LTM: Per-VLAN Default Gateways

Deb Allen, 2008-01-07

Load balancing is only a part of the work LTM is asked to perform in most networks. In addition to handling inbound load balanced requests, LTM is often the default path to the rest of the network or to the outside world, and must support the organization's existing routing scheme for outbound requests initiated by systems on the server VLANs. For most customers, a highly available / redundant gateway configuration provides robust and flexible routing services for outbound requests, and no specific configuration is required on LTM to support it. In cases where multiple egress routers are available but they are not transparently redundant, LTM can be configured to use a pool of gateways, always preferring one over the other but always choosing one that is currently available. In either of those scenarios, the source of the traffic is not considered when choosing a next hop router.

For some customers that's not enough: They need to use a specific next hop for outbound traffic traversing the LTM, based on the origin VLAN. You can think of it as source routing over a singe hop, or a per-origin-VLAN default gateway for LTM. Here are a couple of recent requests:

> *"We are hosting two customer sites with separate firewalls, but both firewalls are connected to an internal network where we have ldap, backup, dns and other infrastructure servers that are used by both customers.*
> *So what we need to do is make the bigip route traffic from webserver A to firewall A and the same for customer B for all internal networks. Is there an easy way to do source routing in the bigip?"*

> *"I have several VLANs 'behind' the F5 LTM and need to have separate default GW for each VLAN. I was looking for a source routing option so i can specify that"*

The Steps

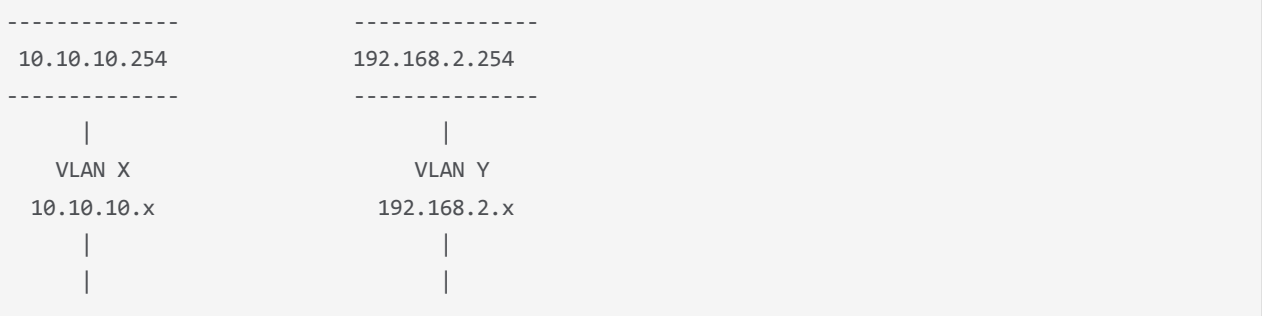
There are a number of steps that must be followed to create the configuration supporting this "per-VLAN" egress routing scheme, most of which take place on the LTM. They are:

1. Define server VLANs and Self-IP addresses on LTM
2. Set the default gateway on servers to the LTM floating Self-IP address
3. Define router VLANs and Self-IP addresses on LTM
4. Define router pools on LTM
5. Define wildcard virtual servers on LTM

I'll explain each in detail in the following sections.

The Network

Here is the basic network diagram I will use to demonstrate the solution:



```
-----------------------------------------
-                                       -
-                 LTM                   -
-                                       -
-----------------------------------------
       |                          |
     VLAN A                     VLAN B
   172.18.10.x                172.18.12.x
       |                          |
     server                     server
```

Server VLANs

By the time you are refining the routing configuration on LTM, you have most likely already defined your server VLANs, but lets review the basic configuration requirements. VLANs are the foundation of the solution, as a specific default gateway configuration will be constructed and enabled on each server VLAN.

You must define a separate server VLAN on LTM for each unique gateway configuration you require. A Self-IP address in the appropriate address space must then be configured on each server VLAN (a floating Self-IP address must be defined if configuring a redundant pair).

Referring back to the diagram above, you would configure VLAN-A on the LTM with Self-IP addresses in the 172.18.10.0/24 subnet, and VLAN-B with Self-IP addresses on the 172.18.12.0/24 subnet.

Server Default Gateways

Once you have defined each of the server VLANs on LTM, and a Self-IP address on each VLAN. (A floating Self-IP address if configuring a redundant pair) you will need to set the default gateway on all the servers to the LTM floating Self-IP address on their VLAN.

Referring to the diagram, the servers at the bottom would have addresses in the 172.18.10.0/24 or 172.18.12.0/24 subnet, and would use the corresponding LTM floating self-IP address as their default gateway.

Router VLANs

You must define separate router VLANs (sometimes called "frontend" or "transit" VLANs) on the LTM, one for each egress router. These VLANs will each contain an egress router and a corresponding local Self-IP address, and will be associated with a specific server VLAN. A Self-IP address in the appropriate address space must then be configured on each router VLAN. (A floating Self-IP address must be defined if configuring a redundant pair).

Referring to the diagram, you would configure VLAN-X on the LTM with Self-IP addresses in the 10.10.10.0/24 subnet, andVLAN-Y with Self-IP addresses on the 192.168.2.0/24 subnet.

Router Pools

Next you must define a router pool for each egress router. In the example above, we will create a pool named Gateway-X with a single pool member: 10.10.10.254:0; and a second pool named Gateway-Y with a single pool member: 192.168.2.254:0.

Wildcard Virtual Servers

The piece that pulls it all together is the Wildcard Virtual Server. A wildcard virtual server listens for all addresses, all ports, and can be configured to listen for any IP protocol. It can also be configured to listen only on a specific VLAN, and to forward traffic without destination port or address translation to a pool - exactly what we need to selectively forward traffic.

To create a virtual server that matches all addresses and ports, configure it with a destination IP of 0.0.0.0/0.0.0.0 on port 0, select "All Protocols", and choose type "PerformanceL4". To support selective routing from only a single VLAN to a single egress router, disable address and port translation, enable the virtual server only on that one VLAN, and add as a resource the pool containing the intended egress router. (The virtual server could also have SNAT enabled if it's required for routing of responses.)

So for this example, you would create a wildcard virtual server (0.0.0.0/0.0.0.0, port 0, All Protocols, type PerformanceL4), enable it only on VLAN-A, and use the Gateway-X pool. Then create a second wildcard virtual server with the same settings, only this time enable it only on VLAN-B and use the Gateway-Y pool.

Summary

With this configuration in place, any traffic outbound from VLAN-A will always egress via the 10.10.10.254 gateway on VLAN-X, and any traffic outbound from VLAN-B will always egress via the 192.168.2.254 gateway on VLAN-Y.

Want more?

If you'd like to hear more about this solution, it was also the topic of a recent DevCentral Post of the Week: LTM, Routing, and Multiple Gateways

Get the Flash Player to see this player.
20080701-PerVlanDefaultGateways.mp3

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com