



ANNUAL REPORT 2023

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.

www.pch.net

CONTENTS

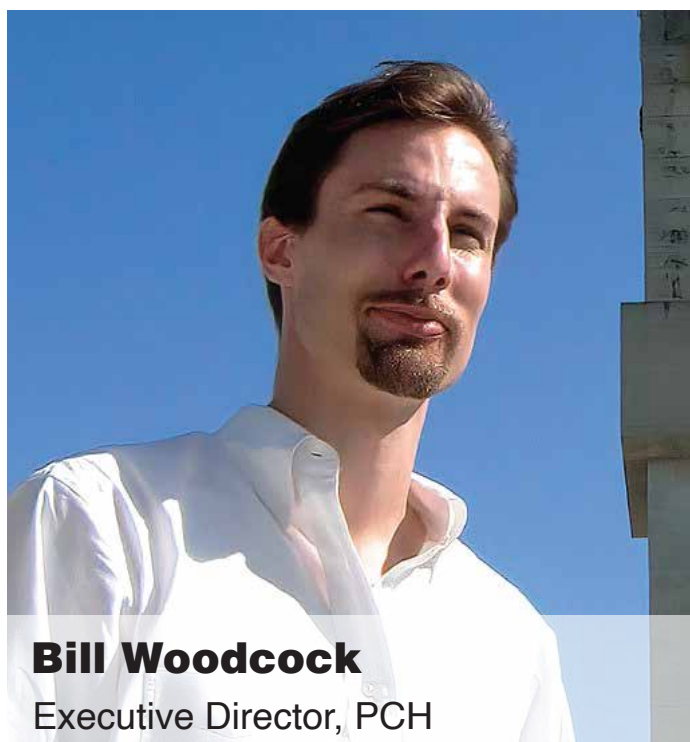
1. Message from the Board and Executive Director	03
2. Intergovernmental Organization: Evolving for Long-Term Effectiveness	04
3. Internet Infrastructure: Strengthening Security & Stability	06
3.1 Domain Name System: Deploying Anycast	07
3.2 Anycast Sites: Focusing on Community Growth	08
3.3 Root Server Operations: Supporting Regions Worldwide	10
3.4 DNS Security: Strengthening Protocol Extensions	12
4. Internet Economy: Enhancing Efficiency and Sustainable Growth	13
4.1 Internet Exchange Points: Improving Economic Value	14
4.2 Peering: Increasing the footprint	15
5. Information Society: Supporting Resilience and Continuous Growth	16
5.1 Memorandum of Understanding: Formalizing Relationships	17
5.2 Sovereign Nations: Repatriating ccTLDs	18
5.3 Partnerships: Building a Better Global Community	19
5.4 Partnerships: Building a Better Global Community with Quad9	21

MESSAGE FROM THE BOARD OF DIRECTORS

For nearly thirty years, Packet Clearing House has acted as the “fire department” of the Internet, responsible for providing operational support and security to critical Internet infrastructure, including Internet exchange points and the core of the Domain Name System. In keeping with its public-benefit not-for-profit charter, PCH provides all of its services for free or at cost, thanks to the support of government grants and many hundreds of generous donor organizations in the Internet’s private sectors.

In this report we highlight PCH’s achievements, with a special focus on 2023. We are immensely grateful to the donors, partners, and volunteers who have made this work possible.

The report is structured on PCH’s three foundational pillars: strengthening the security and stability of the Internet infrastructure; enhancing the efficiency and sustainable



Bill Woodcock

Executive Director, PCH

growth of the Internet economy; and supporting the resilience and continuous development of the information society. In addition to these public-facing goals, we include an inward-facing goal: ensuring the long-term health and effectiveness of PCH as an organization. A major milestone in ensuring organizational stability was the completion of PCH’s transition to intergovernmental treaty organization (IGO) status on August 17 of this year, the result of more than ten years of collaborative effort. This maturation guarantees PCH’s ability to embody the multi-stakeholder principles central to international Internet governance, giving equal representation to our

government stakeholders and solidifying PCH’s ability to serve all of our constituencies in the broad tent of the Internet community for the many years to come.

We cannot emphasize enough our deepest gratitude to all of the signatories of the PCH treaty, our donors, our partners, and our volunteers for their crucial and continuous support and commitment to an Internet that is resilient, reliable, and available to all. We look forward to continuing to develop and strengthen the Internet’s critical infrastructures, economy, and community, together with your support.

-
- **Steve Feldman** (Chairman of the Board), **Sylvie La Perriere** (Director), **Mark Tinka** (Director)
Greg Akers (Director), **Bill Woodcock** (Executive Director)

Intergovernmental Organization

Evolving for Long-Term Effectiveness

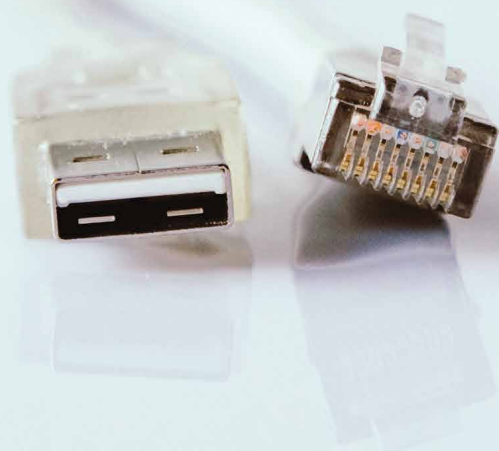
In August of 2023, Packet Clearing House celebrated a successful transition from non-governmental organization headquartered in California to an intergovernmental treaty organization (IGO). PCH's maturity, married with this evolution to our organization's global footing, is the foundation on which we will build in the years to come. As an IGO, we are excited to:

- Sustain our achievements with evolved governance
- Strengthen our relationships with current government business partners
- Seize new opportunities as we engage with the Internet community

In 2023, four governments signed and ratified the founding treaty of PCH as an intergovernmental organization:



The strategic objective of an intergovernmental organization is to close the digital divide between public and private sectors. IGOs ensure that the benefits of a strong, stable, affordable and resilient Internet critical infrastructure are available to any sovereign country and dependent territory in the world. The increased representation of the public sector strengthens the multistakeholder governance model of the Internet confirmed by the World Summit of Information Society (WSIS) in 2005.



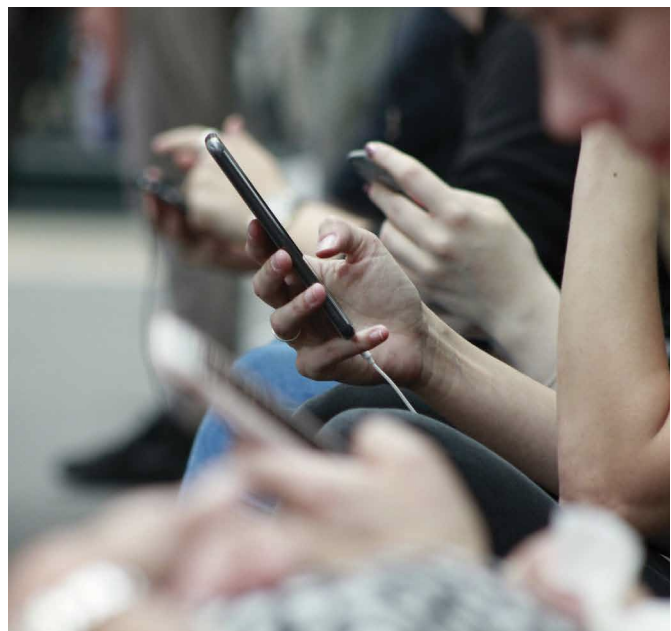
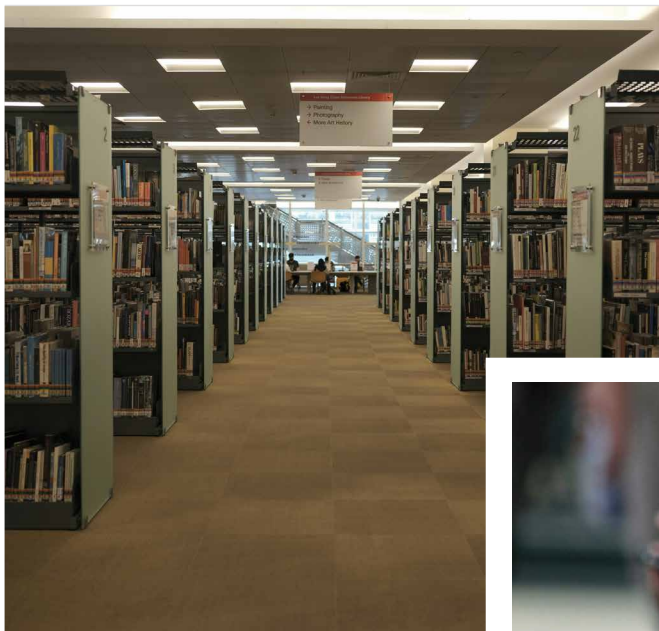
In 2024, we
expect **more**
governments
to join the treaty
and better direct
our focus,
attention,
and
expenditure
of our
resources while
sustaining our
common
achievements.

Internet Infrastructure

Strengthening Security and Stability

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 (DNS) 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 methodology 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

- A swift response to queries processed by a server located close to the user.
- 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.
- There is no single point of failure. Thanks to the extent of the network, its decentralization creates redundancy.

114

World Countries ccTLDs

98

Military & Government
TLDs

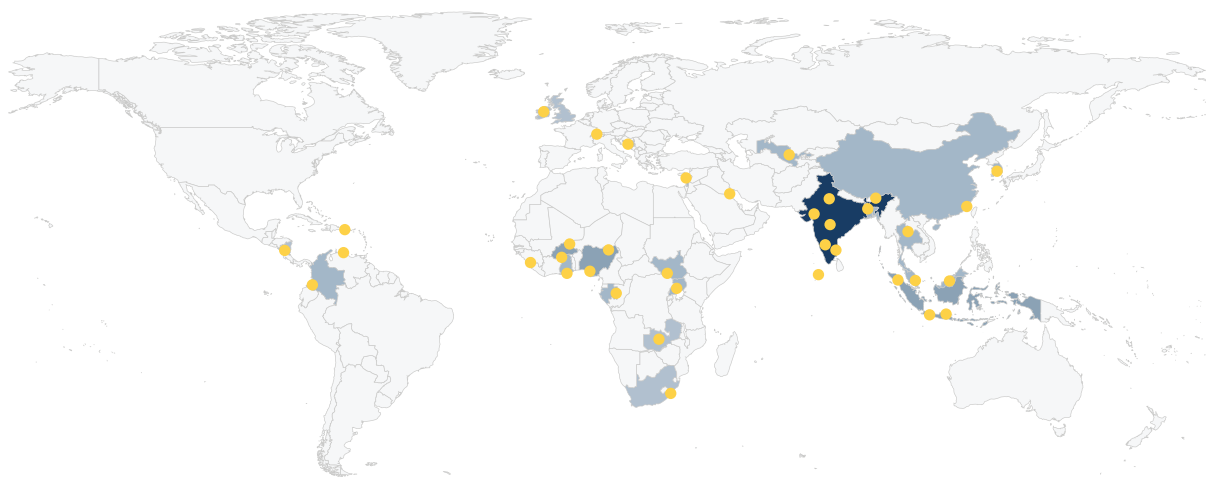
22

Generic TLDs and IDNs

2023,
**TOP LEVEL
DOMAINS
ANYCASTED
BY PCH**


Focusing on Community Growth

- Upgrades made in Accra, Blantyre, Edinburgh, Jakarta, Kigali, Lagos, Ouagadougou, Seoul, St. George's.
- New deployments made in Bobo-Dioulasso, Bogota, Brazzaville, Brunei, Chiang Mai, Conakry, Dhaka, Djibouti, Gqeberha, Hong Kong, Lagos, Lusaka, Malé, Manama, Ramallah, Road Town, San Pedro Sula, Sarajevo, Singapore, Surakarta, Tashkent, Yogyakarta, Zurich.



Spotlight on India

*Thanks to this focused work, the existing Mumbai site received an upgrade, and seven new sites were deployed in Delhi, Chennai, Kolkata, Hyderabad, and Mumbai. This work in India was made possible thanks to partners and donors such as **CTRLS — DE-CIX — EQUINIX — EXTREME IX — IIFON — NIXL**.*



Amongst hundreds of partners and donors, these are the ones that made new deployments in 2023 possible:

4b42 IXP Zurich, Switzerland	Equinix Hong Kong Mumbai	Grenada Internet Exchange Point Grenada
AMS-IX Hong Kong Lagos Singapore	ExtremeIX Delhi Mumbai	Korean Internet Neutral Exchange South Korea
BBIX Hong Kong	ISPAB-NIX Bangladesh	Maldives Internet Exchange Maldives
BFIX Bobo-Dioulasso Ouagadougou	IXP Guinee Guinea	Rwanda Internet Exchange Rwanda
FogIXP	IXPN-Lagos Lagos	Djibouti Internet Exchange Djibouti
BKNIX Chiang Mai	SBIX Zurich	Ghana Internet Exchange Ghana
Borneo-IX Borneo	NMBINX	Lusaka Internet Exchange Lusaka
LINX Scotland	Open IXP	Congo Internet Exchange Congo
CHIX-CH Switzerland	PIT Colombia Honduras	BVI Internet Exchange British Virgin Islands
CitraIX Surakarta Yogyakarta	PSIX Ramallah	BHNIX Bosnia and Herzegovina
Manama-IX Manama	NIXI Chennai Delhi Hyderabad Mumbai	
Kolkata IX Kolkata	Malawi IXP Malawi	

Root Server Operations

Supporting Regions Worldwide

A root server operates in the highest level of the Domain Name System hierarchy, the root zone of the DNS. 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

1. Ask a DNS root server for the IP address of **www.pch.net**. The root server refers the request to .net TLD servers.
2. Ask the .net TLD servers for the IP address of **www.pch.net**. The request is referred this time to the pch.net servers.
3. Query the right server. The request is answered with the **www.pch.net** IP addresses.

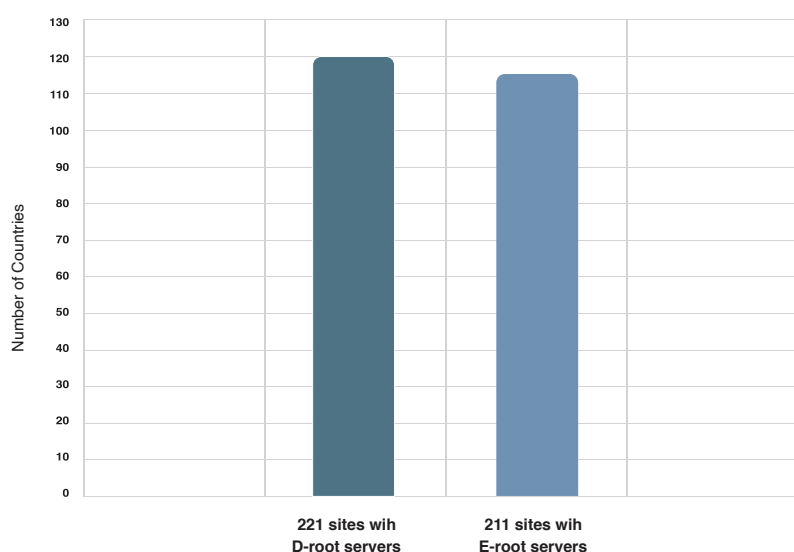
Thirteen root-level IP addresses serve each DNS root zone. Packet Clearing House's anycast routing allows hundreds of root servers to share the same thirteen IP address, which provides redundancy and resilience that protects against failures or attacks. Additionally, requests are distributed based on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

DNS root servers are operated by such organizations as universities, government agencies, and private companies.

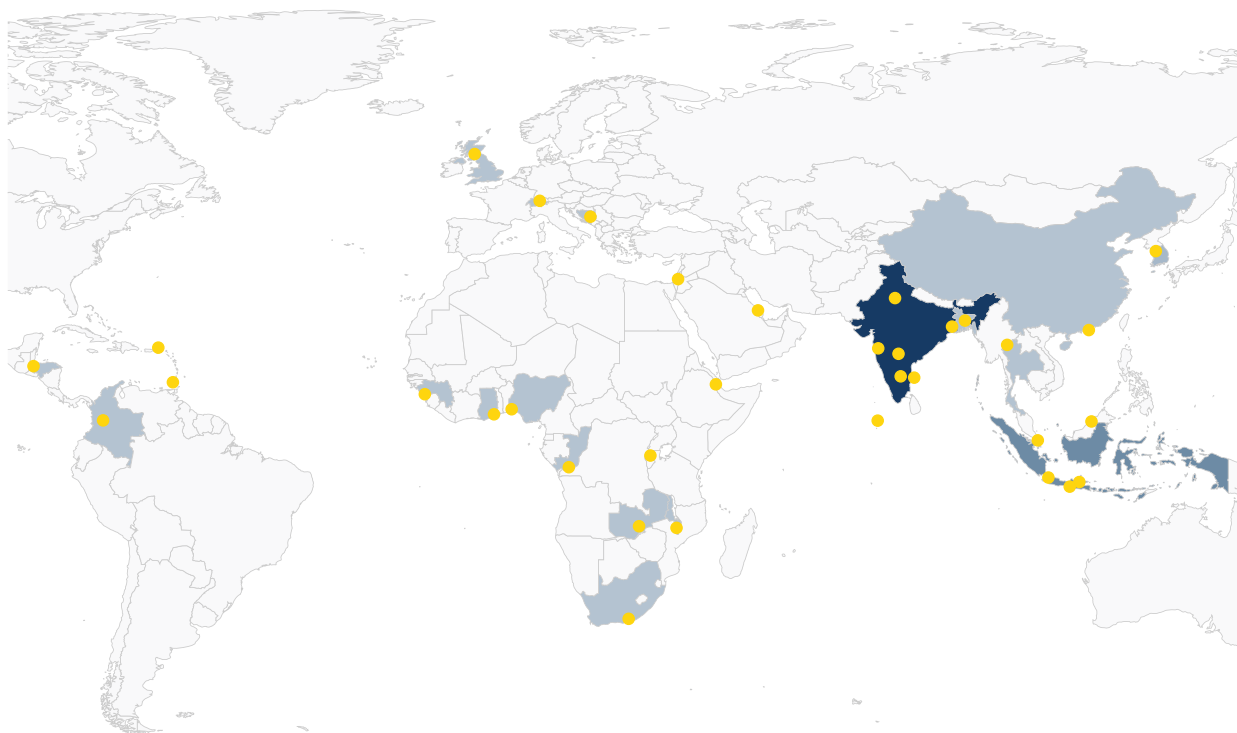
PCH provides DNS anycast services to two root servers:

D-root, operated by the University of Maryland, and
E-root, operated by NASA.

PCH Global Totals:



Newly supported instances of D & E root servers by PCH in 2023



Location	D-root	E-root	Location	D-root	E-root
Accra	1	1	Kigali	1	-
Bangalore	1	1	Kolkata	1	1
Blantyre	-	1	Lagos	2	2
Bogota	1	1	Lusaka	-	1
Brazzaville	1	1	Male	1	1
Brunei	1	1	Manama	1	1
Chennai	1	-	Mumbai	2	2
Chiang Mai	1	1	Ramallah	1	1
Conakry	1	1	Road Town	1	1
Delhi	1	2	San Pedro Sula	1	-
Dhaka	1	1	Sarajevo	1	1
Djibouti	1	1	Seoul	1	1
Edinburgh	-	1	Singapore	1	1
Gqeberha	-	1	St, George's	1	1
Hong Kong	3	3	Surakarta	-	1
Hyderabad	1	1	Yogyakarta	-	1
Jakarta	-	1	Zurich	3	4

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 a unique among DNSSEC service.

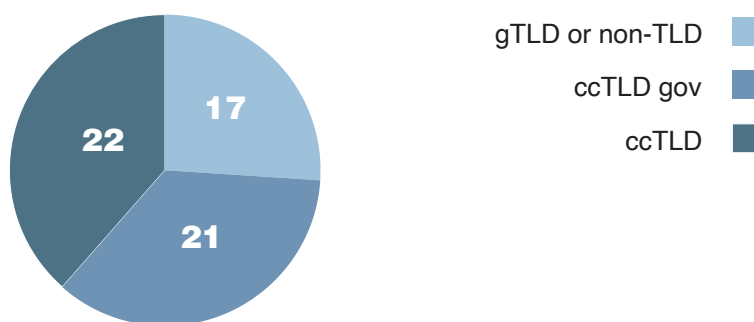
PCH DNSSEC not only adds DNSSEC when it receives a constituent's unsigned zone information but also distributes DNSSEC zones through our own PCH anycast service — and all other designated name servers.

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, and Singapore.

In 2023, PCH conducted a technical refresh for the Zurich key signing facility in Zurich, Switzerland, which also holds HSM replications of the keys and is managed with distinctive software and hardware for additional resilience.

In 2023, PCH DNSSEC evolved to allow commercial constituents that operate under stringent regulations, such as banks, to opt for dedicated key ceremonies in the PCH facilities, or to ask PCH to help create a vault and key ceremony on the constituent's own premises, both with ongoing technical support.

A new service is coming to every type of constituent in 2024, Parallel Signing. With Parallel Signing, constituents can allow PCH to add a second set of keys to a customer's zone that already has DNSSEC, and PCH can coordinate registering the multiple signers according to RFC 8901. Parallel Signing will add extra fault tolerance and resilience to the DNSSEC. These examples are more illustrate why PCH is the leader among DNSSEC providers, chosen by our constituents because of our expertise at providing high-level, proven security certification.



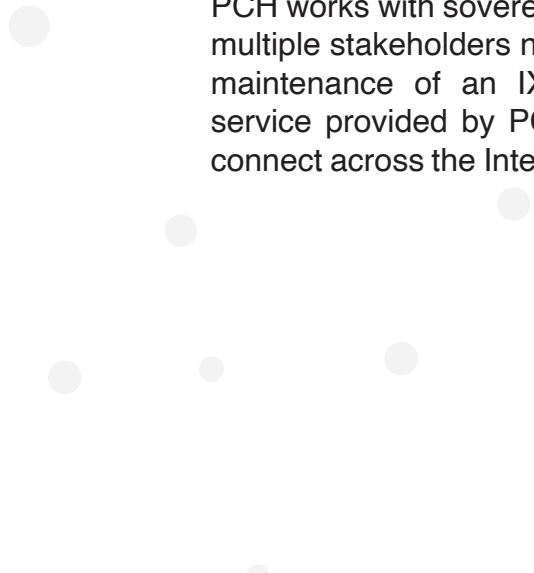
PCH DNSSEC constituents, As of December 31, 2023



Internet Economy

Enhancing Efficiency & Sustainable Growth

IXPs are an essential component to a nation's **Digital Strategy**



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.

Internet Exchange Points

Improving Economic Value

Internet value is measured in bandwidth. Internet exchange points are the places where Internet service providers (ISPs) connect — and it is those places of inter-connection where bandwidth, the value constituents 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 ISPs ferry from an IXP to their constituents. Bandwidth value to their constituents 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.

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 31st 2023, the directory contained 1152 IXPs. Furthermore, PCH publishes statistics on IXP Growth and domestic bandwidth production by country: see https://www.pch.net/ixp/summary_growth_by_country.



Sara and Nishal (PCH team members) giving onsite training to the Chad N'Djamena IX team

2023 Support Highlights to Internet Exchanges

■ Bahrain

DNS and routing efficiency
call with Manama IXP operator

■ Yemen

Launch calls with
operators

■ Zambia

Launch workshops, Technical
assistance

■ Tanzania

DNS and routing efficiency
call with TISPA

■ Rwanda

Training on onsite routing,
Technical assistance

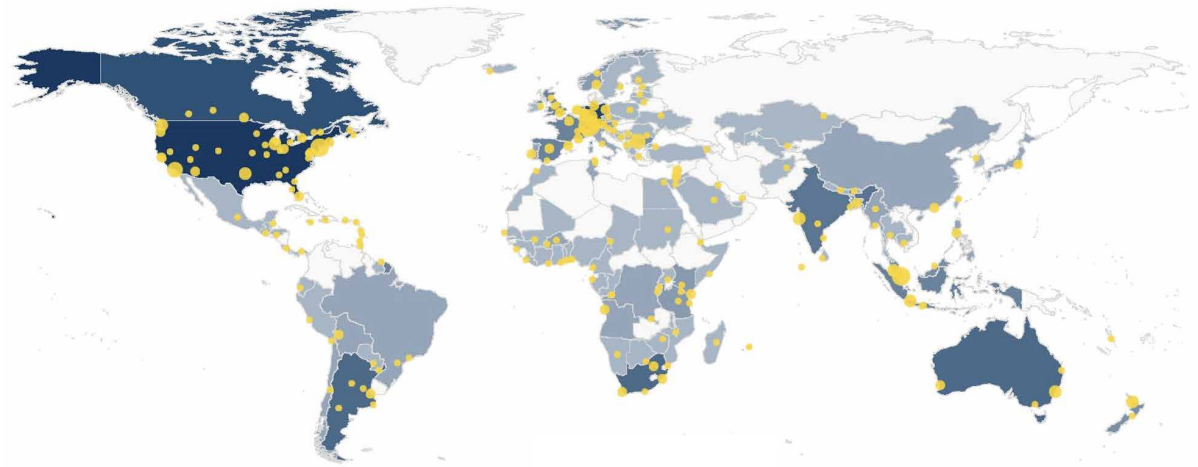
■ Chad

Onsite training, Technical
assistance

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 constituents, 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.



298 sites where PCH is available for peering

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 2023, PCH is available for peering at 298 IXPs worldwide and is one of the largest peering networks globally.

In 2023, PCH reached a total of:

26,304

IPv4 peering sessions

23,604

IPv6 peering sessions

4,843

Peer networks

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

Memorandum of Understanding

Formalizing Relationships

In late 2023, Packet Clearing House began building a portfolio of memoranda of understanding (MoUs) to formalize and document our long history of cooperation with partner intergovernmental and non-governmental organizations. An MoU is an agreement on cooperative projects that defines a form of mutual support within the framework of your activities. In these MoUs, fields of action and opportunities for new projects are identified and carried out.



To date, PCH has established MoU's for the following endeavors. We look forward to growing this list in 2024.

- **AICTO, the Arab ICT Organization**
- **FIRST, Forum of Incident Response and Security Teams**
- **Lesotho Communications Authority**
- **Polisync**
- **SGNIC, Singapore Network Information Center**
- **Smart Africa**
- **USSTI, United States Telecommunication Training Institute**

Sovereign Nations

Repatriating Their ccTLDs

The Domain Name System is the backbone of the Internet. Its resilience and security are essential. Internet content in broadband development, married with promotion and digital security, has brought increasing attention to country code top-level domains, especially as key points of control in the Internet for achieving policy objectives.

Unfortunately, it has been the practice, in some developing nations, that policymakers and regulators have not include the DNS in the development of their national strategic plans. In some cases lack of control of country code top level domains (ccTLDs) is a legacy of colonial relationships.



Where sovereign control is lacking, foreign individuals have swept in to manage the unclaimed ccTLDs for their own benefit and proven unresponsive to the country's Internet community. Such foreign interests profit from these countries' national assets and may compromise their reputations by using their ccTLDs to conduct abusive behavior.

ICANN Governmental Advisory Committee (GAC) representatives of several countries have raised their voices to recall their domain assets, knowing ccTLDs are a vital component of national strategic autonomy.

In 2023, PCH responded to three country requests to assist in repatriation of their national ccTLDs, from Guinea (.GN), Mali (.ML), and Gabon (.GB). PCH worked to ensure the stability, resiliency, and security required during such a process. The steps required included these:

- **Supporting the creation of the registry infrastructure**
- **Supporting DNSSEC signing on the local infrastructure**
- **Providing technical training on operation of the registry infrastructure**

PCH support also included the provision of strategic advice to policymakers and regulators to set up a multistakeholder governance model according to best practices needed to promote a national digital economy that serves the interests of national and international registrants.

Highlighted Partnerships

Building a Better Global Community



ICRC

The International Committee of the Red Cross (ICRC)

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.

AFRINIC
The Internet Numbers Registry for Africa



The Internet Numbers Registry for Africa (AFRINIC)

In 2022, PCH and AFRINIC, the regional Internet registry for Africa, signed an MoU aimed at strengthening the DNS infrastructure through the installation of PCH DNS nodes, which include two DNS root letters and a host of other critical DNS infrastructure. As part of this project, installations or upgrades were performed at six key locations across Africa, over the period 2022–2023. Additionally, PCH and AFRINIC staff undertook training sessions to equip local network operators with the necessary skills to manage and maintain their own DNS infrastructures effectively. These training sessions focused on best practices in DNS management, security, and debugging common problems, ensuring that the investments made have a lasting impact on the region's Internet stability and growth.



The International Internet Flow Quantification (IIFQ)

Since the privatization of the Internet in 1992, no holistic view of the international flows of Internet bandwidth has existed. Governments have little insight into the volumes and directions of international Internet traffic and thus no way of quantifying the relative significance of the other nations with which they exchange traffic. As of November 2023, 159 countries both produce and consume Internet bandwidth, and another 51 countries are consumers only. Understanding the balance of trade in Internet bandwidth helps governments set their ICT strategy.

The International Internet Flow Quantification (IIFQ) project provides a resource for this understanding. IIFQ produces time-series data characterizing international traffic flows, focusing on relative volumes of traffic exchanged between nations. This project is implemented in partnership with the OECD and the Swiss Research and Education Network (SWITCH). The project is in its initial stages, and will be further developed during 2024. For more information please see www.iifq.org.

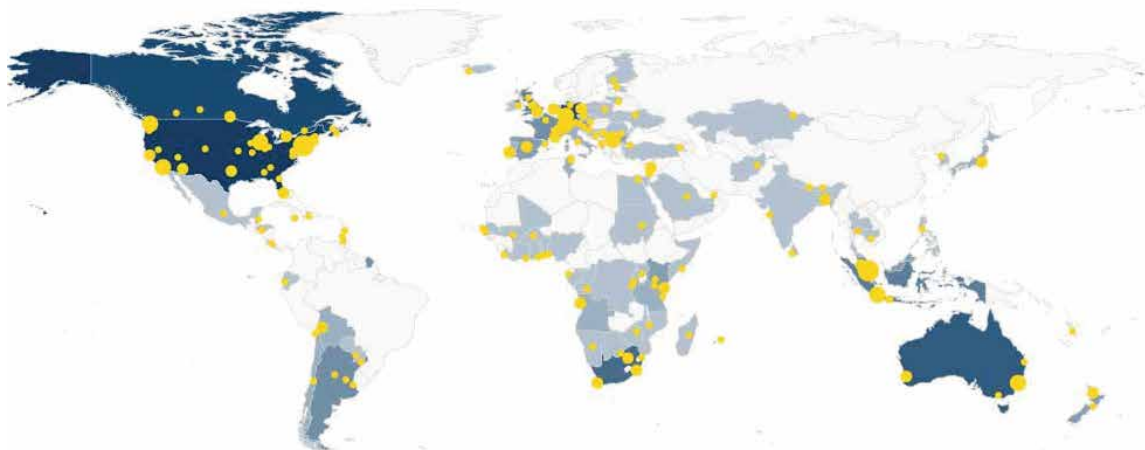
Highlighted Partnerships

Building a Better Global Community with **Quad9**

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.

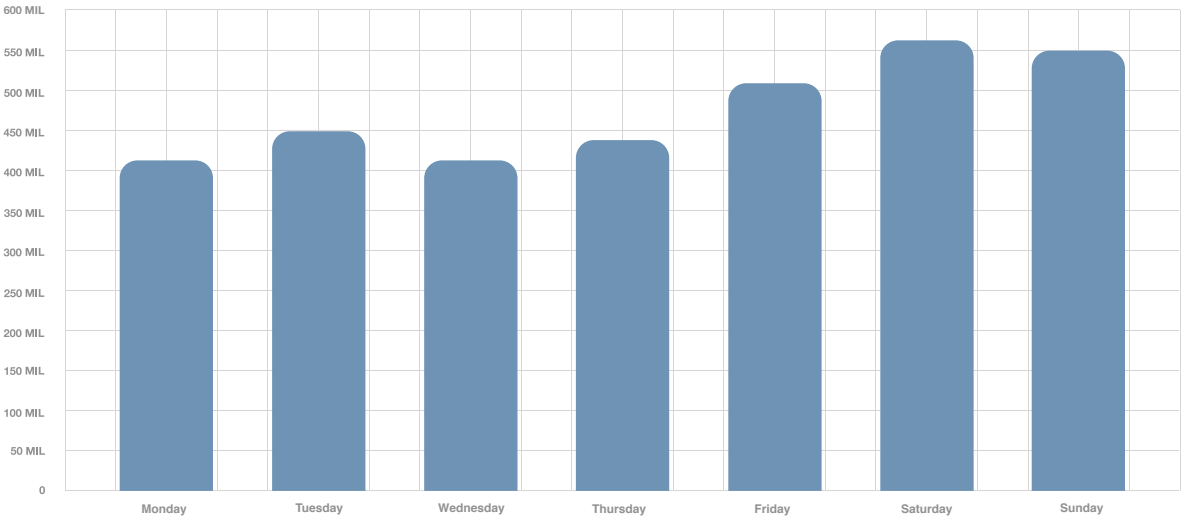
Network operators, commercial organizations, schools, hospitals, and end users can take advantage Quad9's recursive DNS services at no cost and with no contract. Configuration is simple and can be applied dynamically to all clients in a local network via centralized host management (DHCP) with no software 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 2023, 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 for bringing vital services to nations, regions, and networks.



200+ locations where PCH provides Quad9 services

Malicious events blocked per day



One representative week of quad9 blocking events

Quad9 currently 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, or other criminal activities. The majority of these events are processed on PCH-delivered network and co-location capacity.



Packet Clearing House

932 Parker St #3
Berkeley, California 94710
USA

+1 415 831 3100 main voice
+1 415 831 3101 fax

✉ info@pch.net

X www.x.com/PCHglobal

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