[**Network monitoring** is the practice of consistently overseeing a computer network for any failures or deficiencies to ensure continued network performance1](https://www.networkstraining.com/best-open-source-free-network-monitoring-tools/)[2](https://learn.microsoft.com/en-us/training/modules/design-implement-network-monitoring/). It involves collecting and analyzing data from various network components, including routers, switches, firewalls, and endpoints, to identify issues such as device failures, link outages, interface errors, and packet loss.

Here are **five free reference links** where you can learn more about network monitoring:

1. **Nagios Core**: Nagios is a widely used IT management and monitoring software. [Nagios Core, the open-source version, runs natively on Linux and can monitor various hosts and applications, including network services, host resources, and network devices1](https://www.networkstraining.com/best-open-source-free-network-monitoring-tools/). You can find more information and installation details on the Nagios Core website.
2. **Cacti**: Cacti is a network graphing program designed for fast and efficient monitoring. It provides visual representations of network data, including performance metrics, bandwidth usage, and device health. [Cacti is particularly useful for tracking trends and historical data1](https://www.networkstraining.com/best-open-source-free-network-monitoring-tools/). Learn more about Cacti and its features on the Cacti official site.
3. **Azure Monitor**: If you’re interested in cloud-based network monitoring, Azure Monitor is a powerful tool. It allows you to monitor Azure resources, including virtual machines, load balancers, and network traffic. [Microsoft provides free training modules on designing and implementing network monitoring using Azure Monitor](https://www.networkstraining.com/best-open-source-free-network-monitoring-tools/)[2](https://learn.microsoft.com/en-us/training/modules/design-implement-network-monitoring/). Explore these modules on the [Microsoft Learn platform](https://learn.microsoft.com/en-us/training/modules/design-implement-network-monitoring/).
4. **Wireshark**: Wireshark is a popular open-source packet analyzer that helps you capture and analyze network traffic. It’s essential for troubleshooting network issues, understanding protocols, and identifying security threats. [Codecademy offers a tutorial on interacting with Wireshark, creating custom filters, and following network streams](https://www.networkstraining.com/best-open-source-free-network-monitoring-tools/)[3](https://www.codecademy.com/article/tutorial-network-monitoring). Check out the [Wireshark tutorial](https://www.codecademy.com/article/tutorial-network-monitoring) to get started.
5. **SNMP (Simple Network Management Protocol)**: SNMP is a fundamental protocol for network monitoring. It allows you to manage and monitor network devices, retrieve performance data, and detect faults. [DigitalOcean provides an informative tutorial series on SNMP, covering its introduction, installation, configuration, and usage](https://www.networkstraining.com/best-open-source-free-network-monitoring-tools/)[4](https://www.digitalocean.com/community/tutorials/an-introduction-to-snmp-simple-network-management-protocol). Dive into the [SNMP tutorial](https://www.digitalocean.com/community/tutorials/an-introduction-to-snmp-simple-network-management-protocol) to learn more.

Remember that network monitoring is crucial for maintaining a healthy and efficient network, whether you’re managing on-premises infrastructure or cloud-based resources. These free resources will help you gain valuable insights into network performance and troubleshoot issues effectively.