# Network Performance Monitoring Cheatsheet

A comprehensive cheat sheet covering key aspects of Network Performance Monitoring (NPM), including metrics, tools, and techniques for maintaining optimal network health and performance.

## Key Metrics

### Latency

| | |
|---|---|
| **Definition:** | The time it takes for data to travel from source to destination. |
| **Importance:** | High latency can indicate network congestion, routing issues, or slow hardware. |
| **Measurement:** | Measured in milliseconds (ms) using tools like ping, traceroute, or specialized NPM solutions. |
| **Acceptable Values:** | Varies based on application requirements; real-time applications require very low latency (e.g., < 100ms). |
| **Troubleshooting:** | Investigate network paths, optimize routing, upgrade hardware, or implement QoS. |

### Packet Loss

| | |
|---|---|
| **Definition:** | The percentage of packets that fail to reach their destination. |
| **Importance:** | High packet loss leads to retransmissions, degraded application performance, and poor user experience. |
| **Measurement:** | Monitored using network monitoring tools that track packet transmission and reception rates. |
| **Acceptable Values:** | Ideally, packet loss should be close to 0%; values above 1% often indicate a problem. |
| **Troubleshooting:** | Check for network congestion, faulty hardware (cables, NICs), or misconfigured network devices. |

### Throughput

| | |
|---|---|
| **Definition:** | The actual rate of data transfer across the network, typically measured in bits per second (bps). |
| **Importance:** | Low throughput can bottleneck applications and services, leading to slow performance. |
| **Measurement:** | Measured using tools like iperf, speedtest, or network performance monitoring solutions. |
| **Acceptable Values:** | Should align with the network's bandwidth capacity; significant deviations indicate potential issues. |
| **Troubleshooting:** | Identify bandwidth bottlenecks, optimize network configurations, or upgrade network infrastructure. |

## Tools & Techniques

### Ping

| | |
|---|---|
| **Description:** | A basic utility to test the reachability of a network host. Sends ICMP echo requests and measures round-trip time. |
| **Usage:** | `ping <hostname>` or `ping <IP address>` |
| **Limitations:** | Limited information beyond reachability and latency; can be blocked by firewalls. |

### Traceroute/Tracert

| | |
|---|---|
| **Description:** | Traces the route taken by packets to reach a destination, showing each hop along the way. |
| **Usage:** | `traceroute <hostname>` (Linux/macOS) or `tracert <hostname>` (Windows) |
| **Purpose:** | Identify network bottlenecks or routing issues by examining latency at each hop. |

### Network Monitoring Software

| |
|---|
| Comprehensive tools that provide real-time monitoring of network devices, traffic, and performance metrics. |
| **Examples:** SolarWinds Network Performance Monitor, PRTG Network Monitor, Zabbix, Nagios |
| Features often include alerting, reporting, and historical data analysis. |

### SNMP (Simple Network Management Protocol)

| | |
|---|---|
| **Description:** | A protocol used to collect information from and manage network devices. |
| **Components:** | SNMP Manager (collects data) and SNMP Agent (runs on network devices and provides data). |
| **Uses:** | Monitoring device status, bandwidth utilization, CPU load, and memory usage. |

## Advanced Techniques

### NetFlow/IPFIX

| | |
|---|---|
| **Description:** | Network protocols used to collect IP traffic flow information. NetFlow is Cisco's proprietary protocol, while IPFIX is the standardized version (RFC 7011). |
| **Functionality:** | Capture data about network traffic flows, including source/destination IPs, ports, protocols, and volume of traffic. |
| **Usage:** | Analyze network traffic patterns, identify bandwidth-intensive applications, and detect security threats. |

### sFlow

| | |
|---|---|
| **Description:** | A sampling-based network monitoring protocol. It randomly samples network packets and sends flow data to a collector. |
| **Advantages:** | Lower overhead compared to NetFlow/IPFIX, as it doesn't track every single flow. |
| **Disadvantages:** | Less accurate than NetFlow/IPFIX due to sampling. |

### QoS (Quality of Service) Monitoring

| | |
|---|---|
| **Description:** | Monitoring the effectiveness of QoS policies implemented to prioritize network traffic. |
| **Metrics:** | Track packet loss, latency, and jitter for different traffic classes to ensure QoS policies are working as expected. |
| **Benefits:** | Ensures critical applications receive the necessary bandwidth and priority. |

### Deep Packet Inspection (DPI)

Examining the contents of network packets to identify applications, protocols, and potentially malicious traffic.

**Uses:**

Application identification, intrusion detection, and traffic shaping.

## Best Practices

### Baseline Establishment

Establish a baseline of normal network performance to identify deviations and anomalies.

Collect data during periods of normal network activity to understand typical latency, throughput, and packet loss rates.

### Alerting and Thresholds

| | |
|---|---|
| **Configuration:** | Set up alerts to notify administrators when performance metrics exceed predefined thresholds. |
| **Example:** | Alert if latency exceeds 200ms or packet loss exceeds 1%. |
| **Importance:** | Proactive notification allows for quick identification and resolution of network issues. |

### Regular Reporting

Generate regular reports on network performance to track trends, identify recurring issues, and demonstrate the value of network monitoring efforts.

Include data on latency, throughput, packet loss, and device utilization.

### Capacity Planning

| | |
|---|---|
| **Purpose:** | Use network performance data to forecast future capacity needs and plan for upgrades or expansions. |
| **Considerations:** | Factor in expected growth in network traffic, new applications, and increased user demand. |