TUTORIAL · NETWORK SECURITY

Crafting Effective Network Diagrams: A Comprehensive Questionnaire for Modern Organizations

A practical, engineer-ready framework to gather requirements, identify gaps, and produce a network blueprint aligned to your organisation's goals.

Author: Md. Samsel Arifin

Website: msachowdhury.com

Category: Tutorial | Tags: #NetworkDesign #NetworkSecurity #VPN #VoIP #VLAN #Firewall #QoS

Introduction

Creating a reliable and scalable network diagram is one of the most critical tasks for any network security engineer. Before touching a single device or drawing the first node, you need answers — from the business, from the stakeholders, and from the existing infrastructure. This tutorial walks you through a structured questionnaire covering every dimension of a modern network: organisational context, technical requirements, security posture, and budget reality.

Use this as a living checklist before every network design engagement.

Part 1 — Organisational Overview

Before designing anything, understand the business context. These questions set the foundation for every architectural decision that follows.

1. **What type of business does the company operate?**
   Data-driven, service-oriented, or hybrid? This shapes throughput priorities and data-flow patterns.
2. **How many employees or users are there?**
   User count informs network load capacity, DHCP pool sizing, and switch port requirements.
3. **Where are the company's branches located?**
   Multi-site operations require WAN, SD-WAN, or site-to-site VPN. Consider MPLS vs. SD-WAN cost trade-offs early if there are 3+ sites.
4. **Is the company data-driven, service-focused, or both?**
   Core priorities determine whether latency, throughput, or uptime is the primary KPI.
5. **Who are the key stakeholders, sponsors, and end-users?**
   Prioritise network resources for decision-makers and identify who signs off on design changes.
6. **What is the physical size of the main offices and branches?**
   Floor plans affect AP placement, cabling runs, and IDF/MDF locations.
7. **Does the network support the business, is it the business, or both?**
   If the network IS the business (SaaS, fintech), HA pairs, VRRP/HSRP, and dual-ISP BGP are non-negotiable.

Part 2 — Network Characteristics & Capabilities

Assess the current state and define the target state. Each answer maps directly to a design decision.

1. What is the current state of the network?
Establish a baseline — topology, hardware age, known bottlenecks — before proposing changes.

2. Are there existing network documents and consistent standards?
Documentation reveals maturity level and accelerates gap analysis.

3. Do users need to connect remotely?
Drives SSL VPN, Zero Trust NAC, or IPSec tunnel design. For 50+ remote users consider a dedicated VPN concentrator or ZTNA platform.

4. Wireless or wired connections primarily?
Wireless-heavy environments need AP density planning, SSID segmentation per VLAN, WPA3, and a wireless controller.

5. Is VoIP needed?
Requires dedicated VLANs, DSCP EF marking for voice, AF41 for video, and sub-150ms one-way latency.

6. Own DNS/email server or cloud (M365/Google Workspace)?
On-premise adds MX, SPF, DKIM, DMARC complexity. Cloud shifts the ops burden but requires reliable egress.

7. Are ERP or EMS servers running within the network?
Critical servers influence VLAN segmentation, failover planning, and backup bandwidth allocation.

8. Is cloud computing required?
Cloud workloads need SD-WAN or Direct Connect links, and firewall egress policies for cloud CIDRs.

9. What devices will users connect from?
BYOD vs. managed devices changes NAC policy, MDM requirements (Intune, Jamf), and 802.1X config.

10. What are the security and redundancy needs?
Defines firewall tiers (perimeter, internal, DMZ), IDS/IPS placement, dual-ISP failover, and UPS requirements.

11. Will the network be centrally managed?
Requires a management VLAN. Popular stacks: PRTG, LibreNMS, Zabbix, Grafana + Prometheus.

12. Does the company require a public IP address block?
PI space needs ARIN/RIPE allocation and BGP. PA space is simpler but tied to your ISP.

13. How much internet bandwidth does the company currently have?
Capture CIR and burst capacity from the ISP contract as the baseline for upgrade planning.

14. Is the ISP connection static or dynamic?
Static IPs are required for inbound services. Dynamic connections need DDNS or a reverse-proxy.

15. Do they need content filtering and traffic control?
Drives firewall policy, proxy deployment, and DNS filtering (Cisco Umbrella, Cloudflare Gateway).

16. Security priority vs. uninterrupted fast access?
SSL inspection adds ~5–15ms. Both can coexist with proper QoS and SSL offload hardware.

17. Is zero downtime critical?
Requires HA pairs, VRRP/HSRP, dual-ISP BGP failover, and a documented RTO/RPO.

Part 3 — Budget & Vendor Dependencies

Constraints shape architecture. Surface budget and vendor lock-in early.

1. **What is the budget for the network infrastructure?**
   Budget ceiling determines whether you spec Cisco/Palo Alto (high-end), Fortinet/HPE Aruba (mid), or Ubiquiti/open-source (cost-constrained).
2. **Are there device or vendor dependencies?**
   Existing Cisco/Fortinet/Palo Alto investments may restrict choices. Confirm licences, support contracts, and EOL timelines.
3. **Internal IT team or external MSP?**
   MSP-managed networks need simpler ops models. Internal teams can handle complexity but need thorough runbooks.

Quick Reference — Useful Discovery Commands

Run these during network discovery and post-implementation validation:

Purpose	Command
Trace network path	traceroute <destination-ip>
Check DNS resolution	nslookup <domain> / dig <domain>
Scan open ports	nmap -sV -p 1-1024 <target-ip>
Show routing table	ip route show / route print (Windows)
Interface statistics	ip -s link show <iface> / ifconfig
Test VPN tunnel	ping <remote-gateway-ip> (inside VPN)
Bandwidth test	iperf3 -c <server-ip> / speedtest-cli
Active connections	ss -tulnp / netstat -ano
VLAN verification (Cisco)	show vlan brief
Interface VLAN (Cisco)	show interfaces trunk
ARP table	arp -a / ip neigh show
BGP neighbours (Cisco)	show bgp neighbors
Spanning-tree state	show spanning-tree summary
OSPF neighbours	show ip ospf neighbor
Packet capture	tcpdump -i eth0 -w capture.pcap

Conclusion

Answering these questions before touching any design tool transforms a network diagram from a generic topology into a strategic blueprint. It aligns your architecture with real business requirements, surfaces gaps early, and gives stakeholders a shared language for discussing infrastructure decisions. Save this checklist — the 30 minutes spent here will save you days of re-work later.

Need help with your network design?

Whether you're building from scratch or hardening an existing infrastructure, I offer consulting tailored to your organisation's specific needs.

Contact via: msachowdhury.com