# LoRaWAN in Depth

Jonathan Brewer
Network Startup Resource Center
jon@nsrc.org



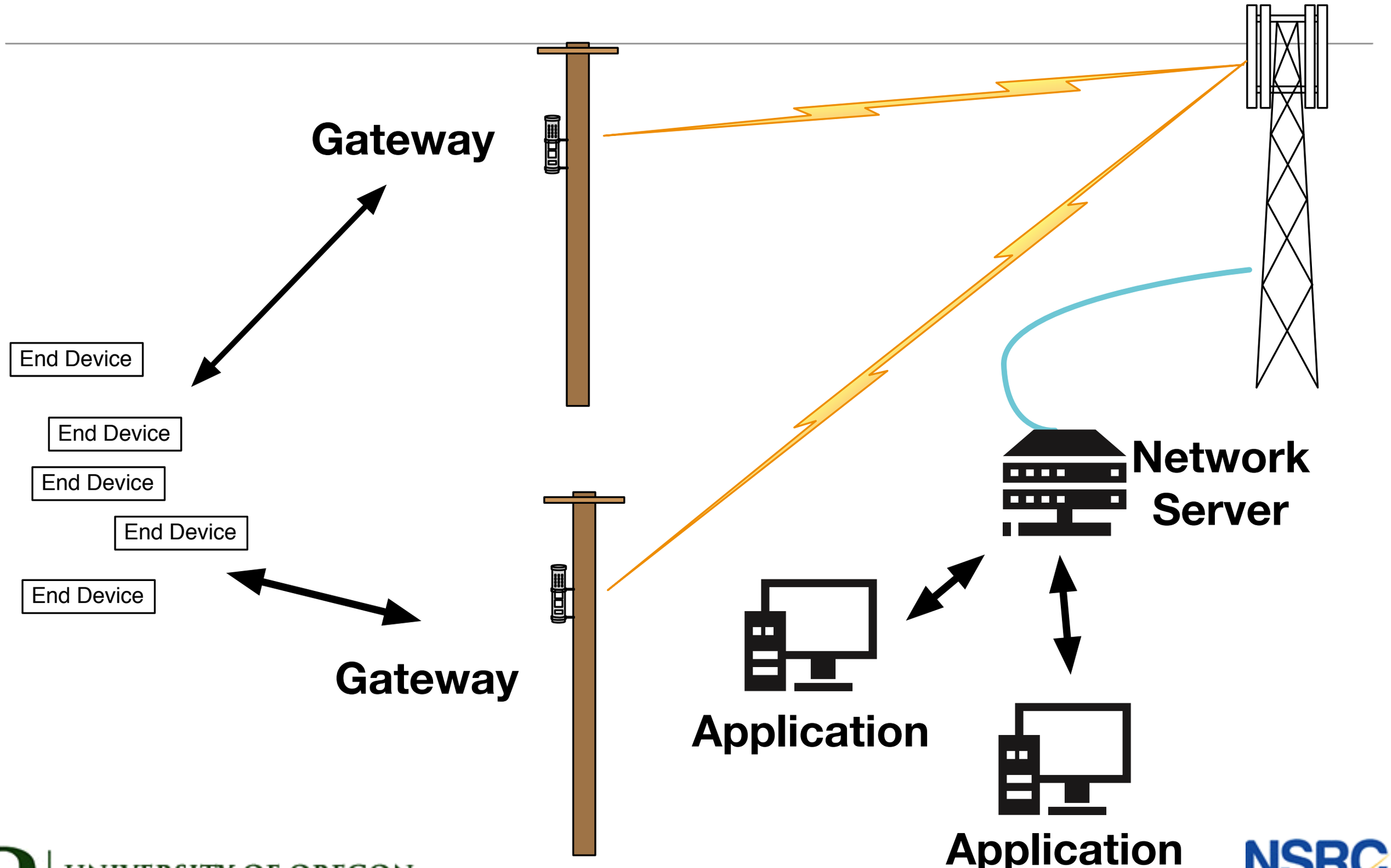
UNIVERSITY OF OREGON

NSRC Network Startup Resource Center

# What is LoRaWAN?

- Wireless Technology for the Internet of Things
- Designed for long range, low power, low data rate
- Supports bi-directional comms, mobility, localisation
- Star topology (not mesh or p2p)
- 0.3-50kbps via adaptive data rate scheme
- Multiple levels of encryption (Network & Application)
- Supports time slot scheduling of device transmission

# LoraWAN Entities



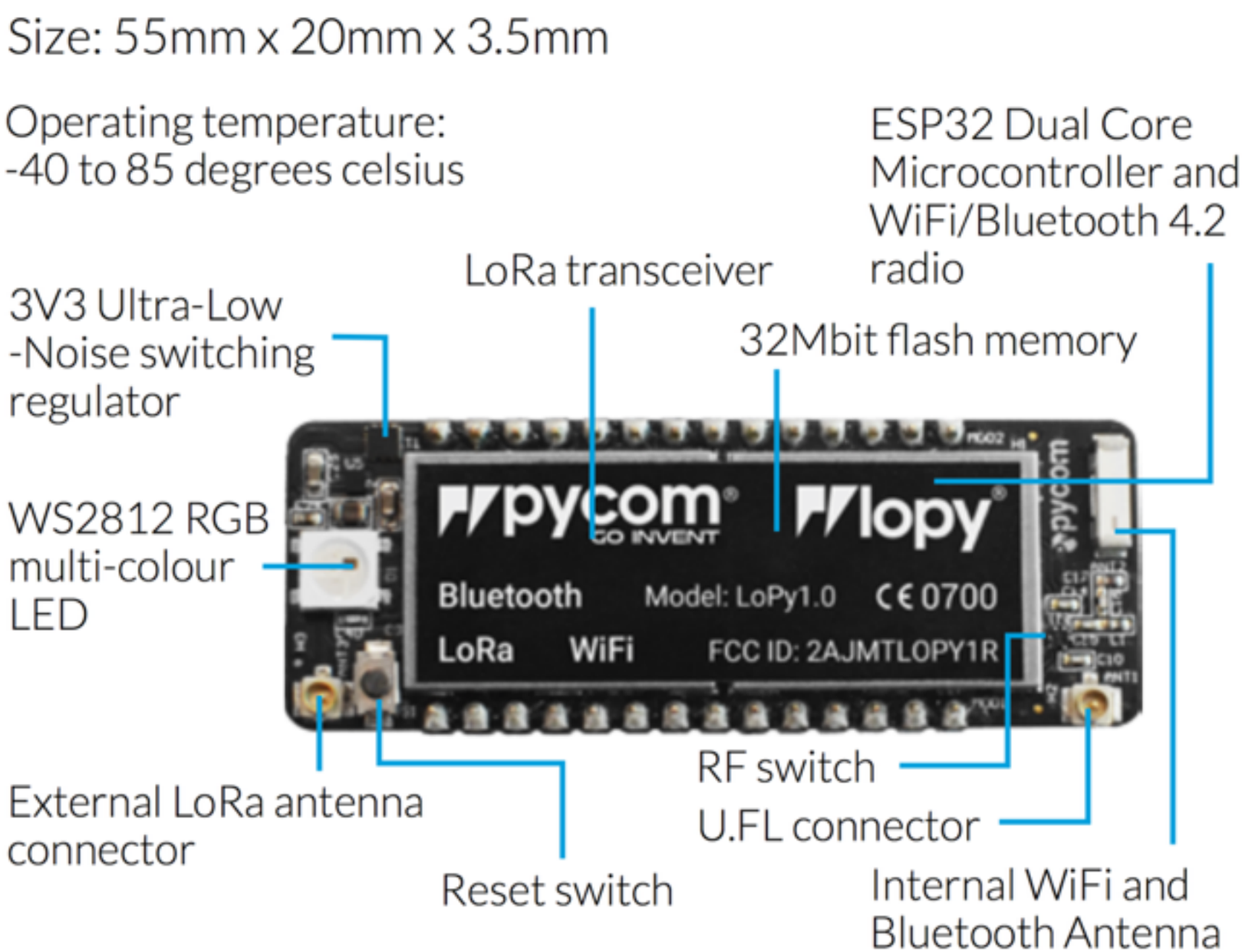
# LoRaWAN Architecture Overview

- Base text sourced from draft-farrell-lpwan-overview
- https://tools.ietf.org/html/draft-ietf-lpwan-overview-07
- Verbatim text is italicised
- Important terms are bolded

# LoRaWAN: End Device

- *a LoRa client device, sometimes called a mote*
- Also sometimes called a node
- *Communicates with gateways*
- And never with other motes or nodes
- Has a globally unique identifier called **DevEUI**
  - In the format of an IEEE EUI64 (64 bit)
- Has a network unique identifier called **DevAddr**
  - Only network unique 32 bit

# LoRaWAN: End Device



# LoRaWAN: Gateway

- *A radio on the infrastructure side*
- *Sometimes called a concentrator or base-station*
- *Communicates with end devices via LoRaWAN*
- *Communicates with a network server via TCP/IP*
- Can co-exist on multi-protocol base stations
- Typically runs a software instance per gateway radio

# LoRaWAN: Gateway



# LoRaWAN: Network Server (NS)

- *The Network Server terminates LoRaWAN MAC layer*
- *for End-Devices connected to the network*
- *It is the centre of the star topology*
- The Network Server decides:
  - which Gateway will talk to which End Device
  - what data rates will be used by End Devices

# LoRaWAN: Network Server (NS)

THE THINGS NETWORK


LORIOT

ResIOT™

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

# LoRaWAN: Join Server (JS)

- *Server on the Internet Side of a Network Server*
- *Processes join requests from end-devices*
- End devices cannot be used without joining a network
- Often combined with the Network Server

# LoRaWAN: Uplink Message

- *Communications from end devices to the network server or application*
- *Received via one or more gateways*
- Uplink Messages received by more than one gateways are de-duplicated by the Network Server

# LoRaWAN: Downlink Message

- *Communications from network server or application*
- *via one gateway*
- *to a single end-device*
- *or a group of end devices*
- Network Server decides which gateway is in the best place to send a downlink message to a particular device.

# LoRaWAN: Application

- *Application layer code running on the end device*
- *Application code running "behind" the network server*
- *Most end devices will run only one application*
  - Identified by a registered IEEE EUI64 value (**AppEUI**)
  - "Applications" typically run on Network Servers
    - Provide for device management
    - Route data to external applications
  - Misleading name: Could be called application router

# LoRaWAN: Encryption

- *All payloads are encrypted*
  - No possibility for attackers to read payloads
  - No possibility for network operator to read payloads
- *and have data integrity*
  - No possibility for changing data in flight
  - No possibility for intercepting & replaying data
- *MAC commands are protected (except frame options)*
  - No possibility for attackers to read metadata

# LoRaWAN: Pre-Joined Devices (**ABP**)

- *End devices must have two symmetric session keys*
- Devices are personalised with AES 128-bit keys
- Network Session Key (**NwkSKey**)
  - Known only by the network operator
  - Protects network metadata
- Application Session Key (**AppSKey**)
  - Common to all End Devices using an Application
  - Known only to the Application Operator

# LoRaWAN: Over the Air Join (**OTAA**)

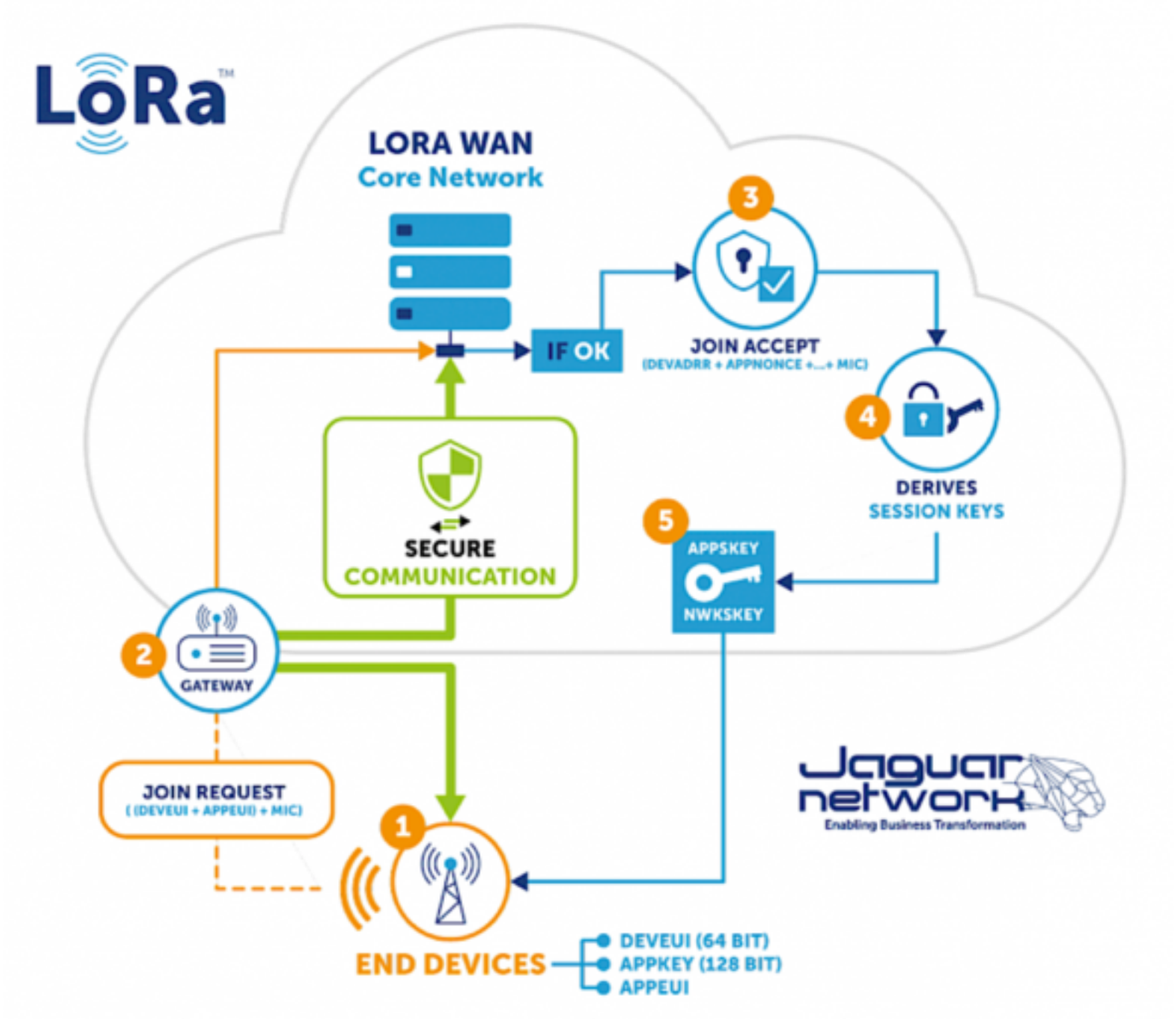
- *End devices must have two symmetric keys*
- Network Session Key (**NwkSKey**)
- Application Key (**AppKey**)
  - Different from the **AppSKey**
  - Unique to every End Device
- Device sends **DevEUI**, **AppEUI**, and **AppKey**
- Network sends data allowing Dev to derive **AppSkey** and **NwkSKey** (then proceed as a pre-joined device)

# LoRaWAN: OTA Join Process

- *LoRa Device sends JOIN_REQUEST (signed with AppKey). The join request contains the following information: AppEUI, DevEUI, DevNonce.*
- *DevNonce is a randomly generated number.*
- *The Network Server receives the JOIN_REQUEST and calculates AppSKey and NwkSKey based on: AppKey, AppNonce, NetID and DevNonce.*
- *As with DevNonce, the AppNonce is another randomly generated number.*
- *Network Server generates JOIN_ACCEPT and includes AppNonce*
- *Device receives JOIN_ACCEPT (encrypted with AppKey). The JOIN_ACCEPT contains the following information: AppNonce, NetID, DevAddr, RFU, RxDely, CFList*
- *Now the Network Server and LoRa device have the same information and the LoRa device can derive the NwkSkey and AppSKey*

http://jensd.be/755/network/lorawan-simply-explained

# LoRaWAN: OTA Join Process




https://www.jaguar-network.com/en/news/lorawan-in-a-nutshell-2-internet-of-things-iot/

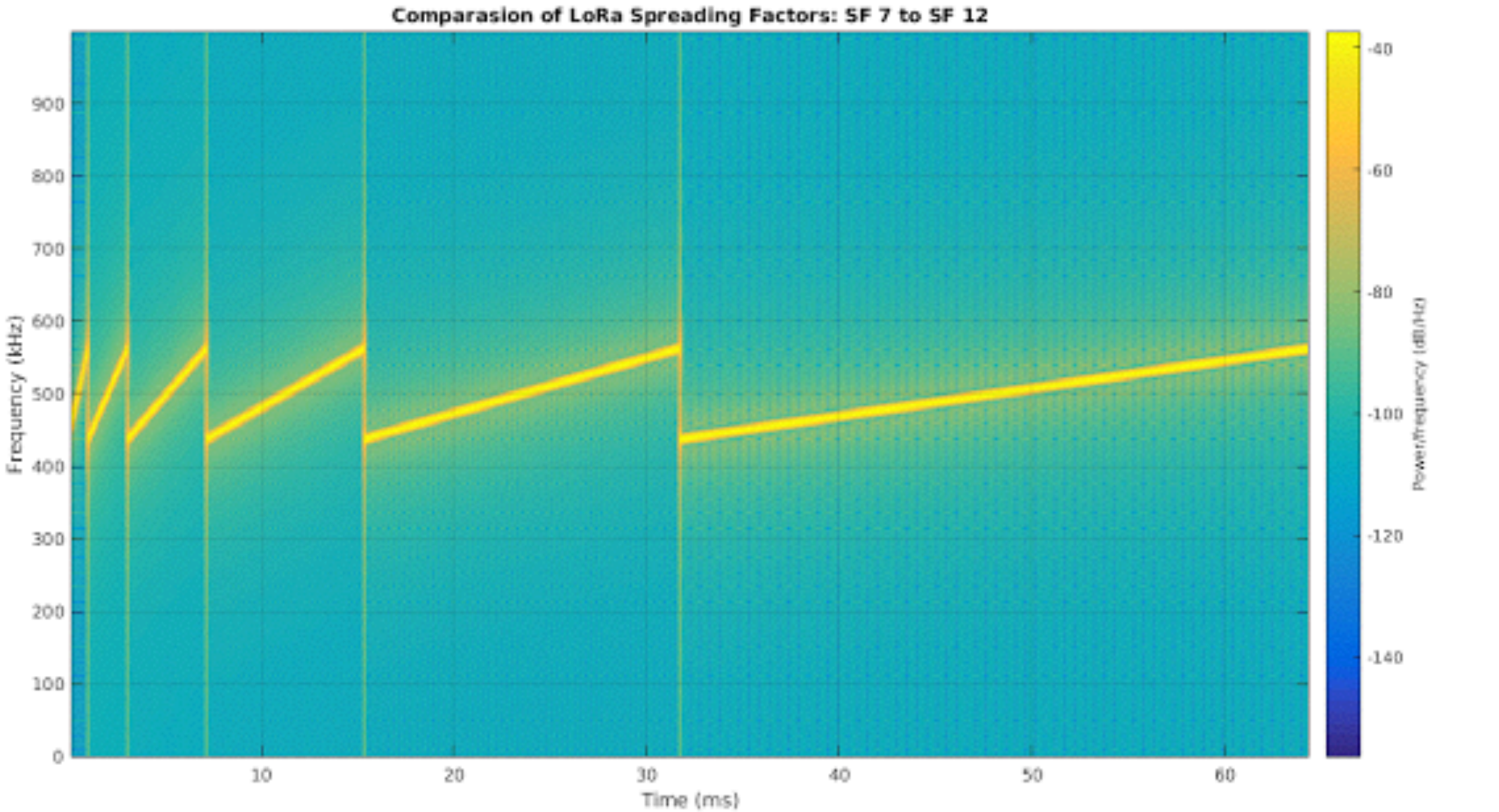
# LoRaWAN: Frequency Bands

- EU 433
- CN 470-510
- CN 779-787
- EU 863-870
- IN 865-867
- US 902-928
- AS 923
- AU 915-928

# LoRaWAN: Chirp Spread Spectrum

- Three Bandwidths Used:
  - 125 KHz
  - 250 KHz
  - 500 KHz
- Six Spreading Factors (SF) Used:
  - SF7 - SF12
  - Each SF step increases air-time by twice

# LoRaWAN: Spreading Factors

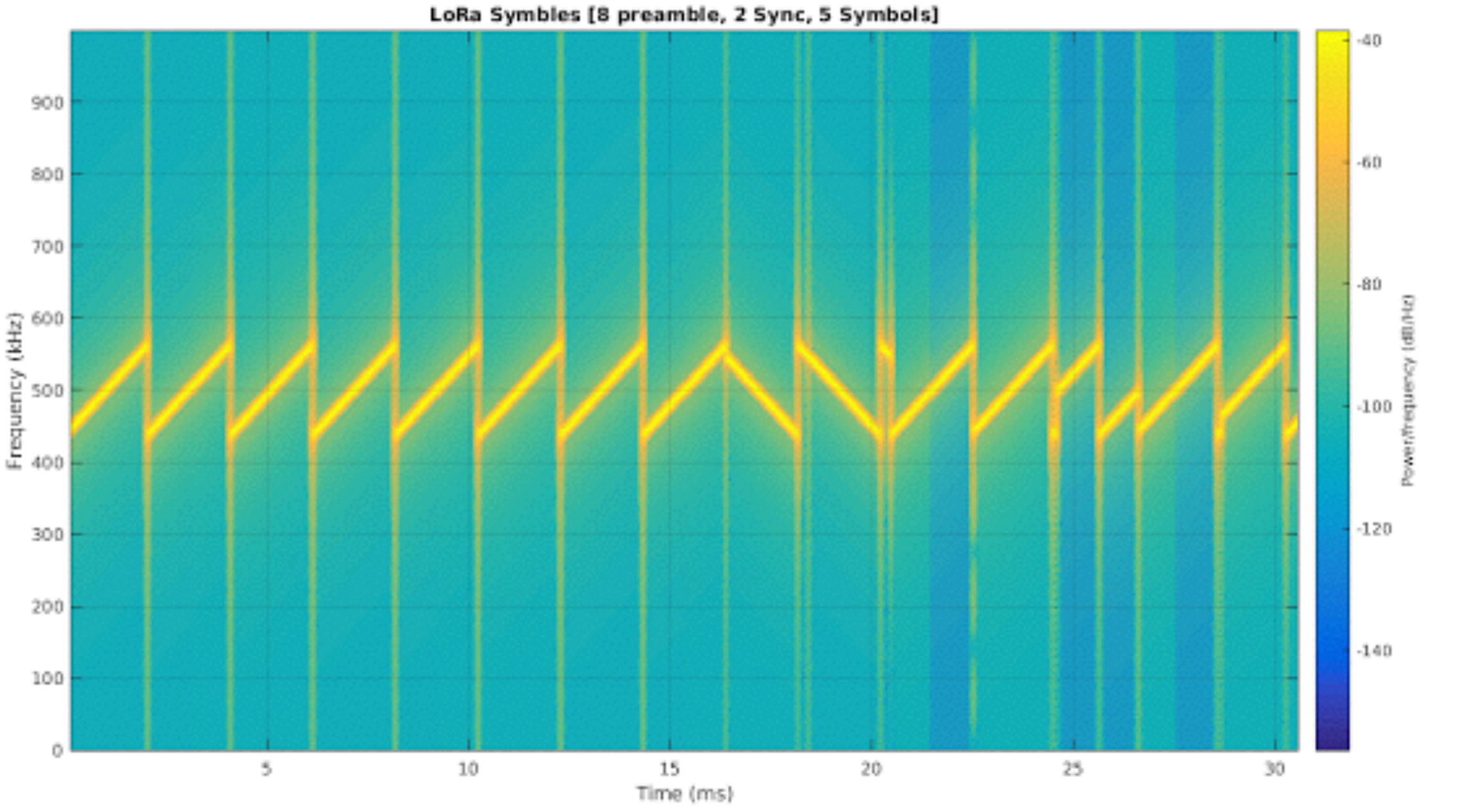



http://www.sghoslya.com/p/lora-is-chirp-spread-spectrum.html

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

# LoRaWAN: Physical Layer Message

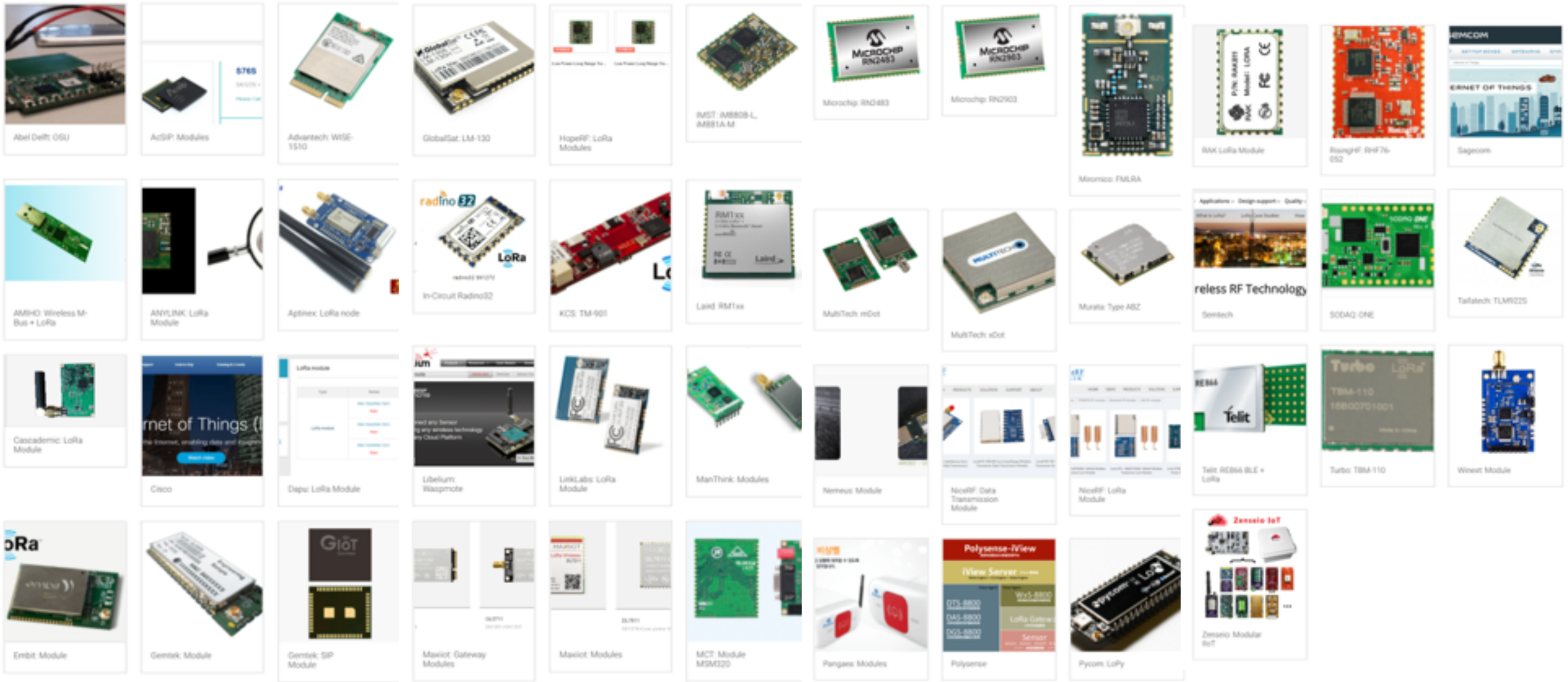



http://www.sghoslya.com/p/lora-is-chirp-spread-spectrum.html

# LoRaWAN: Data Rates

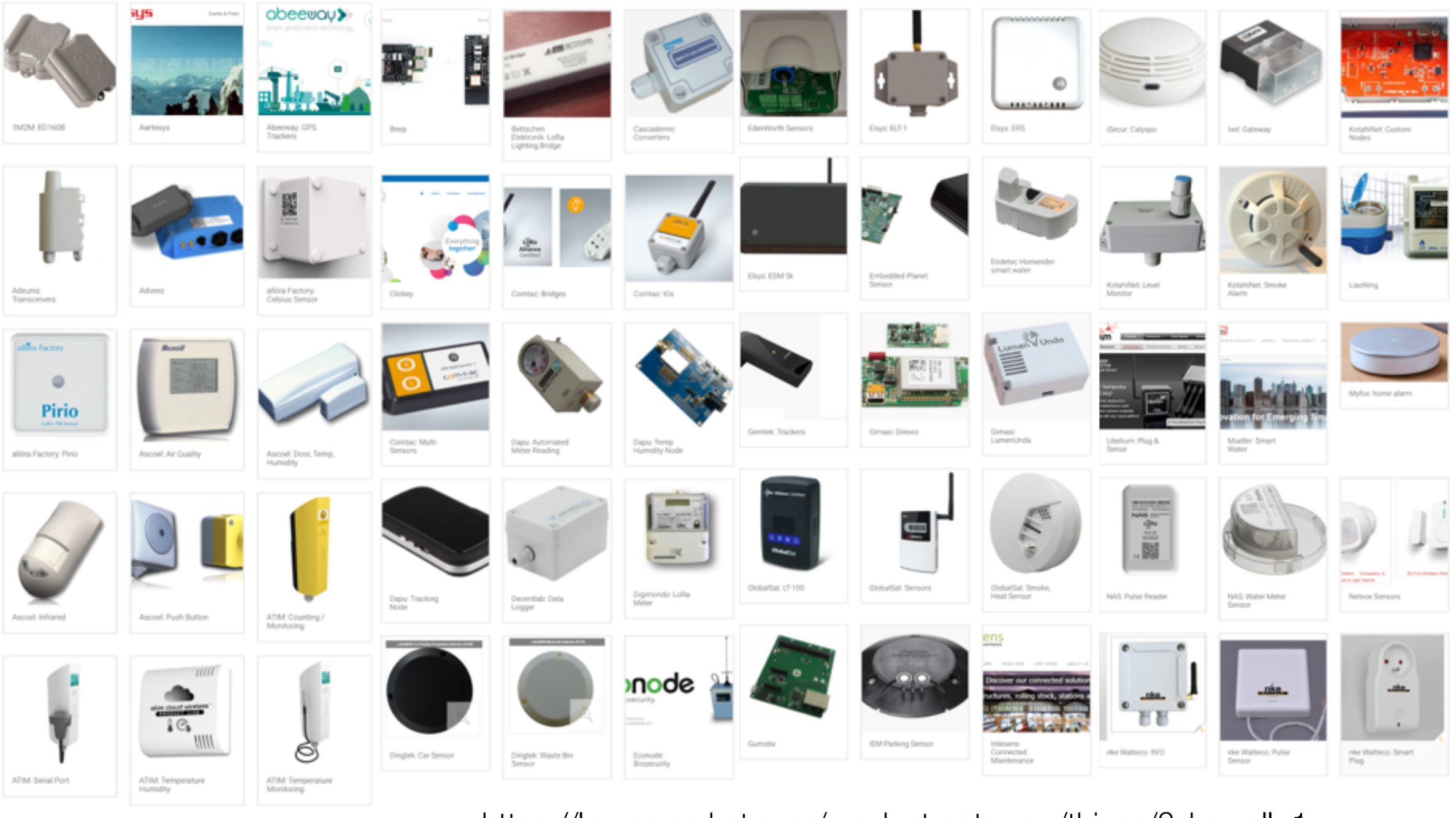
- From Channel Bandwidth * Spreading Factor
- Lowest = SF 12 * 125 KHz = 250 bps
- Highest = SF 7 * 500 KHz = 21.9 kbps
- EU/CN also supports FSK 50 kbps

# LoRaWAN Ecosystem: Modules




https://lpwanmarket.com/product-category/modules/?showall=1

# LoRaWAN Ecosystem: Things




https://lpwanmarket.com/product-category/things/?showall=1

UNIVERSITY OF OREGON

NSRC Network Startup Resource Center

# LoRaWAN Ecosystem: Gateways





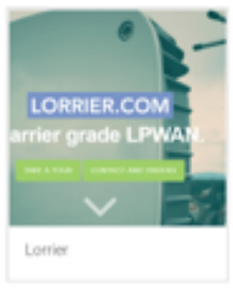






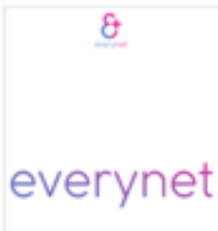























https://lpwanmarket.com/product-category/gateways/?showall=1

# LoRaWAN: Network Servers

- Actility: https://www.actility.com/
- Cable Labs: https://www.loraserver.io/
- EveryNet: http://everynet.com/
- Loriot: https://loriot.io/
- ResIoT: https://www.resiot.io/en/
- The Things Network: https://www.thethingsnetwork.org/

# LoRaWAN: Application Platforms











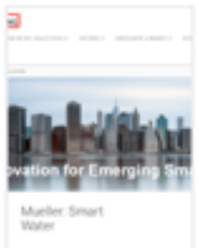








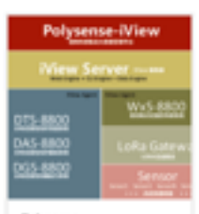





















UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

# LoRaWAN: Selected Platforms

- Actility ThingPark
- Amazon AWS IoT
- EveryNet
- IBM BlueMix
- Microsoft Azure IoT
- MyDevices Cayenne
- OpenChirp
- Stream IoTx