Aruba Central NetConductor

User Guide

a Hewlett Packard
Enterprise company

Copyright Information

Open Source Code

Contents

Chapter 1
About This Document

This document describes the Aruba Central NetConductor and provides detailed instructions for setting up, configuring, and managing all supported deployments.

Intended Audience

This guide is intended for network administrators who manage and monitor networks.

Related Documents

In addition to this document, see the following documents for more details on Aruba Central NetConductor:

- *Aruba Central Online Help* at https://www.arubanetworks.com/techdocs/central/latest/content/home.htm

Conventions

Table 1 lists the typographical conventions used throughout this guide to emphasize important concepts:

Table 1: *Typographical Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: ■ Sample screen output ■ System prompts
Bold	■ Keys that are pressed ■ Text typed into a GUI element ■ GUI elements that are clicked or selected

The following informational icons are used throughout this guide:

NOTE

Indicates helpful suggestions, pertinent information, and important things to remember.

CAUTION

Indicates a risk of damage to your hardware or loss of data.

WARNING

Indicates a risk of personal injury or death.

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	asp.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	lms.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

Chapter 2

Aruba Central NetConductor Overview

With an ever-growing focus on security and scale, the enterprise network is becoming more and more complex in terms of design, deployment, and operations. There is an increasing reliance on BYOD (Bring Your Own Device) and IoT (Internet of Things) for business efficiency and digital transformation initiatives. This increases the risk of security threats to the enterprise due to a sharp increase in the unknown or rogue clients and an ever-expanding threat front. Defining policy manually for these clients using the complex policy constructs available today can prove to be a challenging task for security and network administrators. Furthermore, intent-based networking has become an increasingly popular paradigm that many customers are looking to adopt and implement. The goal of intent-based networking is not only to abstract the underlying complexities of network but instead allow users to design, implement, and operate their networks based on their business intents. Automated network provisioning and orchestration has been identified to achieve this level of abstraction by many network vendors. Thus, the focus has shifted to the security, scalability, and simplification of these networks.

Aruba Central NetConductor is an edge-to-cloud network and security framework designed to tackle these problems for the modern enterprise network. It is tied directly to the Aruba ESP (Edge Services Platform) vision of an edge-to-cloud network. Intelligent overlays are built on highly available underlays and are tied to a full policy-based micro-segmentation model, based on global roles, across the entire network infrastructure of the customer. Role-based policies abstract policy from the underlying network and enable flexible and simplified policy definition and enforcement. This is enhanced by the full automation of the underlay, orchestration of the overlay, a single pane of glass for management and monitoring, and a rich array of complementary services. The Aruba Central NetConductor framework has evolved to enhance the policy and orchestration components to deliver true intent-based network evolution and optimization.

The following are the main pillars of Aruba Central NetConductor:

- **Role-based Segmentation**—Aruba Central NetConductor provides the ability to deploy a zero-trust enforcement model using role-based segmentation. Traditional policies use location specific entities like IP addresses or subnets to define security policies. Role-based policies abstract policy from the underlying network by assigning roles to endpoints or users and using roles to enforce policies. Role-based policies can be enforced in a distributed manner at different parts of the network. Aruba Central NetConductor also provides the ability to automate and simplify policy definition for IoT devices with behavior-based profiling using AI or ML based classification. This greatly simplifies policy definition and ensures consistent policy enforcement across wired and wireless campus networks, the datacenter, and across the WAN.

- **Intelligent Overlays**—Overlay networks provide the ability to deploy flexible services based on ever-changing demands of the endpoints and applications. Decoupling of overlay network from the physical topology enables on-demand deployment of layer 2 and layer 3 services irrespective of underlay physical topology. Overlay networks also enable the ability to carry endpoint or user role information across the network without requiring all devices in the path to understand or manage the roles. Aruba Central NetConductor provides customers the flexibility to choose between centralized overlays or distributed overlays to address their unique requirements. The centralized overlay provides simplified operations and advanced security features for distributed enterprise and smaller campus deployments. For large enterprise campus deployments, Aruba Central

NetConductor provides the ability to use distributed overlays for wired and wireless endpoints. This enables large enterprises to deploy a standards-based and scalable overlay network. Both overlay models support the Colorless Ports feature, which enables automated client on-boarding and access control for ease of operations.

- **Automation and AI Ops**—One of the primary requirements for enterprise campus network is simplicity of deployment, maintenance, and troubleshooting. With cloud-based management provided by Aruba Central, enterprise devices can be on-boarded and managed in a matter of minutes. Intent-based workflows enable architects to deploy and provision the network without the need for technical expertise in the networking protocols and the command line interface. Aruba Central also provides unified policy orchestration for the global network across wired, wireless, and SD-WAN. Aruba Central NetConductor also enhances end user experience and reduces help desk calls with real time problem identification and AI or ML driven actionable insights.

Benefits of Aruba Central NetConductor

The following are some of the key benefits of the Aruba Central NetConductor solution. The objective of this guide is to highlight these capabilities to the customer.

- **Simplified and Consistent Security Policies**
  - Simplified policy definition based on customer identity
  - Security policies agnostic of location, network, and devices
  - Policy follows the endpoint, user, or application across wired and wireless networks
  - Consistent policies across Campus, Branch, and Datacenter
  - Increase scale by eliminating the need for enforcement nodes to maintain endpoint to role mappings to enforce polices
- **Flexible Overlays Agnostic of Underlay Architecture**
  - Flexible choice of centralized or distributed Aruba Central NetConductor fabrics on any underlay physical network architecture
  - Automated stich-up and tear-down of layer 2 and layer 3 services based on customer on-boarding
  - Address requirements of small, distributed enterprise to a large campus network
- **Simplified Network Deployments and Operations with Intent-Driven Workflows**
  - Abstract complexity of the underlying protocols from network architects or operators
  - Enables global orchestration of roles and role-based policies from Aruba Central
  - Unified monitoring and troubleshooting across all device types and network locations
  - Actionable insights enable ease of troubleshooting for network issues

Features for Aruba Central NetConductor

The following features are available as select features in Aruba Central:

1. Global Client Roles
2. Fabric Provisioning Wizard
3. Static VXLAN Tunnels on AOS 10 Gateways

Aruba Central NetConductor Vocabulary

The following table provides a brief description of the technical terms used in this guide.

Table 3: *List of Technical Terms used in this Guide*

Term	Description
Border	Border device persona connects the fabric to external networks. For example, connect fabric to WAN or Internet or firewalls.
Border Gateway Protocol (BGP)	BGP is a standardized routing method that enables the internet to exchange routing information between autonomous systems (AS).
Ethernet VPN (EVPN)	EVPN is an extension of the BGP protocol for layer 2 (bridging) and layer 3 (routing) VPNs.
Edge	Edge is a device persona that connects endpoints to the fabric.
External BGP (eBGP)	Refers to BGP connection between external peers.
Fabric	Fabric is a group of AOS-CX Switches that are part of the BGP-EVPN VXLAN overlay. The overlay fabric is created by configuring VXLAN tunnels between stub and edge Switches.
Group-based Policy (GBP)	GBP is used to segment user traffic in a network by grouping the users into roles based on user authentication at the source or VTEP. Source-based roles will remain effective even if a device authenticates at a different location, or if the device is assigned a different IP address.
Internal BGP (iBGP)	Refers to BGP connection between internal peers.
Inter-Switch Link (ISL)	ISL is a layer 2 interface between two VSX peer Switches. Each VSX Switch must be configured with an ISL link connected to its peer VSX Switch.
Open Shortest Path First (OSPF)	OSPF refers to an Interior Gateway Protocol (IGP). OSPF distributes routing information between routers belonging to a single Autonomous System (AS).
Policy Identifier	Policy Identifier is a unique identification number mapped to a client role.
Stub	Stub is a device persona that supports both static VXLAN tunnels and EVPN VXLAN tunnels.
Switch Virtual Interface (SVI)	An SVI (also known as VLAN interface) refers to a logical layer 3 interface on a Switch.
Virtual Extensible LAN (VXLAN)	VXLAN is an Overlay Technology which address the scalability problems associated with large cloud computing deployments.
Virtual Routing and Forwarding (VRF)	VRF is a technology that allows multiple instances of a routing table to co-exist within the same router simultaneously in an IP-based computer network.
VXLAN Network Identifier (VNI)	Refers to VXLAN network identifier or VXLAN segment ID.
VXLAN Tunnel End Point (VTEP)	An entity that originates and/or terminates VXLAN tunnels.

Chapter 3
Deployment Scenarios

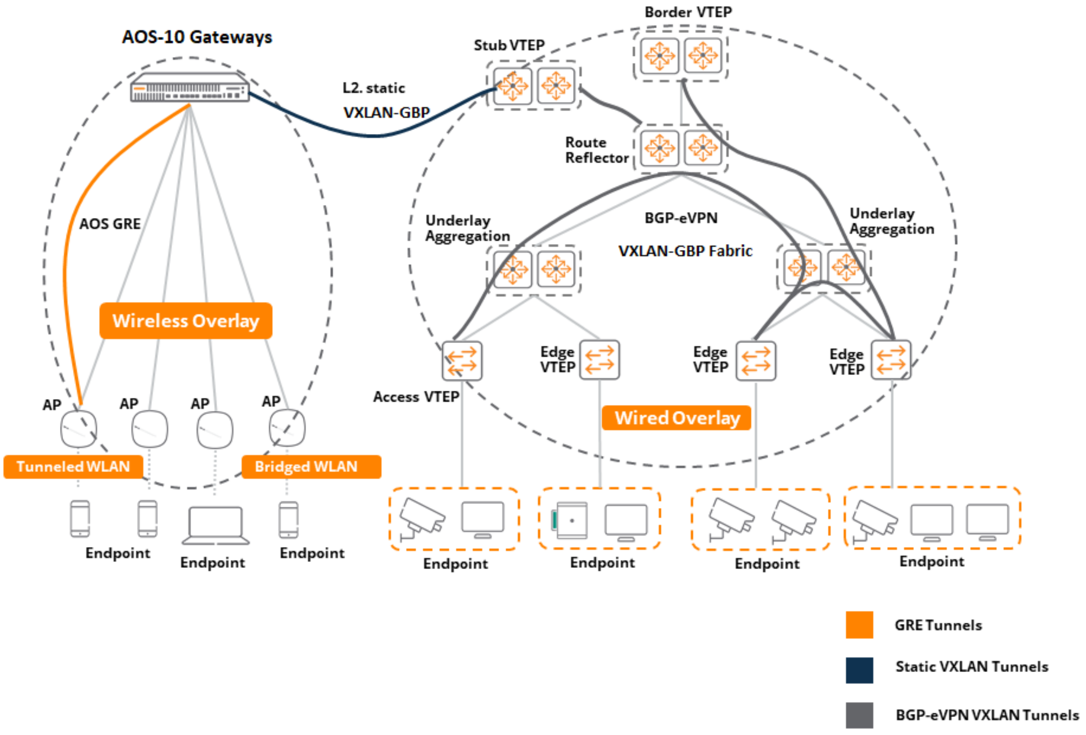
The following section explains the deployment scenarios of Aruba Central NetConductor:

- Distributed Campus-wide Fabric
- Centralized Multi-site Fabric with Aruba SD-Branch
- Centralized Multi-site Fabric with Third-Party SD-WAN

Distributed Campus-wide Fabric

The Distributed Campus-Wide Fabric enables large enterprises to deploy a multi-vendor and scalable overlay across the wired, wireless and wide area network and enables role-based policy enforcement at the edge of the fabric. The fabric consists of a standards-based EVPN-VXLAN fabric on the AOS-CX Switches and is extended to the AOS 10 Gateways using a static VXLAN tunnel. This fabric is based on BGP-EVPN and VXLAN protocols.

Figure 1 *Distributed Campus-wide Fabric Deployment*

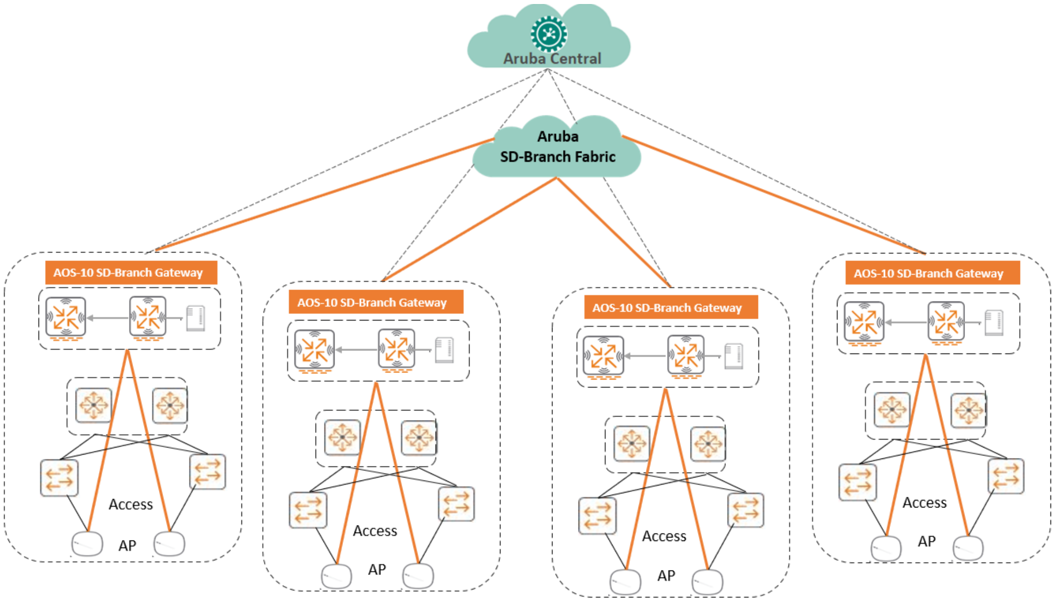


The Distributed Campus-wide Fabric deployment has an IBGP EVPN-VXLAN overlay on the AOS-CX switches, over an OSPF or IBGP underlay network. The underlay routing protocol is enabled to exchange the loopback addresses of all the devices in the fabric. The IBGP fabric is then established by peering all the edge devices in the fabric to the route-reflector, creating a full-mesh VXLAN-EVPN fabric. This fabric is added to the AOS 10 wireless overlay using a static VXLAN tunnel which enables role propagation from the wireless network to the wired network, and vice-versa.

Centralized Multi-site Fabric with Aruba SD-Branch

In the Centralized Multi-site Fabric with Aruba SD-Branch deployment, the AOS 10 Aruba Gateways act as WLAN and user-based tunnel gateways, and enables connectivity and role propagation over the SD-Branch WAN network. The following example explains the Centralized Multi-site Fabric deployment using a AOS 10 Aruba Gateways.

Figure 2 *Centralized Multi-site Fabric with Aruba SD-Branch Deployment*

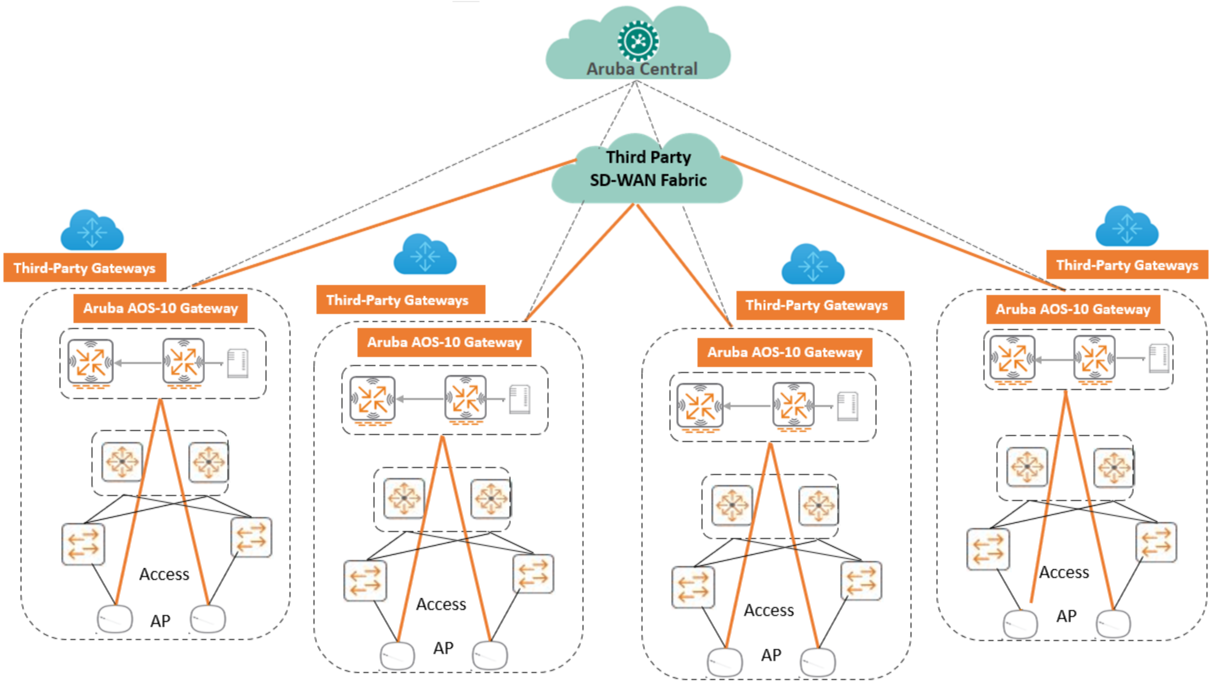


In the Centralized Multi-site Fabric deployment, customers can propagate role information and enforce role-based policies for client traffic across multiple sites connected by an Aruba SD-Branch fabric. The AOS 10 Gateways act as the WLAN and user-based tunnel Gateways for wired and wireless clients within each site, and act as the policy enforcement point for the clients within the site. To enforce role-based policies destined to clients across the fabric. The AOS 10 Gateways encapsulates the client traffic information with VxLAN-BGP and IPSEC, which contain role information in the GPID field in the VXLAN header. The AOS 10 Gateway in the destination site will then enforce the role-based policies for client traffic. Role propagation can also be selectively enabled on a per-group basis for SD-Branch deployments.

Centralized Multi-site Fabric with Third-Party SD-WAN

In the Centralized Multi-site Fabric deployment with Third-Party SD-WAN, the AOS 10Aruba Gateway act as WLAN and user-based tunnel gateways and enables role propagation over a 3rd-party SD-WAN network. The following example explains Centralized Multi-site Fabric deployment using a third-party SD-WAN Gateway.

Figure 3 *Centralized Multi-site with Third-Party SD-WAN Fabric Deployment*



In the Centralized Multi-site Fabric deployment, customers can propagate role information and enforce role-based policies for client traffic across multiple sites connected by an Third-Party SD-WAN fabric. The AOS 10 Gateways act as the WLAN and UBT Gateways for wired and wireless clients within each site and act as the policy enforcement point for the clients within the site. To enforce role-based policies destined to sites across the Third-Party SD-WAN fabric, the AOS 10 Gateways encapsulate the client traffic with VXLAN-GBP and IPSEC which contains the source role information in the GPID field in the VXLAN header. The AOS 10 Gateway in the destination site will then enforce the role-to-role policies for the client traffic. Role propagation can also be selectively enabled on a per subnet basis for third-party WAN deployments.

Chapter 4

Supported Devices

Aruba Access Points

Aruba APs do not participate in role-based enforcement. The AOS 10 Gateways enforce role-based policies for all the wireless clients.

The following table shows the list of AP models and supported software required for deploying Aruba Central NetConductor.

Table 4: *Supported APs*

AP Family	AP Model	Supported Software Versions
300 Series	AP-303, AP-303H, AP-303P, AP-304, AP-305	AOS 10.4.0.0 or later
310 Series	AP-314, AP-315, AP-318	
320 Series	AP-324, AP-325 **NOTE:** The 320 Series AP models with 256 MB of SDRAM, manufactured between August 2015 and January 2016, are not supported with ArubaOS 10.x. These 320 Series AP models have a serial number that begins with DD (for example, DD0003824).	
330 Series	AP-334, AP-335	
340 Series	AP-344, AP-345	
360 Series	AP-365, AP-367	
370 Series	AP-374, AP-375, AP-375EX, AP-375ATEX, AP-377, AP-377EX, AP-387	
500 Series	AP-503H, AP-504, AP-505, AP-505H	
510 Series	AP-514, AP-515, AP-518	
530 Series	AP-534, AP-535	
550 Series	AP-555	
560 Series	AP-565, AP-565EX, AP-567, AP-567EX	
570 Series	AP-574, AP-575, AP-575EX, AP-577, AP-577EX	
580 Series	AP-584, AP-585, AP-585EX, AP-587, AP-587EX	
630 Series	AP-635	
650 Series	AP-655	

NOTE

As of AOS 10.3 release the 6XX series APs are supported in Aruba Central NetConductor.

AOS-CX Switches

The following table lists the AOS-CX switches, supported software versions, and the supported personas in Aruba Central.

Table 5: *Supported AOS-CX Switch Series and Software Versions*

Switch Platform	Supported Software Versions	Supported Persona
AOS-CX 6300 Switch Series	10.10.1020 or later	Edge
AOS-CX 6400 Switch Series	10.10.1020 or later	Edge
AOS-CX 8325 Switch Series	10.10.1020 or later	Route Reflector
AOS-CX 8360 Switch Series	10.10.1020 or later	Edge Stub Border Route Reflector
AOS-CX 8400 Switch Series	10.10.1020 or later	Route Reflector

Data sheets and technical specifications for the supported switch platforms are available at: https://www.arubanetworks.com/products/networking/switches/.

Aruba Gateways

The following table shows a list of Aruba Gateway models and the supported software versions, required for deploying the Aruba Central NetConductor.

Table 6: *Supported Aruba Gateways*

Gateway Family	Gateway Model	Supported Software Versions
7000 Series	7005, 7008, 7010, 7024, 7030	AOS 10.4.0.0 or later
7200 Series	7220, 7240XM, 7280	
9000 Series	9004, 9004-LTE, 9012	
9200 Series	9240	

Chapter 5
Getting Started

Before you get started with your onboarding and provisioning operations, browse through the list of Supported Devices in Aruba Central.

This section includes the following topics:

Prerequisites

Role-Based Policy

VXLAN and BGP-EVPN Overview

Prerequisites

The following prerequisites must be fulfilled to add an overlay to the network.

- All Switches must be onboarded on Aruba Central and added to the same UI group.
- All the required Aruba devices are on-boarded and connected to Aruba Central.
- Underlay is set up before attempting to add any overlay to the network.

Aruba Central NetConductor Licensing

Aruba Central licensing is applicable to Aruba Central NetConductor. Advance licensing is required for Switches, APs, and Gateways.

Aruba Central NetConductor Caveats

Aruba Central NetConductor has the following caveats:

- Roles created globally in Aruba Central will not be applied to APs.
- Existing roles in APs, Gateways, and AOS-CX groups are not populated automatically in Aruba Central.

NOTE

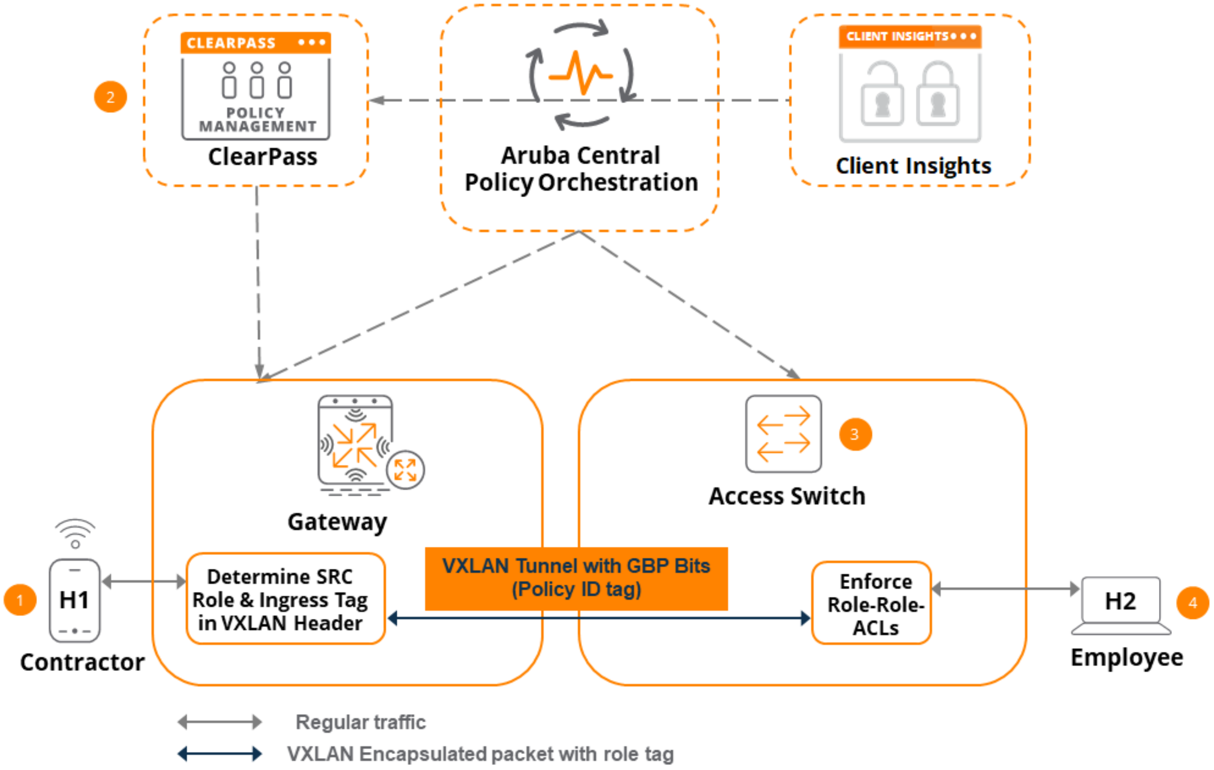
Customer can recreate existing roles on Aruba Central.

- Multicast traffic is supported on the Switch fabric. The configuration is not supported on Aruba Central.
- Only role-to-role policies are allowed. Policies including protocol and port are not supported.

Role-Based Policy

The following section describes how role based policies are distributed and enforced with examples based on authentication and profiling.

Figure 4 *Role-Based Policy—Wired Devices*



Role-Based Policy for Wired Devices Using Identity Store Mapping

The following example describes role based policy enforcement using an identity store to assign roles to wired clients.

1. The wired client H2 (laptop) is connected to an access switch in the network. The access switch sends an 802.1x authentication request to ClearPass.
2. ClearPass has knowledge of the active directory group to which this H2 belongs and the respective role mapping group. In this case, the active directory group is Employee, and the role is Employee. If H2 is a Contractor, then the ClearPass assigns the Contractor role to H2. ClearPass communicates the role for the wired client to the access switch using the "HPE-User-Role" RADIUS attribute as part of the authentication response.
3. When the client H1 (Phone) sends a packet to the client H2 (Laptop), the gateway is now aware that H1 is a Contractor and based on this, it encapsulates the data packet in a VXLAN header and tags the group policy ID of the source role in the GBP field of the VXLAN header.
4. When the packet reaches the Switch where H2 is connected to, the access Switch is aware that the destination role of H2 is an Employee and determines whether the Contractor H1 is allowed to communicate to an Employee H2. If the defined policy between Contractor to Employee is "Deny", then the access Switch blocks the packet. If the defined policy between Contractor to Employee is "Allow", then the access Switch sends the packet to H2.

   For more information about Role-Based Policy support on AOS-CX, refer to Group-based policy.

Role-Based Policy Enforcement for Wired Clients Using Client Profiling

The following example describes role based policy enforcement using profiling to assign roles to wired clients.

For IoT clients such as IP-based light bulbs and cameras, there is usually no active directory group or MAC address directory for these devices. Hence, roles can be assigned to these devices by profiling these devices based static and dynamic attributes. When the light bulb is connected to the access switch, the device is initially authenticated using MAC-Auth and telemetry is sent to the Client Insights service on Aruba Central. Client Insights then profiles the device using attributes such as MAC OUI, DHCP Options and flow data. It uses this data to profile the client with the "IOT" tag and sends this tag to ClearPass. ClearPass now has the MAC address of the client and IOT tag mapping. When the light bulb authenticates, ClearPass assigns the IOT role to the client.

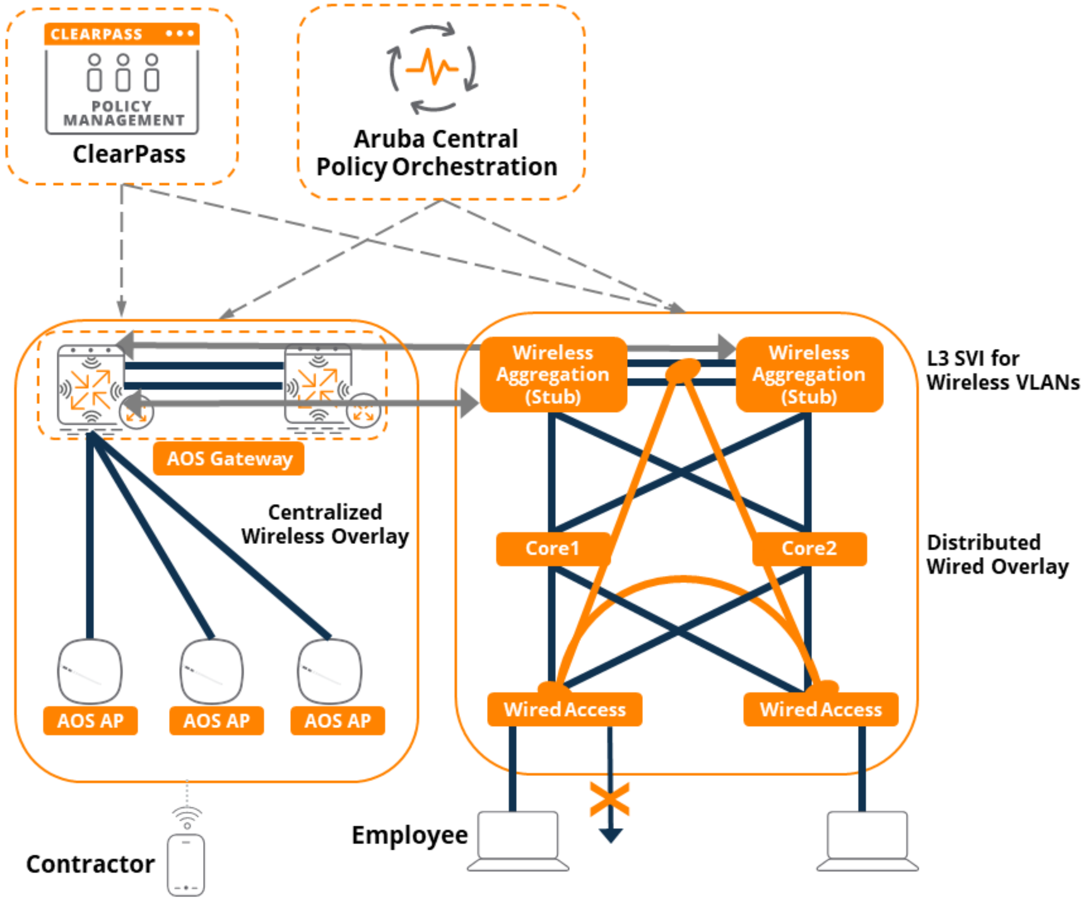
When the IoT client communicates to the laptop with the Employee role, the access Switch which the IOT client is connected to detects that the role for that MAC address is IoT. It encapsulates the data packet in a VXLAN header and tags the group policy ID of the source role in the GBP field of the VXLAN header. The packet then reaches the destination access Switch and determines that the source role is IoT and the destination role is an Employee. If the defined policy between IoT to Employee roles is deny, then the access Switch blocks the packet. If the defined policy between IoT to Employee roles is allow, then the access Switch sends the packet to the Employee laptop.

In an IoT device such as a light bulb which has an IP address, there is no active directory group. There is a device profiling which takes place in the network. When the light bulb is connected to the Switch, the telemetry data is sent to CPDI. CPDI then profiles the device, for example the device's make or device series and tags it with an IoT tag and sends it to ClearPass. ClearPass now has the MAC address of the endpoint and the IoT tag on it. When the endpoint tries to authenticate, ClearPass determines if the tag is IoT, then the role assigned is IoT. The access Switches now have the roles for each of the devices. When the IoT device communicates to a camera at the endpoint, the access Switch detects that the role for that MAC address is IoT and the corresponding group policy ID. The access Switch then adds them in the source header of the VXLAN packet. The packet then reaches the access Switch and determines that the source is IoT and the destination is a camera. If the defined policy IoT to camera is deny, then the access Switch blocks the packet. If the defined policy IoT to camera is allow, then the access Switch delivers the packet.

Role-Based Policy for Wireless Devices

The following example describes role based policy enforcement for wireless clients.

Figure 5 *Role-Based Policy—Wireless Devices*


CLEARPASS
POLICY MANAGEMENT
ClearPass
Aruba Central Policy Orchestration
Wireless Aggregation (Stub)
Wireless Aggregation (Stub)
L3 SVI for Wireless VLANs
AOS Gateway
Centralized Wireless Overlay
Core1
Core2
Distributed Wired Overlay
Wired Access
Wired Access
AOS AP
AOS AP
AOS AP
Employee
Contractor

Wireless clients that connects to an AOS 10 Tunneled WLAN SSID are authenticated by the AOS 10 Gateway via ClearPass, based on either an identity store mapping or client profiling (see above section). The client traffic is tunneled from the AOS 10 APs to the AOS 10 Gateway through a tunneled WLAN. The AOS 10 Gateway authenticates the client with ClearPass and gets the role of the client from ClearPass using the "HPE-User-Role" RADIUS attribute. If the gateway does not have knowledge of both the source and destination role of the traffic, the Gateway encapsulates the data traffic in a VXLAN header and tags the group policy ID of the source role in the GBP field of the VXLAN header. In this example, ClearPass assigns the Contractor role to Phone. The AOS 10 Gateway sends the data traffic on the static VXLAN tunnel to the Wireless Aggregation switch with the GPID of the role Contractor. The destination endpoint in this example is a wired endpoint with the role Employee. The traffic is allowed or denied by the access switch based on the defined Role-Based Policy.

VXLAN and BGP-EVPN Overview

This section introduces you to VXLAN and EVPN, and explains how they can be implemented using Switches.

VXLAN Overview

Virtual eXtensible LAN (VXLAN) is a MAC-in-UDP technology that provides layer 2 connectivity between networks across an IP network. VXLAN is typically used to extend layer 2 segments across an entire data center or between remote data centers. It is also used to provide multi-tenancy services.

VXLAN addresses the requirements of the Layer 2 and Layer 3 data center network infrastructure in the presence of VMs in a multi-tenant environment. It runs over the existing networking infrastructure and provides a means to stretch a Layer 2 network. In short, VXLAN is a Layer 2 overlay scheme on a Layer 3 network. Each overlay is termed a VXLAN segment. Only VMs within the same VXLAN segment can communicate with each other. Each VXLAN segment is identified through a 24-bit segment ID, termed the VXLAN Network Identifier (VNI). This allows up to 16 M VXLAN segments to coexist within the same administrative domain.

The VNI identifies the scope of the inner MAC frame originated by the individual VM. Thus, you could have overlapping MAC addresses across segments but never have traffic cross over since the traffic is isolated using the VNI. The VNI is in an outer header that encapsulates the inner MAC frame originated by the VM. In the following sections, the term VXLAN segment is used interchangeably with the term VXLAN overlay network.

VXLAN Packet Format

Role-to-role policy is defined at the global level in . Role definitions and policy definitions are global to a customer and are distributed by the underlying device configuration system with all the devices as required. These roles and policies are embedded in the VXLAN header.

For more information about different components in the VXLAN Group Based Policy Extension (VXLAN-GBP) header, refer to VXLAN Group Policy Option.

VXLAN Deployment Models

AOS-CX supports the following VXLAN implementations:

- Centralized Routing
- Distributed Routing

Centralized routing and distributed routing defines where the inter-VLAN routing happens. Whether inter-VLAN routing is happening only on the core/border Switches or inter-VLAN routing is performed on the edge devices such as access Switches.

NOTE

Both centralized routing and distributed routing models use EVPN control plane. solution utilizes the distributed routing model.

EVPN VXLAN Overview

EVPN-VXLAN refers to a network fabric that extends layer 2 connectivity as a network overlay over an existing physical network. It is an open standards technology that creates more agile, secure, and scalable networks in campuses and data centers. EVPN-VXLAN consists of:

- Ethernet VPN (EVPN) which is used as the overlay control plane and provides virtual connectivity between different layer 2/3 domains over an IP.
- Virtual extensible LANs (VXLAN), a common network virtualization overlay protocol that expands the layer 2 network address space from 4,000 to 16 million.

How EVPN and VXLAN Work Together

EVPN-VXLAN enables businesses to connect geographically dispersed locations using layer 2 virtual bridging. EVPN-VXLAN provides the scale required by cloud service providers and is often the preferred technology for data center interconnections.

EVPN, as an overlay, supports multi-tenancy and is highly extensible, often using resources from different data centers to deliver a single service. It can provide layer 2 connectivity over physical infrastructure for devices in a virtual network or enable layer 3 routing.

Because it serves as a MAC address learning control plane for overlay networks, EVPN can support different data plane encapsulation technologies.

VXLAN encapsulates layer 2 ethernet frames in layer 3 UDP packets, meaning virtual layer 2 subnets can span underlying layer 3 networks. A VXLAN network identifier (VNI) is used to segment each layer 2 subnet similarly to traditional VLAN IDs.

A VXLAN tunnel endpoint (VTEP) is a VXLAN-capable device that encapsulates and de-encapsulates packets. In the physical network, a Switch typically functions as a layer 2 or layer 3 VXLAN Gateway and is considered a hardware VTEP. The virtual network equivalents are known as software VTEPs, which are hosted in hypervisors such as VMware ESXi or vSphere.

NOTE

For the BGP session for underlay and overlay, currently supports iBGP only.

Global Client Roles

NOTE

Global Client Roles support is selectively available. Contact your Aruba Account Manager to enable it in your Aruba Central account.

Aruba Central allows you to configure client roles for role-to-role policy enforcement. To make client roles more powerful and consistent within the dynamic-segmentation security framework, you can now manage the client roles globally from Aruba Central. For example, if you have five roles in your network, a role-to-role policy is created by defining permissions from one role to another.

Prerequisites

Ensure that all the required Aruba devices are on-boarded and connected to Aruba Central, prior to configuring global client roles and performing selective enablement of subnets.

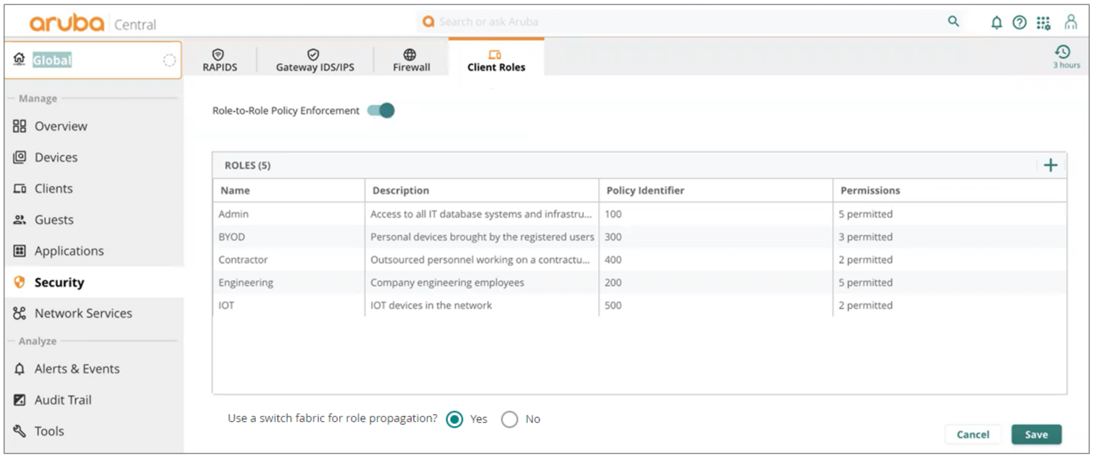
Configuring the Global Client Roles

Global client roles configuration affects all the access Switches and wireless Gateways in the network, as part of the global policy enforcement.

To configure client roles for role-to-role policy enforcement, complete the following procedure:

1. In the **Aruba Central** app, complete the following steps:
   a. Set the filter to **Global**.
   b. Under **Manage**, click **Security > Client Roles**. The **Client Roles** page is displayed.
2. Toggle the **Role-to-Role Policy Enforcement** Switch to the on position, to apply the roles and permissions that are defined.

Figure 6 *Client Roles Page*



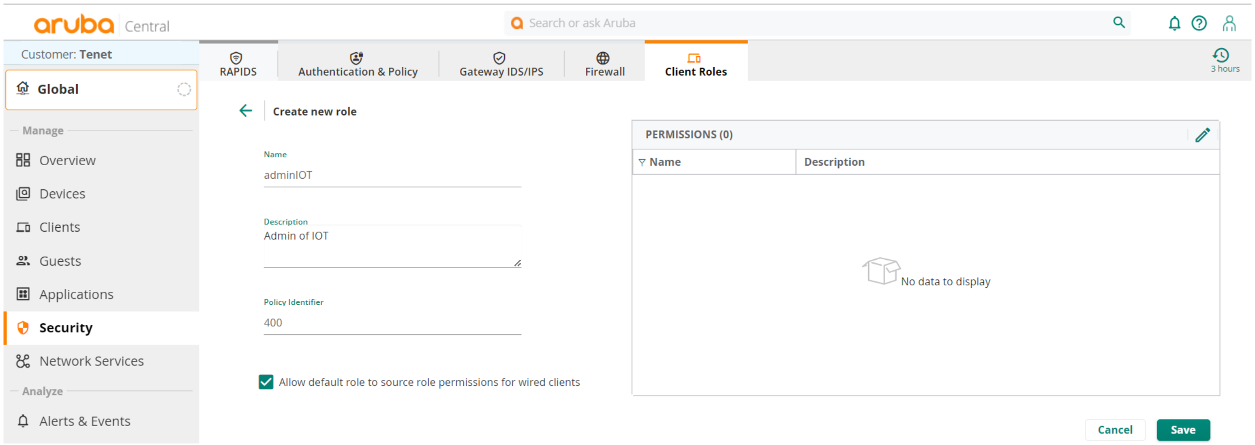
Role-to-Role Policy Enforcement

ROLES (5)

Name	Description	Policy Identifier	Permissions
Admin	Access to all IT database systems and infrastru...	100	5 permitted
BYOD	Personal devices brought by the registered users	300	3 permitted
Contractor	Outsourced personnel working on a contractu...	400	2 permitted
Engineering	Company engineering employees	200	5 permitted
IOT	IOT devices in the network	500	2 permitted

Use a switch fabric for role propagation? ● Yes ○ No

3. In the **Roles** table, click the **+** icon. The **Create new role** page is displayed.



Create new role

Name: adminIOT

Description: Admin of IOT

Policy Identifier: 400

☑ Allow default role to source role permissions for wired clients

4. In the **Create new role** page, configure the following parameters:
   - **Name**—Enter the name of the role that you want to create. For example, Admin.
   - **Description**—Enter the description of the role. For example, all employees in the organization.
   - **Policy Identifier**—Policy Identifier is a unique auto-generated identifier for the role. You can modify identifier, if required. For example, 100.

5. Enable the **Allow default role to source role permissions for wired clients** checkbox if you want to allow unauthenticated client traffic and external traffic (traffic with Policy Identifier 0) for the wired clients.

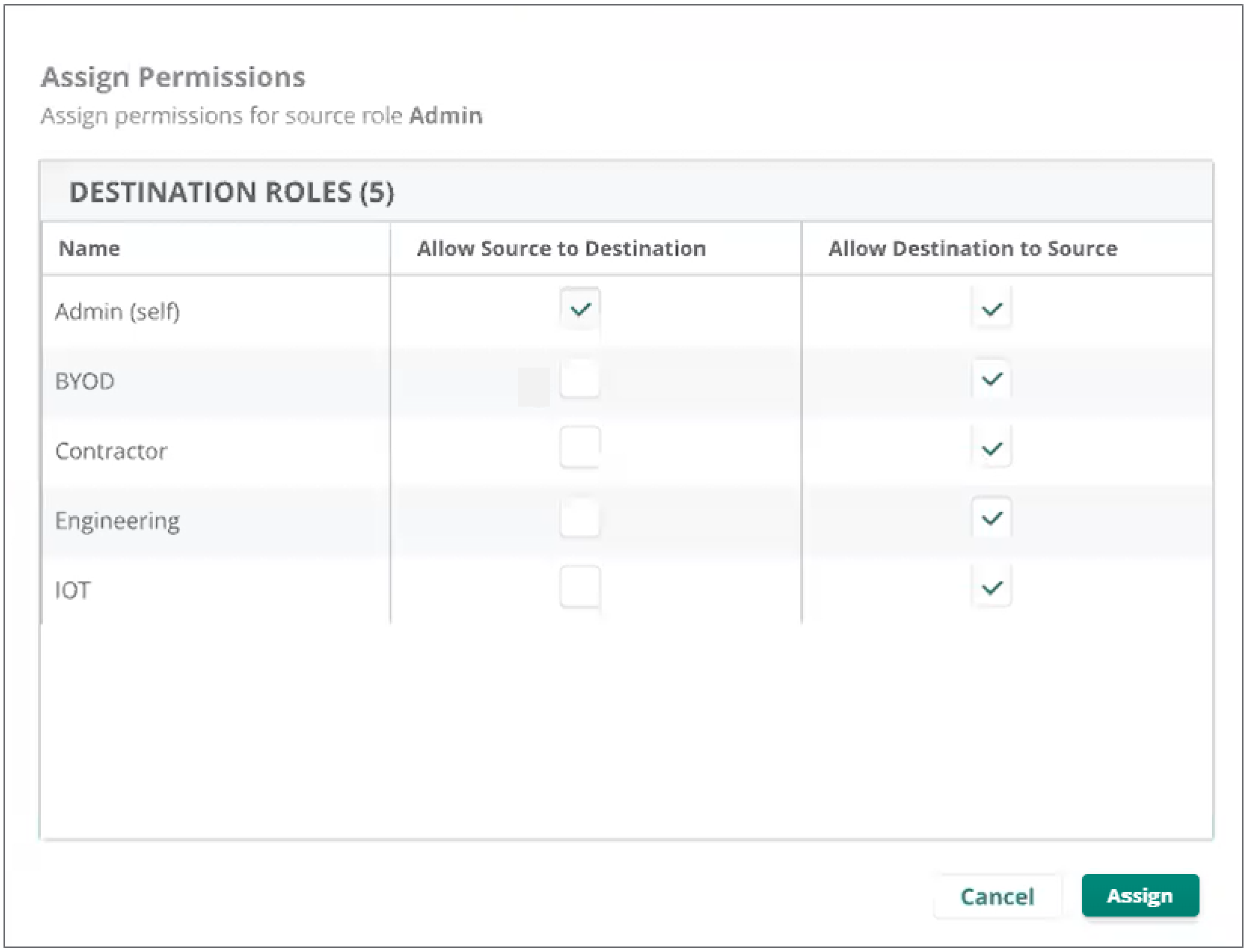
6. In the **Permissions** table, click the ✎ edit icon to create bi-directional policies between roles.

   The **Allow Source to Destination** column is used to enable permissions from the source role to the selected destination role. The **Allow Destination to Source** column is used to enable permissions from the selected destination role to the source role. For example, if you open the **Assign Permissions** window for the Admin role, you must select the check box corresponding to the BYOD role in the **Allow Source to Destination** column to allow network traffic from Admin role to BYOD role. You must click **IOT** under the **Allow Destination to Source** column to allow network traffic from IOT role to Admin role.

NOTE

Selecting either of the check boxes for self, selects both the check boxes by default. Selecting self enables bi-directional network traffic between devices of the same role.

Figure 7 *Assign Permissions Page*



Assign Permissions

Assign permissions for source role **Admin**

DESTINATION ROLES (5)

Name	Allow Source to Destination	Allow Destination to Source
Admin (self)	☑	☑
BYOD	□	☑
Contractor	□	☑
Engineering	□	☑
IOT	□	☑

7. In the **Allow Source to Destination** and the **Allow Destination to Source** columns, select the appropriate check box.
8. Click **Assign**.
9. In the **Use a switch fabric for a role propagation?** options, select **Yes** if you have configured distributed overlay fabric for role propagation. For more information about distributed overlay fabric, see Fabric Provisioning Wizard.
10. In the **Create new role** page, click **Save**.

    The role is created, and the assigned permissions are saved.

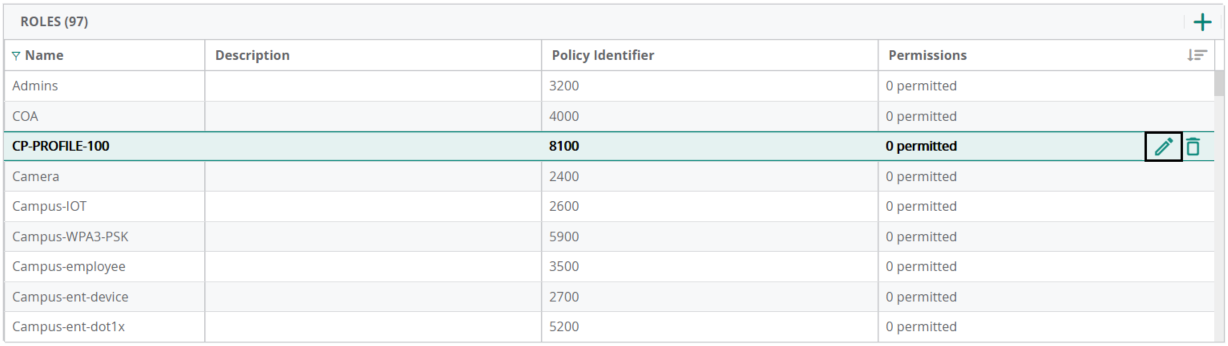
NOTE

Configuring custom policy rules on switches is possible using the Multi-Editor with sequence numbers above 9999.

Editing a Role

To edit a role, complete the following procedure:

1. In the **Aruba Central** app, complete the following steps:
    a. Set the filter to **Global**.
    b. Under **Manage**, click **Security > Client Roles**. The **Client Roles** page is displayed.



ROLES (97)

Name	Description	Policy Identifier	Permissions
Admins		3200	0 permitted
COA		4000	0 permitted
CP-PROFILE-100		8100	0 permitted
Camera		2400	0 permitted
Campus-IOT		2600	0 permitted
Campus-WPA3-PSK		5900	0 permitted
Campus-employee		3500	0 permitted
Campus-ent-device		2700	0 permitted
Campus-ent-dot1x		5200	0 permitted

2. In the **Roles** table, hover over the row, and click the ✎ edit icon.
3. In the **Edit Role** window, modify the required permissions.

The **Allow default role to source role permissions for wired clients** checkbox cannot be modified while editing a role.

4. Click **Save**.

Deleting a Role

To delete a role, complete the following procedure:

1. In the **Aruba Central** app, complete the following steps:
   a. Set the filter to **Global**.
   b. Under **Manage**, click **Security > Client Roles**. The **Client Roles** page is displayed.
2. In the **Roles** table, select the role and click the 🗑 delete icon. The **Confirm Action** window is displayed.
3. Click **Yes**.

Selective Enablement of Subnets

Perform selective enablement of subnets if you have not configured distributed overlay fabric for role propagation. For more information about distributed overlay fabric, see Fabric Provisioning Wizard.

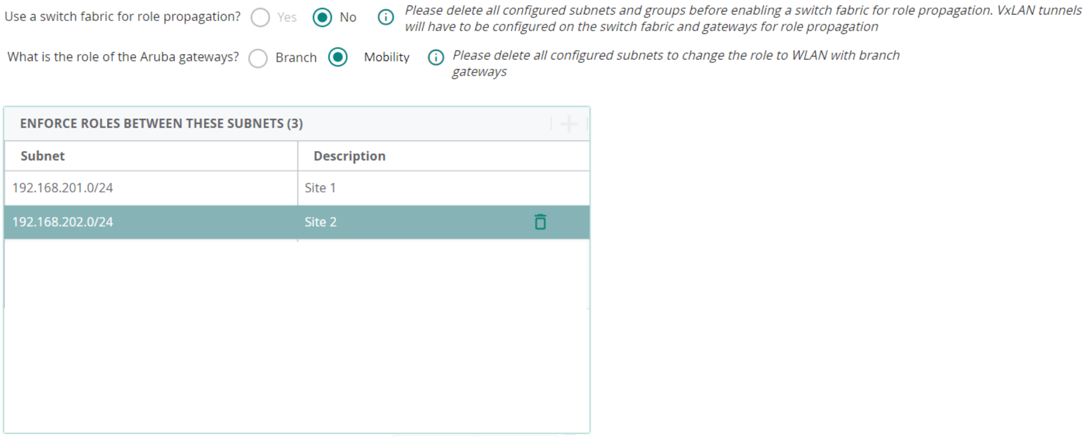
Selective enablement of subnets is used to select the client subnets for which you want to enable role-based policy enforcement on the third-party Gateways. Typically, these client subnets are mapped to different sites in the network.

To selectively enable the subnets that map to the clients in the respective sites using Aruba Central, complete the following procedure:

1. In the **Aruba Central** app, complete the following steps:
   a. Set the filter to **Global**.
   b. Under **Manage**, click **Security > Client Roles**. The **Client Roles** page is displayed.
2. In the **Use a switch fabric for a role propagation?** options, select **No**.

Delete all configured subnets before enabling a switch fabric for role propagation.

3. In the **What is the role of the Aruba gateways?** options, select **Mobility**. Delete all the configured subnets to change the role to Branch Gateways.



Use a switch fabric for role propagation? ○ Yes ● No ⓘ *Please delete all configured subnets and groups before enabling a switch fabric for role propagation. VxLAN tunnels will have to be configured on the switch fabric and gateways for role propagation*

What is the role of the Aruba gateways? ○ Branch ● Mobility ⓘ *Please delete all configured subnets to change the role to WLAN with branch gateways*

ENFORCE ROLES BETWEEN THESE SUBNETS (3)

Subnet	Description
192.168.201.0/24	Site 1
192.168.202.0/24	Site 2

4. Click the **+** icon and then enter the subnet details and the description.
5. Click **Save**.

Deleting a Subnet

To delete a subnet, complete the following procedure:

1. In the **Aruba Central** app, complete the following steps:
   a. Set the filter to **Global**.
   b. Under **Manage**, click **Security > Client Roles**. The **Client Roles** page is displayed.
2. In the **ENFORCE ROLES BETWEEN THESE SUBNETS** table, select the subnet and click the 🗑 delete icon. The **Confirm Action** window is displayed.
3. Click **Yes**.

Selective Enablement of Groups

NOTE

Perform selective enablement of groups if you have not configured distributed overlay fabric for role propagation. For more information about distributed overlay fabric, see Fabric Provisioning Wizard.

Selective enablement of groups is used to select the Aruba Central group for which you want to enable role propagation on AOS 10 SD-Branch gateway. Typically, these client groups are mapped to different SD-WAN branch sites within the Aruba Central network.

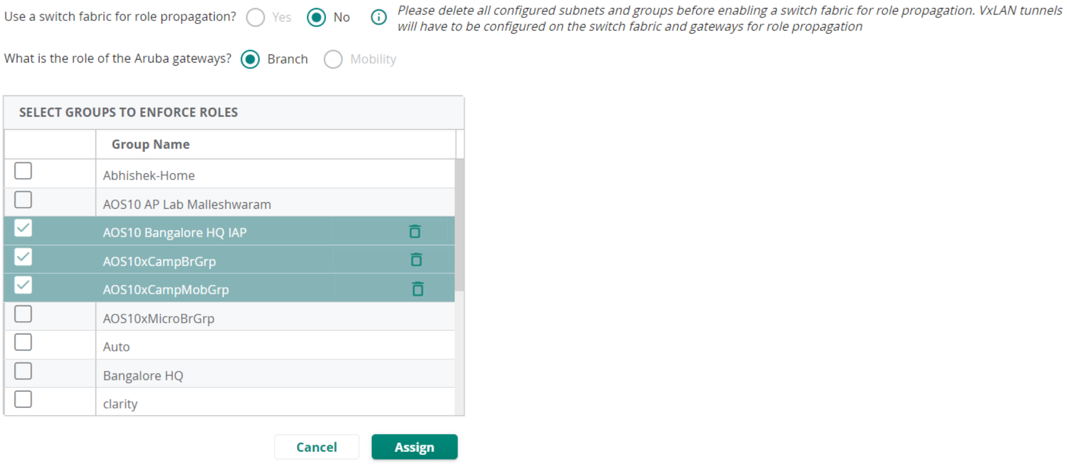
To selectively enable the groups that map to the clients in the respective sites using Aruba Central, complete the following procedure:

1. In the Aruba Central app, complete the following steps:
   a. Set the filter to **Global**.
   b. Under **Manage**, click **Security > Client Roles**. The **Client Roles** page is displayed.
2. In the **Use a switch fabric for a role propagation?** options, select **No**.

NOTE

Delete all configured groups before enabling a switch fabric for role propagation.

3. In the **What is the role of the Aruba gateways?** options, select **Branch**. Delete all configured groups to change the role to WLAN gateways.
4. Click the **+** icon to add the groups.



Use a switch fabric for role propagation? ○ Yes ● No ⓘ *Please delete all configured subnets and groups before enabling a switch fabric for role propagation. VxLAN tunnels will have to be configured on the switch fabric and gateways for role propagation*

What is the role of the Aruba gateways? ● Branch ○ Mobility

SELECT GROUPS TO ENFORCE ROLES

	Group Name	
□	Abhishek-Home	
□	AOS10 AP Lab Malleshwaram	
☑	AOS10 Bangalore HQ IAP	🗑
☑	AOS10xCampBrGrp	🗑
☑	AOS10xCampMobGrp	🗑
□	AOS10xMicroBrGrp	
□	Auto	
□	Bangalore HQ	
□	clarity	

5. Select the groups you want to assign.
6. Click **Assign**.
7. Click **Save**.

Deleting a Group

To delete a role, complete the following procedure:

1. In the Aruba Central app, complete the following steps:
   a. Set the filter to **Global**.
   b. Under **Manage**, click **Security > Client Roles**. The **Client Roles** page is displayed.
2. In the **SELECT GROUPS TO ENFORCE ROLES** table, select the group and click the 🗑 delete icon. The **Confirm Action** window is displayed.
3. Click **Yes**.

Chapter 7

Fabric Provisioning Wizard

Aruba Central allows you to create an overlay fabric by configuring VXLAN tunnels between Stub and Edge Switches and configure overlay segments for the existing overlay fabrics.

Overlay Fabric

The distributed overlay fabric is a group of AOS-CX Switches that are part of the BGP-EVPN VXLAN overlay. The overlay fabric is created by configuring VXLAN tunnels between Stub and Edge Switches. The AOS 10 Gateways also participate in the overlay fabric, using static VXLAN tunnels to the Stub VTEP. Aruba Central allows you to configure the overlay fabric on top of a virtual network using AOS-CX Switches. You can assign a list of fabric personas such as Border VTEP, Route Reflectors, Edge VTEP, or Stub VTEP to the overlay fabric.

Fabric Personas

This section describes the different fabric personas and their functions in the Aruba Central BGP EVPN overlay fabric workflow.

- **Border VTEP**—Refers to a Gateway or an external facing device from the overlay fabric to the external network. Border VTEP participates in the layer 3 VNI or VRF but does not have overlay VLANs or SVIs configured on this device.
- **Route Reflector**—Refers to a concept that is specific to iBGP that is used to optimize route propagation. Route reflector reduces the configuration required on all the devices and optimizes the way BGP sessions are established. In a typical scenario, every edge device in the network peers with every other edge device. To avoid this, a route reflector is introduced where all the devices in the overlay fabric peer with the route reflector which optimizes configuration and route distribution. Core Switches are generally used as route reflectors in an overlay fabric.
- **Edge VTEP**—Refers to a traditional access layer where the clients are onboarded. It is also the layer 3 Gateway for all the clients that are associated with it. Edge VTEP typically has the SVI interface, and it is the entry point of all the wired clients onto the BGP EVPN overlay fabric.
- **Stub VTEP**—Supports static VXLAN and EVPN VXLAN. Stub VTEP is used to establish static VXLAN tunnel to the Gateway and EVPN-VXLAN towards the overlay fabric. Stub VTEP helps to carry role information between EVPN-VXLAN overlay fabric and devices like Gateway that only support Static VXLAN.

Optionally, you can create additional overlay networks, which are on the same VRF and layer 3 VNI, if required. You can also configure the Gateway IP cluster for wireless Gateways.

Prerequisites

Before provisioning the overlay fabric using Aruba Central, ensure that the following prerequisites are completed:

- All Aruba CX switches should be on firmware version 10.10.1020 and above.
- All Switches must be on-boarded on Aruba Central and added to the same UI group.

- All the required Aruba devices are on-boarded and connected to Aruba Central.
- The underlay network must be set up before attempting to add any overlay to the network.
- At least two loopback (loopback 0 and loopback 1) interfaces are configured on all devices of the overlay fabric.
- The IP addresses of the loopback interfaces are unique on each device of the overlay fabric except on the VSX pair (VSX pair has at least one loopback interface whose IP address is the same on both primary and secondary).
- At least one instance of OSPF or BGP should be configured on all devices of the overlay fabric.
- OSPF or BGP router ID should be the IP address of an existing loopback interface.
- OSPF or BGP is configured on at least two loopback interfaces (one is used for OSPF and BGP, and the other for the VXLAN source IP).
- If the device has VSX configuration, the following validations must be performed:
    - The VSX pair has at least one loopback interface with the same IP address (used as VXLAN source IP).
    - Virtual MAC is configured on the device.
    - Virtual MAC is used for VSX configuration.
    - Keep alive is configured.
    - ISL link—LAG interface with member ports is configured.
    - The Virtual MAC should be assigned to the Primary and Secondary switches of the VSX Pair. Virtual MAC is auto-generated and pushed to stand alone devices and VSF conductors only.

NOTE

Configuring the overlay fabric workflow is applicable only to AOS-CX Switches.

Configuring an Overlay Fabric

The following workflow describes the steps to set up the overlay fabric for the AOS-CX Switches.

1. Step 1: Create the Overlay Fabric Name
2. Step 2: Assign Devices and Personas
3. Step 3: Add the Overlay Network
4. Step 4: Creating Static Tunnels from Stub VTEPs to a Gateway Cluster
5. Step 5: View Fabric Summary

Step 1: Create the Overlay Fabric Name

To configure an overlay fabric for the AOS-CX Switch, complete the following steps:

1. In the **Aruba Central** app, complete the following steps:
    - To select a group in the filter:
        a. Set the filter to a group.

           The dashboard context for the group is displayed.

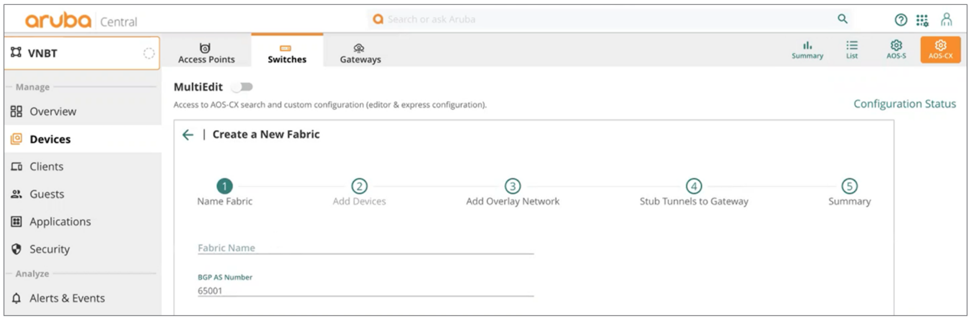
        b. Under **Manage**, click **Devices** > **Switches**.

        c. To view the AOS-CX Switch configuration dashboard, click the **AOS-CX** or **Config** icon.

2. Click **Routing** > **Fabrics**.
3. In the **Fabrics** table, click the **+** icon.

   The **Create a New Fabric** page is displayed.

   Figure 8 *Create a New Fabric Page*



Fabric Name

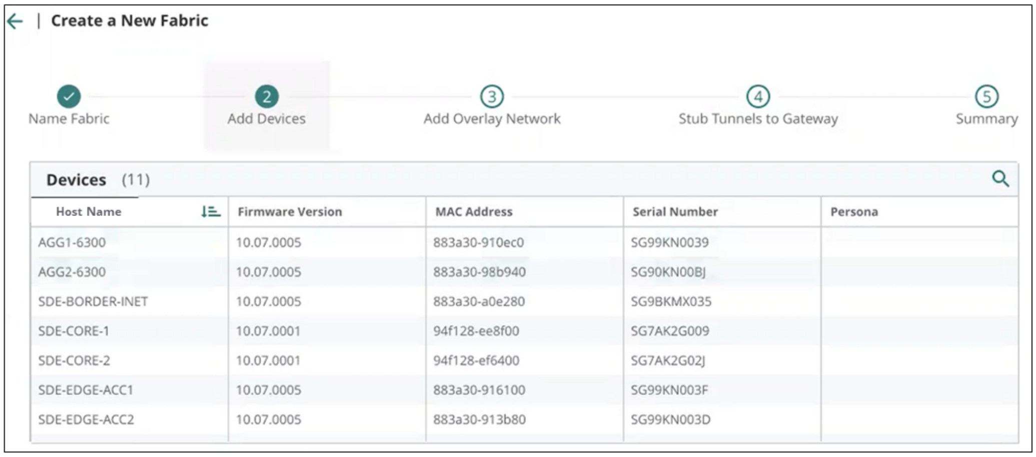
BGP AS Number
65001

4. In the **Fabric Name** field, enter a name.

The value in the **BGP AS Number** field is auto-generated. BGP AS Number can be modified, if necessary.

5. Click **Next**. The **Devices** table is displayed with a list of all the Switches in the network.
6. In the **Host Name** column, in the **Devices** table, select the devices that you want to assign to the Switches on the overlay network. The Assign selected device to window is displayed with a list of Switch personas.

Figure 9 *Create a New Fabric Page*



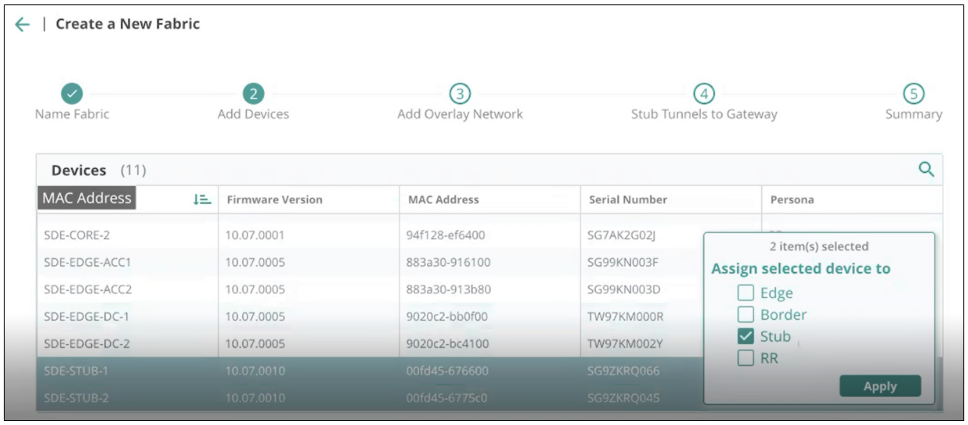
Devices (11)

Host Name	Firmware Version	MAC Address	Serial Number	Persona
AGG1-6300	10.07.0005	883a30-910ec0	SG99KN0039	
AGG2-6300	10.07.0005	883a30-98b940	SG90KN00BJ	
SDE-BORDER-INET	10.07.0005	883a30-a0e280	SG9BKMX035	
SDE-CORE-1	10.07.0001	94f128-ee8f00	SG7AK2G009	
SDE-CORE-2	10.07.0001	94f128-ef6400	SG7AK2G02J	
SDE-EDGE-ACC1	10.07.0005	883a30-916100	SG99KN003F	
SDE-EDGE-ACC2	10.07.0005	883a30-913b80	SG99KN003D	

Step 2: Assign Devices and Personas

To assign the selected devices to a fabric on the virtual network, complete the following steps:

1. In the **Assign selected device to** window, select the persona to which you want to assign the devices.



Create a New Fabric

Devices (11)

MAC Address	Firmware Version	MAC Address	Serial Number	Persona
SDE-CORE-2	10.07.0001	94f128-ef6400	SG7AK2G02J	
SDE-EDGE-ACC1	10.07.0005	883a30-916100	SG99KN003F	
SDE-EDGE-ACC2	10.07.0005	883a30-913b80	SG99KN003D	
SDE-EDGE-DC-1	10.07.0005	9020c2-bb0f00	TW97KM000R	
SDE-EDGE-DC-2	10.07.0005	9020c2-bc4100	TW97KM002Y	
SDE-STUB-1	10.07.0010	00fd45-676600	SG9ZKRQ066	
SDE-STUB-2	10.07.0010	00fd45-6775c0	SG9ZKRQ045	

2 item(s) selected

Assign selected device to

☐ Edge
☐ Border
☑ Stub
☐ RR

2. Click **Apply**.
3. Click **Next**. The **Overlay Networks** section is displayed.

NOTE

Personas under the VSX pair should be the same.

Step 3: Add the Overlay Network

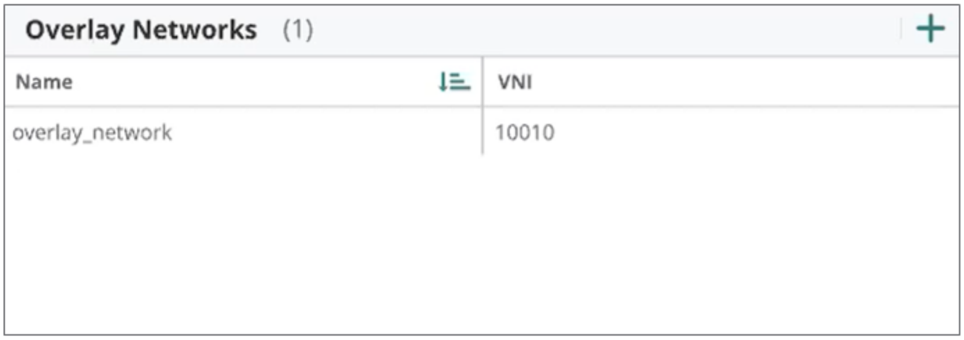
NOTE

A default overlay network is created automatically. You can create, move or delete an additional overlay network, if required.

To create an additional overlay network, complete the following steps:

1. In the **Overlay Networks** table, click the **+** icon.

   Figure 10 *Overlay Networks Table*



Overlay Networks (1)

Name	VNI
overlay_network	10010

2. In the **Name** field, enter a name for the overlay network.
3. In the **VNI** field, enter a virtual tunnel identifier.

NOTE

The VNI is auto-generated, but it can be modified if necessary.

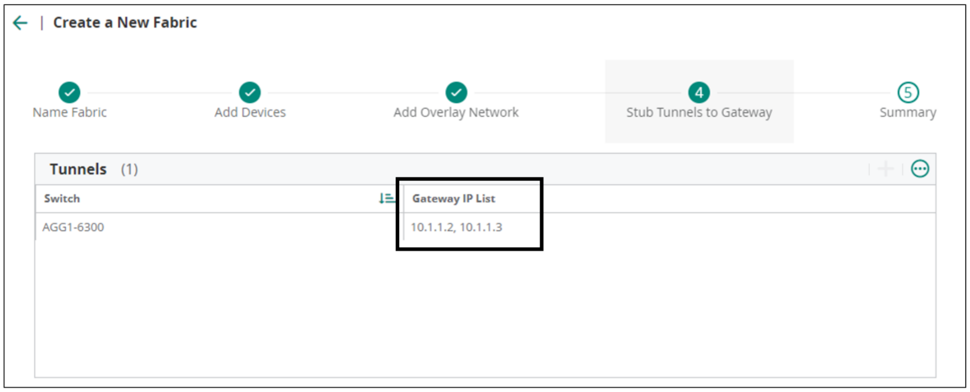
Step 4: Creating Static Tunnels from Stub VTEPs to a Gateway Cluster

To create a static tunnel from Stub VTEP to a Gateway cluster, complete the following steps:

1. In the **Tunnels** table, click the **+** icon.

   The list of Switches and Gateway IP addresses is displayed.

Figure 11 *Stub Tunnels to Gateways Section*



Create a New Fabric

Tunnels (1)

Switch	Gateway IP List
AGG1-6300	10.1.1.2, 10.1.1.3

2. Select a Switch from the **Switch** drop-down list.
3. In the **Gateway IP List** field, enter the IP address of the AOS 10 Gateway, which will be the tunnel termination point for the static VXLAN tunnel.

NOTE

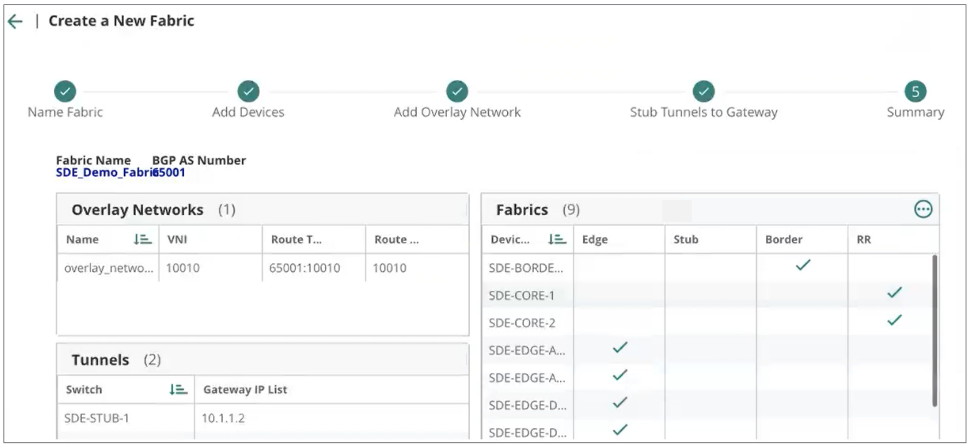
To input multiple values in the **Gateway IP List** parameter, use commas between the IP addresses. For example, 10.1.1.2, 10.1.1.3.

Step 5: View Fabric Summary

To view the fabric summary, complete the following steps:

1. In the **Stub Tunnels to Gateway** page, click **Next**. The **Summary** section is displayed.

Figure 12 *Create a New Fabric Section*



Create a New Fabric

Fabric Name SDE_Demo_Fabric

BGP AS Number 65001

Overlay Networks (1)

Name	VNI	Route T...	Route ...
overlay_netwo...	10010	65001:10010	10010

Tunnels (2)

Switch	Gateway IP List
SDE-STUB-1	10.1.1.2

Fabrics (9)

Devic...	Edge	Stub	Border	RR
SDE-BORDE...			✓	
SDE-CORE-1				✓
SDE-CORE-2				✓
SDE-EDGE-A...	✓			
SDE-EDGE-A...	✓			
SDE-EDGE-D...	✓			
SDE-EDGE-D...	✓			

2. In the **Summary** page, view the fabric summary and check the following:
   - Device personas are assigned correctly
   - Overlay networks are created properly
   - Stub tunnels to the Gateways are configured properly

Modifying an Overlay Network Fabric

To edit or modify a fabric, complete the following steps:

1. Hover over the tunnel row and click the ✎ edit icon.
2. Input the tunnel details.
3. Click **Save**.

   The overlay network fabric is saved.

Deleting an Overlay Network Fabric

To delete a fabric, click the 🗑 delete icon in the tunnel row.

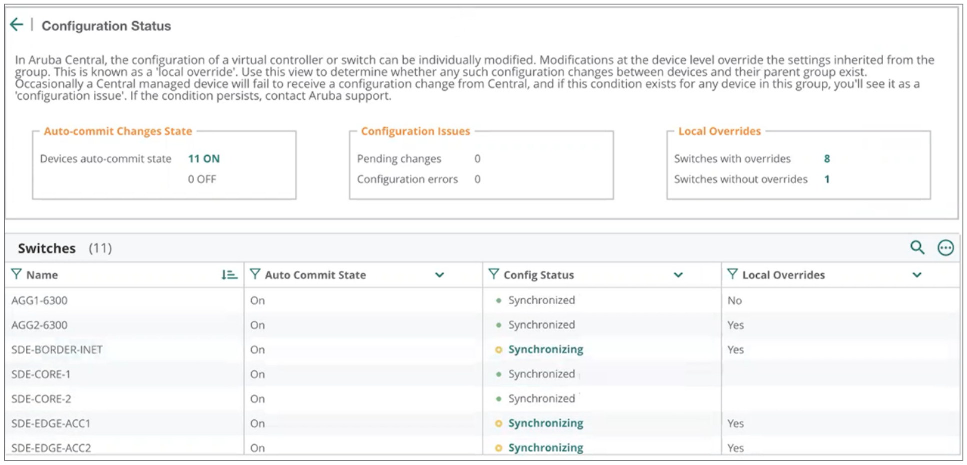
Viewing the Fabric Configuration Status

To view the fabric configuration status, complete the following steps:

1. Under **Switches**, click **Configuration Status**.

   The **Configuration Status** page is displayed.

   Configuration Status Page



← | Configuration Status

In Aruba Central, the configuration of a virtual controller or switch can be individually modified. Modifications at the device level override the settings inherited from the group. This is known as a 'local override'. Use this view to determine whether any such configuration changes between devices and their parent group exist. Occasionally a Central managed device will fail to receive a configuration change from Central, and if this condition exists for any device in this group, you'll see it as a 'configuration issue'. If the condition persists, contact Aruba support.

Auto-commit Changes State

Devices auto-commit state 11 ON
0 OFF

Configuration Issues

Pending changes 0

Configuration errors 0

Local Overrides

Switches with overrides 8

Switches without overrides 1

Switches (11)

Name	Auto Commit State	Config Status	Local Overrides
AGG1-6300	On	● Synchronized	No
AGG2-6300	On	● Synchronized	Yes
SDE-BORDER-INET	On	○ Synchronizing	Yes
SDE-CORE-1	On	● Synchronized	
SDE-CORE-2	On	● Synchronized	
SDE-EDGE-ACC1	On	○ Synchronizing	Yes
SDE-EDGE-ACC2	On	○ Synchronizing	Yes

2. In the **Config Status** column, you can view the configuration status of the overlay network fabric.

Overlay Segment

Overlay segment defines a broadcast domain. This maps the VLAN/VNI that will be deployed on the overlay network. You can define the VLAN ID, IP Subnet, default Gateway, DHCP relay server, and roles that can be present on this segment and define which devices this segment should be enabled on.

Configuring an Overlay Segment

The following workflow describes the steps for configuring overlay segments for the existing overlay fabrics in Aruba Central.

1. Step 1: Configure the Overlay Segment
2. Step 2: Assign Roles
3. Step 3: Select Edge and Stub Devices for the Overlay Segments
4. Step 4: View the Overlay Segment Summary

Step 1: Configure the Overlay Segment

To configure an overlay segment for the AOS-CX Switch, complete the following steps:

1. In the **Aruba Central** app, complete the following steps:
   - To select a group in the filter:
     a. Set the filter to a group.

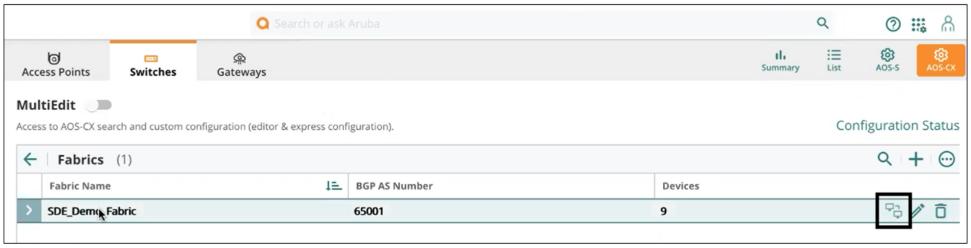
        The dashboard context for the group is displayed.

     b. Under **Manage**, click **Devices** > **Switches**.
     c. To view the AOS-CX Switch configuration dashboard, click the **AOS-CX** or **Config** icon.

2. Click **Routing** > **Fabrics**.

   A list of overlay fabrics is displayed in the **Fabrics** table.

3. In the **Fabrics** table, to select the row for the fabric, click the icon.



MultiEdit

Access to AOS-CX search and custom configuration (editor & express configuration).

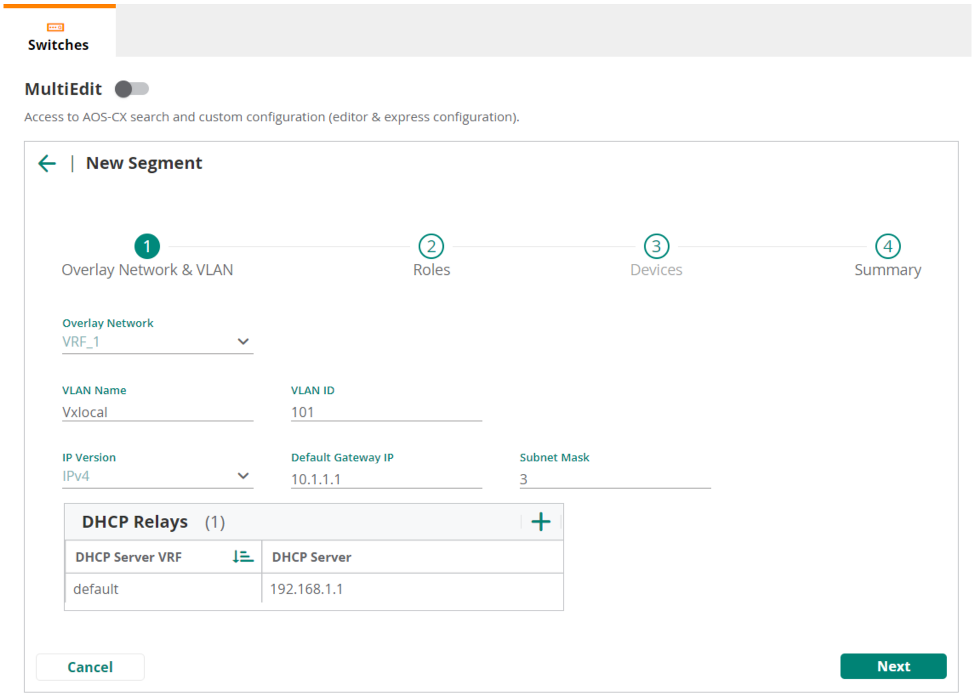
Configuration Status

Fabrics (1)

Fabric Name	BGP AS Number	Devices
SDE_Demo_Fabric	65001	9

The **Overlay Network & VLAN** section is displayed.

Figure 13 *Overlay Network & VLAN Page*



MultiEdit

Access to AOS-CX search and custom configuration (editor & express configuration).

New Segment

Overlay Network: VRF_1

VLAN Name: Vxlocal

VLAN ID: 101

IP Version: IPv4

Default Gateway IP: 10.1.1.1

Subnet Mask: 3

DHCP Relays (1)

DHCP Server VRF	DHCP Server
default	192.168.1.1

The following table describes the columns in the **Devices** table.

Table 7: *Overlay Network & VLAN Table Parameters*

Column	Function
Overlay Network	List of overlay networks. You can select the overlay network that you want to create the service segment for, from the list.
VLAN Name	Option to provide the VLAN name.
VLAN ID	The VLAN ID number.
IP Version	Option to select the IP version. ■ IPv4 ■ IPv6 ■ Dual Stack
Default Gateway IP	Option to define the default Gateway IP for the overlay network.
Subnet Mask	Option to provide the subnet mask for the IP address.
DHCP Server VRF	The default DHCP server VRF value or you can add manually. **Note:** You can manually add multiple DHCP server relays.
DHCP Server	The IP address of the DHCP relay server.

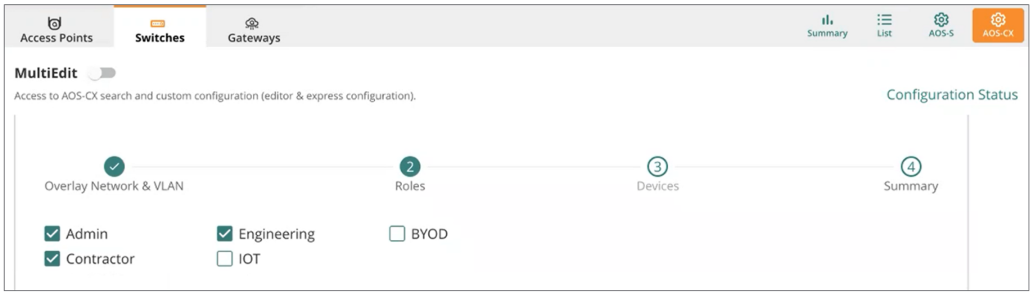
4. In the **Overlay Network & VLAN** table, provide all the details.
5. Click **Next**. The **Roles** section is displayed with a list of all the global roles defined on the **Client Roles** page.

Step 2: Assign Roles

This section indicates the roles that can be assigned to endpoints or users that are part of this segment.

To assign roles that you want to allow to participate in the overlay network segment, complete the following steps:

Figure 14 *Roles Page*



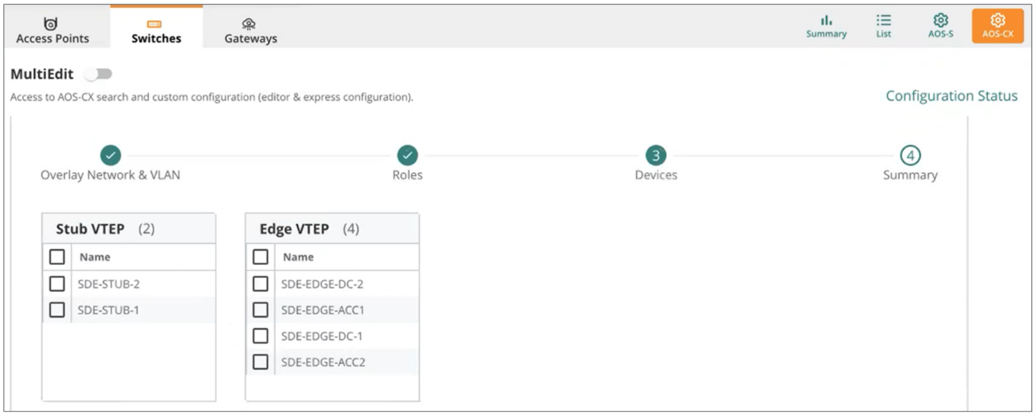
☑ Admin
☑ Contractor
☑ Engineering
☐ IOT
☐ BYOD

1. Select the roles which you want to allow to participate in the overlay network segment.
2. Click **Next**. The **Devices** section is displayed.

Step 3: Select Edge and Stub Devices for the Overlay Segments

In the **Devices** section, select the devices which you want to apply on the segment. You can either select individual devices or select all the devices and attach to the overlay fabric.

Figure 15 *Devices Page*



MultiEdit

Access to AOS-CX search and custom configuration (editor & express configuration).

Stub VTEP (2)
□ Name
□ SDE-STUB-2
□ SDE-STUB-1

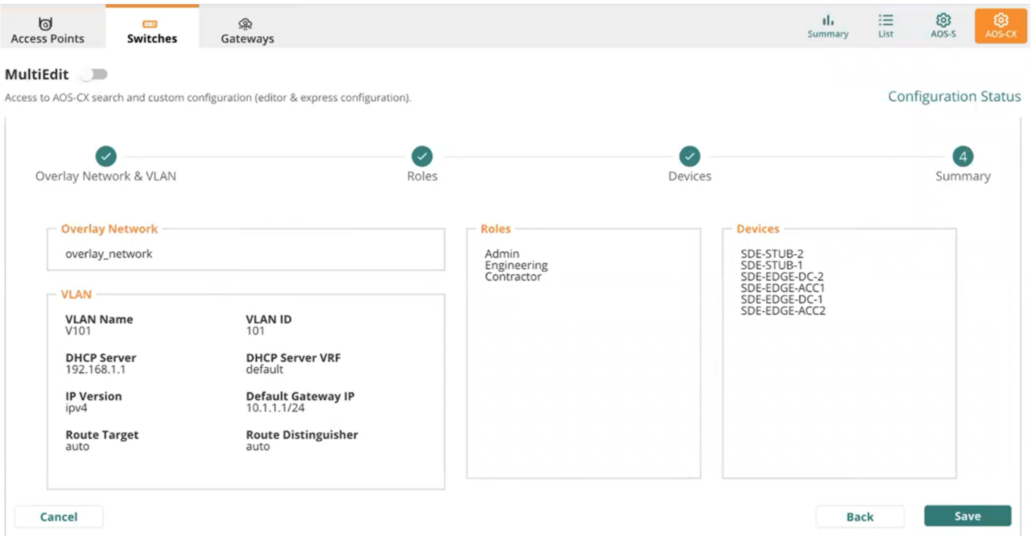
Edge VTEP (4)
□ Name
□ SDE-EDGE-DC-2
□ SDE-EDGE-ACC1
□ SDE-EDGE-DC-1
□ SDE-EDGE-ACC2

Step 4: View the Overlay Segment Summary

To view the overlay segment summary, complete the following steps:

In the **Devices** section, click **Next**. The **Summary** section is displayed where you can view the summary of your configuration.

Figure 16 *Summary Page*



MultiEdit

Access to AOS-CX search and custom configuration (editor & express configuration).

Overlay Network

overlay_network

VLAN

VLAN Name
V101

VLAN ID
101

DHCP Server
192.168.1.1

DHCP Server VRF
default

IP Version
ipv4

Default Gateway IP
10.1.1.1/24

Route Target
auto

Route Distinguisher
auto

Roles

Admin
Engineering
Contractor

Devices

SDE-STUB-2
SDE-STUB-1
SDE-EDGE-DC-2
SDE-EDGE-ACC1
SDE-EDGE-DC-1
SDE-EDGE-ACC2

Viewing the Overlay Fabric

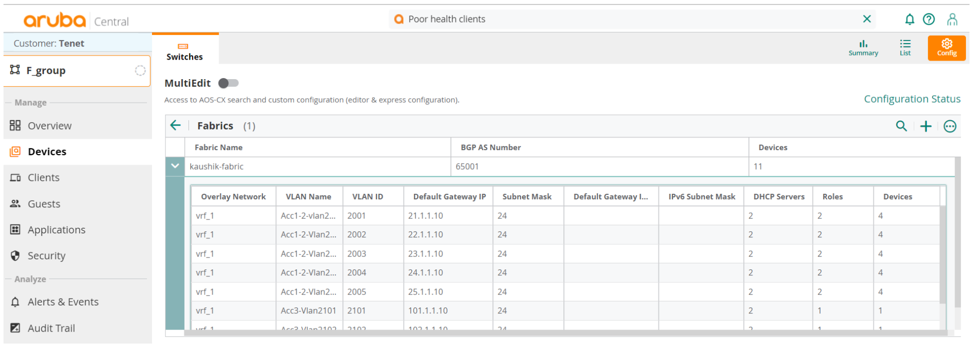
To view the newly created overlay fabric or view an existing fabric, complete the following steps:

1. In the overlay segment row, click the ⌄ arrow down icon to expand the fabric.
2. View the overlay segment.

The following table describes the columns in the **Fabrics** table.

Table 8: *Overlay Segment Table Parameters*

Column	Function
Overlay Network	List of overlay networks.
VLAN Name	The VLAN name.
VLAN ID	The VLAN ID number.
IP Version	The IP version. ■ IPv4 ■ IPv6 ■ Dual Stack
Default Gateway IP	The default Gateway IP for the overlay network.
Subnet Mask	The subnet mask for the IP address.
DHCP Server VRF	The default DHCP server VRF value or you can add manually. **Note:** You can manually add multiple DHCP server relays.
DHCP Server	The IP address of the DHCP relay server.
Roles	The number of roles assigned to this network. **NOTE:** When you delete a role in the **Clients Role** page. The number of updated role is not reflected in this column, unless you edit the overlay segment.
Devices	The number of devices assigned to this network.



MultiEdit

Access to AOS-CX search and custom configuration (editor & express configuration).

Configuration Status

Fabrics (1)

Fabric Name	BGP AS Number	Devices
kaushik-fabric	65001	11

Overlay Network	VLAN Name	VLAN ID	Default Gateway IP	Subnet Mask	Default Gateway I...	IPv6 Subnet Mask	DHCP Servers	Roles	Devices
vrf_1	Acc1-2-vlan2...	2001	21.1.1.10	24			2	2	4
vrf_1	Acc1-2-Vlan2...	2002	22.1.1.10	24			2	2	4
vrf_1	Acc1-2-Vlan2...	2003	23.1.1.10	24			2	2	4
vrf_1	Acc1-2-Vlan2...	2004	24.1.1.10	24			2	2	4
vrf_1	Acc1-2-Vlan2...	2005	25.1.1.10	24			2	2	4
vrf_1	Acc3-Vlan2101	2101	101.1.1.10	24			2	1	1
vrf_1	Acc3-Vlan2102	2102	102.1.1.10	24			2	1	1

Modifying the Overlay Segment

To edit or modify an overlay fabric, complete the following steps:

1. In the overlay segment row, click the ✎ edit icon and provide the required details.
2. Click **Save**.

   The overlay segment is saved.

Deleting the Overlay Segment

To delete an overlay segment, click the 🗑 delete icon in the overlay segment row.

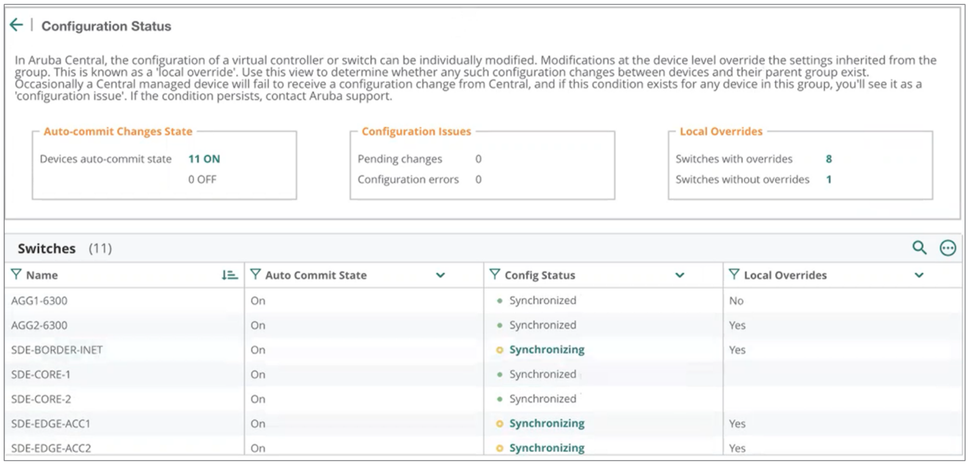
Viewing the Configuration Status

To view the configuration status, complete the following steps:

1. Under **Switches**, click **Fabrics** > **Configuration Status**.

   The **Configuration Status** page is displayed.

   Figure 17 *Configuration Status Page*



Configuration Status

In Aruba Central, the configuration of a virtual controller or switch can be individually modified. Modifications at the device level override the settings inherited from the group. This is known as a 'local override'. Use this view to determine whether any such configuration changes between devices and their parent group exist. Occasionally a Central managed device will fail to receive a configuration change from Central, and if this condition exists for any device in this group, you'll see it as a 'configuration issue'. If the condition persists, contact Aruba support.

Auto-commit Changes State

Devices auto-commit state: 11 ON, 0 OFF

Configuration Issues

Pending changes: 0

Configuration errors: 0

Local Overrides

Switches with overrides: 8

Switches without overrides: 1

Switches (11)

Name	Auto Commit State	Config Status	Local Overrides
AGG1-6300	On	● Synchronized	No
AGG2-6300	On	● Synchronized	Yes
SDE-BORDER-INET	On	○ Synchronizing	Yes
SDE-CORE-1	On	● Synchronized	
SDE-CORE-2	On	● Synchronized	
SDE-EDGE-ACC1	On	○ Synchronizing	Yes
SDE-EDGE-ACC2	On	○ Synchronizing	Yes

2. In the **Config Status** column, you can view the Switch synchronization status.

Chapter 8

Static VXLAN Tunnels on AOS 10 Gateways

Aruba Central allows you to configure a static VXLAN tunnel on Gateways.

Prerequisites

The following prerequisites must be fulfilled to configure static VXLAN tunnels:

- AOS 10 Gateways are configured as Mobility Gateways.
- Gateway Cluster is enabled on Aruba Central.
- The **Role-to-Role Policy Enforcement** toggle must be defined on the **Client Roles** page to enable the global role policies.
- The **Use a switch fabric for a role propagation?** option must be set to **Yes** on the **Client Roles** page to enforce the global role policies on the Switch fabric.

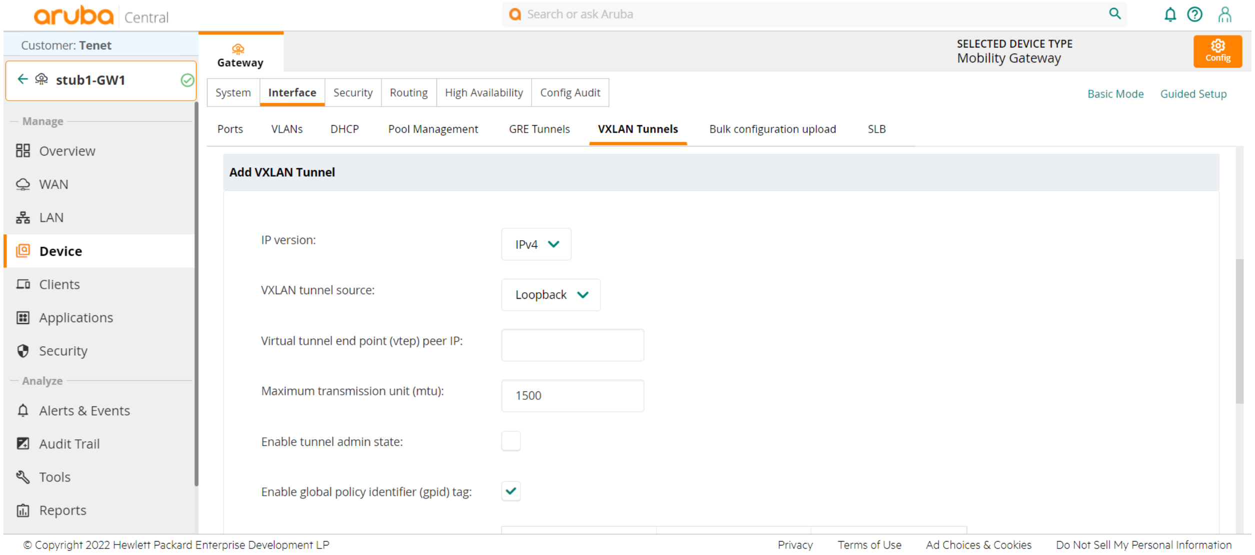
Configuring a Static VXLAN Tunnel on Gateways

To configure a static VXLAN tunnel on a Gateway or VPNC group, complete the following steps:

1. In the **Aruba Central** app, complete the following steps:
    a. Set the filter to a group containing at least one Branch Gateway.
    b. Under **Manage**, click **Devices > Gateways**.
    c. Click **Config**.
2. If you are in the **Basic Mode**, click **Advanced Mode** to access the advanced configuration options.
3. Click **Interface** > **VXLAN Tunnels**. The **VXLAN Tunnels** page is displayed.
4. In the **VXLAN Tunnels** pane, click the **+** icon.

    The **Add VXLAN Tunnel** pane is displayed.

Figure 18 *Add VXLAN Tunnel Page*



Add VXLAN Tunnel

IP version: IPv4

VXLAN tunnel source: Loopback

Virtual tunnel end point (vtep) peer IP:

Maximum transmission unit (mtu): 1500

Enable tunnel admin state: □

Enable global policy identifier (gpid) tag: ☑

The following table describes the parameters in the **Add VXLAN Tunnel** table:

Table 9: *Add VXLAN Tunnel Parameters*

Parameter	Description
IP Version	Select one of the IP versions for the Aruba Gateways, to select the system IP address.
VXLAN tunnel source	Select one of the following VXLAN tunnel sources for the Aruba Gateways, to select the system IP address: ■ **System IP**—Enables the system IP as your tunnel source. ■ **Loopback**—Selecting this option automatically fetches the cluster loopback and the cluster system IPs as your tunnel source. ■ **VLAN**—Selecting this option allows you to choose an L3 VLAN that is configured on the Gateway as your tunnel source. ■ **Static IP**—Selecting this option allows you to input a source IP address.
Source IP address	This field allows you to add the source IP address. This field appears when the **Static IP** option is selected in the **VXLAN Tunnel Source** drop-down.
VLAN interface	This field displays the auto-populated list of L3 VLANs.
Virtual Tunnel End Point (VTEP) peer IP	This is the VTEP peer IP address. For a standalone Switch, this can be the loopback 1 IP address of the Switch. If the peer is a VSX pair, use the logical VTEP IP address of the VSX pair.
Maximum transmission unit (MTU)	Provides the MTU setting for the VXLAN. The value should between 1024 to 9198 to avoid fragmentation within the fabric. **NOTE:** Enable the **Jumbo Frames Processing** toggle at **Devices > Gateways > Security > Firewall** and check the **Jumbo MTU** box at **Devices > Gateways > Interface > Ports**.
Enable tunnel admin state	Select this option to enable the admin state of the VXLAN interface.

Parameter	Description
Enable Global Policy Identifier (GPID) tag	Select this option to enable the GPID tag. This is the GPID that is propagated across the network.

5. In the **Add VXLAN Tunnel** pane, configure the VXLAN parameters as described in the Add VXLAN Tunnel Parameters table based on your network requirements.

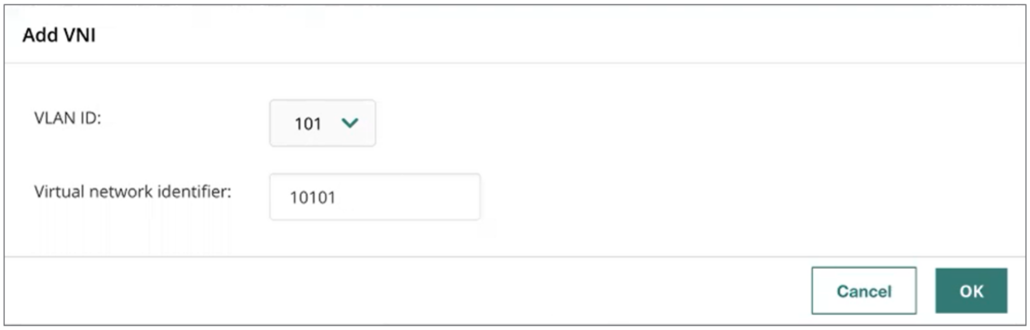
Mapping VLAN and VNI to a VXLAN Tunnel

To map the VLAN and VNI to the VXLAN tunnel, complete the following steps:

1. In the **VLAN/VNI mappings** page, click the **+** icon.

   The **Add VNI** table is displayed.

   Figure 19 *Add VNI table*



Add VNI

VLAN ID: 101

Virtual network identifier: 10101

The following table describes the parameters in the **Add VNI** table:

Table 10: *Add VNI Tab Parameters*

Parameter	Description
VLAN ID	Select a VLAN ID from the list, to on-board the VLAN to the VXLAN tunnel. **Example:** 101, 102, and 103.
Virtual network identifier	VNI is auto-generated. For auto-generation of VNI, 1000 is added to the VLAN ID. **Example:** If the VLAN ID is 101, the VNI is auto-generated as 10101.

2. In the drop-down list, select the **VLAN ID** to on-board the VLAN to the VXLAN tunnel.
3. Click **OK**.
4. Click **Save Settings**.

Chapter 9

Example Use Case

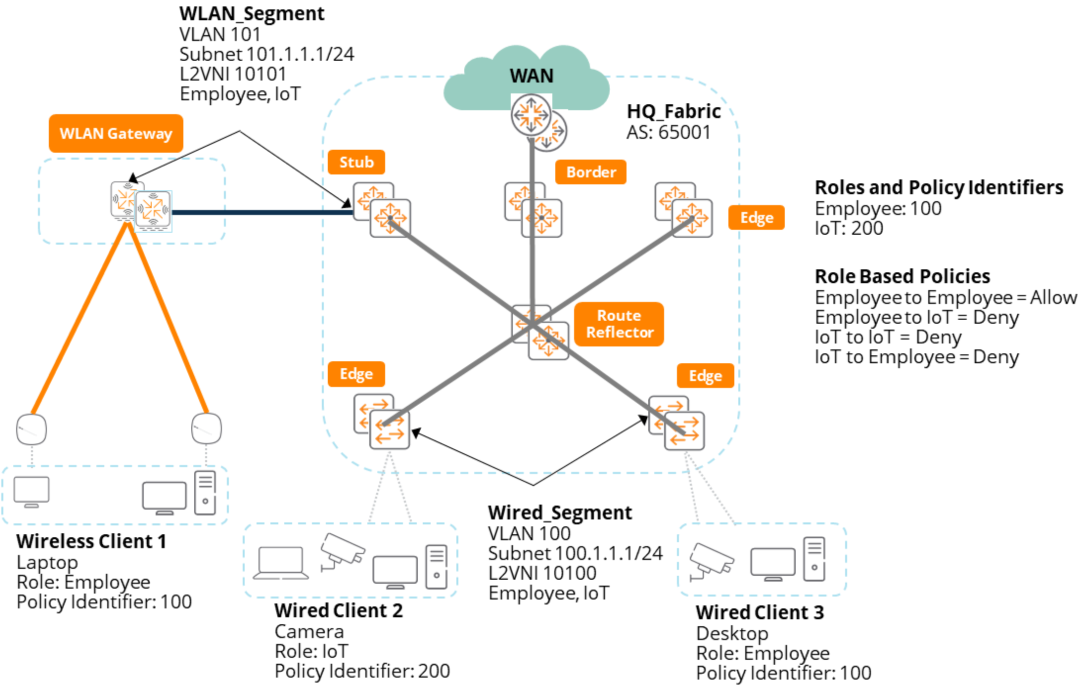
This section describes example use cases for the following deployments:

1. Distributed Campus-wide Fabric
2. Centralized Multi-site Fabric with Aruba SD-Branch
3. Centralized Multi-site Fabric with Third-Party SD-WAN

Distributed Campus-wide Fabric

This section describes an example use case for the Distributed Campus-wide Fabric deployment using Aruba Central.

Figure 20 *Distributed Campus-wide Fabric Use Case*



In the use case, the goal is to enable role-based micro-segmentation across all wired and wireless clients in an enterprise campus. Roles and role-based policies are orchestrated centrally from the **Client Roles** page on Aruba Central. These policies are enforced on the edge VTEPs in a distributed EVPN fabric for wired clients and on the WLAN gateways for wireless clients. The VXLAN-EVPN fabric is provisioned on the AOS-CX switches using the Fabric Provisioning Wizard on Aruba Central.

As depicted in the above diagram, wired and wireless clients that are assigned the employee role are allowed to communicate with other clients with the Employee role, but not to the clients with the IoT role. Conversely, clients with the IoT role are denied access to clients of both the IoT and employee role.

Step 1: Creating the Role and Role-based Policy

The roles and role-based policies are defined in the **Client Roles** page on Aruba Central. In the **Client Roles** page, the Employee role is created with a policy Identifier 100 and the IoT role is created with a Policy Identifier of 200.

Policies for these roles are defined next. The permission for the Employee role is assigned to allow source to destination. This allows communication between the clients with the Employee role. By default, all other role-based communication is denied.

After the permissions are assigned, this role and policy definition is configured on all gateways and switches on the network.

For more information about how to create role and role-based policy using Aruba Central, refer to Global Client Roles.

Step 2: Creating the Overlay Fabric

The next step is to provision an EVPN-VXLAN fabric on the AOS-CX switches to enable propagation of roles across the network and enforce role-based policies for wired clients. In the **Create a New Fabric** page, a new fabric with the name HQ_Fabric is created with BGP AS 65001, which is auto-populated by Aruba Central. After the fabric is created, the configurations for the EVPN-VXLAN fabric and static VXLAN tunnels are pushed to the AOS-CX devices.

For more information about how to create fabric using Aruba Central, refer to Fabric Provisioning Wizard.

Step 3: Creating the Wired and Wireless Segment

The Segment Creation wizard is used to create a wired segment and apply the segment to all the Edge VTEPs in a fabric. A segment is created with the name Wired_Segment, VLAN ID 100, and Default Gateway IP of 100.1.1.1/24. The L2VNI of 10100 is auto-assigned to the segment by Aruba Central. The Employee and IoT role is assigned to the segment and applied to all the wired Edge VTEPs in the fabric.

Similarly, a wireless segment is created and applied to the Stub VTEPs that connect to the WLAN gateways in the network. This segment has a name Wireless_Segment, VLAN ID 101 and Default Gateway IP of 101.1.1.1/24. The Employee and IoT role is also assigned to the segment and applied to all the Stub VTEPs in the fabric.

For more information about how to create wired and wireless segment using Aruba Central, refer to Fabric Provisioning Wizard.

Step 4: Creating Static VXLAN Tunnel on the Gateway

The final step is to create the static VXLAN tunnel on the WLAN gateway. Using the VXLAN Tunnel UI Configuration, a VXLAN tunnel is created using the System IPs of the cluster as the tunnel source and the VTEP IP of the AOS-CX switches as the tunnel peer. The VLAN ID 101 is added to the tunnel to map to the Wireless Segment created on the Stub VTEPs. The tunnel is enabled and GBP role propagation is also enabled on the tunnel. After the mapping is completed, the configurations for the static VXLAN tunnel are pushed to the WLAN gateway.

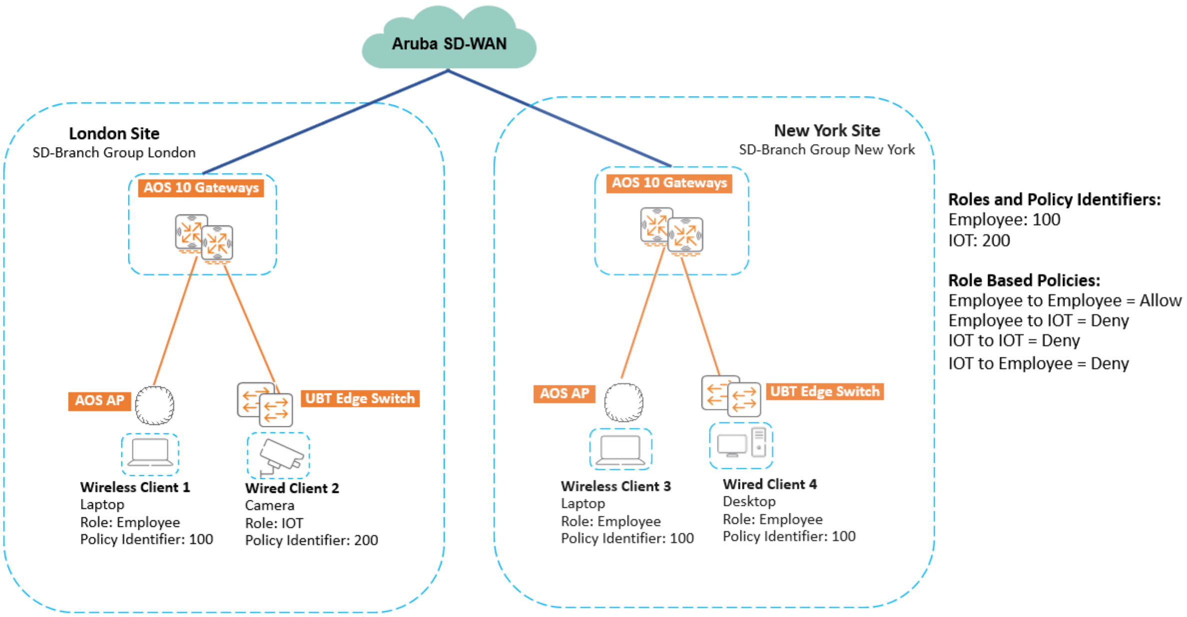
For more information about how to create static VXLAN tunnel on the WLAN gateway using Aruba Central, refer to Static VXLAN Tunnels on AOS 10 Gateways.

Upon successful configuration, role-based policies are enforced across all clients in the network. In the example above, Wireless Client 1 which is authenticated with the role Employee communicates with the Wired Client 3 with role Employee but is denied communication with the Wired Client 2 with role IoT. Similarly, the Wired Client 2 cannot communicate with either Wireless Client 1 or Wired Client 3.

Centralized Multi-site Fabric with Aruba SD-Branch

This section describes an example use case for the Centralized Multi-site Fabric with Aruba SD-Branch deployment using Aruba Central.

Figure 21 *Centralized Multi-site Fabric with Aruba SD-Branch Use case*



The SD-Branch group London maps to the London site and the SD-Branch group New York maps to the New York site. The goal is to enable role-based micro-segmentation across multiple geographic sites connected over an Aruba SD-WAN fabric. Roles and role-based policies are centrally in the **Client Roles** page on Aruba Central. The AOS 10 Gateway is the WLAN gateway for the wireless clients and user-based tunnel Gateway for the wired clients within the site. The role-based policies are enforced on the AOS 10 Gateways for all the clients within the site. Role propagation and role-based policy enforcement is selectively enabled per groups.

As depicted in the above diagram, wired and wireless clients that are assigned the Employee role is allowed to communicate with other clients with the Employee role, but not to the clients with the IoT role. Conversely, clients with the IoT role are denied access to clients of both the IoT and Employee role.

Step 1: Creating Role and Role-based Policy

The roles and role-based policies are defined on the **Client Roles** page on Aruba Central. In the **Client Roles** page, the Employee role is created with a Policy Identifier 100 and the IoT role is created with a Policy Identifier of 200.

Policies for these roles are defined. The permission for the Employee role is assigned to allow source to destination. This allows communication only between the clients with the Employee role. By default, all other role-based communication to the

After the permissions are assigned, the same role and policy definition is configured on all gateways and switches on the network.

For more information about how to create role and role-based policy using Aruba Central, refer to Global Client Roles.

Step 2: Selective Enablement of Groups

The next step is to selectively enable the groups that maps to the respective sites. In the **Client Roles** page, select **No** for **Use a switch fabric for a role propagation?** option, and select the **Branch** option. The respective groups are configured to enable role propagation and role-based policy enforcement for those sites.

For more information about how to selectively enable groups for multi-site using Aruba Central, refer to Selective Enablement of Groups.

After successfully applying the configuration, role-based policies are enforced on all clients in the network.

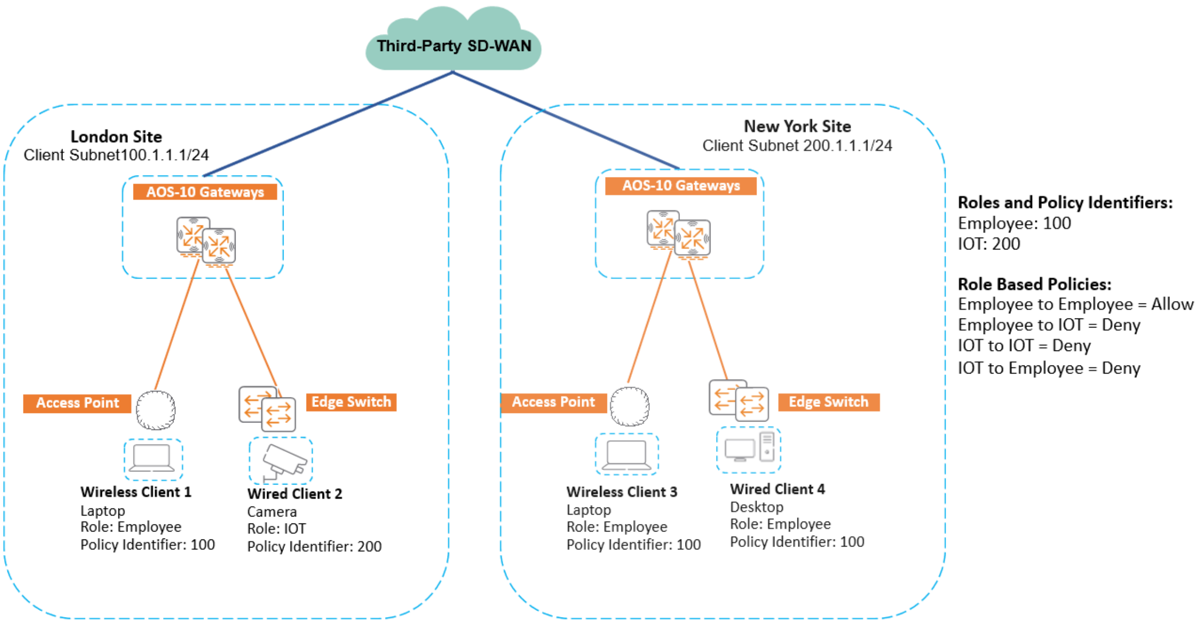
In the above example:

- Wireless Client 1 in the London site, which is authenticated with the role Employee communicates with Wired Client 3 with the role Employee in the New York site, but is denied communication with Wired Client 2 with the role IoT, although it is in the same site and group.
- Similarly, Wired Client 2 cannot communicate with either Wireless Client 1 or Wired Client 3.

Centralized Multi-site Fabric with Third-Party SD-WAN

This section describes an example use case for the Centralized Multi-site Fabric with Third-Party SD-WAN deployment using Aruba Central.

Figure 22 *Centralized Multi-site Fabric with Third-Party SD-WAN Use Case*



In the use case, the client subnet 100.1.1.1/24 maps to clients in the London site and the client subnet 200.1.1.1/24 maps to clients in the New York site. The goal is to enable role-based micro-segmentation across multiple geographic sites connected over a Third-Party SD-WAN fabric. Roles and role-based policies are centrally in the **Client Roles**page on Aruba Central. The third-party gateway is the WLAN gateway for the wireless clients and user-based tunnel Gateway for the wired clients within the site. The role-based policies are enforced on the Third-Party Gateways for all the clients within the site. Role propagation and role-based policy enforcement is selectively enabled per subnets.

As depicted in the above diagram, wired and wireless clients that are assigned the Employee role is allowed to communicate with other clients with the Employee role, but not to the clients with the IoT role. Conversely, clients with the IoT role are denied access to clients of both the IoT and Employee role.

Step 1: Creating Role and Role-based Policy

The roles and role-based policies are defined on the **Client Roles** page on Aruba Central. In the **Client Roles** page, the Employee role is created with a Policy Identifier 100 and the IoT role is created with a Policy Identifier of 200.

Policies for these roles are defined. The permission for the Employee role is assigned to allow source to destination. This allows communication between the clients with the Employee role. By default, all other role-based communication is denied.

After the permissions are assigned, the same role and policy definition is configured on all gateways and switches on the network.

For more information about how to create role and role-based policy using Aruba Central, refer to Global Client Roles.

Step 2: Selective Enablement of Subnets

The next step is to selectively enable the subnets that maps to the clients in the respective sites. In the **Client Roles** page, select **No** for **Use a switch fabric for a role propagation?** option, and select the **Mobility** option. The respective client subnets are configured to enable role propagation and role-based policy enforcement for those sites.

For more information about how to selectively enable subnets for multi-site using Aruba Central, refer to Selective Enablement of Subnets.

After successfully applying the configuration, role-based policies are enforced on all clients in the network.

In the above example:

- Wireless Client 1 in the London site, which is authenticated with the role Employee communicates with Wired Client 3 with the role Employee in the New York site, but is denied communication with Wired Client 2 with the role IoT, although it is in the same site and subnet.
- Similarly, Wired Client 2 cannot communicate with either Wireless Client 1 or Wired Client 3.