Network Migrations and Derisking Transformations

Arista Networks - Solution Services

5/18/2025.v1

Introduction

Network migration is driven by the necessity to modernize legacy systems in response to specific customer contexts, current challenges, and future business needs. Usually, the migration involves transitioning from an incumbent vendor to a new one, introducing the risk of change with new configurations, operating systems, technologies, operations, management, and automated processes. Strategic vendor selection is crucial for achieving the new objectives.

This white paper highlights the importance of risk management inherent in any change, serving as an assurance through services that address one of the primary concerns at the executive level when initiating major transformation projects. It also helps customers define a technology roadmap and outlines how Arista Services mitigate migration risks, minimize operational disruption, and accelerate changes through a phased approach.

Executive drivers for migration

The following key factors are driving organizations to initiate transformation projects and pursue network migration initiatives:

i. **Technology Upgrades:** Enterprises seek superior technologies that offer agility, reliability, scalability, automation, and advanced analytics, along with higher speed, higher port density, and lower space and power consumption, to future-proof their IT environments.

ii. **End-of-Life:** Hardware refresh cycle or legacy systems nearing end-of-life (EOL) increase operational risks, driving the need for migration to supported, secure platforms.

iii. **Security Concerns and Lack of Trust:** Frequent CVEs (Common Vulnerabilities and Exposures) and slow vulnerability management erode trust in incumbent vendors, prompting a shift to more secure alternatives.

iv. **Strategic Vendor Value:** Organizations prefer vendors offering added value through automation, open standards implementation, seamless integration, consistent product portfolio strategy and aligned service models.

v. **Rising Operational Costs:** Managing legacy infrastructure with snowflake designs and proprietary solutions increases OPEX and complexity, driving the need for modern, modular, consistent and replicable POD-based architectures to improve efficiency and reduce costs.

vi. **IT Transformation:** Migration supports IT consolidation and expansion, enabling flexible, scalable architectures to meet evolving business demands.

vii. **Introducing a Second Vendor:** Operating a multi-vendor network enables the use of best-of-breed products, enhances agility, and prevents lock-in to a single vendor's solutions. It also reduces vendor dependency and promotes cost savings through fair competition.

Strategic directions, decision factors and why Arista

Arista is the only vendor offering consistent implementation across all domains—Data Center, Campus, Cloud, Internet, AI and WAN—along with a phased onboarding and transformation approach: simplify, virtualize, and automate.

i. **Simplify** design and operations with Arista's Power of ONE, offering differentiated building blocks.

- ONE Operating System – EOS (Extensible Operating System) provides a consistent, programmable, and highly scalable network OS across all Arista platforms.
- ONE Engineering Model – Architect, Validate, Deploy (AVD) automates configuration management, self-documentation, and validation tests, ensuring engineering consistency through Infrastructure as Code (IaC), and it integrates with a CI Pipeline, GitOps workflows, and 3rd party software tools such as source of record, version control system, provisioning and testing tools.
- ONE Operational Model – CloudVision Portal (CVP) enables centralized network control, visibility and management, simplifying operational workflows and change control processes.

- ONE Security Model – offers Zero Trust security, identity-based access control, network segmentation and threat detection.
- ONE State & AI Data Driven Model – NetDL (Network Data Lake) aggregates and analyzes real-time telemetry data, enabling AI/ML insights for proactive network management.
- ONE Observability Model provides deep packet-level visibility, ensuring continuous observability across the network.

Arista has always invested in a unified approach: **One operating system, One management system, and One operating model**. This is a key differentiator for Arista. It may seem safer to keep the incumbent vendor for a network refresh, but their next-generation products often introduce new lock-in designs, operating systems, and management platforms—making the transition effectively equivalent to switching to a new vendor.

ii. **Virtualize:** Adoption of open standards and proven technologies.

EVPN (Ethernet Virtual Private Network) is a standards-based technology that enables organizations to extend Layer 2 and Layer 3 networks across multiple geographic sites, campuses and data center PODs. It leverages various forwarding planes, including VXLAN over IP or MPLS coupled with Segment Routing (SR), to enable seamless interconnection based on context and legacy infrastructure. EVPN provides feature-rich, open standards with proven technologies, allowing organizations to transition from bespoke solutions that rely on multiple protocols, often complicating management and hindering integration. Additionally, EVPN supports network virtualization and enables the sharing of physical infrastructure while providing overlay segmentation per tenant, ensuring secure and isolated environments.

The choice between VXLAN and MPLS depends on customer use cases and legacy interoperability requirements:

- VXLAN is commonly deployed within Data Center Interconnects (DCI), DC fabrics, and campus environments, providing scalable Layer 2 and Layer 3 overlays with efficient east-west traffic management.
- MPLS is more suitable for WAN environments and service provider networks, offering reliable, high-performance Layer 2 & 3 VPNs and traffic engineering capabilities.

Standards are crucial when selecting a vendor, as they prevent vendor lock in and encourage healthy competition.

iii. **Automate:** Innovate Day 2 operations with a modern operating model (MOM). Reduce OPEX through a consistent end-to-end automation strategy and unified workflows across all domains, complemented by a coherent and standardized telemetry model.

- Heavy automation ensures cloud-like agility through infrastructure as code, digital twin modeling and pre/post-validation. Continuous Integration (CI) pipelines, self-documenting configurations, and version control streamline deployments, reduce errors, and enhance operational reliability and efficiency. This approach follows two key principles: moving away from legacy, CLI-based operations centered on reactive troubleshooting and avoiding making changes to the network due to risk, and transitioning toward automated, software-driven, autonomous network management.

  The goal is to **"build the automation, and automation builds the network"**.

- Strategic lifecycle management focuses on maintaining a balanced and predictable upgrade cycle. Automated audit and infrastructure upgrades ensure equal performance across network, compute, and storage components, while amortizing POD infrastructure together and optimizing resource utilization. This approach prevents uneven technology obsolescence, maintains high performance, and ensures that infrastructure scales effectively with business demands.
- Deep visibility and predictive analytics reduce mean time to detect, analyze, and resolve issues. AI-powered data lakes aggregate and analyze network data, enabling pervasive visibility across the environment. Real-time telemetry supports intelligent workload placement, ensuring optimized performance and resource efficiency. By leveraging predictive analytics, organizations can proactively identify and mitigate potential issues before they impact business operations.

De-risking migration with Arista Services

Arista service support model

After defining the migration landscape and key decisions on new architecture and technology insertions, the next step is to establish a phased approach using Arista Services' proven methods, experiences, and automation tools. This includes defining the migration plan, developing Method of Procedures (MOPs), validating processes and applying lessons learned, while addressing customer concerns and integrating change controls, timelines, operational, legal, and business constraints.

Arista Services, with deep expertise in networking, automation, and software integration, focuses on addressing customer priorities by first understanding their requirements, objectives, and desired outcomes. This involves considering all aspects of the transformation, including network operations, migration, and architecture. Arista Services is engaged in hundreds of simultaneous projects, building extensive experience and exposure to virtually every type of migration scenario involving legacy vendors and diverse CLI-based operating systems. Arista's strategy focuses on open network standards, ensuring interoperability and integration within a multi-vendor environment, offering customers choice and flexibility, as opposed to vendor lock-in solutions.

Typically, customers begin with a design pattern, often a POD-type architecture, which addresses the initial components and sets the foundation for a successful transformation. This approach establishes a modern engineering blueprint with consistent, repeatable designs that can then be automated. However, Arista Services must also address two other key areas: network operations and personnel onboarding. When building a modern network architecture, it naturally follows that it should be operated in a modern way. Arista offers a service model to support the transformation of customer processes and train technical teams with the following approach:

- **Co-participating** Service Engagement: Working with the customer—not just for them—ensuring true collaboration rather than a simple handoff or turnkey solution.
- **Arista Training Services:** Offering formal and customized training courses to enhance the customer's skill set for adopting and operating new solutions.
- **Day 2 Service Support:** Ensuring a smooth transition and handover with specialized support.
    - » A time-based or one-year engagement with **dedicated engineers** ensures a seamless transition to the customer's network team, providing sustainable Day 2 support for GitOps, AVD, and customized integration and automation workflows throughout the deployment and migration phases of the project.
    - » Arista's **Onsite Services** (OSV) model enables the rapid replacement of faulty devices, minimizing downtime and helping maintain network reliability.
    - » **Managed Services** offer end-to-end management of network operations, allowing customers to focus on their core business while Arista handles continuous monitoring, performance tuning, troubleshooting, and proactive issue resolution.

Arista Network and Software Services will deliver the network transformation project across two key areas of focus: GitOps automation, which streamlines configuration and operational workflows, and migration execution tasks, which ensure a smooth and controlled transition to the new network environment. Both workstreams will follow a customized plan developed in close collaboration with the customer's engineering and operation teams.

GitOps automation and CI pipeline

Network migrations will introduce new processes and tools that will lay the foundation for a Modern Operating Model (MOM) and GitOps automation to support Day 2 operations.

The migration tools and automation framework will provide common functions for recurring day 2 operations, including new configuration deployments, validation of operational states, and reusable test cases for large-scale OS upgrades, switch deployments, and new service activations.

Separate collateral papers detail Arista's vision for the CI pipeline and the Modern Operating Model (MOM). During migration, we will leverage automation to execute the migration and establish a foundation for Day 2 operations. Below is an illustration of an example CI pipeline components to support the automation framework:

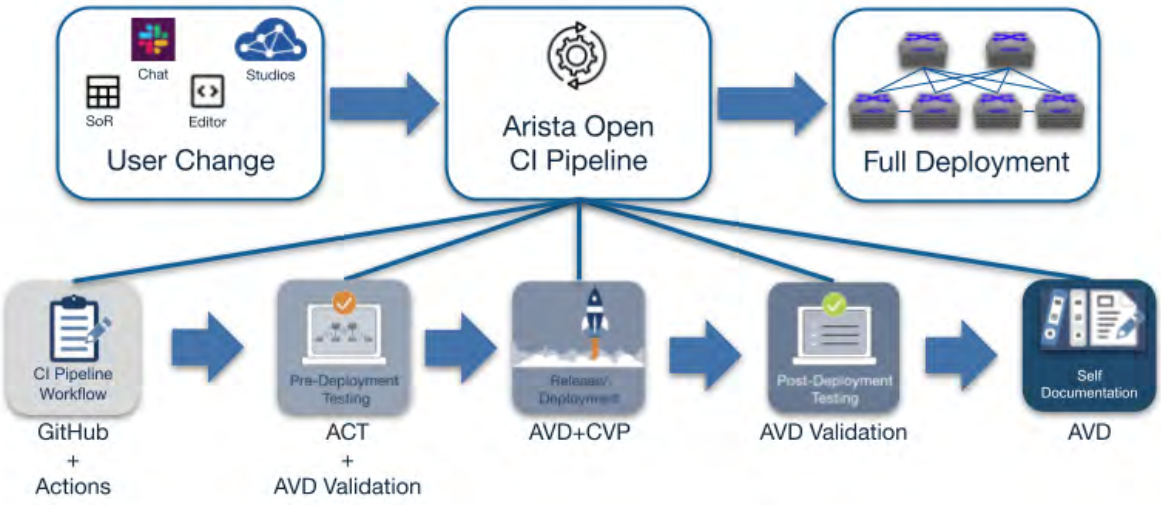

Figure 1: Example of a Continuous Integration (CI) pipeline

Arista's CI pipeline is designed with open, modular and flexible building blocks to ensure seamless integration and automation across various systems. Key components commonly used include, but are not limited to:

- **Third-Party Software** Integration with sources of truth & record (e.g., NetBox, Nautobot, Infoblox) and ticketing systems (ServiceNow) for streamlined operations.
- **GitOps/GitHub:** Version control and change management using GitOps principles for consistent and auditable deployments.
- **AVD (Architect, Validate, Deploy):** Automates the deployment of proven, validated designs, including configuration generation, validation, and self-documentation—through Infrastructure as Code (IaC).
- **ACT (Arista Cloud Test):** Provides a virtualized dev and test environment (digital twin) for validating configurations, automation and simulating network behavior before production deployment.
- **CVP (CloudVision Portal):** A centralized control and management platform for enforcing change control while maintaining operational consistency and visibility throughout the Arista network.

Arista Services offers a structured program to transition toward a Modern Operating Model, broken down into stages within the Network Operations Maturity Model. Customers typically begin by deploying consistent design patterns and implementing in-house automation or integration with IT Service Management (ITSM) systems at varying levels. Over time, they aim to achieve autonomous, software-defined operations, enabling cloud-like agility on-premises. Arista Services empowers the customer automation journey, embedding it in the design and transformation plan from Day 1, starting with initial deployment and migration projects.

Five functional stages for network migration

Arista Services has identified five key milestones or functions to execute and de-risk migrations, applicable to virtually all migration scenarios across various vendors and legacy architectures in any domain. These milestones include:

Discovery, decision making, migration and project planning

The discovery phase focuses on data gathering and analyzing extensive data from hundreds of devices to establish a comprehensive baseline of hardware inventory, network services, operational states, edge connectivity, performance, and scalability. Collection tools capture pre-existing network conditions, identifying inefficiencies and challenges that migration will resolve. This process

enhances data accuracy, improves discovery depth, and informs decision-making by assessing legacy network designs, topologies, scale, and EOL (End-of-Life) hardware. Additionally, these discovery tools can be applied to broader contexts such as network assessments and recurring audits.

Arista Services is prepared to handle various CLI input formats and sources of truth, ranging from CLI-based migration type (including Cisco IOS, IOS XE, IOS XR, NX-OS, JUNOS, JUNOS EVO, and ExtremeXOS) to network controllers such as Cisco ACI and Juniper Apstra, as well as sources of truth like NetBox or Nautobot.

As part of the discovery and migration planning process, Arista Services will provide consulting recommendations and may suggest certain network normalizations and standardizations to address pre-existing conditions in the legacy network. This may include upgrading software versions with known issues, correcting configuration inconsistencies, resolving ad-hoc operational states, IP addressing optimizations, routing polices and access-list adjustments, and converting proprietary protocols (such as EIGRP) to open standards to facilitate seamless integration with other networks as part of the pre-requisites prior to the migration.

The next step is to determine the appropriate migration techniques based on the customer's environment, considering factors such as space and power constraints, if applicable. This decision typically involves choosing between two approaches:

- **Per-device migration** involves replacing equipment and integrating new devices into the legacy network while maintaining a largely identical design. Key considerations include managing hybrid environments and ensuring interoperability between different vendors, as variations in feature and protocol implementations, despite being standards-based, may introduce compatibility issues. To mitigate these risks, we recommend conducting interoperability testing in a lab environment. This scenario is most commonly observed in WAN, Service Provider (SP), and Internet environments with clear Layer 3 boundaries, rather than in campus or data center deployments. It may also be applicable locally when power and rack space are constrained.
- **Per-design migration** involves deploying new equipment in a greenfield mode and interconnecting it in parallel or side by side with the legacy network. The next step is to establish new Layer 2 and Layer 3 connection paths based on existing traffic flows and multi-step migration requirements, enabling the introduction of the new design while minimizing interoperability concerns. This approach ensures a smoother, more granular transition over time, facilitating the adoption of new conventions and logical remapping, such as IP and VLAN translations, while aligning the network with modern operating practices.
- The greenfield activation phase, conducted outside of the production traffic path, presents an opportunity to maximize the benefits of new solutions from day one. This phase enables the adoption of modern technologies and designs, integrating Infrastructure as Code (IaC) and network data modeling through Architect, Validate, Deploy (AVD). Key activities during this phase include:
  - » Build and Move: Build the new environment in parallel, ensuring seamless integration and transition from legacy systems.
  - » Introducing GitOps workflows for version control and automation.
  - » Implementing Zero Touch Provisioning (ZTP) for seamless device onboarding.
  - » Set Network Ready for Use (NRFU) standards.
  - » Plan a modular and partial migration process to minimize disruption by breaking down the migration into manageable steps.

  A key consideration is that although control plane interaction is simplified in this approach, it still requires strict traffic flow management between environments. Layer 2 and Layer 3 path connections ensure that all existing connectivity use cases are maintained. Special attention must be given to traffic load distribution, avoiding congestion points, and ensuring stateful devices in the path (if applicable) handle symmetric routing correctly.

  The following are common specifications for inter-domain connections:

  - » Redundant Multi-Links: Establish multiple links between legacy vendors and new domains across border devices for redundancy and bandwidth peak absorption.

- ◊ Layer 2 and Layer 3 connectivity typically use a shared Active-Active multi-link cross-connected bundle.
- ◊ Layer 2 Loop Prevention: Arista's EVPN implementation provides two potential multi-homing solutions; Multi-chassis LAG (MLAG) and EVPN all-active (A-A) multi-homing.
- ◊ For more details, visit Arista at: https://www.arista.com/assets/data/pdf/Whitepapers/EVPN-DC-Multihoming-for-Resiliency-WP.pdf
- ◊ Trunk the required VLANs on the inter-domain links prior to the workload migration. Dedicate a separate VLAN for the Layer 3 routed path, if applicable.
- ◊ Layer 2 and Layer 3 paths can also use separate physical links.
- ◊ For layer 3 peering, use a routing protocol like BGP to exchange prefixes between domains.

» Edge Port & BPDU Handling between vendors: Verify access port settings and default BPDU behavior to avoid unintended flooding or port blocking due to loop protection. As a best practice to secure the connection, implement storm control between the legacy and new networks, and ensure the legacy proprietary feature, Unidirectional Link Detection (UDLD), is disabled.

» Data plane gateway stitching is used in more complex migration scenarios, particularly when encapsulation translation is required.

The per-design migration scenario is most commonly observed in Data Center and Campus environments, typically within a specific geographic site, but it is also applicable to dual-core multi-vendor deployments in WAN networks.

Configuration Conversion

For **per-device** migration, Arista Services is well-prepared to handle a variety of CLI input formats and sources of truth for CLI-based migrations, including Cisco IOS, IOS XE, IOS XR, NX-OS, JUNOS, JUNOS EVO, and ExtremeXOS, and to convert them to EOS CLI equivalents for device-level migration. Purpose-built tools and scripts are regularly developed, provided that there is a robust parsing method to scrub legacy commands. Templates must be maintained and updated to align with target or latest OS versions, ensuring accurate and consistent device-level configuration conversions. However, this process and the template management may limit the capabilities of these tools.

For **per-design** migration, a more holistic approach is required. We begin with a network-wide assessment with the legacy network, extracting overlay service data (including edge port details, VLANs, and VRF tenants). These variables are structured and exported into the Architect, Validate, Deploy (AVD) framework as YAML files. The YAML files describe various configuration layers: global variables, core routing infrastructure of the new design (Ex. L3LS EVPN/VXLAN), service tenant overlays, and edge connectivity. This structured approach enables automated EOS configuration generation, ensuring AVD becomes the source of truth for generating self-documentation and validation test cases.

This method requires careful mapping of new physical port allocations for edge connections while leveraging pre-established core infrastructure of the greenfield portion of the new design. If applicable, all possible remappings — VLANs, IP addresses, and VRFs — must be specified and transposed.

A critical consideration is translating legacy vendor features to equivalent open-standard or Arista-supported features. Common open-standard edge port features supported across vendors include 802.1X, LLDP, STP/RSTP/MSTP, LACP, 802.1Q VLAN tagging, DHCP snooping, port security, IGMP snooping, Dynamic ARP Inspection (DAI), storm control, DHCP Option 82, QoS (IEEE 802.1p), and access lists, among others.

Proprietary features such as EIGRP, VSTP, EtherChannel, Voice VLAN, and Private VLANs may require normalization with open standards, either prior to migration or during the transition.

Accurate feature mapping, translation, and validation reduce operational risk and ensure seamless migration. Feature translation is currently a manual process and may require additional time, especially with QoS, where hardware-specific chipset behavior can introduce complexity.

Understanding the current configuration and preparing new configuration templates consume the most effort in migration projects. Automating the configuration translation process from other vendor platforms to Arista EOS significantly reduces the risk of human error and accelerates migration timelines. Consistency is achieved by leveraging shared experience, data modeling, and automation framework such as AVD, preventing ad-hoc scripting that often leads to inconsistent outcomes.

By integrating with AVD, the migration approach ensures that the new network is future-proofed for Day 2 operations. This approach minimizes migration errors and delivers consistent, predictable results.

For more details, visit Arista AVD at https://avd.arista.com/

As an alternative to AVD and Infrastructure as Code (IaC), CloudVision Portal (CVP) offers a web-based GUI for automating network operations. It uses Studios and Workspaces to generate and manage configurations. Studios serve as templates for specific network features, while Workspaces apply and manage these configurations across devices. CVP includes built-in and customizable Studios, with Workspaces enabling input edits and device tagging for coordinated changes.

Migration procedure documentation, execution tasks and change controls

Network document creation and migration runbooks are essential for minimizing errors during maintenance windows (MW). Using AVD as the source of truth enables consistent, instant, and fully automated generation of design documentation, ensuring alignment with the overall migration plan.

Migration procedures require detailed Methods of Procedure (MOPs) that define and validate each step. Increasing automation in MOP and runbook generation significantly accelerates the process and enhances accuracy.

Effective traffic management is essential for minimizing service disruption during migration. Proper traffic steering, including draining traffic from affected devices or sites and redirecting it to failover areas, helps reduce downtime and mitigate risks.

Arista **Maintenance Mode** is a predefined device state that can be activated to gracefully drain traffic and trigger rerouting through control-plane coordination. It enables seamless traffic redirection, minimizing disruption during maintenance. Once the process is complete, the device is reintegrated into the network without impact. Maintenance Mode executes a sequence of customizable steps by default—for example: MLAG switchover, BGP maintenance processing via route poisoning, MLAG port-channel link down, and interface rate monitoring.

For more details, visit Arista at https://www.arista.com/en/um-eos/eos-maintenance-mode

Typically, migration execution steps are as follows:

- Migration Procedures: Define step-by-step migration procedures with clear execution guidelines and checkpoints.
- Change Controls: Develop and leverage change control scripts to ensure accurate and consistent execution of migration tasks.
- Validation and Checkpoints: Incorporate validation processes and data checkpoints to confirm that changes have been applied successfully and meet desired outcomes.
- Rollback Procedures: Establish intermediate rollback procedures to revert to the previous state in the event of an unexpected failure or deviations from defined checkpoints.
- Reusable Templates: Utilize pre-validated templates and best practices derived from previous experiences to accelerate task execution and maintain consistency.

To further streamline the migration process, automation should integrate with CloudVision Portal (CVP). Once AVD has generated the EOS configuration and the playbooks have pushed the changes to CloudVision Portal (CVP) in the form of configlets, tasks are automatically created. The customer then creates a change control to sequence the various change steps. Actions within a change control are used to run a series of commands on devices for configuration, diagnostics, or monitoring purposes. CVP offers a range of built-in actions that can be selected when setting up a change control or creating a change control template for re-use across

multiple maintenance windows. CVP Automation benefits for change control are:

- Controlled automation: Automate device changes using structured approval workflows, while clearly highlighting differences between the intended configuration and the running configuration.
- Step-by-step execution: Sequence configuration steps to reduce risk thru built-in or customizable action bundle
- Integrate pre-check & post-check tasks
- Constant record-keeping of all statistics (routes, MACs, ARP, state, etc.) via telemetry, with the ability to look back in time and correlate data with specific changes.
- Template management: leverage CVP for template-driven automation, reducing manual effort and increasing operational efficiency.
- Rollback capabilities to revert changes easily in case of failures or unexpected behavior.
- Real-Time monitoring and alerting mechanisms to detect and address issues immediately, minimizing potential downtime.

By aligning document generation, migration step execution, and CVP change control and real-time monitoring, Arista Services ensures a streamlined, repeatable, and error-free migration process that delivers consistent results across projects.

To validate the overall migration process, we recommend conducting non-impacting pilot testing to verify key steps such as VRF creation, VLAN extension, port provisioning, and performing a dry run of end-device or VM migration. By using non-impact traffic, this approach ensures connectivity between the legacy and new fabric, identifies potential issues early, confirms production readiness, and accurately evaluates the time required—enabling a well-scripted and efficient maintenance window.

Migration validation testing capabilities

Arista Services strongly recommends using a DevOps environment or digital twin for migration accuracy and validation for several reasons:

- **Error mitigation and validation:** A digital twin eliminates conversion and migration errors by enabling lab testing before execution. It simulates the post-migration state, allowing customers to visualize the migration process and assess potential service impacts, ensuring a smoother transition to the production network.
- **Enhancing migration processes:** Digital twins help to refine MOPs, change runbooks, configuration templates, and validation workflows.
- **Modular and flexible CI pipeline integration:** Seamlessly integrate digital twin environments into automation pipelines to support end-to-end migration and pre-deployment validation. Customers can build multiple CI pipelines using Arista's CloudVision Portal (CVP), Git-based version control, Architect, Validate, Deploy (AVD), and pre-/post-validation frameworks. These typically include:

  CloudVision Portal (CVP), Git-based version control, Architect, Validate, Deploy (AVD), and pre-/post-validation frameworks. These typically include:

  » Pre-Validation Pipeline (Development Environment)

  » Deployment Pipeline (Production Environment)

  » Post-Validation Pipeline

  The key differences lie in how outcomes are directed to different environments, and how automated actions and rules are applied across various approval stages and checkpoints. This framework is introduced during the migration process and can also be re-used for Day 2 activities, such as implementing and validating any network changes or performing OS version upgrades.

Arista ACT (Arista Cloud Test) is a high-scale network testing and validation platform that simulates production traffic patterns and network conditions to test network infrastructure, applications, and services. ACT can be used for a virtualized replica or digital twin of a production network environment. It uses Arista vEOS, third-party vendors via BYOL, and CloudVision instance to create a fully functional, software-based model of the physical network. It also supports DevOps and CI/CD pipelines by integrating with automation frameworks and enabling continuous validation.

For more details, refer to the ACT datasheet available at: https://www.arista.com/assets/data/pdf/Datasheets/Cloud-Test-Datasheet.pdf

Pre- and post-migration validation checks for network assurance

The previous section highlights the benefits of using a lab or digital twin for several reasons. This part focuses on performing multiple validation tests and leveraging automation tools on the production network before, during, and after migrations. It helps evaluate outcomes, detect issues, and quickly isolate the root cause of outages during troubleshooting. In case of unexpected events or conditions, it also facilitates rollback by capturing the current state to open a TAC case for further analysis, ensuring confidence to proceed with the migration once the issue is resolved.

Network validation methodologies are as follows:

- **Network Ready for Use (NRFU)** is a critical phase in Arista's deployment methodology, ensuring that a newly built greenfield network environment (for side by side migration) meets operational, performance, and security baselines before introducing production traffic. For greenfield deployments, NRFU validation includes a comprehensive set of pre-production checks, control plane verifications, pilot test traffic validation, underlay and overlay reachability, and service assurance to ensure the network is fully operational and aligned with the design specifications. We recommend conducting failure and recovery tests, if conditions permit, including simulating nodes, links, components, and software failover scenarios to verify redundancy and recovery mechanisms. Additionally, network convergence time should be measured as part of the design validation process.
- Accurate **wiring checks** are essential to prevent misconfigurations and ensure proper connectivity. This includes verifying port mappings, performing LLDP-based topology validation, and conducting interface status checks. Wiring validation should be performed at multiple stages—after rack and stack, during Network Ready for Use (NRFU) testing, and during post-migration assessments.
- **Pre-migration data collection** involves capturing a pre-state snapshot of the legacy network as a record. It verifies pre-existing conditions and documents the operational state of the control and forwarding planes. Discovery tools can be leveraged to collect data from the legacy network and update it with the latest state just before migration. Pre-migration validation ensures a reliable and stable data point of the legacy fabric before initiating migration. This process captures the pre-migration state—including network configurations and operational baselines—for comparison against post-migration results, helping to validate and conclude the maintenance window.
- **Post-migration validation** focuses on ensuring that the network functions as expected after production traffic has been moved to the new network. These tests should validate multiple components, including:
  - **Control plane checks:** Verifying protocol adjacencies, route propagation, and neighbor relationships.
  - **Forwarding plane checks:** Validating data path integrity through traffic tests such as ping, traceroute, and path verification. Arista's CloudVision Connectivity Monitor provides real-time monitoring of network connectivity and health across devices and infrastructure.
  - **Operational state checks:** Ensuring all interfaces, services, and network functions operate as expected. Recording the learned state of MAC and ARP tables validates that all end-hosts can communicate properly after migration.
  - **Device logs and events monitoring** during the migration change window.

- **Pre and post-check testing comparison:** Comprehensive pre- and post-migration validation involves comparing the initial network state with the post-migration state to identify deviations, misconfigurations, or unexpected changes that may impact performance or stability.
  - » Service continuity Checks: Ensuring that all critical services remain operational and behave as expected.
  - » Performance metrics evaluation: Comparing latency, throughput, and packet loss before and after migration to detect anomalies.
  - » End-hosts and interface health checks: Monitoring for failed ports, down interfaces, or degraded hardware components, and comparing all learned MAC/ARP entries from end-hosts to ensure they are populated as expected, matching the pre-migration state.

Automation test tooling and capabilities:

Once we have listed the different migration requirements and steps, it becomes evident that automation is essential to accelerate the collection of maximum data points, self-create appropriate test catalogs, generate validation test reports, and enable real-time capabilities and network visibility. It relies primarily on the following:

- NRFU CVP dashboard

  Arista Services has developed a single-panel real-time dashboard integrated into CVP to perform automated validation during NRFU, ensuring a solid, dependable fabric. This dashboard is also used for ongoing Day 2 monitoring. It provides real-time checks and event monitoring for all primary network functions, including device system health, control plane states, scaling, and event monitoring.

- EOS as a Traffic Generator and On-box Scripting Tool

  Leverage the power of EOS and its embedded utilities to generate custom traffic and create scripts. EOS can simulate custom traffic using built-in tools like iperf and Ethxmit (For more details, see https://arista.my.site.com/AristaCommunity/s/article/traffic-generator-on-arista), sending sampled traffic with numerous MACs and routes to the fabric under test. Additionally, EOS supports creating specific on-box scripts for testing purposes, such as local checks and diagnostic Python health scripts.

- Arista Network Test Automation (ANTA)

  ANTA is an open-source python framework that automates network validation in Arista environments, streamlining NRFU testing and ensuring consistency before and after migration.
  - » Key Features:
    - ◊ Control plane testing: Verifies protocol functionality: BGP, MLAG…etc
    - ◊ Wiring and cabling checks: Ensures correct wiring and maps LLDP with port descriptions and status.
    - ◊ Ensures accurate health and system validation of Arista devices.
    - ◊ Self-generated test catalogs based on the intended design and the active feature set.
    - ◊ Customized test cases can be added by users to the initial test catalogs.
  - » Workflow:
    - ◊ Define test cases: Create YAML-based test cases to validate the network or generate test catalog from AVD
    - ◊ ANTA pre-migration test run: Capture and validate the network's baseline state.
    - ◊ Execute Migration: Apply configuration changes or introduce new devices.
    - ◊ ANTA post-migration test run: Validate and compare the network's state after migration.

- ◊ ANTA generates a test report: Highlight any deviations or errors.

» Use Cases:

- ◊ Automate NRFU testing on preproduction networks.
- ◊ Network audit: Validate live networks periodically or on demand
- ◊ Ensure network health across Arista environments during network changes and migrations.

For more details, visit Arista ANTA at https://anta.arista.com/

- CloudVision Portal (CVP)

  CloudVision Portal (CVP) provides real-time telemetry and monitoring to enhance visibility during migration. Its analytics capabilities offer comprehensive network insights to ensure that network configurations and operations align with customer requirements. Key capabilities include:

  » Real-Time dashboards: Providing instant visibility into network health, traffic patterns, and configuration status. Dashboard capabilities are highly customizable, providing a single view of change steps, progress, device health, and host availability at every stage of the migration.

  » Connectivity monitoring: Validating layer 2 and layer 3 connectivities across the network between multiple end-points, ensuring path continuity, while providing immediate visibility into the health and status of the network.

  » Traffic flow analysis: Analyzing traffic flows through the topology to detect anomalies and ensure optimal performance post-migration.

  » Topology visualization: Presenting a dynamic topology view that highlights connectivity, active links, and potential bottlenecks, helping users visualize device connections and interactions to easily pinpoint problem areas.

  » Event notification: Providing alerts and notifications when network connectivity issues or failures occur, enabling quick identification and resolution.

  » Snapshot function periodically captures command outputs defined in the template, based on the specified schedule. Snapshots provide insights into device configurations, EOS versions, and other key operational aspects, captured per individual device.

  » The compliance function provides a real-time summary of OS image version control, out-of-sync configuration status, known issues, vulnerability alerts, and security compliance across all managed devices.

  For more details, visit Arista CVP at https://www.arista.com/en/products/eos/eos-cloudvision

  ANTA and CVP are complementary, providing a suite of validation and monitoring tools during migration. First, they are highly customizable to fit customer-specific requirements, but also address the different aspects of networks, from control to data planes, including operational states, with real-time capabilities. Arista Services heavily rely on these two tools but also have the capability to develop customized scripts for integration into a CI pipeline. The objective is to ensure everything runs smoothly after migration and that the network state is aligned with the intent defined in the network data modeling (IaC).

Conclusion

This paper outlines the migration journey for large-scale, complex network transformations, adapting to each customer's unique priorities. Migration and transition phases often span months or even years and involve strategic decisions that can significantly impact business performance, especially as IT infrastructure is becoming increasingly mission-critical to enterprise operations. Whether driven by innovation or necessity, choosing the right vendor is critical. The ideal partner aligns with customer goals, supports open standards, enables integration across multivendor environments, and helps avoid vendor lock-in.

Once the decision is made, Arista Services offers tailored migration plans built on proven methodologies, industry best practices, and years of experience. The workflow illustrated in Appendix A shows how complex migrations can be managed with reduced risk from start to finish.

To move forward, contact your Arista SME to explore the next steps—from network discovery to design planning and technology roadmap and insertion, including demos on migration automation and the Modern Operating Model (MOM).

This white paper is the first in a series of publications that will focus on the "HOWs" of migration—covering use cases, processes, considerations, and technical topics. The approach incorporates lessons learned and proven technical methodologies to develop an executable plan that ensures a smooth and efficient transition, while minimizing downtime, accelerating timelines, and, most importantly, de-risking the migration.

Appendix A

The **Network Service Migration Project Workflows** provide a step-by-step guide for transitioning services from legacy network systems to modern Arista-based infrastructure. It covers everything from planning and design to data modeling, testing, execution, and post-migration support for a smooth hand-over to customer operations and automation teams. The goal is to ensure a reliable migration with minimal impact on ongoing operations.

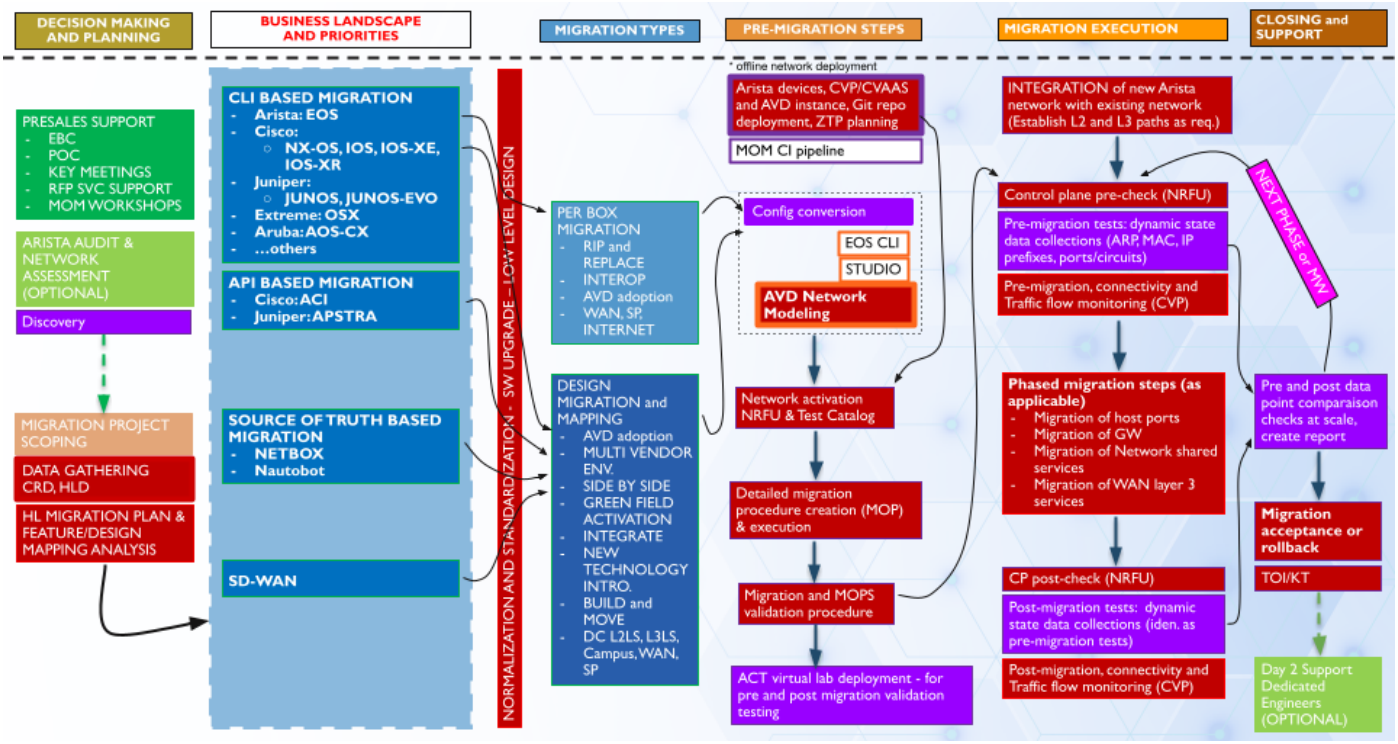

Figure 2: Workflow and key milestones commonly used in network migrations

The next step is to build an actionable project plan to align Arista Services deliverables with this workflow, based on the customer's priorities, requirements, environment, and migration timeline.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office
1390 Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062