



H3C Application-Driven Campus Solution

Campus SDN Solution

Release Date: July, 2020



New H3C Technologies Co., Limited

Solution Overview

H3C Application-Driven Campus (AD-Campus) Solution is innovative campus network solution built on SeerNetwork Architecture (SNA). The solution achieves great integration and convergence to easily reflect intent to network operation. With full lifecycle, open architecture and deep intelligence, AD-Campus is along with partner to be committed to solve existing challenges and assist customers to accelerate digital innovation and transformation.

AD-Campus combines VXLAN and the concept of Software-Defined Networking (SDN) to create a new-generation flexible network. It converts campus network from "user adapts to network" to "network adapts to users", enabling users and devices to roam around campus seamlessly, while remaining consistent user experience and simplified network operation. It reduces complexity of network deployment and maintenance and meets the increased requirements of mobility and massive terminal access on campus network.

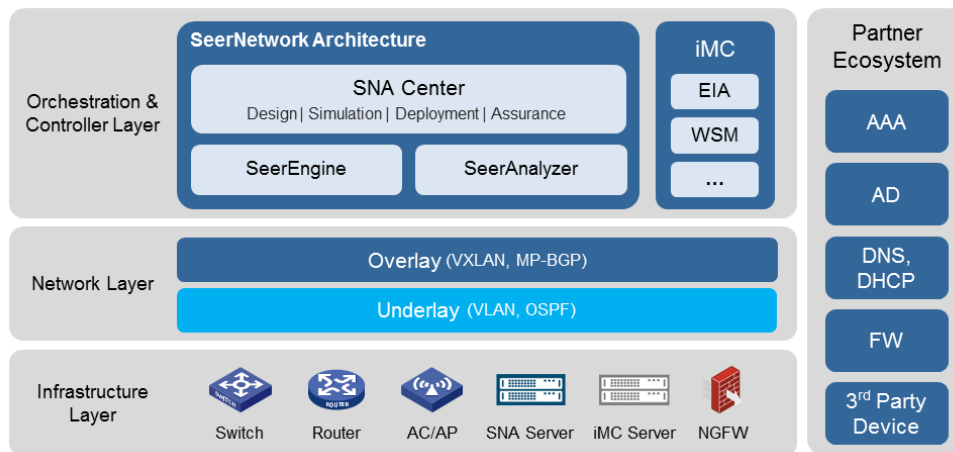


Figure 1. AD-Campus Architecture

Features and Benefits

Intent-based Network

AD-Campus solution adopts SDN architecture, decoupling control plane from infrastructure. As SDN controller, SeerEngine translates business intent into network language to achieve automated end-to-end service provisioning. With GUI and policy matrix, all initialization and policy will be done by several clicks, liberating network engineers or managers from complicated command lines. Furthermore, due to closed loop intent network, the analysis will become feedback to revise existing policy and optimize overall network. Powered by AD-Campus, customer could highly focus on business innovation and enable faster business launch.

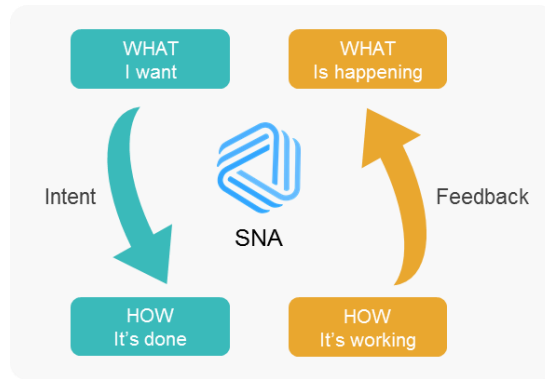


Figure 2. Intent-Based Network

Automation and Simplicity

Configuration becomes more complex with the growth of users and devices. In a traditional campus network, most network installation and changes are manual and primitive, which is prone to human errors.

With AD-Campus solution, customer would design, provision and manage the network on SNA center. The whole system would follow customers' intent and be operated rapidly and simply.

Automated device onboarding: With only three templates (Spine, Leaf, Access), AD-Campus constructs underlay & overlay network automatically without extra manual configuration. There are only four steps to set the entire network to be ready.

- Pre-configure automation templates, including IP & Fabric Plan
- Use scanner or excel to batch import series number
- Power on
- Automatically start deployment

Compared with traditional network, AD-Campus users may experience over 70% reduction in time spent on network automation.

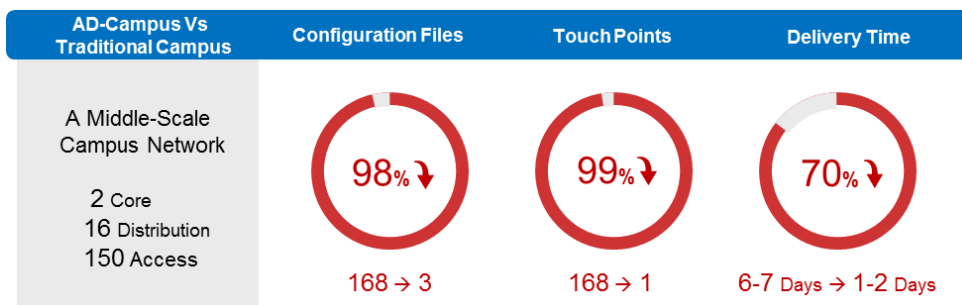


Figure 3. AD-Campus Vs Traditional Campus

Rapid service provisioning: To avoid complicated configuration, misunderstanding of previous code and potential mistake risk by using command lines, AD-Campus saves your effort by automatically distributing policy based on your intent. All the orchestration is clearly shown on the GUI for further operation or correction.

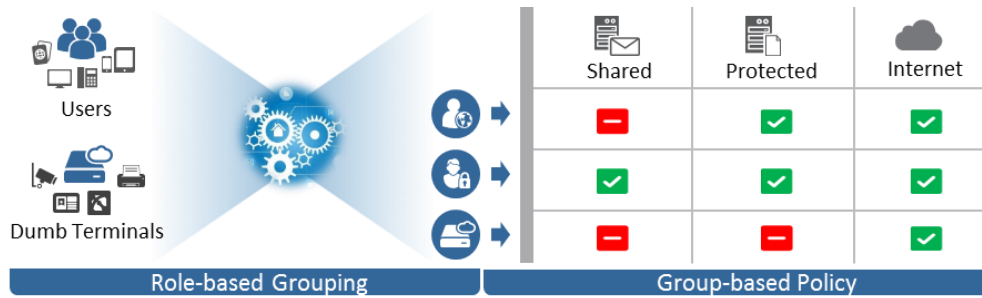


Figure 4. Role-Based Grouping & Group-Based Policy

Expansion & replacement: Once customer needs to expand network or change fault devices, the only thing they need to do is assign specific roles on SNA center for expanded or replaced devices. All the configuration and policy will be synchronized to new devices.

Dumb terminal easy onboarding: Accompanying with explosive development of dumb terminals, network faces authentication and security problems. There are higher requirement on dynamic access authentication to meet the batch deployment demand. Traditional MAC + Port binding may increase the complexity of operation. Furthermore, users pay more attention on privacy, falsification and network attack.

Aiming to solve these pain points, AD-Campus allows fast and secure access at any place of the network. With Automatic Sorting Engine (ASE), it can identify terminals and automatically sort them into correlated groups based on business type with secure isolation.

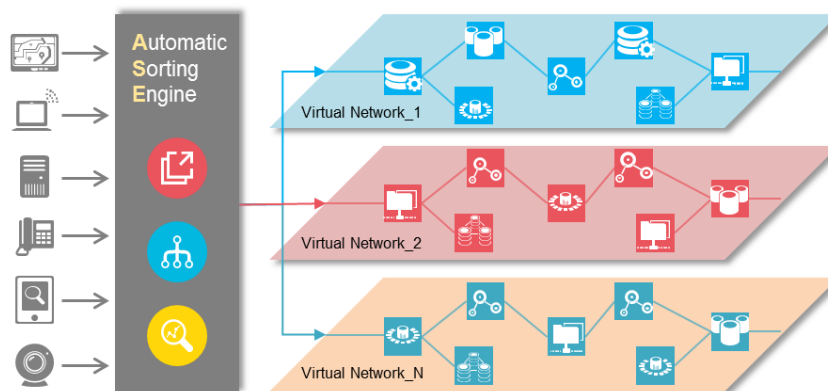


Figure 5. Automatic Sorting Engine

Superior User Experience

In a conventional campus network, IP addresses and security policies change when the users roam. Thus, increasing mobility causes complex network planning, configuration and tests.

AD-Campus creates a location independent campus network, providing optimal experiences for each user on each terminal. Clients can access the network anywhere and anytime without repetitive authentication and authorization. It is also convenient to deploy or move terminals with plug and play function. For network managers, they can easily and efficiently handle management.

AD-Campus constantly delivers customized experience in different scenarios. Users can fix their IP address

or just keep the same roles to acquire seamless experience. With AI empowerment, the solution presents rich information based on different metrics to improve troubleshooting.

- **Client 360***: It provides onboarding time, RF quality, roaming time and other full-scale details about client health, which makes engineers clearly understand how situation clients are and what problem is right now.
- **Wireless optimization***: By locating weak signal issue, access failure issue and roaming issue, AD-Campus gives deep protection of wireless experience.
- **Time travel***: AD-Campus supports display of past events and comprehensive information on timeline, making it easy for engineers to know what happened before and why problems happened.



Figure 6. Superior User Experience

Credibility & Security

To ensure credible access and secure communication, AD-Campus solution provides 5W1H scenario-based authentication and comprehensive security control.

Scenario-based authentication: Besides accounts and codes, AD-Campus realizes flexible and customized requirements by limiting access condition and endpoint type. With this feature, you can allow students to access critical research database in the campus, but not when they are at home using their own laptops.

Segmentation: With policy matrix, customer can easily achieve L2-L4 security control between users and IT resources on campus gateway.

Application-level security: AD-Campus provides service chain to achieve application-level security. In traditional way, you care both service and network. Policies and traffic redirection are always manual and complicated. While in AD-Campus solution, you care only service. The network part is GUI based, automated and virtualized.

Endpoint security: As tremendous endpoints link to network, it is urgent to stabilize network from potential risks due to terminal side.

- **User-endpoint binding:** To meet stringent security and regulatory compliance requirement, AD-Campus provides flexible user-endpoint binding modes, including user-access port binding, user-MAC address binding, and user-IP address binding. Engineer can implement robust control on users and audit their behavior, which is quite efficient to pinpoint problems.
- **Anti-spoofing:** To defend against spoofing attacks, the solution provides dumb terminal anti-spoofing,

* SeerAnalyzer (AIOps) is on roadmap

user-endpoint anti-spoofing and anti-IP spoofing.

- **Endpoint Admission Defense (EAD):** With iNode client, customer could achieve security inspection, behavior auditing and data protection on endpoints.

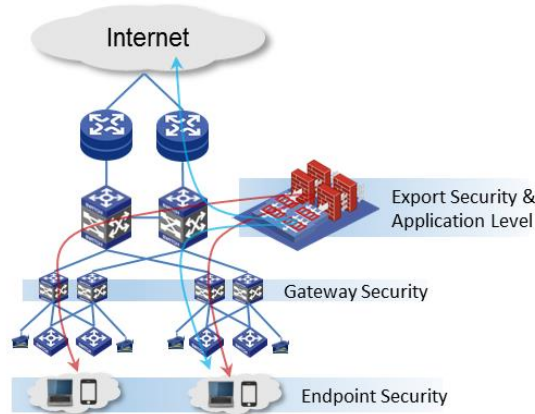


Figure 7. Comprehensive Security

Intelligent O&M

The scale, data traffic and complexity of network are experiencing explosive growth, and traditional O&M becomes tough to handle. AD-Campus introduces SeerAnalyzer* to achieve AIOps.

Health degree*: SeerAnalyzer collects plenty of data from devices, users and application. Tons of data will be transformed, sorted to different factors and fully visualized. With a single dashboard, you can identify network situation, user and service health condition clearly.

Fast troubleshooting*: SeerAnalyzer can trace back past events where malfunction happens and analyze root cause, helping manager reduce interruption and cost.

Trend prediction*: With big data and AI empowerment, SeerAnalyzer may predict future situation. With dynamic threshold, it can trigger alarm more precisely and timely. With traffic and capacity prediction, it can provide best option at the best time.

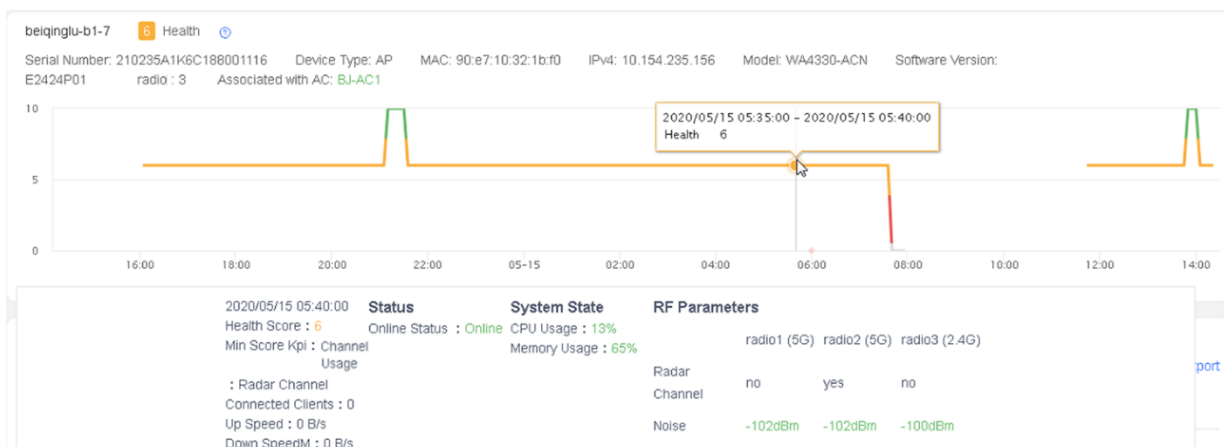


Figure 8. Health Degree of AP

* SeerAnalyzer (AIOps) is on roadmap

Comprehensive Convergence

AD-Campus consistently embeds convergence concept. Through the convergence, the solution has the ability to unify scenarios, simplify operation and centralize management.

Wired & wireless convergence: All wired and wireless O&M will be centralized to one management plane.

Multi-fabric convergence: To ensure unified policy and consistent experience, AD-Campus provides a single platform to design, deployment and management across multi-fabric, which makes the network be adaptable, flexible and efficient

Cross-domain convergence: AD-Campus provides unified orchestration and management between campus and DC, which reduces large number of tasks and supply integrated experience.



Figure 9. Campus-DC Convergence

Values

Simplification

- Automated Deployment and Provisioning
- Superior Consistent Experience
- Cross-Domain Convergence

Enhanced Security

- 5W1H Authentication & Authorization
- Application-Level Security Control

Intelligence

- Continuous Monitoring, Assurance and Optimization
- AI Empowered Troubleshooting & Prediction

Cost Saving & Investment Protection

- Open Architecture (standard RESTful API)
- Third Party Compatibility

Network Model

AD-Campus solution provides three networking models based on different network scales.

Single-Leaf Model: For small and medium-sized networks, propose Single-Leaf model to build cost-effective AD-Campus network.

Standard 3-tier Model: For medium and large-sized networks, propose Standard 3-tier model to build highly automated, extensible and intelligent network.

Multi-Fabric Model: For multi-campus networks, propose Multi-Fabric model to ensure policy consistency.

- Centralized Deployment: Cost-effective, high requirement on consistent service
- Distributed Deployment: High availability, long distance between multiple fabrics.

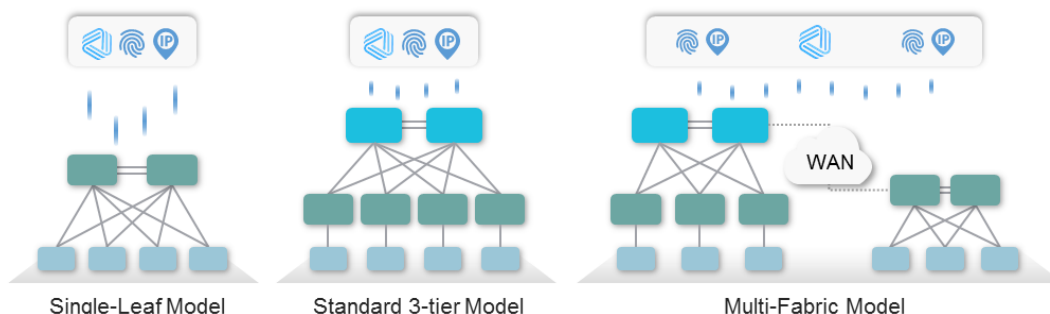


Figure 10. Network Model

Product List

AD-Campus solution provides wide range of available products for hierarchy scenarios.

Product ID	Description
Switch	
Spine	S10500X, S7500E/X
Leaf	S10500X, S7500E/X, S6520X-HI/EI, S5560X-EI
Access	S6520X-SI, S5130S-HI/EI, S3100V3-EI
AC	
WX5860H, WX3840H, WX3820H, WX1800H	
AP	
802.11 ac	WA560, WA538, WA536, WA530, WA530X, WA510H, WA5330, WA5530X,
802.11 ax	WA6622, WA6628, WA6638, WA6330

Ordering Information

Product ID	Description
SNA Center	
LIS-SNACenter-Basic	H3C SNA Center Basic License
LIS-SNACenter-Campus-VAR	H3C SNA Center Software Feature License, 1 Campus Controller Cluster
LIS-SNACenter-SeerAnalyzer-VAR	H3C SNA Center software Feature License, 1 SeerAnalyzer
LIS-vDHCP1000	H3C vDHCP1000 License (Comware 9, Standard Edition, Permanent)
SeerEngine	
LIS-SeerEngine-Campus-BAS1	H3C SeerEngine Campus Additional 1 Server Node License
LIS-SeerEngine-Campus-PSW-VAR	H3C SeerEngine Campus Additional 1 Physical Switch License
LIS-SeerEngine-Campus-PON-VAR	H3C SeerEngine Campus Additional 1 PON Device License
LIS-SeerEngine-Campus-SC-VAR	H3C SeerEngine Campus Additional 1 Service Chain Node License
SeerAnalyzer	
LIS-SeerAnalyzer-Campus	H3C SeerAnalyzer Software Campus Edition License
LIS-SeerAnalyzer-Campus-Analyzer	H3C SeerAnalyzer Software Campus Edition Analyzer License, 1 Managed Node
LIS-SeerAnalyzer-Campus-M-VAR	H3C SeerAnalyzer Software Campus Edition License, 1 Managed Modular NE
LIS-SeerAnalyzer-Campus-F-VAR	H3C SeerAnalyzer Software Campus Edition License, 1 Managed Fixed-Port NE
LIS-SeerAnalyzer-Campus-AP-VAR	H3C SeerAnalyzer Software Campus Edition License, 1 Managed AP
iMC	
SWP-IMC7-IMP	H3C iMC, Intelligent Management Platform Standard Edition
SWP-IMC7-EIA	H3C iMC, End-user Intelligent Access Component
SWP-IMC7-EAD	H3C iMC, Endpoint Admission Defense Component
SWP-IMC7-WSM	H3C iMC, Wireless Service Manager Component
LIS-IMC7-IMP -25/50/100/200/500/1K	H3C iMC, Intelligent Management Platform Standard Edition, 25/50/100/200/500/1000 Licenses
LIS-IMC7-EIA -50/200/500/2K/5K	H3C iMC, End-user Intelligent Access Component, 50/200/500/2000/5000 Licenses
LIS-IMC7-EIA -50/200/500/2K/5K-EIP	H3C iMC, End-user Intelligent Access Component, End-user Intelligent Profiling, 50/200/500/2000/5000 Licenses
LIS-IMC7-EAD -50/200/500/2K/5K	H3C iMC, Endpoint Admission Defense Component, 50/200/500/2000/5000 Licenses
LIS-IMC7-WSM -50/100/200/500/1K/2K/5K	H3C iMC, Wireless Service Manager Component, 50/100/200/500/1000/2000/5000 Licenses
LIS-IMC7-WSM -50/100/200/500/1K/2K/5KAP-L	H3C iMC, Wireless Service Manager Component, Location Service, 50/100/200/500/1000/2000/5000 Licenses (AP)
LIS-IMC7-WSMA -50/100/500-W	H3C iMC, Wireless Service Manager Component, Intrusion Prevention System, 50/100/500 Licenses



The Leader in Digital Solutions

New H3C Technologies Co., Limited

Beijing Headquarters
 Tower 1, LSH Center, 8 Guangshun South Street, Chaoyang District, Beijing, China
 Zip: 100102
 Hangzhou Headquarters
 No.466 Changhe Road, Binjiang District, Hangzhou, Zhejiang, China
 Zip: 310052
 Tel: +86-571-86760000
 Fax: +86-571-86760001

Copyright ©2020 New H3C Technologies Co., Limited Reserves all rights

Disclaimer: Though H3C strives to provide accurate information in this document, we cannot guarantee that details do not contain any technical error or printing error. Therefore, H3C cannot accept responsibility for any inaccuracy in this document. H3C reserves the right for the modification of the contents herein without prior notification

<http://www.h3c.com>