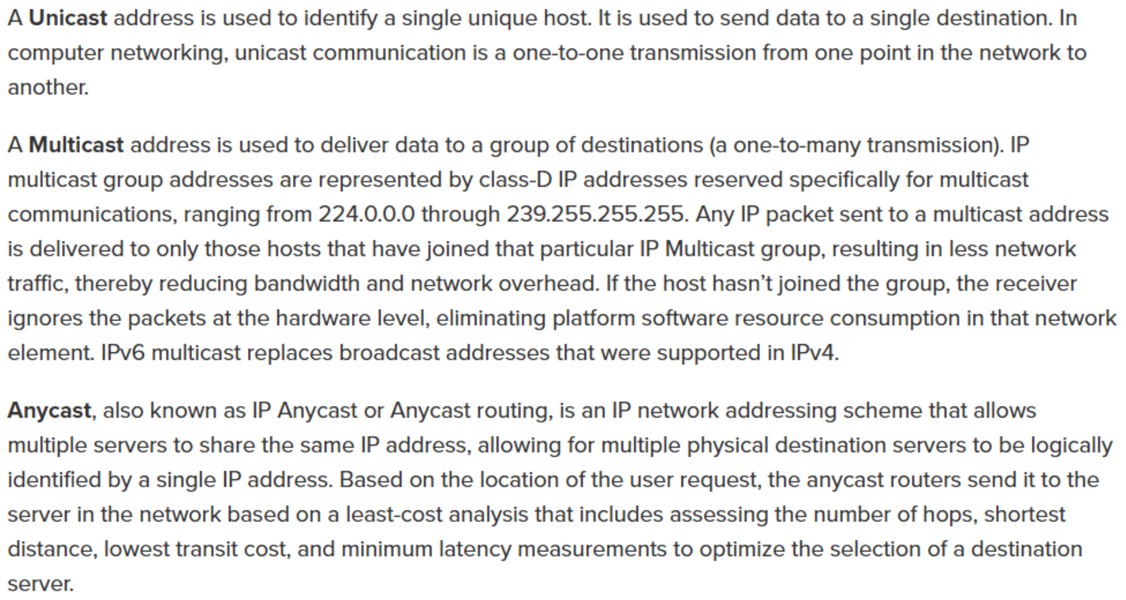
ANYCAST

CDN service providers use Anycast to efficiently distribute content for faster network access in CDN networks. An anycast-enabled CDN assigns the same IP address to multiple edge servers, relying on IP routing to deliver requests to the servers that are nearby in the network to the clients originating the requests. Another CDN anycast methodology used is where anycast-based CDN load balancing provides access to replicated media content. In conjunction with routing protocols, Anycast can optimally route content requests to any one of the replicated content server nodes to maintain service scalability.



A **Unicast** address is used to identify a single unique host. It is used to send data to a single destination. In computer networking, unicast communication is a one-to-one transmission from one point in the network to another.

A **Multicast** address is used to deliver data to a group of destinations (a one-to-many transmission). IP multicast group addresses are represented by class-D IP addresses reserved specifically for multicast communications, ranging from 224.0.0.0 through 239.255.255.255. Any IP packet sent to a multicast address is delivered to only those hosts that have joined that particular IP Multicast group, resulting in less network traffic, thereby reducing bandwidth and network overhead. If the host hasn't joined the group, the receiver ignores the packets at the hardware level, eliminating platform software resource consumption in that network element. IPv6 multicast replaces broadcast addresses that were supported in IPv4.

Anycast, also known as IP Anycast or Anycast routing, is an IP network addressing scheme that allows multiple servers to share the same IP address, allowing for multiple physical destination servers to be logically identified by a single IP address. Based on the location of the user request, the anycast routers send it to the server in the network based on a least-cost analysis that includes assessing the number of hops, shortest distance, lowest transit cost, and minimum latency measurements to optimize the selection of a destination server.

Anycast is associated with the core routing capabilities of the Border Gateway Protocol (BGP). The BGP anycast IP address or prefix is advertised from multiple locations. This route propagates across the Internet, enabling BGP to "advertise" awareness of the shortest path to the advertised prefix and publish multiple secondary sources paths to reach the destination IP address. This enables picking an anycast server "relatively close" to the location of a user's data request.

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.

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.

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.

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.

DNS stands for domain name system, and it's the system that translates domain names (the names of websites) into alphanumeric IP addresses that machines can read. This is known as "resolving" a domain name, and DNS resolvers are the servers that manage the resolving. When a user wants to load a website, the client device needs to query a DNS resolver for the IP address of that website.

Anycast makes DNS resolving much faster. With Anycast DNS, a DNS query will go to a network of DNS resolvers rather than to one specific resolver, and will be routed to whichever resolver is closest and available. DNS queries and responses will follow optimized paths in order to answer queries as quickly as possible.

Anycast also helps keep DNS resolving services highly available. If one DNS resolver goes offline, queries can still be answered by other resolvers in the network.