aruba
a Hewlett Packard
Enterprise company

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.

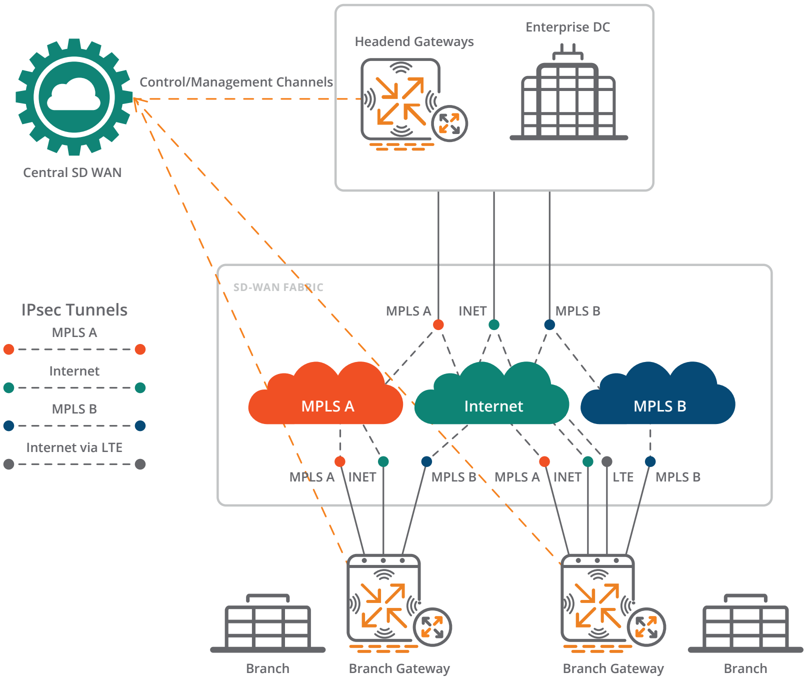


Figure 1: Defining Tunnels and Routes for Branches and Head Ends

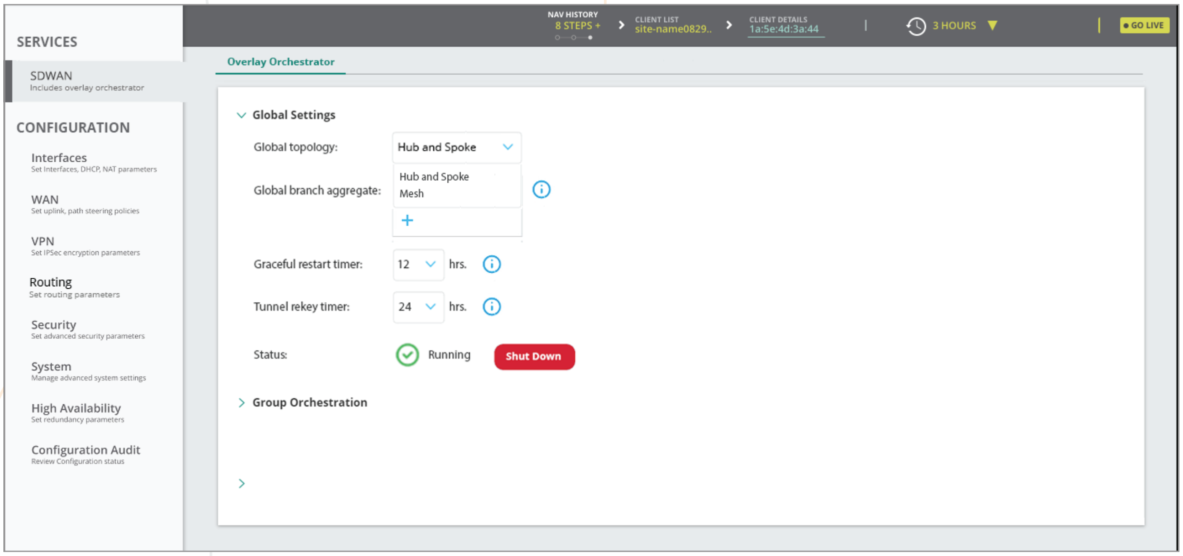
Topology Options

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.


SERVICES
SDWAN
Includes overlay orchestrator
CONFIGURATION
Interfaces
Set Interfaces, DHCP, NAT parameters
WAN
Set uplink, path steering policies
VPN
Set IPSec encryption parameters
Routing
Set routing parameters
Security
Set advanced security parameters
System
Manage advanced system settings
High Availability
Set redundancy parameters
Configuration Audit
Review Configuration status
NAV HISTORY
8 STEPS +
CLIENT LIST
site-name0829..
CLIENT DETAILS
1a:5e:4d:3a:44
3 HOURS
GO LIVE
Overlay Orchestrator
Shut Down

Global Settings

Global topology: Hub and Spoke

Global branch aggregate: Hub and Spoke / Mesh

Graceful restart timer: 12 hrs.

Tunnel rekey timer: 24 hrs.

Status: Running

Group Orchestration

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

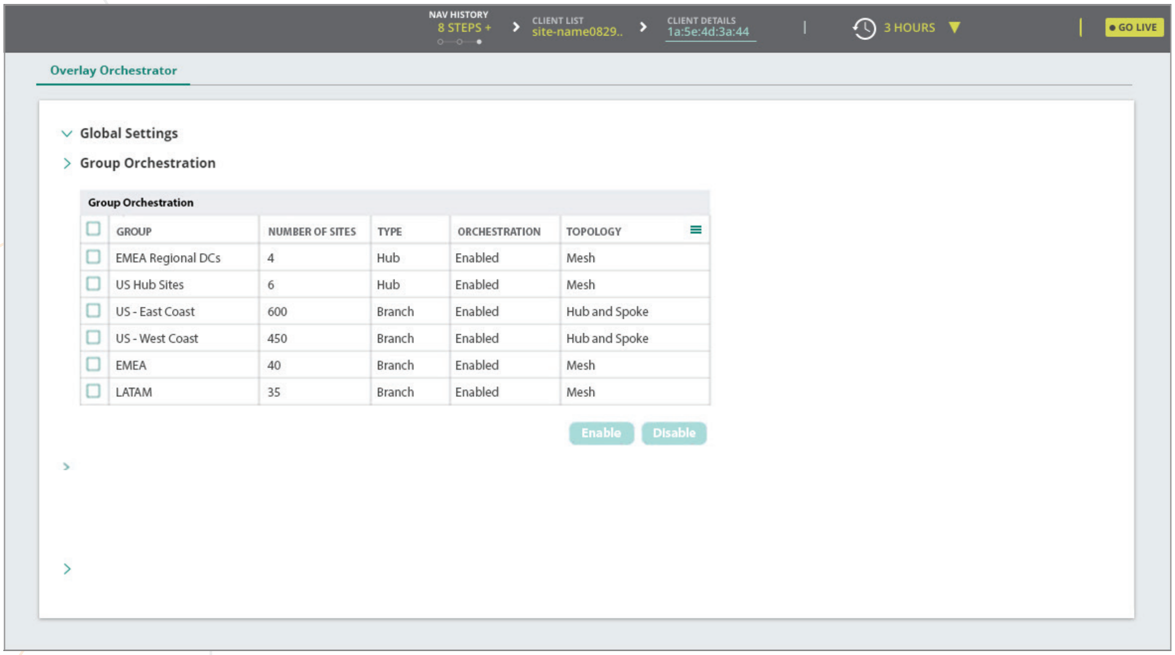
To greatly simplify this process, the SD-WAN Orchestrator manages all interfaces in the WAN, including both their public and private IP addresses. It then automatically sets up tunnels, for example between Carrier A's branch and headend MPLS Interfaces. For optimizing the traffic flows, the orchestrator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



Group Orchestration

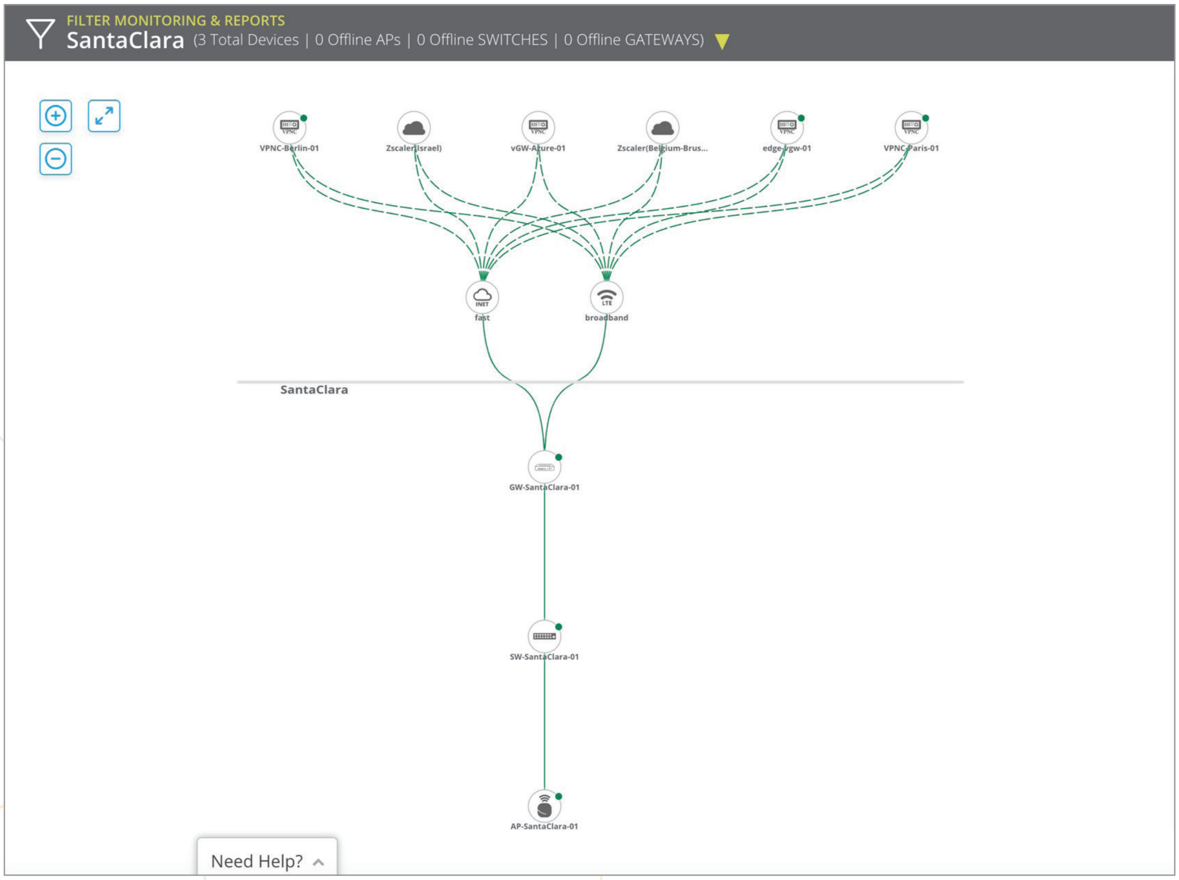
☐	GROUP	NUMBER OF SITES	TYPE	ORCHESTRATION	TOPOLOGY
☐	EMEA Regional DCs	4	Hub	Enabled	Mesh
☐	US Hub Sites	6	Hub	Enabled	Mesh
☐	US - East Coast	600	Branch	Enabled	Hub and Spoke
☐	US - West Coast	450	Branch	Enabled	Hub and Spoke
☐	EMEA	40	Branch	Enabled	Mesh
☐	LATAM	35	Branch	Enabled	Mesh

Figure 3: Group Orchestration

EXAMPLES: ORCHESTRATING AN SD-WAN OVERLAY NETWORK

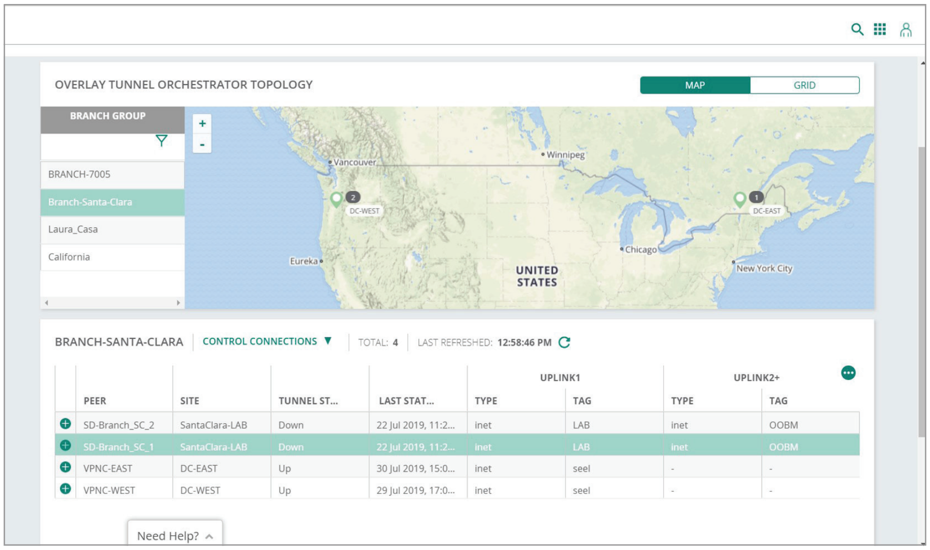
In this example (Figure 4), we're showing a global network with a single branch (one of possibly many), which may connect into any of multiple data centers or cloud provider endpoints.

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.



FILTER MONITORING & REPORTS
SantaClara (3 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)

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



OVERLAY TUNNEL ORCHESTRATOR TOPOLOGY

MAP | GRID

BRANCH GROUP

- BRANCH-7005
- Branch-Santa-Clara
- Laura_Casa
- California

BRANCH-SANTA-CLARA | CONTROL CONNECTIONS ▼ | TOTAL: 4 | LAST REFRESHED: 12:58:46 PM

					UPLINK1		UPLINK2+	
	PEER	SITE	TUNNEL ST...	LAST STAT...	TYPE	TAG	TYPE	TAG
⊕	SD-Branch_SC_2	SantaClara-LAB	Down	22 Jul 2019, 11:2...	inet	LAB	inet	OOBM
⊕	SD-Branch_SC_1	SantaClara-LAB	Down	22 Jul 2019, 11:2...	inet	LAB	inet	OOBM
⊕	VPNC-EAST	DC-EAST	Up	30 Jul 2019, 15:0...	inet	seel	-	-
⊕	VPNC-WEST	DC-WEST	Up	29 Jul 2019, 17:0...	inet	seel	-	-

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

Tunnel Orchestration

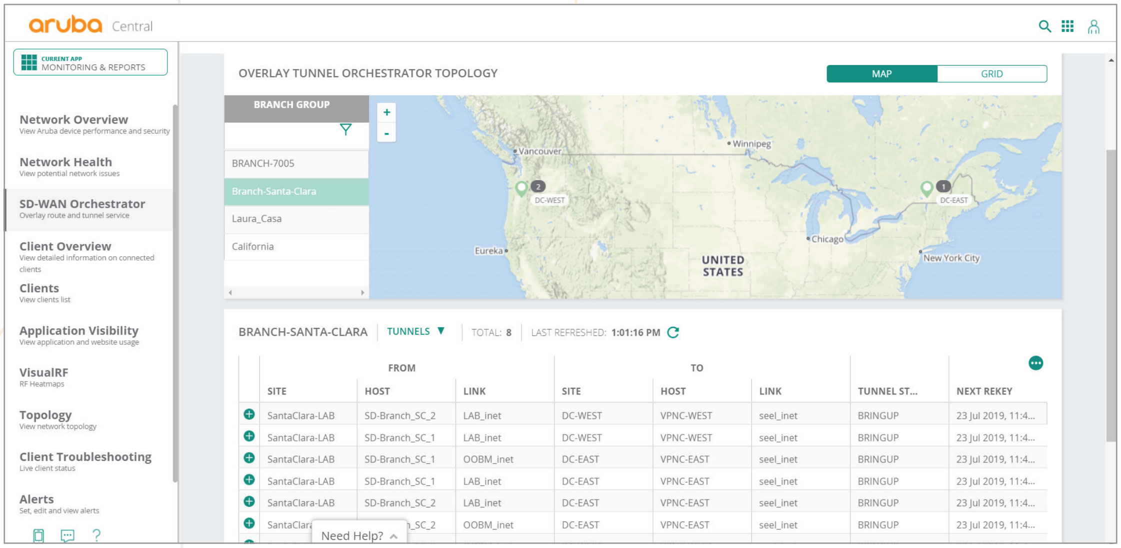
As the administrator, you can divide the network into multiple groups. This allows you to more easily establish and view specific portions of the network as needed. When you then select a branch group, you can look at specific headend gateways (virtual or physical) that the branch can connect to. At 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.



aruba Central

CURRENT APP
MONITORING & REPORTS

Network Overview
View Aruba device performance and security

Network Health
View potential network issues

SD-WAN Orchestrator
Overlay route and tunnel service

Client Overview
View detailed information on connected clients

Clients
View clients list

Application Visibility
View application and website usage

VisualRF
RF Heatmaps

Topology
View network topology

Client Troubleshooting
Live client status

Alerts
Set, edit and view alerts

OVERLAY TUNNEL ORCHESTRATOR TOPOLOGY

MAP | GRID

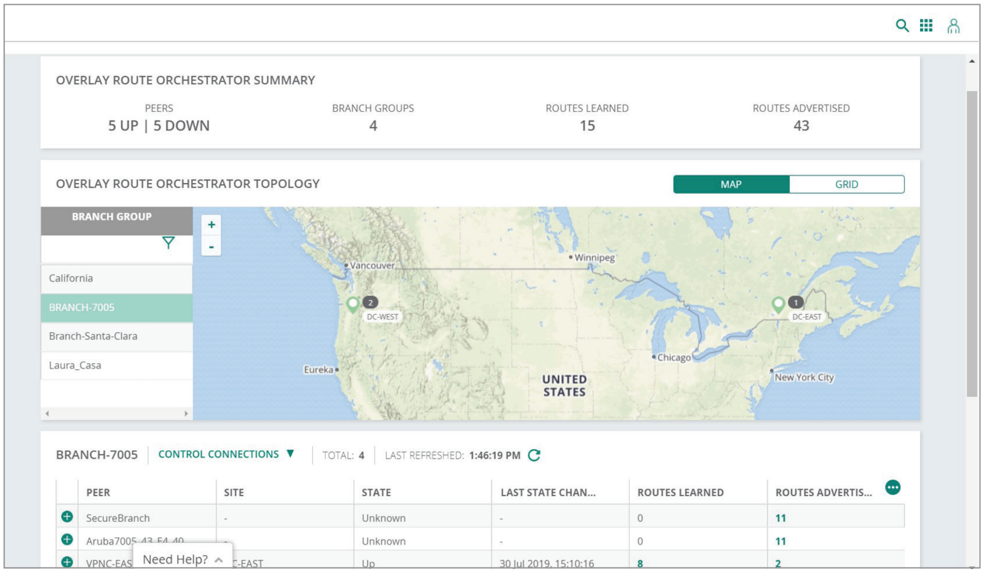
BRANCH GROUP

- BRANCH-7005
- Branch-Santa-Clara
- Laura_Casa
- California

BRANCH-SANTA-CLARA | TUNNELS ▼ | TOTAL: 8 | LAST REFRESHED: 1:01:16 PM

	FROM			TO				
	SITE	HOST	LINK	SITE	HOST	LINK	TUNNEL ST...	NEXT REKEY
⊕	SantaClara-LAB	SD-Branch_SC_2	LAB_inet	DC-WEST	VPNC-WEST	seel_inet	BRINGUP	23 Jul 2019, 11:4...
⊕	SantaClara-LAB	SD-Branch_SC_1	LAB_inet	DC-WEST	VPNC-WEST	seel_inet	BRINGUP	23 Jul 2019, 11:4...
⊕	SantaClara-LAB	SD-Branch_SC_1	OOBM_inet	DC-EAST	VPNC-EAST	seel_inet	BRINGUP	23 Jul 2019, 11:4...
⊕	SantaClara-LAB	SD-Branch_SC_1	LAB_inet	DC-EAST	VPNC-EAST	seel_inet	BRINGUP	23 Jul 2019, 11:4...
⊕	SantaClara-LAB	SD-Branch_SC_2	LAB_inet	DC-EAST	VPNC-EAST	seel_inet	BRINGUP	23 Jul 2019, 11:4...
⊕	SantaClar	_SC_2	OOBM_inet	DC-EAST	VPNC-EAST	seel_inet	BRINGUP	23 Jul 2019, 11:4...

Figure 6: Tunnels from Branches to Headends are Automatically Established



OVERLAY ROUTE ORCHESTRATOR SUMMARY

PEERS	BRANCH GROUPS	ROUTES LEARNED	ROUTES ADVERTISED
5 UP | 5 DOWN	4	15	43

OVERLAY ROUTE ORCHESTRATOR TOPOLOGY

BRANCH-7005 | CONTROL CONNECTIONS ▼ | TOTAL: 4 | LAST REFRESHED: 1:46:19 PM

PEER	SITE	STATE	LAST STATE CHAN...	ROUTES LEARNED	ROUTES ADVERTIS...
SecureBranch	-	Unknown	-	0	11
Aruba7005_43_F4_40	-	Unknown	-	0	11
VPNC-EAS	C-EAST	Up	30 Jul 2019, 15:10:16	8	2

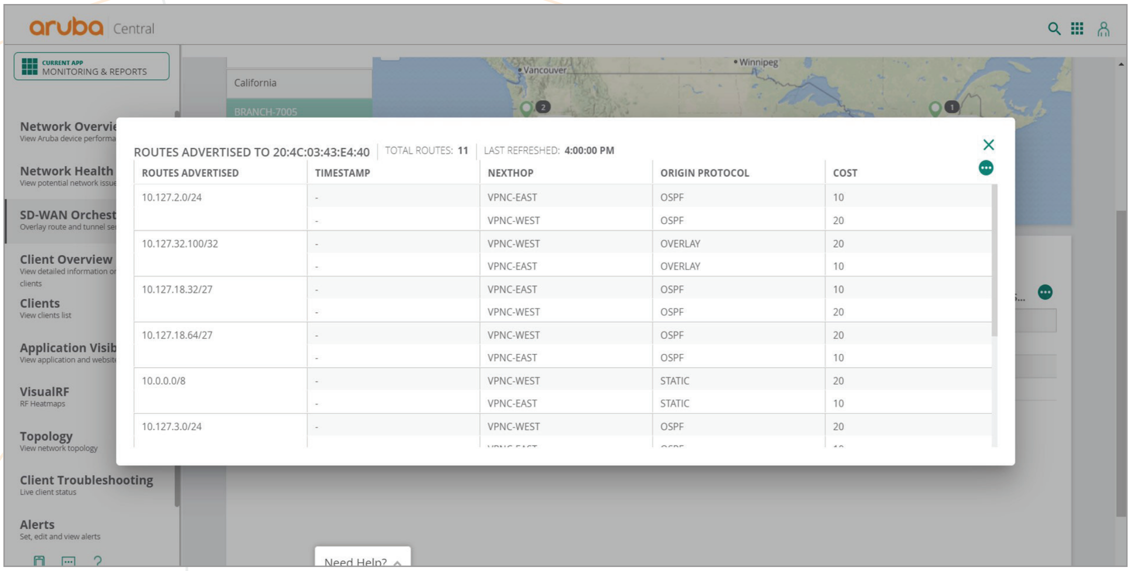
Figure 7: The Route Orchestrator's Control Connections

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.



ROUTES ADVERTISED TO 20:4C:03:43:E4:40 | TOTAL ROUTES: 11 | LAST REFRESHED: 4:00:00 PM

ROUTES ADVERTISED	TIMESTAMP	NEXTHOP	ORIGIN PROTOCOL	COST
10.127.2.0/24	-	VPNC-EAST	OSPF	10
	-	VPNC-WEST	OSPF	20
10.127.32.100/32	-	VPNC-WEST	OVERLAY	20
	-	VPNC-EAST	OVERLAY	10
10.127.18.32/27	-	VPNC-EAST	OSPF	10
	-	VPNC-WEST	OSPF	20
10.127.18.64/27	-	VPNC-WEST	OSPF	20
	-	VPNC-EAST	OSPF	10
10.0.0.0/8	-	VPNC-WEST	STATIC	20
	-	VPNC-EAST	STATIC	10
10.127.3.0/24	-	VPNC-WEST	OSPF	20

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.

a Hewlett Packard
Enterprise company

Contact Us **Share**