**MCSE 1 Lecture 6**

**DNS**

**Domain Name Service (DNS) vs NetBIOS**

NetBIOS can be used to resolve local computer names into IP addresses but, it is not capable of resolving names for hosts belonging to other organizations.

For instance, you can use NetBIOS to communicate between the computers you have at home. If you want to resolve the name of a web site or any other domain name in the Internet, your computer must use DNS.

In figure 1, each of the four organizations can use NetBIOS to resolve names within their respective networks, but when they need to resolve names belonging to one of the other organizations, they must use DNS.

If an organization has its own DNS servers, it can use DNS in place of NetBIOS or in conjunction with NetBIOS to resolve local names as well as remote names in the Internet.

DNS

DNS

Internet

Google.ca

(NetBIOS)

rrc.ca

(NetBIOS)

DNS

DNS

EBay.com

(NetBIOS)

Microsoft.com

(NetBIOS)

Fig. 1 NetBIOS is used locally, DNS is used globally

**ICANN** controls the root level and 1st level DNS servers on the Internet. The Root hint hierarchical DNS structure replaced the dependency upon the **hosts** file in 1984. (The hosts file allows you to statically configure DNS names the same way the lmhosts file allows you to statically configure NetBIOS names).

If you want the world to find your WEB site, you must register your Domain Name with ICANN. ICANN will then add your domain name and IP address to one of its top-level DNS servers. The following explanation illustrates how DNS works on the Internet.

**.**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| edu | com | net | mil | org | **ca** | us | uk | ch | au | fr | gr |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| bc | al | sk | **mb** | on | qu |

1 2 3

**DNS Server**

**at UofM**

**client DNS 4**

**Server U of M’s at RRC Network**

**RRC’s network WWW**

**5 Server**

1 = return IP for .CA, 2 = return IP for .MB, 3 = return IP for DNS server at UofM

4 = return IP for WWW server 5 = client contacts WWW server directly

Fig. 2 How DNS is used to resolve global names in the Internet

Suppose you are sitting at a workstation in Red River College. You want to browse to the Web server at the University of Manitoba; [www.uofm.mb.ca](http://www.uofm.mb.ca)**.**

The client computer sends a DNS request for the IP address of the web server at the University of Manitoba, to the local DNS server at RRC.

The DNS server at RRC does not know what the IP address of [www.uofm.mb.ca](http://www.uofm.mb.ca) so it requests the aid of the root DNS servers in the Internet.

The root DNS server, “**.**”, has the IP address of the “**.ca**” DNS server. This address is returned to the DNS server at RRC.

The DNS server at RRC now contacts the “**.ca**” DNS server with its request. The “**.ca**” DNS server has the IP address of the “**.mb**” DNS server. The IP address of the “**.mb**” DNS server is sent back to the RRC DNS server.

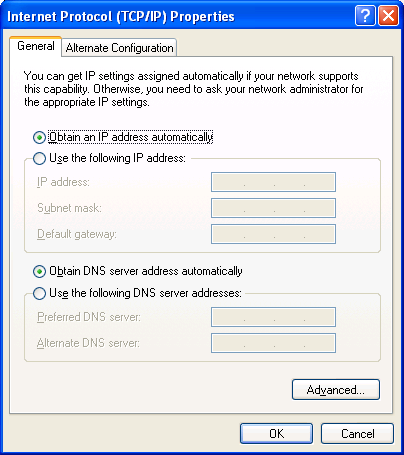
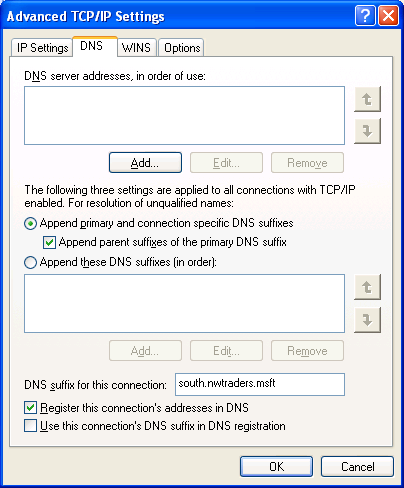
The DNS server at RRC now contacts the “**.mb**” DNS server with its request. The “**.mb**” DNS server has the IP address of the “**.uofm**” DNS server. The IP address of the “**.uofm**” DNS server is sent back to the RRC DNS server.

The DNS server at RRC now contacts the “**.uofm**” DNS server with its request. The “**.uofm**” DNS server has the IP address of the WEB server at the uofm. The IP address of the WEB server is sent back to the RRC DNS server.

The DNS server at RRC passes the IP address of the WEB server [www.uofm.mb.ca](http://www.uofm.mb.ca) to the client you are sitting at. The client now contacts [www.uofm.mb.ca](http://www.uofm.mb.ca) directly.

**Preferred & Alternate DNS Servers**

You can configure the client with a preferred DNS server and multiple alternate DNS servers. This can be done manually on the screen shown in figure 3 or the DHCP server can pass these IPs as DHCP options, to the clients.



**Configure more Alternate DNS servers**

Fig. 3 Configuring the Preferred and Alternate DNS servers on the client

The client will try the preferred DNS server. If it does not respond or if it cannot resolve the query, the client will try the alternate. If the alternate DNS server does not respond or cannot resolve the query, the next alternate DNS server is tried until no more DNS servers are left to try. Configuring multiple DNS servers provides redundancy, load balancing, and helps to keep traffic local.

If a DNS server does not respond the client will temporarily remove it from the list of DNS servers to query. By doing this, the client will not waste time trying a DNS server that has failed or is unreachable.

**How Local DNS Caching Works**

The client that issues DNS queries, caches all the resolved translations for a period specified as the Time-To-Live, TTL. The TTL is set on the **authoritative** DNS server. It passes the TTL to our DNS server which passes the TTL to the client that requested the translation. By default, for Microsoft DNS servers, the TTL = 60 minutes or 1 hour.

The TTL can be changed in the Start of Authority, (SOA) DNS record on the authoritative DNS server. A long TTL means the client will not bother the authoritative DNS server that often. A short TTL means the client’s cache will not fill up too quickly but may have to repeatedly ask the authoritative DNS server for a name resolution.

**Hosts file**

**Resolving a host name**

**client**

**DNS DNS NetBIOS**

**cache server**

Fig. 4 How a host resolves a name using

The **client resolver cache** contains the entries found in the **hosts** file and any fully qualified domain names resolved through DNS resolution.

When an application wants to reference a host by its domain name the client first checks its cache to see if the name has already been resolved.

If cache does not contain the mapping, the client contacts the DNS server to request the resolution of the domain name.

If DNS cannot resolve the domain name it passes the hostname to NetBIOS in the hopes that NetBIOS will be able to resolve it.

If NetBIOS fails, the domain name comes back as not resolvable.

**Negative cache entries**

If a name cannot be resolved by the authoritative DNS, an entry is still kept in cache. This is called a “**negative cache entry**”. These entries are kept for 5 minutes, by default.

Resolved entries in the client’s DNS cache are cleared after their ‘time-to-live’ expires.

The TTL value is supplied by the DNS server that resolved the hostname

For instance, if the DNS server at **uofm.mb.ca** resolves the web site [**www.uofm.mb.ca**](http://www.uofm.mb.ca)**, t**he record that is sent back as a response to the DNS query will contain the TTL as configured on the DNS server for **uofm.mb.ca**.

Resolved entries stay in cache for the TTL time regardless of whether you repeatedly access the same site or not. This helps to reduce the amount of network traffic generated by DNS.

You can view the DNS cache on the client by typing **ipconfig /displaydns**.

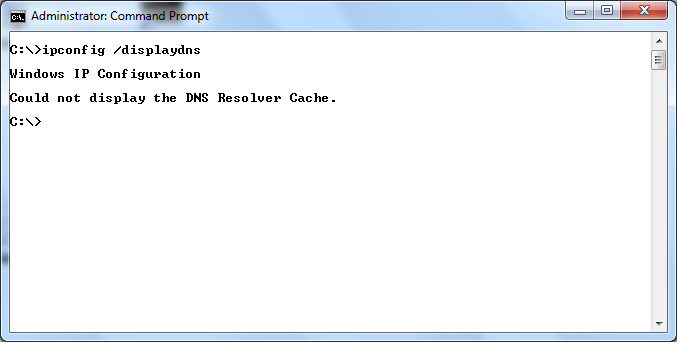


Fig. 5 Displaying the DNS cache on the client machine

In figure 5, there are no entries stored in the DNS cache. Figure 6 shows the DNS cache after we ping Calgary.blacktone.com. You can see there is now an entry in the DNS cache.

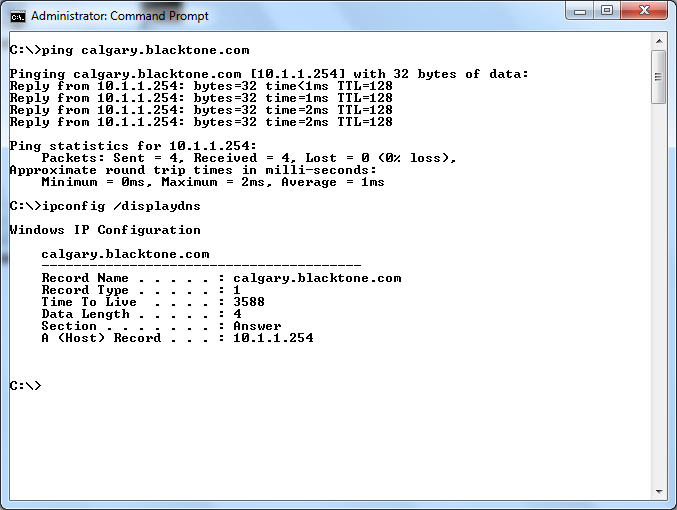


Fig. 6 An entry for Calgary.blacktone.com now shows up in the DNS cache

Notice in figure 6, the Time to Live is 3588 seconds. The actual time to live is 3600 seconds or 1 hour. Each time you display the cache, you will see the TTL has decremented a few more seconds. When the TTL reaches zero, the record is removed from the DNS cache.

You can use **ipconfig /flushdns** to clear the DNS cache. This command only exists in Windows 2000 and later operating systems. See figure 7.

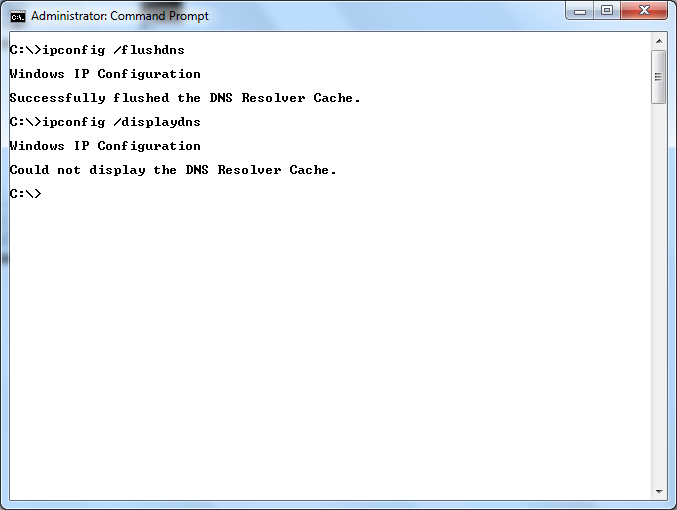


Fig. 7 **ipconfig /flushdns** clears all the learned entries from DNS cache

**Hosts file**

The **hosts** file is a text file that you can edit to add frequently required mappings of host names so bandwidth and CPU cycles are not wasted by trying to contact a DNS server to resolve the name.

Figure 8 shows the contents of the hosts file. The host file consists of an IP address followed by a fully qualified domain name.

The entries added to the hosts file are immediately added to the DNS cache as soon as you save the file.

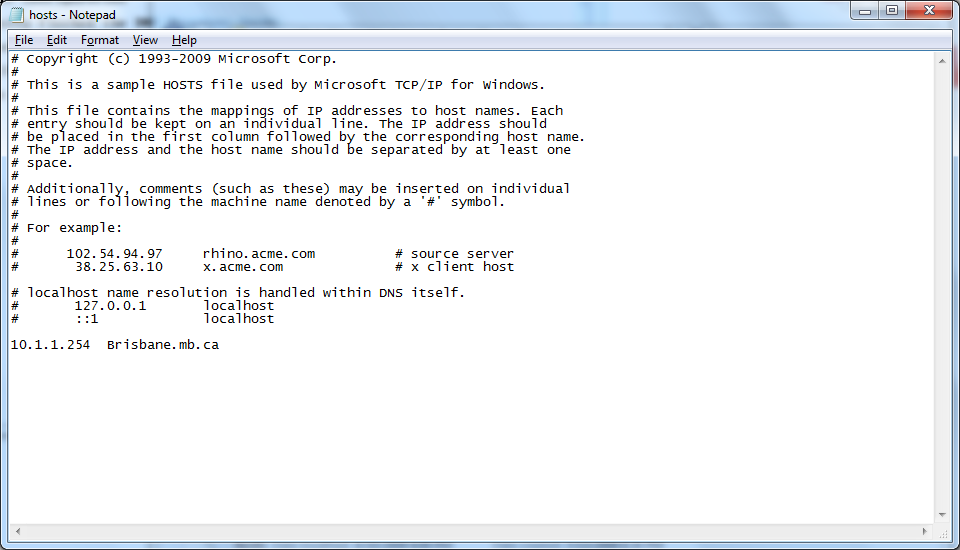
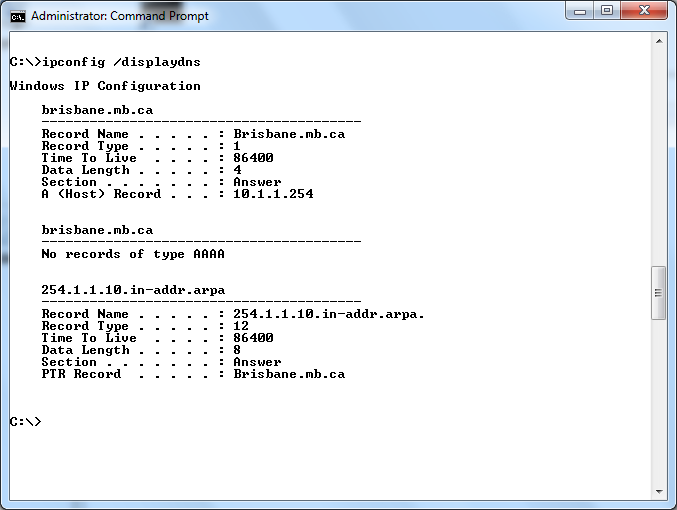


Fig. 8 The **hosts** file showing that a record for Brisbane has been added



**“AAAA” record applies to IPv6. Since IPv6 is turned off, there is no “AAAA” DNS record.**

Fig. 9 The record for Brisbane.mb.ca is immediately added to the DNS cache

Mappings appearing in the DNS cache as a result of an entry in the hosts file remain in the DNS cache until you remove the entry from the hosts file. The TTL of 86400 never decreases in value. If you repeatedly display the cache you will see it always says 86400. Clearing the cache with ipconfig /flushdns will not remove these entries.

The hosts file is found in the **%systemroot%\system32\drivers\etc** directory.

The hosts file allows you to statically configure DNS mappings in much the same way the lmhosts file allowed you to statically configure NetBIOS names.

**DNS and host names**

DNS works with fully qualified domain names, such as **www.rrc.ca**. The server or host name is **www**. The rest of the FQDN, **rrc.ca** is called the **DNS suffix**.

If we joined Ottawa to the same domain as Calgary, Ottawa’s FQDN would become **Ottawa.Blacktone.com**. If Ottawa pinged Halifax, the operating system would tack on the DNS suffix of Ottawa. The ping would be converted into **ping Halifax.Blacktone.com**.

DNS cannot work with only a host name so it tacks on the DNS suffix of the source computer with the understanding that the target computer is probably in the same domain.