🔧Bash & PowerShell Tools for Field Technicians

Built by Wade Callender — AT&T Premises Technician | B.S. Cybersecurity

This repository includes practical Bash and PowerShell scripts I've created or customized based on real-world challenges faced in the field as a Premises Technician at AT&T. These tools improve service workflows, support troubleshooting, and promote safety and documentation standards in dynamic and high-pressure environments.

As someone who recently earned a B.S. in Cybersecurity and has a decade of frontline experience in emergency services and telecom, this repo bridges hands-on knowledge with growing technical expertise.

🛠️Script Categories

🔧NETWORK DIAGNOSTICS

`ping_sweep.sh`

- **Use case**: Quickly identify which devices are active on a customer's LAN during a service call.
- **Real benefit**: Speeds up troubleshooting when customer says, "My printer isn't showing up," or "The smart TV used to work."
- **For new hires**: Teaches subnet structure and host discovery without needing an app or network scan tool.

`trace_route.sh`

- **Use case**: Troubleshoot path-based issues when a customer complains about slow internet *despite speed tests being fine.*
- **Real benefit**: Shows where packets are slowing down — especially useful when identifying external routing delays vs local problems.
- **Training value**: Exposes newer techs to upstream routing and ISP pathing without escalation.

`dns_lookup.sh`

- **Use case**: Diagnose cases where sites like "Facebook won't load" but others do — likely a DNS issue.
- **Real benefit**: You'll resolve DNS-related issues faster than waiting on a helpdesk call.

📋INVENTORY & LOGGING

`device_inventory.sh`

- **Use case**: Document connected device IPs/MACs before or after a job.

- **Real benefit**: Creates a field report that shows everything online — useful for handoffs, escalations, or repeat service visits.
- **Bonus**: Can be shared with customers who want to “see what’s online” or confirm install results.

`save_config.sh`

- **Use case**: Save a snapshot of the current network configuration (routing tables, interfaces).
- **Real benefit**: Allows techs to compare “before/after” changes during troubleshooting or installs.
- **Compliance impact**: Provides documentation that could be used in escalations or to show work was done properly.

🔌CONNECTIVITY MANAGEMENT

`restart_network.sh`

- **Use case**: Restart a misbehaving interface on Linux-based equipment in customer environments.
- **Real benefit**: Reduces downtime, avoids escalation, and teaches new techs CLI-based service recovery.
- **Training opportunity**: Helps newer techs get comfortable with interface-level commands.

`flush_dns.ps1`

- **Use case**: Windows DNS cache issues after router changes or firmware updates.
- **Real benefit**: Speeds up resolution when customers complain about “browser errors” or “can't find site.”
- **Teach-back**: Show how caching works and how to clear stale lookups.

🔐SECURITY & AWARENESS TOOLS

`port_scan.sh`

- **Use case**: Internal scan for open ports using `nmap` or `nc`.
- **Real benefit**: Helps identify vulnerable or misconfigured devices, especially in smart homes.
- **Cybersecurity angle**: A real-world use of your degree — showing how network scanning supports risk analysis.
- **Training potential**: Teach new techs how port exposure relates to security posture.

`wifi_audit.sh`

- **Use case**: Scan router or access point for connected devices.
- **Real benefit**: Catches unknown devices, neighbor leeching, or overloaded guest networks.
- **Customer value**: Educate users on Wi-Fi security and why they should rotate passwords.

🚪Safety, Privacy & Professionalism

AT&T's culture of safety, compliance, and customer trust is at the core of how I use and share these tools. All scripts are designed to:

- ⚠️**Avoid storing or exposing customer credentials**
- ✅Support **OSHA and AT&T ladder & PPE safety standards** (especially when tied to on-prem work)
- 📵Reinforce **data privacy** and best practices in the field
- 🉐Support clean documentation, traceability, and escalation to network engineers

I've also incorporated principles from cybersecurity coursework — including risk-based thinking and root cause analysis — into how I design these tools.

💼Use Cases in the Field

- Fiber optic installs requiring rapid device discovery
- IP conflicts or dropped routes between gateway and ONT
- Latency issues from improperly configured DNS servers
- Verifying resolution after pole climbs or outdoor splicing
- Customer education on secure Wi-Fi practices

📅Career Impact & Training Value

- ✅Helps me showcase **cybersecurity skills applied in the field**
- 7️⃣Resource for **training new AT&T techs** on scripting, security, and install logic
- 🚷Supports **future lateral moves** into AT&T security, engineering, or QA teams
- 🔹 Can be used in **technical interviews**, internal demos, or GitHub portfolios

---

🗜️Future Additions

- `arp_monitor.sh` – Track new MACs on the network to detect rogue devices
- `network_baseline_logger.sh` – Snapshot before/after states during service calls
- `remote_toolkit.ps1` – Common PowerShell commands for remote support

Final Note

Stay safe, document everything, and script with purpose. If you're a fellow Premises Technician, trainer, or someone looking to improve the job with CLI tools and secure practices — fork this, contribute, or reach out.

💜Wade Callender
Dallas, TX
B.S. Cybersecurity (2025)
AT&T Premises Technician ``` Let me know if you'd like a GitHub Pages version or custom visuals next!