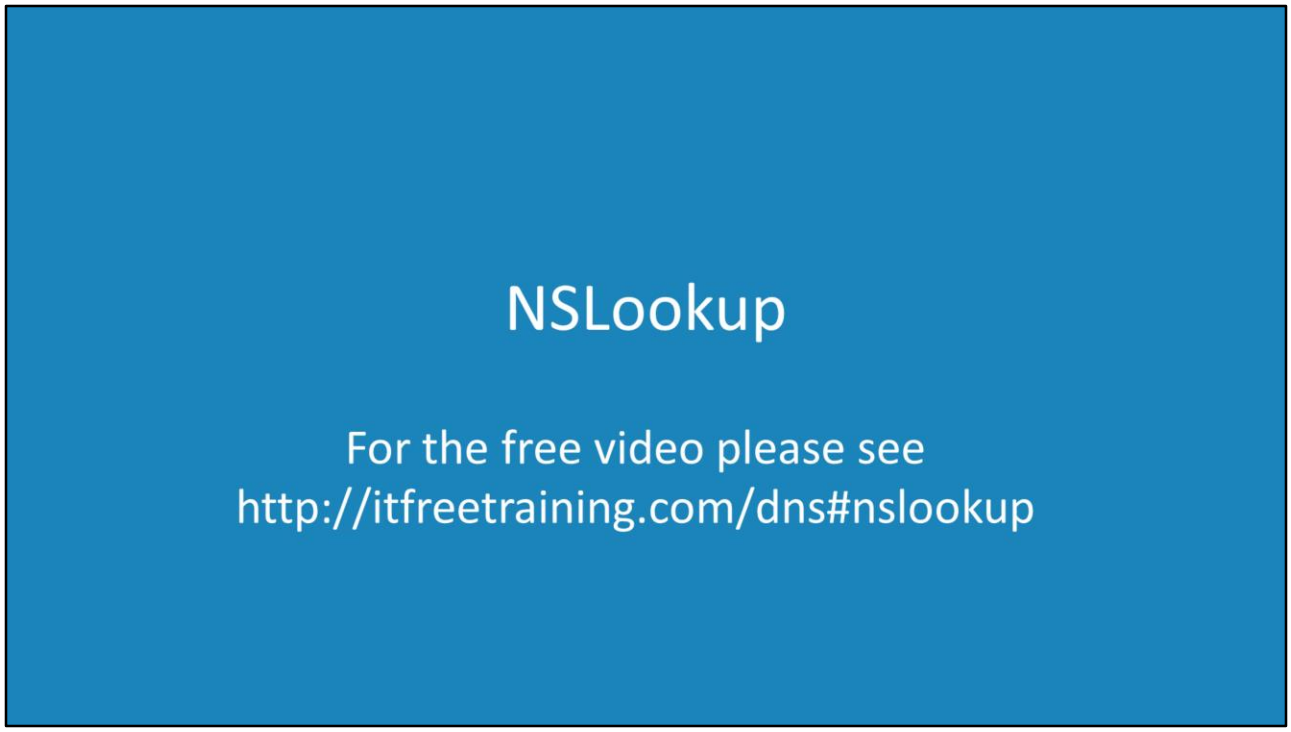
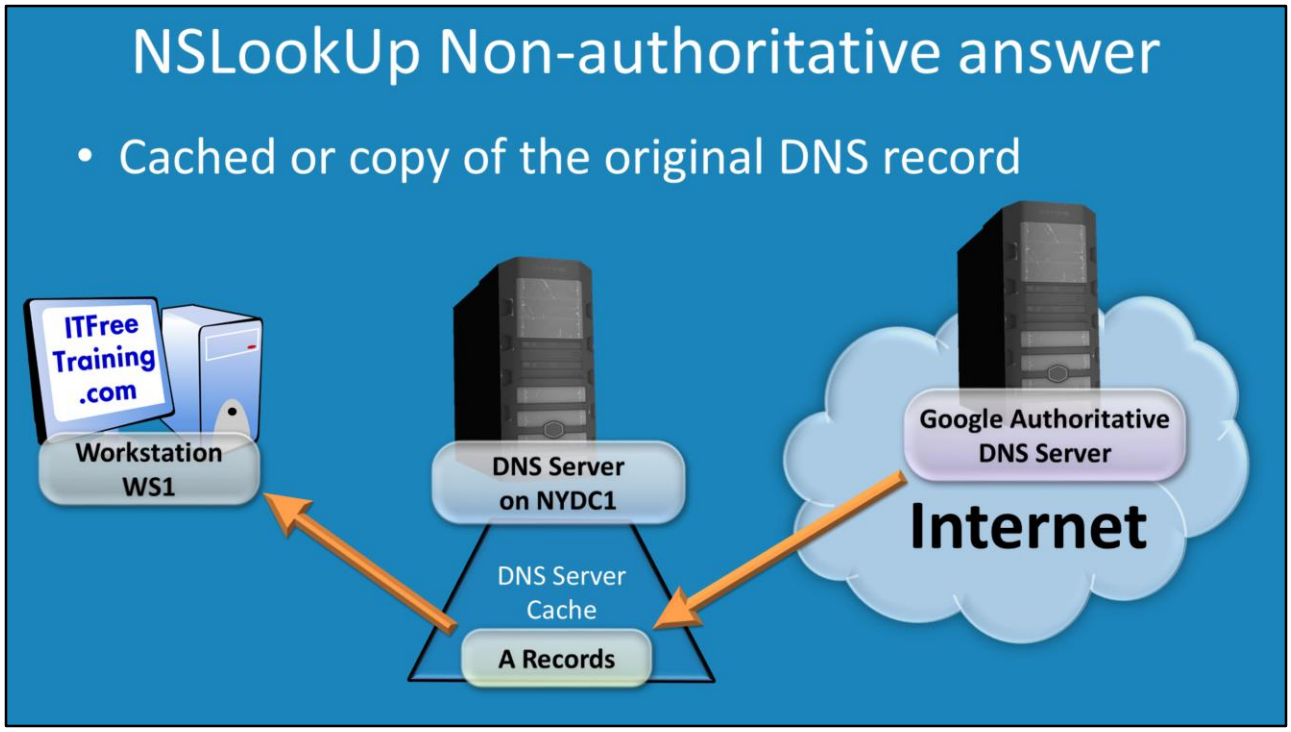


The NSLookup tool is a great tool for troubleshooting DNS problems. This video looks at how to use NSLookup in Windows, however it also available in Linux. NSLookup allows you to control which DNS servers you contact and which DNS records are resolved giving you a real world picture of what is happening with DNS on your network.

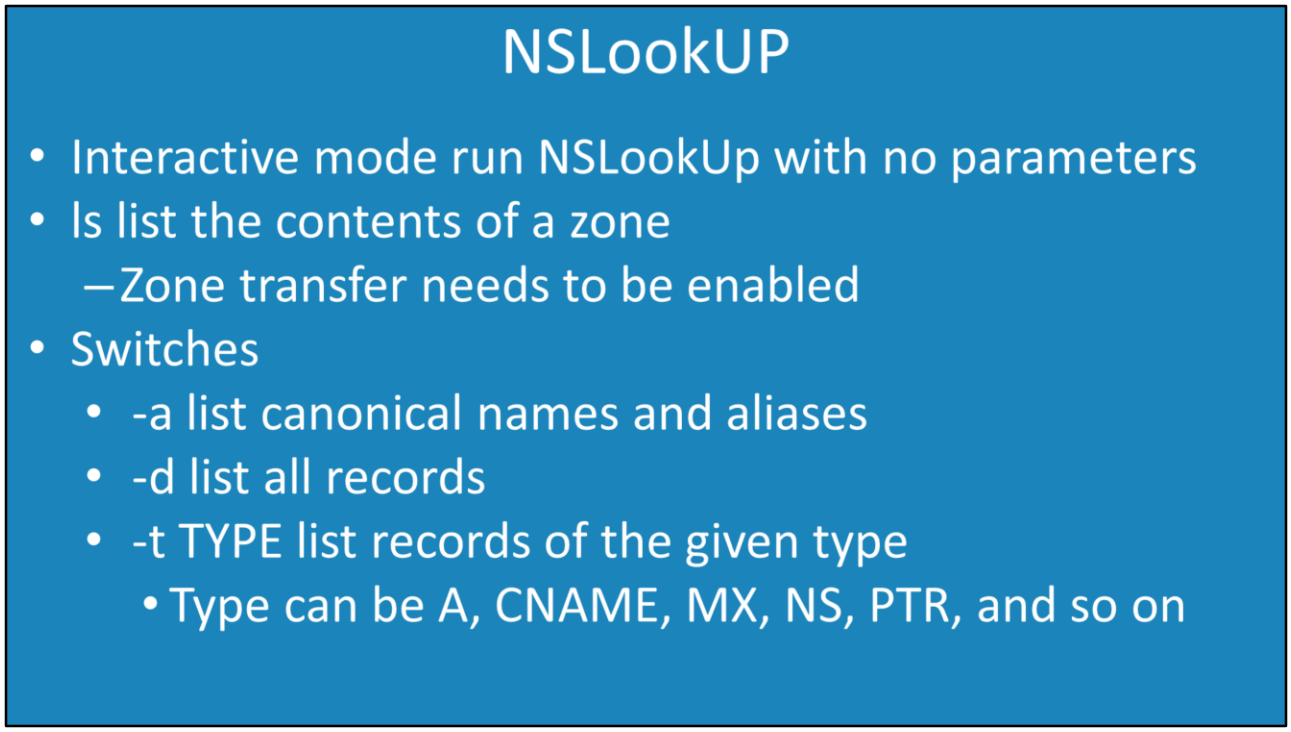
Demonstration

To open NSLookup, open a command prompt from the start menu.
To look at the name server records for a particular website, enter in NSLookup followed by the web address. For example, NSLookup google.com
If when running the command you have the line “Non-authoritative answer:” in the response, this means the result has been obtained from a DNS server that has either cached the results or has an unauthoritative copy rather than from a DNS server that is consider an authoritative DNS server.



NSLookup Non-authoritative answer

When querying a DNS server, a DNS server will first attempt to resolve the request from its cache. If it is not able to do this it will attempt to resolve the query itself. If the DNS server is configured for forwarding, the query will be forwarded to another DNS server, for example the ISP's DNS server and that DNS server will then answer the query from its cache or attempt to resolve it itself. In any DNS zone, there will be DNS records that state which DNS servers are considered to hold authoritative DNS records for that DNS zone. These can be primary or secondary zones. The point to remember is the administrator for that DNS zone has made a decision that these DNS servers should be considered authoritative or contain up-to-date DNS records. For example, a company, if they had permission to do so, could create a secondary zone from another DNS zone. However, it would be up to the company to make sure this secondary zone was keep up to date. If the company was a 3rd party company there is no guarantee that this would occur. For this reason, an administrator should not make a DNS server like this an authoritative DNS server. When an NSLookup returns a DNS record, it will indicate if this is a non- authoritative result with the text "Non-authoritative answer". The important point to remember is that even when forwarding is used you can still get an authoritative answer if the DNS server had to contact an authoritative DNS server in order to obtain an answer. The results shown for NSLookup are based on where the result came from, not which DNS servers were used in the process.



Demonstration NSLookup Interactive

If you run NSLookup without any parameters, this will launch NSLookup into interactive mode. The mode allows you to run multi commands one after the other.

If you enter in a domain name by itself, this will show all the name server records for ITFreeTraining. This is essentially a list of DNS servers that are considered to hold authoritative data for that DNS zone.

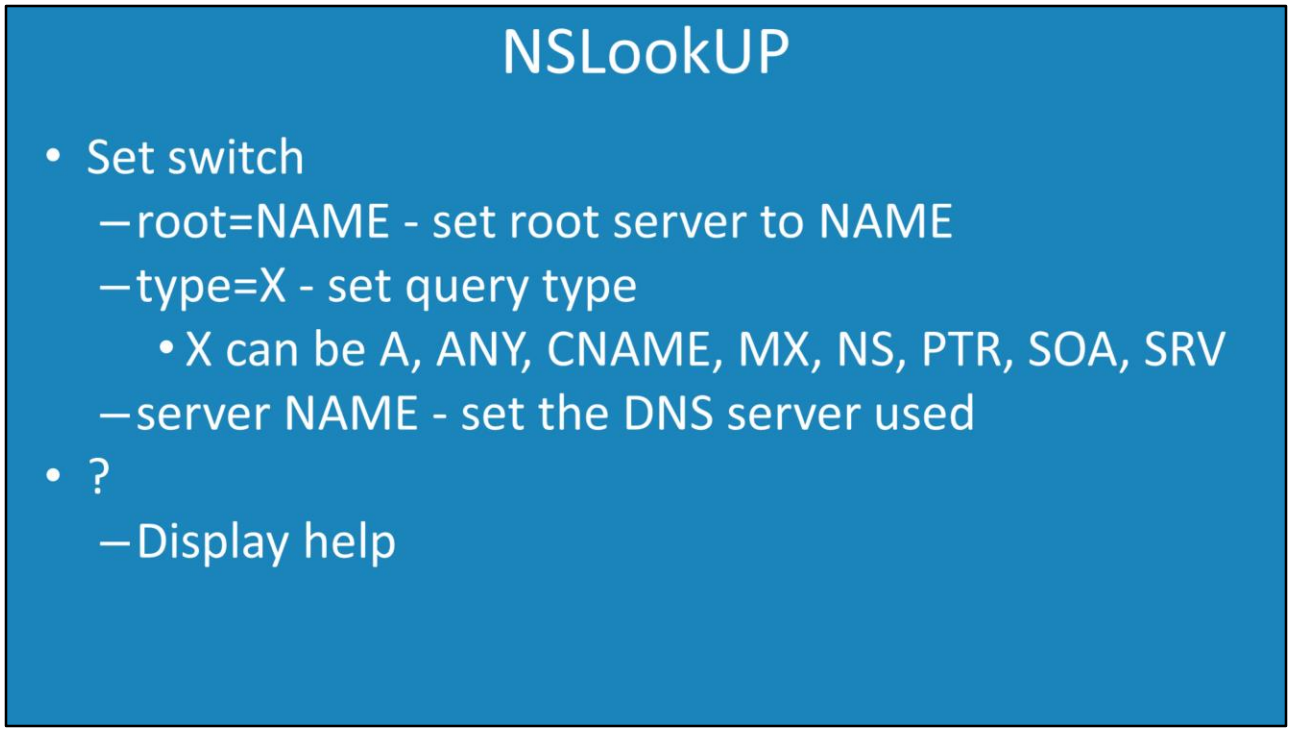
To list the DNS records for a DNS name, run the command "ls" followed by the DNS name. For example, ls ITFreeTraining.local

Most DNS servers will be configured to not allow a list of the DNS records held on that DNS server to be displayed. When you attempt to query the DNS records, you may get an answer back saying query refused.

On Microsoft DNS Server, to configure the DNS server to allow DNS records to be listed, run DNS Manager from Administrative Tools or under Tools in Server Manager. In order to configure the zone transfer properties, right click on the zone and select properties.

To allow DNS records to be listed using ls in NSLookup, zone transfers needs to be enabled on the computer that is asking for that information. This is done on the "Zone Transfers" tab. Once the tick box "Allow zone transfers" is ticked, the administrator is able to select which DNS server zone transfers will be allow or they can choose the option "To any server". If they select the option, "Only to servers listed on the Name Servers tab" this will only allow zone transfers to servers that are list on the tab "Name Servers".

The ls command also supports a number of switches. The –a switch will show only canonical names or aliases. The –d switch will list all DNS records. The "–t TYPE" will allow you to specify the type of DNS record that you want to list. Valid types are A, CNAME, MX, NS and PTR.



NSLookup also allows variables to be configured using the set command. For example, if you want to set the root server that NSLookup uses you can use "root=NAME", where NAME is the name or IP Address of the DNS server that you want to use as the root server. If you want all commands to output certain DNS records, you can do this with the command "type=RECORD" where RECORD is a type of record. For example, A, ANY, CNAME, MX, NS, PTR, SOA or SRV.
If you want to display all DNS records in a zone you can add the –d switch to ls, for example ls –d itfreetraining.local
If you want the output from a command to be saved to a file, you can use the greater than sign followed by the filename to save the output. E.g. ls – d ITFreeTraining.local > output.txt
If you want NSLookup to use a particular DNS server this can be done with the server command followed the name or IP Address of the server. For example, "server 8.8.8.8" for google public DNS server. All NSLookup commands will now use that DNS server. This is useful if you want to compare the results of a number of different DNS servers.
If you run the command "set type=all" this will configure the command to run the following commands with the default parameters. This essentially means that command will output the default results. In some cases, this may not be all the possible records.
If you want additional help you can use the "?" command to show the inbuilt help.

See http://YouTube.com/ITFreeTraining or http://itfreetraining.com for our always free training videos. This is only one video from the many free courses available on YouTube.

References
"Using NSlookup.exe" http://support.microsoft.com/kb/200525