What is Anycast? | How does Anycast work?

Anycast is a network addressing and routing method in which incoming requests can be routed to a variety of different locations.

Learning Center What is a CDN? CDN Benefits CDN Metrics How Caching W

Learning Objectives

After reading this article you will be able to:

- Explain Anycast Network Routing
- Differentiate between Anycast and Unicast
- See How Anycast mitigates DDoS attacks

RELATED CONTENT

What is a CDN?

CDN Performance

Origin Server

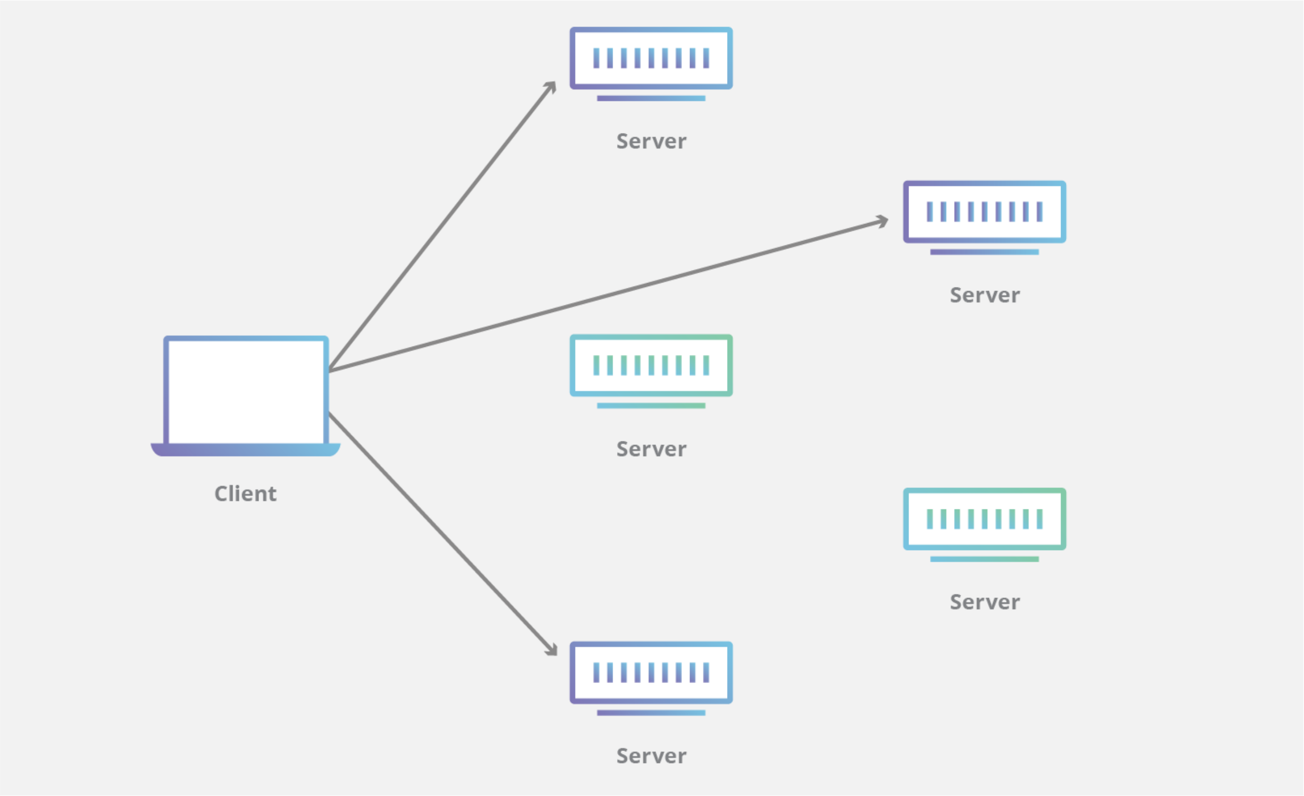
What is an Edge Server?

What is a CDN Data Center?

Copy article link

What is Anycast?

Anycast is a network addressing and routing method in which incoming requests can be routed to a variety of different locations or “nodes.” In the context of a CDN, Anycast typically routes incoming traffic to the nearest data center with the capacity to process the request efficiently. Selective routing allows an Anycast network to be resilient in the face of high traffic volume, network congestion, and DDoS attacks.



How does Anycast Work?

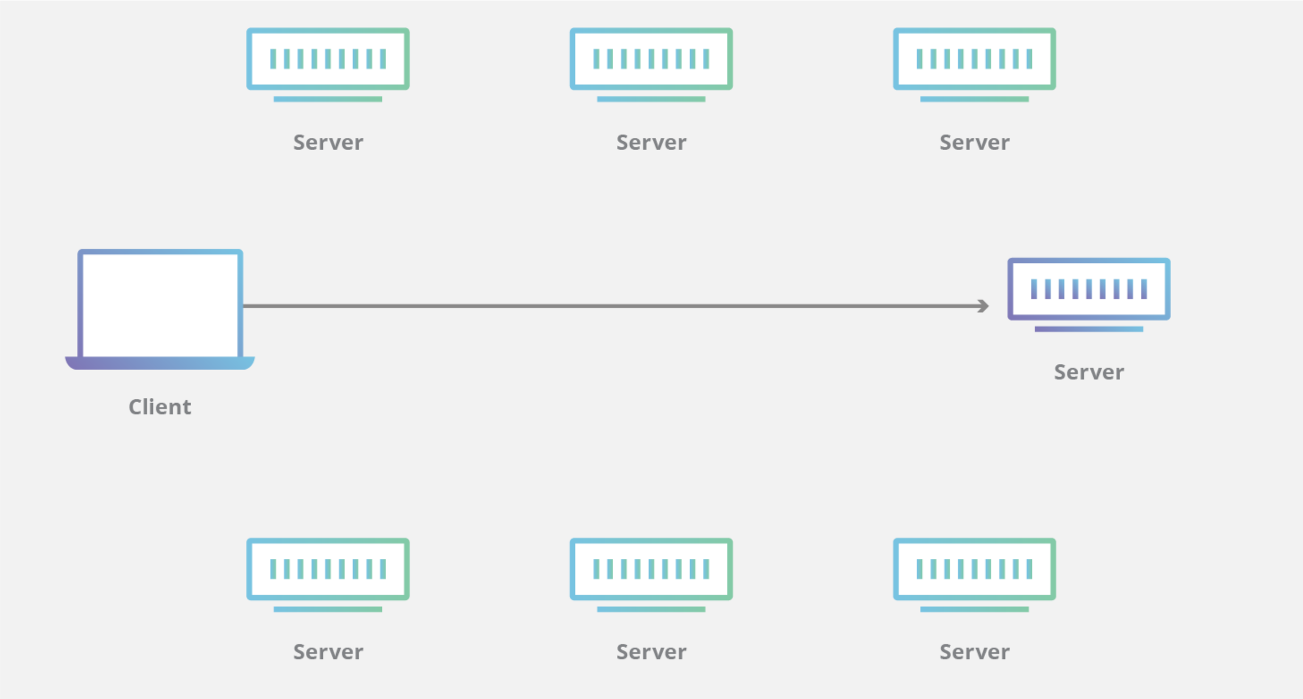
Anycast network routing is able to route incoming connection requests across multiple data centers. When requests come into a single IP address associated with the Anycast network, the network distributes the data based on some prioritization methodology. The selection process behind choosing a particular data center will typically be optimized to reduce latency by selecting the data center with the shortest distance from the requester. Anycast is characterized by a 1-to-1 of many association, and is one of the 5 main network protocol methods used in the Internet protocol.

Why Use an Anycast Network?

If many requests are made simultaneously to the same origin server, the server may become overwhelmed with traffic and be unable to respond efficiently to additional incoming requests. With an Anycast network, instead of one origin server taking the brunt of the traffic, the load can also be spread across other available data centers, each of which will have servers capable of processing and responding to the incoming request. This routing method can prevent an origin server from extending capacity and avoids service interruptions to clients requesting content from the origin server.

What is the Difference between Anycast and Unicast?

Most of the Internet works via a routing scheme called Unicast. Under Unicast, every node on the network gets a unique IP address. Home and office networks use Unicast; when a computer is connected to a wireless network and gets a message saying the IP address is already in use, an IP address conflict has occurred because another computer on the same Unicast network is already using the same IP. In most cases, that isn't allowed.

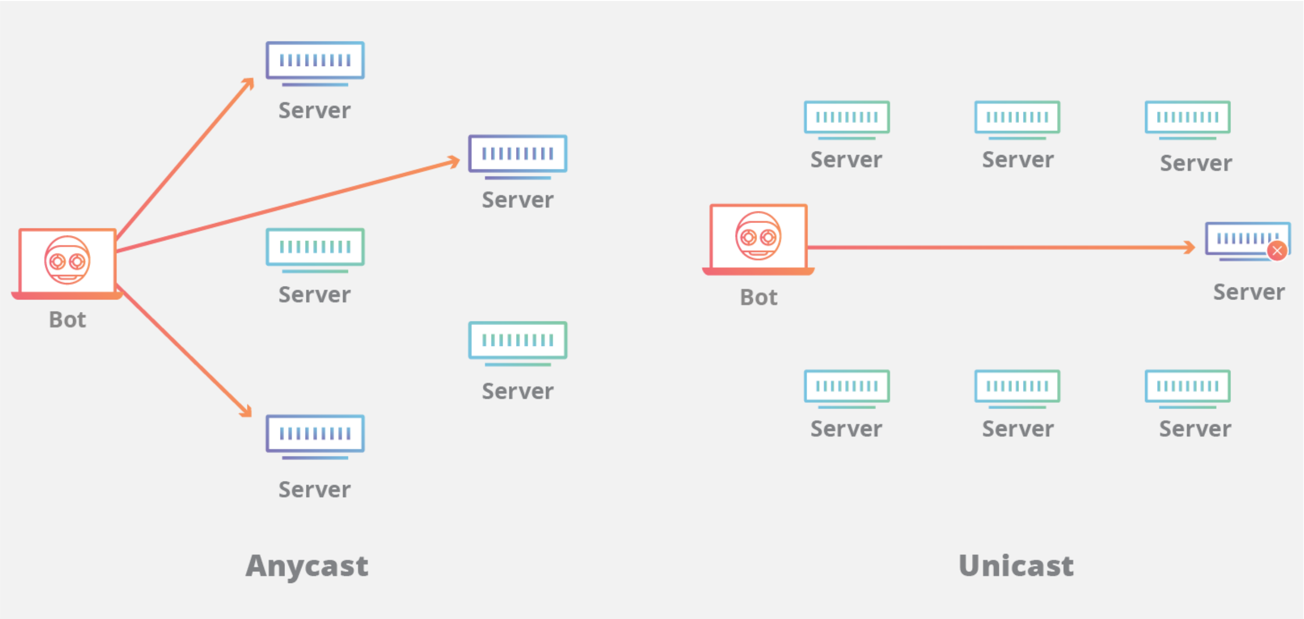


When a CDN is using a unicast address, traffic is routed directly to the specific node. This creates a vulnerability when the network experiences extraordinary traffic such as during a DDoS attack. Because the traffic is routed directly to a particular data center, the location or its surrounding infrastructure may become overwhelmed with traffic, potentially resulting in denial-of-service to legitimate requests.

Using Anycast means the network can be extremely resilient. Because traffic will find the best path, an entire data center can be taken offline and traffic will automatically flow to a proximal data center.

How does an Anycast network mitigate a DDoS attack?

After other DDoS mitigation tools filter out some of the attack traffic, Anycast distributes the remaining attack traffic across multiple data centers, preventing any one location from becoming overwhelmed with requests. If the capacity of the Anycast network is greater than the attack traffic, the attack is effectively mitigated. In most DDoS attacks, many compromised "zombie" or “bot” computers are used to form what is known as a botnet. These machines can be scattered around the web and generate so much traffic that they can overwhelm a typical Unicast-connected machine.



A properly Anycasted CDN increases the surface area of the receiving network so that the unfiltered denial-of-service traffic from a distributed botnet will be absorbed by each of the CDN’s data centers. As a result, as a network continues to grow in size and capacity it becomes harder and harder to launch an effective DDoS against anyone using the CDN.

It is not easy to setup a true Anycasted network. Proper implementation requires that a CDN provider maintains their own network hardware, builds direct relationships with their upstream carriers, and tunes their networking routes to ensure traffic doesn't "flap" between multiple locations. This Cloudflare blog post explains how Cloudflare uses Anycast to load balance without load balancers.