Brazil's IXP requirements, limitations and security issues: a survey

Humberto Silva Galiza de Freitas[1], **Christian Esteve Rothenberg**[2], **Jeronimo Aguiar Bezerra**[3]

[1]Rede Nacional de Ensino e Pesquisa (RNP)
Diretoria de Engenharia e Operações (DEO)
Núcleo de Engenharia de Redes de AmLight (NEG AmLight)
Campinas – SP – Brasil

[2]Universidade Estadual de Campinas (UNICAMP)
Faculdade de Engenharia Elétrica e de Computação (FEEC)
Information & Networking Technologies Research & Innovation Group (INTRIG)
Campinas – SP – Brasil

[3]Florida International University (FIU)
Center for Internet Augmented Research and Assessment (CIARA)
Miami – FL – USA

humberto.galiza@rnp.br, christian@unicamp.br, jbezerra@fiu.edu

Abstract. *lorem ipsum lorem ipsum.*

1. Introduction

Internet eXchange Points (IXP) are the natural successors of the four Network Access Points (NAP) responsible for interconnecting different networks in the early stages of today's Internet. The benefits achieved regarding performance and security are the main reason for the key role that the IXPs plays in the present Internet ecosystem [Norton 2014].

Although the dynamics of operation, criticality, and security aspects of an IXP are well-known and quite often under discussion by the network operators community, only recently the scientific community began to delve into this subject. In this sense, the work of [Ager et al. 2012] pioneered with the flow analysis from a large European IXP. The authors concluded, among other things, that the traffic volume exchanged between the IXP members was analogous to levels observed in a Tier-1 Internet Service Provider (ISP) network.

In the same context in Brazil, the work of [Brito et al. 2015] innovated by bringing for the first time an analysis of the IXP ecosystem in operation in the country. The authors

compiled valuable information about the characterization of the types of members present in these environments and their connectivity graphs at the Autonomous System (AS) level, being able to determine the peering potential in each IXP.

From an operational perspective, despite the fact that the Federal Interconnection eXchange Point (FIX) is considered the first public IXP in Brazil [FIX 2016], the PTTMetro project launched in 2004 and coordinated by the Brazilian Regional Internet Registry Authority (NIC.BR) was, in fact, the responsible for the spreading of regional commercial IXPs in Brazil. Since then, the project has expanded the number of IXPs and the Points of Presence (PoPs) under its management across the country, and thus contributed to the development and improvement of national quality Internet. More recently, the project was renamed to IX.BR, and is currently operating in 24 cities in Brazil, exchanging near 2 Tbps of aggregated traffic [NIC.BR 2016], being considered the 4th biggest in the world based on the number of members [Putta Venkata and Ruan 2016].

Notwithstanding the clear benefits and advances brought about by large-scale deployment of IXPs in Brazil, the current model poses several problems, in the vast majority derived from its own architecture. These issues might end up affecting at different levels its security, scalability, and resiliency. The occurrence of network events or security incidents can compromise all or part of its operation, creating damages to its image and mission. In these cases, insecurity and instability set up in the routing environment contribute to the increase in distrust among the participants, as well as distancing possible new members.

The main contribution of the present work is to bring a Survey of the technical requirements and weaknesses of public IXPs in Brazil, presenting a non-exhaustive list of top security and limitations issues that affect these requirements. Despite the focus on Brazil, this study may contribute to a better understanding about the limitations and improvements that can be adopted in other IXPs using similar models. For each of the identified problems, possible solutions that follows the IXP model assumptions and operations guidelines and also that keeps IXP's stability, availability and scalability are provided.

Moreover, as some of the presented problems can not be addressed due to limitations in the current Ethernet/IP architecture, this paper also contributes in assessing the feasibility of adoption of some concepts from Software-Defined Networking (SDN) and OpenFlow protocol [ONF 2009] to address these deficiencies. The employment of such concepts can be the first step in the transformation of the current IXP model into a lightweight version of Software-Defined Internet eXchange (SDX) concept [Gupta et al. 2015].

The rest of this paper is structured as follows. Section 2 provides an overview about IXP's concepts, architecture and operations activities. Section 3 dissects the current architectural problems and limitations using a bottom-up approach. Following, Section 4, discusses some ongoing research efforts that address the issues raised, including the application of SDN and OpenFlow concepts. We conclude our work and discuss future directions in Section 5.

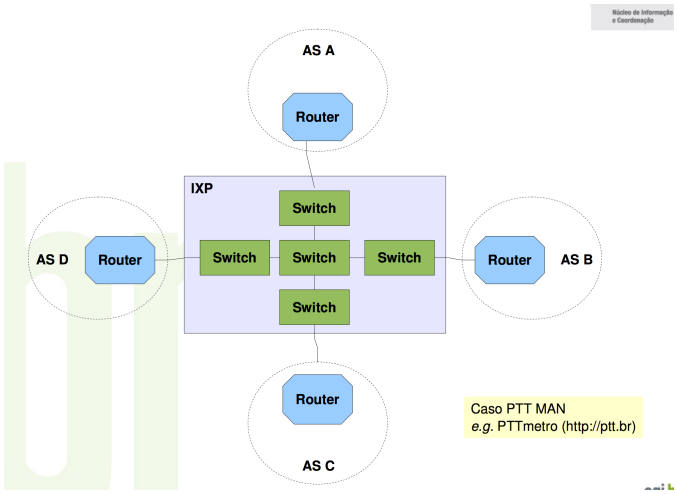

Figure 1. IXP traditional architecture with multiple PoPs. CHANGE PICTURE!!

2. Background

Prior to its worldwide deployment and coverage, the Internet routing was centralized at four NAPs located in the U.S. These NAPs were public exchange facilities where commercial ISPs got interconnected to exchange traffic. As part of the NSFNET transition strategy to the modern Internet, these centralized access points were replaced by distributed IXPs. Currently, they are present in a number of countries, playing a key role in the Internet ecosystem by carrying out a large amount of traffic [Chatzis et al. 2013].

From a design point of view, while the traditional IXPs can be classified into Layer-2 and Layer-3 IXPs, the prevalent model nowadays is the Layer-2 shared medium, like Ethernet, on top of which the IXP services are offered. This choice is due to the simplistic design requirements when providing a Layer-2 topology, as well as the easy and reduced costs for growing the switching fabric when compared to a Layer-3 solution.

As already mentioned, the simplest IXP design includes a Layer-2 pure switch, where the IXP connectors exchange traffic. However, as depicted in Figure 1, to scale this design and assure resiliency in the architecture, more switches may be added to the Layer-2 topology creating a switching fabric. In the same sense, the IXP can expand its own operations to cover a wide area (e.g., a metropolitan region). In this case, besides having multiple switches, the IXP can have multiple PoPs under the same Layer-2 shared medium, where all PoPs are interconnected, creating a full-mesh, or simply a distributed switching fabric.

In general, most IXPs in operation nowadays adopt a technical model where the switching fabric is essentially an enormous flat Ethernet domain, based on different technologies such as IEEE Std 802.1q Medium Access Control (MAC) Bridges, Virtual Bridge Local Area Networks (VLANs) and Virtual Private Lan Service (VPLS) [Kompella and Rekhter 2007, Lasserre and Kompella 2007]. On top of such (distributed) switching fabric, the members are free to set up peering agreements (BGP sessions) with other as they wish to exchange routes.

This method of peering at IXPs were very common in the early stages of IXPs deployment. However, it became a tough operational problem managing a large number

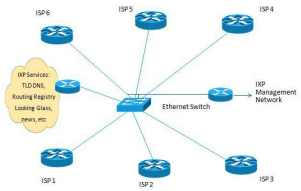

Figure 2. IXP route-server in operation. CHANGE PICTURE!!

of bilateral BGP sessions when the number of IXP members and peering agreements grew. In response to this challenge, the route-servers emerged as a method of interconnecting BGP speaking routers using a third-party system [Jasinska et al. 2016].

In this context, each IXP member set up one or more BGP sessions with the route-server and it, in turn, forwards the route information to each route-server client connected. This method of peering is also known as Multilateral peering, and Figure 2 illustrates the dynamic of its operation. In fact, the route-server operation is very similar to the route-reflector as specified in [Bates et al. 2006], except that it operates over an eBGP session instead of internal BGP (iBGP).

Besides the bilateral and multilateral peering arrangements, additional services may be offered, or even, sold using the peering fabric. A common ”package” often seen in different IXPs around the globe, includes, but do not limit to, DNS TLD service, NTP service, Internet Routing Registry (IRR) service, and Looking Glass. Usually these services are offered and maintened by the IXP operator.

In addition to this set of services, IXP members are allowed to buy/sell IP Transit from/to its partners. This can be achieved very straightforward by setting up a bilateral transit BGP session over the shared VLAN, or by asking the IXP operator to set up a dedicated VLAN between the two members, and then, setting up the transit BGP session. While this practice contrast with the IXP itself definition, in fact, it is a very common practice nowadays due to the easy of deployment, and the possibility of making business with a wide variety of members, in contrast with purchasing or selling IP transit from/to a dedicated partner.

Brazil’s IX.BR project adopted the european IX model [EURO-IX 2012], i.e, the peering fabric is operated by a not-for-profit independent organization, usually NIC.BR and the Brazilian Research and Education Network (RNP), and the fabric may be spread across potentially many competing colocation facilities. Thus, the IX.BR members can choose the facility that best meets their needs. For instance, São Paulo’s city IXP is the biggest one in operation, with around 500 connectors, exchanging near 1.5Tbps of traffic daily. Figure 3 illustrates São Paulo’s city IXP PoPs interconnection in a live traffic map.

Despite of the success of the IXP model, and particularly in Brazil, the country-wide IXP deployment strategy, in the next section we’ll study the problems and limitations posed by the architecture to the current model.

3. Issues and Limitations: Bottom-up Analysis

Introduzir os problemas que afetam o modelo atual...

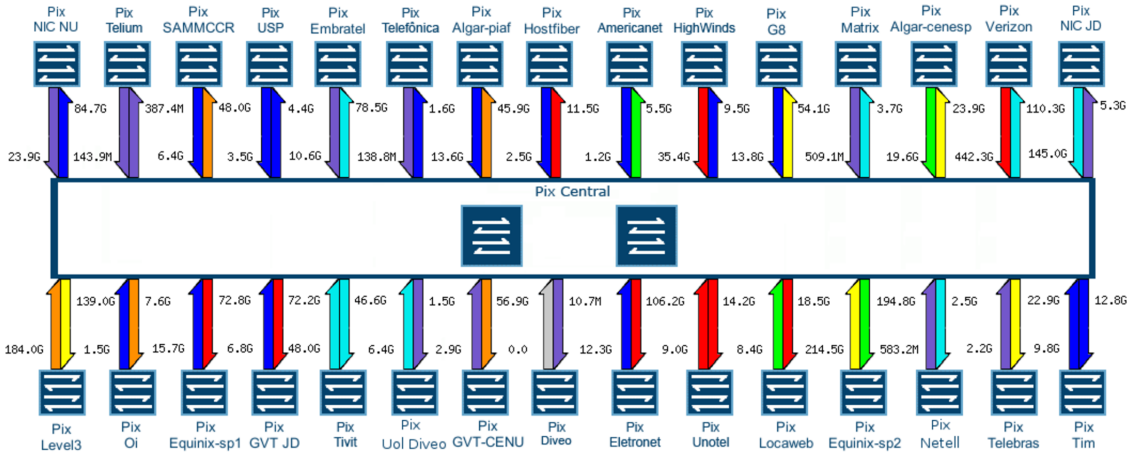

Figure 3. São Paulo's IXP links between colocation facilities (PoPs).

3.1. Infrastructure

3.2. Control Plane

Introduzir os problemas que afetam o plano de controle

3.2.1. *Broadcast Storming* na Matriz de Comutação

As redes de computadores puramente em camada-2 são bem conhecidas por terem problemas de escalabilidade. Ao passo que o tamanho do domínio de *broadcast* aumenta, o nível de tráfego de *broadcast* de protocolos como o *Address Resolution Protocol* (ARP) aumenta. Quantidades significativas de tráfego de *broadcast* constituem uma carga particular para a rede, porque todos os dispositivos desse domínio devem processar e, eventualmente, atuar sobre esse tráfego.

As fontes de *broadcast storming* na matriz de comutação incluem, mas não se limitam a: (1) implementações fracas de protocolos de detecção e prevenção de *loops* na camada 2; (2) erros de configuração por parte dos participantes do IXP. Em casos extremos, essa enxurrada de tráfego *broadcast* podem atingir um nível capaz de reduzir em parte ou no todo a capacidade operacional de uma rede [Narten et al. 2013].

Apesar de o senso comum ao projetar redes de *data center* seja dividir grandes domínios de transmissão em múltiplos segmentos de rede, tal solução não é aplicável a um IXP, pois oferecer um único ambiente compartilhado aos membros é uma das premissas fundamentais do modelo de organização arquitetural de um IXP público. Além disso, o operador do IXP deve ser capaz de distinguir as requisições ARP entre solicitações legítimas e *broadcasts stormings*. Tanto uma política restritiva de bloqueio ARP, quanto um tempo limite muito excessivo no armazenamento da entrada ARP podem resultar no envelhecimento do endereço MAC do membro participante nas tabelas MAC e *Content Addressable Memory* (CAM) do switch, podendo causar *black hole* no tráfego direcionado a esse membro participante.

3.2.2. Quadros Ethernet Desconhecidos e/ou Proibidos na Matriz de Comutação

Usualmente, sob operações normais, o único tráfego de camada-2 permitido na maioria dos IXPs atuais é: (1) ARP (*ethertype*: 0x0806), (2) IPv4 (*ethertype*: 0x0800) e (3) IPv6 (*ethertype*: 0x86dd). Apesar disso, não é incomum ver no meio de comutação compartilhado quadros de protocolos que variam desde *Bridge Protocol Data Unit* (BPDU) e suas variantes, protocolos de descoberta de topologia como IEEE Std 802.1AB - *Link Layer Discovery Protocol* (LLDP), assim como protocolos proprietários de descoberta como o *Cisco Discovery Protocol* (CDP).

A ocorrência de tais *ethertypes* na plataforma de troca de tráfego, bem como quadros gerados nas camadas superiores por protocolos como o *Dynamic Host Control Protocol* (DHCP) [Droms 1997] e IPv6 *Neighbor Discovery/ Router Advertisements* [Narten et al. 2007] está estritamente ligado com a má configuração no dispositivo do membro participante. Quanto maior o número de membros do IXP e de Pontos de Presença (PoPs), mais difícil é rastrear e resolver a ocorrência desse tipo de problemas.

Cada um destes já mencionados *ethertypes* poderia potencialmente impactar a operação normal do IXP levando a uma interrupção total ou parcial do serviço. Embora existam mecanismos simples para abordar facilmente cada uma dessas questões, o processo requer algumas ferramentas de monitoramento de rede, bem como a atenção do operador de rede para registros de eventos (logs) e fluxos de rede. Com base nessas informações reunidas o operador pode desencadear uma ação para resolver o problema.

3.2.3. Concepção e Manutenção de uma Topologia sem *Loops*

Projetar e manter uma topologia livre de *loop* para um IXP não é algo difícil hoje em dia, considerando a vasta variedade de opções de protocolos de resiliência já oferecidas no mercado. No entanto, os problemas desta abordagem podem surgir de uma forma muito simples. Como um membro do IXP pode estender o meio compartilhado do IXP para dentro do seu *backbone*, ele pode causar (intencionalmente ou não) um *loop* de comutação criando mais de um caminho de camada-2 entre o switch de borda do IXP e um switch de rede interno, ou mesmo tendo duas portas ligadas entre si. O *loop* cria um *broadcast storming* e seus efeitos já foram descritos na seção 3.2.1.

Em resposta a esse problema, os operadores de IXPs têm usado principalmente dois recursos: (1) controle de transmissão de tráfego *broadcast*, para limitar o volume de pacotes por segundo (pps) recebido da porta do participante; (2) definir um limite de aprendizagem MAC para 1 na interface atribuída ao membro. Embora ambas as soluções sejam diretas e fáceis de serem implantadas, os operadores de rede precisam configurar manualmente esses parâmetros. Esse processo requer também algumas ferramentas de monitoramento de rede e, além disso, operador de rede precisa estar atento a um possível comportamento estranho da rede.

3.2.4. Ataques Direcionados ao Plano de Controle

Nas implementações iniciais de IXPs, cada membro precisava configurar uma sessão BGP entre si, levando a um esquema de conectividade de roteamento de malha completa, do inglês *full-mesh*. Os Servidores de Rotas, do inglês *Route Servers*, surgiram como uma resposta a este problema de escalabilidade, diminuindo o overhead de configurações BGP, e tornando a tarefa de gerenciamento do próprio IXP mais fácil [Lu and Zhao 2005].

Citar aqui RFC 7948 e 7947 - descrever mais problemas relacionados à operação dos route-servers

Como os *Route Servers* desempenham um papel crucial em qualquer IXP atual, os ataques dirigidos a eles podem causar sérios problemas operacionais à infraestrutura da matriz de troca de tráfego. Os ataques bem conhecidos dirigidos a Servidores de Rotas incluem, mas não estão limitados a, (1) todos os métodos de ataques aplicáveis a meios compartilhados de camada-2 e camada-3 como por exemplo, *mac flooding*, *arp spoofing*, *IP spoofing*, e assim por diante, além de ataques (D)DoS direcionados ao IP do Servidor de rota e ataques do tipo *man-in-the-middle*.

Algumas contramedidas já existem em implementações atuais, abordando especificamente cada um desses pontos. No entanto, proteger e manter a operação do Servidor de Rotas é mais uma tarefa que requer tanto a atenção do operador de rede bem como cuidados extras na configuração dos dispositivos de rede onde o Servidor de Rota se conecta.

3.2.5. Suporte à Engenharia de Tráfego

Devido à natureza do modelo IXP atualmente em uso, o suporte a Engenharia de Tráfego, do inglês *Traffic Engineering* (TE), nas direções de entrada e saída é realizado através da manipulação de atributos BGP. No entanto, essas técnicas são restritas a um lugar comum: o prefixo de destino. Isso compromete a aplicação de uma política mais granular, por exemplo, roteamento baseado na origem do pacote, bem como não fornece uma solução elegante para a resiliência. Por exemplo, se um AS quiser ter mais de uma porta conectada a Pontos de Presença distintos de um mesmo IXP, o BGP não fornece recursos de TE para ter um bom balanceamento de carga de tráfego.

O balanceamento de tráfego de saída é alcançado de maneira direta: com base no prefixo de destino, o participante do IXP pode instalar várias rotas usando caminhos diferentes. No entanto, há que se ressaltar que a grande maioria do tráfego de um Provedor de Internet, por exemplo, é de entrada, uma vez que eles têm os consumidores para o conteúdo. Com base nisso, a engenharia de tráfego de entrada para SA com mais de um provedor *upstream* ou *Multihomed* é alcançado basicamente usando as técnicas de *AS Path Prepending* ou desagregação de prefixos. Ambos os mecanismos são fáceis de implementar, mas geram muitos problemas colaterais, como a poluição da tabela BGP, além de efeitos indesejáveis quando mal configurados, a exemplo de *black hole* no tráfego.

Em termos de escalabilidade, o modelo atual de IXP limita o crescimento dos membros participantes porque a matriz de comutação não tem um mecanismo para suportar a expansão de várias portas com diferentes velocidades. Por exemplo, se um partici-

pante do IXP quiser ter uma porta de 10Gbps em PoP do IXP e outra porta de 100G em outro PoP, o modelo não dá suporte a um mecanismo adequado usando apenas BGP ou mesmo MPLS-TE para conseguir um TE de entrada em direção ao seu *backbone*.

Mesmo no caso em que o participante quer apenas ativar outra porta de capacidade igual (por exemplo, o participante tem uma porta de 10 Gbps e quer outra porta de 10 Gbps), o IXP geralmente oferece uma solução usando IEEE 802.3ad *Link Aggregation Control Protocol* (LACP) como um mecanismo para melhorar sua vazão para a matriz de comutação. No entanto, no caso de o participante não estar conectado localmente (por exemplo, no caso de *peering* remoto) e está usando um circuito virtual alugado ou um circuito MPLS para alcançar o IXP, o LACP não funcionará, devido a particularidades do protocolo envolvendo temporizadores, portas com velocidades diferentes e etc. Portanto, não é uma opção viável.

3.2.6. Suporte à Programabilidade de Rede

O modelo atual de IXP tem um suporte muito limitado ou mesmo não tem suporta à programação de rede. Este recurso poderia trazer benefícios interessantes para os participantes, uma vez que poderia permitir-lhes ter mais capacidades de engenharia de tráfego, com mais opções do que apenas o prefixo de destino como é hoje.

3.3. Data Plane

3.3.1. Roteamento *Hot-Potato*

Devido à arquitetura de meio compartilhado do IXP é trivial para um participante apontar uma rota estática para outro participante usando-o para alcançar uma rede de terceiros. Essa é uma situação de roteamento *Hot-potato* sem autorização. Apesar deste tipo de conduta ser proibida pelos operadores do IXP, é difícil monitorar a ocorrência de tal situação, e cada participante tem que adotar suas próprias medidas para evitar ser utilizado maliciosamente por outro SA na matriz de comutação.

ESCREVER MAIS UM PARAGRAFO

3.3.2. Vazamento de Rotas

Até onde se conhece, o modelo atual de encaminhamento de tráfego em um IXP não tem um mecanismo eficiente para evitar vazamento não-intencional de roteamento. Há relatos de operadores de rede em todo o mundo que mostram esses vazamentos de roteamento dentro de um matriz de comutação causou um monte de problemas, não só para o ambiente IXP, mas para toda a Internet. O que foi feito até hoje é apenas definir um limite máximo de prefixo por participante e no caso de o participante atingir um número definido de prefixos anunciados a sessão BGP será colocado em um estado de *shutdown* administrativo.

Embora esta ação possa evitar a propagação de vazamento de rota, ela não está focada no problema principal: um participante deve anunciar apenas o que é permitido. Esse mecanismo de validação não existe no modelo atual, apesar de existirem relatos de alguns IXP's terem rodado o RPKI para validar a origem do prefixo anunciado.

3.3.3. Sequestro de Prefixos

Além do problema de vazamento de rotas mencionado na subseção 3.3.2, outro problema grave em termos de roteamento e que causa uma grande preocupação aos IXPs atuais e o sequestro de prefixos. Essa e uma situaçao muito mais difícil de ser identificada, uma vez que não existem controles sobre o que cada participante deve anunciar nas sessões BGP com os Servidores de Rotas.

Em resposta a este desafio, todos os participantes, bem como o operador dos Servidores de Rotas, deveriam verificar todos os prefixos sendo anunciados e aceitar apenas aqueles que passarem no processo de validação. No entanto, tal mecanismo não existe hoje como um padrão, e os problemas potenciais podem acontecer de uma maneira muito fácil.

3.3.4. Sequestro de BGP *NEXT_HOP*

Outra preocupação em termos de sequestro é quando um participante anuncia um prefixo e altera maliciosamente o atributo BGP NEXT_HOP. Como não há nenhuma verificação nas informações NEXT_HOP no Servidor de Rota nem na implementação do BGP em cada participante, esse ataque é muito fácil de ser implantado em um matriz de troca de tráfego. Até onde esses autores conhecem, não há atualmente uma solução singular para este problema.

3.3.5. Ataques Originados por Membros

Como já foi evidenciado em outros problemas nesta Seção, o modelo atual de IXP não valida o que está sendo anunciado para os Servidores de Rota. Outra situação que surge a partir dessa caracteristica é que ataques (distribuídos) de negação de serviço, do inglês *(Distributed) Denial of Services* ((D)DoS) podem facilmente ser gerado por participantes do IXP.

A solução mais simples e direta para isso é aplicar filtros *anti-spoofing* e validar usando um mecanismo externo como RPKI para validar o que está sendo anunciado. Embora a aplicação de filtros seja uma tarefa fácil, manualmente manter os filtros é uma tarefa difícil de ser alcançada. Monitorar os fluxos atuais através do matriz também é um bom ponto de partida para identificar esses ataques, porém é uma tarefa muito demorada para os operadores de rede.

3.3.6. Ataques Direcionados a Membros

As mesmas limitações ocorrem quando o (D)DoS é originado fora do matriz, e o alvo é um membro específico do IXP. Esse tipo de ataque pode desestabilizar todo a matriz de comutação, bem como espalhar pela Internet devido ao grau de conectividade que os IXPs representam hoje.

3.4. Management Plane

REVISAR ESSA SEÇÃO Existem vários problemas operacionais que afetam os IXPs hoje. No Brasil, apesar do sucesso do modelo implantado, os operadores de rede têm reivindicado o SLA oferecido pelo operador do IXP (NIC.BR). A maior parte do tempo é gasto com tarefas manuais, como o processo de validação de novos participantes, o preenchimento de formulários e o próprio processo de interação sobre os tickets de suporte.

Neste sentido, existem ferramentas hoje para automatizar essas tarefas, mas a limitação é que a maioria delas não tem os mecanismos adequados para interagir com todos os dispositivos de matriz de comutação usando um modelo uniforme de linguagem ou abstração.

3.5. Cross-Layer issues

DESCREVER PROBLEMAS CROSS-LAYER

4. Ongoing Research Efforts and Challenges

4.1. Anatomia e Evolução dos IXPs

4.2. Resiliência e Escalabilidade

4.3. Performance e Avaliação

4.4. Segurança e Dependabilidade

4.5. Migração e Modelos Híbridos

4.6. SDX: Pontos de Troca de Tráfego Definidos por Software

5. Conclusion

References

Ager, B., Chatzis, N., Feldmann, A., Sarrar, N., Uhlig, S., and Willinger, W. (2012). Anatomy of a large european ixp. In *Proceedings of the ACM SIGCOMM 2012 conference on Applications, technologies, architectures, and protocols for computer communication*, pages 163–174. ACM.

Bates, T., Chen, E., and Chandra, R. (2006). BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP). RFC 4456 (Draft Standard). Updated by RFC 7606.

Brito, S. H. B., Santos, M. A. S., dos Reis Fontes, R., Perez, D. A. L., and Rothenberg, C. E. (2015). Anatomia do ecossistema de pontos de troca de tráfego publicos na internet do brasil. *XXXIII Simpósio Brasileiro de Redes de Computadores (SBRC)*.

Chatzis, N., Smaragdakis, G., and Feldmann, A. (2013). On the importance of internet exchange points for today's internet ecosystem. *arXiv preprint arXiv:1307.5264*.

Droms, R. (1997). Dynamic Host Configuration Protocol. RFC 2131 (Draft Standard). Updated by RFCs 3396, 4361, 5494, 6842.

EURO-IX (2012). European internet exchange association 2012 report on european ixps. Report, European Internet Exchange Association (EURO-IX).

FIX (2016). Ponto federal de interconexão. *online website: http://www.fix.org.br*.

Gupta, A., Vanbever, L., Shahbaz, M., Donovan, S. P., Schlinker, B., Feamster, N., Rexford, J., Shenker, S., Clark, R., and Katz-Bassett, E. (2015). Sdx: A software defined internet exchange. *ACM SIGCOMM Computer Communication Review*, 44(4):551–562.

Jasinska, E., Hilliard, N., Raszuk, R., and Bakker, N. (2016). Internet Exchange BGP Route Server. RFC 7947 (Proposed Standard).

Kompella, K. and Rekhter, Y. (2007). Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling. RFC 4761 (Proposed Standard). Updated by RFC 5462.

Lasserre, M. and Kompella, V. (2007). Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling. RFC 4762 (Proposed Standard).

Lu, X. and Zhao, W. (2005). *Networking and Mobile Computing: 3rd International Conference, ICCNMC 2005, Zhangjiajie, China, August 2-4, 2005, Proceedings*, volume 3619. Springer.

Narten, T., Karir, M., and Foo, I. (2013). Address Resolution Problems in Large Data Center Networks. RFC 6820 (Informational).

Narten, T., Nordmark, E., Simpson, W., and Soliman, H. (2007). Neighbor Discovery for IP version 6 (IPv6). RFC 4861 (Draft Standard). Updated by RFCs 5942, 6980, 7048, 7527, 7559.

NIC.BR (2016). Projeto ix.br - http://www.ix.br. Disponível online.

Norton, W. B. (2014). *The 2014 Internet Peering Playbook: Connecting to the Core of the Internet*. DrPeering Press.

ONF, O. N. F. (2009). Openflow switch specification 1.0.0 (wire protocol 0x01). *Online website: https://www.openflow.org/documents/openflow-spec-v1.0.0.pdf*.

Putta Venkata, R. and Ruan, L. (2016). A region-centric analysis of the internet peering ecosystem.