Cornell AWS Direct Connect FAQs

What are the requirements for using Direct Connect?

VPCs to be connected to Direct Connect **must** be using an officially allocated CIDR block from Cornell's private network. Normally, when a Cornell AWS customer requests Direct Connect, the Cloud Team will allocate a CIDR from Cornell's private network and create a brand new VPC using that CIDR.

What's the cost of using Direct Connect?

Customer Direct Connect costs depend entirely on the volume of traffic sent across the Direct Connect architecture. See Cornell AWS Direct Connect Costs

I don't really use the Direct Connect in my AWS account. Can I remove that feature?

If you do not need or use Direct Connect in your AWS account, you'll be saving Cornell money if you request that Direct Connect be removed. Contact cloud-support@cornell.edu to request that change.

Does Direct Connect remove the need for peering VPCs?

We use a Transit Gateway (TGW) in our Direct Connect architecture. One of the features of this architecture is that all VPCs using Direct Connect are also completed interconnected. In many cases, this removes the need to directly peer VPCs. However there are some situations where VPC-peering still makes sense. See Peering AWS VPCs that Use Direct Connect

What traffic is routed through the Direct Connect?

There are three choices. See diagrams in Cornell AWS Direct Connect Routing Diagrams.

RFC1918 Routing
For Cornell AWS accounts with DC configured for RFC1918 routing, only 10-space traffic (specifically 10.0.0.0/8) is routed from on-campus 10-space to 10-space addresses in Cornell Standard AWS VPCs. This means that traffic from servers and clients with (only) public campus IP addresses cannot access the 10-space networks in a Cornell Standard AWS VPC.

All Campus Routing
For Cornell AWS accounts with DC configured for "All Campus" routing, traffic from campus 10-space as well as traffic from public campus IPs is routed through the DC to the Cornell Standard AWS VPC. This routing can be problematic if you intend to deploy services available to the world in your Cornell Standard VPC.

The campus public IP space consists of the following:

- 128.84.0.0/16
- 128.253.0.0/16
- 132.236.0.0/16
- 192.35.82.0/24
- 192.122.235.0/24
- 192.122.236.0/24

Hybrid Routing

Similar to the "All Campus Routing" above, this configuration brings all of the Cornell campus IP space (10-space and public addresses) over the Direct Connect. Where it differs is in the individual subnet route tables:

- **Private Subnets:** AWS subnets without direct Internet access should use a route table that includes all propagated routes from the Direct Connect (includes campus 10-space and public space).

- **Public Subnets:** AWS subnets with direct Internet access (IGW) should use a route table that *disables* route propagation from Direct Connect and only includes references to campus 10-space addresses.

Can I change the traffic routed through Direct Connect?

The configuration for Cornell campus traffic routed through Direct Connect to your VPC can be altered should your needs change in the future. Moving among the routing options ("RFC 1918", "All-Campus", "Hybrid") may require a review of your subnet route tables to ensure a smooth transition without any negative side-effects. See Cornell AWS Direct Connect Routing Diagrams.

What are the physical details of Cornell's Direct Connect to AWS?

Both the two Direct Connect connections are 1Gbps. These connections run in an active-active configuration. See Cornell AWS Direct Connect Architecture for details.

Is Cornell's Direct Connect monitored?

Yes, both the CIT Cloud and Networks teams monitor the Direct Connect and will be alerted when either connection fails.

Since the pre-2023 Direct Connect architecture utilized campus-based hardware, the traffic volume of those connections were easily viewed on Cornell's MRTG tool. Since the 2023 migration to I2CC as the Direct Connect vendor, MRTG cannot show the DC traffic. Let us know if you really, really need to see these metrics.

Is there a disaster recovery plan for our Direct Connect connectivity?

There is no specific disaster recovery plan for our Direct Connect connectivity. We rely on the high availability baked into the design of our Direct Connect architecture to weather individual connection failures.

Both our I2CC Direct Connect connections are linked directly to the us-east-1 AWS region. In the event of a regional failure of us-east-1, Direct Connect service may be interrupted. Our design does not include multi-region DC connectivity because a vast majority of Cornell AWS accounts using Direct Connect operate only in us-east-1.