Analysis of Influence AS Path Prepending to the Instability of BGP Routing Protocol.

Hirwandi Agusnam[1], Rendy Munadi[2], Istikmal[3]

[1,2,3,]School of Electical Engineering, Telkom University

Jl. Telekomunikasi Terusan Buah Batu Bandung 40257 Indonesia (+6222) 7564 108

* Corresponding author's Email: hirwandiagusnam@gmail.com

Abstract: Border Gateway Protocol (BGP) is a routing protocol used on the Internet to create end-to-end routes across Autonomous Systems (AS) often facing instability issues related to policy patterns implemented in an ISP. BGP routing instability that occurs due to misconfiguration. By performing several AS modifications by multiple ISPs that operate multiple AS for business purposes, ISPs can control the proposed routing and are added in BGP.

Customer and ISP relationships occur multi-homed. If the implementation of inbound traffic engineering in the form of AS path prepending with policy pattern applied together between customer and ISP, it will affect BGP instability. By using the route dampening method approach in addition to discussions and further coordination of information exchange and route negotiations between upstream routers - downstream routers, it is expected that policy differences do not cause conflicts that result in BGP instability.

In this research, the influence of AS path prepending on BGP routing instability is analysed by looking at increasing CPU load. Total consumption of inter AS resources that occur on the internet is greater and needs to be monitored the bandwidth conditions that occur. Increased bandwidth consumption causes report changes on BGP speakers. In addition, trial-and-error using greedy algorithm can predict changes in traffic distribution. The greedy algorithm approach in a systematic and efficient will be obtained to see load balanced conditions that occur. Load balance levels will affect the loading of traffic that plays a role in network stability.

Keywords: Instability BGP, Autonomous System, Policy routing, Prefix, AS path prepending

I. INTRODUCTION

Routing instability refers to the rapid changes of a range of an information network and topology, and results in large quantities of a routing update which is passed to the core Internet router. Fellow border router is limited on any exchange the range of information autonomous system to the destination IP address block using the Border Gateway Protocol (BGP).

Instability of routing BGP due to the result of various types of interruptions such as hardware failures, misconfiguration, attacks by spammers, software bugs, device malfunctions, and policy conflicts. Instability affects performance, CPU load, and balance of traffic load distribution for BGP speakers.

One of the misconfiguration that occurs is on the use of AS path prepending. The use of AS path prepending which is one of the ways to control inbound traffic distribution with inbound traffic engineering can lead to BGP routing instability problem. There are three popular BGP-based approaches for inbound inter-AS traffic engineering: selective advertisement (SA), specific prefix advertisement (SPA), and AS path prepending (ASPP) [1]. Unlike SA and SPA approaches, AS path prepending does not introduce longer prefixes, and at the same time takes advantage of the resiliency protection from multi-homed connections. Although ASPP has been practiced on the Internet for a long time, there has been no systematic study of the phenomenon and the performance of this method. In addition, based on the BGP routing table of routers connected to the AT & T backbone, it was reported that more than 30% of routes have a number of ASPPs and this indicates that ASPP has a significant impact on the current Internet routing structure [2].

II. LITERATURE REVIEW AND SUPPORTING THEORY

A. Unstable Routing

Instability of routing, which is defined informally as a rapidly changing network range and topology information, has a number of sources including router configuration errors, data link problems and transient physical, and software bugs. Instability, also called a "route flap", significantly contributes to poor end-to-end network performance and decreases the overall efficiency of the Internet infrastructure. All these sources of network instability result in a large number of routing updates

being traversed to the Internet core exchange core router. Network instability can spread from router to router and spread throughout the network. At the extreme, the route flap has caused a temporary loss of connectivity for most of the Internet. Overall, instability has three main effects: increased packet loss, delay in time for network convergence, and additional overhead resources heard (memory, CPU, etc.) in the Internet infrastructure [3].

The routing information shared between peers in BGP has two forms: announcement and withdrawal. Announcement of a route indicates that the router has noticed a new network attachment or has made a policy decision to choose another route to the network destination. The route withdrawal is sent when the router makes a new local decision that the network cannot be reached again. There is a distinction between explicit and implicit withdrawal. Explicit withdrawals are matters related to withdrawal messages; whereas an implicit withdrawal occurs when an existing route is replaced with a new route announcement to the destination prefix without interfering withdrawal messages. BGP updates contain multiple route announcement and withdrawal. In an optimal and stable wide area network, routers should only generate routing updates for relatively rare policy changes and the addition of new physical networks.

The flexibility of BGP, coupled with the fact that network administrators BGP in many ways means it is often difficult to determine the cause of routing [5]. Because BGP propagate changes to the best path, one router may send multiple updates based on one trigger event [6]. Furthermore, the propagation of a single update may cause an increase that is caused in other locations [7]. It is even possible that potential policy conflicts may interfere with the entire Internet [8]

Establishing and maintaining route stability within and between networks is critical to maintaining reliable connectivity. Related to the policy made by the provider in this research to overcome the problem of BGP stability with stable BGP configuration deployment. The expected result of this research can overcome the problem of fluctuating network topology by implementing BGP update message processing filtering.

The problem of unstoppable BGP routing instability will have an impact on the router's heavy CPU load as the message process results in higher queue delay of data packets. If the delay is severe enough then Keep - Alive packets are affected so that the performance of the router according to which leads a large number of BGP messages result in the internet getting slower.

AS path prepending is another approach used in policy practice to influence inbound traffic. This approach artificially inflates the AS path by including multiple of its own AS numbers. Since a common criterion for selecting an inter-AS route is based on the shortest AS path length, a sufficient of the AS path will change the routing path [4].

B. Instability of Routing Due to AS Path Prepending

AS Path Prepending is increasing artificial length of AS path. BGP AS path prepending is used to influence inbound traffic to the customer. Outbound traffic is usually done via the BGP local preference attribute. By using inbound traffic engineering, AS use of path prepending is useful as a backup link as the Figure 1.

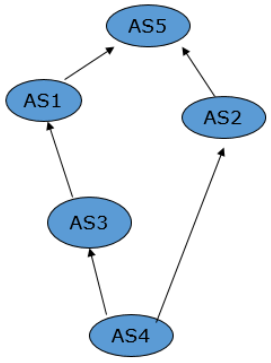

Figure 1. AS path prepending

The criterion for evaluating path-prepending on the Internet is prepending the AS frequency. Different AS have different prepending frequencies. Some AS always add their local ASNs when announcing to the AS neighbor for different reasons such as the use of "back up" lines. AS typically has a 100% prepending frequency while most AS do not use path prepending. It is also possible that AS adds its ASN to a BGP session while not doing this with the others.

BGP AS path prepending is used in active-standby link scenarios. If there are two BGP neighbor ship where the prefix will be advertised, one link for the prefix set or maybe all prefixes can be used as a backup and the way to achieve this setting is to use BGP AS path prepending.

Here, traffic from AS5 to AS4 follows this AS5-AS2-AS4 path. If AS4 wants to redirect traffic to AS3-AS4 links, it sends a route to AS2 in the following way: (Prefix, AS4, (AS4, AS4, AS4)). So AS5 chose another way because according to him AS2-AS4-AS4-AS4 is longer than AS1-AS3-AS4 and AS5 with AS2-AS4 route used as link back up. This is called AS4 prepend link AS2-AS4 twice (or two). For the record: prepending is directional, AS2 can add AS4-AS2 link.

BGP can be used to influence path choice in other AS. There are several reasons why BGP chooses paths that are not the best route that is easy to achieve, for example to

avoid some kind of transit traffic passing through the AS or perhaps to avoid very slow or dense links.

BGP allows AS to independently determine its routing policy based on local and local information with little or no global coordination, so BGP is not secure in the sense that routing policies can lead to conflict and result in persistent and instability-generating flap routines like the simple example seen in Figure 2

At time1, the Internet is stable. In time slot 1, AS1 finds link1 has heavy traffic and prepending link is very helpful to get a stable link. This prepending affects the entire Internet. After some time, at time2, the Internet becomes stable. But AS2 found its traffic is not symmetrical. So AS2 does prepending. AS2 also affects AS1, then at time slot 3, AS1 prepending again. If every AS feels nothing to do to get better results, then there is an emerging process called "converged".

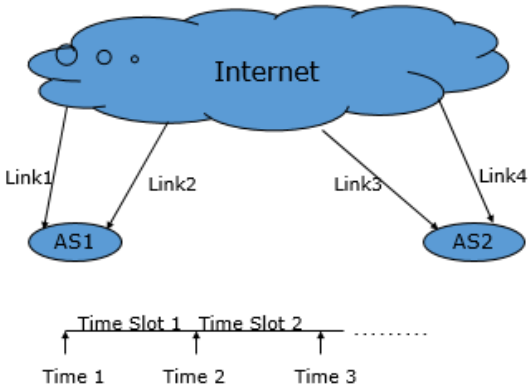

Figure 2. The connection of routing instability due to AS prepending AS path prepending

III. DISAIN AND SCENARIO

A. Policy Modeling on BGP Routing Instability

As a demonstration of the influence of AS path prepending can lead to instability of BGP routing resulting in increased CPU load. Figure 3 shows an interaction between the customer and the ISP. BGP is a policy-based routing protocol for controlling packet traffic based on attributes. Use of attributes such as AS path prepending that is incompatible with local objectives and local information with little or no global coordination can lead to conflicting routing policies and result in persistent routing oscillation.

In network, both AS1 and AS3 are multihoming. For AS1, AS2 can be a more expensive link than AS3, so AS1 wants to link (AS2 → AS1) as backup by using AS path prepending approach. As for the link (AS4 → AS3) used as backup is AS3.

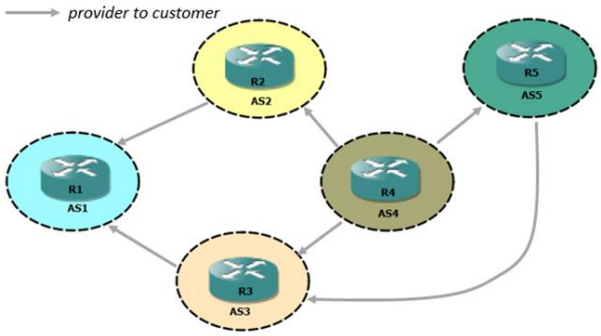

Figure 3. A network showing AS1 and AS3 interactions

In this case, the AS1 prepending policy will raise the prepending length of the link (AS2 → AS1) until no traffic can be diverted to another link, while the AS3 prepending policy will raise the prepending length of the link (AS4 → AS3) until no traffic is can be diverted to other links. In this case there are two local policies satisfactory at the same time without causing conflict.

Furthermore, traffic from AS4 to AS1 passes (AS4, AS5, AS3, AS1). After AS1 and AS3 get the required prepending configuration and run prepending, then the network becomes stable. The local policy of the AS is in the network not to cause conflict.

The prepending action scattered under multiple AS policy conflicts AS can interfere with each other and make the routing unstable because there is no coordination. AS1 assumes the network wants to avoid traffic via AS2 (Figure 4) on the basis of competition and performance. Then AS1 independently prepend (AS2, AS1) directly create the link (AS2 → AS1) as backup. Besides AS1 also ask AS3 provider prepend route prefix AS1 to send to AS2. So the AS1 prepending policy is direct and indirect until no traffic can be diverted, while the prepending policy of AS3 until no traffic on the link (AS4 → AS3) can be diverted. In this case the policy of prepending 2 ISPs (AS1 and AS3) causes conflict and routing becomes unstable.

AS1 customer and AS3 providers (Figure 4) then do AS path prepending to optimize their traffic distribution and can cause interference in the network. If then AS1 prepending makes its traffic distribution better, this will affect the distribution of AS3 traffic. As a result, then AS3 will triggered to create new prepending. But the new prepending of AS3 at the same time causes the change in traffic distribution of AS1 again and then finally AS1 forms a new prepending. Repeated and continuous processes introduce configuration changes prepending

without routing convergence to achieve stable route conditions.

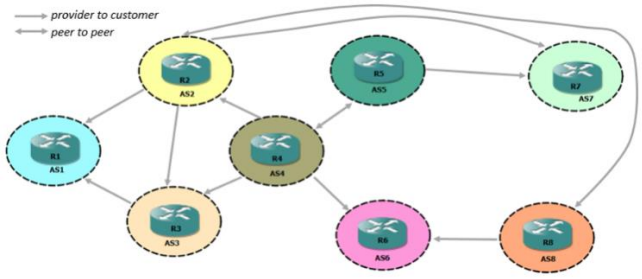

Figure 4. Interference of action prepending by AS1 and AS3

The act of prepending distributed under conflicting policies from different ASes can disrupt each other's AS and make the routing unstable because there is no global coordination. From figure 4, assuming the bandwidth of all links in network is the same, and $c_e = 100 (e \in E)$ then AS1 and AS3 are prepending for inbound load balances on link provider using Greedy AS path prepending Search Algorithm. The load balance rate $f(t(p))$ is measured by the equation:

$$f(t(p)) = \frac{(\sum_{e \in E(v)} t_e / c_e)^2}{|E(v)| \sum_{e \in E(v)} (t_e / c_e)^2} \quad (1)$$

where

e *link logical* between two AS
v the total number of AS
$E(v)$ link that connects AS_v
t traffic intensity
t_e traffic intensity *link* e
c_e bandwidth link e
$t(p)$ current traffic distribution
$t(p')$ new traffic distribution
p current AS path prepending configuration
p' new AS path prepending configuration

For value $f(t(p)) \in (0,1)$, where when $f(t(p))$ close to 0, it means loading traffic at $E(v)$ very skewed. When $f(t(p))$ close to 1, it means loading the traffic at $E(v)$ close to balance.

Using Greedy AS path prepending Search Algorithm can predict changes in the distribution of traffic for the desired AS path prepending configuration and impact on the network. Below is Greedy AS path prepending Search Algorithm:

```
1. while ( TRUE ) {
2. compute f(t(p));
3. let e be the link with most room to add traffic according
   to the desired distribution;
4. if (the prepending length on e > 0) {
5.     p' = p - e;
6.     if f(t(p')) > f(t(p)) {
7.         p = p - e;
8.         continue;
9.     }
10.}
11. let e be the link with most room to reduce traffic
    according to the desired distribution;
12. p'' = p + e;
13. if f(t(p'')) > f(t(p)) {
14.     p = p + e;
15.     continue;
16.}
17. break;
18.}
```

AS6 and AS7 are source prefixes from AS 1 and AS3. As can be seen in table 1, the traffic request can be represented by matrix to specify the traffic intensity from AS6 to AS1 and AS3, and AS7 to AS1 and AS3. The traffic intensity is measured by the equation:

$$t = \frac{aL}{R} \quad (2)$$

where a average *packets rate* coming (*packet per second*)

L average packet length (bits)
R transmission rate (bits per second)

To get the intensity of AS1 and AS3 traffic using formula (2). The result of traffic intensity is in table 1. From the table can be made in the form of matrix $\begin{pmatrix} 20 & 30 \\ 10 & 80 \end{pmatrix}$.

Table 1. Traffic matrix

Traffic Intensity	AS1	AS3
AS6	20	30
AS7	10	80

Taking into account the matrix $T = \begin{pmatrix} 20 & 30 \\ 10 & 80 \end{pmatrix}$ which is the translation of the matrix traffic from table 1 is used to predict the demand for traffic. When there is no prepending in the network, traffic from AS6 to AS1 passes through three paths (AS6, AS4, AS2, AS1), (AS6, AS4,

AS3, AS1). Traffic from AS7 to AS1 passes (AS7, AS2, AS1). So $t_{(2,1)}=\frac{2}{3}*20+10=23.33$. Because AS1 has two links provide, it intuitively chooses a 2: 3 traffic ratio better than a 1: 4 traffic ratio.

In Table 2 shows detailed information about prepending action interference by AS1 and AS3. The first column shows a prepending change based on the Greedy ASPP Search Algorithm. For example, $(2,3)^1$ showing that AS3 decides to increase the length of prepending on links AS2 → AS3 by 1, and $(2,3)^{-1}$ decides to reduce the length of prepending on links AS2→AS3 by 1. This as can be found from the table is the prepending action of AS3 and AS1 interrupt each other's. In this case, the action of prepending on links (AS2, AS3) and (AS2, AS1) that affect each other brings the network back to the original routing and oscillation occurs. There is no solution for both ASes to balance their load at the same time for reasons of instability, which means both ASes have conflicting prepending requirements.

Table 2. Instability of routing is caused by the interference

#Link Prepending	AS1			AS3			AS2	Results
	$t_{(3,1)}$	$t_{(2,1)}$	$f(AS1)$	$t_{(2,3)}$	$t_{(4,3)}$	$f(AS3)$	$t_{(4,2)}$	
ϕ	6.67	23.23	0.76	80	36.67	0.88	6.67	Not done prepending
$(2, 3)^1$	6.67	23.23	0.76	40	76.67	0.91	6.67	AS1 did not get any results. AS3 found that $(2, 3)^1$ could fix its local metric
$(2, 1)^1$	20	10	0.90	40	90	0.87	0.00	AS1 found that $(2, 1)^1$ could fix its local metric. AS3 did not get any results.
$(2, 3)^{-1}$	25	5	0.69	85	50	0.93	0.00	AS1 did not get any results. AS3 finds banlwa $(2, 3)^{-1}$ can fix its local metric
$(2, 1)^{-1}$	6.67	23.23	0.76	80	36.67	0.88	6.67	AS1 found that $(2, 1)^{-1}$ could fix its local metric. AS3 did not get any results.
Returns to original condition ==> oscillation								

With each AS1 and AS3 party assumed to have known the policies that have been implemented, and each party can only benefit by changing its own policies. If there is no mechanism to stop it, where none of them stop prepending to find the best route for AS1 and AS3 that will result in oscillation and the network cannot reach a stable routing condition. After the prepending operation is done, if not obtained $f(AS1)=1$ and $f(AS3)=1$ that means both links are not balanced so that if still done prepending, can cause instability BGP routing.

B. Influence of AS path prepending to link bandwidth and CPU utilization

AS path prepending is essentially a method of selectively adjusting the preference relationships between AS prepending and neighbors. AS path prepending can result in local and global impacts. Locally multi-homed AS can manage traffic that enters links from different providers based on various factors such as price and available capacity. Thus, local AS can do traffic engineering efficiently. Globally, AS prepending can affect the best route chosen by the ASes, which indirectly controls which path the other ASes use to send traffic to itself. For example, AS prepending may affect other ASes for not selecting paths across a given AS. In addition, AS path prepending can increase the total amount of consumption of inter-AS resources on the Internet because traffic again follows the shortest AS path that resulted in increased CPU utilization.

After setting up the initial BGP connection, BGP peer exchanged a set of complete routing information. If the number of routes on the Internet as N, the total path attribute (for all routes N) is received from peer as A, and assumes that the network is distributed evenly between autonomous systems (AS), then the worst-case of bandwidth consumed during the initial exchange between a pair of BGP speakers (P) are:

$$BW=(N+A)*P \qquad (3)$$

When incremental attributes of AS path prepending make the path selection long, bandwidth usage increases. AS path prepending using BGP path vector requires BGP advertisement to prepend repeatedly. A rise in the AS path length increases the number of specific prefix routes affecting the best route selection in the AS upstream. BGP peer receives packets and sends TCP acknowledgment (ACK) to advertise BGP speakers. If the ACK arrives at an exorbitant level for the route processor, the packet returns to the inbound interface queue. BGP speakers receive changes related to the announcement and withdrawal of each ip prefix destination to the neighboring speaker. Increased bandwidth consumption causes report changes on BGP speakers.

The use of AS path prepending in addition may lead to an increase in bandwidth consumption (from equation 3), it can also lead to an increase in CPU utilization. An important and fundamental feature of BGP is that BGP CPU usage depends only on its BGP-related network stability in terms of announcement of BGP update messages. If the BGP network is stable, all BGP routers in the network are in a stable state.

During times of network instability, BGP routers in the network generate routing updates that are exchanged using BGP update messages. The largest load per update message occurs when each update message contains only a single network (single prefix). Routing changes show locality with route attributes. That is, the changed routes tend to have shared route attributes. Some networks can be

grouped into one single update message, thereby significantly reducing the amount of bandwidth required.

Because in a stable state, the link bandwidth and router CPU cycles consumed by the BGP protocol depend only on the stability of the Internet, but are completely independent of the number of networks that make up the Internet, BGP should have no scaling problems in the area of link bandwidth and CPU usage of the router, as the growth of the Internet, provided that the overall stability of AS interconnectivity from the Internet can be controlled.

C. The influence of Load Balance and CPU Load relationships

The factors that can affect the load balance is the size of the bandwidth. As mentioned in (1) $f(t(p)) = \frac{(\sum_{e \in E(v)} t_e / c_e)^2}{|E(v)| \sum_{e \in E(v)} (t_e / c_e)^2}$, the load balance level $f(t(p))$ is an index to measure the feasibility of bandwidth allocation. The value of the feasibility index $f(t(p))$ can be achieved from the comparison of traffic intensity t_e and the bandwidth link e i.e. c_e .

This value can affect bandwidth consumption by paying attention to equation 3 because of the use of AS path prepending. The main impact usage of AS path prepending is the increase in CPU utilization. When the router runs the BGP protocol as a BGP speaker in choosing the shortest path of the AS path, it updates the BGP routing. For every BGP routing update received by the router, there are a few things to do. First, the appropriate RIB-in (routing information base) needs to be updated. Ingress filtering, as defined in the router configuration, should be applied to the route announcement. If not filtered, the route encounters BGP route selection rules and is compared with other routes. If selected, it will be added to the BGP routing table and the corresponding forwarding table entry will be updated. Egress filtering then needs to be applied to every peer BGP (except that sends the original announcement). New BGP Announcement needs to be created and then added to the appropriate RIB-out queue. Such routing update activity of BGP could increase the load on the router CPU. There is a correlation between BGP routing updates and CPU utilization. A number of BGP update message announcements received in the given time period increase the router's load CPU. Each update requires some processing for in-filtering and out-filtering routes, route selection, routing information base (RIB) and forwarding information base (FIB) updates.

Long-term high-use router CPU is not desirable for two main reasons. High utilization potentially increases the amount of time the router spends to process routing changes, increasing the time of the convergence of routes. High route convergence times can lead to packet loss by increasing the window of time where a route for a particular destination is not available. High router CPU utilization can interfere with tasks such as other protocol processing, keep alive message processing and in extreme cases, can cause the router to crash.

As an illustration of equation 3, it appears that when a BGP router requires the process of all BGP updates for all destinations of all BGP peer. Potential addition of CPU load increases very rapidly as the number of services and the frequency of BGP update messages increases as well and eventually bandwidth consumption also increases.

D. Topology and Simulation Scenario

The simulation scenario in this research is to build a network topology of BGP design that uses AS path prepending that causes BGP routing instability.

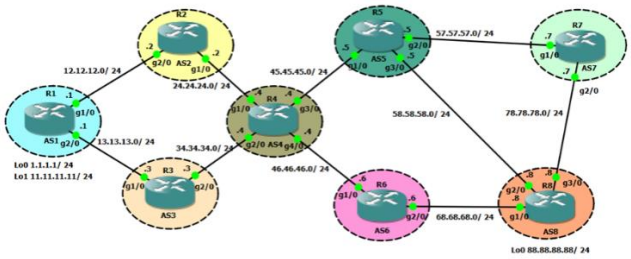

Figure 5. Topology scenario simulation AS path prepending

Since the incoming traffic control used in AS path prepending is more difficult than outbound traffic, it is necessary to be careful in doing the tuning of advertisement sent by AS because AS cannot control the routing decisions of other connected AS. Therefore, in this experiment will be a trial-and-error approach due to the limited internet topology information and routing policies used by remote AS.

Based on the topology in Figure 5, there are several steps performed as follows:

1. Perform the BGP configuration on the eight routers.
2. Checking R8 and checking the path skipped to R1.
3. Check the IP-BGP path in R1 and explain the result.
4. Change the original path from R8 to R1 via R2, now replaced from R8 via R3 using AS path prepending by adding route map filtering

configuration in R1 to peering neighbor ship to R2.

5. Check R8 and check the path skipped to R1.
6. Perform ping test to know the latency and packet loss.
7. Check the CPU utilization on R1.

Flow Chart

To look for routing instability due to the implementation of AS path prepending that influences the BGP routing decision using algorithms by creating the following procedure:

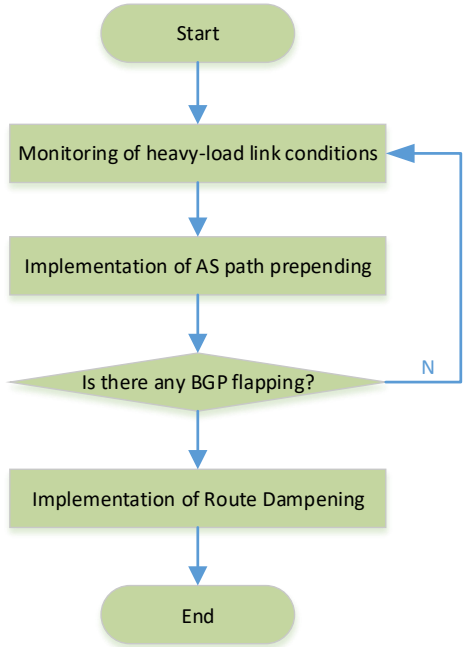

Figure 6. Flow chart Simulation

IV RESULT AND ANALYSIS

A. Simulation Results

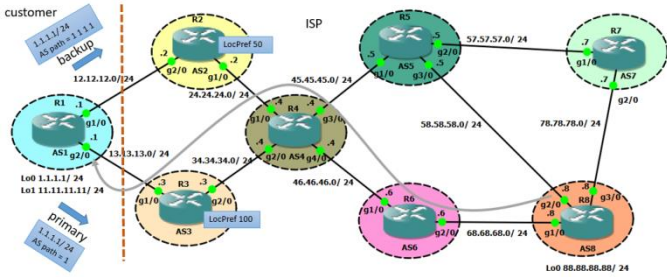

Figure 7. BGP instability topology scenario

Before Implementation of Path Prepending

From Figure 7, it appears that a customer / enterprise has AS1 connected multi - homed. With multi-homed design such, customer / enterprise (AS1) want to create redundancy and backup if the primary link obtained lower quality, as well as low speed internet available as well.

As for good ISP (AS2 and AS3) side will help customer with solution inject attribute BGP local preference in the customer network and provide guidance to the customer against the use of BGP local preference through BGP communities. If the route received directly from the customer has a low local preference (default Loc Pref 100 for primary and Loc Pref 50 for backup), all routes will be skipped, generating the desired traffic flow i.e. avoiding the backup links path.

Often customers are forced to follow less than ideal conditions for ISP services provided because they do not know the internet topology of the two ISPs (AS2 and AS3) where the BGP local preference solution is not working. To overcome this problem by making the effect of BGP route selection in the internet is to extend the AS path attribute. Assuming that the shorter route is chosen AS path by creating multiple copies of AS customer / enterprise (AS1) i.e. as AS path prepending. AS path prepending is configured in CISCO IOS with route-map based on each neighbor outbound filter.

From figure 7, AS1 customer wants one of the available links as a backup. Prefix 1.1.1.1/24 is sent via bac k up link with 3 prepend. AS paths viewed through backup links as upstream ISP that AS1 has path 1 1 1 1. Each BGP neighbor from ISP (AS8) see only AS1 without AS path prepend, because internal BGP speaker choose best path and the best path will be sent to neighbor BGP ISP. Internal BGP speaker receives the prefix of the primary path as BGP AS1, from the AS 1 1 1 1 backups as prepended, so the internal BGP speaker selects a shorter AS path and uses it. Further below is a complete description of the AS configuration the path prepending created.

The initial step needs to be done by checking R8 and see how it gets to R 1.

```
R8#traceroute 1.1.1.1 so
R8#traceroute 1.1.1.1 source 88.88.88.88
Type escape sequence to abort.
Tracing the route to 1.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
  1 68.68.68.6 720 msec 240 msec 116 msec
  2 46.46.46.4 452 msec 256 msec 532 msec
  3 34.34.34.3 752 msec 816 msec 1124 msec
  4 13.13.13.1 924 msec 2024 msec 1916 msec
```

```
R8#sh ip bgp
BGP table version is 6, local router ID is 88.88.88.88
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *   1.1.1.0/24       78.78.78.7                             0 7 5 4 3 1 i
 *                    58.58.58.5                             0 5 4 3 1 i
 *>                   68.68.68.6                             0 6 4 3 1 i
 *   11.11.11.0/24    78.78.78.7                             0 7 5 4 2 1 i
 *                    58.58.58.5                             0 5 4 2 1 i
 *>                   68.68.68.6                             0 6 4 2 1 i
 *   44.44.44.0/24    78.78.78.7                             0 7 5 4 i
 *                    58.58.58.5                             0 5 4 i
 *>                   68.68.68.6                             0 6 4 i
 *>  88.88.88.0/24    0.0.0.0                  0         32768 i
```

It turns from R8 to R1 through R2. As expected, AS8 takes AS2 which is the shortest path based on BGP attributes. To take AS6, AS4, AS3 and AS1 need to configure AS prepending on R1 to R8.

```
R1

R1#sh run | s route-map
 neighbor 12.12.12.2 route-map ASPREPEND out
route-map ASPREPEND permit 10
 match ip address 9
 set as-path prepend 1 1 1
route-map ASPREPEND permit 20
```

Created 1 1 1 because it will be two lines of the AS to reach R1 from R8 is not until R2. To make AS path is longer and less desirable, need to implement the route map to peering neighbor ship between R1 and R2.

The reason for outbound direction because R1 advertise subnet. Then with the command " clear " BGP process in R1 to make changes and see the results that occur on the AS path in R8.

```
R8#sh ip bgp
BGP table version is 6, local router ID is 88.88.88.88
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *   1.1.1.0/24       78.78.78.7                             0 7 5 4 3 1 i
 *                    68.68.68.6                             0 6 4 3 1 i
 *>                   58.58.58.5                             0 5 4 3 1 i
 *   11.11.11.0/24    78.78.78.7                             0 7 5 4 2 1 i
 *                    68.68.68.6                             0 6 4 2 1 i
 *>                   58.58.58.5                             0 5 4 2 1 i
 *   44.44.44.0/24    78.78.78.7                             0 7 5 4 i
 *                    68.68.68.6                             0 6 4 i
 *>                   58.58.58.5                             0 5 4 i
 *>  88.88.88.0/24    0.0.0.0                  0         32768 i
```

Seen the difference now, by taking AS 5-4-3-1 for receiving advertisement from R4 about the best path. BGP only advertise the best path the network to neighbor. Since R4 is seeing AS path goes to R1 longer, it now takes AS3 to get to R1. Next look BGP table form after applying route map.

```
R2#sh ip bgp
BGP table version is 6, local router ID is 24.24.24.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  1.1.1.0/24       24.24.24.4                             0 4 3 1 i
 *                    12.12.12.1                             0 1 1 1 1 i
 *>  11.11.11.0/24    12.12.12.1               0             0 1 i
 *>  44.44.44.0/24    24.24.24.4               0             0 4 i
 *>  88.88.88.0/24    24.24.24.4                             0 4 5 8 i
```

Three " 1 " is added to AS path based on what is in the route map, so from the AS path, R4 will not directly go to R2 to R1 but will take R3 now. If desired traffic to 11.11.11.11 pass AS4 straight to AS3 from R8.

```
R1#sh run | s route-map
 neighbor 12.12.12.2 route-map ASPREPEND out
route-map ASPREPEND permit 10
 match ip address 9
 set as-path prepend 1 1 1
route-map ASPREPEND permit 20

R4#sh ip bgp
BGP table version is 6, local router ID is 44.44.44.44
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  1.1.1.0/24       34.34.34.3                             0 3 1 i
 *   11.11.11.0/24    34.34.34.3                             0 3 1 i
 *>                   24.24.24.2                             0 2 1 i
 *>  44.44.44.0/24    0.0.0.0                  0         32768 i
 *>  88.88.88.0/24    45.45.45.5                             0 5 8 i
 *                    46.46.46.6                             0 6 8 i
```

There is a difference using ACL. Now 1.1.1.1 in R2 has prepend but 11.11.11.11 has no prepend check on R8.

```
R8#sh ip bgp
BGP table version is 6, local router ID is 88.88.88.88
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *   1.1.1.0/24       78.78.78.7                             0 7 5 4 3 1 i
 *                    68.68.68.6                             0 6 4 3 1 i
 *>                   58.58.58.5                             0 5 4 3 1 i
 *   11.11.11.0/24    78.78.78.7                             0 7 5 4 2 1 i
 *                    68.68.68.6                             0 6 4 2 1 i
 *>                   58.58.58.5                             0 5 4 2 1 i
 *   44.44.44.0/24    78.78.78.7                             0 7 5 4 i
 *                    68.68.68.6                             0 6 4 i
 *>                   58.58.58.5                             0 5 4 i
 *>  88.88.88.0/24    0.0.0.0                  0         32768 i


R8#traceroute 11.11.11.1 so 88.88.88.88
Type escape sequence to abort.
Tracing the route to 11.11.11.1
VRF info: (vrf in name/id, vrf out name/id)
  1 58.58.58.5 160 msec 180 msec 240 msec
  2 45.45.45.4 460 msec 392 msec 856 msec
  3 24.24.24.2 528 msec 396 msec 372 msec
  4 12.12.12.1 744 msec 392 msec 520 msec
```

From R8 the traffic to 1.1.1.1 will pass through AS4 to AS3 but 11.11.11.11 it will go straight to R4 then R2 and R1.

After implementation of path prepending

As mentioned earlier, AS path prepending can be used by the ISP to control flow incoming traffic with announcing on some links (R2 int g2/0 and R3 int g1/0), see Figure 7. Prepending will modify the distribution path significantly to AS2 and make the path longer and provide the ability AS1 makes prepend to AS2 3 times.

When AS1 sends BGP community AS path prepending towards both links and expected instability, even though the BGP neighbor comes in a separate state. Does that make both link stop sending learn route (AS2) and put AS3 propagation from AS8, cause update prefix with change of AS path via AS3.

The process starts from instability of the flap route in routing table from one next hop to another. Flapping routes can be reduced by advertising the best external routes and avoiding unnecessary route withdraws. AS1 will shortly advertise to AS2 and AS3, but because it has not received the acknowledgment of AS1 happen flap. A potential flap that too often results intermittent in AS8 reaching 1.1.1.1/ 24. This increases the delay and high latency due to frequent routing updates.

B. Analysis of Simulation Results

In this experiment, it is done by recursive path prepend from not using path prepend until 7 times path prepend from 0 prepend to path prepend value 10 (see Table 3). There are two kinds of explanation of simulation analysis about the influence of path prepand to latency and packet loss as well CPU load.

Latency and Packet Loss

The following table shows the data latency and packet loss of some experiments with the AS path prepending value entered from zero (no prepend) to 10. The latency values vary and fluctuate with not so great differences so in this case for the implementation of AS path prepending from 1 to 10 is not so influential. This correlates with a very good packet loss value of 0% which causes the difference in latency is not so great.

Table 3 Latency and packet loss from implementation of AS path prepending

# AS Path Prepend	Latency (ms)	Packet Loss (%)
0	317	0
1	312	0
3	309	0
5	330	0.4
6	312	0
8	321	0
10	336	0

CPU Load

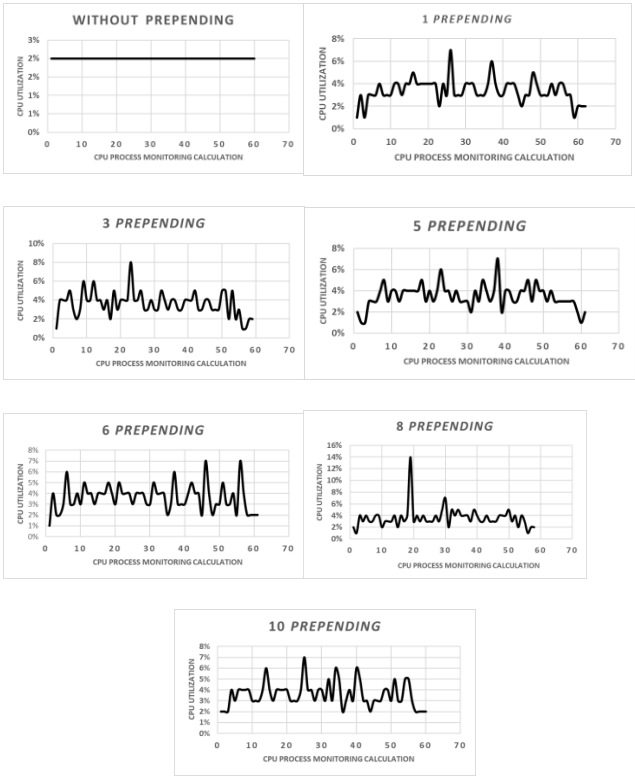

Figure 8. Utilization of CPU

For trial without path prepend seen that there has been no increase in latency and CPU load because the selected path is still by default where FIB can make it as best route.

When loaded with path prepend 1 it appears that the latency not much different when the condition is no prepend and no packet loss that happened. For the CPU load value there is a slight increase, but it does not cause a route change in the routing table R1. This means that after prepending to link int g2/0 router R2 (Figure 7), AS1 receives route advertisement from AS2 neighbor, then AS8 wants to choose a shorter AS path route so that the traffic needs to be forwarded to AS3.

If then prepending is raised to 10 there is no significant change and the R1 router is still stable. Instability has not happened because the performance condition of R1 router is still stable and the router is not experiencing BGP flapping. Routing is still running normally in accordance with the desired path.

Figure 9 shows the average total CPU utilization increase of 3.737%, largest when prepending 3 times and the smallest at prepending once.

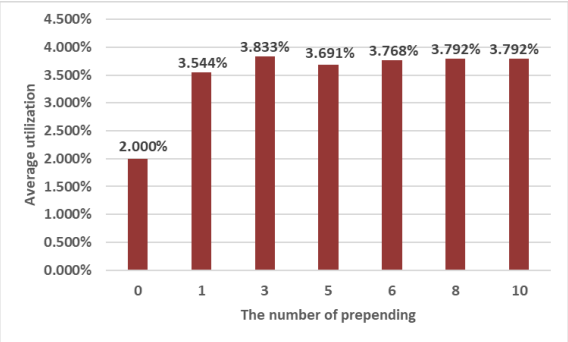

Figure 9. Average CPU Utilization.

C. Step by step AS Path Prepending Implementation

To make AS path prepending can be applied to all parties, in this case that need to be considered for customers and ISPs as follows:

1. Load Balancing:
   Prepending is done because ASes wants to balance the inbound load to meet capacity requirements.
2. Make a backup route:
   Some links only serve as a backup route. One AS may add a link to make the path a backup option for failover purposes.
3. Some AS must be multi homed and customers connect more than 1 physical link and more than 1 provider. Network to be prepending is a multi-homed incoming traffic.
4. Link AS path prepending which are made into multi homed not made as AS transit.
5. Before performing path prepending, observe and monitor CPU load router.
6. Monitoring stability in the network by evaluating the total change in traffic as well as the number of AS pairs affected by the change of routing path.
7. Coordinate between customer and ISP.

IV. Conclusions And Recommendation

A. Conclusion

AS path prepending can affect the performance of an ISP netwok such as an increase in CPU load so it needs to be maintained its implementation as it may affect ISP's routing policy. Although the increase in CPU load occurs about 3.5%, it shows that the effect of AS path prepending is used in several experiments involving many BGP speakers will affect bandwidth consumption and the majority of router CPU cycles are also increasing.

Technically AS path prepending can be applied as a load balanced and back up link with regard to CPU load condition parameters and does not make link path prepending as AS transit.The use of greedy algorithms can help to find ideal load balance performance that can detect possible instability of BGP routing.

Policy disagreements can cause conflicts affecting BGP routing instability due to improper use of policies between customers and ISPs. The creation of some simple policy-related matters as a guide for ISPs to do AS path prepending correctly to avoid instability issues.

The problem of BGP routing protocols is complexity, because the BGP protocol is used to exchange information together (Internet paths) between competing entities (service providers), and must apply what has been agreed upon in the peering interprovider agreement. This agreement often does not have much to do with optimal technical services

B. Recommendation

For recommendations that can be given is related to the use of AS path prepending is expected to have a discussion between custumer with ISP. Some ASes have more advanced mechanisms associated with the attributes used by ISPs to filter because of the non-conformity of paths through which the customer travels. Implementing the steps mentioned in IV. C is expected to eliminate the instability of BGP routing.

References

[1] B. Quoitin, et al, **"Interdomain traffic engineering with BGP,"** IEEE Commun. Mag., vol. 9, no. 3, pp. 280–292, May 2003.

[2] N. Feamster, J. Borkenhagen, and J. Rexford, **"Controlling the impact of BGP policy changes on IP traffic,"** AT&T Research, Tech. Rep. 011106-02, Nov. 2001.

[3] Craig Labovitz, G. Robert Malan and FarnamJahanian, "**Internet Routing Instability**" Published in: IEEE/ACM Transactions on Networking (1998)

[4] Rocky K. C. Chang, Michael Lo, "**Inbound Traffic Engineering for MultihomedASes Using AS Path Prepending"** Published in: Network Operations and Management Symposium, 2004.

[5] Griffin, T.G." **What is the Sound of One Route Flapping**" (2002)

[6]. Mao, Z.M., Bush, R., Griffin, T.G., Roughan, M. **"BGP Beacons**". In: Proc. ACM IMC. (2003)

[7] Feldmann, A., Maennel, O., Mao, M., Berger, A., Maggs, B. **"Locating Internet Routing Instabilities"**. In: Proc. ACM SIGCOMM. (2004).

[8]. Griffin, T.G., Huston, G. **"BGP Wedgies"** RFC 4264. (2005)