Home Network Security Assessment & Hardening

Router: TP-Link Archer AX55 Pro (v2.0)
Firmware: 1.0.5 Build 20240121 rel.56156(5553)
Network Type: Home Network
Assessment Type: Configuration Review & Security Hardening
Date: December 2025

---

1. Executive Summary

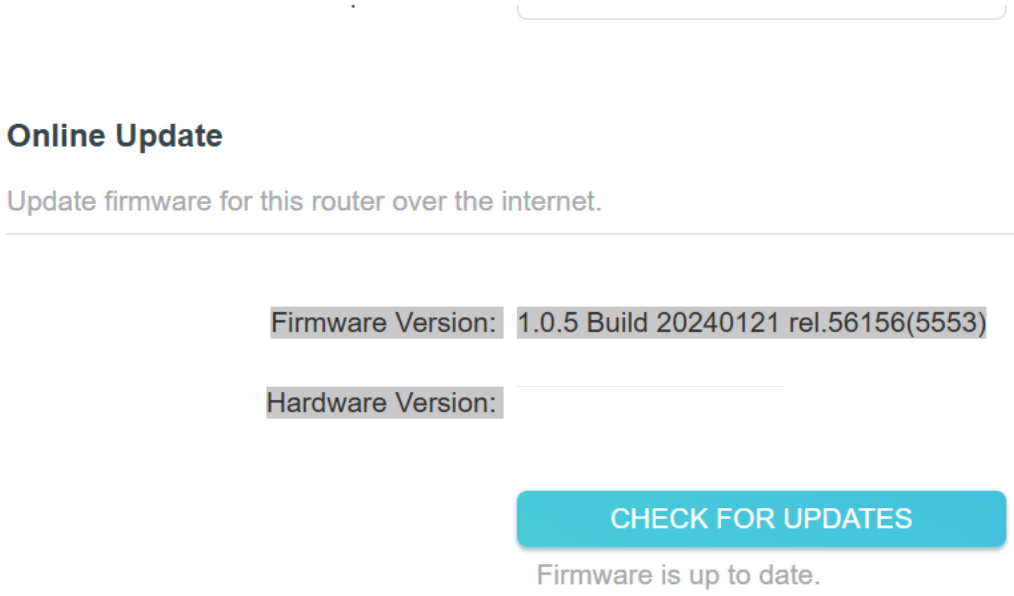
This report documents a security assessment and hardening review of a home network using a TP-Link Archer AX55 Pro router. The goal was to validate existing security controls, identify exposure risks, and ensure the network is configured according to modern home-network security best practices.

The assessment focused on wireless security, device visibility, management access, firmware status, network segmentation, and exposure discovery using passive and active techniques.

---

2. Environment Overview

- **Router Model:** TP-Link Archer AX55 Pro (v2.0)
- **Firmware Status:** Up to date
- **Wireless Security:** WPA3-Personal enabled
- **Network Segmentation:** Main, Guest, IoT networks
- **Total Connected Devices:** ~10
- **Assessment Tools:** Router UI, ARP table review, Nmap scan

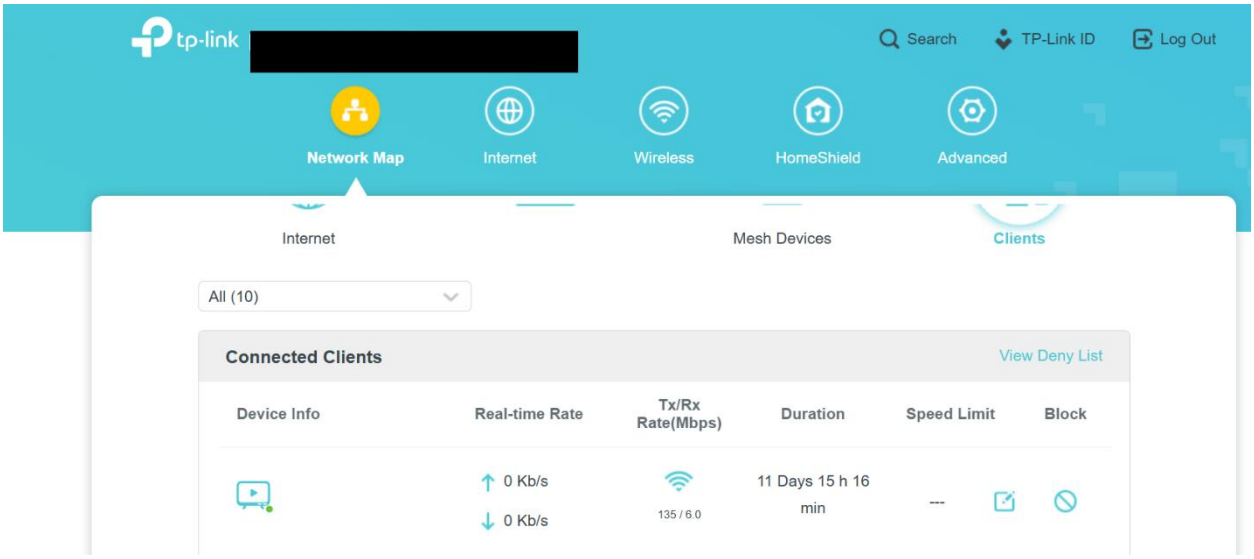


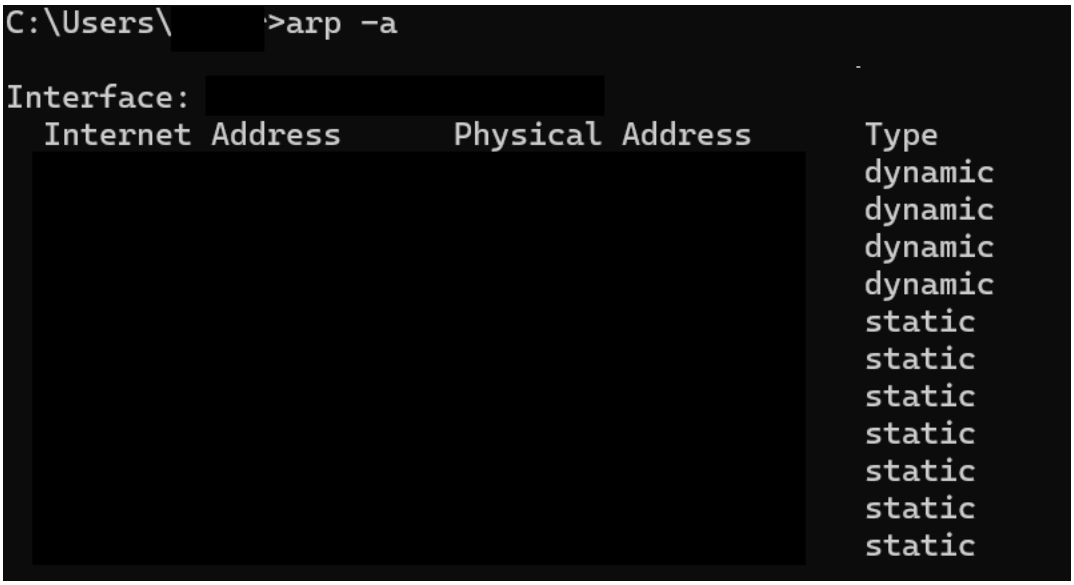
---

3. Connected Devices & Visibility

The router detected 10 active client devices. An ARP table review displayed 11 entries, which is expected behavior due to gateway presence and ARP caching.

This confirms accurate device visibility and no unexpected hosts at the router level.





---

4. Wireless Security Configuration

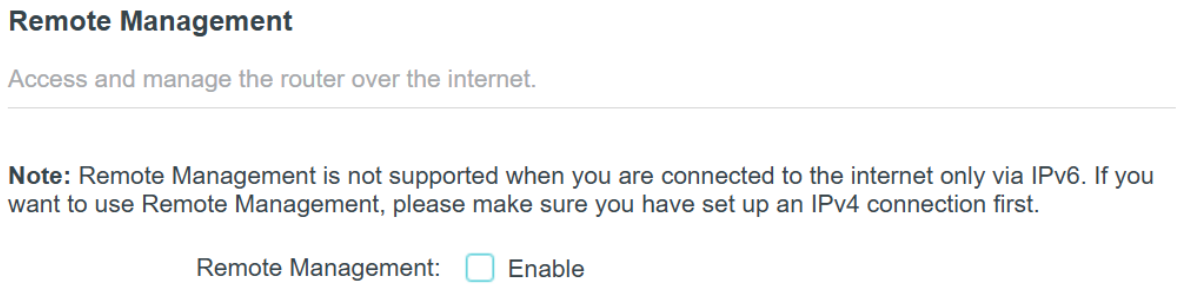
- WPA3-Personal was already enabled
- WPS was fully disabled to prevent brute-force enrollment attacks
- Strong wireless encryption in place with no downgrade mechanisms enabled

---

5. Administrative & Management Security

- Router administrative interface protected with a unique password
- Remote management disabled
- HTTPS login enabled

These settings reduce the attack surface by preventing external management access and protecting administrative credentials during login.

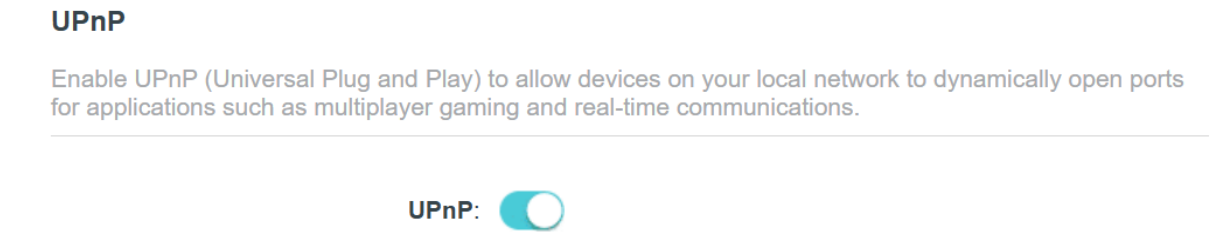


---

6. UPnP & Service Exposure

- UPnP enabled intentionally to support gaming devices (PS5 and PC)
- Risk acknowledged and documented
- No unnecessary port forwards observed

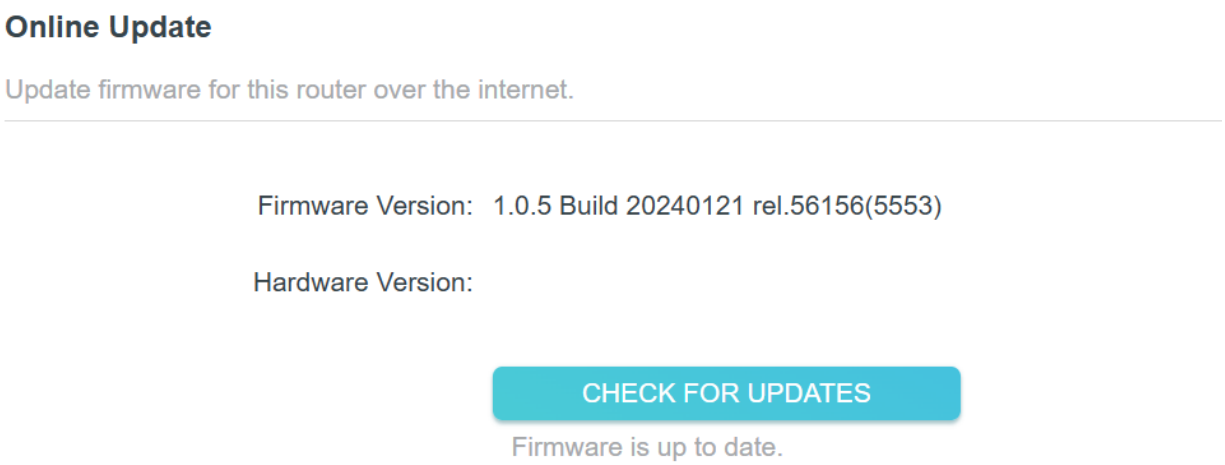
UPnP remains enabled only for functional requirements and is monitored as a known risk tradeoff.

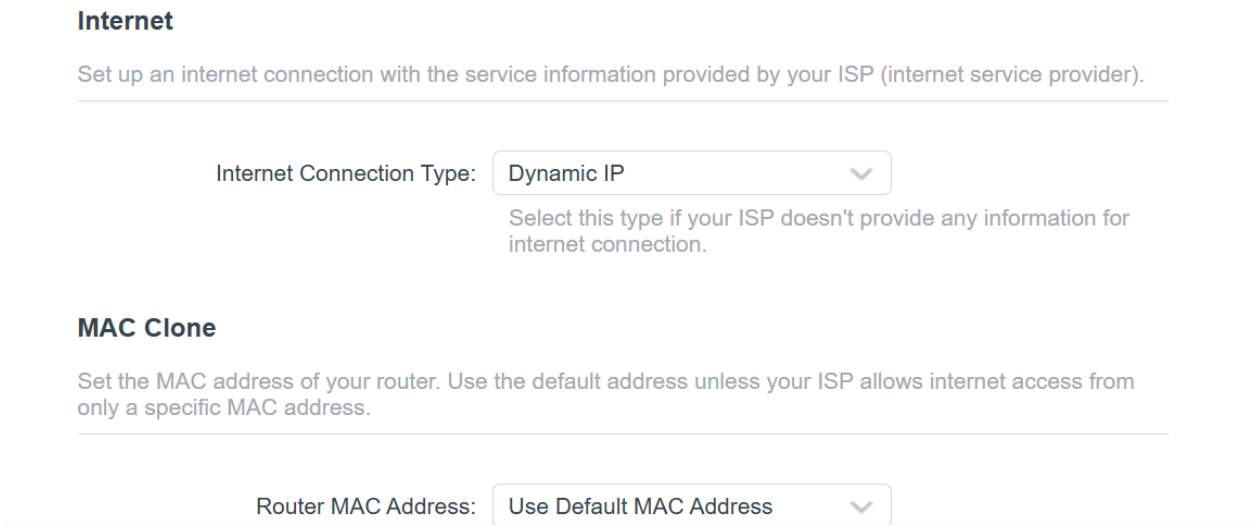


---

7. Firmware & DNS Configuration

- Firmware verified as current
- DNS resolution obtained dynamically from ISP
- No custom DNS filtering or third-party resolvers configured
- Baseline DNS state documented





---

8. Network Discovery & Exposure Testing

An Nmap scan identified **9 hosts**, aligning with known connected devices. No unexpected hosts or exposed services were discovered.

This confirms proper network segmentation and lack of unintended exposure.

```
nmap -sn  192.168.0.0/24
Nmap done: 256 IP addresses (9 hosts up) scanned in 7.46 seconds
```

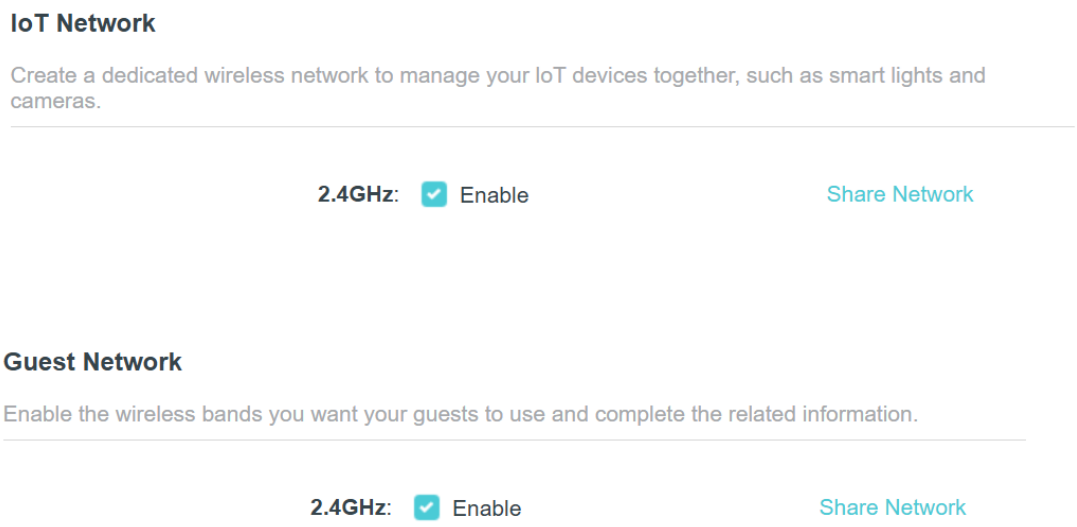
---

9. Network Segmentation & Isolation

The network is segmented into:

- **Primary Network:** Trusted personal devices
- **Guest Network:** Isolated internet-only access
- **IoT Network:** Isolated from internal devices

This segmentation limits lateral movement and reduces impact from compromised or untrusted devices.

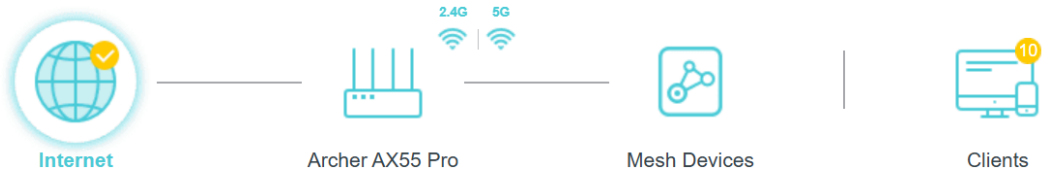


---

10. Final Validation

A final configuration review confirmed:

- No loss of connectivity
- No performance degradation
- Security controls remained active and functional



---

11. Summary & Portfolio Value

This project demonstrates:

- Practical network security assessment skills
- Safe configuration hardening without service disruption
- Risk-based decision making (UPnP tradeoff)
- Documentation suitable for client delivery

This assessment is representative of entry-to-mid level network security hardening engagements.