Jonathan Frederickson
BGP Design

Background

Every device on the Internet must have an IP address to communicate on the network. Within a local network, addresses are distributed using DHCP or static IP configuration. In the backbone of the Internet, however, a more complex protocol is used – BGP.

When an organization purchases address space from a regional authority, they need to advertise it from their routers for other Internet users to be able to reach addresses in their range. This is done using BGP. Full BGP nodes (without a default route) maintain nearly complete copies of the Internet routing table. Entries in this table contain what is known as an AS Path, which looks something like: AS1001-AS2345-AS2345-AS12437-AS8888

Each number in the path is an AS that must be traversed to reach the advertised address space. When new routes are advertised, a BGP node sends out an UPDATE message, causing the node's direct peers to update their routing tables with the new information. Those peers then send the updated information to their peers, and so on. Due to this, it takes some time for new route information to propagate across the entire network; once all nodes agree on the current state of the routing table, BGP is said to have converged.

This process can potentially cause problems if there is a faulty link between a router advertising a range and the rest of the network. When the link comes up, it will advertise its routes to its direct peers. When it goes down, its peers will notice this and notify the rest of the network that these routes are no longer unavailable. If this happens multiple times in rapid succession, however, nodes in the network will constantly be updating and will not converge. This is an issue known as route flapping.

Experiment Design

Riverbed Modeler Academic Edition includes sample BGP networks that I will modify to meet my needs. By advertising routes and disconnecting rapidly in the simulated BGP network, I will attempt to induce route flapping in the network. Riverbed Modeler allows events to be started at specific times during the simulation, which will facilitate demonstration of this issue.

As BGP does not have authentication for route updates, it is possible for a malicious peer to advertise address space that they do not own, causing routing issues for the legitimate user of that space. I will be attempting to model this in Riverbed Modeler as well. However, due to the limitations of the Academic Edition of Riverbed Modeler, it may not be possible to do this, as doing so requires one peer to be configured incorrectly.

Riverbed Modeler Academic Edition supports simulation of the BGP protocol, however the simulation itself is opaque; in full editions of Modeler, it is possible to view and edit the protocol state machine, but in Academic Edition it is not. However, it does allow limited control of the simulated routers through a Cisco-like syntax. This will mostly restrict my simulation of events in the BGP network to those that were preconfigured in Riverbed Modeler, though I will have limited control of the simulation during runtime.

References

- http://faculty.kfupm.edu.sa/coe/ashraf/RichFilesTeaching/COE081_540/BPG_OPNET/Studienarbeit.pdf
- Opnet Modeler/Release 17.5 User Manual - BGP