Hindawi
Journal of Computer Networks and Communications
Volume 2022, Article ID 3955800, 23 pages
https://doi.org/10.1155/2022/3955800

Review Article

Multidomain SDN-Based Gateways and Border Gateway Protocol

Hamad Saud Alotaibi, Mark A. Gregory, and Shuo Li

School of Engineering, RMIT University, Melbourne, VIC 3000, Australia

Correspondence should be addressed to Hamad Saud Alotaibi; s3388813@student.rmit.edu.au

Received 26 August 2021; Accepted 13 April 2022; Published 12 May 2022

Academic Editor: Ihsan Ali

The Internet consists of distributed and interconnected autonomous systems (ASs). The flexibility afforded by the Internet architecture ensures that timely changes to the network topology can occur without centralized control. The Border Gateway Protocol (BGP) is an Internet protocol that routes the Internet traffic and exchanges the information between AS. However, BGP version 4 (BGP-4) currently suffers from a limitation called "high convergence delay" while doing routing updates, which is a very common limitation, damaging the performance of contemporary IP networks. Software-defined networking (SDN) was conceived at the beginning of the 21st century, and over the intervening years, it has gained traction. This technology has significantly enhanced traffic control, management, and monitoring, particularly in data centres and enterprise networks. Challenges have been found including how to provide administrative control, security, management, and monitoring at domain boundaries while introducing the SDN paradigm. In multidomain SDN, BGP-4 is used to exchange the information and route the traffic between domains or diverse AS. In this review, an investigation is provided on using the SDN paradigm to enhance multidomain traffic management and control and to optimize BGP operation. A detailed insight is provided into the penetration of the SDN paradigm into modern networking architectures and how it may help in facilitating future research to improve BGP-4.

1. Introduction

The Internet consists of billions of network devices that are connected. It communicates with the aid of protocols that utilize reachability and routing information to facilitate traffic flow. Carrier and enterprise networks are identified as autonomous systems (ASs) that form separate domains on the Internet. The Border Gateway Protocol version 4 (BGP-4) is a systematic Exterior Gateway Protocol (EGP) that is organized to route the traffic across the Internet and exchange reachability information between ASs [1].

The Internet may be identified as a number of connected AS or domains that utilize heterogeneous network devices, including gateways, firewalls, routers, switches, and other devices. There are inherent differences in how networks may be constructed. For example, data centres (DCs) contain a dynamic network, typically located in the same facility, that can be used to form one or more ASs and domains or part thereof [2]. Carrier and Internet Service Provider (ISP) networks are often geographically dispersed and can be broken down into core, edge, and access networks. An AS is a group of interconnected network devices that are formed into a single administrative domain. An AS has an ID called the Autonomous System Number (ASN), which consists of a 16-bit value within the range 1 to 65535. The ASN is globally unique and is allocated by one of the five regional Internet registries that are authorized by the Internet Assigned Numbers Authority (IANA) [3]. An administrative domain is a grouping of network infrastructure devices that are controlled and operated by a single organization and may have one or more routing domains (Internet Protocol ranges). However, the routing domains cannot span more than one administrative domain.

BGP-4 is characterized as a distributed protocol that provides reachability and routing information exchange between AS. BGP-4 utilizes the shortest path vector protocol [4]. Challenges related to BGP-4 including improved functionality, flexibility, security, and the routing update convergence delay are under constant review [4–7]. Proposals to revise or replace BGP-4 found in the literature identify how important BGP-4 is to the operation of the Internet and it is the global nature of the Internet and the large number of legacy systems that may be the biggest impediments to BGP-4 being substantially upgraded or replaced.

The software-defined networking (SDN) paradigm is being applied to redefine network architectures and a study is underway that aims at applying this paradigm to improve how interdomain traffic flows are managed. By introducing SDN, the data plane can be formed by using low-cost standardized "white-label" boxes that function as data forwarding devices. The control plane is migrated to a new class of network devices, known as controllers, that can manage one or more data plane devices [8].

By adopting the SDN paradigm, the network implementation is simplified as the control logic can be modified based on the underlying network application and device requirements. The three SDN layers are control, application, and infrastructure. There are application programming interfaces (APIs) that have been implemented for operational activities. The APIs include eastbound, westbound, northbound, and southbound. The researchers have highlighted the benefits of SDN in different domains including cloud, IoT, and wireless networks. The authors in [9] have discussed the challenges and problems that can be solved by using SDN in wireless networking. The authors have highlighted the benefits of the standardized OpenFlow protocol. Challenges including traffic management, effective load balancing, and bandwidth utilization can be overcome by utilizing SDN [10].

SDN has been successfully introduced within data centres (DCs) and enterprise networks, and the rollout of SDN to other networks has increased in recent years. Studies and proposals for interdomain routing and control utilizing SDN have identified different approaches to the challenges related to managing administrative control, security, and privacy at AS domain boundaries. Wibowo et al. [11] studied how to utilize SDN to provide improved interdomain link performance and automatic provisioning in an SDN-based multidomain gateway. The authors of [12] provided a comprehensive review on large-scale SDN testbeds. Research has been carried out on how to apply SDN principles to counter the BGP-4 convergence delay when routing updates are applied at AS gateways. For example, the authors of [5] discussed how to obtain an optimal routing table utilizing BGP-4 for SDN networks by comparing the packet transmission latency. The authors of [4] measured the interdomain SDN performance based on network details, such as topology, network size, path or route, and nodes number in a study to identify the time needed to establish convergence after a routing update. The authors of [13] used SDN to improve the interior BGP-4 (iBGP) routing within the same AS and [14] utilized SDN-based domain federation to improve the end-to-end (E2E) Quality of Services (QoS). The authors of [15] used the SDN to enhance the multipath for the BGP protocol.

In [16], Gupta et al. introduced a new approach called (SDX) to handle interdomain routing allowing customized policies to control the way packets are managed. Using SDX, ASs can remotely control traffic, only within their purview. SDX has a policy compilation component that can merge policies to resolve conflicts and respond to the change of BGP-4 routing rules. In SDX, a centralized compression technique is used to minimize the size of the forwarding tables when combining participants inbound and outbound policies. It merges columns with similar SDN policies by specifying the minimum disjoint set. This technique reduces the forward table size but not to a level that can meet the performance requirements of large Internet exchange points. iSDX [17] is a distributed SDX that overcomes the scalability issues associated with large-scale implementations. It optimizes the data and control planes resulting in a reduction in the number of entries in a forwarding table when compared to the centralized SDX approach. The delay to compile the participants' policies is also reduced.

[18] presented a distributed multidomain SDN that is managed by multiple network service providers (NSPs). The proposed framework enables cooperation between NSPs, with each NSP fully controlling its internal network assets and providing inter-NSP services with QoS guarantees.

This enables end-to-end support to different service levels with the service provider and consumer residing in different domains.

There are several initiatives that were implemented before SDN to enhance network management. The earliest initiative in this context is known as Network Control Point (NCP) [19]. NCP was implemented by AT&T for telephone network management. The proposed methodology was limited and not scalable when the number of users of the network increased. A Path Computation Element (PCE) [20] architecture was proposed in the same context to achieve improved QoS. The proposed PCE architecture overcomes the drawback of traffic engineering (TE)-based methodologies. TE-based methodologies have numerous restrictions including high CPU utilization and restricted topology visibility; this topology restriction causes limited scalability. However, PCE overcomes these limitations. Another approach, known as Routing Control Platform (RCP) [21], was introduced to overcome the drawbacks, including complex configurations, limited resources for legacy routers, and no central control points. MBone [22] was another networking approach that was designed to manage bandwidth constraints for video conferencing traffic. However, MBone was deficient as it was not able to deal with large and complex networks with frequently changing topology.

Non-SDN techniques utilize the Interior Gateway Protocols (IGPs) to find forwarding paths for data packets within an AS. Examples of the most common IGP protocols are Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF). There are drawbacks to non-SDN-based network implementations. RIP was designed for smaller networks and is not scalable. Furthermore, the bandwidth required by RIP is high, while the convergence rate is slow due to new route discovery delays [23]. OSPF is based on intense information processing, as it keeps multiple copies of the routing information exchanged over a network. Due to this large amount of information, the memory requirement for OSPF is significant [24]. EIGRP has a slow convergence rate and is also not scalable, especially in the case of hierarchical routing [25].

In non-SDN-based networks, the traditional networking methods utilize complex approaches because the control plane and the forwarding plane are situated in one device, which can manually update the device configuration. BGP-4 affords numerous benefits. However, there are legacy issues. BGP-4 has been updated to overcome some of the issues and research continues. The authors in [19] introduced concepts that aim at minimizing the loops that may occur when using BGP-4 and IGP. SDN also provides dynamic programmability, a concept that permits real-time deployment and updates to overlay applications and services.

1.1. Research Motivation. This review aims at providing a comprehensive overview of existing techniques applied to multidomain gateways and BGP-4. It can be summarized as follows:

(1) The current SDN technology does not have a standard method for communication between controllers in an SDN-based multidomain network [11]

(2) The fundamental limitation of BGP-4 is the high convergence delay [4, 26, 27]

(3) BGP-4 is considered to efficiently transfer routing and reachability information, but it has limitations that affect service delivery and timely updates to routing tables [11, 26]

Therefore, this article aims at providing the research community with a wide review that can be referred to when determining future research directions. Also, it aims at providing a guide to open questions that should be solved to improve the operation of multidomain gateways and BGP-4.

The rest of this article is presented as follows. Section 2 shows an overview of BGP-4 and SDN. Section 3 provides a description of AS, including the types of AS, architecture, and operation. Section 4 provides a description of how BGP-4 is used to provide reachability and routing information. Section 5 provides an introduction to multidomain SDN-based gateways and how SDN can be used to enhance gateway operation. Section 6 provides a review on multidomain SDN-based gateways, and the challenges to be overcome are provided in Section 7. Discussion and future work are provided in Section 8, and conclusion is given in Section 9.

2. Overview

2.1. BGP-4 Overview. The Internet is a combination of the Internet backbone and interconnected core routers, name servers, and computer networks that are formed into AS. BGP-4 is a standard interdomain routing protocol, defined in (RFC4271) [28], that governs how AS exchange routing information. BGP-4 is influenced by the details specified in EGP (RFC904) [29] and fixes a number of issues in its predecessor BGP-3 (RFC1267) [30]. BGP-4 supports destination-based routing where packet forwarding depends on the destination IP address [28]. New features in BGP-4 include mechanisms for Classless Inter-Domain Routing (CIDR) supporting IP prefix-based advertising for a set of destinations. In addition, route aggregation is also supported for AS paths.

BGP-4 can behave in a nondeterministic manner in some cases as described by BGP-4 Wedgies (RFC4264) [31]. Such nondeterminism can be intended and predicted by network administrators, including selecting the longest-lived route. Unexpected multiple local policy interactions can lead to unintended nondeterministic outcomes, which can be acceptable if all stable routes are consistent with the intentions of the policy writer. However, a challenge arises when BGP-4 specifies multiple stable states for a single configuration state and includes states that are not consistent with the policy writer intention. A network administrator should try to avoid unintended nondeterminism leading to unintended states by deliberate service disruption, which includes removing forwarding traffic routes and re-advertise routes to reach an intended BGP-4 state. Griffin and Huston [31] discussed how an intruder can exploit this issue to get the network forwarding configuration into an unintended nondeterministic state. This could lead to a possible inconsistent and undesirable state.

Traffic latency, which is the packets traveling time while traveling from any source to any destination, is affected by the path determined by BGP-4 at gateways along the route. The efficiency and effectiveness of BGP-4 have a direct impact on traffic flow and the cost associated with network operation. Network congestion or incorrect paths can result from invalid BGP-4 routes being advertised. BGP-4 updates the routing table when an update message is received that includes changes to the reachability and routing information used to represent the neighboring network topology. The time taken by BGP-4 to update the routing table is affected by the complexity of the best path identification process and the neighboring network topology. The convergence time [32] is the gap time between when the router receives an update and stable routing with the update incorporated. Convergence is an important concept for dynamic routing within an AS, as it identifies that a set of routers within the Internet work has the same network topology. Interior protocols, for example, RIP, OSPF, and EIGRP, rely on convergence to operate correctly. The Exterior Border Gateway Protocol (eBGP) operates without achieving convergence across all gateways as the Internet is too large for convergence to be achieved [33].

2.1.1. BGP-4 Operation. EBGP uses the concept of sessions to support communication between different ASs. BGP-4 sessions must be established not only between routers within the same AS but also between different eBGP routers located in the different AS. A router located in *AS1* that sends traffic to a router in *AS2* advertises its routes to the gateway router in *AS1* [35]. The routing information will then be exchanged with the gateway router in *AS2*. It is at this point that the edge router in *AS2* will pass the routing information to the destination router in *AS2*. Eventually, the communication process can start between the source and destination routers. Figure 1 illustrates how the BGP-4 is enabled in a network.

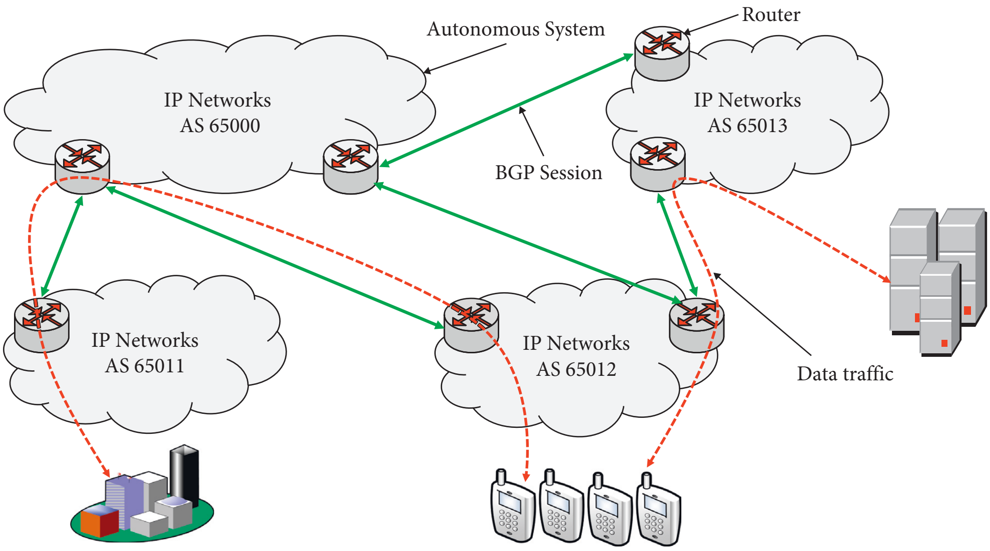

Figure 1: Enabling BGP-4 in a network [34].

From a logical point of view, it may appear that the creation of eBGP peers occurs between two routers; the reality is at least three physical routers are required. As illustrated in Figure 2 [35], the *AS1* router must advertise its route to *AS2* router, which is a gateway device. In this context, *AS2* contains three different routers, that is, *R1*, *R2*, and *R3*. Each of the three routers must be provided with the AS-PATH from the router in *AS1* [36]. The AS-PATH parameter is essential, because it helps to eliminate the probability of loopback occurring. It also acts as a hop count metric that determines the length of the route upon which eBGP packets will be propagated. EBGP routing and configuration also require the next-hop count to include each neighbor within and across AS.

EBGP, similar to BGP-4, faces challenges that are associated with peering and prefix management. EBGP routers require accurate prefixes to optimize routing performance and a resource management allocation issue can occur when an iBGP router obtains new prefixes. The readvertisement of the new routing rules to eBGP routers across the network places a burden on available resources. The process not only consumes network resources but also slows the overall network performance. Other eBGP challenges include load balancing, security, route flapping, scalability, and configuration errors [37].

BGP-4 utilizes several attributes, which are the information that attaches in the BGP update message, to control the selected best path [38]. These attributes are called community attributes, and they consist of four types: well-known mandatory, optional transitive, well-known discretionary, and optional nontransitive. AS administrators are responsible for extracting the community attributes and forwarding the information to the peer routers [27].

2.1.2. BGP Convergence Time. BGP-4 convergence delay occurs for two reasons: building the routing table after route initialization and when routers update their routing tables after changes to the network topology. Changes in the network topology occur due to physical link changes, including additions and failures, and routers are added or removed or through changes to the network prefix. Networks are inherently unstable, causing AS to withdraw previous announcements and best path searches, and announce them again. This is referred to as BGP-4 convergence. According to [39], BGP-4 convergence is becoming a huge challenge for Internet connectivity, and with the increasing rate at which the Internet is growing, BGP-4 convergence delays are growing.

Industrial standards stipulate that the average BGP-4 convergence time should be maintained within a 60–180-second timeline [36]. The timeline refers to the amount of time in which the BGP-4 KEEPALIVE messages should be advertised to network routers. In any case, a BGP-4 convergence time beyond the stipulated limited can be problematic to routing efficiency and eventually to network performance [40]. By default, the time for KEEPALIVE messages is set at 60 seconds, while that for the HOLDTIME is 180 seconds. The time settings are essential since they determine the average convergence time for the BGP-4 routers. The time for the KEEPALIVE messages should be set so that the BGP-4 peers are able to receive the advertised messages before the expiry of the HOLDTIME. The maximum KEEPALIVE message interval should be one-third of the HOLDTIME [36]. This means that a BGP-4 peer sends at least three KEEPALIVE messages before the expiry of the HOLDTIME. The time for KEEPALIVE messages should be set to the minimum possible and should not exceed the 60-second limit. A lower time for KEEPALIVE messages typically results in faster BGP-4 router convergence [41]. There is a significant difference between having time for KEEPALIVE messages of 1 second and 30 seconds.

Maintaining the HOLDTIME at 180 seconds not only helps to improve the convergence time but also aids with fault reduction. In the event that one router within the network fails, it will take a maximum of 180 seconds for all routers within the network to receive KEEPALIVE messages before

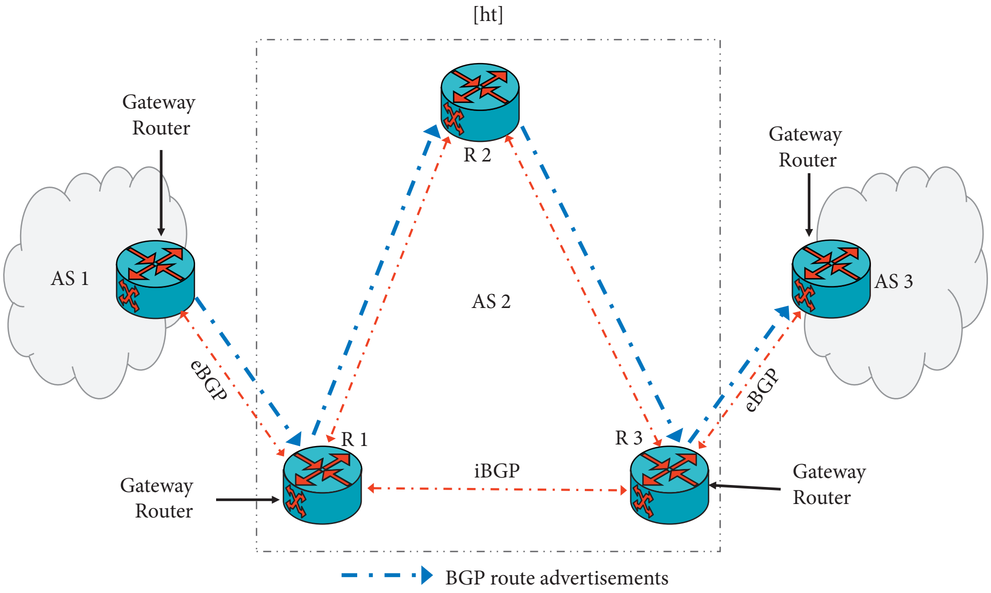

Figure 2: eBGP route advertisement [35].

the BGP-4 session can expire. Figure 2 shows how BGP-4 convergence works and the need to maintain the KEEPALIVE messages within 60 to 180 seconds. For instance, if router *R1* goes into a failure state, then the other routers within the network should be notified within a maximum of 180 seconds. This is because the duration for the KEEPALIVE messages in each router is set at a maximum of 30 seconds [36].

2.2. SDN Overview. The SDN paradigm indicates that the data and control planes separate from each other, with the control plane moved into new network devices known as controllers. A standardized protocol known as OpenFlow passes flow messages between controllers and SDN-enabled data forwarding devices (switches) [42]. Essentially, SDN is associated with two major functions: network control and traffic forwarding. The two functions are accomplished using a dynamically programmable interface and control plane. SDN utilizes network intelligence to ensure that the control of the network is managed by the centralized controllers.

2.2.1. SDN and Legacy Networking Comparison

(a) Legacy Networking. In legacy networking, the data and control layers are tightly integrated on the same network devices (see Figure 3). When a forwarding policy has been set in the network devices, it can only be changed by modifying the configuration of all devices that have been affected [43]. This procedure consumes time and limits the scalability and the flexibility needed to make changes to network configurations due to changing circumstances. Over time, the complexity of legacy networks has increased, adding entropy to the environment, and making the task of reacting to changed network conditions more difficult than reasonable.

(b) SDN. SDN separates the data and control planes with the goal to provide programmatic automated control, provisioning, and policy-based management of network resources. SDN enables logical centralization and makes it easier to create new abstractions and to introduce them into the network [44]. The SDN controller provides flow control and management by using the OpenFlow protocol to pass flow messages to data flow devices, for example, switches. OpenFlow [45, 46] was developed as a collaboration project between Stanford University and the University of California around 2008 [47]. SDN-based networks utilize one or more controllers to provide the flexibility and scalability needed to manage flows moving between OpenFlow compliant switches and routers [48, 49]. The programmatic centralized nature of SDN permits new applications and services to be deployed or upgraded at any time. The increased network awareness and flexibility offered by SDN lead to an improvement in network resource utilization. The SDN architecture is shown in Figure 4.

2.2.2. SDN Architecture. The SDN architecture contains three layers, with each layer utilizing an interface to adjacent layers, as shown in Figure 4. The interconnection between the brain of the network "controller" and flow devices is known as the southbound interface. The OpenFlow protocol is used to standardize message transfer over the southbound interface.

(a) Data Layer. The data plane layer contains the network infrastructure, including, gateways, switches, routers, and wireless access points. Management is needed to set up network elements and assign resources. The southbound interface is responsible for flow-related messages passed between the control and the data layers [50].

(b) Control Layer. The control layer is responsible for network logic; it uses the south and north interface to program the network [50]. The control plane is in a layer, and the data

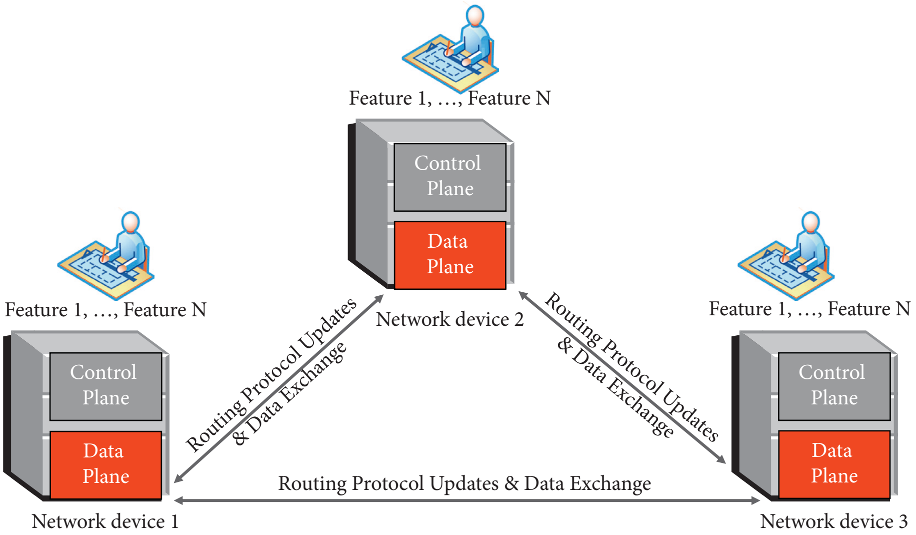
Feature 1, ..., Feature N
Control Plane
Data Plane
Network device 2
Feature 1, ..., Feature N
Control Plane
Data Plane
Network device 1
Feature 1, ..., Feature N
Control Plane
Data Plane
Network device 3
Routing Protocol Updates & Data Exchange
Routing Protocol Updates & Data Exchange
Routing Protocol Updates & Data Exchange

Figure 3: Traditional network architecture.

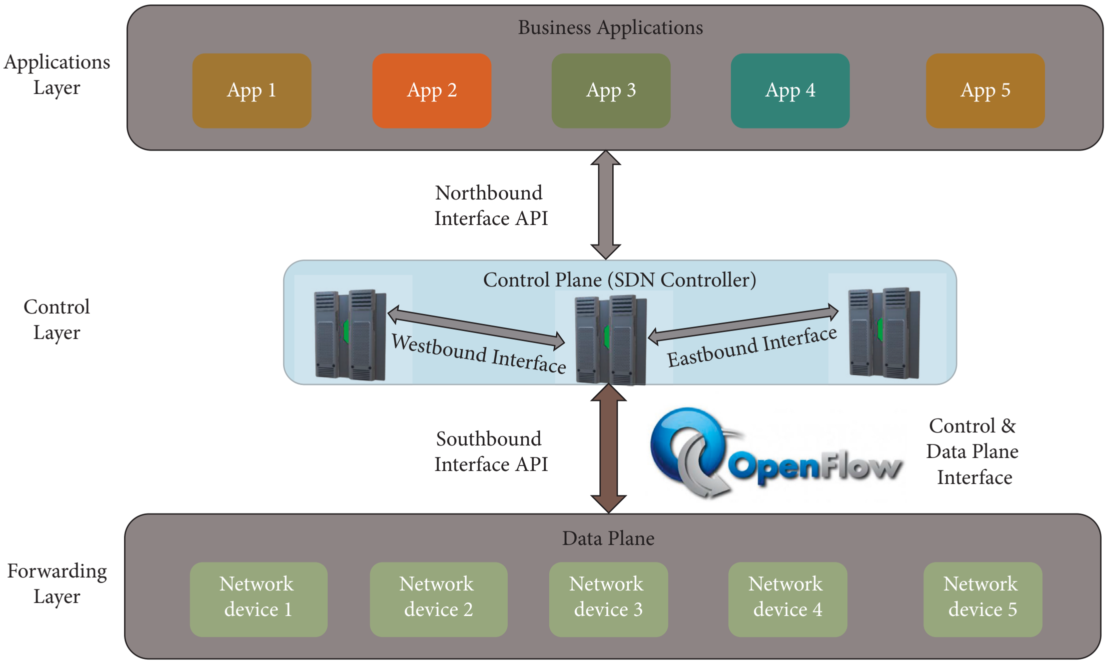

Figure 4: SDN network architecture.

plane is in another different layer and is typically considered to be logically centralized. It can be physically decentralized or centralized, consisting of one or multiple controllers. These controllers manage and control the entire network infrastructure. Nearly all forwarding decisions depend on the controller [51].

(c) Application Layer. The management function, found in the application layer, is responsible for coordinating the service level agreements and contracts that are enforced by the control layer. The application layer provides an overlay environment that enables third-party providers to develop and offer network control and management-related applications and services. This layer is connected to the control layer through nonstandardized APIs known as the northbound interface of the control layer [52].

(d) Southbound Interface (API). The southbound interface utilizes OpenFlow to provide a standardized protocol that transfers flow control messages between the control and the forwarding layers. The primary objective of southbound communication is to manage and monitor the network infrastructure, including gateways, routers, and switches [53].

(e) Northbound Interface (API). The primary function of this interface is to connect the controller with overlay applications and services. The northbound interface API is third-party application and service providers are required to tailor

their solutions for the different controllers in use within networks.

The overlay applications and services provide network management and monitoring capability to manage network resources, monitor traffic flows, and optimize network performance. Functions such as security, routing, reachability, loop avoidance, and path computation can be provided by applications and services using the northbound interface API [60].

(f) Westbound and Eastbound Interfaces (API). For the westbound and eastbound interfaces, standardized protocols have not been defined. However, in the distributed controller design, the eastbound interface API can provide communication between controllers. The SDNi protocol [54] has been proposed as one means of communicating between controllers. The westbound interface is used for communication between SDN network routers and traditional network routers. The proposed approaches for the westbound interface include RouteFlow [61] and BGP-based Transition to SDN (BTSDN) [62].

(g) SDN Protocols. A summary of the existing protocols used in the SDN architecture is provided in Table 1 [63].

2.2.3. SDN Controller Design. SDN controller is the intelligence brain of the entire network. It has the network interface that programs and configures the network [50]. In this layer, the concept of "network operating system abstraction" is introduced, which is used to control the underlying hardware. Nearly all forwarding decisions are dependent on the controller [51].

Scalability is an essential problem in the deployment of SDN controllers, especially in large networks that have multiple data planes. Two approaches are used to implement the design of SDN controllers to accommodate the needs for scalability, availability, and efficiency [64]. Figure 5 illustrates the difference between a single-controller approach and a multicontroller approach, and below are some descriptions for each approach.

(a) Single-Controller Approach. This approach uses a single controller within the SDN architecture. It is the traditional approach of implementing SDN controllers although it is no longer favored due to the fact that it is not reliable and vulnerable to security breaches. The single-controller approach requires the use of multithreaded hardware to ensure that performance overhead is reduced. Nonetheless, the single-controller approach introduces a single point of failure and cannot accommodate scalability as the increase in network size.

(b) Multicontroller Approach. This approach is designed to cater for the limitations found in the single-controller approach. In this context, multiple controllers are physically or logically distributed.

(1) A multicontroller approach that is physically distributed but logically centralized: There is a single central controller that has full control over the entire network [53]. The controllers in the network assume equal responsibility and are synchronized accordingly for effective information sharing. However, if the single central controller fails, the network performance will degrade.

(2) A multicontroller approach that is both logically and physically distributed: Means that each controller can manage its own resources [65].

The physical distribution of SDN controllers can have an arrangement whereby the controllers are positioned on a single level. That means each controller maintains a partial view of the assigned portion of the network [45]. A vertical or hierarchical multicontroller architecture means that the controllers are positioned in multiple levels within the controller plane. Therefore, the controllers can perform different functions and can make independent decisions depending on the corresponding virtual view of the network.

The control layer refers to the various controllers that utilize a Network Operating System (NOS)-based platform, for example, Ryu, POX, and NOX [66]. Applications such as a load balancer and firewall are grouped under the application layer. SDN controller features include the following:

(1) Architecture and design axes

(2) East/Westbound APIs

(3) Programming languages

(4) Support to OpenFlow in the southbound interface

The architecture and design axes determine a distributed or centralized design that offers higher performance and flexibility to the traffic. The east-/westbound APIs include data importing and exporting between controllers, notification and monitoring capability, and models for data consistency algorithm. Programming language, on the other hand, offers good memory management, fast access to memory, low learning curve, multithreading, and interoperability [67].

2.2.4. SDN Controllers' Comparison. SDN can be designed with some different controllers; The SDN controllers are summarized as follows:

(1) NOX controller: It is written using the C++ programming language, and its performance is speedy. The controller has an Open/Flow ratio of 1.0 to 1.3, while it has no BGP-4 library or MPLS library [66].

(2) POX controller: It is written using the Python programming language, and its performance is slow. Its OpenFlow is 1.0, and it has no BGP-4 Library. It, however, has an MPLS library [68].

(3) Ryu controller: It is also written using the Python programming language, and its performance is slow. It features both BGP-4 and MPLS libraries [66].

(4) ONOS controller: ONOS stands for Open Network Operating System. It is a leader among SDN controllers and can play a role in developing next

Table 1: Other SDN-related protocols.

Protocol	Key features
OpenFlow protocol [45]	It has an interface for communication between forwarding and control planes in the SDN architecture (southbound interface).
SDNi [54]	A message exchange protocol that defines the exchange of information among SDN controllers in eastbound/westbound interfaces in various domains.
OVSDB [55]	The primary function of the open virtual switch database management protocol is to manage and control the open virtual switch, which helps to automate the network.
OFCONFIG [56]	The OpenFlow configuration and management protocol include a set of instructions that defines how the OpenFlow controller accesses configuration settings from the OpenFlow switch.
NETCONF [57]	Network configuration protocol provides a mechanism for the configuration, management, retrieval, and uploading of data for the new network device.
RESTCONF [58]	Representational state transfer configuration protocol, which is similar to NETCONF, but it uses HTTP to perform CRUD operations in a data store defined in the YANG data modelling language.
I2RS [59]	Interface to the Routing System Project is an IETF project; its main features involve splitting the routing decisions between the user and the con-troller.

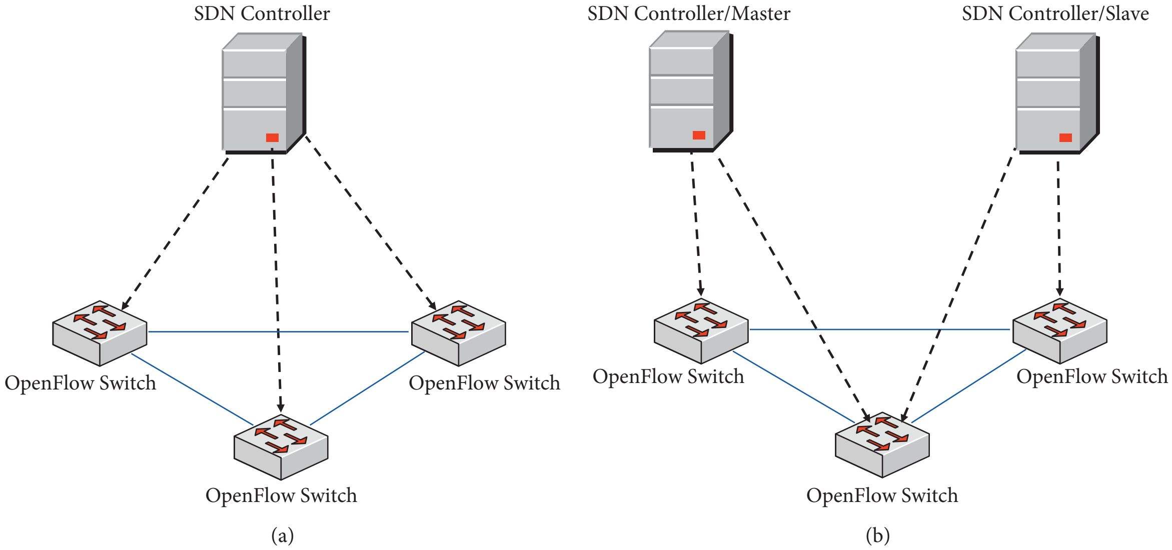

Figure 5: Single and multicontroller approach [11].

generation SDN/NFV solutions. It equally forms the basis for proprietary controllers, like Huawei [67].

(5) ODL controller: Its flow-rate latency performance triumphs over what obtains in the ONOS controller. Generally, it is not as robust as the ONOS controller [68].

3. Autonomous Systems

An AS refers to one or more networks that are administered by a single organization. An AS can also be regarded as an administrative domain that defines how routing is carried out on the Internet. Consequently, an AS can also be regarded as a routing domain. A common network administrator performs the control functions of an AS on behalf of other organizations [3]. A good example of an AS is an ISP. Each AS must be assigned a unique ASN that assists in the routing process when using BGP-4. There are four categories of AS connections, which are provided in the next subsections, where the term "home" in the next context refers to a network or a computer system.

3.1. Single-Homed AS. A single-homed AS is connected to a single network (see Figure 6), and routing policies are restricted to the connected network. A network connected to one service provider is the best example of a single-homed AS. It is worth noting that a single-homed AS does not require an ASN. It has the added advantage of being cost-effective, but it does not create room for redundancy because of the single point of failure [70].

3.2. Dual-Homed AS. A dual-homed AS contains two connections to a service provider network, and each configuration has its own routing prefixes, as shown in Figure 7. A dual-homed AS can contain a primary and a secondary connection; in most cases, the secondary connection provides redundancy. The design of a dual-homed AS includes two routers at the edge, with one on stand-by, to provide the redundancy required by the organization's policies [69].

3.3. Single Multihomed AS. A multihomed AS is connected to one or more external AS (see Figure 8). Each AS contains

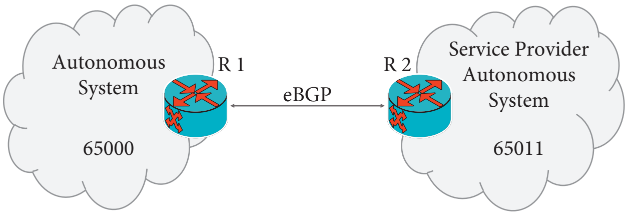

Figure 6: Single-homed AS [69].

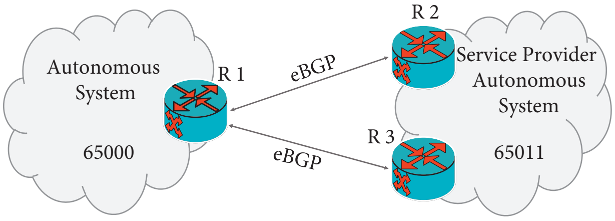

Figure 7: Dual-homed AS [69].

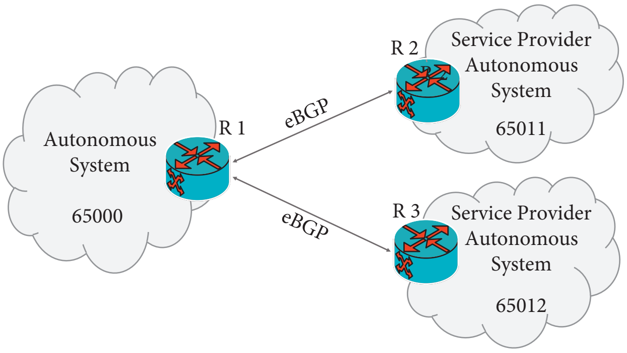

Figure 8: Multihomed AS [69].

its own routing policies, and thus, an organization with a multihomed AS defines routing prefixes for each AS. The advantage of this approach is to maintain edge connectivity in the event that one AS connection fails and to optimize traffic flows. A multihomed AS does not allow network traffic from another AS to pass through it; however, hosts within the AS are able to route traffic to other AS [69].

3.4. Dual Multihomed AS. A dual multihomed design differs from dual-homed in that each of the connections has dual links, as shown in Figure 9. In other words, an organization is connected to two ISPs using two connections for each ISP. This arrangement means that the routers have redundancy, but it is costly to implement and maintain [69].

4. Administrative Domains

An administrative domain is an entity whose function is to control and monitor an AS. However, an AS is a collection of hardware devices and connected networks controlled and managed by a single administrative domain [71]. There are two types of Internet routing used to support administrative domain connectivity.

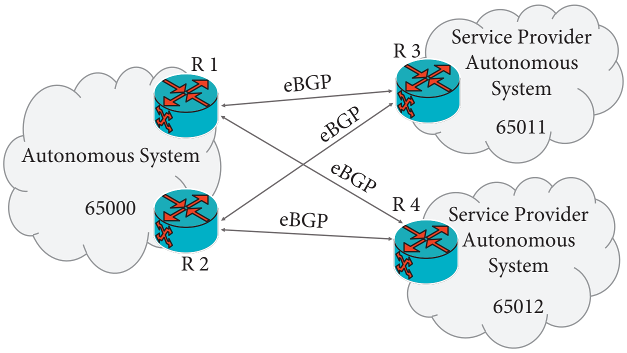

Figure 9: Dual multihomed AS [69].

4.1. Intradomain Routing. Intradomain routing is used to define how network traffic is exchanged within an AS. Intradomain routing is performed using a variety of IGPs. This form of routing uses link states and the distance vector algorithm to support routing functions [72].

4.1.1. Communication Protocol. The communication protocols used in intradomain routing are categorized based on the type of routing algorithm used. In this context, the routing protocols might use the distance vector space algorithm or link states. The most common IGP protocols are IGRP, EIGRP, RIP, and OSPF [73].

4.1.2. Topology Properties. The intradomain topology includes edge border router connections to boarder routers on the edge of other domains [70]. As illustrated in Figure 10, the iBGP represents an intradomain connection between routers within the same AS. The intradomain topology is characterized by multiple domains, with each domain hosting its own network and routers. The routers within the same AS communicate with each other using IGPs. In the majority of cases, intradomain routing supports AS with up to 100 discrete networks, and thus, it is generally implemented as a stub.

4.2. Interdomain Routing. Interdomain routing is applied across AS or separated domains and can be controlled by one or more administrative entities. Each AS or domain is required to have its own routing policies.

4.2.1. Communication Protocol. The communication protocols are used in this routing type for exchanging information with different ASs. These protocols use both classless and classful routing. Notable communication protocols in interdomain routing include eBGP [1].

4.2.2. Topology Properties. The main characteristics of an interdomain topology are the use of edge routers to connect multiple AS, thereby forming the Internet. Edge routers provide connectivity between one AS and another. Moreover, an edge router supports connections to multiple domains or AS. The interdomain topology is composed of a

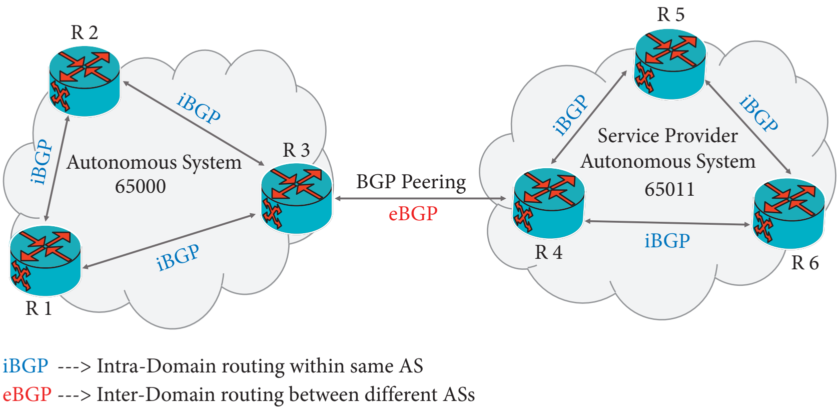

Figure 10: Example of an intra- and interdomain routing topology.

backbone, regions, and stubs. A backbone is the highest level of organization and includes national or international coverage. A region includes ASs that cover metropolitan areas and may include subregions known as areas. A stub sits at the lowest level of the interdomain topology and typically covers a campus-wide domain [74]. ISPs or enterprise organizations can be connected to stubs using direct links. As illustrated in Figure 10, the interdomain topology represents the eBGP connection between two different AS.

5. BGP-4 for Multidomain

BGP-4 supports the exchange of routing and reachability information using what is known as Network Layer Reachability Information (NLRI) [69]. It is a robust routing protocol credited to the evolution of SDNs. Similar to ForCes [75], BGP-4 provides support for network programmability that makes it possible to use encoded policies for the purposes of network filtering and forwarding. SDN controllers can use BGP-4 to push TCP packets. In essence, BGP-4 can be viewed as an enabler of SDN primarily because it takes routing instructions from the SDN controller and implements them throughout the centralized network [63].

5.1. BGP-4 Peering. Adjacent routers or gateways that exchange BGP-4 messages by initiating a BGP-4 session that runs over a Transmission Control Protocol (TCP) connection are peered. The TCP connection offers the perception of a transmission channel that dependably provides an ordered flow of bytes, eliminating the requirement for BGP-4 to deliver error correction or retransmission. The peering process involves a series of steps that require both peers to exchange messages to create a BGP-4 peering session. Figure 11 illustrates how BGP-4 peering is established between the two AS [27]. BGP-4 peering can occur between two routers located within the same AS in which case it is referred to as internal BGP-4 or iBGP. Similarly, the peering process can take place between peers located in different ASs, which is referred in such case to as external BGP-4 or eBGP. The peering process can occur between edge or border routers; such routers are known as eBGP routers. iBGP peering is achieved through interconnection using intermediate routers. The main differences between eBGP and iBGP occur during the process of selecting paths or routes [1]. Further comparison between iBGP and eBGP is summarized in Table 2. In eBGP peering, the routes are distributed to all iBGP routers inside the AS, as well as other eBGP routers belonging to other ASs. Similarly, an eBGP router is capable of learning all the routes associated with the iBGP routers within the AS. Additionally, iBGP peers regularly update the eBGP peer of any changes in routing rules. In both iBGP and eBGP, route propagation is controlled using route maps. In this context, route maps are comprised of a set of rules that contain detailed instructions, which follow the information stored in the routing table.

5.2. BGP-4 Messages. BGP-4 sessions are created and terminated using a series of BGP-4 messages. The message exchange process is essential, because it helps to ensure that BGP-4 peers are able to exchange information without disruption. BGP-4 messages are mainly grouped into four categories: OPEN, UPDATE, KEEPALIVE, and NOTIFICATION [1]. The OPEN message of the BGP-4 is initiated in an established session after the handshake exchange process between two peers. The OPEN message holds the ASN belonging to the initiating router, the version number of the BGP-4 protocol, the BGP-4 identifier, and HOLDTIME. The identifier is 32-bit that contains the router ID with the possession of the advertised prefixes. HOLDTIME is designated in seconds and is provided for each BGP-4 peer, stipulating the amount of time a neighbor can keep the session alive. The UPDATE message, as the name suggests, provides routers with any changes to the route information. It also extracts all previously advertised messages and can also act as a KEEPALIVE with the intention of eliminating unnecessary traffic. The KEEPALIVE message is periodically sent by the router if it does not receive an UPDATE message. Normally, the KEEPALIVE message contains a default value, often set at one-third of the HOLDTIME. Cisco routers, for instance, have a HOLDTIME of 180 seconds, meaning that the KEEPALIVE message has a default value of 60 seconds [36]. Finally, the NOTIFICATION message is issued by the router when there is a problem with the BGP-4 session. The NOTIFICATION message might be issued, for

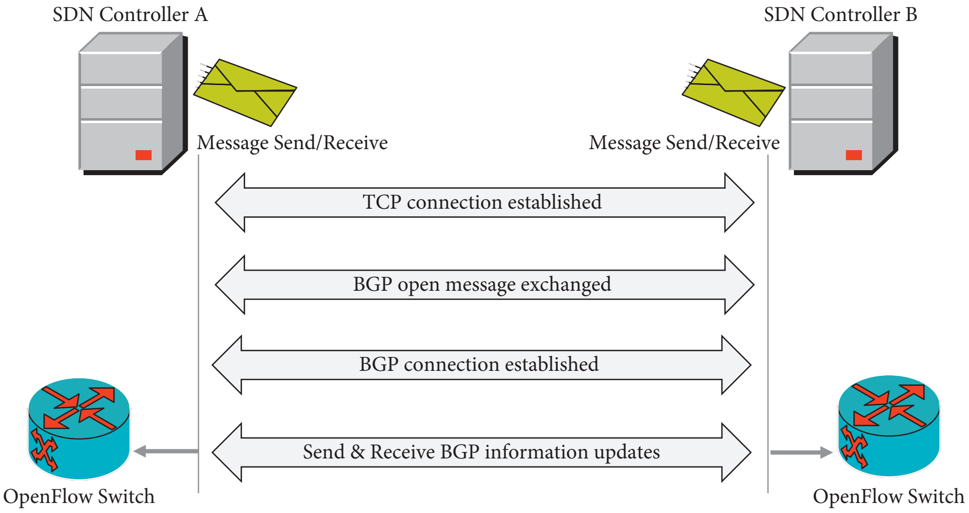
SDN Controller A
SDN Controller B
Message Send/Receive
Message Send/Receive
TCP connection established
BGP open message exchanged
BGP connection established
Send & Receive BGP information updates
OpenFlow Switch
OpenFlow Switch

Figure 11: BGP-4 session establishment peering in multidomain SDN [27].

Table 2: Comparison between iBGP and eBGP [74].

Aspect	iBGP	eBGP
Peering	Occurs in routers within the same AS	Occurs in routers in different AS
Advertisement for routing information	Cannot be advertised back to another iBGP peer	Can be advertised back to an eBGP or iBGP peer
Topology	Full mesh required	Full mesh not required
Attributes	Passed to iBGP peers	Passed to eBGP peers but not iBGP peers
Prepending AS path	Not prepended during iBGP route advertisement	Prepended during eBGP route advertisement
Administrative distance	Distance of 200	Distance of 20
Next hop characteristic	Changed to match the local router during route advertisement	Remains constant during route advertisement
TTL	TTL = 225	TTL = 1, and thus, it is assumed that peers are directly connected
Prevention of loopback	Utilizes BGP-4 split-horizon	Uses the AS path for prevention

instance, when the BGP-4 session suddenly stops or resets with the expiration of HOLDTIME, or when there is a change in the capacity of a neighbor.

5.3. BGP-4 as an SDN Protocol. In SDN applications, as shown in Figure 12, BGP-4 is used as a hybrid controller protocol [76]. According to [77], the proponents of SDN capitalized on the use of OpenFlow to separate the data and control layers in a network. Network operators have supported the SDN architecture in part due to other benefits including programmability and operational agility.

SDN combines the roles of BGP-4 and NETCONF to enhance support for SDN in multivendor environments [4]. It is further argued that BGP-4 provides an alternative to OpenFlow for border networking because it operates in higher state levels, for example, virtual (L3) and physical (L2) topologies and security policies. Therefore, although BGP-4 does not manage flows directly, it indirectly addresses configuration issues and controller interoperability. Controllers can operate using multiple abstraction levels that range from bridging and routing topologies to those that are flow-based [13].

6. Multidomain SDN-Based Gateways

Multidomain SDN is an approach that involves the implementation of SDN in large networks, such as AS. It is an effective approach, because it assists in the control and administration of large enterprise networks, which would otherwise be difficult to implement using manual administration. In the same context, the implementation of SDN in large networks improves the management, monitoring, and control of Internet gateways. Most ISPs are comfortable with BGP-4 in their SDN applications; however, the function of BGP-4 in SDN network applications has not demonstrated enough success to be widely accepted. For instance, data centre users are focused on convergence times, which tend to be undesirable for BGP-4, and therefore, consider BGP-4 to be an SDN protocol for wide-area networks (e.g., SD-WAN). A role as an SDN protocol for applications inside data centres has tended to be rejected. Thus, the issue of convergence time is a major challenge to applications of BGP-4-based SDN in local area networks [4].

The role of the BGP-4 protocol as an optimization capability in wide-area networks means BGP-4 is a facilitator of the growth and benefits of WAN applications. Through

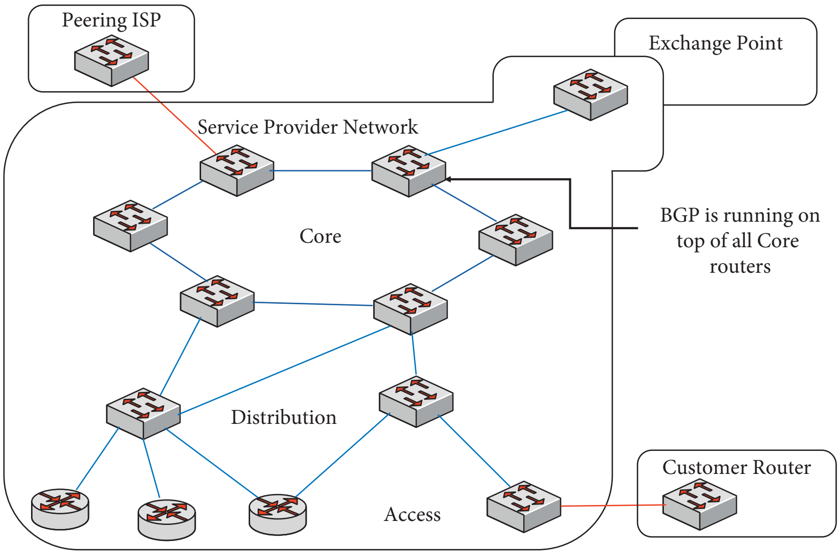

Figure 12: BGP-4 as a hybrid controller protocol for SDN [76].

WAN orchestration and optimization, BGP-4 has enhanced traffic engineering decision-making through useful analysis of customer traffic profiles [13]. Such analysis is efficiently performed using the visibility of customers, IGP domains, and traffic engineering databases, all enabled by BGP-4. Several recent studies have discussed the newest extension of BGP-4 NLRI, known as BGP-4-LinkState, and recommended it as the industry standard for network protocols required for aggregating the network topology information necessary for PCE computation [78]. However, using BGP-4 for multidomain SDN-based networking has some shortcomings that affect network performance and is, therefore, subject to current research. The following subsections include the literature review and recent research on the knowledge gaps.

6.1. Literature Review. Multidomain SDN-based gateways suffer from several challenges, such as the lack of a standardized protocol for control message passing [11]. Moreover, the proposed multidomain SDN communication approaches, for example, DISCO [79], INDOPRONOS [27], and EW-Bridge [80], were mainly focused on the connectivity and reachability but not QoS. Moreover, BGP-4 suffers from a high convergence delay [11, 79, 80] and a lack of focus on end-to-end service delivery [27, 80]. Research has been carried out on BGP-4 performance-related issues. Several methods have been proposed on how to enhance BGP-4 performance and to reduce the convergence delay. Research has also been carried out into SDN technology and how to incorporate SDN into modern network architectures. However, there exists a knowledge gap on how to apply the SDN paradigm to interdomain traffic control and service management. There remains an opportunity for further research into how the SDN paradigm might be used to enhance the efficiency of BGP-4 to achieve a highly reliable, optimized, and effective routing protocol. This research is investigating the shortcomings of the BGP-4 protocol when implementing multidomain SDN-based gateways. We recently proposed a framework called the Multi-State BGP-4 Manager [81]. Research to improve this framework is ongoing.

6.2. Previously Proposed Mechanisms for Applying SDN to Gateways. Past studies have focused on BGP-4 convergence issues. The studies present multiple routing approaches with reduced convergence time. Evidence suggests that BGP-4 is efficient in reachability or robustness, but lacks optimality for end-to-end bandwidth. Even with corrective measures, efficiency is still affected by the destination-based routing of BGP-4, for example, next-hop targeting [15].

The authors in [27] proposed a framework to exchange information in multidomain SDN called INDOPRONOS that aims at reducing human intervention when configuring the network device. The authors use the BGP-4 protocol in their proposed framework, as illustrated in Figure 13. Communication performance was evaluated and focused on the following parameters throughput, average packet loss, roundtrip time, and bandwidth, and there were measured from one network to another before and after the automated provisioning. The convergence delay of routing the traffic from a link to another was 56 seconds. The limitation of the INDOPRONOS framework remains the fundamental limitation of the BGP-4 protocol, the convergence time. Shortening the convergence time could help with improving provisioning performance [27].

The authors in [5] compared latencies when selecting the most satisfactory route to a destination. In the proposed system, the need for route optimization is detected if there is a neighbor on the route that is not the next hop. For identifying the connectedness of an AS neighbor, BGP-4 injects the shortest route to the AS using the AS IP address. In this manner, the latencies are reduced, which also shortens the convergence delays. This particular approach uniquely represents the readiness for the scenario of SDN

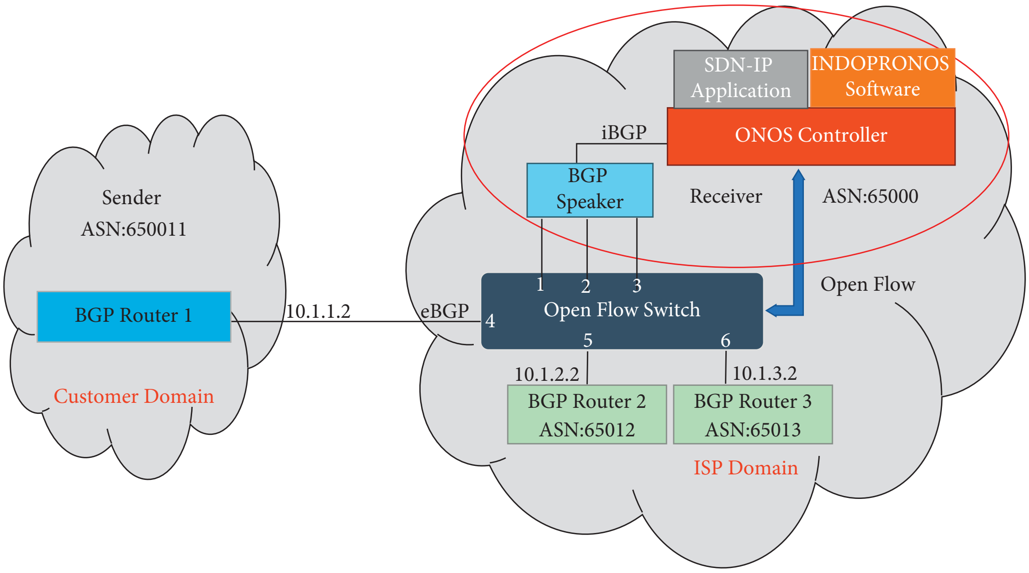

Figure 13: INDOPRONOS framework [27].

failure; for example, the time taken in making new routes does not affect the availability of the route, as nonoptimized routes are continually announced [5].

The authors in [4] developed a framework in an SDN environment to evaluate interdomain routing performance. The proposed model follows the assumption that each node of the network is acquainted with a minimum of one BGP-4 route that approaches every other node in the SDN cluster. In this manner, a particular node (e.g., the source node) initiates a change in routing, either in terms of announcing a new IP prefix or withdrawing from an existing one. Every node reflects the responsiveness to the change in the network on receiving the BGP-4 update in terms of installing a path in its Routing Information Base (RIB) for the new prefix.

Besides interdomain SDN centralization, considerable research is also found on the multipath routing of BGP-4 using SDN. [15] used the SDN to investigate BGP-4 routes and proposed an effective tunnel-based multipath BGP-4 (ETMP-BGP) to provide an end-to-end communication between multidomain and multi-AS (see Figure 14). This resulted in an improvement in average congestion of 86% compared to BGP-4; other schemes improved this measure by only 22% (see Figure 15).

Within ETMP-BGP routing, the adjustment of routes is carried out in a presource manner. This fosters the routes via the detection of traffic across AS-level routes based on feedback from destinations. In this manner, the SDN cluster enables BGP-4 routing to take an entire view of the routing path. The authors then transformed the ETMP-BGP modelling into a linear programming model to further outperform the existing BGP-4 schemes. The performance of that model needs improvement in terms of nodes that are cooperative with the network [15].

[15] proposed a traffic tunnel to minimize the BGP-4 traffic congestion. Another study investigated the BGP-4 convergence issue by utilizing interdomain multipath routing that distributes the routes and tackles overhead messages [83]. However, [15] approach is more effective since ASs forcefully reject tunnels if there is no capacity. [85] also explored a similar phenomenon using an offline-online scheme. [86] presented another unique form to provide

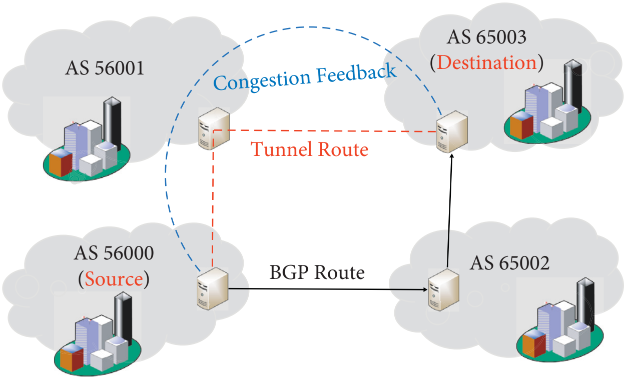

Figure 14: Architecture overview of ETMP-BGP [15]).

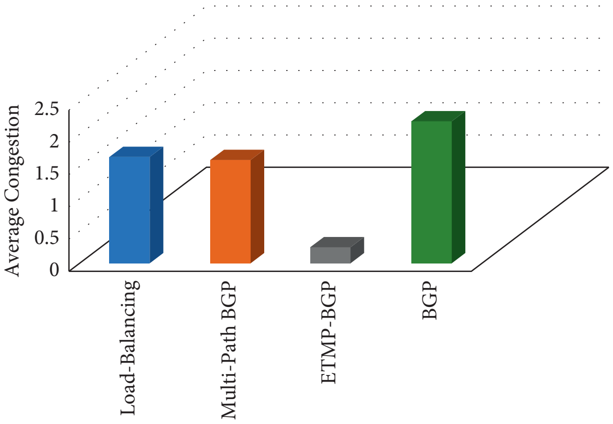

Figure 15: Comparison of routing methods (LB = load balancing, MBGP = multipath BGP-4) [15]).

multipath BGP-4 routing using SDN centralization. The authors added the concept of brokering within the interdomain clustering to mitigate BGP-4 convergence delays. It is stressed that the brokering activities of interdomain centralization are inevitable when the system offers low traffic loss and better link utilization.

The model proposed in [86] has one to five flowbrokers that manage the parameters of end-to-end delay, link utilization, and other domain-related factors. In addition, the performance of the flowbrokers is managed by the LDA machine learning algorithm, which gathers the training data of past parameters comparatively. As a result, an interdomain routing brokering plane is developed to mitigate concerns related to SDN clustering scalability, as shown in Figure 16. This enables decoupling in terms of adequate updating of highly scalable routing.

[87] also exploited the challenges resulting from the increasing consideration of SDN clustering as a solution for BGP-4 convergence issues. In contrast to the brokering architecture of the interdomain SDN clustering model of [86], and the tunnel-based multipath routing framework of [15, 87] introduced the SDN Federation Protocol (SFP) to yield scalability, efficiency, and, most importantly, stability to SDN interconnection. SFP features an innovative pub-sub approach over the typical push control of the BGP-4 protocol. It provides substantially enhanced flexibility, scalability, and system efficiency. The proposed model provides additional benefits, including flexible handling of network information. The packet space and flow set space information add value to the autonomous federation of spanned resources across a number of networks. Following this trend, [14] contributed to this research paradigm by investigating domain federation through SDN to facilitate end-to-end QoS in real-time.

[14] exploited this particular scenario to propose the EMPLaaS framework, which characterizes end-to-end MPLS-as-a-services. It evaluated the legacy MPLS in SDN networks to serve the desired application-centric framework. It is handled by the controller of the SDN cluster, which dynamically sets up the tunnels. The required BGP-4 interoperability is implemented using MPLS service requests that are pay loaded onto the BGP-4 network. In addition, the resulting scenario also features end-to-end responsiveness due to traffic engineering at the application level [14].

EMPLaaS is believed to mitigate the service provisioning limitations of centralized and distributed frameworks across multiple domains. Centralized frameworks specifically cater to the critical needs of the third-party parent entity, which makes the frameworks appropriate for particular subsets rather than the overall network. In contrast, distributed frameworks require no involvement from a third-party entity while developing multiple heterogeneous domains. Based on this, distributed frameworks are reportedly more aligned with general-purpose applications [88]. Therefore, MPLS has been adopted as a distributed framework, while its performance has been enhanced in terms of agility. As a result, a unique in-network model has been proposed that is effective at the operator level, yielding dynamic associations with multiple other network processes. However, the model presented in [14] is limited in terms of real-world deployment since the authors evaluated its performance in a virtual environment.

[13] focused on iBGP deployment schemes that affect the accurate dissemination of messages over the network. iBGP routers are allowed to make the received routes visible to internal peer routers only. The full-mesh deployment scheme ensures the complete dissemination of messages over the network of the network nodes peer, to result in optimal decision-making in all routers eventually. However, this scenario appears unrealistic, because all routers are already involved in several sessions, implying a configuration could not be carried out at all routers. Accordingly, in line with the scalability issues, the full-mesh scheme, although most efficient, is not deployed in large networks. As an alternative, router reflector (RR) mitigates full-mesh scalability challenges, but causes unwanted filtering of prefixes, which are eventually required for the process [89].

The authors in [13] adopted the SDN paradigm of a decoupled control plane and a forwarding plane that integrates logical centralization into the network. In this way, the decision-making considers overall networking needs. To make this idea achievable, the authors proposed a relay-based iBGP multicasting scenario (i.e., the dissemination of messages involving relay nodes). The relay nodes serve as boundaries among the multicast groups, which ultimately garners prefix filtration from other groups. The authors tested the proposal using both a single relay node and multiple relay nodes for every multicast group. While SDN manages the configuration and coordination throughout the multicast trees, the proposed model results in scalable session management that was not compatible with iBGP protocols. The duplicate announcement of prefixes is managed by eliminating unwanted peer sessions [13].

Khan et al. [84] proposed a framework with a multi-controller architecture that reduces packet loss and forwarding loops without multidomain controller synchronization in the network using a loop avoidance scheme. The proposed approach collects the link status to assist with load balancing and routing for the imminent flow on the link between domains to improve throughput in real-time and thwart congestion. The study focuses on reachability issues considering packet drops and loop intervention in the interdomain communication when there is a lack of SDN intercontroller communication. Reachability issues occur when packet drops and forwarding loops prevent traffic flows due to the lack of controller synchronization. The study suggested a mechanism, called Avoid Loop with Tests Packet (ALTP), as a loop prevention measure. Its algorithm can also be used to measure the E2E network latency when multidomain controller synchronization is absent.

Routing is another issue that the researchers focused on. The controller may split the flow, where all the split flows utilize one link during the interdomain data transmission. Flows across multipaths are accommodated by the controller, thus improving throughput. To facilitate solutions to the reachability and routing issues, the study [84] proposed a clear illustration for the bandwidth and load balancing in

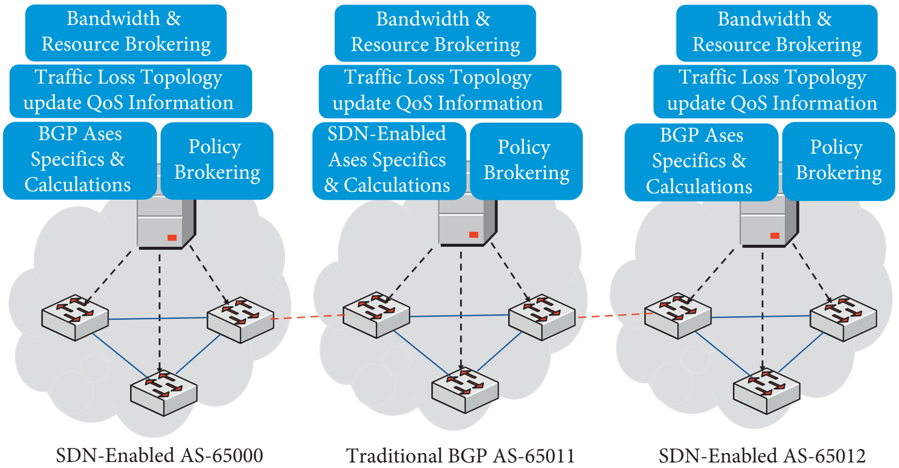
Bandwidth & Resource Brokering
Traffic Loss Topology update QoS Information
BGP Ases Specifics & Calculations
Policy Brokering
Bandwidth & Resource Brokering
Traffic Loss Topology update QoS Information
SDN-Enabled Ases Specifics & Calculations
Policy Brokering
Bandwidth & Resource Brokering
Traffic Loss Topology update QoS Information
BGP Ases Specifics & Calculations
Policy Brokering
SDN-Enabled AS-65000
Traditional BGP AS-65011
SDN-Enabled AS-65012

Figure 16: Brokering architecture with 1 BGP-4 and 2 SDN AS [86].

interdomain SDN. The methodology was designed to increase the network's overall throughput by processing flows on-demand and analyzing the interdomain routing performance. As a result, the proposed methodology improved throughput, reduced the latency of the flow setup process, and reduced the controller workload when compared with a multicontroller architecture.

The ALTP scheme module [84] calculates the source and border node shortest delay path using test packets to facilitate interdomain flows. The result is employed in the load balancing and flow management modules. The load balancing module balances the flow among the shortest paths. Finally, the flow management module moves interdomain flows to the related border switches. This study affirms the usefulness of a flat architecture in terms of network performance when compared to a hierarchical control architecture. Nonetheless, the hierarchical architecture emerges as a better approach in terms of the network scalability and resilience, when compared to flat and single-controller architectures. The extensive experiment results in the study reveal the efficiency of the ALTP scheme in minimizing the latency of the flow setup and fully utilizing the controller workload. The link-load balancing facilitates the multidomain flow throughput improvement. However, this article did not fully consider the resilience and reliability of the control layer.

A summary of the limitations of published work found during the literature review is provided in Table 3.

7. Challenges

7.1. Multidomain SDN Challenges. The proposed multidomain SDN-based solutions have not been fully realized and a number of challenges remain. In this section, the challenges are identified and briefly described.

7.1.1. SDN Controller Placement. In a centralized SDN controller architecture, the responsible controller is connected to forwarding devices. In that design, when the central controller is at risk and fails, the whole network will be tumbled. To address this issue, organizations need to understand the main functions of the central controller as well as increase the reliability of the SDN network; for example, safeguard the central controller in terms of network security and have a backup of the central controller [90]. The SDN controller placement is critical in determining how network control and administration are carried out. In the same context, the SDN paradigm should be implemented in such a way that it is able to handle the routing and forwarding functions in AS [37]. However, the position of the SDN controller in a network implies differences in the configuration of the SDN controller to ensure that it adequately meets the network requirement expectations.

7.1.2. Controller-Switch Communication Overhead. The load on an SDN controller is associated with the traffic flow management process. Packets that are unmatched at the data flow devices cause messages to pass between the controller and data flow device that results in the flow tables in the data flow device being updated to ensure that the traffic is managed according to the local rules and policies. Therefore, a switch receives an unidentified packet, and with the controller, it will exchange control messages, including PACKET_IN and PACKET_OUT messages to install new rules in the forwarding table for the new packet. When there is a high data flow consisting of many unidentified packets, the frequent exchange of the control messages produces controller latency, which degrades network performance [84, 91].

7.1.3. Multidomain SDN-Based Network Multicontroller Communication Overhead. For multidomain SDN-based networks with distributed controllers, the controllers typically have a partial network view. Finding a path across multiple domains relies upon timely updates of the routing and reachability information at the gateways and within networks. A proposed way to solve such an issue is to synchronize the controllers, but this approach could significantly increase traffic between controllers, thus causing

Table 3: Comparison of published works.

Proposed framework	Description	Remarks/Limitations	Base protocol	Difference from other published works
ETMP-BGP [15]	A framework that integrates end-to-end AS-level paths in domains	Focused on enhancing the connectivity in terms of the iBGP not eBGP	BGP-4	It focuses on enhancing the connectivity in terms of eBGP not iBGP.
INDOPRONOS [27]	Method and techniques to support automatic provisioning in multidomain SDN via east/west interfaces	It has enhanced the connectivity between multidomain SDN in terms of reachability, but it has a high BGP-4 convergence delay. Also, it does not fully evaluate scalability and resiliency.	BGP-4	It focuses on how to enhance and minimize the high BGP-4 convergence delay and the scalability scenarios.
SDNi [54]	An IETF draft standard that proposed an automated system protocol to connect multidomain SDN	It does not have any work progress since December 2012.	BGP-4 or SIP	It focuses on multidomain SDN technology using the BGP-4 routing protocol updated.
FASTPLANE [77]	A fast BGP-4 simulation tool for large data centres	It is effective in small to medium size data centres, but not for large data centres. It has some validation of BGP-4 semantics and production bugs in routing policy, network architecture, and router firmware.	BGP-4	It focuses on minimizing the BGP-4 convergence delay on large data centres.
DISCO [79]	It is a distributed SDN control plane for communication between multidomain based on AMQP protocol.	It uses a Floodlight controller and mainly focuses on connectivity and reachability, not QoS.	AMQP, but use BGP-4 Agent for Interoperability	It focuses on connectivity and reachability, keeping the QoS in the packet loss without measuring the BGP convergence delay and scalability parameters.
EMPLaaS [14]	framework to evaluate the MPLS in an SDN environment in the control plane layer.	It been evaluated its performance in a virtual environment not real-world deployment.	BGP-4	It evaluates in a real network environment at RMIT University lab.
SDX [16]	Interconnect SDN with legacy IP Network	SDN-based Internet exchange. It does not test the approach in multidomain SDN.	BGP-4	It focuses on multidomain SDN networks
(Bassey and Nayak, 2018) [13]	They proposed a framework for iBGP environment.	The proposed framework increased the BGP-4 convergence time 30% and 17% compared with the baseline results.	BGP-4	It focuses on minimizing the BGP-4 convergence time.
ONOS SDN-IP [82]	BGP-4 interfacing applications, which enables multidomain SDN and can interconnect SDN domain to legacy IP network.	Between SDN-IP applications or between SDN-IP and legacy IP network not between SDN-IP and SDN-IP networks.	BGP-4	It focuses on multidomain SDN networks.
(Zhou, Wu, Cheng, & Liu, 2017) [83]	It observed to investigating the BGP-4 convergence issue by means of interdomain multipath routing that distributes the routes and tackles the overhead messages.	The model needs more effective since they focused to get improvement in service availability and packet loss without any BGP-4 convergence delay improvements.	BGP-4	It focuses to get improvement in network scalability and BGP-4 convergence delay.

Table 3: Continued.

Proposed framework	Description	Remarks/Limitations	Base protocol	Difference from other published works
An Avoid Loop with Test Packet (ALTP) scheme [84]	A framework with multicontroller architecture that dodges packet drops and forwarding loops without multiple-domain controllers' synchronization in the network using ALTP scheme.	It focuses on reachability issues and it showed an improvement in minimizing the latency of the flow setup and utilizing the workload of the controller comparing with the baseline framework, furthermore, link-load balancing facilitates the improvement of the throughput, under multiple domains. However, it has a limitation in recovery of control layer failure which makes the entire domain disconnected from the other domain.	OSPF, probe test packet scheme, and Link Layer Discovery Protocol	This review is different because it uses BGP-4 as a routing protocol between different SDN domains in different AS, and it focuses on minimizing the BGP-4 convergence delay.

overhead in the network. The synchronization algorithm is yet to be designed and standardized. One method to overcome this problem is proposed in [84], in which test packets are used to create a multidomain path without controller synchronization [91].

7.1.4. Connectivity. SDN controller connectivity is another challenge because, and by default, SDN utilizes the Shortest Path First (SPF) algorithm to select the best route between source and destination, which may produce bottlenecks in the connections between domains since the controller may instruct the switches to transmit all streams using the same interdomain link. If two interdomain relationships are replicated, the controller may use one connection and leave the other connection empty due to the SPF algorithm. The regulation proposed in [92] permits various flows from the sender to the receiver through several connections, resulting in increased throughput and lower link utilization.

7.1.5. Forwarding Loops. The SDN networks may suffer from forwarding loops and packet losses due to a lack of controller coordination across several domains, resulting in routing problems in E2E services spanning multidomain. Due to the inability to update the full view of the switching plane across multidomain, a controller may generate a forwarding route with a loop for a flow, resulting in the flow being routed to its original domain [93].

7.1.6. Scalability. The SDN architecture includes centralized, hierarchical, and distributed controller deployments. However, there are likely to be scenarios where the controller-related control, management, and monitoring traffic could be affected by a network bottleneck. Large data networks, therefore, can overwhelm the controllers, and the performance may be degraded with time [94].

7.1.7. Network Performance. The SDN paradigm introduces a flexible flow-based management technique. Network performance depends on two critical metrics: flows per second and the flow setup time. The flow setup usually works in two modes: reactive and proactive. The two modes have different flow initiation as well as flow limitation overheads [91]. The separation of the data and control planes introduces latency. When dealing with a large network, this separation can lead to large delays, reduced network performance, and scalability issues. Network performance should be continuously monitored to permit network performance issues to be identified.

7.1.8. Reliability. The performance of a typical SDN-controlled network is subject to the efficiency and performance of the controller. In equal measure, the operational efficiency of the BGP-4 relies on the architectural configuration of the underlying network. In the event that the SDN controllers suffer a malfunction, the network performance is affected. Similarly, the BGP-4 efficiency depends on the operational efficiency of the routers within the AS. Essentially, the reliability of an AS or domain depends on the functionality of the dependent entities, notably the BGP-4 [73].

7.1.9. Availability. Any network, regardless of its size and complexity, is subject to issues that affect availability. As SDN is being integrated with BGP-4 and Internet gateways, there is the possibility of failure in any of the devices involved in the integrated architecture. It is paramount to note that some aspects, such as the malfunction of the SDN controller, increased network traffic, and even the failure of the SDN controller function, can greatly affect the reliability of the network [4].

7.1.10. Security. SDN controllers are susceptible to a variety of security issues, which may degrade system performance.

In a Denial of Service (DoS) episode, the absence of controller extensibility may have an influence on productivity. The effect might be more severe in a large network with just one controller or a centralized deployment utilizing multiple distributed controllers. Attackers may target the forwarding layer, the control layer, the APIs, or the application servers, with the following categories of attacks [27]:

(i) Unauthorized applications and policy enforcement might be used to launch attacks at the protocol stack

(ii) Massive traffic volumes that swamp the network flow devices and controllers may induce DoS, causing processing delays or device failure

(iii) A controller hijacking assault occurs when an attacker can gain a connection to the controller and has the controlling ability for the network

(iv) Attacks on layer input caches typically result in data leakage and flow rule changes, which may be devastating

(v) Malicious programs that use insertion assaults

A controller-switch communication flood is a DoS attack that occurs between the controllers and the network switches. There are various defence methodologies, such as preventive rule caching, rule aggregation, improving switch retention time, minimizing switch-controller communication latency, and packet-type categorization depends on traffic analysis. There are also various defence methodologies to counter other assault types on the application and control layers. The examples for such defence methodologies are regulator replication with diversification, controller replication, efficient controller placement, dynamic master controller distribution, and effective controller reassignment [95].

7.1.11. Latency. Typically, latency has a direct correlation with the way in which SDN controllers are placed within the network. Consequently, SDN latency determines the number and quality of controllers that can be placed within the network. Ultimately, network latency determines the way the network handles such issues as bandwidth utilization and routing behaviour [4].

7.1.12. Interoperability. Deployment of SDN-based networking for new network segments today is straightforward. However, the transition from legacy networks to SDN networks can be complex as the legacy networks support active businesses and industries. Enterprise and carrier networks are being transitioned to SDN-based networking, but this process is ongoing. SDN-based networks should be able to operate in conjunction with legacy networks. Network management and monitoring tools that support hybrid environments are necessary to reduce risk, cost, and service disruption. However, the network interfaces and environment need to have multiple systems that coexist to ensure that operations are carried out correctly, and risks are reduced [91].

7.2. Current BGP-4 Limitations. BGP-4 remaining challenges include:

7.2.1. BGP-4 Convergence Issues. BGP-4 routers should update their routing tables continuously in light of any change in the network topology. Convergence is defined as a process in which routers decide that which path to follow from source to destination for sending data packets. This process updates the overall topological map and the routing tables within the domain of the operating network. Convergence plays a vital role and should be accurate for network protocols to behave correctly [96].

BGP-4 is a protocol that selects the best route (between the AS nodes) to the destination based on the suggestion of neighborhood routers. The authors in [97] have measured the routing changes and determined that there is a noticeable delay in the convergence of BGP-4. During the process of delayed convergence, routes are continuously changing, which causes packet loss, traffic congestion, and connectivity disruption. Convergence delay is caused by the detection of loops at the sender side (SSLD) and the usage of withdrawal rate limiting (WRATE). SSLD is based on the optimization strategy in which a router detects the loops in the path before sending the advertisement to the neighboring routers. WRATE is an application based on the withdrawal of advertisement (based on the best path selection) and messages sent to the destination node. However, RFC-1771 [98] does not permit the withdrawal. There is research that considers how to solve the BGP-4 convergence issue. The authors in [99] presented an algorithm named stable path problem (SPP) that analyzes the convergence properties of BGP-4. Obradovic proposed an updated version of SPP based on the real-time evolution of route convergence [100].

Convergence delay is the gap time between the router adopting any update configuration until it is settled. A description of this state is that the system is considered stable if the entries in the main routing table Loc-RIB remain unchanged for a set time. When there is a new entry or network node failure, the main routing table is updated and the updated message is exchanged over the network by BGP-4 speakers until the network topology becomes stable again [101]. In the BGP-4 routing protocol, convergence occurs for two reasons: when building the routing table after route initialization and when routers are updating their routing tables. Changes in the topology of the network arise because of physical links failing, the router being rebooted, and the network prefix being deleted. This makes the network unstable, causing the AS to withdraw previous announcements and search for the best paths, and announce them again. This is referred to as BGP-4 convergence. BGP-4 convergence is becoming a considerable challenge for Internet connectivity given the current rate of growth of the Internet, and it may become even more difficult to manage although BGP-4 has the capability of adapting to new changes and converging to new stable routes [39].

7.2.2. Route Table Management. This issue arises because of the high number of new and updated routes that become available globally during a year. New routes are constantly being advertised on the network, and thus, the router needs to find a way to aggregate the new routes. The aggregation process can be challenging, especially if the AS is segregated into subsections [37].

7.2.3. Large Volume of Routing Information. BGP-4 also deals with a large volume of routing information, including BGP-4 messages, that are constantly being exchanged in the network. This requires an extensive amount of memory, which might lead to overutilization of the available resources, affecting the performance level and leading to slow operational speeds [26].

7.2.4. Erroneous Configuration. There is always a chance that route advertisements can occur erroneously, given the objective to channel traffic to a certain destination. In such a scenario, the filtered traffic will be sent to a certain AS, which may overwhelm the destination with a high volume of traffic. For instance, in 2008, the Pakistan government decided to censor and filter specific YouTube videos from being accessed in the country. By doing so, the Pakistan ISP decided to route all traffic from the YouTube video to a preferred route. Due to configuration errors, all YouTube traffic from around the world was channeled to the preferred destination. The result was a massive outage of YouTube services for more than 80 minutes [102].

7.2.5. Route Flapping. BGP-4 is also affected by route flapping, which has the potential to affect performance. Flapping, in this context, refers to a scenario whereby BGP-4 tends to hold down any routes that appear to be unreliable. Such routes sometimes appear but then suddenly disappear and thus are not convenient for path selection. The flapping process can be time-consuming and has the negative effect of delaying BGP-4 peers from listening to each other [103].

7.2.6. Security. The major limitation worthy of note is that of security, which is often consequent of human errors. Error due to the configuration exposes the system to a total crash or breach in security. Each BGP-4 speaker talks about the responsibility of educating its various neighbors regarding what it possesses. The calculation of its methodology is not complicated. The outcome of this is an increase in the routing table size, thereby birthing plunged delays in the entry to the searching route based on the BGP-4 speaker routing table [66].

BGP-4 is also prone to various security attacks, mostly malicious. For instance, a malicious attacker might manipulate the routing table, redirecting the traffic to another destination. Route hijacking is another security threat, in which a potential attacker announces the victims route prefixes with the aim of directing traffic to another destination. BGP-4 is also prone to DoS attacks that effectively render the whole network inoperable [37].

7.2.7. Scalability. BGP-4 suffers from scalability issues, especially in a full-mesh topology where each router needs to communicate with each other. In a large AS network, maintaining active BGP-4 sessions consumes the available resources, notably, memory and CPU requirements [97].

7.2.8. Load balancing. Load balancing is another BGP-4 challenge, especially in a multihomed AS environment, where inbound links may be overwhelmed by traffic. At the same time, some of the inbound links are under-utilized, creating a need to balance resource use. The problem is further compounded by the fact that BGP-4 does not have the capability to detect congestion [73].

It is worth noting that the challenges can be mitigated in various ways to ensure that BGP-4 continues to perform the required functions to support interdomain routing.

7.2.9. BGP-4 Hijacking. BGP-4 hijacking occurs when hackers or attackers redirect Internet traffic maliciously. The attackers can accomplish this by falsely claiming ownership of IP prefixes that they do not own. Consequently, the attackers can control and even route the traffic to a preferred destination on the Internet. It has also increased tremendously in recent times. It permits malicious autonomous systems to get IP prefixes to spam, intercept, and blackmail traffic [104].

7.2.10. Ghost Entries. BGP-4 does not have any inherent update timer, and the timer may lack the most recent entries leading to "Ghost" entries since the prefixes designated remain unreachable [104].

8. Discussion and Future Work

SDN eliminates the traditional need to perform standard network administrative functions; it is this benefit that provides the justification to utilize the latest SDN technologies to improve BGP-4 and Internet gateway functionality. Many of the SDN functions are designed to enhance network security, stability, reliability, and programmability. In equal measure, the applicability of SDN has proved essential in the enhancement of BGP-4 and gateway performance. There are a variety of BGP-4 and gateway components that can and should be optimized using SDN technologies.

Internet gateways play a significant role in determining how network traffic is handled between networks that utilize different routing protocols. SDN strengths are formulated based on the prospect of minimizing resource usage, primarily because of the dynamic and programmatic nature of the underlying architecture. The implementation of SDN within an AS makes it possible to accentuate the connectivity between autonomous peers. The SDN paradigm should be implemented in AS characterized by networks that use both domain edges and Internet gateways. The introduction of SDN technology should ensure the improved performance of BGP-enabled Internet gateways. The routing and forwarding functions serve as crucial capabilities that characterize both BGP-4 and Internet gateways. These functions are highly complex and thus require the exemplary application of SDN technologies.

Route management requires the utilization of a comprehensive mechanism aimed at ensuring that all routers within the administrative domain are capable of communicating with each other effectively. SDN is hailed as a networking concept whose origin is attributed to the advent of modern Internet routing protocols, specifically BGP-4. It is thus possible to configure routing policies in Internet gateways using the programmable feature of SDN controllers.

It is also essential to highlight the importance of SDN in the implementation of security enhancements in a network. BGP-4 and Internet gateways are prone to security vulnerabilities, necessitating efficient security measures. The SDN application layer is equipped with sufficient security capabilities to enhance the security parameters of the underlying network. Internet gateways are also vulnerable to a variety of security threats that can be resolved using SDN controllers. In addition, researchers should investigate how to improve the substantial BGP-4 convergence delay, which is the major issue for the BGP-4 protocol as it is the Internet routing protocol used today to coordinate the operation of multidomain gateways.

9. Conclusion

SDN is a technology that has improved and continues to improve with other networking technologies, especially routing in large enterprise networks and AS. The configuration and administration of enterprise networks is a complex process, creating the need for an automatic network management process. The incorporation of SDN has been and continues to be a significant step that makes it easier to administer and configure networks. Essentially, SDN helps in the management, control, and administration of both interdomain and intradomain networks using a dynamically and programmable network interface. Additionally, SDN makes it possible to establish and maintain a universal overview with respect to routing and forwarding functions associated with BGP-4 and Internet gateways. This article has provided a review of multidomain SDN-based gateways and an overview of how multidomain BGP-4 operates. It has addressed the AS and administrative domain concepts, the categories of Internet routing systems, and challenges. In addition, it has provided an overview of the SDN and reviewed the previous proposals for enhancing the SDN with gateways and BGP-4.

Data Availability

For this study, the data supporting the findings are available from the corresponding author, "Hamad Saud Alotaibi" "s3388813@student.rmit.edu.au", upon reasonable request.

Conflicts of Interest

This research does not have any conflicts of interest.

Acknowledgments

This study was supported by the Interior Ministry of Saudi Arabia and the Saudi Arabia Cultural Mission. The authors would like to thank Mr. Hoang Do and Dr. Franciscus X.A. Wibowo and the Members of the Next Generation Internet Architecture Research Group at RMIT University. The authors would also like to thank all who contributed to this research.

References

[1] B. E. Vinit Jain, "Troubleshooting BGP: A practical guide to understanding and troubleshooting BGP," 2018, http://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=3.

[2] M. Karakus and A. Durresi, "Quality of service (QoS) in software defined networking (SDN): a survey," *Journal of Network and Computer Applications*, vol. 80, pp. 200–218, 2017.

[3] J. Hawkinson and T. Bates, "Guidelines for creation, selection, and registration of an autonomous system (AS)," 1996, https://www.hjp.at/doc/rfc/rfc1930.html.

[4] P. Sermpezis and X. Dimitropoulos, "Can SDN accelerate BGP convergence?—a performance analysis of inter-domain routing centralization," in *Proceedings of the 2017 IFIP Networking Conference (IFIP Networking) and Workshops*, pp. 1–9, IEEE, Stockholm, Sweden, June 2017.

[5] L. M. Elguea and F. Martinez-Rios, "An efficient method to compare latencies in order to obtain the best route for SDN," *Procedia Computer Science*, vol. 116, pp. 393–400, 2017.

[6] E. L. Fernandes, G. Antichi, I. Castro, and S. Uhlig, "An SDN-inspired model for faster network experimentation," in *Proceedings of the 2018 ACM SIGSIM Conference on Principles of Advanced Discrete Simulation*, pp. 29–32, Rome, Italy, May 2018.

[7] R. B. da Silva and E. Souza Mota, "A survey on approaches to reduce BGP Interdomain routing convergence delay on the internet," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2949–2984, 2017.

[8] A. Abdelaziz, A. Tan Fong, A. Gani, S. Khan, F. Alotaibi, and M. Khurram Khan, "On software-defined wireless network (SDWN) network virtualization: challenges and open issues," *The Computer Journal*, vol. 60, no. 10, pp. 1510–1519, 2017.

[9] N. A. Jagadeesan and B. Krishnamachari, "Software-defined networking paradigms in wireless networks: a survey," *ACM Computing Surveys*, vol. 47, pp. 1–11, 2014.

[10] M. Amadeo, C. Campolo, J. Quevedo et al., "Information-centric networking for the internet of things: challenges and opportunities," *IEEE Network*, vol. 30, no. 2, pp. 92–100, 2016.

[11] F. X. A. Wibowo, M. A. Gregory, K. Ahmed, and K. M. Gomez, "Multi-domain software defined networking: research status and challenges," *Journal of Network and Computer Applications*, vol. 87, pp. 32–45, 2017.

[12] T. Huang, F. R. Yu, C. Zhang, J. Liu, J. Zhang, and Y. Liu, "A survey on large-scale software defined networking (SDN) testbeds: approaches and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, pp. 891–917, 2016.

[13] U. Bassey and A. Nayak, "Relay-based ibgp multicasting in software defined networks," in *Proceedings of the 2018 Tenth International Conference on Ubiquitous and Future Networks*

(ICUFN), pp. 174–179, IEEE, Prague, Czech Republic, July 2018.

[14] S. Hasija, R. Mijumbi, S. Davy, A. Davy, B. Jennings, and K. Griffin, "Domain federation via MPLS and SDN for dynamic, real-time end-to-end QoS support," in *Proceedings of the 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*, pp. 177–181, IEEE, Montreal, Canada, June 2018.

[15] J. G. Gomez, R. Wang, M. H. Chen, and C. F. Chou, "ETMP-BGP: effective tunnel-based multi-path BGP routing using software-defined networking," in *Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 420–425, IEEE, Banff, Alberta, Canada, October 2017.

[16] A. Gupta, L. Vanbever, M. Shahbaz et al., "Sdx: a software defined internet exchange," *ACM SIGCOMM-Computer Communication Review*, vol. 44, pp. 551–562, 2014.

[17] A. Gupta, R. MacDavid, R. Birkner et al., "An industrial-scale software defined internet exchange point," in *Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI '16)*, pp. 1–14, Santa Clara, CA, USA, April 2016.

[18] K. Tolga Bagci and A. Murat Tekalp, "SDN-enabled distributed open exchange: dynamic QoS-path optimization in multi-operator services," *Computer Networks*, vol. 162, Article ID 106845, 2019.

[19] D. F. Asigbe, A. M. Mustapha, C. Agbesi, B. F. Ephraim, A. Bright, and S. Clement, "Performance analysis of interior gateway routing protocol (EIGRP) over open shortest path first (OSPF) protocol," *International Journal Of Scientific & Technology Research (IJSTR)*, vol. 5, pp. 111–117, 2016.

[20] D. Sheinbein and R. P. Weber, "Stored program controlled network: 800 service using SPC network capability," *Bell System Technical Journal*, vol. 61, no. 7, pp. 1737–1744, 1982.

[21] M. Caesar, D. Caldwell, N. Feamster, J. Rexford, A. Shaikh, and J. van der Merwe, "Design and implementation of a routing control platform," in *Proceedings of the 2nd Conference on Symposium on Networked Systems Design & Implementation*, vol. 2, pp. 15–28, Boston, MA, USA, May 2005.

[22] M. R. Macedonia and D. P. Brutzman, "Mbone provides audio and video across the internet," *Computer*, vol. 27, no. 4, pp. 30–36, 1994.

[23] B. Silva, R. Matos, G. Callou et al., "Mercury: an integrated environment for performance and dependability evaluation of general systems," in *Proceedings of the Industrial Track at 45th Dependable Systems and Networks Conference, DSN*, pp. 1–4, Rio de Janeiro, Brazil, June 2015.

[24] V. Baggan, A. K. Sahoo, P. K. Sarangi, and S. P. Chaturvedi, "A comprehensive analysis and experimental evaluation of routing information protocol: an elucidation," *Materials Today Proceedings*, vol. 49, pp. 3040–3045, 2020.

[25] J. W. Guck, A. Van Bemten, M. Reisslein, and W. Kellerer, "Uni-cast QoS routing algorithms for SDN: a comprehensive survey and performance evaluation," *IEEE Communications Surveys & Tutorials*, vol. 20, pp. 388–415, 2017.

[26] "Troubleshooting high CPU caused by the BGP scanner or BGP router process," 2015, https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/107615-highcpu-bgp.html.

[27] F. X. Wibowo and M. A. Gregory, "Multi-domain software defined network provisioning," in *Proceedings of the 2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1–7, IEEE, Sydney, Australia, November 2018.

[28] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4). RFC 4271 (Draft Standard). Updated by RFC 6286," 2006.

[29] D. Mills, "Exterior Gateway Protocol Formal Specification. IETF, Request For Comments 0904 (RFC0904)," 1984.

[30] K. Lougheed and Y. Rekhter, *A Border Gateway Protocol 3 (BGP-3)*, Technical Report. RFC 1267, Cisco Systems, TJ Watson Research Center, IBM Corp, Armonk, NY, USA, 1991.

[31] T. Griffin and G. Huston, *BGP Wedgies*, Network Working Group, RFC 4264, 2005.

[32] H. Berkowitz, E. B. Davies, S. Hares, P. Krishnaswamy, and M. Lepp, "Terminology for benchmarking BGP device convergence in the control plane," 2005, https://www.hjp.at/doc/rfc/rfc4098.html.

[33] T. G. Griffin and G. Wilfong, "An analysis of BGP convergence properties," *ACM SIGCOMM-Computer Communication Review*, vol. 29, no. 4, pp. 277–288, 1999.

[34] Catchpoint Systems Inc, "A BGP guide for the non-network engineer. Technical Report," Catchpoint Systems Inc, 2019, https://blog.catchpoint.com/2019/11/07/bgp-guide-non-network-engineer/.

[35] J. Doyle, "BGP basics: Internal And external BGP. Technical Report. Networking Computing Informa PLC," 2017, https://www.networkcomputing.com/data-centers/bgp-basics-internal-and-external-bgp.

[36] Cisco Networking Academy, "Branch connections," in *Connecting Networks v6 Companion Guide*pp. 850–857, Cisco Networking Academy, 2017, http://www.ciscopress.com/articles/article.asp?p=2832406.

[37] K. Butler, T. R. Farley, P. McDaniel, and J. Rexford, "A survey of BGP security issues and solutions," *Proceedings of the IEEE*, vol. 98, pp. 100–122, 2009.

[38] Y. Rekhter, T. Li, and S. Hares, "A border gateway protocol 4 (BGP-4)," 1994, https://www.hjp.at/doc/rfc/rfc4271.html.

[39] Y. H. Jazyah, "Mathematical model of the relationship between BGP convergence delay and network topologies," *Journal of Computer Science*, vol. 14, no. 1, pp. 1–13, 2018.

[40] B. Wang, "The research of BGP convergence time," in *Proceedings of the 2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference*, pp. 354–357, IEEE, Chongqing, China, August 2011.

[41] E. A. Alabdulkreem, "Reduce BGP convergence time," *International Journal of Innovative Research in Engineering & Management*, vol. 5, no. 1, pp. 15–18, 2018.

[42] Y. Li, D. Zhang, J. Taheri, and K. Li, "Innovation and intellectual property rights," in *Big Data and Software Defined Networks. The Institution of Engineering and Technology. IET Book Series on Big Data. chapter 3*, J. Taheri, Ed., pp. 48–68, 2018, https://pdfs.semanticscholar.org/815c/4901c8e04141a54efdec61da6e8df3518895.pdf.

[43] N. Zhang, P. Yang, S. Zhang et al., "Software defined networking enabled wireless network virtualization: challenges and solutions," *IEEE Network*, vol. 31, no. 5, pp. 42–49, 2017.

[44] L. Xu, J. Huang, S. Hong, J. Zhang, and G. Gu, "Attacking the brain: Races in the SDN control plane," in *Proceedings of the 26th USENIX Security Symposium*, pp. 451–468, Vancouver, BC, Canada, August 2017.

[45] Open Networking Foundation, "SDN architecture," 2014, https://www.opennetworking.org/wp-content/uploads/2013/02/TR_SDN_ARCH_1.0_06062014.pdf.

[46] N. McKeown, T. Anderson, H. Balakrishnan et al., "Open-Flow," *ACM SIGCOMM-Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.

[47] M. Cooney, "What is SDN and where software-defined networking is going. Technical Report 2. NETWORK-WORLD," 2019, https://www.networkworld.com/article/3209131/what-sdn-is-and-where-its-going.html.

[48] B. Davie, T. Koponen, J. Pettit et al., "A database approach to SDN control plane design," *ACM SIGCOMM-Computer Communication Review*, vol. 47, no. 1, pp. 15–26, 2017.

[49] J. S. Marcus and G. Molnar, "Network sharing and 5g in europe: the potential benefits of using SDN or NFV," *DigiWorld Economic Journa*, pp. 113–138, 2017.

[50] Á. Caraguay and L. Villalba, "Monitoring and discovery for self-organized network management in virtualized and software defined networks," *Sensors*, vol. 17, no. 4, p. 731, 2017.

[51] A. Abdelaziz, A. T. Fong, A. Gani et al., "Distributed controller clustering in software defined networks," *PLoS One*, vol. 12, no. 4, Article ID e0174715, 2017.

[52] F. Alam, "SDN fundamentals," 2017, https://www.sanog.org/resources/sanog30/SANOG30-Tutorial_ SDN101_sanog30.pdf.

[53] O. Blial, M. Ben Mamoun, and R. Benaini, "An overview on SDN architectures with multiple controllers," *Journal of Computer Networks and Communications*, vol. 2016, Article ID 9396525, 8 pages, 2016.

[54] H. Yin, H. Xie, T. Tsou, D. Lopez, P. Aranda, and R. Sidi, "SDNi: A message exchange protocol for software defined networks (SDNs) across multiple domains internet draft," 2012, https://tools.BGP-tutorial-The-routing-protocol-that-makes-the-Internet-worki.etf.org/html/draft-yin-sdn-sdni-00.

[55] B. Pfaff and B. Davie, "The open vswitch database management protocol," 2013, http://www.hjp.at/doc/rfc/rfc7047.html.

[56] D. Bansal, S. Bailey, T. Dietz, and A. Shaikh, "Open-flow management and configuration protocol (OF-Config 1.2). Open Networking Foundation, Report, OF-CONFIG 1.2," 2014, https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow-config/of-config-1.2.pdf.

[57] R. Enns, "NETCONF Configuration Protocol," 2006, https://www.hjp.at/doc/rfc/rfc4741.html.

[58] K. Watsen, "NETCONF call home and RESTCONF call home," 2017, http://www.hjp.at/doc/rfc/rfc8071.html URL:.

[59] A. Atlas, J. Halpern, S. Hares, D. Ward, and T. Nadeau, "An architecture for the interface to the routing system," 2013, https://datatracker.ietf.org/doc/rfc7921/?include_text=1.

[60] T. Tairaku, A. Nakao, S. Yamamoto, S. Yamaguchi, and M. Oguchi, "Social data driven SDN network operation using northbound interface," in *Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC)*, pp. 702–706, IEEE, Maui, HI, USA, March 2018.

[61] M. R. Nascimento, C. E. Rothenberg, M. R. Salvador, C. N. Corrêa, S. C. De Lucena, and M. F. Magalhães, "Virtual routers as a service: the routeflow approach leveraging software-defined networks," in *Proceedings of the 6th International Conference on Future Internet Technologies*, pp. 34–37, ACM, Seoul, Korea, June 2011.

[62] P. Lin, J. Bi, and H. Hu, "BTSDN: BGP-based transition for the existing networks to SDN," *Wireless Personal Communications*, vol. 86, no. 4, pp. 1829–1843, 2016.

[63] A. Mendiola, J. Astorga, E. Jacob, and M. Higuero, "A survey on the contributions of software-defined networking to traffic engineering," *IEEE Communications Surveys & Tutorials*, vol. 19, pp. 918–953, 2016.

[64] T. Bakhshi, "State of the art and recent research advances in software defined networking," *Wireless Communications and Mobile Computing*, vol. 2017, Article ID 7191647, 35 pages, 2017.

[65] M. Nkosi, A. Lysko, L. Ravhuanzwo, T. Nandeni, and A. Engelberencht, "Classification of SDN distributed controller approaches: a brief overview," in *Proceedings of the 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, pp. 342–344, IEEE, Durban, South Africa, November 2016.

[66] V. Baggan and S. N. Panda, "Enhancing network path restoration with software defined networking," *International Journal of Applied Engineering Research*, vol. 14, pp. 1910–1916, 2019.

[67] F. J. B. V. Neto, C. J. Miguel, A. C. d. S. de Jesus, and P. N. Sampaio, "SDN controllers-a comparative approach to market trends," in *Proceedings of the 9th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2021)*, pp. 1–5, Zaragoza, Spain, February 2021.

[68] M. B. Dissanayake, A. Kumari, and U. Udunuwara, "Performance comparison of onos and odl controllers in software defined networks under different network typologies," *Journal of Research Technology and Engineering*, vol. 2, no. 3, pp. 94–105, 2021.

[69] L. Agapides, "Single/dual homed and multi-homed designs," 2017, https://forum.networklessons.com/t/single-dual-homed-and-multi-homed-designs/1545.

[70] D. Huang, Q. Cao, A. Sinha et al., "New architecture for intra-domain network security issues," *Communications of the ACM*, vol. 49, no. 11, pp. 64–72, 2006.

[71] S. Hares and D. Katz, "RFC1136: Administrative domains and routing domains: A model for routing in the internet," 1989, http://ftp.yzu.edu.tw/RFC/in-notes/pdfrfc/rfc1136.txt.pdf.

[72] D. Mitra, S. Sarkar, and D. Hati, "A comparative study of routing protocols," *Engineering and Science*, vol. 2, pp. 46–50, 2016.

[73] M. P. Clark, *Data Networks, IP and the Internet: Protocols, Design and Operation*, John Wiley & Sons, Hoboken, NJ, USA, 2003.

[74] R. Govindan and A. Reddy, "An analysis of internet inter-domain topology and route stability," in *Proceedings of the INFO-COM'97*, pp. 850–857, IEEE, Kobe, Japan, April 1997.

[75] A. Doria, J. H. Salim, R. Haas et al., "Forwarding and Control Element Separation (ForCES) Protocol Specification. RFC 5810," 2010, https://www.hjp.at/doc/rfc/rfc5810.html.

[76] I. Pepelnjak, "BGP tutorial: The routing protocol that makes the internet work. TechTarget Network 16," 2016, https://searchnetworking.techtarget.com/feature/.

[77] N. P. Lopes and A. Rybalchenko, "Fast BGP simulation of large datacenters," in *Proceedings of the International Conference on Verification, Model Checking, and Abstract Interpretation*, pp. 386–408, Springer, Cascais, Portugal, January 2019.

[78] M. T. Moubarak, A. D. Elbayoumy, and M. H. Megahed, "Design and implementation of BGP novel control mechanism (BGP-NCM) based on network performance parameters," *Ain Shams Engineering Journal*, vol. 9, no. 4, pp. 2079–2091, 2018.

[79] K. Phemius, M. Bouet, and J. Leguay, “Disco: distributed multi- domain SDN controllers,” in *Proceedings of the 2014 IEEE Network Operations and Management Symposium (NOMS)*, pp. 1–4, IEEE, Krakow, Poland, May 2014.

[80] P. Lin, J. Bi, S. Wolff et al., “A west-east bridge based SDN inter-domain testbed,” *IEEE Communications Magazine*, vol. 53, no. 2, pp. 190–197, 2015.

[81] H. S. Alotaibi, M. A. Gregory, S. Li, and H. Do, “Multi- state border gateway protocol for multi-domain software defined networking–based gateways,” in *Proceedings of the 2020 30th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1–6, IEEE, Melbourne, Australia, November 2020.

[82] A. Koshibe and J. Hart, “SDN-IP architecture. wiki.onosproject.org,” 2016, https://wiki.onosproject.org/display/ONOS/SDN-IP+Architecture.

[83] H. Zhou, C. Wu, Q. Cheng, and Q. Liu, “SDN-LIRU: a lossless and seamless method for SDN inter-domain route updates,” *IEEE/ACM Transactions on Networking*, vol. 25, no. 4, pp. 2473–2483, 2017.

[84] N. Khan, R. Bin Salleh, I. Ali et al., “Enabling reachability across multiple domains without controller synchronization in SDN,” *Computers, Materials & Continua*, vol. 69, no. 1, pp. 945–965, 2021.

[85] N. Solayman, A. El-Sayed, and M. Badawy, “Improvement of border gateway protocol against failure on autonomous systems,” *International Journal of Computer Science Issues (IJCSI)*, vol. 14, p. 14, 2017.

[86] J. O. Abe and H. A. Mantar, “Multi-path routing and brokering in inter-domain or inter-as with SDN: a model,” in *Proceedings of the 2017 Advances in Wireless and Optical Communications (RTUWO)*, pp. 192–197, IEEE, Riga, Latvia, November 2017.

[87] F. Le, C. Leet, C. Makaya, M. Rio, X. Wang, and Y. R. Yang, “SFP: toward a scalable, efficient, stable protocol for federation of software defined networks,” in *Proceedings of the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (Smart- World/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pp. 1–6, IEEE, San Francisco, CA, USA, August 2017.

[88] D. Kyriazis, A. Menychtas, G. Kousiouris et al., “A real-time service oriented infrastructure,” *GSTF Journal on Computing*, vol. 1, pp. 196–204, 2011.

[89] S. Shukla and M. Kumar, “An approach to discover the stable routes in BGP confederations,” *International Journal of Information System Modeling and Design*, vol. 8, no. 2, pp. 134–147, 2017.

[90] O. Lemeshko, J. Papan, M. Yevdokymenko, and O. Yeremenko, “Advanced tensor solution to the problem of inter-domain routing with normalized quality of service,” *Applied Sciences*, vol. 12, no. 2, p. 846, 2022.

[91] A. A. Pranata, T. S. Jun, and D. S. Kim, “Overhead reduction scheme for SDN-based data center networks,” *Computer Standards & Interfaces*, vol. 63, pp. 1–15, 2019.

[92] N. Khan, R. B. Salleh, Z. Khan, and A. Koubaa, “Avoiding forwarding loop across multiple domains without controller synchronization in SDN,” in *Proceedings of the 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*, pp. 122–127, IEEE, Riyadh, Saudi Arabia, November 2020.

[93] Y. Yu, X. Li, X. Leng et al., “Fault management in software-defined networking: a survey,” *IEEE Communications Surveys & Tutorials*, vol. 21, pp. 349–392, 2018.

[94] Z. Latif, K. Sharif, F. Li, M. M. Karim, and Y. Wang, “A comprehensive survey of interface protocols for software defined networks,” 2019, https://arxiv.org/abs/1902.07913.

[95] P. Helebrandt and I. Kotuliak, “Novel SDN multi-domain architecture,” in *Proceedings of the 2014 IEEE 12th IEEE International Conference on Emerging eLearning Technologies and Applications (ICETA)*, pp. 139–143, IEEE, Stary Smokovec, Slovakia, December 2014.

[96] S. U. Masruroh, A. Fiade, and M. F. Iman, “Performance evaluation of routing protocol RIPv2, OSPF, EIGRP with BGP,” in *Proceedings of the 2017 International Conference on Innovative and Creative Information Technology (ICITech)*, pp. 1–7, IEEE, Salatiga, Indonesia, November 2017.

[97] A. Elmokashfi, A. Kvalbein, and C. Dovrolis, “On the scalability of BGP: the roles of topology growth and update rate-limiting,” in *Proceedings of the 2008 ACM CoNEXT Conference*, pp. 1–12, Madrid, Spain, December 2008.

[98] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian, “Delayed Internet routing convergence,” *ACM SIGCOMM-Computer Communication Review*, vol. 30, no. 4, pp. 175–187, 2000.

[99] Y. Rekhter and T. Li, “Rfc1771: A Border Gateway Protocol 4 (BGP-4),” 1995.

[100] D. Obradovic, “Real-time model and convergence time of BGP,” in *Proceedings of the Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, pp. 893–901, IEEE, New York, NY, USA, June 2002.

[101] H. S. Kim and S. I. Kim, “A BGP session takeover method for high availability,” in *Proceedings of the 2015 Seventh International Conference on Ubiquitous and Future Networks*, pp. 153–158, IEEE, Sapporo, Japan, July 2015.

[102] L. Seltzer, “Pakistan drops the BGP bomb,” 2008, https://www.eweek.com/security/pakistan-drops-the-bgp-bomb.

[103] W. Lijun, W. Jianping, and X. Ke, “A variation of route flap damping to improve BGP routing convergence,” in *Proceedings of the 2006 14th IEEE International Workshop on Quality of Service*, pp. 297–301, IEEE, New Haven, CT, USA, June 2006.

[104] S. Cho, R. Fontugne, K. Cho, A. Dainotti, and P. Gill, “Bgp hijacking classification,” in *Proceedings of the 2019 Network Traffic Measurement and Analysis Conference (TMA)*, pp. 25–32, IEEE, Paris, France, June 2019.