Understanding
LoRa Basics™ Modem-E

Semtech

October, 2020

Understanding LoRa Basics™ Modem-E
Technical Paper
October, 2020

semtech.com/LoRa

Page 1 of 12
Proprietary
Semtech

LR1110 – One Chip with Two "Flavors"

The LoRa Edge™ LR1110 is configured by default as a transceiver. The core transceiver functionality features the LoRa® capability that minimizes current consumption while providing ultra-long range spread spectrum communication and high interference immunity. Semtech's patented LoRa modulation technique, used in SX127X, SX126X and LR1110 devices, can achieve a sensitivity of over -148dBm using a low cost crystal and bill of materials. The high sensitivity, combined with the integrated +20 dBm power amplifier, yields industry leading link budget. This makes it optimal for any application requiring range or robustness. LoRa provides significant advantages in both blocking and selectivity over conventional modulation techniques, solving the traditional design compromise between range, interference immunity and energy consumption.

Transceiver Firmware

The architecture of end-node design when employing a transceiver for LoRaWAN® has the application processor hosting the LoRaWAN stack (the logic to support the LoRaWAN MAC), as well as the application logic (read sensor, send update, sleep, wake, etc.). The LoRaWAN stack and interactions with the LoRaWAN network server, including Join and data transport would be the responsibility of the application processor. However, the same LR1110 can be modified with the LoRa Basics™ Modem-E firmware stack.

LoRa Basics Modem-E Firmware

The Modem-E firmware adds a number of features to abstract the operation of the transceiver functionality. The Modem-E firmware allows developers to work at a high level with the LR1110, leaving the details of the LoRaWAN protocol and all communication to the firmware. The Modem-E firmware uses single API commands to exercise all of the interactions for the network. Examples of single-commands through the Modem-E interface are: joining the network, sending a data packet and completing a Wi-Fi scan. The Modem-E firmware also unlocks a significant number of other automated services enabled by LoRa Cloud™ that you can take advantage of through a simple, serial interface to the LR1110 chip. This allows you, as an end-node developer, to focus on the key aspects of the application itself and allocate the communication functionality to the LR1110 with the LoRa Basics Modem-E firmware.

The next couple of sections will review the capabilities of the LoRa Basics Modem-E firmware and also provide a high-level comparison between the Transceiver and Modem-E firmware versions.

Understanding LoRa Basics™ Modem-E
Technical Paper
October, 2020

semtech.com/LoRa

Page 2 of 12
Proprietary
Semtech

LoRa Basics Modem-E Feature Set

Functions of the LoRa Basics Modem-E include:

- LoRaWAN protocol version 1.0.3, Class A, EU863 & US902 Regional parameters
- Single command Join process
- Single command data upload
- Fully-automated device management service (provided through Semtech's LoRa Cloud Device & Application Services)
  - Device Configuration
    - ADR Profile
    - Reporting interval
    - Regulatory region
    - Application-specific status
    - Application layer clock synchronization data
  - Device Status
    - Battery voltage
    - Charge counter/Battery life prediction
    - Temperature
    - Strength of last downlink SNR/RSSI
    - Duration since last reset
    - Duration since last downlink
    - Firmware CRC
    - Crash log data
    - Modem reset count
    - GNSS Almanac status
    - GNSS Almanac debug response
  - Single command large file transfer uplink
  - Single command Reliable Octet Stream Encoding (packet loss prevention and recovery)
  - Clock synchronization
  - OTA Patch Update (coming soon)
  - FUOTA unicast, FUOTA multicast (coming soon)
- Single command GNSS scanning
- Single command passive Wi-Fi scanning
- Automated GNSS assistance, including almanac and timing information (faster GNSS scan time)
- Remote reset and re-keying
- LBT support for LoRaWAN (in Japan only)
- Future upgrades to the LoRaWAN specification and other new features

Comparison: Transceiver vs. LoRa Basics Modem-E

The following chart shows the differences in features between the Transceiver and LoRa Basics Modem-E firmware:

	Transceiver	Modem-E
LoRaWAN Stack	External to LR1110	Internal to LR1110
OTA Patch	NA	Available Soon
Join a network	External to LR1110	Single API call
Send a data packet	External to LR1110	Single API call
Automated GNSS aiding	External to LR1110	Handled automatically
Uplink large file transfer	External to LR1110	Single API call

Figure 2 shows the main elements in a typical end-node using the Transceiver versus using the Modem-E firmware.
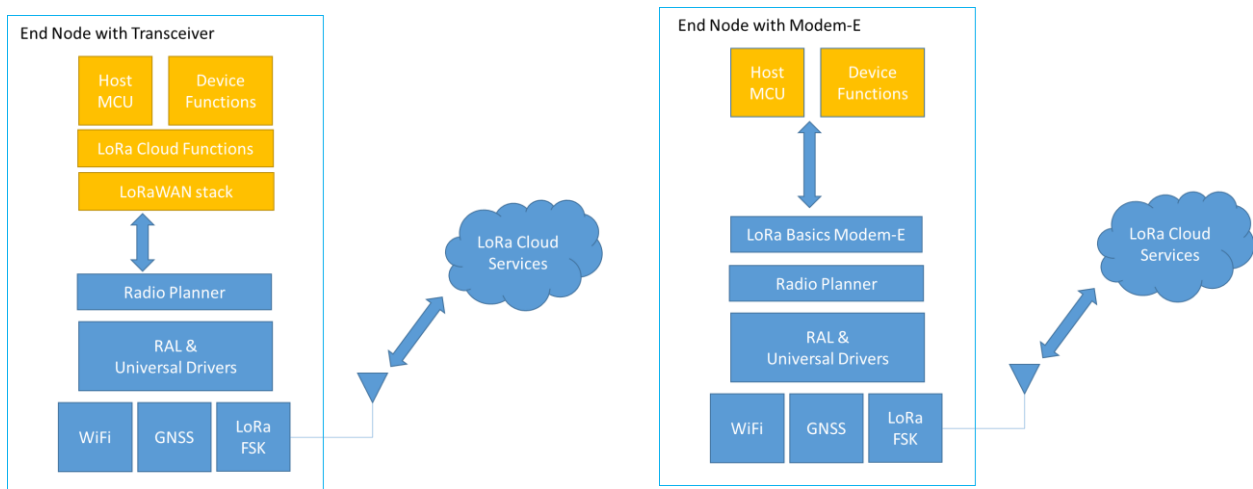

Figure 1: Transceiver end node compared to a Modem-E end node

Preparing Your LoRa Basics Modem-E for a LoRaWAN Network

The LoRa Basics Modem-E is shipped from the factory configured as a LoRa Edge transceiver. The transceiver functionality contains all of the core LoRa capabilities and has secure storage of the provisioning keys of the chip for LoRaWAN. However, to automatically take advantage of all of the integrated features with the LoRa Cloud API, the transceiver must be updated with LoRa Basics Modem-E firmware prior to shipping it as a product.

Upgrading the LoRa Edge LR1110 Transceiver to LoRa Basics Modem-E

The customary point in the end-device assembly process for upgrading the transceiver will be on the device production line. The LoRa Basics Modem-E full embedded firmware image is supplied. To convert the LR1110 from transceiver mode to Modem-E, the Modem-E firmware must be loaded onto a running

Understanding LoRa Basics™ Modem-E
Technical Paper
October, 2020

semtech.com/LoRa

Page 4 of 12
Proprietary
Semtech

LR1110 transceiver, from the transceiver's host controller, via an SPI interface as shown in Figure 2. The LR1110 bootloader will authenticate the firmware and will allow further execution. Only firmware images provided by Semtech can run on the LR1110. The LR1110 will also support patch updates, typically for maintenance in the field.
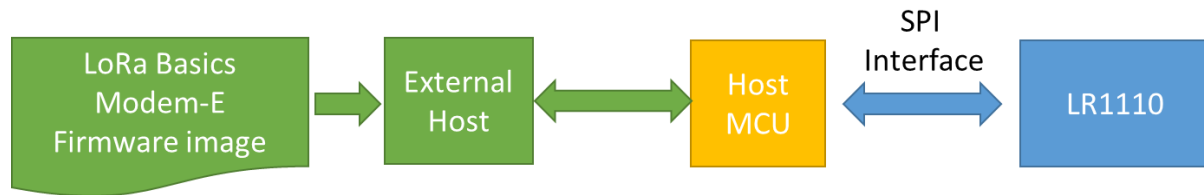

Figure 2: Program the Modem-E firmware with external host

Accessing DevEUI, AppEUI and PIN: Two Methods

LoRa Basics Modem-E is designed specifically for simple, secure provisioning. It comes pre-configured on the LoRa Cloud Device Join service. To access this service, provisioning information must be extracted directly from the LoRa Basics Modem-E. This information can be extracted at any time; however, a logical time for collecting and possibly using the provisioning information is during (or just after) the device firmware is updated. The basic provisioning information is the DevEUI (which is also the ChipEUI) and the PIN/Claim Code. The AppEUI/JoinEUI can also be specified for applications that require this value.

The first method for extracting this data is via the LR1110 SPI interface using the *GetChipEUI* API command for the DevEUI/ChipEUI and the *DeriveRootKeysAndGetPin* command for the PIN/Claim Code. Alternatively, you can use the Modem commands (once the LoRa Basics Modem-E firmware is loaded) and extract the data via the modem interface using the *GetChipEui* and *GetPin* commands respectively for DevEUI and the PIN/Claim Code.

Regardless of which method you use to extract the DevEUI/ChipEUI and PIN/Claim Code, you will need this data to provision the device via the LoRa Cloud Device Join service.

LoRa Basics Modem-E Deployment

A key motivating factors for developing the LR1110 was to simplify and secure the provisioning process of LoRa devices. While end-to-end security is built into the LoRaWAN specification, how device security keys are handled can be confusing and insecure. By building industry-leading security directly into the chip, the keys used to protect both the identity of the device on a LoRaWAN network and the traffic sent to and from the device are never exposed outside of the secure network system. Therefore, there is no need for files, databases, printouts or other, less robust methods of distributing those keys. The provisioning information is accessed directly through the LoRa Basics Modem-E interface and then used to provision

Understanding LoRa Basics™ Modem-E
Technical Paper
October, 2020

semtech.com/LoRa

Page 5 of 12
Proprietary
Semtech

the device via the LoRa Cloud Device Join service. Once the device is claimed via the LoRa Cloud Device Join service, the network will authenticate the device and enable LoRaWAN traffic to flow securely to the designated LoRaWAN Network Server.

The steps involved in deploying an end-node with the LoRa Basics Modem-E firmware are:

1) Create a LoRa Cloud Portal account
2) Create an application ID in your account
3) Claim the device using the DevEUI and Claim/PIN code
4) Select a LoRaWAN network server for your application and device

One of the key features of the new LR1110 chipset is that the keys for LoRaWAN are securely embedded on the device and are never exposed during the manufacturing and deployment process.

The purpose of mapping the network server to your application ID is so that specific parameters can be setup for handling data when operating with that network server. Two common settings for each application definition are the *network server* and *wrapkey*. The *network server* is the identifier of the LoRaWAN network server that will be associated with this Application Owner configuration. The *wrapkey* is a specific token used for encrypting the AppSKey from the LoRaWAN session. (The unencrypted AppSKey is used for encrypting the LoRaWAN payload data between the device and Application Server in LoRaWAN.) The *wrapkey* can be null, indicating that the AppSKey will be passed from the LoRaWAN Network Server to the Application Server without being encrypted. For more information on working with the AppSKey see the [LoRa Cloud Device Join documentation](#).

Once the network server is configured for your application ID on the LoRa Cloud Device Server, the Device Join process can be performed. The network server that sees the join request from the claimed device will forward it on to the LoRa Cloud Device Join service. In turn, the Device Join service will securely access the root keys for the device, processing them on a Hardware Security Module (HSM)[1], which derives the session keys and returns them, along with the Join Response, to the network server. If a *wrapkey* is defined for the application associated with the network server, the AppSKey is returned encrypted. Otherwise, the AppSKey will be in plain text. The network server will send the join response to the device. Once a data message is sent from the device to the network server after the join response has been received, the joining will be complete and the device will be configured to operate on that network server. Figure 3 illustrates the Device Join process:

---

[1] HSM stands for Hardware Security Module. An HSM is a dedicated piece of computer equipment with a defined API that allows for the processing and distribution of secure keys and tokens in a completely self-contained device.
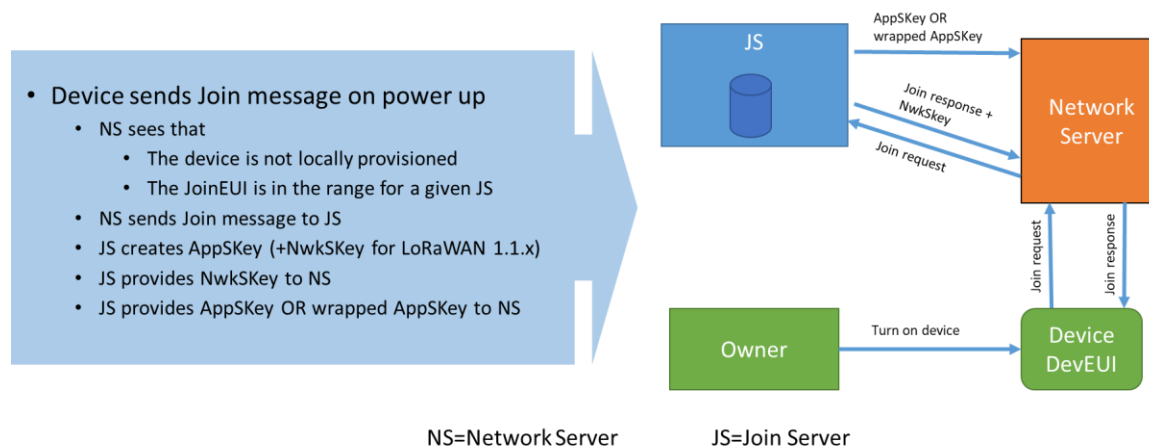
Figure 3: The Device Join process

LoRa Basics Modem-E Operation

The LoRa Basics Modem-E is designed with integration with LoRa Cloud Services in mind. LoRa Cloud Services provide a cloud-based interface and are used to automate and simplify some of the most useful tasks available for devices featuring LoRa. So far, we have discussed the LoRa Cloud Device Join service. There are two other LoRa Cloud services as well: the LoRa Cloud Device & Application Services and the LoRa Cloud Geolocation Service.

The LoRa Cloud Device & Application Services

These services comprise the following features:

1. **Periodically communicating informational messages, such as:**
   - System status, firmware version
   - Charge, voltage, temperature
   - Downlink signal quality
   - Uptime, time since last downlink
   - Device EUI, Join EUI
   - Application-specific status bytes
2. **Triggering client-initiated management commands, such as:**
   - Mute, re-join
   - Soft reset, factory reset
   - Retrieve crash log
   - Change region

Understanding LoRa Basics™ Modem-E
Technical Paper
October, 2020

semtech.com/LoRa

Page 7 of 12
Proprietary
Semtech

- Set ADR profile
- Change reporting interval of periodic info messages

3. **Running advanced, application-layer protocols which solve common LoRaWAN use cases, such as:**
   - Reliable Octet Stream Encoding (ROSE)
   - Large file upload to network
   - Application-Layer Clock Synchronization (ALCSYNC)

The goal of the Device & Application Services is to combine all of the most important features of managing large groups of IoT devices into a single service. Providing a single interface for features like monitoring battery life and managing firmware, greatly simplifies the operation of thousands or millions of devices on a single network. This capability allows developers and systems integrators to focus on the real value of their applications without having to first develop all of the support functionality required, such as the ability to transfer large files from the device to the network that may be necessary for certain customers.

The Device & Application Services are fully compatible with the LoRa Basics Modem-E functionality. This means that the LoRa Basics Modem-E can take advantage of these features without you needing to develop application code on the device or network to have access to this suite of features.

Figure 4 shows the flow of data from a LoRa Basics Modem-E device to a LoRaWAN network server. The network server forwards all traffic to the Application Provider. Some of that traffic has a special application port number (199), which is routed to the Device & Application Services. Regular traffic that does not travel through port 199 is passed to the application logic without modification.
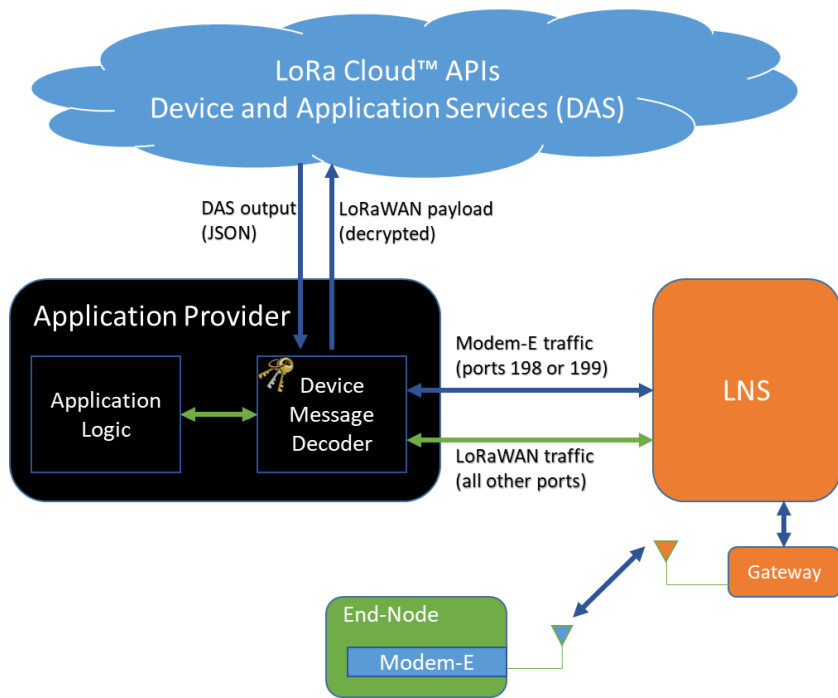

Figure 4: Flow from LoRa Basics Modem-E to Device & Application Services

Understanding LoRa Basics™ Modem-E
Technical Paper
October, 2020

semtech.com/LoRa

Page 8 of 12
Proprietary
Semtech

Owner and Token

In order to use the Device & Application Services for a given LoRa Basics Modem-E device, you must create an Application Owner and then create a token for transmitting data to the Device & Application Services.

To create an Application Owner that can use the Device & Application Services, first login to your LoRa Cloud account (https://www.loracloud.com) and select the **LoRa Cloud Device and Application Services**. From the Device & Application Services landing page, select **Manage Owners**. On the **Manage Owners** page you will create an owner or owners and then set the currently-active owner.

Adding Devices

Devices are managed either through the Device & Application Services API or directly from the LoRa Cloud Device & Application Services web portal. The **Manage Devices** link is used to add devices for a specific application owner. The information required to add a device to the list of managed devices is the DevEUI. Devices can be added one at a time or can be added in bulk by submitting a list of the devices to be added.

Routing the data

After the token is created, it will be used in the API to the Device & Application Services for data transfer to and from the service. When you see port 199, send the token to the Device & Application Services.

The Device & Application Services API is implemented as a HTTP RESTful interface supporting GET, PUT, POST and DELETE. Most reports will return the current status. Some inputs to the Device & Application Services require multiple uploads before a complete result is returned, for example, large file uploads. For the cases where multiple uploads are necessary, a simple "UPLINK_RESPONSE" is returned with no data. For further details, see the LoRa Cloud Device & Application services documentation.

The LoRa Cloud Geolocation Service

The LoRa Basics Modem-E has built-in features for geolocation. This information can be sent to the LoRa Cloud Geolocation API for an estimate of the location a device. When gateways receive a data packet transmitted by LoRa Basics Modem-E devices, they also generate metadata such as received signal-strength, signal-to-noise ratio, and time of arrival (TOA) or time difference of arrival (TDOA). When this metadata from the gateways is assembled into a suitable query and transmitted via the LoRa Cloud Geolocation API, the service is able to calculate the location of the device.

Types of Service

There are three localization technologies available: LoRa, Wi-Fi and GNSS. The LoRa method uses signal strength, signal timing and other metadata from the device signals to calculate a location. Similarly, the Wi-Fi method uses the signal strength of Wi-Fi access points within range of the device to estimate the

Understanding LoRa Basics™ Modem-E
Technical Paper
October, 2020

semtech.com/LoRa

Page 9 of 12
Proprietary
Semtech

device's location. Finally, LoRa Basics Modem-E can measure timing information from multiple GNSS satellite sources to estimate the position of a device based on those signals.

Subscription Level and Tokens

There are different subscription levels for the LoRa Cloud Geolocation service. The subscription that best suits your needs will depend on the monthly traffic levels that will be used by a given application. For example, regardless of subscription level, each account will have two default tokens, primary and secondary. The combined traffic associated with both tokens will be accumulated. The accumulated totals will count towards the monthly total. For the free introductory tier, up to 1,000 locations can be computed every month. If you need to compute more than 1,000 locations in a month, paid plans are available. Paid plan subscription levels range from computing hundreds of thousands of locations to many millions. Log in to the LoRa Cloud Portal and see the **Manage Subscriptions** page in the **LoRa Cloud Geolocation** area for further information on pricing plans.

Getting Location Results

To use the LoRa Cloud Geolocation API, you will need scanned information for LoRa signals, Wi-Fi scan or GNSS measurements, provided by the LoRa Basics Modem-E. The LoRa signals and Wi-Fi scan results will be passed to the API with either the primary or secondary token to the v2 API. For the LoRa signals, this can include RSSI and SNR information as well as TDOA information. If TDOA information from encrypted sources is to be passed to the API for processing, it must be decrypted before being sent to the Geolocation API.

GNSS measurements are passed via the Geolocation API v3 interface to the Geolocation Service. The Geolocation Service will process the measurements passed to the API into a location. GNSS performance can be enhanced with GNSS assistance for both timing and satellite almanac accuracy. This GNSS assistance information can be provided through the LoRa Cloud Device & Application Service.

Getting Almanac Data for GNSS Aiding

GNSS operates by utilizing ranging measurements from a satellite to a receiver (in this case a LoRa Basics Modem-E device). The acquisition of the signals can be improved by providing information about the GNSS satellites and the current local conditions. The LoRa Cloud Device & Application Services allow for timing information to be provided to the LoRa Basics Modem-E through the clock synchronization protocol. Additionally, there are two supported levels of almanac assistance for providing GNSS satellite predictions. The two almanacs are the full almanac, and the "efficient" (i.e., compact) almanac. The full almanac is what it claims—it contains the full slate of almanac data. The *efficient* version is optimized for lower communication bandwidth. Over time, the true satellite positions diverge from the fixed almanac parameters, regardless of which almanac you are using. This means that the almanac must be updated regularly. The Device & Application Services are designed to allow for these updates on a regular basis.

Understanding LoRa Basics™ Modem-E
Technical Paper
October, 2020

semtech.com/LoRa

Page 10 of 12
Proprietary
Semtech

Conclusion: The Value of LoRa Basics Modem-E

The LoRa Basics Modem-E is a new operational paradigm that uses a highly-integrated network architecture for using and managing a new generation of IoT products. It seamlessly integrates device provisioning, management, operations and localization into a single set of APIs that are enabled for LoRa Basics Modem-E devices. The combined functionality not only makes integration into your end devices easier, but allows for scalable solutions within a network infrastructure – all with a minimum amount of development. This solution was developed with modern, low power, long range LoRaWAN infrastructure, thus ensuring interoperability and a strong ecosystem of innovation.

Understanding LoRa Basics™ Modem-E
Technical Paper
October, 2020

semtech.com/LoRa

Page 11 of 12
Proprietary
Semtech

Important Notice

Information relating to this product and the application or design described herein is believed to be reliable, however such information is provided as a guide only and Semtech assumes no liability for any errors in this document, or for the application or design described herein. Semtech reserves the right to make changes to the product or this document at any time without notice. Buyers should obtain the latest relevant information before placing order and should verify that such information is current and complete. Semtech warrants performance of its products to the specifications applicable at the time of sale, and all sales are made in accordance with Semtech's standard terms and conditions of sale.

Contact Information

Semtech Corporation
200 Flynn Road, Camarillo, CA 93012
Phone: (805) 498-2111, Fax: (805) 498-3804
www.semtech.com

Understanding LoRa Basics™ Modem-E
Technical Paper
October, 2020

semtech.com/LoRa

Page 12 of 12
Proprietary
Semtech