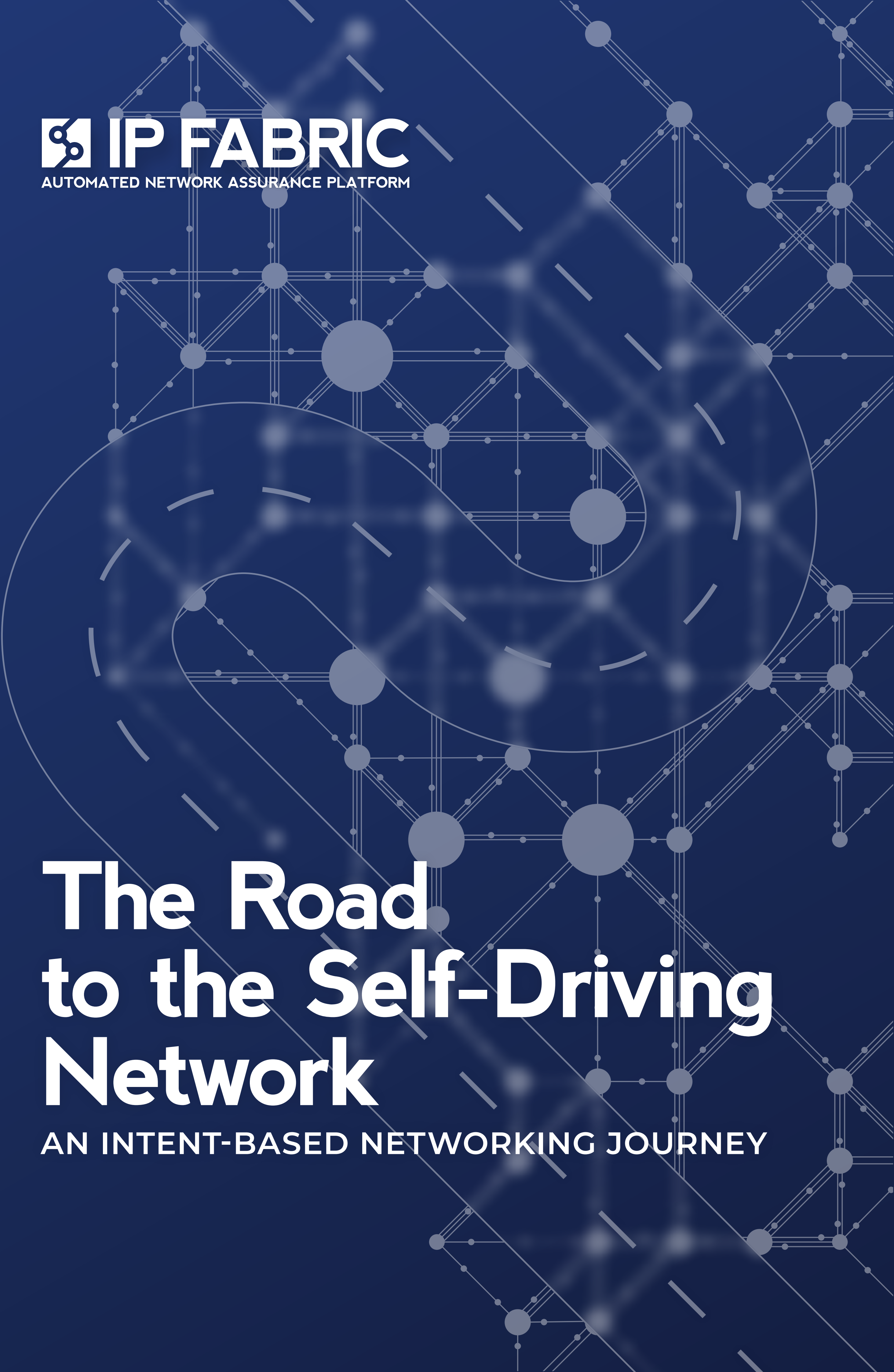
IP FABRIC
AUTOMATED NETWORK ASSURANCE PLATFORM



The Road to the Self-Driving Network

AN INTENT-BASED NETWORKING JOURNEY

1. Introduction

1.1 Overview

Current operating approaches for the network are based on last-century business models. The Business cares little for routing protocols and topologies, VLANs and IP addressing, and much more about consuming connectivity for the delivery of applications and services critical to delivery to customers. As IT becomes more of a commodity, so we have to look at a more service-focused approach to our network operations. In this white paper, we look to answer the fundamental question “Is there a better way to operate your network?”

1.2 Executive Summary

We will first examine how the IT operations narrative is need of a change, to move from talk of infrastructure element management to that of consuming IT to create business outcomes. This will be illustrated using experience and practice from Cloud adoption and framed using Gartner’s “Run-Grow-Transform” model.

The goal of the Self-Driving Network is then set out, showing how operational practices similar to those used in Cloud environments can be used to achieve the ultimate goal of a network providing agility and flexibility with the lowest amount of friction possible.

We then lay out the roadmap as we see it, through the stages of adoption of the management techniques necessary to achieve the elements of the Self-Driving Network. We will focus on the management paradigm known as “Intent-Based Networking” (IBN) - at its approach, adoption and benefits.

We conclude by showing how IP Fabric’s automated Network Assurance platform helps organizations at all stages along that journey.

2. Background

2.1 The Impact of Cloud

Traditionally, organisations have built and maintained their own data centre infrastructures to host corporate applications. Space, power, cooling and manpower costs of maintaining those data centres have been an accepted cost of having the control to deliver service to The Business.

The private offerings of the Public Cloud providers like AWS and Azure have had a huge impact on enterprise IT for a number of reasons, that can be summarised thus:

- Rental of compute, storage and other IT services minimizes capital outlay and infrastructure lifecycle costs
- Provision of infrastructure on-demand in order to develop new solutions, means that there is no longer a need for costly upgrades to DC infrastructure (in terms of finances, resource or time)
- Scale and regionalised provision is available as and when required
- Simple low-friction consumption using APIs to automate provision and configuration of service.

The combination effect is to allow IT departments to create and deliver application services in a much more agile, dynamic manner without the lead times and large capital outlays that a traditional approach would have needed.

2.2 Run-Grow-Transform

In recent years, Gartner have created the “Run-Grow-Transform” model as a simplification to help communicate and classify services for Service Management.

RUN

GROW

TRANSFORM

MANDATE

Maintain current business capabilities

Operational Roles

MANDATE

Expand existing business capabilities

Enhancing Roles

MANDATE

Drive new business capabilities

Innovation Roles

© Gartner 2017

“**Run**” services contribute to the continuing operation of the business – “BAU” or “Keeping the lights on”. The idea is to maintain business capabilities, whilst reducing cost, improving price:performance ratios, and reducing operational risk.

“**Grow**” represents where we expand existing capabilities to deliver measurable business improvements. For example, improve market share, reduce the sales cycle time, or speed time to market for a product.

“**Transform**” activities are used to drive new capabilities in the business, often representing strategic gambles on completely new ways of doing business through the development of brand new capabilities.

Typically, these areas in midsize enterprises equates to roughly a 7/2/1 ratio for Run/Grow/Transform. The goal of using this model to plan for IT spending is to reduce costs in the Run activities to be able to increase the proportion of activity in the Grow and Transform activities.

The adoption of Cloud in the enterprise has allowed exactly this shift towards growth and transformation activities. In this paper we’ll use this model to highlight the service improvements that can be made along the journey to the self-driving network.

2.3 The Self-Driving Network

As we have seen, the benefits of Cloud extend way beyond simple cost – and other areas of IT infrastructure would clearly benefit from similar process changes. Challenges around the management of connectivity are long overdue some attention. Consider that the provision of new services often requires new:

- Physical network infrastructure to support connection to servers and storage
- VLAN and Address allocation
- IP Routing changes
- Firewall and security ACL updates

across all of the domains in the network (wireless, wired, WAN, and data center) to allow access. A "Cloud-like" approach would allow provision of all the elements to be virtualised and automated: the act of service provision would be abstracted to a workflow of templated changes in each network domain to support that service. Ultimately then, capacity management becomes a simple understanding of physical infrastructure constraints and are not influenced by configuration etc.

Observability software would then be used to gather data about the behaviour of the network to:

- Monitor the level of service being provided
- Detect drift from the required service level and act on it, modifying configuration or generating alerts to the operational team
- Provide detailed operational data for the network engineering teams to:
  - Manage infrastructure capacity
  - Deep dive into troubleshooting if required, and
  - Produce summary reports for the service management folk.

The Self-Driving Network is not – at the time of writing at least – a reality but there is a very clear journey mapped out which allows us to take huge leaps in that direction.

2.4 The Starting Point

Since the first local area networks were established, management of connectivity has been managed on a device-by-device basis. Initially, the medium itself was the common element, but as complexity has grown so have the number of devices and the requirement for common config and policy among them to deliver a standard service.

As a result, management and maintenance of the network has been about having access to and an understanding of the config of the individual devices, their interfaces and relationships as they work together to provide service. More often than not, this has meant having a team of folks with CLI access to those devices, experience with the equipment, an understanding of the specific environment and access to documentation to back up their knowledge and experience.

3. The Road

Now that we understand where we start, and where our destination is, we can take a look at the road from traditional network management approaches and understand the stages and the stops along the way.

Network Automation

What? Standardize and template configuration, centralised deployment, collection of network data

How? Scripted command line interface or API requests and low-code systems

Benefits? Speed and consistency of individual operations especially at scale

Service Orchestration

What? Combination of automation tasks across domains and vendors into workflows, incorporating approval, testing and backout

How? Open-source tooling (eg Ansible) or commercial tools (eg Cisco NSO)

Benefits? Infrastructure as Code: services are templated and instantiated across the network based on version-controlled input data especially at scale

Intent-Based Networking

What? Standards-based approach to combine automation/orchestration with "Assurance" to validate behaviour and provide closed-loop feedback

How? For detail, see callout *

Benefits? Introduce autonomy in service provision and assurance: express intent in terms of service abstractions

4. IP Fabric on the Journey

IP Fabric is a Network Assurance tool – its powerful multi-vendor, multi-domain discovery and network modelling capability shines a light into the dark corners of your network, revealing every device and how it contributes to the behaviour of your network. As a result, it has uses at all stages in the journey.

NetworkAutomation

IP Fabric replaces manual documentation practices, visualizes complex network configuration and behavior, assists with identifying issues with devices impacting specific services and carries out compliance checks for configuration standards and regulatory audits.

As you prepare for network automation, IP Fabric ensures that a comprehensive and up-to-date network information is always available, providing all the data you need to validate your Sources of Truth.

Service Orchestration

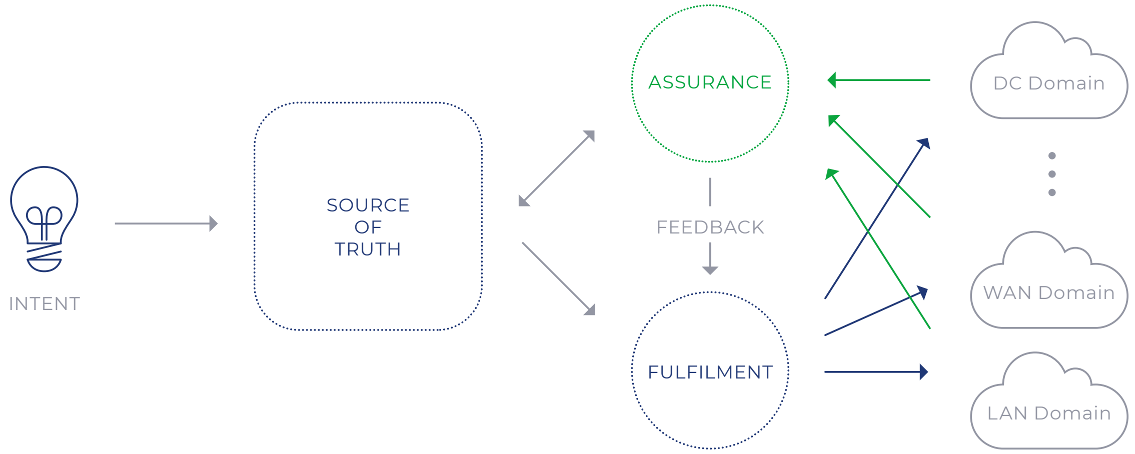
IP Fabric's automated modelling of network data into network snapshots gives the network engineer all the network data they need to build logic for their own automation and integration projects, and all accessible over API.

Through its intent validation rules, IP Fabric can be used to verify that changes have been completed successfully. These checks can then be incorporated into orchestration workflows to provide checks and balances.

Intent-Based Networking

IP Fabric also incorporates a webhook trigger capability which can be used to notify external systems that activity needs to be started on the back of completion of intent verification checks or new snapshots. In this way, drift from network intent can be detected and activities triggered to fix that drift.

Intent-Based Networking (IBN) is a network management paradigm, the elements of which are described in an IRTF draft [iii]. It consists of three main functions:



Source of Truth (SoT) - where business intent is encoded in network terms - this could be a DCIM, IPAM, CMDB; it could be a set of YAML files in a git repository; it could be something as simple as an Excel spreadsheet; or a combination of them. The key is that there is a definitive source for each piece of intended network configuration.

Fulfilment - where intent expressed in the SoT is rendered into network configuration. It consists of automation tasks and orchestration workflows that deliver network service in a consumable fashion. If you require changes to the network at large to support your service, you simply update the SoT and trigger the workflows.

Consider the example of delivering a new application. You might require logical network separation for users and the application workloads located in a public cloud environment. You might create an abstraction of a “slice” of network to be allocated a specific IP address range and present that to the consumer. The detailed configuration deployed by the workflow might be VRFs configured in DC and campus, stitched together over MPLS, with a VPC in AWS connected over BGP into the DC VRF. That VRF might then be routed into the wider network via a firewall. To deliver that, we would need configuration templates and automation tasks for DC Fabric, campus network, WAN, firewalls and AWS VPCs.

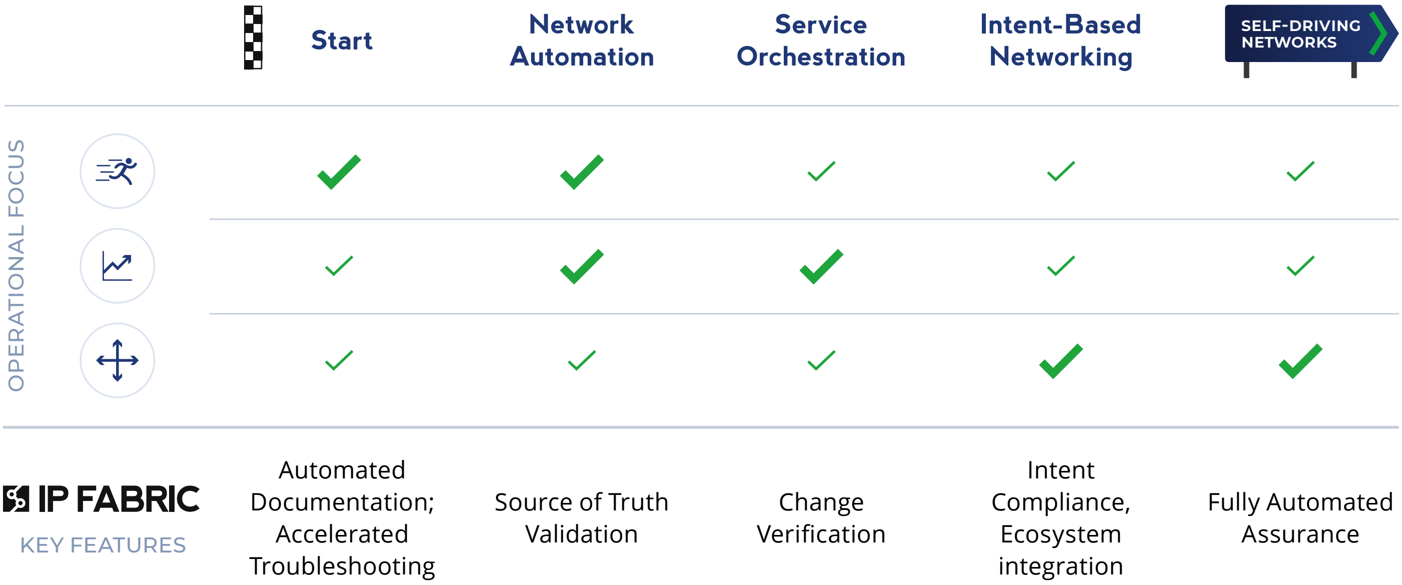
Assurance - Where the network is validated as behaving as we intended and where we introduce a mechanism to trigger the Fulfilment function to fix drift from that intent.

Consider that traditional network monitoring collects data from individual network devices with no implied meaning or context. To validate network behavior, we need to identify the metadata – the relationships between those data points and other background information. This metadata may be inferred using AI/ML techniques or it may simply be a software implementation of a combination of real-world network rules, understanding, and experience.

Once you have the context in the metadata, it is possible to build rules to express desired state – used to update the Source of Truth. Then deriving metadata from collected data points from the live network allows comparison with that intent. This is Network Assurance.

5. Summary

We can see then that following the stages of the journey towards a Self-Driving Network substantively improve the quality of your IT operations, thus allowing you to dedicate progressively more energy and resource to more transformative activity. Working towards the goal of a largely autonomic network operations ecosystem enables your team to focus on your business transformation objectives. And using IP Fabric as Network Assurance supports you at every step of that journey:



	Start	Network Automation	Service Orchestration	Intent-Based Networking	SELF-DRIVING NETWORKS
OPERATIONAL FOCUS	✔	✔	✓	✓	✓
	✓	✔	✔	✓	✓
	✓	✓	✓	✔	✔
IP FABRIC KEY FEATURES	Automated Documentation; Accelerated Troubleshooting	Source of Truth Validation	Change Verification	Intent Compliance, Ecosystem integration	Fully Automated Assurance

We have demonstrated that Cloud service principles bring benefit to IT operations across all pillars. Using similar principles, Intent-Based Networking helps bring the promise of network autonomy that much closer to reality. Thanks to the automated Fulfilment of intent – expressed in the Source of Truth – and through Network Assurance – the validation that the network is performing as you intend and the measurement of drift from that intent – an IBN approach sets you on the right path. And by bringing Network Assurance to your environment today, IP Fabric provides the immediate benefits of holistic visibility of your network, whilst guiding you towards the ultimate destination of the self-driving network.

[i] Simplify Service Portfolio Prioritization and Resource Planning Using Run-Grow-Transform Categorization
by **Deb Curtis, Gartner**

[ii] Top 3 Drivers of Cloud Adoption in Midsize Enterprises
by **Mike Cisek**, **Paul Furtado**

[iii] Intent-Based Networking - Concepts and Definitions
by **Alexander Clemm**, **Laurent Ciavaglia**, **Lisandro Granville**, **Jeff Tantsura**

IP FABRIC

AUTOMATED NETWORK ASSURANCE PLATFORM

CONTACT US

www.ipfabric.io

sales@ipfabric.io

FOLLOW IP FABRIC ON SOCIAL MEDIA