Title: On the mitigation and resolution of classic IXP model problems using SDN and OpenFlow: the first step towards SDX.
Proposer: Humberto Galiza
Author names and affiliations: Humberto Galiza (Rede Nacional de Ensino e Pesquisa – RNP), Jeronimo Bezerra and Julio Ibarra (Florida International University – FIU)
Keywords: SDN, SDX, IXP, Internet, Routing.
Speaker name: Humberto Galiza

Internet eXchange Points (IXP) are the natural successors of the four Network Access Points (NAP) responsible for interconnecting different networks in the early stages of today's Internet. The benefits achieved regarding performance, security, and costs, are the main reason for the key role that the IXPs plays in the present Internet ecosystem.

Although the dynamics of operation, criticality, and security aspects of an IXP are well-known and quite often under discussion in the network operator's community, only recently the scientific community began to delve into this subject. Notwithstanding the clear benefits and advances brought by large-scale IXP's deployments seen in a number of countries, the current model poses several problems, in the vast majority derived from its own architecture. These issues and architectural limitations have been known to affect the control, data and management planes, and might end up affecting at different levels the IXP security, scalability, and resiliency.

Issues affecting the IXP control plane can cause tremendous damages to the IXP operation. While the current discussion today is to decouple or not it from, especially with the novel Software-Defined Networking (SDN) approach, the legacy networks still have to deal with traditional problems affecting its control plane functionality and will continue having to handle for a couple of years during a possible transition to SDN.

Problems such as broadcast storms, prohibited and unknown Ethernet frames transitioning, and building and maintaining a Loop-Free topology in the switching fabric are, among others, a common place to any IXP running nowadays. Besides that, attacks targeted to the IXP control plane (route servers) can easily compromise all or part of its operation, creating damages to its image and mission. In these cases, insecurity and instability set up in the routing environment contribute to the increase in distrust among the participants, as well as distancing possible new members.

Moreover, support for Traffic Engineering (TE) both in inbound and outbound directions are performed only through BGP attributes manipulation. This limitation prevents the application of a most granular exchange policy, for instance, based on specific traffic pattern, and traffic optimization based on a specific application. Also, there's a lack of BGP support for an elegant solution to resiliency in a case where the IXP connector wants to have more than one port connected to distinct Points of Presence (PoPs) of such IXP. In this case, BGP does not provide TE capabilities to have a good traffic load balancing. In summary, the current IXP infrastructure has no or even very limited support to network programmability, which could bring interesting benefits to the IXP tenants.

Regarding scalability, the current IXP model limits the tenants to grow because the fabric does not have a mechanism to support same or multiple speed ports expansion. For instance, if a member wants to have a 10G port connected in an IXP PoP, and a 100G connected in another IXP PoP, they do not have a proper mechanism, using only BGP or even MPLS-TE, to achieve a good TE for the incoming traffic towards their backbone.

In the case that the participant wants to just bring up another similar port, it is usual that the IXP offer IEEE 802.3ad Link Aggregation Control Protocol (LACP) as a mechanism to improve their throughput to the peering fabric. However, LACP has been known as to carry several limitations, especially when the tenant is performing remote peering, or when they are using leased lines or MPLS circuits to reach the peering fabric.

In addition to the problems and limitations in the control plane as mentioned earlier, data plane problems can lead to interruptions in the IXP operation, and even worse, can propagate the incident to other routing points on the Internet. Due to the usage of a shared medium architecture where no routing policy enforcement is implemented, problems such as unauthorized Hot-Potato Routing, Routing leaks, prefix hijacking, and BGP

NEXT_HOP hijacking can easily happen and cause damages to all participants, and even to the entire Internet. Even though mechanisms to assure the routing origin, such as Resource Public Key Infrastructure (RPKI) validation, exists nowadays, it is unusual to see nowadays this kind of validation in the IXPs.

Still in the data plane, due to the lack of validation what is being advertised to the route servers on the exchange, (Distributed) Denial of Services (D)(DoS)attack can easily be generated by an IXP member targeting other tenants or even a host outside the scope of such IXP. While the simplest and straightforward solution to this is to apply anti-spoofing filters in addition to the prefix validation already mentioned, manually maintaining the filters is a hard task to accomplish especially when the number of tenant's and PoPs scale.

In the same sense, the limitation occurs when the the (D)DoS is originated outside of the peering fabric, and the target is a specific member of the IXP. In this case, the attack can destabilize all the switching fabric, as well as spread over the Internet due the degree of connectivity the IXPs represents today.

On the other hand, along with the novel SDN paradigm emerged the concept of Software-Defined Internet Exchange (SDX), an internetworking model that could potentially allow the addition of compute, storage and networking capabilities to multiple domains for traffic exchange, providing them more flexibility and possibilities when compared to the traditional IXP model.

Nevertheless, as occurred with the SDN definition in the early stages, the SDX meaning has different connotations for different individuals, and quite often it depends on the background of this observer. While this classification of SDX covers a wide range of ideas and use cases, especially for research and education communities, these definitions do not cover the mitigation and resolution of the above-mentioned issues and limitations of current industrial IXPs.

This presentation is the first report of an ongoing work, and its main contribution is to bring a survey of the technical requirements and weaknesses of current IXP's infrastructures along with a discussion about the mitigation or resolution process of such identified issue/limitation using the SDN and SDX concepts. The employment of such concepts can be the first step in the transformation of an industrial IXP into a lightweight version of SDX, providing a more robust and flexible Internet traffic exchange platform.

Despite the focus on Brazil, this study may contribute to understand better the limitations and improvements that can be adopted in other IXPs using similar models, including the ones serving the R&E community since both models share some of the identified weaknesses.