

# Smart Home Demo Wall – Build Guide 10

## Harden the Router and Network

Phase	Audience	Example Router	Goal
Guide 10	Builder / instructor	TP-Link Archer AX55 or similar	Secure the simulator network

<b>Purpose</b>	This guide hardens the router and simulator network after the smart-home devices are working. The goal is to reduce unnecessary access while keeping the board useful for demos and later student labs.
----------------	---

### BEFORE YOU HARDEN THE NETWORK

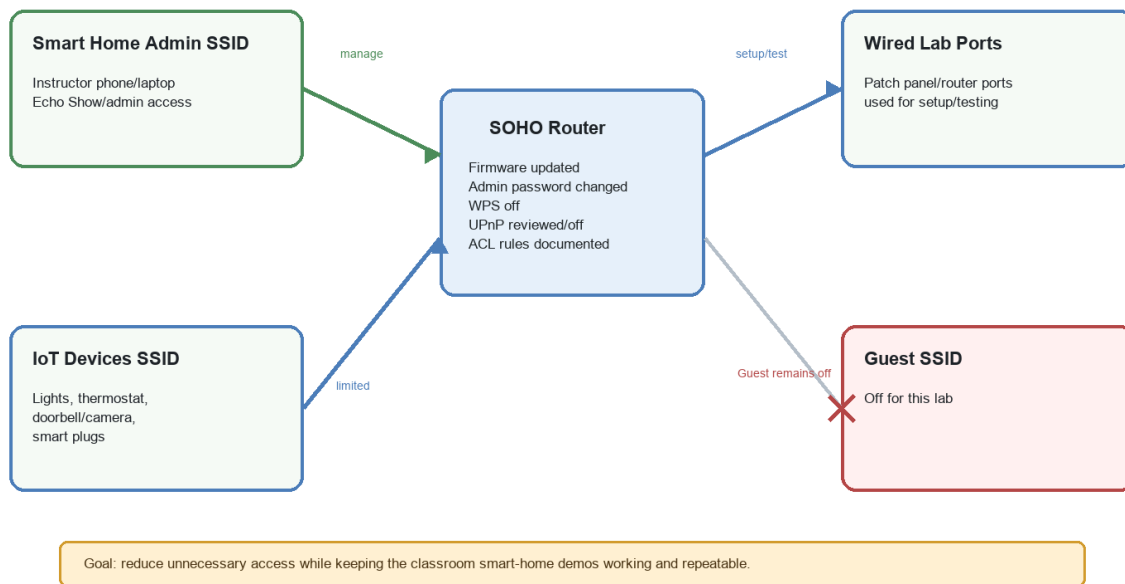
Start from a known working simulator. The lights, Echo Show, thermostat, HVAC simulator, doorbell/camera, router, and patch panel should already be installed and tested.

Done	Hardening Item	Evidence / Notes
<input type="checkbox"/>	Router is powered on and reachable	Record current router login method before changing settings.
<input type="checkbox"/>	Firmware has been checked	Update firmware before changing security controls.
<input type="checkbox"/>	Smart Home Admin SSID works	Instructor phone/laptop can connect and manage the system.
<input type="checkbox"/>	IoT Devices SSID works	Smart devices are online and visible in their apps.
<input type="checkbox"/>	Guest SSID is off	Leave guest off unless a later lab specifically enables it.
<input type="checkbox"/>	Demo routines still run	Run one known routine before hardening so there is a baseline.

## HARDENED NETWORK MODEL

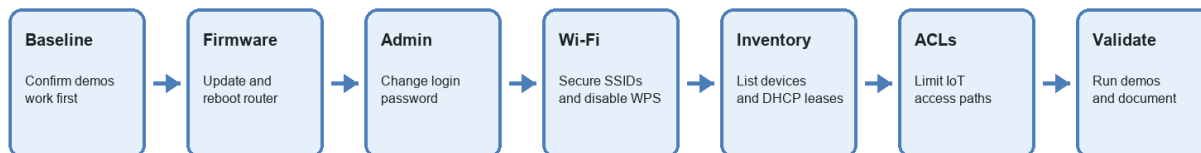
Use two working zones for this simulator: an admin zone for the instructor/demo controller and an IoT zone for smart-home devices. The guest network stays off for this lab.

### Hardened simulator network model



## HARDENING WORKFLOW

### Router hardening workflow



If a hardening change breaks a demo, document it, roll back only that setting, and test again.

**1** Confirm baseline operation  
Run one light demo, one HVAC simulator demo, and one Alexa routine before changing router security settings.

**2** Update firmware first  
Log in to the router, check firmware, install updates, and allow the router to reboot fully.

**3** Change the router administrator password  
Use a strong password. Record the storage location for the password, not the password itself, in student-facing documents.

**4** Secure Wi-Fi settings  
Use WPA2/WPA3 where available, strong SSID passwords, and clear SSID names for Smart Home Admin and IoT Devices.

**5** Disable WPS  
Turn off WPS so devices cannot be added by push-button or PIN pairing during the demo.

**6** Review UPnP  
Disable UPnP unless a specific smart-home device requires it for the lab. If enabled, document why.

**7** Create the device inventory  
Record each device, MAC address if available, assigned IP address, app used, and network zone.

**8** Apply ACL or isolation rules  
Limit IoT Devices from reaching admin devices where the router supports it. Keep required internet/cloud access for demos.

**9** Validate and document  
Run every demo again and write down which settings were changed.

## RECOMMENDED SECURITY SETTINGS

Setting	Recommended Lab Value	Reason
Router firmware	Current version installed	Fixes known bugs and security issues before the lab starts.
Router admin password	Changed from default	Prevents default-label password use during demos.
Remote management	Off unless required	Reduces external management exposure.
WPS	Off	Prevents easy unauthorized Wi-Fi enrollment.
Guest SSID	Off for now	Keeps the simulator focused on Admin and IoT networks.
Wi-Fi encryption	WPA2/WPA3 personal where available	Protects wireless traffic with modern authentication.
SSID passwords	Strong unique values	Avoids reuse with personal or campus networks.
UPnP	Off unless documented	Reduces automatic port-opening behavior.
DHCP	On, with known range	Keeps setup simple while allowing inventory tracking.
DHCP reservations	Use for key devices if available	Makes troubleshooting easier for thermostat, Echo Show, camera, and admin laptop.

## DHCP AND DEVICE INVENTORY

Confirm DHCP is enabled on the router and record the active DHCP range. For a classroom simulator, DHCP reservations are useful for devices that are checked often, such as the Echo Show, thermostat, camera, and instructor laptop.

Device	Network	MAC / Serial	IP Address	Reserved?
Instructor laptop/phone	Smart Home Admin			
Echo Show 5	Smart Home Admin or IoT Devices			
Smart thermostat	IoT Devices			
Doorbell/camera	IoT Devices			
Smart light 1	IoT Devices			
Smart light 2	IoT Devices			
Router LAN	Management		192.168.0.1	N/A

## ACCESS CONTROL LIST PLAN

<b>Teaching Note</b>	MAC filtering is useful for inventory discussions, but it should not be taught as strong security by itself. The stronger controls are good passwords, firmware updates, WPS off, network separation, and tested ACL/isolation rules.
----------------------	---

Traffic Path	Allow / Block	Reason
Admin device to router management page	Allow	Instructor or builder must manage the simulator.
Admin device to smart-device apps/cloud	Allow	Needed to configure and test devices.
IoT devices to internet/cloud services	Allow	Most smart devices require vendor cloud access.
IoT devices to admin laptop/phone	Block if supported	Reduces device-to-admin exposure.
Guest clients to simulator devices	Block / Guest off	Guest network is not used in this lab.
Unknown wireless clients	Block by password control	Do not share SSID passwords outside the lab team.

## VALIDATION TESTS

Done	Hardening Item	Evidence / Notes
<input type="checkbox"/>	Admin device can log in to router	Use the new router admin password.
<input type="checkbox"/>	Smart Home Admin SSID connects	Confirm internet and router management access.
<input type="checkbox"/>	IoT Devices SSID connects smart devices	Confirm all expected devices show online.
<input type="checkbox"/>	Alexa routine runs	Run Good Morning or Away Mode.
<input type="checkbox"/>	Smart light responds	Test app and voice control.
<input type="checkbox"/>	Thermostat can call HVAC simulator	Confirm correct LED response.
<input type="checkbox"/>	Doorbell/camera loads	Confirm app or Echo Show display response.
<input type="checkbox"/>	Guest SSID remains off	Confirm it is not visible or not enabled.
<input type="checkbox"/>	ACL/isolation does not break demos	If broken, document the rule and adjust only that setting.

## TROUBLESHOOTING AFTER HARDENING

Issue	Likely Cause	Fix
Device disappeared from app	SSID password changed or device joined wrong network	Reconnect device to IoT Devices SSID and retest.
Alexa routine partly fails	One device offline or blocked by isolation	Test each device manually, then review ACL rules.
Cannot reach router admin page	Admin device on IoT SSID or wrong gateway	Move admin device to Smart Home Admin SSID and browse to router IP.
Camera feed fails	Cloud access blocked or weak Wi-Fi	Allow required internet access and move camera/router closer for testing.
Thermostat app offline	Thermostat lost Wi-Fi after password change	Reconnect thermostat to IoT Devices SSID.
Hardening change broke several demos	Rule too broad	Disable the last rule, test, then create a narrower rule.

## FINAL HARDENING CHECKLIST

Done	Hardening Item	Evidence / Notes
<input type="checkbox"/>	Firmware updated and router rebooted	Record firmware version/date.
<input type="checkbox"/>	Router admin password changed	Record secure storage location.
<input type="checkbox"/>	Smart Home Admin and IoT Devices SSIDs secured	Record SSID names and storage location for passwords.
<input type="checkbox"/>	WPS disabled	Confirm setting after router reboot.
<input type="checkbox"/>	Guest SSID off	Leave disabled for this phase.
<input type="checkbox"/>	UPnP reviewed	Off unless a lab need is documented.
<input type="checkbox"/>	DHCP range recorded	Reservations added where useful.
<input type="checkbox"/>	Device inventory completed	Include device name, app, network, and IP.
<input type="checkbox"/>	ACL/isolation rules tested	Demos still work after hardening.
<input type="checkbox"/>	Router configuration backed up	Export/save config if router supports it.

## NEXT PHASE

After the router and network are hardened, the simulator is ready for repeatable instructor demos, user-guide field setup, and student troubleshooting labs. Later labs can intentionally break one setting at a time so students can diagnose Wi-Fi, DHCP, ACL, app, and device-cloud problems.

**Prepared by Sonny Bever**

Copyright © 2026 Sonny Bever. All rights reserved.

For classroom, booth, and smart-home simulator training use.