CLOUDSWITCHED

FREE RESOURCE — GUIDE

Network Performance Monitoring Guide

SNMP, NetFlow, alerting thresholds, and baseline metrics for proactive network management. Detect and resolve performance issues before they impact your business.

5	99.9%	5min	Free
MONITORING PILLARS	UPTIME TARGET	ALERT THRESHOLD	MONITORING GUIDE

Why Network Monitoring Matters

Proactive monitoring detects problems before users report them. Without monitoring, you are reactive — discovering issues only when staff complain. A well-monitored network reduces downtime by up to 85% and enables capacity planning based on real data.

1 Monitoring Fundamentals

Understand the core protocols and methods used for network monitoring.

SNMP (Simple Network Management Protocol) is the industry standard for device monitoring. It collects metrics from routers, switches, firewalls, and servers including CPU utilisation, memory usage, interface statistics, and uptime.

NetFlow / sFlow provides detailed traffic flow data showing which applications, users, and protocols are consuming bandwidth. This is essential for capacity planning and security analysis.

ICMP (Ping) provides basic reachability and latency monitoring. While simple, it is the fastest way to detect device or link failures.

PROTOCOL	WHAT IT MONITORS	BEST FOR	TYPICAL TOOLS
SNMP v3	Device health, interface stats, CPU, memory	Infrastructure monitoring	PRTG, Zabbix, LibreNMS
NetFlow/sFlow	Traffic flows, bandwidth by app/user	Capacity & security analysis	PRTG, ntopng, SolarWinds
ICMP Ping	Reachability, latency, packet loss	Basic uptime monitoring	Any monitoring tool
Syslog	Device logs, events, errors	Troubleshooting, security	Graylog, ELK, Splunk
SNMP Traps	Real-time alerts from devices	Immediate event notification	PRTG, Zabbix, Nagios

2 What to Monitor & Baseline Metrics

Define what to monitor and establish baselines for normal performance.

You cannot detect anomalies without knowing what normal looks like. Collect baseline data for at least 2 weeks (ideally 4) to establish patterns before setting alert thresholds.

METRIC	BASELINE PERIOD	NORMAL RANGE	WARNING THRESHOLD	
WAN bandwidth utilisation	4 weeks	20–40%	70% sustained 10 min	90% sustained 5 min
Switch CPU utilisation	2 weeks	5–15%	60%	80%
Firewall CPU utilisation	2 weeks	10–30%	70%	85%
Latency (to internet)	2 weeks	5–20ms	50ms	100ms
Packet loss	2 weeks	0–0.1%	0.5%	1%
WiFi client count per AP	4 weeks	Varies	80% of AP capacity	95% of AP capacity
DHCP pool utilisation	2 weeks	30–60%	80%	90%

Alerting Best Practice

Configure alerts at two levels: Warning (investigate when convenient) and Critical (investigate immediately). Avoid alert fatigue by tuning thresholds to your environment. If an alert fires more than once a day without action needed, the threshold is too sensitive.

3 Alerting & Escalation

Configure meaningful alerts and establish clear escalation procedures.

Every critical alert should have a defined response: who is notified, what they should check, and when to escalate. Document this in a runbook alongside your monitoring configuration.

ALERT CATEGORY	NOTIFICATION METHOD	RESPONSE TIME	ESCALATION
Device down (critical)	SMS + email + Teams	5 minutes	Escalate to vendor after 15 min
Interface down	Email + Teams	15 minutes	Check physical, escalate if not resolved in 30 min
High bandwidth	Email	30 minutes	Investigate source, escalate if sustained
Security event	SMS + email	Immediate	Follow incident response plan
Backup failure	Email	1 hour	Investigate and retry, escalate if second failure

4 Capacity Planning & Reporting

Use monitoring data to plan for future capacity and demonstrate network health.

Monthly network reports should include: uptime percentage, average and peak bandwidth utilisation, top bandwidth consumers, alert summary, and recommendations. Use trend analysis to predict when upgrades will be needed — do not wait until you hit capacity.

- → **Bandwidth trends:** If WAN utilisation is growing at 10% per quarter, plan an upgrade 2 quarters before you hit 80%.
- → **WiFi density:** As headcount grows, monitor client counts per AP. Plan additional APs before users experience degradation.
- → **Switch port availability:** Track used vs. available ports. Order additional switches before you run out.
- → **ISP SLA validation:** Use monitoring data to verify your ISP is meeting contracted bandwidth and uptime commitments. This is valuable evidence if you need to claim service credits.

Notes

info@cloudswitched.com
New London House, 6 London St, London EC3R 7LP

Prepared by: ____________________________ Date: ____________________________ Approved by: ____________________________