OpenWeave
Pairing

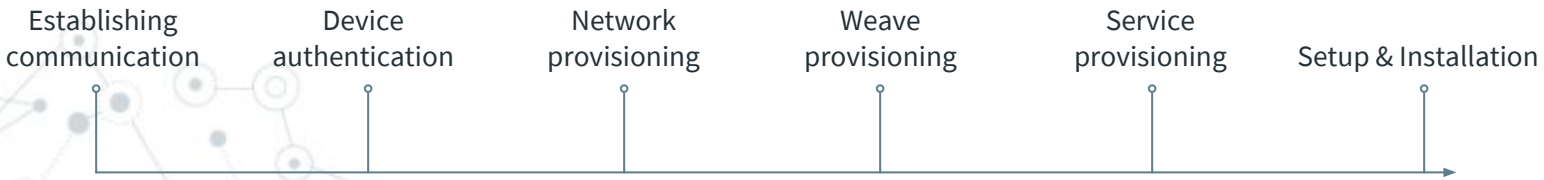
Pairing

Pairing, or out of box (OOB), is the process of setting up and configuring a device for a user

Weave provisioning is a key aspect of the pairing flow

Weave creates a virtual private network between the devices in the home

This network is called a Weave fabric



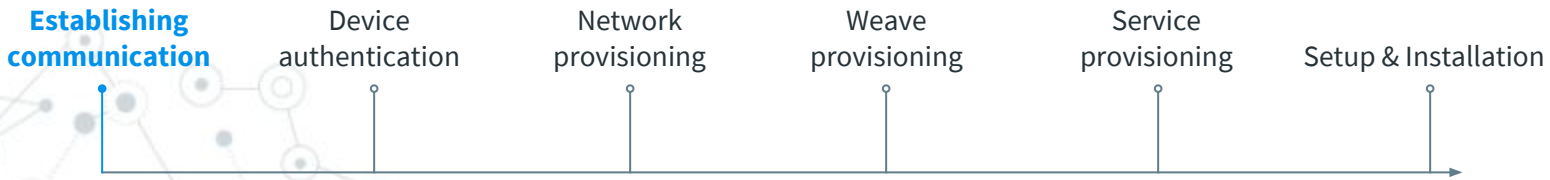
Establishing Device Communication

The first step is to establish communication with the new device. The rendezvous protocols have several mechanisms depending on the hardware capabilities of that device.

The Pairing process and protocols are largely the same regardless of the communication mechanism chosen.

Three supported mechanisms

- Soft AP
- Bluetooth Low Energy (BLE)
- 802.15.4/Thread (a.k.a. Thread Assisted Pairing)



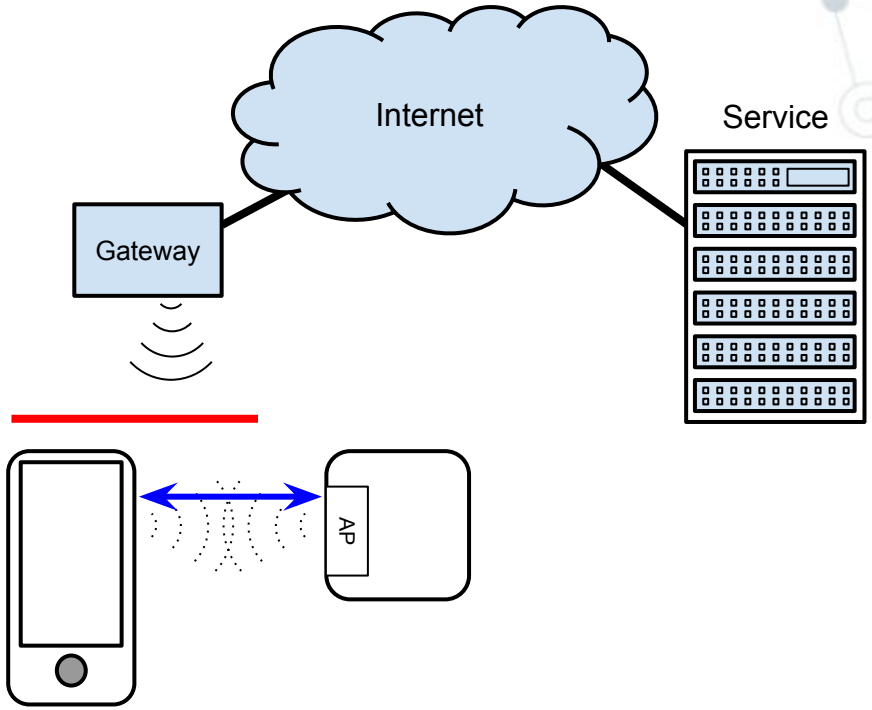
Soft AP

Process

- Wake device
- Connect to device WiFi
- Establish IPv6 addresses
- Connect device with TCP

Features

- WiFi-enabled devices only
- Requires manual WiFi configuration on iOS
- Mobile disconnected from home network / Internet during pairing.



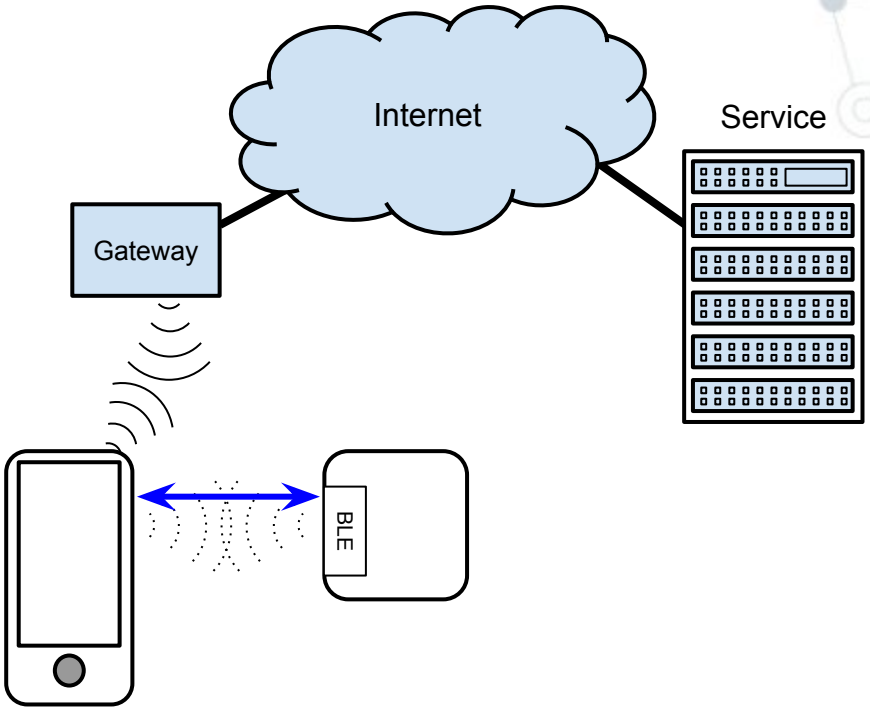
BLE

Process

- Wake device
- Device advertises as unpaired device
- Mobile scans for and connects to device

Features

- No manual WiFi configuration required
- No loss of WiFi connectivity
- Uses existing Weave pairing protocols
- Slow (low data rate)
- Can be used to bootstrap other networks



Establishing communication | Device authentication | Network provisioning | Weave provisioning | Service provisioning | Setup & Installation

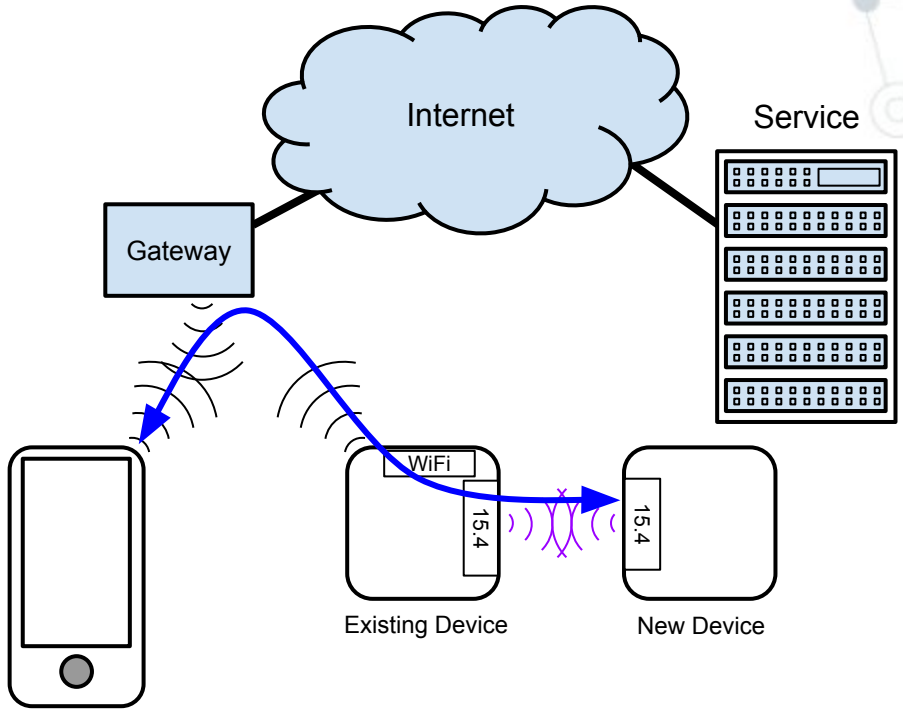
Thread Assisted

Process

- Connect to existing device over home WiFi
- Enable 15.4 joining on existing device
- Press button on new device
- New device hunts for joinable PAN
- New device provisionally joins existing PAN
- Existing device forwards comm. to/from new device

Features

- Supports 15.4 only devices
- No manual WiFi config / loss of connectivity
- Cannot be used for first device



Device authentication

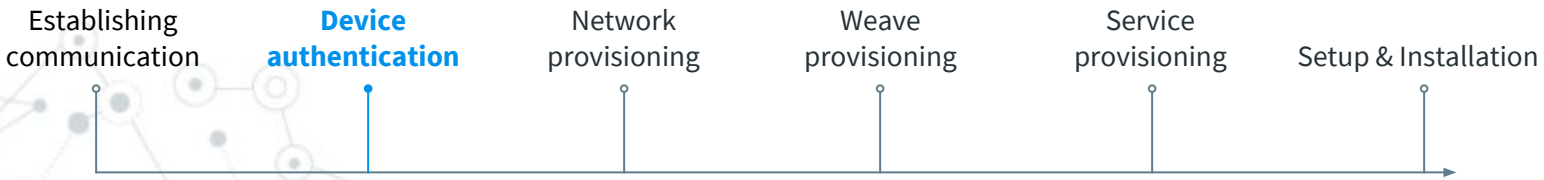
After establishing communication. The device must be authenticated.

Purpose:

- Identify type of device, serial number, capabilities, etc.
- Authenticate device
- Establish secure channel for pairing

Security Goals

- Prevent unauthorized access to user's account / personal data
- Block device ‘spoofing’ attacks
- Prevent leak of user's network credentials
- Protect the pairing code
- Ensure device authenticity



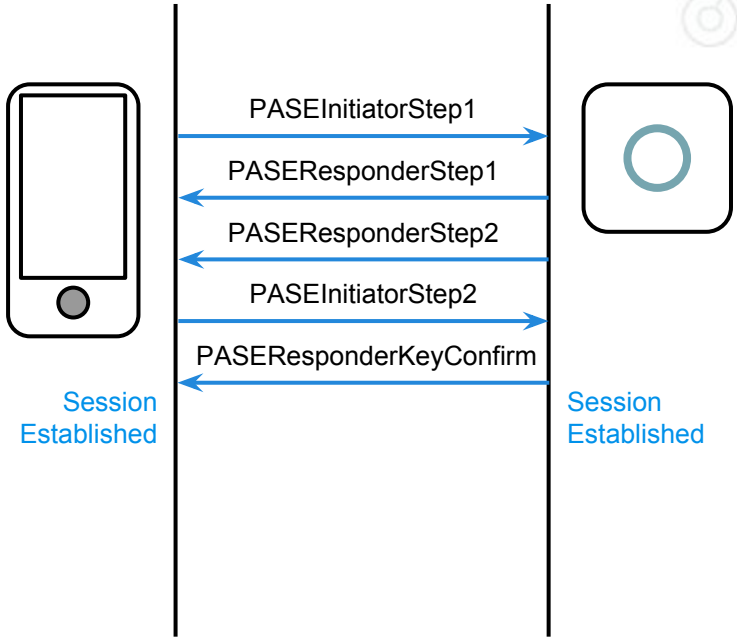
Password Authenticated Session Establishment (PASE)

Weave PASE Protocol

- Based on J-PAKE crypto protocol
- Mutual authentication w/low-entropy secret (pairing code)
- Resistant to man-in-the-middle attacks
- Perfect forward secrecy
- Integer field math now, EC soon
- Recently completed crypto proof

Features

- Proves to device that user has physical possession
- Proves to user that phone is talking to correct device
- Establishes secure channel for rest of pairing



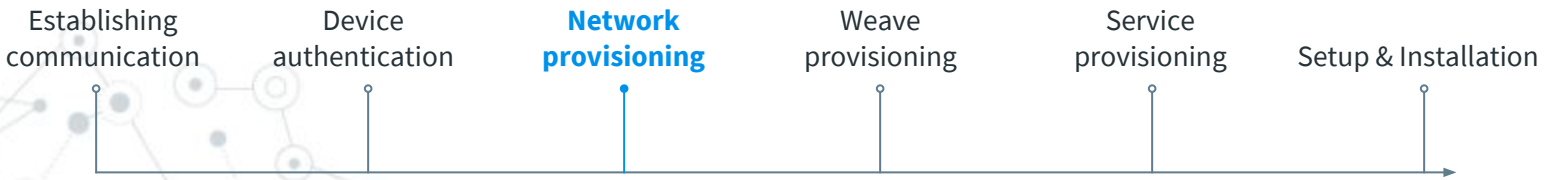
Establishing communication | **Device authentication** | Network provisioning | Weave provisioning | Service provisioning | Setup & Installation

Network Provisioning

Once the device is authenticated, the next step is to get it connected to a network.

Currently supported networks:

- Wi-Fi
- Thread



Weave Network Provisioning Profile

Generalized protocol for network configuration / management

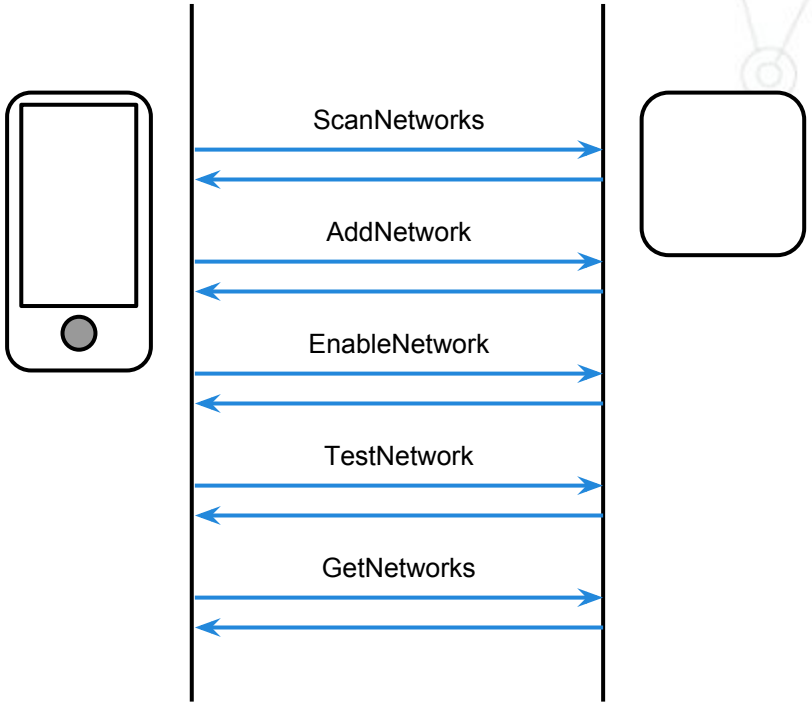
- Supports both WiFi and Thread

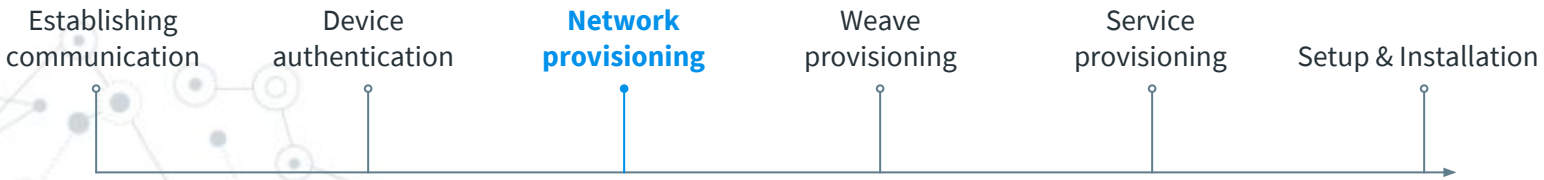
Individual requests for each operation

Can be used outside of pairing

- WiFi password change
- Retrieving credentials from existing device

Future support for bulk password change





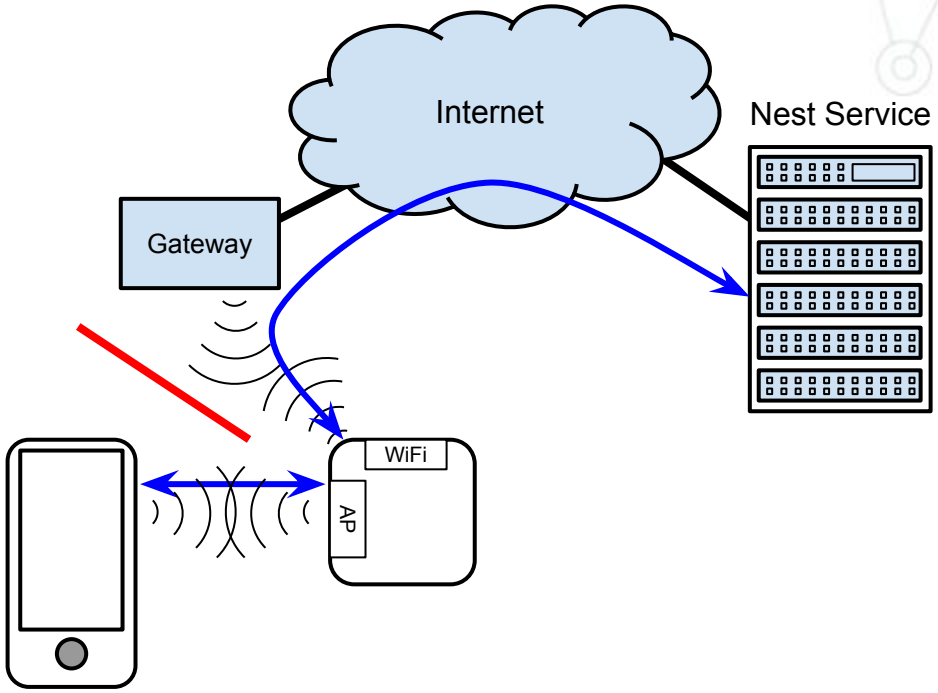
WiFi Network Provisioning

Process

- Scan WiFi networks
- Select WiFi network and enter credentials (1st device pairing only)
- Connect to home network
- Test connectivity to Internet / service

Features

- Based on Weave Network Provisioning Profile
- Good UX in case of bad password
- Requires simultaneous station/AP mode when using Soft AP for pairing



Establishing communication | Device authentication | **Network provisioning** | Weave provisioning | Service provisioning | Setup & Installation

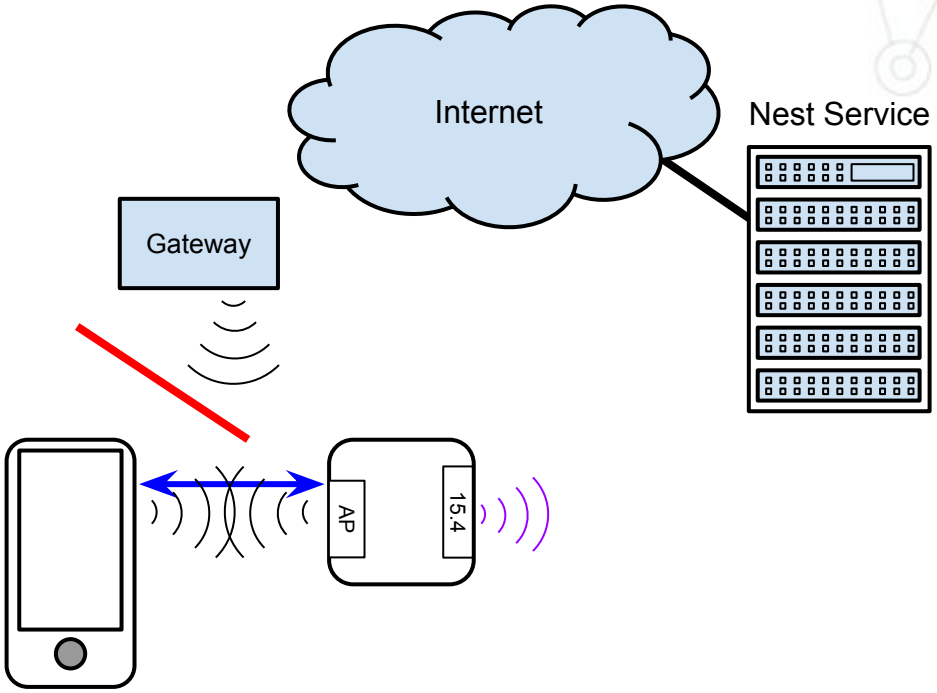
Thread Network Provisioning

Process (1st device)

- Energy scan / channel selection
- Form new Thread PAN
- PAN name derived from Weave Fabric id **`NEST-PAN-6F4B`**
- Unique PAN extended id
- Random network key

Features

- Occurs automatically at time of fabric provisioning (details below)
- Channel fixed for lifetime of PAN



Establishing communication | Device authentication | **Network provisioning** | Weave provisioning | Service provisioning | Setup & Installation

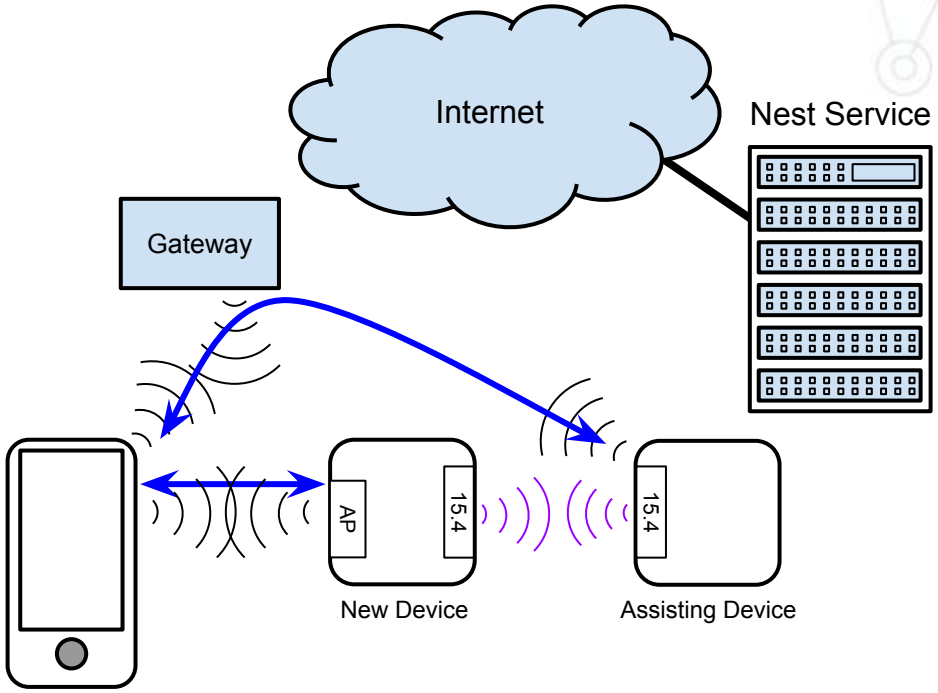
Thread Network Provisioning

Process (2nd device)

- GetNetworks (from assisting device)
- AddNetwork (using info from assisting device)
- EnableNetwork (results in device joining PAN)

Features

- New device scans for PAN to determine channel
- Assisting device must be active at time of join
- Commissioner must have extracted network info from existing device prior to provisioning



Establishing communication | Device authentication | **Network provisioning** | Weave provisioning | Service provisioning | Setup & Installation

Weave Provisioning

Even though it's on a network, the device isn't able to communicate through Weave messages until it's been provisioned for the fabric.

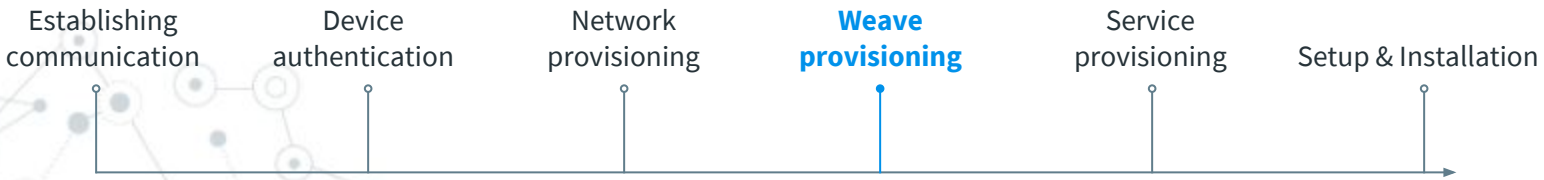
Creating a fabric:

- Generating a unique Fabric Id (64-bit global id)
- Generating fabric shared keys for message transmission
- Persisting above in durable storage

Joining a fabric:

- Acquiring and persisting fabric configuration

Performed via Fabric Provisioning Profile

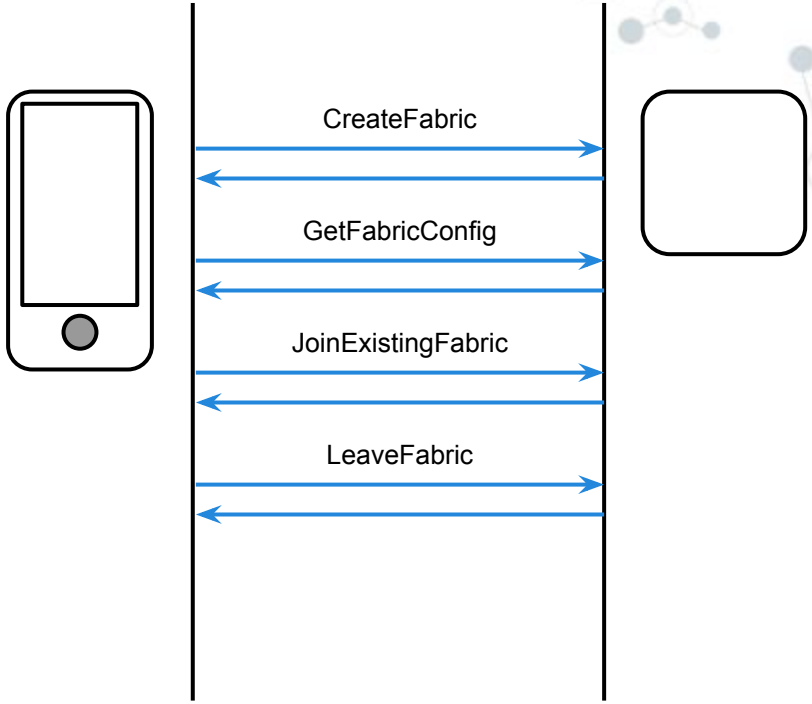


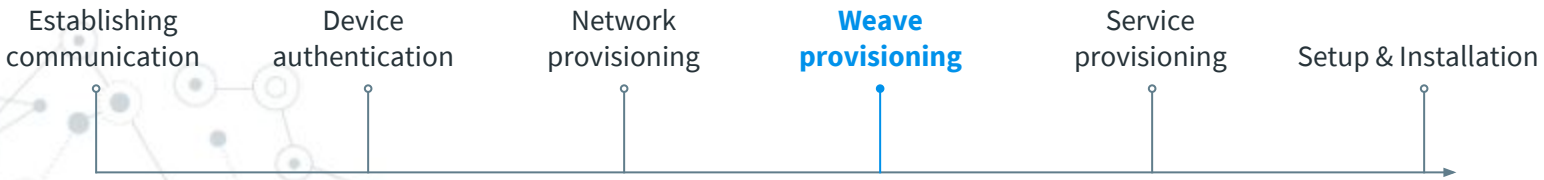
Weave Fabric Provisioning Profile

Protocol for managing membership in a fabric

Defines fabric config as transportable container of information about a fabric

- Fabric ID
- Fabric Keys
- Key Lifetime / Rotation Scheme





Weave Provisioning

Process (1st device)

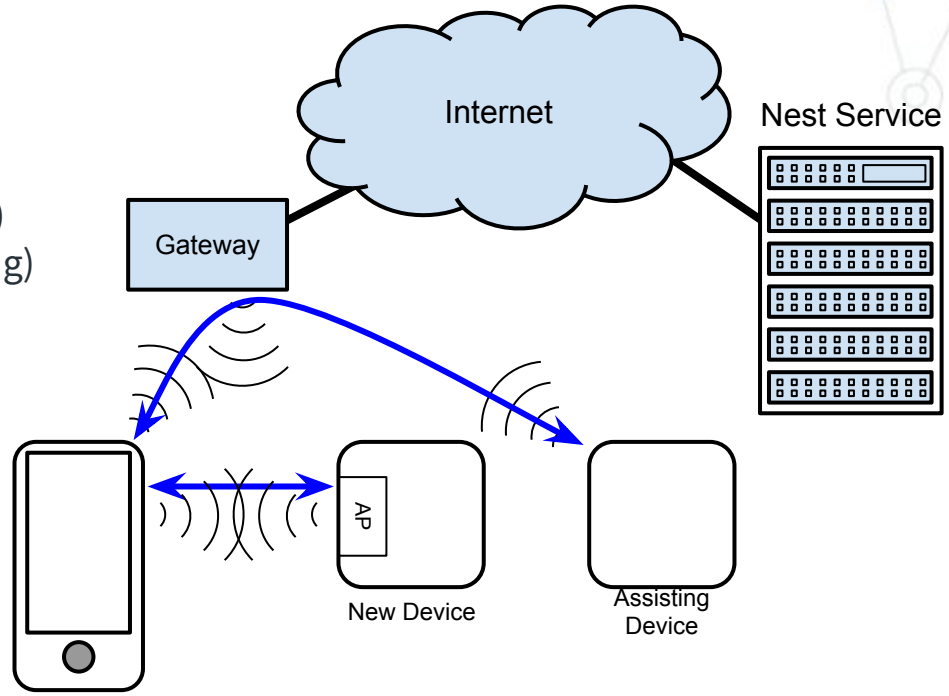
- CreateFabric

Process (2nd device)

- GetFabricConfig (from assisting device)
- JoinExistingFabric (passing fabric config)

Features

- - No direct communication required between devices



Establishing communication | Device authentication | Network provisioning | **Weave provisioning** | Service provisioning | Setup & Installation

Service Provisioning

The last step to get the device 'connected' is to provision it with cloud services and the user's account.

Configure device to talk to the Nest service

Establishes the first contact point for service

Provides information allowing device to auth service

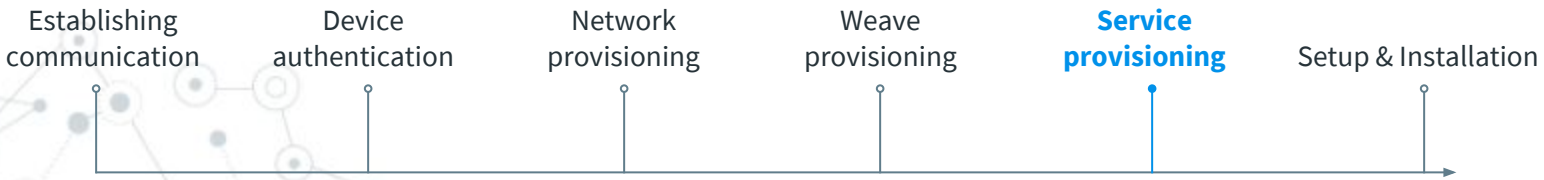
Supports directing devices to different service instances

- e.g. production, field-test, QA, etc.

Uses pairing token to authorize device to user's account

Allows service to confirm authenticity of device

Performed via Service Provisioning Profile



Weave Service Provisioning Profile

Manages device's relationship with service and account

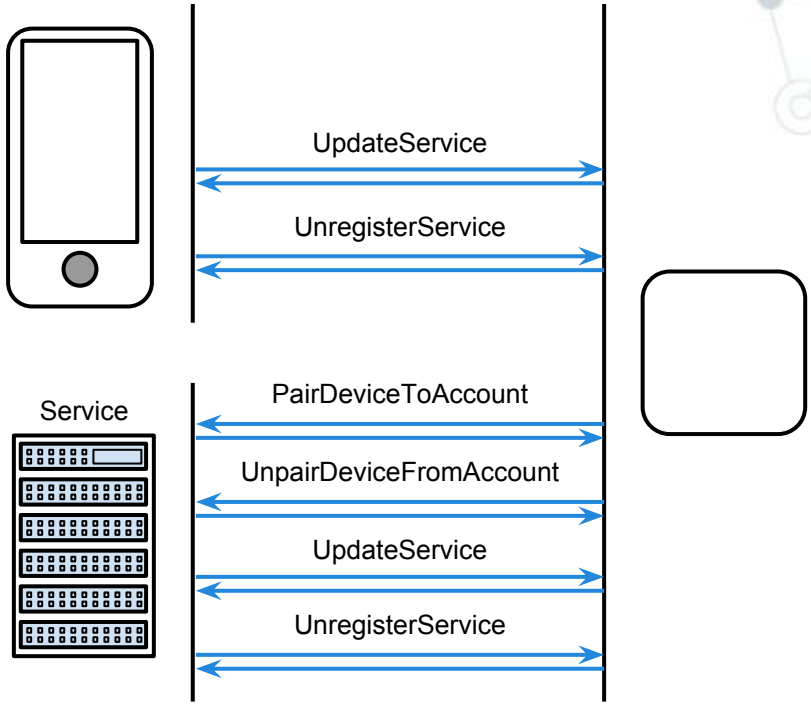
Defines service config as standard container of information about a service

- Address (host/port) of service directory endpoint
- List of trusted CA certificates for service

Includes commissioner-to-device, and device-to-service interactions

Supports a single device having relationships with multiple services

- E.g. Nest service and partner service



Establishing communication | Device authentication | Network provisioning | Weave provisioning | **Service provisioning** | Setup & Installation

Weave Service Provisioning Process

Commissioner gets pairing token from service

RegisterServicePairAccount sent to device

- Service config
- Pairing token
- Initial device configuration

Device persists service config

Device connects to service

- Device authenticates service (via server certificate)
- Service authenticates device (via device certificate)

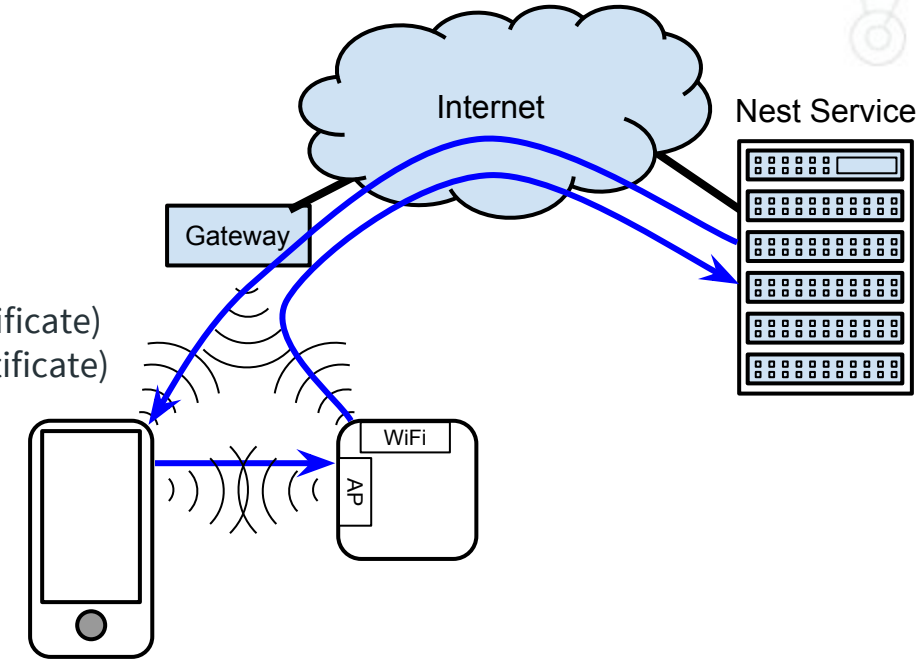
Device sends PairDeviceToAccount to service

- Pairing token
- Initial device configuration

Service verifies pairing token

Service associates device with account

Service stores initial device configuration



Establishing communication | Device authentication | Network provisioning | Weave provisioning | **Service provisioning** | Setup & Installation

Setup & Installation

At this point the pairing process is complete, but most products require additional configuration before they can be useful.

Product specific configuration is the last phase of OOB

Product and device-type specific phase

Includes

- Initial settings configuration
- Installation, wiring walk-through
- Sensor calibration
- Product feature education