FACULTAD DE INGENIERIA Y CIENCIAS AGROPECUARIAS

DISEÑO DE ALGORITMO PARA EL CONTROL DE POSICIONAMINETO DE NODOS EN UNA RED MANET

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingenieros en Redes y Telecomunicaciones

Profesor Guía
MsC. Jorge Wilson Granda Cantuña

Autores
Joselyn Katherine Vásconez Vásconez
Rubén Farías Melo

Año
2016

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con los estudiantes, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

Jorge Wilson Granda Cantuña
Magister en Ingeniería Eléctrica
C.I. 1708594187

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaramos que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

Joselyn Katherine Vásconez Vásconez.	Rubén Farías Melo.
CI: 1723558183	CI: 1722755350

AGRADECIMIENTOS

Este trabajo es el resultado de años de esfuerzo y dedicación, queremos agradecer a nuestras familias, pilar fundamental de nuestra vida; personas tan importantes, como nuestros padres, hermanos, parejas e hijos que día a día nos han guiado por un camino de éxitos.

A nuestro tutor el Ing. Jorge Granda que con su paciencia, conocimiento y esfuerzo nos ha guiado en el desarrollo de este proyecto para cumplir este logro importante para nuestra vida profesional y personal.

DEDICATORIA

Dedicamos este trabajo al futuro de nuestros hijos, que gracias a su motivación hemos podido llegar a culminar una parte de nuestras carreras estudiantiles. A nuestros padres que a lo largo de nuestra vida han velado por nuestro bienestar y educación siendo nuestro apoyo en todo momento, depositando su entera confianza y sin dudar ni un instante en nuestra inteligencia y capacidad

RESUMEN

El presente trabajo contiene el desarrollo de un algoritmo para el control del posicionamiento de nodos en una red MANET; así mismo analiza los requerimientos para garantizar que dicho algoritmo cumpla con los parámetros de diseño mínimos.

Entre los parámetros de diseño se contempla el no aislamiento de los nodos determinando la distancia máxima de separación.

En caso que uno de los nodos se encuentre a la distancia máxima de comunicación se envían alertas para evitar el aislamiento de los mismos.

Mediante la implementación de una simulación de interacción entre los nodos de la red, se puede observar la aplicación de los parámetros de diseño del algoritmo y por lo tanto el cumplimiento del objetivo del trabajo.

Para conseguir el resultado esperado se ha realizado la investigación de los diferentes algoritmos de comunicación de las redes MANET, y así poder determinar cuál se ajusta a los parámetros planteados para este trabajo; posterior al análisis comparativo de estos algoritmos se realiza la implementación de la simulación.

ABSTRACT

This work involves the development of an algorithm for controlling the positioning of nodes in a MANET, likewise the requirements are analyzed to ensure that the algorithm meets the minimum design parameters.

Among the design parameters of the isolation it not contemplated nodes, determining the maximum separation distance.

If one of the nodes is at the maximum communication distance alerts are sent to avoid isolating them.

By implementing a simulation of interaction between network nodes, one can observe the application of the design parameters of the algorithm and thus meeting the objective of the work.

To achieve the expected result has been conducted research of different algorithms MANET communication networks, so you can determine which one fits the parameters set for this work; after the comparative analysis of these algorithms implementing the simulation.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

MANET (Mobile Ad-hoc NETwork) es una nueva tecnología emergente que permite a los usuarios comunicarse sin infraestructura preestablecida, independientemente de la ubicación geográfica de los mismos, es por eso que muchas veces se hace referencia como una red sin infraestructura; estas redes brindan comunicación a dispositivos móviles en zonas de difícil acceso donde no se puede armar y configurar redes que requieren un gran despliegue de infraestructura; dentro de los factores más destacables para el despliegue de una red MANET influyen variables como la geografía de la zona y las limitaciones de los recursos para la operación, como la cobertura y la energía de la red celular.

Una red ad-hoc es auto-organizada, adaptativa y descentralizada, donde la organización de la red y la entrega de mensajes se realiza por los propios nodos. Los dispositivos son capaces de detectar la presencia de otros nodos, y también de realizar la configuración necesaria para facilitar la comunicación y el intercambio de datos y servicios entre ellos; a su vez una red ad-hoc permite que los dispositivos mantengan las conexiones a la red, así mismo el ingreso y remoción de los dispositivos en la red es muy fácil.

Una característica de este tipo de redes es la posibilidad de que se integran a redes de infraestructura con la finalidad de entregar acceso a Internet e Intranet, a través de los nodos móviles que llegan a formar parte de la red MANET.

Debido a la movilidad nodal, la topología cambia rápida e impredeciblemente en el tiempo. A medida que las redes inalámbricas permitieron la movilidad, y debido a la popularidad alcanzada por los dispositivos móviles, las redes inalámbricas ad-hoc se han convertido en uno de los campos de investigación más activos e interesantes dentro de las Redes y Comunicaciones.

1. MARCO TEÓRICO

En este capítulo se describen los conceptos básicos inherentes a las redes MANET.

1.1 Redes Inalámbricas

Las WLAN (redes de área local inalámbricas) son redes que se comunican por medio de la interfaz aire, es decir que no necesita cables; la comunicación se la realiza por medio de ondas electromagnéticas; la recepción y la transmisión se realizan por medio de antenas. Es importante mencionar que para desplegar este tipo de redes existe el estándar 802.11 del IEEE (Institute of Electrical and Electronics Engineers) donde se definen los elementos necesarios a tener en cuenta para la implementación de este tipo de redes; si bien no es necesarios contar con todos elementos para desplegar una red inalámbrica se va a mencionar estos elementos.

Estación Inalámbrica (Wireless Station, STA): es una entidad lógica que posee una dirección de control de acceso al medio (MAC), así como una interfaz de la capa física para el medio inalámbrico. (IEEE, s.f., pág. 21)

Punto de acceso (Access Point, AP): es una entidad que en sí contienen una STA, y permite interconectar varias STA para formar una red. Proporcionan acceso a la distribución de servicios e incorporan funcionalidades que los permiten convertirse en enrutadores (routers), con capacidad para enrutar paquetes y asignar direcciones IP mediante el protocolo DHCP (Dynamic Host Configuration Protocol). (IEEE, s.f., pág. 5)

Sistema de distribución (Distribution System, DS): es un sistema utilizado para interconectar un conjunto de servicios básicos (BSS) e integrarlos a una red LAN para crear un conjunto de servicio extendido (ESS). El sistema de distribución lo conforman el conjunto de AP’s interconectados entre sí. Por lo general el DS está implementado sobre Ethernet.

Conjunto de servicios básicos (Basic Service Set, BSS): un BSS es el conjunto conformado por un Access Point y su STA; tienen un identificador de 6 bytes (BSSID – BSS Identification). La pertenencia a un BSS no implica que la comunicación inalámbrica con todos los demás miembros de la BSS sea posible.

Conjunto de servicios extendidos (Extended Service Set, ESS): es el conjunto de WLAN’s que se interconectan entre sí, son conformados por los BSS, y los AP’s; los STA’s y el DS constituyen un ESS. Un ESS es identificado con un identificador de 32 caracteres (ESSID – ESS Identification). En un ESS las estaciones pueden realizar roaming, es decir, que pueden cambiar de AP dependiendo de la calidad de la señal, dentro del ESS.

Los modos de operación de una red WLAN pueden ser del modo ad-hoc o del modo infraestructura.

1.1.1 Modo Infraestructura

En el modo infraestructura el BSS la WLAN está conformada por un AP y varias STA's que se conectan a él. Estas WLAN son las que se puede encontrar en la mayoría de hogares y empresas, donde el AP funciona como puerta de enlace hacia el Internet. En la Figura 1 se muestra un ejemplo de una red inalámbrica en modo infraestructura.

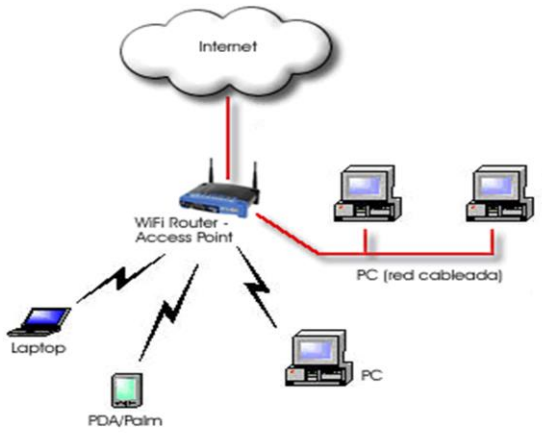


Figura 1 Ejemplo red inalámbrica modo infraestructura

1.1.2 Modo Ad-Hoc

En el modo ad-hoc la WLAN está conformada únicamente por STA's. Para formar la WLAN no se necesita un AP central que sea parte del BSS, las estaciones se conectan entre ellas, punto a punto. Los STA’s realizan las tareas de transmisor, emisor y receptor de información, por lo que para permitir el reenvío de los paquetes entre los nodos, el uso de protocolos de enrutamiento se hace muy necesario. A continuación en la figura 2 se muestra un ejemplo de una red inalámbrica en modo Ad-Hoc.

Figura 2 . Ejemplo red inalámbrica modo ad-hoc

1.2 Redes Ad-Hoc.

Como Christensson (2006) menciona, "ad hoc" es una frase latina que significa "para este fin"; se utiliza para describir soluciones que se desarrollan sobre ese instante y con un propósito específico. Dentro de las redes de computadores, una red ad hoc hace referencia a una conexión de red establecida para una sola sesión y no requiere de un enrutador o una estación base inalámbrica.

Un ejemplo fácil de la necesidad de implementar de una red Ad-Hoc, es cuando se requiere transferir un archivo entre dos computadores, para esto se crea una red ad hoc entre los dos computadores para transferir el archivo. Así mismo si necesita compartir archivos con más de un computador, se puede configurar una red mutli-hop ad hoc, que puede transferir datos a través de múltiples nodos.

Básicamente, una red ad hoc es una conexión de red temporal creado para un propósito específico. Si la red está configurada por un período de tiempo más largo, se convierte en una red de área local (LAN). (Christensson, 2006)

1.3 Redes MANET

MANET es el acrónimo de “Mobile Ad-hoc NETworks”, (Redes Ad-hoc Móviles) es un tipo de red ad-hoc en la que los nodos poseen propiedades de movilidad y autoconfiguración, es decir, están montadas sobre plataformas móviles; así mismo es una red en la que todos los dispositivos (nodos) se encuentran en igualdad de condiciones y se conectan para un servicio o actividad concreta. Esto significa que todos los nodos tienen las mismas funcionalidades; por esta razón, todos pueden ser nodos de origen y destino de las comunicaciones, esta igualdad de condiciones significa que los elementos que la conforman no tienen funcionalidades específicas, como enrutadores o destinos finales.

Cada uno de los nodos de la MANET puede realizar las funciones de emisor, receptor, y a su vez reenviar los paquetes como un router, la comunicación dentro de la red va a depender del rango de transmisión que use el dispositivo. Sólo es posible la comunicación si cada uno de los nodos participa en la transmisión de datos.

Los dispositivos en este tipo de redes son capaces de conocer automáticamente cual es el camino para llegar al destino final; (esto dependerá del tipo de protocolo que se utiliza para establecer rutas para formar la red MANET); cada dispositivo que forma parte de una MANET debe ser capaz de enrutar paquetes hacia los otros dispositivos de la red. Por lo tanto, el mayor reto de estas redes es mantener la información correcta y actualizada en todos los nodos sobre la topología de la red, a medida que estos se van desplazando; por esto los dispositivos que forman parte de la red, deberán tener mayor capacidad de procesamiento.

Al moverse, los dispositivos cambian sus conexiones con los otros nodos de manera dinámica, dependiendo la potencia de emisión de la señal, el ancho de banda o el estado del enlace del mismo; es por esto que la topología es sumamente dinámica y variable en este tipo de redes, normalmente la cantidad de nodos interconectados es muy grande, es por esto la importancia de trabajar en grupos de trabajo.

Debido a las características de las redes MANET estas han ido evolucionando muy rápidamente.

1.3.1 Historia y evolución de las Redes MANET

En cuanto a los inicios o la historia, según (Manoj, 2004), la retransmisión multisalto tiene orígenes en el año 500 antes de Cristo. Darío rey de Persia, ideo un sistema de comunicaciones revolucionario que usaba para enviar mensajes y noticias desde su capital a las provincias remotas de su imperio. Consistía en un sistema de rutas en las que los hombres colocados estratégicamente en estructuras altas podrían comunicarse mediante voz e ir transmitiendo el mensaje salto a salto. Este método era 25 veces más rápido que un mensajero de la época.

En la primera generación las redes MANET fueron usadas para diferentes escenarios militares. La Agencia de Proyectos de Investigación Avanzada de la Defensa (DARPA) inició la investigación acerca de la viabilidad de utilizar las comunicaciones de radio por medio de conmutación de paquetes para proporcionar comunicaciones confiables entre computadores. El primer sistema de redes Ad-Hoc fueron las redes de radio paquetes (PRNET) cada nodo móvil tenía una interfaz de radio de difusión que proporcionan varias ventajas tales como el uso de un solo canal, y la facilidad de la movilidad de apoyo; los principales problemas que enfrenta el proyecto PRNET incluyen los de obtención, mantenimiento y utilización de la información de topología, y el flujo de control de errores sobre los enlaces inalámbricos, la reconfiguración de caminos para manejar las pausas de ruta que surgen debido a la movilidad de los nodos y routers, procesamiento y capacidad de almacenamiento de los nodos, y el intercambio de canal distribuido (Manoj, 2004).

La segunda generación que va desde el año 1980 hasta mitad de la década de 1990; continuó con el mismo objetivo principal que para el sistema de redes Ad-Hoc de primera generación es decir, ayudar a las operaciones de combate militar. Dentro de esta generación se crearon los Sistemas de información móviles globales (GloMo), los cuales proveen una red con capacidades de auto organización, auto aprovisionamiento.

Con la invención de las computadoras portátiles y dispositivos de comunicación basado en ondas de radio en la década de los 90's, el concepto de redes ad-hoc comerciales comienza a ser un negocio a ser tomado en cuenta. Con la idea principal que una red MANET permite crear una colección de nodos móviles se propusieron crear conferencias para la investigación de esta potencial tecnología.

Posterior a esto se promocionaron las aplicaciones comerciales como el Bluetooth y los sensores Ad-Hoc, permitiendo a los usuarios hacer uso de esta tecnología para mejorar la comunicación. Bluetooth es un claro ejemplo de un dispositivo que pertenece a una red MANET, ya que al mismo tiempo cumple las funciones de cliente y de servidor sin necesidad de conexión a un equipo central.

Actualmente son muchos los proyectos que se manejan para las redes MANET; existen proyectos de investigación dentro de las universidades, otros proyectos son llevados a cabo por comunidades de usuarios y a nivel comercial existen empresas que venden y despliegan este tipo de redes.

1.3.2 Características

1.3.2.1 Existencia temporal

Las redes MANET se forman con un propósito determinado, generalmente luego de cumplir su propósito dejan de existir. Es decir que en la mayoría de los casos la red existe durante un periodo limitado de tiempo.

1.3.2.2 Auto Organización

A continuación se describe la Auto Organización que es un aspecto importante en una red MANET; y que posee tres características:

- Auto formación

Para formar una red los dispositivos que se encuentran dentro del rango de otros se vinculan entre sí, esto sin necesidad de intervención externa.

- Auto reparación

Sin afectar el funcionamiento de los demás nodos, la red se reorganiza de manera automática tanto cuando los nodos se unen o abandonan la red.

- Auto protección

La información que fluye dentro de la red es resguardada por los nodos que la conforman, con esto la red se defiende contra amenazas que puedan comprometer la seguridad de la red.

1.3.2.3 Operación distribuida

Dentro de la operación distribuida y los nodos pueden o no tener conocimiento de toda la red, dependiendo del tipo de protocolo que se use, la información que contienen independiente del protocolo, es la información sobre los vecinos que se encuentran dentro de su rango de transmisión. El ruteo y la seguridad se diseñan de tal manera que bajo estas condiciones los dispositivos puedan seguir operando eficientemente.

1.3.2.4 Rango de conectividad limitado

Debido a que dentro de una red MANET los nodos utilizan radio frecuencia para comunicarse, el rango de transmisión se vuelve limitado. El rango de comunicación puede incrementarse si el nodo que origina la comunicación envía los paquetes a otros nodos que están dentro de su rango de frecuencia, y por consecuencias estos pueden actuar como routers y reenviar los paquetes hasta llegar a su destino. (Aldabbas, Alwadan, & Janicke, 2012)

Dentro del RFC 2501 que hace referencia al grupo de trabajo para las MANET en la IETF (Internet Engineering Task Force) se destacan las siguientes características adicionales para las redes móviles (Corson & Macker, 1999):

- Topología dinámica.
- Ancho de banda limitado.
- Operación con energía limitada.
- Seguridad física limitada.

1.3.2.5 Topología dinámica

Los nodos son libres de moverse arbitrariamente dentro de una red MANET; así, la topología de red que es típicamente multisalto puede cambiar al azar y rápidamente en momentos impredecibles y a diferentes velocidades, y esto puede ocasionar que los nodos se encuentren fuera del alcance de los otros, ocasionando aislamientos.

Este cambio dinámico de topología torna difícil establecer la conectividad dentro de la red, la cual debe mantenerse para permitir que la comunicación continúe sin interrupciones.

La topología dinámica en las redes inalámbrica ad hoc puede ser controlada mediante la variación de la potencia de transmisión de cada nodo. El control de topología es el problema que se presenta con el cambio de la potencia de transmisión del nodo, por lo que las redes ad hoc mantienen una topología de red especifica tratando de reducir al mínimo el consumo de energía y aumentar el tiempo de vida.

Las MANET también pueden ser clasificadas de acuerdo a su topología de red; los nodos en una red ad-hoc están divididos en tres tipos: flat, hierarchical y aggregate.

Flat Ad-Hoc Network

Dentro de una red tipo flat todos los nodos tienen la misma responsabilidad y no hay distinción entre nodos individuales. Todos los nodos pueden tener todas las mismas funcionalidades dentro de la red. Los mensajes de control tienen que ser transmitidos globalmente a través de la red; esta es apropiada para redes que cambian dinámicamente. (Loo, Lloret, & Hamilton, 2011, págs. 12-14).

Hierarchical Ad-Hoc Network

Una red de tipo jerárquica consiste en varios clústeres, cada uno representa una red independiente pero comúnmente interconectadas, dentro de estas redes existen dos tipos de nodos:

- Nodos Maestros, son los administradores del clúster y son responsables de enviar la data a los otros clústeres.
- Nodos Normales, se comunican dentro del clúster con los demás nodos de manera directa y con otros nodos de otro clúster lo realizan a través del nodo maestro.

Este tipo de arquitectura es recomendable para casos de baja movilidad, respecto a las redes flat, estas proveen mayor escalabilidad. (Loo, Lloret, & Hamilton, 2011, págs. 12-14).

Aggregate Ad-Hoc Network

Las redes tipo aggregate, dividen la red en un conjunto de zonas, cada nodo pertenece a dos niveles de topología (nivel nodo y nivel zona); es por esto que cada nodo posee dos identificadores dentro de la red, un Id de Nodo y un Id de Zona. Debido a esta división, esta arquitectura soporta la integración de las topologías de tipo flat y jerárquicas.

Un ejemplo de esta integración se muestra en la figura 3.

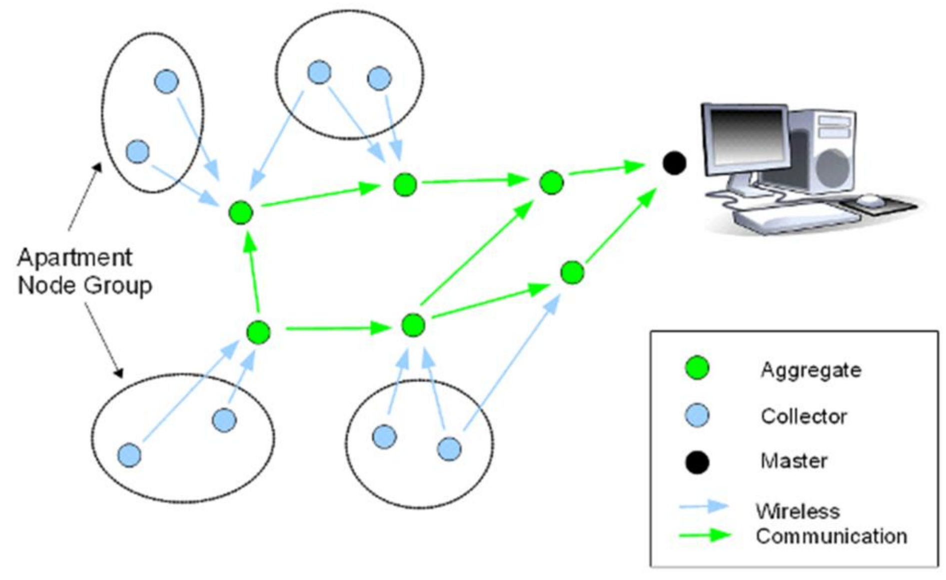


Figura 3 Ejemplo de una red Ad-Hoc del tipo Aggregate.

1.3.2.6 Ancho de banda limitado

Las conexiones inalámbricas aún tienen un ancho de banda limitado con respecto a las redes cableadas, así mismo el throughput que se puede llegar a tener luego de las pérdidas por efectos de ruido, acceso múltiple, obstáculos, etc, es mucho menor que la máxima tasa de transmisión; es por esto que los nodos de una red móvil ad-hoc suelen ser inestables y propensos a tener errores en la transmisión.

El envío periódico de actualizaciones de enrutamiento de red consume un alto ancho de banda. A menudo, los cambios desde una actualización periódica de enrutamiento a la siguiente no van a variar, pero cada nodo debe continuar enviando estas actualizaciones periódicas para que otros nodos sigan considerando que el nodo es accesible a través de estas rutas. Las actualizaciones de enrutamiento de los hosts móviles fuera de rango de transmisión no interferirán con los otros hosts de otras redes, pero los hosts móviles que se encuentran dentro del rango de transmisión, se ven afectados por un alto consumo de ancho de banda por el envío de las actualizaciones de enrutamiento de la red en la que se encuentran dichos hosts.

Respecto a la falta de ancho de banda, la mejor opción para contrarrestarlo, es clasificar el tráfico dentro de clases de QoS y priorizar tráfico de acuerdo a la importancia del mismo.

Por otro lado para poder contrarrestar el problema de la limitación del ancho de banda se debe realizar un correcto análisis del algoritmo de comunicación que se va a utilizar en la red a implementarse teniendo en cuenta la topología, aplicación y tamaño de la misma.

1.3.2.7 Operación con energía limitada

La energía requerida para asegurar que los nodos en una MANET funcionen correctamente proviene de una batería, es por esto que la energía es uno de los recursos que se debe optimizar para que el tiempo de vida y funcionamiento de un nodo se alargue. Con base en este factor uno de los criterios más importantes para el diseño de un sistema es la conservación de la energía.

El envío periódico de actualizaciones de enrutamiento reduce el tiempo útil de las baterías. La mayoría de los hosts móviles en una red ad hoc van a trabajar con la alimentación de la batería, y la transmisión de cada uno paquete gasta una cantidad significativa de energía de la batería (Transmisión de un paquete, en efecto, pone en marcha una porción de energía de la batería de la máquina en el aire). A pesar de que para recibir un paquete generalmente se requiere menos energía que para el envío de uno, la necesidad de recibir estas actualizaciones periódicas de enrutamiento limita la eficiencias que necesita para conservar su batería, por ir cambiando de estado a "en reposo" o "en espera" modo que se usa cuando no está “ocupado”.

1.3.2.8 Seguridad física limitada

Las redes móviles inalámbricas son generalmente más propensas a las amenazas de seguridad física que las redes cableadas. El aumento de la posibilidad de espionaje, la suplantación de identidad, y los ataques de denegación de servicio se deben considerar cuidadosamente en estas redes. Existen técnicas de seguridad a nivel de enlace que se aplican a menudo dentro de redes inalámbricas para reducir las amenazas de seguridad. Como ventaja, la naturaleza descentralizada de control de la red MANET ofrece robustez adicional contra los puntos únicos de fallo.

Se debe tener en cuenta que además de las limitaciones mencionadas, los nodos de una MANET presentan otras limitaciones como la potencia de transmisión, carga de la batería, capacidad de almacenamiento y procesamiento.

Estas limitaciones de las redes MANET antes mencionadas vienen dadas principalmente por el factor “enrutamiento”; que es uno de los factores más importantes para la comunicación entre los nodos de una red, es por esto que la evaluación del mejor protocolo se vuelve un tema crítico previo a la implementación de una solución con este tipo de redes.

1.4 Aplicaciones

Las redes MANET hacen referencia a redes que no requieren de una infraestructura fija, por lo que son fácilmente desplegables. Estas resultan útiles en entornos dónde sea muy costoso instalar una infraestructura fija, dónde las características del terreno no lo permitan o en la mayoría de los casos dónde se requiera de un despliegue rápido. Con esta premisa se describen varias aplicaciones en las cuales se pueden usar las redes MANET:

1.4.1 Entornos Militares:

Las redes MANET permiten establecer la comunicación entre diferentes unidades, vehículos o centros de mando; los participantes de una misión pueden utilizar un medio de comunicaciones conjunto que permita a cada uno de los nodos tácticos como por ejemplo helicópteros, aviones, soldados, comunicarse entre sí al mismo tiempo que están conectados con los centros de comando y control.

Por otro lado, la posibilidad de construir redes bajo demanda es importante debido a que en los ambientes que se encuentran los participantes, son hostiles, y se carecen de infraestructura o la misma es inadecuada.

1.4.2 Situaciones de Emergencia

Las redes MANET pueden ser desplegadas ya sea por desastres naturales, o cuando equipos de emergencia o rescate tienen que actuar de manera rápida, debido a su rápido despliegue si no existe la posibilidad de instalar una infraestructura fija o la que existe ha quedado inutilizada, una red MANET es una solución rápida y eficaz para muchas situaciones de emergencia.

En el caso de un accidente, catástrofe natural u otras situaciones de emergencia, cuando los canales de comunicación más comunes no son viables. Las redes MANET permiten a los equipos médicos y de salvamento estar interconectados mientras se mueven por el escenario, ya sea en un vehículo motorizado o a pie.

1.4.3 Entornos Civiles

Para entornos civiles las aplicaciones de las MANET son muy extensas. Se puede llegar a crear redes de sensores para entornos agrícolas, la cual resulta más rentable que implementar una infraestructura fija. Adicional se pueden crear redes MANET para compartir información entre los asistentes de reuniones importantes por ejemplo un congreso, una conferencia, una clase, etc.

Otros entornos donde se puede llegar a compartir información y donde las redes MANET son útiles, es, en aeropuertos, estadios, cafeterías, centros comerciales, museos.

En situaciones de tráfico urbano resulta muy útil, se podría llegar a platear un escenario en el que los vehículos se encuentren equipados con sistemas de conexión inalámbrica que permita una comunicación entre ellos y con estaciones estáticas, de esta manera se podría informar el estado actual del tráfico.

1.4.4 Redes de área personal

Las redes PAN (Personal Área Network) son redes que están compuestas por dispositivos de uso personal como un equipo portátil, un dispositivo móvil, una PDA, etc. Al utilizar una red MANET nos facilita la comunicación entre ellos.

2. ANÁLISIS DEL ALGORITMO

En este capítulo se realizará un análisis comparativo de los diferentes algoritmos existentes, y que se puedan utilizar para el control del posicionamiento de nodos en una red MANET, al final del mismo se identifica un algoritmo adaptable al concepto de operación propuesto en este proyecto.

2.1 Tipos de protocolos

Existen protocolos de encaminamiento creados específicamente para el uso en las redes cableadas, estos no son eficientes para usarlos en redes móviles debido a la movilidad de los dispositivos, es por esto que han sido modificados con la finalidad de ofrecer mejores soluciones de enrutamiento en redes móviles y se acoplen a un entorno dinámico que poseen las MANET, permitiendo superar problemas tales como una topología dinámica, recursos de ancho de banda limitada y seguridad.

La función más importante de los protocolos de enrutamiento de una red MANET, son el descubrir y mantener las rutas entre los nodos que se encuentran formando la red.

Dentro de una red MANET son los nodos los que tienen la tarea de realizar el encaminamiento o ruteo que garantizara el funcionamiento normal de la red; por esta razón si uno de los nodos dejará de enrutar los paquetes, se puede poner en riesgo el correcto funcionamiento de la red; para evitar este inconveniente existen varios tipos de protocolos que contiene la funcionalidad necesaria dentro de su configuración.

Entre los diferentes tipos de protocolos existentes para crear redes MANETs se pueden diferenciar tres grandes grupos: protocolos proactivos, reactivos e híbridos. En el primer grupo, los nodos mantienen información de encaminamiento hacia todos los dispositivos de la red. En el segundo grupo, los nodos actualizan las tablas de encaminamiento solamente en caso de necesidad. Por último, el tercer grupo intenta incorporar las ventajas de los protocolos proactivos y reactivos.

2.1.1 Protocolos Proactivos

Dentro de los protocolos proactivos cada uno de los nodos cuenta con información de las rutas dentro de una tabla, para mantener actualizadas las tablas los nodos constantemente realizan un intercambio de mensajes. Gracias a la tabla de encaminamiento los dos pueden elegir la mejor ruta ofreciendo una rápida respuesta ante cualquier solicitud.

Una de las principales características es que, aunque no exista movilidad entre los nodos que componen la red o no cambie la topología, siempre va a haber un número mínimo de mensajes enviados para mantener la conexión y tener constancia de los nodos que forman la red.

Dentro de este tipo de protocolos se pueden describir los siguientes: DSDV, WRP y OLSR.

DSDV (Destination Sequenced Distance-Vector)
Basa su funcionamiento en la actualización de una tabla de rutas donde aparece cada destino con su distancia (número de saltos), su número de secuencia que indica cuál es la información más actualizada, y el siguiente salto hacia el nodo final. Debido a que está dentro del grupo de proactivos, siempre tiene conocimiento de todos los dispositivos de la topología.

Es el protocolo de enrutamiento típico para las MANETs, que se basa en el algoritmo Distributed Bellman-Ford. (Perkins & Bhagwat, 1994, págs. 234-244) En DSDV, cada ruta se marca con un número de secuencia que se origina por el destino, lo que indica la antigüedad de la ruta. Cada nodo gestiona su propio número de secuencia asignándole dos veces mayor que la anterior (número par de secuencias) cada vez. Cuando una actualización de ruta con un número más alto de secuencia es recibida, se sustituye la antigua ruta. En caso de diferentes rutas con el mismo número de secuencia, la ruta con una mejor métrica se utiliza. Las actualizaciones son transmitidas periódicamente o inmediatamente cuando se detecta cualquiera cambio de topología significativa. Hay dos formas de realizar actualización de ruteo: “full dump” (volcado completo), en el que un nodo transmite la tabla de ruteo completa, y la “incremental update” (actualización incremental), en el que un nodo sólo los envía las entradas que han cambiado desde la última actualización.

Para evitar las fluctuaciones en la actualización de las rutas, DSDV emplea datos de "tiempo de estabilización", que se utiliza para predecir el tiempo cuando la ruta se vuelve estable. En DSDV, una caída de enlace puede ser detectado por el protocolo de capa 2, o en su lugar puede ser deducido si no hay transmisiones recibidas de un antiguo nodo vecino dentro de un lapso de tiempo.

WRP (Wireless Routing Protocol)

Es un protocolo del tipo proactivo, basado en tablas con el objetivo de mantener la información de enrutamiento entre todos los nodos en la red; se diferencia de DSDV en la forma de mantener las rutas y en el procedimiento de actualización. Mientras que DSDV solamente contiene una tabla, WRP mantiene varias con el fin de tener información más precisa. Cada nodo de la red es responsable del mantenimiento de cuatro tablas:

- Tabla de distancias (DT)
- Tabla de enrutamiento (RT)
- Tabla de enlace costo (LCT)
- Tabla de lista de retransmisión de mensajes (LMR).

Cada entrada del LMR contiene el mensaje de actualización con su número respectivo de secuencia, un contador de retransmisiones, una confirmación de llegada con una entrada por vecino, y la lista de actualizaciones enviadas en el mensaje de actualización. Los registros de LMR que se actualizan en un mensaje de actualización necesitan ser retransmitidos y los vecinos deben reconocer la retransmisión. (Murthy & García, 1996, págs. 183-197)

Los nodos se enteran de la existencia de sus vecinos por la recepción de "acknowledgments" (acuses de recibos) y otros mensajes. Si un nodo no se encuentra enviando mensajes, debe enviar una mensaje *Hello* dentro de un período de tiempo especificado para garantizar la conectividad. De lo contrario, la falta de mensajes desde el nodo indica el fallo de ese enlace; esto puede causar una falsa alarma. Cuando un móvil recibe un mensaje *Hello* de un nodo nuevo, ese nuevo nodo se añade a la tabla de enrutamiento del móvil; y el móvil envía una copia de la información de la tabla de enrutamiento al nuevo nodo. En la figura 4 se muestra la forma de propagación de los mensajes WRP.

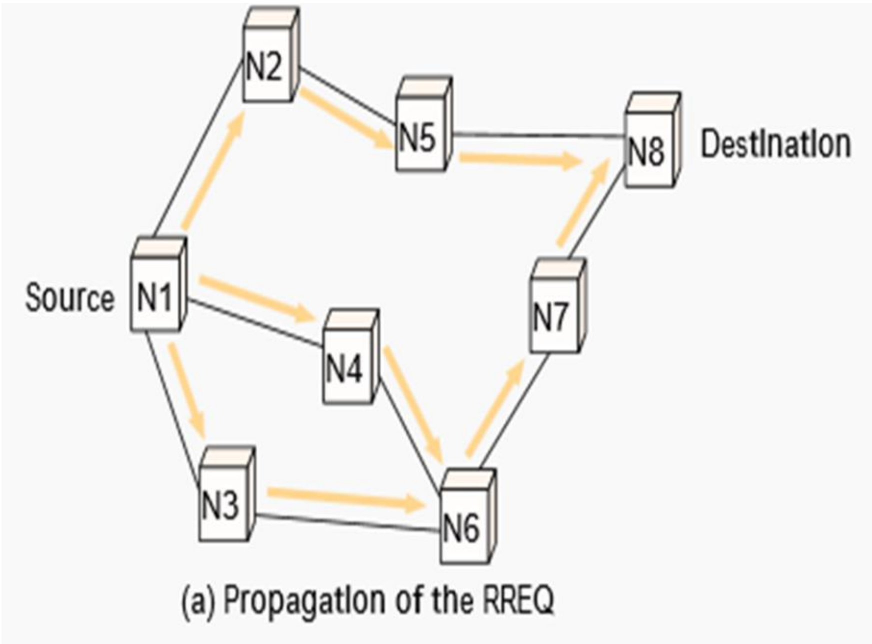


Figura 4 Propagación de los mensajes en WRP.

WRP es reconocido por su forma en la que consigue no entrar en un bucle. WRP, se caracteriza porque los nodos de enrutamiento comunican la distancia detallada y la información desde el segundo al último lugar de salto de cada destino en las redes inalámbricas. WRP entra en la clasificación de algoritmos de ruta de investigación, es importante mencionar la siguiente excepción. Impide el problema "count-to-infinity" (cuenta al infinito) Exige a cada uno de los nodos realizar la verificación de coherencia del predecesor, esta información es reportada por todos sus vecinos. (Tanenbaum, 1996, págs. 357-358). Esto último elimina situaciones de bucle y proporciona una ruta de convergencia más rápida cuando ocurre un evento de fallo de enlace.

OLSR (Optimized Link State Routing)

OLSR pertenece a la familia de protocolos de enrutamiento proactivo para redes ad hoc móviles. El protocolo hereda la estabilidad de un algoritmo de estado de enlace y tiene la ventaja de tener rutas inmediatamente disponibles cuando sea necesario debido a su naturaleza proactiva. OLSR es una optimización a través del protocolo de estado de enlace clásico, adaptado para las redes móviles ad hoc. (Clausen & Jacquet, 2003) Se caracteriza por intentar optimizar el número de mensajes de control que se producen en la red.

El hecho de que todos los dispositivos estén continuamente retransmitiendo mensajes de control para informar sobre la topología es un proceso costoso visto desde la señalización participe y el ancho de banda. OLSR minimiza la sobrecarga de las inundaciones del tráfico de control mediante el uso de los nodos seleccionados, llamados MPRs (MultiPoint Relays), para retransmitir mensajes de control.

Esta técnica reduce significativamente el número de retransmisiones requeridas para inundar un mensaje a todos los nodos de la red. En segundo lugar, OLSR solo requiere un estado de enlace parcial para ser inundado, con el fin de proporcionar rutas de trayectoria más cortas.

La idea de MPRs es minimizar la sobrecarga de mensajes de inundaciones en la red mediante la reducción de las retransmisiones redundantes en la misma región. Cada nodo de la red selecciona un conjunto de nodos en su vecindario simétrica salto-1 que pueden retransmitir sus mensajes. Este conjunto de nodos vecinos seleccionados se llama el conjunto Multipoint Relay (MPR) de ese nodo. Los vecinos del nodo N que no están en su conjunto MPR, reciben y procesan mensajes de difusión, pero no se retransmiten los mensajes de difusión recibidos desde el nodo N. A continuación se muestra la diferencia entre la propagación clásica y la OLSR.

El conjunto mínimo de información de estado de enlace es, que todos los nodos seleccionados, como MPRs, deben declarar los enlaces a sus selectores MPR. Información topológica adicional, se puede utilizar, para fines de redundancia.

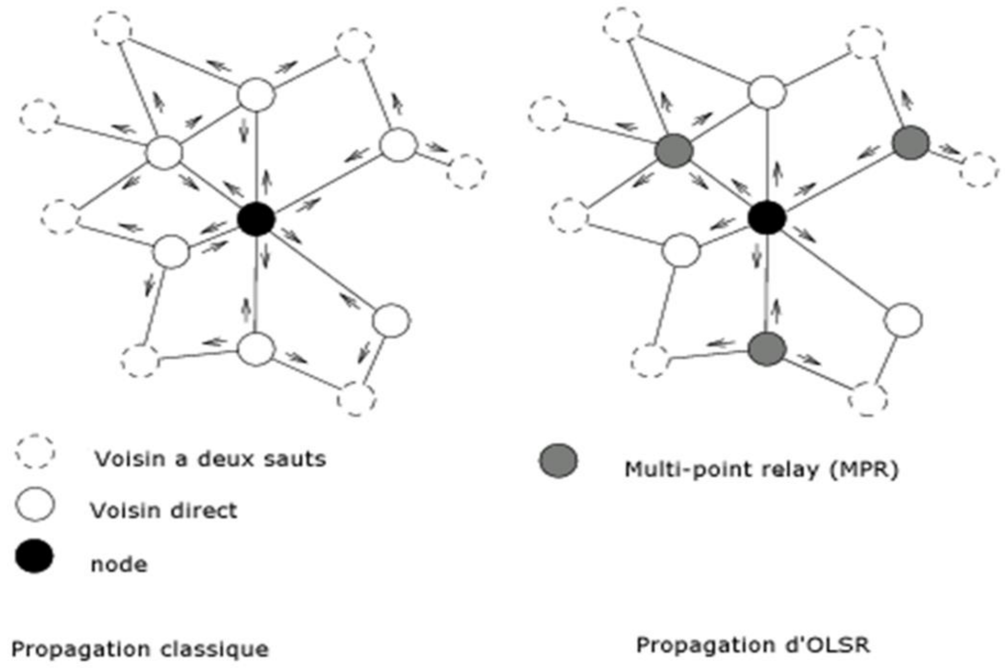


Figura 5 Comparativa entre la propagación clásica y OLSR.

Cada nodo mantiene información sobre el conjunto de vecinos que han seleccionado como MPR. Este conjunto se llama el MPR. Un nodo obtiene esta información de los mensajes HELLO periódicas recibidas de los vecinos.

Mediante la definición de un conjunto de tipos de mensajes, que deben ser reconocidos por todas las implementaciones del OLSR, será posible extender el protocolo mediante la introducción de tipos de mensajes adicionales, sin dejar de ser capaz de mantener la compatibilidad con implementaciones más antiguas. Los tipos de mensajes requeridos para la funcionalidad básica del OLSR son:

- Mensajes Hello, realizan la tarea de detección de enlace, la detección y la señalización del vecino MPR.
- Mensajes TC, realizan la tarea de declaración de topología (publicación de estados de enlace).
- Mensajes MID, realizan la tarea de declarar la presencia de múltiples interfaces en un nodo.

OLSR puede optimizar los cambios topológicos al reducir el intervalo de tiempo máximo para la transmisión periódica de mensajes de control.

Así mismo, como OLSR continuamente mantiene las rutas a todos los destinos de la red, este protocolo es beneficioso para los patrones de tráfico en un gran subconjunto de nodos que se comunican con otro gran subconjunto de nodos. El protocolo esta adecuado para redes grandes y densas, debido a que la optimización realizada al usar MPRs funciona bien en este contexto. Mientras más grande y más denso sea una red, mejor es la optimización que se puede lograr en comparación con el algoritmo de estado de enlace clásico.

OLSR está diseñado para trabajar de una manera completamente distribuida y no depende de ninguna entidad central. El protocolo no requiere una transmisión fiable de mensajes de control, cada nodo envía periódicamente mensajes de control, y por lo tanto puede soportar una pérdida razonable de algunos mensajes. Estas pérdidas se producen con frecuencia en las redes de radio debido a las colisiones u otros problemas de transmisión.

OLSR se comunica utilizando un formato de paquete unificado para todos los datos relacionados con el protocolo. El propósito de esto es para facilitar la extensibilidad del protocolo sin romper la compatibilidad hacia atrás.

El diseño básico de cualquier paquete en OLSR se muestra en la figura 6 (omitiendo cabeceras IP y UDP)

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Packet Length         |    Packet Sequence Number     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Message Type |     Vtime     |         Message Size          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Originator Address                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time To Live |   Hop Count   |    Message Sequence Number    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
:                            MESSAGE                            :
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Message Type |     Vtime     |         Message Size          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Originator Address                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time To Live |   Hop Count   |    Message Sequence Number    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
:                            MESSAGE                            :
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figura 6 Formato paquete en OLSR.

2.1.2 Reactivos

Los protocolos reactivos basan su funcionamiento en la actualización de las rutas solamente cuando sean necesarias, se realiza el descubrimiento de rutas únicamente cuando se desea establecer una conexión. Los protocolos reactivos presentan periodos de reconocimiento de rutas bastante cortas ya que su trabajo es bajo demanda, optimizando el tiempo de entregas en un tiempo menor, manejan mecanismos que permiten el mantenimiento de la ruta y el descubrimiento.

La característica principal es que, si hay movilidad o cambio en la topología, los dispositivos no actualizan sus tablas de encaminamiento a menos que lo requieran. De hecho, no se conoce cómo es la red completa porque no se sabe cuáles son las tablas de los demás nodos, por lo que únicamente hay disponible información sobre las rutas activas.

Algunos tipos de protocolos que entran dentro de este grupo son los AODV, DSR, y ABR.

AODV (Ad-hoc On-demand Distance Vector)

El algoritmo vector distancia bajo demanda ad hoc, permite enrutamiento dinámico, auto arrancable, y multisalto, entre nodos móviles participantes que deseen establecer y mantener una red ad hoc. AODV permite a los nodos móviles obtener rutas rápidamente para nuevos destinos, y no requiere de nodos para mantener rutas a destinos que no están en comunicación activa. AODV permite a los nodos móviles responder a los fallos de enlaces y los cambios en la topología de red en una manera oportuna.

El funcionamiento de AODV es libre de bucles, y evita el problema Bellman-Ford "contar hasta el infinito", ofrece una rápida convergencia cuando la topología de red hoc cambia. Cuando los enlaces se rompen, AODV hace que el conjunto de nodos afectados sean notificados de manera que sean capaces de invalidar las rutas utilizando el enlace perdido.

Una característica distintiva de AODV es el uso de un número de secuencia de destino para cada entrada de ruta. El número de secuencia de destino es creado por el destino que se incluye junto con cualquier información de las rutas que envía al nodo solicitante. Usando números de secuencia de destino asegura la no existencia de bucles y es fácil de programar. Dada la posibilidad de elegir entre dos rutas hacia un destino, un solicitante nodo debe elegir el que tenga el mayor número de secuencia. Por esto, no utiliza mensajes de control hasta que un nodo determinado no necesita una ruta hacia un destino.
Las solicitudes de ruta (RREQ), Ruta Respuestas (RREPs), y errores de ruta (RERRs) son los tipos de mensajes definidos por AODV. Estos tipos de mensajes se reciben a través de UDP, y aplica procesamiento de cabecera IP normal. Así que, por ejemplo, se espera que el nodo solicitante use su dirección IP como la dirección IP originador de los mensajes.

Para mensajes de broadcast, es utlizada la dirección IP (255.255.255.255) de difusión limitada. Esto significa que tales mensajes no se reenvían a ciegas. Sin embargo, la operación de AODV requiere ciertos mensajes para ser difundido ampliamente, tal vez en toda la red inalámbrica de tipo ad hoc. Las gamas de propagación de tales RREQs se indican por el TTL (tiempo de vida) en la cabecera IP. Típicamente no se requiere fragmentación (Perkins, 2003).

AODV es un protocolo de enrutamiento, y se ocupa de la gestión de la tabla de rutas. La información de la tabla de rutas debe mantenerse incluso para rutas de corta duración, tales como las que se creó para almacenar temporalmente los caminos de vuelta hacia los nodos RREQs originarios.

AODV usa los siguientes campos con cada ruta entrada de la tabla:

- Dirección IP de destino
- Secuencia de destino basada en números
- Bandera número válido de sucesión de destino
- Otros indicadores del estado y de encaminamiento (por ejemplo, válido, inválido, reparables, siendo reparado)
- Interfaz de red
- Hop Count (número de saltos necesarios para llegar a destino)
- Siguiente salto
- Lista de Precursores
- Lifetime (tiempo de caducidad de la ruta)

Administrar el número de secuencia es crucial para evitar bucles de enrutamiento, aun cuando los enlaces se rompen y un nodo ya no es asequible para abastecer su propia información sobre su número de secuencia. Un destino se convierte inalcanzable cuando un enlace se rompe o se desactiva. Cuando estas condiciones ocurren, la ruta se invalida por las operaciones que implican al número de secuencia y marca el estado del registro de las tablas de enrutamiento, como inválido.

DSR (Dynamic Source Routing)

El protocolo de enrutamiento de origen dinámico (DSR) es de enrutamiento sencillo y eficaz diseñado específicamente hacia su uso en redes inalámbricas ad hoc multi-hop de nodos móviles. DSR aprueba que la red sea totalmente auto-organizada y auto-configurable, sin tener que utilizar infraestructura de red existente. El protocolo se compone de los dos mecanismos principales de "Route Discovery" (descubrimiento de rutas) y "Route Maintenance" (mantenimiento de ruta), que trabajan juntos para permitir que los nodos descubran y mantengan las rutas a cualquier destino de la red ad hoc. (Johnson, 2007)

Todos los aspectos del protocolo operan por completo bajo demanda, permitiendo que la sobrecarga de paquetes de enrutamiento de DSR pueda escalar de forma automática para únicamente reaccionar a cambios en las rutas actualmente en uso.

Este protocolo permite múltiples rutas a cualquier destino y permite que cada nodo origen pueda seleccionar y controlar las rutas utilizadas en el encaminamiento de sus paquetes, por ejemplo, para su uso en el balanceo de carga.

Otras ventajas del protocolo DSR incluyen una garantía de “loop-free routing” (enrutamiento libre de lazos), su funcionamiento en redes que contienen enlaces unidireccionales, y, una recuperación muy rápida cuando existen cambios de rutas en la red. El protocolo DSR está diseñado principalmente para las redes móviles ad hoc de hasta unos doscientos nodos y es diseñado para funcionar bien incluso con muy altas tasas de movilidad.

Los nodos de red cooperan para reenviar paquetes entre ellos, para permitir la comunicación a través de múltiples saltos entre los nodos que no están directamente dentro de alcance de transmisión inalámbrica uno de otro.

Como los nodos en la red pueden desplazarse, unirse o abandonar la red, y a su vez como cambian las condiciones de transmisión inalámbrica tales como fuentes de interferencia, todo el enrutamiento es determinado y mantenido por el protocolo de enrutamiento DSR automáticamente.

Dado que el número o secuencia de saltos intermedios necesarios para llegar a cualquier destino puede cambiar en cualquier momento, la topología de red será dinámica.

El protocolo DSR cuenta con dos principales mecanismos que permiten el descubrir y mantener la ruta de origen de la red.

Descubrimiento de rutas es el mecanismo por el cual un nodo Origen que se desea enviar un paquete a un nodo de destino D obtiene una ruta de origen a D.

Descubrimiento de rutas sólo se utiliza en el caso que caso que el nodo Origen desea enviar un paquete a D y actualmente no conozca una ruta a D.

Funcionamiento básico del descubrimiento de rutas en DSR

Cuando el nodo de origen realiza él envió de un paquete nuevo dirigido a varios nodos que pertenecen al destino, el nodo que se encuentra en el origen ubica en el encabezado del paquete una "ruta de inicio" dando la sucesión de saltos que el paquete debe seguir su camino hacia el destino.

Normalmente, el emisor obtendrá una ruta de origen adecuada mediante la búsqueda en su "Ruta Caché" de rutas previamente aprendidas; si ninguna ruta se encuentra en su caché, el protocolo de descubrimiento de rutas iniciará de forma dinámica para encontrar una nueva ruta a este nodo de destino. El nodo de origen se llama "initiator" y el nodo destino "target" de la Ruta Descubrimiento.

Mantenimiento de rutas es el mecanismo de detectar por medio del nodo S, la ruta durante su uso de origen hacia el destino, se debe tomar en cuenta que si la topología de red ha cambiado de tal manera que ya no puede utilizar su ruta a D porque un enlace a lo largo de la ruta ya no funciona. Cuando el mantenimiento de rutas indica una ruta de origen se rompe, S puede intentar utilizar cualquier otra ruta que pasa a conocer a D, o puede invocar descubrimiento de rutas de nuevo para encontrar una nueva ruta para los paquetes posteriores a la Ruta D.

El mantenimiento de esta ruta se utiliza sólo cuando S está enviando paquetes a D.

Al utilizar una ruta de origen para realizar el envío o reenvío de un paquete, cada uno de los nodos que transmite el paquete es comprometido de confirmar que los datos pueden fluir a través del enlace de dicho nodo al siguiente salto.
En DSR, el descubrimiento y mantenimiento de rutas, funcionan de forma totalmente bajo demanda, y están diseñados para permitir enlaces unidireccionales y rutas asimétricas. Es importante mencionar que es posible que un enlace entre dos nodos pueda no funcionar de igual manera en ambas direcciones, debido a los diferentes niveles de potencia de transmisión o fuentes de interferencia.

A diferencia de otros protocolos, DSR no requiere paquetes periódicos de ningún tipo en ninguna capa dentro de la red.

Este comportamiento por completo bajo demanda y la falta de actividad periódica permite que el número de paquetes de sobrecarga generados por DSR desciendan todo el camino hasta cero, esto cuando todos los nodos están aproximadamente estacionarios entre sí y cuando todas las rutas para la actual comunicación han sido descubiertas.

Como los nodos empiezan a moverse más o como los patrones de comunicación cambian, los paquetes de enrutamiento de DSR envían de forma automática únicamente lo que se necesita para realizar un seguimiento de las rutas actualmente en uso.

Cambios en la topología de red que no afectan a las rutas actualmente en uso son ignorados y no causan reacción del protocolo.

ABR (Associativity-Based Routing)

Es un protocolo diseñado para redes inalámbricas ad hoc donde los equipos móviles actúan como routers en un entorno inalámbrico sin estaciones base. El protocolo ABR permite que las redes se “formen” y “deformen” de forma rápida, sin la necesidad de la mediación del usuario y el uso de infraestructuras de redes fijas. A diferencia de algunos enfoques existentes basados en vectores de estado de enlace y la distancia, ABR no trata de mantener consistente la información de encaminamiento en cada nodo. (Toh, 1999).

ABR es un protocolo de enrutamiento iniciado por el origen y bajo demanda, se basa en el concepto de la longevidad de una ruta. Una ruta es de larga vida si se mantiene siendo válida en el tiempo y que los nodos en la ruta no migran constantemente fuera del rango de conectividad de sus vecinos inmediatos anteriores y posteriores en la ruta.

ABR basa su funcionamiento en la estabilidad entre los dispositivos. (Toh, 1997, págs. 103-139) Cada nodo clasifica como estable o inestable los enlaces que tenga a su disposición en función de las pérdidas de mensajes HELLO que se produzcan.

Cuando un dispositivo requiere una ruta hacia el lugar de destino, manda un mensaje de petición de rutas RREQ. Una vez recibido, cada nodo intermedio retransmite el mensaje incorporando información acerca de sus enlaces. El destino final espera durante un periodo de tiempo delimitado para recibir varias de estas peticiones, las analiza viendo cuál ha transcurrido por nodos más estables y escoge la que vaya a proporcionar una comunicación más fiable. En el caso en que dos rutas sean igual de seguras, se elige el que tenga menor número de saltos. Si también coincidieran en el número de saltos, se utiliza un mecanismo aleatorio para dilucidar el camino final.

El protocolo ABR consta de tres fases, que incluyen formas de cómo nuevas rutas deben crearse cada vez que se cambian las rutas de edad. Estas fases son: fase de descubrimiento de rutas, fase de reconstrucción de la ruta (RRC), y la fase de eliminación de la ruta.

Inicialmente, cuando un nodo SRC desea una ruta, la fase de descubrimiento de ruta se invoca. Cuando un enlace de una ruta establecida cambia debido al movimiento de cualquier nodo, la fase de RRC se invoca. Cuando el origen ya no desea la ruta, la fase de eliminación de la ruta es iniciada. La fase de descubrimiento de ruta consiste en un ‘broadcast query (BQ)' y un ‘await reply’ (Reply).

Cuando un nodo origen (SRC) requiere una ruta, se enviará un paquete de control BQ y esperará una respuesta desde el nodo destino (DEST). El nodo DEST selecciona la mejor ruta entre todas las rutas posibles y responde de nuevo al nodo SRC.

La fase de eliminación de rutas se utilizará cuando un nodo SRC ya no requiere una ruta, y consiste en la emisión de un paquete “route deletion” (RD) transmitido desde el nodo de SRC por lo que todos los nodos intermedios, retiraran la entrada de esta ruta específica de sus tablas de enrutamiento.
En la figura 7 se puede observar la gráfica del funcionamiento del protocolo ABR.

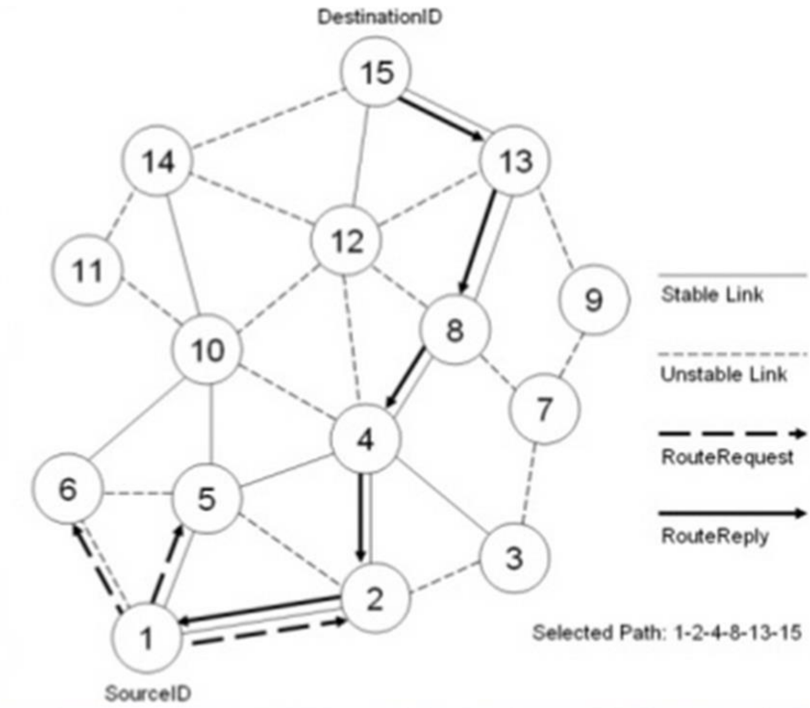


Figura 7 Funcionamineto Protocolo ABR.

2.2 Comparación entre los protocolos reactivos y proactivos.

Tabla 1 Comparación protocolos reactivos y proactivos.

Características	Proactivos	Reactivos
Estructura	Plana y en algunos casos jerárquica (OLSR).	En la mayoría de los casos plana, excepto en CBRP
Disponibilidad de las rutas	Siempre disponibles.	Se determinan cuando son requeridas.
Volumen de tráfico de control	Alto.	Menor que los protocolos proactivos.
Actualizaciones periódicas	Se utilizan. Algunos protocolos tienen mecanismos para usar las actualizaciones en función de la necesidad (OLSR).	No se utilizan. Únicamente para comprobar la disponibilidad de los nodos vecinos.
Sobrecarga por datos de control	Alta.	Baja.
Tiempo en obtener una ruta	Bajo.	Alto.
Requerimientos de almacenamiento	Altos.	Depende del número de rutas que se mantengan. Menor que los protocolos proactivos.
Ancho de banda necesario	Alto.	Bajo.
Energía consumida	Alta.	Baja.
Tiempo de retardo	Bajo si las rutas están determinadas.	Mayor que en los proactivos.
Escalabilidad	Por encima de los 100 nodos.	Por encima de varios cientos de nodos.

Después de conocer y analizar los diferentes protocolos de las redes MANET se ha definido el uso del protocolo AODV debido a que este es el que mejor se ajusta a los requisitos de diseño que se plantea en el presente proyecto; a través de la siguiente tabla comparativa se pueden observar las ventajas contra DSDV.

Tabla 2 Comparación protocolos AODV y DSDV.

AODV	DSDV
Reactivo	Proactivo
No conoce todos los nodos de la red	Conoce todos los dispositivos de la topología
Enrutamiento dinámico	Enrutamiento dinámico
Multisalto	Multisalto
Libre de bucles	Se pueden crear bucles
Rápida convergencia	Lenta convergencia
Número de secuencia para cada nodo dentro de la tabla de rutas	Cada nodo maneja su número de secuencia
No usa mensajes de control	Alto tráfico de mensajes de actualización
Bajo volumen de tráfico	Alto volumen de tráfico (debido a los mensajes enviados)
Bajo tiempo de retardo	Mayor tiempo de retardo
Baja escalabilidad	Alta escalabilidad
Bajo consumo de energía	Alto consumo de energía

3. DISEÑO DEL ALGORITMO Y FASE DE PRUEBA

En este capítulo se realiza el diseño y el desarrollo del algoritmo de control del posicionamiento de los nodos, y se plantea el escenario de pruebas, el cual se enfoca en realizar validaciones y análisis de resultados, permitiendo demostrar el cumplimiento de los requisitos de diseño.

3.1 Diseño del algoritmo

A continuación me listan los materiales y las herramientas utilizadas para el diseño y desarrollo del algoritmo, así mismo se muestra el diagrama funcional del algoritmo.

3.1.1 Herramientas y materiales utilizados

Materiales

El módulo escogido para la comunicación de la red Manet es el XBee S1, este módulo XBee de 2,4 GHz, permite una comunicación muy fiable y simple entre microcontroladores, ordenadores, sistemas; realmente cualquier dispositivo con un puerto serial.

Xbee S1 Explorer, es una base serial a USB. Esta unidad funciona con todos los módulos XBee incluyendo la Serie 1. Se conecta un cable USB mini, y se tiene acceso a los pines de serie y de programación de la unidad XBee.

La placa escogida como microcontrolador es el Arduino Uno, esta es una placa electrónica que cuenta con 14 pines digitales de entrada/salida, 6 entradas analógicas, un cristal de cuarzo de 16 MHz, una conexión USB, un conector de alimentación, y un botón de reinicio; además cuenta con su propio entorno de desarrollo (IDE), donde se programa la comunicación con el módulo XBee; este se conecta a un ordenador con un cable USB o la corriente con un adaptador de CA a CC o una batería.

Baterías, baterías de 9v para proporcionar la energía necesaria para el funcionamiento del módulo.

El dispositivo que va a procesar la información es una Laptop, la cual mediante una interfaz gráfica desarrollada en Visual Studio muestra los resultados obtenidos por el algoritmo.

Herramientas

La herramienta escogida para el desarrollo del programa de comunicación entre el Arduino y el módulo XBee es el Arduino Software, esta es una plataforma de código abierto; además como se menciona anteriormente, esta es la plataforma oficial de desarrollo para los arduinos; este entorno de desarrollo está dirigido para realizar proyectos interactivos.

Para la interfaz gráfica se ha seleccionado la herramienta Microsoft Visual Studio, es una plataforma de desarrollo distribuida por Microsoft, ésta herramienta permite generar aplicaciones para el uso del usuario final, además permite la programación de la comunicación serial utilizada por los dispositivos de este proyecto.

La herramienta utilizada para los dibujos y diagramas es Microsoft Visio, es una aplicación cuyo objetivo es facilitar la visualización de la información, esto ayuda a comprender con solo un vistazo la topología de conexión entre los diferentes componentes.

3.1.2 Diagrama de conexión

En la figura 8 se muestra el diagrama general de conexión de la red Manet para el laboratorio planteado.

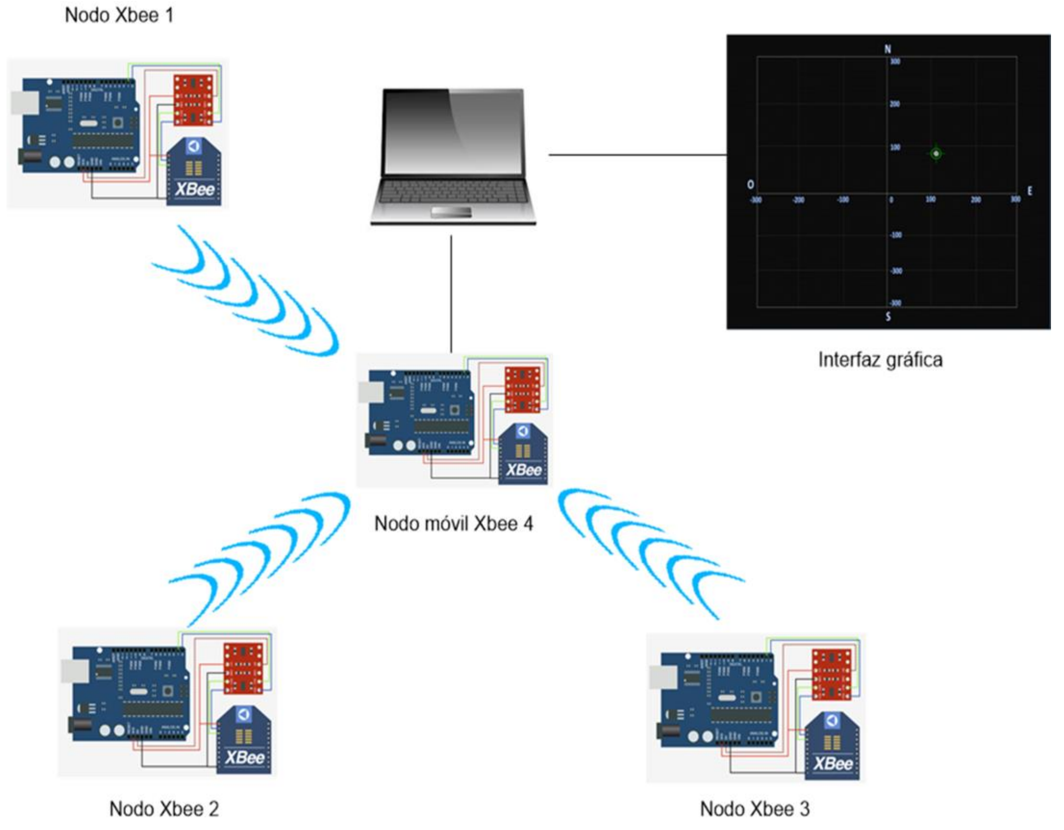


Figura 8 Diagrama de conexión red MANET.

3.1.3 Requisitos de diseño

- Calcular la posición del nodo móvil a medida que se mueve alrededor de los nodos bajo el método de triangulación.
- Enviar información a través de la red MANET.
- Visualizar alertas cuando el nodo móvil se aleje de los nodos.

3.2 Desarrollo del algoritmo

El algoritmo propuesto va a obtener la posición de los nodos a partir del método llamado triangulación, el cual permite obtener las coordenadas de un punto del cual no se conoce su posición, a partir de la medición de distancias a puntos de coordenadas conocidas previamente. Esta técnica es la base del posicionamiento de todos los sistemas GNSS (Sistema Global de Navegación por Satélite).

La ecuación básica en el plano es:

$\rho = \sqrt{(x_e - x)^2 + (y_e - y)^2}$ (Ecuación 1)

Donde ρ es el valor observado, (x_e, y_e) son las coordenadas conocidas y (x, y) las coordenadas que no se conocen. Como las incógnitas son dos el problema requiere un mínimo de dos ecuaciones. Así el problema queda planteado como:

$\rho 1 = \sqrt{(x_{e1} - x)^2 + (y_{e1} - y)^2}$ (Ecuación 2)

$\rho 2 = \sqrt{(x_{e2} - x)^2 + (y_{e2} - y)^2}$ (Ecuación 3)

En términos generales no se puede afirmar que con solo dos ecuaciones la solución será única y por lo tanto es imprescindible una ecuación más para resolver el problema.

$\rho 3 = \sqrt{(x_{e3} - x)^2 + (y_{e3} - y)^2}$ (Ecuación 4)

Para entender mejor el método de cálculo de trilateración se plantea el método gráfico.

Una solución sencilla consiste en realizar un gráfico y deducir del mismo la respuesta. Así para el caso de tener los siguientes puntos de coordenadas conocidas:

Tabla 3 Puntos de Coordenadas

punto	*x*	*y*
1	2	2
2	3	3
3	4	2

Las siguientes distancias desde el punto incógnita a cada uno de ellos:

Tabla 4 Distancias entre puntos

segmento	*distancia*
Punto 1 – punto desconocido	$\sqrt{2}$
Punto 2 – punto desconocido	1
Punto 3 – punto desconocido	$\sqrt{2}$

El problema se resuelve trazando los círculos con centro en cada punto conocido y radio igual a la distancia punto conocido - punto desconocido. Quedan representada entonces todas las posibles posiciones del punto desconocido mediante circunferencias y una sola de ellas será la correcta: ***la intersección de todas las circunferencias.*** Esto se puede visualizar en la figura 9.

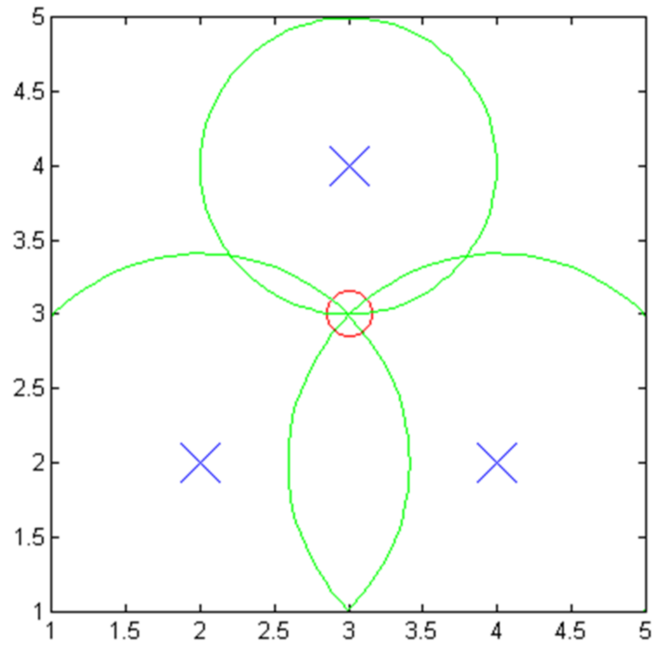


Figura 9 Método trilateración

Luego del análisis realizado se llegó al desarrollo de dos ecuaciones que se usará en la implementación:

$$X = \frac{(d_1)^2 - (d_2)^2 + x^2}{2(x)} \qquad \text{(Ecuación 5)}$$

$$y = \frac{(d_1)^2 - (d_3)^2 + y^2}{2(y)} \qquad \text{(Ecuación 6)}$$

Después de haber entendido cómo se realiza el cálculo de la posición de los nodos móviles, a continuación se plantea la implementación.

3.2.1 Levantamiento de datos bajo interpolación

A continuación se muestra los datos obtenidos bajo muestreo manual; este muestreo manual se lo realiza bajo pruebas de separación de los nodos a distancias preestablecidas, los resultados enviados en hexadecimal por los módulos XBee son relacionados con la distancia y con estos resultados se obtiene los datos para la interpolación.

Tabla 5 Muestreo de interpolación.

Hexadecimal	**CM**
37	5
55	100
67	200
73	300

Posterior al análisis de los datos citados anteriormente, se logró obtener una ecuación la cual permite tener una relación de hexadecimal a centímetros (cm) para que esta información pueda ser interpretada por la aplicación; esta ecuación matemática sirve para interpretar los datos de entrada en el serial. La ecuación mencionada se la visualiza en la figura 10.

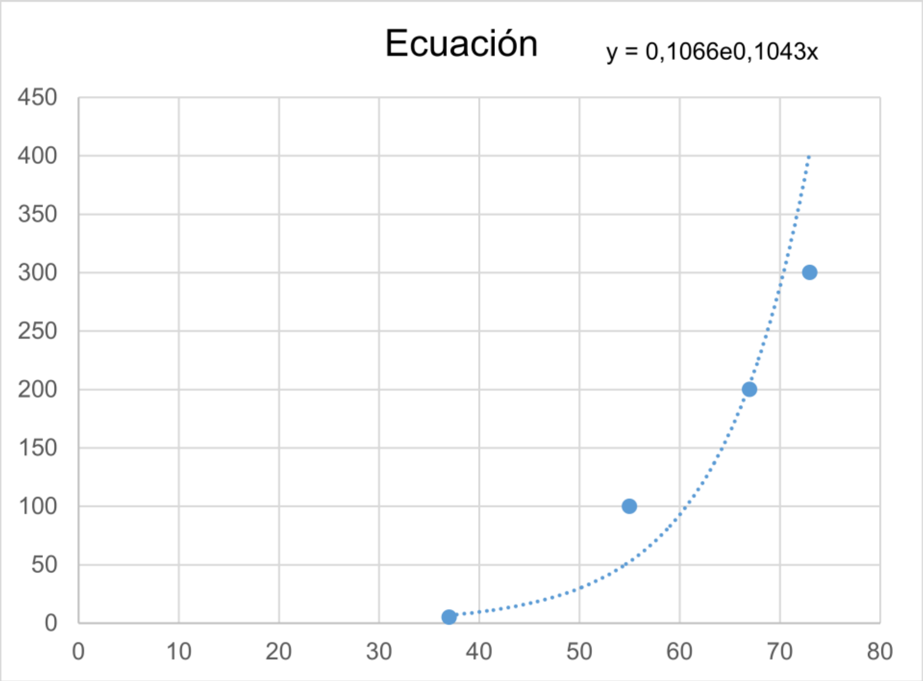


Figura 10 Ecuación de interpolación.

3.2.2 Conexión Xbee - Arduino

Inicialmente se debe conectar el módulo Xbee S1 al Arduino Uno, esto se lo realiza mediante una placa Xbee Explorer, como se muestra en la siguiente figura:

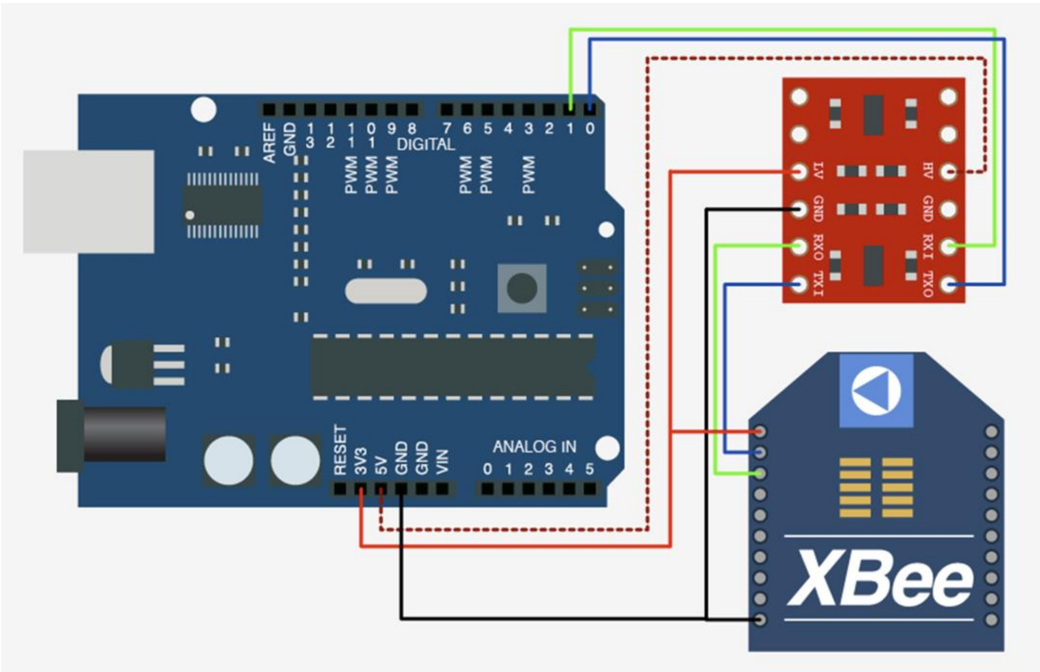


Figura 11 Diagrama conexión Xbee – Xbee Xplorer – Arduino Uno.

Una vez realizada la conexión entre estos módulos se procede con la programación del Arduino Uno.

3.2.3 Programación del Arduino Uno

Para programar el Arduino con el fin que reciba la información del Xbee se coloca el módulo XBee S1 en el Arduino Uno, que tiene el microcontrolador, a este se lo programa con un código que envía vía serial los datos de posición y MAC del nodo en hexadecimal.

En la siguiente imagen se detalla la conexión entre los Pin de un Xbee con un Arduino.

Pin connections between Arduino and XBee

XBee	Arduino
VCC or 3.3 V	3V3
TX or DOUT	RX or 0
RX or DIN	TX or 1
GND	GND

Figura 12 Pines conexión arduino – xbee.

Una vez que se tiene todos los datos en el Arduino se procede a pasar los mismos a la laptop que será la encargada de representarlos a través de la interfaz gráfica.

3.2.4 Programación de la interfaz gráfica

La interfaz gráfica ha sido desarrollada mediante el lenguaje de programación C# y ha sido plasmada a través del IDE (Entorno de desarrollo integrado) Microsoft Visual Studio.

En esta interfaz se muestran los datos enviados por los módulos Xbee S1.

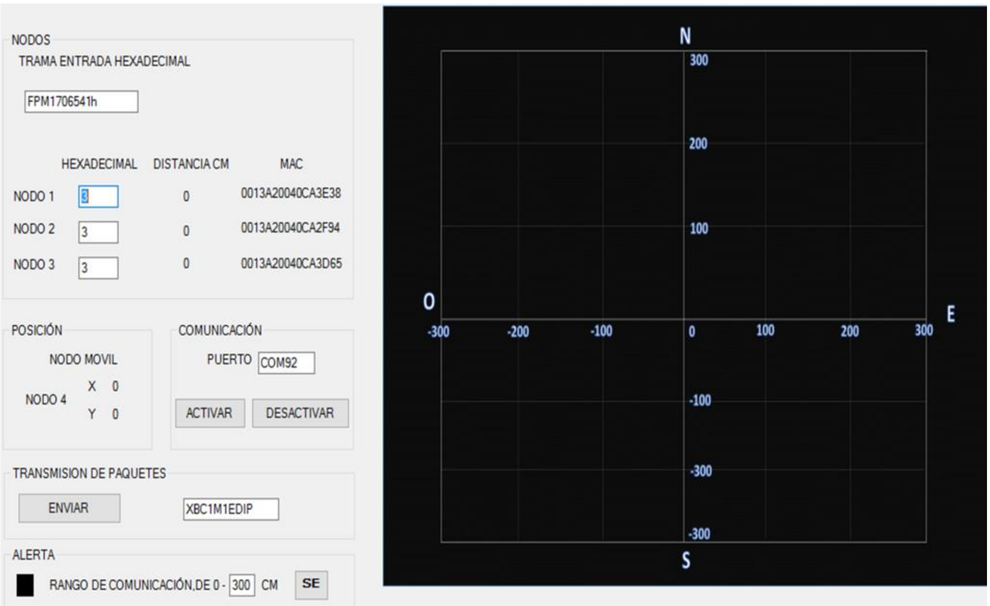


Figura 13 GUI para visualizar el funcionamiento del algoritmo.

3.3 Escenario de Pruebas

Para realizar la validación del funcionamiento del algoritmo, se plantea el siguiente escenario de pruebas:

Se plantean 3 nodos que permiten realizar el cálculo de la trilatearción Nodo 1, Nodo 2, Nodo 3; el Nodo 4 es el nodo móvil, sobre el cual se va a realizar el control de posicionamiento.

Cuando el Nodo 4 que es el nodo móvil se aleje más de 3 metros de los nodos de trilateración, se va a visualizar la alerta.
El nodo móvil empieza a enviar toda clase de información a través de la red, para fines prácticos; la información escogida para mostrarla en la interfaz gráfica es su identificación o en otros términos su nombre.

Con este simple escenario de pruebas se demuestra la implementación del algoritmo.

3.3.1 Simulación

A continuación se muestran los datos de entrada para la simulación.

Tabla 6 Datos entrada Nodos 1, 2, 3.

Nodo	MAC	Distancia del Nodo 4
1	0013A20040CA3E38	182
2	0013A20040CA2F94	109
3	0013A20040CA3D65	9

Con esos datos de entrada se obtiene la posición del Nodo 4 dando como resultado la posición en X=185 y en Y=205; así mismo se recibo el nombre del dispositivo (XBC1M1EDIP).

Como se observa en la siguiente figura, no se visualiza alerta debido a que está dentro del rango establecido (3 metros).

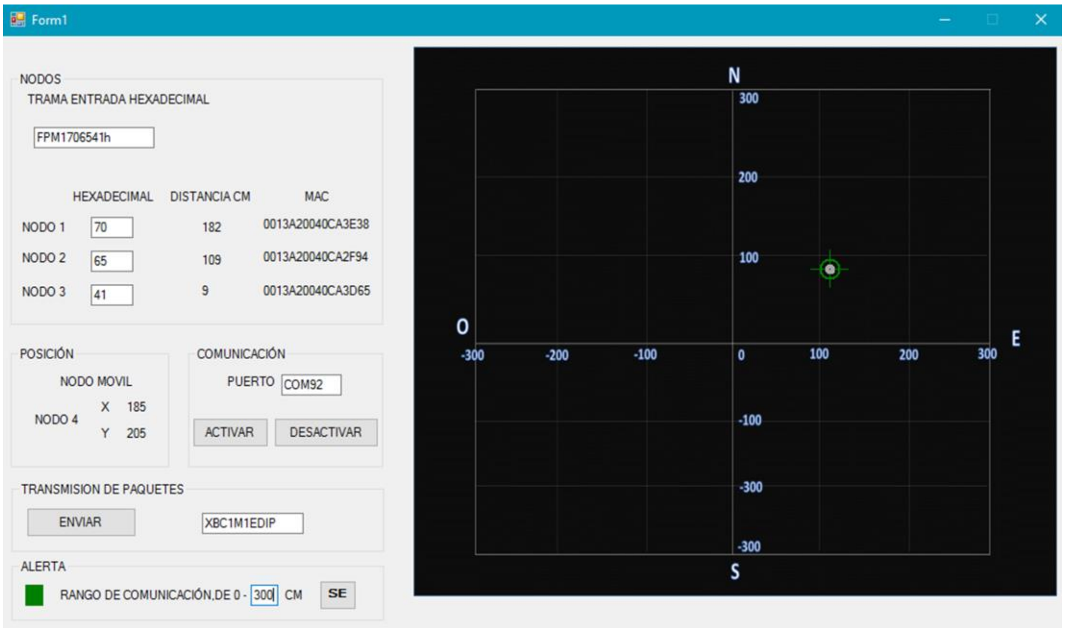


Figura 14 Resultado simulación dentro del rango.

Una vez que el nodo se desplaza a través del escenario, se obtienen nuevos datos.

Tabla 7 Datos entrada Nodos 1, 2, 3.

Nodo	MAC	Distancia del Nodo 4
1	0013A20040CA3E38	300
2	0013A20040CA2F94	140
3	0013A20040CA3D65	117

Con esos datos de entrada se obtiene la posición del Nodo 4 dando como resultado la posición en X=267 y en Y=277; así mismo se recibo el nombre del dispositivo (XBC1M1EDIP).

Como se observa en la siguiente figura, se visualiza una alerta debido a que el nodo está fuera del rango establecido (3 metros).

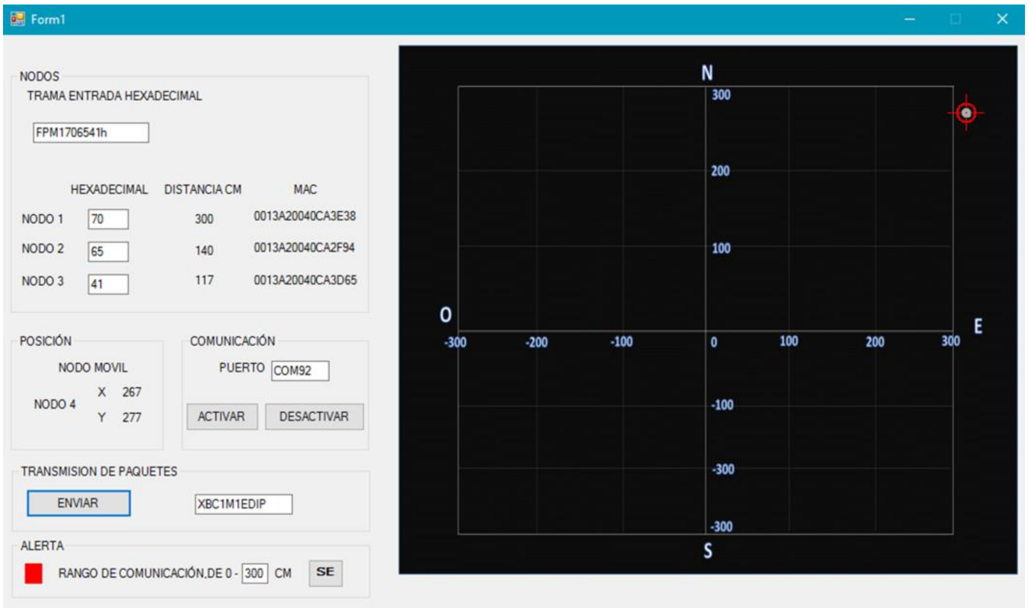


Figura 15 Resultado simulación fuera del rango.

Con esta simulación se ha logrado validar el correcto funcionamiento del algoritmo, y el cumpliendo de los requisitos de diseño.

4. CONCLUSIONES Y RECOMENDACIONES

En este capítulo se da a conocer las conclusiones y recomendaciones que se han obtenido luego de la evaluación del desempeño del algoritmo desarrollado en este proyecto.

4.1 Conclusiones

Tras el desarrollo de este proyecto, se han cubierto los objetivos planteados, puesto que se ha desarrollado con éxito un algoritmo que es capaz de conseguir el posicionamiento de nodos de una red MANET, el mismo que cuenta con los mínimos requisitos de diseño establecidos.

El protocolo de enrutamiento AODV está diseñado para redes móviles ad hoc con poblaciones de decenas de miles de nodos móviles. AODV puede manejar bajas, moderadas, y relativamente altas tasas de movilidad, así como una variedad de niveles de tráfico de datos.

AODV está diseñado para su uso en redes donde todos los nodos pueden confiar en los demás, porque se sabe que no hay nodos de intrusos maliciosos. AODV ha sido diseñado para reducir la difusión de control de tráfico y eliminar la sobrecarga en los datos de tráfico, con el fin de mejorar la escalabilidad y el rendimiento.

Los mecanismos de seguridad para las redes MANET se deben diseñar considerando las limitaciones de energía y ancho de banda.
El método de trilateración mediante el uso de las fórmulas ofrece una manera muy precisa de obtener matemáticamente la posición de los nodos.
Existen varios tipos de algoritmos de enrutamiento que de acuerdo al tipo de información que se va a manejar pueden resultan más útiles que otros, siempre se debe evaluar la funcionalidad que se le va a dar a red, previo a la elección de los protocolos.

4.2 Recomendaciones

La comunicación mediante dispositivos Xbee es altamente recomendable debido a que trabajan en la frecuencia libre de 2,4 GHz, y trabajan con el estándar IEEE 802.15.4 que provee un marco referencial para la implementación y desarrollo de nuevas formas de comunicación.

Se recomienda el uso de las redes MANET debido a que son sistemas de baja transferencia de datos, bajo consumo de energía y de bajo costo, con esta características compiten favorablemente contra otros tipos de redes móviles. A pesar de su relativa simplicidad comparada con otros estándares, este provee confiabilidad, flexibilidad y escalabilidad.

Debido a que dentro de las redes MANET se maneja tráfico tanto en tiempo real como en tiempo no real, se puede visualizar la posibilidad de que estas redes permitan elegir libremente y de acuerdo al tipo de tráfico que se maneje; una combinación de 2 tipos de protocolos tanto de transmisión en tiempo real como no real.

REFERENCIAS

Aldabbas, H., Alwadan, T., & Janicke, H. (2012). *Data Confidentiality in Mobile Ad hoc Networks.* (Vol. 4). Leicester, Inglaterra: International Journal of Wireless & Mobile Networks (IJWMN).

Christensson, P. (2006). *Ad Hoc Network Definition.* Recuperado el 12 de Mayo de 2016, de http://techterms.com

Clausen, T., & Jacquet, P. (2003). *Optimized Link State Routing Protocol (OLSR).* Recuperado el 15 de Mayo de 2016, de https://www.ietf.org/rfc/rfc3626.txt

Corson, S., & Macker, J. (1999). *Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations.* Recuperado el 12 de Mayo de 2016, de http://tools.ietf.org/html/rfc2501

IEEE. (s.f.). *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* Recuperado el 15 de Mayo de 2016, de http://standards.ieee.org/getieee802/download/802.11-2012.pdf

Johnson, D. (2007). *The Dynamic Source Routing Protocol (DSR).* Recuperado el 15 de Mayo de 2016, de https://www.rfc-editor.org/rfc/pdfrfc/rfc4728.txt.pdf

Loo, J., Lloret, J., & Hamilton, J. (2011). *Mobile Ad Hoc Networks: Current Status and Future Trends.* Florida, Estados Unidos: Taylor & Francis Group, LLC.

Manoj, C. (2004). *Ad Hoc Wireless Networks Architectures and Protocols.* Prentice Hall Communications Engineering and Emerging Technologies Series.

Murthy, S., & García, J. (1996). *An Efficient Routing Protocol for Wireless Networks.* Santa Cruz, Estados Unidos: Springer-Verlag.

Perkins, C. (2003). *Ad hoc On-Demand Distance Vector (AODV) Routing.* Recuperado el 15 de Mayo de 2016, de https://www.rfc-editor.org/rfc/rfc3561.txt

Perkins, C., & Bhagwat, P. (1994). *Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers.* Londres, Inglaterra: ACM SIGCOMM 94.

Tanenbaum, A. S. (1996). *Computer Networks.* Nueva Jersey, Estados Unidos: Prentice Hall.

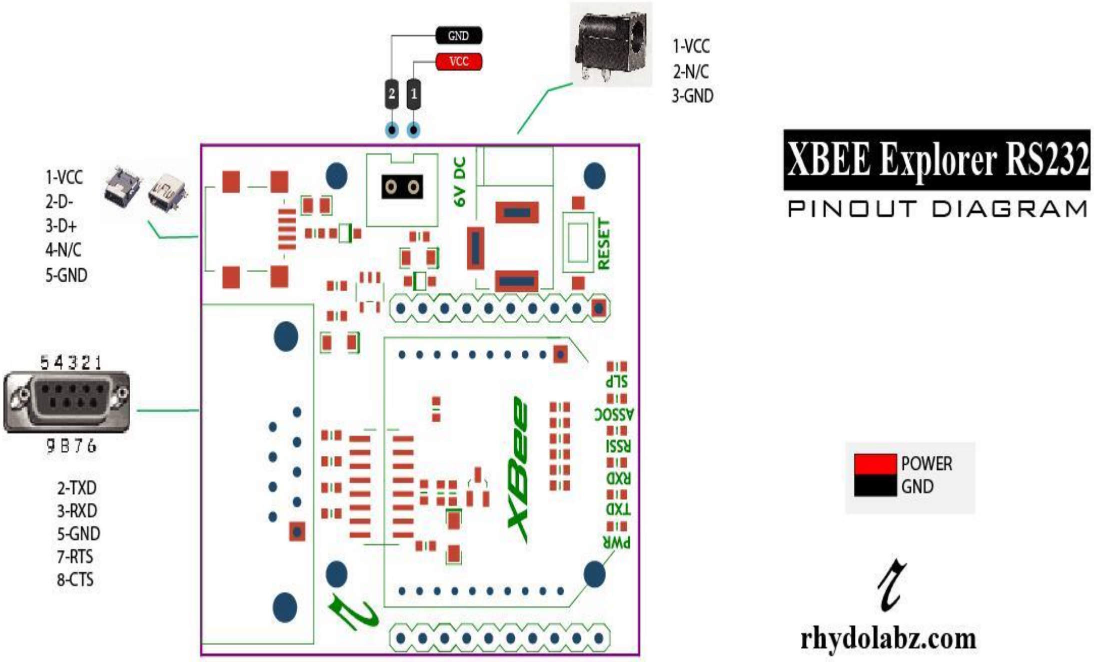
Toh, C. (1997). *Associativity-Based Routing for Ad-Hoc Mobile Networks.* Cambridge, Inglaterra: Kluwer Academic Publishers.

Toh, C. (1999). *Long-lived Ad Hoc Routing based on the Concept of Associativity.* Recuperado el 15 de Mayo de 2016, de https://www.ietf.org/proceedings/46/I-D/draft-ietf-MANET-longlived-adhoc-routing-00.txt

ANEXOS

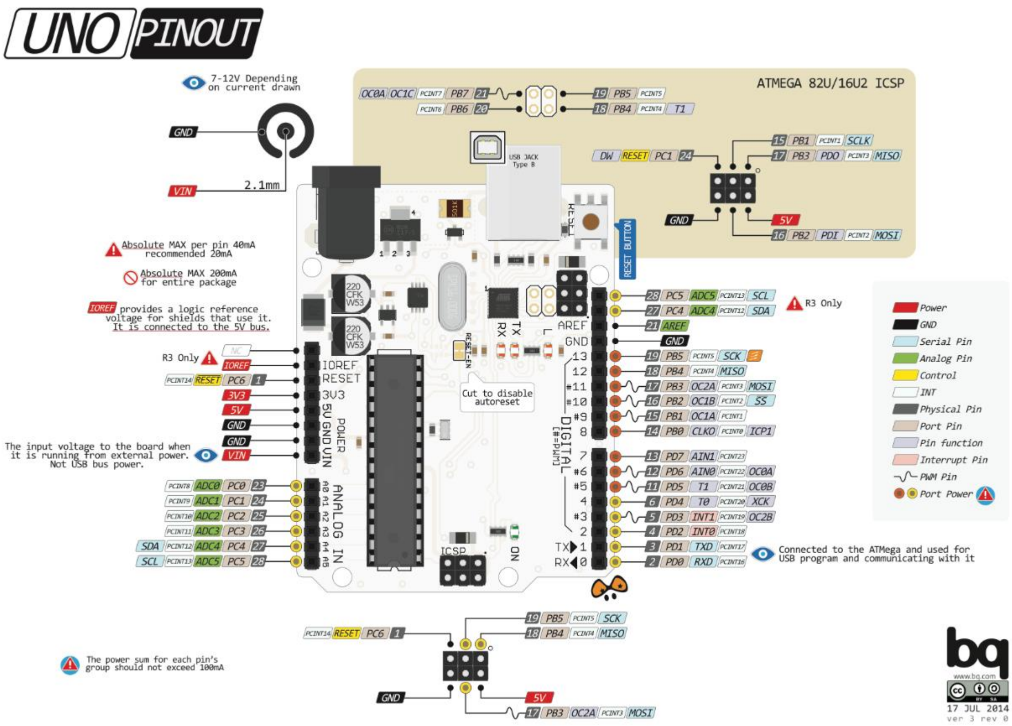
ANEXO 1

Diagrama PinOut Xbee Xplorer



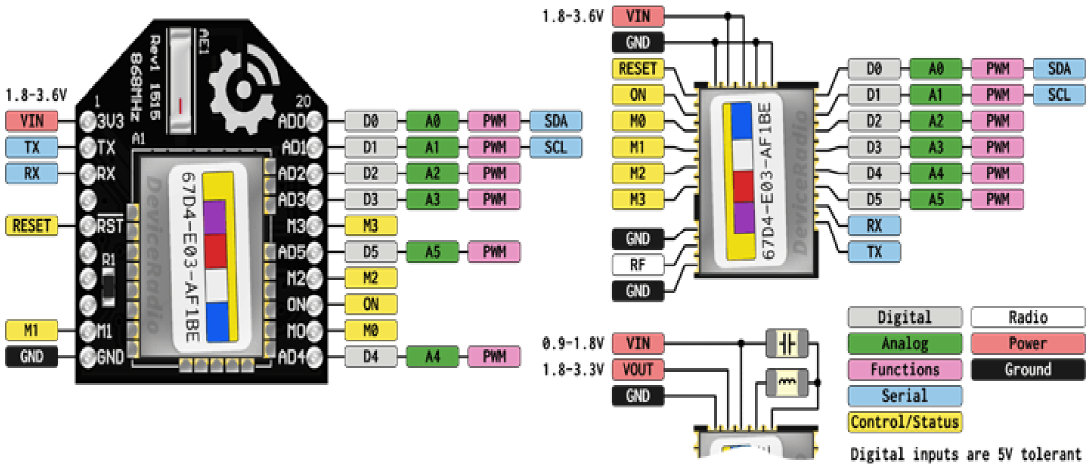
ANEXO 2

Diagrama PinOut Arduino Uno



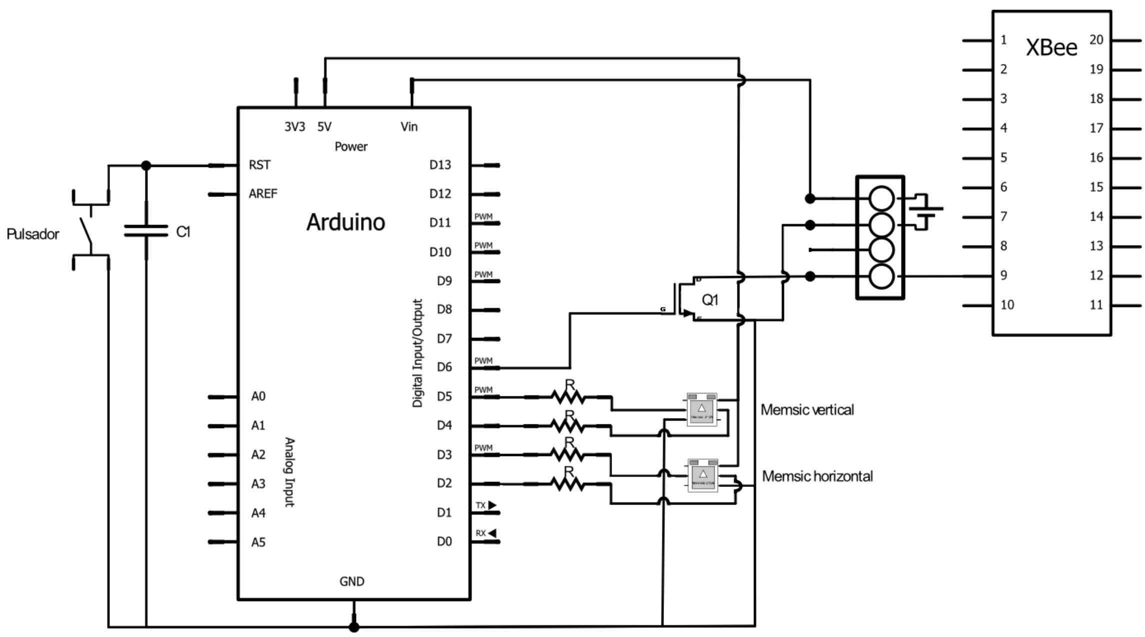
ANEXO 3

Diagrama PinOut Xbee S1



ANEXO 4

Diagrama Conexión Xbee - Arduino



ANEXO 5
Data Sheet Xbee

XBee®/XBee-PRO® RF Modules

Product Manual v1.xEx - 802.15.4 Protocol

For RF Module Part Numbers: XB24-A...-001, XBP24-A...-001

IEEE® 802.15.4 RF Modules by Digi International

Digi International Inc.
11001 Bren Road East
Minnetonka, MN 55343
877 912-3444 or 952 912-3444
http://www.digi.com

90000982_B
2009.09.23

Technical Support:	Phone:	(866) 765-9885 toll-free U.S.A. & Canada (801) 765-9885 Worldwide 8:00 am - 5:00 pm [U.S. Mountain Time]
	Live Chat:	www.digi.com
	Online Support:	http://www.digi.com/support/eservice/login.jsp
	Email:	rf-experts@digi.com

Contents

1. XBee®/XBee-PRO® RF Modules

The XBee and XBee-PRO RF Modules were engineered to meet IEEE 802.15.4 standards and support the unique needs of low-cost, low-power wireless sensor networks. The modules require minimal power and provide reliable delivery of data between devices.

The modules operate within the ISM 2.4 GHz frequency band and are pin-for-pin compatible with each other.

Key Features

Long Range Data Integrity

XBee

- Indoor/Urban: up to 100’ (30 m)
- Outdoor line-of-sight: up to 300’ (90 m)
- Transmit Power: 1 mW (0 dBm)
- Receiver Sensitivity: -92 dBm

XBee-PRO

- Indoor/Urban: up to 300’ (90 m), 200' (60 m) for International variant
- Outdoor line-of-sight: up to 1 mile (1600 m), 2500' (750 m) for International variant
- Transmit Power: 63mW (18dBm), 10mW (10dBm) for International variant
- Receiver Sensitivity: -100 dBm

RF Data Rate: 250,000 bps

Advanced Networking & Security

Retries and Acknowledgements

DSSS (Direct Sequence Spread Spectrum)

Each direct sequence channels has over 65,000 unique network addresses available

Source/Destination Addressing

Unicast & Broadcast Communications

Point-to-point, point-to-multipoint and peer-to-peer topologies supported

Low Power

XBee

- TX Peak Current: 45 mA (@3.3 V)
- RX Current: 50 mA (@3.3 V)
- Power-down Current: < 10 µA

XBee-PRO

- TX Peak Current: 250mA (150mA for international variant)
- TX Peak Current (RPSMA module only): 340mA (180mA for international varian
- RX Current: 55 mA (@3.3 V)
- Power-down Current: < 10 µA

ADC and I/O line support

Analog-to-digital conversion, Digital I/O

I/O Line Passing

Easy-to-Use

No configuration necessary for out-of box RF communications

Free X-CTU Software (Testing and configuration software)

AT and API Command Modes for configuring module parameters

Extensive command set

Small form factor

Worldwide Acceptance

FCC Approval (USA) Refer to Appendix A [p64] for FCC Requirements.

Systems that contain XBee®/XBee-PRO® RF Modules inherit Digi Certifications.
ISM (Industrial, Scientific & Medical) **2.4 GHz frequency band**

Manufactured under **ISO 9001:2000** registered standards

XBee®/XBee-PRO® RF Modules are optimized for use in the United States, Canada, Australia, Japan, and Europe. Contact Digi for complete list of government agency approvals.

Specifications

Table 1-01. Specifications of the XBee®/XBee-PRO® RF Modules

Specification	XBee	XBee-PRO
Performance		
Indoor/Urban Range	Up to 100 ft (30 m)	Up to 300 ft. (90 m), up to 200 ft (60 m) International variant
Outdoor RF line-of-sight Range	Up to 300 ft (90 m)	Up to 1 mile (1600 m), up to 2500 ft (750 m) international variant
Transmit Power Output (software selectable)	1mW (0 dBm)	63mW (18dBm)* 10mW (10 dBm) for International variant
RF Data Rate	250,000 bps	250,000 bps
Serial Interface Data Rate (software selectable)	1200 bps - 250 kbps (non-standard baud rates also supported)	1200 bps - 250 kbps (non-standard baud rates also supported)
Receiver Sensitivity	-92 dBm (1% packet error rate)	-100 dBm (1% packet error rate)
Power Requirements		
Supply Voltage	2.8 – 3.4 V	2.8 – 3.4 V
Transmit Current (typical)	45mA (@ 3.3 V)	250mA (@3.3 V) (150mA for international variant) RPSMA module only: 340mA (@3.3 V) (180mA for international variant)
Idle / Receive Current (typical)	50mA (@ 3.3 V)	55mA (@ 3.3 V)
Power-down Current	< 10 µA	< 10 µA
General		
Operating Frequency	ISM 2.4 GHz	ISM 2.4 GHz
Dimensions	0.960" x 1.087" (2.438cm x 2.761cm)	0.960" x 1.297" (2.438cm x 3.294cm)
Operating Temperature	-40 to 85° C (industrial)	-40 to 85° C (industrial)
Antenna Options	Integrated Whip, Chip or U.FL Connector, RPSMA Connector	Integrated Whip, Chip or U.FL Connector, RPSMA Connector
Networking & Security		
Supported Network Topologies	Point-to-point, Point-to-multipoint & Peer-to-peer	
Number of Channels (software selectable)	16 Direct Sequence Channels	12 Direct Sequence Channels
Addressing Options	PAN ID, Channel and Addresses	PAN ID, Channel and Addresses
Agency Approvals		
United States (FCC Part 15.247)	OUR-XBEE	OUR-XBEEPRO
Industry Canada (IC)	4214A XBEE	4214A XBEEPRO
Europe (CE)	ETSI	ETSI (Max. 10 dBm transmit power output)*
Japan	R201WW07215214	R201WW08215111 (Max. 10 dBm transmit power output)*
Austraila	C-Tick	C-Tick

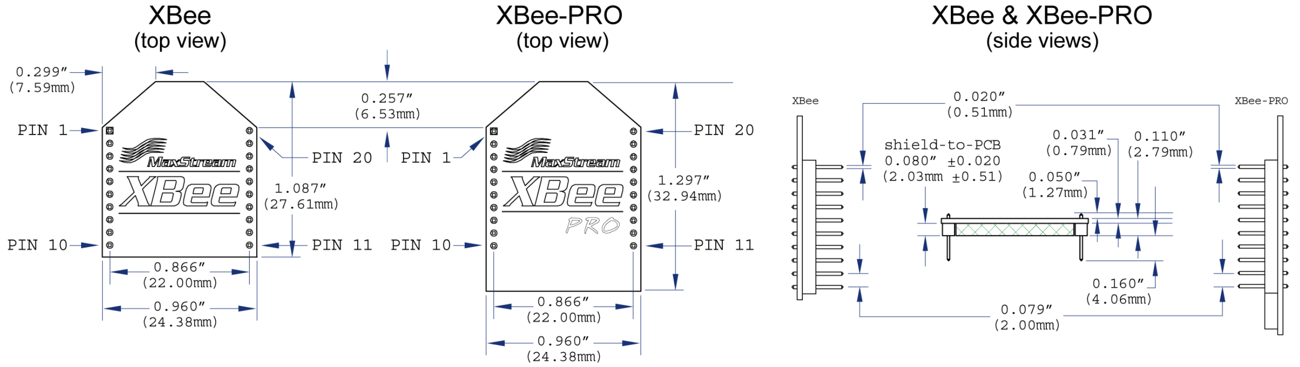
* See Appendix A for region-specific certification requirements.

Antenna Options: The ranges specified are typical when using the integrated Whip (1.5 dBi) and Dipole (2.1 dBi) antennas. The Chip antenna option provides advantages in its form factor; however, it typically yields shorter range than the Whip and Dipole antenna options when transmitting outdoors.For more information, refer to the "XBee Antennas" Knowledgebase Article located on Digi's Support Web site

Mechanical Drawings

Figure 1-01. Mechanical drawings of the XBee®/XBee-PRO® RF Modules (antenna options not shown)

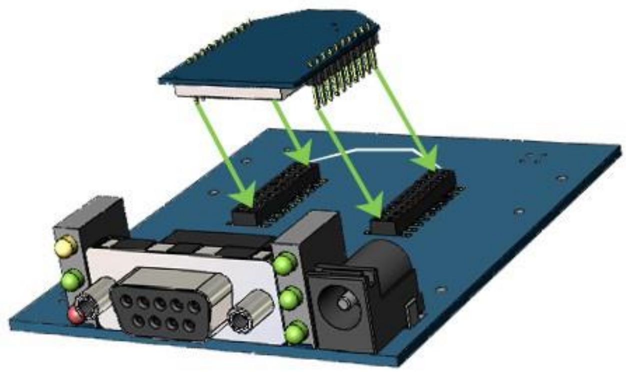
The XBee and XBee-PRO RF Modules are pin-for-pin compatible.



Mounting Considerations

The XBee®/XBee-PRO® RF Module was designed to mount into a receptacle (socket) and therefore does not require any soldering when mounting it to a board. The XBee Development Kits contain RS-232 and USB interface boards which use two 20-pin receptacles to receive modules.

Figure 1-02. XBee Module Mounting to an RS-232 Interface Board.



The receptacles used on Digi development boards are manufactured by Century Interconnect. Several other manufacturers provide comparable mounting solutions; however, Digi currently uses the following receptacles:

- Through-hole single-row receptacles -
  Samtec P/N: MMS-110-01-L-SV (or equivalent)
- Surface-mount double-row receptacles -
  Century Interconnect P/N: CPRMSL20-D-0-1 (or equivalent)
- Surface-mount single-row receptacles -
  Samtec P/N: SMM-110-02-SM-S

Digi also recommends printing an outline of the module on the board to indicate the orientation the module should be mounted.

Pin Signals

Figure 1-03. XBee®/XBee-PRO® RF Module Pin Numbers

(top sides shown - shields on bottom)

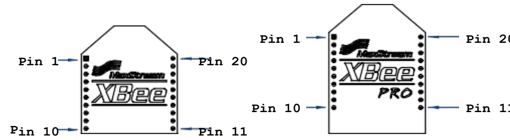


Table 1-02. Pin Assignments for the XBee and XBee-PRO Modules
(Low-asserted signals are distinguished with a horizontal line above signal name.)

Pin #	Name	Direction	Description
1	VCC	-	Power supply
2	DOUT	Output	UART Data Out
3	DIN / **CONFIG**	Input	UART Data In
4	DO8*	Output	Digital Output 8
5	**RESET**	Input	Module Reset (reset pulse must be at least 200 ns)
6	PWM0 / RSSI	Output	PWM Output 0 / RX Signal Strength Indicator
7	PWM1	Output	PWM Output 1
8	[reserved]	-	Do not connect
9	DTR / SLEEP_RQ / DI8	Input	Pin Sleep Control Line or Digital Input 8
10	GND	-	Ground
11	AD4 / DIO4	Either	Analog Input 4 or Digital I/O 4
12	**CTS** / DIO7	Either	Clear-to-Send Flow Control or Digital I/O 7
13	ON / **SLEEP**	Output	Module Status Indicator
14	VREF	Input	Voltage Reference for A/D Inputs
15	Associate / AD5 / DIO5	Either	Associated Indicator, Analog Input 5 or Digital I/O 5
16	**RTS** / AD6 / DIO6	Either	Request-to-Send Flow Control, Analog Input 6 or Digital I/O 6
17	AD3 / DIO3	Either	Analog Input 3 or Digital I/O 3
18	AD2 / DIO2	Either	Analog Input 2 or Digital I/O 2
19	AD1 / DIO1	Either	Analog Input 1 or Digital I/O 1
20	AD0 / DIO0	Either	Analog Input 0 or Digital I/O 0

* Function is not supported at the time of this release

Design Notes:

- Minimum connections: VCC, GND, DOUT & DIN
- Minimum connections for updating firmware: VCC, GND, DIN, DOUT, RTS & DTR
- Signal Direction is specified with respect to the module
- Module includes a 50k ∧ pull-up resistor attached to **RESET**
- Several of the input pull-ups can be configured using the PR command
- Unused pins should be left disconnected

Electrical Characteristics

Table 1-03. DC Characteristics (VCC = 2.8 - 3.4 VDC)

Symbol	Characteristic	Condition	Min	Typical	Max	Unit
V_{IL}	Input Low Voltage	All Digital Inputs	-	-	0.35 * VCC	V
V_{IH}	Input High Voltage	All Digital Inputs	0.7 * VCC	-	-	V
V_{OL}	Output Low Voltage	I_{OL} = 2 mA, VCC >= 2.7 V	-	-	0.5	V
V_{OH}	Output High Voltage	I_{OH} = -2 mA, VCC >= 2.7 V	VCC - 0.5	-	-	V
II_{IN}	Input Leakage Current	V_{IN} = VCC or GND, all inputs, per pin	-	0.025	1	μA
II_{OZ}	High Impedance Leakage Current	V_{IN} = VCC or GND, all I/O High-Z, per pin	-	0.025	1	μA
TX	Transmit Current	VCC = 3.3 V	-	45 (XBee) / 215, 140 (PRO, Int)	-	mA
RX	Receive Current	VCC = 3.3 V	-	50 (XBee) / 55 (PRO)	-	mA
PWR-DWN	Power-down Current	SM parameter = 1	-	< 10	-	μA

Table 1-04. ADC Characteristics (Operating)

Symbol	Characteristic	Condition	Min	Typical	Max	Unit
V_{REFH}	VREF - Analog-to-Digital converter reference range		2.08	-	V_{DDAD}*	V
I_{REF}	VREF - Reference Supply Current	Enabled	-	200	-	μA
		Disabled or Sleep	-	< 0.01	0.02	μA
V_{INDC}	Analog Input Voltage[1]		V_{SSAD} - 0.3	-	V_{DDAD} + 0.3	V

1. Maximum electrical operating range, not valid conversion range.

* V_{DDAD} is connected to VCC.

Table 1-05. ADC Timing/Performance Characteristics[1]

Symbol	Characteristic	Condition	Min	Typical	Max	Unit
R_{AS}	Source Impedance at Input[2]		-	-	10	k Ω
V_{AIN}	Analog Input Voltage[3]		V_{REFL}		V_{REFH}	V
RES	Ideal Resolution (1 LSB)[4]	2.08V < V_{DDAD} < 3.6V	2.031	-	3.516	mV
DNL	Differential Non-linearity[5]		-	±0.5	±1.0	LSB
INL	Integral Non-linearity[6]		-	±0.5	±1.0	LSB
E_{ZS}	Zero-scale Error[7]		-	±0.4	±1.0	LSB
F_{FS}	Full-scale Error[8]		-	±0.4	±1.0	LSB
E_{IL}	Input Leakage Error[9]		-	±0.05	±5.0	LSB
E_{TU}	Total Unadjusted Error[10]		-	±1.1	±2.5	LSB

1. All ACCURACY numbers are based on processor and system being in WAIT state (very little activity and no IO switching) and that adequate low-pass filtering is present on analog input pins (filter with 0.01 μF to 0.1 μF capacitor between analog input and VREFL). Failure to observe these guidelines may result in system or microcontroller noise causing accuracy errors which will vary based on board layout and the type and magnitude of the activity.

Data transmission and reception during data conversion may cause some degradation of these specifications, depending on the number and timing of packets. It is advisable to test the ADCs in your installation if best accuracy is required.

2. R_{AS} is the real portion of the impedance of the network driving the analog input pin. Values greater than this amount may not fully charge the input circuitry of the ATD resulting in accuracy error.
3. Analog input must be between V_{REFL} and V_{REFH} for valid conversion. Values greater than V_{REFH} will convert to $3FF.
4. The resolution is the ideal step size or 1LSB = $(V_{REFH}–V_{REFL})/1024$
5. Differential non-linearity is the difference between the current code width and the ideal code width (1LSB). The current code width is the difference in the transition voltages to and from the current code.
6. Integral non-linearity is the difference between the transition voltage to the current code and the adjusted ideal transition voltage for the current code. The adjusted ideal transition voltage is (Current Code–1/2)*$(1/((V_{REFH}+E_{FS})–(V_{REFL}+E_{ZS})))$.
7. Zero-scale error is the difference between the transition to the first valid code and the ideal transition to that code. The Ideal transition voltage to a given code is (Code–1/2)*$(1/(V_{REFH}–V_{REFL}))$.
8. Full-scale error is the difference between the transition to the last valid code and the ideal transition to that code. The ideal transition voltage to a given code is (Code–1/2)*$(1/(V_{REFH}–V_{REFL}))$.
9. Input leakage error is error due to input leakage across the real portion of the impedance of the network driving the analog pin. Reducing the impedance of the network reduces thiserror.

10. Total unadjusted error is the difference between the transition voltage to the current code and the ideal straight-line transfer function. This measure of error includes inherent quantization error (1/2LSB) and circuit error (differential, integral, zero-scale, and full-scale) error. The specified value of E_{TU} assumes zero E_{IL} (no leakage or zero real source impedance).

2. RF Module Operation

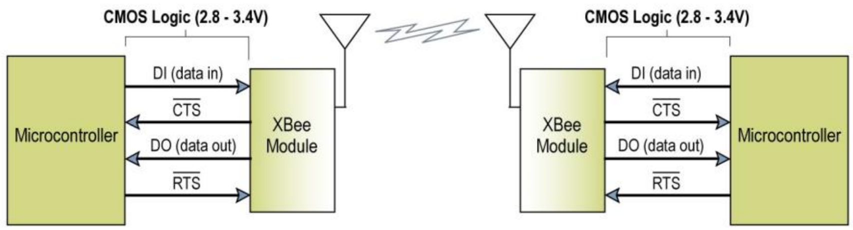
Serial Communications

The XBee®/XBee-PRO® RF Modules interface to a host device through a logic-level asynchronous serial port. Through its serial port, the module can communicate with any logic and voltage compatible UART; or through a level translator to any serial device (For example: Through a Digi proprietary RS-232 or USB interface board).

UART Data Flow

Devices that have a UART interface can connect directly to the pins of the RF module as shown in the figure below.

Figure 2-01. System Data Flow Diagram in a UART-interfaced environment
(Low-asserted signals distinguished with horizontal line over signal name.)

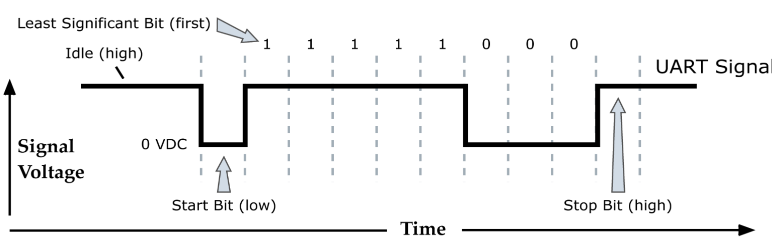


Serial Data

Data enters the module UART through the DI pin (pin 3) as an asynchronous serial signal. The signal should idle high when no data is being transmitted.

Each data byte consists of a start bit (low), 8 data bits (least significant bit first) and a stop bit (high). The following figure illustrates the serial bit pattern of data passing through the module.

Figure 2-02. UART data packet 0x1F (decimal number "31") as transmitted through the RF module
Example Data Format is 8-N-1 (bits - parity - # of stop bits)



Serial communications depend on the two UARTs (the microcontroller's and the RF module's) to be configured with compatible settings (baud rate, parity, start bits, stop bits, data bits).

The UART baud rate and parity settings on the XBee module can be configured with the BD and SB commands, respectively. See the command table in Chapter 3 for details.

Transparent Operation

By default, XBee®/XBee-PRO® RF Modules operate in Transparent Mode. When operating in this mode, the modules act as a serial line replacement - all UART data received through the DI pin is queued up for RF transmission. When RF data is received, the data is sent out the DO pin.

Serial-to-RF Packetization

Data is buffered in the DI buffer until one of the following causes the data to be packetized and transmitted:

1. No serial characters are received for the amount of time determined by the RO (Packetization Timeout) parameter. If RO = 0, packetization begins when a character is received.
2. The maximum number of characters that will fit in an RF packet (100) is received.
3. The Command Mode Sequence (GT + CC + GT) is received. Any character buffered in the DI buffer before the sequence is transmitted.

If the module cannot immediately transmit (for instance, if it is already receiving RF data), the serial data is stored in the DI Buffer. The data is packetized and sent at any RO timeout or when 100 bytes (maximum packet size) are received.

If the DI buffer becomes full, hardware or software flow control must be implemented in order to prevent overflow (loss of data between the host and module).

API Operation

API (Application Programming Interface) Operation is an alternative to the default Transparent Operation. The frame-based API extends the level to which a host application can interact with the networking capabilities of the module.

When in API mode, all data entering and leaving the module is contained in frames that define operations or events within the module.

Transmit Data Frames (received through the DI pin (pin 3)) include:

- RF Transmit Data Frame
- Command Frame (equivalent to AT commands)

Receive Data Frames (sent out the DO pin (pin 2)) include:

- RF-received data frame
- Command response
- Event notifications such as reset, associate, disassociate, etc.

The API provides alternative means of configuring modules and routing data at the host application layer. A host application can send data frames to the module that contain address and payload information instead of using command mode to modify addresses. The module will send data frames to the application containing status packets; as well as source, RSSI and payload information from received data packets.

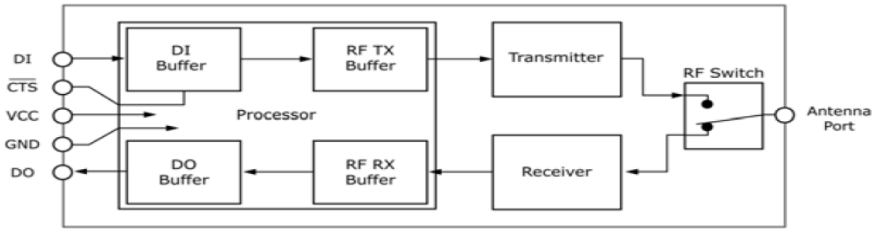
The API operation option facilitates many operations such as the examples cited below:

-> Transmitting data to multiple destinations without entering Command Mode
-> Receive success/failure status of each transmitted RF packet
-> Identify the source address of each received packet

To implement API operations, refer to API sections [p57].

Flow Control

Figure 2-03. Internal Data Flow Diagram



DI (Data In) Buffer

When serial data enters the RF module through the DI pin (pin 3), the data is stored in the DI Buffer until it can be processed.

Hardware Flow Control (CTS). When the DI buffer is 17 bytes away from being full; by default, the module de-asserts CTS (high) to signal to the host device to stop sending data [refer to D7 (DIO7 Configuration) parameter]. CTS is re-asserted after the DI Buffer has 34 bytes of memory available.

How to eliminate the need for flow control:

1. Send messages that are smaller than the DI buffer size (202 bytes).
2. Interface at a lower baud rate [BD (Interface Data Rate) parameter] than the throughput data rate.

Case in which the DI Buffer may become full and possibly overflow:

If the module is receiving a continuous stream of RF data, any serial data that arrives on the DI pin is placed in the DI Buffer. The data in the DI buffer will be transmitted over-the-air when the module is no longer receiving RF data in the network.

Refer to the RO (Packetization Timeout), BD (Interface Data Rate) and D7 (DIO7 Configuration) command descriptions for more information.

DO (Data Out) Buffer

When RF data is received, the data enters the DO buffer and is sent out the serial port to a host device. Once the DO Buffer reaches capacity, any additional incoming RF data is lost.

Hardware Flow Control (RTS). If RTS is enabled for flow control (D6 (DIO6 Configuration) Parameter = 1), data will not be sent out the DO Buffer as long as RTS (pin 16) is de-asserted.

Two cases in which the DO Buffer may become full and possibly overflow:

1. If the RF data rate is set higher than the interface data rate of the module, the module will receive data from the transmitting module faster than it can send the data to the host.
2. If the host does not allow the module to transmit data out from the DO buffer because of being held off by hardware or software flow control.

Refer to the D6 (DIO6 Configuration) command description for more information.

ADC and Digital I/O Line Support

The XBee®/XBee-PRO® RF Modules support ADC (Analog-to-digital conversion) and digital I/O line passing. The following pins support multiple functions:

Table 2-01. Pin functions and their associated pin numbers and commands
AD = Analog-to-Digital Converter, DIO = Digital Input/Output
Pin functions not applicable to this section are denoted within (parenthesis).

Pin Function	Pin#	AT Command
AD0 / DIO0	20	D0
AD1 / DIO1	19	D1
AD2 / DIO2	18	D2
AD3 / DIO3 / (COORD_SEL)	17	D3
AD4 / DIO4	11	D4
AD5 / DIO5 / (ASSOCIATE)	15	D5
DIO6 / (RTS)	16	D6
DIO7 / (CTS)	12	D7
DI8 / (DTR) / (Sleep_RQ)	9	D8

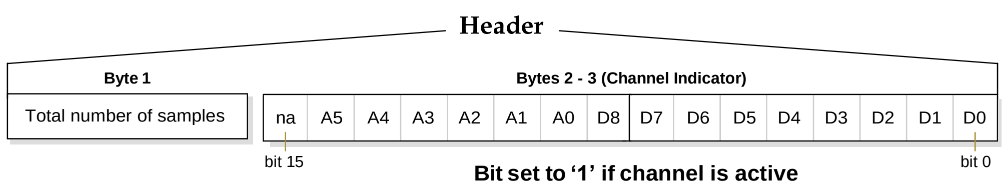
To enable ADC and DIO pin functions:

For ADC Support:	Set ATDn = 2
For Digital Input support:	Set ATDn = 3
For Digital Output Low support:	Set ATDn = 4
For Digital Output High support:	Set ATDn = 5

I/O Data Format

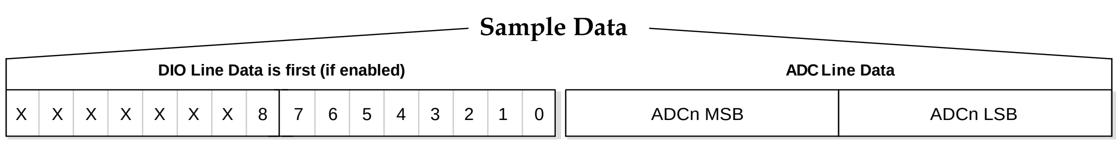
I/O data begins with a header. The first byte of the header defines the number of samples forth-coming. The last 2 bytes of the header (Channel Indicator) define which inputs are active. Each bit represents either a DIO line or ADC channel.

Figure 2-04. Header



Sample data follows the header and the channel indicator frame is used to determine how to read the sample data. If any of the DIO lines are enabled, the first 2 bytes are the DIO sample. The ADC data follows. ADC channel data is represented as an unsigned 10-bit value right-justified on a 16- bit boundary.

Figure 2-05. Sample Data



API Support

I/O data is sent out the UART using an API frame. All other data can be sent and received using Transparent Operation [refer to p11] or API framing if API mode is enabled (AP > 0).

API Operations support two RX (Receive) frame identifiers for I/O data (set 16-bit address to 0xFFFE and the module will do 64-bit addressing):

- 0x82 for RX (Receive) Packet: 64-bit address I/O
- 0x83 for RX (Receive) Packet: 16-bit address I/O

The API command header is the same as shown in the "RX (Receive) Packet: 64-bit Address" and "RX (Receive) Packet: 64-bit Address" API types [refer to p63]. RX data follows the format described in the I/O Data Format section [p13].

Applicable Commands: AP (API Enable)

Sleep Support

Automatic wakeup sampling can be suppressed by setting SO bit 1.When an RF module wakes, it will always do a sample based on any active ADC or DIO lines. This allows sampling based on the sleep cycle whether it be Cyclic Sleep (SM parameter = 4 or 5) or Pin Sleep (SM = 1 or 2). To gather more samples when awake, set the IR (Sample Rate) parameter.

For Cyclic Sleep modes: If the IR parameter is set, the module will stay awake until the IT (Samples before TX) parameter is met. The module will stay awake for ST (Time before Sleep) time.

Applicable Commands: IR (Sample Rate), IT (Samples before TX), SM (Sleep Mode), IC (DIO Change Detect), SO (Sleep Options)

DIO Pin Change Detect

When "DIO Change Detect" is enabled (using the IC command), DIO lines 0-7 are monitored. When a change is detected on a DIO line, the following will occur:

1. An RF packet is sent with the updated DIO pin levels. This packet will not contain any ADC samples.
2. Any queued samples are transmitted before the change detect data. This may result in receiving a packet with less than IT (Samples before TX) samples.

Note: Change detect will not affect Pin Sleep wake-up. The D8 pin (DTR/Sleep_RQ/DI8) is the only line that will wake a module from Pin Sleep. If not all samples are collected, the module will still enter Sleep Mode after a change detect packet is sent.

Applicable Commands: IC (DIO Change Detect), IT (Samples before TX)

NOTE: Change detect is only supported when the Dx (DIOx Configuration) parameter equals 3,4 or 5.

Sample Rate (Interval)

The Sample Rate (Interval) feature allows enabled ADC and DIO pins to be read periodically on modules that are not configured to operate in Sleep Mode. When one of the Sleep Modes is enabled and the IR (Sample Rate) parameter is set, the module will stay awake until IT (Samples before TX) samples have been collected.

Once a particular pin is enabled, the appropriate sample rate must be chosen. The maximum sample rate that can be achieved while using one A/D line is 1 sample/ms or 1 KHz (Note that the modem will not be able to keep up with transmission when IR & IT are equal to "1" and that configuring the modem to sample at rates greater than once every 20ms is not recommended).

Applicable Commands: IR (Sample Rate), IT (Samples before TX), SM (Sleep Mode)

I/O Line Passing

Virtual wires can be set up between XBee®/XBee-PRO® Modules. When an RF data packet is received that contains I/O data, the receiving module can be setup to update any enabled outputs (PWM and DIO) based on the data it receives.

Note that I/O lines are mapped in pairs. For example: AD0 can only update PWM0 and DI5 can only update DO5. The default setup is for outputs not to be updated, which results in the I/O data being sent out the UART (refer to the IU (Enable I/O Output) command). To enable the outputs to be updated, the IA (I/O Input Address) parameter must be setup with the address of the module that has the appropriate inputs enabled. This effectively binds the outputs to a particular module's input. This does not affect the ability of the module to receive I/O line data from other modules - only its ability to update enabled outputs. The IA parameter can also be setup to accept I/O data for output changes from any module by setting the IA parameter to 0xFFFF.

When outputs are changed from their non-active state, the module can be setup to return the output level to it non-active state. The timers are set using the Tn (Dn Output Timer) and PT (PWM Output Timeout) commands. The timers are reset every time a valid I/O packet (passed IA check) is received. The IC (Change Detect) and IR (Sample Rate) parameters can be setup to keep the output set to their active output if the system needs more time than the timers can handle.

Note: DI8 cannot be used for I/O line passing.

Applicable Commands: IA (I/O Input Address), Tn (Dn Output Timeout), P0 (PWM0 Configuration), P1 (PWM1 Configuration), M0 (PWM0 Output Level), M1 (PWM1 Output Level), PT (PWM Output Timeout), RP (RSSSI PWM Timer)

Configuration Example

As an example for a simple A/D link, a pair of RF modules could be set as follows:

Remote Configuration	Base Configuration
DL = 0x1234	DL = 0x5678
MY = 0x5678	MY = 0x1234
D0 = 2	P0 = 2
D1 = 2	P1 = 2
IR = 0x14	IU = 1
IT = 5	IA = 0x5678 (or 0xFFFF)

These settings configure the remote module to sample AD0 and AD1 once each every 20 ms. It then buffers 5 samples each before sending them back to the base module. The base should then receive a 32-Byte transmission (20 Bytes data and 12 Bytes framing) every 100 ms.

XBee®/XBee-PRO® Networks

The following terms will be used to explicate the network operations:

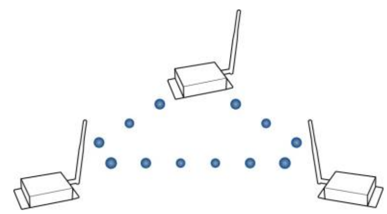
Table 2-02. Terms and definitions

Term	Definition
PAN	Personal Area Network - A data communication network that includes one or more End Devices and optionally a Coordinator.
Coordinator	A Full-function device (FFD) that provides network synchronization by polling nodes [NonBeacon (w/ Coordinator) networks only]
End Device	*When in the same network as a Coordinator* - RF modules that rely on a Coordinator for synchronization and can be put into states of sleep for low-power applications.
Association	The establishment of membership between End Devices and a Coordinator. Association is only applicable in NonBeacon (w/Coordinator) networks.

Peer-to-Peer

By default, XBee®/XBee-PRO RF Modules are configured to operate within a Peer-to-Peer network topology and therefore are not dependent upon Master/Slave relationships. NonBeacon systems operate within a Peer-to-Peer network topology and therefore are not dependent upon Master/ Slave relationships. This means that modules remain synchronized without use of master/server configurations and each module in the network shares both roles of master and slave. Digi's peer-to-peer architecture features fast synchronization times and fast cold start times. This default configuration accommodates a wide range of RF data applications.

Figure 2-06. Peer-to-Peer Architecture



A peer-to-peer network can be established by configuring each module to operate as an End Device (CE = 0), disabling End Device Association on all modules (A1 = 0) and setting ID and CH parameters to be identical across the network.

NonBeacon (w/ Coordinator)

A device is configured as a Coordinator by setting the CE (Coordinator Enable) parameter to “1”. Coordinator power-up is governed by the A2 (Coordinator Association) parameter.

In a Coordinator system, the Coordinator can be configured to use direct or indirect transmissions. If the SP (Cyclic Sleep Period) parameter is set to “0”, the Coordinator will send data immediately. Otherwise, the SP parameter determines the length of time the Coordinator will retain the data before discarding it. Generally, SP (Cyclic Sleep Period) and ST (Time before Sleep) parameters should be set to match the SP and ST settings of the End Devices.

Association

Association is the establishment of membership between End Devices and a Coordinator. The establishment of membership is useful in scenarios that require a central unit (Coordinator) to relay messages to or gather data from several remote units (End Devices), assign channels or assign PAN IDs.

An RF data network that consists of one Coordinator and one or more End Devices forms a PAN (Personal Area Network). Each device in a PAN has a PAN Identifier [ID (PAN ID) parameter]. PAN IDs must be unique to prevent miscommunication between PANs. The Coordinator PAN ID is set using the ID (PAN ID) and A2 (Coordinator Association) commands.

An End Device can associate to a Coordinator without knowing the address, PAN ID or channel of the Coordinator. The A1 (End Device Association) parameter bit fields determine the flexibility of an End Device during association. The A1 parameter can be used for an End Device to dynamically set its destination address, PAN ID and/or channel.

For example: If the PAN ID of a Coordinator is known, but the operating channel is not; the A1 command on the End Device should be set to enable the 'Auto_Associate' and 'Reassign_Channel' bits. Additionally, the ID parameter should be set to match the PAN ID of the associated Coordinator.

Coordinator / End Device Setup and Operation

To configure a module to operate as a Coordinator, set the CE (Coordinator Enable) parameter to '1'. Set the CE parameter of End Devices to '0' (default). Coordinator and End Devices should contain matching firmware versions.

NonBeacon (w/ Coordinator) Systems

The Coordinator can be configured to use direct or indirect transmissions. If the SP (Cyclic Sleep Period) parameter is set to '0', the Coordinator will send data immediately. Otherwise, the SP parameter determines the length of time the Coordinator will retain the data before discarding it. Generally, SP (Cyclic Sleep Period) and ST (Time before Sleep) parameters should be set to match the SP and ST settings of the End Devices.

Coordinator Start-up

Coordinator power-up is governed by the A2 (Coordinator Association) command. On power-up, the Coordinator undergoes the following sequence of events:

1. Check A2 parameter- Reassign_PANID Flag

Set (bit 0 = 1) - The Coordinator issues an Active Scan. The Active Scan selects one channel and transmits a request to the broadcast address (0xFFFF) and broadcast PAN ID (0xFFFF). It then listens on that channel for beacons from any Coordinator operating on that channel. The listen time on each channel is determined by the SD (Scan Duration) parameter value.

Once the time expires on that channel, the Active Scan selects another channel and again transmits the BeaconRequest as before. This process continues until all channels have been scanned, or until 5 PANs have been discovered. When the Active Scan is complete, the results include a list of PAN IDs and Channels that are being used by other PANs. This list is used to assign an unique PAN ID to the new Coordinator. The ID parameter will be retained if it is not found in the Active Scan results. Otherwise, the ID (PAN ID) parameter setting will be updated to a PAN ID that was not detected.

Not Set (bit 0 = 0) - The Coordinator retains its ID setting. No Active Scan is performed.

2. Check A2 parameter - Reassign_Channel Flag (bit 1)

Set (bit 1 = 1) - The Coordinator issues an Energy Scan. The Energy Scan selects one channel and scans for energy on that channel. The duration of the scan is specified by the SD (Scan Duration) parameter. Once the scan is completed on a channel, the Energy Scan selects the next channel and begins a new scan on that channel. This process continues until all channels have been scanned.

When the Energy Scan is complete, the results include the maximal energy values detected on each channel. This list is used to determine a channel where the least energy was detected. If an Active Scan was performed (Reassign_PANID Flag set), the channels used by the detected PANs are eliminated as possible channels. Thus, the results of the Energy Scan and the Active Scan (if performed) are used to find the best channel (channel with the least energy that is not used by any detected PAN). Once the best channel has been selected, the CH (Channel) parameter value is updated to that channel.

Not Set (bit 1 = 0) - The Coordinator retains its CH setting. An Energy Scan is not performed.

3. Start Coordinator

The Coordinator starts on the specified channel (CH parameter) and PAN ID (ID parameter). Note, these may be selected in steps 1 and/or 2 above. The Coordinator will only allow End Devices to associate to it if the A2 parameter "AllowAssociation" flag is set. Once the Coordinator has successfully started, the Associate LED will blink 1 time per second. (The LED is solid if the Coordinator has not started.)

4. Coordinator Modifications

Once a Coordinator has started:
Modifying the A2 (Reassign_Channel or Reassign_PANID bits), ID, CH or MY parameters will cause the Coordinator's MAC to reset (The Coordinator RF module (including volatile RAM) is not reset). Changing the A2 AllowAssociation bit will not reset the Coordinator's MAC. In a non-beaconing system, End Devices that associated to the Coordinator prior to a MAC reset will have knowledge of the new settings on the Coordinator. Thus, if the Coordinator were to change its ID, CH or MY settings, the End Devices would no longer be able to communicate with the non-beacon Coordinator. Once a Coordinator has started, the ID, CH, MY or A2 (Reassign_Channel or Reassign_PANID bits) should not be changed.

End Device Start-up

End Device power-up is governed by the A1 (End Device Association) command. On power-up, the End Device undergoes the following sequence of events:

1. Check A1 parameter - AutoAssociate Bit

Set (bit 2 = 1) - End Device will attempt to associate to a Coordinator. (refer to steps 2-3).

Not Set (bit 2 = 0) - End Device will not attempt to associate to a Coordinator. The End Device will operate as specified by its ID, CH and MY parameters. Association is considered complete and the Associate LED will blink quickly (5 times per second). When the AutoAssociate bit is not set, the remaining steps (2-3) do not apply.

2. Discover Coordinator (if Auto-Associate Bit Set)

The End Device issues an Active Scan. The Active Scan selects one channel and transmits a BeaconRequest command to the broadcast address (0xFFFF) and broadcast PAN ID (0xFFFF). It then listens on that channel for beacons from any Coordinator operating on that channel. The listen time on each channel is determined by the SD parameter.

Once the time expires on that channel, the Active Scan selects another channel and again transmits the BeaconRequest command as before. This process continues until all channels have been scanned, or until 5 PANs have been discovered. When the Active Scan is complete, the results include a list of PAN IDs and Channels that are being used by detected PANs.

The End Device selects a Coordinator to associate with according to the A1 parameter "Reassign_PANID" and "Reassign_Channel" flags:

Reassign_PANID Bit Set (bit 0 = 1)- End Device can associate with a PAN with any ID value.

Reassign_PANID Bit Not Set (bit 0 = 0) - End Device will only associate with a PAN whose ID setting matches the ID setting of the End Device.

Reassign_Channel Bit Set (bit 1 = 1) - End Device can associate with a PAN with any CH value.

Reassign_Channel Bit Not Set (bit 1 = 0)- End Device will only associate with a PAN whose CH setting matches the CH setting of the End Device.

After applying these filters to the discovered Coordinators, if multiple candidate PANs exist, the End Device will select the PAN whose transmission link quality is the strongest. If no valid Coordinator is found, the End Device will either go to sleep (as dictated by its SM (Sleep Mode) parameter) or retry Association.

Note - An End Device will also disqualify Coordinators if they are not allowing association (A2 - AllowAssociation bit); or, if the Coordinator is not using the same NonBeacon scheme as the End Device. (They must both be programmed with NonBeacon code.)

3. Associate to Valid Coordinator

Once a valid Coordinator is found (step 2), the End Device sends an AssociationRequest message to the Coordinator. It then waits for an AssociationConfirmation to be sent from the Coordinator. Once the Confirmation is received, the End Device is Associated and the Associate LED will blink rapidly (2 times per second). The LED is solid if the End Device has not associated.

4. End Device Changes once an End Device has associated

Changing A1, ID or CH parameters will cause the End Device to disassociate and restart the Association procedure.

If the End Device fails to associate, the AI command can give some indication of the failure.

XBee®/XBee-PRO® Addressing

Every RF data packet sent over-the-air contains a Source Address and Destination Address field in its header. The RF module conforms to the 802.15.4 specification and supports both short 16-bit addresses and long 64-bit addresses. A unique 64-bit IEEE source address is assigned at the factory and can be read with the SL (Serial Number Low) and SH (Serial Number High) commands. Short addressing must be configured manually. A module will use its unique 64-bit address as its Source Address if its MY (16-bit Source Address) value is "0xFFFF" or "0xFFFE".

To send a packet to a specific module using 64-bit addressing: Set the Destination Address (DL + DH) of the sender to match the Source Address (SL + SH) of the intended destination module.

To send a packet to a specific module using 16-bit addressing: Set DL (Destination Address Low) parameter to equal the MY parameter of the intended destination module and set the DH (Destination Address High) parameter to '0'.

Unicast Mode

By default, the RF module operates in Unicast Mode. Unicast Mode is the only mode that supports retries. While in this mode, receiving modules send an ACK (acknowledgement) of RF packet reception to the transmitter. If the transmitting module does not receive the ACK, it will re-send the packet up to three times or until the ACK is received.

Short 16-bit addresses. The module can be configured to use short 16-bit addresses as the Source Address by setting (MY < 0xFFFE). Setting the DH parameter (DH = 0) will configure the Destination Address to be a short 16-bit address (if DL < 0xFFFE). For two modules to communicate using short addressing, the Destination Address of the transmitter module must match the MY parameter of the receiver.

The following table shows a sample network configuration that would enable Unicast Mode communications using short 16-bit addresses.

Table 2-03. Sample Unicast Network Configuration (using 16-bit addressing)

Parameter	RF Module 1	RF Module 2
MY (Source Address)	0x01	0x02
DH (Destination Address High)	0	0
DL (Destination Address Low)	0x02	0x01

Long 64-bit addresses. The RF module's serial number (SL parameter concatenated to the SH parameter) can be used as a 64-bit source address when the MY (16-bit Source Address) parameter is disabled. When the MY parameter is disabled (MY = 0xFFFF or 0xFFFE), the module's source address is set to the 64-bit IEEE address stored in the SH and SL parameters.

When an End Device associates to a Coordinator, its MY parameter is set to 0xFFFE to enable 64-bit addressing. The 64-bit address of the module is stored as SH and SL parameters. To send a packet to a specific module, the Destination Address (DL + DH) on the sender must match the Source Address (SL + SH) of the desired receiver.

Broadcast Mode

Any RF module within range will accept a packet that contains a broadcast address. When configured to operate in Broadcast Mode, receiving modules do not send ACKs (Acknowledgements) and transmitting modules do not automatically re-send packets as is the case in Unicast Mode.

To send a broadcast packet to all modules regardless of 16-bit or 64-bit addressing, set the destination addresses of all the modules as shown below.

Sample Network Configuration (All modules in the network):

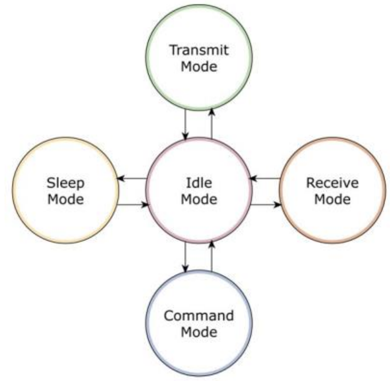
- DL (Destination Low Address) = 0x0000FFFF
- DH (Destination High Address) = 0x00000000 (default value)

NOTE: When programming the module, parameters are entered in hexadecimal notation (without the "0x" prefix). Leading zeros may be omitted.

Modes of Operation

XBee®/XBee-PRO® RF Modules operate in five modes.

Figure 2-07. Modes of Operation



Idle Mode

When not receiving or transmitting data, the RF module is in Idle Mode. The module shifts into the other modes of operation under the following conditions:

- Transmit Mode (Serial data is received in the DI Buffer)
- Receive Mode (Valid RF data is received through the antenna)
- Sleep Mode (Sleep Mode condition is met)
- Command Mode (Command Mode Sequence is issued)

Transmit/Receive Modes

RF Data Packets

Each transmitted data packet contains a Source Address and Destination Address field. The Source Address matches the address of the transmitting module as specified by the MY (Source Address) parameter (if MY >= 0xFFFE), the SH (Serial Number High) parameter or the SL (Serial Number Low) parameter. The <Destination Address> field is created from the DH (Destination Address High) and DL (Destination Address Low) parameter values. The Source Address and/or Destination Address fields will either contain a 16-bit short or long 64-bit long address.

The RF data packet structure follows the 802.15.4 specification.

[Refer to the XBee/XBee-PRO Addressing section for more information]

Direct and Indirect Transmission

There are two methods to transmit data:

- Direct Transmission - data is transmitted immediately to the Destination Address
- Indirect Transmission - A packet is retained for a period of time and is only transmitted after the destination module (Source Address = Destination Address) requests the data.

Indirect Transmissions can only occur on a Coordinator. Thus, if all nodes in a network are End Devices, only Direct Transmissions will occur. Indirect Transmissions are useful to ensure packet delivery to a sleeping node. The Coordinator currently is able to retain up to 2 indirect messages.

Direct Transmission

A Coordinator can be configured to use only Direct Transmission by setting the SP (Cyclic Sleep Period) parameter to "0". Also, a Coordinator using indirect transmissions will revert to direct transmission if it knows the destination module is awake.

To enable this behavior, the ST (Time before Sleep) value of the Coordinator must be set to match the ST value of the End Device. Once the End Device either transmits data to the Coordinator or polls the Coordinator for data, the Coordinator will use direct transmission for all subsequent data transmissions to that module address until ST time occurs with no activity (at which point it will revert to using indirect transmissions for that module address). "No activity" means no transmission or reception of messages with a specific address. Global messages will not reset the ST timer.

Indirect Transmission

To configure Indirect Transmissions in a PAN (Personal Area Network), the SP (Cyclic Sleep Period) parameter value on the Coordinator must be set to match the longest sleep value of any End Device. The sleep period value on the Coordinator determines how long (time or number of beacons) the Coordinator will retain an indirect message before discarding it.

An End Device must poll the Coordinator once it wakes from Sleep to determine if the Coordinator has an indirect message for it. For Cyclic Sleep Modes, this is done automatically every time the module wakes (after SP time). For Pin Sleep Modes, the A1 (End Device Association) parameter value must be set to enable Coordinator polling on pin wake-up. Alternatively, an End Device can use the FP (Force Poll) command to poll the Coordinator as needed.

CCA (Clear Channel Assessment)

Prior to transmitting a packet, a CCA (Clear Channel Assessment) is performed on the channel to determine if the channel is available for transmission. The detected energy on the channel is compared with the CA (Clear Channel Assessment) parameter value. If the detected energy exceeds the CA parameter value, the packet is not transmitted.

Also, a delay is inserted before a transmission takes place. This delay is settable using the RN (Backoff Exponent) parameter. If RN is set to “0”, then there is no delay before the first CCA is performed. The RN parameter value is the equivalent of the “minBE” parameter in the 802.15.4 specification. The transmit sequence follows the 802.15.4 specification.

By default, the MM (MAC Mode) parameter = 0. On a CCA failure, the module will attempt to re-send the packet up to two additional times.

When in Unicast packets with RR (Retries) = 0, the module will execute two CCA retries. Broadcast packets always get two CCA retries.

Acknowledgement

If the transmission is not a broadcast message, the module will expect to receive an acknowledgement from the destination node. If an acknowledgement is not received, the packet will be resent up to 3 more times. If the acknowledgement is not received after all transmissions, an ACK failure is recorded.

Sleep Mode

Sleep Modes enable the RF module to enter states of low-power consumption when not in use. In order to enter Sleep Mode, one of the following conditions must be met (in addition to the module having a non-zero SM parameter value):

- Sleep_RQ (pin 9) is asserted and the module is in a pin sleep mode (SM = 1, 2, or 5)
- The module is idle (no data transmission or reception) for the amount of time defined by the ST (Time before Sleep) parameter. [NOTE: ST is only active when SM = 4-5.]

Table 2-04. Sleep Mode Configurations

Sleep Mode Setting	Transition into Sleep Mode	Transition out of Sleep Mode (wake)	Characteristics	Related Commands	Power Consumption
Pin Hibernate (SM = 1)	Assert (high) Sleep_RQ (pin 9)	De-assert (low) Sleep_RQ	Pin/Host-controlled / NonBeacon systems only / Lowest Power	(SM)	< 10 µA (@3.0 VCC)
Pin Doze (SM = 2)	Assert (high) Sleep_RQ (pin 9)	De-assert (low) Sleep_RQ	Pin/Host-controlled / NonBeacon systems only / Fastest wake-up	(SM)	< 50 µA
Cyclic Sleep (SM = 4)	Automatic transition to Sleep Mode as defined by the SM (Sleep Mode) and ST (Time before Sleep) parameters.	Transition occurs after the cyclic sleep time interval elapses. The time interval is defined by the SP (Cyclic Sleep Period) parameter.	RF module wakes in pre-determined time intervals to detect if RF data is present / When SM = 5	(SM), SP, ST	< 50 µA when sleeping
Cyclic Sleep (SM = 5)	Automatic transition to Sleep Mode as defined by the SM (Sleep Mode) and ST (Time before Sleep) parameters or or on a falling edge transition of the SLEEP_RQ pin.	Transition occurs after the cyclic sleep time interval elapses. The time interval is defined by the SP (Cyclic Sleep Period) parameter.	RF module wakes in pre-determined time intervals to detect if RF data is present. Module also wakes on a falling edge of SLEEP_RQ	(SM), SP, ST	< 50 µA when sleeping

The SM command is central to setting Sleep Mode configurations. By default, Sleep Modes are disabled (SM = 0) and the module remains in Idle/Receive Mode. When in this state, the module is constantly ready to respond to serial or RF activity.

Pin/Host-controlled Sleep Modes

The transient current when waking from pin sleep (SM = 1 or 2) does not exceed the idle current of the module. The current ramps up exponentially to its idle current.

Pin Hibernate (SM = 1)

- Pin/Host-controlled
- Typical power-down current: < 10 µA (@3.0 VCC)
- Wake-up time: 13.2 msec

Pin Hibernate Mode minimizes quiescent power (power consumed when in a state of rest or inactivity). This mode is voltage level-activated; when Sleep_RQ (pin 9) is asserted, the module will finish any transmit, receive or association activities, enter Idle Mode, and then enter a state of sleep. The module will not respond to either serial or RF activity while in pin sleep.

To wake a sleeping module operating in Pin Hibernate Mode, de-assert Sleep_RQ (pin 9). The module will wake when Sleep_RQ is de-asserted and is ready to transmit or receive when the CTS line is low. When waking the module, the pin must be de-asserted at least two 'byte times' after CTS goes low. This assures that there is time for the data to enter the DI buffer.

Pin Doze (SM = 2)

- Pin/Host-controlled
- Typical power-down current: < 50 µA
- Wake-up time: 2 msec

Pin Doze Mode functions as does Pin Hibernate Mode; however, Pin Doze features faster wake-up time and higher power consumption.

To wake a sleeping module operating in Pin Doze Mode, de-assert Sleep_RQ (pin 9). The module will wake when Sleep_RQ is de-asserted and is ready to transmit or receive when the CTS line is low. When waking the module, the pin must be de-asserted at least two 'byte times' after CTS goes low. This assures that there is time for the data to enter the DI buffer.

Cyclic Sleep Modes

Cyclic Sleep Remote (SM = 4)

- Typical Power-down Current: < 50 μA (when asleep)
- Wake-up time: 2 msec

The Cyclic Sleep Modes allow modules to periodically check for RF data. When the SM parameter is set to '4', the module is configured to sleep, then wakes once a cycle to check for data from a module configured as a Cyclic Sleep Coordinator (SM = 0, CE = 1). The Cyclic Sleep Remote sends a poll request to the coordinator at a specific interval set by the SP (Cyclic Sleep Period) parameter. The coordinator will transmit any queued data addressed to that specific remote upon receiving the poll request.

If no data is queued for the remote, the coordinator will not transmit and the remote will return to sleep for another cycle. If queued data is transmitted back to the remote, it will stay awake to allow for back and forth communication until the ST (Time before Sleep) timer expires.

Also note that $\overline{\text{CTS}}$ will go low each time the remote wakes, allowing for communication initiated by the remote host if desired.

Cyclic Sleep Remote with Pin Wake-up (SM = 5)

Use this mode to wake a sleeping remote module through either the RF interface or by the de-assertion of Sleep_RQ for event-driven communications. The cyclic sleep mode works as described above (Cyclic Sleep Remote) with the addition of a pin-controlled wake-up at the remote module. The Sleep_RQ pin is edge-triggered, not level-triggered. The module will wake when a low is detected then set $\overline{\text{CTS}}$ low as soon as it is ready to transmit or receive.

Any activity will reset the ST (Time before Sleep) timer so the module will go back to sleep only after there is no activity for the duration of the timer. Once the module wakes (pin-controlled), further pin activity is ignored. The module transitions back into sleep according to the ST time regardless of the state of the pin.

[Cyclic Sleep Coordinator (SM = 6)]

- Typical current = Receive current
- Always awake

NOTE: The SM=6 parameter value exists solely for backwards compatibility with firmware version 1.x60. If backwards compatibility with the older firmware version is not required, always use the CE (Coordinator Enable) command to configure a module as a Coordinator.

This mode configures a module to wake cyclic sleeping remotes through RF interfacing. The Coordinator will accept a message addressed to a specific remote 16 or 64-bit address and hold it in a buffer until the remote wakes and sends a poll request. Messages not sent directly (buffered and requested) are called "Indirect messages". The Coordinator only queues one indirect message at a time. The Coordinator will hold the indirect message for a period 2.5 times the sleeping period indicated by the SP (Cyclic Sleep Period) parameter. The Coordinator's SP parameter should be set to match the value used by the remotes.

Command Mode

To modify or read RF Module parameters, the module must first enter into Command Mode - a state in which incoming characters are interpreted as commands. Two Command Mode options are supported: AT Command Mode [refer to section below] and API Command Mode [p57].

AT Command Mode

To Enter AT Command Mode:

Send the 3-character command sequence "+++" and observe guard times before and after the command characters. [Refer to the "Default AT Command Mode Sequence" below.]

Default AT Command Mode Sequence (for transition to Command Mode):

- No characters sent for one second [GT (Guard Times) parameter = 0x3E8]
- Input three plus characters ("+++") within one second [CC (Command Sequence Character) parameter = 0x2B.]
- No characters sent for one second [GT (Guard Times) parameter = 0x3E8]

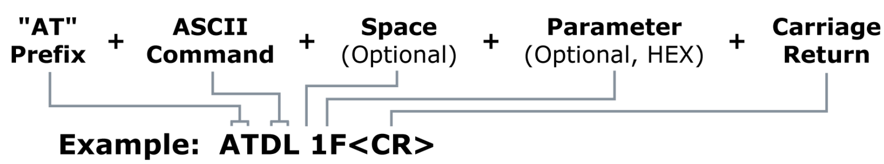
All of the parameter values in the sequence can be modified to reflect user preferences.

NOTE: Failure to enter AT Command Mode is most commonly due to baud rate mismatch. Ensure the 'Baud' setting on the "PC Settings" tab matches the interface data rate of the RF module. By default, the BD parameter = 3 (9600 bps).

To Send AT Commands:

Send AT commands and parameters using the syntax shown below.

Figure 2-08. Syntax for sending AT Commands



To read a parameter value stored in the RF module's register, omit the parameter field.

The preceding example would change the RF module Destination Address (Low) to "0x1F". To store the new value to non-volatile (long term) memory, subsequently send the WR (Write) command.

For modified parameter values to persist in the module's registry after a reset, changes must be saved to non-volatile memory using the WR (Write) Command. Otherwise, parameters are restored to previously saved values after the module is reset.

System Response. When a command is sent to the module, the module will parse and execute the command. Upon successful execution of a command, the module returns an "OK" message. If execution of a command results in an error, the module returns an "ERROR" message.

To Exit AT Command Mode:

1. Send the ATCN (Exit Command Mode) command (followed by a carriage return).
   [OR]
2. If no valid AT Commands are received within the time specified by CT (Command Mode Timeout) Command, the RF module automatically returns to Idle Mode.

For an example of programming the RF module using AT Commands and descriptions of each configurable parameter, refer to the RF Module Configuration chapter [p26].

3. RF Module Configuration

Programming the RF Module

Refer to the Command Mode section [p25] for more information about entering Command Mode, sending AT commands and exiting Command Mode. For information regarding module programming using API Mode, refer to the API Operation sections [p57].

Programming Examples

Setup

The programming examples in this section require the installation of Digi's X-CTU Software and a serial connection to a PC. (Digi stocks RS-232 and USB boards to facilitate interfacing with a PC.)

1. Install Digi's X-CTU Software to a PC by double-clicking the "setup_X-CTU.exe" file. (The file is located on the Digi CD and www.digi.com/xctu.)
2. Mount the RF module to an interface board, then connect the module assembly to a PC.
3. Launch the X-CTU Software and select the 'PC Settings' tab. Verify the baud and parity settings of the Com Port match those of the RF module.

NOTE: Failure to enter AT Command Mode is most commonly due to baud rate mismatch. Ensure the 'Baud' setting on the 'PC Settings' tab matches the interface data rate of the RF module. By default, the BD parameter = 3 (which corresponds to 9600 bps).

Sample Configuration: Modify RF Module Destination Address

Example: Utilize the X-CTU "Terminal" tab to change the RF module's DL (Destination Address Low) parameter and save the new address to non-volatile memory.

After establishing a serial connection between the RF module and a PC [refer to the 'Setup' section above], select the "Terminal" tab of the X-CTU Software and enter the following command lines ('CR' stands for carriage return):

Method 1 (One line per command)

Send AT Command	System Response
+++	OK <CR> (Enter into Command Mode)
ATDL <Enter>	{current value} <CR> (Read Destination Address Low)
ATDL1A0D <Enter>	OK <CR> (Modify Destination Address Low)
ATWR <Enter>	OK <CR> (Write to non-volatile memory)
ATCN <Enter>	OK <CR> (Exit Command Mode)

Method 2 (Multiple commands on one line)

Send AT Command	System Response
+++	OK <CR> (Enter into Command Mode)
ATDL <Enter>	{current value} <CR> (Read Destination Address Low)
ATDL1A0D,WR,CN <Enter>	OK<CR> OK<CR> OK<CR>

Sample Configuration: Restore RF Module Defaults

Example: Utilize the X-CTU "Modem Configuration" tab to restore default parameter values.

After establishing a connection between the module and a PC [refer to the 'Setup' section above], select the "Modem Configuration" tab of the X-CTU Software.

1. Select the 'Read' button.
2. Select the 'Restore' button.

Remote Configuration Commands

The API firmware has provisions to send configuration commands to remote devices using the Remote Command Request API frame (see API Operation). This API frame can be used to send commands to a remote module to read or set command parameters.

The API firmware has provisions to send configuration commands (set or read) to a remote module using the Remote Command Request API frame (see API Operations). Remote commands can be issued to read or set command parameters on a remote device.

Sending a Remote Command

To send a remote command, the Remote Command Request frame should be populated with values for the 64 bit and 16 bit addresses. If 64 bit addressing is desired then the 16 bit address field should be filled with 0xFFFE. If any value other than 0xFFFE is used in the 16 bit address field then the 64 bit address field will be ignored and 16 bit addressing will be used. If a command response is desired, the Frame ID should be set to a non-zero value.

Applying Changes on Remote

When remote commands are used to change command parameter settings on a remote device, parameter changes do not take effect until the changes are applied. For example, changing the BD parameter will not change the actual serial interface rate on the remote until the changes are applied. Changes can be applied using remote commands in one of three ways:

Set the apply changes option bit in the API frame

Issue an AC command to the remote device

Issue a WR + FR command to the remote device to save changes and reset the device.

Remote Command Responses

If the remote device receives a remote command request transmission, and the API frame ID is non-zero, the remote will send a remote command response transmission back to the device that sent the remote command. When a remote command response transmission is received, a device sends a remote command response API frame out its UART. The remote command response indicates the status of the command (success, or reason for failure), and in the case of a command query, it will include the register value.

The device that sends a remote command will not receive a remote command response frame if:

The destination device could not be reached

The frame ID in the remote command request is set to 0.

Command Reference Tables

XBee®/XBee-PRO® RF Modules expect numerical values in hexadecimal. Hexadecimal values are designated by a “0x” prefix. Decimal equivalents are designated by a “d” suffix. Commands are contained within the following command categories (listed in the order that their tables appear):

- Special
- Networking & Security
- RF Interfacing
- Sleep (Low Power)
- Serial Interfacing
- I/O Settings
- Diagnostics
- AT Command Options

All modules within a PAN should operate using the same firmware version.

Special

Table 3-01. XBee-PRO Commands - Special

AT Command	Command Category	Name and Description	Parameter Range	Default
WR	Special	**Write**. Write parameter values to non-volatile memory so that parameter modifications persist through subsequent power-up or reset. Note: Once WR is issued, no additional characters should be sent to the module until after the response "OK\r" is received.	-	-
RE	Special	**Restore Defaults**. Restore module parameters to factory defaults.	-	-
FR (v1.x80*)	Special	**Software Reset**. Responds immediately with an OK then performs a hard reset ~100ms later.	-	-

* Firmware version in which the command was first introduced (firmware versions are numbered in hexadecimal notation.)

Networking & Security

Table 3-02. XBee®/XBee-PRO® Commands - Networking & Security (Sub-categories designated within {brackets})

AT Command	Command Category	Name and Description	Parameter Range	Default
CH	Networking {Addressing}	**Channel**. Set/Read the channel number used for transmitting and receiving data between RF modules (uses 802.15.4 protocol channel numbers).	0x0B - 0x1A (XBee) 0x0C - 0x17 (XBee-PRO)	0x0C (12d)
ID	Networking {Addressing}	**PAN ID**. Set/Read the PAN (Personal Area Network) ID. Use 0xFFFF to broadcast messages to all PANs.	0 - 0xFFFF	0x3332 (13106d)
DH	Networking {Addressing}	**Destination Address High**. Set/Read the upper 32 bits of the 64-bit destination address. When combined with DL, it defines the destination address used for transmission. To transmit using a 16-bit address, set DH parameter to zero and DL less than 0xFFFF. 0x000000000000FFFF is the broadcast address for the PAN.	0 - 0xFFFFFFFF	0
DL	Networking {Addressing}	**Destination Address Low**. Set/Read the lower 32 bits of the 64-bit destination address. When combined with DH, DL defines the destination address used for transmission. To transmit using a 16-bit address, set DH parameter to zero and DL less than 0xFFFF. 0x000000000000FFFF is the broadcast address for the PAN.	0 - 0xFFFFFFFF	0
MY	Networking {Addressing}	**16-bit Source Address.** Set/Read the RF module 16-bit source address. Set MY = 0xFFFF to disable reception of packets with 16-bit addresses. 64-bit source address (serial number) and broadcast address (0x000000000000FFFF) is always enabled.	0 - 0xFFFF	0
SH	Networking {Addressing}	**Serial Number High**. Read high 32 bits of the RF module's unique IEEE 64-bit address. 64-bit source address is always enabled.	0 - 0xFFFFFFFF [read-only]	Factory-set
SL	Networking {Addressing}	**Serial Number Low**. Read low 32 bits of the RF module's unique IEEE 64-bit address. 64-bit source address is always enabled.	0 - 0xFFFFFFFF [read-only]	Factory-set
RR (v1.xA0*)	Networking {Addressing}	**XBee Retries**. Set/Read the maximum number of retries the module will execute in addition to the 3 retries provided by the 802.15.4 MAC. For each XBee retry, the 802.15.4 MAC can execute up to 3 retries.	0 - 6	0
RN	Networking {Addressing}	**Random Delay Slots.** Set/Read the minimum value of the back-off exponent in the CSMA-CA algorithm that is used for collision avoidance. If RN = 0, collision avoidance is disabled during the first iteration of the algorithm (802.15.4 - macMinBE).	0 - 3 [exponent]	0
MM (v1.x80*)	Networking {Addressing}	**MAC Mode.** MAC Mode. Set/Read MAC Mode value. MAC Mode enables/disables the use of a Digi header in the 802.15.4 RF packet. When Modes 0 or 3 are enabled (MM=0,3), duplicate packet detection is enabled as well as certain AT commands. Please see the detailed MM description on page 47 for additional information.	0 - 3 0 = Digi Mode 1 = 802.15.4 (no ACKs) 2 = 802.15.4 (with ACKs) 3 = Digi Mode (no ACKs)	0
NI (v1.x80*)	Networking {Identification}	**Node Identifier.** Stores a string identifier. The register only accepts printable ASCII data. A string can not start with a space. Carriage return ends command. Command will automatically end when maximum bytes for the string have been entered. This string is returned as part of the ND (Node Discover) command. This identifier is also used with the DN (Destination Node) command.	20-character ASCII string	-
ND (v1.x80*)	Networking {Identification}	**Node Discover.** Discovers and reports all RF modules found. The following information is reported for each module discovered (the example cites use of Transparent operation (AT command format) - refer to the long ND command description regarding differences between Transparent and API operation). MY<CR> SH<CR> SL<CR> DB<CR> NI<CR><CR> The amount of time the module allows for responses is determined by the NT parameter. In Transparent operation, command completion is designated by a <CR> (carriage return). ND also accepts a Node Identifier as a parameter. In this case, only a module matching the supplied identifier will respond. If ND self-response is enabled (NO=1) the module initiating the node discover will also output a response for itself.	optional 20-character NI value	
NT (v1.xA0*)	Networking {Identification}	**Node Discover Time.** Set/Read the amount of time a node will wait for responses from other nodes when using the ND (Node Discover) command.	0x01 - 0xFC [x 100 ms]	0x19

Table 3-02. XBee®/XBee-PRO® Commands - Networking & Security (Sub-categories designated within {brackets})

AT Command	Command Category	Name and Description	Parameter Range	Default
NO (v1xC5)	Networking {Identification}	**Node Discover Options**. Enables node discover self-response on the module.	0-1	0
DN (v1.x80*)	Networking {Identification}	**Destination Node.** Resolves an NI (Node Identifier) string to a physical address. The following events occur upon successful command execution: 1. DL and DH are set to the address of the module with the matching Node Identifier. 2. "OK" is returned. 3. RF module automatically exits AT Command Mode If there is no response from a module within 200 msec or a parameter is not specified (left blank), the command is terminated and an "ERROR" message is returned.	20-character ASCII string	-
CE (v1.x80*)	Networking {Association}	**Coordinator Enable**. Set/Read the coordinator setting.	0 - 1 0 = End Device 1 = Coordinator	0
SC (v1.x80*)	Networking {Association}	**Scan Channels**. Set/Read list of channels to scan for all Active and Energy Scans as a bitfield. This affects scans initiated in command mode (AS, ED) and during End Device Association and Coordinator startup: bit 0 - 0x0B bit 4 - 0x0F bit 8 - 0x13 bit12 - 0x17 bit 1 - 0x0C bit 5 - 0x10 bit 9 - 0x14 bit13 - 0x18 bit 2 - 0x0D bit 6 - 0x11 bit 10 - 0x15 bit14 - 0x19 bit 3 - 0x0E bit 7 - 0x12 bit 11 - 0x16 bit 15 - 0x1A	0 - 0xFFFF [bitfield] (bits 0, 14, 15 not allowed on the XBee-PRO)	0x1FFE (all XBee-PRO Channels)
SD (v1.x80*)	Networking {Association}	**Scan Duration**. Set/Read the scan duration exponent. ***End Device*** - Duration of Active Scan during Association. ***Coordinator*** - If 'ReassignPANID' option is set on Coordinator [refer to A2 parameter], SD determines the length of time the Coordinator will scan channels to locate existing PANs. If 'ReassignChannel' option is set, SD determines how long the Coordinator will perform an Energy Scan to determine which channel it will operate on. 'Scan Time' is measured as (# of channels to scan] * (2 ^ SD) * 15.36ms). The number of channels to scan is set by the SC command. The XBee can scan up to 16 channels (SC = 0xFFFF). The XBee PRO can scan up to 13 channels (SC = 0x3FFE). Example: The values below show results for a 13 channel scan: If SD = 0, time = 0.18 sec SD = 8, time = 47.19 sec SD = 2, time = 0.74 sec SD = 10, time = 3.15 min SD = 4, time = 2.95 sec SD = 12, time = 12.58 min SD = 6, time = 11.80 sec SD = 14, time = 50.33 min	0-0x0F [exponent]	4
A1 (v1.x80*)	Networking {Association}	**End Device Association**. Set/Read End Device association options. bit 0 - ReassignPanID 0 - Will only associate with Coordinator operating on PAN ID that matches module ID 1 - May associate with Coordinator operating on any PAN ID bit 1 - ReassignChannel 0 - Will only associate with Coordinator operating on matching CH Channel setting 1 - May associate with Coordinator operating on any Channel bit 2 - AutoAssociate 0 - Device will not attempt Association 1 - Device attempts Association until success Note: This bit is used only for Non-Beacon systems. End Devices in Beacon-enabled system must always associate to a Coordinator bit 3 - PollCoordOnPinWake 0 - Pin Wake will not poll the Coordinator for indirect (pending) data 1 - Pin Wake will send Poll Request to Coordinator to extract any pending data bits 4 - 7 are reserved	0 - 0x0F [bitfield]	0
A2 (v1.x80*)	Networking {Association}	**Coordinator Association**. Set/Read Coordinator association options. bit 0 - ReassignPanID 0 - Coordinator will not perform Active Scan to locate available PAN ID. It will operate on ID (PAN ID). 1 - Coordinator will perform Active Scan to determine an available ID (PAN ID). If a PAN ID conflict is found, the ID parameter will change. bit 1 - ReassignChannel - 0 - Coordinator will not perform Energy Scan to determine free channel. It will operate on the channel determined by the CH parameter. 1 - Coordinator will perform Energy Scan to find a free channel, then operate on that channel. bit 2 - AllowAssociation - 0 - Coordinator will not allow any devices to associate to it. 1 - Coordinator will allow devices to associate to it. bits 3 - 7 are reserved	0 - 7 [bitfield]	0

Table 3-02. XBee®/XBee-PRO® Commands - Networking & Security (Sub-categories designated within {brackets})

AT Command	Command Category	Name and Description	Parameter Range	Default
AI (v1.x80*)	Networking {Association}	**Association Indication**. Read errors with the last association request: 0x00 - Successful Completion - Coordinator successfully started or End Device association complete 0x01 - Active Scan Timeout 0x02 - Active Scan found no PANs 0x03 - Active Scan found PAN, but the CoordinatorAllowAssociation bit is not set 0x04 - Active Scan found PAN, but Coordinator and End Device are not configured to support beacons 0x05 - Active Scan found PAN, but the Coordinator ID parameter does not match the ID parameter of the End Device 0x06 - Active Scan found PAN, but the Coordinator CH parameter does not match the CH parameter of the End Device 0x07 - Energy Scan Timeout 0x08 - Coordinator start request failed 0x09 - Coordinator could not start due to invalid parameter 0x0A - Coordinator Realignment is in progress 0x0B - Association Request not sent 0x0C - Association Request timed out - no reply was received 0x0D - Association Request had an Invalid Parameter 0x0E - Association Request Channel Access Failure. Request was not transmitted - CCA failure 0x0F - Remote Coordinator did not send an ACK after Association Request was sent 0x10 - Remote Coordinator did not reply to the Association Request, but an ACK was received after sending the request 0x11 - [reserved]	0 - 0x13 [read-only]	-
DA (v1.x80*)	Networking {Association}	**Force Disassociation**. End Device will immediately disassociate from a Coordinator (if associated) and reattempt to associate.	-	-
FP (v1.x80*)	Networking {Association}	**Force Poll**. Request indirect messages being held by a coordinator.	-	-
AS (v1.x80*)	Networking {Association}	**Active Scan**. Send Beacon Request to Broadcast Address (0xFFFF) and Broadcast PAN (0xFFFF) on every channel. The parameter determines the time the radio will listen for Beacons on each channel. A PanDescriptor is created and returned for every Beacon received from the scan. Each PanDescriptor contains the following information: CoordAddress (SH, SL)<CR> CoordPanID (ID)<CR> CoordAddrMode <CR> 0x02 = 16-bit Short Address 0x03 = 64-bit Long Address Channel (CH parameter) <CR> SecurityUse<CR> ACLEntry<CR> SecurityFailure<CR> SuperFrameSpec<CR> (2 bytes): bit 15 - Association Permitted (MSB) bit 14 - PAN Coordinator bit 13 - Reserved bit 12 - Battery Life Extension bits 8-11 - Final CAP Slot bits 4-7 - Superframe Order bits 0-3	0 - 6	-
ED (v1.x80*)	Networking {Association}	**Energy Scan**. Send an Energy Detect Scan. This parameter determines the length of scan on each channel. The maximal energy on each channel is returned & each value is followed by a carriage return. An additional carriage return is sent at the end of the command. The values returned represent the detected energy level in units of -dBm. The actual scan time on each channel is measured as Time = [(2 ^ED) * 15.36] ms. Note the total scan time is this time multiplied by the number of channels to be scanned (refer to SD parameter).	0 - 6	-
EE (v1.xA0*)	Networking {Security}	**AES Encryption Enable**. Disable/Enable 128-bit AES encryption support. Use in conjunction with the KY command.	0 - 1	0 (disabled)
KY (v1.xA0*)	Networking {Security}	**AES Encryption Key**. Set the 128-bit AES (Advanced Encryption Standard) key for encrypting/decrypting data. The KY register can not be read.	0 - (any 16-Byte value)	-

* Firmware version in which the command was first introduced (firmware versions are numbered in hexadecimal notation.)

RF Interfacing

Table 3-03. XBee/XBee-PRO Commands - RF Interfacing

AT Command	Command Category	Name and Description	Parameter Range	Default
PL	RF Interfacing	**Power Level**. Select/Read the power level at which the RF module transmits conducted power.	0 - 4 (XBee / XBee-PRO) 0 = -10 / 10 dBm 1 = -6 / 12 dBm 2 = -4 / 14 dBm 3 = -2 / 16 dBm 4 = 0 / 18 dBm XBee-PRO International variant: PL=4: 10 dBm PL=3: 8 dBm PL=2: 2 dBm PL=1: -3 dBm PL=0: -3 dBm	4
CA (v1.x80*)	RF Interfacing	**CCA Threshold**. Set/read the CCA (Clear Channel Assessment) threshold. Prior to transmitting a packet, a CCA is performed to detect energy on the channel. If the detected energy is above the CCA Threshold, the module will not transmit the packet.	0x24 - 0x50 [-dBm]	0x2C (-44d dBm)

* Firmware version in which the command was first introduced (firmware versions are numbered in hexadecimal notation.)

Sleep (Low Power)

Table 3-04. XBee®/XBee-PRO® Commands - Sleep (Low Power)

AT Command	Command Category	Name and Description	Parameter Range	Default
SM	Sleep (Low Power)	**Sleep Mode**. Set/Read Sleep Mode configurations.	0 - 5 0 = No Sleep 1 = Pin Hibernate 2 = Pin Doze 3 = Reserved 4 = Cyclic sleep remote 5 = Cyclic sleep remote w/ pin wake-up 6 = [Sleep Coordinator] for backwards compatibility w/ v1.x6 only; otherwise, use CE command.	0
SO	Sleep (Low Power)	Sleep Options Set/Read the sleep mode options. Bit 0 - Poll wakeup disable 0 - Normal operations. A module configured for cyclic sleep will poll for data on waking. 1 - Disable wakeup poll. A module configured for cyclic sleep will not poll for data on waking. Bit 1 - ADC/DIO wakeup sampling disable. 0 - Normal operations. A module configured in a sleep mode with ADC/DIO sampling enabled will automatically perform a sampling on wakeup. 1 - Suppress sample on wakeup. A module configured in a sleep mode with ADC/DIO sampling enabled will not automatically sample on wakeup.	0-4	0
ST	Sleep (Low Power)	**Time before Sleep.** <NonBeacon firmware> Set/Read time period of inactivity (no serial or RF data is sent or received) before activating Sleep Mode. ST parameter is only valid with Cyclic Sleep settings (SM = 4 - 5). Coordinator and End Device ST values must be equal. Also note, the GT parameter value must always be less than the ST value. (If GT > ST, the configuration will render the module unable to enter into command mode.) If the ST parameter is modified, also modify the GT parameter accordingly.	1 - 0xFFFF [x 1 ms]	0x1388 (5000d)
SP	Sleep (Low Power)	**Cyclic Sleep Period.** <NonBeacon firmware> Set/Read sleep period for cyclic sleeping remotes. Coordinator and End Device SP values should always be equal. To send Direct Messages, set SP = 0. *End Device* - SP determines the sleep period for cyclic sleeping remotes. Maximum sleep period is 268 seconds (0x68B0). *Coordinator* - If non-zero, SP determines the time to hold an indirect message before discarding it. A Coordinator will discard indirect messages after a period of (2.5 * SP).	0 - 0x68B0 [x 10 ms]	0
DP (1.x80*)	Sleep (Low Power)	**Disassociated Cyclic Sleep Period.** <NonBeacon firmware> *End Device* - Set/Read time period of sleep for cyclic sleeping remotes that are configured for Association but are not associated to a Coordinator. (i.e. If a device is configured to associate, configured as a Cyclic Sleep remote, but does not find a Coordinator, it will sleep for DP time before reattempting association.) Maximum sleep period is 268 seconds (0x68B0). DP should be > 0 for NonBeacon systems.	1 - 0x68B0 [x 10 ms]	0x3E8 (1000d)

* Firmware version in which the command was first introduced (firmware versions are numbered in hexadecimal notation.)

Serial Interfacing

Table 3-05. XBee-PRO Commands - Serial Interfacing

AT Command	Command Category	Name and Description	Parameter Range	Default
BD	Serial Interfacing	**Interface Data Rate**. Set/Read the serial interface data rate for communications between the RF module serial port and host. Request non-standard baud rates with values above 0x80 using a terminal window. Read the BD register to find actual baud rate achieved.	0 - 7 (standard baud rates) 0 = 1200 bps 1 = 2400 2 = 4800 3 = 9600 4 = 19200 5 = 38400 6 = 57600 7 = 115200 0x80 - 0x3D090 (non-standard baud rates up to 250 Kbps)	3
RO	Serial Interfacing	**Packetization Timeout**. Set/Read number of character times of inter-character delay required before transmission. Set to zero to transmit characters as they arrive instead of buffering them into one RF packet.	0 - 0xFF [x character times]	3
AP (v1.x80*)	Serial Interfacing	**API Enable**. Disable/Enable API Mode.	0 - 2 0 =Disabled 1 = API enabled 2 = API enabled (w/escaped control characters)	0
NB	Serial Interfacing	**Parity.** Set/Read parity settings.	0 - 4 0 = 8-bit no parity 1 = 8-bit even 2 = 8-bit odd 3 = 8-bit mark 4 = 8-bit space	0
PR (v1.x80*)	Serial Interfacing	**Pull-up Resistor Enable**. Set/Read bitfield to configure internal pull-up resistor status for I/O lines Bitfield Map: bit 0 - AD4/DIO4 (pin11) bit 1 - AD3 / DIO3 (pin17) bit 2 - AD2/DIO2 (pin18) bit 3 - AD1/DIO1 (pin19) bit 4 - AD0 / DIO0 (pin20) bit 5 - RTS / AD6 / DIO6 (pin16) bit 6 - DTR / SLEEP_RQ / DI8 (pin9) bit 7 - DIN/CONFIG (pin3) Bit set to “1” specifies pull-up enabled; “0” specifies no pull-up	0 - 0xFF	0xFF

* Firmware version in which the command was first introduced (firmware versions are numbered in hexadecimal notation.)

I/O Settings

Table 3-06. XBee-PRO Commands - I/O Settings (sub-category designated within {brackets})

AT Command	Command Category	Name and Description	Parameter Range	Default
D8	I/O Settings	**DI8 Configuration**. Select/Read options for the DI8 line (pin 9) of the RF module.	0 - 1 0 = Disabled 3 = DI (1,2,4 & 5 n/a)	0
D7 (v1.x80*)	I/O Settings	**DIO7 Configuration**. Select/Read settings for the DIO7 line (pin 12) of the RF module. Options include CTS flow control and I/O line settings.	0 - 1 0 = Disabled 1 = CTS Flow Control 2 = (n/a) 3 = DI 4 = DO low 5 = DO high 6 = RS485 Tx Enable Low 7 = RS485 Tx Enable High	1
D6 (v1.x80*)	I/O Settings	**DIO6 Configuration**. Select/Read settings for the DIO6 line (pin 16) of the RF module. Options include RTS flow control and I/O line settings.	0 - 1 0 = Disabled 1 = RTS flow control 2 = (n/a) 3 = DI 4 = DO low 5 = DO high	0

Table 3-06. XBee-PRO Commands - I/O Settings (sub-category designated within {brackets})

AT Command	Command Category	Name and Description	Parameter Range	Default
D5 (v1.x80*)	I/O Settings	**DIO5 Configuration**. Configure settings for the DIO5 line (pin 15) of the RF module. Options include Associated LED indicator (blinks when associated) and I/O line settings.	0 - 1 0 = Disabled 1 = Associated indicator 2 = ADC 3 = DI 4 = DO low 5 = DO high	1
D0 - D4 (v1.xA0*)	I/O Settings	**(DIO4 -DIO4) Configuration**. Select/Read settings for the following lines: AD0/DIO0 (pin 20), AD1/DIO1 (pin 19), AD2/DIO2 (pin 18), AD3/DIO3 (pin 17), AD4/DIO4 (pin 11). Options include: Analog-to-digital converter, Digital Input and Digital Output.	0 - 1 0 = Disabled 1 = (n/a) 2 = ADC 3 = DI 4 = DO low 5 = DO high	0
IU (v1.xA0*)	I/O Settings	**I/O Output Enable.** Disables/Enables I/O data received to be sent out UART. The data is sent using an API frame regardless of the current AP parameter value.	0 - 1 0 = Disabled 1 = Enabled	1
IT (v1.xA0*)	I/O Settings	**Samples before TX.** Set/Read the number of samples to collect before transmitting data. Maximum number of samples is dependent upon the number of enabled inputs.	1 - 0xFF	1
IS (v1.xA0*)	I/O Settings	**Force Sample.** Force a read of all enabled inputs (DI or ADC). Data is returned through the UART. If no inputs are defined (DI or ADC), this command will return error.	8-bit bitmap (each bit represents the level of an I/O line setup as an output)	-
IO (v1.xA0*)	I/O Settings	**Digital Output Level.** Set digital output level to allow DIO lines that are setup as outputs to be changed through Command Mode.	-	-
IC (v1.xA0*)	I/O Settings	**DIO Change Detect.** Set/Read bitfield values for change detect monitoring. Each bit enables monitoring of DIO0 - DIO7 for changes. If detected, data is transmitted with DIO data only. Any samples queued waiting for transmission will be sent first.	0 - 0xFF [bitfield]	0 (disabled)
IR (v1.xA0*)	I/O Settings	**Sample Rate.** Set/Read sample rate. When set, this parameter causes the module to sample all enabled inputs at a specified interval.	0 - 0xFFFF [x 1 msec]	0
IA (v1.xA0*)	I/O Settings {I/O Line Passing}	**I/O Input Address**. Set/Read addresses of module to which outputs are bound. Setting all bytes to 0xFF will not allow any received I/O packet to change outputs. Setting address to 0xFFFF will allow any received I/O packet to change outputs.	0 - 0xFFFFFFFFFFFFFFFF	0xFFFFFFFF FFFFFFFF
T0 - T7 (v1.xA0*)	I/O Settings {I/O Line Passing}	**(D0 - D7) Output Timeout.** Set/Read Output timeout values for lines that correspond with the D0 - D7 parameters. When output is set (due to I/O line passing) to a non-default level, a timer is started which when expired will set the output to it default level. The timer is reset when a valid I/O packet is received.	0 - 0xFF [x 100 ms]	0xFF
P0	I/O Settings {I/O Line Passing}	**PWM0 Configuration**. Select/Read function for PWM0 pin.	0 - 2 0 = Disabled 1 = RSSI 2 = PWM Output	1
P1 (v1.xA0*)	I/O Settings {I/O Line Passing}	**PWM1 Configuration**. Select/Read function for PWM1 pin.	0 - 2 0 = Disabled 1 = RSSI 2 = PWM Output	0
M0 (v1.xA0*)	I/O Settings {I/O Line Passing}	**PWM0 Output Level**. Set/Read the PWM0 output level.	0 - 0x03FF	-
M1 (v1.xA0*)	I/O Settings {I/O Line Passing}	**PWM1 Output Level**. Set/Read the PWM1 output level.	0 - 0x03FF	-
PT (v1.xA0*)	I/O Settings {I/O Line Passing}	**PWM Output Timeout.** Set/Read output timeout value for both PWM outputs. When PWM is set to a non-zero value: Due to I/O line passing, a time is started which when expired will set the PWM output to zero. The timer is reset when a valid I/O packet is received.]	0 - 0xFF [x 100 ms]	0xFF
RP	I/O Settings {I/O Line Passing}	**RSSI PWM Timer.** Set/Read PWM timer register. Set the duration of PWM (pulse width modulation) signal output on the RSSI pin. The signal duty cycle is updated with each received packet and is shut off when the timerexpires.]	0 - 0xFF [x 100 ms]	0x28 (40d)

* Firmware version in which the command was first introduced (firmware versions are numbered in hexadecimal notation.)

Diagnostics

Table 3-07. XBee®/XBee-PRO® Commands - Diagnostics

AT Command	Command Category	Name and Description	Parameter Range	Default
VR	Diagnostics	**Firmware Version**. Read firmware version of the RF module.	0 - 0xFFFF [read-only]	Factory-set
VL (v1.x80*)	Diagnostics	**Firmware Version - Verbose**. Read detailed version information (including application build date, MAC, PHY and bootloader versions). The VL command has been deprecated in version 10C9. It is not supported in firmware versions after 10C8	-	-

Table 3-07. XBee®/XBee-PRO® Commands - Diagnostics

AT Command	Command Category	Name and Description	Parameter Range	Default
HV (v1.x80*)	Diagnostics	**Hardware Version**. Read hardware version of the RF module.	0 - 0xFFFF [read-only]	Factory-set
DB	Diagnostics	**Received Signal Strength**. Read signal level [in dB] of last good packet received (RSSI). Absolute value is reported. (For example: 0x58 = -88 dBm) Reported value is accurate between -40 dBm and RX sensitivity.	0x17-0x5C (XBee) 0x24-0x64 (XBee-PRO) [read-only]	-
EC (v1.x80*)	Diagnostics	**CCA Failures.** Reset/Read count of CCA (Clear Channel Assessment) failures. This parameter value increments when the module does not transmit a packet because it detected energy above the CCA threshold level set with CA command. This count saturates at its maximum value. Set count to "0" to reset count.	0 - 0xFFFF	-
EA (v1.x80*)	Diagnostics	**ACK Failures**. Reset/Read count of acknowledgment failures. This parameter value increments when the module expires its transmission retries without receiving an ACK on a packet transmission. This count saturates at its maximum value. Set the parameter to "0" to reset count.	0 - 0xFFFF	-
ED (v1.x80*)	Diagnostics	**Energy Scan**. Send 'Energy Detect Scan'. ED parameter determines the length of scan on each channel. The maximal energy on each channel is returned and each value is followed by a carriage return. Values returned represent detected energy levels in units of -dBm. Actual scan time on each channel is measured as Time = [(2 ^ SD) * 15.36] ms. Total scan time is this time multiplied by the number of channels to be scanned.	0 - 6	-

* Firmware version in which the command was first introduced (firmware versions are numbered in hexadecimal notation.)

AT Command Options

Table 3-08. XBee®/XBee-PRO® Commands - AT Command Options

AT Command	Command Category	Name and Description	Parameter Range	Default
CT	AT Command Mode Options	**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.	2 - 0xFFFF [x 100 ms]	0x64 (100d)
CN	AT Command Mode Options	**Exit Command Mode**. Explicitly exit the module from AT Command Mode.	--	--
AC (v1.xA0*)	AT Command Mode Options	**Apply Changes**. Explicitly apply changes to queued parameter value(s) and re-initialize module.	--	--
GT	AT Command Mode Options	**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.	2 - 0x0CE4 [x 1 ms]	0x3E8 (1000d)
CC	AT Command Mode Options	**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.	0 - 0xFF	0x2B ('+' ASCII)

* Firmware version in which the command was first introduced (firmware versions are numbered in hexadecimal notation.)

Command Descriptions

Command descriptions in this section are listed alphabetically. Command categories are designated within "< >" symbols that follow each command title. XBee®/XBee-PRO® RF Modules expect parameter values in hexadecimal (designated by the "0x" prefix).

All modules operating within the same network should contain the same firmware version.

A1 (End Device Association) Command

<Networking {Association}> The A1 command is used to set and read association options for an End Device.

Use the table below to determine End Device behavior in relation to the A1 parameter.

AT Command: ATA1

Parameter Range: 0 – 0x0F [bitfield]

Default Parameter Value: 0

Related Commands: ID (PAN ID), NI (Node Identifier), CH (Channel), CE (Coordinator Enable), A2 (Coordinator Association)

Minimum Firmware Version Required: v1.x80

Bit number	End Device Association Option
0 - ReassignPanID	0 - Will only associate with Coordinator operating on PAN ID that matches Node Identifier
	1 - May associate with Coordinator operating on any PAN ID
1 - ReassignChannel	0 - Will only associate with Coordinator operating on Channel that matches CH setting
	1 - May associate with Coordinator operating on any Channel
2 - AutoAssociate	0 - Device will not attempt Association
	1 - Device attempts Association until success Note: This bit is used only for Non-Beacon systems. End Devices in a Beaconing system must always associate to a Coordinator
3 - PollCoordOnPinWake	0 - Pin Wake will not poll the Coordinator for pending (indirect) Data
	1 - Pin Wake will send Poll Request to Coordinator to extract any pending data
4 - 7	[reserved]

A2 (Coordinator Association) Command

<Networking {Association}> The A2 command is used to set and read association options of the Coordinator.

Use the table below to determine Coordinator behavior in relation to the A2 parameter.

AT Command: ATA2

Parameter Range: 0 – 7 [bitfield]

Default Parameter Value: 0

Related Commands: ID (PAN ID), NI (Node Identifier), CH (Channel), CE (Coordinator Enable), A1 (End Device Association), AS Active Scan), ED (Energy Scan)

Minimum Firmware Version Required: v1.x80

Bit number	End Device Association Option
0 - ReassignPanID	0 - Coordinator will not perform Active Scan to locate available PAN ID. It will operate on ID (PAN ID).
	1 - Coordinator will perform Active Scan to determine an available ID (PAN ID). If a PAN ID conflict is found, the ID parameter will change.
1 - ReassignChannel	0 - Coordinator will not perform Energy Scan to determine free channel. It will operate on the channel determined by the CH parameter.
	1 - Coordinator will perform Energy Scan to find a free channel, then operate on that channel.
2 - AllowAssociate	0 - Coordinator will not allow any devices to associate to it.
	1 - Coordinator will allow devices to associate to it.
3 - 7	[reserved]

The binary equivalent of the default value (0x06) is 00000110. ‘Bit 0’ is the last digit of the sequence.

AC (Apply Changes) Command

<AT Command Mode Options> The AC command is used to explicitly apply changes to module parameter values. 'Applying changes' means that the module is re-initialized based on changes made to its parameter values. Once changes are applied, the module immediately operates according to the new parameter values.

AT Command: ATAC

Minimum Firmware Version Required: v1.xA0

This behavior is in contrast to issuing the WR (Write) command. The WR command saves parameter values to non-volatile memory, but the module still operates according to previously saved values until the module is re-booted or the CN (Exit AT Command Mode) command is issued.

Refer to the "AT Command - Queue Parameter Value" API type for more information.

AI (Association Indication) Command

<Networking {Association}> The AI command is used to indicate occurrences of errors during the last association request.

Use the table below to determine meaning of the returned values.

AT Command: ATAI

Parameter Range: 0 - 0x13 [read-only]

Related Commands: AS (Active Scan), ID (PAN ID), CH (Channel), ED (Energy Scan), A1 (End Device Association), A2 (Coordinator Association), CE (Coordinator Enable)

Minimum Firmware Version Required: v1.x80

Returned Value (Hex)	Association Indication
0x00	Successful Completion - Coordinator successfully started or End Device association complete
0x01	Active Scan Timeout
0x02	Active Scan found no PANs
0x03	Active Scan found PAN, but the Coordinator Allow Association bit is not set
0x04	Active Scan found PAN, but Coordinator and End Device are not configured to support beacons
0x05	Active Scan found PAN, but Coordinator ID (PAN ID) value does not match the ID of the End Device
0x06	Active Scan found PAN, but Coordinator CH (Channel) value does not match the CH of the End Device
0x07	Energy Scan Timeout
0x08	Coordinator start request failed
0x09	Coordinator could not start due to Invalid Parameter
0x0A	Coordinator Realignment is in progress
0x0B	Association Request not sent
0x0C	Association Request timed out - no reply was received
0x0D	Association Request had an Invalid Parameter
0x0E	Association Request Channel Access Failure - Request was not transmitted - CCA failure
0x0F	Remote Coordinator did not send an ACK after Association Request was sent
0x10	Remote Coordinator did not reply to the Association Request, but an ACK was received after sending the request
0x11	[reserved]
0x12	Sync-Loss - Lost synchronization with a Beaconing Coordinator
0x13	Disassociated - No longer associated to Coordinator
0xFF	RF Module is attempting to associate

AP (API Enable) Command

<Serial Interfacing> The AP command is used to enable the RF module to operate using a frame-based API instead of using the default Transparent (UART) mode.

AT Command: ATAP

Parameter Range:0 – 2

Parameter	Configuration
0	Disabled (Transparent operation)
1	API enabled
2	API enabled (with escaped characters)

Default Parameter Value:0

Minimum Firmware Version Required: v1.x80

Refer to the API Operation section when API operation is enabled (AP = 1 or 2).

AS (Active Scan) Command

<Network {Association}> The AS command is used to send a Beacon Request to a Broadcast (0xFFFF) and Broadcast PAN (0xFFFF) on every channel. The parameter determines the amount of time the RF module will listen for Beacons on each channel. A 'PanDescriptor' is created and returned for every Beacon received from the scan. Each PanDescriptor contains the following information:

AT Command: ATAS

Parameter Range: 0 – 6

Related Command: SD (Scan Duration), DL (Destination Low Address), DH (Destination High Address), ID (PAN ID), CH (Channel)

Minimum Firmware Version Required: v1.x80

CoordAddress (SH + SL parameters)<CR> (NOTE: If MY on the coordinator is set less than 0xFFFF, the MY value is displayed)
CoordPanID (ID parameter)<CR>
CoordAddrMode <CR>
- 0x02 = 16-bit Short Address
- 0x03 = 64-bit Long Address

Channel (CH parameter) <CR>
SecurityUse<CR>
ACLEntry<CR>
SecurityFailure<CR>
SuperFrameSpec<CR> (2 bytes):
- bit 15 - Association Permitted (MSB)
- bit 14 - PAN Coordinator
- bit 13 - Reserved
- bit 12 - Battery Life Extension
- bits 8-11 - Final CAP Slot
- bits 4-7 - Superframe Order
- bits 0-3 - Beacon Order

GtsPermit<CR>
RSSI<CR> (- RSSI is returned as -dBm)
TimeStamp<CR> (3 bytes)
<CR> (A carriage return <CR> is sent at the end of the AS command.

The Active Scan is capable of returning up to 5 PanDescriptors in a scan. The actual scan time on each channel is measured as Time = [(2 ^ (SD Parameter)) * 15.36] ms. Total scan time is this time multiplied by the number of channels to be scanned (16 for the XBee, 12 for the XBee-PRO).

NOTE: Refer the scan table in the SD description to determine scan times. If using API Mode, no <CR>'s are returned in the response. Refer to the API Mode Operation section.

BD (Interface Data Rate) Command

<Serial Interfacing> The BD command is used to set and read the serial interface data rate used between the RF module and host. This parameter determines the rate at which serial data is sent to the module from the host. Modified interface data rates do not take effect until the CN (Exit AT Command Mode) command is issued and the system returns the 'OK' response.

When parameters 0-7 are sent to the module, the respective interface data rates are used (as shown in the table on the right).

The RF data rate is not affected by the BD parameter. If the interface data rate is set higher than the RF data rate, a flow control configuration may need to be implemented.

AT Command: ATBD

Parameter Range:0 – 7 (standard rates)
0x80-0x3D090 (non-standard rates up to 250 Kbps)

Parameter	Configuration (bps)
0	1200
1	2400
2	4800
3	9600
4	19200
5	38400
6	57600
7	115200

Default Parameter Value:3

Non-standard Interface Data Rates:
Any value above 0x07 will be interpreted as an actual baud rate. When a value above 0x07 is sent, the closest interface data rate represented by the number is stored in the BD register. For example, a rate of 19200 bps can be set by sending the following command line "ATBD4B00". NOTE: When using Digi's X-CTU Software, non-standard interface data rates can only be set and read using the X-CTU 'Terminal' tab. Non-standard rates are not accessible through the 'Modem Configuration' tab.

When the BD command is sent with a non-standard interface data rate, the UART will adjust to accommodate the requested interface rate. In most cases, the clock resolution will cause the stored BD parameter to vary from the parameter that was sent (refer to the table below). Reading the BD command (send "ATBD" command without an associated parameter value) will return the value actually stored in the module's BD register.

Parameters Sent Versus Parameters Stored

BD Parameter Sent (HEX)	Interface Data Rate (bps)	BD Parameter Stored (HEX)
0	1200	0
4	19,200	4
7	115,200*	7
12C	300	12B
1C200	115,200	1B207

* The 115,200 baud rate setting is actually at 111,111 baud (-3.5% target UART speed).

CA (CCA Threshold) Command

<RF Interfacing> CA command is used to set and read CCA (Clear Channel Assessment) thresholds.

Prior to transmitting a packet, a CCA is performed to detect energy on the transmit channel. If the detected energy is above the CCA Threshold, the RF module will not transmit the packet.

AT Command: ATCA

Parameter Range: 0 – 0x50 [-dBm]

Default Parameter Value: 0x2C
(-44 decimal dBm)

Minimum Firmware Version Required: v1.x80

CC (Command Sequence Character) Command

<AT Command Mode Options> The CC command is used to set and read the ASCII character used between guard times of the AT Command Mode Sequence (GT + CC + GT). This sequence enters the RF module into AT Command Mode so that data entering the module from the host is recognized as commands instead of payload.

AT Command: ATCC
Parameter Range: 0 – 0xFF
Default Parameter Value: 0x2B (ASCII "+")
Related Command: GT (Guard Times)

The AT Command Sequence is explained further in the AT Command Mode section.

CE (Coordinator Enable) Command

<Networking {Association} The CE command is used to set and read the behavior (End Device vs. Coordinator) of the RF module.

AT Command: ATCE

Parameter Range:0 – 1

Parameter	Configuration
0	End Device
1	Coordinator

Default Parameter Value:0

Minimum Firmware Version Required: v1.x80

CH (Channel) Command

<Networking {Addressing}> The CH command is used to set/read the operating channel on which RF connections are made between RF modules. The channel is one of three addressing options available to the module. The other options are the PAN ID (ID command) and destination addresses (DL & DH commands).

AT Command: ATCH
Parameter Range: 0x0B – 0x1A (XBee) 0x0C – 0x17 (XBee-PRO)
Default Parameter Value: 0x0C (12 decimal)
Related Commands: ID (PAN ID), DL (Destination Address Low, DH (Destination Address High)

In order for modules to communicate with each other, the modules must share the same channel number. Different channels can be used to prevent modules in one network from listening to transmissions of another. Adjacent channel rejection is 23 dB.

The module uses channel numbers of the 802.15.4 standard.

Center Frequency = 2.405 + (CH - 11d) * 5 MHz (d = decimal)

Refer to the XBee/XBee-PRO Addressing section for more information.

CN (Exit Command Mode) Command

<AT Command Mode Options> The CN command is used to explicitly exit the RF module from AT Command Mode.

AT Command: ATCN

CT (Command Mode Timeout) Command

<AT Command Mode Options> The CT command is used to set and read the amount of inactive time that elapses before the RF module automatically exits from AT Command Mode and returns to Idle Mode.

Use the CN (Exit Command Mode) command to exit AT Command Mode manually.

AT Command: ATCT
Parameter Range:2 – 0xFFFF [x 100 milliseconds]
Default Parameter Value: 0x64 (100 decimal (which equals 10 decimal seconds))
Number of bytes returned: 2
Related Command: CN (Exit Command Mode)

D0 - D4 (DIOn Configuration) Commands

<I/O Settings> The D0, D1, D2, D3 and D4 commands are used to select/read the behavior of their respective AD/DIO lines (pins 20, 19, 18, 17 and 11 respectively).

Options include:

- Analog-to-digital converter
- Digital input
- Digital output

AT Commands:
ATD0, ATD1, ATD2, ATD3, ATD4

Parameter Range:0 - 5

Parameter	Configuration
0	Disabled
1	n/a
2	ADC
3	DI
4	DO low
5	DO high

Default Parameter Value:0

Minimum Firmware Version Required: 1.x.A0

D5 (DIO5 Configuration) Command

<I/O Settings> The D5 command is used to select/read the behavior of the DIO5 line (pin 15).

Options include:

- Associated Indicator (LED blinks when the module is associated)
- Analog-to-digital converter
- Digital input
- Digital output

AT Command: ATD5

Parameter Range:0 - 5

Parameter	Configuration
0	Disabled
1	Associated Indicator
2	ADC
3	DI
4	DO low
5	DO high

Default Parameter Value:1

Parameters 2-5 supported as of firmware version 1.xA0

D6 (DIO6 Configuration) Command

<I/O Settings> The D6 command is used to select/read the behavior of the DIO6 line (pin 16). Options include:

- RTS flow control
- Analog-to-digital converter
- Digital input
- Digital output

AT Command: ATD6

Parameter Range:0 - 5

Parameter	Configuration
0	Disabled
1	RTS Flow Control
2	n/a
3	DI
4	DO low
5	DO high

Default Parameter Value:0

Parameters 3-5 supported as of firmware version 1.xA0

D7 (DIO7 Configuration) Command

<I/O Settings> The D7 command is used to select/read the behavior of the DIO7 line (pin 12). Options include:

- CTS flow control
- Analog-to-digital converter
- Digital input
- Digital output
- RS485 TX Enable (this output is 3V CMOS level, and is useful in a 3V CMOS to RS485 conversion circuit)

AT Command: ATD7

Parameter Range:0 – 5

Parameter	Configuration
0	Disabled
1	CTS Flow Control
2	n/a
3	DI
4	DO low
5	DO high
6	RS485 TX Enable Low
7	RS485 TX Enable High

Default Parameter Value:1

Parameters 3-7 supported as of firmware version 1.x.A0

D8 (DI8 Configuration) Command

<I/O Settings> The D8 command is used to select/read the behavior of the DI8 line (pin 9). This command enables configuring the pin to function as a digital input. This line is also used with Pin Sleep.

AT Command: ATD8

Parameter Range:0 – 5
(1, 2, 4 & 5 n/a)

Parameter	Configuration
0	Disabled
3	DI

Default Parameter Value:0

Minimum Firmware Version Required: 1.xA0

DA (Force Disassociation) Command

<(Special)> The DA command is used to immediately disassociate an End Device from a Coordinator and reattempt to associate.

AT Command: ATDA

Minimum Firmware Version Required: v1.x80

DB (Received Signal Strength) Command

<Diagnostics> DB parameter is used to read the received signal strength (in dBm) of the last RF packet received. Reported values are accurate between -40 dBm and the RF module's receiver sensitivity.

AT Command: ATDB

Parameter Range [read-only]:
0x17-0x5C (XBee), 0x24-0x64 (XBee-PRO)

Absolute values are reported. For example: 0x58 = -88 dBm (decimal). If no packets have been received (since last reset, power cycle or sleep event), "0" will be reported.

DH (Destination Address High) Command

<Networking {Addressing}> The DH command is used to set and read the upper 32 bits of the RF module's 64-bit destination address. When combined with the DL (Destination Address Low) parameter, it defines the destination address used for transmission.

An module will only communicate with other modules having the same channel (CH parameter), PAN ID (ID parameter) and destination address (DH + DL parameters).

AT Command: ATDH

Parameter Range: 0 – 0xFFFFFFFF

Default Parameter Value: 0

Related Commands: DL (Destination Address Low), CH (Channel), ID (PAN VID), MY (Source Address)

To transmit using a 16-bit address, set the DH parameter to zero and the DL parameter less than 0xFFFF. 0x000000000000FFFF (DL concatenated to DH) is the broadcast address for the PAN.

Refer to the XBee/XBee-PRO Addressing section for more information.

DL (Destination Address Low) Command

<Networking {Addressing}> The DL command is used to set and read the lower 32 bits of the RF module's 64-bit destination address. When combined with the DH (Destination Address High) parameter, it defines the destination address used for transmission.

AT Command: ATDL
Parameter Range: 0 - 0xFFFFFFFF
Default Parameter Value: 0
Related Commands: DH (Destination Address High), CH (Channel), ID (PAN VID), MY (Source Address)

A module will only communicate with other modules having the same channel (CH parameter), PAN ID (ID parameter) and destination address (DH + DL parameters).

To transmit using a 16-bit address, set the DH parameter to zero and the DL parameter less than 0xFFFF. 0x000000000000FFFF (DL concatenated to DH) is the broadcast address for the PAN.

Refer to the XBee/XBee-PRO Addressing section for more information.

DN (Destination Node) Command

<Networking {Identification}> The DN command is used to resolve a NI (Node Identifier) string to a physical address. The following events occur upon successful command execution:

AT Command: ATDN
Parameter Range: 20-character ASCII String
Minimum Firmware Version Required: v1.x80

1. DL and DH are set to the address of the module with the matching NI (Node Identifier).
2. 'OK' is returned.
3. RF module automatically exits AT Command Mode.

If there is no response from a modem within 200 msec or a parameter is not specified (left blank), the command is terminated and an 'ERROR' message is returned.

DP (Disassociation Cyclic Sleep Period) Command

<Sleep Mode (Low Power)>

NonBeacon Firmware

End Device - The DP command is used to set and read the time period of sleep for cyclic sleeping remotes that are configured for Association but are not associated to a Coordinator. (i.e. If a device is configured to associate, configured as a Cyclic Sleep remote, but does not find a Coordinator; it will sleep for DP time before reattempting association.) Maximum sleep period is 268 seconds (0x68B0). DP should be > 0 for NonBeacon systems.

AT Command: ATDP
Parameter Range: 1 - 0x68B0 [x 10 milliseconds]
Default Parameter Value:0x3E8 (1000 decimal)
Related Commands: SM (Sleep Mode), SP (Cyclic Sleep Period), ST (Time before Sleep)
Minimum Firmware Version Required: v1.x80

EA (ACK Failures) Command

<Diagnostics> The EA command is used to reset and read the count of ACK (acknowledgement) failures. This parameter value increments when the module expires its transmission retries without receiving an ACK on a packet transmission. This count saturates at its maximum value.

AT Command: ATEA
Parameter Range:0 - 0xFFFF
Minimum Firmware Version Required: v1.x80

Set the parameter to "0" to reset count.

EC (CCA Failures) Command

<Diagnostics> The EC command is used to read and reset the count of CCA (Clear Channel Assessment) failures. This parameter value increments when the RF module does not transmit a packet due to the detection of energy that is above the CCA threshold level (set with CA command). This count saturates at its maximum value.

Set the EC parameter to "0" to reset count.

AT Command: ATEC
Parameter Range:0 – 0xFFFF
Related Command: CA (CCA Threshold)
Minimum Firmware Version Required: v1.x80

ED (Energy Scan) Command

<Networking {Association}> The ED command is used to send an "Energy Detect Scan". This parameter determines the length of scan on each channel. The maximal energy on each channel is returned and each value is followed by a carriage return. An additional carriage return is sent at the end of the command.

AT Command: ATED
Parameter Range:0 – 6
Related Command: SD (Scan Duration), SC (Scan Channel)
Minimum Firmware Version Required: v1.x80

The values returned represent the detected energy level in units of -dBm. The actual scan time on each channel is measured as Time = [(2 ^ ED PARAM) * 15.36] ms.

Note: Total scan time is this time multiplied by the number of channels to be scanned. Also refer to the SD (Scan Duration) table. Use the SC (Scan Channel) command to choose which channels to scan.

EE (AES Encryption Enable) Command

<Networking {Security}> The EE command is used to set/read the parameter that disables/enables 128-bit AES encryption.

The XBee®/XBee-PRO® firmware uses the 802.15.4 Default Security protocol and uses AES encryption with a 128-bit key. AES encryption dictates that all modules in the network use the same key and the maximum RF packet size is 95 Bytes.

AT Command: ATEE		
Parameter Range:0 – 1		
	Parameter	Configuration
	0	Disabled
	1	Enabled
Default Parameter Value:0		
Related Commands: KY (Encryption Key), AP (API Enable), MM (MAC Mode)		
Minimum Firmware Version Required: v1.xA0		

When encryption is enabled, the module will always use its 64-bit long address as the source address for RF packets. This does not affect how the MY (Source Address), DH (Destination Address High) and DL (Destination Address Low) parameters work

If MM (MAC Mode) > 0 and AP (API Enable) parameter > 0:
With encryption enabled and a 16-bit short address set, receiving modules will only be able to issue RX (Receive) 64-bit indicators. This is not an issue when MM = 0.

If a module with a non-matching key detects RF data, but has an incorrect key: When encryption is enabled, non-encrypted RF packets received will be rejected and will not be sent out the UART.

Transparent Operation --> All RF packets are sent encrypted if the key is set.

API Operation --> Receive frames use an option bit to indicate that the packet was encrypted.

FP (Force Poll) Command

<Networking (Association)> The FP command is used to request indirect messages being held by a Coordinator.

AT Command: ATFP
Minimum Firmware Version Required: v1.x80

FR (Software Reset) Command

<Special> The FR command is used to force a software reset on the RF module. The reset simulates powering off and then on again the module.

AT Command: ATFR

Minimum Firmware Version Required: v1.x80

GT (Guard Times) Command

<AT Command Mode Options> GT Command is used to set the DI (data in from host) time-of-silence that surrounds the AT command sequence character (CC Command) of the AT Command Mode sequence (GT + CC + GT).

The DI time-of-silence is used to prevent inadvertent entrance into AT Command Mode.

Refer to the Command Mode section for more information regarding the AT Command Mode Sequence.

AT Command: ATGT

Parameter Range:2 – 0x0CE4 [x 1 millisecond]

Default Parameter Value:0x3E8 (1000 decimal)

Related Command: CC (Command Sequence Character)

HV (Hardware Version) Command

<Diagnostics> The HV command is used to read the hardware version of the RF module.

AT Command: ATHV

Parameter Range:0 – 0xFFFF [Read-only]

Minimum Firmware Version Required: v1.x80

IA (I/O Input Address) Command

<I/O Settings {I/O Line Passing}> The IA command is used to bind a module output to a specific address. Outputs will only change if received from this address. The IA command can be used to set/read both 16 and 64-bit addresses.

Setting all bytes to 0xFF will not allow the reception of any I/O packet to change outputs. Setting the IA address to 0xFFFF will cause the module to accept all I/O packets.

AT Command: ATIA

Parameter Range:0 – 0xFFFFFFFFFFFFFFFF

Default Parameter Value:0xFFFFFFFFFFFFFFFF (will not allow any received I/O packet to change outputs)

Minimum Firmware Version Required: v1.xA0

IC (DIO Change Detect) Command

<I/O Settings> Set/Read bitfield values for change detect monitoring. Each bit enables monitoring of DIO0 - DIO7 for changes.

If detected, data is transmitted with DIO data only. Any samples queued waiting for transmission will be sent first.

AT Command: ATIC

Parameter Range:0 – 0xFF [bitfield]

Default Parameter Value:0 (disabled)

Minimum Firmware Version Required: 1.xA0

Refer to the "ADC and Digital I/O Line Support" sections of the "RF Module Operations" chapter for more information.

ID (Pan ID) Command

<Networking {Addressing}> The ID command is used to set and read the PAN (Personal Area Network) ID of the RF module. Only modules with matching PAN IDs can communicate with each other. Unique PAN IDs enable control of which RF packets are received by a module.

AT Command: ATID

Parameter Range: 0 – 0xFFFF

Default Parameter Value:0x3332 (13106 decimal)

Setting the ID parameter to 0xFFFF indicates a global transmission for all PANs. It does not indicate a global receive.

IO (Digital Output Level) Command

<I/O Settings> The IO command is used to set digital output levels. This allows DIO lines setup as outputs to be changed through Command Mode.

AT Command: ATIO
Parameter Range: 8-bit bitmap (where each bit represents the level of an I/O line that is setup as an output.)
Minimum Firmware Version Required: v1.xA0

IR (Sample Rate) Command

<I/O Settings> The IR command is used to set/read the sample rate. When set, the module will sample all enabled DIO/ADC lines at a specified interval. This command allows periodic reads of the ADC and DIO lines in a non-Sleep Mode setup. A sample rate which requires transmissions at a rate greater than once every 20ms is not recommended.

AT Command: ATIR
Parameter Range: 0 - 0xFFFF [x 1 msec] (cannot guarantee 1 ms timing when IT=1)
Default Parameter Value:0
Related Command: IT (Samples before TX)
Minimum Firmware Version Required: v1.xA0

Example: When IR = 0x14, the sample rate is 20 ms (or 50 Hz).

IS (Force Sample) Command

<I/O Settings> The IS command is used to force a read of all enabled DIO/ADC lines. The data is returned through the UART.

When operating in Transparent Mode (AP=0), the data is retuned in the following format:

AT Command: ATIS
Parameter Range: 1 - 0xFF
Default Parameter Value:1
Minimum Firmware Version Required: v1.xA0

All bytes are converted to ASCII:
number of samples<CR>
channel mask<CR>
DIO data<CR> (If DIO lines are enabled<CR>
ADC channel Data<cr> <-This will repeat for every enabled ADC channel<CR>
<CR> (end of data noted by extra <CR>)

When operating in API mode (AP > 0), the command will immediately return an 'OK' response. The data will follow in the normal API format for DIO data.

IT (Samples before TX) Command

<I/O Settings> The IT command is used to set/read the number of DIO and ADC samples to collect before transmitting data.

One ADC sample is considered complete when all enabled ADC channels have been read. The module can buffer up to 93 Bytes of sample data.

AT Command: ATIT
Parameter Range: 1 - 0xFF
Default Parameter Value:1
Minimum Firmware Version Required: v1.xA0

Since the module uses a 10-bit A/D converter, each sample uses two Bytes. This leads to a maximum buffer size of 46 samples or IT=0x2E.

When Sleep Modes are enabled and IR (Sample Rate) is set, the module will remain awake until IT samples have been collected.

IU (I/O Output Enable) Command

<I/O Settings> The IU command is used to disable/enable I/O UART output. When enabled (IU = 1), received I/O line data packets are sent out the UART. The data is sent using an API frame regardless of the current AP parameter value.

AT Command: ATIU

Parameter Range:0 – 1

Parameter	Configuration
0	Disabled – Received I/O line data packets will be NOT sent out UART.
1	Enabled – Received I/O line data will be sent out UART

Default Parameter Value:1

Minimum Firmware Version Required: 1.xA0

KY (AES Encryption Key) Command

<Networking {Security}> The KY command is used to set the 128-bit AES (Advanced Encryption Standard) key for encrypting/decrypting data. Once set, the key cannot be read out of the module by any means.

AT Command: ATKY

Parameter Range:0 – (any 16-Byte value)

Default Parameter Value:0

Related Command: EE (Encryption Enable)

Minimum Firmware Version Required: v1.xA0

The entire payload of the packet is encrypted using the key and the CRC is computed across the ciphertext. When encryption is enabled, each packet carries an additional 16 Bytes to convey the random CBC Initialization Vector (IV) to the receiver(s). The KY value may be "0" or any 128-bit value. Any other value, including entering KY by itself with no parameters, is invalid. All ATKY entries (valid or not) are received with a returned 'OK'.

A module with the wrong key (or no key) will receive encrypted data, but the data driven out the serial port will be meaningless. A module with a key and encryption enabled will receive data sent from a module without a key and the correct unencrypted data output will be sent out the serial port. Because CBC mode is utilized, repetitive data appears differently in different transmissions due to the randomly-generated IV.

When queried, the system will return an 'OK' message and the value of the key will not be returned.

M0 (PWM0 Output Level) Command

<I/O Settings> The M0 command is used to set/read the output level of the PWM0 line (pin 6).

Before setting the line as an output:

1. Enable PWM0 output (P0 = 2)
2. Apply settings (use CN or AC)

The PWM period is 64 µsec and there are 0x03FF (1023 decimal) steps within this period. When M0 = 0 (0% PWM), 0x01FF (50% PWM), 0x03FF (100% PWM), etc.

AT Command: ATM0

Parameter Range:0 – 0x03FF [steps]

Default Parameter Value:0

Related Commands: P0 (PWM0 Enable), AC (Apply Changes), CN (Exit Command Mode)

Minimum Firmware Version Required: v1.xA0

M1 (PWM1 Output Level) Command

<I/O Settings> The M1 command is used to set/read the output level of the PWM1 line (pin 7).

Before setting the line as an output:

1. Enable PWM1 output (P1 = 2)
2. Apply settings (use CN or AC)

AT Command: ATM1

Parameter Range:0 – 0x03FF

Default Parameter Value:0

Related Commands: P1 (PWM1 Enable), AC (Apply Changes), CN (Exit Command Mode)

Minimum Firmware Version Required: v1.xA0

MM (MAC Mode) Command

<Networking {Addressing}> The MM command is used to set and read the MAC Mode value. The MM command disables/enables the use of a Digi header contained in the 802.15.4 RF packet. By default (MM = 0), Digi Mode is enabled and the module adds an extra header to the data portion of the 802.15.4 packet. This enables the following features:

- ND and DN command support
- Duplicate packet detection when using ACKs
- "RR command
- "DIO/AIO sampling support

The MM command allows users to turn off the use of the extra header. Modes 1 and 2 are strict 802.15.4 modes. If the Digi header is disabled, ND and DN parameters are also disabled.

Note: When MM=0 or 3, application and CCA failure retries are not supported.

AT Command: ATMM

Parameter Range:0 – 3

Parameter	Configuration
0	Digi Mode (802.15.4 + Digi header)
1	802.15.4 (no ACKs)
2	802.15.4 (with ACKs)
3	Digi Mode (no ACKs)

Default Parameter Value:0

Related Commands: ND (Node Discover), DN (Destination Node)

Minimum Firmware Version Required: v1.x80

MY (16-bit Source Address) Command

<Networking {Addressing}> The MY command is used to set and read the 16-bit source address of the RF module.

By setting MY to 0xFFFF, the reception of RF packets having a 16-bit address is disabled. The 64-bit address is the module's serial number and is always enabled.

AT Command: ATMY

Parameter Range: 0 – 0xFFFF

Default Parameter Value: 0

Related Commands: DH (Destination Address High), DL (Destination Address Low), CH (Channel), ID (PAN ID)

NB (Parity) Command

<Serial Interfacing> The NB command is used to select/read the parity settings of the RF module for UART communications.

Note: the module does not actually calculate and check the parity; it only interfaces with devices at the configured parity and stop bit settings.

AT Command: ATNB

Parameter Range: 0 – 4

Parameter	Configuration
0	8-bit no parity
1	8-bit even
2	8-bit odd
3	8-bit mark
4	8-bit space

Default Parameter Value: 0

Number of bytes returned: 1

ND (Node Discover) Command

AT Command: ATND
Range: optional 20-character NI value
Related Commands: CH (Channel), ID (Pan ID), MY (Source Address), SH (Serial Number High), SL (Serial Number Low), NI (Node Identifier), NT (Node Discover Time)
Minimum Firmware Version Required: v1.x80

<Networking {Identification}> The ND command is used to discover and report all modules on its current operating channel (CH parameter) and PAN ID (ID parameter). ND also accepts an NI (Node Identifier) value as a parameter. In this case, only a module matching the supplied identifier will respond.

ND uses a 64-bit long address when sending and responding to an ND request. The ND command causes a module to transmit a globally addressed ND command packet. The amount of time allowed for responses is determined by the NT (Node Discover Time) parameter.

In AT Command mode, command completion is designated by a carriage return (0x0D). Since two carriage returns end a command response, the application will receive three carriage returns at the end of the command. If no responses are received, the application should only receive one carriage return. When in API mode, the application should receive a frame (with no data) and status (set to 'OK') at the end of the command. When the ND command packet is received, the remote sets up a random time delay (up to 2.2 sec) before replying as follows:

Node Discover Response (AT command mode format - Transparent operation):
MY (Source Address) value<CR>
SH (Serial Number High) value<CR>
SL (Serial Number Low) value<CR>
DB (Received Signal Strength) value<CR>
NI (Node Identifier) value<CR>
<CR> (This is part of the response and not the end of command indicator.)

Node Discover Response (API format - data is binary (except for NI)):
2 bytes for MY (Source Address) value
4 bytes for SH (Serial Number High) value
4 bytes for SL (Serial Number Low) value
1 byte for DB (Received Signal Strength) value
NULL-terminated string for NI (Node Identifier) value (max 20 bytes w/out NULL terminator)

NI (Node Identifier) Command

AT Command: ATNI
Parameter Range: 20-character ASCII string
Related Commands: ND (Node Discover), DN (Destination Node)
Minimum Firmware Version Required: v1.x80

<Networking {Identification}> The NI command is used to set and read a string for identifying a particular node.

Rules:

- Register only accepts printable ASCII data.
- A string can not start with a space.
- A carriage return ends command
- Command will automatically end when maximum bytes for the string have been entered.

This string is returned as part of the ND (Node Discover) command. This identifier is also used with the DN (Destination Node) command.

NO (Node Discover Options) Command

AT Command: ATNO
Parameter Range: "0-1
Related Commands: ND (Node Discover), DN (Destination Node)
Minimum Firmware Version Required: v1.xC5

<Networking {Identification}> The NO command is used to suppress/include a self-response to Node Discover commands. When NO=1 a module doing a Node Discover will include a response entry for itself.

NT (Node Discover Time) Command

<Networking {Identification}> The NT command is used to set the amount of time a base node will wait for responses from other nodes when using the ND (Node Discover) command. The NT value is transmitted with the ND command.

Remote nodes will set up a random hold-off time based on this time. The remotes will adjust this time down by 250 ms to give each node the ability to respond before the base ends the command. Once the ND command has ended, any response received on the base will be discarded.

AT Command: ATNT
Parameter Range: 0x01 - 0xFC [x 100 msec]
Default: 0x19 (2.5 decimal seconds)
Related Commands: ND (Node Discover)
Minimum Firmware Version Required: 1.xA0

P0 (PWM0 Configuration) Command

<I/O Setting {I/O Line Passing}> The P0 command is used to select/read the function for PWM0 (Pulse Width Modulation output 0). This command enables the option of translating incoming data to a PWM so that the output can be translated back into analog form.

With the IA (I/O Input Address) parameter correctly set, AD0 values can automatically be passed to PWM0.

AT Command: ATP0
The second character in the command is the number zero (“0”), not the letter “O”.

Parameter Range: 0 - 2

Parameter	Configuration
0	Disabled
1	RSSI
2	PWM0 Output

Default Parameter Value: 1

P1 (PWM1 Configuration) Command

<I/O Setting {I/O Line Passing}> The P1 command is used to select/read the function for PWM1 (Pulse Width Modulation output 1). This command enables the option of translating incoming data to a PWM so that the output can be translated back into analog form.

With the IA (I/O Input Address) parameter correctly set, AD1 values can automatically be passed to PWM1.

AT Command: ATP1

Parameter Range: 0 - 2

Parameter	Configuration
0	Disabled
1	RSSI
2	PWM1 Output

Default Parameter Value: 0

Minimum Firmware Version Required: v1.xA0

PL (Power Level) Command

<RF Interfacing> The PL command is used to select and read the power level at which the RF module transmits conducted power.

When operating in Europe, XBee-PRO 802.15.4 modules must operate at or below a transmit power output level of 10dBm. Customers have 2 choices for transmitting at or below 10dBm:

- Order the standard XBee-PRO module and change the PL command to "0" (10dBm),
- Order the International variant of the XBee-PRO module, which has a maximum transmit output power of 10dBm.

AT Command: ATPL

Parameter Range: 0 - 4

Parameter	XBee	XBee-PRO	XBee-PRO International variant
0	-10 dBm	10 dBm	PL=4: 10 dBm
1	-6 dBm	12 dBm	PL=3: 8 dBm
2	-4 dBm	14 dBm	PL=2: 2 dBm
3	-2 dBm	16 dBm	PL=1: -3 dBm
4	0 dBm	18 dBm	PL=0: -3 dBm

Default Parameter Value: 4

PR (Pull-up Resistor) Command

<Serial Interfacing> The PR command is used to set and read the bit field that is used to configure internal the pull-up resistor status for I/O lines. "1" specifies the pull-up resistor is enabled. "0" specifies no pull up.

AT Command: ATPR
Parameter Range: 0 – 0xFF
Default Parameter Value: 0xFF (all pull-up resistors are enabled)
Minimum Firmware Version Required: v1.x80

bit 0 - AD4/DIO4 (pin 11)
bit 1 - AD3/DIO3 (pin 17)
bit 2 - AD2/DIO2 (pin 18)
bit 3 - AD1/DIO1 (pin 19)
bit 4 - AD0/DIO0 (pin 20)
bit 5 - AD6/DIO6 (pin 16)
bit 6 - DI8 (pin 9)
bit 7 - DIN/CONFIG (pin 3)

For example: Sending the command "ATPR 6F" will turn bits 0, 1, 2, 3, 5 and 6 ON; and bits 4 & 7 will be turned OFF. (The binary equivalent of "0x6F" is "01101111". Note that 'bit 0' is the last digit in the bitfield.

PT (PWM Output Timeout) Command

<I/O Settings {I/O Line Passing}> The PT command is used to set/read the output timeout value for both PWM outputs.

When PWM is set to a non-zero value: Due to I/O line passing, a time is started which when expired will set the PWM output to zero. The timer is reset when a valid I/O packet is received.

AT Command: ATPT
Parameter Range: 0 – 0xFF [x 100 msec]
Default Parameter Value: 0xFF
Minimum Firmware Version Required: 1.xA0

RE (Restore Defaults) Command

AT Command: ATRE

<(Special)> The RE command is used to restore all configurable parameters to their factory default settings. The RE command does not write restored values to non-volatile (persistent) memory. Issue the WR (Write) command subsequent to issuing the RE command to save restored parameter values to non-volatile memory.

RN (Random Delay Slots) Command

<Networking & Security> The RN command is used to set and read the minimum value of the back-off exponent in the CSMA-CA algorithm. The CSMA-CA algorithm was engineered for collision avoidance (random delays are inserted to prevent data loss caused by data collisions).

AT Command: ATRN
Parameter Range: 0 – 3 [exponent]
Default Parameter Value: 0

If RN = 0, collision avoidance is disabled during the first iteration of the algorithm (802.15.4 - macMinBE).

CSMA-CA stands for "Carrier Sense Multiple Access - Collision Avoidance". Unlike CSMA-CD (reacts to network transmissions after collisions have been detected), CSMA-CA acts to prevent data collisions before they occur. As soon as a module receives a packet that is to be transmitted, it checks if the channel is clear (no other module is transmitting). If the channel is clear, the packet is sent over-the-air. If the channel is not clear, the module waits for a randomly selected period of time, then checks again to see if the channel is clear. After a time, the process ends and the data is lost.

RO (Packetization Timeout) Command

<Serial Interfacing> RO command is used to set and read the number of character times of inter-character delay required before transmission.

RF transmission commences when data is detected in the DI (data in from host) buffer and RO character times of silence are detected on the UART receive lines (after receiving at least 1 byte).

AT Command: ATRO
Parameter Range:0 – 0xFF [x character times]
Default Parameter Value: 3

RF transmission will also commence after 100 Bytes (maximum packet size) are received in the DI buffer.

Set the RO parameter to '0' to transmit characters as they arrive instead of buffering them into one RF packet.

RP (RSSI PWM Timer) Command

<I/O Settings {I/O Line Passing}> The RP command is used to enable PWM (Pulse Width Modulation) output on the RF module. The output is calibrated to show the level a received RF signal is above the sensitivity level of the module. The PWM pulses vary from 24 to 100%. Zero percent means PWM output is inactive. One to 24% percent means the received RF signal is at or below the published sensitivity level of the module. The following table shows levels above sensitivity and PWM values.

AT Command: ATRP
Parameter Range:0 – 0xFF [x 100 msec]
Default Parameter Value: 0x28 (40 decimal)

The total period of the PWM output is 64 µs. Because there are 445 steps in the PWM output, the minimum step size is 144 ns.

PWM Percentages

dB above Sensitivity	PWM percentage (high period / total period)
10	41%
20	58%
30	75%

A non-zero value defines the time that the PWM output will be active with the RSSI value of the last received RF packet. After the set time when no RF packets are received, the PWM output will be set low (0 percent PWM) until another RF packet is received. The PWM output will also be set low at power-up until the first RF packet is received. A parameter value of 0xFF permanently enables the PWM output and it will always reflect the value of the last received RF packet.

RR (XBee Retries) Command

<Networking {Addressing}> The RR command is used set/read the maximum number of retries the module will execute in addition to the 3 retries provided by the 802.15.4 MAC. For each XBee retry, the 802.15.4 MAC can execute up to 3 retries.

AT Command: ATRR
Parameter Range: 0 – 6
Default: 0
Minimum Firmware Version Required: 1.xA0

This values does not need to be set on all modules for retries to work. If retries are enabled, the transmitting module will set a bit in the Digi RF Packet header which requests the receiving module to send an ACK (acknowledgement). If the transmitting module does not receive an ACK within 200 msec, it will re-send the packet within a random period up to 48 msec. Each XBee retry can potentially result in the MAC sending the packet 4 times (1 try plus 3 retries). Note that retries are not attempted for packets that are purged when transmitting with a Cyclic Sleep Coordinator.

SC (Scan Channels) Command

<Networking {Association}> The SC command is used to set and read the list of channels to scan for all Active and Energy Scans as a bit field.

This affects scans initiated in command mode [AS (Active Scan) and ED (Energy Scan) commands] and during End Device Association and Coordinator startup.

AT Command: ATSC

Parameter Range: 1-0xFFFF [Bitfield]
(bits 0, 14, 15 are not allowed when using the XBee-PRO)

Default Parameter Value: 0x1FFE (all XBee-PRO channels)

Related Commands: ED (Energy Scan), SD (Scan Duration)

Minimum Firmware Version Required: v1.x80

bit 0 - 0x0B	bit 4 - 0x0F	bit 8 - 0x13	bit 12 - 0x17
bit 1 - 0x0C	bit 5 - 0x10	bit 9 - 0x14	bit 13 - 0x18
bit 2 - 0x0D	bit 6 - 0x11	bit 10 - 0x15	bit 14 - 0x19
bit 3 - 0x0E	bit 7 - 0x12	bit 11 - 0x16	bit 15 - 0x1A

SD (Scan Duration) Command

<Networking {Association}> The SD command is used to set and read the exponent value that determines the duration (in time) of a scan.

End Device (Duration of Active Scan during Association) - In a Beacon system, set SD = BE of the Coordinator. SD must be set at least to the highest BE parameter of any Beaconing Coordinator with which an End Device or Coordinator wish to discover.

AT Command: ATSD

Parameter Range: 0 – 0x0F

Default Parameter Value: 4

Related Commands: ED (Energy Scan), SC (Scan Channel)

Minimum Firmware Version Required: v1.x80

Coordinator - If the 'ReassignPANID' option is set on the Coordinator [refer to A2 parameter], the SD parameter determines the length of time the Coordinator will scan channels to locate existing PANs. If the 'ReassignChannel' option is set, SD determines how long the Coordinator will perform an Energy Scan to determine which channel it will operate on.

Scan Time is measured as ((# of Channels to Scan) * (2 ^ SD) * 15.36ms). The number of channels to scan is set by the SC command. The XBee RF Module can scan up to 16 channels (SC = 0xFFFF). The XBee PRO RF Module can scan up to 12 channels (SC = 0x1FFE).

Examples: Values below show results for a 12-channel scan

If SD = 0, time = 0.18 sec	SD = 8, time = 47.19 sec
SD = 2, time = 0.74 sec	SD = 10, time = 3.15 min
SD = 4, time = 2.95 sec	SD = 12, time = 12.58 min
SD = 6, time = 11.80 sec	SD = 14, time = 50.33 min

SH (Serial Number High) Command

<Diagnostics> The SH command is used to read the high 32 bits of the RF module's unique IEEE 64-bit address.

The module serial number is set at the factory and is read-only.

AT Command: ATSH

Parameter Range: 0 – 0xFFFFFFFF [read-only]

Related Commands: SL (Serial Number Low), MY (Source Address)

SL (Serial Number Low) Command

<Diagnostics> The SL command is used to read the low 32 bits of the RF module's unique IEEE 64-bit address.

The module serial number is set at the factory and is read-only.

AT Command: ATSL

Parameter Range: 0 – 0xFFFFFFFF [read-only]

Related Commands: SH (Serial Number High), MY (Source Address)

SM (Sleep Mode) Command

<Sleep Mode (Low Power)> The SM command is used to set and read Sleep Mode settings. By default, Sleep Modes are disabled (SM = 0) and the RF module remains in Idle/ Receive Mode. When in this state, the module is constantly ready to respond to either serial or RF activity.

* The Sleep Coordinator option (SM=6) only exists for backwards compatibility with firmware version 1.x06 only. In all other cases, use the CE command to enable a Coordinator.

AT Command: ATSM

Parameter Range: 0 – 6

Parameter	Configuration
0	Disabled
1	Pin Hibernate
2	Pin Doze
3	(reserved)
4	Cyclic Sleep Remote
5	Cyclic Sleep Remote (with Pin Wake-up)
6	Sleep Coordinator*

Default Parameter Value: 0

SO (Sleep Mode Command)

Sleep (Low Power) Sleep Options Set/Read the sleep mode options.

Bit 0 - Poll wakeup disable

- 0 - Normal operations. A module configured for cyclic sleep will poll for data on waking.
- 1 - Disable wakeup poll. A module configured for cyclic sleep will not poll for data on waking.

Bit 1 - ADC/DIO wakeup sampling disable.

- 0 - Normal operations. A module configured in a sleep mode with ADC/DIO sampling enabled will automatically perform a sampling on wakeup.
- 1 - Suppress sample on wakeup. A module configured in a sleep mode with ADC/DIO sampling enabled will not automatically sample on wakeup.

AT Command: ATSO

Parameter Range:	0-4
Default Parameter Value:	

Related Commands: SM (Sleep Mode), ST (Time before Sleep), DP (Disassociation Cyclic Sleep Period, BE (Beacon Order)

SP (Cyclic Sleep Period) Command

<Sleep Mode (Low Power)> The SP command is used to set and read the duration of time in which a remote RF module sleeps. After the cyclic sleep period is over, the module wakes and checks for data. If data is not present, the module goes back to sleep. The maximum sleep period is 268 seconds (SP = 0x68B0).

The SP parameter is only valid if the module is configured to operate in Cyclic Sleep (SM = 4-6). Coordinator and End Device SP values should always be equal.

To send Direct Messages, set SP = 0.

AT Command: ATSP

Parameter Range:	NonBeacon Firmware: 0-0x68B0 [x 10 milliseconds]
Default Parameter Value:	

Related Commands: SM (Sleep Mode), ST (Time before Sleep), DP (Disassociation Cyclic Sleep Period, BE (Beacon Order)

NonBeacon Firmware

End Device - SP determines the sleep period for cyclic sleeping remotes. Maximum sleep period is 268 seconds (0x68B0).

Coordinator - If non-zero, SP determines the time to hold an indirect message before discarding it. A Coordinator will discard indirect messages after a period of (2.5 * SP).

ST (Time before Sleep) Command

<Sleep Mode (Low Power)> The ST command is used to set and read the period of inactivity (no serial or RF data is sent or received) before activating Sleep Mode.

NonBeacon Firmware

Set/Read time period of inactivity (no serial or RF data is sent or received) before activating Sleep Mode. ST parameter is only valid with Cyclic Sleep settings (SM = 4 - 5).

Coordinator and End Device ST values must be equal.

AT Command: ATST	
Parameter Range:	NonBeacon Firmware: 1 – 0xFFFF [x 1 millisecond]
Default Parameter Value:	
Related Commands: SM (Sleep Mode), ST (Time before Sleep)	

T0 - T7 ((D0-D7) Output Timeout) Command

AT Commands: ATT0 – ATT7
Parameter Range:0 – 0xFF [x 100 msec]
Default Parameter Value:0xFF
Minimum Firmware Version Required: v1.xA0

<I/O Settings {I/O Line Passing}> The T0, T1, T2, T3, T4, T5, T6 and T7 commands are used to set/read output timeout values for the lines that correspond with the D0 - D7 parameters. When output is set (due to I/O line passing) to a non-default level, a timer is started which when expired, will set the output to its default level. The timer is reset when a valid I/O packet is received. The Tn parameter defines the permissible amount of time to stay in a non-default (active) state. If Tn = 0, Output Timeout is disabled (output levels are held indefinitely).

VL (Firmware Version - Verbose)

AT Command: ATVL
Parameter Range:0 – 0xFF [x 100 milliseconds]
Default Parameter Value: 0x28 (40 decimal)
Minimum Firmware Version Required: v1.x80 – v1.xC8

<Diagnostics> The VL command is used to read detailed version information about the RF module. The information includes:
application build date; MAC, PHY and bootloader versions; and build dates. This command was removed from firmware 1xC9 and later versions.

VR (Firmware Version) Command

AT Command: ATVR
Parameter Range: 0 – 0xFFFF [read only]

<Diagnostics> The VR command is used to read which firmware version is stored in the module.

XBee version numbers will have four significant digits. The reported number will show three or four numbers and is stated in hexadecimal notation. A version can be reported as "ABC" or "ABCD". Digits ABC are the main release number and D is the revision number from the main release. "D" is not required and if it is not present, a zero is assumed for D. "B" is a variant designator. The following variants exist:

- "0" = Non-Beacon Enabled 802.15.4 Code
- "1" = Beacon Enabled 802.15.4 Code

WR (Write) Command

AT Command: ATWR

<(Special)> The WR command is used to write configurable parameters to the RF module's non-volatile memory. Parameter values remain in the module's memory until overwritten by subsequent use of the WR Command.

If changes are made without writing them to non-volatile memory, the module reverts back to previously saved parameters the next time the module is powered-on.

NOTE: Once the WR command is sent to the module, no additional characters should be sent until after the “OK/r” response is received.

API Operation

By default, XBee®/XBee-PRO® RF Modules act as a serial line replacement (Transparent Operation) - all UART data received through the DI pin is queued up for RF transmission. When the module receives an RF packet, the data is sent out the DO pin with no additional information.

Inherent to Transparent Operation are the following behaviors:

- If module parameter registers are to be set or queried, a special operation is required for transitioning the module into Command Mode.
- In point-to-multipoint systems, the application must send extra information so that the receiving module(s) can distinguish between data coming from different remotes.

As an alternative to the default Transparent Operation, API (Application Programming Interface) Operations are available. API operation requires that communication with the module be done through a structured interface (data is communicated in frames in a defined order). The API specifies how commands, command responses and module status messages are sent and received from the module using a UART Data Frame.

API Frame Specifications

Two API modes are supported and both can be enabled using the AP (API Enable) command. Use the following AP parameter values to configure the module to operate in a particular mode:

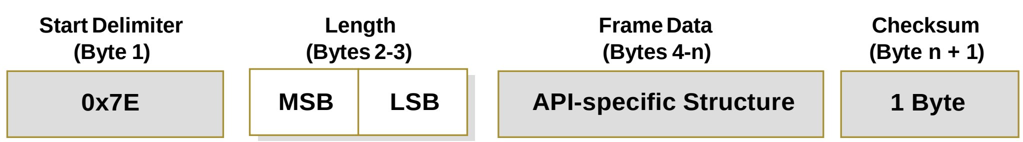
- AP = 0 (default): Transparent Operation (UART Serial line replacement)
  API modes are disabled.
- AP = 1: API Operation
- AP = 2: API Operation (with escaped characters)

Any data received prior to the start delimiter is silently discarded. If the frame is not received correctly or if the checksum fails, the data is silently discarded.

API Operation (AP parameter = 1)

When this API mode is enabled (AP = 1), the UART data frame structure is defined as follows:

Figure 3-01. UART Data Frame Structure:

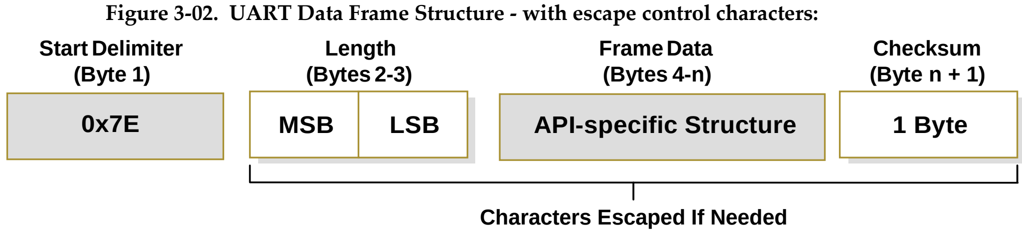


MSB = Most Significant Byte, LSB = Least Significant Byte

API Operation - with Escape Characters (AP parameter = 2)

When this API mode is enabled (AP = 2), the UART data frame structure is defined as follows:

Figure 3-02. UART Data Frame Structure - with escape control characters:



MSB = Most Significant Byte, LSB = Least Significant Byte

Escape characters. When sending or receiving a UART data frame, specific data values must be escaped (flagged) so they do not interfere with the UART or UART data frame operation. To escape an interfering data byte, insert 0x7D and follow it with the byte to be escaped XOR'd with 0x20.

Data bytes that need to be escaped:

- 0x7E – Frame Delimiter
- 0x7D – Escape
- 0x11 – XON
- 0x13 – XOFF

Example - Raw UART Data Frame (before escaping interfering bytes):
0x7E 0x00 0x02 0x23 0x11 0xCB

0x11 needs to be escaped which results in the following frame:
0x7E 0x00 0x02 0x23 0x7D 0x31 0xCB

Note: In the above example, the length of the raw data (excluding the checksum) is 0x0002 and the checksum of the non-escaped data (excluding frame delimiter and length) is calculated as: 0xFF - (0x23 + 0x11) = (0xFF - 0x34) = 0xCB.

Checksum

To test data integrity, a checksum is calculated and verified on non-escaped data.

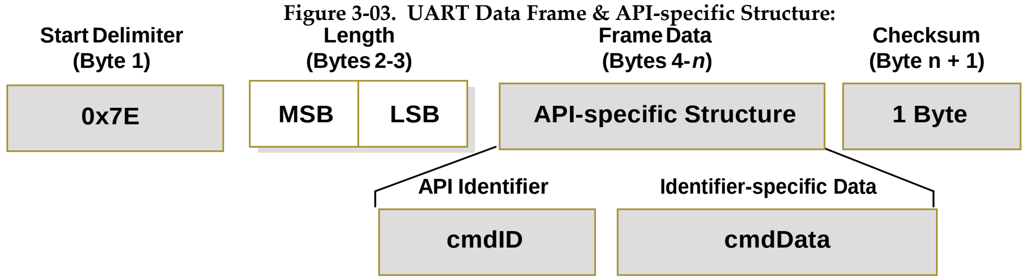
To calculate: Not including frame delimiters and length, add all bytes keeping only the lowest 8 bits of the result and subtract from 0xFF.

To verify: Add all bytes (include checksum, but not the delimiter and length). If the checksum is correct, the sum will equal 0xFF.

API Types

Frame data of the UART data frame forms an API-specific structure as follows:

Figure 3-03. UART Data Frame & API-specific Structure:

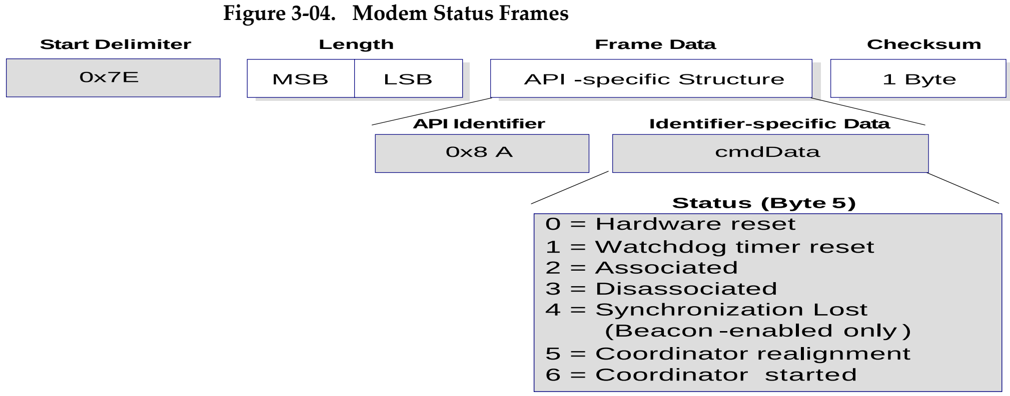


The cmdID frame (API-identifier) indicates which API messages will be contained in the cmdData frame (Identifier-specific data). Refer to the sections that follow for more information regarding the supported API types. Note that multi-byte values are sent big endian.

Modem Status

API Identifier: 0x8A
RF module status messages are sent from the module in response to specific conditions.

Figure 3-04. Modem Status Frames



AT Command

API Identifier Value: 0x08

The "AT Command" API type allows for module parameters to be queried or set. When using this command ID, new parameter values are applied immediately. This includes any register set with the "AT Command - Queue Parameter Value" (0x09) API type.

Figure 3-05. AT Command Frames

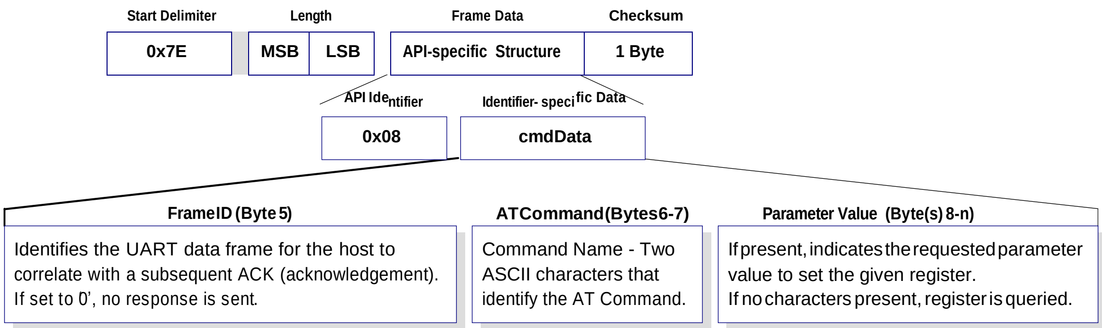


Figure 3-06. Example: API frames when reading the DL parameter value of the module.

Byte 1	Bytes 2-3		Byte 4	Byte 5	Bytes 6-7		Byte 8
0x7E	0x00	0x04	0x08	0x52 (R)	0x44 (D)	0x4C (L)	0x15
Start Delimiter	Length*		API Identifier	Frame ID**	AT Command		Checksum

** Length [Bytes] = API Identifier + Frame ID + AT Command*

*** "R" value was arbitrarily selected.*

Figure 3-07. Example: API frames when modifying the DL parameter value of the module.

Byte 1	Bytes 2-3		Byte 4	Byte 5	Bytes 6-7		Bytes 8-11	Byte 12
0x7E	0x00	0x08	0x08	0x4D (M)	0x44 (D)	0x4C (L)	0x00000FFF	0x0C
Start Delimiter	Length*		API Identifier	Frame ID**	AT Command		Parameter Value	Checksum

** Length [Bytes] = API Identifier + Frame ID + AT Command + Parameter Value*

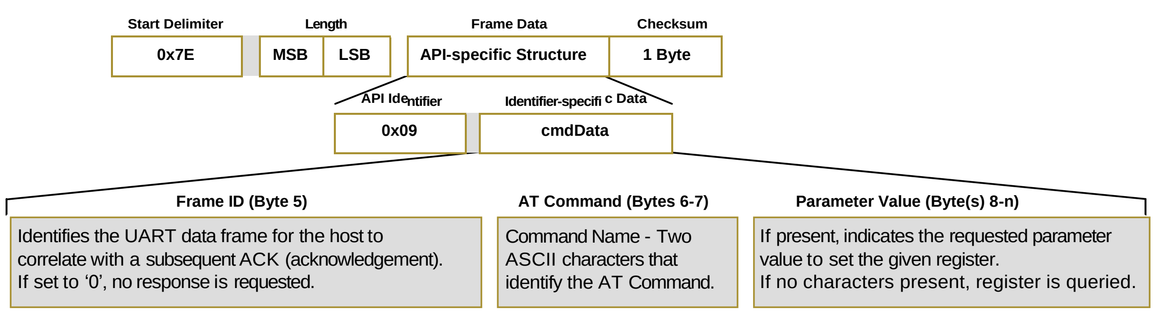
*** "M" value was arbitrarily selected.*

AT Command - Queue Parameter Value

API Identifier Value: 0x09

This API type allows module parameters to be queried or set. In contrast to the "AT Command" API type, new parameter values are queued and not applied until either the "AT Command" (0x08) API type or the AC (Apply Changes) command is issued. Register queries (reading parameter values) are returned immediately.

Figure 3-08. AT Command Frames
(Note that frames are identical to the "AT Command" API type except for the API identifier.)



AT Command Response

API Identifier Value: 0x88

Response to previous command.

In response to an AT Command message, the module will send an AT Command Response message. Some commands will send back multiple frames (for example, the ND (Node Discover) and AS (Active Scan) commands). These commands will end by sending a frame with a status of ATCMD_OK and no cmdData.

Figure 3-09. AT Command Response Frames.

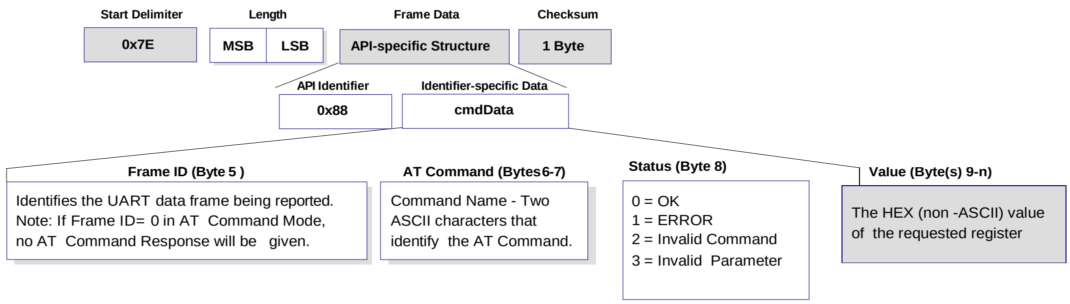
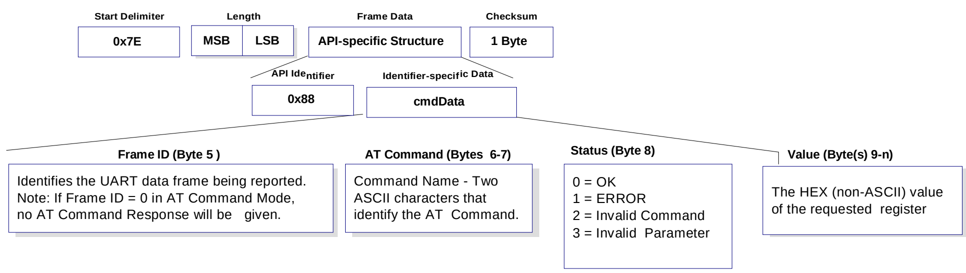


Figure 3-10. AT Command Response Frames.

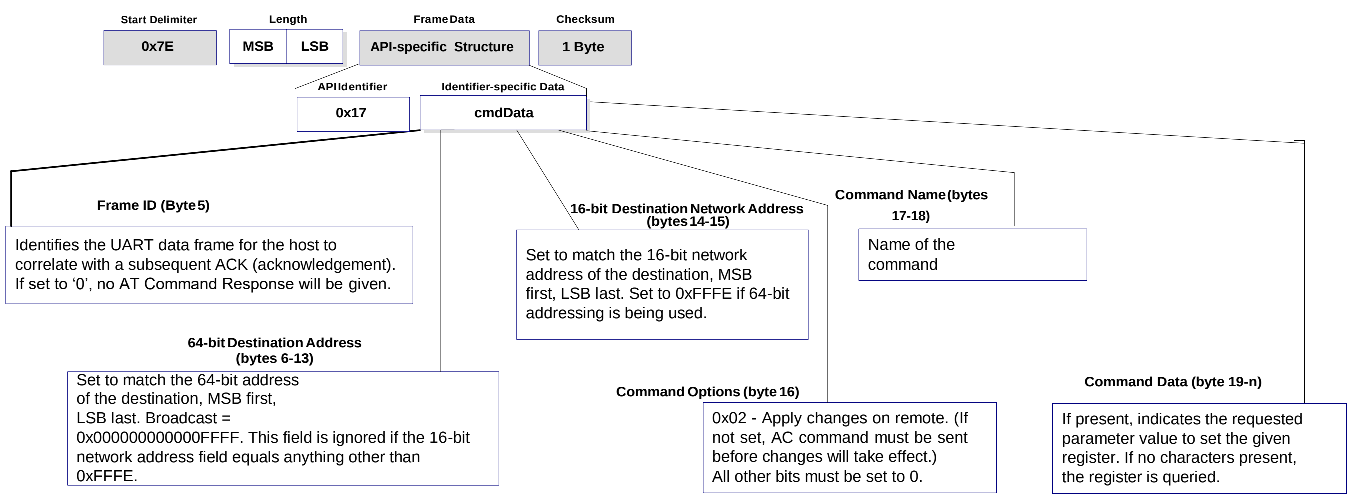


Remote AT Command Request

API Identifier Value: 0x17

Allows for module parameter registers on a remote device to be queried or set

Figure 3-11. Remote AT Command Request

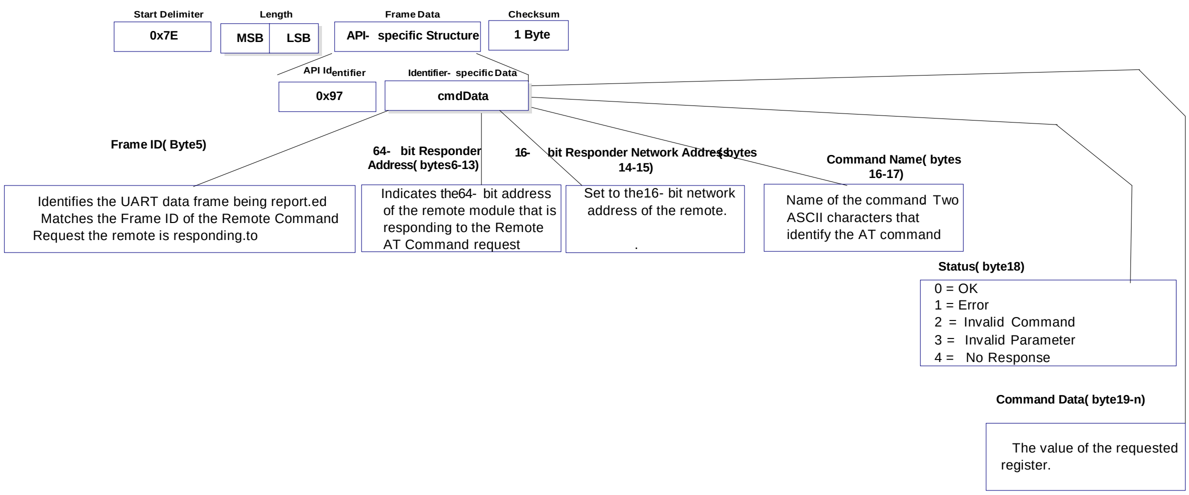


Remote Command Response

API Identifier Value: 0x97

If a module receives a remote command response RF data frame in response to a Remote AT Command Request, the module will send a Remote AT Command Response message out the UART. Some commands may send back multiple frames--for example, Node Discover (ND) command.

Figure 3-12. Remote AT Command Response.

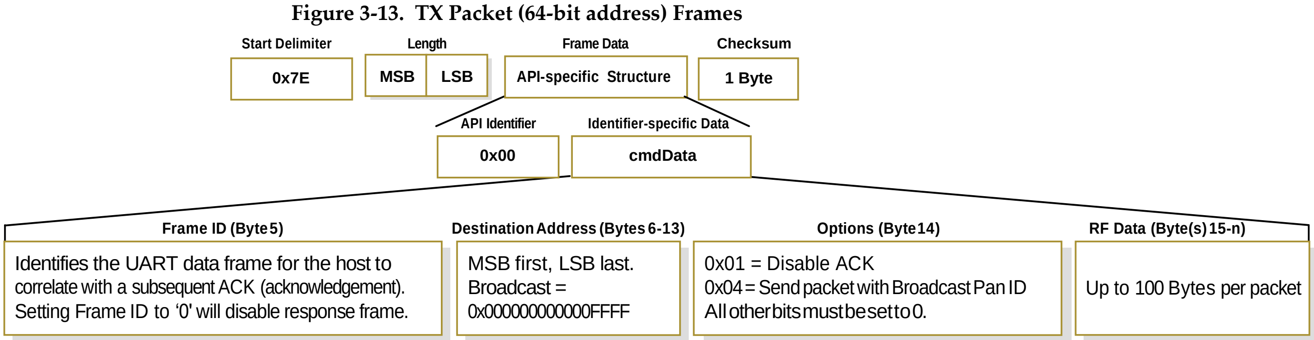


TX (Transmit) Request: 64-bit address

API Identifier Value: 0x00

A TX Request message will cause the module to send RF Data as an RF Packet.

Figure 3-13. TX Packet (64-bit address) Frames

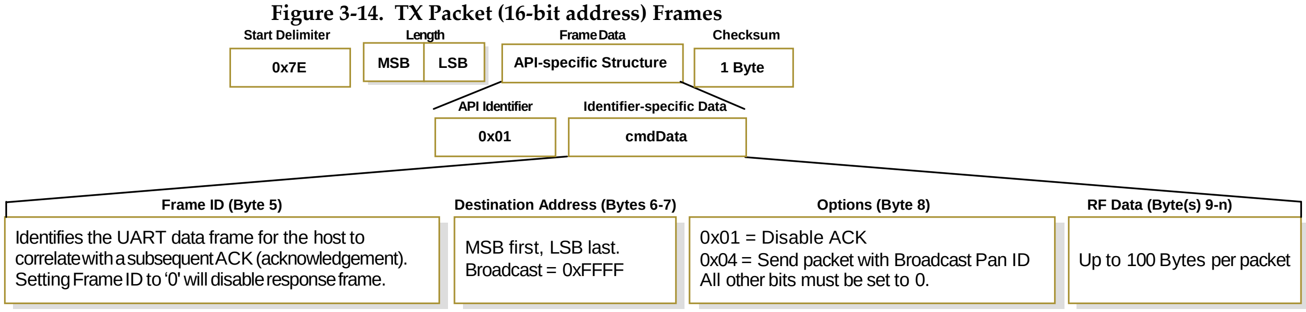


TX (Transmit) Request: 16-bit address

API Identifier Value: 0x01

A TX Request message will cause the module to send RF Data as an RF Packet.

Figure 3-14. TX Packet (16-bit address) Frames

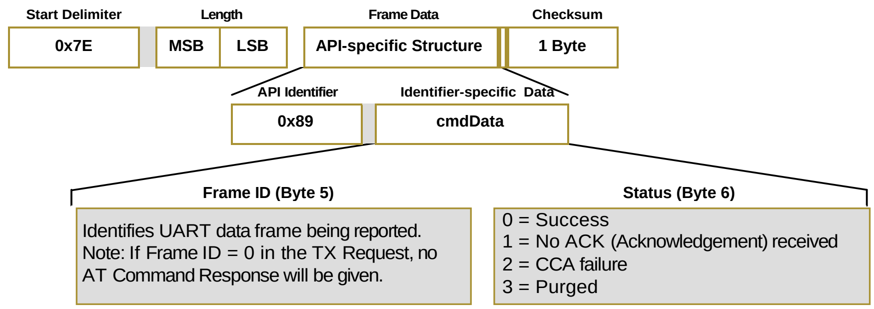


TX (Transmit) Status

API Identifier Value: 0x89

When a TX Request is completed, the module sends a TX Status message. This message will indicate if the packet was transmitted successfully or if there was a failure.

Figure 3-15. TX Status Frames



NOTES:

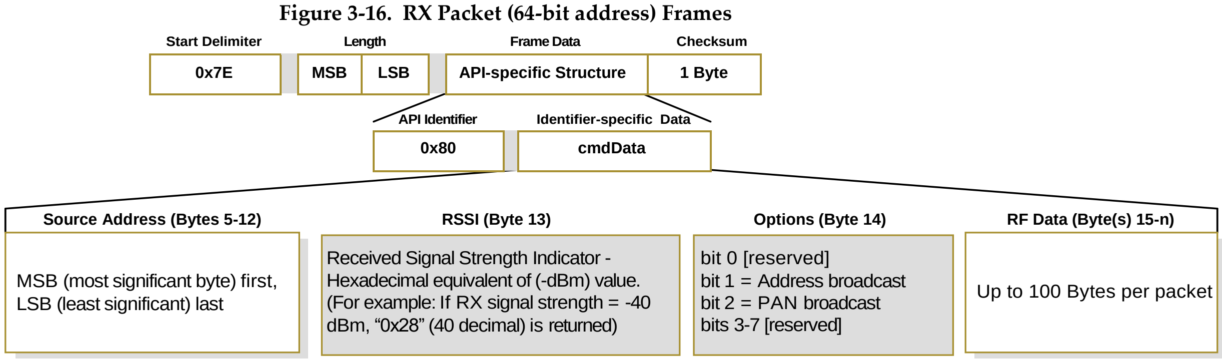
- "STATUS = 1" occurs when all retries are expired and no ACK is received.
- If transmitter broadcasts (destination address = 0x000000000000FFFF), only "STATUS = 0 or 2" will be returned.
- "STATUS = 3" occurs when Coordinator times out of an indirect transmission. Timeout is defined as (2.5 x SP (Cyclic Sleep Period) parameter value).

RX (Receive) Packet: 64-bit Address

API Identifier Value: 0x80

When the module receives an RF packet, it is sent out the UART using this message type.

Figure 3-16. RX Packet (64-bit address) Frames

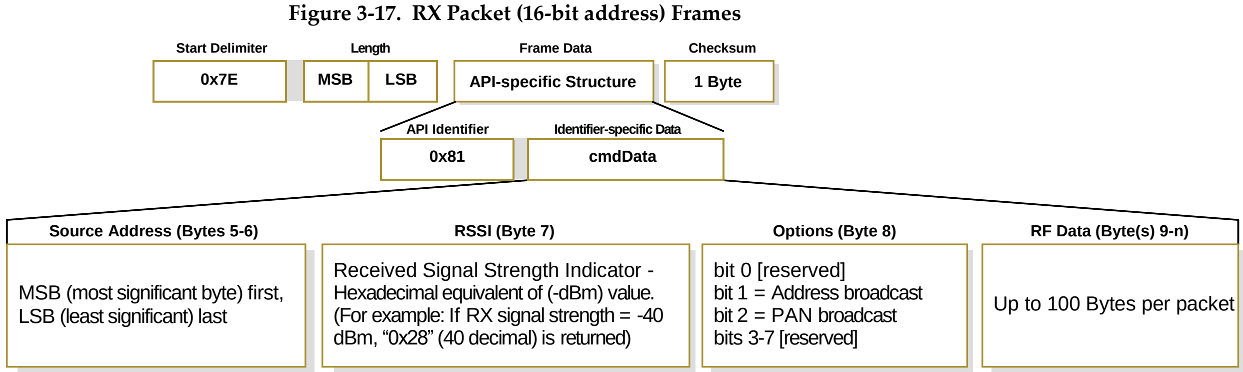


RX (Receive) Packet: 16-bit Address

API Identifier Value: 0x81

When the module receives an RF packet, it is sent out the UART using this message type.

Figure 3-17. RX Packet (16-bit address) Frames



Appendix A: Agency Certifications

United States (FCC)

XBee®/XBee-PRO® RF Modules comply with Part 15 of the FCC rules and regulations. Compliance with the labeling requirements, FCC notices and antenna usage guidelines is required.

To fulfill FCC Certification requirements, the OEM must comply with the following regulations:

1. The system integrator must ensure that the text on the external label provided with this device is placed on the outside of the final product [Figure A-01].
2. XBee®/XBee-PRO® RF Modules may only be used with antennas that have been tested and approved for use with this module [refer to the antenna tables in this section].

OEM Labeling Requirements

WARNING: The Original Equipment Manufacturer (OEM) must ensure that FCC labeling requirements are met. This includes a clearly visible label on the outside of the final product enclosure that displays the contents shown in the figure below.

Figure 4-01. Required FCC Label for OEM products containing the XBee®/XBee-PRO® RF Module

Contains FCC ID: OUR-XBEE/OUR-XBEEPRO**

The enclosed device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (*i.*) this device may not cause harmful interference and (*ii.*) this device must accept any interference received, including interference that may cause undesired operation.

* The FCC ID for the XBee is "OUR-XBEE". The FCC ID for the XBee-PRO is "OUR-XBEEPRO".

FCC Notices

IMPORTANT: The XBee®/XBee-PRO® RF Module has been certified by the FCC for use with other products without any further certification (as per FCC section 2.1091). Modifications not expressly approved by Digi could void the user's authority to operate the equipment.

IMPORTANT: OEMs must test final product to comply with unintentional radiators (FCC section 15.107 & 15.109) before declaring compliance of their final product to Part 15 of the FCC Rules.

IMPORTANT: The RF module has been certified for remote and base radio applications. If the module will be used for portable applications, the device must undergo SAR testing.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Re-orient or relocate the receiving antenna, Increase the separation between the equipment and receiver, Connect equipment and receiver to outlets on different circuits, or Consult the dealer or an experienced radio/TV technician for help.

FCC-Approved Antennas (2.4 GHz)

XBee/XBee-PRO RF Modules can be installed using antennas and cables constructed with standard connectors (Type-N, SMA, TNC, etc.) if the installation is performed professionally and according to FCC guidelines. For installations not performed by a professional, non-standard connectors (RPSMA, RPTNC, etc) must be used.

The modules are FCC-approved for fixed base station and mobile applications on channels 0x0B - 0x1A (XBee) and 0x0C - 0x17 (XBee-PRO). If the antenna is mounted at least 20cm (8 in.) from nearby persons, the application is considered a mobile application. Antennas not listed in the table must be tested to comply with FCC Section 15.203 (Unique Antenna Connectors) and Section 15.247 (Emissions).

XBee RF Modules (1 mW): XBee Modules have been tested and approved for use with all of the antennas listed in the tables below (Cable-loss IS NOT required).

XBee-PRO RF Modules (60 mW): XBee-PRO Modules have been tested and approved for use with the antennas listed in the tables below (Cable-loss IS required when using antennas listed in the second table.

The antennas in the tables below have been approved for use with this module. Digi does not carry all of these antenna variants. Contact Digi Sales for available antennas.

Antennas approved for use with the XBee®/XBee-PRO® RF Modules (Cable-loss is not required.)

Part Number	Type (Description)	Gain	Application*	Min. Separation
A24-HASM-450	Dipole (Half-wave articulated RPSMA - 4.5”)	2.1 dBi	Fixed/Mobile	20 cm
A24-HABSM	Dipole (Articulated RPSMA)	2.1 dBi	Fixed	20 cm
A24-HABUF-P5I	Dipole (Half-wave articulated bulkhead mount U.FL. w/ 5” pigtail)	2.1 dBi	Fixed	20 cm
A24-HASM-525	Dipole (Half-wave articulated RPSMA - 5.25")	2.1 dBi	Fixed/Mobile	20 cm
A24-QI	Monopole (Integrated whip)	1.5 dBi	Fixed	20 cm

Antennas approved for use with the XBee RF Modules (Cable-loss is required)

Part Number	Type (Description)	Gain	Application*	Min. Separation	Required Cable-loss
Omni-Directional Class Antennas					
A24-Y6NF	Yagi (6-element)	8.8 dBi	Fixed	2 m	1.7 dB
A24-Y7NF	Yagi (7-element)	9.0 dBi	Fixed	2 m	1.9 dB
A24-Y9NF	Yagi (9-element)	10.0 dBi	Fixed	2 m	2.9 dB
A24-Y10NF	Yagi (10-element)	11.0 dBi	Fixed	2 m	3.9 dB
A24-Y12NF	Yagi (12-element)	12.0 dBi	Fixed	2 m	4.9 dB
A24-Y13NF	Yagi (13-element)	12.0 dBi	Fixed	2 m	4.9 dB
A24-Y15NF	Yagi (15-element)	12.5 dBi	Fixed	2 m	5.4 dB
A24-Y16NF	Yagi (16-element)	13.5 dBi	Fixed	2 m	6.4 dB
A24-Y16RM	Yagi (16-element, RPSMA connector)	13.5 dBi	Fixed	2 m	6.4 dB
A24-Y18NF	Yagi (18-element)	15.0 dBi	Fixed	2 m	7.9 dB
Omni-Directional Class Antennas					
A24-C1	Surface Mount	-1.5 dBi	Fixed/Mobile	20 cm	-
A24-F2NF	Omni-directional (Fiberglass base station)	2.1 dBi	Fixed/Mobile	20 cm	
A24-F3NF	Omni-directional (Fiberglass base station)	3.0 dBi	Fixed/Mobile	20 cm	
A24-F5NF	Omni-directional (Fiberglass base station)	5.0 dBi	Fixed/Mobile	20 cm	
A24-F8NF	Omni-directional (Fiberglass base station)	8.0 dBi	Fixed	2 m	
A24-F9NF	Omni-directional (Fiberglass base station)	9.5 dBi	Fixed	2 m	0.2 dB
A24-F10NF	Omni-directional (Fiberglass base station)	10.0 dBi	Fixed	2 m	0.7 dB
A24-F12NF	Omni-directional (Fiberglass base station)	12.0 dBi	Fixed	2 m	2.7 dB
A24-F15NF	Omni-directional (Fiberglass base station)	15.0 dBi	Fixed	2 m	5.7 dB
A24-W7NF	Omni-directional (Base station)	7.2 dBi	Fixed	2 m	
A24-M7NF	Omni-directional (Mag-mount base station)	7.2 dBi	Fixed	2 m	
Panel Class Antennas					
A24-P8SF	Flat Panel	8.5 dBi	Fixed	2 m	1.5 dB
A24-P8NF	Flat Panel	8.5 dBi	Fixed	2 m	1.5 dB
A24-P13NF	Flat Panel	13.0 dBi	Fixed	2 m	6 dB
A24-P14NF	Flat Panel	14.0 dBi	Fixed	2 m	7 dB
A24-P15NF	Flat Panel	15.0 dBi	Fixed	2 m	8 dB
A24-P16NF	Flat Panel	16.0 dBi	Fixed	2 m	9 dB

Antennas approved for use with the XBee®/XBee-PRO® RF Modules (Cable-loss is required)

Part Number	Type (Description)	Gain	Application*	Min. Separation	Required Cable-loss
A24-C1	Surface Mount	-1.5 dBi	Fixed/Mobile	20 cm	-
A24-Y4NF	Yagi (4-element)	6.0 dBi	Fixed	2 m	8.1 dB
A24-Y6NF	Yagi (6-element)	8.8 dBi	Fixed	2 m	10.9 dB
A24-Y7NF	Yagi (7-element)	9.0 dBi	Fixed	2 m	11.1 dB
A24-Y9NF	Yagi (9-element)	10.0 dBi	Fixed	2 m	12.1 dB
A24-Y10NF	Yagi (10-element)	11.0 dBi	Fixed	2 m	13.1 dB
A24-Y12NF	Yagi (12-element)	12.0 dBi	Fixed	2 m	14.1 dB
A24-Y13NF	Yagi (13-element)	12.0 dBi	Fixed	2 m	14.1 dB
A24-Y15NF	Yagi (15-element)	12.5 dBi	Fixed	2 m	14.6 dB
A24-Y16NF	Yagi (16-element)	13.5 dBi	Fixed	2 m	15.6 dB
A24-Y16RM	Yagi (16-element, RPSMA connector)	13.5 dBi	Fixed	2 m	15.6 dB
A24-Y18NF	Yagi (18-element)	15.0 dBi	Fixed	2 m	17.1 dB
A24-F2NF	Omni-directional (Fiberglass base station)	2.1 dBi	Fixed/Mobile	20 cm	4.2 dB
A24-F3NF	Omni-directional (Fiberglass base station)	3.0 dBi	Fixed/Mobile	20 cm	5.1 dB
A24-F5NF	Omni-directional (Fiberglass base station)	5.0 dBi	Fixed/Mobile	20 cm	7.1 dB
A24-F8NF	Omni-directional (Fiberglass base station)	8.0 dBi	Fixed	2 m	10.1 dB
A24-F9NF	Omni-directional (Fiberglass base station)	9.5 dBi	Fixed	2 m	11.6 dB
A24-F10NF	Omni-directional (Fiberglass base station)	10.0 dBi	Fixed	2 m	12.1 dB
A24-F12NF	Omni-directional (Fiberglass base station)	12.0 dBi	Fixed	2 m	14.1 dB
A24-F15NF	Omni-directional (Fiberglass base station)	15.0 dBi	Fixed	2 m	17.1 dB
A24-W7NF	Omni-directional (Base station)	7.2 dBi	Fixed	2 m	9.3 dB
A24-M7NF	Omni-directional (Mag-mount base station)	7.2 dBi	Fixed	2 m	9.3 dB
A24-P8SF	Flat Panel	8.5 dBi	Fixed	2 m	8.6 dB
A24-P8NF	Flat Panel	8.5 dBi	Fixed	2 m	8.6 dB
A24-P13NF	Flat Panel	13.0 dBi	Fixed	2 m	13.1 dB
A24-P14NF	Flat Panel	14.0 dBi	Fixed	2 m	14.1 dB
A24-P15NF	Flat Panel	15.0 dBi	Fixed	2 m	15.1 dB
A24-P16NF	Flat Panel	16.0 dBi	Fixed	2 m	16.1 dB
A24-P19NF	Flat Panel	19.0 dBi	Fixed	2 m	19.1 dB

*** If using the RF module in a portable application** (For example - If the module is used in a handheld device and the antenna is less than 20cm from the human body when the device is operation): The integrator is responsible for passing additional SAR (Specific Absorption Rate) testing based on FCC rules 2.1091 and FCC Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields, OET Bulletin and Supplement C. The testing results will be submitted to the FCC for approval prior to selling the integrated unit. The required SAR testing measures emissions from the module and how they affect the person.

RF Exposure

WARNING: To satisfy FCC RF exposure requirements for mobile transmitting devices, a separation distance of 20 cm or more should be maintained between the antenna of this device and persons during device operation. To ensure compliance, operations at closer than this distance is not recommended. The antenna used for this transmitter must not be co-located in conjunction with any other antenna or transmitter.

The preceding statement must be included as a CAUTION statement in OEM product manuals in order to alert users of FCC RF Exposure compliance.

Europe (ETSI)

The XBee RF Modules have been certified for use in several European countries. For a complete list, refer to www.digi.com

If the XBee RF Modules are incorporated into a product, the manufacturer must ensure compliance of the final product to the European harmonized EMC and low-voltage/safety standards. A Declaration of Conformity must be issued for each of these standards and kept on file as described in Annex II of the R&TTE Directive.

Furthermore, the manufacturer must maintain a copy of the XBee user manual documentation and ensure the final product does not exceed the specified power ratings, antenna specifications, and/or installation requirements as specified in the user manual. If any of these specifications are exceeded in the final product, a submission must be made to a notified body for compliance testing to all required standards.

OEM Labeling Requirements

The 'CE' marking must be affixed to a visible location on the OEM product.

CE Labeling Requirements

The CE mark shall consist of the initials "CE" taking the following form:

- If the CE marking is reduced or enlarged, the proportions given in the above graduated drawing must be respected.
- The CE marking must have a height of at least 5mm except where this is not possible on account of the nature of the apparatus.
- The CE marking must be affixed visibly, legibly, and indelibly.

Restrictions

Power Output: When operating in Europe, XBee-PRO 802.15.4 modules must operate at or below a transmit power output level of 10dBm. Customers have two choices for transmitting at or below 10dBm:

a. Order the standard XBee-PRO module and change the PL command to 0 (10dBm)

b. Order the International variant of the XBee-PRO module, which has a maximum transmit output power of 10dBm (@ PL=4).

Additionally, European regulations stipulate an EIRP power maximum of 12.86 dBm (19 mW) for the XBee-PRO and 12.11 dBm for the XBee when integrating antennas.

France: Outdoor use limited to 10 mW EIRP within the band 2454-2483.5 MHz.

Norway: Norway prohibits operation near Ny-Alesund in Svalbard. More information can be found at the Norway Posts and Telecommunications site (www.npt.no).

Declarations of Conformity

Digi has issued Declarations of Conformity for the XBee RF Modules concerning emissions, EMC and safety. Files can be obtained by contacting Digi Support.

Important Note:

Digi does not list the entire set of standards that must be met for each country. Digi customers assume full responsibility for learning and meeting the required guidelines for each country in their distribution market. For more information relating to European compliance of an OEM product incorporating the XBee RF Module, contact Digi, or refer to the following web sites:

CEPT ERC 70-03E - Technical Requirements, European restrictions and general requirements: Available at www.ero.dk/.

R&TTE Directive - Equipment requirements, placement on market: Available at www.ero.dk/.

Approved Antennas

When integrating high-gain antennas, European regulations stipulate EIRP power maximums. Use the following guidelines to determine which antennas to design into an application.

XBee-PRO RF Module

The following antenna types have been tested and approved for use with the XBee Module:

Antenna Type: Yagi
RF module was tested and approved with 15 dBi antenna gain with 1 dB cable-loss (EIRP Maximum of 14 dBm). Any Yagi type antenna with 14 dBi gain or less can be used with no cable-loss.

Antenna Type: Omni-directional
RF module was tested and approved with 15 dBi antenna gain with 1 dB cable-loss (EIRP Maxi-

mum of 14 dBm). Any Omni-directional type antenna with 14 dBi gain or less can be used with no cable-loss.

Antenna Type: Flat Panel
RF module was tested and approved with 19 dBi antenna gain with 4.8 dB cable-loss (EIRP Maximum of 14.2 dBm). Any Flat Panel type antenna with 14.2 dBi gain or less can be used with no cable-loss.

XBee-PRO RF Module (@ 10 dBm Transmit Power, PL parameter value must equal 0, or use International variant)

The following antennas have been tested and approved for use with the embedded XBee-PRO RF Module:

- Dipole (2.1 dBi, Omni-directional, Articulated RPSMA, Digi part number A24-HABSM)
- Chip Antenna (-1.5 dBi)
- Attached Monopole Whip (1.5 dBi)

The RF modem encasement was designed to accommodate the RPSMA antenna option.

Canada (IC)

Labeling Requirements

Labeling requirements for Industry Canada are similar to those of the FCC. A clearly visible label on the outside of the final product enclosure must display the following text:

Contains Model XBee Radio, IC: 4214A-XBEE
Contains Model XBee-PRO Radio, IC: 4214A-XBEEPRO

The integrator is responsible for its product to comply with IC ICES-003 & FCC Part 15, Sub. B - Unintentional Radiators. ICES-003 is the same as FCC Part 15 Sub. B and Industry Canada accepts FCC test report or CISPR 22 test report for compliance with ICES-003.

Japan

In order to gain approval for use in Japan, the XBee RF module or the International variant of the XBee-PRO RF module (which has 10 dBm transmit output power) must be used.

Labeling Requirements

A clearly visible label on the outside of the final product enclosure must display the following text:

ID: 005NYCA0378

Appendix B. Additional Information

1-Year Warranty

XBee®/XBee-PRO® RF Modules from Digi Intenational, Inc. (the "Product") are warranted against defects in materials and workmanship under normal use, for a period of 1-year from the date of purchase. In the event of a product failure due to materials or workmanship, Digi will repair or replace the defective product. For warranty service, return the defective product to Digi, shipping prepaid, for prompt repair or replacement.

The foregoing sets forth the full extent of Digi's warranties regarding the Product. Repair or replacement at Digi's option is the exclusive remedy. THIS WARRANTY IS GIVEN IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, AND DIGI SPECIFICALLY DISCLAIMS ALL WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL DIGI, ITS SUPPLIERS OR LICENSORS BE LIABLE FOR DAMAGES IN EXCESS OF THE PURCHASE PRICE OF THE PRODUCT, FOR ANY LOSS OF USE, LOSS OF TIME, INCONVENIENCE, COMMERCIAL LOSS, LOST PROFITS OR SAVINGS, OR OTHER INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, TO THE FULL EXTENT SUCH MAY BE DISCLAIMED BY LAW. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES. THEREFORE, THE FOREGOING EXCLUSIONS MAY NOT APPLY IN ALL CASES. This warranty provides specific legal rights. Other rights which vary from state to state may also apply.