

## TECH BRIEF

# SEAMLESS SD-WAN ORCHESTRATION

A simplified model using Aruba Central

## INTRODUCTION

SD-WAN inherently addresses many of the configuration issues in operating a large distributed network. It utilizes transport independent overlay tunnels and centralized traffic routing, based on policies that take into account both user and application roles. This alone simplifies WAN management.

But as distributed networks may handle tens of thousands of users and devices across a large number of locations, it can still be very complex to manually configure tunnels and routing tables. This can be further complicated for networks that include a disparate set of networking equipment at the branches.

Administrators need a way to simplify the process and make it less error-prone. To assist in this, Aruba Central, a highly scalable cloud-native management system, includes an SD-WAN Orchestrator. This allows IT to quickly and efficiently set up routes and tunnels—based on business policy—across the entire organization: branch offices, headquarters, enterprise data centers, and even virtual private clouds (VPC) inside providers such as Amazon Web Services (AWS) or Microsoft Azure.

## ABOUT THE ARUBA SD-WAN ORCHESTRATOR

The Aruba SD-WAN Orchestrator is based on a cloud-native, multi-tenant control plane which scales in line with customer growth. Competing orchestrators are virtual machine (VM)-based control plane elements that must be scaled manually as requirements grow and exceed the limitations of the VMs.

The benefit of the SD-WAN Orchestrator is that WAN links are automatically discovered and tunnels are orchestrated based on business and topological needs, such as mapping data centers to branch offices. The Orchestrator only sets up tunnels between sites that need them. Similarly, routes are only advertised between gateways that have reachability between each other.

## KEY BENEFITS

- Major administrative cost savings for distributed enterprises
- Greatly simplified management of wide area networks
- Flexible topology choices include hub and spoke and full mesh
- Rapid establishment of any-any connectivity based on business intent
- Any combination of uplink types across the SD-WAN fabric
- Cloud-native, multitenant control plane scales in line with customer growth
- Removes need to manually setup VPN tunnels or routes between sites

Customers no longer have to set up individual overlay tunnels or configure independent routing policies per device. Figure 1 provides a simplified example.

In this example, the branch gateways have multiple uplink types, including two different carrier MPLS offerings as well as Internet access (either wired or via LTE). You can imagine that with hundreds or thousands of branches, or multiple data centers and perhaps one or more VPCs, configuring routing paths can get very complex. For instance, you would need to know IP addresses, interface names, link types, etc.

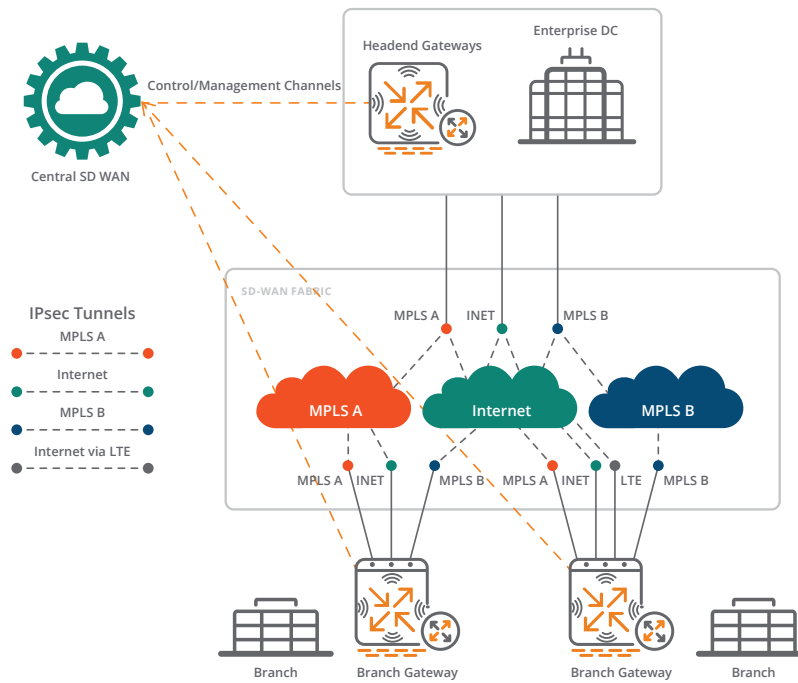


Figure 1: Defining Tunnels and Routes for Branches and Head Ends

### Topology Options

The orchestrator provides a number of flexible choices for the SD-WAN overlay topology based on business connectivity needs. The following topology options apply to all nodes in the fabric:

- Hub and Spoke: all branches are connected to their respective hubs in the priority order
- Full Mesh: Full mesh of tunnels to every node, all sites connected to all other sites

These options are easily selected in the Overlay Orchestrator (Figure 2).

You can also set graceful restart times and tunnel rekey timers according to your site security standards.

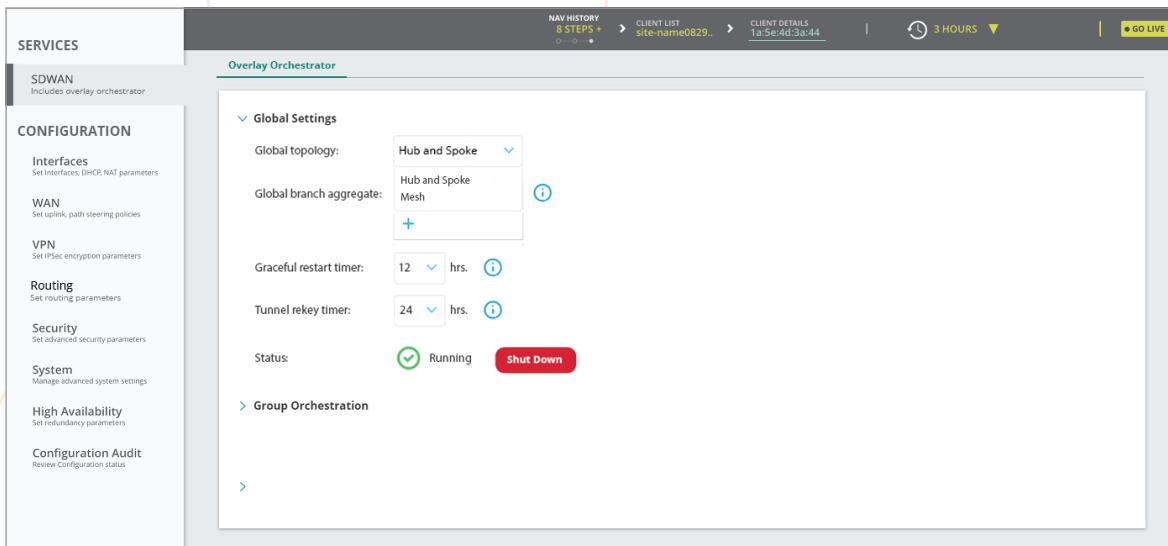


Figure 2: Overlay Orchestrator Dropdown Menu



### Group Level Orchestration Policies

For large deployments, the network is typically grouped into hierarchy of sites based on the region. You will most often set the different topologies for different regions using group level policies. In this case (Figure 3), choices could be made at a per-group level to select the overlay topology.

The hub and the branch groups in different regions are shown with the number of sites. Each region can have its own topology depending on the connectivity needs.

### Orchestrated Setup of Routing, Tunnels and Key Exchanges

To greatly simplify this process, the SD-WAN Orchestrator manages all interfaces in the WAN, including both their public and private IP addresses. It then automatically sets up tunnels, for example between Carrier A's branch and headend MPLS Interfaces. For optimizing the traffic flows, the orchestrator will also attempt to stay within the same carriers on Internet circuits.

Branch Gateways (BGWs) establish secure Internet Protocol security (IPsec) over the Internet or other untrusted networks to other gateways. To manage the keys for the VPN tunnels, Aruba Central orchestrates tunnel setup centralized key management, handling both key exchange and key rotation. IT only needs to provide the overlay topology and the list of hubs in the preferred order.

Routing policy is also centralized, based on the overlay topology provided. Routes are automatically distributed from the orchestrator, along with the associated affinity.

The following are automation assists in the orchestration process:

- Discovering public/private IP addresses
- Exchanging keys
- Building tunnels
- Learning routes from hub/branch sites
- Advertising routes across the WAN with appropriate costs, and
- Redistributing routes on the LAN side with appropriate costs.

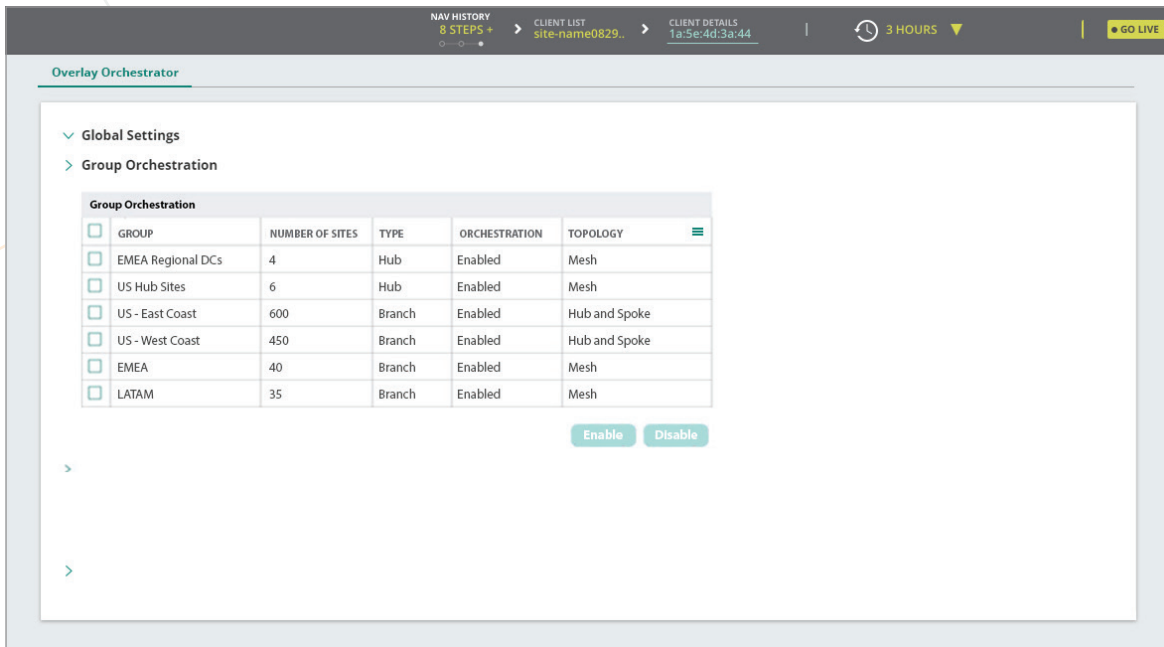


Figure 3: Group Orchestration



### EXAMPLES: ORCHESTRATING AN SD-WAN OVERLAY NETWORK

In this example (Figure 4), we're showing a global network with a single branch (one of possibly many), which may connect into any of multiple data centers or cloud provider endpoints.

Orchestration of the needed paths for this network is very simple. Aruba Central provides a simplified view of the connectivity and status to each of your corporate and cloud data centers. From this view, you can quickly “double click” to gain better visibility into each of the tunnels, WAN links, branches, and Aruba headend and virtual gateways.

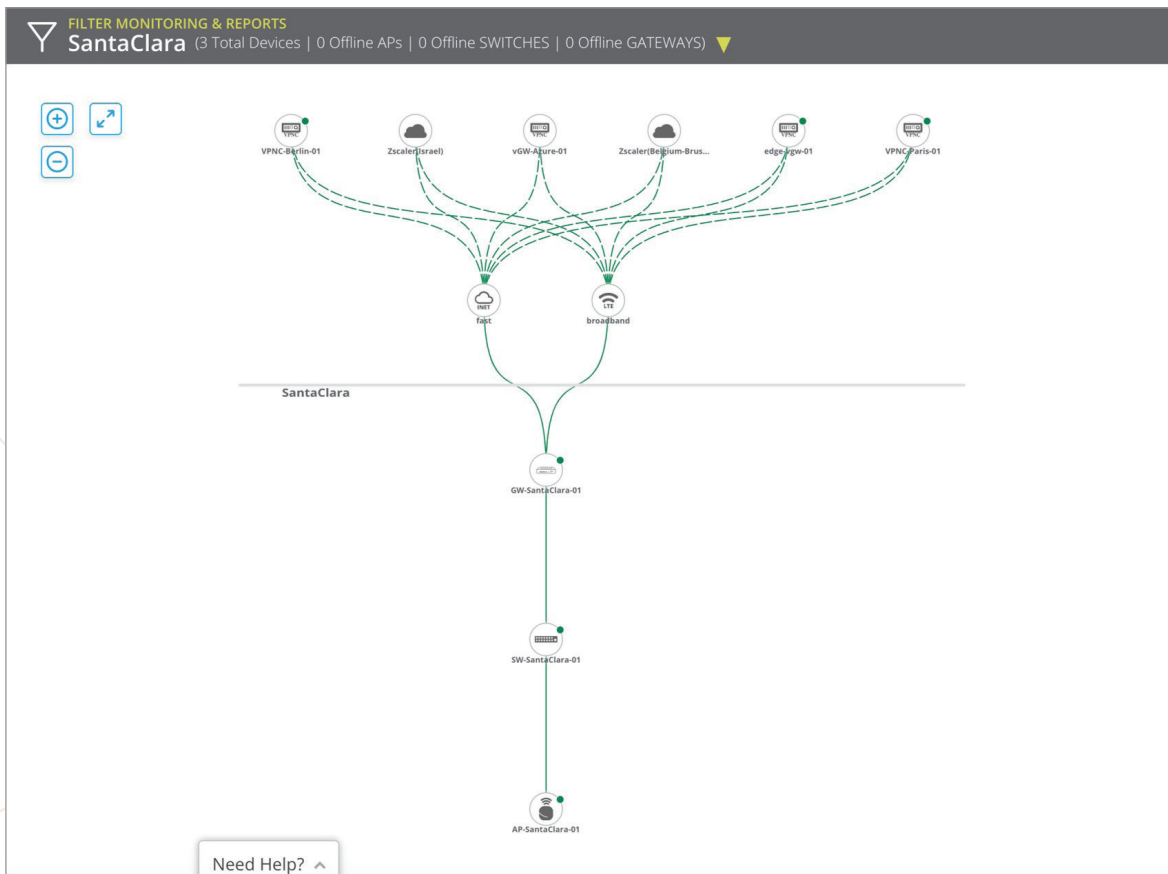


Figure 4: Topology View of Global Network from Branch Office View

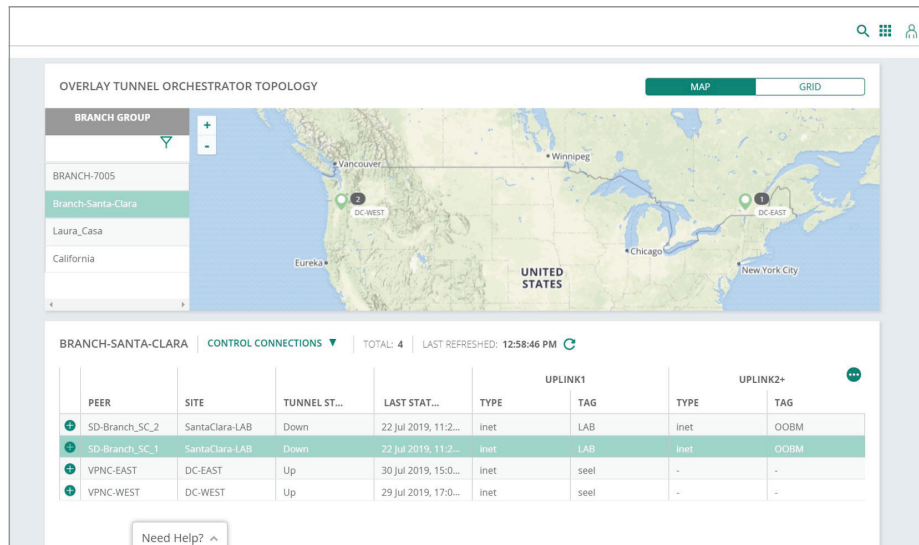


Figure 5: Tunnel Orchestrator's Control Connections for a Selected Branch Group

### Tunnel Orchestration

As the administrator, you can divide the network into multiple groups. This allows you to more easily establish and view specific portions of the network as needed. When you then select a branch group, you can look at specific headend gateways (virtual or physical) that the branch can connect to. At that point, you select which sites need tunnel connections: this is effectively "intent-based configuration" as the Orchestrator takes care of actually establishing the tunnels.

By logically partitioning branch sites into groups, you can easily configure group-based policies and monitor the network at an easily-managed level of abstraction. For

example, Figure 5 illustrates how the administrator can monitor the connections between branch gateways and the SD-WAN Orchestrator.

The administrator can thus view all of the tunnels being established for the North America group.

In the image below, Figure 6 shows a list of all the IPsec tunnels that are orchestrated for the selected branches.

The tunnels are automatically established based on the preconfigured policies.

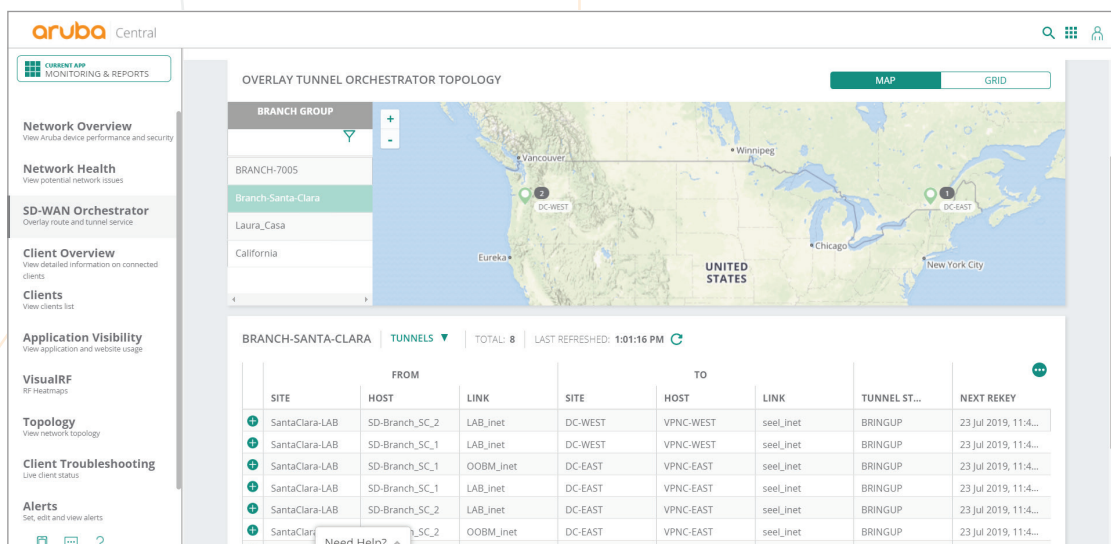


Figure 6: Tunnels from Branches to Headends are Automatically Established

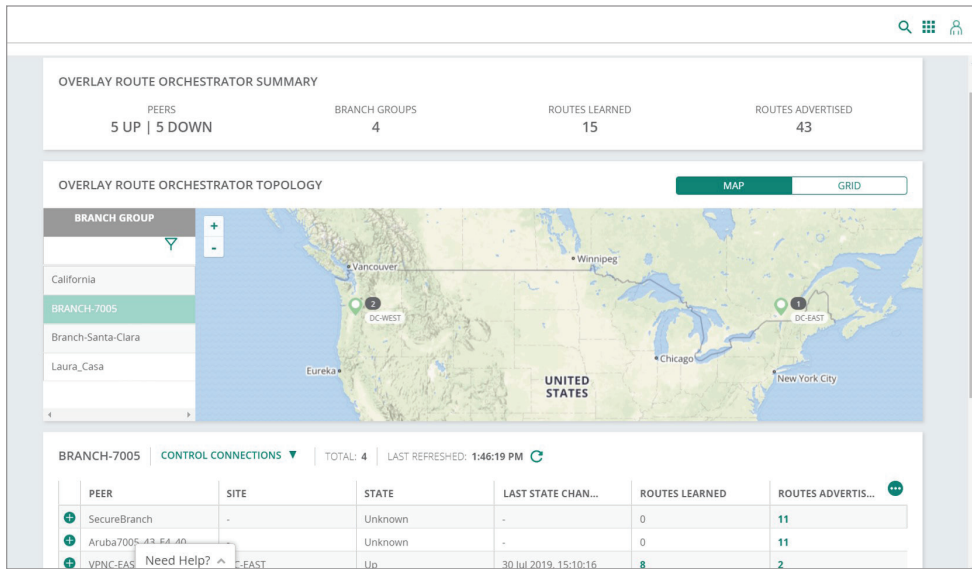


Figure 7: The Route Orchestrator's Control Connections

### Route Orchestration

The orchestration of routes is similarly automated, regardless of how many headend locations or branches you are connecting to. There is no need for legacy routing protocols on the SD-WAN overlay network—you can redistribute routes that are established from underlay protocols (such as BGP or OSPF) or from other methods (such as static routes).

Figure 7 shows the Route Orchestrator.

The Route Orchestrator displays each of the control connections as it learns multiple routes from different endpoints. It is also advertising the connected routes from the branch to the SD-WAN Orchestrator, which in turn advertises to multiple locations based on the preconfigured policies. If you want to see all the learned or advertised routes (Figure 8), you can click on those values in the Control Connections view.

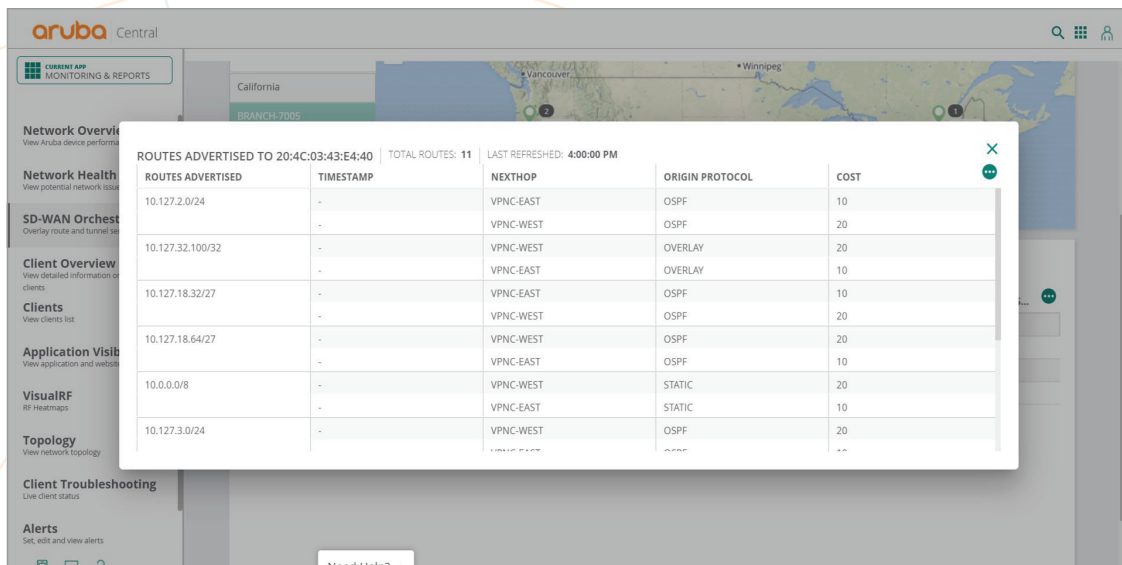


Figure 8: Learned and Advertised Routes



All routing information is set up and maintained in the Route Orchestrator. For each endpoint and advertised route, the Route Orchestrator lists the next hop, the originating protocol, and the cost.

## CONCLUSION

The value proposition of the SD-WAN Orchestrator is in the simplified management and optimal reachability of your entire SD-WAN deployment. Aruba's approach and underlying technology has been designed to simplify the IT experience for the world's most complex distributed enterprise networks. This approach has also led to an improved user experience: better performance for services and applications while administrators enjoy the simplicity of moving to SD-WAN. This results in major improvements to the bottom line of the business.