Mesh Network Change Management

A community mesh network is shared infrastructure. Changes to configuration - channel presets, node roles, frequency settings - can disrupt all users if done carelessly. This page covers change management practices that keep the network stable and community trust intact.

Why Change Management Matters

Unlike a traditional IT network with change control systems, community mesh networks are informal. A single operator changing the channel name or PSK on a key repeater can silently disconnect all users who have that repeater in their channel config. Changes that seem small to one operator can have large effects on the whole network.

Changes That Require Community Coordination

Change Type	Impact	Required Notice
Channel name or PSK change	All users on that channel lose connectivity until they update	Required - announce in advance, coordinate cutover time
Modem preset change	All nodes on different preset cannot hear this repeater	Required - network-wide coordination needed
Frequency slot change	Same as preset change	Required
Hop limit change (reduce)	May isolate edge nodes from network core	Recommended
Node role change	Affects routing if changing to/from Router	Recommended
Firmware update (minor)	Minimal - backward compatible	Good practice to announce
Firmware update (major)	May affect interoperability with older nodes	Required for key infrastructure

Change Type	Impact	Required Notice
Node taken offline (temporary)	Routing reroutes; may cause gaps	Recommended - notify community
Node permanently removed	Route cache entries become stale	Required - update network documentation

Change Communication Channels

Establish at least one out-of-band (non-mesh) communication channel for network announcements:

- Community Discord server with a #network-changes channel
- Signal or Telegram group for operators
- Email list for major announcements
- Ham radio net for ARES-affiliated networks

Announce significant changes at least 48 hours in advance for planned maintenance. Emergency changes (a node causing harm to the network) can happen immediately but should be communicated as soon as possible.

Testing Changes Before Deploying

1. Test configuration changes on a non-critical node first (a personal portable node, not the main community repeater)
2. Verify the change works as expected with a test partner node
3. Document the before-and-after configuration
4. Have a rollback plan: know how to undo the change if it causes problems
5. Apply to production during low-traffic hours

Maintaining a Network Configuration Ledger

Keep a simple spreadsheet or wiki page with current configuration for every community node:

- Node name and operator
- Physical location
- Current firmware version
- Channel configuration (name, PSK, preset)

- Role setting
- Last configuration change date and who made it

This ledger prevents "mystery configuration" situations where no one knows why a node is behaving unexpectedly because the original operator is no longer reachable.

Revision #2
Created 2026-05-03 05:51:14 UTC by Mesh America Admin
Updated 2026-05-03 13:01:44 UTC by Mesh America Admin