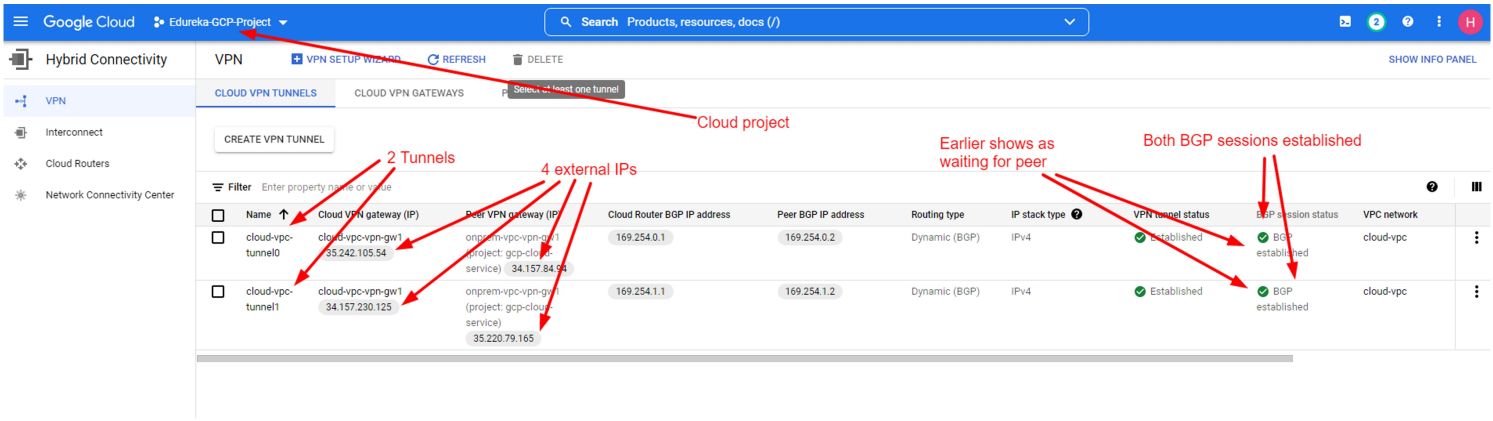
14-3 - Cloud VPN HA + BGP - Verification Steps - 10 min

30 June 2022 17:14

=============== Verify ====================

Switch to Cloud project and check the Routers and VPN tunnels - They should show Green button established



Name	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	Cloud Router BGP IP address	Peer BGP IP address	Routing type	IP stack type	VPN tunnel status	BGP session status	VPC network
cloud-vpc-tunnel0	cloud-vpc-vpn-gw1 35.242.105.54	onprem-vpc-vpn-gw1 (project: gcp-cloud-service) 34.157.84.94	169.254.0.1	169.254.0.2	Dynamic (BGP)	IPv4	✓ Established	✓ BGP established	cloud-vpc
cloud-vpc-tunnel1	cloud-vpc-vpn-gw1 34.157.230.125	onprem-vpc-vpn-gw1 (project: gcp-cloud-service) 35.220.79.165	169.254.1.1	169.254.1.2	Dynamic (BGP)	IPv4	✓ Established	✓ BGP established	cloud-vpc

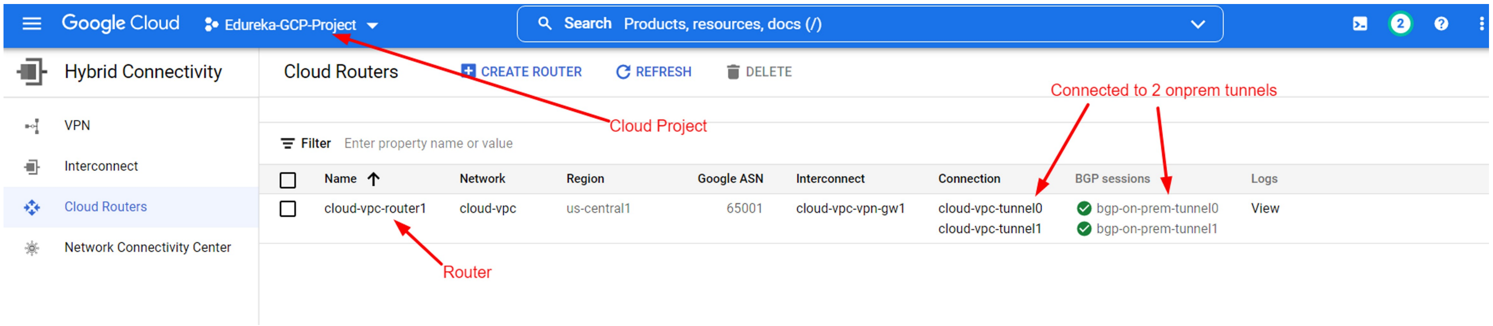
Cloud project

2 Tunnels

4 external IPs

Earlier shows as waiting for peer

Both BGP sessions established



Name	Network	Region	Google ASN	Interconnect	Connection	BGP sessions	Logs
cloud-vpc-router1	cloud-vpc	us-central1	65001	cloud-vpc-vpn-gw1	cloud-vpc-tunnel0 cloud-vpc-tunnel1	✓ bgp-on-prem-tunnel0 ✓ bgp-on-prem-tunnel1	View

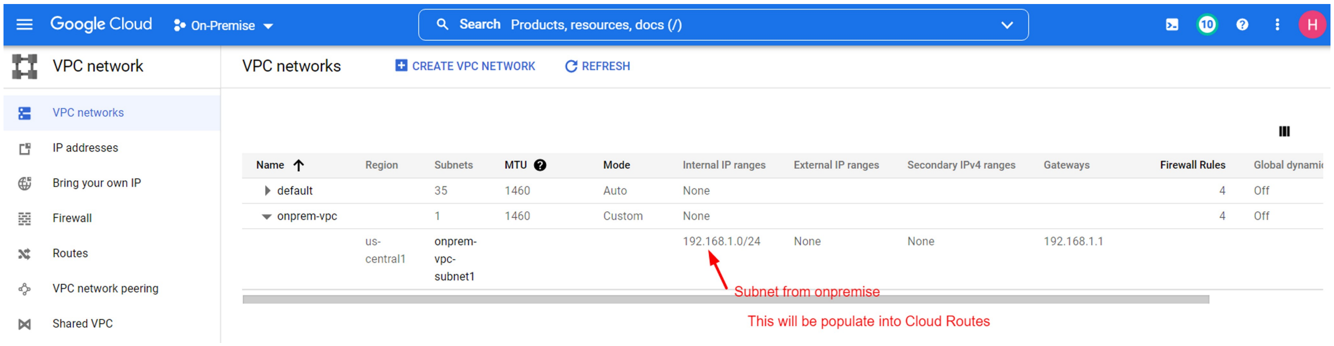
Cloud Project

Connected to 2 onprem tunnels

Router

SSH into cloud VM and Ping to private IP of onprem VM - It should work
SSH into onprem VM and Ping to private IP of cloud VM - It should work

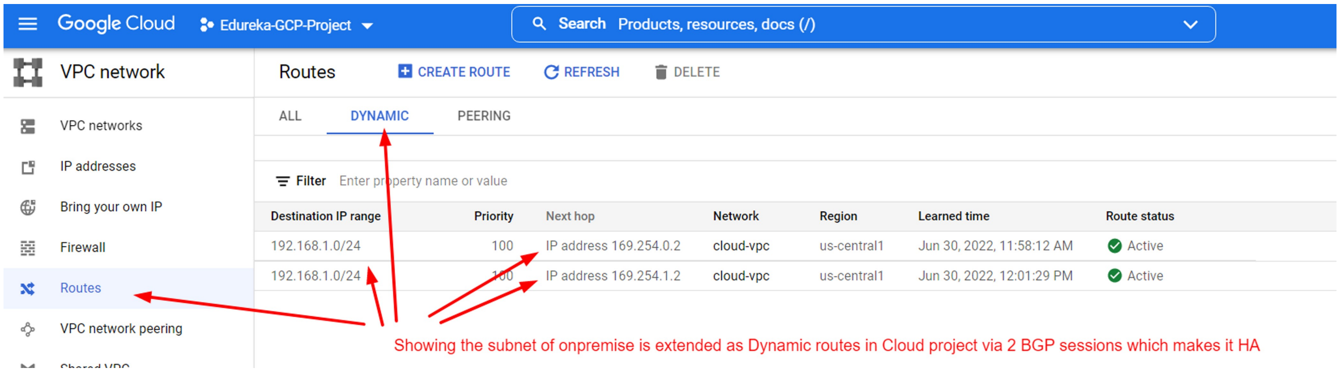
================= Dynamic Routing ============================



Name	Region	Subnets	MTU	Mode	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateways	Firewall Rules	Global dynami
default		35	1460	Auto	None				4	Off
onprem-vpc		1	1460	Custom	None				4	Off
	us-central1	onprem-vpc-subnet1			192.168.1.0/24	None	None	192.168.1.1		

Subnet from onpremise

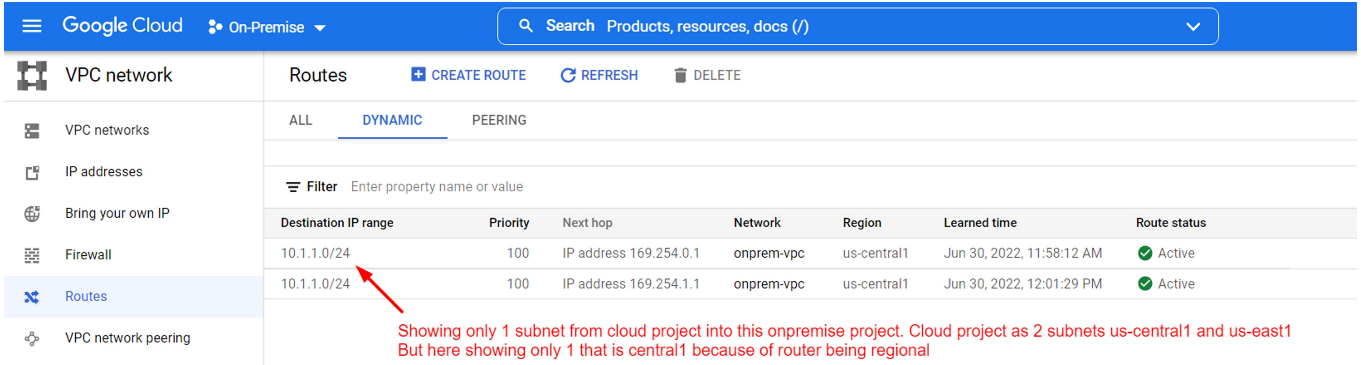
This will be populate into Cloud Routes



Destination IP range	Priority	Next hop	Network	Region	Learned time	Route status
192.168.1.0/24	100	IP address 169.254.0.2	cloud-vpc	us-central1	Jun 30, 2022, 11:58:12 AM	✓ Active
192.168.1.0/24	100	IP address 169.254.1.2	cloud-vpc	us-central1	Jun 30, 2022, 12:01:29 PM	✓ Active

Showing the subnet of onpremise is extended as Dynamic routes in Cloud project via 2 BGP sessions which makes it HA

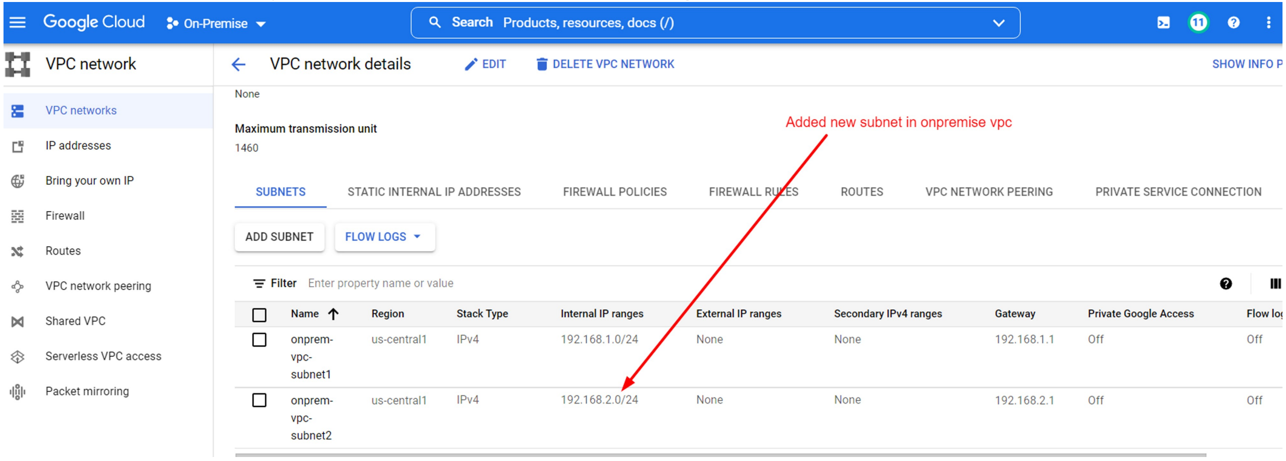
Vice-versa is also true for the given region only because the routes are controlled by **Router which is regional.**



Destination IP range	Priority	Next hop	Network	Region	Learned time	Route status
10.1.1.0/24	100	IP address 169.254.0.1	onprem-vpc	us-central1	Jun 30, 2022, 11:58:12 AM	✓ Active
10.1.1.0/24	100	IP address 169.254.1.1	onprem-vpc	us-central1	Jun 30, 2022, 12:01:29 PM	✓ Active

Showing only 1 subnet from cloud project into this onpremise project. Cloud project as 2 subnets us-central1 and us-east1
But here showing only 1 that is central1 because of router being regional

Add a new subnet in onpremise network with us-central1 region



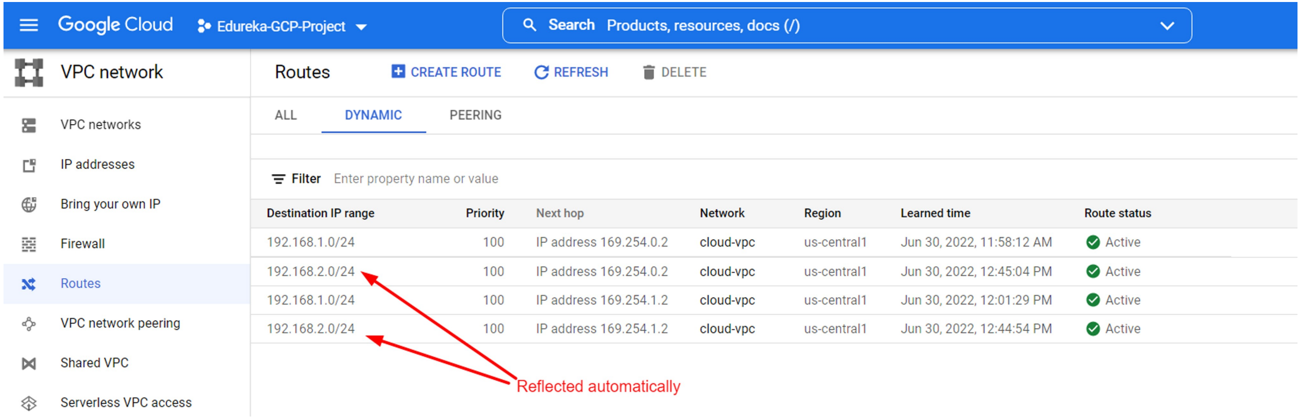
None

Maximum transmission unit
1460

Added new subnet in onpremise vpc

□	Name ↑	Region	Stack Type	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateway	Private Google Access	Flow lo
□	onprem-vpc-subnet1	us-central1	IPv4	192.168.1.0/24	None	None	192.168.1.1	Off	Off
□	onprem-vpc-subnet2	us-central1	IPv4	192.168.2.0/24	None	None	192.168.2.1	Off	Off

It is reflected in cloud project dynamic routes:



Destination IP range	Priority	Next hop	Network	Region	Learned time	Route status
192.168.1.0/24	100	IP address 169.254.0.2	cloud-vpc	us-central1	Jun 30, 2022, 11:58:12 AM	✓ Active
192.168.2.0/24	100	IP address 169.254.0.2	cloud-vpc	us-central1	Jun 30, 2022, 12:45:04 PM	✓ Active
192.168.1.0/24	100	IP address 169.254.1.2	cloud-vpc	us-central1	Jun 30, 2022, 12:01:29 PM	✓ Active
192.168.2.0/24	100	IP address 169.254.1.2	cloud-vpc	us-central1	Jun 30, 2022, 12:44:54 PM	✓ Active

Reflected automatically

Vice-versa is also true.

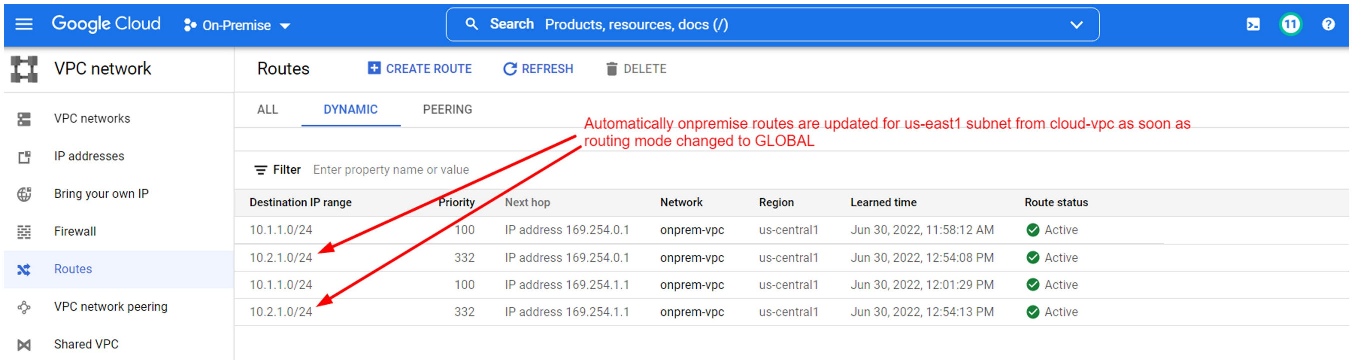
How can we make router to see all the regions and advertise them automatically?

We need to update the cloud router routing node as GLOBAL (default regional)
Check before: Shows routingMode: REGIONAL and x_gcloud_bgp_routing_mode: REGIONAL
gcloud compute networks describe cloud-vpc

Update routing mode:
gcloud compute networks update cloud-vpc --bgp-routing-mode GLOBAL

Now it shows: routingMode: GLOBAL and x_gcloud_bgp_routing_mode: GLOBAL

Check the us-east1 subnet route is reflected in onpremise dynamic routes:



Automatically onpremise routes are updated for us-east1 subnet from cloud-vpc as soon as routing mode changed to GLOBAL

Destination IP range	Priority	Next hop	Network	Region	Learned time	Route status
10.1.1.0/24	100	IP address 169.254.0.1	onprem-vpc	us-central1	Jun 30, 2022, 11:58:12 AM	✓ Active
10.2.1.0/24	332	IP address 169.254.0.1	onprem-vpc	us-central1	Jun 30, 2022, 12:54:08 PM	✓ Active
10.1.1.0/24	100	IP address 169.254.1.1	onprem-vpc	us-central1	Jun 30, 2022, 12:01:29 PM	✓ Active
10.2.1.0/24	332	IP address 169.254.1.1	onprem-vpc	us-central1	Jun 30, 2022, 12:54:13 PM	✓ Active

Quick Question - Can I create a VM using the new subnet created in on-premise VPC? - **No, because it is not shared. Only the routes are made available to that subnet from this cloud vpc dynamically using BGP session.**

What happens if I delete one of the tunnel:
Go to Cloud project and delete the tunnel0
Check the ping from cloud vm to onprem vm -> It should still work because it is HA

================END======================================