Network Automation Trends and Strategy

Contents

How is the network automation market evolving? What is a network automation strategy? Do you need a network automation strategy? Get answers for all these questions and more.

Network automation has grown throughout the years in enterprise and service provider IT organizations, and its growth is predicted to continue to increase. According to a recent market research published by Meticulous Research, the network automation market is expected to grow at a CAGR of 22.8% from 2021 to 2028[1]. This growth is mainly due to increasing network complexity originated by businesses demanding higher agility and higher reliability. All this growth has created the need for companies to develop network automation strategies.

This paper does not aim to be a technical deep-dive on network automation, rather it discusses the need for a network automation strategy. It starts with a description of what network automation is, followed by key use cases. Furthermore, it emphasizes the benefits that network automation brings to IT organizations.

A network automation strategy generally involves: (1) developing a vision, (2) settings goals, objectives and strategies, (3) determining tactics to achieve the goals, and (4) mobilizing resources to execute the tactics. We will show you a simple, concise and easy to consume document outline for your network automation strategy and help you answer these three questions:

- Where are we?
- Where do we want to go?
- How do we get there?

What is Network Automation?

Network automation refers to the process of automating deployment, configuration, testing/validation and operation of network devices, that can be physical (routers, switches, access points, firewalls, etc) or virtual (public cloud networking, virtual machines, containers, virtual network functions, etc). Network automation can be applied to a broad range of enterprise and service provider network services, with relevant examples listed below.

Enterprise automation:

- Datacenter networks including access ports, port-channels, routing, quality of service, firewalls & load balancer policies, hypervisors, virtual machines and containers among other.
- Public Cloud tenants, virtual networks, subnets, security groups, load balancers, compute services, storage services and serverless functions.
- Campus and OT (Operational Technology) networks including wired and wireless access, network access control, macro-segmentation and micro-segmentation.
- Wide Area Network (WAN) customer premises equipment, overlay virtual private networks, application aware routing, quality of service and routing policies.

[1] Network Automation Market by Component, Deployment Mode, Industry Size, Networking Type (Physical Networking, Virtual Networking, Hybrid Networking), Industry Vertical (CSPs, Data Centers, and Enterprises)- Global Forecast to 2028

Service Provider automation:

- Residential ADSL and Fiber To The Home (FTTH).
- Small and Midsize Business (SMB) and Enterprise Virtual Private Network (VPN) access, security and routing policies.
- Virtual Network Functions (VNF) including routers, firewalls, load balancers and virtual Evolved Packet Core (vEPC) components.
- Enterprise to public cloud VPN connectivity including cloud edge routers.

Network automation applies to the full service lifecycle including day 0 network onboarding, day 1 configuration and day 2 operation and optimization. The automation use cases in each stage of the lifecycle will be different, examples are:

- Day 0: Zero touch network device deployment (plug&play), sometimes referred to as onboarding. Deployment of device security certificates. Virtual Machine deployment and attachment to network.
- Day 1: Network configuration and management using device templates defined by network engineering teams or prescribed by a network controller. Network segmentation configuration based on traffic behavior analytics.
- Day 2: Network configurations updates/changes. Identify and fix security vulnerabilities based on AI/ML. Capacity planning. Hardware and software lifecycle management.

Benefits of Network Automation

Today, up to 95% of the network changes are performed manually[2]. This often leads to inconsistent networks which are the result of configurations being built by different engineers, poorly documented operations runbooks, or human errors. These configuration inconsistencies often result in network downtime, decreased service velocity and increased operational costs.

Network automation can address the above shortcomings of manual interventions by offering:

- **Faster response to new requirements:** By increasing the level of automation in networks, IT teams can focus their efforts on delivering value to the business. Automation enables lower cost of operations, while improving service levels and faster response to new service/application requirements and deployments.
- **Higher reliability:** With the replacement of manual by automated tasks, network devices are configured more consistently and are less prone to human errors. With automation, network availability improves and we have more reliable networks.
- **Reduced operational expenses:** Automation helps reduce operational expenditure, it eliminates manual, time-consuming and repetitive tasks. Policy-driven provisioning and guided remediation increase network uptime and reduce time spent managing network operations.
- **Standardized configurations:** In order to achieve network automation efficiency, network configuration templates must be standardized first. Having design blueprints with standardized templates and well-defined service logic eliminates ambiguity to software engineers writing the automation software.

[2] https://www.cisco.com/c/en/us/solutions/automation/network-automation.html#~why-automate

- **Faster network changes:** Time to apply network changes is reduced when the tasks are executed and validated by an automation tool instead of a network operator.
- **Facilitate offsite IT teams:** Network automation controllers are optimized for remote access, they provide dashboard with clean and organized workflows that makes remote management easy.

Furthermore higher levels of automation, such as closed-loop automation systems and self-driving networks, provide organizations with all the previous benefits and more:

- **Augmented intelligence:** Constantly and excessively evaluating the collected data for you. Finding the outliers and letting you know in ways no human can.
- **Dynamic optimization/remediation:** Constantly ensuring the desired state of the network is maintained. Using machine learning to choose the best way to implement the desired state and take automated corrective action to maintain that state.
- **Simplified troubleshooting:** Remediation activities are simplified when they are fully or partially automated. Furthermore, automation enables AIOps by automatically collecting and parsing data.
- **Better network insights:** Many network automation tools, specifically network controllers, increase visibility on your infrastructure and provide network insights. Network operations teams can take proactive actions to correct network issues before they impact the business. AI/ML network insights reduce time spent managing network operations and improve user experience.
- **Enhanced security:** Security automations tools improve ongoing understanding of application flows to detect potential threats. Reduce attack surface with automated micro-segmentation through AI/ML based customized analysis and recommendations. Automatic detection and enforcement of compliance. Better tracking of security posture.

Network Automation tools

Today, there are innumerous automation tools on the market, some of the most popular ones are: Terraform, Ansible, Chef, Kibana, Grafana, Splunk and Python. These are tools that organizations use to build their own automation solutions. Consider that most of the previously named tools are not fixed tools, but rather modular ones that can be tailored and adapted to achieve your network automation goals.

Furthermore, there are also network controllers. In the last few years, we have seen a proliferation of software-defined networking solutions, which are architectures that separate the data plane from the control plane. Software-Defined WAN (SD-WAN) is an example of that. In a software-defined network the intelligence is centralized in a network controller which performs multiple functions including the automation of the network. Other examples are Software-Defined campus LAN (SD-LAN) and Software-Defined Data Center (SD-DC).

Automation also refers to the use of AIOps - artificial intelligence for IT operations - that collect and contextualize network operational data real-time, enabling closed-loop automation mechanisms which apply network changes to remediate problems before they have an impact to the service, optimizing end user experience.

As enterprise organizations progress in the adoption of network automation in the different networking domains (IoT, Campus, WAN, Data Center, Colo, Public Cloud), multidomain service orchestration will be vital to effectively manage the end-to-end service delivery and operations. Service orchestration platforms will leverage network controllers (e.g. SD-WAN, SD-LAN, SD-DC) as well as accommodate non-controller based networks automation (e.g. Ansible, Terraform, direct to device) to address the network lifecycle from plan/design to operate, to software conformance, and finally to audit/compliance.

Some example of enterprise use cases delivered by multidomain service orchestrators include day0/1 deployments, software conformance, configuration audit and compliance, inter-domain connectivity, security policies, end-to-end Quality of Service (QoS), backup/restore and Infrastructure as Code (IaC). Use cases may address individual domains such as campus, or multiple domains such as SASE (SD-WAN and Cloud Security). In addition to streamlining the automation and orchestration of infrastructure across multiple and disparate domains, multidomain service orchestrators integrate northbound with AIOps, ITSM, ITOM and ITAM, enabling end-to-end IT services management and operation.

Complementary to network automation is processes and workflows automation. Typically, uses cases that automate end-to-end business outcomes require both device configuration/automation and process automation. Examples of processes automation are human approvals tasks, fetching configuration parameters from external databases, gathering user input for configuration parameters or manual interventions to address errors. Process automation and network automation tools need to be integrated.

Figure 1 describes a sample multidomain enterprise architecture encompassing service orchestration northbound, southbound, east-west and process automation.

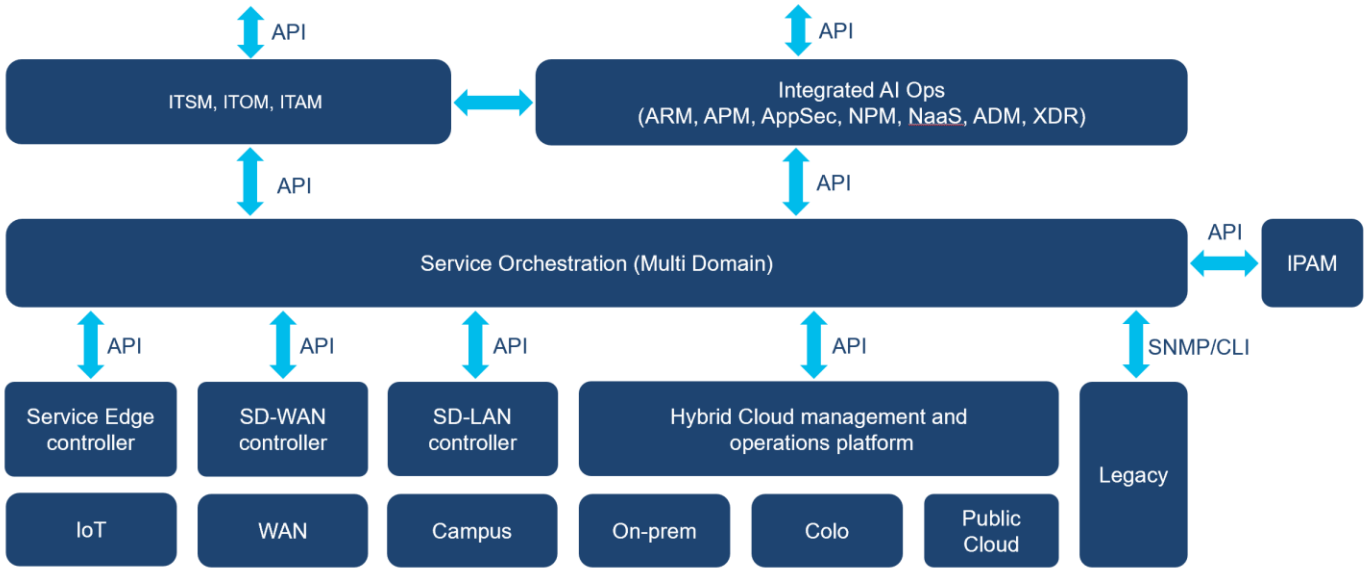

Figure 1.
Enterprise multidomain architecture

Because of the broad spectrum of network automation use cases, there is no single tool that can address all of them, but a landscape of open-source and vendor tools that address the different needs, which complement and often also overlap with each other.

You should favor the tools that fulfil your desired business outcomes. It is worth noting that the higher level of automation and orchestration your network is in, the more benefits you are able to harness.

Network Automation maturity

We like to classify the maturity level of an organization's network automation according to one of the following categories:

(1) **Manual device configuration.** The network still relies on manual provisioning and configuration, device-by-device via CLI or SNMP.

(2) **Basic configuration automation.** There are some basic image and device configuration automation and advanced service provisioning.

(3) **Controller-based per-domain automated provisioning.** There has been great progress with controller-based automation in one or more network domains. This allows secure, scalable and consistent day 0 and day 1 provisioning for specific device groups.

(4) **Controller-based, network-wide automated provisioning.** There is already controller-based automation across the network for policy-based day 0 and day 1 provisioning and configuration, delivered consistently from private and/or trusted public cloud. A service orchestration tool has been deployed to enable end-to-end orchestration.

(5) **Automated provisioning of devices in a self-organized, self-diagnosing and dynamically updated network.** The network has advanced self-optimization capabilities, with the introduction of Day 0, Day 1 and Day 2 automation based on business policy and network-based machine learning, powered by AIOps technologies.

You should aim to achieve a higher level of automation, for example level 4 or 5, as these will carry more benefits to your organization and align to the current industry trends as shown in the following sections.

Network Automation market trends

Today, businesses are asking IT for more agile changes, higher availability for the services and reduced operational costs. These asks, together with the fact that networks are growing in size and complexity, are increasing the role network automation plays on IT organizations.

IT Automation and Orchestration Trends in enterprise

As described in Gartner's Market Guide for Network Automation and Orchestration Tools, network automation and orchestration tools are moving from niche functions used by individual employees within Infrastructure and Operations (I&O) to providing robust solutions that allow network operations to be increasingly automated[3]. As an example, we can look at the enterprise networking domain, where there is an increasing transformation from environments where engineers developed scripts or used automation tools to optimize their own work (for example automation of repetitive tasks like the creation of a VLAN in hundreds of campus switches) to controller based intent-based networking solutions for Campus, Datacenter and WAN that automatically detect faulty network behaviors such as high CPU-usage and apply remediation configurations. But, is this enough?

Gartner uses the term **Hyperautomation**, defined as a business-driven, disciplined approach that organizations use to rapidly identify, vet and automate as many business and IT processes as possible[4], this includes network automation.

[3] https://www.gartner.com/en/documents/3990134

[4] https://www.gartner.com/en/information-technology/glossary/hyperautomation

According to Gartner Top Strategic Tech Trends for 2021, hyperautomation has been trending at an unrelenting pace over the past few years, mainly because of the pent-up demand for operationally resilient business processes. As business executives demand a path to digital operational excellence, there is often a backlog of requests from business stakeholders for automation using one or more technologies. Hyperautomation is irreversible and inevitable. Everything that can be automated will be automated. Competitive pressures for efficiency, efficacy and business agility are forcing organizations to address it. Organizations that resist the pressures will struggle to remain competitive or to differentiate[5].

Achieving a higher level of automation, 4 or 5 in the maturity scale described earlier (end-to-end service orchestration, AIOps, closed-loop automation), will put you in the path to digital operational excellence and enable you to address in an agile way requests from business stakeholders.

IT Automation and Orchestration Predictions and Recommendations

Since Gartner introduced the Hyperautomation concept in 2020, they have made a few predictions in this domain:

- By 2024, organizations will lower operational costs by 30% by combining Hyperautomation technologies with redesigned operational processes.
- By 2024, 80% of Hyperautomation offerings will have limited industry-specific depth mandating additional investment for Intellectual Property (IP), curated data, architecture, integration and development.
- By 2024, more than 70% of the large global enterprises will have over 70 concurrent Hyperautomation initiatives mandating governance or facing significant instability.

The above are broad automation related predictions which network automation is a subset of. Gartner has also published network automation specific predictions in Market Guide for Network Automation and Orchestration Tools, according to this document:

- By 2023, 15% of on-premises data center networking activities will be integrated into a continuous integration/continuous (CI/CD) delivery pipeline, an increase of more than 15 times from early 2020.
- By 2023, 60% of data center networking configuration activities will be automated, up from 30% in early 2020.
- By 2023, 40% of product and platform teams will use AIOps for automated change risk analysis in DevOps pipelines, reducing unplanned downtime by 20%.
- By 2025, 50% of enterprises will have devised Artificial Intelligence (AI) orchestration platforms to operationalize AI, up from fewer than 10% in 2020.

[5] https://www.gartner.com/en/information-technology/trends/top-strategic-technology-trends-hyperautomation-gb-pd

Likewise, an IDC's survey highlights that over 90% of enterprises claim that they pursue fully autonomous networks for service agility, flexibility, and cost-effectiveness[6]. IDC describes it as, Level 5: The network is fully automated and self-driving throughout the life cycle, capable of applying policy and troubleshooting and remediating events. Operators trust that the network can function and adapt to almost every known scenario. Furthermore, IDC mentions organizations at level 4 or level 5 deploy nearly twice as much digital capabilities (for example BYOD, IoT applications, high definition video, location aware applications) than organizations at level 2[7].

Gartner recommendations to Infrastructure and Operations (I&O) leaders responsible for managing network infrastructure include[8]:

- Deliver improved network agility to support organizational requirements by focusing on network automation and orchestration and measuring the relevant business outcomes.
- Accelerate their automation/orchestration transition by identifying the necessary orchestration-related culture issues and skills missing from their organization and choosing vendors that will help fill those gaps, as well as adjusting training and hiring patterns.
- Accelerate digital and cloud initiatives by treating network automation and orchestration as a strategic priority and investing in personnel and tooling accordingly.
- Mature automation and orchestration initiatives by implementing complementary tools and managing them with a view toward enabling AIOps leading to improved digital activities.

Likewise, IDC recommends adoption of higher levels of network automation to increase agility, enable innovation, enhance customer experience, and improve productivity and product growth. For example an increase from level 3 to 4 – as per above-mentioned maturity levels – is predicted to reduce time to market of a new product in 40% and improve the performance of critical applications by 22%[9].

As a summary, we can clearly see the intent to evolve into closed-loop and fully autonomous self-driving network solutions due to the evolving business requirements and benefits. Organizations are increasingly adopting network automation and that trend seems to continue.

[6] https://e.huawei.com/en/material/networking/data-center-network/db203d3fd662498d9a4a7375dfdd7664

[7] https://www.cisco.com/go/dnaadvisor

[8] https://www.gartner.com/en/documents/3990134/market-guide-for-network-automation-and-orchestration-to

[9] https://ibn-assessment.cisco.com/go/cisco/ibn/?lang=en-us

What is a Network Automation Strategy?

Your organization most likely has many strategies in place, for example a marketing strategy or a financial strategy. Network automation should not be different, there is an increasing need for organizations to have a network automation strategy in place because of its massive adoption across the industry and the need for IT teams to follow a clear direction. Although network automation has plenty of benefits, blind adoption can lead to tool sprawl, reduced return of investment, and even increased complexity in network management and operations.

A strategy can be described as a representation of where an organization is, where they want to go, and the path to get there[10]. Furthermore, a network automation strategy should be supported by five pillars as shown in Figure 2:

- **Business alignment** – It should support and enable the business.
- **Technology adoption** – It should reflect what technologies are in use and which will be adopted.
- **Operating model** – It should reflect owners and maintainers for projects and tools.
- **Roadmap** – It should document what is ahead in terms of projects, decommissions and tools.
- **Skills** – It should display what skills are required or will need to be acquired.

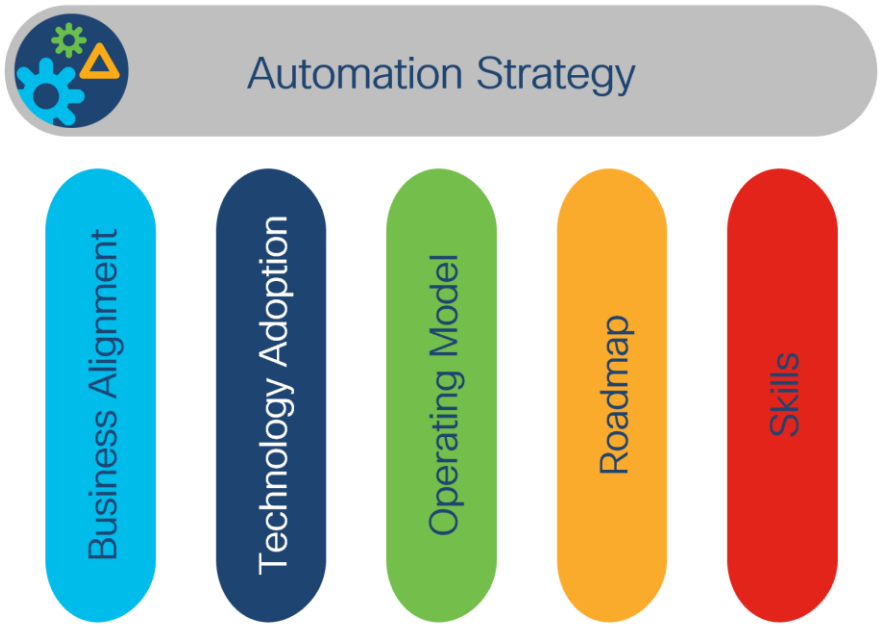

Figure 2.
Automation Strategy Pillars

[10] https://www.ciscopress.com/store/network-automation-made-easy-9780137506613

Automation Maturity Assessment

With the supporting pillars in mind, the first step is to understand where the organization currently stands. This tries to answer the question: **“Where are we?”**

A common approach is to undertake an assessment. It is not a requirement, however, most organizations do not know where they stand in regard to automation. The lack of understanding can be the result of several factors such as:

- Scattered automation efforts throughout the company.
- Lack of visibility into team’s automation processes.
- Tool adoption not monitored at the global level.

The assessment that typically works best is a questionnaire-based assessment forwarded to all relevant teams (network and cloud operations, network and cloud engineering, network and cloud architectures, site reliability, etc).

The result from this exercise should be: (1) an inventory of all the tools in use, (2) a maturity score for each of the tools in terms of current investment and industry alignment, (3) a list of skills available within the organization, (4) an understanding of which of the five above-mentioned network automation maturity categories your organizations stand in.

From this step, you are aware of what you possess. You can then start to work on answering the question: **“Where do we want to be?”**.

Network Automation Strategy Outline

A network automation strategy outline should be represented in a document format. This document expresses the strategy in a simple, concise and easy to consume way for any person in the organization. It should answer the two questions: **“Where do we want to be?”** and **“How will we get there?”**.

This document can have different sections and formats depending on the organization priorities, however we consider the following ones to be mandatory:

- Goals, Objectives, Strategies and Tactics
- Key Performance Indicators

Other common sections that you may also encounter are:

- Influences (e.g. organization structure, culture, skills)
- References to other strategy documents

It is important to note, that the highest quality strategy documents are created by stakeholders with different backgrounds from different areas (for example business, technology, operations). A diverse set of stakeholders allows assumptions to be challenged instead of taken for granted.

Goals, Objectives, Strategies and Tactics

This is the main section of your network strategy document, other sections exist to give context and further details to this section. In here, you define the following four concepts for your company:

- **Goals** – High level purposes.
- **Objectives** – Specific outcomes that define the goals.
- **Strategies** – How to achieve the goals.
- **Tactics** – Low-level actions to follow.

Goals are broad statements that typically reflect desired destinations. They are often the "what" that you are trying to achieve. Although a goal reflects an end state, it is not actionable; that is the role of objectives. Examples could be: advance from maturity stage 2 (basic configuration automation) to stage 5 (automated provisioning of devices in a self-organized, self-diagnosing and dynamically updated network powered by AI/ML) to enable the resiliency, agility and network digital experience that business team is demanding.

Objectives are actionable, specific, and measurable. Furthermore, they should be realistic and achievable. They define what needs to be done to achieve the previously defined goals; therefore, objectives do not exist in isolation but are always linked to goals. Examples could be: "decrease time to deploy network configurations by 70%", "reduce the time spent in troubleshooting activities by 30%" or "increase the number of fully monitored devices by 50%".

Strategies are high-level plans to follow to achieve goals. They specify, from a high level, how you are going to fulfill your intentions. Examples could be: "adopt controller-based network-wise automated provisioning for day-0 deployments", "adopt an automated tool for on-premises compute and cloud provisioning" or "deploy an artificial intelligence for IT operations (AIOps) platform".

Finally, tactics are specific low-level methods of implementing strategies. Examples could be: "deploy a specific software-defined networking solution in headquarters campus network", "enable the team on Terraform" or "invite AIOps tool vendors to tender/bid and run a pilot for two tools".

From this section, any reader should be able to answer the two previously posed questions: **"Where do we want to be?"** and **"How will we get there?"**.

Execution Plan

Once the low level actions (tactics) are defined, the next step will be to craft the execution plan. It is a separate document that describes workstreams, tasks, start and end dates, effort estimation, task owners, and dependencies. Creating a high level visual representation of this helps IT team visualize the **“How will we get there?”**.

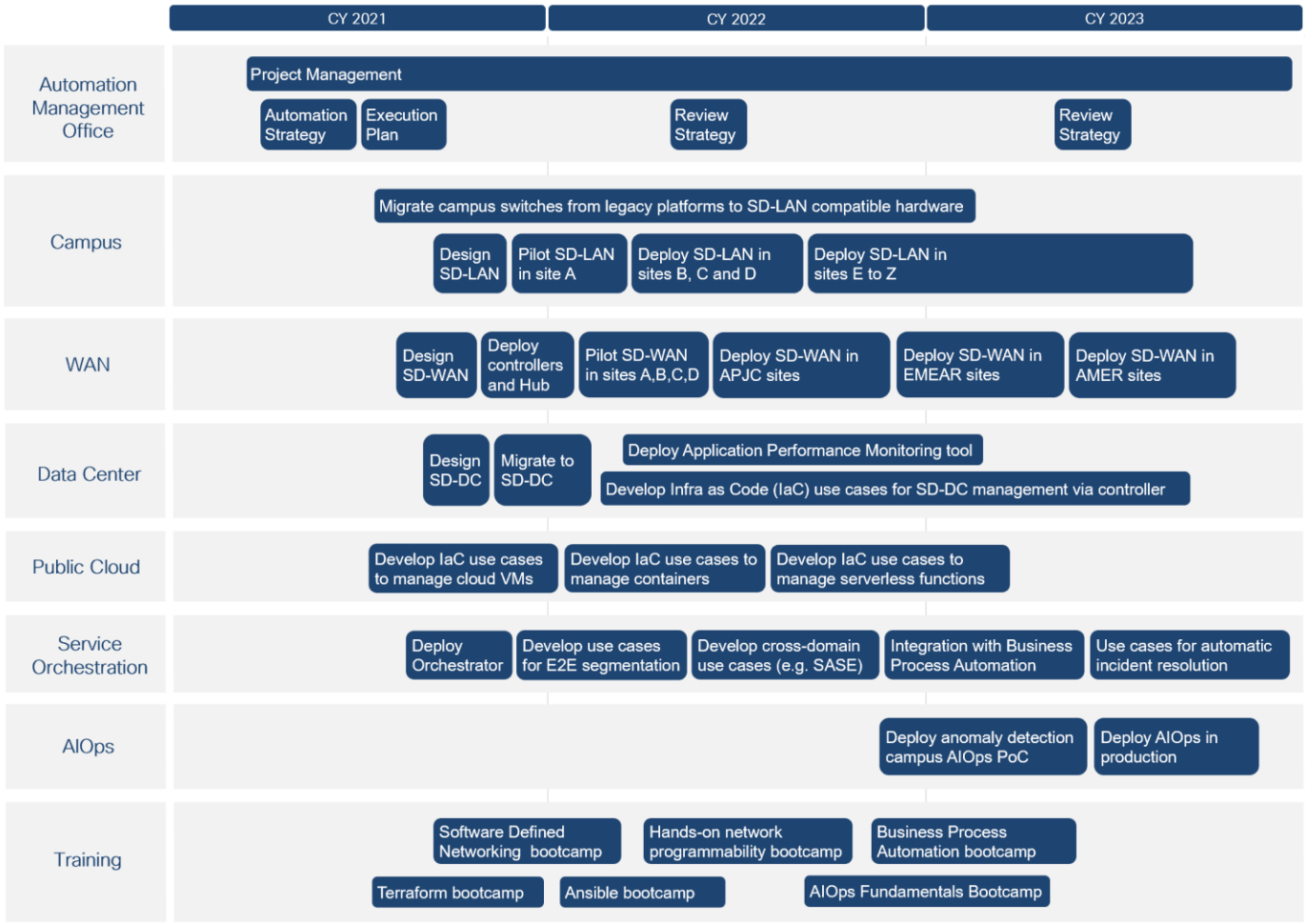

Figure 3.
Automation Strategy Roadmap

Best practices for executions plans

We have identified the following as best practices when crafting network automation execution plans:

- Prioritize use cases that need to be automated considering the business impact but also the implementation complexity.
- Capture use case requirements across multiple users and organizations (e.g. Planning, Engineering, Operations, Security).
- Plan to design and develop solutions using Agile and CI/CD tools and processes.
- Plan to leverage automated testing for end-to-end functional (including user interface, process automation, device configuration) and scale testing.
- Plan to design solutions with flexibility to accommodate evolution to new device types, new services and new configurations.

Key Performance Indicators

Key Performance Indicators (KPIs) are used to measure, track and report how the organization is performing in relation to its objectives. All objectives should have KPIs attached, it is important to design relevant and well-understood KPIs.

KPIs should be designed with the S.M.A.R.T. criteria in mind, meaning they should be:

- **Specific** – target a specific area for improvement.
- **Measurable** – quantify or at least suggest an indicator of progress.
- **Assignable** – specify who will do it.
- **Realistic** – state what results can realistically be achieved, given available resources.
- **Time-related** – specify when the result(s) can be achieved.

Examples of KPIs could be: “total number of network devices managed by a software-defined networking controller”, “number of network use cases developed in service orchestration tool” or “number of network issues resolved by AIOps and closed-loop automation”.

Challenges and best practices

It is important to balance the work that goes into creating, maintaining and reporting on the KPIs against the value created.

A challenge is choosing, developing and defining what to measure. Organizations and departments often copy KPIs from other organizations or departments, and these might not accurately reflect their own business or operations. This often results in failure to positively impact results and leads to the abandoning of the KPIs because the resources put into measuring are effectively wasted. It is paramount to have KPIs that resonate with your company’s objectives, that is the only way they are effective. Understand what data does your organization need to understand and improve network automation operations.

Another challenge is the form of communication of the KPIs. KPIs should be easily accessible, for example on a dashboard, and communicated often so individuals can understand where we are and where we target to go. Often KPIs are hidden in long documents reported at the end of fiscal year or fiscal quarter, this can lead to people being unaware of the KPIs and therefore not actively progress on them.

Best practices dictate that having KPIs will allow you to adjust your strategy accordingly, you should review and have a report cadence on them. A strategy is not something you create and forget, it is something you adjust and improve. Furthermore, you can and should optimize and review the KPIs themselves in the case they are not providing your initially expected insights.

Influences

There will be technology, organization structure, organization culture, employee technical skills and other factors that will affect the strategy, we refer to them as **influences**.

Some organizations add an **influences** section to their strategy document because they want readers to understand why some decisions were made over others.

Not all decisions are obvious, for example, choosing Ansible over Terraform for a specific project. However, for a specific organization this decision could be derived from the fact that all their developers are better versed in Ansible.

Organization structure

Challenges in a network automation project can also be non-technical for example related to the organization structure. This often arises in long and complex projects, when several teams are involved in the same project but each of them has its own agenda. Managing synergies and priorities in this environment becomes difficult and often result in conflicts. Organization structure will often influence the network automation strategy.

For example, in an organization with a transformational, multi-year network automation project, the customer identified the need for a new end-to-end (E2E) solution architecture team. In their network automation strategy document, they highlighted this need and also their responsibilities in regard to this project as shown below:

- **Evolution of the network automation solution.** Look into the long-term perspective and work on optimizing the whole network automation solution. Interlock with the different service stakeholders.
- **Manage changes.** Look at the overall picture, the end-to-end solution architecture team is empowered to prioritize changes and manage cross-organization synergies.
- **Discuss changes.** When a service stakeholder is requesting changes, the end-to-end solution architecture team will discuss the impact to other teams and be able to define what is best for the whole.

Some organizations choose to add this type of “influence” as it contributes to their goals, objectives, strategies and tactics. In the case of this organizations’ example, one of their strategies was to create this end-to-end architecture team and having the detailed information under the influences section made any reader aware of what it was trying to address and how.

Culture and skills

Organizational culture along with employees' skills are the two most influential human factors when building a strategy. More often than not, they are worth highlighting in the influences section.

Culture plays a special role in the planning of transitions. For example, an organization that does all management activities in a manual way will require investment in education and sensibilization before adopting automation practices. Simply giving them automation tools might not work as well as in an organization that already has an automation mindset but is lacking financial investment for adoption.

Technical skills are required for success. Choosing a less optimal automation tool over another for a specific use case can be the correct choice if the available skills at the organization match the less optimal tool.

Organizations need to have a good understanding of what skills they have available and if they match their automation strategy direction. In the case they do not, they can opt to upskill their workforce or hire externals. Either way, this should be reflected on the strategy document.

Other Strategy Documents

Organizations have several strategies, and they can impact each other. The network automation strategy should reflect the overall business strategy, however, it is often impacted by data, security or financial strategies already in place.

Imagine you create your network automation strategy according to the methodology presented in this paper, and one of your strategies is to use the cloud to store all your data in order to reduce storage costs. This is in line with your network automation goals and objectives, however, your organization’s data strategy mandates all data to be on-premises. These are conflicting strategies and must be addressed.

In this section, organizations highlight why specific decisions were made and cross reference those decisions to any corresponding influential strategy document.

Summary

In this paper we have covered what network automation encompasses and the numerous benefits it provides when properly adopted by enterprise and service provider IT organizations.

We have presented five levels for classification of an organization’s automation maturity, as well as different types of tools that enterprises use such as command line, network controllers, service orchestrators and AIOps.

We have presented automation market trends, relating them to historical data and future predictions, where we can clearly see the rapid growth in usage and relevance of network automation in the industry, producing the need to create and adopt network automation strategies.

Lastly, we have described what a network automation strategy is and how the typical network strategy document is structured, going into details of what each section represents and what value it brings.

If not already done, you should start working with your team to answer the three questions about your organization’s automation strategy: ”Where are we?”, “Where do we want to go?”, “How do we get there?”, making clear for everyone in the IT organization where you are headed and how, while enjoying the many benefits of network automation.

Authors

Ivo Pinto, Technical Leader, CTO Office Cisco Customer Experience

Asier Arlegui Lacunza, Principal Architect, Cisco Customer Experience

Reviewers

Vijay Raghavendran, Distinguished Engineer, CTO Office Cisco Customer Experience

Oliver Boehmer, Principal Architect, Cisco Customer Experience

Andrew Fraser, IT Transformation Executive, Cisco IT

Mike Keohane, Principal Engineer, Cisco Engineering

Manish Jain, Director, Cisco Customer Experience Product Management

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA 09/21