**Information on OSPF & BGP and compare with EIBP**

Invented in the 1980's Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) are one of the most widely implemented routing protocols. Due to heavy internet traffic, a component failure in a network is inescapable. OSPF uses Link state updates (LSU) and Link state acknowledgment (LSA) packets to share the routing information. BGP was the first protocol that addressed the issue of Classless Inter-Domain Routing (CIDR) which gave the flexibility of advertising the routing information over the public networks mitigating to some extent, the issue of uniquely available IP addresses. BGP uses UPDATE packets to share the same. These protocols broadcast a component failure all over the network topology using these update packets. So, in the case of wider areas that have over 1000's routers connected with each other, it would lead to an increase in packet overhead and delays the ongoing traffic. Our goal in this project is to address this issue by introducing Expedited Internet Bypass Protocol (EIBP) for communication within and between two Autonomous Systems. Throughout our entire report, we will discuss how EIBP stores the location of the routers and communicate various scenarios such as updating the routing table, deleting router information, and forwarding the messages between the autonomous systems. In the result section, we are going to compare the results of how OSPF responds to a link failure versus EIBP.

It has been observed that over the past decade internet users have increased by at least 10 percent every year with almost 5 billion users reported in January of 2022 alone. This increase in global penetration demands the continuous availability of unique public IP addresses, consistency in network connections, and security. The ever-changing network environments gave birth to “Dynamic routing protocols” that exchange routing information actively depending upon the addition, deletion or failure of a router. The two protocols we will be looking into are OSPF and BGP. Both routing protocols mainly differ with respect to how they detect other routers in the same area and what information they share when they are sharing the route information. Before we talk about OSPF and BGP we first need to know about Autonomous systems. The formal definition of an Autonomous system is "An Autonomous System (AS) is a collection of routers whose prefixes and routing policies are under common administrative control. This could be a network service provider, a large company, a university, a division of a company, or a group of companies".

OSPF is an open standard Interior gateway protocol meaning it is designed to be used within a single Autonomous System. OSPF learns the routes by learning about every router and subnet within the entire network, which results in all the routers having the same information about the network as the others. Routers configured to run OSPF learn the network information by sending out what's called Link-state advertisements (LSA), thus OSPF is also known as a Link state routing protocol. The LSA contains information about the subnets and the routers. To explain the workings of OSPF let us suppose there are 6 routers that have formed adjacency (read as neighbor relationship) with each other. If one link goes down the affected router will let all its neighboring routers (directly connected) know what just happened, then each router that receives this update will then tell all their neighbors. This would happen every time a change occurs thus increasing the network overhead by sharing Link state Updates (which contain LSA's) and LSA.

BGP on the other hand is an Exterior gateway protocol which means it is designed to exchange information between two Autonomous systems that can be separated over different ISPs (Internet service providers). BGP is a path vector protocol and was introduced to address the issue of routing loops that existed with some of the older protocols. However, the introduction of path vectors has made the issue of routing not just exponentially but factorially worse. Because BGP is guaranteed to provide path availability when a route goes down, it essentially means that while BGP chooses a primary route with a path length of for example 1 to exchange the information between ASs when that route is no longer available due to issues such as link failure between two BGP nodes it will choose the next best route which has let's say for example a path length of 2, and if that fails it will find the next best route and so on. Things get interesting when you get into thousands of ASs which are sharing major backbones with each other. The problem with BGP is that it explores every single path of every single length in the process of converging. Which mathematically means the upper bound on BGP convergence is factorial and factorial is a really big number.

The goal of EIBP (Extended Internet bypass protocol) is to work in conjunction with the existing Internet and its routing protocols. EIBP works in Layer 2.5 above Layer 2 and below Layer 3 independent of the protocols in the Data link and Network layer. To implement a small-scale EIBP for Intra-AS routing within an Autonomous System (AS) the routers in the AS will be arranged in three tiers namely: “first tier” would consist of the core router, “the second tier” will have distribution routers and the “third tier” will comprise of access routers. The core router will act as the backbone of this virtual structure with distribution routers separating the access domains and forming a bridge between the core routers and the access routers. Tier addresses are assigned by the higher tier router to the lower tier router. For example, as seen in figure 1 the core router CR1 has a tier address of 1.1, it assigns the distribution router tier address of “2.1:1” with ‘2’ being the tier value (TV) and ‘1:1’ can be explained with the notion ‘x:y’ where ‘x’ is the router ID of the core router and ‘y’ is the port number of the core router(CR1) through which the distribution router(DR1) is connected. Similarly, the access routers are assigned addresses by the distribution routers.

Our 3-tier core-distribution-access router structure in an AS connects to the access routers from the ISP's AS. Figure 1 displays the connectivity between the transit core routers and the ISP AS. The delivery of the packet from AS1 to IP2 in AS2 is conducted through the transit AS which receives the packet from the core router in AS1 and forwards it to the core router present in AS2 which delivers it to IP2. EIBP reels in the incoming IP packet, encapsulating them with an EIBP header that contains the address of the destination AR. The decision of the next forwarding is calculated by the source AS which compares the destination address and finds the address is different from the one that is on its network and thus chooses to forward it to the core router in Transit AS that is closest to the destination AR address. The core router then decapsulates the packet to deliver it to the ISP AS access router and using Intra-AS EIBP the packet is successfully delivered to the customer's core router in AS2.

Current routing protocols such as Open Shortest Path First are impacted significantly whenever there is a change in the routing topology and thus affect the network performance.  Routers in the networking environment update their routing table whenever there is a change in the link state of adjacent routers. The convergence when there is a change in the topology such as an interface or device failure. The change in the topology must be disseminated to all ASs participating in Inter-AS communications. The resulting operations cause high load and stress on the network components.

But EIBP is a novel approach to routing and forwarding. EIBP will reduce the convergence latency and the control overhead to stabilize the Inter-AS routing tables at the border gateways.

With the growing complexity of the internet, the interconnection between Autonomous systems, and the heavy internet traffic, it is necessary to explore innovative routing techniques for an efficient and cost-effective end-to-end service. One way to implement this is by controlling the packet overhead to achieve a minimum convergence time. EIBP will de-escalate the recovery time on interface link failures by several magnitudes and provide a means for simplified routing.

OSPF [3] is a great routing protocol, however, there is one major drawback. Once an OSPF network becomes colossal, the link state changes generate excessive LSAs and cause flooding within the whole area. The routers then must run the SPF using this new database. If the region size is ever expanding this leads to a higher network “Overhead” and the routers require more RAM to store the adjacency topology.