COMMONROOM NETWORKS FOUNDATION www.commonroom.info

ISEA Institute for Social Entrepreneurship in Asia

Foreign, Commonwealth & Development Office

RHIZOMATICA

APC

SCHOOL OF COMMUNITY NETWORK LEARNING SERIES

2026

INTERNET FOR DISASTER PREPAREDNESS



Internet For

Disaster Preparedness

◆ ◇ ◆ ◇ ◆ ◇ ◆

Building Resilient Communication Infrastructure
for Disaster-Prone Communities

Published by
Common Room Networks Foundation
Bandung, West Java, Indonesia

Second Edition — September 2025
First English Edition — July 2026

Publication Credits

Programme Coordinator	Gustaff H. Iskandar
Executive Coordinator	Ressa Ria Lestari
Chief Editor	Tisha Amelia Anwar, Agni Yoga Airlangga
Administration	Ridha Nadhira Nida, Andriani Kesa
Art Director	Gustaff H. Iskandar
Writers	Anita Khairunnisa and Winingsih (Bitread)

English Translation

Translation Project Coordinator	Akhmat Safrudin
Translator	Rudi Dwi Hartanto

Contributing Institutions & Resource Persons

Perkumpulan AirPutih	
APJII	
Combine Resource Institution	
ICT Watch	
JRKI	
Jarindes Contributors	• Willdan Hidayatullah (Jasa Raharja Banten) • Abah Ugi Sugriana Rakasiwi (Kasepuhan Gelaralam) • Anis Faisal Reza / Abah Lala (Gugus Mitigasi Lebak Selatan) • Gilang Darmawan (SPNF SKB Kab. Lebak) • Rizal Saipul Anwar (RAPI 3003 Kab. Lebak)

Indonesia Publisher

Common Room Networks Foundation (Common Room)

Jl. Cigadung Asri I No. 3, Kel. Cigadung, Kec. Cibeunying Kaler, Kota Bandung, West Java 40191, Indonesia

Website: http://www.commonroom.info

Email: email.commonroom@gmail.com

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0). Visit https://creativecommons.org/licenses/by-nc-sa/4.0/



Foreword

At the end of 2021, Common Room launched the Community Internet School (Sekolah Internet Komunitas / SIK) programme at the Rural ICT Camp held in hybrid format from Kampung Adat Ciptagelar. As the programme developed, SIK came to involve participants from ten villages across ten provinces. These included participants from Pulo Aceh (Aceh Besar district), Kampung Adat Ciptagelar (Sukabumi district), Ketemenggungan Tae (Sanggau district), Desa Mata Redi (Central Sumba district), Jayapura district (Papua province), Desa Tembok (Buleleng district), and others.

We subsequently realised that several of these programme areas are located in disaster-prone zones. Floods, earthquakes, tsunamis, landslides, and storms are among the disasters that frequently occur in SIK programme areas. One stark example is Pulo Aceh, which was devastated by the tsunami at the end of 2004. The Aceh Tsunami, which occurred approximately nineteen years ago, destroyed much of Pulo Aceh. More than half of its population became victims of a disaster on a scale that exceeded our collective imagination. From the experience of the Aceh Tsunami, we learned to anticipate disasters so that the risk of damage and loss of life can be reduced in the future.

This Internet and Disaster Preparedness Training Module is a supplementary resource to the ten core SIK training modules. It is divided into two main parts: a technical guide to developing disaster-resilient internet infrastructure, and guidance on utilising internet networks for disaster mitigation. The development of this module involved several institutions and communities active in community internet development and disaster response in Indonesia. This initiative is one of our efforts to build community resilience and preparedness, and to reduce the risk of disasters that may occur in the future.

Through this module, we hope that we can learn together to anticipate and face disaster events. Stay resilient!

Bandung, 26 September 2023

Gustaff H. Iskandar

Common Room Networks Foundation

Table of Contents

Foreword iii

PART I — UNIVERSAL PRINCIPLES

Chapter 1 — Building Disaster-Resilient Internet Infrastructure 1

A. Developing Disaster-Resilient Internet Infrastructure 3

B. Equipment for Disaster-Resilient Internet Infrastructure 10

C. Technology Options for Disaster-Resilient Infrastructure 13

D. Key Considerations for Infrastructure Placement 19

Chapter 2 — Utilising the Internet for Disaster Mitigation 25

A. First Responders 27

B. Community Involvement in Disaster Mitigation 50

C. Beware of Disaster Hoaxes 52

PART II — CASE STUDY: THE JARINDES MODEL (INDONESIA)

Chapter 3 — The Jarindes Radio Communication Network 55

A. What Is Jarindes? 55

B. How Jarindes Works 58

C. Effectiveness of Jarindes 68

D. Jarindes Network Topology 69

Chapter 4 — How to Build a Jarindes-Type System 76

A. Solar Power System 77

B. Radio Repeater 81

C. Antenna Configuration 90
D. Antenna Installation Tutorial 92
E. Testing and Tuning 94
F–I. Operational Tips, Siren, Auto-Broadcast, SSTV 98

PART III — ADOPTING THE MODEL

Chapter 5 — Transferable Principles and Implementation Scenarios 116
A. Design Principles from Jarindes 117
B. The Network Protocol Stack 120
C. Implementation Scenarios for Philippine/SEA Communities 122

CHAPTER

01

BUILDING DISASTER-RESILIENT INTERNET INFRASTRUCTURE

In this chapter, you will hopefully learn:

- ✓ Understand the disaster risk profiles of Indonesia and the Philippines as archipelagic nations on the Ring of Fire.
- ✓ Identify the five requirements for disaster-resilient internet infrastructure.
- ✓ Explain the concept of network redundancy and why it is critical for disaster preparedness.
- ✓ List the key equipment and technology options for building resilient connectivity.

The Disaster Challenge of Indonesia

Indonesia is an archipelagic nation located between two continents and two oceans, making it highly susceptible to a wide range of disasters, from earthquakes, tsunamis, and volcanic eruptions to floods, landslides, and tropical storms. Indonesia's population must understand disaster preparedness measures, at minimum those relating to the hazards that threaten their own regions, in order to minimise casualties, losses, and large-scale destruction.

Case Study — Philippines

The Philippines: A Parallel Disaster Profile

The Philippines shares Indonesia's position on the Pacific Ring of Fire and faces a comparable, in some respects even more intense disaster profile.

The Philippines is struck by an average of 20 typhoons per year (Indonesia receives almost none), in addition to the same earthquake and volcanic risks. Typhoon Haiyan (Yolanda) in 2013, which killed over 6,300 people and displaced 4 million, remains one of the deadliest natural disasters in Philippine history.

More recently, Super Typhoon Odette (Rai) in December 2021 destroyed over 1.5 million homes across the Visayas and Mindanao. Both countries face the common challenge that disaster events routinely destroy telecommunications infrastructure, cutting off the very communities that need communication the most.

Understanding the types of disasters is essential:

Natural Disasters	Events triggered by natural forces: earthquakes, tsunamis, volcanic eruptions, floods, droughts, typhoons/cyclones, and landslides.
Non-Natural Disasters	Events caused by non-natural factors: technological failures, industrial accidents, epidemics, and pandemics.
Social Disasters	Events caused by human action: social conflict between groups or communities, and terrorism.

In an era of rapid technological development, the internet has become one of the primary tools for disaster risk reduction, mitigation, and response. Communication towers and networks now reach even the outermost regions. However, when a natural disaster strikes, internet connectivity itself is often disrupted. Preparing for this possibility is itself a critical part of disaster preparedness.

A. Developing Disaster-Resilient Internet Infrastructure

Given the speed at which the internet can transmit information, it is often our sole hope for spreading critical messages when disaster strikes. Our dependence on the internet makes securing its connectivity a strategic priority. If a natural disaster occurs, communication to report conditions and request assistance is the first thing people wait for. Securing internet networks is therefore a critical focus of disaster preparedness.

The first step before beginning any preparedness strategy is to understand the internet infrastructure in your area. Different regions will have different installations, equipment, and capacity levels.

In many parts of Indonesia and the Philippines, existing internet infrastructure was not designed with disaster resilience in mind. This module will help us prepare the fundamental elements we need to know.

Requirements for Disaster-Resilient Internet Infrastructure

There are five key requirements for developing disaster-resilient internet infrastructure:

1. **Network Redundancy** — multiple communication paths that are interconnected, reducing vulnerability to any single point of failure.
2. **Adequate Resources** — sufficient power, equipment, and personnel to maintain internet operations during a disaster.
3. **Physical Protection** — strong physical safeguards for infrastructure against threats such as earthquakes, floods, and storms.
4. **Monitoring and Early Warning** — effective systems that provide advance notice, allowing time for preventive action or evacuation.
5. **Distributed Data Storage** — data stored across multiple locations or using cloud computing, ensuring that critical information survives even if one site is destroyed.

Case Study — Indonesia

BTS Installation in the Lembang Fault Zone, West Java

The Lembang Fault is one of the most active fault lines in West Java. Based on palaeoseismological studies, this 29-kilometre fault has the potential to release its energy in a periodic cycle of approximately 500 years.

Base Transceiver Stations (BTS) have been built in this high-risk area as part of disaster mitigation efforts. These BTS installations serve critical functions: emergency communication, disaster monitoring, facilitating information access, and supporting post-disaster recovery.

However, building telecommunications infrastructure in a known fault zone raises fundamental questions about physical protection and redundancy — the very principles outlined above.

Case Study — Philippines

Taal Volcano Eruption and BTS Vulnerability, Batangas (2020)

When Taal Volcano erupted in January 2020, BTS installations in Batangas province were exposed to volcanic ashfall — a different physical mechanism from seismic shaking, but with the same result: degraded or destroyed telecommunications infrastructure.

Globe Telecom and Smart Communications both reported cell site damage from ash accumulation and power outages across the 14-kilometre danger zone. The eruption demonstrated that BTS hardening must account not only for ground shaking but also for airborne particulate hazards — a consideration particularly relevant in the Philippines, which has 24 active volcanoes.

1. Network Redundancy

Redundancy in a network is essential for maintaining reliability. A network redundancy strategy is often known as a disaster recovery plan, as it involves identifying critical network elements whose failure would result in prolonged outages.

Redundancy works by anticipating link or port failures so that the network can continue to operate. If a disruption occurs, redundancy allows the network to be restored quickly, minimising or even eliminating the risk of total network failure.

The following measures contribute to building network redundancy:

a. Separate Physical Paths

Using separate physical paths to connect the network reduces the risk that a single disruption will cause total network failure. Examples include using different fibre optic routes or engaging multiple internet service providers (ISPs) to connect the network.

b. Distributed Data Centres

Distributing data centres or primary servers across different geographic locations ensures that if a disaster or disruption affects one location, data centres in other locations can continue operations and maintain service availability.

c. Load Balancing

Load balancing distributes data traffic evenly across available paths. If one path experiences disruption or overload, traffic can be diverted to another path, maintaining internet availability and access speed.

d. Proactive Monitoring

Conducting proactive monitoring of the internet network is essential. By identifying potential problems or disruptions early, corrective action can be taken quickly to minimise the impact on services.

e. Backup Power and Reliable Equipment

Using backup power sources such as batteries or generators ensures that network operations continue during main power supply failures. Using reliable, high-quality hardware and network equipment also reduces the risk of device failure.

f. Smart Routing Technology

Smart routing technology, such as Border Gateway Protocol (BGP), can automatically divert data traffic if one path is disrupted, routing it through alternative paths that are still functioning. Dynamic routing protocols can also help manage network traffic efficiently and speed up network recovery after a failure.

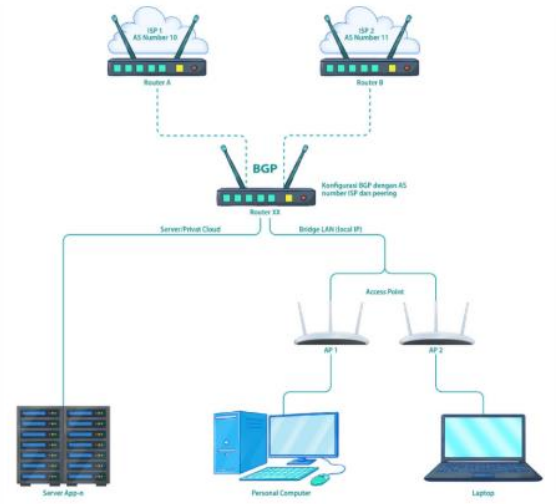


Figure 1Illustration of Load Balancing and BGP (source:personal)

Case Study — Indonesia

Lessons from Palu and Cianjur: When Internet Infrastructure Collapsed

The earthquake and tsunami that struck Palu and Donggala in 2018 demonstrated that disaster can occur anywhere, at any time. Volunteers reported extreme difficulty reaching disaster locations due to damaged infrastructure and unsafe transportation. More critically, cellular and internet networks collapsed completely in the aftermath.

A similar situation occurred during the magnitude 5.6 earthquake that struck Cianjur, West Java, on 21 November 2022. Smartfren reported that two of its 152 BTS in Cianjur went offline due to power supply disruption. The same pattern occurred in Palu and Donggala. These events underscore the urgent need for redundancy planning in disaster-prone areas.

Case Study — Philippines

Super Typhoon Haiyan (Yolanda) and the Tacloban Communications Blackout (2013)

Super Typhoon Haiyan made landfall in the Eastern Visayas on 8 November 2013 with sustained winds exceeding 300 km/h. The storm destroyed over 2,000 cell sites across the region. Tacloban City experienced a total communications blackout lasting approximately five days — during the most critical phase of the emergency response. The Philippine government's after-action review identified the absence of redundant backhaul routes as the primary cause of the prolonged blackout — the same structural vulnerability described in the Palu case. More recently, Typhoon Odette (Rai) in December 2021 knocked out approximately 80% of cell sites in Cebu and Bohol, with some island municipalities taking weeks to restore connectivity.

2. Maintaining Resources and Protection Systems

Maintaining the operational capacity of internet infrastructure in anticipation of disaster situations is crucial. This ensures the continuity of communication and information access for affected communities. The following resources and support systems should be considered:

Backup Energy Sources	Generators or batteries with sufficient capacity for several days of operation, to overcome power outages caused by disasters.
Alternative Communication Paths	Satellite links, radio, or emergency cellular networks that are resilient to disaster, essential when fibre optic cables or antennas are damaged.
Trained Technical Teams	Personnel trained in emergency response who can carry out rapid and efficient network repairs and maintenance.
Data Backups	Copies of critical data and network configurations stored securely and centrally, facilitating post-disaster recovery.
Emergency Communication and Evacuation Plans	Organised emergency communication systems and evacuation plan for personnel working in data centres and critical infrastructure.
Collaboration	Coordination with government agencies, telecommunications providers, communities, and aid organisations to strengthen disaster response capacity.
Physical Security	Strong physical safeguards to prevent damage, unauthorised access, and theft, including during the chaos that disaster situations can create.

B. Equipment for Disaster-Resilient Internet Infrastructure

Every disaster situation has different infrastructure needs, depending on the specific conditions and geography of the area. The choice of equipment and technology must be informed by analysis of the geographical structure and input from experts. Previous experience is also critically important.

The following is a recommended equipment list for building disaster-resilient internet infrastructure:

1. Redundant Routers	Routers supporting VRRP or HSRP protocols to ensure network traffic availability if one router fails. Multiple interconnected routers allow automatic traffic diversion.
2. Multiple ISPs	Connecting to more than one ISP increases redundancy. If one ISP experiences disruption, the network remains connected through the other.
3. Multiple Points of Presence (PoP)	Geographically distributed PoPs increase redundancy. If one PoP is affected by disaster, the network can be routed through others.
4. Backup Power Supply	Generators or batteries ensuring network infrastructure remains operational during power outages — critical for maintaining connectivity.
5. Fibre Optic Cables	Highly recommended for disaster resilience due to their strength, reliability, and immunity to electromagnetic interference.
6. Microwave Links	Radio frequency transmission as an alternative when fibre optic is damaged or unavailable. Can be established quickly and operate across physical obstacles. Highly recommended for archipelagic geographies.
7. Mobile Network Units	Portable cellular units that can establish temporary cellular networks when existing infrastructure is damaged or unavailable.
8. Satellite Communication	Satellite systems as a backup option for restoring connectivity when terrestrial infrastructure is severed. Provides reliable long-distance communication.

C. Technology Options for Disaster-Resilient Infrastructure

After understanding the recommended equipment, let us examine the technologies that can be considered for disaster-resilient infrastructure:

1. VSAT (Very Small Aperture Terminal)

VSAT uses geostationary satellites orbiting at approximately 36,000 km altitude to provide internet connectivity. VSAT can connect isolated or disaster-affected areas where terrestrial telecommunications infrastructure may be damaged or unavailable.

Advantages	Available in remote areas; flexible scale from one terminal to many; mobile. Can be used on ships or vehicles; highly reliable even in bad weather; increasingly high speeds supporting video streaming and conferencing.
Disadvantages	High cost for implementation and operation; higher latency than terrestrial networks (600+ ms); weather disruption possible (heavy rain, thick clouds); requires specialist technical maintenance; limited satellite capacity under heavy simultaneous use.

2. Wireless Systems

Wireless systems use radio waves, infrared, or other electromagnetic frequencies to transmit data without physical cables.

Advantages	High mobility; easily scalable; simple access without physical ports; wide coverage for remote areas; simultaneous multi-user connectivity.
Disadvantages	Speed limited by distance and interference; security vulnerabilities if not properly configured; limited range affected by physical obstacles; frequency interference; battery dependency; significant initial investment.

3. Wired Networks

Wired networks using fibre optic, copper (ADSL, coaxial), and Ethernet cables generally provide high speeds and stable connections.

Advantages	High speed and stable connectivity; multiple cable options; not affected by weather or environmental interference.
Disadvantages	Requires existing cable infrastructure or new installation; high construction and maintenance costs; limited by physical distance.

4. DSL (Digital Subscriber Line)

DSL transmits data over existing telephone lines (copper wire), allowing simultaneous voice calls and data transmission.

Advantages	Uses existing telephone infrastructure; faster than dial-up; more stable than dial-up.
Disadvantages	Speed depends on distance from exchange; relatively slow compared to modern cable or wireless; vulnerable to telephone line quality issues.

5. Cellular Networks

Cellular networks (3G, 4G/LTE, 5G) provide wireless internet connectivity through mobile infrastructure. Speed and signal quality vary by location and available infrastructure.

Advantages	Mobile connectivity anywhere with cellular coverage; wide deployment; increasing speeds with newer technology (4G, 5G).
Disadvantages	Speed and signal quality depend on network conditions and location; data quotas may limit usage; can be affected by weather and congestion.

6. WiMAX

WiMAX uses microwave frequencies to provide wireless internet access across wide areas. Often used in rural or remote regions.

Advantages	Wide coverage; high speed within range of the WiMAX transmitter; suitable for rural or remote areas.
Disadvantages	Speed and quality decrease with distance from transmitter; weather and interference effects; infrastructure may not be available in all areas.

7. LEO Satellite Connectivity (Starlink and Similar)

Low Earth Orbit (LEO) satellite constellations represent a fundamentally new category of disaster-response connectivity. Unlike traditional VSAT (geostationary at 36,000 km), LEO satellites orbit at approximately 550 km, providing latency of 20–40ms. Fast enough for real-time voice calls, video conferencing, and coordination applications.

LEO satellite services such as Starlink have been deployed in disaster response scenarios across Southeast Asia since 2024, with increasingly large-scale deployments in 2025 and 2026. A single Starlink terminal can provide connectivity within a radius of 500 metres to 1 kilometre, supporting up to 60 simultaneous users at speeds of approximately 100 Mbps.

Advantages	Extremely low latency compared to VSAT (20–40 ms vs 600+ ms); independent of terrestrial infrastructure; rapid deployment (operational within hours); portable terminals suitable for disaster zones;direct-to-device (D2D) capability allows ordinary smartphones to connect to satellites without a dish.
Disadvantages	Requires clear sky view (obstructed by dense forest canopy or buildings); subscription-based cost model; terminal hardware cost (~USD 300–600); power requirement (~75–100W, requiring solar panel or generator in off-grid areas); reliance on a single commercial provider (SpaceX); limited coverage radius per terminal.

Case Study — Indonesia

Cyclone Senyar and the Sumatra Floods: Indonesia's First Large-Scale LEO Satellite Disaster Response (November–December 2025)

Cyclone Senyar only the second tropical cyclone documented in the Strait of Malacca since reliable records began made landfall on northern Sumatra on 26 November 2025. By 9 December, the provinces of Aceh, North Sumatra, and West Sumatra simultaneously experienced catastrophic flooding. 3,414 mobile base stations went offline, resulting in a 66.99% disruption to communications across the disaster area. Over 440 people were killed and 1.8 million affected.

The Donated Starlink Units from Starlink and Indonesia Government were prioritised for government command posts, volunteer gathering points, and villages cut off by destroyed bridges. The Ministry also deployed 52 portable solar-powered battery boxes specifically to power the Starlink terminals. Various Bridge connecting the community to the outside world had been torn into by floodwaters, trapping over 3,000 residents. A Starlink terminal installed on the roof of a village hall provided 100 Mbps broadband within two hours of activation. Villagers made video calls to family members for the first time since the disaster began.

Notably, a disaster radio repeater was simultaneously operational at the summit of Mount Singgalang in West Sumatra. Combining Starlink and Community Radio.

The satellite provides data connectivity to the outside world; the radio network handles local voice communication and mass alerting across terrain that individual terminals cannot cover. This event marked the first large-scale use of LEO satellites in Indonesia for disaster response.

Case Study — Philippines

Starlink in Philippine Disaster Response: From Typhoon Opong to the Mindanao Earthquake (2025–2026)

The Philippines has seen multiple Starlink disaster deployments in rapid succession, establishing LEO satellite as a standard component of the national disaster response toolkit. In September 2025, Severe

Tropical Storm Opong (Bualoi) devastated Masbate province in the eastern Philippines, leaving communications networks in disarray across a province of nearly one million people. DICT Secretary Henry Aguda personally delivered 10 Starlink units, and SpaceX subsequently donated 100 additional units. Installation began on 15 October 2025 at barangay halls, healthcare facilities, and military response units. A 2kW solar-powered station was deployed alongside the terminals to ensure continuous operation without grid power. In June 2026, a magnitude 7.8 earthquake struck off the coast of Mindanao in the Cotabato Trench.

Globe Telecom, in partnership with Starlink, activated direct-to-device (D2D) satellite connectivity — the first time this technology was used for disaster response in the Philippines. Approximately 700,000 Globe and TM subscribers in South Cotabato, Sultan Kudarat, and Sarangani provinces could access free WhatsApp messaging and SMS directly from their existing smartphones no Starlink dish required, no ground-based cell tower needed.

The service was provided free for 30 days while terrestrial networks were rebuilt.The D2D deployment represents the next evolution: where traditional Starlink requires a physical terminal, D2D allows any compatible LTE smartphone to connect directly to orbiting satellites. This eliminates the logistics of distributing terminals entirely, a critical advantage when roads and bridges are destroyed.

IMPORTANT: *LEO satellite connectivity is a powerful addition to the disaster communication toolkit, but it does not replace the need for community-owned, locally maintained infrastructure such as radio networks. Starlink terminals require power, a subscription, and depend on a single commercial provider*

Radio repeaters, once built, operate independently and indefinitely. The most resilient disaster communication strategy

combines both: satellite for internet backhaul and external coordination, radio for local voice communication and mass alerting.

D. Key Considerations for Infrastructure Placement

1. GIS Mapping

Geographic Information Systems (GIS) use internet technology to provide access to and share geographic information related to disasters. GIS mapping can simplify the analysis of which telecommunications assets are in critical danger zones, enabling authorities to shut down and reroute communications during emergency periods. GIS applications in disaster contexts include:

- Mapping disaster-prone areas (floods, earthquakes, forest fires, landslides).
- Real-time disaster tracking and early warning through integration with weather monitoring, sensors, and live data.
- Evacuation planning and emergency response, including identifying routes, shelter locations, hospitals, and logistics centres.
- Post-disaster recovery: mapping damage, identifying recovery priorities, and coordinating reconstruction.
- Public participation and collaboration through open mapping platforms.

2. Determining Infrastructure Location

Disaster-resilient internet infrastructure must be built and placed in safe locations. A comprehensive risk assessment and site survey must be conducted before determining placement. Key factors include:

Distance from Natural Hazards	Avoid placing infrastructure in flood zones, earthquake-prone areas, or regions at high risk from tropical storms. Choose locations that are naturally protected.
Physical Security	Select locations with adequate physical security measures: restricted access, surveillance systems, and security patrols to protect against theft and vandalism.
Protected Structures	Ensure infrastructure is housed in buildings or enclosures designed to protect equipment from moisture, dust, extreme temperatures, physical damage, and theft.
Reliable Energy Supply	Ensure the location has a reliable power supply and adequate backup power (generators, batteries, solar panels).
Network Connectivity	Ensure the location has good access to network infrastructure: cellular coverage, fibre optic access, or submarine cable access as appropriate.
Legal and Regulatory Compliance	Comply with relevant land use regulations, zoning requirements, and environmental regulations. In Indonesia: AMDAL (Environmental Impact Assessment). In the Philippines: ECC (Environmental Compliance Certificate) under DENR.

Case Study — Indonesia

Tsunami Early Warning Batteries Stolen in Agam, West Sumatra (2019)

Widespread public indifference to disaster mitigation has led to numerous cases of detection equipment being stolen or vandalised.

The Agam District BPBD (Regional Disaster Management Agency) reported that two battery units from the Early Warning System (EWS) along the Tiku coastline were stolen. The theft disabled the EWS at night (when it could not rely on solar power alone). Of the ten EWS units installed along the Tiku coastline, nine were BNPB-funded and one was owned by BMKG.

The importance of tsunami detection systems was underscored by the December 2018 Anak Krakatau eruption, where the undetected tsunami killed hundreds along the coasts of Banten and Lampung. Even tsunami buoys placed in open waters have been stolen, equipment worth nearly one billion rupiah that could save many lives.

Case Study — Philippines

Parallel Challenges: PHIVOLCS Monitoring Station Vandalism

The Philippines faces similar challenges. PHIVOLCS (Philippine Institute of Volcanology and Seismology) has reported recurring problems with monitoring equipment in remote volcano observatories: solar panels stolen, sensor cables cut for copper salvage, and rain gauges vandalised. The community ownership principle described in Chapter 2, involving local communities in the maintenance and protection of disaster mitigation equipment — directly addresses this problem in both countries. When communities understand and feel ownership over the equipment, vandalism and theft decrease dramatically.

CHAPTER

02

UTILISING THE INTERNETFOR DISASTER MITIGATION

In this chapter, you will hopefully learn:

- ✓ Define the role of a first responder and list the essential skills required.
- ✓ Identify the personal and team equipment needed for disaster response operations.
- ✓ Explain how internet connectivity supports disaster monitoring, communication, volunteer management, and logistics.
- ✓ Describe the importance of community involvement in disaster mitigation.
- ✓ Recognise disaster related hoaxes and apply verification techniques to prevent their spread.

In daily life, we are all inseparable from the internet. The internet helps connect those who are far away and makes difficult tasks easier. Critically, the internet can also be leveraged for disaster mitigation. Using the internet in disaster mitigation can increase the opportunity to map and access the resources needed.

Internet in Disaster Mitigation: Key Functions

Monitoring & Early Warning	Internet-connected sensors can provide real-time data on environmental changes and deliver early warnings to at-risk communities.
Communication & Information Dissemination	In emergencies, the internet enables faster and more effective communication: warnings, evacuation routes, safe locations, and aid resources.
Disaster Management	Centralised web-based systems for collecting, storing, and accessing disaster data. These systems support logistics tracking, aid coordination, field assessment, and recovery monitoring.
Volunteer Management	Online training and education for volunteers. Enables remote volunteer participation: data collection, damage mapping, and online communication with survivors.

Challenges

- Not all areas have reliable and stable network infrastructure.
- Power supply disruption during disasters impedes internet use.
- Communities may lack access to or understanding of internet-based mitigation tools.

- Insufficient data security and privacy protections.
- Organisations and individuals may lack the expertise to manage disaster-related technology and data.

A. First Responders



Figure 2 A training exercise for first responders (source:wikimedia)

A first responder is an individual or team with specialised training and skills to provide initial assistance and early response in emergencies, including during disasters. They are the first to arrive at a disaster site to provide direct aid to victims and begin rescue efforts.

1. Essential Skills

Emergency Response Training	Formal training in emergency response and search and rescue (SAR), including knowledge of disaster management principles, incident command systems, and protocols for various emergencies.
Medical Training	Knowledge and skills in first aid: CPR, bleeding control, fracture immobilisation, wound care, and burn treatment. Also, basic health and safety knowledge: hygiene, sanitation, infection prevention, crowd control, and personal safety.
Problem-Solving	The ability to rapidly assess situations, make critical decisions, and adapt to changing circumstances. Must be able to think clearly, prioritise tasks, and produce effective solutions under pressure.
Cultural Sensitivity	Disaster-affected communities may come from diverse backgrounds, cultures, and languages. Cultural sensitivity and the ability to work respectfully with people from different communities is essential.
Communication & Coordination	Essential for coordinating with other responders, giving instructions to affected people, and offering support. Clear and compassionate communication, even under extreme pressure.
Teamwork & Collaboration	Disaster response is a collaborative effort. First responders must work with other responders, volunteers, government agencies, and community members.

2. Understanding of Technology and Information Skills

In the modern era, technology and information skills are critically important for first responders. This includes basic electronics repair skills (identifying faults, replacing components) and advanced network management (network design, security management). A professional first responder should be able to plan, implement, and secure complex computer networks — ensuring that networks operate efficiently, securely, and reliably during crisis situations.

3. Personal Equipment



Figure 3 Philippine Army 525th Engineering Combat Battalion (source:abscbnnnews)

A first responder must not depend on organisations for equipment; they must maintain their own personal gear to ensure safety and effectiveness. Equipment needs vary by disaster type and role, but the following categories are essential:

Personal Protection	Safety helmet, headlamp, safety glasses, N95 mask/respirator, cut-resistant and chemical-resistant gloves, safety boots, high-visibility vest, tactical clothing, rain gear, sleeping bag, emergency blanket.
Hygiene & Sanitation	Personal medications and prescriptions, hygiene supplies (toothbrush, soap), disposable gloves for contaminated materials.
Water & Food	Emergency food bars, water bottles/hydration packs, water purification tablets or filters, portable stove and outdoor cooking gear.
Lighting & Visibility	Durable LED flashlight with spare batteries/power bank, chemical glow sticks, emergency flares.

First Aid & Medical	Basic medical kit (bandages, antiseptic, pain relief, antibiotics, antihistamine, rehydration salts, burn cream, eye drops), CPR mask, emergency blanket.
Utility Tools	Multi-tool knife, duct tape, cable ties, rope, crowbar, carabiner clips, portable shovel, tarpaulin.
Communication	VHF/UHF two-way radio (handy talkie), mobile phone with power bank, whistle or signal device for communication when networks are unavailable.
Navigation & Mapping	GPS device, compass, smartphone with GPS/barometric/altimeter sensors, offline GIS maps of the affected area.



Figure 4 Personal Safety Gear (source:personal documentation)

4. Team Equipment

Command & Control	Computers, laptops, tablets, projector, large screen display, command tent or temporary shelter.
Communication & Mapping	GPS navigation devices, base station radios, cellular signal boosters, satellite phones, noise-cancelling radio headsets, real-time messaging applications.
Transport & Documentation	Vehicles (4x4, van, SUV), trailer for equipment, clipboard, notebooks, pens, markers, adhesive labels, digital camera or smartphone for documenting damage.



Figure 5 Vertical Rescue Equipment (Personal Documentation)

5. Vertical Rescue Equipment

Many disaster-prone areas in Indonesia and the Philippines are in highland or mountainous terrain. First responders require specialised vertical rescue equipment including single rope systems (static and dynamic ropes, harnesses, ascenders, descenders, pulleys, carabiners), anchoring equipment, fall protection systems, rescue stretchers and evacuation chairs, portable ladders and platforms, personal protective equipment for heights, and climbing/access tools.

IMPORTANT: *Proper training, certification, and strict adherence to safety protocols are essential when using vertical rescue equipment. Never attempt vertical rescue operations without formal training.*



Other References

- **Selected Survival Gear List, Home Survival Kit Guide, Survival Kit**
- **Stocks by Survivalist, UNHCR Emergency Handbook, FEMA EM**
- **First Aid Check List, AED First Responders Supplies, The Kit Builds**
- **Anatomy of First Aid Kit, Build a Survival Kit, Make a Disaster Plan**

6. Radio Equipment

During disasters, radio communication is often the most effective and reliable tool available. Essential radio equipment includes:

Base Stations & Repeaters	Multi-band, multi-mode radios; cross-band VHF/UHF repeaters; high-gain vertical antennas; waterproof and rugged equipment; Radio Over IP (ROIP) interoperability systems.
Handheld & Mobile Radios	VHF/UHF handy talkies, mobile rig radios with antennas and mounting hardware.
Infrastructure	Towers, masts, antennas, power supply equipment including generators, battery backup systems, and off-grid solar power.

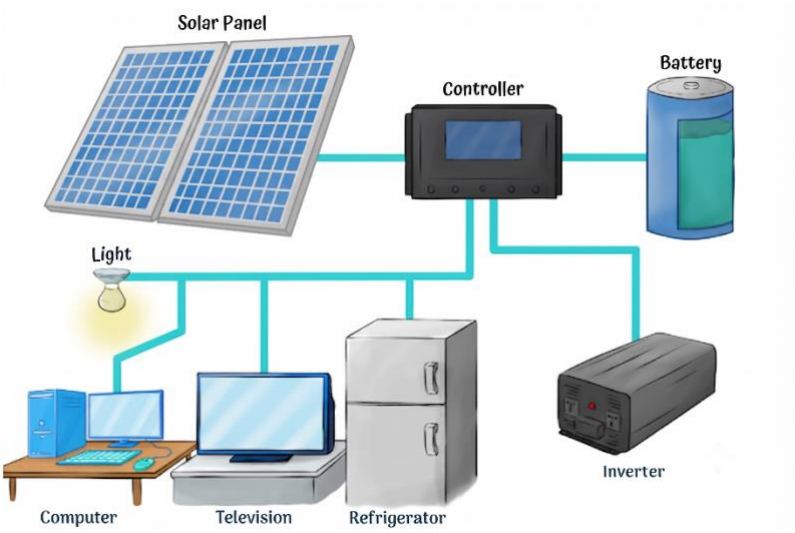


Figure 6 Solar Panel powering the key peripherals during disaster (source: Personal Documentation)

7. Power Supply Equipment

During disasters, grid power is likely to be limited or completely unavailable. Solar power systems provide a reliable and sustainable energy source for communication devices, lighting, medical equipment, and other essential electronics.

Essential solar power equipment includes: photovoltaic panels (portable/foldable designs recommended), solar charge controllers (MPPT for maximum efficiency), deep-cycle batteries (sealed lead-acid or lithium-ion), power inverters (pure sine wave for clean AC output), portable solar generator kits, solar-powered lighting and water purification systems, and solar-powered communication chargers.

8. Wireless Access Equipment

When terrestrial internet infrastructure is disrupted, wireless connectivity becomes critical. Essential wireless equipment includes:

Portable Satellite Internet	VSAT dishes/terminals, modems/routers, tripod antenna mounts. LEO HTS (High Throughput Satellite) such as Starlink recommended for lower latency.
Portable Cellular Routers	Routers with built-in modems (3G/4G/5G), multiple SIM card slots, Ethernet ports, external antennas or signal boosters.
Mesh Network Equipment	Self-forming, self-healing wireless mesh devices; battery-powered mesh nodes for temporary connectivity in remote locations.
Long-Range Wi-Fi	High-gain directional antennas, extended-range Wi-Fi access points and routers, wireless bridges and repeaters.
Mobile Hotspots	Portable Wi-Fi hotspots (MiFi devices) with internal cellular modems; battery-powered for enhanced portability.
Power & Backup	Portable generators, power banks, solar power systems, UPS devices for uninterruptible supply.

9. Local Network Equipment

In remote areas, traditional internet infrastructure is likely to be disrupted or unavailable. First responders should prepare alternative local networking methods:

- Mesh networks: ad hoc WLAN mesh networks for local connectivity without traditional infrastructure. Modern tools like Meshtastic enable smartphone-based mesh networking using inexpensive LoRa radio modules.
- Wi-Fi hotspots:portable MiFi devices or access points for temporary local wireless networks.
- Point-to-point wireless links: high-gain directional antennas connecting remote locations over long distances.
- Physical data transfer ('sneakernet'): using USB drives, HDDs, or SD cards carried by hand or vehicle between locations with and without internet access.

- Briar: a messaging application that works over Bluetooth, Wi-Fi, and Tor, enabling encrypted communication between phones without any internet infrastructure.

10. Access Points

Given the importance of internet access for communication, information dissemination, evacuation coordination, and general support, creating public access points during disaster response is essential. Potential approaches include:

- Collaborating with local businesses (cafes, restaurants) to provide public Wi-Fi.
- Setting up mobile charging and internet stations in public areas (parks, community squares, village halls).
- Establishing temporary internet tents or kiosks at affected or high-traffic locations.
- Providing access within emergency shelters and evacuation centres.
- Setting up internet access at community centres and public facilities.
- Deploying mobile internet vehicles equipped with VSAT or Starlink connectivity.
- Partnering with telecommunications providers for free public access.
- Establishing dedicated information centres with computers, internet, and support personnel.

B. Community Involvement in Disaster Mitigation

When volunteers arrive in disaster-affected areas, they sometimes maintain distance from local residents. This is a mistake. The involvement of local communities is critically important for building resilience and delivering an effective disaster response.

Local residents possess irreplaceable knowledge about their environment, climate, weather patterns, and the hazards specific to

their area. By involving local communities, responders can access this knowledge to plan more effective interventions. Communities can observe environmental changes, report suspicious changes, and assist in disaster risk surveys.

Involving communities in the mitigation process increases their awareness of potential hazards, enables them to contribute to emergency response planning and evacuation drills, and builds a sense of shared ownership over mitigation equipment and infrastructure. When communities feel ownership, they are far more likely to protect and maintain early warning systems and other disaster infrastructure.

Case Study — Indonesia

Missing Tsunami Buoys in Indonesian Waters



Figure 7 Tsunami Buoy illustration

Buoys are floating devices that detect waves caused by undersea earthquakes. In Indonesia, the buoy system is known as Ina-TEWS (Indonesia Tsunami Early Warning System), launched by BMKG in November 2008. Tragically, many buoys have been stolen from Indonesian waters.

In 2018, then-Coordinating Minister for Maritime Affairs Luhut Binsar Pandjaitan confirmed that buoys in Aceh and Palu had been stolen, directly hampering early warning capability and contributing to the loss of lives that could have been saved. The theft of equipment worth nearly one billion rupiah per unit underscores the need for community ownership and awareness.

IMPORTANT: *When you see disaster mitigation equipment in any area, do not damage it, do not move it, and do not take it. This applies equally to EWS systems, seismic sensors, rain gauges, tide gauges, and radio repeaters. These devices save lives.*

C. Beware of Disaster Hoaxes

During disasters, people immediately search for information about what has happened. In the digital age, information spreads faster than ever, but so does misinformation. False or misleading information spreads widely through social media platforms and messaging applications (WhatsApp, Telegram, Line), causing confusion, panic, and interference with disaster response efforts.

The following steps can help you avoid disaster hoaxes:

6. Use Official Information Sources obtain information from trusted official sources. In Indonesia: BNPB, BMKG, BPBD, and verified government social media accounts. In the Philippines: NDRRMC (National Disaster Risk Reduction and Management Council), PAGASA (Philippine weather bureau), PHIVOLCS (volcanology and seismology), and verified official accounts. Fact-checking resources: Rappler Fact Check, VERA Files (Philippines), Cek Fakta / Mafindo (Indonesia).
7. Verify Before Sharing: if you receive unfamiliar or shocking information via text, social media, or email, do not share it

immediately. Verify the source first. Check the official website or social media of the information source.

8. Recognise Hoax Indicators: hoaxes often feature spelling errors, poor grammar, and highly sensational content. If information seems implausible or contradicts official reports, it is likely false.
9. Do Not Share Unconfirmed Information: if the source is unclear and there is no official confirmation from relevant authorities, do not share the information. Sharing unconfirmed information inadvertently spreads hoaxes and causes unnecessary panic.
10. Educate Yourself and Others: improving digital literacy and information literacy helps you become more discerning in evaluating and sharing information. By consuming and sharing only accurate and beneficial information, you help yourself and others.



Figure 8 PIA Screenshot (source:personal documentation)

CHAPTER

03

THE JARINDES RADIO COMMUNICATION NETWORK

In this chapter, you will hopefully learn:

- ✓ Understand what Jarindes is and why it was developed in Kasepuhan Gelaralam.
- ✓ Explain the hybrid analog-digital architecture that makes Jarindes effective.
- ✓ Describe the HT-Kadus system, the Pangapungan repeater, and the siren system.
- ✓ Understand how SSTV enables image transmission over radio without internet.
- ✓ Describe the Jarindes network topology and how information flows through the system.

This chapter presents the Jarindes system as a documented case study. Jarindes (Jaringan Informasi Desa, Village Information Network) is a community-owned radio communication network developed at Kasepuhan Gelaralam, a traditional indigenous community in Sukabumi district, West Java, Indonesia.
It is presented here as an inspiring and replicable model of community-owned disaster communication infrastructure.

A. What Is Jarindes?

Jarindes is an independent communication network built on Handy Talkie (HT) radio technology, integrated with limited internet access, at Kasepuhan Gelaralam. It is not merely a technology system — it is a comprehensive solution that fundamentally addresses the community's vital need for valid and timely information.



Figure 9Example of HT Radio Device

Jarindes is significant for several reasons:

1. It provides a backup communication channel: when internet fails, Jarindes keeps information flowing.
2. It integrates digital and analog technology: combining SSTV encoder applications and digital controller modules with analog radio (HT and repeater), creating a flexible and efficient system.

3. It bridges tradition and modernity:built on the foundation of the Indonesian *kentongan* (traditional wooden alarm signal), Jarindes adapts the spirit of gotong royong (mutual cooperation) with modern radio technology.
4. It builds communication resilience in critical areas: in areas with no cellular coverage (blankspot) and high disaster risk (earthquakes, tsunamis, landslides), Jarindes provides an independent, resilient communication channel that does not depend on external infrastructure.
5. It is easy to maintain and resilient, the relatively simple system design ensures easy maintenance and operational durability.
6. It serves the broader community, its functions extend beyond emergency communication to include daily coordination, agricultural and cultural information broadcasting, and connecting remote hamlets.
7. It focuses on disaster information for indigenous communities, delivering accurate and timely disaster information adapted to the cultural context and needs of the community.
8. It encourages creativity, mutual cooperation, and discipline, the system's development and operation foster community innovation and social cohesion.



Figure 10 Repeater Workflow

B. How Jarindes Works

In principle, all devices in the Jarindes network from the HTs used by community members, to the Jarindes siren, to sensor modules are connected to a Repeater placed at the summit of Mount Pangapungan. This repeater functions as the 'heart of the network.' Every time voice, a warning, or data is transmitted through the radio

frequency, the repeater receives, amplifies, and redistributes the signal across the entire Jarindes coverage area. This mechanism ensures that every message can spread quickly and reliably, regardless of the challenging geographic terrain.



Figure 11 Pangapungan Tower (source: personal documentation)

1. HT-Kadus (Handy Talkie UHF Frequency Radio)

At the front line of Jarindes communication is the HT Peer-to-Peer (PTP) system known as 'HT-Kadus.' These devices are distributed to village heads (Kepala Dusun / Kadus) and key community figures across the territory. Each HT-Kadus has a unique call sign (e.g. 'Kadus-1' or 'Kemit-Pawon') for easy identification. HT-Kadus operates in two communication modes:

Direct Mode (PTP)	When two HTs are within close range (typically under 1 km with no major obstacles), they can communicate directly — like a standard walkie-talkie. Ideal for coordination between personnel in the same area.
Network Mode (via Repeater)	When users are far apart or separated by hilly terrain, the HT sends its signal to the Pangapungan Repeater. The repeater receives, amplifies, and re-broadcasts the signal across the entire coverage area, ensuring messages reach distant recipients.

2. The Pangapungan Repeater



Figure 12 Pangapungan Repeater (Personal Documentation)

The Pangapungan Repeater is the most critical component of the Jarindes architecture. It is an electronic unit equipped with a tower antenna and backup battery power, strategically placed at the highest point of Mount Pangapungan. It functions like a 'relay station' or 'giant signal amplification tower' reaching every corner of the Kasepuhan.

Coverage	With its elevated position, the repeater achieves a coverage radius of 20 to 50 kilometres depending on terrain and antenna height.
Power Source	Powered by solar panels connected to batteries, making it fully independent of the PLN grid, essential in rural areas where grid power is unreliable.
Frequency	Operates on VHF (144–148 MHz) and UHF (400–520 MHz) bands, which offer good range and reasonable penetration through forested terrain.

3. The Jarindes Siren

The Jarindes Siren is a modern evolution of the traditional kentongan. It integrates with the HT system, allowing leaders to use their HT as a wireless microphone to broadcast announcements

through loudspeakers mounted on the siren tower, reaching the entire community. It operates in two modes:

Emergency/ Disaster Mode	The siren sounds a predetermined alarm pattern, providing an emergency warning to all residents.
Announcement Mode	The system broadcasts spoken information (from the HT microphone) through the loudspeaker, allowing leaders to deliver important announcements to the community at large.

The siren is activated using specific DTMF codes verified by an Arduino controller module, preventing unauthorised activation. Its effective sound range is approximately 1–2 kilometres per siren unit.

4. Automated Voice Broadcast ('Jadwal Bewara')

The automated voice broadcast feature allows the system to transmit pre-recorded messages on a schedule. A timer module at Imah Gede (the centre of traditional governance) automatically sends recorded audio to the Pangapungan Repeater at predetermined times. The repeater broadcasts the message to all active HT-Kadus units and through the Jarindes Siren loudspeakers simultaneously. Example messages include reminders for communal work, agricultural schedules, and prayer times.

5. SSTV: Sending Images via Radio

Slow-Scan Television (SSTV) is a technique that allows Jarindes to transmit images through radio audio signals. A smartphone application (SSTV Encoder) converts a digital image into a sequence of audio tones. These tones are transmitted through the HT and distributed via the repeater. On the receiving end, the Robot36 application decodes the audio back into a viewable image. This is particularly valuable in areas without stable internet — enabling visual situation reports, damage photography, and identity verification entirely over radio.

C. Effectiveness of Jarindes

Terrain-Proof	HT radio operates reliably in areas with no cellular signal, making it a vital solution in hilly, rural terrain.
Low Cost	After initial equipment investment, operational costs are minimal — limited to HT batteries and repeater maintenance.
Self-Reliant	The network is entirely managed and operated by the community itself, with no dependence on external operators.
Multi-Function	Jarindes simultaneously serves as a voice communication system, mass information broadcaster, early warning system, and basic data transfer tool (images via SSTV).

D. Jarindes Network Topology

The Jarindes network forms a hybrid radial-mesh topology centred on key infrastructure. The frequency distribution follows the geographic contours of the territory and is adapted to the community's dynamic communication needs.

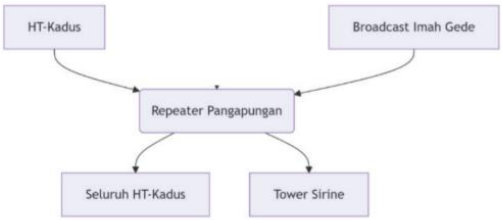


Figure 13 How Repeater Works

The topology comprises four key elements:

1. Pangapungan Repeater (Connectivity Hub)	Located at the highest point of the territory. Radiates signals in all directions. Receives, amplifies, and redistributes signals from all network elements.
2. Jarindes Sirens (Broadcast Nodes)	Siren towers at Gelaralam and Ciptagelar, connected bidirectionally to the repeater via dedicated radio links. Each broadcasts through loudspeakers and relays information to/from the repeater.
3. Imah Gede Base Station(Official Source)	Located at the centre of traditional governance. One-to-many broadcast: official announcements are sent to the repeater and simultaneously distributed to all HT-Kadus units and Jarindes Sirens.
4. HT-Kadus(Field Nodes)	The most distributed element: held by village heads, security officers, farming coordinators, and mitigation officers across all settlements. Capable of both PTP and repeater-assisted communication.

CHAPTER

04

HOW TO BUILD AJARINDES-TYPE SYSTEM

In this chapter, you will hopefully learn:

- ✓ Design and install a solar power system for an off-grid radio repeater.
- ✓ Understand the components and signal flow of a simple HT-based repeater (RX → COR → TX).
- ✓ Configure a dual-antenna repeater without a duplexer.
- ✓ Measure and optimise SWR (Standing Wave Ratio) for antenna systems.
- ✓ Build and program a Jarindes-type siren system using Arduino and DTMF codes.
- ✓ Transmit and receive images via SSTV using Android smartphones and HT radios.

This chapter provides the full technical guide for building a Jarindes-type radio repeater system. The approach uses two Handy Talkie (HT) units as the core of the repeater — an effective and cost-efficient solution. The system integrates with an off-grid solar panel for power independence, essential for remote areas and disaster situations.

A. Solar Power System

In the context of disaster preparedness, a solar-powered repeater is an absolute necessity. Solar power ensures the repeater can operate independently and continuously, regardless of grid power status. The Kasepuhan Gelaralam community has a long history of solar energy adoption, predating even the installation of their micro-hydro power plant (PLTMH).

The reference specification used at Pangapungan Hill is a 300 WP (Watt Peak) solar panel paired with a 12V 100Ah battery. This combination has proven sufficient to operate a simple repeater for 24 hours a day, 7 days a week.

300 WP Solar Panel	Designed to produce a maximum of 300 Watts under standard test conditions (1000 W/m² irradiance, 25°C cell temperature). Actual output varies with weather, time of day, and panel orientation. Physical size: approximately 1.5–2 square metres.
12V 100Ah Battery	Stores approximately 1,200 Wh (1.2 kWh) of energy. Can theoretically power a 60W repeater for 20 hours without any solar input. Deep-cycle sealed lead-acid (SLA) or lithium-ion batteries are recommended.
Solar Charge Controller	Regulates battery charging from the solar panel. MPPT (Maximum Power Point Tracking) controllers are recommended for maximum efficiency.
Cables & Connectors	Connect all components correctly and safely. Include appropriate fuses and circuit protection.

B. Radio Repeater (Pancar Ulang)

A repeater is an electronic device designed to extend the range of one-way radio communication. It works by receiving a weak radio signal, cleaning and amplifying it, then re-transmitting it at greater power on a different frequency. By placing the repeater at a strategic high point (e.g. a hilltop or tower), it can cover a much larger area than any individual HT.



Figure 14 RX COR TX (Personal Documentation)

Repeater Component Chain: RX → COR → TX

The core of a simple repeater consists of three elements:

Radio RX (Receiver)	The 'ear' of the repeater. Receives the weak incoming signal from a user's HT on the input frequency, amplifies and filters it, and passes it to the controller.
COR (Carrier Operated Relay)	The 'brain' of the repeater. Detects the COS (Carrier Operated Squelch) signal from the RX, which indicates a valid incoming transmission. When COS is detected, COR automatically activates the PTT on the TX radio and routes audio from RX to TX.
Radio TX (Transmitter)	The 'voice' of the repeater. Re-transmits the amplified audio signal on the output frequency (a different frequency from the input, known as the offset). This is what reaches all other HTs and sirens in the network.

The complete signal flow:

a user presses PTT on their HT and speaks → the signal is received by Radio RX → RX generates a COS signal → COR detects COS and activates PTT on Radio TX → TX re-transmits the audio on the output frequency → all HTs and sirens on the network receive the message.

When the user releases PTT, the COS signal disappears, COR releases TX PTT, and the repeater returns to standby. Here is the list of necessary components:

Component	Type	Quantity
Radio RX	HT- WLN KD-C1	1
Radio TX	HT- UV5R Model	1
Resistor	3.3K Ohm	1
Resistor	1K Ohm	1
Capacitor	470 uF/16V	1
Capacitor	47 uF/16V	1
Capacitor	100 nF	1
Diode	1N4148	2
Transistor	C1815	1
PCB	PCB-1 Layer	1
Cable	DC Cable	1
Jack	Headset Socket	1
DC Converter	Buck Converter XL4015	2

C. Antenna Configuration

Dual-Antenna Configuration (No Duplexer)

The Jarindes repeater uses two separate antennas, one for transmission (TX) and one for reception (RX) — without a duplexer. This is a simpler and more economical configuration. The key requirement is adequate physical separation between the two antennas (typically 5–10 metres vertical separation for UHF

frequencies) to prevent the TX signal from interfering with RX reception.

Advantages	Lower cost than duplexer configurations; simpler to implement; adequate performance for community-scale networks.
Disadvantages	Requires sufficient tower space for antenna separation; potential interference if separation is inadequate; placement planning is critical.

D. Antenna Installation

Proper antenna installation is critical for optimal repeater performance. Key steps include:

9. Select a tower location with good line-of-sight to the target coverage area.
10. Identify TX and RX frequencies and select appropriate omnidirectional UHF antennas.
11. Calculate minimum antenna separation (wavelength formula: $\lambda = c/f$, where $c = 3\times10^8$ m/s and f = frequency in Hz).
12. Install RX antenna at the highest point; TX antenna below it with calculated separation.
13. Run high-quality coaxial cable (e.g. RG-8) from each antenna to the repeater location, using cable clamps and drip loops.
14. Install lightning arrestors on each cable at the building entry point.
15. Connect proper grounding (grounding rod with heavy-gauge cable).
16. Connect cables to the repeater: RX antenna to RX port, TX antenna to TX port.

E. Testing and Tuning (SWR Measurement)



Figure 15 Standing Wave Ratio

Before operating the repeater, use an SWR (Standing Wave Ratio) meter to verify antenna system efficiency. An ideal SWR is close to 1:1, meaning nearly all power is transmitted and minimal power is reflected back. High SWR (above 2:1 or 3:1) indicates impedance mismatch, which can cause power loss, overheating, and damage to the transmitter.

SWR measurement procedure: connect the meter between the transceiver and the coaxial cable leading to the antenna. Set to low power, calibrate the forward reading, then switch to reflected/SWR reading. If SWR is too high, check connections, cable condition, and antenna tuning.

F. Operational Tips

- Add heatsinks to voltage regulators and the TX HT to prevent overheating.
- Add a Timer of Talk (TOT) to limit TX duration (recommended maximum: 3 minutes).
- Install LED monitoring indicators: Power ON (green), RX active (yellow), TX active (red).

With this system, the repeater should achieve an effective range of 3–15 km depending on terrain.

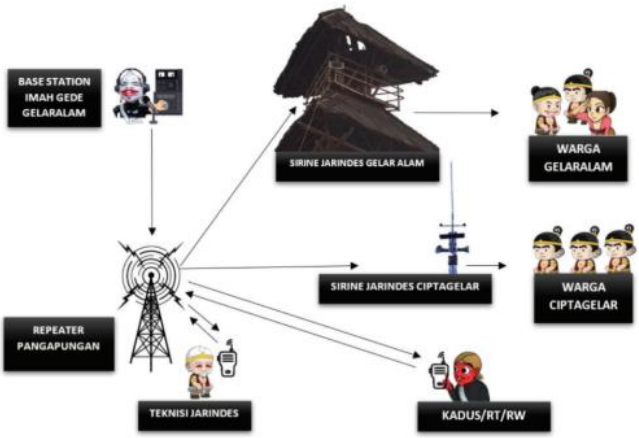


Figure 16 Repeater stations transmit a circular signal (frequency) that covers almost the entire map of the indigenous territory, like an invisible web.

G. The Jarindes Siren System

The Jarindes Siren adopts the traditional kentongan concept for modern village information dissemination. It works by allowing users to broadcast their voice through an HT, which is received by the siren unit's radio and amplified through horn speakers. The system uses Arduino-controlled DTMF code verification (e.g. *456#01) to prevent unauthorised activation. Two operational concepts exist:



Figure 17Sirens Jarindes (personal documentation)

Concept 1 — Direct Short-Range Access	The HT transmits directly to a nearby siren unit on a dedicated frequency (no DTMF code required). Simple and fast, but limited to the siren tower's direct radio range.
Concept 2 — Wide-AreaAccess via Repeater	The HT transmits to the repeater, which processes the DTMF code via Arduino and activates the siren system across the entire network. Information simultaneously reaches all HT users and all siren loudspeakers.

H. Automated Broadcast System

The automated broadcast system uses a timer switch to trigger pre-recorded MP3 messages at scheduled times. The MP3 player automatically activates the HT's PTT via a relay, broadcasting the recording through the repeater to the entire network. Components: timer switch, HT radio, MP3 player with SD card, relay module, 12V power supply (adapter, transformer, or solar panel).

I. SSTV Image Transmission via HT and Android

This innovation enables digital image transmission through the Jarindes radio network using Android smartphones. The process:

17. A user takes a photo on their Android phone and opens it in the SSTV Encoder application.
18. The app converts the image into a sequence of audio tones (the characteristic SSTV 'chirping' sound).
19. Audio is sent from the phone's headphone jack to the HT's audio input via a cable adapter.
20. The HT's VOX (Voice-Operated Exchange) feature automatically activates PTT when audio is detected.
21. The audio signal is transmitted through the repeater to all receiving HTs.
22. On the receiving end, a connected Android phone running the Robot36 decoder app automatically detects the SSTV signal and reconstructs the image in real time.
23. The decoded image is saved as a PNG file on the receiving device.

This method is invaluable for visual situation reports, damage documentation, identity verification, and distributing visual information, all without any internet connection. Image quality depends on radio signal strength and audio quality.

CHAPTER

05

TRANSFERABLE PRINCIPLES ANDIMPLEMENTATION SCENARIOS

In this chapter, you will hopefully learn:

- ✓ Extract the core design principles that make Jarindes effective and replicable.
- ✓ Understand the Jarindes network protocol stack and how each layer serves a function.
- ✓ Map Jarindes components to modern technological equivalents.
- ✓ Apply the model to three concrete Philippine/SEA implementation scenarios.
- ✓ Understand how LEO satellite connectivity and community radio complement each other.

The Jarindes system described in Chapters 3 and 4 is a working, community-owned disaster communication network operating in a specific geographic and cultural context. This chapter extracts the transferable principles, maps the technical architecture to a replicable framework, and provides concrete implementation scenarios for Philippine and Southeast Asian communities.

A. Design Principles from Jarindes

Six core design principles make Jarindes effective. Any community seeking to replicate the model should adopt these principles, even if the specific technology choices differ.

1. Hybrid Analog-Digital Architecture	The Jarindes backbone is analog radio (HT + repeater), which works when internet and cellular fail. Digital modules (SSTV, Arduino siren controller, automated scheduling) add capabilities that pure analog cannot provide. The lesson: use analog for reliability and digital for functionality. Do not build a system that depends entirely on either one.
2. High-Point Repeater ('Find Your Pangapungan')	Every community has a high point. a hilltop, a tall building, a telecommunications tower, a church steeple. The repeater goes there. The principle is that height equals coverage: a repeater at 500 metres elevation with a clear line of sight can cover 20–50 km in every direction. The higher and more centrally located, the better.
3. Solar-Powered Independence	The system must not depend on grid power, because grid power is the first thing that fails in a disaster. Solar panels and batteries provide 24/7 operation regardless of grid status. This principle applies equally to repeaters, siren units, and charging stations.
4. Cultural Integration ('Map to Existing Structures')	Jarindes works because it maps onto existing social structures: the kepala dusun (village head) system, the kentongan tradition, the adat (customary law) governance. Any replication must similarly map onto the target community's existing governance and communication norms. In the Philippines, this means the barangay structure: Barangay Captain, Purok leaders, BDRRMC. The HTs go to the people who already have authority and responsibility for community communication.

5. Layered Communication Modes	Jarindes is not one tool — it is a stack of communication modes, each serving a different need: PTP (nearby voice), repeater-assisted (distant voice), siren (mass broadcast), SSTV (visual data), automated scheduling (timed announcements). A resilient system layers multiple modes so that if one fails, others remain available.
6. Community Ownershipand Maintenance	The system is operated, maintained, and repaired by the community itself. No external operator is needed. This is what makes it sustainable: the community has full control, full understanding, and full motivation to maintain the system because they built it and they depend on it.

B. The Network Protocol Stack

Understanding the Jarindes architecture in protocol terms makes it easier to map to modern equivalents and to design new implementations:

Physical Layer	UHF radio (400–520 MHz), solar power, coaxial cable, omnidirectional antennas, horn speakers.
Link Layer	FM voice modulation, DTMF signalling (siren activation codes), VOX-triggered PTT (for SSTV and automated broadcast).
Application Layer	Voice communication (real-time), SSTV (image transfer), timed broadcast (scheduled messaging), siren activation (emergency alerting).

Mapping to modern equivalents:

Jarindes Component	Modern Equivalent
HT-Kadus PTP	Meshtastic node-to-node (LoRa radio)
Repeater relay	LoRa gateway or mesh relay node
DTMF siren activation	IoT MQTT triggers or webhook-based alert systems
SSTV image transfer	LoRa image transfer or Briar encrypted messaging
Automated broadcast	Scheduled push notifications or community alert system APIs
Kentongan/siren	Community PA system or mobile phone mass-alert (Cell Broadcast)

C. Implementation Scenarios

Scenario 1 — Coastal Barangay in Eastern Visayas (Typhoon-Prone)

A coastal barangay in Leyte or Samar faces annual typhoon risk. Cellular infrastructure routinely fails during storms. The poblacion has a cell tower and a municipal hall.

The 'Pangapungan'	Cell tower or municipal building rooftop — install a solar-powered UHF repeater at the highest available point.
The 'HT-Kadus'	Distribute HTs to Barangay Tanods, Purok leaders, and BDRRMC members. Each HT holder is responsible for relaying information within their sitio.
The 'Siren'	Horn speakers at the barangay hall and at coastal sitios, activated via DTMF codes from any authorised HT.
Governance	BDRRMC (Barangay Disaster Risk Reduction Management Committee) replaces the Kasepuhan adat governance as the coordinating body.
Integration	PAGASA typhoon warnings received via NDRRMC SMS blast or Starlink terminal at the barangay hall → relay through the radio network to all HT holders and sirens.
Estimated Cost	Basic system (1 repeater, 10 HTs, 2 siren units, solar power): approximately PHP 150,000–250,000 (USD 2,500–4,500).

Scenario 2 — Mountain Barangay in Cordillera (Earthquake/Landslide-Prone)

A remote mountain barangay in Benguet or Mountain Province has minimal cellular coverage and faces earthquake and landslide risk. The community has traditional leadership structures (datu, council of elders).

The 'Pangapungan'	Highest ridge above the community — install repeater with clear line-of-sight to all settlements.
The 'HT-Kadus'	Distribute HTs following existing IP (Indigenous Peoples) authority lines: tribal leaders, sitio coordinators, and designated disaster wardens.
The 'Siren'	Loudspeaker units at community gathering points, activated from any authorised HT via repeater.
Integration	PHIVOLCS seismic alerts received via Starlink or cellular connection at the community centre → relay through radio network. Meshtastic nodes on smartphones provide a complementary digital layer for HT holders who also carry phones.
Cultural Parallel	The IP community's traditional alarm systems (agung/gong, signal fires) serve the same function as the Kasepuhan kentongan. The radio network modernises but does not replace these traditions.

Scenario 3 — Island Municipality in Palawan or BARMM (Tsunami/Storm Surge Risk)

An isolated island municipality with limited connectivity faces tsunami and storm surge risk. The community includes both land-based settlements and near-shore fishing boats.

The 'Pangapungan'	Highest point on the island (lighthouse, hilltop, or dedicated tower) with a repeater covering both land and near-shore waters.
The 'HT-Kadus'	Distribute HTs to barangay captains on land AND to fishing boat captains operating within radio range. This extends the network's reach to maritime users — a dimension not present in the original Jarindes.
Satellite Backhaul	A Starlink terminal at the municipal hall provides internet backhaul, with the Jarindes-type radio network handling last-mile distribution to scattered sitios and boats beyond the terminal's Wi-Fi radius.
Integration	Philippine Coast Guard (PCG) distress frequencies monitored alongside the local network. SSTV capability allows fishing boats to transmit photographic reports of approaching weather or at-sea emergencies.
Licensing	NTC licensing for amateur radio use, or coordination with the local PARA chapter for community broadcasting permits under RA 3846 (Radio Control Law).

The Jarindes model is not a fixed blueprint to be copied exactly. It is a set of proven design principles, hybrid architecture, high-point repeater, solar independence, cultural integration, layered communication, community ownership.

That can be adapted to any disaster-prone community's geography, governance, and needs. The specific equipment and configuration will differ; the principles remain the same.

References

ANTARA News. (2025). Ministry restores 145 BTS, provides Starlink devices in W. Sumatra. https://en.antaranews.com/news/395005/

ANTARA News. (2025). RI Govt sends Starlink units, aid to flood-hit North Sumatra. https://en.antaranews.com/news/394229/

Common Room Networks Foundation. (2025). Modul Pelatihan Internet dan Kebencanaan, Cetakan Kedua. Bandung: Common Room.

BNPB (National Disaster Management Agency, Indonesia). Disaster statistics and EWS reports. https://bnpb.go.id/

NDRRMC (National Disaster Risk Reduction and Management Council, Philippines). Disaster response reports. https://ndrrmc.gov.ph/

PAGASA (Philippine Atmospheric, Geophysical and Astronomical Services Administration). Typhoon bulletins and climate data. https://bagong.pagasa.dost.gov.ph/

PHIVOLCS (Philippine Institute of Volcanology and Seismology). Seismic and volcanic monitoring. https://www.phivolcs.dost.gov.ph/

BMKG (Indonesian Agency for Meteorology, Climatology, and Geophysics). Earthquake and tsunami early warning. https://www.bmkg.go.id/

DICT (Department of Information and Communications Technology, Philippines). (2025). DICT Rolls Out 100 Starlink Units Donated by SpaceX Across Masbate Province. https://dict.gov.ph/

Globe Telecom / Starlink. (2026). Satellite-to-mobile D2D deployment for Mindanao earthquake response. Philippine media coverage via Inquirer, GadgetMatch, and Developing Telecoms.

Perkumpulan AirPutih. Emergency internet and disaster telecommunications resources.

PETZL. Professional Activity Handbooks and Safety Guides. https://www.petzl.com/

SpaceX / Starlink. (2025). Emergency Response: Indonesia and Sri Lanka Flood Response. https://starlink.com/support/