

Task 8 Network Design Guide

This guide helps you build a clear, assessable high value domestic network design using a real floorplan and UniFi Design Center evidence.

Step 1: Select A Suitable Property

Choose a house listing from realestate.com.au that includes a clear floorplan.

Choose a property that has enough network design complexity, such as:

- multiple bedrooms
- study or home office
- theatre, games room or large living area
- garage or workshop
- outdoor entertaining area
- multiple storeys
- security camera or smart home opportunities

Avoid tiny or unclear floorplans because they make the network design too shallow.

Step 2: Analyse The Requirements

Do not start by placing access points. Start by reading the floorplan like a client brief.

Ask:

- Where will people work, study, stream or game?
- Where are fixed devices likely to need ethernet?
- Which spaces need strong Wi-Fi?
- Which outdoor areas need coverage?
- Which smart home, IoT or camera devices need network access?
- Which devices should be separated from the main private network?
- Where would the internet service likely enter the house?
- Where could a central network cabinet or rack be located?

Step 3: Identify The Network Type

The home needs a **local area network (LAN)** because devices inside the property need to share local network access.

The home also needs a **wide area network (WAN)** connection because the LAN connects to an internet service provider.

A **personal area network (PAN)** may apply to very short-range personal devices, such as a phone connected to earbuds or a smartwatch. Do not describe the whole house network as a PAN.

Step 4: Choose The Topology

Use a **star topology** for the main domestic LAN. In a star topology, wired devices connect back to a central point, usually a switch or PoE switch. Wireless access points also connect back to the LAN.

Why this suits the scenario:

- it is common in modern homes
- it supports reliable ethernet runs to key rooms
- it allows central management and troubleshooting
- it supports PoE access points and cameras
- one cable fault usually affects one device or area, not the whole LAN

Step 5: Place The Main Hardware

Hardware	Function in this design
Modem or ONT	Connects the home to the internet service provider connection.
Gateway/router	Directs traffic between the home LAN and the internet/WAN.
Firewall function	Controls allowed and blocked traffic to protect the network.
Switch or PoE switch	Connects wired LAN devices and may provide power to access points or cameras.
Wireless access point	Provides Wi-Fi coverage to rooms and outdoor spaces.
NIC	Allows a device to connect to the network using wired or wireless hardware.
Bridge or mesh link	Connects a network segment where cabling is not available; use only if justified.

Use this build order when placing and explaining hardware:

Build order	Place or explain	Why it is needed	Evidence to include
1	Internet/WAN entry	Shows the external provider network before the home LAN.	WAN or ISP entry label, or a written assumption.
2	Modem or ONT	Connects the property to the internet service.	Label in topology or UniFi evidence.
3	Gateway/router/firewall	Routes between LAN and WAN and filters traffic.	Topology path and security reason.
4	Switch or PoE switch	Central point for wired star topology.	Switch label and branches to APs/devices.
5	Ethernet/PoE links	Reliable wired backhaul and fixed-device connections.	Ethernet/PoE labels or hardware/media table.
6	Wireless access points	Wi-Fi access to the wired LAN.	Device placement and heatmap screenshots.
7	Wired fixed devices	Shows suitable media selection for high-demand devices.	Device list and written justification.
8	Guest/IoT/camera/home office networks	Shows security and segmentation decisions.	Security/topology explanation.
9	Optional bridge/mesh/cellular/satellite	Solves a specific limitation only where needed.	Limitation plus reason for the optional link.

Step 6: Select Transmission Media

Medium	Suitable use	Reason
Twisted pair ethernet	Access points, cameras, home office, TV/media, gaming console, printer, NAS and switch links	Reliable, common and suitable for fixed high-demand devices.
Wireless	Phones, tablets, laptops and guest devices	Supports mobile devices and flexible use across the house.
Fibre optic	ISP connection or high-speed link if supplied or justified	High bandwidth and long-distance performance. Often appears as the provider connection rather than internal home cabling.
Cellular	Backup internet option	Useful for high availability if the primary internet fails.
Satellite	Rural or remote properties with limited fixed internet options	Use only if the selected property location or scenario makes it reasonable.

Step 7: Use UniFi Design Center Evidence

Your UniFi evidence should show:

- the floorplan imported or recreated
- access point placement
- coverage or heatmap evidence
- important wired device locations
- network core location
- device list or export evidence where possible
- screenshot evidence that supports your choices

The UniFi floorplan is not enough by itself. You also need to explain the logical network structure.

Step 8: Add Network Segmentation

For a high value domestic network, a single flat Wi-Fi network is usually weak.

Consider:

- family/private network
- guest network
- IoT or smart home network
- camera/security network
- home office network

Explain why separation helps. For example, guest devices should not access private computers, NAS devices, cameras or smart home management interfaces.

Step 9: Add Protocols

Email uses communication protocols:

- **SMTP** sends outgoing email.
- **IMAP** lets users access and sync mailbox folders across devices.
- **POP3** downloads email to a device and is less suitable if users need email across multiple devices.

For a home office user, IMAP is usually more suitable than POP3 because the user may access email from a laptop, phone and web browser.

Step 10: Add Security And Malware Responses

The design should include:

- strong authentication for network administration and Wi-Fi access
- separate guest and IoT access where suitable
- encryption for Wi-Fi and cloud services
- firewall rules or isolation between networks
- anti-malware protection, updates and safe-use practices

Link the protection to real risks such as cameras, smart locks, home office files, personal data, payment information and guest devices.

Step 11: Justify The Design

A strong justification follows this pattern:

I recommend [design choice] because [technical reason]. This suits the selected property because [floorplan, user, device, reliability or security link].

Example:

I recommend using ceiling-mounted wireless access points connected by twisted pair ethernet to a PoE switch because this gives reliable backhaul and central power. This suits the selected property because the living area, bedrooms and outdoor entertaining area need strong Wi-Fi coverage without relying on a weak single router in one corner of the house.