The Sharkfest 2015 Megalodon Challenge

Introduction

The Megalodon Challenge is bigger and a lot more complex than the usual Sharkfest capture file challenges. There are no highly specific questions that can be answered with a definitive answer. The general idea is to have participants solve a real world network analysis problem, with all its confusion, drawbacks and uncertainties.

To achieve that kind of experience all participants will receive the same rather large capture files that have been taken (and sanitized, of course) from a real life analysis job solved by myself in November 2014.

Scenario

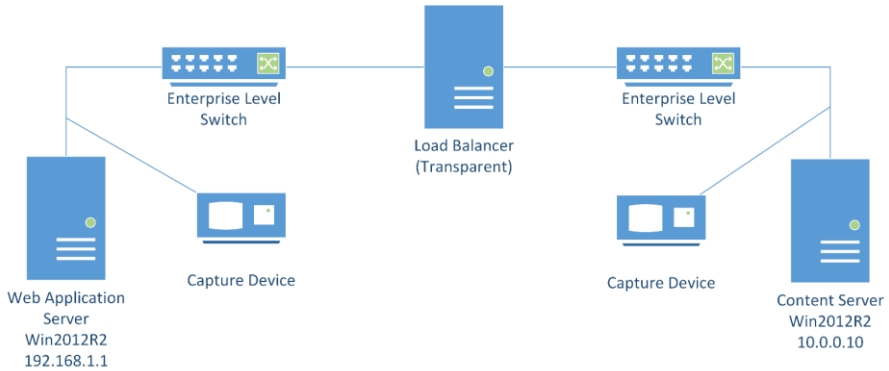
It all started with a phone call on a Sunday afternoon. The CTO of a company in the online travel business called me about a problem his development team had with the new online web portal that was about to go live in the next couple of days.

During the preparation of the new portal the team had performed a stress test to check how the web pages would behave under high load. Unfortunately, the test had not been successful, and to makes matters worse nobody knew exactly why not. At a certain point in time during the test there would be unanswered page requests, but it was unclear if it was a network problem, an application framework problem, or something in the application logic itself. Or maybe even something else entirely.

The good thing about the situation was that the problem had already been pinpointed to the communication behavior between two server nodes that were part of the web portal infrastructure. The first server was a web application server, querying a content server for web page elements. It seemed that at a certain point in time, the web application server would not get a reply for some of its requests anymore.

The capture setup

Designing a capture setup can be a complex task, but in this situation it was actually pretty simple: both the application load balancer and the content server were captured at the same time. Both servers were running a Windows 2012 operating system, and both were connected with Gigabit links to switches. The communication had to run through an additional transparent network load balancer. This is the network diagram:



Your task

Determine the cause of the problem. You should work towards a solution proposal you can give the customer in your report. In the end, the customer needs an action plan or at least a recommendation. You should also be able to tell if “it’s the network” or not.

In this challenge, while your role is being the network analyst, I (Jasper) will "play" the customer. So if…

- …you have questions about anything that you think will help in your analysis, just ask me. You may get a more or less specific answer.
- …there is anything you need, tell me. Maybe I can help.
- …you get stuck, talk to me as well for some hints to keep you going

I'll make myself available at the Reef as often as I can, but I'm also reachable via email or Twitter (see "Contact Info").

Materials

- Capture files on “Shark” USB-Stick handed out by Jasper (please return, there’s only a few of them)

Contact info

Challenge PDF: http://www.packet-foo.com/megalodon2015/challenge.pdf
Email: jasper@packet-foo.com, use topic "Megalodon Challenge"
Twitter: @packetjay