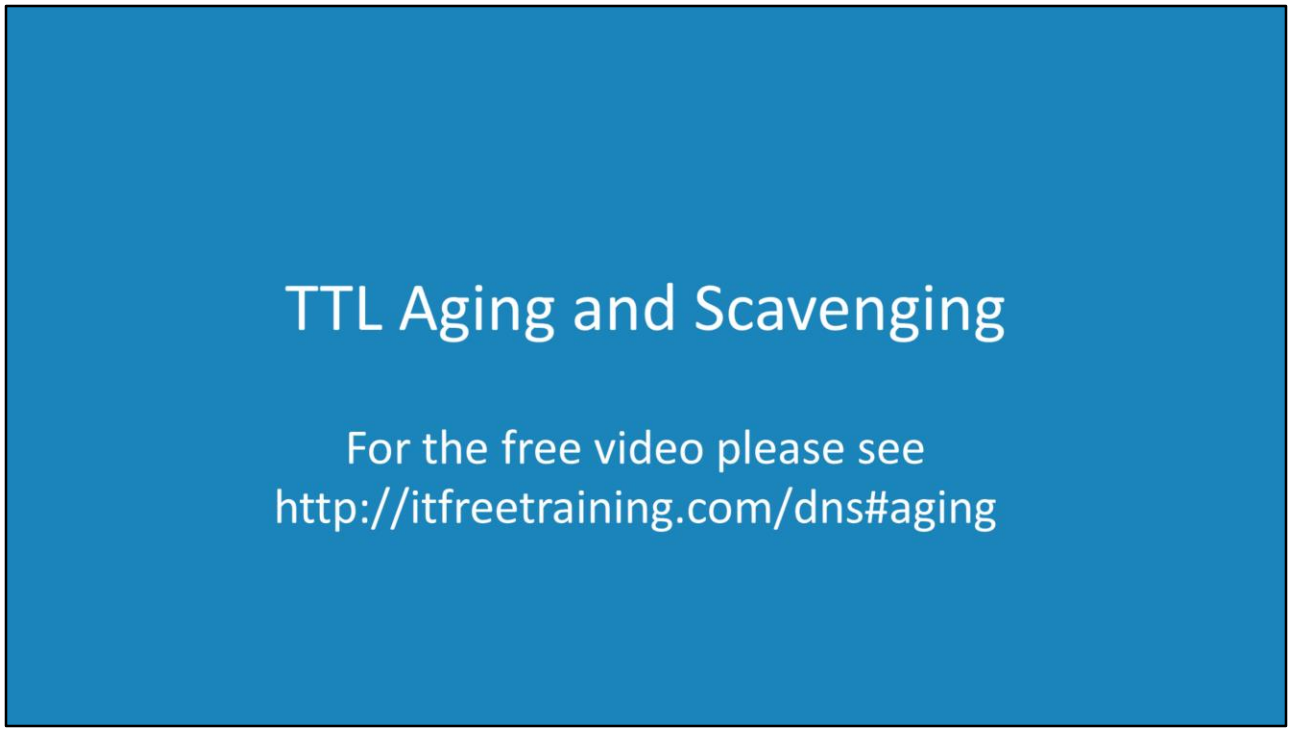
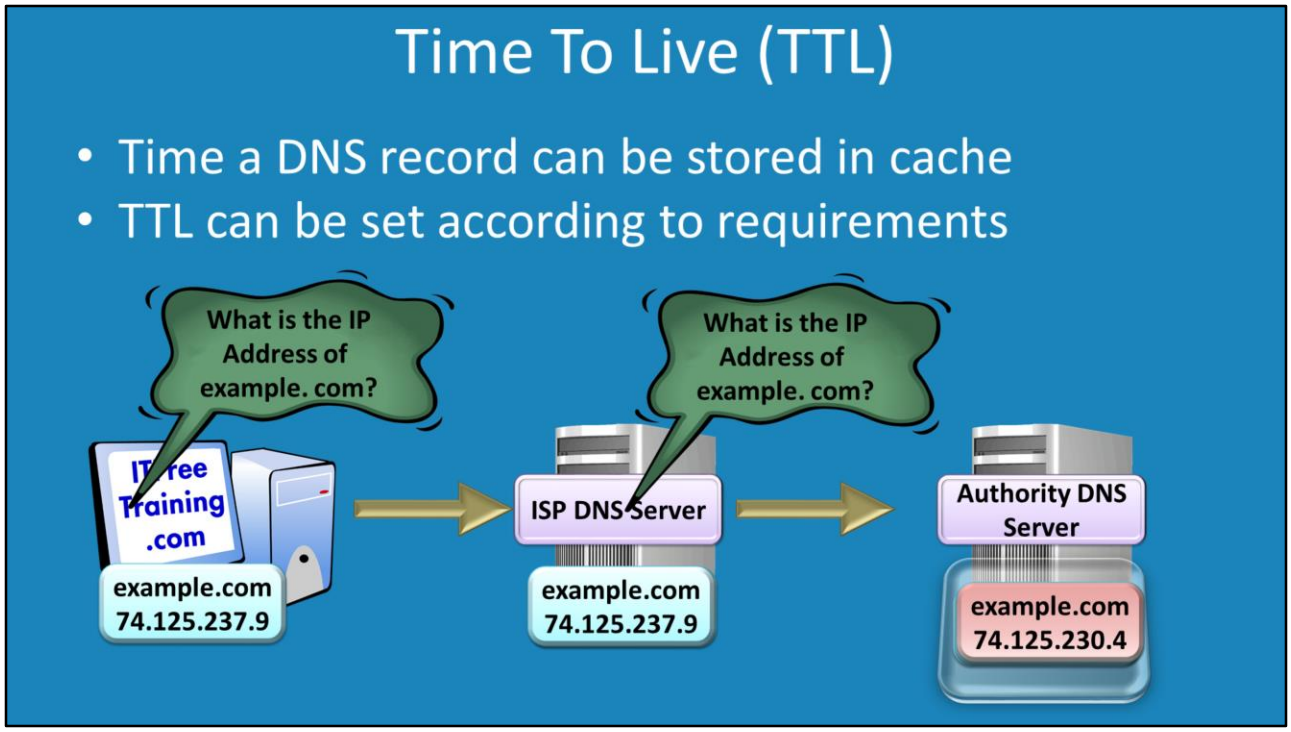


The DNS settings looked at in this video determine how long DNS records remain on the DNS server or in the DNS cache. DNS supports automatic removal of DNS records from the database if the appropriate options have been configured. This video looks at how to configure those options and the effects this can have on your network if the settings are not managed correctly

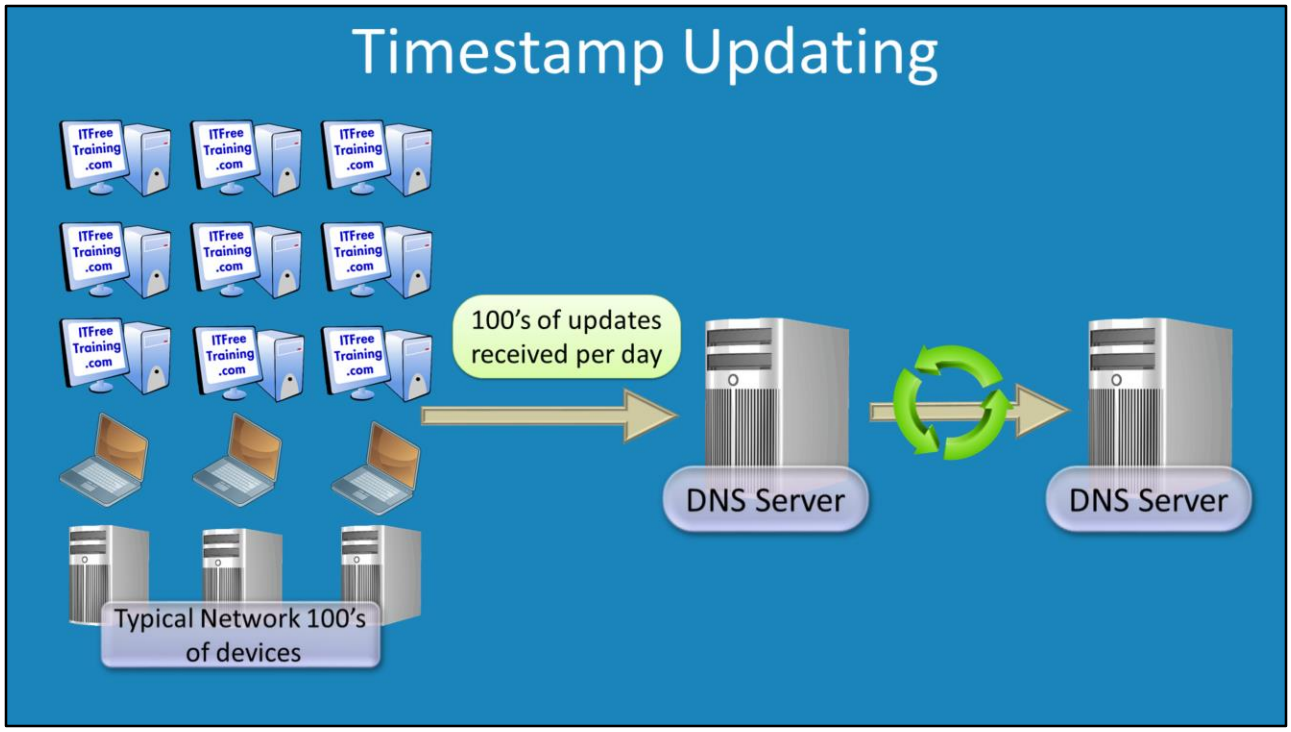


Time To Live (TTL)

Each DNS record has a time to live (TTL) setting. This value is configured by the DNS administrator. When a DNS record is stored in DNS cache, this DNS record can only be used for the time period stated in the time to live setting. When this expires, the DNS record must be obtained again. In the case of a work station, this means the working contacting a DNS server to obtain the DNS record again. In the case of a DNS server, the DNS server must obtain the DNS record again from another DNS server or from the authoritative DNS server for that DNS domain. This gives the administrator control over how long changes to a DNS records will take to have effect on the network. The lower the time to live setting is configured means changes to the DNS record will take less time to take effect on the network. This is because the DNS record will be discarded from the cache sooner and the DNS server will be forced to query a new copy of the DNS record. A lower setting does result in more DNS queries being sent to an authority DNS server which puts more load on the DNS server. A higher time to live setting means less queries to the authority DNS server, however this also means that changes to the DNS records take longer to take effect on the network.

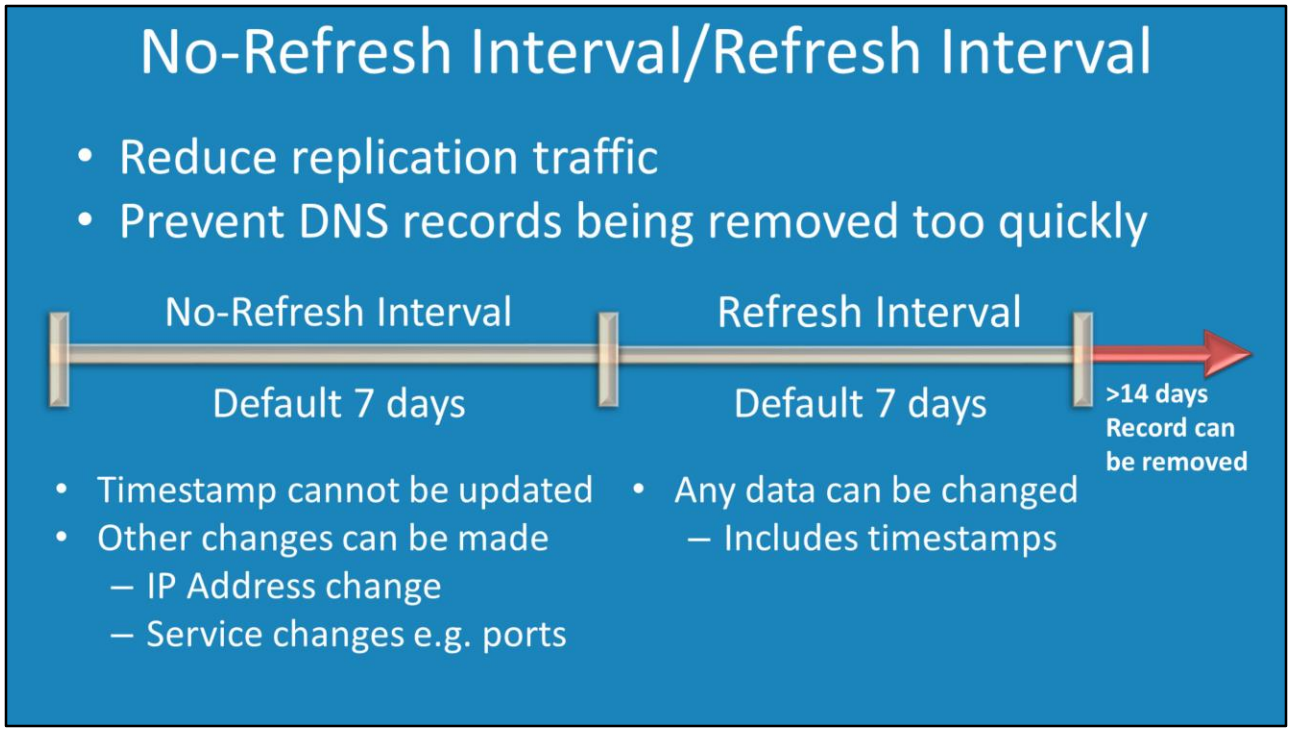
DNS Record Aging

Each DNS record has a timestamp which indicates when the DNS record was created or when it was last updated. Dynamic updates allow a client to create their own DNS records on a DNS server. If dynamic updates are enabled, the client is able to update this timestamp. The DNS server, if configured, has the ability to go through and remove DNS records that have not been updated for a set time period. This has to be configured for the DNS server and is not configured by default. When a client starts up and dynamic updates are enabled on the DNS server, the client can request the timestamp to be updated. Depending on the settings on the DNS server will determine when and if the DNS client can update the DNS record.



Timestamp Updating

On a typical network, each time a client starts up that supports dynamic updates, it will attempt to register its DNS records in the DNS server. In most cases, even when using DHCP, the client will have the same IP address and computer name each day when it starts up. This is because DHCP has a lease time and these lease times generally are configured to span over several days. For this reason, typically the only change to the DNS record when the client attempts to update its DNS record is the timestamp. For this reason, if there are a lot of clients on the network, this means that there are a lot of DNS record changes where only the time stamp has changed. All these changes need to be replicated to the DNS server that is holding that zone file which, in a large company, can result in a lot of network traffic.

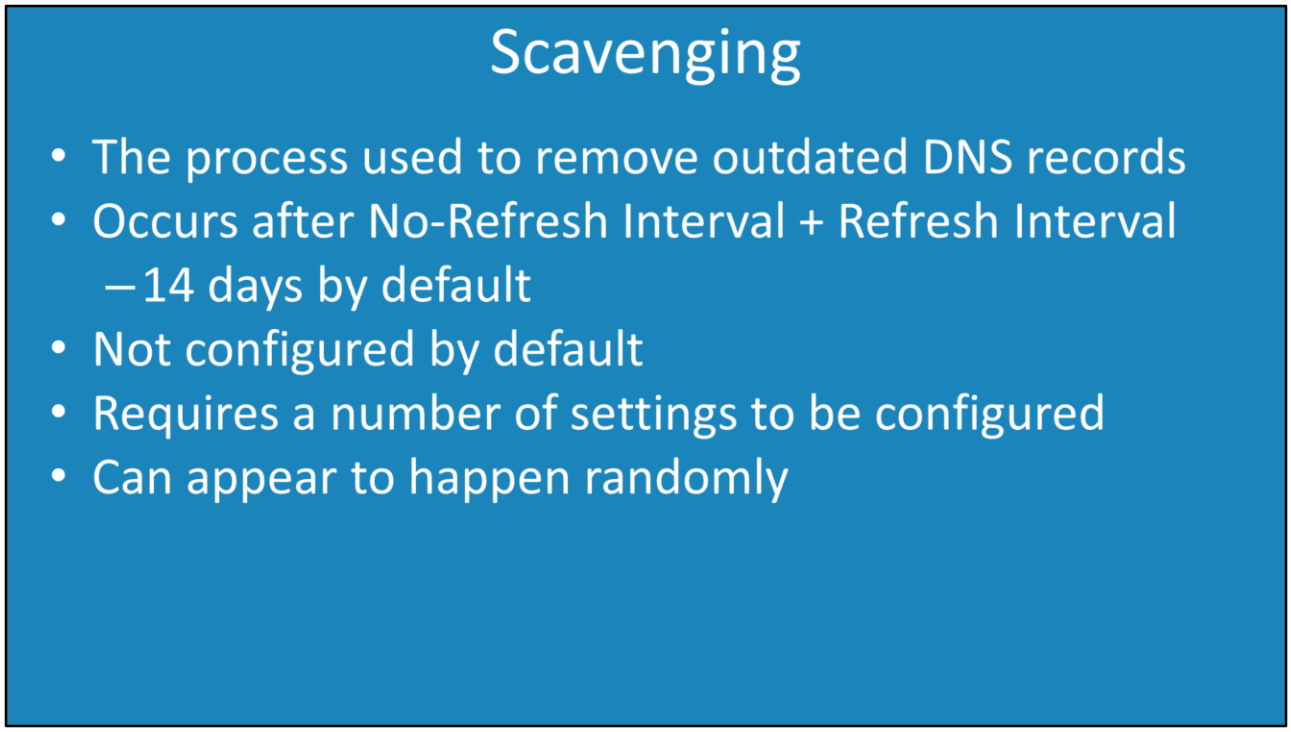


No-Refresh Interval/Refresh Interval

There are two settings that determine when a DNS record can be updated using dynamic updates. The combination of the two settings provide a method to reduce replication traffic while also preventing a DNS record from being removed too quickly.

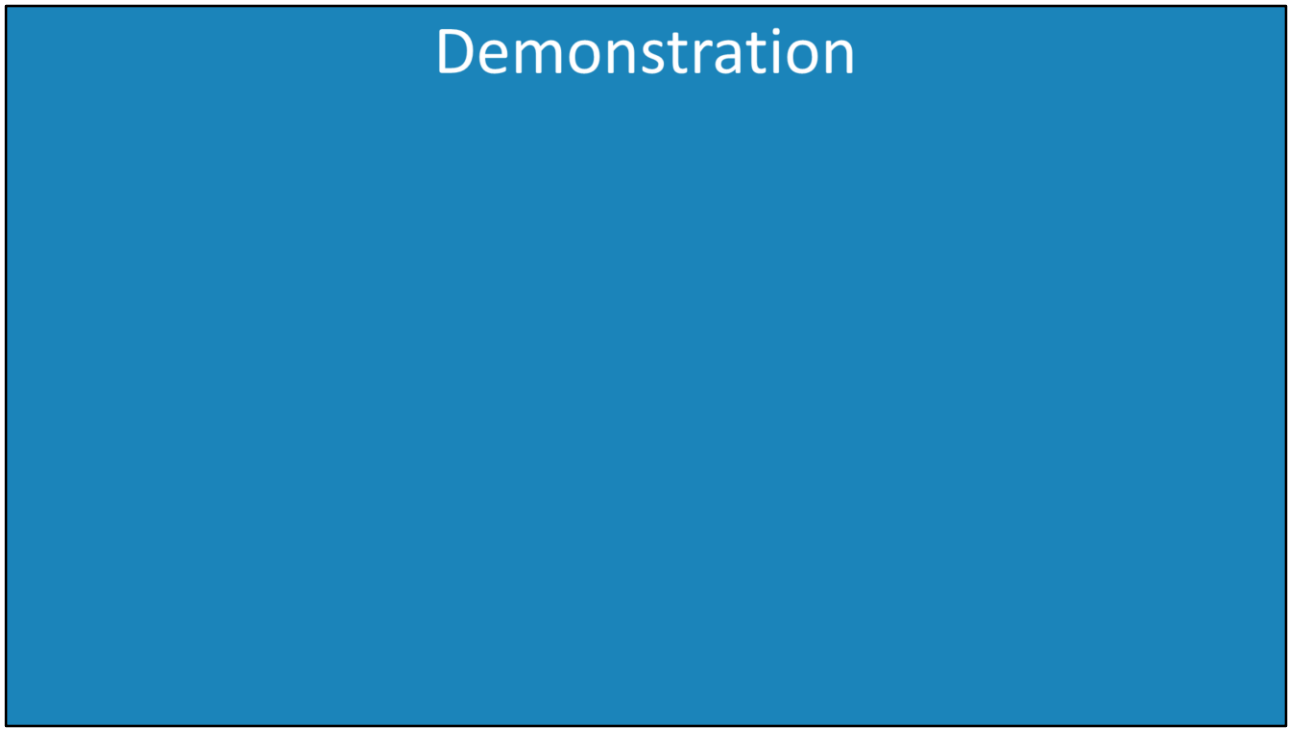
No-Refresh Interval: This value is set by default to 7 days. When a DNS record is first created a timestamp is set in the record. If a request is received to update the DNS record using dynamic update during the No-Refresh interval period, the update will be ignored if the update does not make any changes to the DNS record. This means that if all the details are the same, for example, name, IP Address, port or any other details in the DNS record, the update will be ignored. If this was not to occur, every time a DNS record was updated using dynamic update, the timestamp would be updated and this would require the DNS record to be replicated to all DNS servers that hold that DNS zone. This setting reduces the amount of replication that occurs.

Refresh Interval: This setting by default is also configured to 7 days. This comes into effect once the no-refresh internal setting has past. Given the default of 7 days for each, this means that the refresh interval comes in to play from day 8 to day 14. During this period, any update for a DNS record received during this time period will not be ignored like it was during the no-refresh interval. This includes updates when no details in the DNS record have changed, for example only the timestamp in the DNS record has changed.



Scavenging

This is the process of removing old DNS records from the DNS server. A record will not be scavenged until a number of days have passed. The number of days will be No-Refresh Internal plus Refresh Internal. If you take the default settings for these values, they are both 7 days. This means that a DNS record will need to be in the DNS data for 7 + 7 = 14 days before it will be considered for scavenging. If in this time period the DNS record is updated in any way, including refreshing the DNS record during the 8 to 14 day period, the timestamp will be updated and another 14 days will need to pass if the DNS record is not updated before the DNS record can be considered for scavenging or removing. Scavenging does not happen by default and needs to be configured. This involves configuring a number of settings. Since scavenging is performed by a background process in DNS, the process may seem to happen randomly. It however can also be triggered manually in the DNS Manager, however there may be a delay before you see any changes. If you enable scavenging, this can also remove resource records that are used by Active Directory. These are created automatically by Domain Controllers, however if you do not have dynamic updates on the DNS server enabled the timestamps on these DNS records will not be updated. The end result is that these DNS records will be removed meaning clients will not be able to find Active Directory resources on the network. Before you enabled scavenging, you should ensure that dynamic updates are working correctly on the network.



Demonstration

This demonstration uses Remote Server Administration Tools on Windows 8 to access a Windows Server running DNS server.

1. To open DNS manager open DNS that is found in administrative tools in the control panel.

In order for scavenging to work, it must be configured on the zone and also the DNS record must be enabled for scavenging.

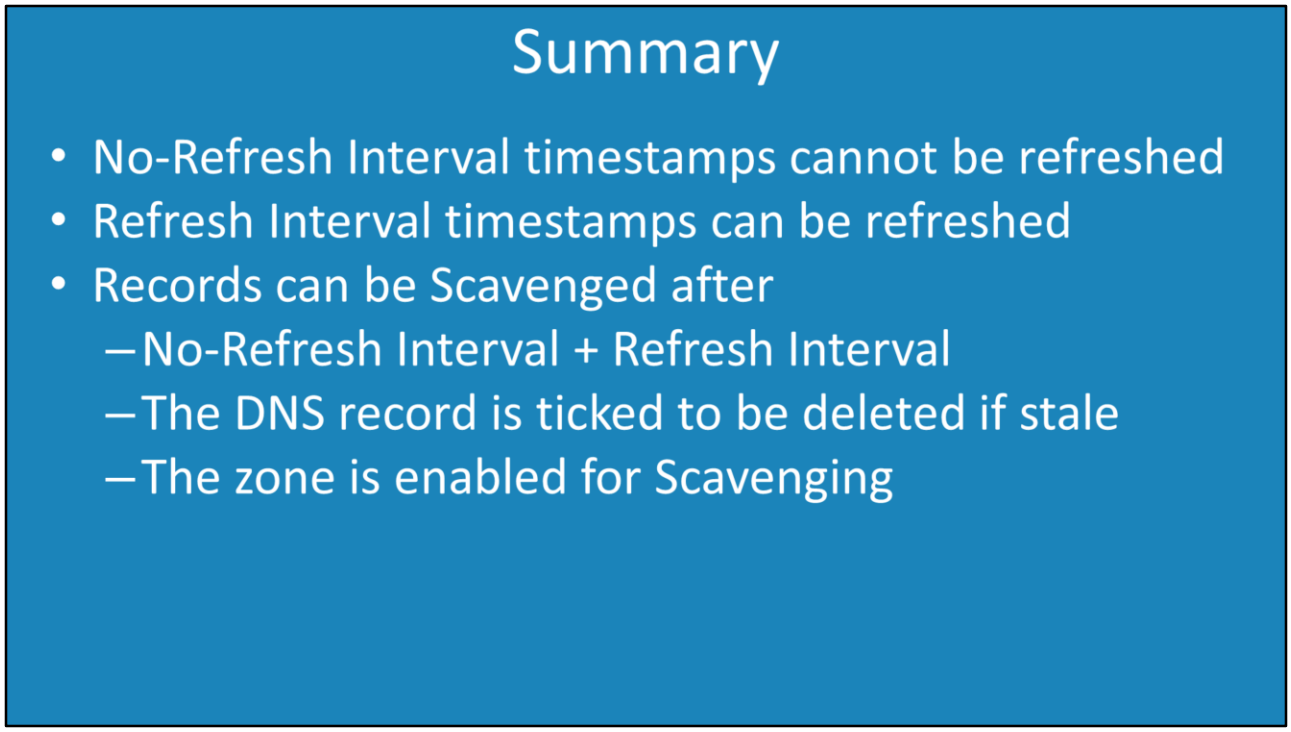
2. In order to check the scavenging settings in a DNS record, right click the DNS record and select properties. If the scavenging options are missing, you will need to first select advanced under the view option to show advanced features like scavenging. In the properties for the DNS record will be a tick box “Delete this record when it becomes stale”. This effectively enables the DNS record to be scavenged. Below this is the time stamp of when the record was created or last updated. It is important to note at the bottom is the Time To Live (TTL) for the DNS record. This value indicates how long a DNS server or client can keep a DNS record in its cache before it is removed and must be re-queried. It is important to keep this setting in mind as even if the DNS record is scavenged, clients and DNS servers will keep using the old DNS record in the cache until this value expires.

3. In order for scavenging to occur, the zone needs to be configured to allow scavenging. To do this, right click the zone and select properties. In the properties for the zone file, press the button aging. In order to enable scavenging, the tick box “Scavenge stale resource records” must be ticked. Once enabled, the two settings No-

refresh internal and Refresh internal come into effect. No-Refresh interval determines how long a DNS records timestamp cannot be updated if there are no changes to the DNS record. Refresh interval is the period of time after No-refresh interval in which a DNS record can be updated with any changes, including only timestamp changes. With Scavenging enabled, DNS records will be removed after the time period No-refresh interval plus Refresh interval which is 14 days by default.

4. If you right click the DNS server name in the DNS Manager, a menu will appear with the option “Set Aging/Scavenging for All Zones”. This option configures the default No-Refresh Interval and Refresh internal for new Active Directory Integrated zones. There is a tick box “Apply these settings to the existing Active Directory-Integrated zones.” If you tick this option it will change these settings for all existing Active Directory Integrated zones, but not for zone files like primary or secondary zone files.

5. Scavenging will happen by itself given enough time. If you want to manually start the process, right click the DNS server name in DNS manager and select the option Scavenge Stale Resource Records. It should be pointed out that in order for a DNS record to be removed the following must be true. The DNS record timestamp must be greater than No-Refresh Internal plus Refresh Internal, the DNS zone must be enabled for scavenging and the DNS record must also be enabled for scavenging.



Summary
Using dynamic update, a DNS record during the No-Refresh interval time can only be updated if there are changes to the details in the DNS record. If there are no changes, the DNS record will remain the same and thus the timestamp on the DNS record will not be updated. After the time period after No-fresh Interval the DNS record can be updated regardless of whether the DNS record has changed or if only the timestamp is changing. Once the time period No-Refresh interval + Refresh Interval has passed, the DNS record is eligible for scavenging or can be automatically removed. In order for this to occur, the DNS record needs to be ticked for deleted if stale in the properties and the zone needs to be enabled for scavenging.

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
"MCTS 70-640 Configuring Windows Server 2008 Active Directory Second edition" pg 482