DNS Caching and Simple Failover

Depending on the application and other circumstances, DNS caching may affect how quickly users are re-directed to a backup server by Simple Failover.
Of course you need to compare this to the alternative:
Without Simple Failover, as long as your main server is unavailable, NO users will be able to access your services.

In general however, DNS records updated by Simple Failover will be accessible to the vast majority of users immediately or within a few minutes.

This document provides a short introduction to how DNS caching works, how it is implemented by different applications, and how this affects Simple Failover.

DNS caching and TTLs

As DNS records are passed from the original DNS server (one of the primary or secondary DNS servers for the record domain name), via other DNS servers (resolvers), DNS caches, and finally to a client application (for example a web-browser), they are cached (stored for later use) in several places along the way.

Each DNS record has a TTL (time to live) value attached.
This value is controlled by the original DNS server, and represents the length of time that other DNS servers and applications are allowed to store this DNS record before they must discard it and request a new copy if needed again.

Whenever a DNS server or application passes a cached DNS record to another DNS server or application, the DNS record must be provided with the current TTL value (= original TTL value less the time it has been cached).
This ensures that all cached copies of a DNS record around the Internet will always expire according to original TTL value provided when the record was requested from the original DNS server.

For example, if you wanted to be able to change the IP address of your web-server and for everyone to see this within 2 minutes, you would set the DNS record TTL value to 2 minutes.
This way when you change the DNS record IP address, all cached copies of the DNS record with the old IP address around the Internet, would timeout within the 2 minutes of changing the record.

This is exactly how Simple Failover works!
By setting a low TTL value on your DNS records, it is able to change the DNS records when needed and for this to take effect very quickly.

It is often said that it takes 24 to 72 hours for DNS changes to propagate throughout the Internet.
This is true for domain registration changes (such as initial registration, or changing registrar or DNS server), because the Internet root DNS server operate with 24 hour TTLs.
However, this does not affect individual DNS records such as the record for “www.yourname.com”, for which you can set your own TTL value.

Unfortunately, not all DNS servers and applications fully honor the DNS record TTL value. The following is a discussion of some of these deviations and their impact.

DNS servers

The vast majority of DNS servers around the Internet use TTL values correctly as outlined above, and standard DNS server installations do this out of the box by default.
However, in some cases it is possible to re-compile or re-configure the DNS server software to work differently.

It has been suggested that some ISPs configure their DNS servers to cache all DNS records for a minimum period (such as 60 minutes) in an attempt to reduce DNS network traffic.
This may have been the case in the past, but this does not appear to be very common today, probably because more and more web sites and Internet services depend on quick updates to DNS records.

DNS network packets are extremely compact and take up very little bandwidth compared to everything else we send across the Internet, so this is not a good place to look for bandwidth savings anyway.

“www.cnn.com” is one example of a well-known larger web site, which depends on low TTL values to enable quick changes to their web site (they currently use DNS TTL values of 5 minutes).

Also, many small web-sites today depend on low TTL values because they run on ADSL or cable connections with dynamic IP addresses, and therefore require frequent DNS updates (when their IP address changes).

Obviously, any ISP who chooses to cache DNS records beyond their original TTL value will potentially cause a lot of problems for their own users.

Windows operating system DNS cache

Microsoft Windows 2000 and later includes a DNS cache - the “DNS Client” service. You can display the contents of this DNS cache by typing “IPCONFIG /displaydns” at a command prompt, or clear it by typing “IPCONFIG /flushdns”.

This DNS cache honors TTLs as described earlier in this document, and so this does not cause any caching beyond the original TTL.

Earlier Windows versions did not have this DNS caching service, and instead sent all DNS requests directly to the DNS server.

Client Applications

Most client applications rely on the operating system and/or local DNS servers for DNS resolution and caching, and do not implement any type of DNS caching themselves.
There is however one signification exception to this - Internet browser applications:

Microsoft Internet Explorer browsers

Internet Explorer 4, 5, and 7 by default caches all DNS record for a period of 30 minutes no matter what the TTL value is.
This means that there is up to a 30-minute delay before they will discover DNS changes.
This of course only affects visitors who have visited the web site immediately before a DNS update. New visitors or return visitors who closed their browser or waited more than 30 minutes since their last visit are not affected.

It is possible to adjust the length of time I.E. caches DNS records by updating a registry setting on the client machine. But this is of course only practical in an intranet scenario.

Internet Explorer v. 6 does not cache DNS A-record responses. It only caches DNS CNAME-record responses. Simple Failover only uses DNS A-records.
This means that this browser version practically discover DNS changes made by Simple Failover instantly.

Firefox and other Mozilla/Netscape browsers

All versions of the Firefox and Mozilla/Netscape browsers since mid 2004 by default cache all DNS records for 1 minute no matter what the TTL value is.
This means that they will discover DNS changes within one minute.

Earlier versions of Mozilla/Netscape browsers cache all DNS records for 15 minutes no matter what the TTL value is.

References:
This document is based on our own lab results and observations.

Last updated: November 14th 2006.