

AI-03151 Emergency Portable Field Network

Owner	Ⓒ Rigel Arcayan
Tags	Project
Created time	@November 11, 2025 5:36 AM

I need to design a portable, emergency Local Area Network (LAN) with internet access using an iOS hotspot (LTE) as the internet source. Do not use ICS, use pfsense.

My existing equipment includes:

1. Primary Laptop (Latitude E4310): Running Windows Server 2016 with a Hyper-V Ubuntu server VM, Home Assistant VM, pfsense VM and a Docker Lab. It has both Wi-Fi and LAN connectivity.
2. Secondary Laptop (Latitude E4300): Running bare-metal Ubuntu 25.0 with Docker, connected via LAN.
3. Networking Gear: An 8-port Power over Ethernet (PoE) switch and two PoE Cisco Wireless Access Points (WAPs).

Perfect — you already have a capable setup for a **self-contained, portable emergency LAN** with internet access through an **iOS hotspot** while avoiding Internet Connection Sharing (ICS). Using **pfSense** as the firewall/router is the professional way to handle routing, DHCP, and NAT control.

Let's go step-by-step.

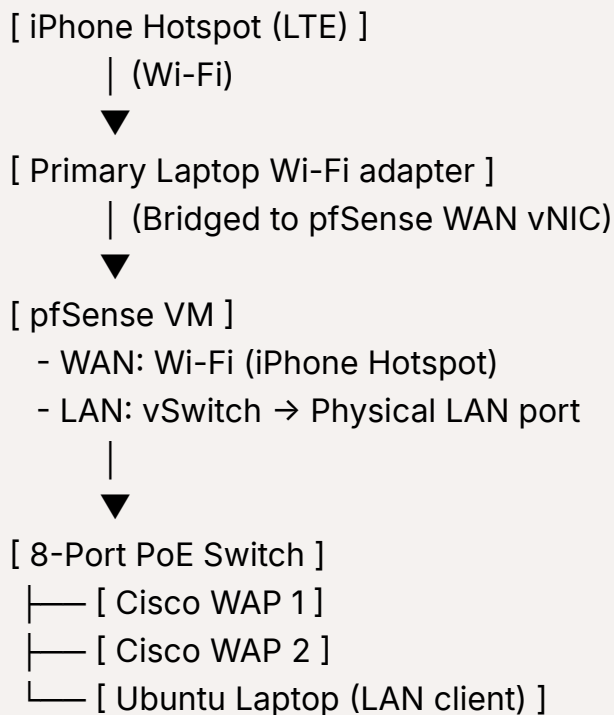
OBJECTIVE

Design a **portable LAN** powered by **iOS hotspot LTE** as WAN source, using **pfSense VM** on your primary laptop as the router/firewall, feeding LAN connectivity to a **PoE switch**, **secondary laptop**, and **Cisco WAPs**.

HIGH-LEVEL DESIGN OVERVIEW

Component	Role	Notes
iOS Hotspot	Internet (WAN source)	Connect via Wi-Fi to the host (Windows Server 2016)
pfSense VM	Router, DHCP, NAT	Two virtual NICs: one bridged to Wi-Fi (WAN), one bridged to LAN adapter
Windows Server 2016 (Host)	Hyper-V Host + Network Bridge point	Handles virtual switching between pfSense and LAN
8-port PoE Switch	LAN Distribution	Feeds secondary laptop + WAPs
Cisco PoE WAPs	Wi-Fi extension	LAN access, optional SSID for guests or IoT
Ubuntu Laptop	Client node	Docker services connected via wired LAN

NETWORK FLOW (Simplified)



STEP-BY-STEP IMPLEMENTATION

1. Configure Windows Server 2016 Networking

- Ensure **Wi-Fi** connects to your **iPhone hotspot** for internet.
- Do **NOT** enable ICS.
- In **Hyper-V Manager** → **Virtual Switch Manager**, create:
 - **vSwitch_WAN**: External switch bound to **Wi-Fi adapter** (uncheck "Allow management OS to share")
 - **vSwitch_LAN**: External switch bound to **Ethernet LAN port**

Now pfSense will use:

- `vSwitch_WAN` for WAN (to hotspot)
 - `vSwitch_LAN` for LAN (to your PoE switch)
-

2. Configure pfSense VM (Hyper-V)

VM NIC Setup:

- **Adapter 1**: Connect to `vSwitch_WAN`
- **Adapter 2**: Connect to `vSwitch_LAN`

pfSense Configuration:

- **WAN interface**: DHCP (it'll get a 172.x.x.x or 192.168.x.x from your iPhone)
- **LAN interface**: Static (e.g. 10.10.10.1/24)
- **DHCP Server**: Enable on LAN (range 10.10.10.100–10.10.10.200)
- **NAT**: Automatic outbound NAT → enabled by default

Optional Hardening:

- Disable IPv6 unless needed
 - Enable pfBlockerNG for threat filtering
 - Limit DNS to 1.1.1.1 or 8.8.8.8 (static on WAN)
-

3. Connect Physical LAN

1. Plug **Primary Laptop LAN port** → **PoE switch**.
2. Plug **Ubuntu Laptop** and **Cisco WAPs** into the switch.
3. Verify all devices receive 10.10.10.x IPs via pfSense DHCP.

4. Configure Cisco WAPs

- **Mode:** Access Point (Bridge)
- **DHCP:** Disabled
- **Gateway:** 10.10.10.1 (pfSense)
- **SSID 1:** Internal LAN (WPA2)
- **SSID 2 (Optional):** Guest VLAN (can be configured later in pfSense VLANs)

5. Testing & Validation

Test	Expected Result
From pfSense → Ping 8.8.8.8	✓ Successful
From Ubuntu laptop → ping 10.10.10.1	✓ Successful
From Ubuntu laptop → ping 8.8.8.8	✓ Successful
From Ubuntu laptop → browse internet	✓ Works via iPhone LTE

If everything passes, your portable emergency network is live.

OPTIONAL IMPROVEMENTS

Feature	Tool	Purpose
Captive Portal	pfSense built-in	Control LAN/Wi-Fi access
VPN Gateway	WireGuard / OpenVPN	Secure remote access
Monitoring	pfSense Dashboard + NetFlow	Track bandwidth per device
Dynamic DNS	DuckDNS or Cloudflare	Reach pfSense remotely via LTE IP



ACTION PLAN SUMMARY

Step	Task	Tool
1	Connect iPhone hotspot to host Wi-Fi	iOS + Windows
2	Create 2 virtual switches (Wi-Fi & LAN)	Hyper-V
3	Assign both NICs to pfSense VM	pfSense VM
4	Configure pfSense DHCP + NAT	pfSense WebGUI
5	Connect LAN port → PoE switch	Physical
6	Connect WAPs + Ubuntu	Physical
7	Test connectivity	Ping + Browser

Would you like me to include **IP addressing, VLANs, and firewall rules** in the next layer of design (for isolation, Home Assistant, Docker, and IoT segmentation)? It's the next logical step for a fully self-contained, resilient mobile lab.

Excellent. Let's now evolve your portable emergency LAN into a **professionally segmented network** that cleanly separates and protects your environments — pfSense, Docker Lab, Home Assistant, and IoT — while retaining full internet access via the iOS hotspot.



OVERVIEW: WHAT WE'RE ADDING

We'll introduce:

1. **Four VLANs** for clean segmentation
2. **IP addressing plan** for each zone
3. **Firewall rules** (who can talk to who)
4. **Switch & WAP VLAN setup**
5. **Optional pfSense services** (DNS, VPN, captive portal)



1. VLAN STRUCTURE AND IP PLAN

VLAN	Purpose	Subnet	Example Devices	Access Rules
10 (MGMT)	Management	10.10.10.0/24	pfSense GUI, switches, WAPs	Only admin laptop access
20 (SERVER)	Core servers	10.10.20.0/24	Home Assistant VM, Ubuntu Docker host	Full outbound, restricted inbound
30 (IOT)	Smart devices	10.10.30.0/24	Sensors, cameras, plugs	Internet-only access
40 (GUEST)	Temporary clients	10.10.40.0/24	Guest phones/laptops	Internet only, no LAN access

All VLANs will exit through pfSense → WAN → iPhone hotspot.

2. PFSENSE CONFIGURATION

Interface Setup

1. Inside pfSense, go to **Interfaces** → **Assignments** → **VLANs**
2. Create VLANs on the **LAN physical interface**:
 - VLAN 10 (MGMT)
 - VLAN 20 (SERVER)
 - VLAN 30 (IOT)
 - VLAN 40 (GUEST)
3. Assign each VLAN a new interface (OPT1–OPT4)
4. Enable and name them:
 - MGMT (VLAN10) – IP: 10.10.10.1/24
 - SERVER (VLAN20) – IP: 10.10.20.1/24
 - IOT (VLAN30) – IP: 10.10.30.1/24
 - GUEST (VLAN40) – IP: 10.10.40.1/24

DHCP Setup

- **Enable DHCP** on each VLAN with:
 - MGMT: 10.10.10.100–150
 - SERVER: 10.10.20.100–150
 - IOT: 10.10.30.100–150
 - GUEST: 10.10.40.100–150

NAT

- Keep **Automatic Outbound NAT** (pfSense will NAT all VLANs to the iPhone WAN).

3. FIREWALL RULES (Layered Access)

Source VLAN	Destination	Action	Description
MGMT	Any	✓ Allow	Admin has full control
SERVER	WAN + MGMT	✓ Allow	Servers can update OS and be managed
SERVER	IOT, GUEST	✗ Block	Prevent cross-network traffic
IOT	WAN only	✓ Allow	Internet access only
IOT	MGMT/SERVER	✗ Block	No lateral movement
GUEST	WAN only	✓ Allow	Guests can surf internet only
GUEST	All local	✗ Block	Full isolation

You can manage all this in **Firewall → Rules → [VLAN Interface]** in pfSense.

4. POE SWITCH CONFIGURATION

VLAN Tagging

In your **PoE switch web GUI or CLI**:

- **Port 1** (to pfSense LAN): **Trunk** — Tagged VLANs 10,20,30,40
- **Port 2** (to Home Assistant/Docker server): **Access VLAN 20**
- **Port 3** (to WAP1): **Trunk VLANs 20,30,40**

- **Port 4** (to WAP2): **Trunk VLANs 20,30,40**
- **Remaining ports:** assign as needed per zone

This allows each WAP to broadcast multiple SSIDs per VLAN.

5. CISCO WAP CONFIGURATION

On each Cisco AP:

- **SSID 1:** "ServerNet" → VLAN 20
- **SSID 2:** "IoTNet" → VLAN 30
- **SSID 3:** "GuestNet" → VLAN 40

Disable DHCP on the WAP; let pfSense handle it.

6. OPTIONAL PFSENSE ADD-ONS

Feature	Use Case
pfBlockerNG	Ad-blocking, country block
WireGuard VPN	Secure remote access to your lab
Dynamic DNS (DuckDNS, Cloudflare)	Remote access via LTE IP
DNS Resolver (unbound)	Local name resolution
Captive Portal (Guest VLAN)	Control guest Wi-Fi logins

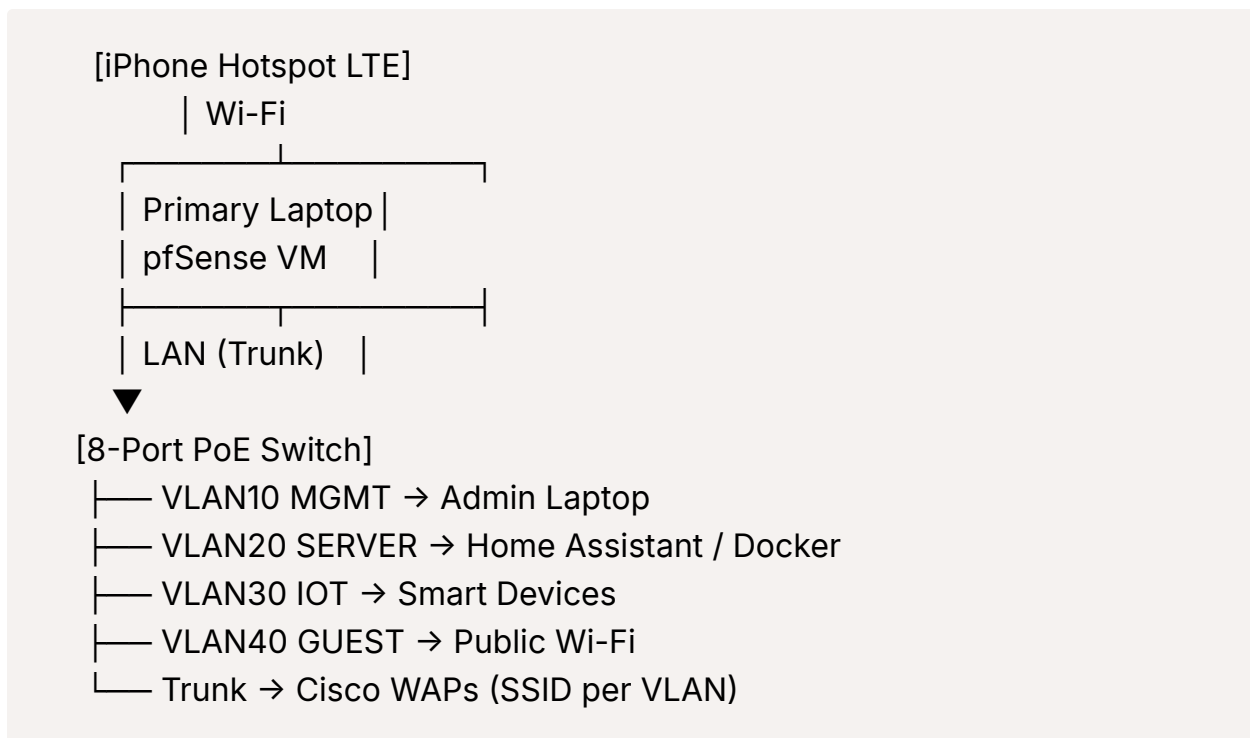
7. TESTING MATRIX

Test	Expected
Ping 10.10.10.1 from admin laptop	✓ OK
Ping 10.10.20.1 from Home Assistant	✓ OK
IoT device internet access	✓ OK
IoT device → Server ping	✗ Blocked
Guest Wi-Fi → Internet	✓ OK
Guest Wi-Fi → LAN ping	✗ Blocked

8. ACTION PLAN SUMMARY

Step	Task	Platform
1	Create VLANs in pfSense	pfSense
2	Assign IPs & enable DHCP	pfSense
3	Apply firewall rules	pfSense
4	Tag VLANs on LAN switch	PoE Switch
5	Map SSIDs to VLANs	Cisco WAPs
6	Connect servers and test	Physical
7	Add pfBlockerNG + DDNS	pfSense
8	Validate isolation & routing	Ping/Traceroute

RESULTING TOPOLOGY (Simplified)



Would you like me to extend this into a **portable "Pelican-case wiring and power layout"** (including PoE switch power, router VM power management, and cable routing best practices)? It's the next step to make your emergency LAN field-ready.

Excellent — let’s now turn your **pfSense-based emergency LAN** into a **field-deployable, Pelican-case unit** — compact, self-powered, and robust enough for rapid deployment during disasters, power outages, or field operations.

Below is a professional-grade design that merges your existing hardware (Latitude laptops, PoE switch, WAPs) into a transportable, single-case system.

OBJECTIVE

Design a **portable, powered Pelican-case LAN** that:

- Uses **iPhone LTE hotspot** as internet source (WAN)
- Hosts **pfSense, Home Assistant, and Docker Lab** via Hyper-V
- Distributes LAN through **PoE switch** and **Cisco WAPs**
- Runs 4+ hours on battery power
- Deploys in <5 minutes

1. SYSTEM OVERVIEW

Layer	Component	Function
Internet Layer	iPhone Hotspot (LTE)	Primary WAN source via Wi-Fi
Routing Layer	pfSense VM on Latitude E4310	DHCP, VLAN, NAT, Firewall
Compute Layer	Ubuntu VM / Home Assistant / Docker Lab	Automation, control, lab
Distribution Layer	8-Port PoE Switch	LAN backbone (data + power)
Access Layer	Cisco PoE WAPs (x2)	Wireless access for VLANs
Power Layer	UPS/Power Bank + DC Distribution	Field power redundancy
Enclosure	Pelican Case (1550–1600 series)	Physical protection & portability

2. PHYSICAL LAYOUT (TOP VIEW)

[Left Compartment]	
- Laptop 1 (pfSense host)	
- Laptop 2 (Docker/Ubuntu)	
[Center Compartment]	
- 8-Port PoE Switch	
- Power Strip / DC Bus	
- Cabling Patch Area	
[Right Compartment]	
- 2x Cisco WAPs (stacked or hinged)	
- LTE iPhone mount w/ vent cable port	

Add **vented grommets** for airflow and **rubber gaskets** for cable exits.

3. POWER SYSTEM DESIGN

Main Power Options

Power Source	Connection	Use
AC mains (110–240V)	via power strip	Normal operation
UPS (100–300W)	inline	Brownout buffer
DC battery (12–24V)	via inverter or DC adapter	Field operation
USB-C PD 100W power bank	laptop power	Lightweight mobility

Power Draw Estimate

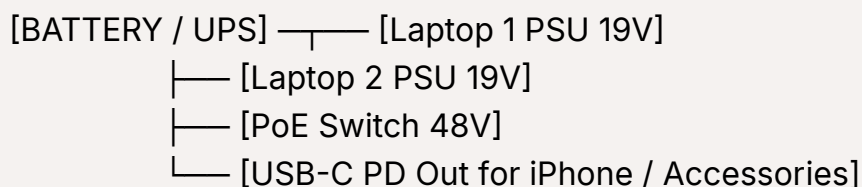
Device	Power	Runtime (on 300Wh battery)
Laptop 1 (pfSense VM)	25–30W	~8–10 hrs

Device	Power	Runtime (on 300Wh battery)
Laptop 2 (Ubuntu)	20W	~10 hrs
PoE Switch	10–15W (no PoE load)	~12 hrs
2x Cisco WAPs	20–25W	~8 hrs
Total (Avg)	75–90W	3–4 hrs on 300Wh , extendable to 6–8 hrs on 600Wh

Recommended battery packs:

- EcoFlow River 2 / Anker 757 / Bluetti EB3A (AC/DC + USB-C PD)
- Include inline **12V DC barrel outputs** for switch and APs

4. POWER DISTRIBUTION WIRING



- Use **Anderson Powerpole** or **XT60 connectors** for modular DC distribution
- Use **labelled inline fuses** (5A–10A) per branch
- Add a **voltmeter module** to monitor battery health

5. NETWORK CABLING LAYOUT

From	To	Cable	Notes
Laptop 1 (LAN port)	PoE Switch Port 1	Cat6 (Trunk VLANs 10/20/30/40)	Tagged VLAN trunk
PoE Switch Port 2	Laptop 2	Cat6	Access VLAN 20
PoE Switch Ports 3–4	Cisco WAPs	Cat6	Trunk VLANs 20/30/40

From	To	Cable	Notes
PoE Switch Port 5+	Open for LAN devices	-	Flexible use

Use **flat Cat6 patch cables** with **color coding**:

- Red = WAN
- Blue = Server VLAN
- Yellow = IoT
- Green = Guest

6. NETWORK LOGIC SUMMARY (ON THE MOVE)

Path	Function
iPhone LTE → Wi-Fi	Internet uplink
Wi-Fi → pfSense (WAN)	WAN DHCP via Hyper-V vSwitch
pfSense (LAN trunk) → PoE Switch	VLAN distribution
VLAN 20 → Ubuntu/Home Assistant	Server subnet
VLAN 30 → IoT	Isolated automation
VLAN 40 → Guests	Internet-only
VLAN 10 → Management	Admin access only

7. FIELD DEPLOYMENT CHECKLIST

Step	Action	Notes
1	Power on battery or AC	Ensure all devices energize
2	iPhone hotspot ON	Connect to Wi-Fi (SSID "RigelLTE")
3	pfSense WAN connects	Verify DHCP lease
4	Check pfSense dashboard	WAN IP + gateway = OK
5	Verify LAN DHCP	Clients receive correct VLAN IP
6	Confirm WAP SSIDs active	ServerNet / IoTNet / GuestNet

Step	Action	Notes
7	Ping + Internet test	Validate outbound & isolation
8	Begin Docker / Home Assistant services	Ready for operations

8. FIELD MAINTENANCE TIPS

Tip	Purpose
Store 3–6 short Cat6 patch cables in lid pouch	Fast field setup
Keep a spare USB Wi-Fi adapter	Backup WAN
Use velcro cable ties for rapid teardown	Prevent tangle
Add external antenna port for LTE tether	Better signal
Regularly update pfSense snapshots	Easy recovery
Label VLAN color codes and ports	No confusion under stress



ACTION PLAN SUMMARY

Step	Task	Category
1	Select Pelican 1550–1600 case	Hardware
2	Mount PoE switch & power strip	Layout
3	Install 12V/48V DC distribution bus	Power
4	Prepare short color-coded Cat6 patch cables	Cabling
5	Configure VLANs, pfSense, WAPs	Network
6	Test 4-hour battery runtime	Power validation
7	Label and laminate quick setup guide	Field ops
8	Final test end-to-end LTE-to-LAN	Deployment-ready

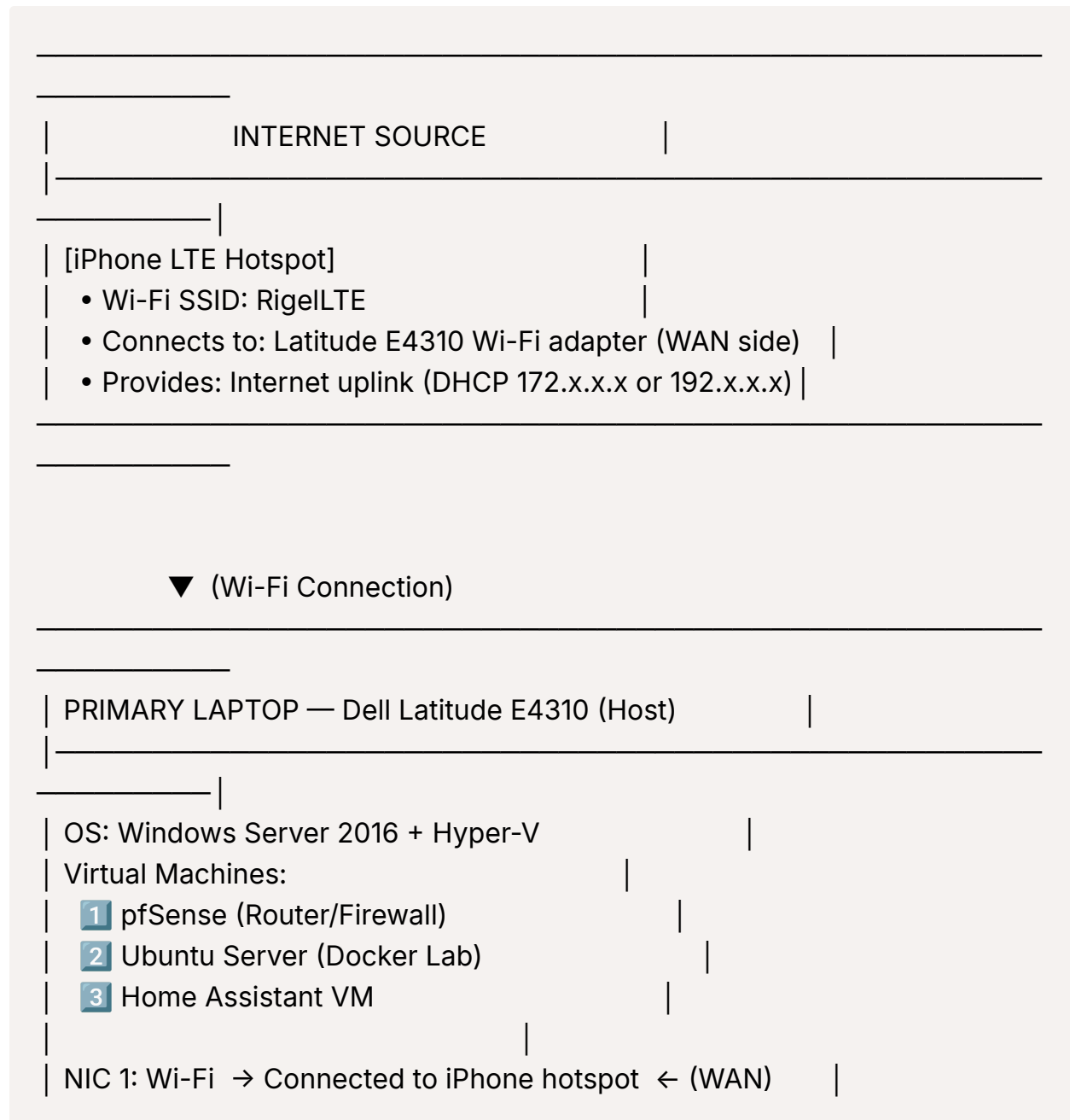
Would you like me to **add a labeled wiring diagram (topology + power flow)** for this Pelican-case LAN — text-based schematic now or image-based diagram next?

Perfect — here's your **text-based wiring and power topology diagram** for your **Portable pfSense Emergency LAN (Pelican-case setup)**.

It shows **data flow, power distribution, and physical connections** for quick field deployment.

TEXT-BASED SYSTEM DIAGRAM

Portable Emergency LAN — pfSense + LTE Hotspot



| NIC 2: LAN Port → vSwitch_LAN (Trunk VLANs 10,20,30,40) |
| pfSense vNIC Assignments: |
| - WAN → Wi-Fi (vSwitch_WAN) |
| - LAN → Ethernet (vSwitch_LAN) |
| LAN IP: 10.10.10.1/24 (Gateway for all VLANs) |
| VLANs configured: |
| VLAN10 MGMT - 10.10.10.0/24 |
| VLAN20 SERVER- 10.10.20.0/24 |
| VLAN30 IOT - 10.10.30.0/24 |
| VLAN40 GUEST - 10.10.40.0/24 |
| DHCP: Active on all VLANs |
| NAT: Automatic outbound via iPhone WAN |

▼ (Ethernet Trunk)

| 8-Port PoE Switch (Managed) |

| Port 1: Trunk to pfSense LAN (Tagged VLANs 10/20/30/40) |
| Port 2: Access VLAN 20 (Ubuntu Laptop) |
| Port 3: Trunk VLANs 20/30/40 (Cisco WAP 1) |
| Port 4: Trunk VLANs 20/30/40 (Cisco WAP 2) |
| Ports 5–8: Optional client ports (assign VLAN as needed) |
| PoE Power: 48V DC from Pelican DC Bus |

▼ (LAN Distribution)

| SECONDARY LAPTOP — Dell Latitude E4300 |

OS: Ubuntu 25.0 (bare-metal) |
Connected via LAN Port → PoE Switch Port 2 (VLAN 20) |
IP: 10.10.20.x assigned by pfSense |
Role: Docker Host / Lab Services |

▼ (Wireless Access)

CISCO PoE WIRELESS AP #1 (Trunked VLANs 20/30/40) |

SSID1: ServerNet → VLAN20 (Admin/Server Access) |
SSID2: IoTNet → VLAN30 (IoT Devices) |
SSID3: GuestNet → VLAN40 (Guest Internet Only) |
DHCP Source: pfSense (per VLAN) |
Gateway: 10.10.x.1 (pfSense LAN IP per VLAN) |

CISCO PoE WIRELESS AP #2 (Trunked VLANs 20/30/40) |
— Config identical to WAP #1 for coverage redundancy — |

POWER DISTRIBUTION |

POWER SOURCE OPTIONS: |

- AC mains (110–240V) → Power strip
- UPS (100–300W) inline backup
- Portable Power Station (300–600Wh) → DC Bus

DC BUS OUTPUTS (with fuses & labels):

- 19V → Laptop 1 PSU (pfSense Host)
- 19V → Laptop 2 PSU (Ubuntu)
- 48V → PoE Switch (PoE Injected to WAPs)
- USB-C PD (100W) → iPhone charging / accessories

ESTIMATED LOAD: 75–90W total

→ Runtime ~4 hrs (300Wh) or ~8 hrs (600Wh)

CABLING COLOR CODE

- Red = WAN (Wi-Fi)
- Blue = VLAN20 (Server)
- Yellow = VLAN30 (IoT)
- Green = VLAN40 (Guest)
- White = VLAN10 (Mgmt)
- Black = Power (DC Lines)

QUICK DEPLOYMENT SEQUENCE

1. **Power up** battery or plug AC → power bus
2. **Turn on both laptops** (pfSense host boots first)

3. **Connect iPhone hotspot** to Latitude E4310 Wi-Fi
4. **Verify pfSense WAN IP lease**
5. **Confirm VLAN DHCP leases** on LAN and WAPs
6. **Bring up WAPs** (auto-SSID broadcast)
7. **Ping + browse test** from Ubuntu and Wi-Fi clients
8. **Deploy Home Assistant & Docker services**

FIELD NOTES

- If WAN fails (hotspot drops), pfSense remains operational — LAN and Docker Lab continue offline.
- Add a **USB LTE modem or 5G router** later for dual WAN redundancy.
- A small **OLED voltmeter + fan module** keeps power visible and heat under control inside the case.
- Optional **mount**: use Velcro or 3D-printed brackets for the switch and power module on the Pelican base.

Would you like me to expand this next into a **disaster-ready checklist and troubleshooting flow**, covering quick fixes for “no internet,” “no DHCP,” or “no VLAN isolation” in field conditions?

Perfect — let’s create a **disaster-ready troubleshooting and operational checklist** for your **portable pfSense emergency LAN**, so you can quickly fix common problems in the field without diving into complex configs. This covers **internet issues, DHCP failures, VLAN problems, and basic device recovery**.

DISASTER-READY FIELD CHECKLIST

1 POWER & DEVICE CHECK

Step	Check	Action
1	Battery/UPS power	Verify voltage >90% and AC/DC switch ON
2	Laptops ON	Ensure primary (pfSense host) boots first

Step	Check	Action
3	PoE Switch ON	Check LEDs; verify PoE status for WAPs
4	Cisco WAPs ON	LEDs steady → ready for clients

Tip: Keep **spare fuses** and **extra short power cables** in the Pelican lid pouch.

2 WAN / INTERNET TROUBLESHOOTING

Symptom	Quick Test	Fix
No internet	On pfSense, check Status → Interfaces → WAN IP	Reconnect iPhone hotspot; verify Wi-Fi adapter on host
WAN IP not assigned	Run <code>ping 8.8.8.8</code> from pfSense shell	Reboot hotspot; toggle pfSense WAN DHCP
Slow internet	Ping 8.8.8.8 latency	Move iPhone for better LTE signal; consider external antenna

Tip: Keep a **USB LTE dongle** as backup WAN if hotspot fails.

3 LAN / DHCP TROUBLESHOOTING

Symptom	Quick Test	Fix
Client gets no IP	<code>ipconfig</code> or <code>ifconfig</code> → no DHCP	Verify pfSense LAN interface up; check DHCP service
Wrong VLAN IP	Client IP outside VLAN subnet	Confirm switch port VLAN assignment (trunk vs access)
No access to server	Ping pfSense LAN IP from client	Confirm VLAN tagging on switch/WAP; reboot client

4 VLAN / FIREWALL TROUBLESHOOTING

Symptom	Quick Test	Fix
VLAN isolation not working	Ping from Guest → Server	Check pfSense firewall rules; verify switch trunk tagging
IoT can't reach internet	Ping 8.8.8.8 from IoT device	Confirm pfSense NAT & VLAN gateway 10.10.30.1

Symptom	Quick Test	Fix
Management laptop can't reach pfSense GUI	Ping 10.10.10.1	Ensure laptop is in VLAN10; check switch port config

5 WIRELESS ACCESS POINT ISSUES

Symptom	Quick Test	Fix
SSID not visible	Scan Wi-Fi	Check PoE and AP LEDs; reboot AP
Wrong VLAN on Wi-Fi	Ping pfSense VLAN gateway	Confirm AP VLAN mapping matches SSID
Device cannot get IP	Wi-Fi connected but no internet	Confirm DHCP relay / VLAN assignment in pfSense

6 DOCKER / HOME ASSISTANT ISSUES

Symptom	Quick Test	Fix
VM not starting	Hyper-V console	Ensure pfSense VM boots first; check vSwitch connection
Docker Lab unreachable	Ping Docker VM IP	Verify LAN VLAN, firewall rules, and Docker network config
Home Assistant offline	Ping 10.10.20.x	Ensure VM running; VLAN20 routing correct

7 QUICK FIELD RESET SEQUENCE

1. **Power cycle hotspot**
2. **Reboot pfSense VM** (primary laptop)
3. **Ping WAN & LAN IPs**
4. **Reboot switch** (if VLANs not passing)
5. **Reboot WAPs** (if Wi-Fi clients fail)
6. **Reconnect clients**
7. **Confirm DHCP and internet**

8. Resume Docker/Home Assistant services

8 FIELD BEST PRACTICES

- Keep **all patch cables short and labeled**.
- Maintain **Pelican lid checklist**: USB Wi-Fi adapter, spare patch cables, fuses, small screwdriver, Velcro straps.
- Use **LED monitoring**: switch + WAP LEDs indicate VLAN and PoE health.
- Document **hotspot SSID & password** in waterproof card inside the case.
- Take **pfSense config backup** on USB/Cloud for instant restore.

9 TROUBLESHOOTING FLOW (SUMMARY)

[No Internet]

|
├─ Check WAN IP on pfSense → OK? → Yes → Check NAT/firewall → No
→ Fix NAT
|
└─ No WAN IP → Reconnect hotspot → Reboot pfSense WAN

[No LAN IP / DHCP]

|
├─ Check pfSense LAN VLANs → DHCP Enabled? → No → Enable
|
└─ Switch port VLAN mismatch → Correct tagging

[VLAN Isolation Fails]

|
├─ Check firewall rules → Adjust
└─ Check switch trunk/tagging → Correct

[Wi-Fi Problems]

|
├─ SSID down → Reboot AP

- └ Wrong VLAN → Fix AP VLAN config
- └ No DHCP → Confirm pfSense DHCP relay for VLAN

This checklist ensures you can **rapidly restore your portable LAN**, maintain internet access, and keep IoT / server / guest VLANs properly segmented — all **without touching complex pfSense configs under stress**.

If you want, I can also create a **“5-minute rapid deploy procedure”** — a step-by-step field deployment guide **from Pelican case closed to fully operational network**, optimized for emergencies.

Do you want me to do that next?

Perfect — here’s a **5-Minute Rapid Deployment Guide** for your **Pelican-case portable pfSense emergency LAN**. It’s designed for **emergency or field use**, minimizing setup steps while ensuring all VLANs, WAN, and Wi-Fi work correctly.

5-MINUTE RAPID DEPLOY PROCEDURE

Step 0 — Pre-Deployment Prep (Done Ahead of Time)

- Case packed with laptops, PoE switch, WAPs, patch cables, power sources, iPhone, and Velcro ties.
- Labeled cables for VLANs & power.
- pfSense configuration pre-saved and backed up.
- Battery/UPS fully charged.
- iPhone LTE hotspot credentials memorized or printed.

Step 1 — Power Up (0:00–0:45 sec)

1. Open Pelican case.
2. Turn ON **battery / UPS**. Check voltmeter → confirm voltage >90%.
3. Power ON **primary laptop** (pfSense VM host) first.
4. Power ON **secondary laptop** (Ubuntu / Docker) and **PoE switch**.

5. PoE switch powers WAPs automatically. Check LEDs: steady green = OK.
-

Step 2 — Connect Internet (0:45–1:30 min)

1. Turn ON **iPhone LTE hotspot** → SSID: RigellTE.
 2. Primary laptop Wi-Fi connects to hotspot → pfSense WAN gets DHCP IP.
 3. Verify WAN IP on pfSense dashboard → ping 8.8.8.8 to confirm internet.
-

Step 3 — Verify LAN & VLANs (1:30–2:30 min)

1. Connect **secondary laptop** to LAN port → should get 10.10.20.x (Server VLAN).
 2. Ping pfSense LAN interfaces for VLANs:
 - MGMT: 10.10.10.1
 - SERVER: 10.10.20.1
 - IOT: 10.10.30.1
 - GUEST: 10.10.40.1
 3. Confirm **DHCP leases** on pfSense for all VLANs.
-

Step 4 — Wi-Fi Check (2:30–3:30 min)

1. Confirm Cisco WAPs powered and broadcasting SSIDs:
 - ServerNet → VLAN20
 - IoTNet → VLAN30
 - GuestNet → VLAN40
 2. Connect a test device to each SSID → verify correct IP and internet.
 3. Ping gateway from each VLAN → ensures isolation works.
-

Step 5 — Start Services (3:30–4:30 min)

1. On primary laptop VM, start **Home Assistant VM**.

2. On secondary laptop, start **Docker Lab services**.
 3. Ensure all services get correct VLAN IPs.
-

Step 6 — Final Verification & Documentation (4:30–5:00 min)

1. Ping from client devices → internet and VLAN gateway.
 2. Confirm WAP coverage and VLAN isolation.
 3. Check voltmeter → battery >75% for runtime.
 4. Close case lid partially, leaving ventilation ports open for airflow.
 5. Ready for operation.
-

FIELD TIPS

- Keep **short Velcro straps** to secure laptops in place.
 - Use **colored patch cables** for VLANs to avoid mistakes.
 - Maintain a **printed mini-diagram** of VLANs, SSIDs, and IP ranges inside lid.
 - For WAN failure: switch hotspot off/on, or plug in a **backup USB LTE dongle**.
 - Quick **reboot sequence** if something fails: pfSense VM → PoE switch → WAPs → clients.
-

This procedure ensures that from **Pelican case closed → fully operational network** takes **5 minutes or less**, with proper internet access, VLAN segmentation, and Wi-Fi coverage.

If you want, I can also create a **“field troubleshooting quick reference card”** — a one-page text sheet you can laminate inside the Pelican case for rapid problem-solving without laptops.

Do you want me to do that next?

Perfect — here’s a **Field Troubleshooting Quick Reference Card** for your **Pelican-case portable pfSense emergency LAN**. It’s designed as a **one-page laminated guide** for rapid problem-solving in the field.



FIELD TROUBLESHOOTING QUICK REFERENCE — PORTABLE PfSense LAN

1 POWER CHECK

Symptom	Action
No power to laptops/switch/WAPs	1. Verify battery/UPS ON2. Check DC/AC connections3. Check inline fuses4. Verify voltmeter >90%
Short runtime	Use higher-capacity battery or reduce laptop brightness / CPU load

2 WAN / INTERNET

Symptom	Quick Fix
No internet	1. Check pfSense WAN IP2. Reconnect iPhone hotspot3. Ping 8.8.8.8 from pfSense4. Reboot pfSense WAN interface
Slow LTE	Move iPhone for better signalUse external antenna if available
WAN IP not assigned	Toggle Wi-Fi adapterRestart pfSense WAN DHCP

3 LAN / DHCP

Symptom	Quick Fix
Client gets no IP	1. Check pfSense LAN DHCP active2. Confirm client VLAN assignment3. Reboot client if needed
Wrong IP / VLAN	Verify switch port VLAN config (trunk vs access)Check pfSense VLAN IP range

4 VLAN / FIREWALL

Symptom	Quick Fix
VLAN isolation fails	1. Check pfSense firewall rules per VLAN2. Verify switch port trunking/tagging3. Confirm client VLAN assignment
IoT cannot reach internet	Ensure NAT + gateway correct on pfSense VLAN30
Admin cannot reach pfSense GUI	Confirm device in VLAN10; check switch/access port

5 WIRELESS ACCESS POINTS

Symptom	Quick Fix
SSID not visible	1. Check WAP PoE power2. Reboot AP3. Confirm SSID VLAN mapping
Devices connect but no internet	Confirm VLAN DHCP relay on pfSenseCheck firewall rules
Wrong VLAN on Wi-Fi	Adjust AP VLAN mapping

6 DOCKER / HOME ASSISTANT

Symptom	Quick Fix
VM not running	Boot pfSense VM firstCheck Hyper-V VM assignment
Docker Lab unreachable	Verify LAN VLAN assignmentCheck firewall rules
Home Assistant offline	Confirm VM runningCheck VLAN20 routing to pfSense

7 RAPID RESET SEQUENCE

1. Reboot **iPhone hotspot** → wait for WAN IP.
2. Reboot **pfSense VM**.
3. Verify **WAN + LAN IPs**.
4. Reboot **PoE switch** → reset WAPs.
5. Reconnect **clients** → verify VLAN IPs & internet.

6. Start **Docker / Home Assistant** services.

8 QUICK FIELD TIPS

- Keep **colored patch cables**: Red=WAN, Blue=Server, Yellow=IoT, Green=Guest
- Maintain spare **USB Wi-Fi adapter & fuses** in case of failure
- Always **check voltmeter** before deploying >3 hours
- Label ports and VLANs inside Pelican lid for instant reference
- Backup pfSense config on USB/Cloud → fast restore

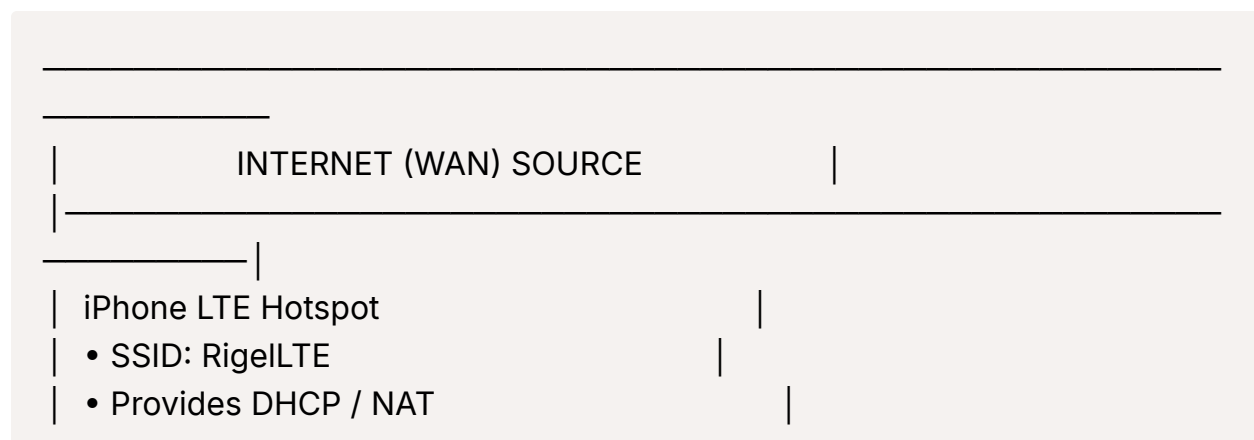
This card is **ready to print and laminate**, small enough to fit inside your Pelican case lid for **instant troubleshooting under pressure**.

If you want, I can also make a **“emergency network workflow diagram”** — a single-page text schematic showing **WAN → pfSense → VLANs → clients → WAPs** for visual reference in the field.

Do you want me to do that next?

Perfect — here’s a **Field Emergency Network Workflow Diagram (Text-Based)** for your Pelican-case portable pfSense LAN. It’s a **single-page schematic** you can print or keep laminated for visual guidance in the field.

EMERGENCY NETWORK WORKFLOW — TEXT SCHEMATIC



| Wi-Fi WAN connection



| PRIMARY LAPTOP — Latitude E4310 (Host with Hyper-V) |

| Virtual Machines: |

| |— pfSense VM (Router / Firewall) |

| |— Ubuntu VM (Docker Lab) |

| |— Home Assistant VM |

| WAN → Wi-Fi adapter → iPhone LTE |

| LAN → vSwitch → PoE Switch trunk (VLANs 10/20/30/40) |

| Trunked Ethernet (LAN)



| 8-Port PoE Switch (Managed) |

| Ports: |

| 1 → Trunk to pfSense LAN (VLAN 10/20/30/40) |

| 2 → Access VLAN20 (Ubuntu / Docker host) |

| 3 → Trunk VLANs 20/30/40 → Cisco WAP #1 |

| 4 → Trunk VLANs 20/30/40 → Cisco WAP #2 |

| 5-8 → Optional VLAN access / client connections |

| VLAN Distribution



| CISCO WAPs (PoE) |

| SSID Mapping: |

| ServerNet → VLAN20 (Admin / Server Access) |

| IoTNet → VLAN30 (IoT Devices) |

| GuestNet → VLAN40 (Guest Internet Only) |

| DHCP served by pfSense per VLAN |

| Wireless / LAN Access



| CLIENTS / DEVICES |

| VLAN10 MGMT → Admin laptop |

| VLAN20 SERVER → Secondary laptop / Docker / Home Assistant |

| VLAN30 IOT → Smart sensors, cameras, plugs |

| VLAN40 GUEST → Guest devices / phones |

| Internet access only per firewall rules |

| FIELD POWER DISTRIBUTION

| Battery / UPS → DC Bus |

| └─ 19V → Laptop 1 & Laptop 2 |

| └─ 48V → PoE Switch → WAPs |

| └─ USB-C PD → iPhone / Accessories |

| RAPID TROUBLESHOOT / RESET FLOW

[No Internet] → Check WAN IP → Reconnect Hotspot → Reboot pfSense WAN
[No LAN IP] → Check DHCP → Check VLAN assignments → Reboot client
[VLAN Issue] → Firewall rules → Switch trunk/tag → Reboot WAPs
[Wi-Fi Issue] → AP power → VLAN mapping → Restart AP
[Docker / HA offline] → Start VM → Confirm VLAN / LAN IP → Resume service
s

✓ FIELD NOTES:

- VLAN color codes: Red=WAN, Blue=Server, Yellow=IoT, Green=Guest, White=Mgmt
- All devices connect **through pfSense LAN trunk → switch → WAPs or LAN ports**
- DHCP & firewall rules **centralized in pfSense** → simplifies client troubleshooting
- Battery and UPS → continuous operation if mains fail

This schematic gives a **complete visual workflow**: from **internet source** → **pfSense** → **VLANs** → **clients** → **wireless / wired access** → **power flow** → **troubleshooting** — all in one page.

If you want, I can **combine the 5-minute deployment, troubleshooting card, and workflow diagram into a single “Pelican Case Field Guide”** — fully consolidated for rapid field operations.

Do you want me to do that?