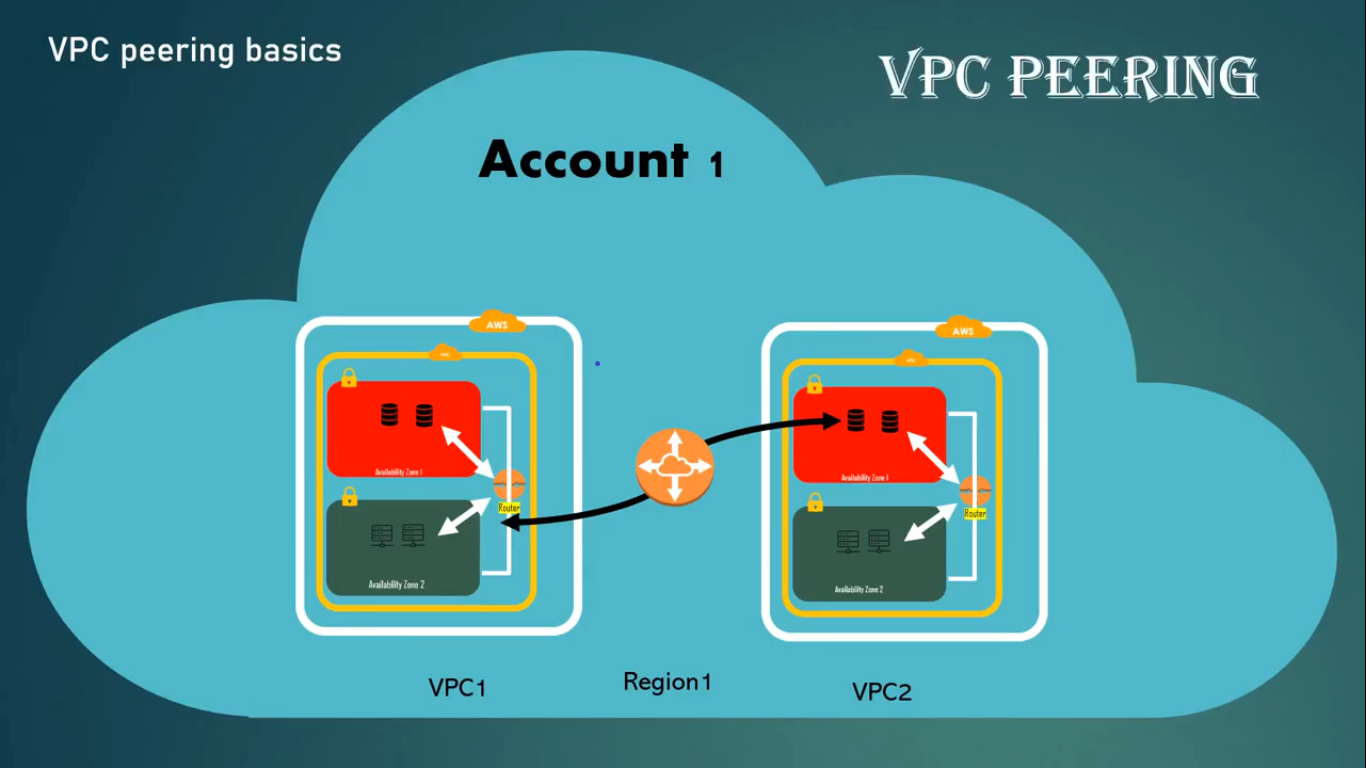
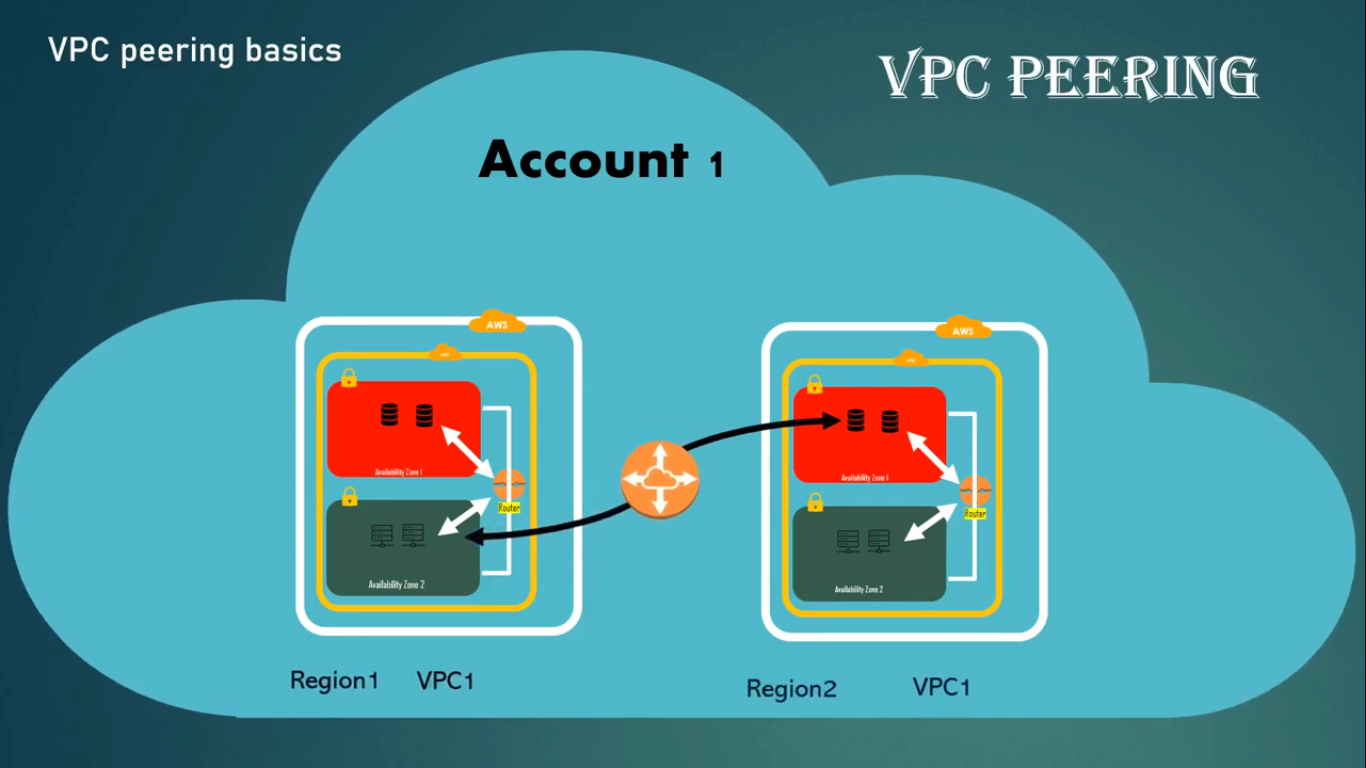
VPC Peering

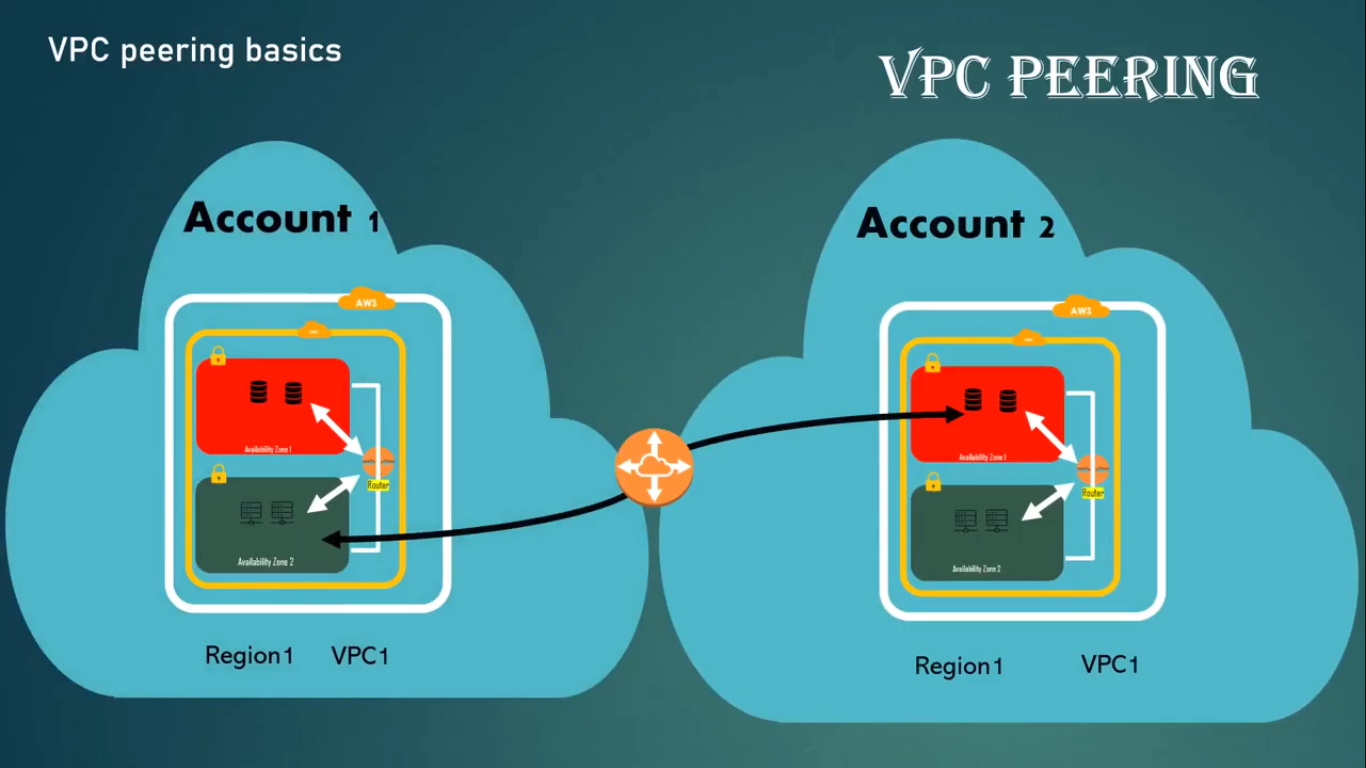
1. We cannot use ‘routing’ technique for VPC’s available multiple regions.
2. For this we need ‘peering’ technique.



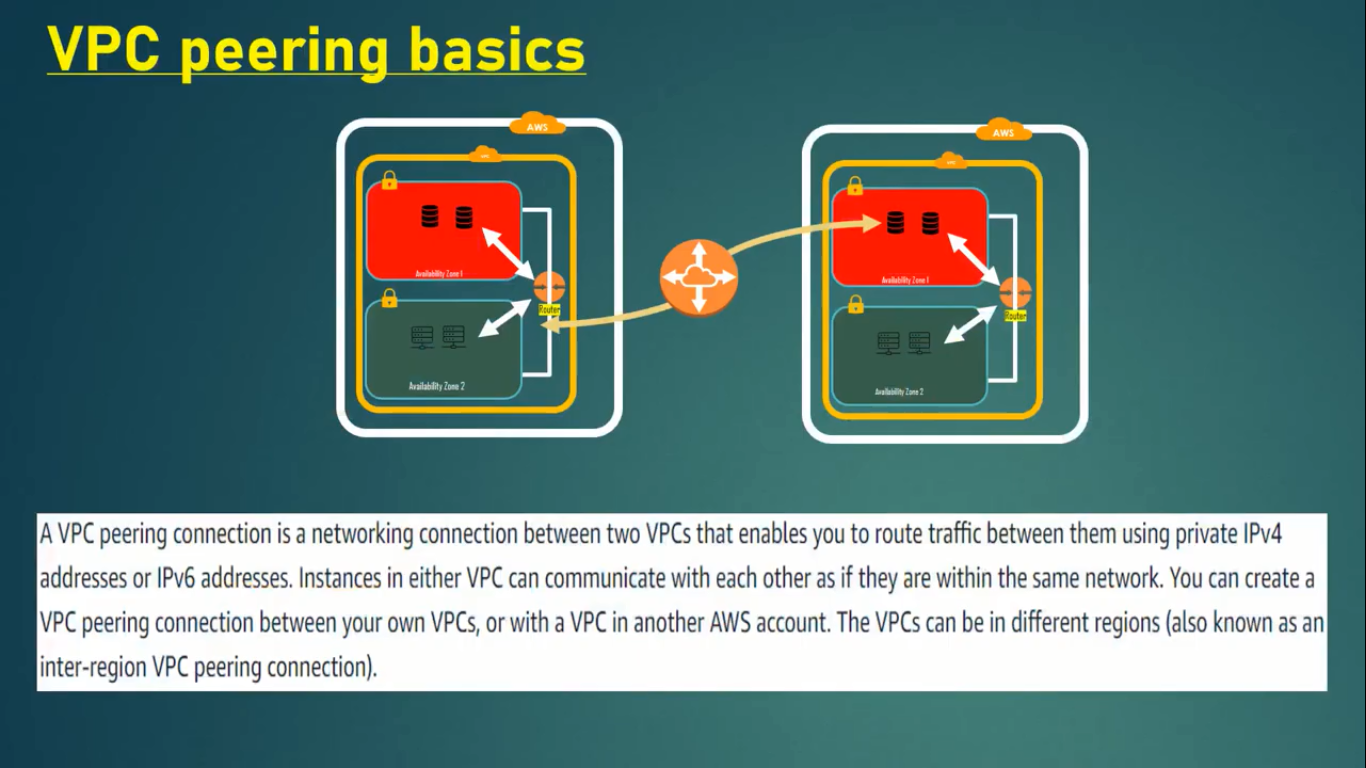
1. For VPC’s under different regions also we use ‘peering’.

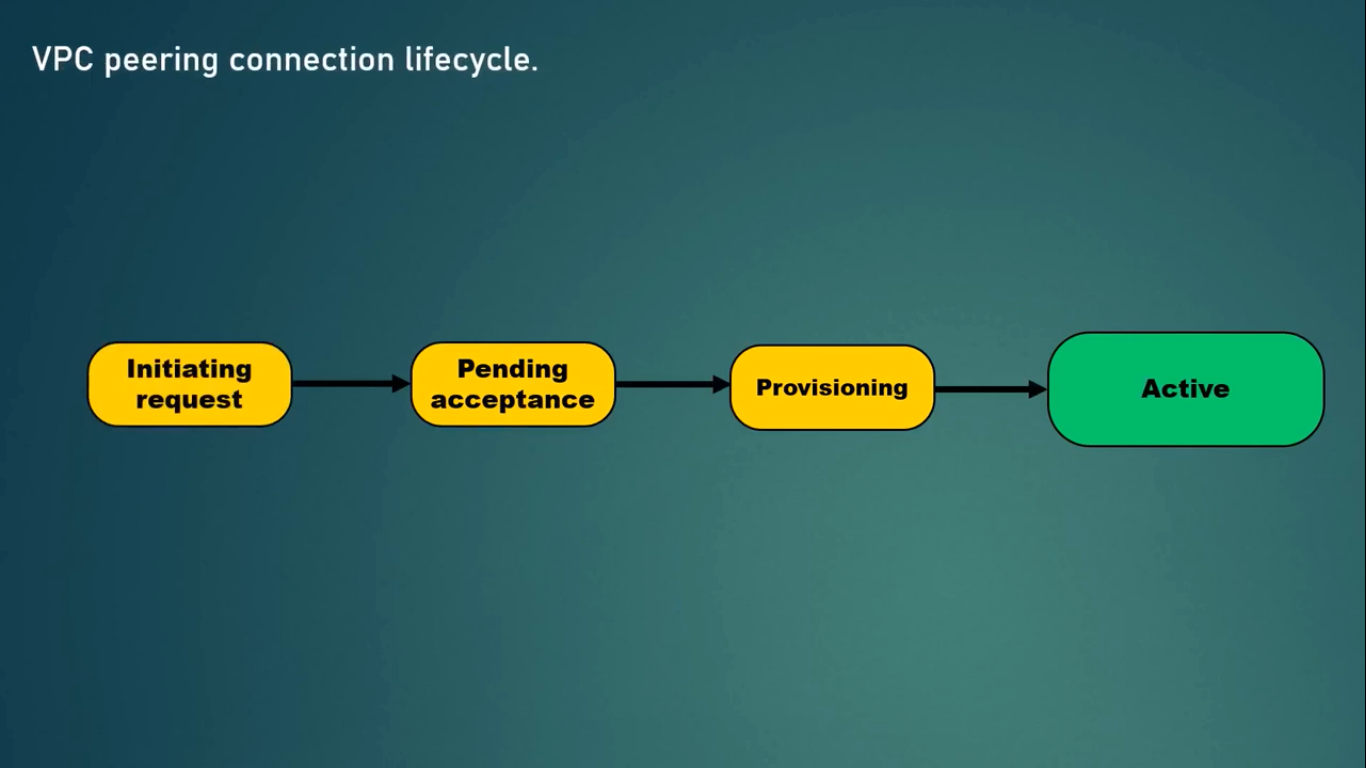


1. Even ‘peering’ is done on VPC’s available under different AWS accounts.

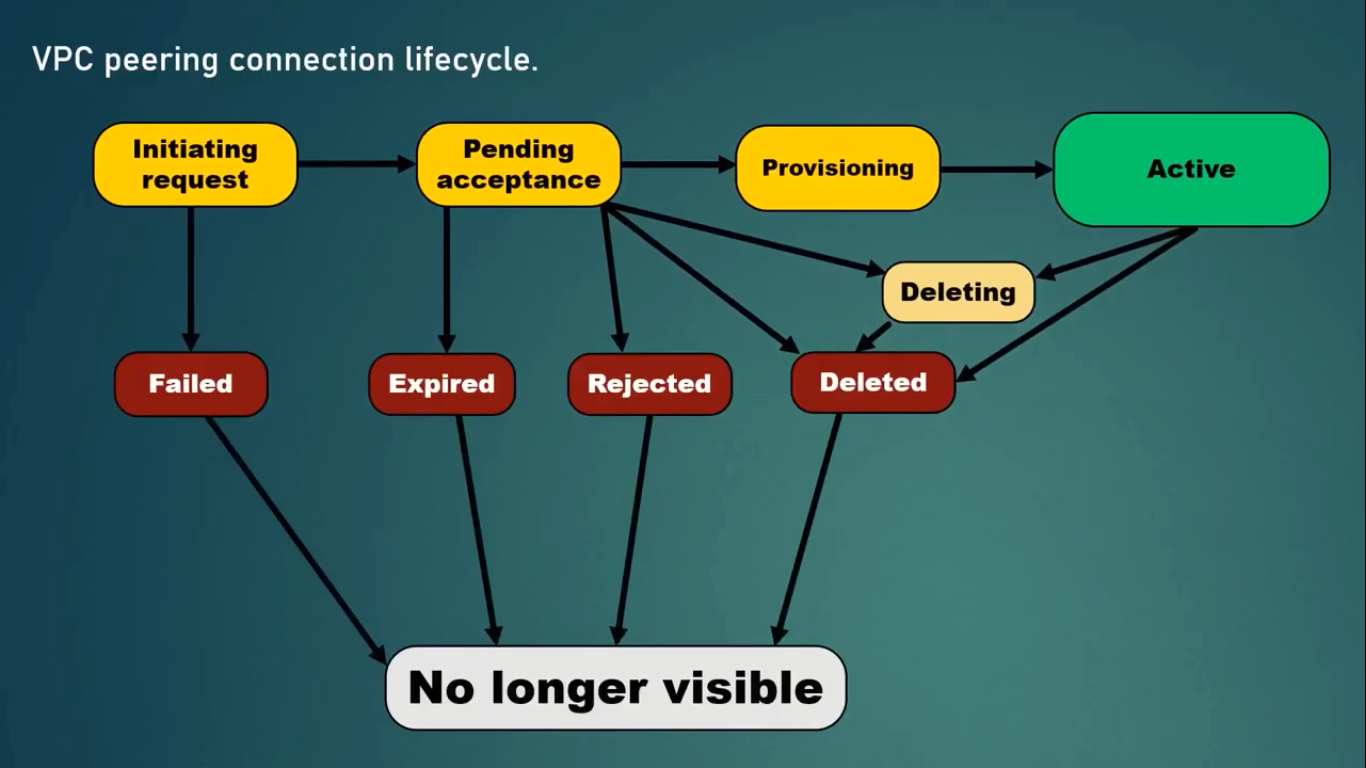


1. According to AWS, peering is defined as followes:



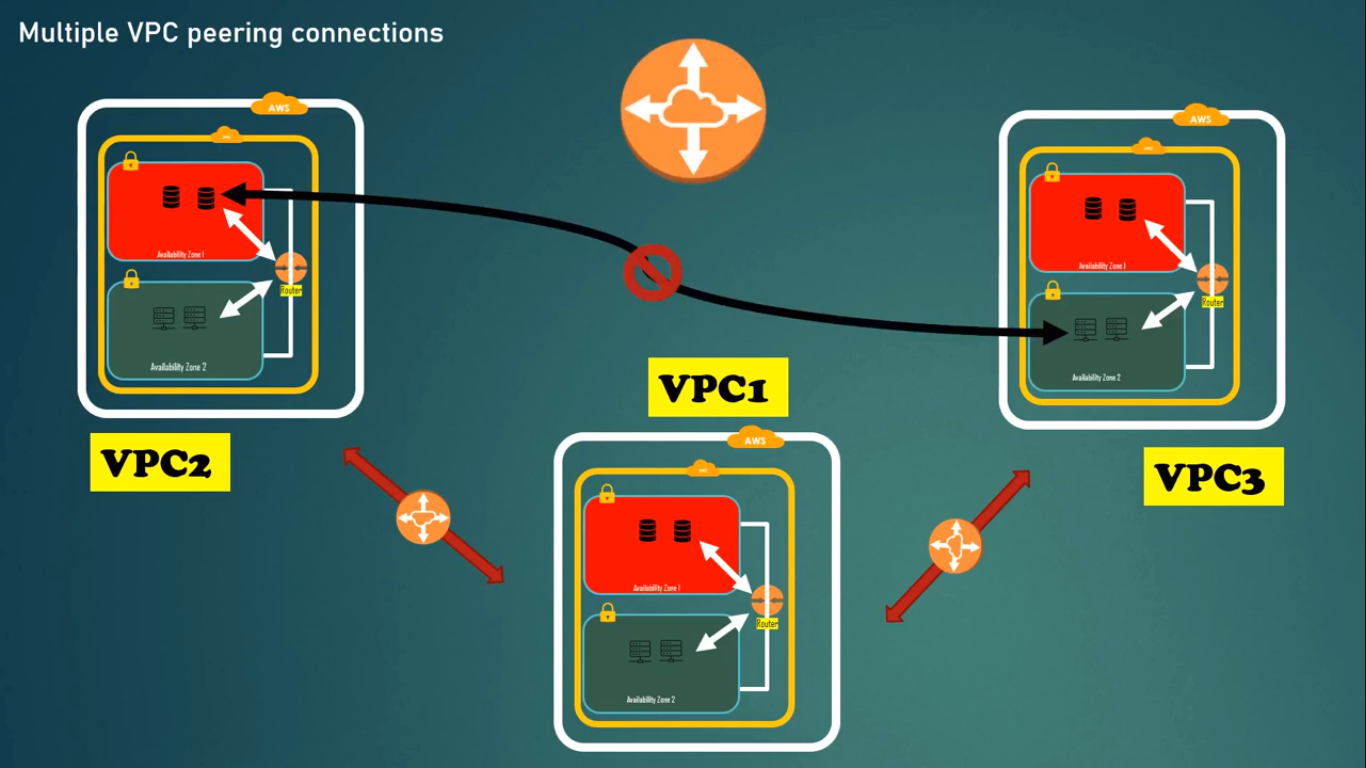


1. Whenever you request for a peering among two different VPC”s, we first initiate the request.
2. There are 2 chances here:
   1. Either request may fail (or)
   2. Request can go to ‘Pending Acceptance’ state.
3. VPC request once failed cannot be re-initiated.
4. Failed requests appear in console for 2 hours and then disappear.
5. If the request gets to ‘pending acceptance’ state, that means the accepter or sender should take an action like ‘provision’ or ‘reject’ or ‘delete’ on the pending acceptance request.
6. The ‘pending acceptance’ request will remain for 7 days, waiting for the response.
7. After 7 days, this request will be expired.
8. If the request is rejected by the receiver than the sender can see the rejected request for 2 days in their account.
9. If the request enters to ‘provisioning’ status, then the request is almost accepted.
10. It the request is in ‘active’ status, then the request activation is confirmed.
11. If the request is active, then communication access is generated between the two VPC environments.
12. Once a request is active, then receiver cannot reject it, but can delete the request.
13. If the request is deleted, an VPC’s are in same region, then the request is immediately deleted.
14. If the VPC’s are in different regions, then the request first enters to ‘deleting’ state and then get deleted.



Multiple VPC peering connections:

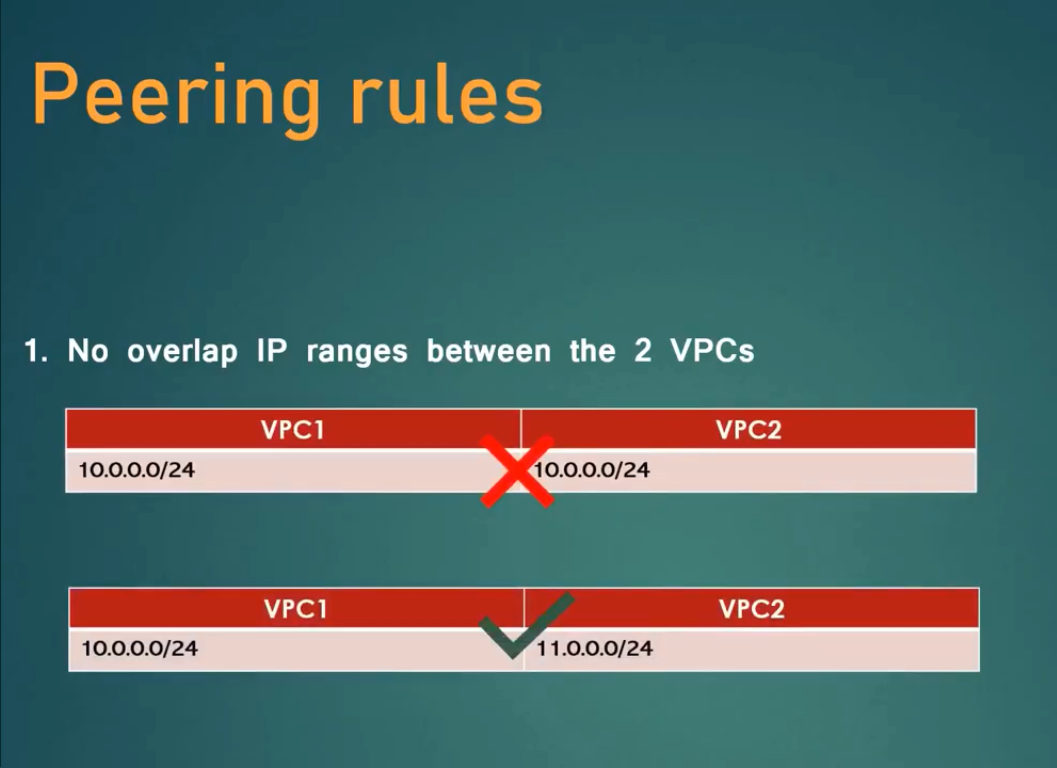
1. A VPC connection is a ‘one to one’ relationship between two VPC’s.
2. You can create multiple VPC peering connections for each VPC that you own.
3. But transitive peering relationships are not supported.
4. You do not have any peering relationship with VPC’s that your VPC is not directly peered with.

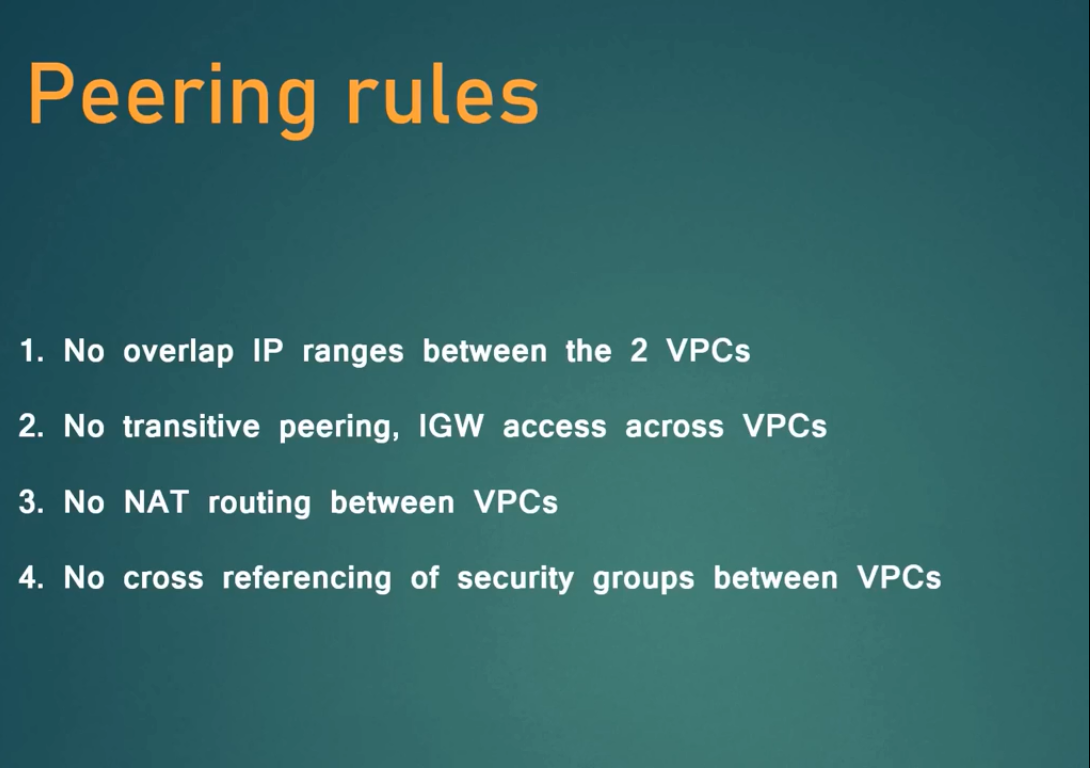


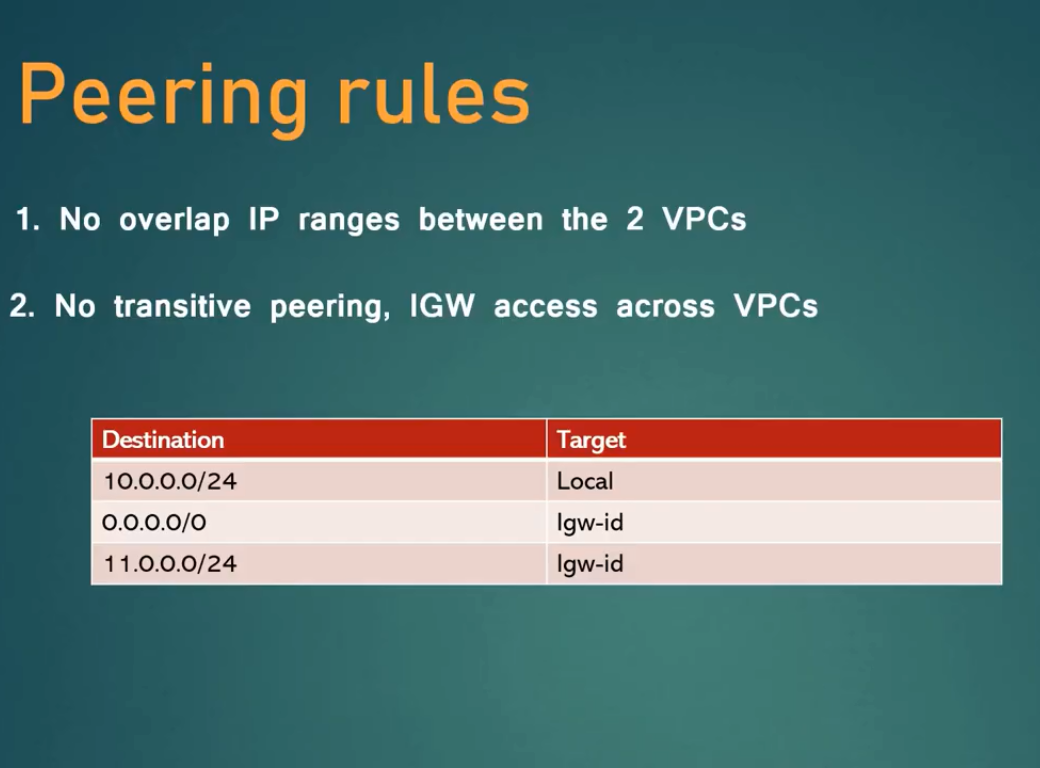
1. You can establish VPC peering between
   1. VPC1 and VPC2 or
   2. VPC1 and VPC3 or
   3. VCP2 and VPC3
2. But from the above diagram, we cannot communicate from VPC2 with VPC3, since they are not directly peered.
3. Every communication must be ‘one to one’.

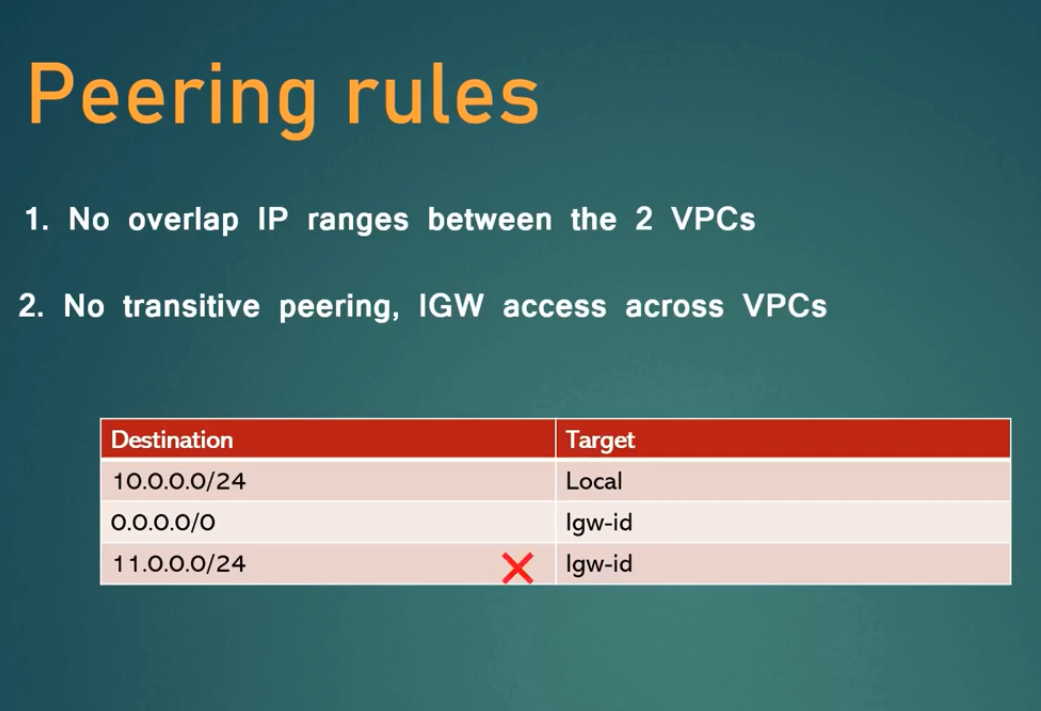
NOTE: No two VPC’s which you want to peer, should be in same CIDR range.

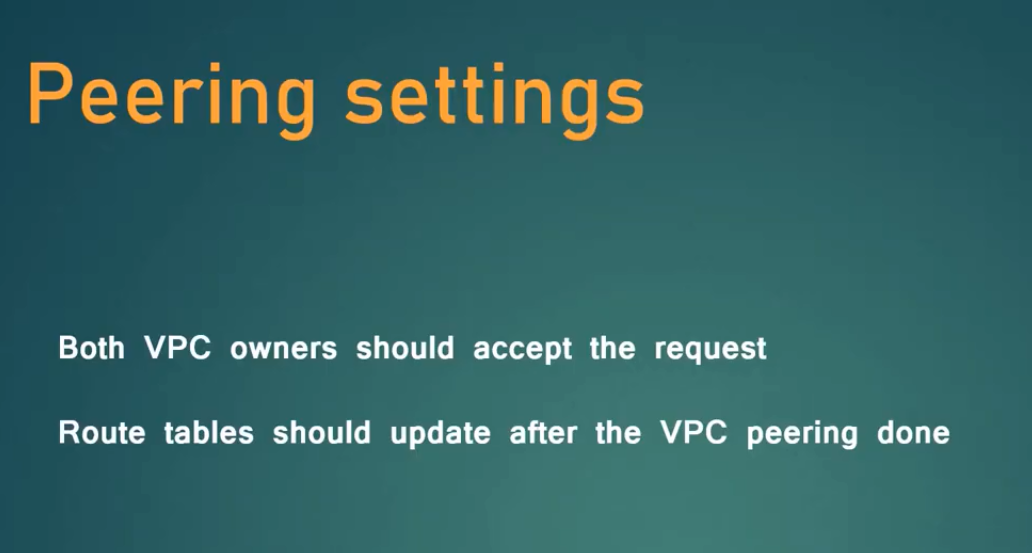
NOTE: If two VPC’s are already in peering, then you cannot establish another VPC connection with those VPC’s.











Hands On:

Creating 2 VPC’s in same region, and establishing connection:

1. Create a VPC with name: FirstVPC\_Region1
2. CIDR range: 10.0.0.0/24
3. Create two subnets related to the above VPC.
4. First subnet name: PublicSubnet\_VPC1
5. CIDR range: 10.0.0.0/25
6. Second subnet name: PrivateSubnet\_VPC1
7. CIDR range: 10.0.0.128/25
8. Now create Internet Gateway: FirstVPC\_IGW
9. Go to ‘Actions’ in IGW and attach the above FirstVPC\_Region1 to IGW.
10. Now create Route tables and select the FirstVPC\_Region1 to Route tables.
    1. FirstRT \_VPC1\_Public
    2. FirstRT \_VPC1\_Private
11. Now under Routes, go to ‘Subnet associations’ and click ‘edit subnets’.
12. Associate public subnet to public route table and private to private route table.
13. Now go to ‘routes’ :
    1. For public route attach 0.0.0.0/0 for internet.(select Internet Gatway)
    2. For private no need to attach any ip addresses for internet.
14. First VPC settings have been completed.

Create 2nd VPC in same Region:

1. VPC name: SecondVPC\_Region1

NOTE: you cannot have same CIDR range of 1st VPC, for this 2nd VPC.

1. CIDR range: 11.0.0.0/24
2. Create subnets:
   1. PublicSubnet\_VPC2, CIDR: 11.0.0.0/25
   2. PrivateSubnet\_VPC2, CIDR: 11.0.0.128/25
3. Select SecondVPC\_Region1
4. Now Create IGW: SecondVPC\_IGW
5. Attach to VPC: SecondVPC\_Region1
6. Now create Route Tables:
   1. SecondRT\_VPC2\_Public
   2. SecondRT\_VPC2\_Private
7. Select VPC: SecondVPC\_Region1 for both the above Route tables.
8. Now do the ‘Subnet Associations’ and ‘Routes’ for public subnet.
9. Second VPC settings have been completed.

Launching Instances for VPC’s in the same Region:

1. For first instance: VPC1\_Public\_Instance
   1. Network: FirstVPC\_Region1
   2. Subnet: PublicSubnet\_VPC1
   3. Auto-assign Public IP: Enable
2. For second instance: VPC1\_Private\_Instance
   1. Network: SecondVPC\_Region1
   2. Subnet: PrivateSubnet\_VPC1
   3. Auto-assign Public IP: Enable
3. For third instance: VPC2\_Public\_Instance
   1. Network: FirstVPC\_Region2
   2. Subnet: PublicSubnet\_VPC2
   3. Auto-assign Public IP: Enable
4. For fourth instance: VPC2\_Private\_Instance
   1. Network: SecondVPC\_Region2
   2. Subnet: PrivateSubnet\_VPC2
   3. Auto-assign Public IP: Enable
5. Generate passwords for all the 4 windows instances and save the username, password and public ipv4 addresses in a separate text file.
6. Steps to connect to Windows instance:

1. After creating AWS Windows Instance wait for few min's and, generate a password.

2. GO to Actions, Security, Get Windows Password option.

3. Browse the downloaded PEM file.

4. Decrypt Password.

5. Save the user name Ex: Administrator

6. Save the password.

7. Go to instances, select your instance and copy its public IPv4 address.

8. On your windows system, press Cntrl+R

9. Type the command 'mstsc'.

10.Copy the ec2 ipv4 address and press 'Connect'.

11. Enter the saves user name and password.

12. You may now successfully connected to your windows ec2 instance.

Task 1:

1. Check whether you can inter connect between Public Instance and Private Instance of same VPC.
   1. First connect to VPC1\_Public instance.
   2. Copy the private ipv4 address of VPC1\_Private instance.
   3. Go to the VPC1\_Public instance connect page and press Cntrl+R.
   4. Provide the VPC1\_Private instance ip address.
   5. Provide the username and password of VPC1\_Private instance.
   6. If we could able to connect VPC1\_Private from VPC1\_Public instance, than our task is successful.

Task 2:

1. Check whether you can connect between Public instance of one VPC to Private instance of another VPC.
   1. It will not connect, because there is no peering between those two VPC’s.
   2. First peer the two instances.
   3. Go to VPC, select the option ‘Peering Connections’.
   4. Select ‘Create Peering Connection’.
   5. Peering Connection Name tag: VPC1\_to\_VPC2\_Region\_Ohio
   6. VPC(Requester): FirstVPC\_Region1
   7. VPC(Accepter): SecondVPC\_Region1
   8. Select ‘Create Peering Connection’.
   9. Now request will be in ‘Pending Acceptance’ state.
   10. Since both VPC’s are in same account and same region, select ‘Actions’ and select ‘Accept Request’.
   11. Now request will be in ‘Active’ state.
   12. Now go to Route Tables, select FirstRT\_VPC1\_Public, and select ‘Routes’ tab and ‘Edit Routes’.
   13. Select ‘Add Route’ and provide Destination: 11.0.0.0/24, Target: Peering Connection, Select VPC1\_to\_VPC2\_Region\_Ohio
   14. Now go to Routes, select SecondRT\_VPC2\_Private, Edit Routes, Add route.
   15. Destination: 10.0.0.0/24, Target: Peering Connection, Select VPC1\_to\_VPC2\_Region\_Ohio
   16. Now try to connect the instances from both the VPC’s.