Protocolo ZigBee

Introducción a ZigBee

- Desarrollado por consorcio de empresas → ZigBee Alliance.
- Estándar de comunicación inalámbrico bidireccional.
- Aplicación en:
  - Automatización de edificios → domótica.
  - Automatización industrial → redes de sensores.
  - Sensores médicos.
- Estándar IEEE 802.15.4 → MAC/PHY.

Introducción a ZigBee

- Comparativa → larga duración batería:

	ZigBee™ 802.15.4	Bluetooth™ 802.15.1	Wi-Fi™ 802.11b	GPRS/GSM 1XRTT/CDMA
Application Focus	Monitoring & Control	Cable Replacement	Web, Video, Email	WAN, Voice/Data
System Resource	4KB-32KB	250KB+	1MB+	16MB+
Battery Life (days)	100-1000+	1-7	.1-5	1-7
Nodes Per Network	255/65K+	7	30	1,000
Bandwidth (kbps)	20-250	720	11,000+	64-128
Range (meters)	1-75+	1-10+	1-100	1,000+
Key Attributes	Reliable, Low Power, Cost Effective	Cost, Convenience	Speed, Flexibility	Reach, Quality

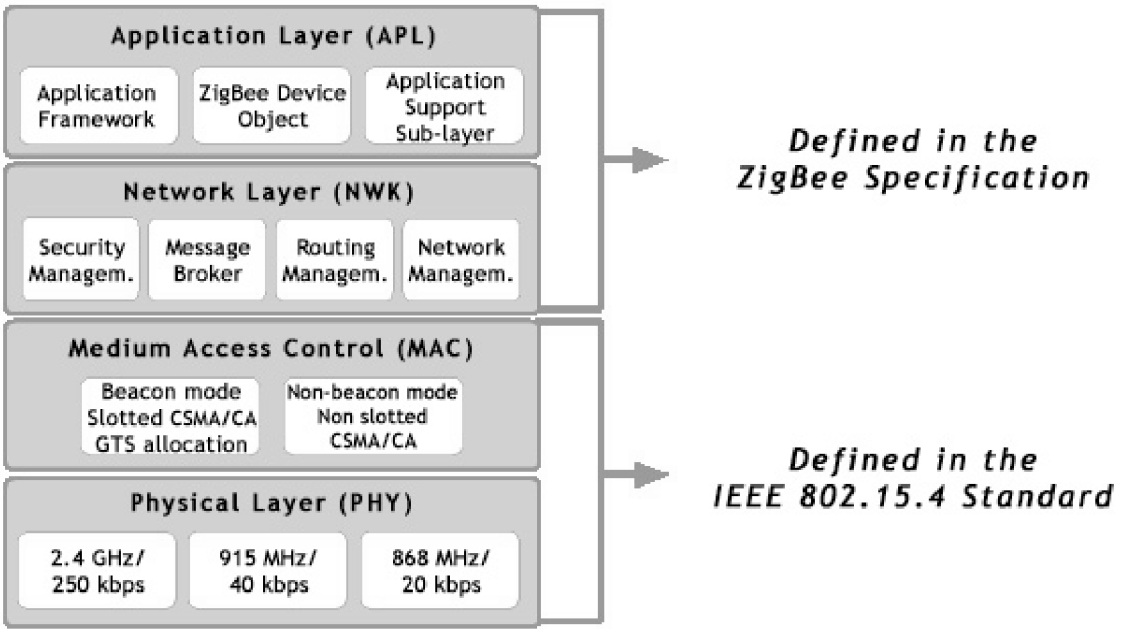
Introducción a ZigBee

- Capas (modelo OSI):

ZigBee Layer	Description
PHY	Defines the physical operation of the ZigBee device including receive sensitivity, channel rejection, output power, number of channels, chip modulation, and transmission rate specifications. Most ZigBee applications operate on the 2.4 GHz ISM band at a 250kbps data rate. See the IEEE 802.15.4 specification for details.
MAC	Manages RF data transactions between neighboring devices (point to point). The MAC includes services such as transmission retry and acknowledgment management, and collision avoidance techniques (CSMA-CA).
Network	Adds routing capabilities that allows RF data packets to traverse multiple devices (multiple "hops") to route data from source to destination (peer to peer).
APS (AF)	Application layer that defines various addressing objects including profiles, clusters, and endpoints.
ZDO	Application layer that provides device and service discovery features and advanced network management capabilities.

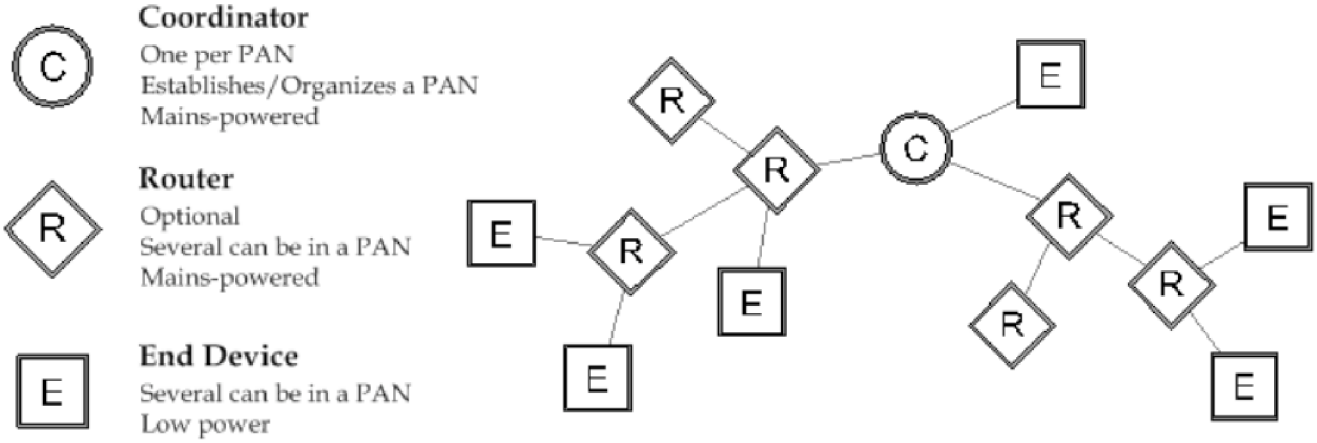
Introducción a ZigBee

- Capas (modelo OSI):



Introducción a ZigBee

- Se definen tres tipos de dispositivos:
  - Coordinator (coordinador).
  - Router.
  - End Device (dispositivo final).



Introducción a ZigBee

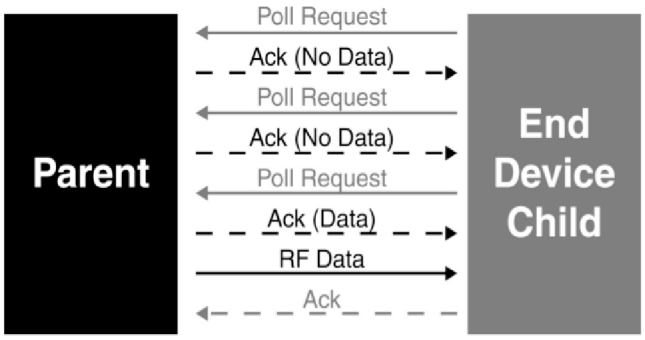
- Coordinator (coordinador):
  - Selecciona un canal, un identificador e inicia una PAN (Personal Area Network).
  - Permite a routers y a dispositivos finales unirse a la PAN.
  - No puede dormir (conectado a la red eléctrica).
  - Rutado de paquetes.
  - Almacena paquetes de dispositivos finales para permitirles dormir.

Introducción a ZigBee

- Router:
  - Debe unirse a una PAN antes de transmitir, recibir o rutar paquetes.
  - Permite a routers y a dispositivo finales unirse a la PAN.
  - No puede dormir (conectado a la red eléctrica).
  - Rutado de paquetes.
  - Almacena paquetes de dispositivos finales para permitirles dormir.

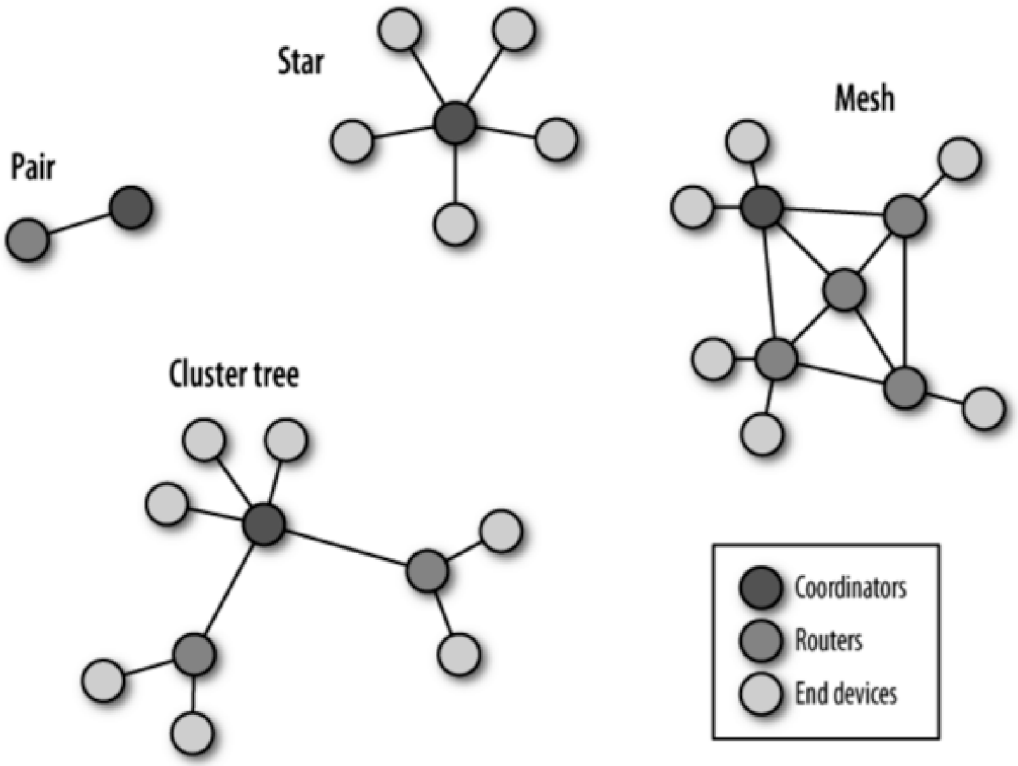
Introducción a ZigBee

- End Device (dispositivo final):
  - Debe unirse a una PAN antes de transmitir o recibir paquetes.
  - No permite a routers ni a dispositivos finales unirse a la PAN.
  - Siempre debe transmitir y recibir paquetes a través de su padre (un coordinador o un router).
  - Puede dormir (para ahorrar batería).
  - No puede rutar paquetes.



Introducción a ZigBee

- Topologías de red:

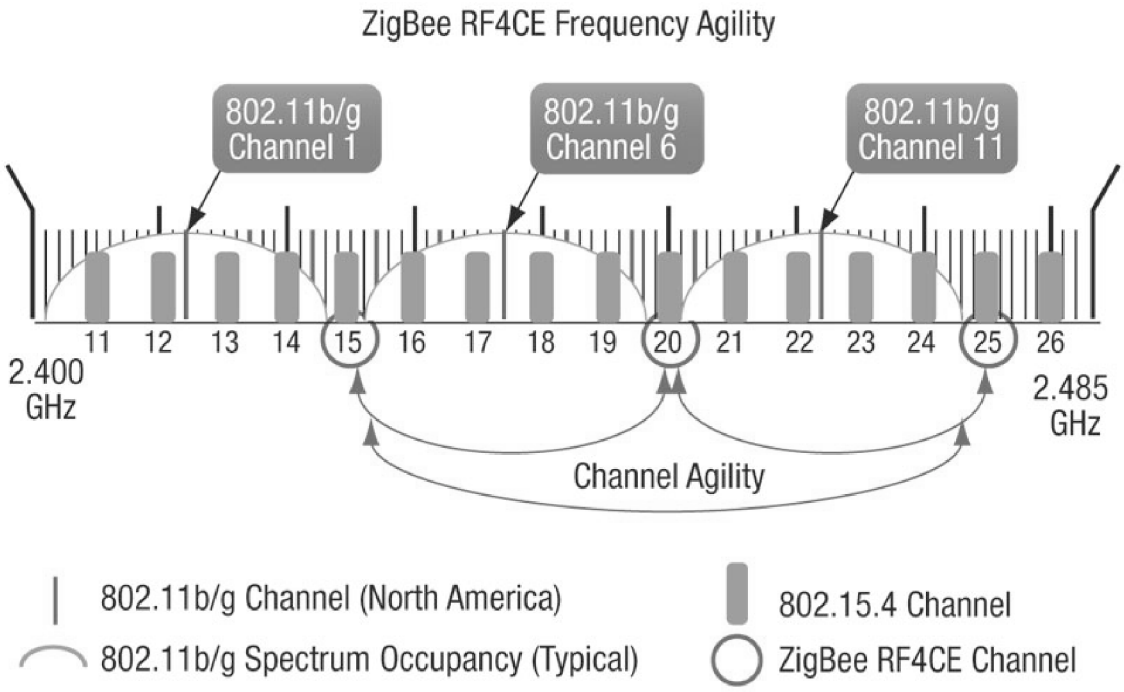


Introducción a ZigBee

- Selección de canal:
  - El estándar IEEE 802.15.4 define 16 canales en la banda de 2,4 GHz.
  - El coordinador debe selecciona un buen canal y un PAN ID único:
    - Realiza escaneo de canales para descubrir actividad RF → Energy scan
    - Realiza escaneo de canales para descubrir PAN cercanas → PAN scan.

Introducción a ZigBee

- Selección de canal:



Introducción a ZigBee

- Selección de PAN ID:
  - Cada PAN utiliza un identificador único.
  - Los dispositivos pueden estar preconfigurados para unirse a un PAN ID determinado o pueden descubrir y conectarse a PAN cercanas.
  - Originalmente el PAN ID era de 16 bits:
    - Utilizado en el campo de dirección de capa MAC.
    - Posibilidad de conflictos entre redes cercanas.
  - Extended PAN ID de 64 bits:
    - Resolución de conflictos con PAN ID de 16 bits.

Introducción a ZigBee

- Direccionamiento de dispositivos:
  - Cada dispositivo tiene una dirección única de 64 bits asignada durante su fabricación.
  - Cada dispositivo recibe una dirección de 16 bits cuando se une a una red → network address.
    - El coordinador siempre tiene la dirección 0x0000.
    - El resto de dispositivo recibe un dirección aleatoria.
  - En las transmisiones se utiliza la dirección de 16 bits para el origen y el destino.

Introducción a ZigBee

- APS (Application Support Sub-layer):
  - Capa de aplicación.
  - Orientada a objetos.
  - Añade soporte para los siguientes objetos:
    - Profile.
    - Cluster.
    - Endpoint.

Introducción a ZigBee

- APS → Profile:
  - Descripción de dispositivos incluyendo su funcionalidad requerida.
  - Perfiles públicos → ZigBee Alliance.
  - Perfiles privados → Fabricante.
  - Ejempos:
    - Home Automation.
    - Smart Energy.
    - Commercial Building Automation.
  - Cada perfil tiene asociado una identificador de 16 bits (Profile ID).
    - El Profile ID 0x0000 está reservado al ZigBee Device Profile (ZDP) y debe estar implementado en todos los dispositivos.

Introducción a ZigBee

- APS → Cluster:
  - Tipo de mensaje de aplicación dentro de un perfil.
  - Definen funciones únicas, servicios o acciones.
  - Ejemplos:
    - Home Automation:
      - On/Off.
      - Level Control.
      - Color control.
  - Cada cluster tiene asociado una identificador de 16 bits (Cluster ID).

Introducción a ZigBee

- APS → Endpoint:
  - Cada endpoint equivale a una aplicación distinta (funcionalmente equivale a un puerto TCP/IP).
  - Un dispositivo puede soportar uno o más endpoints.
  - Cada endpoint se asocia a un determinado perfil.
  - Ejemplos:
    - Un dispositivo puede implementar un endpoint del perfil Smart Energy y segundo endpoint con un perfil privado.
  - Cada endpoint se identifica con un byte (rango válido de 1 a 240).
    - El endpoint 0 está asociado al ZigBee Device Profile (ZDP) y se denomina ZigBee Device Objects (ZDO) endpoint.

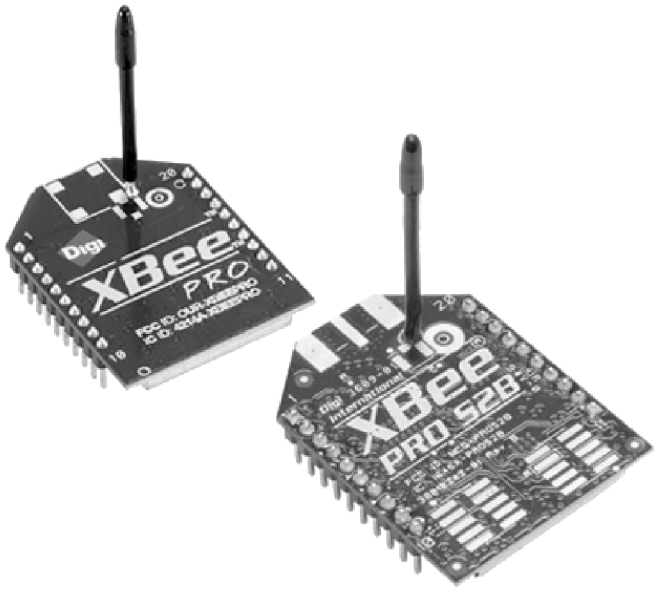
Introducción a ZigBee

ZDO Command	Cluster ID
Network (16-bit) Address Request	0x0000
Network (16-bit) Address Response	0x8000
IEEE (64-bit) Address Request	0x0001
IEEE (64-bit) Address Response	0x8001
Node Descriptor Request	0x0002
Node Descriptor Response	0x8002
Simple Descriptor Request	0x0004
Simple Descriptor Response	0x8004
Active Endpoints Request	0x0005
Active Endpoints Response	0x8005
Match Descriptor Request	0x0006
Match Descriptor Response	0x8006
Complex Descriptor Request	0x0010
Complex Descriptor Response	0x8010
User Descriptor Request	0x0011
User Descriptor Response	0x8011
User Descriptor Set	0x0014
Management Network Discovery Request	0x0030
Management Network Discovery Response	0x8030
Management LQI (Neighbor Table) Request	0x0031
Management LQI (Neighbor Table) Response	0x8031
Management Rtg (Routing Table) Request	0x0032
Management Rtg (Routing Table) Response	0x8032
Management Leave Request	0x0034
Management Leave Response	0x8034
Management Permit Join Request	0x0036
Management Permit Join Response	0x8036
Management Network Update Request	0x0038
Management Network Update Notify	0x8038

Módulo XBee

Módulo XBee

- XBee ZB RF Module.
- Firmware Versions:
  - **20xx - Coordinator - AT/Transparent Operation**
  - 21xx - Coordinator - API Operation
  - **22xx - Router - AT/Transparent Operation**
  - 23xx - Router - API Operation
  - **28xx - End Device - AT/Transparent Operation**
  - 29xx - End Device - API OperationAPS → Endpoint



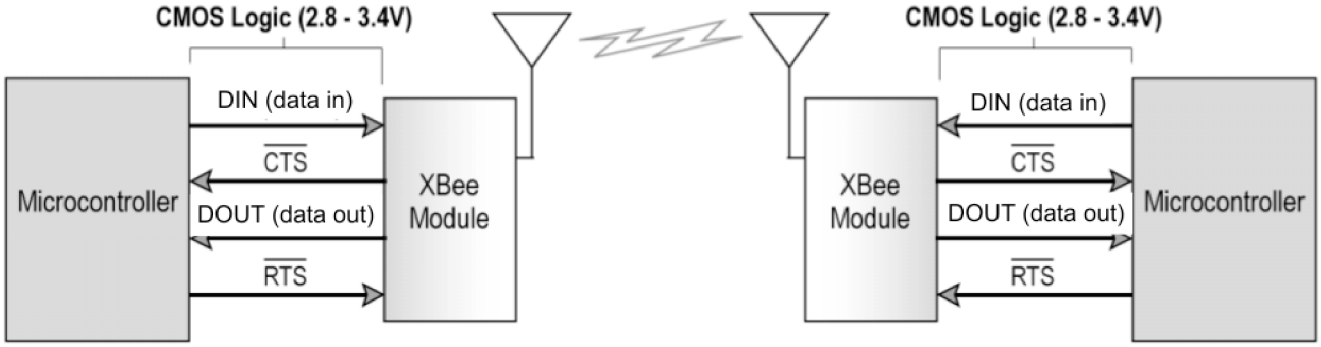
Módulo XBee

- Comparación AT/Transparent vs API:

Transparent Operation Features	
Simple Interface	All received serial data is transmitted unless the module is in command mode.
Easy to support	It is easier for an application to support transparent operation and command mode
API Operation Features	
Easy to manage data transmissions to multiple destinations	Transmitting RF data to multiple remotes only requires changing the address in the API frame. This process is much faster than in transparent operation where the application must enter AT command mode, change the address, exit command mode, and then transmit data. Each API transmission can return a transmit status frame indicating the success or reason for failure.
Received data frames indicate the sender's address	All received RF data API frames indicate the source address.
Advanced ZigBee addressing support	API transmit and receive frames can expose ZigBee addressing fields including source and destination endpoints, cluster ID and profile ID. This makes it easy to support ZDO commands and public profile traffic.
Advanced networking diagnostics	API frames can provide indication of IO samples from remote devices, and node identification messages.
Remote Configuration	Set / read configuration commands can be sent to remote devices to configure them as needed using the API.

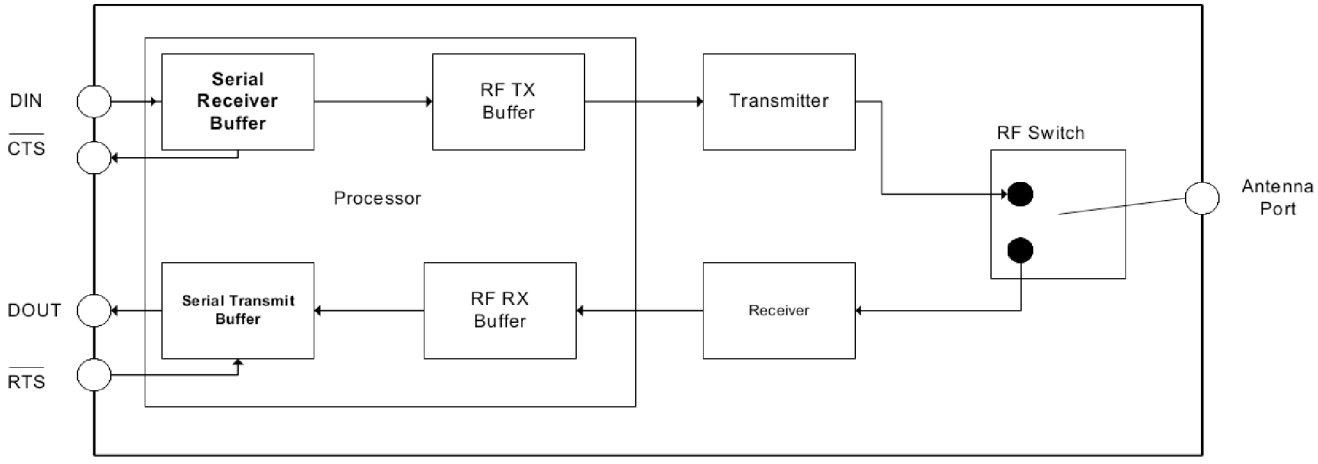
Módulo XBee

- Comunicación serie:
  - UART (por defecto 9600-8-N-1).
  - CTS y RTS no conectados en XBeeCape.



Módulo XBee

- Comunicación serie:
  - TX/RX buffers.



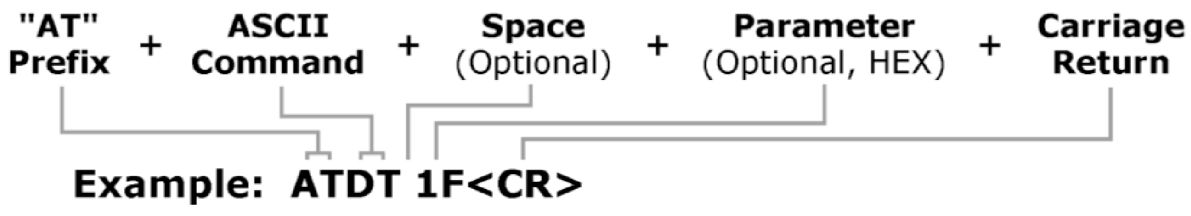
Módulo XBee

- Modos de operación:
  - Idle mode.
  - Transmit mode.
  - Receive mode.
  - Command mode.
  - Sleep mode.

Módulo XBee

- Modo comandos:
  - Entrar al modo comandos AT:
    - No enviar nada durante 1 segundo (command guard time).
    - Enviar “+++” en 1 segundo (command sequence character).
    - No enviar nada durante 1 segundo.

      → Se recibe respuesta “OK\r”.
  - Enviar comandos AT:



  - Salir del modo comandos AT:
    - Enviar comando “ATCN” o esperar command mode timeout.

Módulo XBee

- Comandos AT:

AT Command	Name and Description	Node Type[1]	Parameter Range	Default
CT	**Command Mode Timeout.** Set/Read the period of inactivity (no valid commands received) after which the RF module automatically exits AT Command Mode and returns to Idle Mode.	CRE	2 - 0x028F [x 100 ms]	0x64 (100d)
CN	**Exit Command Mode.** Explicitly exit the module from AT Command Mode.	CRE	--	--
GT	**Guard Times**. Set required period of silence before and after the Command Sequence Characters of the AT Command Mode Sequence (GT + CC + GT). The period of silence is used to prevent inadvertent entrance into AT Command Mode.	CRE	1 - 0x0CE4 [x 1 ms] (max of 3.3 decimal sec)	0x3E8 (1000d)
CC	**Command Sequence Character**. Set/Read the ASCII character value to be used between Guard Times of the AT Command Mode Sequence (GT + CC + GT). The AT Command Mode Sequence enters the RF module into AT Command Mode. The CC command is only supported when using AT firmware: 20xx (AT coordinator), 22xx (AT router), 28xx (AT end device).	CRE	0 - 0xFF	0x2B ('+' ASCII)

XBee®/XBee-PRO® ZB RF Modules → 10. XBee Command Reference Tables

Módulo XBee

- Manejo de un coordinador:
  - Crear una red.

Command	Description
ID	Used to determine the 64-bit PAN ID. If set to 0 (default), a random 64-bit PAN ID will be selected.
SC	Determines the scan channels bitmask (up to 16 channels) used by the coordinator when forming a network. The coordinator will perform an energy scan on all enabled SC channels. It will then perform a PAN ID scan and then form the network on one of the SC channels.
SD	Set the scan duration period. This value determines how long the coordinator performs an energy scan or PAN ID scan on a given channel.
ZS	Set the ZigBee stack profile for the network.
EE	Enable or disable security in the network.
NK	Set the network security key for the network. If set to 0 (default), a random network security key will be used.
KY	Set the trust center link key for the network. If set to 0 (default), a random link key will be used.
EO	Set the security policy for the network.

Módulo XBee

- Ejemplo de creación de red en un coordinador:
  - Configurar el PAN ID deseado o 0 para generar PAN ID aleatorio [ID].
  - Configurar la máscara de canales a escanear [SC].
  - Guardar los cambios con [WR].
  - Aplicar los cambios con [AC] o [CN].
  - Monitorizar el estado con [AI].

Módulo XBee

- Manejo de un dispositivo final:
  - Descubrir redes cercanas → PAN scan.
  - Unirse a una red → Association request.

Command	Description
ID	Sets the 64-bit PAN ID to join. Setting ID=0 allows the router to join any 64-bit PAN ID.
SC	Set the scan channels bitmask that determines which channels an end device will scan to find a valid network. SC on the end device should be set to match SC on the coordinator and routers in the desired network. For example, setting SC to 0x281 enables scanning on channels 0x0B, 0x12, and 0x14, in that order.
SD	Set the scan duration, or time that the end device will listen for beacons on each channel.
ZS	Set the stack profile on the device.
EE	Enable or disable security in the network. This must be set to match the EE value (security policy) of the coordinator.
KY	Set the trust center link key. If set to 0 (default), the link key is expected to be obtained (unencrypted) during joining.

Módulo XBee

- Ejemplo de unión a red de un dispositivo final:
  - Configurar el PAN ID deseado o 0 para unirse a cualquier PAN [ID].
  - Configurar la máscara de canales a escanear [SC].
  - Aplicar los cambios con [AC] o [CN].
  - Monitorizar el estado con [AI]
  - Si el dispositivo se une a la red comprobar:
    - El canal con [CH].
    - El PAN ID de 64 bits con [OP].
    - El PAN ID de 16 bits con [OI].
    - El perfil con [ZS].