Understanding Channels and PSKs

Overview

Meshtastic supports up to **8 simultaneous channels** (index 0 - 7). Channel 0 is the primary channel; channels 1 - 7 are secondary channels used for specific groups or purposes.

Channel Anatomy

Every channel has three defining properties:

- **Name** - a human-readable label used to match channels between nodes.
- **PSK (Pre-Shared Key)** - a pre-shared key that is 0 bytes (no encryption), 16 bytes (AES-128), or 32 bytes (AES-256), used to encrypt and decrypt messages on that channel.
- **Role** - one of `PRIMARY`, `SECONDARY`, or `DISABLED`.

AES-CTR Encryption per Channel

Each channel is encrypted independently with AES-CTR using its PSK. The key length depends on the PSK: the default public channel uses the built-in single-byte default key and is effectively AES-128, while a channel configured with a generated 32-byte PSK uses AES-256. All nodes that possess the matching channel settings and PSK can decrypt traffic on that channel. Relay nodes forward ciphertext blindly - they do not need the PSK to relay packets, only the destination nodes need it to decrypt.

The Default "LongFast" Public Channel

LongFast is the default modem preset. The default primary channel uses the well-known, publicly documented default key (`AQ==`, a single 0x01 byte) and an empty/default name - it is intentionally not secret. Any Meshtastic device running stock firmware with default settings can read messages on this channel. It exists as a shared public mesh for interoperability.

Creating a Private Channel

To create a private channel, set a custom name and generate a random PSK. Only the PSK provides confidentiality - the channel name and its derived hash are effectively public, so the name does not protect your messages. This protection is also defeated if a gateway on the channel uplinks to MQTT without `mqtt.encryption_enabled` set true, which republishes the traffic in cleartext. Share access via QR code (see page 2).

Channel Roles

- **PRIMARY** - the node broadcasts NodeInfo, position packets, and telemetry on this channel. There is exactly one primary channel per node (index 0).
- **SECONDARY** - carries only messages explicitly addressed to or sent on that channel. No automatic position or telemetry broadcasts.
- **DISABLED** - the channel slot is configured but inactive.

Running Multiple Channels Simultaneously

A single node can participate in up to 8 channels at once. A node floods and relays packets it hears (subject to channel-hash matching and duplicate suppression) independent of whether it holds the PSK - being configured with a channel governs whether it can decrypt that traffic, not whether it relays it. This makes it possible to bridge a private club channel and the public mesh on the same hardware - the node relays both transparently.

Channel Index 0 vs. Named Secondary Channels

Index 0 (the primary channel) carries the majority of mesh traffic: NodeInfo, position, telemetry, and general messages. Indices 1 - 7 carry traffic only for the specific groups or functions those channels are assigned to. Most community deployments use channel 0 for public connectivity and one or more secondary channels for group communications.

Revision #3
Created 2026-05-03 05:26:43 UTC by Mesh America Admin
Updated 2026-06-09 12:08:31 UTC by Mesh America Admin