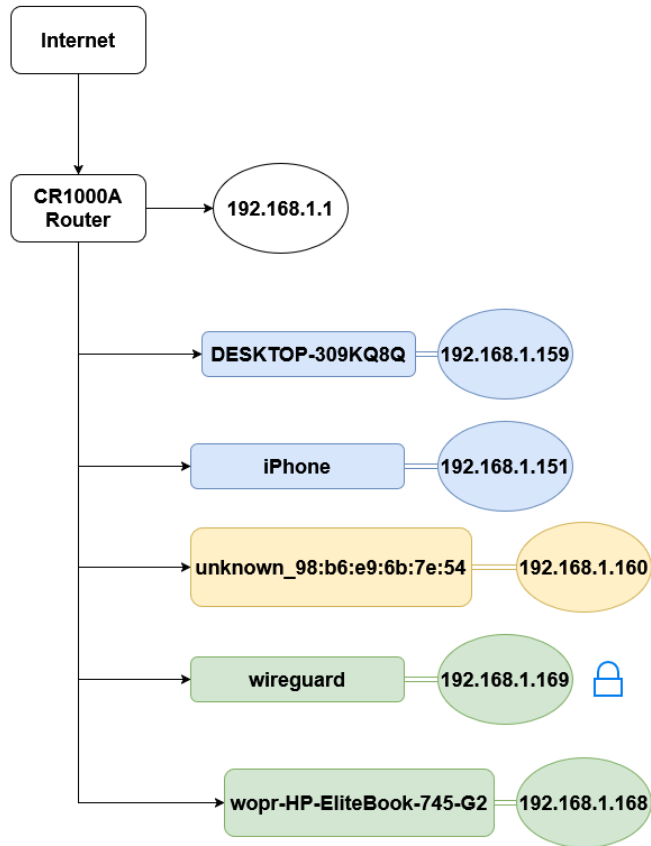


Network Audit - 10/16/25



Conducted security assessment of home network infrastructure.

Identified 4 medium-priority weaknesses requiring attention and solutions:

- Configured isolated guest network
- Changed default administrative credentials to strong password
- Disabled WPS to prevent brute-force attacks
- Verified minimal port forwarding exposure (only required VPN service)

Current security posture: GOOD

Remaining action: Monitor for firmware updates via ISP (manual updates unavailable)

Device Inventory:

ISP: AT&T Fiber/DSL

Gateway: CR1000A

Total Devices: 5 (2 wired, 3 wireless)

Security: WPA2

Device	Connection Type	Frequency/ Port	MAC Address	Purpose
iPhone	Wireless	5GHz	9c:79:e3:db:e0:e9	Personal mobile device
Nintendo Switch	Wireless	2.4GHz	98:b6:e9:6b:7e:54	Gaming console
WireGuard VPN	Wired	Ethernet	bc:24:11:ee:61:68	VPN gateway/secure tunnel
HP Elitebook 745-G2	Wired	Ethernet	58:20:b1:74:38:ff	Laptop running Proxmox

Note: All devices were eventually accounted for and authorized. Nintendo Switch originally flagged as "unknown" due to generic hostname – resolved through MAC address vendor lookup (Nintendo Co. Ltd.)

No guest network (Medium Priority)

Wi-Fi > Guest Network

Guest Network

Apply Changes

Band	Wi-Fi Name	Wi-Fi Password	Wi-Fi Disabled
2.4 GHz	Verizon_4LSKGT-Guest	●●●●●●●●●●	<input type="checkbox"/>

Issue: Visitors must connect to primary network, granting access to all internal devices

Risk: Guest devices could potentially access shared folders, printers, other network resources

Impact: Violates principle of least privilege and network segmentation best practices

Remediation: Created separate guest network

Guest Network

Apply Changes

Band	Wi-Fi Name	Wi-Fi Password	Wi-Fi Enabled
2.4 GHz	C3PO	Guest2025!	<input checked="" type="checkbox"/>

Security Set encryption type used to secure the Wi-Fi traffic.	WPA2
--	------

Administrative Credentials (Default) - REMEDIATED

Issue: Unable to verify if default admin credentials have been changed

Risk: Default passwords are publicly documented and easily exploited

Impact: Unauthorized config changes, DNS hijacking, malware injection possible

Remediation: Changed password to secure version and saved it.

Firmware Update Policy (Low Risk) - REMEDIATED

Issue: No documented schedule for firmware updates

Current Version: 3.6.0.2_BD

Date Checked: 10/16/25

Risk: Known vulnerabilities may remain unpatched

Impact: Potential for remote exploitation of router

Remediation: Router does not support automatic firmware updates or those done by the network user, only the network provider can do this.

WPS Status (Medium Risk) - REMEDIATED

Issue: Wi-Fi Protected Setup status not verified

Risk: WPS has known vulnerabilities allowing brute force attacks, meaning anyone in Wi-Fi range can gain access

Recommendation: Should be disabled if enabled

Remediation: Disabled WPS entirely. Devices will connect via standard password authentication only.

Wi-Fi Protected Setup

Enable Wi-Fi Protected Setup

WPS Enabled 

Wi-Fi Protected Setup is an easy way to add Wi-Fi devices to your network. To use this feature, your Wi-Fi client device needs to support WPS.

 Wi-Fi devices may briefly lose connectivity when turning WPS on or off.

Option 1 (Recommended)

If your client device has a WPS button, press it and then click the button below to start WPS registration.

Start WPS

Option 2

If your client device has a WPS PIN, enter that number below (usually found on a sticker on the back of the device) and click "Register".

Enter PIN

Register

Wi-Fi Protected Setup

Enable Wi-Fi Protected Setup

WPS Disabled 

Wi-Fi Protected Setup is an easy way to add Wi-Fi devices to your network. To use this feature, your Wi-Fi client device needs to support WPS.

 Wi-Fi devices may briefly lose connectivity when turning WPS on or off.

Firewall Check-Up - REMEDIATED

Issue: Routine firewall security and port configuration check-up

Risk: Unnecessary port forwarding rules allow easy access to the internal network of your home




Impact: Potential exploitation of the entire home network.

Remediation:

Port Forwarding Configuration:

1. WireGuard VPN (UDP 51820 goes to 192.168.1.168:51820)
 - Purpose: Secure remote VPN access
 - Status: Required, properly configured
2. System Rules (TCP 4567, 4577 goes to 127.0.0.1)
 - Purpose: Router management/diagnostic (AT&T built-in)
 - Status: Cannot be modified via GUI (system-level)
 - Risk: Low - forwards to localhost, not internal network

Follows the principle of least privilege. Only required VPN service exposed externally. System management ports isolated to the router itself.

Application	Original Port	Protocol	Fwd to Addr	Fwd to Port	Schedule	
	4577	TCP	127.0.0.1	4577	Always	
	4567	TCP	127.0.0.1	4567	Always	
WireGuard	51820	UDP	192.168.1.168	51820	Always	<input checked="" type="checkbox"/>   

Before:

- No guest network segmentation
- WPS enabled (brute-force vulnerability)
- Default admin credentials (unverified)
- Unknown device on network

After Remediation:

- ✓ Guest network configured with AP isolation
- ✓ WPS disabled
- ✓ Strong admin password set
- ✓ All devices identified and documented
- ✓ Port forwarding minimized to essential services only

Risk Reduction: Medium → Low

Ongoing Security Maintenance:

Weekly:

- Review connected devices list for unauthorized access
- Monitor guest network usage

Monthly:

- Contact ISP to verify firmware is up to date (version 3.6.0.2_BD as of 10/16/25)
- Review firewall logs for suspicious activity

Quarterly:

- Rotate admin password
- Re-audit port forwarding rules
- Test guest network isolation

Annually:

- Full network security assessment
- Update network documentation

Conclusion:

This audit successfully identified and remediated multiple security vulnerabilities in a residential network. The implementation of guest network segmentation, WPS disablement, and credential hardening especially improved the security posture.

The network now follows industry best practices including:

- Network segmentation (main vs. guest)
- Principle of least privilege (minimal port exposure)
- Strong authentication (complex passwords, WPS disabled)
- Documentation and monitoring procedures

Key Limitation: Firmware updates require ISP intervention. Recommend quarterly contact with AT&T to ensure security patches are applied.

What I Learned: This process gave me hands-on experience with router administrations, network segmentation, and security best practices. Key takeaways include the necessity of proper device identification (MAC Address Lookup), security risks of convenient features like WPS, and the value of network segmentation even in residential contexts. This process also reinforced that real security is an ongoing practice with regular monitoring and updates, not a one-and-done deal.

Overall Security Rating: Good

Primary Remaining Risk: Firmware update dependency on ISP