

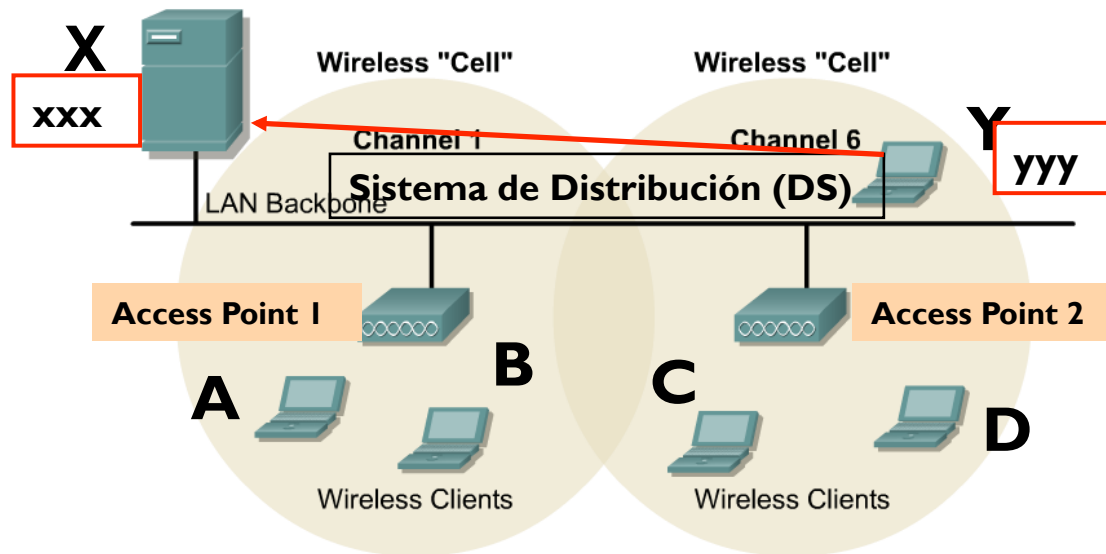
# Capa MAC del 802.11 (Continuación)

Fundamentos de Redes Inalámbricas  
ITESM CEM

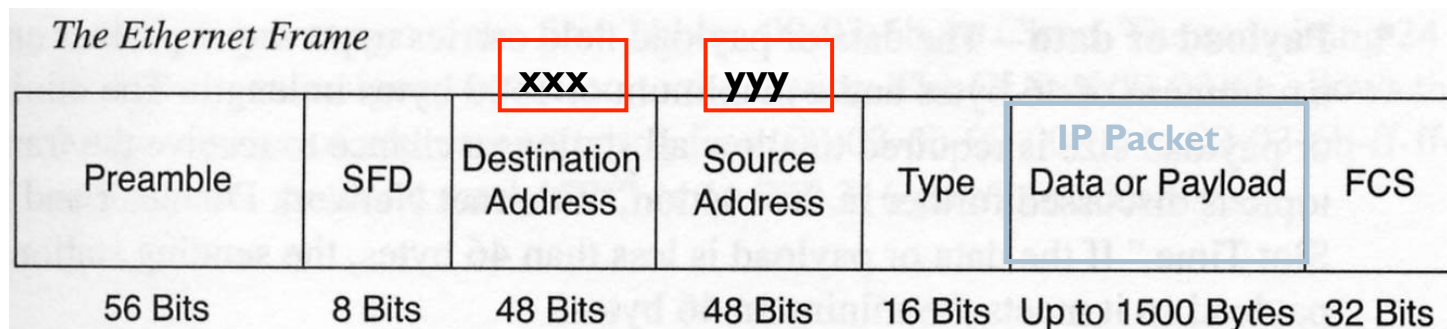


# Tramas del 802.11 y Direccionamiento

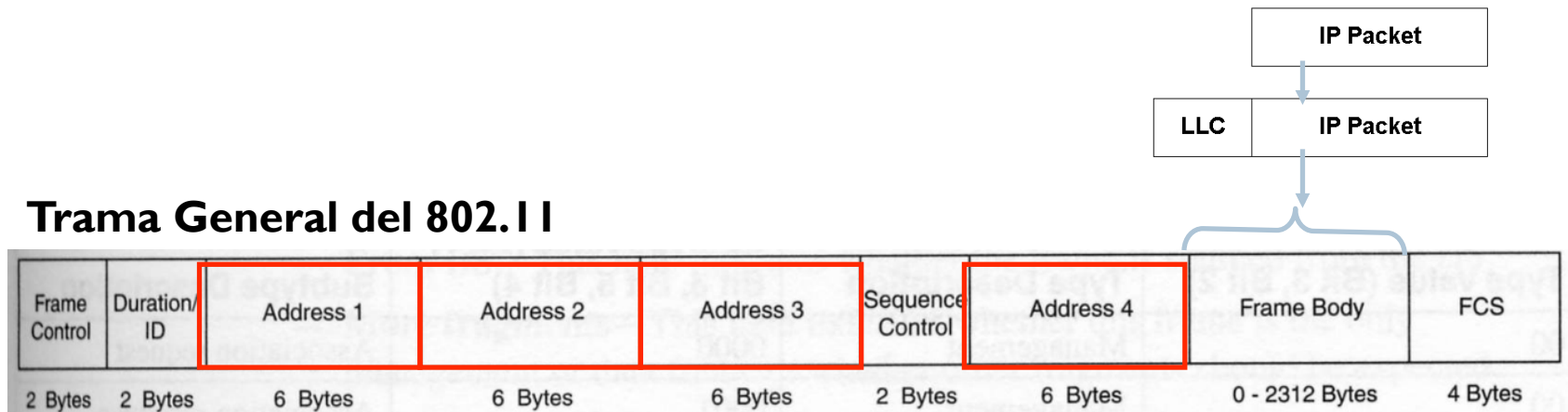
# Direccionamiento en Ethernet



**xxx** **yyy** ← Pseudo dirección MAC de nodos



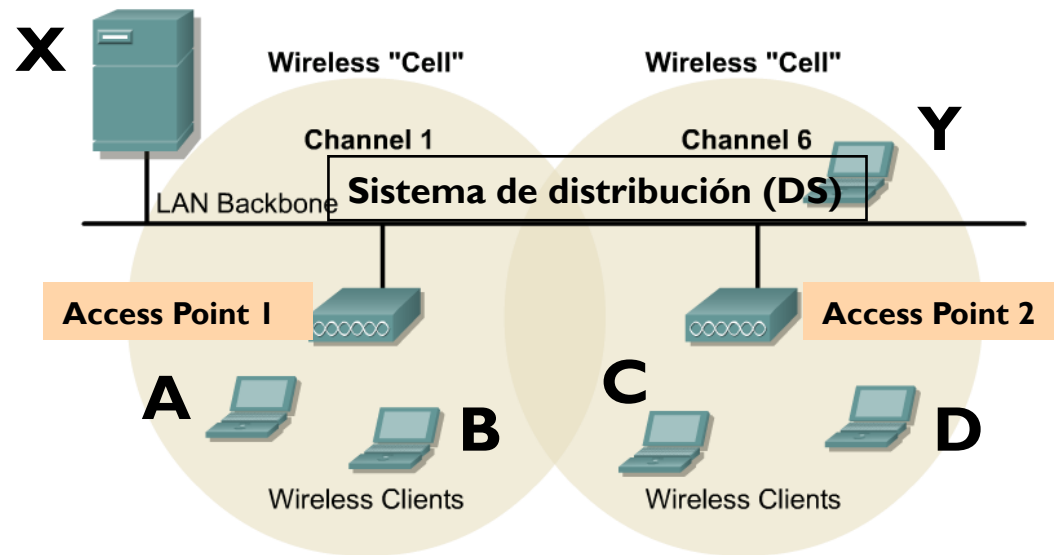
# Direccionamiento en el 802.11



- ▶ Cuatro campos de dirección.
- ▶ El número y función de los campos de dirección depende de la fuente y el destino de la trama 802.11.
- ▶ La dirección 4 es opcional y no es comúnmente utilizada a menos que se tenga un sistema de distribución inalámbrico

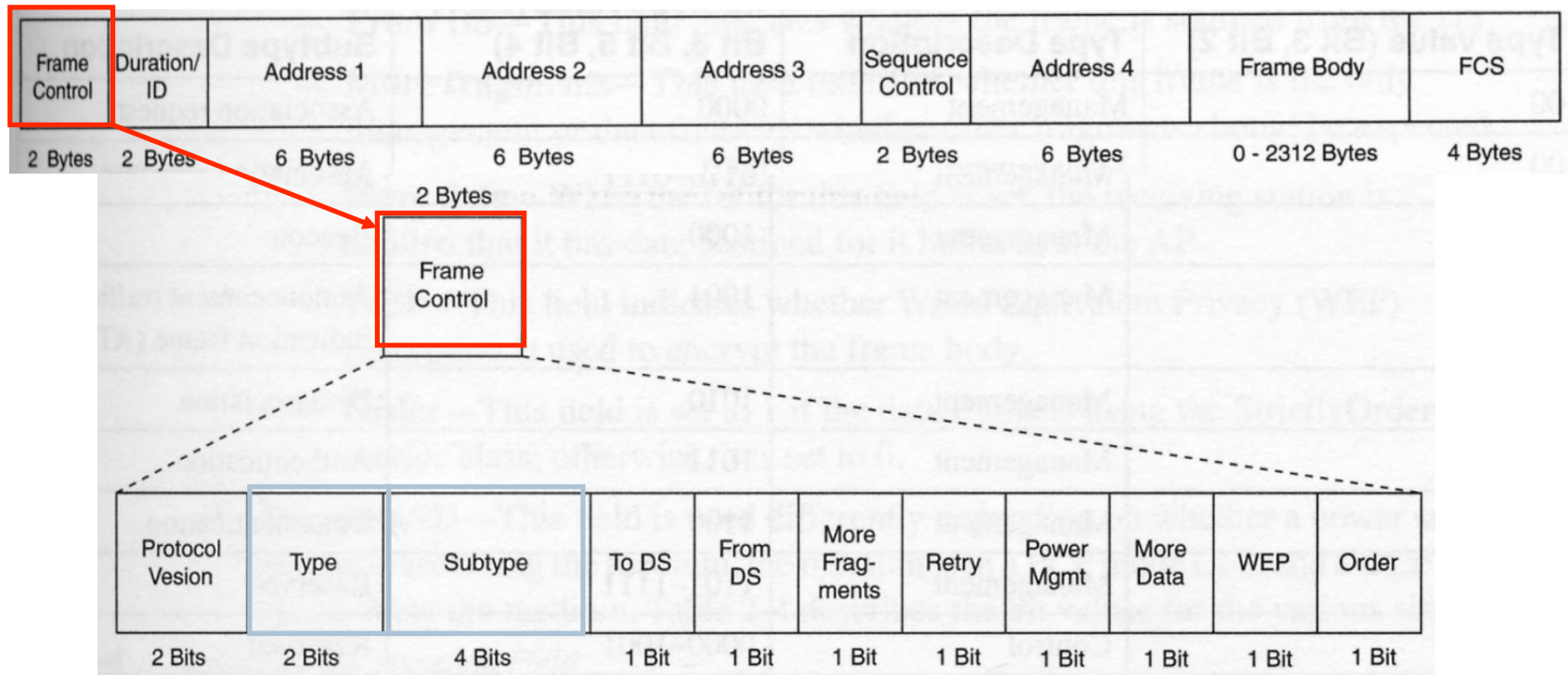


# Direcccionamiento en el 802.11



- ▶ **Sistema de distribución (DS)**
  - ▶ “Es el componente lógico del 802.11 utilizado para reenviar tramas hacia su destino. El 802.11 no especifica una tecnología en particular como sistema de distribución.” Matthew Gast
  - ▶ El DS es la red de salida desde el AP.
  - ▶ Puede ser una red alamburada (Ethernet) o una inalámbrica (puente inalámbrico) o cualquier otra cosa.

## Trama General del 802.11



# Tramas del 802.11

---

## ▶ Tramas de datos (**Type = 10**)

- ▶ Data (**Subtype = 0000**)
- ▶ Null data (**Subtype = 0100**)
- ▶ Data+CF+Ack
- ▶ Data+CF+Poll
- ▶ Data+CF+Ac+CF+Poll
- ▶ CF-Ack
- ▶ CF-Poll
- ▶ CF-Cak+CF-Poll

## ▶ Tramas de control (**Type = 01**)

- ▶ RTS (**Subtype = 1011**)
- ▶ CTS (**Subtype = 1100**)
- ▶ ACK (**Subtype = 1101**)
- ▶ CF-End
- ▶ CF-End+CF-Ack

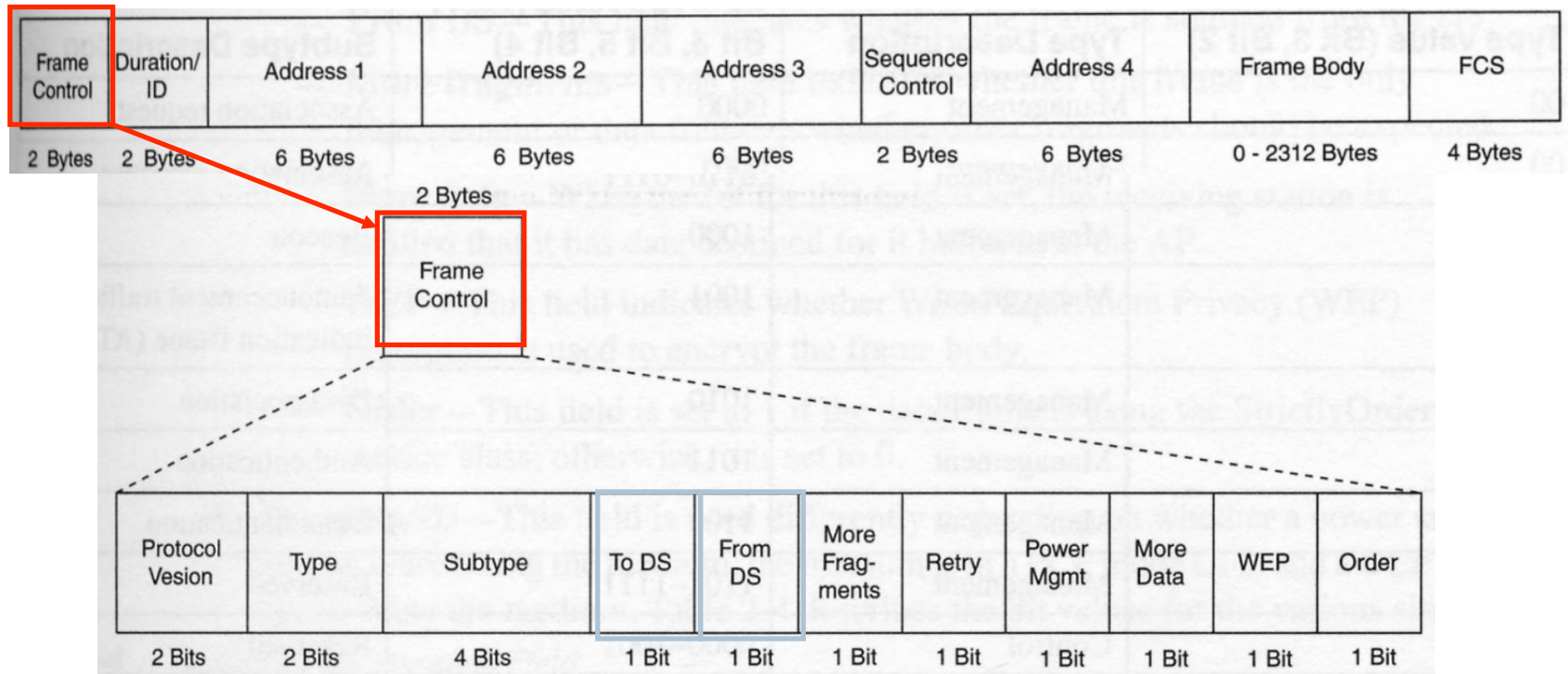
## ▶ Tramas de administración (**Type = 00**)

- ▶ Beacon (**Subtype = 1000**)
- ▶ Probe Request
- ▶ Probe Response
- ▶ Authentication (**Subtype = 1011**)
- ▶ Deauthentication (**Subtype = 1100**)
- ▶ Association Request
- ▶ Association Response
- ▶ Reassociation Request
- ▶ Reassociation Response
- ▶ Disassociation
- ▶ Announcement Traffic Indication



# Direccionamiento en el 802.11 – Campo Control

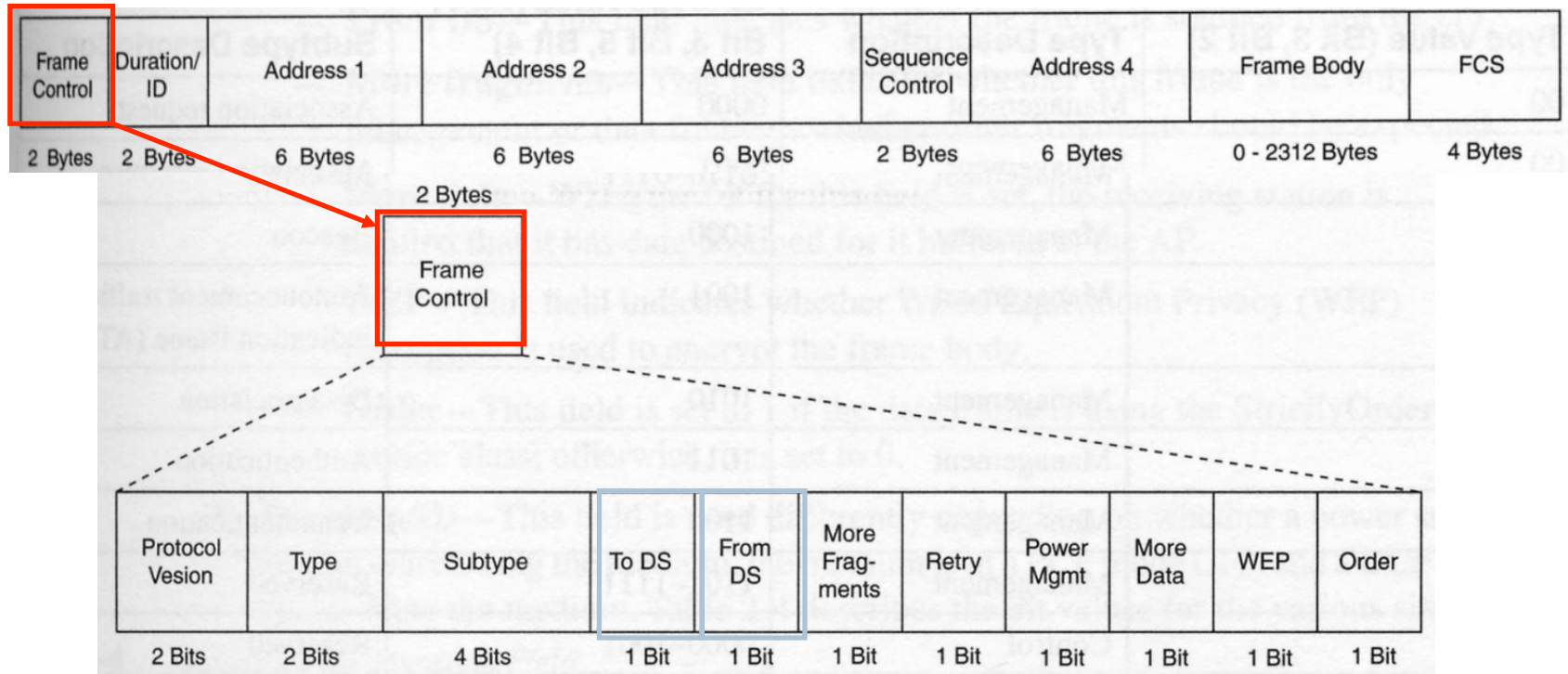
## Trama General del 802.11



- ▶ **Hacia el DS:** indica si la trama está dirigida al DS (1 bit).
- ▶ **Del DS:** indica si la trama proviene del DS (1 bit).

# Direccionamiento en el 802.11 – Campo Control

## Trama General del 802.11



### Función

IBSS o inalámbrico a inalámbrico  
 Inalámbrico a alámbrado via AP  
 Alámbrado a inalámbrico via AP  
 Alámbrado a alámbrado

### ToDS

0  
1  
0  
1

### FromDS

0  
0  
1  
1

Nos enfocaremos en estos 3.

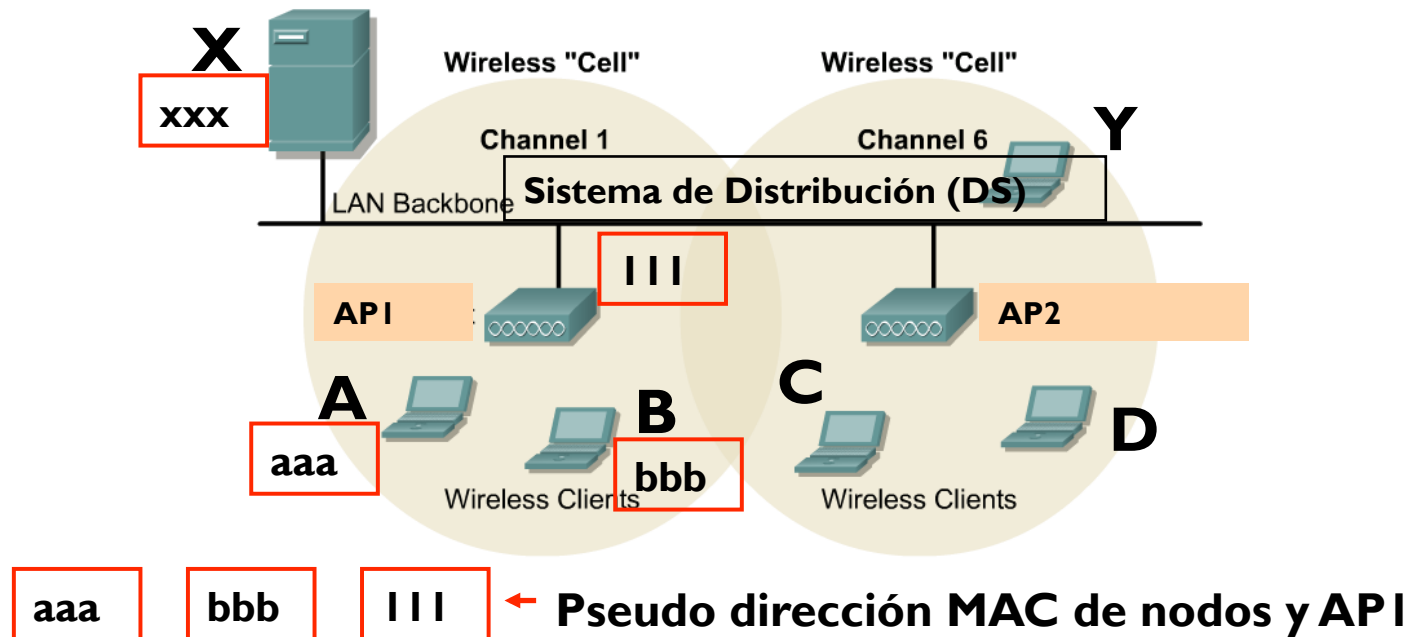
# Direccionamiento en el 802.11 – Campo Control

Frame Control	Duration/ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS
2 Bytes	2 Bytes	6 Bytes	6 Bytes	6 Bytes	2 Bytes	6 Bytes	0 - 2312 Bytes	4 Bytes

## *A Protocol Decode of the Frame Control Subfields*

```
DLC: Frame Control Field #1 = B0
DLC:      .... ..00 = 0x0 Protocol Version
DLC:      .... 00.. = 0x0 Management Frame
DLC:      1011 .... = 0xB Authentication (Subtype)
DLC: Frame Control Field #2 = 00
DLC:      .... ..0 = Not to Distribution System
DLC:      .... ..0. = Not from Distribution System
DLC:      .... .0.. = Last fragment
DLC:      .... 0... = Not retry
DLC:      ...0 .... = Active Mode
DLC:      ..0. .... = No more data
DLC:      .0.. .... = Wired Equivalent Privacy is off
DLC:      0... .... = Not ordered
```

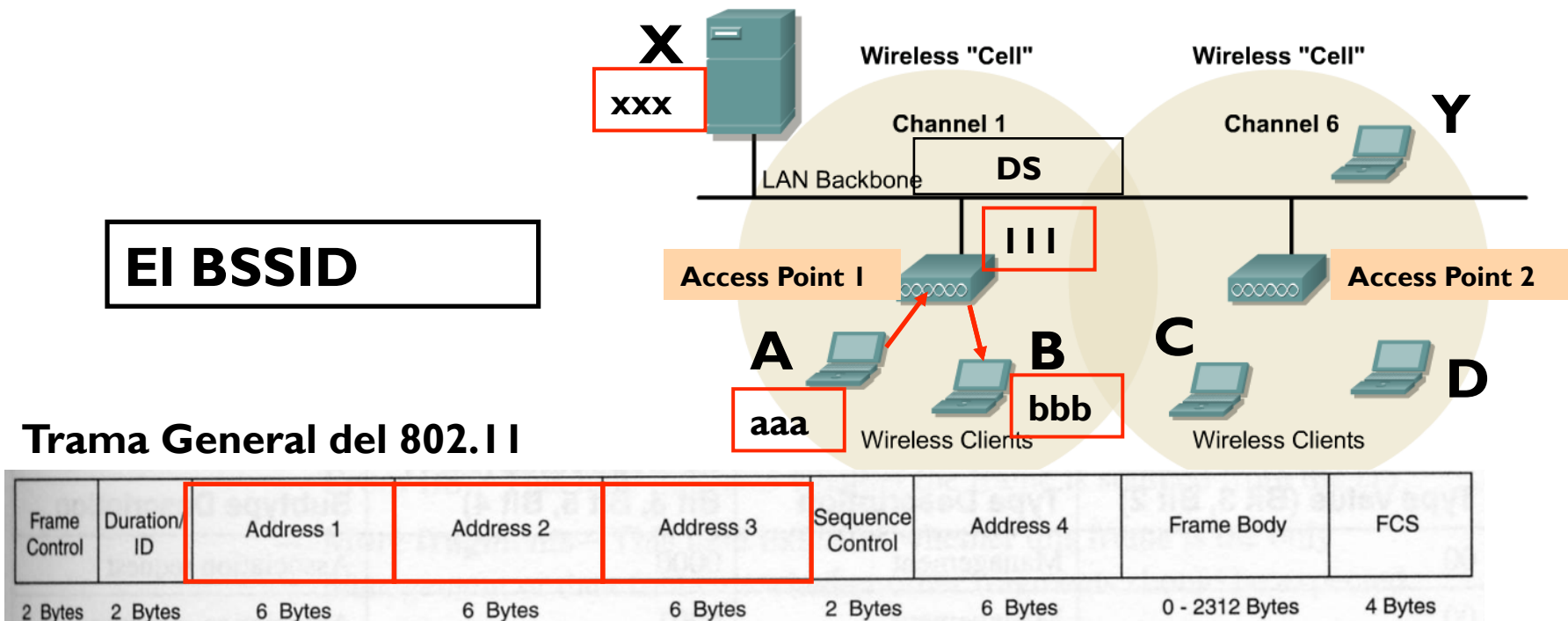
# Direccionamiento en el 802.11



- ▶ Analicemos las siguientes opciones:
  - ▶ Nodo A hacia Nodo B
  - ▶ Nodo A hacia Nodo X
  - ▶ Nodo X hacia Nodo A
- ▶ Tramas desde y hacia un BSS deben ir vía el AP.



# Direccinamiento en el 802.11



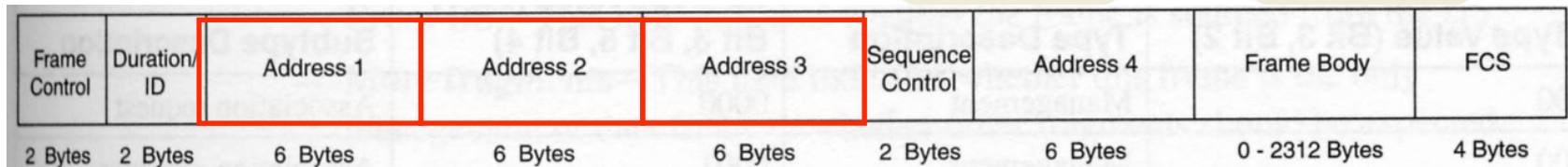
- ▶ A cada BSS se le asigna un BSSID:
  - ▶ BSSID – Identificador de 48 bits que permite distinguir al AP al cual se encuentra asociado dentro de la red.
  - ▶ Normalmente se toma la dirección MAC del AP.
  - ▶ Los APs tienen más de una dirección MAC



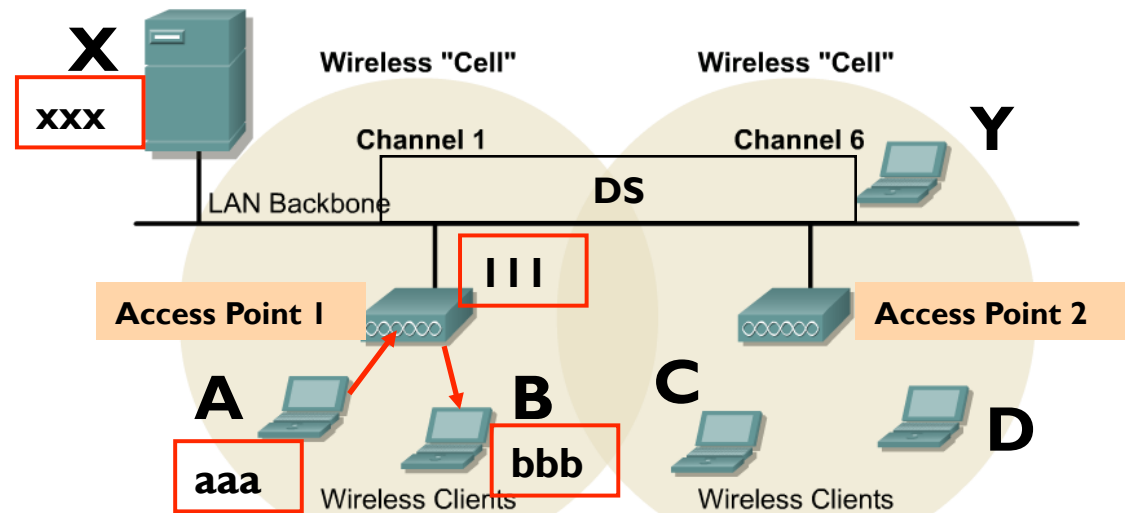
# Direccionamiento en el 802.11

**Nodo A a nodo B**

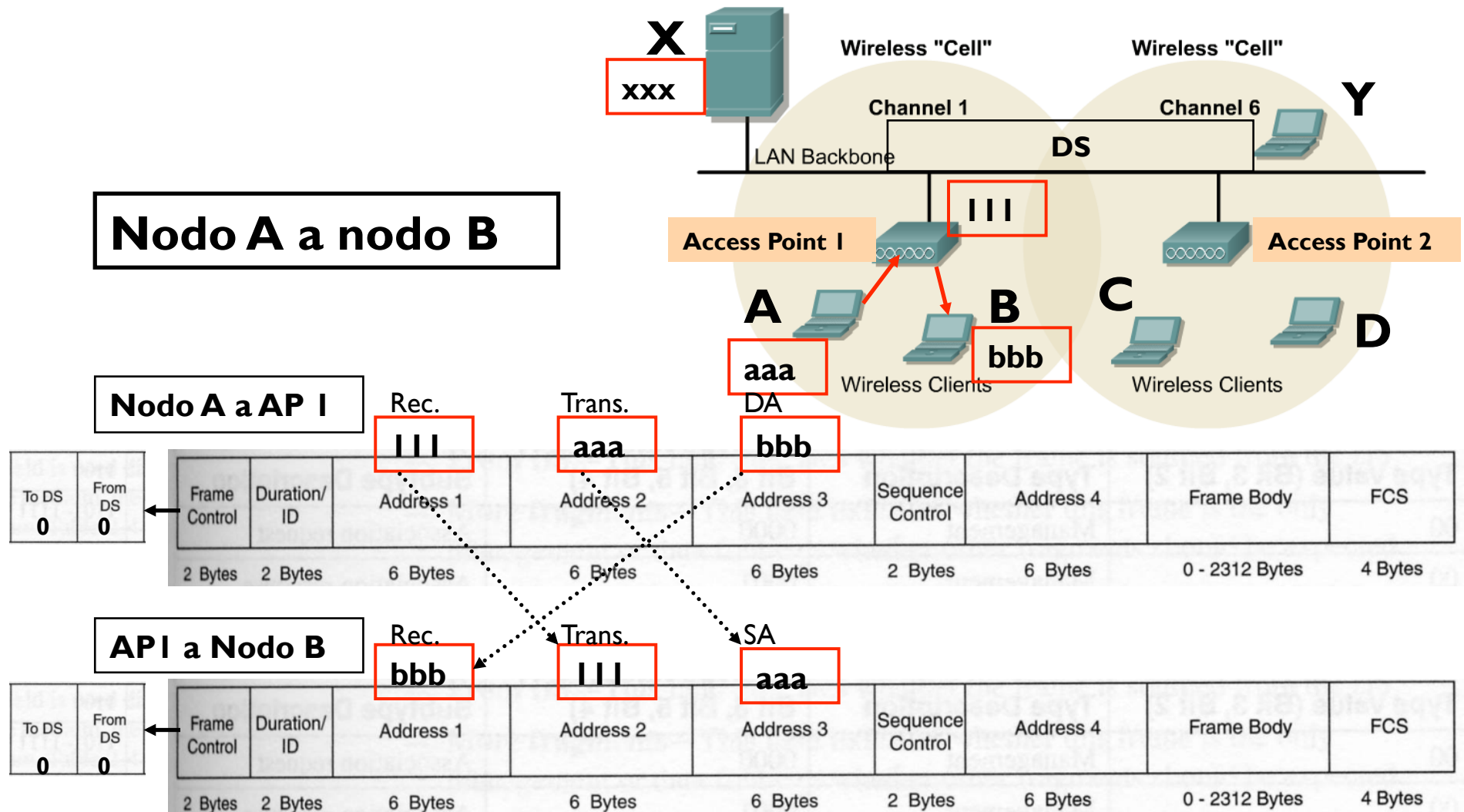
## Trama General del 802.11



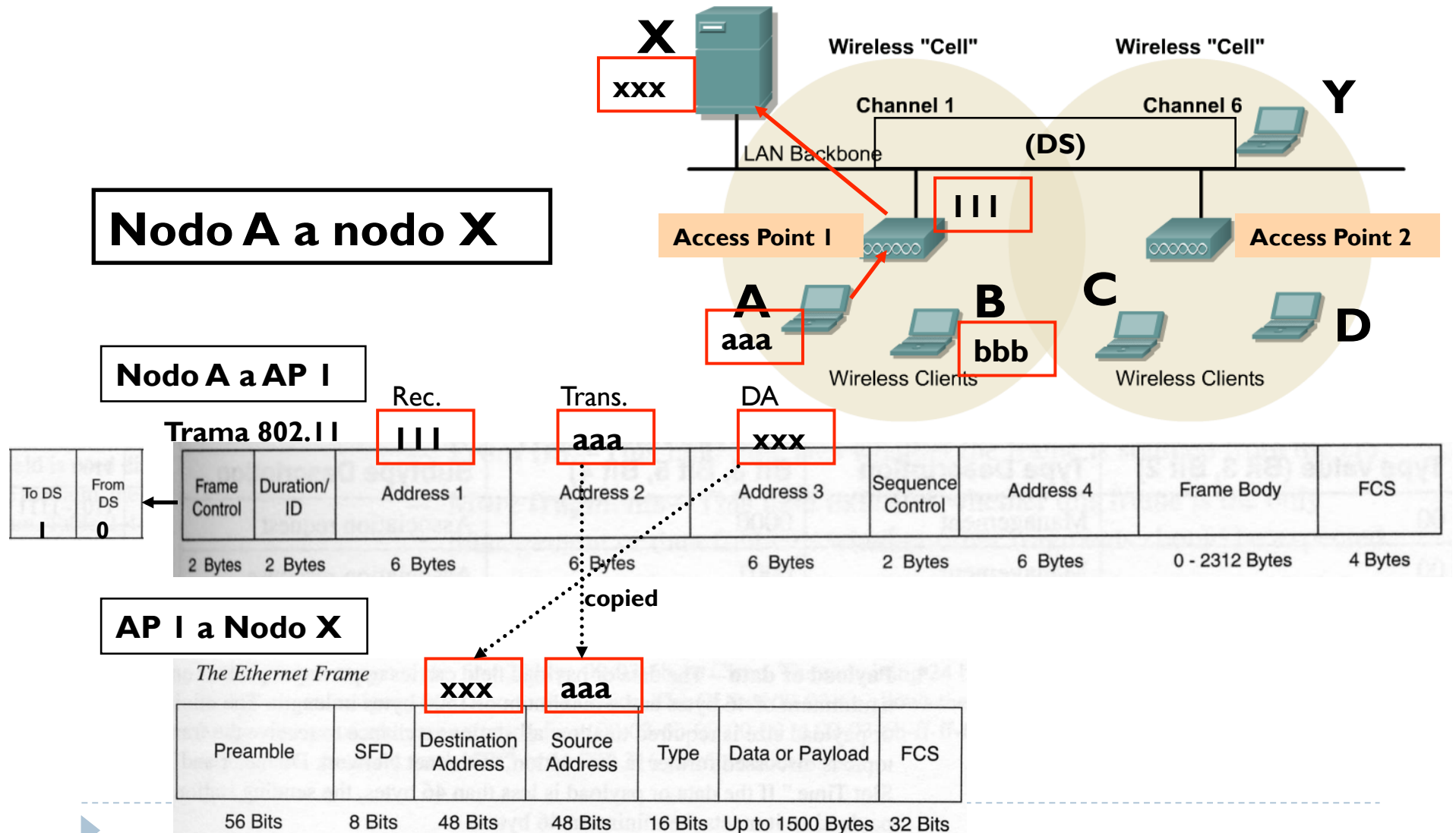
- ▶ Address 1 – Dirección del Receptor
- ▶ Address 2 – Dirección del Transmisor
- ▶ Address 3 – Dirección Fuente Ethernet, Dirección Destino Ethernet, o BSSID
- ▶ Transmisor: Envía una trama al medio inalámbrico, pero no fue necesariamente quien creó la trama.
- ▶ Receptor: Recibe una trama del medio inalámbrica, pero puede no ser el destino, sino un intermediario.



# Direccionamiento en el 802.11

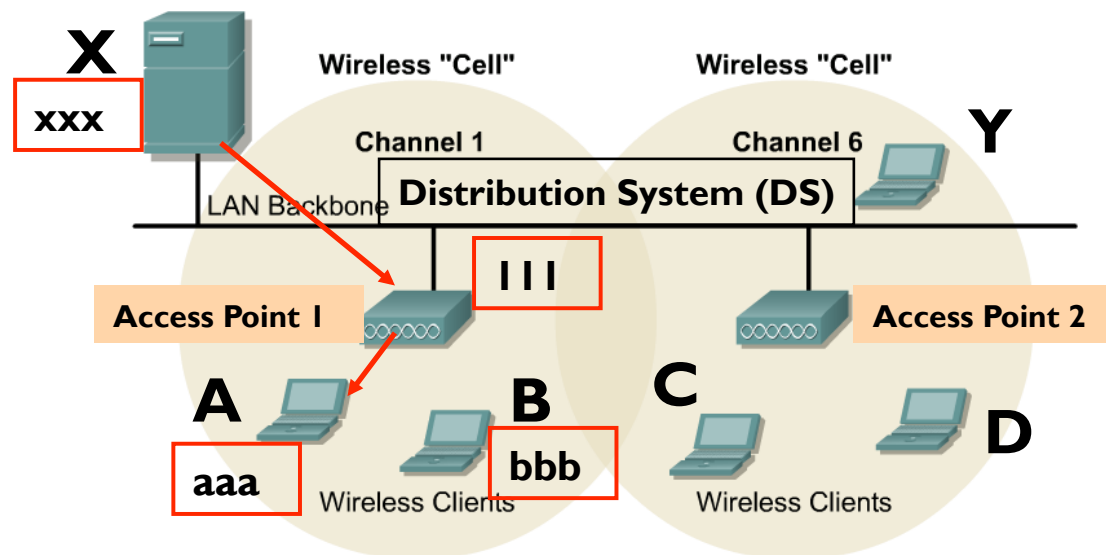


# Direccinamiento en el 802.11

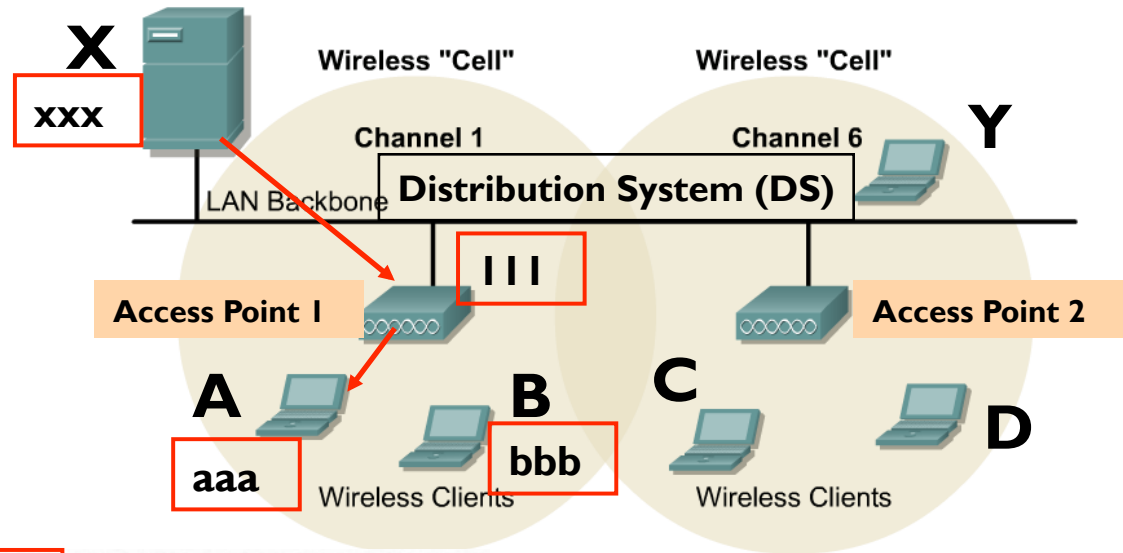


## Direccionamiento en el 802.11

### Nodo X a nodo A

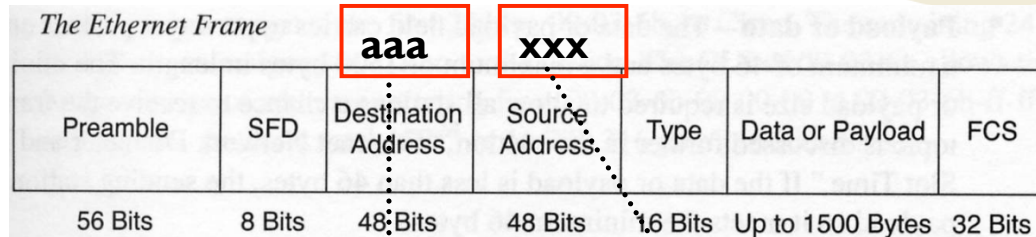


# Direccionamiento en el 802.11

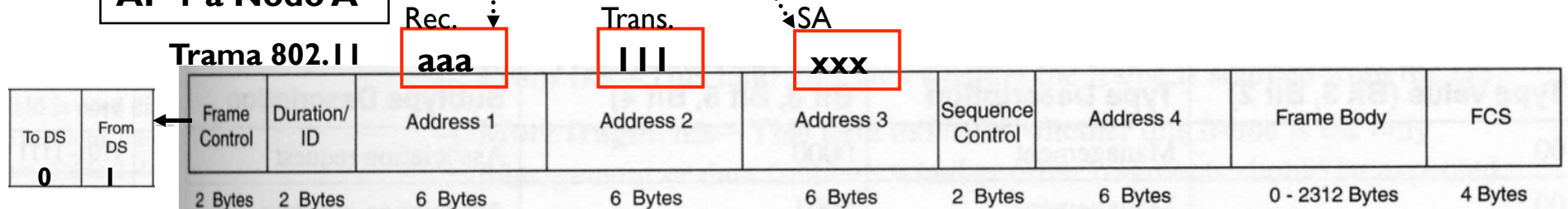


**Nodo X a Nodo A**

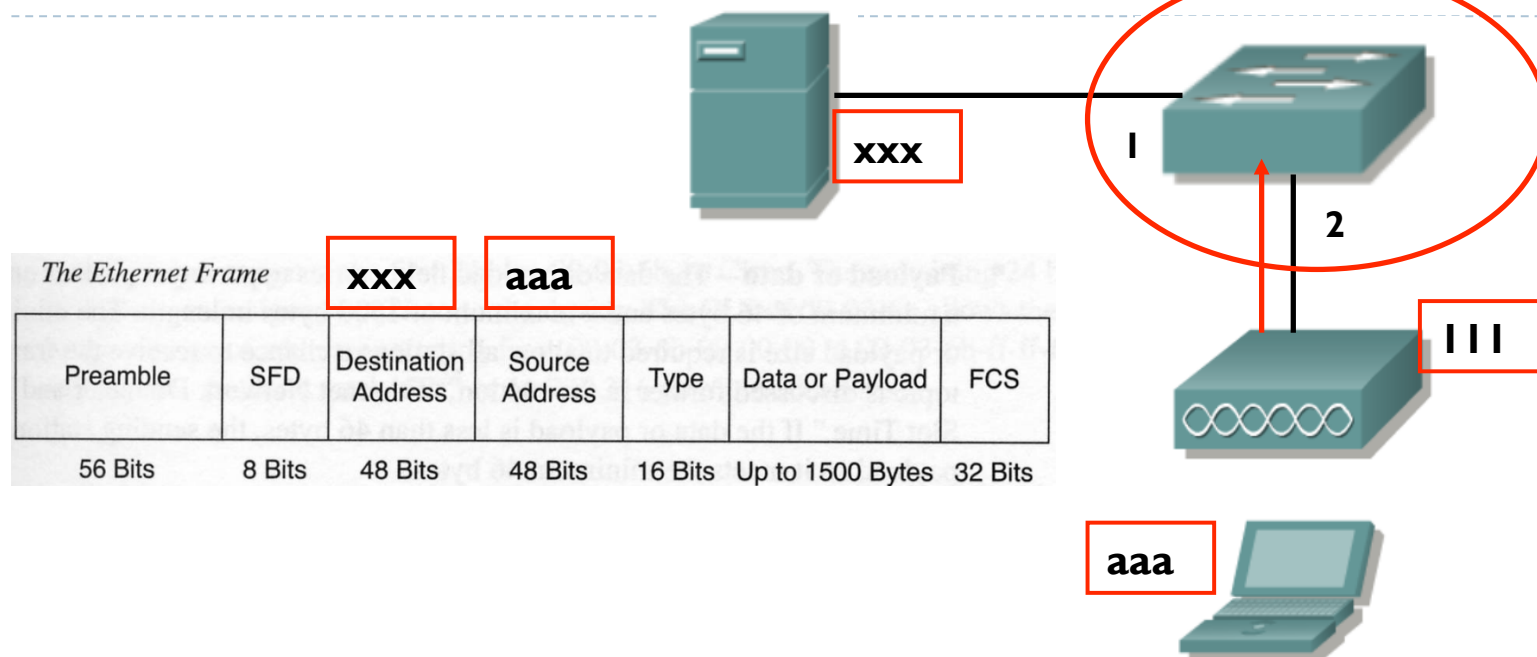
**Nodo X a AP I**



**AP I a Nodo A**



# Direccionamiento en el 802.11



- ▶ **¿Cómo saben los switches de Ethernet dónde se encuentra una estación?**
  - ▶ Para ellos es transparente la existencia de un AP
  - ▶ El switch aprende que la dirección MAC aaa se encuentra en el puerto 2 y es lo que coloca en su tabla MAC

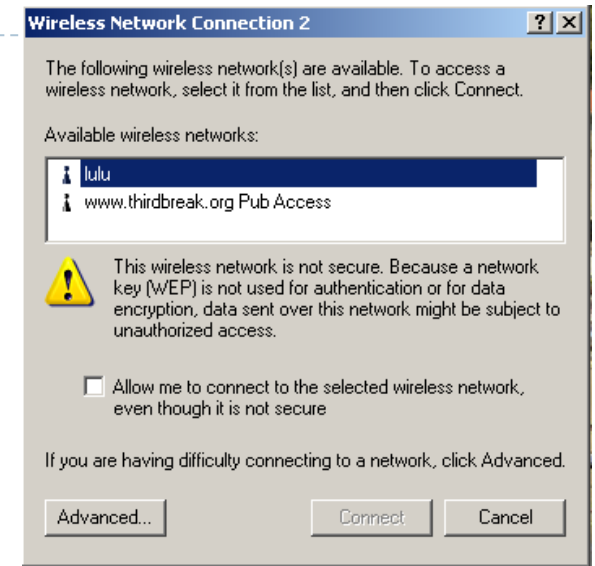
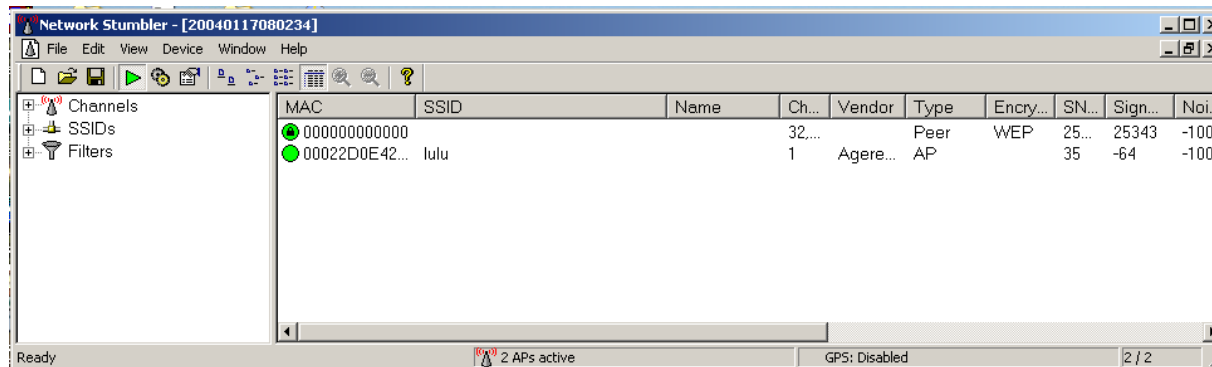
# Operaciones de la capa MAC del 802.11

## **Conectividad de la estación**

Operaciones de ahorro de energía

Formatos de las tramas 802.11

# Conectividad de la estación



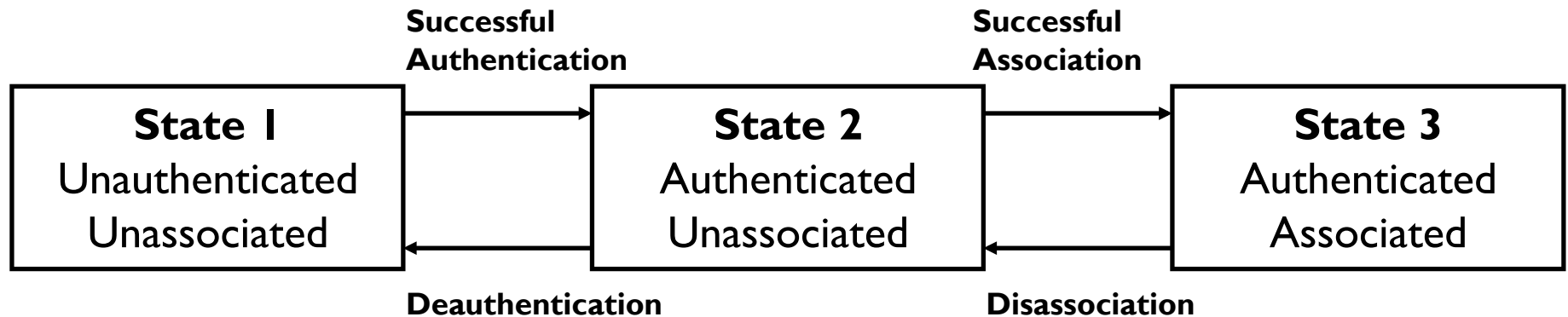
- ▶ Para que exista conectividad el AP y la estación deben mínimo compartir un SSID.
- ▶ ¿Cómo sabe el cliente sobre la existencia de los APs?
- ▶ Antes de que conectarse a una red el cliente debe descubrir dicha red.
- ▶ Vemos el proceso completo...



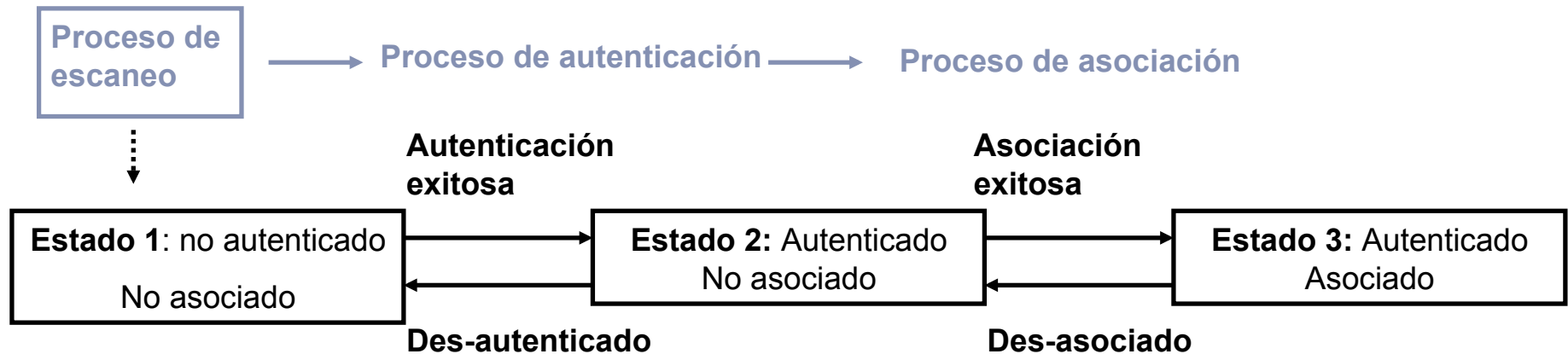


# Conectividad de la estación

---



# Conectividad de la estación



## ► Procesos:

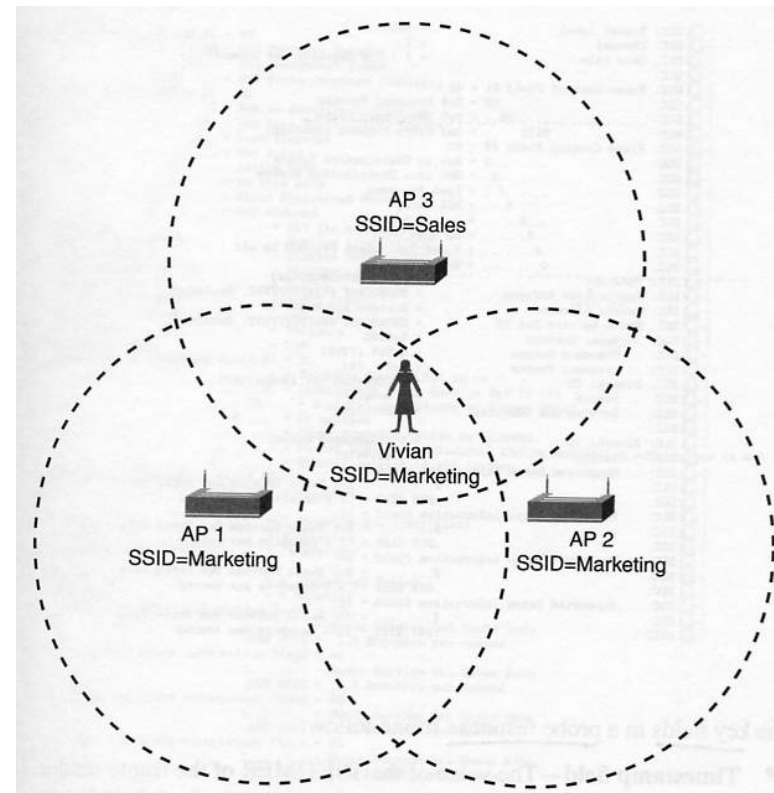
- Probe (o escanéo)
  - Authentication
  - Association
- Sólo hasta completar los 3 procesos es que se permitirá la comunicación del cliente.



# Conectividad de la estación – Probe

---

- ▶ El proceso de reconocimiento es realizado por la estación cliente
  - ▶ Pasivo - Señalizaciones
  - ▶ Activo – Peticiones *probe*
- ▶ Depende del controlador de la tarjeta inalámbrica o del software utilizado.
- ▶ Cisco utiliza escaneo activo para la conexión pero pasivo para pruebas.
- ▶ Las señalizaciones se envían y procesan aún en escaneo pasivo.



# Conectividad de la estación

- ▶ **Reconocimiento pasivo**
  - ▶ La estación se mueve en cada canal y espera tramas de señalización de un AP.
  - ▶ Registra las señalizaciones recibidas.
- ▶ Las tramas de señalización permiten a una estación conocer todo lo necesario para iniciar comunicación con el AP incluyendo:
  - ▶ SSID
  - ▶ Tasas de transmisión soportadas
- ▶ Kismet/KisMAC utiliza escaneo pasivo

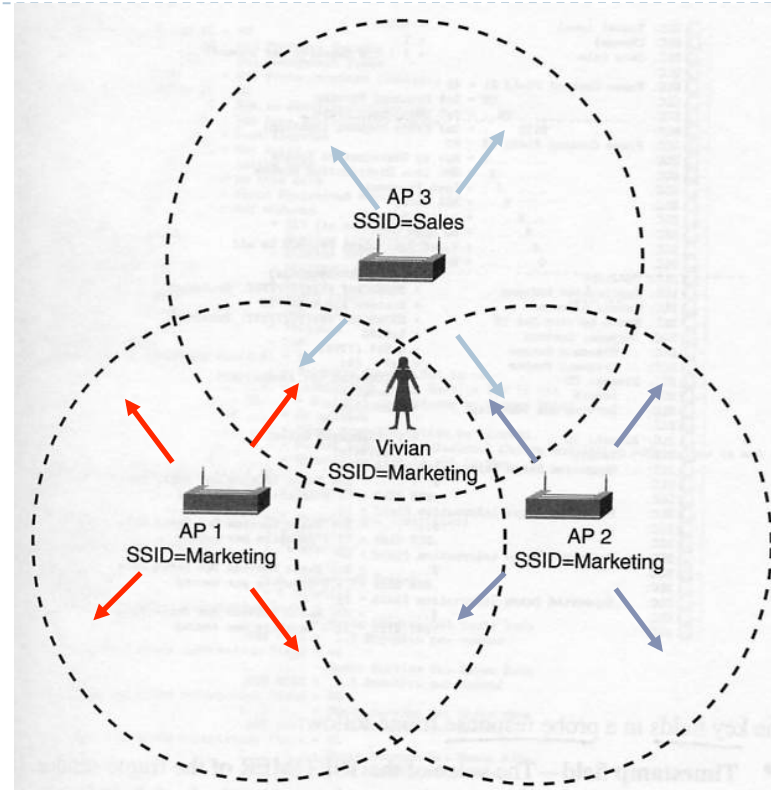


Figure 2-59 Frame Format of a Beacon Frame

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Time-stamp Field	Beacon Interval Field	Capability Information Field	SSID IE	Supported Rates IE	FH/DS Parameter Set IE	CF Parameter Set IE (Optional)	IBSS Parameter Set IE (Optional)	TIM IE (Optional)
---------------	----------	----	----	-------	------------------	------------------	-----------------------	------------------------------	---------	--------------------	------------------------	--------------------------------	----------------------------------	-------------------

# Conectividad de la estación

Figure 2-59 Frame Format of a Beacon Frame

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Time-stamp Field	Beacon Interval Field	Capability Information Field	SSID IE	Supported Rates IE	FH/DS Parameter Set IE	CF Parameter Set IE (Optional)	IBSS Parameter Set IE (Optional)	TIM IE (Optional)
---------------	----------	----	----	-------	------------------	------------------	-----------------------	------------------------------	---------	--------------------	------------------------	--------------------------------	----------------------------------	-------------------

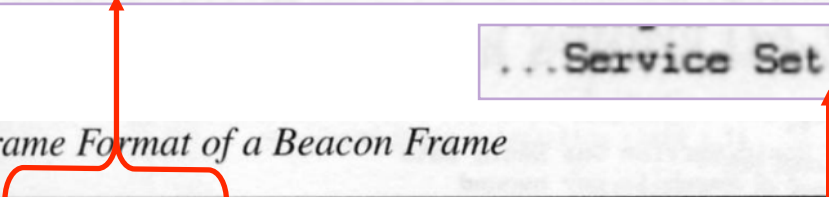
- ▶ Un **intervalo de señalización** común es de 100 unidades de tiempo.
- ▶ *Beacon interval* es el número de unidades de tiempo entre transmisiones de señalizaciones.
  - ▶ Una unidad de tiempo son 1,024 microsegundos o cerca de 1 milisegundo.
  - ▶ Un intervalo de señalización de 100 es equivalente a 100 milisegundos or 0.1 segundos.
  - ▶ Esto equivaldría a **10 señalizaciones por segundo**.

# Conectividad de la estación

Destination Address = BROADCAST FFFFFFFFFF, Broadcast  
Source Address = Station Aironet482745  
Basic Service Set ID = Aironet482745

...Service Set Identity = "powersave"

Figure 2-59 Frame Format of a Beacon Frame



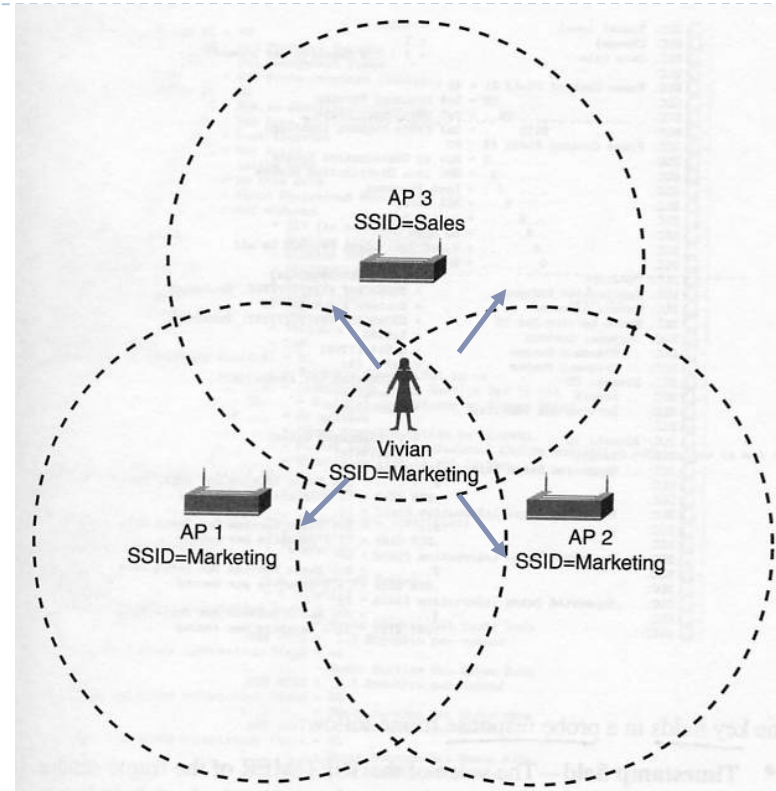
Frame Control	Duration	DA	SA	BSSID	Sequence Control	Time-stamp Field	Beacon Interval Field	Capability Information Field	SSID IE	Supported Rates IE	FH/DS Parameter Set IE	CF Parameter Set IE (Optional)	IBSS Parameter Set IE (Optional)	TIM IE (Optional)
---------------	----------	----	----	-------	------------------	------------------	-----------------------	------------------------------	---------	--------------------	------------------------	--------------------------------	----------------------------------	-------------------

## ► Características del AP (opciones)

- El SSID puede ser “escondido” o “encubierto” en la trama de señalización.
- No enviar señalizaciones del AP a nivel difusión.

# Conectividad de la estación

- ▶ **Reconocimiento activo: *Probe Request***
  - ▶ No obligatorio en el 802.11.
  - ▶ Una trama ***Probe Request*** es enviada en cada canal (1 – 11) por el cliente.
  - ▶ APs que las reciban deben responder con una trama ***Probe Response*** si:
    - ▶ El SSID coincide o
    - ▶ *Probe Request* tiene un **SSID de difusión** (0 byte SSID)
- ▶ NetStumbler utiliza reconocimiento activo



## Del cliente:

### *Frame Format of the Probe Request Frame*

Frame Control	Duration	DA	SA	BSSID	Sequence Control	SSID IE	Supported Rates IE
---------------	----------	----	----	-------	------------------	---------	--------------------



## A Protocol Decode of a Probe Request Frame

Del cliente

Dirección fuente es el cliente (nodo)

El SSID puede ser también un SSID de difusión el cual provoca un *Probe Response* de todos los APs.

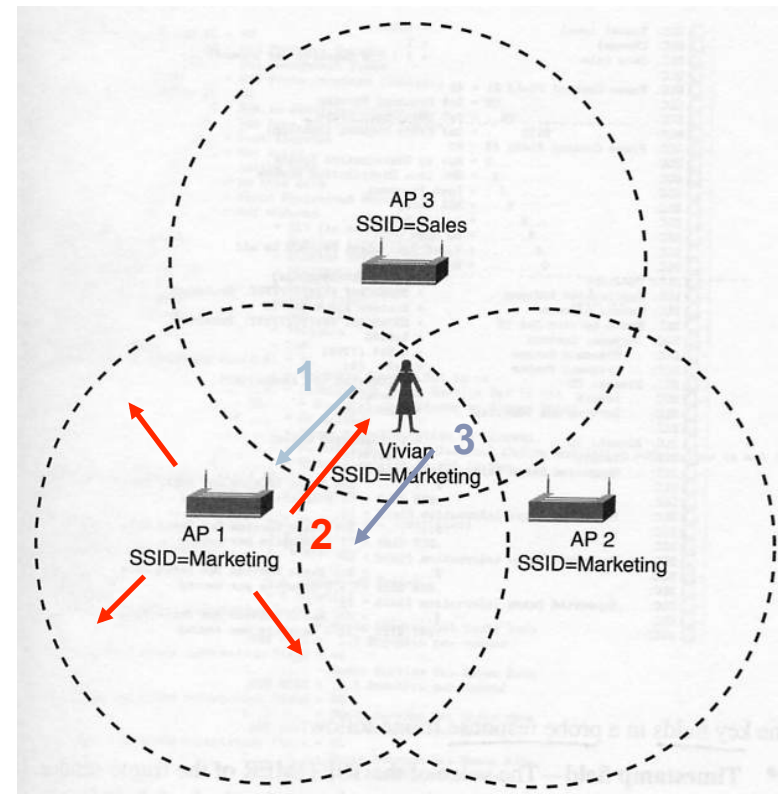
```
DLC: Signal level = 100%
DLC: Channel = 1
DLC: Data rate = 2 ( 1.0 Megabits per second)
DLC:
DLC: Frame Control Field #1 = 40
DLC:      .... 00 = 0x0 Protocol Version
DLC:      .... 00.. = 0x0 Management Frame
DLC:      0100 .... = 0x4 Probe request (Subtype)
DLC: Frame Control Field #2 = 00
DLC:      .... 0 = Not to Distribution System
DLC:      .... 0. = Not from Distribution System
DLC:      .... 0.. = Last fragment
DLC:      .... 0... = Not retry
DLC:      ...0 .... = Active Mode
DLC:      ..0. .... = No more data
DLC:      .0.. .... = Wired Equivalent Privacy is off
DLC:      0... .... = Not ordered
DLC: Duration = 0 (in microseconds)
DLC: Destination Address = BROADCAST FFFFFFFF, Broadcast
DLC: Source Address = Station Aironet502F3F
DLC: Basic Service Set ID = BROADCAST FFFFFFFF, Broadcast
DLC: Sequence Control = 0x5690
DLC:   ...Sequence Number = 0x569 (1385)
DLC:   ...Fragment Number = 0x0 (0)
DLC: Element ID = 0 (Service Set Identifier)
DLC:   ...Length = 9 octet(s)
DLC:   ...Service Set Identity = "marketing"
DLC:
DLC: Element ID = 1 (Supported Rates)
DLC:   ...Length = 4 octet(s)
DLC:   ...Supported Rates information field = 02
DLC:      0... .... = Not Basic Service Set Basic Rate
DLC:      .000 0010 = 1.0 Megabits per second
DLC:   ...Supported Rates information field = 04
DLC:      0... .... = Not Basic Service Set Basic Rate
DLC:      .000 0100 = 2.0 Megabits per second
DLC:   ...Supported Rates information field = 0B
DLC:      0... .... = Not Basic Service Set Basic Rate
DLC:      .000 1011 = 5.5 Megabits per second
DLC:   ...Supported Rates information field = 16
DLC:      0... .... = Not Basic Service Set Basic Rate
DLC:      .001 0110 = 11.0 Megabits per second
```



# Conectividad de la estación

## ► Reconocimiento Activo: *Probe Response*

- En BSSs el **AP** es responsable de responder a *Probe Requests* con ***Probe Responses***.
- ***Probe Responses*** son tramas unicast.
- ***Probe Responses*** deben ser reconocidas (ACK) por el receptor (cliente).
- Al igual que una señalización, las tramas *Probe Response* permiten a una estación el conocer todo lo necesario para iniciar comunicación con el AP incluyendo:
  - SSID
  - Tasas de transmisión soportadas



## Del AP

Figure 2-63 Frame Format of the Probe Response Frame

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Time-stamp Field	Beacon Interval Field	Capability Information Field	SSID IE	Supported Rates IE	FH/DS Parameter Set IE	CF Parameter Set IE (Optional)	IBSS Parameter Set IE (Optional)
---------------	----------	----	----	-------	------------------	------------------	-----------------------	------------------------------	---------	--------------------	------------------------	--------------------------------	----------------------------------

Figure 2-64 A Protocol Decode of the Probe Response Frame

## Del AP

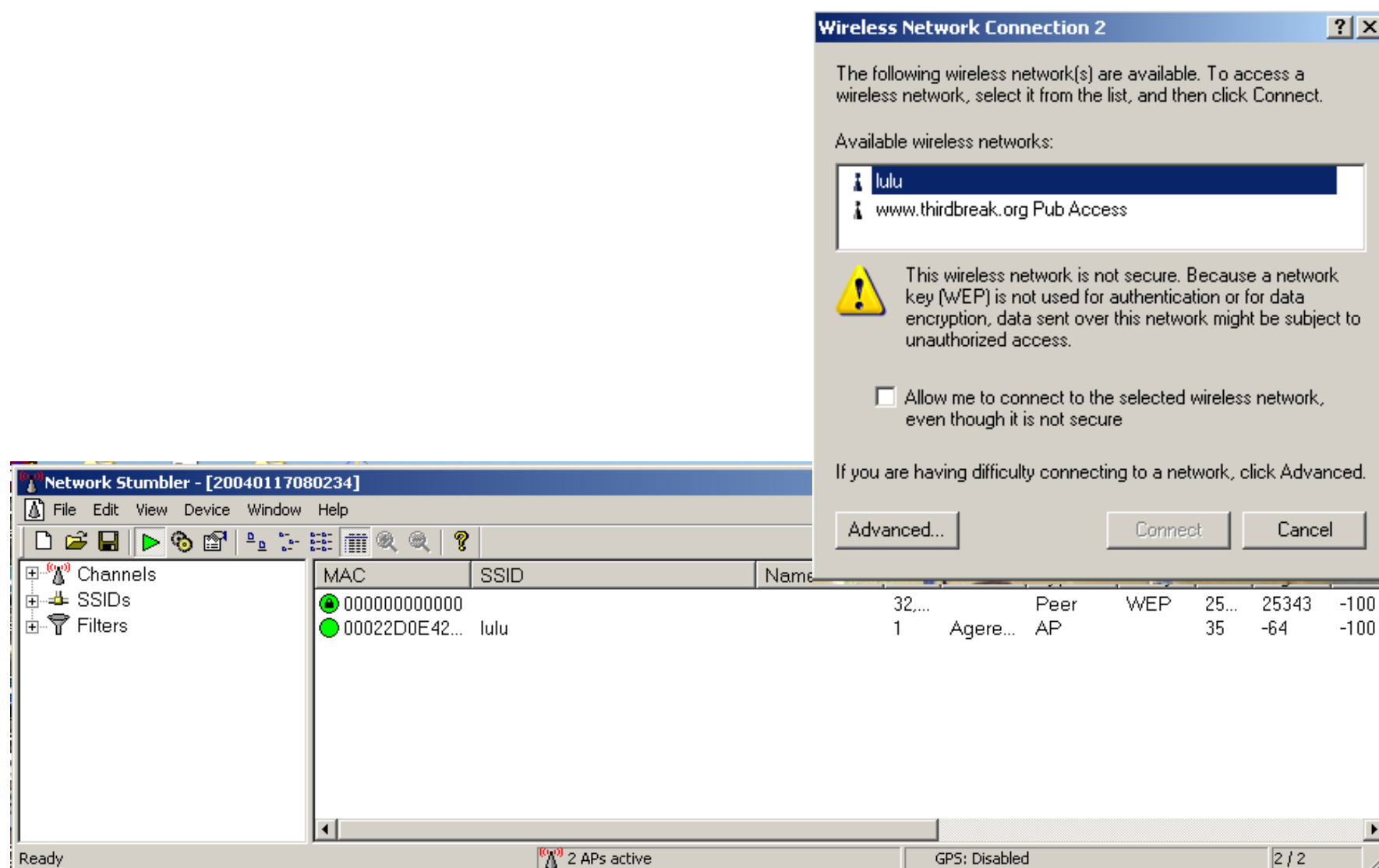
Dirección Destino es el cliente que envió el *Probe Request*

Dirección Fuente es el AP (BSSID)

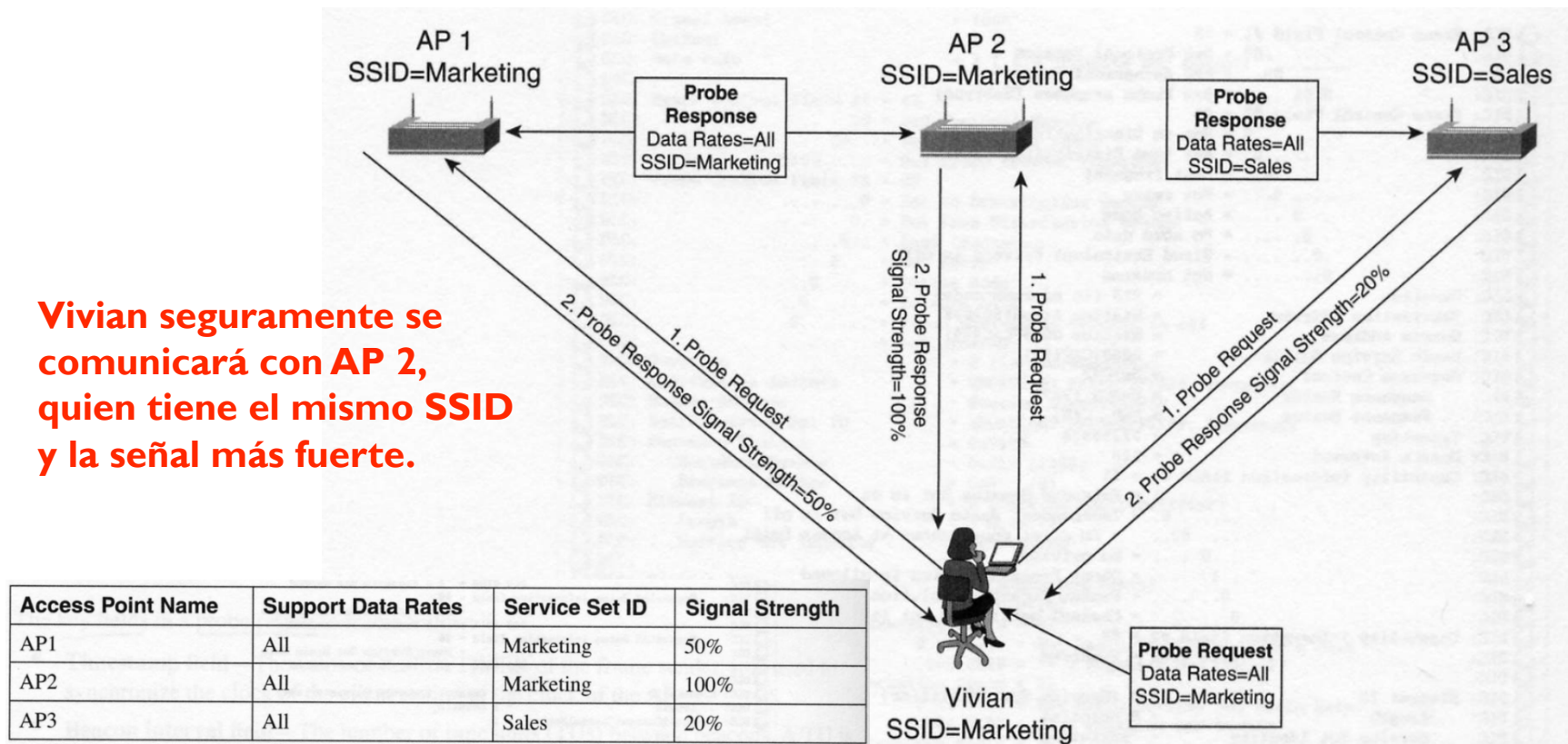
- La señalización contiene información que permite a la estación continuar su intento de unirse a la red:
  - SSID
  - Tasas de red soportadas
  - Privacidad:
    - WEP
    - Ninguna (open)

```
DLC: Frame Control Field #1 = 50
DLC:      .... ..00 = 0x0 Protocol Version
DLC:      .... 00.. = 0x0 Management Frame
DLC:      0101 .... = 0x5 Probe response (Subtype)
DLC: Frame Control Field #2 = 00
DLC:      .... ..0 = Not to Distribution System
DLC:      .... ..0 = Not from Distribution System
DLC:      .... ..0 = Last fragment
DLC:      .... 0... = Not retry
DLC:      .... ..0 = Active Mode
DLC:      .... ..0 = No more data
DLC:      .... ..0 = Wired Equivalent Privacy is off
DLC:      0... .... = Not ordered
DLC: Duration = 213 (in microseconds)
DLC: Destination Address = Station Aironet502F3F
DLC: Source Address = Station 00097CAC4391
DLC: Basic Service Set ID = 00097CAC4391
DLC: Sequence Control = 0x2C30
DLC: ... Sequence Number = 0x2C3 (707)
DLC: ... Fragment Number = 0x0 (0)
DLC: Timestamp = 72298844
DLC: Beacon Interval = 100
DLC: Capability information field #1 = 21
DLC:      .... ..1 = Extended Service Set is on
DLC:      .... ..0 = Independent Basic Service Set is off
DLC:      .... ..0 = No point coordinator at Access Point
DLC:      .... ..0 = No privacy
DLC:      .... ..1 = Short Preamble option is allowed
DLC:      .... ..0 = Packet Binary Convolutional Coding Modu
DLC:      .... 0... = Channel agility is not in use
DLC: Capability information field #2 = 00
DLC:      0000 0000 = Reserved
DLC: Element ID = 0 (Service Set Identifier)
DLC:      Length = 2 octet(s)
DLC: ... Service Set Identity = "marketing"
DLC: Element ID = 1 (Supported Rates)
DLC:      Length = 4 octet(s)
DLC: ... Supported Rates information field = 82
DLC:      1... .... = Basic Service Set Basic Rate
DLC:      .000 0010 = 1.0 Megabits per second
DLC: ... Supported Rates information field = 84
DLC:      1... .... = Basic Service Set Basic Rate
DLC:      .000 0100 = 2.0 Megabits per second
DLC: ... Supported Rates information field = 8B
DLC:      1... .... = Basic Service Set Basic Rate
DLC:      .000 1011 = 5.5 Megabits per second
DLC: ... Supported Rates information field = 96
DLC:      1... .... = Basic Service Set Basic Rate
DLC:      .001 0110 = 11.0 Megabits per second
DLC: Element ID = 3 (Direct Sequence Parameter set)
DLC:      Length = 1 octet(s)
DLC: ... dot11CurrentChannelNumber = 1
```

# Capturando el *Probe Request*

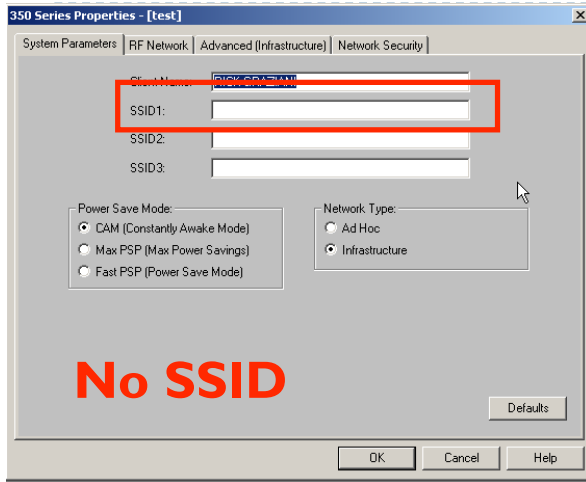


**Vivian seguramente se comunicará con AP 2, quien tiene el mismo SSID y la señal más fuerte.**



- ▶ **802.11 no define cómo una estación elige a un AP.**
- ▶ El fabricante se encarga de ello.
- ▶ Puede ser, Mismos SSIDs, Fuerza de la señal, Tasas de transmisión soportadas.

# Conectividad de la estación



¡No hice nada y ya estoy en Internet!



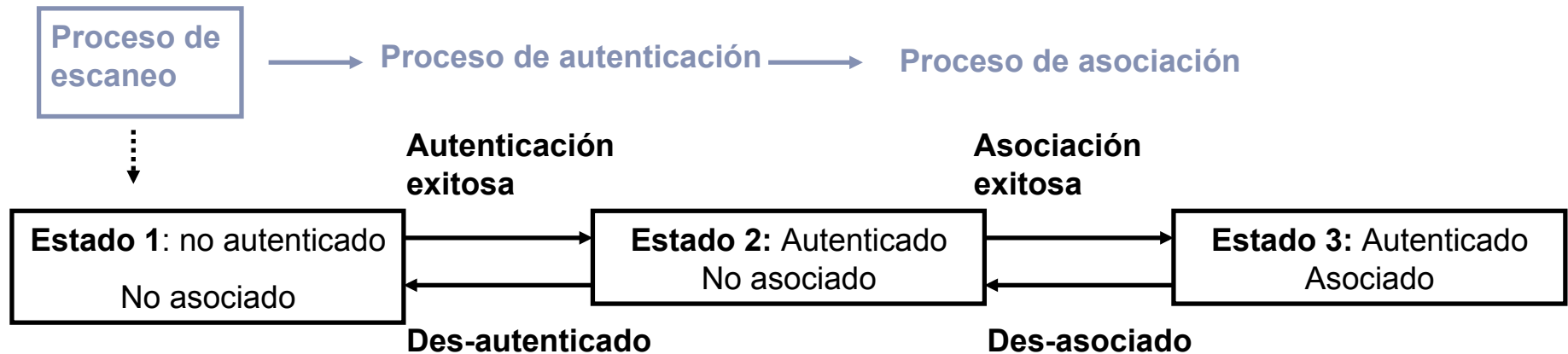
Probe Request →  
Broadcast (no) SSID  
ACK →

Probe Response  
SSID = tsunami

- ▶ APs pueden ser configurados para permitir o no clientes con SSID.
- ▶ Cisco usa el SSID tsunami como predeterminado y en modo “guest”



# Conectividad de la estación



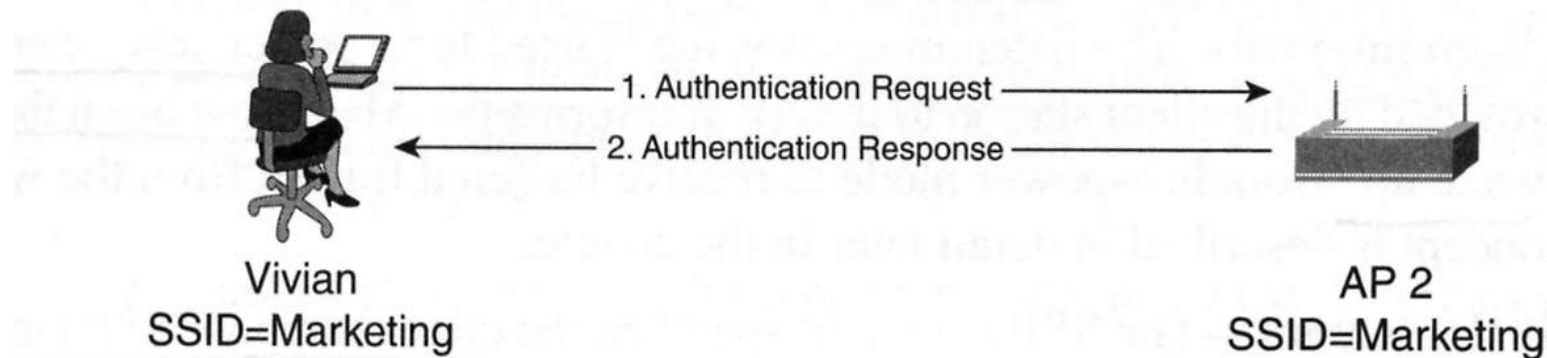
## ► Procesos:

- Probe (o escanéo)
  - **Authentication**
  - Association
- Sólo hasta completar los 3 procesos es que se permitirá la comunicación del cliente.



# Proceso de autenticación

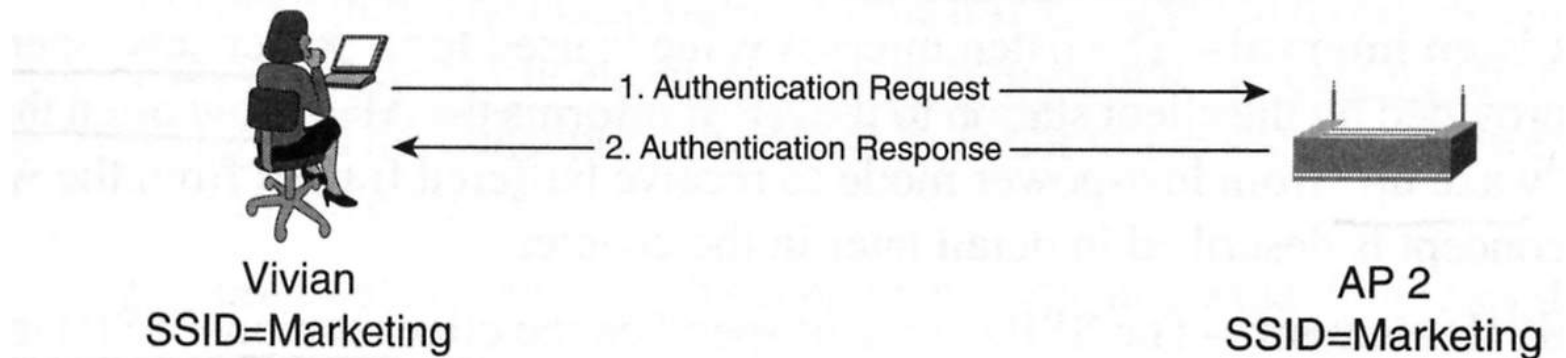
## *The Authentication Process*



- ▶ En una red alambrada, la autenticación es implícitamente proveída por el cable físico de una PC hacia el switch
- ▶ Autenticación es el proceso de asegurar que las estaciones intentando asociarse con la red (AP) están autorizadas a hacerlo.
- ▶ 802.11 especifica dos tipos de autenticación:
  - ▶ Open-system
  - ▶ Shared-key (utiliza WEP)

# Proceso de autenticación – Sistema abierto

## *The Authentication Process*



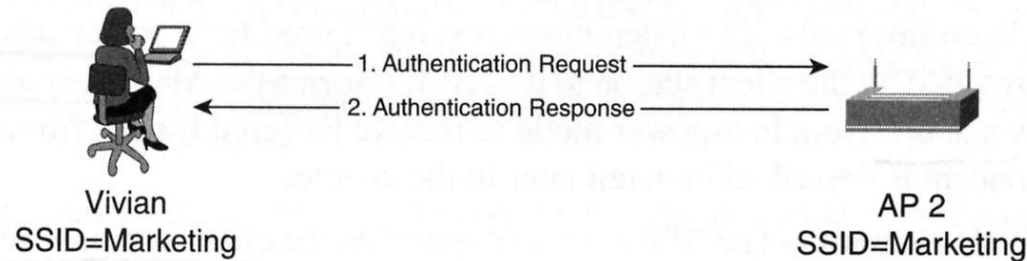
## *Frame Format of the Authentication Frame*

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Authentication Algorithm Numer Field	Authentication Transaction Sequence Numer Field	Status Code Field	Challenge Text IE (Optional)
---------------	----------	----	----	-------	------------------	--------------------------------------	---	-------------------	------------------------------

- ▶ **Open-system** significa “**no autenticación**”.
- ▶ Open-system es el único método requerido por el 802.11
  - ▶ Es posible comprar un AP que no soporte llave compartida.
- ▶ El cliente y la estación intercambian tramas de autenticación.



### The Authentication Process



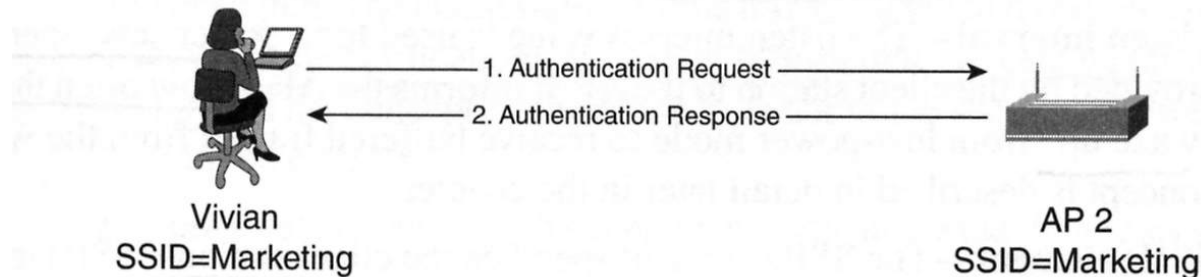
### Frame Control omitted in this Authentication Response

```
Duration                = 213 (in microseconds)
Destination Address      = Station 0006D7863845
Source Address           = Station Aironet482745
Basic Service Set ID     = Aironet482745
Sequence Control         = 0x00B0
... Sequence Number      = 0x00B (11)
... Fragment Number      = 0x0 (0)
Authentication algorithm number = 0 (Open System)
Authentication transaction sequence number = 2
Status code              = 0 (Successful)
```

- ▶ El cliente:
  - ▶ Authentication Algorithm Number = 0 (open-system)
  - ▶ Authentication Transaction Sequence Number = 1
- ▶ El AP:
  - ▶ Authentication Algorithm Number = 0 (open-system)
  - ▶ Authentication Transaction Sequence Number = 2
  - ▶ Status Code = 0 (Successful)

# Proceso de autenticación – Llave compartida

## *The Authentication Process*



## *Frame Format of the Authentication Frame*

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Authentication Algorithm Numer Field	Authentication Transaction Sequence Numer Field	Status Code Field	Challenge Text IE (Optional)
---------------	----------	----	----	-------	------------------	--------------------------------------	---	-------------------	------------------------------

- ▶ Utiliza WEP (Wired Equivalent Privacy) y sólo puede ser utilizado por productos que soporten WEP.
- ▶ WEP algoritmo de cifrado de capa 2 basado en el algoritmo RC4.
- ▶ 802.11 requiere que cualquier estación que soporte WEP soporte autenticación de llave compartida.
- ▶ El AP y el cliente deben compartir una llave secreta.

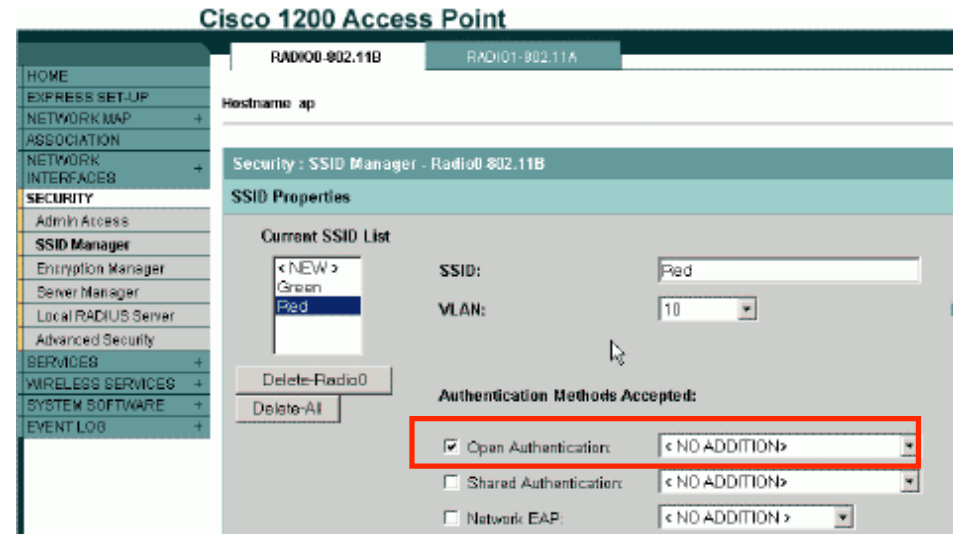
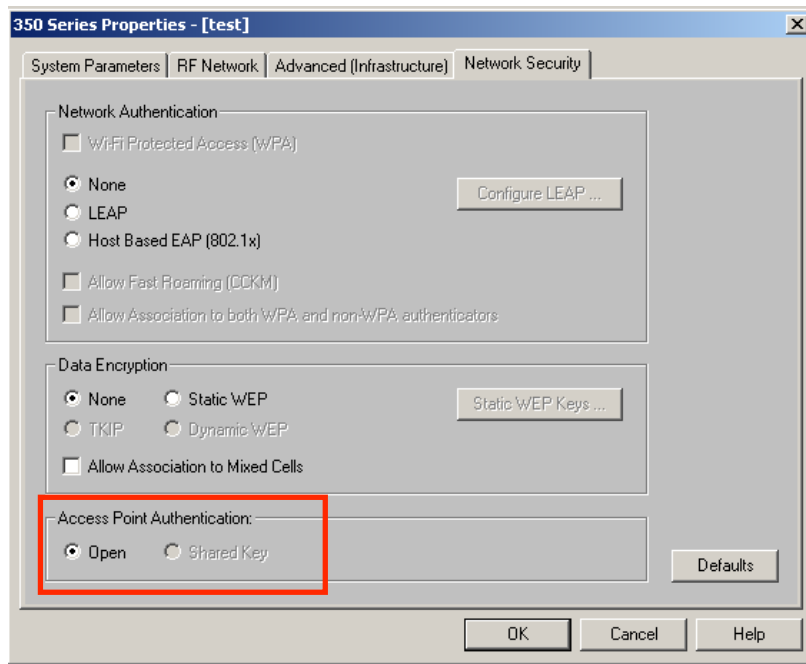
# Proceso de autenticación – Llave compartida

## *Frame Format of the Authentication Frame*

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Authentication Algorithm Number Field	Authentication Transaction Sequence Number Field	Status Code Field	Challenge Text IE (Optional)
---------------	----------	----	----	-------	------------------	---------------------------------------	--	-------------------	------------------------------

- ▶ El cliente:
  - ▶ Authentication Algorithm Number = 1 (shared-key)
  - ▶ Authentication Transaction Sequence Number = 1
- ▶ El AP:
  - ▶ Authentication Algorithm Number = 1 (shared-key)
  - ▶ Set Authentication Transaction Sequence Number = 2
  - ▶ Status Code = 0 (Successful)
  - ▶ Challenge Text
- ▶ El cliente:
  - ▶ Authentication Algorithm Number = 1 (shared-key)
  - ▶ Authentication Transaction Sequence Number = 3
  - ▶ Challenge Text
- ▶ El AP:
  - ▶ Authentication Algorithm Number = 1 (shared-key)
  - ▶ Authentication Transaction Sequence Number = 4
  - ▶ Status Code = 0 (Successful)

# Proceso de autenticación



# Proceso de autenticación

## ▶ Autenticación

▶ Open-System

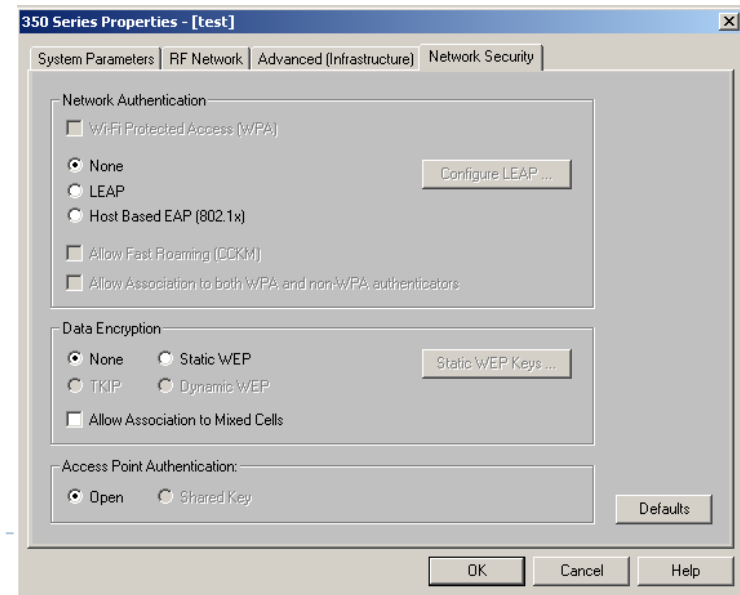
▶ Shared-Key (WEP)

## ▶ Cifrado

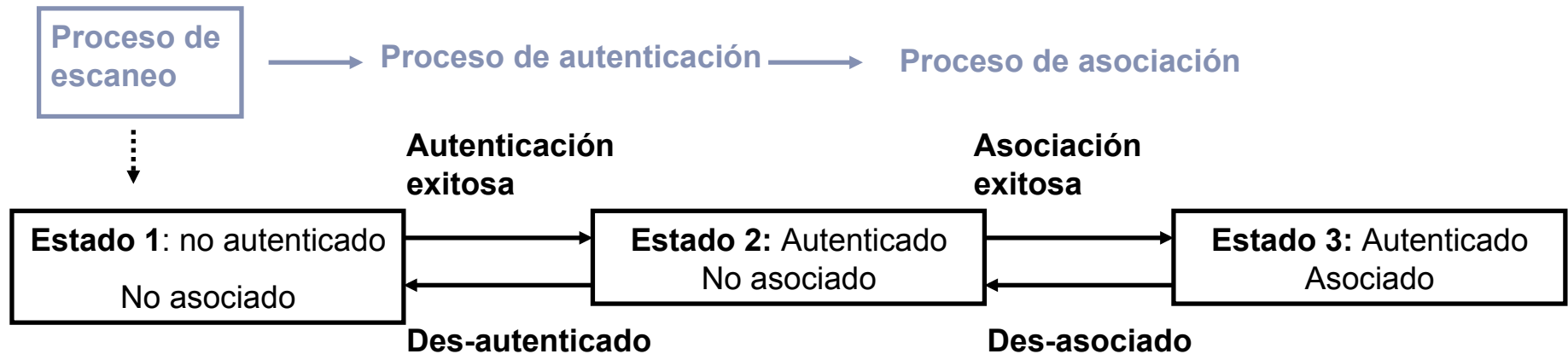
▶ None

▶ WEP

sólo



# Conectividad de la estación



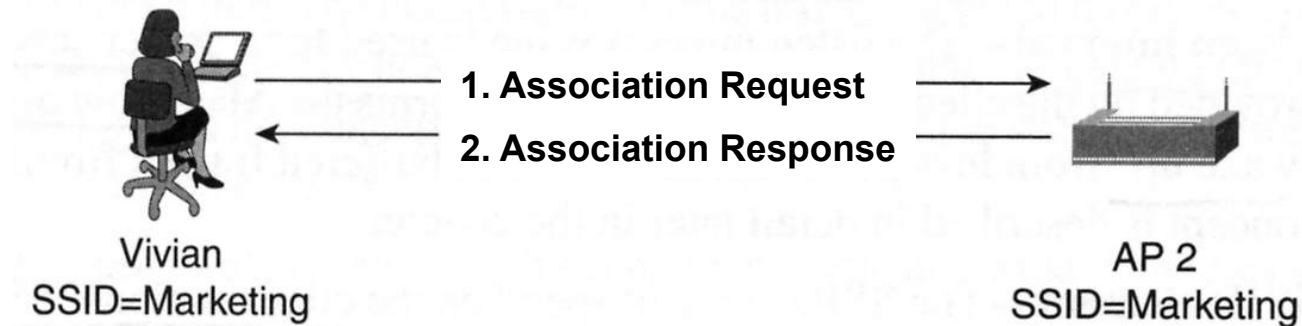
## ► Procesos:

- Probe (o escanéo)
  - Authentication
  - **Association**
- Sólo hasta completar los 3 procesos es que se permitirá la comunicación del cliente.



# Proceso de asociación

---



- ▶ Una estación inalámbrica puede asociarse **sólo a un AP** (restricción del 802.11)
- ▶ Durante el proceso de asociación del 802.11 el AP mapea a la estación inalámbrica con un puerto lógico conocido como **Association Identifier (AID)**.





# Proceso de asociación

## *Frame Format of the Association Request Frame*

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Capability Information Field	Listen Interval Field	SSID IE	Supported Rates IE
---------------	----------	----	----	-------	------------------	------------------------------	-----------------------	---------	--------------------

## *Frame Format of the Association Response Frame*

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Capability Information Field	Status Code Field	AID Field	Supported Rates IE
---------------	----------	----	----	-------	------------------	------------------------------	-------------------	-----------	--------------------

- ▶ Trama *Association Request* (del cliente)
  - ▶ **Listen Interval** – Utilizado en operaciones de ahorro de energía. Informa al AP qué tan seguido se despertará para recibir tramas guardadas.
  - ▶ **Supported Rates** – Qué tasas de transmisión son soportadas por el cliente.
- ▶ Trama *Association Response* (del AP)
  - ▶ **Status Code** – Indica éxito o razón de falla success or reason for failure.
  - ▶ **AID** – Valor asignado para operaciones de ahorro de energía.
  - ▶ **Supported Rates** – Qué tasas de transmisión son soportadas por el AP.

# Proceso de asociación

## *Frame Format of the Association Request Frame*

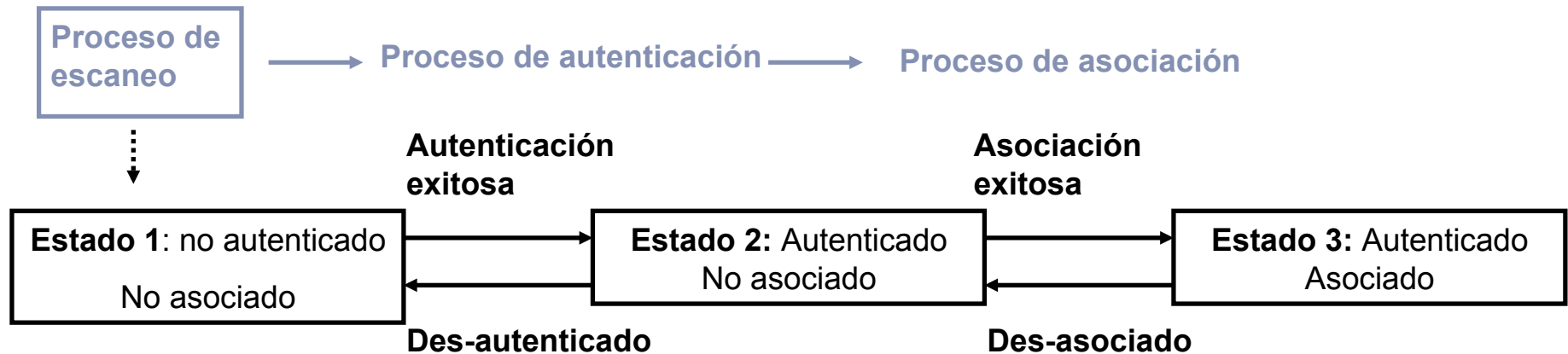
Frame Control	Duration	DA	SA	BSSID	Sequence Control	Capability Information Field	Listen Interval Field	SSID IE	Supported Rates IE
---------------	----------	----	----	-------	------------------	------------------------------	-----------------------	---------	--------------------

## *Frame Format of the Association Response Frame*

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Capability Information Field	Status Code Field	AID Field	Supported Rates IE
---------------	----------	----	----	-------	------------------	------------------------------	-------------------	-----------	--------------------

- ▶ **Trama Association Request (Del cliente)**
  - ▶ El AP agrega la dirección fuente del cliente inalámbrico en su tabla de direcciones fuente.
  - ▶ Así es como el AP sabe si las tramas van a la interfaz inalámbrica (802.11) o a la interfaz alamburada (803.3/Ethernet).

# Conectividad de la estación



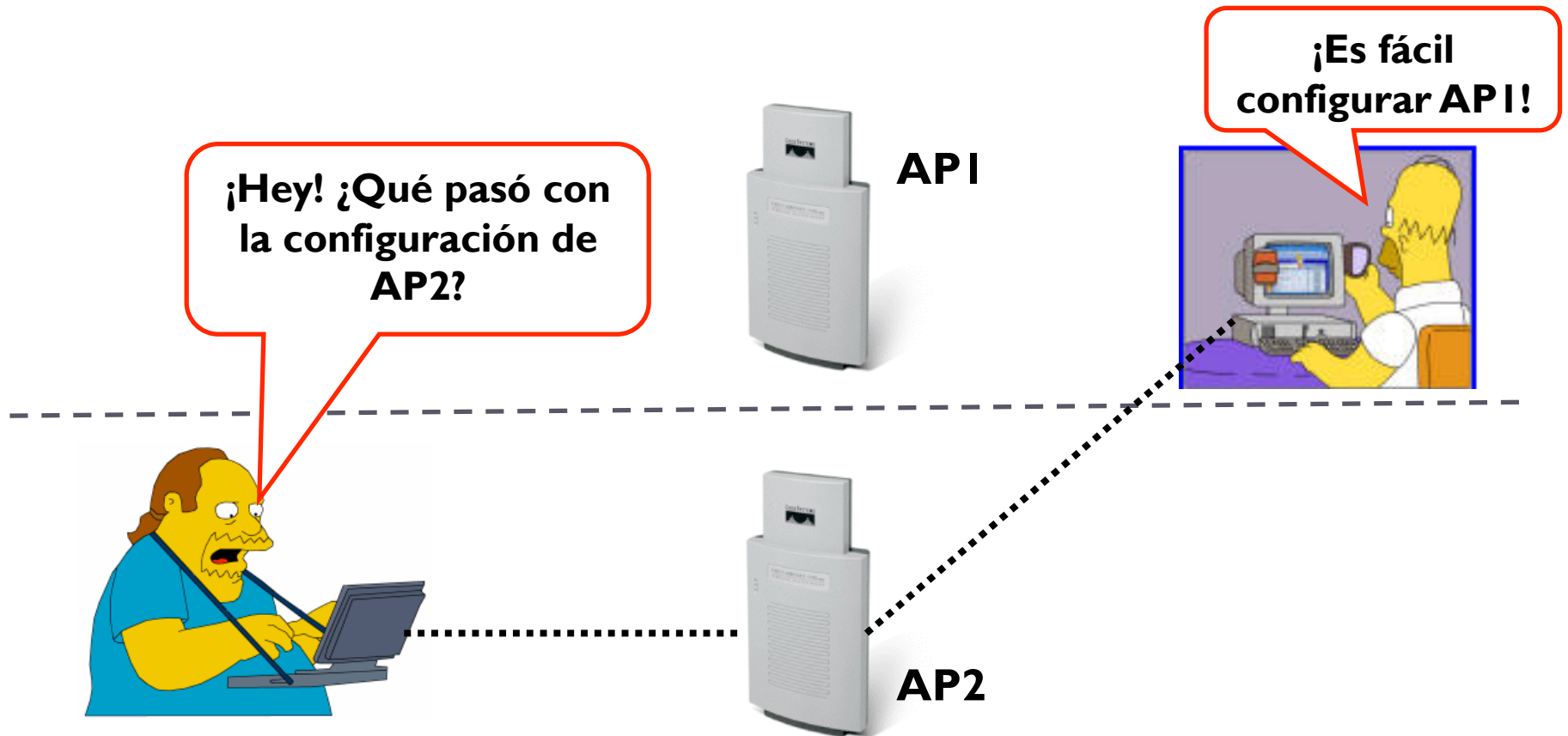
## ► Procesos:

- Probe (o escanéo)
  - Authentication
  - Association
- Sólo hasta completar los 3 procesos es que se permitirá la comunicación del cliente.



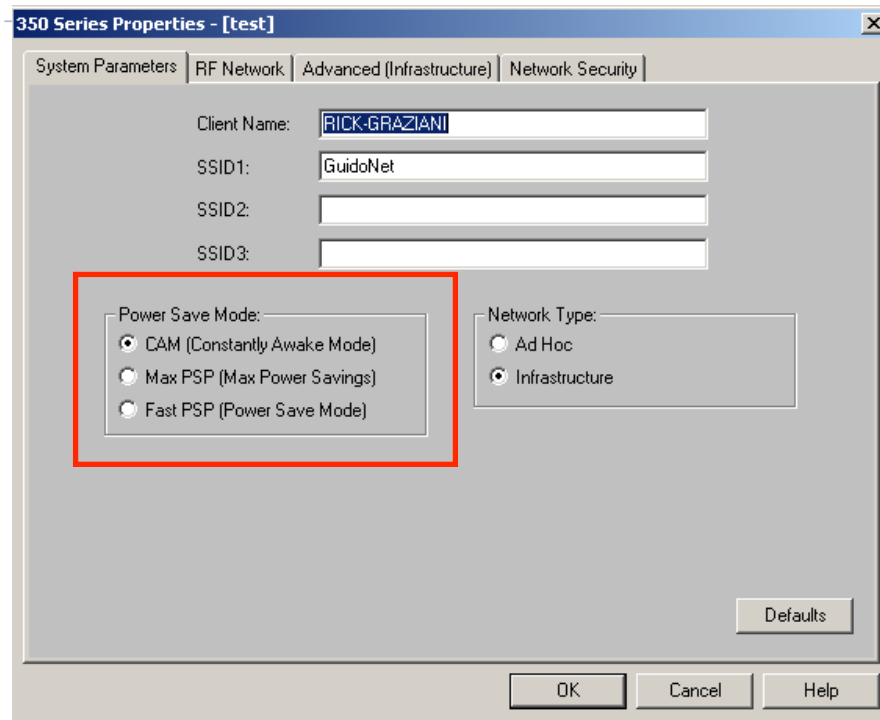
# Nota ... en el laboratorio

---



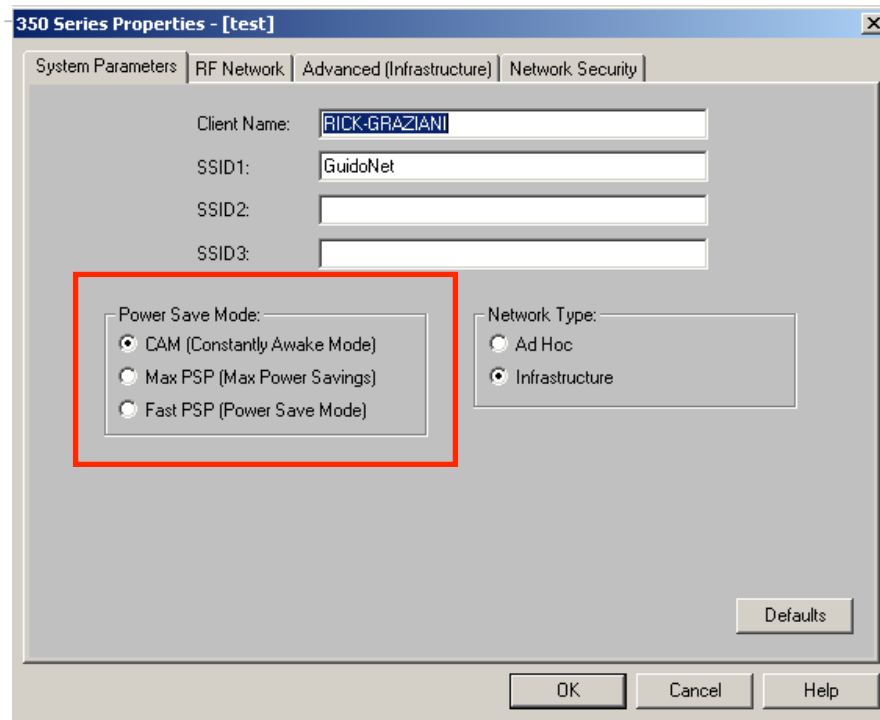
# Operaciones de ahorro de energía

# Operaciones de ahorro de energía (PS)



- ▶ Un factor importante en inalámbricas es la movilidad la cual va relacionada con el tiempo de vida de la batería.
- ▶ Para preservar batería la especificación del 802.11 provee de operaciones de ahorro de energía en los clientes inalámbricos.
- ▶ Las categorías de ahorro de energía en el 802.11 incluye:
  - ▶ Tramas unicast
  - ▶ Tramas broadcast/multicast

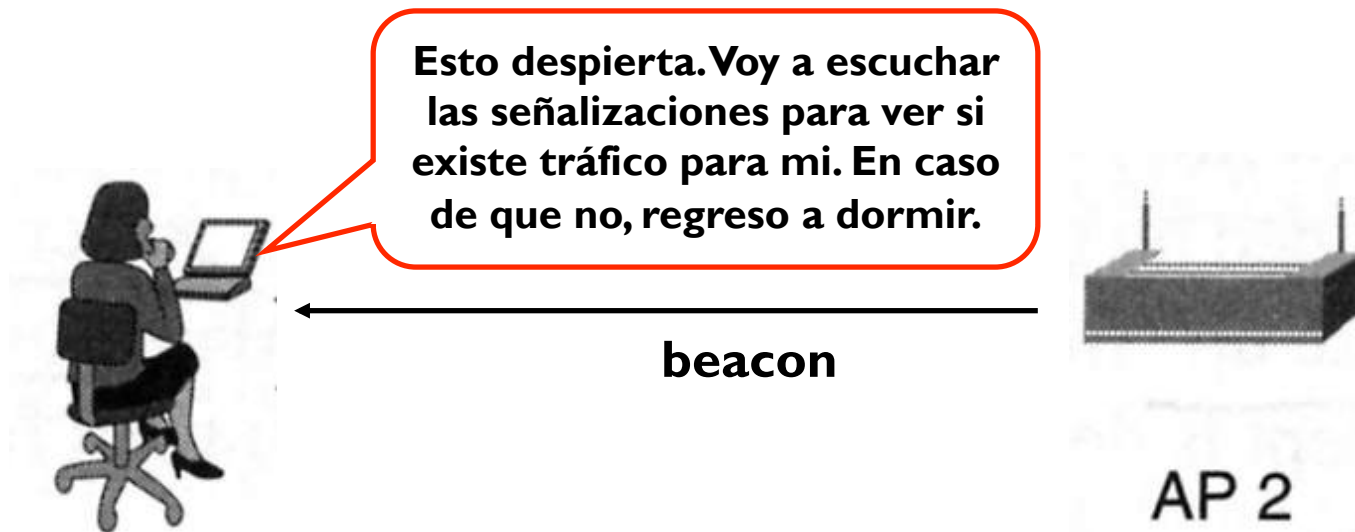
# Operaciones de ahorro de energía (PS)



- ▶ El ACU (ADU) de Cisco tiene tres opciones de ahorro de energía:
  - ▶ CAM (Constantly Awake Mode)
  - ▶ MAX PSP (Max Power Savings)
  - ▶ Fast PSP (Fast Power Saving Mode)
- ▶ TAREA

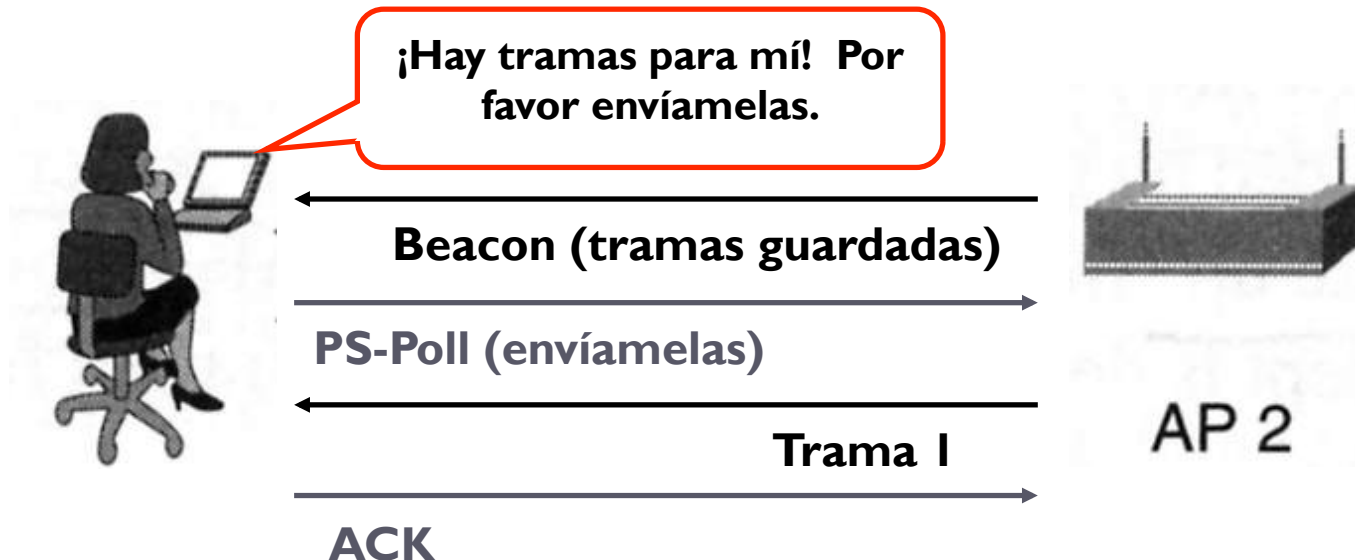


# Operaciones de ahorro de energía (PS)



- ▶ Un cliente entra a ahorro de energía apagando su interfaz de radio.
- ▶ El AP guarda tramas dirigidas para dicha estación mientras ésta se encuentra en modo PS.
- ▶ En un cierto intervalo el cliente despierta para escuchar las señalizaciones del AP.
- ▶ La señalización contiene información indicado si el AP tiene tramas o no para la estación.
- ▶ Si no hay tramas la estación regresa a modo PS.

# Operaciones de ahorro de energía

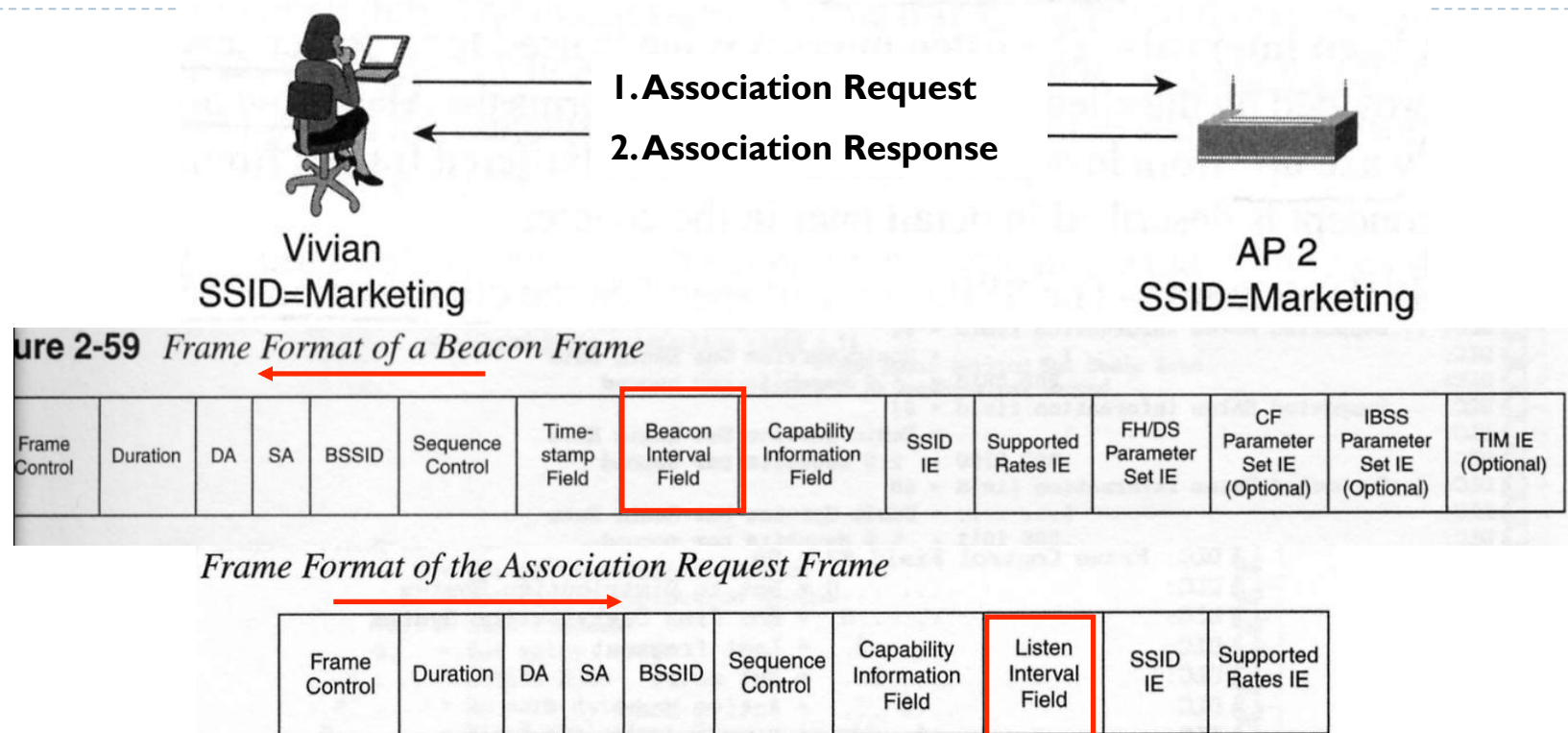


## ► Las bases:

- Si hay tramas guardadas, la estación pedirá por ellas hasta que ya no haya.
- El AP enviará las tramas a la estación.



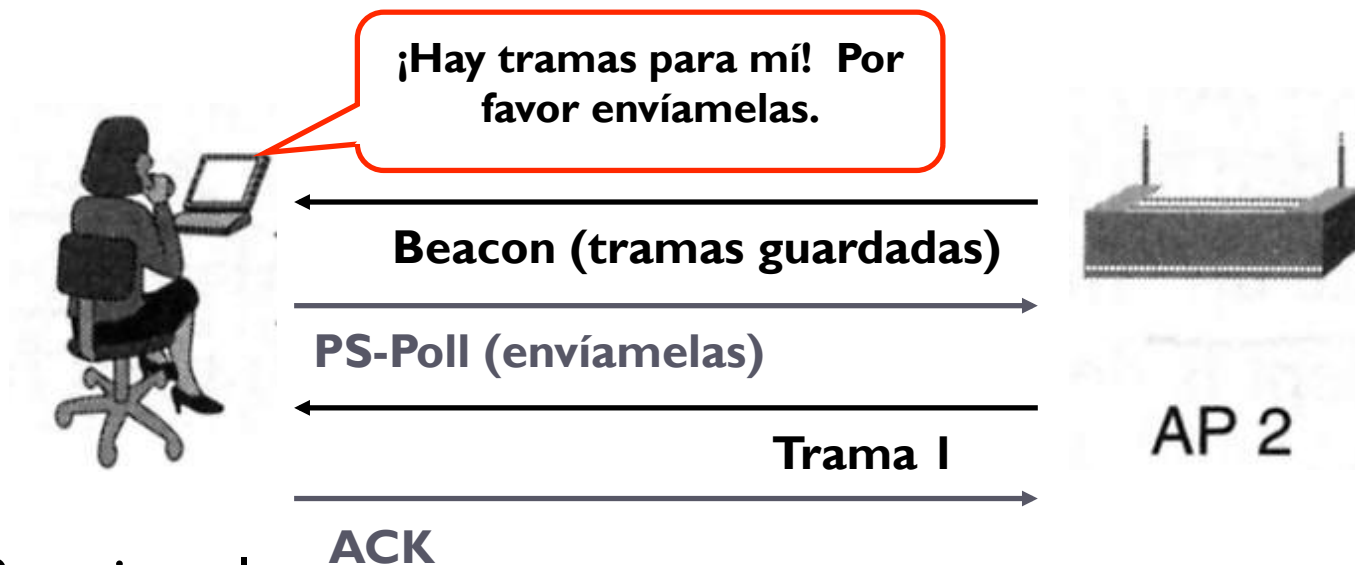
# Operaciones de ahorro de energía para tramas unicast



- ▶ Cuando un cliente se asocia con el AP, especifica su intervalo de escucha.
- ▶ *Listen interval* – El número de señalizaciones que el cliente esperará mientras en modo PS antes de cambiar a modo activo (despierto).
- ▶ El número de señalizaciones por segundo puede variar por AP, pero la trama de señalización ha dicho al cliente qué tan seguido serán enviadas las señalizaciones (*beacon interval*), el cliente sabe cuándo despertar.

# Operaciones de ahorro de energía para tramas unicast

---



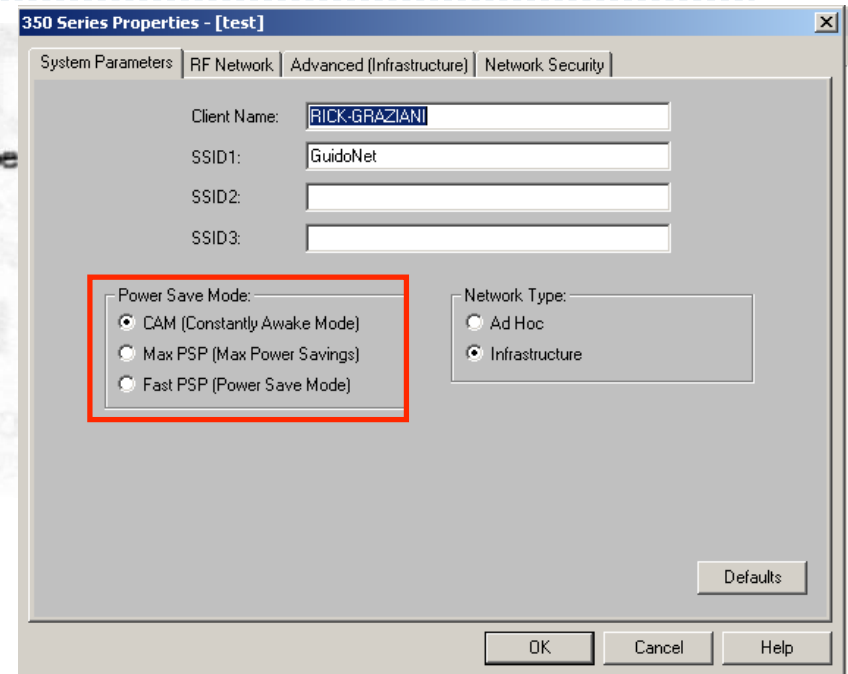
## ► Por ejemplo:

- Si el ***listening interval*** en el cliente es **200**, el cliente despertará cada **200 señalizaciones**.
- Si el ***beacon interval*** del AP es **100** (10 señalizaciones por segundo) el cliente **despertará cada 20 segundos** para ver si existen tramas guardadas para él.

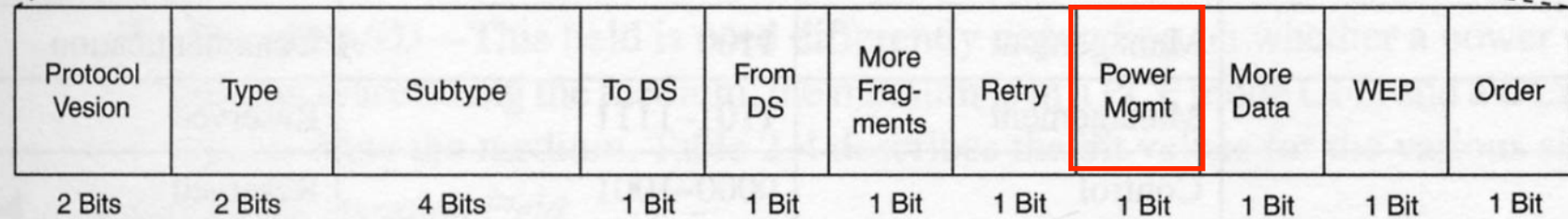


# Operaciones de ahorro de energía (PS)

```
Frame Control Field #1 = A4
.....00 = 0x0 Protocol Version
.....01.. = 0x1 Control Frame
1010 .... = 0xA Power Save (PS)-Poll (Subtype
Frame Control Field #2 = 10
.....0 = Not to Distribution System
.....0. = Not from Distribution System
.....0.. = Last fragment
.....0... = Not retry
...1.... = Power Save Mode
...0.... = No more data
.0... .. = Wired Equivalent Privacy is off
0... .. = Not ordered
```



- ▶ ¿Cómo sabe el AP que una estación está en modo PS?
- ▶ Varias tramas contienen esta información, desde el proceso de conectividad de la estación, PS-Polling y tramas de datos. Esto debido a que el usuario puede estar cambiando el estatus.
- ▶ Esta información está contenida en el subcampo de **Power Management** del campo **Frame Control** que existe en la mayoría de las tramas 802.11.
  - ▶ 0 = Active mode, 1 = Power Save Mode
  - ▶ Tramas del AP siempre tendrán un valor de 0 (no puede ir a dormir)



# Un poco más de detalle sobre operaciones de PS para tramas unicast

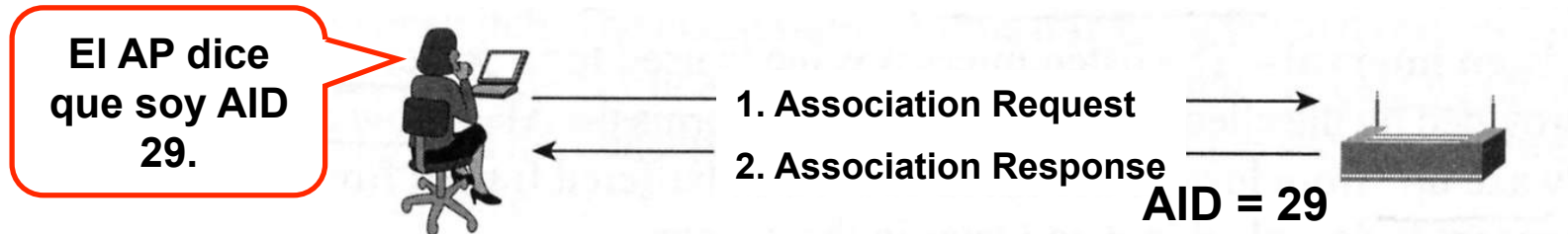


Figure 2-59 Frame Format of a Beacon Frame

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Time-stamp Field	Beacon Interval Field	Capability Information Field	SSID IE	Supported Rates IE	FH/DS Parameter Set IE	CF Parameter Set IE (Optional)	IBSS Parameter Set IE (Optional)	TIM IE (Optional)
---------------	----------	----	----	-------	------------------	------------------	-----------------------	------------------------------	---------	--------------------	------------------------	--------------------------------	----------------------------------	-------------------

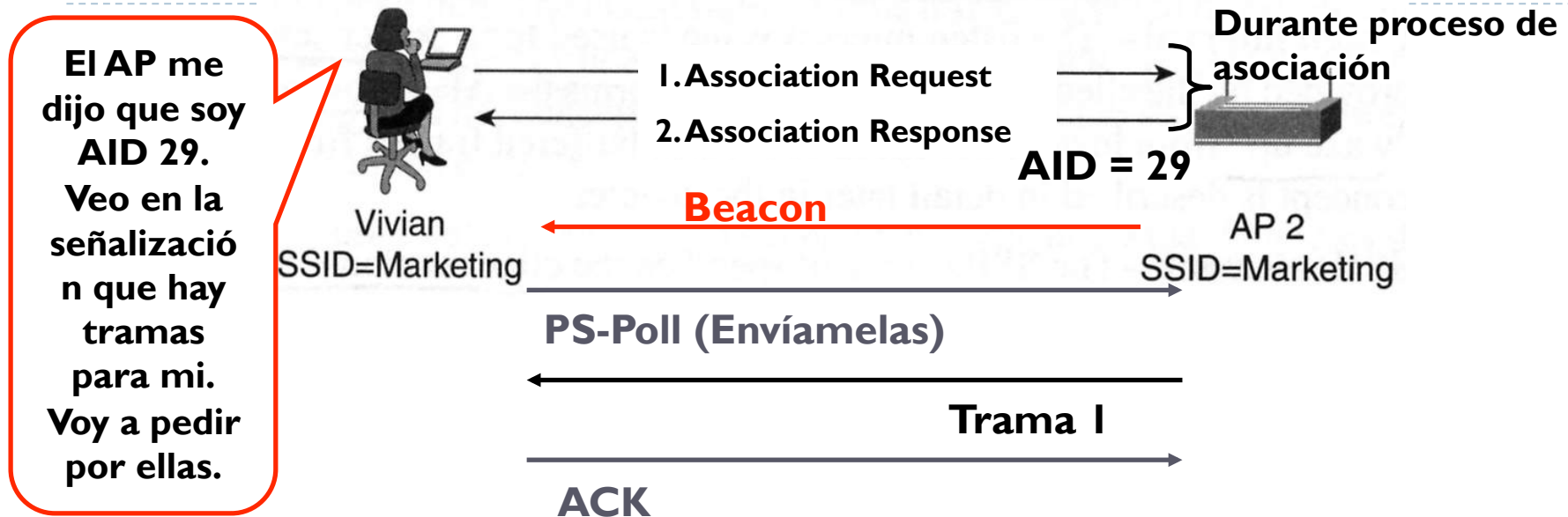
Table 2-2 An Example of the Traffic Indication Virtual Bitmap

AID	1	2	3	...	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	...	2007
Flag	0	0	0	...	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	...	0

- ▶ Cada estación recibe un **Association Identifier** (AID) durante la fase de asociación que lo identifica de manera única con el AP.
- ▶ El campo **TIM** (**Traffic Indication Map**) en cada señalización le indica a la estación si existen tramas guardadas para ella en el AP.
- ▶ Si la “**bandera**” = 0 entonces no hay tramas guardadas, si la “**bandera**” = 1 entonces hay tramas guardadas en el AP.



## Un poco más de detalle sobre operaciones de PS para tramas unicast



- ▶ La estación envía un **PS-Poll** con su **AID** para obtener las tramas.

## Frame Format of the PS-Poll Frame

Frame Control	AID	BSSID	TA	FCS
2 Bytes	2 Bytes	6 Bytes	6 Bytes	4 Bytes


### A Protocol Decode of PS-Poll Frame

```

DLC: ----- DLC Header -----
DLC:
DLC: Frame 58 arrived at 20:37:49.1643: frame size is 16 (0010 hex) bytes.
DLC: Signal level = 100%
DLC: Channel = 1
DLC: Data rate = 2 ( 1.0 Megabits per second)
DLC:
DLC: Frame Control Field #1 = A4
DLC:      ....00 = 0x0 Protocol Version
DLC:      ....01.. = 0x1 Control Frame
DLC:      1010 .... = 0xA Power Save (PS)-Poll (Subtype)
DLC: Frame Control Field #2 = 10
DLC:      ....0 = Not to Distribution System
DLC:      ....0 = Not from Distribution System
DLC:      ....0.. = Last fragment
DLC:      ....0.. = Not retry
DLC:      ...1 .... = Power Save Mode
DLC:      ..0. .... = No more data
DLC:      .0.. .... = Wired Equivalent Privacy is off
DLC:      0... .... = Not ordered
DLC: Association ID = 29
DLC: Basic Service Set ID = Station Aironet482745
DLC: Transmitter Address = Station 0006D7863845
  
```

# Un poco más de detalle sobre operaciones de PS para tramas unicast

## A Protocol Decode of a TIM Element


 DLC: Element ID = 5 (Traffic Indication Map)  
 DLC: ...Length = 5 octet(s)  
 DLC: ...Delivery Traffic Indication Message Count = 5 - 1F0  
 DLC: ...Delivery Traffic Indication Message Period = 10 - 4000  
 DLC: ...Bitmap control field = 03  
 DLC: .....1 = Traffic Indicator bit  
 DLC: 0000 001. = 1 Bitmap offset  
 DLC: ...Partial Virtual Bitmap = 0020

**Table 2-2** An Example of the Traffic Indication Virtual Bitmap

AID	1	2	3	...	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	...	2007
Flag	0	0	0	...	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	...	0

# Operaciones de ahorro de energía para tramas Broadcast/Multicast

## *A Protocol Decode of a TIM Element*

```
DLC: Element ID = 5 (Traffic Indication Map)
DLC: Length = 5 octet(s)
DLC: ...Delivery Traffic Indication Message Count = 5 - 1F 0
DLC: ...Delivery Traffic Indication Message Period = 10 - 9V 1E
DLC: ...Bitmap control field = 03
DLC: .... 1 = Traffic Indicator bit
DLC: 0000 001. = 1 Bitmap offset
DLC: ...Partial Virtual Bitmap = 0020
```

- ▶ Tráfico **broadcast** y **multicast** es guardado por el AP para todas las estaciones (incluyendo estaciones en modo normal) cuando al menos una estación se encuentra en modo PS.
- ▶ El administrador de la red define el intervalo en el que el cliente debe despertar para recibir tráfico broadcast y multicast.
- ▶ Un TIM especial, conocido como **DTIM (Delivery Traffic Indication Map)** indica si hay tráfico broadcast/multicast almacenado en el AP.
  - ▶ Si el campo **DTIM Count** es 0 el AP tiene tramas multicast/broadcast.
- ▶ Información DTIM no es enviada en cada señalización sino en cada **DTIM count period** (décima señalización para este ejemplo), y la “sincronía depende del fabricante.

# Formatos de las Tramas 802.11

# Formatos de las Tramas 802.11 (Algunas de ellas)

---

- ▶ Los siguientes diagramas son FYI y fueron tomados del libro *Cisco Press book 802.11 Wireless LAN Fundamentals* by Pejman Roshan and Jonathan Leary.

## Tramas del 802.11

- Tramas de datos
  - Data
  - Null data
  - Data+CF+Ack
  - Data+CF+Poll
  - Data+CF+Ac+CF+Poll
  - CF-Ack
  - CF-Poll
  - CF-Cak+CF-Poll
- Tramas de Control
  - RTS
  - CTS
  - ACK
  - CF-End
  - CF-End+CF-Ack
- Tramas de Administración
  - Beacon
  - Probe Request
  - Probe Response
  - Authentication
  - Deauthentication
  - Association Request
  - Association Response
  - Reassociation Request
  - Reassociation Response
  - Disassociation
  - Announcement Traffic Indication



## Trama de datos del 802.11

Frame Control	Duration/ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS
2 Bytes	2 Bytes	6 Bytes	6 Bytes	6 Bytes	2 Bytes	6 Bytes	0 - 2312 Bytes	4 Bytes

**Figure 2-59** *Frame Format of a Beacon Frame*

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Time-stamp Field	Beacon Interval Field	Capability Information Field	SSID IE	Supported Rates IE	FH/DS Parameter Set IE	CF Parameter Set IE (Optional)	IBSS Parameter Set IE (Optional)	TIM IE (Optional)
---------------	----------	----	----	-------	------------------	------------------	-----------------------	------------------------------	---------	--------------------	------------------------	--------------------------------	----------------------------------	-------------------

*Frame Format of the Probe Request Frame*

Frame Control	Duration	DA	SA	BSSID	Sequence Control	SSID IE	Supported Rates IE
---------------	----------	----	----	-------	------------------	---------	--------------------

**Figure 2-63** *Frame Format of the Probe Response Frame*

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Time-stamp Field	Beacon Interval Field	Capability Information Field	SSID IE	Supported Rates IE	FH/DS Parameter Set IE	CF Parameter Set IE (Optional)	IBSS Parameter Set IE (Optional)
---------------	----------	----	----	-------	------------------	------------------	-----------------------	------------------------------	---------	--------------------	------------------------	--------------------------------	----------------------------------





### *Frame Format of the Authentication Frame*

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Authentication Algorithm Numer Field	Authentication Transaction Sequence Numer Field	Status Code Field	Challenge Text IE (Optional)
---------------	----------	----	----	-------	------------------	--------------------------------------	---	-------------------	------------------------------

### *Frame Format of the Association Request Frame*

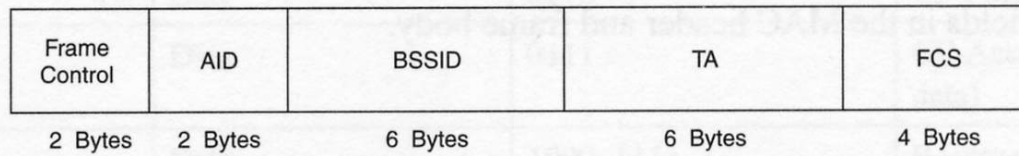
Frame Control	Duration	DA	SA	BSSID	Sequence Control	Capability Information Field	Listen Interval Field	SSID IE	Supported Rates IE
---------------	----------	----	----	-------	------------------	------------------------------	-----------------------	---------	--------------------

### *Frame Format of the Association Response Frame*

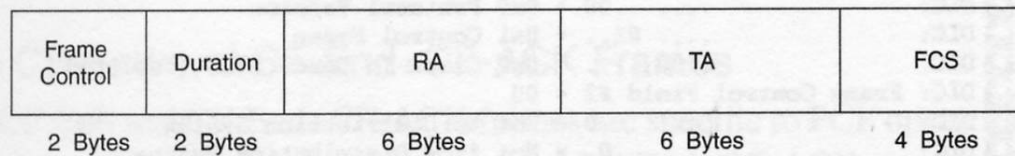
Frame Control	Duration	DA	SA	BSSID	Sequence Control	Capability Information Field	Status Code Field	AID Field	Supported Rates IE
---------------	----------	----	----	-------	------------------	------------------------------	-------------------	-----------	--------------------



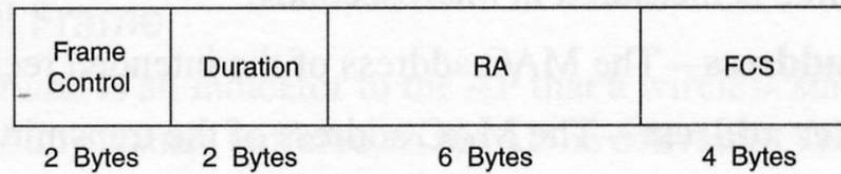
### *Frame Format of the PS-Poll Frame*



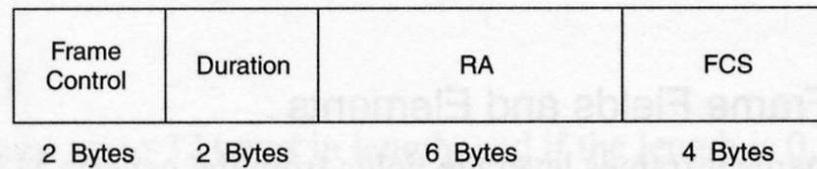
### *Frame Format for the RTS Frame*



### *Frame Format for the CTS Frame*



### *Frame Format for the ACK Frame*



## 2-33 The Frame Control Subfields

