DANZ Monitoring Fabric™

Simple, Scalable, Economical

Arista Networks

Our mission is to deliver next-generation data center networking and monitoring solutions — enabling enterprises to realize the benefits of simplified productivity, improved scalability, and pervasive security with a dramatically improved TCO.

DANZ Monitoring Fabric is a next-generation network packet broker (NPB) architected for pervasive, network visibility delivering real-time and historical insights into your physical and virtual environments.

DANZ Monitoring Fabric Overview

DANZ Monitoring Fabric (DMF) is the industry's first network packet broker (NPB) that leverages an SDN-controlled fabric using high-performance, merchant-silicon switches, and industry-standard x86 servers to deploy highly scalable, agile, and flexible network visibility and security solutions. Traditional box-based, hardware-centric NPBs are architecturally constrained to meet emerging security and visibility demands of cloud-native data centers. DMF addresses the challenges of traditional NPB solutions, by enabling a scale-out fabric for enterprise-wide security and monitoring, a single pane of glass for operational simplicity, and multi-tenancy for multiple IT (NetOps, DevOps, SecOps) teams.

Architecture: SDN Software powered Pervasive Network Visibility

DMF's architecture is inspired by Hyperscale Networking designs, which consist of merchant-silicon switch hardware, SDN controller software, and centralized tool deployment.

The DMF architecture consists of the following components:

- High-availability pair of SDN-enabled DMF controllers — VMs or hardware appliances — that enable centralized configuration and simplified monitoring and troubleshooting.
- Merchant-silicon switches - Leverages high-performance, production-grade switches from Arista, Dell and Accton.
- DMF Service Node (optional). DPDK-powered, x86-based appliance that connects to the DMF fabric (either singly or as part of a service-node chain) to provide advanced packet functions like deduplication, packet slicing, header stripping, regex matching, packet masking, UDP replication, and IPFIX/NetFlow generation.
- DMF Recorder Node (optional). x86-based appliance that connects to the DMF fabric, managed by the controller to provide petabyte packet recording, querying, and replay functions.
- DMF Analytics Node (optional). x86-based appliance that integrates with the DMF fabric to provide multi-terabit, security, and performance analytics with configurable historical time-series dashboards.

АО Акметрон akmetron.ru

DMF utilizes the underlying cost efficiencies of the high performance, merchant-silicon switches, as well as the industry-standard x86 based appliances.

Significant CAPEX/OPEX Savings

The DMF enables a high-performance, integrated NPB + analytics + packet capture solution that supports rapid detection and analysis of network performance and security anomalies. DMF leverages merchant-silicon switches and commodity hardware to provide significant savings, both capital and operational. By contrast, the traditional NPB-based approach has high TCO due to ever-expanding box-by-box deployment, proprietary NPB hardware, and under-utilization of tools or inefficient use of them due to organizational silos.

Open, Industry-Standard Hardware Economics

DMF utilizes the underlying cost efficiencies of the high performance, merchant-silicon switches, as well as the industry-standard x86 based appliances. As a result, DMF is much more cost-effective for pervasive, scale-out monitoring.

SDN-Enabled Operational Efficiencies

DMF is provisioned and managed through the single pane of glass, thanks to the DMF controller CLI, GUI or REST APIs. This operating model allows for easier integration with existing management systems and monitoring tools. This SDN approach hence significantly reduces the operating costs associated with box-by-box management of traditional NPBs.

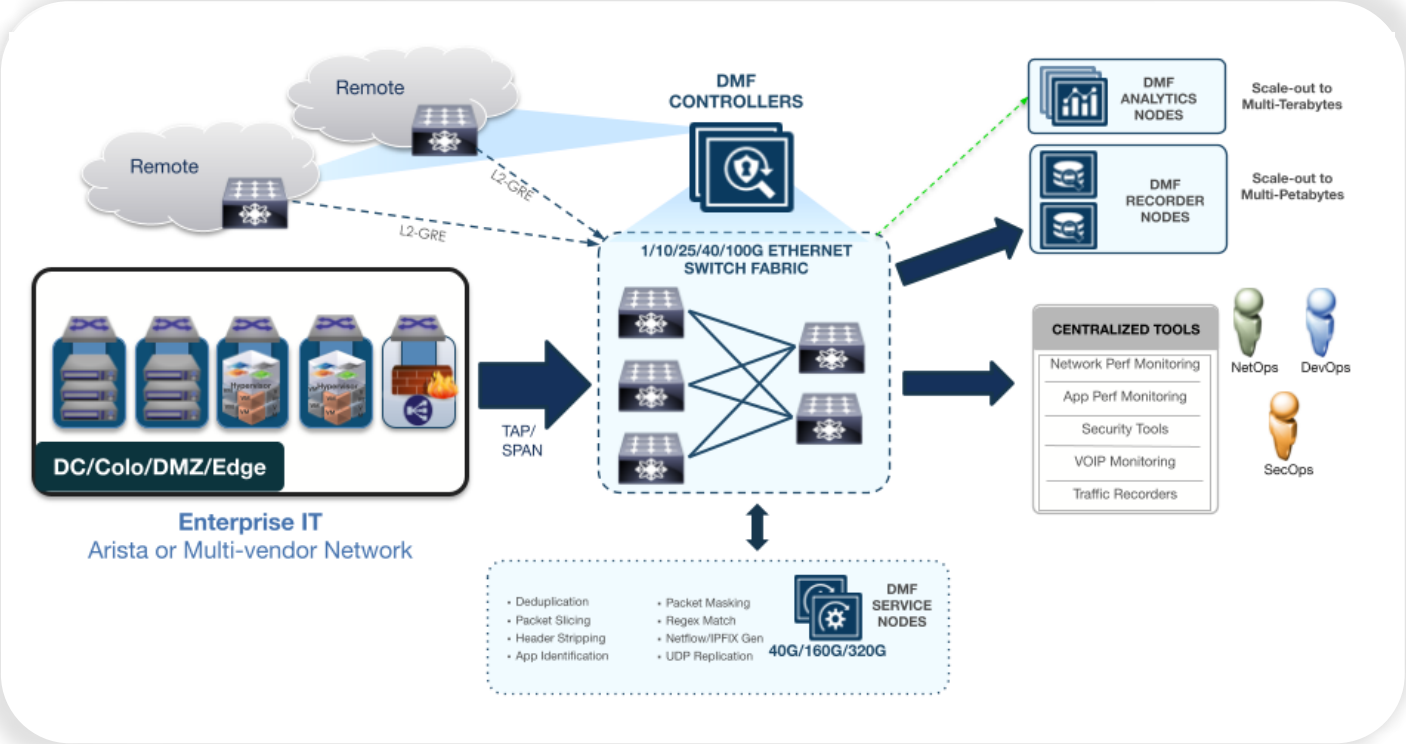

Figure 1: DANZ Monitoring Fabric (DMF) Architecture

DANZ Monitoring Fabric Product Description

DMF switches are deployed adjacent to the production network by connecting to SPAN / TAP ports from the production network.

The DMF controller serves as the single, central point of management for all deployed switches. The controller enables pervasive security and visibility for physical, and virtual workloads for single, and multi-site deployments.

DMF provides both basic and advanced NPB functions. In addition to basics such as filtering, aggregation, replication, and load-balancing, it also provides advanced packet functions like deduplication and packet slicing. DMF's advanced functions leverage the DPDK-powered, x86-based service nodes, supported by unique multi-tenant, monitoring-as-a-service functions on a scaled-out switch fabric managed centrally by the DMF controller. DMF Controller also integrates with x86-based analytics and recorder nodes to capture cloud-native data center traffic at scale. The nodes also support deep application-level analytics. The DMF Recorder Node allows high-performance packet recording, querying, and replay functions. The DMF Analytics Node provides unprecedented network visibility to monitor, discover, and troubleshoot network and application performance issues, as well as accelerate the discovery of root causes of security breaches. With DMF Recorder and Analytics nodes, users can achieve deep network telemetry for traditional data center environments. With these tools, the network team can replay past conversations across users and applications with a single click.

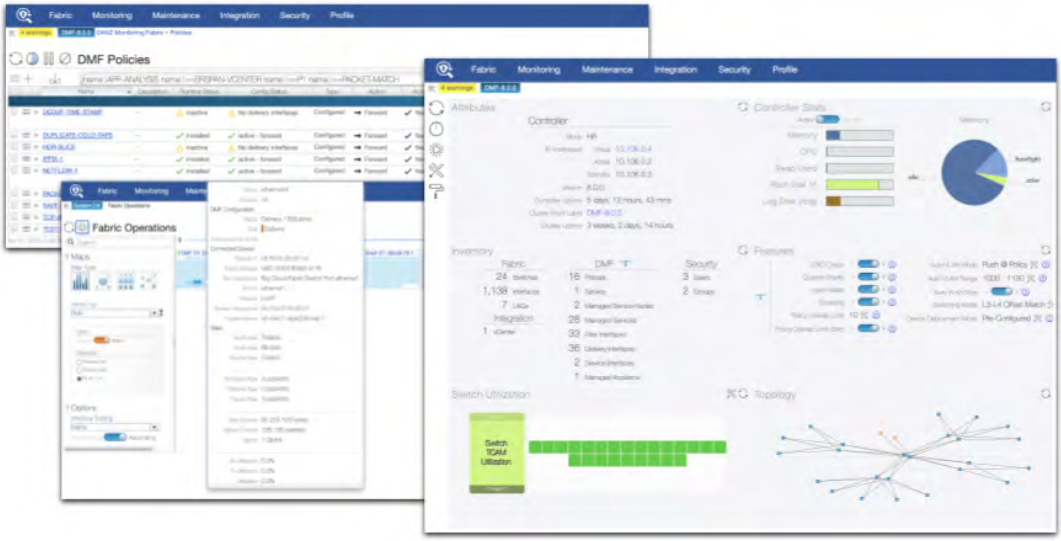

Figure 2: DANZ Monitoring Fabric Graphical User Interface (GUI)

Datacenter networks are transitioning to modern 10G/40G, 25G/100G, and 40G/100G designs to meet the demands of cloud computing, data analytics, and 4G/5G LTE mobile services. The corresponding traffic monitoring networks also need to transition to next-generation designs. The exponential growth in data center size, bandwidth, and traffic and the demand for monitoring a greater portion of network traffic together test the limits of traditional monitoring/visibility designs. The traditional box-by-box approach based on proprietary network packet brokers (NPBs) has proven to be cost-prohibitive and too operationally complex for organization-wide monitoring.

With DMF scale-out architecture, simplified operations, and open switch economics, DMF is rapidly becoming an attractive alternative to legacy NPBs. Two popular use cases have emerged:

- Pervasive security and visibility: monitor or secure every link.
- Multi-site Monitoring: monitor or secure remote DCs/POPs/ branches/sites/environments.

DMF supports topology agnostic, highly scalable fabrics. Depending on the customers' requirements, a range of topologies is supported—from a single-switch fabric to a scale-out, multi-switch/ multi-layer fabric. A typical multi-layer DMF fabric design has a layer of switches labeled as filter switches and a layer of switches labeled as delivery switches. Most switch interfaces in the filter-switch layer are wired to passive optical taps or switch/router/ firewall SPAN ports in the production network; they are configured as filter interfaces in the DMF controller software user interface. Switch interfaces in the delivery-switch layer are wired to tools and are configured as delivery interfaces. Filter interfaces (where packets come into the fabric) and delivery interfaces (where packets go out of the fabric to tools) represent the primary functions of DMF.

Monitor every location: Enterprises can extend DMF across L3 WAN to enable monitoring of remote DCs/POPs, colo facilities, campus/branch locations, and retail environments. This allows centralized monitoring tools and staff in a few data centers, dramatically reducing CapEx and Opex while empowering operations teams to monitor networks across the entire organization. By simply deploying a commodity Ethernet switch at each monitored location, the entire DMF (including remote location switches) is operated and managed centrally via the DMF controller with high availability.

Feature	Description / Benefit
Advanced Filtering & Deeper Packet Matching Capabilities	• L2/L3/L4 header filtering on ingress and packet replication (as required) in the fabric for multiple egress tools. • Deeper Packet Matching (DPM) with masking (up to 128 bytes in packet). Supports matching on inner header fields for encapsulated packets (e.g MPLS, VXLAN, GRE) and/or protocols (e.g. GTP, SCTP). • IPv4 and IPv6 based filtering. • IPv4, IPv6, MAC Address masking, TCP Flags, DSCP matching. • Support filtering on inner VLAN of a Q-in-Q packet • Support PTP timestamping the packets
Specialized Packet Functions	• Packet De-duplication—Enhances tool efficiency, by dropping duplicate packets. • Packet Slicing—Improves security and tool throughput by stripping off the payload. • TCP Session Slicing - Improves tool throughput by forwarding only a few packets at the beginning of the TCP session. • Packet Masking—Improves security by hiding user/confidential information such as Credit card, SSN, passwords, medical or financial data to comply with SOX, HIPAA, and PCI regulations. • Regex Pattern matching—Improves filtering of traffic based on regex patterns anywhere within the packet. • Header stripping for VXLAN, Cisco Fabric Path, LISP, GENEVE, PPPoE, ERSPAN, and MPLS packets. A generic user-defined header stripping function is also supported.

АО Акметрон akmetron.ru

Feature	Description / Benefit
Specialized Packet Functions (Contd.)	• IPFIX/Netflow/sFlow Generation Function is also supported. • Flow-diff calculates latency (based on PTP timestamps) between any two specified points in the network. • L2GRE tunnel packet decapsulation. • VLAN tag stripping—Useful for stripping RSPAN tag. • VLAN tag push—Useful for filter interface tagging. • Match on inner packet post stripping. • UDP Replication – Supports replication of UDP packets like NetFlow, IPFIX, sFlow, Syslog, and SNMP and sends them to multiple, different collectors • Additional specialized packet functions (like SSL decryption) can be realized by service chaining 3rd party NPBs as service nodes
Virtual Workload Monitoring (VM)	• Support scalable, agentless monitoring of Virtual Machines. • Support centralized, dynamic VM monitoring.
DMF Recorder Node	• Enables Traffic Capture for Cloud-Native Network Defense & Rapid Remediation at Scale • Leverages easy-to-use, scale-out, high-performance industry-standard x86 based appliances • Integrated/centralized configuration and operational workflows via DMF Controller • Feature-rich capturing, querying, and replay functions • Supports L4 payload file extraction from recorded packets • Supports packet deduplication on query • Supports PTP / NTP based timestamping • Programmable and scriptable via REST APIs
DMF Analytics Node	• Leverages easy-to-use, scale-out, high-performance industry-standard x86 based appliances. • Enables pervasive visibility for real-time and historical data delivering a Network Time machine. • Machine Learning and Application Dependency maps provide deeper insights and rapid remediation. • Supports various health/capacity planning/troubleshooting dashboards. • Supports network performance views like Top Talkers, Top Apps, TCP connection/ latency tracking. • Supports Security views identifying rogue DHCP/DNS servers, identifies IP/MAC spoofing. • Support various host views such as New Hosts seen and what OS is on the hosts. • Supports automatic alerting on exceeding various thresholds such as link utilization. • Supports sFlow/NetFlow collection to provide real-time visibility, including tunneled or encapsulated traffic, enable detection of security attacks like DoS/DDoS and support sub-second triggering. • Supports integration with Infoblox IPAM to import extensible attributes • Supports ingestion of Kafka topics

АО Акметрон akmetron.ru

Feature	Description / Benefit
Pervasive Visibility (Monitor or Tap Every Rack)	• Packet filtering, aggregation, tool port load-balancing, and packet replication functions. • Single switch or scale-out 1/2/3 layer fabric designs: 1G, 10G, 25G, 40G, 100G and 400G. • Centralized fabric/policy definition and instrumentation of open Ethernet switches within the network. • Programmatic event-triggered monitoring (via REST API). • Multiple overlapping match rules per filter interface based on a variety of L2, L3, L4 header, as well as via deeper packet matching (DPM) attributes. • Time/packet-based scheduling of policies. • Efficient utilization of open Ethernet switch capabilities via Controller Policy Optimizer Engine.
High Performance, Highly Scalable Network Monitoring Fabric	• Resilient architecture for High Availability and disaster recovery use cases. • Auto Fabric Path Computation that detects and responds to failures in the monitoring network. • Policy-based load balancing of core links with failover detection to efficiently utilize fabric bandwidth and ensure resiliency. • Detection of service node/link failure and an option to bypass the service. • Link aggregation (LAG) in the open Ethernet fabric (including across core links, service node links, and delivery links). • Tagging policy or tap (filter) interfaces. • Supports a variety of security and monitoring tool vendors. • Supports a variety of NPBs as stand-alone or chained service nodes.
Centralized Management, Configuration, Troubleshooting	• DMF Controller is the single pane of glass for fabric and policy management. • Policies can be configured from a centralized controller to forward flows from multiple filter interfaces to multiple delivery interfaces, including optional service nodes. Packet replication is made at the last common node to optimize the fabric bandwidth. • GUI, REST API, and CLI for configuration and viewing operational state. • Centralized interface, flow, and congestion-statistics collection. • Simplified install/upgrade of the fabric via the DMF Controller (zero-touch fabric). • Supports Ansible-enabled automated workflows to backup configs, reset the entire deployment to factory default, and rebuild the DMF fabric with the Golden config. • Supports virtual IP addresses for the controller high-availability pair.
Multi-DC/Multi-Site Tunneling (Tap Every Location)	• Centralized monitoring of remote DCs/POPs/branches/sites (across L3 WAN). • Support tools located in a single tool farm in a centralized DC. • Replication of packets across tunnels. • Tunneling at 1G, 10G, 25G, 40G,100G and 400G bandwidths. • Rate limiting of monitored traffic before entering L3 WAN. • Tunneling enabled on a per-switch basis.

Feature	Description / Benefit
Multi-DC/Multi-Site Tunneling (Tap Every Location)	• Centralized monitoring of remote DCs/POPs/branches/sites (across L3 WAN). • Support tools located in a single tool farm in a centralized DC. • Replication of packets across tunnels. • Tunneling at 1G, 10G, 25G, 40G,100G and 400G bandwidths. • Rate limiting of monitored traffic before entering L3 WAN. • Tunneling enabled on a per-switch basis.
Security and Controlled Access (Monitoring as a Service)	• TACACS+, RADIUS-based authentication and authorization. • Role-based access control (RBAC) for administratively defined access control per user. • Multi-tenancy for advanced overlapping policies across multiple user groups to monitor the traffic from the same tap interface to various tool interfaces. • Tenant-aware Web-based management GUI, CLI, and REST API. • Self-service monitoring across multiple groups/business units using the same underlying infrastructure.
Fabric wide CRC check (Graphical User Interface)	Allow/Disallow bad CRC packets in the production network to reach the tools for analysis.
Rich Web-Based GUI	• The dashboard shows the resources used by the fabric as well as a bird's eye-view of the topology. • A highly attractive as well as functional GUI topology view that shows: • All the switches/ports in the fabric. • Paths taken across the fabric on a per-policy basis. • An intelligent context-sensitive properties panel triggered by a mouse-over on a topology object. • Customizable tabular views that persist according to user preferences. • Various table export options like JSON and CSV are available throughout the GUI. • Presents a highly intuitive, simplified management and operations workflow.
Switch Platform Support	<u>Arista Switch Platform Support</u> **General-purpose monitoring** Support for general-purpose monitoring with Arista 10G/25G, 40G/100G and 200G/400G platforms: • 24x10G + 2x100G • 32x10G + 2x100G • 48x25G + 8x100G • 48x25G + 12x100G • 96x25G + 8x100G • 2x10G + 32x100G • 2x10G + 64x100 • 24x100G + 12x400G • 48x100G + 8x400G • 24x200G + 8x400G • 32x400G

АО Акметрон akmetron.ru

Feature	Description / Benefit
Switch Platform Support (Contd.)	**Mission-critical monitoring** Support for mission-critical monitoring with Arista deep-buffer, large TCAM 10G, 25G, 40G/100G and 400G platforms: • 24x10G + 24x25G + 6x100G • 24x10G + 2x100G • 40x10G + 2x200G • 48x10G + 6x100G • 40x25G + 6x100G • 48x25G + 6x100G • 48x25G + 8x100G • 24x40G + 12x100G • 30x40G + 6x100G • 40x40G + 16x100G • 72x40G + 16x100G • 30x100G • 36x100G + 2x400G • 48x100G + 8x40G • 60x100G • 36x100G + 2x400G • 32x100G + 4x400G • 60x100G • 96x100G • 24x400G • 36x400G • 54x400G For the complete list of supported switch vendors/configurations and optics cables included in the DANZ Monitoring Fabric Hardware Compatibility List (HCL), please contact the Arista Sales Team (sales@arista.com).

DMF Controller Appliance Specification

The DMF Controller can be deployed either as a virtual machine appliance on an existing server or as a hardware appliance.

Controller VM Appliance Specifications

The DMF Controller is available as a virtual machine appliance for the following environments.

Environment	Version
Linux KVM	• Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 20.04 Please refer to the Hardware Compatibility List for release specific details.
VMware ESXi	• Version 6.5.0 • Version 6.7.0 • Version 7.0.2 • Version 8.0

Note: The above table explicitly indicates the Major/Minor/Maintenance versions tested and supported by DMF. Versions other than the ones listed above will not be supported.

АО Акметрон akmetron.ru

Minimum VM Requirements
8 vCPU with a minimum scheduling of 2GHz
32 GB of virtual memory
400 GB of Hard disk
1 virtual network interface reachable from physical switches

Note: A VM's performance depends on many other factors in the hypervisor setup, and as such, we recommend using hardware appliance for production deployment.

DMF Controller Hardware Appliance Specification (DCA-DM-C660)

The DMF controller is available as an enterprise-class, 2-socket, 1U rack-mount hardware appliance designed to deliver the right combination of performance, redundancy, and value in a dense chassis.

Arista DMF Controller: DCA-DM-C660

Feature	Technical Specifications
	DCA-DM-C660
Processor	Intel Xeon Silver 2 sockets (12 cores)
Form Factor (H x W x D)	1U Rack Server (4.28cm x 43.4cm x 69.3cm)
Weight	42.8 lbs
Memory	4 x 16GB
Hard Drive	2 x 4TB SATA (with RAID support)
Networking	2 x 10Gb;
Power	Max Power: 515 watts Input Current: 4.7 Amps Input Voltage: 100V - 240V auto-sensing
Mean Time Between Critical Failures (MTBCF)	115,000 hours

DMF Service Node Hardware Appliance Specification (DCA-DM-SNR660, DCA-DM-SN760L)

The DMF Service Node appliance is an enterprise-class, 2-socket, rack-mount hardware appliance, designed to deliver the right combination of performance and value.

It is available in 2 form factors:

- 1U w/ 4x25G bidirectional interfaces
- 2U w/ 4x100G bidirectional interfaces

The DMF Service Node provides specialized packet functions like deduplication, packet slicing, header stripping, regex matching, packet masking, UDP replication, and IPFIX/NetFlow generation. Once connected to the fabric, the DMF controller auto-discovers the service node and becomes the single, central point of management and configuration of the service node. This highly scalable architecture allows chaining of multiple service nodes that are connected to the fabric via the service node chaining function of the DMF.

Arista DMF Service Node: DCA-DM-SNR660

Arista DMF Service Node: DCA-DM-SN760L

Feature	Technical Specifications	
	DCA-DM-SNR660 Service Node (4 x 25G)	**DCA-DM-SN760L Service Node (4 x 100G)**
Processor	Intel Xeon 1 socket (24 cores)	Intel Xeon 2 socket (36 cores)
Form Factor (H x W x D)	1U Rack Server 4.28cm x 43.40cm x 71.30cm	2U Rack Server 8.68cm x 43.40cm x 77.30cm
Weight	42.8 lbs	60.6 lbs
Memory	8 x16GB RDIMM, 5600 MT/s, Single Rank	16 x 32GB RDIMM, 5600 MT/s, Single Rank
Hard Drive	1 x 960GB SSD	1 x 960GB NVMe
Networking	4 x 25Gb; 2 x 1Gb	4 x 100Gb; 2 x 1Gb
Power	Input Power: 395 watts Max Power: 308 watts Input Current: 3.7 Amps Input Voltage: 100V - 240V auto-sensing	Input Power: 871 watts Max Power: 569 watts Input Current: 8.1 Amps Input Voltage: 100V - 240V auto-sensing
Mean Time Between Critical Failures (MTBCF)	77,400 hours	82,800 hours

DMF Analytics Node Hardware Appliance Specification (DCA-DM-AN660)

The DMF Analytics Node appliance is an enterprise-class, 2-socket, rack-mount hardware appliance designed to deliver the right combination of performance and value. It is available in a 1RU form-factor.

DMF Analytics Node provides scale-out analytics with configurable, historical time-series-based dashboards for health, performance, capacity planning, and security. It also acts as a collector for NetFlow and sFlow packets to provide real-time application-level visibility, including tunneled or encapsulated traffic, enable detection of security attacks like DoS/DDoS, and support sub-second triggering. The highly intuitive and customizable GUI dashboards support a Google-like search to quickly drill down and focus on the possible issues. It not only provides a variety of reporting and alerting functions but also allows the user to easily share custom dashboard views with other team members for collaborative analysis, troubleshooting, and remediation.

Arista DMF Analytics Node: DCA-DM-AN660

Feature	Technical Specification
Processor	Intel Xeon 2 sockets (12 cores)
Form Factor (H x W x D)	1U Rack Server (4.28cm x 43.4cm x 69.3cm)
Weight	43 lbs
Memory	8 x 16GB
Hard Drive	2 x 2TB SATA, 2 x 1.92 TB SSD SAS
Networking	2 x 1Gb; 2 x 10Gb; 2 x 10Gb Base-T
Power	Max Power: 597 watts Max Input Current: 5.1 Amps Input Voltage: 100V - 240V auto-sensing
Mean Time Between Critical Failures (MTBCF)	94,300 hours

DMF Recorder Node Hardware Appliance Specification (DCA-DM-RN760, DCA-DM-RN760L)

The DMF Recorder Node appliance is an enterprise-class, 2-socket, rack-mount hardware appliance, designed to deliver the right combination of performance, capacity, and value.

It is available in 2 form-factors:

- 2RU with 1x25G interface and a total available storage of 96TB
- 2RU with 1x25G interface and a total available storage of 192 TB.

The DMF Recorder Node provides high-performance packet recording, querying, and replay functions. Once connected to the fabric, the DMF controller auto-discovers the recorder node, ensuring a single point of configuration and device lifecycle management. Multiple recorder nodes can be clustered together to present a view of a single, logical recorder node that allows users to store more network traffic for longer periods and retrieve packets from the single logical recorder node interface via the controller. This architecture provides true scale-out characteristics while maintaining the agility and simplicity in the user workflows. The recorder node provides feature-rich capture, query, and replay functions. The recorder node allows the user to replay the specifics of an event to derive the root cause and predict future trends for various performance issues and security threats.

Arista DMF Recorder Node: DCA-DM-RN760

Arista DMF Recorder Node: DCA-DM-RN760L

Feature	Technical Specifications	
	DCA-DM-RN760	DCA-DM-RN760L
Processor	Intel Xeon 2 sockets (24 cores)	Intel Xeon 2 sockets (24 cores)
Form Factor (H x W x D)	2U Rack Server (8.68cm x 43.4cm x 68.6cm)	2U Rack Server (8.68cm x 43.4cm x 68.6cm)
Weight	63.5 lbs	63.5 lbs
Memory	8 x 16GB	16 x 16GB
Hard Drive	12 x 8TB SAS HDD, 2 x 1.92TB SAS SSD	12 x 16TB SAS HDD, 2 x 7.68TB SAS SSD
Networking	2 x 1Gb Base-T; 2 x 25Gb	2 x 1Gb Base-T; 2 x 25Gb
Power	Max Power: 1067 watts Max Input Current: 9.9 Amps Input Voltage: 100V - 240V auto-sensing	Max Power: 1111 watts Max Input Current: 10.3 Amps Input Voltage: 100V - 240V auto-sensing
Mean Time Between Critical Failures (MTBCF)	52,700 hours	52,700 hours

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

Copyright © 2026 Arista Networks, Inc. All rights reserved. CloudVision, and EOS are registered trademarks and Arista Networks is a trademark of Arista Networks, Inc. All other company names are trademarks of their respective holders. Information in this document is subject to change without notice. Certain features may not yet be available. Arista Networks, Inc. assumes no responsibility for any errors that may appear in this document. February 24, 2026