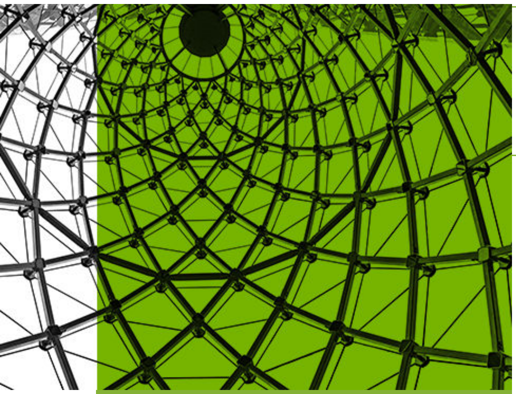

JUNIPER APSTRA

Product Overview

Juniper Apstra, a turnkey, multivendor automation solution, allows customers to design, build, deploy, and operate data center networks from a single pane of glass, simplifying and automating data center operations. Apstra provides a singular view into the relationships and interdependencies between millions of data center elements. With continuous real-time validation, Apstra enables you to instantly pinpoint and quickly resolve issues across all infrastructure silos, regardless of vendor or hardware.

Product Description

In this era of unprecedented change, people have changed how they work, live, and play. Digital transformation is underway everywhere, and data center traffic has increased at a rapid pace. To ensure business success, you need to adapt quickly to the changes coming all around you. To achieve that, Juniper® Apstra software transforms your data center network operations by providing simplicity, reliability, and multivendor support.

Juniper Apstra is a software-only, multi-vendor, intent-based networking solution that provides closed-loop automation and assurance to provide a complete fabric management solution.

Apstra translates business intent and technical objectives to essential policy and device-specific configuration, and it continuously self-validates and resolves issues to assure compliance. You specify the “what” (network topology, VLANs, desired capacity, redundancy requirements, access rules, and more), and Apstra delivers the “how.”

The Apstra software is installed as one or a set of virtual machines (VMs) to connect and manage devices via agents installed on or off the devices.

You can design your rack types and fabric network using Apstra templates. Details such as single/dual-homing of servers, collapsed/3-stage/5-stage style of fabric, Ethernet VPN (EVPN)/IP fabric, and IPv4/IPv6 underlay can be specified as part of the template type and options. Once the fabric template is completed, it can be instantiated into blueprints, each representing an actual physical network. The allocation of the managed devices and network resources (“build phase”) is done within the blueprints**.** As the blueprint is built, Apstra automatically produces the necessary configuration for devices, providing an abstraction layer across vendors. Apstra provides continuous validation against intent and policy assurance, and it identifies configuration drift in real time, confirming that security policies are enforced as intended. Once the user commits the changes, the incremental configuration is pushed to the Juniper, Cisco, Arista, or Dell-EMC devices**.**

Apstra manages the entire network life cycle, giving you the ability to easily expand and scale your network, as well as extract meaningful device telemetry. Apstra keeps your intent in check with the actual status of the network, providing you with actionable insights into your network to ensure that your goals are met.

Features and Benefits

Apstra offers the following features:

Intent-Based Network Design and Operations

Intent-based data center automation increases application availability and reliability, simplifies deployment and operations, and dramatically reduces costs for enterprises, cloud service providers, and telco data centers. As the only intent-based networking technology to be hardware- and device OS-vendor agnostic, Apstra delivers on the vision of complete end-to-end data center automation, integrating capabilities such as group-based policies, enterprise scale, and significant intent-based analytics enhancements.

Life-Cycle Management for Data Center Networks

Typically, architects design the network and operators manage it, resulting in a breakdown in information sharing and the absence of a single source of truth (SSOT). Architects are not aware of changes made to the network, and operators are not fully informed of the capabilities and known limits of the system. Apstra eliminates these issues by creating an SSOT in the intent datastore and tracking all network moves, additions, and changes. Not only does Apstra track changes made to the network by other systems, but it also provides simple workflows for implementing changes across the entire network.

Advanced Telemetry—Intent-Based Analytics

Operators frequently find themselves drowning in telemetry data collected by their managed systems. Apstra's intent-based analytics let you define expert-level rules and embed them into the network management system, ensuring that system checks are continuously running and updated immediately with any network changes.

Scalability in Small and Large Data Centers

Apstra was designed to handle the largest data centers in the world, supporting hundreds of thousands of connected servers. This is achieved through support for 3-stage or 5-stage Clos IP fabrics with EVPN-Virtual Extensible LAN (VXLAN) deployed as the overlay. Apstra also supports smaller fabric designs. In edge data centers, for example, only a couple of switches are deployed, but the number of deployments is large and highly distributed. Apstra can easily consolidate all operations across the edge data centers into a single management interface. Regardless of the number and scale of deployments, is focused on intent and on translating that intent to configuration. Operators can easily make changes to these roles, driving large-scale changes to configurations across multiple vendors and network designs. To satisfy these demands, Apstra is built with a high-throughput, highly scalable graph datastore that tracks all changes in real time, relieving the organization from having to manage individual IP addresses or configurations. This allows operators to focus on business-specific needs rather than low-level troubleshooting or reconfiguring of the network management system following every network change.

Intent Time Voyager

A key operational feature for any network operator is rapidly recovering from human error. This is typically a complex, vendor-specific process that requires a complete understanding of the full state of all boxes and their relationships to each other at certain points in time. The Intent Time Voyager feature speeds time to resolution by enabling the operator to move the entire state of the network (intent, configuration, and continuous validations) backward or forward with a few simple clicks, returning it to a specific point in time. This unique ability is enabled by its foundational intent-based approach, including its SSOT and assurance validations.

Data Center Interconnect

As networks expand and applications require greater geographic diversity, a number of vendor-specific proprietary features have been introduced to address stretched Layer 2 domains and active/active topologies. Apstra supports an industry-standard EVPN-VXLAN overlay that extends Layer 2 application segments outside of the Apstra-managed topology. This allows architects to integrate multiple disparate computing centers for effective load balancing, legacy migration, disaster recovery, or resource sharing.

Access List Policies Assurance

Apstra security policy provides a simple user interface and API that allows users to define policies to control the flow of traffic between virtual networks, IP endpoints, and routing zones. The policy is automatically applied as an L3 ACL on the relevant enforcement points, radically simplifying the management and reducing the size of access control lists. Furthermore, Apstra can detect conflicts when multiple policies are applied within a blueprint overlap and automatically resolve the conflicts based on user settings such as "more specific first" or "more generic first". Users can search existing policies based on source/destination object and by type of traffic (protocol and port number) to determine if a certain traffic flow is affected by any active policies.

Support for All Modern Network Platforms

Apstra offers the industry's first and only vendor-agnostic intent-based networking platform, allowing enterprises to design a network without consideration for the hardware platforms that will eventually be deployed. The tools used to design and manage the network are the same, regardless of which vendor hardware or network operating system is ultimately selected. This translates to a massive reduction in OpEx by eliminating the need to maintain staff expertise in multiple platforms and vendor nuances. There is also an opportunity to reduce CapEx by allowing all modern vendors to be considered for inclusion in an Apstra-managed environment.

VMware Integrations

Apstra tightly integrates with VMware NSX-T and VMware vCenter to provide network operators visibility into virtual workloads and networks. The built-in validation speeds up the troubleshooting of virtual networking, port-group/fabric VLAN/Link Aggregation Control Protocol (LACP) mismatch, and VM traffic issues. Remediation workflows help users resolve misconfiguration of VLANs faster by automatically suggesting the correct network fabric changes.

Flexible Connectivity

Apstra software offers flexible connectivity configuration options for servers, firewalls, and external routers. These connectivity options can be quickly attached to any port in the fabric, with deterministic configuration to ensure that all protocols are properly functioning. They leverage the Apstra graph model, providing integrated operational statistics and workflows tailored to the selected design.

Specifications

Network Design

- 3-stage and 5-stage Clos design
- Collapsed fabric design (Edge data centers)
- 3-stage Clos with L2 access switches
- High availability switches at the access layer
- IPv4 fabric (non-EVPN)
- IPv6 fabric RFC-5549 (non-EVPN)
- EVPN fabric
- Virtual routing and forwarding tables (VRFs)
- L2/L3 virtual networks (IPv4/IPv6)
- Intra-rack (VLAN), or inter-rack (VXLAN) virtual networks
- Single or dual homing of external systems (MLAG/vPC/CLAG/ESI)
- L3 sub-interfaces
- Dynamic Host Configuration Protocol (DHCP) relay
- External BGP peering
- Dynamic BGP neighbors
- Granular import/export routing policies
- Static routes
- Security policy (firewall filters/access control lists)
- Remote EVPN gateways for L2/L3 Data Center Interconnect (DCI)
- Cabling map: anti-affinity policies

Device OS

- Junos® operating system
- Junos OS Evolved
- Junos OS on Juniper vQFX virtual devices
- Cisco NX-OS and NX-OSv
- Arista EOS and vEOS
- Enterprise SONiC

Telemetry Services

- Address Resolution Protocol (ARP) table
- Media access control (MAC) table
- BGP session
- Hostname
- Interface and interface counters
- Transceiver information
- Link aggregation group/multichassis link aggregation group (LAG/MLAG) information

- Link Layer Discovery Protocol (LLDP) information
- MAC table
- Resource utilization
- Route table
- EVPN flooding table
- Active configuration

Intent-Based Analytics (IBA)

- Anomaly detection
- Real-time and historical
- Telemetry streaming via protocol buffers
- Extensible telemetry collection
- Custom dashboards and widgets
- Programmable
- Tags and property sets for custom probes
- IBA predefined probes
- Bandwidth utilization
- Critical services: utilization, trending, alerting
- Leafs Hosting Critical Services: utilization, trending, alerting
- Device system health
- Device traffic and headroom
- LAG imbalance
- ESI imbalance
- Equal-cost multipath (ECMP) imbalance
- EVPN-VXLAN type-3 route validation
- EVPN-VXLAN type-5 route validation
- VXLAN flood list validation
- EVPN host flaps detection
- BGP flapping detection
- Hot/cold fabric ports
- Interface flapping
- Multi-agent detector (Arista only)
- Total east-west traffic
- OS version
- Interface errors (overloaded interface bandwidth)
- Sustained interface discards
- Small form-factor pluggable transceiver (SFP)
- Display external routes
- Power supply anomalies probe
- Hypervisor and fabric VLAN configuration mismatch
- VMs without fabric configured VLANs
- Hypervisor and fabric LAG configuration mismatch
- Hypervisor missing LLDP configuration
- Hypervisor maximum transmission unit (MTU) mismatch
- Hypervisor MTU check
- Hypervisor redundancy check

Root-Cause Identification

- Connectivity fault model
- Cabling fault model
- Anomaly summarization

Platform

- Apstra server backup/restore
- Apstra server health reporting
- RESTful APIs
- Graph model and GraphQL/QE API
- Apstra CLI
- Apstra Developer SDK (Python)
- Extensible on-box or off-box device agents
- Multiuser administration
- Role-based access control
- Self-integrity check

Security

- Multiuser administration
- Role-based access control
- LDAP authentication
- TACACS+ authentication
- RADIUS authentication
- Active Directory authentication
- 802.1x Network Admission Control
- Traffic control with ACLs
- HTTPS UI
- Apstra server security hardening
- Headless operation

Blueprint Customization

- Template types and options
- Connectivity templates
- Configlets
- Property sets
- Tags management
- Resource pool management
- Day-2 rack modifications
- Day-2 fabric extension

Virtual Infrastructure Integration

- VMware vCenter
- VMware NSX-T

Day-2 Operations

- Staged/commit workflows
- Rollback network state (Intent Time Voyager)
- Add/remove generic systems
- Add/update/remove racks
- Add/remove pods
- Network OS upgrade/downgrade
- Change/add interface
- Break/form lags
- Device maintenance
- Device decommissioning
- Device replacement
- Virtual network management
- Policies management

Policy Assurance

- Configuration drift detection
- Access list policies—conflict detection and resolution
- Routing zone constraint policies

Device Management

- Zero-touch provisioning (ZTP)
- Device agent installer
- Life-cycle management
- Device quarantine
- Device maintenance

An open-source catalog of IBA probe configurations is available to enable an ecosystem with customers, partners, and other third parties.

Installation Requirements Hypervisors

- VMware ESXi
- QEMU/KVM for Ubuntu
- Microsoft Hyper-V

Ordering Information

Please contact your Juniper sales representative for information on ordering Juniper Apstra.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end-users. Our solutions deliver industry-leading insight, automation, security, and assurance to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability, and equality.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240 1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700

Driven by Experience™