Network + Section 9 - Network Services

Network Services

- Dynamic Host Configuration Protocol (DHCP) - Assigns devices with IP addresses and also provides them a subnet mask, default gateway, and DNS server.
    - Operates over ports 67 and 68 using UDP.
- Domain Name System (DNS) - Converts domain names to IP addresses using a hierarchical and decentralized system of naming.
    - Phone book for the internet.
    - Operates over UDP and TCP using port 53.
    - When DNS is conducting a domain name query or lookup, it's going to use UDP to accept that request from a client and send a response from that server back.
    - If DNS is doing a zone transfer it will use TCP.
        - Zone Transfer - Sharing of information between DNS servers about which domain names they have and their associated IP addresses.
- Network Time Protocol (NTP) - Synchronized clocks between systems communicating over a packet-switched, variable-latency data network.
    - TCP/IP networks are packet switched networks. NTP is going to be used for the synchronization of time across our IP-connected servers using TCP.
    - Sevt over UDP using port 123.
- OBJ 1.6 Explain the use and purpose of network services.

DHCP

- Dynamic Host Configuration Protocol (DHCP) - Provides an IP address to every machine on the network and eliminates configuration errors.
    - Scope - A list of valid IP addresses available for assignment or lease to a client computer or endpoint device on a given subnet.
    - You can tell your DHCP server what IP addresses should be used in your scope and you can even reserve some of those IPs. This is known as an excluded range in your scope.
    - DHCP Reservation - Excludes some IP addresses from being handed out to devices unless they meet a certain condition.
        - Reservation can be set up based on its MAC address, once the MAC address has been recognized the DHCP server will assign the static address.
- DHCP automates the process of configuring all devices whenever they come online. When a device comes online it will reach out to the DHCP server and begin the process.
    - Discover - Device reached out to the DHCP server.
    - Offer - DHCP server will offer an IP address from the scope.
    - Request - Device request to take the IP address offered from the DHCP server.
    - Acknowledge - DHCP server will acknowledge that it will be leasing the IP address used by this client.
        - Default lease time for IP addresses at home is 24 hours.
        - In a corporate setting it may be 7 or 30 days.
    - There are 4 key pieces of information that the client is receiving once it's been assigned an IP address.

        - IP Address - The client knows where it's located on the network due to its IP address.
        - Subnet mask
        - Default gateway IP - Where the router is with the gateway address.
        - DNS server IP - How to convert the domain names to IP addresses using the DNS servers IP.
    - IP addresses can also be statically assigned.
    - Whenever you're configuring DHCP, if DHCP is not successful and it's not able to negotiate its way through the process it's going to default to its alternative configuration set by the system administrator inside the OS. By default it will be assigned an APIPA address.
    - As a system admin you can configure your device to fall back to a known good static IP address as your alternate configuration instead.
    - When configuring the DHCP server one thing that can be done is to configure the scope options. These are…
        - Subnet mask - which is going to be applied to all devices requesting that configuration.
        - Default gateway - gateway the devices should use.
        - DNS Server - to include the IP address configuration for those devices.
        - Lease time
    - Another DHCP configuration that needs to be done is…
        - DHCP Relay - Forwards DHCP packets between clients and servers.
            - DHCP relay is used when the client device and the DHCP server are not located on the same subnet or network.
            - DHCP device can be configured to pick up and Discovery requests and forward that request to the DHCP server on the other network on behalf of your client acting as a middleman.
    - DHCP operates using the User Datagram Protocol (UDP)
        - IP Helper - Forwards several different kinds of UDP broadcasts across the router and can be used in conjunction with the DHCP relay.
        - If the DHCP client and server are on different network segments, the router and the client's network segment has to be configured with an IP helper address. For DHCP to work properly and forward those requests over to the DHCP server.

DNS

- Domain Name System (DNS) - Helps network clients find a website using human-readable hostnames instead of numeric IP addresses.
- The way DNS works is…
    - The user's computer gets told to go to someplace like SyB.com and it reaches out to a DNS server and asks who is SyB.com?
    - The DNS will reply and say, "I know who SyB.com", its IP address is x.x.x.x.
    - The client then gets redirected to a web server, using their router, and their way in connection since they know the right IP address to use as their destination.
    - As home users we will usually rely on the ISP to do this process for us.
    - If you're running your own website or large organization you will most likely have your own DNS server. You will be responsible for setting up your own DNS records that dictate what servers at what IP addresses for what purposes.

        - This allows you to run your own domain name and host resolution which will convert those domain names to IP addresses.
- Fully-Qualified Domain Name (FQDN) - A domain name that is under a top-level provider.
    - Top level domain is .com but there are many others like .net, .org, .edu, .mil, etc…
    - If using the example of www.SYB.com this qualifies as a FQDN but there are other examples like ftp.SYB.com, mail.SYB.com, these all are a FQDN. All three of these are FQDNs. When entering these you are providing the service you want to reach (ftp, www, mail) a dot (.) then a domain name (SYB), a dot (.) and the top level domain (com).
- DNS is going to be set up as a hierarchy. This occurs at 5 different levels.
    - Root - Highest level in the DNS hierarchy tree. Answers request in the root zone. These servers contain the lists of all top-level domains. Example….com, .net,.org…etc.
    - Top-Level Domain - These are broken into 2 categories.
        - Organizational Hierarchies - .com, .net, .org, etc.
        - Geographical Hierarchies - .uk, .fr, .it, etc…
    - Second-Level Domain - sits below the Top-level domain and for instance would be SYB.com
    - Subdomain - If you wanted to create a server under the second-level domain of SYB.com (support.SYB.com).
    - Host - refers to a specific machine or server on the network.
- Uniform Resource Locator (URL) - Contains the FQDN with the method of accessing information.
    - www.SYB.com is the FQDN but when adding an HTTPS or HTTP it becomes a URL, https://www.SYB.com. Including one of these two protocols allows you to gain access to the website either securely or not secure. If gaining access using FTP it would look like this ftp://ftp..SYB.com.

DNS Record	Description	Function
A	**Address**	**Links a hostname to an IPv4 address**
AAAA	**Address**	**Links a hostname to an IPv6 address**
CNAME	**Canonical Name**	**Points a domain to another domain or subdomain**
MX	**Mail Exchange**	**Directs emails to a mail server**
SOA	**Start of Authority**	**Stores important information about a domain or zone**
PTR	**Pointer**	**Correlates an IP address with a domain name**
TXT	**Text**	**Adds text into the DNS**
SRV	**Service**	**Specifies a host and port for a specific service.**
NS	**NameServer**	**Indicates which DNS nameserver has the athority**

- CNAME records can only be used to point to another domain or subdomain, not to an IP address.
- MX has priority numbers that can be set to prioritize different email servers. For example if I have mail1.syb.com and it has a value of 10 and I have another one mail2.syb.com with a value of 20 it will try to send it to mail1.syb.com, the lower the priority value the more important. If priority values are the same to balance the load then the values must be set to the same value, 10/10, all incoming emails are going to alternate between each server.
- SOA can contain information like when the domain was last updated, the email address of the administrator of the domain, or how long a server should wait prior to sending an update for all of its DNS records to other zones. This is critical when a DNS server is attempting to conduct a zone transfer.
    - Zone Transfers - Sends DNS records data from the primary nameserver to a secondary nameserver.
        - Zone transfer uses the TCP protocol to transfer data.
- Pointer records are used to conduct a reverse DNS lookup.
    - Reverse DNS Lookup - Determines what the domain name is for a given IP address.
        - This can be useful when you are trying to prove your domain name is not associated with SPAM or troubleshooting an email delivery issue, or trying to create a better logging environment by converting your IP addresses back into domain names.
    - When storing an IP address in a pointer record, it'll be reversed .in-addr.arpa will be added at the end. For example if your IP address is 33.44.55.66.in-addr.arpa will be added at the end of the IP.
        - Advanced Research Projects Agency Network (ARPAnet) - First top-level domain that was defined for what would become the internet.
            - Used for managing network infrastructure.
    - When you conduct this type of lookup, you're trying to determine the host name based on a given IP. This process is known as a reverse dns lookup.
        - Reverse DNS Lookup - Determines the hostname based on the given IP.
        - Forward Lookup - Uses DNS to find the IP address for a given domain name.
- Text records were used to add human readable notes into DNS records over time, over time machine readable text was also added to these records as well, and that's what is mostly seen these days. You're not limited to one text record.
    - On the example provided on Dions training course, he has a text record called fdkey.support, and a text string of 32 hexadecimal digits inside the DNS records. This allows their support system "Freshdesk" to verify he owns the domain name, diontraining.com, so they are authorized to send out emails on their behalf to students when his team replies inside their system to a support ticket. This is domain ownership verification.
- Service record is used to specify a host and a port for a specific service such as a voiceover IP, instant messaging, etc… when using a service record you can specify a port along with your IP address.
    - Example. If Dion wanted to use an xmpp chat server and link it to port 5223, he could do this with a service record like this.
        - _xmpp._tcp.diontraninig.com. 86400 IN SRV 10 5 5223 chat.diontraining.com
    - This is a single SRV record in a DNS server.
    - This would say that he is using the XMPP service with the TCP protocol. The time to live will be updated every 84600 seconds which is 24 hours, the class is set to IN which

stands for internet, and it's an SRV or service record. The priority is 10 and wait is 5, these two settings are used for prioritization and load balancing across multiple servers. Finally the port number is set which is 5223 and the target server which is chat.diontraining.com.

- Nameserver - Type of DNS server that stores all the DNS records for a given domain.
    - Type of record used to indicate which DNS nameserver in the world is going to be the authoritative one for that domain. This is important because DNS uses a hierarchical model, the servers need to know who owns that server to make changes to it.
    - Namaserver is a type of DNS server that stores all the DNS records for a given domain, including all the types on the list. There can be a primary nameserver or a backup nameserver, you can also use a cloud service provider the cloudflare.
- DNS can be used internally or externally.
    - Internal DNS - Allows cloud instances on the same network access each other using internal DNS names.
        - To do this internal A records are created, and internal Pointer records are also created in the reverse zone.
        - Cloud providers will create and remove these DNS clouds when you spin up virtual machines in your private cloud.
    - External DNS - Records created around the domain names from a central authority and used on the public Internet.
        - For each DNS record there is a TTL Time to Live.
            - Time to Live (TTL) - Tells the DNS resolver how long to cache a query before requesting a new one.
        - DNS Resolver/ DNS Cache - Makes a local copy of every DNS entry it resolves as you connect to websites. This speeds up the process of gaining access to sites.
        - Recursive Lookup - DNS server communicates with several other DNS servers to hunt down the IP address and return to the client.
            - With a recursive lookup a DNS resolver is saying, "I don't know what this domain's IP is, but I'm going to ask my DNS server and that server will hunt it down until it finds it and then tell me that IP".
        - Iterative Lookup - Each DNS server responds directly to the client with an address for another DNS server that may have the correct IP address.
            - Your DNS resolver is going to ask the DNS server what the IP for the domain is. If the DNS server doesn't know it's going to tell your resolver to ask the next DNS server, and that server will provide its IP. This process continues until it finds that IP for that domain.
- What do you need to know for the exam…
    - Need to know how dns works. By using its various record types to convert domain names to IP addresses and vice versa. The chart and all the information pertaining to the table.

NTP

- Network Time Protocol (NTP) - Synchronized clocks between systems communicating over a packet-switched, variable-latency data network.
    - NTP is going to be used to synchronize the time across all of our IP-connected servers.
    - Sent over UDP using port 123. The current version of NTP is version 4.

    - NTP is used to synchronize all the clocks of all participating computers to within a few milliseconds of UTC (Coordinated Universal Time).
    - You can use an internal NTP server that is accurate within a few milliseconds or you can use an external NTP server that is publicly available but the accuracy of this is within tens of milliseconds.
    - NTP is important because a lot of the security protocols rely on reliable time for things to work properly.
    - If things between your server and the client are off for 5 minutes you may get a logging error that prevents you from logging into the domain.
- There are three components of NTP
    - Stratum
    - Clients
    - Servers
- NTP is designed to use a hierarchical semi-layered system of time sources. Each layer of this system is known as a stratum.
    - Stratum 0 - is the most precise timekeeping devices we have access to. (Atomic Clock, GPS). These are known as reference clocks. NTP servers cannot be considered Stratum 0 clocks and only used as reference clocks.
    - Stratum 1 - First Stratum 1 servers will use stratum 1. Any computer in which its time source is synchronized to within a few microseconds. These are known as primary time servers.
    - Stratum 2 - These servers are connected to a synchronized stratum 1 server.
    - Stratum 3 is connected with a synchronized stratum 2 and so on and so on. Each time, we add a little bit more of delay and things become a bit further from Stratum 0.
- NTP can handle a maximum of 15 stratum levels. If something is classified as a 16 Stratum device that means that it is unsynchronized.