IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

A Review of Scalability Issues in Software-Defined Exchange Point (SDX) Approaches: State-of-the-Art

ABDIJALIL ABDULLAHI[1,3], SELVAKUMAR MANICKAM[1], AND SHANKAR KARUPPAYAH[2]

[1]National Advanced IPv6 Centre, Universiti Sains Malaysia, 11800 Pulau Pinang, Malaysia
[2]National Advanced IPv6 Centre, Universiti Sains Malaysia, 11800 Pulau Pinang, Malaysia
[3]Faculty of Computing, SIMAD University, Mogadishu, Somalia

Corresponding author: Selvakumar Manickam (e-mail: selva@usm.my).

ABSTRACT Internet Exchange Points (IXPs) interconnect heterogeneous networks and transfer substantial traffic volumes. In the past decade, the number of IXPs has seen tremendous growth, with more operators connecting to these IXPs even though these IXPs faced various inter-domain routing limitations. Routers based on Border Gateway Protocol (BGP) forwards packets only based on destination IP prefix and selects only routes learned from their neighbors. IXPs designed using Software-Defined Network (SDN), called SDX, offer solutions for existing inter-domain routing problems. This paper presents the existing scalability limitations of inter-domain routing at IXP and how traditional IXP structural design can be transformed into a highly scalable SDX design by exploiting the SDN platform's functionalities in different use cases of SDX. The paper then reviewed how the SDX improved various IXP operators' scalability by reviewing and analyzing the latest SDX models and approaches, which provide enhanced policies to enhance providers' management operations and offer good quality of services (QoS) to the various participating members. Finally, we discussed the open issues and challenges in this area that need further study and a solution to tackle them.

INDEX TERMS Internet exchange point, border gateway protocol, software-defined network, software-defined exchange, inter-domain routing, peering.

I. INTRODUCTION

The Internet is divided into autonomous systems, i.e., ASes. Each AS is under a specific administrative domain that manages and responsible for its operations. The Internet leverages Border Gateway Protocol (BGP), an interdomain routing protocol, to achieve the peering and reachability of information between different AS[1]. Today, network providers are required to work together to improve their operations and services effectively. Thus, Internet Exchange Point is a vantage point where various enterprise networks exchange IP traffic using a standard inter-domain protocol, BGP, to create a peering relationship with other ASes.

Furthermore, Internet eXchange Points (IXP) is a curial part of today's Internet ecosystem. IXP operators provide a layer-2 switching fabric facility, and the participants connect their edge router to IXP fabric. IXPs allows different Internet providers to minimize their transit costs and localize and create paths shorter between the endpoints [2], [3]. Currently, IXPs connect hundreds of operators and transfer a large amount of traffic, sometimes reaching terabytes per second. IXPs presence spread globally and even covers remote regions; thus, around eighty percent (80%) announced address space traverse across the IXPs[4].

Though the Internet adopted a structural design that hinders significant innovations and advanced improvement, recent architecture faced several problems, including delayed convergence, policy conflicts, security inefficiency against DDoS attacks, and routing inconsistencies and anomalies[1]. In the same way, Internet routing lacks flexibility and reliability and also challenging to manage. Internet providers relied upon inefficient mechanisms such as AS path prepending, communities, selective announcements, local preferences, and others to manage traffics, prevents attacks, and identify peering agreements. These shortcomings come from inter-domain routing protocol behavior. BGP forwards packets using only IP

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3069808, IEEE Access

prefix of destination also affects only direct neighbors and establishes indirect expression policy[5].

A new networking platform has emerged to decouple the data plane from the control plane to tackle the aforementioned issues. The concept called Software-Defined Networking (SDN) increases the flexibility and reliability of inter-domain routing by separating the planes[6]. The SDN has also reshaped the network's design to offer new inter-domain traffic delivery capabilities [7]. In the beginning, SDN was only implemented in inter-domain routing and provided the functionalities. Today's SDN provides the required functionalities to the IXP operators to improve local routing. IXPs become an important place to implement SDN benefits[2]. Software-Defined Exchange Point (SDX) has been proposed to enable flexibility in IXP operators and allow IXP members to manage the service providers' traffic exchange leveraging policies. These policies advanced inbound traffic engineering and application-specific peering and enhanced the control routing decisions of IXPs [8], [9].

This paper discusses the improvement of scalability of Internet exchange points by exploiting SDN functionalities to enable IXP operators to advance their capabilities and manageability to provide good services into their member networks. This work extensively presents the models and approaches related to the improvement of scalability and performance of IXPs that previous studies proposed like iSDX[7], ENDEAVOUR[4], Umbrella[2], SDIX[6], and COIN[10] to tackle the various challenges of inter-domain routing by deploying SDX. Then we analyze how these approaches are changed the way IXP operators provide the services into different autonomous systems. Also, they implemented several policies that enhanced the manner of inter-domain routing, especially the BGP protocol route, and forward the packets in the network domain. The contribution of this paper can be summarized as follows:

- Present the existing challenges and issues of IXPs related to architecture and inter-domain routing protocol limitations considering the scalability and performance.
- Analyze the previous models and approaches of software-defined exchange point; SDX related to scalability by exploiting the software-defined network functionalities and compare these models focused on different aspects.
- Identify some challenges and open issues of IXP operators when deployed the SDN features that are important to solve and find ways to achieve better management and good services in the IXP environment.

Other sections of this paper are structured as follows. Section II presented a brief overview of IXPs, while Section III discusses the existing scalability challenges of IXPs. Also in section IV argued the development in IXP architecture along with its different use cases. Additionally, section V looked at the SDN-enabled frameworks and models for developing Internet Exchange Points (IXPs). Finally, the domain and conclusion's open issues and challenges are discussed in sections VI and VII.

II. INTERNET EXCHANGE POINT(IXP)

IXP is defined as a physical infrastructure where many networks can join and create agreements privately to develop their network resources to transfer traffic on the Internet. The networks that IXP interconnect include Internet Service Providers (ISPs) like Comcast, AT&T, Telmex; content providers like Google, Facebook, Amazon; universities, banks, and other network organizations[11]. Similarly, IXP is a physical infrastructure that can be used to simplify the traffic exchange between ISPs. According to their business model, technological and social characteristics at IXP, Internet providers can decide to exchange their traffic between them or not. Also, the ISPs can make a peer connection outside of IXPs but peering via IXPs is much less expensive[12]. The study[13] stated that the key business model of IXPs is to manage and operate a physical infrastructure of private and public interconnection. The IXP offers a service of layer-2 switching fabric and connects the access router of each member(ASes) to that switch fabrics. At IXPs, members create a BGP session when deciding to peer with each other and exchange their traffic using IXP's infrastructure. Peering at IXP extends Internet architecture and supports creating BGP sessions to enable the exchange traffic between ASes[14]. IXP operators interconnect various network providers to enable the peering relationship using BGP; a BGP is a de facto protocol for the inter-domain routing system[15].

Similarly, BGP is a distance-vector routing protocol and used as an exterior gateway protocol currently. Each access router shares with its neighbor routing reachability information using route advertisement and other attributes. The router assesses all incoming routes using those attributes, and then forwards the best routes to its neighbor routers[16].

Last two decades, IXPs have become a crucial part of the Internet peering ecosystem due to the widespread development of peering after the launch of the first IXP. The original IXP at the national level in developed countries has been increased to join local or regional IXPs placed in cities and towns. These growths and improvements have been answered by the increasing needs of applications, including higher bandwidth, lower packet loss, and lower latency[17], [18]. IXPs offer great benefits for Internet players, including reducing latency (all local traffic are not routed to international hop); decreasing cost (ISP does not pay transit cost for global upstream to send domestic traffic). Simultaneously, it also increases autonomy (IXPs enhanced local Internet infrastructure's reliability and power by reducing the reliance on global connectivity for local communication)[19].

Internet eXchange Points (IXPs) have become a vital element of the Internet infrastructure in the last decades because of connecting various network providers and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3069808, IEEE Access

transferring huge inter-domain traffics volumes. Commonly, IXPs can be of different kinds. Some are small IXPs that offer services to regional or national network members, and others are large IXPs that provide services to international or connecting hundreds of members[19]. Furthermore, IXP providers are constantly growing; IXPs business models are also continuing to grow. The non-profit business model of IXPs is primarily designed to charge per port considering the speed of ISP's link to the IXP, While the profit-model of IXPs charges different services with switching fabric like space and other facilities[9].

On the other hand, the IXPs significantly impact the Internet, bringing significant and apparent effects on Internet structure and its routes. IXP providers reduce path lengths moderately in most networks, along with the hypergiants (Google, Netflix) have extensive reduction. Additionally, the IXPs minimized the reliance on transit providers[20]. Figure 1 illustrates the traditional design of the IXP. The figure demonstrates the Points of Presence (POP) of four (4) Internet Service Providers (ISPs). Also, it shows each ISP has its border router, which use to connect an IXP. A Layer-2 switch comes together with the different ISPs, as illustrated in the figure "Ethernet Switch." Additionally, the figure showed two kinds of interconnection, i.e., private peering and public peering.

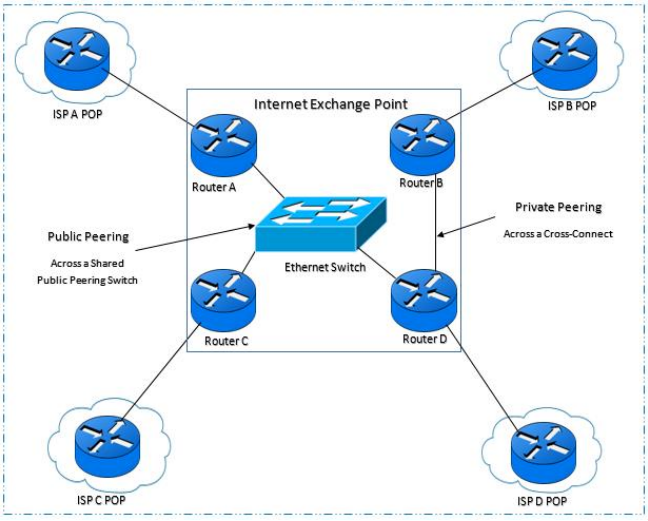

FIGURE 1. Traditional IXP architecture[21].

III. EXISTING ISSUES AND CHALLENGES IN IXPS

Internet Exchange Points (IXPs) are essential building blocks of today's great-performance and scalable connectivity. Typically, IXP offers a facility similar to a layer-2 switching fabric, interconnecting hundreds of network providers and enabling them to transfer traffic directly. Similarly, IXPs interconnect many network domains and transfer large traffic volumes. So, IXP management and infrastructure have met difficulties to grow progressively. Hence, the limitations that mostly IXPs encounter include layer-2 switch packets forwarding restrictions like the absence of load balancing, loops, and broadcast storms[6].

Similarly, traditional IXP structural design limitations that studies quantified include layer-2 switching fabric, BGP control plane, manual policy enforcement, and scarce monitoring and visibility[21]. IXP providers meet to address the challenges and actions to respond to the needs of their users. IXP operation management's significant problem is to handle elephant flows that different from other flows according to traffic size and duration[22]. The existing IXPs have faced the challenges of data plane policies such as inbound traffic engineering, application-specific peering, redirection middle-boxes, and wide-area server load balancing. Additionally, the existing difficulties of IXPs mainly come from the inter-domain routing limitations; BGP only routes to the destination IP prefix and uses indirect path selection mechanisms[23].

Internet routing, particularly inter-domain routing, faced shortcomings that inhibits innovation in new kinds of end-to-end networks and services. Thus, routers create local routing decisions considering policies in which operators and their services have limited control, resulting in routing decisions that have not improved for any particular operator and services[9]. IXPs offer multiple path opportunities, but BGP protocol supports a policy that can select only a single path between two endpoints. The BGP protocol does not provide a way to use different paths to meet various application requirements, including performance, security, reliability, and others[24]. Similarly, another study [25] specified that BGP met another difficulty which is low converging speed.

The Internet encompassed a massive and increasing quantity of Autonomous Systems (ASes). ASes share routes and reachability information by using the inter-domain routing protocol, or BGP. Currently, the inter-domain routing system is less flexible. It comprises the developing requirements of current inter-domain routing like effective routing policies in ASes, a new Internet routing scheme, and multi-path routing. Thus, the routing decision of BGP is based on only IP prefixes of destination. In ASes, each edge router has decided only information learned from next-hop while the different paths of inter-domain routing could transfer the traffics. Routing that relied on destination IP prefix needs to determine the best path for a specific destination. Typically, ASes select only the best routes learned from neighbors, while different optimal routes have been ignored and are not considered remote route options[26].

Additionally, the BGP suffers from several concerns associated with low convergence speed and security vulnerabilities. The BGP version's change is difficult due to extensive use globally and other technical challenges[27]. Table 1 provides the scalability challenges of dividing two aspects: data plane and control plane. It demonstrates the different studies that talked about these aspects by showing "Y" means yes and "N" means no.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3069808, IEEE Access

TABLE 1. Existing scalability challenges for IXPs.

Authors	Scalability aspects	
	Data plane (Layer-2 fabric)	Control plane (BGP)
Martins et al. [6]	Y	N
Kumar. [21]	Y	Y
Griffioen et al.[9]	N	Y
Wang et al. [26]	N	Y
Gupta et al [5]	N	Y
Silva et al.[22]	Y	N
Warraich et al.[23]	Y	Y
Wolf et al.[24]	N	Y
Chen et al.[25]	N	Y
Sermpezis & Dimitropoulos.[27]	N	Y

IV. DEVELOPMENT IN IXPS ARCHITECTURE

The development of interconnections between network enterprises is increasing, content providers (e.g., Facebook, Netflix, Google) are looking into improving their customer experience. They have a significant need to connect directly with Internet Service Providers (ISPs) to reduce the network's problems and delays and advance user expectations. Nevertheless, the increasing demand for interconnection enhances the significance of Internet Exchange Points (IXPs), which offer various services and pricing models applicable to their public and private users' needs. The traditional interconnection architecture works as illustrated in figure 2; the data plane consists of a layer-1 for private interconnection among two network ISPs. A layer-2 switch connects multiple ISPs for public peering.

Similarly, BGP works as a control plane that manages different networks, either the private or public domains. In the case of public peering, it consists of ISP border routers and a router server attached to the IXP fabric. The normal decoupling of the control plane and data plane in the interconnection architecture adopts SDN[28].

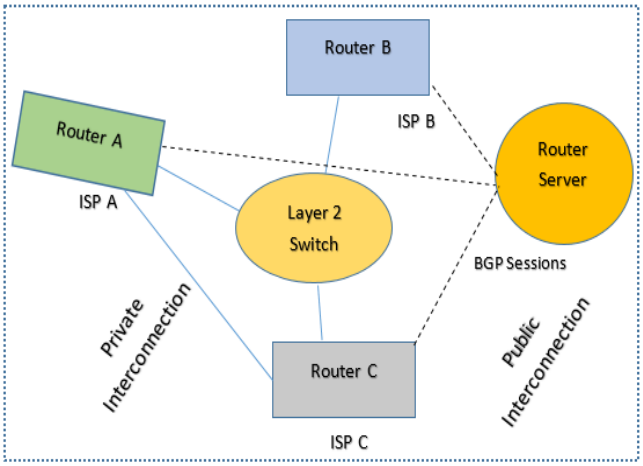

FIGURE 2. Previous interconnection architecture.

SDN is defined as a new mechanism that provides a flexible network and better management by decoupling the data plane and control plane via software applications. The control plane is mainly responsible for packet forwarding under controllers' rules, although it uses network devices like routers and switches. The control plane also allows ISPs and network administrators to manage and supervise the network and offer a robust environment to implement multiple network applications and services. SDN supports advanced features such as network security, network virtualization, and green networking and can be applied in software and used in networks with real traffic[29]. Similarly, SDN is a networking paradigm that was newly developed to route the traffic efficiently by using a powerful programmable controller.

Furthermore, the ability to route packet flows is better than BGP forwarding prefixes of destination. The SDN provides different providers a capability to specify and apply routing policies on traffics that become SDN fascinating in inter-domain routing. The number of network providers that connect IXPs is increasing rapidly. As mentioned earlier, a new concept of inter-networking, i.e., SDX, emerged to advance the management and flexibility of routing decisions for network operators at IXPs[9].

A. SDX: SOFTWARE DEFINED EXCHANGE POINT

Software-Defined Exchange has been developed as a model to provide network operators with finer granularity and excellent control over forwarding. SDX allows operators to exchange traffic better than today's approach and can create at much fewer time scales than others. Likewise, SDX will enable operators to build a new way for end-to-end paths on the network. It also enables the possibility to offer various service levels to network operators and charge appropriately[9]. Another study [30] highlighted that SDX is a joint of the different administrative domains that can exchange their resources like computing, storage, and networking resources.

Deployment of SDX on the Internet is increasing progressively. SDX contributes to an inter-domain routing system flexibility and reliability and allows participants fine-grained policies to change their default BGP route. The policies facilitate traffic management capabilities like advanced inbound traffic engineering and application-specific peering[8]. Furthermore, SDX is a new interworking model that enables administrative domains to share storage, computing, and networking resources independently. SDX is a new idea implemented in many different disciplines like cloud computing[31]. Figure 3 illustrates the transformation from the previous IXP design to an improved SDN-based IXPs, i.e., SDX. The SDX design comprises the different components: Programmable fabric, SDX controller, and application. The SDX enables APIs to provide advanced services to IXP members. Also, IXP members use a router server to exchange BGP routes. it stores all the inbound route information from members and forward it without change to

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3069808, IEEE Access

the other IXP members. Applications develop high-level policies to control IXP fabric. The SDX controller converts high-level policies into low-level rules to apply to the IXP fabric and monitor network activities[32].

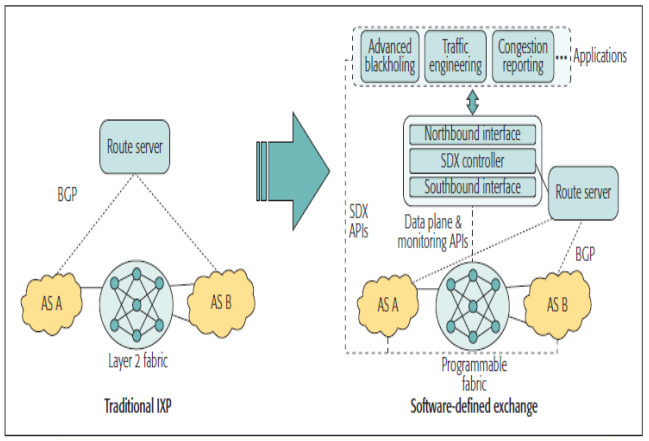

FIGURE 3. **Development of IXP architecture into SDN-enabled**[32].

B. SDX USE CASES

This section describes the applications and use-cases that SDX provides to enable flexible policies and efficient IXP operators. The suggested use-cases include wide-area load balancing, redirection of middle-boxes, inbound traffic engineering, and application-specific peering[5]. Likewise, the study indicated another use case known is known as advanced black-holing[32]. We explain each use case in detail, as follows:

1) APPLICATION SPECIFIC-PEERING

Video services need high-bandwidth (e.g., YouTube, Amazon Prime, and Netflix) and significantly impact overall traffic volume. BGP is unable to differentiate this type of traffic, i.e., real-time traffic. Hence, ISPs had to resort to a unique mechanism for tackling the high-bandwidth services, so SDX provides application-specific peering, allowing AS to exchange traffic depending on the need of the specific applications.

2) INBOUND TRAFFIC ENGINEERING

BGP can effectively manage the outbound traffic, but it cannot control the inbound traffic because BGP relies on routing IP prefix of destination and uses indirect techniques like ASP path, communities, selective advertisement affect the neighbors. Though, IXP participants need to advance the mechanisms of controlling incoming traffic from other neighbors. Therefore, SDX provides a platform that allows AS to directly manage and control incoming traffic by applying forwarding rules and deploying switches at the IXP.

3) REDIRECTION THROUGH MIDDLEBOXES

Middle-boxes like firewalls, network address translators, load balancers offers many services to the networks. These tools and devices are costly in large ISPs due to geographic areas and difficult to place in every location. Large ISPs tried to perform a technique to direct the traffic into specific middle-boxes, but it is a complex task when using routing protocols. Thus, SDX enables ISPs to steer traffic and redirect fixed subsets via one or more middle-boxes.

4) WIDE-AREA SERVER LOAD BALANCING

Typically, clients send requests to servers, so content providers must balance these requests across different servers by using DNS. The DNS servers met various limitations to manage and balance requests from clients. So, SDX allows content providers to balance the load based on clients' requests that traverse the clusters of servers by broadcasting anycast prefixes and changing the destination IP address to contest the selected hosting location depending on any fields in the packet header.

5) ADVANCED BLACK-HOLING

A mechanism that enables AS to request its neighbors to discard packets destined to a particular IP prefix. Unfortunately, black-holing cannot differentiate the legitimate packets and unwanted or malicious packets. Thus, all packets are dropped. SDX offers operators an Advanced black-holing mechanism to manage and drop rules as fine-grained and discarded only unwanted packets to reduce such risks.

V. SDN-BASED APPROACHES AND MODELS FOR IMPROVING SCALABILITY OF INTERNET EXCHANGE POINT

This section introduces recent platforms and models that facilitate IXP operators in managing their operations and offering good services to the various IXP members by using the SDN functionalities.

A. iSDX: MODEL OF SOFTWARE-DEFINED INTERNET EXCHANGE POINT FOR INDUSTRIAL-SCALE

Previously proposed SDX architectures are not compatible with large IXP operators. So, iSDX becomes the first SDX architecture that can work with large IXPs topology. Former SDX controllers cannot manage the extensive forwarding packets and require much time to process this operation. iSDX contributes to the SDX scalability to reduce the forwarding table size and compilation time. Initially, SDX designs encountered two scalability challenges. The first one is related to the control plane. The second is associated with the data plane as stated by the authors: 1) The way the policies of different network operators can be put together into one forwarding table entry. 2) the IXP switch cannot manage the amount of forwarding table entries from the control plane, and also, the forwarding entries at the switch grow excessively[7].

To tackle these limitations and reach the principles of minimizing compilation time, the number of forwarding table entries, and reducing the number of updates to the forwarding table when BGP routes change. Therefore, the study suggested two approaches: 1) Partitioning the computation of the control-plane. 2) SDN and BGP forwarding.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3069808, IEEE Access

1) PARTITIONING COMPUTATION OF CONTROL PLANE

Control planes for all IXP participants are performed by a centralized SDX controller that facilitates handling large and single combined policies. The policies between the different IXP participants carry out dependently. The authors tackle this challenge by splitting the computation of the control plane of disparate IXP members. This approach allows the computation of each participant's policies separately. However, computation partitioning simplifies policy compression more appropriately by processing a small portion and minimizing the computation time and data plane state. This mechanism also carries out a compilation of policies to scale out as routes grow and the number of IXP members.

2) DECOUPLING SDN AND BGP FORWARDING

In the former SDX designs, the SDN and BGP policies computes collectively that causes increasing the amount of forwarding table entries and making recompilation of forwarding table entries if any change of BGP routing occurs affect the cost of the operation. The study suggested this approach to tackle this problem, which allows the SDX to encode a separate tag the reachability information of BGP. This approach reduces the number of forwarding table entries. It minimizes the number of updates of the forwarding table when BGP routes' change occurs by encoding all BGP best paths' reachability information into the destination MAC addresses.

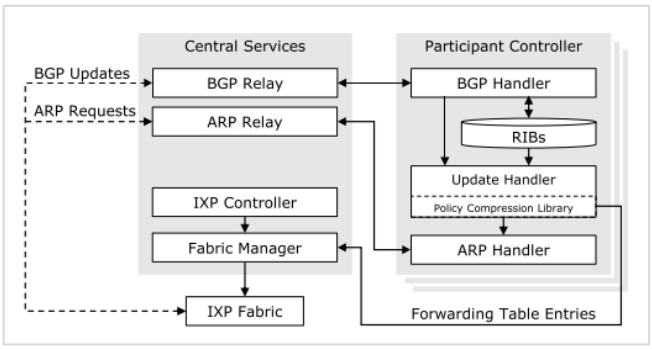

FIGURE 4. iSDX architecture[7].

Figure 4 shows the iSDX design that the study proposed applying the approaches and solving the limitations as mentioned earlier, data plane and control plane. The study suggested the first SDX design that tackles the scalability challenges for large-scale IXP topologies. So, they proposed two mechanisms: compression and partitioning. Moreover, iSDX architecture implemented one of the largest IXPs globally. The result demonstrated the reduction of forwarding table entries and computation time considering two orders of magnitude.

B. ENDEAVOUR: SCALABLE PLATFORM OF SDN ARCHITECTURE FOR IXPS

Some IXPs applied multi-hop architecture, so ENDEAVOUR is an SDN model for IXP operators. It enables the applicability of multi-hop IXP topologies, extends the scalability, and minimizes the switching fabric problems about broadcast traffic. Deploying multi-hop IXP topologies with fully SDN functionalities has significant challenges[4].

The authors identified such problems that met the existing IXP topologies and how to solve e these problems: 1) The challenge related to the way of distributing rules of different IXP switches to reduce the resource consumption. To deal with that issue, ENDEAVOUR tried to limit core switches' tasks and operate them for intra-fabric forwarding tasks. Similarly, the study identified the approach which minimizes the number of routing policies installed in the edge switches. 2) The authors specified the challenge of multi-hop topologies and required various mechanisms to recover fails in different switches and withdraw the BGP route quickly. The researchers stated three approaches to solving this issue: bouncing packets back to the ingress switch, injection of recovery information in the packets, and duplication of outbound policies. As shown in figure 5, the study implemented the architecture to solve multi-hop IXP topologies' challenges. ENDEAVOUR design comprises various components: SDX controller interface, member controller, Members Information Base, a Fabric Manager, and other Fabric Manager elements such as Edge Forwarding Handler (EFH) and Core Forwarding Handler (CFH).

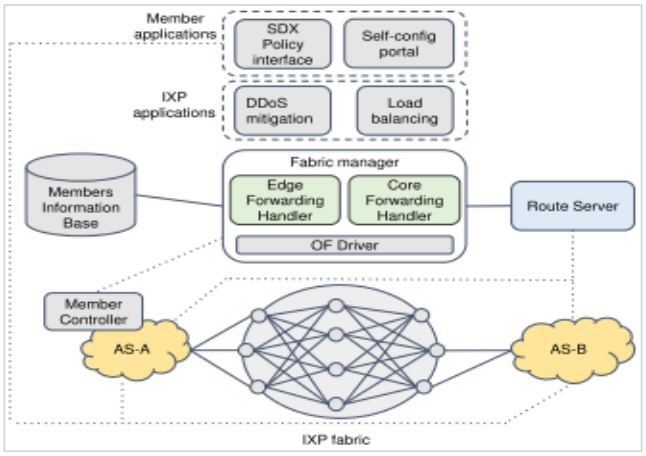

FIGURE 5. The ENDEAVOUR design[4].

The following sections have discussed the approaches proposed the study to tackle the challenges of multi-hop IXPs:

1) DUPLICATING OUTBOUND POLICIES

In a single switch topology, the policies are stored within one switch. It easy to re-compute the policies if a failure occurs and make recovery easier. Nevertheless, the multi-hop topology needs to distribute the different policies of participants across all switches. So, this approach duplicates the outbound and inbound policies on different switches. It also saves the vMAC copy in the header of the packet. When a link fails, this approach performs to compute a new output port again considering the member's policies and the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3069808, IEEE Access

changed vMAC of the packet using the proposed architecture component (i.e., Edge Handler Controller) at the affected egress switch. The Edge Handler Controller uses the iSDX tables to perform a re-computation. Each member must keep all participants inbound and outbound tables that bring the forwarding state's mass-replication in this approach.

2) BOUNCE PACKETS BACK TO INGRESS SWITCH

The first approach results in the enormous duplication of the forwarding state, packet latency, and bandwidth waste. This approach allows a technique that the forwarding packets bounce back to an ingress switch when a link fails to address the issues mentioned. The Edge Handler Controller element performs a re-computation of a new egress port using the iSDX platform tables.

2) INJECT RECOVERY INFORMATION INTO PACKETS

This method tries to tackle the overheads that might cause the above approaches by keeping the additional information in a packet header. The OpenFlow does not provide the switches with a capacity to recirculate the operation when a failure occurs. The egress switch enables this information to reroute packets into any link failures between the participants' devices and the fabric. Additionally, this approach promises a fast reroute. To perform this operation, it keeps the additional SDX and Umbrella tables into the switch, bringing the processing delay and cost of switch memory.

One of the aspects that assessed the study is the distribution of flows in the edges that confirmed that the distribution and replication of participants' outbound policies on different switches primarily improve scalability. Additionally, other aspects that evaluated the study include IXP internal load balancing, black-holing, and finally assessed forwarding state recovery those are demonstrated the importance and contribution of the proposed architecture (ENDEAVOUR).

C. UMBRELLA: A NEW SDN ARCHITECTURE FOR IXP FABRIC

Models that improve the scalability and deploy multi-hop topology are more critical for IXP providers. So, Umbrella is a new model that enables a robust and resilient switching fabric and minimizes the risks that cause the data plane's dependability on the control plane. Umbrella is also deployed for any topology of IXP, either it is single or multi-hop topologies. Umbrella provides SDN programmability to manage the control traffic in the data plane. Umbrella also allows a platform for eliminating the learning mechanisms of actual MAC in traditional IXPs networks. The traffic of the broadcasted Address Resolution Protocol (ARP) is managed directly within the data plane. The model also reduced resource utilization, cost of management and extended the scalability by performing an encoded path of layer2[2].

This model simplifies the fabric's management and makes the controller's work to supervise the network—two ways of Umbrella to enhance the former SDN models for IXPs. First, Umbrella provides a robust and scalable fabric for complex IXP same as the iSDX model. Second, the implementation of Umbrella promises the applicability to any IXP topology to support SDX architectures rather than iSDX, which is only deployable to a single topology of IXPs. Figure 6 illustrates the suggested design of Umbrella to minimize the control-data plane risks and reduces the broadcast storms.

The study suggested four approaches to apply the platform of Umbrella, which focuses on the dependency of the control-data plane to provide a reliable and robust forwarding fabric inside the IXP.

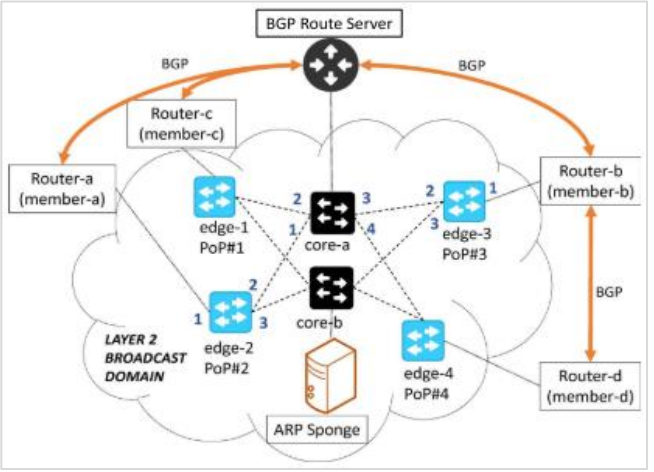

FIGURE 6. **Umbrella architecture**[2].

1) NO BROADCAST TRAFFIC

A Layer-2 shared broadcast domain has many side effects in previous IXPs. They perform rules to restrict these effects. For instance, in advance, the IXPs must know the MAC address of the participant's router. Then, IXP allows the allocation of the edge switch's Ethernet port and the access control list of that MAC address configuration. Therefore, the IXP must know the location of all participants' routers. Hence, to tackle those side effects, the Umbrella eradicates the necessity of location discovery approaches (i.e., ARP request or Neighbor Discovery (ND) for IPv6) according to broadcast packets. Umbrella also reduces the role of ARP-proxy, which has an active role with previous SDX architectures. Umbrella exploits the OpenFlow (OF) capability that provides the ability to translate the broadcast packets into unicast. They suggested a mechanism of label-oriented forwarding to reduce the number of rules in the core switch of IXP. Umbrella promises fabric scalability because the amount of flow table entries per core switch will scale with the amount of active physical ports in the switch itself.

2) A LABEL SWITCHING MECHANISM

Umbrella allows the traditional switches utilization in the core to void the upgrading switches cost. The edge switches require the OF capability to re-configure the layer-2 destination field, but core switches need only to transfer the packet using simple access filtering rules. Though this mechanism applies to single switch topology, it is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3069808, IEEE Access

challenging to implement on multi-hop fabric. In a single topology, the core switch requires to encode the output port into the most significant of the destination MAC address. In multi-hop topology, packets travel across different core switches, and it needs to encode the new scheme that separates the output ports of different switches. However, to adapt the Umbrella with multi-hop topology, it needs to manipulate the source routing under the following process. First, the initial edge switch chooses the route. Second, encoding the output ports into stack labels in the MAC destination address. Lastly, considering the stack's upper value, each core switch processes the frame and bursts the stack before transferring the frame. In this case, each node (i.e., switch) requires only to find at most significant byte without regarding its place in route towards the target. Bursting out from the destination's MAC address, the last label usage needs header rewriting abilities. In this case, possible only in the core switches that have the OpenFlow capabilities. Specifically, each core switch needs two action tables (i.e., copy-field, forwarding).

3) ROUTER SERVERS AND UMBRELLA

The members connect to IXP have one of two relationships to exchange traffic; bilateral and multilateral relationships. In both of the relationships, the Umbrella handles the forwarding of their BGP traffic. With bilateral peerings, the TCP connection acts as the BGP session like normal data plane traffic that traverses the IXP. The switch manages the traffic using its rules without any intervention of the control plane. In multilateral peerings, the switch directed the incoming traffic of BGP into the route server using the single rule of an edge switch. On the other hand, the management of outbound traffic is performed automatically via the edge switches' existing policies.

4) FAILURE RECOVERY AND DETECTION

Umbrella depends on OpenFlow (OF) features to tackle link failure of the data plane. Primarily, OpenFlow uses the Group Fast Failover mechanism to respond to link failure. This mechanism has a table that enables a fast failover. This table can be manipulated to supervise the interfaces, forwarding action, and the status of ports of the switch without the controller. In the data plane, the recovering failure is more complex. In this case, the Umbrella controller implements the protocols (i.e., Local Link Discovery, Bidirectional Forwarding Detection). When the data plane's failure is noticed, the Umbrella controller only modifies the configuration of the edge switch with the fallback route.

The study stated that the Umbrella platform was implemented on two IXPs (i.e., TouSIX, NSPIXP-3 OSAKA). The deployment on TouSIX eliminated many problems of its operations and minimized the dependability of the network administrator. Around 97% Umbrella reduced the broadcast traffic of ARP with Fabric. At the same time, approximately 8% CPU usage is reduced in the switches. Moreover, the Umbrella was implemented on NSPIXP-3 OSAKA, and the result showed the elimination of ARP traffic positively.

D. CONTROL INBOUND TRAFFIC (COIN): AN SDN MODEL FOR DEVELOPING A ROUTING SYSTEM OF CONTROL PLANE.

Traditional BGP routing control mechanisms of incoming traffic are a difficult task. COIN is a model designed to advance the control plane's routing system that applies to the BGP by exploiting SDN technologies. COIN is also enabling to control the inbound traffic of multi-homed ASes and change the decision process of BGP[10]. In this framework, ISPs utilize SDN to control network flows that designate to ASes.

COIN applies to the current BGP protocol, the de-facto inter-domain routing of the Internet. Also, this framework deploys the path-vector of the BGP protocol to keep track of the network's visibility. To avoid loops, the COIN implements the path-vector mechanism. BGP path-vector approach does not support additional important traffic engineering metrics (e.g., capacity, delay). Therefore, COIN exchange further information of network (e.g., bandwidth utilization) from participants using open interfaces. Figure 7 depicts the design of the COIN structure. It helps to manage incoming traffic and keeping with the compatibility of the previous BGP. It also provides interfaces to enable the peering of ASes with each other and exchange agreements (i.e., bilateral) and the way will be implemented the traffic control.

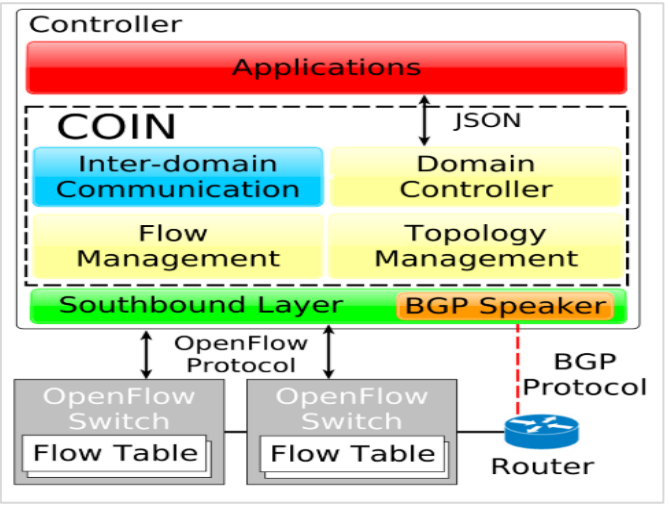

FIGURE 7. COIN Framework Architecture[10].

The study quantified that BGP follows a forwarding pattern of destination-based. COIN framework manipulated and identified the packet flows by implementing the SDN network. It allows the improvement of a new routing system of the control plane that is not based on BGP protocol. This framework promises interoperability with previous BGP protocol. COIN performs the improvement inter-domain

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3069808, IEEE Access

routing system, specifically traffic engineering that does not support the BGP protocol and carrying important metrics like capacity links.

Finally, the ASes can facilitate finding out the multi-path of the Internet by deploying the COIN application. Similarly, the ASes can send the incoming traffic into multiple paths using the path diversity concept. This review showed the result that guarantees the multi-path issue's solution to manage incoming traffic concerning bandwidth availability.

E. SDIX: IXP MANAGEMENT FRAMEWORK BASED ON SDN.

Current IXPs do not have adequate management for operations and services, and they do not support advanced policies to improve their manageability. SDIX framework is used to manage IXPs infrastructure, which deploys SDN capabilities to support flexible and reliable policies and achieve the IXP operators' management goals. SDIX simplifies and improves different activities of IXP management. This framework uses SDN-enabled switches to forward rules and performs IXPs configurations and policies to advance management operations. Additionally, SDIX supports SDN functionalities that cannot support previous layer-2 networks, and it offers new capabilities for IXPs[6].

The researchers suggested the SDIX Framework solve the management challenges of IXPs exploiting the functionalities of software-defined networking. SDIX simplifies the IXP data plane's control and management by deploying the ONOS controller and OpenFlow switches. It also implements some components of the SDN-IP application. SDIX's interface enables the administrative functions (e.g., adding new member, route server, remove IXP member, isolation zones, bi-lateral relationship) for IXP operators and other policies for control data planes. The framework allows IXP providers to control packets' packet forwarding policies that manage the traffic flows that traverse the IXP fabric.

However, the work suggested policies that allow enriched traffic engineering (e.g., maximizing bandwidth, reducing latency, load balancing) and shortest routing paths. SDIX implemented policies include IPForwarding Policy, BestPathForwarding Policy, Route Server Policy, MACFilitering Policy, MACForwarding Policy, and VLANTranslation Policy. Therefore, when the study configured and verified the SDIX framework, they found that SDIX improves the scalability and reduces the amount of OpenFlow rules.

The study described the operational benefits provided by the SDIX framework and how to solve the management limitations of IXPs, such as control and filter unwanted traffic, monitor traffic, centralize management information, set up new members, and configure traffic forwarding.

1) TRAFFIC FORWARDING CONFIGURATION

The SDIX framework suggested policies that enable network providers to decouple configuration rules in the switch from the controller's policies. The SDIX implement configured policies by deploying the OpenFlow switch. Implementing the policies and OpenFlow enables IXPs to specify more effective policies like traffic engineering and better utilization than traditional mechanisms in Ethernet switches (i.e., EAPS and STP). The SDIX framework allows providers to prevent traffic forwarding problems like sidestepping.

2) ADDING NEW MEMBER

The framework adds new members and an approach to isolate rapidly before membership with fabric and tested it in the quarantine area. This concept provides IXP operators to avoid misconfiguration risks when a new member is added to the production fabric.

3) MAINTAINING IXP MEMBERS

The framework reduces the operational activities related to IXP members. For instance, altering a port of IXP that connects the member router automatically modifies traffic forwarding rules.

4) CHECK UNWANTED TRAFFIC

The SIDX provides richer forwarding policies that allow IXP operators to easily clean unwanted traffic like BestBathForwarding, IPForwarding, and RouteServers.

G. Comparison and contrast of approaches and models

This section describes the comparison and differences between the previous SDX models and methods according to policies, scalability features, and applicability of different topologies in IXP providers. Table 2 illustrates the detail of this section.

F. Summary of SDX approaches and models

The iSDX framework, the first solution of SDN designed for large IXP operators, improves the previous SDX project and only implements the single topology of IXPs. iSDX suggested two approaches to reduce forwarding table size, policy computation time, and update rates of the forwarding table. The first mechanism is related to splitting the computation of the control plane about different participants. The second mechanism is related to separating the SDN from BGP forwarding.

The ENDEAVOUR framework, a model for multi-hop IXP topologies, provides high scalability and limits traditional broadcast traffic methods in the switch. The model depends on the concept of iSDX to decouple the SDN control plane and BGP despite that ENDEAVOUR is deployable with multi-hop topology. In contrast, the iSDX applies to the single-hop topology. ENDEAVOUR stated three approaches to solve the issues: injection of recovery information in the packets, bouncing packets back to the ingress switch, and duplication of outbound policies.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3069808, IEEE Access

TABLE 2. Comparisons and contrasts of SDX models and approaches.

SDX Models	Policies	Scalability Improvement	Deployable Topology
iSDX[7]	Compression and partitioning of forwarding policies.	Minimizing policy compilation time Reducing forwarding table size. Decreasing the rate changes of the forwarding table if routes of BGP altered.	Deployed only on a large single Topology of IXP providers.
ENDEAVOUR[4]	Facilitates policies that duplicate the outbound and inbound policies of different members. Simplifies policies that make a recovery if a link failure occurs in the network.	Reducing the utilization of IXP resources by distributing the forwarding rules on different switches. Minimizing the number of routing policies deployed in switches that connect member routers (i.e., edge switches). Avoiding redundant replication of the forwarding state, an unused bandwidth, and raising packet latency. Promising recovery if the link fails occurs and quick route withdrawal of BGP.	Implemented both on single and multi-hop IXP topologies.
Umbrella[2]	Helps the policies that eliminate the traditional mechanisms for discovering MAC address. Having policies that detect the failure of the network and perform a recovery.	Reducing the hazards of data plane which rely on the control plane by limiting the role of controller. Decreasing the need for traditional approaches of broadcast packets to find the location like ARP and IPv6 ND. Minimizing the necessity of the ARP-proxy role. Translating the broadcast packets into unicast.	Deployed both on single and multi-hop IXP topologies.
COIN[10]	Policies perform controlling Inbound traffic from ISPs to multi-homed autonomous systems.	Enabling incoming traffic management of multi-homed ASes exploiting the SDN features. Supporting the Ases to find out the path diversity of the Internet.	Managed only for Multi-homed autonomous systems.
SDIX[6]	Policies enable to perform a more advanced traffic engineering and path shortening for IXP operators.	Enhancing the capabilities of layer-2 to enable traffic forwarding configuration. Deploying great management policies to improve management activities. Minimizing configuration problems.	Implemented on single topology for IXP providers.

Umbrella, a new SDN approach that improves the switching fabric capability to avoid risks that cause data plane dependability on the control plane, applies to existing IXP topologies. This model eradicates the approaches of broadcast traffic to find the location by using a feature of translating broadcast packets into unicast by exploiting the capacity of OpenFlow(OF). Furthermore, the Umbrella concept was deployed on IXPs globally and evaluated the importance of suggested architecture regarding data plane performance and flow rules.

Control Inbound Traffic (COIN), a framework to advance the control plane's routing scheme compatible with traditional BGP. COIN support to control the inbound traffic of multi-homed Ases. It performs allocating weights to links and partitioning bandwidth among the various links to facilitate incoming traffic management.

The SDIX framework, an IXP management framework, applied SDN functionalities to provide IXP operators flexible and robust policies to achieve the advanced administration of IXP operations and services. SDIX supports the different policies to solve scalability limitations of the management operations of IXPs and to eliminate BGP shortcomings and maintenance overhead.

VI. CHALLENGES AND OPEN ISSUES

SDX improves the scalability of IXP operators at the inter-domain level. It provides highly flexible and powerful policies that enable them to manage their operations better and provide good services. However, there are still open issues and challenges in the domain that requires further research to expand the SDX scalability. We point out in this section some of those issues that require to improve and solve.

1) ROUTING POLICIES

In the past decade, IXP deployment has been rising rapidly. IXP operators have different models. Some are small, and others are large IXPs that might connect over 700 members, and each member has numerous prefixes, and each participant needs a separate control traffic flow policy. However, some studies attempted to tackle these challenges, like the original design of SDX[5] and iSDX[7]. The SDX design enables policy compilation

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3069808, IEEE Access

from different participants' policies, but it can only manage small-sized IXP providers. The iSDX model suggested the approaches that partition participants' policies use to reduce the computation time and decouple the BGP and SDN forwarding to minimize the number of forwarding table entries. The iSDX can handle large topology IXPs, but it can only manage the limited prefixes of participants' policies. Therefore, reducing the forwarding table size and minimizing the forwarding table update rate in multi-hop IXP topologies are challenge in today's SDX.

2) ARP-PROXY

To exchange traffic in the IXP environment requires knowing the MAC address, and it uses the ARP protocol. In SDX architecture, the SDN controller works with a router server (RS) to ensure that BGP and SDN control planes can exchange the traffic flows to each other with a nominal delay. Most of the studies proposed architectures with the centralized ARP proxy, leading to delay in channel control and failure to all connection approaches such as TCP and BGP. The study implemented Umbrella[2], a mechanism that eliminates the need for location discovery in broadcast packets and renders active ARP-proxy used in earlier SDX designs unnecessary. The Umbrella design follows the complicated mechanism of broadcasting packets, so it needs a simpler and straightforward approach.

3) DISTRIBUTING FORWARDING RULES

In the distributed environment of IXPs, there are interconnected switches. Some of them are edge switches connected to members' routers, and others are core switches that connected edge switches. In this case, the SDX met a limitation related to distributing forwarding rules on the different switches. Similarly, the way to minimize the number of routing policies on various switches to reduce resource utilization. The ENDEAVOUR framework[4] proposed simplifying the distributing forwarding rules by installing routing policies only on the edge switches and frees the resources from core switches. This framework also suggested reducing the amount of routing policies installed in the edge switches by deploying the outbound policies on edge switches where member policy connected to and limit duplication forwarding state. The ENDEAVOUR used mechanisms that still utilize more resources to distribute forwarding rules and minimize routing policies.

4) LINK FAILURE

Link failure rerouting is simple in a single topology environment. It is more complex in a multi-hop topology environment because the failure might affect many switches and does not quickly recover from a failure as a single switch. Therefore, today's studies developed many mechanisms that tackle this aspect and proposed different approaches for this issue, but they do not overcome all problems and improve. The Umbrella[2] and ENDEAVOUR[4] proposed ways that tackle these challenges. Umbrella used the group fast failover to respond to the link failure. This mechanism is not a high-performance rerouting failure because it only monitors the status of ports and interfaces of the switches, and it is not considering other vital features. Simultaneously, the ENDEAVOUR enabled the approaches that can recover the failure quickly, but it might cause other problems such as the cost of switch memory and packet processing delay.

VII. CONCLUSION

Internet Exchange Point (IXP) is an integral element of the Internet ecosystem. IXP providers require to advance the scalability aspects and to solve the existing IXP challenges and inter-domain routing limitations. SDN has emerged to shape the network structural design and add the functionalities that enhance the inter-domain routing system. Then, SDN deployed on IXP brings to develop the new platform known as SDX. SDX develops the network providers in different aspects like security, privacy, and scalability. This paper focuses on the SDX scalability aspects to improve the management and operation of IXP operators and offer an excellent service to their network members. We argued many SDN- enabled models and approaches that solved many challenges of IXPs and network enterprises in different ways. These models facilitated the network operators to use SDN programmable fabrics and robust policies that enable multiple functionalities like controlling and efficiently forwarding traffic and simplifying the management services.

REFERENCES

[1] R. Bennesby, E. Mota, P. Fonseca, and A. Passito, "Innovating on interdomain routing with an inter-SDN component," in *2014 IEEE 28th International Conference on Advanced Information Networking and Applications*, 2014, pp. 131–138.

[2] M. Bruyere *et al.*, "Rethinking IXPs' architecture in the age of SDN," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 12, pp. 2667–2674, 2018.

[3] L. Barolli, *Web, Artificial Intelligence and Network Applications*, vol. 927, no. October. Springer International Publishing, 2019.

[4] G. Antichi *et al.*, "ENDEAVOUR: A scalable SDN architecture for real-world IXPs," *IEEE J. Sel. Areas Commun.*, 2017.

[5] A. Gupta *et al.*, "SDX: A software defined Internet exchange," *Comput. Commun. Rev.*, vol. 44, no. 4, pp. 551–562, 2014.

[6] L. F. C. Martins, I. Cunha, and D. Guedes, "An SDN-based Framework for Managing Internet Exchange Points," *Proc. - IEEE Symp. Comput. Commun.*, vol. 2018-June, pp. 996–1001, Nov. 2018.

[7] A. Gupta *et al.*, "An industrial-scale software defined Internet exchange point," in *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)*, 2016, pp. 1–14.

[8] R. Birkner, A. Gupta, N. Feamster, and L. Vanbever, "SDX-based flexibility or Internet correctness? Pick two!," *SOSR 2017 - Proc. 2017 Symp. SDN Res.*, no. i, pp. 1–7, 2017.

[9] J. Griffioen, T. Wolf, and K. L. Calvert, "A coin-operated software-defined exchange," *2016 25th Int. Conf. Comput. Commun. Networks, ICCCN 2016*, pp. 1–8, 2016.

[10] W. J. A. Silva and D. F. H. Sadok, "Control inbound traffic: Evolving the control plane routing system with Software Defined Networking," *IEEE Int. Conf. High Perform. Switch. Routing, HPSR*, vol. 2017-June, 2017.

[11] F. R. Rosa, "Internet Node as a Network of Relationships: Sociotechnical Aspects of an Internet Exchange Point," *SSRN Electron. J.*, pp. 1–19, 2018.

[12] J. C. C. Restrepo and R. Stanojevic, "IXP traffic: A macroscopic view," *Proc. 7th Lat. Am. Netw. Conf. LANC 2012*, no. Section 4, pp. 1–8, 2012.

[13] B. Ager, N. Chatzis, A. Feldmann, N. Sarrar, S. Uhlig, and W. Willinger, "Anatomy of a large European IXP," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 4, pp. 163–174, 2012.

[14] A. Basit, S. Qaisar, S. H. Rasool, and M. Ali, "SDN Orchestration for Next Generation Inter-Networking: A Multi-path Forwarding Approach," *IEEE Access*, vol. 5, no. c, pp. 13077–13089, 2017.

[15] W. J. A. Silva and D. F. H. Sadok, "A survey on efforts to evolve the control plane of inter-domain routing," *Inf.*, vol. 9, no. 5, 2018.

[16] D. Herrmann, M. Turba, A. Kuijper, and I. Schweizer, "Inbound interdomain traffic engineering with LISP," in *39th annual IEEE conference on local computer networks*, 2014, pp. 458–461.

[17] A. Basit, S. Qaisar, M. Ali, M. Naeem, M. Bruyere, and J. J. P. C. Rodrigues, "Interconnecting networks with optimized service provisioning," *Telecommun. Syst.*, vol. 73, no. 2, pp. 223–239, 2020.

[18] D. Ó Briain, D. Denieffe, D. Okello, and Y. Kavanagh, "Enabling models of Internet eXchange Points for developing contexts," *Dev. Eng.*, vol. 5, no. September 2020, p. 100057, 2020.

[19] M. Kende and C. Hurpy, "Assessment of the impact of Internet Exchange Points – empirical study of," no. April, 2012.

[20] T. Böttger *et al.*, "Shaping the Internet: 10 Years of IXP Growth," Oct. 2018.

[21] H. Kumar, "Re-architecting Internet Exchange Points for security and flexibility using Software Defined Networking Himal Kumar of the requirements for the degree of Master of Philosophy The School of Electrical Engineering and," 2017.

[22] M. V. B. da Silva, J. A. Marques, L. P. Gaspary, and L. Z. Granville, "Identifying elephant flows using dynamic thresholds in programmable IXP networks," *J. Internet Serv. Appl.*, vol. 11, no. 1, 2020.

[23] S. H. Warraich, Z. Aziz, H. Khurshid, R. Hameed, A. Saboor, and M. Awais, "SDN enabled and OpenFlow compatible network performance monitoring system," *arXiv*, pp. 1–10, 2020.

[24] T. Wolf, A. Nagutney, J. Griffioen, and K. L. Calvert, "Enhancing Interdomain Transport via Economic Software-Defined Exchange Points," *2019 Int. Conf. Comput. Netw. Commun. ICNC 2019*, pp. 473–479, 2019.

[25] C. Chen, B. Li, D. Lin, and B. Li, "Software-defined inter-domain routing revisited," in *2016 IEEE International Conference on Communications (ICC)*, 2016, pp. 1–6.

[26] Y. Wang, J. Bi, K. Zhang, and Y. Wu, "A framework for fine-grained inter-domain routing diversity via SDN," *Int. Conf. Ubiquitous Futur. Networks, ICUFN*, vol. 2016-Augus, pp. 751–756, 2016.

[27] P. Sermpezis and X. Dimitropoulos, "Can SDN accelerate BGP convergence?," *arXiv Prepr. arXiv1702.00188*, 2017.

[28] H. Kumar, C. Russell, V. Sivaraman, and S. Banerjee, "A software-defined flexible inter-domain interconnect using ONOS," *Proc. - Eur. Work. Software-Defined Networks, EWSDN* , vol. 2016-Octob, pp. 43–48, 2017.

[29] W. Xia *et al.*, "A Survey on Software-Defined Networking," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 1, pp. 27–51, 2015.

[30] J. Chung, J. Cox, R. Clark, and H. Owen, "FAS: Federated auditing for software-defined exchanges," in *SoutheastCon 2017*, 2017, pp. 1–8.

[31] J. Chung, H. Owen, and R. Clark, "SDX architectures: A qualitative analysis," in *SoutheastCon 2016*, 2016, pp. 1–8.

[32] M. Chiesa *et al.*, "Inter-domain networking innovation on steroids: Empowering IXPs with SDN capabilities," *IEEE Commun. Mag.*, vol. 54, no. 10, pp. 102–108, 2016.

ABDIJALIL ABDULLAHI received a B.Sc. degree in information technology and an M.Sc. degree in networking and data communication from SIMAD University, Mogadishu, Somalia, in 2014 and 2018, respectively, where he is currently pursuing the PhD degree with the National Advanced IPv6 Center (NAv6), Universiti Sains Malaysia (USM). His research interests include software-defined networking, inter-domain routing, and the Internet ecosystem.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3069808, IEEE Access

SELVAKUMAR MANICKAM is the senior lecturer at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. He received his Bachelor of Computer Science and Master of Computer Science in 1999 and 2002, respectively. He obtained his PhD from Universiti Sains Malaysia (USM) in 2013. His research interests are Internet security, cloud computing, IoT, Android and open source technology. He is an Executive Council member of Internet Society (ISOC), Malaysian Chapter and also the Head of Internet Security Working Group under Malaysian Research and Education Network (MyREN).

SHANKAR KARUPPAYAH is currently a Senior Lecturer and researcher at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. He obtained his B.Sc Computer Science (USM), Malaysia and the M.Sc. Software Systems Engineering (KMUTNB), Thailand. He obtained his PhD in 2016 from Technische Universität Darmstadt in the field of Cyber Security. His main research interests are P2P Botnets, Distributed Systems and Cyber Security in general. To date, he has authored and co-authored many articles in journals, workshops, and conference proceedings. He is also a reviewer in many esteemed network and security journals.