PCH
Packet Clearing House

2024 ANNUAL REPORT

Packet Clearing House

1004A O Reilly Avenue
The Presidio of San Francisco
San Francisco CA 24129-2600
USA
+1 415 831 3100 main voice
+1 415 831 3101 fax

www.pch.net

CONTENTS

Message from the Board of Directors

Bill Woodcock
Secretary General, PCH

- **Steve Feldman**
  Chairman of the Board
- **Sylvie La Perriere**
  Director
- **Mark Tinka**
  Director
- **Greg Akers**
  Director
- **Bill Woodcock**
  Secretary General

In **2024**,
Packet Clearing House
celebrated
thirty years of service
as **“the Internet’s fire department,”**
ensuring the **security** and
operational support of the
world’s **critical communications infrastructure**,
including Internet exchange
points and the core of the
Domain Name System.

With the invaluable support of dozens of governments and hundreds of private-sector donors, PCH continues to provide its services at no cost to beneficiaries, in accordance with its public-benefit not-for-profit mission.

In this year’s report, we emphasize PCH’s 2024 accomplishments as well as revisiting thirty years of history. We focus on the three outward-facing pillars of PCH’s mission: strengthening the security and stability of the Internet infrastructure; enhancing the efficiency and sustainable growth of the Internet economy; and supporting the resilience and continuous development of the information society.

It would be impossible to fully convey the depth of our gratitude to all of PCH’s treaty signatory nations, our donors, partners, and volunteers for their support and their commitment to an Internet that is reliable and accessible to all. We look forward to continuing to strengthen the Internet’s key infrastructures, economy, and community with their ongoing help.

Mission and Founding Principles

PCH exists to safeguard and improve the world's critical communications infrastructure. These aspects are fundamental:

- A funding model based principally upon in-kind donations (e.g., power, fiber, servers) from both governments and the private sector.
- Focused advocacy, including the world's first anti-spam legislation and regulatory protections for resources such as the .org domain.

PCH's role as "**the fire department for the Internet**" highlights its role in providing essential services without commercializing them, ensuring societal benefit and robust infrastructure.

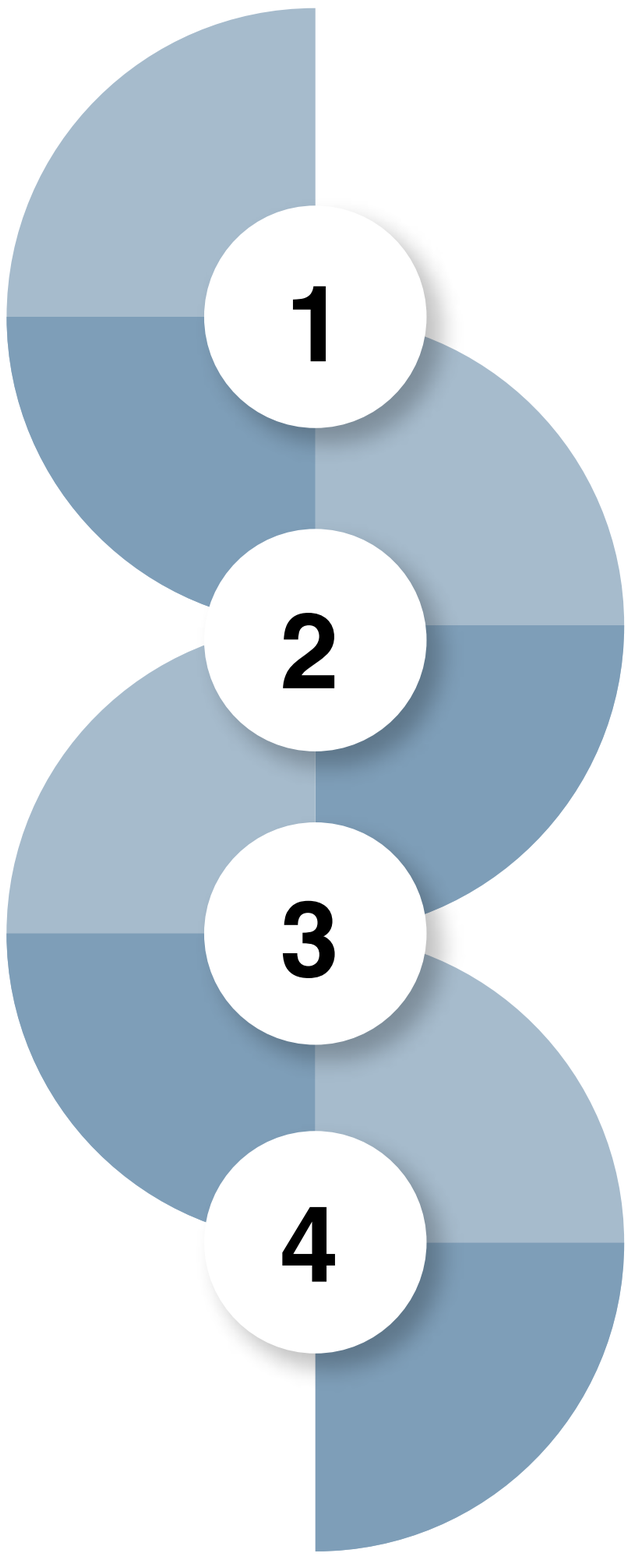
PCH's mission is to underpin critical communications infrastructure, ensuring that it remains functional and accessible to the public. It focuses on several core areas:

Internet Exchange Points

The sources of Internet bandwidth, Internet exchange points (IXPs) are where Internet service providers meet to exchange traffic.

Regulation and Public Policy

PCH helps national communication regulators and ministries understand Internet technical, economic, and governance issues and develop policies that benefit the public.



Core of the Domain Name System

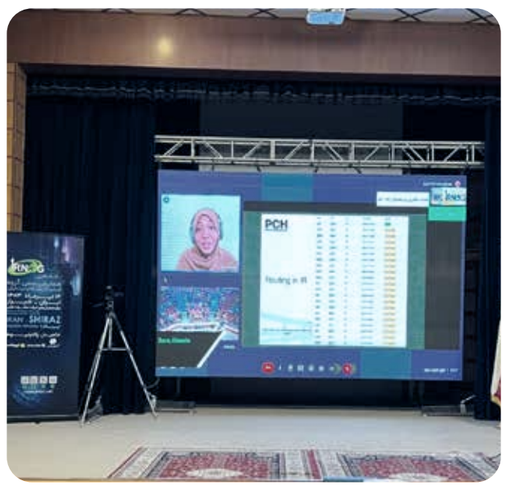
The Domain Name System (DNS) is the distributed directory that allows anything on the Internet to find anything else on the Internet.

Cybersecurity Coordination

PCH operates a "CERT (Computer Emergency Response Team) of Last Resort" and facilitates communication and coordination among cybersecurity emergency responders.









History of **Packet Clearing House**

30-Year Anniversary


Packet Clearing House was founded in September 1994 as the culmination of a series of meetings of more than two dozen private-sector Internet service providers organized by Christopher Alan and Mark Kent. It was an outcome of the 1993 National Information Infrastructure plan, by which Vice President Al Gore organized the transition of the Internet from U.S. Department of Defense central planning to global private-sector governance. PCH initially functioned as an unincorporated joint project of Internet service providers, using seconded staff and facilities, and was formalized as a California 501(c)(3) not-for-profit public-benefit corporation (similar to ICANN, another outcome of the NII), in November 2000.

Historical Milestones of Packet Clearing House

Formation as a Collaborative Project

PCH began as a joint initiative among Internet service providers in the United States. This marked the transition from a government-funded Internet to a privatized model driven by market demands.

Expansion into the Domain Name System

Recognizing the Domain Name System as a fundamental component of Internet infrastructure, PCH began supporting its development and scaling. PCH's work has been instrumental in ensuring the reliability and resilience of DNS services worldwide.

Advocacy for Anti-Spam Legislation

PCH led efforts to enact the world's first anti-spam legislation, demonstrating its commitment to addressing emerging challenges in Internet governance and communication security.

Formal Incorporation

After several years as an unincorporated joint project, PCH incorporated as a California 501(c)(3) not-for-profit public-benefit organization. This robust and sustainable financial model enables PCH to better serve its global constituency.

Ongoing - Advocacy for Public Internet Resources

Notable efforts include preventing the commercialization of the .org domain by private equity interests, safeguarding its use for nonprofits worldwide, and encouraging adoption of modern DNS security protocols, such as DANE (DNS-based Authentication of Named Entities), which has seen rapid global adoption.

1993

1994

Focus on Internet Exchange Points

Beginning in 1994, PCH supported the establishment and operation of Internet exchange points, which are critical for enabling data exchange between networks. This became one of PCH's primary areas of expertise and continues to be a cornerstone of its work.

1995

1996

Introduction of Anycast Technology

PCH contributed to the development and implementation of anycast, a technique allowing the same IP address to be hosted on multiple servers worldwide. This innovation improved the scalability and resilience of the DNS.

1997

Late 1990s

Focus on Regulatory and Policy Issues

PCH began working with governments and regulatory bodies to address critical issues, such as the equitable management of IP addresses (e.g., IPv4 and IPv6), protection of public resources such as the .org domain from commercial exploitation, and establishing best practices for Internet governance.

2001

2006

Introduction of DNSSEC

PCH supported the Puerto Rico .PR becoming the second DNSSEC signed ccTLD.

2019

Transition to Intergovernmental Treaty Organization

On August 17, 2023, PCH transitioned from non-governmental organization (NGO) to intergovernmental organization (IGO), the culmination of a twelve-year process and the beginning of a new and larger chapter in the fulfillment of its mission.

2023

Our daily lives are **increasingly dependent** on accessible and resilient information.

PCH meets the challenge with the reach of anycast DNS, the strength of its root server operations, and protocol extensions that safeguard data.

Domain Name System

Deploying Anycast

In the vast ecosystem of the Internet, where rapid and reliable connectivity is presumed available for daily function, the Domain Name System is a core element. The DNS translates human-readable domain names (for example, www.pch.net) into machine-readable Internet Protocol (IP) addresses used to communicate with all Internet servers. Given its critical role, ensuring the efficiency and resilience of the DNS is paramount. For this reason, PCH promotes DNS anycast, a technology that enhances the quality and capability of the DNS.

DNS anycast deploys a unique routing method in which one IP address is simultaneously available at multiple locations on the Internet. This technique ensures that, when an end user initiates a connection to an IP address, the user is seamlessly directed to the closest server site available.

Three Key Advantages of DNS Anycast

1. A swift response to queries processed by a server located close to the user.
2. Defense against distributed denial of service (dDOS) attacks through load-sharing traffic. By dispersing incoming (and often malicious) traffic across its extensive network, anycast naturally diminishes the impact of threats.
3. There is no single point of failure. Thanks to the extent of the network, its decentralization creates redundancy.

116

World Countries **ccTLDs**

98

Military and Government **TLDs**

22

Generic **TLDs** and **IDNs**

Anycast Sites

Focusing on Community Growth

Packet Clearing House's unique DNS anycast network is the result of thirty years of collaboration with partners and sponsors globally. We are committed to enhancing the Internet's structural resilience. In 2024, this goal was accomplished with

- upgrades made in Berlin, Bucharest, Buenos Aires, Calgary, Cape Town, Kansas City, Nairobi, Roseau, San José, Tampere, Tokyo and Vienna

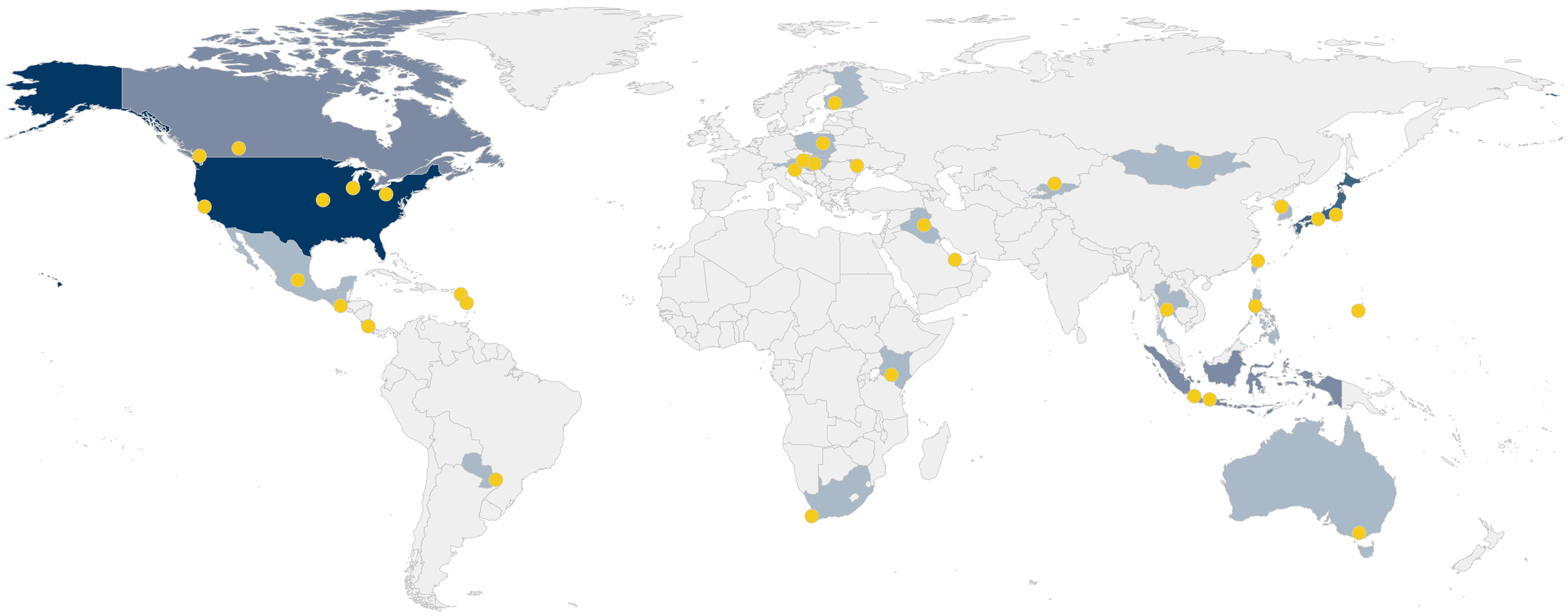
- new deployments made in Baghdad, Bangkok, Basseterre, Bishkek, Bratislava, Budapest, Chicago, Chișinău, Ciudad del Este, Doha, Fremont, Guatemala City, Jakarta, Ljubljana, Manila, Melbourne, Osaka, Pittsburgh, Queretaro, Semarang, Seoul, Taipei, Tamuning, Tokyo, Ulaanbaatar, Vancouver and Warsaw

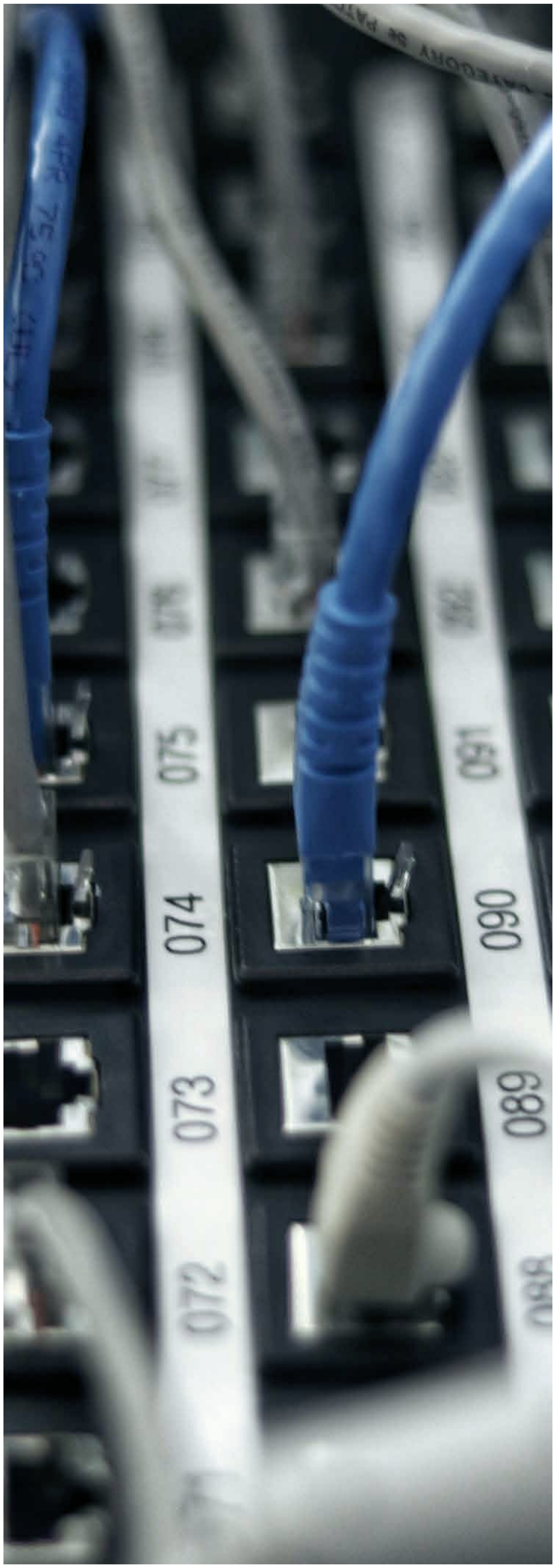
Spotlight on **Japan**

A highlight of 2024 is in the result of the work done with our partners in Japan. Before 2024, PCH was present at two locations in the country. The need for handling substantial DNS traffic with improved efficiency and reliability was the catalyst of our increased focus in Japan.

Thanks to this focused work, PCH now has eight sites, deployed in Tokyo and Osaka. This work in Japan was made possible thanks to partners and donors such as **BBIX**, **DIX-IE**, **EQUINIX**, **JPIX** and **INIXP**.

In **2024**, PCH **deployed 27 new sites** and **12 upgrades**, In **29 countries**.





Among hundreds of partners and donors, these are the ones that made new deployments in 2024 possible:

AIX
Jakarta, Indonesia

BBIX
Bangkok, Thailand
Osaka, Japan
Tokyo, Japan

BCIX
Berlin, Germany

CABASE
Buenos Aires, Argentina

BIX
Budapest, Hungary

Citra-IX
Semarang, Indonesia

CRIX
San Jose, Costa Rica

CSIX
Vancouver, Canada

DACS-IX West
Fremont, USA

DANIX
Roseau, Dominica

DE-CIX Chicago
Chicago, USA

DIX-IE
Tokyo, Japan

EPIX Jakarta
Jakarta, Indonesia

Equinix
Melbourne
Osaka
Seoul
Tokyo

Guam IX
Tamuning, Indonesia

INIXP Asia
Tokyo, Japan

InterLAN-IX
Bucharest, Romania

IRAQ-IXP
Baghdad, Iraq

IX CDE
Cludad del Este, Paraguay

JPIX
Osaka, Japan
Tokyo, Japan

KCIX
Kansas City, USA

KG-IX
Bishkek, Kyrgyzstan

KIXP
Nairobi, Kenya

MD-IX
Chișinău, Moldova

MHK-IX
Manila, Philippines

MISPA-IXP
Ulaanbaatar, Mongolia

NAPAfrica
Cape Town, South Africa

PIT Guatemala
Guatemala City, Guatemala

PIT-IX
Pittsburgh, USA

PIT MX
Qeretaro, Mexico

QIXP
Doha, Quatar

SIX Bratislava
Bratislava, Slovakia

SIX.SI
Ljubljana, Slovenia

SKNIX
Basseterre, Saint Kitts and Nevis

STUIX
Taipei, Taiwan

THINX Warsaw
Warsaw, Poland

TREX
Tampere, Finland

UNM-Exch
Vancouver, Canada

VIX
Vienna, Austria

YYCIX
Calgary, Canada

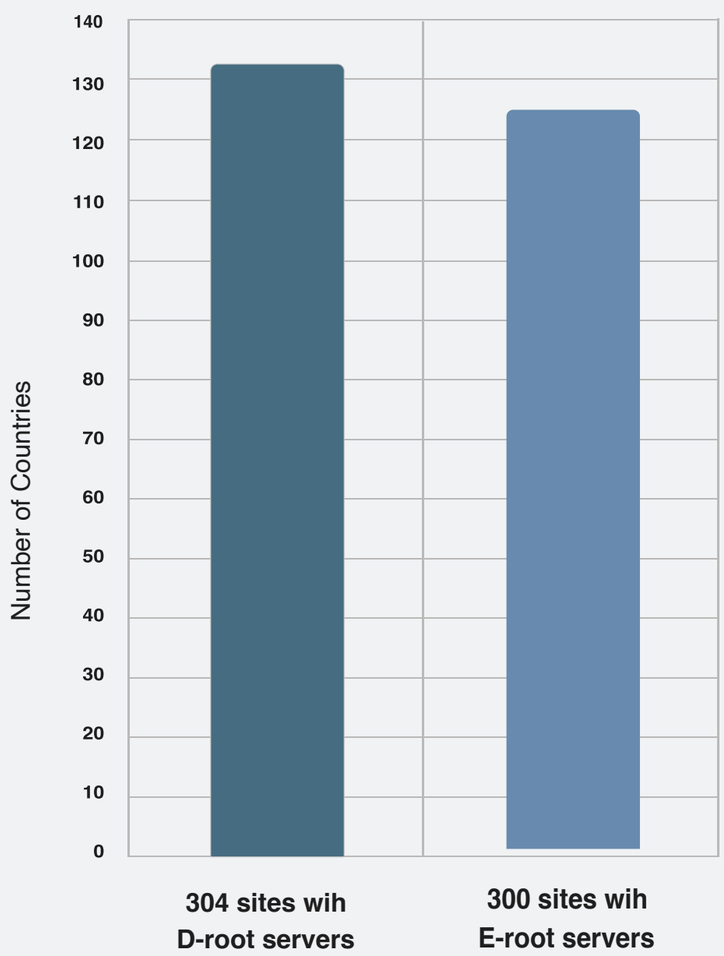
Root Server Operations

Supporting Regions Worldwide

A root server operates in the highest level (or root zone) of the DNS hierarchy. A root server answers queries for records stored or cached in the root zone, such as the names and IP addresses of top-level domains (TLDs) like .com, .org, and .net. A DNS root server also refers requests to appropriate TLD servers, which then direct queries to specific domain name servers.

For example, to visit www.pch.net your device's resolver will

- ask a DNS root server to supply the IP address of www.pch.net. The root server refers the request to .net TLD servers.
- ask the .net TLD servers for the IP address of www.pch.net. The request is referred this time to the pch.net servers.
- query the right server. The request is answered with the www.pch.net IP addresses.



Thirteen root-level IP addresses serve each DNS root zone. Packet Clearing House's anycast routing allows hundreds of root servers to share the same thirteen IP addresses, which provides redundancy and resilience that protects against failures or attacks. Additionally, requests are distributed based on load and proximity, giving end users a fast response.

DNS root servers are operated by such organizations as universities, government agencies, and private companies. PCH provides DNS anycast services to two root servers: D-root, operated by the University of Maryland, and E-root, operated by NASA.

Root servers were deployed by PCH in the following cities in 2024: **Baghdad**, **Bangkok**, **Basseterre**, **Bishkek**, **Bratislava**, **Budapest**, **Chisinau**, **Ciudad del Este**, **Fremont**, **Guatemala City**, **Jakarta**, **Johannesburg**, **Ljubljana**, **Manila**, **Melbourne**, **Osaka**, **Pittsburgh**, **Queretaro**, **Seoul**, **Tamuning**, **Tokyo**, **Ulaanbataar**, **Vancouver** and **Warsaw**.

Domain Name System Security

Strengthening Protocol Extensions

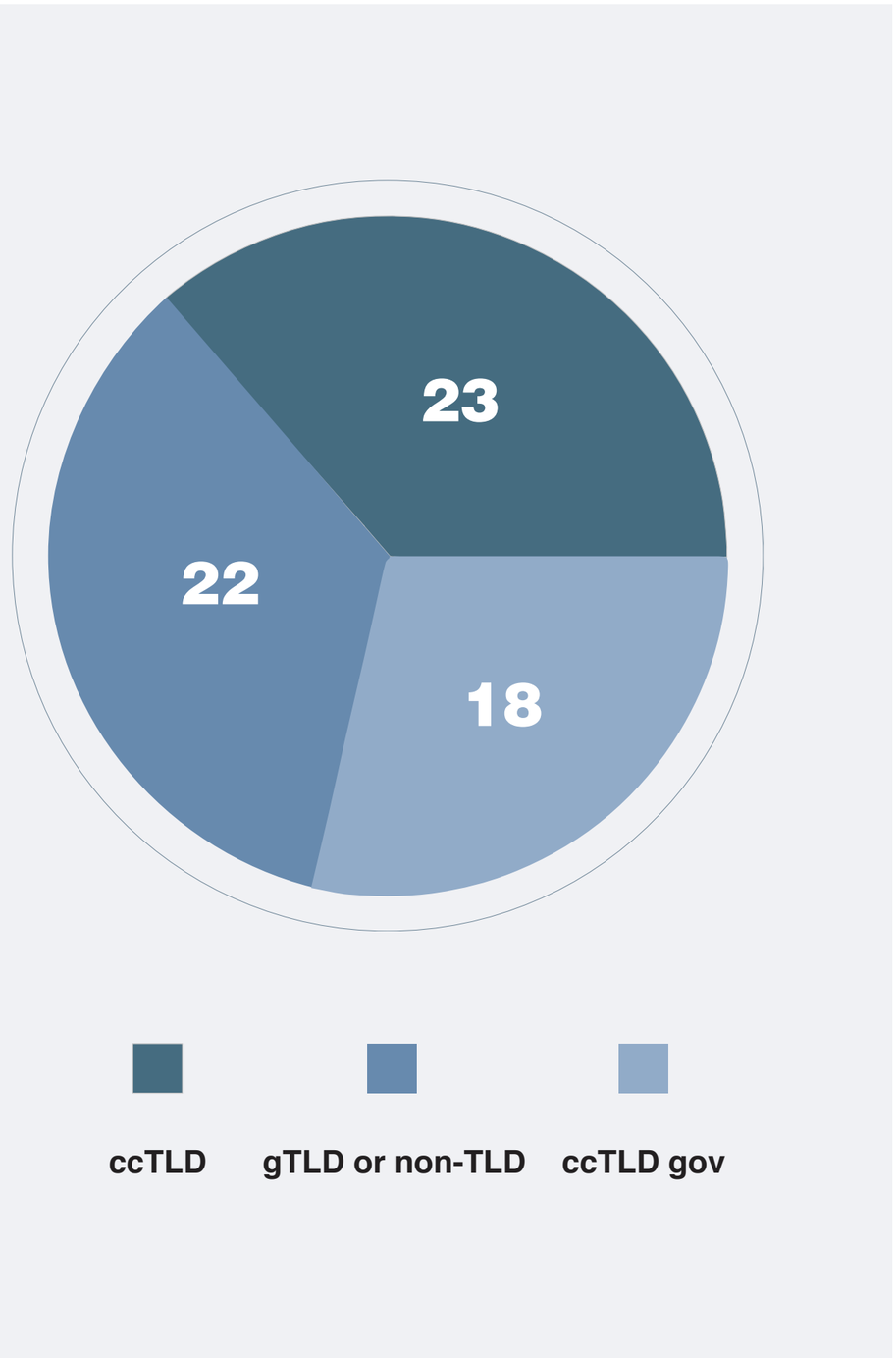
DNS Security (DNSSEC) is a protocol extension that verifies that a message sent over the Internet came from its expected sending server and not a malicious party. DNSSEC also ensures that the integrity of the message is uncompromised. As an inline signing service, PCH DNSSEC is unique among DNSSEC services.

PCH DNSSEC not only adds DNSSEC when it receives a customer's unsigned zone information but also distributes DNSSEC zones through our own PCH anycast service — and all other designated name servers.

PCH DNSSEC creates and stores DNSSEC keys with FIPS-4 certified hardware security modules (HSMs). At least once a year, publicly streamed and archived key ceremonies are held in our secure vault facilities in San Jose, California, USA, Singapore, and Zurich, Switzerland, which also holds HSM replications of the keys and is managed with distinctive software and hardware for additional resilience.

PCH is also strongly committed to sharing knowledge with the DNS community. In 2024 at OARC 42, PCH introduced its DNSSEC signer upgrade, summarizing the key properties of PCH's DNSSEC bump-in-the-wire signer, which has been in operation since 2010. Furthermore, PCH conducted a workshop on "Internet Estable, Resiliente y Segura mediante DNS Anycast y DNS Recursivo" at the ANDINA LINK Smart Cities Expo, held in Cartagena, Colombia. The workshop covered building a resilient DNS anycast infrastructure and included an introduction to Quad9, an open DNS recursive service that offers free security and enhanced privacy.

PCH DNSSEC customers, as of December 31, 2024



Internet Economy

Enhancing Efficiency & Sustainable Growth

PCH works with sovereign nations to coordinate with multiple stakeholders necessary for the creation and maintenance of an IXP. Once built, the peering service provided by PCH helps these communities connect across the Internet to exchange data without the burden of a third party.

Building local Internet Exchange Points is essential to a nation's

Digital Strategy

Internet Exchange Points

Improving Economic Value

Internet value is measured in bandwidth. Internet exchange points are the places where Internet service providers connect — and it is those places of interconnection where bandwidth, the value customers are buying, is produced. Countries without their own IXPs must use suppliers outside the country. They therefore have a net import of Internet bandwidth and net export of capital, often resulting in higher prices for Internet services for their residents.

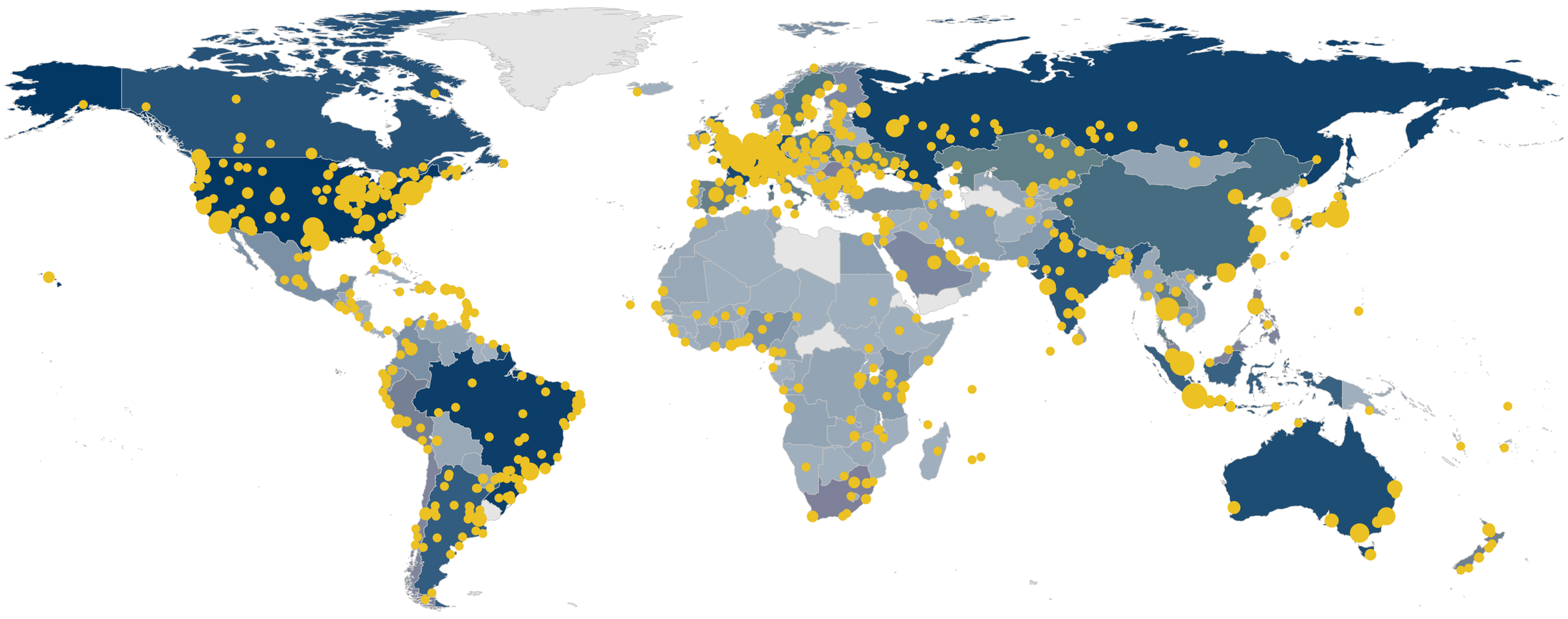
An internal IXP gives a country or region the ability to become a supplier of Internet bandwidth, creating revenue as a net exporter. Additionally, a local IXP lowers the Internet traffic the service providers ferry from an IXP to their customers. Bandwidth value to their customers increases, while the cost of bandwidth lowers.

PCH provides support to Internet exchange facilities at every point of their development, from the process of formation to their growth in structures already up and running. Beyond the supply of the switching equipment that forms the technological core of exchanges, our most valuable contributions are often in the forms of education, technical expertise, and mediation with policy and economic officials of the local government. Some concrete examples of the support provided to Internet exchanges in 2024:

- Providing strategic advice and assistance to the Rwanda Internet Community and Technology Alliance (RICTA), the organization responsible for operating RINEX and the .RW ccTLD

- Donating equipment to the Kinshasa Internet Exchange (KINIX), Grenada IX, Gambia IX and the Malawi Research and Education Network (MAREN), supporting their connection to Malawi IXP

As part of its research initiatives, PCH maintains an index of all Internet exchanges worldwide in the IXP Directory, https://www.pch.net/ixp/dir. On December 31, 2024, the directory contained 1,184 IXPs. Furthermore, PCH publishes statistics on IXP growth and domestic bandwidth production by country: see https://www.pch.net/ixp/summary_growth_by_country.

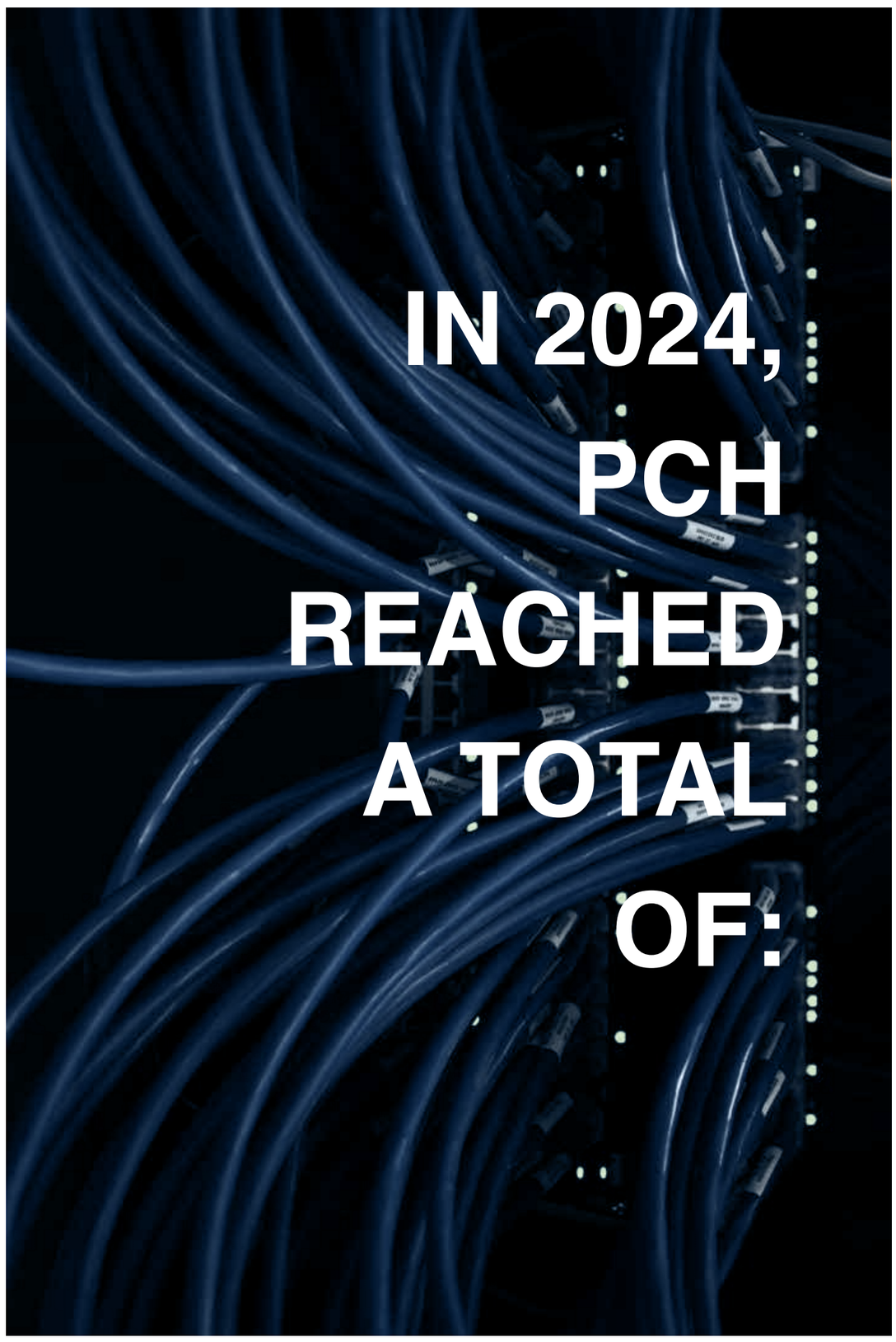


Peering

Increasing the Footprint

Peering is the process by which two Internet networks connect and exchange traffic at an Internet exchange point. Peering allows IXPs to hand off traffic between each other's customers, without having to pay a third party to carry that traffic across the Internet for them. Peering typically produces a more direct path between two networks, thereby reducing the distance that data has to travel, resulting in lower latency and improved user experience.

Packet Clearing House has an open peering policy: we are happy to interconnect with any other network that operates in accord with generally recognized best practices. As of December 2024, PCH is available for peering at 329 IXPs worldwide and is one of the largest peering networks globally. PCH also supports local peering communities through knowledge sharing. In 2024 PCH led two workshops at the Malawi Internet Development Workshop held in Mangochi. The sessions, titled "What You Know About Peering Is Wrong!" and "Quad9: Free, Secure, and Fast DNS," aimed to enhance participants' understanding of critical Internet infrastructure topics. At the Central Asia Peering and Interconnection Forum (CAPIF-3), PCH presented best practices in peering, highlighting the differences between local and global peering scopes. At Peering 6.0 in Jakarta, Indonesia, PCH conducted a peering tutorial in collaboration with APNIC.



35,061
IPv4 peering sessions

4,915
Peer networks

26,475
IPv6 peering sessions

Information Society

Supporting Resilience and Continuous Development

PCH contributes its expertise to the success of projects led by other organizations to better the global Internet infrastructure.

Supporting Innovative Open-Source Projects

1. Digital Emblems

Digital emblems are the 21st-century evolution of the visual sigils that identify people, places, and objects that enjoy special protections or require special identification under international law. Digital emblems aim to address the shortcomings of traditional visual emblems through a set of global open standards that may be implemented without licensing fees or restrictions.

Each digital emblem consists of a set of records associated with a person, place, or object; or with digital data at rest or in transit; or with networked digital services. They identify the protected item and communicate the nature of the protections it enjoys and which body of international law defines those protections. Each digital emblem is signed with a cryptographic certificate the validity of which can be constrained both geographically and temporally. The authenticity of digital emblems can be evaluated using simple, publicly documented algorithms, which are free for anyone to use and can be built into web browsers that run on commonplace mobile telephones or computers, or more specialized hardware like cameras or handheld wireless scanners.

Standards-based validation of digital emblems can vastly simplify the work of customs and immigrations agents. It can also be incorporated easily in military equipment and processes, to ensure that protected entities are not targeted by military actions.

While nighttime may render the “Press” emblem painted on a press facility invisible to a drone or loitering munition, the RFID transponder or geographic bounds of a digital emblem can silently and efficiently ensure that it is not targeted.

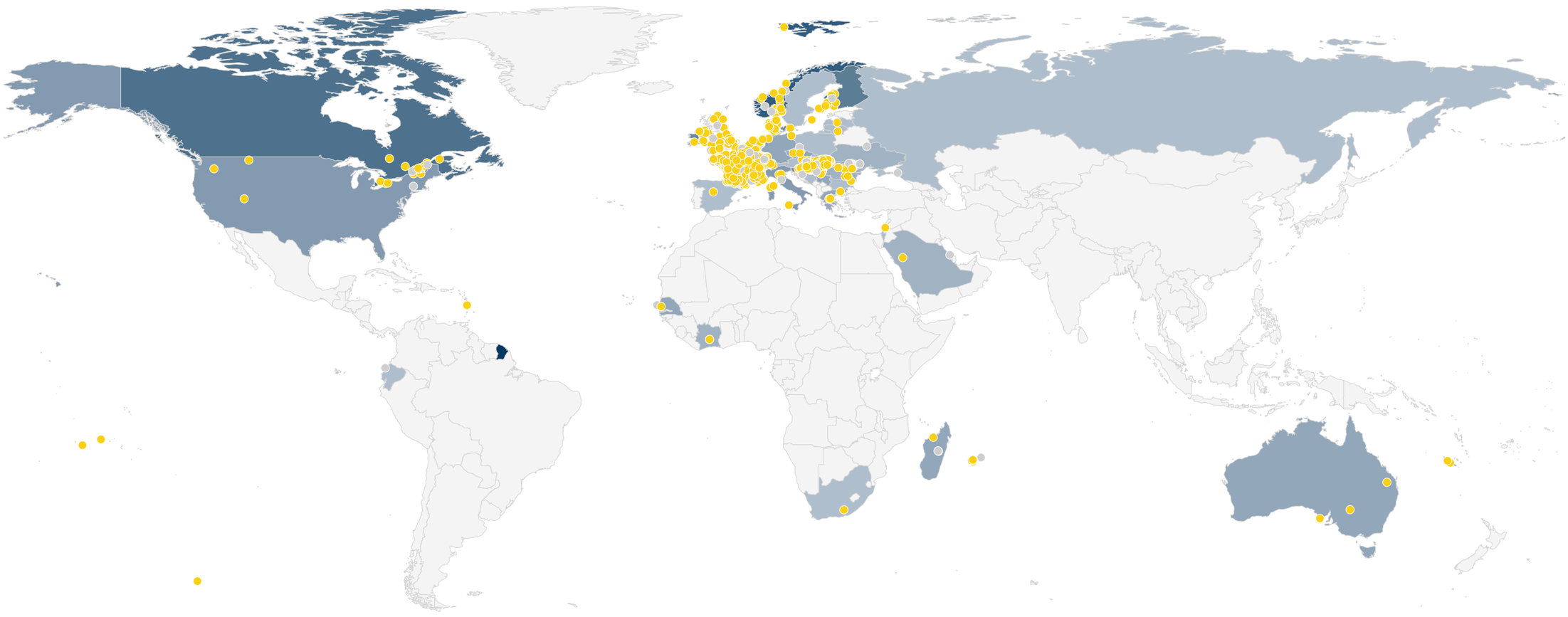
Digital emblems can also protect diplomatic pouch shipments, diplomatic couriers, and diplomatic envoys. Trademarked goods can also be marked with digital emblems to prevent counterfeit goods. Digital emblems can also be used to protect endangered species of fauna and flora to curtail illegal trade of these species.

During 2024, PCH led collaborative efforts at the Internet Engineering Task Force (IETF), the global standards body for Internet protocols that ensure that all parties have free and open access to the information and tools necessary to implement them. Two preliminary investigative meetings were held, and the leadership of the IETF began review of the charter for a long-term working group.

2. Real-Time Kinematics

Real-Time Kinematics (RTK) and Networked Transport of RTCM via Internet Protocol (NTRIP) are a pair of protocols that provide improved accuracy to receivers of Global Navigation Satellite Systems (GNSS) signals like GPS, Galileo, BeiDou, and GLONASS, which broadcast timing signals from satellites in orbit. Without the improvements RTK and NTRIP offer, the finest precision these GNSS systems can offer is about three meters, which is insufficient for applications such as self-driving vehicles and precision agriculture. With RTK and NTRIP, that can be reduced to millimeters or single-digit centimeters, depending upon the receiver’s distance from the nearest RTK ground reference station.

RTK ground reference stations receive GNSS signals at known locations, calculate the difference between known ground truth and what can be derived from the satellite signals, and publish a correction stream which is accurate to the millimeter level for their specific location. The degree of applicability of the correction stream decreases as a function of the distance from the ground reference station. It is therefore imperative to have ground reference stations close to consumers of the data, and to have them operate in a resilient mesh. NTRIP achieves that goal by providing a content-aware load-balancing front end, on fast servers in reliable datacenters, between the many small RTK ground reference stations and the even more numerous consumers of RTK data, which include



everything from aircraft and city buses to lawn mowers and mobile phones.

PCH is applying its expertise in global resilient operation of critical communications infrastructure to the GNSS ecosystem, by designing and deploying next-generation hardened RTK ground reference stations and operating the global NTRIP front-end for the RTK system. This deployment mirrors the similar work we have done to harden the global DNS and Network Time Protocol (NTP) infrastructures against natural disasters and intentional attacks.

In 2024, PCH initiated design of the second generation of the RTK ground reference stations, based on RISC-V open hardware, and began the process of deploying the global NTRIP load-balancing infrastructure, publishing data from approximately 2,000 ground reference stations, concentrated largely in France and Hungary. In future years we will work on the third generation hardware and effect dense deployment across many more countries.

3. IXP History Collection

The IXP History Collection is an ongoing project that documents histories of the Internet exchange points at the core of the Internet's topology. IXP histories are inextricably linked to the commercialization of the Internet, and their development is a significant milestone in the global history of media and communications. Efforts should therefore be made to ensure that we preserve IXP histories for future generations.

The main purpose of the project is to collect and preserve networking and IXP histories that may otherwise be lost from the global record. In particular, the project is concerned with the fragility of electronic information and born-digital documents, records, and multimedia, otherwise known as born-digital heritage. As a starting point, the project utilizes the Internet Exchange Directory maintained by PCH, one of the earliest organized efforts to develop and maintain a database for recording and tracking the establishment, development, and global growth of IXPs.

The project then focuses on documenting IXP histories through as many online sources as possible (e.g., websites/pages, reports, journals, magazines/newspaper articles, old emails on public mail lists). To do this, the project is using Zotero Groups (free and open-source reference management software) to manage the archival/bibliographic data and its metadata. This effort is currently underway as a work in progress here: Zotero | Groups > IXP History Collection - Information Directory. In addition, the project actively pursues the web archiving of publicly accessible online sources using the Save Page functions in the Internet Archive's Wayback Machine and Arquivo.pt. To date, the project has collected over 7,500 bibliographic sources and is currently in the final edits of a forthcoming publication with a historical timeline and background information of the earliest IXPs for the period 1988–1995.

Though the IXP History Collection directory has a large representation of sources in English, PCH is attempting to include as many sources as possible. To make this resource as inclusive and multilingual as possible, the project is reaching out to the global IXP community to assist by anonymously suggesting multilingual sources using the form provided HERE. The project is also soliciting digital file donations of fringe materials such as images of schematic drawings/doodles, technical graphics, photographs of racks, switches, cables, and, of course, photographs of the people involved in the running of early IXPs. Collecting and preserving the annual reports of the early IXPs would be a major bonus for our effort. For more information about the project, see the IXP History Collection - Development Strategy (2024).

Partnerships

Building a Better Global Community

The International Committee of the Red Cross

This partnership was initiated as a consequence of the ICRC's intention to reach Internet and communications technology (ICT) autonomy — to build the capacity to support its own ICT needs without external dependencies. PCH championed this approach and is proud to share its experience with the ICRC. The steps taken by the ICRC to gain strategic ICT autonomy represent an example to other such key organizations and governments.

Smart Africa

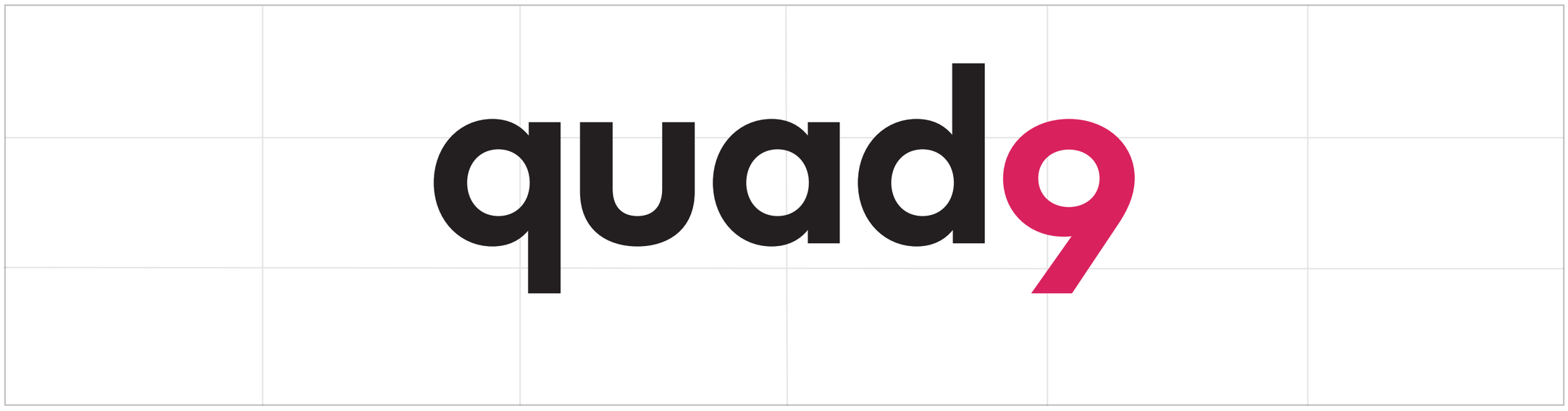
Packet Clearing House and Smart Africa have partnered to drive Africa's digital transformation by strengthening Internet governance, infrastructure, security, and capacity building across the continent. This collaboration is dedicated to developing robust regulatory frameworks that enhance African digital sovereignty, including initiatives to repatriate national ccTLDs and support data-driven ICT policymaking. Aligned with Smart Africa's vision, PCH will contribute to building critical Internet infrastructure to expand connectivity and economic growth across the region. Additionally, the partnership will prioritize cybersecurity by securing core Internet infrastructure.

By engaging with key Internet governance stakeholders, PCH and Smart Africa are committed to fostering inclusive connectivity, effective regulation, and sustainable ICT development across Africa. PCH also actively supports Smart Africa's efforts within the framework of the Working Group on Internet Governance, chaired by Burkina Faso. This initiative aims to develop a continental master plan to address key issues related to Africa's digital sovereignty, with its first meeting taking place alongside ICANN80 sessions in Kigali.

Further reinforcing their commitment to these goals, PCH and Smart Africa collaborated during the ICANN81 meeting in Istanbul to organize a parallel event focused on raising awareness about the importance of prioritizing strategies to address DNS and sovereignty challenges. This event included a ministerial training and peer learning session on ccTLD processes and regulatory frameworks for governments, lawmakers, and members of the Coalition for Digital Africa.

Network Operators Groups

PCH is committed to sharing knowledge and offering practical support to Network Operators Group (NOG) communities worldwide, through sponsorships and capacity building. 2024 examples are a workshop on Network Essentials given at NpNOG-9, insights on how to build and manage a global DNS anycast network at IranNOG-6, and practical guidance on the full life cycle of peering at MENOG-24.



Quad9 is an open DNS recursive service with a strong focus on both security and high-level privacy. Although the Quad9 resolver services are provided with PCH deployments, Quad9 is a fully independent organization supported by multiple partners. PCH partners with Quad9 to serve end user Internet security and drive compliance with European privacy regulations.

Network operators, commercial organizations, schools, hospitals, and other end users can take advantage of Quad9's recursive DNS services at no cost and with no contract. Configuration is simple and can be applied dynamically to all clients in a local network via centralized host management (DHCP) with no software or downloads. Users immediately receive the benefits of Quad9 protection, with connection to malicious hosts blocked before any attempted connection. More than twenty-five different threat intelligence partners supply Quad9 with dynamic lists of hostnames that present risk to end users, and in turn Quad9 provides insights to the groups that are performing vital cybersecurity services for the Internet in general.

In 2024, Quad9 significantly expanded its footprint by partnering with PCH. Quad9 is hosted in almost all of PCH's new installations and is offered as a valuable service on the Internet exchange platforms where it is available. Quad9 is a highly visible brand to end users. With significantly increased adoptions, Quad9's service has been tested and verified as superior protection performance. Our partnership with Quad9 increases PCH's appeal as a provider of vital services to nations, regions, and networks.

As of 2024, Quad9 blocks more than 670 million malicious events per day on average and has reached up to 1.5 billion events in a single day. These events represent intercepted connection attempts from botnets and ransomware as well as user-interactive security events like phishing, stalkerware, and other criminal activities. The majority of these events are processed on PCH-delivered network and co-location capacity.

Packet Clearing House

Packet Clearing House is the intergovernmental treaty organization responsible for providing operational support and security to critical Internet infrastructure, including Internet exchange points and the core of the domain name system since 1994.

info@pch.net

www.x.com/PCHglobal

www.linkedin.com/company/packet-clearing-house

www.pch.net