**DNS and DHCP**

**DNS**

Domain Name System

* Used to resolve a hostname to an IP addr

Can think of it like a phone book

* When you press a name, you don’t call the name
* The phone book resolves the name and calls the number associated with it

**How does it work?**

* When you type in ‘www.redteamnation.com into your browser, the OS will look for a local DNS server that was set up
  + In most cases it will be your router/gateway
* The OS will interact with the local DNS client to contact the DNS server at the router
  + The OS will check if it knows the IP itself first to resolve locally, if not itll contact the DNS client
  + The local resolutions are kept in the **hostfile on windows** or on **the resolve file on Linux**
* The router will also check its own local db for a resolution

The router has a recursive resolver that will handle the request from the client

* Attempts to find a local resolution
* If not, it’ll continue the process and upstream the request

The router then looks at its own DNS setting to identify the Root Server

* **Root server** handles the ‘.com’ part

It will then send the DNS request to that Root Server to resolve

The Root server then has setting for the Top-Level Domain (TLD) DNS servers

The TLD knows the name server of the domain you’re trying to reach i.e., Redteamnation.com

* The request is now forwarded to the domains DNS server to resolve the IP
* This DNS server is synced with many, many other DNS servers and many website hosts have their own DNS servers, again, these are all synced though
* The IP is resolved and the chain unfolds in reverse to get the IP back to the client
* The first router will cache the domain name and the IP for future reference for a quicker look up next time

**DHCP**

**Dynamic Host Configuration Protocol**

Provides IP addr, DNS and gateway info to a client that doesn’t have one (new on the network)

* Works based on a pool of available IPs that the DHCP server has
* Can assign static IPs that do not change
* This was needed as manually handling millions of IPs isn’t feasible

DHCP is a UDP-based protocol

Commonly on ports 67 and 68

**DORA -** The core 4 steps DHCP does to assign an IP

* Discover
* Offer
* Request
* Acknowledgement

**Discover**

* Client will send DHCP discover packet to the broadcast address 255.255.255.255
  + This address is a broadcast address
  + Packet will be sent to everyone on the network
  + Then when it reaches the switch, it’ll be upstreamed and sent out to everybody again and so on
  + This is to try and reach out to every dst IP possible
* Inside of the request, the clients IP is 0.0.0.0 as it doesn’t have an IP yet
* The client is reachable through its MAC addr
* The packet also contains a transaction ID
  + Will be used throughout the entire DORA process to communicate and trace everything
  + Keeping everything on track because MACs can be spoofed

**Offer**

* The DHCP server listening for the discover packets will respond to th client directly
* DHCP server responds with
  + Its own IP
  + A new IP for the client
  + Lease info
    - Expiry
  + Transaction ID from original request
  + DNS name and gateway the client should use

**Request**

* Client will send a request back to the DHCP server
  + Note that this is still done via the client packets sent to the broadcast addr
* Client will accept the new IP
* A new transaction ID is generated at this time

**Acknowledgement**

* DHCP server will now send the ACK back to the client that they are confirming the IP being taken and the lease info
* The client will then take the info received and configure the OS with these settings
  + New IP
  + Subnet mask
  + DNS IPs