

# How Anycast Works to Bring Content Closer to Your Visitors

When you type `www.someplace.com` into the address bar of your browser and press enter, the site is displayed in your browser in (hopefully) a few seconds. There are a number of things happening behind the scenes to route your request to that site so you can view the content. [Border gateway protocol](#) (BGP) ensures that your request arrives at the server for that site via the best route through the internet.

There are a few methodologies to address the target server, and in this post we will discuss one of them, anycast addressing, in detail.

## What is Anycast?

In [anycast](#), a collection of servers share the same IP address and send data from a source computer to the server that is topographically the closest. This helps cut down on latency and bandwidth costs, improves load time for users, and improves availability. It is important to remember that topographically closer does not inherently mean geographically closer, though this is often the case.

Anycast is linked with the BGP protocol which ensures that all of a router's neighbors are aware of the networks that can be reached through that router and the topographical distance to those networks. The main principle of anycast is that an IP address range is advertised in the BGP messages of multiple routers. As this propagates across the Internet, routers become aware of which of their neighbors provides the shortest topographical path to the advertised IP address.

## Addressing Methods

These other primary addressing methods are available to route traffic.

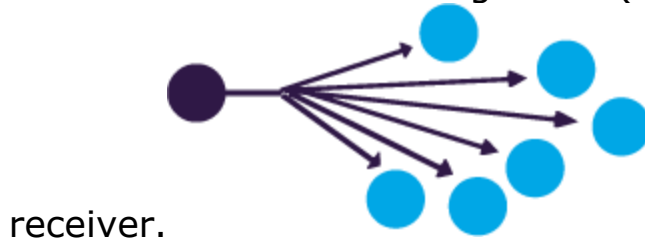
- **Unicast addressing** uses a *one-to-one* association, where each destination address is uniquely identified as a single receiver endpoint. Traditional DNS deployments are configured with



- **Multicast addressing** uses a *one-to-unique many* association, where datagrams are routed from a single sender to multiple selected endpoints in a single transmission, using a multicast group address. A common use of multicast is streaming audio, where the audio is published via multicast addressing and clients pick up the routed stream as a channel.



- **Broadcast addressing** uses a *one-to-many* association, where datagrams are routed from a single sender to all other connected endpoints in a single transmission, using a broadcast address. The network automatically replicates datagrams as needed for all network segments (links) that contain an eligible

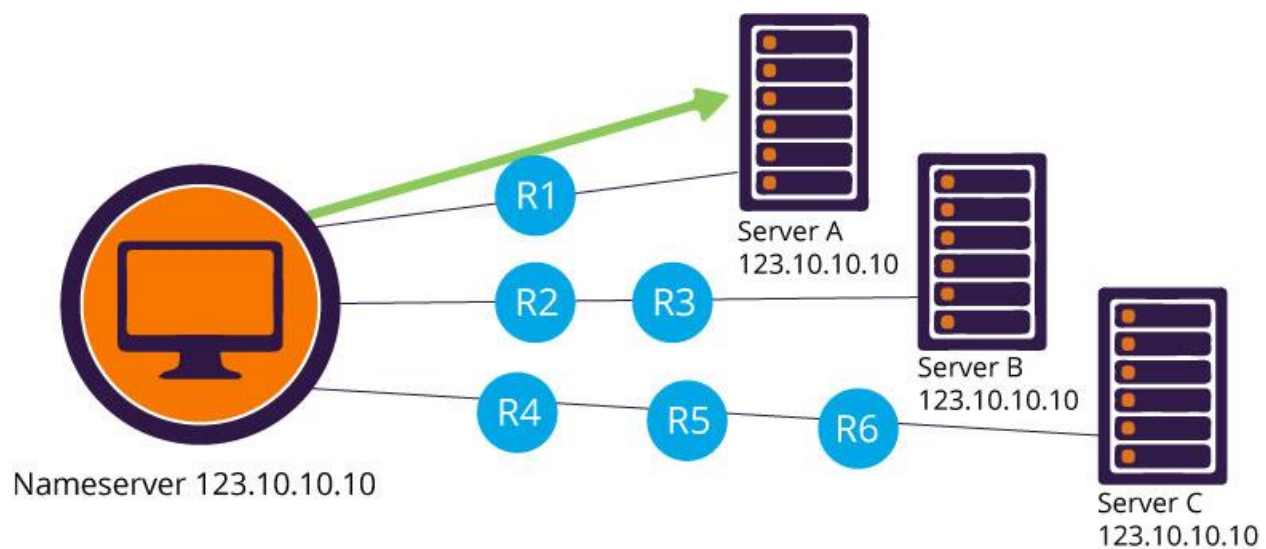


## DNS Anycast

With Unicast, [DNS](#) client resolvers can be configured with multiple DNS name server targets. In the event the resolver doesn't receive any response from the first server on the list, it will typically wait a time out value, before it switches to the second server (and

subsequent servers) in the resolver list. The next time the resolver has to perform a look up, it won't "remember" servers in the list were non-responsive, and it will start querying with the first server in the list even though it is still unavailable. Depending on the operating system of the client, it could be one to five seconds as it rotates through the resolver list each time, attempting the failed server.

DNS client resolvers configured with anycast addresses virtually eliminate this latency, since the resolution is handled by the routing protocol. In the diagram below a single DNS client workstation, configured with the anycast DNS IP address of 123.10.10.10, is shown performing DNS resolution against its closest of three DNS name servers deployed using the same anycast IP address.



The client's DNS resolver can resolve against any one of the three DNS servers shown above. Layer 3 routing would send our DNS client's packets through router R1 due to the routing topology. Should router R1 or Server A fail, our DNS client's packets would automatically be rerouted to the next nearest DNS server via routers R2 and R3. Additionally, the route to our server A, would be removed from the routing tables, thus preventing

further use of that name server. Server A won't be used until it is restored and the IP anycast address routes reinjected to the network.

Let's draw an analogy from everyday life to make all of this a bit more understandable.

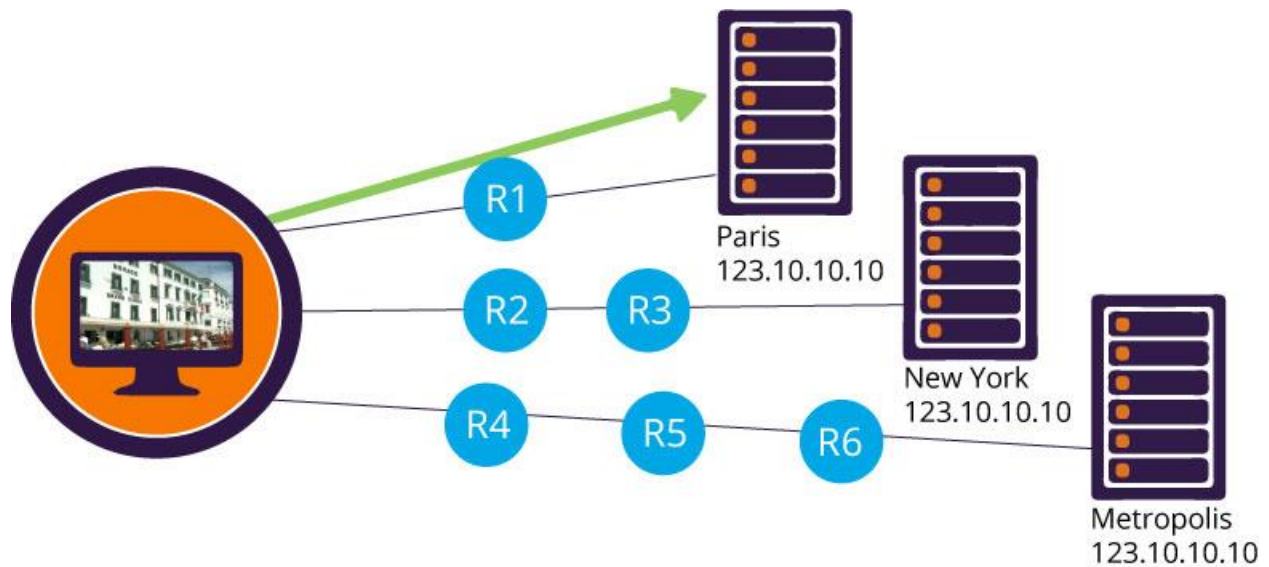
Imagine the shoes you've wanted are on sale and are available at all branches of a department store chain. Just like in anycast, you can be serviced at many identical sites, with no reason to prefer any specific site. So you enter "Marks and Spencer" into Waze, and the navigator will take you the nearest available branch to purchase those shoes. If the road to the nearest branch is blocked, Waze will take you to the next nearest branch.

## **Why Anycast?**

The question, you might be asking, is why use anycast routing instead of the simpler unicast routing, which will get your request to that same IP address.

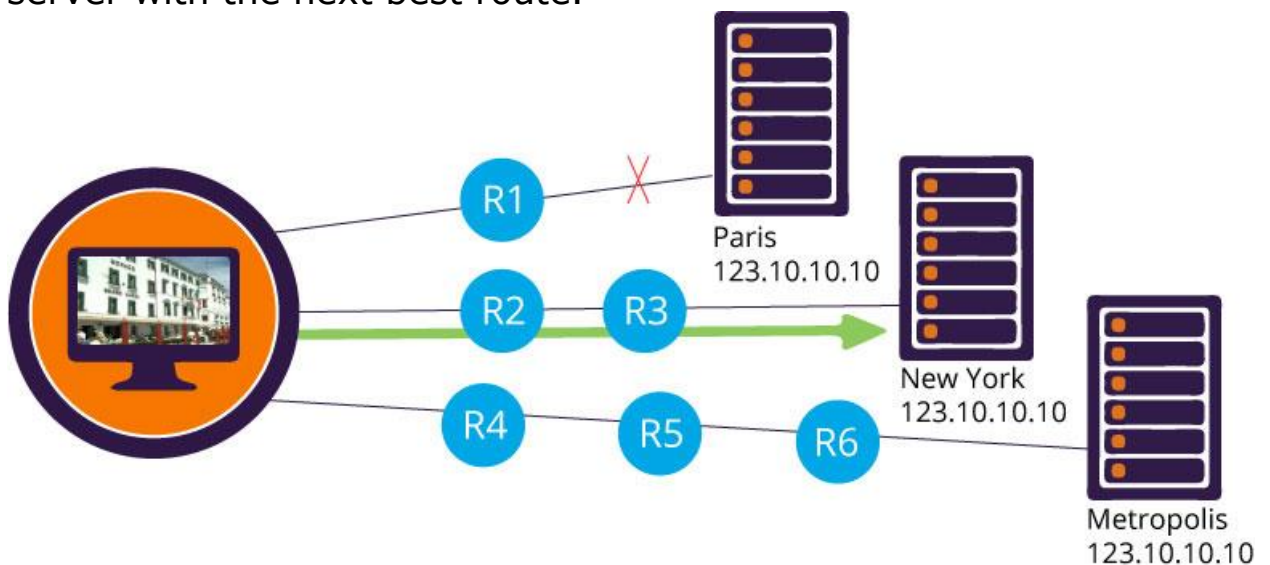
Unicast routing is certainly adequate and appropriate for a site with a single web server to accommodate a moderate amount of traffic. Imagine you are sitting with your computer at a café on the Canal Grande and accessing [www.venicegazette.com](http://www.venicegazette.com), which has 843 hits an hour. That site will have one web server and your request will quickly be routed to that Unicast address.

However it will not be so simple when you next access [www.dailyplanet.com](http://www.dailyplanet.com) to read Lois Lane's latest article. Since that paper has millions of subscribers, there are multiple web servers each with the same IP address, dispersed geographically, to serve requests.



The advantages of anycast in such a scenario are:

- **Performance improvement** — Traffic is routed with negligible latency to the user as discussed above
- **Service reliability** – With redundant servers, the service is more highly available. For example, if the Paris server is under maintenance, service will automatically be routed to an available server with the next best route.



- **Load balancing** – Routing to multiple servers will effectively balance load among the servers, improving site speed

- **Reduces impact of DoS attacks** – The denial of service attack will likely be localized to a server and therefore not impact the entire service

Reference: <https://www.imperva.com/blog/how-anycast-works/>