DATA SHEET

ARUBA EDGECONNECT ENTERPRISE SD-WAN PLATFORM

As cloud-based application adoption continues to accelerate, geographically distributed enterprises increasingly view the wide area network (WAN) as critical to connecting users to applications.

As enterprise applications migrate from the corporate data center to the cloud, private line connections such as multi-protocol label switching (MPLS) have proven to be overly rigid and expensive. With greater reliance on the internet, the opportunity to achieve “cloud speed” is better served by integrating broadband services into the WAN transport mix.

Recently acquired from Silver Peak, the Aruba EdgeConnect Enterprise SD-WAN platform enables enterprises to dramatically reduce the cost and complexity of building a WAN by leveraging broadband to connect users to applications. By empowering customers to use broadband connections to augment or replace their current MPLS networks, Aruba improves customer responsiveness, increases application performance, and significantly reduces capital and operational expenses by up to 90 percent.

ARUBA EDGECONNECT ENTERPRISE SD-WAN PLATFORM

Three components comprise the Aruba EdgeConnect Enterprise SD-WAN platform:

• **Aruba EdgeConnect Enterprise** physical or virtual SD-WAN appliances (supporting any common hypervisors and public clouds) deployed in branch offices to create a secure, virtual network overlay. This enables customers to move to a broadband WAN at their own pace, whether site-by-site, or via a hybrid WAN approach that leverages MPLS and broadband internet connectivity.

• **Aruba WAN Orchestrator**, included with the Aruba EdgeConnect Enterprise SD-WAN platform, provides unprecedented levels of visibility into both legacy and cloud applications with the unique ability to centrally assign policies based on business intent to secure and control all WAN traffic. Policy automation speeds and simplifies the deployment of multiple branch offices and enables consistent policies across applications.

Moreover, customers can launch the Aruba WAN Orchestrator software directly from Aruba Central. Aruba Central provides the ability to view the enterprise-wide SD-WAN topology, health status, and alarms of all EdgeConnect Enterprise appliances in the SD-WAN in addition to other Aruba wired and wireless network devices.

• **Aruba WAN Boost** WAN Optimization is an optional WAN optimization performance pack that combines Aruba WAN optimization technologies with Aruba EdgeConnect Enterprise to create a single, unified WAN edge platform. Aruba WAN Boost allows companies to accelerate performance of latency-sensitive applications and minimize transmission of repetitive data across the WAN in a single, unified SD-WAN edge platform.

ARUBA EDGECONNECT ENTERPRISE KEY FEATURES

• **Business Intent Overlays**: Aruba EdgeConnect Enterprise is built upon an application-specific virtual WAN overlay model. Multiple overlays may be defined to abstract the underlying physical transport services from the virtual overlays, each supporting different QoS, transport, failover and security policies. Groups of applications are mapped to different business intent overlays to deliver applications to users in alignment with business requirements. Business intent overlays may also be deployed to extend micro-segmentation of specific application traffic from the data center across the WAN to help maintain security compliance mandates.
Path conditioning
Advanced network and application performance capabilities

• **Path Conditioning**: This feature provides private-line-like performance over the public internet. Includes techniques to overcome the adverse effects of dropped and out-of-order packets that are common with broadband internet and MPLS connections to improve application performance.

• **Packet order correction**: Reordering any out-of-sequence packets (POC)

First-packet iQ Application Classification:
EdgeConnect Enterprise First-packet iQ application classification identifies applications on the first packet to deliver trusted SaaS and web traffic directly to the Internet while directing unknown or suspicious traffic to the data center firewall or IDPS. Identifying applications on the first packet is especially important when branches are deployed behind Network Address Translation (NAT); the correct path must be selected based on the first packet to avoid session interruption.

Saas Express: Real-time updates on WAN path performance to reach, ensure that users connect to hundreds of Software-as-a-Service (SaaS) applications using the fastest path available. Automated daily updates of the application IP address database to Aruba EdgeConnect Enterprise appliances keep pace with SaaS and web address changes. Additionally, the SaaS Express feature uses synthetic polling reinforced by actual packet observations to continuously identify the best end-to-end path to reach a given SaaS application.

Secure Internet Breakout: Granular, intelligent traffic steering enabled by First-packet iQ eliminates the inefficiency of backhauling all HTTP/HTTPS traffic to the data center. The solution eliminates the potential for wasted bandwidth and performance bottlenecks for trusted SaaS and web traffic. Trusted traffic is sent directly across the Internet while unknown or suspicious traffic may be sent automatically to more robust security services in accordance with corporate security policies.

Unified Threat Management (UTM): The integration of Aruba Threat Defense with EdgeConnect Enterprise extends advanced intrusion detection and prevention (IDPS) capabilities to the SD-WAN fabric. Both physical and virtual instances of EdgeConnect Enterprise leverage Aruba threat infrastructure and threat feeds from Aruba Central, enabling enterprises to deliver east-west lateral security and secure internet breakout from branch office locations. Threat logging provides network and security analytics back to Aruba Central or a third-party SIEM such as Splunk to deliver comprehensive edge-to-cloud UTM capabilities.
• **Fine-grained Segmentation**: Aruba ClearPass integration with EdgeConnect Enterprise augments application intelligence with the user and device identity and role-based policy, enabling fine-grained segmentation. The additional identity-based context enables consistent security policy enforcement that can be enforced network-wide, from edge to the cloud, while also accelerating troubleshooting and problem resolution.

• **Zone-based Stateful Firewall**: Centrally visualize, define and orchestrate granular security policies and create secure end-to-end zones across any combination of users, application groups and virtual overlays, pushing configuration updates to sites in accordance with business intent. Using simple templates to create unique zones that enforce granular perimeter security policies across LAN-WAN-LAN and LAN-WAN-Data Center use cases.

• **Best-of-Breed Secure Access Service Edge (SASE)**: Aruba EdgeConnect Enterprise automates the integration with leading cloud security partner solutions from Zscaler, Netskope, Check Point, Palo Alto Networks, McAfee, Symantec and others to create a seamless secure access service edge architecture. Automated orchestration, using a drag-and-drop interface, enables IT to configure consistent enterprise-wide security policies based on business requirements.

• **Routing**: Aruba EdgeConnect Enterprise supports standard Layer 2 and Layer 3 open networking protocols such as VLAN (802.1Q), LAG (802.3ad), IPv4 and IPv6 forwarding, GRE, IPsec, VRRP, WCCP, PBR, BGP (version 4), OSPF.

• **High Availability**: The Aruba EdgeConnect Enterprise HA cluster protects from hardware, software and transport failures. High Availability is achieved by providing fault tolerance on both the network side (WAN) and on the equipment side. The Aruba EdgeConnect Enterprise appliances are inter-connected with a HA link that allows tunnels over each underlay to connect to both appliances.

• **Zero-Touch Provisioning**: A plug-and-play deployment model enables Aruba EdgeConnect Enterprise to be deployed at a branch office in seconds, automatically connecting with other Aruba EdgeConnect Enterprise instances in the data center, other branches, or in cloud Infrastructure as a Service (IaaS) such as Amazon Web Services, Microsoft Azure, Oracle Cloud Infrastructure and Google Cloud Platform.

• **WAN Hardening**: Each WAN overlay is secured edge-to-edge via 256-bit AES encrypted tunnels. No unauthorized outside traffic can enter the branch. With the option to deploy Aruba EdgeConnect Enterprise directly onto the internet, WAN hardening secures branch offices without the appliance sprawl and operating costs of deploying and managing dedicated firewalls.

**ARUBA WAN ORCHESTRATOR KEY FEATURES**

• **Single Screen Administration**: Enables quick and easy implementation of network-wide business intent policies, which eliminates complex and error-prone policy changes at every branch

• **Real-Time Monitoring and Historical Reporting**: Provides specific details into application, location, and network statistics, including continuous performance monitoring of loss, latency, and packet ordering for each enterprise customers’ network path. All HTTP and native application traffic are identified by name and location, and alarms and alerts allow for faster resolution of network issues

• **Bandwidth Cost Savings Reports**: Documents the cost savings for moving to broadband connectivity

Aruba WAN Orchestrator enables centralized definition and automated distribution of network-wide business intent policies to multiple branch offices.

**INTEGRATION WITH MICROSOFT AZURE VIRTUAL WAN (vWAN) AND AWS TRANSIT GATEWAY NETWORK MANAGER (TGNM)**

By integrating the Microsoft Azure vWAN and AWS Transit Gateway Network Manager (TGNM) REST APIs, the EdgeConnect Enterprise enables customers to quickly build a cloud on-ramp and automate network deployments, removing the manual complexity of connecting branch offices.
to local Azure or AWS Points of Presence (PoPs). The API integration enables Aruba EdgeConnect Enterprise to identify the locations of branches in the network and determine the closest VPN Gateway (vWAN hub or head-end gateway in AWS) to connect to. Aruba EdgeConnect Enterprise automatically establishes standards-based IPsec tunnels and, configuring both of the tunnel endpoints for each branch to a VPN Gateway.

Key Features:

- Automate branch connectivity to Azure and AWS Points of Presence (PoPs)
- Simplify network expansion and troubleshooting
- Faster onboarding to applications and workloads — both to and from Azure and AWS
- Optimized routing within Azure or AWS network
- Centralized Network Monitoring
- Global Network Visibility
- Cohesive policy configuration

DELIVERING THE HIGHEST QUALITY OF EXPERIENCE FOR MICROSOFT 365

With the Microsoft 365 REST API integration, Aruba continuously learns and discovers new Microsoft 365 end points and/or IP addresses and automatically re-configures Aruba EdgeConnect Enterprise if a new, closer Microsoft 365 end point becomes available. By doing so, users always achieve optimal Office 365 connectivity and performance by reducing the round-trip time (RTT). The EdgeConnect Enterprise has been independently tested and certified to support the Microsoft 365 Connectivity Principles. As a result of the independent testing, the Aruba EdgeConnect Enterprise platform has been inducted into the Microsoft Office 365 Networking Partner Program and has been given the official “Works with Microsoft 365” designation.

EXTEND WAN FABRIC TO THE CLOUD

Deploy virtual Aruba EdgeConnect Enterprise appliances in a public cloud such as AWS, Azure, Google Cloud Platform, or Oracle Cloud to optimize connections between branch locations and the cloud using all the SD-WAN benefits. If a brownout or blackout occurs, the remaining link(s) continue to carry traffic so that users don’t notice any disruption to voice calls, audio and video conferences, or any other application. Ruggedized first mile between the branch and the public cloud delivers better network performance, reliability, and quality.
ZERO TRUST: SECURING THE EDGE BY ROLE, CONTEXT, AND APPLICATION

With the increase in mobile devices, remote workers, cloud-hosted applications, and IoT connected devices, enterprises must align their security policies based on business intent while also striving for consistency. Aruba ClearPass integration with EdgeConnect Enterprise augments application intelligence with user and device identity and role-based policy, enabling fine-grained segmentation. This additional identity-based context enables consistent security policies that can be enforced network-wide, from edge to cloud, while also accelerating troubleshooting and problem resolution.

As a new user or device connects to the network and registers with ClearPass, the Aruba WAN Orchestrator (control plane for Aruba EdgeConnect Enterprise) connects via the ClearPass API. Aruba WAN Orchestrator propagates security policy information related to user, device type, role, and security posture to all EdgeConnect Enterprise appliances in the network.

Because IoT devices are agentless, it is not possible to run a third-party VPN or ZTNA client on them. Thus, a SASE architecture doesn’t fully address the security challenges posed by the IoT devices in the enterprise network.

With the Aruba ClearPass zero trust security framework, the network can identify and segment IoT devices and traffic at the network edge and isolate it from other traffic in the network. This new layer of context enables fine-grained segmentation without the complexity of managing multiple VLANs.

For example, a fine-grained segmentation policy can prevent IoT security cameras from accessing credit card transactions or HVAC systems. Zero trust dynamic segmentation helps enterprises isolate any potential security threats by device type, role, and application while helping them meet industry compliance requirements such as PCI, HIPAA, and SOX.

VIRTUAL ROUTING AND FORWARDING (VRF) SEGMENTATION

Network managers can configure and manage separate addressing, routing and security policies consistently with the EdgeConnect Enterprise across end-to-end segments and micro-segments for traffic traversing large-scale multinational enterprises and federations of independent companies. Advanced segmentation eliminates the arduous task of manually stitching together VRF, firewall and NAT policies in a consistent manner, dramatically simplifying the management of diverse scenarios and providing unprecedented flexibility when contending with overlapping IP address spaces.

SAAS EXPRESS

With SaaS Express, EdgeConnect Enterprise ensures that the application traffic is routed to the optimal SaaS entry point, even if it differs from the location’s default. Since SaaS applications constantly change, including the IP addresses used to access them, SaaS Express keeps a continuously updated SaaS application database. Aruba WAN Orchestrator polls and downloads the latest application updates daily from the database, including the most up-to-date IP addresses, and then shares this information with all the EdgeConnect Enterprise appliances. Through this process, all the appliances in the network receive the latest application definitions, and as applications change, appliances have the latest signatures that allow them to optimally steer traffic according to business policies.
Today many customers provision broadband service from different internet providers at a branch to transport SaaS traffic. However, maintaining and updating the identity of the best end-to-end path is challenging since the network still experiences variable packet loss or latency, slowing down the application.

The SaaS Express feature uses synthetic polling reinforced by actual packet observations to continuously identify the best path to reach a set of well-known applications to tackle this challenge. SaaS Express always finds the best possible end-to-end path to improve the application performance regardless of how the customer chooses to breakout the SaaS traffic.

Scenario 1, based on synthetic measurements, ISP2 is chosen because the latency experienced by this connection is 45ms, which is significantly lower than that experienced by ISP1.

Automated daily SaaS application updates with the most up-to-date IP address information ensure all appliances in the network have the latest application definitions to route accordingly.
For instance, in scenario 1, two ISPs are provisioned, and SaaS traffic is broken out locally from the branch. Based on synthetic measurements, ISP2 is chosen because the latency experienced by this connection is 45ms, which is significantly lower than that experienced by ISP1. However, if subsequent flows experience higher latency over ISP2, application traffic flows will be automatically switched to ISP1 to ensure optimal application performance.

In scenario 2, application traffic is steered through a cloud security provider for advanced inspection before being sent to the destination. The primary Atlanta cloud security POP is closer to the New York branch than the secondary Dallas cloud security POP. But the end-to-end path through the Atlanta POP has a higher latency than the path through the Dallas POP. Therefore, application traffic is automatically sent to the secondary Dallas POP to achieve superior application performance since end-to-end path latency is only 45ms.

**SPLUNK INTEGRATION**

Security information and event management (SIEM) tools help to proactively identify potential security threats and vulnerabilities before they have a chance to disrupt business operations and affect revenue. Aruba has introduced a custom application for Splunk, called Aruba EdgeConnect Security App. Easily downloadable from Splunkbase, this app leverages the network data provided by the Aruba EdgeConnect Enterprise SD-WAN platform with Splunk’s extensive investigation and visualization capabilities to deliver advanced security reporting and analysis. Compatible with both Splunk Enterprise and Splunk Cloud, the Aruba EdgeConnect Security App provides a dashboard view of all security event notifications stemming from EdgeConnect Enterprise devices. Using Splunk, IT can filter, sort, navigate, and view the collective security event notifications generated across the entire SD-WAN fabric, overall trends, and top talkers to help organizations pinpoint network events that warrant further investigation.
EFFICIENT DNS QUERY RESOLUTION
A critical step in the DNS proxy is to resolve the DNS query quickly. With Aruba EdgeConnect Enterprise, customers can reach DNS servers in close proximity to branch sites eliminating backhaul of the DNS request to the remote data centers where enterprise DNS servers are hosted. From the branch location itself, DNS requests can be made directly to Global DNS servers, which reduces the impact of latency in establishing a SaaS application session, thereby improving SaaS application performance.

SUPPORT FOR CUSTOM USER-DEFINED APPLICATIONS
Many organizations continue to support applications customized for or internal to the company that are hosted in the corporate data center. Such custom applications are critical for the enterprise and with the EdgeConnect Enterprise, customers can ensure optimal performance of these applications. From Aruba WAN Orchestrator, IT can easily configure a custom application definition that enables Aruba EdgeConnect Enterprise to identify it on the first packet.

ARUBA WAN ORCHESTRATOR ENABLES FASTER SD-WAN DEPLOYMENTS
Aruba WAN Orchestrator, included with Aruba EdgeConnect Enterprise for on-premise installations and available as an optional Aruba cloud-hosted service subscription, enables zero-touch provisioning of Aruba EdgeConnect Enterprise appliances in the branch. Aruba Orchestrator automates the assignment of business intent policies to ensure faster and easier connectivity across multiple branches, eliminating the configuration drift that can come from manually updating rules and access control lists (ACLs) on a site-by-site basis. Aruba WAN Orchestrator enables customers to:

• Avoid WAN reconfigurations by delivering applications to users in customized virtual overlays
• Align application delivery to business goals through virtual WAN overlays based on business intent
• Simplify branch deployments with Aruba EdgeConnect Enterprise profiles that describe the virtual and physical configuration of the location

In addition to centralized and automated control of the entire SD-WAN topology, Aruba WAN Orchestrator provides specific detail into WAN performance, including:

• Detailed reporting on application, location, and network statistics
• Continuous performance monitoring of throughput, loss, latency, jitter and packet ordering for all network paths
• Identification of all application traffic by name and location
• Alarms and alerts to visualize and prioritize software and hardware issues within the WAN allow for faster problem resolution
• Bandwidth cost savings report for documenting the cost savings of moving to broadband

GAIN CONTROL OVER THE CLOUD
Gain an accurate picture of how Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS) and are being used within your organization.

• Name-based identification and reporting of all cloud applications
• Tracking of SaaS provider network traffic
• Cloud Intelligence provides Internet mapping of optimal egress to SaaS services

EDGE TO CLOUD SECURITY
Advanced capabilities provide cloud-first enterprises with the control to centralize and automate security policy governance and safely connect users directly to applications. They enable distributed enterprises to centrally segment users, applications and WAN services into secure zones.

Aruba WAN Orchestrator enables centralized and automated overlay management.
and automate application traffic steering across the LAN and WAN in compliance with predefined security policies, regulatory mandates and business intent. For enterprises with multivendor security architectures, Aruba WAN Orchestrator offers seamless drag and drop service chaining to next-generation security infrastructure and services.

**BOOST APPLICATION PERFORMANCE AS NEEDED**

Aruba WAN Boost is an optional WAN Optimization performance that includes:

- Latency Mitigation: TCP and other protocol acceleration techniques are applied to all traffic, minimizing the effects of latency on application performance and significantly improving application response times across the WAN.
- Data Reduction: Data compression and deduplication eliminates the repetitive transmission of duplicate data. Aruba Boost inspects WAN traffic at the byte-level and stores content in local data stores. Advanced finger-printing techniques recognize repetitive patterns for local delivery. Data Reduction can be applied to all IP-based protocols, including TCP and UDP.

---

### Business intent overlays configured with Aruba WAN Orchestrator

<table>
<thead>
<tr>
<th>Apps, IaaS, PaaS</th>
<th>Circuits</th>
<th>Bonding + SLA</th>
<th>Topology</th>
<th>SaaS, Cloud, Internet Apps</th>
<th>Internet Policy &amp; Firewall</th>
<th>Overlay Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Real Time Overlay</strong></td>
<td>[Image]</td>
<td>High Availability</td>
<td>Loss: 1%</td>
<td>WebEx, zoom</td>
<td>Best Circuit + Local Firewall</td>
<td>FW Zone: Real Time QoS: Real Time Boost: Disabled</td>
</tr>
<tr>
<td>[Image]</td>
<td>[Image]</td>
<td>Loss: 1%</td>
<td>Latency: 400ms</td>
<td>zoom</td>
<td>Best Circuit + Local Firewall</td>
<td>Local Firewall</td>
</tr>
<tr>
<td>[Image]</td>
<td>[Image]</td>
<td>Loss: 1%</td>
<td>Latency: 400ms</td>
<td>zoom</td>
<td>Best Circuit + Local Firewall</td>
<td>Local Firewall</td>
</tr>
</tbody>
</table>

| **Enterprise Apps Overlay** | [Image] | High Quality | Loss: 2% | Office 365, Box, Slack, Zscaler | Best Circuit + Cloud Firewall | FW Zone: Restrict QoS: Enterprise Boost: Enabled |
| [Image] | [Image] | Loss: 2% | Latency: 600ms | Box, Slack | Best Circuit + Cloud Firewall | Datacenter (Backup) |

| **Default Overlay** | [Image] | High Efficiency | Loss: 5% | Facebook, YouTube, Netflix | Load Balance + Cloud Firewall | FW Zone: Default QoS: Best Effort Boost: Disabled |
| [Image] | [Image] | Loss: 5% | Latency: 800ms | Netflix, YouTube | Load Balance + Cloud Firewall | Datacenter (Backup) |

**WHY ADD ARUBA WAN BOOST?**

Aruba EdgeConnect Enterprise appliances alone provide enhanced application performance for broadband or hybrid WAN deployments, utilizing the included packet-based tunnel bonding, dynamic path control (DPC), and path conditioning for overcoming the adverse effects of dropped and out-of-order packets that are common with Internet connections.

However, sometimes additional performance is needed for specific applications or locations. As distance between locations increases over the WAN, application performance degrades.
This has less to do with the available bandwidth, and is more about the time it takes to send and receive data packets over distance, and the number of times data must be re-sent.

**ARUBA WAN BOOST USE CASE EXAMPLES**

- Customers replicating to a disaster recovery (DR) site thousands-of-miles away might want to add Aruba WAN Boost to ensure recovery point objectives (RPOs) are not compromised.
- Enterprises with remote sites located in rural areas, or with sites that are exceptionally farther away from the company's data center, might want to add Aruba Boost to overcome the effects of high latency.

With Aruba WAN Boost, customers gain the flexibility to enable enhanced WAN optimization capabilities where and when it is needed in a fully integrated solution. Aruba Boost is licensed per-megabit-per-second, per-month, so customers do not have to pay for WAN optimization across the entire network.

**OVERCOME EFFECTS OF LATENCY**

The time it takes for information to go from sender to receiver and back is referred to as network latency. Since the speed of light is constant, WAN latency is directly proportional to the distance traveled between the two network endpoints. Aruba offers a variety of TCP acceleration techniques to mitigate WAN latency, including Window Scaling, Selective Acknowledgement, Round-Trip Measurement, and High Speed TCP.

Windows and other applications that rely on the Common Internet File System (CIFS) often take longer to perform common file operations over distance, such as retrieving and sharing files. Aruba WAN Boost helps these applications not only by improving the underlying TCP transport, but also by accelerating CIFS through CIFS read-ahead, CIFS write-behind, and CIFS metadata optimizations.

**INCREASE THROUGHPUT**

As packets flow through Aruba EdgeConnect Enterprise appliances, Aruba WAN Boost inspects WAN traffic at the byte-level and stores content in local data stores. As new packets arrive, Aruba computes fingerprints of the data contained within the packets, and checks to see whether these fingerprints match data that is stored locally.

If the remote appliance contains the information, there is no need to resend it over the WAN. Instead, specific start-stop instructions are sent to deliver the data locally.

"One-click" on-demand WAN optimization with Aruba Boost accelerates applications and maximizes available bandwidth for other applications.
## ARUBA EDGECONNECT ENTERPRISE HARDWARE PORTFOLIO

<table>
<thead>
<tr>
<th>Model</th>
<th>EdgeConnect Enterprise US</th>
<th>EdgeConnect Enterprise XS</th>
<th>EdgeConnect Enterprise S-P</th>
<th>EdgeConnect Enterprise M-H</th>
<th>EdgeConnect Enterprise L-H</th>
<th>EdgeConnect Enterprise XL-H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typical Deployment</td>
<td>Small Branch/ Home Office</td>
<td>Small Branch</td>
<td>Large Branch</td>
<td>Head Office/DC Large Hub</td>
<td>Data Center Large Hub</td>
<td>Data Center Large Hub</td>
</tr>
<tr>
<td>Typical WAN Bandwidth**</td>
<td>1–200 Mbps</td>
<td>2–1000 Mbps</td>
<td>10–3000 Mbps</td>
<td>50–5000 Mbps</td>
<td>2–10 Gbps</td>
<td>2–10 Gbps</td>
</tr>
<tr>
<td>Simultaneous Connections</td>
<td>256,000</td>
<td>256,000</td>
<td>256,000</td>
<td>2,000,000</td>
<td>2,000,000</td>
<td>2,000,000</td>
</tr>
<tr>
<td>Recommended WAN Boost up to</td>
<td>25 Mbps</td>
<td>250 Mbps</td>
<td>500 Mbps</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
<td>5 Gbps</td>
</tr>
<tr>
<td>Redundancy/ FRUs</td>
<td>No</td>
<td>No</td>
<td>SSD and Power (AC or DC)</td>
<td>SSD and Power</td>
<td>SSD and Power</td>
<td>SSD, NVMe, Power</td>
</tr>
<tr>
<td>Data Path Interfaces</td>
<td>3 x RJ45 10/100/1000</td>
<td>4 x RJ45 10/100/1000</td>
<td>8 x RJ45 4 x 1/10G Optical</td>
<td>8 x RJ45 4 x 1/10G Optical</td>
<td>6 x 1/10G Optical</td>
<td>6 x 1/10/25G Optical</td>
</tr>
</tbody>
</table>

*EC-XL-H comes pre-equipped with NVMe for maximum WAN optimization (Boost)
*EC-M-H, EC-S-P, EC-L-H, and EC-XL-H all support pluggable optics
*See software compatibility table for minimum software releases required to support the new EC-H models
**WAN Bandwidth assumes bidirectional traffic (symmetric up-link and down-link). For total WAN throughput (Rx+Tx), multiply these numbers by 2.
***For best performance, EdgeConnect Enterprise Operating System Release 9.1 or higher is recommended

---

## ARUBA EDGECONNECT ENTERPRISE SD-WAN PLATFORM SPECIFICATION SHEETS

- **ULTRA-SMALL**
- **EXTRA-SMALL**
- **SMALL**
- **MEDIUM**
- **LARGE**
- **EXTRA-LARGE**

### ARUBA EDGECONNECT ENTERPRISE TECHNICAL SUPPORT

<table>
<thead>
<tr>
<th>Term</th>
<th>Support is included as part of the Aruba EdgeConnect Enterprise subscription license</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web-based support portal</td>
<td>Unlimited access 24 / 7 / 365 includes software downloads, technical documentation, and online knowledge base</td>
</tr>
<tr>
<td>Software updates</td>
<td>Major and minor features releases; maintenance releases</td>
</tr>
<tr>
<td>Technical support</td>
<td>24 / 7 / 365 phone / e-mail / web (Global Technical Assistance Centers — TAC)</td>
</tr>
<tr>
<td>Response time</td>
<td>30 minutes for high priority (P1) — critical</td>
</tr>
<tr>
<td>HW warranty and maintenance</td>
<td>Refer to the Aruba EdgeConnect Enterprise warranty and maintenance policies data sheet for further information</td>
</tr>
</tbody>
</table>
FLEXIBLE DEPLOYMENT MODELS

- Aruba EdgeConnect Enterprise Virtual (EC-V) — Download and install Aruba EdgeConnect Enterprise from anywhere in the world. The software runs on all common hypervisors, including VMware ESXi, Microsoft Hyper-V, Citrix XenServer, and KVM. Aruba customers who have an IaaS presence in AWS, Microsoft Azure, Oracle Cloud Infrastructure or Google Cloud Platform can deploy Aruba EdgeConnect Enterprise within their hosted cloud environment.

- Aruba EdgeConnect Enterprise Physical (EC) — For enterprises that are not virtualized in the branch, choose one of the Aruba EdgeConnect Enterprise hardware appliance models for plug-and-play deployment.

ARUBA EDGECONNECT ENTERPRISE SUBSCRIPTION LICENSING

Aruba EdgeConnect Enterprise licenses are sold as a subscription, in either single or multi-year increments (1, 2, 3, 4 and 5 years) at multiple bandwidth tiers.

Aruba EdgeConnect Enterprise includes Aruba WAN Orchestrator that can be installed either on premise or in a customer’s virtual private cloud. An optional cloud-hosted Aruba WAN Orchestrator license provides a highly reliable alternative deployment model supporting all Aruba WAN Orchestrator features without the complexity of managing on premise virtual compute and storage resources. Large global enterprises with multiple business units (BU) or subsidiaries that have a requirement to support different regional QoS or security policies can optionally deploy Aruba WAN Orchestrator Global Enterprise. This cloud-hosted SaaS application centrally manages and monitors multiple Aruba EdgeConnect Enterprise SD-WAN fabrics.

Aruba WAN Boost is an optional WAN optimization performance pack that may be ordered and deployed flexibly to sites that require application acceleration. Aruba WAN Boost is offered in 100Mbps or 10Gbps blocks.