5.5.3 DNS Facts

The Domain Name System (DNS) is a hierarchical distributed database that maps logical host names 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.

Parts of a DNS

The DNS is made up of the following components:

Component	Description
. (dot) domain	The . (dot) domain, or *root* domain, denotes a fully qualified, unambiguous domain name.
Top-Level Domain (TDL)	A TDL is the last part of a domain name (for example, .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 host name and all domain names separated by periods. The final period (which is for the root domain) is often omitted and only implied.
Additional Domains (Second-Level Domains)	Additional domains are second-level domains with names registered to an individual or organization for use on the internet. These names are based on an appropriate top-level domain, depending on the type of organization or geographic location where a name is used. Yahoo.com and microsoft.com are examples of additional domains in your DNS structure.
Host Name	The host name is the part of a domain name that represents a specific host. For example, "www" is the host name of www.example.com.
Records	*Records* are used to store entries for host names, IP addresses, and other information in the zone database. Each host has at least one record in the DNS database that maps the host name to the IP address. Common resource records include: ▪ The A (Host Address) record maps an IPv4 (32-bit) DNS host name to an IP address. This is the most common resource record type. ▪ The AAAA (Quad-A) record maps an IPv6 (128-bit) DNS host name to an IP address. ▪ The PTR (Pointer) record maps an IP address to a host name (by pointing to an A record). ▪ The MX (Mail Exchanger) record identifies servers that can be used to deliver email. ▪ The CNAME (Canonical Name) record provides alternate names (or aliases) to hosts that already have a host record. If you only use a single A record with multiple CNAME records, when the IP address changes, you only have to modify the A record. ▪ The NS (Name Server) resource record identifies all name servers that can perform name resolution for the zone. Typically, there is an entry for the primary server and all secondary servers for the zone (all authoritative DNS servers). ▪ The SRV (Service Locator) record identifies the resources that provide a service. This allows clients to find services, such as domain controllers, through DNS. Windows automatically creates these records as needed. ▪ The SPF (Sender Policy Framework) record identifies authorized email servers. SPF records are created using TXT records. DNS uses the SPF record to verify that the host that sent the mail is authorized to use the DNS name. ▪ DKIM (Domain Keys Identified Mail) is an email authentication method that uses a digital signature to validate email and make it easier to identify spoofed emails. The sending mail server signs the email with the private key, and the receiving mail server uses the public key in the domain's DNS information to verify the signature. One domain can have several DKIM keys publicly listed in DNS, but each matching private key is only on one mail server. DKIM records are created using TXT records.
Authoritative Server	An *authoritative server* is a DNS server that has a 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**.

Recursion Process

When you use the host name 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 host name.
2. If the information is not in the cache, it checks the Hosts file. The Hosts file is a static text file that contains host-name-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.

DNS Facts

The following are some additional facts about DNS:

- A forward lookup finds the IP address for a given host name. A *reverse lookup* finds the host name 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:
  - Configure a single DNS suffix for clients using a DHCP option on the DHCP server.
  - Configure multiple suffixes by adding them to the client manually.