Network inventory

Acme Ltd

Devices seen from ACME-LT-04

Seen from	Date	Networks
ACME-LT-04	27 October 2026	1 subnet

This is a **passive** inventory: it lists the devices this computer already knows about from its own records, so the Cyber Essentials scope can be checked for completeness. It did not scan the network or sign in to anything, and used no passwords. It reflects the devices **ACME-LT-04** has recently communicated with, so run it on a computer that has been on the network a while, and on each separate network or site, for the fullest picture.

Devices seen	With a name	Wi-Fi security	Gateways
9	**4 of 9**	**WPA2**	**1 router**
on this network	from DNS	✓ Looks good	default gateway

Worth your attention

? Worth checking 1 open (passwordless) wireless network is in range. Check whether any belong to the business.

? Worth checking Confirm the router/firewall and any managed switches and Wi-Fi access points by signing in to them (see the checklist in this report). This tool cannot read their settings.

BLACKDOWN DIGITAL · SAMPLE DATA

This computer's network connection

Connection	Wi-Fi
Adapter	Intel(R) Wi-Fi 6E AX211 160MHz
This computer's address	192.168.1.50
Router (default gateway)	192.168.1.1
DNS server(s)	192.168.1.1
Addresses given out by	DHCP server at 192.168.1.1

Networks in scope

This computer is on: **192.168.1.0/24**. Every network the business uses is in scope, including other sites, home workers' networks and any guest network, so check those separately.

Devices seen on this network

Devices ACME-LT-04 has recently communicated with. The make is worked out from the hardware (MAC) address, and needs the free IEEE oui.csv file to be filled in (see the end of this report). This tool does not identify what each device is beyond the hints below, and does not read their settings.

Address	Name	Hardware (MAC) address	Make (from MAC)	Role
192.168.1.1	-	`00-1D-AA-3F-21-04`	Not identified	Router / firewall, DNS server, DHCP server
192.168.1.2	-	`44-D9-E7-10-2A-9B`	Not identified	
192.168.1.3	-	`78-8A-20-55-6C-01`	Not identified	
192.168.1.10	acme-nas	`00-11-32-8C-44-AA`	Not identified	
192.168.1.20	brother-printer	`00-1B-A9-7D-3E-10`	Not identified	
192.168.1.50	ACME-LT-04	`84-7B-EB-11-22-33`	Not identified	This computer
192.168.1.51	ACME-DT-01	`B8-CA-3A-90-1F-77`	Not identified	
192.168.1.80	-	`6A-11-22-33-44-55`	Randomised MAC (often a phone or privacy setting)	
192.168.1.99	-	`00-99-97-AB-CD-EF`	Not identified	

BLACKDOWN DIGITAL · SAMPLE DATA

Wireless

Connected network (SSID)	Acme-Office
Security	WPA2-Personal
Encryption	CCMP
Radio / band	802.11ax 5 GHz

Wireless networks this computer can see

Network (SSID)	Security	Encryption	Signal
Acme-Guest	WPA2-Personal	CCMP	72%
Acme-Office	WPA2-Personal	CCMP	86%
BTHub6-ABCD	WPA2-Personal	CCMP	40%
FREE-WIFI	Open ? Worth checking	None	30%

This lists wireless networks in range, which may include neighbours. Any that belong to the business should use WPA2 or WPA3, and a guest network should be kept separate from the main one.

BLACKDOWN DIGITAL · SAMPLE DATA

Confirm these on the kit itself

This passive inventory cannot read the settings inside your routers, switches and other network kit. These are the Cyber Essentials points to confirm by signing in to each device (or with Blackdown Digital's help). Tick them off against the device list above.

Router / firewall

- The default administrator password has been changed to a strong, unique one.
- There is no remote administration from the internet, or if there is, it is protected by multi-factor authentication or limited to trusted addresses.
- Incoming connections from the internet are blocked unless there is a documented business need (no unnecessary port forwarding).
- The firmware is a version the maker still supports, and updates are applied.
- UPnP is turned off unless something genuinely needs it.

Managed switches

- The default administrator password has been changed.
- The firmware is still supported and kept up to date.
- Any unused management access (Telnet, old web interfaces) is turned off; use HTTPS or SSH.

Wi-Fi

- The main Wi-Fi uses WPA2 or WPA3 with a strong passphrase.
- The access point admin password has been changed from the default.
- A guest Wi-Fi, if offered, is separate from the network the business devices use.

Servers, NAS and other devices

- Each is running software the maker still supports and is kept updated.
- Default passwords have been changed and only needed accounts exist.
- The old SMBv1 file-sharing protocol is turned off on NAS boxes.
- Printers and other devices with a web admin page have had their default password changed.

About this report

Produced by the Blackdown Digital Cyber Essentials Network Inventory, version 1.10.0.0, on 27 Oct 2026, 12:21 UTC, from ACME-LT-04. It is passive: it read only this computer's own network records, signed in to nothing, used no passwords, and changed nothing. Device makes are blank because no MAC lookup file was found. To fill them in, download the free IEEE registry from https://standards-oui.ieee.org/oui/oui.csv and save it as oui.csv next to this tool, then run it again. This report lists device names and addresses, so please treat it as confidential. It is a readiness aid, not a Cyber Essentials certificate.

BLACKDOWN DIGITAL · SAMPLE DATA