Understanding BGP

Jonathan Frederickson

February 14, 2015

1 Background

Border Gateway Protocol, or BGP, is a protocol used for routing between autonomous systems (AS) on the internet. ISPs run autonomous systems to exchange routing information with each other. Large corporations often do so as well if multihoming is required; that is, it allows the same address space to be used at multiple locations.

BGP can also be used within an AS - this scenario is called iBGP, or Interior Border Gateway Protocol. In this configuration, the network must be arranged in a full-mesh topology. That is, all nodes in the network must peer with all other nodes.

Despite being an integral part of today's internet, BGP is not without its problems. In particular, the only thing preventing any customer with an AS from maliciously inserting routes into the global routing table is filtering performed by the ISP. If one is able to locate an ISP that does not perform this filtering, it is possible to hijack routes of other internet traffic. This has occurred before; in one instance, a large portion of YouTube traffic was routed through Pakistan due to a configuration error.

In the global internet, to facilitate filtering of BGP traffic, many ISPs use what is known as "routing registries." These provide a standardized way to publish information about the routes they announce, which allows other ISPs to use that information when determining which routes to accept from another peer.

Additionally, there is a problem known as route flapping that can increase load on core routers and prevent routers from converging, or agreeing on the current state of the routing table. This occurs when a router continuously advertises a network as available and then unavailable, or via one route then another. There are ways of containing the effects of route flapping, such as BGP dampening.

As the internet grows larger, the increased size of the global routing table is also becoming a concern. While most BGP routers do not have a complete copy of the global routing table, some have a large portion of it. There are now enough routes to fill up the ternary content-addressable memory (TCAM) of some networking hardware, which is memory used to speed up routing table lookups; these devices now need to use ordinary RAM, which is significantly slower.

2 Project Summary

The ultimate goal of this project is to gain an understanding of how BGP works and what its current problems are. I plan to conduct a thorough literature review on the topic of BGP operation and common issues such as route flapping and BGP security. I plan to use Riverbed Modeler Academic Edition (MAE) to illustrate identified phenomena in BGP networks. MAE is powerful network simulation software which allows modeling various networks with a multitude of configurations, including BGP. I plan to use MAE to reproduce and analyze BGP issues commonly seen in large-scale networks such as the Internet. Additionally, MAE includes several sample BGP network models which would be a starting point for my study of BGP configuration in Modeler software.

I plan to create a model of a BGP network where one or more such issues as link failure, route flapping, traffic hijacking and/or rerouting are occurring. I hope that such a simulation study will provide me with an additional insight into BGP operation and its issues. I plan to report my finding in the summary paper which will describe my endeavors studying BGP protocol.

3 Limitations

Implementing solutions to studied BGP problems is outside the scope of this project. Additionally, Modeler Academic Edition may not support all of the features of BGP, which may prevent me from modeling all desired BGP phenomena.