

# Intro to Network Baselines

Reading

20 minutes

✓ Status

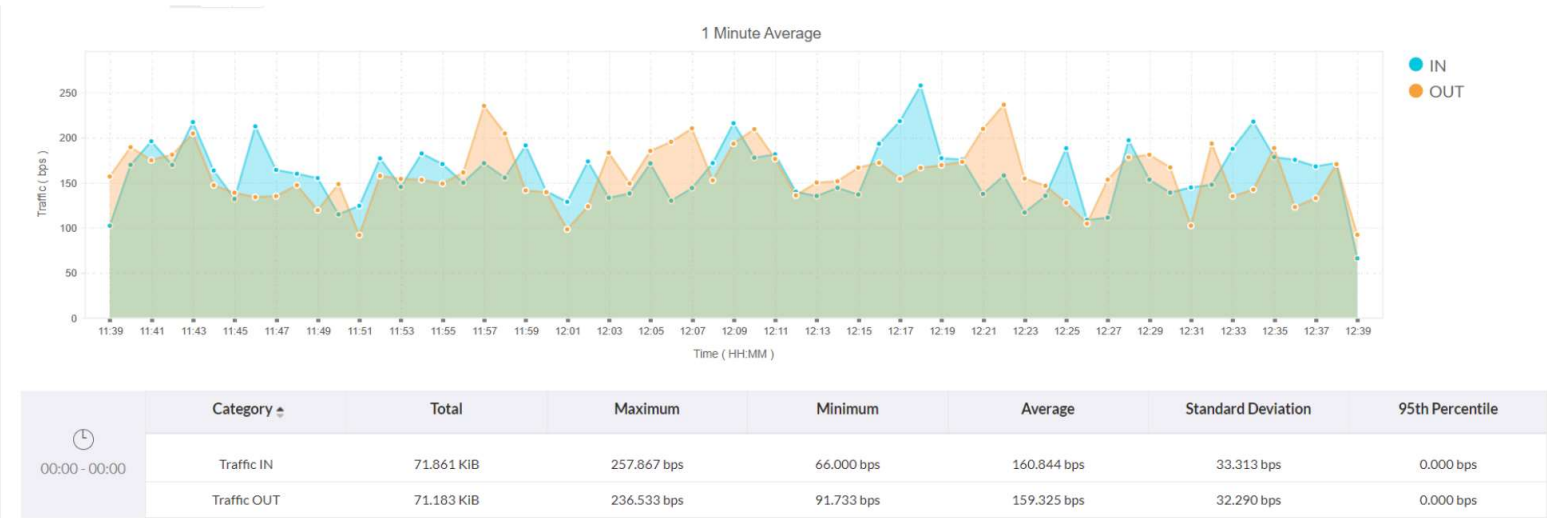
Incomplete

## Introduction

Network administrators face difficulty when the networks they manage start behaving strangely. In some cases, the effects can be seen in slow transmission times, dropped connections and corrupted data.

Establishing a **network baseline** is therefore extremely useful in helping to figure out what is considered "normal" for a given network. When this is established, you can more easily recognize when things aren't normal, which makes troubleshooting much more manageable.

In this reading, you will understand how to establish a network baseline, recognize irregularities, and determine what kind of threats they may pose.



Source: <https://www.manageengine.com/products/netflow/real-time-network-traffic-monitor.html>

# Analysis

Now let's do a quick breakdown of common of the common fields you will find in a network traffic chart.

**bps:** The unit of measurement on the left side is bps and this stands for bit per second. This is not to be confused with byte per second, which is Bps. There are 8 bits in a byte, therefore bps is much smaller than Bps.

**In/Ingress:** This refers to how much traffic is coming into the network.

**Out/Egress:** This refers to how much traffic is leaving the network.

**Average, Standard Deviation, Minimum and Maximum:** These statistics are extremely important when it comes to establishing a baseline and creating alerts on what will be considered "abnormal" network traffic.

## Reading

All networks have a typical traffic pattern throughout the average workday. Depending on the organization's core hours of operation and volume of traffic on the network, traffic patterns may be low outside the core hours of operation and high during working hours.

In Cyber Security, network baselines refer to the normal or expected behavior of a network. This includes information about the devices, protocols, and traffic that are typically present on the network, as well as the patterns of usage and communication.

Network baselines can be used to detect and respond to security incidents and anomalies by allowing security teams to identify abnormal behavior that deviates from the established baseline.

According to Cisco, the objective of a baseline is to:

- Determine the current status of network devices.
- Compare that status to standard performance guidelines.
- Set thresholds to alert you when the status exceeds those guidelines.

The baseline takes snapshots of the network when you know it's normal, so you have something to use as a reference point.

## Establishing the Network Baseline - Process

A network baseline is established by recording information about the devices and traffic that are measured during known normal operation. Comprehensive data about the typical usage and status of the network provides the ability to compare future information against what is known to be the norm to highlight inconsistencies for investigation. Data should be collected on various aspects of network traffic, such as:

- List of devices in use on the network and their IP addresses and ports
- List of protocols and services in use
- Amount and timing of traffic
- Patterns of communication and usage
- Records of user and device authentication


Once it is clearly established what your network looks like under normal operation, it becomes easier to detect and respond to potential security incidents. This is done by monitoring network activity in real time and comparing current activity to the recorded baseline to identify significant departures from usual operation. For example, changes in the IP address, port, or

protocols used by a device that are not part of the established baseline, could indicate a potential security incident.

# References

- 1. [Cacti](#)

✓ Mark Completed




Previous

Network Monitoring with Wireshark

Next

Visualizing What's Happening Lab - Windows Logging



## How well did this activity help you to understand the content?

Let us know how we're doing










# W01D5

Fri Jun 28

> Lectures (1)

✓ Work (11)

7 hrs

-  [Traffic Monitoring](#)
-  [Network Monitoring with Wireshark](#)
-  [Intro to Network Baselines](#)
-  [Visualizing What's Happening Lab - Windows Logging](#)
-  [Group Share and Feedback](#)
-  [Recap Terminal Commands: Windows and Linux](#)
-  [Understand the environment and Wireshark](#)
-  [Check the Commands](#)
-  [Tech Interviews](#)

 [Tls: How it Works](#)



 [Tls: What to Expect](#)



> **Other** (1)

---

[W01D5 Schedule »](#)

Powered by Lighthouse Labs.