



How to Build a Reliable Source of Truth

Most organizations don't have a single source of truth; they have several. Some data lives in your monitoring tool, while other data lives in your CMDB, your IPAM, and maybe even an Excel sheet or two. Each "**source of truth**" only shows you a fragment of your network, leaving you to put the pieces together yourself. But your SoT shouldn't be a document or a spreadsheet you maintain; it should be a continuous feedback loop based on your network's actual behavior. IP Fabric makes it easy to gather a complete and contextualized view of your actual network state, so you can feed it into your chosen source of truth for continuous validation. Read on to see how this works in 4 steps.

Step 1: Run a Snapshot

IP Fabric kicks off the discovery process by using CLI commands and API calls to communicate with vendors, pinpointing all their devices and known neighbors until 100% of them are found. From there, the platform also maps out each device's connections and configurations, automatically checking them against your business intent. You can choose to create your own custom checks or deploy IP Fabric's series of 160+ built-in checks, which are based on standards for leading security and regulatory frameworks. The results of your snapshot and intent checks are then presented in IP Fabric's normalized, user-friendly GUI.

Step 2: Push the Snapshot Data via API

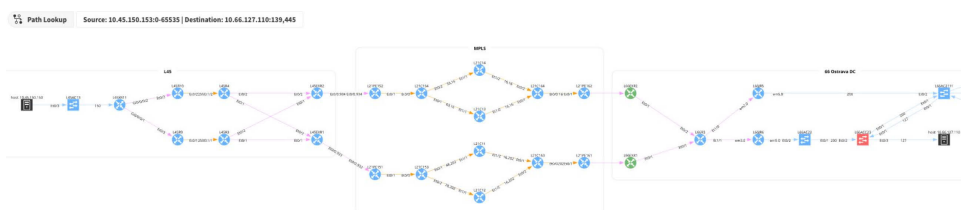
IP Fabric's NetBox plugin that automatically pushes IP Fabric's network data to NetBox. That data can easily be queried either via API or NetBox's GUI.

Step 3: Scan for Inconsistencies

IP Fabric's plugin automatically creates a new branch in NetBox, and highlights any differences between this newest IP Fabric snapshot and your NetBox source of truth. Maybe you see an IP address that's configured a certain way in NetBox, but it's been manually changed on a device. This creates a conflict of information, where your source of truth tells you one thing, but your network is telling you another. Maybe that IP address was changed for a reason, or maybe it was an accident. In this case, a human or AI agent can step in to correct the situation—and with the depth of insights from IP Fabric, they'll know exactly where to start their investigation.

Step 4: Remediate Configuration Drift

Now you know exactly what's drifted. But before you remediate the issue, you can run an end-to-end path lookup in IP Fabric to simulate the effect the change will have on your network. You can also run another snapshot after implementing the change, to ensure it had the intended effect. From there, IP Fabric will automatically sync with your NetBox source of truth.



Learn more about IP Fabric's snapshots in our [self-guided demo](#).

Get in Touch.

Visit IP Fabric's website for demos, customer stories, and more.

