



Load-Aware Entity Location with BIG-IP DNS Services

We all know it: when it comes to data, not all subscribers are the same. Use varies wildly from person to person. Some listen to music and watch videos on every device, everywhere they go. Others prefer to spend their time playing games, engaged on social media, or sending email. And some even use their cell phones as, well, phones, conducting business and talking with friends and family.

Different subscriber use patterns produce uneven load on elements of the packet core network, particularly the gateways. Traditionally, this problem has been addressed by using purpose-built hardware and ensuring that each gateway has ample spare capacity. However, providers are rapidly embracing virtualization. In order to build the most robust NFV-based architecture, elements will be smaller, and capacity will be expanded by adding more instances of the necessary elements, rather than making the instances bigger.

Ideally, new subscriber sessions should be attached to gateways with lower relative load. Since MMEs locate an appropriate SGW and PGW using DNS, and an SGSN also uses DNS to locate an appropriate GGSN, the DNS server could be used to help an MME or SGSN make a decision based on load.

Consider the PGW location procedure used by an MME. The MME constructs a NAPTR host lookup name based on the required APN. For example, it could start by using `internet.apn.epc.mnc001.mcc001.3gppnetwork.org`. From the resulting list, the MME performs a sub-selection, taking into account the service parameters. This yields a candidate set of PGWs. Based on the record flag, each candidate hostname requires either an address record (A or AAAA) lookup or an SRV lookup. Since DNS record order ordinarily implies nothing about reachability or load, the candidate set will be unordered and some of the elements in the set may not even be reachable. Although SRV records can communicate load information using the weight field, it's usually a static value, so it most often indicates capability, rather than instantaneous available load.

F5 BIG-IP DNS provides a robust, highly-customizable method to enable elements to take load and reachability into account when making gateway selections. This mechanism is built on top of the BIG-IP platform's proven, powerful global-service load-balancing (GSLB) function. Using a special type of BIG-IP scripted monitor (External Monitor) BIG-IP DNS collects information about each node, then assigns a weighted score. The higher the system load, the lower the weight. Because an External Monitor is a script running on the BIG-IP control plane, the information used to compute the weight can be any factor that an operator deems relevant. For example, a monitor might use CPU load, memory load, and the count of current contexts through the system.

Moreover, a different monitor can be used for different elements. Imagine you have three PGW vendors. One of the vendors exposes the necessary data via SNMP, another exposes it only via its CLI, while the third exposes some information via SNMP and other information via its CLI. You could assign a different monitor for each target type. The External Monitor could even collect information from a separate system; for example, a RESTful interface exposed by your NMS.

Because the monitor is a script, each operator can select not only the desired data set, but can determine how to mix the data elements. Again, imagine that CPU, memory, and current context count are used as the load factors. If CPU utilization is the most important factor, it could contribute 50% of the score value, while memory and contexts would each contribute 25%.

When the locating entity queries BIG-IP DNS for the appropriate NAPTR records, it returns a list in order of relative load, from lightest to heaviest. If SRV records are used, the weight score can also be populated into the SRV weight field. This allows for more refined load distribution between the gateway elements. The NAPTR order preference and SRV precedence fields can also be manipulated. For example, if the load for a particular gateway is over a specific threshold, the preference field could be set to a higher value, minimizing its use while in this state.

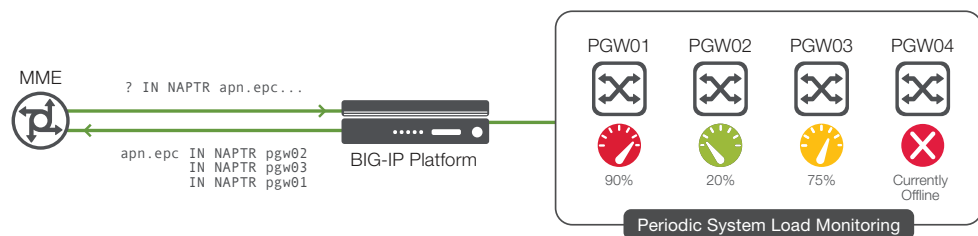


Figure 1: Load Aware DNS Responses

When responding to appropriate queries, BIG-IP DNS can operate in screening mode or answer by delegation. In screening mode, all queries are directed to a BIG-IP DNS listener. The listener responds to hostnames for which it's configured and passes all other requests to a pool of local DNS servers. When in screening mode, you can take advantage of DNS-specific DDoS protection on the BIG-IP platform, as well as health-aware load-balancing to the local DNS servers. Delegation can occur by alias (CNAME record) redirection or by NS delegation of the appropriate zones.

In addition to the load detection, BIG-IP DNS can also perform other health checks, including GTP echo requests, ICMP ping, UDP port reachability, and many others. As with the load-aware monitoring, different health checks can be assigned to different targets. Disabling a target—for instance, when it's taken out of rotation for maintenance—is also as easy as clicking a checkbox.

Of course, these days, many operators want to automate the configuration of their various nodes using orchestration systems or SDN controllers. BIG-IP DNS exposes all of its configuration elements over a RESTful interface. F5 also provides modules for Ansible, Puppet, Chef, OpenStack HEAT, and other systems. Moreover, BIG-IP DNS allows operators to create custom workflows using iApps, exposing those workflows using custom REST endpoints.

BIG-IP DNS load-aware entity location provides a simple, powerful, highly-customizable system so you spend less time worrying about operational concerns, and more time creating amazing new services for your customers.

