ESP Data Center Design

Validated Solution Guide

Aruba Solution TME

May 20, 2022

Table of Contents

ESP Data Center Design

This guide is intended to help an IT professional understand the following design considerations for a data center environment:

- Hardware selection
- Software selection
- Topology
- High availability
- Scalability
- Application performance
- Security

NOTE:

For the most up-to-date information on ESP Data Center solutions, please visit the following: Validated Solution Guide Program

Introduction

The Aruba ESP (Edge Services Platform) data center is built on technology that provides tools for transforming the data center into a modern, agile, services delivery platform that satisfies the requirements of organizations large, small, distributed, and centralized. The ArubaOS-CX (AOS-CX) operating system simplifies operations and maintenance with a common switch OS across campus, branch, and data center, managed from the cloud or on-premises and backed by Artificial Intelligence (AI) that provides best-practices guidance throughout the network lifecycle.

Converged Ethernet is changing the way compute hosts access modern data center storage. Dedicated storage area networks (SANs) are no longer required. Lossless Ethernet and bandwidth management protocols ensure timely reads and writes over a traditional IP LAN. The cost savings and operational simplicity of converged Ethernet are major drivers for transformation.

At the same time, network topologies have become virtualized. While this virtualization promotes the flexibility required to meet transformational data center requirements, it can add complexity to implementation and management. The Aruba ESP data center mitigates these challenges with automation in the management plane and the capabilities of AOS-CX, such as automated configuration backups and built-in alerts.

Securing applications and hosts in a data center is critical to maintaining application availability, data integrity, and business continuity. New threats continue to emerge around ransomware, data exfiltration, and denial of service. Policy and security enforcement involves many tools and is applied at many different layers. The new Aruba CX 10000 series switch with Pensando introduces an industry-first distributed services data center switch, capable of performing in-line firewall services at wire-speed in the switch itself, focusing on the high level of east-west traffic typical in a data center environment.

When designing a new or transformed data center, the first step is to understand the organization's cloud applications strategy. This will determine which applications will remain on-premises and the right size for the data center. When establishing a new data center intended to grow and adapt, plan to implement a spine-and-leaf underlay supporting software-defined overlay networks. The Aruba CX 10000, 83xx, and 84xx switching platforms provide a best-in-class suite of products featuring a variety of high-throughput port configurations and industry-leading OS modularity providing real-time analytics and always-up performance.

Purpose of This Guide

This guide covers the Aruba ESP data center network design, including reference architectures and their associated hardware and software. It explains the requirements that shaped the design and the benefits it provides. This guide introduces Aruba data center solutions that support options for both distributed and centralized workloads and provides best-practices recommendations for designing a next-generation spine-and-leaf data center fabric using VXLAN and BGP EVPN.

This guide assumes the reader has equivalent knowledge to an Aruba Certified Switching Associate.

Design Goals

The overall goal is to create a high-reliability, scalable design that is easy to maintain and adapt to the changing needs of business. The solution components are limited to a specific set of products required for optimal operations and maintenance. The key features addressed by the Aruba ESP data center network include:

- Zero downtime upgrades
- High throughput
- Security
- Converged storage networking
- Flexible segmentation
- Third-party integration

This guide can be used to design new networks or to optimize and upgrade existing networks. It is not intended as an exhaustive discussion of all options but rather to present commonly recommended designs, features, and hardware.

Audience

This guide is written for IT professionals who need to design an Aruba ESP data center network. These IT professionals can fill a variety of roles:

- Systems engineers who need a standard set of procedures for implementing solutions
- Project managers who create statements of work for Aruba implementations
- Aruba partners who sell technology or create implementation documentation

Customer Use Cases

Data center networks are changing rapidly. The most pressing challenge is maintaining operational stability and visibility while securely placing compute and storage resources where they best serve users. In addition, data center teams are being asked to support the rapid pace of DevOps environments, including connecting directly with public cloud infrastructure. Given the rapidly changing landscape for data center requirements, it's critical that network and system engineers get the tools they need to simplify and automate complex infrastructure configurations.

This guide discusses the following use cases:

- Pay-as-you-grow designs that support network and compute workload elasticity
- Ease of use and agility to quickly deploy and manage workloads using compute, hypervisor, and network orchestration
- Improved operations with data center visibility from compute host to network infrastructure
- Workload mobility, security, and multi-tenancy using standards-based overlay technologies
- Network infrastructure automation and management
- Data aggregation and pre-processing

Aruba ESP Data Center Network Design

The Aruba Edge Services Platform (ESP) Data Center provides flexible and highly reliable designs that ensure efficient access to applications and data for all authorized users while simplifying operations and accelerating service delivery.

Aruba ESP data center includes the following key features and capabilities:

- Modern connectivity—Design efficient and scalable networks using the full range of port densities and speed options available in the Aruba CX 8xxx and CX 10000 switch families.
- Automation—Automated fabric configuration makes building high-performance, scalable data center networks more efficient and less error prone.
- Analytics—On-box and cloud analytics ensure alerts are never missed and that intermittent failures are diagnosed quickly.
- Storage networking—Advanced protocols enable lossless Ethernet with bandwidth reservation and congestion management.
- Host integration—Virtual network visualization is part of the physical network topology for end-to-end management.

The Aruba ESP data center network design may contain one or more of the following elements:

- Aruba Central
- Aruba Fabric Composer
- Aruba NetEdit
- Pensando Policy and Services Manager
- Aruba CX 10000 Ethernet switches with Pensando
- Aruba CX 8xxx Ethernet switches
- Aruba CX 6xxx Ethernet switches for out-of-band (OOB) network management
- Aruba integration into HPE solutions

Aruba ESP Data Center Network Design Options

The Aruba ESP data center supports centralized and distributed workloads anywhere within an organization. Each design supports host uplink bundling, providing throughput and resiliency for mission-critical workloads. Layer 2 domains can be flexibly deployed to suit application requirements and virtual host mobility.

Aruba CX switches provide a robust platform for Layer 3 services in the data center. When deployed in a spine-and-leaf topology, a Layer 3 data center network eliminates the need for loop-avoidance protocols and is optimized for high capacity and non-oversubscribed low-latency performance.

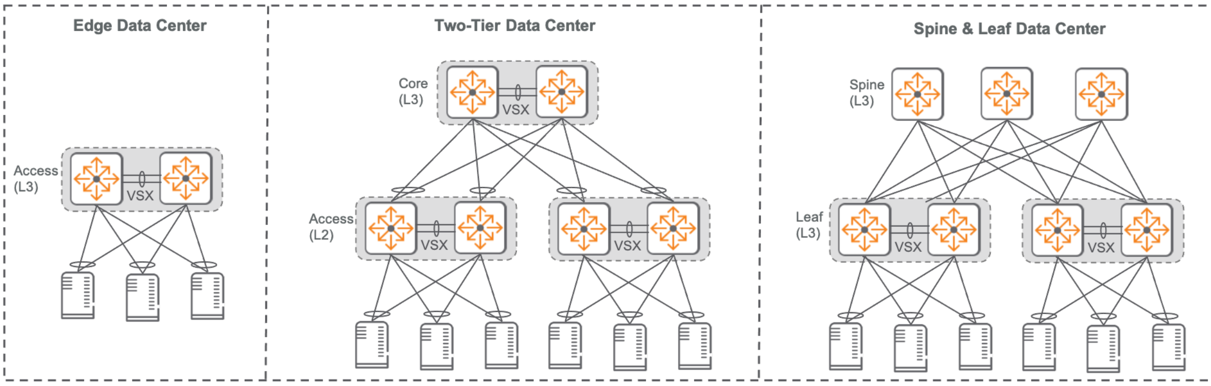

Figure 1: Aruba Data Center Designs

Edge Data Center Overview

Enterprises that have migrated most of their workloads to the cloud—and do not need an on-premises data center—can use their existing campus network wiring closets or small server rooms to deploy workloads at the edge. This design uses the same AOS-CX switches to provide server access that already provide wired connectivity to users and Internet of Things (IoT) devices. The edge data center also supports high-bandwidth and low-latency access to compute and storage resources for distributed workloads that may not be well suited to cloud deployments.

Two-Tier Data Center Overview

Enterprises with significant, existing, on-premises workloads spanning multiple workgroups will often require a traditional, two-tier data center design. The two-tier approach ensures sufficient bandwidth and reliability using legacy protocols such as Link Aggregation Control Protocol (LACP), Spanning Tree Protocol (STP), and Open Shortest Path First (OSPF). Hosts are dual-homed to top-of-rack (ToR) switches using Virtual Switch Extension (VSX) link aggregation group (LAG). Each ToR switch is dual-homed to the core. Loops are primarily prevented by the use of LACP to aggregate redundant links.

Spine-and-Leaf Data Center Overview

Enterprises with growing on-premises workloads and those with workloads spread across data centers should leverage the efficiencies of a Clos-based spine-and-leaf architecture. In most cases, a migration to the spine-and-leaf design should be paired with the implementation of a Virtual Extensible LAN (VXLAN) overlay topology. The spine-and-leaf design ensures high reliability through the use of redundant Layer 3 links between leaf nodes and spine switches. Equal-cost multipath (ECMP) routing ensures load balancing and fast failover if a link or switch goes down.

The fully meshed architecture enables simple, horizontal growth by adding another spine switch as needed. VXLAN provides a Layer 2 over Layer 3 tunneling solution, which enables customers to modernize the underlay while preserving legacy service requirements by allowing for physically dispersed Layer 2 segments in the overlay. VXLAN also enables highly segmented designs, which can go beyond traditional VLANs when creating secure, discrete groups of resources within the data center.

This guide addresses the most common use cases of an Aruba spine-and-leaf data center network. For more complex projects not covered in this guide, contact an Aruba or partner SE for design verification.

Aruba ESP Data Center Architecture for Spine and Leaf

Aruba ESP is an evolution of Aruba's end-to-end architecture, providing a Unified Infrastructure with centralized management leveraging Artificial Intelligence Operations (AIOps) for an improved operational experience that helps enable a Zero Trust Security policy. Aruba ESP is the industry's first platform that is purpose-built for the new requirements of the Intelligent Edge.

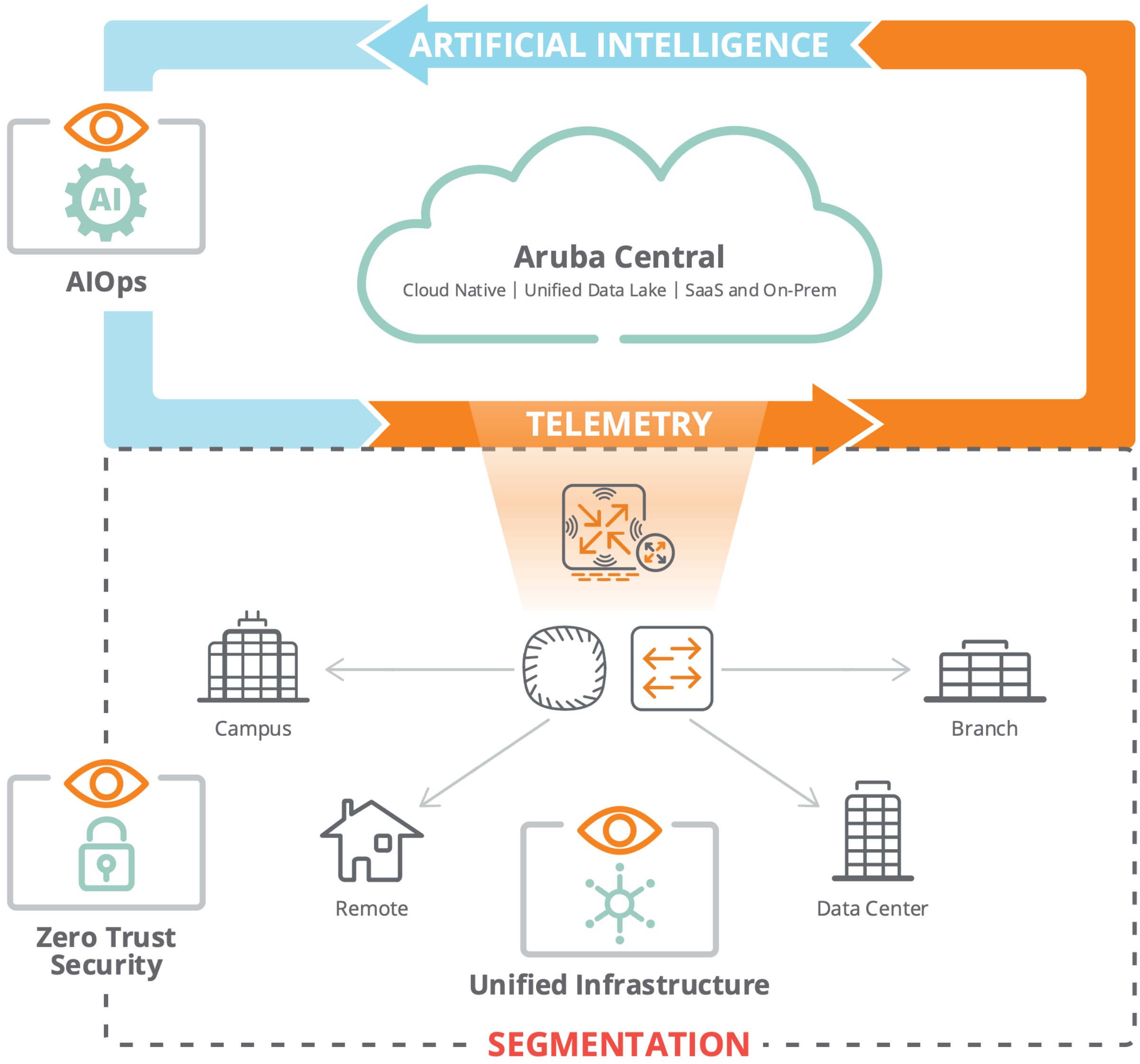

Figure 2: ESP Architecture

Aruba ESP Architecture Layers

Aruba ESP offers a breadth of services, including onboarding, provisioning, orchestration, security, analytics, location tracking, and management. AI Insights reveal issues before they impact users. Intuitive workflow-centric navigation allows the organization to accomplish tasks quickly and easily using views that present multiple dimensions of correlated data. Policies are created centrally, and features like Dynamic Segmentation allow the network administrator to implement them over an existing infrastructure. This is because the Aruba ESP architecture is built in distinct layers, as shown in the following figure.

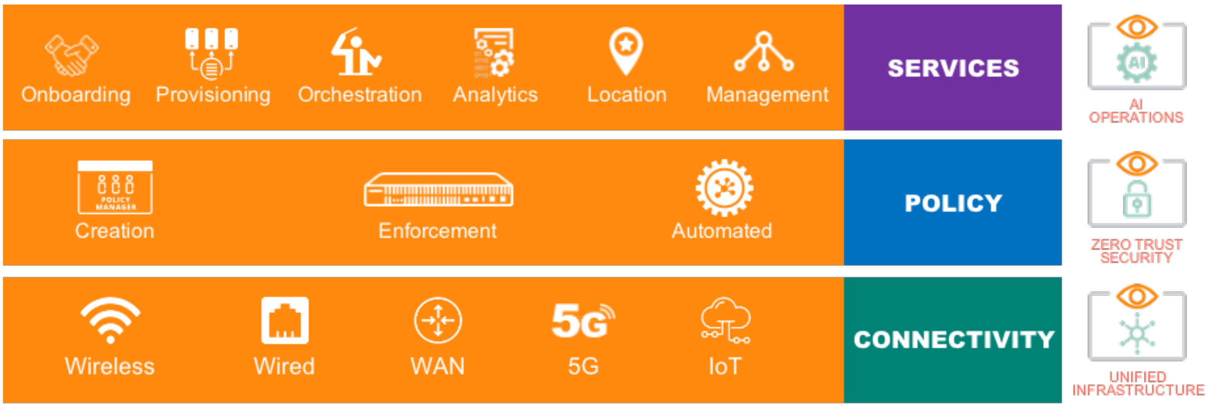

Figure 3: ESP Layers

Aruba ESP Data Center Connectivity Layer

The connectivity layer for the Aruba ESP data center is implemented on Aruba CX 8xxx and 10000 series Ethernet switches, which provide low latency and high bandwidth on a fault-tolerant platform designed to carry data center traffic.

Underlay Network

The underlay network is implemented using a spine-and-leaf fabric topology. It is deployed as a Layer 3 routed network. Each leaf is connected to each spine over a routed port, and OSPF is the routing protocol. Layer 2 services are not required in the underlay but can be provided for workloads using virtual overlay networks. The spine-and-leaf underlay topology optimizes performance, increases availability, and reduces latency because each leaf is never more than one hop across multiple load-balanced paths to all other leaf switches.

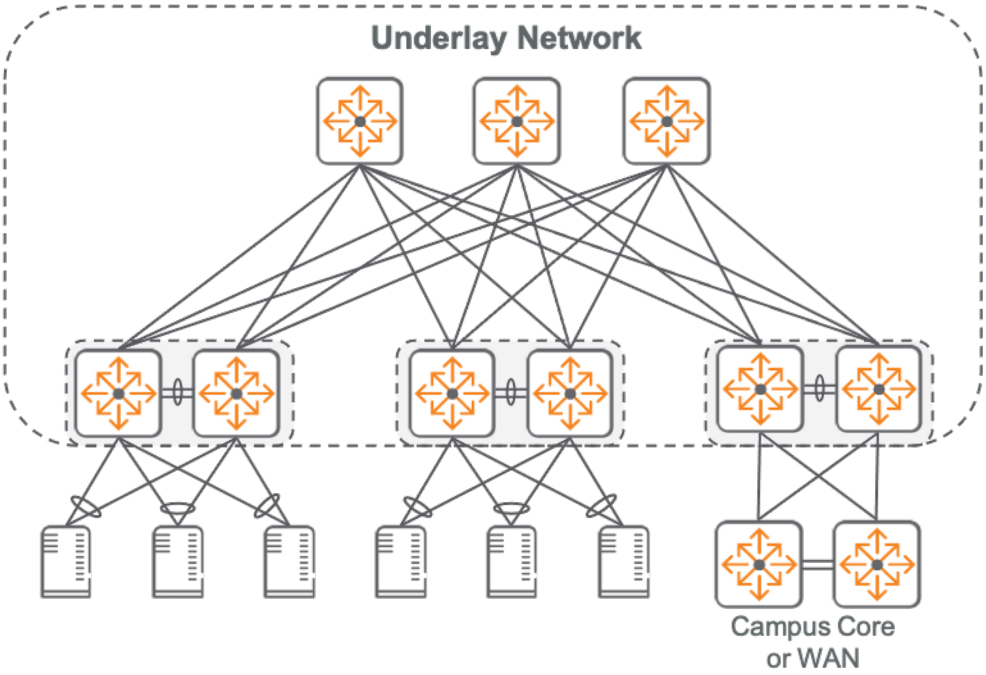

Figure 4: Underlay Network

The spine-and-leaf topology provides a flexible, scalable network design that can expand to accommodate a growing data center without disrupting the existing network. It is easy to begin with a small one- or two-rack fabric that can increase capacity without having to replace existing hardware. ToR ports on leaf switches are used to incrementally add compute capacity to a rack. Ports on spine switches are used to add additional racks to the fabric.

The maximum size of the fabric is determined by the port density on the spine, and this is an important consideration for supporting future growth. A minimum of two spine switches is recommended for any size fabric to provide high availability and fault tolerance. Additional spine switches increase overall fabric capacity and reduce the fault domain in case a spine must be taken out of service.

Aruba ESP Data Center Policy Layer

The policy layer for the Aruba ESP data center is implemented by the use of overlay technologies and traffic filtering mechanisms for isolating user and application traffic.

Overlay Network

An overlay network is implemented using VXLAN tunnels that provide both Layer 2 and Layer 3 virtualized network services to workloads directly attached to the leaf switches. Similar to a traditional VLAN ID, a VXLAN Network Identifier (VNI) identifies an isolated Layer 2 segment in a VXLAN overlay topology. Symmetric Integrated Routing and Bridging (IRB) allows the overlay networks to support contiguous Layer 2 forwarding and Layer 3 routing across leaf nodes.

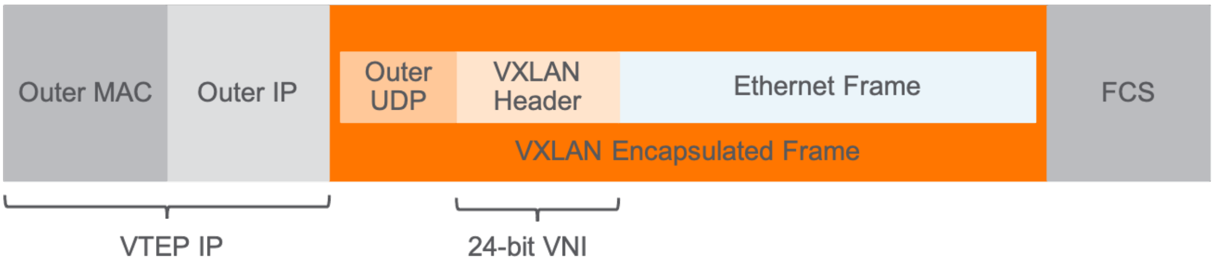

Figure 5: VXLAN Frame

A VXLAN Tunnel End Point (VTEP) is the function within leaf switches that handles the origination and termination of point-to-point tunnels forming an overlay network. A single logical VTEP is implemented when redundant leaf switches are deployed in a rack. Spine switches provide IP transport for the overlay tunnels but do not participate in the encapsulation/decapsulation of VXLAN traffic.

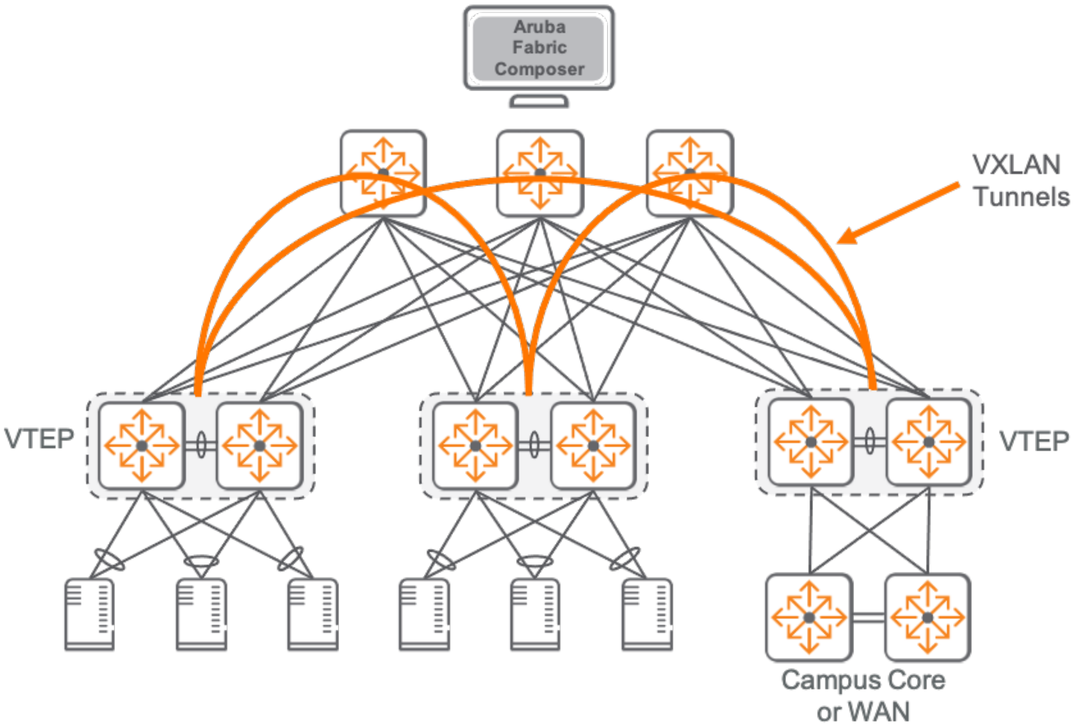

Figure 6: Overlay Network

Attached hosts are learned at the leaf switch using Ethernet link layer protocols. Remote learning across the VXLAN fabric is accomplished using Multiprotocol Border Gateway Protocol (MP-BGP) as the control plane protocol and a dedicated Ethernet virtual private network (EVPN) address family for advertising host IP and MAC prefixes. This approach minimizes flooding while enabling efficient, dynamic discovery of remote hosts within the fabric.

Security and Segmentation

In a VXLAN spine-and-leaf design, a pair of leaf switches is the single entry and exit point to the data center. This *border leaf* is not required to be dedicated to that function. Compute hosts and firewalls may also be attached. Typically, the border leaf is where a set of policies are implemented to control access into the data center network. These policies are the first layer of security for data center applications. They limit access to only permitted networks and hosts while also monitoring those connections. The data center perimeter is usually protected in one or both of the following ways:

- Border leaf ACLs—When IP subnets inside the data center are designed in a way that map to security groups or business functions, Access Control Lists (ACL) at the border leaf can provide policy enforcement from user locations into data center applications. If subnets cannot be mapped to security groups, the ACLs can become difficult to manage and scale in larger environments. The primary benefit of perimeter ACLs is that they can be implemented directly on the switching infrastructure to enforce a policy foundation from which to establish data center access. Policies implemented using switch ACLs specifically target Layer 3 and Layer 4 constructs. Switch ACLs are not stateful or application-aware.
- Perimeter firewalls—Dedicated security systems at the perimeter can offer advanced monitoring, application-aware policy enforcement, and threat detection. Perimeter firewalls are typically deployed in transparent or routed mode. In transparent mode, the firewalls behave like a bump in the wire, meaning all allowed user and network control traffic pass transparently through them. In routed mode, a firewall will participate in the routing control plane and can be deployed in a configuration that limits the amount of traffic subject to deep inspection. It is important to note that stateful firewalls require symmetric forwarding to correctly apply policy to the subsequent flow.

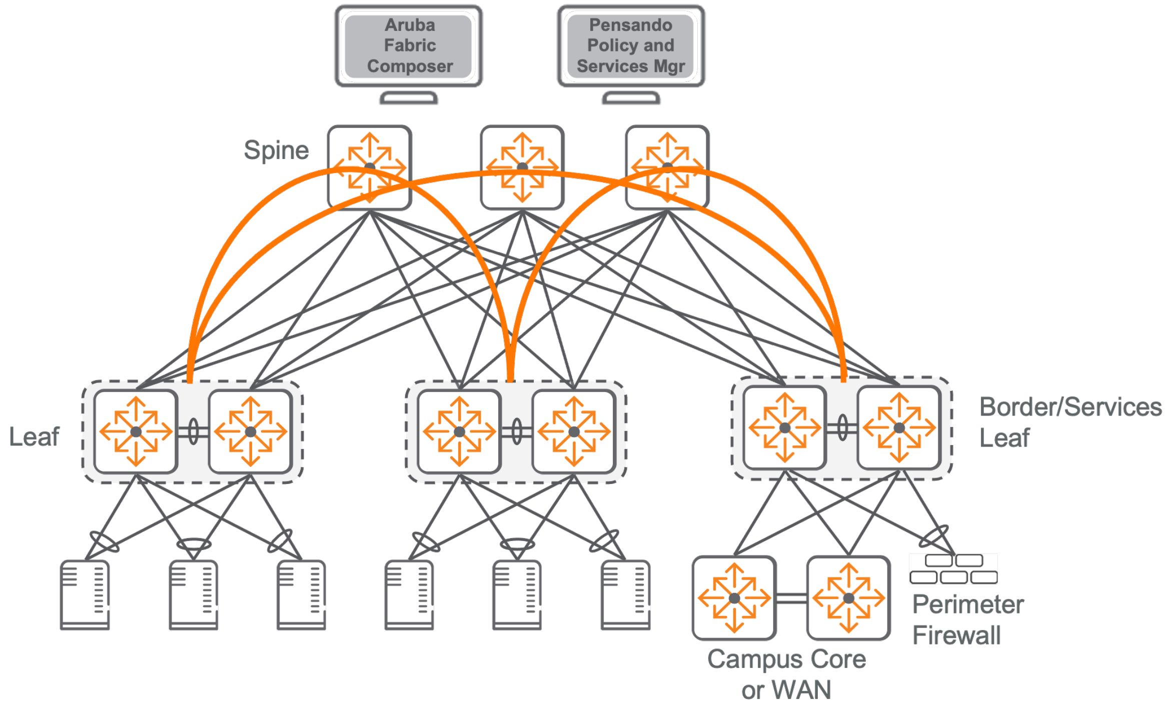

Figure 7: Data Center Policy

Policy inside a VXLAN spine and leaf data center can be implemented using two methods at the network layer: inline using distributed services switches (DSSs) or centrally using a firewall appliance in a services leaf.

- Distributed Services Switch Policy Enforcement — The Pensando programmable data processing unit (DPU) extends Aruba CX 10000 series switches to include stateful firewall capabilities. Leveraging this built-in hardware feature, firewall enforcement is provided inline as part of the switch fabric. There are several advantages to this approach. Firewall policy can be granular to the host with support for microsegmentation. Data center hosts can use local gateways, so east-west traffic flows are optimized between data center hosts. There is no requirement to hairpin data through a services leaf firewall. The Pensando DPU provides wire-rate performance and can alleviate resource consumption on virtualized firewall services processing large data flows by moving firewall services to dedicated switch hardware.
- Services Leaf Policy Enforcement — Another commonly deployed policy enforcement approach is placing a firewall appliance in a services leaf. Firewalls connected at the services leaf are used as the default gateway for hosts requiring specific services accessible through the firewall. An advantage of this approach is the ease with which a Layer-2 overlay network can be used to transport host traffic to the firewall. The disadvantage is that it relies on a centralized gateway and prevents the use of an active gateway at every ToR for optimal forwarding. Similar to a border leaf, the services leaf does not need to be dedicated to this function.

Some vendors offer virtualized firewall services within a hypervisor environment. This approach can provide granular, service-level policy enforcement while also allowing for the use of active gateways. VMware NSX is an example of a product that can integrate in this way. VXLAN overlays may be implemented in both hardware and software to achieve optimal network virtualization and distributed firewall services while securing east–west traffic inside the data center.

Aruba ESP Data Center Services Layer

The Aruba ESP data center solutions include management plane choices enabling an organization to apply the approach that suits their needs best.

- Aruba Central provides a cloud management solution for the end-to-end Aruba ESP solution.
- Aruba Fabric Composer (AFC) is a fabric automation tool that provides a simplified, workflow-based method of fabric configuration also offered as an on-premises solution.
- Aruba NetEdit provides the same multidevice configuration editor and topology mapper now found in Aruba Central in an on-premises offering.

Aruba Central

Aruba Central is designed to simplify the deployment, management, and optimization of network infrastructure. The use of integrated Artificial Intelligence (AI)-based Machine Learning (ML), and Unified Infrastructure management provides an all-encompassing platform for digital transformation in the enterprise.

Aruba Central provides advanced services to facilitate transformational data center rollouts. With NetEdit MultiEditor capability now integrated into Central, it's possible to deploy complex, multidevice, multilayer configurations from the cloud to your data center. The Network Analytics Engine provides real-time alerts on the state of your switches and allows for rapid analysis of intermittent problems. Aruba Central is cloud-hosted for elasticity and resilience, which also means that users never have to be concerned with system maintenance or application updates.

Workflow-based configurations within Central allow for efficient, error-free deployments of Aruba solutions anywhere in the world. The workflows are based on common best-practice approaches to network configuration. They enable new devices to come online quickly using new or existing network configurations.

AIOps

According to Gartner Glossary, "AIOps combines big data and machine learning to automate IT operations processes, including event correlation, anomaly detection and causality determination."

Aruba AIOps, driven by Aruba Central, eliminates manual troubleshooting tasks, reduces average resolution time, and automatically discovers network optimizations. Aruba's next-generation AI uniquely combines network- and user-centric analytics to identify and inform staff of anomalies. It also applies decades of networking expertise to analyze and provide prescriptive actions.

AI Insights are available to monitor connectivity performance, radio frequency (RF) management, client roaming, airtime utilization, and wired and SD-WAN performance. Each insight is designed to reduce trouble tickets and ensure service-level agreements (SLAs) by addressing network connectivity, performance, and availability challenges.

AI Assist uses event-driven automation to trigger the collection of troubleshooting information, to identify issues before they impact the business, and virtually eliminate the time-consuming process of log file collection and analysis. Once log information is automatically collected, IT staff are alerted with relevant logs that can be viewed and even shared with Aruba TAC, who can more quickly assist with root cause determination and remediation.

Aruba Fabric Composer

AFC provides API-driven automation and orchestration capabilities for the Aruba ESP data center. AFC discovers and interrogates data center infrastructure to automate and accelerate spine-and-leaf fabric provisioning as well as day-to-day operations across rack-scale compute and storage infrastructure. AFC orchestrates a set of switches as a single entity called a *fabric* and allows the operator to orchestrate data center resources using an application-centric approach to visualizing network and host infrastructure.

Visualization of the data center network fabric includes physical and virtual network topologies as well as host infrastructure through integration with ArubaOS-CX, HPE iLO Amplifier, HPE SimpliVity, VMware vSphere, and other leading data center products. In addition to providing a complete view across the fabric, AFC makes network provisioning accessible to more than just network staff. It provides a platform for orchestrated deployment of host and networking resources across the fabric through a guided workflow user interface. AFC ensures a consistent and accurate configuration of a spine-and-leaf data center whether or not an overlay network is also deployed.

AFC is an end-to-end data center network management tool recommended for new data center deployments based on a spine-and-leaf fabric topology. It is particularly helpful when also deploying an overlay topology using VXLAN-EVPN. AFC will configure both the underlay and overlay routing automatically using basic IP information provided by the operator.

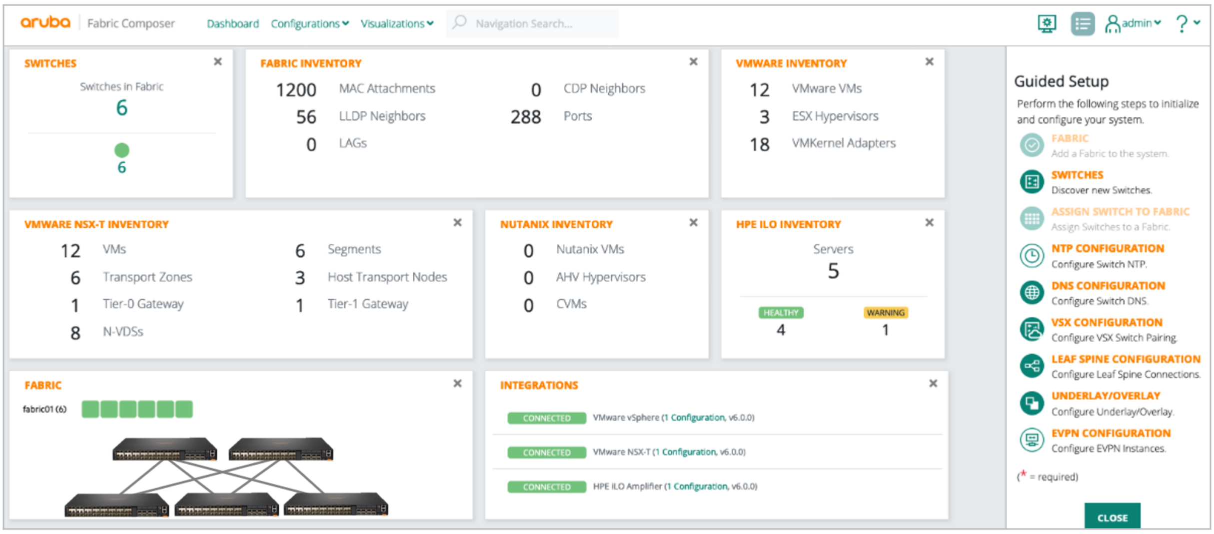

Figure 8: Aruba Fabric Composer

Pensando Policy and Services Manager

The Pensando Policy and Services Manager (PSM) provides an API based management platform for programming and monitoring Pensando DPUs integrated into Aruba CX 10000 switches. AFC provides single-pane-of-glass configuration and orchestration for both switch fabric and PSM-managed services.

Aruba NetEdit

Aruba NetEdit enables IT teams to automate the configuration of multiple switches to ensure deployments are consistent, conformant, and error-free. It enables automation workflows without the overhead of programming by providing operators with a user-friendly interface similar to command line. NetEdit also provides a dynamic network topology view to ensure an up-to-date view of the network.

When deploying an Aruba ESP data center network using on-premises tools, NetEdit should be deployed for detailed configuration management. While Aruba Fabric Composer enables fast, error-free spine-and-leaf implementations, NetEdit provides the ability to tailor that configuration when necessary. Together, Fabric Composer and NetEdit deliver an automated, integrated, and validated network configuration ready to support the needs of any data center network.

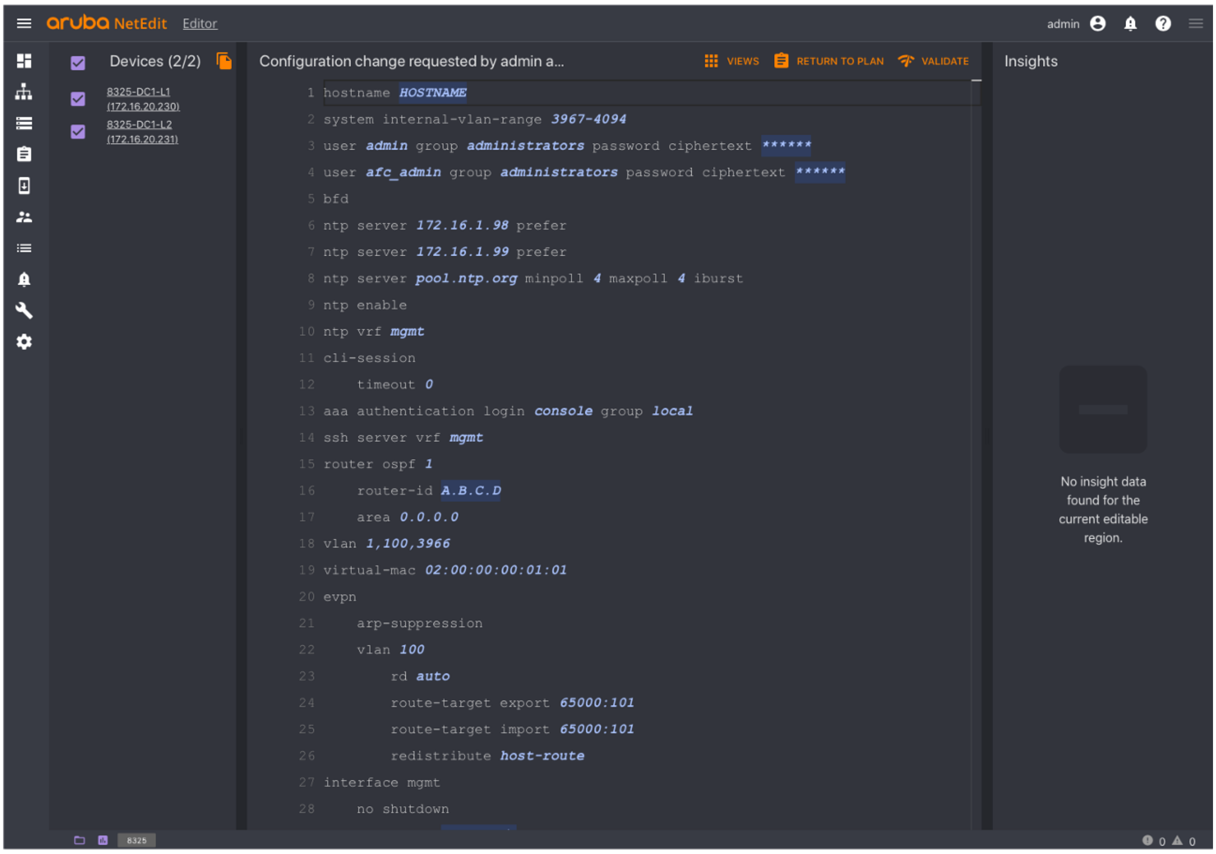

Figure 9: NetEdit

Aruba Network Analytics Engine

Aruba Network Analytics Engine (NAE) provides a built-in framework for monitoring and troubleshooting networks. It automatically interrogates and analyzes network events to provide unprecedented visibility into outages and anomalies. Using these insights, IT can detect problems in real time and analyze trends to predict or even avoid future security and performance issues

A built-in time-series database delivers event and correlation history along with real-time access to network-wide insights to help operators deliver better experiences. Rules-based real-time monitoring and intelligent notifications automatically correlate to configuration changes. Integrations with Aruba NetEdit and third-party tools such as ServiceNow and Slack provide the ability to generate alerts to trigger actions within an IT service management process.

NAE runs within the AOS-CX operating system in the Aruba CX 6xxx, CX 8xxx, and CX 10000 switch series. NAE agents test for conditions on the switch, its neighboring devices, or on traffic passing through the network, and then take actions based on the result of the test.

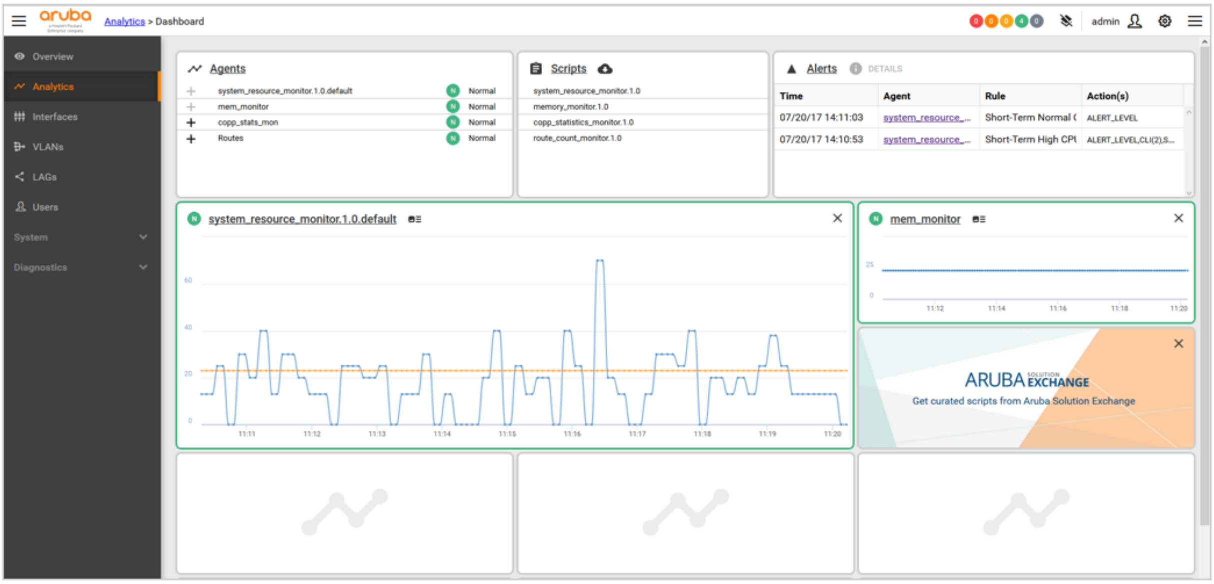

Figure 10: Network Analytics Engine

Choosing an Approach

In general, small, edge-connected data centers are best managed using Aruba Central to ensure consistent configuration anywhere in the world. Larger, centrally located data centers will likely require the use of Aruba NetEdit so that detailed, custom configurations can be written and deployed automatically to multiple network devices.

Plans to build a spine-and-leaf data center topology should include AFC. When planning to deploy a VXLAN overlay, AFC is highly recommended to simplify the configuration of underlay and overlay services as well as Layer 3 segments. And when deploying PSM with Aruba CX 10000 switches, AFC is recommended to manage firewall rule and policy creation.

Additional Data Center Services

Planning a data center network involves more than just network infrastructure. It's also necessary to ensure that services are available to bring switches and hosts online and to ensure devices can send log messages to a syslog server accessible to people and applications.

It may be useful to leverage the Zero Touch Provisioning (ZTP) capabilities of Aruba switches. To do so, the network must provide a Dynamic Host Configuration Protocol (DHCP) server on a management LAN with a route to the Internet. In addition to the default gateway address, devices will also require at least one domain name service (DNS) server to resolve hostnames required for connectivity to Aruba Central and the Aruba Activate service.

Network Time Protocol (NTP) ensures that log data from across the network and in the cloud is time stamped correctly for later analysis. NTP is also required for public key infrastructure (PKI) to function correctly. PKI is required for a variety of access security approaches today. A log management or security information and event management (SIEM) solution is a part of most data centers today. Knowing which will be implemented will help with establishing a configuration baseline for all switches in the network.

Aruba ESP Data Center Design for Spine and Leaf

To successfully design a spine-and-leaf data center, it is important to consider all layers of the data center network. This section provides general design considerations across the different layers of the Aruba ESP data center. The reference architecture section will include hardware-specific recommendations that you can use to finalize your design.

Connectivity Layer Design

This section provides design recommendations and best practices for physical connectivity of compute and network infrastructure.

Compute Host Connectivity

The first step to design a data center is to identify which types of connectivity are required by the compute hosts. Server hardware will typically have an Ethernet RJ45 port for a lights-out management device such as HPE iLO. Application connectivity is commonly over redundant links using RJ45 or small form factor pluggable (SFP) ports.

The lights-out port is typically connected using a Cat5e or Cat6 copper patch cable into a switch on the management LAN. Typically, the host-to-leaf connections will be 10 Gb or 25 Gb using SFP+/SFP28 fiber modules, copper direct-attach cables (DAC), or active optical cables (AOC). DACs have limited distance support and can be harder to manage due to the thicker wire gauge when compared against optical cables. AOCs support longer distances than DACs, are thinner, and are easier to manage. Both DACs and AOCs cost less than separate fiber patch cables and optical transceivers but only operate at a single speed.

It is important to verify that both the host network interface controller (NIC) and the ToR switch are compatible with the same DAC or AOC. When separate transceivers and optical cables are used, it is also important to verify transceiver compatibility with the host NIC, ToR switch, and optical cable type. The supported transceiver on the host will usually be different than the supported transceiver on the switch. Always consult with a structured cabling professional when planning a new or upgraded data center.

When deploying a converged network for IP storage traffic, look for NIC cards supporting offload of storage protocols. Similarly, ensure the hardware also supports VXLAN offloading. These features will help to minimize latency of storage traffic by reducing the load on a host CPU.

Applications can be hosted directly on a server using a single operating system. This is commonly referred to as a bare-metal server. Multiple hosts can be virtualized on a single physical server using a hypervisor software layer. Examples of this would be VMware ESXi or Microsoft Hyper-V.

Hypervisors generally contain some form of virtual switch that provides connectivity to each virtual machine (VM) using Layer 2 VLANs or VXLAN tunnels for segmentation. A successful spine-and-leaf design should support Layer 2 and Layer 3 connectivity using untagged and VLAN-tagged ports to match the connectivity required to the server and/or virtual switch inside the server. AFC provides visibility and orchestration of the configuration required to ensure that the connectivity between the server and Aruba ToR switches is properly established.

Out-of-Band Management

The Aruba ESP data center spine-and-leaf design uses a dedicated management LAN connecting to switch management ports and host lights-out management (LOM) ports. Typically, a single management switch is deployed at every rack for OOB management. A dedicated management switch ensures reliable connectivity to data center infrastructure for automation, orchestration, and traditional management access.

Top-of-Rack Design

Deploying switches in the ToR position enables shorter cable runs between hosts and switches. The result is a more modular solution with host-to-switch cabling contained inside a rack enclosure and only switch uplinks exiting the enclosure. This approach helps reduce complexity when adding racks to the data center.

In the Aruba ESP data center, each rack is serviced by a redundant pair of VSX configured switches. This allows dual-homed hosts to be connected to two physical switches using a link aggregation bundle for fault tolerance and increased bandwidth.

VSX enables a distributed and redundant architecture that is highly available during upgrades. It virtualizes the control plane of two switches to function as one device at Layer 2 and as independent devices at Layer 3. From a data-path perspective, each device does an independent forwarding lookup to decide how to handle traffic. Some of the forwarding databases, such as the MAC and ARP tables, are synchronized between the two devices via the VSX control plane over a dedicated inter-switch link (ISL) trunk. Each switch builds the Layer 3 forwarding databases independently.

When deploying a pair of switches in VSX mode, ensure at least three ports connect the switches to each other. A minimum of two ports are members of a link-aggregation data path between the switch pair and should be the same speed as the uplinks ports. A third can be any available lower speed port to preserve uplinks for future spine and VSX link-aggregation connectivity.

For backward compatibility and to support future growth, choose a ToR switch that supports connectivity rates of 1, 10, or 25 Gb/s. These connection speeds can be implemented using the same fiber-optic media types that makes it easy to increase bandwidth by simply upgrading transceivers or DACs/AOCs. Keep the following in mind when selecting a ToR switch:

- DSS feature requirements: The Aruba CX 10000 is required in a data center design that leverages the inline stateful firewall inspection performed by the Pensando Elba ASIC.
- Number of and type of server connections: Typical rack server configurations support 48 host-facing ports, but lower-density ToR options are available in the Aruba CX 8360 series.

- Host connectivity speed: To simplify management, consolidate hosts connecting at the same speeds to the same racks and switches. Adapting the port speed settings of a particular interface between 25 and 10 Gb may impact a group of adjacent interfaces. Consider interface group size when planning for a rack requiring multiple connection speeds.
- Number of uplink ports: ToR switch models support a range of uplink port densities. When using VSX for redundancy, two uplink ports are used for ISLs providing data-path redundancy and cannot be used for spine connectivity.
- ToR-to-spine connectivity: The amount and port speed of the uplinks will define the oversubscription rate from the hosts to the data center fabric. As an example, in a four-spine deployment at 100 Gb, a non-oversubscribed fabric can be implemented for racks of 40 servers connected at 10 Gb.
- Cooling design: Different ToR models are available for port-to-power and power-to-port cooling. In power-to-port configurations, an optional air-duct kit can isolate hot air from servers inside the rack. Cabling can absorb heat and restrict airflow. Short cable routes and good cable management will improve the airflow efficiency.

Spine Design

The spine layer provides aggregation for leaf switches. In a spine-and-leaf design, each ToR switch is connected to each spine switch. Each leaf-to-spine connection should use the same link speed to ensure multiple equal-cost paths within the fabric. This allows ECMP based routing to ensure connectivity if a link goes down.

The port capacity of the spine switches will define the maximum number of racks the data center can connect. In the case of a redundant ToR design, the maximum number of racks will be half the port count on the spine switch. Two spines is the recommended minimum for high availability. Additional spines increase overall fabric capacity and reduce the size of the fault domain in case a spine is out of service.

- Determine rack media and bandwidth requirements.
- Determine whether single or redundant ToR switches will be installed.
- Determine how many racks are needed for current compute and storage requirements.
- Determine the spine switches required to support the planned racks.
- Design the data center network for no more than 50% capacity to leave room for growth.

If the network will have more than two spine switches, pay attention to the number of uplink ports available on the chosen ToR switch. Each ToR switch must connect to each spine for ECMP to work effectively.

In deciding where to place your spine switches, also consider their distance from the leaf switches and what media type you will use to connect them. Leaf-to-spine connections will be either 40 Gb or 100 Gb fiber using quad SFP (QSFP) transceivers or AOCs, in which, similar to DACs, the cable and transceiver are integrated.

Underlay IP Design

The underlay of a spine-and-leaf data center network is the layer which provides IP connectivity between spine-and-leaf switches. The underlay is the part of the network that ensures VXLAN tunneled traffic (the overlay network) can be forwarded across the fabric.

The Aruba ESP data center uses OSPF as the underlay routing protocol. OSPF is a widely used and well understood Interior Gateway Protocol (IGP) that provides straightforward configuration and fast convergence. A single OSPF area and point-to-point interfaces are recommended to minimize the complexity and time required for establishing neighbor adjacencies.

Configure the data center switches for a jumbo maximum transmission unit (MTU) of 9198 bytes. This accommodates the storage protocols likely to be deployed and the expanded frame header used by VXLAN.

Policy Layer Design

This section provides design recommendations and best practices for the policy layer design of the data center network.

Management Network

Organizations should plan to build a physically separate management LAN and role-based access control on the network devices. This means that login to a switch requires authentication against an enterprise directory. That would typically be accomplished using the TACACS+ protocol and a policy server such as Aruba ClearPass Policy Manager. Logging facilities, log management, and log analysis should also be considered.

Establishing a separate management network ensures data center switch reachability is not unintentionally blocked when modifying data plane policy.

Purpose of Policy and Segmentation

Security policy plays a key role in reducing the attack surface exposed by data center hosts, constraining the options for lateral threat movement once a host has been compromised, and preventing data exfiltration. Blocking unnecessary protocols constrains the available tactics a threat actor can use in host exploitation, which can be applied to both north-south and east-west data center traffic. Scoping allowed outbound traffic inhibits command and control structures and blocks common methods of data exfiltration.

Overlay Control Plane Design

Host mobility refers to the ability to move physical or virtual hosts within a data center network without changing the host network configuration. This flexibility is powerful when paired with virtualized hosts and can ensure optimized compute resources, high availability of applications, and efficient connectivity for distributed workloads.

To maintain a data center overlay and successfully forward traffic through it, VTEPs within the fabric require reachability information about fabric connected endpoints. A distributed, dynamic control plane is recommended for the following reasons:

- Traditional flood and learn techniques can consume large amounts of bandwidth due to the replication of traffic in a large spine-and-leaf environment.
- Network configuration is simplified as the ToR switches will automatically learn about other ToR switches inside the fabric.
- A distributed control plane provides redundancy and a consistent topology state across the data center fabric switches.
- A distributed control plane allows optimal forwarding via the use of distributed gateways at the ToR switches. This makes it possible for the default gateway address to remain the same across the fabric.

The use of MP-BGP with EVPN address families between VTEPs provides a standards-based, highly scalable control plane for sharing endpoint reachability information with native support for multi-tenancy. MP-BGP has been used for many years by service providers to offer secure Layer 2 and Layer 3 VPN services at very large scale. Network operations are simplified by using an iBGP design with route reflectors so that peering is only required between leaf switches and the spine. Some of the BGP control plane constructs that you should be familiar include the following:

- Virtual Routing & Forwarding (VRF)—A VRF is a layer 3 virtualized routing instance, which consists of a unique route table, member interfaces that forward traffic based on the route table, and routing protocols that build the route table. A VRF may contain overlapping IP addresses with another VRF, because the individual route tables are discrete.

- Route distinguisher (RD)—In order to support multi-tenancy and the likelihood of overlapping IP addressing, an RD value is pre-pended to IPv4 or IPv6 prefixes when exported into BGP from a VRF. The combined RD + IPv4/IPv6 prefix value creates a new unique prefix that allows a single BGP address family to carry otherwise overlapping IPv4/IPv6 prefixes. The RD should be unique for each VRF, which is mapped to a VXLAN Layer 3 VNID.
- Route target (RT)—Route targets are used as an attribute to identify the VRF network associated with a prefix when exported, and as a criteria for importing prefixes into a VRF route table. Route targets in the IPv4 address family are used to perform route leaking between VRFs by importing prefixes with route targets that were exported by other VRFs.
- Route reflector (RR)—To optimize the process of sharing reachability information between VTEPs, the use of route reflectors at the spine allows for simplified iBGP peering. This design allows for all VTEPs to have the same iBGP peering configuration and eliminates the need for full mesh of iBGP neighbors.
- Address family (AF)—Different types of routing tables (such as IPv4 unicast, IPv6 unicast, and Layer 3 VPN) are supported in MP-BGP. The Layer 2 VPN address family (AFI=25) and the EVPN address family (SAFI=70) are used to advertise IP and MAC address information between BGP speakers. The EVPN address family routing table contains reachability information for establishing VXLAN tunnels between VTEPs.

The Aruba ESP data center design uses two spine layer switches as iBGP route reflectors. The number of destination prefixes and overlay networks consumes physical resources in the form of forwarding tables and should be taken into consideration when designing the network. The reference architecture section provides hardware guidelines for scaling the design of the data center network.

Segmentation Policy Prerequisites

Data center applications are deployed in many different ways. Applications can be implemented as VMs using hypervisors or hosted in bare-metal servers. Containerized apps are highly distributed and usually require connectivity between multiple compute and service nodes. In some cases, a single data center will host applications for multiple tenants while offering a set of shared services across them. Because of how applications are deployed in a modern data center—with the majority of traffic contained within the data center—it would be incorrect to assume that all security threats are external.

Successful data center policy design begins with understanding the requirements of the applications that will run in the environment. It is often necessary to re-profile legacy applications when there is not sufficient documentation of the requirements. From a networking perspective, application profiling should document all network connections required for that application to run successfully. These might be to backend databases or to cloud-hosted services. To properly define policy regarding which connections must be permitted and which will be denied, it's first necessary to know the application profile.

Similarly, a profile of the users accessing the applications and data is typically required. Never leave a data center wide open to a campus, even if it is assumed to be a secure environment. To restrict access, understand the various user profiles associated with the applications and data required. It's important to identify on-campus, remote branch, mobile field workers, and public Internet requirements so that appropriate data center access profiles can be developed to represent their unique requirements.

Virtual Routing Domain Segmentation

Common best practice is to use the minimum number of VRFs required to achieve clearly defined organizational goals, as each additional VRF increases the complexity of a network. VRFs are employed to support the following use cases:

- Separate production and development application environments. This provides a development sandbox while minimizing risk to production application uptime, and it supports overlapping IP space when required.
- Apply policy to segmented traffic requiring strict regulatory compliance, such as PCI or HIPAA.
- Apply policy to segmented traffic from hosts identified by organizational policy as requiring segmentation and possessing a common set of security requirements. These sets of hosts often share a common administrative domain.
- Isolate Layer 3 route reachability in a multi-tenancy data center, while supporting overlapping IP space.

Data center routes likely need to be shared with campus network segments. One method is where a data center VRF peering is made with the main campus routing instance. Segmentation into the campus can be achieved by using a VRF-lite handoff, where a direct VRF-to-VRF peering is made between a data center border VRF and its campus VRF neighbor.

Inter-VRF Route Forwarding (IVRF) can be used within a data center to share IP prefixes between VRFs. For example, to provide shared services in a data center, a services VRF can be created to offer a common set of resources and IVRF allows reachability between the application and services VRFs.

VLAN Segmentation

In addition to limiting broadcast domain size, a VLAN and its associated IP subnet is used to group sets of data center hosts by role, application, and administrative domain.

VLANs that are members of the same VRF have layer 3 reachability between subnets. These layer 3 boundaries then become a key point of policy enforcement. VLAN ACLs are typically used to enforce a base policy between subnets in a VRF. When more sophisticated policy requirements arise, the common solution is to deploy a centralized firewall and make it the default gateway for application subnets. This generally results in sub-optimal, inefficient traffic patterns. The Aruba ESP data center provides the option of deploying CX 10000 ToR switches which offer hardware-based, Layer 4 firewall capabilities at the host's uplink switch, thereby reducing the need to hair-pin traffic.

Microsegmentation

Microsegmentation extends policy enforcement down to the individual workload and network host level. The Aruba CX 10000 series switch provides a complete and consistent microsegmentation strategy that can be applied across a broad set of data center hosts. Similar to a hypervisor-based firewall, the CX 10000 provides the ability to segment between VM guests on the same VM host using a private VLAN (PVLAN) mechanism. The CX 10000 provides a single, data center microsegmentation strategy supporting all hypervisor types (VMware, Microsoft Hyper-V, KVM, etc.) and bare metal servers. Using the CX 10000 in place of a hypervisor-based implementation offloads policy enforcement cycles from a VM host CPU to dedicated switch hardware.

Microsegmentation can be applied to a subset of hosts requiring a high level of scrutiny, or it can be applied more broadly to maximize a data center's security posture.

Using Aruba CX 10000 Policy

The Aruba CX 10000 with Pensando provides a powerful policy enforcement engine. This section provides background information and details on how implement CX 10000 firewall policy.

CX 10000 Environments

Applying a consistent PSM-based policy across a data center fabric is more easily achieved when all leaf switches are CX 10000. A mixed environment of DSS and non-DSS capable switches is supported, however, administrators must be mindful of these considerations:

- VM and bare metal hosts requiring firewall policy must be cabled to CX 10000 switches.
- Procedures must be created to prevent automated and manual VM guest migration from a CX 10000 connected VM host to a VM host that is connected to a non-DSS switch, when the VM guest requires DSS-based policy enforcement.
- A combined set of both egress and ingress policies must often be created to achieve defined security goals.

Host Mobility Implications

Ubiquitous host mobility within a fabric requires that all leaf switches support the same capabilities. The stateful firewall security policies supported on a DSS switch are not available on non-DSS switches. VM mobility must be constrained accordingly. For example, when using dynamic tools such as VMware's Distributed Resource Scheduler (DRS), care must be taken to ensure that virtual switch and port group resources are defined to prevent automated movement of a VM guest requiring firewall services to a VM host that is not connected to a DSS switch.

PSM Networks and Policy Basics

PSM associates a *Network* object with a VLAN configured on a CX 10000 switch. Defining a Network informs the switch to forward routed traffic associated with the VLAN to the DSM-based firewall for Layer 4 policy enforcement.

PSM firewall policy is a set of rules that specify source and destination addresses, and the type of traffic allowed using IP protocol and port number. Policy is applied to a Network in either an egress or ingress direction. The direction is from the perspective of the connected host. Traffic sourced from the host is considered egress, and traffic destined to the host is considered ingress.

An ingress rule is applied to traffic routed to the CX 10000 from other switches in the network. An ingress policy cannot be applied between two hosts attached to the same Aruba CX 10000 switch. When using an EVPN fabric overlay, policy is applied to traffic arriving from hosts that are layer 2 adjacent in the fabric overlay, but reside on discrete switches within the fabric. Ingress policy is not applied to layer 2 traffic that is bridged over a Layer-2 link from an adjacent switch.

Routed egress traffic is always forwarded to the DSM for policy enforcement, when a policy is applied to a Network. Egress policy is required to filter traffic between hosts attached to the same CX 10000 switch. Layer 2 bridged traffic is not inspected by the DSM, with the exception of layer 2 traffic forwarded to another fabric switch in an EVPN fabric overlay.

In a CX 10000-only environment, a set of egress policies can be used to specify allowed east-west data center traffic, while leaving the the primary role of north-south inbound policy enforcement to the data center at the border leaf. In a mixed environment of DSS and non-DSS switches, ingress rules are required for complete east-west data center policy enforcement, which brings inbound sessions in scope for the Network where ingress PSM policy is applied.

PSM Policy Considerations

Policy is applied at the VLAN layer, so network requirements of all VLAN members must be considered when creating a policy rule set. When an ingress rule is applied, all routed traffic destined to hosts within the VLAN from other switches must be considered, including all layer 2 EVPN forwarded traffic. When defining an egress rule, all communication sourced by hosts on the VLAN must be considered. Rules allowing underlying services are required when applying an egress policy to a Network, because traffic not explicitly allowed to be sourced by hosts will be blocked by the implicit deny rule. Rules supporting services such as DNS, logging, and authentication must be defined.

Rules in a policy are applied in the order they appear in the list. An implicit deny all rule is applied at the end of a rule set. Rules that are used more often should appear higher in the list.

It is best practice to define a complete set of rules before applying a policy to a Network. If the complete rule set is unknown, an allow-all rule can be applied to collect log data on observed traffic. A complete rule set can be built by inserting rules to allow more specific traffic above the allow-all rule. When no wanted traffic is hitting the allow-all rule at the bottom of the rule set, remove it.

Aruba Reference Architecture for Data Center

The Aruba ESP (Edge Services Platform) data center reference architecture supports high-availability compute racks using redundant top-of-rack (ToR) switches connected in a Layer 3 spine-and-leaf topology. The spine-and-leaf topology optimizes performance and provides a horizontally scalable design that can expand to accommodate a growing data center without disrupting existing network components. A data center can start with as few as two spine switches. When additional capacity is required, up to four spine switches can be deployed in a single fabric. The following figure shows the reference architecture with three spine switches.

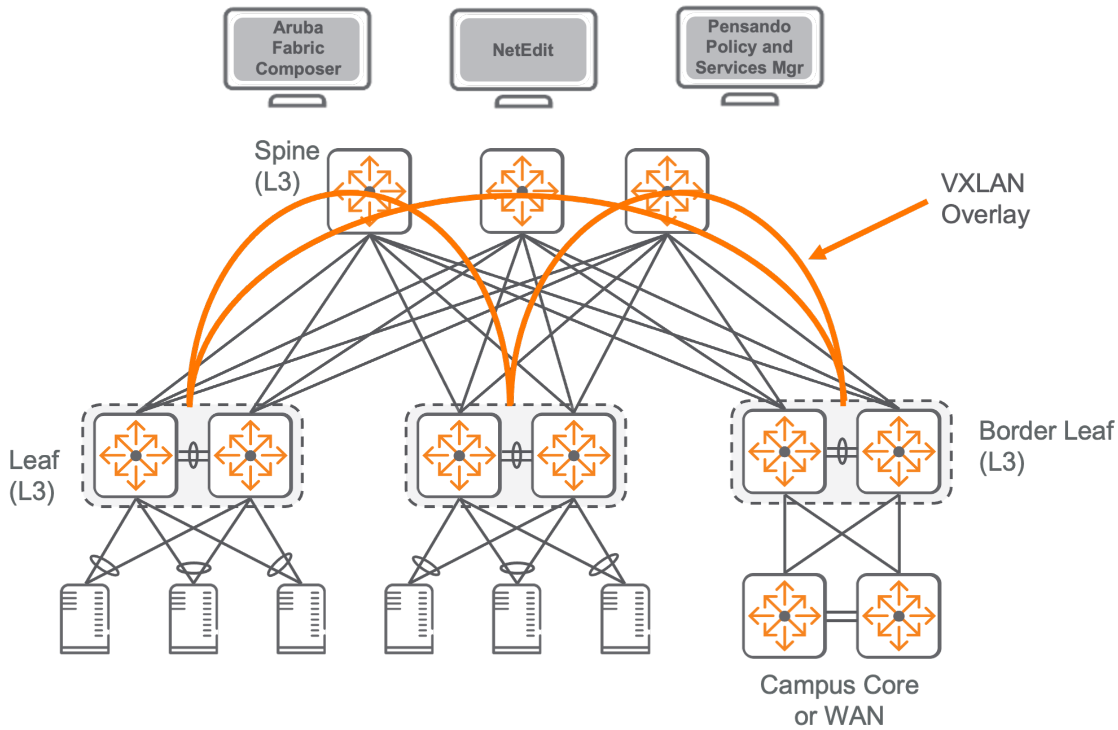

Figure 11: Spine and Leaf: Dual Top of Rack

Certain application environments do not require high availability at the individual compute host. In this case, a single ToR switch per rack will provide a more cost-effective data center network. In this type of implementation, the number of compute hosts deployed per rack should be kept low because a ToR switch under maintenance impacts connectivity to all compute hosts in the rack. The following topology shows a single ToR design with two spine switches.

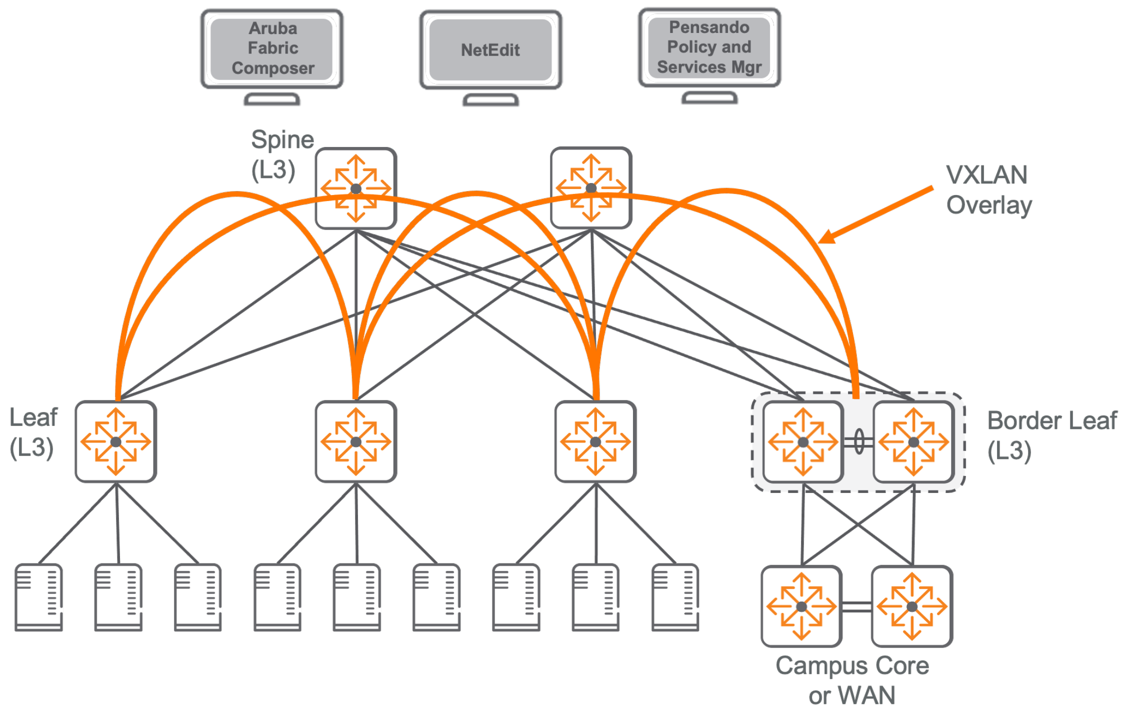

Figure 12: Spine and Leaf: Single Top of Rack

Reference Architecture Components Selection

The following section provides guidance for hardware selection based on your compute host, availability, and bandwidth requirements.

Aruba CX Data Center Switches

The Aruba CX portfolio offers three models of fixed configuration data center switches. The CX 10000 and 8325 models offer high port density, while the CX 8360 model offers a variety of port configurations for small and medium spine-and-leaf topologies. All models offer the following data center switching capabilities:

- High-speed, fully distributed architecture with line-rate forwarding
- High availability and in-service ToR upgrades with VSX
- Cloud-native and fully programmable modern operating system built on a microservices architecture
- Error-free network configuration with software-defined orchestration tools
- Distributed analytics and guided troubleshooting provide full visibility and rapid issue resolution
- Hot-swappable and redundant load-sharing fans and power supplies
- Power-to-port and port-to-power cooling options for different data center designs
- Jumbo frame support for 9198 byte frames

- Advanced Layer 2 and Layer 3 features to support VXLAN spine and leaf with MP-BGP / EVPN control plane
- Distributed active gateways for supporting host mobility

The Aruba CX 10000 distributed services switch supports additional features to consider when selecting a leaf switch model. The on-board Pensando DPU currently supports in-line stateful firewall enforcement and enhanced traffic visibility. Future functions will include encryption services, DDoS protection, load-balancing, and NAT.

Spine Switches

The Aruba ESP data center reference architecture is built around two 1RU high-density spine switches with QSFP ports capable of 40/100 GbE speeds. The Aruba CX 8325 can support up to 32 compute racks in a single ToR switch topology or up to 16 compute racks in a dual ToR switch topology. The Aruba CX 8360 can support up to 12 compute racks in a single ToR switch topology or up to 6 compute racks in a dual ToR switch topology.

The primary function of spine switches is to make routing decisions for the overlay. The primary design considerations when choosing a spine switch are:

- Port density
- Ports speeds
- Routing table sizes

Table 1: Spine Switches

SKU	Description	Maximum Rack Capacity
JL626A	8325: 32-port 40/100 GbE QSFP+/QSFP28, port-to-power airflow	32 single ToR / 16 dual ToR
JL627A	8325: 32-port 40/100 GbE QSFP+/QSFP28, power-to-port airflow	32 single ToR / 16 dual ToR
JL708A	8360: 12-port 40/100 GbE QSFP+/QSFP28, port-to-power airflow	12 single ToR / 6 dual ToR
JL709A	8360: 12-port 40/100 GbE QSFP+/QSFP28, power-to-port airflow	12 single ToR / 6 dual ToR

Leaf Switches

There are three leaf-switch models to choose from in the Aruba ESP Data Center reference architecture. All models are 1RU ToR switches that support high-density racks using 10GbE copper or SFP+ ports. SFP ports on the Aruba CX 8360 model also support 10GBASE-T transceivers.

For redundant ToR designs, the high- and medium-density SKUs provide the minimum of four uplink ports that are required for a two-spine-switch topology. For non-redundant ToR design, medium- and low-density SKUs provide the minimum of two uplink ports required for a two-spine-switch topology.

The Aruba CX 10000 distributed services switch adds firewall features typically provided by dedicated appliances in a services leaf or attached compute hosts as in-line switch fabric features. The Aruba CX 10000 switch should be selected when these features are required by downstream hosts or to meet other data center goals. These features are not available on other CX switch models. A mix of different ToR leaf switch models can connect to a common spine. The CX 10000, 8325, and 8360 can be installed in leaf racks that do not require a distributed service switch features.

The following table summarizes the leaf SKUs available with their corresponding supported designs.

Table 2: **Leaf Switches**

SKU	Description	Rack Design	Spine Design
R8P13A	10000: 48-port 1/10/25 GbE SFP/SFP+/SFP28, 6-port 40/100 GbE QSFP+/QSFP28, port-to-power airflow	High Density / Dual ToR	2 to 3 switches
R8P14A	10000: 48-port 1/10/25 GbE SFP/SFP+/SFP28, 6-port 40/100 GbE QSFP+/QSFP28, power-to-port airflow	High Density / Dual ToR	2 to 3 switches
JL624A	8325: 48-port 1/10/25 GbE SFP/SFP+/SFP28, 8-port 40/100 GbE QSFP+/QSFP28, port-to-power airflow	High-density / dual ToR	2–4 switches
JL625A	8325: 48-port 1/10/25 GbE SFP/SFP+/SFP28, 8-port 40/100 GbE QSFP+/QSFP28, power-to-port airflow	High-density / dual ToR	2–4 switches
JL706A	8360: 48-port 100M / 1GbE / 10GbE 10GBASE-T, 4-port 40/100 GbE QSFP+/QSFP28, port-to-power airflow	High-density / dual ToR	2 switches
JL707A	8360: 48-port 100M / 1GbE / 10GbE 10GBASE-T, 4-port 40/100 GbE QSFP+/QSFP28, power-to-port airflow	High-density / dual ToR	2 switches
JL700A	8360: 32-port 1/10/25 GbE SFP/SFP+/SFP28, 4-port 40/100 GbE QSFP+/QSFP28, port-to-power airflow	Medium-density / dual ToR	2 switches
JL701A	8360: 32-port 1/10/25 GbE SFP/SFP+/SFP28, 4-port 40/100 GbE QSFP+/QSFP28, power-to-port airflow	Medium-density / dual ToR	2 switches
JL710A	8360: 24-port 1/10 GbE SFP/SFP+, 2-port 40/100 GbE QSFP+/QSFP28, port-to-power airflow	Medium-density / single ToR	2 switches
JL711A	8360: 24-port 1/10 GbE SFP/SFP+, 2-port 40/100 GbE QSFP+/QSFP28, port-to-power airflow	Medium-density / single ToR	2 switches
JL702A	8360: 16-port 1/10/25 GbE SFP/SFP+/SFP28, 2-port 40/100 GbE QSFP+/QSFP28, port-to-power airflow	Low-density / single ToR	2 switches

SKU	Description	Rack Design	Spine Design
JL703A	8360: 16-port 1/10/25 GbE SFP/SFP+/SFP28, 2-port 40/100 GbE QSFP+/QSFP28, power-to-port airflow	Medium-density / single ToR	2 switches

Out-of-Band Management Switches

The Aruba ESP data center reference architecture uses a management LAN built on dedicated switching infrastructure to ensure reliable connectivity to data center infrastructure for automation, orchestration, and traditional management access. The following table lists the recommended switch models.

Table 3: Out-of-Band Management Switches

SKU	Description	Host ports
JL667A	Aruba CX 6300F 48-port 1 GbE and 4-port SFP56 Switch	48
JL668A	Aruba CX 6300F 24-port 1 GbE and 4-port SFP56 Switch	24
JL663A	Aruba CX 6300M 48-port 1 GbE and 4-port SFP56 Switch	48
JL664A	Aruba CX 6300M 24-port 1 GbE and 4-port SFP56 Switch	24
JL724A	Aruba 6200F 24G 4SFP+ Switch	24
JL726A	Aruba 6200F 48G 4SFP+ Switch	48
JL678A	Aruba 6100 24G 4SFP+ Switch	24
JL676A	Aruba 6100 48G 4SFP+ Switch	48

Aruba Fabric Composer

Aruba Fabric Composer (AFC) is offered as a self-contained ISO or virtual machine OVA and can be installed in both virtual and physical host environments as a single instance or as a high-availability, three-node cluster. AFC is available as an annual per-switch software subscription.

AFC supports the Aruba CX 10000, 8325, and 8360 series switches recommended for spine and leaf roles. It also supports Aruba CX 6300, 6400, and 8400 series switches.

Ordering information for AFC is at the end of the solutions overview.

Pensando Policy and Services Manager

The Pensando Policy and Services Manager (PSM) runs as a virtual machine OVA on a host. PSM requires vCenter for installation, and it is deployed as a high-availability, quorum-based cluster of three VMs.

PSM supports Aruba CX 10000 series switches. Management of PSM is integrated into AFC.

PSM can be downloaded from the Aruba Support Portal. Entitlement to PSM is included with the purchase of an Aruba CX 10000 switch by adding the R9H25AAE SKU.

NetEdit

NetEdit runs as a VM OVA on a host. Aruba NetEdit is available from the Aruba Service Portal. Customers must visit the Aruba Airheads Community and create an Airheads account in order to download the NetEdit software.

Ordering information for Aruba NetEdit is at the end of this data sheet.

Reference Architecture Physical Layer Planning

The following section provides guidance for physical layer planning of your data center switches.

Cables and Transceivers

Please refer to the following documents to make sure that you select supported cables and transceivers as you plan for physical connectivity inside your data center:

HPE Server Networking Transceiver and Cable Compatibility Matrix

ArubaOS-Switch and ArubaOS-CX Transceiver Guide

Port Speed Groups

When planning for ToR configurations that require server connectivity at multiple speeds, it is important to note that setting the speed of a port might require adjacent ports to then operate at that same speed.

Aruba CX 8325 and Aruba CX 10000 switches have a default speed of 25GbE. Changing the speed to 10GbE will impact groups of 12 ports on the Aruba CX 8325 and groups of four ports on the Aruba CX 10000. Aruba CX 8360 switches allow individual ports to operate at different speeds without impacting adjacent ports unless Media Access Control security (MACSec) is in use. Ports configured to use MACSec must all be configured to operate at the same speed.

Split Ports

Breakout cables can be used to split a 40 Gb/s or 100 Gb/s port, into four lower-speed connections (4x10 Gb/s and 4x25 Gb/s). Please refer to the ArubaOS-Switch and ArubaOS-CX Transceiver Guide for selecting supported breakout cables and switch support for split ports.

Media Access Control Security

MACsec is a standard defined in IEEE 802.1AE that extends standard Ethernet to provide frame-level encryption on point-to-point links. This feature is typically used in environments where additional layers of data confidentiality are required or where it is impossible to physically secure the network links between systems. Please refer to the following table for details of MACsec support in the Aruba switching portfolio:

Table 4: MACsec Support in Aruba Switches

SKU	Description	Supported Ports
JL700A	8360: 32-port 1/10/25 GbE SFP/SFP+/SFP28, 4-port 40/100 GbE QSFP+/QSFP28, port-to-power airflow	1–4 SFP+/SFP28
JL701A	8360: 32-port 1/10/25 GbE SFP/SFP+/SFP28, 4-port 40/100 GbE QSFP+/QSFP28, power-to-port airflow	1–4 SFP+/SFP28

Reference Architecture Capacity Planning

The following section provides capacity planning guidance for the Aruba ESP data center spine-and-leaf reference architecture.

Bandwidth Calculations

A spine-and-leaf network design provides maximum flexibility and throughput for Aruba ESP data center implementation. To achieve the greatest level of performance, a spine-and-leaf topology can be designed for zero oversubscription of bandwidth. This results in a data center network that will never be congested because the bandwidth available to hosts is equal to the bandwidth between leaf-and-spine switches.

A significant advantage of a spine-and-leaf design is that additional capacity can be added as needed by adding additional spine switches and/or increasing the speed of the uplinks between leaf-and-spine switches. A rack with 40 dual-homed servers with 10 GbE NICs could theoretically generate a total load of 800G of traffic. For that server density configuration, a 1:1 (non-oversubscribed) fabric could be built with four spine switches using 4x100 GbE links on each. In practice, most spine-and-leaf topologies are built between 2.4:1 and 6:1 server-to-fabric oversubscription ratio.

Network and Compute Scaling

The Aruba ESP data center reference architecture provides enough capacity for most deployments. With distributed gateways and symmetric IRB forwarding, the MAC and ARP tables are localized to directly attached compute nodes and not impacted by the number of racks. The amount of IP prefixes will be a function of the total number of nodes, fabric links, and also the number of physical and/or virtualized servers. The border leaf is typically the node with the highest control plane load as it handles both internal and external connections. Route summarization is a good practice to reduce the redistribution of IP prefixes between domains.

The Aruba ESP data center reference architecture was thoroughly tested in an end-to-end solution environment that incorporates best-practices deployment recommendations, applications, and load profiles that represent production environments.

Please refer to the product data sheets on Aruba Campus Core and Aggregation Switches for detailed specifications not included in this guide. The following table provides validated multi-dimensional profiles to you can use for spine-and-leaf design capacity planning.

Table 5: Validated Multi-Dimensional Profiles

Feature	8325 Leaf	8360 Leaf	8325 Spine	8360 Spine
Host scale—IPv4/ARP	30,000	50,000	N/A	N/A
Host scale—IPv6/ND	15,000	50,000	N/A	N/A
Routing—IPv4 routes	10,000	16,000	72,000	100,000
Routing—IPv6 routes	1000	8000	20,000	100,000
Routing—OSPF neighbors	4	4	128	64
VXLAN—overlay VRFs (Layer 3 VNI)	32	32	N/A	N/A
VXLAN—host VLANs (Layer 2 VNI)	1024	512	N/A	N/A
Active gateway SVIs	1000	512	N/A	N/A

Summary

Data center networks are changing rapidly. The most pressing challenge is maintaining operational stability, security, and visibility while placing compute and storage resources where they best serve users. In addition, data center teams are being asked to support the rapid pace of DevOps environments, including connecting directly with public cloud infrastructure. Given the rapidly changing landscape for data center requirements, it's critical that network and system engineers get the tools they need to simplify and automate complex infrastructure configurations.

The Aruba Networks ESP Data Center is built on technology that provides tools for transforming the data center into a modern, agile, services delivery platform that satisfies the requirements of organizations large, small, distributed, and centralized. ArubaOS-CX simplifies operations and maintenance with a common switch OS across campus, branch, and data center, managed from the cloud or on-premises, and backed by AI that provides best-practices guidance throughout the network lifecycle.

What's New in This Version

The following changes were made since Aruba last published this guide: - Expanded policy layer design guidance. - Expanded PSM and Aruba CX 10000 details.

aruba
a Hewlett Packard Enterprise company

www.arubanetworks.com

3333 Scott Blvd. Santa Clara, CA 95054
1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550