

Quick Network Design Checklist

01

Business & site requirements

Locations and users number, growth plans, critical applications, support model, budget boundaries, and outage tolerance.

02

Current topology & dependencies

WAN circuits, ISP handoffs, VLANs, routing, firewall zones, VPNs, SaaS/cloud dependencies, and third-party managed links.

03

Risk, security & resilience

Single points of failure tolerance, exposed services, identity controls, backup, logging, and recovery expectations.

Engineering checklist

Area	What to be checked
WAN & Internet	Primary/backup links, bandwidth fit, public IPs, NAT, failover behavior, ISP diversity.
Routing & IP plan	VLANs, subnets, gateways, static/dynamic routing, overlap risk, summarization, DHCP/DNS/NTP dependencies.
Security zones	Firewall policy, exposed management, corporate separation, guest access, VPN access, least-privilege segmentation.
WiFi & LAN	AP placement, PoE budget, roaming, SSIDs, guest access, switch uplinks, cabling, and port capacity.
Cloud & remote users	SaaS/cloud reachability, VPN/ZTNA options, branch-to-cloud paths, identity and MFA dependencies.
Operations	Monitoring, logging, backups, alerting, documentation, handover process, rollback plan, and acceptance checks.
Growth readiness	Spare switch ports, IP capacity, ISP lead times, equipment lifecycle, licensing model, and future site onboarding.

Typical outcome

A practical design pack, not only advice:

- current-state summary and key risks
- target-state diagram and traffic flow
- IP/VLAN/routing and security-zone recommendations
- implementation phases, rollback notes, and acceptance checks

Typical engagement flow

- 01 Discovery requirements and constraints
- 02 Review topology, risks, and dependencies for existing setup
- 03 Compare options
- 04 Design target architecture and migration path for existing setup or offer one
- 05 Growth limit analysis
- 06 Handover diagrams, checklist, and next actions

When this checklist is useful

Trigger	Why it matters
New office, relocation, or growth phase	Early design avoids expensive rework, rushed cabling, poor WiFi coverage, and undersized WAN capacity.
Cloud migration or more remote users	Traffic paths, identity, MFA, VPN/ZTNA, and security inspection should be reviewed before users feel performance or access issues.
Security concerns or unclear ownership	Clear zones, access policy, monitoring, backups, and documentation reduce operational risk and make support easier.