5.5.3 DNS Facts

The Domain Name System (DNS) is a hierarchical, distributed database that maps logical hostnames to IP addresses. DNS is a distributed database because no one server holds all of the DNS information. Instead, multiple servers hold portions of the data, as follows:

- Each division of the database is held in a *zone* database file.
- Zones typically contain one or more domains, although additional servers might hold information for child domains.
- DNS servers hold zone files and process name resolution requests from client systems.

The DNS is made up of the following components:

Component	Description
. (dot) domain	The . (dot) domain, also called the *root* domain, denotes a fully qualified, unambiguous domain name.
Top-level domain (TDL)	A TDL is the last part of a domain name (e.g., .com, .edu, .gov). TDLs are managed by the Internet Corporation of Assigned Names and Numbers (ICANN).
Fully qualified domain name (FQDN)	The FQDN includes the hostname and all domain names, separated by periods. The final period (for the root domain) is often omitted and only implied.
Additional domains	Additional domains are
Host name	The host name is the part of a domain name that represents a specific host. For example, with "www" is the host name of www.example.com.
Records	*Records* are used to store entries for hostnames, IP addresses, and other information in the zone database. Each host has at least one record in the DNS database that maps the hostname to the IP address. The following are common resource records: - The A record maps an IPv4 (32-bit) DNS hostname to an IP address. This is the most common resource record type. - The AAAA record maps an IPv6 (128-bit) DNS hostname to an IP address. - The PTR record maps an IP address to a hostname (it "points" to an A record). - The MX record identifies servers that can be used to deliver email. - The CNAME record provides alternate names (or aliases) to hosts that already have a host record. Using a single A record with multiple CNAME records means that when the IP address changes, only the A record needs to be modified.
Authoritative server	An *authoritative server* is a DNS server that has a full, complete copy of all the records for a particular domain.
Dynamic DNS (DDNS)	DDNS enables clients or the DHCP server to update records in the zone database. Without dynamic updates, all A (host) and PTR (pointer) records must be configured manually. With dynamic updates, host records are created and deleted automatically whenever the DHCP server creates or releases an IP address lease. Dynamic updates occur when: - A network host's IP address is added, released, or changed. - The DHCP server changes or renews an IP address lease. - The client's DNS information is manually changed using **ipconfig /registerdns**.

When you use the hostname of a computer (for example, if you type a URL such as www.mydomain.com), recursion is employed to find the IP address. *Recursion* is the process by which a DNS server uses root name servers and other DNS servers to perform name resolution. The following steps occur:

1. The host looks in its local cache to see if it has recently resolved the hostname.
2. If the information is not in the cache, it checks the Hosts file. The Hosts file is a static text file that contains hostname-to-IP address mappings.
3. If the IP address is not found, the host contacts its preferred DNS server. If the preferred DNS server can't be contacted, the host continues contacting additional DNS servers until one responds.
4. The host sends the name information to the DNS server. The DNS server checks its cache and Hosts file. If the information is not found, the DNS server checks any zone files that it holds for the requested name.
5. If the DNS server can't find the name in its zones, it forwards the request to a root zone name server. This server returns the IP address of a DNS server that has information for the corresponding top-level domain (such as .com).
6. The first DNS server requests the information from the top-level domain server. The server returns the address of a DNS server with the information for the next highest domain. This process continues until a DNS server is contacted that holds the necessary information.
7. The DNS server places the information in its cache and returns the IP address to the client host. The client host also places the information in its cache and uses the IP address to contact the desired destination device.

The following are some additional facts about DNS:

- A *forward lookup* finds the IP address for a given hostname. A *reverse lookup* finds the hostname from a given IP address.
- Root DNS servers hold information for the root zone (.). Root servers answer name resolution requests by supplying the address of the corresponding top-level DNS server (servers authoritative for .com, .edu, and similar domains).
- On very small networks, you could configure a HOSTS file with several entries to provide limited name resolution services. However, you would have to copy the HOSTS file to each client. The work involved in this solution is only suitable for temporary testing purposes or for overriding information that might be received from a DNS server.
- On the client, you should configure a list of DNS suffixes you want to append to unqualified DNS names submitted by clients for resolution, as follows:
    - You can configure a single DNS suffix for clients using a DHCP option on the DHCP server.
    - To configure multiple suffixes, you must add them manually to the client.