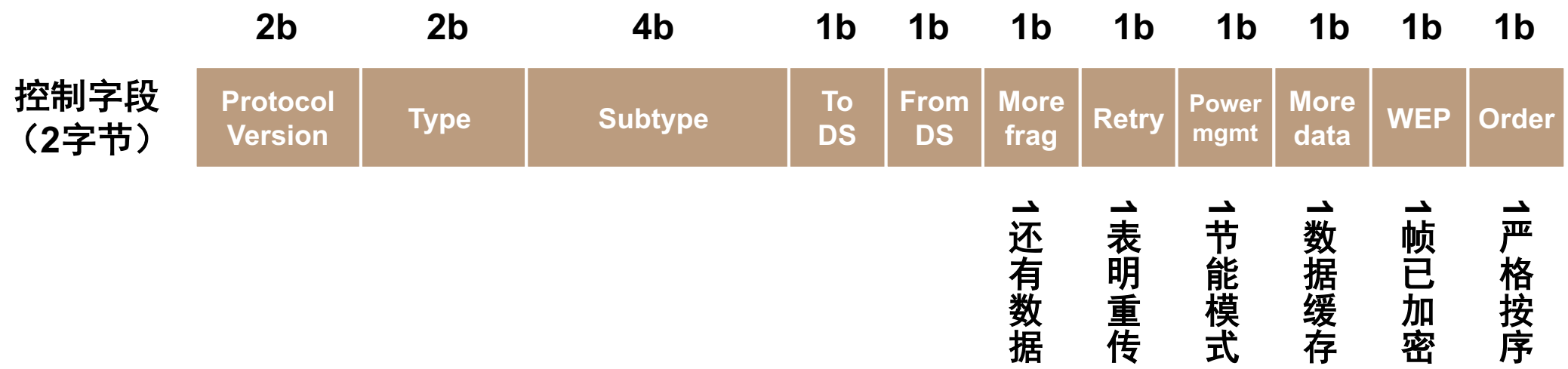
案例学习四

IEEE802.11之帧格式

IEEE802.11MAC帧结构

- **Frame control**
  两个字节的控制字段具有多种用途
- **Duration/ID**
  表示下一个发送帧可能持续的时间
- **Address 1~4**
  每个地址含义由”控制”字段的DS解释
- **Sequence control**
  序列号用来过滤掉重复帧以及分段
- **Data**
  包含任意长度的数据
- **Checksum**
  802. 11采用4个字节的校验码

IEEE802.11MAC帧控制字段



Type确定帧功能

- 管理(00)
- 控制(01)
- 数据(10)
- 保留(11)

- 802.11网卡收到一个帧首先进行CRC校验，校验正确后
- 依据TYPE字段区分帧的类型和具体帧的子类别
- 采取协议规定的动作

WEP： Wired Equivalent Privacy

IEEE 802.11MAC帧管理帧和控制帧

	2b	2b	4b	1b	1b	1b	1b	1b	1b	1b	1b
控制字段（2字节）	Version 0	Type	Subtype	To DS	From DS	More frag	Retry	Power mgmt	More data	WEP	Order

管理帧（11个,type=00）

- Association request
- Association response
- Re-association request
- Re-association response
- Dissociation
- Probe request
- Probe response
- Beacon
- Announcement traffic indication message
- Authentication
- De-authentication

- 管理帧负责移动节点与AP之间的链路建立和管理事务

- 控制帧负责与传输和能耗有关的事务

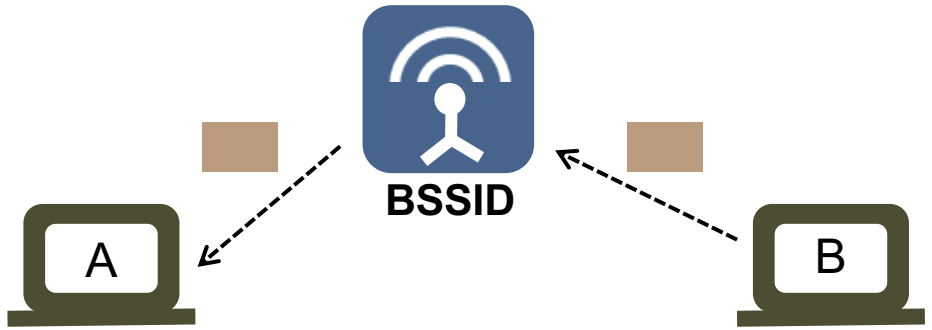
控制帧（6个,type=01）

- ACK
- RTS/CTS
- Power save-poll
- 节能模式
- CF-end
- CF-end + CF-ack

IEEE802.11MAC帧的地址字段

A通过AP接收来自B的数据帧

- fromDS=1
- SA=B的地址
- DA=A的地址
- BSSID=AP的地址



B通过AP给A发送数据帧

- toDS=1
- SA=B的地址
- DA=A的地址
- BSSID=AP的地址

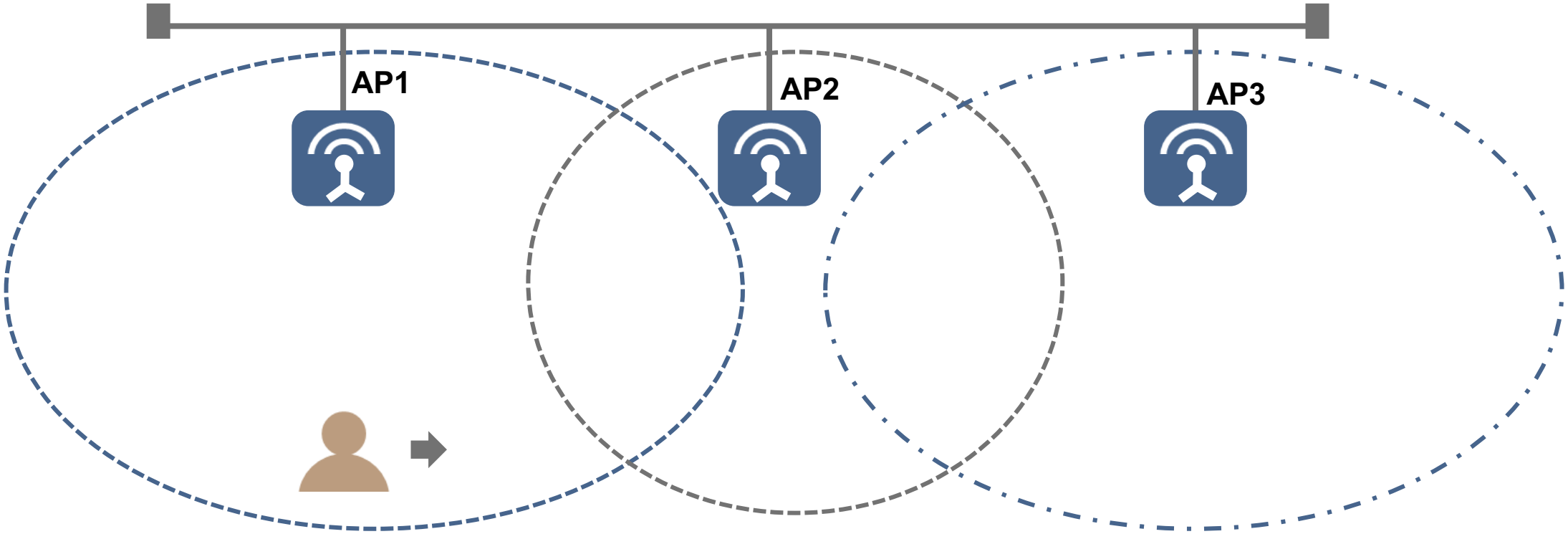
to DS	from DS	Address1 物理接收者	Address2 物理发送者	Address3 逻辑发送/接收者	Address4
0	0	DA	SA	BSSID	--
0	1	DA	BSSID	SA	--
1	0	BSSID	SA	DA	
1	1	RAP	TAP	DA	SA

物理发送者/接收者始终是AP

- 无线自组织网络
- 接收AP发来的帧
- 通过AP发送帧
- 分属两个AP下通信

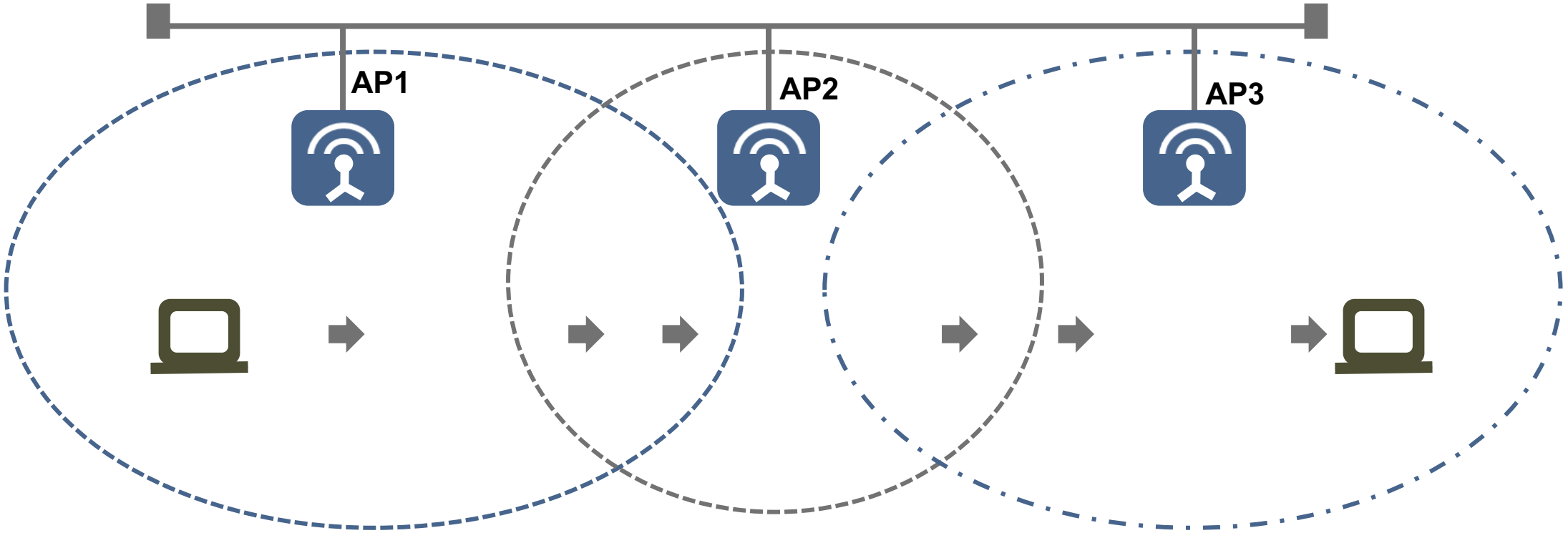
DS: Distribution System/ BSSID：Base Service Set Identification

IEEE802.11使用场景



- 每个AP周期性地在自己的工作信道上发送信标帧(Beacon)
- 相邻AP必须工作在不同的信道（以防干扰）
- 各个AP的信号覆盖区必须重叠才能为移动节点提供无缝无线接入服务

移动节点的漫游过程



t0: AP1信号最强

t1: AP1信号变弱笔记本开始扫描

t2: 发送Probe request帧

t3: 收到AP2和AP3的Probe response帧

t4: 选择信号最强的AP3

t5: 发送Reassociation request帧

t6: 收到Reassociation response帧