IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 October 2023, accepted 31 October 2023, date of publication 8 November 2023, date of current version 15 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3331609

RESEARCH ARTICLE

Analysis of Internet Traffic in Ecuador

DAVID PONCE[1], CHRISTIAN TIPANTUÑA[1], AND CRISTIAN ESPINOSA[2]

[1]Departmento de Electrónica, Telecomunicaciones y Redes de Información (DETRI), Escuela Politécnica Nacional, Quito 170525, Ecuador
[2]Asociación de Empresas Proveedoras de Servicios de Internet, Valor Agregado, Portadores y Tecnologías de la Información (AEPROVI), Quito 170505, Ecuador

Corresponding author: Christian Tipantuña (christian.tipantuna@epn.edu.ec)

The authors acknowledges the support from Escuela Politécnica Nacional and Asociación de Empresas Proveedoras de Servicios de Internet, Valor Agregado, Portadores y Tecnologías de la Información (AEPROVI).

ABSTRACT This paper presents a comprehensive analysis of Internet traffic growth and behavior in Ecuador over five years, focusing on the impact of the COVID-19 pandemic on this trend. This period allows us to analyze the behavior of the Internet before, during, and after the pandemic from a quantitative point of view, given that a study related to this topic has not been presented in the country in recent years. This study examines the fundamental concepts of autonomous systems (AS) and Internet exchange points. AEPROVI (Association of Internet Service Providers, Value-added Services, Carriers, and Information Technologies) provides the data for traffic analysis. This data has allowed us to analyze the distribution of assigned and utilized IPv4 and IPv6 addresses, local prefix exchanges of major AS, and bit rate capacities used by major Internet Service Providers. In addition, this study investigates how the pandemic increased the demand for virtual education and telework, resulting in an unanticipated surge in Internet traffic that placed additional burdens on existing infrastructure. The paper also highlights how ISPs responded by increasing the capacity of their links, resulting in a significant increase in the bit rate (throughput) used during the study period.

INDEX TERMS Internet traffic, ASN, COVID-19, IXP, ISPs.

I. INTRODUCTION

The history of the Internet dates back to the early 1970s, when the ARPANET (Advanced Research Projects Agency Network) communications network emerged in the United States, connecting military and research bases during the Cold War. Over time, this network expanded, and different universities, research centers, and later, major corporations joined, seeking to improve the efficiency of their businesses [1]. During the 1990s, a significant change occurred in the structure and function of ARPANET. The network was transformed into what we now know as the Internet. With the emergence of the Hypertext Transfer Protocol (HTTP) and the Hypertext Markup Language (HTML), the World Wide Web (WWW) was created, allowing users to access information and services online from anywhere in the world. In addition, the emergence of web browsers such as Netscape Navigator and Microsoft Internet Explorer facilitated navigation and access to information on the network [1].

As the Internet expanded worldwide, technologies and applications emerged, such as instant messaging, email, video conferencing, social networking, and e-commerce. The growing need for greater connection capacity and data speed led to the introduction of new technologies, such as broadband access and mobile technology [1]. In Ecuador, access to the Internet began to develop in the mid-1990s with the emergence of the first Internet Service Providers (ISPs) in the country. Internet adoption in Ecuador accelerated in the 2000s with the emergence of new technologies such as broadband and mobile technology, which facilitated access to the network [2].

This paper formally analyzes the growth and behavior of Internet traffic in Ecuador over the past five years (from December 2017 to November 2022). The motivation for conducting this study is to quantitatively understand the current distribution of assigned IPv4 and IPv6 addresses, the exchange of prefixes (network address plus mask) at the local level, information about the main Autonomous Systems (AS) assigned and used in the country, and the capacity in terms of bit rate used by the main Internet service providers. The analysis aims to be conducted from the perspective of an Internet Exchange Point (IXP) in

The associate editor coordinating the review of this manuscript and approving it for publication was P. K. Gupta.

Ecuador, explicitly taking into account the information from the Network Access Point (NAP) of Ecuador (NAP.EC), which is managed by the Association of Internet Service Providers, Value-added Services, Carriers, and Information Technologies (AEPROVI) [3].

An approach is taken for five years considering the impact of unplanned growth in Internet traffic, largely due to the COVID-19 pandemic. The COVID-19 pandemic significantly impacted Internet traffic worldwide, and Ecuador was no exception. The country's demand for Internet access and online connectivity increased dramatically with the need to implement social distancing measures and remote work. Internet traffic surged, increasing demand for network infrastructure and driving the expansion and modernization of Ecuador's Internet network [4]. The need to work, study, and socialize from home has increased the demand for Internet services such as video conferencing, content streaming, and online shopping. In addition, digital entertainment, such as online gaming, has experienced a significant increase in users. All of this has led to the rise in Internet traffic, which has tested the infrastructure and capacity of ISPs.

The rest of the paper is organized as follows. Subsection I-A presents the theoretical framework related to the evolution, definitions, and metrics used for measuring Internet traffic in Ecuador, as well as an explanation of the COVID-19 situation in Ecuador. Section II outlines obtaining and processing Internet traffic information from various AS in the country through AEPROVI. Section III reports the results obtained from processing the Internet traffic information of the different AS in Ecuador. Various plots are displayed to quantitatively illustrate the growth of AS and IPv4/IPv6 prefixes of the main AS used in the country. Additionally, an analysis is conducted to understand how the Internet traffic in Ecuador has evolved in terms of effective bit transmission speed (throughput) before, during, and after the COVID-19 pandemic. Finally, conclusions and future work are outlined in Section IV.

A. INTERNET EVOLUTION IN ECUADOR

Since the introduction of the Internet in Ecuador in the 1990s, many technological changes and advancements have led to a significant increase in Internet adoption in Ecuadorian territory. Figure 1 summarizes the most important milestones in the evolution of the Internet in Ecuador from its beginnings to the present day. Through this timeline, we can explore the significant landmarks and developments that have taken place in the country about the Internet and how they have influenced society, the economy, and culture. This information is highly relevant for understanding how the country's technological landscape has changed and impacted the population's lives. Moreover, analyzing the evolution of the Internet in Ecuador can provide a broader insight into the use of the Internet in developing countries and its impact on economic and social growth.

The timeline in Fig. 1 provides a general overview of the evolution of the Internet in Ecuador over the years, from the first established nodes in 1991 and 1992 through the popularization of Internet usage in the 1990s to the consolidation and growth in businesses and educational systems in the early years of the new millennium [5]. In 2007, a breakthrough occurred with connecting the fiber optic ring through the SAm-1 system, which increased Internet connectivity capacity and reduced network response times. In 2013, the Organic Communication Law was approved, allowing for unrestricted Internet access by ISPs [5]. The National Plan for Good Living from 2014 to 2017 focused on reducing illiteracy and increasing the use of ICTs in the country, while digital growth in recent years has been characterized by a significant increase in the number of Internet users in Ecuador, with 76% of the active population actively connected and generating web traffic [5].

It is important to note that the timeline reflects not only the technological evolution in the country but also the public policies and regulations that have influenced Internet access in Ecuador. However, in 2020, the pandemic caused by COVID-19 arrived in Ecuador, causing a radical change in how the Internet was used in the country. The health crisis generated an urgent need for connectivity, accelerating the transition to a digital world and allowing many people to work, study, and carry out their daily activities from home. Thus, the pandemic accelerated Ecuador's digitization process and highlighted the country's existing digital divide. In this sense, the need for public policies that allow for greater digital inclusion and adequate infrastructure to guarantee access to the Internet throughout the national territory became evident.

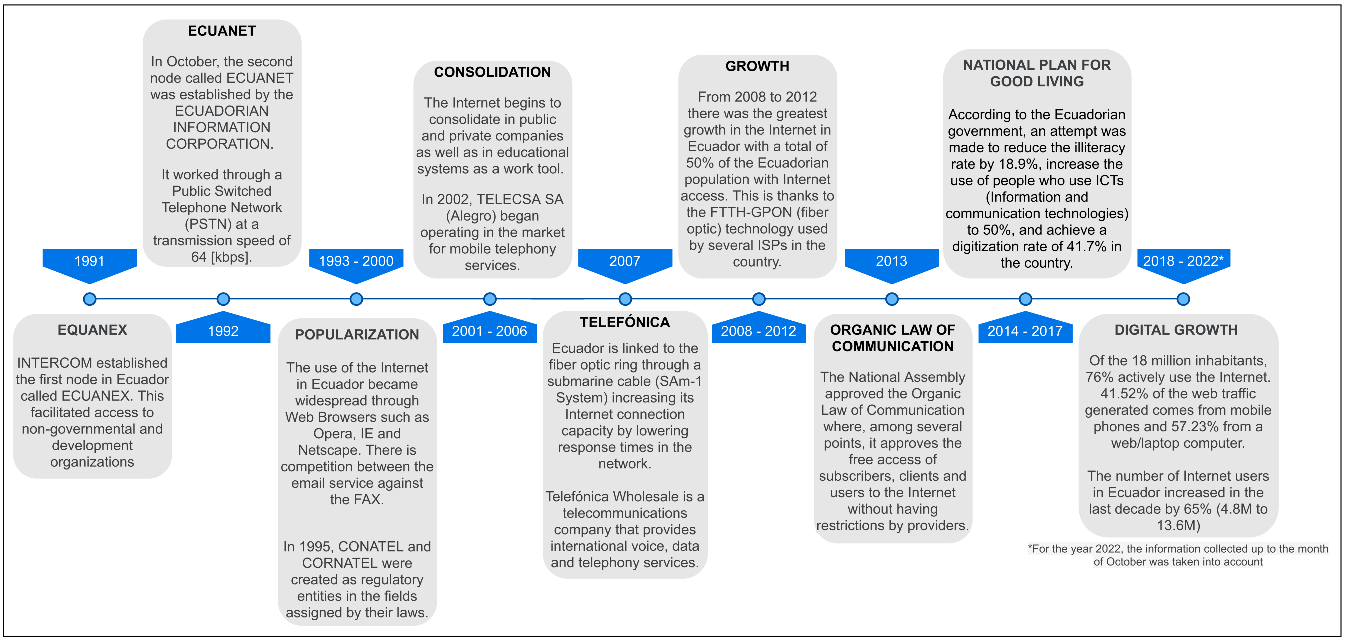
1) CORONAVIRUS IN ECUADOR

COVID-19 (an abbreviation for coronavirus disease 2019) is an infectious disease caused by the SARS-CoV-2 coronavirus that was first identified in Wuhan, China, in late 2019. Since then, it has spread to many parts of the world, causing a global pandemic [6].

In Ecuador, the first confirmed positive case of COVID-19 was reported on February 29, 2020, by the Ministry of Public Health of Ecuador. A month later, in 1924, confirmed cases and 58 deaths were reported. As a result of this "exponential" growth, the National Emergency Operations Committee (COE) took prevention measures for the well-being of the Ecuadorian population, which are explained below [7]:

- Closure of air and sea borders.
- Suspension of social/mass events (maximum capacity allowed 30 people).
- Indefinite suspension of in-person education activities (at all educational levels: primary, secondary, higher education institutions).
- Telematic work mode for educational institutions.
- Telematic work mode (whenever work needs and nature allows it).

These prevention measures resulted in many families hiring Internet services for the first time, users subscribing



1991

EQUANEX

INTERCOM established the first node in Ecuador called ECUANEX. This facilitated access to non-governmental and development organizations

1992

ECUANET

In October, the second node called ECUANET was established by the ECUADORIAN INFORMATION CORPORATION.

It worked through a Public Switched Telephone Network (PSTN) at a transmission speed of 64 [kbps].

1993 - 2000

POPULARIZATION

The use of the Internet in Ecuador became widespread through Web Browsers such as Opera, IE and Netscape. There is competition between the email service against the FAX.

In 1995, CONATEL and CORNATEL were created as regulatory entities in the fields assigned by their laws.

2001 - 2006

CONSOLIDATION

The Internet begins to consolidate in public and private companies as well as in educational systems as a work tool.

In 2002, TELECSA SA (Alegro) began operating in the market for mobile telephony services.

2007

TELEFÓNICA

Ecuador is linked to the fiber optic ring through a submarine cable (SAm-1 System) increasing its Internet connection capacity by lowering response times in the network.

Telefónica Wholesale is a telecommunications company that provides international voice, data and telephony services.

2008 - 2012

GROWTH

From 2008 to 2012 there was the greatest growth in the Internet in Ecuador with a total of 50% of the Ecuadorian population with Internet access. This is thanks to the FTTH-GPON (fiber optic) technology used by several ISPs in the country.

2013

ORGANIC LAW OF COMMUNICATION

The National Assembly approved the Organic Law of Communication where, among several points, it approves the free access of subscribers, clients and users to the Internet without having restrictions by providers.

2014 - 2017

NATIONAL PLAN FOR GOOD LIVING

According to the Ecuadorian government, an attempt was made to reduce the illiteracy rate by 18.9%, increase the use of people who use ICTs (Information and communication technologies) to 50%, and achieve a digitization rate of 41.7% in the country.

2018 - 2022*

DIGITAL GROWTH

Of the 18 million inhabitants, 76% actively use the Internet. 41.52% of the web traffic generated comes from mobile phones and 57.23% from a web/laptop computer.

The number of Internet users in Ecuador increased in the last decade by 65% (4.8M to 13.6M)

*For the year 2022, the information collected up to the month of October was taken into account

FIGURE 1. Evolution of internet in ecuador [5].

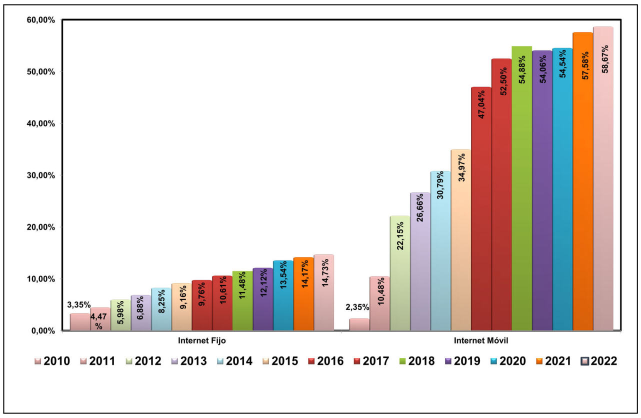


FIGURE 2. Fixed and mobile internet accounts per 100 inhabitants in ecuador - 2020 [8].

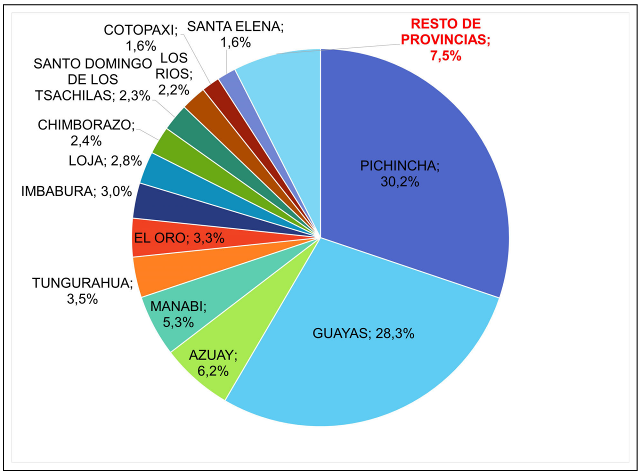


FIGURE 3. Fixed Internet accounts by province - 2020 [8].

to more robust Internet plans, or even switching providers. Table 1 and Fig. 2 present statistics from the Telecommunications Regulation and Control Agency (ARCOTEL) in 2020, showing that the number of Internet users increased by 1.90% compared to 2019 and a growth of 3.57% compared to 2021. Figure 3 shows the increase in fixed Internet accounts in 2020 by province, with Pichincha and Guayas being the provinces with the highest user increase compared to 2019.

The data in Table 1, Fig. 2, and Fig. 3 allow us to analyze the geographical distribution of Internet users, which helps identify possible digital inequalities and gaps that may exist. In Ecuador in 2020, the most used Internet access technologies by users were mobile, such as 4G connection and USB modem connection, followed by fixed broadband and Wi-Fi networks, providing a complete picture of the connectivity situation in the country, which is essential to develop policies and strategies aimed at improving access and quality of Internet services for the benefit of the population [8].

B. TERMINOLOGIES USED IN TRAFFIC MEASUREMENT

1) INTERNET PROTOCOL (IP)

Internet Protocol (IP) is a fundamental communication protocol within the Internet architecture. It defines a comprehensive set of regulations governing data packets' routing, addressing, and fragmentation, enabling efficient traversal across interconnected networks while ensuring their accurate delivery to the intended destinations. These data packets encompass discrete information units and have IP headers containing essential routing information. These headers facilitate the packet forwarding process by intermediary routers,

TABLE 1. Statistics on fixed and mobile Internet accounts per 100 inhabitants [8].

Fixed and mobile Internet accounts						
Year	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**
Fixed Internet	10,606%	11,480%	12,120%	13,542%	14,166%	14,727%
Mobile Internet	52,495%	54,882%	54,064%	54,541%	57,579%	58,670%
Total	63,10%	66,36%	66,18%	68,08%	71,75%	73,40%

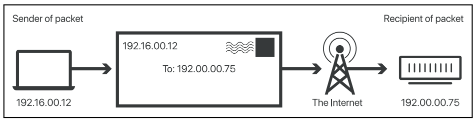


FIGURE 4. IP illustrative example, based on [9].

directing the packets along the optimal path toward their respective destinations. Each node or domain participating in the Internet ecosystem has a unique IP address, a numerical label that plays a pivotal role in the precise data routing. As stipulated by the IP protocol, this addressing scheme forms the backbone of the Internet's communication fabric, ensuring seamless data transmission across diverse network topologies. IP's conceptual framework and operational intricacies are formally documented in several RFCs (Request for Comments), essential references that continually refine and define the protocol's specifications [9].

Refer to Fig. 13 for an example to better understand the TCP/IP layer model operation, referring to Fig. 4.

2) INTERNET SERVICE PROVIDER (ISP)

ISPs, or Internet Service Providers, provide Internet access services to their customers. To achieve this, ISPs use various network technologies and protocols, such as DSL, coaxial cable, fiber optics, and wireless technologies, such as Wi-Fi or 5G. In addition to providing Internet connectivity, ISPs may offer additional services such as web hosting, domain name registration, email, server management, and computer security [10]. In 2020 (during the COVID-19 pandemic), the leading ISPs in Ecuador were the National Telecommunications Corporation (CNT EP) and Megadatos S.A. (trading as Netlife), as shown in Fig. 5.

3) AUTONOMOUS SYSTEM (AS)

An Autonomous System (AS) is defined as a group of IP networks that share their own (internal and external) routing policy and operate independently [11]. This routing policy applies to a single network or a group of networks that one or multiple administrators manage under a single administrative entity. Internal networks within an AS communicate through Interior Gateway Protocol (IGP) routing protocols, while an AS shares its routing information with other AS through Exterior Gateway Protocol (EGP) routing protocols [12], as shown in the example in Fig. 6.

Each AS has an identifier (ASN: Autonomous System Number) of size 16 or 32 bits assigned as indicated in Table 2. The detail about the assigned RFC is described below.

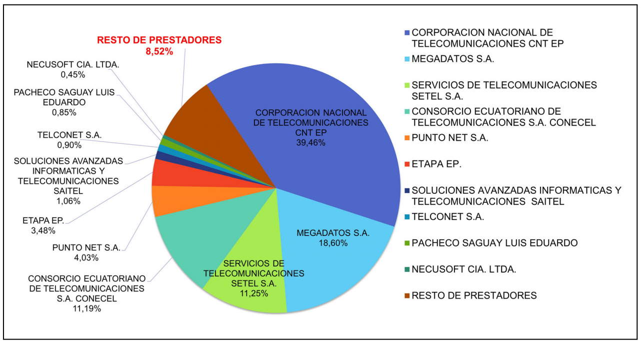


FIGURE 5. Main and fixed Internet services providers - 2020 [8].

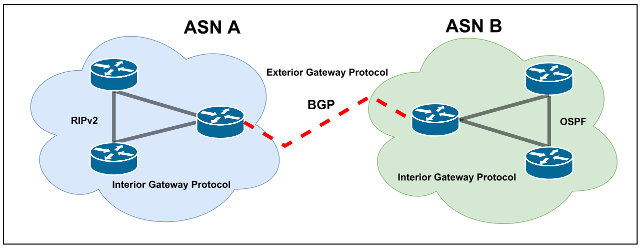

ASN A
ASN B
Exterior Gateway Protocol
BGP
RIPv2
OSPF
Interior Gateway Protocol
Interior Gateway Protocol

FIGURE 6. Example of connection between ASs, based on [12].

TABLE 2. Distribution of ASNs [11].

Autonomous System Number (ASN)	
Range	**Assignment**
0 and 65535	Reserved
[1 - 64495]	Public Internet
[64496 - 64511]	RFC 5737
[64512 - 64534]	Private
[65536 - 65551]	RFC 5398
[65552 - 4294967295]	Public Internet

- **RFC 5737**: Reserved IPv4 address blocks for documentation purposes [13].
- **RFC 5398**: Reservation of AS number for documentation use [14].

RFC 5737 and 5398 are two documents that describe the reservation of network resources. RFC 5737 describes blocks of IPv4 addresses reserved for use in documentation and testing and should not be used on the public Internet. Likewise, RFC 5398 describes the reservation of ASNs for use in documentation, providing a range of ASNs that can be used for these purposes (documentation and testing), helping to maintain the integrity of the public Internet by preventing unauthorized use of IP addresses and ASNs [13], [14].

4) BORDER GATEWAY PROTOCOL (BGP)

Routing protocols are essential for properly functioning the Internet, as they are responsible for directing network traffic through the best possible route. These protocols can be divided into two main categories: internal and external.

1) **Internal (IGP: Interior Gateway Protocol):** It is a routing protocol used to exchange routing information within an AS, within a private or corporate network. Routing protocols that are used as IGPs include OSPF, EIGRP, RIP, and IS-IS. Each protocol has its characteristics and advantages, and the choice of one or the other depends on the needs and design of the network [11].
2) **External (EGP: Exterior Gateway Protocol):** It is a routing protocol that exchanges routing information between various AS. It is essential in the interconnection of different networks and is used by ISPs to exchange routing table information with other ISPs and content networks, such as Content Delivery Networks (CDNs). A CDN is a type of network focused on improving the quality of the Internet (QoS: Quality of Service). Its main function is to replicate/distribute content from an origin server to different mirrors scattered across the Internet and serve requests from a mirror near where those requests originate. These mirror servers are the closest to the node that made the request(s) [11].

   It is important to note that routing protocols must be compatible to allow effective communication and interconnection of different networks [11].

The BGP table is a routing table used by the edge routers of an AS to make routing decisions in a network. This table contains information such as the destination IP address, the destination ASN, and the next hop required to reach the destination, as well as information about the reachable networks and the paths to reach those networks through other AS. Through the BGP table, better quality and lower cost routes can be established to send traffic from one AS to another. It is updated as routers exchange routing information and is, therefore, essential to ensure the connectivity and efficiency of the Internet network [15]. BGP uses TCP as its transport protocol at layer 4 of the 7-layer OSI model. To initiate the transmission of information (BGP session), a TCP connection is established between a pair of routers, after which they begin to exchange routing information as follows:

- **Learn routes:** It means that BGP is incorporating (learning) into the BGP table any route the neighboring routers are reporting (advertising).
- **Announce routes:** It means that BGP informs (announces) its neighboring routers that it has (contains) the route that any neighboring router requires to reach a given destination, and that route is found in the routing table.

Figure 7 simulates a BGP connection between two ISPs within the same AS.

A BGP session must first be established to exchange BGP table information between routers *R1_GYE* and *R1_UIO*. Network route updates are then exchanged in both directions. Once each router's BGP table has been updated with the routing information received via the BGP session, the next step is to use the routing information to determine the best route to the destination networks [16]. BGP uses an update-based system, which sends routing information only when there are changes in the network topology. This way, the amount of information transmitted through the network is minimized, and unnecessary traffic overload is avoided. In addition, BGP uses a system of prefixes (IPv4 and IPv6) to identify networks and routes, allowing greater flexibility in routing traffic through multiple networks and ISPs [16].

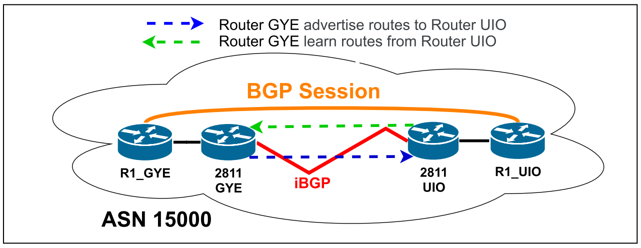

Router GYE advertise routes to Router UIO
Router GYE learn routes from Router UIO
BGP Session
R1_GYE
2811 GYE
iBGP
2811 UIO
R1_UIO
ASN 15000

FIGURE 7. BGP protocol operation, based on [11].

5) TRANSPORT PROVIDERS

They are ISPs or telecommunications companies that manage their wide area network (network infrastructure) and provide Internet connectivity to other AS through their network, allowing data to travel from one network to another. These providers are commonly used by smaller networks that cannot afford the necessary infrastructure to connect directly to other networks [17]. If the ISP covers large geographic areas with high-speed networks, giving connections to other networks, the ISP is known as a backbone provider. ISPs that target customers as end users are known as access providers [10].

6) INTERNET EXCHANGE POINT (IXP)

An Internet Exchange Point (IXP: Internet Exchange Point) is an interconnection facility where ISPs become members to exchange traffic with other ISPs through the physical infrastructure [18]. These physical infrastructures are usually housed in Data Centers where Internet infrastructure companies, such as CDNs and ISPs, connect to exchange traffic [19]. Figure 8 presents a basic connection between an ISP and a CDN to an IXP.

IXPs provide benefits to both end users and ISPs because by connecting directly to the exchange point, it is possible to route traffic more efficiently, reducing network latency as well as reducing operating costs, and improving the speed of data transmission, guaranteeing an excellent QoS [19]. One of the Internet infrastructure companies that connect through IXPs are CDNs [20].

7) DATA CENTERS

Data centers are fundamental infrastructures within modern networks. They are highly specialized facilities that house

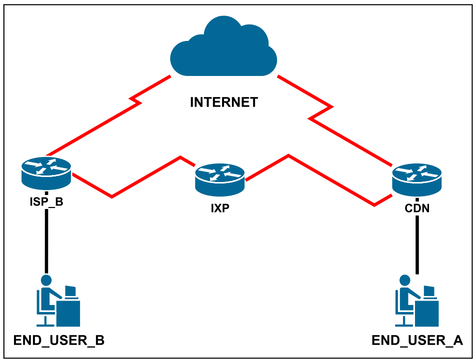


FIGURE 8. Basic IXP topology, based on [19].

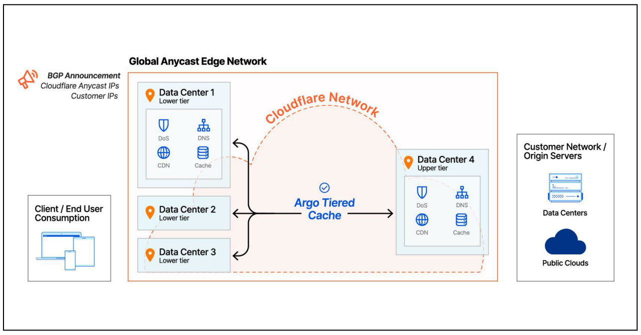


FIGURE 9. Traffic flow: Argo Tiered Cache, Smart Tiered Cache topology, based on [23].

and manage many servers and networking equipment. A Data Center is a facility that houses interconnected computing equipment with access to the Internet, intended to host and manage critical data, including websites, CDN servers, and caches, for an entity or company. These centers can be privately owned by an organization or provide services (such as Telecommunications Service Providers), partially or entirely, to third parties. Moreover, they can establish Internet connections through dedicated, third-party, or carrier-provided links. Data centers can also connect to IXPs and host some or all of the services offered by these IXPs [21].

Based on their infrastructure and ability to provide uninterrupted service, data centers receive certifications at different levels, such as Tier I (basic), Tier II (redundant), Tier III (increased redundancy), and Tier IV (fully fault-tolerant) [21].

The main objective of CDNs is to speed up loading time by "bringing" content or its services closer to users, reducing latency, and using trunk links. They also avoid link congestion that would otherwise occur near the origin server [22].

To replicate content from central sites or applications, CDNs use cache or mirror servers and anycast technology (which uses BGP and allows different servers, no matter where they are located, to use the same IP address). This is where CDNs have their cache servers hosted in data centers or IXPs. In this way, they "get closer" to users worldwide, allowing address requests to be resolved more quickly [22].

Those interested in developing CDN networks are normally large content or application providers that seek to expand their services regionally or globally, obtain a greater number of users, and offer them the best quality or experiences in their services. These content or application generators, such as Google, Netflix, or Facebook invest in their own CDN networks and negotiate to locate the corresponding servers in the IXPs of different countries [22].

Figure 9 illustrates how Cloudflare CDN operates within a data center: traffic flow #1 displays the traffic flow when a client request is received by a data center closest to the client, Data Center 1. Since there is nothing locally cached on the ingress data center and tiered caching is enabled, a request is sent to the upper-tier data center to request a copy of the content to cache. Because the upper tier data center also does not have the content cached, it sends the request to the origin server, caches the received content upon response, and responds to the lower tier data center with the cached content. The lower tier data center caches the content and responds to the client [23].

Notice that when a new request for the same content is made to another data center (traffic flow #2), Data Center 2, the content is not locally cached; however, the content is retrieved from the upper tier data center, where it was cached from the first request for the same content [23].

With the upper tier data center returning the cached content for the second request, the trip to the origin server is prevented, resulting in higher cache hit ratios, faster response times, saved bandwidth cost between the Cloudflare network and the origin server, and reduced load on the origin server responding to requests [23].

C. METRICS TO EVALUATE IN A NETWORK

The most important metrics to evaluate within a network are described below:

1) **Latency:** This is when a data packet travels from its source to its destination. It is typically measured in milliseconds [ms] and can be affected by various factors such as distance, network congestion, and routing. High latency can result in slow response times and reduced overall performance [10].
2) **Packet loss:** Packet loss is the percentage of data packets lost during transmission. This can occur due to various factors, such as network congestion, routing issues, or hardware failure. High packet loss can cause data retransmission and reduced network performance [10].
3) **Jitter:** Jitter is the variability in latency between packets. Jitter can be caused by network congestion, routing issues, or other factors and can significantly affect voice and video quality. Jitter is usually measured in milliseconds [ms] [24].
4) **Bandwidth:** Bandwidth measures the data transmitted over a network connection in a specific period, usually measured in bits per second [bps]. Bandwidth is a critical metric for networks that support real-time

applications such as video conferencing and online gaming [25].

5) **Availability:** Availability measures the percentage of time that a network is accessible and functional. Network downtime can be caused by hardware failure, network congestion, or other factors and can have a significant business impact. High availability is crucial for critical applications and services [10].
6) **Security:** Security measures the level of protection against unauthorized access, attacks, and data breaches. This includes protection against hacking, viruses, malware, and other cyber attacks. Network security is essential to protect sensitive data and maintain the confidentiality and integrity of information [10].
7) **Reliability:** Reliability measures the ability of the network to deliver data without errors or failures. Network reliability is crucial for critical applications and services and is often measured in terms of the percentage of time that a network is operational and delivering error-free data. High reliability ensures data is transmitted accurately and consistently [10].
8) **Throughput:** Throughput is the amount of data that can be transferred over a network in a given period, measured in bits per second [bps]. It is important to remember that throughput is not equal to the speed of the contracted Internet service because it may be limited by geographical distance, the type of connection technology used, and the limitations of the ISP network [10].

D. TRAFFIC MEASUREMENTS

1) PASSIVE MEASUREMENT

Passive traffic measurement is performed by observing the traffic flowing through the network without interrupting or affecting it. This technique is commonly used to measure data flow on the network, which involves counting the number of packets and bytes transmitted through routers, switches, or any other network device. It can be done using specialized software tools that capture packets passing through a network device and extract relevant information, such as the source/destination IP address, the protocol used, and the packet length. These tools can be configured to analyze and report specific information of interest, such as traffic volume, data transfer rate, and bandwidth used, among others [10].

2) ACTIVE MEASUREMENT

They are carried out by sending test traffic to the network. An example of measurement is the maximum load capacity of the network by sending packets and increasing the transmission speed until the network is saturated [10].

E. INSTITUTIONS THAT MANAGE THE INTERNET IN ECUADOR

Internet administration around the world is carried out through various organizations and entities. The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization responsible for coordinating the assignment of unique identifiers on the Internet, including domain names, IP addresses, and protocol parameters. The Internet Engineering Task Force (IETF) is an open community of experts dedicated to the research, development, and standardization of Internet technologies [26]. Another regional Internet administration organization is the Latin American and Caribbean Internet Address Registry (LACNIC).

LACNIC is a non-profit organization that distributes and administers IP addresses and AS numbers in the Latin American and Caribbean region. LACNIC is a member of the Number Resources Organization (NRO), which coordinates the global distribution of Internet resources such as IP addresses, ASNs, and protocol parameters in the different layers of the OSI model [27]. In Ecuador, the legal entity that manages Internet traffic is called AEPROVI.

1) AEPROVI

The Association of Internet, Value Added, Carriers, and Information Technology Service Providers (AEPROVI) is a non-profit entity in the country's telecommunications and information technology sector. Their mission is to promote, protect, spread, and develop the Internet as a means of social, political, and economic progress within the Ecuadorian territory [28]. Since July 4, 2001, AEPROVI has been the promoter of implementing a network infrastructure called NAP Ecuador (NAP.EC).

F. NAP ECUADOR

The network access point infrastructure in Ecuador (abbreviated NAP.EC) allows the exchange of local Internet traffic originated and received in the country. This local traffic exchange is done through an agreement (also known as a Peering agreement[1]) between AEPROVI and the participants [3]. Within the signing of agreements between the NAP.EC and the different ASNs, different Internet services are hosted that give added value to the local traffic exchange, such as copies of the DNS servers of the root domain, .EC domain server, and nodes of CDN networks [3].

1) NETWORK TOPOLOGY - NAP.EC

The NAP.EC network infrastructure is hosted in the cities of Quito and Guayaquil. The different AS connect from their edge switch to the respective CDN server of the IXP through an ethernet switch (link layer or layer 2 infrastructure) with the BGP protocol. This infrastructure works with its number of AS and manages its range of public domain IP addresses [30]. Figure 10 presents the logical topology network, which currently works NAP.EC. There are 19 ASs connected *directly* to the NAP.EC network infrastructure [30].

[1] **Peering Agreement:** It is a mutual agreement between two or more ASNs to exchange traffic directly between them, without the need to pass through third-party networks or transit providers. This allows an improvement in the quality of service and cost reduction [29].

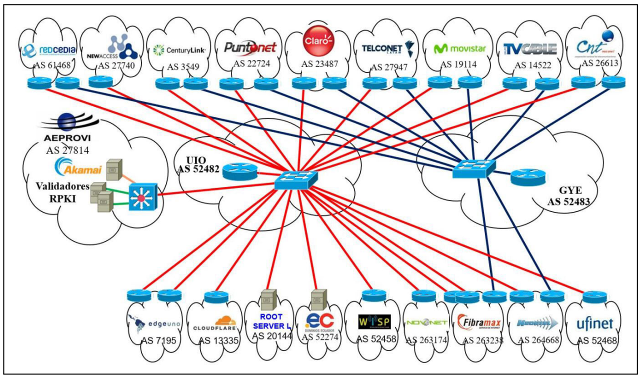


FIGURE 10. Logical topology NAP.EC, updated date of March 2023 [30].

It is important to note that even if there are only 19 AS directly connected to the NAP.EC, these may be connected to other AS indirectly through the transit providers (see Section I-B5) that they use to reach the NAP. Furthermore, some ASs may be larger than others and have a greater presence in the IXP, being able to have direct connections with more AS. In addition, there is a WAN (WAN: Wide Area Network), where the topology has redundant links because AS are connected both in Quito and Guayaquil. The information is stored and managed by AEPROVI, connected to the NAP.EC AS.

2) POLICIES ON TRAFFIC EXCHANGE - NAP.EC

The exchange of traffic between the different AS is done in two different ways:

1) **Multilateral mandatory:** Any participating AS that subscribes to the NAP.EC must mandatorily exchange traffic with all other AS that are subscribed to the NAP.EC [31].
2) **Selective multilateral:** Those AS that subscribed with special agreements with AEPROVI to connect to an IXP only exchange traffic with those AS that, likewise, have special agreements with AEPROVI and agree with the peering conditions established above [31].

3) ROUTING POLICIES - NAP.EC

NAP.EC works under fifteen routing policies that allow managing Internet traffic in Ecuador [32]. These policies are available in Annex V-A of this paper.

II. METHODOLOGY

This section describes obtaining and processing Internet traffic information in Ecuador from the different AS in the country through the information provided by AEPROVI. In addition, it details how to carry out the data extraction and its subsequent tabulation through the use of scripts developed for this purpose.

A. GENERAL PROCESS

Figure 11 presents the procedure for analyzing the behavior of Internet traffic in Ecuador. The Business Process Modeling Notation[2]) to represent the entire general process.

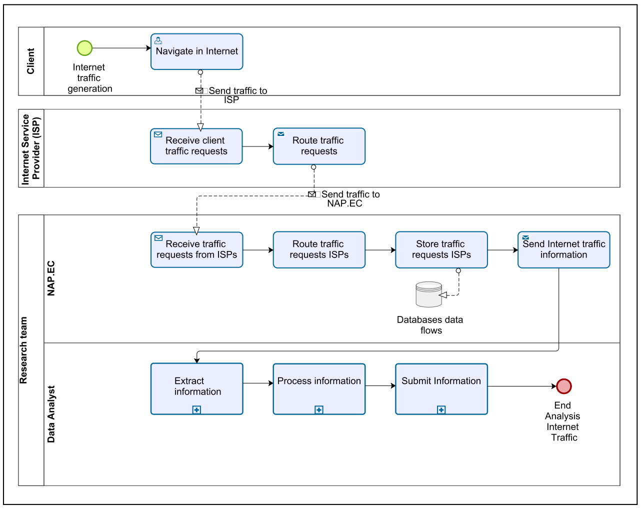

Client
Internet traffic generation
Navigate in Internet
Send traffic to ISP
Internet Service Provider (ISP)
Receive client traffic requests
Route traffic requests
Send traffic to NAP.EC
Research team
NAP.EC
Receive traffic requests from ISPs
Route traffic requests ISPs
Store traffic requests ISPs
Send Internet traffic information
Databases data flows
Data Analyst
Extract information
Process information
Submit Information
End Analysis Internet Traffic

FIGURE 11. Internet traffic analysis process.

In Fig. 11, the interaction between three roles is observed: the client, ISP, and the research group of NAP.EC and the data analyst. The process begins when the client generates Internet traffic by making a query in a web browser. Then, it interacts with the ISP to send the traffic generated in the web browser, where the ISP is in charge of receiving and routing the traffic requests sent to the NAP.EC. Then, the NAP is responsible for receiving the ISP traffic requests, routing, and storing them. It is important to mention that the NAP stores data flows; it does not discriminate the type of information that reaches it (*i.e.*, data, voice, video, among others, see *Annex V-A - Routing Policies*). Finally, this information is sent to the data analyst of the research team, who is in charge of extracting, processing, and loading (ETL: Extract, Transform, Load) the Internet traffic information in Ecuador.

B. NAP.EC DATA ANALYSIS

With the help of the information provided by the NAP.EC research team, Internet traffic information is extracted and processed through all the AS directly connected to the NAP.EC, both in the ASs of the city of Quito and Guayaquil. An explanation is presented at the network equipment (routers) level within the NAP to better understand the ETL process of Internet traffic information.EC topology.

C. INFORMATION EXTRACTION BY NAP.EC

From the routers located in the cities of Quito and Guayaquil corresponding to the AS within the NAP.EC, information is extracted from the routing tables within the AS of the NAP. The following commands obtain all the information from the routing tables.

[2] **BPMN:** Business Process Modeling Notation was used to standardize the modeling of business processes through a common language to facilitate the understanding of performance and development of one or several activities [33].

1) TABLE OF ADDRESSING IPv4 PREFIXES

Command 1 allows the display of the contents of the BGP routing table. The output shows the status of BGP connections, the number of advertised prefixes, and the current BGP routing table, including the IP addresses of the prefixes, their next hop, and the route attributes [34].

Command 1. IPv4 routing table.

```
show ip bgp
```

Some of the route attributes include [34]:

1) AS_PATH: Indicates the path followed by the route through the ASs to reach the destination. For example, if the AS_PATH is 65001 65002 65003, the path has passed through ASs 65001, 65002, and 65003.
2) NEXT_HOP: Indicates the IP address of the next hop to reach the next AS in the route. For example, if the NEXT_HOP is 192.168.1.1, the next hop to reach the next AS is through the IP address 192.168.1.1.
3) LOCAL_PREF: It is an attribute used to determine the local preference of a route. For example, if multiple routes are available to reach the same destination, the router chooses the route with the highest LOCAL_PREF.
4) ORIGIN: Indicates how the route originated. It can be IGP, EGP, or incomplete.
5) COMMUNITY: It is a set of optional attributes used to identify a group of routes. For example, if a group of routes has the COMMUNITY "no-export", these routes are not exported from the AS.

Table 3 presents an example of a BGP route. In this example, route 192.168.1.0/24 has been learned through AS 65001, has a LOCAL_PREF of 100, and originated via IGP. The next hop to reach the next network is through the IP address 10.0.0.1.

2) TABLE OF ADDRESSING IPv6 PREFIXES

Command 2 allows retrieving information about the BGP routing table entries for IPv6 unicast routes on the NAP.EC routers (Quito and Guayaquil). This command displays information about the BGP routes that the router has learned, including the network prefix, next hop, and various route attributes such as AS route and local preference (administrative distance). This command is used to verify the BGP routing information that the router has learned [34].

Command 2. IPv6 routing table.

```
show ip bgp ipv6 unicast
```

When two AS are connected, they use BGP to exchange information about routing tables to route traffic between them correctly. To identify incoming and outgoing traffic, BGP uses a concept called "local preference" or "administrative distance". The local preference value is set by the ASN originating the route and determines the preferred route within an AS when multiple routes are available to the same destination [35]. Table 4 presents all the administrative distance values of all the routing protocols that the routers support.

TABLE 3. Example attributes of a BGP route, based on [34].

Prefix	Next_Hop	AS_Path	Loc_Pref	Origin
192.168.1.0/24	10.0.0.1	65001	100	IGP

TABLE 4. Administrative distances [35].

Protocol	Administrative distance
Directly connected	0
Static route	1
EIGRP route summary	5
external BGP	20
EIGRP internal	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
ODR	160
EIGRP external	170
BGP internal	200
Unknown	255

Administrative distance refers to the measure of the reliability of a route in a network. An integer assigned to a specific route determines the best route if multiple routes are available to reach the same destination. The lowest administrative distance value is considered the best route. In the case of BGP, a higher administrative distance value is considered the best path [35].

Once the concepts related to the routing tables (BGP) with IPv4 and IPv6 prefixes have been explained, two scenarios are simulated for a better understanding of the information about the routing tables regarding the incoming and outgoing traffic of the routers corresponding to the AS that manage the NAP.EC.

3) SIMULATION OF INCOMING/OUTGOING TRAFFIC WITHIN NAP.EC

Figure 12 simulates a scenario of a connection between two AS to facilitate an understanding of the information extraction process regarding the BGP tables, differentiating the incoming and outgoing traffic within an AS.

In particular, for the example, the analysis is carried out from the point of view of the **ASN A**, through each router's GigabitEthernet (GE) interfaces. In the case of the ASN A router, outgoing traffic is presented by the blue lines, which go from ASN A to ASN B. Outgoing traffic originates from the GE interface of the ASN A router and is directed towards the interface ASN B router GE. This traffic consists of data packets sent from the ASN A router to the ASN B router, such as emails, files, and messages. On the other hand, the incoming traffic is presented through the green lines, which go from ASN B to ASN A. The incoming

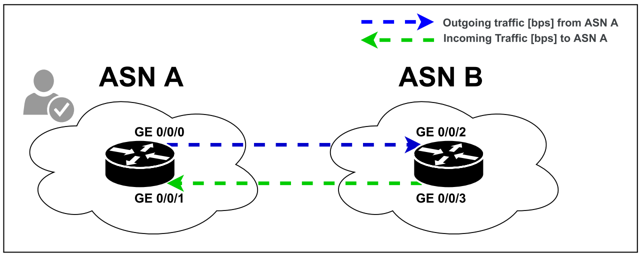

Outgoing traffic [bps] from ASN A
Incoming Traffic [bps] to ASN A
ASN A
ASN B
GE 0/0/0
GE 0/0/2
GE 0/0/1
GE 0/0/3

FIGURE 12. In/Out traffic example between two AS.

traffic originates from the GE interface of the ASN B router and goes to the GE interface of the ASN router A. This traffic consists of responses to previous requests, such as requests for information, file requests, responses to emails, and messages. The symbology used in Fig. 12 presents the following information regarding the interfaces of each router.

- **GE 0/0/1 and GE 0/0/0** are the router's incoming and outgoing gigabit ethernet interfaces corresponding to ASN A.
- **GE 0/0/2 and GE 0/0/3** are incoming and outgoing gigabit ethernet interfaces of the router corresponding to ASN B.

Once the case in Fig. 12 has been presented, Fig. 13 simulates an example of Internet traffic generation from the point of view of an end user who has an ISP that is directly connected to the NAP.EC topology until the information reaches the NAP.EC routers through a CDN connected to the IXP to explain how Internet traffic is generated in Ecuador within the NAP.EC topology (Fig. 10).

A user from the city of Quito is considered to be connected to an ISP with ASN 263328 and wishes to access the streaming platform called Twitch[3] to see your favorite content creator. To do this, follow the procedure described below:

1) The user writes the official page's web address (URL: Uniform Resource Locator) and performs the search in his web browser.
2) The web browser generates an HTTP request (HTTP: Hypertext Transfer Protocol), and it is sent from the application layer (according to the OSI model) to the destination server, the ISP.
3) At the application layer, the HTTP request is formed and sent to the transport layer, where it is packaged into segments and sent over the network via TCP or UDP. The segments are then encapsulated into IP packets at the network layer and then encapsulated into frames at the data link layer for transmission over the physical network, eventually reaching the ISP's network router (ASN 263328).
4) The ISP processes the query. Within the ISP, several servers store and send the data streams of Internet traffic (for example, a NAP server and a DNS server) regarding the query made by the user.

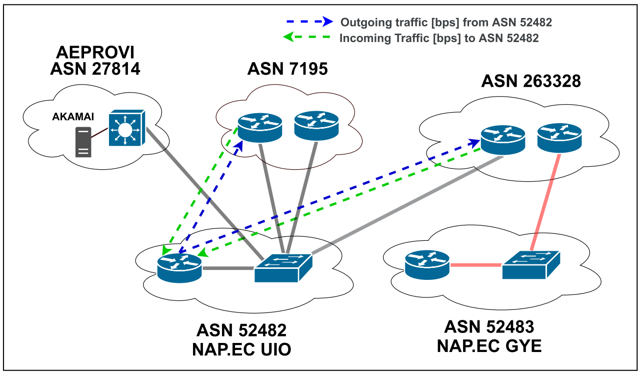


FIGURE 13. Example In/Out traffic within the NAP.EC topology.

5) Because the domain is not found in the router's routing table corresponding to the ISP (ASN 263328), it routes the query through the router of the NAP.UIO of ASN 52482. The NAP.UIO looks in its table of routing what is the ASN that has access to the IP address of the web page and routes the ISP query.
6) In particular, the ASN 7195, through a CDN, has access to the resource, so it routes the request first to the NAP.UIO and then the NAP.UIO generates outgoing traffic, routing the request to the ISP, and finally, the content reaches the end user.

All the information previously presented in this section allows a better understanding of the information extraction phase regarding Internet traffic in Ecuador through the AS directly connected to the NAP.EC. The information comes from the BGP routing tables within the NAP.EC topology, allowing us to know the number of IPv4 and IPv6 prefixes and the distribution of AS assigned and used. Next, it is explained how the information processing phase generated by the BGP routing tables is carried out.

D. INFORMATION PROCESSING BY NAP.EC

Two scripts developed in the Python programming language are utilized for the information processing phase of Internet traffic in Ecuador. These scripts enable the retrieval and processing of information regarding AS, IPv4, and IPv6 prefixes. In this processing phase, the information from the routing tables of the corresponding AS in NAP.EC is matched with the information provided by the Hurricane Electric (HE) BGP Routing tool,[4] in collaboration with LACNIC [38].

Sections II-D1 and II-D2 describe how the information about AS in Ecuador is processed and how the IPv4/IPv6 prefixes are obtained, respectively.

[3] **Twitch:** It is a video streaming platform so that people can share your gaming, creative or talk show content with a live audience [36].

[4] **Hurricane Electric (HE):** HE is a global Internet backbone network. It operates multiple IPv4 and IPv6 backbone networks across continents, including South America. Additionally, it is connected to over 250 IXPs, exchanging traffic with over 9,200 different networks. HE operates in two data centers located in California, USA [37].

1) OBTAINING INFORMATION ON AUTONOMOUS SYSTEMS IN ECUADOR

***Note:** The functions are explained descriptively because this script contains confidential credential information and copyright restrictions.*

For the processing phase of information about AS in Ecuador, NAP.EC utilizes a Python script to obtain AS information. Figure 14 illustrates the flowchart of the implemented script. This script employs functions that gather BGP information from the routing tables of the three routers corresponding to the three ASs in Ecuador: NAP.EC QUITO, NAP.EC GUAYAQUIL, and AEPROVI. The gathered information is processed, and different text files containing AS information in Ecuador are generated as output. Subsequently, the collected data is sent for analysis by the data analyst. The processing of this information enables the identification of patterns and trends in the growth of Internet traffic in Ecuador. The analysis of this information also provides valuable insights for network optimization, bottleneck identification, and network troubleshooting, which are essential for planning and improving the country's Internet infrastructure.

Moreover, using Python for processing this information is a suitable choice as it is a powerful programming language, easy to learn, and popular for data processing and analysis. Additionally, the implemented script is scalable,[5] capable of handling substantial amounts of data, making it suitable for processing AS information in Ecuador, particularly information regarding BGP routing tables.

The following are descriptions of all the relevant processes of the script to obtain AS information in the country:

1) **BGP Routing Table Retrieval:** The function *consulta* allows obtaining the BGP routing tables for IPv4 and IPv6 prefixes on the NAP.EC routers, connected in both Quito and Guayaquil. To achieve this, two lines of code are executed using the *os.system()* function. The first line executes the *sshpass* command, providing the router's IP address (*ip*), username (*username*), and password (*password*) as input arguments for the function. This line runs the *show ip bgp* command, redirecting its output to a text file named *bgpIPv4.txt*. Similarly, the second line of code runs the *show bgp ipv6 unicast* command, redirecting its output to a text file named *bgpIPv6.txt*. Thus, the BGP information from the NAP.EC routers are retrieved securely using the SSH protocol.

2) **Retrieval of AS connected to Quito/Guayaquil:** The function *def informacionASTodo(direccion1, direccion2)* allows obtaining a list of all the AS directly connected to the Quito (NAP.UIO), Guayaquil (NAP.GYE), and AEPROVI (NAP AEPROVI) NAPs. This subroutine takes two input arguments, file paths for the generated IPv4 and IPv6 BGP information files from the previous *consulta(ip, username, password)* function.
The function initializes a list with the three AS of Ecuador. Then it opens the IPv4 BGP information file, reading it line by line and checking if each line contains specific characters. If it does, it splits the line into a list of AS numbers from the IPv4 and IPv6 BGP routing tables and checks if each traversed AS is not yet in the list. If it isn't, it adds it to the list. The function repeats the same process for the second file and returns the list of AS working with both IPv4 and IPv6 addressing for the Quito and Guayaquil AS.

3) **Creation of AS list in Ecuador:** The function *def crearArchivo(listaUIO, listaGYE)* is used to create a file called *datosASTotales.txt* that contains the number of elements in the list of ASs located in Quito and Guayaquil. The function takes two input arguments: the first list *listaUIO* contains the AS located in Quito, and the second list *listaGYE* contains the AS located in Guayaquil. The function writes to the file: the names of each AS, followed by the ASN, and then the number of elements in the second list.

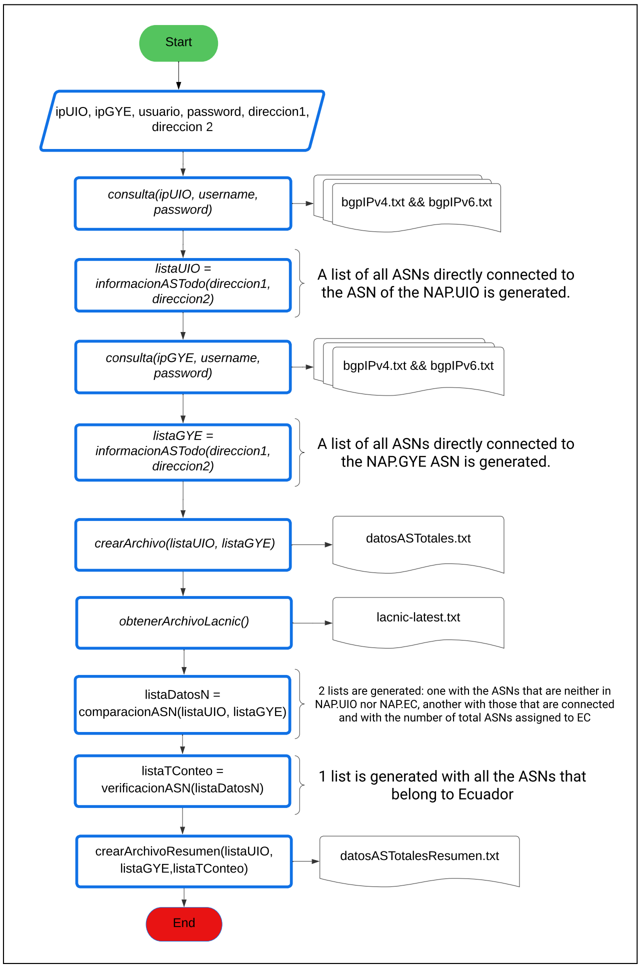

Start
ipUIO, ipGYE, usuario, password, direccion1, direccion 2
consulta(ipUIO, username, password)
bgpIPv4.txt && bgpIPv6.txt
listaUIO = informacionASTodo(direccion1, direccion2)
A list of all ASNs directly connected to the ASN of the NAP.UIO is generated.
consulta(ipGYE, username, password)
bgpIPv4.txt && bgpIPv6.txt
listaGYE = informacionASTodo(direccion1, direccion2)
A list of all ASNs directly connected to the NAP.GYE ASN is generated.
crearArchivo(listaUIO, listaGYE)
datosASTotales.txt
obtenerArchivoLacnic()
lacnic-latest.txt
listaDatosN = comparacionASN(listaUIO, listaGYE)
2 lists are generated: one with the ASNs that are neither in NAP.UIO nor NAP.EC, another with those that are connected and with the number of total ASNs assigned to EC
listaTConteo = verificacionASN(listaDatosN)
1 list is generated with all the ASNs that belong to Ecuador
crearArchivoResumen(listaUIO, listaGYE,listaTConteo)
datosASTotalesResumen.txt
End

FIGURE 14. Flowchart of the script to obtain information from AS in EC.

[5] A script is considered scalable when it can handle large volumes of data and increase its processing capacity efficiently without compromising performance [39].

Code 3. Function to obtain LACNIC information.

```
def obtenerArchivoLacnic():
    os.system("wget␣ftp://ftp.lacnic.net
        /pub/stats/lacnic/delegated-
        lacnic-latest")
    os.system("grep␣'|EC|'␣delegated-
        lacnic-latest␣|␣grep␣'asn'␣>␣
        lacnic-latest")
    os.system("rm␣delegated-lacnic-
        latest")
```

4) **Obtaining LACNIC file:** The function *def obtenerArchivoLACNIC()* downloads the file *'delegado-lacnic-latest'* that includes information about the ASs assigned by LACNIC and filters it to include only the AS assigned to Ecuador. Code 3 presents the function to retrieve the download file from LACNIC servers.
This function downloads and filters a file from the LACNIC FTP server that contains information about the AS assigned by LACNIC. The LACNIC FTP service provides datasets on IP addresses and AS assignments for the general public. These datasets include information such as IP address blocks and AS assigned to organizations, as well as delegated AS. Delegated AS refer to the practice where organizations delegate some or all of their ASs to other organizations, such as their clients or other networks they connect to. This allows the organization that owns the AS block to manage the routing of their clients' or partners' networks instead of each one obtaining their own ASN. Delegating ASNs also enables better management and control of the routing table and allows for more efficient use of resources, such as IP addresses. Finally, this function processes the information from the *'delegado-lacnic-latest'* file using three commands: the first command uses *'wget'* to download the file from the LACNIC FTP server. The second command uses 'grep' to search for lines that contain the strings |*EC*| and 'asn' in the downloaded file and saves them in a new file called *'lacnic-latest'*.

5) **Comparing LACNIC File with AS List:** The function *def comparacionASN(listaUIO, listaGYE)* compares the AS in Quito/Guayaquil lists with the AS in the 'lacnic-latest' file, which contains information about the AS assigned by LACNIC. To obtain the ASN from the LACNIC file, the data is preprocessed, where the lines are read and split by the '|' character. The function checks if the AS is present in the *listaUIO* or *listaGYE*. If the AS is not in the *listaUIO*, it is added to the *listaDatosUIO*. If it is not in the *listaGYE*, it is added to the *listaDatosGYE*. Then, a new file named *datosASN-LACNIC.txt* is created, and the number of AS found and not found in NAP.EC-UIO/NAP.EC-GYE is written. It also keeps track of the total number of AS and the AS assigned to Ecuador but not in NAP.EC-UIO or NAP.EC-GYE.

6) **Verification of Ecuadorian AS:** Through the function *def verificacionASN(listaASND)*, which takes as input the array of three lists *listaDatosN* generated by the function *comparacionASN(listaUIO, listaGYE)*, the verification of Ecuadorian AS is performed. For each list, the function calls the *revisionWeb(asn)* function and checks each ASN to determine whether it is in use. Finally, the script prints the sum of AS in use and not in use, the total number of AS, and returns a list containing all the AS in and not in use.

7) **Generation of Final File for Ecuadorian AS:** The function *crearArchivoResumen* generates a file called *datosASTotalesResumen.txt*. The first part presents the concatenation of all the previously generated text files. It includes the AS assigned to Ecuador that are not in NAP.EC or on the Internet, and the number of AS assigned to Ecuador that are not in NAP.EC but are on the Internet. Then, it writes the count of AS assigned to Ecuador that are not in NAP.EC or on the Internet, lists all the corresponding AS list elements. Finally, it writes the count of AS assigned to Ecuador that are not in NAP.EC but are on the Internet.

Section II-D2 presents the information processing phase about IPv4 and IPv6 prefixes of all ASs connected to the NAP.EC.

2) OBTAINING INFORMATION IPv4/IPv6 PREFIXES

For this processing phase, NAP.EC uses a Python script to collect information about IPv4/IPv6 prefixes from each AS directly connected to NAP.EC. Figure 15 shows the flowchart of the implemented script. Different text files are obtained from the script with the information of all the IPv4/IPv6 prefixes used and assigned in Ecuador. The data analyst later analyzes the collected data.

Next, all the relevant processes of the Python script to obtain information on IPv4/IPv6 prefixes in the country are described.

1) **Library import:** Imports the "getpass" library, which provides a secure way of handling passwords by hiding user input from the terminal display.

2) An interactive menu is created for the user to obtain information from the neighbors of the Quito and Guayaquil NAP routers.
   - The *first* and *second* options allow obtaining information on the BGP neighbors of the Quito and Guayaquil NAP routers. These options are not explained in detail since they focus more on the analysis of RPKIs[6] from BGP.

[6] **RPKI (Resource Public Key Infrastructure):** It is a security system used in the Border Gateway Protocol (BGP) to validate the authenticity and authority of routing routes on the Internet. RPKI is based on digital certificates that verify that a BGP route advertisement comes from an authorized entity and that the advertised routes are authorized to be advertised. If an advertisement is not verified, it is considered untrusted and is rejected or treated differently [40].

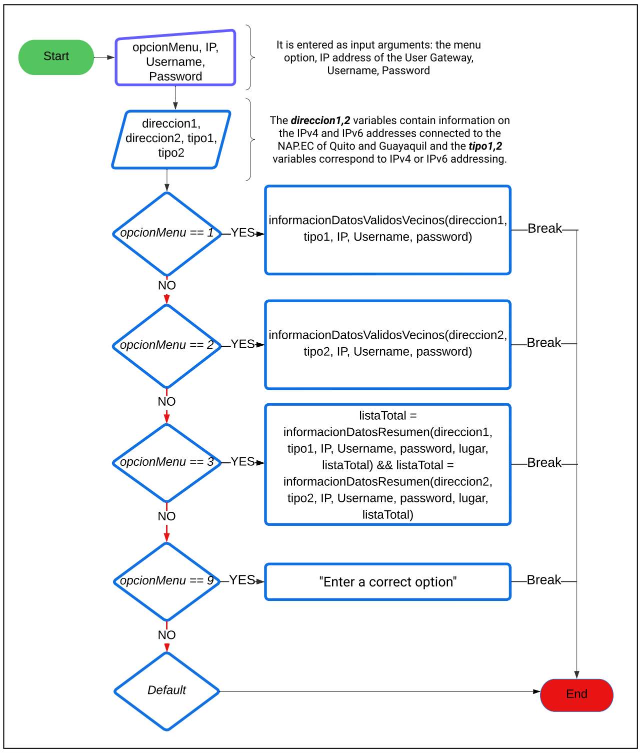

Start
opcionMenu, IP, Username, Password
It is entered as input arguments: the menu option, IP address of the User Gateway, Username, Password
direccion1, direccion2, tipo1, tipo2
The **direccion1,2** variables contain information on the IPv4 and IPv6 addresses connected to the NAP.EC of Quito and Guayaquil and the **tipo1,2** variables correspond to IPv4 or IPv6 addressing.
opcionMenu == 1
YES
informacionDatosValidosVecinos(direccion1, tipo1, IP, Username, password)
Break
NO
opcionMenu == 2
YES
informacionDatosValidosVecinos(direccion2, tipo2, IP, Username, password)
Break
NO
opcionMenu == 3
YES
listaTotal = informacionDatosResumen(direccion1, tipo1, IP, Username, password, lugar, listaTotal) && listaTotal = informacionDatosResumen(direccion2, tipo2, IP, Username, password, lugar, listaTotal)
Break
NO
opcionMenu == 9
YES
"Enter a correct option"
Break
NO
Default
End

FIGURE 15. Flowchart of the script to obtain IPv4/IPv6 prefix information in EC.

  - The code reads the text files *bgpIPv4.txt* and *bgpIPv6.txt*, which contains neighbor information from the BGP routing tables of IPv4 and IPv6 prefixes and uses the Python "os" library to execute the "sshpass" command to connect to the NAP routers using SSH.
  - Subsequently, two BGP commands (1 and 2 commands) are sent to show the routes of the specific neighbor. The output of this command is saved in a file called "response". The "response" file is opened and specific patterns are searched for, such as 'V*', 'I*', and 'N*'. These patterns indicate validation, invalidation, and unavailability of prefixes in the BGP routing table. The corresponding counters are incremented for each occurrence of these patterns.
  - Finally, the results are written to a file called *DatosVecinos.txt*.
- The *last* option allows you to obtain a general summary of the information on the routers in Quito and Guayaquil. The code uses a function called *summaryDatainformation()* to collect the necessary information and save it to a text file. This function again enters the commands 1 and 2 via SSH into the routers (Quito/Guayaquil) to obtain BGP route information. The outputs of the commands are processed, and the number of prefixes that are valid, invalid, and not found are counted, storing the results in a list. The function *GenerarResumenGeneral()* is called to generate a summary file from a list of data, which includes information from the Quito and Guayaquil routers.
  - ***GenerateGeneralSummary(listTotal):*** This function tabulates the data by ASN, grouping the number of IPv4 and IPv6 prefixes. The results are written to a tabular format file that includes the following columns: N, COMPANY, ASN, QTY. PREF. IPv4, QTY. PREF. IPv6.

This ends the information processing phase regarding Internet traffic in Ecuador by the NAP.EC research team. The data is transformed from the BGP routing tables within the NAP.EC topology, allowing us to know the number of IPv4 and IPv6 prefixes and the distribution of AS assigned and used. The data analyst follows a specific process explained below to extract and tabulate (process) all this data provided by AEPROVI.

E. INFORMATION PROCESSING BY DATA ANALYST

The need to use a script for information extraction arises when many text files need to be processed repetitively, which is tedious and time-consuming if done manually. A VBA script allows you to automate this process, allowing you not only to save time but also to reduce human errors and increase the accuracy of the result. Furthermore, once the script has been generated, it is possible to reuse it in the future, making it an effective and cost-effective solution to expedite procedures that require the processing of text files. The source codes are available in [41].

1) EXTRACTION OF IPv4/IPv6 PREFIX INFORMATION

To efficiently extract IPv4/IPv6 prefix information, a macro is created with Visual Basic to tabulate the information in an Excel table. This script aims to count the number of IPv4/IPv6 prefixes from a text file. This process is carried out for all the months in the observation period. The operation of the script is described below.

1) Create an instance of the Excel application.
2) The user selects the text file corresponding to the summary of IPv4/IPv6 prefixes according to the month of the period to be analyzed.
3) Store the column of AS and the column of IPv4/IPv6 prefixes in arrays of the selected text file.
4) Compare the AS in the text file with the AS in the Excel sheet and write the number of corresponding IPv4/IPv6 prefixes in the spreadsheet only if there is a match.
5) If there is no ASN match, create a new record and write the corresponding IPv4/IPv6 prefixes.
6) Repeat steps 1 to 5, until the information extraction process for all the months of the period is finished.

From the code presented in the Github repository, the information is organized in an Excel file called *ProcesamientoData.xlsm* that contains all the information regarding the IPv4/IPv6 prefixes from December 2017 to November 2022.

TABLE 5. Processed data about IPv4 prefixes, based on [42].

ASN	N°	September_2022	October_2022	November_2022
27814	**1**	16	16	16
263174	**2**	6	6	6
13335	**3**	2605	2650	2750
61468	**4**	86	86	86
26613	**5**	705	684	681
23487	**6**	451	452	453
263238	**7**	0	0	0
19582	**8**	0	0	0
52458	**9**	0	0	0

Table 5 presents the processing of the last three months of the period (September, October, and November 2022) and the first nine AS in the list.

Similarly, the process of extracting information about AS's effective transmission speed (throughput) is carried out.

2) EXTRACT INFORMATION ABOUT AS THROUGHPUT

A macro is created with Visual Basic to efficiently tabulate the information regarding AS's effective transmission speed (throughput), presented in an Excel file. This file contains all the information regarding AS and incoming/outgoing (average) throughput corresponding to the two routers of Quito and Guayaquil of the NAP.EC, all in separate spreadsheets for each router.

1) Create an Excel application instance, via a *FileDialog* object[7] and select an Excel file.
2) Store the AS column and the incoming/outgoing throughput columns in arrays of each spreadsheet (corresponding to the Quito and Guayaquil routers) of the selected Excel file.
3) Compare the AS of the selected Excel file with the AS in the Excel sheet (Quito/Guayaquil) and write the value corresponding to the corresponding incoming/outgoing throughput in the spreadsheet only if there is a match.
4) If there is no ASN match, create a new record and write the value corresponding to the incoming/outgoing throughput.
5) Repeat steps 1 to 5, until the information extraction process for all the months of the period is finished.

Based on this code, the information is organized in an Excel file called *ProcesamientoData.xlsm* that contains all the information regarding the capacity of the AS links directly connected to the NAP.EC. The period is from November 2017 to November 2022. Table 6 presents the processing of the last month (November 2022) and the first nine AS in the list concerning the effective transmission speed of each AS connected to the UIO NAP. The tabulated data represents the throughput of each link, measured in [Mbps].

TABLE 6. Data processed about the throughput of AS connected to the UIO NAP, based on [42].

ASN	N°	Incoming_Nov_2022	Incoming_Nov_2022
263174	1	27	136
26613	2	4998	19700
23487	3	29900	19600
263238	4	0	0
19582	5	0	0
52458	6	0	0
0	7	0	0
27740	8	136	316
19114	9	20000	6237

Once the section corresponding to the information extraction phase regarding Internet traffic in Ecuador has been presented by the data analyst, the following phases of processing and presentation of the information are presented. The data is tabulated within an Excel file; then, the information is processed and loaded into Power BI. The motivation for using Power BI lies in its ability to process large amounts of data and turn it into useful information for decision-making. Power BI allows you to explore information visually and discover patterns and trends that might go unnoticed. In addition, today, mastering data visualization tools such as Power BI is essential to compete in a market where data (transformed into information) is the most important asset for most organizations.

F. PROCESSING AND PRESENTATION OF INFORMATION

Power BI's Power Query Editor (PQE) is used for the information processing phase collected by the data analyst. PQE is a Power BI feature that allows users to connect to and extract data from multiple sources. Provides an easy-to-use interface for data modeling, cleansing, and transformation operations [44]. Once the information is loaded, we proceed with the presentation of the graphs within a dashboard in Power BI. These graphs are presented in detail in Section III.

III. RESULTS

This section presents the results obtained from processing information about AS, IPv4/IPv6 prefixes, and throughput of each AS in Ecuador from December 2017 to November 2022 (observation period). In turn, an analysis is carried out before, during, and after the pandemic caused by COVID-19. All the information presented is based on empirical and statistical data provided by AEPROVI [42].

A. ANALYSIS OF AUTONOMOUS SYSTEMS IN ECUADOR

Figure 16 presents Ecuador's autonomous systems evolution in the observation period.

The increase in AS within the NAP.EC IXP denotes a growing number of ISPs and AS interconnecting in the IXP. This interconnection allows Internet traffic to be efficiently distributed and delivered directly between ISPs instead of going down a longer and more expensive route through transit providers as more AS are connected to the NAP.EC IXP, there is an increase in traffic volume because more devices and networks are interconnected. In addition, direct interconnection also improves QoS for end users because

[7] The **FileDialog** object in Excel is a tool that allows users to select a file or folder on their system local files, using a standard dialog window provided by the operating system. This is especially useful when the user must select a specific file to perform a task in a macro or plugin [43].

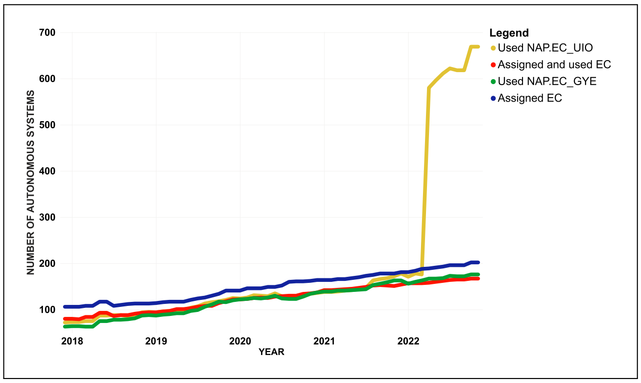


FIGURE 16. Evolution of the number of AS in Ecuador, based on [42].

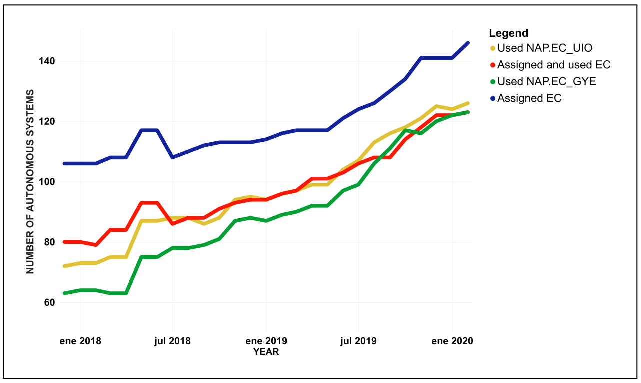


FIGURE 17. Evolution of number of AS in Ecuador before COVID-19, based on [42].

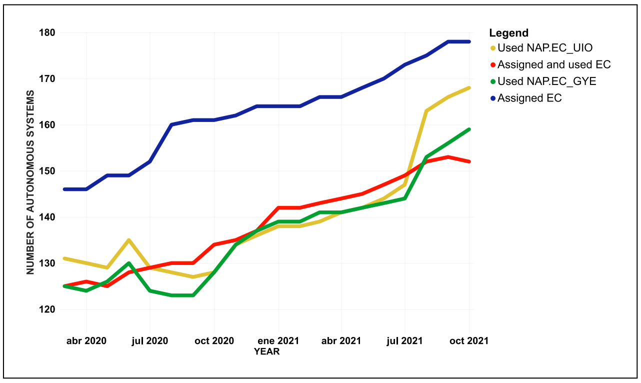


FIGURE 18. Evolution of the number of AS in Ecuador during COVID-19, based on [42].

traffic is delivered quickly and with lower latency. The evolution of AS growth in Ecuador before, during, and after the pandemic caused by COVID-19 is presented below.

Analysis before COVID-19: Fig. 17 presents the evolution of the number of AS in Ecuador before the pandemic. The observation period is considered from December 2017 to February 2020.

Analysis during COVID-19: Fig. 18 presents the evolution of the number of AS in Ecuador during the pandemic. The observation period is considered from March 2020 to October 2021.

Analysis after COVID-19: Fig. 19 presents the evolution of the number of AS in Ecuador after the pandemic. The observation period is considered from November 2021 to February 2022.

The Equation 1 represents the net growth rate formula[8] which allows quantitative knowledge of the growth in the number of AS in Ecuador during each pandemic period.

$$\frac{V_f - V_i}{V_f} \times 100\%, \tag{1}$$

where:

- V_i: Represents the number of AS in an initial period.
- V_f: Represents the number of AS in a final period.
- $(V_f - V_i)$: Represents the absolute change in the number of AS during the considered period.
- $\frac{V_f - V_i}{V_f}$: It is the relation between the absolute change in the number of AS and the number of AS at the end of the period. Multiplied by 100, it represents the net growth rate of AS in Ecuador during the period considered.

Table 7 summarizes the evolution of the number of AS used. The evolution of AS assigned and used in Ecuador during the pandemic increased 36.25%. After the pandemic, it increased 42.50% in both situations compared to before the pandemic in the country. The 36.25% increase in AS assigned and used in Ecuador during the pandemic is justified by the need for a robust digital infrastructure (solid and reliable network infrastructure) to meet the needs of a large number of people who work and study from home as a consequence of the prevention measures presented by the National COE. In particular, online video conferencing and collaboration platforms such as Microsoft Teams and Zoom significantly impacted Internet traffic during the pandemic. As a result, many ISPs have invested in expanding their infrastructure and improving QoS to meet the growing demand.

In addition, the presence of more AS in the NAP.EC IXP is also an indicator of the maturity of the Internet market in Ecuador because there are more active ISPs and AS in the country. During the pandemic, the growth of AS in the NAP.EC was 58.33% compared to the situation in the country before the pandemic.

Within the observation period, Table 7 presents a **specific event**, which is the increase of 754.17% in the number of AS used in the NAP.EC of Quito, compared to the situation in the country before the pandemic. This was largely due to the presence of Cloudflare's CDN in Ecuador, enabling more CDNs through the peering channel on the NAP.EC, Cloudflare enabled more efficient distribution of content across the network. This led to an increase in the number of AS used in the IXP by all directly connected AS in the NAP.EC. Cloudflare's CDN offers a wide range of services, including intelligent traffic routing, content optimization, protection against DDoS attacks, and delivery of static and

[8] It is a measure used to calculate the change in a variable in a given period, considering both growth and decrease. It is commonly used in finance, business, and economics to measure the growth of a company, an industry, or an economy, in general, [45].

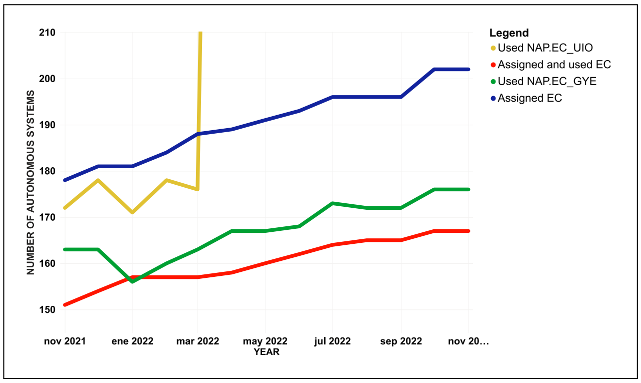


FIGURE 19. Evolution of number of AS in Ecuador after COVID-19, based on [42].

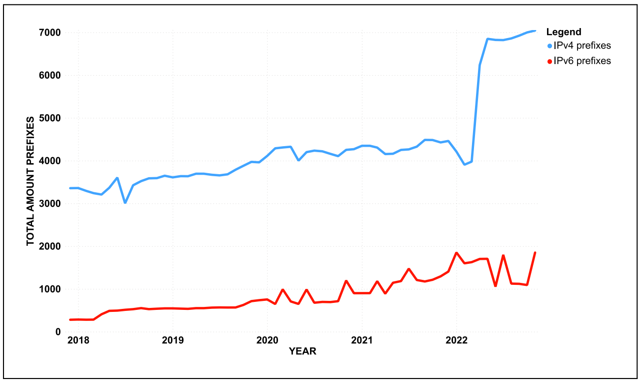


FIGURE 20. Evolution of number of IPv4/IPv6 prefixes in Ecuador, based on [42].

dynamic content through its network of servers distributed worldwide. The growing demand for these services from ISPs and other players in the telecommunications market is another crucial factor contributing to the increase in ASs used in NAP.EC [46].

B. ANALYSIS OF IPv4/IPv6 PREFIXES IN ECUADOR

Figure 20 presents the evolution of the number of IPv4 and IPv6 prefixes in Ecuador. There were a total of 31 AS directly connected to the NAP.EC during the observation period from December 2017 to November 2022.

A growing trend is observed in the number of IPv4 and IPv6 prefixes. This growth is due to more networks being added and more devices being connected to the Internet because each device uses/requires a unique IP address to connect to the Internet. This increases the number of prefixes needed to identify each of them. The growing demand for online services, such as teleworking, virtual education, and social interaction, causes this increase in devices connected to the Internet. This, in turn, generates an increase in the data traffic that circulates through the network. The growing demand for online services not only increases the number of devices connected to the Internet but also leads to the creation of new applications and services that require the creation of new networks and the assignment of new IP addresses. All of this, in turn, increases the number of prefixes required to identify and route the traffic generated by these devices and services.

The growth in IPv6 arises due to the following factors:

1) Scarcity of IPv4 prefixes compels both IXP and ISP to utilize this protocol in devices and end clients.
2) Decisions by CDNs to deliver their content through IPv6 addressing.

The Cloudflare CDN has witnessed an escalation in IPv4/IPv6 addressing as they provide end users with more networks and devices to access their content, including secure traffic (HTTPS).

The growth of the digital economy in Ecuador is an example of how the growing demand for online services generates new applications and services. This growth increases the number of companies and organizations that use the Internet to offer services and products, which demands creating new networks and assigning new IP addresses. Consequently, the number of prefixes needed to identify and route the traffic generated by these devices and services increases [47].

Table 8 presents the net growth rate of the current distribution of IPv4 and IPv6 addresses assigned and used in Ecuador.

During the pandemic, the number of IPv4 prefixes used and assigned increased 25.38% and after the pandemic, they increased 47.89% both compared to the situation before the pandemic. One of the factors for the growth of IPv4 prefixes is the greater demand for IP addresses in Ecuador due to the increase in the number of devices connected to the Internet and the greater use of online services. As more devices require Internet access, more IP addresses are needed. This drives the growth of IPv4 prefixes. IPv6 prefixes during the pandemic increased 69.63%, and after the pandemic, they increased 138.31% in both situations compared with the situation before the pandemic. The growth of IPv6 prefixes results from awareness about the importance of this technology, which allows for increasing the number of available IP addresses. ISPs and enterprises must adopt IPv6 as a long-term solution to address the shortage of IPv4 addresses.

1) EVOLUTION IN PANDEMIC OF IPv4/IPv6 PREFIXES

At each stage of the pandemic, an analysis is carried out from the point of view of three ISPs with AS: 26613, 19169, and 23487 and a CDN: 13335 (Cloudfare) connected to the NAP.EC IXP. The four selected AS represent a representative sample of ISPs and CDNs in Ecuador. These four AS (*i.e.*, the 12.90% of participants within the NAP.EC) generated approximately 62.37% of the total Internet traffic in Ecuador (these are empirical and statistical data from the NAP.EC). The CDN is included because it is essential in storing and distributing web content worldwide. Figure 21 and Table 9 present the net growth rate of the four representatives AS concerning the distribution of IPv4 prefixes before, during, and after the pandemic.

TABLE 7. Net growth rate number of AS in Ecuador, based on [42].

FEATURE	CORONAVIRUS COVID-19 PANDEMIC			
	BEFORE	DURING	AFTER	POINT EVENT
NAP.EC QUITO	75,000%	133,333%	144,444%	829,167%
NAP.EC GUAYAQUIL	95,238%	152,381%	158,730%	179,365%
NAP ECUADOR	83,333%	141,667%	144,444%	829,167%
USED ECUADOR	53,750%	90,000%	96,250%	108,750%

TABLE 8. Net growth rate of number of IPv4/IPv6 prefixes in Ecuador, based on [42].

FEATURE	CORONAVIRUS COVID-19 PANDEMIC		
	BEFORE	DURING	AFTER
IPv4 PREFIXES	28,041%	53,424%	75,927%
IPv6 PREFIXES	49,686%	119,318%	187,996%

Figure 22 and Table 10 present the net growth rate of the four representatives AS concerning the distribution of IPv6 prefixes before, during, and after the pandemic.

ASN 19169 has an increase of 102.35% in the number of IPv4 prefixes and an increase of 64.62% in the number of IPv6 prefixes used and assigned during the pandemic compared to the previous situation. In general, each AS has an increase of at least 70%. The pandemic has exposed the growing reliance on digital networks for business continuity, employment, education, healthcare, and other essential services. As a result, ISPs have been forced to increase user capacities within their networks to quickly handle unexpected traffic spikes and scale their systems during attacks or high-demand events.

C. THROUGHPUT ANALYSIS OF AUTONOMOUS SYSTEMS IN ECUADOR

Figure 23 and Fig. 24 present the average throughput of the AS of the NAP.EC corresponds to the cities of Quito and Guayaquil, based on the information generated by the 31 AS, directly connected in the NAP.EC during the observation period from December 2017 to November 2022.

For the router located in Quito NAP, there is a growth of approximately 212% in throughput (incoming and outgoing) within each router's serial interface during the observation period. This is because, in recent years, there has been greater adoption of online technologies, such as video and music streaming services, instant messaging applications, and social networks. These online services generated a large percentage of Internet traffic growth and contributed to increased data input and output on the router's serial interfaces.

Similarly, for the router located in Guayaquil NAP, a growth of approximately 91% in throughput (incoming and outgoing) is observed within each router's serial interface during the entire observation period. It is observed that the amount of data transmission rate (average) of the NAP of Guayaquil, compared to the information of the NAP of Quito, is lower. This is because, according to the NAP, more AS are directly connected in Quito NAP.EC topology (see Fig. 10) generates more Internet traffic within each serial interface of the Quito NAP router. Table 11 presents the throughput growth in the two NAP.EC routers.

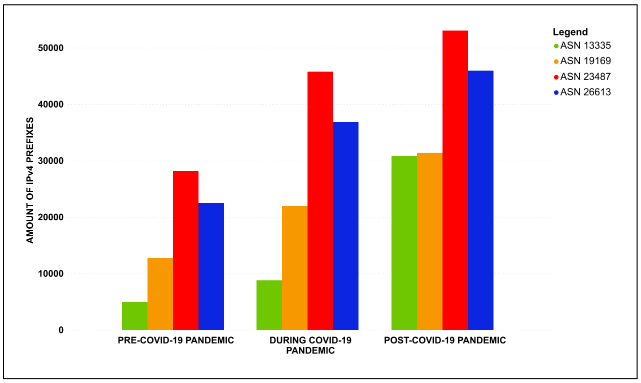


FIGURE 21. Evolution of the number of IPv4 prefixes of the most representative AS, based on [42].

TABLE 9. Net growth rate number of IPv4 prefixes of most representative AS, based on [42].

ASN	CORONAVIRUS COVID-19 PANDEMIC		
	BEFORE	DURING	AFTER
13335	15.76%	125.45%	1792.12%
19169	43.24%	145.59%	450.59%
23487	3.05%	72.76%	115.90%
26613	14.33%	111.91%	208.51%

During the pandemic, the average input throughput increased 75.35% and 49.25% in the NAPs of Guayaquil and Quito, respectively, both situations compared to the situation before the pandemic. This situation originated due to increased connected devices such as mobile phones, tablets, laptops, and IoT devices (Internet-connected devices). This contributes to the increase in the average data input and output throughput on the router interfaces. Also, during the pandemic, many companies and schools were forced to adopt telecommuting and telematics education to allow employees and students to work and study from home. The increased demand for bandwidth created a challenge for ISPs, who had to scale/change their link capacities to provide higher data throughput and improve QoS for the end user.

1) EVOLUTION IN AS THROUGHPUT PANDEMIC

As in Section III-B1, at each stage of the pandemic, an analysis is carried out from the point of view of three ISPs with AS: 26613, 19169, and 23487 and a CDN: 3549 (Centurylink) connected to the NAP IXP both to the NAP of Quito and the NAP of Guayaquil. Figure 25 and Fig. 27

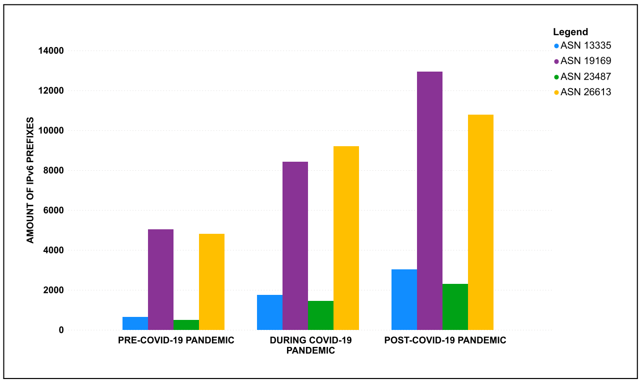


FIGURE 22. Evolution of the number of IPv6 prefixes of the most representative ASs, based on [42].

TABLE 10. Net growth rate number of IPv6 prefixes of most representative AS, based on [42].

ASN	CORONAVIRUS COVID-19 PANDEMIC		
	BEFORE	DURING	AFTER
13335	57.78%	105.56%	232.22%
19169	9.23%	73.85%	166.15%
23487	50.83%	102.50%	155.83%
26613	6.12%	19.69%	33.26%

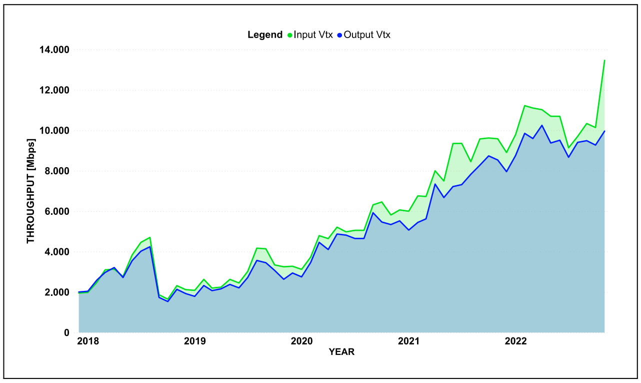


FIGURE 23. Throughput evolution of NAP.UIO, based on [42].

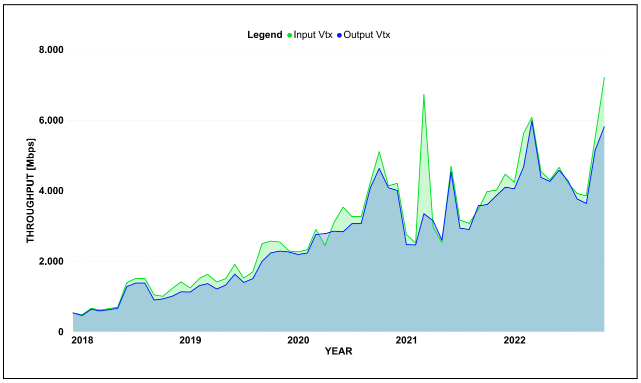


FIGURE 24. Throughput evolution of NAP.GYE, based on [42].

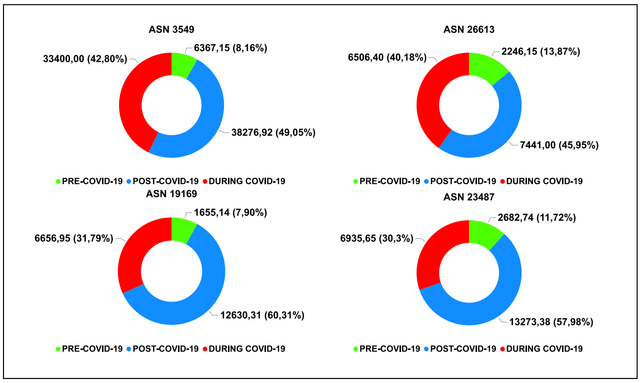


FIGURE 25. Evolution of input throughput in Quito NAP, based on [42].

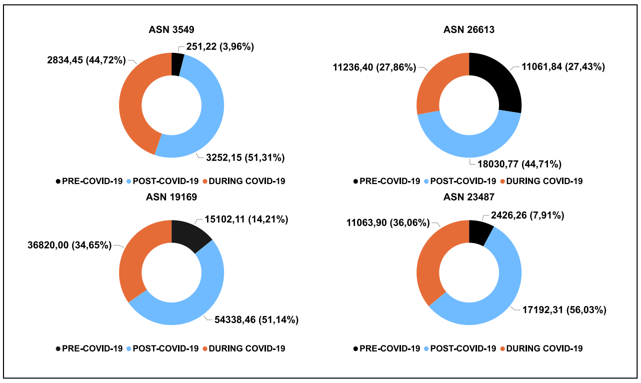


FIGURE 26. Evolution of output throughput in Quito NAP, based on [42].

present the net growth rate of the four representatives AS concerning input throughput (measured in [Mbps]) during the entire pandemic stage on the two routers of the NAP of Quito and Guayaquil.

For the router located in Quito NAP during the pandemic, the average input throughput increased 424.51%, 189.69%, 302.40% and 158.53% for the AS: 3549, 26613, 19169 and 23487 respectively, all measurements compared to the situation before the pandemic. For the router located in Guayaquil NAP, during the pandemic, the average input throughput increased 357.59%, 192.69%, 112.68% and 185.96% for the AS: 3549, 26613, 19169 and 23487, respectively. All measurements compared to the situation before the pandemic.

The results obtained in this study demonstrate an increase in Internet traffic during the COVID-19 pandemic in all the metrics considered: number of AS, number of IPv4 and IPv6 prefixes, and effective transmission speed. This increase in traffic is attributed to various factors, such as the increase in telecommuting and online education, as well as increased demand for online entertainment and services due to lockdowns and mobility restrictions. These results are of great importance to understanding the behavior of the Internet during an exceptional situation such as the COVID-19 pandemic and to plan future traffic management and network infrastructure strategies. In addition, these results may also impact the Telecommunications industry and ISPs, who could use them to improve the quality and capacity of their services at times of high demand.

TABLE 11. Net growth rate throughput routers NAP.EC Quito/Guayaquil, based on [42].

ROUTER	CORONAVIRUS COVID-19 PANDEMIC					
	BEFORE		DURING		AFTER	
	TRAFFIC INPUT	TRAFFIC OUTPUT	TRAFFIC INPUT	TRAFFIC OUTPUT	TRAFFIC INPUT	TRAFFIC OUTPUT
NAP.EC GYE	34,067%	31,786%	109,423%	99,301%	246,143%	208,215%
NAP.EC UIO	9,109%	7,282%	58,364%	50,834%	127,278%	100,493%

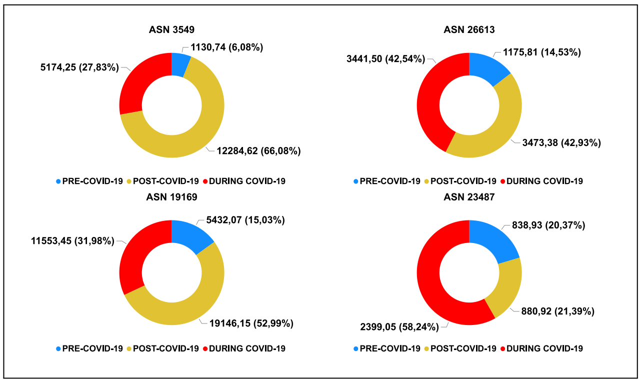


FIGURE 27. Evolution of input throughput in Guayaquil NAP, based on [42].

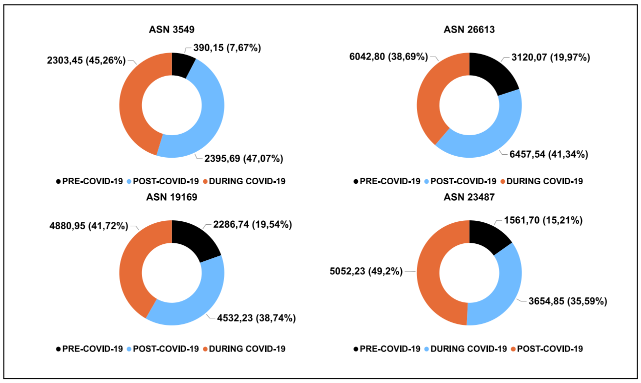


FIGURE 28. Evolution of output throughput in Guayaquil NAP, based on [42].

IV. CONCLUSION

The measurement of Internet traffic growth in Ecuador can be approached from different perspectives. This study obtained empirical data (data obtained through direct observation/experience, which can be objectively measured and verified) through the BGP tables of all routers in the NAP.EC was used to analyze the increase in traffic from the Internet from the perspective of an IXP. Factors such as the growth in the number of AS, the distribution of IPv4/IPv6 prefixes used and assigned in Ecuador, and the throughput of each link of the AS connected to the NAP were considered. This approach allowed for obtaining a more precise and detailed view of traffic behavior in the country and facilitating the identification of patterns and trends in traffic growth at the local level.

With an increased number of interconnected autonomous systems within the NAP.EC exchange point, there is a rise in the volume of traffic flowing through this infrastructure. Consequently, there is a greater generation of local traffic (traffic originating and terminating in Ecuador).

The pandemic significantly impacted the way people work and interact around the world. Daily life has continued normally for almost a year since its inception, thanks to increased digitization and Internet use. The Internet was critical in supporting online education, work, and entertainment. This evidenced the importance of Internet communications and services in modern life. The 93.16% increase in Internet traffic in Ecuador (from the point of view of the growth of IPv4/IPv6 prefixes) after the pandemic reflected the importance of access to digital technology in today's society. Likewise, the pandemic has highlighted the need to strengthen the Internet infrastructure to meet the population's growing demands. In this sense, traffic engineering is presented as a fundamental tool to improve the capacity and efficiency of networks, thus guaranteeing stable and quality connectivity at all times.

The unplanned growth of the Internet in Ecuador during the pandemic presented challenges and opportunities for the country's development, including the need to improve connectivity in rural areas, investment in infrastructure, and training of the population in using and using ICTs. ISPs and CDNs contributed to the growth of Internet traffic in Ecuador by connecting within the IXP. Thus, CDNs play an essential role in improving QoS and end-user experience. Storing content on servers close to the end user reduces latency and network congestion. This improves the upload speed (transmission from a device to the Internet) and reduces the waiting time for accessing online resources. In addition, using CDNs also lowers data transmission costs, benefiting both end users and ISPs.

The Internet has become part of people's daily lives, making everyday life easier, faster, and more straightforward, providing access to a large amount of information, and contributing to the country's personal, social, and economic development. For this reason, each ISP needs to strengthen its network infrastructure through the investment of high-quality hardware and software, such as routers and switches, to improve the capacity and efficiency of its network and the deployment of new technologies, such as fiber optics, to improve the speed and reliability of the Internet connection.

As authors, we recommend that future work focus on the development of tools that can eliminate this effect such that ISPs in Ecuador and Internet Regulation Agencies must collaborate to keep the following information up-to-date and publicly accessible:

- Number of IPv4/IPv6 prefixes generated by their ASNs.
- Number of IPv4/IPv6 prefixes generated by clients from other ASNs.
- The regulatory agency should have a mapped overview of the IPv4/IPv6 throughput circulating within the various ASNs nationwide.
- Develop collaborative tools (e.g., Hurricane Electric, Lacnic-Latest, script generation for processing ASN-related data) between ISPs and Regulatory Agencies to facilitate easy collection of the information mentioned above.
- Utilize AEPROVI (administrators of Ecuador's Internet traffic exchange point) named NAP.EC to inquire about all traffic originating/terminating within Ecuador.

Regarding data processing, it is essential to look for information about local traffic rather than global traffic to ensure that the definitions and the way of measuring traffic are relevant to the context in which you work. The filtering and scope of the search for information from publications/bibliography about how to measure Internet traffic varies according to the study objectives. Opting for open-source tools for the data loading and presentation phase, such as Tableau, Apache Superset, or Metabase, is suggested. This is because using tools with paid licenses, such as Power BI, can limit the ability to share reports and dashboards with the general public freely.

V. ANNEX I

A. ROUTING POLICIES - NAP.EC

1) The routing protocol used is Border Gateway Protocol 4, BGP-4 (RFC 4271, 4760 and their respective updates).
2) A single BGP session per connection to a route server.
3) Connections with autonomous system numbers (ASN) for private use (RFC 1930, 6996, 7300) or for documentation (RFC 5398) are not accepted.
4) The ASPATH of the prefixes must not contain ASNs for private or documentation use. The maximum length allowed for the ASPATH is 10 ASNs.
5) Default routes and special use IPv4 and IPv6 address ranges are discarded (private, documentation, experimental or research use networks, ranges reserved by IANA, RFC 1918, RFC 4193, RFC 5735, RFC 5737, RFC 6598, RFC 6890).
6) IPv4 prefixes with masks between 12 and 24 bits are accepted.
7) IPv6 prefixes with masks between 29 and 48 bits are accepted.
8) eBGP multi-hop is not allowed.
9) Providers must advertise the same prefixes over all their connections to NAP.EC.
10) A maximum number is handled for the number of prefixes received from the participants.
11) Suppose the participant wishes to configure a maximum for the number of prefixes received from NAP.EC should consult and coordinate the appropriate value with the NAP.EC administration.
12) All received prefixes are assigned a zero value for the MED attribute.
13) Prefixes in RPKI state "invalid" are discarded. When a participant is informed of the presence of this scenario with some prefix, it must stop announcing it or fix the error immediately if the IP resource is under the administration of another organization (partner or client), the NAP.EC participant that announces said prefix must forward the communication to the appropriate technical contacts and carry out the respective follow-up until the routing problem is resolved. If the participant does not solve the problem promptly or the problems are repeated, the connection will be terminated until the problem is resolved.
14) Received prefixes are assigned a local preference of: 100 in case of 'valid' RPKI origin and 50 in case of 'not-found' RPKI origin. 'All' prefixes are advertised from NAP.EC with community "no-export".
15) In NAP.EC neither applications nor "valid public" prefixes are filtered, this must also be fulfilled on the participant side.

REFERENCES

[1] D. I. J. Joskowicz, "A brief history of telecommunications," Inst. Elect. Eng. Republic Uruguay, Version 12, Feb. 2016, pp. 43–46.

[2] E. Comercio. (2021). *The Internet in Ecuador: A Brief Historical Review*. El Comercio. Accessed: Nov. 15, 2022. [Online]. Available: https://www.elcomercio.com/tendencias/internet-ecuador-resea-historica.html

[3] AEPROVI. *Presentation and History—AEPROVI*. Accessed: Nov. 15, 2022. [Online]. Available: https://aeprovi.org.ec/index.php/en/napec/presentation

[4] R. Líderes. (2020). *Growth of Internet Traffic in Ecuador Skyrockets Due to COVID-19*. Revista Líderes. Accessed: Nov. 15, 2022. [Online]. Available: https://www.revistalideres.ec/lideres/crecimiento-trafico-internet-ecuador-covid.html

[5] ARCOTEL. *Internet, Statistical Bulletin of the Telecommunications Sector*. Accessed: Nov. 15, 2022. [Online]. Available: https://www.arcotel.gob.ec/internet-boletin-estadistico-del-sector-de-telecomunicaciones/

[6] (2020). *Coronavirus Disease (COVID-19) Definition*. [Online]. Available: https://www.who.int/europe/emergencies/situations/covid-19

[7] S. Ogonaga and S. Chiriboga, "COVID-19 in ecuador: Descriptive analysis of the most affected provinces and cities," *GICOS, J. Community Health Res. Group*, vol. 5, no. 2, pp. 67–82, 2020.

[8] ARCOTEL. (2022). *Internet Access Service Accounts and Users*. [Online]. Available: https://www.arcotel.gob.ec/internet-boletin-estadistico-del-sector-de-telecomunicaciones/

[9] Cloudflare. (2023). *What is the Internet Protocol?* Accessed: Aug. 28, 2023. [Online]. Available: https://www.cloudflare.com/learning/network-layer/internet-protocol/

[10] N. Brownlee and C. Loosley, "Fundamentals of internet measurement: A tutorial," *CMG J. Comput. Resource Manag.*, vol. 102, pp. 203–217, Jan. 2001.

[11] Mariela Rocha. *Border Gateway Protocol*. Accessed: Nov. 15, 2022. [Online]. Available: https://www.lacnic.net/innovaportal/file/3139/1/bgp-rosario-lacnic30.pdf

[12] P. Ayabaca and H. Iván, "Autonomous systems for internet service providers," B.S. thesis, DETRI, Escuela Politécnica Nacional, Nov. 2001. Accessed: Nov. 15, 2022.

[13] C. M. Arkko J. and L. Vegoda, "IPv4 address blocks reserved for documentation," Internet Requests Comments, RFC Editor, USC Inf. Sci. Inst., Marina del Rey, California, RFC 5737, Jan. 2010. [Online]. Available: https://www.rfc-editor.org/rfc/rfc5737.html

[14] G. Huston. (Jan. 2010). *Autonomous System (AS) Number Reservation for Documentation Use*. [Online]. Available: https://www.rfc-editor.org/rfc/rfc5737.html

[15] J. Rexford, Z. Wang, and X. Xiao, "The borders of the border gateway protocol," in *Proc. ACM SIGCOMM Conf.*, 1996, pp. 231–242.

[16] Y. Rekhter and T. Li. (2006). *A Border Gateway Protocol 4 (BGP-4)*. Internet Engineering Task Force (IETF). [Online]. Available: https://tools.ietf.org/html/rfc4271

[17] M. Foster, "The differences between transit and transport providers," *Global Telecoms Bus.*, vol. 12, no. 5, pp. 32–33, 2012. [Online]. Available: https://www.globaltelecomsbusiness.com/article/b1f5tg63v4zvnw/the-differences-between-transit-and-transport-providers

[18] J. Padilla, "Analysis of internet traffic behavior during the COVID-19 pandemic: The case of Colombia," *Entre Ciencia e Ingenieria*, vol. 14, no. 28, pp. 26–33, 2020.

[19] B. Rasciute. (Sep. 19, 2022). *What is Internet Exchange Point? A Beginners Guide to IXP*. [Online]. Available: https://www.ipxo.com/blog/internet-exchange-point-duplicate/

[20] G. Peng, "CDN: Content distribution network," 2004, *arXiv:cs/0411069*.

[21] H. Huici and R. Iglesias. (2020). *Inter-Connected: Study on Points of Internet Exchange (IXP) and Its Advantages Using Three Latin American Case Studies*. [Online]. Available: https://descargas.lacnic.net/lideres/hector-huici/hector-huici-informe.pdf

[22] R. Echeberría, "Internet infrastructure in Latin America: Traffic exchange points, content distribution networks, submarine cables, and data centers," Subregional Headquarters of ECLAC in Mexico, Corporate MCS, Blv. Miguel de Cervantes Saavedra, Mexico, 2020. Accessed: Nov. 15, 2022. [Online]. Available: https://repositorio.cepal.org/items/3eac272f-f3dc-47e8-b583-5f52ef9ce001

[23] C. Docs. *(S/F) Cloudflare CDN Reference Architecture*. Accessed: Nov. 15, 2022. [Online]. Available: https://developers.cloudflare.com/reference-architecture/cdn-reference-architecture/

[24] E. Balestrieri, F. Picariello, S. Rapuano, and I. Tudosa, "Review on jitter terminology and definitions," *Measurement*, vol. 145, pp. 264–273, Oct. 2019.

[25] V. Ramasubramanian, D. Malkhi, F. Kuhn, M. Balakrishnan, A. Gupta, and A. Akella, "On the treeness of Internet latency and bandwidth," in *Proc. 11th Int. Joint Conf. Meas. Model. Comput. Syst.*, Jun. 2009, pp. 61–72.

[26] IETF. (2021). *About the IETF*. [Online]. Available: https://www.ietf.org/about/

[27] LACNINC. *About LACNIC*. Accessed: Nov. 15, 2022. [Online]. Available: https://www.lacnic.net/1004/2/lacnic/about-lacnic

[28] AEPROVI. *About US—Aeprovi*. Accessed: Nov. 15, 2022. [Online]. Available: https://aeprovi.org.ec/index.php/es/quienes-somos

[29] M. Chiesa, R. di Lallo, G. Lospoto, H. Mostafaei, M. Rimondini, and G. Di Battista, "Prixp: Preserving the privacy of routing policies at internet exchange points," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM)*, 2017, pp. 435–441.

[30] AEPROVI. *Topology*. Accessed: Nov. 15, 2022. [Online]. Available: https://aeprovi.org.ec/index.php/es/napec/topologia

[31] AEPROVI. *Routing Policies*. Accessed: Nov. 15, 2022. [Online]. Available: https://aeprovi.org.ec/index.php/es/napec/politicas-enrutamiento

[32] AEPROVI. *Traffic Exchange Policies (Peering Policies)*. Accessed: Nov. 15, 2022. [Online]. Available: https://aeprovi.org.ec/index.php/es/napec/politicas-peering

[33] Object Mnagement Group. *Charter: Current BPMN Specification*. Accessed: Nov. 15, 2022. [Online]. Available: https://www.bpmn.org/

[34] Cisco Systems. (2022). *Cisco IOS IP Routing: BGP Command Reference*. Cisco Press. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios/iproute_bgp/command/reference/irg_book/irg_bgp5.html

[35] (2020). *What is Administrative Distance*. [Online]. Available: https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/15986-admin-distance.html

[36] J. Deng, F. Cuadrado, G. Tyson, and S. Uhlig, "Behind the game: Exploring the twitch streaming platform," in *Proc. Int. Workshop Netw. Syst. Support Games (NetGames)*, 2015, pp. 1–6.

[37] Hurricane Electric Internet Services. *About Hurricane Electric*. Accessed: Nov. 15, 2022. [Online]. Available: https://www.he.net/about_us.html

[38] T. Xing, P. Li, S. Zhang, and W. Shang, "Internet resource allocation: Who gets what and why," *Proc. Comput. Sci.*, vol. 130, pp. 563–568, 2018. Accessed: Nov. 15, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S187705091731181X

[39] G. Antoniou, "Scalable computing: Practice and experience," *Scalable Comput., Pract. Exper.*, vol. 17, no. 3, pp. 219–220, 2016.

[40] C. De Launois, L. Andersson, R. Austein, G. Huston, M. Lepinski, and S. Weiler, "An infrastructure to support secure internet routing. request for comments," BBN Technol., Cambridge, MA, USA, 2012. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6480.html

[41] D. Ponce and C. Tipantuña. (Feb. 2023). *Analysis of Internet Traffic in Ecuador Repository*. [Online]. Available: https://github.com/davidjponce/Analisis_Trafico_Internet_EC

[42] C. Espinosa, "BGP tables of nap.ec: ASN, prefixes, and throughput," Asociación de Empresas Proveedoras de Servicios de Internet, Valor Agregado, Portadores y Tecnologías de la Información (AEPROVI), Quito, Ecuador, Nov. 2022.

[43] Microsoft. (2021). *FileDialog Object (Excel)*. Microsoft Corporation. Accessed: Feb. 19, 2023. [Online]. Available: https://docs.microsoft.com/en-us/office/vba/api/excel.filedialog

[44] Microsoft. (2022). *Power Query Editor Documentation*. [Online]. Available: https://learn.microsoft.com/en-us/power-query/power-query-what-is-power-query

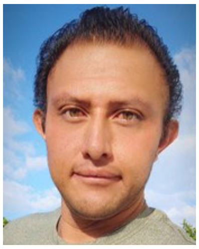
[45] E. F. Brigham and J. F. Houston, *Fundamentals of Financial Management*, 14th ed. Mason, OH, USA: South-Western Cengage Learning, 2015.

[46] A. McDonald, M. Bernhard, L. Valenta, B. VanderSloot, W. Scott, N. Sullivan, J. A. Halderman, and R. Ensafi, "403 forbidden: A global view of CDN geoblocking," in *Proc. Internet Meas. Conf.*, 2018, pp. 218–230.

[47] G. Atzeni and O. Carboni, "Digital economy and productivity growth," *Econ. Innov. New Technol.*, vol. 26, nos. 1–2, pp. 22–37, 2017.

DAVID PONCE received the degree in information technology engineering from Escuela Politécnica Nacional, in March 2023, where he is currently pursuing the master's degree in systems information and data science. He primarily focuses on information analysis and process automation, utilizing business intelligence tools to optimize business processes and generate actionable insights. He has developed skills in data manipulation and visualization to create accurate and meaningful reports. With a passion for technology and a desire to contribute to the field of information and data science, he aims to drive innovation and progress in the industry.

CHRISTIAN TIPANTUÑA received the bachelor's degree in telecommunications engineering from Escuela Politécnica Nacional, Ecuador, in 2011, the M.Sc. degree in wireless systems and related technologies from Politecnico di Torino, Turin, Italy, in 2013, and the Ph.D. degree in network engineering from Universitat Politécnica de Catalunya, Barcelona, Spain, in 2022. He is currently a member of the Grupo de investigación en Redes Inalámbricas, Escuela Politécnica Nacional. His current research interests include UAV-enabled communications, wireless networks, software-defined radio (SDR), optical networks, and machine learning applied to communications systems and networks.



CRISTIAN ESPINOSA received the engineering degree in electronics and information networks from the National Polytechnic School, in 2015. He has published several scientific articles in high-impact journals about 6LoWPAN networks and the IEEE 802.15.4 protocol. Since 2015, he has been with the company AEPROVI, which manages the critical Internet backbone infrastructure of the National Internet traffic exchange point of Ecuador called NAP.EC. For more than eight years, he has been a CISCO-certified instructor and holds various certifications from CISCO, JUNIPER, and HUAWEI.