Copyright Information

Copyright © 2020 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
6280 America Center Drive
San Jose, CA 95002
USA
Revision History .................................................................................................................. 5

1 Overview .......................................................................................................................... 6
   1.1 Background .................................................................................................................. 6
   1.2 Requirements .............................................................................................................. 8
   1.3 SD-WAN Orchestrator Overview ............................................................................... 9

2 Overlay Tunnel Orchestrator ......................................................................................... 11
   2.1 Solution Overview ...................................................................................................... 11
   2.2 WAN Uplinks on the BGW and VPNC ...................................................................... 13
   2.3 DC Preference on BGWs ............................................................................................ 16
   2.4 Enable Orchestrator at the Group Level .................................................................... 17
   2.5 Cloud Survivability ..................................................................................................... 18

3 Overlay Route Orchestrator ........................................................................................... 20
   3.1 Solution Overview ...................................................................................................... 20
   3.2 Automatic Route Cost ................................................................................................ 22
   3.3 Route Redistribution .................................................................................................. 24
   3.4 Route Summarization ................................................................................................ 27
   3.5 Branch-to-Branch Communication .......................................................................... 31
   3.6 Overlay Route Filtering ............................................................................................. 32
   3.7 Transport Routing Attributes in SD-WAN .............................................................. 35
   3.8 Branch Redundancy ................................................................................................... 37

4 Monitoring and Troubleshooting .................................................................................. 40
   4.1 Control Connection .................................................................................................... 40
   4.2 Overlay Tunnel Orchestration .................................................................................. 42
   4.3 Overlay Route Orchestration ..................................................................................... 47

5 Reference Architectures .................................................................................................. 51
   5.1 Single Data Center L3 Scenario ............................................................................... 52
   5.2 Single Data Center L2 Scenario ............................................................................... 54
   5.3 Multiple Data Centers Scenario ............................................................................... 56
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4</td>
<td>L3 High Availability</td>
<td>59</td>
</tr>
<tr>
<td>5.5</td>
<td>Active-Active Data Centers</td>
<td>63</td>
</tr>
<tr>
<td>5.6</td>
<td>Traffic Segmentation at the Data Center</td>
<td>65</td>
</tr>
<tr>
<td>5.7</td>
<td>Dynamic Data Center Path Computation</td>
<td>70</td>
</tr>
<tr>
<td>5.8</td>
<td>Orchestrated Hub Mesh</td>
<td>75</td>
</tr>
<tr>
<td>5.9</td>
<td>Manual Hub Mesh</td>
<td>88</td>
</tr>
<tr>
<td>5.10</td>
<td>Multipath Scenario</td>
<td>94</td>
</tr>
<tr>
<td>6</td>
<td>Reference</td>
<td>99</td>
</tr>
</tbody>
</table>
## Revision History

The following table lists the revisions of this document:

<table>
<thead>
<tr>
<th>Revision</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>Initial Publication</td>
</tr>
<tr>
<td>Version 1.1</td>
<td>Minor formatting changes</td>
</tr>
<tr>
<td>Version 2.0/2.1</td>
<td>SD-WAN Orchestrator 2.0/2.1 updates:</td>
</tr>
<tr>
<td></td>
<td>• Overlay Route Attribute Transport</td>
</tr>
<tr>
<td></td>
<td>• Overlay Route Filtering</td>
</tr>
<tr>
<td></td>
<td>• BGP Multipath</td>
</tr>
<tr>
<td></td>
<td>• Cloud Survivability</td>
</tr>
<tr>
<td></td>
<td>• More Reference Architectures Included</td>
</tr>
<tr>
<td>Version 2.2</td>
<td>SD-WAN Orchestrator 2.2 updates:</td>
</tr>
<tr>
<td></td>
<td>• Orchestrated Hub Mesh</td>
</tr>
<tr>
<td></td>
<td>• Dynamic Data Center Path Computation</td>
</tr>
</tbody>
</table>

*Table 1* Revision History
1 Overview

To simplify SD-WAN configuration for large branches, Aruba introduced the SD-WAN Orchestrator to automatically setup IP Security (IPsec) tunnels and configure dynamic routing between Branch Gateways (BGW) and headend VPN Concentrators (VPNC). This guide seeks to describe the SD-WAN Orchestrator service, as well as the steps to enable the SD-WAN Orchestration service for SD-Branch deployments.

1.1 Background

The Aruba SD-WAN solution provides a centralized control plane function with the service offered from the Aruba Cloud Platform. The Aruba SD-WAN Orchestrator is based on a cloud-native, multi-tenant control plane which is auto-scaled with customer network growth.

In a SD-WAN deployment without SD-WAN Orchestration, the user had to specify the full configuration required to bring up IPsec tunnels between branch and headend gateways to form the overlay topology. The user had to pick the correct interface type (Internet, MPLS or LTE), enter the Public IP addresses of the VPNCs, set the IKE parameters and so on.

If the user required a tunnel through a common Internet service provider (ISP), the user had to enter the specific details as part of the configuration, which included selecting the correct uplink on BGW and the correct Public IP address on the VPNC. As such, this configuration workflow was cumbersome and prone to misconfigurations.

Also, there was no support for dynamic protocols or orchestrated routes through the overlay tunnels. Static routes pointing to each data center were configured with different costs in order to provide redundancy in case of a failure. For large deployments, which may have hundreds of locations, having the routing achieved based on static routes is not scalable or easy to administer.

![Figure 1 - Traditional Network](image)
Automated Overlay Tunnel and Route Orchestrator processes were created to address all these manual configurations and to automate the existing workflow.

<table>
<thead>
<tr>
<th>Without Aruba SD-WAN Orchestratior</th>
<th>With Aruba SD-WAN Orchestrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Create IPsec overlay manually or semi-automatic (IPsec peers, parameter, certificates, etc.).</td>
<td>• The IPsec overlay is created through Tunnel Orchestration.</td>
</tr>
<tr>
<td>• Setup routing protocol over IPsec tunnel (BGP peering, route-maps, etc.).</td>
<td>• Reachability information is being distributed through Route Orchestration; redistribution is done through a single group configuration.</td>
</tr>
<tr>
<td>• Create routing policies to ensure reachability, failover, etc. (This includes route-maps and redistribution.)</td>
<td>• Routing policies are as simple as setting a Hub preference at the group level. Redistribution takes care of ensuring symmetry.</td>
</tr>
<tr>
<td>• Multiple if not all devices need to be touched to set this up, and configuration elements need to be synced and aligned to create the overlay network.</td>
<td>• Devices do not need to be touched to configure the overlay topology and routing policy – it’s done at group level for all devices.</td>
</tr>
<tr>
<td>• Adding a site or a hub may or may not be easy depending on the original design, but it may likely require touching the configuration at multiple points.</td>
<td>• When a site is added to a group it learns the set overlay topology and orchestration will do what’s needed to create tunnels and route policy.</td>
</tr>
<tr>
<td>• Changing routing policy, or path preference (primary, secondary VPNC) would very likely require touching the routing policy or parts of it on every device.</td>
<td>• Adding a new Hub is as simple as adding it to the Hub preference on group level. No routing reconfiguration is required.</td>
</tr>
<tr>
<td>• Coordinated changes are hard to undertake as multiple steps in a timely manner are needed (error prone).</td>
<td>• Changing path preference is done by changing Hub preference setting; routing costs will be adapted and this will be translated into VPNC routing.</td>
</tr>
<tr>
<td>• Scalable design taking all future changes into consideration right from the start is key.</td>
<td>• Scalability is built into the orchestration itself, helping to avoid getting stuck with a non-scaling routing design.</td>
</tr>
</tbody>
</table>
1.2 Requirements

Note the following prerequisites are required for the SD-WAN Orchestrator service:

- Aruba Gateways are provisioned and connected to Aruba Central.
- Aruba Gateways running minimum ArubaOS 8.4.0.0-1.0.6.4 or a later software version.
- Certain capabilities described in this guide would require ArubaOS 8.5.0.0-2.0.
1.3 SD-WAN Orchestrator Overview

The SD-WAN Orchestrator automates tunnel configuration between the branch and hub sites. 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 Aruba Overlay Tunnel Orchestrator removes the complexity and scalability issues associated with setting up a large number of IPsec tunnels. It also eliminates the need for the user to specify Internet Key Exchange (IKE) related configuration (i.e., certificate, encryption type, etc.) for every tunnel. With the SD-WAN Orchestrator, Aruba simplifies the configuration required for the tunnels and eases the burden of configuration, which is expected from a cloud-based management platform.

In order to build an SD-WAN network, the first step is to bring up an overlay network that is independent of the underlying WAN circuits. In order to do this, the administrator will identify the uplink interfaces in all nodes with the corresponding service provider. Once that's available, the SD-WAN Orchestrator instructs the establishment of IPsec tunnels according to the policy. This is referred to as **Tunnel Orchestration**.

The Aruba **Route Orchestrator** enables the distribution of routing information across all sites including branches and headends. It provides route distribution across sites in a dynamic way according to the topology and routing segmentation policy configurations.

The main functions of the Aruba Overlay Route Orchestrator include:

- Learning routes from hub/branch sites.
- Advertising routes across the SD-WAN network with appropriate costs.
- Redistributing routes into the LAN side with appropriate costs.
The SD-WAN Orchestrator's goal is to build the SD-WAN Overlay and provide dynamic routing with minimal intervention from the user's side.

Figure 2 - SD-WAN Orchestrator
2 Overlay Tunnel Orchestrator

2.1 Solution Overview

The Aruba Overlay Tunnel Orchestrator allows to easily build overlay mappings. The Tunnel Orchestrator discovers the WAN uplinks of the devices and associated attributes in order to orchestrate the tunnels between endpoints. A tunnel agent registers each uplink and associated attributes with the Overlay Tunnel Orchestrator. Hence, the Overlay Tunnel Orchestrator gathers all the necessary information from the tunnel agent running on every device.

The main functions of Aruba Overlay Tunnel Orchestrator include:

- Discovering public/private IP addresses and uplinks attributes.
- Exchanging keys and sending keys to devices.
- Building IPsec tunnels.
- Refreshing keying material before old key expires.

NOTE As the overlay IPsec tunnels are being orchestrated by the SD-WAN Orchestrator, any ISAKMP security associations on the branch gateway (BGW) or headend (VPNC) will **NOT** be seen.
The following figure illustrates the tunnel orchestration process:

Figure 3 – Overlay Tunnel Orchestrator
2.2 WAN Uplinks on the BGW and VPNC

The Overlay Tunnel Orchestrator requires to configure uplinks on the BGW and VPNC, so that Tunnel Orchestrator can learn the WAN interfaces that will be used for terminating IPsec tunnels. The BGW typically has multiple uplinks and each one can have different characteristics such as link type (Internet, MPLS, LTE, etc) and a label/tag to identify the service provider for that uplink (ATT, Verizon, Orange, Telmex, etc.). The VPNC may also have multiple WAN uplinks of different type from various service providers.

The Overlay Tunnel Orchestrator looks at the uplink configuration elements to select the correct topology mapping based on the following mechanism:

- The uplink type (INET/MPLS/Metro/LTE) field must match on both sides of the uplinks.
- MPLS links:
  - The <label> field must loosely match between VPNCs and BGWs (case-insensitive substring match between the two provider names).
  - Tunnels are brought only between uplinks that match <type> and <label> (loosely in the case of label).
- Internet/LTE/Metro links:
  - Try to match the <label> field as the objective is to create a tunnel through the same service provider network.
  - If <label> matches, then pick the corresponding pair of uplinks.
  - If <label> does not match, then each WAN uplink on BGW will pick the first available INET uplink on VPNC to form a tunnel.

NOTE LTE and Metro uplink types are available only on the branch. They both correspond to “INET” type on the VPNC side.

The following figure illustrates the IPsec mapping procedure between BGWs and VPNCs.

NOTE In the example shown in the following figure, the VPNC has three uplinks. The number of uplinks was selected to help exemplify better the mechanism.
Figure 4 - Tunnel Mappings
Configure the uplinks and assign a label to them on the Gateway Management > WAN > Uplink page both on the BGW and VPNC. This can be done at the group or device level in the case of Branch Gateway (BGW), but must be done at the device level for the headend gateways (VPNC).

**Figure 5 – WAN Uplinks**

Health Check has to be enabled on the BGW in order to mark the uplinks as reachable. Also, the gateway needs to have default-gateways configured for the tunnels to come up, as the health-check tests reachability for:

- Default-gateway
- Health-Check IP/FQDN
- Tunnel destination

Use pqm.arubanetworks.com as remote FQDN to be used for Health Check probes. If Health Check will probe that default-gateway is unreachable, IPsec tunnels won't come up. If Health Check IP/FQDN is unreachable, this is not affecting the bringup of the IPsec tunnels.

**NOTE** When using orchestrated overlay, health check probes are used instead of DPD to validate tunnel state.
2.3 DC Preference on BGWs

On the BGW, set DC preference to define the hubs (VPNC) branch gateways will be connected to. DC preference can only be configured at group level. The DC order of preference will influence:

- The route costs that Orchestrator applies to the branch routes installed on the VPNCs in each hub site. The primary hub receives a cost of 10 (preferred), while the secondary hub receives a cost of 20 (least preferred). If we have additional VPNCs, the cost will increment by 10 for each VPNC based on their order.
- On the BGW, the hub routes to the primary VPNC are installed in the overlay routing table with a cost of 10 and the routes to additional hubs are incremented by 10.

Configure DC Preference on the BGW at group level under Gateway Management > VPN > SD-WAN Overlay > DC Preference:

<table>
<thead>
<tr>
<th>Preference</th>
<th>Hub Group</th>
<th>VPNC1</th>
<th>VPNC2</th>
<th>VPNC3</th>
<th>VPNC4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Oakmead-DC1</td>
<td>Oakmead-DC1-1</td>
<td>1st</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Oakmead-DC2</td>
<td>Oakmead-DC2-1</td>
<td>2nd</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Higher DC Preference -> Lower routing cost

Figure 6 - DC Preference
2.4 Enable Orchestrator at the Group Level

As a last step, it is recommended to configure the Overlay mode as **Orchestrated** and **Enable Orchestrator** at the group level under **Gateway Management > VPN > SD-WAN Overlay**, both on the BGW and VPNC.

![Figure 7 - Enable SD-WAN Orchestrator](image)
2.5 Cloud Survivability

Users can modify the Tunnel rekey timer, which is the timer value used between Branch Gateway (BGW) and headend (VPNC) to exchange keys for IPsec tunnel. The configured rekey timer value is between 60 - 1209600 secs (14 days). Default value is set to 24 hours.

- When the Tunnel rekey timer (T) is configured, the trigger for rekey will start at T/6 time prior to the expiration (for example, if 24 hours is the tunnel rekey time, the first rekey will be triggered at 20 hours after the tunnel is established).
- The device will send rekey request 10 times from the T/6 time to expiry time T. The device will send these 10 rekey request at periodic intervals calculated based on the expiry time. For example, if 24 hours is the expiry time, T = 1440 minutes and T/6 = 240 minutes; the device will send a rekey request every 24 minutes for 10 times.

The tunnel rekey timer can be changed from the Network Services > SD-WAN Overlay global settings page.

![Figure 8 – Tunnel Re-key Interval](image)

![Figure 9 – Tunnel Rekey Timer](image)
NOTE Users can also set **Graceful restart timer** to keep the tunnel up, and maintain route state on the device when it loses connectivity to cloud. The default value is 12h, but it can range between 1h and one week.

During rekeying, if the cloud connection fails, the tunnel keys expire. The expiration of authentication keys causes the tunnels to go offline, resulting in network traffic disruption.

**Cloud Survivability** is a unique Aruba feature which mitigates traffic disruption between Aruba devices. If the cloud connection fails for any reason, the devices remain connected, through WAN connections. Devices can re-establish IPsec tunnels between them based on tunnel configurations which were received from SD-WAN Orchestrator using legacy IKE/IPsec tunnel establishment. When cloud connectivity failure is detected during the rekeying process, the tunnels seamlessly switch over to legacy IKE IPsec tunnels.

NOTE Cloud Survivability feature requires SD-WAN 2.1 code.

Cloud Survivability is triggered when:
- Devices on both sides of the tunnel have no connectivity to the SD-WAN Orchestration.
- Tunnel Orchestration pushes new keys to the gateway, but the gateway did not receive the new keys.
- The gateway is unable to bring up the tunnel using the Tunnel Orchestration keys received.

Once the survivability tunnel is UP, there will be no change in the routing table. Fallback to SD-WAN Orchestration tunnel will be done during the next rekey.

![Figure 10 – Tunnel in Survivability Mode](image)

Attention! Tunnels "survive" in the scenario when the gateway is rebooted. Routes do not, as the graceful restart timer is reset after reboot.
3 Overlay Route Orchestrator

3.1 Solution Overview

The SD-WAN Overlay Route service consists of a Route Orchestrator in the cloud. Branch and headend devices connect to the SD-WAN Orchestrator service using the Control Connection - Overlay Agent Protocol (OAP). The OAP runs in a separate process on each device and interacts with the underlay routing stack, to get route prefixes and advertise them to the Overlay Agent (OA) and ISAKMPD daemon services. The Route Orchestrator sends route updates to OAP, then OAP passes them to the underlay routing stack.

The OAP control channel is a Remote Procedure Calls-based (gRPC) communication channel, which allows multiple streams over a single TCP connection. Each application (for example, Routing Service, Tunnel Service) can share the same TCP connection, but use their own streams. This communication happens independently of the management web socket established by devices managed by Aruba Central. Given the nature of this communication, the control-channel communication has a higher preference than the management channel.

The Aruba Overlay Route Orchestrator enables the distribution of routing information across all sites (branches and headends). It provides route distribution capabilities across sites in a dynamic way according to the topology and routing segmentation policy configurations. The Route Orchestrator learns routing information via redistribution from different routing sources (connected, static routes, OSPF, BGP) from different sites across the SD-WAN overlay. Using the SD-WAN overlay architecture, we can interconnect the sites without concerning how we can interconnect and redistribute the traffic from various routing sources.

**Route Orchestration** is the automation of routing between nodes. For this purpose, the SD-WAN Orchestrator operates like a horizontally scalable routing service for the SD-WAN:

- Routes learned by the different gateways participating in the SD-WAN network will be advertised (or redistributed) into the SD-WAN.
- Likewise, routes learned via the SD-WAN overlay will be redistributed or advertised to other routing protocols running on the VPNC (BGP, OSPF).
- When a given prefix is reachable through multiple paths, the cost is set as per the configured policy.

From the perspective of the Route Orchestrator, the DC preference determines the cost of the routes. A different cost based on the order of configuration is being assigned to the redistributed routes. This means the primary VPNC automatically gets a lower metric (cost 10) assigned than the secondary VPNC (cost 20). This cost is applied to the subnets that are being redistributed into the overlay (and implicitly into the data center via OSPF or BGP), as well as the data center subnets that are redistributed via the overlay and advertised to the Branch.
The following figure illustrates the Route Orchestration process:

Figure 11 - SD-WAN Orchestrator Architecture
3.2 Automatic Route Cost

From an overlay routing perspective, the DC preference determines the cost of the specific routes. When the Orchestrator is enabled on the branches, the DC preference has to be specified. For example:

- The BGW's primary VPNC is the primary next hop hub for the BGW to reach other subnets; that is why the Route Orchestrator assigns a cost of 10 to the routes received from primary VPNC and only those routes will be installed into the routing table.
- The BGW's secondary VPNC is the backup next hop hub for BGW; the routes learned from the secondary VPNC have a cost of 20 and they will not be installed in the routing table until the routes through the primary VPNC are withdrawn.

![Figure 12 - Routes Auto-cost](image)

Auto-cost is reflected in cost associated to the learned routes from each VPNC. Based on the DC preference order the routes are learned with a costs of 10,20,30,etc.
### Figure 13 – Auto-cost in learned routes table

<table>
<thead>
<tr>
<th>Route</th>
<th>Age (Last Update)</th>
<th>Origin</th>
<th>Cost</th>
<th>Next Hop</th>
<th>Interface</th>
</tr>
</thead>
</table>
3.3 Route Redistribution

To redistribute routes from BGW into the overlay, add the redistribution rules at the BGW group level, Gateway Management > Routing > Overlay Routing > Redistribution Routes.

![Gateway Management Interface]

*Figure 14 - BGW into Overlay*
To redistribute routes from headend into the overlay, add the redistribution rules at the VPNC group level, Gateway Management > Routing > Overlay Routing > Redistribution Routes.

![Overlay Routing](image)

*Figure 15 - Headend into Overlay*
To redistribute routes from the overlay into BGP or OSPF on the headend, add the redistribution rules at the VPNC group level, **Gateway Management > Routing > BGP/OSPF > Redistribute.**

Figure 16 - Headend Routes into BGP or OSPF
3.4 Route Summarization

At the Branch—Although Overlay Route Orchestration takes care of distributing subnets to all Gateways, it is still a best practice to use route summarization for directly connected subnets. This reduces the amount of routes advertised and reduce the route table entries in all BGWs and VPNCs (as some platforms have limited capabilities) as automatically reduces the amount of updates that are sent.

![Figure 17 - BGW Auto-Aggregate Connected Subnets](image1)

![Figure 18 – Routes Advertised without Auto-Aggregate](image2)
In the scenario when branch connected subnets are not a continuous range of subnets and can't be aggregated in a single aggregate route, auto-aggregate functionality is providing the option to configure the length of the aggregate. In this way any eventual gaps in the range of subnets are included as part of the aggregate created with a larger prefix-length. We can see in the next example that the previous example 190.3.8.200/29 was not included in the auto-aggregates generated. Specifying a prefix-length of /24, will create a /24 aggregate which will include all subnets.
At the Headend: For every hub group, use **Gateway Management > VPN > SD-WAN Overlay > DC Aggregate Routes.**
For branch-to-branch communications: In the **Network Services > SDWAN Overlay > Global branch aggregate** table, add the IP aggregate range(s) that will be advertised to all the branches. This summary range representing branch subnets will be advertised from all hubs configured in a BGW group (each honed with their respective metric).

Aruba recommends defining an IP aggregation range to reduce the routing table size of the branch gateways.

---

**Figure 18 - Global Aggregate Route**
3.5 Branch-to-Branch Communication

The **Allow branch-to-branch** feature is used by the Route Orchestrator to advertise branch routes to other BGWs, so the users from each BGW can communicate with each other through the VPNC.

By disabling this functionality, we can prevent spoke-to-spoke communication through the VPNC for those architectures where the communication is not desired (this is frequent in public cloud vGWs where the hub shouldn't be used as transit). By default, this feature is enabled on each VPNC, making them the transit gateways for branch-to-branch communication.

![Figure 22 - Branch to Branch Communication](image-url)
3.6 Overlay Route Filtering

Redistribution rules allow advertising routing information from connected, static, OSPF, and BGP protocols into overlay routing. Routing information from these routing sources is not automatically redistributed into overlay routing and it needs to be configured.

Route maps allow to configure filtering criteria by defining a set of rules or match statements with permit or deny conditions for the prefixes which we advertise to the SD-WAN overlay. Route maps can be used to set filters to overlay redistributed routes if routing source is BGP, OSPF, static, IAP-VPN, etc.

NOTE

The route maps configuration sections are common for BGP, OSPF and Overlay routing protocol. Only the applicable commands for the given protocol are applied and rest will be ignored. Please be sure to configure the right route-map applicable to the corresponding routing protocol.

Using unsupported match conditions will result in undesired results.

![Figure 23 – Overlay Route Filtering](image_url)
If only a certain route from the data center needs to be advertised to branches via the overlay (for example the network where ClearPass Policy Manager is installed), then we can configure a prefix list to match only that subnet and redistribute it via route-map to the overlay.

Figure 24 – Create Prefix-list to Match Data Center Route

Figure 25 – Route-map Matching Data Center Route
Redistributing BGP to Overlay routing and setting the route-map will allow only the permitted subnets to be redistributed.

<table>
<thead>
<tr>
<th>SYSTEM</th>
<th>WAN</th>
<th>INTERFACE</th>
<th>SECURITY</th>
<th>VPN</th>
<th>ROUTING</th>
<th>HIGH AVAILABILITY</th>
<th>CONFIG AUDIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Routes</td>
<td>Policy-Based Routing</td>
<td>NextHop Configuration</td>
<td>RIP</td>
<td>OSPF</td>
<td>BGP</td>
<td>Overlay Routing</td>
<td></td>
</tr>
</tbody>
</table>

- Route Map
- Prefix List
- Redistribution Routes

<table>
<thead>
<tr>
<th>Redistribution Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOURCE PROTOCOL</td>
</tr>
<tr>
<td>Static</td>
</tr>
<tr>
<td>BGP</td>
</tr>
</tbody>
</table>

**Figure 26 – Advertise Only Permitted Prefixes to Overlay**

To verify the advertised routes in the Aruba Central UI, go to **All devices > Gateways > List of Online Gateways > <Select your device>** and then click the **Overlay** tab and select **Routes Advertised** from the **Overlay Details** drop-down.

**Figure 27 – Only Permitted BGP Routes are Advertised to Overlay**
3.7 Transport Routing Attributes in SD-WAN

Starting with the Aruba SD-WAN 8.5.0.0-2.0 release, SD-WAN Orchestrator transports source protocol attributes to SD-WAN Route Orchestrator. Route attributes are carried over to/from receiver/sender side and can be redistributed to local underlay routing in the data center or branch network.

The SD-WAN Orchestrator now carries BGP attributes such as Origin, AS-Path or Community which give us the mechanisms of designing the desired route segmentation of the network.

➤ List of BGP attributes transported by Route Orchestrator:
  • Origin
  • AS-Path
  • Atomic Aggregate and Aggregate-AS attributes
  • Community (including Ext-Community and Large-Community)

➤ List of BGP attributes not transported by Route Orchestrator:
  • Next-Hop
  • Local Preference
  • MED
  • Originator ID

---

**NOTE**

Even if the MED value can be set in the route map used for redistributing BGP routes to the overlay, this is **not** done for transporting (MED is a non-transitive attribute). The goal of setting MED is to influence return routing costs in the case of branch HA.

---

A route map includes a set of match statements to determine if a route matches the criteria defined in the statement and then apply the permit or deny rule accordingly. An additional set of parameters could be configured to adjust the attributes and metrics for routes that match the criteria defined in the match statement.

Gateways can use route maps to set OSPF/BGP attributes. Route-maps can be used to selectively advertise routes based on the corresponding attributes.

---

**NOTE**

The cost and metric-type options available in the existing redistribute command are retained. For the other attributes set via route map, the route map values take precedence.
Route attributes can be matched and set while redistributing to the overlay. If route map is not used, route attributes received in the underlay will be carried if route map is not used to change the attributes.

ATTENTION

For more details as to how route attributes can be used in SD-WAN architecture, please check the “Traffic Segmentation at the Data Center” and “L3 High Availability” scenarios from Reference Architectures section.
3.8 Branch Redundancy

**Directly Connected.** For a branch deployed in HA with directly connected subnets to the gateways, in order to avoid loops or asymmetric traffic, only the gateway having the VRRP Master role advertises connected subnets to SD-WAN overlay. SD-WAN Orchestrator gets the notifications from VRRP about the VLANs for which the local gateway is the VRRP Master and hence it redistributes those connected subnets to the overlay only on that gateway. When VRRP roles are changed, the subnets are withdrawn when the gateway ceases to have the VRRP Master.

![Figure 28 – Connected Subnets](image)

**Static Routing/OSPF/BGP.** For a branch deployed in HA running static routes, OSPF or BGP in the branch network, both gateways redistribute routes to the SD-WAN overlay but set different costs to the routes. This method ensures improved route convergence time on certain failure conditions of a branch gateway.

The branch gateway is advertising the routes with a better cost to the VPNC having the 1st prioriy. The primary VPNC will receive the routes with a cost of 10 and increment +1 to the other gateway. For example, the standby branch gateway will send the routes with a cost of 11.
When running static routing/OSPF/BGP in a branch deployment, we need to manipulate the cost of the links that connect the branch gateways and branch switch/router such that one branch gateway is preferred. For example, set the link cost between Branch01 and Branch switch/router as 10 and the link cost between Branch02 and Branch switch/router as 20. Both Branch01 and Branch02 will redistribute the routes to the SD-WAN overlay but the Branch switch/router will prefer Branch01 over Branch02 for reachability to such routes due to lower cost.

![Dynamic Protocols in Branch HA](image)

Branch routes seen at the VPNCs have costs incrementing by 1 with each branch gateway, 10 and 11 in the example below:

<table>
<thead>
<tr>
<th>Route</th>
<th>Date/Time</th>
<th>Type</th>
<th>Cost</th>
<th>Hub</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.90.123.128/25</td>
<td>04 Feb 2020, 18:36:55</td>
<td>Static</td>
<td>10</td>
<td>GW-Bilbao-1</td>
</tr>
</tbody>
</table>

![Branch Static Route Costs on the VPNCs](image)
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Date/Time</th>
<th>Protocol</th>
<th>Cost</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.90.123.32/27</td>
<td>04 Feb 2020, 15:16:10</td>
<td>OSPF</td>
<td>10</td>
<td>GW-Bilbao-1</td>
</tr>
<tr>
<td>04 Feb 2020, 15:16:10</td>
<td>OSPF</td>
<td>11</td>
<td>GW-Bilbao-2</td>
<td></td>
</tr>
</tbody>
</table>

*Figure 31 – Branch OSPF Route Costs on the VPNCs*
4 Monitoring and Troubleshooting

The order of the verifications should be to check the Control Connection, then the Tunnel Orchestrator, and finally the Route Orchestrator. The outcome can be verified from the Aruba Central monitoring dashboards and also from the CLI available though the Central Remote Console.

4.1 Control Connection

If none of the tunnels are UP or even the IPsec mappings are not received from the SD-WAN Orchestrator, the first thing to check is if the Control channel is CONNECTED. Any other states such as DISCONNECTED or CONNECTING means the Gateway has not established communication with the SD-WAN Orchestrator. Troubleshoot Control channel connectivity issues before proceeding to the next steps.

To verify the Control channel connection in the Aruba Central UI, go to All Devices > Gateways > List of Online Devices. Select the Gateway, click the Overlay tab and then, select Control Connections from the Overlay Details drop-down:

![Figure 32 – Control Connection UI](image)

To verify the Control channel connection through the CLI, connect to the Gateway through the Remote Console and run the “show ip oap” command.

**CLI Output:**

```
(ArubaGW) #show ip oap
OAP Status
Admin State:     UP
Oper State:      UP
Master:          127.0.0.1:50050
Channel:         CONNECTED <-Connection status
Serial:          CNC6JS04P
MAC:             20:4c:03:0a:65:30
```
Site ID: 20:4c:03:0a:65:30
Tunnel If: tsgw
Graceful-restart-timer: 43200 seconds
Channel UP since: Wed 2019-07-31 16:41:56 PDT
Channel Down count: 1 <- # of times channel flapped
Learnt Routes: 14 <- # of routes learnt from Route Orchestrator
Advertised Routes: 4 <- # of routes push up to Route Orchestrator
Tunnels: 6 <- # of tunnels push up from Tunnel Orchestrator
Keepalive sent: 32558
Keepalive received: 38934
Keepalive pending: 0
PCM Gen ID IPv4: 1565064234954621

To verify the websocket connection to Aruba Central from the gateway, use the “show aruba-central details” command:

(ArubaGW) #show aruba-central details
Aruba Central
----------    ----
Parameter                  Value
Aruba Central IP/URL       internal.central.arubanetworks.com
Connection Status          Up
Time of last disconnect    N/A
SmartAmon MON Bootstrap Status Done
Number of times WS connected 1 <- # of times connection flapped
Time of last connect       Tue Jul 30 15:52:07 2019

To verify the control channel connection from the gateway, use “show aruba-central control-channel” command. For unstable connection issues, it may need to run the command a couple times with a couple minutes gap to see if the Number of State Changes counter is increasing.

(ArubaGW) #show aruba-central control-channel
Control Channel URL: internal-h2.central.arubanetworks.com
Connection State: READY
Time Last Connect: Thu Apr 11 15:42:44 2019
Number of State Changes: 1 <- # of times control-channel flapped

To further debug the control-channel, sometimes it's useful to see if the Calls Failed counter is increasing. If the counter is increasing for both TunsRpcSvc and CloudBgpSvc service, then it is likely that there is a issue with the cloud service.

(ArubaGW) #show aruba-central control-channel-counters
Service/Method Calls initiated Calls Completed Calls Failed US Rx US Rx_Err US Tx US Tx_Err DS Rx DS Rx_Err DS Tx DS Tx_Err Last Call Failure Reason
    tuns.TunsRpcSvc/Tunnel-Cha            13                0           12           46797       0      46797       0           59684       0           59684       0           59684       0           59684       0       Cancelled
    CloudBgpSvc/Cloud-Bgp                 3                0            2           35594       0      35594       0           254563       0           254563       0           254563       0           254563       0       Unimplemented
Total Initiated Calls: 16
Total Completed Calls: 0
Total Failed Calls: 14
Total Forwarded Messages: 396638
Proxy Rx Errors: 0
4.2 Overlay Tunnel Orchestration

When SD-WAN Orchestrator is enabled, all the IPsec-maps for tunnels created between VPNCs and BGWs are pushed from SD-WAN Orchestrator. If some tunnels fail to establish, the first thing to check is if all the IPsec maps have been received properly from the Tunnel Orchestrator, or if the uplinks of VPNCs and BGWs are configured properly and IP connectivity between them is available.

**NOTE**
As the overlay IPsec tunnels are being orchestrated by the SD-WAN Orchestrator, so any ISAKMP security associations on the BGW or VPNC will **NOT** seen.

To verify the IPsec maps in the Aruba Central UI, go to All devices > Gateways > List of Online Gateways > <Select your device> > and then, click the Tunnels tab:

![Tunnels UI](image)

To verify the IPsec map via CLI, access the Gateway through Remote Console and run the **“show crypto-local ipsec-map”** command.

**CLI Output:**

```
(ArubaGW) #show crypto-local ipsec-map
```
Crypto Map Template "data-vpnc-20:4c:03:21:a0:ac-verizon_inet" 9999
Alias Map Name: BGW1-Pod16:verizon_inet::VPNC1-Pod16:verizon_inet
Peer gateway: 172.16.14.27
Peer MAC: "20:4c:03:21:a0:ac"
Interface: VLAN 4094
Source network: 172.16.94.52/255.255.255.255
Destination network: 1.2.1.17/255.255.255.255
Initiator (Y/N): Y
Tunnel Trusted (Y/N): Y
Forced NAT-T (Y/N): Y
Force-Tunnel-Mode (Y/N): Y
Uplink LoadBalance (Y/N): Y
UUID: 2ef158f6-61be-45cb-bdbf-28a98a2320b4
Pair-UUID: f5ab80a0-ace2-4cdc-90df-b0823f407fca
Key Valid: Yes
Created Time: Thu May 23 15:10:33 2019
IN SPI: F14A4100, OUT SPI: 5B650900
Sos Program: Ingress: Yes Egress: Yes
Boot-Strap State: Done
HCM Probe State: Up

Total number of maps: 2
To verify the IPsec tunnels in the Aruba Central UI, go to All devices > Gateways > List of Online Gateways > select your device > and then, click the Overlay tab and select Interfaces from the Overlay Details drop-down:

![Overlay Tunnels UI](image)

To verify the IPSec tunnels from the Gateway CLI, log in to Gateway CLI through Remote Console and run the “show ip oap tunnel” and “show crypto ipsec sa” commands.

**CLI Output:**

```
(ArubaGW) #show ip oap tunnel
OAP Tunnel Table

<table>
<thead>
<tr>
<th>Tunnel</th>
<th>Device ID</th>
<th>Map ID</th>
<th>State</th>
<th>Routes</th>
<th>Up time</th>
</tr>
</thead>
<tbody>
<tr>
<td>data-vpnc-20:4c:03:0a:62:d0-att_mpls</td>
<td>20:4c:03:0a:62:d0</td>
<td>0x50004</td>
<td>up</td>
<td>7</td>
<td>0d-16h:0m:28s</td>
</tr>
<tr>
<td>data-vpnc-20:4c:03:0a:62:d0-verizon_inet</td>
<td>20:4c:03:0a:62:d0</td>
<td>0x50003</td>
<td>up</td>
<td>7</td>
<td>0d-16h:14m:28s</td>
</tr>
<tr>
<td>data-vpnc-20:4c:03:21:a0:ac-att_mpls</td>
<td>20:4c:03:21:a0:ac</td>
<td>0x50002</td>
<td>up</td>
<td>7</td>
<td>0d-16h:0m:28s</td>
</tr>
<tr>
<td>data-vpnc-20:4c:03:21:a0:ac-verizon_inet</td>
<td>20:4c:03:21:a0:ac</td>
<td>0x50001</td>
<td>up</td>
<td>7</td>
<td>0d-16h:14m:28s</td>
</tr>
</tbody>
</table>
```

```
(ArubaGW)#show crypto ipsec sa
Tunnel Service SA Information

<table>
<thead>
<tr>
<th>Initiator IP</th>
<th>Responder IP</th>
<th>SPI(IN/OUT)</th>
<th>Flags</th>
<th>Start Time</th>
<th>Inner</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.1.27</td>
<td>10.0.16.27</td>
<td>4762a00 /44a8a00</td>
<td>UTlt</td>
<td>May 23</td>
<td></td>
</tr>
<tr>
<td>15:24:32</td>
<td>-</td>
<td>f14a4100/5b65900</td>
<td>UTlt</td>
<td>May 23</td>
<td></td>
</tr>
<tr>
<td>172.16.94.52</td>
<td>172.16.14.27</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
Under site Topology map, it can be seen the tunnels created between BGW and VPNCs. VPNC devices are displayed per data center groups with the corresponding DC preference.

![Topology Map](image)

**Figure 35 – Topology Map**

To globally view the details of orchestrated overlay tunnels for all the devices, go to **Network Services > SD-WAN Overlay > Overlay Tunnel Orchestrator** page.
Figure 36 – SD-WAN Tunnel Orchestrator
4.3 Overlay Route Orchestration

Follow the following steps to check the routing table:

- Check Advertised Routes to the SD-WAN Overlay
- Check Received Routes from the SD-WAN Overlay
- Check the routes installed in the routing table
- View globally under SD-WAN Orchestrator Map the details of orchestrated overlay routes

1. **Check Advertised Routes.** To verify the advertised routes in the Aruba Central UI, go to **All devices > Gateways > List of Online Gateways > <Select your device>** and then, click the **Overlay** tab and select **Routes Advertised** from the Overlay Details drop-down.

![Overlay Advertised Routes UI](image)

To verify the advertised routes from the Gateway CLI, run the **`show ip oap advertise`** command.

**CLI Output:**

```
(London-DC-1) #show ip oap advertise

Codes:  A - advertised, D - dirty, S - summarized route
        AR - aggregate route, SR - static aggregate route
OAP Prefixes advertised to PCM
------------------------------------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Codes</th>
<th>Prefix</th>
<th>Nexthop</th>
<th>Interface</th>
<th>Protocol</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>10.21.0.0/16</td>
<td>10.21.251.97</td>
<td>vlan 4092</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>A</td>
<td>169.254.145.169/32</td>
<td>::</td>
<td>tunnel interface</td>
<td>static</td>
<td>1</td>
</tr>
<tr>
<td>A</td>
<td>10.2.100.2/32</td>
<td>::</td>
<td>tunnel interface</td>
<td>static</td>
<td>1</td>
</tr>
<tr>
<td>A</td>
<td>169.254.239.157/32</td>
<td>::</td>
<td>tunnel interface</td>
<td>static</td>
<td>1</td>
</tr>
<tr>
<td>A</td>
<td>10.11.0.0/16</td>
<td>::</td>
<td>tunnel interface</td>
<td>ebgp</td>
<td>0</td>
</tr>
</tbody>
</table>
```

![Overlay Advertised Routes CLI Output](image)
2. **Check Received Routes.** To verify the received routes in the Aruba Central UI, go to All devices > Gateways > List of Online Gateways > <Select your device> and then, click the Overlay tab and select Routes Learned from the Overlay Details drop-down:

![Figure 38 - Overlay Received Routes UI](image)

To view on the CLI the received routes from SD-WAN Overlay, run the "show ip oap route" command:

**CLI Output:**

```plaintext
(ArubaGW) #show ip oap route
OAP Route Table
-------------
Prefix               Nexthop          Protocol Metric Tunnel                  MapId
-------------          -----------          --------  ------                  ------
2.2.2.1/32          00:1a:1e:01:a2:a0 direct 10  data-vpnc-00:1a:1e:01:a2:a0-comcast_inet 0x50001
2.2.2.2/32          00:1a:1e:02:70:c8 direct 20  data-vpnc-00:1a:1e:02:70:c8-comcast_inet 0x50008
10.0.0.0/8           00:1a:1e:01:a2:a0 static 10  data-vpnc-00:1a:1e:01:a2:a0-comcast_inet 0x50001
                      00:1a:1e:02:70:c8 static 10  data-vpnc-00:1a:1e:02:70:c8-comcast_inet 0x50001
10.127.2.0/24        00:1a:1e:01:a2:a0 ospf   10  data-vpnc-00:1a:1e:01:a2:a0-comcast_inet 0x50001
                      00:1a:1e:02:70:c8 ospf   20  data-vpnc-00:1a:1e:02:70:c8-comcast_inet 0x50001
10.127.3.0/24        00:1a:1e:01:a2:a0 ospf   10  data-vpnc-00:1a:1e:01:a2:a0-comcast_inet 0x50001
                      00:1a:1e:02:70:c8 ospf   20  data-vpnc-00:1a:1e:02:70:c8-comcast_inet 0x50001
10.127.11.0/24       00:1a:1e:01:a2:a0 ospf   10  data-vpnc-00:1a:1e:01:a2:a0-comcast_inet 0x50001
10.127.12.0/24       00:1a:1e:01:a2:a0 ospf   10  data-vpnc-00:1a:1e:01:a2:a0-comcast_inet 0x50001
10.127.16.0/20       00:1a:1e:01:a2:a0 ospf   10  data-vpnc-00:1a:1e:01:a2:a0-comcast_inet 0x50001
                      02:1a:1e:5e:4b:42 overlay 30
                      02:1a:1e:4b:eb:eb overlay 40
10.127.18.0/27       00:1a:1e:01:a2:a0 ospf   10  data-vpnc-00:1a:1e:01:a2:a0-comcast_inet 0x50001
                      00:1a:1e:02:70:c8 ospf   20  data-vpnc-00:1a:1e:02:70:c8-comcast_inet 0x50001
10.127.18.32/27      00:1a:1e:01:a2:a0 ospf   10  data-vpnc-00:1a:1e:01:a2:a0-comcast_inet 0x50001
                      00:1a:1e:02:70:c8 ospf   20  data-vpnc-00:1a:1e:02:70:c8-comcast_inet 0x50001
10.127.18.64/27      00:1a:1e:01:a2:a0 ospf   10  data-vpnc-00:1a:1e:01:a2:a0-comcast_inet 0x50001
                      00:1a:1e:02:70:c8 ospf   20  data-vpnc-00:1a:1e:02:70:c8-comcast_inet 0x50001
10.127.32.100/32     00:1a:1e:01:a2:a0 overlay 10
                      00:1a:1e:02:70:c8 overlay 20
                      02:1a:1e:5e:4b:42 overlay 30
```
3. Finally, verify the routes installed in the global routing table. To view the Route Table in the Aruba Central UI, go to All devices > Gateways > List of Online Gateways > <Select your device> > and then, click the Route Table tab:

![Figure 39 - Route Table UI](image)

4. To globally view the details of orchestrated overlay tunnels, go to Network Services > SD-WAN Orchestrator > Overlay Route Orchestrator page. To view the overlay route for each group and the devices in a group, click the branch group in the Map view. The route details for branch Gateways deployed in the selected branch group is displayed towards the bottom of the page. Under Control Connection view, click the number of Routes Advertised or Routes Learned to view the details of the routes advertised or learned by the device.
Figure 40 – Total Routes Learned and Advertised to Device

Figure 41 – The Routes Advertised to Device by SD-WAN Orchestrator

Figure 42 - SD-WAN Route Orchestrator
5 Reference Architectures

Branches can connect to multiple hubs, where each VPNC can be deployed in L2 or L3. The SD-WAN Orchestrator detects if the VPNCs are L2 redundant, in which case it only builds a tunnel to the VRRP Master VPNC. If the VPNCs are L3 redundant, the SD-WAN Orchestrator builds tunnels to both VPNCs.

Let's see how to set SD-WAN Orchestration in the following use cases:

- Single Data Center L3 Scenario
- Single Data Center L2 Scenario
- Multiple Data Centers (L3 or L2 inside the data center)
- Data Center High Availability
- Active-Active Data Centers
- Traffic Segmentation at the Data Center
- Hub Mesh
- Multipath Scenario
5.1 Single Data Center L3 Scenario

Hubs can be deployed in Layer 3 mode in the data center. A Layer 3 data center topology requires the uplinks to be configured as follows:

- For MPLS, the Private IP should be set to the interface IP of the corresponding VPNC.
- For INET, the Public IP should be set to the static-NAT'd Public IP of the VPNC.

![Figure 43 - Single Data Center L3](image)

Active tunnels are created to both VPNCs with routes advertised to both of them. Overlay routes have weighted costs to prefer one VPNC (as detailed in the table).

SD-WAN routing costs get automatically translated when redistributing branch subnets into the dynamic routing protocols usually found in the data center. As such:

- When using OSPF, the Overlay cost (10, 20, etc.) is automatically translated to OSPF metric, and routes can be redistributed as type E1 or E2, depending on what suits the topology best.
- When using BGP, the Overlay Routing cost (10, 20, etc.) is automatically translated into AS Path prepend, and subsequent VPNCs would prepend their AS incrementally (prepend-local-as=0, 1, etc.).
In DC preference, the VPNC can be set as primary and secondary. We would use a single configuration line if both VPNCs belong to the same group, or two configuration lines if each VPNC has its own group. The VPNC with the first preference will have a cost of 10, the VPNC with the second preference will have a cost of 20.

<table>
<thead>
<tr>
<th>DC Preference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hubs</td>
</tr>
<tr>
<td>PREFERENCE</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>

*Figure 44 – Data Center L3 DC Preferences*

The load can easily be distributed between VPNCs by having 2 branch groups with inverse priorities, and then distributing traffic evenly towards both VPNCs (check next scenarios).
5.2 Single Data Center L2 Scenario

Hubs can be deployed in Layer 2 mode in the data center. Virtual Router Redundancy Protocol (VRRP) provides a Virtual IP (VIP) address which is shared among the routers, with one designated as the Master router and the other as Backup. In case the Master fails, the Virtual IP address is mapped to a Backup router's IP address, which is taking the Master role.

A Layer 2 data center topology requires the uplinks to be configured as follows:

- For MPLS uplinks, the Private IP needs to be set to the VRRP VIP for both MPLS uplinks of the VPNCs.
- For INET uplinks, the Private IP needs to be set to the VRRP VIP for both INET uplinks of the VPNCs. The Private IP of the VRRP VIP needs to be static-NAT’d to the Public IP of the VRRP VIP.

For one-armed VPNCs, due to the nature of the design where VIP address stands for both uplinks, we need to configure a single uplink per each circuit (INET or MPLS). The SD-WAN Tunnel Orchestrator is aware that VPNCs are running in L2 and it will create tunnels with the VPNC that has the Master VRRP role. The SD-WAN Tunnel Orchestrator also sends the IPsec mappings to the VRRP Backup VPNC, but those tunnels will of course be down until the VRRP roles change.

<table>
<thead>
<tr>
<th>SRC</th>
<th>DST</th>
<th>TYPE</th>
<th>Tag</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>VPNC1</td>
<td>INET</td>
<td>GREEN</td>
<td>10</td>
</tr>
<tr>
<td>Branch</td>
<td>VPNC1</td>
<td>MPLS</td>
<td>RED</td>
<td>10</td>
</tr>
<tr>
<td>Branch</td>
<td>VPNC2</td>
<td>INET</td>
<td>GREEN</td>
<td>10</td>
</tr>
<tr>
<td>Branch</td>
<td>VPNC2</td>
<td>MPLS</td>
<td>RED</td>
<td>10</td>
</tr>
</tbody>
</table>

Figure 45 - Single Data Center L2
In DC preference, the VPNC can be set as primary and secondary (single configuration line).

![Table](image)

*Figure 46- Data Center L2 DC Preference*
### 5.3 Multiple Data Centers Scenario

Branches can connect to multiple hubs, where each data center can be L2 or L3 (as described above). The SD-WAN Orchestrator detects if the VPNCs are L2 redundant, in which case it only builds a tunnel to the VIP address of the VRRP (VPNC having the Master role). If they're L3 redundant, it builds tunnels to both VPNCs.

![Multiple Data Centers Diagram](image)

**Table 1: Multiple Data Centers Example**

<table>
<thead>
<tr>
<th>SRC</th>
<th>DST</th>
<th>Type</th>
<th>Tag</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>VPNC-W1/VPNC-W2</td>
<td>INET</td>
<td>GREEN</td>
<td>10</td>
</tr>
<tr>
<td>Branch</td>
<td>VPNC-W1/VPNC-W2</td>
<td>MPLS</td>
<td>RED</td>
<td>10</td>
</tr>
<tr>
<td>Branch</td>
<td>VPNC-E1</td>
<td>INET</td>
<td>GREEN</td>
<td>30</td>
</tr>
<tr>
<td>Branch</td>
<td>VPNC-E1</td>
<td>MPLS</td>
<td>RED</td>
<td>30</td>
</tr>
<tr>
<td>Branch</td>
<td>VPNC-E2</td>
<td>INET</td>
<td>GREEN</td>
<td>40</td>
</tr>
<tr>
<td>Branch</td>
<td>VPNC-E2</td>
<td>MPLS</td>
<td>RED</td>
<td>40</td>
</tr>
</tbody>
</table>

**Figure 47 - Multiple Data Centers**

Even inside the same data center, we can combine and have the pair of VPNCs deployed in L3 for MPLS circuit and in L2 for INET. See example.
To address a scenario with multiple data centers, multiple configuration lines will be used to set the order of DC preference. This requires configuring the VPNCs in a separate group per data center as a single group can’t be configured in multiple configuration lines.

For every additional VPNC, the cost will increment by 10 for each VPNC. For example, the VPNC from the first line will have a cost of 10, the VPNC from the second line will have a cost of 20, the first VPNC from the third line will have a cost of 30 and the second VPNC from the third line will have a cost of 40.

<table>
<thead>
<tr>
<th>SRC</th>
<th>DST</th>
<th>Type</th>
<th>Tag</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch</td>
<td>VPNC1/VPNC2</td>
<td>INET</td>
<td>GREEN</td>
<td>10</td>
</tr>
<tr>
<td>Branch</td>
<td>VPNC1</td>
<td>MPLS</td>
<td>RED</td>
<td>10</td>
</tr>
<tr>
<td>Branch</td>
<td>VPNC2</td>
<td>MPLS</td>
<td>RED</td>
<td>20</td>
</tr>
</tbody>
</table>

**Figure 48 – Same Data Center**

**Figure 49 – Multiple DCs Preference**
The IPsec mappings are also different for L3 and L2 scenarios as the Orchestrator differentiates each scenario.

For example, an IPsec mapping for L3 data center:

```
Crypto Map Template"data-vpnc-20:4c:03:21:a0:ac-att_mpls" 9999
Alias Map Name: BGW1-Pod16:att_mpls::VPNC1-Pod16:att_mpls
Peer gateway: 10.0.16.27
Peer MAC: "20:4c:03:21:a0:ac"
Interface: VLAN 4093
Source network: 10.0.1.27/255.255.255.255
Destination network: 2.2.2.17/255.255.255.255
Initiator (Y/N): Y
Tunnel Trusted (Y/N): Y
Forced NAT-T (Y/N): Y
Force-Tunnel-Mode (Y/N): Y
Uplink LoadBalance (Y/N): Y
UUID: 5bbca96e-09b2-485b-8c40-35ad3718704c
Pair-UUID: 5bbff954-b54d-4eb4-bb1f-60ace6c7b07
Key Valid: Yes
Created Time: Thu May 23 15:24:33 2019
IN SPI: 4762A00, OUT SPI: 44A8A00
Sos Program: Ingress: Yes Egress: Yes
Boot-Strap State: Done
HCM Probe State: Up
```

For example, an IPsec mapping for L2 data center, where we can see that tunnel headend is the VIP address of the VRRP:

```
Crypto Map Template"data-vpnc-00:0b:86:9a:19:77-lghh_lg_inet" 9999
Alias Map Name: BGW_2_Aruba7005_88_7D_58:lghh_lg_inet::VPNC_1_Aruba7010_9A_19_77:uplink_vpnc1_inet
Peer gateway: 121.162.129.16
Peer MAC: "00:0b:86:9a:19:77"
Interface: VLAN 4094
Source network: 10.10.40.2/255.255.255.255
Destination network: 2.2.2.2/255.255.255.255
Initiator (Y/N): Y
Tunnel Trusted (Y/N): Y
Forced NAT-T (Y/N): Y
Force-Tunnel-Mode (Y/N): Y
Uplink LoadBalance (Y/N): Y
UUID: b5a695ff-462b-4f02-a368-7aec697bf8a2
Pair-UUID: 2b4fb6fd-5687-48c1-9de8-ac4b73727be9
Key Valid: Yes
Created Time: Mon Sep 2 21:53:02 2019
IN SPI: F4CA1400, OUT SPI: SC409400
Sos Program: Ingress: No Egress: No
Boot-Strap State: Done
HCM Probe State: Up
Last Down Reason: Unknown
VRRP: Yes VPCN:Active
VRRP Standby Info: ---
Peer MAC: 20:4c:03:21:a0:ac
Destination network: 2.2.2.2/255.255.255.255
UUID: 74cff8b1-1b16-472b-5a6b-498c-92b3e7fa989
Pair-UUID: 5bf52626-6c0c-498c-9519-92b3e7fa989
Key Valid: Yes
Created Time: Mon Sep 2 21:42:37 2019
IN SPI: 78693A00, OUT SPI: C191F2C0
Sos Program: Ingress: No Egress: No
```
5.4 L3 High Availability

The traffic originated at the data center should prefer the hub having the higher DC preference. Based on the DC preference configured on the branches, the SD-WAN Orchestrator will also incrementally prepend its AS number when advertising branch prefixes.

![Diagram showing L3 High Availability](image)

*Figure 50 - Automatic AS Prepend*

For example, the routes advertised to the hub having the highest preference will have an overlay cost of 10, which translates to no AS prepended. A route advertised to a hub having the fourth preference will have an overlay cost of 40, which is advertised with its own AS number prepended 3 times.

To see all the received routes attributes sent to the data center core router from the CLI, run the “show ip bgp <prefix>” and “show ip bgp neighbours <peer> routes” commands.

CLI Output:

```
(London-DC-Core) #show ip bgp neighbors 10.2.100.1 routes
Status codes: > - Best Path, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete, m - multipath
BGP Route Path Table
```

```bash
#show ip bgp neighbors 10.2.100.1 routes
Status codes: > - Best Path, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete, m - multipath
BGP Route Path Table
```
Same automatic mechanism is applied for data centers which are running OSPF. For example, the routes advertised to the hub having the highest preference will have an overlay cost of 10, which translates that
Overlay routes are advertised to OSPF with an automatic metric of 10. The overlay routes advertised to OSPF from the second hub are redistributed to OSPF with an automatic metric of 20.

To see all the received routes costs sent to the data center core router from the CLI, run the “show ip route” and “show ip ospf database” commands. In OSPF database we can see that branch prefixes have been learned from first hub with a metric of 10 and from the second hub with a metric of 20.

**CLI Output:**

```sh
(Bucuresti-DC-Core) # show ip route | include 5.5.5
O(E2)  5.5.5.1  /32 [10] via 10.127.2.2
O(E2)  5.5.5.2  /32 [10] via 10.127.2.2
```

**OSPF Database Table (for LSA-Type: AS-EXTERNAL)**

<table>
<thead>
<tr>
<th>Area ID</th>
<th>LSA Type</th>
<th>Link ID</th>
<th>Adv Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
</tr>
</thead>
</table>

---

*Figure 51 – Automatic Advertised Metric*
<table>
<thead>
<tr>
<th>N/A</th>
<th>AS-EXTERNAL</th>
<th>5.5.5.2</th>
<th>9.9.9.2</th>
<th>1469</th>
<th>0x80000001</th>
<th>58fb</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netmask: 255.255.255.255</td>
<td>Metric Type 2, Fwd Addr 0.0.0.0, Tag 0</td>
<td>Tos 0, <strong>Metric 20</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>N/A</th>
<th>AS-EXTERNAL</th>
<th>5.5.5.2</th>
<th>9.9.9.1</th>
<th>24</th>
<th>0x80000001</th>
<th>f965</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netmask: 255.255.255.255</td>
<td>Metric Type 2, Fwd Addr 0.0.0.0, Tag 0</td>
<td>Tos 0, <strong>Metric 10</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>N/A</th>
<th>AS-EXTERNAL</th>
<th>5.5.5.1</th>
<th>9.9.9.2</th>
<th>1470</th>
<th>0x80000001</th>
<th>62f2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netmask: 255.255.255.255</td>
<td>Metric Type 2, Fwd Addr 0.0.0.0, Tag 0</td>
<td>Tos 0, <strong>Metric 20</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>N/A</th>
<th>AS-EXTERNAL</th>
<th>5.5.5.1</th>
<th>9.9.9.1</th>
<th>24</th>
<th>0x80000001</th>
<th>45c</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netmask: 255.255.255.255</td>
<td>Metric Type 2, Fwd Addr 0.0.0.0, Tag 0</td>
<td>Tos 0, <strong>Metric 10</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.5 Active-Active Data Centers

One of the purposes for deploying Active-Active Data Centers is to distribute the load between them. It also allows the sending of branch traffic to the nearest VPNC to minimize latency. This can be easily achieved by having two branch groups with inverse priorities and distributing the traffic evenly towards both VPNCs.

Both VPNCs are advertising the same prefixes, as such the branches will learn the same prefixes from both VPNCs. The DC Preference will determine the main VPNC for each branch.

Active-Active data centers can be configured even within the same data center, by inverting DC Preference between branch groups.
Figure 54 – Active-Active Within the Same Data Center
5.6 Traffic Segmentation at the Data Center

A common requirement is to advertise a specific set of prefixes from the VPNC to the core router/switch. BGP communities can be used as a mechanism to achieve this objective. By marking the prefixes with the BGP community, the VPNC can match on BGP communities to selectively advertise prefixes to BGP neighbours.

Attributes can be matched in the route-map used to redistribute routes to the overlay from BGP or from BGP to the overlay using:

- IP addresses (using prefix-lists)
- Community (using community value)
**On the Branch:** Configure route redistribution to the overlay and set the corresponding community for the prefixes advertised to the data center.

To verify the advertised route attributes from the gateway's CLI, run the "show ip oap advertise verbose" command.

**CLI Output:**

```
(Branch-SC_1) #show ip oap advertise verbose

Codes: A - advertised, D - dirty, S - summarized route
       AR - aggregate route, SR - static aggregate route
OAP Prefixes advertised to PCM
------------------------------------------------------------------------------------------------------------------

<table>
<thead>
<tr>
<th>Codes</th>
<th>Prefix</th>
<th>Nexthop</th>
<th>Interface</th>
<th>Protocol</th>
<th>Metric</th>
<th>Flags</th>
<th>GenId</th>
<th>Attrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>190.3.8.200/29</td>
<td>vlan 300</td>
<td>connected</td>
<td>0</td>
<td>0x3</td>
<td>1582875184644858</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A S</td>
<td>190.3.8.216/29</td>
<td>vlan 301</td>
<td>connected</td>
<td>0</td>
<td>0x43</td>
<td>1582875184644868</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A S</td>
<td>190.3.8.232/29</td>
<td>vlan 302</td>
<td>connected</td>
<td>0</td>
<td>0x43</td>
<td>1582875184644870</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A S</td>
<td>190.3.8.248/29</td>
<td>vlan 303</td>
<td>connected</td>
<td>0</td>
<td>0x43</td>
<td>1582875184644872</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>10.127.24.0/27</td>
<td>vlan 100</td>
<td>connected</td>
<td>0</td>
<td>0x3</td>
<td>1582875184644862</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
[bgp:(cmnty:65000:10)]
```
**On the Hub**: On the receiver hub, the community will be used as a match condition to permit in BGP only prefixes having the as attribute the match communities. Configure the route-map matching the corresponding community and apply it when redistributing overlay routes into BGP or on the route map configured on the outbound interface applied to the BGP peering.
Figure 59 - Apply Route Map to Overlay Routes

The route map can be configured on the outbound direction applied to the BGP peering for setting the advertised prefixes per peer.

Figure 60 - Apply Route-map to Outbound Direction
To see all the received routes attributes carried by Route Orchestrator from the hub CLI, run the "**show ip oap route verbose**" command.

**CLI Output:**

```
(London-DC-1) #show ip oap route verbose

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Nexthop</th>
<th>Protocol</th>
<th>Metric</th>
<th>Tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.5.1/32</td>
<td>20:4c:03:1a:28:f4</td>
<td>direct</td>
<td>50</td>
<td>default-vpnip-master-ipsecmap-20:4c:03:1a:28:f4-blue_inet</td>
</tr>
<tr>
<td>5.5.5.2/32</td>
<td>20:4c:03:1a:29:6c</td>
<td>direct</td>
<td>50</td>
<td>default-vpnip-master-ipsecmap-20:4c:03:1a:29:6c-blue_inet</td>
</tr>
<tr>
<td>172.110.0.2/32</td>
<td>20:4c:03:1a:28:f4</td>
<td>direct</td>
<td>50</td>
<td>default-vpnip-master-ipsecmap-20:4c:03:1a:28:f4-blue_inet</td>
</tr>
</tbody>
</table>
```
5.7 Dynamic Data Center Path Computation

Central 2.5.2 release introduces a new dynamic data center path computation configuration to allow the route orchestrator to use the best path computation using various route attributes, while selecting the next hops for the data center routes.

By default, the Overlay Route Orchestrator uses the manually configured data center preference for the next hop selection while announcing data center routes to the branches. You can now enable the dynamic data center path computation and bypass the default SD-WAN Overlay Route computation.

SD-WAN Orchestrator Dynamic Cost – With/Without

<table>
<thead>
<tr>
<th>GW</th>
<th>Network</th>
<th>NextHop</th>
<th>Cost (Without DynCost)</th>
<th>Cost (With DynCost)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGW1</td>
<td>10.11.0.0/16</td>
<td>VPNC-London1</td>
<td>10</td>
<td>30 (10+20)</td>
</tr>
<tr>
<td>BGW1</td>
<td>10.11.0.0/16</td>
<td>VPNC-London2</td>
<td>20</td>
<td>40 (20+20)</td>
</tr>
<tr>
<td>BGW1</td>
<td>10.11.0.0/16</td>
<td>VPNC-US1</td>
<td>50</td>
<td>60 (20+20)</td>
</tr>
<tr>
<td>BGW1</td>
<td>10.11.0.0/16</td>
<td>VPNC-US2</td>
<td>60</td>
<td>80 (20+20)</td>
</tr>
</tbody>
</table>

*Note: Orchestrator is adding to all DC preference values the last preference value of the new elected DCs.

We can see in the diagram that VPNC-US1 and VPNC-2 have been calculated as better paths after Dynamic Cost was enable, as a their DC preference changed to 10, respectively 20. In order to keep the previous order of the hubs, the new DC preference value of VPNC-2 (20) will be added to the previous elected hubs, changing their preference to 30 (10+20), respectively 40 (20+20).

Let's examine dynamic cost algorithm by using another example. The following 10.12.0.0/16 prefix is being advertised to the SD-WAN Orchestrator by 6 VPNCs with the DC preferences displayed in the table. After Dynamic Cost is enabled, based on the route attributes associated to the routes (which will be detailed below), SD-WAN Orchestrator determines that the route advertised by London DC (VPNC-London1 and VPNC-London2) is most prefered and 10, respectively 20 costs are retained. Also, it is computed that the next prefered route is advertised by the US DC (VPNC-US1 and VPNC-US2). The algorithm is keeping the initial DC
preferences associated to VPNC-US1 and VPNC-US2 and in order to avoid that any other hub will have a lower DC preference, it sums VPNC-US2 DC preference (60) to all the other remaining VPNCs.

<table>
<thead>
<tr>
<th>GW</th>
<th>Network</th>
<th>NextHop</th>
<th>Cost Without DynCost</th>
<th>Cost With DynCost</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGW1</td>
<td>10.12.0.0/16</td>
<td>VPNC-London1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>BGW1</td>
<td>10.12.0.0/16</td>
<td>VPNC-London2</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>BGW1</td>
<td>10.12.0.0/16</td>
<td>VPNC-Bucuresti1</td>
<td>30</td>
<td>90 (30+60*)</td>
</tr>
<tr>
<td>BGW1</td>
<td>10.12.0.0/16</td>
<td>VPNC-Bucuresti2</td>
<td>40</td>
<td>100 (40+60*)</td>
</tr>
<tr>
<td>BGW1</td>
<td>10.12.0.0/16</td>
<td>VPNC-US1</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>BGW1</td>
<td>10.12.0.0/16</td>
<td>VPNC-US2</td>
<td>60</td>
<td>60*</td>
</tr>
</tbody>
</table>

*Note: Orchestrator is adding to all DC preference values the last preference value of the new elected DCs.

Figure 62 – DynCost Costs Example

To enable dynamic data center path computation, the functionality is globally enabled from SD-WAN Orchestrator configuration, **Network Services > SD-WAN Overlay > Global Settings**.

Figure 63 – Enable Dynamic DC Path Computation
After dynamic data center path computation is enabled, SD-WAN Orchestrator computes the path on behalf of branch gateways for routes learned from data center. The following path computation algorithm will be used for determining the order of datacenter learned paths:

- Choose the path corresponding to the route which is advertised by lowest routing protocol administrative distance:
  - Connected - 0
  - Static - 1
  - eBGP - 100
  - OSPF - 110
  - iBGP – 200

- If multiple data center routes are learned from the same protocol, then the following order of preference is used:
  - Static
    - Prefer path (VPNC) advertising the route with lowest cost.
    - If all above parameters are the same then fall back to VPNC configured DC preference.
  - eBGP/iBGP
    - Prefer the path (VPNC) with the shortest autonomous system (AS) length.
    - Prefer the path (VPNC) with the lower origin code. Routes learned from an IGP have a lower origin code than those that have incomplete origin codes.
    - Prefer the path (VPNC) with the lowest multiple exit discriminator (MED) metric.
    - If all above parameters are the same then fall back to VPNC configured DC preference.
  - OSPF
    - Prefer path (VPNC) advertising the route with lowest cost.
    - If all above parameters are the same then fall back to VPNC configured DC preference.

In the scenario from the previous diagram, we are advertising the same subnet A via BGP from the main data center, but for fallback reasons we are advertising the same subnet A also from the secondary data center. The prefix is advertised to the first datacenter with a longer AS Path length than the prefix advertised by the
second datacenter. Without dynamic data center path computation enabled, the best path is chosen based on the hub which is having the highest DC preference configured:

![Figure 64 - Prefix Learnt via highest DC preference](image)

![Figure 65 - Prefix costs without Dynamic DC Enabled](image)

With dynamic data center path computation enabled, the best path is chosen based on dynamic data center computation rules described previously and due to shortest AS path length, the path via secondary data
center will be chosen as the best path. In order to reflect the changes, the DC preferences are dynamically changed to reflect the computed new paths.

![Figure 66 – Prefix Learned via Shortest Path](image1)

![Figure 67 – Prefix costs with Dynamic DC Enabled](image2)
5.8 Orchestrated Hub Mesh

5.8.1 Overview

Central 2.5.2 release introduces orchestrated hub mesh topology. A hub site is a headquarter or data center that includes one or more gateways operating as VPNCs. Central 2.5.2 release introduces the usage of orchestrated overlay tunnels to connect a hub site with one or more hub sites, thereby building an SD-WAN hub mesh topology.

When a hub mesh topology is configured between two or more hub sites, hub mesh links are formed between the VPNCs of the selected hub groups. The hub mesh links create an overlay network that securely transports traffic between the VPNCs of the selected hub groups.

The SD-Branch deployment includes at least one hub group with one or more VPNCs that terminate IPsec-based VPN tunnels initiated from the Branch Gateways. Based on the deployment size and redundancy
requirements, you can deploy one or more VPNCs at each hub group. The following figure illustrates the hub mesh topology between three data centers:

![Figure 68 – Hub Mesh](image-url)
5.8.2 Hub Mesh Design

5.8.2.1 Branch originated routes are always preferred

In a SD-WAN architecture, the routes originated at the branches are always prefered across SD-WAN Overlay. In order to achieve this design requirement, no manual configuration is required. SD-WAN Orchestrator will automatically assign the correct administrative distance and corresponding metrics for seamlessly achieving this, eliminating the need to design and manually maintain highly complex routing architectures.

The administrative distance (AD) and metric for branch originated routes are assigned as following:

- Branch routes are always preferred over overlay on directly connected VPNC, hence advertised to direct VPNC as with a Low Overlay AD (90), which is more preferred. Branch route cost will be set according to VPNC preference connectivity (10 for primary VPNC, 20 for secondary VPNC, etc.).
- Branch routes are always preferred over underlay on remotely connected VPNC, hence advertised to a remote VPNC as High Overlay AD (250), which is less preferred. Branch route cost will be set as 1000 to remotely connected VPNC.

NOTE

By default branch overlay administrative distance will have a lower value (90) than any underlay protocol (eBGP, iBGP, OSPF) but higher than the administrative distance of a connected and static route, which will make it more prefered to be added in the routing table than any other dynamic routing protocol.
5.8.2.2 VPNC originated routes have higher priority over underlay

In a SD-WAN architecture, the routes originated at the VPNC are always preferred over underlay routing protocol and have less preference over SD-WAN Hub Mesh network. SD-WAN Orchestrator will automatically assign the correct administrative distance and corresponding metrics for seamlessly achieving this as we will see below.

The administrative distance (AD) and metric for VPNC originated routes are assigned as following:

- VPNC routes are always preferred over overlay when advertised to branch gateways, hence are advertised to direct branch gateways with a Low Overlay AD (90), which is more preferred. The VPNC routes will be learned on the branches with the corresponding costs according to VPNC preference connectivity (10 for primary VPNC, 20 for secondary VPNC, etc.).
- VPNC routes are always preferred over underlay on remotely connected VPNC, hence advertised to a remote VPNC as High Overlay AD (250), which is less preferred. VPNC route cost will be set as 1000 to remotely connected VPNC.

**NOTE** By default hub overlay administrative distance (AD) will have a lower value (250) than any underlay protocol (eBGP, iBGP, OSPF, connected, static), which will make it less preferred.
5.8.2.3 Best Path Calculation

SD-WAN Orchestrator works in a similar way as a link state routing protocol. Depending on the node where a network is sourced, a route can be reachable across various paths present in a SD-WAN hub mesh overlay. When there are multiple routes to a particular network in a mesh overlay, the type of the route influences the path that is selected and installed by each router in the routing table. The difference between the types of routes is the way in which the metric for the route is calculated, depending on how they are advertised while being redistributed on the SD-WAN Overlay. Hubs which are part of the hub mesh overlay use these criteria to select the best route to be installed in the routing table.

SD-WAN Orchestrator has visibility across all overlay topology and all routes learned from all the nodes. Once VPNC has the routes and topology then the VPNC can compute the SPF (Shortest Path First) for each specific
route destination. SPF costs will reflect the computation of how to reach each node and then add the corresponding metrics to the paths to reach the routes advertised by each node.

A prefix can be reachable via more paths, then the SD-WAN Orchestrator compares the metric, choose the lowest metric, who will be the best path to reach the route, if the routes metrics are the same, all paths are selected as the best route.

<table>
<thead>
<tr>
<th>Route</th>
<th>Type</th>
<th>Next. Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>SubnetA</td>
<td>INET/MPLS</td>
<td>AWS</td>
</tr>
<tr>
<td>SubnetB</td>
<td>INET/MPLS</td>
<td>Azure</td>
</tr>
<tr>
<td>SubnetC</td>
<td>INET/MPLS</td>
<td>GCP</td>
</tr>
<tr>
<td>SubnetD</td>
<td>INET/MPLS</td>
<td>On-Prem</td>
</tr>
</tbody>
</table>

The VPNC does the route resolution based on route advertisement, topology information and current local tunnel status. For directly connected nodes, SPF is not performed. For the non-direct connected nodes, the best destination is chosen from route advertisement and then SPF is run to select the best path to reach destination.

**NOTE**

SD-WAN Orchestrator is not only computing which is the best path to reach the route, it is computing and calculating the next best alternatives to reach the corresponding destination in case the best path is not available. By having the information already available in the overlay database, failover to the next best path available is a quickly determined, reducing significantly the failover time.
The following path computation algorithm will be used for determining the order of datacenter learned paths:

- Choose the path corresponding to the route which is advertised by lowest routing protocol administrative distance:
  - Connected - 0
  - Static - 1
  - eBGP - 100
  - OSPF – 110
  - iBGP – 200

- If multiple data center routes are learned from the same protocol, then the following order of preference is used:
  - Static
    - Prefer path (VPNC) advertising the route with lowest cost.
    - If all above parameters are the same then fall back to VPNC configured DC preference.
  - eBGP/iBGP
    - Prefer the path (VPNC) with the shortest autonomous system (AS) length.
    - Prefer the path (VPNC) with the lower origin code. Routes learned from an IGP have a lower origin code than those that have incomplete origin codes.
    - If all above parameters are the same then fall back to VPNC configured DC preference.
  - OSPF
    - Prefer path (VPNC) advertising the route with lowest cost.
    - If all above parameters are the same then fall back to VPNC configured DC preference.

Let’s examine best path selection algorithm by using the example. The following 10.11.0.0/16 prefix is being advertised to the SD-WAN Orchestrator by 4 VPNCs with the following attributes:

<table>
<thead>
<tr>
<th>Route Prefix</th>
<th>AFI/SAFI</th>
<th>Originator ID</th>
<th>Next Hops</th>
</tr>
</thead>
</table>
| 10.11.0.0/16 | IPv4: UNICAST | 1. 02:1a:1e:3e:8e:3 | Gw: 02:1a:1e:3e:8e:3, PrefixType: HUB, ProtoType: EBGP, SiteId: 02:1a:1e:3e:8e:3, AsPath: [65000 65101], BgpOriginType: IGP, Med: 100, topolId: 1, vpcnTopolId: 1004, ...
|              |          | 2. 02:1a:1e:72:18:b4 | Gw: 02:1a:1e:72:18:b4, PrefixType: HUB, ProtoType: EBGP, SiteId: 02:1a:1e:72:18:b4, AsPath: [65000 65101], BgpOriginType: IGP, Med: 100, topolId: 1, vpcnTopolId: 1004, ...
|              |          | 3. 02:1a:1e:a2:36:6d | Gw: 02:1a:1e:a2:36:6d, PrefixType: HUB, ProtoType: EBGP, SiteId: 02:1a:1e:a2:36:6d, AsPath: [65001 65001 65101 65101 6513], Community: [6003:1000], BgpOriginType: IGP, Med: 51, topolId: 1, vpcnTopolId: 1004, ...
|              |          | 4. 02:1a:1e:3:0e:4 | Gw: 02:1a:1e:3:0e:4, PrefixType: HUB, ProtoType: EBGP, SiteId: 02:1a:1e:3:0e:4, AsPath: [65001 65001 65101 65101 6513], Community: [6003:1000], BgpOriginType: IGP, Med: 100, topolId: 1, vpcnTopolId: 1004, ...

*Figure 72 – Example of a Prefix from SD-WAN Orchestrator Database*
We can see that the prefix originated from EBGP by all 4 VPNCs, as such the best path selection for BGP will be applied as described previously. Based on the shortest AS Path length the first 2 VPNCs would be best paths, followed by the 3rd VPNC (longer AS Path and originated with a metric of 51) and 4rd VPNC (longer AS Path and originated with a metric of 100).

Based on the best path calculation, the SD-WAN Orchestrator will automatically assign a metric to each path.

- The 1st two VPNCs will automatically receive a metric of 1000, which is marking them as best.
- 2nd VPNC will automatically receive a metric of 1002.
- 3rd VPNC will automatically receive a metric of 1003.

**NOTE**

Please note that metric 1001 was skipped from the previous metric assignments, as two VPNCs are eligibles as best. If only one VPNC would have been selected as best, then the next automatically assigned metric would be 1001.

**IMPORTANT!** Now that we know which VPNC originated the prefix with the best metrics, based on all paths received, each node is performing a SFP locally and it is calculating with the best path to reach the best originated VPNC.

By checking the routing table of a hub which is part of the SD-WAN mesh (different that the 4 hubs which are originating the prefix), we can easily notice by looking to the metrics that there are 7 paths with metric 1000 which can be used to reach the 2 VPNCs which are marked as best. 2 next-hops are selected as bests based on the local SFP and shortest hops to reach the destination.

**Figure 73 – Best Paths Selected**
5.8.3 Multi-Cloud Mesh

Many customers are seeing the Cloud services as an extension of their on-premises data centers. In most of the cases the on-premises applications will need to communicate with the applications hosted in the cloud. In order to achieve this requirement, a hybrid architecture between on-premises and cloud data centers needs to be considered.

In a hybrid architecture, based on the characteristics of the communication between the on-prem and cloud applications, the cloud providers are proposing few ways to establish the connectivity.

- Accessing the cloud resources using **public IPs over the Internet**. Although this is the easier option to connect, the disadvantage of this method is that it might not be the most preferable from a security and network performance perspective.
- Accessing the cloud resources using a **Site-to-Site IPsec tunnel over the Internet**. Using public Internet, an encrypted tunnel can be set up between on-premises data centers and Cloud data centers. Although this option is more preferable from the security point of view, for an on-premises large data center or a mixed cloud environment, it might become cumbersome to manually configure the mesh of IPsec tunnels between all the hubs and administer and troubleshoot the routing table built on the top of the tunnels.
- Accessing the cloud resources using a **dedicated private circuit** like AWS DirectConnect or Azure RouteExpress. This option is the best one to achieve higher performance and to remove the uncertainty of using the Internet. However, also this option will show its limits when multi cloud hybrid architectures are required. Maintaining the routing table across multiple data centers will start to be challenging.

Using Aruba multi-cloud hub mesh design, all the scenarios and limits described previously can be addressed by seamlessly enabling hub mesh across all the data centers which require connectivity. SD-WAN Orchestrator will automatically build and bring up all tunnels and advertise routes with the corresponding costs for each datacenter. This architecture can be created in a matter of a few of minutes after enabling the hub mesh topology which eliminates the need to manually maintain or design complex routing topologies.

Furthermore, by using the hub mesh design, customers which have a dedicated circuit and an Internet circuit will be able to automatically build tunnels over both circuits compared with the scenario without a virtual gateway when the customer use the dedicated circuit as the main circuit and Internet as a backup connection. Caution by using this design only when the bandwidth of the both circuits are similar. This would not be
advisable if the connection speed of the dedicated circuit is higher than Internet circuit, as it may lead to not properly utilizing the circuits.

**Multi-Cloud Mesh**

*Figure 74 – Multi-Cloud Mesh*
5.8.4 Configuring Hub Mesh

To configure a hub mesh topology, in the global dashboard, navigate to Network Services > SD-WAN Overlay > Config icon > Mesh > Hub mesh. The path is displayed in the following image.

![Hub Mesh Configuration Image]

To configure a hub mesh topology for the SD-WAN overlay network, complete the following steps:

- Under Network Services > SD-WAN Overlay > Config icon > Click the Mesh tab.
- To add a mesh topology, expand Hub Mesh and click +. Provide a name to the new topology in the Hub Mesh Topology table, and click OK.
- Select the newly added mesh topology and click the edit icon.
- Select the groups to be included in the Hub mesh topology. Click Apply.

The following are the important guidelines for a hub mesh topology:

**NOTE**
- Up to eight hub groups are allowed.
- A hub site can be configured in only one mesh topology.
5.8.5 Hub Mesh Map

Aruba Central provides a separate dashboard to monitor the status of tunnels and routes. In the global dashboard, navigate to **Network Services > SD-WAN Overlay** and click the List view to monitor overlay tunnels and routes.

If the branch group is configured with a hub mesh topology, you can see the hub mesh links between the data centers in SD-WAN map view. Hover over the tunnel link to view the number of active tunnels between the data centers.

![Figure 76 – Hub Mesh Topology](image)

The source and destination Site details, tunnel state, and rekey information are presented in a pop-up window upon clicking the hub mesh tunnel link.

![Figure 77 – Hub Mesh Tunnels Details](image)
When a branch group with hub-mesh configuration is selected, its geographical representation is seen on the map. Under map view are displayed the tunnels and routes corresponding to the branch group.

Figure 78 – Hub Mesh Preferences
5.9 Manual Hub Mesh

Aruba supports mesh topologies between the on-premise hubs (VPNC) or cloud hubs (vGW). In a mesh topology, all or partial hubs are connected to the other hubs. The hubs are connected to one another through site-to-site IPsec tunnels. Using a mesh, we can connect any type of hub and create an overlay mesh between all the data centers.

Mesh topology is highly redundant by creating a mesh of tunnels over all available uplinks and using BGP mechanisms of exchanging routes between each peer.

Figure 79 – Hub Mesh
For an easier identification of the hubs and a simplified configuration, it is recommended to create a loopback address on each hub and source the site-to-site tunnels and the BGP peering from the loopback address. Set a loopback IP address from **Gateway Management > General > Loopback Interface**:

![Figure 80 – Configure Loopback Address](image)

**NOTE** Remember, this step has to be done for all hubs which will be configured as part of hub mesh.

The next step would be to create the IPSec tunnels between the hubs from **Gateway Management > VPN > Site to Site**. For this setup, the following are the recommended parameters for source/destination network:

- Source network/mask: `<Local Loopback IP>/32`
- Destination network/mask: `<Peer Loopback IP>/32`
### Site to Site IPSec

<table>
<thead>
<tr>
<th>Name:</th>
<th>to-us-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled:</td>
<td>✓</td>
</tr>
<tr>
<td>Priority:</td>
<td>202</td>
</tr>
<tr>
<td>Source network type:</td>
<td>IP Address</td>
</tr>
<tr>
<td>Source network:</td>
<td>10.2.100.1</td>
</tr>
<tr>
<td>Source subnet mask:</td>
<td>255.255.255.255</td>
</tr>
<tr>
<td>Destination network type:</td>
<td>IP Address</td>
</tr>
<tr>
<td>Destination network:</td>
<td>10.1.100.2</td>
</tr>
<tr>
<td>Destination subnet mask:</td>
<td>255.255.255.255</td>
</tr>
<tr>
<td>IKE version:</td>
<td>v2</td>
</tr>
</tbody>
</table>

#### IKE policy:

- **NAME**
  - default.aes

#### Transforms:

- 

#### Remote peer addressing:

- **Static**

#### Peer gateway type:

- **IP Address**

#### Peer gateway IPv4:

- 13.52.166.142

#### VLAN:

- 4094
Figure 81 – Site to Site

For the rest of the tunnel parameters, use the following:

- Peer Gateway IPv4: Public IP address of the hub
- VLAN: 4094
- Trusted, Enforce NAT-T, Pre-Connect, Force tunnel
- PFS Group 14
The last step is to configure to establish an eBGP peering between the hubs and to start exchanging prefixes. Enable BGP from **Gateway Management > Routing > BGP > General**:

![Enable BGP](image1)

**Figure 82 – Enable BGP**

![BGP Configuration](image2)

**Figure 83 – BGP Configuration**

Where allowall route-map is matching all prefixes received or advertised by the peer, the route map can be modified to provide a higher control of advertised and received prefixes. For example, to advertise and receive
only ClearPass Policy Manager management address prefix or an Active Directory prefix, see the following figure.

<table>
<thead>
<tr>
<th>IP Routes</th>
<th>Policy-Based Routing</th>
<th>NextHop Configuration</th>
<th>OSPF</th>
<th>BGP</th>
<th>Overlay Routing</th>
</tr>
</thead>
</table>

- **General**
- **Neighbors**
- **Advertise Networks**
- **Community List**
- **Route Map**

### Route maps

<table>
<thead>
<tr>
<th>NAME</th>
<th>SEQUENCE</th>
<th>ACTION</th>
<th>MATCH IP</th>
<th>MATCH NEXTHop</th>
<th>MATCH COMMUNITY</th>
<th>SET</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow all</td>
<td>10</td>
<td>permit</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

*Figure 84 - Route-map Applied to BGP Neighbor*
5.10 Multipath Scenario

Starting with the Aruba SD-WAN 8.5.0.0-2.0 release, BGP multipath can be enabled on the Aruba gateway. Traffic is load balanced across paths using Equal-Cost Multi-Path (ECMP) load balancing.

BGP paths with the same BGP path selection attributes (Local preference, AS Path, Origin code, MED, IGP metric) qualify for multipath next-hops.

**NOTE**  
AS Path can be different, but AS length should be the same in order to qualify an AS path as equal cost path.

**Example Scenario** — To connect to a AWS Transit Gateway, we need to connect using two IPsec tunnels. Each AWS IPsec tunnel can do 1.25Gbps throughput (Source: AWS). Using multipath, we can increase the traffic sent towards the AWS Transit Gateway and achieve up to 4Gbps throughput in the largest vGW.
Control plane BGP protocol has no limit on number of paths received from BGP peers. However, there is a limit on number of ECMP routes that datapath supports based on platform type. ECMP limit per all platform (70xx, 90xx, 72xx, vGW) is 16.

Enabling multipath is global and the configuration is applicable for all the BGP neighbors.
To verify if BGP multipath computation is enabled, go to All devices > Gateways > List of Online Gateways > <Select your device> and then, click the BGP tab and select Neighbors from the drop-down. Multipath computation can be verified per each BGP neighbor.

![Figure 87 - ECMP Enabled](image)

**Figure 87 - ECMP Enabled**

BGP Details > Routes table will show all the paths from which a prefix is learned. The paths selected for multipath are marked with “★” in the output.

![Figure 88 - ECMP Paths in BGP table](image)

**Figure 88 - ECMP Paths in BGP table**
To verify multipath routes installed in the routing table, go to All devices > Gateways > List of Online Gateways > <Select your device> and then click the Routing tab and filter by protocol to display only BGP installed routes.

![Figure 89 - ECMP Paths in the Routing Table](image)

“show ip route” shows the selected paths for a certain prefix.

CLI Output:

```
(London-DC-2) #show ip route bgp

Codes: C - Connected, O - OSPF, IA - OSPF Inter Area, E1 - OSPF External Type 1,
       E2 - OSPF External Type 2, B I - BGP Interior, B E - BGP Exterior, S - Static,
       V - RAPNG VPN/Branch, I - Crypto-Cfgset, N - Not Redistributed, Bc - Cloud Overlay Protocol.

   B  10.127.30.2/32   [100/0] ipsec map to-tgw-1
       [100/0] ipsec map to-tgw-2
   B  10.127.30.1/32   [100/0] ipsec map to-tgw-1
       [100/0] ipsec map to-tgw-2
   B  169.254.115.124/30  [100/0] ipsec map to-tgw-1
       [100/0] ipsec map to-tgw-2
   B  169.254.57.88/30   [100/0] ipsec map to-tgw-1
       [100/0] ipsec map to-tgw-2
   B  10.127.26.0/27     [100/0] ipsec map to-tgw-1
       [100/0] ipsec map to-tgw-2
   B  172.101.1.64/27    [100/0] ipsec map to-tgw-1
       [100/0] ipsec map to-tgw-2
   B  10.100.1.1/32      [100/0] ipsec map to-tgw-1
       [100/0] ipsec map to-tgw-2
   B  10.22.251.32/27    [100/0] ipsec map to-tgw-1
       [100/0] ipsec map to-tgw-2
   B  10.22.251.96/27    [100/0] ipsec map to-tgw-1
       [100/0] ipsec map to-tgw-2
   B  10.22.251.64/27    [100/0] ipsec map to-tgw-1
       [100/0] ipsec map to-tgw-2
```

| B 10.11.0.0/16 | 100/0 ipsec map to-tgw-1 |
| 100/0 ipsec map to-tgw-2 |
6 Reference

- Aruba SD-Branch User Documentation:
  https://help.central.arubanetworks.com/latest/documentation/online_help/content/gateways/cfg/overlay-orchestration/sdwan-oto-oro.htm

- Aruba SD-WAN with Public Cloud (AWS) Tech Note:
  https://asp.arubanetworks.com/downloads/documents/RmlsZToyNWI4ZTBIY1iOTM5LTExZTktODZIOTC1hZjVlZjg1MzBkMzA%3D

- Aruba SD-WAN with Public Cloud (Azure) Tech Note:
  https://asp.arubanetworks.com/downloads/documents/RmlsZTpjOGM1OGRxYS04OGjjLTExZWEtODIwZC03M2Y4MDNkYml3YTY%3D