**Twisting Traffic with Border Gateway Protocol - Part 1**

**What is Traffic Engineering?**

Well, imagine having your own Enterprise and connecting it to internet. To do so you will need to get connection from an ISP. Now that the basic requirements are met you would be able to connect to the internet and the rest of the internet would be able to connect to you. As your enterprise scales you would need to look into other aspects other than basic connectivity, like redundancy, availability etc. When such requirements come into play, the options available are,

* Dual Homing
* Multihoming
* Dual Multihoming

In all of the above schemes what you have is two or more links exiting your AS, Now that you have redundant links you would want to be able to make use of it in the best way possible, especially in the case of Multihoming where you have separate connections to two different ISP’s. BGP comes with ways that you can use to manipulate traffic being sent across these links according to your need and wish and the process of doing this is called Traffic engineering.

**Why is Traffic engineering Important in Internet?**

In a WAN network like the internet, that scales throughout the world, with routers all around that are not under the control of a single authority, the shortest path does not always mean the best path. There are a variety of factors like latency, bandwidth, packet loss that determine what is best. Depending on the application needs, the definition of “best path” can change. Since, routing protocols does not take into consideration these network performance aspects and aim at connectivity they can sometimes mislead you. Well BGP also is a routing protocol and does not help you in knowing about the performance of the network. However, the trick is that if the user can somehow know about these performance factors beforehand when connecting to certain destinations, he/she could then use the BGP attributes to engineer traffic across a different link.

**How does BGP make Traffic engineering possible?**

The one-word answer is attributes. The internet is an interconnection of many networks around the world. For example, consider that for some reason you want to tell a packet to take a path to reach the destination. Due to the nature of IP forwarding this is not possible as IP forwarding is a hop by hop mode of transmission. So how can you then possibly make the IP packet to choose a predetermined path to destination. The answer is if you could somehow know the path before you send out the packet you could make use of it. This is where BGP helps you to get information regarding the paths to reach a network. This is one of the critical points on how traffic engineering can be accomplished. Attributes are the lifeline of BGP and is what helps in decision making and with Traffic engineering.

Note: BGP does not eliminate the IP forwarding hop by hop nature and provides path only with respect to Autonomous system.

**Engineering the Outgoing Traffic:**

Attribute manipulations in BGP are done using route polices and can be done on a per neighbour basis.

The Enterprise that we imagined at the start of the document is connected to two ISP1 and ISP2 and in a Dual multihomed setup as shown below. Assume R1 connected links is the primary path that all high priority business traffic(70.1.1.0/24) should take, and the links connected to R2 are a backup link with low bandwidth that some low priority enterprise traffic can exit and the way that you have done to establish this is through load balancing on R3 using BGP multipath(60.1.1.0/24 and 60.1.2.0/24).

We see that R1 itself being the primary exit is connected to two ISP’s (ISP 1 and ISP 2). Consider that link to ISP1 is a higher delay link than ISP2(lower delay link) and even though path through ISP1 is shorter, imagine you want to switch some traffic (70.1.1.0/24) that is delay sensitive through ISP2.

When BGP runs on its own with its own election rules. We see that all traffic exits through R1 through the link connected to ISP1 since it is shorter AS path and elected.

Now to fit in our above requirement and manipulate BGP to engineer traffic let us see how we use the below ways to do so.

1. Setting Local preference:
2. Manipulating AS-Path
3. Using Communities

**A diagram of a network

AI-generated content may be incorrect.**

**Setting Local preference:**

At R1 set the local preference of route 70.1.1.0/24 is set as 130 for neighbour ISP2.

This makes the route to R1 in R3 preferred rather than a multipath route as in the BGP election process Local\_Pref is considered before AS-path. In R1 even though for the 70.1.1.0/24 network, path through ISP1 has shorter AS path, path through ISP2 is preferred as we modified the local\_prefrence against the route received from ISP2.

To take advantage of Local path attribute in an Enterprise scenario an Enterprise should have a Dual Multihomed topology with IBGP running inside, otherwise you could use the weight metric to easily establish this.

**Manipulating AS-Path:**

AS-path is another way to achieve the same mentioned above. This method is mostly preferred for Stub AS like an Enterprise connecting to the internet.

For example, instead of modifying the Local pref on 70.1.1.0/24, you could prepend an additional two AS’s on to 70.1.1.0/24 received from ISP1. Now 70.1.1.0/24 from ISP2 would have a shorter As-path and would be selected.

However, unlike the Local\_pref attribute this prepended AS\_path when propagated inside the IBGP network will not result in getting the traffic towards R1 as the route from R2 would have a shorter AS-path and be preferred. Hence this technique should be used with care and is often most useful in a multihomed scenario without IBGP running inside enterprise.

AS-path can also be used if you wish that your traffic should not go through an AS, you could achieve it by matching the as path in the incoming route and you could choose to drop them.

**Using Communities:**

Communities can tell more about the route and differs a bit from the above two cases like using the Local preference and AS path.

When using communities, both ISP and the enterprise should work hand in hand and only modifying the settings at the Enterprise alone like the above two methods will not work. For example, the ISP’s can give different communities (or rather colour) to the route based on origination, from a geographical perspective like a city or country.

The enterprise could use this information as a tag and chose to deny the route or engineer traffic on a particular link.

This method of marking a route with community is often referred to as colouring.

Note: The article assumes that the reader has an average knowledge of the BGP protocol.

**References:**

1.Building Reliable networks with Border Gateway Protocol (by Beijnum Iljitsch Van).

2.Interdomain traffic engineering with BGP, <https://inl.info.ucl.ac.be/system/files/commag-may2003.pdf>

3. Traffic Engineering with BGP, <https://www.net.t-labs.tu-berlin.de/teaching/ss09/IR_seminar/talks/traffic_engineering_ludwig.handout.pdf>