Considering Jurisdiction When Assessing End-to-End Network Neutrality

Márcio Barbosa de Carvalho
Federal University of Rio Grande do Sul, Brazil

Vinícius Garcez Schaurich
Federal University of Rio Grande do Sul, Brazil

Lisandro Zambenedetti Granville
Federal University of Rio Grande do Sul, Brazil

Network Neutrality is an Internet principle that needs to be enforced by normative, which is valid just within a jurisdiction that is usually limited by the borders of a country or region. However, existing solutions designed to assess end-to-end neutrality violations do not consider the normative jurisdictions. We argue that jurisdiction-aware violation detection can be achieved through further steps that can be added to current solutions. As a proof-of-concept, we propose a prototype (JurisNN) to expose and discuss the challenges and open issues that need to be faced to consider the normative jurisdiction when assessing end-to-end Network Neutrality.

Network Neutrality (NN) is not a principle taken for granted across the Internet. It is quite the opposite actually: wherever NN is expected to be respected, it needs to be enforced by a normative that both defines NN parameters and specifies which situations would be considered as NN violations. That normative is stated by legislators and regulatory agencies whose acts are limited to their jurisdiction (a geographic area where their acts are valid), which is usually limited by the borders of a country. That means, in the end, that different countries can define NN and its implications in different ways. As a result, the definition of NN varies from country to country!

NN violations can happen anywhere in the path between two communication points in the Internet. That can occur, for example, at the Internet Service Providers (ISPs) that connect end-user devices to the network, or even at the core of the Internet backbone itself. We argue that for a real neutral Internet, the detection of NN violations must explicitly consider where, in an end-to-end path, those violations occur. However, since NN varies from country to country, some behaviors in one part of the Internet may be considered NN violations, while in other parts the same behaviors may not represent NN violations at all. We thus extend our claim stating that for

NN violation detection to be effective, it shall consider the diverse definitions of NN found in the end-to-end path.

Several solutions have been proposed and deployed to detect NN violations. Usually, they measure the network traffic searching for abnormal behavior that could represent NN violations. However, such solutions ignore the diverse NN definitions found on the end-to-end path, thus actually failing to determine whether a NN violation is underway. Thus, we can say that abnormal network behavior observed by these solutions is, in fact, a Traffic Differentiation (TD) that must be evaluated against NN normative to be classified as a NN violation.

In this article, we argue that jurisdiction-aware violation detection can be achieved through further steps after the execution of current NN violation detection solutions. As a proof-of-concept (POC), we developed a prototype (JurisNN) that implements the additional steps to decide whether a TD is really a NN violation considering the normative jurisdiction. JurisNN assumes existing NN violation detection solution with the capability to point where, along the path, a TD is happening. Relying on existent systems deployed for both end-user and Internet core vantage points, JurisNN can be adopted by any Internet stakeholder (*e.g.*, end-users, regulatory agencies, academia) to perform jurisdiction-aware NN assessment for both local traffic or cross-border traffic.

Although JurisNN is a functional prototype for jurisdiction-aware NN violation assessment solution, which proves a case, the most important contribution of this article is to bring attention to the jurisdiction issue that, to the best of our knowledge, was not raised so far. In this sense, JurisNN was used to discuss the challenges and open issues that need to be faced to consider jurisdiction when assessing end-to-end NN. JurisNN was also used to discuss how to evaluate the NN of Internet links that cross countries that adopted different (or even no) violation definitions.

EXAMPLES OF DIVERGENT NN NORMATIVE

In order to observe real-world examples of networks subject to divergent normative between two (or more) countries, we consider the case of submarine cables. These cables expose the NN normative divergence that can be faced traversing a single network hop, just like a country border. They do not impair our analysis because our concerns are not related specifically to them, but to the situation that they expose. Obviously, our discussion applies also to other links such terrestrial fiber optics or wireless links.

We use the website Submarine Cable Map[1] to discover the submarine cables in operation that connect Brazil to other countries that is summarized in Table 1. Then, we studied the NN normative stated in these countries to choose representative examples of divergent NN normative. The chosen countries are marked with a star (*) in Table 1, whose NN normative is briefly presented in this section.

Table 1. List of submarine cables connecting Brazil to other countries

Submarine Cable	Connected Countries
America Movil Submarine Cable System-1 (AMX-1)	Brazil*, Colombia, Dominican Republic, Guatemala, Mexico, United States of America (USA)*
Americas-II	Brazil*, Curacao, French Guiana, Martinique, Puerto Rico (USA), Venezuela, USA*, Trinidad and Tobago
Atlantis-2	Argentina, Brazil*, Canary Islands (Spain)*, Cape Verde, Portugal*, Senegal
BRUSA	Brazil*, USA*
GlobeNet	Bermuda, Brazil*, Colombia, USA*, Venezuela

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/MIC.2018.2877836, IEEE Internet Computing

Monet	Brazil*, USA*
Seabras-1	Brazil*, USA*
South American Crossing (SAC)/Latin American Nautilus (LAN)	Argentina, Brazil*, Chile, Panama, Peru, Venezuela, Virgin Islands (USA)*
South America-1 (SAm-1)	Argentina, Brazil*, Chile, Colombia, Dominican Republic, Ecuador, Guatemala, Peru, USA*
Tannat	Brazil*, Uruguay*

Brazil has NN guaranteed as an Internet principle since 2014. The Brazilian NN normative states that ISPs must treat all packets equally. Few exceptions are allowed for traffic discrimination and degradation, which include emergency services and indispensable technical requirements. These discriminations and degradations cannot harm users and must be proportional, isonomic, and transparent. ISPs are also prohibited to monitor, block, filter, or analyze the contents of packets.

The European Union (EU) has a NN normative since 2016 when the Body of European Regulators for Electronic Communications (BEREC) stated its NN normative that applies to all EU state members, including Portugal and Spain, which are marked in Table 1. The European NN normative states that ISPs must treat all packets equally. This principle also allows day-to-day traffic management if they can be technically justified. Few exceptions are allowed for traffic blocking, discrimination, and degradation, which include legal obligations, integrity of the network, congestion management, and exceptional temporary situations. ISPs are prohibited from applying traffic prioritization.

The USA does not have explicit NN normative since early 2018, when the Federal Communications Commission (FCC), the US Internet regulatory agency, rolled back the Title II regulation of the Internet. This former normative had prohibited ISPs from blocking or throttling legal services and applications and had prohibited paid prioritization. The current lack of explicit NN normative drives the allegations of NN violations to the Federal Trade Commission (FTC), such as all claims against anti-trust allegations. Implicitly, the traffic management adopted by ISPs should not hurt anti-trust commercial rules. However, non-neutral traffic management actions (*e.g.*, blocking, throttling, paid prioritization) can be allowed if their motivations can be justified along an anti-trust claim.

Uruguay does not have an explicit NN normative. There is a law project proposed in 2011 that states the NN normative,[2] but it is still in the Uruguayan parliament along the legal process to decide whether it will become a law. However, it is implicit (as in the USA) that excesses committed by ISPs may be claimed in the Uruguayan justice system.

It becomes evident that there are divergent NN normative stated in different countries, and this divergence can vary in a wide spectrum ranging from explicit and rigid rules to no rule at all. Among the explicit ones, for instance, there are different ranges of which traffic management motivations are allowed for degradation and discrimination. Bringing the submarine cables examples, we show that communications can be under this divergence passing through a single link, just like crossing a checkpoint in a country border.

From the technical point-of-view, the normative divergence prevents the adoption of a homogeneous NN detection solution for the whole Internet. Indeed, different regions would require specific solutions designed to detect at least the set of traffic management techniques that are prohibited in that region or the whole set of possible traffic management techniques prohibited along the Internet. However, each traffic management technique requires its own set of measurements for its detection. For instance, a traffic blocking can be detected trying to connect different applications from a unique vantage point identifying those applications that are blocked, or even the same application from different vantage points identifying where an application is being blocked. In turn, user discrimination requires metrics (*e.g.*, throughput, response time, packet loss) from multiple vantage points for performance comparison among different users. These different measurements may influence the architecture of a NN violation detection solution, for instance, the choice for a local or a distributed solution.

Despite our focus here in normative divergences, the jurisdiction issue is also about applying the correct normative over the detected TD. In fact, nowadays most of the traffic is confined in the same country due to adoption of content caches. However, even this traffic should be evaluated under the normative stated in that country. Cross-border traffic still leverages the jurisdiction problem because it imposes normative transitions, even being reduced due to adoption of caches.

EXISTING NN VIOLATION DETECTION SOLUTIONS

There is a variety of techniques related to NN violation detection. We bring representative examples of solutions as a general view of the state-of-the-art, in the context of this article, of this variety of techniques for collecting and processing measurement results. A comprehensive list of network neutrality solutions can be found in the survey by Garrett *et. al.*[3]

The solutions can vary in terms of the technique adopted to collect measurements about communications to check for NN violations. The most used technique is the collection of measurements related to artificial communications introduced in the network for this purpose, which are called active measurements. A less used technique is the measurement through observation of actual communications that are being performed by network users, which are called passive measurements. There are also solutions that combine both techniques, which are called hybrid measurements.

Neubot[4] is a client application running in background in the end-user computer. It performs active measurements against Test Servers (client-server mode) or other Neubot clients (overlay mode). The collected information is sent to the Master Server. Although the information collected is publicized in the project website, there is no information about the processing made over the collected information or what is considered a NN violation for Neubot.

NANO[5] is an application designed to run in the end-user computer. NANO performs passive measurements that are sent to a centralized server for further processing. NANO collects a set of variables about the end-user computer (*e.g.*, operating system, CPU usage), about the current network communications (*e.g.*, port number, protocol), and provided by the user (*e.g.*, ISP, geographic location) to perform a confounding factor analysis to find which factors influence the performance observed. If the factor "ISP" is responsible for a performance discrepancy, it means that the ISP performs TD, which characterizes a NN violation for NANO.

Gnutella Rogue Super Peer (RSP)[6] adopts a technique that induces clients in a Gnutella Peer-to-Peer (P2P) system to test their ISP for port blocking, which is a specific kind of TD. Authors introduced an RSP into Gnutella network that receives client's requests and responds with a "busy" message indicating an IP address and port where the client can find another Super Peer. However, the "busy" message indicates the IP address of a Measurement server used to check if the client's ISP is blocking such port. Gnutella RSP adopts a hybrid measurement technique because clients are induced to introduce an artificial packet into their networks (active measurement) and the Measurement Server observes if that packet is received (passive measurement).

Network tomography is a technique related to the inference of link characteristics and network components without measuring them directly. As an example of such approach, Zhiyong Zhang and colleagues[7] propose an algorithm based on a linear system of equations formed by link relations and end-to-end measurements. If the linear system does not have a solution, it indicates that the network is not neutral. This approach is also able to identify, under certain conditions, links or sequence of links that are non-neutral.

DiffProbe[8] proposes a network tomography approach based on active measurements to identify whether the ISP is applying TD. Furthermore, it identifies the scheduling algorithm employed in the router that differentiates the traffic. It uses an actual communication (suspected of being discriminated) and an artificial one that is slightly different from the actual one just to have a different classification, thus, overcoming the differentiation. The authors apply statistical algorithms between the two measurements to identify the scheduling algorithm employed in the router.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/MIC.2018.2877836, IEEE Internet Computing

Adkintun[9] is a platform developed to monitor the fulfilling of the Chilean NN normative by ISPs. It is among the few solutions that rely on the normative definitions to assess NN violations. It relies on probes deployed in user's homes (such as, an instrumented wireless router or a client application) that perform active measurements and send the results to Adkintun servers. The server processes the collected measurements and presents the results to users through a web portal.

ISPANN[10] is an architecture designed to help ISP network administrators to audit if their networks violate the NN normative stated in the country where the ISP operates. The solution collects directly from devices the network configuration to be analyzed by a set of algorithms that are chosen according to the country NN normative. Therefore, for ISPANN, the definition of what is a NN violation comes directly from the NN normative. Thus, it is also among the few solutions that rely on the normative definitions to assess NN violations.

Although both Adkintun and ISPANN consider the definitions stated in the NN normative, they are not a general approach to tackle the jurisdiction when detecting network neutrality violations. ISPANN is designed to help administrators to assess their network configurations according to the normative. The jurisdiction issue is solved, in this context, by the administrator choosing the correct normative to assess the network configuration according to the country where the ISP operates. In turn, for Adkintun, the jurisdiction is tackled by omission assuming that measurement traffic is confined within Chilean borders. However, the jurisdiction issue should not be tackled by omission since it is an important aspect that should be considered to point NN violations.

JURISDICTION-AWARE NN VIOLATION DETECTION

We argue that jurisdiction-aware NN violation detection can be achieved through further steps after the execution of current NN violation detection solutions. These solutions already perform TD Detection and TD Positioning steps depicted in Figure 1. Therefore, we developed a prototype (JurisNN) for Jurisdiction Assessment step assuming information from previous steps provided by current NN violation detection solutions, referred afterward as TD Detection and Positioning solutions.

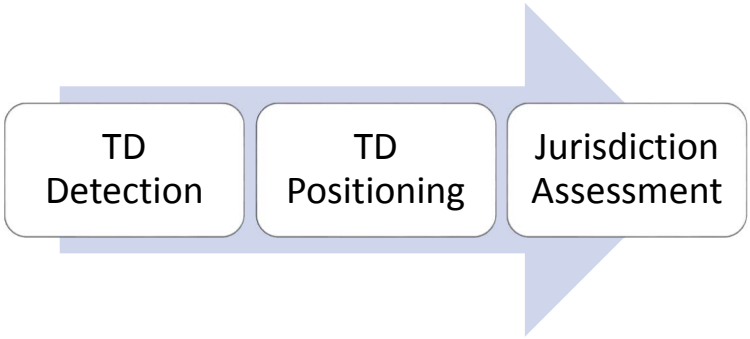

Figure 1. NN violation detection flow introducing jurisdiction awareness. We argue that jurisdiction-aware NN violation detection can be achieved through further processing over information provided by existing TD Detection and Positioning solutions

The JurisNN architecture, which was implemented in Python 3, is depicted in Figure 2. It receives information through arguments provided by TD Detection and Positioning solutions (Figure 2, step 1). The information provided is the TD type (*e.g.*, blocking, throttling), the link sequence that introduces TD (*e.g.*, IP addresses of its endpoints), transport protocol information (*e.g.*, TCP/UDP ports), and its application (if available). Then, JurisNN can judge whether the detected TD is really a NN violation.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/MIC.2018.2877836, IEEE Internet Computing

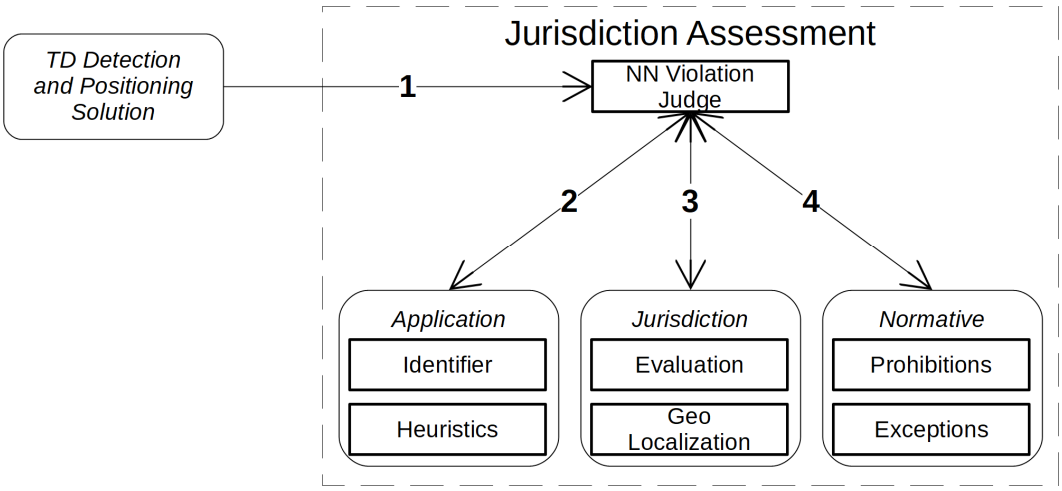

Figure 2. JurisNN architecture for Jurisdiction Assessment. Architecture designed to perform Jurisdiction Assessment over detected TD information provided by TD Detection and Positioning solution

The impaired application can be inferred from transport protocol ports by the *Identifier* class of *Application* module (Figure 2, step 2) using the IANA transport registry information. However, applications can change their transport protocol ports. Indeed, it is a common practice to overcome firewalls and simpler TD techniques introduced by ISPs. Ideally, TD Detection and Positioning solutions should inform the application because they know it in active measurements or may have access to the actual traffic in passive measurements, which enables the employment of more accurate application identification techniques, such as Deep Packet Inspection (DPI). The *Heuristics* class of the *Application* module informs the direction that an application is commonly impaired: downstream, upstream or both directions. The *Evaluation* class of *Jurisdiction* module uses this information to decide about the correct jurisdiction if a non-neutral Internet link crosses borders.

Both the heuristic about the impaired application and the IP addresses of the non-neutral sequence link endpoints are informed to the *Evaluation* class of the *Jurisdiction* module (Figure 2, step 3). The *Geo Localization* class retrieves the country where each IP belongs to, using the GeoLite2 country database.[11] Although this method can be inaccurate, it is enough for our POC. Indeed, the architecture can support further mechanisms for Geo Localization. If the IP addresses belong to the same country, which is the most common situation nowadays due to deployment of content caches, the jurisdiction already is determined without further actions. Otherwise, it means that the non-neutral link sequence cross country's borders, thus, requiring both the use of application heuristics by the Evaluation class to decide the jurisdiction and the higher accuracy of TD positioning to point the non-neutral Internet link.

Usually, Internet links or a sequence of them are classified as non-neutral. However, a network link is often a passive agent. Indeed, devices in link's endpoints introduce the non-neutral behavior of the link. The Evaluation class needs to decide which device is more probable to be introducing TD in the Internet link classified as non-neutral among the endpoint devices (one closer to the user and another closer to the application server). The application heuristic helps this decision by using usual asymmetries of the application traffic. For instance, web applications often send more data than receive. Therefore, they are commonly impaired in the downstream direction. Thus, the link endpoint device closer to the application server is the most probable to be impairing a web application traffic because it is the last device in the downstream direction just before the observed TD. This assumption drives the decision of the Evaluation class about the jurisdiction when an Internet link crosses country's borders. However, there are applications that send and receive a similar amount of traffic (*e.g.*, BitTorrent), hindering this heuristic establishment and requiring more accurate TD Positioning.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/MIC.2018.2877836, IEEE Internet Computing

With information about the jurisdiction of where TD is happening, the *Normative* module can be consulted about the stated NN normative through its *Prohibitions* and *Exceptions* classes (Figure 2, step 4). JurisNN uses a dictionary to model prohibitions and exceptions. As the normative is usually related to application classes (*e.g.,* emergency services, all applications), the dictionary is indexed by country and TD type and returns application classes. For instance, to model the Brazilian normative instruction "few exceptions are allowed for traffic discrimination …, which include emergency services", the dictionary needs two entries: "(BR, discrimination) = (prohibited, all applications)" and "(BR, discrimination) = (exception, emergency services)". Since the interpretation of application classes may differ in different normative, JurisNN has also a dictionary indexed by the country and application class which returns the applications interpreted as of that class in that country.

Finally, the *NN Violation Judge* decides whether the TD type is allowed in that jurisdiction. If it is not, it evaluates whether the application is an exception. If it is not, a NN violation was detected! Otherwise, the TD detected is allowed in the jurisdiction or the application is an exception. Therefore, the detected TD cannot be raised as a NN violation!

CHALLENGES TO BE FACED TO HAVE AN ACCURATE JURISDICTION-AWARE NN VIOLATION DETECTION

Although our prototype represents a possible solution towards jurisdiction-aware NN violation detection, it can be improved if some challenges are faced.

We introduced application heuristics in the architecture to overcome the inaccuracy of TD Positioning. In fact, we recognize that is hard to identify the sequence of links that introduce TD. Indeed, JurisNN needs a variable level of accuracy in TD Positioning. For instance, in traffic served from local caches, all devices on the path are in the same country easing the jurisdiction assessment, thus, reducing the accuracy required. However, special care should be given to ensure that this traffic is not being routed abroad along the path. Indeed, JurisNN just needs a more accurate TD Positioning when TD is introduced in links that cross country borders. Just in this last case, JurisNN needs to use application heuristics. Heuristics could be improved by TD Detection solution that knows the direction of the detected abnormal network behavior, thus, inferring the heuristic directly from the observed network traffic.

The NN normative has details that are hard to introduce into a Normative module. For instance, definitions like "emergency services" may have different meanings. From the legislator view, an emergency service can be a web application used by authorities to deal with public emergencies. From a network administrator view, it can be a signaling protocol to deal with network congestions. We point out that normative definitions are imprecise. Usually, they are stated by willing people with different skills, which can drive to misinterpretation. To be modeled, the normative should be clearer.

While reflecting about the JurisNN architecture design, we faced a normative gap that should be cleared. Imagine a device hosted in one country serving connections just to another country (like in the submarine cables example). This device is degrading the performance of one link that just serves connections from/to the other country. In this situation, which normative should be applied over the device: the normative of the country where it is hosted or the normative of the country of the communications that are being degraded? This may require an international law interpretation to evaluate properly this TD under the lights of the NN normative jurisdiction issue.

CONCLUSION

Although end-to-end jurisdiction-aware NN assessment can be achieved by adopting the JurisNN prototype, some challenges must be faced to improve its accuracy, especially investigation efforts towards the improvement of TD Positioning accuracy. Despite current inaccuracies, the Jurisdiction Assessment is a required step to identify properly NN violations according to the

normative that defines them. Otherwise, without considering the NN normative, one cannot point Network Neutrality violations at all.

ACKNOWLEDGEMENTS

We want to thank the Coordination of Higher Education and Graduate Training (CAPES) for the financial support that made this research possible.

REFERENCES

1. TeleGeography, “Submarine Cable Map,” https://www.submarinecablemap.com, 2018, [Online; accessed 20-June-2018].
2. Parlamiento del Uruguay, “Proyecto de Ley 123457,” https://parlamento.gub.uy/documentosyleyes/ficha-asunto/123457, 2018, [Online; accessed 20-June-2018].
3. T. Garrett, L. E. Setenareski, L. M. Peres, L. C. E. Bona and E. P. Duarte, "Monitoring Network Neutrality: A Survey on Traffic Differentiation Detection," in IEEE Communications Surveys & Tutorials, vol. PP, no. 99, 2018.
4. S. Basso, A. Servetti, and J. C. De Martin, “The network neutrality bot architecture: A preliminary approach for self-monitoring of internet access QoS,” in Proceedings - IEEE Symposium on Computers and Communications, 2011.
5. M. B. Tariq, M. Motiwala, N. Feamster, and M. Ammar, “Detecting network neutrality violations with causal inference,” in Proceedings - International Conference on Emerging Networking Experiments and Technologies. ACM, 2009, pp. 289–300.
6. R. Beverly, S. Bauer, and A. Berger, The Internet Is Not a Big Truck: Toward Quantifying Network Neutrality. Passive and Active Network Measurement, 2007, pp. 135–144.
7. Z. Zhang, O. Mara, and K. Argyraki, “Network neutrality inference,” Computer Communications Review, vol. 44, no. 4, pp. 63–74, 2014.
8. P. Kanuparthy and C. Dovrolis, “DiffProbe: Detecting ISP service discrimination,” in Proceedings - IEEE INFOCOM, 2010.
9. J. Bustos-Jimenez and C. Fuenzalida, “All packets are equal, but some are more equal than others,” in Proceedings - Latin America Networking Conference (LANC ’14). ACM, 2014, pp. 5:1–5:8.
10. V. G. Schaurich, M. Carvalho, and L. Z. Granville, “ISPANN: a policy-based ISP auditor for network neutrality violation detection,” in Proceedings - IEEE International Conference on Advanced Information Networking and Applications (AINA-2018), May 2018.
11. MaxMind, “GeoLite2,” https://dev.maxmind.com/geoip/geoip2/geolite2/, 2018, [Online; accessed 20-June-2018].

ABOUT THE AUTHORS

Márcio Barbosa de Carvalho received his B.Sc. (2010) and M.Sc. (2015) degrees in computer science from Federal University of Rio Grande do Sul (UFRGS). He is currently a Ph.D. student in the Institute of Informatics of UFRGS. His current research interests include network neutrality and network softwarization. Contact him at mbcarvalho@inf.ufrgs.br.

Vinícius Garcez Schaurich received his B.Sc. degree in computer engineering from Federal University of Rio Grande do Sul (UFRGS) in 2015. He is currently an M.Sc. student in the Institute of Informatics of UFRGS. His current research interests include network neutrality and network management. Contact him at vgschaurich@inf.ufrgs.br.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/MIC.2018.2877836, IEEE Internet Computing

Lisandro Zambenedetti Granville received his M.Sc. (1998) and Ph.D. (2001) degrees in computer science from Federal University of Rio Grande do Sul (UFRGS). He is currently an associate professor with the Institute of Informatics of UFRGS. He is a previous member of the Brazilian Internet Committee (CGI.br), previous Chair of the Committee on Network Operations and Management (CNOM) of IEEE ComSoc, and current co-chair of the Network Management Research Group (NMRG) of the IRTF, and current president of the Brazilian Computer Society (SBC). Lisandro's interests include: network neutrality, network virtualization, and network management. Contact him at granville@inf.ufrgs.br.