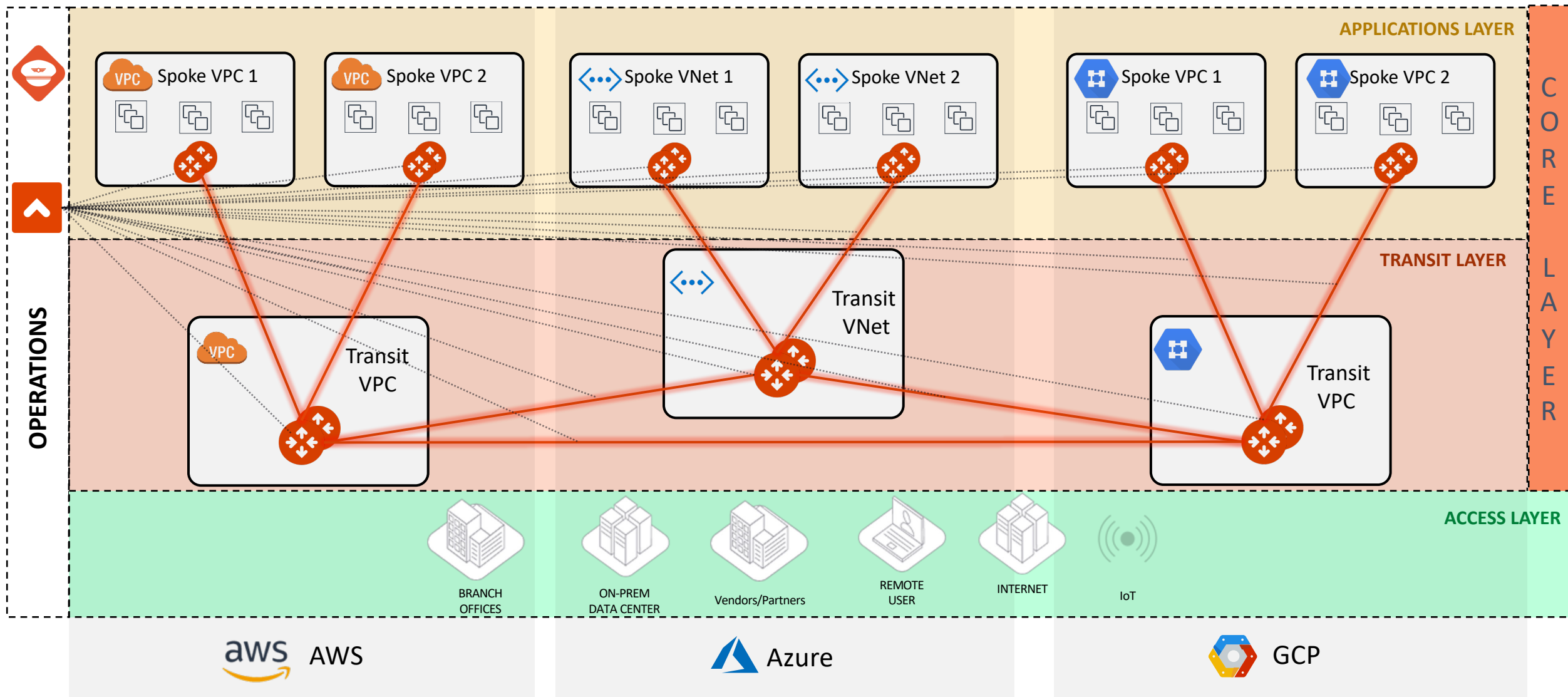


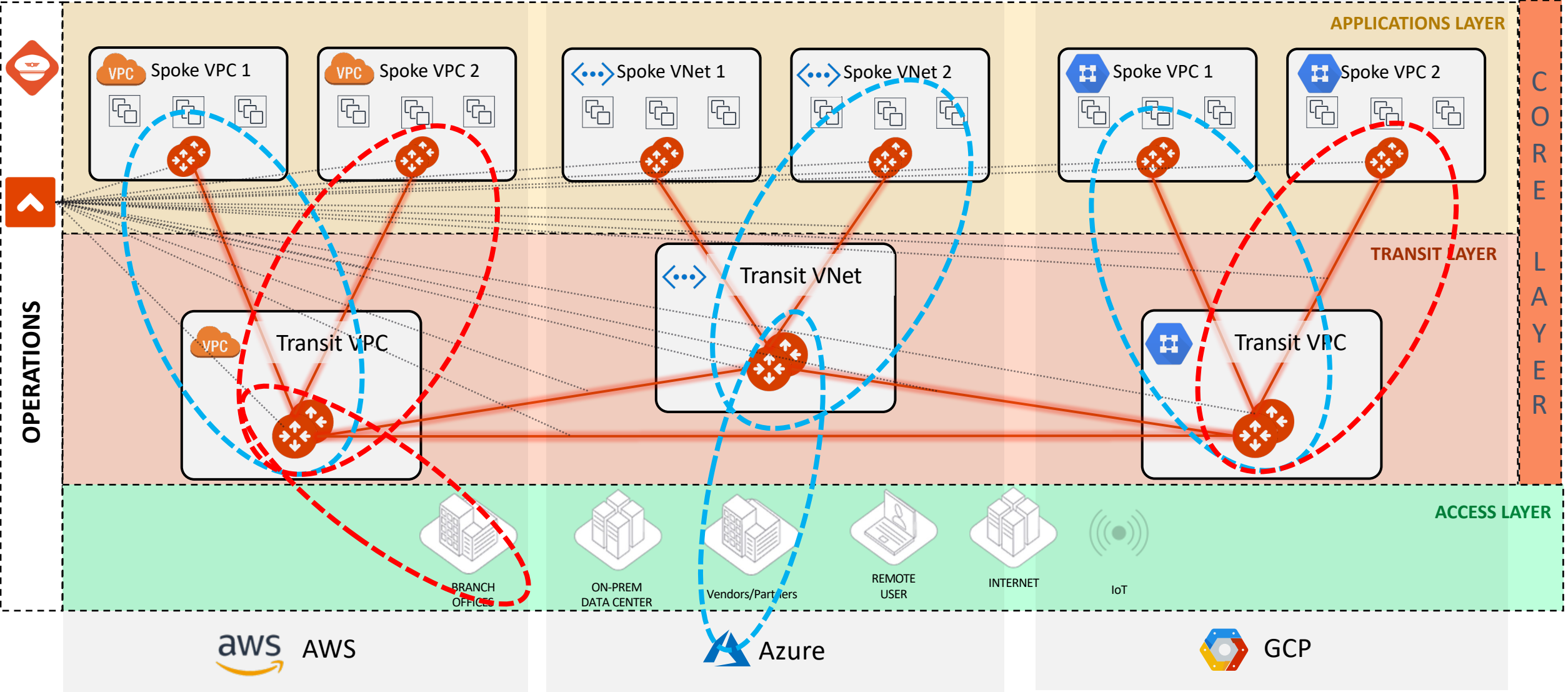


Network Segmentation

MCNA Deployment: the Foundations

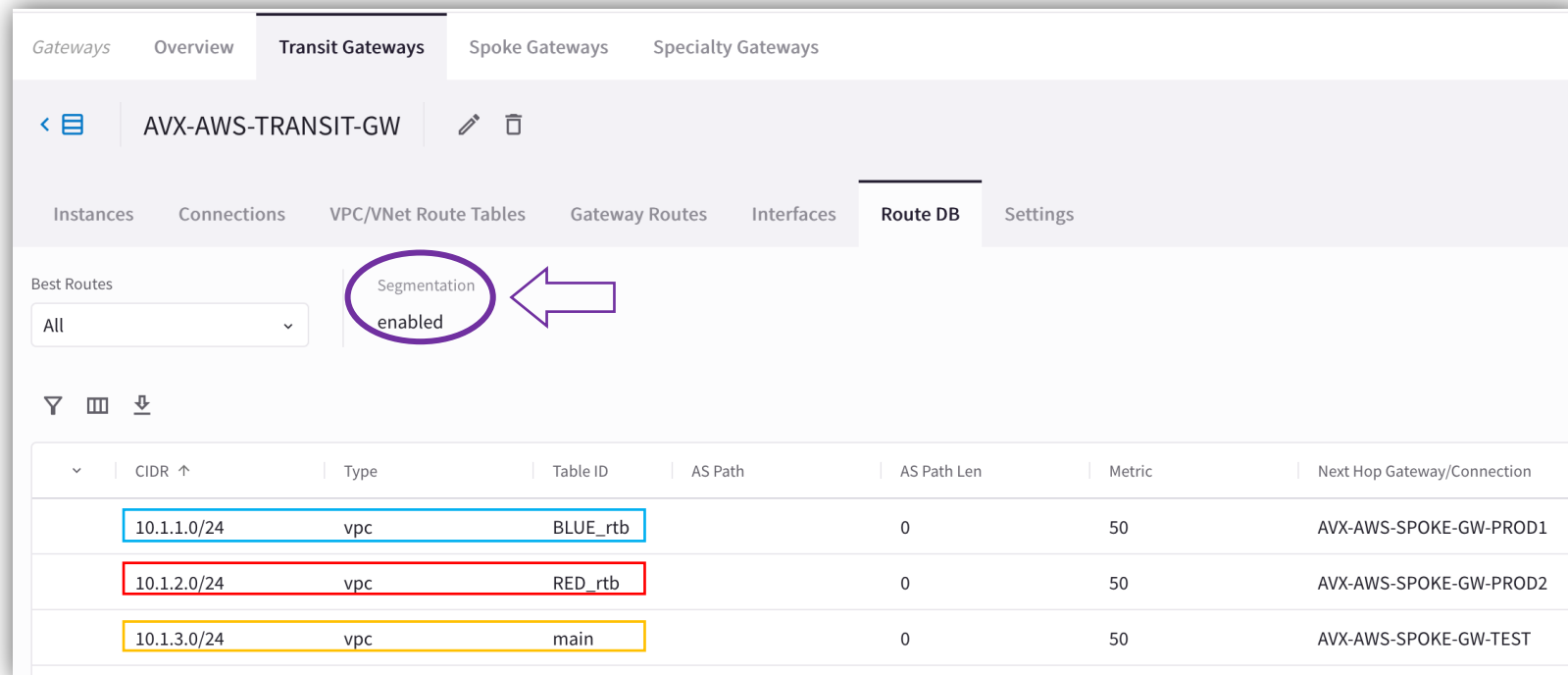


Global Segmentation with Network Domains



Order of Operations for activating the Network Segmentation

- 1) Enable Network Segmentation on the relevant Transit Gateway(s)
- 2) Create Network Domains (aka Segments)
- 3) Associate Spoke Gateways and/or Site2Cloud connections to the Network Domains
- 4) Apply the Connection Policy (*optional*)

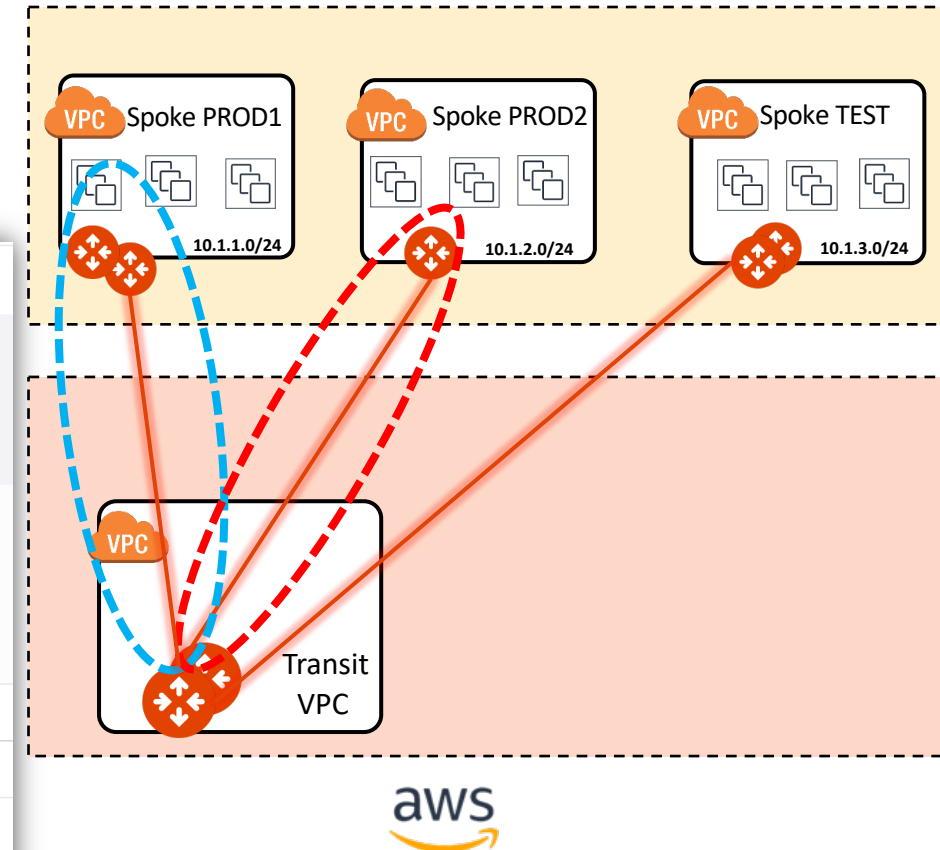


Best Routes

All

Segmentation enabled

CIDR	Type	Table ID	AS Path	AS Path Len	Metric	Next Hop Gateway/Connection
10.1.1.0/24	vpc	BLUE_rtb		0	50	AVX-AWS-SPOKE-GW-PROD1
10.1.2.0/24	vpc	RED_rtb		0	50	AVX-AWS-SPOKE-GW-PROD2
10.1.3.0/24	vpc	main		0	50	AVX-AWS-SPOKE-GW-TEST



PATH: COPILOT > Cloud Fabric > Gateways > Transit Gateways > select the relevant GW > **Route DB** (equivalent of RIB)

Multiple Routing Domains on the Transit GW

Gateways Overview **Transit Gateways** Spoke Gateways Specialty Gateways

< AVX-AWS-TRANSIT-GW

Instances Connections VPC/VNet Route Tables **Gateway Routes** Interfaces Route DB Settings

Gateway Instance: AVX-AWS-TRANSIT-GW Network Domain: **BLUE**

	Destination	Via	Interface	Next Hop IP	Next Hop Gateway	Metric
^	default	blackhole				400
^	10.1.1.0/24		tun-034790D0-0	3.71.144.208	AVX-AWS-SPOKE-GW-PROD1	100
			tun-129D3D38-0	18.157.61.56	AVX-AWS-SPOKE-GW-PROD1-1	100
	10.1.1.0/24		tun-0A0B0068-0	10.11.0.104	AVX-AWS-TRANSIT-GW-1	200

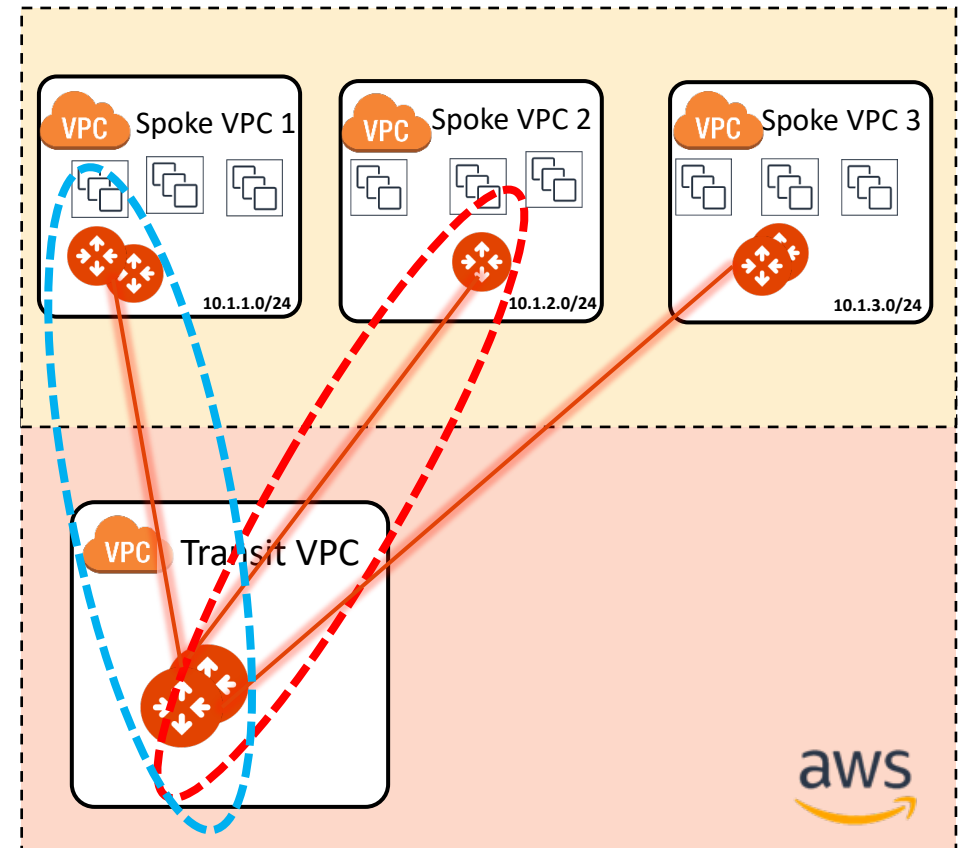
Gateways Overview **Transit Gateways** Spoke Gateways Specialty Gateways

< AVX-AWS-TRANSIT-GW

Instances Connections VPC/VNet Route Tables **Gateway Routes** Interfaces Route DB Settings

Gateway Instance: AVX-AWS-TRANSIT-GW Network Domain: **RED**

	Destination	Via	Interface	Next Hop IP	Next Hop Gateway	Metric
^	default	blackhole				400
	10.1.2.0/24		tun-0349032B-0	3.73.3.43	AVX-AWS-SPOKE-GW-PROD2	100
	10.1.2.0/24		tun-0A0B0068-0	10.11.0.104	AVX-AWS-TRANSIT-GW-1	200



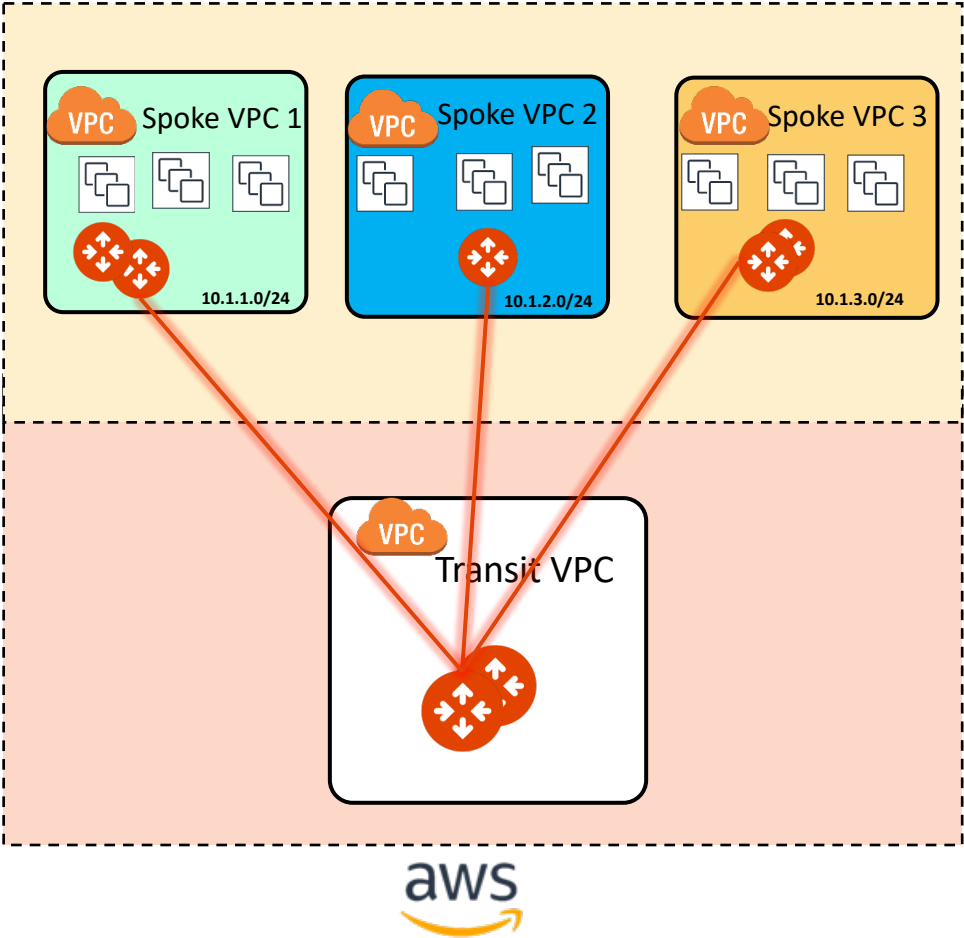
- A single Spoke gateway or a Cluster of Spoke Gateways can be associated to a unique domain!
- **PATH:** COPILOT > Cloud Fabric > Gateways > Transit Gateways > select the relevant GW > **Gateway Routes** and then filter based on the network domain (i.e. VRF)

CAVEAT: The specific Network Domain view (aka vrf) is only available on the Transit GW. The Spoke GW has only the main routing table (aka grt).

Connection Policy

- The Connection policy allows the **inter-domain** communication or **inter-segment** communication (is akin to the *vrf leaking* from the MPLS technology).
- The connection policy establishes a **bidirectional** connectivity (merging the network domains' RTBs).
- In the example on the right, there are three domains:
 - ❑ Green
 - ❑ Blue
 - ❑ Yellow
- If the Blue domain acts as the Shared Services Domain, **It will be connected to both the GREEN domain and the YELLOW domain.**

Name	Associations	Connected To
YELLOW	AVX-AWS-SPOKE-GW-TEST	BLUE
GREEN	AVX-AWS-SPOKE-GW-PROD1	BLUE
BLUE	AVX-AWS-SPOKE-GW-PROD2	GREEN, YELLOW



- **CAVEAT:** a connection policy can't be applied on the main RTB (aka Global Routing Table).

Tools for Operating your Network Segmentation

Network Segmentation Visibility

- CoPilot: verify the Network Domains

PATH: COPILOT > Networking > Network Segmentation > Network Domains

The screenshot displays the Aviaatrix CoPilot interface. On the left is a dark sidebar with a search bar and a menu containing: Dashboard, Cloud Fabric, Networking (highlighted with a red box), Network Segmentation (highlighted with a red box), Connectivity, Security, SmartGroups, Cloud Resources, Monitor, Diagnostics, Billing & Cost, Administration, and Settings. The main content area shows the 'Network Segmentation' section with tabs for 'Overview' and 'Network Domains' (the latter is highlighted with a red box). Below the tabs are buttons for '+ Network Domain', 'Transit Gateways', and filter/download icons. A table lists network domains:

Name	Associations	Connected To
BU2	ace-azure-east-us-spoke2, + 1 more	
BU1	ace-gcp-us-east1-spoke1, + 3 more	

Overlaid on the right is a modal titled 'Configure Transit Gateways for Network Segmentation'. It includes a message: 'Show filters transit gateways have to be enabled to support network segmentation on them.' Below this is a table of transit gateways:

Name	Cloud	Region	IP Address Space	
ace-aws-eu-west-1-transit1	aws	eu-west-1	10.1.200.0/23	<input checked="" type="checkbox"/> Enabled
ace-azure-east-us-transit1	arm	East US	192.168.200.0/23	<input checked="" type="checkbox"/> Enabled
ace-gcp-us-east1-transit1	gcp	us-east1	172.16.200.0/23	<input checked="" type="checkbox"/> Enabled

At the bottom of the modal, it says 'Total 3 Transit Gateways'. The modal has 'Cancel' and 'Save' buttons at the bottom right.

Network Segmentation Visibility

- CoPilot: create/modify the Network Domains

PATH: COPILOT > Networking> Network Segmentation > Network Domains > pencil icon (edit)

The screenshot displays the AviaTrix CoPilot interface. On the left is a dark sidebar with a search bar and a menu containing: Dashboard, Cloud Fabric, Networking (highlighted with a red box), Network Segmentation (highlighted with a red box), Connectivity, Security, SmartGroups, Cloud Resources, Monitor, Diagnostics, Billing & Cost, Administration, and Settings. The main panel shows the 'Network Segmentation' section with tabs for 'Overview' and 'Network Domains' (the latter is highlighted with a red box). Below the tabs is a '+ Network Domain' button and a 'Transit Gateways' filter. A table lists network domains:

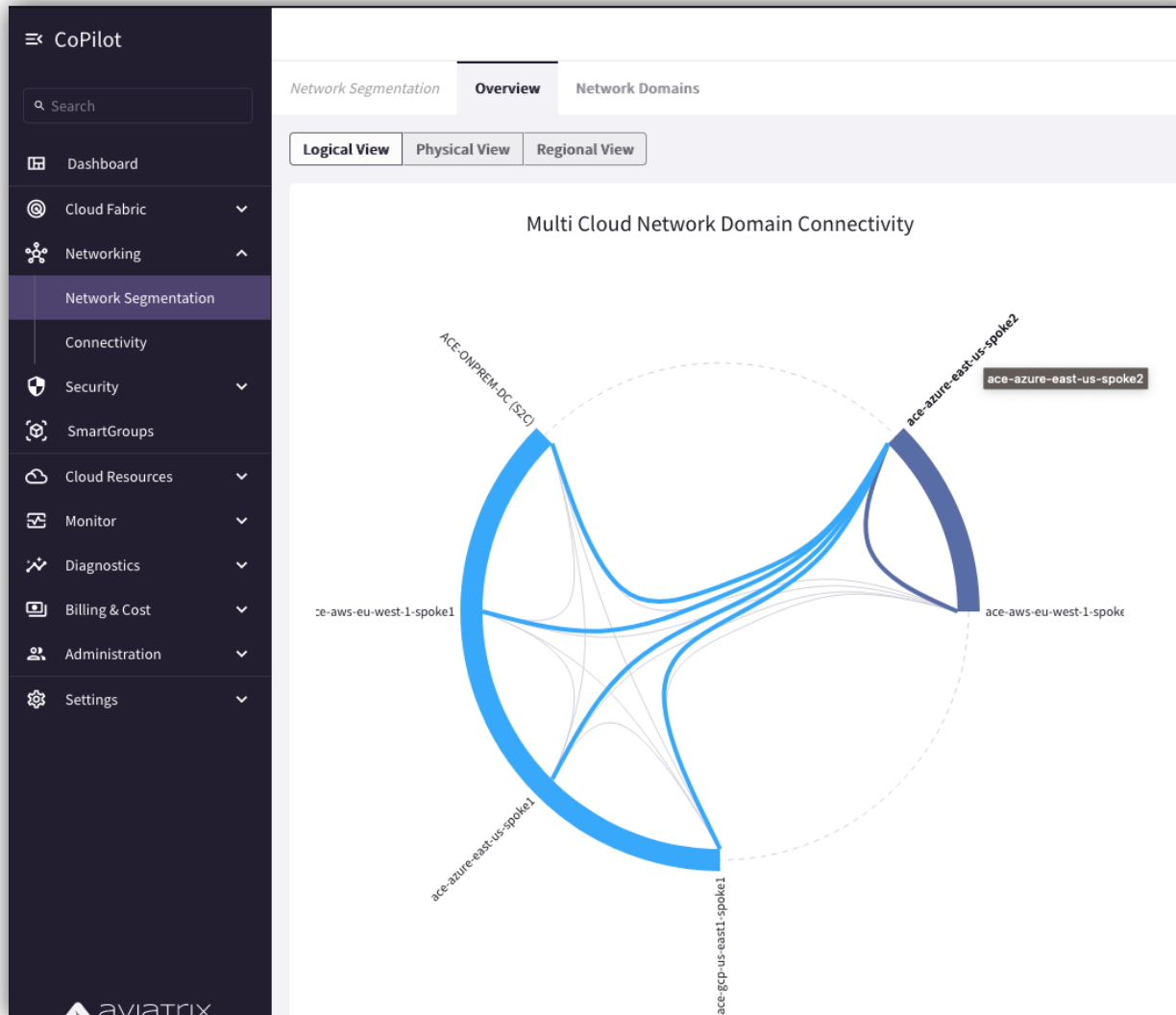
Name	Associations	Connected To
BU2	ace-azure-east-us-spoke2, + 1 more	
BU1	ace-gcp-us-east1-spoke1, + 3 more	

Red boxes highlight the 'Networking' menu item, the 'Network Segmentation' menu item, and the 'Network Domains' tab. A red arrow points to the pencil icon in the action column of the BU2 row. An 'Edit Network Domain: BU2' modal is open in the foreground, showing the 'Name' field with 'BU2', the 'Associations' field with 'ace-azure-east-us-spoke2' and 'ace-aws-eu-west-1-spoke2', and the 'Connect to Network Domain' field with 'BU1' selected. The modal has 'Cancel' and 'Save' buttons at the bottom right.

Network Segmentation Visibility

- CoPilot: verify the Network Relationships

PATH: COPILOT > Networking > Network Segmentation > Overview > Logical View





Next:
Lab 1 Network Domains &
Connection Policy