At a glance

HPE Aruba Networking Central NetConductor Use Cases

Cloud-native network orchestration and automation for Zero Trust and SASE security from edge to cloud

Businesses are accelerating their digital transformation initiatives to deliver new user experiences, implement new business models, and achieve greater IT efficiency. The network is a critical enabler that determines the agility with which businesses can innovate. With the rapid adoption of IoT driven use cases and hybrid work initiatives, network strategies need to flexibly adapt to changing business demand, and this has key implications for security.

Traditional security approaches that focus primarily on the perimeter of the network become ineffective as standalone security strategies. With HPE Aruba Networking's built-in foundation for Zero Trust and Secure Access Service Edge (SASE) security frameworks, HPE Aruba Networking ESP (Edge Services Platform) offers edge-to-cloud security by applying rigorous security best practices and controls to previously trusted network resources.

Why adopt role-based access security?

A fundamental concept of both Zero Trust and SASE security frameworks is the implementation of access control policies that grant least-privilege resource access for a device or user, restricting them from accessing resources that are not required to complete their tasks. Access control policies based on IP-addresses, subnets, or users' locations result in a highly manual, error-prone network configuration that cannot scale at the pace that the business demands.

HPE Aruba Networking's market-leading Dynamic Segmentation establishes least-privilege access to IT resources by segmenting traffic based on roles and associated access permissions. Dynamic Segmentation unifies role-based access and policy enforcement across wired, wireless, and WAN networks, ensuring that users and devices can only communicate with destinations consistent with their role—keeping traffic secure and separate.

What is HPE Aruba Networking Central NetConductor?

As networks get increasingly complex and globally distributed, organizations need to segment traffic more efficiently, control access to sensitive applications, and ensure data privacy. Organizations are exploring the adoption of network overlays and protocols such as EVPN/VXLAN for scale, standardization, increased protection, and efficiency gains. They are also looking for effortless deployment and provisioning of network infrastructure with minimal manual intervention. However, these initiatives require a high level of expertise and introduce significant configuration complexity and management overhead, overburdening both IT and security teams.

HPE Aruba Networking Central NetConductor addresses the above problem with cloud-native security services, simplified network configuration with overlay and underlay-based enforcement, enabling organizations to automatically configure network infrastructure for optimal performance and consistently enforce granular access control security policies at global scale for both campus and data center environments. With HPE Aruba Networking Central NetConductor, Dynamic Segmentation can be managed from the cloud with the ability to centrally define and enforce access policies either in a distributed or centralized fashion, based on the choice of overlay. HPE Aruba Networking Central NetConductor provides network administrators and security teams a shared toolset for protecting and optimizing the network.

The following use cases elaborate the capabilities of HPE Aruba Networking Central NetConductor solution components with potential deployment scenarios in customer environments across industries.

Use case #1: Identification and securing of network endpoints

Problem:

A global healthcare provider was modernizing their wired and wireless network to enable future-ready infrastructure with scalability, automation, and built-in security. Adapting to post-pandemic expectations, they wanted to provide improved clinical experiences, personalized patient care and the ability to rapidly introduce new digital processes.

Solution components

Client Insights—Built-in, AI-powered client visibility and fingerprinting capability that leverages infrastructure telemetry and ML-based classification models to eliminate network blind spots.

Cloud Auth—Enables frictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores.

Policy manager—Defines user and device groups and creates the associated access enforcement rules for the physical network.

Fabric wizard—Simplifies the creation of overlays for both campus and data center environments using an intuitive, graphical user interface and automatic generation of configuration instructions that are pushed to switches and gateways.

Network wizard—Simplifies the creation of underlay network comprising of campus and data center CX switches. This wizard enables IT teams to achieve significant time savings and eliminate manual errors by automatically identifying and enforcing configuration and network topology

However, with the blurring of physical boundaries of care and rapid proliferation of guest and IoT devices, the organization needed to ensure that all medical devices, users, and things are profiled and correctly assigned network access. Security blind spots would mean exposure to vulnerabilities, risking adherence to data privacy guidelines. Given their scale of operation, an additional solution for device visibility was not a preferred option.

Solution:

With Client Insights on Central, the customer was able to implement AI-powered client identification and profiling without installing additional collectors or agents. Client Insights leverages native infrastructure telemetry from access points, switches, gateways, and clients. ML-based classification models are used to identify and accurately profile a wide variety of clients, including a diverse set of IoT devices. Client Insights also allows for continuous monitoring of clients, which as a component of HPE Aruba Networking Central NetConductor or when paired with ClearPass provides closed loop, end-to-end access control.

With Client Insights, the healthcare provider was able to accurately profile devices including medical devices such as patient monitors, infusion pumps, and lab diagnostic equipment, pairing it with ClearPass to restrict access to authorized users. This was a critical first step in their journey to adopt role-based access security globally using HPE Aruba Networking Central NetConductor.

Use case #2: Accelerated network deployments with automatic topology identification

Problem:

A large university spanning across multiple sites was planning to refresh its decade-old switches with CX switches. Their centralized IT team that caters to 10,000+ students, had to configure and provision 1000 switches over the summer break of 3 months. Such massive infrastructure refresh projects occur very rarely for this university, and the team was not adequately skilled to support this initiative.

They used to manually configure and provision switch interfaces individually, which took on an average 2 hours per switch. Given the scale of this project and the timelines involved, this approach was not feasible, as it was error-prone and prevented IT teams from focusing on higher priority critical tasks. Hence, they were looking for a solution that could provide a streamlined and automated way to configure and deploy their switches efficiently.

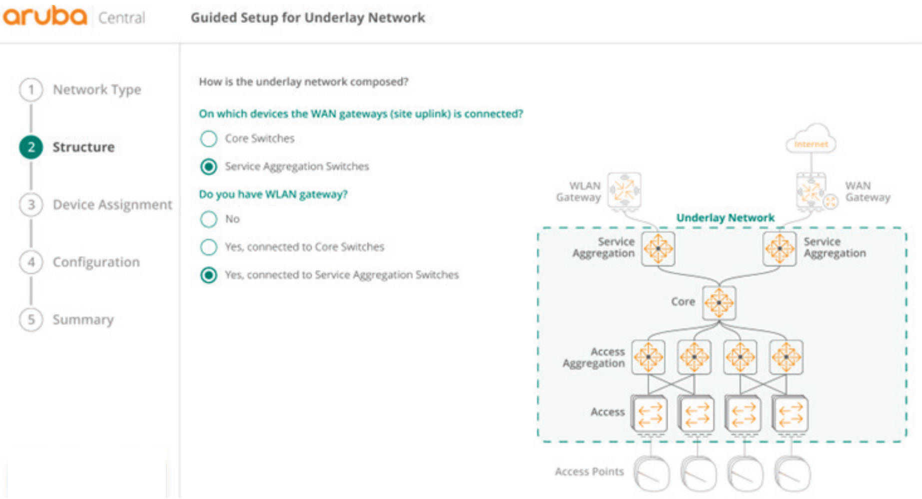
Solution components

Group policy identifier (GPID)— Carries client policy information in traffic for in-line policy enforcement, reducing configuration and security overheads

Fabric-capable HPE Aruba Networking switches and gateways—Supports configuration and enforcement based on the routing instructions and access privileges defined in the group policy identifier.

Solution:

With HPE Aruba Networking Central NetConductor network wizard, this customer was able to create underlays by automatically discovering the physical topology (see Figure 1) and configuring the underlay network for their campus sites. The guided set-up of the network wizard allowed the IT team to build their L3 network quickly and seamlessly. With minimal inputs, the topology was automatically discovered, and the IT teams could toggle between the topology view and list view to identify the core, access, and aggregation switches. Configuring the L3 links between the switches was a breeze, as individual device IP address was intelligently applied from the IP subnet pool provided by the IT team, and they no longer had to manage individual switch interfaces, saving a lot of time and effort. This entire process did not require coding or advanced technical knowledge and was successfully conducted by L1/L2 engineers. The university was able to streamline operations and simplify network configuration by starting with the network wizard and subsequently make incremental configuration changes using the UI-based approach if any of the switches required additions/deletion of configurations.



How is the underlay network composed?

On which devices the WAN gateways (site uplink) is connected?

○ Core Switches

● Service Aggregation Switches

Do you have WLAN gateway?

○ No

○ Yes, connected to Core Switches

● Yes, connected to Service Aggregation Switches

Figure 1. Guided setup for undelay network

Use case #3: Automated policy enforcement at global scale

Problem:

A multinational chemical manufacturer was undertaking a network modernization initiative for enhanced scale and agility, as part of their global expansion. With a large, distributed network involving office and industrial environments, their current approach to policy management was getting prohibitively complex and inefficient.

Every change or addition required manual updates to several lines of ACL statements at multiple touchpoints. Apart from operational complexity, this CLI-codified knowledge was not easily transferable and relied heavily on individual expertise, imposing an organizational risk.

The campus environment was comprised of wireless-capable devices including guest devices, IoT devices, managed workplace devices, conferencing room technology, smart building technology, and printers. Data centres contain physical and virtual servers, storage, and backup equipment, as well as security and monitoring systems. The industrial environment supported production equipment, lab research equipment, assembly line controls, site security and industrial IoT. Each of these environments have a complex matrix of access policies to maintain security.

The organization was looking for a centralized, overlay-based approach to access policies that was easy to implement and required minimal manual intervention on a day-to-day basis.

Solution:

With the HPE Aruba Networking Central NetConductor policy manager, the customer was able to simplify and automate policy management across their global network. Policy manager enabled the translation of security intent into policy design with centralized definition of user and device groups and associated role-based policies, abstracting the underlying complexity of physical network constructs (See Figure 2).

For example, network administrators could translate rules such as “Allow a research engineer access to the lab equipment from the workstation, deny access from a personal device, or grant HR employee access to payroll applications running on virtual machines in the data center, while restricting access to SAP® applications” into network policies via business intent workflows, eliminating the creation and maintenance of hundreds of ACL statements and dynamic port reconfigurations.

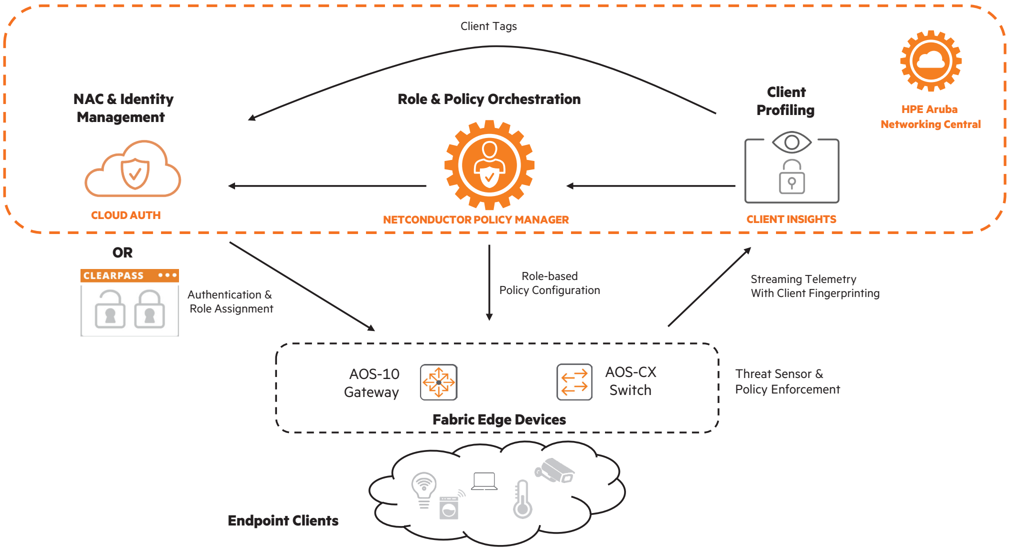

Client Tags
NAC & Identity Management
Role & Policy Orchestration
Client Profiling
HPE Aruba Networking Central
CLOUD AUTH
NETCONDUCTOR POLICY MANAGER
CLIENT INSIGHTS
OR
CLEARPASS
Authentication & Role Assignment
Role-based Policy Configuration
Streaming Telemetry With Client Fingerprinting
AOS-10 Gateway
AOS-CX Switch
Threat Sensor & Policy Enforcement
Fabric Edge Devices
Endpoint Clients

Figure 2. Global role-based policy orchestration with HPE Aruba Networking Central NetConductor

The role information is propagated through a standards-based EVPN/VXLAN distributed overlay fabric and is interpreted inline by HPE Aruba Networking Central CX switches and gateways for continuous enforcement. If the security status of a client changes, its role is automatically modified to restrict access; that role change is then propagated to the network. This is done by embedding group policy identifiers (GPID) that carry policy information into the packet header, allowing the network to carry access control information via the traffic itself. Central NetConductor also allows centralized policy enforcement for smaller office environments with the help of firewall and gateways.

An additional point of delight for the customer was the seamless integration with ClearPass NAC that they were already using for their wireless environment and interoperability with a third-party NAC solution that they were leveraging for their wired environment.

Use case #4: Automated fabric deployment and orchestration

Problem:

A transport and locomotive manufacturing major with hundreds of global sites, consisting of multiple buildings was undertaking site expansions in multiple locations in support of a new business initiative. As part of this, they were considering the use of an overlay fabric to allow certain legacy industrial applications that leveraged Ethernet protocols to be distributed across the campus. They also wanted to accomplish this without extensive IP address remapping.

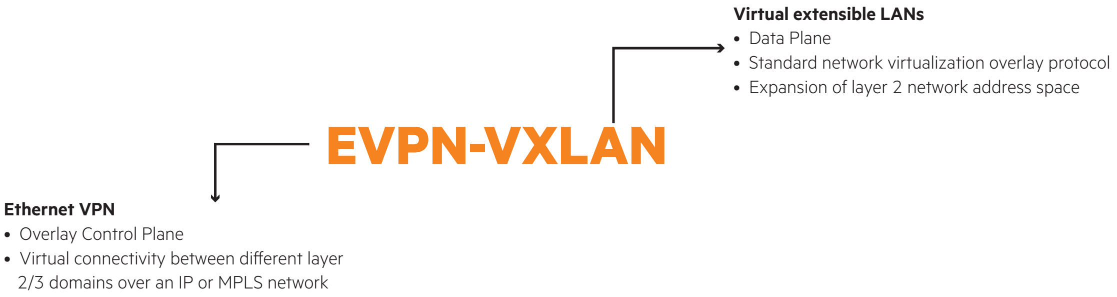
However, with a centralized team of IT experts and shortage of specialist skills, they were skeptical about the complexity involved in deploying and maintaining a fabric with minimal local IT expertise. It was also important to eliminate redundant tasks and downtime due to human errors, which could lead to delays in time to production.

Solution:

With the HPE Aruba Networking Central NetConductor fabric wizard, the customer was able to simplify and accelerate the deployment of an overlay fabric by close to 80%. The automation and resultant gain in efficiency was a force multiplier that resulted in faster time to production.

Fabric wizard leverages simple UI-driven workflows to translate business intent into fabric-wide configurations. The resultant CLI configurations are automatically pushed to the underlying devices, transforming a week-long process involving thousands of lines of manual code and configuration rules, into one that can be accomplished in minutes without introducing human errors. The IT team did not require extensive knowledge of fabric concepts such as EVPN, VTEPs, VNIs, and VRFs and there was no CLI coding dependency on local IT teams. Central NetConductor also orchestrates the stitching of multiple fabrics across the network, allowing customers to horizontally scale and eliminate the need for dedicated hardware as end-to-end role propagation and policy enforcement is possible using the CX border switches

They also intend to leverage the overlay fabric to adopt role-based access policies with HPE Aruba Networking Central NetConductor policy manager across their hundreds of globally distributed sites.



Virtual extensible LANs
- Data Plane
- Standard network virtualization overlay protocol
- Expansion of layer 2 network address space

Ethernet VPN
- Overlay Control Plane
- Virtual connectivity between different layer 2/3 domains over an IP or MPLS network

Figure 3. EVPN/VXLAN standards-based overlay fabric

Use case #5: Third-party interoperability and phased migration

Problem:

An automotive manufacturer with manufacturing plants and corporate offices in all major geographical regions wanted to implement end-to-end segmentation with group-based policies across their global network.
They were looking for a granular and consistent approach to define user/device groups and policies to govern which applications and services these groups can access.

Their larger locations had thousands of switches, tens of thousands of access points, and at least hundred thousand client endpoints. Managing a network of this scale with constant manual intervention was leading to operational inefficiency and increased cost.

While it was evident that the use of an overlay fabric would alleviate these scale challenges, the customer had third-party network infrastructure in their core environment. Given strategic business priorities and budgetary constraints, an infrastructure refresh with a forklift upgrade was not a viable option.

Solution:

With HPE Aruba Networking Central NetConductor, the customer was able to deploy an intelligent overlay across the global enterprise based on the widely adopted EVPN/VXLAN protocols (See Figure 3). Because no proprietary mechanisms were involved and a standards-based technology stack was leveraged, the customer's existing third-party network devices could participate in the underlying physical network with no rip and replace.

UI-based intuitive workflows helped them translate their business intent into validated configurations that were then automatically deployed. The overlay health is also constantly monitored for AI-powered recommendations and automated troubleshooting by HPE Aruba Networking Central.

This provided the organization much-needed agility and helped free up their IT teams to focus on strategic projects. They are now on a phased migration path to unify management of their wired and wireless network with HPE Aruba Networking Central.

Use case #6: Solution adoption flexibility

Problem:

A global financial services provider was implementing digital transformation initiatives for improved customer and employee experiences. While they wanted to deliver a consistent omni-channel experience for their customers, they also wanted to enable secure hybrid work capabilities for their employees to work from anywhere.

This required a streamlined implementation of role-based policies across their global environment. The customer was already leveraging Dynamic Segmentation for role-based access across branches in some of their major locations.

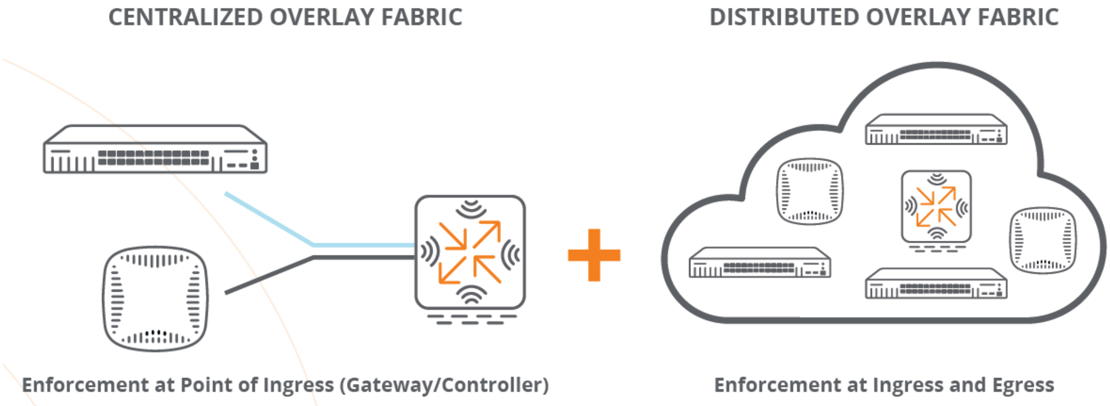

CENTRALIZED OVERLAY FABRIC
DISTRIBUTED OVERLAY FABRIC
Enforcement at Point of Ingress (Gateway/Controller)
Enforcement at Ingress and Egress

Figure 4. Global role-based policy orchestration with HPE Aruba Networking Central NetConductor

They now wanted to unify role-based access and policy enforcement globally across their wired, wireless, and WAN networks while still protecting their current investments in environments that were leveraging gateways for greater security and scale.

Solution:

With HPE Aruba Networking Central NetConductor, the customer was able to adopt a distributed overlay-based approach across their larger campus environments. Adoption of a distributed overlay fabric in these environments ensured high performance and scalability, while eliminating the need to send traffic outside its optimal path for security inspection.

They were also able to retain the existing centralized overlay based approach in the smaller branches that had limited IT personnel and required a simple, easy-to-deploy approach. HPE Aruba Networking gateways function as ingress policy enforcement points in the centralized model which makes use of GRE tunnels between switches, access points, and gateways, delivering enhanced security with stateful, Layer 7 Policy Enforcement Firewall and deep packet inspection capabilities.

Because centralized and distributed models can co-exist in an environment, the customer plans to move to a distributed approach over-time with policies centrally defined through HPE Aruba Networking Central NetConductor policy manager and enforcement carried out by access devices.

Key takeaways

As customers across industries modernize their networks, they are faced with unique visibility and security challenges that necessitate the adoption of role-based access policies as a foundation for implementing Zero Trust and SASE security frameworks. However, customers do not want a one size-fits-all solution that requires an overhaul of the existing environment.

HPE Aruba Networking Central NetConductor provides cloud-native security services for network orchestration and policy management, simplifying policy design and network operations with intent-driven automated workflows. Although optimized for HPE Aruba Networking, HPE Aruba Networking Central NetConductor is specifically designed for flexibility and interoperability, enabling customers with networks of any size and complexity to adopt the solution at a pace defined by their business needs.

Learn more at

arubanetworks.com/CentralNetConductor

Make the right purchase decision.
Contact our presales specialists.

Contact us

Visit **ArubaNetworks.com**

Hewlett Packard
Enterprise