

NETWORK SETUP GUIDE

A practical guide to setting up reliable home, office and small-business networks — from internet connection to Wi-Fi, wired devices and security.

THE CALLSAVE RULE

A good network should be reliable, secure, easy to manage and ready to grow. Start with the customer's needs, then choose the router, switches, access points, cabling and internet service around those requirements.

1. The basic network

DEVICE	JOB
Internet / ISP connection	Provides the connection to the internet.
Router / firewall	Connects the local network to the internet and manages routing, firewalling and often DHCP/Wi-Fi features.
Switch	Connects wired devices such as PCs, printers, servers, access points and cameras. Managed switches add more control and segmentation options.
Wi-Fi access point	Provides wireless connectivity to phones, laptops, tablets and other Wi-Fi devices.
Ethernet cabling	Carries data between network equipment and wired devices.
UPS	Keeps critical networking equipment running during short power interruptions and helps reduce downtime.

2. Simple network layout

Internet/ISP → Router/Firewall → Switch → Access Points + PCs + Printers + CCTV + Other devices

For small businesses, switches and routers form the core of the network, while access points provide wireless connectivity. A scalable design can later support CCTV, VoIP, additional users and other connected systems.

3. Before you install

- ☐ Number of users and devices
- ☐ Number of rooms / floors
- ☐ Internet speed required
- ☐ Wi-Fi coverage areas
- ☐ CCTV requirements
- ☐ Printers / POS / servers
- ☐ Guest Wi-Fi requirement
- ☐ Future expansion
- ☐ Power availability and UPS requirement

ROUTER, SWITCH & WI-FI SELECTION

4. Router / firewall checklist

- ☐ Suitable for the number of users and expected internet bandwidth.
- ☐ Firewall enabled and configured.
- ☐ Strong administrator credentials configured.
- ☐ DHCP configured correctly unless another device provides it.
- ☐ Firmware kept current according to the manufacturer's support process.
- ☐ Remote management disabled unless genuinely required and securely configured.
- ☐ VPN capability considered for remote staff where needed.
- ☐ Dual-WAN/failover considered for businesses that cannot afford internet downtime.

5. Switch checklist

OPTION	WHEN TO USE
Unmanaged switch	Simple plug-and-play networks where advanced control is not required.
Managed switch	Business networks needing VLANs, monitoring, port control, QoS or other management features.
PoE switch	When powering devices such as compatible access points, IP cameras or VoIP phones over Ethernet is useful.

6. Wi-Fi access point checklist

- ☐ Do a coverage survey rather than guessing how many access points are needed.
- ☐ Place access points to provide useful coverage where people actually work.
- ☐ Avoid hiding APs inside metal cupboards or behind large obstructions.
- ☐ Use separate staff and guest networks where appropriate.
- ☐ Use modern Wi-Fi security supported by the equipment and clients.
- ☐ Use wired backhaul where practical for business access points.
- ☐ Test roaming and coverage in all important areas.

Guest Wi-Fi should be separated from internal business resources so visitors can access the internet without unnecessarily exposing company devices or files. VLAN-based segmentation is one way to separate user groups on suitable equipment.
[cite][turn0search5][turn0search3]

7. Internet package selection

SITE	CALLSAVE STARTING POINT
Small home	Choose speed based on household users, streaming, work-from-home and smart devices.
Small office	Consider user count, cloud applications, VoIP, video calls, CCTV remote access and backups.
Busy business	Consider higher bandwidth, business support, static/public IP requirements where justified, and backup connectivity.

CABLING, SECURITY & BASIC CONFIGURATION

8. Cabling checklist

- ☐ Use suitable Ethernet cable for the intended network speed and environment.
- ☐ Keep data cabling neat, labelled and documented.
- ☐ Avoid unnecessary sharp bends and poor terminations.
- ☐ Separate data cabling appropriately from electrical cabling according to applicable installation practices.
- ☐ Test installed network cables and label both ends.
- ☐ Outdoor runs require suitable protection against weather, UV and physical damage.
- ☐ Fibre should be considered for long-distance links or electrically noisy environments where appropriate.

9. Basic network security

- ☐ Change all default router, switch and access-point passwords.
- ☐ Use unique administrator credentials.
- ☐ Keep firmware updated.
- ☐ Use strong Wi-Fi security and passwords.
- ☐ Separate guest Wi-Fi from business devices.
- ☐ Consider VLANs for staff, guest, CCTV, VoIP and IoT where the equipment supports it.
- ☐ Disable services and ports that are not needed.
- ☐ Keep a secure record of network configuration and recovery information.
- ☐ Restrict physical access to the router, switches and network cabinet.

10. Basic setup sequence

STEP	CALLSAVE PROCESS	ACTION
01	CONNECT ISP	Confirm the ISP connection works before installing the internal network.
02	INSTALL ROUTER	Connect the ISP equipment to the router WAN/Internet port.
03	CONFIGURE ROUTER	Set administrator credentials, internet settings, DHCP and firewall.
04	INSTALL SWITCH	Connect the switch to the router and verify link status.
05	INSTALL ACCESS POINTS	Connect APs, preferably by wired Ethernet/PoE where practical.
06	CREATE WI-FI	Set staff Wi-Fi and, where required, a separate guest network.
07	CONNECT DEVICES	Add PCs, printers, CCTV, POS and other equipment.
08	TEST	Check internet, Wi-Fi coverage, wired connectivity, printing and critical systems.
09	DOCUMENT	Record equipment, locations, IP ranges, Wi-Fi names, configuration and handover information.

Cisco's current small-business guidance similarly separates the roles of routers, switches and access points and recommends designing networks for growth and reliability. [\[cite\]](#)[turn0search0](#)[turn0search1](#)

CALLSAVE NETWORK SITE CHECKLIST

Use this during a customer visit to turn a simple “I need Wi-Fi” request into a clear network proposal.

CUSTOMER / SITE	_____
	☐ Home ☐ Office ☐ Retail ☐ Workshop ☐ Warehouse ☐ Other
USERS	_____ people
	PCs: ____ Phones: ____ Printers: ____ CCTV: ____ Other: ____
FLOORS / AREAS	_____
	_____ Speed: _____
ROUTER	☐ Existing ☐ New
	☐ None ☐ 5/8 port ☐ 16 port ☐ 24 port ☐ 48 port ☐ Other
POE	☐ No ☐ Yes — cameras/APs/phones
	☐ 1 AP ☐ 2 APs ☐ 3+ APs ☐ Site survey required
GUEST WI-FI	☐ Yes ☐ No
	☐ Yes ☐ No
UPS	☐ No ☐ Yes
	☐ Low ☐ Medium ☐ High

CALLSAVE HANDOVER CHECKLIST

- ☐ All network devices labelled.
- ☐ All Ethernet points tested.
- ☐ Wi-Fi coverage tested.
- ☐ Staff and guest Wi-Fi tested separately.
- ☐ Internet speed tested.
- ☐ CCTV/POS/printers tested where applicable.
- ☐ UPS tested.
- ☐ Firmware/configuration recorded.
- ☐ Customer shown how to connect devices.
- ☐ Customer given support/contact information.
- ☐ Secure configuration backup completed where supported.

CALLSAVE NETWORK PACKAGES

PACKAGE	TYPICAL BUILD	BEST FOR
ESSENTIAL	Router + basic switch + 1 access point	Homes and very small offices
BUSINESS	Business router/firewall + managed/PoE switch + multiple APs + guest Wi-Fi	SMEs, retail, offices and workshops
PRO	Business firewall + managed PoE switching + multiple APs + VLANs + UPS + monitoring/backup connectivity	Larger businesses and sites with CCTV, VoIP or critical connectivity

CALLSAVE SOLAR & EV CHARGING SOLUTIONS

Reliable connectivity for the systems that keep your business running — Wi-Fi, CCTV, POS, computers, printers, EV chargers and smart energy equipment.

Network designs should be adapted to the actual site, equipment and security requirements. Final electrical work, structured cabling, ISP requirements and any regulated installations should be completed by appropriately qualified professionals.

Further reading: Cisco's current small-business networking guidance covers routers, switches, access points, guest Wi-Fi and scalable network design. [\[cite\]](#)[turn0search0](#)[turn0search5](#)[turn0search4](#)