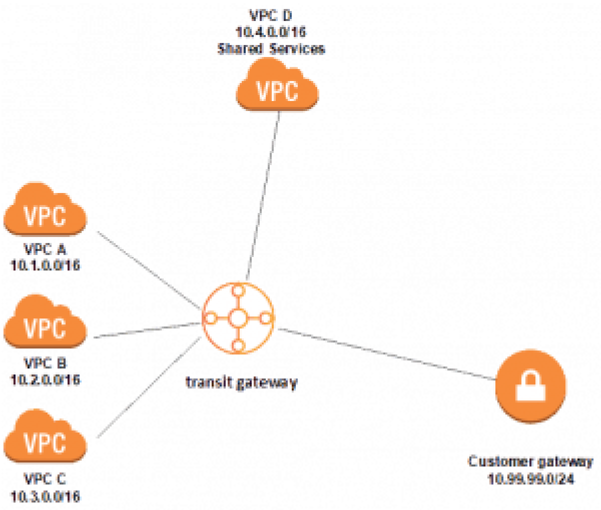
Amazon AWS VPC vs Transit Gateway

Here we will have 3 VPC as follow and if you remember VPC do not offer transitive Peering; in order to make a peering between all VPC ; we need to make sure all VPC are peer together and this take a lots of time and effort.

That is if VPC1 is peering VPC2 and the if VPC2 is peering with VPC3, then VPC1 can not peer with VPC3, In order all talked to each other we need to full mesh peering.



That is it will follow Hub and spoke topology ;

That is VPC4=10.4.0.0/16 will act as Hub ; and the rest of VPC will be Spok

For example VPC1 =10.1.0.0/16 will be spoke

VPC2= 10.2.0.0/16 wil be spoke

VPC3=10.3.0.0/16 will be spoke.

So after we finish all EC2 instance in each VPC will be able to talked to each other.

Step 1) We will need to create a VPC1=10.1.0.0/16 and also create IGW and attached to VPC1;Then we will create public Subnet 10.1.1.0/24 in Subnet 1

As we see when I created VPC 1 =10.1.0.0/16 , the AWS has created a Routing table for me ;lets give the Name “ This was created by system when I created a VPC 10.1.0.0/16

Step 2) I need to create a new Custom RT ;and call it “ Public Routing table for 10.1.0.0/16” goes to internet ; then add entry to 0.0.0.0 and point to IGW that was called “VPC1 IGW”

Step 3) Remember make sure go to Subnet Association and associate Subnet 10.1.1.0/24 ; with above Custom Routing Table.

Step 4) I will do same concept for :

VPC 2 = 10.2.0.0/16

Public Subnet = 10.2.1.0/24

Create an IGW VPC2 ; and attached to VPC2

Created a new RT for VPC 2

Subnet Association

Step 5) I will need to do above task for :

VPC 3 = 10.3.0.0/16

Public Subnet = 10.3.1.0/24

Create an IGW VPC3 ; and attached to VPC3

Created a new RT for VPC 3

Subnet Association

Step 6) Now I will go to EC2 and I will bootup an Amazon Linux AMI and put on each corresponding Subnet and each corresponding VPC ;

Lets called it as follow :

PC1-10.1.0.0 (put inside VPC1 , subnet 10.1.1.0/24)

PC2-10.2.0.0 (put inside VPC2 , subnet 10.2.1.0/24)

PC3-10.3.0.0 (put inside VPC3 , subnet 10.3.1.0/24)

Step 7) Now in order each EC2 talked to each other I need to do VPC peering; that is

VPC1 peer with VPC2 and VPC2 peer with VPC 3 and remember we do not have transitive Peering so VPC1 cannot talk to VPC3 , so in order to do this I need to have another VPC peering between VPC1 and VPC3

As we see this will get harder as we get more VPC , so in order to solve the problem Amazon came with Transit Gateway

Step 8) Now I will start my actual Lab in here

Step 9) I go in top ; then click on VPC; then on right side I go to transit gateway

Step 10) Lets create it and I will call it :

Name: ASMTransitgateway

Description : This will be used for VPC1 , and VPC2, and VPC3

Step 10) Give AS for BGP = 64512 and rest of value leave as default

Step 11) Now I will to go and attached VPC1, VPC2 and VPC3 to above transit gateway

Step 12) Go to left and click transit gateway attachment ; then pick VPC1 and give name VPC1 and pick Public Subnet 1

Step 13) Do same concept for VPC2 , and VPC 3 and after 5 ins you should get all VPC available

Step 14) Now when all is good on step13 ; when I go to left and look at transit gateway routing table I will see all the routes from VPC1,VPC2,VPC3 in here , so route has been propagated in here

Step 15) Now if I SSH to EC2 lcoated in VPC 1 (10.1.0.0/24) I will not be able to ping an EC2 located on 10.2.1.x or 10.3.1.X Why ? Since remember I need to go to each Routing table of VPC1, and VPC2 and VPC 3 add a corresponding Route and point to transit gateway.

Step 16) that is I need to have this

For VPC1 :

10.1.0.0/16 local

0.0.0.0/0 IGW

10.2.0.0/16 transit gateway (I need to add this entry)

10.3.0.0/16 transit gateway (I need to add this entry)

For VPC2 :

10.2.0.0/16 local

0.0.0.0/0 IGW

10.1.0.0/16 transit gateway (I need to add this entry)

10.3.0.0/16 transit gateway (I need to add this entry)

For VPC3 :

10.3.0.0/16 local

0.0.0.0/0 IGW

10.1.0.0/16 transit gateway (I need to add this entry)

10.2.0.0/16 transit gateway (I need to add this entry)

Step 17) Now I will SSH to EC2 on VPC1 = that is 10.1.1.x network and I should be able to ping VPC2 = 10.2.1.x and VPC3=10.3.1.x

Step 18) As we see now all EC2 can talk to each other ; so the key to remember when you create transit gateway and attached to the VPC; it will learn all routes from VPC1 , VPC2, and VPC3 , and make sure you go to corresponding Routing table of VPC1, VPC2 and VPC 3 and update the routing table . Make sure delete all Transit Gateway in order not to get charged.