MODERN & PROFESSIONAL EDITION

HOW TO BUILD A HOME COMPUTER NETWORK

A PRACTICAL GUIDE TO PLANNING, SETTING UP AND SECURING YOUR HOME NETWORK

RELIABLE
SECURE
MODERN
STEP BY STEP
FOR EVERY HOME

VLAN · WI-FI · FIREWALL · NAS · SMART HOME

A practical illustrated networking guide

∿ by **NumQuora** · numquora.com

Contents

How to Build a Home Computer Network – an illustrated practical guide to VLANs, Wi-Fi, firewall, NAS and smart home. Chapters follow the order of the build in three phases. Click a chapter to jump to it; official tutorials are linked at the end of each chapter. Published by **NumQuora** – free online calculators and converters at numquora.com.

QS	**QuickStep** – the whole build on one page	03

PHASE 1 · BUILD

01	Network fundamentals	04
02	Reference architecture at a glance	05
03	Planning and site survey	06
04	The build order	07
05	Choosing equipment	08
06	Cabling, termination and testing	09
07	Sizing PoE and UPS	11

PHASE 2 · CONFIGURE

08	Initial setup of the gateway and controller	12
09	IP addressing, DNS and DHCP	13
10	VLAN segmentation	14
11	Trunks, access ports and port profiles	15
12	Moving to VLANs without locking yourself out	16
13	Wi-Fi engineering and channel planning	17

PHASE 3 · SECURE & RUN

14	Firewall, security and how to prove it	18
15	Secure remote access with a VPN	20
16	NAS – network storage	21
17	Backups and a real restore test	22
18	Smart home hub and IoT	23
19	Troubleshooting and rollout	24
20	Updates and change management	25

PRACTICAL APPENDICES

A	Example IP and VLAN plan	26
B	Controller configuration walkthrough	26
C	Firewall policy matrix	27
D	NAS checklist	27
E	Smart home integration pattern	28
F	Troubleshooting commands	28
G	Deployment acceptance sheet	29

QUICKSTEP

Home Network Field Guide · by NumQuora

Home network in 9 steps.

Gateway · VLANs · Wi-Fi · firewall · NAS · smart home · VPN

9	3	4
steps	phases	VLANs

TARGET NETWORK

Internet → ONT → Gateway → Switch → Access points, PC / TV, Cameras · IoT, Guests, NAS, Smart home

- VLAN 10 Trusted 192.168.10.0/24
- VLAN 20 IoT 192.168.20.0/24
- VLAN 30 Guest 192.168.30.0/24
- VLAN 40 Servers 192.168.40.0/24

PHASE 1 BUILD

01 Plan

ch. 3–4

- Floor plan: APs, outlets, cabinet
- Count ports, add 20–30 % spare
- IP + VLAN plan before buying

+30 % ports · 1 cabinet

✓ Done when every outlet has a number + VLAN

02 Cable & rack

ch. 6–7

- Cat6 home runs to a patch panel
- T568B both ends, untwist ≤ 13 mm
- Test and label every run
- UPS ≥ 300 W on the core

≤ 90 m · T568B

✓ Done when all runs pass the tester

03 Gateway

ch. 8

- ONT → gateway WAN port
- Stable firmware update
- Strong password + MFA
- Export the first backup

MFA · backup

✓ Done when internet works on a LAN laptop

PHASE 2 CONFIGURE

04 Switch & APs

ch. 5, 8

- Adopt switch first, then APs
- Rename devices by location
- PoE budget + 30 % reserve
- Same firmware everywhere

PoE +30 %

✓ Done when all devices online

05 VLANs & DHCP

ch. 9–12

- Networks 10 / 20 / 30 / 40
- Pool .100–.249, gateway .1
- NAS .10, smart home hub .30
- Uplinks trunk, devices access

4 VLANs · .1 / .100+

✓ Done when test client gets the right subnet

06 Wi-Fi

ch. 13

- SSIDs: Home 10 · IoT 20 · Guest 30
- 2.4 GHz: 20 MHz, ch 1 / 6 / 11
- 5 GHz: 40–80 MHz, unique per AP
- Medium power, not maximum

−67 dBm · 1 / 6 / 11

✓ Done when walk test passes in every room

PHASE 3 SECURE & RUN

07 Firewall

ch. 14

- Default: block between zones
- Trusted → Servers: 443, 445, 8123
- Smart home hub→ IoT: needed ports
- IoT / Guest: no admin; check IPv6

default block

✓ Done when isolation tests pass per VLAN

08 NAS, hub & VPN

ch. 15–18

- NAS: HTTPS, MFA, least rights
- Smart home hub on a mini-PC
- WireGuard VPN, no port forwards
- Check CGNAT before relying on VPN

UDP 51820

✓ Done when VPN works from mobile data

09 Backup & docs

ch. 17, 20

- 3-2-1: NAS + USB + off-site
- Restore one file + one hub backup
- Export configs, save the diagram
- Sign the acceptance sheet

3-2-1 · restore test

✓ Done when sheet signed, copies offline

TROUBLESHOOT BOTTOM-UP

the first "no" tells you where to look

Link → IP address → Gateway → Internet → DNS → App

- ✓ **Backup first** before every change
- ✓ **One change** at a time, then test
- ✓ **Wired admin path** that you don't touch
- ✓ **No port forwards** to admin pages – VPN

PHASE 1 · BUILD

01 Network fundamentals

From internet service to reliable local connectivity

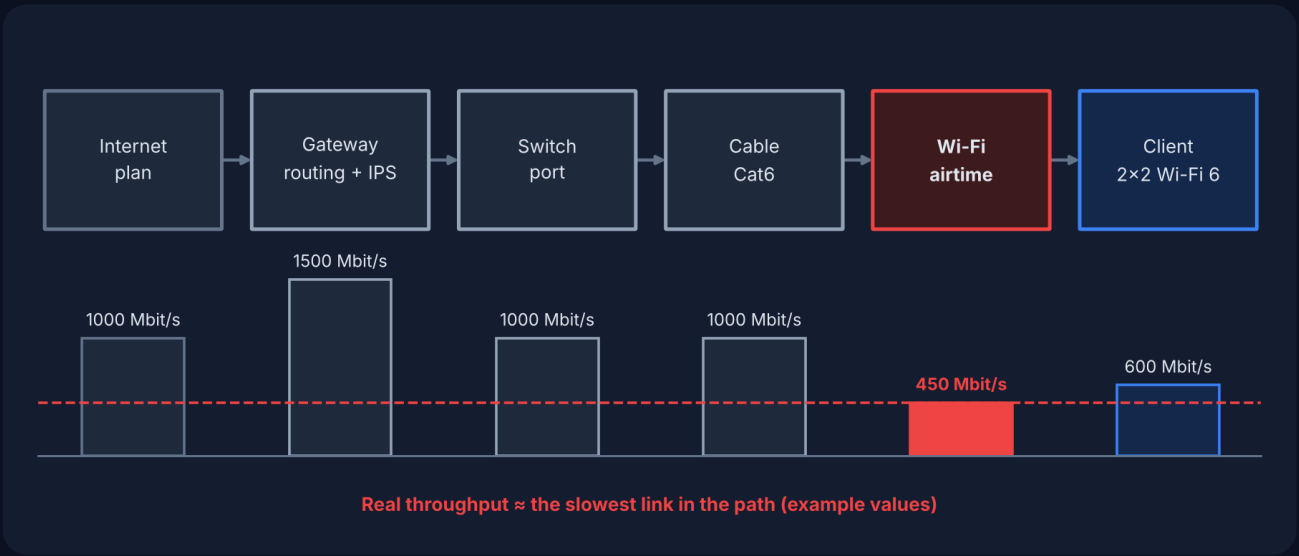


Figure 1.1 The whole path counts: real throughput is set by the slowest link, here the Wi-Fi airtime.

How traffic moves

An internet service terminates at an ONT or modem. The gateway routes between the local network and the internet, applies NAT and firewall policies, and usually provides DHCP. A switch expands wired ports; access points bridge wireless clients onto selected LANs.

Build a simple topology

Connect the ONT to the gateway WAN port, the gateway LAN to a managed switch, and access points and wired clients to switch ports. Avoid chaining multiple consumer routers in routing mode; it creates double NAT and complicates discovery and port forwarding.

What to measure

Document service speed, wall construction, floor count, number of wired devices, PoE requirements, outdoor coverage and the location of network cabinets. Design for concurrent demand rather than advertised peak Wi-Fi rates.

Understand the bottlenecks

A 2.5 GbE gateway port does not make a 1 GbE switch or client faster. Throughput is limited by the slowest relevant link, radio airtime, interference, cabling quality, routing capacity (especially with IPS/IDS enabled) and the remote service.

Acceptance test

Confirm each client gets the correct address and DNS, reaches its permitted services, and cannot reach blocked networks. Save a topology diagram and a baseline speed/latency test for future comparisons.

Further reading

↗ Networking fundamentals – what is a LAN (Cloudflare)

PHASE 1 · BUILD

02 Reference architecture at a glance

One picture of everything in this guide

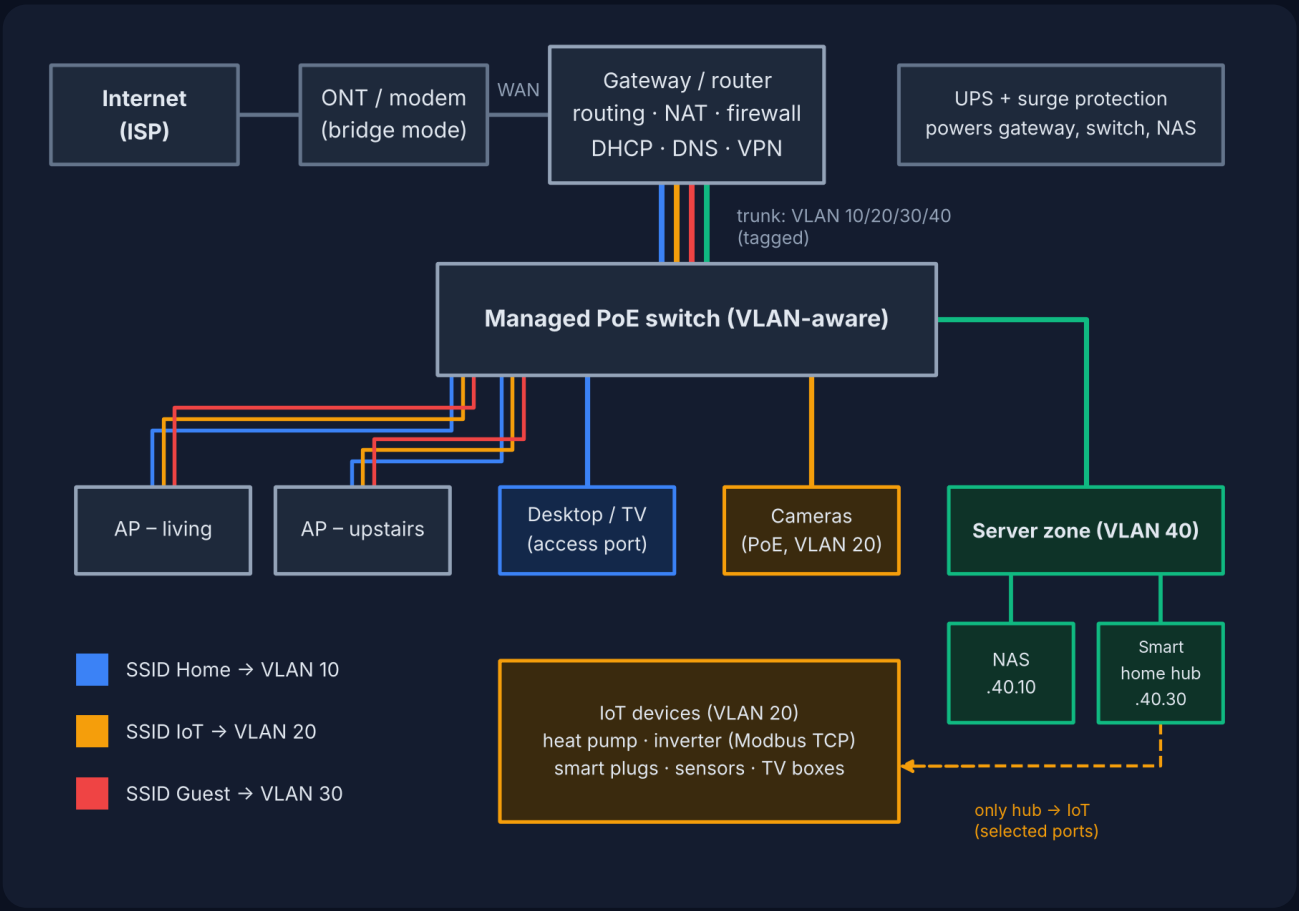


Figure 2.1 Reference home network: colours mark VLANs, multi-colour lines are tagged trunks.

How to read the diagram

The gateway is the only device that routes between VLANs, so every firewall rule lives there. The switch and the access points only *carry* VLANs: uplinks are trunks (several colours on one cable), while end devices sit on access ports with one colour. The server zone holds the NAS and the smart home hub, and the hub is the only system allowed to open connections into the IoT VLAN.

Use it as your template

01 Redraw the diagram for your house: real room names, real device counts, real port numbers.

02 Mark which devices need PoE and which outlets are on which switch port – this becomes your port schedule.

03 Write the VLAN colour next to every outlet on the floor plan. Colours are easier to follow than numbers.

04 Store the drawing with the configuration backups and update it after every change (chapter 20).

PHASE 1 · BUILD

03 Planning and site survey

Design coverage, capacity and resilience before buying

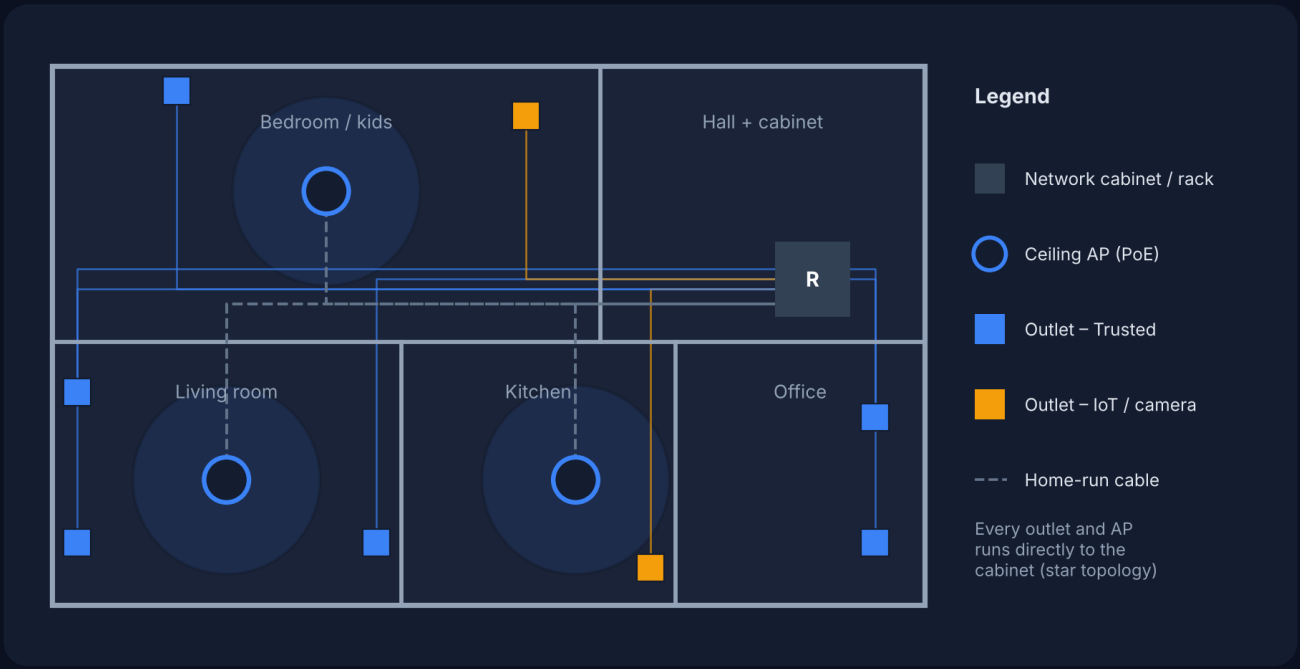


Figure 3.1 Example floor plan: ceiling APs near where people use devices, every outlet home-run to one cabinet.

Survey the property

Mark rooms, floor slabs, reinforced walls, wiring routes and network outlets on a floor plan. Place access points near the areas of use rather than inside metal cabinets. Test real signal and roaming after installation.

Estimate port count

Count desktops, TVs, NAS, smart home hub, cameras, access points, controllers and spare outlets. Add 20–30 percent spare ports and verify the switch PoE power budget as well as port-level PoE capabilities.

Plan structured cabling

Use home-run Cat6 or Cat6A cable from each outlet to a patch panel. Separate low-voltage data runs from mains according to local rules; preserve bend radius and avoid untwisting pairs excessively at terminations.

Power and cooling

Use a ventilated location with stable power and an appropriately sized UPS for gateway, switch, NAS and server. Estimate actual watts and runtime (chapter 7); label both ends of each cable and maintain a port inventory.

Design deliverables

Produce a floor plan, rack layout, port schedule, IP plan, VLAN list, Wi-Fi SSID plan, firewall matrix and rollback procedure. Keep a copy available offline in case the network becomes inaccessible.

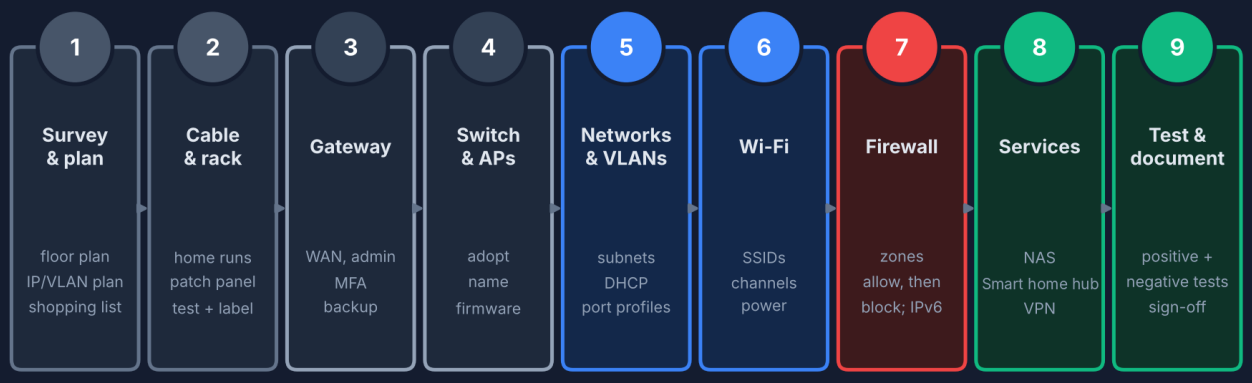
Further reading

↗ Example (UniFi): getting started

PHASE 1 · BUILD

04 The build order

Nine phases, each finished before the next starts



Checkpoint after every phase: export a backup · test · write down what changed

Figure 4.1 Recommended sequence. Most outages in new networks come from doing phases 5–7 at the same time.

PHASE	KEY WORK	DONE WHEN...
1 Survey & plan	Floor plan, AP positions, IP/VLAN plan (App. A), bill of materials	Every outlet has a port number and a VLAN
2 Cable & rack	Home runs to patch panel, keystones, labels, UPS (ch. 6–7)	Every run passes the tester; labels match the schedule
3 Gateway	WAN as ISP specifies, strong admin password, MFA, first backup (ch. 8)	Internet works from a laptop on the LAN port
4 Switch & APs	Adopt, rename by location, update firmware	All devices adopted, online, same stable firmware
5 Networks & VLANs	Networks, DHCP pools, port profiles (ch. 9–12)	Test client gets an address in each VLAN
6 Wi-Fi	SSIDs mapped to VLANs, channels, power (ch. 13)	Walk test: signal ≥ −67 dBm in rooms that matter
7 Firewall	Zones and policies from the matrix (ch. 14), IPv6	All isolation tests give the expected result
8 Services	NAS, smart home, VPN, backups (ch. 15–18)	Remote VPN works; a restore has been tested
9 Test & document	Appendix G sheet, diagrams, exports	Sheet signed; copies stored offline

TIP Do the work in a planned window when nobody needs the internet – phases 3–7 interrupt connectivity.

PHASE 1 · BUILD

05 Choosing equipment

Routers, switches, access points and uplinks

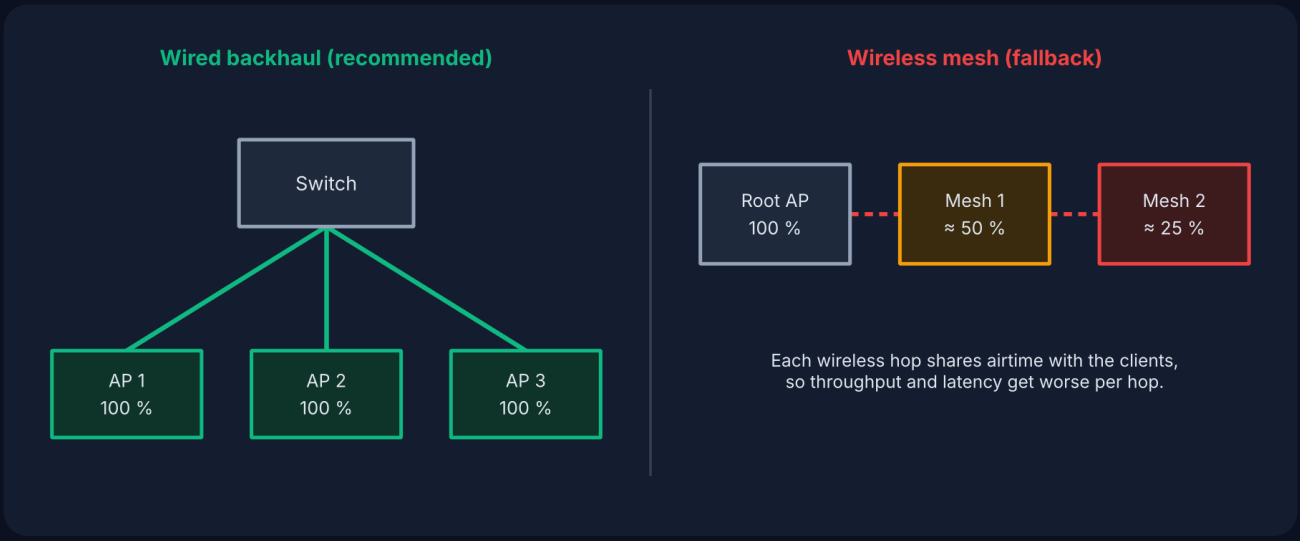


Figure 5.1 Several wired APs keep full speed; every wireless mesh hop costs airtime and latency.

Gateway selection

Select a gateway with sufficient WAN throughput under the security features you intend to enable. Check controller support, VLAN routing, VPN options, 2.5/10 GbE needs and firmware lifecycle.

Managed switches

For segmentation, choose a VLAN-aware managed switch. Check PoE standards, total power budget, fan noise, uplink capacity and the number of ports required by wired endpoints.

Access points

Choose Wi-Fi 6/6E/7 equipment for actual client compatibility and spectrum conditions. Multiple properly placed wired APs usually outperform one high-power router. Wireless mesh is a fallback when Ethernet is impossible.

Optical handoff

Confirm whether the provider supplies a separate ONT or an integrated optical router. Bridge or passthrough availability is provider-specific; double NAT may be acceptable but should be understood.

Procurement checklist

Verify rack space, mounting brackets, PoE injectors if needed, patch cords, keystones, patch panel, UPS, surge protection and spare ports. Check regional radio regulations and compatible power adapters.

Further reading

↗ Example (UniFi): PoE availability and modes

PHASE 1 · BUILD

06 Cabling, termination and testing

Reliable physical links are the foundation

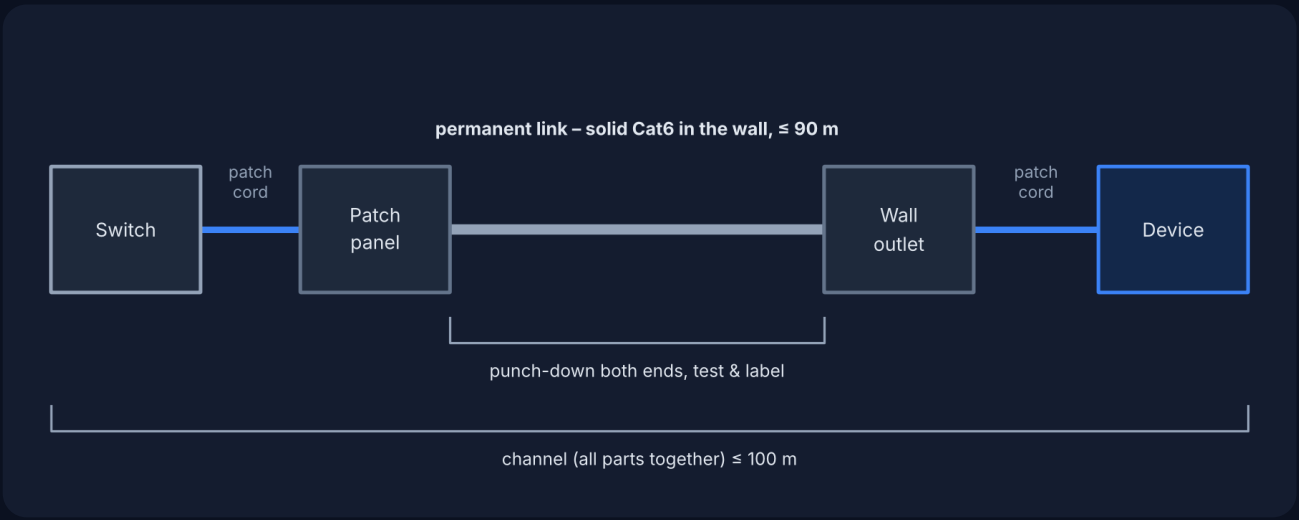


Figure 6.1 Structured cabling: a fixed permanent link in the wall, short patch cords at both ends.

Cable choice

Solid copper Cat6 is a practical default for fixed residential runs; Cat6A may help where 10 GbE or interference conditions justify it. Avoid copper-clad aluminium (CCA) and damaged cable.

Termination

Terminate permanent cable into rated keystone jacks and a patch panel. Keep pair twists close to the contact and use the same T568A or T568B scheme at both ends of a link.

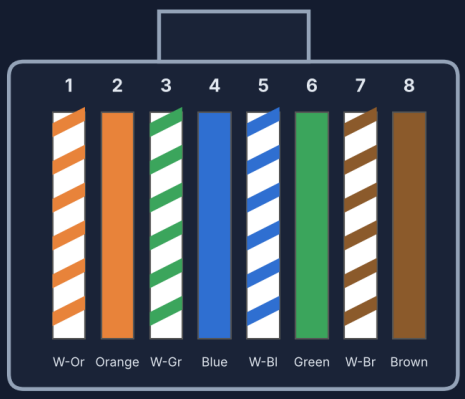
PoE and grounding

Confirm PoE class and switch budget before powering APs or cameras. Shielding and earthing require a consistent design; follow local electrical and lightning-protection requirements.

Rack finishing

Separate power from data, use short labelled patch leads and leave service loops. Photograph final patching and update the port schedule after every change.

Terminating a cable run



T568B – clip down, contacts facing you

Pair map

Pins 1-2	orange pair	data pair A
Pins 3-6	green pair (split!)	data pair B
Pins 4-5	blue pair	data / PoE
Pins 7-8	brown pair	data / PoE

Same standard (A or B) at both ends. Untwist ≤ 13 mm.

Figure 6.2 T568B colour order (common in Europe). T568A swaps the orange and green pairs.

Procedure – keystone and patch panel

01 Leave a 30 cm service loop at both ends, then strip about 40 mm of jacket without nicking the conductors.

02 Remove the separator, fan the pairs out and keep each pair twisted as close to the contact as possible (untwist at most 13 mm).

03 Lay the wires into the keystone/patch panel following the printed B-colour code; punch down with an impact tool and trim the ends.

04 Fit the cap or strain relief so the jacket, not the conductors, takes the pull.

05 Test with a wiremap tester: all 8 wires in order, no open, short, reversed or split pair. Certification testers additionally measure demanding electrical parameters.

06 Connect the run to the switch and check that it negotiates the expected speed (1 or 2.5 Gbit/s) with zero errors after a large file copy.

07 Label both ends with the same ID (e.g. *2F-BED1-A*) and enter it in the port schedule.

CAUTION A cable that passes a cheap tester can still fail at speed – a **split pair** (wrong pairs on 3-6) shows as a link at 100 Mbit/s or many errors. Re-terminate rather than live with it.

Further reading

↗ Ethernet cable categories (Fluke Networks)

PHASE 1 · BUILD

07 Sizing PoE and UPS

Add up the watts before you buy

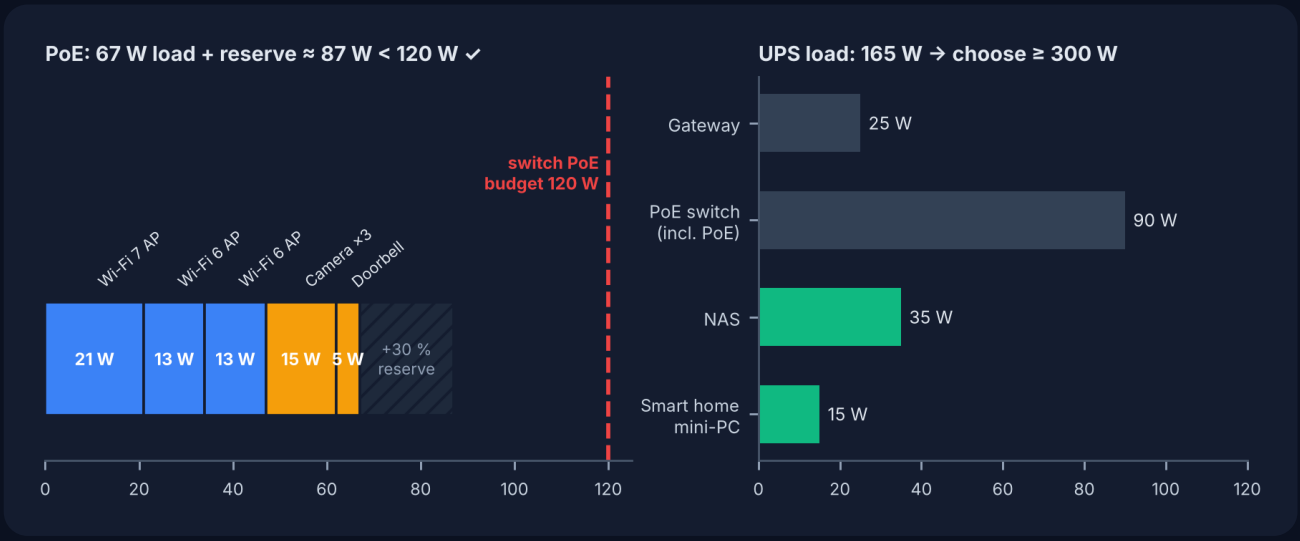


Figure 7.1 Example PoE and UPS budgets. Use the maximum power from each datasheet, not the typical value.

PoE budget

01 List every PoE device and its maximum consumption from the datasheet (example: 21 + 13 + 13 + 15 + 5 = 67 W).

02 Check each device's PoE class against the port: 802.3af (PoE) ≤ 15.4 W, 802.3at (PoE+) ≤ 30 W, 802.3bt (PoE++) 60–90 W per port.

03 Add 30 % reserve for future devices and cold starts: 67 W × 1.3 ≈ 87 W.

04 Choose a switch whose **total** PoE budget is higher (here a 120 W switch is enough; a 60 W model is not).

UPS sizing and safe shutdown

01 Add the steady load of everything on the UPS: gateway 25 W + switch incl. PoE 90 W + NAS 35 W + Home Assistant mini-PC 15 W = 165 W.

02 Pick a UPS with 50–70 % headroom in **watts** (not VA): ≥ 300 W. Check its runtime chart at 165 W – aim for ≥ 10–15 minutes.

03 Connect the UPS USB cable to the NAS and enable its **network UPS server** function (most NAS systems offer this as NUT / "UPS server" in the power settings).

04 Configure other servers and PCs on the UPS as NUT clients of the NAS so they shut down when the battery is low.

05 Shutdown order: smart home hub → NAS. Gateway and switch run until the battery is empty so shutdown messages can travel.

06 Test once a year: unplug the UPS from mains and watch the shutdown happen in the correct order.

Further reading

↗ Example (UniFi): PoE availability and modes

PHASE 2 · CONFIGURE

08 Initial setup of the gateway and controller

From adoption to stable routing and switching

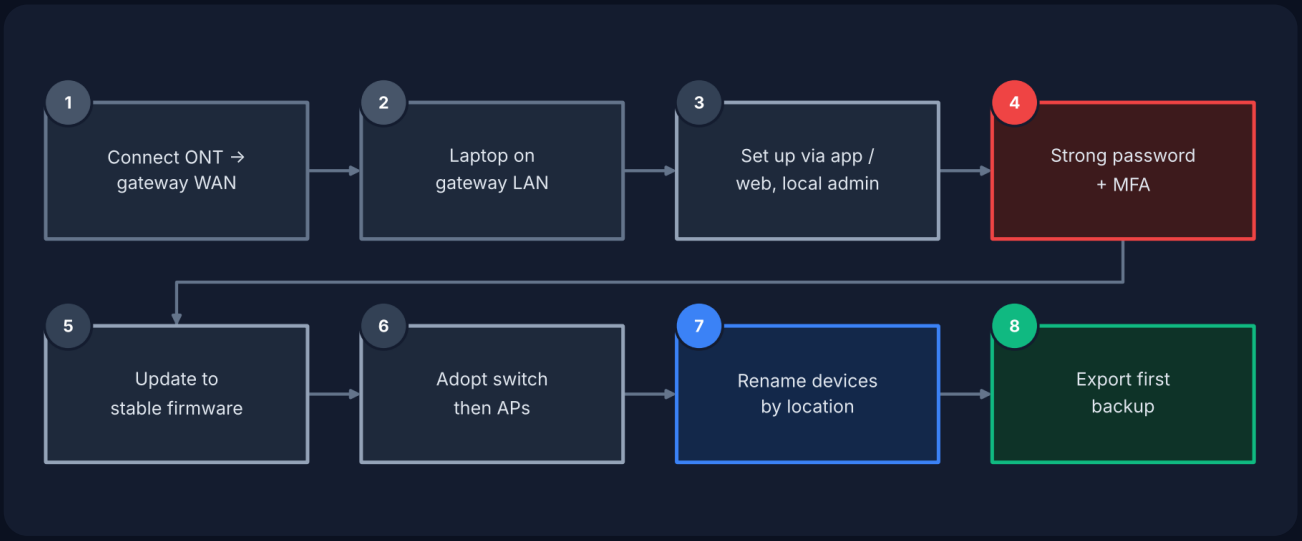


Figure 8.1 First-day setup sequence for the gateway and adopted devices.

Initial adoption

Connect the gateway and network controller, update to a tested stable firmware, adopt switches and APs, and assign descriptive device names. Change administrative credentials and enable MFA where available.

WAN and LAN

Set WAN addressing as specified by the ISP. Create a trusted LAN, verify the DHCP scope, configure DNS resolvers and check that clients receive the gateway as their default route.

Switch port profiles

Configure uplinks as trunks carrying only required VLANs; endpoint ports are access/untagged on one network. AP uplinks usually need management plus SSID VLANs. The detailed procedure is in chapter 11.

Configuration backups

Export a controller backup after initial adoption and after major changes. Record the gateway model, controller version and any deviations from default behaviour.

Verification

Test internet, DNS, IPv4/IPv6 as deployed, wired negotiation and AP adoption. Avoid changing WAN, VLANs and firewall policies simultaneously without a rollback path.

Further reading

↗ Example (UniFi): WAN and LAN port configuration
↗ Example (UniFi): creating VLANs

PHASE 2 · CONFIGURE

09 IP addressing, DNS and DHCP

Predictable names and addresses reduce failures

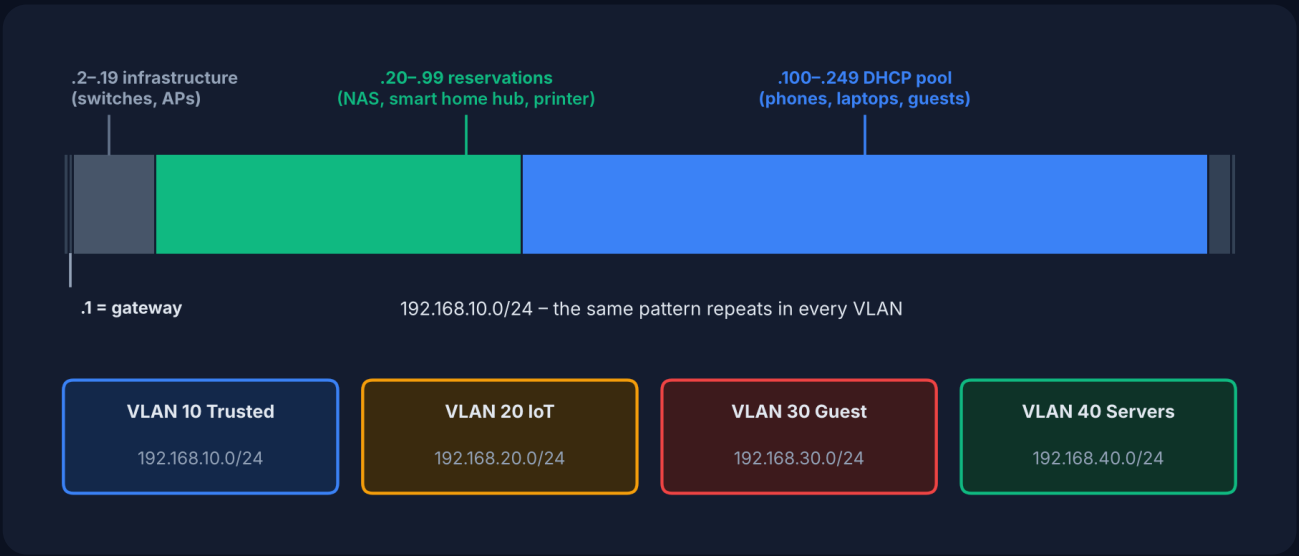


Figure 9.1 One address layout reused in every VLAN: gateway, infrastructure, reservations, then the DHCP pool.

Addressing example

Use 192.168.10.0/24 for trusted clients, 192.168.20.0/24 for IoT and 192.168.30.0/24 for guests. Assign gateway .1, reserve a documented static/reservation range and keep DHCP pools separate.

DHCP reservations

Reserve addresses for NAS, smart home hub, printers and infrastructure using stable device identifiers (MAC). Avoid manually assigning an address inside an active DHCP pool.

DNS design

Choose trusted upstream resolvers and decide whether local hostnames are served by the gateway or another DNS server. Ensure all VLANs can reach approved DNS while preventing bypass if policy requires it.

IPv6 considerations

Do not assume IPv4 firewall rules protect IPv6. If IPv6 is enabled, verify prefix delegation, router advertisements, DNS, guest isolation and equivalent firewall behaviour.

Diagnostic sequence

Check link, address, gateway, DNS resolution and then application connectivity. A successful ping to an IP with a failed name lookup points toward DNS rather than the physical link.

Further reading

↗ IP addressing and DHCP overview (Microsoft)

PHASE 2 · CONFIGURE

10 VLAN segmentation

Separate trust zones without breaking required services

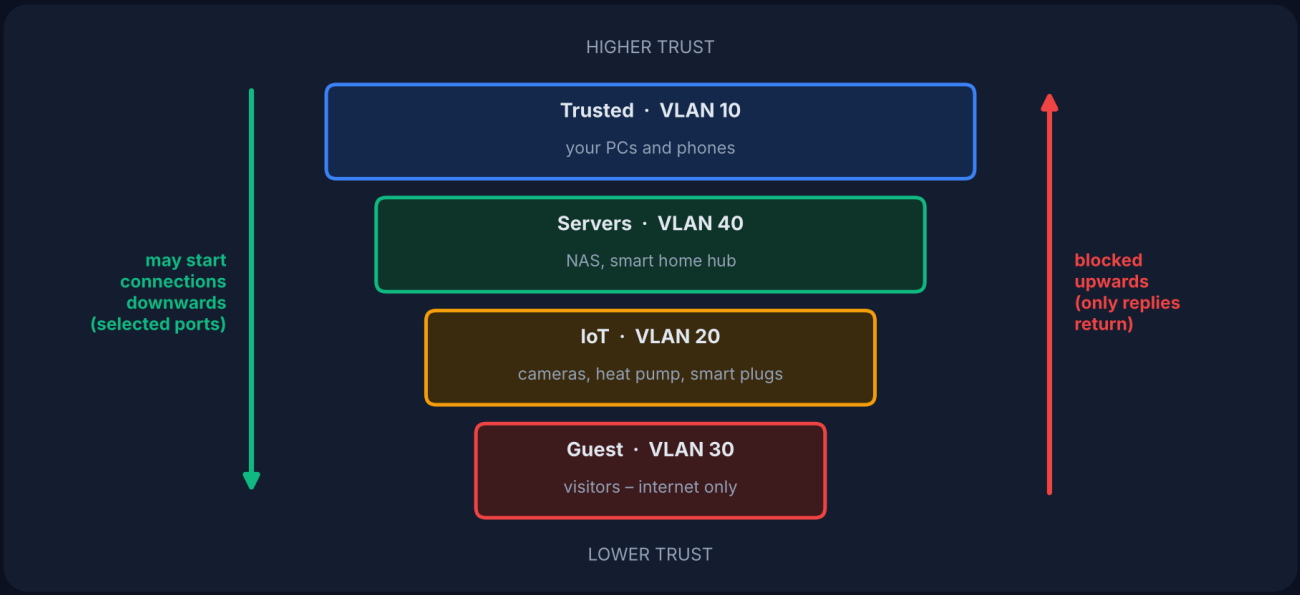


Figure 10.1 Trust zones: higher zones may open selected connections to lower ones, never the other way round.

Segmentation plan

Use VLAN 10 Trusted, VLAN 20 IoT, VLAN 30 Guest and optionally VLAN 40 Servers. Subnets and VLAN IDs are examples; choose values that do not conflict with VPN or upstream networks.

Tagged vs untagged

An access port places untagged client traffic into one VLAN. A trunk carries tagged VLANs to switches and APs. Native/management VLAN choices must match at both ends.

Service exceptions

Allow IoT to reach only necessary DNS, NTP and selected automation endpoints. Some discovery protocols use multicast and may require an mDNS reflector or targeted routing.

Firewall approach

Start with deny inter-VLAN access and add explicit rules for established traffic and approved services. Confirm direction, rule ordering and whether a platform treats local gateway traffic separately.

Prove isolation

From guest and IoT clients, attempt connections to NAS management, smart home hub admin and trusted workstations. Verify approved smart-home control still works and log unexpected drops.

Further reading

- ↗ Example (UniFi): creating VLANs
- ↗ Example (UniFi): network and client isolation

11 Trunks, access ports and port profiles

Getting tagged and untagged right the first time

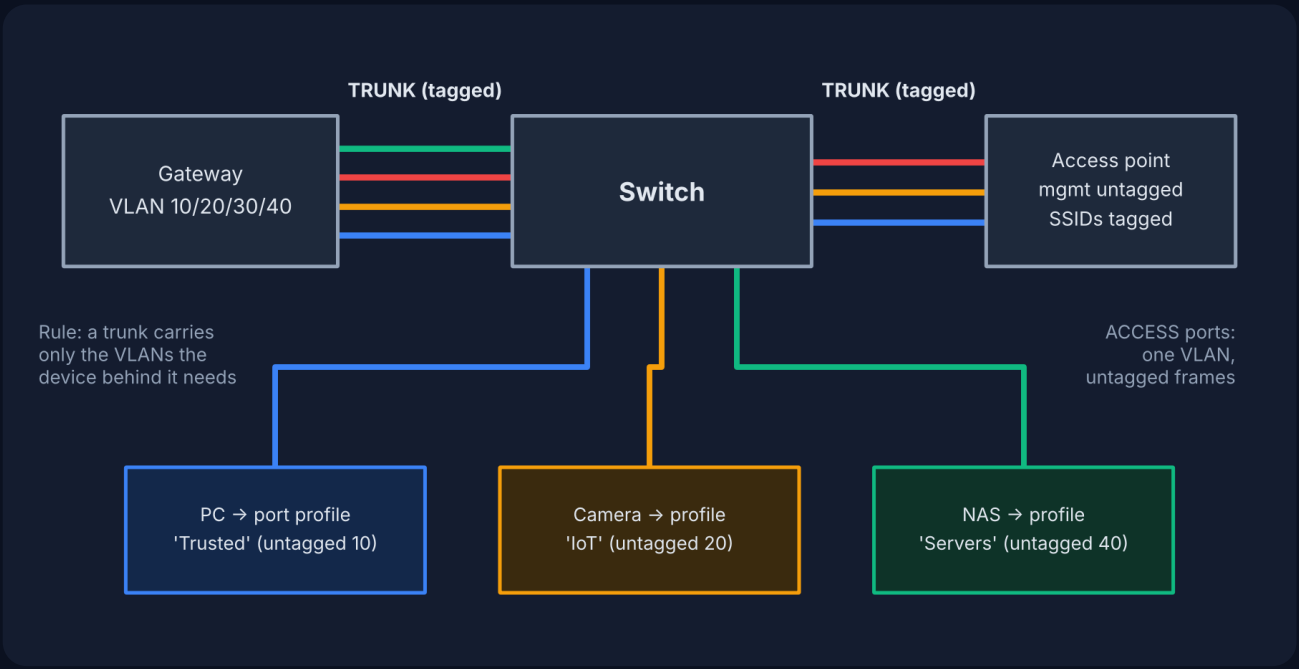


Figure 11.1 Trunks carry several tagged VLANs; access ports deliver exactly one VLAN, untagged.

Procedure – configure switch ports

01 List every switch port in a table: port number, connected device, required VLAN, PoE yes/no.

02 Uplink to the gateway: native/untagged = management (default) network; tagged = all VLANs used anywhere downstream.

03 Access-point ports: native = management network; tagged = only the VLANs used by its SSIDs (10, 20, 30). Not 40 – no SSID uses it.

04 End-device ports: set the native network to the device's VLAN and **block all tagged VLANs**. In the UI: device → Ports → select port → Native VLAN / Network, Tagged VLAN Management = Block All.

05 Server ports (NAS, smart home hub): access port with native = Servers (VLAN 40) and no tagged VLANs.

06 Disable unused ports or put them in an empty “parking” VLAN so a visitor plugging in a cable gets nothing.

07 Plug a laptop into each port in turn and confirm it gets an address from the expected subnet.

CAUTION Switches and APs must have the management network as **native** on their uplink. A wrong native VLAN is the classic reason an AP or switch disappears after a change.

PHASE 2 · CONFIGURE

12 Moving to VLANs without locking yourself out

A safe order for converting a flat network

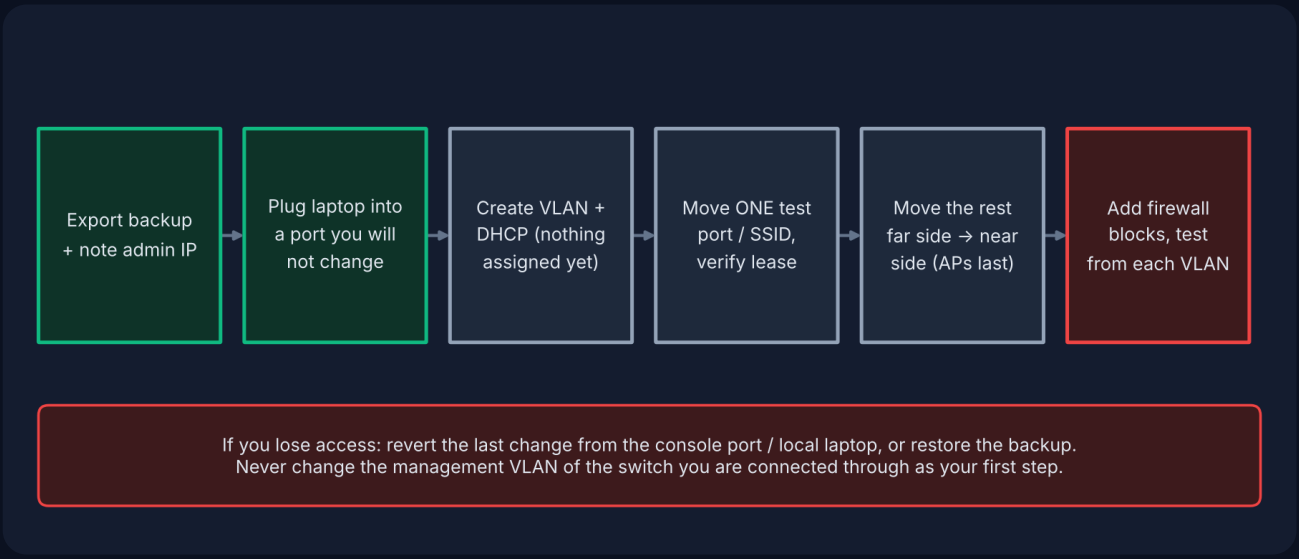


Figure 12.1 Work from the edge towards your own connection, and keep one known-good path open.

Procedure

01 Export a controller backup and write down the current admin IP and the management network subnet.

02 Connect your laptop by cable to a port you will **not** touch during the change. Wi-Fi is not a safe admin path – SSIDs will move.

03 Create the new networks (Trusted 10, IoT 20, Guest 30, Servers 40) with DHCP enabled. Creating a VLAN changes nothing yet, because no port or SSID uses it.

04 Move a single test port or a temporary test SSID into the new VLAN. Check address, gateway, DNS and internet from a test device.

05 Move ports from the far end of the network inwards: end devices first, then AP SSIDs, uplinks of downstream switches last.

06 Give the NAS and smart home hub their new reserved addresses (Appendix A) and update bookmarks, SMB drive mappings and hub integrations that used the old IPs.

07 Only now add the blocking firewall policies (chapter 14), then run the isolation tests.

08 Export a new backup and update the port schedule.

CAUTION If the controller becomes unreachable, connect directly to the gateway LAN port, which normally stays on the default network, and undo the last step. As a last resort, restore the backup from step 1.

PHASE 2 · CONFIGURE

13 Wi-Fi engineering and channel planning

Coverage, channels, roaming and SSIDs

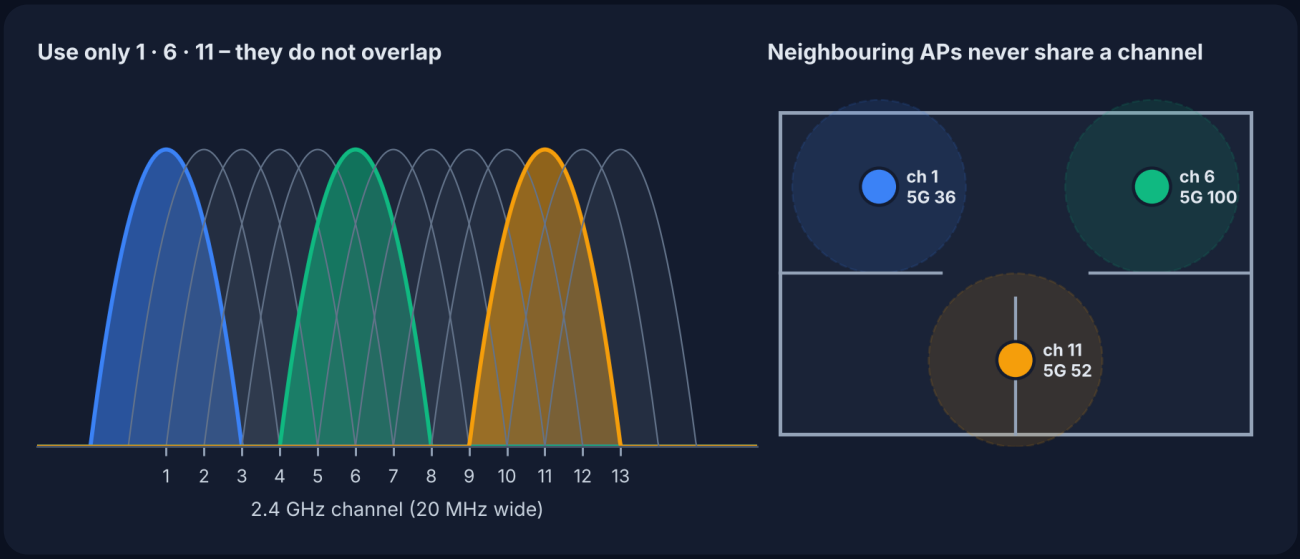


Figure 13.1 Only channels 1, 6 and 11 avoid overlap at 2.4 GHz; neighbouring APs get different channels on both bands.

SSID design

Use a small number of SSIDs: trusted, IoT and guest where needed, each mapped to its intended network. Excessive SSIDs consume airtime and complicate troubleshooting.

Security modes

Use WPA2-AES or WPA3 as client support permits, with strong unique passphrases. A separate IoT SSID can preserve compatibility without weakening the trusted SSID.

Roaming

A client chooses when to roam. Improve cell overlap and AP placement before tuning roaming-assistance features; validate older IoT clients before enabling aggressive options.

Procedure – channels and power

01 Scan the air first (any Wi-Fi analyser app, e.g. WiFiman or NetSpot). Note which channels the neighbours use and how strong they are.

02 2.4 GHz: 20 MHz width, channels 1/6/11 only, transmit power Low or Medium. This band is for range and IoT, not for speed.

03 5 GHz: 40 MHz in dense surroundings, 80 MHz in a detached house. Give neighbouring APs different channels. DFS channels (52–144) are often quiet but may move briefly when radar is detected.

04 6 GHz (Wi-Fi 6E/7): only for clients that support it; 160 MHz works well in a single room but walls absorb this band quickly.

05 Set power so a client sees about −67 dBm or better where it is used and the next AP becomes stronger where you want it to roam. Max power everywhere makes clients cling to distant APs.

06 Measure signal, noise, retransmissions and real throughput near and far from APs; then walk the house on a video call. Fix AP position before advanced settings.

07 Record the final channel/power per AP in the documentation.

BAND	WIDTH	TYPICAL USE	WATCH OUT FOR
2.4 GHz	20 MHz	IoT, long range, through walls	Neighbours, Bluetooth, microwaves
5 GHz	40 / 80 MHz	Phones, laptops, TVs	DFS radar moves, thick walls
6 GHz	80 / 160 MHz	Newest clients, same room	Short range; client support

Further reading

↗ Example (UniFi): creating Wi-Fi SSIDs

PHASE 3 · SECURE & RUN

14 Firewall, security and how to prove it

Least privilege for everyday home networking

DESTINATION →

SOURCE ↓	Trusted	IoT	Guest	Servers	Gateway (DNS/NTP)	Gateway admin	Internet
Trusted	—	ALLOW	BLOCK	ALLOW HTTPS, SMB	ALLOW	ALLOW	ALLOW
IoT	BLOCK	—	BLOCK	LIMITED MQTT, hub API	ALLOW	BLOCK	LIMITED if needed
Guest	BLOCK	BLOCK	—	BLOCK	ALLOW DNS only	BLOCK	ALLOW
Servers	LIMITED replies only*	LIMITED hub → IoT ports	BLOCK	—	ALLOW	BLOCK	ALLOW
VPN users	ALLOW	BLOCK	BLOCK	LIMITED selected	ALLOW	LIMITED MFA	ALLOW
Internet	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	BLOCK	—

Figure 14.1 Zone matrix (source rows, destination columns). *Servers may answer Trusted, but never start connections to it.

Threat model

Protect administrator accounts, management interfaces, backups and devices that cannot receive frequent updates. Place cameras and IoT devices in lower-trust zones.

Rule order

Firewall processing is order-dependent. Permit established/related flows, explicitly allow required management and service traffic, then block undesired inter-VLAN paths. Verify platform-specific defaults.

Hardening

Disable unused services and UPnP where not required, apply security updates, use separate admin accounts, enable logs and back up configurations. Test restore procedures.

Incident response

If a device is compromised, isolate its switch port or VLAN, rotate affected credentials, inspect logs, update firmware and restore only from trusted backups.

Procedure – zone-based firewall

01 Translate the matrix into zones. In zone-based controllers (e.g. UniFi 9.x) the built-in zones are Internal, External, Gateway, VPN, Hotspot (guest) and DMZ; create custom zones **IoT** and **Servers** and move the networks into them.

02 Set the default action between zones to **Block** wherever the matrix says BLOCK.

03 Add ALLOW policies for the LIMITED cells with exact ports: Trusted → Servers TCP 443 (NAS admin), 445 (SMB), 8123 (hub); hub (192.168.40.30) → IoT on integration ports; IoT → hub TCP 1883 (MQTT) and 8123.

04 Allow return traffic for established connections (stateful) – otherwise allowed sessions break.

05 Let every zone reach the gateway for DNS (53) and DHCP; block the gateway admin page from IoT and Guest.

06 Repeat the same intent for IPv6, or leave IPv6 disabled on IoT and Guest until you can test it.

07 Run the tests below from a device in each VLAN and save the results with the backup.

FROM	TEST COMMAND	EXPECTED
IoT phone/PC	`Test-NetConnection 192.168.40.10 -Port 443`	Fails (NAS admin blocked)
IoT	`nc -vz 192.168.40.30 8123`	Succeeds (hub reachable)
Guest	`ping 192.168.10.1 / nslookup example.com`	Ping fails, DNS works
Guest	`nc -vz 192.168.20.25 80`	Fails (no access to IoT)
Trusted	`Test-NetConnection 192.168.40.10 -Port 445`	Succeeds (NAS file shares)
Outside (mobile data)	`Open https://<your-public-IP>:443`	No answer (nothing exposed)

TIP Test from a device *inside* the source VLAN. Testing from your admin PC only proves what Trusted can do.

Further reading

↗ Example (UniFi): zone-based firewall
↗ Guest WiFi best practices

15 Secure remote access with a VPN

Reach home without opening admin pages to the internet

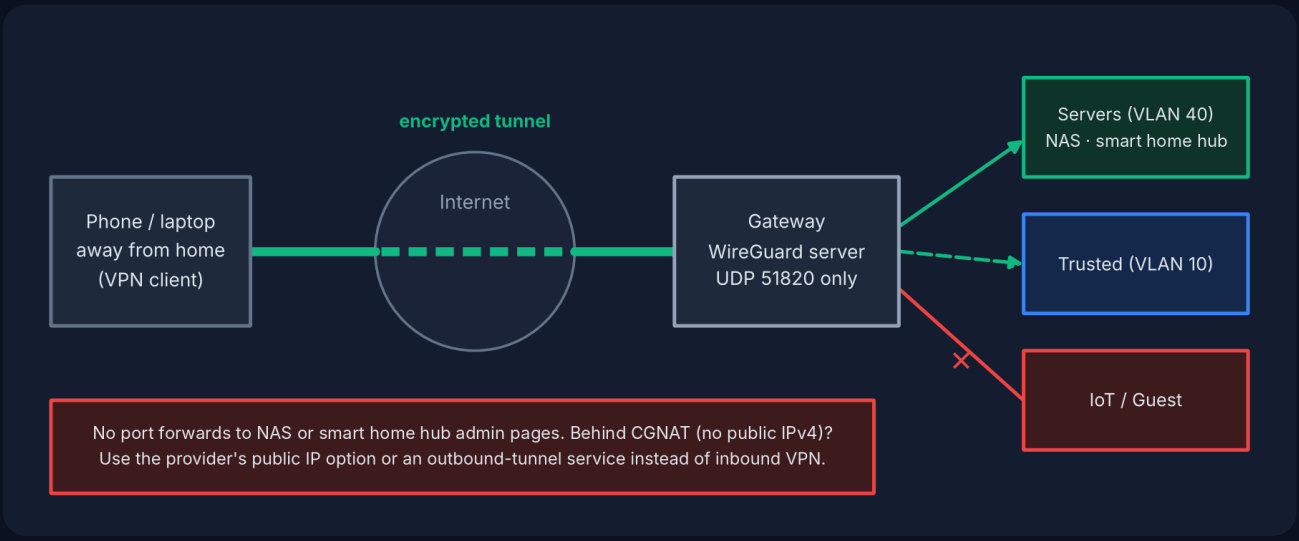


Figure 15.1 One encrypted UDP port instead of many open admin ports. VPN users get only the zones they need.

Why a VPN

Prefer a well-maintained VPN or trusted remote-access solution to exposing NAS or smart home hub admin interfaces directly to the internet. Use MFA and device-level access control.

Procedure – WireGuard on the gateway

01 Check whether you have a public IPv4 address: compare the WAN IP shown on the gateway with the address shown by a “what is my IP” site. If the WAN IP is in 100.64.0.0/10 (CGNAT) or the two differ, inbound VPN will not work – ask the ISP for a public IP or use an outbound-tunnel solution (e.g. UniFi Teleport, Tailscale).

02 Create a WireGuard VPN server on the gateway (e.g. UniFi: Settings → VPN → VPN Server). Use a separate subnet that does not exist at home or at typical hotels, e.g. 192.168.50.0/24.

03 If the public IP changes, set up dynamic DNS so clients connect to a name, not a number.

04 Create one client per device (phone, laptop) – never share a key – and import it by scanning the QR code in the WireGuard app.

05 Put the VPN zone into the firewall matrix: allow Servers and Trusted as needed, block IoT and Guest.

06 Test from mobile data with Wi-Fi switched off: open the NAS and smart home hub by their internal addresses.

07 When a phone is lost, delete only that client's key.

DONE WHEN Remove old port forwards to the NAS admin page and to the smart home hub once the VPN works. UPnP should be off.

16 NAS – network storage

Shared storage for the whole household, kept under control

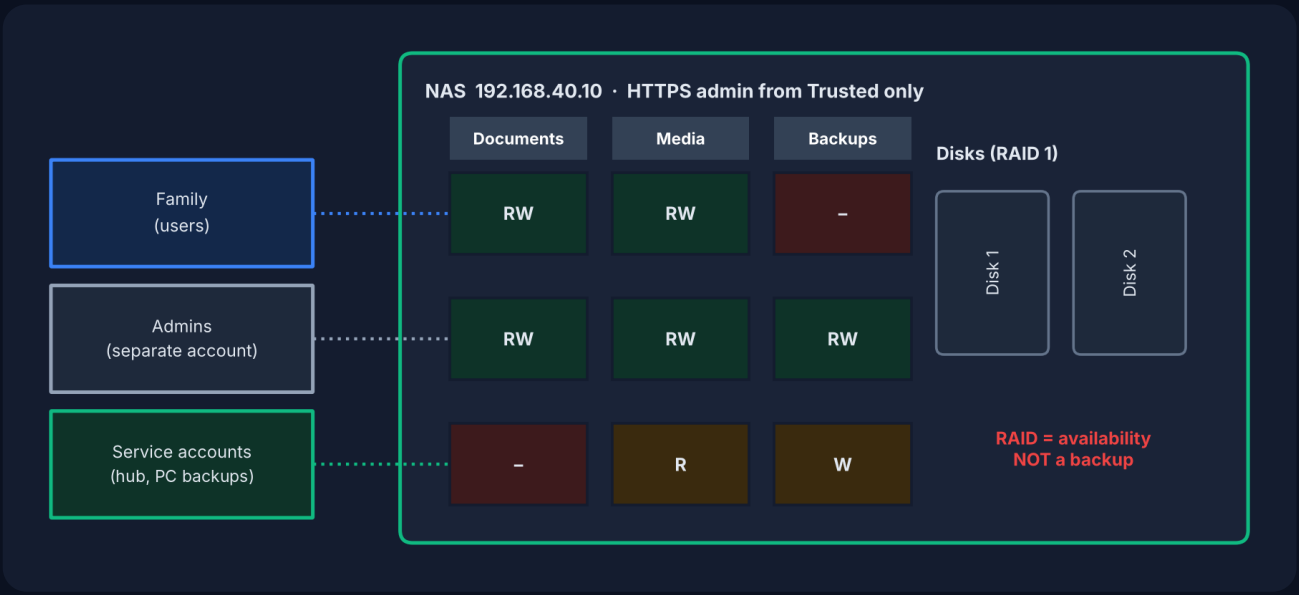


Figure 16.1 Groups get only the folder rights they need; RAID keeps the NAS running after a disk failure but is not a backup.

Choosing a NAS

Any NAS with current security updates, SMB file sharing, snapshots, user/group permissions and a built-in backup app will do. Two disks in RAID 1 (mirror) are a sensible home minimum; use NAS-rated disks and check the vendor's update lifecycle before buying.

Addressing and administration

Give the NAS a DHCP reservation and a stable hostname. Keep the admin interface reachable only from trusted management devices; use HTTPS, disable the default admin account, and enable MFA for administrators.

Storage layout

Use separate shared folders for documents, media and backups with least-privilege permissions. RAID improves availability but is not a substitute for an independent backup (chapter 17).

Services and hardening

Enable only the services you use – usually SMB for file sharing, plus NFS if needed. Disable old SMB1, UPnP, QuickConnect-style cloud relays and unused apps. Turn on automatic security updates and e-mail alerts for disk health and failed logins.

Performance checks

Measure SMB transfer speed, disk health (SMART), backup duration and uplink negotiation. Consider 2.5 GbE only when the disks, the switch and the clients can benefit.

PHASE 3 · SECURE & RUN

17 Backups and a real restore test

A backup counts only after you have restored from it

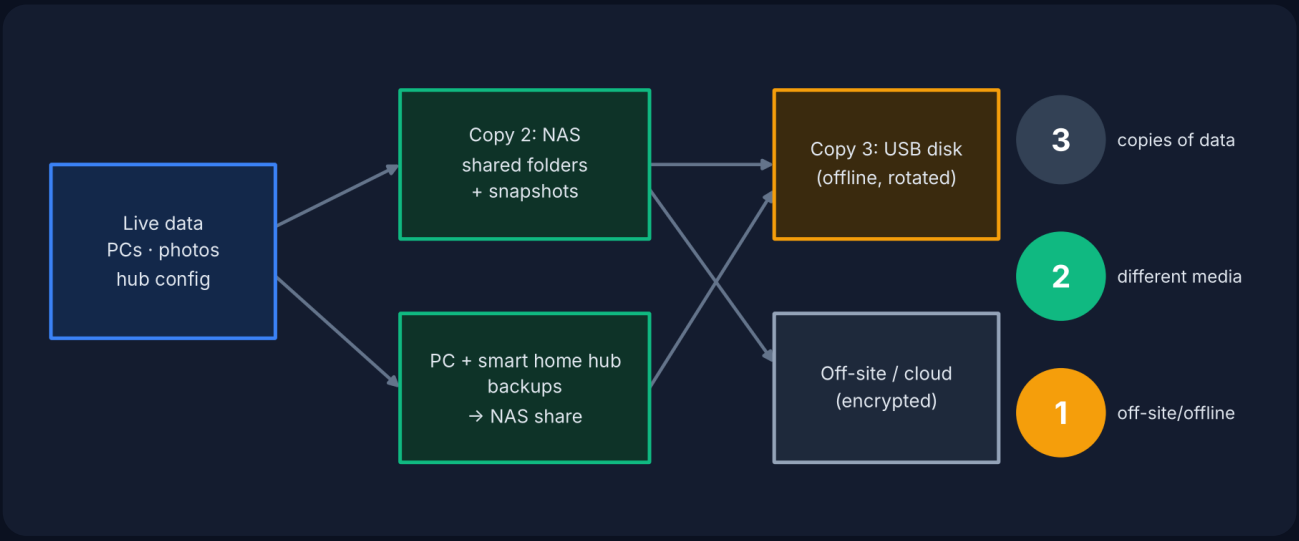


Figure 17.1 3-2-1: three copies, two kinds of media, one copy away from the house or disconnected.

WHAT	HOW	WHERE / HOW OFTEN
Controller configuration	Settings → System → Backups (auto) + manual export after changes	Download to NAS; weekly + after changes
Smart home hub	Settings → System → Backups, automatic, encrypted	Network storage on NAS; daily, keep 7
PCs and laptops	Windows File History / backup app, macOS Time Machine	Backups share on NAS; daily
NAS shared folders	Snapshots (where the file system supports them) + the NAS backup app	Snapshots hourly/daily; backup to USB + cloud
Passwords / keys	Password manager export, encrypted	Offline USB in a safe place

Procedure – yearly restore drill

01 Pick one item of each type: one file, one PC backup, one hub backup, the controller config.

02 Restore the file from the USB or cloud copy to a *different* folder and open it.

03 Restore a folder from a PC backup to a spare location and check the files open.

04 Load the hub backup on a spare device or a fresh test installation and confirm automations and integrations appear.

05 Write down how long each restore took – this is your real recovery time.

CAUTION RAID and snapshots protect against a failed disk, not against ransomware that encrypts the NAS or a fire. Keep one copy offline or immutable.

Further reading

↗ Example (Home Assistant): backups

PHASE 3 · SECURE & RUN

18 Smart home hub and IoT

Integrate smart devices without losing control

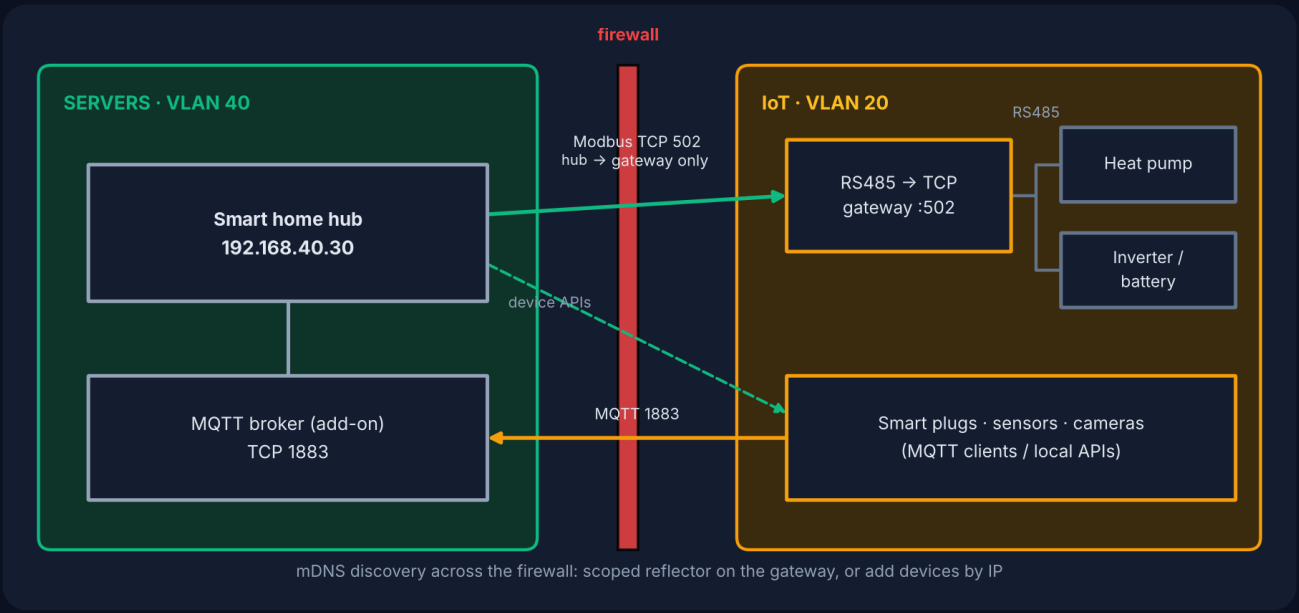


Figure 18.1 The smart home hub in the server zone reaches IoT devices only through narrow, documented ports.

Deployment choices

Run the hub (e.g. Home Assistant, openHAB, ioBroker) on a dedicated low-power mini-PC or a vendor appliance. Use an SSD rather than an SD card, give it a stable address and send its automatic backups to the NAS.

Network placement

Place the hub in a trusted or server VLAN and permit only required access to IoT devices. Document ports for MQTT, Modbus TCP, device APIs and discovery.

Discovery challenges

mDNS and SSDP do not automatically traverse VLANs. Use carefully scoped multicast support, manual IP integrations or a gateway reflector as appropriate.

Example integrations

An RS485-to-TCP gateway can expose a heat pump or inverter on a controlled IoT segment. Limit which hub host may connect to its TCP service and avoid opening it to the internet.

Operations

Monitor entity availability, DHCP reservations, latency and backups. Use an isolated test path before changing heating, cooling, battery or safety-related automations.

Further reading

↗ Example (Home Assistant): installation
↗ Example (Home Assistant): backups

PHASE 3 · SECURE & RUN

19 Troubleshooting and rollout

Test methodically and document the final state

Figure 19.1 Ask the questions in order; the first NO tells you where to look.

Layered diagnosis

Start with power, link lights and cable test; continue with switch port/VLAN, DHCP lease, default route, DNS and finally application logs. Change one variable at a time.

Common faults

Wrong native VLAN can hide an AP; a DHCP conflict can cause intermittent loss; poor 2.4 GHz placement can destabilise IoT; double NAT can complicate inbound connectivity.

Useful commands

Treat ping failure cautiously because ICMP may be blocked. The controller's client entry shows VLAN, AP, signal and lease; firewall logs show which policy dropped a packet. Full command list: Appendix F.

Commissioning

Test every outlet, VLAN, SSID, VPN, backup job, UPS shutdown and management login. Save firmware versions, topology, address plan and an export of firewall rules, then sign off Appendix G.

Maintenance calendar

Monthly: review alerts and backups. Quarterly: inspect firmware and account access. Annually: restore a backup, check UPS batteries, validate diagrams and retire unused devices.

Further reading

↗ Example (UniFi): help centre / troubleshooting

PHASE 3 · SECURE & RUN

20 Updates and change management

Keep it current without breaking it

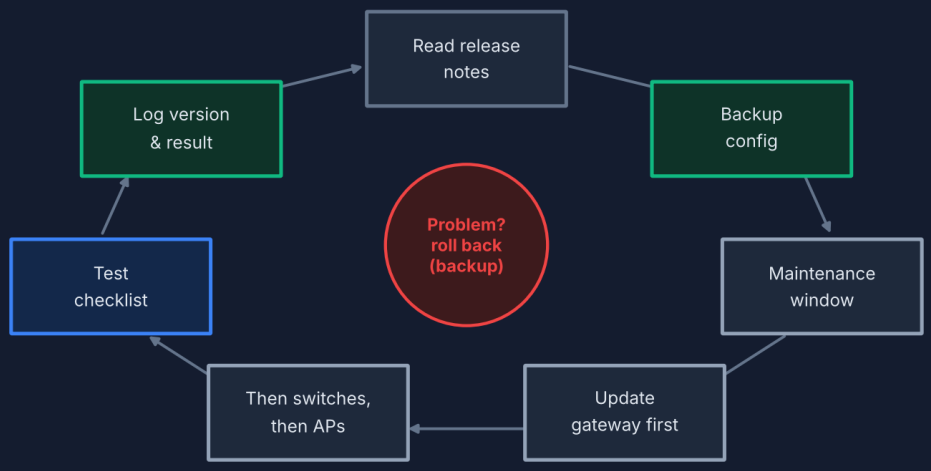


Figure 20.1 The same loop for every firmware update or configuration change.

Procedure – firmware update

01 Read the release notes; skip early-access releases on a network you depend on. Wait about a week after a release.

02 Export a backup and note current versions of gateway, controller, switches and APs.

03 Update the controller/gateway first, then switches, then access points one at a time – not all APs together.

04 After each step run a short checklist: internet, one client per VLAN, Wi-Fi on each SSID, VPN, hub dashboard.

05 If something is broken, roll back the device or restore the backup before trying fixes.

06 Record the change in the log below.

DATE	DEVICE / AREA	CHANGE	RESULT / ROLLBACK	BY
2026-11-02	Gateway	Firmware x.y.z → x.y.z+1	OK, all tests passed	admin

TIP NAS: install updates when no backup job is running and check disk health afterwards. Smart home hub: always tick “create backup before updating”.

REFERENCE

A Example IP and VLAN plan

Practical appendix

NETWORK	VLAN	SUBNET	GATEWAY	DHCP POOL	RESERVATIONS
Trusted	10	`192.168.10.0/24`	.1	.100–.249	printer .20
IoT	20	`192.168.20.0/24`	.1	.100–.249	RS485 gateway .20
Guest	30	`192.168.30.0/24`	.1	.100–.249	–
Servers	40	`192.168.40.0/24`	.1	.100–.149	NAS .10 · smart home hub .30
VPN	–	`192.168.50.0/24`	.1	assigned per client	–

The addresses are illustrative. Configure each network in the controller as a routed VLAN with its own DHCP pool. Restrict management interfaces to Trusted or a dedicated Management VLAN.

REFERENCE

B Controller configuration walkthrough

Practical appendix

01 Settings → Networks: create Trusted / IoT / Guest / Servers.

02 Set VLAN IDs 10 / 20 / 30 / 40.

03 Set gateway/subnet and DHCP range for each network.

04 Settings → WiFi: map the Home SSID to the Trusted network.

05 Map the IoT SSID to IoT and the Guest SSID to Guest.

06 Switch uplinks: allow the required tagged VLANs.

07 Endpoint ports: assign the intended untagged network and block other tagged VLANs.

TIP Menu names vary by vendor and release. Confirm the exact UI labels and policy model in your installed version, and keep the gateway management path available while changing switch profiles.

Further reading

↗ Example (UniFi): creating VLANs
↗ Example (UniFi): network and client isolation
↗ Example (UniFi): WAN and LAN port configuration

REFERENCE

C Firewall policy matrix

Practical appendix

SOURCE → DESTINATION	ACTION	NOTE
Trusted → Internet	ALLOW	
Trusted → Servers	ALLOW selected ports	HTTPS, SMB, smart home hub
IoT → Internet	ALLOW only if required	cloud-dependent devices only
IoT → hub 192.168.40.30	ALLOW selected integrations	MQTT 1883, hub 8123
IoT → Trusted	DENY	
Guest → RFC1918 private	DENY	all private ranges
Guest → Internet	ALLOW	
WAN → management	DENY unsolicited	use VPN instead

Use stateful return traffic and evaluate local gateway/DNS rules separately where required. Explicitly test IPv6 and any VPN interfaces. Rule order and object semantics depend on the gateway firmware.

Further reading

↗ Example (UniFi): zone-based firewall
↗ Guest WiFi best practices

REFERENCE

D NAS checklist

Practical appendix

- ☐ Reserve the NAS IP address and enable HTTPS administration
- ☐ Disable the default admin account; enable MFA for administrators
- ☐ Create users and groups with least privilege
- ☐ Disable unused services (SMB1, UPnP, cloud relay, unused apps)
- ☐ Configure snapshots where supported
- ☐ Set an independent backup target (USB + cloud) and schedule
- ☐ Enable the network UPS server and disk health alerts
- ☐ Restore test: verify files and smart home hub configuration

CAUTION Keep NAS administration off Guest and IoT. Never treat RAID as backup. Verify backups are readable after a simulated device failure.

REFERENCE

E Smart home integration pattern

Practical appendix

ITEM	PATTERN
Hub host	Fixed/reserved address 192.168.40.30
MQTT broker	Allow selected IoT devices only (TCP 1883)
Modbus TCP	Allow the hub to the RS485 gateway TCP port 502 only
mDNS	Scoped reflector or manual IP discovery
Snapshots / backups	NAS plus external destination
Monitoring	Device availability, latency and errors

CAUTION For inverter, battery and heat-pump control, prefer read-only discovery first. Validate register maps and fail-safe logic before permitting write commands. Modbus TCP is typically unencrypted: isolate it.

Further reading

↗ Example (Home Assistant): installation
↗ Example (Home Assistant): backups

REFERENCE

F Troubleshooting commands

Practical appendix

QUESTION	WINDOWS	LINUX / MACOS
Link and speed?	`Get-NetAdapter`	`ip link · ethtool eth0`
Which IP / gateway / DNS?	`ipconfig /all`	`ip addr ; ip route ; resolvectl status`
Gateway reachable?	`ping 192.168.10.1`	`ping -c 4 192.168.10.1`
Internet reachable?	`ping 1.1.1.1`	`ping -c 4 1.1.1.1`
DNS works?	`nslookup example.com`	`dig example.com`
Path to a host?	`tracert 1.1.1.1`	`traceroute 1.1.1.1 · mtr 1.1.1.1`
TCP port open?	`Test-NetConnection host -Port 443`	`nc -vz host 443`
Renew DHCP lease	`ipconfig /release && ipconfig /renew`	`sudo dhclient -r && sudo dhclient`

Run commands on a test host inside the affected VLAN. Verify switch port membership, lease information and firewall logs. DNS and ICMP policies may affect the interpretation of tests.

Further reading

↗ Example (UniFi): help centre / troubleshooting

REFERENCE

G Deployment acceptance sheet

Practical appendix

- ☐ WAN connectivity and expected throughput
- ☐ All cable runs labelled and tested
- ☐ Switch PoE budget and AP adoption verified
- ☐ Each SSID maps to the correct VLAN
- ☐ Guest and IoT isolation tested
- ☐ NAS / smart home hub reachable only as intended
- ☐ Backups, restore, VPN and UPS shutdown tested
- ☐ Configuration exports and diagrams saved

INSTALLED BY	DATE	SIGNATURE

Sign off the installation only after both positive and negative access tests. Keep a dated copy of this checklist and re-run it after significant network changes.