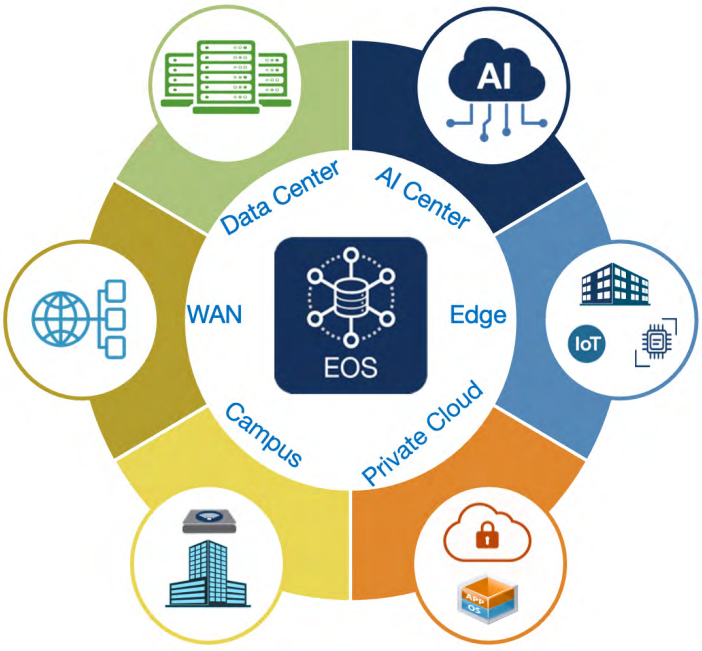
Arista Smart System Upgrade: Ensuring Business Continuity for Modern Network Operations

Keeping Pace with AI, Data Center and Campus Innovation

Deploying and taking advantage of new technology is top of mind for most organizations. Balancing the business benefits of adopting a rapid pace of innovation with the associated risks is a constant struggle, one many are losing. A major inhibitor to technology adoption is the ability to transparently insert new functionality into existing facilities without adversely impacting critical applications.

The difficulty in doing this has had an almost paralytic effect on the adoption of new feature development, not just in the data center, but in the enterprise campus and beyond. The opportunity cost of this inertia; delayed access to a technology transition, loss of ability to scale new workloads or even prevention of bringing new network capacity to a manufacturing plant, AI fabric or data center facility.



Hitless Upgrades by Function and Use Case

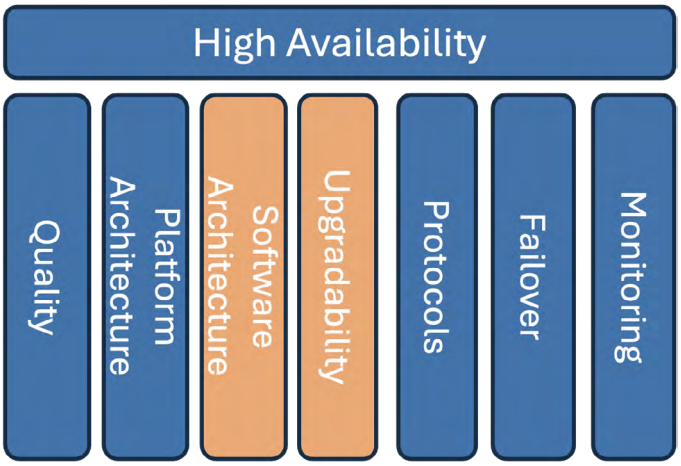
Mitigating Security Vulnerabilities and CVEs

Beyond feature innovation, network infrastructure is increasingly targeted by sophisticated cyber threats, making the rapid remediation of Common Vulnerabilities and Exposures (CVEs) a critical operational mandate, increasingly so as AI-driven vulnerability discovery has compressed the time between identifying a software flaw and weaponizing it. Historically, network administrators hesitated to deploy necessary security patches due to the inevitable downtime and the risk of disrupting critical campus workflows or data center applications. However, as the attack surface expands with ubiquitous IoT integration and hybrid workspace models, delaying operating system updates is no longer a viable security posture. Modern organizations require a resilient mechanism to seamlessly apply critical security updates and CVE patches to the network immediately, removing the need to wait for scarce, disruptive maintenance windows.

Continuous Operations

The traditional function of scheduled weekend maintenance windows is rapidly becoming obsolete. Today's globally distributed workforces, round-the-clock digital services, and always-on automated systems demand a network infrastructure that supports continuous operations. IT teams are challenged to perform routine maintenance, qualification of new software and functionality, complex software upgrades and infrastructure expansions seamlessly, without introducing latency, dropping packets, or disrupting user sessions. To achieve this true continuous operation state, the network architecture must inherently support hitless maintainability, ensuring that the underlying infrastructure remains highly resilient and fully functional even as individual switch components are proactively serviced, patched, or replaced.

This paper will discuss how Arista ensures business uptime and continuity through two key contributing factors to High Availability - Software Architecture and Upgradability.



Arista High Availability Model

High Availability through Software Architecture

Arista's Operating System - EOS - maintains a multi-process state-sharing architecture that is also the key to providing high resiliency. This architectural advantage allows both resiliency to security flaws as well as providing the ability to minimize the attack surface and blast radius if a defect were to exist. Specifically, the modular, state-sharing architecture provides a hardened structure with:

- Publish-Subscribe Architecture: In-memory publish-subscribe database (NetDB) that decouples system state from individual network processes, allowing for seamless fault recovery, rapid convergence, and live software patching.
- Plane Separation: EOS provides inherent separation between the control plane (software management) and the data plane (hardware forwarding) to help ensure that failures in the control plane do not affect traffic on the data plane.
- Agent Isolation: Within a plane, there is further separation between software agents running inside the network operating system. Issues impacting a single protocol are contained within that agent and do not spread to other parts of the system. This separation of agents also enables targeted fixes to affected components with minimal impact on the overall system.
- Process Restartability: Because system state is decoupled from the software processes (agents), individual processes can fail and restart independently, instantly resynchronizing their state without disrupting overall operations
- Memory and Message Safety: Arista EOS uses a framework that enforces best practices for memory management, message passing, and other parts of the code that have historically been sources of vulnerabilities. This framework is designed to prevent these common categories of security defects from occurring in the first place.

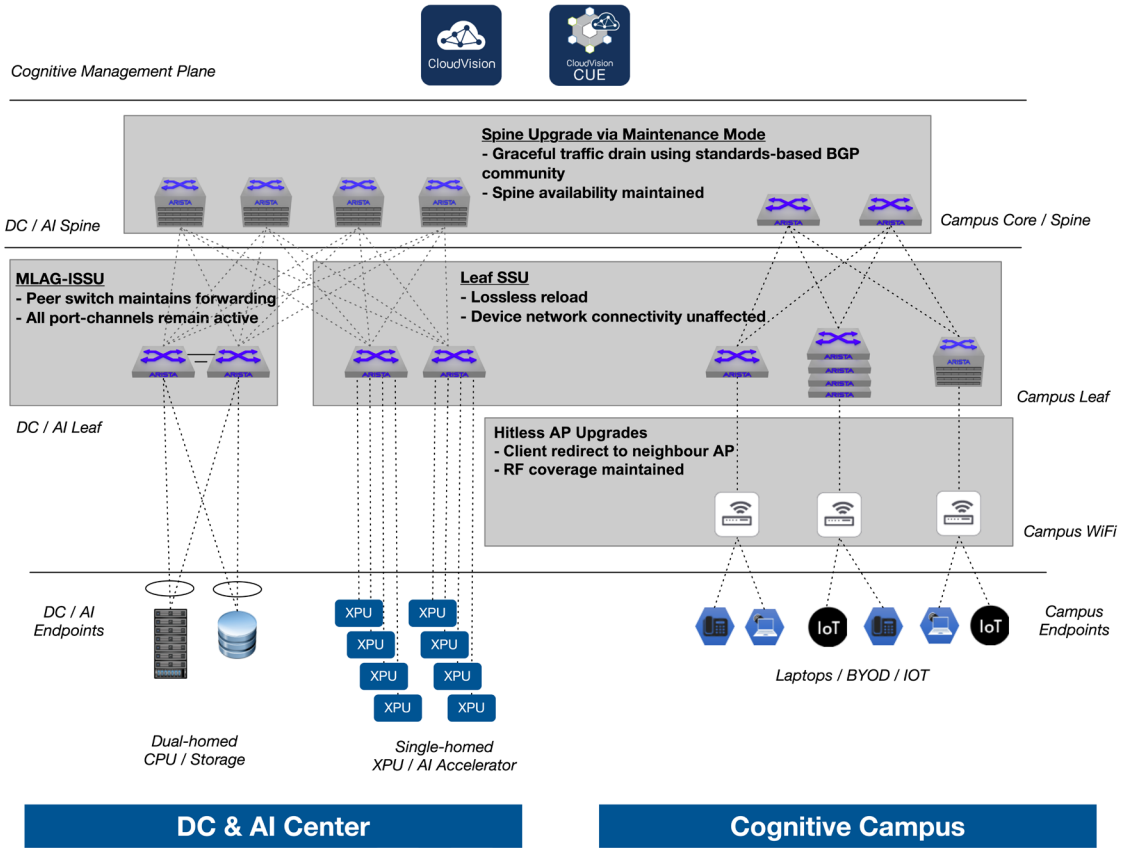
Introducing Arista EOS Smart System Upgrade

Smart System Upgrade is a network solution designed to address one of the most complicated and challenging tasks facing network administrators: infrastructure maintenance. Changes to the underlying network infrastructure can affect large numbers of devices and cause significant outages. Combining native EOS functions and intelligent automated workflows built into Arista's CloudVision orchestration platform, Smart System Upgrade takes a broader network perspective to software maintenance by allowing network switches to be transparently upgraded while traffic is either diverted or continues to flow unaffected and without impact.

Arista's approach to Smart System Upgrades is to provide a framework designed to eliminate downtime across specific functions or architectural layers in the network. Depending on the functional location, different methods apply and are further explained throughout this guide.

Network Function	Operational Feature	Primary Mechanism
Layer 3 Spine	Maintenance Mode	Protocol-driven graceful shutdown
Dual-homed Access / Leaf Layer 2 Spine	MLAG ISSU	Dual-peer sequential
Single-homed Access / Leaf	Leaf SSU	Control-plane restart / Data-plane persistence
Wireless Access Point	Hitless AP Upgrades	Client Redirection

The following diagram shows the functional layers and network use-cases to which the different upgrade mechanisms apply.



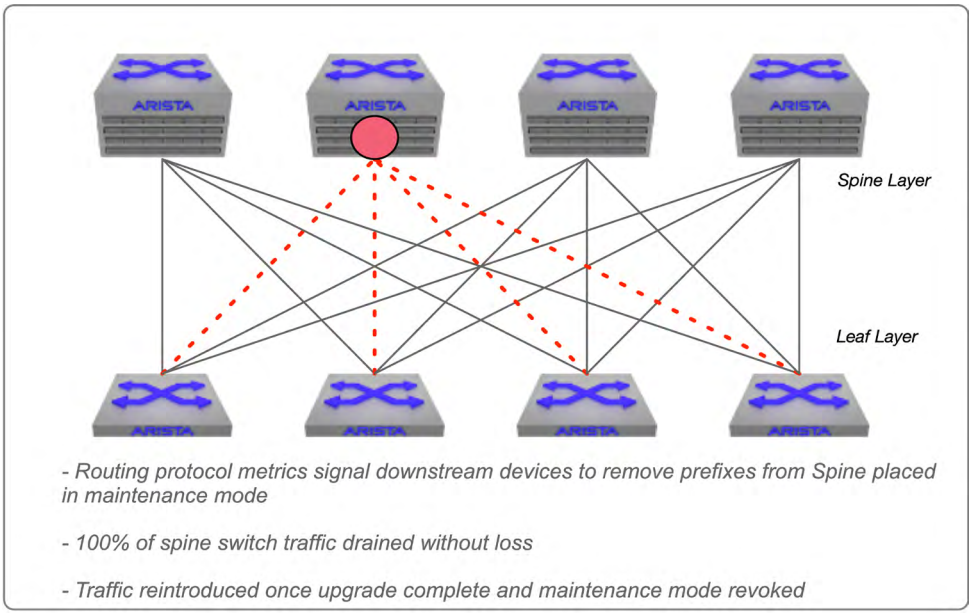
Hitless Upgrades by Function and Use Case

Smart System Upgrade Deployment Models: Spine, Leaf, and MLAG ISSU

Arista's Smart Upgrade functionality is designed to accommodate the varied roles devices play within a modern leaf-spine architecture. By tailoring the maintenance process to the specific layer in the topology, hitless operations are ensured across the entire network infrastructure.

Spine Upgrades with Maintenance Mode

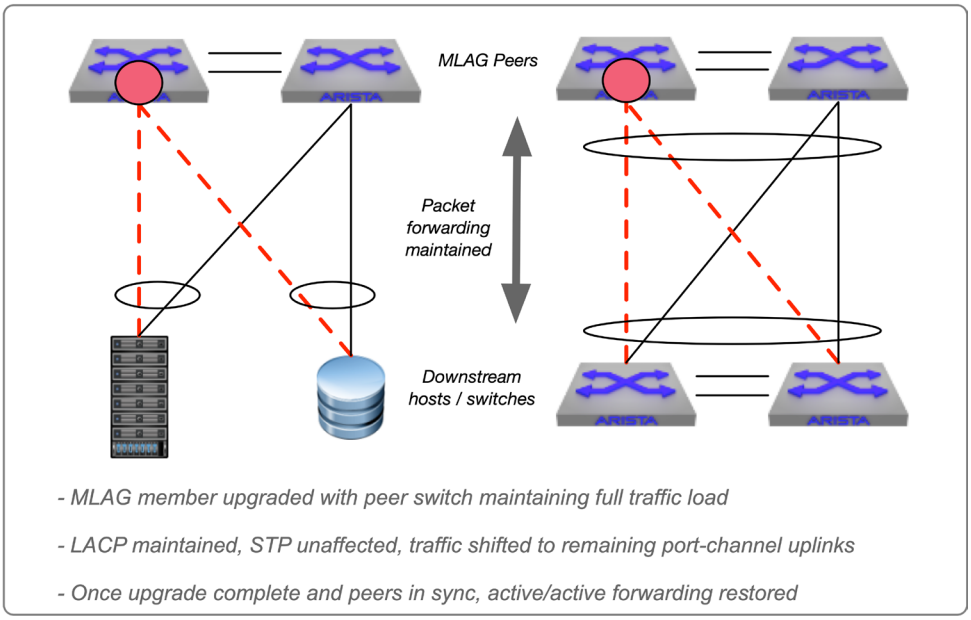
Spine switches act as the high-capacity backbone of the network topology. Spine upgrades leverage the Maintenance Mode feature built into EOS to gracefully isolate a spine switch from the active network. Through intelligent interaction with routing protocols like BGP, PIM and OSPF, Maintenance Mode signals to adjacent leaf switches to dynamically reroute traffic around the targeted spine. This is accomplished by systematically increasing route metrics or withdrawing routes, allowing the spine to be upgraded, restarted, or physically replaced without dropping active flows.



Spine Upgrade with Maintenance Mode

MLAG ISSU (Multi-Chassis Link Aggregation ISSU)

For hosts, servers, and downstream switches that are dual-attached using MLAG, Arista provides MLAG ISSU (Multi-Chassis Link Aggregation In-Service Software Upgrade). This process enables one member of an MLAG pair to undergo a complete software upgrade while the surviving peer seamlessly absorbs the full traffic load. MLAG ISSU operates sequentially across both peer switches, taking one switch offline temporarily shifts the LACP bundle to remaining active links of the peer switch without causing a Spanning Tree recalculation or host-level link failure. Once the upgraded switch returns, the MLAG pair resynchronizes and restores active/active forwarding before the process is repeated on the second peer.

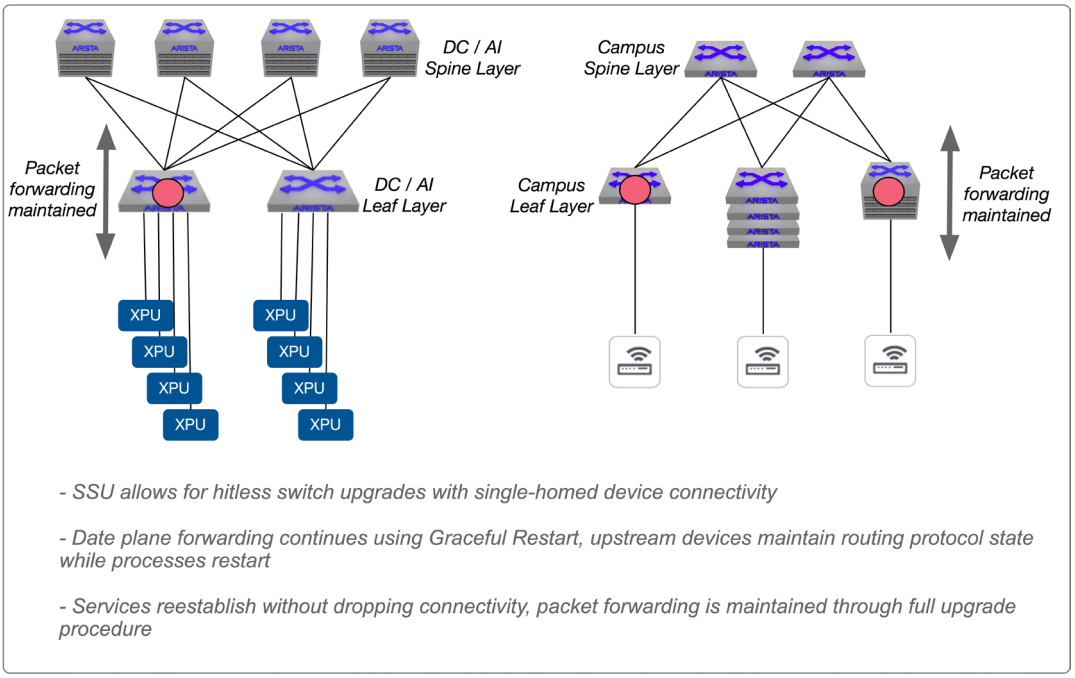


MLAG ISSU

Leaf SSU

Leaf switches sit at the edge of the fabric, connecting directly to end-hosts, hypervisors, storage arrays and AI accelerators in the Data Center, or access points and user devices in the Campus. Leaf SSU addresses the complexity of upgrading the network edge where downstream device connectivity is not dual-homed and redundant and minutes of downtime caused by a switch reload is an unacceptable operational outcome. By optimizing the software upgrade procedure in EOS, Leaf SSU guarantees uptime and lossless operations regardless of the device connectivity model (single-homed, dual-homed, LAG), removing the costly overhead of change control procedures due to planned downtime. In mission-critical environments such as hospitals or industrial settings where there is simply no availability of downtime at all, SSU unlocks the capability to completely mitigate risk and unlock access to new functionality, this includes continuous delivery of Power over Ethernet (PoE) during an upgrade. Similarly in AI fabrics where any form of downtime affects training Job Completion Time at significant cost, Leaf-SSU becomes a mandatory requirement.

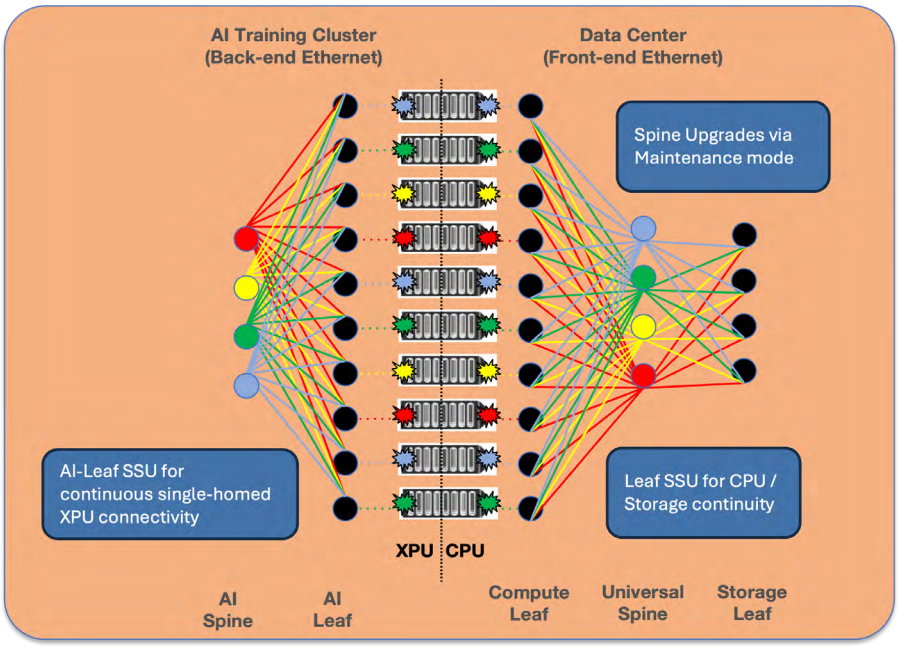
Leaf SSU streamlines and optimizes the upgrade process, significantly reducing the reload time. Even while the system reboots, Leaf SSU keeps network connections active by continuing to send LACP and STP control plane messages whilst maintaining data plane forwarding through protocols that support "graceful restart". This allows network services to reestablish without dropping connections, preventing interruptions to the data flow.



Leaf SSU

Smart System Upgrade For AI Fabrics

In the high-stakes environment of modern AI fabrics, where massive GPU clusters continuously process complex training models over weeks or months, network downtime directly translates to astronomical costs in idle compute and degraded Job Completion Times (JCT). Arista's Smart System Upgrade provides a critical advantage in these heavily utilized architectures by decoupling the switch's control plane from the data plane during the upgrade cycle. This architectural modularity ensures that the massive, sensitive flows of RoCEv2 (RDMA over Converged Ethernet) traffic remain uninterrupted while the underlying EOS is updated. By eliminating the need to drain switch traffic or halt operations for elusive maintenance windows, Leaf SSU empowers network operators to rapidly deploy vital security patches, routing enhancements, and AI-driven telemetry features without ever pausing the workload. Ultimately, this guarantees continuous utilization of expensive AI infrastructure and safeguards the seamless, lossless data transmission required for large-scale machine learning.



Smart System Upgrade for AI Networks

Fully Extending to the Cognitive Campus

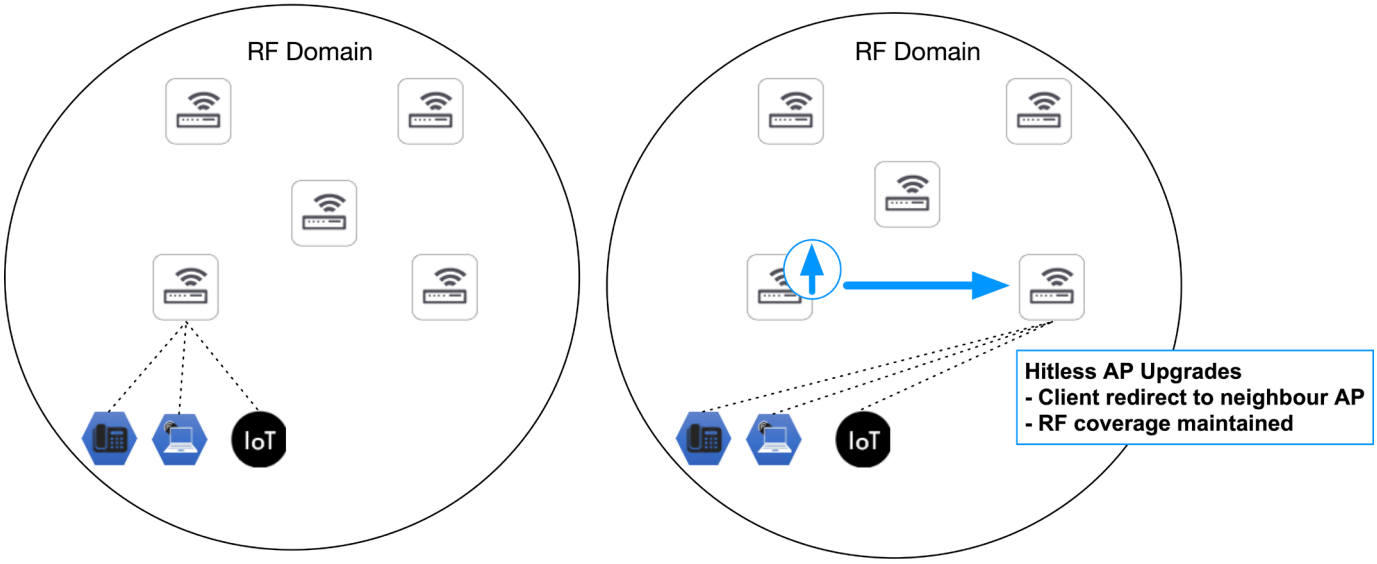
As enterprise networks evolve, the campus is no longer just a hub for basic user connectivity; it is the operational backbone for mission-critical industries. In healthcare environments, continuous network availability is quite literally a matter of life or death, underpinning real-time patient monitoring systems, mobile electronic health records (EHR), and critical telemetry devices. Similarly, in industrial and manufacturing sectors, the campus fabric drives automated assembly lines, precision robotics, and Industrial Internet of Things (IIoT) sensors, where even a brief disruption can result in massive production losses, stalled supply chains, or immediate safety hazards. For the hi-tech industry, high-performance campus environments must support rigorous R&D testing, continuous software delivery (CI/CD) pipelines, and the secure transfer of massive intellectual property datasets without interruption. Across all these highly demanding domains, hitless network operations and continuous availability are not just IT goals, they are absolute prerequisites for business continuity, innovation, and safety.

Campus networks operations of course extend into the similarly mission-critical wireless domain, Arista's hitless upgrade procedures cover access-point operations too.

Hitless Wi-Fi AP Upgrades

Arista's Hitless Wi-Fi AP upgrades eliminate network downtime during access point firmware updates by intelligently orchestrating upgrades to prevent coverage gaps. Traditional AP upgrades cause 3-5 minutes of downtime per device, which creates significant disruption in environments requiring continuous operations like hospitals and manufacturing facilities. Hitless upgrades address this by using RF neighborhood information to ensure only one AP in a given coverage area upgrades at a time, while neighboring APs continue serving clients. When an AP begins its upgrade, connected clients are automatically redirected to nearby access points without dropping their connections, then seamlessly reconnected once the upgrade completes.

The system works by creating dynamic RF neighborhood lists for each AP based on signal strength (typically -70 dBm minimum RSSI), continuously updating these lists throughout the upgrade process to adapt to changing conditions. This sequential, coordinated approach is particularly effective in dense Wi-Fi deployments with sufficient redundancy; the procedure leverages APs with scanning capabilities via a dedicated third radio to identify neighbors. Managed through CloudVision, Hitless Wi-Fi AP Upgrade can be enabled for both manual and scheduled upgrades across all Arista AP platforms, making it a key component of Arista's Cognitive Campus solution for organizations requiring 24/7 network availability.



Hitless Wi-Fi Upgrades

Multi-domain Orchestration: CloudVision Change Control and Upgrade Operations

Executing a network-wide upgrade effectively requires sophisticated orchestration to manage the sequential and parallel tasks necessary to achieve a hitless rollout. Arista CloudVision acts as the centralized Management Plane, aggregating metrics from all devices to provide insights into the overall health of the network. This provides operators with a full state history of the network for debugging transient or intermittent issues and underpins the orchestration of maintenance tasks.

Automating Smart System Upgrades with Change Control

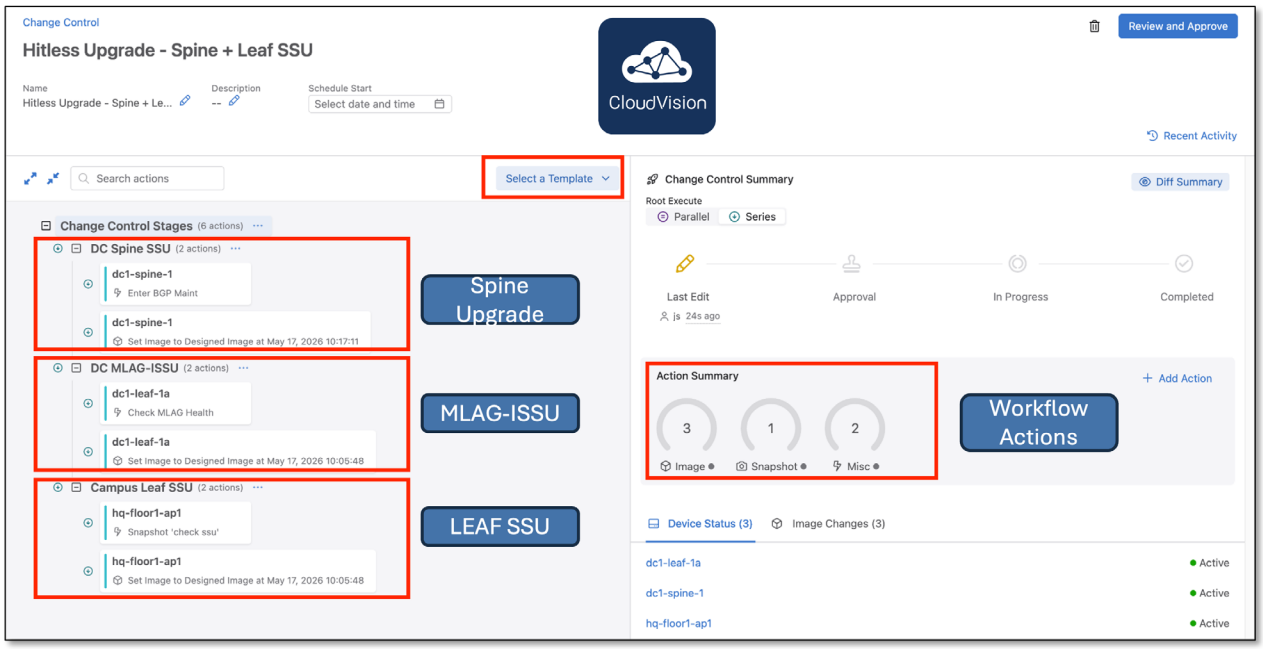
CloudVision incorporates a comprehensive Change Control framework designed to automate configuration updates, image upgrades and operations across the entire network topology. Instead of manually coordinating maintenance modes on individual switches, administrators can leverage CloudVision Change Control to orchestrate the entire process.

- Customizable Workflows: Change Control allows operators to build structured workflows that dictate the exact sequence of upgrade operations. Upgrades can be structured to proceed serially (e.g., upgrading one device at a time) or in parallel across different domains, fully integrated with EOS Maintenance Mode to ensure traffic is drained before a device is rebooted
- Pre- and Post-Validation Checks: Before initiating an upgrade, CloudVision can execute customizable pre-flight checks to verify network health, route counts, and connectivity states. After an upgrade operation completes on a node, post-flight checks validate that the device has successfully rejoined the network, re-established neighbor adjacencies, and resumed forwarding traffic properly before the workflow proceeds to the next device.
- Automated Rollback Mechanisms: If a post-validation check fails or an anomaly is detected, CloudVision can halt the Change Control workflow and optionally trigger an automated rollback to the previous known-good state, significantly reducing the risk associated with network-wide upgrades.
- Snapshot Views: CloudVision captures network state snapshots pre- and post-change control, empowering operators with rapid, side-by-side comparisons to definitively confirm the success of an upgrade or identify regressions.

Change Control Image Reload Options

Every software upgrade in CloudVision Change Control is executed as a Set Image action, providing several reload modes designed to minimize traffic disruption and downtime based on device roles and capabilities.

- **Smart System Upgrade (Leaf SSU):** Maintains control plane continuity and data plane forwarding by gracefully restarting the device. Within the Set Image action, administrators can configure fallback behaviors:
  - » *SSU Only:* Fails if any warnings or errors occur
  - » *SSU Only - Ignore Warnings:* Fails only if errors occur
  - » *SSU Preferred:* Reverts to a normal reload if any warnings or errors occur
  - » *SSU Preferred - Ignore Warnings:* Reverts to a normal reload only if errors occur
- **In-Service Software Upgrade (ISSU) for MLAG:** For MLAG pairs, administrators can select the Normal reload mode and stage "Check MLAG Health" actions before and after the Set Image action, ensuring image upgrades are completed in series while the peer handles traffic.
- **Maintenance Mode:** For standalone non Leaf-SSU compatible devices, upgrades gracefully drain traffic to ensure zero packet loss. This uses the Normal reload mode bracketed by "Enter BGP Maintenance Mode" and "Exit BGP Maintenance Mode" actions run in series.



CloudVision Automated Smart System Upgrade Workflows

Summary

Arista Smart System Upgrades are designed to address the most challenging IT workflows across AI fabrics, traditional data centers and enterprise and industrial campus networks. Combining protocol-based graceful shutdown, insertion, and unique redirection techniques, traffic can be diverted around the devices under maintenance, in the leaf / access layers, packet forwarding simply continues forwarding through the device upgrade with applications unaffected. Operations teams and network administrators now have the ability to perform seamless maintenance to any infrastructure element faster and smarter. Empowered by CloudVision, organizations can fully automate these upgrade operations, leveraging the consistent multi-domain capabilities to ensure continuous availability, verified stability, and robust operational agility.

Further Reading

Arista Tech Library (requires login)
https://tech-library.arista.com/solution_guides/ssu/

Arista EOS Documentation
https://www.arista.com/en/um-eos/eos-smart-system-upgrade

Arista Cloudvision Network Wide Upgrade
https://www.arista.io/help/articles/videos-network-wide-upgrade

Arista Cloudvision Upgrade Workflow Documentation
https://www.arista.io/help/articles/provisioning-configure-change-control-reload-options

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