



Use Case Scenarios

Liberty Communication Systems, Inc. · lcs.network

Scenario 1 — Two client RNodes with a solar transport node on the mountain

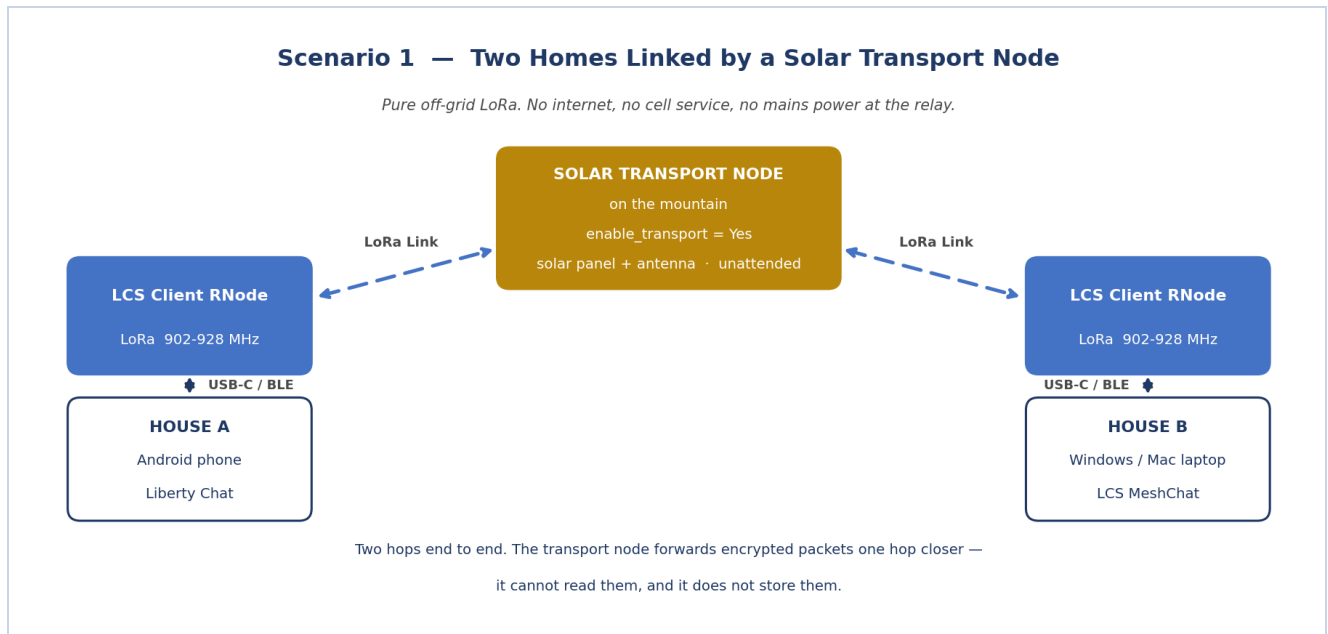


Figure 1 — Off-grid LoRa messaging across a relay.

Requirements

- One LCS Client RNode per household, connected by USB-C or Bluetooth to a phone or computer
- One LCS Solar Transport Node, positioned high with line of sight to both homes
- Matching frequency and preset on every radio unit

How it works

- The transport node re-broadcasts announces and forwards encrypted packets. No other device in the chain needs to be configured to account for it.
- Each user announces once. Both households appear in each other's peer list by display name.
- Messages route automatically across two hops, end-to-end encrypted, with signed delivery receipts.

Notes

- Use **Long Fast** for maximum text range. PTT voice clips work well on this link.
- Live voice calls require **Short Fast** or faster, which reduces range. Half-duplex mode is recommended.

- The transport node is unattended and holds no messages. Offline devices receive messages when their host reconnects and a fresh path is established.

Scenario 2 — Liberty Chat and LCS MeshChat connected through the internet

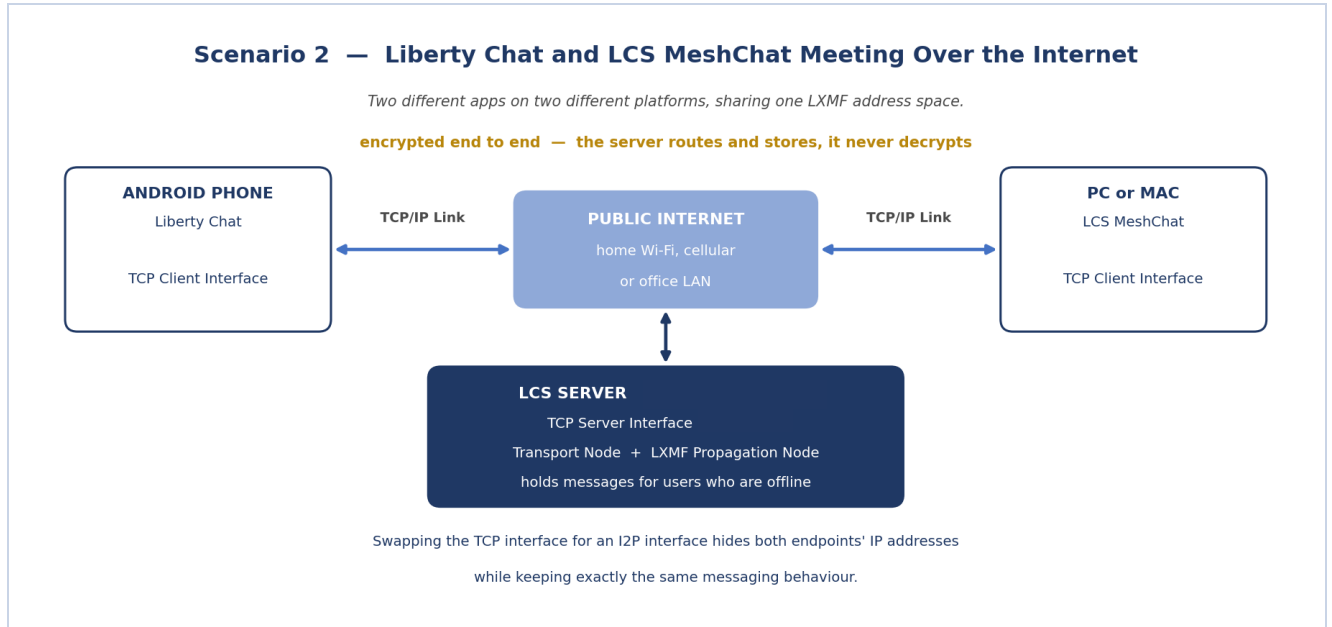


Figure 2 — Two applications meeting on the LCS TCP server.

Requirements

- An Android phone running Liberty Chat, with any internet connection
- A Windows or Mac computer running LCS MeshChat
- A TCP Client interface on each, pointed at the server
- No radio hardware

How it works

- Both apps open an outbound TCP connection to the LCS server. No public IP, static address, or port forwarding is needed on either end.
- The server acts as a transport node, learning both announces and routing between them. As a propagation node, it holds messages for offline users and delivers them on reconnection.
- Liberty Chat and LCS MeshChat are different applications on different operating systems, but both speak LXMF. Contacts, delivery receipts, attachments, and voice all function normally between them.

Notes

- This is the fastest way to verify the network before radio hardware is available.
- Bandwidth over TCP supports Opus high-bandwidth voice and full-quality live calls.
- Replacing the TCP interface with I2P hides both endpoints' IP addresses. Application behaviour is unchanged.

Scenario 3 — Two mobile Command Center Gateways over packet radio

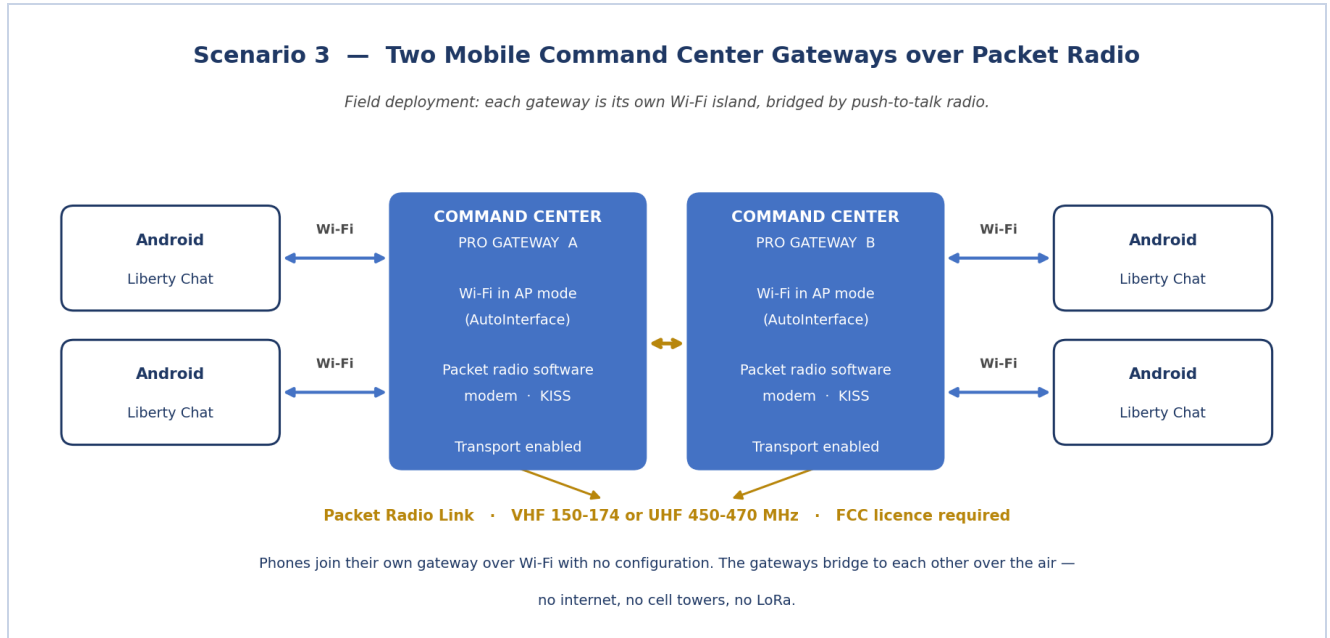


Figure 3 — Field deployment: two Wi-Fi islands bridged by packet radio.

Requirements

- Two Command Center PRO Gateways in Wi-Fi AP mode
- A push-to-talk radio on each gateway, driven by the built-in software modem
- Android phones running Liberty Chat at each site, joined to their local gateway's Wi-Fi
- FCC licence for encrypted operation on 150–174 MHz or 450–470 MHz

How it works

- Each gateway broadcasts its own Wi-Fi network. Phones join via AutoInterface with no IP configuration required.
- The gateways link to each other over packet radio using KISS framing through the software modem.
- Announces from Site A propagate to Site B over the RF link; messages route automatically in both directions.

Notes

- Packet radio provides greater range than LoRa at comparable power, making it the appropriate long-haul medium here.
- The packet radio link is half-duplex and slower than LoRa at short range — expect text and PTT voice clips across the RF hop rather than live calls.
- Each gateway holds mail for its own site. A phone that loses power receives its queued messages when it rejoins the Wi-Fi network.
- Assign a shared network name and passphrase to close the deployment to devices on the same channel.

Scenario 4 — Two homes with IP RNodes on the local Wi-Fi

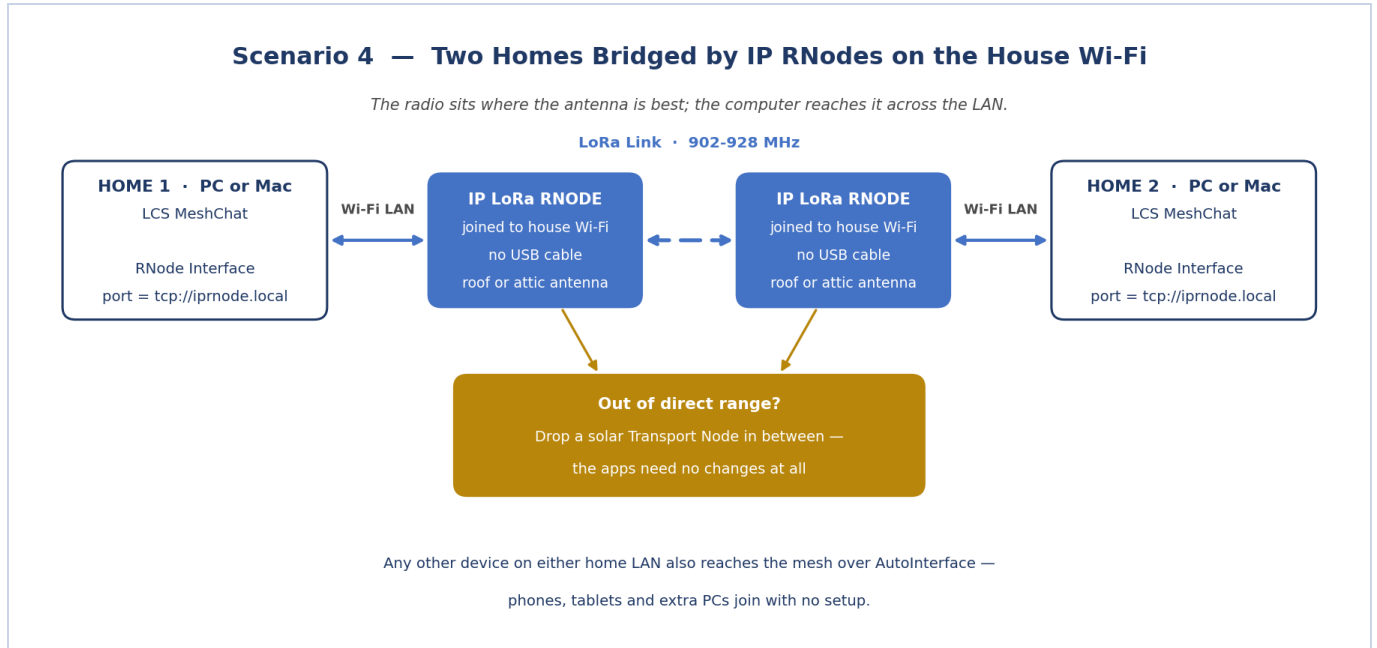


Figure 4 — The radio near the antenna, the application anywhere on the LAN.

Requirements

- One IP LoRa RNode per house, joined to that house's Wi-Fi network
- LCS MeshChat on a PC or Mac in each house
- An RNode interface in MeshChat configured with port = tcp://iprnode.local

How it works

- The RNode is accessed over the LAN, allowing it to be positioned in an attic or near a window for antenna performance while the computer stays at a desk.
- LCS MeshChat treats the Wi-Fi-connected RNode identically to a USB-connected unit.
- The two RNodes communicate directly over LoRa, carrying LXMf traffic between houses.

Notes

- Any other device on either home LAN — phones, tablets, additional computers — can also participate via AutoInterface with no configuration.
- If the two homes are out of direct LoRa range, add a solar transport node between them. No application changes are required; the path simply becomes two hops.
- Run LCS MeshChat as a propagation node on at least one machine so that offline devices receive queued messages on reconnection.

Scenario 5 — Two RNode user clusters joined by packet radio

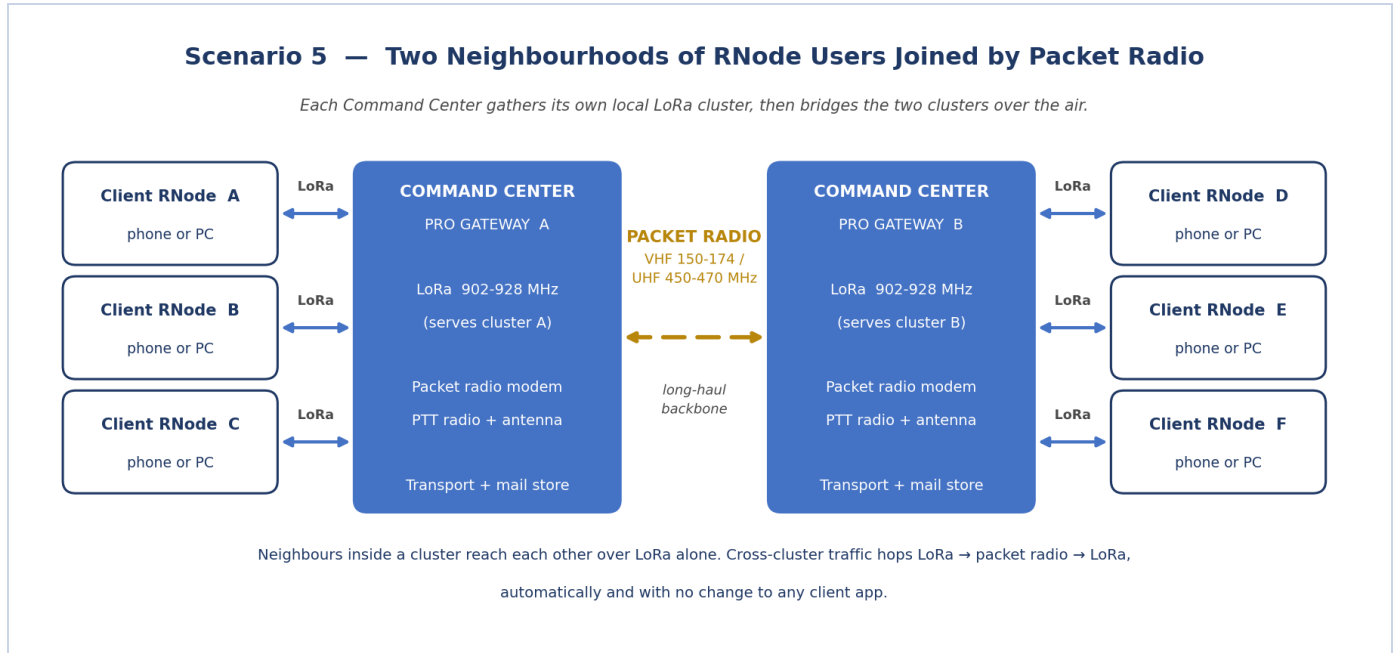


Figure 5 — Two local LoRa clusters bridged over packet radio.

This topology connects two geographically separate groups — neighbouring towns, two ends of a valley, a base camp and a forward site. Each Command Center Gateway serves a local cluster of RNode users over LoRa. The packet radio link carries cross-cluster traffic between the two gateways.

Requirements

- Two Command Center PRO Gateways, positioned for best antenna performance at each site
- A push-to-talk radio on each gateway, driven by the built-in software modem
- A cluster of LCS Client RNodes at each site — one per user, connected by USB-C or Bluetooth to a phone or computer
- FCC licence for encrypted operation on the business band

How it works

- **Within a cluster**, users reach the gateway and often each other directly over LoRa. Local traffic does not touch the packet radio link.
- **Between clusters**, each gateway bridges LoRa to packet radio. A message from Site A to Site D crosses three hops: LoRa in, packet radio across, LoRa out.
- Announces propagate the same path. Users at Site A see Site B users appear in their peer list by name without any manual routing step.
- Both gateways run as transport nodes and propagation nodes, holding mail for their own segment independently.

Why this topology

- **Each radio medium is used where it is most effective.** LoRa is licence-free and suited to short local links. Packet radio provides substantially greater range on comparable power for the single long hop between sites.
- **The backbone stays quiet.** Most traffic is local and remains on LoRa. The packet radio link carries only cross-cluster traffic.

- **It scales by adding gateways.** A third site joins by placing a third Command Center on the same packet radio channel; no client device reconfiguration is required.
- **Individual segments remain operational if the backbone link fails.** Cross-site messages queue at each propagation node and are delivered when the link is restored.

Notes

- All RNodes within a cluster must share the same frequency, bandwidth, spreading factor, and coding rate. A mismatch produces silence rather than a degraded link.
- Live voice calls between sites are marginal over the packet radio hop. Within a cluster on a fast LoRa preset they are more feasible.

Reference Links

- Liberty Communication Systems, Inc. — <https://lcs.network/>

RF RADIATION WARNING (WI-FI / LORA RADIO)

RF RADIATION WARNING: This product transmits radiofrequency (RF) electromagnetic radiation via Wi-Fi and/or LoRa radio protocols. The International Agency for Research on Cancer (IARC) has classified RF radiation as a possible human carcinogen (Group 2B). Peer-reviewed research has identified potential associations between RF electromagnetic field (RF-EMF) exposure and adverse effects on human fertility, including possible reductions in sperm count and pregnancy rates. Individuals with pacemakers, implantable cardiac defibrillators, or other active medical implants, or those with known heart conditions, should consult a physician before use, as RF radiation may interfere with implanted devices. Prolonged close-range exposure should be minimized as a precautionary measure. LIBERTY COMMUNICATION SYSTEMS, INC. EXPRESSLY DISCLAIM ALL LIABILITY FOR ANY HEALTH EFFECTS, INJURY, OR DAMAGE ARISING FROM RF EXPOSURE ASSOCIATED WITH THIS PRODUCT. By using this product, the user assumes all risk associated with RF exposure and acknowledges having read this warning.

LITHIUM BATTERY WARNING (LI / LI-ION / LIFEPO₄)

LITHIUM BATTERY WARNING: This product contains or is intended for use with lithium-based batteries (Lithium Metal, Lithium-Ion, and/or Lithium Iron Phosphate / LiFePO₄). Lithium batteries present a risk of fire, explosion, severe burns, and toxic gas release if punctured, crushed, short-circuited, overcharged, exposed to heat, or improperly handled, stored, or disposed of. The U.S. Consumer Product Safety Commission (CPSC) has identified thermal runaway — a self-sustaining internal reaction that can cause rapid heat generation, fire, and expulsion of flaming gases — as an unreasonable risk of death and injury. Use only manufacturer-approved chargers; never charge unattended or on flammable surfaces; store in a cool, dry location away from children; and dispose of only at a certified battery recycling facility in accordance with federal, state, and local regulations. Lithium batteries are regulated hazardous materials under 49 CFR Parts 171–180 (DOT/PHMSA). LIBERTY COMMUNICATION SYSTEMS, INC. EXPRESSLY DISCLAIM ALL LIABILITY FOR ANY INJURY, DEATH, OR PROPERTY DAMAGE ARISING FROM MISUSE, IMPROPER CHARGING, IMPROPER STORAGE, OR IMPROPER DISPOSAL OF ANY LITHIUM-BASED BATTERY. By using this product, the user assumes all responsibility and acknowledges having read this warning.

ENCRYPTION & LEGAL USE DISCLAIMER (RETICULUM NETWORK / HARDWARE / SERVER)

ENCRYPTION & LEGAL USE DISCLAIMER: This product incorporates end-to-end encryption and cryptographic authentication technology, including but not limited to the Reticulum Network Stack and associated hardware, software, and server infrastructure. This product is intended **solely for lawful purposes** and must be used in full compliance with all applicable federal, state, local, and international laws and regulations, including but not limited to laws governing encrypted communications, radio frequency transmission, unlicensed spectrum use, export controls, and data privacy. The use of encryption technology for illegal purposes — including but not limited to obstruction of law enforcement, facilitation of criminal activity, unauthorized interception of communications, or evasion of lawful surveillance — is strictly prohibited. **Liberty Communication Systems, Inc.** expressly disclaims all liability for any illegal, unauthorized, or improper use of this hardware, network, or server infrastructure by any end user or third party. By purchasing, activating, or using this product, the user represents and warrants that they will use it exclusively for lawful purposes and assumes sole and full legal responsibility for any and all consequences arising from their use of this product.

