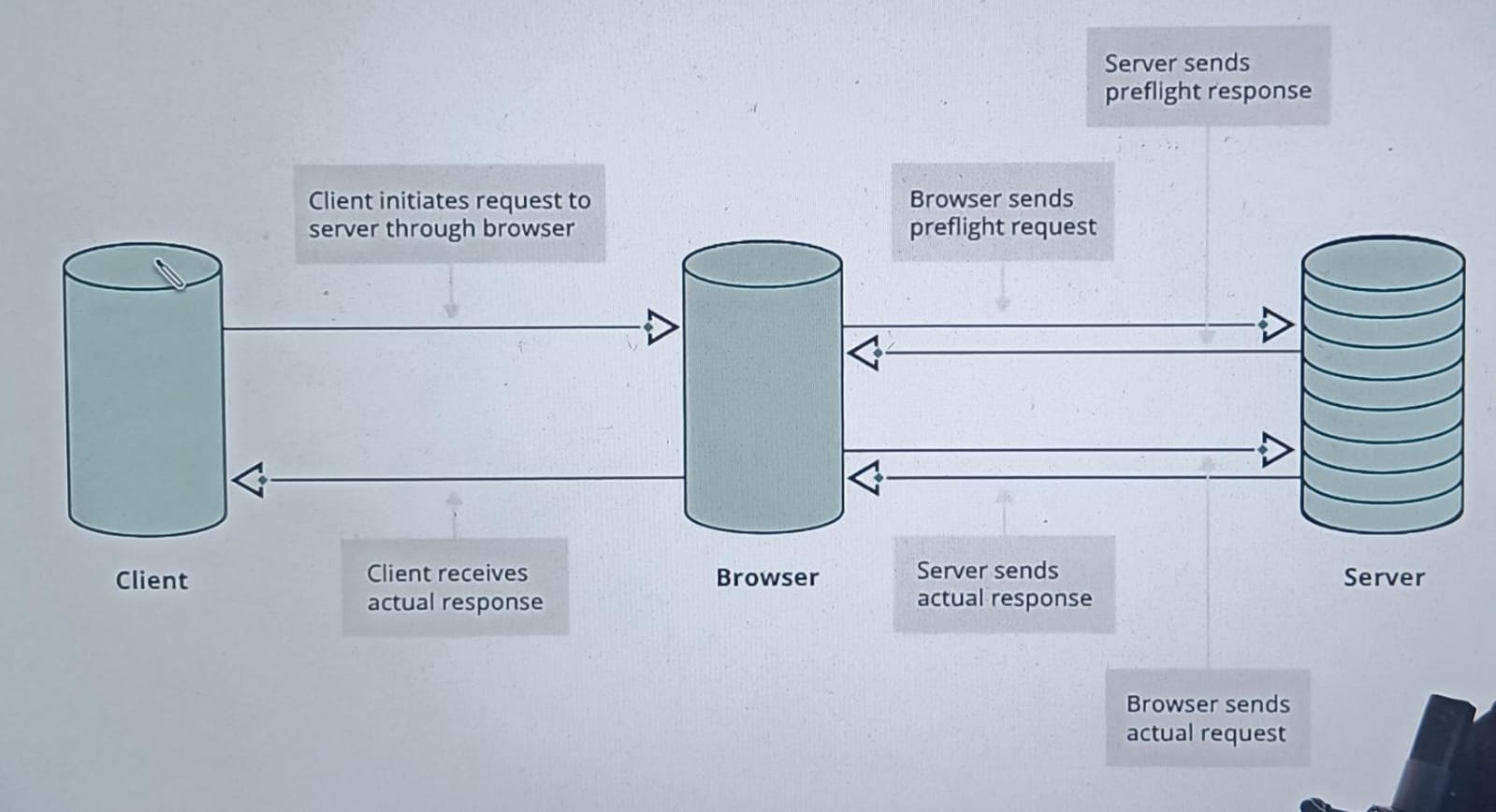
CORS –

If you wanted to access something which is cross domain then I am going to ensure that if the other domain where you are accessing is giving you a permission in order to access the resource or not.

So, consider example if you have 2 domains, you have some api.abc.com and you are a person who is using a def.com so you need to access the data , this can be any data this can be any API or other kind of data, these resources are any of these like images, js or css. Now what your browser is going to do your browser is ensure that do you have access to these resources even though these resources are public, so this def.com cannot access this api.abc.com until and unless your abc.com permits that who is going to force that law, is the browser, browser is going to enforce that cross-domain requests are has to be go through certain validation, what are those validation we will get into those details?

* SOP (Same Origin Policy) – you cannot access to the other domain until and unless basically you are on the same domain, so by default it will permit for same domain if it is another domain, it is going to do something extra.
* Cross Origin Request (different – protocol, port, subdomain) -
* CORS Header
  + Access-control-allow-origin
  + Access-control-allow-methods
  + Access-control-allow-headers
  + Access-control-allow-credentials
  + Access-control-expose-headers



You are a client which is your JavaScript code probably it can be written in react or angular it can be any code basically that you have written, now using any mechanism like fetch or axios you may be doing any of these, you requesting some thing the request first goes to the browser now browser will check ohh you are making a cross origin request which is anything different port, different protocol or different sub domain all of these basically are the cross domain request so before it go and make the respective method like get, post, put, delete whichever it trying to do first browser will go to the server with something which is called preflight request what this pre flight request is meant by?

You are making a request with a METHOD: which is called OPTIONS in this case, now once you make the request your server will check ohh may be the req is coming from the def.com and I am basically abc.com probably if that is permitted on the server, lets allow that and let it make the original request if not please terminate from then and there itself.

Now by default the request for same origin nothing to worry about, if it is cross origin, protocol, port, subdomain, domain now how does it basically ensure that, when you get the response in the response basically server set these headers using these headers it get to know ither i need to permit the next request or not these are the headers basically which are set in the response and this is how browser identify shall I send the consecutive request to the server or I should not send the request.