Digi XBee® BLU

User Guide

User Guide

Revision history–90002567

Revision	Date	Description
A	May 2024	Initial release.

Trademarks and copyright

Digi, Digi International, and the Digi logo are trademarks or registered trademarks in the United States and other countries worldwide. All other trademarks mentioned in this document are the property of their respective owners.

© 2023 Digi International Inc. All rights reserved.

Disclaimers

Information in this document is subject to change without notice and does not represent a commitment on the part of Digi International. Digi provides this document “as is,” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose. Digi may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time.

Warranty

To view product warranty information, go to the following website:

www.digi.com/howtobuy/terms

Customer support

Gather support information: Before contacting Digi technical support for help, gather the following information:

- Product name and model
- Product serial number (s)
- Firmware version
- Operating system/browser (if applicable)
- Logs (from time of reported issue)
- Trace (if possible)
- Description of issue
- Steps to reproduce

Contact Digi technical support: Digi offers multiple technical support plans and service packages. Contact us at +1 952.912.3444 or visit us at www.digi.com/support.

Feedback

To provide feedback on this document, email your comments to

techcomm@digi.com

Include the document title and part number (Digi XBee® BLU User Guide, 90002567 A) in the subject line of your email.

Contents

Digi XBee® BLU User Guide

Safety instructions

Configure the XBee® BLU

Get started with BLE

BLE reference

File system

Get started with MicroPython

Serial communication

SPI operation

Modes

I/O support

Sleep support

General Purpose Flash Memory

AT commands

Operate in API mode

Frame descriptions

Digi XBee® BLU User Guide

This manual describes the operation of the XBee® BLU.

Applicable firmware and hardware

This user guide supports the following firmware:

- v. 40xx XBee BLU

It supports the following hardware:

- XBee BLU

Safety instructions

Safety instructions

XBee modules

- The XBee radio module cannot be guaranteed operation due to the radio link and so should not be used for interlocks in safety critical devices such as machines or automotive applications.
- The XBee radio module has not been approved for use in (this list is not exhaustive):
  - medical devices
  - nuclear applications
  - explosive or flammable atmospheres
- There are no user serviceable components inside the XBee radio module. Do not remove the shield or modify the XBee in any way. Modifications may exclude the module from any warranty and can cause the XBee radio to operate outside of regulatory compliance for a given country, leading to the possible illegal operation of the radio.
- Use industry standard ESD protection when handling the XBee module.
- Take care while handling to avoid electrical damage to the PCB and components.
- Do not expose XBee radio modules to water or moisture.
- Use this product with the antennas specified in the XBee module user guides.
- The end user must be told how to remove power from the XBee radio module or to locate the antennas 20 cm from humans or animals.

Инструкции за безопасност

XBee модули

- Радио модулът XBee не може да бъде гарантиран за работа поради радиовръзката и затова не трябва да се използва за блокировки в критични за безопасността устройства като машини или автомобилни приложения.
- Радио модулът XBee не е одобрен за използване в (този списък не е изчерпателен):
  - медицински изделия
  - ядрени приложения
  - експлозивна или запалима атмосфера
- В радиомодула XBee няма компоненти, които могат да се обслужват от потребителя. Не премахвайте щита и не модифицирайте XBee по никакъв начин. Модификациите могат да изключат модула от всякаква гаранция и да накарат радиото XBee да работи извън регулаторното съответствие за дадена държава, което води до възможна незаконна работа на радиото.
- Използвайте стандартна ESD защита при работа с XBee модула.
- Внимавайте, докато боравите, за да избегнете електрически повреди на печатната платка и компонентите.
- Не излагайте радиомодулите XBee на вода или влага.

- Използвайте този продукт с антените, посочени в ръководствата за потребителя на модула XBee.
- Крайният потребител трябва да бъде казано как да премахне захранването от радиомодула XBee или да разположи антените на 20 см от хора или животни.

Sigurnosne upute

XBee moduli

- Radio modulu XBee ne može se jamčiti rad zbog radio veze i stoga se ne smije koristiti za blokade u sigurnosnim kritičnim uređajima kao što su strojevi ili automobilske aplikacije.
- XBee radio modul nije odobren za upotrebu u (ovaj popis nije konačan):
  - medicinskih uređaja
  - nuklearne primjene
  - eksplozivne ili zapaljive atmosfere
- Unutar XBee radio modula nema komponenti koje može servisirati korisnik. Nemojte uklanjati štit i ni na koji način modificirati XBee. Izmjene mogu isključiti modul iz bilo kakvog jamstva i mogu uzrokovati rad XBee radija izvan usklađenosti s propisima za određenu zemlju, što može dovesti do mogućeg nezakonitog rada radija.
- Koristite standardnu ESD zaštitu pri rukovanju XBee modulom.
- Budite oprezni tijekom rukovanja kako biste izbjegli električna oštećenja PCB-a i komponenti.
- Ne izlažite XBee radio module vodi ili vlazi.
- Koristite ovaj proizvod s antenama navedenim u korisničkim vodičima za XBee modul.
- Krajnjem korisniku se mora reći kako da isključi napajanje iz XBee radio modula ili da locira antene 20 cm od ljudi ili životinja.

Bezpečnostní instrukce

moduly XBee

- Rádiový modul XBee nemůže zaručit provoz kvůli rádiovému spojení, a proto by neměl být používán pro blokování v zařízeních kritických z hlediska bezpečnosti, jako jsou stroje nebo automobilové aplikace.
- Rádiový modul XBee nebyl schválen pro použití v (tento seznam není vyčerpávající):
  - zdravotnické prostředky
  - jaderné aplikace
  - výbušné nebo hořlavé atmosféry
- Uvnitř rádiového modulu XBee nejsou žádné uživatelsky opravitelné součásti. Neodstraňujte štít ani nijak neupravujte XBee. Úpravy mohou vyjmout modul z jakékoli záruky a mohou způsobit, že rádio XBee bude fungovat mimo zákonnou shodu pro danou zemi, což povede k možnému nezákonnému provozu rádia.

- Při manipulaci s modulem XBee používejte standardní ochranu ESD.
- Při manipulaci buďte opatrní, aby nedošlo k elektrickému poškození desky plošných spojů a součástí.
- Nevystavujte rádiové moduly XBee vodě nebo vlhkosti.
- Používejte tento produkt s anténami uvedenými v uživatelských příručkách modulu XBee.
- Koncový uživatel musí být informován, jak odpojit napájení rádiového modulu XBee nebo jak umístit antény 20 cm od lidí nebo zvířat.

Sikkerhedsinstruktioner

XBee moduler

- XBee-radiomodulet kan ikke garanteres drift på grund af radioforbindelsen og bør derfor ikke bruges til aflåsninger i sikkerhedskritiske enheder såsom maskiner eller bilapplikationer.
- XBee-radiomodulet er ikke godkendt til brug i (denne liste er ikke udtømmende):
  - medicinsk udstyr
  - nukleare applikationer
  - eksplosive eller brandfarlige atmosfærer
- Der er ingen komponenter, der kan repareres af brugeren, inde i XBee-radiomodulet. Fjern ikke skjoldet eller modificer XBee på nogen måde. Ændringer kan udelukke modulet fra enhver garanti og kan få XBee-radioen til at fungere uden for lovgivningsoverholdelse for et givet land, hvilket kan føre til den mulige ulovlige drift af radioen.
- Brug industristandard ESD-beskyttelse, når du håndterer XBee-modulet.
- Vær forsigtig under håndteringen for at undgå elektrisk beskadigelse af printet og komponenterne.
- Udsæt ikke XBee-radiomoduler for vand eller fugt.
- Brug dette produkt med de antenner, der er specificeret i XBee-modulets brugervejledninger.
- Slutbrugeren skal fortælles, hvordan man fjerner strømmen fra XBee-radiomodulet eller placerer antennerne 20 cm fra mennesker eller dyr.

Veiligheidsinstructies

XBee-modules

- De werking van de XBee-radiomodule kan niet worden gegarandeerd vanwege de radioverbinding en mag daarom niet worden gebruikt voor vergrendelingen in veiligheidskritieke apparaten zoals machines of autotoepassingen.
- De XBee-radiomodule is niet goedgekeurd voor gebruik in (deze lijst is niet uitputtend):

  - o medische apparaten
  - o nucleaire toepassingen
  - o explosieve of ontvlambare atmosferen
- Er zijn geen door de gebruiker te onderhouden componenten in de XBee-radiomodule. Verwijder het schild niet en wijzig de XBee op geen enkele manier. Modificaties kunnen de module uitsluiten van enige garantie en kunnen ertoe leiden dat de XBee-radio werkt buiten de regelgeving voor een bepaald land, wat kan leiden tot de mogelijke illegale werking van de radio.
- Gebruik industriestandaard ESD-bescherming bij het hanteren van de XBee-module.
- Wees voorzichtig bij het hanteren om elektrische schade aan de printplaat en componenten te voorkomen.
- Stel XBee-radiomodules niet bloot aan water of vocht.
- Gebruik dit product met de antennes die zijn gespecificeerd in de gebruikershandleidingen van de XBee-module.
- De eindgebruiker moet worden verteld hoe de voeding van de XBee-radiomodule moet worden losgekoppeld of hoe de antennes op 20 cm van mensen of dieren moeten worden geplaatst.

Ohutusjuhised

XBee moodulid

- XBee raadiomooduli tööd ei saa raadiolingi tõttu garanteerida ja seetõttu ei tohiks seda kasutada ohutuse seisukohalt oluliste seadmete (nt masinad või autorakendused) blokeerimiseks.
- XBee raadiomoodulit ei ole heaks kiidetud kasutamiseks (see loetelu ei ole ammendav):
  - meditsiiniseadmed
  - tuumarakendused
  - plahvatusohtlik või tuleohtlik keskkond
- XBee raadiomoodulis ei ole kasutaja poolt hooldatavaid komponente. Ärge eemaldage kaitset ega muutke XBee mingil viisil. Muudatused võivad mooduli garantiist välja jätta ja XBee raadio töötab väljaspool antud riigi regulatiivseid vastavusi, põhjustades raadio võimaliku ebaseadusliku kasutamise.
- Kasutage XBee mooduli käsitsemisel tööstusharu standardset ESD-kaitset.
- Olge käsitsemisel ettevaatlik, et vältida PCB ja komponentide elektrikahjustusi.
- Ärge jätke XBee raadiomooduleid vee või niiskuse kätte.
- Kasutage seda toodet XBee mooduli kasutusjuhendis kirjeldatud antennidega.
- Lõppkasutajale tuleb öelda, kuidas XBee raadiomoodulilt toide eemaldada või antennid inimestest või loomadest 20 cm kaugusele paigutada.

Turvallisuusohjeet

XBee moduulit

- XBee-radiomoduulin toimintaa ei voida taata radiolinkin vuoksi, joten sitä ei tule käyttää turvallisuuden kannalta kriittisten laitteiden, kuten koneiden tai autosovellusten, lukitsemiseen.
- XBee-radiomoduulia ei ole hyväksytty käytettäväksi (tämä luettelo ei ole tyhjentävä):
  - lääketieteelliset laitteet
  - ydinvoimasovellukset
  - räjähdysvaarallisiin tai syttyviin tiloihin
- XBee-radiomoduulin sisällä ei ole käyttäjän huollettavia osia. Älä poista suojusta tai muokkaa XBeetä millään tavalla. Muutokset voivat sulkea moduulin takuun ulkopuolelle ja aiheuttaa sen, että XBee-radio toimii tietyn maan säädöstenmukaisuuden ulkopuolella, mikä johtaa radion mahdolliseen laittomaan käyttöön.
- Käytä alan standardia ESD-suojausta käsitellessäsi XBee-moduulia.
- Ole varovainen käsitellessäsi, jotta vältät piirilevyn ja komponenttien sähkövauriot.
- Älä altista XBee-radiomoduuleja vedelle tai kosteudelle.
- Käytä tätä tuotetta XBee-moduulin käyttöoppaissa määriteltyjen antennien kanssa.
- Loppukäyttäjälle on kerrottava, kuinka XBee-radiomoduulin virta katkaistaan tai antennit sijoitetaan 20 cm:n etäisyydelle ihmisistä tai eläimistä.

Consignes de sécurité

Modules XBee

- Le fonctionnement du module radio XBee ne peut pas être garanti en raison de la liaison radio et ne doit donc pas être utilisé pour les verrouillages dans des dispositifs critiques pour la sécurité tels que des machines ou des applications automobiles.
- Le module radio XBee n'a pas été approuvé pour une utilisation dans (cette liste n'est pas exhaustive) :
  - dispositifs médicaux
  - applications nucléaires
  - atmosphères explosives ou inflammables
- Il n'y a aucun composant réparable par l'utilisateur à l'intérieur du module radio XBee. Ne retirez pas la protection et ne modifiez en aucune façon le XBee. Les modifications peuvent exclure le module de toute garantie et peuvent entraîner le fonctionnement de la radio XBee en dehors de la conformité réglementaire pour un pays donné, ce qui peut entraîner un fonctionnement illégal de la radio.
- Utilisez la protection ESD standard de l'industrie lors de la manipulation du module XBee.
- Soyez prudent lors de la manipulation afin d'éviter des dommages électriques au circuit imprimé et aux composants.

- N'exposez pas les modules radio XBee à l'eau ou à l'humidité.
- Utilisez ce produit avec les antennes spécifiées dans les guides d'utilisation du module XBee.
- L'utilisateur final doit savoir comment couper l'alimentation du module radio XBee ou placer les antennes à 20 cm des humains ou des animaux.

Sicherheitshinweise

XBee-Module

- Der Betrieb des XBee-Funkmoduls kann aufgrund der Funkverbindung nicht garantiert werden und sollte daher nicht für Verriegelungen in sicherheitskritischen Geräten wie Maschinen oder Automobilanwendungen verwendet werden.
- Das XBee-Funkmodul ist nicht zugelassen für den Einsatz in (diese Liste ist nicht vollständig):
  - Medizinprodukte
  - nukleare Anwendungen
  - explosive oder brennbare Atmosphären
- Das XBee-Funkmodul enthält keine vom Benutzer zu wartenden Komponenten. Entfernen Sie nicht die Abschirmung oder modifizieren Sie das XBee in irgendeiner Weise. Modifikationen können das Modul von jeglicher Garantie ausschließen und dazu führen, dass das XBee-Funkgerät außerhalb der gesetzlichen Vorschriften für ein bestimmtes Land betrieben wird, was zu einem möglichen illegalen Betrieb des Funkgeräts führen kann.
- Verwenden Sie beim Umgang mit dem XBee-Modul ESD-Schutz nach Industriestandard.
- Seien Sie vorsichtig bei der Handhabung, um elektrische Schäden an der Leiterplatte und den Komponenten zu vermeiden.
- XBee-Funkmodule nicht Wasser oder Feuchtigkeit aussetzen.
- Verwenden Sie dieses Produkt mit den in den Benutzerhandbüchern des XBee-Moduls angegebenen Antennen.
- Dem Endbenutzer muss mitgeteilt werden, wie er das XBee-Funkmodul von der Stromversorgung trennt oder die Antennen 20 cm von Menschen oder Tieren entfernt aufstellt.

Οδηγίες ασφαλείας

Μονάδες XBee

- Η μονάδα ραδιοφώνου XBee δεν μπορεί να εγγυηθεί τη λειτουργία της λόγω της ραδιοζεύξης και επομένως δεν πρέπει να χρησιμοποιείται για ασφάλειες σε κρίσιμες για την ασφάλεια συσκευές, όπως μηχανήματα ή εφαρμογές αυτοκινήτου.
- Η μονάδα ραδιοφώνου XBee δεν έχει εγκριθεί για χρήση σε (αυτή η λίστα δεν είναι εξαντλητική):

  - ιατροτεχνολογικά προϊόντα
  - πυρηνικές εφαρμογές
  - εκρηκτικές ή εύφλεκτες ατμόσφαιρες
- Δεν υπάρχουν εξαρτήματα που να μπορούν να επισκευαστούν από το χρήστη μέσα στη μονάδα ραδιοφώνου XBee. Μην αφαιρείτε την ασπίδα και μην τροποποιείτε το XBee με κανέναν τρόπο. Οι τροποποιήσεις ενδέχεται να αποκλείουν τη μονάδα από οποιαδήποτε εγγύηση και μπορεί να προκαλέσουν τη λειτουργία του ραδιοφώνου XBee εκτός της συμμόρφωσης με τους κανονισμούς για μια δεδομένη χώρα, οδηγώντας σε πιθανή παράνομη λειτουργία του ραδιοφώνου.
- Χρησιμοποιήστε βιομηχανική προστασία ESD κατά το χειρισμό της μονάδας XBee.
- Προσέχετε κατά το χειρισμό για να αποφύγετε ηλεκτρική βλάβη στο PCB και στα εξαρτήματα.
- Μην εκθέτετε τις μονάδες ραδιοφώνου XBee σε νερό ή υγρασία.
- Χρησιμοποιήστε αυτό το προϊόν με τις κεραίες που καθορίζονται στους οδηγούς χρήσης της μονάδας XBee.
- Πρέπει να ενημερωθεί ο τελικός χρήστης πώς να αφαιρέσει την τροφοδοσία από τη μονάδα ραδιοφώνου XBee ή να εντοπίσει τις κεραίες σε απόσταση 20 cm από ανθρώπους ή ζώα.

Biztonsági utasítások

XBee modulok

- Az XBee rádiómodul működése nem garantálható a rádiókapcsolat miatt, ezért nem használható biztonsági szempontból kritikus eszközök, például gépek vagy autóipari alkalmazások reteszelésére.
- Az XBee rádiómodul nem engedélyezett a következő területeken való használatra (ez a lista nem teljes):
  - orvosi eszközök
  - nukleáris alkalmazások
  - robbanásveszélyes vagy gyúlékony légkör
- Az XBee rádiómodulban nincsenek felhasználó által javítható alkatrészek. Ne távolítsa el a pajzsot, és semmilyen módon ne módosítsa az XBee-t. A módosítások kizárhatják a modult a jótállásból, és az XBee rádió működését az adott ország jogszabályi előírásaitól eltérően okozhatják, ami a rádió esetleges illegális működéséhez vezethet.
- Az XBee modul kezelésekor használjon ipari szabványos ESD védelmet.
- A kezelés során ügyeljen arra, hogy elkerülje a PCB és az alkatrészek elektromos károsodását.
- Ne tegye ki az XBee rádiómodulokat víznek vagy nedvességnek.
- Használja ezt a terméket az XBee modul használati útmutatójában meghatározott antennákkal.

- A végfelhasználót tájékoztatni kell arról, hogyan távolítsa el az XBee rádiómodul áramellátását, vagy hogyan helyezze el az antennákat az emberektől vagy állatoktól 20 cm-re.

Istruzioni di sicurezza

Moduli XBee

- Il funzionamento del modulo radio XBee non può essere garantito a causa del collegamento radio e quindi non deve essere utilizzato per gli interblocchi in dispositivi critici per la sicurezza come macchine o applicazioni automobilistiche.
- Il modulo radio XBee non è stato approvato per l'uso in (questo elenco non è esaustivo):
  - dispositivi medici
  - applicazioni nucleari
  - atmosfere esplosive o infiammabili
- Non ci sono componenti riparabili dall'utente all'interno del modulo radio XBee. Non rimuovere lo scudo o modificare in alcun modo l'XBee. Le modifiche possono escludere il modulo da qualsiasi garanzia e possono causare il funzionamento della radio XBee al di fuori della conformità normativa per un determinato paese, portando al possibile funzionamento illegale della radio.
- Utilizzare la protezione ESD standard del settore durante la manipolazione del modulo XBee.
- Prestare attenzione durante la manipolazione per evitare danni elettrici al PCB e ai componenti.
- Non esporre i moduli radio XBee all'acqua o all'umidità.
- Utilizzare questo prodotto con le antenne specificate nelle guide per l'utente del modulo XBee.
- L'utente finale deve sapere come togliere l'alimentazione al modulo radio XBee o come posizionare le antenne a 20 cm da persone o animali.

Drošības instrukcijas

XBee moduļi

- Radio moduļa XBee darbība nevar tikt garantēta radio savienojuma dēļ, tāpēc to nevajadzētu izmantot bloķēšanai drošības ziņā kritiskās ierīcēs, piemēram, mašīnās vai automobiļos.
- XBee radio modulis nav apstiprināts lietošanai (šis saraksts nav pilnīgs):
  - medicīniskās ierīces
  - kodolprogrammas
  - sprādzienbīstamā vai uzliesmojošā vidē

- XBee radio moduļa iekšpusē nav neviena komponenta, ko lietotājs varētu apkopt. Nenoņemiet vairogu un nekādā veidā nepārveidojiet XBee. Modifikācijas rezultātā modulis var tikt izslēgts no jebkādas garantijas un var izraisīt XBee radio darbību, kas neatbilst noteiktās valsts normatīvajiem aktiem, izraisot iespējamu nelegālu radio darbību.
- Strādājot ar XBee moduli, izmantojiet nozares standarta ESD aizsardzību.
- Rīkojoties, rīkojieties uzmanīgi, lai izvairītos no PCB un komponentu elektriskiem bojājumiem.
- Nepakļaujiet XBee radio moduļus ūdens vai mitruma iedarbībai.
- Izmantojiet šo izstrādājumu ar antenām, kas norādītas XBee moduļa lietotāja rokasgrāmatās.
- Galalietotājam ir jāpaskaidro, kā atvienot XBee radio moduļa strāvu vai novietot antenas 20 cm attālumā no cilvēkiem vai dzīvniekiem.

Saugos instrukcijos

XBee moduliai

- Negalima garantuoti, kad „XBee“ radijo modulis veiks dėl radijo ryšio, todėl jo neturėtų būti naudojamas blokuoti saugai svarbiuose įrenginiuose, pvz., mašinose ar automobiliuose.
- XBee radijo modulis nebuvo patvirtintas naudoti (šis sąrašas nėra baigtinis):
  - medicinos prietaisai
  - branduolinės programos
  - sprogioje ar degioje aplinkoje
- XBee radijo modulio viduje nėra komponentų, kuriuos vartotojas galėtų prižiūrėti. Jokiu būdu nenuimkite skydo ir nekeiskite XBee. Dėl modifikacijų moduliui gali būti netaikoma jokia garantija, o „XBee“ radijas gali veikti ne pagal tam tikros šalies norminius reikalavimus, o tai gali sukelti neteisėtą radijo naudojimą.
- Dirbdami su XBee moduliu naudokite pramonės standartinę ESD apsaugą.
- Dirbdami būkite atsargūs, kad nepažeistumėte PCB ir komponentų.
- Saugokite XBee radijo modulius nuo vandens ar drėgmės.
- Naudokite šį gaminį su antenomis, nurodytomis XBee modulio vartotojo vadove.
- Galutiniam vartotojui turi būti paaiškinta, kaip atjungti XBee radijo modulio maitinimą arba nustatyti antenas 20 cm atstumu nuo žmonių ar gyvūnų.

Sikkerhetsinstruksjoner

XBee-moduler

- XBee-radiomodulen kan ikke garanteres drift på grunn av radiolinken, og bør derfor ikke brukes til forriglinger i sikkerhetskritiske enheter som maskiner eller bilapplikasjoner.
- XBee-radiomodulen er ikke godkjent for bruk i (denne listen er ikke uttømmende):

  - medisinsk utstyr
  - kjernefysiske applikasjoner
  - eksplosive eller brennbare atmosfærer
- Det er ingen komponenter som kan repareres av brukeren inne i XBee-radiomodulen. Ikke fjern skjoldet eller modifiser XBee på noen måte. Endringer kan ekskludere modulen fra enhver garanti og kan føre til at XBee-radioen fungerer utenfor regelverket for et gitt land, noe som kan føre til ulovlig drift av radioen.
- Bruk industristandard ESD-beskyttelse når du håndterer XBee-modulen.
- Vær forsiktig ved håndtering for å unngå elektrisk skade på PCB og komponenter.
- Ikke utsett XBee radiomoduler for vann eller fuktighet.
- Bruk dette produktet med antennene spesifisert i XBee-modulens brukerveiledninger.
- Sluttbrukeren må bli fortalt hvordan man fjerner strømmen fra XBee-radiomodulen eller plasserer antennene 20 cm fra mennesker eller dyr.

Instrukcje bezpieczeństwa

Moduły XBee

- Moduł radiowy XBee nie może zagwarantować działania ze względu na łącze radiowe, dlatego nie należy go używać do blokad w urządzeniach o krytycznym znaczeniu dla bezpieczeństwa, takich jak maszyny lub aplikacje motoryzacyjne.
- Moduł radiowy XBee nie został dopuszczony do użytku w (lista ta nie jest wyczerpująca):
  - wyroby medyczne
  - zastosowania nuklearne
  - atmosferach wybuchowych lub łatwopalnych
- Wewnątrz modułu radiowego XBee nie ma żadnych elementów, które mogłyby być serwisowane przez użytkownika. Nie zdejmuj osłony ani nie modyfikuj XBee w żaden sposób. Modyfikacje mogą wykluczyć moduł z jakiejkolwiek gwarancji i spowodować, że radio XBee będzie działać niezgodnie z przepisami obowiązującymi w danym kraju, co może prowadzić do nielegalnego działania radia.
- Podczas obsługi modułu XBee należy stosować standardową ochronę ESD.
- Podczas obsługi należy zachować ostrożność, aby uniknąć uszkodzeń elektrycznych PCB i komponentów.
- Nie wystawiaj modułów radiowych XBee na działanie wody lub wilgoci.
- Używaj tego produktu z antenami określonymi w podręcznikach użytkownika modułu XBee.
- Użytkownik końcowy musi zostać poinformowany, jak odłączyć zasilanie modułu radiowego XBee lub zlokalizować anteny w odległości 20 cm od ludzi lub zwierząt.

Instruções de segurança

Módulos XBee

- O módulo de rádio XBee não pode ter operação garantida devido ao link de rádio e, portanto, não deve ser usado para intertravamentos em dispositivos críticos de segurança, como máquinas ou aplicações automotivas.
- O módulo de rádio XBee não foi aprovado para uso em (esta lista não é exaustiva):
  - o dispositivos médicos
  - o aplicações nucleares
  - o atmosferas explosivas ou inflamáveis
- Não há componentes que possam ser reparados pelo usuário dentro do módulo de rádio XBee. Não remova a blindagem nem modifique o XBee de forma alguma. As modificações podem excluir o módulo de qualquer garantia e fazer com que o rádio XBee opere fora da conformidade regulatória de um determinado país, levando à possível operação ilegal do rádio.
- Use proteção ESD padrão da indústria ao manusear o módulo XBee.
- Tome cuidado ao manusear para evitar danos elétricos à PCB e aos componentes.
- Não exponha os módulos de rádio XBee à água ou umidade.
- Use este produto com as antenas especificadas nos guias do usuário do módulo XBee.
- O usuário final deve ser informado sobre como remover a energia do módulo de rádio XBee ou localizar as antenas a 20 cm de humanos ou animais.

Instructiuni de siguranta

module XBee

- Nu se poate garanta funcționarea modulului radio XBee din cauza conexiunii radio și, prin urmare, nu trebuie utilizat pentru interblocări în dispozitive critice pentru siguranță, cum ar fi mașini sau aplicații auto.
- Modulul radio XBee nu a fost aprobat pentru utilizare în (această listă nu este exhaustivă):
  - dispozitive medicale
  - aplicații nucleare
  - atmosfere explozive sau inflamabile
- Nu există componente care să poată fi reparate de utilizator în interiorul modulului radio XBee. Nu îndepărtați scutul și nu modificați XBee în niciun fel. Modificările pot exclude modulul din orice garanție și pot face ca radioul XBee să funcționeze în afara conformității cu reglementările pentru o anumită țară, ceea ce duce la o posibilă funcționare ilegală a radioului.
- Folosiți protecția ESD standard în industrie când manipulați modulul XBee.
- Aveți grijă în timpul manipulării pentru a evita deteriorarea electrică a PCB-ului și a componentelor.

- Nu expuneți modulele radio XBee la apă sau umezeală.
- Utilizați acest produs cu antenele specificate în ghidurile utilizatorului modulului XBee.
- Utilizatorului final trebuie să i se spună cum să scoată alimentarea de la modulul radio XBee sau să găsească antenele la 20 cm de oameni sau animale.

Bezpečnostné inštrukcie

moduly XBee

- Rádiový modul XBee nemôže byť zaručený kvôli rádiovému spojeniu, a preto by sa nemal používať na blokovanie v zariadeniach kritických z hľadiska bezpečnosti, ako sú stroje alebo automobilové aplikácie.
- Rádiový modul XBee nebol schválený na použitie v (tento zoznam nie je úplný):
  - zdravotnícke pomôcky
  - jadrové aplikácie
  - výbušné alebo horľavé atmosféry
- Vo vnútri rádiového modulu XBee sa nenachádzajú žiadne používateľsky opraviteľné komponenty. Neodstraňujte štít ani žiadnym spôsobom neupravujte XBee. Úpravy môžu vyňať modul zo záruky a môžu spôsobiť, že rádio XBee bude fungovať mimo zhody s predpismi pre danú krajinu, čo vedie k možnej nezákonnej prevádzke rádia.
- Pri manipulácii s modulom XBee používajte štandardnú ochranu pred ESD.
- Pri manipulácii buďte opatrní, aby ste predišli elektrickému poškodeniu dosky plošných spojov a komponentov.
- Rádiové moduly XBee nevystavujte vode ani vlhkosti.
- Tento produkt používajte s anténami špecifikovanými v používateľských príručkách modulu XBee.
- Koncový používateľ musí byť informovaný o tom, ako odpojiť napájanie rádiového modulu XBee alebo ako umiestniť antény 20 cm od ľudí alebo zvierat.

Varnostna navodila

XBee moduli

- Radijskega modula XBee ni mogoče zagotoviti delovanja zaradi radijske povezave in ga zato ne smete uporabljati za zaklepanje v varnostno kritičnih napravah, kot so stroji ali avtomobilske aplikacije.
- Radijski modul XBee ni bil odobren za uporabo v (ta seznam ni izčrpen):
  - medicinskih pripomočkov
  - jedrske aplikacije
  - eksplozivne ali vnetljive atmosfere
- V radijskem modulu XBee ni komponent, ki bi jih lahko popravil uporabnik. Ne odstranjujte ščita in na noben način ne spreminjajte XBee. Spremembe lahko modul izključijo iz kakršne

koli garancije in lahko povzročijo, da radio XBee deluje zunaj zakonske skladnosti za dano državo, kar vodi do možnega nezakonitega delovanja radia.

- Pri ravnanju z modulom XBee uporabite standardno industrijsko zaščito pred ESD.
- Pri rokovanju pazite, da se izognete električnim poškodbam tiskanega vezja in komponent.
- Radijskih modulov XBee ne izpostavljajte vodi ali vlagi.
- Ta izdelek uporabljajte z antenami, navedenimi v uporabniških priročnikih modula XBee.
- Končnemu uporabniku je treba povedati, kako odstraniti napajanje z radijskega modula XBee ali naj locira antene 20 cm od ljudi ali živali.

Instrucciones de seguridad

Módulos XBee

- No se puede garantizar el funcionamiento del módulo de radio XBee debido al enlace de radio y, por lo tanto, no debe usarse para enclavamientos en dispositivos críticos para la seguridad, como máquinas o aplicaciones automotrices.
- El módulo de radio XBee no ha sido aprobado para su uso en (esta lista no es exhaustiva):
  - dispositivos médicos
  - aplicaciones nucleares
  - atmósferas explosivas o inflamables
- No hay componentes reparables por el usuario dentro del módulo de radio XBee. No quite el escudo ni modifique el XBee de ninguna manera. Las modificaciones pueden excluir el módulo de cualquier garantía y pueden hacer que la radio XBee funcione fuera del cumplimiento normativo de un país determinado, lo que puede provocar una operación ilegal de la radio.
- Utilice la protección ESD estándar de la industria al manipular el módulo XBee.
- Tenga cuidado al manipularlo para evitar daños eléctricos en la PCB y los componentes.
- No exponga los módulos de radio XBee al agua ni a la humedad.
- Utilice este producto con las antenas especificadas en las guías de usuario del módulo XBee.
- Se debe indicar al usuario final cómo desconectar la alimentación del módulo de radio XBee o ubicar las antenas a 20 cm de personas o animales.

Säkerhets instruktioner

XBee-moduler

- XBee-radiomodulen kan inte garanteras funktion på grund av radiolänken och bör därför inte användas för förreglingar i säkerhetskritiska enheter som maskiner eller biltillämpningar.
- XBee-radiomodulen har inte godkänts för användning i (denna lista är inte uttömmande):

  - medicinsk utrustning
  - kärnkraftstillämpningar
  - explosiv eller brandfarlig atmosfär
- Det finns inga komponenter som användaren kan reparera inuti XBee-radiomodulen. Ta inte bort skölden eller modifiera XBee på något sätt. Ändringar kan utesluta modulen från alla garantier och kan göra att XBee-radion fungerar utanför bestämmelserna för ett visst land, vilket kan leda till att radion kan användas olagligt.
- Använd industristandard ESD-skydd när du hanterar XBee-modulen.
- Var försiktig vid hanteringen för att undvika elektriska skador på kretskortet och komponenterna.
- Utsätt inte XBee radiomoduler för vatten eller fukt.
- Använd den här produkten med antennerna som specificeras i XBee-modulens användarguider.
- Slutanvändaren måste informeras om hur man kopplar bort strömmen från XBee-radiomodulen eller för att placera antennerna 20 cm från människor eller djur.

Configure the XBee® BLU

Configure the device using XCTU

XBee Configuration and Test Utility (XCTU) is a multi-platform program that enables users to interact with Digi radio frequency (RF) devices through a graphical interface. The application includes built-in tools that make it easy to set up, configure, and test Digi RF devices.

For instructions on downloading and using XCTU, see the *XCTU User Guide*.

Once you install XCTU, click the XCTU icon to open the program.

Custom defaults

Custom defaults allow you to preserve a subset of the device configuration parameters even after returning to default settings using RE (Restore Defaults). This can be useful for settings that identify the device—such as NI (Network Identifier).

Set custom defaults

Use %F (Set Custom Default) to set custom defaults. When the XBee® BLU receives **%F** it takes the next command it receives and applies it to both the current configuration and the custom defaults.

To set custom defaults for multiple commands, send a **%F** before each command.

Restore factory defaults

!C (Clear Custom Defaults) clears all custom defaults, so that RE (Restore Defaults) will restore the device to factory defaults. Alternatively, R1 (Restore Factory Defaults) restores all parameters to factory defaults without erasing their custom default values.

Limitations

There is a limitation on the number of custom defaults that can be set on a device. The number of defaults that can be set depends on the size of the saved parameters and the devices' firmware version. When there is no more room for custom defaults to be saved, any command sent immediately after a **%F** returns an error.

Custom configuration: Create a new factory default

You can create a custom configuration that is used as a new factory default. This feature is useful if, for example, you need to maintain certain settings for manufacturing or want to ensure a feature is always enabled. When you use RE (Restore Defaults) to perform a factory reset on the device, the custom configuration is set on the device after applying the original factory default settings.

The custom configuration is stored in non-volatile memory using a wear-leveling technology. This means that the custom configuration may be written multiple times to the same page of flash memory before doing an erase on that page, which reduces the number of erasures and the time to write the custom configuration.

You can use !C (Clear Custom Defaults) to clear all values in the custom configuration at any time.

Set a custom configuration

1. Open XCTU and load your device.
2. Enter Command mode, or do the following process in API mode, according to your preference.
3. Perform the following process for each configuration that you want to set as a factory default.
   a. Send the Set Custom Default command, **AT%F**. This command enables you to enter a custom configuration.
   b. Send the custom configuration command.

Clear all custom configuration on a device

After you have set configurations using %F (Set Custom Default), you can return all configurations to the original factory defaults.

1. Open XCTU and load the device.
2. Enter Command mode.
3. Send **AT!C**.

XBee bootloader

You can update firmware on the XBee® BLU serially. This is done by invoking the XBee bootloader and transferring the firmware image using XMODEM.

This process is also used for updating a local device's firmware using XCTU.

XBee devices use a modified version of Silicon Labs' Gecko bootloader. This bootloader version supports a custom entry mechanism that uses module pins DIN, $\overline{\text{DTR}}$/SLEEP_RQ, and $\overline{\text{RTS}}$.

To invoke the bootloader using hardware flow control lines, do the following:

1. Set $\overline{\text{DTR}}$/SLEEP_RQ low (CMOS0V) and RTS high.
2. Send a serial break to the DIN pin and power cycle or reset the module.
3. When the device powers up, set $\overline{\text{DTR}}$/SLEEP_RQ and DIN to low (CMOS0V) and $\overline{\text{RTS}}$ should be high.
4. Terminate the serial break and send a carriage return at 115200 baud to the device.
5. If successful, the device sends the Silicon Labs' Gecko bootloader menu out the DOUT pin at 115200 baud.
6. You can send commands to the bootloader at 115200 baud.

Note Disable hardware flow control when entering and communicating with the bootloader.

All serial communications with the module use 8 data bits, no parity bit, and 1 stop bit.

You can also invoke the bootloader from the XBee application by sending %P (Invoke Bootloader).

Send a firmware image

After invoking the bootloader, a menu is sent out the UART at 115200 baud. To upload a firmware image through the UART interface:

1. Look for the bootloader prompt **BL >** to ensure the bootloader is active.
2. Send an ASCII **1** character to initiate a firmware update.
3. After sending a **1**, the device waits for an XModem CRC upload of a .gbl image over the serial line at 115200 baud. Send the .gbl file to the device using standard XMODEM-CRC.

If the firmware image is successfully loaded, the bootloader outputs a “complete” string. Invoke the newly loaded firmware by sending a **2** to the device.

If the firmware image is not successfully loaded, the bootloader outputs an "aborted string". It returns to the main bootloader menu. Some causes for failure are:

- Over 1 minute passes after the command to send the firmware image and the first block of the image has not yet been sent.
- A power cycle or reset event occurs during the firmware load.
- A file error or a flash error occurs during the firmware load. The following table contains errors that could occur during the XMODEM transfer.

Error	Cause	Workaround
0x18	This error is observed when a serial upload attempt has been abruptly discontinued by invoking **Ctrl+C** and subsequently another attempt is made to upload a gbl by pressing **1** on the bootloader menu.	Press **2** on the bootloader menu. The bootloader performs a reboot and the menu gets displayed again. Now press **1** and begin uploading the gbl.

Software libraries

One way to communicate with the XBee® BLU is by using a software library. The libraries available for use with the XBee® BLU include:

- XBee Java library
- XBee Python library

The XBee Java Library is a Java API. The package includes the XBee library, its source code and a collection of samples that help you develop Java applications to communicate with your XBee devices.

The XBee Python Library is a Python API that dramatically reduces the time to market of XBee projects developed in Python and facilitates the development of these types of applications, making it an easy process.

XBee Multi Programmer

The XBee Multi Programmer is a combination of hardware and software that enables partners and distributors to program multiple Digi Radio frequency (RF) devices simultaneously. It provides a fast and easy way to prepare devices for distribution or large networks deployment.

The XBee Multi Programmer board is an enclosed hardware component that allows you to program up to six RF modules thanks to its six external XBee sockets. The XBee Multi Programmer application communicates with the boards and allows you to set up and execute programming sessions. Some of the features include:

- Each XBee Multi Programmer board allows you to program up to six devices simultaneously. Connect more boards to increase the programming concurrency.
- Different board variants cover all the XBee form factors to program almost any Digi RF device.

Download the XBee Multi Programmer application from: digi.com/support/productdetail?pid=5641

See the *XBee Multi Programmer User Guide* for more information.

Get started with BLE

Bluetooth® Low Energy (BLE) is a RF protocol that enables you to connect your XBee device to another device. Both devices must have BLE enabled.

For example, you can use your cellphone to connect to your XBee device, and then from your phone, configure and program the device.

Digi created the Digi XBee Mobile SDK, a set of libraries, examples and documentation that help you develop mobile applications to interact with XBee devices through their BLE interface. For this purpose, we provide two easy-to-use libraries that allow you to create XBee mobile native apps:

- XBee Library for Xamarin, to develop cross-platform mobile applications using C# language (iOS and Android).
- XBee Library for Android, to develop Android applications using Java.

The XBee is the server and allows client devices, such as a cellphone, to configure the XBee or data transfer with the User Data Relay frame.

Enable BLE on the XBee® BLU

To enable BLE on a XBee® BLU and verify the connection:

1. Set up the XBee® BLU and make sure to connect the antenna to the device.
2. Enable BLE and configure the BLE password.
3. Get the Digi XBee Mobile phone application.
4. Connect with BLE and configure your XBee® BLU.

Enable BLE and configure the BLE password

Some of the latest XBee devices support Bluetooth Low Energy (BLE) as an extra interface for configuration. If you want to use this feature, you have to enable BLE. You must also enable security by setting a password on the XBee® BLU in order to connect, configure, or send data over BLE.

Use XCTU to configure the BLE password. Make sure you have installed or updated XCTU to version 6.4.2 or newer. Earlier versions of XCTU do not include the BLE configuration features. See Download and install XCTU for installation instructions.

Before you begin, you should determine the password you want to use for BLE on the XBee® BLU and store it in a secure place. We recommend a secure password of at least eight characters and a random combination of letters, numbers, and special characters. We recommend using a security management tool such as LastPass or Keepass for generating and storing passwords for many devices.

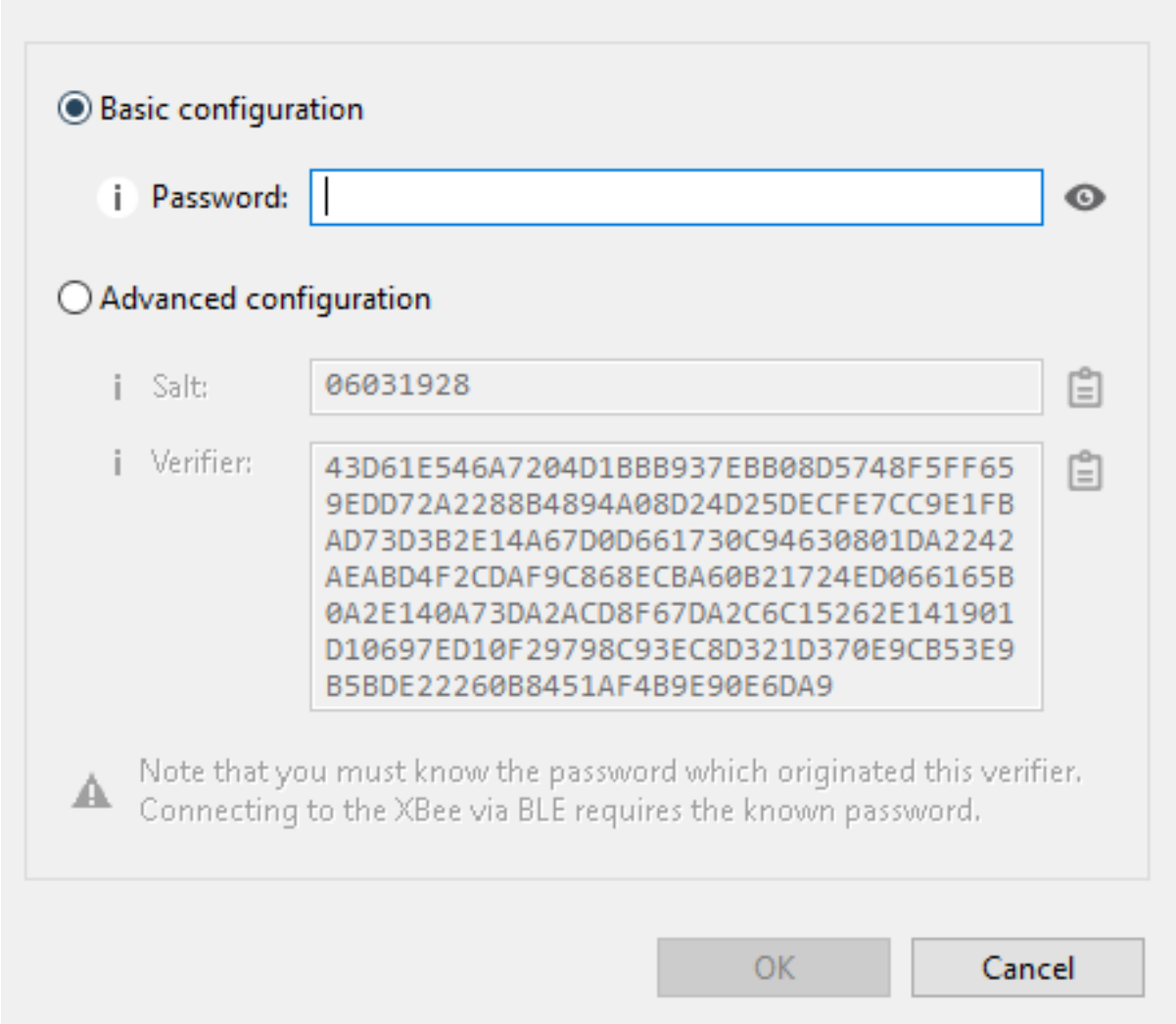
Note When you enter the BLE password in XCTU, the salt and verifier values are calculated as you set your password. For more information on how these values are used in the authentication process, see BLE Unlock Request - 0x2C.

1. Launch XCTU .
2. Switch to Configuration working mode .
3. Select a BLE compatible radio module from the device list.
4. Select **Enabled[1]** from the **BT Bluetooth Enable** command drop-down.

5. Click the **Write setting** button . The **Bluetooth authentication not set** dialog appears.

Note If BLE has been previously configured, the **Bluetooth authentication not set** dialog does not appear. If this happens, click **Configure** in the Bluetooth Options section to display the **Configure Bluetooth Authentication** dialog.

6. Click **Configure** in the dialog. The **Configure Bluetooth Authentication** dialog appears.
7. In the **Password** field, type the password for the device. As you type, the **Salt** and **Verifier** fields are automatically calculated and populated in the dialog as shown above. This password is used when you connect to this XBee device via BLE using the Digi XBee Mobile app.



8. Click **OK** to save the configuration.

Get the Digi XBee Mobile phone application

To see the nearby devices that have BLE enabled, you must get the free Digi XBee Mobile application from the iOS App Store or Google Play and downloaded to your phone.

1. On your phone, go to the App store.
2. Search for: **Digi XBee Mobile**.
3. Download and install the app.

The Digi XBee Mobile application is compatible with the following operating systems and versions:

- Android 5.0 or higher
- iOS 11 or higher

Connect with BLE and configure your XBee® BLU

You can use the Digi XBee Mobile application to verify that BLE is enabled on your XBee® BLU.

1. Get the Digi XBee Mobile phone application.
2. Open the Digi XBee Mobile application. The **Find XBee devices** screen appears and the app automatically begins scanning for devices. All nearby devices with BLE enabled are displayed in a list.
3. Scroll through the list to find your XBee device.
   The first time you open the app on a phone and scan for devices, the device list contains only the name of the device and the BLE signal strength. No identifying information for the device displays. After you have authenticated the device, the device information is cached on the phone.
4. Tap the XBee device name in the list. A password dialog appears.
5. Enter the password you previously configured for the device in XCTU.
6. Tap **OK**. The **Device Information** screen displays. You can now scroll through the settings for the device and change the device's configuration as needed.

BLE reference

XBee BLE feature set

This section lists BLE features as well through which interface(s) they can be configured or interacted with.

General

BLE MAC Address

The EUI-48 Bluetooth MAC address displayed in the module's advertisements.

Interface	Documentation link if available
AT Commands	BL (Bluetooth Address)
API Frames	Local AT Command Request - 0x08
MicroPython	xbee.atcmd()

On-Demand Enable/Disable

BLE can be enabled or disabled on command. This can be useful to reduce power usage by disabling BLE when not needed.

Interface	Documentation link if available
AT Commands	BT (Bluetooth Enable)
API Frames	Local AT Command Request - 0x08
MicroPython	ble.active()

Advertising

Legacy

The default advertising mode. Uses 3 advertising channels (37, 38, 39) and has a smaller advertising payload size of 31 bytes. The default advertisement displays the protocol name of the XBee. This can be overridden by using the **BI** command or by using `ble.gap_advertise()`.

Interface	Documentation link if available
AT Commands	BI (Bluetooth Identifier)
API Frames	Local AT Command Request - 0x08
MicroPython	ble.gap_advertise()

Extended

More enhanced advertising then legacy advertising. Uses all 40 channels and can display payloads of up to 191 bytes.

Interface	Documentation link if available
AT Commands	Not supported
API Frames	Not supported
MicroPython	ble.gap_advertise()

Periodic Without Response

Sends advertising data out on regular event intervals. Observer devices can discover and synchronize to the advertising schedule by communicating with the broadcaster. The main purpose of this feature is to save on battery life as scanners will only need to be in RX mode during the advertising period. See `ble.sync_scan` for syncing to a periodic advertiser.

Interface	Documentation link if available
AT Commands	Not supported
API Frames	Not supported
MicroPython	ble.gap_advertise()

Power Level

The advertising power level can be configured using the BP command.

Interface	Documentation link if available
AT Commands	BP (Bluetooth Power)
API Frames	Local AT Command Request - 0x08
MicroPython	xbee.atcmd()

GAP Scan

Legacy

The XBee can initiate scans for legacy advertisements. This is the main method used to find and connect to other BLE devices.

Interface	Documentation link if available
AT Commands	■ GS (GAP Scan) ■ DG (GAP Scan Duration) ■ WG (GAP Scan Window) ■ IG (GAP Scan Interval) ■ FG (Advertisement Data Filter)
API Frames	■ Gap Scan Request - 0x34

Interface	Documentation link if available
	■ GAP Scan Legacy Advertisement Response - 0xB4 ■ GAP Scan Status - 0xB5
MicroPython	ble.gap_scan()

Extended

The XBee also can scan for and output extended advertisements which contain more data fields as well as payload bytes than legacy advertisements.

Interface	Documentation link if available
AT Commands	■ GS (GAP Scan) ■ DG (GAP Scan Duration) ■ WG (GAP Scan Window) ■ IG (GAP Scan Interval) ■ FG (Advertisement Data Filter)
API Frames	■ Gap Scan Request - 0x34 ■ Bluetooth GAP Scan Extended Advertisement Response - 0xB7 ■ GAP Scan Status - 0xB5
MicroPython	ble.gap_scan()

Periodic Sync

An XBee can synchronize to a periodically advertising device using sync information provided in the associated extended advertisement of a periodically advertising device. See `ble.gap_scan` for how to initiate a device to periodically advertise.

Interface	Documentation link if available
AT Commands	Not supported
API Frames	Not supported
MicroPython	ble.sync_scan()

GATT Client

Multiple Connections

The XBee BLU currently supports up to two simultaneous connections to GATT servers.

GAP Connect

XBee's can connect to other BLE devices to access their GATT services.

Interface	Documentation link if available
AT Commands	Not supported
API Frames	Not supported
MicroPython	ble.gap_connect()

GATT Interaction

XBee's can interact with GATT servers over a GAP connection. GATT attributes can be discovered; characteristics and descriptors can be written to, read, or subscribed to if the server supports those operations.

Interface	Documentation link if available
AT Commands	Not supported
API Frames	Not supported
MicroPython	ble.gap_connection

XBee Connect

XBee's can connect to other XBee's and use the API service characteristics to send API frames to a remote XBee. This allows operations such as configuration, data transfer, and OTA firmware updates.

Interface	Documentation link if available
AT Commands	Not supported
API Frames	Not supported
MicroPython	ble.xbee_connect()

PHY Configuration

The PHY configuration can be modified for a given GATT server connection. This can be updated to improve speed and power usage with the 2M PHY option or increase range and sensitivity with the 125K or 500K Coded PHY options.

Interface	Documentation link if available
AT Commands	Not supported
API Frames	Not supported
MicroPython	ble.phyconfig()

GATT Server

XBee API Service Configuration

Configure the XBee for using the API GATT service. XBee's support sending/receiving API frames via this service. See API Request characteristic and API response characteristic for more information.

Interface	Documentation link if available
AT Commands	■ $S (SRP Salt) ■ $V, $W, $X, $Y commands (SRP Salt verifier)
API Frames	Local AT Command Request - 0x08
MicroPython	ble.atcmd()

Dynamic GATT Database

New user configured services can be dynamically appended to the static services of the XBee. These can be configured with properties such as reading, writing, notifications, or indications. Attributes can also be configured to only be interacted with if the client has the needed security privileges.

Interface	Documentation link if available
AT Commands	Not supported
API Frames	Not supported
MicroPython	■ ble.gattdb_register_services() ■ ble.gattdb_read() ■ ble.gattdb_write()

Security

Encrypted Advertisements

Advertisement data payloads can be encrypted to secure data being transferred via advertisements. An encryption key can be set on the advertiser and read over a GATT connection from a client with the necessary security privileges to decrypt the payload.

Interface	Documentation link if available
AT Commands	Not supported
API Frames	Not supported
MicroPython	■ ble.set_encryption_key() ■ ble.gatt_write_key() ■ ble.encrypt_adv_data() ■ ble.decrypt_adv_data()

Pairing and Bonding

Xbee's support pairing and bonding.

Interface	Documentation link if available
AT Commands	Not supported
API Frames	Not supported
MicroPython	■ ble.config() ■ ble.gap_connection.secure()

BLE advertising behavior and services

When the Bluetooth radio is enabled, periodic BLE advertisements are transmitted. The advertisement data includes the product name in the Complete Local Name field. When an XBee device connects to the Bluetooth radio, the BLE services are listed:

- Device Information Service
- XBee API BLE Service

Device Information Service

The standard Device Information Service is used. The Manufacturer, Model, and Firmware Revision characters are provided inside the service.

XBee API BLE Service

You can configure the XBee® BLU through the BLE interface using API frame requests and responses. The API frame format through Bluetooth is equivalent to setting **AP** = **1** and transmitting the frames over the UART or SPI interface. API frames can be executed over Bluetooth regardless of the AP setting.

The BLE interface allows these frames:

- BLE Unlock Request - 0x2C
- User Data Relay Input - 0x2D
- Response - 0xAC
- Local AT Command Request - 0x08
- Queue Local AT Command Request - 0x09

This API reference assumes that you are familiar with Bluetooth and GATT services. The specifications for Bluetooth are an open standard and can be found at the following links:

- Bluetooth Core Specifications: bluetooth.com/specifications/bluetooth-core-specification
- Bluetooth GATT: bluetooth.com/specifications/gatt/generic-attributes-overview

The XBee API BLE Service contains two characteristics: the API Request characteristic and the API Response characteristic. The UUIDs for the service and its characteristics are listed in the table below.

Characteristic	UUID
API Service UUID	53da53b9-0447-425a-b9ea-9837505eb59a
API Request Characteristic UUID	7dddca00-3e05-4651-9254-44074792c590
API Response Characteristic UUID	f9279ee9-2cd0-410c-81cc-adf11e4e5aea

API Request characteristic

UUID: 7dddca00-3e05-4651-9254-44074792c590

Permissions: Writeable

XBee API frames are broken into chunks and transmitted sequentially to the request characteristic using write operations. Valid frames are then processed and the result is returned through indications on the response characteristic.

API frames do not need to be written completely in a single write operation to the request characteristic. In fact, Bluetooth limits the size of a written value to 3 bytes smaller than the configured Maximum Transmission Unit (MTU), which defaults to 23, meaning that by default, you can only write 20 bytes at a time.

After connecting you must send a valid Bluetooth Unlock API Frame in order to authenticate the connection. If the BLE Unlock API - 0x2C frame has not been executed, all other API frames are silently ignored and are not processed.

API Response characteristic

UUID: f9279ee9-2cd0-410c-81cc-adf11e4e5aea

Permissions: Readable, Indicate

Responses to API requests made to the request characteristic are returned through the response characteristics. This characteristic cannot be read directly.

Response data is presented through indications on this characteristic. Indications are acknowledged and re-transmitted at the BLE link layer and application layer and provide a robust transport for this data.

File system

Directory structure

The XBee® BLU's internal flash appears in the file system as **/flash**, the only entry at the root level of the file system. Files and directories other than **/flash** cannot be created within the root directory, only within **/flash**.

Paths

- Paths starting with a forward slash are "absolute" and must start with **/flash** to be valid.
- All other paths are relative to the current working directory.
- The directory **..** refers to the parent directory, so an operation on **../filename.txt** that takes place in the directory **/flash/test** accesses the file **/flash/filename.txt**.
- The directory **.** refers to the current directory, so **ATFS ls .** is the same as **ATFS ls**, which lists files in the current directory.
- Names are case-insensitive, so **FILE.TXT**, **file.txt** and **FiLe.TxT** all refer to the same file.
- File and directory names are limited to 64 characters, and can only contain letters, numbers, periods, dashes and underscores. A period at the end of the name is ignored.
- The full, absolute path to a file or directory is limited to 255 characters.

Limitations

The file system on the XBee® BLU has a few limitations when compared to conventional file systems:

- When a file on the file system is deleted, the space it was using is only reclaimed if it is found at the end of the file system. Deleted data that is contiguous with the last placed deleted file is also reclaimed.
- The file system can only have one file open for writing at a time.
- The file system cannot create new directories while a file is open for writing.
- Files cannot be renamed.
- The contents of the file system will be lost when any firmware update is performed. See Update the firmware over-the-air in General Purpose Flash Memory for information on how to put files on a device after a firmware over-the-air (FOTA) update.

XCTU interface

XCTU releases starting with 6.4.0 include a **File System Manager** in the **Tools** menu. You can upload files to and download files from the device, in addition to renaming and deleting existing files and directories. See the File System manager tool section of the *XCTU User Guide* for details of its functionality.

Get started with MicroPython

This user guide provides an overview of how to use MicroPython with the XBee® BLU. For in-depth information and more complex code examples, refer to the *Digi MicroPython Programming Guide*. Continue with this user guide for simple examples to get started using MicroPython on the XBee® BLU.

About MicroPython

MicroPython is an open-source programming language based on Python 3.0, with much of the same syntax and functionality, but modified to fit on small devices with limited hardware resources, such as an XBee® BLU.

For more information about MicroPython, see www.micropython.org.

For more information about Python, see www.python.org.

MicroPython on the XBee® BLU

The XBee® BLU has MicroPython running on the device itself. You can access a MicroPython prompt from the XBee® BLU when you install it in an appropriate development board (XBDB or XBIB), and connect it to a computer via a USB cable.

Note MicroPython is only available through the UART interface and does not work with SPI.

The examples in this user guide assume:

- You have XCTU on your computer. See Configure the device using XCTU.
- You have a serial terminal program installed on your computer. For more information, see Use the MicroPython Terminal in XCTU. This requires XCTU 6.3.10 or higher.
- You have an XBee® BLU installed on an appropriate development board such as an XBIB-U-DEV or an XBDB-U-ZB.
- The XBee® BLU is connected to the computer via a USB cable and XCTU recognizes it.

Use XCTU to enter the MicroPython environment

To use the XBee® BLU in the MicroPython environment:

1. Use XCTU to add the device(s); see Configure the device using XCTU and Add devices to XCTU.
2. The XBee® BLU appears as a box in the **Radio Modules** information panel. Each module displays identifying information about itself.
3. Click this box to select the device and load its current settings.

   Note To ensure that MicroPython is responsive to input, Digi recommends setting the XBee UART baud rate to 115200 baud. To set the UART baud rate, select **115200 [7]** in the **BD** field and click the **Write** button. We strongly recommend using hardware flow control to avoid data loss, especially when pasting large amounts of code or text. For more information, see UART flow control.
4. To put the XBee® BLU into MicroPython mode, in the **AP** field select **MicroPython REPL [4]** and click the **Write** button  .
5. Note which COM port the XBee® BLU is using, because you will need this information when you use the MicroPython terminal.

Use the MicroPython Terminal in XCTU

You can use the MicroPython Terminal to communicate with the XBee® BLU when it is in MicroPython mode.[1] This requires XCTU 6.3.10 or higher. To enter MicroPython mode, follow the steps in Use XCTU to enter the MicroPython environment. To use the MicroPython Terminal:

1. Click the **Tools** drop-down menu and select **MicroPython Terminal**. The terminal window opens.
2. Click **Open** to open the Serial Port Configuration window.
3. In the **Select the Serial/USB port** area, click the COM port that the device uses.
4. Verify that the baud rate and other settings are correct.
5. Click **OK**. The **Open** icon changes to **Close**, indicating that the device is properly connected.

If the **>>>** prompt appears, you are connected properly. You can now type or paste MicroPython code in the terminal.

MicroPython examples

This section provides examples of how to use some of the basic functionality of MicroPython with the XBee® BLU.

Example: hello world

1. At the MicroPython **>>>** prompt, type the Python command: **print("Hello, World!")**
2. Press **Enter** to execute the command. The terminal echos back **Hello, World!**

Example: enter MicroPython paste mode

In the following examples it is helpful to know that MicroPython supports paste mode, where you can copy a large block of code from this user guide and paste it instead of typing it character by character. To use paste mode:

1. Copy the code you want to run. For example, copy the following code that is the code from the "Hello world" example:

```
print("Hello World")
```

Note You can easily copy and paste code from the online version of this guide. Use caution with the PDF version, as it may not maintain essential indentations.

2. In the terminal, at the MicroPython **>>>** prompt type **Ctrl-+E** to enter paste mode. The terminal displays **paste mode; Ctrl-C to cancel, Ctrl-D to finish**.
3. Right-click in the MicroPython terminal window and click **Paste** or press **Ctrl+Shift+V** to paste.

[1] See Other terminal programs if you do not use the MicroPython Terminal in XCTU.

4. The code appears in the terminal occupying one line. Each line starts with its line number and three "=" symbols. For example, line 1 starts with **1===**.
5. If the code is correct, press **Ctrl**+**D** to run the code; “Hello World” should print.

> **Note** If you want to exit paste mode without running the code, or if the code did not copy correctly, press **Ctrl**+**C** to cancel and return to the normal MicroPython **>>>** prompt).

Example: use the time module

The time module is used for time-sensitive operations such as introducing a delay in your routine or a timer.

The following time functions are supported by the XBee® BLU:

- **ticks_ms()** returns the current millisecond counter value. This counter rolls over at 0x40000000.
- **ticks_diff()** compares the difference between two timestamps in milliseconds.
- **sleep()** delays operation for a set number of seconds.
- **sleep_ms()** delays operation for a set number of milliseconds.
- **sleep_us()** delays operation for a set number of microseconds.

> **Note** The standard **time.time()** function cannot be used, because this function produces the number of seconds since the epoch. The XBee module lacks a realtime clock and cannot provide any date or time data.

The following example exercises the various sleep functions and uses **ticks_diff()** to measure duration:

```
import time

start = time.ticks_ms()  # Get the value from the millisecond counter

time.sleep(1)          # sleep for 1 second
time.sleep_ms(500)     # sleep for 500 milliseconds
time.sleep_us(1000)    # sleep for 1000 microseconds

delta = time.ticks_diff(time.ticks_ms(), start)

print("Operation took {} ms to execute".format(delta))
```

Example: AT commands using MicroPython

AT commands control the XBee® BLU. The "AT" is an abbreviation for "attention", and the prefix "AT" notifies the module about the start of a command line. For a list of AT commands that can be used on the XBee® BLU, see AT commands.

MicroPython provides an **atcmd()** method to process AT commands, similar to how you can use Command mode or API frames.

The **atcmd()** method accepts two parameters:

1. The two character AT command, entered as a string.
2. An optional second parameter used to set the AT command value. If this parameter is not

provided, the AT command is queried instead of being set. This value is an integer, bytes object, or string, depending on the AT command.

The following is example code that queries and sets a variety of AT commands using **xbee.atcmd()**:

```
import xbee

# Set the NI string of the radio
xbee.atcmd("NI", "XBee3 module")

# Configure a BLE power using two different data types
xbee.atcmd("BP", 2) # Hex
xbee.atcmd("BP", b'\x02') # Bytes

# Read some AT commands and display the value and data type:
print("\nAT command parameter values:")
commands =["BL", "BP", "NI", "CK"]

for cmd in commands:
 val = xbee.atcmd(cmd)
 print("{}: {:20} of type {}".format(cmd, repr(val), type(val)))
```

This example code outputs the following:

```
AT command parameter values:
BL: '0x84b4db1231d6'    of type <class 'str'>
BL: b'\x84\xb4\xdb\x121\xd6' of type <class 'bytes'>
BP: 2                   of type <class 'int'>
NI: 'XBee3 module'      of type <class 'str'>
CK: 10506               of type <class 'int'>

# Read some AT commands and display the value and data type:
print("\nAT command parameter values:")
commands =["BL", "BP", "NI", "CK"]

bl_value = xbee.atcmd("BL")
hex_bl_value = hex(int.from_bytes(bl_value, 'big'))
print("{}: {:20} of type {}".format(commands[0],
repr(hex_bl_value), type(hex_bl_value)))


for cmd in commands:
 val = xbee.atcmd(cmd)
 print("{}: {:20} of type {}".format(cmd, repr(val), type(val)))
```

Exit MicroPython mode

To exit MicroPython mode:

1. In the XCTU MicroPython terminal, click the green **Close** button  .
2. Click **Close** at the bottom of the terminal to exit the terminal.
3. In XCTU's Configuration working mode  , change **AP API Enable** to another mode and click the **Write** button  . We recommend changing to Transparent mode **[0]**, as most of the examples use this mode.

Other terminal programs

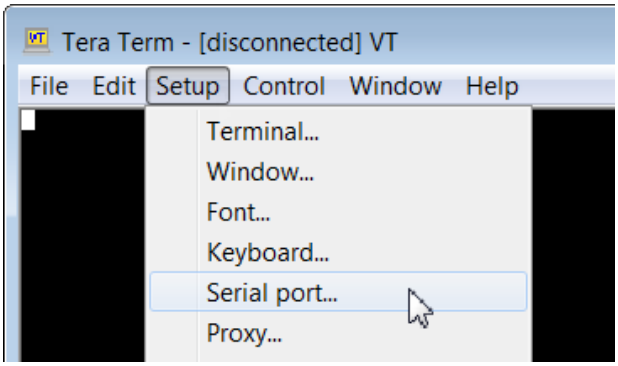
If you do not use the MicroPython terminal in XCTU, you can use other terminal programs to communicate with the XBee® BLU. If you use Microsoft Windows, follow the instructions for Tera Term; if you use Linux, follow the instructions for picocom. To download these programs:

- Tera Term for Windows, see ttssh2.osdn.jp/index.html.en.
- Picocom for Linux, see developer.ridgerun.com/wiki/index.php/Setting_up_Picocom_-_Ubuntu
- Source code and in-depth information, see github.com/npat-efault/picocom.

Tera Term for Windows

With the XBee® BLU in MicroPython mode (**AP** = **4**), you can access the MicroPython prompt using a terminal.

1. Open Tera Term. The **Tera Term: New connection** window appears.
2. Click the **Serial** radio button to select a serial connection.
3. From the **Port:** drop-down menu, select the COM port that the XBee® BLU is connected to.
4. Click **OK**. The **COMxx - Tera Term VT** terminal window appears and Tera Term attempts to connect to the device at a baud rate of 9600 bps. The terminal will not allow communication with the device since the baud rate setting is incorrect. You must change this rate as it was previously set to 115200 bps.
5. Click **Setup** and **Serial Port**. The **Tera Term: Serial port setup** window appears.



6. In the **Tera Term: Serial port setup** window, set the parameters to the following values:
   - **Port**: Shows the port that the XBee® BLU is connected on.
   - **Baud rate**: 115200
   - **Data**: 8 bit
   - **Parity**: none
   - **Stop**: 1 bit
   - **Flow control**: hardware
   - **Transmit delay**: N/A
7. Click **OK** to apply the changes to the serial port settings. The settings should go into effect right away.

8. To verify that local echo is not enabled and that extra line-feeds are not enabled:
   a. In Tera Term, click **Setup** and select **Terminal**.
   b. In the **New-line** area of the **Tera Term: Serial port setup** window, click the **Receive** drop-down menu and select **AUTO** if it does not already show that value.
   c. Make sure the **Local echo** box is not checked.
9. Click **OK**.
10. Press **Ctrl**+**B** to get the MicroPython version banner and prompt.

```
MicroPython v1.20.0-1829-gcf5c2e9fb on 2023-07-20; XBee BLE with EFR32MG
Type "help()" for more information.
>>>
```

Now you can type MicroPython commands at the **>>>** prompt.

Use picocom in Linux

With the XBee® BLU in MicroPython mode (**AP** = **4**), you can access the MicroPython prompt using a terminal.

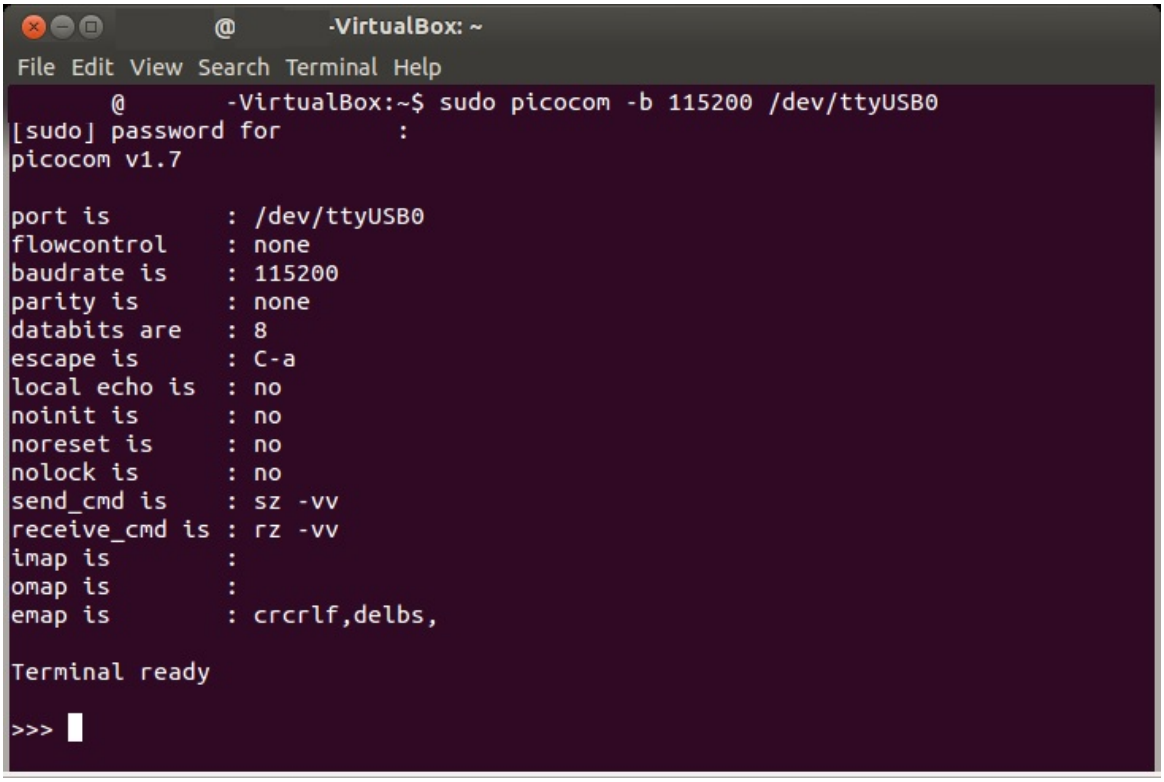
Note The user must have read and write permission for the serial port the XBee® BLU is connected to in order to communicate with the device.

1. Open a terminal in Linux and type **picocom -b 115200 /dev/ttyUSB0**. This assumes you have no other USB-to-serial devices attached to the system.
2. Press **Ctrl**+**B** to get the MicroPython version banner and prompt. You can also press **Enter** to bring up the prompt.

If you do have other USB-to-serial devices attached:

1. Before attaching the XBee® BLU, check the directory **/dev/** for any devices named **ttyUSBx**, where **x** is a number. An easy way to list these is to type: **ls /dev/ttyUSB***. This produces a list of any device with a name that starts with **ttyUSB**.
2. Take note of the devices present with that name, and then connect the XBee® BLU.
3. Check the directory again and you should see one additional device, which is the XBee® BLU.
4. In this case, replace **/dev/ttyUSB0** at the top with **/dev/ttyUSB<number>**, where **<number>** is the new number that appeared.

   It connects and shows "Terminal ready".



You can now type MicroPython commands at the **>>>** prompt.

Micropython help ()

When you type the **help()** command at the prompt, it provides a link to online help, control commands and also usage examples.

```
>>> help()
Welcome to MicroPython!
For online docs please visit http://docs.micropython.org/.
Control commands:
CTRL-A -- on a blank line, enter raw REPL mode
CTRL-B -- on a blank line, enter normal REPL mode
CTRL-C -- interrupt a running program
CTRL-D -- on a blank line, reset the REPL
CTRL-E -- on a blank line, enter paste mode
CTRL-F -- on a blank line, enter flash upload mode
For further help on a specific object, type help(obj)
For a list of available modules, type help('modules')
------------------------------------------------------
------------------------------------------------------
```

When you type **help('modules')** at the prompt, it displays all available Micropython modules.

```
------------------------------------------------------
>>> help("modules")
__main__ micropython uhashlib ustruct
ble uarray uio usys
builtins ubinascii ujson utime
```

```
digi            ucryptolib      umachine    xbee
gc              uerrno          uos

Plus any modules on the filesystem

---------------------------------------------------------
```

When you import a module and type **help()** with the module as the object, you can query all the functions that the object supports.

```
>>> import sys
>>> help(sys)
object <module 'sys'> is of type module
__name__ -- sys
path -- ['.frozen', '', '/flash', '/flash/lib']
argv -- ['']
version -- 3.4.0; MicroPython v1.20.0-1829-gcf5c2e9fb on 2023-07-20
version_info -- (3, 4, 0)
implementation -- ('micropython', (1, 20, 0), 'XBee BLE with EFR32MG', 262)
platform -- xbee-blu
byteorder -- little
maxsize -- 2147483647
exit -- <function>
stdin -- <io.FileIO 0>
stdout -- <io.FileIO 1>
stderr -- <io.FileIO 2>
modules -- {}
print_exception -- <function>
```

Serial communication

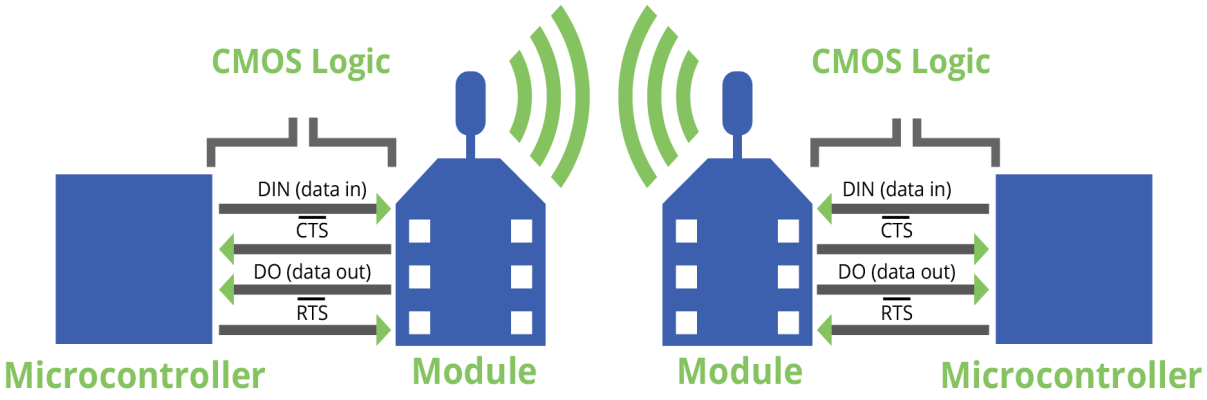
Serial interface

The XBee® BLU interfaces to a host device through a serial port. The device can communicate through its serial port:

- Through logic and voltage compatible universal asynchronous receiver/transmitter (UART).
- Through a level translator to any serial device, for example through an RS-232 or USB interface board.
- Through SPI, as described in SPI communications.

UART data flow

Devices that have a UART interface connect directly to the pins of the XBee® BLU as shown in the following figure. The figure shows system data flow in a UART-interfaced environment. Low-asserted signals have a horizontal line over the signal name.

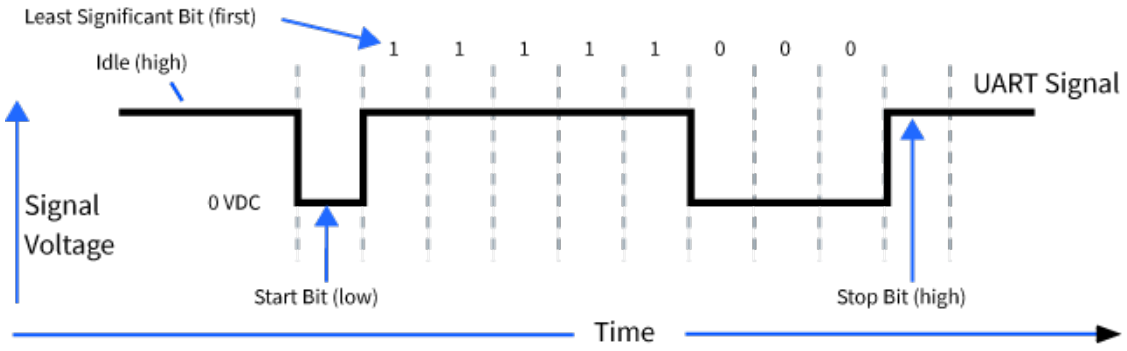


Serial data

A device sends data to the XBee® BLU's UART as an asynchronous serial signal. When the device is not transmitting data, the signals should idle high.

For serial communication to occur, you must configure the UART of both devices (the microcontroller and the XBee® BLU) with compatible settings for the baud rate, parity, start bits, stop bits, and data bits.

Each data byte consists of a start bit (low), 8 data bits (least significant bit first) and a stop bit (high). The following diagram illustrates the serial bit pattern of data passing through the device. The diagram shows UART data packet 0x1F (decimal number 31) as transmitted through the device.

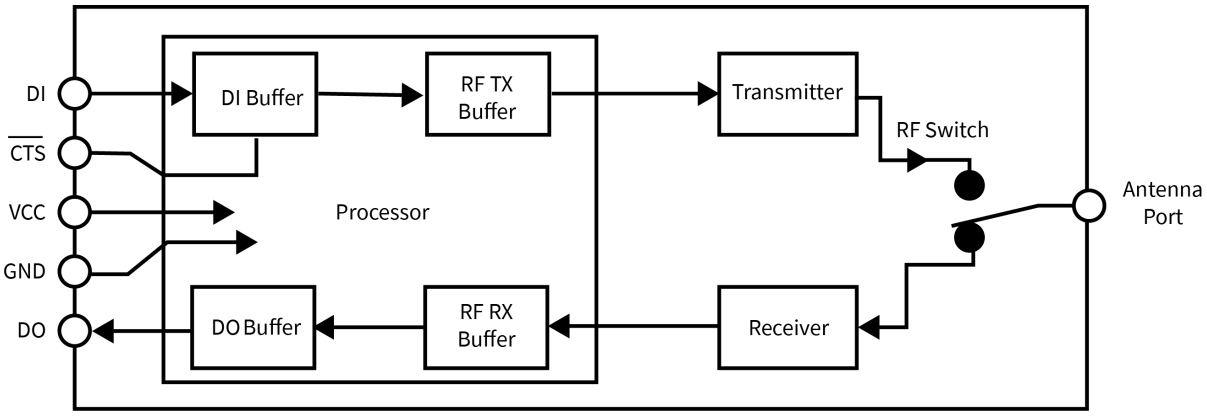


You can configure the UART baud rate, parity, and stop bits settings on the device with the **BD**, **NB**, and **SB** commands respectively. For more information, see UART interface commands.

Flow control

The XBee® BLU maintains buffers to collect serial and RF data that it receives. The serial receive buffer collects incoming serial characters and holds them until the device can process them. The serial transmit buffer collects the data it receives via the RF link until it transmits that data out the serial port. The following figure shows the process of device buffers collecting received serial data.

Use D6 (DIO6/RTS Configuration) and D7 (DIO7/CTS Configuration) to set flow control.



Clear-to-send ($\overline{CTS}$) flow control

If you enable $\overline{CTS}$ flow control (D7 (DIO7/CTS Configuration)), when the serial receive buffer is more than **FT** bytes full, the device de-asserts $\overline{CTS}$ (sets it high) to signal to the host device to stop sending serial data. The device reasserts $\overline{CTS}$ after the serial receive buffer has less than **FT** bytes in it. See FT (Flow Control Threshold) to configure and read this threshold.

$\overline{RTS}$ flow control

If you set D6 (DIO6/RTS Configuration) to enable $\overline{RTS}$ flow control, the device does not send data in the serial transmit buffer out the DOUT pin as long as $\overline{RTS}$ is de-asserted (set high). Do not de-assert $\overline{RTS}$ for long periods of time or the serial transmit buffer will fill. If the device receives an RF data packet and the serial transmit buffer does not have enough space for all of the data bytes, it discards the entire RF data packet.

If the device sends data out the UART when $\overline{RTS}$ is de-asserted (set high) the device could send up to five characters out the UART port after $\overline{RTS}$ is de-asserted.

SPI operation

This section specifies how SPI is implemented on the device, what the SPI signals are, and how full duplex operations work.

SPI communications

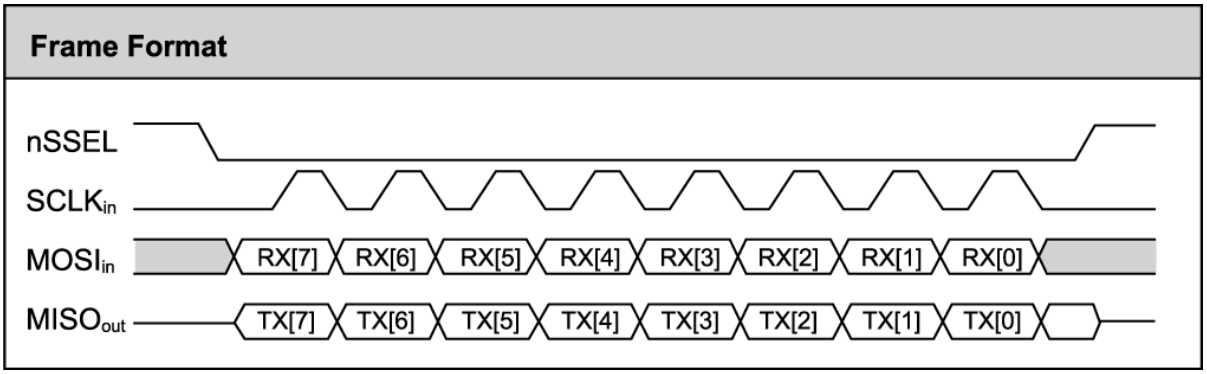
The XBee® BLU supports SPI communications in slave mode. Slave mode receives the clock signal and data from the master and returns data to the master. The following table shows the signals that the SPI port uses on the device.

Signal	Direction	Function
SPI_MOSI (Master Out, Slave In)	Input	Inputs serial data from the master
SPI_MISO (Master In, Slave Out)	Output	Outputs serial data to the master
SPI_SCLK (Serial Clock)	Input	Clocks data transfers on MOSI and MISO
SPI_$\overline{\text{SSEL}}$ (Slave Select)	Input	Enables serial communication with the slave
SPI_$\overline{\text{ATTN}}$ (Attention)	Output	Alerts the master that slave has data queued to send. The XBee® BLU asserts this pin as soon as data is available to send to the SPI master and it remains asserted until the SPI master has clocked out all available data.

In this mode:

- SPI clock rates up to 5 MHz (burst) are possible.
- Data transmission format is most significant bit (MSB) first; bit 7 is the first bit of a byte sent over the interface.
- Frame Format mode 0 is used. This means CPOL= 0 (idle clock is low) and CPHA = 0 (data is sampled on the clock's leading edge).
- The SPI port only supports API Mode (**AP** = 1).

The following diagram shows frame format mode 0 for SPI communications.



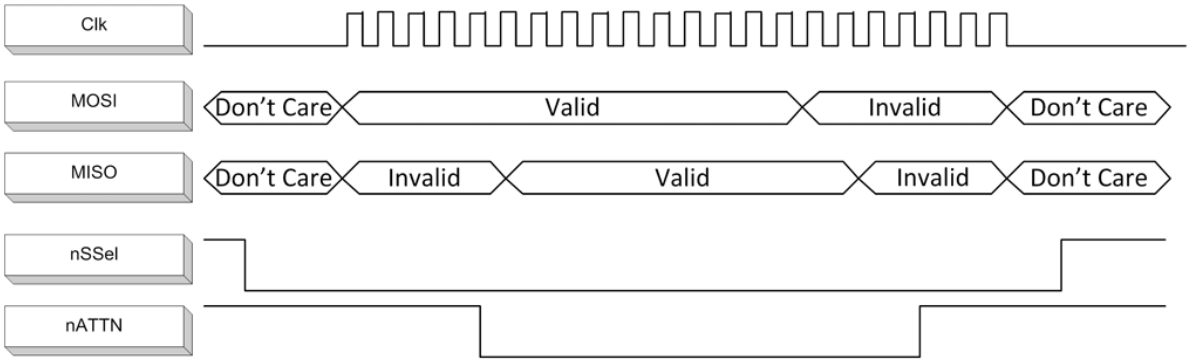
SPI mode is chip to chip communication. We do not supply a SPI communication interface on the XBee development evaluation boards included in the development kit.

Full duplex operation

When using SPI on the XBee® BLU the device uses API operation without escaped characters to packetize data. The device ignores **AP** configuration because SPI does not operate in any other mode. SPI is a full duplex protocol, even when data is only available in one direction. This means that whenever a device receives data, it also transmits, and that data is normally invalid. Likewise, whenever a device transmits data, invalid data is probably received. To determine whether or not received data is invalid, the firmware places the data in API packets.

SPI allows for valid data from the slave to begin before, at the same time, or after valid data begins from the master. When the master sends data to the slave and the slave has valid data to send in the middle of receiving data from the master, a full duplex operation occurs, where data is valid in both directions for a period of time. Not only must the master and the slave both be able to keep up with the full duplex operation, but both sides must honor the protocol.

The following figure illustrates the SPI interface while valid data is being sent in both directions.



Low power operation

Sleep modes generally work the same on SPI as they do on UART. However, the addition of SPI mode provides an option to configure another pin as a sleep pin.

By default, Digi configures DIO8 (SLEEP_REQUEST) as a peripheral and during pin sleep it wakes the device and puts it to sleep. This applies to both the UART and SPI serial interfaces.

If SLEEP_REQUEST is not configured as a peripheral and SPI_SSEL is configured as a peripheral, then pin sleep is controlled by SPI_SSEL rather than by SLEEP_REQUEST. Asserting SPI_SSEL by driving it low either wakes the device or keeps it awake. Negating SPI_SSEL by driving it high puts the device to sleep.

SPI_SSELcan be configured to both control sleep and to indicate that the SPI master has selected a particular slave device. This configuration provides an advantage where the pin sleep implementation on SPI mode requires one less physical pin. It does have the disadvantage that it puts the device to sleep whenever the SPI master unintentionally negates SPI_SSEL.

To effectively use the pin sharing configuration, the user/design must have control of the SPI_SSELpin to the extent that it can control pin sleep. This makes the SLEEP_REQUEST pin available for a different purpose. Without control of SPI_SSEL while using it for sleep request, the device may go to sleep at inopportune times.

If the device is one of multiple slaves on the SPI, then the device sleeps while the SPI master talks to the other slave, but this is acceptable in most cases.

If you do not configure either pin as a peripheral, then the device stays awake, being unable to sleep in **SM**1 mode.

Select the SPI port

To force SPI mode on through-hole devices, hold DOUT/DIO13 low while resetting the device until SPI_ATTN asserts. This causes the device to disable the UART and go straight into SPI communication mode. Once configuration is complete, the device queues a modem status frame to the SPI port, which causes the SPI_ATTN line to assert. The host can use this to determine that the SPI port is configured properly.

On surface-mount devices, forcing DOUT low at the time of reset has no effect. To use SPI mode on the SMT modules, assert the SPI_SSEL low after reset and before any UART data is input.

Forcing DOUT low on TH devices forces the device to enable SPI support by setting the following configuration values to 1 (peripheral):

Through-hole	Micro and Surface-mount	SPI signal
D1 (DIO1/ADC1/TH_SPI_ATTN Configuration)	P9 (DIO19/SPI_ATTN Configuration)	ATTN
D2 (DIO2/ADC2/TH_SPI_CLK Configuration)	P8 (DIO18/SPI_CLK Configuration)	SCLK
D3 (DIO3/ADC3/TH_SPI_SSEL Configuration)	P7 (DIO17/SPI_SSEL Configuration)	SSEL
D4 (DIO4/TH_SPI_MOSI Configuration)	P6 (DIO16/SPI_MOSI Configuration)	MOSI
P2 (DIO12/TH_SPI_MISO Configuration)	P5 (DIO15/SPI_MISO Configuration)	MISO

Note The ATTN signal is optional–you can still use SPI mode if you disable the SPI_ATTN pin (**D1** on through-hole or **P9** on surface-mount devices).

As long as the host does not issue a **WR** command, these configuration values revert to previous values after a power-on reset. If the host issues a **WR** command while in SPI mode, these same parameters are written to flash, and after a reset the device continues to operate in SPI mode.

If the UART is disabled and the SPI is enabled in the written configuration, then the device comes up in SPI mode without forcing it by holding DOUT low. If both the UART and the SPI are configured (P3 (DIO13/UART_DOUT) through P9 (DIO19/SPI_ATTN Configuration) are set to 1) at the time of reset, then output goes to the UART until the host sends the first input to the SPI interface. As soon as the first input comes on the SPI port, then all subsequent output goes to the SPI port and the UART is disabled.

After the first input arrives on the SPI port, all subsequent output goes to the SPI port and the UART is disabled.

When the master asserts the slave select (SPI_SSEL) signal, SPI transmit data is driven to the output pin SPI_MISO, and SPI data is received from the input pin SPI_MOSI. The SPI_SSEL pin has to be asserted to enable the transmit serializer to drive data to the output signal SPI_MISO. A rising edge on SPI_SSEL causes the SPI_MISO line to be tri-stated such that another slave device can drive it, if so desired.

If the output buffer is empty, the SPI serializer transmits the last valid bit repeatedly, which may be either high or low. Otherwise, the device formats all output in API mode 1 format, as described in Operate in API mode. The attached host is expected to ignore all data that is not part of a formatted API frame.

Force UART operation

If you configure a device with only the SPI enabled and no SPI master is available to access the SPI slave port, you can recover the device to UART operation by holding DIN / CONFIG low at reset time. DIN/CONFIG forces a default configuration on the UART at 9600 baud and brings up the device in Command mode on the UART port. You can then send the appropriate commands to the device to configure it for UART operation. If you write those parameters, the device comes up with the UART enabled on the next reset.

Modes

API operating mode

API operating mode is an alternative to Transparent operating mode. API mode is a frame-based protocol that allows you to direct data on a packet basis. The device transmits and receives UART or SPI data in packets, also known as API frames. This mode allows for structured communications with computers and microcontrollers.

The advantages of API operating mode include:

Command mode

Enter Command mode

When using the default configuration values for GT (Guard Time) and CT (Command Mode Timeout), you must enter **+++** preceded and followed by one second of silence—no input—to enter Command mode. However, both **GT** and **CC** are configurable. This means that the silence before and after the escape sequence—**GT**—and the escape characters themselves—**CC**—can be changed. For example, if **GT** is **5DC** and **CC** is **31**, then Command mode can be entered by typing **111** preceded and followed by 1.5 seconds of silence. When the entrance criteria are met the device responds with **OK\r** on UART signifying that it has entered Command mode successfully and is ready to start processing AT commands.

Note Do not press **Return** or **Enter** after typing **+++** because it interrupts the guard time silence and prevents you from entering Command mode.

When the device is in Command mode, it listens for user input and is able to receive AT commands on the UART. If **CT** time (default is 10 seconds) passes without any user input, the device drops out of Command mode and returns to the previous operating mode. You can force the device to leave Command mode by sending CN (Exit Command Mode).

You can customize the command character, the guard times and the timeout in the device's configuration settings. For more information, see CC (Command Character), CT (Command Mode Timeout) and GT (Guard Time).

Troubleshooting

Failure to enter Command mode is often due to baud rate mismatch. Ensure that the baud rate of the connection matches the baud rate of the device. By default, BD (UART Baud Rate) = **3** (9600 b/s).

There are two alternative ways to enter Command mode:

- A serial break for six seconds enters Command mode. You can issue the "break" command from a serial console, it is often a button or menu item.
- Asserting DIN (serial break) upon power up or reset enters Command mode. XCTU guides you through a reset and automatically issues the break when needed.

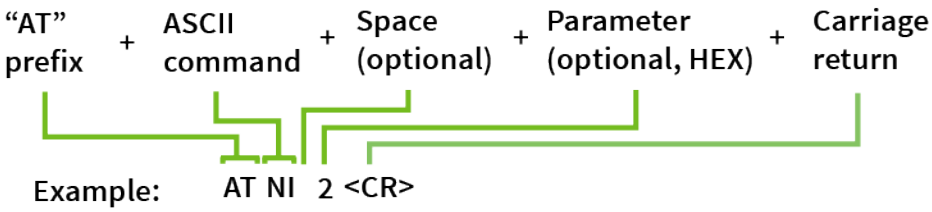
Note You must assert $\overline{\text{RTS}}$ for both of these methods, otherwise the device enters the bootloader.

Both of these methods temporarily set the device's baud rate to 9600 and return an **OK** on the UART to indicate that Command mode is active. When Command mode exits, the device returns to normal operation at the baud rate that **BD** is set to.

Send AT commands

Once the device enters Command mode, use the syntax in the following figure to send AT commands. Every AT command starts with the letters **AT**, which stands for "attention." The AT is followed by two characters that indicate which command is being issued, then by some optional configuration values.

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



The preceding example changes NI (Network Identifier) to **2**.

Multiple AT commands

You can send multiple AT commands at a time when they are separated by a comma in Command mode; for example, **ATNIMy XBee,AC<cr>**.

Note The behavior of the comma is the same as the behavior of the <CR> in the previous example except that the next command following the comma is not preceded by AT. The only real purpose of the comma is to reduce keystrokes.

The preceding example changes the **NI (Node Identifier)** to **My XBee** and makes the setting active through AC (Apply Changes).

Parameter format

Refer to the list of AT commands for the format of individual AT command parameters. Valid formats for hexidecimal values include with or without a leading **0x** for example **FFFF** or **0xFFFF**.

Response to AT commands

When using AT commands to set parameters the XBee® BLU responds with **OK<cr>** if successful and **ERROR<cr>** if not.

Apply command changes

Any changes you make to the configuration command registers using AT commands do not take effect until you apply the changes. For example, if you send the **BD** command to change the baud rate, the actual baud rate does not change until you apply the changes. To apply changes:

1. Send AC (Apply Changes).
2. Send WR (Write). In this case, changes are only applied following a reset. The **WR** command by itself does not apply changes.
   or:
3. Exit Command mode. You can exit Command mode in two ways: Either enter the **CN** command or wait for Command mode to timeout as specified by the **CT** parameter.

Make command changes permanent

Send a WR (Write) command to save the changes. **WR** writes parameter values to non-volatile memory so that parameter modifications persist through subsequent resets.

Send an RE (Restore Defaults) followed by **WR** to restore parameters back to their factory defaults. The next time the device is reset the default settings are applied.

Exit Command mode

1. Send CN (Exit Command Mode) followed by a carriage return.
   or:
2. If the device does not receive any valid AT commands within the time specified by CT (Command Mode Timeout), it returns to Transparent or API mode. The default Command mode timeout is 10 seconds.

For an example of programming the device using AT Commands and descriptions of each configurable parameter, see AT commands.

I/O support

The following topics describe analog and digital I/O line support and output control.

Digital I/O support

Digital I/O is available on lines DIO0 through DIO9 (D0 (DIO0/ADC0/Commissioning Configuration) - D9 (DIO9/ON_SLEEP Configuration)) and DIO12 through DIO19 (P2 (DIO12/TH_SPI_MISO Configuration) - P9 (DIO19/SPI_ATTN Configuration)).

Function	MMT Pin	SMT Pin	TH Pin	AT Command
DIO0	31	33	20	D0 (DIO0/ADC0/Commissioning Configuration)
DIO1	30	32	19	D1 (DIO1/ADC1/TH_SPI_ATTN Configuration)
DIO2	29	31	18	D2 (DIO2/ADC2/TH_SPI_CLK Configuration)
DIO3	28	30	17	D3 (DIO3/ADC3/TH_SPI_SSEL Configuration)
DIO4	23	24	11	D4 (DIO4/TH_SPI_MOSI Configuration)
DIO5	26	28	15	D5 (DIO5/Associate Configuration)
DIO6	27	29	16	D6 (DIO6/RTS Configuration)
DIO7	24	25	12	D7 (DIO7/CTS Configuration)
DIO8	9	10	9	D8 (DIO8/DTR/SLP_Request Configuration)
DIO9	25	26	13	D9 (DIO9/ON_SLEEP Configuration)
DIO12	5	5	4	P2 (DIO12/TH_SPI_MISO Configuration)
DIO13	3	3	2	P3 (DIO13/UART_DOUT Configuration)
DIO14	4	4	3	P4 (DIO14/UART_DIN Configuration)
DIO15	16	17	-	P5 (DIO15/SPI_MISO Configuration)
DIO16	15	16	-	P6 (DIO16/SPI_MOSI Configuration)
DIO17	14	15	-	P7 (DIO17/SPI_SSEL Configuration)
DIO18	13	14	-	P8 (DIO18/SPI_CLK Configuration)
DIO19	11	12	-	P9 (DIO19/SPI_ATTN Configuration)

Digital sampling is enabled on these pins if configured as 3, 4, or 5 with the following meanings:

- 3 is digital input.
  - Use PR (Pull-up/Down Resistor Enable) to enable internal pull up/down resistors for each digital input. Use PD (Pull Up/Down Direction) to determine the direction of the internal pull up/down resistor. All disabled and digital input pins are pulled up by default.
- 4 is digital output low.
- 5 is digital output high.

Analog I/O support

Analog input is available on **D0** through **D3**. Configure these pins to **2** (ADC) to enable analog sampling.

Function	MMT Pin	SMT Pin	TH Pin	AT Command
ADC0	31	33	20	D0 (DIO0/ADC0/Commissioning Configuration)
ADC1	30	32	19	D1 (DIO1/ADC1/TH_SPI_ATTN Configuration)
ADC2	29	31	18	D2 (DIO2/ADC2/TH_SPI_CLK Configuration)
ADC3	28	30	17	D3 (DIO3/ADC3/TH_SPI_SSEL Configuration)

AV (Analog Voltage Reference) specifies the analog reference voltage used for the 10-bit ADCs. Analog sample data is represented as a 2-byte value. For a 10-bit ADC, the acceptable range is from **0x0000** to **0x03FF**. To convert this value to a useful voltage level, apply the following formula:

ADC / 1023 (vREF) = Voltage

Example

An ADC value received is 0x01AE; to convert this into a voltage the hexadecimal value is first converted to decimal (0x01AE = 430). Using the default **AV** reference of 1.25 V, apply the formula as follows:

430 / 1023 (1.25 V) = 525 mV

I/O behavior during sleep

When the device sleeps (**SM !** = **0**) the I/O lines are optimized for a minimal sleep current.

Digital I/O lines

Digital I/O lines set as digital output high or low maintain those values during sleep. Disabled or input pins continue to be controlled by the **PR**/**PD** settings. Peripheral pins (with the exception of $\overline{\text{CTS}}$) are set low during sleep and SPI pins are set high. Peripheral and SPI pins resume normal operation upon wake.

Sleep support

Sleep is implemented to support installations where a mains power source is not available and a battery is required. In order to increase battery life, the device sleeps, which means it stops operating. It can be woken by a pin.

Sleep pins

The following table describes the five external device pins associated with sleep.

The only sleep mode supported by this device is pin sleep. This means that the sleep state is controlled by a pin. Normally, this is the **SLEEP_REQ** pin, but **DIO0** may also be used to awaken the device, if it is configured as the commissioning button. A third pin to control sleep is the **SPI_SSEL** pin.

Pin name	Description
$\overline{\text{DTR}}$ /SLEEP_RQ	For **SM** = **1**, high puts the device to sleep and low wakes it up.
SPI_$\overline{\text{SSEL}}$	This pin operates the same as SLEEP_RQ when **D8** is **0**.
$\overline{\text{CTS}}$	If **D7** = **1**, high indicates that the device is asleep and low indicates that it is awake and ready to receive serial data.
ON_$\overline{\text{SLEEP}}$	Low indicates that the device is asleep and high indicates that it is awake and ready to receive serial data.
DIO0	When configured as a peripheral (1), this is a commissioning button. In this default condition, DIO0 can also awaken a device from pin sleep.

Sleep conditions

Since instructions stop executing while the device is sleeping, it is important to avoid sleeping when the device has work to do. For example, the device will not sleep if any of the following are true:

1. The device is operating in Command mode, or in the process of getting into Command mode with the **+++** sequence.
2. The device is processing AT commands from API mode
3. Something is queued to the serial port and that data is not blocked by $\overline{\text{RTS}}$ flow control

If each of the above conditions are false, then sleep may still be blocked in these cases:

1. Enough time has not expired since the device has awakened.
   a. If the device is operating in pin sleep, the amount of time needed for one character to be received on the UART is enough time.
2. Sleep Request pin is not asserted when operating in pin sleep mode

General Purpose Flash Memory

General Purpose Flash Memory

XBee® BLU provides blocks of flash memory that an application can read and write to. This memory provides a non-volatile data storage area that an application uses for many purposes. Some common uses of this data storage include:

- Storing logged sensor data
- Buffering firmware update data for a host microcontroller
- Storing and retrieving data tables needed for calculations performed by a host microcontroller

The General Purpose Memory (GPM) is also used to store a firmware update file for over-the-air firmware updates of the device itself.

The usage of sleep during a GPM update is unsupported. Users are recommended to turn off sleep on the target device, perform the update, and then switch sleep back on to avoid data loss and increase the update speed.

Access General Purpose Flash Memory

Byte offset in payload	Number of bytes	Field name	General field description
0	1	GPM_CMD_ID	Specific GPM commands are described in detail in the topics that follow.
1	1	GPM_OPTIONS	Command-specific options.
2	2*	GPM_BLOCK_NUM	The block number addressed in the GPM.
4	2*	GPM_START_INDEX	The byte index within the addressed GPM block.
6	2*	GPM_NUM_BYTES	The number of bytes in the GPM_DATA field, or in the case of a READ, the number of bytes requested.
8	varies	GPM_DATA	
* Specify multi-byte parameters with big-endian byte ordering.			

When a device sends a GPM command to another device via a unicast, the receiving device sends a unicast response back to the requesting device's source endpoint specified in the request packet. It does not send a response for broadcast requests. If the source endpoint is set to the DIGI_DEVICE endpoint (0xE6) or Explicit API mode is enabled on the requesting device, then the requesting node outputs a GPM response as an explicit API RX indicator frame (assuming it has API mode enabled).

The format of the response is similar to the request packet:

Byte offset in payload	Number of bytes	Field name	General field description
0	1	GPM_CMD_ID	This field is the same as the request field.
1	1	GPM_STATUS	Status indicating whether the command was successful.
2	2*	GPM_BLOCK_NUM	The block number addressed in the GPM.
4	2*	GPM_START_INDEX	The byte index within the addressed GPM block.
6	2*	GPM_NUM_BYTES	The number of bytes in the GPM_DATA field.
8	varies	GPM_DATA	
* Specify multi-byte parameters with big-endian byte ordering.			

General Purpose Flash Memory commands

This section provides information about commands that interact with GPM:

PLATFORM_INFO_REQUEST (0x00)

A PLATFORM_INFO_REQUEST frame can be sent to query details of the GPM structure.

Field name	Command-specific description
GPM_CMD_ID	Should be set to PLATFORM_INFO_REQUEST (0x00).
GPM_OPTIONS	This field is unused for this command. Set to 0.
GPM_BLOCK_NUM	This field is unused for this command. Set to 0.
GPM_START_INDEX	This field is unused for this command. Set to 0.
GPM_NUM_BYTES	This field is unused for this command. Set to 0.
GPM_DATA	No data bytes should be specified for this command.

PLATFORM_INFO (0x80)

When a PLATFORM_INFO_REQUEST command request has been unicast to a node, that node sends a response in the following format to the source endpoint specified in the requesting frame.

Field name	Command-specific description
GPM_CMD_ID	Should be set to PLATFORM_INFO (0x80).
GPM_STATUS	Indicates success if 0. Otherwise, an error occurred (see Possible Errors Returned from GPM Commands).

Field name	Command-specific description
GPM_BLOCK_NUM	Indicates the number of GPM blocks available.
GPM_START_INDEX	Indicates the size, in bytes, of a GPM block.
GPM_NUM_BYTES	The number of bytes in the GPM_DATA field. For this command, this field will be set to 0.
GPM_DATA	No data bytes are specified for this command.

Example

A PLATFORM_INFO_REQUEST sent to a device with a serial number of 0x0013a200407402AC should be formatted as follows (spaces added to delineate fields):

7E 001C 11 01 0013A200407402AC FFFE E6 E6 0023 C105 00 00 00 00 0000 0000 0000 24

Assuming all transmissions were successful, the following API packets would be output the source node's serial interface:

7E 0007 8B 01 FFFE 00 00 00 76

7E 001A 91 0013A200407402AC FFFE E6 E6 0023 C105 C1 80 00 0077 0200 0000 EB

ERASE (0x01)

The ERASE command erases (writes all bits to binary 1) one or all of the GPM flash blocks. You can also use the ERASE command to erase all blocks of the GPM by setting the GPM_NUM_ BYTES field to 0.

Field name	Command-specific description
GPM_CMD_ID	Should be set to ERASE (0x01).
GPM_OPTIONS	There are currently no options defined for the ERASE command. Set this field to 0.
GPM_BLOCK_NUM	Set to the index of the GPM block that should be erased. When erasing all GPM blocks, this field is ignored (set to 0).
GPM_START_INDEX	The ERASE command only works on complete GPM blocks. The command cannot be used to erase part of a GPM block. For this reason GPM_START_INDEX is unused (set to 0).
GPM_NUM_BYTES	Setting GPM_NUM_BYTES to 0 has a special meaning. It indicates that every flash block in the GPM should be erased (not just the one specified with GPM_BLOCK_NUM). In all other cases, the GPM_NUM_BYTES field should be set to the GPM flash block size.
GPM_DATA	No data bytes are specified for this command.

ERASE_RESPONSE (0x81)

When an ERASE command request has been unicast to a node, that node sends a response in the following format to the source endpoint specified in the requesting frame.

Field name	Command-specific description
GPM_CMD_ID	Should be set to ERASE_RESPONSE (0x81).
GPM_STATUS	Indicates success if 0. Otherwise, an error occurred (see Possible Errors Returned from GPM Commands).
GPM_BLOCK_NUM	Matches the parameter passed in the request frame.
GPM_START_INDEX	Matches the parameter passed in the request frame.
GPM_NUM_BYTES	The number of bytes in the GPM_DATA field. For this command, this field will be set to 0.
GPM_DATA	No data bytes are specified for this command.

Example

To erase flash block 42 of a target radio with serial number of 0x0013a200407402ac format an ERASE packet as follows (spaces added to delineate fields):

Assuming all transmissions were successful, the following API packets would be output the source node's serial interface:

7E 0007 8B 01 FFFE 00 00 00 76

7E 001A 91 0013A200407402AC FFFE E6 E6 0023 C105 C1 81 00 002A 0000 0000 39

WRITE (0x02) and ERASE_THEN_WRITE (0x03)

The WRITE command writes the specified bytes to the GPM location specified. Before writing bytes to a GPM block it is important that the bytes have been erased previously. The ERASE_THEN_WRITE command performs an ERASE of the entire GPM block specified with the GPM_BLOCK_NUM field prior to doing a WRITE. WRITE commands cannot index past the end of a GPM block boundary.

Field name	Command-specific description
GPM_CMD_ID	Should be set to WRITE (0x02) or ERASE_THEN_WRITE (0x03).
GPM_OPTIONS	There are currently no options defined for this command. Set this field to 0.
GPM_BLOCK_NUM	Set to the index of the GPM block that should be written.
GPM_START_INDEX	Set to the byte index within the GPM block where the given data should be written.
GPM_NUM_BYTES	Set to the number of bytes specified in the GPM_DATA field. Only one GPM block can be operated on per command. For this reason, GPM_START_INDEX + GPM_NUM_BYTES cannot be greater than the GPM block size. The number of bytes sent in an explicit API frame (including the GPM command fields) cannot exceed the maximum payload size of the device. The maximum payload size can be queried with the **NP** command.
GPM_DATA	The data to be written.

WRITE _RESPONSE (0x82) and ERASE_THEN_WRITE_ RESPONSE (0x83)

When a WRITE or ERASE_THEN_WRITE command request has been unicast to a node, that node sends a response in the following format to the source endpoint specified in the requesting frame.

Field name	Command-specific description
GPM_CMD_ID	Should be set to WRITE_RESPONSE (0x82) or ERASE_THEN_ WRITE_RESPONSE (0x83)
GPM_STATUS	Indicates success if 0. Otherwise, an error occurred (see Possible Errors Returned from GPM Commands).
GPM_BLOCK_NUM	Matches the parameter passed in the request frame
GPM_START_INDEX	Matches the parameter passed in the request frame
GPM_NUM_BYTES	The number of bytes in the GPM_DATA field. For this command, this field will be set to 0
GPM_DATA	No data bytes are specified for these commands

Example

To write 15 bytes of incrementing data to flash block 22 of a target radio with serial number of 0x0013a200407402ac a WRITE packet should be formatted as follows (spaces added to delineate fields):

7E 002B 11 01 0013A200407402AC FFFE E6 E6 0023 C105 00 C0 02 00 0016 0000 000F 0102030405060708090A0B0C0D0E0F C5

Assuming all transmissions were successful and that flash block 22 was previously erased, the following API packets would be output the source node's serial interface:

7E 0007 8B 01 FFFE 00 00 00 76

READ (0x04)

You can use the READ command to read the specified number of bytes from the GPM location specified. Data can be queried from only one GPM block per command.

Field name	Command-specific description
GPM_CMD_ID	Should be set to READ (0x04).
GPM_OPTIONS	There are currently no options defined for this command. Set this field to 0.
GPM_BLOCK_NUM	Set to the index of the GPM block that should be read.
GPM_START_INDEX	Set to the byte index within the GPM block where the given data should be read.
GPM_NUM_BYTES	Set to the number of data bytes to be read. Only one GPM block

Field name	Command-specific description
	can be operated on per command. For this reason, GPM_START_INDEX + GPM_NUM_BYTES cannot be greater than the GPM block size. The number of bytes sent in an explicit API frame (including the GPM command fields) cannot exceed the maximum payload size of the device. You can query the maximum payload size with the **NP** AT command.
GPM_DATA	No data bytes should be specified for this command.

READ_RESPONSE (0x84)

When a READ command request has been unicast to a node, that node sends a response in the following format to the source endpoint specified in the requesting frame.

Field name	Command-specific description
GPM_CMD_ID	Should be set to READ_RESPONSE (0x84).
GPM_STATUS	Indicates success if 0. Otherwise, an error occurred (see Possible Errors Returned from GPM Commands).
GPM_BLOCK_NUM	Matches the parameter passed in the request frame.
GPM_START_INDEX	Matches the parameter passed in the request frame.
GPM_NUM_BYTES	The number of bytes in the GPM_DATA field.
GPM_DATA	The bytes read from the GPM block specified.

Example

To read 15 bytes of previously written data from flash block 22 of a target radio with serial number of 0x0013a200407402ac a READ packet should be formatted as follows (spaces added to delineate fields):

7E 001C 11 01 0013A200407402AC FFFE E6 E6 0023 C105 00 C0 04 00 0016 0000 000F 3B

Assuming all transmissions were successful and that flash block 22 was previously written with incrementing data, the following API packets would be output the source node's serial interface:

7E 0007 8B 01 FFFE 00 00 00 76

7E 0029 91 0013A200407402AC FFFE E6 E6 0023 C105 C1 84 00 0016 0000 000F 0102030405060708090A0B0C0D0E0F C3

FIRMWARE_VERIFY (0x05) and FIRMWARE_VERIFY_AND_INSTALL (0x06)

Use the FIRMWARE_VERIFY and FIRMWARE_VERIFY_AND_INSTALL commands when remotely updating firmware on a device. For more information about firmware updates , see Update the firmware over-the-air. These commands check if the GPM contains a valid over-the-air update file. For the FIRMWARE_VERIFY_AND_INSTALL command, if the GPM contains a valid firmware image, it will send a GPM response and then the device resets and begins using the new firmware.

Field name	Command-specific description
GPM_CMD_ID	Should be set to FIRMWARE_VERIFY (0x05) or FIRMWARE_VERIFY_AND_INSTALL (0x06)
GPM_OPTIONS	Reserved. Set to 0.
GPM_BLOCK_NUM	This field is unused for this command. Set to 0.
GPM_START_INDEX	This field is unused for this command. Set to 0.
GPM_NUM_BYTES	This field is unused for this command. Set to 0.
GPM_DATA	This field is unused for this command

Note The target device will be unable to receive RF packets for a short period of time (around half a second) while verifying the firmware after receiving either of these commands.

FIRMWARE_VERIFY_RESPONSE (0x85)

When a FIRMWARE_VERIFY command request has been unicast to a node, that node sends a response in the following format to the source endpoint specified in the requesting frame.

Field name	Command-specific description
GPM_CMD_ID	Should be set to FIRMWARE_VERIFY_RESPONSE (0x85)
GPM_STATUS	Indicates success if 0. Otherwise, an error occurred (see Possible Errors Returned from GPM Commands).
GPM_BLOCK_NUM	This field is unused for this command. Set to 0.
GPM_START_INDEX	This field is unused for this command. Set to 0.
GPM_NUM_BYTES	This field is unused for this command. Set to 0.
GPM_DATA	This field is unused for this command

FIRMWARE_VERIFY _AND_INSTALL_RESPONSE (0x86)

When a FIRMWARE_VERIFY_AND_INSTALL command request has been unicast to a node, that node sends a response in the following format to the source endpoint specified in the requesting frame.

Note If the firmware image is valid, after that node sends the response the device will reset and begin using the new firmware.

Field name	Command-specific description
GPM_CMD_ID	Should be set to FIRMWARE_VERIFY_AND_INSTALL_RESPONSE (0x86).
GPM_STATUS	Indicates success if 0. Otherwise, an error occurred (see Possible

Field name	Command-specific description
	Errors Returned from GPM Commands).
GPM_BLOCK_NUM	This field is unused for this command. Set to 0.
GPM_START_INDEX	This field is unused for this command. Set to 0.
GPM_NUM_BYTES	This field is unused for this command. Set to 0.
GPM_DATA	This field is unused for this command.

Example

To verify a firmware image previously loaded into the GPM on a target device with serial number 0x0013a200407402ac, format a FIRMWARE_VERIFY packet as follows (spaces added to delineate fields):

7E 001C 11 01 0013A200407402AC FFFE E6 E6 0023 C105 00 00 05 00 0000 0000 0000 1F

Assuming all transmissions were successful and that the firmware image previously loaded into the GPM is valid, the following API packets would be output the source node's serial interface:

7E 0007 8B 01 FFFE 00 00 00 76

7E 001A 91 0013A200407402AC FFFE E6 E6 0023 C105 C1 85 00 0000 0000 0000 5F

Possible Errors Returned from GPM Commands

Below are listed possible errors that may return from sending a GPM command:

Return Code	Description
0x00	Success
General command failures	
0x01	General failure
0x02	Bad payload length
0x03	Tried to access memory block beyond the max available
0x04	Attempted to read/write across a block boundary
0x05	Attempted to read/write with a valid file system mounted
0x06	Unrecognized GPM command
0x07	GPM is currently busy executing another GPM command
Erase command failures	
0x10	Flash erase operation failed
Write command failures	
0x20	Flash write operation failed
0x21	Flash write would have created a valid FS header. Writing a file system

Return Code	Description
	into GPM is disallowed due to security concerns.
Read command failures	
0x30	Flash read operation failed
0x31	Tried to read more than can be transmitted in a single packet
0x32	Couldn't get a buffer to send read updates
Verify and install failures	
0x40	Firmware verify operation failed
0x41	The given image is not compatible with this device
0x42	The given image appears corrupted or invalid
0x50	Firmware install operation failed

Update the firmware over-the-air

The XBee® BLU supports firmware over-the-air (FOTA) updates. To perform an FOTA update on the XBee® BLU, you will need an active BLE connection and the use of the provided API GATT service. For more information, see API request characteristic. In this section, the node performing the update is considered the server and the node being updated is the client.

This section provides instruction on how to update your firmware using wired updates and over-the-air updates.

Over-the-air firmware updates

The over-the-air firmware update method provided is a robust and versatile technique that you can tailor to many different networks and applications. OTA updates are reliable and minimize disruption of normal network operations.

In the following sections, we refer to the node that will be updated as the target node. We refer to the node providing the update information as the source node. In most applications the source node is locally attached to a computer running update software.

There are three phases of the over-the-air update process:

1. Distribute the new application
2. Verify the new application
3. Install the application

Distribute the new application

The first phase of performing an over-the-air update on a device is transferring the new firmware file to the target node. Load the new firmware image in the target node's GPM prior to installation. XBee® BLUs use a a Gecko Bootloader (.gbl) file for both serial and over-the-air firmware updates. These firmware files are available on the Digi Support website and via XCTU.

Send the contents of the .gbl file to the target device using general purpose memory WRITE commands. Erase the entire GPM prior to beginning an upload of an .gbl file. The contents of the .gbl file should be stored in order in the appropriate GPM memory blocks. The number of bytes that are sent in an individual GPM WRITE frame is flexible and can be catered to the user application.

Example

The example firmware version has an .gbl file of 55,141 bytes in length. Based on network traffic, we determine that sending a 128 byte packet every 30 seconds minimizes network disruption. For this reason, you would divide and address the .gbl as follows:

GPM_BLOCK_NUM	GPM_START_INDEX	GPM_NUM_BYTES	.gbl bytes
0	0	128	0 to 127
0	128	128	128 to 255
0	256	128	256 to 383
--	--	--	--
0		128	
1	0	128	
1	128	128	
--	--	--	--
--	--	--	--
26	1536	128	54784 to 54911
26	1664	128	54912 to 55039
26	1792	101	55040 to 55140

Install the application

When the entire .gbl file is uploaded to the GPM of the target node, you can issue a FIRMWARE_VERIFY_AND_INSTALL command. Once the target receives the command it verifies the .gbl file loaded in the GPM. If it is valid, then the device installs the new firmware. This installation process can take up to eight seconds. During the installation the device is unresponsive to both serial and RF communication. To complete the installation, the target module resets. AT parameter settings which have not been written to flash using the **WR** command will be lost.

Important considerations

Write all parameters with the **WR** command before performing a firmware update.

Because explicit API Tx frames can be addressed to a local node (accessible via the SPI or UART) or a remote node (accessible over the RF port) the same process can be used to update firmware on a device in either case.

Verify the new application

For an uploaded application to function correctly, every single byte from the .gbl file must be properly transferred to the GPM. To guarantee that this is the case, GPM VERIFY functions exist to ensure that all bytes are properly in place. The FIRMWARE_VERIFY function reports whether or not the uploaded data is valid. The FIRMWARE_VERIFY_AND_INSTALL command reports if the uploaded data is invalid. If the data is valid, it begins installing the application. No installation takes place on invalid data.

AT commands

Bluetooth Low Energy (BLE) commands

The following AT commands are BLE commands.

BT (Bluetooth Enable)

BT enables or disables the Bluetooth functionality.

Parameter range

Parameter	Description
0	Bluetooth functionality is disabled.
1	Bluetooth functionality is enabled.

Default

1

BL (Bluetooth Address)

BL reports the EUI-48 Bluetooth device address. Due to standard XBee AT Command processing, leading zeroes are not included in the response when in Command mode.

Parameter range

N/A

Default

N/A

BI (Bluetooth Identifier)

A human-friendly name for the device. This is the name that will appear in bluetooth advertisement messages.

If using XBee Mobile, adjustments to the filter options will be needed if this value is populated.

Parameter range

A string of case-sensitive ASCII printable characters from 1 to 22 bytes in length.

Default

0x20 (an ASCII space character)

BP (Bluetooth Power)

Sets the power level for Bluetooth Advertisements. All other BLE transmissions are sent at 8 dBm.

Parameter range

Parameter	Description
0	-20 dBm
1	-10 dBm
2	0 dBm
3	8 dBm

Default

3 = 8 dBm

GS (GAP Scan)

A diagnostic tool to perform a scan for nearby Bluetooth advertisements. Discovered advertisements will be printed out the serial port with the following fields:

Size in bytes	Field Name	Description
6	Address	BLE MAC address that is the target of the connection
1	Address Type	Specifies if it is RANDOM or PUBLIC
1	Packet Type	The bitfield is structured in the following format: ■ Bit 0: Advertisement is connectable ■ Bits 1-7: Reserved
1	RSSI	The received signal strength of the advertisement, in -dBm.
1	Data length	Length of the payload
VAR_LEN	Data	Payload (only printable ASCII characters are displayed)

The BLE scanner offers four configurable parameters that can be set with their respective AT commands:

- DG (GAP Scan Duration): The duration value specifies the amount of time, in seconds, for which the GAP scan should run. This value determines how long the BLE device will actively scan for nearby devices
- IG (GAP Scan Interval), WG (GAP Scan Window): Use IG and WG to optionally configure the scan duty cycle. The radio will actively scan advertisements during the window duration of every scan interval period.
- FG (Advertisement Filter ID): You can apply a filter that will limit which advertisements are sent out the serial port. This filter checks the advertisements payload to determine whether it should display the advertisement or not.

Note The GS command is designed to be a quick diagnostic tool only. Some of its functionalities are limited and it is recommended to perform the scan through either an API frame or MicroPython

interface. Advantages of using other methods are longer scan durations and easier visibility of advertising payload.

Parameter range

N/A

Default

N/A

DG (GAP Scan Duration)

Sets or displays the duration of the GAP scan.

Parameter range

0x1-0x258 (x 1 s) (10 minutes)

Default

0x03 seconds

WG (GAP Scan Window)

Sets or displays the time in which the radio is actively scanning during the interval period. GAP Scan Window cannot be larger than the GAP Scan Interval.

Parameter range

0x9C4-0X270FD8F (x 1 us) (41 seconds)

Default

0X2BF2 (x 1 us) (11.25 milliseconds)

IG (GAP Scan Interval)

Sets or displays the GAP Scan Interval period used for the scan duty cycle.

Parameter range

0x9C4-0X270FD8F (x 1 us) (41 seconds)

Default

0x138800 (x 1 us) (1.28 seconds)

FG (Advertisement Data Filter)

Sets or displays the filter that will be used for the GAP scan. The filter only accepts ASCII characters. After the filter is set, the scan will only display advertisements containing the text passed as a filter. To disable the filter, the user needs to set FG back to the default value of 0x20 (an ASCII space character).

Parameter range

A string of case-sensitive ASCII printable characters from 1 to 22 bytes in length.

Default

0x20 (an ASCII space character)

$S (SRP Salt)

Note You should only use this command if you have already configured a password on the XBee device and the salt corresponds to the password.

The Secure Remote Password (SRP) Salt is a 32-bit number used to create an encrypted password for the XBee® BLU. Use the **$S** command in conjunction with the **$V**, **$W**, **$X**, and **$Y** verifiers. Together, the command and the verifiers authenticate the client for the BLE API Service without storing the XBee password on the XBee® BLU.

Configure the salt in the **$S** command. In the **$V**, **$W**, **$X**, and **$Y** verifiers, you specify the 128-byte verifier value, where each command represents 32 bytes of the total 128-byte verifier value.

Note The XBee® BLU does not allow for **0** to be valid salt. If the value is **0**, SRP is disabled and you are not able to authenticate using Bluetooth.

Parameter range

0 - FFFFFFFF

Default

0

$V, $W, $X, $Y commands (SRP Salt verifier)

Use the **$V**, **$W**, **$X**, and **$Y** verifiers in conjunction with $S (SRP Salt) to create an encrypted password for the XBee® BLU. Together, **$S** and the verifiers authenticate the client for the BLE API Service without storing the XBee password on the XBee device.

Configure the salt with the **$S** command. In the **$V**, **$W**, **$X**, and **$Y** verifiers, you specify the 128-byte verifier value, where each command represents 32 bytes of the total 128-byte verifier value.

Parameter range

0 - FFFFFFFF

Default

0

MicroPython commands

The following commands relate to using MicroPython on the XBee® BLU.

PS (Python Startup)

Sets whether or not the XBee® BLU runs the stored Python code at startup.

Range

0 - 1

Parameter	Description
0	Do not run stored Python code at startup.
1	Run stored Python code at startup.

Default

0

Sleep settings commands

The following commands enable and configure the low power sleep modes of the device.

SM (Sleep Mode)

Sets or displays the sleep mode of the device.

Parameter range

0 - 1

Parameter	Description
0	The module is always awake
1	Sleep mode is controlled by the **SLEEP_REQ** line
6	MicroPython sleep(with optional pin wake). For complete details see the Digi MicroPython Programming Guide.

Default

0

API configuration commmands

The following commands affect how API mode operates.

AP (API Enable)

Set or read the API mode setting. The device can format the RF packets it receives into API frames and sends them out the serial port.

When you enable API, you must format the serial data as API frames because Transparent operating mode is disabled.

Note Transparent mode (**AP 0**) is not available on this product.

Parameter range

1, 2, 4

Default

1

AO (API Options)

Parameter range

0 - 1

Parameter	Description
0	API Rx Indicator - 0x90, this is for standard data frames.
1	API Explicit Rx Indicator - 0x91, this is for Explicit Addressing data frames.

Default

0

NP (Maximum Packet Payload Bytes)

Parameter range

Default

N/A

UART interface commands

BD (UART Baud Rate)

This command configures the serial interface baud rate for communication between the UART port of the device and the host.

The device interprets any value between 0x4B0 and 0x0EC400 as a custom baud rate. Custom baud rates are not guaranteed and the device attempts to find the closest achievable baud rate. After setting a non-standard baud rate, query **BD** to find the actual operating baud rate before applying changes.

Parameter range

Standard baud rates: 0x0 - 0x0A

Non-standard baud rates: 0x4B0 - 0x0EC400

Parameter	Description
0x0	1200 b/s
0x1	2400 b/s
0x2	4800 b/s
0x3	9600 b/s
0x4	19200 b/s
0x5	38400 b/s

Parameter	Description
0x6	57600 b/s
0x7	115200 b/s
0x8	230,400 b/s
0x9	460,800 b/s
0xA	921,600 b/s

Default

0x03 (9600 baud)

NB (Parity)

Set or read the serial parity settings for UART communications.

The device does not actually calculate and check the parity. It only interfaces with devices at the configured parity and stop bit settings for serial error detection.

Parameter range

0 - 2

Parameter	Description
0	No parity
1	Even parity
2	Odd parity

Default

0

SB (Stop Bits)

Sets or displays the number of stop bits for UART communications.

Parameter range

0 - 1

Parameter	Description
0	One stop bit
1	Two stop bits

Default

0

FT (Flow Control Threshold)

Set or display the flow control threshold.

The device de-asserts $\overline{\text{CTS}}$ when **FT** bytes are in the UART receive buffer. It re-asserts $\overline{\text{CTS}}$ when somewhat less than **FT** bytes are in the UART receive buffer. "Somewhat less than" allows for hysteresis so that $\overline{\text{CTS}}$ is not toggling rapidly when close to **FT** bytes are in the UART receive buffer.

Parameter range

0x42 - 0x36E bytes

Default

0x2BB

AT Command options

The following commands affect how Command mode operates.

CC (Command Character)

Sets or displays the character value used to break from data mode to Command mode. The command character must be sent three times in succession while observing the minimum guard time (**GT**) of silence before and after this sequence.

The default value (**0x2B**) is the ASCII code for the plus (**+**) character. You must enter it three times within the guard time to enter Command mode. To enter Command mode, there is also a required period of silence before and after the command sequence characters of the Command mode sequence (**GT** + **CC** + **GT**). The period of silence prevents inadvertently entering Command mode. For more information, see Enter Command mode.

Parameter range

0 - 0xFF

Recommended: 0x20 - 0x7F (ASCII)

Default

0x2B (the ASCII plus character: **+**)

CT (Command Mode Timeout)

Sets or displays the Command mode timeout parameter. If the local device enters Command mode and does not receive any valid AT commands within this time period, Command mode silently exits.

Parameter range

2 - 0x1770 (x 100 ms)

Default

0x64 (10 seconds)

GT (Guard Time)

Set the required period of silence before and after the command sequence characters of the Command mode sequence, **GT** + **CC** + **GT**. The period of silence prevents inadvertently entering Command mode if a data stream in Transparent mode includes the **CC** character. For more information, see Enter Command mode.

Parameter range

0x2 - 0x6D3 (x 1 ms)

Default

0x3E8 (one second)

UART pin configuration commands

The following commands are related to pin configuration for the UART interface.

D6 (DIO6/RTS Configuration)

Sets or displays the DIO6/$\overline{\text{RTS}}$ configuration.

Parameter range

0, 1, 3 - 5

Parameter	Description
0	Disabled
1	$\overline{\text{RTS}}$ flow control
2	N/A
3	Digital input
4	Digital output, low
5	Digital output, high

Default

0

D7 (DIO7/CTS Configuration)

Sets or displays the DIO7/$\overline{\text{CTS}}$ configuration.

Parameter range

0, 1, 3 - 7

Parameter	Description
0	Disabled

Parameter	Description
1	$\overline{\text{CTS}}$ flow control
2	N/A
3	Digital input
4	Digital output, low
5	Digital output, high
6	RS-485 enable, low
7	RS-485 enable, high

Default

1

P3 (DIO13/UART_DOUT)

Parameter range

0, 1, 3 - 5

Parameter	Description
0	Disabled
1	UART DOUT
2	N/A
3	Digital input
4	Digital output, low
5	Digital output, high

Default

1

P4 (DIO14/UART_DIN Configuration)

Parameter range

0, 1, 3 - 5

Parameter	Description
0	Disabled
1	UART DIN

Parameter	Description
2	N/A
3	Digital input
4	Digital output, low
5	Digital output, high

Default

1

SMT/MMT SPI interface commands

P5 (DIO15/SPI_MISO Configuration)

Sets or displays the DIO15/SPI_MISO configuration.

This only applies to surface-mount and micro devices.

Parameter range

0, 1, 4, 5

Parameter	Description
0	Disabled
1	SPI_MISO
2	N/A
3	N/A
4	Digital output, low
5	Digital output, high

Default

1

P6 (DIO16/SPI_MOSI Configuration)

Sets or displays the DIO16/SPI_MOSI configuration.

This only applies to surface-mount and micro devices.

Parameter range

0, 1, 4, 5

Parameter	Description
0	Disabled
1	SPI_MOSI
2	N/A
3	N/A
4	Digital output, low
5	Digital output, high

Default

1

P7 (DIO17/SPI_SSEL Configuration)

Sets or displays the DIO17/SPI_$\overline{\text{SSEL}}$ configuration.
This only applies to surface-mount and micro devices.

Parameter range

0, 1, 4, 5

Parameter	Description
0	Disabled
1	SPI_$\overline{\text{SSEL}}$
2	N/A
3	N/A
4	Digital output, low
5	Digital output, high

Default

1

P8 (DIO18/SPI_CLK Configuration)

Sets or displays the DIO18/SPI_CLK configuration.
This only applies to surface-mount and micro devices.

Parameter range

0, 1, 4, 5

Parameter	Description
0	Disabled
1	SPI_CLK
2	N/A
3	N/A
4	Digital output, low
5	Digital output, high

Default

1

P9 (DIO19/SPI_ATTN Configuration)

Sets or displays the DIO19/SPI_$\overline{\text{ATTN}}$ configuration.

This only applies to surface-mount and micro devices.

Parameter range

0, 1, 4, 5

Parameter	Description
0	Disabled
1	SPI_$\overline{\text{ATTN}}$
2	N/A
3	N/A
4	Digital output, low
5	Digital output, high

Default

1

I/O settings commands

The following commands configure the various I/O lines available on the XBee® BLU.

Note See Digital I/O support for physical I/O pin mapping for the supported module form factors.

D0 (DIO0/ADC0/Commissioning Configuration)

Parameter range

0 - 5

Parameter	Description
0	Disabled
1	Commissioning Pushbutton
2	ADC
3	Digital input
4	Digital output, low
5	Digital output, high

Default

1

D1 (DIO1/ADC1/TH_SPI_ATTN Configuration)

Sets or displays the DIO1/ADC1/TH_SPI_$\overline{\text{ATTN}}$ configuration.

Parameter range

SMT/MMT: 0, 2 - 5

TH: 0 - 5

Parameter	Description
0	Disabled
1	SPI_$\overline{\text{ATTN}}$ for the through-hole device N/A for the surface-mount device
2	ADC
3	Digital input
4	Digital output, low
5	Digital output, high

Default

0

D2 (DIO2/ADC2/TH_SPI_CLK Configuration)

Sets or displays the DIO2/ADC2/TH_SPI_CLK configuration.

Parameter range

SMT/MMT: 0, 2 - 5

TH: 0 - 5

Parameter	Description
0	Disabled
1	SPI_CLK for through-hole devices N/A for surface-mount devices
2	ADC
3	Digital input
4	Digital output, low
5	Digital output, high

Default

0

D3 (DIO3/ADC3/TH_SPI_SSEL Configuration)

Sets or displays the DIO3/ADC3/TH_SPI_$\overline{\text{SSEL}}$ configuration.

Parameter range

SMT/MMT: 0, 2 - 5

TH: 0 - 5

Parameter	Description
0	Disabled
1	SPI_$\overline{\text{SSEL}}$ for the through-hole device N/A for surface-mount device
2	ADC
3	Digital input
4	Digital output, low
5	Digital output, high

Default

0

D4 (DIO4/TH_SPI_MOSI Configuration)

Sets or displays the DIO4/TH_SPI_MOSI configuration.

Parameter range

0, 3 - 5

TH: 0, 1, 3 - 5

Parameter	Description
0	Disabled
1	SPI_MOSI for the through-hole device N/A for the surface-mount and micro device
2	N/A
3	Digital input
4	Digital output, low
5	Digital output, high

Default

0

D5 (DIO5/Associate Configuration)

Sets or displays the DIO5/ASSOCIATED_INDICATOR configuration.

Parameter range

0, 1, 3 - 5

Parameter	Description
0	Disabled
1	Associate LED indicator - blinks when associated
2	N/A
3	Digital input
4	Digital output, low
5	Digital output, high

Default

1

D8 (DIO8/DTR/SLP_Request Configuration)

Sets or displays the DIO8/$\overline{\text{DTR}}$/SLP_RQ configuration.

Note If **D8** is configured as DTR/Sleep_Request (**1**), the line will be left floating while the device sleeps. Leaving **D8** set to **1** and the corresponding pin not connected to anything external to the device may result in higher sleep current draw.

Parameter range

0, 1, 3 - 5

Parameter	Description
0	Disabled
1	$\overline{\text{DTR}}$/Sleep_Request (used with pin sleep and cyclic sleep with pin wake)
2	N/A
3	Digital input
4	Digital output, low
5	Digital output, high

Default

1

D9 (DIO9/ON_SLEEP Configuration)

Sets or displays the DIO9/ON_$\overline{\text{SLEEP}}$ configuration.

Parameter range

0, 1, 3 - 5

Parameter	Description
0	Disabled
1	ON/$\overline{\text{SLEEP}}$ indicator
2	N/A
3	Digital input
4	Digital output, low
5	Digital output, high

Default

1

P2 (DIO12/TH_SPI_MISO Configuration)

Sets or displays the DIO12/TH_SPI_MISO configuration.

Parameter range

0, 3 - 5

TH: 0, 1, 3 - 5

Parameter	Description
0	Disabled

Parameter	Description
1	SPI_MISO for the through-hole device N/A for the surface-mount and micro device
2	N/A
3	Digital input
4	Digital output, low
5	Digital output, high

Default

0

PR (Pull-up/Down Resistor Enable)

The bit field that configures the internal pull-up resistor status for the I/O lines.

- If you set a **PR** bit to 1, it enables the pull-up/down resistor
- If you set a **PR** bit to 0, it specifies no internal pull-up/down resistor.

PR and **PD** only affect lines that are configured as digital inputs (**3**) or disabled (**0**).
The following table defines the bit-field map for **PR** and **PD** commands.

Bit	I/O line
0	DIO4
1	DIO3
2	DIO2
3	DIO1
4	DIO0
5	DIO6
6	DIO8
7	DIO14
8	DIO5
9	DIO9
10	DIO12
11	N/A
12	N/A
13	DIO7
14	DIO13

Bit	I/O line
15	DIO15
16	DIO16
17	DIO17
18	DIO18
19	DIO19

Note See Digital I/O support for I/O pin mapping.

Parameter range

SMT/MMT: 0 - 0xFFFFF

Default

0xE7FF

PD (Pull Up/Down Direction)

The resistor pull direction bit field (1 = pull-up, 0 = pull-down) for corresponding I/O lines that are set by the **PR** command.

See PR (Pull-up/Down Resistor Enable) for the bit mappings.

Parameter range

SMT/MMT: 0 - 0xFFFFF

Default

0xE7FF

LT (Associate LED Blink Time)

Set or read the Associate LED blink time. If you use D5 (DIO5/Associate Configuration) to enable the Associate LED functionality (DIO5/Associate pin), this value determines the on and off blink times for the LED when the device has joined the network.

If **LT** = **0**, the device uses the default blink rate of 250 ms.

For all other **LT** values, the firmware measures **LT** in 10 ms increments.

Parameter range

0, 0x14 - 0xFF (x 10 ms)

Default

0

AV (Analog Voltage Reference)

The analog voltage reference used for A/D sampling.

ADC lines are 10-bit analog inputs.

Parameter range

0 - 2

Parameter	Description
0	1.21 V reference
1	2.42 V reference
2	VDD reference

Default

0

Location commands

The following commands are user-defined parameters used to store the physical location of the deployed device.

LX (Location X–Latitude)

User-defined GPS latitude coordinates of the node that is displayed on Digi Remote Manager and Network Assistant.

Parameter range

0 - 15 ASCII characters

Default

One ASCII space character (0x20)

LY (Location Y–Longitude)

User-defined GPS longitude coordinates of the node that is displayed on Digi Remote Manager and Network Assistant.

Parameter range

0 - 15 ASCII characters

Default

One ASCII space character (0x20)

LZ (Location Z–Elevation)

User-defined GPS elevation of the node that is displayed on Digi Remote Manager and Network Assistant.

Parameter range

0 - 15 ASCII characters

Default

One ASCII space character (0x20)

Diagnostic commands – firmware/hardware Information

The following read-only commands are diagnostics that provide more information about the device.

NI (Network Identifier)

The node identifier is a user-defined name or description of the device.

Parameter range

A string of case-sensitive ASCII printable characters from 1 to 20 bytes in length. A carriage return or a comma automatically ends the command.

Default

0x20 (an ASCII space character)

DD (Device Type Identifier)

Stores the Digi device type identifier value. Use this value to differentiate between multiple types of devices (for example, sensors or lights).

This command can optionally be included in network discovery responses by setting bit 1 of **NO**.

Parameter range

0 - 0xFFFFFFFF

Default

0x1A0000

SH (Serial Number High)

This value is read-only and it never changes.

Parameter range

0 - 0xFFFFFFFF

Default

Set in the factory

SL (Serial Number Low)

This value is read-only and it never changes.

Parameter range

0 - 0xFFFFFFFF [read-only]

Default

Set in the factory

VR (Firmware Version)

Reads the firmware version on a device.

The most significant byte represents the hardware and region.

Example:

- 0x90: XR 900 US
- 0x92: XR 900 AUS

Parameter range

0x4000 - 0x40FF

Default

Set in the firmware

VH (Bootloader Version)

Reads the bootloader version of the device.

Parameter range

N/A

Default

N/A

HV (Hardware Version)

Display the hardware version number and revision number of the device. The upper byte is the Hardware version and the lower byte is the hardware revision.

The hardware version distinguishes one radio type from another.

The hardware revision for a particular module can change for a variety of reasons and should not be used as the sole determination that a module's functionality has changed from previous revisions. The revision may change for various reasons including a new software version, a minor hardware modification, or even due to a label update. Furthermore, the firmware on a module may be upgraded or downgraded by a user thus making it different from the firmware version it was manufactured with. Thus the revision number is not a reliable indicator of the firmware version on the module. If an explanation for the revision number is not found in the release notes and it is a concern, contact Digi Support. In most cases the revision number does not relay any useful information to the consumer and it can be ignored.

Parameter range

0 - 0xFFFF [read-only]

Pre-defined **HV** values for XBee® BLUs:

Pre-defined upper byte values for XBee® BLUs:

- 0x5C - XBee BLU Micro (MMT) and Surface Mount (SMT)
- 0x5D - XBee BLU Through Hole (TH)

Default

Set in the factory

%C (Hardware/Software Compatibility)

Specifies what firmware is compatible with this device's hardware. **%C** is compared to the to the "compatibility_number" field of the firmware configuration xml file. Firmware with a compatibility

number lower than the value returned by **%C** cannot be loaded onto the board. If an invalid firmware is loaded, the device will not boot until a valid firmware is reloaded.

Parameter range

[read-only]

Default

N/A

%V (Supply Voltage)

Reads the voltage on the Vcc pin in mV.

Parameter range

0 - 0xFFFF (in mV) [read only]

Default

N/A

TP (Temperature)

The current module temperature in degrees Celsius. The temperature is represented in two's complement, as shown in the following example:

1 °C = 0x0001 and -1°C = 0xFFFF

Parameter range

0 - 0xFFFF (Celsius) [read-only]

Default

N/A

CK (Configuration CRC)

Reads the cyclic redundancy check (CRC) of the current AT command configuration settings to determine if the configuration has changed.

After a firmware update this command may return a different value.

Parameter range

0 - 0xFFFF [read-only]

Default

N/A

D% (Manufacturing Date)

Reads the manufacturing date of the module.

The format of the value given for ATD% is 16 hex characters, i.e. ATD%DDDDDDHH000FFFFF, where DDDDDD represents the manufacturing date as the number of days since 1/1/1900: 1/1/2000=0x008EAC, etc. HH represents the hour based on a 24-hour clock. 000 is three empty

hex digits. FFFFF represents the test fixture serial number as a decimal (this number is not converted to hex).

Parameter range

0 - 0xFFFFFFFFFFFFFFFF [read-only]

Default

N/A

Memory access commands

This section details the executable commands that provide memory access to the device.

FR (Software Reset)

Resets the device. The device responds immediately with an **OK** and performs a reset 100 ms later.

If you issue **FR** while the device is in Command mode, the reset effectively exits Command mode.

Parameter range

N/A

Default

N/A

AC (Apply Changes)

This command applies changes to all command parameters configured in Command mode.

Any of the following also applies changes the same as issuing an **AC** command:

- Exiting Command mode with a **CN** command.
- Exiting Command mode via timeout.
- Receiving a 0x08 API command frame.
- Issuing a 0x08 Local AT Command API frame.
- Issuing a remote 0x17 AT Command API frame with option bit 1 set.

Example: Altering the UART baud rate with the **BD** command does not change the operating baud rate until after an **AC** command is received; at this point, the interface immediately changes baud rates.

Parameter range

N/A

Default

N/A

WR (Write)

Immediately writes parameter values to non-volatile flash memory so they persist through a power cycle. .

Note Once you issue a **WR** command, do not send any additional characters to the device until after you receive the **OK** response. Use the **WR** command sparingly; the device's flash only supports 10,000 erase/write cycles.

Parameter range

N/A

Default

N/A

RE (Restore Defaults)

Parameter range

N/A

Default

N/A

Custom Default commands

The following commands are used to assign custom defaults to the device. Send RE (Restore Defaults) to restore custom defaults. You must send these commands as local AT commands, they cannot be set using Remote AT Command Request frame - 0x17.

%F (Set Custom Default)

When **%F** is received, the XBee® BLU takes the next command received and applies it to both the current configuration and the custom defaults, so that when defaults are restored with RE (Restore Defaults) the custom value is used.

Parameter range

N/A

Default

N/A

!C (Clear Custom Defaults)

Clears all custom defaults. This command does not change the current settings, but only changes the defaults so that RE (Restore Defaults) restores settings to the factory values.

Parameter range

N/A

Default

N/A

R1 (Restore Factory Defaults)

Restores factory defaults, ignoring any custom defaults set using %F (Set Custom Default).

Parameter range

N/A

Default

N/A

Operate in API mode

API mode overview

API mode provides a structured interface where data is communicated through the serial interface in organized packets and in a determined order. This enables you to establish complex communication between devices without having to define your own protocol. The API specifies how commands, command responses and device status messages are sent and received from the device using the serial interface or the SPI interface.

We may add new frame types to future versions of the firmware, so we recommend building the ability to filter out additional API frames with unknown frame types into your software interface.

Use the AP command to set the operation mode

Use AP (API Enable) to specify the operation mode:

AP command setting	Description
AP = 1	API operation.
AP = 2	API operation with escaped characters (only possible on UART).

The API data frame structure differs depending on what mode you choose.

API frame format

An API frame consists of the following:

- Start delimeter
- Length
- Frame data
- Checksum

API operation (AP parameter = 1)

This is the recommended API mode for most applications. The following table shows the data frame structure when you enable this mode:

Frame fields	Byte	Description
Start delimiter	1	0x7E
Length	2 - 3	Most Significant Byte, Least Significant Byte
Frame data	4 - number (n)	API-specific structure
Checksum	n + 1	1 byte

Any data received prior to the start delimiter is silently discarded. If the frame is not received correctly or if the checksum fails, the XBee replies with a radio status frame indicating the nature of the failure.

API operation with escaped characters (AP parameter = 2)

Setting API to 2 allows escaped control characters in the API frame. Due to its increased complexity, we only recommend this API mode in specific circumstances. API 2 may help improve reliability if the serial interface to the device is unstable or malformed frames are frequently being generated.

When operating in API 2, if an unescaped 0x7E byte is observed, it is treated as the start of a new API frame and all data received prior to this delimiter is silently discarded. For more information on using this API mode, see the Escaped Characters and API Mode 2 in the Digi Knowledge base.

API escaped operating mode works similarly to API mode. The only difference is that when working in API escaped mode, the software must escape any payload bytes that match API frame specific data, such as the start-of-frame byte (0x7E). The following table shows the structure of an API frame with escaped characters:

Frame fields	Byte	Description	
Start delimiter	1	0x7E	
Length	2 - 3	Most Significant Byte, Least Significant Byte	Characters escaped if needed
Frame data	4 - n	API-specific structure	
Checksum	n + 1	1 byte	

Start delimiter field

This field indicates the beginning of a frame. It is always 0x7E. This allows the device to easily detect a new incoming frame.

Escaped characters in API frames

If operating in API mode with escaped characters (**AP** parameter = 2), when sending or receiving a serial data frame, specific data values must be escaped (flagged) so they do not interfere with the data frame sequencing. To escape an interfering data byte, insert 0x7D and follow it with the byte to be escaped (XORed with 0x20).

The following data bytes need to be escaped:

- 0x7E: start delimiter
- 0x7D: escape character
- 0x11: XON
- 0x13: XOFF

Note Since software flow control is not implemented on this device, having hex values of 0x11 and 0x13 in the API frame isn't a reason to use AP = 2.
Since 0x7D is the escape character itself, the only value of AP = 2 is to distinguish a 0x7E in the data compared to the start delimiter 0x7E.

To escape a character:

1. Insert 0x7D (escape character).
2. Append it with the byte you want to escape, XORed with 0x20.

In API mode with escaped characters, the length field does not include any escape characters in the frame and the firmware calculates the checksum with non-escaped data.

Example: escape an API frame

To express the following API non-escaped frame in API operating mode with escaped characters:

Start delimiter	Length	Frame type	Frame Data	Checksum
			Data	
7E	00 0F	17	01 00 13 A2 00 40 AD 14 2E FF FE 02 4E 49	6D

You must escape the 0x13 byte:

1. Insert a 0x7D.
2. XOR byte 0x13 with 0x20: 13 ⊕20 = 33

The following figure shows the resulting frame. Note that the length and checksum are the same as the non-escaped frame.

Start delimiter	Length	Frame type	Frame Data	Checksum
			Data	
7E	00 0F	17	01 00 7D 33 A2 00 40 AD 14 2E FF FE 02 4E 49	6D

The length field has a two-byte value that specifies the number of bytes in the frame data field. It does not include the checksum field.

Length field

The length field is a two-byte value that specifies the number of bytes contained in the frame data field. It does not include the checksum field.

Frame data

This field contains the information that a device receives or will transmit. The structure of frame data depends on the purpose of the API frame:

Start delimiter	Length		Frame data								Checksum
			Frame type	Data							
1	2	3	4	5	6	7	8	9	...	n	n+1
0x7E	MSB	LSB	API frame type	Data							Single byte

- **Frame type** is the API frame type identifier. It determines the type of API frame and indicates how the Data field organizes the information.
- **Data** contains the data itself. This information and its order depend on the what type of frame that the Frame type field defines.

Multi-byte values are sent big-endian.

Calculate and verify checksums

To calculate the checksum of an API frame:

1. Add all bytes of the packet, except the start delimiter 0x7E and the length (the second and third bytes).
2. Keep only the lowest 8 bits from the result.
3. Subtract this quantity from 0xFF.

To verify the checksum of an API frame:

1. Add all bytes including the checksum; do not include the delimiter and length.
2. If the checksum is correct, the last two digits on the far right of the sum equal 0xFF.

Frame descriptions

The following sections describe the API frames.

Local AT Command Request - 0x08

Response frame: Local AT Command Response - 0x88

Description

This frame type is used to query or set command parameters on the local device. Any parameter that is set with this frame type will apply the change immediately. If you wish to queue multiple parameter changes and apply them later, use the Queue Local AT Command Request - 0x09 instead.

When querying parameter values, this frame behaves identically to Queue Local AT Command Request - 0x09: You can query parameter values by sending this frame with a command but no parameter value field–the two-byte AT command is immediately followed by the frame checksum. When an AT command is queried, a Local AT Command Response - 0x88 frame is populated with the parameter value that is currently set on the device. The Frame ID of the 0x88 response is the same one set by the command in the 0x08 request frame.

Format

The following table provides the contents of the frame. For details on frame structure, see API frame format.

Offset	Size	Frame Field	Description
0	8-bit	Start Delimiter	Indicates the start of an API frame.
1	16-bit	Length	Number of bytes between the length and checksum.
3	8-bit	**Frame type**	Local AT Command Request - **0x08**
4	8-bit	**Frame ID**	Identifies the data frame for the host to correlate with a subsequent response. If set to**0**, the device will not emit a response frame.
5	16-bit	**AT command**	The two ASCII characters that identify the AT Command.
7-n	variable	**Parameter value (optional)**	If present, indicates the requested parameter value to set the given register. If no characters are present, it queries the current parameter value and returns the result in the response.
EOF	8-bit	Checksum	0xFF minus the 8-bit sum of bytes from offset 3 to this byte (between length and checksum).

Examples

Each example is written without escapes (**AP** = **1**) and all bytes are represented in hex format. For brevity, the start delimiter, length, and checksum fields have been excluded.

Set the local command parameter

Set the **NI** string of the radio to "**End Device**".

The corresponding Local AT Command Response - 0x88 with a matching Frame ID will indicate whether the parameter change succeeded.

7E 00 0E **08 A1 4E 49 45 6E 64 20 44 65 76 69 63 65** 38

Frame type	Frame ID	AT command	Parameter value
0x08	0xA1	0x4E49	0x456E6420446576696365
Request	*Matches response*	*"NI"*	*"End Device"*

Query local command parameter

Query the temperature of the module–**TP** command.

The corresponding Local AT Command Response - 0x88 with a matching Frame ID will return the temperature value.

7E 00 04 **08 17 54 50** 3C

Frame type	Frame ID	AT command	Parameter value
0x08	0x17	0x5450	(omitted)
Request	*Matches response*	*"TP"*	*Query the parameter*

Queue Local AT Command Request - 0x09

Response frame: Local AT Command Response - 0x88

Description

This frame type is used to query or set queued command parameters on the local device. In contrast to Local AT Command Request - 0x08, this frame queues new parameter values and does not apply them until you either:

- Issue a Local AT Command using the 0x08 frame
- Issue an **AC** command—queued or otherwise

When querying parameter values, this frame behaves identically to Local AT Command Request - 0x08: You can query parameter values by sending this frame with a command but no parameter value field—the two-byte AT command is immediately followed by the frame checksum. When an AT command is queried, a Local AT Command Response - 0x88 frame is populated with the parameter value that is currently set on the device. The Frame ID of the 0x88 response is the same one set by the command in the 0x09 request frame.

Format

The following table provides the contents of the frame. For details on frame structure, see API frame format.

Offset	Size	Frame Field	Description
0	8-bit	Start Delimiter	Indicates the start of an API frame.
1	16-bit	Length	Number of bytes between the length and checksum.
3	8-bit	**Frame type**	Queue Local AT Command Request - **0x09**
4	8-bit	**Frame ID**	Identifies the data frame for the host to correlate with a subsequent response. If set to**0**, the device will not emit a response frame.
5	16-bit	**AT command**	The two ASCII characters that identify the AT Command.
7-n	variable	**Parameter value (optional)**	If present, indicates the requested parameter value to set the given register at a later time. If no characters are present, it queries the current parameter value and returns the result in the response.
EOF	8-bit	Checksum	0xFF minus the 8-bit sum of bytes from offset 3 to this byte (between length and checksum).

Examples

Each example is written without escapes (**AP** = **1**) and all bytes are represented in hex format. For brevity, the start delimiter, length, and checksum fields have been excluded.

Queue setting local command parameter

Set the UART baud rate to 115200, but do not apply changes immediately.

The device will continue to operate at the current baud rate until the change is applied with a subsequent **AC** command.

The corresponding Local AT Command Response - 0x88 with a matching Frame ID will indicate whether the parameter change succeeded.

7E 00 05 **09 53 42 44 07** 16

Frame type	Frame ID	AT command	Parameter value
0x09	0x53	0x4244	0x07
Request	*Matches response*	*"BD"*	*7 = 115200 baud*

Query local command parameter

Query the temperature of the module (**TP** command).

The corresponding 0x88 - Local AT Command Response frame with a matching Frame ID will return the temperature value.

7E 00 04 **09 17 54 50** 3B

Frame type	Frame ID	AT command	Parameter value
0x09	0x17	0x5450	(omitted)
Request	*Matches response*	*"TP"*	*Query the parameter*

Explicit Addressing Command Request - 0x11

Response frame: Extended Transmit Status - 0x8B

Description

This frame type is only used for GPM commands on this product.

Query NP (Maximum Packet Payload Bytes) to read the maximum number of payload bytes that can be sent in a GPM request.

64-bit addressing

- For broadcast transmissions, set the 64-bit destination address to **0x000000000000FFFF**
- For unicast transmissions, set the 64-bit address field to the address of the desired destination node

Reserved endpoints

For serial data transmissions, the **0xE8** endpoint should be used for both source and destination endpoints.

The active Digi endpoints are:

- **0xE8** - Digi Data endpoint
- **0xE6** - Digi Device Object (DDO) endpoint

Reserved cluster IDs

The following cluster IDs can be used on the **0xE8** data endpoint:

- **0x0023** - General Purpose Memory cluster ID: allows for reading and writing flash on the device.

Reserved profile IDs

The Digi profile ID should always be **0xC105**.

Format

The following table provides the contents of the frame. For details on frame structure, see API frame format.

Offset	Size	Frame Field	Description
0	8-bit	Start Delimiter	Indicates the start of an API frame.
1	16-bit	Length	Number of bytes between the length and checksum.
3	8-bit	**Frame type**	Explicit Addressing Command Request - **0x11**

Offset	Size	Frame Field	Description
4	8-bit	**Frame ID**	Identifies the data frame for the host to correlate with a subsequent response. If set to**0**, the device will not emit a response frame.
5	64-bit	**64-bit destination address**	Not used.
13	16-bit	**16 bit address**	Not used.
15	8-bit	**Source Endpoint**	Source endpoint for the transmission. Serial data transmissions should use **0xE8**.
16	8-bit	**Destination Endpoint**	Destination endpoint for the transmission. Serial data transmissions should use **0xE8**.
17	16-bit	**Cluster ID**	The Cluster ID that the host uses for GPM access is 0x0023.
19	16-bit	**Profile ID**	The Profile ID should always be **0xC105**.
21	8-bit	**Broadcast radius**	Not used.
22	8-bit	**Transmit options**	Not used.
23-n	variable	**Command data**	Data to be sent to the destination device. Up to **NP** bytes per packet.
EOF	8-bit	Checksum	0xFF minus the 8-bit sum of bytes from offset 3 to this byte (between length and checksum).

Examples

Each example is written without escapes (**AP** = **1**) and all bytes are represented in hex format. For brevity, the start delimiter, length, and checksum fields have been excluded.

Loopback Packet

Sending a loopback transmission to an device with the 64-bit address of **0013A20012345678** using Cluster ID **0x0012**. To better understand the raw performance, retries and acknowledgements are disabled.

The corresponding Extended Transmit Status - 0x8B response with a matching Frame ID can be used to verify that the transmission was sent.

The destination will not emit a receive frame, instead it will return the transmission back to the sender. The source device will emit the receive frame–the frame type is determined by the value of **AO**–if the packet looped back successfully.

7E 00 1A **11 F8 00 13 A2 00 12 34 56 78 FF FE E8 E8 00 12 C1 05 00 01 54 78 44 61 74 61** 41

Frame type	Frame ID	64-bit dest	Source EP	Dest EP	Cluster	Profile	Bcast radius	Tx options	Command data
0x11	0xF8	0x0013A200 12345678	0xE8	0xE8	0x0012	0xC105	0x00	0x01	0x547844617461
Explicit request	*Matches response*	*Destination*	*Digi data*	*Digi data*	*Data*	*Digi profile*	*N/A*	*Disable retries*	*"TxData"*

BLE Unlock Request - 0x2C

Response frame: BLE Unlock Response frame - 0xAC

Description

This frame type is used to authenticate a connection on the Bluetooth interface and unlock the processing of AT command frames across this interface. The frame format for the BLE Unlock Request - 0x2C and BLE Unlock Response frame - 0xAC are identical.

The unlock process is an implementation of the SRP (Secure Remote Password) algorithm using the RFC5054 1024-bit group and the SHA-256 hash algorithm . The SRP identifying user name, commonly referred to as *I*, is fixed to the username **apiservice**.

Upon completion, each side will have derived a shared session key which is used to communicate in an encrypted fashion with the peer. Additionally, a Modem Status - 0x8A with the status code **0x32 (Bluetooth Connected)** is emitted. When an unlocked connection is terminated, a Modem Status frame with the status code **0x33 (Bluetooth Disconnected)** is emitted.

The following implementations are known to work with the BLE SRP implementation:

- github.com/cncfanatics/SRP

You need to modify the hashing algorithm to SAH256 and the values ofNandgto use the RFC5054 1024-bit group.

- github.com/cocagne/csrp
- github.com/cocagne/pysrp

Format

The following table provides the contents of the frame. For details on frame structure, see API frame format.

Offset	Size	Frame Field	Description
0	8-bit	Start Delimiter	Indicates the start of an API frame.
1	16-bit	Length	Number of bytes between the length and checksum.

Offset	Size	Frame Field	Description
3	8-bit	**Frame type**	BLE Unlock Request - **0x2C** BLE Unlock Response - **0xAC**
4	8-bit	**Step**	Indicates the phase of authentication and interpretation of payload data: 1. Client presents *A* value 2. Server presents *B* and *salt* 3. Client present *M1* session key validation value 4. Server presents *M2* session key validation value and two 12-byte nonces See the phase tables below for more information. Step values greater than 0x80 indicate error conditions: **0x80** = Unable to offer *B*–cryptographic error with content, usually due to *A mod N == 0* **0x81** = Incorrect payload length **0x82** = Bad proof of key **0x83** = Resource allocation error **0x84** = Request contained a step not in the correct sequence
5-n	varies	**Payload**	Payload structure varies by Step value. Refer to the phase tables below for the structure of this field.
EOF	8-bit	Checksum	0xFF minus the 8-bit sum of bytes from offset 3 to this byte–between length and checksum.

Phase tables

The following fields are inserted as the payload data depending on the phase of the authentication process

Phase 1 (Client presents A)

Offset	Size	Frame Field	Description
5	1024-bit (128 bytes)	A	One-time ephemeral client public key. If the *A* value is zero, the server will terminate the connection.

Phase 2 (Server presentsBand salt)

Offset	Size	Frame Field	Description
5	32-bit (4 bytes)	Salt	The SRP Salt value from the **$S** command.

Offset	Size	Frame Field	Description
9	1024-bit (128 bytes)	B	One-time ephemeral host public key.

Phase 3 (Client presentsM1)

Offset	Size	Frame Field	Description
5	256-bit (32 bytes)	M1	SHA256 hash algorithm digest.

Phase 4 (Server presents M2)

Offset	Size	Frame Field	Description
5	256-bit (32 bytes)	M2	SHA256 hash algorithm digest .
37	96-bit (12 bytes)	Tx nonce	Random nonce used as the constant prefix of the counter block for encryption/decryption of data transmitted to the API service by the client.
49	96-bit (12 bytes)	Rx nonce	Random nonce used as the constant prefix of the counter block for encryption/decryption of data received by the client from the API service.

Upon completion of *M2* verification, the session key has been determined to be correct and the API service is unlocked and will allow additional API frames to be used. Content from this point will be encrypted using AES-256-CTR with the following parameters:

- **Key**: The entire 32-byte session key.
- **Counter**: 128 bits total, prefixed with the appropriate nonce shared during authentication. Initial remaining counter value is 1.

  The counter for data sent into the XBee API Service is prefixed with the TX *nonce* value–see the **Phase 4** table, above–and the counter for data sent by the XBee to the client is prefixed with the *RX nonce* value.

Examples

Example sequence to perform AT Command XBee API frames over BLE

1. Discover the XBee® BLU through scanning for advertisements.
2. Create a connection to the GATT Server.
3. Optional, but recommended: request a larger MTU for the GATT connection.
4. Turn on indications for the API Response characteristic.

5. Perform unlock procedure using BLE Unlock Request - 0x2C unlock frames.
6. Once unlocked, you may send Local AT Command Request - 0x08 frames and receive AT Command Response frames received.
   a. For each frame to send, form the API Frame, and encrypt through the stream cipher as described in the unlock procedure.
   b. Write the frame using one or more write operations.
   c. When successful, the response arrives in one or more indications. If your stack does not do it for you, remember to acknowledge each indication as it is received. Note that you are expected to process these indications and the response data is not available if you attempt to perform a read operation to the characteristic.
   d. Decrypt the stream of content provided through the indications, using the stream cipher as described in the unlock procedure.

User Data Relay Input - 0x2D

Response frame: TX Status frame - 0x89

Output frame: User Data Relay Output - 0xAD

Description

Use cases

- You can use this frame to send data to an external processor through the XBee UART/SPI via the BLE connection. Use a cellphone to send the frame with UART interface as a target. Data contained within the frame is sent out the UART contained within an Output Frame. The external processor then receives and acts on the frame.
- Use an external processor to output the frame over the UART with the BLE interface as a target. This outputs the data contained in the frame as the Output Frame over the active BLE connection via indication.

Format

The following table provides the contents of the frame. For details on frame structure, see API frame format.

Error cases

Errors are reported in a TX Status frame - 0x89 frame that corresponds with the Frame ID of the Relay Data frame:

Error code	Error	Description
0x7C	Invalid Interface	The user specified a destination interface that does not exist or is unsupported.
0x7D	Interface not	The destination interface is a valid interface, but is not in a state

Error code	Error	Description
	accepting frames	that can accept data. For example: UART not in API mode, BLE does not have a GATT client connected, or buffer queues are full.

If the message was relayed successfully, no status will be generated.

Bluetooth Gap Scan Request - 0x34

Response frames:

- Bluetooth GAP Scan Status - 0xB5
- Bluetooth GAP Scan Legacy Advertisement Response - 0xB4

Description

The Bluetooth Low Energy (BLE) GAP Scan API provides a way to initiate and control Bluetooth GAP scans on a BLE device. GAP scans are used to discover nearby BLE devices and gather information about them.

When a GAP scan request is sent a Bluetooth GAP Scan Status - 0xB5 will be received as feedback for the user regarding the state of the Scanner. If the scanner has successfully started, the user will receive Bluetooth GAP Scan Legacy Advertisement Response - 0xB4 frames with beacon information.

The GAP Scan API frame is used to start or stop a Bluetooth GAP scan. It allows for the configuration of six essential fields:

1. **Start** or **Stop the Scan**: This value determines whether the scan should start or stop.
2. **Duration**: The duration value specifies the amount of time, in seconds, for which the GAP scan should run. This value determines how long the BLE device will actively scan for nearby devices.
3. **Window** and **Interval**: Use the window and interval to optionally configure the scan duty cycle. The radio will actively scan advertisements during the window duration of every scan interval period.
4. **Filter Type**: The filter type controls which devices are considered valid scan results. Bluetooth devices transmit the payload using length, type, and value (LTV) format. Therefore, when the filter is enabled, it will filter all advertisements containing Complete Local Name (0x09) and Short Local Name (0x08) types.
5. **Filter**: The filter value is used in conjunction with the filter type to specify the device(s) to include or exclude from the scan results. The filter only accepts ASCII characters. After the filter is set, the scan will only display advertisements containing the text passed as a filter.

Format

The following table provides the contents of the frame. For details on frame structure, see API frame format.

Offset	Size	Field Name	Description
0	8-bit	Start Delimiter	Indicates the start of an API frame.
1	16-bit	Length	Number of bytes between the length and checksum.
3	8-bit	Frame Type	Bluetooth Scan Request - 0x34.
4	8-biy	Start Command	To start a scan, this value must be set to **0x01**. To stop a running scan, this value must be set to **0x00**
5	16-bit	Scan Duration	Scan duration should be set to **0x00** - **0xFFFF** (x 1 s) (18.20 hrs.). If scan is set to **0x00**, the scan will run indefinitely.
7	32-bit	Scan Window	The range is from **0x9C4** - **0x270FD8F** (x 1 us) (41 s). The window cannot be bigger than the scan interval.
11	32-bit	Scan Intervals	The range is from **0x9C4** - **0x270FD8F** (x 1 us) (41 s). The interval cannot be smaller than the scan window.
15	8-bit	Filter Type	Supported Filter Types: ■ **0x00**: Filter disabled ■ **0x01**: Filter advertisements containing Complete Local Name (0x09) and Short Local Name (0x08) types
16-n	variable	Filter ID (optional)	The range for the Filter ID is from 0-22 bytes; it can only accept up to 22 characters.
EOF	8-bit	Checksum	0xFF minus the 8-bit sum of bytes from offset 3 to this byte (between length and checksum).

Examples

Each example is written without escapes (AP=1) and all bytes are represented in hex format. For brevity, the start delimiter, length, and checksum fields have been excluded.

Start Bluetooth scanner without filtering responses.

The request will start the scanner with the following parameters:

- Duration: 10 seconds
- Window: 11.25 milliseconds
- Interval: 1.28 seconds

7E 00 0D 34 01 00 0A 00 00 2B F2 00 13 88 00 00 08

Frame Type	Starts Command	Scan Duration	Scan Window	Scan Interval	Filter Type
0x34	0x01	0x000A	0x0002BF2	0x00138800	0x00
Request	*Start Scan*	*10s*	*11250 us*	*128000 us*	*No filtering*

Start Bluetooth scanner with filtering responses

The request will start the scanner with the following parameters:

- Duration: 10 seconds
- Window: 11.25 milliseconds
- Interval: 1.28 seconds
- Filter ID: Tester

7E 00 13 34 01 00 0A 00 00 2B F2 00 13 88 00 01 54 65 73 74 65 72 90

Frame Type	Starts Command	Scan Duration	Scan Window	Scan Interval	Filter Type	Filter
0x34	0x01	0x000A	0x0002BF2	0x00138800	0x546573746572	0x546573746572
Request	*Start Scan*	*10s*	*11250 us*	*128000 ux*	*Filtering*	*"Tester"*

Stop Bluetooth scanner

The request will stop the scanner. This option is useful if the user manually stops the scanner.
7E 00 0D 34 00 00 00 00 00 00 00 00 00 00 00 CB

Frame Type	Starts Command	Scan Duration	Scan Window	Scan Interval	Filter Type
0x34	0x00	0x0000	0x00000000	0x00000000	0x00
Request	*Stop Scan*	*None*	*None*	*None*	*None*

Local AT Command Response - 0x88

Request frames:

- Local AT Command Request - 0x08
- Queue Local AT Command Request - 0x09

Description

This frame type is emitted in response to a local AT Command request. Some commands send back multiple response frames; for example, ND (Network Discovery). Refer to individual AT command descriptions for details on API response behavior.

This frame is only emitted if the Frame ID in the request is non-zero.

Format

The following table provides the contents of the frame. For details on frame structure, see API frame format.

Offset	Size	Frame Field	Description
0	8-bit	Start Delimiter	Indicates the start of an API frame.
1	16-bit	Length	Number of bytes between the length and checksum.
3	8-bit	**Frame type**	Local AT Command Response - **0x88**
4	8-bit	**Frame ID**	Identifies the data frame for the host to correlate with a prior request.
5	16-bit	**AT command**	The two ASCII characters that identify the AT Command.
7	8-bit	**Command status**	Status code for the host's request: **0** = OK **1** = ERROR **2** = Invalid command **3** = Invalid parameter
8-n	variable	**Command data (optional)**	If the host requested a command parameter change, this field will be omitted. If the host queried a command by omitting the parameter value in the request, this field will return the value currently set on the device.
EOF	8-bit	Checksum	0xFF minus the 8-bit sum of bytes from offset 3 to this byte (between length and checksum).

Examples

Each example is written without escapes (**AP** = **1**) and all bytes are represented in hex format. For brevity, the start delimiter, length, and checksum fields have been excluded.

Set local command parameter

Host set the NI string of the local device to "**End Device**" using a 0x08 request frame.

The corresponding Local AT Command Response - 0x88 with a matching Frame ID is emitted as a response:

7E 00 05 **88 01 4E 49 00** DF

Frame type	Frame ID	AT command	Command Status	Command data
0x88	0xA1	0x4E49	0x00	(omitted)
Response	*Matches request*	*"NI"*	*Success*	*Parameter changes return no data*

Query local command parameter

Host queries the temperature of the local device—TP command—using a 0x08 request frame.

The corresponding Local AT Command Response - 0x88 with a matching Frame ID is emitted with the temperature value as a response:

7E 00 07 **88 01 54 50 00 FF FE** D5

Frame type	Frame ID	AT command	Command Status	Command data
0x88	0x17	0x5450	0x00	0xFFFE
Response	*Matches request*	*"TP"*	*Success*	*-2 °C*

Modem Status - 0x8A

Description

This frame type is emitted in response to specific conditions. The status field of this frame indicates the device behavior.

Format

The following table provides the contents of the frame. For details on frame structure, see API frame format.

Offset	Size	Frame Field	Description
0	8-bit	Start Delimiter	Indicates the start of an API frame.
1	16-bit	Length	Number of bytes between the length and checksum.
3	8-bit	**Frame type**	Modem Status - **0x8A**
4	8-bit	**Modem status**	Complete list of modem statuses: **0x00** = Hardware reset or power up **0x01** = Watchdog timer reset **0x0D** = Voltage supply limit exceeded–see **Over-voltage detection** in the *XBee 3 RF Module Hardware Reference Manual*. **0x32** = BLE Connect **0x33** = BLE Disconnect
EOF	8-bit	Checksum	0xFF minus the 8-bit sum of bytes from offset 3 to this byte (between length and checksum).

Modem status codes

Statuses for specific modem types are listed here.

Examples

Each example is written without escapes (**AP** = **1**) and all bytes are represented in hex format. For brevity, the start delimiter, length, and checksum fields have been excluded.

Boot status

When a device powers up, it returns the following API frame:

7E 00 02 **8A 00** 75

Frame type	Modem Status
0x8A	0x00

Frame type	Modem Status
Status	Hardware Reset

Extended Transmit Status - 0x8B

Request frames:

- Transmit Request - 0x10
- Explicit Addressing Command Request - 0x11

Description

This frame type is emitted when a network transmission request completes. The status field of this frame indicates whether the request succeeded or failed and the reason. This frame type provides additional networking details about the transmission.

This frame is only emitted if the Frame ID in the request is non-zero.

Note Broadcast transmissions are not acknowledged and always return a status of **0x00**, even if the delivery failed.

Format

The following table provides the contents of the frame. For details on frame structure, see API frame format.

Offset	Size	Frame Field	Description
0	8-bit	Start Delimiter	Indicates the start of an API frame.
1	16-bit	Length	Number of bytes between the length and checksum.
3	8-bit	**Frame type**	Transmit Status - **0x8B**
4	8-bit	**Frame ID**	Identifies the data frame for the host to correlate with a prior request.
5	16-bit	**Reserved**	Unused.
7	8-bit	**Reserved**	Unused.
8	8-bit	**Delivery status**	Complete list of delivery statuses: **0x00** = Success **0x03** = Message purged **0x74** = Message too long
9	8-bit	**Reserved**	Unused.
EOF	8-bit	Checksum	0xFF minus the 8-bit sum of bytes from offset 3 to this byte (between length and checksum).

Explicit Receive Indicator - 0x91

Request frames:

- Explicit Addressing Command Request - 0x11

Description

This frame type is emitted when a device configured with explicit API output–AO (API Options) bit1 set–receives a packet.

Typically this frame is emitted as a result of a GPM operation because there is no network to receive data from.

Format

The following table provides the contents of the frame. For details on frame structure, see API frame format.

Offset	Size	Frame Field	Description
0	8-bit	Start Delimiter	Indicates the start of an API frame.
1	16-bit	Length	Number of bytes between the length and checksum.
3	8-bit	**Frame type**	Explicit Receive Indicator - **0x91**
4	64-bit	**64-bit source address**	The sender's 64-bit address.
14	8-bit	**Source endpoint**	Endpoint of the source that initiated transmission.
15	8-bit	**Destination endpoint**	Endpoint of the destination that the message is addressed to.
16	16-bit	**Cluster ID**	The Cluster ID that the frame is addressed to.
18	16-bit	**Profile ID**	The Profile ID that the fame is addressed to.
21-n	variable	**Received data**	The RF payload data that the device receives.
EOF	8-bit	Checksum	0xFF minus the 8-bit sum of bytes from offset 3 to this byte (between length and checksum).

User Data Relay Output - 0xAD

Input frame: User Data Relay Input - 0x2D

Description

This frame type is emitted when user data is relayed to the serial port from a local interface: BLE or the serial port.

Format

The following table provides the contents of the frame. For details on frame structure, see API frame format.

Error cases

Errors are reported in a Transmit Status - 0x89 frame that corresponds with the Frame ID of the Relay Data frame:

Error code	Error	Description
0x7C	Invalid Interface	The user specified a destination interface that does not exist or is unsupported.
0x7D	Interface not accepting frames	The destination interface is a valid interface, but is not in a state that can accept data. For example: UART not in API mode, BLE does not have a GATT client connected, or buffer queues are full.

If the message was relayed successfully, no status will be generated.

Examples

Each example is written without escapes (**AP** = **1**) and all bytes are represented in hex format. For brevity, the start delimiter, length, and checksum fields have been excluded.

Relay from Bluetooth (BLE)

A mobile phone sends a serial data message to the XBee device's BLE interface. The message is flagged to be sent out of the serial port of the XBee device. The following frame outputs the relayed data:

```
7E 00 0C AD 01 52 65 6C 61 79 20 44 61 74 61 BA
```

Frame type	Source interface	Data
0xAD	0x01	0x52656C61792044617461
Output	*Bluetooth*	*"Relay Data"*

Bluetooth GAP Scan Legacy Advertisement Response - 0xB4

Request frame: Bluetooth Gap Scan Request - 0x34

Description

This frame type is emitted whenever the Bluetooth scanner detects a legacy advertisement from nearby devices during a GAP scan. This response frame provides valuable information about the detected advertisement including their addresses, advertisement types, signal strengths, and additional data contained within the advertisement payload.

Format

The following table provides the contents of the frame. For details on frame structure, see API frame format.

Offset	Size	Field Name	Description
0	8-bit	Start Delimiter	Indicates the start of an API frame.
1	16-bit	Length	Number of bytes between the length and checksum.
3	8-bit	**Frame Type**	Bluetooth Scan Response - **0xB4**
4	48-bit	**Address**	The BLE MAC address of the received advertisement.
10	8-bit	**Address type**	Indicates whether the Bluetooth address is a public address or a randomly generated address.
11	8-bit	**Advertisement flags**	Bit field that indicates advertisement flags: ■ Bit 0: Device is connectable ■ Bit 1-7: Reserved
12	8-bit	**RSSI**	The received signal strength of the advertisement, in -dBm.
13	8-bit	**Reserved**	Unused.
14	8-bit	**Payload length**	Specifies the length of the advertisement payload.
16-n	variable	**Payload**	The actual data payload of the advertisement which can contain various information elements, manufacturer-specific data, or other relevant details about the advertising device.
EOF	8-bit	Checksum	0xFF minus the 8-bit sum of bytes from offset 3 to this byte (between length and checksum).

Bluetooth GAP Scan Status - 0xB5

Request frame: Bluetooth Gap Scan Request - 0x34

Description

This frame type is emitted in response to a Bluetooth GAP Scan Request and whenever the Bluetooth scan timer has timed out. The status field of this frame indicates the Bluetooth scanner state.

Format

The following table provides the contents of the frame. For details on frame structure, see API frame format.

Offset	Size	Field Name	Description
0	8-bit	Start Delimiter	Indicates the start of an API frame.
1	16-bit	Length	Number of bytes between the length and checksum.
3	8-bit	**Frame Type**	Bluetooth Scan Request - **0xB5**
4	8-bit	**Scan Status**	Reflects the status of the Bluetooth scanner: ■ **0x00**: Scanner has successfully started ■ **0x01**: Scanner is currently running ■ **0x02**: Scanner has successfully stopped ■ **0x03**: Scanner was unable to start or stop ■ **0x04**: Invalid parameters
EOF	8-bit	Checksum	0xFF minus the 8-bit sum of bytes from offset 3 to this byte (between length and checksum).

Bluetooth GAP Scan Extended Advertisement Response - 0xB7

Request frame: Bluetooth Gap Scan Request - 0x34

Description

This frame type is emitted whenever the Bluetooth scanner detects an extended advertisement from nearby devices during a GAP scan. This response frame provides valuable information about the detected advertisement including their addresses, advertisement types, signal strengths, and additional data contained within the advertisement payload.

Format

The following table provides the contents of the frame. For details on frame structure, see API frame format.

Offset	Size	Field Name	Description
0	8-bit	**Start delimiter**	Indicates the start of the API frame.
1	16-bit	**Length**	Number of bytes between the length and the checksum.
3	8-bit	**Frame type**	Bluetooth Scan Response with extended advertisement (**0xB7**).
4	48-bit	**Source address**	The BLE MAC address of the received advertisement.
10	8-bit	**Address type**	■ **0x0**: Public Address Type ■ **0x1**: Private randomly generated address
11	8-bit	**Advertisement flags**	Bit field that indicates advertisement flags: ■ Bit 0: Device is connectable ■ Bit 1-7: Reserved
12	8-bit	**RSSI**	The received signal strength of advertisement in -dBm.
13	8-bit	**Reserved**	
14	8-bit	**Adv. SID**	Advertising set identifier.
15	8-bit	**Primary PHY**	The preferred PHY for connecting with this device: ■ **0x1**: 1M PHY ■ **0x2**: 2M PHY ■ **0x4**: LE coded PHY 125k ■ **0x8**: LE coded PHY 500k ■ **0xFF**: Any PHY supported
16	8-bit	**Secondary PHY**	The secondary preferred PHY for connecting with this device:

Offset	Size	Field Name	Description
			■ **0x1**: 1M PHY ■ **0x2**: 2M PHY ■ **0x4**: LE coded PHY 125k ■ **0x8**: LE coded PHY 500k ■ **0xFF**: Any PHY supported
17	8-bit	**TX power**	TX power in dBm Range: -127 to +126 +127 means information is not available
18	16-bit	**Periodic interval**	Periodic advertising interval ■ 0: No periodic advertising ■ Range: 0x06 - 0xFFFF in 1.25ms units ■ Time range: 7.5 mSec to 81.92 Seconds
19	8-bit	**Data completeness**	■ **0x0**: All advertisement data has been reported ■ **0x1**: Advertisement data incomplete and more will come ■ **0x2**: Advertisement data incomplete but no more will come
20	8-bit	**Payload Length**	Specifies the length of the advertisement payload.
21-n	Variable	**Payload**	Can contain various advertisement data elements (e.g manufacturing specific data or relevant details about the advertising device).
n+1	8-bit	**Checksum**	0xFF minus the 8-bit sum of bytes from offset 3 to this byte (between length and checksum).