cnm.

Management Operations of the IEEE 802.11

Mei Yen Cheong

meiyen.cheong@hut.fi

S-72.333 Postgraduate Seminar on Radio Communications

Helsinki University of Technology

April 13, 2004

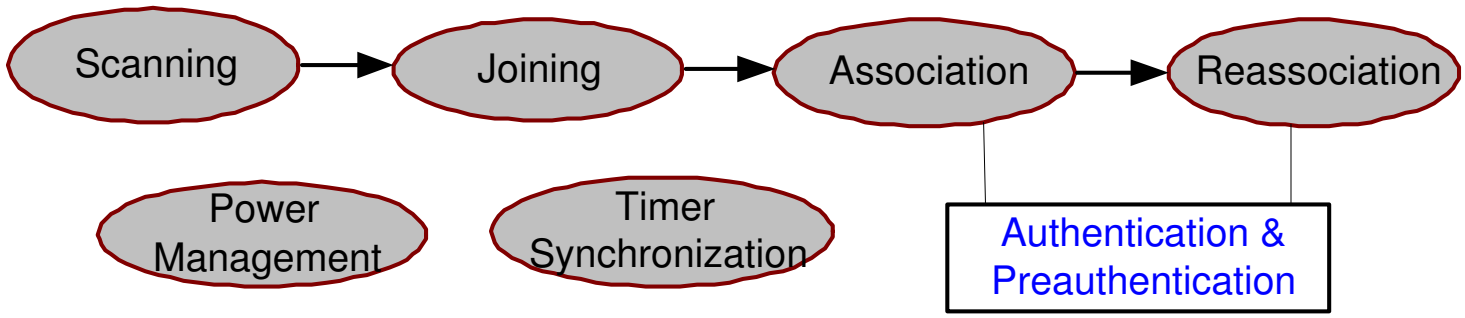
Contents

- Introduction
- Management Architecture of 802.11
- Management Operations
  - Procedure for MS to gain access to 802.11 network:

    Scan → Join → Association → Reassociation.
  - Power management
  - Timer synchronization

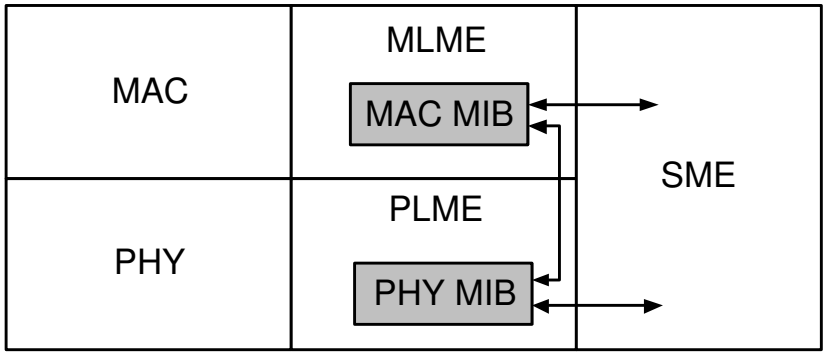
Introduction

- Disadvantages of wireless connection are:-
  - Unreliable medium
  - lack of physical boundaries (security problems)
  - power limitation of mobile terminals
- Management operations of 802.11 address these problems.



Management Architecture (1/2)

- System management entity (SME)
  - not normally specify by 802.11
  - method which users and device drivers interact with the 802.11 network interface and status enquiry.
  - can alter the MAC and PHY Management Information bases (MIBs).

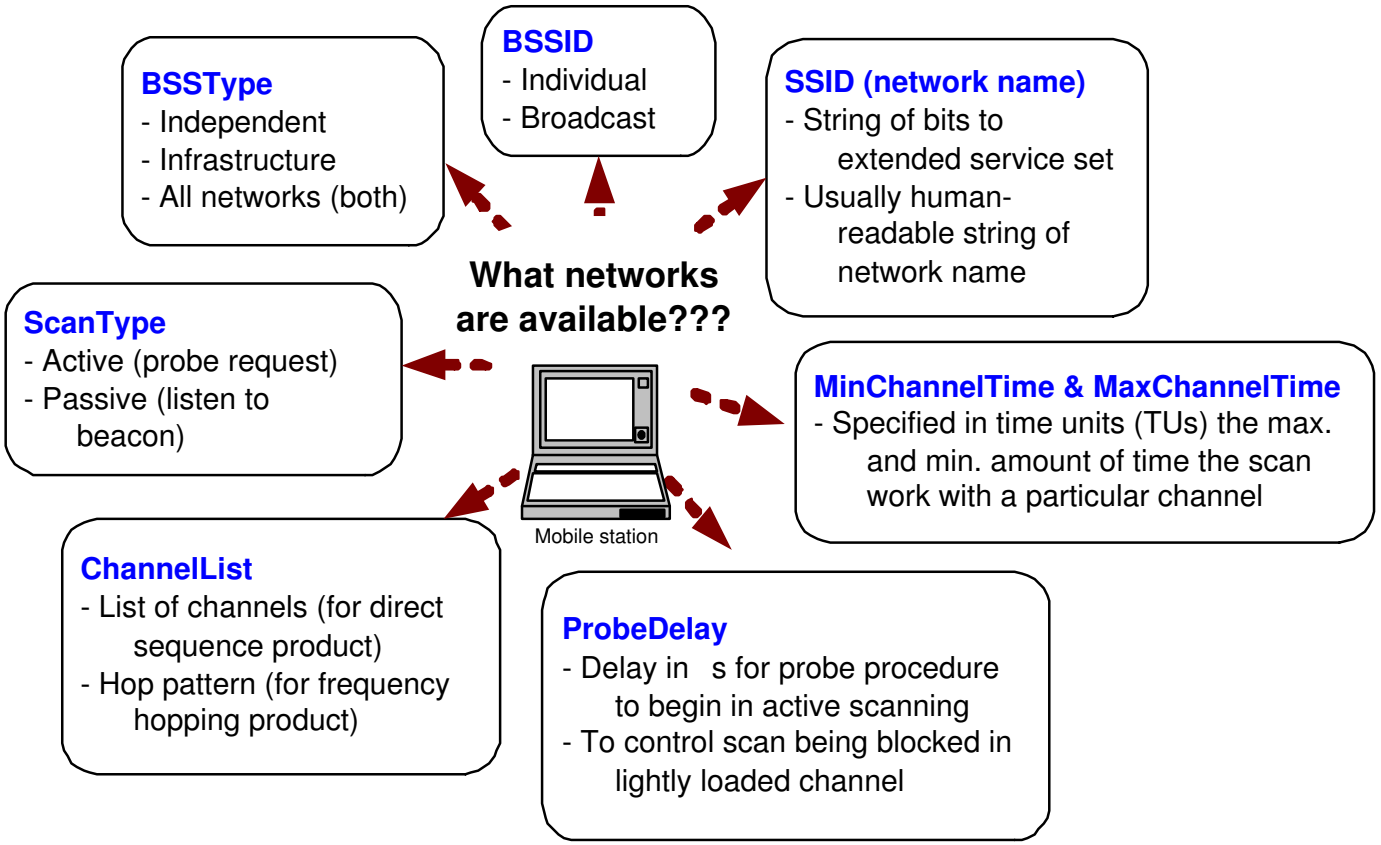


Management Architecture (2/2)

- MAC layer management entity (MLME) & Physical-layer management entity (PLME)
  - have access to Management Information Base (MIB) to gain status information & to invoke certain actions
  - MAC can make corresponding changes to the PHY MIB
- Capabilities of device drivers vary depending on the product.
- However, possible capabilities are defined within the management features of the 802.11 protocols.

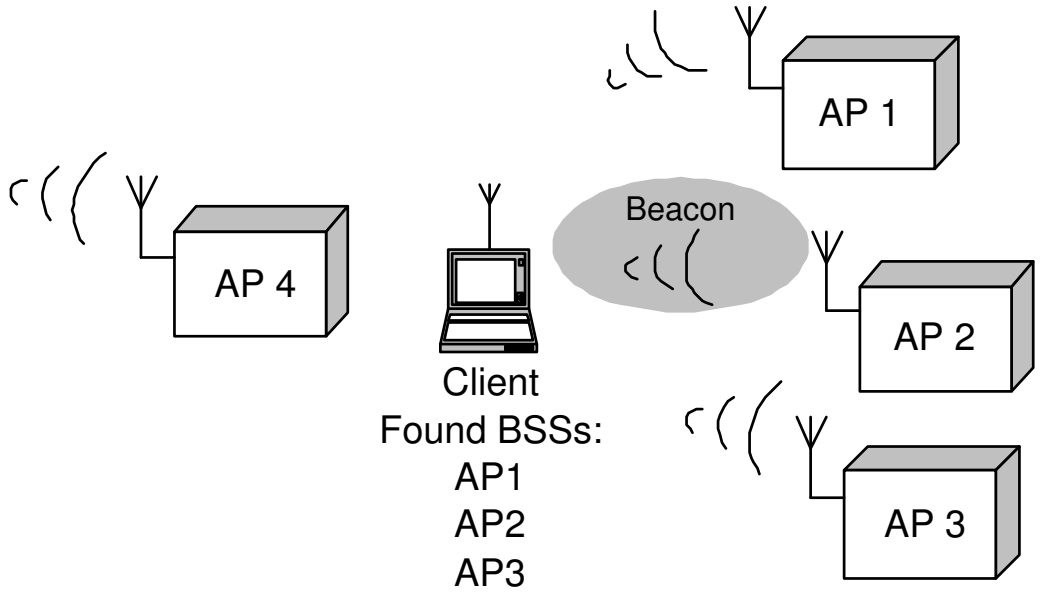
Scanning

- Parameters involve in scanning procedure



Passive scanning

- Station sweeps thro' the channels, listens and records information from received Beacons.
- Beacons contains information of parameters in the basic service set (BSS).

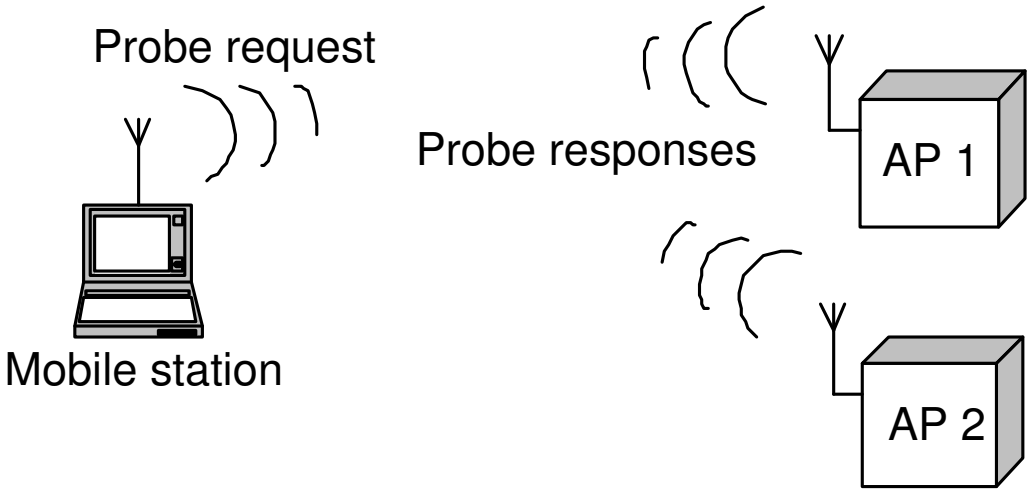


Active scanning (1/2)

- Station detects for channel in use.
- Station sends *Probe Request* to seek response from the network.
- Network with the requested extended service set sends a *Probe Response* upon hearing the *Probe Request*.
  - Individual SSID triggers single *Probe Response*.
  - Broadcast SSID triggers *Probe Response* form all networks in the area.

Active scanning (2/2)

- In infrastructure network, the APs are responsible for sending *Probe Response*.
- For BSS the station that transmitted the last Beacon is responsible for *Probe Response*.



Scan Report

- Lists all scan discovered BSSs and their parameters.
- Complete parameter list enables station to join network.
- Extra parameters in the report are:-
  - *Beacon interval*
  - *DTIM* period - for power-saving mechanism
  - *Timing parameter* - for synchronization of station and BSS's timer.
  - *PHY, CF and IBSS parameters*
  - *BSSBasicRateSet* - list the data rates the station must support to join the network.

Joining (1/2)

- Precursor to association which does not enable network access.
- Choosing BSS to join is an implementation-specific decision, may involve user intervention.
- BSSs of the same ESS are allow to make decision, common criteria are power level and signal strength.

Joining (2/2)

Joining a selected BSS requires

- Matching local parameters required by BSS
- Matching PHY parameters.
- Synchronizing timing inofrmation of station and rest of network.
- Matching WEP & high-rate capabilities.
- Adopt the Beacon interval and DTIM period of BSS.

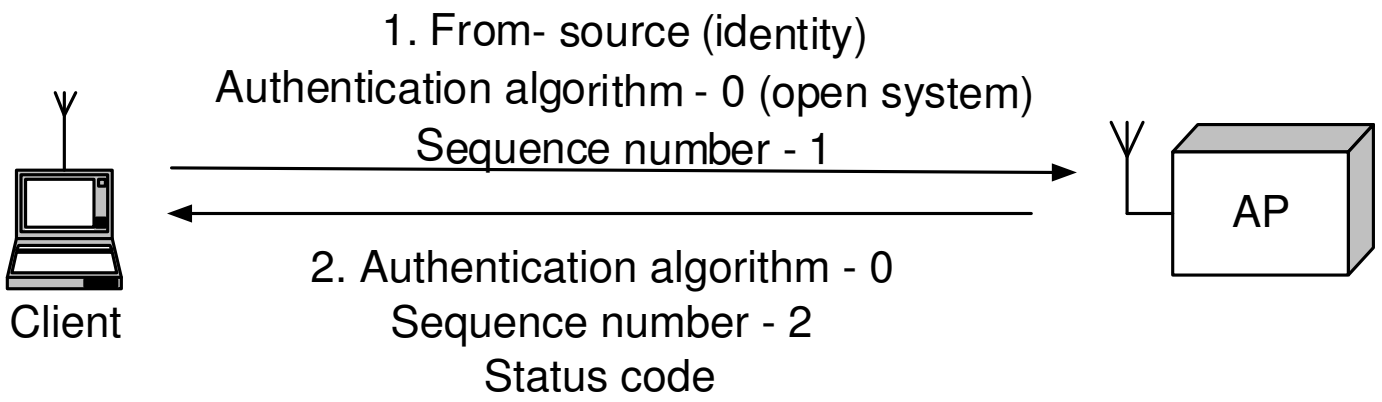
Authentication

- Security procedure before station is allow to access the network.
- Two approaches specified by 802.11.
  - *open system* authentication
  - *shared-key* authentication
- Any station can authenticate with another station.
- Currently, for infrastructure network, only station needs to authenticate to network and not vice-versa.

  Note: This makes man-in-the-middle attack possible.

Open-System Authentication (1/2)

- Access point (AP) accepts the mobile station without verifying its identity.
- The AP records the MAC address of the station as its identity.



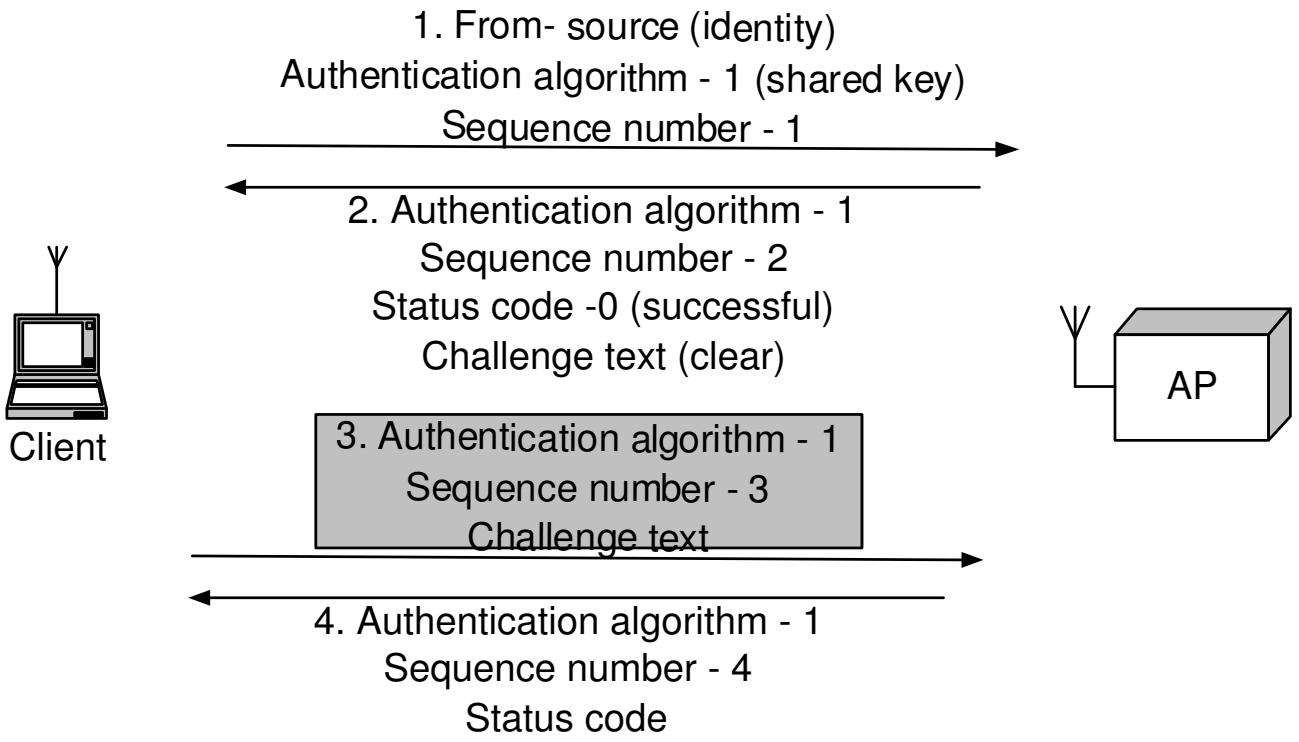
Open-System Authentication (2/2)

- *Address Filtering* is a method to provide some security in open-system authentication.
- Some products provide an "authorized MAC address list".
- Network administrator can enter a list of authorized client addresses.
- Trivial file transfer protocol (TFTP) servers can be implemented to push authorized addresses to multiple access points (minimize need for separate distribution).

Shared-Key Authentication (1/2)

- Only possible on products that implement Wired Equivalent Privacy (WEP) since this authentication method makes use of WEP.
- A shared-key is distributed to all stations before authentication is attempted.
- This method requires verification of station's identity using the Challenge Text before allowing admission to the network.
- The Challenge Text (128 bytes) is generated using the WEP keystream generator with a random key and initialization vector.

Shared-Key Authentication (2/2)



- The Challenge Text in the 3 rd sequence is processed with WEP, therefore is hidden.

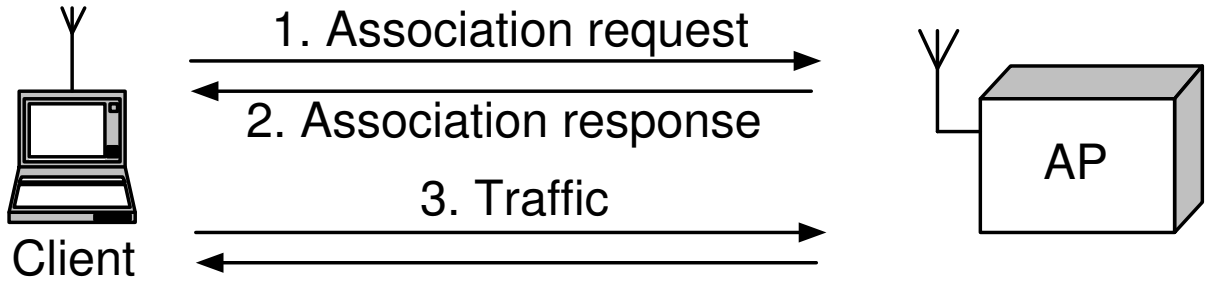
Preauthentication

- Authentication does not have to take place immediately before association.
- Preauthentication is authentication done during the scanning process.
- Preauthetication allows a station to:-
  - associate with an AP quickly.
  - reassociate with the APs immediately upon moving into their coverage area.

Association (1/2)

- Authenticated stations can associate with an AP to gain full access to network.
- Association allows the distributed system to track the mobile location.
- Once association is completed, the AP must register the station on the network so that frames for the station are delivered to the AP.
- Registration can be done by sending a gratuitous ARP so that the MAC address of the station is associated with the switch port of the AP.

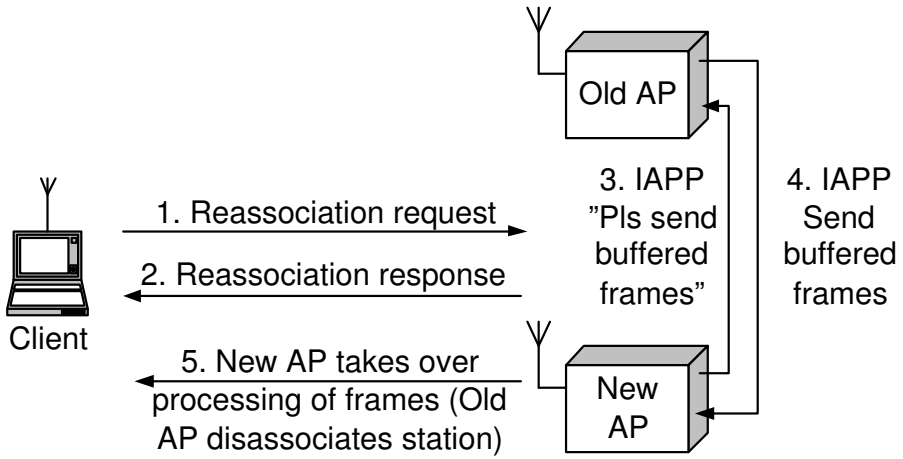
Association (2/2)



- Successful: Status code 0 and Association ID (AID).
- Unsuccessful: Status code $\neq$ 0 and end of procedure.
- Unauthenticated stations will receive Deauthentication frame from the AP.

Reasociation

- Mobility management - moves an association from old AP to new AP in the same ESS.
- On backbone, interactions between APs is invoked (IAPP).
- The old AP terminates the association after transferring buffered frames to new AP.



Power Management

- Power saving features are important for mobile stations due to scarce resource of battery power.
- Switching off the transceiver is one of the most effective power savings in wireless network.
- Power saving (PS) modes:-
  - Sleeping - transceiver is off.
  - Active - transceiver is on.
- Power conservation in 802.11 is achieved by maximizing the sleeping time without sacrificing connectivity.

Power Management in Infrastructure Networks (1/2)

- Access points play a key role in power management for infrastructure networks due to:-
  - AP knows the location of mobile stations and a mobile station can communicate its PS mode AP.
  - APs remain active all the time due to continuous power supply and easier implementation of buffer system.
- Power management tasks of APs:-
  - Buffer frames for sleeping mobile stations.
  - Announce periodically of buffer status.

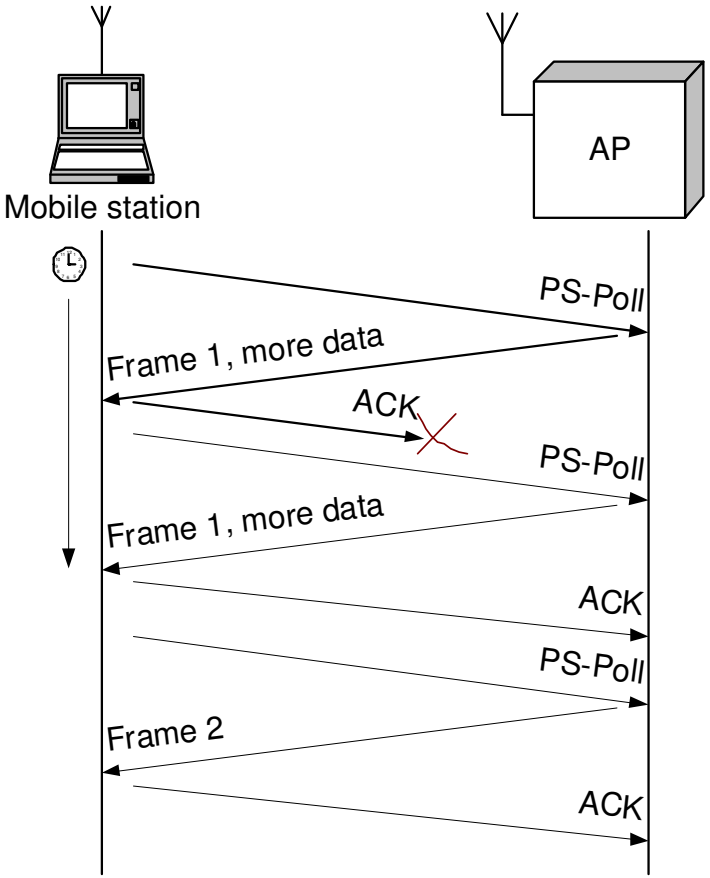
Power Management in Infrastructure Networks (2/2)

- Mobile station only power up the receiver to listen to buffer status instead of periodically transmitting polling frames.
- Mobile station can sleep as long as the number of Beacon periods defined in the *Listen Interval* parameter during association.
- The *Listen Interval* therefore defines the maximum buffer space reserved for the associated station.
- Buffered frames may be discarded without after each listen interval.

Unicast buffering & delivery (1/2)

- APs periodically transmit a *Traffic Indication Map* (TIM) in its Beacon frames.
- TIM composed of 2008 bits which each bit corresponds to a particular AID.
- During the station listening time, TIM in the Beacon frame is examine whether frames are buffered for it.
- *PS-Poll Control* frames is used to retrieve buffered frames.

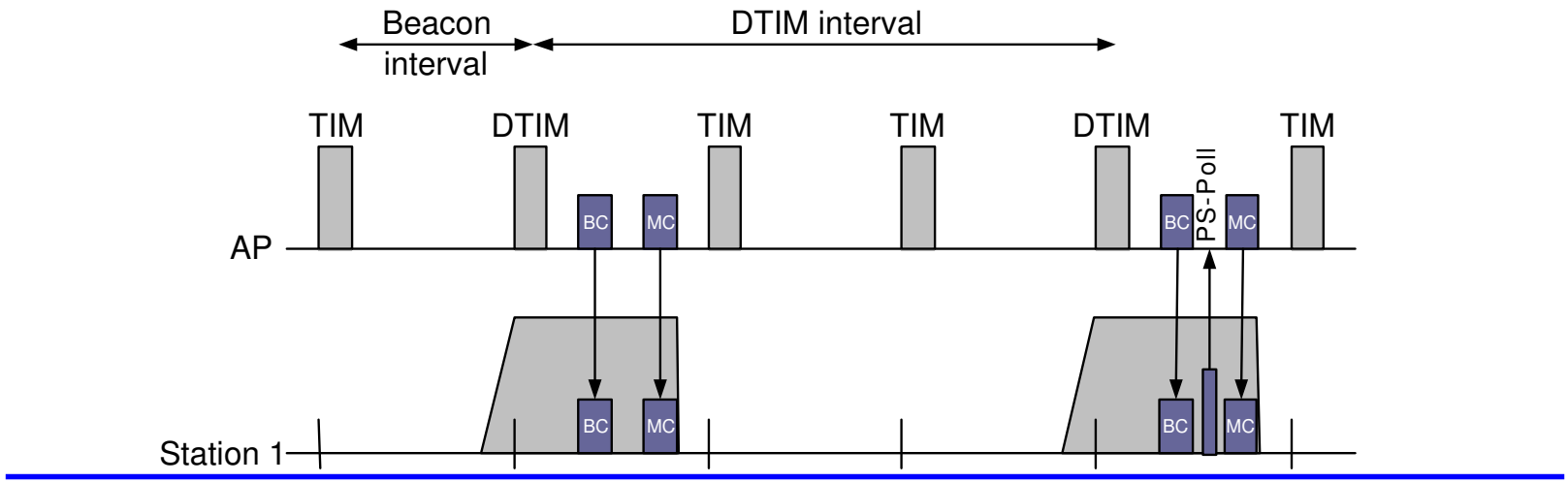
Unicast buffering & delivery (2/2)



- Each *PS-Poll* frame retrieves only one buffered frame.
- Positive acknowledgement need to be signaled for one second before the next PS-Poll.
- AP sends a frame in response and if more frames are still in buffer, the *More Data* bit in the Control field is set to 1.

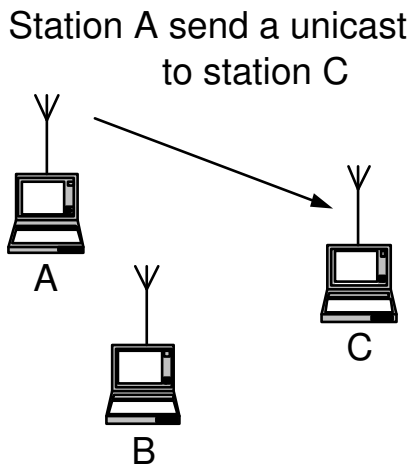
Delivering multicast & broadcast frames

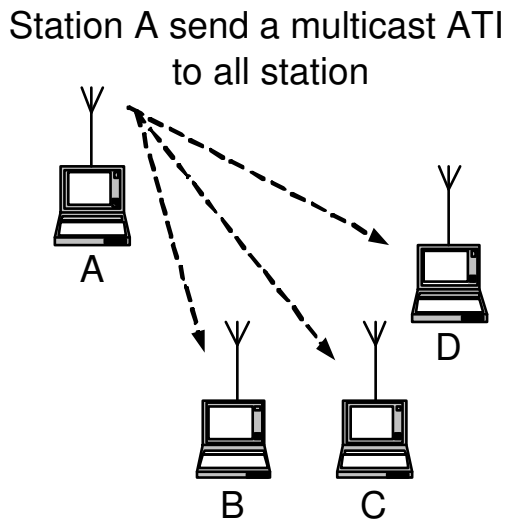
- Multicast & broadcast frames are indicated using AID "0"; Setting bit 1 of TIM to "0".
- At fixed number of Beacon intervals, special TIM called Delivery TIM (DTIM) is sent.
- Multiple buffered frames are sent after each DTIM.



Power Management in IBBS (1/3)

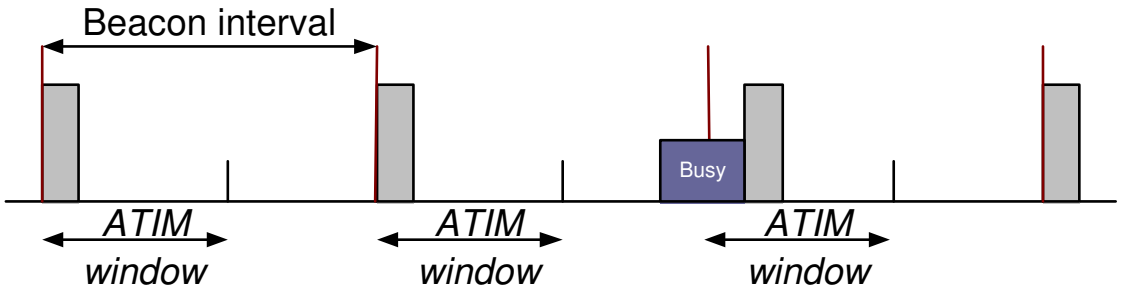
- In an Independent Basic Service Set (IBSS), the station that has buffered data is responsible to ensure receiver(s) is(are) active.
- Announcement Traffic Indication Message (ATIM) is sent to keep receiving station(s) awake.





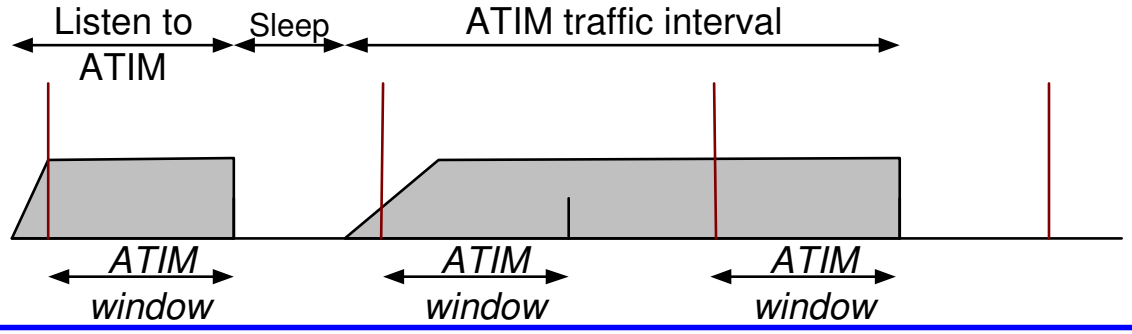
Power Management in IBBS (2/3)

- All stations in an IBSS listen for ATIM frames during a period after the Beacon called *ATIM window*.
- *ATIM window* is an IBSS specific parameter.
- ATIM window remains constant, staring at the target Beacon interval and extending a fixed amount of time.



Power Management in IBBS (3/3)

- Stations that neither transmit nor receive ATIM is permitted to sleep.
- A station that transmits and/or receives ATIM it must stay active until the conclusion of the next ATIM window.
- Only Beacons, RTS, CTS, ACK and ATIM can be sent in the *ATIM window*.



Timer Synchronization

- Timing information is important in wireless network for:-
  - Coordination of transmission time/pattern.
  - Medium reservation
- In 802.11, *Timing Syncronization Function* (TSF) is used to synchronize all stations in the network.
- TSF are periodically announced in the Beacon frames.
- In infrastructure network, APs are responsible maintaining the TSF while for IBSS, the process is distributed.

Exercise

- What are the management operations involved in gaining access to a 802.11 networks? Draw sequence diagram to show the procedures.
- What is the difference between JOINING a network and ASSOCIATING to a network?
- Describe the Power Management in Infrastructure network and independent BSS.