

3. Network Architecture

3.1 Overview

TheDen Home Network is designed for segmentation, performance, and manageability using VLANs to isolate traffic and prevent lateral movement between device classes. A router (Protectli FW6D running OPNSense) handles routing/NAT, VLAN termination, and DNS. A WiFi AP (UniFi 6+) connects directly to the FW6D via an 802.1Q trunk, broadcasting eight SSIDs across isolated VLANs.

3.2 Design Goals

- Isolation: Each VLAN has a clear and limited purpose.
- Visibility: All inter-VLAN and WAN traffic passes through OPNsense for inspection and logging.
- Control: Only authorized management systems can alter network configuration.
- Scalability: VLAN framework supports future expansion and additional IoT segmentation.

3.3 Physical Topology

[AT&T BGW320-500]

| (Fiber handoff)

|

[Protectli FW6D Firewall (OPNsense)]

└─ igb0 -> WAN (DHCP from ISP)

└─ igb1 -> 802.1Q Trunk to UniFi U6+ AP (VLANs 10,20,30,40,50,60,70,80,99)

└─ igb2 -> Admin (192.168.100.0/24)

|

[UniFi U6+ AP]

└─ SSID "thedenhome" -> VLAN 10

└─ SSID "thedenmobile" -> VLAN 20

└─ SSID "thedeniot" -> VLAN 30

└─ SSID "thedenguest" -> VLAN 40

└─ SSID “thedenprinter” -> VLAN 50

└─ SSID “thedenwork1” -> VLAN 60

└─ SSID “thedenwork2” -> VLAN 70

└─ SSID “thedenwork3” -> VLAN 80

3.4 Interface Summary

Interface	Description	VLAN	IP/Subnet	Notes
igb0	WAN	—	DHCP (public)	Connection to modem
igb1	LAN Trunk	10-99	—	VLAN trunk from AP
igb2	ADMIN	—	192.168.100.1/24	Ethernet mgmt port
vlan0.10	VLAN10_HOME	10	192.168.10.1/24	Personal computers
vlan0.20	VLAN20_MOBILE	20	192.168.20.1/24	Cellphones and tablets
vlan0.30	VLAN30_IOT	30	192.168.30.1/24	Smart devices
vlan0.40	VLAN40_GUEST	40	192.168.40.1/24	Guest WiFi
vlan0.50	VLAN50_PRINT	50	192.168.50.1/24	Printer VLAN
vlan0.60	VLAN60_WORK1	60	192.168.60.1/24	Work VLAN #1
vlan0.70	VLAN70_WORK2	70	192.168.70.1/24	Work VLAN #2
vlan0.80	VLAN80_WORK3	80	192.168.80.1/24	Work VLAN #3
vlan0.99	VLAN99_MGMT	99	192.168.99.1/24	WiFi AP VLAN

3.5 Subnet IP Addressing

VLAN	Subnet	Gateway	DHCP Range
VLAN10_HOME	192.168.10.0/24	192.168.10.1	100-200
VLAN20_MOBILE	192.168.20.0/24	192.168.20.1	100-200
VLAN30_IOT	192.168.30.0/24	192.168.30.1	100-200
VLAN40_GUEST	192.168.40.0/24	192.168.40.1	100-200
VLAN50_PRINT	192.168.50.0/24	192.168.50.1	100-200
VLAN60_WORK1	192.168.60.0/24	192.168.60.1	100-200
VLAN70_WORK2	192.168.70.0/24	192.168.70.1	100-200

VLAN80_WORK3	192.168.80.0/24	192.168.80.1	100-200
VLAN99_MGMT	192.168.99.0/24	192.168.99.1	100-200
ADMIN	192.168.100.0/24	192.168.100.1	100-200

Revision #1

Created 2026-07-12 20:34:57 UTC by Chris Landis

Updated 2026-07-12 20:36:19 UTC by Chris Landis