# What is AWS Direct Connect?

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection, you can create virtual interfaces directly to public AWS services (for example, to Amazon S3) or to Amazon VPC, bypassing internet service providers in your network path. An AWS Direct Connect location provides access to AWS in the Region with which it is associated. You can use a single connection in a public Region or AWS GovCloud (US) to access public AWS services in all other public Regions.

The following diagram shows how AWS Direct Connect interfaces with your network.


    AWS Direct Connect
  

## AWS Direct Connect Components

The following are the key components that you use for AWS Direct Connect:

**Connections**

Create a connection in an AWS Direct Connect location to establish a network connection from your premises to an AWS Region.

**Virtual interfaces**

Create a virtual interface to enable access to AWS services. A public virtual interface enables access to public services, such as Amazon S3. A private virtual interface enables access to your VPC. For more information,

When you create a private virtual interface to a VPC, you need a private virtual interface for each VPC to which to connect. For example, you need three private virtual interfaces to connect to three VPCs.

**(Recommended) Configure Redundant Connections**

To provide for failover, we recommend that you request and configure two dedicated connections to AWS, as shown in the following figure. These connections can terminate on one or two routers in your network.


                Redundant connection diagram
            

There are different configuration choices available when you provision two dedicated connections:

* Active/Active (BGP multipath). This is the default configuration, where both connections are active. AWS Direct Connect supports multipathing to multiple virtual interfaces within the same location, and traffic is load-shared between interfaces based on flow. If one connection becomes unavailable, all traffic is routed through the other connection.
* Active/Passive (failover). One connection is handling traffic, and the other is on standby. If the active connection becomes unavailable, all traffic is routed through the passive connection. You need to prepend the AS path to the routes on one of your links for that to be the passive link.

# AWS Direct Connect Connections

AWS Direct Connect enables you to establish a dedicated network connection between your network and one of the AWS Direct Connect locations.

There are two types of connections:

* Dedicated Connection: A 1G or 10G physical Ethernet connection associated with a single customer. Customers can request a dedicated connection through the AWS Direct Connect console, the CLI, or the API.
* Hosted Connection: A 1G or 10G physical Ethernet connection that an AWS Direct Connect Partner provisions on behalf of a customer. Customers request a hosted connection by contacting a partner in the AWS Direct Connect Partner Program, who provisions the connection.

# Requesting Cross Connects at AWS Direct Connect Locations

After you have downloaded your Letter of Authorization and Connecting Facility Assignment (LOA-CFA), you must complete your cross-network connection, also known as a cross connect. If you already have equipment located in an AWS Direct Connect location, contact the appropriate provider to complete the cross connect. After the cross connect is established, you can create the virtual interfaces using the AWS Direct Connect console.

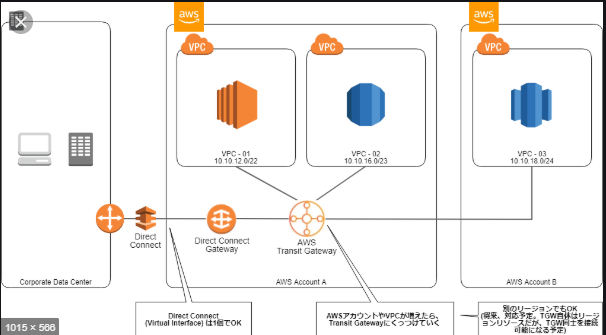
If you do not already have equipment located in an AWS Direct Connect location, you can work with one of the partners in the AWS Partner Network (APN). They help you to connect to an AWS Direct Connect location. An AWS Direct Connect connection can provide access to resources in other Regions. For more information.

# AWS Direct Connect Virtual Interfaces

You must create one of the following virtual interfaces to begin using your AWS Direct Connect connection.

* Private virtual interface: A private virtual interface should be used to access an Amazon VPC using private IP addresses.
* Public virtual interface: A public virtual interface can access all AWS public services using public IP addresses.
* Transit virtual interface: A transit virtual interface should be used to access one or more Amazon VPC Transit Gateways associated with Direct Connect gateways.

A connection of less than 1 Gbps supports only one virtual interface.



## Hosted Virtual Interfaces

To use your AWS Direct Connect connection with another AWS account, you can create a hosted virtual interface for that account. The owner of the other account must accept the hosted virtual interface to begin using it. A hosted virtual interface works the same as a standard virtual interface and can connect to public resources or a VPC.

## Creating a Transit Virtual Interface to the Direct Connect Gateway

To connect your AWS Direct Connect connection to the transit gateway, you must create a transit interface for your connection. Specify the Direct Connect gateway to which to connect.

**Important**

If you associate your transit gateway with one or more Direct Connect gateways, the Autonomous System Number (ASN) used by the transit gateway and the Direct Connect gateway must be different. For example, if you use the default ASN 64512 for both the transit gateway and the Direct Connect gateway, the association request fails.

# Setting Network MTU for Private Virtual Interfaces or Transit Virtual Interfaces

AWS Direct Connect supports an Ethernet frame size of 1522 or 9023 bytes (14 bytes Ethernet header + 4 bytes VLAN tag + bytes for the IP datagram + 4 bytes FCS) at the link layer.

The maximum transmission unit (MTU) of a network connection is the size, in bytes, of the largest permissible packet that can be passed over the connection. The MTU of a virtual private interface can be either 1500 or 9001 (jumbo frames). The MTU of a transit virtual interface can be either 1500 or 8500 (jumbo frames). You can specify the MTU when you create the interface or update it after you create it. Setting the MTU of a virtual interface to 8500 (jumbo frames) or 9001 (jumbo frames) can cause an update to the underlying physical connection if it wasn't updated to support jumbo frames. Updating the connection disrupts network connectivity for all virtual interfaces associated with the connection for up to 30 seconds.

After you enable jumbo frames for your private virtual interface, you can only associate it with a connection or LAG that is jumbo frame capable. Jumbo frames are supported on virtual private interfaces attached to a virtual private gateway or a Direct Connect gateway.

# Deleting Virtual Interfaces

Delete one or more virtual interfaces. Before you can delete a connection, you must delete its virtual interface.

# Link Aggregation Groups

A link aggregation group (LAG) is a logical interface that uses the Link Aggregation Control Protocol (LACP) to aggregate multiple connections at a single AWS Direct Connect endpoint, allowing you to treat them as a single, managed connection.

You can create a LAG from existing connections, or you can provision new connections. After you've created the LAG, you can associate existing connections (whether standalone or part of another LAG) with the LAG.

The following rules apply:

* All connections in the LAG must use the same bandwidth.
* You can have a maximum of four connections in a LAG. Each connection in the LAG counts towards your overall connection limit for the Region.
* All connections in the LAG must terminate at the same AWS Direct Connect endpoint.

Important –

* For existing connections, connectivity to AWS is interrupted during the creation of the LAG.
* If the connection is already associated with another LAG, you cannot re-associate it if removing the connection causes the original LAG to fall below its threshold for the minimum number of operational connections.
* Convert a connection to standalone by disassociating it from a LAG. You can't disassociate a connection if it causes the LAG to fall below its threshold for the minimum number of operational connections.

All LAGs have an attribute that determines the minimum number of connections in the LAG that must be operational for the LAG itself to be operational. By default, new LAGs have this attribute set to 0. You can update your LAG to specify a different value—doing so means that your entire LAG becomes non-operational if the number of operational connections falls below this threshold. This attribute can be used to prevent over-utilization of the remaining connections.

All connections in a LAG operate in Active/Active mode.

**Note**

When you create a LAG or associate more connections with the LAG, we may not be able to guarantee enough available ports on a given AWS Direct Connect endpoint.

# Direct Connect Gateways

Use AWS Direct Connect gateway to connect your VPCs. You associate an AWS Direct Connect gateway with either of the following gateways:

* A transit gateway when you have multiple VPCs in the same Region
* A virtual private gateway

A Direct Connect gateway is a globally available resource. You can create the Direct Connect gateway in any public Region and access it from all other public Regions.

# Virtual Private Gateway Associations

You can use an AWS Direct Connect gateway to connect your AWS Direct Connect connection over a private virtual interface to one or more VPCs in your account that are located in the same or different Regions. You associate a Direct Connect gateway with the virtual private gateway for the VPC. Then, you create a private virtual interface for your AWS Direct Connect connection to the Direct Connect gateway. You can attach multiple private virtual interfaces to your Direct Connect gateway.

In the following diagram, the Direct Connect gateway enables you to use your AWS Direct Connect connection in the US East (N. Virginia) Region to access VPCs in your account in both the US East (N. Virginia) and US West (N. California) Regions.


                Direct connect gateway
            

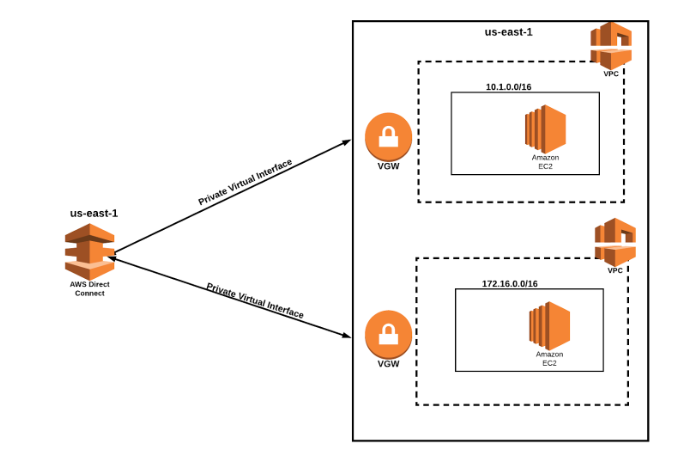
The following rules apply:

* You cannot use a Direct Connect gateway to connect to a VPC in the China Regions.
* The VPCs to which you connect through a Direct Connect gateway cannot have overlapping CIDR blocks
* The transit virtual interface can be in any location, but currently the transit gateway must reside in the United States.
* You cannot create a public virtual interface to a Direct Connect gateway.
* A Direct Connect gateway supports communication between attached private virtual interfaces and associated virtual private gateways only. The following traffic flows are not supported:
  + Direct communication between the VPCs that are associated with the Direct Connect gateway.
  + Direct communication between the virtual interfaces that are attached to the Direct Connect gateway.
  + Direct communication between a virtual interface attached to a Direct Connect gateway and a VPN connection on a virtual private gateway that's associated with the same Direct Connect gateway.
* You cannot associate a virtual private gateway with more than one Direct Connect gateway and you cannot attach a private virtual interface to more than one Direct Connect gateway.
* A virtual private gateway that you associate with a Direct Connect gateway must be attached to a VPC.
* A virtual private gateway association proposal expires 7 days after it is created.
* An accepted virtual private gateway proposal, or a deleted virtual private gateway proposal remains visible for 3 days.

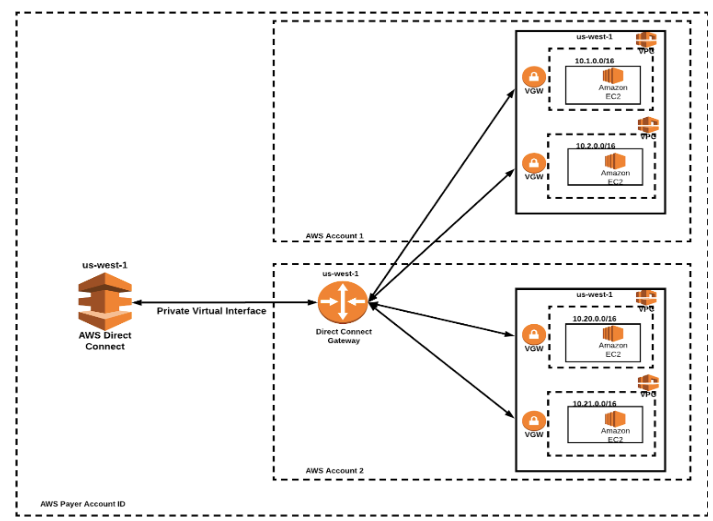
To connect your AWS Direct Connect connection to a VPC in the same Region only, you can create a Direct Connect gateway. Or, you can create a private virtual interface and attach it to the virtual private gateway for the VPC.

To use your AWS Direct Connect connection with a VPC in another account, you can create a hosted private virtual interface for that account. When the owner of the other account accepts the hosted virtual interface, they can choose to attach it either to a virtual private gateway or to a Direct Connect gateway in their account. For more information, see [AWS Direct Connect Virtual Interfaces](https://docs.aws.amazon.com/directconnect/latest/UserGuide/WorkingWithVirtualInterfaces.html).

BEFORE



AFTER



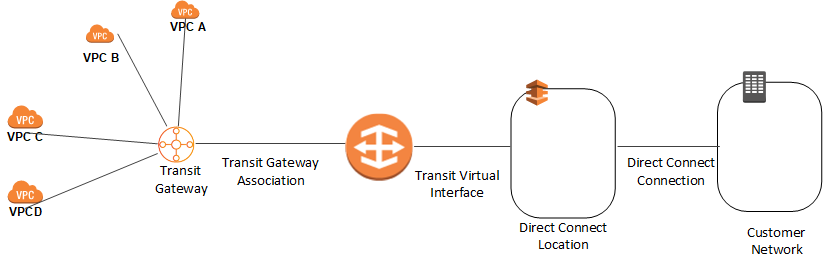
# Transit Gateway Associations

You can use an AWS Direct Connect gateway to connect your AWS Direct Connect connection over a transit virtual interface to the VPCs or VPNs that are attached to your transit gateway. You associate a Direct Connect gateway with the transit gateway. Then, create a transit virtual interface for your AWS Direct Connect connection to the Direct Connect gateway.

This configuration offers the following benefits. You can:

* Manage a single connection for multiple VPCs or VPNs that are in the same Region.
* Advertise prefixes from on-premises to AWS and from AWS to on-premises.

The following diagram illustrates how the Direct Connect gateway enables you to create a single connection to your Direct Connect connection that all of your VPCs can use.



The solution involves the following components:

* A transit gateway that has VPC attachments.
* A Direct Connect gateway.
* An association between the Direct Connect gateway and the transit gateway.
* A transit virtual interface that is attached to the Direct Connect gateway.

The following rules apply:

* You cannot use a Direct Connect gateway and a transit gateway in the China Regions.
* You cannot attach a Direct Connect gateway to a transit gateway when the Direct Connect gateway is already associated with a virtual private gateway or is attached to a private virtual interface.
* A Direct Connect gateway supports communication between attached transit virtual interfaces and associated transit gateways only.
* The transit virtual interface can be in any location, but currently the transit gateway must reside in the United States.

The following Regions support transit gateway associations:

* US East (N. Virginia)
* US East (Ohio)
* US West (N. California) - San Francisco
* US West (Oregon) - Portland
* AWS GovCloud (US-East)
* AWS GovCloud (US-West)
* Canada (Central) Region - Montreal
* EU (Ireland) - Dublin

# Logging AWS Direct Connect API Calls Using AWS CloudTrail

AWS Direct Connect is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS Direct Connect. CloudTrail captures all API calls for AWS Direct Connect as events. The calls captured include calls from the AWS Direct Connect console and code calls to the AWS Direct Connect API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for AWS Direct Connect. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to AWS Direct Connect, the IP address from which the request was made, who made the request, when it was made, and additional details.

# Monitoring AWS Direct Connect

## Monitoring Tools

AWS provides various tools that you can use to monitor an AWS Direct Connect connection. You can configure some of these tools to do the monitoring for you, while some of the tools require manual intervention. We recommend that you automate monitoring tasks as much as possible.

### Automated Monitoring Tools

You can use the following automated monitoring tools to watch AWS Direct Connect and report when something is wrong:

* **Amazon CloudWatch Alarms** – Watch a single metric over a time period that you specify. Perform one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The action is a notification sent to an Amazon SNS topic. CloudWatch alarms do not invoke actions simply because they are in a particular state; the state must have changed and been maintained for a specified number of periods.
* **AWS CloudTrail Log Monitoring** – Share log files between accounts and monitor CloudTrail log files in real time by sending them to CloudWatch Logs. You can also write log processing applications in Java and validate that your log files have not changed after delivery by CloudTrail.

### Manual Monitoring Tools

Another important part of monitoring an AWS Direct Connect connection involves manually monitoring those items that the CloudWatch alarms don't cover. The AWS Direct Connect and CloudWatch console dashboards provide an at-a-glance view of the state of your AWS environment.

* The AWS Direct Connect console shows:
  + Connection status (see the **State** column)
  + Virtual interface status (see the **State** column)
* The CloudWatch home page shows:
  + Current alarms and status
  + Graphs of alarms and resources
  + Service health status

In addition, you can use CloudWatch to do the following:

* + Create [customized dashboards](https://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/CloudWatch_Dashboards.html) to monitor the services you care about.
  + Graph metric data to troubleshoot issues and discover trends.
  + Search and browse all your AWS resource metrics.
  + Create and edit alarms to be notified of problems.

# Troubleshooting AWS Direct Connect

The following topics can help you troubleshoot issues with your AWS Direct Connect connection.

## Troubleshooting Layer 1 (Physical) Issues

If you or your network provider are having difficulty establishing physical connectivity to an AWS Direct Connect device, use the following steps to troubleshoot the issue.

1. Verify with the colocation provider that the cross connect is complete. Ask them or your network provider to provide you with a cross connect completion notice and compare the ports with those listed on your LOA-CFA.
2. Verify that your router or your provider's router is powered on and that the ports are activated.
3. Ensure that the routers are using the correct optical transceiver, auto-negotiation is disabled, and port speed and full-duplex mode are manually configured. For more information, see [Network Requirements](https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html#overview_requirements).
4. Verify that the router is receiving an acceptable optical signal over the cross connect.
5. Try flipping (also known as rolling) the Tx/Rx fiber strands.
6. Check the Amazon CloudWatch metrics for AWS Direct Connect. You can verify the AWS Direct Connect device's Tx/Rx optical readings (10-Gbps port speeds only), physical error count, and operational status.

The following flow chart contains the steps to diagnose issues with the physical connection.

## Troubleshooting Layer 2 (Data Link) Issues

If your AWS Direct Connect physical connection is up but your virtual interface is down, use the following steps to troubleshoot the issue.

1. If you cannot ping the Amazon peer IP address, verify that your peer IP address is configured correctly and in the correct VLAN. Ensure that the IP address is configured in the VLAN subinterface and not the physical interface (for example, GigabitEthernet0/0.123 instead of GigabitEthernet0/0).
2. Verify if the router has a MAC address entry from the AWS endpoint in your address resolution protocol (ARP) table.
3. Ensure that any intermediate devices between endpoints have VLAN trunking enabled for your 802.1Q VLAN tag. ARP cannot be established on the AWS side until AWS receives tagged traffic.
4. Clear your or your provider's ARP table cache.
5. If the above steps do not establish ARP or you still cannot ping the Amazon peer IP, [contact AWS Support](https://aws.amazon.com/support/createCase).

The following flow chart contains the steps to diagnose issues with the data link.

## Troubleshooting Layer 3/4 (Network/Transport) Issues

Consider a situation where your AWS Direct Connect physical connection is up and you can ping the Amazon peer IP address. If your virtual interface is down and the BGP peering session cannot be established, use the following steps to troubleshoot the issue:

1. Ensure that your BGP local Autonomous System Number (ASN) and Amazon's ASN are configured correctly.
2. Ensure that the peer IPs for both sides of the BGP peering session are configured correctly.
3. Ensure that your MD5 authentication key is configured and exactly matches the key in the downloaded router configuration file. Check that there are no extra spaces or characters.
4. Verify that you or your provider are not advertising more than 100 prefixes for private virtual interfaces or 1,000 prefixes for public virtual interfaces. These are hard limits and cannot be exceeded.
5. Ensure that there are no firewall or ACL rules that are blocking TCP port 179 or any high-numbered ephemeral TCP ports. These ports are necessary for BGP to establish a TCP connection between the peers.
6. Check your BGP logs for any errors or warning messages.

The following flow chart contains the steps to diagnose issues with the BGP peering session.

## Troubleshooting Routing Issues

Consider a situation where your virtual interface is up and you've established a BGP peering session. If you cannot route traffic over the virtual interface, use the following steps to troubleshoot the issue:

1. Ensure that you are advertising a route for your on-premises network prefix over the BGP session. For a private virtual interface, this can be a private or public network prefix. For a public virtual interface, this must be your publicly routable network prefix.
2. For a private virtual interface, ensure that your VPC security groups and network ACLs allow inbound and outbound traffic for your on-premises network prefix.
3. For a private virtual interface, ensure that your VPC route tables have prefixes pointing to the virtual private gateway to which your private virtual interface is connected. For example, if you prefer to have all your traffic routed towards your on-premises network by default, you can add the default route (0.0.0.0/0 or ::/0) with the virtual private gateway as the target in your VPC route tables.
   * Alternatively, enable route propagation to automatically update routes in your route tables based on your dynamic BGP route advertisement. You can have up to 100 propagated routes per route table. This limit cannot be increased. For more information, see [Enabling and Disabling Route Propagation](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html#EnableDisableRouteProp) in the Amazon VPC User Guide.