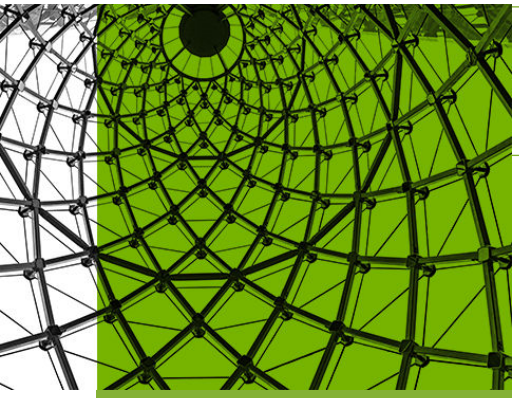

JUNIPER APSTRA DATASHEET

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

— continuous real-time validation that enables you to instantly pinpoint and quickly resolve issues across all infrastructure silos

— a complete fabric management solution, regardless of vendor, for single vendor and multivendor environments

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, multivendor, 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.

Support for All Network Designs

Apstra solves the deployment and operational complexity of next-generation data center networks by providing easy-to-deploy and highly validated fabric reference designs that can be used for any network size and cover multiple use cases. However, some data centers may require specific or out-of-the-box topologies, protocols, or architectures that are not addressed by these templates.

Apstra's "freeform reference design" allows you to build the design you want, how you want it. You can leverage any feature, protocol, or architecture that fits your deployment scenario. Freeform presents an interactive canvas to visually design or model any arbitrary network topology. The configuration is administered via Configuration Templates that grant you complete control over the configuration on the devices.

You can still leverage the same simple and powerful life-cycle management features from device operating system upgrades, simple device deployments, pre-deployment data center modeling, device telemetry, analytics dashboards, to powerful Intent-Based Analytics and Intent Time Voyager.

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, several 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.

Flow Data

Apstra Flow, a multivendor network observability solution for modern data centers, delivers unprecedented insights at any scale for network performance, availability, and security. Apstra Flow provides complete network visibility and in-depth analysis of traffic patterns so administrators can pinpoint the cause of a problem and resolve the issues. Having this extensive visibility optimizes network performance, enhances security, and improves capacity planning and cost control.

Apstra Flow provides granular information about network traffic flows, including source and destination IP addresses, ports, protocols, and the amount of data transmitted. When network administrators have this information, they can better understand the network's performance and identify potential issues such as congestion, high latency, or packet loss.

Network engineers can leverage the insights from Apstra Flow to implement strategies that optimize network traffic flow, reducing latency, balancing loads across network paths, and ensuring the most efficient use of available resources.

Apstra Flow's ability to enrich multivendor network traffic with organization-specific information enables more in-depth analysis and a better understanding of network traffic patterns, resource usage, and security risks. Apstra Flow, helps organizations improve their security posture; detect and respond to threats more effectively; and maintain compliance with regulatory requirements.

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 Fabric Design and 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. Apstra also supports complete flexibility in the fabric design via a "Freeform" template, to manage less conventional and/or legacy architectures.

Table 1: Features by Tier

Feature	Standard	Advanced	Premium	Connector for VMware
Network Design				
3-stage and 5-stage Clos design	X	X	X	
Collapsed fabric design (Edge data centers)	X	X	X	
3-stage Clos with L2 access switches	X	X	X	
High Availability switches at the access layer	X	X	X	
Freeform design (any network design)	X	X	X	
IPv4 fabric (non-EVPN)	X	X	X	
IPv6 fabric RFC-5549 (non-EVPN)	X	X	X	
EVPN fabric	X	X	X	
Virtual routing and forwarding tables (VRFs)	X	X	X	
L2/L3 virtual networks (IPv4/IPv6)	X	X	X	
Intra-rack (VLAN), or inter-rack (VXLAN) virtual networks	X	X	X	
Single or dual homing of external systems (MLAG/vPC/CLAG/ ESI)	X	X	X	
L3 sub-interfaces	X	X	X	
Dynamic Host Configuration Protocol (DHCP) relay	X	X	X	
External BGP peering	X	X	X	
Dynamic BGP neighbors	X	X	X	
Granular import/export routing policies	X	X	X	
Static routes	X	X	X	
Remote EVPN gateways for L2/L3 Data Center Interconnect (DCI)		X	X	
Integrated Interconnect/VXLAN Stitching (DCI)		X	X	
Mixed vendor fabrics (i.e. Fabrics with non-Juniper devices)			X	
Device OS				
Junos® operating system and vJunos-switch	X	X	X	
Junos OS Evolved and vJunosEvolved	X	X	X	
Cisco NX-OS and NX-OSv			X	
Arista EOS and vEOS			X	
Enterprise SONiC			X	
Telemetry Services				
Address Resolution Protocol (ARP) table	X	X	X	
Media access control (MAC) table	X	X	X	
BGP session	X	X	X	
Hostname	X	X	X	
Interface and interface counters	X	X	X	
Transceiver information	X	X	X	
Link aggregation group/multichassis link aggregation group (LAG/MLAG) information	X	X	X	
Link Layer Discovery Protocol (LLDP) information	X	X	X	
Resource utilization (disk, memory, CPU)	X	X	X	
Device Environmental Health (power supply, fan temperature, etc))	X	X	X	
Telemetry services health	X	X	X	
Custom Telemetry Collector (any additional telemetry)		X	X	
IP Route table	X	X	X	
Active configuration	X	X	X	
EVPN flooding table		X	X	
EVPN routing table		X	X	
Flow data (sFlow, NetFlow, IPFIX, and IFA)			X	
Intent-Based Analytics (IBA)				
Custom dashboards and widgets	X	X	X	
Programmable Probes	X	X	X	
Tags and property sets for custom probes	X	X	X	

Feature	Standard	Advanced	Premium	Connector for VMware
Device system health and environmental checks	X	X	X	
Device traffic and headroom	X	X	X	
LAG imbalance	X	X	X	
MLAG imbalance*	X	X	X	
ESI imbalance*	X	X	X	
Equal-cost multipath (ECMP) imbalance for fabric interfaces	X	X	X	
Telemetry streaming via protocol buffers*		X	X	
IBA predefined probes*		X	X	
Bandwidth utilization		X	X	
Critical services: utilization, trending, alerting*		X	X	
Leafs Hosting Critical Services: utilization, trending, alerting*		X	X	
Drain traffic anomaly		X	X	
Equal-cost multipath (ECMP) imbalance for spine to super spine interfaces*		X	X	
Equal-cost multipath (ECMP) imbalance for external interfaces		X	X	
Spine fault tolerance*		X	X	
EVPN-VXLAN type-3 route validation*		X	X	
EVPN-VXLAN type-5 route validation*		X	X	
VXLAN flood list validation*		X	X	
EVPN host flaps detection*		X	X	
BGP flapping detection		X	X	
Hot/cold fabric ports		X	X	
Hot/cold spine to super spine*		X	X	
Hot/cold specific interfaces		X	X	
Packet discard		X	X	
Interface flapping		X	X	
Total east-west traffic*		X	X	
Optical transceivers		X	X	
Display external routes*		X	X	
Connectivity fault model*		X	X	
Cabling fault model*		X	X	
Extensible telemetry collection*			X	
Multi-agent detector (Arista only)*			X	
Hypervisor and fabric VLAN configuration mismatch*				X
VMs without fabric configured VLANs*				X
Hypervisor and fabric LAG configuration mismatch*				X
Hypervisor missing LLDP configuration*				X
Hypervisor maximum transmission unit (MTU) mismatch*				X
Hypervisor MTU check*				X
Hypervisor redundancy check*				X
Platform				
Apstra server backup/restore	X	X	X	
Apstra server health reporting	X	X	X	
Apstra sever upgrades	X	X	X	
RESTful APIs	X	X	X	
API User Guides and API Explorer	X	X	X	
Graph model and GraphQL/QE API	X	X	X	
Apstra CLI	X	X	X	
Apstra Developer SDK (Python)	X	X	X	
Extensible on-box or off-box device agents	X	X	X	
Multiuser administration	X	X	X	
Role-based access control	X	X	X	

Feature	Standard	Advanced	Premium	Connector for VMware
Self-integrity check	X	X	X	
Security				
Multiuser administration	X	X	X	
Role-based access control	X	X	X	
LDAP authentication	X	X	X	
TACACS+ authentication	X	X	X	
RADIUS authentication	X	X	X	
Active Directory authentication	X	X	X	
HTTPS UI	X	X	X	
Apstra server security hardening	X	X	X	
API driven operation	X	X	X	
Blueprint Customization				
Template types and options	X	X	X	
Connectivity templates	X	X	X	
Configlets with granular scope (ex: interface level)	X	X	X	
Config templates (Freeform only)	X	X	X	
Property sets	X	X	X	
Tags management	X	X	X	
Resource pool management	X	X	X	
Day-2 rack modifications	X	X	X	
Day-2 fabric extension	X	X	X	
Day-2 Operations				
Staged/commit workflows	X	X	X	
Rollback network state (Intent Time Voyager)	X	X	X	
Add/remove generic systems	X	X	X	
Add/update/remove racks	X	X	X	
Add/remove pods	X	X	X	
Network OS upgrade/downgrade	X	X	X	
Change/add interface	X	X	X	
Turning interface up/down	X	X	X	
Break/form lags	X	X	X	
Device maintenance	X	X	X	
Device decommissioning	X	X	X	
Device replacement	X	X	X	
Resource utilization	X	X	X	
Virtual network management with bulk operations	X	X	X	
Policy Assurance				
Configuration drift detection	X	X	X	
Routing Zone constraint policies	X	X	X	
Access list policies—conflict detection and resolution			X	
802.1x Network Admission Control			X	
Traffic control with ACLs			X	
Policies management			X	
Cabling map: anti-affinity policies			X	
Security policy (firewall filters/access control lists)			X	
Device Management				
Universal zero-touch provisioning (ZTP) with Graphical User Interface	X	X	X	
Device agent installer	X	X	X	
Life-cycle management	X	X	X	
Device quarantine	X	X	X	
Device maintenance	X	X	X	

Feature	Standard	Advanced	Premium	Connector for VMware
Virtual Infrastructure Integration				
VMware vCenter				X
VMware NSX-T				X

*Probes marked are not available in Freeform design

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