7. IEEE 802.11 Wireless LAN MAC Standard

Wireless LAN Architecture

- Major differences between Wireless LAN and Wired LANs:
  - Destination address does not equal destination location.
    - » In wired LANs, an address is equivalent to a physical address.
    - » In 802.11, the addressable unit is a station (STA).
      - The STA is a message destination, but not a fixed location.
  - The media impacts the design
    - » The PHY layers used in 802.11 are fundamentally different from wired media.
    - » 802.11 PHYs:
      - Have limited physical point to point connection ranges.
      - Use a shared medium.
      - Are unprotected from outside signals.
      - Are significantly less reliable than wired PHYs.
      - Have dynamic topologies.

Wireless LAN Architecture

- Impact of handling mobile stations
  - A portable station is one that is moved from location to location, but is only used while at a fixed location.
  - Mobile stations actually access the LAN while in motion.
  - Propagation effects blur the distinction between portable and mobile stations.
- Interaction with other 802 layers
  - 802.11 is required to appear to higher layers (LLC) as a current 802 style LAN.
  - Station mobility has to be handled within the MAC layer.

802.11 Wirelss LAN Characteristics

- 1, 2, 5.5, 11, 22, 33, 6, 9, 12, 18, 24, 36, 48, 54, 72, 150 500 Mbps
- Transmission medium: Radio
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) Protocol
  - Provides priority scheme using different contention windows (IEEE 802.11e)
    - Provides delay guaranteed transmission service.
- CSMA/CA avoids most of the collisions so that the transmission delay can be guaranteed.
- Bandwidth fairness is guaranteed or not (to observe long time).
- By employing the CSMA/CA protocol, the bandwidth employed by each station may be different.
  - Needs load sharing scheme in the near future ?

802.11 Wirelss LAN Characteristics

- **Changes and additions to IEEE Std. 802.11-1999:**

- **(1). IEEE Std 802.11a-1999--High-speed Physical Layer Extension in the 5 GHz Band:**
  - **Frequency range: 5.15-5.25, 5.25-5.35, and 5.725-5.825 GHz.**
  - **System: orthogonal frequency division multiplexing (OFDM).**
  - **Data payload communication capability: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.**

- **(2). IEEE Std 802.11b-1999--High-speed Physical Layer Extension in the 2.4 GHz Band:**
  - **Frequency range: 2.4 - 2.4835 GHz.**
  - **System: Direct Sequence Spread Spectrum (DSSS).**
  - **Data payload communication capability: 1, 2, 5.5, and 11Mbps.**

802.11 Wirelss LAN Characteristics

- (3). IEEE Std 802.11g-2003—Further Higher-Speed Physical Layer Extension in the 2.4GHz Band
  - Frequency range: 2.4 GHz.
  - System: hybrid DSSS and OFDM.
  - Data payload communication capability: 22, 33 / 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.
- (4). IEEE Std 802.11e-2003—Medium Access Control (MAC) Enhancements for Quality of Services (QoS)
- (5). IEEE Std 802.11i-2003—Enhanced Security
  - WEP
  - TKIP
  - WRAP
  - CCMP

802.11 Wirelss LAN Characteristics

- **IEEE 802.11s：Mesh Networking, Extended Service Set（ESS）（July 2011）**
- **IEEE 802.11aa：Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: MAC Enhancements for Robust Audio Video Streaming**
- **IEEE 802.11ac： Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications--Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz.**
- **IEEE 802.11ad：Very High Throughput 60 GHz (December 2012) - see WiGig**

802.11 Wirelss LAN Characteristics

- IEEE 802.11ae：IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Prioritization of Management Frames

- IEEE 802.11af：Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Television White Spaces (TVWS) Operation

802.11 Architecture Components

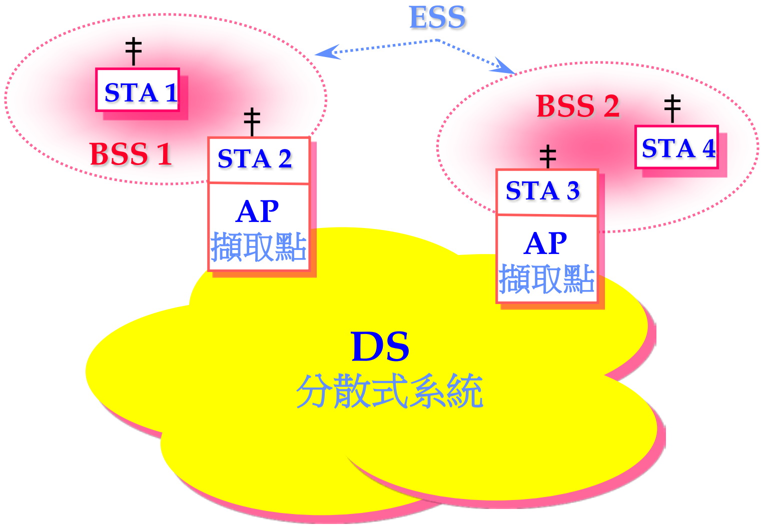
- Wireless Medium (WM):
  - The medium used to implement a wireless LAN.
- Station (STA):
  - Any device that contains an 802.11 conformable MAC and PHY interface to the wireless medium.
- Station Services (SS):
  - The set of services that support transport of MSDUs (MAC Service Data Units) between Stations within a BSS.
- Basic Service Set (BSS):
  - A set of STAs controlled by a single CF (Co-ordination Function).
  - The BSS is the basic building block of an 802.11 LAN.
  - The members of a BSS can communicate to each other directly.
  - If a station moves out of it's BSS coverage area, it can no longer directly communicate with other members of the BSS.
- The Independent BSS as an Ad-Hoc Network
  - This mode of operation is possible when 802.11 LAN stations are close enough to form a direct connection (without pre-planning).

802.11 Architecture Components

- Distribution System (DS):
  - A system used to interconnect a set of BSSs to create an ESS.
  - Used in Infrastructure Network
- Distribution System Medium (DSM):
  - The medium used by a DS (for BSS interconnections)
  - 802.11 logically separates the WM from the DSM.
  - Each logical medium is used for different purposes by different components of the architecture.
  - The DS enables mobile device support by providing the logical services necessary to handle address to destination mapping and seamless integration of multiple BSSs.

802.11 Architecture Components

- Distribution System Services (DSS):
  - The set of services provided by the DS which enables the MAC to transport MSDUs between BSSs within an ESS.
- Access Point (AP):
  - Any entity that has STA functionality and provides access to the DS.
  - An AP is a STA which provides access to the DS by providing DS services in addition to Station Services.



802.11 Architecture Components

- STA to AP Association is Dynamic
  - The association between a station and a BSS is dynamic (STAs turn on, turn off, come within range and go out of range).
  - To become a member of an infrastructure BSS, a station must become Associated.

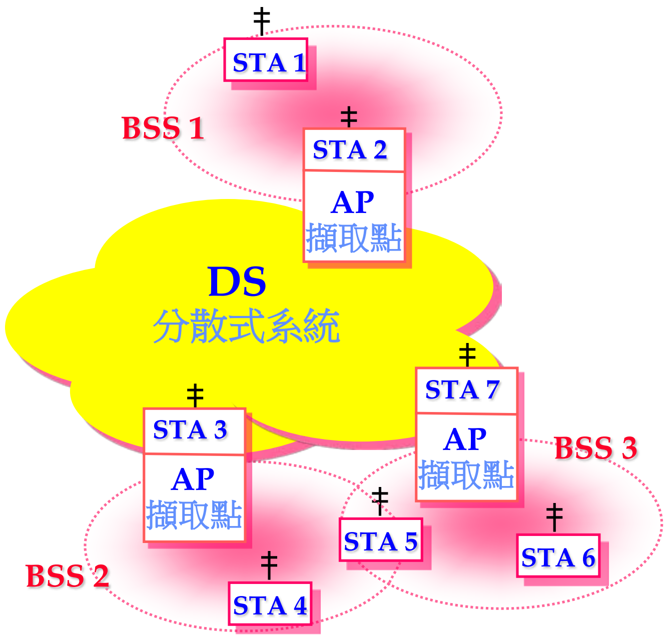
- Distributed System Concepts:
  - Extend an 802.11 network with multiple BSSs named as ESS.
  - The architecture component used to interconnect BSSs is the Distributed System.

802.11 Architecture Components

- ESS: The large coverage network
  - The DS and BSSs allow 802.11 to create a wireless network of arbitrary size and complexity.
- Extended Service Set (ESS):
  - A set of interconnected BSSs which appears as a single BSS.
  - The ESS network appears the same to an LLC layer as an independent BSS network.
  - Stations within an ESS can communicate and mobile stations may move from one BSS to another (within the same ESS) transparently to LLC.
- Basic Service Area (BSA):
  - The members of a BSS within the area can communicate.
- Extended Service Area (ESA):
  - The members of a ESS within the area can communicate.
  - An ESA is larger than or equal to a BSA.

802.11 Architecture Components

- The following are possible
  - The BSSs may partially overlap. This is commonly used to arrange contiguous coverage within a physical volume.
  - The BSSs could be physically disjoint.
  - The BSSs may be physically collocated.
- Max number of overlapping BSSs
  - 3 in DSSS 2.4GHz
  - 26 in FHSS 2.4GHz
  - 12 in OFDM 5GHz
- Question : Is it possible for a single BSS to utilizes multiple channels ?

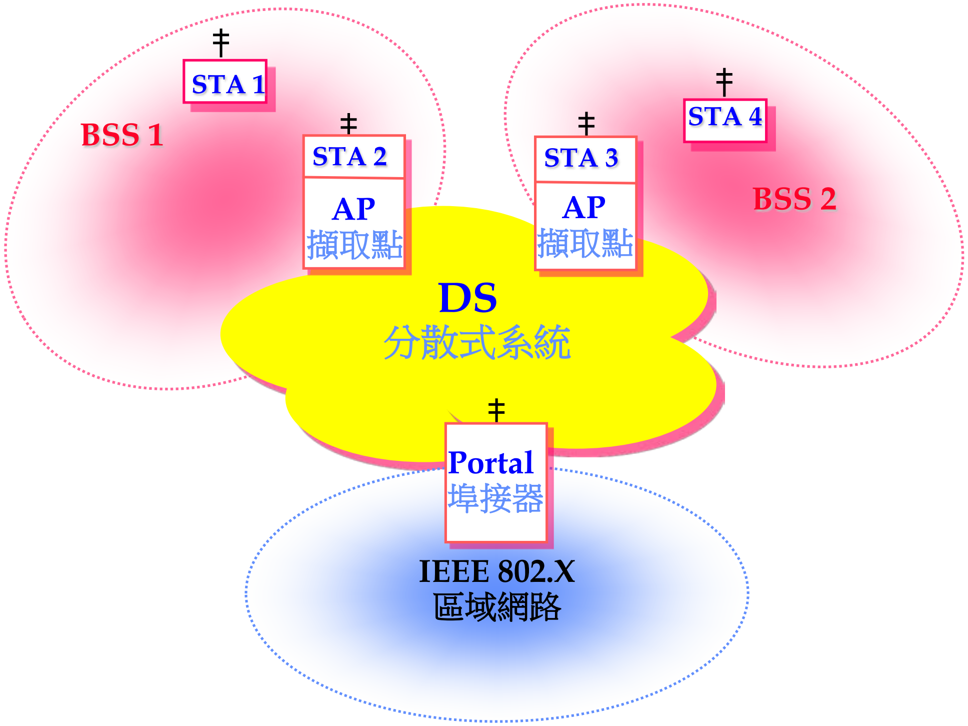


802.11 Architecture Components

- One (or more) independent BSS, or ESS networks may be physically present in the same space as one (or more) ESS networks.
    - » An ad-hoc network is operating in a location which also has an ESS network.
    - » Physically adjacent 802.11 networks have been set up by different organizations.

Integration with Wired LANs

- To integrate the 802.11 architecture with a traditional wired LAN, a logical architecture component (Portal) is introduced.
- All data from non-802.11 LANs enters the 802.11 architecture via a portal.



Portals and Bridges

- Bridges were originally designed to provide range extension between like-type MAC layers.
- In 802.11, arbitrary range (coverage) is provided by the ESS architecture (via the DS and APs) making the PHY range extension aspects of bridges unnecessary.
- Bridges are also used to interconnect MAC layers of different types. Bridging to the 802.11 architecture raises the questions of which logical medium to bridge to; the DSM or the WM ?
- The portal must also consider the dynamic membership of BSSs and the mapping of address and location required by mobility.
- Physically, a portal may, or may not, include bridging functionality depending on the physical implementation of the DS.

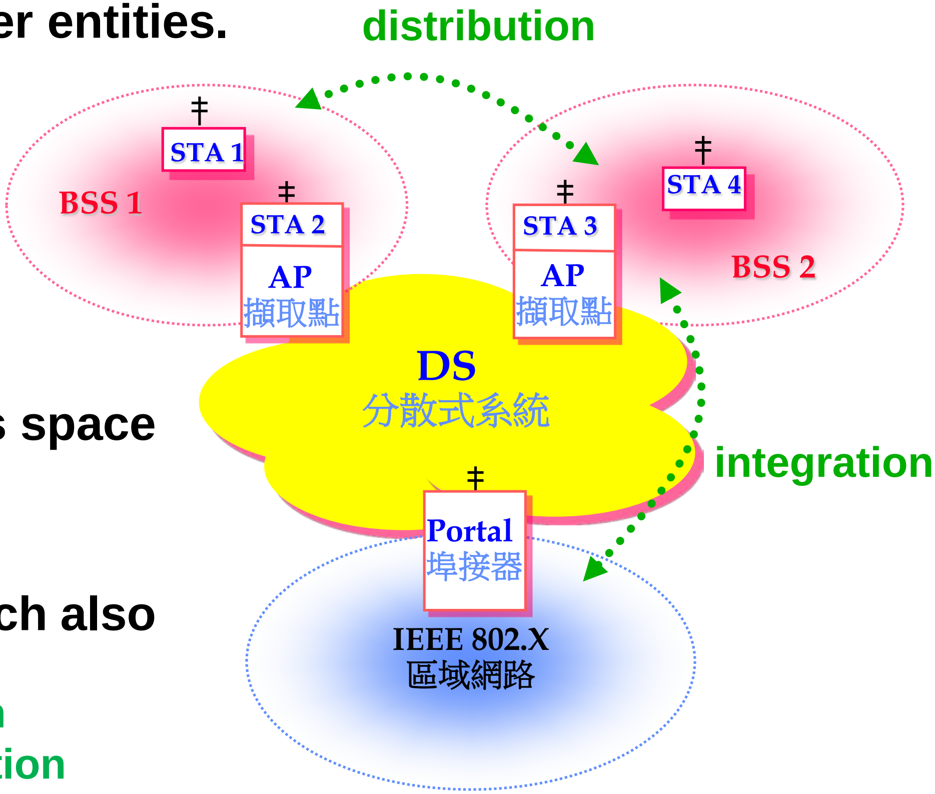
Logical Service Interface

- The DS may not be identical to an existing wired LAN and can be created from many different technologies including current 802.x wired LANs.
- 802.11 does not constrain the DS to be either Data Link or Network Layer based. Nor constrain a DS to be either centralized or distributed.
- 802.11 specifies services instead of specific DS implementations. Two categories of services are defined: Station Service (SS) and Distribution System Service (DSS).
- The complete set of 802.11 architectural services are:

1. Authentication
2. Association
3. Disassociation
4. Distribution
5. Integration
6. Reassociation
7. Deauthentication
8. Privacy
9. MSDU delivery

Logical Service Interface

- **Station Service (SS):**
  - Present in every 802.11 station, including APs.
  - Are specified for use by MAC layer entities.
  - The SS subset is:
    - » Authentication
    - » Deauthentication
    - » Privacy
    - » MSDU delivery
- **Distribution System Services**
  - Used to cross media and address space logical boundaries.
  - Provided by the DS.
  - They are accessed via a STA which also provides DSS.
  - The DSS subset is:
    - »Association
    - »Disassociation
    - »Distribution
    - »Integration
    - »Reassociation



Multiple Logical Address Spaces

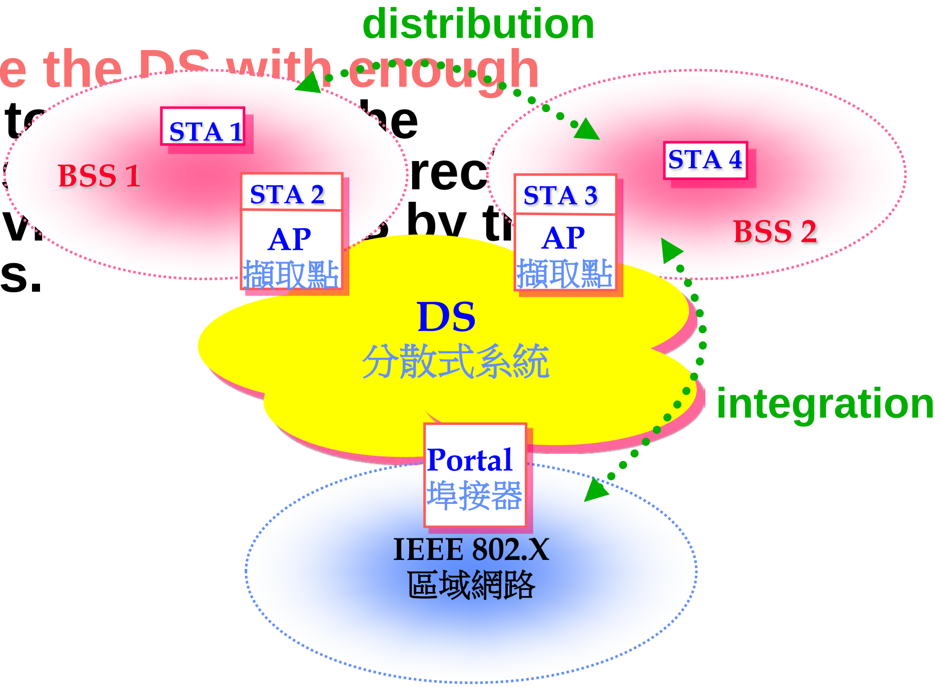
- The WM, DSM, and an integrated wired LAN may all be different physical media. Each of these components may be operating within different address spaces.
- 802.11 only uses and specifies the use of WM address space.
  - Each 802.11 PHY operates in a single medium: WM.
- 802.11 has chosen to use the IEEE 802 48-bit address space.
- A multiple address space example is one where DS uses network layer addressing. In this case the WM address space and the DS address space would be different.

Overview of the Services

- There are nine services specified by 802.11.
- Six to support MSDU delivery between stations, and three to control 802.11 access and confidentiality.
- Each of the services is supported by one or more MAC frames.
- Some of the services are supported by MAC Management messages and some by MAC Data messages.
- 802.11 MAC layer uses three types of messages:
  - Data : handled via the MAC data service path.
  - Management: handled via the MAC Management Service data path.
  - Control
- The following examples assume an ESS network environment.

Distribution of Message Within a DS

- **Distribution**:
  - The service which (by using Association information) delivers MSDUs within the DS.
- Consider a data message being sent from STA1 to STA4 via STA2 (Input AP) and STA3 (Output AP). The input AP gives the message to the Distribution Service of the DS.
- How the message is delivered within the DS is not specified by 802.11.
- All 802.11 is required is to provide the DS with enough information for the DS to be able to he "output" point which corresponds rec The necessary information is prov by th three Association related services.
  - Association
  - Reassociation
  - Disassociation



Distribution of Message Within a DS

- Integration:
  - The service which enables delivery of MSDUs between the DS and an existing network.
- If the Distribution Service determines that the intended recipient of a message is a member of an integrated LAN, the "output" point would be a Portal instead of an AP.
- Messages which are distributed to a Portal cause the DS to invoke the Integration service (conceptually in the Distribution Service).
- The Integration service is responsible for accomplishing whatever is needed to deliver a message from the DSM to the integrated LAN media, including any required media or address translation.

Distribution Services (1/4)

- The information required for the Distribution service to operate is provided by the Association services.
- Before a data message can be handled by the Distribution service, a STA must be "Associated".
- Mobility types:
  - No-transition
    - Static - no motion
    - Local movement - movement within a Basic Service Area
  - BSS-transition: movement from one BSS to another BSS within the same ESS.
  - ESS-transition: movement from one BSS in one ESS to another BSS in an independent ESS.
- Different Association services support the different categories of mobility.

Distribution Services (2/4)

- Association:
  - The service which establishes an initial Association between a station and an access point.
- Before a STA is allowed to send data frame via an AP, it must first become associated with the AP.
- At any given time, a mobile STA may be associated with no more than one AP. This ensures that the DS can determine which AP is serving a specified STA.
- An AP may be associated with many mobile STAs at one time.
- A station learns what APs are present and requests to establish an association by invoking the Association service.
- Association is always initiated by the mobile STA.
- Association is sufficient to support no-transition mobility.
- Association is necessary, but not sufficient, to support BSS-transition mobility.

Distribution Services (3/4)

- **Reassociation:**
  - The service which enables an established Association (of a STA) to be transferred from one AP to another AP (within an ESS).
- The Reassociation Service is invoked to "move" a current association from one AP to another. This keeps the DS informed of the current mapping between AP and STA as the station moves from BSS to BSS within an ESS.
- Reassociation also enables changing association attributes of an established association while the STA remains associated with the same AP.
- Reassociation is always initiated by the mobile STA.

Distribution Services (4/4)

- Disassociation:
  - The service which deletes an existing Association.
- The Disassociation Service is invoked whenever an existing Association must be terminated, and can be invoked by either party to an Association (mobile STA or AP).
- Disassociation is a notification (not a request) and can not be refused by either party to the association.
- APs might need to disassociate STAs to enable the AP to be removed from a network for service or for other reasons.
- STAs are encouraged to Disassociate whenever they leave a network.

Access and Confidentiality Control Services (1/2)

- Wired LAN design assume the closed, non-shared nature of wired media.
- The open, shared medium nature of an 802.11 LAN violates those assumptions.
- Two services are required for 802.11 to provide functionality equivalent to that which is inherent to wired LANs.
  - Authentication : used instead of the wired media physical connection.
    - » Now be further enhanced with IEEE 802.1x port-based authentication
  - Privacy : used to provide the confidential aspects of closed wired media.
    - » Now be further extended IEEE 802.11i enhanced sceurity
- Authentication:
  - The service used to establish the identity of Stations to each other.

Access and Confidentiality Control Services (2/2)

- **In a wired LAN, access to a physical connection conveys authority to connect to the LAN. This is not a valid assumption for a wireless LAN.**
- **An equivalent ability to control LAN access is provided via the Authentication service, which is used by all stations to establish their identity with stations they wish to communicate with.**
- **If a mutually acceptable level of authentication has not been established between two stations, an association shall not be established.**

Authentication Service

- **802.11 supports a general authentication ability which is sufficient to handle authentication protocols ranging from unsecured to public key cryptographic authentication schemes. (OPEN system and Shared Key)**
- **802.11 provides link level (not end-to-end or user-to-user) authentication between 802.11 stations.**
- **802.11 authentication is simply used to bring the wireless link up to the assumed physical standards of a wired link. If desired, an 802.11 network can be run without authentication.**
- **802.11 provides support for challenge/response (C/R) authentication.**
- **The three steps of a C/R exchange are:**
  - **Assertion of identity**
  - **Challenge of Assertion**
  - **Response to Challenge**

Authentication Service

- Examples of a C/R exchange are:
- An open system example:
  - (a) Assertion: I'm station 4.
  - (b) Challenge: Null.
  - (c) Response: Null.
  - (d) Result: Station becomes Authenticated.
- A password based example:
  - (a) Assertion: I'm station 4.
  - (b) Challenge: Prove your identity.
  - (c) Response: Here is my password.
  - (d) Result: If password OK, station becomes Authenticated.
- A Cryptographic challenge/response based example:
  - (a) Assertion: I'm station 4.
  - (b) Challenge: Here is some information (X) I encrypted with your public key, what is it ?
  - (c) Response: The contents of the challenge is X (only station 4's private key could have recovered the challenge contents).
  - (d) Result: OK, I believe that you are station 4.

Authentication Service

- 802.11 uses 802.10 services to perform the actual challenge and response calculations.
- A Management Information Base (MIB) function is provided to support inquires into the authentication algorithms supported by a STA.
- 802.11 requires mutually acceptable, successful, bi-directional authentication.
- A STA can be authenticated with many other STAs (and APs) at any given instant.
- The Authentication service (could be time consuming) can be invoked independently of the Association service.
- Pre-authentication is typically done by a STA while it is already associated with an AP which it previously authenticated with.
- 802.11 does not require that STAs pre-authenticate with APs.
- However, Authentication is required before an Association can be established. Thus, pre-authentication can speedup the reassociation process.