information

MDPI

Review

A Survey on Efforts to Evolve the Control Plane of Inter-Domain Routing

Walber José Adriano Silva * and Djamel Fawzi Hadj Sadok

Center for Informatics, Federal University of Pernambuco, Recife 50740-560, Brazil; jamel@gprt.ufpe.br
* Correspondence: wjas@cin.ufpe.br; Tel.: +55-81-2126-8430

Received: 4 April 2018; Accepted: 14 May 2018; Published: 18 May 2018

Abstract: The Internet's default inter-domain routing protocol is the Border Gateway Protocol (BGP). With the BGP, dozens of thousands of Autonomous Systems (ASs) exchange network layer reachability information to manage connectivity among them. The BGP was introduced in the early stages of the Internet, and although the BGP is one of the most successful protocols, new desirable features have been difficult to incorporate into the network over the decades. Thus, this paper classifies previous works to evolve the control plane of inter-domain routing into three types of approaches: brand new design; incremental improvement; inter-domain communication. The main goal of this paper is to provide an understanding of what approaches have been taken to evolve the inter-domain routing control plane. This survey also discusses why the control plane's issues are hard to evolve and future perspectives for that topic.

Keywords: Board Gateway Protocol; control plane; Internet; Software-Defined Networking

1. Introduction

The last decade has been marked by profound advances in Information and Communication Technologies (ICT). It is expected that computer networks will continue to play an important role in the adoption of new ICT, for example the Internet of Things (IoT) [1], edge computing [2], 5G [3,4] and others [5]. Furthermore, one of the paramount computer network environments is the inter-domain.

The main routing technology used in inter-domain routing is the Board Gateway Protocol (BGP) [6]. The BGP is the standard protocol of the Internet, and it is the "glue" that allows different administrative networks, or Autonomous Systems (ASs), to reach other networks. An AS tunes its BGP configurations to express policies that reflect how the AS connects to others to accommodate its business requirements. Besides that, this protocol has allowed Internet exchange reachability information and network traffic since its early stages.

The BGP has a great capacity to scale and significantly contribute to the success of the Internet, but it is nonetheless one of the most inflexible and ossified protocols [7–9]. The lack of end-to-end guarantees of Quality of Service (QoS), complex network management, slow convergence, limitations of routing policy enforcement implications and its capabilities are a few drawbacks of the BGP. For example, the BGP does not have robust traffic engineering techniques to control inbound traffic [10] and the current Internet routing table explosion is a side effect of the application of BGP traffic engineering tasks by multi-homed ASs, in which it is desired to increase the reliability of their domains by advertising multiple subnets of their network prefixes [11].

Furthermore, the Internet topology and traffic patterns have been changing since its inception, from a pure hierarchical topology (well-defined tree structure) to a flat AS-level topology (more connected and without a well-defined structured topology) [12]. One cause of the Internet topology changing is the expansion of Content Delivery Networks (CDNs) and Internet Exchange

Points (IXPs). They have been increasing the path diversity of the Internet, where CDNs and IXPs introduced additional AS connectivity to intensify Internet traffic among ASs [13,14].

Nonetheless, the BGP's destination-based forwarding paradigm limits the granularity of distributing network traffic among the multiple paths of the current Internet topology. Hence, the BGP is not capable of exploring the full potential of path diversity in the current Internet, because it computes just one "best" next hop for each network prefix. New promising technologies such as 5G [4] and the Internet of Things (IoT) [1] have very ambitious requirements (for example, low latency and high bandwidth links) that will stress the network's capabilities, especially in the inter-domain environment. Addressing those network requirements within an Internet not designed to support them is a challenging task. Therefore, new network architectures and technologies have to emerge to explore the full potential of the current Internet infrastructure [15].

There are many surveys of the BGP that describe its issues, for example the BGP anomaly [16], security [17,18], the expressiveness and safety of policies [19], transient loops [20], scalability [21], low convergence [22], and others. However, as far as we know, this is the first survey of inter-domain routing to focus on the control plane of the inter-domain routing. Although the Internet relies mostly on the BGP control plane for inter-domain routing, this survey also includes approaches to change the control plane that goes beyond the BGP.

Thus, the contribution of this survey is providing an original classification, i.e., to evolve the control plane of the inter-domain routing. In addition, this paper discusses the challenges for the evolution of current and new control planes. The remaining structure of the paper is organized as follows: Section 2 depicts the related surveys. Section 3 provides an overview of important concepts used in inter-domain routing, such as the BGP decision process and traffic engineering tools of the BGP, and others. Section 4 presents the challenges of making new solutions for the control plane of the inter-domain. Section 5 classifies the previous works to evolve the control plane; Section 6 discusses and reports the lessons learned from this survey. Section 7 provides the final thoughts of this survey.

2. Related Surveys

This section depicts the scope of this survey, as well as the related surveys on approaches to change the inter-domain routing control plane. Table 1 compiles the major surveys related to this work. The main idea here is to explain how this survey is different and complements other related surveys to provide a more understandable and comprehensive state-of-the-art revision for the control plane of inter-domain routing.

Table 1. Compilation of related surveys. BGP, Border Gateway Protocol.

Proposal and Authors	Main Focus
Yannuzzi et al. [19]	Issues in inter-domain routing
Bennesby and Mota [22]	BGP convergence
Butler et al. [17]	BGP security
Singh, Das and Jukan [15]	Multipath routing and provisioning

First, currently, the inter-domain routing control plane of the Internet is distributed through different ASs and embedded into the router devices. In general, the control plane of the device is anything that is necessary in order to make all the network protocols work. This includes the drivers for each network interface, as well as the Network Operational System (NOS). Specifically, the BGP control plane is the software responsible for establishing a connection to other BGP devices, creating the inter-domain high-level topology, computing paths to reachable networks and applying filters and advertise routes to allow other networks to share the global state of this AS-level topology and connectivity.

Because the BGP is currently the main inter-domain routing protocol, it is natural to assign the control plane of the BGP as the control plane of the Internet itself. However, this statement

does not hold, since there are other inter-domain routing protocols also composing the Internet. For example, a domain that uses the Path Computation Element (PCE) architecture can use Resource Reservation Protocol (RSVP-Traffic Engineering (TE)) to exchange inter-domain routing information between domains [23].

Furthermore, this survey will not cover obsolete protocols for inter-domain routing, such as the Exterior Gateway Protocol (EGP) [24] and Inter-Domain Routing Protocol (IDRP) [25]. Although those protocols share fundamental properties with the BGP [26], e.g., distributed path selection computation and the control plane embedded into network appliances, they never reach the wide deployment and the success of the BGP. Thereby, it is worth restricting the scope of this survey to tackle the approaches to evolve the control plane of inter-domain routing with special attention to BGP and also "clean-slate" architecture designs and innovative technologies.

Regarding related surveys, Yannuzzi et al. [19] organized and presented several distinct issues on inter-domain routing works, where for each issue description, one main effort was presented to resolve it. The authors considered multi-homing scalability issues, lack of multipath routing, limited traffic engineering capabilities, convergence time, and others. The majority of those issues still remain open, and one of the reasons for that is the currently widely-deployed Version 4 of the BGP (defined in 2006 [6]) embedded into network appliances. Hence, the addition of new capabilities, functionalities or modification of the BGP often takes years from the first draft specification until it reaches the production environment. This difficult and long process of making changes in inter-domain routing with the BGP is called "ossification" of the protocol, and it is depicted in Section 4.1.

Bennesby and Mota [22] focused on the long convergence time required by the BGP. They presented a good and detailed survey about approaches to reduce the delay of the BGP inter-domain routing convergence on the Internet. They indicated approaches to execute experiments and to measure the convergence time on the Internet and also organized the inter-domain convergence works into five categories: efficient policy configuration; speeding up; limiting path exploration; centralized control; multi-path. Despite the fact that approaches to improve the BGP convergence time of inter-domain routing affects the control plane of BGP routing systems, the focus of this survey is primarily on those approaches that seek to evolve the control plane behavior of inter-domain routing.

Security is another field that is affected in inter-domain routing. The design of BGP and its wide deployment on the Internet have been frustrating efforts to change the inter-domain systems. Those systems are notoriously susceptible to myriad types of attacks from incorrect configuration [27] to well-orchestrated initiatives, such as botnet [28]. Thus, BGP systems can be used to directly or indirectly produce anomalies in the inter-domain [16], because the BGP has no effective mechanisms to check the accuracy of routing information. For example, the standard BGP does not provide an efficient authentication measure for advertising routes. Butler et al. [17] compiled the proposed security extensions to the BGP and discussed the difficult trade-off between acceptable costs and practical and suitable improved security measures. Although security plays a paramount role in the inter-domain routing system, it is not the primary aim of this survey.

Other initiatives to overcome BGP limitations also affect the control plane. For example, the BGP follows a destination-based forwarding paradigm [6], and that approach does not allow one to explore the path diversity of the current Internet topology. An extensive survey about multi-path routing and provision on the Internet is provided by Singh, Das and Jukan [15]. They depicted the multi-path problem using the entire TCP/IP model (layers: application, transport, network, link and physical), where all network layers present particular challenges and issues. For inter-domain routing, the focus will be on the network layer and how approaches to change the control plane can incorporate the multi-path capabilities.

Therefore, this survey presents a more comprehensive literature review about approaches to evolve the control plane of inter-domain routing. Moreover, it provides readers with insights into the promising efforts and how the problem of evolving the control plane of inter-domain routing may be better addressed.

3. Background

The Internet is a collection of tens of thousands of independently operated networks, simply called Autonomous Systems (ASs). An AS can be an Internet Service Provider (ISP), a campus, a content provider or any other independently operated networks. Thus, to carry traffic from one AS to another, an AS requires two types of routing system: intra-domain routing; and inter-domain routing.

Intra-domain routing is the process routing network traffic inside any single autonomous system in as a fast, effective and reliable way as possible. Examples of protocols for intra-domain routing are Open Shortest Path First (OSPF), Routing Information Protocol (RIP) and internal BGP (iBGP). However, for inter-domain routing, the focus is on applying routing policies and distributing routing reachability information among ASs. For the inter-domain routing system, the external BGP [6] (BGP from now on) is the standard protocol of the Internet.

3.1. BGP Control Messages

The BGP exchanges messages between ASs using the Transmission Control Protocol (TCP). The TCP port number 179 is allocated exclusively for the BGP protocol. The advantage of using TCP is avoiding the BGP control plane having to manage message delivery and flow control between BGP speakers (or peers), which simplified the BGP design. Thus, a BGP peer has a reliable way to exchange Network Layer Reachability Information (NLRI) and compose the Routing Information Base (RIB).

Each BGP peer needs to be manually configured with a set of parameters to enable a BGP connection [6,19]. There are four types of BGP control messages to be exchanged after a TCP connection is established between two BGP peers [6]:

- OPEN message: sent to open a BGP session and to verify the connection's parameters;
- UPDATE message: to transfer network reachability information by advertising and withdrawing routes;
- KEEPALIVE message: periodically sent to ensure that the connection between the peers is still reachable;
- NOTIFICATION message: used in response to special or error conditions.

Additionally, the BGP is a path vector protocol, and it uses a sequence of Autonomous System Numbers (ASNs) for characterizing the path. Thereby, when the BGP updates travel through different ASs, the BGP routers prepend their ASN to the AS-Path attribute. The AS-Path attribute of BGP carries the ASNs that a given network prefix traversed. If a router receives a BGP update message and detects its own ASN in the AS-Path attribute, then the router will ignore the update because it is a routing loop once the message has already passed through the AS.

Each BGP update message contains NLRI and BGP information to apply the routing process. For the BGP, the RIB is constructed through the BGP decision process executed in the BGP control plane.

3.2. BGP Control Plane

The BGP Control Plane is the place where decisions about how to handle the network traffic are made and where the traffic is sent. Figure 1 presents an abstraction of a BGP router in which the BGP control plane is modeled.

The responsibilities of the control plane are managing network traffic, setting system configuration and the exchange of routing information. To set up the control plane, an *User Interface* is provided and is often the command line of the network appliance.

The BGP control plane uses UPDATE messages to exchange Network Layer Reachability Information (NLRI) with other routers to create the topology view of the network state and to build the routing table. The BGP configuration reflects the business model of the organization that executes it. The main goal of the BGP is to reflect the desired inter-domain routing policy of a particular AS. The BGP routing decision process applies the filtering and export for a given AS to learn routes from

its neighbor and re-advertise them. The final goal of this BGP decision process defines one "best" route per prefix.

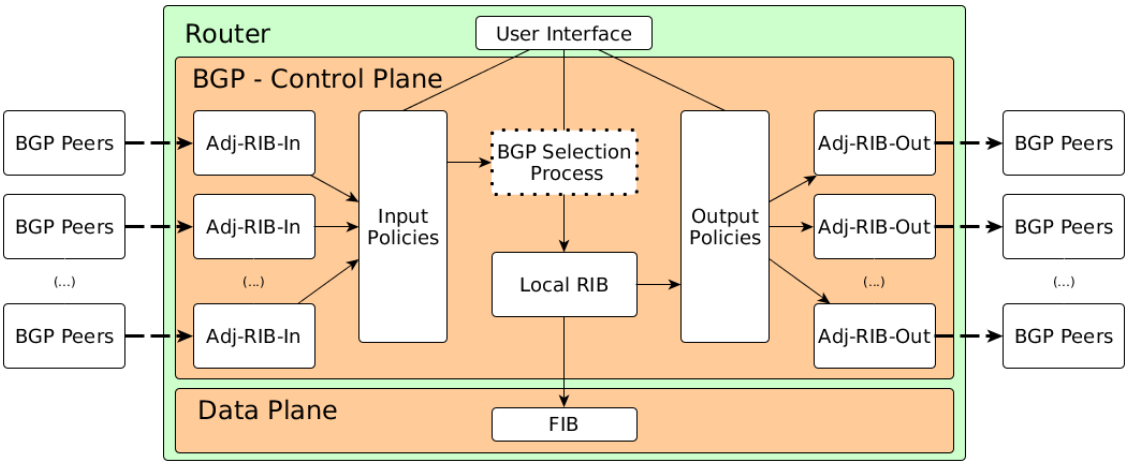


Figure 1. Model of the BGP control plane. RIB, Routing Information Base.

Once a TCP connection of the BGP is established and the route information is exchanged, the Routing Information Base (RIB) is filled. The adjacency table *Adj-RIB-In* is the input for the BGP routing decision process, and it is where the attribute manipulation is also carried out (such as checking *communities* values). Then, the import policy/filter determines which routes are acceptable from each BGP peer. This generates a new database called the Local Routing Information Base *Local RIB* that stores all acceptable routes learned from all BGP peers plus the internal routes, which are routes that belong to the AS and were learned through intra-domain routing protocols. Thereby, to construct the Local RIB, the control plane compiles information of the BGP, and all other routing protocols (for example, injected by OSPF and RIP) and static routes enter by the network operator.

Once the routes are learned, the BGP control plane has to decide a single "best" next hop of each destination. First, if the prefixes learned are unique, then they are installed in the forwarding table of the BGP appliance, and the longest prefix matching is applied. However, if some prefixes have the same subnet mask, but different next hops, then the BGP uses its tie-break algorithm to decide what is the next hop for a given network prefix. Table 2 presents that algorithm, where the priority indicates the sequence of the criterion used in this process. The first criterion for the BGP route selection process is preferred high *Local preference* values, which is a numerical value that a network operator, in the local AS, can assign to a particular route. If the *Local preference* value is equal for more than one route, then the BGP will follow another tie-break criterion. This way, the BGP decision process selects just one *best* route towards each destination.

The finalization of the BGP decision process is the export policy/filter that determines which routes can be sent to each *Peer*. Again, the attribute manipulation is also applied on the routes, and then, they are stored in the *Adj-RIB-Out* database. Then, other *Peers* can learn the routes available for them. All the routing information is then processed to update the routing tables of the BGP router. The control plane functions do not process each individual packet of the device. This responsibility belongs to the data plane elements.

The *Data Plane* is also known as the *Forwarding Plane*. It forwards network traffic to the next hop along the route to the selected destination following the logic given by the control plane. The Forwarding Information Base (FIB) stores the information of which interface packets should be forward to. Thus, the *Data Plane* elements (e.g., routers or switches) use the FIB to forward incoming and outgoing packets or frames to one of its interfaces. For a BGP router, all packets pass through the *Data Plane* of the router.

Table 2. The BGP path selection decision process. AS, Autonomous System; MED, Multi-Exit Discriminator.

Priority	Criterion
1	Prefer route with highest Local preference
2	Path originated by a local router
3	Path with shorter AS-path length
4	Path with lowest origin code
5	Lower MED values for routes from the same neighboring AS
6	Prefer routes learned from external BGP (eBGP) rather than internal BGP (iBGP)
7	Path with closest next-hop
(...)	Other BGP tie-break

3.3. Traffic Engineering with BGP

Control of the outbound network traffic is an easy task. Since an AS controls the decision process on its BGP routes, it can select each best path to reach a particular destination through its peers. The AS can rely on the *Local preference* attribute, for example. By assigning appropriate values, the AS indicates which route should be considered as the best route to the BGP routers [29].

However, it is not a simple task to control inbound network traffic because it requires techniques to be applied that do not guarantee its effectiveness [30]. A network operator can use the following techniques to influence the incoming network traffic with the BGP [31]:

- Selective advertisement: to rely on selective advertisements and announce different route advertisements on different links;
- AS-path prepending: by default, the BGP prefers the route with the shortest AS-Path length when two or more routes exist to reach a particular prefix. Increasing the AS Path length of a particular route may change the way that the BGP selects the best routes and consequently how the other AS traffic is handled;
- Multi-Exit Discriminator (MED): MED is a hint to external neighbor routers about the preferred path into an AS that has multiple entry points. This suggestion can, or not, be acceptable for the neighbors;
- Communities: are "tags" associated with advertisement prefixes and appended pre-arranged communities can be used to influence path selection of other ASs if the neighbors consider those communities in their routing decision process.

Therefore, network operators can only rely on the manipulation of the BGP's attributes to apply any traffic engineering technique. However, for inbound traffic engineering, those approaches only try to influence the routing decisions of external ASs, in order to obtain their desired inbound traffic distribution.

Nonetheless, because each AS selects preferred routes based on its own policies, usually the BGP inbound techniques lead to a trial-and-error process with no guarantees of success. Therefore, the agreements, contracts and AS relationships dictate how the configuration of the BGP should be performed for a given AS.

3.4. AS Relationships

AS relationships determine how routing policies must be set up to absolve the business constraints, agreements and requirements. They may be complex and are not, usually, exposed for public access. However, it is possible to abstract the relationships among ASs by simplifying them into one of the two types:

- Customer-to-provider: the relationship where the AS provider is paid by the customer AS to carry customer network traffic from or to other networks;

- Peer-to-peer: the ASs involved agree to share the costs of the connectivity among them, and then, all traffic between them is free of charge.

Furthermore, the customer-to-provider relationship ensures that AS providers are paid by the customer regardless of the direction in which traffic flows. Thus, for a particular AS, it is preferable to first route traffic for customer links, then peer-to-peer links and finally to provider links (when it is acceptable). Because the volume of traffic matters to define a transit AS profit, it is mandatory to control how the inbound and outbound traffic is routed. Besides, for non-transit ASs' (stub ASs) control, the inbound traffic is mandatory to reach the full utilization of their inter-domain links.

4. Issues in the Evolution of the Inter-Domain Routing Control Plane

There has been a myriad of publications on the inter-domain routing field, and despite the success of the Internet, it still has some crucial issues and research challenges regarding its operation and design that need to be addressed. This section presents the most evident issues described in related works that impact the evolution of the control plane inter-domain routing systems. Each issue is explained and systematized into the following types: ossification; backward compatibility; distributed configuration; complexity routing policies; coordination among ASs; traffic engineering.

4.1. Ossification

The Internet architecture is no longer a coherent whole. It has various components such as transport protocols, router mechanism, firewalls, load balancers, security mechanisms and other middle-boxes. Furthermore, the BGP is one of the most successful protocols on the Internet, and although many researchers have indicated issues related to the BGP since its inception (e.g., lack of end-to-end service guarantees, long convergence time, security issues [17]), practical deployments for new network architecture and protocols in the inter-domain environment are difficult to achieve.

The major problem for evolving the inter-domain routing system is called "ossification", where the architecture becomes very dependent on the protocol and new features are inherently difficult to introduce into the network [9,32,33]. For the BGP, the ossification is due to economic reasons and the fact that backward compatibility has to be assured since there is no flag day to switch to a new architecture. Thus, all BGP appliances have to execute the same version of the protocol to operate appropriately, or anomalies in the network may occur (e.g., BGP black holes).

In other words, the BGP is an inflexible protocol as a consequence of the control and data plane being embedded into the network hardware, and hence, whether the protocol is operational depends on the network equipment used. The dependency between a specific infrastructure and the hardware required creates a barrier to architectural innovation in the inter-domain routing. Hence, a new feature for the BGP has to have a minimum integration within heterogeneous networks and interoperate through different administrative domains (e.g., the Internet). Those requirements frustrated new proposals to evolve the BGP and the ecosystem of inter-domain routing [34].

4.2. Backward Compatibility

A new feature for the BGP has to have a minimum integration within heterogeneous networks and operate through different administrative domains (e.g., the Internet). Those requirements frustrated new proposals to evolve the BGP and the ecosystem of inter-domain routing [34]. One of the main reasons for this is new proposals that have to be maintained with the infrastructure already built, and ASs will not rely on immature technologies that do not prove to be profitable or are not operable with other ASs on which they depend [35].

Thus, the difficult-to-change architecture of the Internet creates a mandatory requirement for integration among different proposals and the BGP. The backward compatibility imposes a limitation to "clean-slate" proposals. Brand new and incompatible BGP proposals are considered unrealistic [36]. In fact, in the more than two decades since the first version of the BGP protocol [37], much scientific

and industrial effort have been made to overcome the BGP limitations and failed to make it a flexible protocol. The backward compatibility with the BGP for the new approaches in the inter-domain environment continues to be a mandatory requirement.

However, a major criticism of the BGP is that it is not suitable for the next generation of inter-domain networks [35]. The main argument to sustain that claim is any new proposal for inter-domain routing has to be part of traditional networks to operate on the Internet and those proposals will be restricted by the limitations of the BGP.

Moreover, the BGP is a widely-adopted protocol used in the infrastructure of the major part of the Internet. It is an inflexible protocol, and it is difficult to incorporate new changes into the network infrastructure. Therefore, the control plane of the inter-domain routing must be evolved instead of receiving a revolution. Evolving the Internet control plane is not an easy task because to be practical and useful, it is almost mandatory to have backward compatibility with the current technologies [19].

4.3. Complexity Introduced by the Distributed Configuration

The traditional approach for the inter-domain routing is through a fully-distributed path selection computation in IP routers that limits the capacity of individual ASs in terms of the management scalability of path selection [38]. A network configuration that changes frequently, to suit the business and organization's desires, is a counterproductive challenge.

Thus, the big challenge of distributed configuration concerns the complexity of keeping a consistent network policy through all routers. For example, Figure 2 presents the problem of applying the following policy: allow the learning routes advertised by ISP_B to be installed into the customer network routers whilst not allowing those routes to be re-advertised to ISP_A.

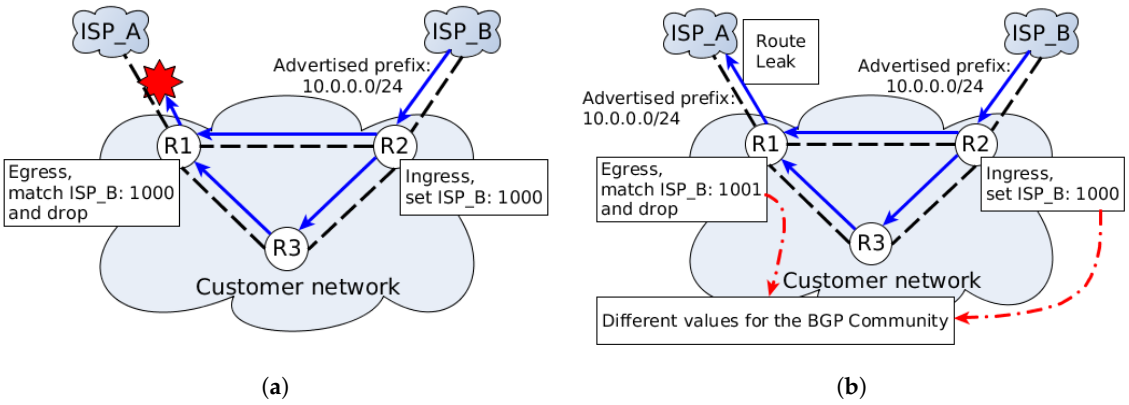


Figure 2. Example of the distributed configuration for the deployment of a routing policy. (**a**) Distributed configuration using the *Communities* of the BGP; (**b**) different values cause the violation of the routing policy (route leak).

One way to implement this policy is to use communities of the BGP. Then, suppose that a network operator installs the community value of 1000 to routes learned from ISP_B, and for every board router (in the case of Figure 2, just R1), configure an outbound filter to deny all prefixes with the community value of 1000 (indicating that those prefixes come from ISP_B). In Figure 2a, routers R1 and R2 have the correct values of the BGP Community. However, when the number of board routers is several and there is a high frequency of changes/updates in routing policies, a distributed configuration may be a bad idea for the control plane of the routing system due to it being hard to trace incorrect configurations that violate the routing policies. Figure 2b presents a scenario where the given routing policy was violated because of the incorrect value of the BGP community used in R1 (1001 instead of 1000), which caused a route leak of the ISP_B prefix to reach ISP_A.

The complexity of managing the configuration in distributed devices to make them operate with the acceptable network behavior can be a challenging task. Additionally, network management is a complex activity due to it requiring the enforcement of the high-level administration network policies in the network.

To impose those requirements, it is necessary to individually visit each network device and perform low-level instructions/commands (often vendor-specific) on them. Depending on the number of network devices, carrying out such procedures is slow and error-prone [39], and a local network error can affect all the other networks. For example, for the famous case of the Pakistan Telecom incident BGP misconfiguration, in which the access to YouTube in that country was restricted, the company advertised an unauthorized prefix causing many ASs to lose access to the site. Hence, the complexity introduced by a distributed configuration can affect not only the specific network where a misconfiguration occurs, but also the whole inter-domain routing environment.

4.4. Conflicts and Uncertainty in Inter-Domain Routing Policies

The BGP incorporated routing and policy requirements into one seamless protocol. For inter-domain routing, each BGP router has its own view of the network state and applies routing policies based on its local configuration. This led to the concept of the routing policy, which can be understood as how routing decisions are made to compose the network reachability state [16]. The difference between routing and policy control is that the first is more related to an engineering effort and the second is strictly about business [35]. Both functions are embedded into the BGP current protocol version, despite the fact that its original design was only for routing purposes.

Moreover, different types of ASs deploy different types of routing policies into their domains, and that diversity of policies can eventually lead to conflicted ones. An example is the application of inbound traffic engineering techniques using the BGP techniques. The main idea of an AS to control its inbound traffic is to fulfil the AS' businesses interests. However, applying the BGP mechanisms for inbound traffic control (such as *Selective advertisement* or *AS-path prepending* [30]) is a counter-productive approach because it is not possible to guarantee the effectiveness of the desirable results.

In fact, the BGP techniques try to influence the routing decisions of external ASs, in order to obtain their desired inbound traffic distribution. Hence, a network operator that uses those approaches leads to a trial-and-error process, since other ASs can easily ignore or withdraw the BGP *suggestions* coming through BGP update messages. Indeed, the problem of inter-domain routing traffic engineering can be seen as a conflicting one, in which the interactions between ASs can be modeled as game theory and nonlinear programming [30].

Besides, it is very tricky to discover what the network traffic distribution of the inter-domain environment will be when policies between domains have to change. The prediction of how much bandwidth will be consumed or how the traffic will be distributed when a domain desires to change its inter-domain routing policies for a given prefix are difficult to estimate [40]. Therefore, proposals to evolve the control plane of inter-domain routing have to provide schemes, mechanisms or protocols to overcome the BGP limitations to express new and refined policies that avoid conflicts and uncertainty in the inter-domain routing policies.

4.5. Coordination among ASs

The inter-domain routing on the Internet is characterized by the use of best efforts for carrying network traffic, where thousands of distributed and connected ASs make their own decisions about how traffic should be routed and forwarded. Besides, it is assumed that packets can be lost and suffer delays, but the overall network will still to be operational and functional. Although the resilience requirement is one of the main concerns, other attributes are desirable for the inter-domain routing environment. For example, some network applications, such as Voice over IP (VoIP), require guarantees from the network for its appropriate utilization, and to provide end-to-end requirements, it is fundamental to have some level of coordination among ASs.

In the inter-domain routing, the coordination between ASs depends on the technology used. In general, each AS provides the manual configuration of BGP router peers to exchange NLRI. Those configurations are aligned with the routing policies and describe what is or not allowed to be advertised between neighbor ASs. Thus, the coordination among domains is often restricted to ASs that have a previous business relationship or some type of an agreement, such as a customer-to-provider relationship. For example, if a stub AS requests (usually via e-mail) the verification of the BGP configuration to a transit AS that does not have any formal relationship with the requested AS, it is expected that the request may not be fulfilled by the transit AS (often ignored).

One motivation for improving the coordination among ASs for inter-domain routing is security [17,18]. For example, that it is difficult to enforce and track the origin of ASs that advertise a given IP prefix is a security issue that threatens the inter-domain routing system. Relying on the BGP attributes (e.g., AS-Path attribute) for such tasks has demonstrated its ineffectiveness over the last few decades. Thereby, deliberate network attacks (e.g., Man-In-The-Middle (MITM) or Distributed Denial of Service (DDoS) [41] attacks), or even misconfigurations or errors [42] in a BGP router can cause and affect connectivity problems on the whole Internet. Those issues occur because the standard control plane of the BGP was not designed to provide security mechanisms for ASs' trust of the NLRI advertised on the Internet.

4.6. Traffic Engineering in the Inter-Domain

The traffic engineering inside an AS is performed using intra-domain routing systems, which are the processes of routing inside any single AS with the purpose of delivering the packets as efficiently as possible. To manage intra-domain routing, there are a couple of routing protocols, for example OSPF. Each protocol has its own direct mechanisms to reach the goal of applying traffic engineering techniques. However, inter-domain routing that fulfills traffic engineering requirements (e.g., QoS) is more tricky.

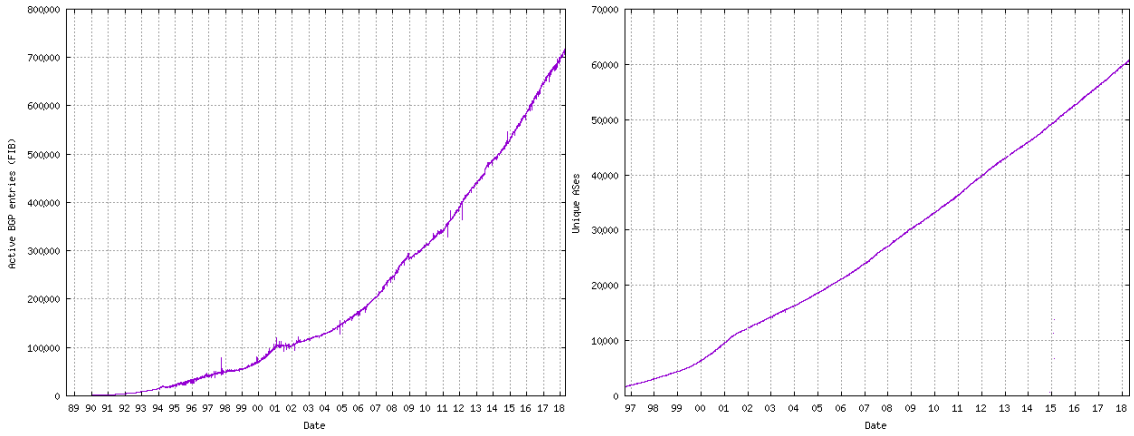
The major design focus of the BGP was a routing protocol capable of applying routing policies and scale when exchanging connectivity information, once scalability is a paramount requirement for inter-domain routing protocols. The BGP has proven its scalability and efficiency to impose routing policies over years of deployment. Nonetheless, ASs that use exclusively the BGP for inter-domain routing cannot receive other types of routing information other than connectivity. Besides, due to the fact that the BGP is designed to use only one best route to each destination entry (see Section 3.2), the control plane has limited connectivity information for routing in a more optimized route selection when it is possible.

For example, due to the lack of direct mechanisms to explore the path diversity of the Internet, ASs have been seeking to improve resilience requirements for their domains, and a common technique to reach that goal is the ASs splitting their prefixes and advertising them for different paths. The side effect of this technique is the Internet routing table growth.

Figure 3 presents the Internet routing table size growth over almost the last two decades. As is depicted in Figure 4, the Internet is composed mostly of stub ASs, and the exhaustion of IPv4 (re-use), provider-independence addressing and load balancing and fail-over techniques for multi-homing ASs are stressing the current inter-domain routing scheme [19]. The exponentially-growing table size on the Internet is a scalability issue that threatens the future of the Internet, and the consequences are, for example, expensive router devices and increased delays for convergence time [22].

On the one hand, BGP does not transport network metrics, such as capacity, bandwidth or cost, to create the topology state of its path-vector algorithm. Having those types of information is crucial to apply traffic engineering optimization tasks over network traffic. On the other hand, flooding inter-domain routing with AS internal network metrics can impose an overhead in the communication between domains, revealing sensitive operational information (for example, bandwidth utilization in inter-domain links) or detailing their view of the network status. Therefore, exploring the full potential of Internet path diversity, avoiding the side-effects of TE techniques and having appropriate

tools for managing traffic engineering tasks in the inter-domain environment with security and in alignment with the ASs' business requirements are the trade-offs for the next generation of inter-domain routing proposals.



(**a**) Active BGP entries (**b**) Unique number of ASs

Figure 3. The Internet scalability issue caused by the application of traffic engineering of stub ASs. (**a**) The exponential growth of routing table size captured by active BGP entries at FIB since 1989. Furthermore; (**b**) is the unique number of ASs on the Internet from 1997 until 2018. The data were extracted from http://www.cidr-report.org/as2.0/.

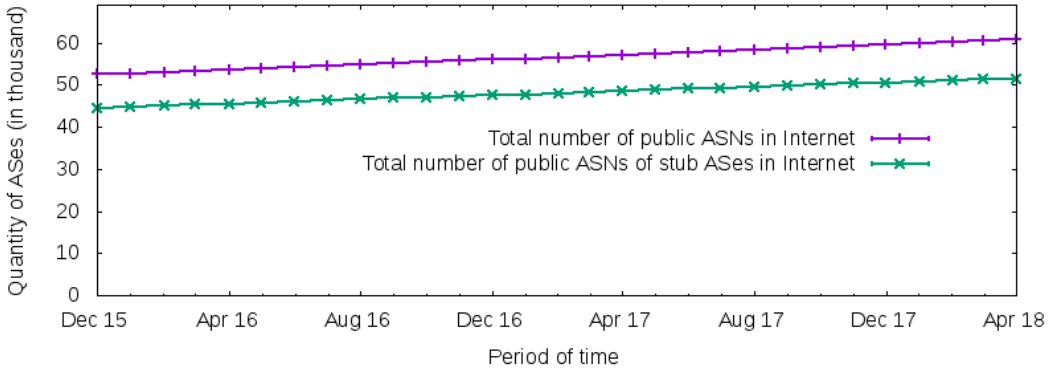


Figure 4. The total number of ASs and stub ASs on the Internet from December of 2015 to April of 2018.

5. Classification of Efforts for Evolving the Control Plane

This section is dedicated to exploring the classification of efforts to change the inter-domain control plane. First, each one of the criteria is depicted and explained. After that, the different works to evolve the control plane of inter-domain routing are classified based on the criteria chosen.

5.1. The Criteria

5.1.1. Concepts

The concept type used in the proposals is one classification criterion for works to evolve the control plane . The concept is the set of principles and designs adopted by a work in the literature to approach the network research problem. Thereby, this survey classifies two concept types: *Traditional* and *Software-Defined Networking (SDN)*.

- Traditional: The traditional networks are characterized as all the network logic embedded into network appliances. They have a distributed nature, and to solve a specific networking problem they, need to act individually on the affected appliances and apply manual changes in their configuration.

Traditional network protocols have been developed and deployed by combining software and hardware into network devices (e.g., TCP/IP). In other words, closed and proprietary network systems have been produced with long development cycles (usually years) and bring new network functionalities that frequently require the acquisition of new hardware with such features. Besides, proprietary boxes often alter the configuration, as well as the compatibility of APIs (Application Programming Interfaces) across vendors (and even across different products from the same vendors [43]). Therefore, legacy and discontinued products make the integration with new network devices a hard to often impossible task [44].

- SDN: Software-Defined Networking (SDN) is emerging as a new network paradigm [45–48]. SDN proposes a separation of software-hardware from devices (vertical integration). Thereby, SDN has the potential to enable new technologies, network programmability and the flexibility of functionalities on network devices.

A major feature of SDN is the decoupled control and data plane. This allows a centralization logic of the control to be fully aware of the network state, enforce network policies, routing decisions, forwarding information, and so forth. Many technologies apply the concepts of SDN. The most notable one is the OpenFlow protocol [49]. OpenFlow is an instantiation of the concepts of SDN [43], which is becoming a standard de facto instance of SDN in the academic and industry field [50].

Touching upon OpenFlow, it provides a programmable interface between the OpenFlow controller (the network logic) and OpenFlow Switches (forwards packets based on controller logic). Besides, OpenFlow rules follow the concept of flow, which is a sequence of packets sent from a particular source to a particular destination following a given path [39]. The OpenFlow rules are capable of identifying and matching TCP/IP header fields, which can provide fine-grained rules for the definition of traffic flows inside OpenFlow networks.

5.1.2. Approach

The approach can be a new architecture or network protocol to evolve inter-domain routing systems or both.

- Architecture: This is when a work describes a network system that details its functions and the interactions between its components or other network systems.
- Protocol: This is when a work depicts a set of rules and conventions for operation and communication between different network entities.
- Architecture/protocol: This includes either the architecture or protocol approach.

5.1.3. Control Plane Placement

Other criteria adopted in this survey are the control plane placement [51,52], which can be as follows:

- Distributed: Each control plane element is uniquely responsible for composing the network state and performing the routing computation. Thus, those elements perform independent computation about routes and are capable of managing the portion of the network that is directly connected to it.
- Centralized: This approach is based on a single control plane that manages all the network devices.
- Logical centralized: Although multiple elements to manage the network can exist, one layer of abstraction aggregates all those elements into a seamless solution.

5.1.4. Explore Path Diversity

The current inter-domain routing protocol follows the BGP's destination-based forwarding paradigm, which indicates that all forwarding decisions about IP packets will rely exclusively on the IP destination header field. Hence, BGP will only select one "best" route per prefix when it is constructing the RIB. Thus, even when there are multiple paths to reach a given network, only one of them will be selected [15,53]. Unlocking the full potential of the Internet path diversity (such as resilience or QoS) is a goal of various previous works. This work analyzes the following criteria to explore path diversity:

- Overlay: The control plane creates networks that run independently on top of another network.
- Sourcing routing: The sender has the possibility of specifying the paths that the packet will take through the network.
- Based on flows: This is the set of network rules that the control plane defines and includes the sequences of nodes that a given packet has to pass between source and destination.
- Inter-domain negotiations: The solution provides mechanisms to allow each path to negotiate to explore the path diversity of the network.
- Alternative routes: Instead of using one single best path per prefix, alternative routes try to achieve resilience, security or optimize bandwidth utilization for inter-domain interconnections exploring the availability of multiple paths.
- Not Applied (N/A): This is when the work does not provide direct evidence of how it explores the path diversity. It can occur, for example, when the research is just an architecture description or other high-level abstraction.

5.2. Efforts to Evolve the Control Plane of Inter-Domain Routing

The efforts to evolve the inter-domain routing control plane were classified as follows: *Brand new design*; *Incremental improvement*; and *Inter-domain communication*.

5.2.1. Brand New Design

Clean-slate redesigns seem to be a very attractive approach to make a new control plane for inter-domain routing without the cumbersome backward compatibilities requirements. For traditional networks, a new protocol for inter-domain routing has the potential to overcome the limitations and drawbacks of the BGP. Table 3 compiles works with a brand new design for inter-domain routing using the criteria presented in Section 5.1.

Feedback-Based Routing (FBR) [54] was inspired by standard engineering practice of design dynamic systems with feedback control theory. Thus, instead of using just connectivity information for routing like the BGP, FBR creates the network state based on connectivity and structural information (such as quality and state of inter-domain links) received from routers that composed the final solution. FBR developed and used its own protocol for inter-domain routing, the Wide-area Relay Addressing Protocol (WRAP). With WRAP, FBR applies a sourcing routing scheme where the core routers of the Internet should be in charge of propagating structural information while the routing decisions occur at the routers at the edge of the network, in which they compute the network routing to achieve the end-to-end performance requirements.

Bandwidth-Aware Routing in Overlay Networks (BARON) [55] was a proposal to overcome the limitations of the default best effort Internet routing. Hence, overlay routing was used to improve end-to-end performance parameters, especially the bandwidth requirement. Furthermore, to create a feasible and scalable solution, BARON explores the Distributed Information Nodes (DINs) database that was used to distribute the node information across the network. The major drawback of overlay solutions for evolving inter-domain routing is that they normally imply additional complexity regarding the overhead that the tunnels introduce in order to be properly managed.

Table 3. Classification for proposals to evolve the inter-domain routing with a brand new design. FBR, Feedback-Based Routing; BARON, Bandwidth-Aware Routing in Overlay Networks; MBGP, Multi-Path BGP; AMIR, Another Multipath Interdomain Routing; NIRA, New Internet Routing Architecture; MLV, Multi-dimension Link Vector; RCS, Route Chaining System; SDI, Software-Defined Inter-domain.

Proposal and Authors	Concepts	Approach	Control Plane Placement	Explore Path Diversity
FBR, Zhu, Gritter and Cheriton [54]	Traditional	Protocol	Distributed	Sourcing routing
BARON, Lee et al. [55]	Traditional	Architecture	Distributed	Overlay
MBGP, Fujinoki [56]	Traditional	Protocol	Distributed	Alternative routes
Multipath BGP, Beijnum et al. [57]	Traditional	Protocol	Distributed	Alternative routes
AMIR, Qin et al. [58]	Traditional	Protocol	Centralized	Sourcing routing
NIRA, Yang et al. [59]	Traditional	Architecture and Protocol	Distributed	Sourcing routing
MLV, Chen et al. [60]	SDN	Architecture and Protocol	Centralized	Based on flows
RCS, Wang et al. [61]	SDN	Architecture	Distributed	Inter-domain negotiations
SDI, Wang, et al. [62]	SDN	Architecture	Distributed	Inter-domain negotiations

Fujinoki [56] proposed the Multi-Path BGP (MBGP) to improve the network bandwidth utilization and avoid dis-connectivity when an external link fails. MBGP was a new network protocol to explore the multipath with a solution based on BGP updates. Furthermore, to overcome a single route for a destination network, the Multipath BGP [57] proposed a change in the BGP's path selection and path dissemination rules to explore the utilization of multiple paths in concurrence without compromising loop-freeness. Although MBGP and Multipath BGP are solutions to increase the exploration of path diversity on the Internet, the proposals were only tested in simulations, and how the network traffic should be split across multiple paths was not appropriately discussed.

Another Multipath Interdomain Routing (AMIR) [58] was a proposal for a new AS-level routing scheme to explore the use of concurrent multiple paths on the Internet. AMIR was designed to compute primary and alternative paths based on negotiating path provisioning among neighboring ASs. The AMIR scheme explores the best available paths for forwarding data in a source routing fashion. Thereby, a given domain can receive multiple paths from its inter-domain partners and choose the best one. Hence, AMIR had the potential to improve the experience of user applications from the network perspective and had the benefit of allowing a more intensified business relationship between ASs that deploy the solution.

Regarding the architecture scheme, the work of Yang et al. [59] presents a new inter-domain routing architecture called NIRA ("New Internet Routing Architecture") that gives the end-host (users) and stub ASs the ability to choose the sequence of ISPs that their packets can take. On the current Internet, the routes are chosen by ASs running the BGP without considered the network source to make routing decisions. The main idea of NIRA was to give the users the ability to choose routes for the Internet from a source routing approach. Thus, the users could select routes that lead to improvement of their network performance, reliability or user satisfaction. Although the NIRA's objective was to transform the Internet architecture, it requires the adoption of a new network protocol called the Topology Information Propagation Protocol (TIPP) to work properly.

Applying the SDN concepts, the Multi-dimension Link Vector (MLV) [60] presented a new mechanism to exchange the network view. MLV uses the OpenFlow protocol [49] in its data plane elements and enables flexible inter-domain routing in an SDN network federation. MLV is a solution based on a link vector algorithm for representing the inter-domain state of the network. With the exchanging of the link vector data structure and the fine-grained rules provided by OpenFlow, the network operator could make decisions regarding paths combining that information. Despite the fact that MLV was a proposal to evolve inter-domain routing among SDN networks, the link vector data structure imposes scalability concerns.

The Route Chaining System (RCS) [61] follows the concept of SDN networks to allow ASs to select routes that do not follow the standard BGP algorithm and explore the possibility of diversity paths of the Internet. RCS focuses on control traffic on transit ASs from the AS source to destinations and also

requires an inter-domain communication layer between ASs to enable the multiple and distributed control planes to be connected to compose the solution.

Software-Defined Inter-domain (SDI) routing [62] advances into the inter-domain support of flexible routing policies to forwarding packets, where multiple fields of the IP packet header could be used for matching (flow-level), instead of just using the BGP's destination-based forwarding paradigm. SDI also provides a mechanism to treat a large number of flow table entries required to represent the forwarding fine-grained flows. For the control plane placement, the SDI solution keeps each domain with its own control plane, which computes paths individually. To explore the path diversity between SDI domains, flow schemes are exchanged.

Summary: Clean-slate proposals are suitable for a very specific application, when used, and cannot be broadly adopted because they are incompatible with the current control plane of the Internet. In addition to traditional solutions, a new protocol proposal must be executed inside network devices or all network devices that utilize such solutions need to be modified, and such a situation may require CAPEX (CAPital EXpenditure) and OPEX (OPerational EXpenditure) to be operational. For example, the network staff would need to be trained for new proposals or protocols, as well as acquire new network devices that support those clean-slate solutions. For the inter-domain routing system with the SDN solutions, those whose approaches are not compatible with the BGP have little practical appeal for wide adoption (such as MLV [60]), and solutions that propagate a detailed representation of the network state suffer from scalability limitations.

5.2.2. Incremental Improvement

Proposals are made to incorporate new BGP network capabilities by changing the protocol behavior, extensions of the BGP or additional control information that is used with the BGP protocol. Table 4 presents the works related to incremental improvements of inter-domain routing.

Table 4. Classification for proposals to evolve the inter-domain routing with incremental improvements. MIRO, Multi-path Interdomain ROuting; R-BGP, Resilient BGP; YAMR, Yet Another Multipath Routing Protocol; STAMP, Selective Announcement Multi-Process; COIN, COntrol INbound; iSDX, Industrial-Scale Software-Defined Internet Exchange Point.

Proposal and Authors	Concepts	Approach	Control Plane Placement	Explore Path Diversity
RCP, Feamster et al. [38]	Traditional	Architecture	Logical Centralized	N/A
MIRO, Xu et al. [63]	Traditional	Architecture and Protocol	Distributed	Inter-domain negotiations
R-BGP, Kushman et al. [64]	Traditional	Protocol	Distributed	Alternative routes
YAMR, Ganichev et al. [65]	Traditional	Protocol	Distributed	Alternative routes
STAMP, Liao et al. [66]	Traditional	Protocol	Distributed	Alternative routes
COIN, Silva and Sadok [34]	SDN	Architecture	Centralized	Based on flows
SIREN, Kotronis et al. [36]	SDN	Architecture	Centralized	Based on flows
SDX and iSDX, Feamster et al. [67,68]	SDN	Architecture and Protocol	Logical Centralized	Inter-domain negotiations
Silva [10]	SDN	Architecture	Centralized	Based on flows

For inter-domain routing, the authors in [38] claimed that the fully-distributed path selection computation in IP routers limits the capacity of individual ASs in terms of management scalability of path selection. Thus, they proposed a Routing Control Platform (RCP), a platform that avoids the complexity of fully-distributed path computation in the inter-domain routing system by centralizing routing control logic. Due to the architecture network abstraction designed by the RCP, it did not describe how, in fact, to explore the path diversity of inter-domain routing; hence, these criteria are not applicable to the RCP. However, the RCP is one important area of research and a precursor of SDN concepts, in which it is indicated that the control plane of a domain should be built in a centralized way [43].

In addition to centralized routing control and to enable multipath routing on the Internet (the BGP uses a single best path), Multi-path Interdomain ROuting (MIRO) [63] proposed the use of overlay networks and specific packet tags to enable multiple paths for inter-domain routing. The idea was to allow a new control plane logic where ASs negotiate alternative paths, as needed, from their

ISPs. MIRO defaults to the single-path routing provided by the conventional BGP, but allows ASs to negotiate alternative paths as needed. This provides flexibility where required while remaining compatible with BGP. Compared to source routing, MIRO gives transit ASs more control over the flow of traffic in their networks.

An idea to protect the inter-domain links against failures is the Resilient BGP (R-BGP) [64]. R-BGP produces failover paths to mitigate the unavailability of the best path selected from the BGP decision process. Thus, when a link fails, the failover path was already computed and ready to be used, avoiding the path exploration time for discovering new paths to networks affected by the failed link. Furthermore, to avoid unavailability when external links fail, Yet Another Multipath Routing Protocol (YAMR) [65] is a resilient solution that explores advertising additional paths that are not contained in the primary path (resulting from the BGP's best path algorithm). Thus, each alternative path receives a label that identifies the links the path needs to avoid. YAMR is deployed in a distributed way, where the control plane of YAMR can be implemented as an extension of the BGP protocol.

The main contribution of the Selective Announcement Multi-Process (STAMP) protocol is executing several BGP instances inside the AS that is used to discover complementary paths [66]. The goal of those complementary paths is established paths that are not affected by the same set of network events. Thus, the STAMP requires minimal modification of the BGP process to become an operational solution and to achieve an improvement in routing stability compared with the standard BGP protocol.

The integration between SDN technologies and BGP has already been investigated and implemented by some researchers [36,69]. The integration with SDN solutions and BGP networks is vital to a practical deployment of SDN proposals. In fact, modern SDN controllers have mechanisms to exchange BGP information with BGP speaker components that behave as legacy routers. For example, the Open Network Foundation (ONF) ATRIUM project proposes a framework to support BGP by use of the ONOS controller [70] and Quagga [71]. Another widely-used SDN controller is the Ryu [72] support, interworking between OpenFlow and BGP, since a BGP function is installed in the Ryu SDN framework.

The COntrol INbound traffic (COIN) framework [34] proposed to evolve the control plane routing system with the OpenFlow protocol. The COIN framework expanded the Ryu SDN controller to provide mechanisms for controlling inbound traffic from ISPs to its multi-homed ASs customers. Thus, the customers could manage how network traffic reaches them through the use of applications in the SDN controllers' ISPs. Those applications, when required and allowed, override the BGP behavior of the ISPs' network infrastructure to fulfil the customer's network traffic management requirements.

With the focus on merging SDN and traditional network concepts, SIREN [36] presented a proposal to integrate the control plane of those two approaches. It combines BGP and SDN principles to improve the convergence time of the BGP at the inter-domain level. To reach that goal, SIREN allows an AS to outsource routing functionality and export it to its ISP control. SIREN is an extension of the previous idea explored in Kotronis et al. [73]. However, a pitfall of SIREN is that this approach limits the ability of the innovation of an AS, considering that a domain has to be subordinate to the requirements established by the outsourcing agreements for managing its network.

Using the idea of overriding the BGP behavior, the proposal of Software-Defined Internet exchange (SDX) [67] and its extension Industrial-Scale Software-Defined Internet Exchange Point (iSDX) [68] explore the SDN centralized control inside the Internet Exchange Point (IXP). iSDX allows the reduction of the forwarding table size of OpenFlow devices used by the IXP participants, the creation of more flexible forwarding policies and the end-to-end enforcing of QoS. iSDX requires a brokerage system to establish multilateral peering; innovation is processed in the Layer 2 scheme (using Ethernet MAC addresses), and a third party orchestrates traffic between participants.

Silva [10] presented a new architecture to manage network traffic in the inter-domain using OpenFlow networks. The idea of the proposed architecture was to use BGP and SDN technologies to provide new mechanisms that allow different ASs to coordinate how traffic should be handled

between them using network applications inside SDN controllers. Thereby, a proof of concept scenario demonstrated that stub ASs can appropriately manage network traffic towards its domain by controlling the parameters of those network applications in its ISPs. The achieved results indicated the potential of the idea to apply different strategies for routing in the inter-domain environment.

Summary: Works to incrementally improve the inter-domain routing try to add capabilities to the BGP control plane, such as exploring path diversity for resilience purposes or increasing the available bandwidth of a domain. One major limitation of the BGP that is tackled by related works with incremental improvement is searching for multipath solutions for inter-domain routing. Thus, instead of using only the one best route per prefix, the use of alternative routes has the potential to improve resilience against link failures, bandwidth availability and security [15,74,75].

5.2.3. Inter-Domain Communication

The control communication between different domains is also an important criterion to be analyzed in related works. Table 5 depicts the related works that evolve the inter-domain control plane routing using some inter-domain communication mechanism.

Table 5. Classification of proposals to evolve inter-domain communication.

Proposal and Authors	Concepts	Approach	Control Plane Placement	Explore Path Diversity
ADD-PATH [76]	Traditional	Protocol	Distributed	Alternative routes
North-Bound Distribution of Link-State and Traffic Engineering (TE) Information, Gredler et al. [77]	Traditional	Protocol	Distributed	Inter-domain negotiations
BGP Administrative Shutdown Communication, Snijders et al. [78]	Traditional	Protocol	Distributed	N/A
RouteFlow, Nascimento et al. [79]	SDN	Architecture	Centralized	Based on flows
WE-Bridge [80]	SDN	Protocol	Distributed	Inter-domain negotiations
Inter-SDN, Bennesby et al. [81]	SDN	Architecture	Centralized	Based on flows
Alto, Alimi et al. [82]	SDN	Protocol	Logically centralized	Based on flows

For ASs that exchange control information with the BGP protocol, they can use the BGP attributes for that purpose. For example, an AS may set MED or Communities' values to alter how the control plane of other ASs selects routes [83,84]. However, the BGP attributes have limited scope and effectiveness [16], and consequently, new signaling mechanisms between different control planes emerged to overcome those restrictions.

To tackle the ability of the BGP advertising just one best route per prefix, ADD-PATH is an extension to the BGP that uses its capability to advertise, identify and add multiple paths to a destination [76]. The standard behavior of the BGP produces and advertises only one best-path to a given address prefix. If two NLRIs are advertised with the same value of the address prefix, the latest advertisement will override the previous one in the RIB. ADD-PATH allows the advertisement of multiple paths for the same address prefix without the new paths implicitly replacing any previous ones. The main idea of this BGP extension is instead of using the address prefix as the primary identifier of a path, it uses a *Path Identifier*, in which each path receives a unique identifier, and that allows multiple values of address prefixes to exist in the RIB.

By exchanging, the topology and information about the current state of the network among routing components are typically used as the interior routing protocol (for example, OSPF) for such tasks.

Generally, the ASs are not willing to reveal their internal infrastructure or the business relationship information among other ASs because of security or business concerns. However, in some scenarios, the link-state or Traffic Engineering (TE) information can be shared with external components of a domain, for example, applications that require end-to-end TE (this is the case of the SIREN [36] proposal where the external control plane was responsible for computing the routing of the customer domain or Multi-Protocol Label Switching Traffic Engineering (MPLS-TE) with Path Computation Element (PCE). The North-Bound Distribution of Link-State and Traffic Engineering (TE) Information [77] describes a mechanism to collect and share link-state and TE information with external components by a new BGP NLRI encoding format.

Another extension for BGP to improve the communication among BGP neighbors is the BGP Administrative Shutdown Communication [78], defined in RFC 8203. It tackles the lack of information when a BGP session was reset or shutdown. Thus, the solution adds a short text message as part of the notification message of the BGP [6]. The purpose of that message is to notify operators about the event that caused the BGP closure.

RouteFlow [79] controls and configures flows of OpenFlow switches using Quagga [71] as the main engine. RouteFlow becomes a proxy for the OpenFlow controller, where all the network logic follows traditional network protocols with inter-domain routing executing the BGP protocol. Furthermore, RouteFlow provides virtualized IP routing services over OpenFlow-enabled hardware, with the main idea of the proposed architecture adopting a west/eastbound interface to make a deeper integration of the routing engines of an ISP and its customers.

As recent surveys indicate, there is not yet a standard west/eastbound SDN interface to exchange network control information between different SDN controllers [39,80,85]. Thereby, to allow the communication between SDN controllers in the inter-domain ecosystem, the authors in [80] proposed an interface for SDN to exchange reachability and topology information, the WE-Bridge [80]. The goals were to present a peer-to-peer mechanism that has to be resilient, secure and exchange network control information for ASs. WE-Bridge was used by RCS [61] and SDI [62] to exchange control information between SDN controllers.

To exchange routing information between SDN domains (a domain that deploys SDN technologies), the Inter-SDN Routing Component [81] was proposed to tackle the problem of integration between the different control planes. Using TCP connections, the new exchange mechanism is inspired by the BGP and incorporates messages similar to the BGP (OPEN, UPDATE, KEEPALIVE and NOTIFICATION), uses RIBs (RIB-In, Local RIB, RIB-Out) and simplifies the route selection decision process. The Inter-SDN claims that the way to solve inter-domain issues is through architectural abstraction (SDN applications) and extensibility properties (the network programmability).

Application-Layer Traffic Optimization (ALTO) [82] (defined in RFC 7285) is the most detailed specification for a standardization of the east/westbound interface for SDN controllers. It provides a network information service with the goal of exporting resources and parameters to network applications. ALTO is based on abstract maps of a network that simplify the state of a network and the applications that can effectively use them.

Summary: Traditional network approaches for inter-domain communications focus on adding new capabilities or modifications to the BGP's messages. However, those approaches require a long cycle (months or years) of development until they reach the production environment. The SDN and traditional network have one point in common: those initiatives tackle the challenge of managing a huge number of network devices that requires coordination among multiple control planes.

In fact, to overcome BGP control plane limitations for inter-domain communication, SDN approaches seek an integration with BGP and coordination between SDN controllers. Additionally, SDN network applications require complex network information that is hidden through inter-domain routing to allow the propriety execution of optimization algorithms in the network [86].

6. Further Discussion and Lessons Learned

This section discusses the topic of the control plane for inter-domain routing and provides some insights into the content in the previous sections.

6.1. Inter-Domain Routing Limitations

The BGP will never select two, or more, next hops per prefix. It always chooses a unique best hop per prefix. Different from internal routing protocols (e.g., the ECMP) where multiple destinations are allowed to a given prefix for load balancing proposes, the BGP standard protocol does not incorporate this behavior. Hence, to network, operators maximize the utilization of external links, and they have to split the traffic using a subnet of the prefix, which has the side effect of increasing the global routing table (Figure 3).

The use of multiple links may have the consequence of improving path diversity and network reliability [74]. The BGP can filter routes by matching prefix, prefix-length and/or based on different path attributes that are associated with each BGP route and are part of an update message. However, the forwarding data plane elements can only forward the packet based on destination prefixes, once the BGP follows a destination-based forwarding paradigm [6]. In other words, routers can only apply their policies and forward decision based on the destination address of the IP packet.

Routing systems that use source addresses, policy-based routing or are based on application requirements cannot be deployed on the current Internet as this is not supported by the current BGP logic of control. Furthermore, novel network applications may require some other fields in the packet header to optimize the inter-domain routing path or simply to distinguish routing by source addresses [60]. Those requirements are not available with the use of the BGP.

Moreover, it has long been known that the Internet architecture has several issues, despite the Internet's unparalleled success. Highly rigid and static, the traditional networking infrastructure was initially designed to operate for a particular type of traffic (text-based content), and that does not satisfy today's increasingly demanding users that request interactive and dynamic multimedia streams. Along with the multimedia trends, the recent emergence of new and innovate technologies, e.g., IoT, has been pressuring the inter-domain infrastructure to support those new types of network demands.

Previous works have attempted to solve these architectural deficiencies with brand new designs or incremental improvements, which have had limited success [87]. On the one hand, the resistance to these new efforts stems from the requirement that new solutions must be mature enough and have obvious benefits. In other words, an AS will not risk its business existence in adopting technologies with unproven scalability, reliability, interoperability and consistency. Moreover, the current Internet's infrastructure took years to reach its current size, and a myriad of ASs is still expecting to reach the Return on Investment (ROI) from that.

On the other hand, many ASs are searching for ways to increase their profit: be more agile to address business requirement changes, provide a network that reduces cost, simplifies operations and supports new and innovative products and services. Thereby, the next generation control plane needs to be more suitable to their business needs, and it is expected that automation [88] and intelligent network traffic control systems [89] will play an important role in evolving the inter-domain routing.

Therefore, to bridge the gap between what is expected and desirable on architectural evolvability and what is feasibly deployable has to include, among other ideas, modularity solutions with BGP compatibility and extensive support of automation.

6.2. New Business Relationships

In traditional networks, the agreements to exchange traffic are usually between ASs that have some physical connection between them. Only in specific places of the Internet is this condition not applied (for example, IXPs). Thereby, through BGP peers, ASs apply the BGP configuration that reflects

the business relationships previously established and that limits the types of business relationships between ASs.

Thus, it is expected that ASs will gain more advantages of the next generation of the control plane for the Internet because this allows them to control and explore the full potential of the Internet-wide infrastructure. For example, the observation of CAIDA's AS relationship database [90] allows the characterization of multi-homed ASs. Considering the period from December of 2015 to April of 2018, Figure 4 presents the total number of public ASNs in CAIDA's AS relationship database, as well as the total number of stub ASs with public ASNs. Therefore, this graph indicates that the majority of ASs on the Internet are stub ASs, and as discussed, its control of routes is limited by the physical bound with its neighbor ASs.

Outsourcing the AS routing logic is one way to establish new business relationships on the Internet [73]. Offloading the routing functions of a customer AS to an external trusted contractor (e.g., transit AS) can optimize inter-domain traffic engineering, evolve inter-domain routing and allow the implementation of collaborative security and troubleshooting schemes.

Another idea is to transit ASs to provide mechanisms to stub ASs that manage its routes [10]. A type of relationship where any ASs can establish a relationship with other non-neighbor ASs is very difficult to achieve in the current Internet architecture, since many network operational tasks (such as manual configuration) are needed. Furthermore, the relationship must make sense from the business perspective, and security mechanisms have to be deployed to guarantee an acceptable level of trust between the domains.

Thus, to establish new business relationships between multiple ASs, a reliable and secure mechanism has to emerge for inter-domain routing. The manual configuration of the BGP and the use of TCP [17] to exchange NLRI are not enough for the next generation of the control plane for inter-domain routing that has to incorporate new mechanisms to exchange and establish network relationships through any AS on the Internet to enable dynamic resources, bandwidth and routing.

Previous works in the field indicate the values of collaboration among ASs with different business models [91–93]. For example, exploring a more intensified collaboration between ASs that produces (e.g., CDN) and consumes the content (e.g., users) can produce gains for all participants [94,95]. Moreover, with new inter-domain communication mechanisms, it will be possible to deploy visionary solutions such as an economy plane for the Internet [96].

6.3. SDN as an Enabling Technology

One of the major features of the BGP is the scalability of the protocol due to its fully-distributed nature. The size-effect of distributed control of the BGP is causing the protocol "chattiness" [19] and the long convergence time [22], since every BGP speaker has to generate the global view of the network state to make decisions about routing. The centralization of inter-domain routing control has the potential to mitigate the BGP issues [7,35,36]. A bird's eye view of the centralized solution has the potential to identify misconfiguration, avoid route leaks, address the satisfaction and dissatisfaction among ASs [31] and understand and perform troubleshooting; all sorts of undesired network behavior will be exposed to the centralized control.

With SDN technologies, the consistency of the network state is encouraged by the principle of logical centralization [52]. The inter-domain routing centralization has the potential to benefit the application of traffic engineering techniques, enforcement of routing policies, network troubleshooting and other desirable features. For example, the proposal of iSDX [68] uses the SDN centralized control in an IXP to allow the creation of more flexible forwarding policies, the reduction of the forwarding table size of OpenFlow devices used by the IXP participants and the end-to-end enforcing of QoS.

The adoption of SDN technologies has the potential to solve the management decentralization problem of the traditional network, as discussed in [97]. Other previous proposals that use exclusively traditional network technologies [38,59] required extensions for the BGP or a brand new network

protocol to make them operational. This results in a difficult scenario that is not easy to deploy or manage for ASs because of CAPEX, OPEX, security and reliability concerns.

New network services can emerge if the current inter-domain routing system allows the evolution of the routing control plane. The traditional network mostly applies the decentralization of the routing decision, and with the advent of SDN concepts, the logical centralization of the routing control plane may enable inter-domain routing evolution.

Thereby, a good question to pose regarding SDN is the following: Why have SDN technologies not yet changed the inter-domain landscape? First of all, it is worth noting that the SDN paradigm is a brand new approach to design networks (although it inherits ideas from other approaches [43]), which is different from the traditional network that has been the main paradigm to construct networks since the Internet's inception. Thereby, the technologies that instantiate SDN concepts are in their early stages, and as they are not mature technologies, wide adoption is not expected.

The most successful SDN technology is the OpenFlow protocol. This protocol has some hindrance regarding memory and signaling utilization [98] because OpenFlow switches usually use Ternary Content Addressable Memory (TCAM) as the main memory to match a flow. That type of memory is very fast, however having the drawback of being expensive with a high energy consumption. Therefore, the fine-grained OpenFlow rules can represent a cumbersome inter-domain environment where the number of prefixes (or flows) is tremendously high [62]. Flow management is almost mandatory for the real deployment of the OpenFlow protocol in inter-domain routing, and that problem can be understood as an extension of the rule placement problem inside OpenFlow networks. A detailed survey about flow management can be seen in the work of Nguyen et al. [45].

Another drawback of the OpenFlow networks is the reliability between controllers and the data plane elements (OpenFlow switches). Once the control and data plane is decoupled, when the control becomes unavailable, the forwarding elements may not continue to work appropriately. Some works claim that the data plane elements need to have some capabilities to fix those scenarios, and a mix of control and data plane programmability can be the key for future network solutions. Ideas for allowing data plane elements to become more flexible and programmable are in their infancy, such as P4 [99] or OpenState [100], and those technologies could resolve the flexibility and performance of OpenFlow switches.

Therefore, to be practical, an OpenFlow solution must manage the flows (installation, aggregation and eviction) and maintain a trade-off among rule installation and the signaling overhead between OpenFlow switches and the OpenFlow controller to maintain the availability of the network [45,101]. For ASs, and especially ISPs, new proposals cannot be adopted for inter-domain routing that represent a risk (reliability, availability, performance, security and other requirements) to their business unless substantial profit is imminent [36].

7. Conclusions

There is still much to be done until the BGP control plane is fully replaced as the main routing core system of the Internet. None of the efforts researched in this work provide all the features to reach that goal. SDN technologies seem to be a prominent technical field for new network architectures, and they are receiving much academic and industrial attention. Beyond the technical requirements, the new proposals to evolve inter-domain routing must be aligned with network operator business vision.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]

2. Baktir, A.C.; Ozgovde, A.; Ersoy, C. How Can Edge Computing Benefit from Software-Defined Networking: A Survey, Use Cases, and Future Directions. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2359–2391. [CrossRef]
3. Raza, M.R.; Fiorani, M.; Skubic, B.; Martensson, J.; Wosinska, L.; Monti, P. Power and cost modeling for 5G transport networks. In Proceedings of the International Conference on Transparent Optical Networks, Budapest, Hungary, 5–9 July 2015; pp. 1–7.
4. Gupta, A.; Jha, R.K. A Survey of 5G Network: Architecture and Emerging Technologies. *IEEE Access* **2015**, *3*, 1206–1232. [CrossRef]
5. Huang, T.; Yu, F.R.; Zhang, C.; Liu, J.; Zhang, J.; Liu, Y. A Survey on Large-Scale Software Defined Networking (SDN) Testbeds: Approaches and Challenges. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 891–917. [CrossRef]
6. Rekhter, Y.; Li, T.; Hares, S. A Border Gateway Protocol 4 (BGP-4). Network Working Group Request for Comments: 4271. 2006. Available online: https://www.rfc-editor.org/info/rfc4271 (accessed on 16 May 2018).
7. Kotronis, V. Centralizing Routing Control Across Domains: Architectural Approach and Prominent Use Cases. Ph.D. Thesis, University of Athens, Athens, Greece, 2015.
8. Hakiri, A.; Gokhale, A.; Berthou, P.; Schmidt, D.C.; Gayraud, T. Software-defined networking: Challenges and research opportunities for future internet. *Comput. Netw.* **2014**, *75*, 453–471. [CrossRef]
9. Chowdhury, N.M.M.K.; Boutaba, R. A survey of network virtualization. *Comput. Netw.* **2010**, *54*, 862–876. [CrossRef]
10. Silva, W.J.A. An Architecture to Manage Incoming Traffic of Inter-Domain Routing Using OpenFlow Networks. *Information* **2018**, *9*, 92. [CrossRef]
11. Potaroo.net. Advertised AS Count. 2016. Available online: http://bgp.potaroo.net/as2.0/bgp-average-aspath-length.txt (accessed on 16 May 2018).
12. Luckie, M.; Huffaker, B.; Dhamdhere, A.; Giotsas, V.; Claffy, K. AS relationships, customer cones, and validation. In Proceedings of the 2013 Conference on Internet Measurement Conference—IMC '13, Barcelona, Spain, 23–25 October 2013; pp. 243–256.
13. Labovitz, C.; Iekel-Johnson, S.; McPherson, D.; Oberheide, J.; Jahanian, F. Internet inter-domain traffic. In Proceedings of the ACM SIGCOMM 2010 Conference on SIGCOMM—SIGCOMM '10, New Delhi, India, 30 August–3 September 2010; p. 75.
14. Ager, B.; Chatzis, N.; Feldmann, A.; Sarrar, N.; Uhlig, S.; Willinger, W. Anatomy of a large european IXP. *ACM SIGCOMM Comput. Commun. Rev.* **2012**, *42*, 163. [CrossRef]
15. Singh, S.K.; Das, T.; Jukan, A. A Survey on Internet Multipath Routing and Provisioning. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2157–2175. [CrossRef]
16. Al-musawi, B.; Branch, P.; Armitage, G. BGP Anomaly Detection Techniques: A Survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 377–396. [CrossRef]
17. Kevin, B.; Toni, F.; Patrick, M.; Jennnifer, P. A survey of BGP security—Issues and solutions. *Proc. IEEE* **2010**, *98*, 100–122.
18. Narayanan, A. A Survey on BGP Issues and Solutions. *arXiv* **2009**, arXiv:0907.4815. [CrossRef]
19. Yannuzzi, M.; Masip-Bruin, X.; Bonaventure, O. Open issues in interdomain routing: A survey. *IEEE Netw.* **2005**, *19*, 49–56. [CrossRef]
20. Qiu, J.; Wang, F.; Gao, L. BGP rerouting solutions for transient routing failures and loops. In Proceedings of the IEEE Military Communications Conference MILCOM, Washington, DC, USA, 23–25 October 2006.
21. Rexford, J. Rethinking internet routing. In Proceedings of the Fourtieth Annual ACM Symposium on Theory of Computing—STOC '08, Victoria, Canada, 17–20 May 2008; p. 55.
22. Bennesby, R.; Mota, E. A survey on approaches to reduce BGP interdomain routing convergence delay on the Internet. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2949–2984.
23. Paolucci, F.; Cugini, F.; Giorgetti, A.; Sambo, N.; Castoldi, P. A survey on the path computation element (PCE) architecture. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 1819–1841. [CrossRef]
24. Mills, D. Exterior Gateway Protocol Formal Specification. 1984. Available online: https://tools.ietf.org/html/rfc904 (accessed on 16 May 2018).
25. Kunzinger, C. Inter-Domain Routing Protocol, 1994. Available online: https://tools.ietf.org/html/draft-kunzinger-idrp-ISO10747-01 (accessed on 16 May 2018).

26. Varadhan, K.; Govindan, R.; Estrin, D. Persistent route oscillations in inter-domain routing. *Comput. Netw.* **2000**, *32*, 1–16. [CrossRef]
27. Zargar, S.T.; Joshi, J.; Tipper, D. A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 2046–2069. [CrossRef]
28. Hoque, N.; Bhattacharyya, D.; Kalita, J. Botnet in DDoS Attacks: Trends and Challenges. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2242–2270. [CrossRef]
29. Ludwig, C. Traffic engineering with BGP. In *Seminar "Internet Routing"*; Technical University Berlin: Berlin, Germany, 2009; pp. 1–10.
30. Wang, N.; Ho, K.H.; Pavlou, G.; Howarth, M. An Overview of Routing Optimization for Internet Traffic Engineering. *IEEE Commun. Surv. Tutor.* **2008**, *10*, 36–56. [CrossRef]
31. Cardona, J.C.; Vissicchio, S.; Lucente, P.; Francois, P. "I Can't Get No Satisfaction": Helping Autonomous Systems Identify Their Unsatisfied Inter-domain Interests. *IEEE Trans. Netw. Serv. Manag.* **2016**, *13*, 43–57. [CrossRef]
32. Esteves, R.P.; Granville, L.Z.; Boutaba, R. On the management of virtual networks. *IEEE Commun. Mag.* **2013**, *51*, 80–88. [CrossRef]
33. Chowdhury, M.K.N.; Boutaba, R. Network virtualization: State of the art and research challenges. *IEEE Commun. Mag.* **2009**, *47*, 20–26. [CrossRef]
34. Silva, W.J.A.; Sadok, D.F.H. Control Inbound Traffic: Evolving the Control Plane Routing System with Software Defined Networking. In Proceedings of the 18th International Conference on High Performance Switching and Routing (HPSR), Campinas, Brazil, 18–21 June 2017.
35. Thai, P.; De Oliveira, J.C. Decoupling policy from routing with software defined interdomain management: Interdomain routing for SDN-based networks. In Proceedings of the International Conference on Computer Communications and Networks, ICCCN, Nassau, Bahamas, 30 July–2 August 2013.
36. Kotronis, V.; Gamperli, A.; Dimitropoulos, X. Routing centralization across domains via SDN: A model and emulation framework for BGP evolution. *Comput. Netw.* **2015**, *92*, 227–239. [CrossRef]
37. Rekhter, Y.; Li, T. A Border Gateway Protocol 4 (BGP-4). Request for Comments: 1771. 1995. Available online: https://tools.ietf.org/html/rfc1771 (accessed on 16 May 2018).
38. Feamster, N.; Balakrishnan, H.; Rexford, J.; Shaikh, A.; van der Merwe, J. The case for separating routing from routers. In Proceedings of the ACM SIGCOMM Workshop on Future Directions in Network Architecture—FDNA '04, Portland, OR, USA, 30 August 30–3 September 2004; p. 5.
39. Kreutz, D.; Ramos, F.M.V.; Veríssimo, P.E.; Rothenberg, C.E.; Azodolmolky, S.; Uhlig, S. Software-Defined Networking: A Comprehensive Survey. *Proc. IEEE* **2015**, *103*, 14–76. [CrossRef]
40. De Deus, M.A.; Carvalho, P.H.; Leite, J.P. Internet capacity: Optimizing autonomous system inbound traffic using specialist knowledge as support for decision-making. *Ann. Telecommun.* **2015**, *70*, 331–343. [CrossRef]
41. Somani, G.; Gaur, M.S.; Sanghi, D.; Conti, M.; Buyya, R. DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions. *Comput. Commun.* **2017**, *107*, 30–48. [CrossRef]
42. Alshamrani, H.; Ghita, B. IP prefix hijack detection using BGP connectivity monitoring. In Proceedings of the IEEE International Conference on High Performance Switching and Routing, HPSR, Yokohama, Japan, 14–17 June 2016; pp. 35–41.
43. Feamster, N.; Rexford, J.; Zegura, E. The road to SDN: An Intellectual History of Programmable Networks. *ACM SIGCOMM Comput. Commun. Rev.* **2014**, *44*, 87–98. [CrossRef]
44. Scott-Hayward, S.; Natarajan, S.; Sezer, S. A Survey of Security in Software Defined Networks. *IEEE Commun. Surv. Tutor.* **2015**, *PP*, 1–33. [CrossRef]
45. Nguyen, X.N.; Saucez, D.; Barakat, C.; Turletti, T. Rules Placement Problem in OpenFlow Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1273–1286. [CrossRef]
46. Lin, P.; Hart, J.; Krishnaswamy, U. Seamless interworking of SDN and IP. In Proceedings of the SIGCOMM '13, ACM SIGCOMM 2013 Conference on SIGCOMM, Hong Kong, China, 12–16 August 2013; Volume 43, pp. 475–476.
47. Nencioni, G.; Helvik, B.E.; Gonzalez, A.J.; Heegaard, P.E.; Kamisinski, A. Availability Modelling of Software-Defined Backbone Networks. In Proceedings of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN-W 2016, Toulouse, France, 28 June–1 July 2016; pp. 105–112.

48. Silva, W.J.A.; Dias, K.L.; Sadok, D.F.H. A Performance Evaluation of Software Defined Networking Load Balancers Implementations. In Proceedings of the International Conference on Information Networking (ICOIN), Da Nang, Vietnam, 11–13 January 2017.
49. McKeown, N.; Anderson, T.; Balakrishnan, H.; Parulkar, G.; Peterson, L.; Rexford, J.; Shenker, S.; Turner, J. OpenFlow: Enabling Innovation in Campus Networks. *ACM SIGCOMM Comput. Commun. Rev.* **2008**, *38*, 69–74. [CrossRef]
50. Pfaff, B.; Lantz, B.; Heller, B.; Barker, C.; Cohn, D.; Casado, M. *OpenFlow Switch Specification—1.3 Version*; Open Networking Foundation: Menlo Park, CA, USA, 2012; 105p.
51. Heller, B.; Sherwood, R.; McKeown, N. The controller placement problem. *ACM SIGCOMM Comput. Commun. Rev.* **2012**, *42*, 473. [CrossRef]
52. Bannour, F.; Souihi, S.; Mellouk, A. Distributed SDN Control: Survey, Taxonomy and Challenges. *IEEE Commun. Surv. Tutor.* **2017**, *20*, 333–354, doi:10.1109/COMST.2017.2782482. [CrossRef]
53. He, J.; Rexford, J. Toward internet-wide multipath routing. *IEEE Netw.* **2008**, *22*, 16–21.
54. Zhu, D.; Gritter, M.; Cheriton, D.R. Feedback based routing. *ACM SIGCOMM Comput. Commun. Rev.* **2003**, *33*, 71–76. [CrossRef]
55. Lee, S.J.; Banerjee, S.; Sharma, P.; Yalagandula, P.; Basu, S. Bandwidth-aware routing in overlay networks. In Proceedings of the IEEE INFOCOM, the 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 2405–2413.
56. Fujinoki, H. Multi-Path BGP (MBGP): A Solution for Improving Network Bandwidth Utilization and Defense against Link Failures in Inter-Domain Routing. In Proceedings of the 16th IEEE International Conference on Networks, New Delhi, India, 12–14 December 2008; p. 6.
57. Van Beijnum, I.; Crowcroft, J.; Valera, F.; Bagnulo, M. Loop-freeness in multipath BGP through propagating the longest path. In Proceedings of the 2009 IEEE International Conference on Communications Workshops, ICC 2009, Dresden, Germany, 14–18 June 2009.
58. Qin, D.; Yang, J.; Liu, Z.; Wang, H.; Zhang, B.; Zhang, W. AMIR: Another multipath interdomain routing. In Proceedings of the International Conference on Advanced Information Networking and Applications (AINA), Fukuoka, Japan, 26–29 March 2012; pp. 581–588.
59. Yang, X.; Clark, D.; Berger, A.W. NIRA: A new inter-domain routing architecture. *IEEE/ACM Trans. Netw.* **2007**, *15*, 775–788. [CrossRef]
60. Chen, Z.; Bi, J.; Fu, Y.; Wang, Y.; Xu, A. MLV: A Multi-dimension Routing Information Exchange Mechanism for Inter-domain SDN. In Proceedings of the 2015 IEEE 23rd International Conference on Network Protocols (ICNP), San Francisco, CA, USA, 10–13 November 2015; pp. 438–445.
61. Wang, Y.; Bi, J.; Zhang, K.; Wu, Y. A Framework for Fine-Grained Inter-Domain Routing Diversity Via SDN. In Proceedings of the 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN), Vienna, Austria, 5–8 July 2016; pp. 751–756.
62. Wang, Y.; Bi, J.; Lin, P.; Lin, Y.; Zhang, K. SDI: A multi-domain SDN mechanism for fine-grained inter-domain routing. *Ann. Telecommun.* **2016**, *71*, 625–637. [CrossRef]
63. Xu, W.; Rexford, J. MIRO: Multi-path Interdomain Routing. In Proceedings of the 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Pisa, Italy, 11–15 September 2006; pp. 171–182.
64. Kushman, N.; Kandula, S.; Katabi, D.; Maggs, B.M. R-BGP: Staying Connected In a Connected World. In Proceedings of the 4th USENIX Conference on Networked Systems Design & Implementation—NSDI '07, Cambridge, MA, USA, 11–13 April 2007; p. 14.
65. Ganichev, I.; Dai, B.; Godfrey, P.B.; Shenker, S. YAMR: Yet Another Multipath Routing Protocol. *ACM SIGCOMM Comput. Commun. Rev.* **2010**, *40*, 13–19. [CrossRef]
66. Liao, Y.; Gao, L.; Guerin, R.; Zhang, Z.L. Reliable interdomain routing through multiple complementary routing processes. In Proceedings of the 2008 ACM CoNEXT Conference—CONEXT '08, Madrid, Spain, 9–12 December 2008; pp. 1–6.
67. Gupta, A.; Vanbever L.; Shahbaz, M.; Donovan P. S.; Schlinker, B.; Feamster, N.; Rexford, J.; Shenker, S.; Clark, R.; Katz-Bassett, E. SDX: A software defined internet exchange. In Proceedings of the 2014 ACM conference on SIGCOMM, Chicago, IL, USA, 17–22 August 2014; pp. 551–562.

68. Gupta, A.; MacDavid, R.; Birkner, R.; Canini, M.; Feamster, N.; Rexford, J.; Vanbever, L. An Industrial-Scale Software Defined Internet Exchange Point. In Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), Santa Clara, CA, USA, 16–18 March 2016; pp. 1–14.
69. Kotronis, V.; Dimitropoulos, X.; Klöti, R.; Ager, B.; Georgopoulos, P.; Schmid, S. Control Exchange Points: Providing QoS-enabled End-to-End Services via SDN-based Inter-domain Routing Orchestration. *Linx* **2014**, *2429*, 2443.
70. ONOS. A New Carrier-Grade SDN Network Operation System Designed for High Availability, Performance, Scale-Out. 2017. Available online: http://onosproject.org/ (accessed on 16 May 2018).
71. Quagga. Quagga Routing Suite. Available online: http://www.nongnu.org/quagga/ (accessed on 16 May 2018).
72. Ryu. A Component-Based Software Defined Networking Framework-Ryu. 2016. Available online: https://osrg.github.io/ryu/ (accessed on 16 May 2018).
73. Kotronis, V.; Dimitropoulos, X.; Ager, B. Outsourcing the routing control logic: Better internet routing based on SDN principles. In Proceedings of the 11th ACM Workshop on Hot Topics in Networks, Redmond, WA, USA, 29–30 October 2012; pp. 55–60.
74. Cvjetic, A.; Smiljanic, A. Improving BGP protocol to advertise multiple routes for the same destination prefix. *IEEE Commun. Lett.* **2014**, *18*, 106–109. [CrossRef]
75. Li, M.; Lukyanenko, A.; Ou, Z.; Yla-Jaaski, A.; Tarkoma, S.; Coudron, M.; Secci, S. Multipath Transmission for the Internet: A Survey. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2887–2925. [CrossRef]
76. Walton, D.; Retana, A.; Chen, E.; Scudder, J. *Advertisement of Multiple Paths in BGP—RFC 7911*; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2016; pp. 1–8.
77. Gredler, E.H.; Medved, J.; Previdi, S.; Farrel, A.; Ray, S. *North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP*; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2016; pp. 1–48.
78. Snijders, J.; Heitz, J.; Scudder, J. *BGP Administrative Shutdown Communication*; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2017.
79. Nascimento, M.R.; Rothenberg, C.E.; Salvador, M.R.; Corrêa, C.N.A.; de Lucena, S.C.; Magalhães, M.F. Virtual routers as a service: The RouteFlow Approach Leveraging Software-Defined Networks. In Proceedings of the 6th International Conference on Future Internet Technologies—CFI '11, Seoul, Korea, 13–15 June 2011; p. 34.
80. Lin, P.; Bi, J.; Chen, Z.; Wang, Y.; Hu, H.; Xu, A. WE-bridge: West-east bridge for SDN inter-domain network peering. In Proceedings of the IEEE INFOCOM, 2014 IEEE Conference on Computer Communications Workshops, Toronto, ON, Canada, 27 April–2 May 2014; pp. 111–112.
81. Bennesby, R.; Mota, E.; Fonseca, P.; Passito, A. Innovating on interdomain routing with an inter-SDN component. In Proceedings of the International Conference on Advanced Information Networking and Applications (AINA), Victoria, BC, Canada, 13–16 May 2014; pp. 131–138.
82. Alimi, R.; Penno, R.; Yang, Y.; Kiesel, S.; Previdi, S.; Roome, W.; Shalunov, S.; Woundy, R. *Application-Layer Traffic Optimization (ALTO) Protocol Applications*; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2014.
83. King, T.; Dietzel, C.; Snijders, J.; Doering, G.; Hankins, G. *BLACKHOLE Community*; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2016.
84. Heitz, J.; Snijders, J.; Patel, K.; Bagdonas, I.; Hilliard, N. *BGP Large Communities Attribute Abstract*; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2017.
85. Kreutz, D.; Ramos, F.M.; Verissimo, P. Towards secure and dependable software-defined networks. In Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking—HotSDN '13, Hong Kong, China, 16 August 2013; p. 55.
86. Muqaddas, A.S.; Giaccone, P.; Bianco, A.; Maier, G. Inter-controller Traffic to Support Consistency in ONOS Clusters. *IEEE Trans. Netw. Serv. Manag.* **2017**, *14*, 1018–1031. [CrossRef]
87. Raghavan, B.; Casado, M.; Koponen, T.; Ratnasamy, S.; Ghodsi, A.; Shenker, S. Software-defined internet architecture. In Proceedings of the 11th ACM Workshop on Hot Topics in Networks—HotNets-XI, Redmond, WA, USA, 29–30 October 2012; pp. 43–48.
88. Datta, A.; Rastogi, A.; Barman, O.R.; D'Mello, R.; Abuzaghleh, O. An Approach for Implementation of Artificial Intelligence in Automatic Network Management and Analysis. *Online Eng. Int. Things* **2018**, *22*, 901–909.

89. Fadlullah, Z.; Tang, F.; Mao, B.; Kato, N.; Akashi, O.; Inoue, T.; Mizutani, K. State-of-the-Art Deep Learning: Evolving Machine Intelligence Toward Tomorrow's Intelligent Network Traffic Control Systems. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2432–2455. [CrossRef]
90. CAIDA. Center for Applied Internet Data Analysis—CAIDA. Available online: http://data.caida.org/datasets/as-relationships/serial-2/ (accessed on 16 May 2018).
91. Chanda, A.; Westphal, C. Content Based Traffic Engineering in Software Defined Information Centric Networks. In Proceedings of the 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Turin, Italy, 14–19 April 2013; pp. 3397–3402.
92. Wichtlhuber, M.; Reinecke, R.; Hausheer, D. An SDN-based CDN/ISP collaboration architecture for managing high-volume flows. *IEEE Trans. Netw. Serv. Manag.* **2015**, *12*, 48–60. [CrossRef]
93. Rao, A.; Legout, A.; Lim, Y.S.; Towsley, D.; Barakat, C.; Dabbous, W. Network characteristics of video streaming traffic. In Proceedings of the Seventh COnference on Emerging Networking EXperiments and Technologies (CoNEXT), Tokyo, Japan, 6–9 December 2011; pp. 1–12.
94. Poese, I.; Frank, B.; Ager, B.; Smaragdakis, G.; Feldmann, A. Improving content delivery using provider-aided distance information. In Proceedings of the 10th Annual Conference on Internet Measurement—IMC '10, Melbourne, Australia, 1–30 November 2010; p. 22.
95. Poese, I.; Frank, B.; Smaragdakis, G.; Uhlig, S.; Feldmann, A.; Maggs, B. Enabling content-aware traffic engineering. *Comput. Commun. Rev.* **2012**, *42*, 22–28. [CrossRef]
96. Wolf, T.; Griffioen, J.; Calvert, K.; Dutta, R.; Rouskas, G.; Nagurney, A. ChoiceNet: Toward an Economy Plane for the Internet. *ACM SIGCOMM Comput. Commun. Rev.* **2014**, *44*, 58–65. [CrossRef]
97. Chen, C.; Li, B.; Lin, D.; Li, B. Software-Defined Inter-Domain Routing Revisited. In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016.
98. Silva, W.J.A. Performance Evaluation of Flow Creation Inside an OpenFlow Network. In Proceedings of the XXXV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais—SBrT2017, São Pedro, Brazil, 3–6 September 2017; pp. 102–106.
99. Bosshart, P.; Varghese, G.; Walker, D.; Daly, D.; Gibb, G.; Izzard, M.; McKeown, N.; Rexford, J.; Schlesinger, C.; Talayco, D.; et al. P4: Programming Protocol-Independent Packet Processors. *ACM SIGCOMM Comput. Commun. Rev.* **2014**, *44*, 87–95. [CrossRef]
100. Bianchi, G.; Bonola, M.; Capone, A.; Cascone, C. OpenState: Programming Platform-independent Stateful OpenFlow Applications Inside the Switch. *ACM SIGCOMM Comput. Commun. Review* **2014**, *44*, 44–51. [CrossRef]
101. Silva, W.J.A. Avoiding Inconsistency in OpenFlow Stateful Applications Caused by Multiple Flow Requests. In Proceedings of the International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 5–8 March 2018; pp. 543–548.