Section 10: Network Naming

71. Understanding DNS

Domain Name system (DNS) - Resolves IP address from Fully Qualified Domain Names (FQDN)

Host name - "www"
Top Level Domain - ".com"
Secondary Domain - the middle - www."TotalSeminars".com

DNS Settings are on your computer.

Root DNS Servers - these reach to the Top level domain, and then the top level domain finds the IP that you are looking for.

In our computers and DNS servers is a cache of IP addres information for a time to enable faster resolution

Try google DNS server 8.8.8.8

DNS resolves FQDNs to IP addresses

www.totalsem.com is an example of an FQDN

.com and .edu are examples of top-level domains (TLDs)

Applying DNS

```
External DNS Server - Registered on the internet
```

The internet runs on two primary DNS softwares:

```
1. Bind (Unix/Linux)
2. Microsoft windows server
```

To Set up a DNS server

```
1. Create a Domain
	Interior Domain - classroom.local (Can talk to the internet, but also is the **"Authoritative DNS Server"** for the local Domain)
2. Add a number of records to "look up Zones"
	Primary look up zones - "Forward Look-Up Zones"

SOA - Start of Authority - The primary DNS server for the zone "classroom.local". "The Big Cheese"
NS - Name Servers - Every Name server that is part of classroom.local
```

Hosts:

Records to put into a forward lookup zone:

The A record (IPV4) "Student 1"
Quadruple Record (IPV6)

Canonical Name - (Alias/CNAME) - use this for any host or record. Ex. "fred" -> fred.classroomlocal.com

MX Record - Mail Server - Special host record call the "MX Record"

Its easy to spoof mail so what we do is create a **"Reverse Look-Up Zone"** - Uses IP to get Domain name, **Does not** use a Domain name to get an IP.

PTR - Pointer Record

A reverse look up zone will resolve an IP address to a Fully Qualifed Domain Name
A Forward Look up zone will resolve a Fully Qualified Domain Name to an IP address

SRV Record - Server Record/Server location - Pretty rare, specific services require them
TXT Record - Two types

1. DKIM - A key/certificate, allow you to be able to autenticate an individual person trying to use the email as a legitimate user
2. SPF - "tells the record to accept any from a designated IP address"

Quick Review:

*Be comfortable (definitionally) with each record type and what they are used for
*Get on NameCheap.com to play with DNS

CNAM record creation makes an alias, or "Known name" oftern created for user interfacing

A reverse lookup zone will resolve an IP address to an FQDN, and are used by mail servers

TXT records, DKMI, and SPF are used to identify e-mail users and reduce spam

#

73. The Hosts File

Host file was used in the early day of the internet before DNS. It was a TXT file which contained IP addresses and their names

DNS replaced the host file, but it still exists and it's any computer that runs TCP/IP. It will take precedence over the DNS.

*The host file contains IP addresses and their corresponding names

*Every computer that runs TCP/IP has a host file

*The hosts file takes precedence over DNS

---

74. Net Command

Windows command line:

net
net view - shows systems on your work group
net user - shows who you are in the network
net view \nameofcomputer - shows us the shares on that particular system
net use - maps a drive (assigns a drive letter to a folder) -> net use w: \win10desktop\shareme
w: - Shows us the drive
net share - shares a resource on the network by using a pathway
net accounts - shows what type of settings we have for all of our accounts
net start - shows all different service that are network based that are running on the system

*The net command is a very old command that helps manage a network

*The net commands has many different options to manage a network (net use, net share, etc)

*The net view command shows everything that is on the network

---

75. Windows Name Resolution

NetBIOS - if you are not on a domain this is traditionally used for name resolution. Ports 137, 138, 139

LLMNR (Link Local Multicast Name Resolution) runs on UDP Port 5355 - Name resolving system better than NetBIOS

nbtstat - a tool used to understand whats going on in your windows network (Works great with NetBIOS, but doesnt play well with LLMNR)

Every windows system has their own Registered name

Lot of Commands for nbtstat:

nbtstat
nbtstat -n - tells you the systems register information (name)
nbtstat -c - tells us other names on the system, this is a cache of other names
nbtstat -a computername - shows us the registered information (name for another computer)

nbtstat -r - shows whats been going on lately but nbtstat has not been update so it appears weird

nbtstat -R - clears your cache
nbtstat -RR - Take all your registered information and rebroadcast

nbtstat is a NetBIOS tool

*NetBios is an old protocol that manages the connections based on the names of the computers within a LAN

*Link Local Multicast Name Resolution (LLMNR) is a protocol tha allows hosts to name resolution for hosts on the same local link

*nbtstat is a diagnostic command that can be useful, but has soem issues with LLMNR

---

76. Dynamic DNS

DDNS (Dynamic DNS) - you have some kind of client that runs behind the NAT part of a router and it will talk to a DNS service on the internet and they will grab a WAN IP and the WAN IP will be placed on to a Domain name you choose.

DDNS company in example is TZO - www.tzo.com

*Dynamic DNS enables you to use a DHCP-assigned IP address for connection
*DDNS providers can update IP information

---

77. DNS Troubleshooting

1. Clue you have a DNS problem is that you can't use DNS, web browers will often tell you the problem
   *Verify DNS is a problem by using the IP address of a known website and try to access it. If you can access an IP address by typing it in you have a DNS problem
2. Check for misconfiguration - it is standard for you to have two DNS settings (A Perferred and and Alternate)
3. Your DNS saves a cache of saved locations. Sometimes those locations change so we have to clear the cache

*You can put in replacement DNS servers (Ex. 8.8.8.8 <- google DNS)

*Determine if your DNS server good? Two tools to use

1. nslookup - Run nslookup to see default DNS server information (syntax -> nslookup -> server 8.8.8.8) (good for windows)

2. DIG (Domain Information Groper) - check DNS server information (good for unix)

Both nslookup and DIG are very powerful tools (huge security problem) so a lot of DNS servers dont allow queries however you can look to see if something is a DNS server up and running or is it a DNS

3. Ping is a good tool to use. (Ping resolves FQDN with IP)

**Exam really hits on output. Know what an nslookup output looks like. It will be on the exam.

*Use an IP address of a Website to test connectivity without DNS
*Run ipconfig /flushdns to clear the DNS resolver cache
*Run nslookup or dig to check the status of a DNS server

QUIZ

1. In what folder is the HOSTS file located in a Windows computer?
   a. C:\etc
   **b. C:\Windows\Systems32\Drivers\etc••
   c. C:\Windows\etc
   d. C:\Windows\System32\etc
2. What command will assigne a drive letter to a network share?
   a. Net assign
   b. Net drive
   c. Net share
   d. Net Use
3. The primary command-line tool to troubleshoot Windows naming issues is what?
   a. nbtstat
   b. netstat
   c. ipconfig
   d. net
4. What is the job of DDNS?
   a. DDNS allows a local device to randomly change its DNS name
   b. DDNS rotates the IP address of a local device
   c. DDNS tracks IP address changes of a local device and updates DNS to reflect those changes
   d. DDNS prevents the IP address of a local device from being changed
5. A website just changed its IP address and a user is unable to reach it by typing the site's domain name into their browser. What command can the user run to make the computer learn the website's new IP address?
   a. ipconfig/updatednscache

b. ipconfig /flushdns

c. ipconfig /all

d. ipconfig /dnsupdate