AWS TransitGateway:- It is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. As you grow the number of workloads running on AWS, you need to be able to scale your networks across multiple accounts and Amazon VPCs to keep up with the growth.

* Before transit gateway was introduced, there were two methods as below.

i) Transit VPC with IPSec.(Limits apply when you use this method)

Ii) VPN connection per VPC .(Limits apply when you use this method)

All methods above were combined/implemented with use of one AWS service called Transit Gateway after this concept was introduced.

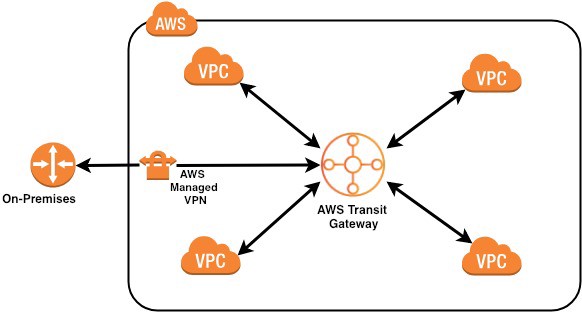
After TGW:-

i)Centralized hub for routing between Amazon VPC’s and on-premises to AWS.  
ii) TGW is an region-level construct today & 50 Gbps of bandwidth per availability zone in b/w VPC’s & 1.25 Gbps per VPN connection with ECMP.( **Equal-cost multi-path routing**), you can distribute traffic over multiple tunnels.

iii)10,000 route per gateway & 5000 Amazon VPC attachment per TGW.

iv) Multiple route tables per TGW to handle traffic in an effective manner.

Eg:-



**Note:-**

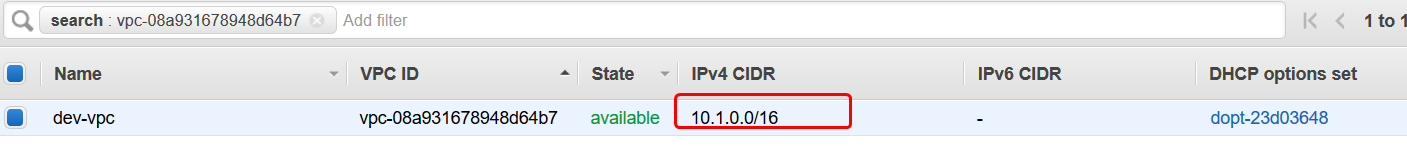
1. Attachment:- The connection from Amazon VPC and VPN to TGW
2. Association:- The route table used to route packets coming from an attachment(from an Amazon VPC and VPN).
3. Propogation:- The route table where the attachment’s routes are installed.

Please refer this screenshot /attachment if you have any confusion in creating CIDR ranges for different VPC’s

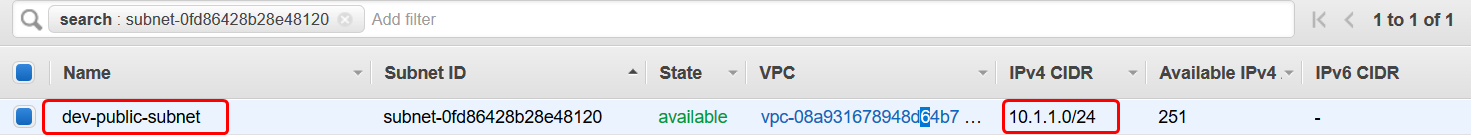


**Scenario-1:-** Create three VPC’s and associated subnets and route table and IGW and launch instances in respective VPC’s to test connectivity using telnet.

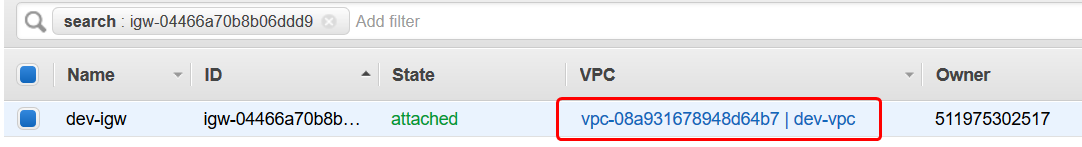
Step1:- Create VPC with name:- dev-vpc with CIDR as shown below.



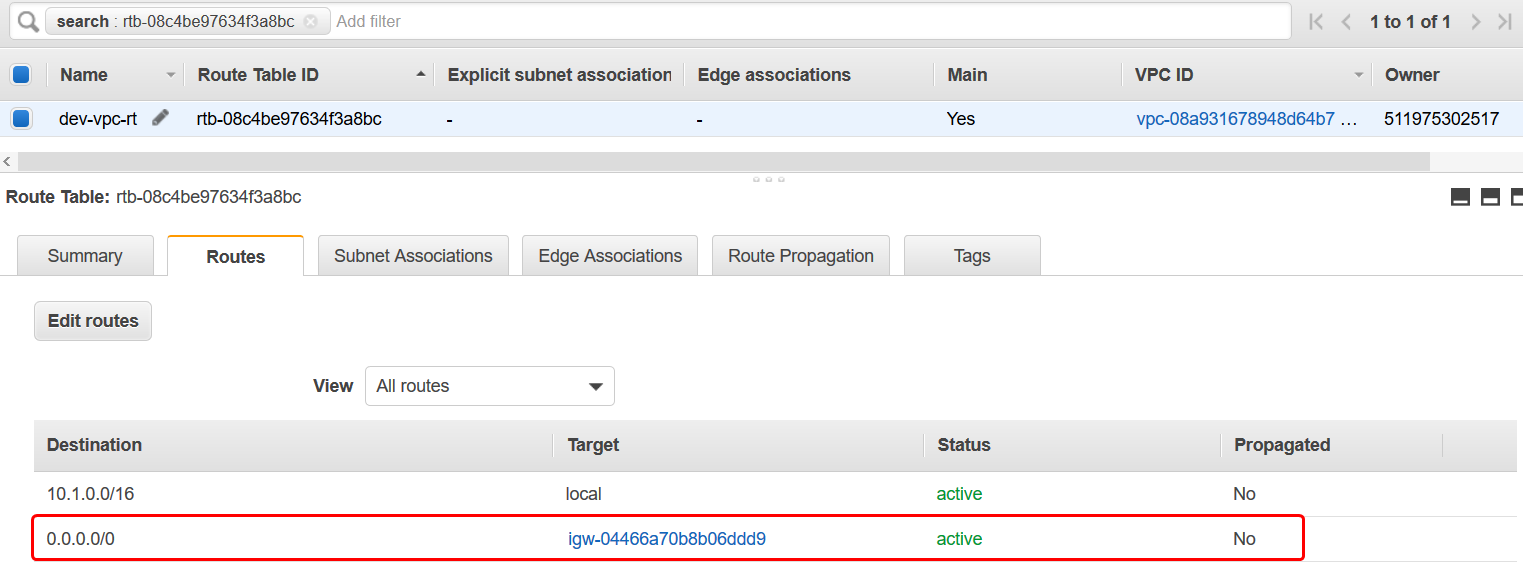
Step 2:- Create public subnet with CIDR as shown below.



Step 3:- Create IGW and attach it to respective VPC.



Step 4:- Go to route tables and edit the routes to Destination:- 0.0.0.0/0 & target it to Internet Gateway as shown below.



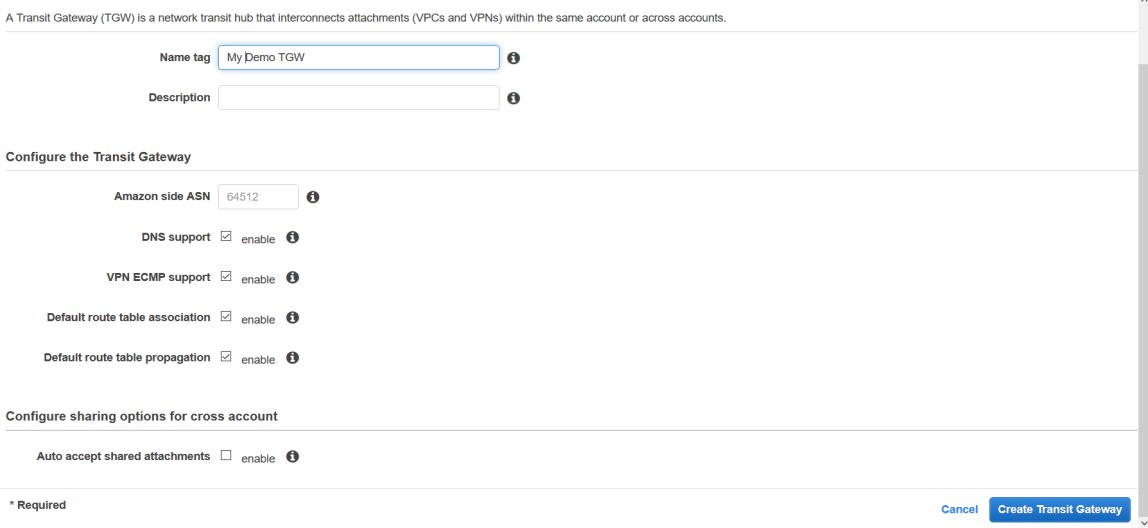
Follow the same process as we did for previous VPC and create other two VPC’s named qa-vpc & Shared-vpc.

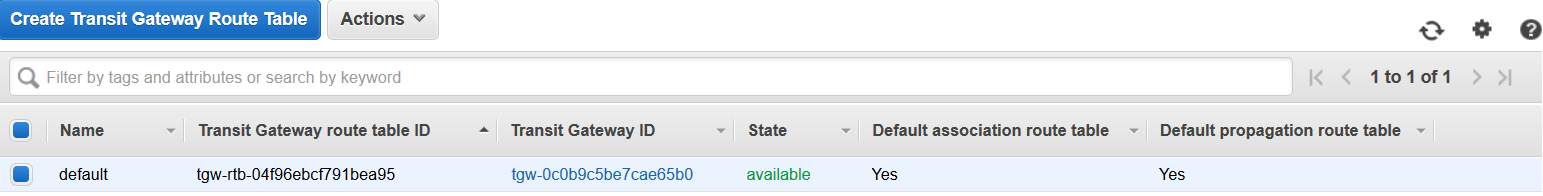
**Step5**:- Launch one instance in every VPC you created earlier.

Login to every instance and install telnet. (🡺 **yum install telnet**)

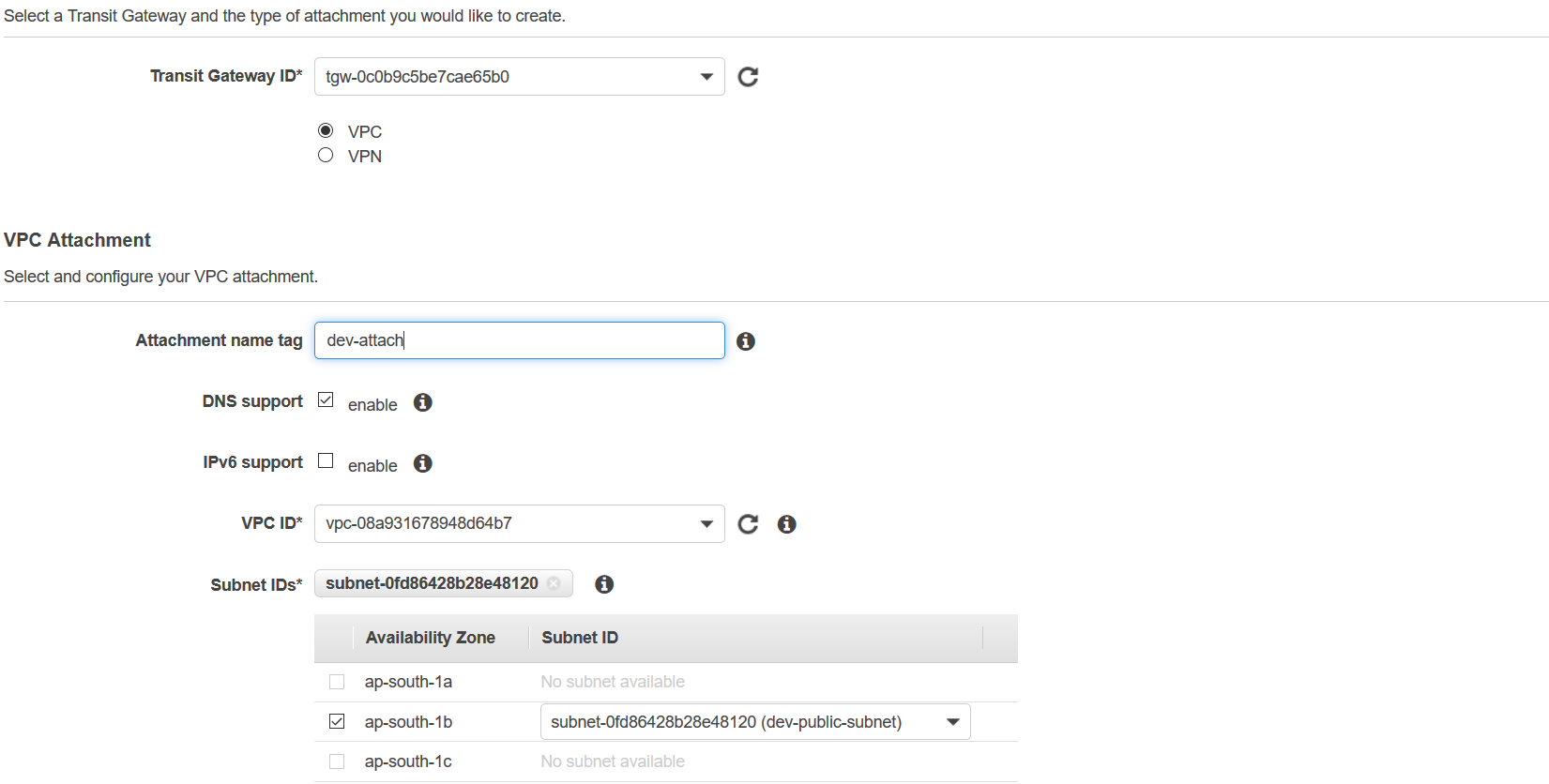
You cannot communicate with these instances because the VPC’s are not connected with each other.

Step5:- Create Tranist Gateway with name:- Demo TGW as show below screenshots & while creation of TGW, automatically one default TGW route table will be created & name it as default for your understanding.

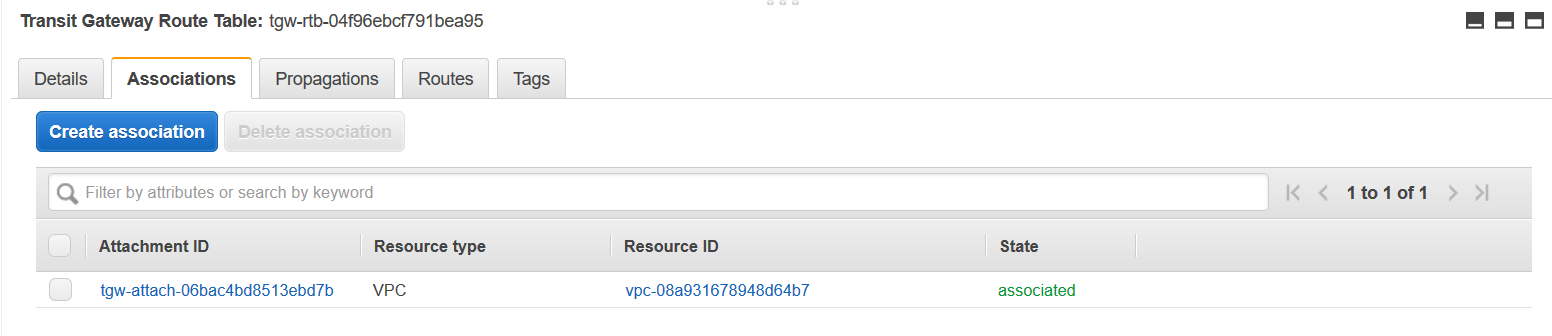


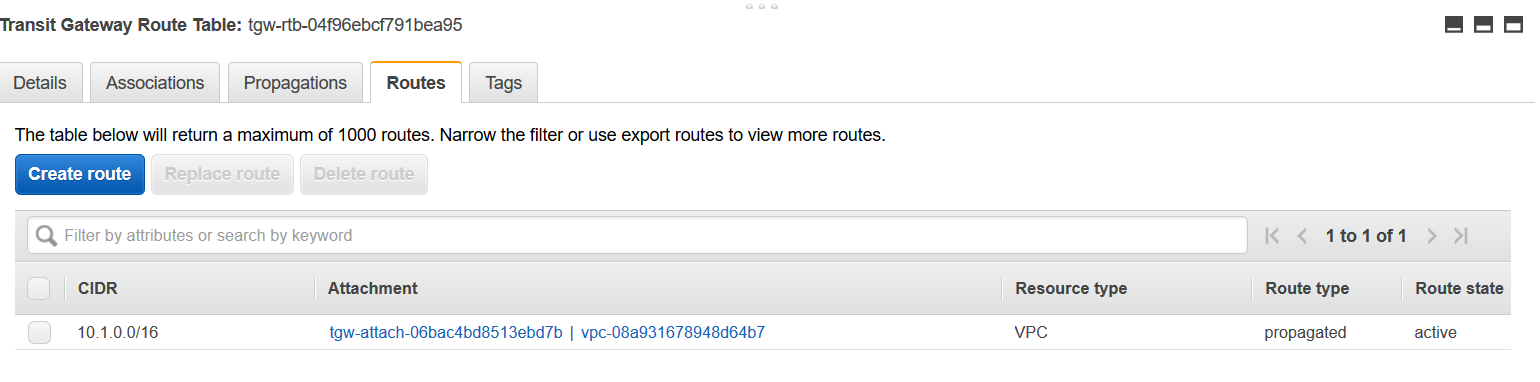


Step6:- Now create VPC attachments for Dev & QA VPC;s you created earlier. Refer screenshot below and at the end click on Create Transit Gatewy attachment. (To test connectivity b/w different VPC’s).



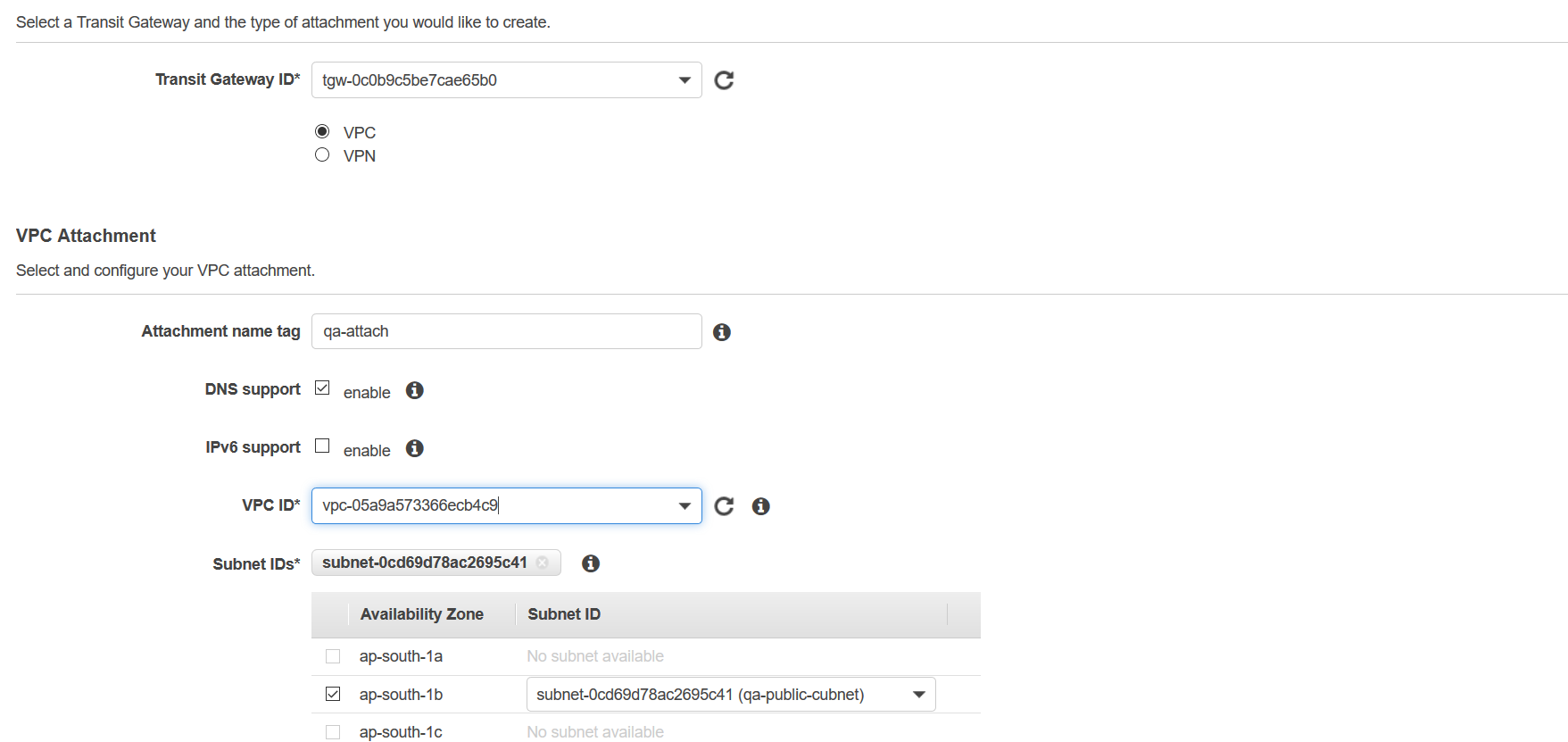
If you go & check the associations and propogations and rouites in Transit Gateway route table, you can see those which are updated automatically as seen in screenshot below.





Note:- While creating Transit Gateway attachments, make sure you have selected respective VPC’s.

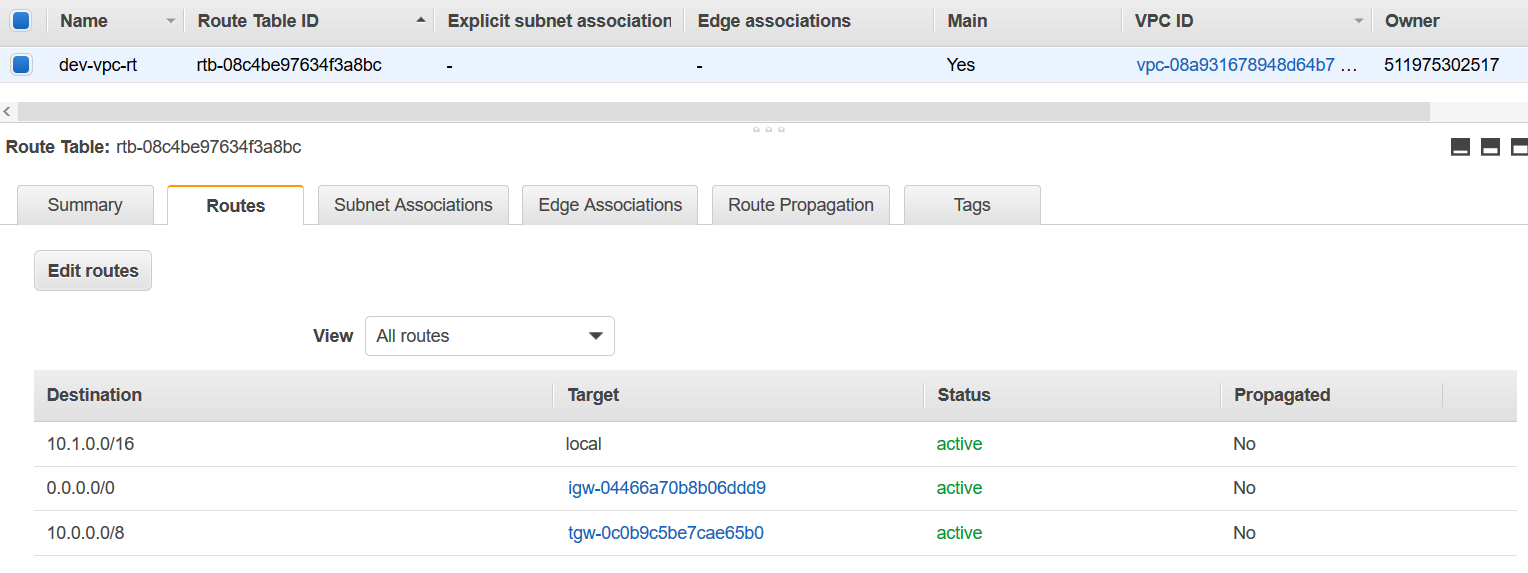
Step7:- Create one more TGW attachment for Qa-VPC you created earlier.



Step8:- Now perform the test connectivity b/w Dev-VPC & QA-VPC as shown below.

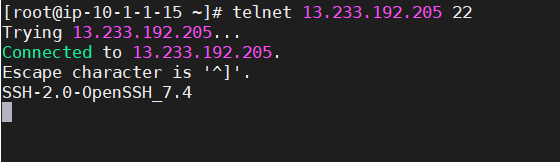
Login to respective instance and type command:- telnet with IP of instance.

But still VPC’s can’t communicate with each other, so you have to go to every VPC route tables of respective VPC’s and add **10.0.0.0/8** to Transit Gateway as shown below.

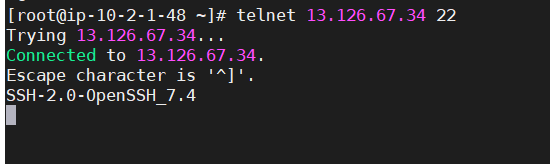


Do the same thing in QA-VPC route table also & now you can test the connectivity b/w both VPC’s. If you get the response as shown in screenshot, then both the VPC;s are communicating successfully.

1. telnet IP address port number(SSH)

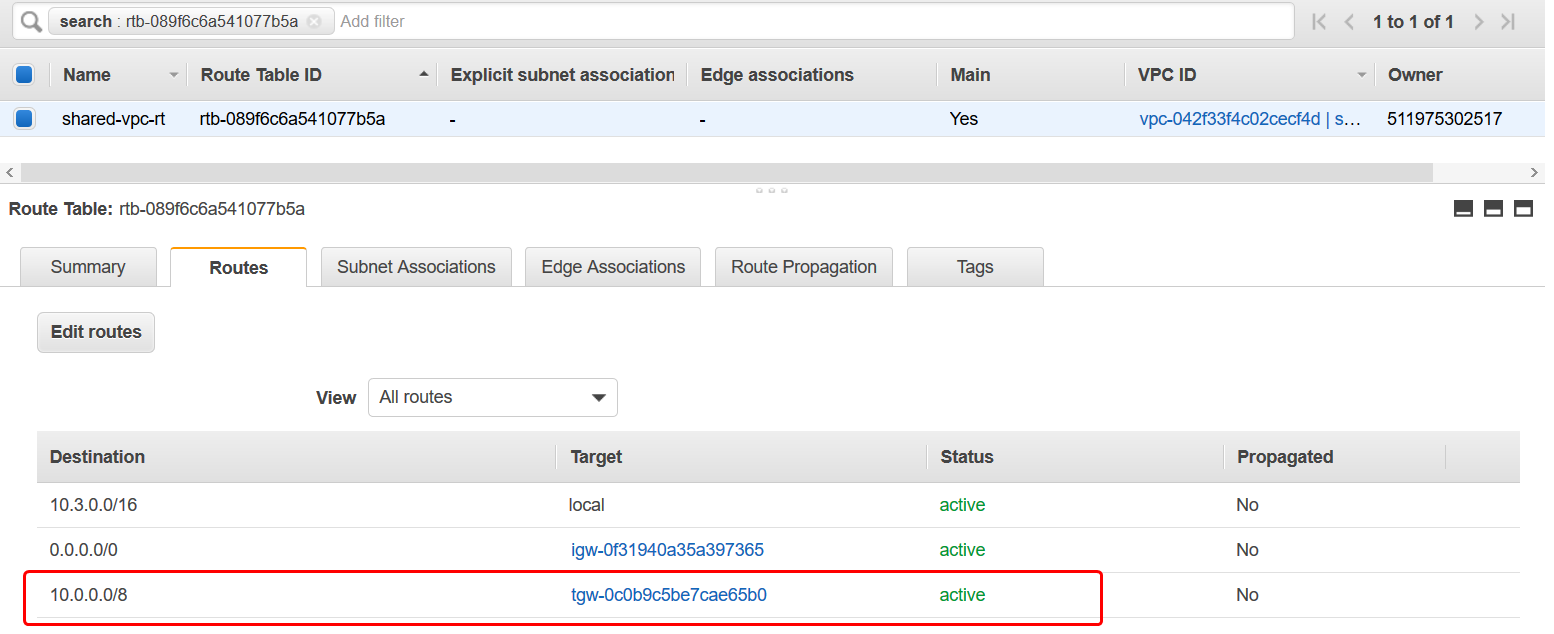


ii)



The above screenshot tell that we are able to communicate with the servers launched in Dev-VPC and QA-VPC.

Step 9:- Create transit gateway attachment for one more VPC(Shared-VPC) and add the routes 10.0.0.0/8 in VPC route table and route it to Transit Gateway as shown below.

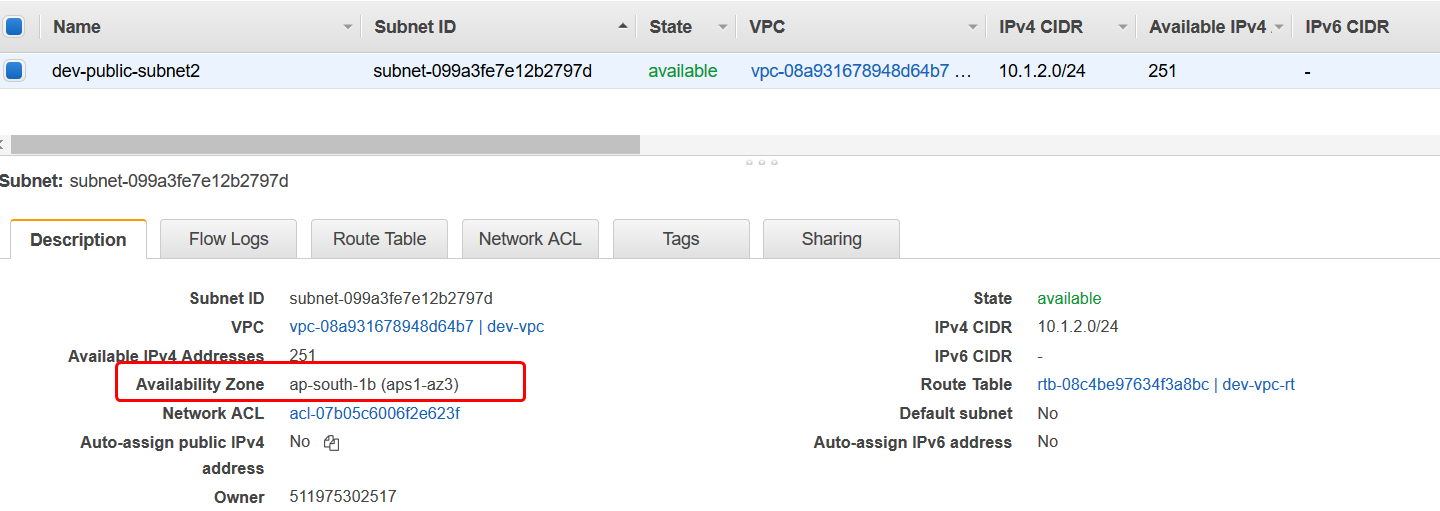


Finally, you can communicate with all three VPC’s with each and every other VPC’s.

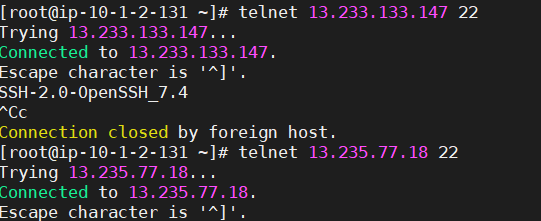
**Note:- Additional testing to check the different scenarios:-**

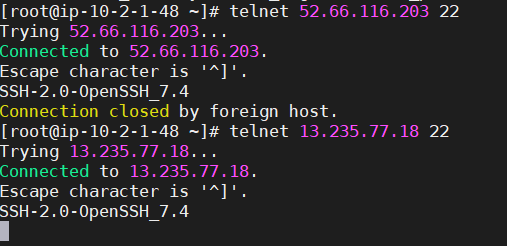
1. Create a new subnet in existing availability zone of Dev-VPC and create one VM in same VPC and check all the connectivity b/w both QA & Shared.

Step1:- Go to subnets and create one more public subnet in same VPC same availability zone where you created first subnet for Dev-VPC as shown below.



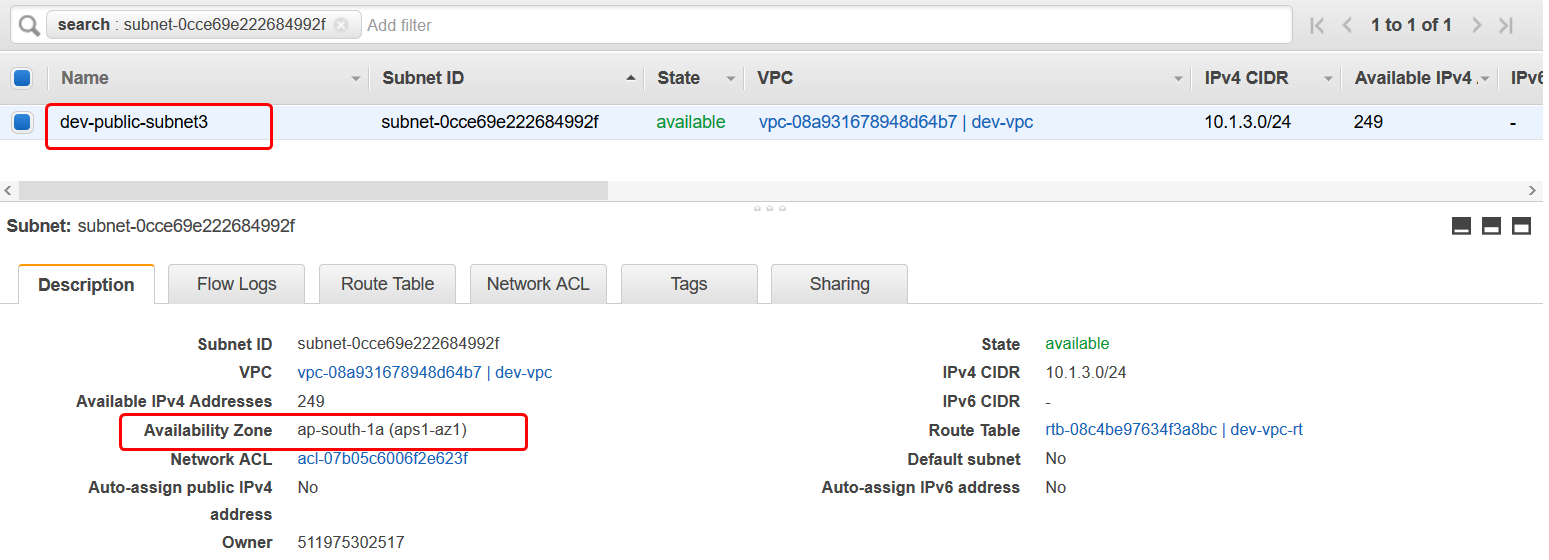
Since we are using main route table, so no need to modify any routes and also in Transit Gateway attachments of the respective VPC.. If you login and perform telnet with IP address of all servers from any one server. It will show the o/P as below.



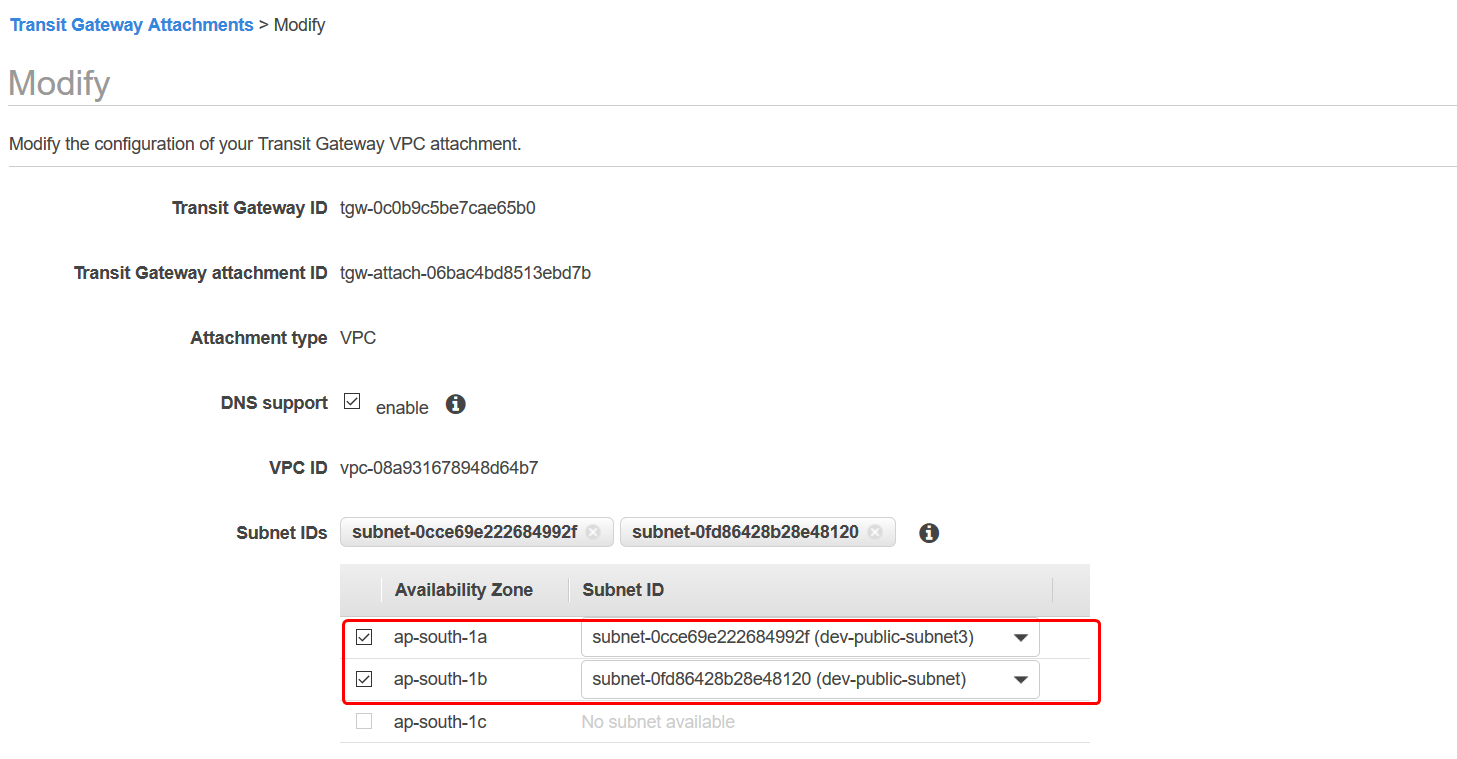


Note:- Any subnets coming under same availability zone & same VPC, no need to any changes in route table & Transit Gateway attachments.

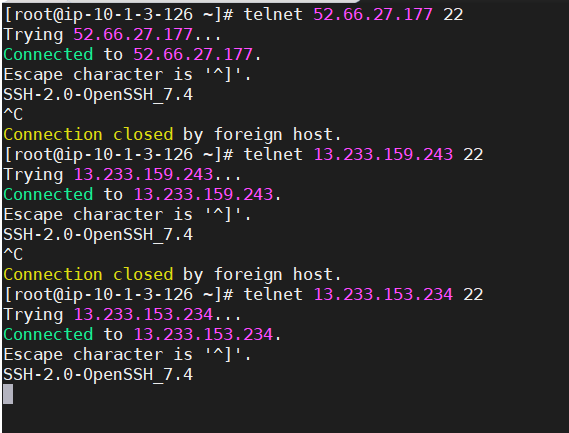
1. Create a new subnet in new availability zone for Dev-VPC & launch one instance in new subnet created and then check connectivity b/w all VPC’s as shown below.



Step1:- But you cannot communicate with the VPC’s, the you have created subnet in different availability zone. So you need to go to Transit Gateway attachments and enable the new subnet created by you and modify it as shown below.

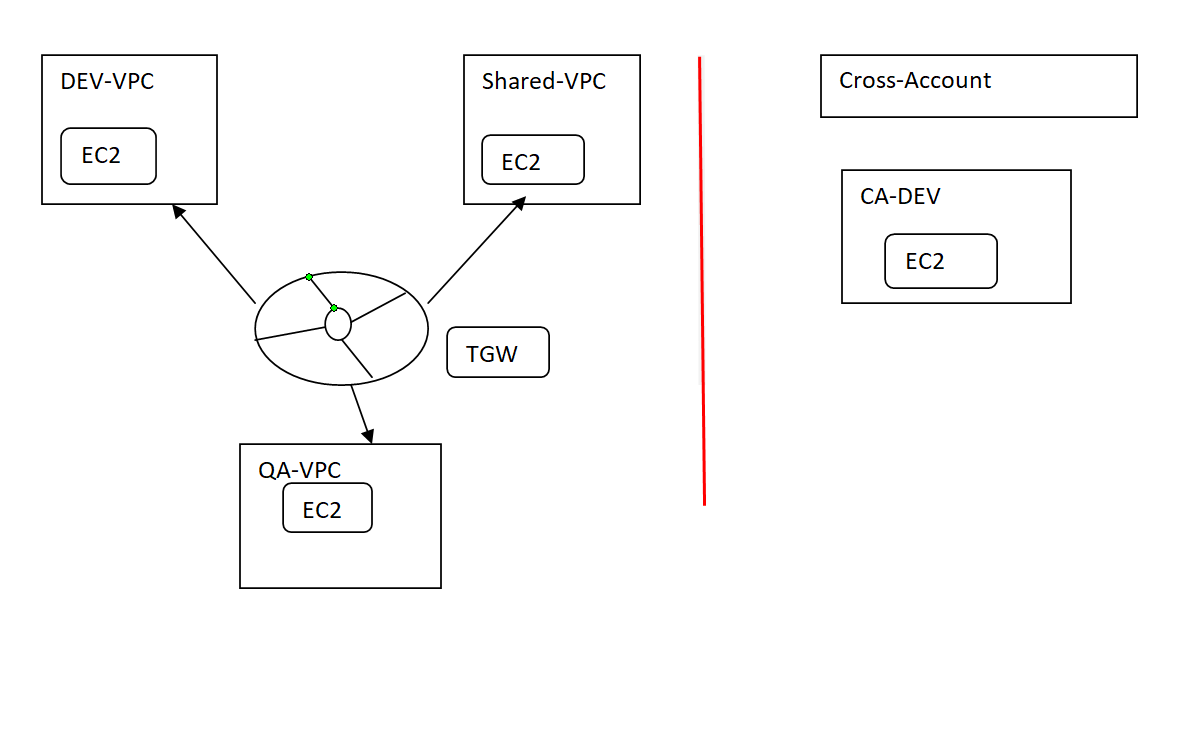


Step2:- After modifying the attachment, it is possible to communicate b/w different VPC’s as shown below.



Now you are able to communicate with all VPC’s as shown in above screenshot.

* **Shared Transit Gateway with Cross-Account.**



EC2

DEV-VPC

Cross-Account

EC2

CA-DEV

TGW

EC2

QA-VPC

Shared-VPC

EC2

EC2

DEV-VPC

Cross-Account

EC2

CA-DEV

TGW

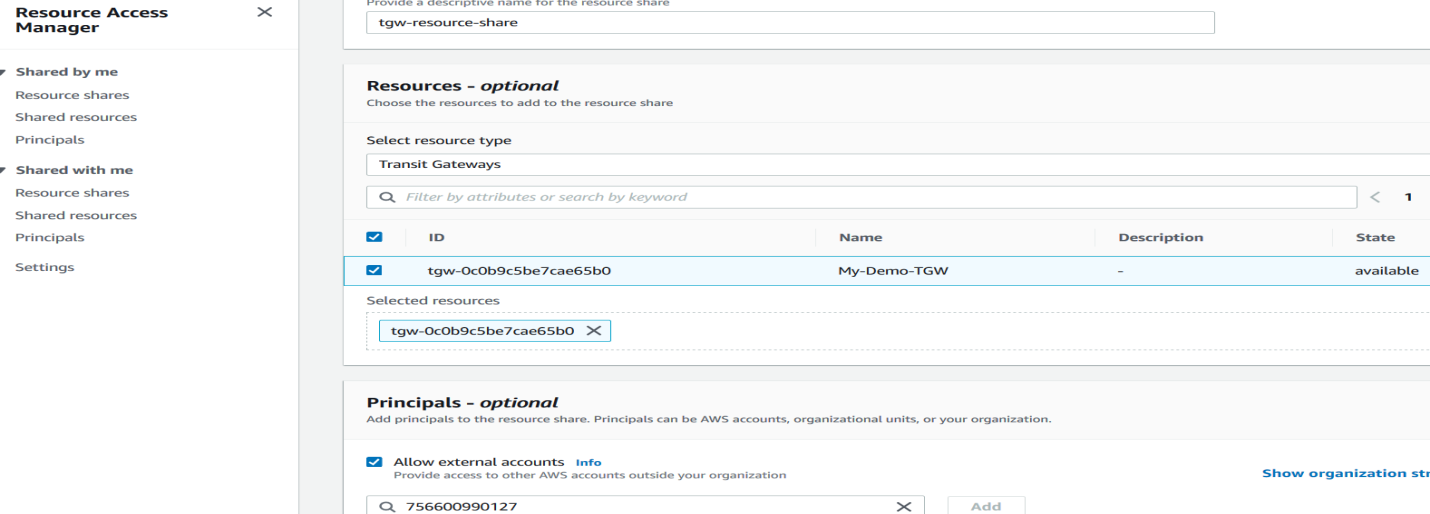
EC2

QA-VPC

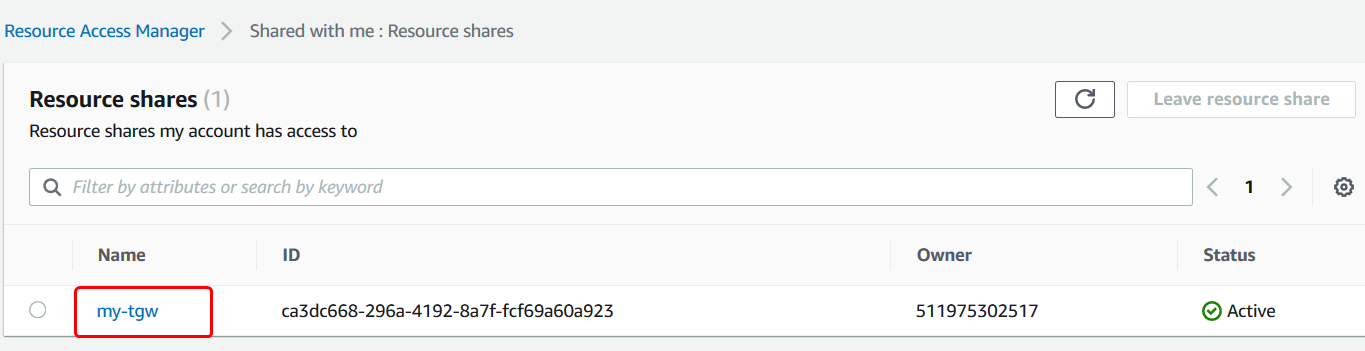
Shared-VPC

EC2

Step1:- Go to Resource Access Manager and share the transit Gateway to other account by giving account id of it as shown below.

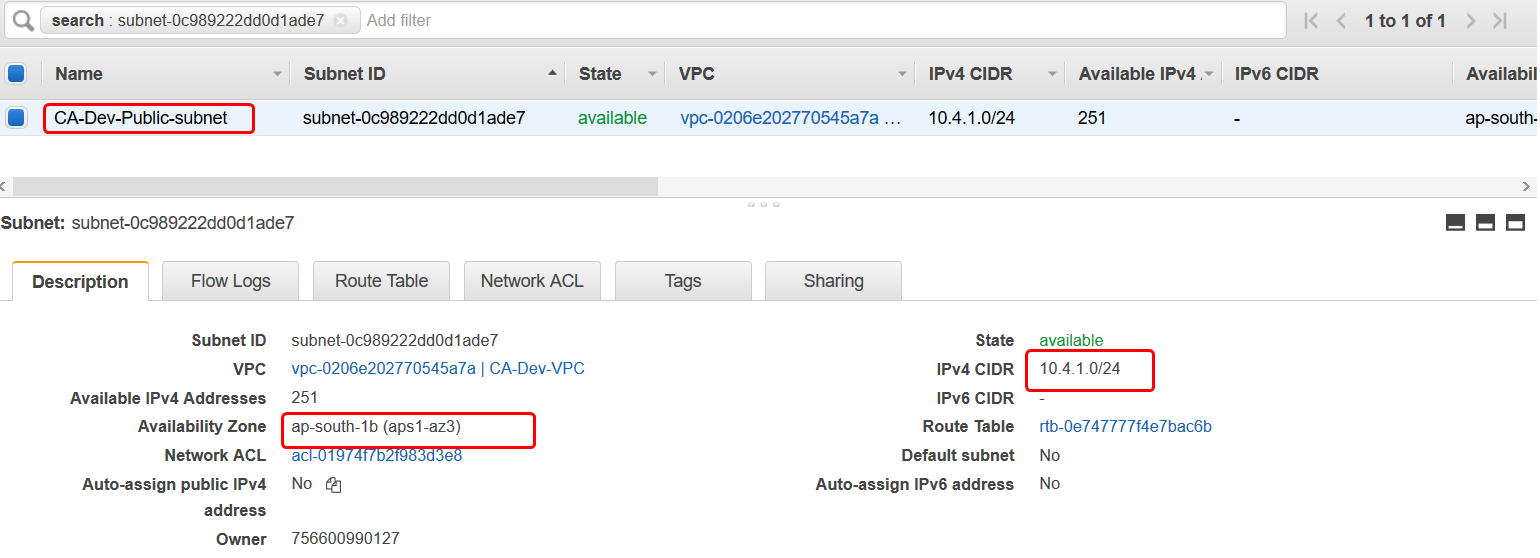


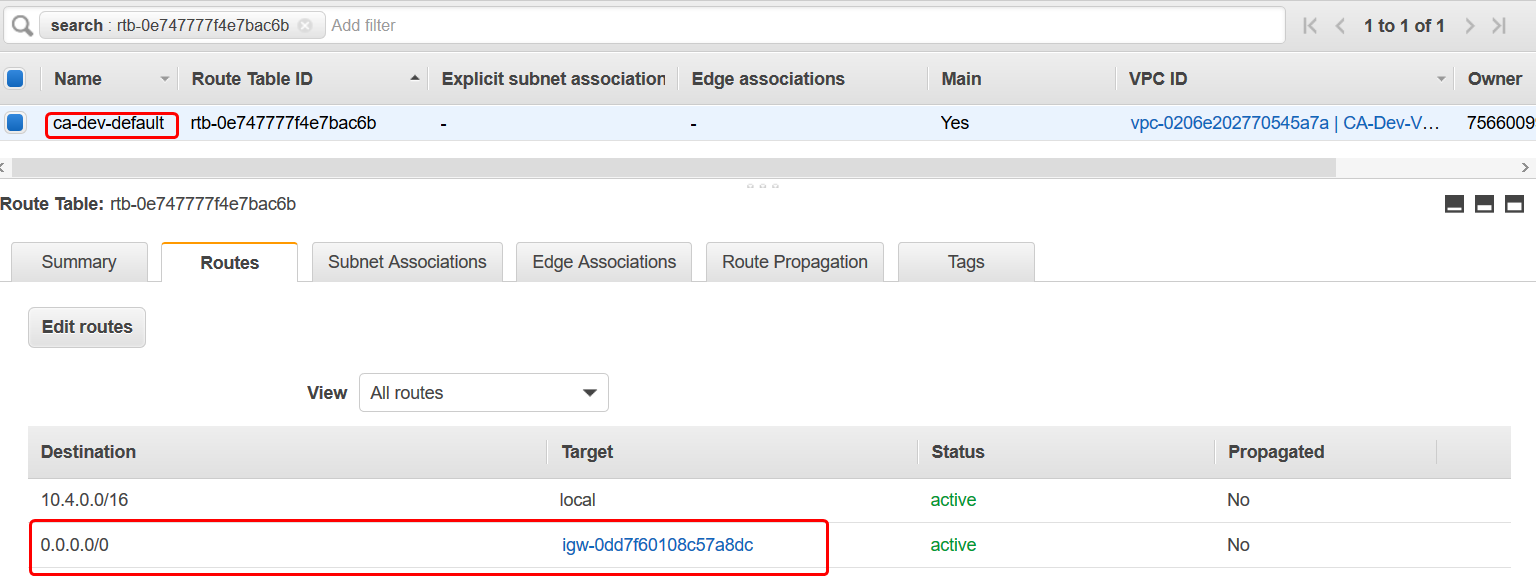
Step2:- Go to the account you have shared your transit gateway and accept the resources shared from other account as shown below.(Note:-**Check in same region where you created TGW, TGW is regional only)**



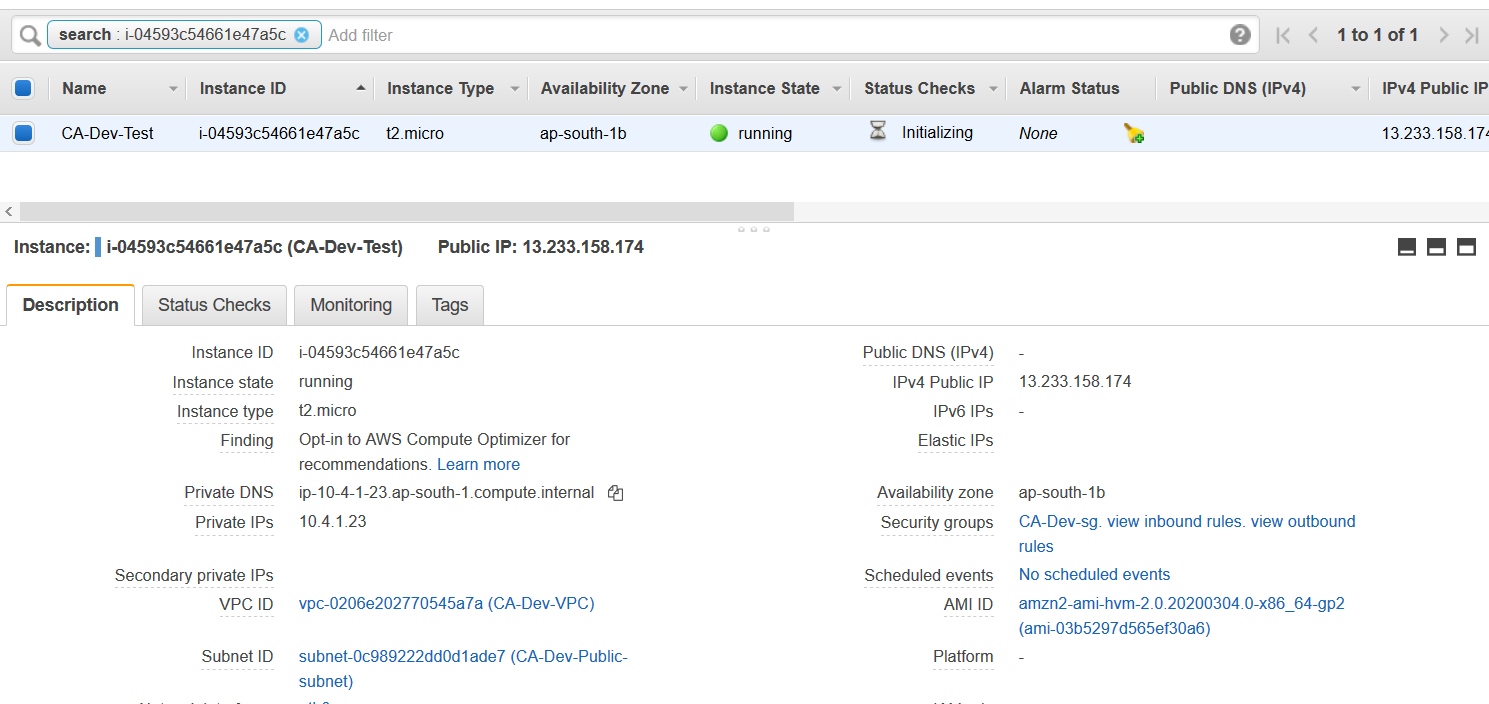
Step3:- Create VPC, subnets and IGW as shown below and add the route to IGW in route tables as shown below.



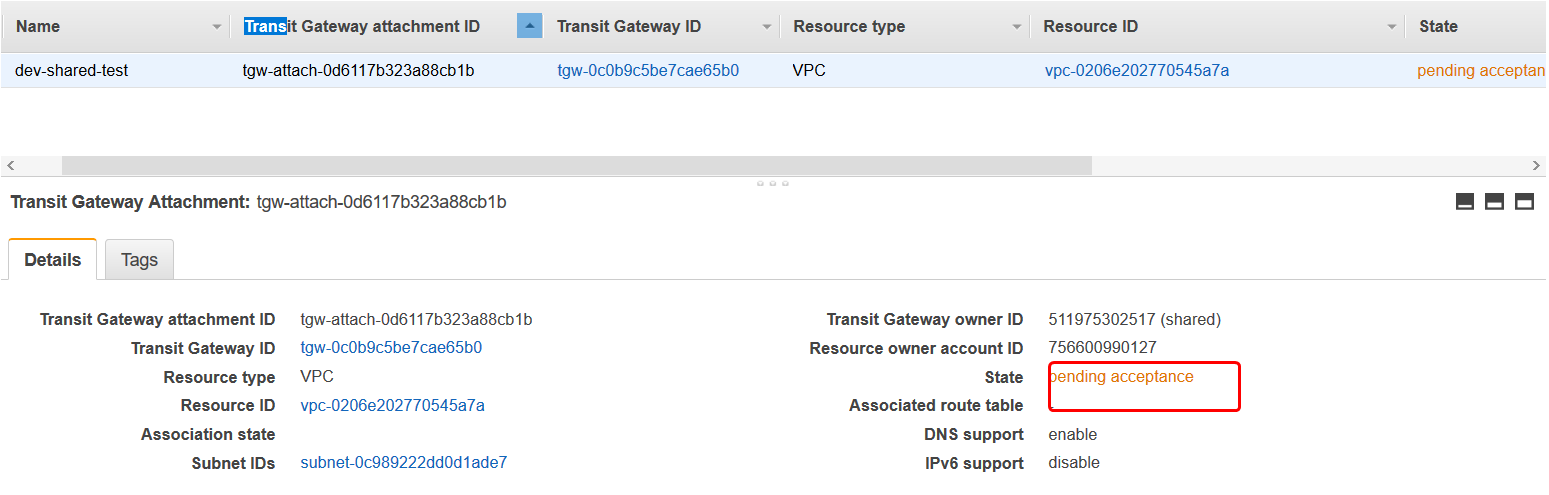




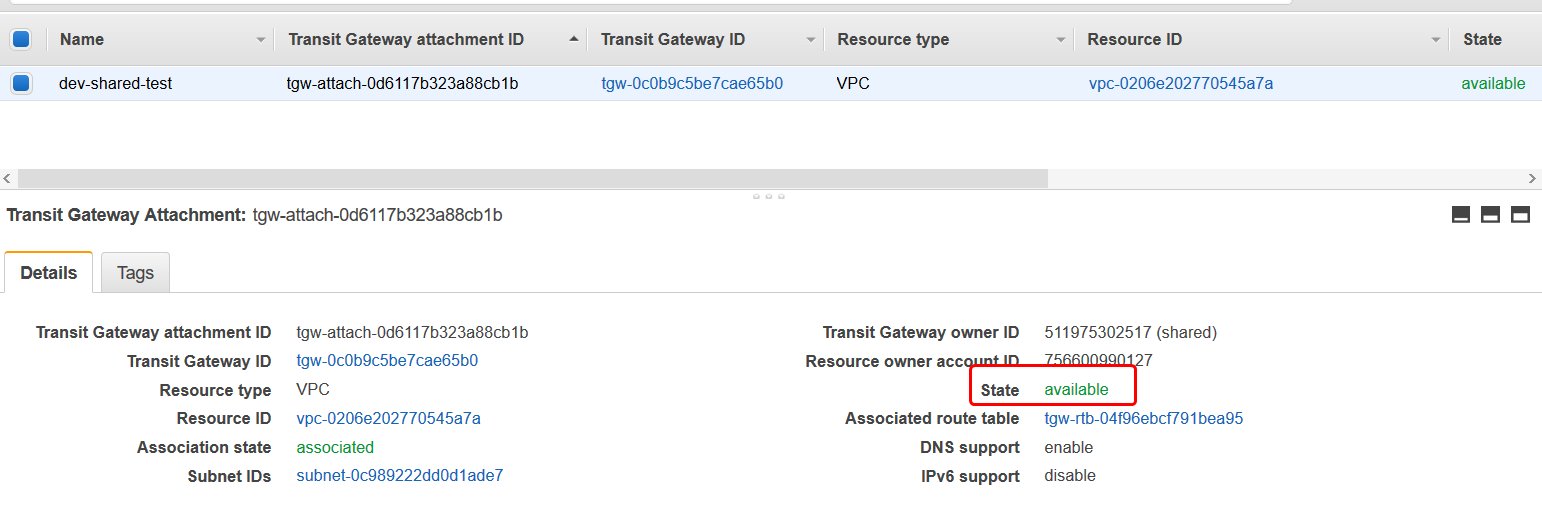
Step4:- Create Ec2 instance in same VPC & subnet you created as above.



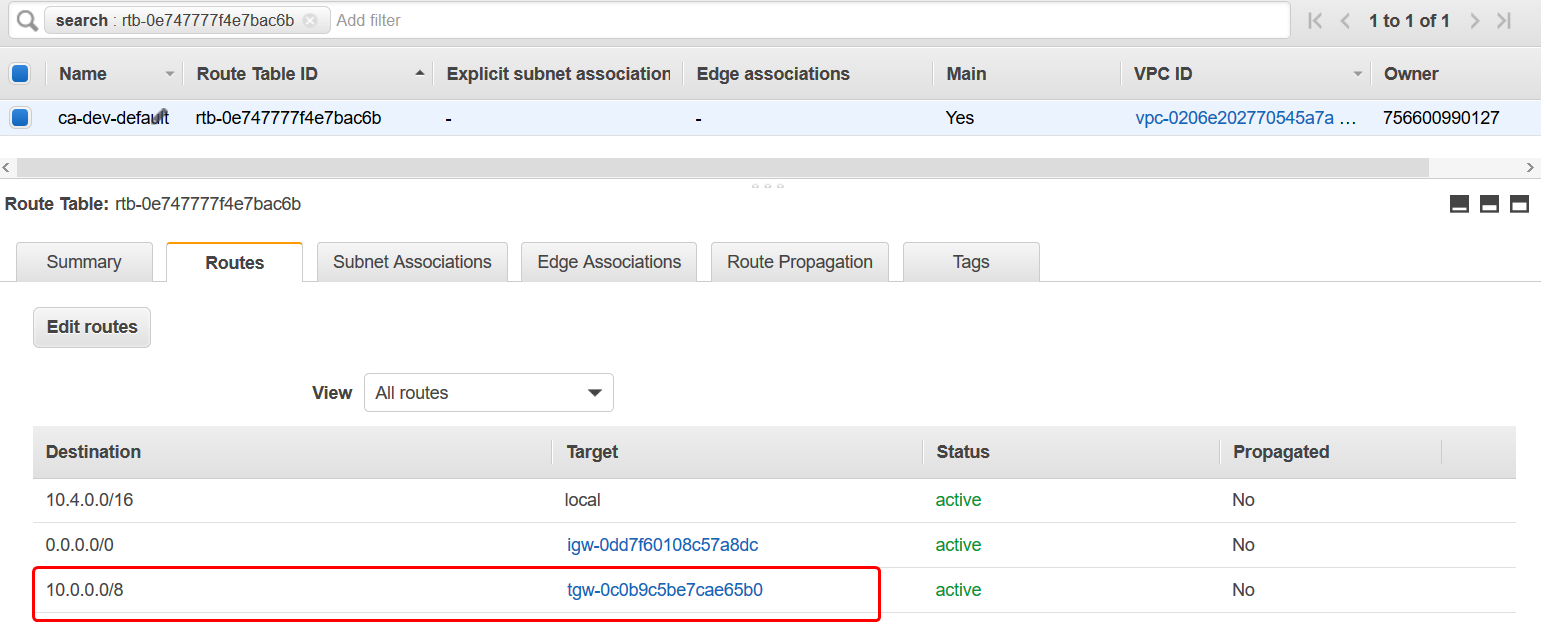
Step5:- Create VPC attachments and accept them in source account from which you shared Transit Gateway as shown below.

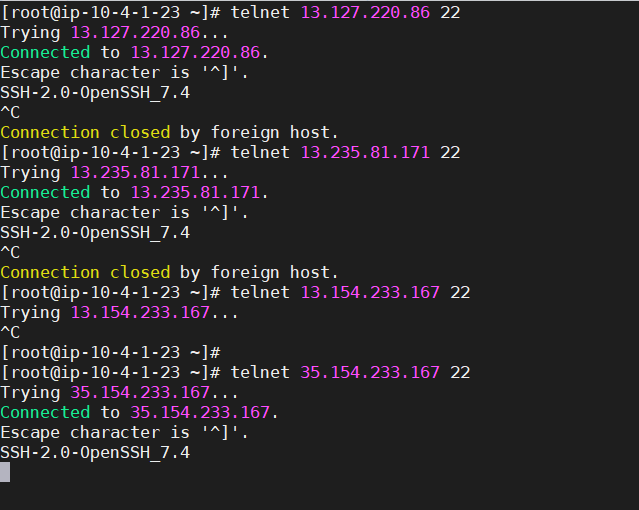


Once you accept it comes into available state as shown in below screenshot.



Step6:- Now test the connectivity b/w cross-account VPC and the three VPC’s in main account which will result in failure because we have not added the Transit gateway route in CA-dev VPC of other region, so please add it and then test connectivity as shown below.

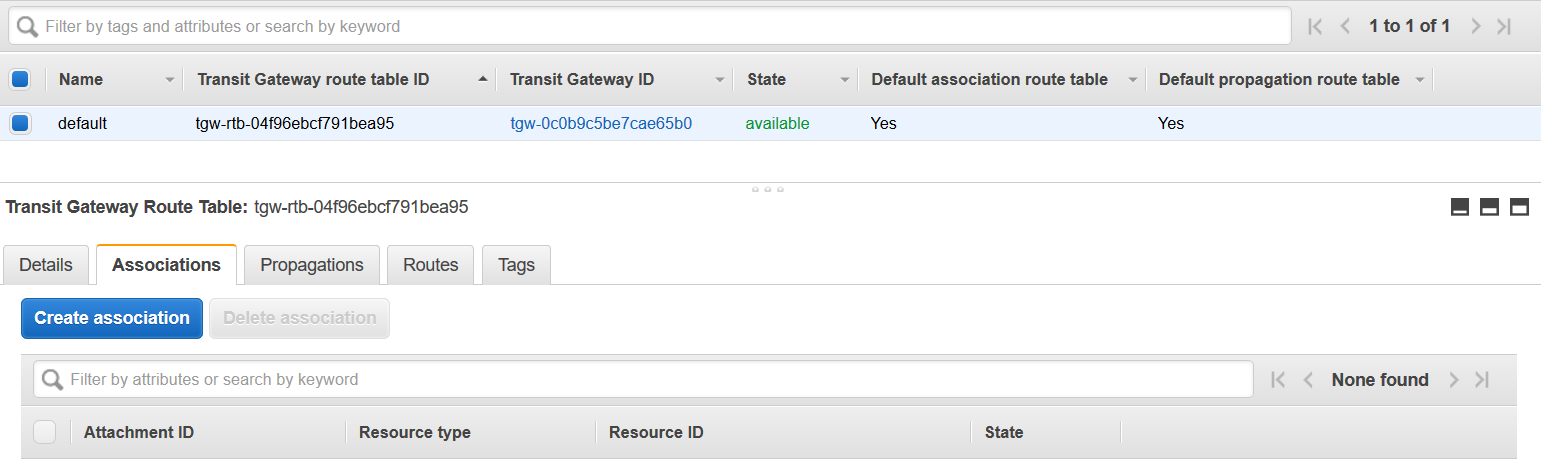




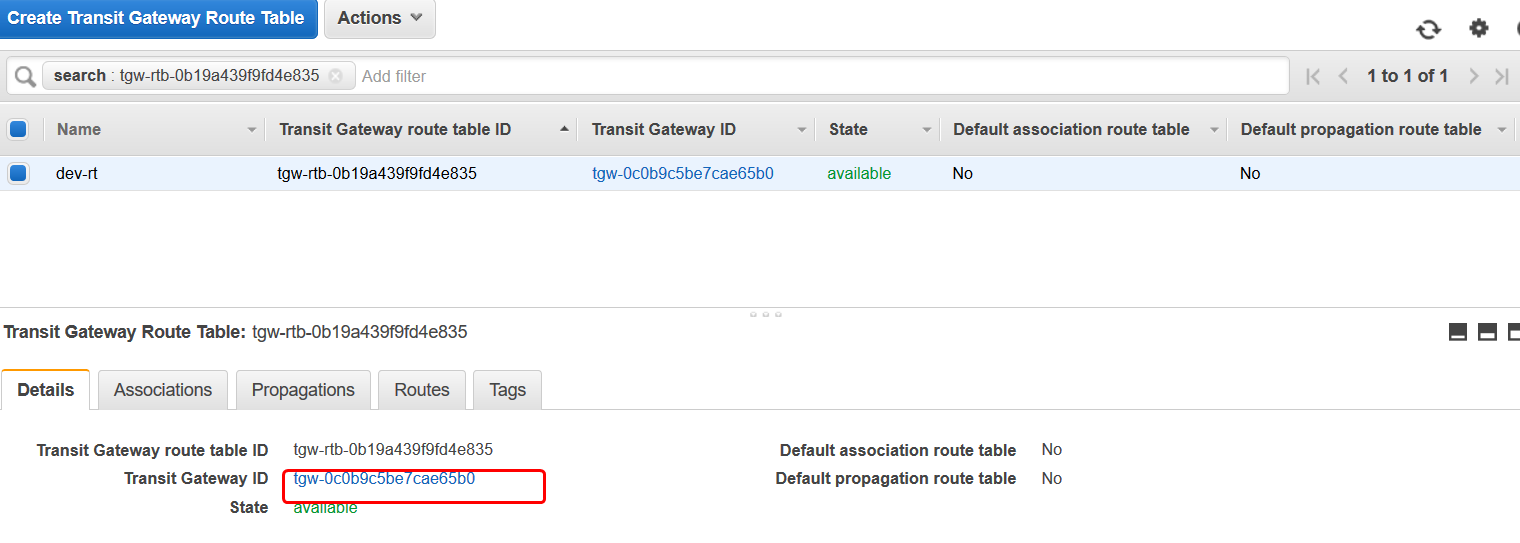
Now you can successfully communicate with other VPC in cross-account as shown in above screenshot.

* **Scenario1:-** Transit Gateway with Custom routes & test connectivity b/w VPC’s.(Only specific).

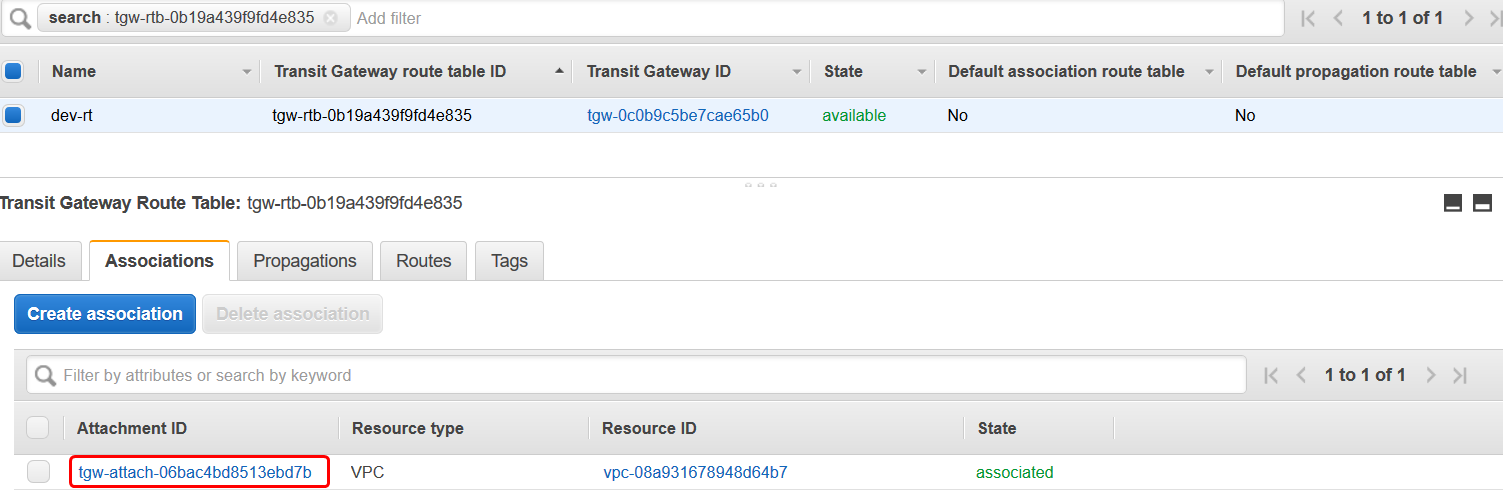
Step1:- Clean up the current assosicatoions so that you can setup your own custom routes.there wont be any associations $& propogations in TGW Route table.

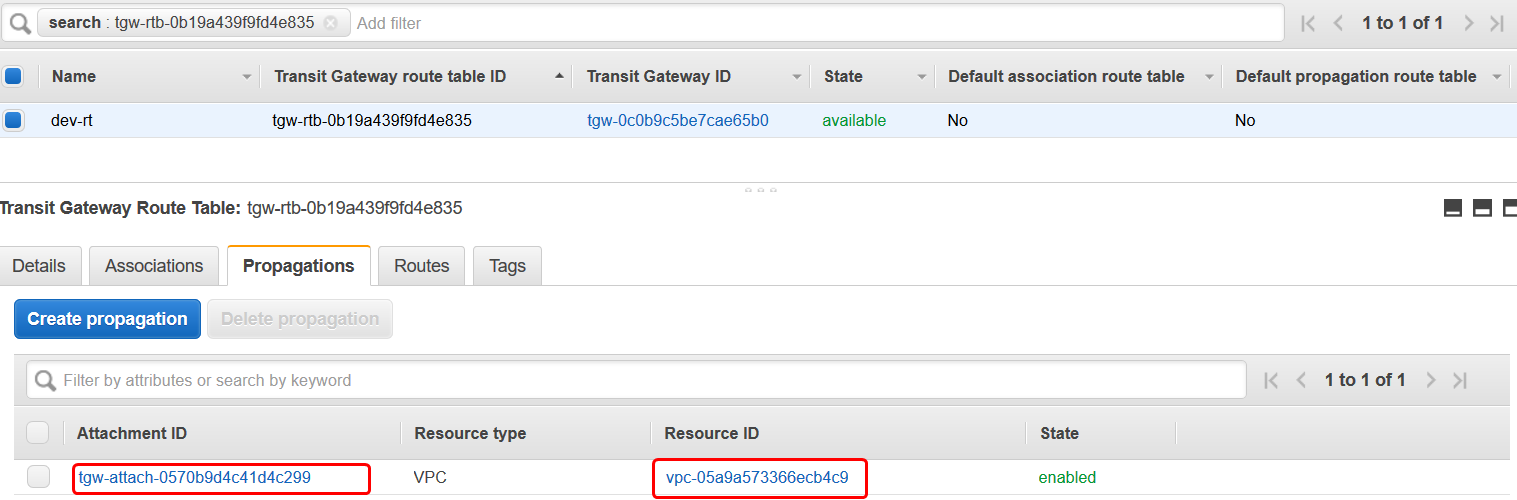


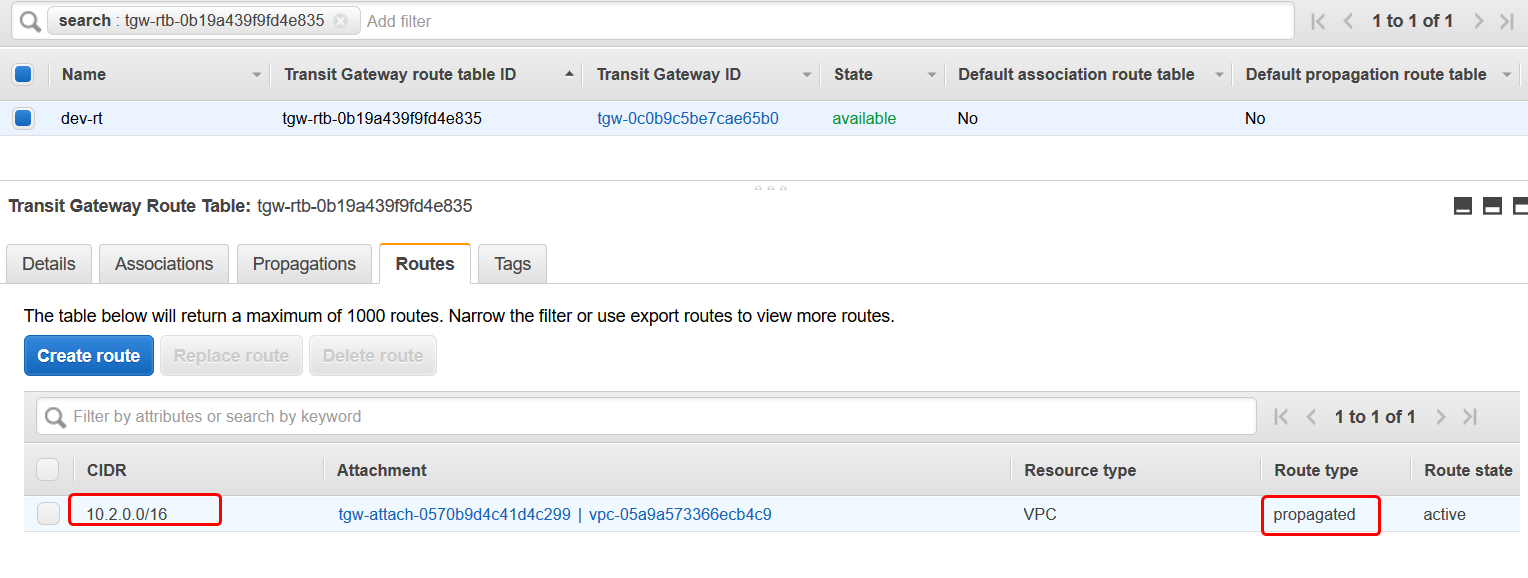
**Step2**:- Implement TGW custom rout table b/w Dev & QA VPC as shown below.



Create association to dev-attach and propogate it to qa-attach as shown below.

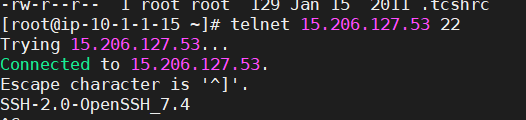


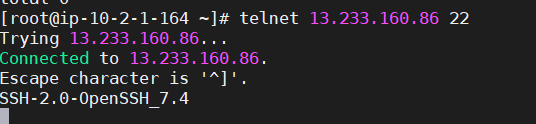




Also create custom transit gateway route table for QA-VPC also as shown in above screenshots**.** While associating you can select sameVPC & while propagating select different VPC (For Eg:- QA-VPC ).

Step3:- Now you can test connectivity b/w Dev & QA VPC. So it returns the output as shown below.

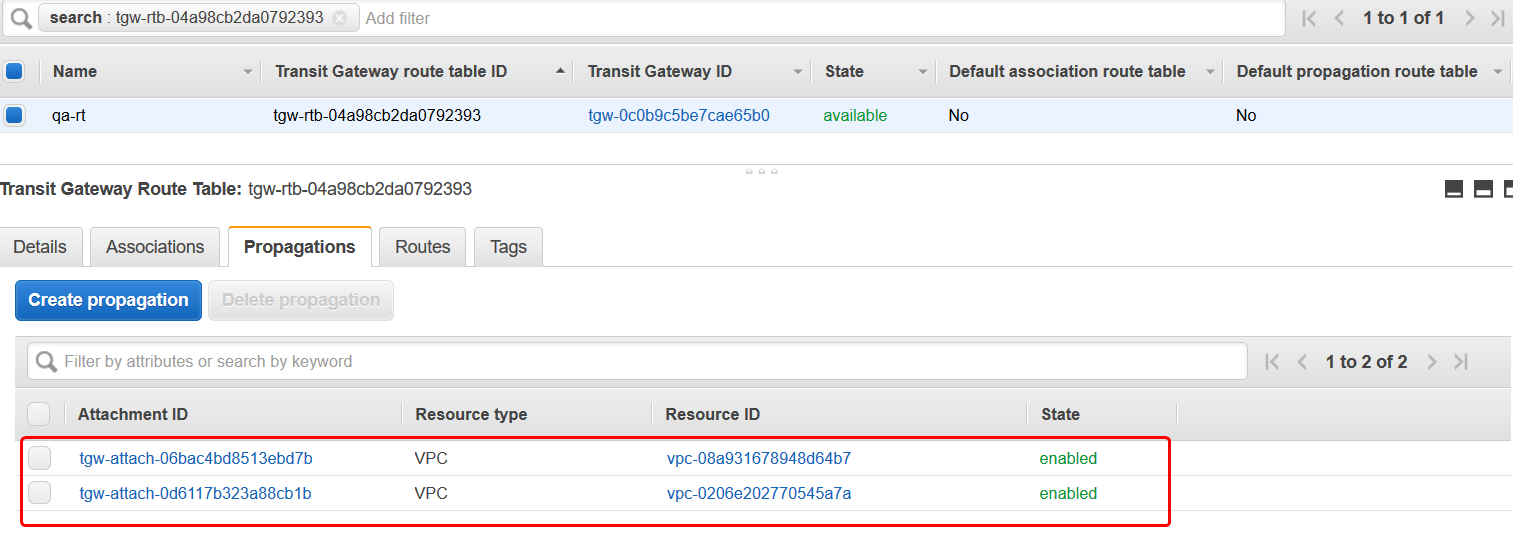




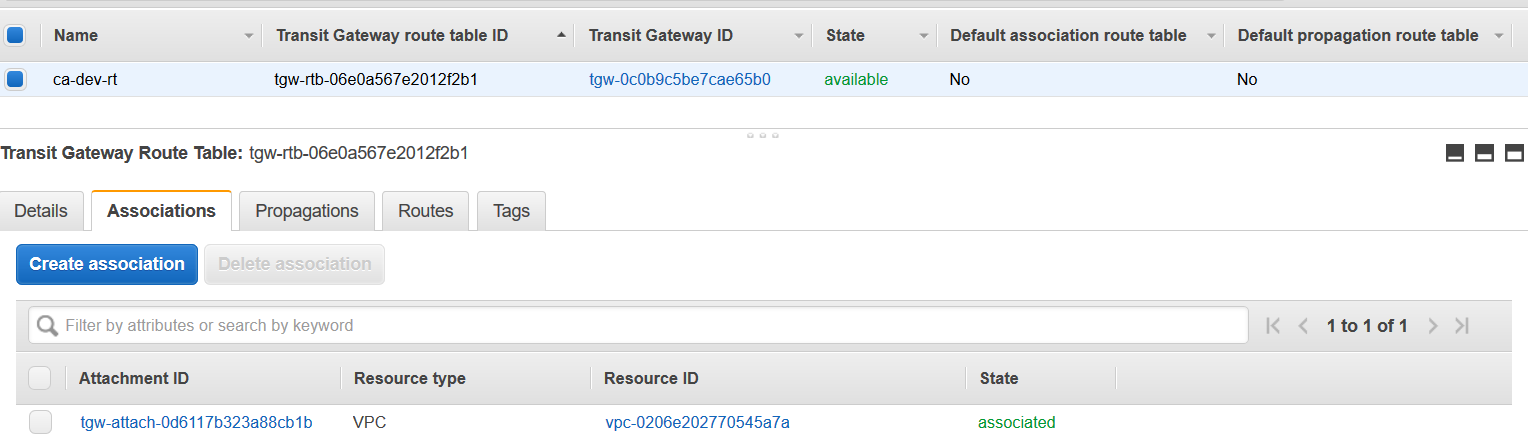
Scenario2:- In the same way, create custom Transit Gateway route table for Shared & Dev VPC. Test connectivity b/w those two VPC’s. Process is same as we created earlier. (Try it out if you have patience).

Scenario3:- Implement custom route table b/w QA-VPC and Cross-account VPC’s

Step1:- Go to Transit Gayteway route table and select qa-attach you created earlier and just add the propogation route to ca-dev VPC which is in cross-account as shown below.

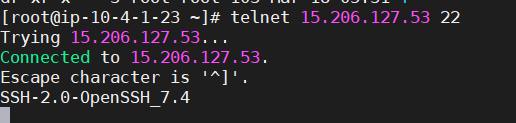


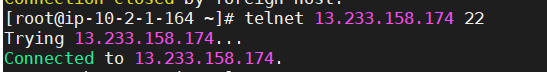
Step2:- Do it in same for ca-dev-rt also as shown in below screenshots.





Step3:- Now you can test the connectivity b/w QA-VPC & Cross-account VPC using telnet command as shown below.





Now you are able to successfully communicate b/w QA VPC & Cross-account VPC.

Step4:**-** Perform negative tests & it should fail.

1. Dev -> ca-dev -🡪 should fail
2. QA -> Shared -🡪 should fail
3. CA-dev -> Dev -🡪 should fail
4. CA-Dev -> Shared -🡪 should fail