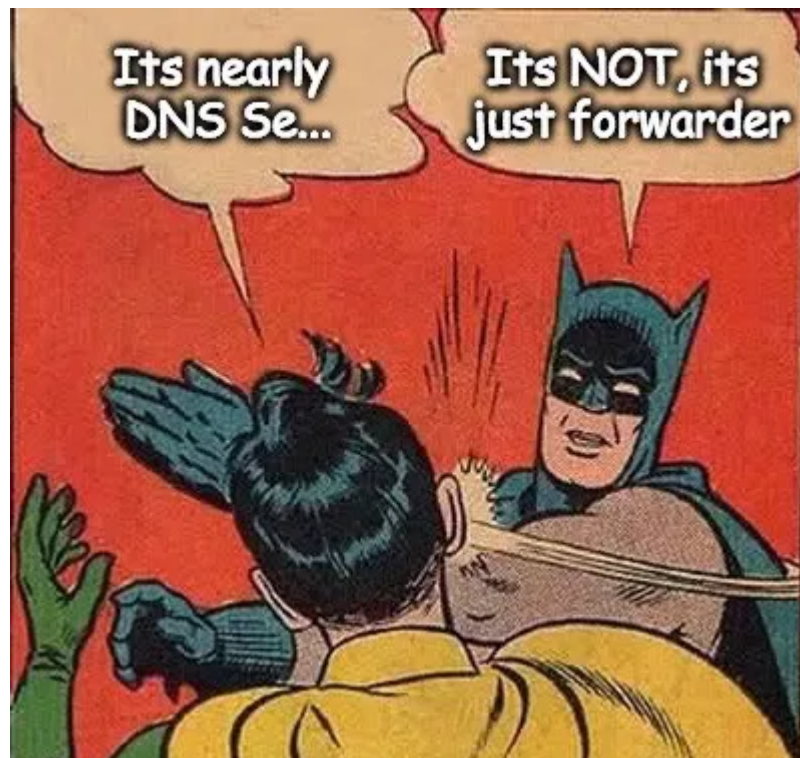


Anatomy of DNS Forwarding capability in NSX for vSphere

There seems to be a little uncertainty or confusion about the DNS forwarding feature in Edge device of NSX for vSphere 6.1.x. and so some clarification we feel is necessary.

Firstly and to make this crystal clear, the NSX for vSphere Edge device can be configured as a DNS forwarder. This is "**not**" an authoritative DNS server; the NSX for vSphere Edge device is acting just as a DNS forwarder (resolver).



What happens here is, the NSX for vSphere Edge device will forward the client's DNS request to one of the configured external DNS server(s).

When the NSX for vSphere Edge device get's a response back from the external DNS server(s), the NSX for vSphere Edge device will **cache** these requests and then send back the response(s) to the clients. Also be aware that the NSX for vSphere Edge device does not **periodically synchronize** its DNS database with the primary DNS server, we mention above the NSX for vSphere Edge device is just acting as a DNS forwarder not an authoritative DNS server.

You will also notice when configuring this feature that the NSX for vSphere Edge DNS Cache default is set to 16. But 16 what? That is **16 MB**.

So obviously next, you will ask what is the minimum and maximum NSX for vSphere Edge DNS Cache size that can be set? Well the answer is that the minimum is **1 MB** and the maximum is **8192 MB** (however this depends on what the physical memory of the NSX for vSphere Edge form factor is).

You may also be wondering how long on the NSX for vSphere Edge device do we cache these responses for? The length of time for which a record may be retained in the cache of a caching name server is controlled by the **Time To Live (TTL)** field associated with each resource record. Each DNS record received from the upper DNS server will provide the TTL for it. The NSX for vSphere Edge device will save the record in the cache until the TTL time has expired.

Well that's about the theoretical anatomy of DNS forwarder. Let us now take a look at the NSX for vSphere v6.1.x API Guide with regards to this specific feature.

Configure DNS servers:

URL : <https://<nsxmgr-ip>/api/4.0/edges/{edgeId}/dnsClient>

Method : PUT

```
<dnsClient>
<primaryDns>10.117.0.1</primaryDns>
<secondaryDns>10.117.0.2</secondaryDns>
<domainName>vmware.com</domainName>
<domainName>example.com</domainName>
</dnsClient>
```

So, are you still struggling a little to understand the use case of why we have such a DNS forwarder feature in the NSX for vSphere Edge device?

Firstly, and generally the NSX for vSphere Edge device is deployed as a gateway device. It has external access to the upper DNS server or Internet. Internal clients want to resolve DNS names etc, so if the NSX for vSphere Edge device does not act as forwarder, you have to assign a NAT address for each client or public address for each client so the client can access the external network or internet.