ARISTA | ACADEMY

CAMPUS

Operations & Engineering

Arista Academy Campus Track

The Campus track equips network professionals with the knowledge and skills required to configure, troubleshoot, and manage Arista Layer 2 and 3 Campus network designs. You will explore key topics such as Arista Campus Architecture, CloudVision (CVP/CV-CUE), Layer 2 and 3 Wired Campus Networks, Wireless Fundamentals, Campus Wireless Deployment, and Campus Security. This course also includes hands-on labs to reinforce theoretical knowledge with practical application. The Campus track is divided into two distinct sub-tracks: Operations and Engineering. The Operations sub-track focuses on Day-2 tasks such as telemetry and troubleshooting, while the Engineering sub-track concentrates on the design and architecture of L2 campus networks.

Who Should Enroll

Network engineers and administrators managing campus network infrastructure and responsible for troubleshooting and maintaining campus networks.

Learning Format

Arista Campus track is available as Self-Paced learning (Academy Digital) or Private live instructor lead class (Academy Live).
Additional supplemental content is available with Academy Digital

Skills Developed

- Understand and implement Arista's modern Layer 2/3 Campus network solutions.
- Configure and manage wired and wireless campus networks.
- CloudVision for network automation and management.
- Strengthen campus network security using Zero Trust principles.

Prerequisites

- Solid understanding of Layer 2/3 network technologies and protocols
- Understanding of Spine/Leaf designs is a benefit

CERTIFICATION

Campus Operations and Engineering sub-tracks each have an optional practical exam. Achieving both certifications automatically grants you the Campus PROFESSIONAL certification. Alternatively, you may take the PROFESSIONAL exam directly bypassing the SPECIALIST exam.

WIRED ENGINEERING SUB-TRACK

Arista campus architecture

Arista Cognitive Campus Solution

- Arista Cognitive Campus Overview

Arista campus architecture overview

- Traditional campus architecture overview
- Arista Universal cloud network architecture
- Campus fabric architecture

Arista Campus Design

- Campus network design options
- Design 1- L2LS with external gateway
- Design 2- L2LS
- Design 3- L2LS with VXLAN-EVPN
- Design 4- L3LS
- Design 5- L3LS with Border leafs
- Design 6- L3LS with VXLAN-EVPN
- Design 7- L3LS with VXLAN-EVPN and Border leafs

Resiliency solutions

- Cognitive PoE
- Stateful Switchover (SSO)
- Smart System Upgrades (SSU)

Arista stacking

- SWAG Overview
- SWAG Architecture
- MLAG vs SWAG
- SWAG Provisioning

Building a L2 wired campus network

VLANs and Inter-VLAN routing

- VLAN Overview
- Configuring Access and Trunk Ports
- Introduction to Inter-VLAN Routing
- Configuring Sub Interfaces
- Configuring SVIs
- Troubleshooting VLANs
- *Lab - Configuring VLANs*

Spanning Tree

- Spanning Tree Overview
- STP Enhancements
- Configuring STP on an Arista Switch
- Troubleshooting STP on an Arista Switch
- *Lab - Configuring MSTP*

LACP

- LACP Overview
- Configuring LACP
- Troubleshooting LACP

MLAG

- MLAG Overview
- Configuring MLAG
- Troubleshooting MLAG
- *Lab - Deploying MLAG*

First Hop Redundancy Protocol

- FHRP Overview
- Configuring VRRP
- Configuring VARP
- *Lab - Configuring VARP*

Build L2LS Campus network using CLI

- Configuring L2LS Campus with CLI

Build L2LS Campus network using CVP configlets

- L2LS Campus design and topology overview
- Configure L2LS campus with CVP configlets

Build L2LS Campus network using CVP Studios

- Onboarding devices to Studios
- Configure L2LS network using Studios
- Configure access interfaces
- Submit workspace and execute change control
- Configure L2LS Campus w/ext gateway using Studios
- *Lab – Deploying L2 Campus with Studios*

Building a L3 wired campus network

L2LS Review

- L2LS Design Review
- L2LS Example

L3LS Design

- Introduction to L3LS Design
- VXLAN and EVPN Importance in L3LS Design
- Why BGP Underlay in L3LS Design

Introduction to BGP

- Introduction to BGP and Routing
- BGP Functions and Facts
- BGP Operation
- BGP Route Advertisement

eBGP Underlay configuration

- L3LS eBGP underlay configuration
- eBGP load balancing configuration
- eBGP configuration enhancements

WIRED ENGINEERING SUB-TRACK

BGP underlay deployment options
- BGP with MLAG
- Variations of BGP in L3LS
- *Lab – L3LS Campus underlay with eBGP*

VXLAN Overview
- Introduction to VXLAN
- VXLAN load balancing with ECMP

VXLAN Control plane options
- ARP refresher
- VXLAN Multicast control plane
- VXLAN HER control plane
- Configuring VXLAN HER
- VXLAN VCS control plane
- VXLAN EVPN control plane
- *Lab – Configure VXLAN data plane with HER*

VXLAN with MLAG
- Introduction to VXLAN with MLAG
- Configuring VXLAN with MLAG

VXLAN best practices
- MTU and Jumbo frames
- DF Bit, VTEP, MLAG, and Timers

EVPN Fundamentals
- Introduction to EVPN
- EVPN terminology
- VRF Operations
- MP-BGP control plane
- Configuring MP-eBGP for EVPN
- EVPN route type 2 (MAC-IP)
- EVPN route type 5 (IP Prefix)
- EVPN route type 3 (IMET)
- *Lab – L2 VPN*

EVPN advanced concepts
- VLAN based service interface
- VLAN aware bundle service interface
- Introduction to IRB
- Symmetric IRB vs asymmetric IRB
- Symmetric IRB deep dive
- Configuring symmetric IRB
- Configuring asymmetric IRB
- *Lab – L3 EVPN Symmetric IRB*

EVPN design best practices
- iBGP between MLAG pairs and eBGP multihop command
- eBGP for underlay and overlay

Build L3LS Campus network using CVP Studios
- Configuring L3LS Campus with CVP Studios
- Configuring L3LS Campus with VXLAN and EVPN using Studios
- *Lab – Deploying L3LS Campus with VXLAN and EVPN using Studios*

WIRELESS ENGINEERING - DIGITAL SUPPLEMENTAL

Wireless

Wireless signalling basics
- Introduction to radio frequency waves and signals
- Radio frequency wave properties
- Radio frequency wave propagation

Measuring wireless signals
- Measuring signal strength
- Antennas
- Radiated power measurement

Representing data in radio frequency waves
- Modulation
- DSSS vs OFDM
- OFDMA

Wi-Fi standards
- Radio frequency channels
- 802.11 standards

WLAN Communications
- 802.11 frames
- Wireless client association
- Wireless frame transmission
- Wireless client roaming

802.11 Standards enhancements
- 802.11i MAC security
- 802.11k Radio resource measurement
- 802.11r Fast BSS transition
- 802.11v Wireless network management
- 802.11w Protected management frames
- 802.11e QOS

Deploying Campus wireless networks

Campus wireless architecture
- Traditional Campus wireless architecture
- Arista Campus wireless architecture

Arista CV-CUE
- CV-CUE overview
- Deploying CV-CUE
- Navigating CV-CUE
- Using checkpoints in CV-CUE
- *Lab – Navigating CV-CUE*

Deploying access points in campus
- Onboarding access points to CV-CUE
- Assigning APs to locations and AP groups
- *Lab – Configuring folders and groups*

Managing Aps in CV-CUE
- Configuring AP devices settings
- Connecting AP using LAG
- Configuring AP radio settings

Configuring network profiles
- Configuring port profiles
- Configuring radius servers
- Configuring role profiles
- Configuring tunnel interfaces

Configuring basic enterprise SSID settings
- Understanding mandatory SSID settings
- Understanding types of SSID security
- Understanding SSID network types
- Configuring a WLAN with PSK/GPSK
- Configuring a WLAN with 802.1x
- *Lab – Configuring basic SSID settings*

Configuring advanced enterprise SSID settings
- Enabling access control for clients
- Optimizing RF settings
- Enabling traffic shaping & QOS

Configuring WIPS
- WIPS overview
- Configuring WIPS settings

Securing the Campus network

Zero Trust overview
- Why Zero Trust security
- Zero Trust model
- Zero trust stages
- Challenges with Zero Trust implementation
- Arista Zero Trust solutions

Security basics
- Security basics overview
- ACL overview
- IP Locking
- IP source guard
- Private VLANs
- AAA overview
- RADsec and RADsec proxy
- Encryption and PKI
- EAP overview
- *Lab – Deploying control plane ACLs*
- *Lab – Segmentation using private VLANs*

WIRED OPERATIONS SUB-TRACK

Campus operations with CloudVision

CloudVision overview

- Why CloudVision
- Approaches to network automation
- Introduction to CloudVision
- CVP implementation options

CloudVision setup

- CVP clustering
- CVP Multi-node OVA installation
- CVaaS initial onboarding
- Upgrading CVP
- CVP backup and restore
- Getting familiar with CVP interface
- CVP profiles
- CVP help center
- License key management using CVP
- *Lab – Navigating CVP*

CloudVision Provisioning

Device registration

- Connecting devices to CloudVision
- Manual onboarding

Network provisioning

- Containers
- Configuration sources
- Designed and running config
- Configlets
- Tasks and change control
- Applying configlets to containers
- Reconcile
- *Lab – Configlets*
- Snapshots and staging
- Redesigned change control UI
- Rollback
- *Lab – Snapshots*
- *Lab – Change Control*
- Image repository

Zero touch provisioning

- Zero touch provisioning (ZTP)
- Deploying and onboarding vEOS to CVP using ZTP
- Zero Touch replacement (ZTR)
- Replacing a device using ZTR

CloudVision Campus Studios

Studios overview

- Introduction to Studios and Tags
- Workspaces
- Studio deployment and execution
- *Lab – Using Studios*
- *Lab – Clean up Studios*

Studios in action

- New Studios UI
- Static configuring Studio
- Management connectivity Studio
- Software management Studio
- Authentication Studio
- Mirroring Studio
- Provisioning new devices with ZTP and Studios
- *Lab – Static configuration Studio*

Operating L2LS Campus network with CVP Studios

- Onboarding devices to Studios
- Configure L2LS network using Studios
- Configure access interfaces
- Submit workspace and execute change control
- Managing L2LS campus gateway connectivity with Studios
- Add a new VLAN to L2LS campus
- Modifying VLAN settings in L2LS campus
- Connecting new host to L2LS campus
- *Lab – Deploying L2 Campus with Studios*

Campus Zero Touch operations

- CloudVision Campus dashboard overview
- CloudVision Campus Day 1 – Onboarding
- CloudVision Campus Day 2 – Provisioning and Diagnostics
- CloudVision endpoint analyzer
- *Lab – Day 2 operations with L2 Campus Studios*

Operating L3LS Campus network with CVP Studios

- Configuring L3LS Campus with CVP Studios
- Configuring L3LS Campus with VXLAN and EVPN using Studios
- Adding new access pods to L3LS Campus
- Adding new spines to L3LS Campus
- Adding new VRFs to L3LS Campus
- Add new VLANs to L3LS Campus
- Modifying VRF and VLAN settings for L3LS Campus
- Changing underlay protocol in L3LS Campus
- Connecting new hosts to L3LS Campus
- *Lab – Deploying L3LS Campus with VXLAN and EVPN using Studios*
- *Lab – Day 2 operations with L3 Campus Studios*

WIRED OPERATIONS SUB-TRACK

Monitoring Campus with CVP

Monitoring devices with CVP

- Network hierarchy
- Compliance overview
- Device input power
- 802.1x details in endpoint search
- *Lab – Monitoring Campus with network hierarchy*

Dashboards

- Dashboards overview
- Dashboards enhancements
- Device connectivity health panel dashboard
- Compliance counts dashboard
- Syslog filters dashboard
- Dashboard tabs layout
- Exporting and importing dashboards

Events

- Events overview
- Event groups
- Compliance events
- Config sanity check events
- *Lab – Dashboards and Events*

Topology

- Introduction to topology
- Topology icons and settings
- Custom topology hierarchies
- User defined topology filters
- *Lab - Topology*

EOS Operations upgrades

EOS reloads and upgrades

- Understanding EOS upgrades
- Standard upgrade vs smart system upgrade
- Upgrading EOS with CLI
- Upgrading EOS with CVP
- MLAG ISSU upgrade and reload with CLI
- Chassis upgrade and reload
- MLAG upgrade and reload with CVP

EOS monitoring tools

- SNMP
- sFLow
- Watch and Diff commands
- Latency Analyzer (LANZ)
- Port mirroring

Advanced Event Management (AEM)

- AEM – CLI scheduler
- AEM – Event monitor
- AEM – Event manager
- *Lab - AEM*

Troubleshooting EOS hardware and software

- System and software troubleshooting
- SFP and physical errors
- Arista EOS health checks – CLI and CVP
- Hardware troubleshooting
- Memory and flash errors
- Tcpdump and Iperf
- Installing extensions
- Recovery procedures

WIRELESS OPERATIONS - DIGITAL SUPPLEMENTAL

Managing Wireless operations

Introduction to CV-CUE

- Introducing CV-CUE

CV-CUE operations overview

- CV-CUE features overview
- Wired and wireless monitoring
- Auto Wi-Fi threat detection and prevention
- Auto network assurance
- Auto issue locationing
- Auto client connectivity troubleshooting
- Auto client and network performance issue troubleshooting
- Auto Application troubleshooting
- *Lab – Navigating CV-CUE*

Device firmware update in CV-CUE

- Hitless AP upgrades

CV-CUE AIOps

- Explore overview dashboard
- Analyze app experience using the overview dashboard
- Explore feed dashboard
- Perform operations with Cognitive maps
- Map view persona-based workflows
- Floor plan coverage and throughput SLA

Wi-Fi visibility with CV-CUE

- Reactive and proactive troubleshooting
- Monitor Wi-Fi with CUE dashboard
- Monitor clients with CUE
- Monitor Access Points and RFs with CUE
- Monitor Wi-Fi with Cognitive maps and alerts
- Proactive Wi-Fi monitoring with client connectivity test
- Monitor Wi-Fi with Map views and feed
- View and Compare configuration checkpoints
- *Lab – Monitoring wireless clients*
- *Lab – Monitoring access points*

Wi-Fi visibility with CloudVision

- Monitor devices with CloudVision campus health dashboard
- Telemetry between CVP and CV-CUE

Troubleshoot Wi-Fi issues with CV-CUE

- Proactive network assurance
- Troubleshoot wrong PSK issue
- Troubleshoot RADIUS access reject issue
- Troubleshoot No DHCP IPv4 address issue
- Troubleshoot Low RSSI and low data rate issues
- Troubleshoot high retry rate issue
- Troubleshoot DNS failures IPv4 issue
- Troubleshot Rogue AP issue
- Day in the life of CV-CUE network operator
- *Lab – Client connectivity test*
- *Lab – Troubleshoot Client connectivity issues*

SECURITY ANGNI/MSS - DIGITAL SUPPLEMENTAL

Securing the Campus Network

Zero Trust Overview

- Why Zero trust security
- Zero trust model
- Zero trust stages
- Challenges with Zero trust implementation
- Arista Zero trust solution

Security basics

- Security basics overview
- ACL overview
- IP locking
- IP source guard
- Private VLANs
- AAA overview
- RADsec and RADsec proxy
- Encryption and PKI
- EAP overview
- *LAB – Deploying control plane ACLs*
- *LAB – Segmentation using private VLANs*

Network access control with AGNI

AGNI Overview

- Why do you need NAC
- Introduction to AGNI

AGNI deployment

- AGNI deployment options
- AGNI on-prem design options
- Load balancing across an AGNI node group
- AGNI failover scenarios
- AGNI on-prem setup
- Navigating AGNI

AGNI node operations

- AGNI backup and restore operation
- AGNI cluster operations

Configuring AGNI

- AGNI configuration workflow
- Integrating AGNI with concourse applications
- Configuring identity providers (IDP)
- Adding users and user groups
- Adding access devices
- Generating RADsec certificates for access devices
- Configuring AGNI NAC policies

User and device onboarding

- Generating client certificates manually
- Onboarding suing certificate-based authentication
- Onboarding using MAC authentication
- Onboarding using UPSK

Guest onboarding

- Guest onboarding overview
- Configuring guest onboarding using Guestbook

Monitoring and troubleshooting in AGNI

- Monitoring user and devices sessions

AGNI deployment

- AGNI deployment options
- AGNI on-prem design options
- Load balancing across an AGNI node group
- AGNI failover scenarios
- AGNI on-prem setup
- Navigating AGNI

AGNI node operations

- AGNI backup and restore operation
- AGNI cluster operations

Configuring AGNI

- AGNI configuration workflow
- Integrating AGNI with concourse applications
- Configuring identity providers (IDP)
- Adding users and user groups
- Adding access devices
- Generating RADsec certificates for access devices
- Configuring AGNI NAC policies

Segmentation with MSS

MSS overview

- Introduction to MSS

MSS Campus design

- MSS design and deployment options
- MSS Design 1 – bridge-based wireless
- MSS Design 1 – Incremental insertion of MSS in a brownfield bridge-based wireless campus
- MSS Design 2 – Tunnel-based WiFi
- MSS Design 2 – Incremental insertion of MSS in a brownfield tunnel-based wireless campus

MSS configuration

- MSS configuration workflow
- MSS configurating the ZTX appliance
- Configuring MSS in CloudVision

Troubleshooting MSS

- Show commands and troubleshooting considerations

Headquarters
5453 Great America Parkway
Santa Clara, California 95054
408-547-5500

Training
training@arista.com
www.training.arista.com

Sales
sales@arista.com
408-547-5501
866-497-0000