FREE RESOURCE

Network Reliability Checklist

10 critical checkpoints, with what good looks like and a quick-win fix for each

RUTE Solutions · rutesolutions.com · +1 (321) 337-9898

Use this checklist to audit your network and identify the gaps that turn into outages, audit findings, or middle-of-the-night incidents. Whether you operate one site or hundreds, the same ten items show up. For each one we cover what we look for, what good looks like, and one fix you can ship this quarter.

How to use it

Grade each checkpoint honestly as Pass or Needs Work, tally your passes, then check your score band on the last page.

1 Circuit Redundancy

Do critical sites have backup internet circuits from different providers or technologies?

WHY IT MATTERS

Single-circuit sites face complete outages whenever the carrier hiccups. Dual circuits with automatic failover compress downtime from hours into seconds and keep payment, voice, and operations online through individual provider failures.

WHAT GOOD LOOKS LIKE

Two diverse uplinks at every revenue-impacting site (fiber + fixed wireless or LTE/5G), policy-based routing for transactional traffic, sub-30-second failover validated under simulated failure.

QUICK WIN YOU CAN SHIP THIS QUARTER

Pick your three highest-revenue sites this week. Add a fixed-wireless or cellular backup uplink and route POS or order-entry traffic across both via SD-WAN policy.

SELF-GRADE ☐ Pass ☐ Needs Work

2 Network Segmentation

Are corporate, guest, IoT, cameras, OT, and production systems isolated by policy?

WHY IT MATTERS

Flat networks let a single compromised camera or IoT device pivot into the rest of your environment. Segmentation contains incidents, simplifies troubleshooting, and is what auditors look for under PCI DSS, HIPAA, and IEC 62443.

WHAT GOOD LOOKS LIKE

Dedicated VLANs for corporate, guest, IoT, voice, video, and OT traffic. Inter-zone flows allow-listed at the firewall, with documented justification per rule. Guest never touches operational.

QUICK WIN YOU CAN SHIP THIS QUARTER

Stand up a dedicated guest SSID this week with bandwidth caps and zero access to internal subnets. Single largest-impact change you can make in an afternoon.

SELF-GRADE ☐ Pass ☐ Needs Work

3 Configuration Backups

Are router, switch, and firewall configs backed up automatically and version-controlled?

WHY IT MATTERS

Hardware failures without recent config backups stretch recovery from minutes to days while your team rebuilds policy from memory. Version control also lets you diff changes and roll back fast when a deploy goes sideways.

WHAT GOOD LOOKS LIKE

Nightly automated config pulls from every device into a git repository, with named tags for known-good states. RMA replacements load the last config and the network re-converges within a maintenance window.

QUICK WIN YOU CAN SHIP THIS QUARTER

Wire up RANCID, Oxidized, or your vendor's native backup tool against your top 10 devices this week. Push the configs to a private git repo. Even a manual cron job beats nothing.

SELF-GRADE ☐ Pass ☐ Needs Work

4 Monitoring & Alerting

Do you receive actionable alerts before users report issues?

WHY IT MATTERS

Reactive troubleshooting wastes hours per incident and erodes user trust. Real monitoring with clear escalation paths catches link flaps, capacity drift, and silent device failures before they cascade.

WHAT GOOD LOOKS LIKE

Per-link health dashboards, latency and packet-loss baselines per site, alerts that route to the right team within minutes. Alert fatigue is low because thresholds are tuned to actual incident history, not vendor defaults.

QUICK WIN YOU CAN SHIP THIS QUARTER

Audit your last quarter of alerts. Anything that fired more than 10 times without an action taken gets silenced or its threshold re-derived from real incidents. Cut the noise before tuning the signal.

SELF-GRADE ☐ Pass ☐ Needs Work

5 Change Management Process

Are network changes documented, peer-reviewed, and tested before deployment?

WHY IT MATTERS

Roughly 70% of network outages are self-inflicted by an unplanned change. A lightweight change process with a rollback plan prevents the 11pm fire that started as a "quick" config push.

WHAT GOOD LOOKS LIKE

Every production change has a written ticket with the diff, the test plan, the rollback steps, and a peer review. Standard changes follow a template; risky ones get a maintenance window.

QUICK WIN YOU CAN SHIP THIS QUARTER

Adopt a single-page change record this week. Five fields: change description, devices affected, rollback steps, peer reviewer, validation steps. No ticket, no change.

SELF-GRADE ☐ Pass ☐ Needs Work

6 Wireless Capacity Planning

Is wireless designed for the device density and applications you actually run?

WHY IT MATTERS

Undersized Wi-Fi creates the support tickets nobody likes ("the network is slow") and forces workarounds that erode trust. Proper survey-driven design prevents coverage gaps, channel interference, and roaming failures across hand-held devices, voice headsets, and laptops.

WHAT GOOD LOOKS LIKE

Predictive RF design with a real building model, validated onsite under load with the actual client devices. AP density sized to peak concurrent users, with separate SSIDs for IoT and BYOD. Wi-Fi 6/6E/7 where capacity demands it.

QUICK WIN YOU CAN SHIP THIS QUARTER

Run a free Wi-Fi heatmap with NetSpot, Ekahau Survey, or your vendor's tool at your busiest site. The dead zones and channel collisions you find tomorrow are usually the same ones causing today's tickets.

SELF-GRADE ☐ Pass ☐ Needs Work

7 Firmware & Patch Management

Are network devices on supported firmware with known CVEs patched?

WHY IT MATTERS

Outdated firmware exposes networks to active exploits and the same kernel bugs that destabilize your devices week to week. Cyber insurers also increasingly verify patch posture before binding or renewing.

WHAT GOOD LOOKS LIKE

Inventory of every device with its firmware version, CVE exposure, and EOL date. Quarterly patch cycle for non-critical, monthly for security fixes, with a tested rollback path. Nothing running EOL firmware in production.

QUICK WIN YOU CAN SHIP THIS QUARTER

Pull a list of every network device and its firmware version this week. Anything more than two minor versions behind, or past EOL, gets put on the patch backlog. The list itself is half the work.

SELF-GRADE ☐ Pass ☐ Needs Work

8 Documentation & Diagrams

Do you have current network diagrams, IP allocation, and contact lists?

WHY IT MATTERS

Outdated docs slow troubleshooting, onboarding, and incident response. The cost shows up as longer MTTR and the kind of knowledge silos that turn one engineer's vacation into a crisis.

WHAT GOOD LOOKS LIKE

Living network diagram per site updated alongside changes (not after). IP allocation in IPAM, not a spreadsheet from 2019. Vendor and ISP contacts in the runbook with current account numbers.

QUICK WIN YOU CAN SHIP THIS QUARTER

Create a one-page "site map" for your most complex location: physical and logical topology, key VLANs, ISPs and account numbers, after-hours contacts. Refresh quarterly. Pin it in your team's wiki.

SELF-GRADE ☐ Pass ☐ Needs Work

9 QoS for Voice & Critical Apps

Is voice and business-critical traffic prioritized end-to-end during congestion?

WHY IT MATTERS

Without QoS, a single bulk transfer or someone streaming the game can degrade voice quality and break transactional systems. Proper marking and queuing ensure predictable performance for the traffic the business actually depends on.

WHAT GOOD LOOKS LIKE

DSCP marking at the source, trust boundary defined at the access edge, queuing applied on every congestion-prone link. Voice MOS, video conferencing health, and POS latency tracked as KPIs, not anecdotes.

QUICK WIN YOU CAN SHIP THIS QUARTER

Mark and prioritize voice (DSCP EF) on your WAN edge this week. It is the smallest QoS change with the most user-visible payoff. Layer in transactional and conferencing later.

SELF-GRADE ☐ Pass ☐ Needs Work

10 Incident Response Runbooks

Do you have written, tested procedures for the failure scenarios you actually face?

WHY IT MATTERS

Runbooks reduce stress and human error during outages. The team that has rehearsed "what if the primary firewall dies" recovers in minutes; the team that has not is reading documentation while the business loses revenue.

WHAT GOOD LOOKS LIKE

Runbooks for the top five failure modes (ISP outage, firewall failure, DC core down, ransomware suspected, AD compromise) with steps, who owns each step, escalation tree, and a clean drill in the last 12 months.

QUICK WIN YOU CAN SHIP THIS QUARTER

Pick your most-feared incident this week and write a one-page runbook for it. Walk a junior engineer through it on paper. Fix what they cannot follow. That is the runbook.

SELF-GRADE ☐ Pass ☐ Needs Work

How did you score?

Tally your "Pass" answers. The result is less about a grade and more about where to spend your next reliability budget.

8-10

Excellent

Your network is well-managed. Use this as your hardening backlog and keep the cadence.

5-7

Good Start

Solid foundation with measurable gaps. Address the lowest-scoring items first; they tend to be the cheapest fixes.

0-4

Needs Attention

High risk of outages and audit findings. Worth a focused engagement to remediate the structural items before the next incident.

Want a second pair of eyes on the gaps?

We run focused network reliability reviews against this exact checklist. We will benchmark your environment, prioritize the items by impact and effort, and leave you with a written remediation plan your team can execute or hand to us.

- Identify and prioritize risk areas by impact and effort
- Validate the architectural items (segmentation, redundancy, QoS) against your real traffic
- Implement monitoring, alerting, and runbooks your team will actually use
- Hand it back documented end to end, so the platform is yours, not ours

Schedule a Network Reliability Review https://rutesolutions.com/contact