LoRa Alliance™
Wide Area Networks for IoT

LoRaWAN ™ 101

A Technical Introduction

LoRa Alliance™
Wide Area Networks for IoT

LoRa-Alliance.org

Who are the LoRa® Alliance?

- The LoRa® Alliance is an open, non-profit association of members (http://lora-alliance.org/)
- Alliance members collaborate to drive the global success of the LoRaWAN™ protocol
- Mission: to standardize Low Power Wide Area Networks
- “ENABLING THINGS TO HAVE A GLOBAL VOICE”

Strategy Committee
Roadmap & Security

Technical Committee
Specification & feature updates

Marketing Committee
Brand, Media, Trade-shows, Open House

Certification Committee
Test Specs & Accreditation

Specification Updates

- LoraWAN ™ 1.0.0 -> 1.0.1 -> 1.0.2 -> 1.1

- 1.0.2 in final review now, release this quarter
- Clarifications enabling NA certification program to launch
- Moves regional parameters to separate doc
  - Much easier to make progress outside IPR process
  - Rapid increase in number of countries covered
- Adds support for cluster of APAC countries
  - Commands to modify regional freqs & Tx powers

- Specification is free to download now

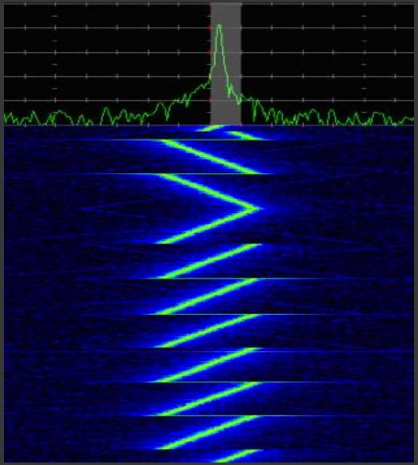
  https://www.lora-alliance.org/Contact/RequestSpecificationForm.aspx

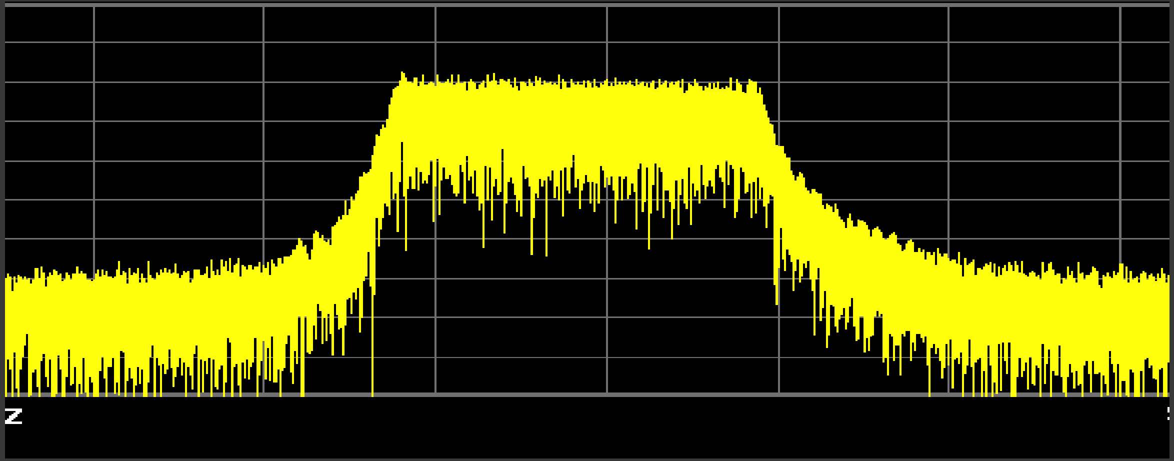
Specification Updates

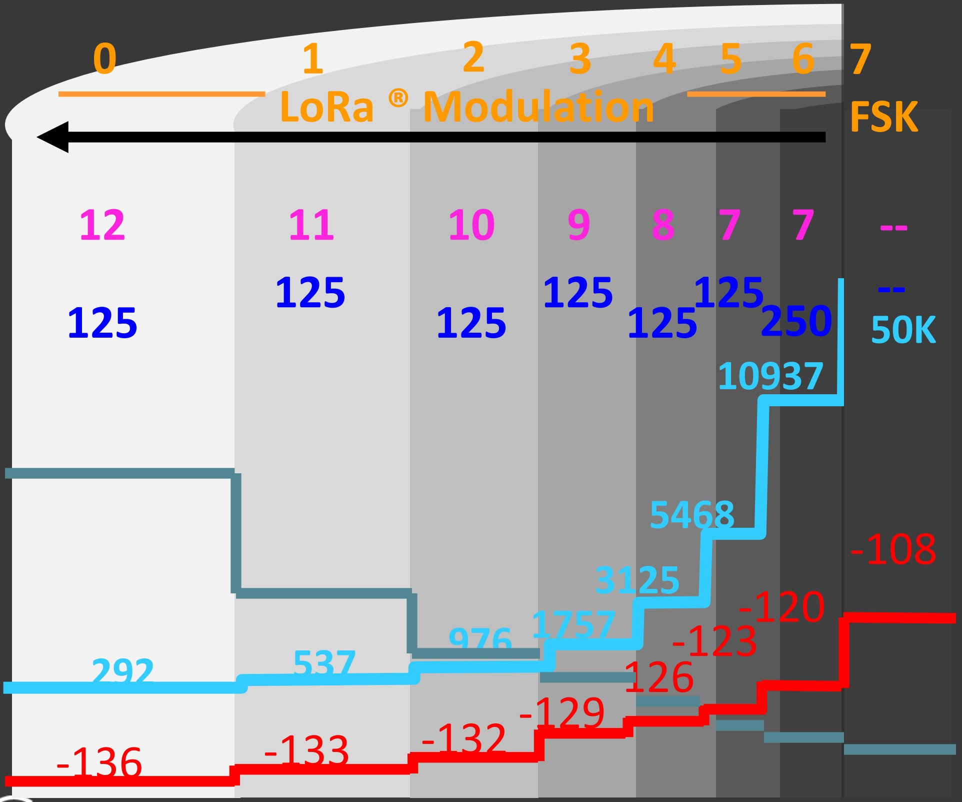
- LoraWAN ™ 1.0.0 -> 1.0.1 -> 1.0.2 -> 1.1

- 1.1 in development, due mid 2017
- Adds:
  - Passive & Handover roaming capabilities
  - Class B clarifications
  - Class A/C temporary switching
- Needs back-end interfaces to standardise
- Alliance is committed to backward compatibility

- A Spread Spectrum Technology
  - Developed by Semtech Corporation (http://www.semtech.com/)
  - Chirped-FM modulation, symbols of ramping frequency
  - Processing gain = increased receive sensitivity
  - Enables longer range at expense of lower data rate







Data Rate (DR)	0	1	2	3	4	5	6	7
Spreading Factor (SF)	12	11	10	9	8	7	7	--
Bandwidth (BW) (kHz)	125	125	125	125	125	125	250	--
Bitrate (BR) (bps)	292	537	976	1757	3125	5468	10937	50K
Receive Sensitivity (dBm)	-136	-133	-132	-129	126	-123	-120	-108

Data Rate (DR)

Range

Spreading Factor (SF)

Bandwidth (BW) (kHz)

Bitrate (BR) (bps)

Receive Sensitivity (dBm)

Time-on-air & consumption

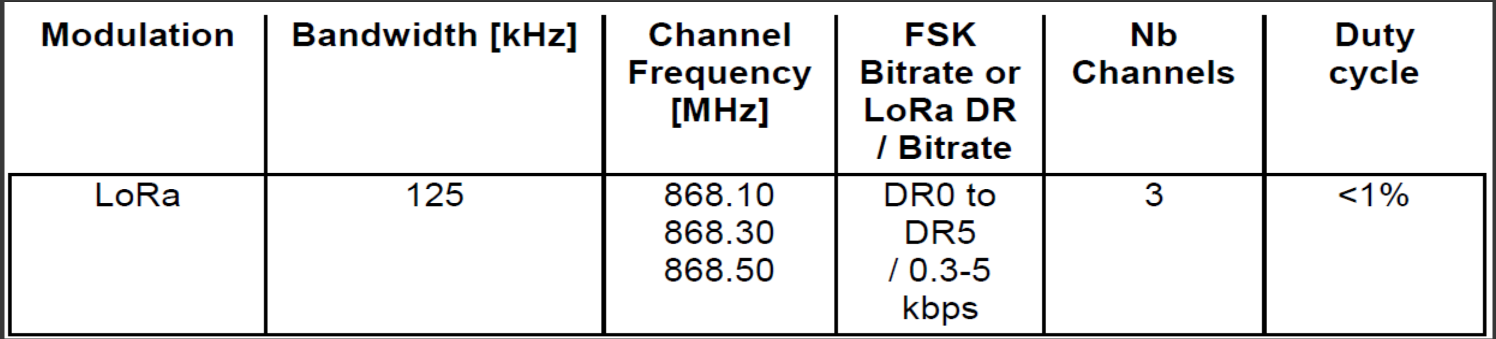
LoRa Alliance™
Wide Area Networks for IoT

LoRa-Alliance.org

ADR = Adaptive Data Rate

- LoRaWAN can auto-magically manage SF for each end-device:
  - To optimize for fastest data rate versus range
  - For maximize battery life, and
  - Achieves maximum network capacity

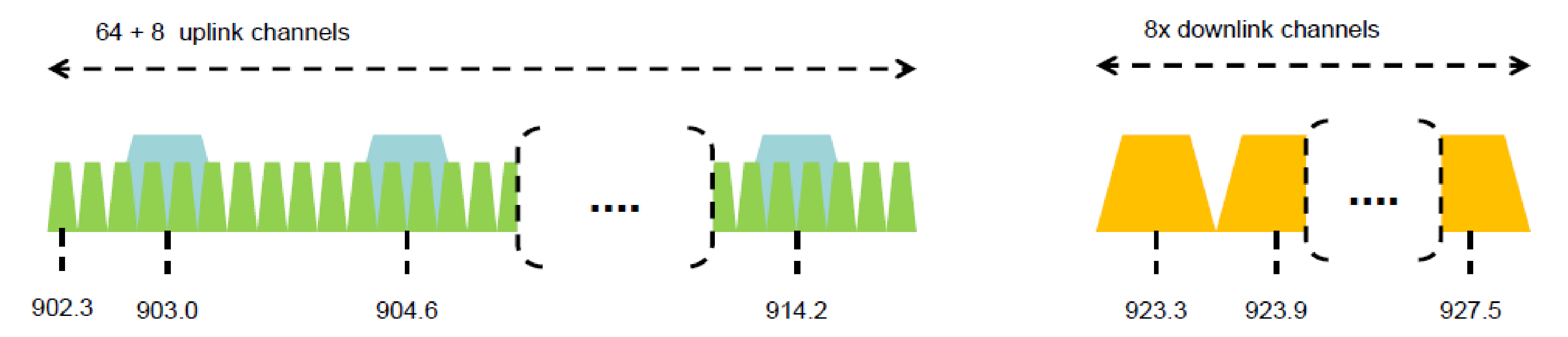
- License free Sub-GHz Frequencies
  - Europe: 868 MHz Band
  - Network channels can be freely attributed by the network operator
  - 3 mandatory channels that all gateways should constantly receive:



Modulation	Bandwidth [kHz]	Channel Frequency [MHz]	FSK Bitrate or LoRa DR / Bitrate	Nb Channels	Duty cycle
LoRa	125	868.10 868.30 868.50	DR0 to DR5 / 0.3-5 kbps	3	<1%

  - EU gateways are typically using 8 channels
  - End-devices must be capable of at least 16 channels

- License free Sub-GHz Frequencies
  - North America: 915 MHz Band
  - Upstream: 64 channels numbered 0 to 63, DR0 to DR3
  - Upstream: 8 channels numbered 64 to 71, DR4
  - Downstream: 8 channels numbered 0 to 7, DR8 to DR13



- Low Power Wide Area Network (LPWAN)
  - Bidirectional, acknowledged
  - Simple Star Network Topology
  - Low data rate
  - Low cost
  - Long battery life
  - Long Range

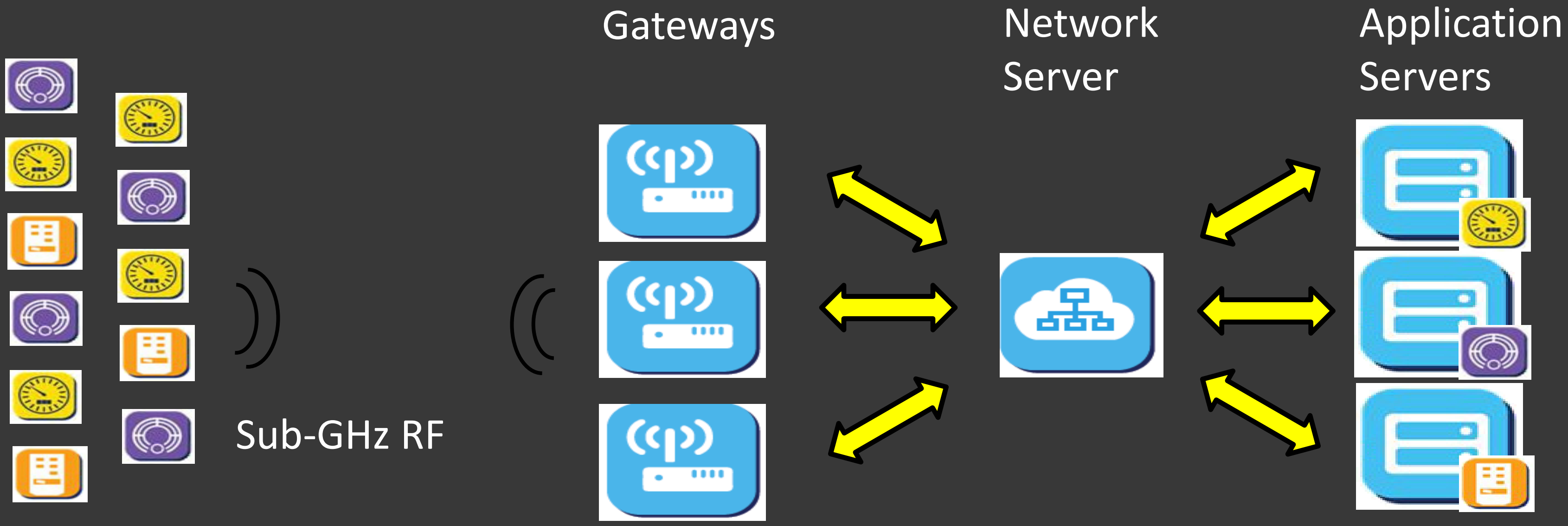
Enables simpler network architecture:

- ***No repeaters***
- ***No mesh routing complexity***

- Ideal for:
  - Internet of Things (IoT) & Machine-to-Machine (M2M)
  - Industrial Automation
  - Low Power Applications
  - Battery Operated Sensors
  - Smart City, Agriculture, Metering, Street lighting

http://lora-alliance.org/What-Is-LoRa/Technology

LoRaWAN™ Network Topology



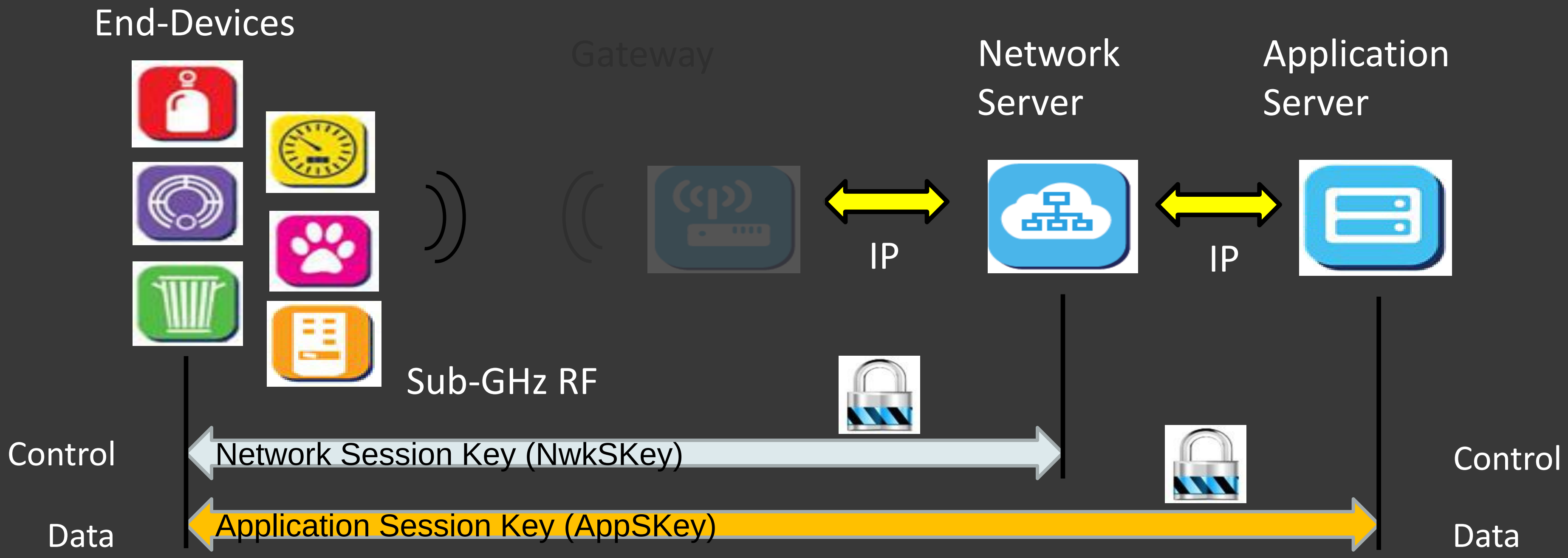
LoRa Alliance™
Wide Area Networks for IoT

LoRa-Alliance.org

LoRaWAN™ Network Protocol Security

- Based on 802.15.4 Security
  - AES-128
- Enhancements:
  - Network Session Key (NwkSKey)
  - Application Session Key (AppSKey)

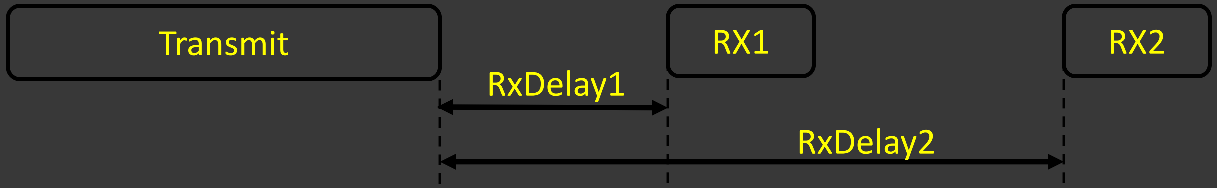
Logical Data Flow (Programmer's Model)



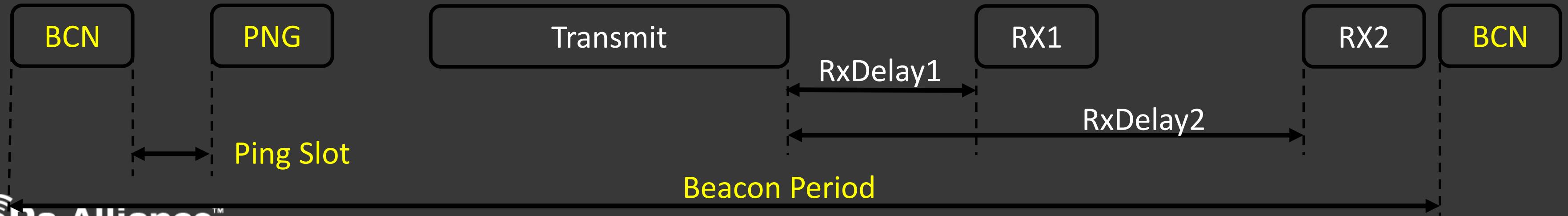
LoRa Alliance™
Wide Area Networks for IoT

- Each end-device class has different behavior depending on the choice of optimization:
  - Battery Powered – Class A
  - Low Latency – Class **B**
  - No Latency – Class **C**

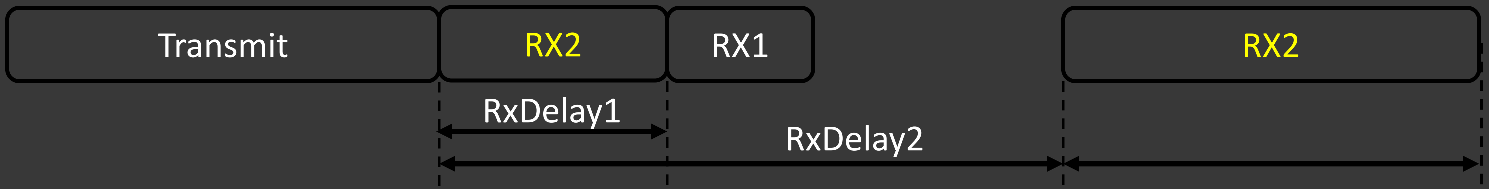
- Battery Powered – Class A
  - Bidirectional communications
  - Unicast messages
  - Small payloads, long intervals
  - End-device initiates communication (uplink)
  - Server communicates with end-device (downlink) during predetermined response windows:



- Low Latency – Class B
  - Bidirectional with scheduled receive slots
  - Unicast and Multicast messages
  - Small payloads, long intervals
  - Periodic beacon from gateway
  - Extra receive window (ping slot)
  - Server can initiate transmission at fixed intervals



- No Latency – Class C
  - Bidirectional communications
  - Unicast and Multicast messages
  - Small payloads
  - Server can initiate transmission at any time
  - End-device is constantly receiving



Extends RX2 until next TX

- Before an end-device can communicate on the LoRaWAN network, it must be activated
- The following information is required:
  - Device Address (DevAddr)
  - Network Session Key (NwkSKey)
  - Application Session Key (AppSKey)

Let’s mention each of these in detail…

- Device Address (DevAddr)
  - 32-bit identifier
  - Unique within the network
  - Present in each data frame
  - Shared between End-device, Network Server, and Application Server
- Differentiates nodes within the network, allowing the network to use the correct encryption keys and properly interpret the data

- Network Session Key (NwkSKey)
  - 128-bit AES encryption key
  - Unique per end-device
  - Shared between End-device and Network Server
- Provides message integrity for the communication
- Provides security for end-device to Network Server communication

- Application Session Key (AppSKey)
  - 128-bit AES encryption key
  - Unique per end-device
  - Shared between End-device and Application Server
  - Used to encrypt / decrypt application data messages
- Provides security for application payload

- To exchange this information, two activation methods are available:

Over-the-Air Activation (OTAA)

- Based on Globally Unique Identifier
- Over the air message handshaking

Activation By Personalization (ABP)

- Shared keys stored at production time
- Locked to a specific network

Over-the-Air-Activation (OTAA)

- End-device transmits Join Request to application server containing:
  - Globally unique end-device identifier (DevEUI)
  - Application identifier (AppEUI)
  - Authentication with Application key (AppKey)
- End-device receives Join Accept from application server

(continued…)

Over-the-Air-Activation (OTAA)

- End-device authenticates Join Accept
- End-device decrypts Join Accept
- End-device extracts and stores Device Address (DevAddr)
- End-device derives:
  - Network Session Key (NwkSKey)
  - Application Session Key (AppSKey)

Security Keys

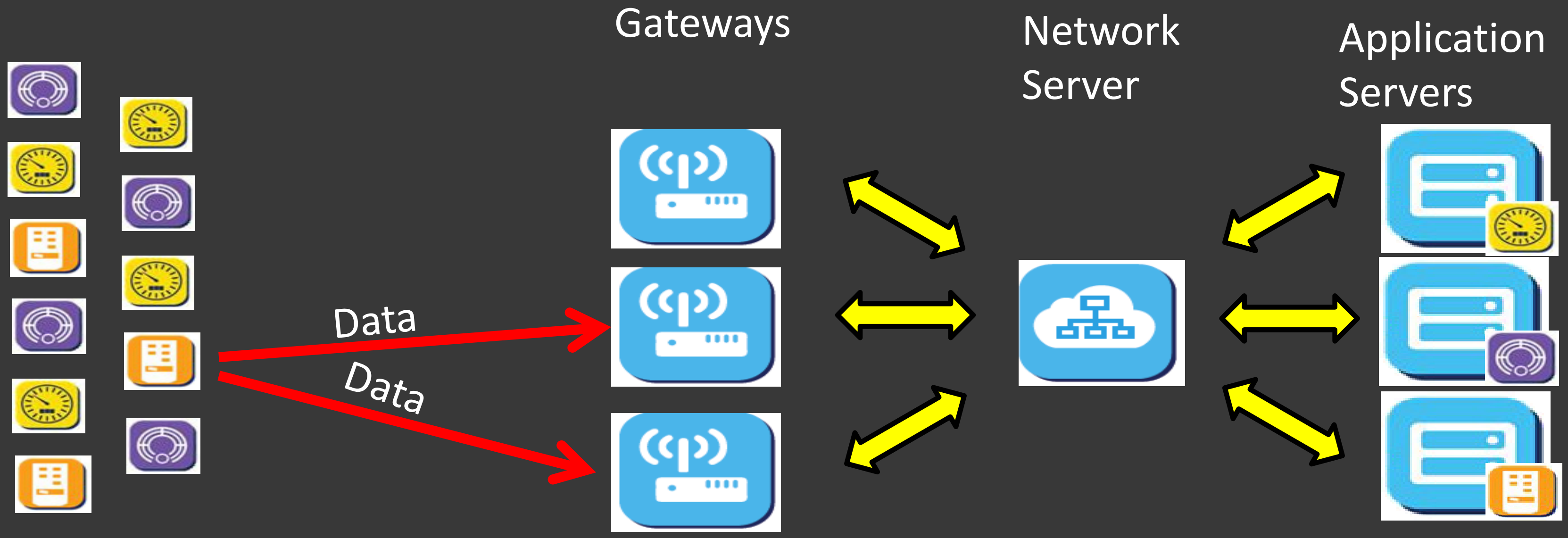
LoRa Alliance™
Wide Area Networks for IoT

LoRa-Alliance.org

Activation By Personalization (ABP)

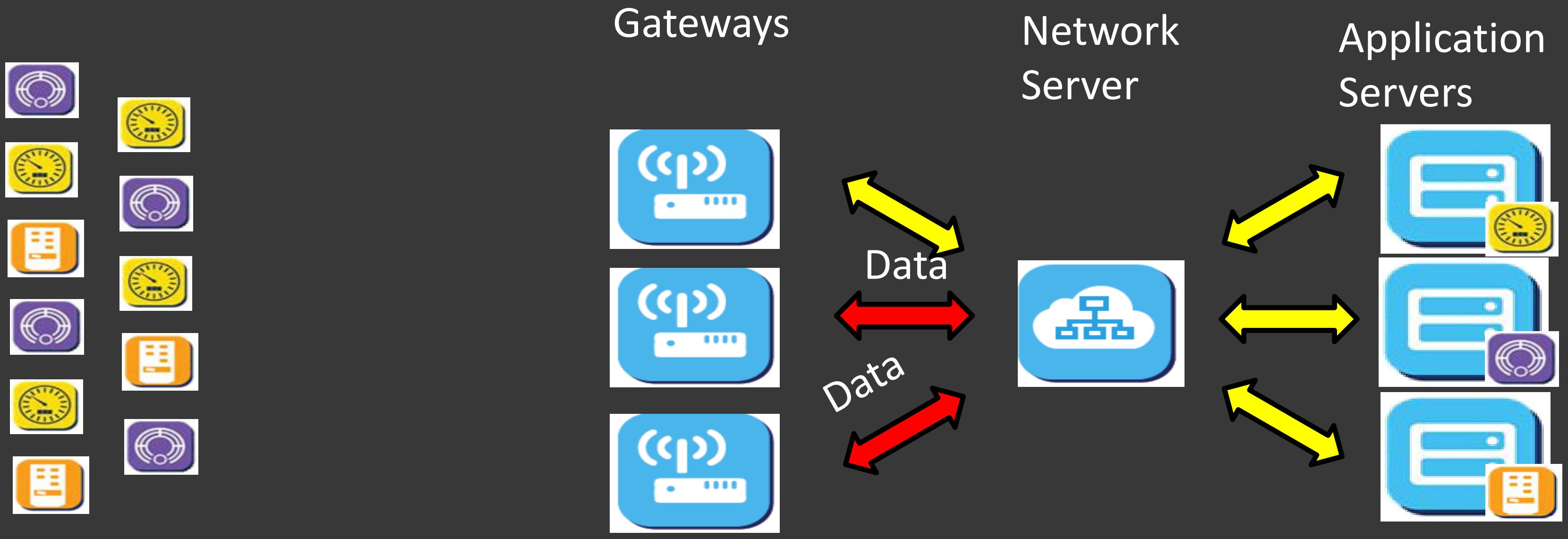
- The following information is configured at production time:
  - Device Address (DevAddr)
  - Network Session Key (NwkSKey)
  - Application Session Key (AppSKey)
- No over the air handshaking
- Device is ready to communicate on the network without any additional procedure.

Confirmed-Data Message



1. Vending Machine transmits data. It is received by two Gateways.

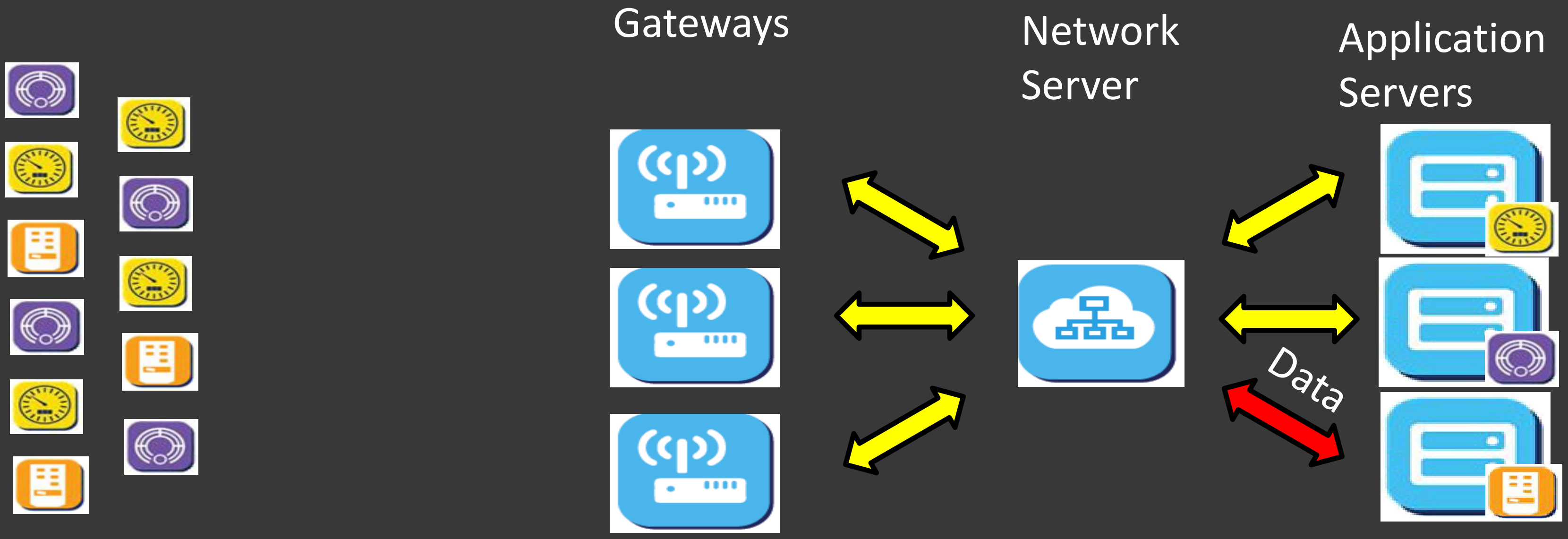
Confirmed-Data Message



2. Both gateways “pass through” the data to the Network Server.

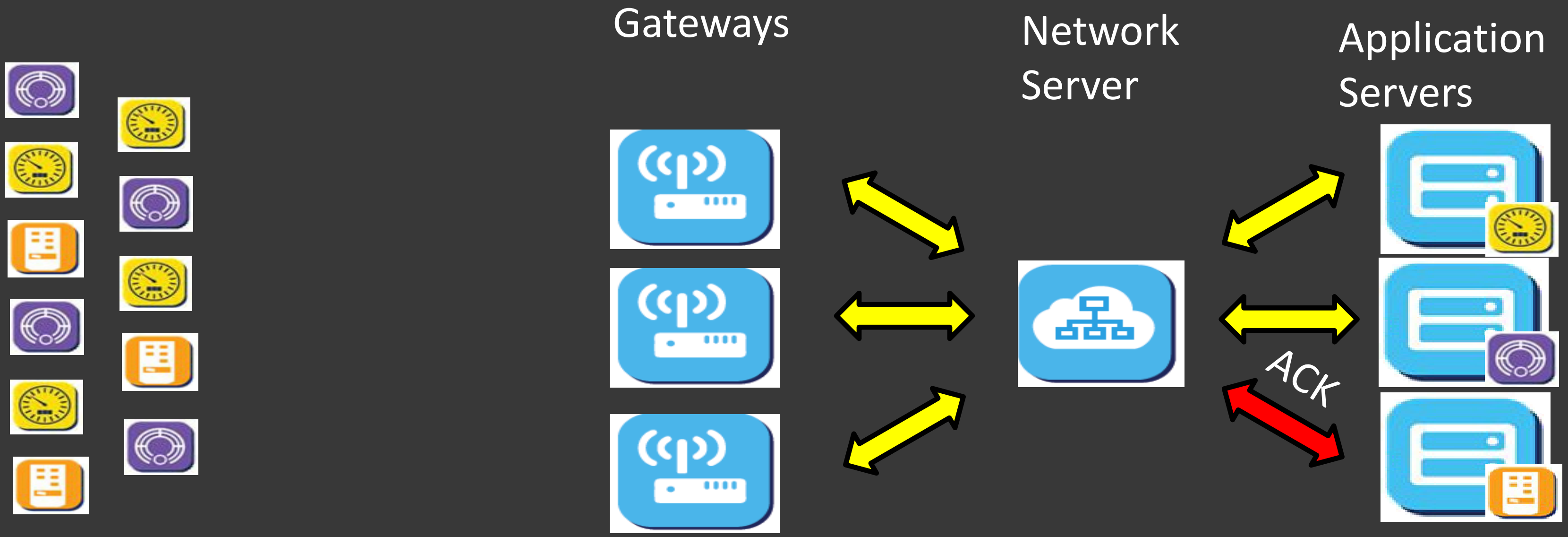
LoRa Alliance™
Wide Area Networks for IoT

Confirmed-Data Message



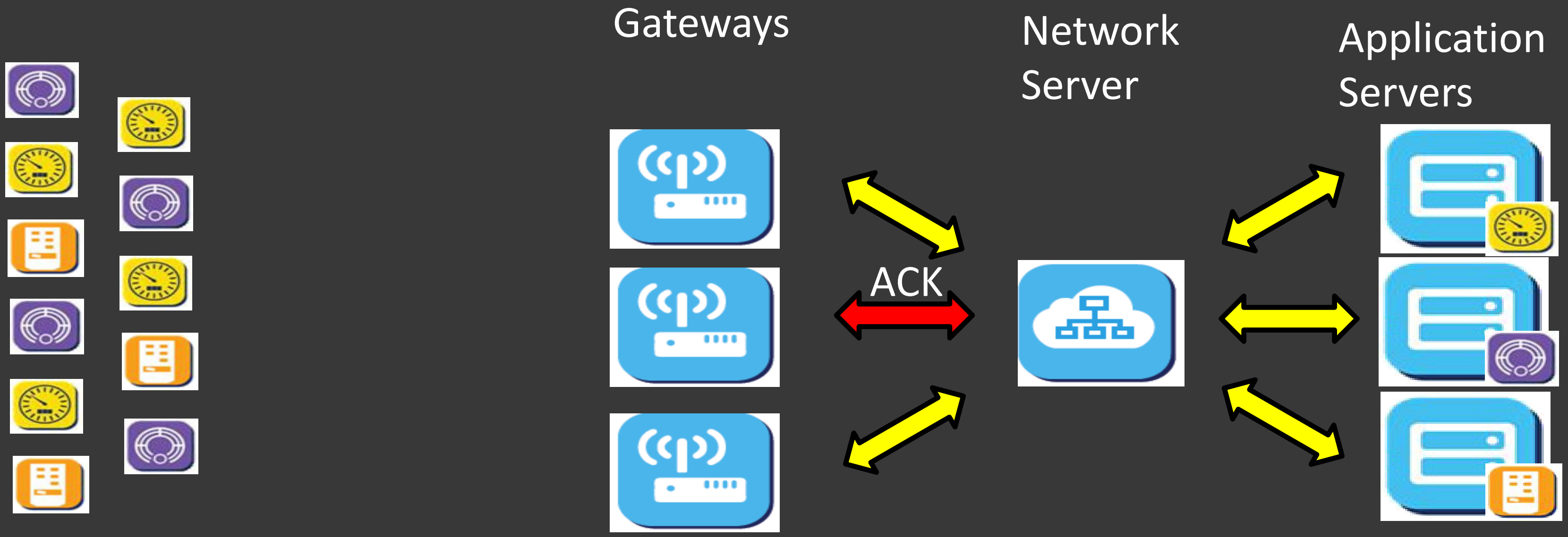
3. The Network Server forwards the data to the Vending Machine Applications Server

Confirmed-Data Message



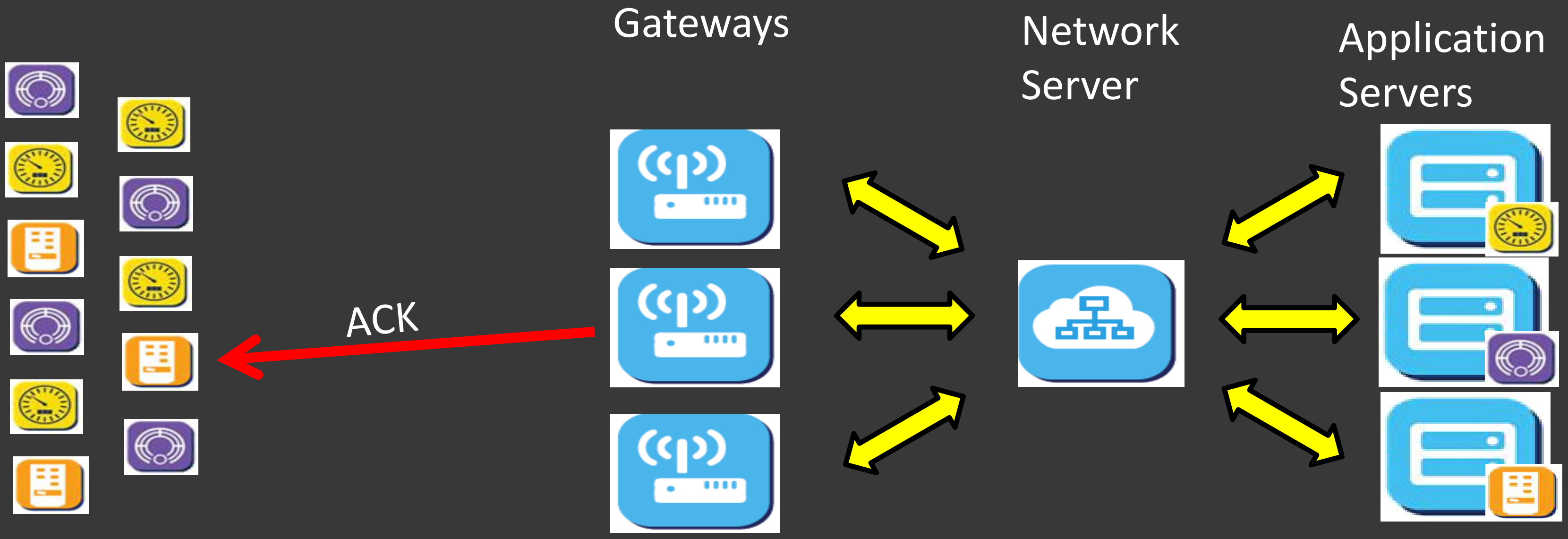
4. The Vending Machine Applications Server sends an acknowledgement

Confirmed-Data Message



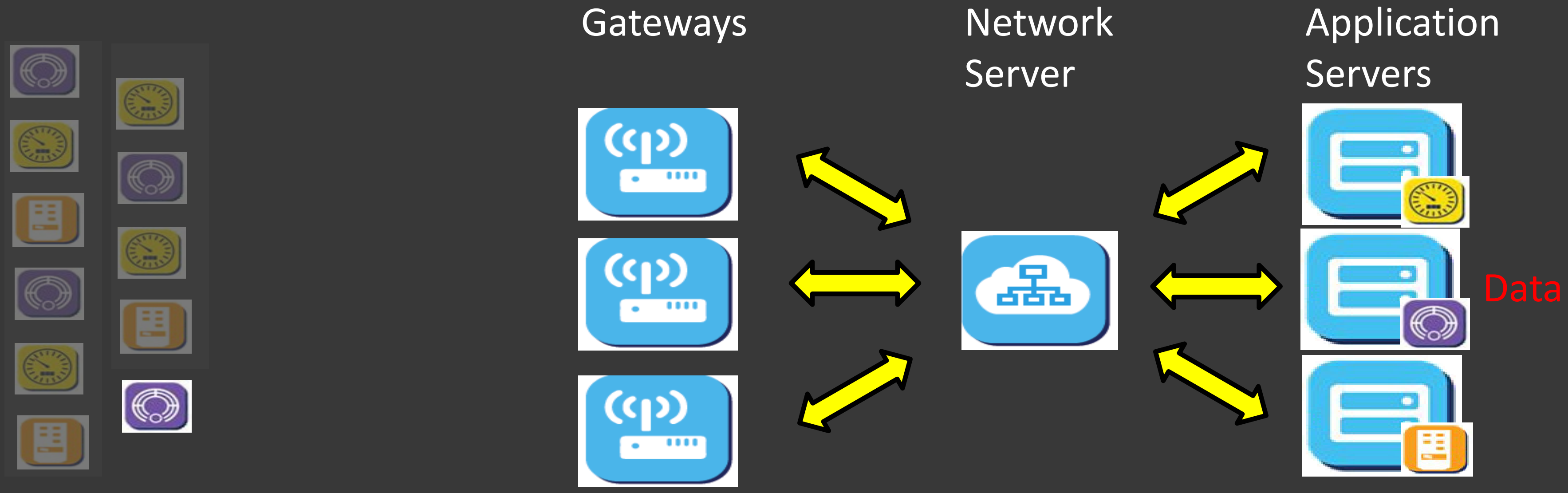
5. The Network Server selects the best path (gateway) to transmit the acknowledgement to the end-device.

Confirmed-Data Message



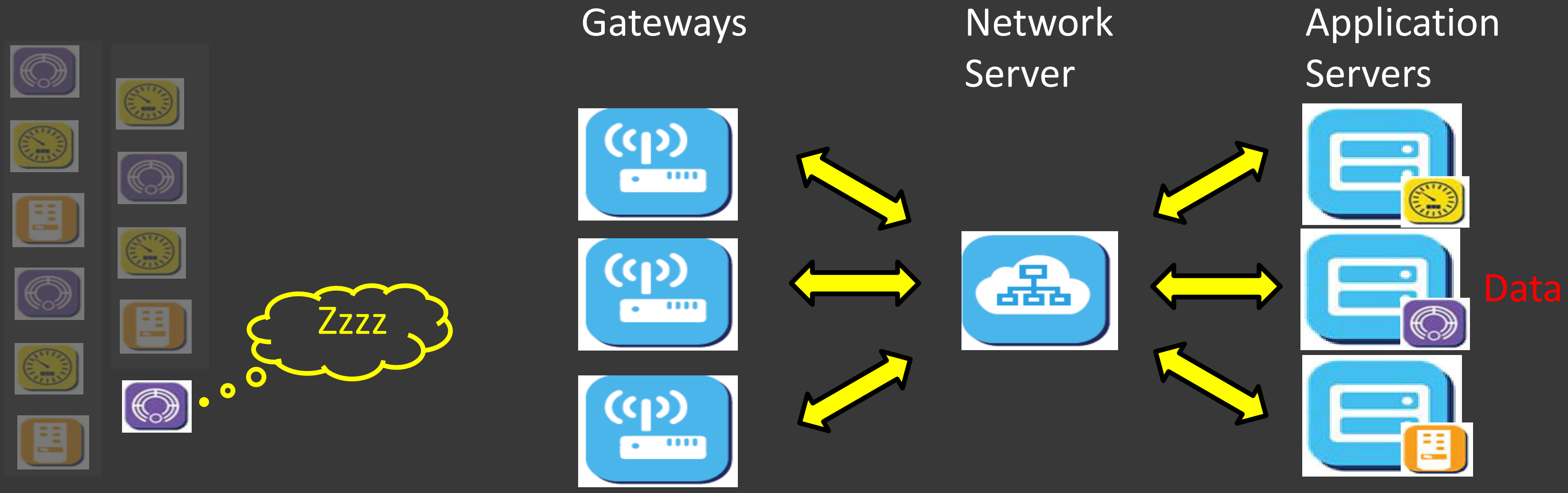
6. The Gateway transmits the acknowledgement to the end-device

Application Server Data Message



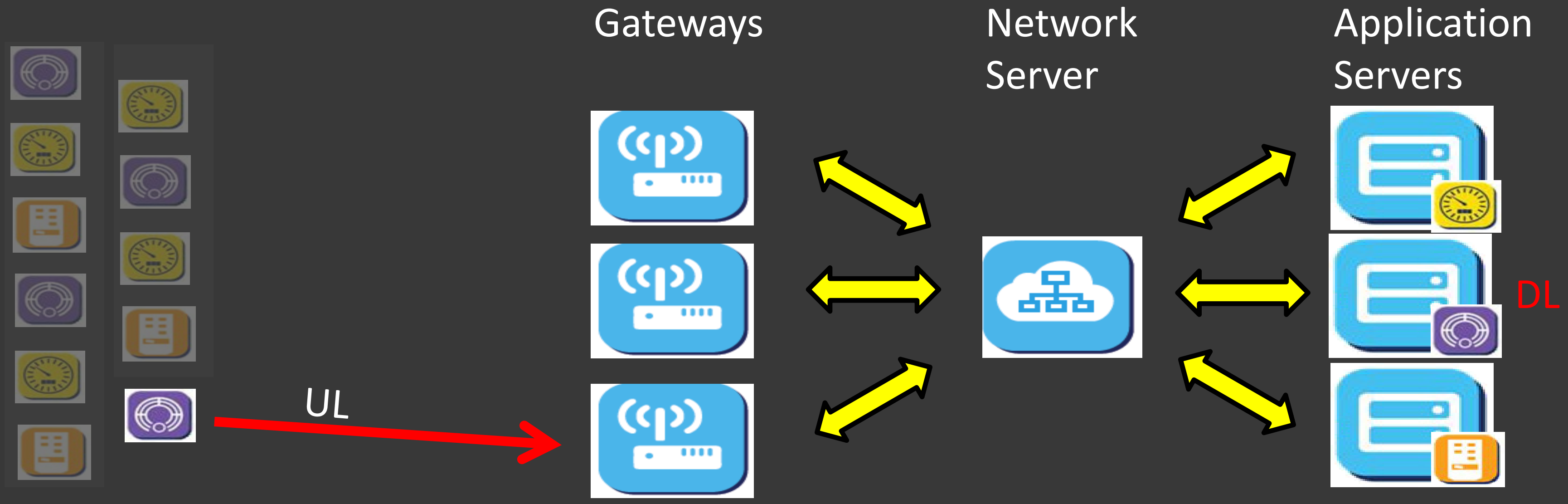
1. The Smoke Detector Application Server has Data for the highlighted Smoke Detector

Application Server Data Message



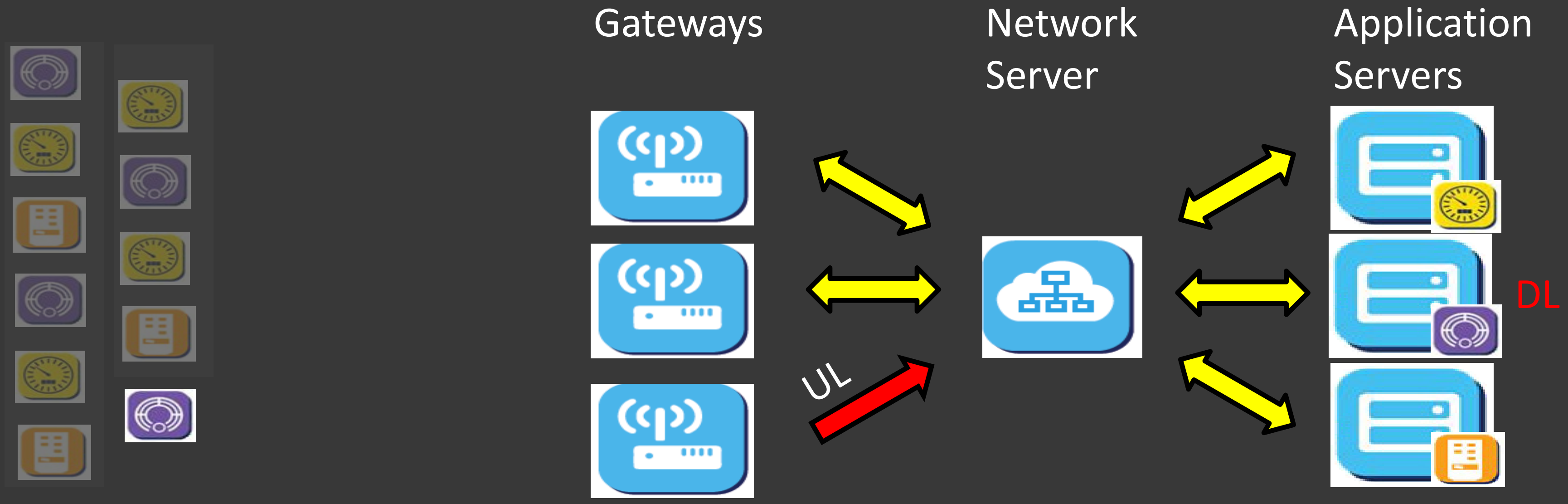
2. However, it has to wait until the Smoke Detector wakes up and transmits a Data Message

Application Server Data Message



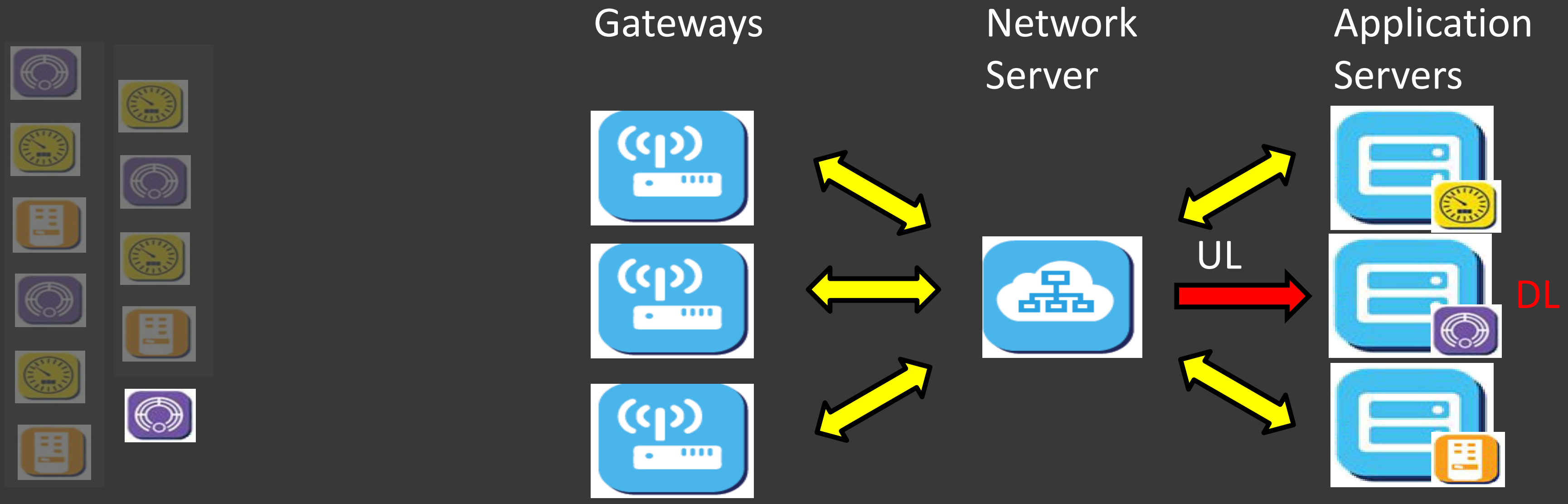
3. When the Smoke Detect transmits, the Data Message moves Upstream

Application Server Data Message



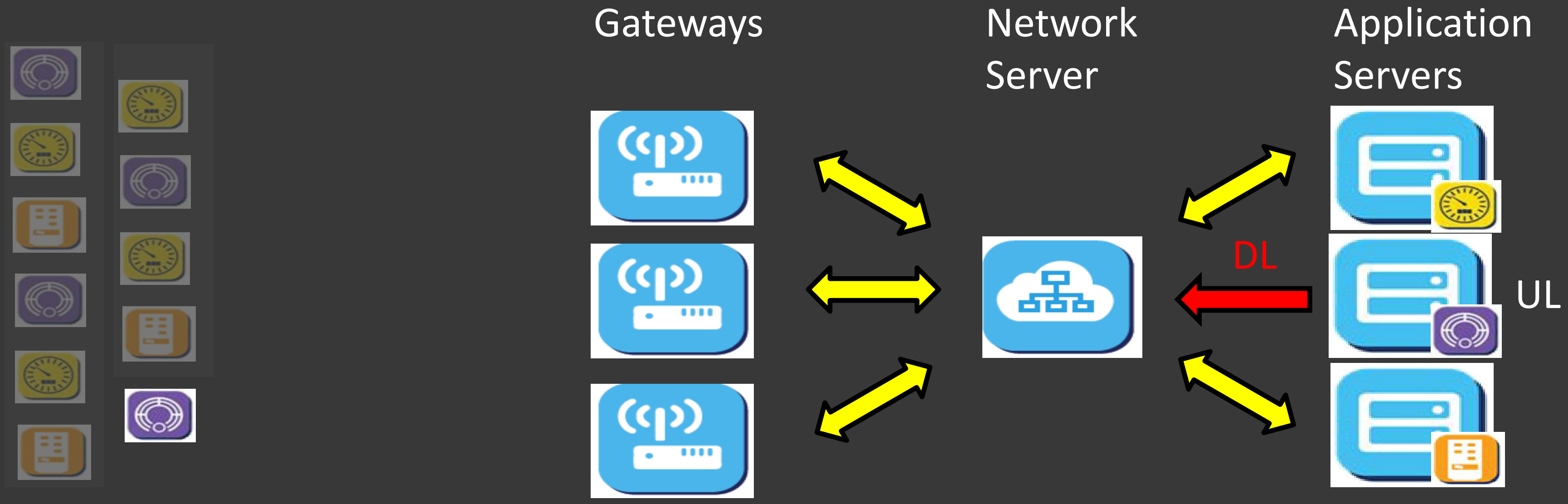
4. Passed through the Gateway…

Application Server Data Message



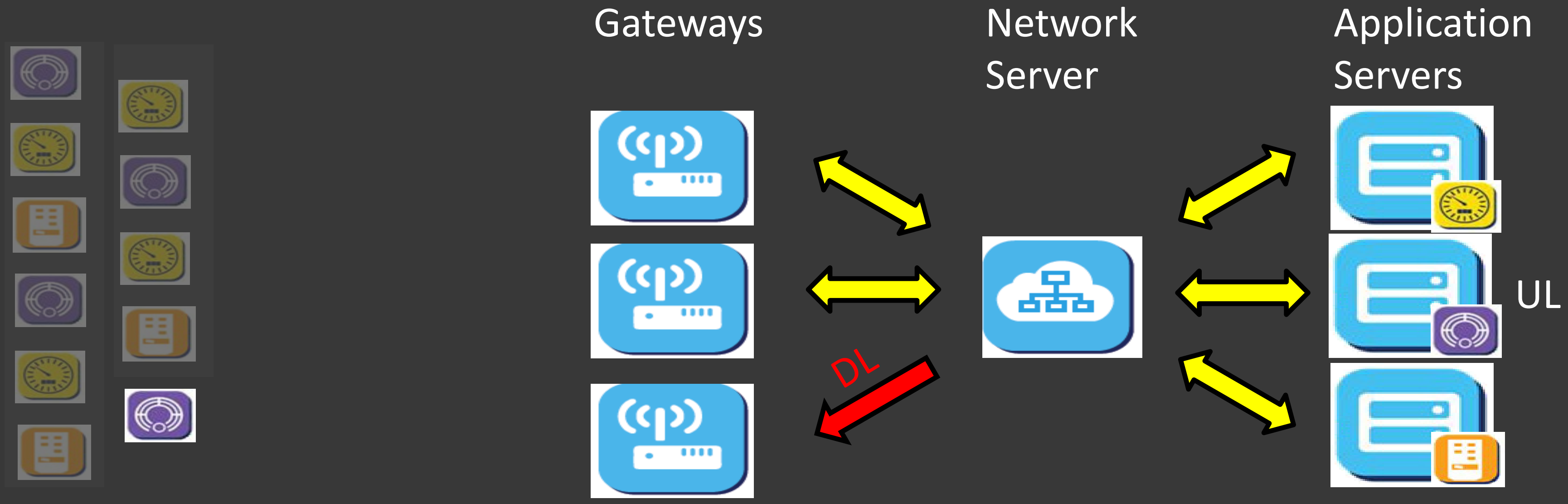
5. … and the Network Server sends to the Smoke Detector Application Server.

Application Server Data Message



6. The Smoke Detector Application Server can now send the data message to the Smoke Detector.

Application Server Data Message



7. The Network Server sends the Data Message to the appropriate Gateway.

LoRa Alliance™
Wide Area Networks for IoT

Thank you, come and join us…

The LoRa Alliance ™

“ENABLING THINGS TO HAVE A GLOBAL VOICE”

LoRa Alliance™
Wide Area Networks for IoT

LoRa-Alliance.org