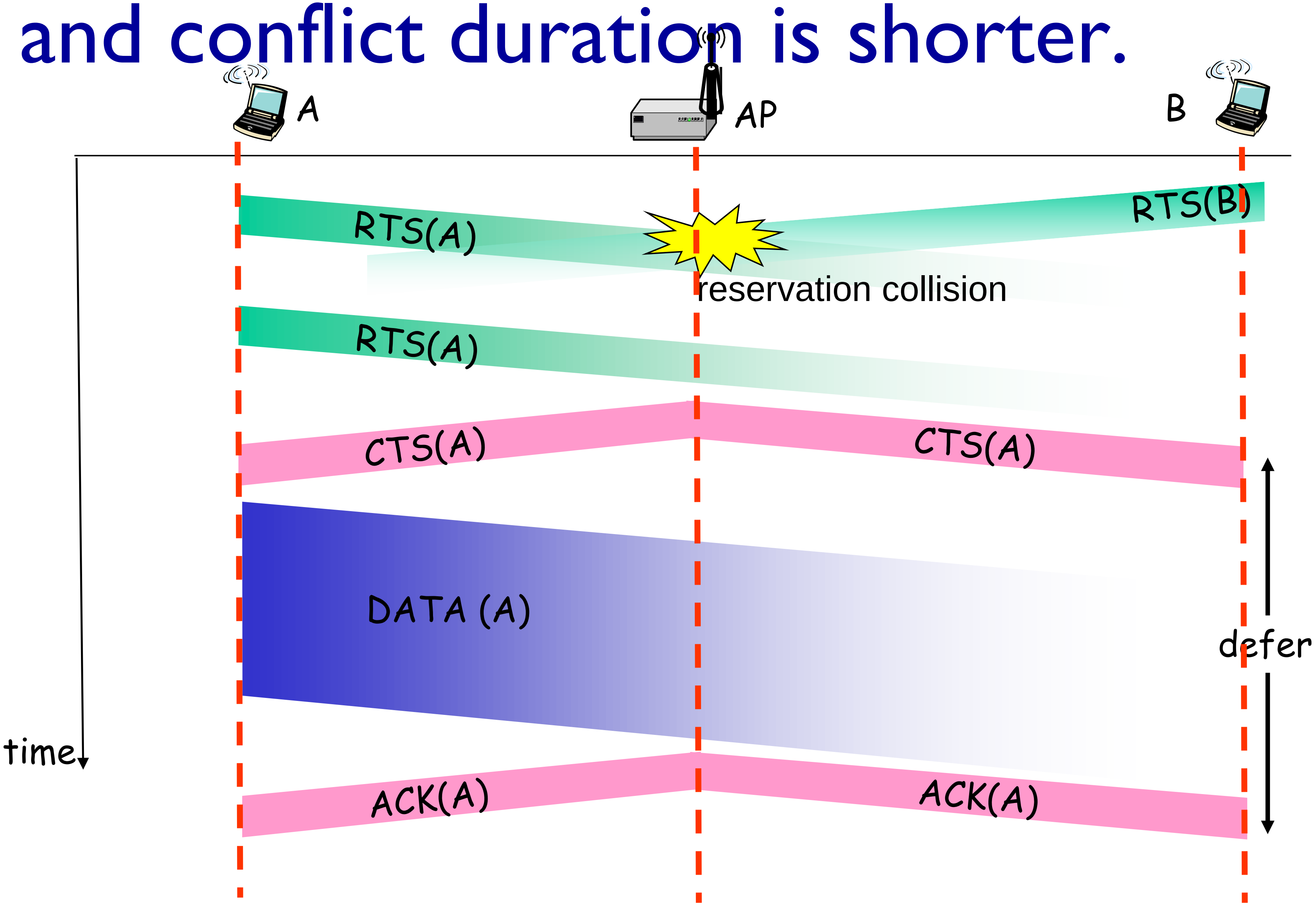
- C can receive RTS, but not CTS. and C can send data to other sites.
- D gets CTS, E gets RTS and CTS.Therefore, D and E cannot send data in the communication stage between A and B.



Use RTS and CTS to avoid conflicts



RTS and CTS frames are shorter and conflict duration is shorter.

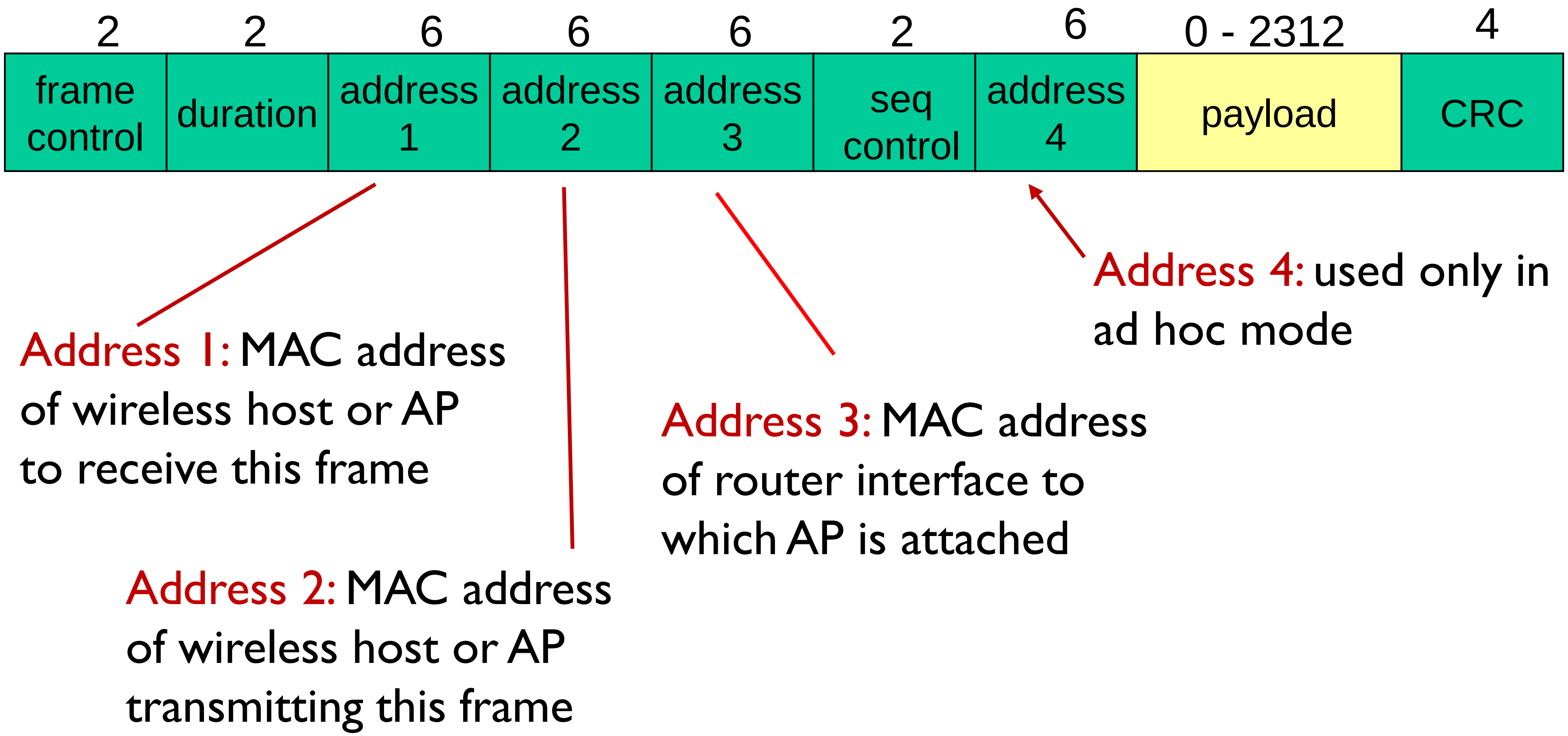


4 802.11 MAC FRAME

1. IEEE 802.11 Wireless LAN
2. 802.11 LAN architecture
3. IEEE 802.11 MAC Protocol: CSMA/CA
4. 802.11 MAC FRAME
5. 802.11: advanced capabilities

- There are three types: control frame, data frame and management frame.
- 802.11 MAC frame mainly consists of three parts: the header, frame body and frame check sequence.
- Frame header is 30 bytes in total, the complexity of the frame is reflected in the frame header.
- The data portion of the frame, no more than 2312 bytes.
- Frame check sequence FCS is the tail, 4 bytes.

802.11 frame: addressing



2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

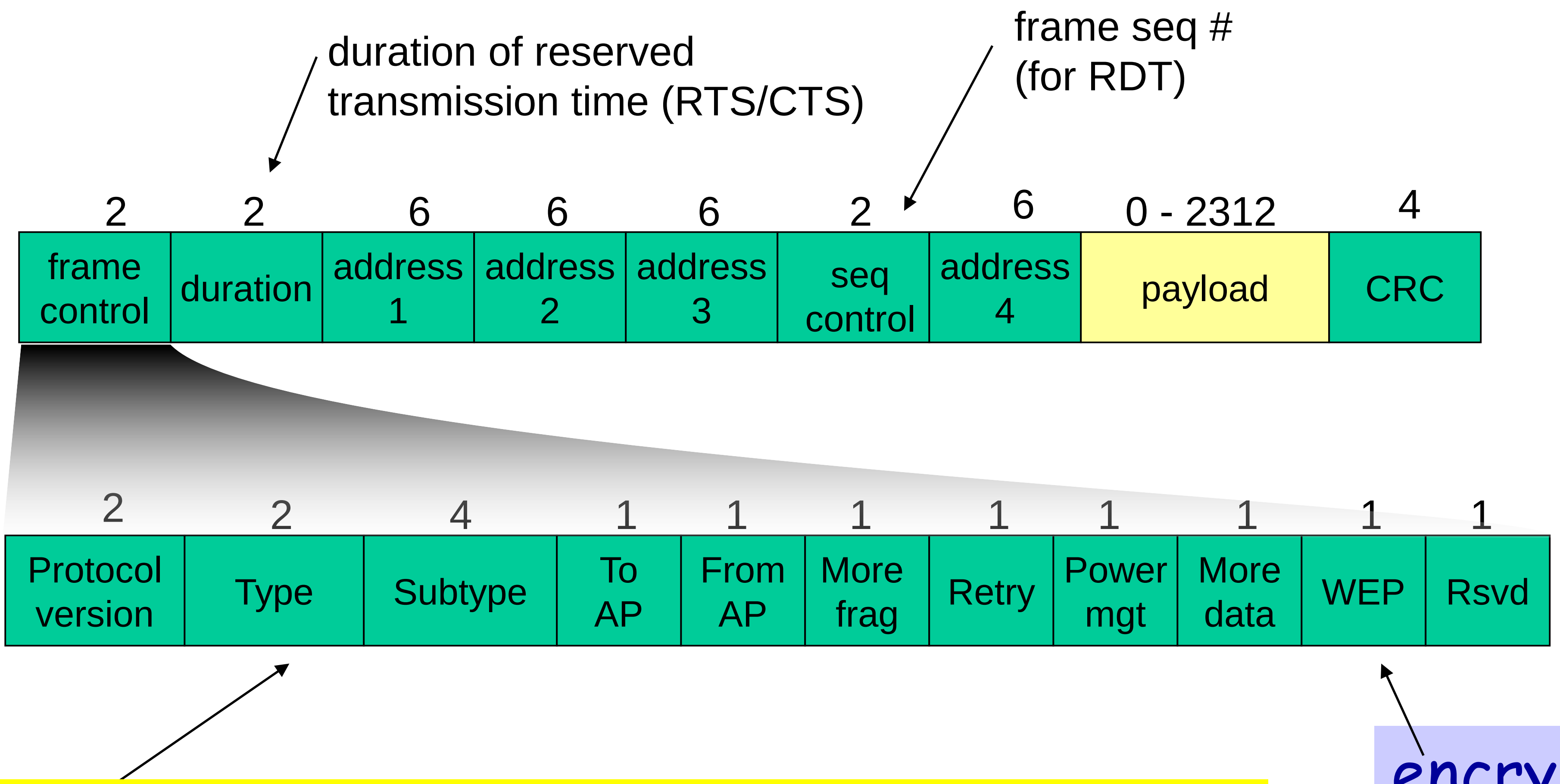
Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 frame: more



duration of reserved transmission time (RTS/CTS)

frame seq # (for RDT)

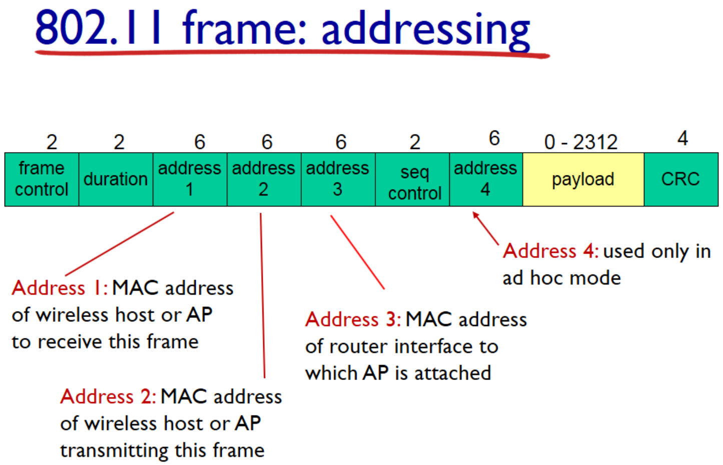
2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

2	2	4	1	1	1	1	1	1	1	1
Protocol version	Type	Subtype	To AP	From AP	More frag	Retry	Power mgt	More data	WEP	Rsvd

Frame type:management, control, and data frames. (RTS, CTS, ACK, data)

encry ption

802.11 frame's ADDR.



802.11 frame: addressing

2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

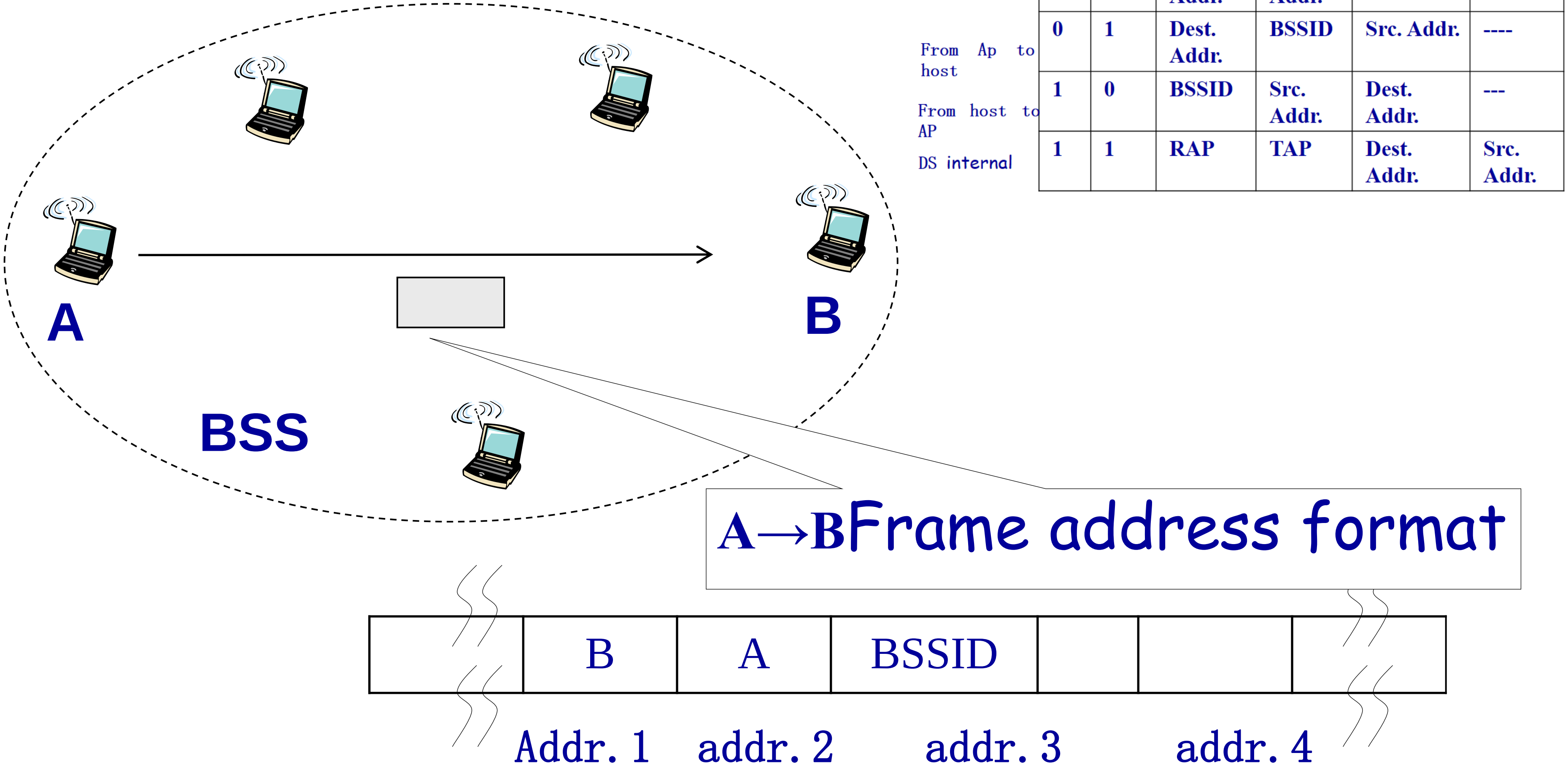
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

	to DS	from DS	ADDR. 1	ADDR. 2	ADDR.3	ADDR .4
Ad hoc	0	0	Dest. Addr.	Src. Addr.	BSSID	----
From Ap to host	0	1	Dest. Addr.	BSSID	Src. Addr.	----
From host to AP	1	0	BSSID	Src. Addr.	Dest. Addr.	---
DS internal	1	1	RAP	TAP	Dest. Addr.	Src. Addr.

Ad hoc's data Frame address format

	to DS	from DS	ADDR. 1	ADDR. 2	ADDR.3	ADDR .4
Ad hoc	0	0	Dest. Addr.	Src. Addr.	BSSID	----
From Ap to host	0	1	Dest. Addr.	BSSID	Src. Addr.	----
From host to AP	1	0	BSSID	Src. Addr.	Dest. Addr.	---
DS internal	1	1	RAP	TAP	Dest. Addr.	Src. Addr.



A→BFrame address format

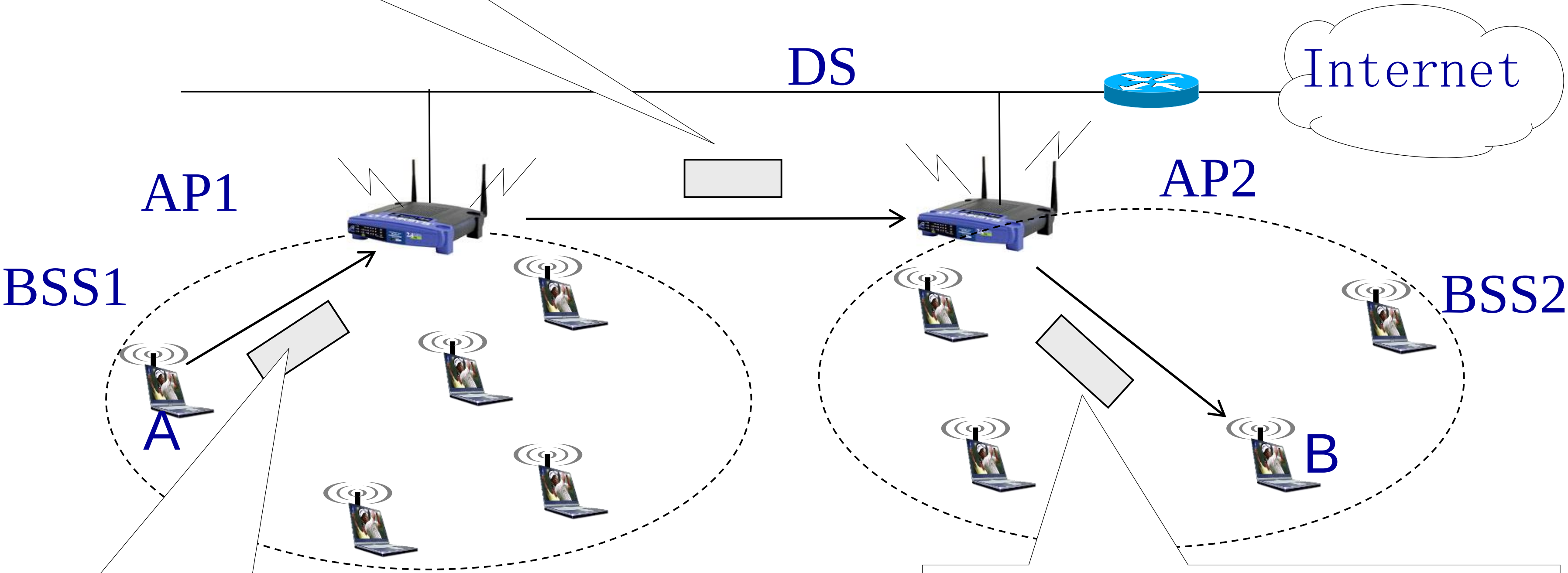
	B	A	BSSID			
	Addr. 1	addr. 2	addr. 3		addr. 4	

Frame address format

	to DS	from DS	ADDR. 1	ADDR. 2	ADDR.3	ADDR .4
Ad hoc	0	0	Dest. Addr.	Src. Addr.	BSSID	----
From Ap to host	0	1	Dest. Addr.	BSSID	Src. Addr.	----
From host to AP	1	0	BSSID	Src. Addr.	Dest. Addr.	---
DS internal	1	1	RAP	TAP	Dest. Addr.	Src. Addr.

3) AP1→AP2’s frame addr. format

	AP2	AP1	B		A	
	Addr. 1	addr. 2	addr. 3		addr. 4	



1) A→AP1frame addr. format

	AP1	A	B			
	Addr. 1	addr. 2	addr. 3		addr. 4	

2) AP2→B’s frame addr. format

	B	AP2	A			
	Addr. 1	addr. 2	addr. 3		addr. 4	

802.11 frame: addressing

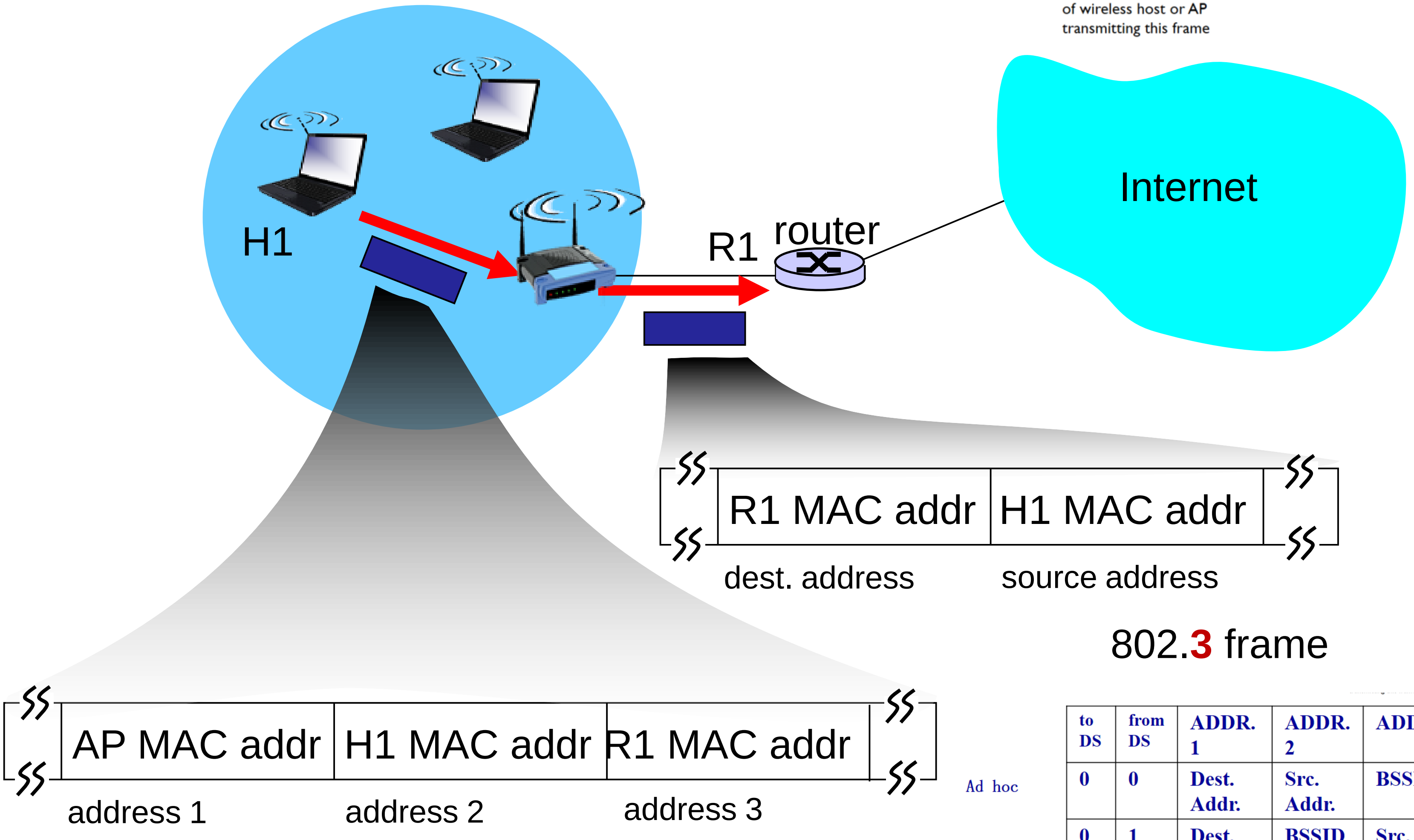
2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode



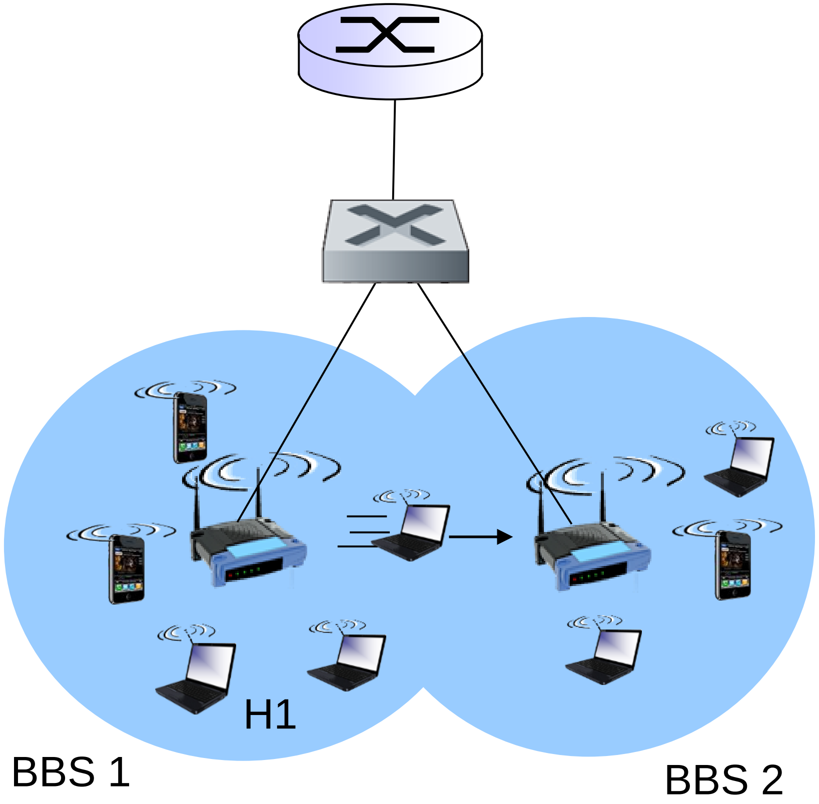
802.3 frame

802.11 frame

	to DS	from DS	ADDR. 1	ADDR. 2	ADDR.3	ADDR .4
Ad hoc	0	0	Dest. Addr.	Src. Addr.	BSSID	----
From Ap to host	0	1	Dest. Addr.	BSSID	Src. Addr.	----
From host to AP	1	0	BSSID	Src. Addr.	Dest. Addr.	---
DS internal	1	1	RAP	TAP	Dest. Addr.	Src. Addr.

802.11: mobility within same subnet

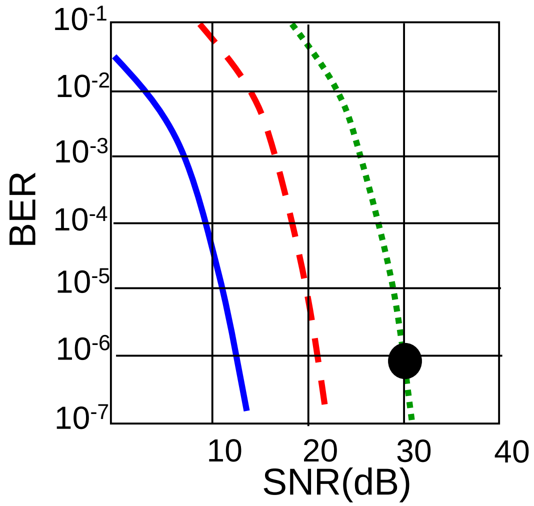
- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning : switch will see frame from H1 and "remember" which switch port can be used to reach H1

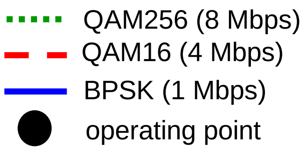


5 802.11: advanced capabilitie

Rate adaptation

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





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

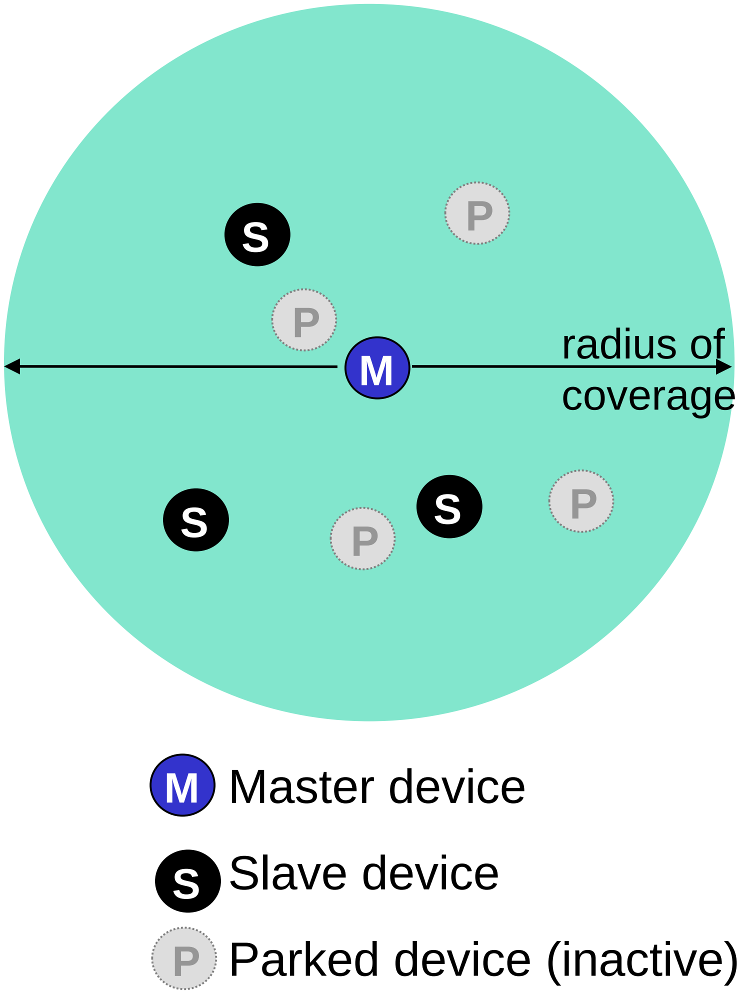
802.11: advanced capabilities

power management

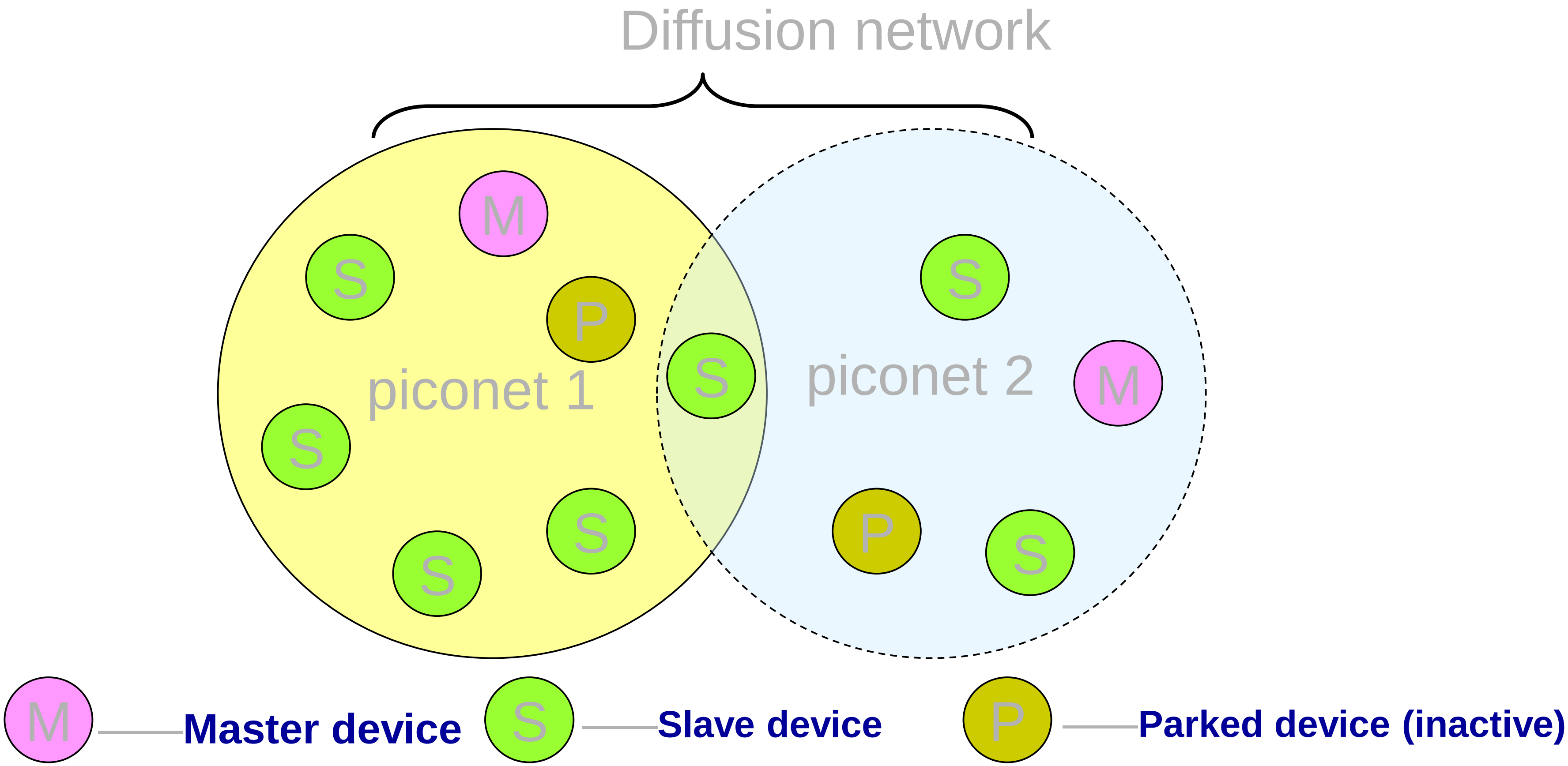
- node-to-AP: "I am going to sleep until next beacon frame"
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame

802.15: personal area network

- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- master/slaves:
  - slaves request permission to send (to master)
  - master grants requests
- 802.15: evolved from Bluetooth specification
  - 2.4-2.5 GHz radio band
  - up to 721 kbps



Piconet and diffusion net in bluetooth system



Diffusion network

piconet 1

piconet 2

M S P S S S S

S S M P S

M — Master device

S — Slave device

P — Parked device (inactive)

6.3 IEEE 802.11 wireless LANs ("Wi-Fi") - summary

1. CSMA/CA? backoff's example?
2. 802.11 frame's ADDR?
3. What's hidden terminal, exposed station ?

Chapter 6 outline

6.1 Introduction

Wireless

6.2 Wireless links, characteristics

- CDMA

6.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

6.4 Cellular Internet access

- architecture
- standards (e.g., GSM)

Mobility

6.5 Principles: addressing and routing to mobile users

6.6 Mobile IP

6.7 Handling mobility in cellular networks

6.8 Mobility and higher-layer protocols

6.9 Summary

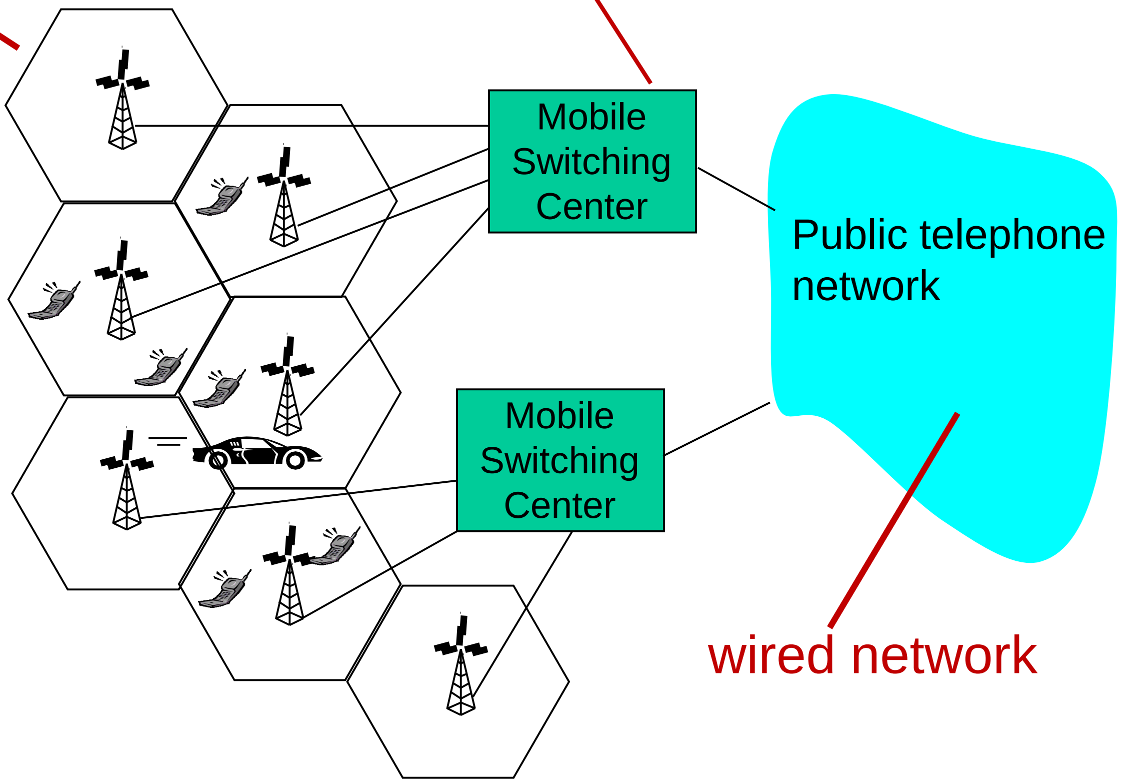
Components of cellular network architecture

MSC

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

cell

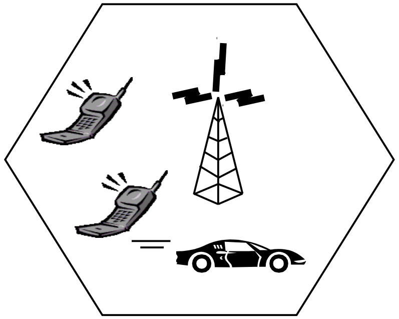
- covers geographical region
- *base station* (BS) analogous to 802.11 AP
- *mobile users* attach to network through BS
- *air-interface:* physical and link layer protocol between mobile and BS

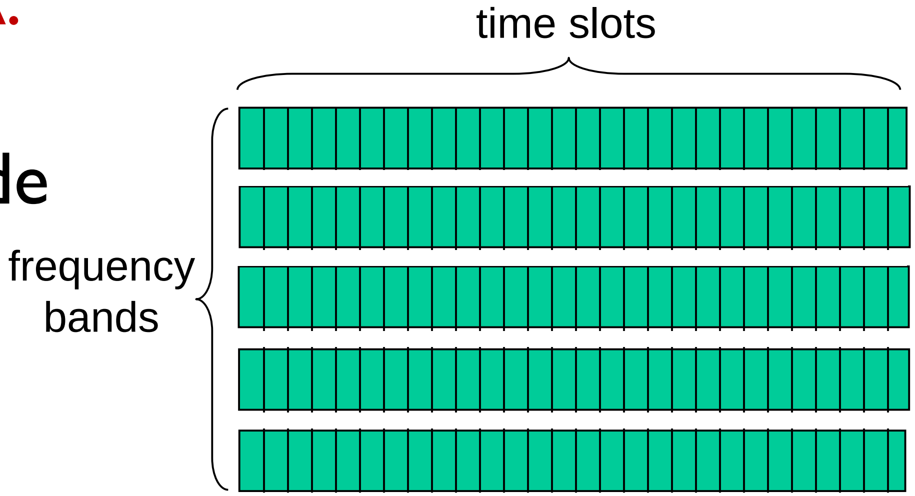


Cellular networks: the first hop

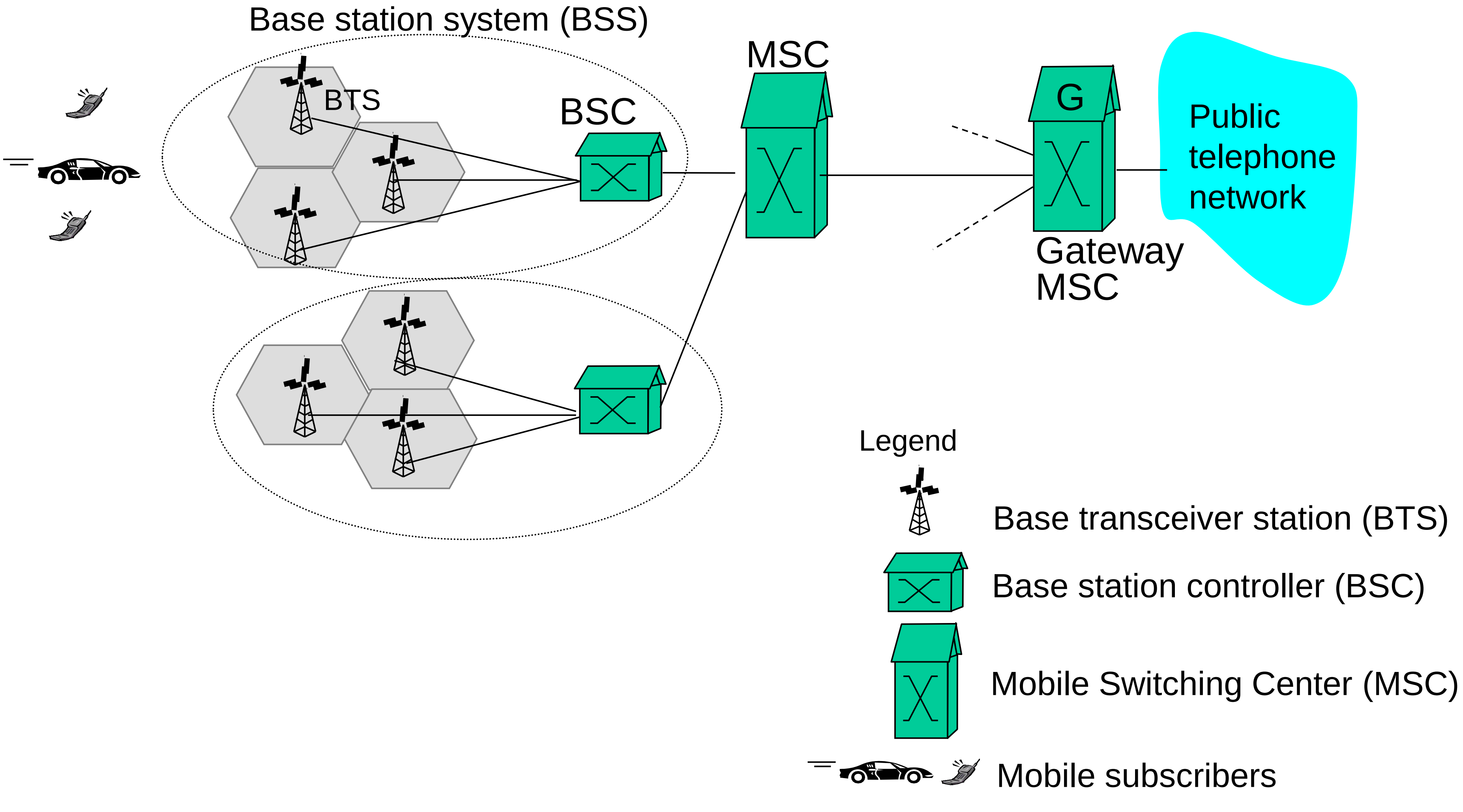
Two techniques for sharing mobile-to-BS radio spectrum

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





2G (voice) network architecture



Base station system (BSS)

BTS

BSC

MSC

G

Gateway MSC

Public telephone network

Legend

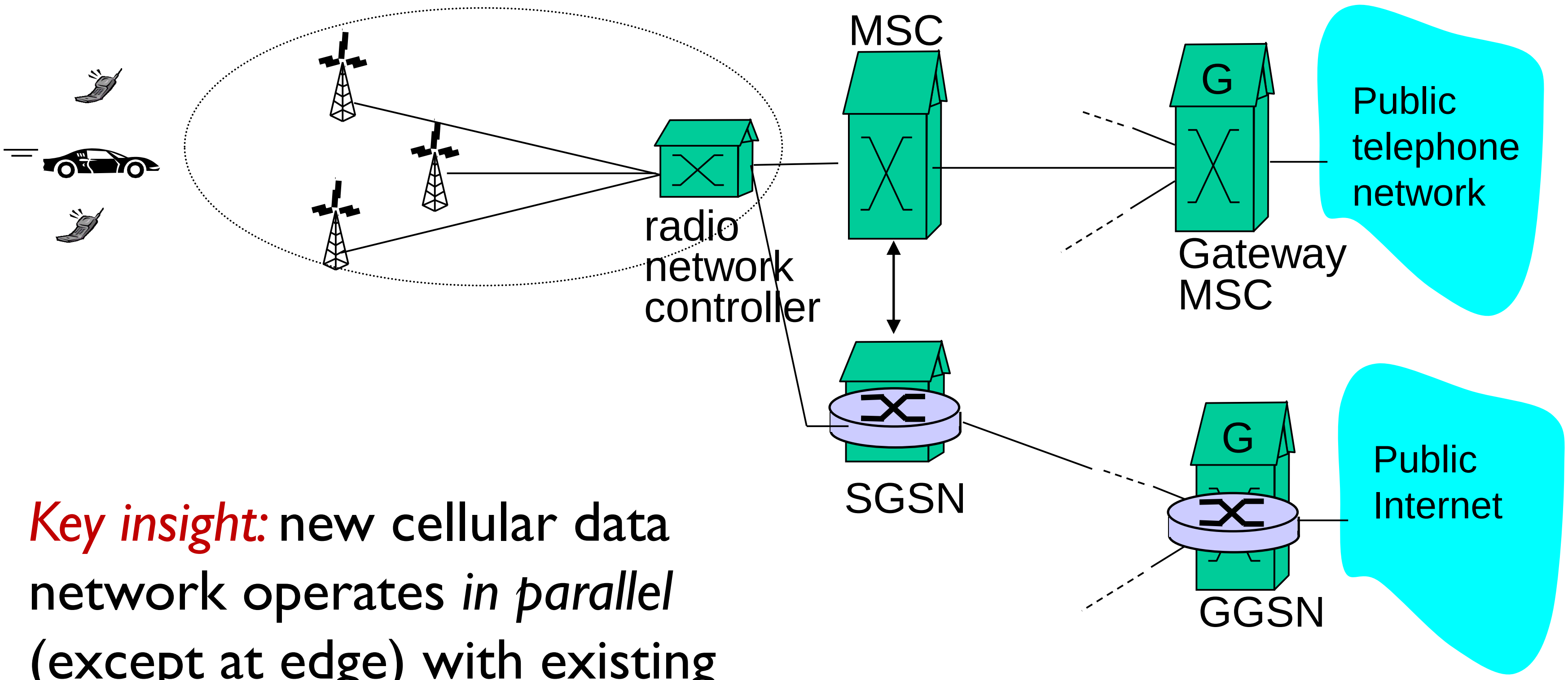
Base transceiver station (BTS)

Base station controller (BSC)

Mobile Switching Center (MSC)

Mobile subscribers

3G (voice+data) network architecture



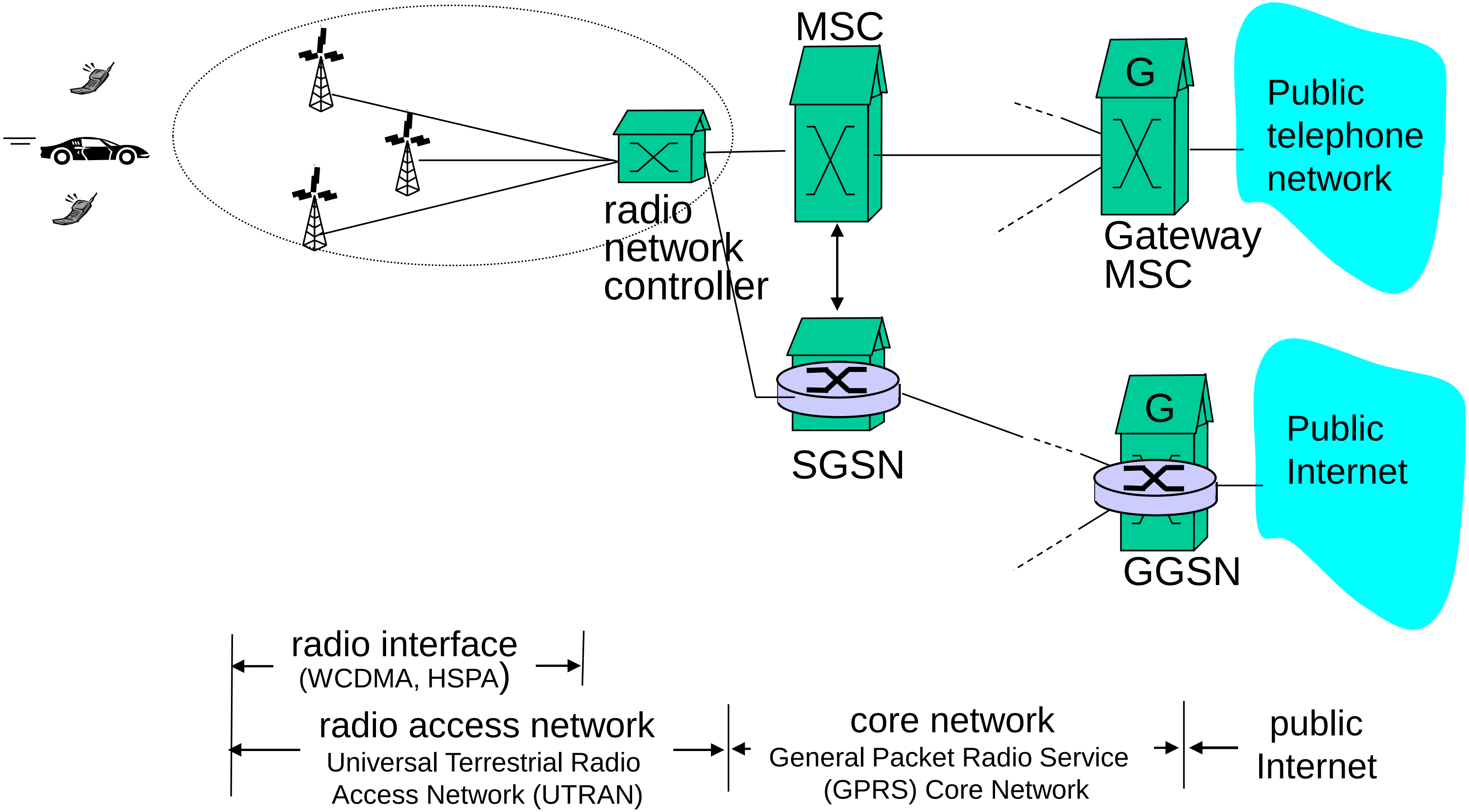
Key insight: new cellular data network operates *in parallel* (except at edge) with existing cellular voice network

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

Serving GPRS Support Node (SGSN)

Gateway GPRS Support Node (GGSN)

3G (voice+data) network architecture



MSC

G

Public telephone network

radio network controller

Gateway MSC

SGSN

G

Public Internet

GGSN

radio interface (WCDMA, HSPA)

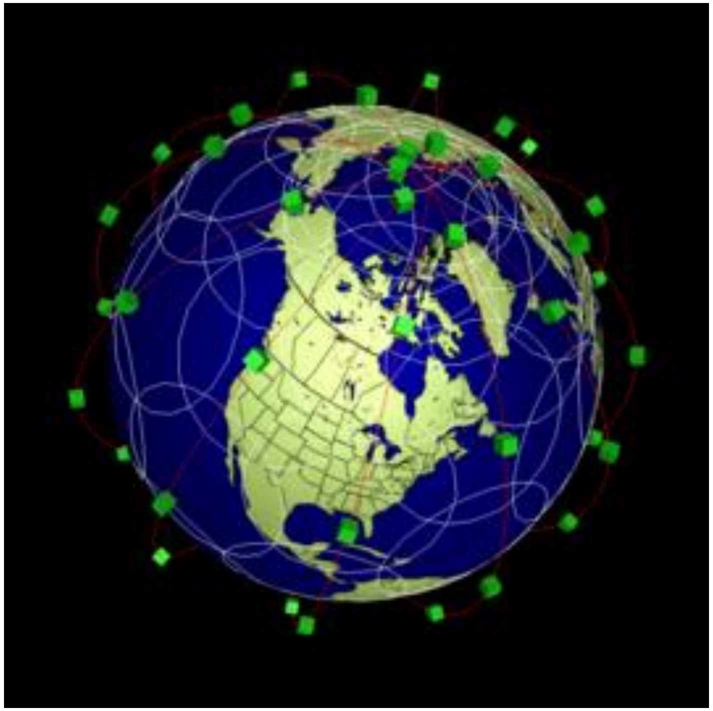
radio access network
Universal Terrestrial Radio Access Network (UTRAN)

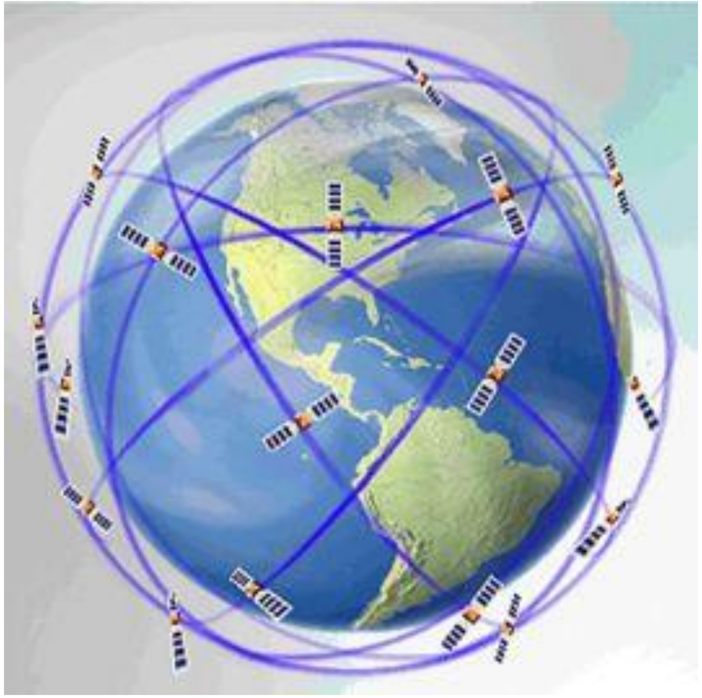
core network
General Packet Radio Service (GPRS) Core Network

public Internet

Satellite communication system

- 铱星（Iridium）系统
- Globalstar系统





802.20 technology

In terms of physical layer technology, taking OFDM((Orthogonal Frequency Division Multiplexing) and MIMO as the core, resources in time domain, frequency domain and space domain are fully explored, which greatly improves the spectral efficiency of the system.

In terms of design concept, the performance of pure IP architecture based on packet data to deal with sudden data service is also better than the existing 3G technology.

In addition, the im
have a greater adv

WiMax(Worldwide Interoperability for Microwave Access),WiMAX is 802·16

Wireless Ad hoc's network

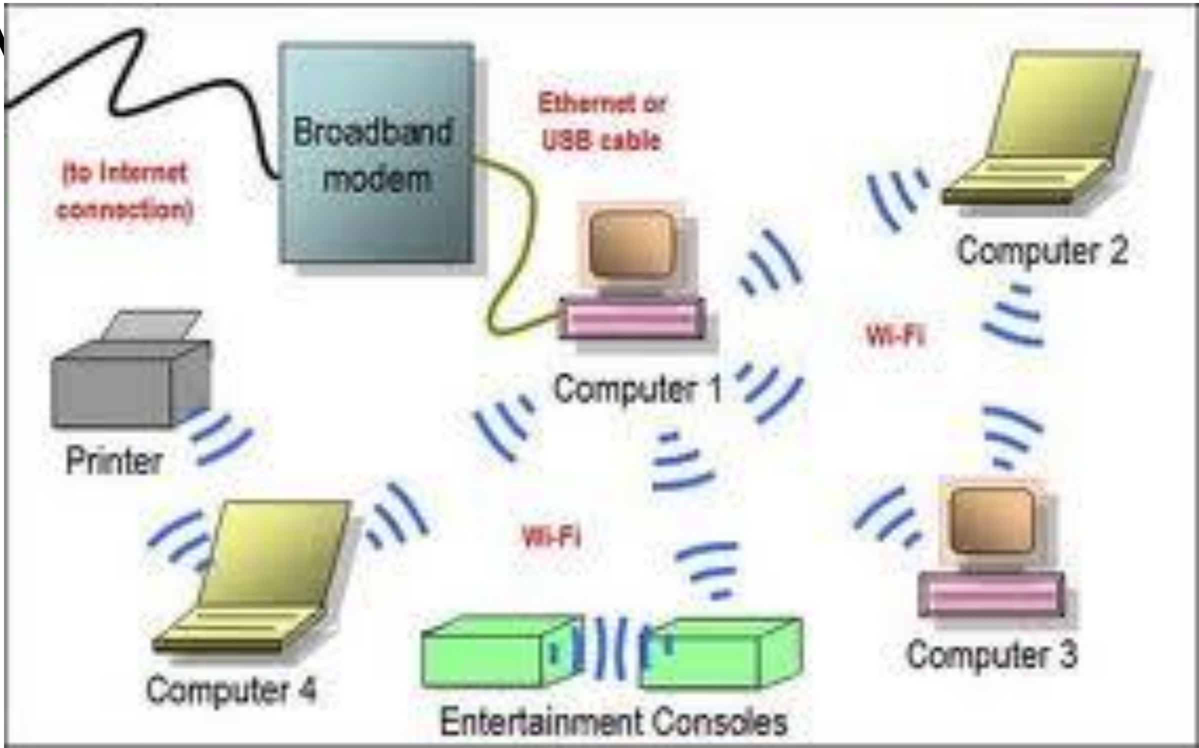
Ad Hoc derives from Latin, meaning "for this" and is extended to "for this purpose only," meaning "set for a particular purpose," meaning that Ad Hoc is a network v

purpose.IEEE802.1

the word "Ad hoc

special Ad hoc mu

network based on



Wireless Ad hoc network

1. Hierarchical structure of wireless Ad hoc network protocol, Features of wireless Ad hoc network, and definition.
2. Key technologies of wireless Ad hoc network
3. On-demand routing protocol for wireless Ad hoc networks
4. Table driven routing protocol for wireless Ad hoc networks

Look at the current wireless network architecture

Ad Hoc Networks

Wireless networks can be divided in two fundamental categories:

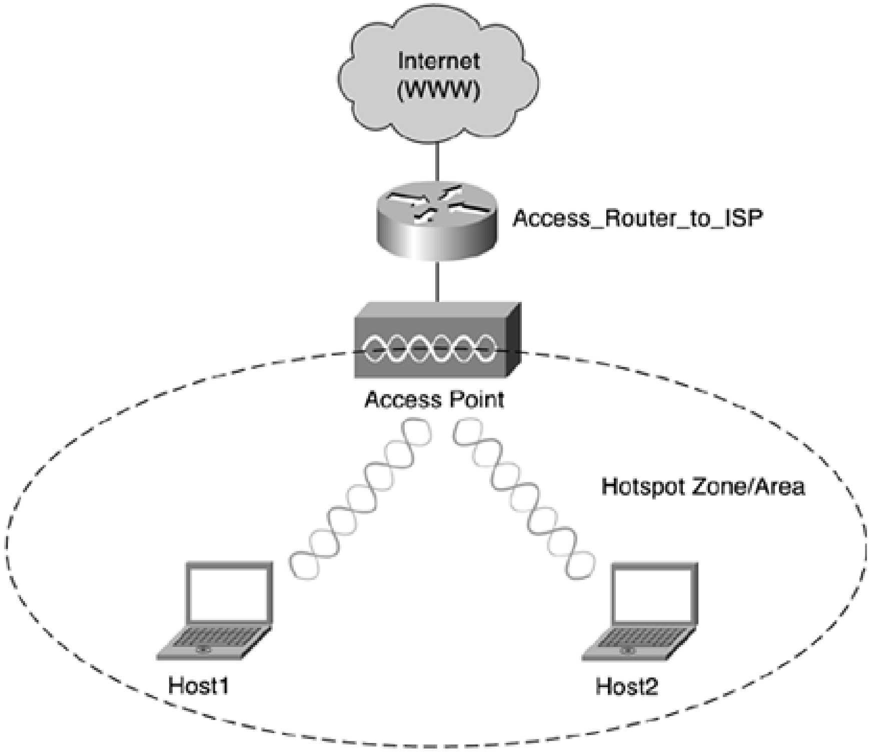
- **Infrastructure-based**

Wireless clients connecting to a base-station (APs, Cell Towers) that provides all the traditional network services (routing, address assignment)

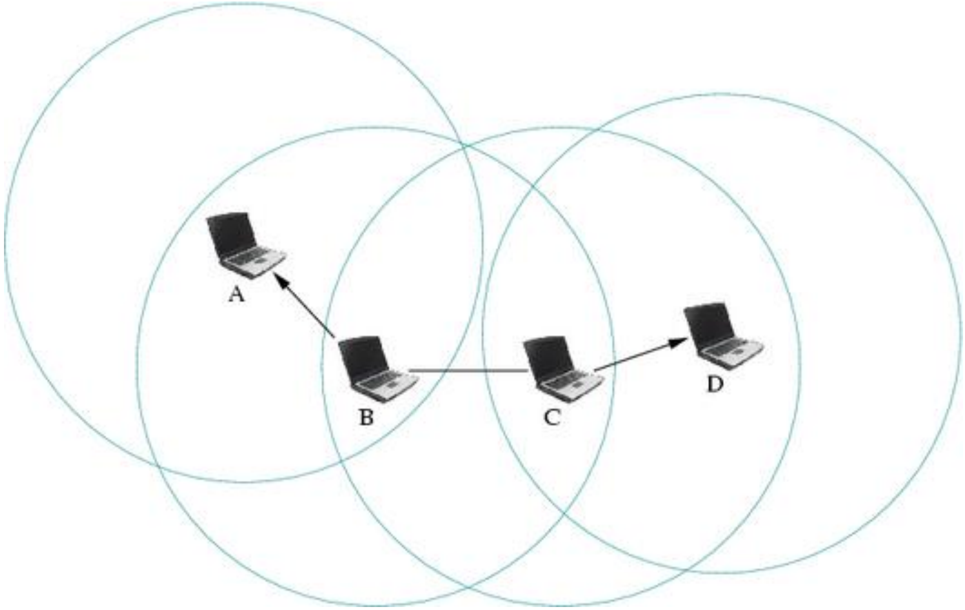
- **Infrastructure-less**

The clients themselves must provide all the traditional services to each other

Ad Hoc Networks



An infrastructure wireless network



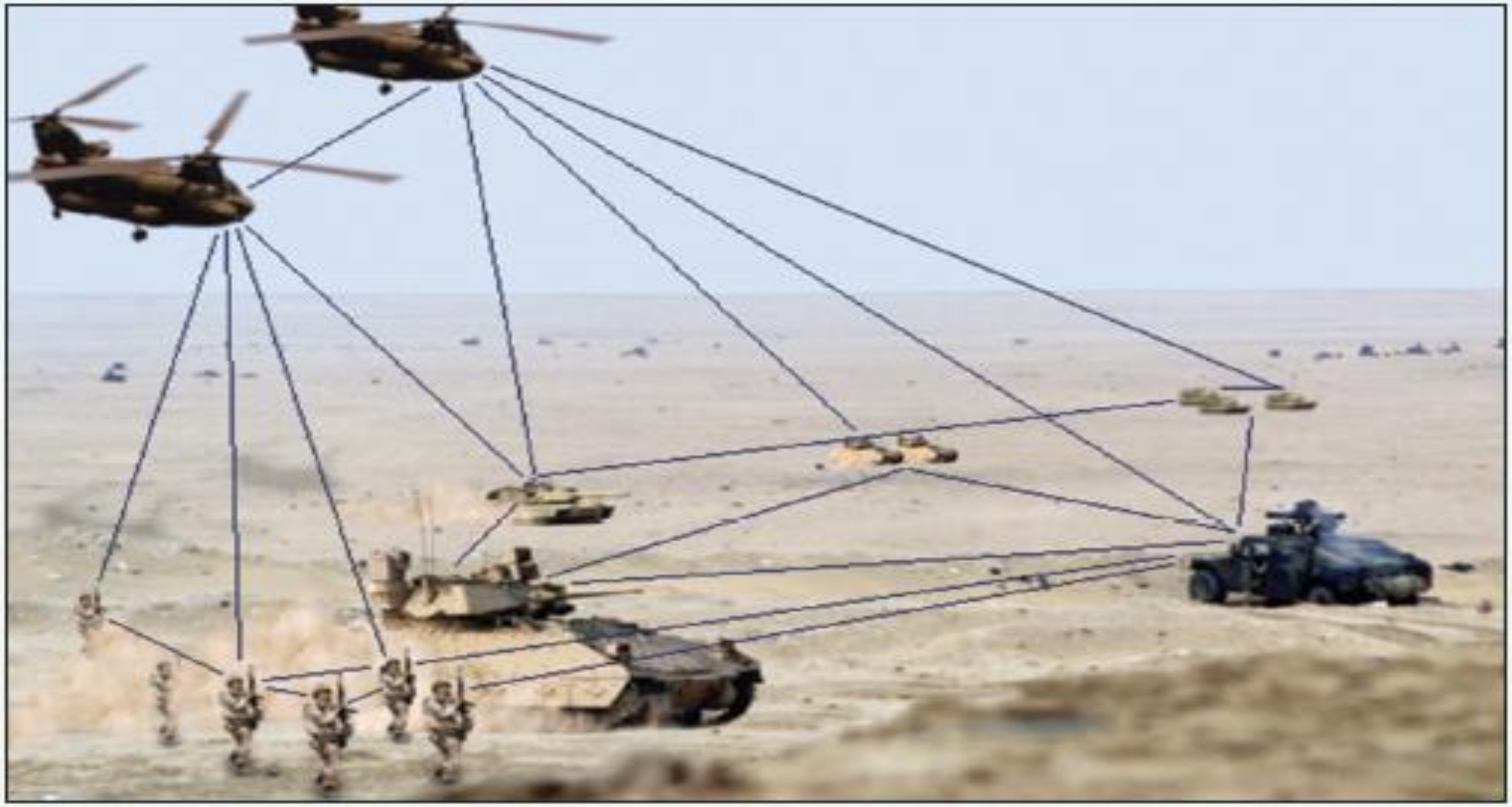
An Ad-hoc network

Ad Hoc Networks

Ad-hoc networks main features:

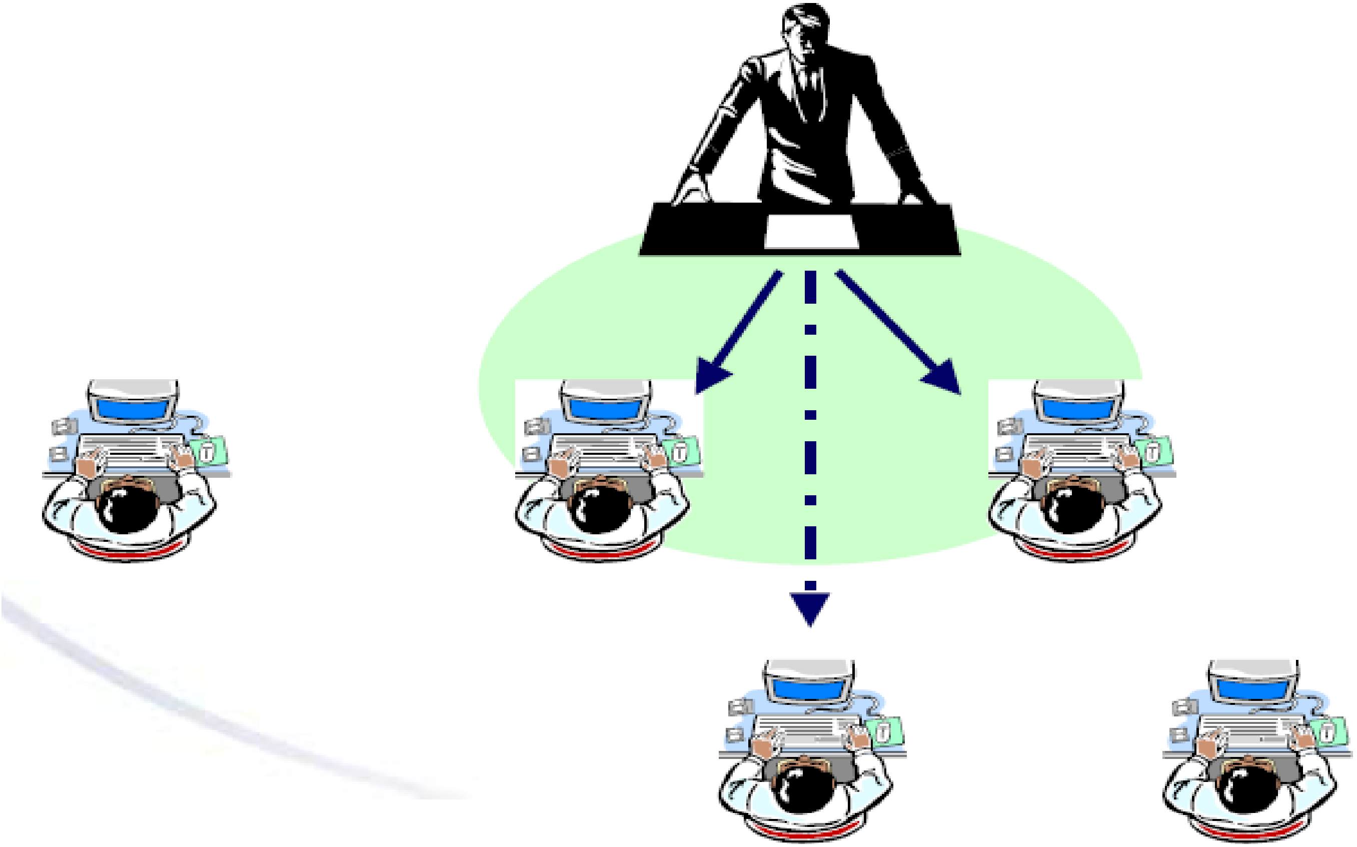
- Decentralized
- Do not rely on preexisting infrastructure
- Each node participates in routing by forwarding data to neighbor nodes
- Fast network topology changes due to nodes' movement

Military Battlefield.

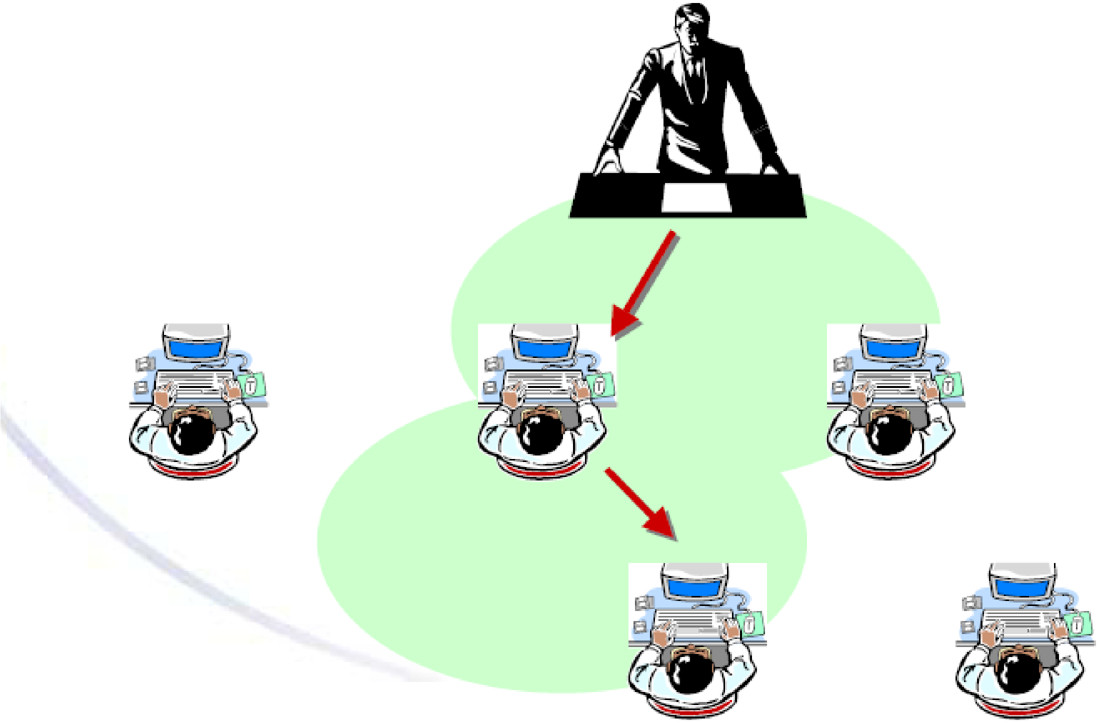


Ad hoc peer-to-peer wireless networking, or mobile mesh networking, can link battlefield forces without fixed infrastructure.

Single Hop AD-HOC

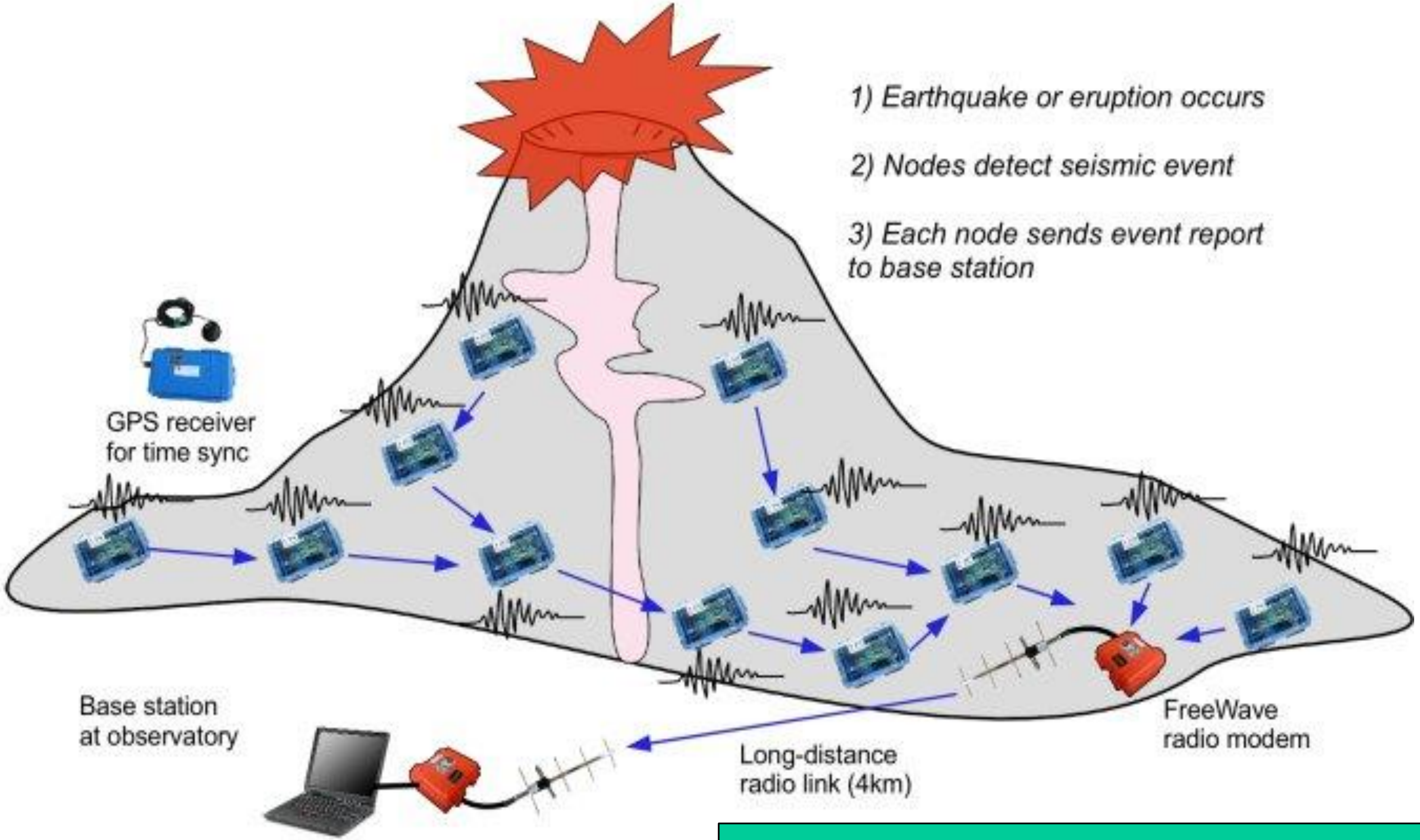


Multi-Hop AD-HOC



Source: http://ae.hc.cust.edu.tw/new_website/attachments/article/146/Lecture%2014.ppt

Wireless Sensor Networks


1) Earthquake or eruption occurs
2) Nodes detect seismic event
3) Each node sends event report to base station
GPS receiver for time sync
Base station at observatory
Long-distance radio link (4km)
FreeWave radio modem

It's other application?

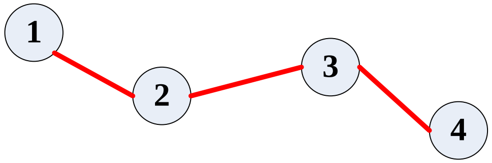
Ad Hoc Networks

Why do we need ad-hoc networks?

- ❑ More laptop users
- ❑ More smartphones users (e.g.. Android phones, iPhones)
- ❑ More devices with Wi-Fi-support (e.g.. televisions, hi-fi, home-theaters, media servers etc.)
- ❑ Moving users, vehicles, etc.
- ❑ Outdoors places

- ✓ In all these occasions there is no centralized infrastructure (such APs)
- ✓ So ad-hoc network is a necessity

Ad hoc network research

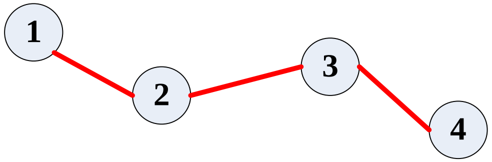


- 1991 IEEE 802.11 first proposed "Ad Hoc network"
  - Self-organizing, pair equation, multi-hop wireless mobile communication network
- In 1997, IETF established MANET working group
  - IP-based wireless multi-hop network routing
- IRTF established ANS research group in 2003
- Other research institutions

Ad Hoc：For the specific purpose only

MANET：Mobile Ad-hoc Networks
ANS：Ad Hoc Networks Scalability

Ad Hoc's defintion



- A multi-hop temporary autonomous system consisting of a group of terminal nodes with wireless communication transceiver
- Each (mobile) terminal has both router and host functions:
  - As the host....
  - As a router...
- Inter-nodes routing usually need many hops
- No network infrastructure is required and can be quickly built anywhere, anywhere

Multi-hop wireless networks, self-organizing networks, networks without fixed facilities, or peer-to-peer networks

Conclusion

What's ad-hoc?

Features of ad hoc?

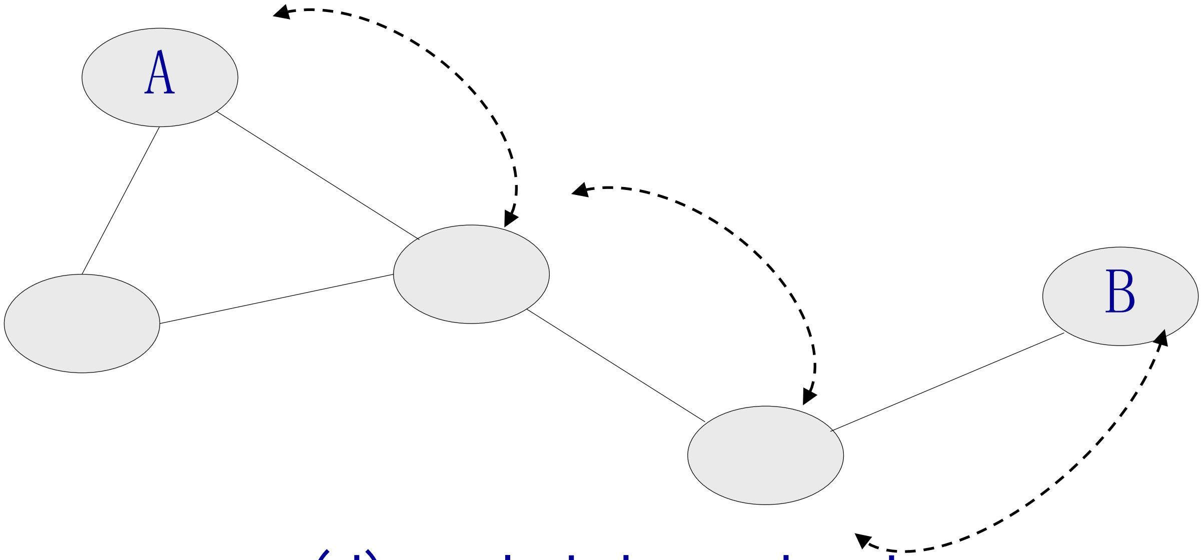
wireless Ad hoc network

1. Hierarchical structure of wireless Ad hoc network protocol, Features of wireless Ad hoc network, and definition.
2. Key technologies of wireless Ad hoc network
3. On-demand routing protocol for wireless Ad hoc networks
4. Table driven routing protocol for wireless Ad hoc networks

2 Key technologies of wireless Ad hoc network

- Ad hoc network is very different from traditional 802.11 wireless LAN and 802.16 wireless metropolitan area network in application requirements, protocol design and networking, so the research of Ad hoc network technology has its particularity.
- Research on key technologies of Ad hoc network mainly focuses on **channel access**, **routing protocol**, **QoS**, **multicast and broadcast**, and **security**.

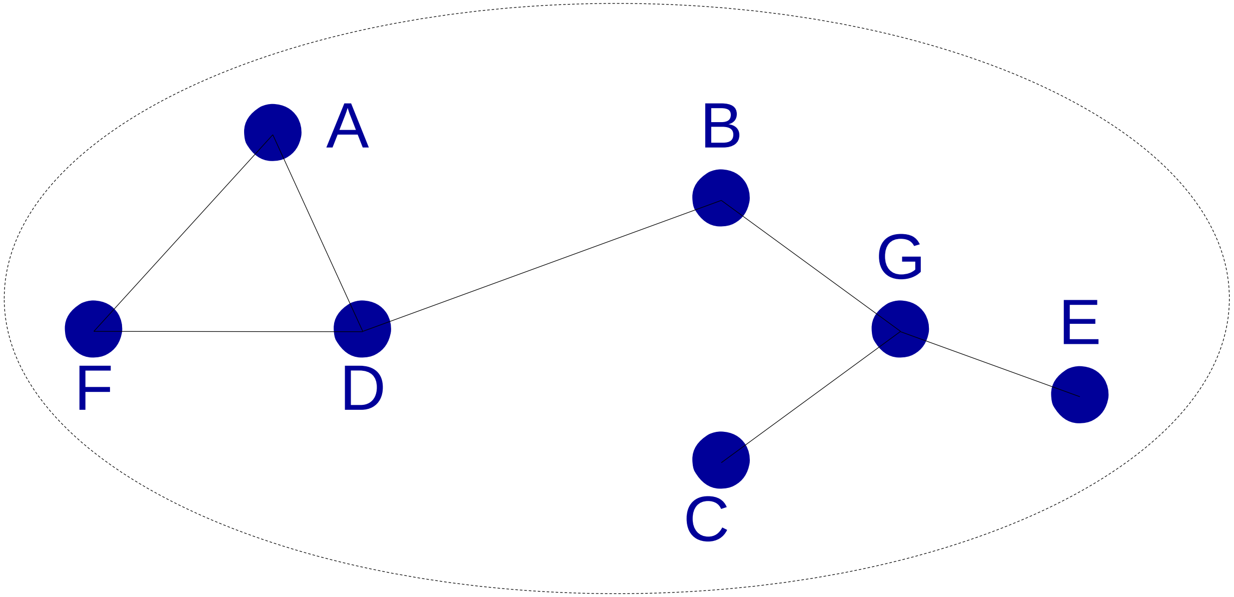
l Ad hoc networks share wireless channels in a way that is different from the wireless LAN described in the IEEE802.11 protocol. It uses "multi-hop Shared broadcast channels," but it is not one-hop Shared.



(d) multi-hop sharing

2 wireless ad hoc network structure

- Ad hoc networks generally have two structures, namely, plane structure and hierarchical structure.
- In plane structure, all nodes have equal status, so it can also be called pair equation structure.



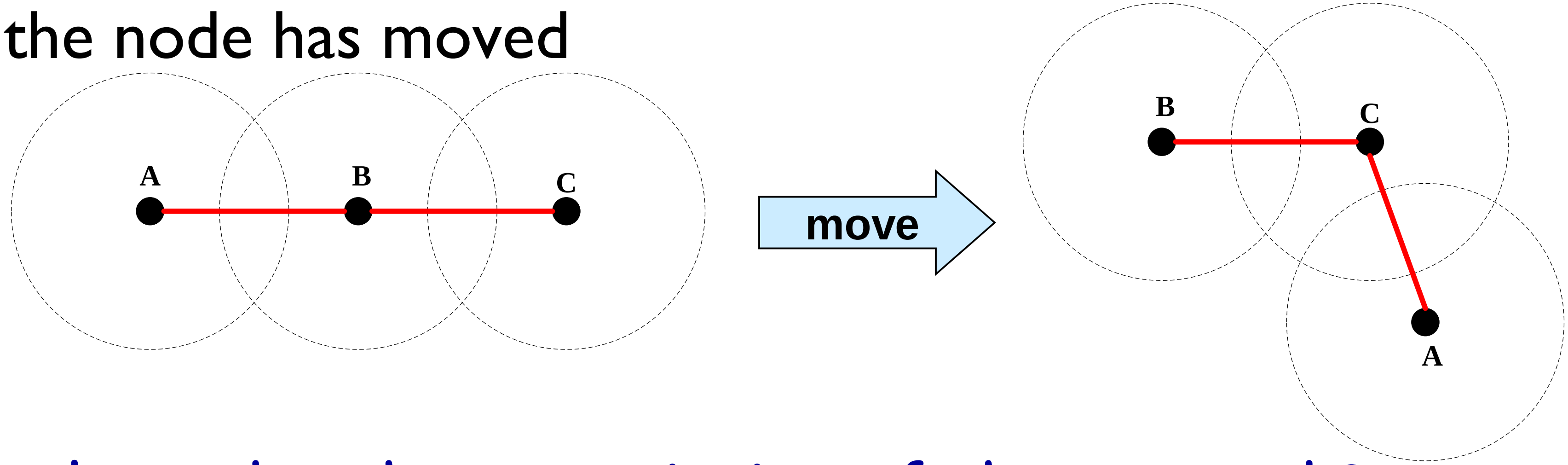
Hierarchical structure

- In the hierarchical structure, the network is divided into clusters. Each cluster consists of one cluster head and several cluster members, which form a higher-level network. In a higher-level network, clusters can be formed again to form a higher-level network up to the highest level.
- In the hierarchical structure, the cluster head node is responsible for forwarding data between clusters. For example, when node A in cluster 1 wants to communicate with node B in cluster 2,
  - Node A first sends the data to the cluster head of cluster 1;
  - The cluster head of cluster 1 analyzed and found that B forwards the data to the cluster head of cluster 2 in cluster 2 (it may need to be forwarded by other cluster heads);
  - After the cluster head of cluster 2 receives the data, it finds that B is a member of its own cluster and sends the data to B.

3 Ad hoc route protocol

- Two nodes that need to communicate may not be within the range of each other's wireless signals
- Other nodes are required to undertake the forwarding work
- A new route needs to be created after the node has moved

Multi-hop route



analyze the characteristics of the network?

1. Ad hoc route' features

1. dynamic network topology.
2. The existence of a one-way channel.
3. limited wireless transmission bandwidth.Wireless channels provide much lower network bandwidth than wired channels.In addition, the collision, signal attenuation, noise interference and so on caused by competing and sharing wireless channels.
4. limitations of wireless mobile terminals.Batteries are used to provide power, less memory and lower CPU performance.This requires the routing algorithm can be simple and effective, the implementation of the program code is short and concise, but also need to consider how to save energy and other issues.

In view of the features, can traditional routing protocols be used?

Traditional routing protocols are not suitable for Ad Hoc networks

- Dynamically changing network topology
  - Nodes join, leave, move, etc
  - Before the routing algorithm converges, the network topology changes
- Limited system bandwidth, energy and other resources
  - Periodic notification of routing information severely reduces system performance
- A one-way wireless transmission channel
  - Traditional routing protocols generally assume that links are symmetric

□ Adapt to network dynamic changes

□ Reduce routing overhead

□ Introduce on-demand routing

□ Energy and other constraints are considered in routing

Ad-hoc routing algorithms

Hottest routing algorithm categories:

❑ **Pro-active (table-driven) routing**

Maintains fresh lists of destinations & their routes by periodically distributing routing tables

Disadvantages:

1. Respective amount of data for maintenance
2. Slow reaction on restructuring and failures

(e.g. OSLR, DSDV…)

❑ **Reactive (on-demand) routing**

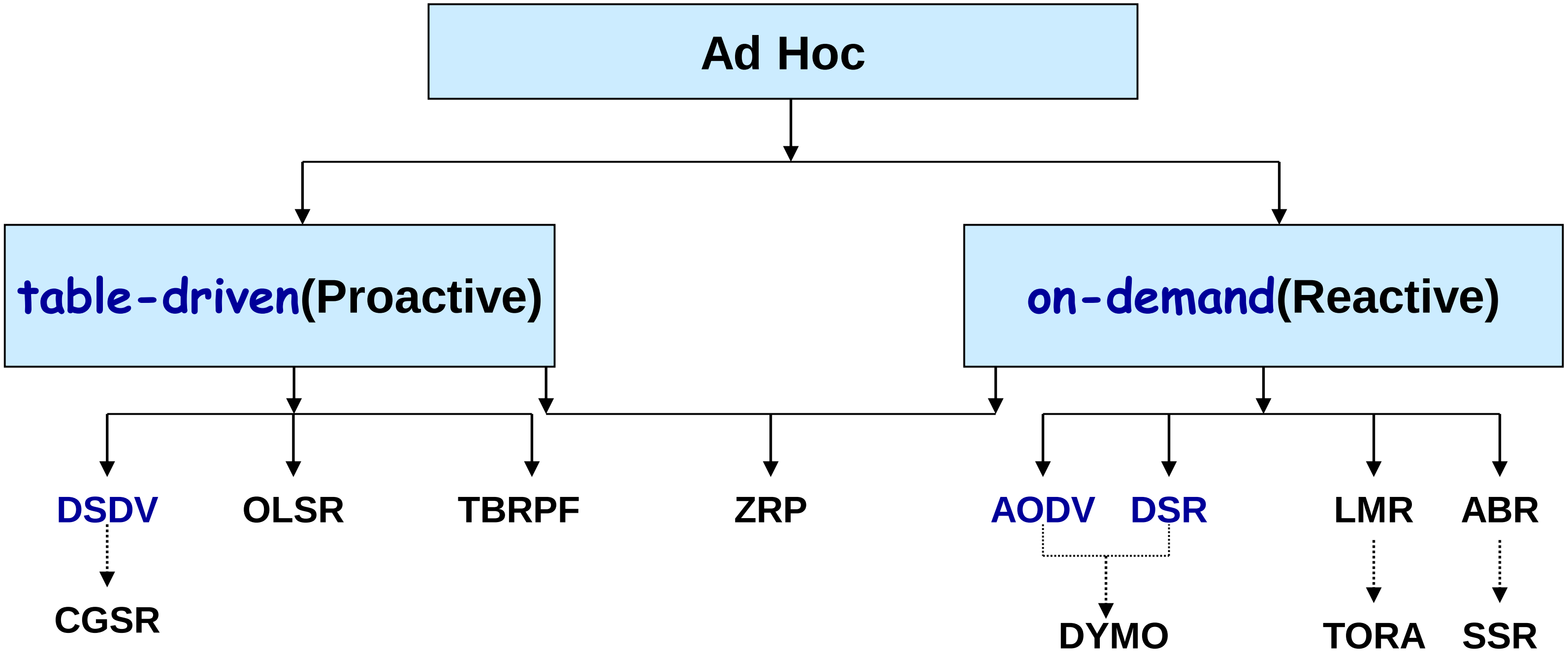
On demand route discovery by flooding the network with Route Request packets

Disadvantages:

1. High latency time in route finding
2. Flooding can lead to network clogging

(e.g. AODV, DSR…)

2. Ad-hoc routing algorithms's classification



□DSDV:Destination-Sequenced Distance-Vector Routing

□CGSR:group Capitel off switch routing protocol

□OLSR: Optimized Link State Routing

□TBRPF: Topology Dissemination Based on Reverse-Path Forwarding

□ZRP: Zone Routing Protocol

□AODV: Ad Hoc On Demand Distance Vector

□DSR: Dynamic Source Routing

□ DYMO: Dynamic MANET On-demand Routing

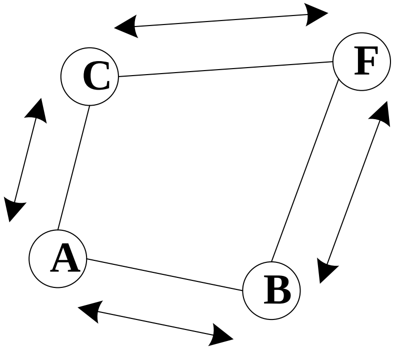
□LMR: Lightweight Mobile Routing

□ABR: Associatively-based routing

□SSR: Single stability routing

□TORA: Temporally-ordered routing

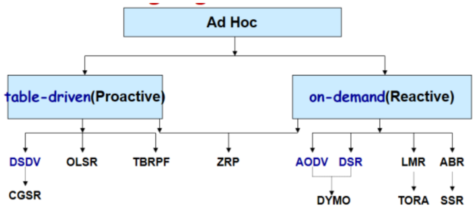
Route based on Table Driven



❖ Proactive routing

- Traditional distributed shortest path routing protocol
  - Link state or distance vector
  - *All nodes periodically update "reachable" information*
- Each node maintains a route to all other nodes in the network
- All routes exist and are readily available
- DSDV、OLSR

•Routing latency is low, but routing overhead is high



□DSDV:Destination-Sequenced Distance-Vector Routing

□CGSR:group Capitel off switch routing protocol

□OLSR: Optimized Link State Routing

□TBRPF: Topology Dissemination Based on Reverse-Path Forwarding

□ZRP: Zone Routing Protocol

□AODV: Ad Hoc On Demand Distance Vector

□DSR: Dynamic Source Routing

□ DYMO: Dynamic MANET On-demand Routing

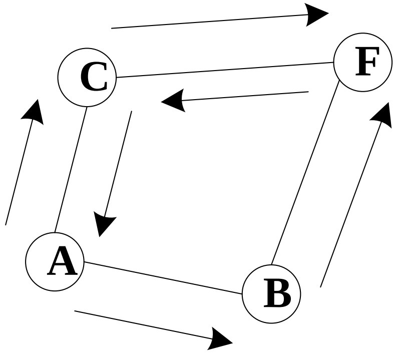
□LMR: Lightweight Mobile Routing

□ABR: Associatively-based routing

□SSR: Single stability routing

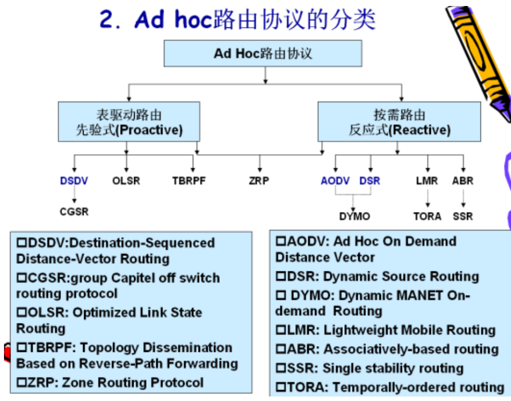
□TORA: Temporally-ordered routing

Route based on On-demand



- Reactive routing
  - The source node determines the route through the route discovery process as needed
  - The flood control system is adopted for control messages
- Implementation technology
  - Source routing (groups carry complete routing information)
- DSR、AODV

•Routing delay is large, but routing overhead is small



2. Ad hoc路由协议的分类

Ad Hoc路由协议

表驱动路由
先验式(Proactive)

按需路由
反应式(Reactive)

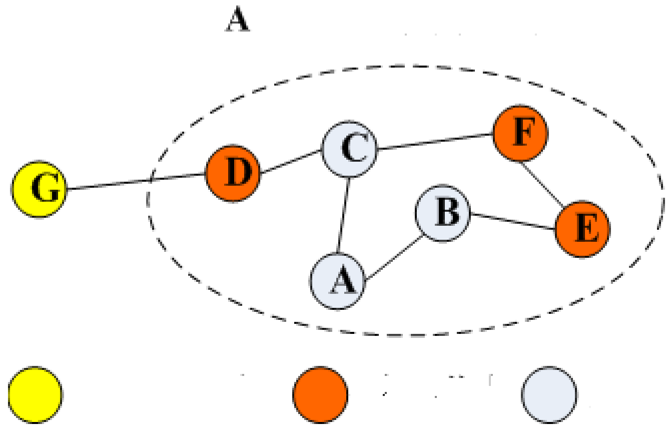
DSDV OLSR TBRPF ZRP AODV DSR LMR ABR

CGSR DYMO TORA SSR

□DSDV:Destination-Sequenced Distance-Vector Routing
□CGSR:group Capitel off switch routing protocol
□OLSR: Optimized Link State Routing
□TBRPF: Topology Dissemination Based on Reverse-Path Forwarding
□ZRP: Zone Routing Protocol

□AODV: Ad Hoc On Demand Distance Vector
□DSR: Dynamic Source Routing
□ DYMO: Dynamic MANET On-demand Routing
□LMR: Lightweight Mobile Routing
□ABR: Associatively-based routing
□SSR: Single stability routing
□TORA: Temporally-ordered routing

Hybrid routing

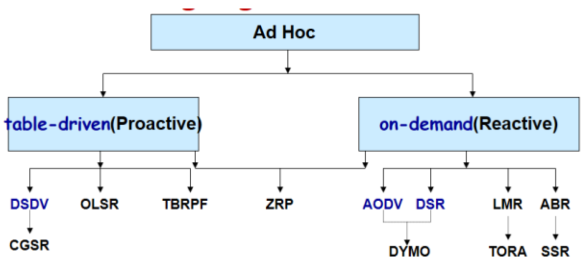


- Ad Hoc networks are divided into zone
  - Each node uses table-driven routing within the zone
  - On-demand routing is used for nodes outside the zone
- The difference between cluster and zone
  - All nodes in the cluster communicate directly with the cluster head, and the communication between nodes in the cluster is usually two hops
  - There is no limit to the size of the region, and communication between nodes in the r hop
- ZRP : Zone Routing Protocol

cluster?
zone?

SUMMARY?

- ✓ Channel access, routing protocols, etc
- ✓ In routing protocols, the characteristics of routing protocols,
- ✓ the classification of protocols.
- ✓ What is the difference between table-driven routing/on-demand driven routing/hybrid routing?...



□DSDV:Destination-Sequenced Distance-Vector Routing
□CGSR:group Capitel off switch routing protocol
□OLSR: Optimized Link State Routing
□TBRPF: Topology Dissemination Based on Reverse-Path Forwarding
□ZRP: Zone Routing Protocol

□AODV: Ad Hoc On Demand Distance Vector
□DSR: Dynamic Source Routing
□ DYMO: Dynamic MANET On-demand Routing
□LMR: Lightweight Mobile Routing
□ABR: Associatively-based routing
□SSR: Single stability routing
□TORA: Temporally-ordered routing

Ad-Hoc on-demand Distance Vector Routing (AODV) - Nokia centre Charles E. Perkins etc

- General info
- Path Discovery
- Path Maintenance
- Local Connectivity Maintenance
- An example
- Conclusion

(AODV) General info

- Reactive algorithms like AODV create routes on-demand. They must however, reduce as much as possible the acquisition time

- We could largely **eliminate** the need of periodically system-wide broadcasts

- AODV uses **symmetric** links between neighboring nodes. It does not attempt to follow paths between nodes when one of the nodes can not hear the other one

(AODV) General info

- Nodes that have not participate yet in any packet exchange (inactive nodes), they do not maintain routing information

- They do not participate in any periodic routing table exchanges

(AODV) General info

- Each node can become aware of other nodes in its neighborhood by using **local** broadcasts known as **hello messages**

- neighbor routing tables organized to :
  1. optimize response time to local movements
  2. provide quick response time for new routes requests

(AODV) General info

AODV main features:

- Broadcast route discovery mechanism
- Bandwidth efficiently (small header information)
- Responsive to changes in network topology
- Loop free routing

Outline

- Ad-Hoc on-demand Distance Vector Routing (AODV)
  - General info
  - Path Discovery
  - Path Maintenance
  - Local Connectivity Maintenance
  - An example
  - Conclusion

(AODV) Path Discovery

- Initiated when a source node needs to communicate with another node for which it has no routing info

- Every node maintains two counters:
  - node_sequence_number
  - broadcast_id

- The source node broadcast to the neighbors a route request packet (called RREQ)

(AODV) Path Discovery

- RREQ structure

<src_addr, src_sequence_#, broadcast_id, dest_addr, dest_sequence_#, hop_cnt>

- src_addr and broadcast_id uniquely identifies a RREQ

- broadcast_id is incremented whenever source node issues a RREQ

- Each neighbor either satisfy the RREQ, by sending back a routing reply (RREP), or rebroadcast the RREQ to its own neighbors after increasing the hop_count by one.

(AODV) Path Discovery

- If a node receives a RREQ that has the same <src_addr, broadcast_id> with a previous RREQ it drops it immediately

- If a node cannot satisfy the RREQ, stores:
  - Destination IP
  - Source IP
  - broadcast_id
  - Expiration time (used for **reverse path process**)
  - src_sequence_#

(AODV) Path Discovery

1. **Reverse Path Setup**

- In each RRQE there are:
  - src_sequence_#
  - the last dest_sequence_#

- src_sequence_# used to maintain freshness information about the reverse route to the source

- dest_sequnece_# indicates how fresh a route must be, before it can be accepted by the source

(AODV) Path Discovery

1.**Reverse Path Setup** (continue)

- As RREQ travels from source to many destinations, it automatically sets up the reverse path, from all nodes back to the source.

But how does it work?

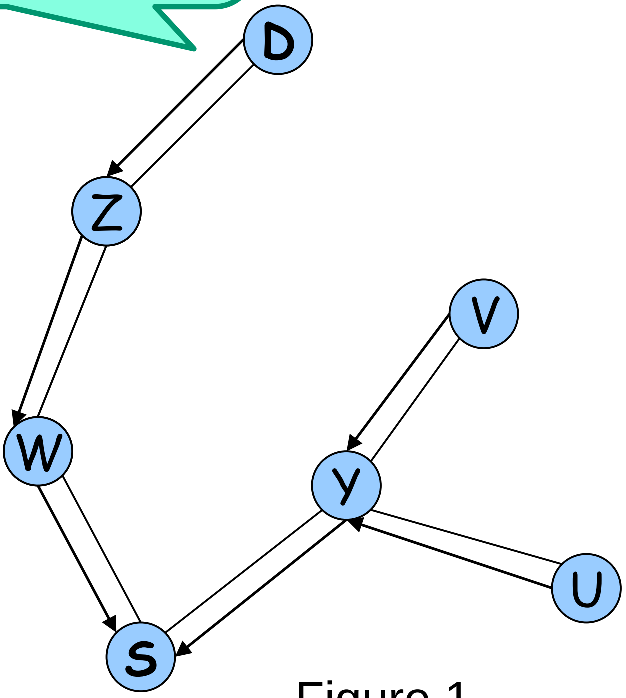
- Each node records the address of the neighbor from which it received the first copy of the RREQ

- These entries are maintained for at least enough time, for the RREQ to traverse the network and produce a reply

(AODV) Path Discovery

1. **Reverse Path Setup** (continue)

RREQ reached destination
Reversed path is fully set up
From which RREP can travel
back to S



S Source node

D Destination node

W Z Neighbor nodes

Z, V, U can not satisfy RREQ

i. Set up reverse path
ii. Rebroadcast RREQ to neighbors

S sends RREQ

Figure 1

(AODV) Path Discovery

2. Forward Path Setup

- A node receiving a RREP propagates the first RREP for a given source towards the source (using the reverse path that has already established)

- Nodes that are not in the path determined by the RREP will time out after 3000 ms and will delete the reverse pointers

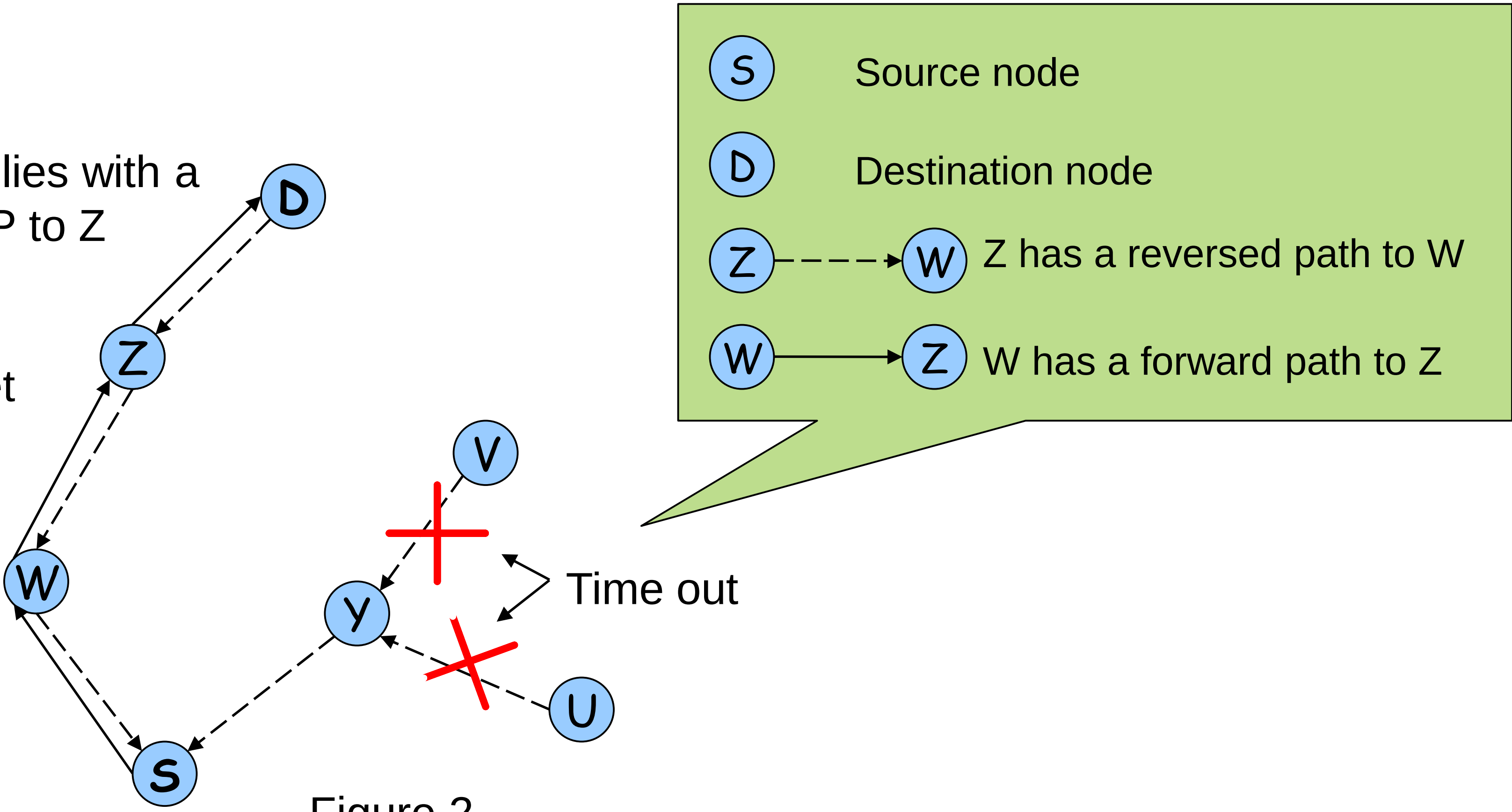
(AODV) Path Discovery

- 2. Forward Path Setup (continue)

D replies with a RREP to Z

Z receives RREP and set up a forward pointer

The same for the other nodes



Time out

Source node

Destination node

Z has a reversed path to W

W has a forward path to Z

Figure 2

(AODV) Path Discovery

2. Forward Path Setup (Conclusion)

- Minimum number of RREPs towards source

- The source can begin data transmission as soon as the first RREP received and update later its routing information if it learns of a better route

Outline

- Ad-Hoc on-demand Distance Vector Routing (AODV)
  - General info
  - Path Discovery
  - Path Maintenance
  - Local Connectivity Maintenance
  - An example
  - Conclusion

(AODV) Path Maintenance

- Movement of nodes not lying along an active path does NOT affect the route to that path's destination

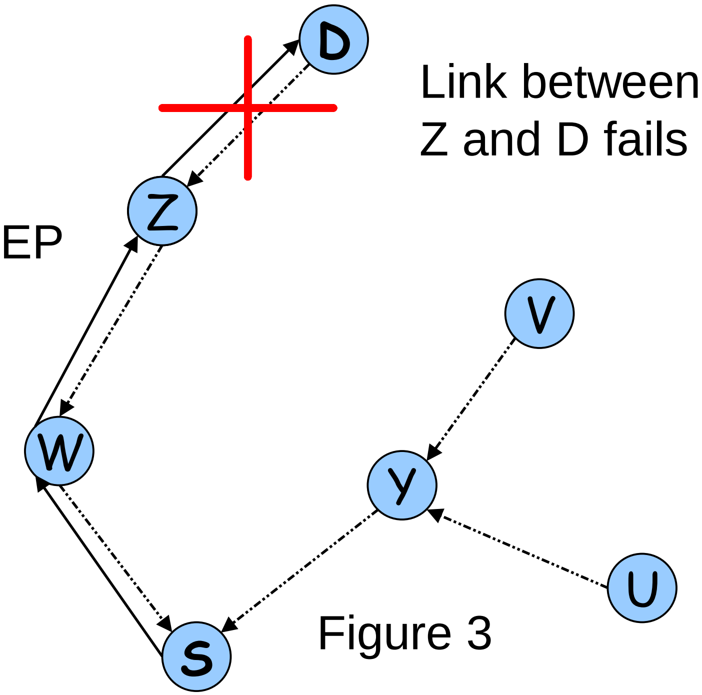
- If **the source node** moves, it can simply re-initiate the route discovery procedure

- If **the destination or some intermediate node** moves, a special RREP is sent to the affected nodes

- To find out nodes movements **periodic** hello messages can be used, or (LLACKS) link-layer acknowledgments (far less latency)

(AODV) Path Maintenance

- When a node is unreachable the special RREP that is sent back towards the source, contains a new sequence number and hop count of ∞



Link between Z and D fails

Z sents a special RREP

So do W

Figure 3

So now source must find a new path. To do that, it sents a RREQ with a new greater sequence number

Outline

- Ad-Hoc on-demand Distance Vector Routing (AODV)
  - General info
  - Path Discovery
  - Path Maintenance
  - Local Connectivity Maintenance
  - An example
  - Conclusion

(AODV) Local Connectivity Maintenance

- Nodes learn of their neighbors in one or two ways:

1. Whenever a node receives a broadcast from a neighbor it update its local connectivity information about this neighbor

2. If a neighbor has not sent any packets within hello_interval it broadcasts a **hello message**, containing its identity and its sequence number

(AODV) Local Connectivity Maintenance

How **hello messages** work:

❑ Hello messages do not broadcasted outside the neighborhood because they contain a TTL (time to leave) value of 1.

❑ Neighbors that receive the hello message update their local connectivity information to the node that have broadcasted the hello message

(AODV) Local Connectivity Maintenance

How hello messages work: (continue)

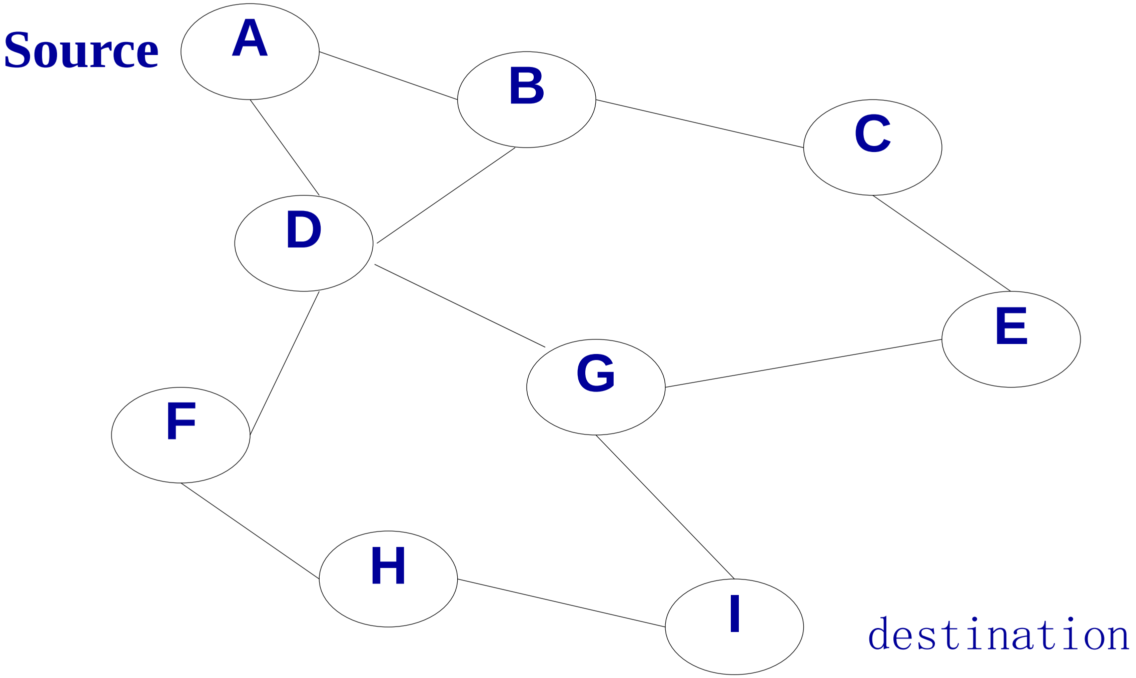
- Receiving a hello from a new neighbor, or failing to receive allowed_hello_loss (typically 2) consecutive hello messages from a node previously in the neighborhood, indicates that the local connectivity has changed

Outline

- Ad-Hoc on-demand Distance Vector Routing (AODV)
  - General info
  - Path Discovery
  - Path Maintenance
  - Local Connectivity Maintenance
  - An example
  - Conclusion

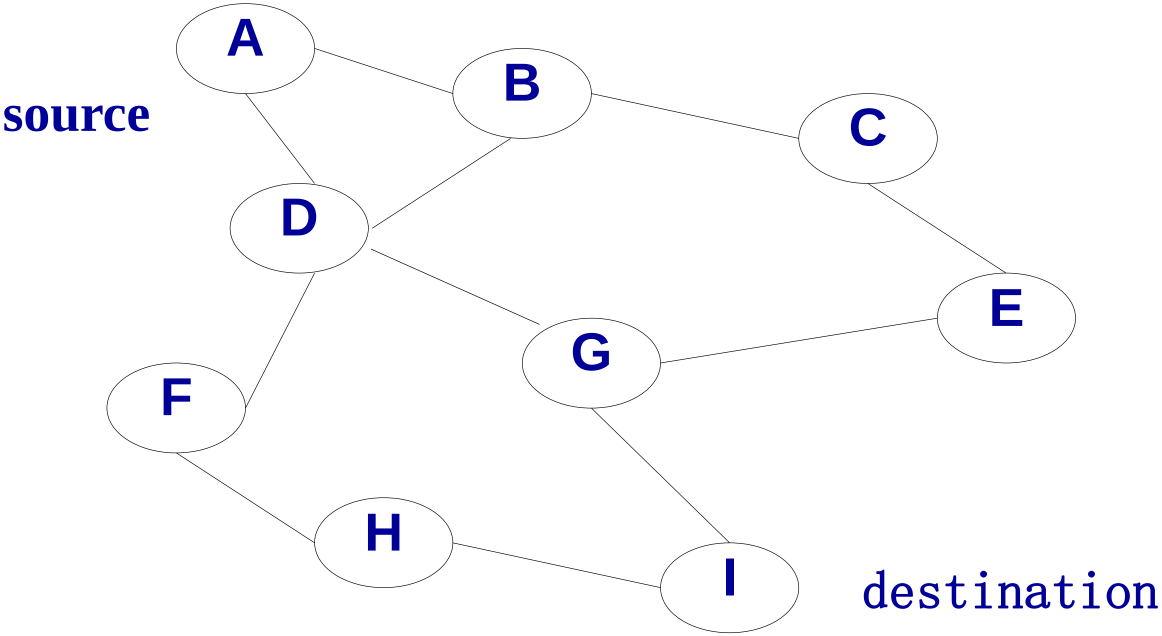
AODV ‘s example

- If source A send message to node I. Each AODV’s node has one table
- A checks the routing table, if no table entry is found about destination I, it must find A route to I. So, A creates A routing request for the **RREQ** message and broadcasts it.

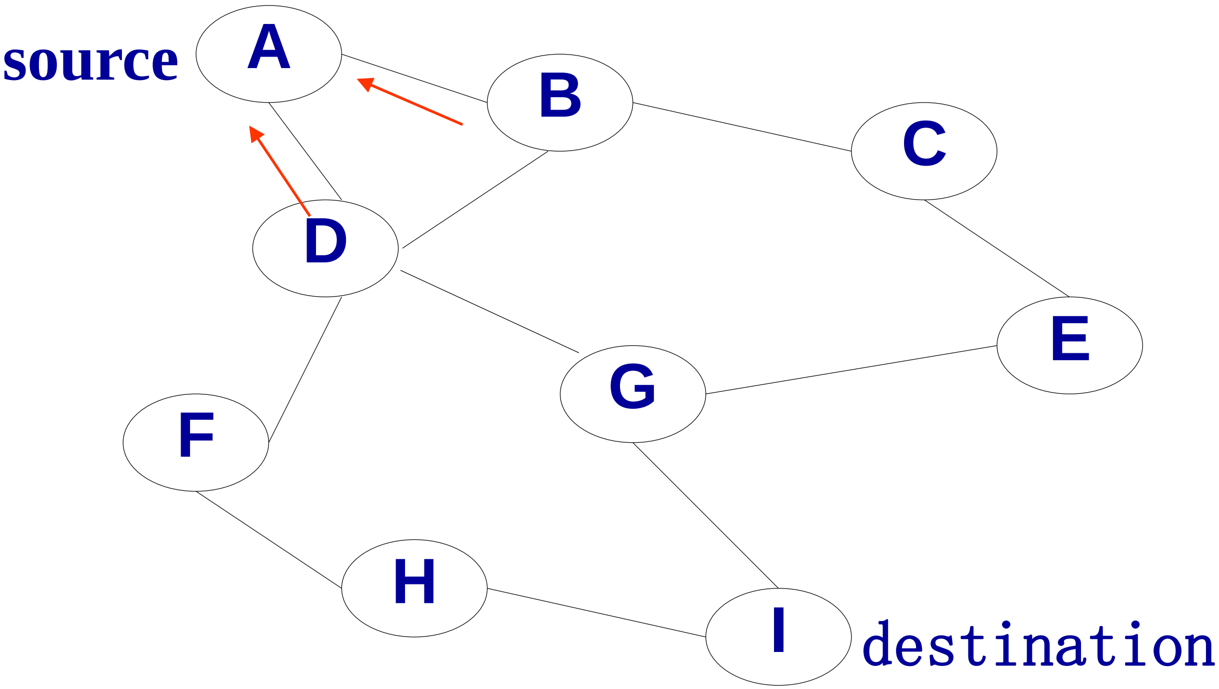


Processing of RREQ message of A by neighbor node B or D

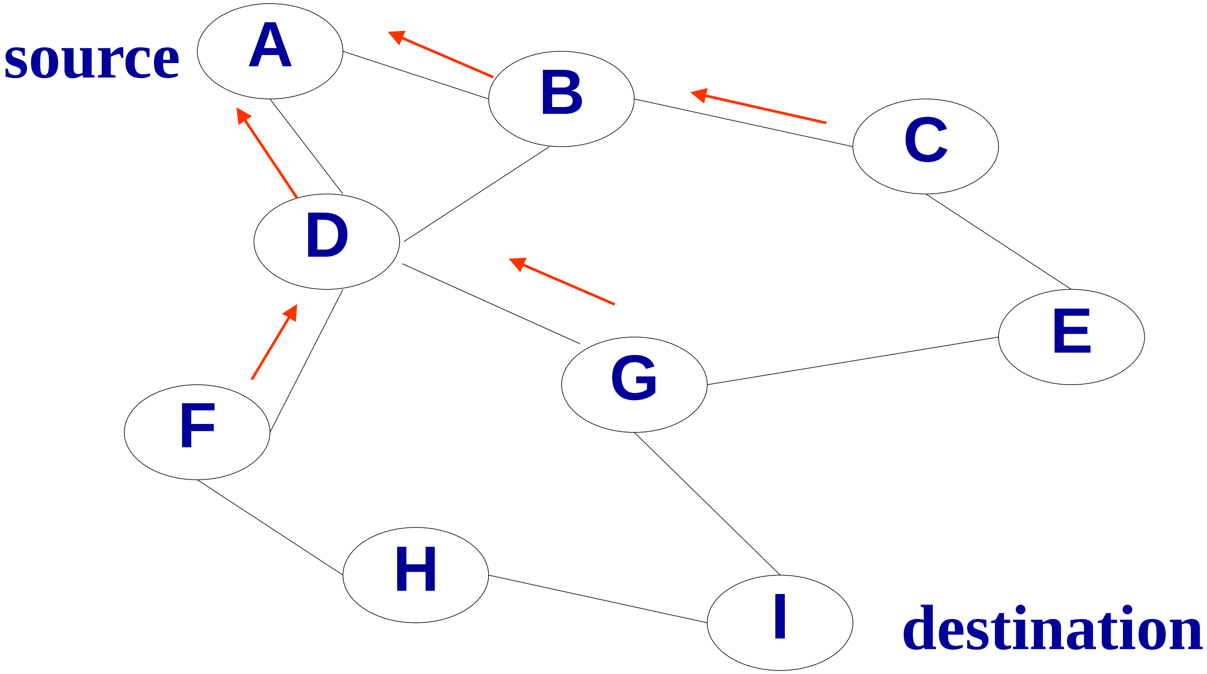
- (1) B/D after receiving A's RREQ, find < source IP address, request ID> pair, if repeated, discarded, end; If it is not repeated, the information is written to the history table. Go to step (2) .
- (2) In the routing table to find the destination address in RREQ. If A **newer** route to I is found, return the RREP message to A, or perform step (3). (**newer routes** refer to the destination number stored in the routing table >= the destination number in the RREQ message)



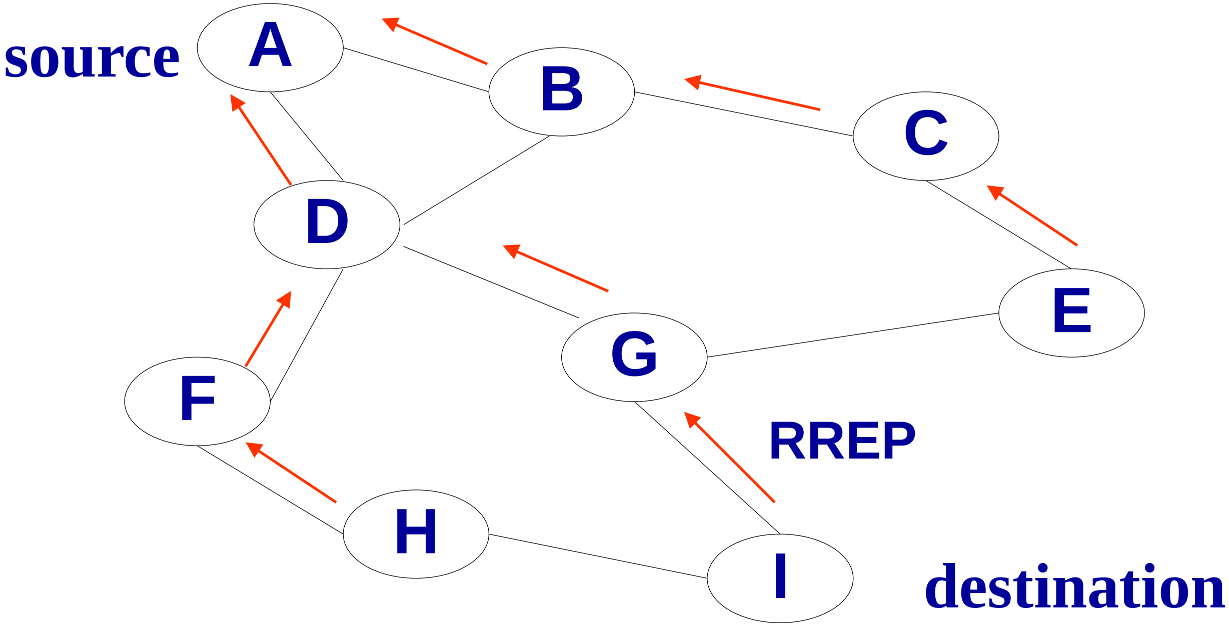
- (3) B and D do not know the newer path to I, so increase the value of the "hops" field by 1, and rebroadcast RREQ to its neighbor node.
- Construct **the reverse route** to source node A at the same time: **Dest=A, NextHop=A, HopCount=1.**
- Reverse routing is used for later routing reply messages back to the source node. Set a reverse routing lifetime at the same time.



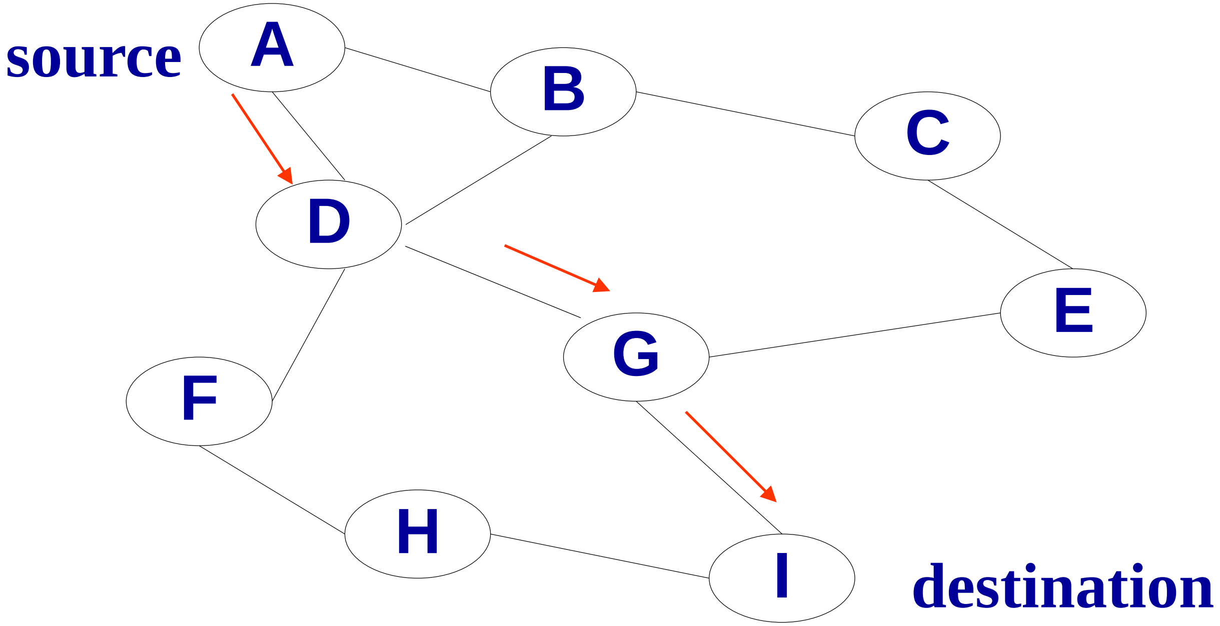
- (4) D received B RREQ, according to < source IP address, request ID> pair, discard the repeated RREQ. B does the same thing.
- (5) C receives the RREQ of B, constructs the reverse route to A: Dest=A, NextHop=B, HopCount=2, rebroadcasts the RREQ, and sets the lifetime.
- F will do something similar to C after receiving RREQ.
- After G receives the RREQ forwarded by D, it broadcasts RREQ, constructs the reverse route to A: Dest=A, NextHop=D, HopCount=2, and sets the lifetime.



- 6) after node I receives the routing request message forwarded by node G, it establishes the reverse routing Dest=A, NextHop=G, HopCount=3 to the source node A
- then return an RREP along the reverse route.



- (7) I use unicast to send RREP to G, because I received RREQ from G. After G receives the routing reply message, it establishes the forward route to node I: Dest=I, NextHop=I, HopCount = 1, LifeTime, and unicast RREQ to node D.
- (8) D received RREP after the implementation of similar to the operation of the 7th step.
- (9) after receiving RREP, establishe forward routing to I: Dest=I, NextHop=D, HopCount=3, LifeTime.



AODV routing maintenance process

- In Ad hoc networks, the topology of a network often changes.AODV routing maintenance process, the following three points need to be explained.
- the movement of nodes unrelated to active routing does not affect the route from source node to destination node;
- The routing discovery process is reinitiated by the source node if the source node movement makes the route unavailable;
- When the destination node or the intermediate node of the active route moves, the link will be interrupted, and the "upstream node" of the link will actively send a RERR message.

Outline

- Ad-Hoc on-demand Distance Vector Routing (AODV)
  - General info
  - Path Discovery
  - Path Maintenance
  - Local Connectivity Maintenance
  - Conclusion

(AODV) Conclusion

AODV main features:

- Nodes store only the routes they need
- Need for broadcast is minimized
- Reduces memory requirements and needless duplications
- Quick response to link breakage in active routes
- Loop-free routes maintained by use of destination sequence numbers
- Scalable to large populations of nodes

AODV

AODV main features

Path Discovery (Reverse Path Setup,Forward Path Setup)

Path Maintenance

Local Connectivity Maintenance.

2018.12.13

Outline

- Dynamic Source Routing (DSR)
  - General
  - Basic Route Discovery
  - Basic Route Maintenance
  - An example
  - Conclusion

- Comparison of AODV and DSR

(DSR) General

Two main mechanisms that work together to allow the discovery and maintainance of source routes:

- Route discovery

- Route maintainance

(DSR) General

Route discovery:

- Is the mechanism by which a source node S, obtains a route to a destination D

- Used only when S attempt to send a packet to D and does not already knows a route to D

(DSR) General

Route maintainance:

- Is the mechanism by which source node S is able to detect if the network topology has changed and can no longer use its route to D

- If S knows another route to D, use it

- Else invoke route discovery process again to find a new route

- Used <u>only</u> when S wants to send a packet to D

(DSR) General

- Each mechanism operate entirely on demand

- DSR requires no periodic packets of any kind at any level

- **Uni-directional** and **asymmetric routes** support
  (e.g. send a packet to a node D through a route and receive a packet D from another route)

DSR

- 路由发现（Route Discovery）
  - Start only if the source node needs to send data
  - Helps the source node get the route to the destination node
- 路由维护（Route Maintenance）
  - Monitor the availability of the current route when the source node sends data to the destination node
  - When a network topology change causes a routing failure, switch to another route or restart the routing discovery process

Routing discovery and routing maintenance are on-demand

- ✓ **Periodic routing advertisement are not required**
- ✓ **No link state awareness is required**
- ✓ **Neighbor detection is not required**

Outline

- Dynamic Source Routing (DSR)
  - General
  - Basic Route Discovery
  - Basic Route Maintenance
  - An example
  - Conclusion

- Comparison of AODV and DSR

(DSR) Basic Route Discovery

When S wants to sent a packet to D:

- it places in the header of the packet a source route giving the sequence of hops that the packet should follow on its way to D

- S obtains a suitable source route by searching its route table

- If no route found for D, S initiate the Route Discovery protocol to dynamically find a new route to D

(DSR) Basic Route Discovery

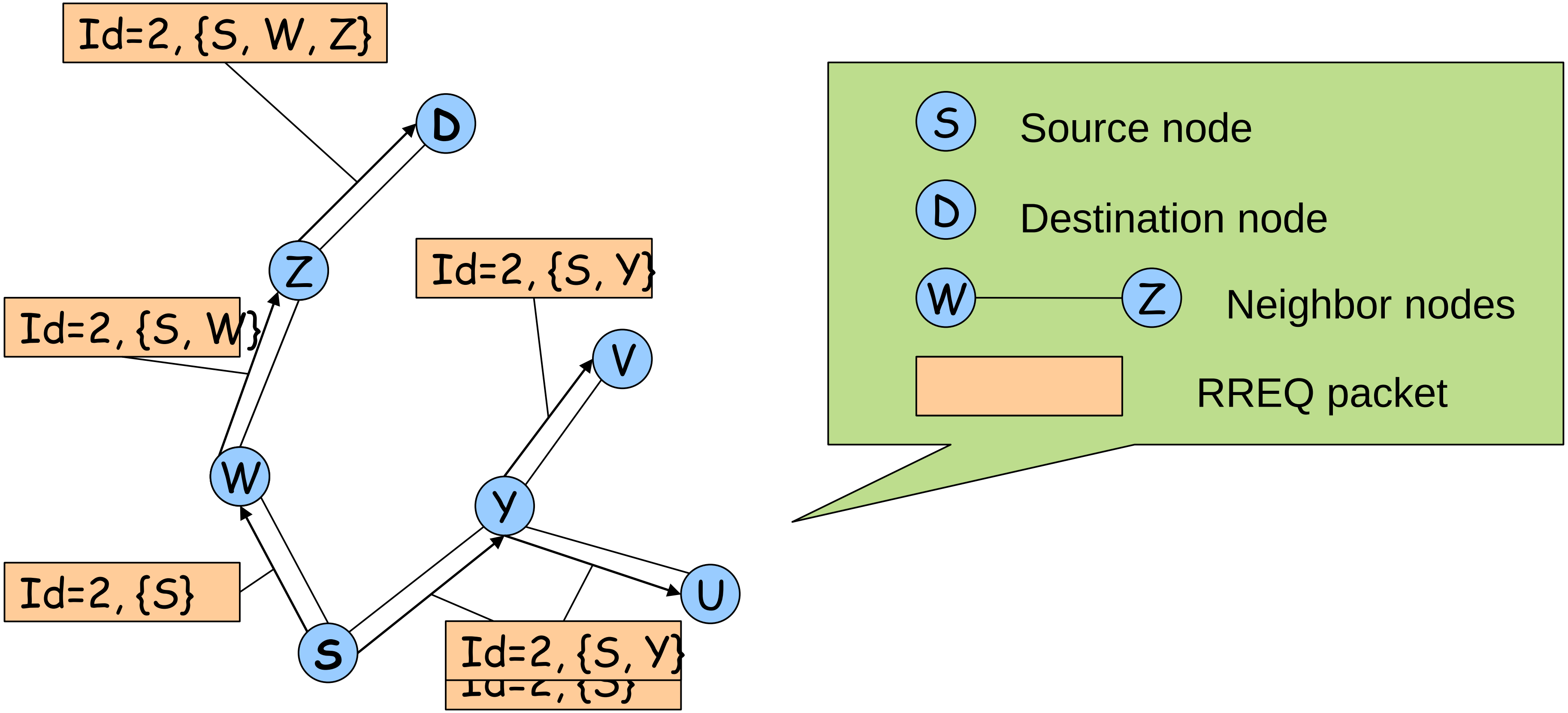
Sender

- Broadcasts a Route Request Packet (RREQ)
- RREQ contains a unique **Request ID** and the address of the sender

Receiver

- If this node is **the destination node**, or **has route to the destination** send a Route Reply packet (RREP)
- Else if is the source, drop the packet
- Else if is already in the RREQ's route table, drop the packet
- Else append the node address in the RREQ's route table and broadcast the updated RREQ

(DSR) Basic Route Discovery



S sends
RREQ

Figure 4

(DSR) Basic Route Discovery

When a RREQ reaches the destination node, a RREP must be sent back to source

The destination node:

- ❑ Examine its own Route Cache for a route back to source
- ❑ If found, it use this route to send back the RREP
- ❑ Else, the destination node starts a new Route Discovery process to find a route towards source node

✓ In protocols that **require bi-directional links** like 802.11, **the reversed route list of the RREQ packet** can be used, in order to avoid the second Route Discovery

Outline

- Ad-Hoc on-demand Distance Vector Routing (AODV)
- Dynamic Source Routing (DSR)
  - General
  - Basic Route Discovery
  - Basic Route Maintenance
  - An example
  - Conclusion
- Comparison of AODV and DSR

(DSR) Basic Route Maintenance

Each node transmitting a packet:

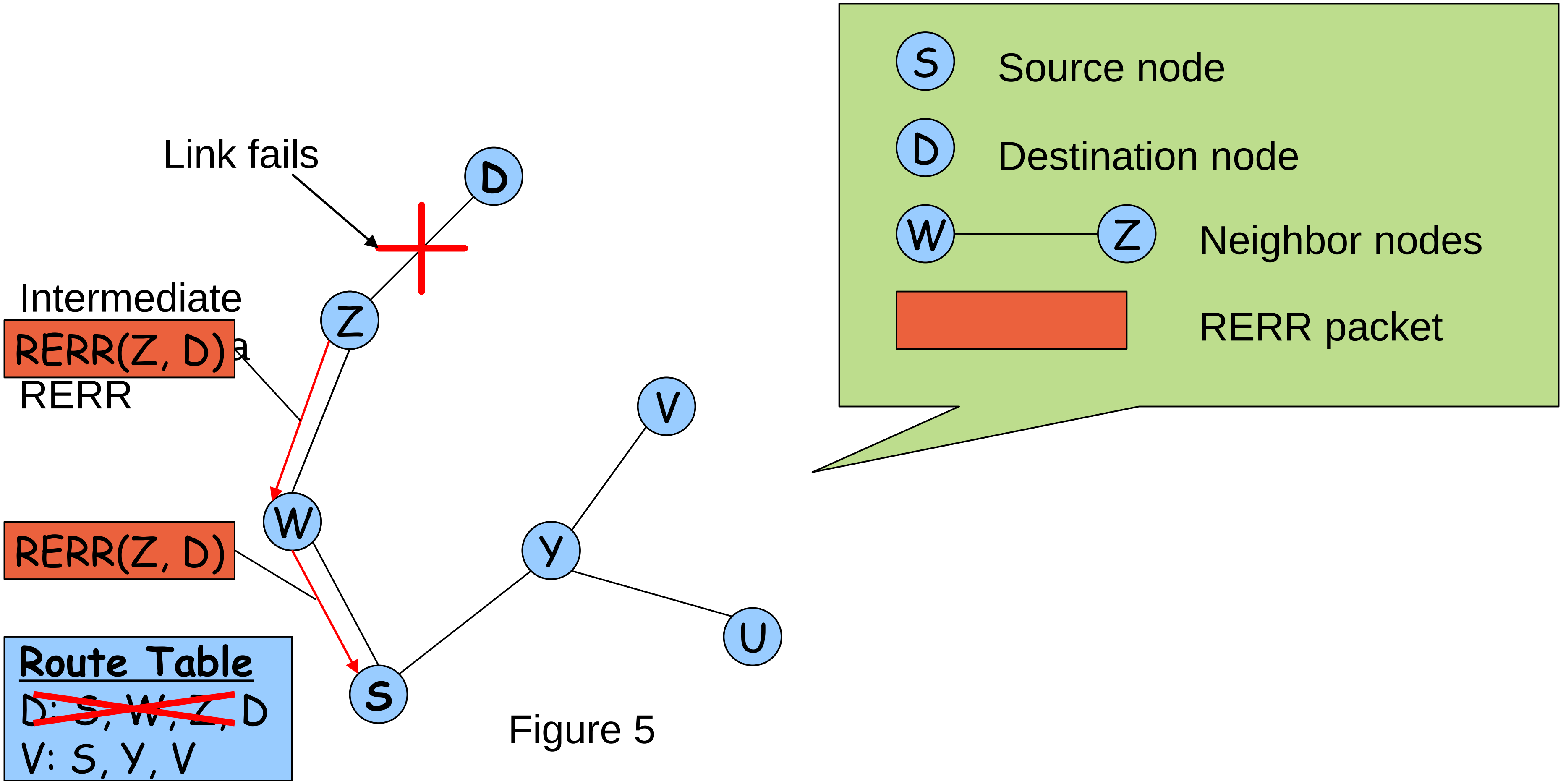
- is responsible for confirming that the packet has been received by the next hop along the source route
- The confirmation it is done with a standard part of MAC layer (e.g. Link-level ACKs in 802.11)
- If none exists, a DSR-specific software takes the responsibility to sent back an ACK
- When retransmissions of a packet in a node reach a maximum number, a Route Error Packet (RERR) is sent from the node back to the source, identifying the broken link

(DSR) Basic Route Maintenance

The source:

- Removes from the routing table the broken route
- Retransmission of the original packet is a function of upper layers (e.g. TCP)
- It searches the routing table for another route, or start a new Route Discovery process

(DSR) Basic Route Maintenance



Route Table

~~D: S, W, Z,~~ D

V: S, Y, V

S	Source node
D	Destination node
W — Z	Neighbor nodes
🟥	RERR packet

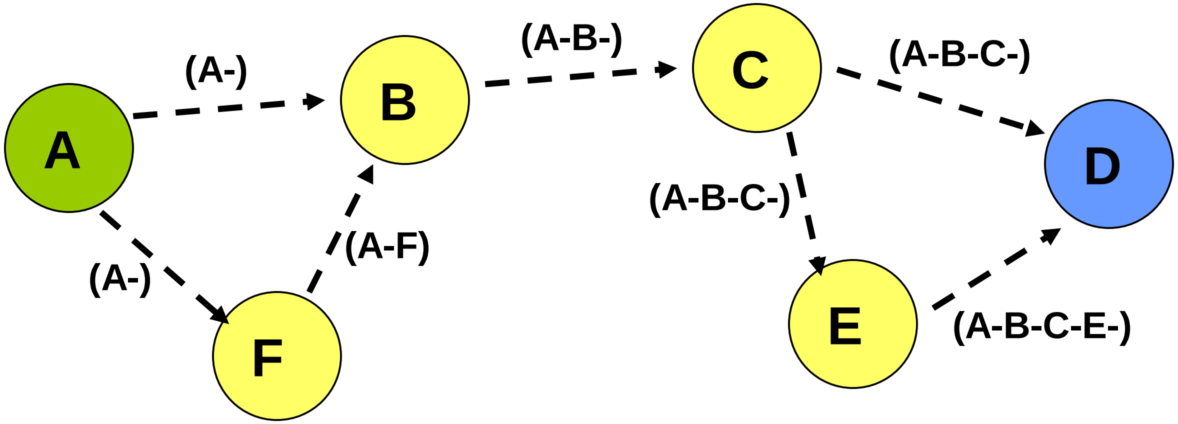
Figure 5

Outline

- ❑ Ad-Hoc on-demand Distance Vector Routing (AODV)
- ❑ Dynamic Source Routing (DSR)
  - ➢ General
  - ➢ Basic Route Discovery
  - ➢ Basic Route Maintenance
  - ➢ An example
  - ➢ Conclusion
- ❑ Comparison of AODV and DSR

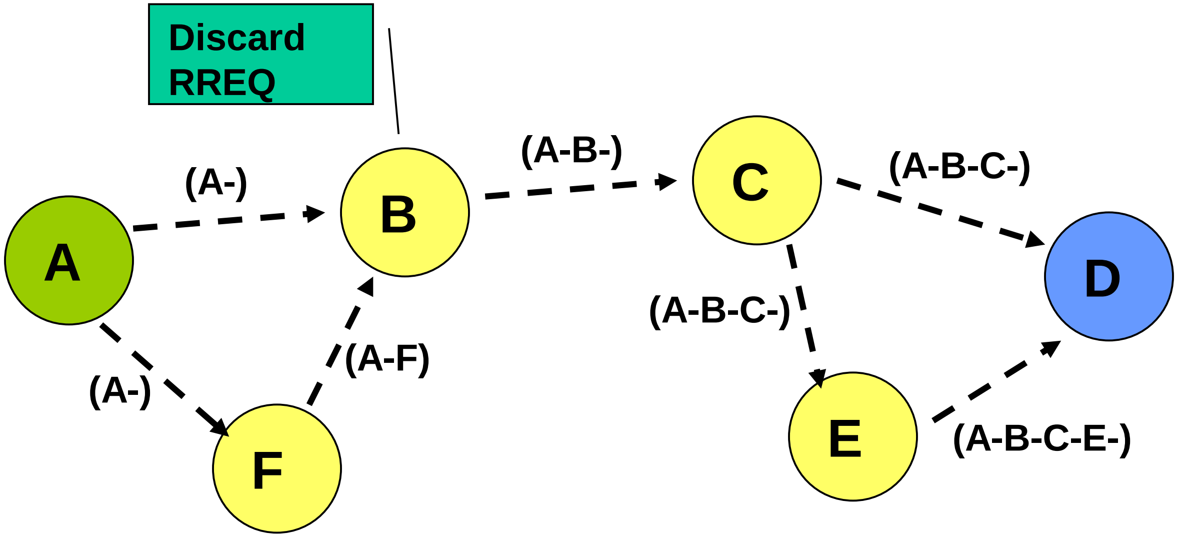
DSR Route Discovery : Route request

- The source node broadcasts the Route Request (RREQ: Route Request) message to the neighbor node, including:
  - Source node address
  - Destination node address
  - Routing record (intermediate node in the routing from source to destination node)
  - Request ID
- After the intermediate node receives the RREQ, it attaches its address to the routing record



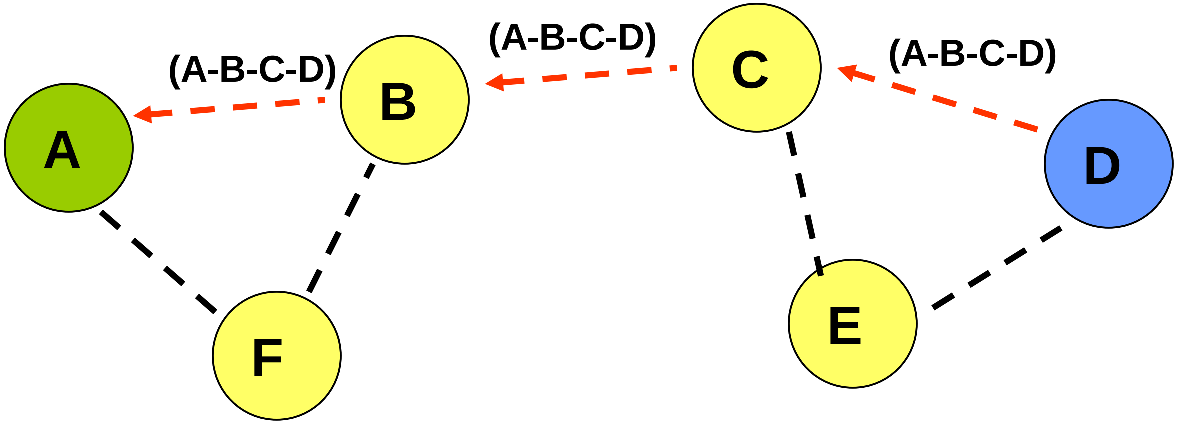
DSR Route Discovery : intermediate node deal with…

- The intermediate node maintains a list of < source node addresses, request ID> sequence pairs
- Judge repeat RREQ?
  - If < source node address and request ID> in the received RREQ message exist in the list of sequence pairs of the node
  - If a repetition is detected, the intermediate node discards the RREQ message



DSR Route Discovery： Router reply

- After the destination node receives the RREQ, it returns the RREP: Route Reply message to the source node
  - Copies the routing record in the RREQ message
- After the source node receives the RREP, route information is cached locally



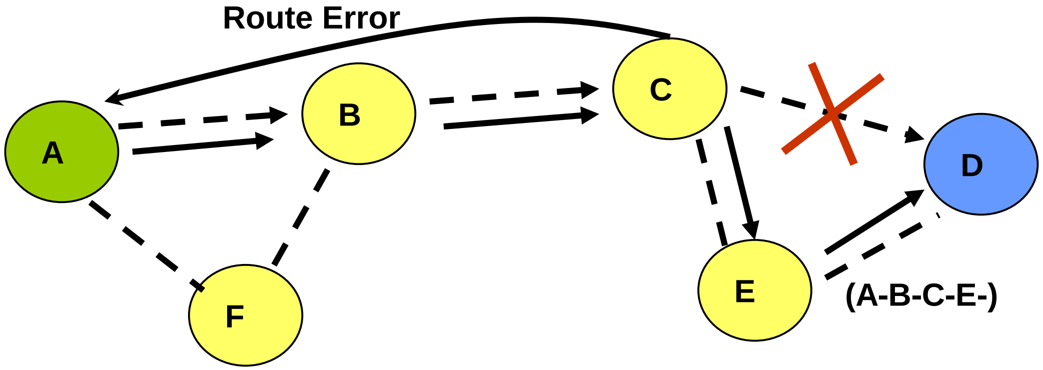
Are the back and forth paths consistent?

DSR Route Discovery ：Symmetric/asymmetric channels

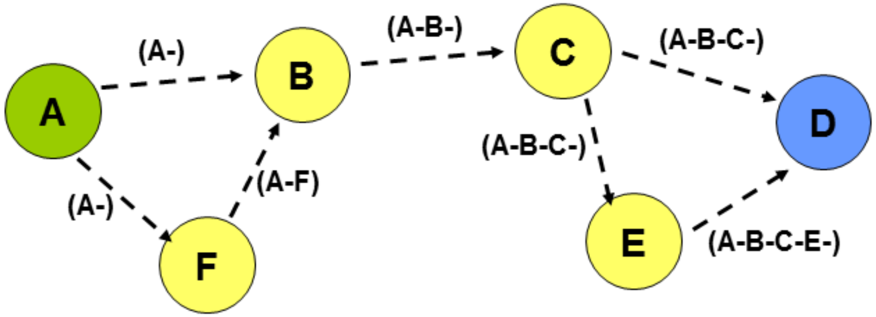
- If source-destination routing is a symmetric channel
  - The route from the destination node to the source node is the reverse route from the source node to the destination node
- If source-destination routing is asymmetric channel
  - If the destination node's routing cache has a route to the source node, it is used directly
  - Otherwise the destination node needs to initiate a routing request to the source node, with the RREP message slightly carried in the new RREQ message

Route Maintenance?

DSR Route Maintenance



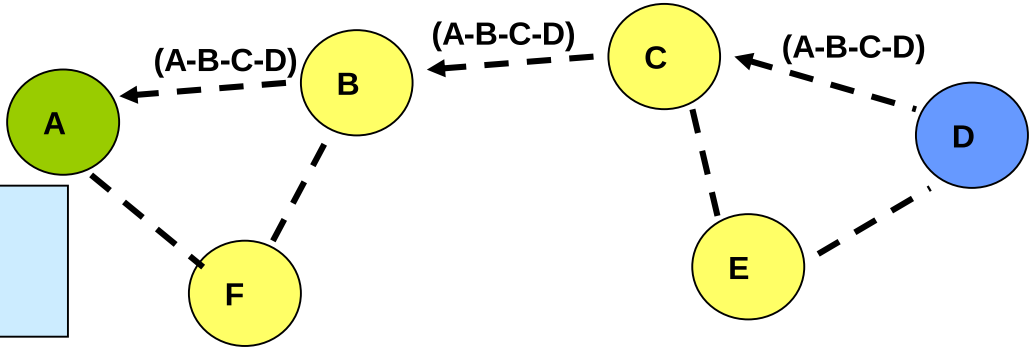
- Point-to-point verification mechanism
  - If the data packet is resent the maximum number of times and no ACK of the next hop is received, a routing error RRER message is sent to the source side indicating the BAD link
  - The source side removes the route from the route cache
  - If another route to the destination node exists in the source-side route cache, it is used to group by resend
  - Otherwise, the routing discovery process is restarted



optimize ?

DSR optimization： router cache memory

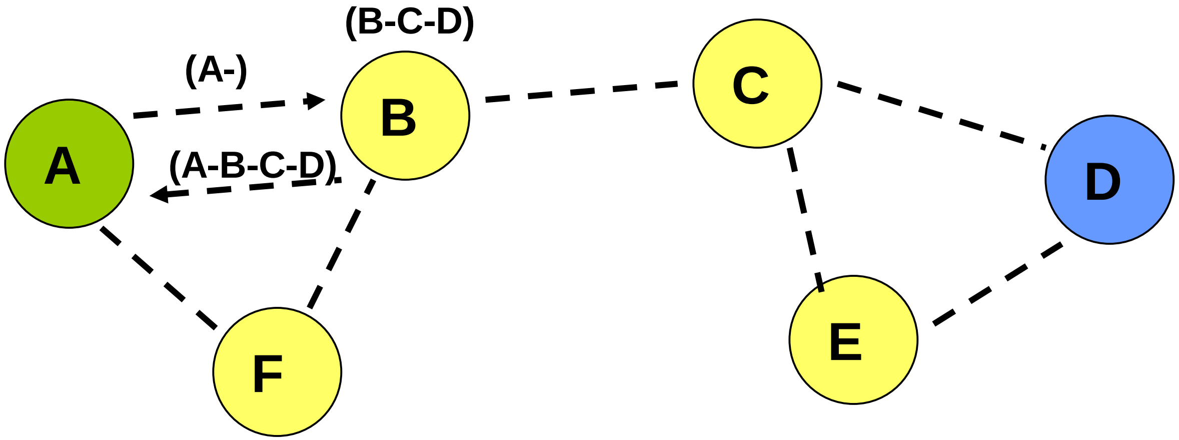
- Each node caches the new path it acquires in any way
- **Forward RREQ and data grouping**
- Obtain the routing of all nodes in the routing record from this node to RREQ or data packet, for example, E forwards RREQ(a-b-c) to obtain the routing to A (c-b-a).
- **Forward the RREP**
- Get the routing of this node to all nodes in the RREP routing record, for example, B forwarding RREP(a-b-c-d) to get the routing to D (c-d)
- **Listens for packets sent by adjacent nodes**
- RREQ, RREP, data grouping, etc



All assume that the channel is symmetric

DSR optimization： router cache memory-using?

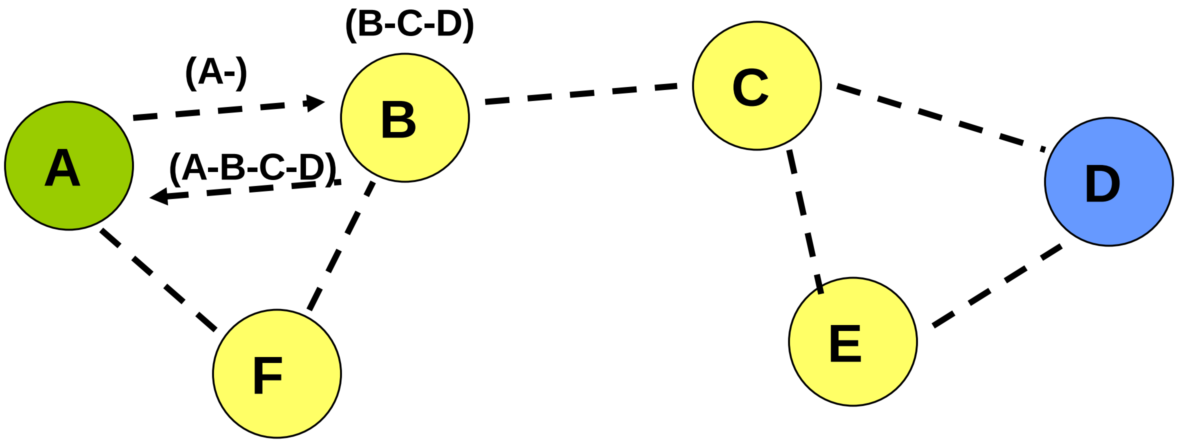
- The intermediate node uses the cached route to the destination node to respond to RREQ
  - Routing record in RREP = routing record in RREQ + cached routing to the destination node
  - For example, the cache of node B already has the route b-c-d to destination node D, so a-b-c-d is used to respond to the RREQ of A



DSR optimization: ERROR router cache memory

- Changes in network topology invalidate cached routing

Sets the expiration date of the cache route, which is deleted



RREP storm problem?
How to set?

DSR's featurres

- advantages
  - Maintaining routes only between nodes that need to communicate reduces routing maintenance overhead
  - Routing caching technology can further reduce the cost of routing discovery
  - Using route caching technology, multiple routes to destination nodes can be found
  - Support for asymmetric channels
- disadvantages
  - Using the source node routing, each data packet header should carry routing information, **increasing network overhead**
  - Because of the use of broadcast, the control message for routing discovery may spread to the entire network node
  - Error routing cache problem
  - RREP storm problem

Outline

- Ad-Hoc on-demand Distance Vector Routing (AODV)
- Dynamic Source Routing (DSR)
  - General
  - Basic Route Discovery
  - Basic Route Maintenance
  - An example
  - Conclusion
- Comparison of AODV and DSR

(DSR) Conclusion

- Excellent performance for routing in multi-hop wireless ad hoc networks

- Very low routing overhead even with continuous rapid motion, which scales to :
  1. zero when nodes are stationary
  2. the affected routes when nodes are moving

- Completely self-organized & self-configuring network

- Entirely on-demand operation. No periodic activity of any kind at any level

DSR

Outline

- Comparison of AODV and DSR

Comparison of AODV and DSR

Main common features:

- On-demand route requesting
- Route discovery based on requesting and replying control packets
- Broadcast route discovery mechanism

Comparison of AODV and DSR

Main common features: (continue)

- Route information is stored in all intermediate nodes along the established path
- Inform source node for a broken links
- Loop-free routing

Comparison of AODV and DSR

Main differences:

- ❑ DSR can handle **uni and bi-directional** links, AODV uses only **bi-directional**

- ❑ In DSR, using a single RREQ - RREP cycle, source and intermediate nodes can learn routes to other nodes on the route

- ❑ DSR maintains many alternate routes to the destination, instead of AODV that maintains at most one entry per destination

Comparison of AODV and DSR

Main differences: (continue)

- DSR doesn't contain any explicit mechanism to expire stale routes in the cache , In AODV if a routing table entry is not recently used , the entry is expired
- DSR can't prefer "fresher" routes when faced multiple choices for routes. In contrast, AODV always choose the fresher route (based **on destination sequence** numbers)

Comparison of AODV and DSR

Main differences: (continue)

- ❑ DSR's RREQ has variable length depending on the nodes that the packet has traveled. AODV's RREQ size is constant

- ❑ As a result DSR's header overhead may increase as more nodes become active, so we expect that AODV throughput in those scenarios to be better

Comparison of AODV and DSR

Test bench set up:

❑ 100 nodes, some of them as sources

❑ Nominal bit rate of 2 Mb/s

❑ Nominal node range of 250 m

❑ Continuously moving nodes

Comparison of AODV and DSR

Performance metrics	DSR	AODV
Packets delivered /Packets sent (%)	56.88	83.66
Average delay (s)	1.36	0.26

Routing Packets	DSR	AODV
Route requests	37774	228094
Route replies	82710	17753
Route errors	26591	9808
Total	147075	255655

Application and routing statistics for an example scenario for a network of 100 nodes with continuous mobility and 40 sources

Conclusion

- ❑ DSR outperforms AODV in less stressful situations (i.e., smaller number of nodes and lower load and/or mobility)

- ❑ AODV outperforms DSR in more stressful situations (e.g., more load, higher mobility)

- ❑ DSR commonly generates less routing load than AODV

- ❑ Poor delay and throughput of DSR due to lack of any mechanism **to expire stale routes** or **determine the freshness of routes**

Ad hoc Route based on Table Driven

- Table-driven routing protocol, also known as prior routing protocol or active routing protocol, is a table-based routing protocol.Its routing discovery strategy is similar to traditional routing protocols.
- In active routing protocols, each node of the network **periodically sends the latest routing information**, and each node stores one or more routing tables to store the routing information to all other nodes in the network.
- When the network topology changes, the nodes broadcast routing update messages throughout the network, and the nodes receiving the updated messages update their tables to maintain consistent, timely and accurate routing information.

DSDV's protocol

- **DV algorithm**
- Simple and easy to implement
- Small storage space required (only routing information is exchanged with neighboring nodes)
- **Make sure there is no routing loop**
- Each table entry in the routing table has a destination number
- **Quick response to topological changes**
- Start routing advertisement immediately if the routing table changes significantly
- However, wait for advertisement of unstable routes to slow down routing fluctuations
- **Prior (table driven) routing**
- The node maintains routing information to all destinations
- Routing information must be periodically updated (no dormant nodes)
- There is a communication overhead even if the network topology does not change
- Maintained routes may never be used

1. DSDV's route table

- Based on the traditional distance vector DV algorithm, to prevent the possible routing loop generated by DV algorithm. DSDV adopts the sequence number(序号) mechanism, and sets the sequence number for each route to distinguish the old route from the new one.
- Time-driven and event-driven technologies are adopted to control the transmission of routing tables to minimize the occupation of routing and other control information on wireless channels, to improve the utilization rate of wireless channels.
- DSDV routing table structure is as follows:

Dest.	Next	Metric	Seq. Nr	Install Time	Stable Data
A	A	0	A-550	001000	Ptr_A
B	B	1	B-102	001200	Ptr_B
C	B	3	C-588	001200	Ptr-C
D	B	4	D-312	001200	Ptr_D

DSDV route table

Dest.	Next	Metric	Seq. Nr	Install Time	Stable Data
A	A	0	A-550	001000	Ptr_A
B	B	1	B-102	001200	Ptr_B
C	B	3	C-588	001200	Ptr-C
D	B	4	D-312	001200	Ptr_D

- **Sequence number**, generated at the destination end, to prevent routing loops from appearing and to ensure that routing information is up to date
- 安装时间（Install Time）
  - the creation time of a table entry to delete an expired table entry
- 稳定数据(Stable Data)，is pointer
  - Points to a table containing routing stability information
    - destination ADDR.
    - 最近沉淀时间(last settling time)
    - 平均沉淀时间(average settling time)
  - Used to mitigate routing fluctuations in the network

For the same destination, nodes received the multiple routing information from other nodes, the settling time is defined as the time interval between the first route and the best route.

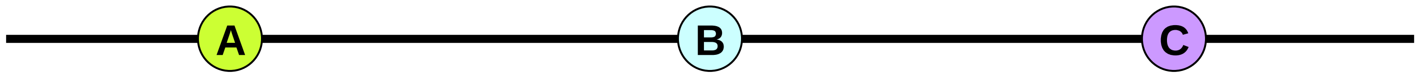
2. DSDV route Information advertisment

- Periodically advertisment each neighbor of its routing information
  - Destination node address
  - Metric: the overhead to the destination node, which is usually the number of hops to the destination node
  - destination sequence
  - Other information (e.g. hardware address, etc.)
- Rules for **setting sequence information**
  - Before each advertisment, increase destination number (using even Numbers only)
  - If a node is no longer reachable (timeout), the node's sequence number is incremented by **1** (odd ordinal number) and the metric is set to infinity

DSDV's route selection

- Choosing a route with a larger destination sequence.
  - number ensures that the latest information from the destination node is always used
  - When the destination number is equal, select a route with a better metric

DSDV protocol operation: the routing table before udpating



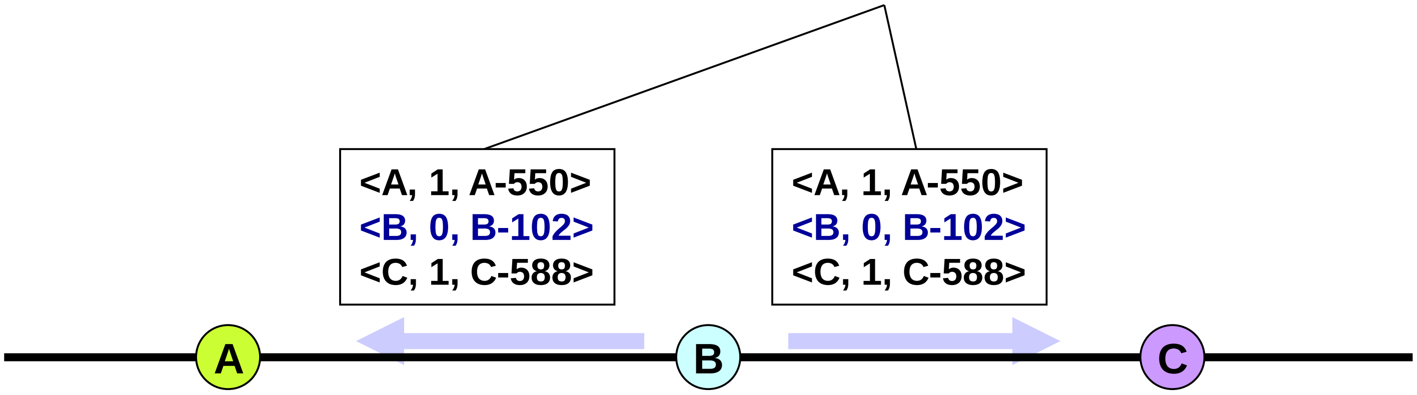
Dest.	Next	Metric	Seq
A	A	0	A-550
B	B	1	B-100
C	B	2	C-588

Dest.	Next	Metric	Seq
A	A	1	A-550
B	B	0	B-100
C	C	1	C-588

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-100
C	C	0	C-588

DSDV protocol operation : Routing announcement

- B increments the number 100 to 102, later
- B broadcasts routing information to neighbors A and C, including destination seq. Numbers



<A, 1, A-550>
<B, 0, B-102>
<C, 1, C-588>

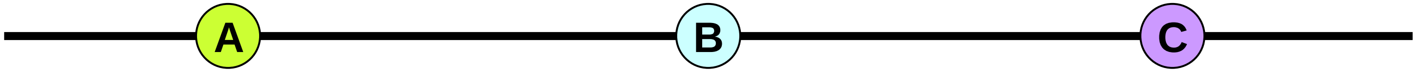
<A, 1, A-550>
<B, 0, B-102>
<C, 1, C-588>

Dest.	Next	Metric	Seq
A	A	0	A-550
B	B	1	B-100
C	B	2	C-588

Dest.	Next	Metric	Seq
A	A	1	A-550
B	B	0	B-102
C	C	1	C-588

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-100
C	C	0	C-588

DSDV protocol operation : the router table after unpdating



Dest.	Next	Metric	Seq
A	A	0	A-550
B	B	1	B-102
C	B	2	C-588

Dest.	Next	Metric	Seq
A	A	1	A-550
B	B	0	B-102
C	C	1	C-588

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-102
C	C	0	C-588

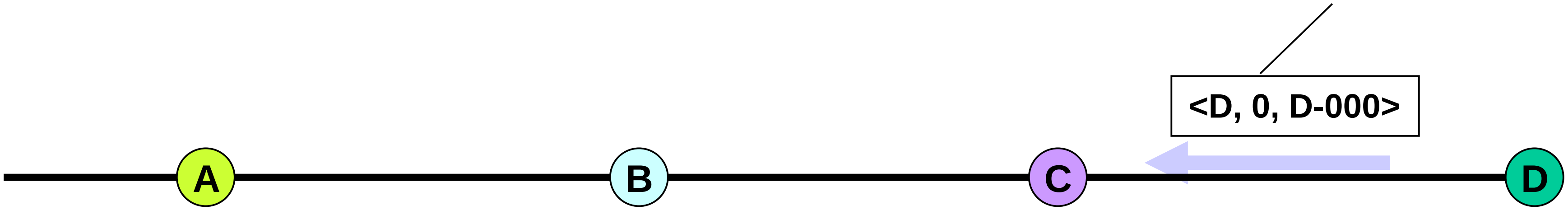
3. DSDV's response to topology changes

- Router Advertisement Immediately
  - Information about the new path or link being disconnected, and metric being changed is immediately passed to the neighbor nodes
- Two technology are available:
  - Full update: sends all routing information in your routing table
  - Incremental updates: send only those table entries that have changed in the routing table (which can be included in a separate group)

How to do?

DSDV protocol operation :
join for new node

1. D the 1st broadcast,
 send seq. num. D-000



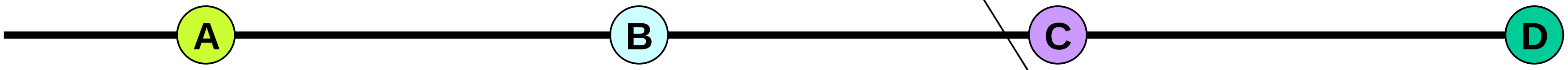
Dest.	Next	Metric	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

Dest.	Next	Metric	Seq.
A	A	1	A-550
B	B	0	B-104
C	C	1	C-590

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-104
C	C	0	C-590

DSDV protocol operation : join for new node

2. Insert D to node C seq. num. is D-000



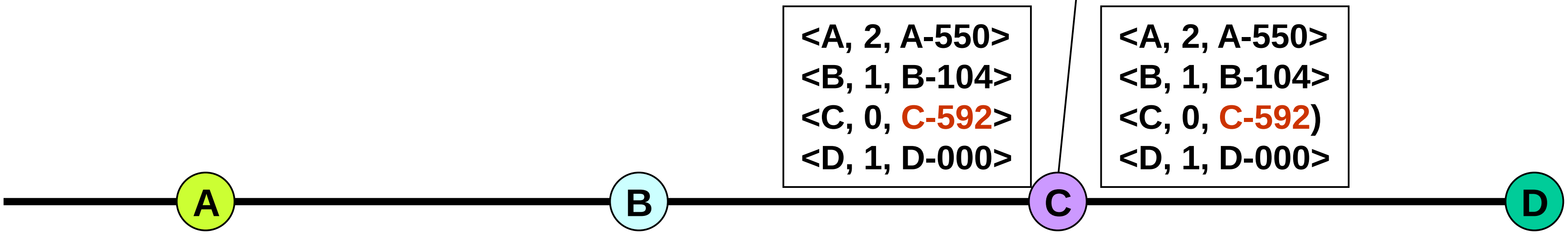
Dest.	Next	Metric	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

Dest.	Next	Metric	Seq.
A	A	1	A-550
B	B	0	B-104
C	C	1	C-590

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-104
C	C	0	C-590
D	D	1	D-000

DSDV protocol operation : join for new node

C increments its seq. num. number to c-592 and immediately broadcasts its new routing table



<A, 2, A-550>
<B, 1, B-104>
<C, 0, C-592>
<D, 1, D-000>

<A, 2, A-550>
<B, 1, B-104>
<C, 0, C-592)
<D, 1, D-000>

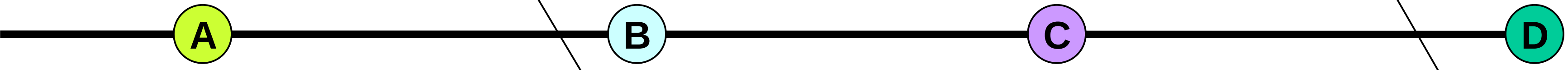
Dest.	Next	Metric	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

Dest.	Next	Metric	Seq.
A	A	1	A-550
B	B	0	B-104
C	C	1	C-590

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-104
C	C	0	C-592
D	D	1	D-000

4. B gets the new routing information and updates it's table

D gets the routing table information from C and generates its own routing table



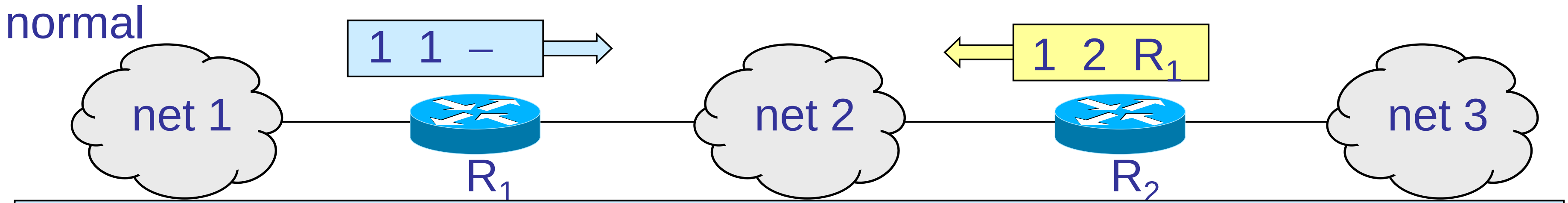
Dest.	Next	Metric	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

Dest.	Next	Metric	Seq.
A	A	1	A-550
B	B	0	B-104
C	C	1	C-592
D	C	2	D-000

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-104
C	C	0	C-592
D	D	1	D-000

Dest.	Next	Metric	Seq.
A	C	3	A-550
B	C	2	B-104
C	C	1	C-592
D	D	0	D-000

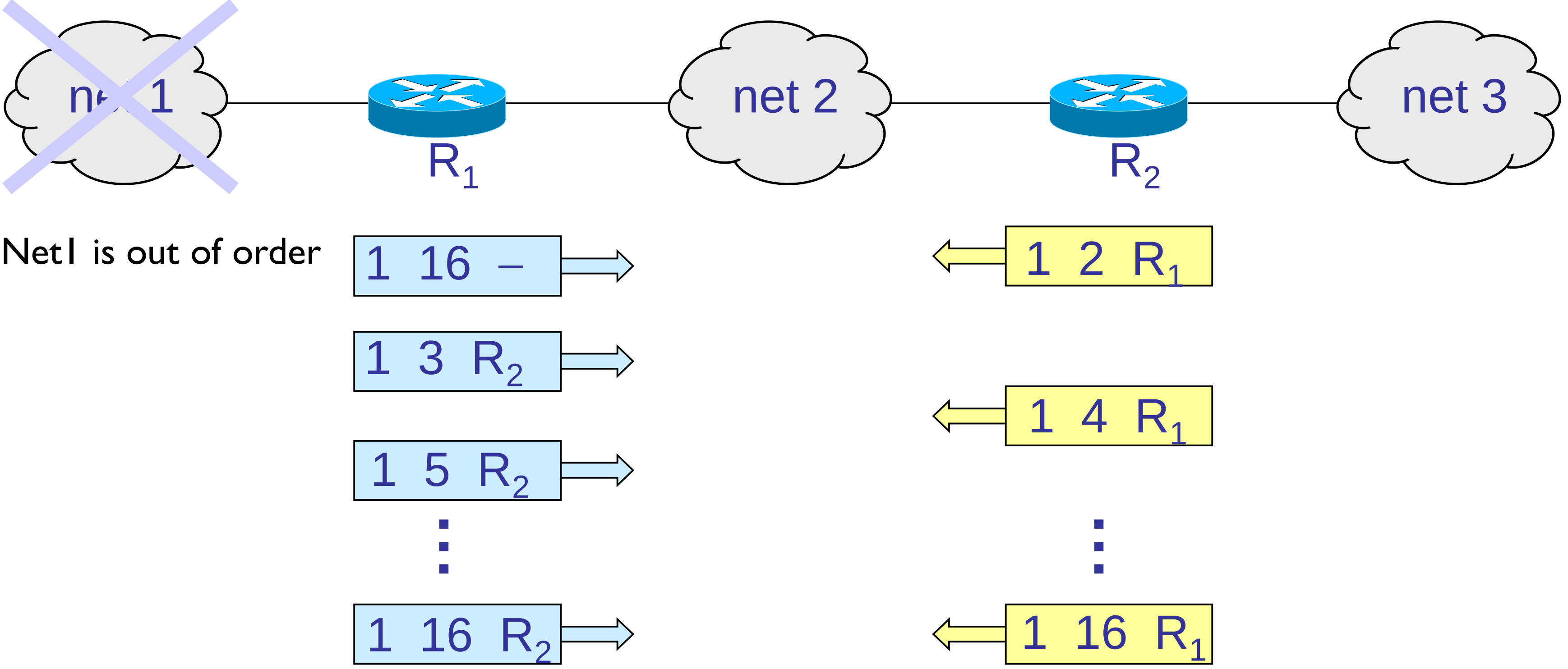
Something wrong with the link? RIP review?



1 1 –

1 2 R_1

Good news travels fast, bad news travels slow



Net1 is out of order

1 16 –

1 2 R_1

1 3 R_2

1 4 R_1

1 5 R_2

⋮

⋮

1 16 R_2

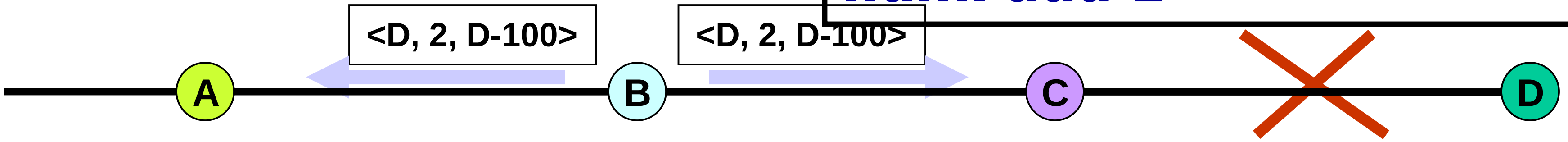
1 16 R_1

And then keep updating it, and keep updating it until the distance from R1 and R2 to net 1 is 16, and then R1 and R2 know that that net 1 is not reachable.

DSDV protocol operation ：the link is disconnected

2. B broadfast to D’s route information

1. C detect the link was disconnected →make seq. num. add 1



Dest.	Next	Metric	Seq.
…	…	…	
D	B	3	D-100

Dest.	Next	Metric	Seq.
…	…	…	
D	C	2	D-100

Dest.	Next	Metric	Seq.
…	…	…	
~~D~~	~~D~~	~~1~~	~~D-100~~
D	D	∞	D-101

Because the seq. number in the routing information of B broadcasting to D is less than the seq. number of D maintained by C, C considers that B broadcasting is the expired routing information and does not accept it

→

avoids the cycle

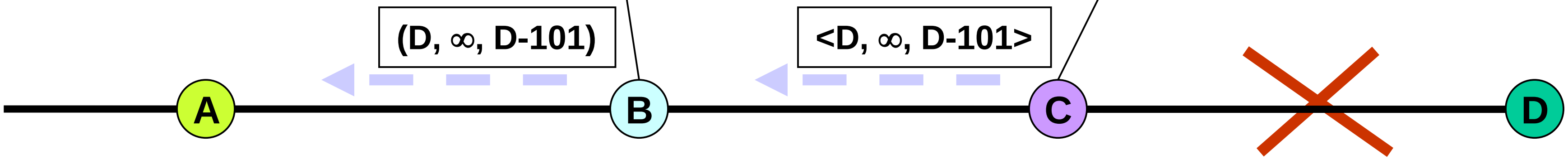
→

Avoid infinite counting

DSDV protocol operation : immediately advertising

4. B immediately sends the update message to A(the update information has A larger seq. number, so it will replace the original table item in A).

C immediately passes the update information to B (the update information has a larger seq. number, so it will replace the original table item in B)

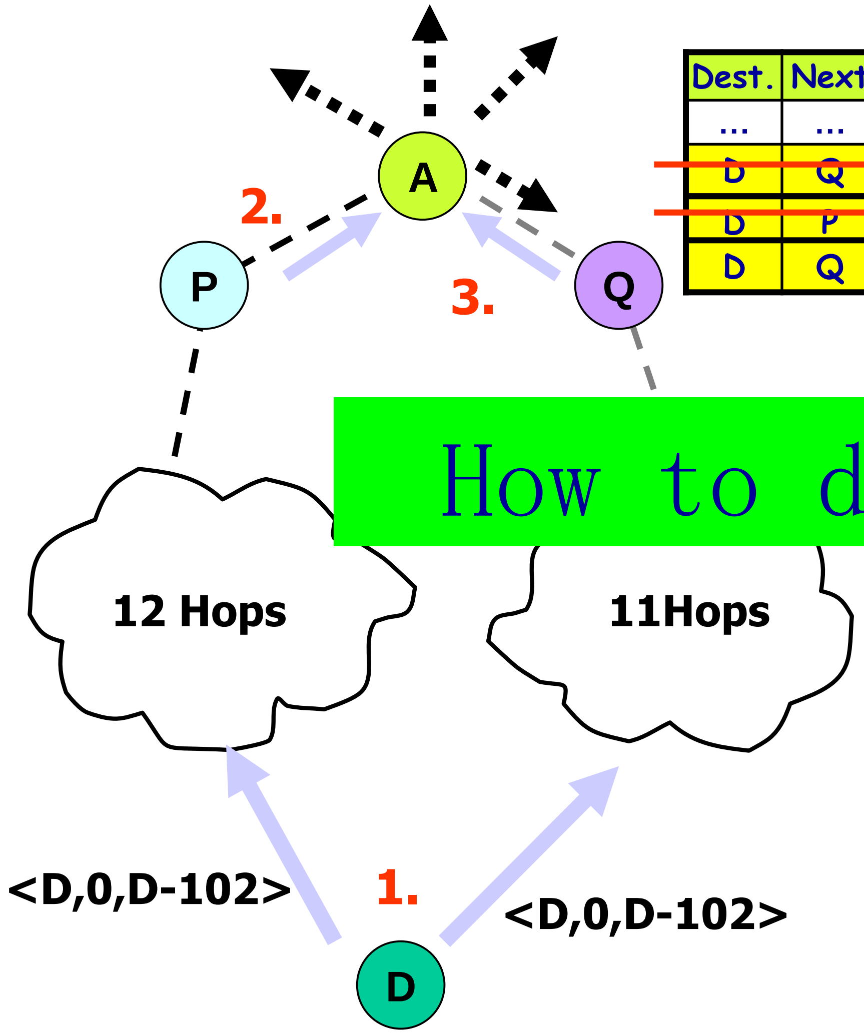


Dest.	Next	Metric	Seq.
…	…	…	
~~D~~	~~B~~	~~3~~	~~D-100~~
D	B	∞	D-101

Dest.	Next	Metric	Seq.
…	…	…	
~~D~~	~~C~~	~~2~~	~~D-100~~
D	C	∞	D-101

Dest.	Next	Metric	Seq.
…	…	…	
D	D	∞	D-101

4. DSDV protocol operation：Routing fluctuations



How to do?

Dest.	Next	Metric	Seq.
…	…	…	
~~D~~	~~Q~~	~~14~~	~~D-100~~
~~D~~	~~P~~	~~15~~	~~D-102~~
D	Q	14	D-102

1. D advertises route information, seq. D-102

2. A receives update message <D, 15, D-102> from P

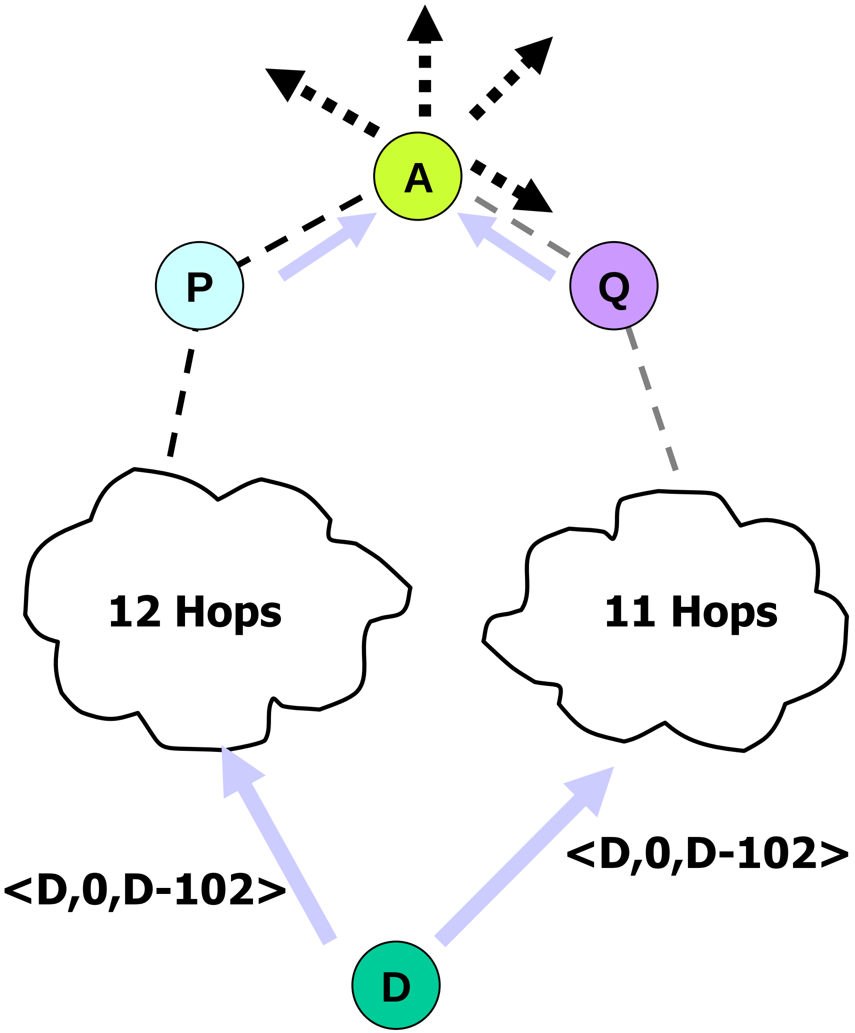
Update route inofrmatin to node D. and immediately router advertise

3. A receives update information <D, 14, D-102> from node Q

Update route inofrmatin to node D. and immediately router advertise

Since there is time difference when the routing update message of D or any node arrives at node A, unnecessary fluctuation of routing table of routing advertisement will be caused

4. DSDV protocol operation：Reduce Routing fluctuations



- The most recent and average settling time for each route is recorded in a separate table
  - Settling Time：The time interval between the first route and the best route
  - Stable data pointer to the routing table
- A updates the routing table when the first route with the new seq. number arrives, but waits some time while before broadcasting the route
  - Waiting time=2*(avg. Setting Time)

It can alleviate the routing fluctuation problem of large networks, and avoiding unnecessary advertisement and saving bandwidth

DSDV advantages and disadvantages

- advantages
  - Simple (basically the same as DV algorithm)
  - Routing loops are avoided by means of destination seq. num.
  - No routing discovery delay (prior routing)
- disadvantages
  - Routing must be advertised by all nodes, so dormancy is not supported
  - Slow convergence (characteristics of DV routing)
  - Overhead: most routing information is never used
  - Scalability is a major problem (all proactive routing exists)

DSDV SUMMARY

- The basic principle of DSDV protocol is that each node maintains a routing table to other nodes, and the contents of the table are routing "next hop" nodes.The innovation of DSDV is to set a seq. number for each route. The route with a large seq. number is the **preferred** route, while the route with the same seq. number and **fewer hops is the preferred route**. Under normal circumstances, the seq. number of the nodes is monotone increasing even.

Mobile IP

Mobility

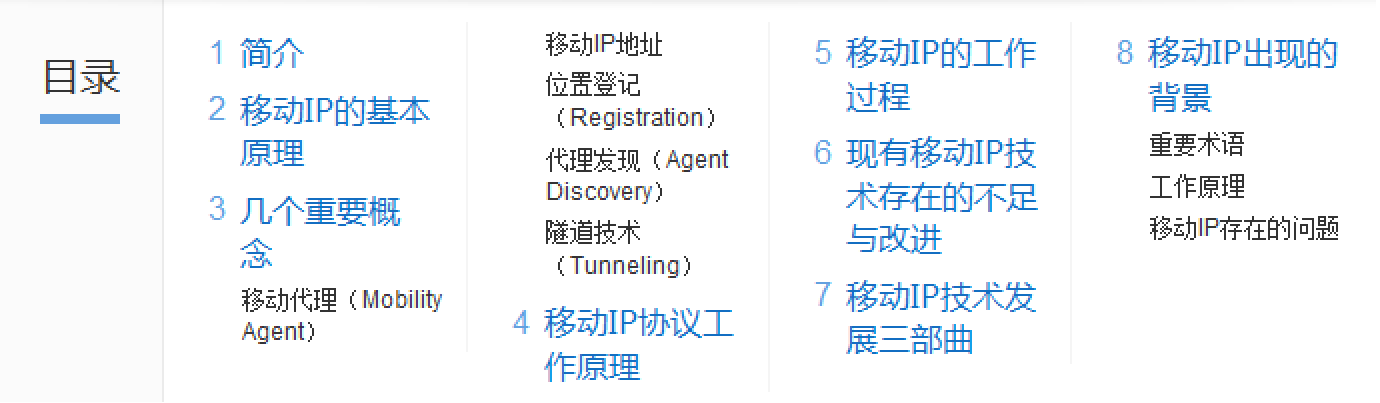
6.5 Principles: addressing and routing to mobile users

6.6 Mobile IP

6.7 Handling mobility in cellular networks

6.8 Mobility and higher-layer protocols

6.9 Summary



目录

1 简介
2 移动IP的基本原理
3 几个重要概念
移动代理（Mobility Agent）
移动IP地址
位置登记（Registration）
代理发现（Agent Discovery）
隧道技术（Tunneling）
4 移动IP协议工作原理
5 移动IP的工作过程
6 现有移动IP技术存在的不足与改进
7 移动IP技术发展三部曲
8 移动IP出现的背景
重要术语
工作原理
移动IP存在的问题

Mobility IP

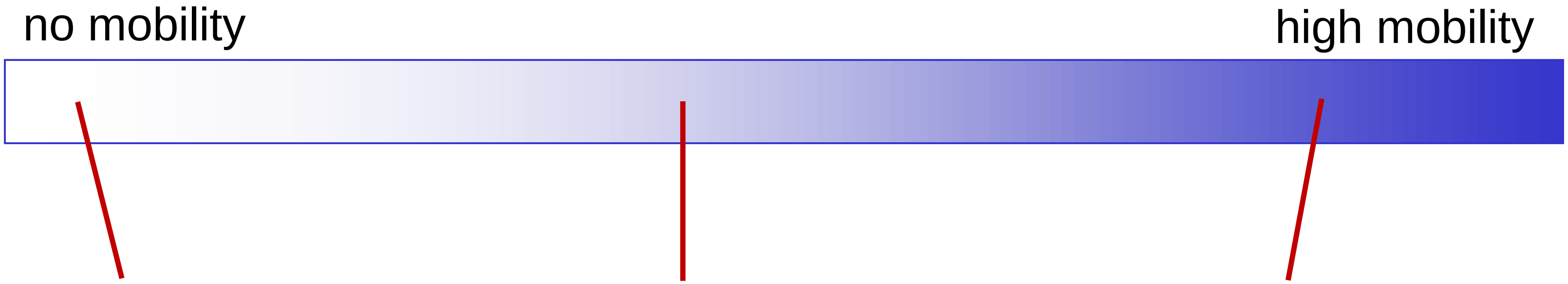
- Mobile IP is the deep integration of mobile communication and IP, and also a profound change of the existing mobile communication mode. It will truly realize the integration of voice and data. Its goal is to integrate wireless voice and data into a technical platform for transmission, which is IP protocol.
- How to enable people to access the Internet at **any time and anywhere**, which is a hot topic of current Internet technology research and the goal of the next generation of real personal communication technology. Mobile IP technology in wireless access makes **multimedia global network** connection that people have been dreaming of possible, which adapts to the needs of the universal computing era.
- The current mobile communication adopts **circuit switching mode**, which always takes up **fixed bandwidth** resources when users talk. This mode of communication is suitable for voice services, but not for IP type services. In order to adapt to the rapid growth of data service demand, the existing circuit switched mobile communication network must be reformed, people need a packet switched based wireless network, this new network structure is the future structure of mobile IP.

Mobility IP

- Mobile IP is not a simple superposition of mobile communication technology and Internet technology, nor a simple superposition of wireless voice and wireless data. It will truly realize the business integration of voice and data. The goal of mobile IP is to integrate wireless voice and data into a technical platform for transmission, which is IP protocol. The future mobile network will achieve full packet switching, including voice and data are carried by IP packet, the gap between voice and data will disappear. The IP process of mobile communication is as follows:
- IP transformation of mobile services; Grouping evolution of mobile network; The realization of full IP in mobile communication system.

What is mobility?

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

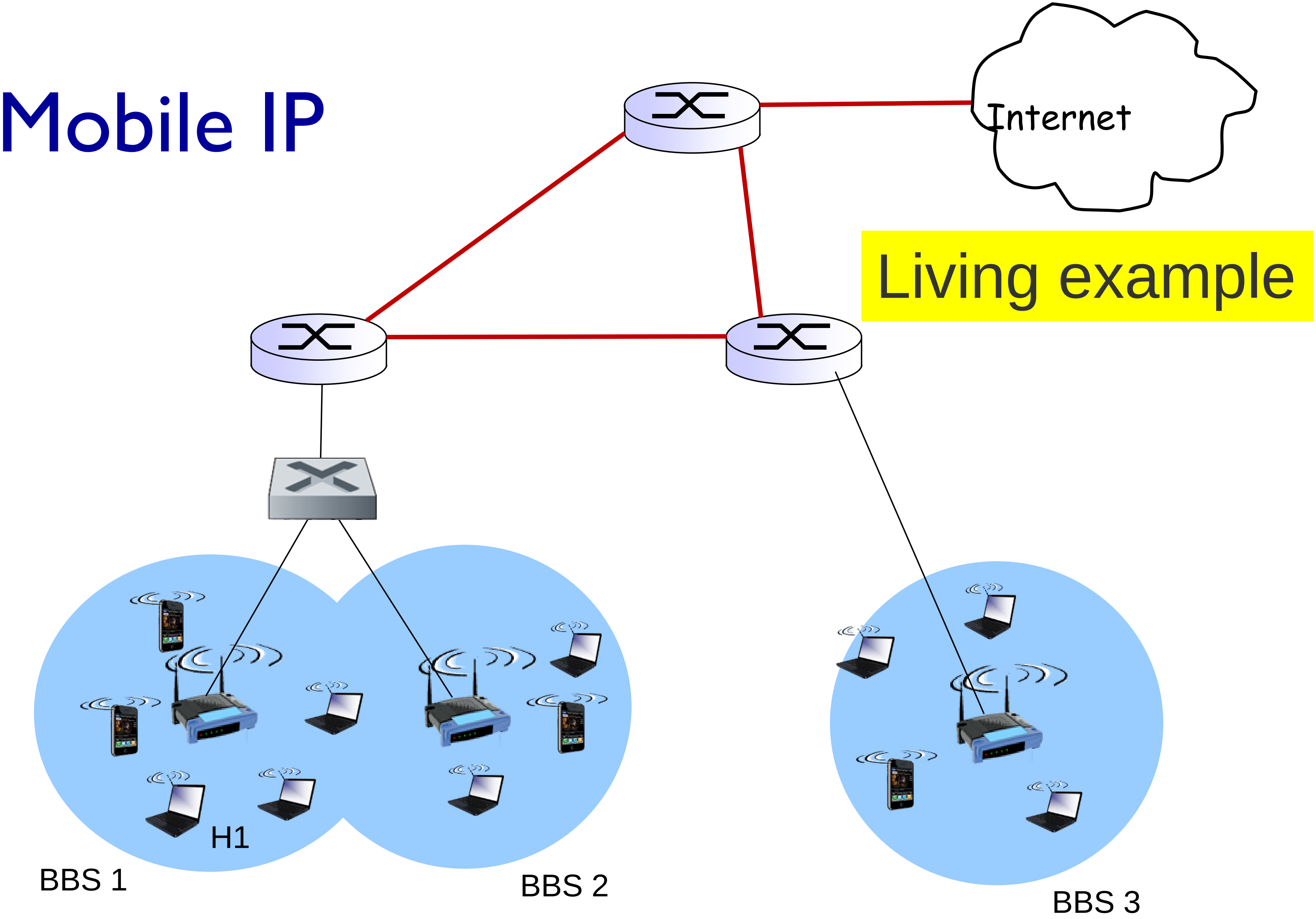


mobile wireless user, using same access point

mobile user, connecting/ disconnecting from network using DHCP.

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

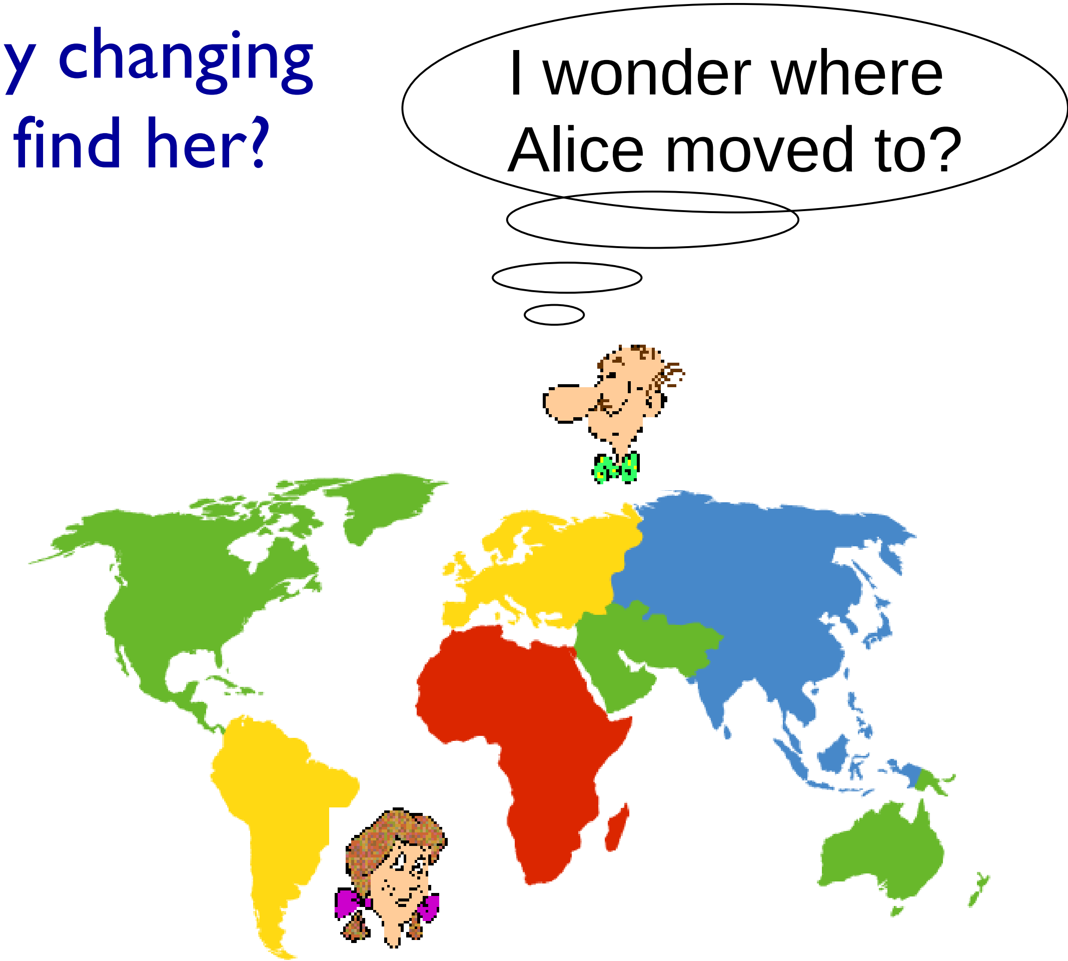
Mobile IP



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

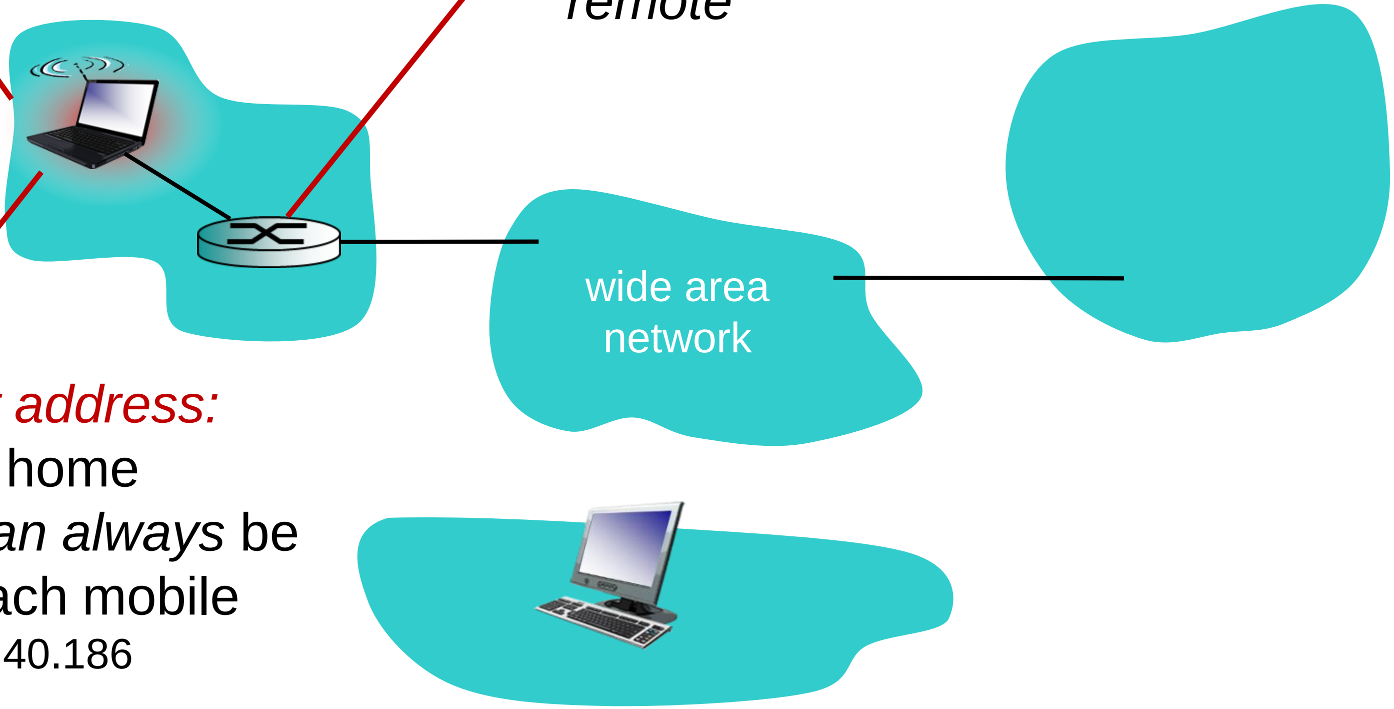
Can previous technologies solve these problems?

- *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
- *change mobile node IP*

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, when mobile is remote



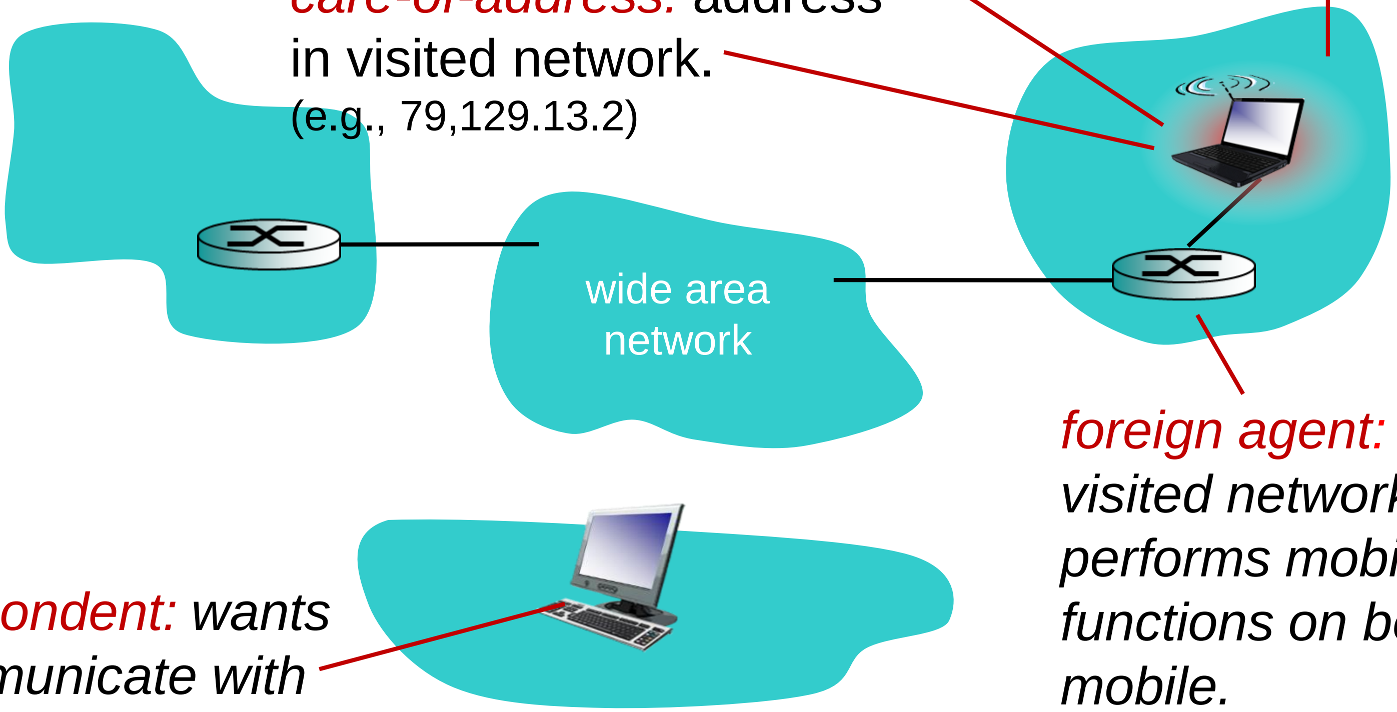
permanent address: address in home network, *can always* be used to reach mobile
e.g., 128.119.40.186

Mobility: more vocabulary

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

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

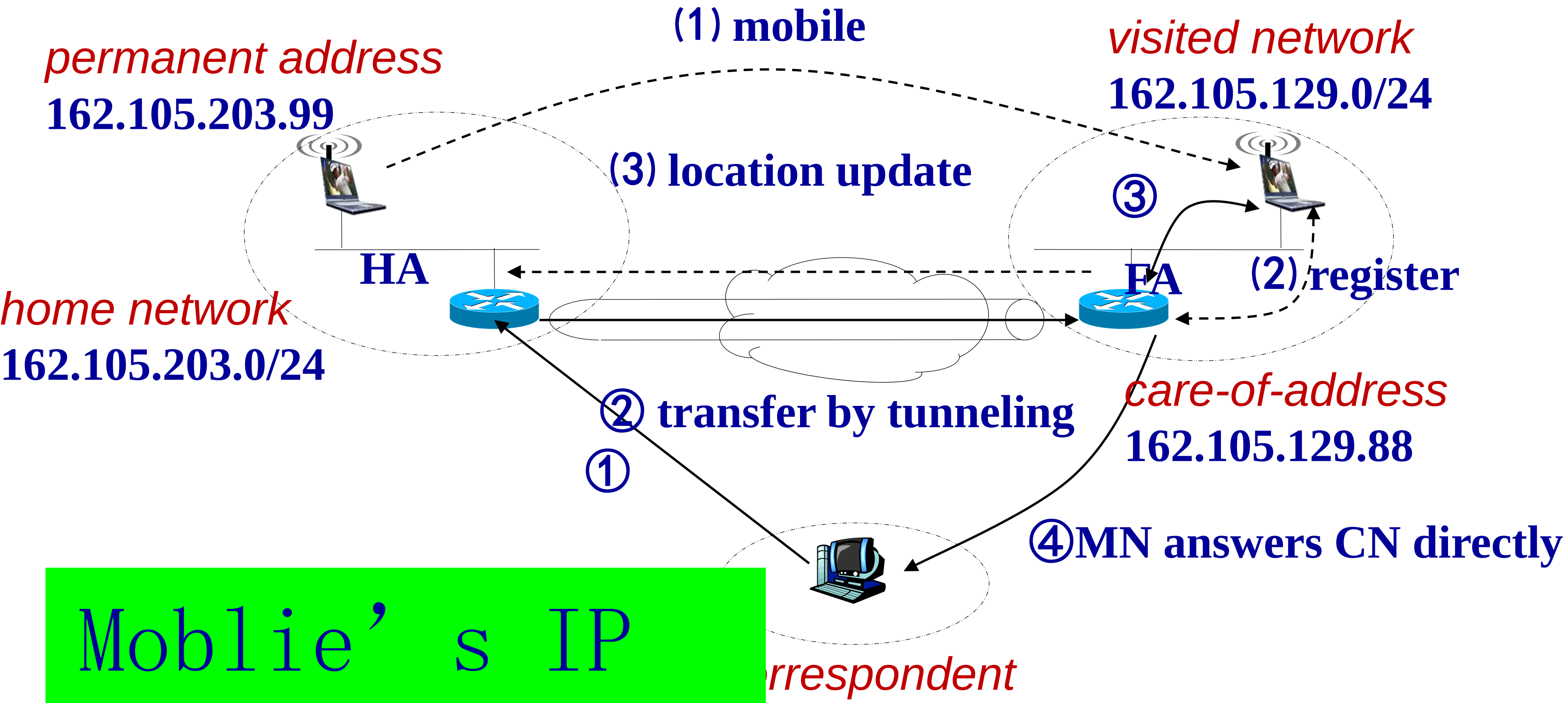
care-of-address: address in visited network. (e.g., 79,129.13.2)



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

correspondent: wants to communicate with mobile

Moblie IP’s conceptual model



Moblie’s IP function?

Mobile IP has three main functions

Agent discovery. Through proxy discovery, the mobile node can determine its current location and get a forwarding address.

Registration. Through registration, the mobile node requests services from the field agent and notifies the home agent of its forwarding address;

Routing technology. The mechanism by which a mobile node routes its outgoing or outgoing packets when it is connected to a foreign link.

To achieve these functions, some control messages for mobile IP are defined.

The proxy discovery and registration messages are defined in RFC2002/3220/3344.

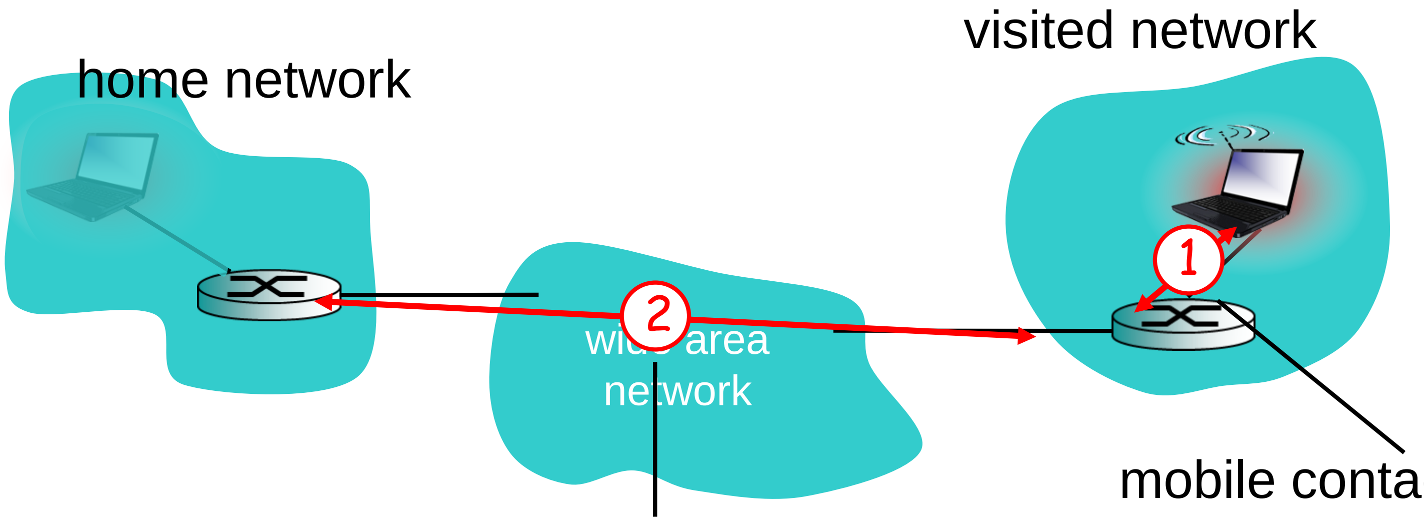
Mobility: approaches

- *let routing handle it:* ro dvertise permanent address of mobile-nodes-in-r sual routing table exchange.
  - routing tables each mobile located
  - no changes to e

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



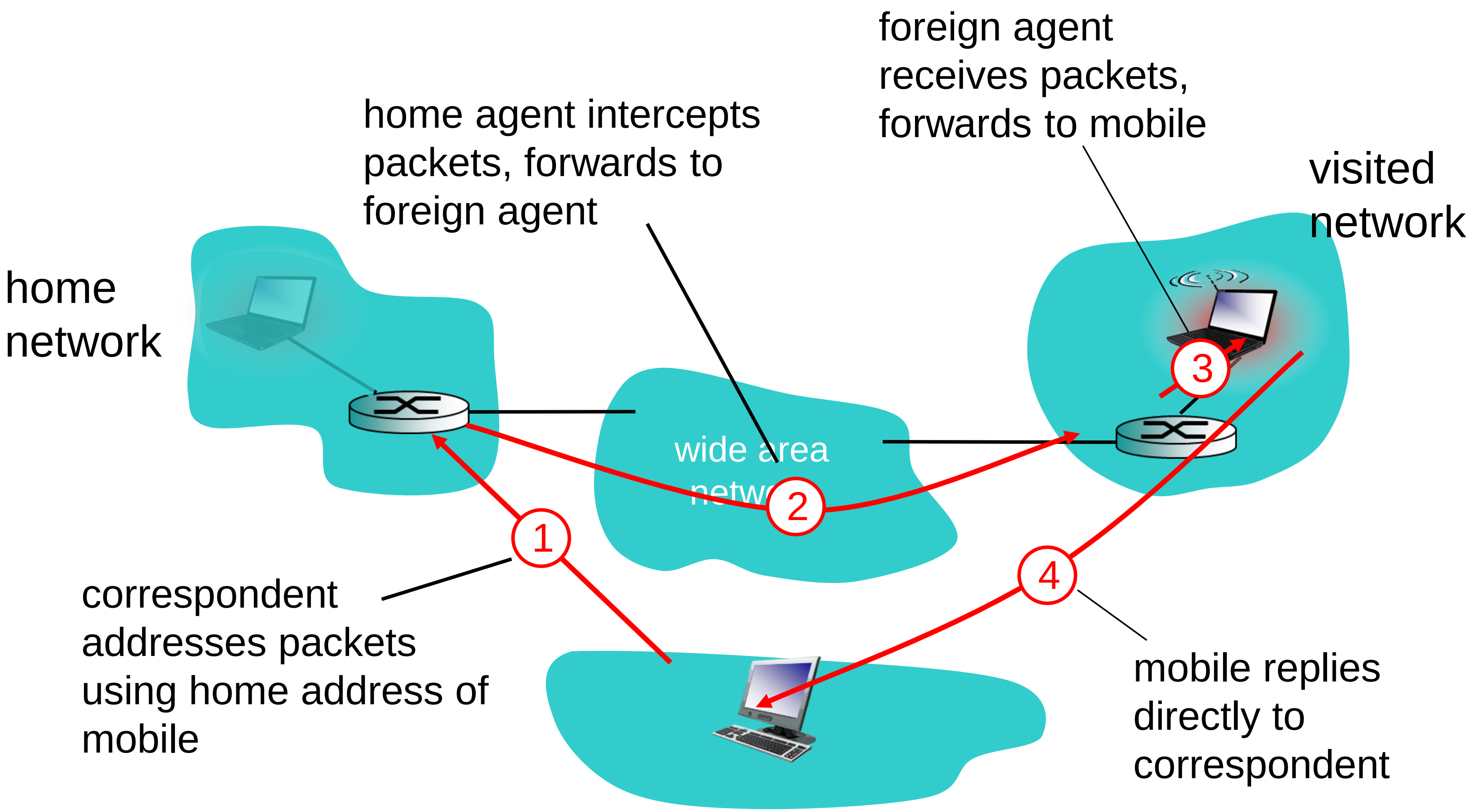
foreign agent contacts home agent home: “this mobile is resident in my network”

mobile contacts foreign agent on entering visited network

end result:

- foreign agent knows about mobile
- home agent knows location of mobile

Mobility via indirect routing



home agent intercepts packets, forwards to foreign agent

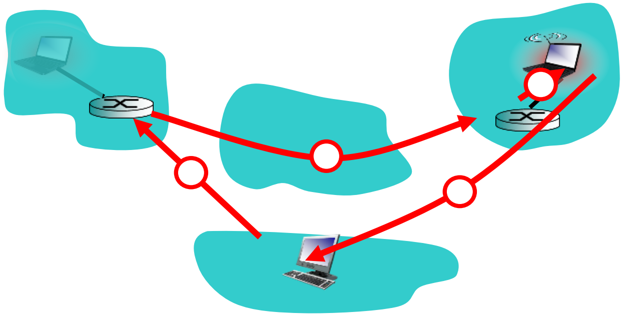
foreign agent receives packets, forwards to mobile

correspondent addresses packets using home address of mobile

mobile replies directly to correspondent

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
- foreign agent functions may be done by mobile itself
- triangle routing: correspondent-home-network-mobile
  - inefficient when correspondent, mobile are in same network

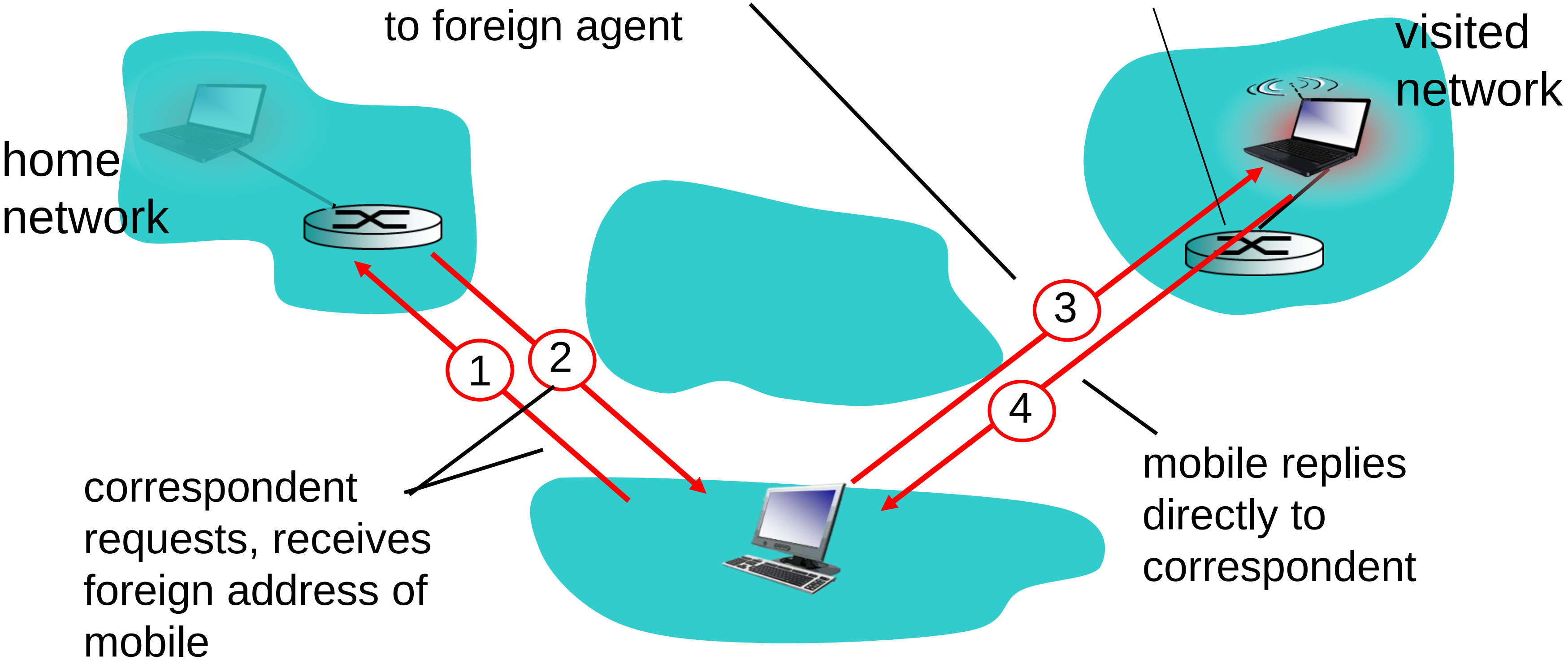


Any question?

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)
- mobility, changing foreign networks transparent: *on going connections can be maintained!*

Mobility via direct routing



correspondent forwards to foreign agent

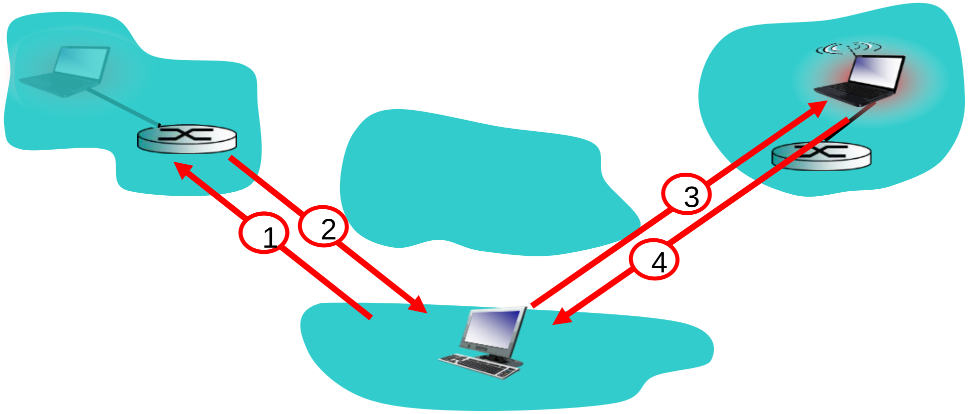
foreign agent receives packets, forwards to mobile

correspondent requests, receives foreign address of mobile

mobile replies directly to correspondent

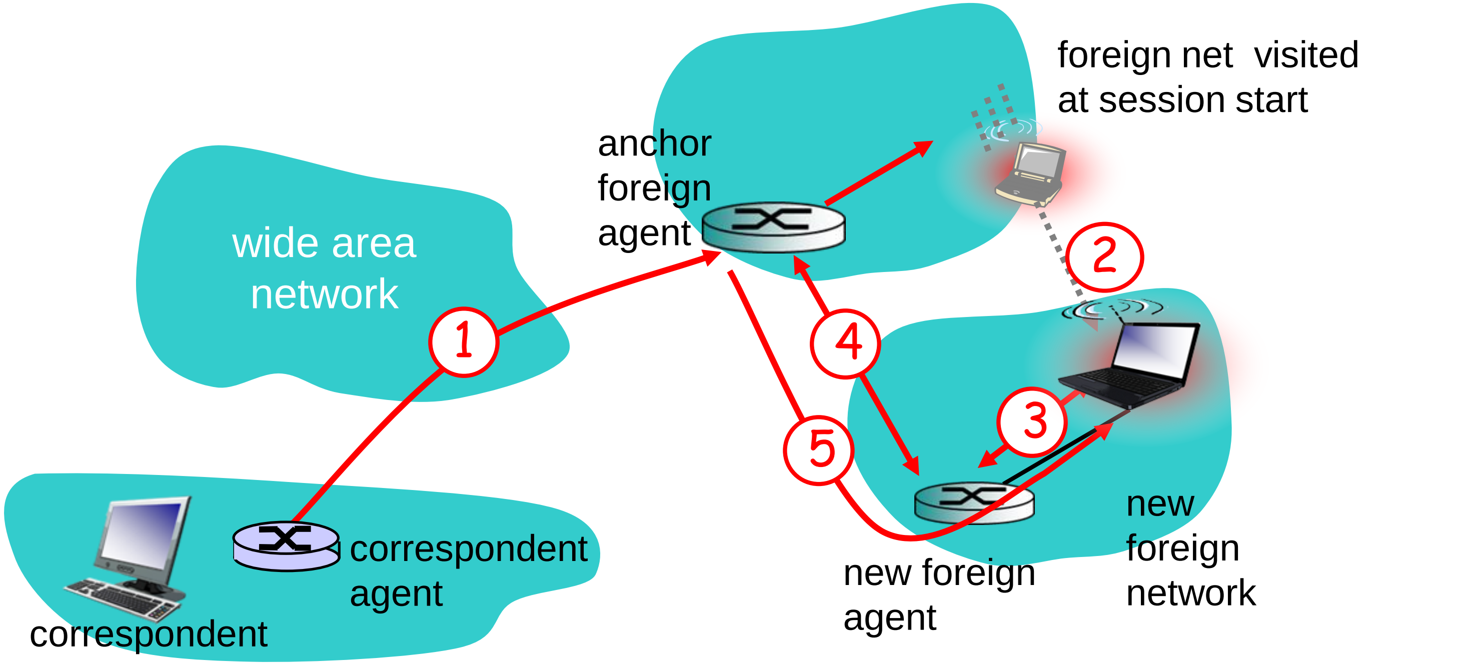
Mobility via direct routing: comments

- 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)



Chapter 6 outline

Mobility

6.5 Principles: addressing and routing to mobile users

6.6 Mobile IP

6.7 Handling mobility in cellular networks

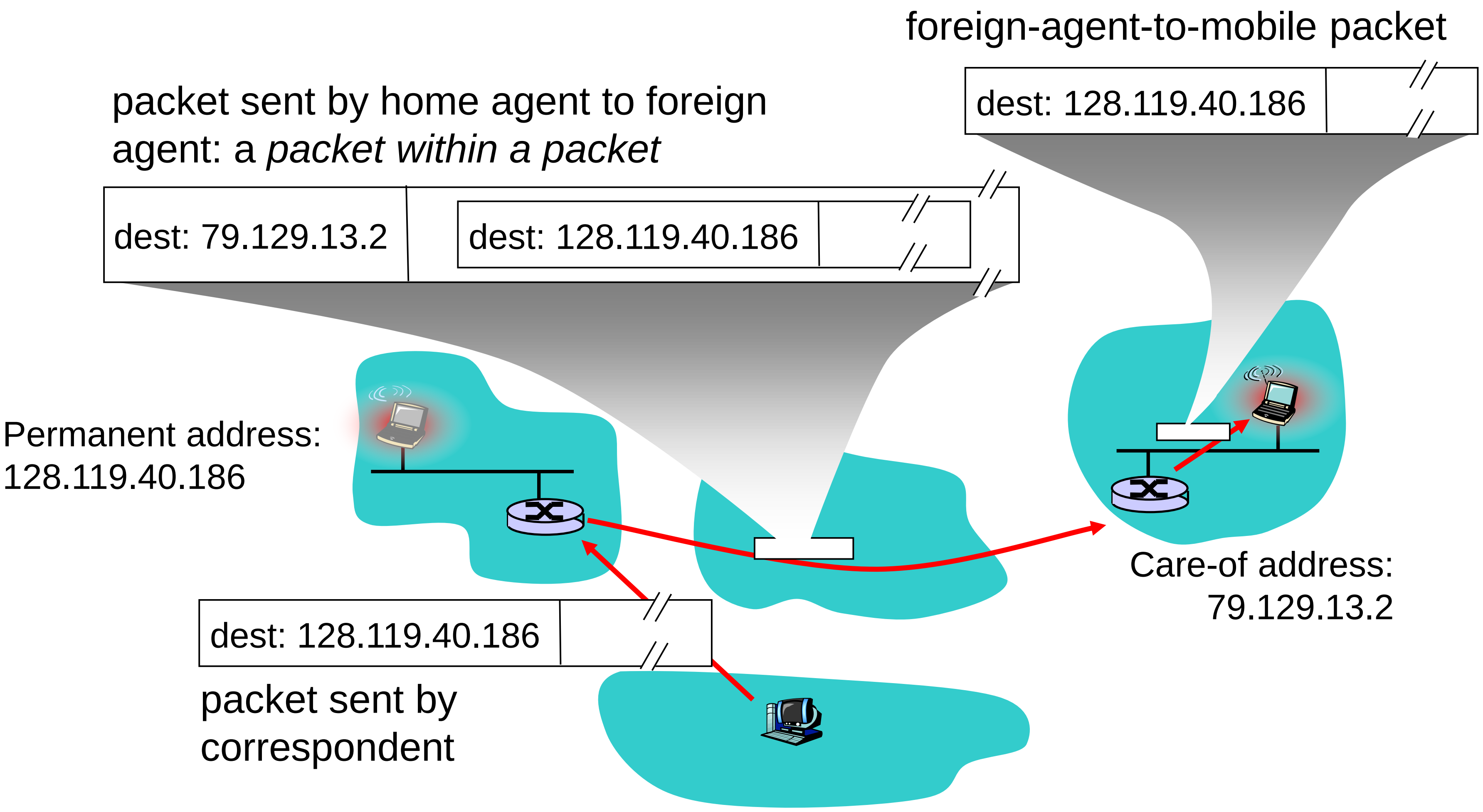
6.8 Mobility and higher-layer protocols

6.9 Summary

Mobile IP

- RFC 3344
- has many features we' ve seen:
  - home agents, foreign agents, foreign-agent registration, care-of-addresses, encapsulation (packet-within-a-packet)
- **three components to standard???**
  - indirect routing of datagrams
  - agent discovery
  - registration with home agent

Mobile IP: indirect routing



foreign-agent-to-mobile packet

packet sent by home agent to foreign agent: a *packet within a packet*

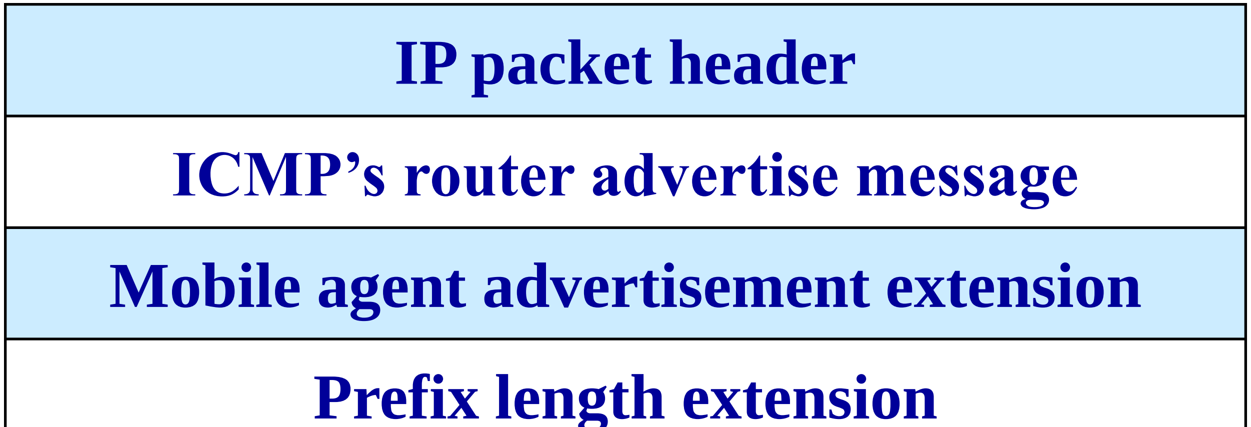
Permanent address: 128.119.40.186

Care-of address: 79.129.13.2

packet sent by correspondent

Agent discovery

- Mobile agents broadcast or multicast agent advertisement messages over the network.
    - A mobile node can determine whether a proxy exists on the network
    - Determine the identity (IP address) and function of the agent.
- **Agent advertisement message** and **agent request message** are realized based on the router advertisement message and router request message defined in ICMP router discovery message [RFC1256].
- Schematic diagram of the agent advertisement message



IP packet header

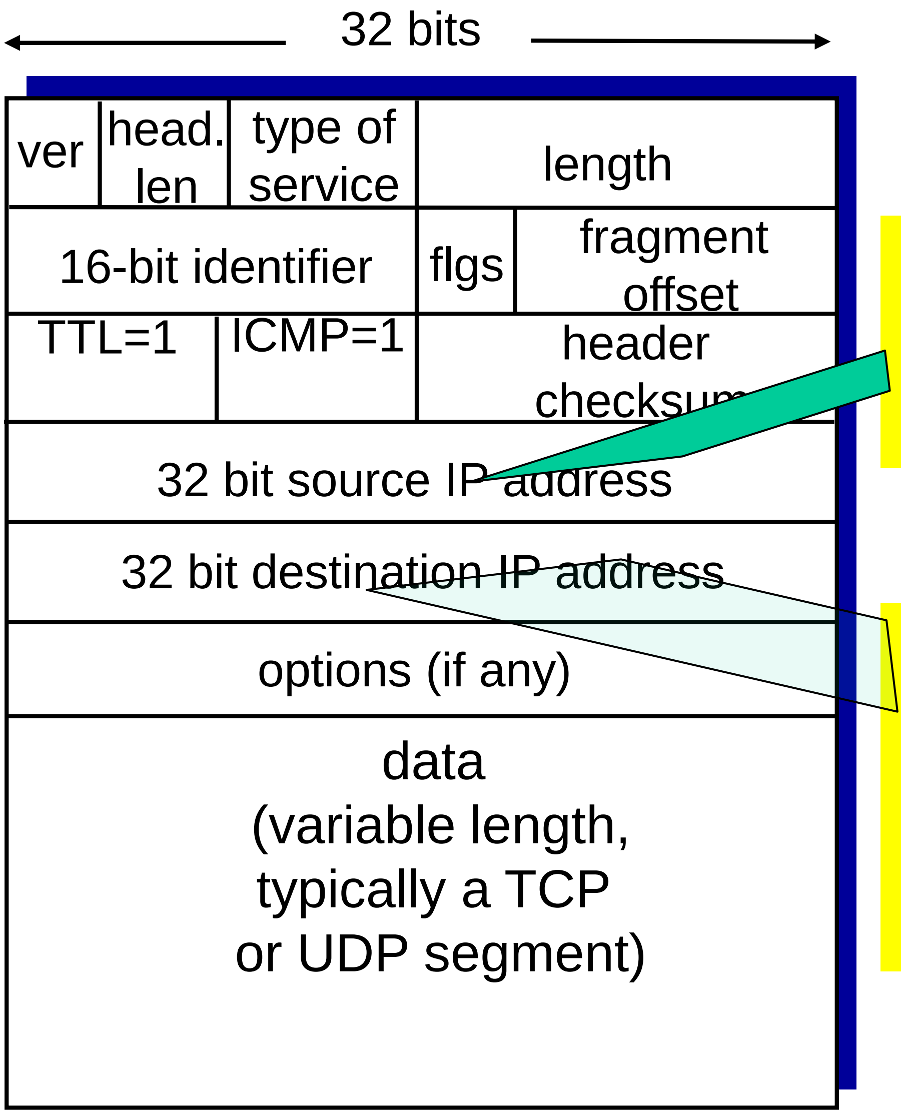
ICMP's router advertise message

Mobile agent advertisement extension

Prefix length extension

Encapsulates the IP packet header field of the agent **advertisement message**

- 224.0.0.1Multi cast address that represents all hosts and routers on the local network
- 255.255.255.255 local broadcast addr.。

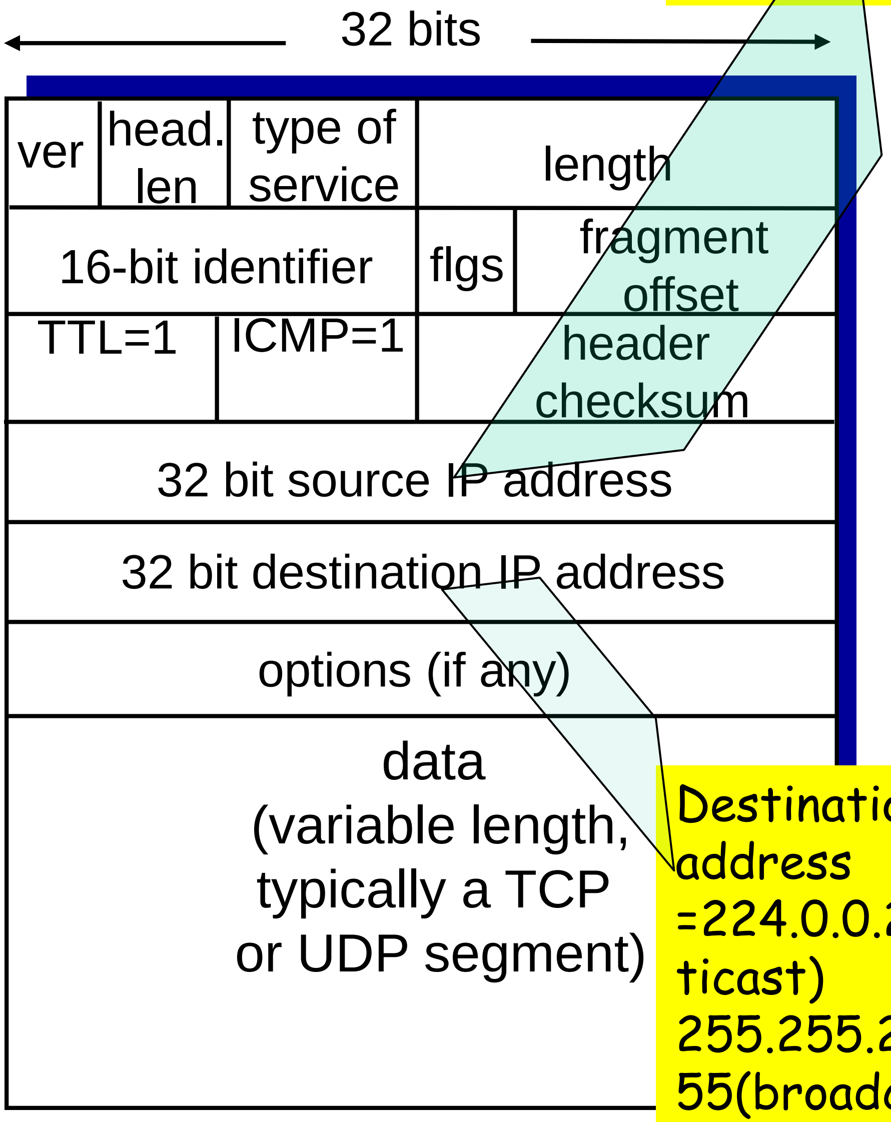


Source IP address = home or foreign agent address

Destination IP address =224.0.0.1(multicast) or 255.255.255.255(broadcast)

2. agent request message

- The mobile node uses the agent request message to send the agent advertisement message to the mobile agent.
- The proxy request message is basically equivalent to an ICMP router request message.

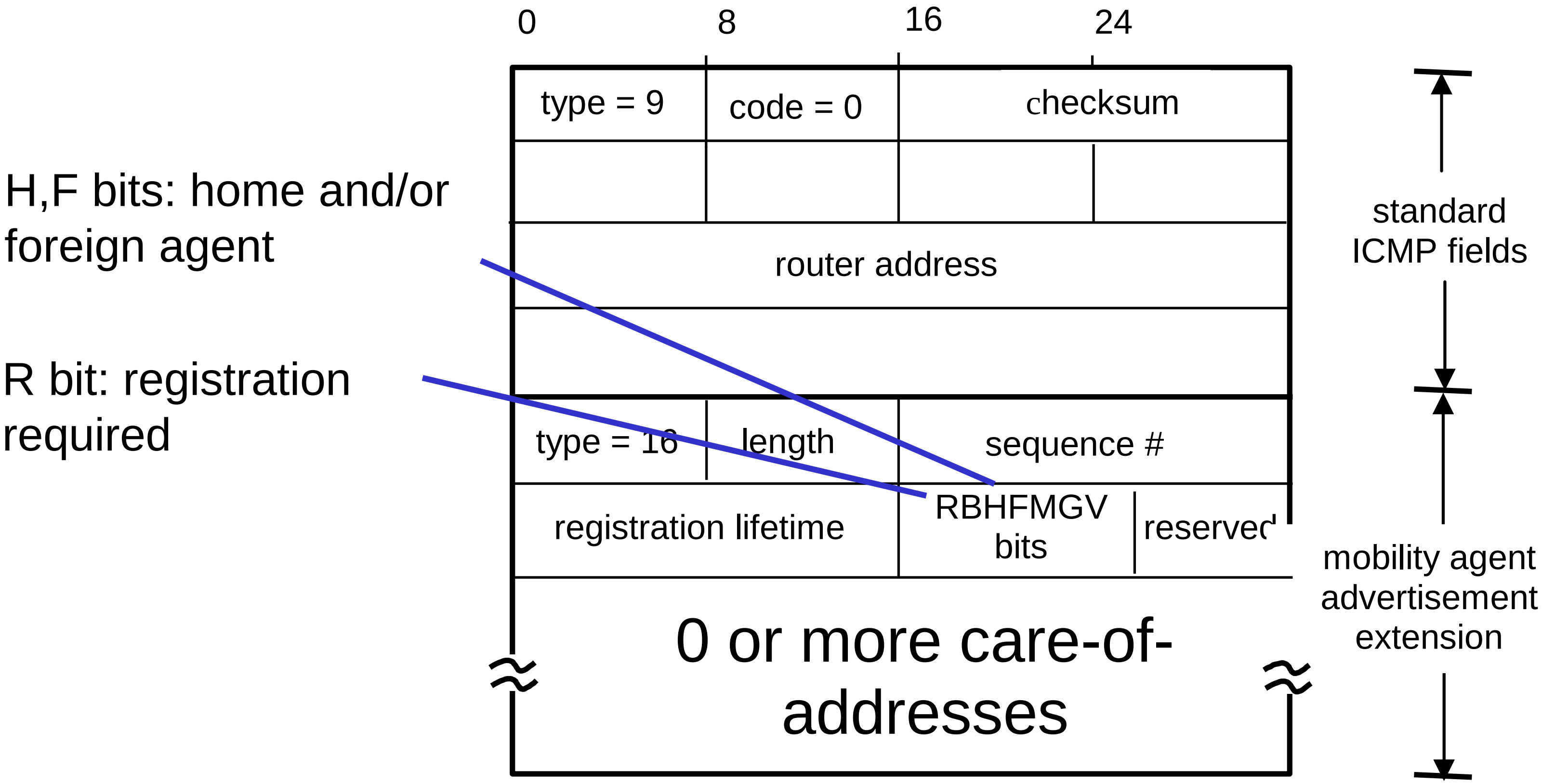


Source IP address = the home address of the mobile node

Destination IP address =224.0.0.2(multicast) or 255.255.255.255(broadcast)

Mobile IP: agent discovery

- *agent advertisement:* foreign/home agents advertise service by broadcasting ICMP messages (typefield = 9)



H,F bits: home and/or foreign agent

R bit: registration required

0 8 16 24

type = 9 | code = 0 | checksum

router address

standard ICMP fields

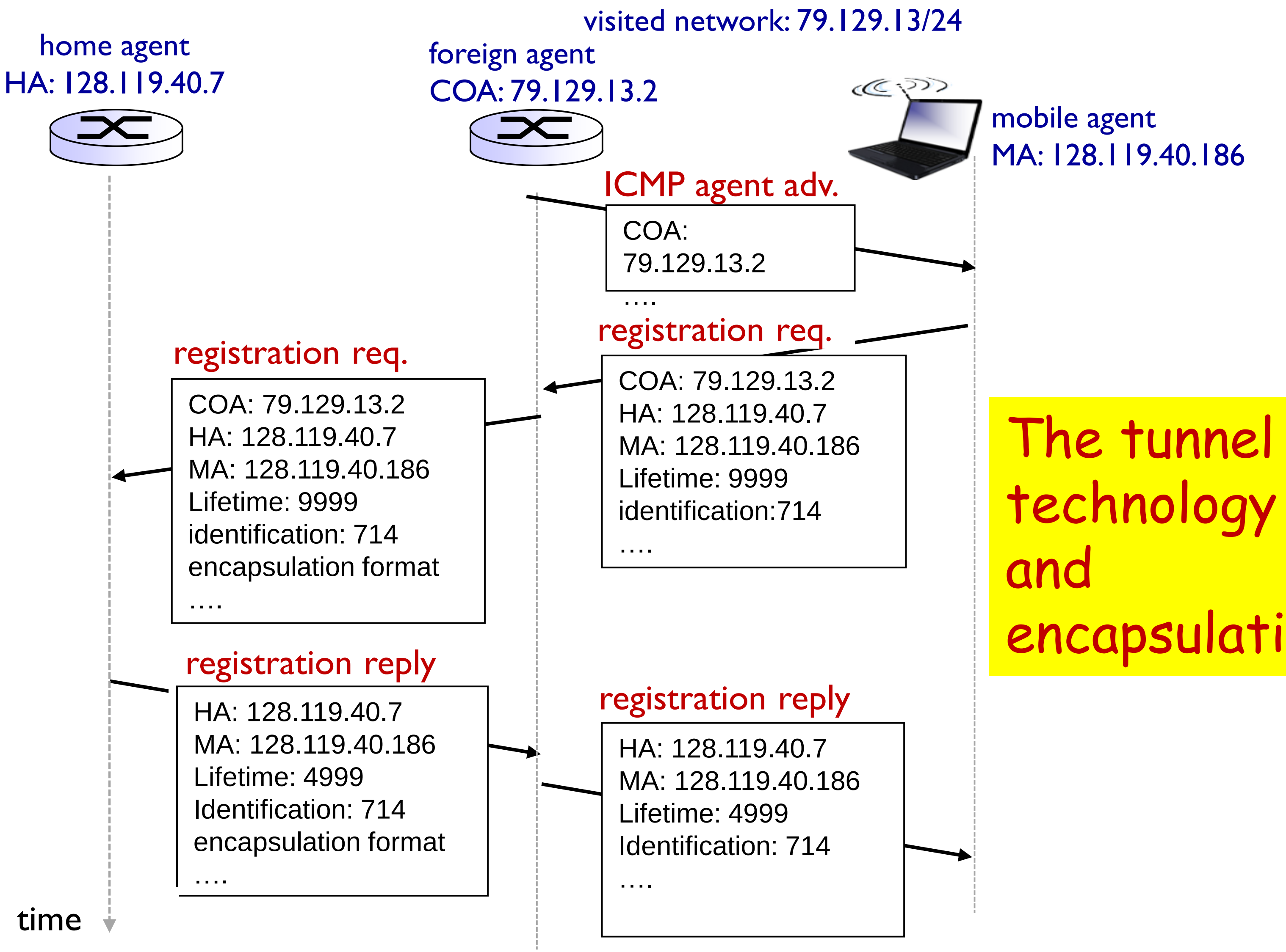
type = 16 | length | sequence #

registration lifetime | RBHFMGV bits | reserved

0 or more care-of-addresses

mobility agent advertisement extension

Mobile IP: registration example



visited network: 79.129.13/24

home agent
HA: 128.119.40.7

foreign agent
COA: 79.129.13.2

mobile agent
MA: 128.119.40.186

ICMP agent adv.

COA:
79.129.13.2
….

registration req.

COA: 79.129.13.2
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 9999
identification:714
….

registration req.

COA: 79.129.13.2
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 9999
identification: 714
encapsulation format
….

registration reply

HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
….

registration reply

HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
….

time

The tunnel technology and encapsulation

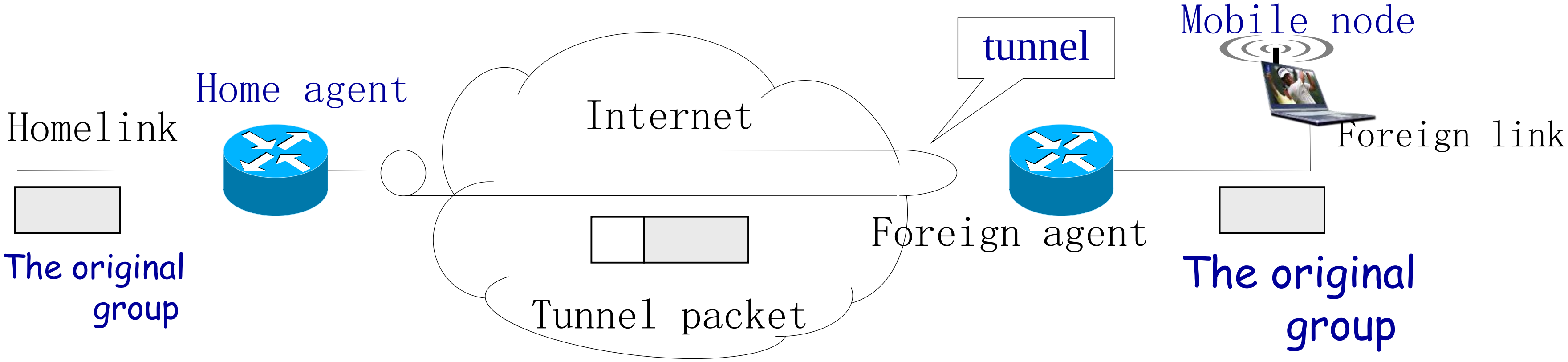
The tunnel technology

- Mobile IP uses tunneling technology to packet the IP of the communication pair and encapsulate it with the IP first part, so that the packet can reach the field network accessed by the mobile node through the standard IP routing technology, and then be unsealed and delivered to the mobile node.
- There are three types of tunnel encapsulation.
- At either end of the tunnel are wrappers and unwrappers, which are configured on the home and foreign agents of the mobile node (or the mobile node itself), respectively.

✓ **IP in IP** encapsulation
✓ **the min** encapsulation
✓ **GRE** encapsulation

11.5.1 IP in IP encapsulation

- IP in IP encapsulation is a protocol enforced Internet standard used to encapsulate the entire IPv4 packet in the data portion of a new IPv4 packet.



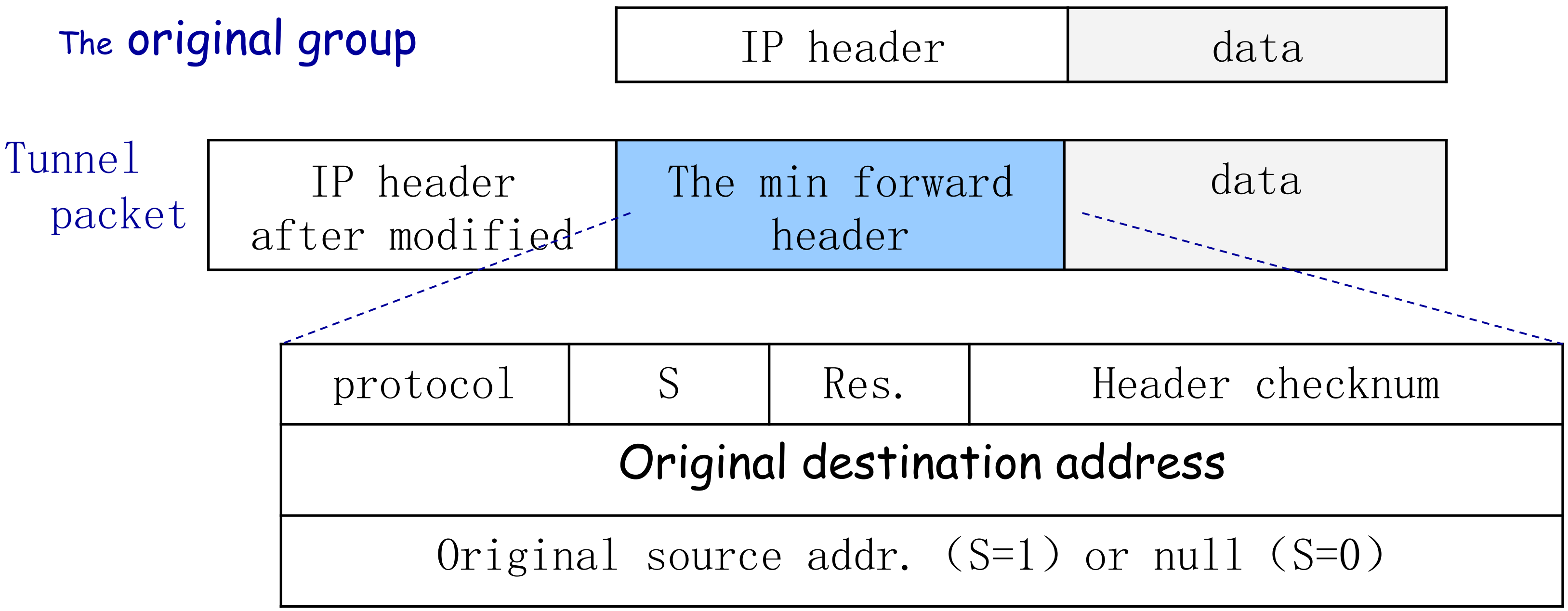
The original group

IP header	data

Tunnel packet

IP header	IP header	data

✓the min encapsulation



The original group

IP header | data

Tunnel packet

IP header after modified | The min forward header | data

protocol | S | Res. | Header checknum

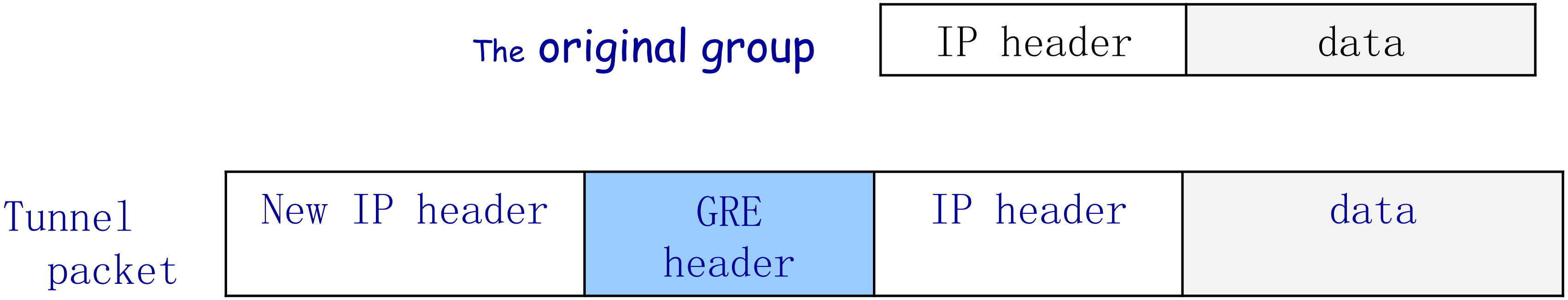
Original destination address

Original source addr. (S=1) or null (S=0)

11.5.3 GRE encapsulation

- Before two kinds of tunnel support only IP encapsulation technology, and GRE (Generic routing encapsulation) can encapsulate IP protocol, it also support other network layer protocol, allows a protocol data packet, encapsulated in another kind of protocol data packet payload, is a multi-protocol tunnel encapsulation technology.
- It adds the GRE package header to the original IP packet header, and then adds a new IP header.The minimum length of the GRE header is 4 bytes

GRE encapsulation



The original group

IP header | data

Tunnel packet

New IP header | GRE header | IP header | data

Routing forwarding

- In mobile IP networks, due to the mobility of nodes, ordinary routers cannot complete IP packet forwarding.
- In addition to routers, the home agent and the foreign agent are required to forward packets to mobile nodes connected to the foreign network together.
- Home agents forward it to the forwarding address of mobile nodes. Home agents and foreign agents must support tunneling technology encapsulated by "**IP in IP**".

Mobile IPv6

- Support for mobility is an optional part of the IPv4 protocol, and mobility is an integral part of the IPv6 protocol.
- The IPv4 protocol does not have enough address space to assign addresses to each mobile device. Mobile IPv6 can meet the needs of large-scale mobile users through simple extensions.
- In mobile IPv4, when the communication pair communicates with the mobile host, the triangular path of mobile IP is formed.

What’ s the triangular ?

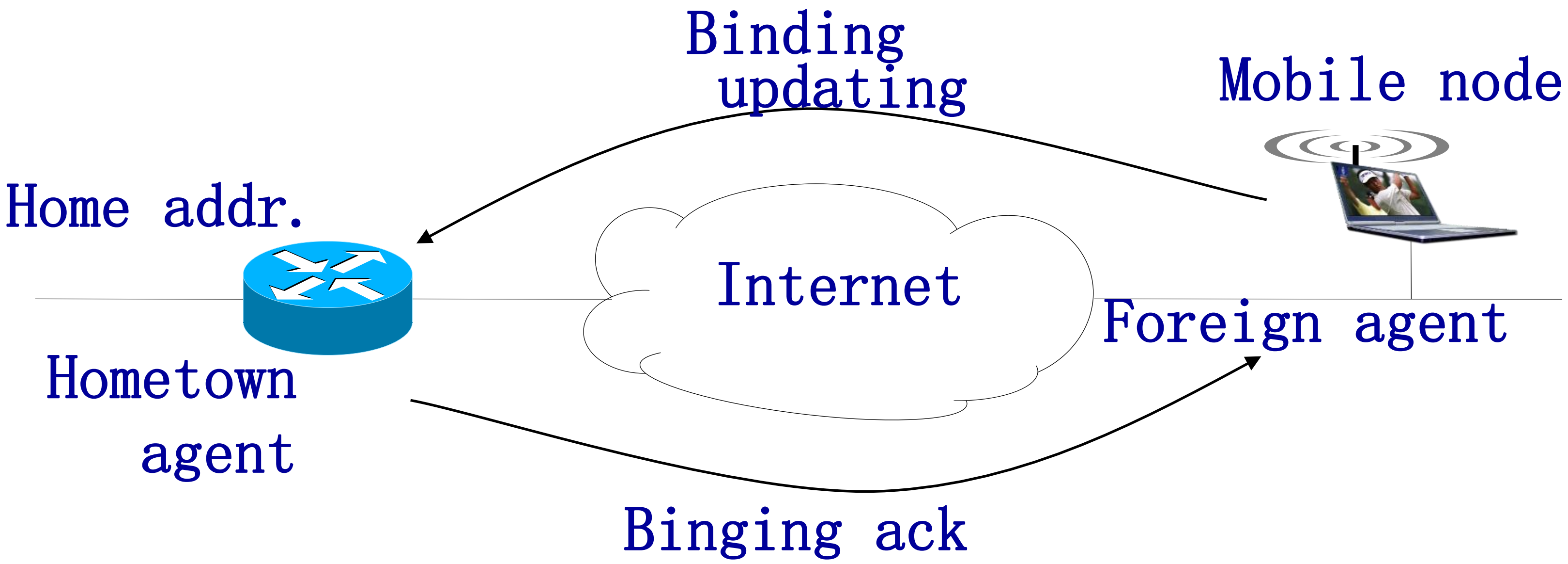
How it works for mobile IPv6?

- Mobile IPv6 follows some of the basic concepts and technologies of mobile IPv4. Mobile IPv6 does not require a foreign agent to forward the grouping of mobile nodes.
- In mobile IPv6, both tunneling and source routing technologies are used to transfer packets to mobile nodes connected to external links.
- The high-level functionality of mobile IPv6 is similar to that of mobile IPv4, and is similar to the three elements of mobile IPv4: proxy discovery, registration, and routing.

✓ Location determination and movement detection of mobile nodes

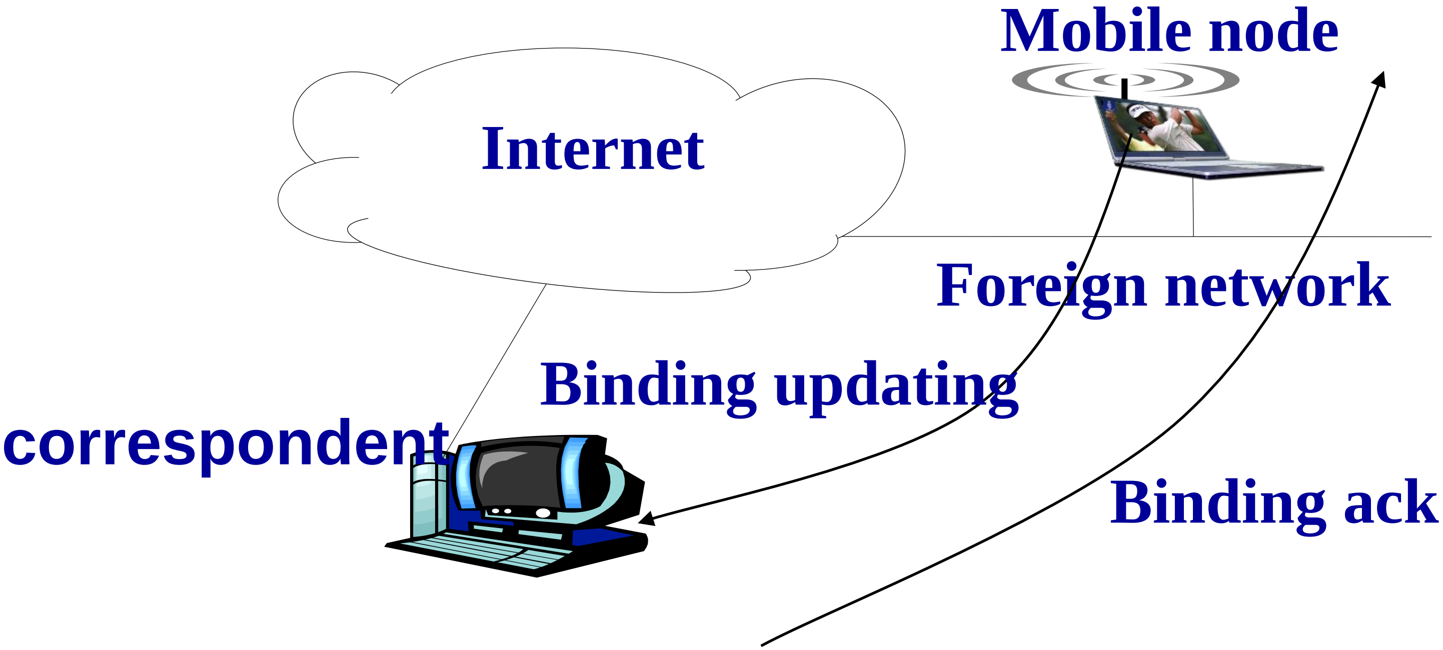
✓ Mobile binding of the home agent

Mobile binding of the home agent



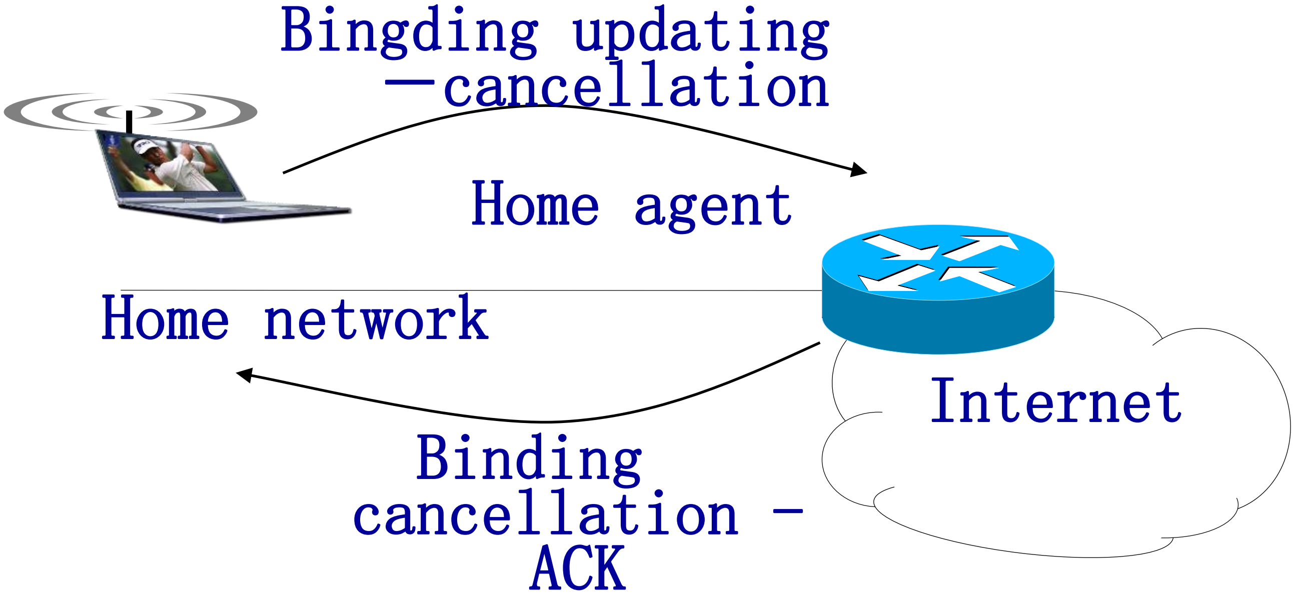
correspondent binding

- correspondent dynamically learns and updates the address binding information of the mobile node. How does it work?



The cancellation of registration

- When the mobile node returns to its home link, it tells the home agent that it is no longer connected to the foreign link and needs to log out the original transfer address.



5. The operation of mobile IPv6

- Mobile nodes adopt IPv6 router discovery mechanism to determine their current location.
- A mobile node connected to its home link works as any fixed host and router.
- When a mobile node is connected to a foreign link, it uses the IPv6 defined **address automatic configuration method** to obtain the transfer address on a foreign link.
- The mobile node advertise the home agent

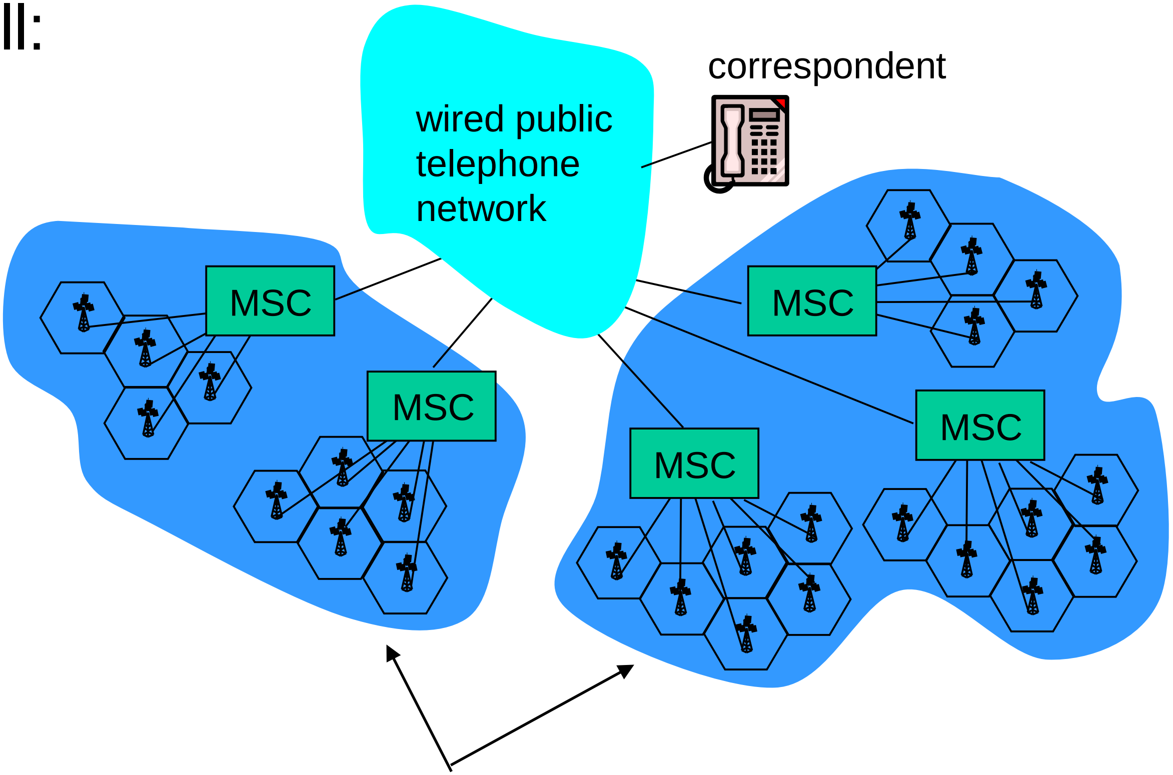
Mobile IPv6 versus mobile IPv4

- Mobile IPv6 inherits many basic features of mobile IPv4 and borrows some concepts of mobile IPv4, such as mobile nodes, home agents, home addresses, and transfer addresses.
- But mobile IPv6 does not have the concept of a foreign agent and a foreign agent forwarding address.
- IPv6 design draws on the mobile IPv4 protocol development experience, combined with many new features of IPv6

- 1. address
- 2. optimize the routing
- 3. Home agent
- 4. security

Components of cellular network architecture

recall:

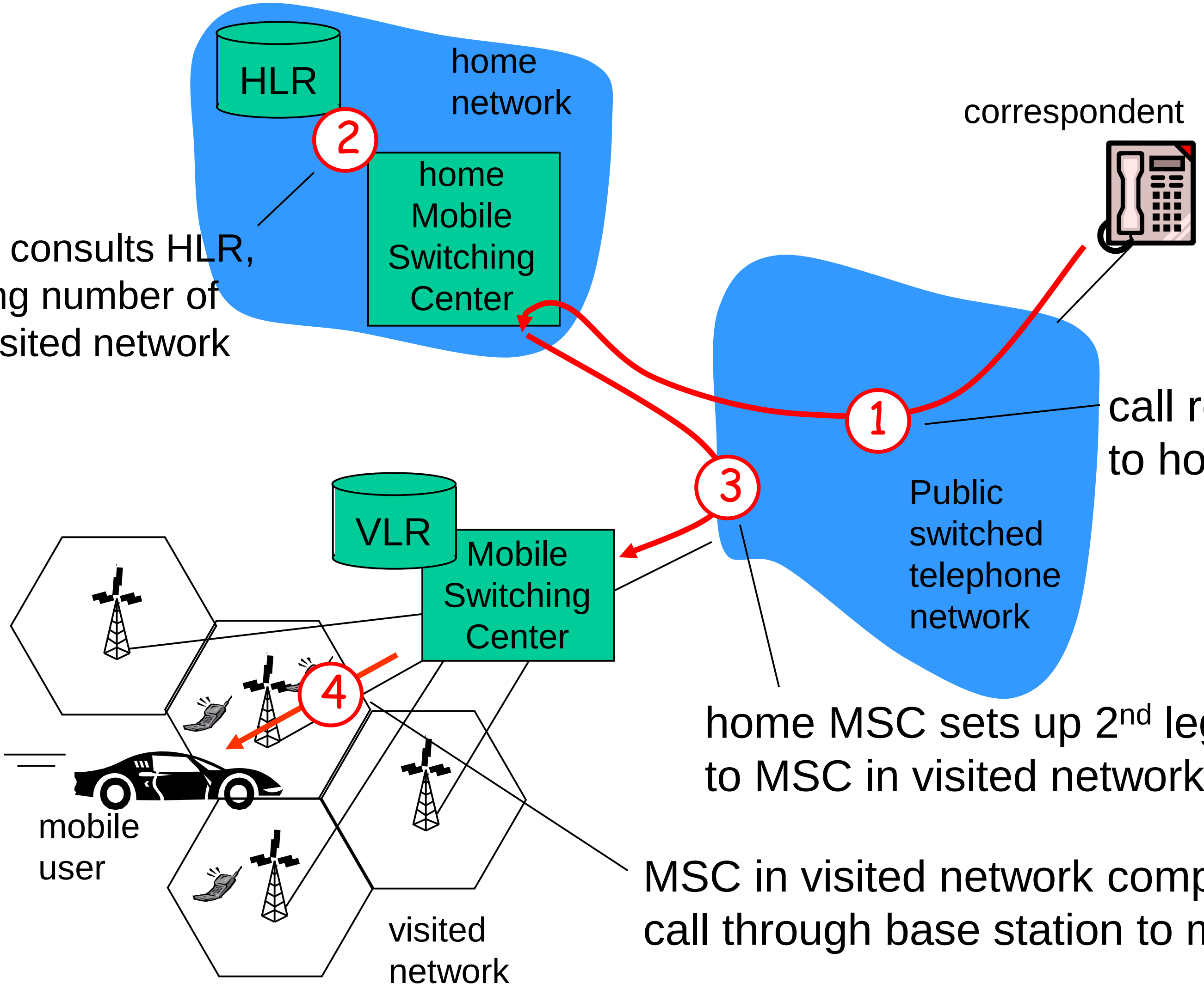


different cellular networks, operated by different providers

Handling mobility in cellular networks

- *home network:* network of cellular provider you subscribe to (e.g., Sprint PCS, Verizon)
  - *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



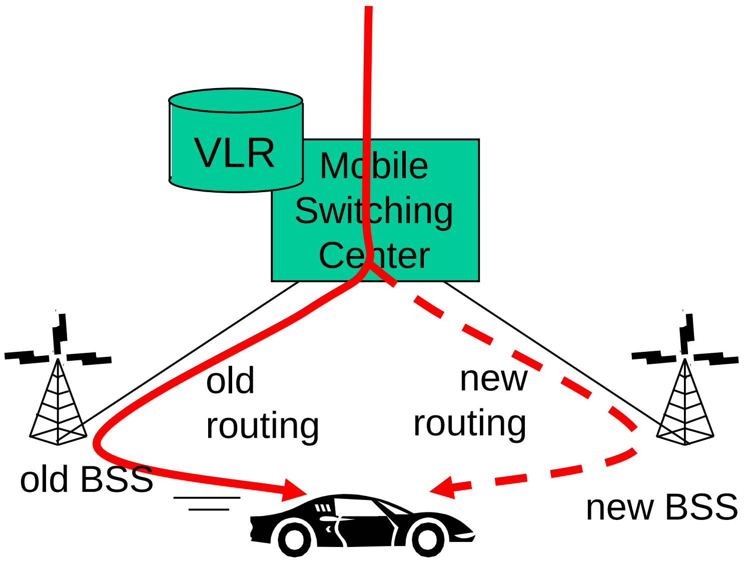
home MSC consults HLR, gets roaming number of mobile in visited network

call routed to home network

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

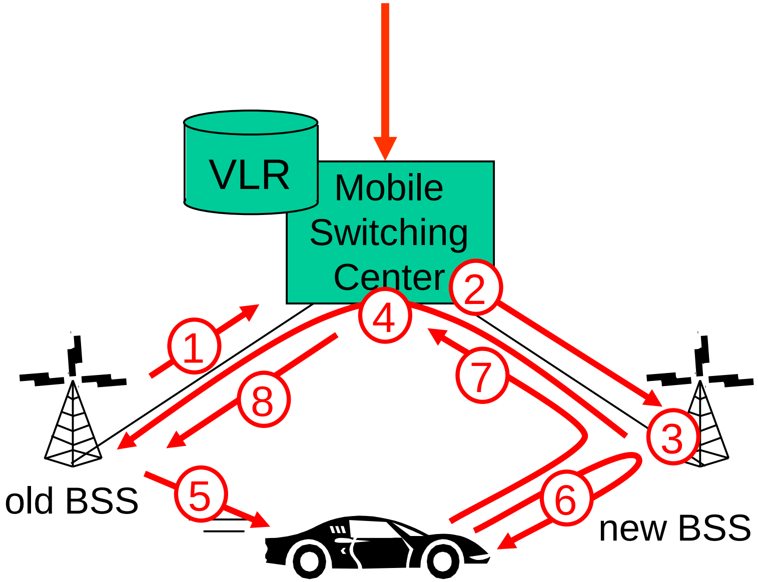
MSC in visited network completes call through base station to mobile

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
  - GSM doesnt mandate why to perform handoff (policy), only how (mechanism)
- handoff initiated by old BSS

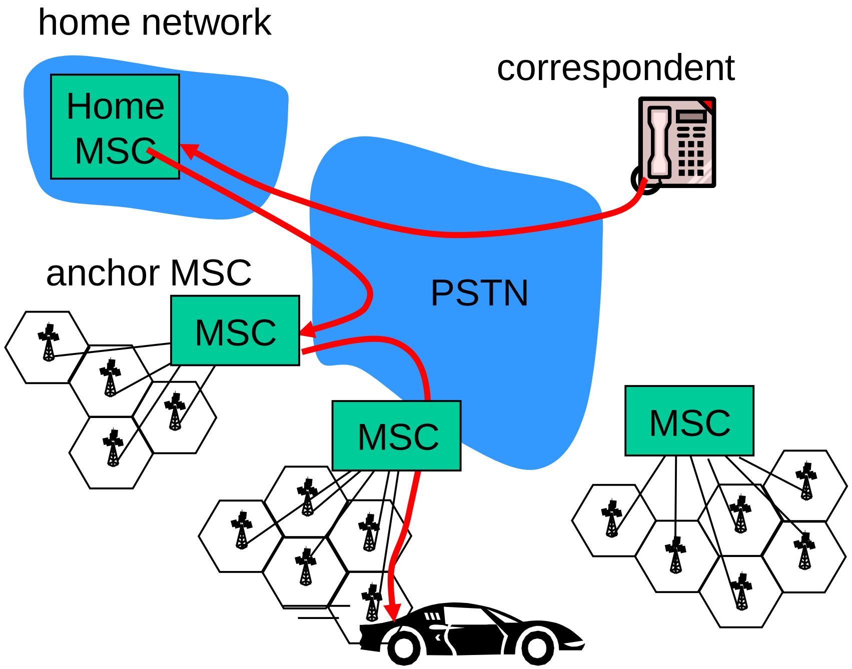
GSM: handoff with common MSC



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

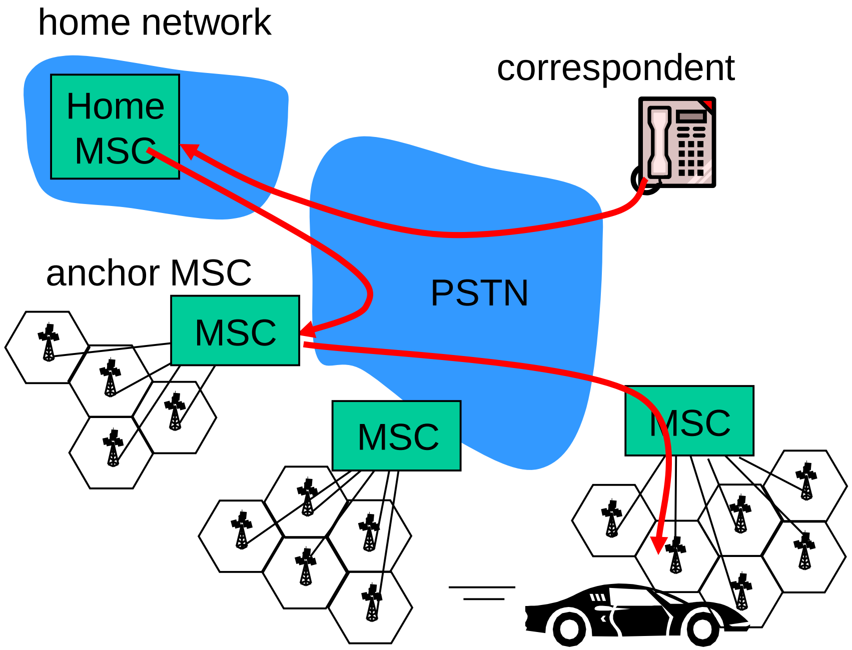
GSM: handoff between MSCs



(a) before handoff

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

GSM: handoff between MSCs



(b) after handoff

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

Mobility: GSM versus Mobile IP

GSM element	Comment on GSM element	Mobile IP element
Home system	Network to which mobile user's permanent phone number belongs	**Home network**
Gateway Mobile Switching Center, or "home MSC". Home Location Register (HLR)	Home MSC: point of contact to obtain routable address of mobile user. HLR: database in home system containing permanent phone number, profile information, current location of mobile user, subscription information	**Home agent**
Visited System	Network other than home system where mobile user is currently residing	**Visited network**
Visited Mobile services Switching Center. **Visitor Location Record (VLR)**	Visited MSC: responsible for setting up calls to/from mobile nodes in cells associated with MSC. VLR: temporary database entry in visited system, containing subscription information for each visiting mobile user	**Foreign agent**
Mobile Station Roaming Number (MSRN), or "roaming number"	Routable address for telephone call segment between home MSC and visited MSC, visible to neither the mobile nor the correspondent.	**Care-of-address**

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
  - limited bandwidth of wireless links

Chapter 6 summary

Wireless

- wireless links:
  - capacity, distance
  - channel impairments
  - CDMA
- IEEE 802.11 ("Wi-Fi")
  - CSMA/CA reflects wireless channel characteristics
- cellular access
  - architecture
  - standards (e.g., GSM, 3G, 4G LTE)

Mobility

- principles: addressing, routing to mobile users
  - home, visited networks
  - direct, indirect routing
  - care-of-addresses
- case studies
  - mobile IP
  - mobility in GSM
- impact on higher-layer protocols