Domain Name System (DNS)

DNS is a hierarchical naming system. We call it 'hierarchical' because it looks like an upside-down tree. At the top of the tree is the root, which is represented by a period. Below the root are the top-level domains, which encompass such domains as .com, .edu, .gov, and so on.

Below each top-level domain are additional domains that are typically assigned to different organizations. For example, you might have a domain from Microsoft, another for mycompany, and so on. The DNS name space is referred to as 'distributed' because this portion of the name space is delegated to different organizations. Microsoft is in charge of maintaining the name space for its organization.

www is a hostname

At the end of the hierarchy are the actual hostnames that represent specific hosts. For instance, you may have servers in your organization named server1, server2, and www.

FQDN Fully Qualified Domain Name

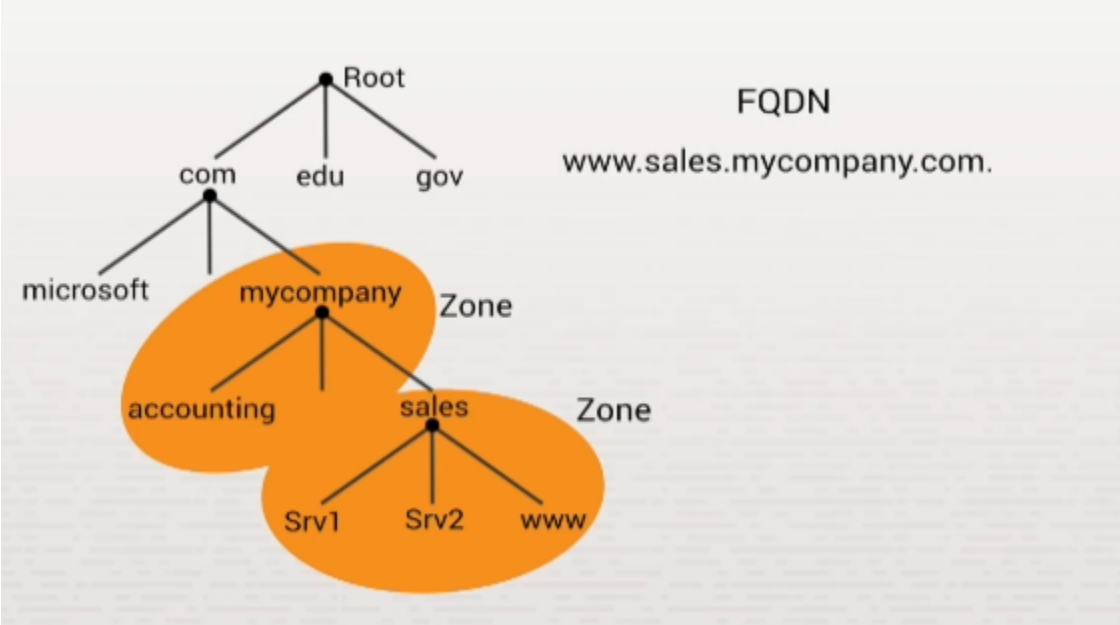
When you refer to a specific computer, you start with the hostname and then work your way back up the hierarchy to the root. This is called the fully qualified domain name, or FQDN.

For example, the fully qualified domain name of the host named www would be www.sales.mycompany.com. Notice that each domain is separated from the host and other domains with a period.

The FQDN also includes the name of the root, which is just another period. The trailing period is usually omitted, but technically, it is there. The FQDN of a host starts with the host portion of the name followed by each domain up the tree to the root.

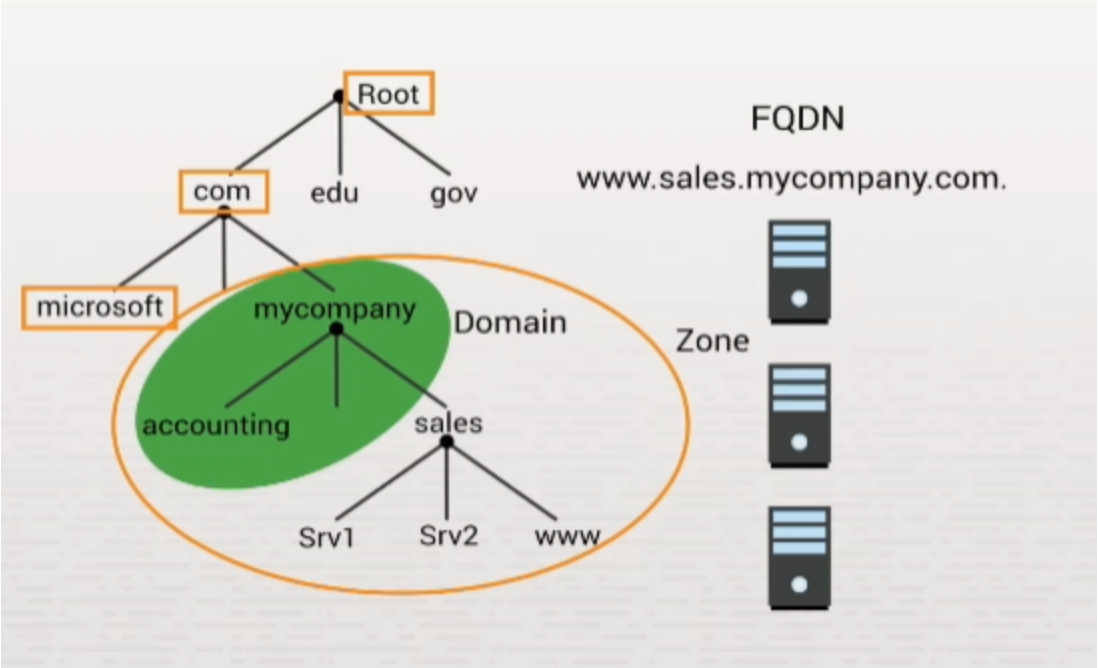
DNS Zone

Another concept you need to be familiar with is a DNS zone. A zone is an area of the name space under the administrative control of one server or that resides on a single DNS server. DNS servers maintain a part of the name space. At every level, there are servers that maintain a specific portion of the name space. In this case, mycompany may have a single DNS server, and the mycompany name space would be encompassed in a single zone. You could add another server at a later time that stores information about just the sales subdomain. In this situation, there would be a zone here and a zone that includes the rest of the name space.



At the top of the hierarchy are the root DNS servers. Root servers are servers on the internet that keep track of everything within the root domain. This includes the IP address of the servers at various levels. Within the .com domain there are servers that maintain information about subdomains within that domain. Microsoft has set up its own DNS servers to maintain information about hosts within the Microsoft domain.

The term "zone" refers to the actual database that resides on a DNS server. The term "domain" identifies a division within the DNS name space. A zone could encompass multiple domains, or it might include one domain only.



Resolution Process

First, the computer looks in its own local hosts file for an IP address mapping for www.comptia.org.

The hosts file is a text file on your computer that maps host names to IP addresses. The hosts file was originally used for name resolution in the early days of IP networking. But today, they are only minimally used because they are hard to keep updated. The hosts file still exists on all modern operating systems, and your computer will still consult it first to resolve a host name into an IP address.

If the computer can't find a mapping for the host name in the hosts file, it will submit the host name to a DNS server for resolution. This DNS server might be on your private network. It might be an external DNS server at your ISP or in the cloud somewhere, or it might be a publicly accessible DNS server on the internet.

When you configure IP networking on your computer, you usually configure it with the IP address of a DNS server that it should use for resolving host names. In this example, the computer asks the DNS server for the IP address www.comptia.org. At this point, the name resolution process can get complex.

First, the DNS server looks within all of its own zones for the requested host name. If a DNS server has a locally zone configured with name resolution information within it, it is said to be authoritative for that zone. In other words, it doesn't have to ask any other DNS server for help because it already has an IP address mapping for the host name being resolved.

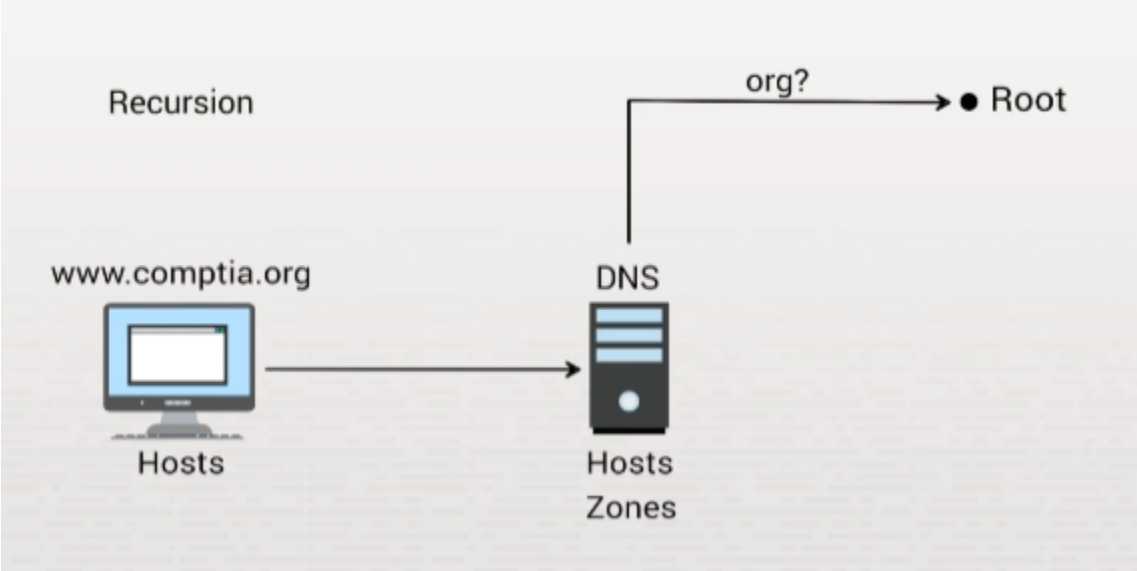
In this example, the DNS server will look for www.comptia.org within its own database. If the server finds that address, it responds directly to your computer with the appropriate IP address for that host.

If the computer doesn't find that address, then the server needs to get help from another DNS server using a process called recursion.

Recursion Process

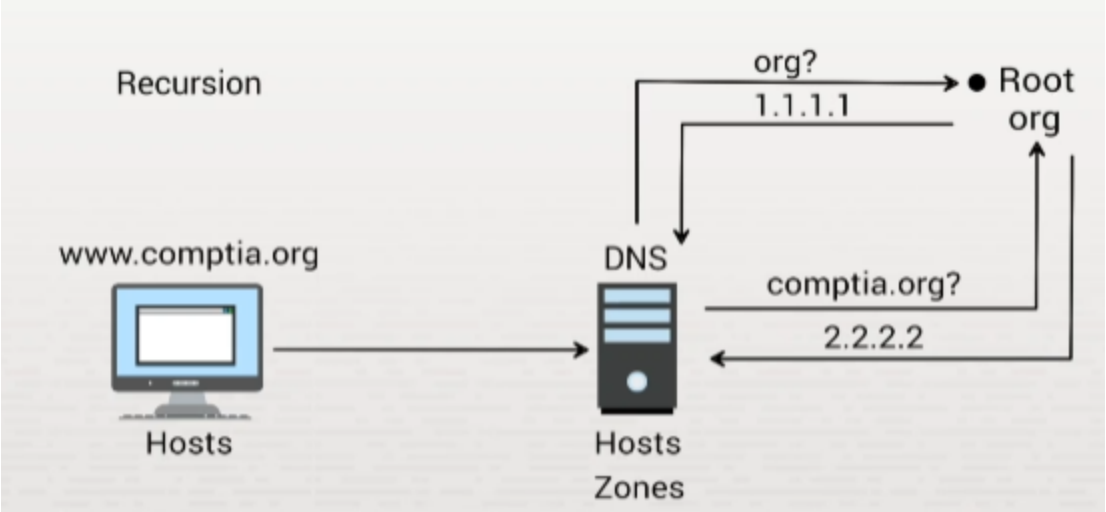
The first thing the DNS server does during the recursion process is contact a root domain server on the internet and ask that server for the IP address of a top-level domain DNS server, in this case, the .org domain.

All DNS servers are configured with the IP addresses of the root domain servers. They don't know the IP address of any other DNS servers on the internet.

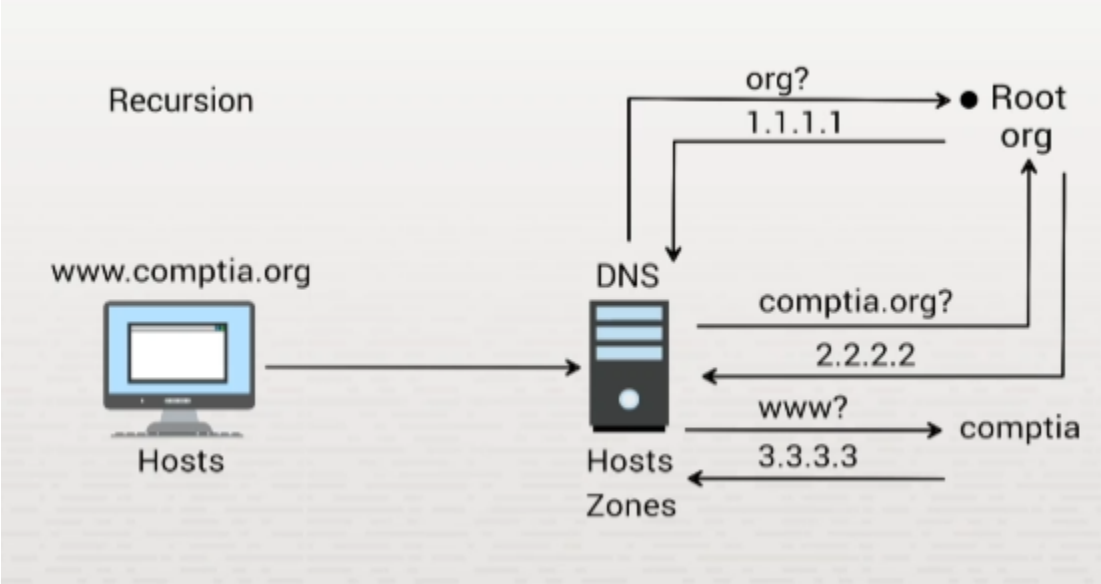


The DNS server submits this request to the root server and asks for the IP address of the .org DNS server. The root server looks in its database and returns the IP address of a DNS server that stores information for the .org domain. Let's say it's 1.1.1.1 in this case.

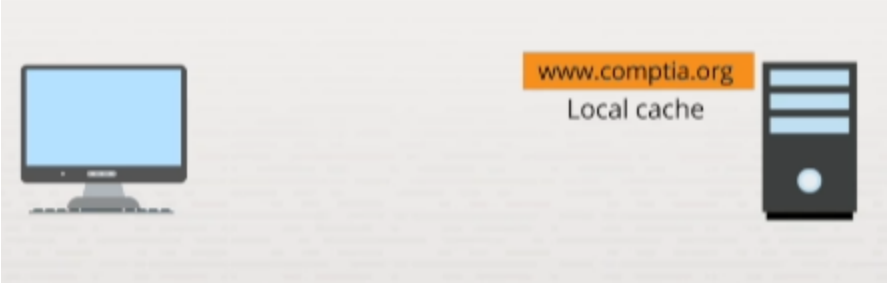
At this point, the DNS server submits another request to the .org DNS server that it was referring to, asking for the IP address of a DNS server that is authoritative for the comptia.org zone. The .org DNS server looks in its database, and it returns an IP address for a DNS server for comptia.org. Let's say it's 2.2.2.2.



Finally, the DNS server submits another request to the DNS server that is authoritative for the CompTIA zone and asks it for the IP address of the host named www. The CompTIA DNS server responds with the answer--let's say 3.3.3.3. At this point, your computer finally has the appropriate IP address and can contact the server named www at comptia.org. This is how the recursion process works.



After recursion, your DNS server keeps a copy of the mapping for www.comptia.org in its local cache. This eliminates the need to go through the whole recursion process again the next time another client asks it to resolve the same host name.



The local computer that initially made the request also puts the IP address in its own name resolution cache. The next time you open a browser and try to access the same website, the computer can look in its own local cache to get the appropriate IP address mapping without asking the DNS server to resolve it. The cache is typically only valid as long as the computer remains running. If you shut it down, the cache is flushed. The entries in the local DNS cache probably have an expiration date. If your computer is left on for several days, the entries in the cache will be gradually removed as each one expires.

DNS servers can also be configured to submit name resolution requests directly to another DNS server. This is called a caching-only DNS server.

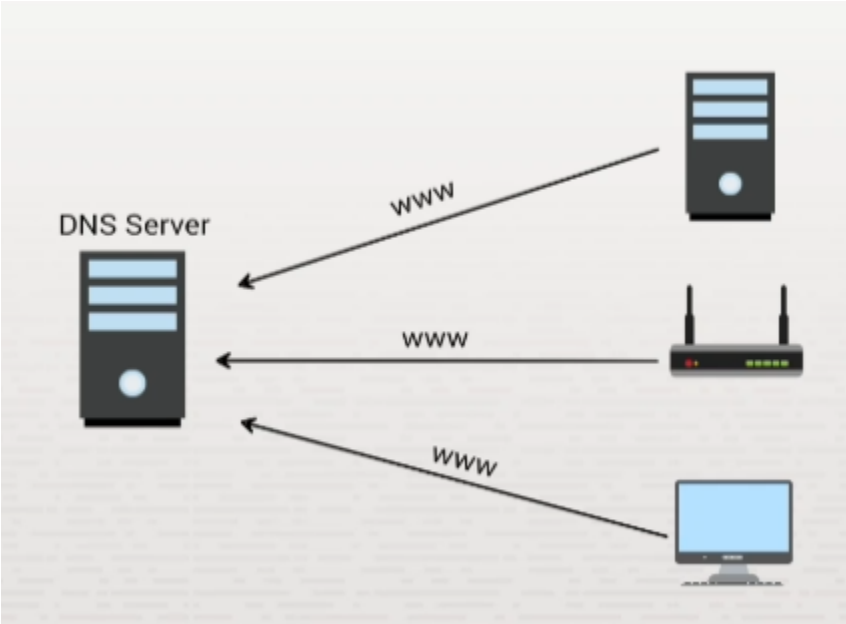
Caching-Only Name Server

A caching-only DNS server does not contain zone information or a zone database file. Instead, its job is to build up an extensive name resolution cache that can be used to resolve hostnames for a client. You might do this, for example, if you have a DNS server on your private network, but you want the DNS servers on your ISP's network to do all of the recursion work.

In this case, when your workstation submits a request to the caching-only DNS server, it forwards that request directly to another DNS server, and then this DNS server uses the

recursion process to resolve the name. The address is cached by your DNS server and then returned back to your workstation.

DNS servers can be configured with IP address mappings for internal network hosts. This allows computers to resolve internal hostnames and map them to IP addresses. Typically, DNS servers are populated with mappings for network infrastructure devices, such as servers and routers. However, mappings for workstations can also be added. Most workstations use addresses that have been dynamically assigned by a DHCP server. Manually maintaining DNS records for DHCP clients would require an inordinate amount of administrative overhead.

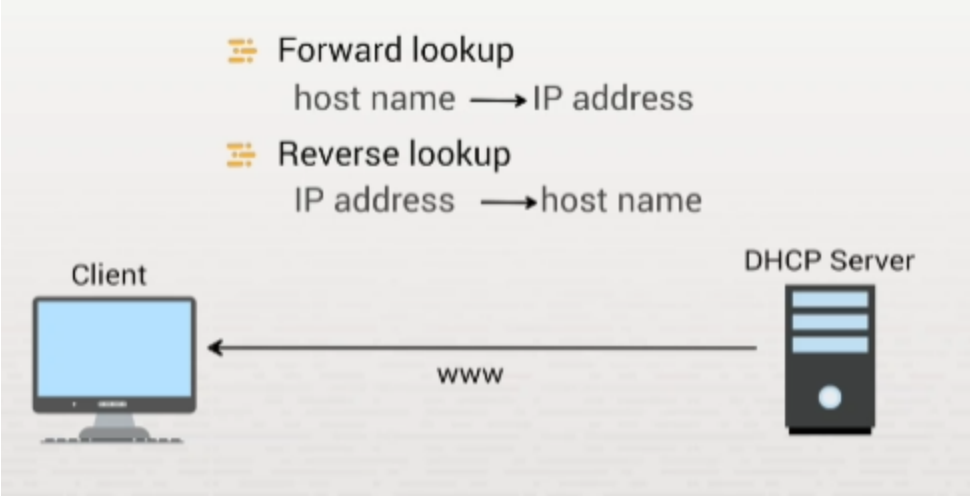


DDNS

To make things easier, most DHCP and DNS servers support a feature called Dynamic DNS, or DDNS. Using DDNS, the DHCP server sends an update to the DNS server whenever it assigns an address to a DHCP client. The DNS server then automatically creates the appropriate mapping that can be used for name resolution. When the DHCP lease is released or expires, then the mapping is automatically removed from the DNS server.

There are a couple of additional DNS-related concepts you should be familiar with:

- **Forward Lookup:** The process of resolving a hostname to an IP address is called a forward lookup. It takes a known hostname and returns an IP address.
- **Reverse Lookup:** You can also perform a reverse lookup by giving an IP address to the DNS server and asking it to return the corresponding hostname.



DNS Records

On the DNS server, IP address mappings are contained in records.

- An A record maps an IPv4 (32-bit) DNS hostname to an IP address. This is the most common resource record type.
- An AAAA record, also called a quad-A record, maps an IPv6 (128-bit) DNS hostname to an IP address.
- A PTR record maps an IP address to a hostname (in this way, it points to an A record).
- A MX record identifies servers that can be used to deliver email.
- A 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 one A record needs to be modified.
- An SRV record is used to locate a particular host that provides a particular service. SRV records are created automatically by Windows as needed.
- An NS Record identifies DNS servers or the zone; there is one NS record in the zone for each DNS server that has a copy of that zone.
- SPF and DKIM records are quick methods for improving your email delivery rates. With this addition to your DNS entries, you're telling recipients that you've authorized a third-party to send emails on your behalf.

Summary
That's it for this lesson. In this lesson, we reviewed how DNS works. First, we looked at the hierarchical DNS structure and the name resolution process. We looked at the role of the hosts file and explained the recursion process. We also discussed how a caching-only name server works. We briefly reviewed how DDNS works. Then we ended this lesson by discussing several DNS records stored by a DNS server.

DNS Facts

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

How DNS Works

DNS is a distributed database; 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.

In 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 can configure a Hosts file with several entries to provide limited name resolution services. However, you have to copy the Hosts

file to each client. The work involved in this solution is suitable only 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.

DNS Components

DNS is made up of the following components:

Component	Description
. (dot) domain	The . (dot) domain, the *root* domain, denotes a fully qualified, unambiguous domain name.
Top-Level Domain (TLD)	A TLD is the last part of a domain name (for example, .com, .edu, .gov). TLDs 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 implied.
Additional domains (Second-level domains)	Additional domains are second-level domains that have 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 Canonical Name (CNAME) record provides alternate names (aliases) to hosts that already have a host record. If you use only a single A record with multiple CNAME records, you have to modify only the A record when the IP address changes. ● The Name Server (NS) 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 Service Locator (SRV) 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 Sender Policy Framework (SPF) 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. ● Domain Keys Identified Mail (DKIM) 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 on only 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 the ipconfig /registerdns command.

Recursion Process

Recursion is the process by which a DNS server uses root name servers and other DNS servers to perform name resolution. When you use the host name of a computer, such as www.mydomain.com, recursion is employed to find the IP address. 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 Configuration Facts

Logical Hostname to IP Address Process

The following table describes the difference between a router or switch, and a workstation when resolving a logical hostname to an IP address:

Device Details Router or Switch DNS name resolution looks for information in the following places (in this order):

1. Static DNS entries
2. DNS server query (if enabled)

Workstation DNS name resolution looks for information in the following places (in this order):

1. Local DNS cache
2. HOSTS file
3. DNS server query (Primary)
4. DNS server query (Secondary)

Additional DNS servers are queried only if the primary DNS server did not respond (e.g., it is offline).

Configuration Commands

Use the following commands to configure DNS services on a router or switch:

Command	Description
router(config)#**ip host** ***[name] a.b.c.d***	Creates static DNS entries.
router(config)#**ip domain-name** ***[name]***	Configures the router default domain (for DNS).
router(config)#**ip name-server** ***a.b.c.d***	Sets the default DNS name server.
router(config)#**ip domain-lookup**	Enables the router to use DNS to identify IP addresses from hostnames.

router(config)**#no ip domain-lookup**	Disables the broadcast name resolution of hostnames.
router**#show hosts**	Displays a list of known IP hosts.