# Arista Cognitive Campus Network

ARISTA

Enterprises continue adapting their hybrid workspace paradigms to improve workforce productivity. At the same time, campus administrators are retooling to address mounting security, support and collaboration challenges in the distributed workforce. Meanwhile, campus IoT device deployments continue growing, increasing productivity but adding administrative and trust complexities.

While price/performance improvements of campus switched LAN and Wi-Fi technologies remains an important criteria for infrastructure upgrades, there is a new emphasis on automated provisioning, cognitive real time telemetry, troubleshooting, and remediation tools that improve productivity while containing costs associated with NetOps and SecOps teams. Operators also look for user-friendly point and click feature that support a more diverse group of net admins, to streamline upkeep of campus and edge workspace networks.

When planning new deployments, network administrators look to reduce TCO by using standards-based solutions that leverage their infrastructure, applications, team experience and knowledge of industry standard CLIs. Key decision criteria include: reliability, ease of maintainability, and a simplified, comprehensive, administrative experience that streamlines operations. Furthermore, administrators look for automation tools that deliver predictable, repeatable and successful outcomes when managing their evolving network campus and edge workspaces.

Arista's Cognitive Campus delivers a comprehensive feature set needed to manage the networking challenges encountered in dispersed enterprise workspaces. As workers expect constant access to corporate and cloud resources, Arista's Cognitive Campus workspaces fulfills constant availability requirements, delivering hitless upgrading and patching, lossless failover, and proactive remediation to avoid client connectivity issues. Enhanced real-time telemetry, sourced from EOS' Cognitive Management Plane (CMP), is fed to a comprehensive Network Datalake (NetDL). This dataset is used by CloudVision to streamline provisioning, and provide cognitive fault detection, remediation and compliance validation.

Arista's Cognitive Campus Architecture delivers cognitive provisioning, analytics, problem detection and compliance solutions that are augmented through a broad ecosystem of third party solutions that ensures the cost effective and reliable operation of campus enterprise workspaces.

# ARISTA

#### **Extending Cloud Grade Principles to the Campus** 1990's 2000's 2020's Era Internet Intranet Cloud & IoT Ubiquitous Wiring Closet Mobile & Voice Devices Endpoints Information & **Business Systems** IoT & Cloud Native Applications & Telephony Email Unified Edge Campus Availability Network Connectivity Cognitive NetDB Quality of Service Needs IoT & AI Driven

#### The Future is Campus Workspaces with AI and Software Driven Cognition

Figure 1: Evolution of the Cognitive Campus Network

Cloud computing economics continue to drive innovations in the design, provisioning, and management of campus enterprise networks. Many cloud grade principals have become best practices across campus workspaces. These include: streamlined, cost efficient leaf/spine topologies, highly automated management platforms that provide point and click provisioning and change management workflows (simplifying common deployment and configuration tasks). Rich real time telemetry to support security mitigation, proactive remediation, and specialized applications (e.g. location for asset tracking), plus a modular, self healing, hot patchable network operating system that facilitates regulatory and industry standard compliance requirements.



#### Figure 2: Cognitive Universal Campus Edge Network

The goal of the cognitive campus is to ensure the workforce remains productive while administrators adapt to hybrid workspace models; ensuring quality of experience while leveraging machine intelligence to streamline provisioning, monitoring, troubleshooting, and remediation. The cognitive campus builds on a reliable, consistent, cost-effective network that also supports scalability for small and large enterprises alike. It delivers quality and consistency to help administrators avoid the pitfalls of inefficient legacy architectures that are brittle, costly to deploy and maintain, and are plagued with siloed operating systems and management tools.

#### Innovations in Campus Technologies

ARISTA

Campus administrators shouldn't settle for table stakes services like VoIP, QoS, RADIUS, or 802.1X in hybrid workspaces. They should expect state of the art behavioral Network Access Control (NAC), microsegmentation capabilities and cognitive threat hunting supporting existing and new workloads. These authentication services should also serve workers in distributed remote home/office use cases. Of equal consideration are embedded security options such as MACsec encryption and Wireless Intrusion Protection services (WIPs) that serve important roles for securing the campus edge. Finally, real-time telemetry and in-band network detection and response (NDR) sensors offer threat hunting and visibility across all appliances in campus workspaces, complementing today's security solutions.

Operational benefits of new generation campus edge platforms include standards based interoperability, so it will work in brownfield environments and not require a costly forklift refresh. New architectures should utilize wirespeed, cloud grade technologies that combine cost effective, open standards systems supporting 10/25/40/50/100G Spline uplinks to evolving 10/100M, 1G, 2.5-5MGig, 10GBase-T and WIFI 6/6E and 7 access technologies.

Cost savings and performance gains are obtained by collapsing legacy access-aggregation-core topologies to an elegant two tier campus leaf-spine or spline as shown in Figure 3.



Figure 3: Single Tier Campus Leaf Spine or Spline™

Collapsing the mid-tier aggregation and core layers reduces equipment count and costs, while increasing reliability. Next generation, active-active, dynamic load sharing, improves spine-leaf performance and reliability. This removes the "reliability or performance" compromise of legacy architectures.

New cloud campus spine and leaf architectures deliver advanced reliability and enable hitless maintenance capabilities, preventing network degradation and failure. Finally, open L2, L3, virtual overlay, and segmentation feature sets are scalable, interoperable, and dynamically reconfigurable; giving network designers the flexibility to accommodate workload variety and graceful evolution. Examples range from reconfigurable route scale to supporting open standards based EVPN-VXLAN in the campus, letting managers integrate with, and transcend the limitations of 802.1Q 4K VLANs to the possibility of 16 million unique VNIs (Virtual Network Interfaces) to accommodate device and workload proliferation.

#### Leaf Spine Stacking(LSS) and Switch Aggregation Group (SWAG)

Legacy stacking architectures were intended to simplify expansion and management of grouped campus wiring closet switches. Their principal benefits were a single point (IP address) of management and no chassis overhead cost. However, the goal to deliver an economical, scalable and manageable campus platform remains challenging due to complexities of distributed software and hardware architectures that share state, and fate, among stacked devices. Regrettably, vendors have scaled back expectations, underwhelming administrators with:

#### arista.com

- Brittle software patching and upgrade procedures that take minutes of user downtime to implement
- Mandatory homogeneity in stacked switches to avoid exposure to untested and unsupported configurations.
- Proprietary, costly, one-size fits all, stacking cabling schemes.
- ... to name a few.

ARISTA

Arista's stacking architecture offers administrators flexibility of device types, standard ethernet cables for stacking, plus stack management options either through CloudVision and/or single point CLI (IP address) stack administration.

#### Leaf-Spine Stack

Arista LSS leverages EOS MLAG to interconnect peers and leaf switches into a wiring closet stack that can be easily managed through CloudVision as a collective entity. LSS uses industry standard LACP-LAG, supporting dynamic load balancing, to deliver active/active connectivity to stacked switches. LSS uses Ethernet interconnects, allowing administrators economical choices from 1G-100G as needs and budget dictate.

Field validated in thousands of customer deployments, LSS-MLAG is simple, reliable, standards-based, and interoperable with other LAG capable devices. Maintenance and expansion, using MLAG-ISSU and SSU is hitless, while monitoring and software lifecycle management is simplified through Arista's CloudVision management platform, or other industry standard DevOps tools. Finally, CloudVision studios offers LSS provisioning automations to simplify wiring closet deployments. CloudVision Day-N quick actions also lets administrators add and change the stack using point and click actions.



#### SWitch AGgregation (SWAG) Stack

EOS is adding new capabilities in its SWAG feature set that builds upon the reliability, maintainability and flexibility of EOS. SWAG delivers single IP address management for operators whose workflows benefit from consolidation of management points.



Figure 4: SWAG Ring Topology Shown in CloudVision



In addition to a single management point that serves for control and monitoring, SWAG provides redundancy features through paired supervisor (control-plane) nodes, which control other worker node (dataplane forwarding) switches in the stack. SWAG supervisors interact with worker nodes through agents that coordinate EOS SysDB state among diverse switches in the stack. Spanning tree, LACP-LAG and LLDP-MED state, among many others, are coordinated as a logical entity. Management tools, user applications and endpoint devices perceive a single switch. SWAG is deployable in multiple topologies including chain, redundant ring and redundant LSS topologies. With planned support for up to 48 devices in a stack, these topologies offer new possibilities for distributed switch stacks in various enterprises.

#### **EOS Foundation**

Since SWAG builds upon EOS, it inherits EOS' fault isolation and self healing properties, hitless maintainability and renowned quality and reliability. Finally, as with all Arista platforms, SWAG is fully manageable through CloudVision.



Figure 5: EOS SWAG and CloudVision LSS Management

#### **Reliability of Cognitive Wired PoE**

Until recently, the only innovations one could point to in PoE systems came through increased power: moving from 15W 802.3af, to 30W 802.3at and the latest upgrades of up to 90W using type 4 802.3bt. Arista drives additional innovations to improve both the reliability and efficiency of wired and wireless systems. Following are the capabilities of Cognitive PoE:

#### **Continuous PoE**

Continuous PoE expands on reliable power distribution, not only in cases of FRU failure(power redundancy), but also in cases involving system patching and maintenance. Continuous PoE ensures power even when the system is rebooted or encounters any form of software issue. Administrators can also utilize port prioritization so campus switches can degrade gracefully in case of power starvation. Essential services, like badge readers, or security cameras would have priority over non-essential IP phones or similar non-critical devices.

#### **Concurrent PoE**

Concurrent PoE is designed for use cases where common power is required across all switched ports. Only the most power efficient switches coupled with high density power sources can fulfill this requirement.

#### **Dynamic PoE**

Dynamic PoE allows switches to measure the difference between the power requested (LLDP-MED) and what is actually used. The excess unused power can therefore be reallocated to other devices thereby extending the switch's power budget and economy.

#### Cognitive, Real-Time Telemetry for the Enterprise

Enterprise operators appreciate the advantages of real time monitoring services that can deliver more information, more efficiently. The symptomatic telemetry gaps of SNMP polling systems can't keep pace with the real time demands of workforce collaboration and conferencing apps. Real time monitoring, coupled with AI/ML performance and correlation analytics that track workspace infrastructure, workgroups, applications and users, is what helps the operations team maintain SLAs, pinpoint or even anticipate potential problems, and rationalize infrastructure investment.

To achieve these goals, campus infrastructure platforms must deliver comprehensive real-time telemetry, beyond bytes and drops, to include throughput and latency data at the client, workgroup, and application level. These services should use standard publish/ subscribe oriented APIs, like OpenConfig's gNMI/gRPC protocols, for interoperability and flexibility. Campus networking systems must be able to glean and report on the thousands of user and application flows in the enterprise, detailing throughput, payload, latency and congestion, to name a few. Therefore, telemetry services must be customizable, with the ability to filter and capture well known, and to be defined, traffic types. Monitoring systems should thoughtfully interpret and summarize telemetry data in customizable formats that are user friendly. Management tools must add value, allowing all levels of administrators to easily identify and troubleshoot service issues. Lastly, administrators should expect no compromise in reliability, performance or manageability.

Table 1: Legacy vs Modern Telemetry		
Traditional / Legacy Approach	Campus Telemetry Requirements	
Polling Approach (1-15 min)	Real-time Streaming	
State scope limited to MIB definition	Complete state history	
Per-Switch Per Device	Network-wide scope	
Static, discrete events. Manually correlated	Dynamic event correlation	
Bandwidth, drops, failure alerts	Correlation, trendlining, predictive analytics	

#### Wireless Mobility Services Improving Reliability, Scale, and Location

In the post pandemic era WiFi's ubiquitous mobility is invaluable. Workers' expectations of continuous connectivity can be challenging since WiFi is affected by many factors like radio integrity, resource overloading or authentication faults. Cognitive WiFi systems should monitor the workspace spectrum to discover, notify and even adjust radio configurations to ensure continuous access to the workforce. Dynamic resource management services should assist with day one provisioning and validation, yet be ready to cognitively reconfigure due to future environmental changes and service impacts.

WiFi's scaling potential also opens possibilities for private multi-tenancy use cases in enterprises. Similar to ad-hoc networks, Unique Pre-Shared Key (U-PSK) networks offer flexible virtual workspaces where users can collaborate privately, use resources personally, and segment themselves from other workers. Supporting private WiFi workspaces should leverage industry standards alongside guest portal registration services that help provision and segment workgroups. Administrators should also expect to employ a variety of WiFi devices to address different use cases encountered in carpeted campus, outdoor, hospitality venues or higher-ed locales.

Locating mobile workers and business critical IoT assets is another natural extension of WiFi services. Various options exist for providing RF location services in the enterprise: WiFI based triangulation, Bluetooth Low Energy (BLE) beacons and various bespoke RF based systems. All provide location services and open APIs that support wayfinding, locating, footfall monitoring and asset tracking use cases, to name a few. What's most important is the WiFi architecture supports a large ecosystem of partner solutions so the workforce can pick best of breed options for their needs.

# ARISTA

#### Arista's Cognitive Campus Workspaces

Arista's vision and framework for the Cognitive Campus Network, leverages cloud capabilities and state of the art merchant silicon to deliver critical services that automate deployment, configuration, visibility, troubleshooting and security. The Arista Cognitive Campus delivers spine/spline, leaf, wireless infrastructure, plus access and security services through a common architecture that seamlessly integrates with the greater enterprise network. The cognitive campus provides real-time telemetry and actionable analytics through a uniform management architecture that integrates with an ecosystem of industry leading solutions partners as shown in Figure 6.

Category	Joint Value Proposition	Key Partners	
Endpoint Security	<ul> <li>Speed up investigations and response with integrated xDR</li> <li>Gain situational awareness across managed &amp; unmanaged devices</li> </ul>	Carbon Black. Microsoft Trellix CROWDSTRIKE	
Security Information and Event Management (SIEM)	<ul> <li>Optimize response workflows with high-fidelity detection</li> <li>Deliver rich network context to other SIEM data sources</li> </ul>	sumo logic splunk > Hicrosoft	
Ticketing, Orchestration & Automation	<ul> <li>Automate investigation, response and forensic tasks</li> <li>Establish standardized workflows using context from the network</li> </ul>	Servicen w Phantom	
Perimeter Security	<ul> <li>Contain threats by blocking command and control/data exfiltration in real-time</li> <li>Protect the entire enterprise by blocking access to attacker infrastructure</li> </ul>	CHECK POINT FERTIDET	
Cloud & SaaS	<ul> <li>Enable security monitoring of cloud workloads</li> <li>Gain insights into threats that spread laterally from traditional to cloud infrastructure</li> </ul>	AWS Georgie Clous Petform	
Plus Fully Docum	ented and Supported API/Webhooks for Additional Integ	rations	

Figure 6: Management, Security, and Identity Partnerships

Leveraging Arista's flagship CloudVision management platform, Arista campus networks deliver industry leading automation for provisioning and maintenance, plus cognitive fault detection and isolation. Arista's Cognitive Management Plane (CMP) provides comprehensive, real time telemetry of network health and user traffic to AI Autonomous Virtual Assistants (AVA) that help administrators quickly pinpoint and resolve issues before they impact users.

#### ZeroTrust Networking Architecture

Arista's Zero Trust Network (ZTN) architecture offers a holistic approach to campus security, segmentation and threat detection and endpoint analytics. Arista's Guardian for Network Identity (AGNI) provides identity and agentless IoT access control and segments campus workloads leveraging conventional (.1Q and VXLAN) segmentation services. Arista's Multidomain Segmentation Services (MSS) augments segmentation enforcement to the device level, without the need for proprietary protocols or forklift upgrades. Concurrently, Arista offers the ZTX flow profiling solution that analyzes all enterprise workflows and validates workflow segmentation actions against intended policies. Lastly, Arista's Network Detection and Response (NDR) solution hunts for cyber attack threats in campus traffic flows, leveraging AI to present actionable reports to InfoSec personnel with corresponding quarantine updates to AGNI to isolate suspect devices.

Collectively, Arista's Cognitive Campus networking solution optimizes performance, enhances security and streamlines deployment, maintenance and troubleshooting, significantly reducing downtime, costly cyber breaches and TCO.

#### 1. Splines for Collapsed Campus Fabric

ARISTA

Arista has uniquely extended cloud grade capabilities to the campus with the modular 7300X3 and fixed-config 7050X3 switching platforms. These platforms provide a suite of cognitive features that streamline deployment and ensure high availability operations and maintainability. Self healing, hitless upgrades and live patching are cognitive actions that avoid impact on the infrastructure. Arista's Smart System Upgrade (SSU) feature enables switch operating software to be completely upgraded while the platform continues to process campus traffic.

The X3 series switches provide a variety of connectivity options: 1-10G, multi-rate 10/25G SFP+, 40G, 50G and 100G QSFP. These platforms support dynamic load balancing and buffer allocation available to all networked ports to help avoid data loss from link faults, congestion or micro-bursts. The splines work with all devices that support static or dynamic port aggregation to preserve and enhance the installed base investment.

#### 2. Cognitive Leaf Wired Switches

Arista continues expanding its portfolio of cognitive, secure, high performance and high PoE budget connectivity, delivering 10M through 10GBase-T, MACsec security, 802.1Q/VXLAN segmentation and power options for all campus user workloads. The CCS-700 series of platforms delivers a variety of connection options optimized for user desktops, POE appliances and IoT devices. Cognitive 802.3af-t/bt POE delivers up to 90W, with speed options ranging from 10Mbps - 1Gbps, 100M-5G, and 1G-10Gbps over UTP, supporting every conceivable campus workload. High speed SFP and QSFP uplinks support speeds from 1Gbps to 100Gbps delivering flexibility and scalability in network designs.

All Arista campus platforms run Arista's common binary EOS, providing a comprehensive, open standard, layer 2, 3, and overlay networking feature set including MLAG, 802.1Q, EVPN/VXLAN virtualization, and Macro-segmentation services, to name a few. Arista EOS supports standards-based 802.1X and RADIUS access control plus LLDP Media Endpoint Discovery (MED) device identification services to automate admission and segmentation of appliances, users, and applications in the campus.

## Arista Cognitive Campus 700-Series Portfolio



Figure 7: Versatile desktop, fixed config, and modular PoE switching running EOS

The 7050X3 and 7300X3 Spline, plus the CCS-720 series fixed configuration and CCS-750X series modular POE switches share the same silicon architecture, and are designed to provide scale-up capacities with dynamic traffic load balancing, and real time



flow monitoring of all campus workloads. Dynamic load balancing is an enhancement that balances traffic by monitoring rates of existing flows then adding new flows to the lesser utilized paths. This performance optimizing feature interoperates with all devices that support link aggregation to ensure trouble-free interoperability and migration.

Arista's campus switching also provides real-time Flow tracker telemetry. Supporting CloudVision and flexible IPFIX APIs, Flow tracker allows administrators to capture an unlimited variety of key performance indicators and traffic flows in real time. Administrators can focus on infrastructure, device, application and user data for security, SLA monitoring, and troubleshooting use cases. The combined telemetry of the campus leaf and spline helps administrators better understand the proliferation of mobile, diverse and bursty traffic generated by campus users and devices. Salient EOS features and their benefits enhancing the cognitive campus are listed below in Figure 8.



Figure 8: Key Attributes of Cognitive Campus Platforms

Finally, Arista's campus portfolio accommodates a variety of L2, L3 and overlay scaling demands with the help of its dynamically configurable Unified Forwarding Table (UFT). Unlike other static architectures with fixed L2 MAC and L3 routing tables, the networking processors in the 720XP/750XP series platforms let administrators select from multiple profiles optimized for either L2 MAC addressing, L3 host addressing or IPV4-6 route table scale. This simplifies design considerations because a common platform can be optimized for various campus use cases. Consistent with other Arista platforms, the 720D/P/XP and 750XP series supports wire speed L2 VLAN, L3 routing and L2 over L3 VXLAN that transcends 4K VLANs to more than 16.7 million industry standard VXLAN virtual networks. Campus-wide dynamic segmentation of workgroups is accomplished through 802.1Q, EVPN and Arista's innovative Multi-domain Segmentation Services (MSS) with orchestration support from CloudVision. EVPN and MSS are friendly to brownfield infrastructures, supporting graceful additions or migrations. Finally, CloudVision extends segmentation orchestration to data center and cloud based workloads.

#### 3. Cognitive Unified Edge: (CUE) for WiFi

Arista's distributed data plane architecture for WiFi embeds manageability, telemetry and 802.1Q plus overlay VXLAN segmentation within the access points. This controller-less architecture continues to evolve with Arista's expanding family of Wi-Fi 6E cognitive access points. The AP-C300 series of 4X4 WiFi 6E capable APs, including the new wall/desk mountable W-318, complements the 802.11ax C200 series APs, expanding networking capacity by utilizing the 6GHz band (where allowed). These APs are backwards compatible with Wi-Fi 5-6, supporting upstream/downstream MU-MIMO and OFDMA communications, improving performance and user density compared to legacy Wi-Fi architectures. Finally, certain AP models offer optional third scanning radios for dedicated WIPs services, as well as BLE and Zigbee. Arista WiFi supports locationing solutions based on BLE WiFI as well as custom solutions from partners like Aeroscout<sup>™</sup>.

The CUE Wi-Fi manager, available as an on premise or in cloud service, not only provisions and monitors the WIFI network, it also helps secure, monitor, and optimize the wireless workforce's quality of experience. CUE provides an extensive feature set designed to optimize wireless productivity, secure the infrastructure, streamline provisioning worldwide and quickly troubleshoot and remediate user problems with the support of cognitive autonomous virtual assistants (AVA).

These features include:

ARISTA

- Client Journey: Connection troubleshooting dashboard to streamline identification of campus users' connectivity problems. The dashboard simplifies access troubleshooting including Wi-Fi association, authentication and address allocation, to name a few.
- Inference based Wi-Fi client problem diagnosis: CUE leverages AI/ML heuristics, applied to individual client sessions, to
  analyze and diagnose probable causes of degraded Wi-Fi client experience. As illustrated in Figure 9, the cloud based AVA
  AI offers troubleshooting tips and possible remediation steps to administrators, reducing troubleshooting complexity and
  downtime while improving operations staff and client productivity.

			Marcon Come They, Mokin, Generalmanin (48,04,07,517) *	α < : Θ	Recommendations     Dual-band clients operating in 2.4 GHz     There are dual-band clients operating in 2.4 GHz     instead of 5 GHz	8
•	Machine Learning for automatic client connectivity and Performance Issues		Anere Socie (Adual Doministrations), 287 Unit Marian Mill (455-1/10/1717) Data hand Clarens Generation 2.2 (Hits Q < # ##		Enable band steering for following SSIDs in the index notes	
•	Automatically identifies root causes and provides remediation recommendations	Status Succe Serry Models, Co. Davis band Clients Open	mananet HEAS HOTESTIG * * stable Communication (32) Stable Communication (32) Stable Communication (32) Stable Team in the dual function commong = 21 (DVF measured of Tone 1) (1) Stable Team in the dual function common of an dwarehu waith (there down 1) (1) Stable Team in the dual function common of the dwarehu waith (there down 1) (1) (1) (1) (1) (1) (1) (1) (1) (1) (		2	
		Client Connection Logs 🛩	Successfully Connected     Manage Internet Middle Stars, 19th     Amage Lances, 19th     Amage Lances, 19th     Amage Lances, 19th     Del Star Middle Stars, 19th     Del Stars, 19t	4000 • 744404 • 1964 • 2 - 8014-000 • 8880 - 00,0,4,602 • 9880 - 9860 • 9880 - 9860 • 1980 - 9860 • 1981 • Leader		
	Arrent Composition Arrent Arrent Arr	Jan 15, 2019 10:22:12 AM	IP Fabrics Manage James (2019) Start Start, Disk Manage James (2019) Start, Disk Start, Disk Start, Disk Matheware Into Start Start Matheware Into Start S	IS3+4100C 01         IS300           CID0,07,401C0         Mission           Security         Mission           Security         Mission           Viter Vol1710         Leaders		

Figure 9: Client Inference Problem Resolution

- Site specific Inference based troubleshooting: he focus of CUE's inference tools can be expanded from individual devices, to AP, and site level views, addressing issues impacting user groups or workloads. CUE's AVA AI can be targeted to an AP, floor or location to help assess problems that may be common to users, applications or a site. Power settings, channelization, interference and infrastructure deployment are among the factors evaluated for remediation recommendations.
- Client and Infrastructure Location Services: A properly instrumented Wi-Fi infrastructure offers both administrators and clients the ability to locate assets and resources in the cognitive campus network. Arista wireless platforms utilize Wi-Fi, BLE and AVA AI technologies to discover, locate and facilitate mapping of client and IoT devices in the campus. Administrators can refine their view of the cognitive Wi-Fi network using a variety of filters/views aimed to identify:
  - > Slow or intermittent clients
  - > Clients exhibiting weak signals, high error or retry rates
  - > Clients not meeting Quality of Experience (QoE) expectations for key applications.
  - > Clients that are failing to connect.
  - > Expanded applications monitoring for user Quality of Experience

#### arista.com



CUE Wi-Fi can monitor performance of collaboration tools like Microsoft teams and Zoom, in addition to Webex, Skype, GotoMeeting, Google Hangouts plus others. With this expanded capability, administrators can ensure the productivity of users' collaborative applications.



Figure 10: Application Quality of Experience for Business Critical Applications

Finally, Arista supports partner enabled Wi-Fi location services to provide enhanced location capabilities to help organizations track vital resources and workforce movements in the campus.

#### **Client Location Monitoring**

CUE collects a multitude of real-time client telemetry used to improve and ensure user and application Quality of Experience. CUE's AVA AI correlates data from a comprehensive WIFI database to provide actionable troubleshooting assistance and KPI trend analysis that's helpful to NetOps administrators.



Figure 11: Visualize Client Location and RF Coverage

• Wi-Fi Tracers:

ARISTA

- > Wireless Intrusion Prevention System to protect against rogue devices
- > Application and Internet reachability tools to diagnose connectivity problems
- > Wi-Fi airwave health scanning tools that don't compromise Wi-Fi resources
- > Extended testing and troubleshooting incorporating guest and BYOD web portals
- CUE's connection troubleshooting dashboard can diagnose typical problems with web provisioning portals. Portal accessibility and functionality enhance the client journey suite of diagnostic tools, extending analysis from the airwaves to association, registration, network services and finally quality of Wi-Fi experience.

CUE's tools streamline and automate provisioning, securing, troubleshooting and ensuring client Quality of Experience throughout all workspaces in the distributed campus enterprise.

As enterprises adapt to hybrid workspace deployments, campus net admins are tasked to securely extend accessibility of business critical IT functions to workers. Arista's cognitive Wi-Fi solution offers secure VPN overlay features in its APs, extending the campus network to branch, remote and home office workspaces. Leveraging hardware accelerated IPSEC tunneling services, Arista Wi-Fi APs interoperate with leading VPN concentrator solutions to extend campus services under the enterprise's existing security infrastructure. The W-318 is well suited for providing combined WIFI-6E plus multiport Ethernet switching in a compact, wall or desk mounted unit.

### Arista Remote Access WiFi - Extending the Cognitive Edge

- Extends Arista Cognitive Campus Edge to telecommuters, branch and remote workers
  - Client Journey
  - Application Quality of Experience
  - Wireless Intrusion Protection (WIPS)
- Investment Protection Works with industry standard Firewalls or VPN concentrators
  - Tested with Palo Alto Networks, CheckPoint, Fortinet and other leading vendors
  - No additional investment required at the DC
- Ease of configuration and ease of deployment
  - True 'zero touch' provisioning at remote sites
  - Plug and Play operation
  - Ideal for remote worker/telecommuter deployments



Figure 12: Extending CUE across Distributed Campus Workspaces

The WIFI CUE managers' Zero Touch Provisioning (ZTP) services simplify remote office AP deployment, allowing administrators to drop ship APs to their distributed workforce who simply plug the device into their home network. Fully managed by CUE and with AP support for optional tunneled Ethernet connectivity, Arista's remote access solution fulfills the need for administrators to connect their socially distant workforce.

#### 4. Cognitive Reliability and Manageability with Arista EOS

ARISTA

Arista's transformational Extensible Operating System (EOS) provides a common software foundation for the cognitive campus network. EOS brings all its advantages to the campus with cloud grade control, monitoring, virtualization, scale and reliability. Arista's unique modular, fault isolating and self-healing architecture isolates software defects, supports live patching and redefines hitless upgrade and rollback. The same binary EOS image is used across Arista's entire product line: from campus to cloud. Doing so ensures that EOS quality and reliability is consistently validated across the thousands of Arista customer data center, cloud and campus networks.

Core to Arista's EOS architecture is the Cognitive Management Platform (CMP) that supports open standard configuration and monitoring APIs to support industry leading DevOps and monitoring solutions. Unlike legacy polling or inter-processor communication (IPC) schemes, The CMP is purpose-built to share all state in real time.

The CMP in Arista EOS, feeds Arista's Enterprise-wide Network DataLake or NetDL. NetDL provides a single source of network data 'truth' and a common sensor/collector architecture that enables forensics and analytics for threat hunting, network packet brokers, network detection and response, network performance monitoring, and application performance monitoring. By collaborating with a variety of industry leaders, Arista is able to deliver powerful production customer benefits. These data-driven network models can be transformed into insights that deliver actionable operational outcomes.



Figure 13: Open Architecture Supports Best of Breed Solutions

#### 5. CloudVision and Cognitive Unified Edge (CUE): Arista's Management Architecture for the Campus Enterprise

Campus operators value campus management platforms for their time saving features, cognitive insights for trouble shooting and remediation, versatility across many platforms and use cases and their ease of use. For over a decade, Arista has been developing CloudVision and CUE to fulfill a variety of use cases ranging from data center overlay networks to small campus switching and WIFI deployments. The CloudVision platform (CVP) is deployable either on-premises, or as a cloud service (CVaaS). Enterprises can select whichever option that best suits their sys-admin, cloud budget and data privacy requirements. Finally, flexible subscription models for CVP and CVaaS help optimize the IT administration budget.

#### **CloudVision-CUE Direct Connect**

Understandably, some enterprises may be averse to cloud based services because of corporate policies requiring internet service cut-offs in cases of cyber attack. Arista acknowledges customer concerns and has initiated its CVaaS direct connect

#### arista.com



service. Available through Equinix, CVaaS Direct Connect provides private network connections to CVaaS, CUE, AGNI and NDR services. In the event of an internet cut-off, administrators will still have secure private access to all management, NAC, and threat hunting services.

Arista's CUE WIFI portal works alongside CloudVision, providing WIFI operators provisioning, management and WIPs workflows exclusive to WIFI operations. CUE offers an intuitive provisioning hierarchy that lets operators define enterprise security and segmentation policies that are consistently applied throughout the wireless enterprise, while at the same time, allowing customization at the regional or branch level. CUE's customer journey monitor, allows operators to quickly identify and address various WIFI challenges including RF, authentication, and network addressing issues. However, CUE interacts with CVP, leveraging a common Network Datalake (NetDL) to show comprehensive, event, topology and endpoint flow information across the wired and WIFI enterprise.

#### 6. Arista Validated Designs (AVD) for Campus Deployments plus Day-"N" Quick Actions

Campus managers face the dilemma of a fixed NetOps budget, while the campus network's complexity, and size continues to grow. Compounding this problem is the scarcity of campus networking professionals in the field. For this reason, IT managers look to point and click provisioning tools and automation systems to lighten and distribute campus networking workloads.

Arista has worked with customers to develop AVD templates that work with the CloudVision management system to templatize initial campus provisioning workflows into provisioning studios. Templates are customizable, allowing operators to support a spectrum of features or use cases. Operators can employ a combination of scripting automation and declarative point and click provisioning,

For Day-N, moves, adds and changes, CloudVision quick action studios provide point and click port configuration tools that allow networking specialists to create point and click workflows for common tasks so IT generalists can effectively own daily maintenance of enterprise campus workspaces.

### CloudVision for the Campus

Day	-0/1
Deploy Available Desices	
No. 1.10 1.10	
Inford Haddalin Devices Transmission of anticipations	
Second and saless Acce	Ended here
NUTRY DESCRIPTION	= =
Apartic Daylogueset Datals Cross in Account of Pass darks in Territory of Represent Type 1 Trans. Strategy 10, 10	14 Aug.
negat 0	
National States of Contract of	
mart O	
No. 1 a Tank	

Guided device onboarding and tagging

Campus network onboarding & deployment

Access Pod / Virtual stack deployment & expansion

Day-2		
Assign Profile		
tenpue	Device	
H3 Campon Ped 5450 Assense Ped Pear 2	· · · · · · · · · · · · · · · · · · ·	
Plus 2 Part iPulla Santa et inne nomen pode er unfgert nomine		

Assign Interface Profile Create Campus

Service/VLAN

Virtual stack upgrades

Diagnostic Tooling		
interface Diag	pantics for hy-ind-to - + Othernet1 -	
Calle for	Average and a set of the set of a	
	Interface control	

Interface control (admin state & power)

Copper cable testing

Virtual stack switch replacement

### **Quick Actions**

#### Feature Highlights

- Guided workflows designed to address common provisioning tasks
- Automate steps required to execute changes on the network, while maintaining change control audit trail and history
- Continued evolution for L1 operator workflows

#### Benefits:

- Single 'click' workflows for performing standard operational tasks
- More intuitive configuration steps

Use-Case Applicability Campus, WAN, DC

#### Out-of-the-Box Guided Workflows for Common Operations

Figure 14: Point and click Day-0 through N Workflows

ARISTA

Networking specialists can configure pre-built profiles, such as user or appliance port configurations, to the service desk team, allowing them to make short work of typical provisioning activities. Quick actions studios provides a forms builder workspace that lets dev-ops and NetOps specialists customize existing workflows or create entirely new processes for use by the whole NetOps staff. These workflows integrate into CloudVision's existing change management system to ensure compliance to change management procedures while also leveraging CloudVision's automated remediation tools.



Figure 15: Quick Actions Operator Studio

CloudVision Studios allows campus staff to codify the expertise of the enterprise's NetOps specialists, maintain and customize workflows using standard tools, and lastly, allow the greater IT staff to utilize these workflows to streamline management of the enterprise net.

#### 7. Zero Trust Networking Framework: AI Driven Threat Detection, Response plus Multidomain Segmentation Services

The explosive proliferation of client and IoT devices in the enterprise correlates to an increased and often unmonitored attack surface and elevated risks of malicious attacks. Infosec managers have no other option but to leverage AI/ML systems that can aggregate enterprise scale data flows and constantly hunt for patterns in traffic that signal a data probe or ransomware attack.

Arista's Network Detection and Response(NDR), is the only advanced network detection and response solution that provides the InfoSec team with answers to threats, rather than alerts lacking context. NDR combines artificial intelligence with human expertise. Arista NDR autonomously models and hunts for both insider and external attacker behaviors while providing triage, digital forensics, and incident response support across the distributed enterprise network.

The Arista NDR can also be embedded in Campus switches. These AVA sensors deeply analyze millions of network sessions to autonomously discover, profile and classify every device, user and application across any network. Using a multi-dimensional machine learning approach, NDR models complex adversarial behaviors and connects the dots across entities, time, protocols and attack stages. Unlike legacy network detection and response tools that rely primarily on unsupervised learning to spot anomalies from "normal" baselines, Arista NDR compares entity behaviors to the peer group and the rest of the organization and brings together secure threat hunting in the campus for malware, IOT and disparate devices.





Network Detection and Response (NDR) for the Cognitive Campus

#### Simplified Deployment

- · Up and running quickly with a simple license add-on
- NDR Nucleus can run on-premise or delivered as SaaS

#### High Efficacy of Detections

- Broader Visibility
  - Converts "packets" into "people", "devices", "applications" and "external organizations"
- Better Security
  - Al-based threat detection for privilege escalation, credential access, lateral movement
  - Bring threat hunting and incident response expertise to every organization

#### Figure 16: AVA Sensors for Campus Threat Hunting

Arista NDR monitoring sensors can be deployed in high traffic areas or run as a process on Arista campus switches. NDR Sensors are deployed locally ensuring that sensitive data does not leave your network. Sensors send summarized metadata to the NDR Nucleus which can be deployed on premises or in the NDR cloud. NDR Nucleus leverages Arista's EntitylQ technology to build a graph of network connected devices and their networked relationship.

EntityIQ does this by analyzing device communications, leveraging AI to glean devices from traffic flow data. Arista NDR leverages EntityIQ to Analyze all devices through Adversarial modeling. Arista NDR provides pre-configured adversarial models which can be customized by administrators through an easy to use AMI interface. Finally, Arista's Ava expert system not only automates the investigation and remediation process, it can also use concourse APIs in Arista Guardian for Network Identity (AGNI) to reclassify suspicious users or appliances to be quarantined from corporate workloads.

#### Identity, Access, Segmentation and Monitoring: Arista's ZTN Framework

A perennial challenge to campus and information security administrators is the maintenance and updating of users, groups, devices and segmentation policies in the campus enterprise. Legacy network access control (NAC) implementations further complicate this challenge with their complex workflows, complex integrations and costly patching and upgrades.



Figure 17: Streamlined Integration with Identity Managers



Arista's AGNI solution streamlines maintenance, onboarding and integration, while also automating reclassification of suspicious actors so managers can quickly quarantine malicious activities before there's pervasive harm. Concourse APIs in AGNI facilitate integrations with major security partners, supporting automatic reclassification actions against suspicious users or appliances. AGNI supports a variety of user identity tools, Pre-shared keys and certificates, including guest, web, and BYOD services to preserve existing workflows and investments.

Equally critical to the Zero Trust Network Framework are segmentation services to ensure workgroup and workload security. Arista campus wired and wireless platforms support common standard segmentation features such as 802.1Q, VRFs and VXLAN. Arista builds upon these industry standards by providing Multidomain Segmentation Services (MSS) that delivers pinpoint, intra and intersegment policies to address appliance to appliance or client to client threats.

Arista MSS correlates endpoints with workgroups and identity tags. These tags are only used within Arista platforms for policy actions. No proprietary network encapsulations! Network traffic is standard, supporting interoperability in brownfield deployments. Arista CloudVision orchestrates tags in MSS, and with workgroups among popular NAC solutions, including AGNI, allowing MSS to enforce policy set by NAC platforms.

Together, AGNI, MSS and NDR work together to automatically monitor, segment and secure the campus network, greatly reducing threat remediation time, human factor errors and their associated costs. At the same time, Arista's ZTN framework improves operator responsiveness to new threats and workloads, while improving overall uptime and workgroup productivity.

#### **Cognitive Campus: Client to Cloud Use Cases**

As campus networks evolve to support new workloads, many examples and use cases are emerging:

- Deploying and managing branch networks at scale
- Enhanced client to cloud automation
- Monitoring the distributed campus workforce and appliances
- End-point monitoring to pinpoint performance hotspots
- Cognitive Zero Trust Network Architecture

Here are a few examples:

#### 1. CloudVision and CUE Managing the Extended Network

Fast and fault-free provisioning of edge or enterprise branch networks relies on provisioning tools leveraging templatized, validated network topologies so workers and IoT appliances can reliably connect to resources. Arista's Validated Design (AVD) architecture offers a suite of provisioning templates for both wired and WIFI, that's deployable by CloudVision and CUE WIFI manager. Using Arista's ubiquitous EOS, operators have myriad options, from conventional 802.1Q/L2 networks to sophisticated multisegment, multisite EVPN networks. These architectures are supported across Arista's entire WIFI and switching portfolio, from the compact 710P series switches, to stacked SWAG platforms, to the modular 750X series.

Likewise, Arista's CUE WIFI manager allows operators to templatize designs for workgroups and segments, (including guest and dynamic WIFI segments using Unique Pre-Shared Keys [U-PSK]) for quick Zero Touch provisioning from on prem or cloud servers. Arista CUE provides consistent provisioning, monitoring and troubleshooting across the entire portfolio of C200(WIFI6), C300(6E) and the new C400(WIFI7) series access points. CUE's included WIPs services provide unparalleled perimeter monitoring and remediation of wireless devices stemming from misconfiguration or malicious actors. Lastly, Arista CloudVision and CUE platforms are field proven to manage thousands of devices in global enterprises.



Figure 18: Campus Enterprise Portfolio

#### 2. Cognitive Use Case: Securing Users and Resources in the Campus

ARISTA

Campus administrators struggle to manage the interaction of users and IoT appliances and their corresponding workloads. While firewalls and agent monitors help manage client to server workflows, they don't address agentless IoT clients nor lateral communications between clients or appliances. The challenge of securing and protecting information is paramount, but extreme measures may degrade or outright break legitimate applications. Lastly, the complexities of maintaining heterogeneous legacy infrastructure can be its own full-time job as managers must certify discrete platform images for different parts of their multi-tiered network.

Arista Multi-domain Segmentation Services (MSS) builds upon conventional network access control (NAC) functions (such as AGNI), and standards based segmentation (e.g. 802.1Q, VXLAN, etc). MSS delivers micro segmentation enforcement capabilities in Arista campus platforms to enforce inter and intra-segment policies on IoT appliances as well as conventional user clients and servers. MSS achieves this by identifying segment members through their IP network traffic and then drop, permit or redirect according to security policy.



Figure 19: Automation and Feedback Delivering Continuous Security

MSS architecture also provides policy monitoring and compliance feedback which is provided by Arista's ZTX appliance. Working with CloudVision, ZTX reports existing and new workflows, and helps correlate workflow changes, pre and post policy enforcement. ZTX and CVP helps administrators validate policy efficacy while also protecting against adverse effects on known good workflows.

Adding network based threat detection to this security portfolio helps fulfill the InfoSec team's objectives of monitoring, classifying, segmenting and validating security policy in the enterprise. NDR sensor agents in Arista platforms send traffic to the Nucleus threat analyzers, searching for known threat vectors. In the event of a hit, NDR alerts Arista's AGNI NAC through the concourse API, so the offending devices are quarantined to mitigate any security breaches.

#### 3. Connecting and Monitoring the Distributed Workforce

ARISTA

Arista Wi-Fi supports standard IPSEC tunneling features that allow remote workers to securely connect into the campus network and have complete access to enterprise resources. The remote workforce simply plugs in their access point and it automatically boots and receives credentials to connect to the campus. The W-318's embedded TPM module ensures secure boot and provides IP-SEC hardware acceleration, delivering up to 1Gbps of encrypted network traffic to support demanding, I/O intensive, remote user applications.

**Geographic Views** 

## **Global Enterprise Management**

ARISTA



Figure 20: Global Manageability and Remote Connectivity

Arista's Zero Touch Provisioning (ZTP), lets administrators templatize configurations, streamlining deployment, maintenance and control.

Arista's WIFI coverage feature and end point locator leverages Wi-Fi telemetry collected by CUE to show approximate client locations and portray coverage performance of users and assets in campus offices as seen in Figure 21.



Figure 21: RF coverage and Workforce/Asset Tracking and Reporting

These WIFI visualization tools streamline RF based troubleshooting, offering operators insights to the health of the campus WIFI network.

4. Cognitive Use Case - Intelligent Workflow and Endpoint Monitoring

ARISTA



Figure 21: CloudVision Telemetry Visualization from Client to Cloud

Arista Campus LAN and Wi-Fi platforms deliver real-time device flow tracking and real-time telemetry to CloudVision, so administrators can monitor key performance indicators and maintain service levels in the cognitive campus network. CloudVision's endpoint Analyzer and IoTvision visualize device connections and correlate network, application and IoT/user flow data, alerting administrators of performance or security issues. Administrators can review alerts and historical data to pinpoint and remedy network anomalies before applications are adversely impacted or users even notice.

IoTvision: An evolution of CloudVision's device analyzer, IoTvision extends visibility, classification and monitoring to all networked IoT devices, wired or Wi-Fi. CloudVision's analytics turbines process flowtracker and SFlow session telemetry to identify, locate and correlate all kinds of campus appliances like sensors, security devices, phones and printers, to name a few. IoTvision's database catalogs appliances, allowing administrators to locate devices, review their communications sessions, identify MAC/IP details and more signatures when possible. IoTvision is a key asset for administrators who need to know the status and interaction of business critical worker devices, security systems, and facilities appliances.

#### arista.com

**Campus Operator** 

Workflows

## **Endpoint Overview**

ARISTA



Figure 22: Expanding Monitoring and Visibility to Campus IoT Devices

## 5. Cognitive Use Case - Comprehensive Campus Security: from WIPS perimeter monitoring, to Access control, Segmentation, and Security Validation

Campus security officers must balance security requirements against worker productivity. To optimize the balance of security and accessibility, campus administrators and infosec personnel must look for campus networking solutions that preserve existing infrastructure and applications while supporting a large ecosystem of segmentation partners that offer a variety of credential, single sign-on, or IoT-centric behavioral authentication systems.



Architects are wise to avoid closed architectures, opting for economical, open, standards-based segmentation services to partition critical workloads or isolate

suspect workflows across a campus-wide, multi-vendor environment. For pinpoint workgroup and device segmentation, Arista offers Multi-domain Segmentation Services (MSS). Arista campus platforms, key traffic to workgroups and segments interdevice communications according to policies defined, through CloudVision's studios or identity services like AGNI or other prominent NAC solutions. Using these segmentation options, the campus is dynamically configured to enforce security policy with no impact to other workloads. Arista's ZTX network traffic analyzer validates enforcement efficacy while also identifying flow anomalies requiring InfoSec scrutiny. Lastly, NDR sensor agents in Arista switches allow AVA NDR to identify new threats and not only alert InfoSec of the issue but also propose AGNI policy adjustments to protect against the threat. Arista's combined ZTN solution simplifies campus network administration, and helps automate security enforcement, supporting standard traffic segmentation technologies.

Easy Wi-Fi accessibility poses a continuous security challenge to campus administrators. To ensure the security of campus airwaves, cognitive Wi-Fi systems must continuously monitor the campus perimeter, and accurately sort valid corporate WIFI devices and users from perimeter threats and harmless neighbors. Arista's Cognitive Wireless Intrusion Protection Services (WIPS) provides a comprehensive architecture. Starting with dedicated scanning resources at the edge, telemetry is fed to Arista's Cognitive WIPs turbines which constantly log, identify and categorize performance and threat assessments to ensure the security and availability of the campus Wi-Fi.





Figure 23: Key Attributes of Cognitive Wi-Fi Including Intrusion Detection/Prevention

Arista's patented technology helps WIPS quickly identify rogue access points, evil twins and impersonators, allowing AVA automation to pinpoint corrective measures that secure corporate WIFI resources.

#### Summary

Embracing the new hybrid workforce model requires thoughtful assessment of the performance, availability and safeguarding of critical workload applications throughout the enterprise. Increasing dependency on workforce collaboration and meeting tools, coupled with the growing adoption of IoT devices has dramatically increased the list of business critical applications requiring assurance. Designs must evolve from brittle complexity to uniform networking systems leveraging automation, to quickly adapt to constant evolutions while simultaneously lowering TCO.

Arista's expanded campus platform portfolio, running its universal EOS, managed from the edge to home office with CloudVision, and secured with Arista's Zero Trust, NAC, segmentation and NDR threat monitoring, delivers the next level of dependable performance and user experience, for network administrators and the distributed workforce.

The contrast between other's AI networking hype, with its inherent idiosyncrasies and immaturity, versus Arista's pragmatic automation and cognitive, data-driven actions, is clear. Arista's portfolio of cognitive campus LAN, Wi-Fi and holistic network security offerings, founded on EOS, and managed by CloudVision, allows IT managers to implement an adaptive and cognitive campus architecture that will meet the enterprise's current and future challenges.

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 © 2024 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. December 3, 2024 02-0078-12