Transit Gateway

* A networking service that uses a hub and spoke model to enable customers to connect their on-premises data centers and their Amazon Virtual Private Clouds (VPCs) to a single gateway.
* With this service, customers only have to create and manage a single connection from the central gateway into each on-premises data center, remote office, or VPC across your network.
* If a new VPC is created, it is automatically connected to the Transit Gateway and will also be available to every other network that is also connected to the Transit Gateway.

Diagram

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface

Description automatically generated

**Features**

* **Inter-region peering**
  + Transit Gateway leverages the AWS global network to allow customers to route traffic across AWS Regions.
  + Inter-region peering provides an easy and cost-effective way to replicate data for geographic redundancy or to share resources between AWS Regions.
* **Multicast**
  + Enables customers to have fine-grain control on who can consume and produce multicast traffic.
  + It allows you to easily create and manage multicast groups in the cloud instead of the time-consuming task of deploying and managing legacy hardware on-premises.
  + This multicast solution is also scalable so the customers can simultaneously distribute a stream of content to multiple subscribers.
* **Automated Provisioning**
  + Customers can automatically identify the Site-to-Site VPN connections and the on-premises resources with which they are associated using AWS Transit Gateway.
  + Using the Transit Gateway Network Manager, you can also manually define your on-premises network.

Diagram

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with medium confidence

Setup Transit Gateway

2.1 Create Transit Gateway

Navigate to [Transit Gateways console](https://console.aws.amazon.com/vpc/home?#TransitGateways:sort=transitGatewayId) and click on “Create Transit Gateway”.

[Graphical user interface, text, application

Description automatically generated](https://networking.workshop.aws/beginner/lab1/030_tgw/image45.png)

Create Transit Gateway using default settings. Please note that the Amazon side ASN or Multicast support cannot be changed after the transit gateway is created.

[Graphical user interface

Description automatically generated](https://networking.workshop.aws/beginner/lab1/030_tgw/image46.png)

A few moments later, TGW will transition from “pending” to “available” state.

2.1 Create Transit Gateway attachments subnets

According to best practices it is recommended to use a separate small /28 subnet for each transit gateway VPC attachment in case of using NACLs with Transit Gateways. [Link](https://docs.aws.amazon.com/vpc/latest/tgw/tgw-nacls.html).

Navigate to [VPC Subnets](https://console.aws.amazon.com/vpc/home?#subnets:)

* Create subnets for VPC A for 2 AZs
  + VPC A - AZ1 TGW (10.0.2.0/28) and VPC A - AZ2 TGW (10.0.3.0/28)
* Create subnets for VPC B for 2 AZs
  + VPC B - AZ1 TGW (10.1.2.0/28) and VPC B - AZ2 TGW (10.1.3.0/28)
* Create subnets for VPC C for 2 AZs
  + VPC C - AZ1 TGW (10.2.2.0/28) and VPC C - AZ2 TGW (10.2.3.0/28)

2.2 Create Transit Gateway attachments

Under “VPC Dashboard” - “Transit Gateways”, navigate to [Transit Gateway Attachments](https://console.aws.amazon.com/vpc/home?#TransitGatewayAttachments:sort=transitGatewayAttachmentId) and click on “Create Transit Gateway Attachment.”

[Text

Description automatically generated with low confidence](https://networking.workshop.aws/beginner/lab1/030_tgw/image47.png)

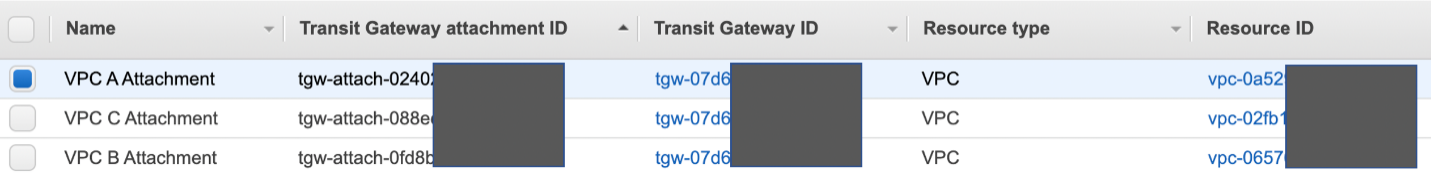
Create the VPC attachment for both availability zones in “VPC A” by choosing subnets we created on previous step for TGW:

[Graphical user interface

Description automatically generated with medium confidence](https://networking.workshop.aws/beginner/lab1/030_tgw/nid_create_tgw_att.png)

Repeat these steps to create attachments for “VPC B” and “VPC C”.

Upon completion, you should see three Transit Gateway attachments:

[](https://networking.workshop.aws/beginner/lab1/030_tgw/image49.png)

3 Check Transit Gateway route table

Navigate to “Transit Gateways” - [Transit Gateway Route Tables](https://console.aws.amazon.com/vpc/home?#TransitGatewayRouteTables:sort=transitGatewayRouteTableId).

[Graphical user interface, application

Description automatically generated](https://networking.workshop.aws/beginner/lab1/030_tgw/image50.png)

You should see one Route Table, click on it. Click on “Routes” tab. Your routing table should be populated with “VPC A”, “VPC B”, “VPC C” routes:

[Graphical user interface, application

Description automatically generated](https://networking.workshop.aws/beginner/lab1/030_tgw/image51.png)

4 Update Route Tables of VPCs

Navigate to [Route Tables](https://console.aws.amazon.com/vpc/home?#RouteTables:sort=routeTableId), select “VPC A Route Table”, click on “Routes” tab and click “Edit routes”:

[Text

Description automatically generated](https://networking.workshop.aws/beginner/lab1/030_tgw/image52.png)

Add route entries for “VPC B” and “VPC C”. To simplify the configuration, create a single 10.0.0.0/8 route pointing to the Transit Gateway. You can do this because the local route is more specific and therefore in this instance 10.0.0.0/16 will traverse the more specific local route and anything else in the 10.0.0.0/8 will traverse the less specific route to the transit gateway.

[Graphical user interface

Description automatically generated](https://networking.workshop.aws/beginner/lab1/030_tgw/image53.png)

Repeat these steps for “VPC B’s” and VPC C’s” routing tables.

5 Check EC2 connectivity via TGW

Proceed to [EC2 Console](https://console.aws.amazon.com/ec2/v2/home?#Instances:instanceState=running).

Connect to EC2 instance in “VPC A” (via “Session Manager”).

Try pinging private IPs of instances deployed in “VPC B” and “VPC C”. Ping should be successful.

Connect to EC2 instance in “VPC B”. Try pinging private IPs of instances deployed in “VPC A” and “VPC C”. Ping should be successful.

You validated that EC2 instances in all three VPCs can reach each other using Transit Gateway.