Setting Channel Keys and Network Identity

Your channel configuration defines who can communicate on your mesh. Getting it right from the start saves painful re-configuration later as your network grows.

Understanding Channel Keys

Both Meshtastic and MeshCore use a shared channel key (Pre-Shared Key or PSK) that all nodes on a given channel must share to communicate. The key serves two functions:

- **Confidentiality** - Nodes without the key cannot decode messages, preventing outsiders from reading your mesh traffic. Note this is confidentiality, **not authentication**: because every member shares the same key, any member can forge or impersonate messages on the channel. A shared PSK does not prove who sent a message.
- **Network segmentation** - Multiple community networks can coexist on the same frequency by using different keys

Important: If you use the Meshtastic default key ("AQ==", which is base64 for the single byte 0x01 - the publicly known default key, *not* "all-zeros"), the firmware expands it into the well-known default PSK and your messages are readable by every Meshtastic node in range. For a community network, always set a custom channel key.

Generating a Strong Channel Key

Meshtastic channel encryption uses AES-256-CTR when a 32-byte (256-bit) key is used. Custom PSKs can be 0, 128-bit (16 bytes), or 256-bit (32 bytes). Generate a strong 256-bit key:

```
# Generate a random 256-bit key (32 bytes, base64 encoded)
python3 -c "import os, base64; print(base64.b64encode(os.urandom(32)).decode())"
```

Distributing Channel Keys

Methods for sharing your channel key with new members:

- **QR code** - Meshtastic generates a channel QR code that encodes the full channel configuration (name, key, modem preset). Share via your website or print at events. The most convenient method.
- **Deep link URL** - Meshtastic channel QR codes encode as an HTTPS web URL of the form `https://meshtastic.org/e/#<base64url>`, with the channel settings carried in the URL fragment after the `#`. Can be posted as a clickable link in your community documentation.
- **Manual entry** - For MeshCore and technical users, document the key as a base64 string in your private community documentation.

Key distribution security: Your channel key doesn't need to be secret from trusted community members, but don't publish it on your public website. Share it in your community Discord/Signal or at in-person events.

Multi-Channel Strategy

Consider running multiple channels for different purposes:

Channel Name	Key	Purpose
Community-Public	Published freely	General community chatter, newcomer welcome
Community-Ops	Members only	Network operations, node status updates
EmComm	Emergency teams only	Your group's own coordination and drills (see caveat below)

EmComm channel caveat: A private "EmComm" channel is fine for your own group's coordination and drills under unlicensed Part 15 (915 MHz ISM) operation, but it is **not** a substitute for authorized public-safety or amateur-radio emergency channels. Two limits apply: an encrypted channel **cannot** be used by stations operating under amateur radio (Part 97), which prohibits messages encoded to obscure their meaning; and formal ARES/RACES/served-agency traffic must stay on authorized, often monitorable channels. During a real activation, follow your served agency's and ARES/RACES communication plan rather than relying on a private encrypted hobby-mesh channel.

Network Name and Node Naming Conventions

Establish naming standards early. Consistent naming makes the node list immediately informative:

- **Meshtastic long name format:** [City/Area]-[Location]-[Type] - e.g., "PDX-WestHills-Repeater" or "SEA-Capitol-Hill-Node"
- **Short name** (4 bytes): Use initials + number - "WH01", "CH02"
- **Repeater nodes:** Include "Rpt" or "Rep" in the name to distinguish from client nodes
- **Room servers:** Include "RS" - "PDX-RS01"

Revision #3
Created 2026-05-03 06:20:48 UTC by Mesh America Admin
Updated 2026-06-10 04:30:34 UTC by Mesh America Admin