

***Challenge

- First need to associate the remote TGW from the primary region
- Then add route of 10.0.8.0/24 to the remote TGW

Advanced Architecting on AWS – Lab 2: Configuring Transit Gateways



© 2021 Amazon Web Services, Inc. and its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. All trademarks are the property of their owners.

Corrections, feedback, or other questions? Contact us at [AWS Training and Certification](#).

Lab Overview

Lab Overview

You can connect Amazon Virtual Private Cloud (Amazon VPC) pairs using peering. However, managing point-to-point connectivity across many Amazon VPCs, without the ability to centrally manage the connectivity policies, can be operationally costly and cumbersome. For on-premises connectivity, you need to attach your AWS VPN to each individual Amazon VPC. This solution can be time-consuming to build and hard to manage when the number of VPCs grows into the hundreds.

With AWS Transit Gateway, you only have to create and manage a single connection from the central gateway to each VPC, on-premises data center, or remote office across your network. A transit gateway acts as a hub that controls how traffic is routed among all the connected networks, which act like spokes. This hub-and-spoke model significantly simplifies management and reduces operational costs because each network only has to connect to the transit gateway and not to every other network. Connect any new VPC to the transit gateway, and the VPC is then automatically available to every other network that is connected to the transit gateway. This ease of connectivity simplifies the ability to scale your network as you grow.

In this lab, you build and configure routing via transit gateways with multiple levels of complexity. You start by inspecting existing VPCs, subnets, route tables, and Amazon Elastic Compute Cloud (Amazon EC2) instances. You then create a transit gateway and attach four existing VPCs to the gateway. You investigate the default route table on the transit gateway, which allows all-all communication between VPCs attached to the transit gateway. After confirming a functional transit gateway, you then modify the route tables on the transit gateway to isolate communication between specific VPCs. Lastly, you peer two transit gateways across regional boundaries to show how you can configure a global network with transit gateways.

The ability to peer transit gateways between different AWS Regions enables customers to extend this connectivity and build global networks spanning multiple AWS Regions. Traffic using inter-region transit gateway peering always stays on the AWS global network and never traverses the public internet. This reduces threat vectors, such as common exploits and distributed denial of service (DDoS) attacks. Inter-region transit gateway peering encrypts inter-region traffic with no single point of failure.

Objectives

After completing this lab, you will be able to:

- Configure a transit gateway
- Attach VPCs to a transit gateway
- Control and customize routing with AWS Transit Gateway
- Peer transit gateways between two Regions
- Use Network Manager to visualize and analyze your network

Prerequisites

This lab requires:

- Access to a notebook computer with Wi-Fi and Microsoft Windows, macOS, or Linux (Ubuntu, SuSE, or Red Hat)
- An internet browser such as Chrome, Firefox, or Microsoft Edge
- A plaintext editor

Duration

This lab requires approximately **60** minutes to complete.

AWS Services Not Used in This Lab

AWS services that are not used in this lab are disabled in the lab environment. In addition, the capabilities of the services used in this lab are limited to what the lab requires. Expect errors when accessing other services or performing actions beyond those provided in this lab guide.

Lab Environment

As part of the lab, four EC2 instances are provisioned on separate VPCs in a primary

region. One EC2 instance and a transit gateway are provisioned in a remote region. You configure a transit gateway in the primary region, attach the VPCs to the transit gateway, update the routes, and verify that all EC2 instances within the primary region can communicate with each other. You then peer your transit gateway with the remote region and verify the network connections between all EC2 instances. Finally, you create route filters to limit connections between certain VPCs only.

All backend components, such as Amazon EC2 instances and AWS Identity and Access Management (IAM) roles, are built into your lab already.

AWS Transit Gateway: Connect your Amazon VPCs and on-premises networks to a single gateway. With Transit Gateway, your network is streamlined and scalable.

Amazon VPC: Launch AWS resources into a virtual network that you define. This virtual network closely resembles a traditional network that you would operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

AWS Transit Gateway Network Manager: Centrally manage your network across AWS and on-premises sites. Visualize your global network in a centralized dashboard as a logical diagram or geographic map. Monitor your network using Amazon CloudWatch metrics and events for changes in network topology, routing, and connection status.

The following diagram shows the resources provisioned for this lab and how they are connected at the end of the lab:



Start Lab

1. At the top of your screen, launch your lab by choosing **Start Lab**

This starts the process of provisioning your lab resources. An estimated amount of time to provision your lab resources is displayed. You must wait for your resources to be provisioned before continuing.

i If you are prompted for a token, use the one distributed to you (or credits you have purchased).

2. Open your lab by choosing **Open Console**

This opens an AWS Management Console sign-in page.

3. On the sign-in page, configure:

- **IAM user name:** `awsstudent`
- **Password:** Paste the value of **Password** from the left side of the lab page
- Choose **Sign In**

⚠ Do not change the Region unless instructed.

Common Login Errors

Error: You must first log out

Amazon Web Services Sign In

You must first log out before logging into a different AWS account.

To logout, [click here](#)

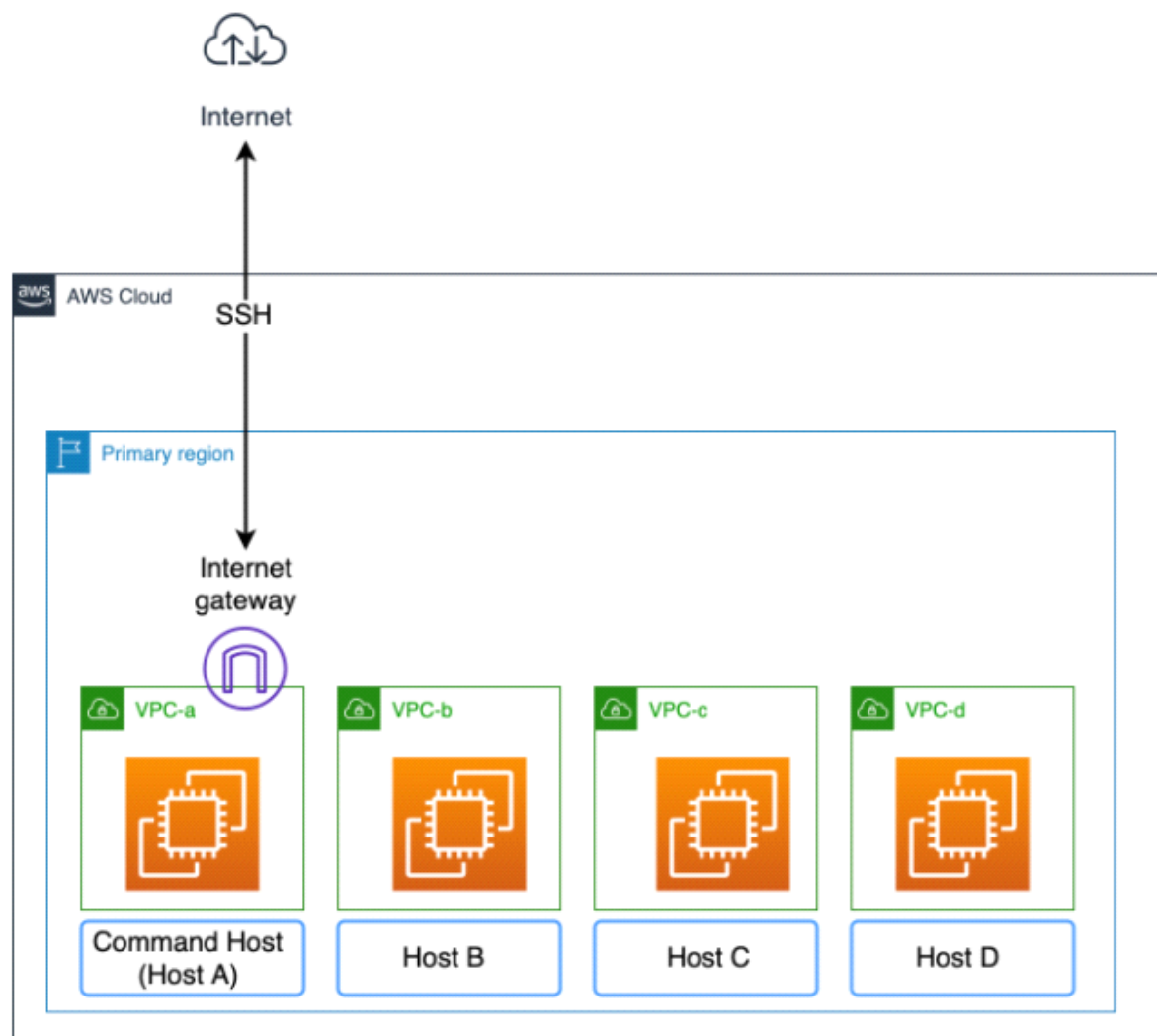
If you see the message, **You must first log out before logging into a different AWS account:**

- Choose **click here**

- Close your browser tab to return to your initial lab window
- Choose [Open Console](#) again

Task 1: Review the Network Topology and Create the Baseline

In this task, use the Internet Control Message Protocol (ICMP) to validate network reachability between the Command Host and other hosts. There are four Amazon EC2 instances, labelled host A thru D, in the same primary region, and each with their own VPC. Host A is in a public subnet and will be used as the command host. The following diagram shows this current configuration of the lab environment:



4. In the AWS Management Console, on the **Services** menu, choose **EC2**.

5. In the **Resources** section, choose **Instances (running)**.

Notice that four EC2 instances are running.

6. Choose each instance and review the **VPC ID** and **Subnet ID** contained in the **Details** tab.

Notice that each of the EC2 instances is hosted in a separate VPC.

7. Copy the **CommandHostSessionManagementUrl** value from the left side of the lab page, paste it in a new browser tab, and press ENTER.

The terminal for the Command Host instance opens.

Now, ping the public IP address for each of the instances. The IP addresses are found on the left side of the lab page. As you complete the next steps, record the results in your text editor. The following table is an example:

Table A: Ping Test Results

Host	Result
Host B	Pass/Fail
Host C	Pass/Fail
Host D	Pass/Fail

8. Run the following command. Replace *<Host IP address>* with the **HostB** IP address from the left side of the lab page:

```
ping <Host IP address>
```

9. After a few seconds, break the ICMP ping request by pressing CTRL+C.

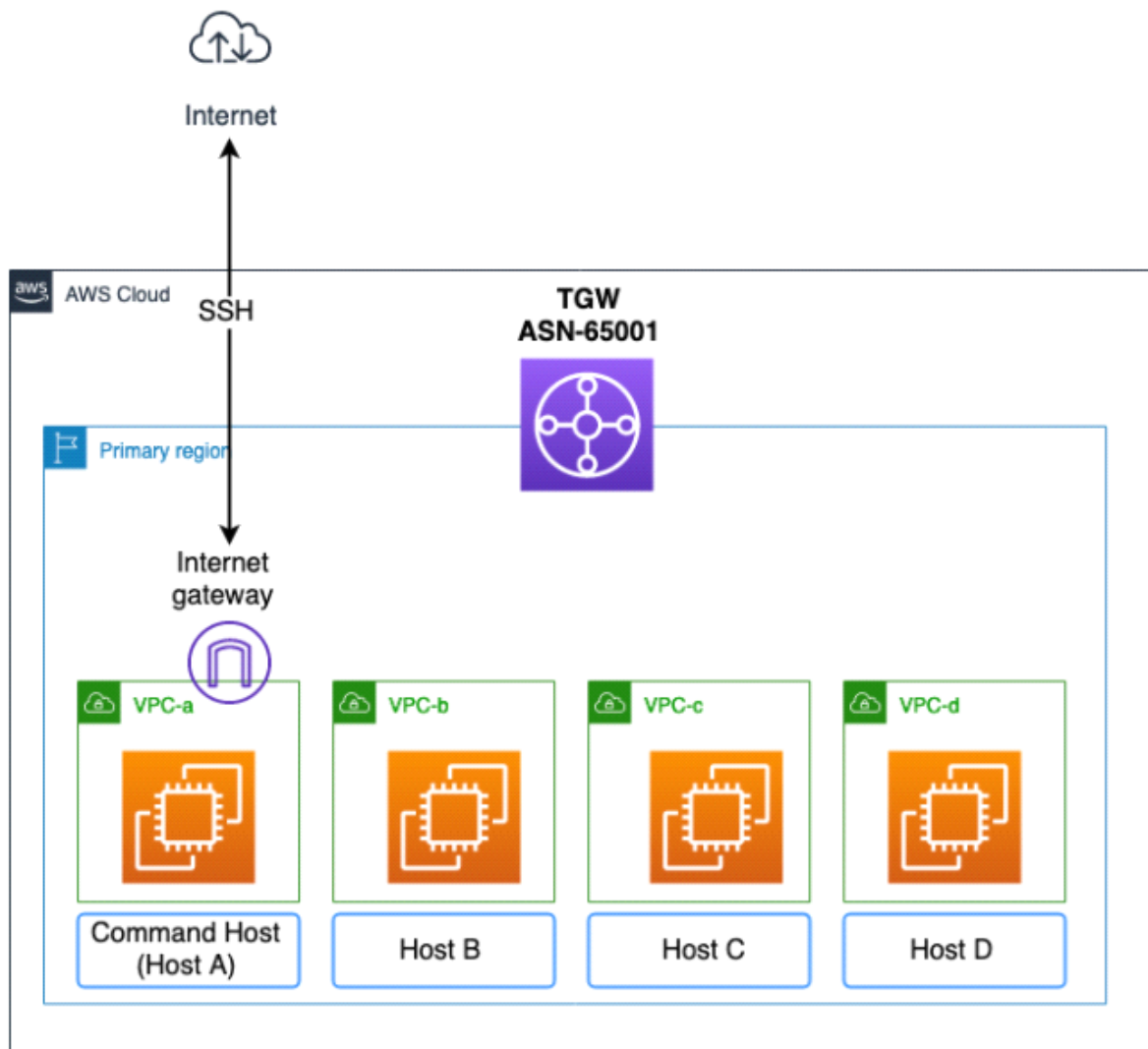
10. Repeat the previous steps to ping **HostC** and **HostD**.

Note: As each host is in its own private subnet with no routing configured between

— returns each host to its own private subnet with no routing configured between them. In this case, the ICMP ping is expected to have a timeout failure for each host.

Task 2: Create a Transit Gateway

In this task, you create a transit gateway in your primary region. A *transit gateway* is a network transit hub that interconnects attachments (VPCs and VPNs) within the same account or across accounts.



11. In the AWS Management Console, on the **Services** menu, choose **VPC**.

12. In the left navigation pane, scroll down to locate the **Transit Gateways** section.

12. In the left navigation pane, scroll down to locate the **Transit Gateways** section.

13. Choose **Transit Gateways**.

The 'Create Transit Gateway' page is displayed.

14. At the top of the page, choose **Create Transit Gateway**.

15. Configure the following:


- **Name tag:** maintransitgw
- **Amazon side ASN:** 65001
- Uncheck **VPN ECMP support**
- Uncheck **Default route table association**
- Uncheck **Default route table propagation**
- Choose **Create Transit Gateway**

Here you have used the private Autonomous System Number (ASN) for your transit gateway and enabled DNS support for the VPC attached to the transit gateway.

16. When the *Create Transit Gateway request succeeded* message is displayed, choose **Close** to return to the **Transit Gateways** page.

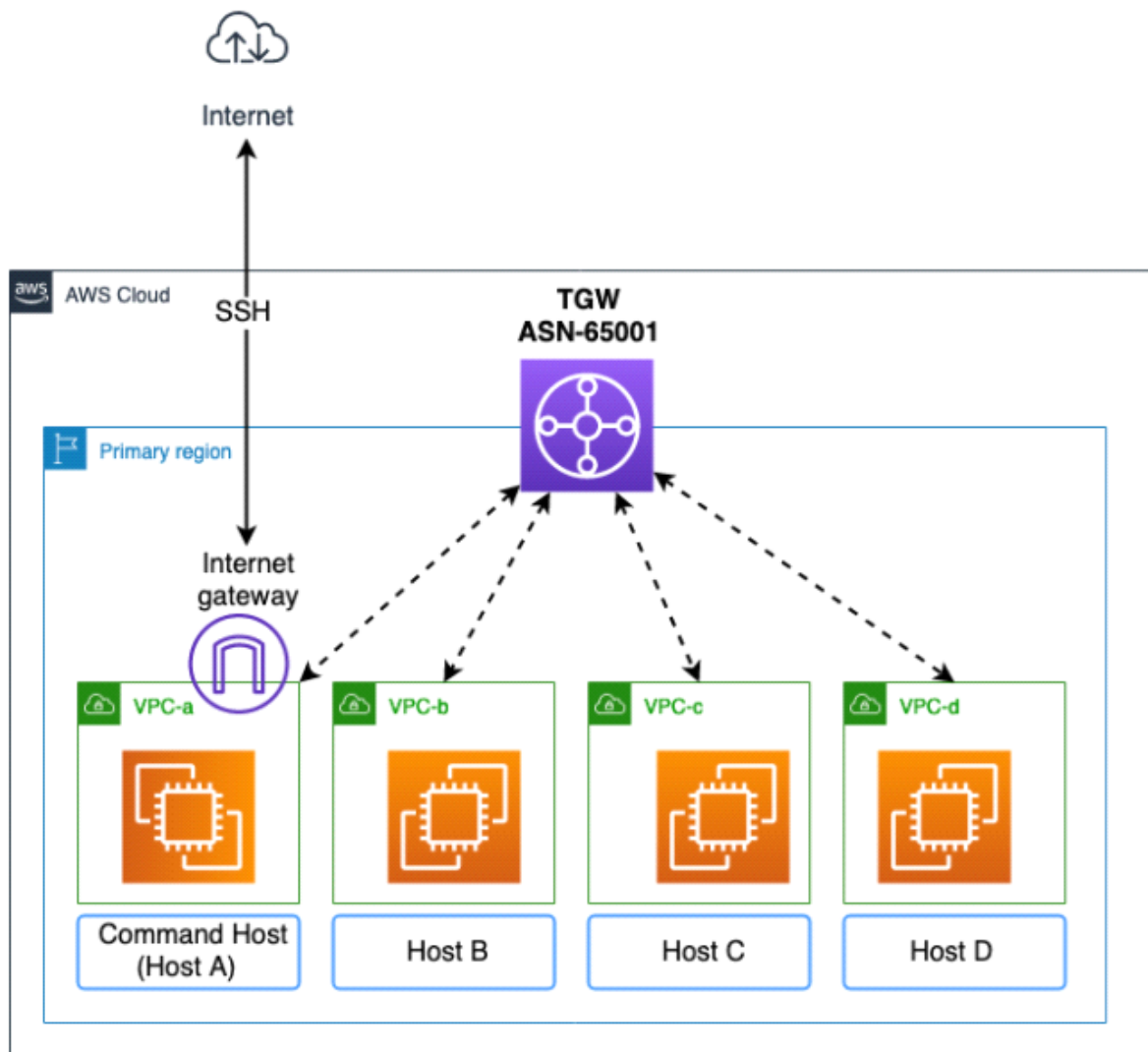
 **Note** It may take a few minutes to create the Transit Gateway.

17. Record the **Transit Gateway ID** in your text editor.

 **Learn more** A transit gateway acts as a regional virtual router for traffic flowing between your VPCs and VPN connections. For more information, refer to the link [How Transit Gateways Work](#).

Task 3: Create Transit Gateway Attachments

In this task, you attach the VPCs to the transit gateway, as shown in the following diagram:



18. In the left navigation pane, in the **Transit Gateways** section, choose **Transit Gateway Attachments**.

19. At the top of the page, choose **Create Transit Gateway Attachment**.

The 'Create Transit Gateway Attachment' page is displayed.

20. Configure the following:



- **Transit Gateway ID:** Select the transit gateway ID
- **Attachment type:** VPC
- **Attachment name tag:** vpc-a
- **VPC ID*:** Select the VPC with the name **vpc-a**
- Choose **Create attachment**

21. When the *Create Transit Gateway Attachment request succeeded* message is

displayed, choose **Close** to return to the **Transit Gateway Attachments** page.

 **Note** It may take a few minutes to create the Transit Gateway attachment.

22. Repeat the previous steps to attach **vpc-b**, **vpc-c**, and **vpc-d** to the transit gateway.

 **Caution** Wait for the state of all transit gateway attachments to be *available* before proceeding to the next task. To refresh the status, choose the refresh  icon at the top of the page.

Task 4: Create the Transit Gateway Route Table

In this task, use transit gateway route tables to configure routing for your transit gateway attachments. A *route table* controls how traffic flows for all associated attachments.

23. In the left navigation pane, in the **Transit Gateways** section, choose **Transit Gateway Route Tables**.

24. At the top of the page, choose **Create Transit Gateway Route Table**.

The 'Create Transit Gateway Route Table' page is displayed.

25. Configure the following:

- **Name Tag:** `maintransitgw-rt`
- **Transit Gateway ID*:** Select the transit gateway ID
- Choose **Create Transit Gateway Route Table**


26. When the *Create Transit Gateway route table request succeeded* message is displayed, choose **Close** to return to the **Transit Gateway Route Tables** page.

 **Note** It may take a few minutes for the route table to be created.

27. Refresh the page until the state shows *available*.


Create Route Table Associations

In this task, you associate a transit gateway route table with transit gateway attachments. Associating an attachment to a route table allows traffic to be sent from the attachment to the target route table.

 **Note** You can associate a transit gateway attachment with only one route table. Each route table can be associated with zero to many attachments and can forward packets to other attachments.


28. Select the transit gateway route table.


29. Select the **Associations** tab.

30. Choose .


The '*Create association*' page is displayed.

31. Configure the following:

- **Choose attachment to associate***: Select the attachment ID with the name tag **vpc-a**
- Choose 

32. When the *Transit Gateway route table association request succeeded* message is displayed, choose  to return to the **Transit Gateway Route Tables** page.

33. Repeat the previous steps to add associations for **vpc-b**, **vpc-c**, and **vpc-d** to the route table.

 **Note** It may take a few minutes for each association to be created. Refresh the page until the state of all attachments shows *associated*.

Create Route Propagations

In this task, use route propagation to add a route from a route table to an

In this task, use route propagation to add a route from a route table to an attachment. Adding a propagation enables routes to be propagated from an attachment to the target transit gateway route table. An attachment can be propagated to multiple route tables.

34. Select the **Propagations** tab.

35. Choose **Create propagation**.

The 'Create propagation' page is displayed.

36. Configure the following:

- **Choose attachment to propagate***: Select the attachment ID with the name tag **vpc-a**
- Choose **Create propagation**

37. When the *Transit Gateway route table propagation request succeeded* message is displayed, choose **Close** to return to the **Transit Gateway Route Tables** page.

38. Repeat the previous steps to create propagations for **vpc-b**, **vpc-c**, and **vpc-d**.

When you finish, you can review the subnets for all of the VPCs populated on the **Routes** tab.

Task 5: Update the VPC Route Tables

In this task, you add a route for the private subnet in each VPC to point to the transit gateway as the target destination. This way any traffic destined to any private subnet other than the local subnet is routed to the transit gateway.

39. In the left navigation pane, scroll up to the **Virtual Private Cloud** section, and choose **Route Tables**.


40. Select the route table with the name **vpc_a-public**.

41. From the **Actions** menu at the top of the page, choose **Edit routes**.

The 'Edit routes' page is displayed.

42. Choose **Add route** and configure the following:

- **Destination:** `10.0.0.0/8`
- **Target:** Copy and paste the transit gateway ID you copied in Task 1
- Choose **Save routes**

 **Note** For **Target**, you can also type `tgw` and choose the transit gateway with the name **maintransitgw**.

43. When the *Routes successfully edited* message is displayed, choose **Close** to return to the **Route Tables** page.

44. Repeat the previous steps to add this route to the **vpc_b-private**, **vpc_c-private**, and **vpc_d-private** route tables.

Network Validation

45. Copy the **CommandHostSessionManagementUrl** value from the left side of the lab page, paste it in a new browser tab, and press ENTER. The terminal for the Command Host instance opens.

Now, ping the IP address for each of the other instances. As you complete the next steps, record the results in your text editor.

46. Run the following command. Replace *<Host IP address>* with the **HostB** IP address from the left side of the lab page:

```
ping <Host IP address>
```

47. After a few seconds, break the ICMP ping request by pressing CTRL+C.

48. Repeat the previous steps to ping **HostC** and **HostD**.

49. Notice that **HostE** is in remote region and repeat the previous steps to ping **HostE**

? Question Your network reachability test should be successful for **HostB**, **HostC**, and **HostD**. However, it fails for **HostE**. Why?

Task 6: Create a Peering Connection to the Remote Region Transit Gateway

In this task, you peer your primary region transit gateway with a remote region transit gateway. AWS Transit Gateway uses the Autonomous System Number (ASN) to peer with another transit gateway. Border Gateway Protocol (BGP) is the routing protocol used for peering.

Record the Transit Gateway ID of the Remote Region

50. In the AWS Management Console, on the **Services** menu, choose **VPC**.

You now change the AWS Region to the **remote region**.

51. To the left of these lab instructions is a region labeled **RemoteRegion**.

52. At the top-right corner of the AWS console, choose the Region name, and select the Region that matches the **RemoteRegion** value found on the left side of the lab page.

53. In the left navigation pane, scroll down to the **Transit Gateways** section, and choose **Transit Gateways**.

54. Record the **Transit Gateway ID** for the remote gateway in your text editor.

Create the Transit Gateway Peering Connection

In this task, you add a peering connection with the remote region transit gateway.


In this task, you add a peering connection with the remote region transit gateway. You configure the peering connection in the primary region.

You now change the AWS Region back to the **primary region**.

55. To the left of these lab instructions is a region labeled **PrimaryRegion**.
56. At the top-right corner of the page, choose the Region name, and select the Region that matches the **PrimaryRegion** value found on the left side of the lab page.
57. In the left navigation pane, scroll down to the **Transit Gateways** section, and choose **Transit Gateway Attachments**.
58. At the top of the page, choose **Create Transit Gateway Attachment**.

The 'Create Transit Gateway Attachment' page is displayed.

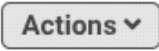
59. Configure the following:
 - **Transit Gateway ID:** Select the transit gateway
 - **Attachment type:** **Peering Connection**
 - **Attachment name tag:** `remote-vpc-e`
 - **Account:** **My account**
 - **Region:** Select the remote region name
 - **Transit gateway (accepter)*:** Copy and paste the transit gateway ID for the remote region that you recorded in the previous section
 - Choose **Create attachment**
60. When the *Create Transit Gateway Attachment request succeeded* message is displayed, choose **Close** to return to the **Transit Gateway Attachments** page.



 **Note** The state of the attachment changes to *initiating request* and then to *pending acceptance*.


Accept the Transit Gateway Peering Request - Remote Region



The target transit gateway must approve the peering connection request. In this task, you allow the peering connection from the **primary region** to the **remote region**.

You now change the AWS Region to the **remote region**.

61. To the left of these lab instructions is a region labeled **RemoteRegion**.
62. At the top-right corner of the AWS consol, choose the Region name, and select the Region that matches the **RemoteRegion** value found on the left side of the lab page.
63. In the left navigation pane, scroll down to the **Transit Gateways** section, and choose **Transit Gateway Attachments**.
64. Select the transit gateway attachment with the **Resource type** of *Peering*.
65. From the  menu, choose **Accept**.


 **Note** If **Accept** is not available, periodically choose the refresh  icon at the top of the page, and wait until the state changes to *pending acceptance*.

66. To confirm, choose .

 **Note** It may take a few minutes for the state of the attachment to change from **pending** to **available**. Periodically choose the refresh  icon at the top of the page, and wait until the state shows **available**.

Update the Route Table Association - Remote Region

In this task, you associate an attachment to a route table. This enables traffic to be sent from the attachment to the target route table.

67. In the left navigation pane, scroll down to the **Transit Gateways** section, and choose **Transit Gateway Route Tables**.
68. Choose the **Associations** tab.
69. Choose .

The '*Create association*' page is displayed.

70. Configure the following:

- **Choose attachment to associate***: Select the attachment ID with no name tag and has a **Resource Type** of *peering*
- Choose **Create association**

71. When the *Transit Gateway route table association request succeeded* message is displayed, choose **Close** to return to the **Transit Gateway Route Tables** page.

Update the Transit Gateway Route Table - Remote Region

In this task, you modify the default route of the remote region transit gateway to point to the peering transit gateway. By doing so, you can route traffic other than the local subnet to the peering transit gateway.

72. In the left navigation pane, scroll down to the **Transit Gateways** section, and choose **Transit Gateway Route Tables**.

73. Select the transit gateway route table with the name **remote-rt**.

74. Select the **Routes** tab.

75. Select the route with CIDR **0.0.0.0/0**.

76. Choose **Replace static route**

The '*Replace static route*' page is displayed.

77. Configure the following:

- **Choose attachment**: Select the attachment ID of the remote peer connection, which does not have a name tag and has a **Resource Type** of *peering*
- Choose **Replace static route**

78. When the *Replace Transit Gateway route request succeeded* message is displayed, choose **Close** to return to the **Transit Gateway Route Tables** page.

Update the VPC Route Table - Remote Region

In this task, you add a default route to point to the transit gateway. This enables

HostE to send non-local traffic to the transit gateway.


79. In the left navigation pane, scroll up to the **Virtual Private Cloud** section, and choose **Route Tables**.

80. Select the route table with the name **vpc_e-private**.

81. From the **Actions** menu, choose **Edit routes**.

82. Choose **Add route** and configure the following:

- **Destination:** `0.0.0.0/0`
- **Target:** Copy and paste the transit gateway ID of the remote region
- Choose **Save routes**

 **Note** For **Target**, you can also type `tgw` and choose the transit gateway with the name **remote-tgw**.


83. When the *Routes successfully edited* message is displayed, choose **Close** to return to the **Route Tables** page.

Network Validation

84. Repeat the steps from Task 1 to ping **HostB**, **HostC**, **HostD**, and **HostE**. Record your results.

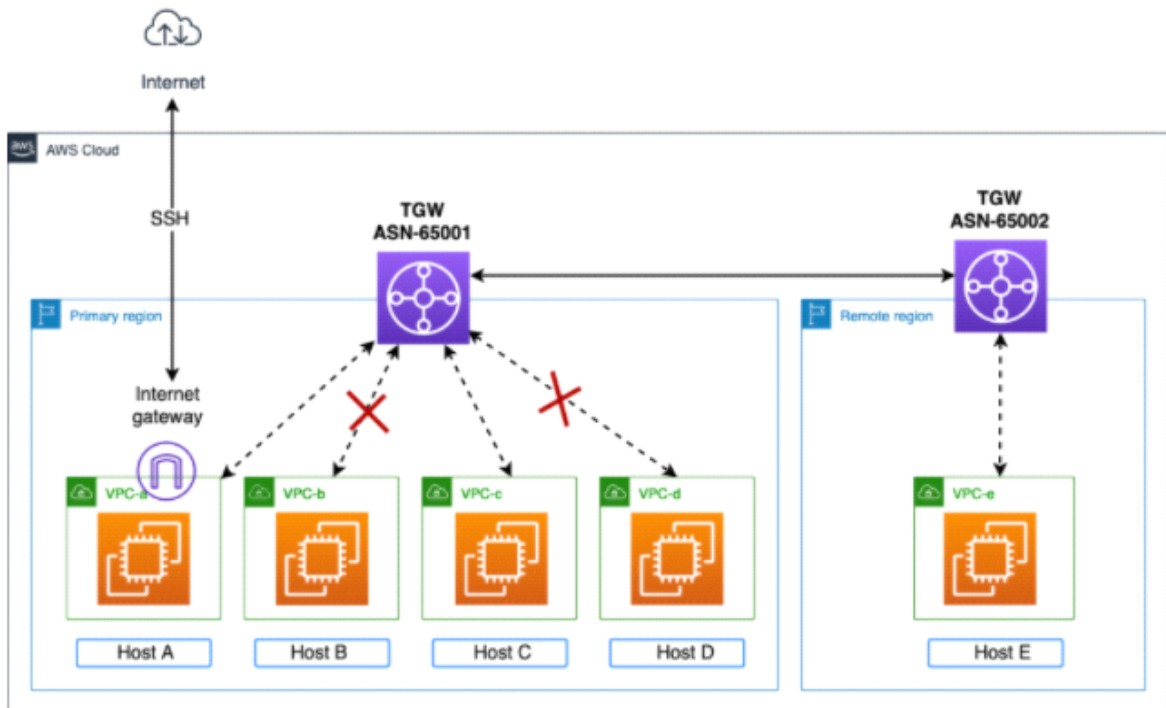
Challenge: Notice that the Command Host is still not able to ping HostE. Update the routes in the primary region so that the Command Host can ping HostE.

 [Select the link here](#) for the solution.

 **Note** After updating the routes, you should be able to reach all of the hosts.

Task 7: Create Route Filters

In this task, you use blackhole routes to filter your traffic. You create blackhole routes for subnets in VPC B and VPC D, as shown in the following diagram:



A *blackhole route* in your transit gateway route table drops traffic that matches the route.


85. To the left of these lab instructions is a region labeled **PrimaryRegion**.
86. At the top-right corner of the page, choose the Region name, and select the Region that matches the **PrimaryRegion** value found on the left side of the lab page.
87. In the AWS Management Console, on the **Services** menu, choose **VPC**.
88. In the left navigation pane, scroll down to the **Transit Gateways** section, and choose **Transit Gateway Route Tables**.
89. Select the **maintransitgw-rt** route table. From the **Actions** menu, select **Create static route**.

The 'Create static route' page is displayed.

90. Configure:

- **CIDR*:** `10.2.2.0/24`
- Select **Blackhole**
- Choose **Create static route**


91. When the *Create Transit Gateway route request succeeded* message is displayed, choose **Close** to return to the **Transit Gateway Route Tables** page.

 **Note** Choose the **Routes** tab to review the new route. If it does not immediately appear, refresh the page after a few seconds until the route appears.

92. Repeat the previous steps to add a blackhole route for the VPC D subnet (`10.4.4.0/24`).

Network Validation

93. Repeat the steps from Task 1 to ping **HostB**, **HostC**, **HostD**, and **HostE**. Record your results.

 **Note** The network reachability test to HostB and HostD should fail.

Task 8: Visualize and Analyze Your Network (Optional)

In this task, use Network Manager to visualize your global network in a centralized dashboard as a logical diagram or geographic map. Then, use the route analyzer to check routes between the Command Host and HostE.

94. In the AWS Management Console, on the **Services** menu, choose **VPC**.

95. In the left navigation pane, scroll down to the **Transit Gateways** section, and choose **Network Manager**.

96. Choose **Create a Global Network**

The 'Create global network' page is displayed.


97. Configure the following:

- **Name:** TGW-Network
- **Description:** Transit Gateway Network
- Choose **Create global network**

98. On the Global networks page, choose the ID that contains **global-network-xxxx**.

99. On the TGW-Network Dashboard, choose **Register Transit Gateway** to add your transit gateways for monitoring.

100. Select both transit gateways, and choose **Register Transit Gateway**

 **Note** It may take a few minutes for the state to change from *pending* to *available*. Periodically refresh the page until the state shows *available*.

Visualize the Network

101. To return to the network dashboard page, in the left navigation pane, choose **Dashboard**.

102. Review the **Geographic**, **Topology**, and **Monitoring** tabs.

On this dashboard, you can visualize your global network in a topology diagram and a geographical map. You can review utilization metrics, such as bytes in/out, packets in/out, and packets dropped. You can also review alerts for changes in the topology, routing, and up/down connection status.

Analyze a Route

103. Choose the **Route Analyzer** tab.

104. Configure the following:

Source

- **Transit Gateway:** *maintransitgw*
- **Transit Gateway attachment:** *vpc-a*
- **IP address:** Copy and paste the *CommandHostPrivateIP* IP address from the left side of the lab page
- Select **Include return path in results**


Destination

- **Transit Gateway:** *remote-tgw*
- **Transit Gateway attachment:** *vpc-e*
- **IP address:** Copy and paste the *HostE* IP address from the left side of the lab page

105. To analyze the network path, choose **Run route analysis**.

You can review the forward and return network path between the Command Host and HostE. You can use this feature to troubleshoot network issues between two endpoints.

Conclusion

 Congratulations! You now have successfully:


- Configured a transit gateway
- Attached VPCs to a transit gateway
- Controlled and customized routing with AWS Transit Gateway
- Peered transit gateways between two Regions
- Used Network Manager to visualize and analyze your network


End Lab

Follow these steps to close the console, end your lab, and evaluate the experience.

106. Return to the AWS Management Console.

107. On the navigation bar, choose **awsstudent@<AccountNumber>**, and then choose **Sign Out**.

108. Choose  **End Lab**

109. Choose  **OK**

110. (Optional):

- Select the applicable number of stars ☆
- Type a comment
- Choose **Submit**
 - 1 star = Very dissatisfied
 - 2 stars = Dissatisfied
 - 3 stars = Neutral
 - 4 stars = Satisfied
 - 5 stars = Very satisfied

You may close the window if you don't want to provide feedback.

For more information about AWS Training and Certification, see <http://aws.amazon.com/training/>.

Your feedback is welcome and appreciated.

If you would like to share any feedback, suggestions, or corrections, please provide the details in our [AWS Training and Certification Contact Form](#).


Appendix

Challenge Solution


Update the Route Table Association for the Primary Region

First, add the remote peering attachment to the route table.


111. Ensure you are in the **primary region** within the console.


 **Note** To change the Region: At the top-right corner of the page, choose the Region name, and select the Region that matches the **PrimaryRegion** value found on the left side of the lab page.

112. In the left navigation pane, scroll down to the **Transit Gateways** section, and choose **Transit Gateway Route Tables**.

113. On the **Associations** tab, choose 

114. Configure:


- **Choose attachment to associate***: Select the **Attachment ID** with the name tag **remote-vpc-e**
- Choose 

115. When the *Transit Gateway route table association request succeeded* message is displayed, choose  to return to the **Transit Gateway Route Tables** page.

Update the Transit Gateway Route Table for the Primary Region

Second, add a static route table to add the VPC E subnet from the remote region to point to the peering transit gateway association. This way, the transit gateway can route traffic destined to VPC E.

116. Select the **maintransitgw** transit gateway.


117. On the **Routes** tab, choose 

118. Configure:

118. Configure:

- **CIDR*:** 10.0.0.0/16
- **Choose attachment:** Select the attachment ID with the name tag **remote-vpc-e**
- Choose **Create static route**

119. When the *Create Transit Gateway route request succeeded* message is displayed, choose **Close** to return to the **Transit Gateway Route Tables** page.

 **Note** Choose the **Routes** tab to review the new route. If it does not immediately appear, refresh the page after a few seconds until the route appears.

Network Validation

120. Repeat the steps from Task 1 to ping **HostB**, **HostC**, **HostD**, and **HostE**. Record your results.

The Command Host should now be able to successfully ping Host E.

[Select the link here](#) to continue to the next task.