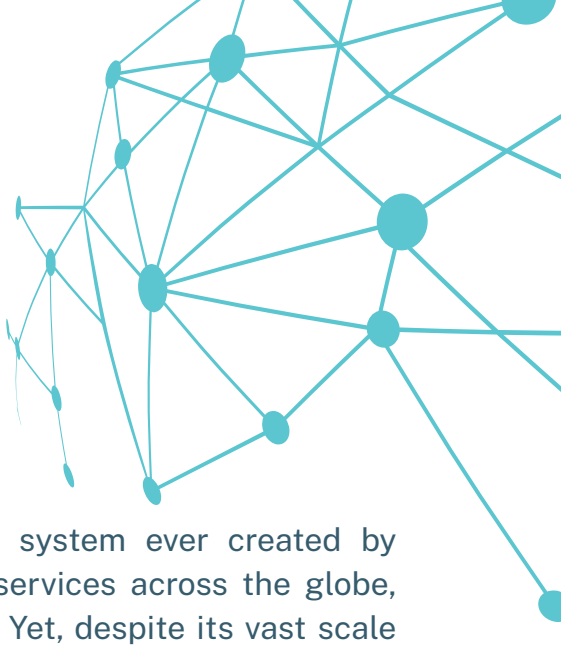
AIORI Internet Measurement Platform for Academia

https://portal.aiori.in

V1 | Aug 2025



Preface

The Internet is one of the largest and most complex system ever created by humankind. It connects billions of people, devices, and services across the globe, shaping how we communicate, learn, trade, and innovate. Yet, despite its vast scale and importance, the Internet is not a single centrally managed entity. It is a federation of thousands of networks that interconnect, evolve, and operate dynamically. This distributed and constantly changing nature makes the Internet both resilient and fragile — and it is precisely why measurement is so critical.

Internet measurement is the process of observing, testing, and analyzing the Internet's behavior. Just as doctors monitor a patient's vital signs to keep them healthy, Internet measurement helps us understand the "health" of the networked world. It uncovers bottlenecks, ensures resilience, and strengthens security. Measurement also plays a key role in policymaking, research, and education, guiding how the Internet adapts to new challenges such as cybersecurity threats, IPv6 adoption, cloud and edge computing, IoT, 5G, and quantum-safe cryptography.

The AIORI Internet Measurement Network (AIORI-IMN) was conceived in this spirit. India has long lacked a community Internet measurement platform that could be used across academia, industry, and government. AIORI-IMN fills this gap by providing a distributed, flexible, and secure system of Remote Endpoints (anchors), coordinated through a central platform. It enables users — from students to researchers — to perform measurements ranging from simple commands like ping and traceroute to advanced protocol-level experiments with DNSSEC, TLS, and BGP.

AIORI-IMN is more than a technical system. It is a learning platform designed to bring Internet measurement into classrooms and research labs. With its points-based educational model, students can conduct real-world measurements as part of their assignments, while faculty can monitor and guide their progress. In this way, the platform transforms theory into practice, allowing students to experience the Internet not just as users, but as explorers and innovators.

The project also aligns with global best practices. Initiatives such as MANRS (Mutually Agreed Norms for Routing Security) and KINDNS (Knowledge-Sharing and Instantiating Norms for DNS and Naming Security) highlight the importance of operational discipline for a safe and resilient Internet. Similarly, protocol-level enhancements like DNSSEC for domain name security and RPKI for routing security form the technical backbone of trust. AIORI-IMN contributes to this larger ecosystem by creating a platform where such protocols and best practices can be studied, tested, and deployed in real-world settings.

This book is the outcome of that vision. It combines Internet fundamentals, architectural insights, and hands-on usage of the AIORI-IMN platform. For students, it provides a guided path from the basics of TCP/IP to real experiments. For faculty, it offers a framework to design assignments and foster practical learning. For researchers and practitioners, it opens the door to deeper exploration of protocols, measurements, and security practices.

The Internet will continue to grow in scale and complexity, and with it, the importance of measurement will only increase. It is our hope that this book not only explains the design and use of AIORI-IMN, but also inspires a new generation of engineers, educators, and researchers to contribute to the future of the Internet — making it more secure, more resilient, and more inclusive for all.

How to read this book?

This book is not just a manual — it is an invitation to explore the Internet hands-on. Each chapter is designed to guide you step by step, from understanding the foundations of the Internet to conducting real measurements using the AIORI-IMN platform. Depending on whether you are a student, faculty member, or researcher, you can choose your own path through the chapters.

Here's a roadmap to help you:

Chapter 1: The Internet

Introduces the Internet's history, architecture, and working principles. Learn about TCP/IP layers, Autonomous Systems (ASNs), IXPs, DNS, and Internet governance structures. Perfect for students starting from fundamentals.

Chapter 2: The AIORI Internet Measurement Network Architecture

Explains the design philosophy and layered architecture of AIORI-IMN. Covers the roles of UI/Analytics, Controller, and Worker (Remote Endpoints). Useful for understanding how the platform is engineered.

Chapter 3: About the AIORI Internet Measurement Portal

Gives an overview of the national portal (v2.aiori.in), its objectives, and features for students, faculty, and researchers. A high-level view before diving into usage.

Chapter 4: Registration and Login

Step-by-step guide to registering as a user or faculty, logging in, and setting up accounts. Start here if you're a new user.

Chapter 5: Dashboard Widgets

Explains the portal dashboard: IP details, points balance, anchors, queries, and discussion forums. Learn how to navigate your workspace.

Chapter 6: Running Measurements

Shows how to execute measurements from maps or menus, select anchors, define zones, and set time ranges. This is your first hands-on experience with AIORI-IMN.

Chapter 7: PING

Dedicated to the Ping tool. Learn how to run single, zone-based, and time-range pings, and interpret reports in multiple formats (JSON, CSV, charts).

Chapter 8: DNS

Walks through DNS measurements, including DNS queries, DNS with PDM (RFC 8250), and interpreting JSON results. Builds on DNS theory from Chapter 1 with hands-on practice.

Chapter 9: TRACEROUTE

Explains how to perform traceroute measurements, analyze routing paths, and understand Internet topology through examples.

Chapter 10: Using Academic Feature

Covers the points-based learning system. Faculty can allocate points to students, create assignments, and monitor progress. Students use points to run queries and submit results. This chapter is essential for educational use cases.

Chapter 11: Hosting an Anchor

Provides a complete guide to deploying your own measurement anchor (using SBCs or VMs). Covers prerequisites, setup, registration, best practices, and monitoring. C

Tips for Readers

- If you are a student: Focus on Chapters 1–3 (concepts), 6–9 (hands-on tasks), and 10 (academic use).
- If you are a faculty member: Use Chapters 3, 5, 6, and 10 to manage classes and assignments.
- If you are a researcher or practitioner: Concentrate on Chapters 2, 7–11 for deeper insights into measurements and deployment.

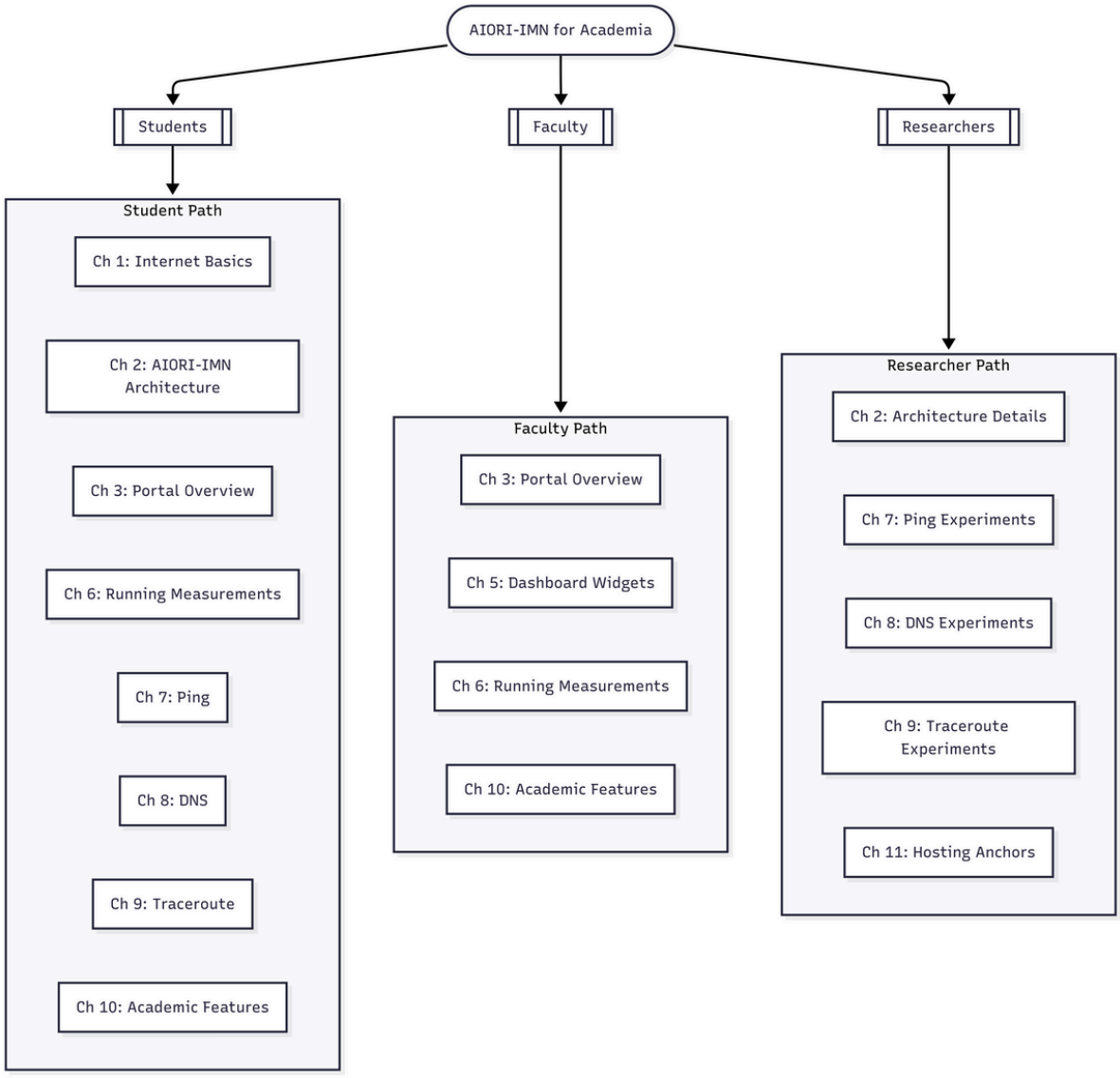


Table of Content

1. The Internet

1. Introduction

The Internet is a global network of networks that connects billions of devices and people. It powers communication, online learning, banking, shopping, entertainment, and even critical services like healthcare and transportation. For engineering students, understanding how the Internet works is essential because it forms the foundation of modern computing, networking, and cybersecurity. At the same time, the Internet is constantly evolving, built on protocols that were not originally secured by design, and today's society places an ever-increasing dependency on real-time, secure systems to keep everything from financial transactions to medical services running safely.

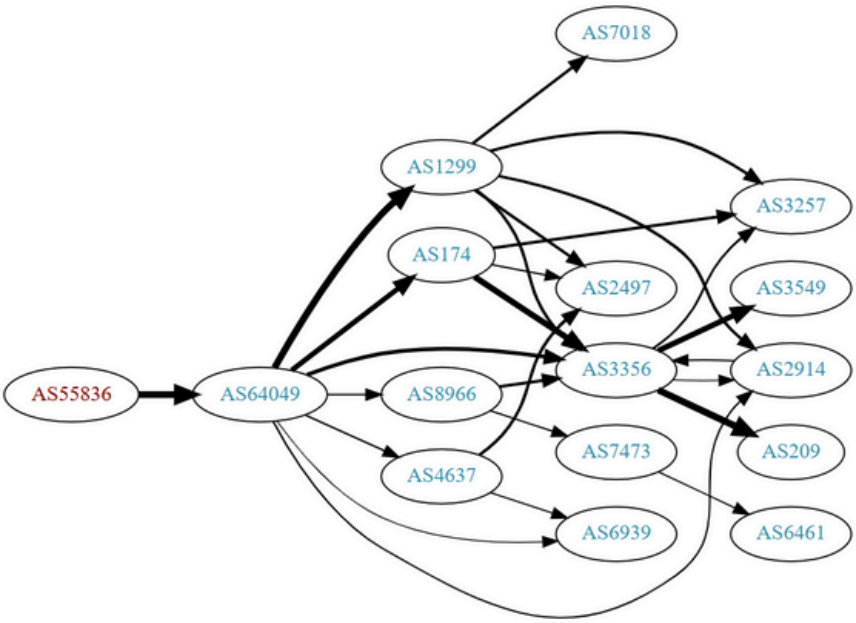


Figure 1: Source: https://bgpview.io/asn/55836#graph

The **Figure 1** shows how the Internet is built as a "network of networks" using Autonomous Systems (AS). Each AS is a large network, such as an Internet Service Provider, a university, or a content provider, and it is uniquely identified by an AS Number (ASN). In the figure, AS55836 (on the left) connects upstream to AS64049, which in turn peers with many other large ASes such as AS1299, AS174, and AS3356. The arrows represent routing relationships, and their thickness indicates the relative volume of BGP routes exchanged — thicker lines mean more prefixes (and typically stronger or more significant connectivity). You'll explore this topic in more depth in Section 5

2. Evolution of the Internet

- 1960s – ARPANET: Initially developed by the U.S. Department of Defense's ARPA as a research network to share computing resources.
- 1970s – Protocol Development: Vint Cerf and Bob Kahn introduced the TCP/IP protocol suite, which became the Internet's backbone.
- 1980s – Expansion: Universities and research institutions connected. Domain Name System (DNS) was introduced in 1983.
- 1990s – Commercialization: The World Wide Web (WWW), created by Tim Berners-Lee, popularized Internet use.
- 2000s–Today: The rise of broadband, mobile Internet, social media, cloud computing, and now the Internet of Things (IoT) and 5G.

3. Key Characteristics of the Internet

- Decentralized architecture – No single entity owns or controls it entirely.
- Interoperability – Devices and networks communicate using standard protocols (e.g., TCP/IP, HTTP, DNS).
- Scalability – Can grow to accommodate billions of devices.
- Resilience – Designed to survive failures by rerouting traffic.
- Openness – Anyone can innovate, deploy services, and connect.

4. Internet Architecture

The Internet is built on a layered architecture, often aligned with the TCP/IP model:

- Application Layer: Services such as HTTP, DNS, SMTP, FTP, VoIP.
- Transport Layer: Reliable data delivery (TCP), faster datagram service (UDP).
- Internet Layer: IP addressing and routing (IPv4, IPv6) BGP (ASN).
- Network Access Layer: Physical and data link technologies (Ethernet, Wi-Fi, 5G).

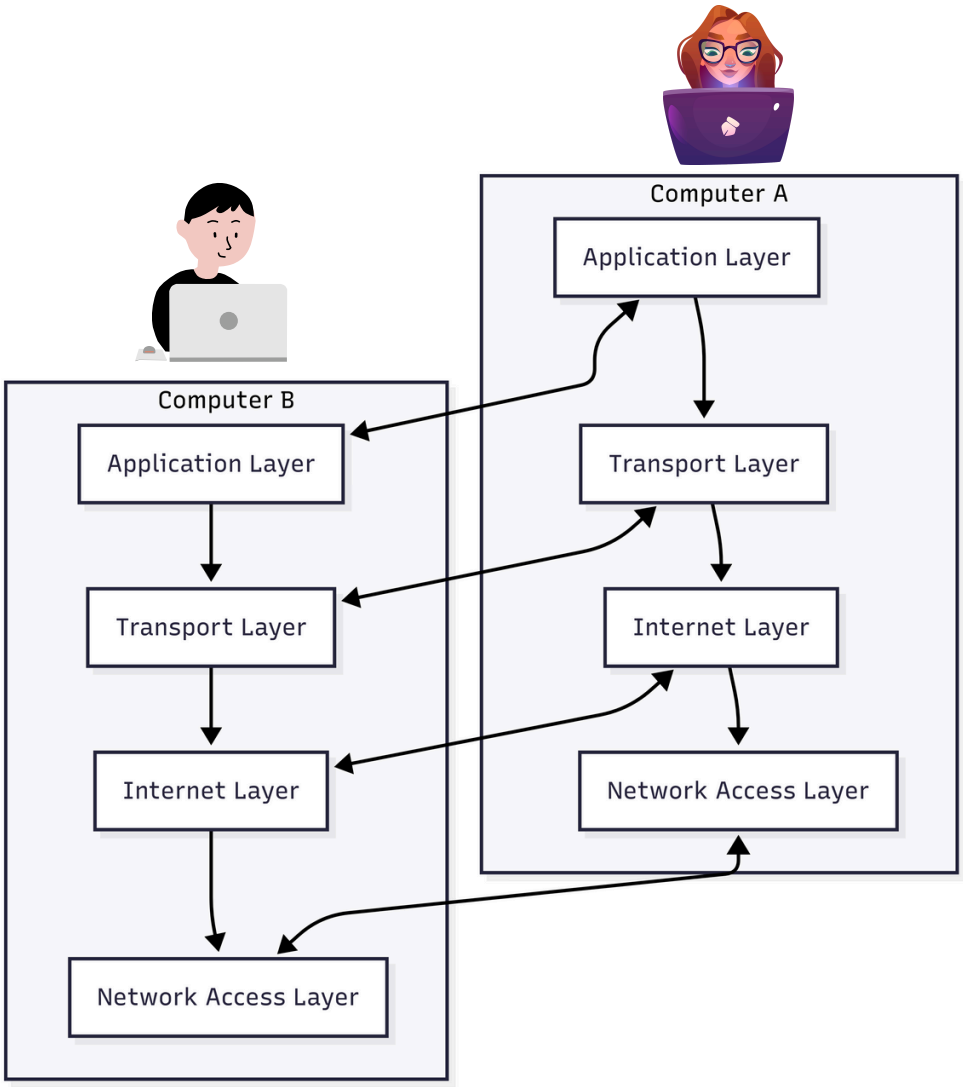


Figure 2: The TCP/IP Network Stack

This diagram illustrates the TCP/IP layered model in action between two computers communicating over the Internet. Each computer has four layers — Application, Transport, Internet, and Network Access. When Computer A sends a message (for example, a student sending an email using Gmail), the message originates in the Application Layer (email client). It is then passed down to the Transport Layer (where TCP ensures reliability and segments the data), then to the Internet Layer (where the message is given the destination IP address), and finally to the Network Access Layer (which actually transmits the data across the physical network, like Wi-Fi or Ethernet). The message travels over the Internet to Computer B. On arrival, the process works in reverse: the Network Access Layer receives the bits, the Internet Layer ensures they're addressed correctly, the Transport Layer reassembles the message in order, and finally, the Application Layer delivers it to the email program so the recipient can read it.

In short, this layered approach ensures that even though applications like Gmail, WhatsApp, or Zoom differ, they can all reliably communicate because each layer of the Internet protocol stack handles its own responsibility independently.

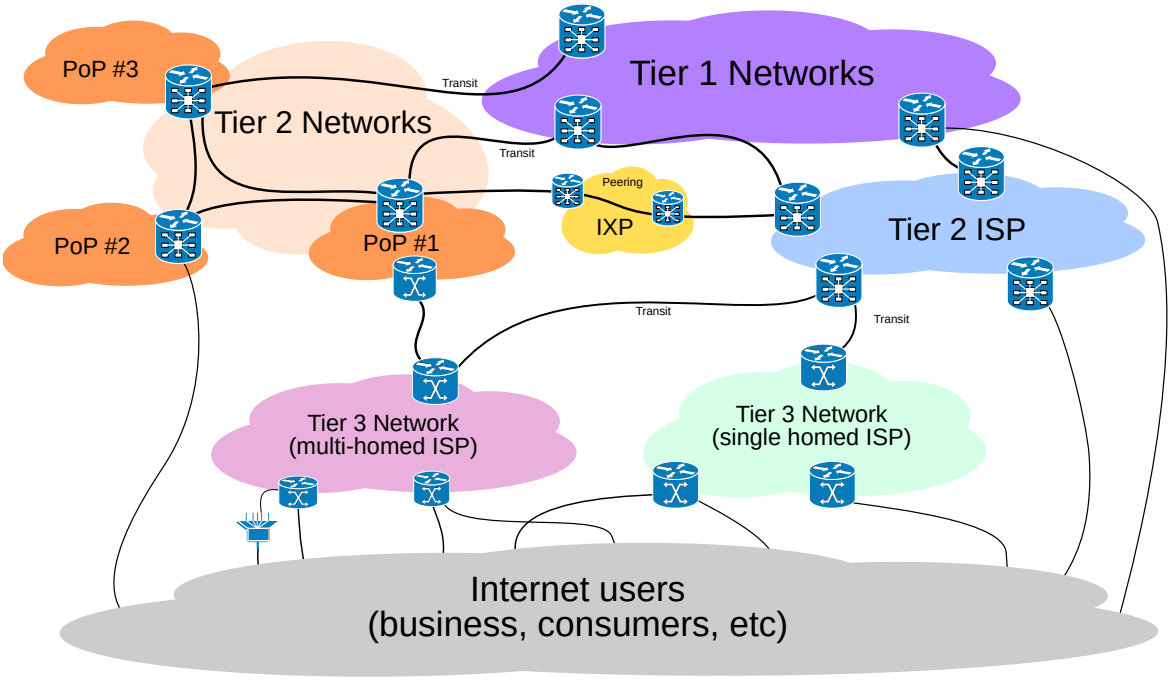


Figure 3: By Ludovic.ferre - Internet Connectivity Distribution&Core.svg, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=10030716

The layered Internet diagram shows how connectivity is structured from the end-users at the edge to the global Internet core. At the bottom, individual users connect through local access networks such as Wi-Fi, mobile networks, or broadband. These local networks link into regional Internet Service Providers (ISPs), which aggregate traffic from thousands or millions of customers. Multiple regional ISPs then interconnect with national or international ISPs, forming a larger fabric of networks. At the top are the Internet core networks and exchange points, including major Internet Exchange Points (IXPs) and Tier-1 backbone providers, where vast amounts of global traffic are exchanged. This hierarchical layering ensures scalability: end-users don't connect directly to the entire Internet, but instead rely on a chain of providers and exchanges to carry their data. It also explains the Internet's resilience — if one path fails, routing protocols like BGP can redirect traffic through alternative connections across different layers.

5. Numbers and Names of Internet

5.1 Numbers (IPv4, IPv6, ASN)

The Internet is often described as a “network of networks”. Instead of being a single unified system, it is composed of thousands of interconnected networks run by Internet Service Providers (ISPs), enterprises, universities, governments, and content providers. These networks exchange traffic using BGP having unique identifiers Autonomous System Numbers (ASNs).

Every device or network on the Internet needs a unique identity to communicate, and this is done using IP addresses (like a digital postal address) and (used by large networks such as ISPs, universities, or companies). These identifiers are not randomly chosen — they are carefully assigned to ensure global uniqueness.

5.2 IANA, RIRs and NIRs helps managing unique identifiers

At the highest level, the global pool of IP addresses and Autonomous System Numbers (ASNs) is managed by the Internet Assigned Numbers Authority (IANA), which operates under ICANN. IANA is responsible for maintaining the master registries of these resources and then distributing large blocks to the five Regional Internet Registries (RIRs):

- APNIC (Asia-Pacific),
- RIPE NCC (Europe, Middle East),
- ARIN (North America),
- LACNIC (Latin America/Caribbean), and
- AFRINIC (Africa).

In some countries, National Internet Registries (NIRs) further allocate addresses and ASNs locally on behalf of their RIR — for example, **IRINN in India** works under APNIC. From there, ISPs, universities, enterprises, and organizations receive their allocations, which are finally assigned to end users and devices. This top-down structure (IANA → RIRs → NIRs → ISPs/organizations → users) ensures uniqueness, fairness, and global coordination so that no two networks accidentally use the same IP space or ASN.

5.3 Names of Internet

On the Internet, names are human-friendly identifiers that we use to access websites, applications, and services—like google.com or iitg.ac.in. Names are important because people find them much easier to remember and use than long strings of numbers called IP addresses (e.g., 2404:6800:4007:80f::200e for Google). Just as we use names for people, places, or objects in daily life to make communication simple, names on the Internet make it possible for users to navigate the digital world without worrying about technical details. The Domain Name System (DNS) is the system that manages these names and translates them into the underlying IP addresses that computers need to connect with each other. This translation is what allows you to type a name in your browser and instantly connect to the right server anywhere in the world. For students, understanding DNS begins with recognizing that names are the bridge between people and the technical Internet, making it accessible, usable, and meaningful in everyday life.

5.4 DNS (Domain Name System)

The Domain Name System (DNS) is a hierarchical and distributed system that stores information in the form of resource records (RRs) such as A, AAAA, MX, and TXT. At the top of the hierarchy sit the root servers, run by 12 organizations as 13 logical identities, with more than 1900 Anycast instances worldwide to ensure resilience and low latency. Beneath the root are Top-Level Domains (TLDs), including country-code TLDs (ccTLDs) like .in or .uk and generic TLDs (gTLDs) each delegated to authoritative servers for their zones. Recursive resolvers act on behalf of users, querying the hierarchy step by step—from root to TLDs to authoritative servers—to fetch the needed records. To protect integrity and prevent tampering, DNSSEC adds cryptographic signatures to the data.

Because DNS is the backbone of almost every Internet activity, measurement of DNS is equally important. Measuring availability, latency, query success, Anycast performance, and DNSSEC validation helps identify misconfigurations, attacks, and bottlenecks. It also ensures that users receive fast, secure, and reliable responses worldwide. In short, DNS is a decentralized, cooperative system, and continuous measurement is vital to keep it robust, trustworthy, and resilient for billions of daily users.

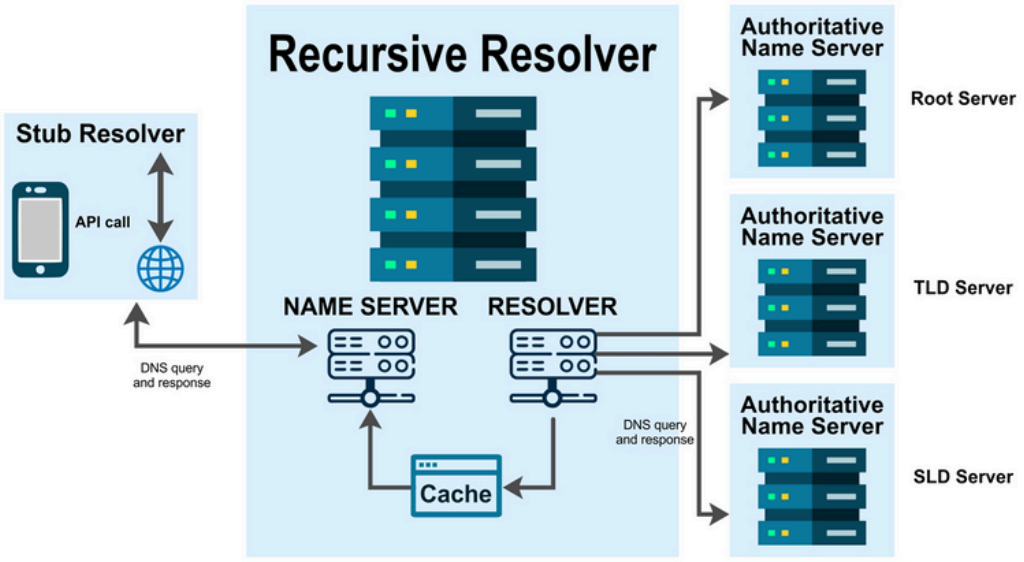


Figure 4: THE DNS

In addition to servers, the Domain Name System (DNS) also relies on several key stakeholders who manage how domain names are created, sold, and maintained:

- **Registry:** The organization that operates a Top-Level Domain (TLD). For example, Verisign operates .com and .net, while NIXI operates .in. A registry maintains the authoritative database of all domain names under its TLD and ensures their proper functioning.
- **Registrar:** Companies accredited by the registry that sell domain names to the public (e.g., GoDaddy, Namecheap, BigRock). They provide the interface for end users to search for, purchase, and manage domain names, acting as intermediaries between registries and registrants.
- **Registrant:** The end user or organization that registers a domain name (e.g., you registering mywebsite.in). The registrant chooses the domain name, pays the registrar, and configures the authoritative DNS servers that control how the domain resolves.
- **ICANN (Internet Corporation for Assigned Names and Numbers):** A global, non-profit body that coordinates the DNS at the top level. ICANN oversees the policies for TLD management, accredits registrars, and ensures the overall stability, security, and interoperability of the DNS. It does not sell domain names directly but ensures that registries, registrars, and root servers all operate under a consistent global framework.
- Together, these stakeholders form the governance and operational ecosystem of DNS, ensuring that when you type a domain name, it can be resolved reliably anywhere in the world.

5.5 Root Servers

When the Internet began transitioning from ARPANET in the 1980s, the DNS was introduced to replace the cumbersome hosts.txt file. To make DNS queries scalable, a small set of root servers was created in 1985 to hold the “root zone file” (the starting point of all DNS lookups).

By design, the DNS protocol limited responses to 512 bytes (due to early UDP constraints). This meant that only 13 root server addresses (A through M) could be reliably published in the root zone. These became known as the “13 Root Servers”, though each represents a logical identity, not a single machine.

Today, these 13 logical servers are run by 12 independent organizations (such as Verisign, ICANN, RIPE NCC, ISC, NASA, University of Maryland, etc.). Geographically, the original placements were 10 in the USA, 2 in Europe, and 1 in Japan — a reflection of the Internet’s early history. Over time, Anycast technology has expanded these into 1900+ physical instances worldwide, bringing the root closer to users everywhere.

List of Root Servers

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	170.247.170.2, 2801:1b8:10::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Figure 5: https://www.iana.org/domains/root/servers

5.6 Example Walkthrough: Query for icann.org

1. You type icann.org in a browser.
2. The browser asks the recursive resolver.
3. The resolver checks its cache; if not found, it queries a Root Server, which replies with the address of the .org TLD servers.
4. The resolver asks the .org TLD server, which responds with the authoritative server for iifon.org.
5. The resolver queries the authoritative server, which returns the IP address.

Finally, your browser connects to the IP address to load the website.

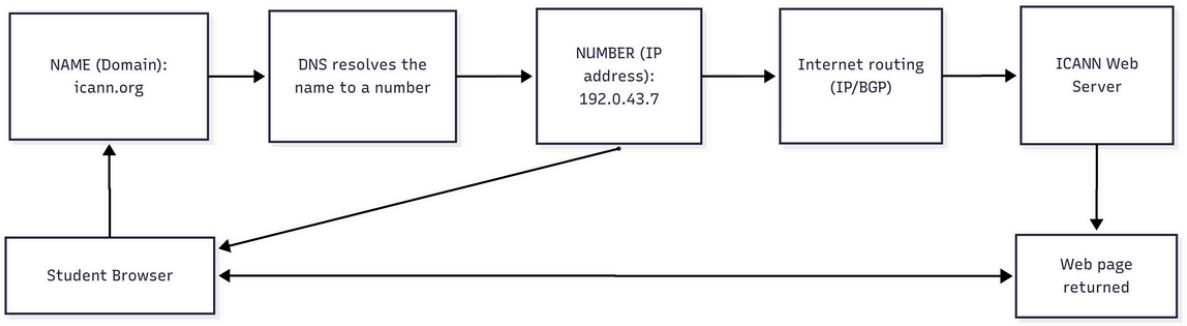


Figure 6: The DNS Walkthrough

5.7 Internet Exchange Points (IXPs)

- An Internet Exchange Point (IXP) is a physical infrastructure where multiple networks (ISPs, content providers, CDNs) meet to exchange traffic locally.
- IXPs reduce dependence on international transit providers, cut costs, and improve latency.
- Example: At an IXP in India, two ISPs can exchange traffic directly instead of routing it via Singapore or Europe.
- IXPs are critical for regional Internet resilience and play a major role in data localization.

5.7 Submarine Cables

Submarine cables are the hidden backbone of the global Internet, carrying over 95% of international data traffic across oceans. These are fiber-optic cables laid on the seabed, stretching thousands of kilometers, and connecting continents to enable fast communication, cloud services, banking, video streaming, and everyday Internet use. Each cable contains multiple optical fibers that transmit data as pulses of light at near the speed of light, with repeaters placed every 50–100 km to boost signal strength. Submarine cables are crucial because satellites, while useful, cannot match their capacity, reliability, and low latency. They are owned and operated by consortia of telecom companies, governments, and increasingly by big tech firms like Google, Meta, and Microsoft. For students, submarine cables are important to understand as they highlight the physical and geopolitical foundations of the Internet—they are vulnerable to natural disasters, anchor drags, or even sabotage, and disruptions can severely impact a country's Internet connectivity and economy.

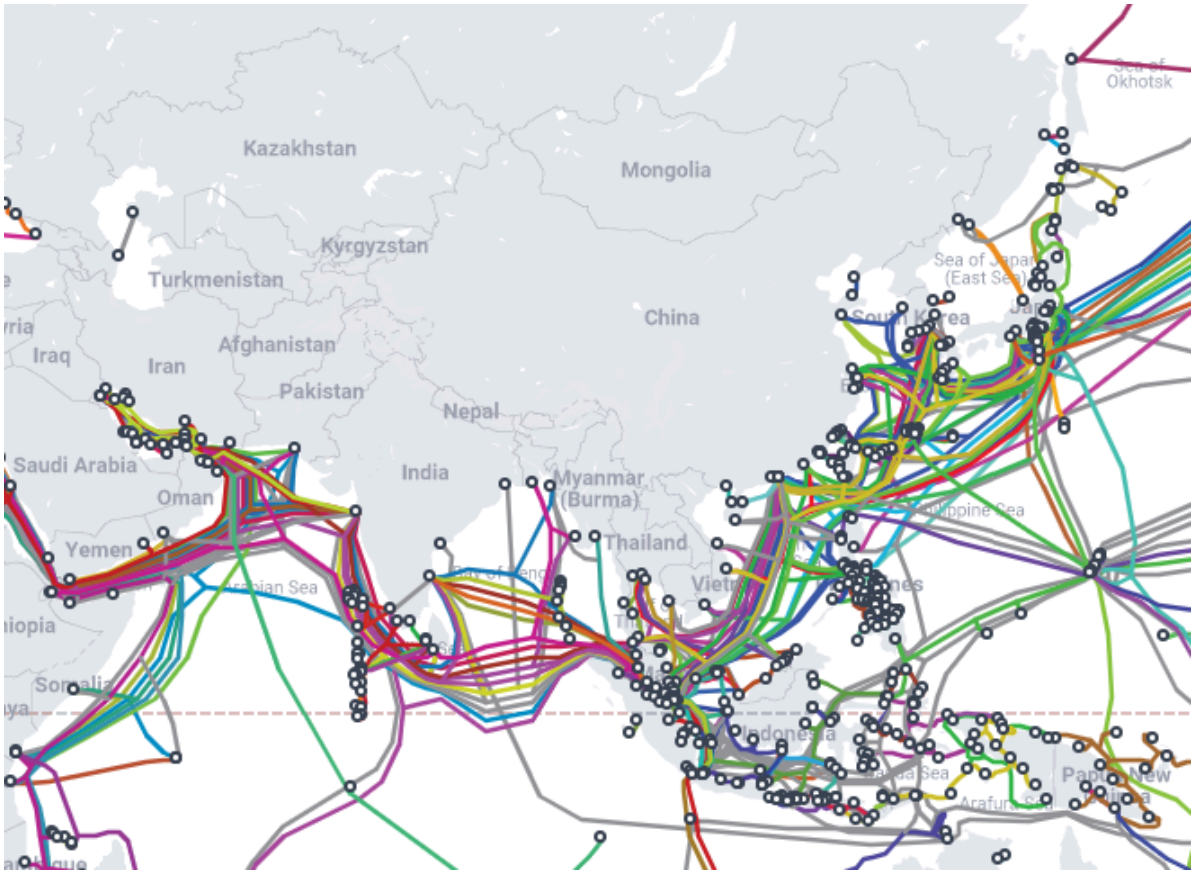


Figure 7: Source - https://www.submarinecablemap.com/

5.7 Low earth Orbit Satellites

Low Earth Orbit (LEO) satellites are satellites that orbit the Earth at relatively low altitudes, typically between 500 km and 2,000 km above the surface. Because they are much closer to Earth than traditional geostationary satellites, LEO satellites can provide faster Internet connectivity with lower latency (signal delay), making them especially useful for real-time applications like video calls, online gaming, and remote education. Thousands of LEO satellites can work together in a constellation to cover the entire globe, ensuring even remote or rural areas have access to the Internet. Projects like Starlink, OneWeb, and Amazon's Kuiper are building such constellations to bring high-speed Internet to underserved regions. For students, LEO satellites are important to study because they represent how space technology, communication networks, and innovation are shaping the future of a more connected world, while also raising questions about space traffic, debris management, and global digital inclusion.

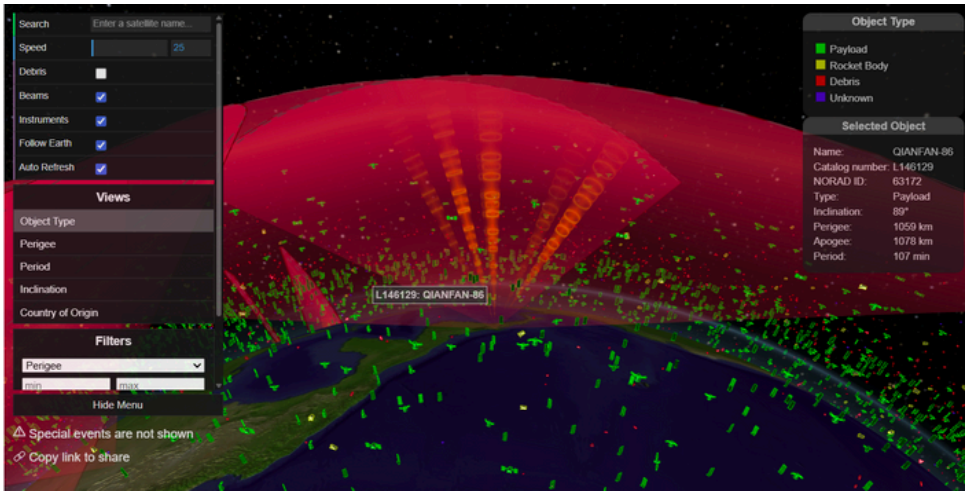


Figure 8: https://platform.leolabs.space/visualization

Measuring Low Earth Orbit (LEO) satellites is important to verify how well they deliver low-latency Internet services, since their proximity to Earth promises faster response times compared to geostationary satellites. Continuous measurement helps track coverage gaps and signal quality, ensuring that rural and remote areas actually receive stable connectivity. Because LEO satellites move rapidly, performance monitoring is essential to study handover events, where user connections shift from one satellite to another, and to detect any service disruptions. Measurements also provide data on packet loss, throughput, and jitter, which are critical for applications like video calls, online education, or gaming. Finally, keeping accurate measurements supports safety and sustainability, as it contributes to monitoring orbital congestion, preventing collisions, and comparing LEO performance with traditional infrastructures like submarine cables.

6. Internet Security

The Internet was originally designed in the 1970s for a small community of trusted researchers. At that time, security threats like hacking, phishing, or DDoS attacks were not anticipated. As a result, the Internet's core protocols (IP, DNS, BGP) were built for connectivity and resilience, not for security. Over time, as the Internet became the backbone of society, we had to add security "patches" and extensions to protect communication, data, and users.

6.1 DNSSEC (Domain Name System Security Extensions)

- DNS was designed without authentication — meaning attackers could forge DNS responses (DNS spoofing).
- DNSSEC was added to provide cryptographic signatures for DNS data, ensuring users can verify that a DNS response is authentic and not tampered with.

6.2 RPKI (Resource Public Key Infrastructure)

- The Border Gateway Protocol (BGP) that connects Autonomous Systems was designed without security, making it vulnerable to BGP hijacks.
- RPKI allows network operators to cryptographically verify that an AS is authorized to announce a specific IP prefix, preventing route leaks and hijacks.

6.3 SSL/TLS (Secure Sockets Layer / Transport Layer Security)

- Originally, HTTP traffic was unencrypted, meaning anyone could eavesdrop.
- SSL/TLS added encryption and authentication, creating HTTPS for secure web browsing, online banking, and e-commerce.

6.4 IPsec (Internet Protocol Security)

- The original IP protocol had no security features.
- IPsec adds encryption and authentication at the network layer, enabling secure tunnels between two endpoints (widely used in VPNs).

6.5 VPN (Virtual Private Network)

- A VPN uses IPsec or TLS to create an encrypted “tunnel” across the Internet, protecting user data from surveillance and allowing safe access to private networks.

6.6 IPv6 Security Improvements

- While IPv6 was mainly designed to expand the address space, it also integrates better support for IPsec, neighbor discovery security, and improved packet handling compared to IPv4.

6.7 Email Security

Email protocols such as SMTP, POP3, and IMAP were originally designed without encryption or authentication, making them easy to intercept or spoof. Several security mechanisms have since been added:

- STARTTLS: Adds transport-layer encryption to email delivery.
- S/MIME (Secure/Multipurpose Internet Mail Extensions): Provides end-to-end encryption and digital signatures for emails.
- PGP (Pretty Good Privacy): Allows users to encrypt and sign emails independently using public/private keys.
- SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting & Conformance): Protect against email spoofing and phishing by verifying that emails come from authorized servers.

7. Internet Security Operational Best Practices

7.1 MANRS (Mutually Agreed Norms for Routing Security)

MANRS is a global initiative originally supported by the Internet Society and now operated by the Global Cyber Alliance. It builds on best practices to secure Internet routing by rallying ISPs, IXPs, CDNs, cloud providers, and equipment vendors around a shared framework

.

Key actions defined by MANRS include:

- Filtering: Ensuring that only valid IP prefixes and AS paths are announced
- Anti-Spoofing: Preventing packets with forged source addresses
- Coordination: Publishing up-to-date contact information for incident response
- Global Validation: Making routing data available to others for verification

MANRS also supports operational compliance via the MANRS Observatory, which monitors routing security metrics across networks

More Details: https://manrs.org

7.2 KINDNS (Knowledge-Sharing and Instantiating Norms for DNS and Naming Security)

An ICANN-supported initiative designed to help DNS operators (authoritative and recursive) implement essential, easy-to-adopt security practices . This initiative:

- Identifies a small set of mutually agreed best practices that any operator — big or small — can implement to improve DNS security and operational resilience.
- Offers voluntary self-assessment tools and dashboards, enabling operators to evaluate their current practices and commit as "goodwill ambassadors" to continuous improvement

Engages the global DNS community through feedback loops, webinars, assessments, and localized outreach, aiming to grow adoption and refine practices over time.

8. Internet Organizations

The Internet works because many independent organizations collaborate globally to maintain its naming, numbering, standards, and governance. Here are some of the most important ones students should know:

ICANN (Internet Corporation for Assigned Names and Numbers)

- A non-profit organization responsible for coordinating the Domain Name System (DNS) and ensuring that every domain name and IP address is unique.
- Oversees domain registries (like .com, .org, .in) and accredits registrars.
- Coordinates global Internet governance with a multistakeholder approach.

IANA (Internet Assigned Numbers Authority)

- A function operated by ICANN that manages the global allocation of IP address blocks, AS Numbers, DNS Root Zone, and protocol parameters.
- Think of it as the top of the “naming and numbering” hierarchy.

PTI (Public Technical Identifiers)

- An affiliate of ICANN that performs the IANA functions (technical operations for IP addresses, DNS root zone management, and protocol parameter registries).
- Provides the operational backbone for IANA’s responsibilities.

ISOC (Internet Society)

- A global non-profit that promotes an open, globally connected, secure, and trustworthy Internet.
- Supports Internet standards development (especially through IETF), capacity-building, and initiatives like MANRS (routing security).

IETF (Internet Engineering Task Force)

- An open global community of engineers, researchers, and developers who create and maintain the technical standards that make the Internet work (like TCP/IP, HTTP, DNS, BGP).
- Publishes standards as RFCs (Request for Comments).

RIRs (Regional Internet Registries)

- There are 5 RIRs worldwide (APNIC, RIPE NCC, ARIN, LACNIC, AFRINIC).
- They manage the allocation of IP addresses and AS Numbers in their regions.

APNIC (Asia-Pacific Network Information Centre)

- The RIR for the Asia-Pacific region.
- Allocates IP addresses and ASNs to ISPs, universities, and organizations in Asia-Pacific countries.
- Provides training, security initiatives, and Internet measurement services.

NIXI (National Internet Exchange of India)

- A not-for-profit company under the Government of India.
- Operates Internet Exchange Points in India (to keep domestic Internet traffic local), the .IN ccTLD registry, and the IRINN (Indian Registry for Internet Names and Numbers).

IRINN (Indian Registry for Internet Names and Numbers)

- An NIR (National Internet Registry) under APNIC.
- Allocates IP addresses and AS Numbers within India.
- Helps Indian ISPs and organizations with Internet number resources at the national level.

9. Importance of Measuring the Internet

The Internet is a dynamic, ever-changing system. Unlike traditional infrastructures such as electricity grids or highways, it is not centrally managed. Instead, it is a federation of thousands of independent networks. To keep it reliable, secure, and efficient, engineers and researchers must continuously measure the Internet.

9.1 Ensuring Performance and Quality of Service

- Measurement of latency, packet loss, and bandwidth helps ensure smooth online activities such as video calls, cloud applications, and streaming.
- It identifies congestion points and supports network optimization.

9.2 Diagnosing and Fixing Problems

- Tools like ping, traceroute, and DNS show where delays or failures occur along a path.
- Measurement allows engineers to detect misconfigurations, outages, or inefficient routing paths.

9.3 Security and Resilience

- Measurement detects incidents such as BGP hijacks, route leaks, or DDoS attacks.
- Monitoring DNS traffic helps guard against cache poisoning and other manipulations.

9.4 Planning and Policy Making

- Regulators and policymakers rely on Internet measurement to assess coverage, digital divide, and readiness for new technologies such as IPv6 and 5G.
- Measurement data supports informed governance and investment decisions.

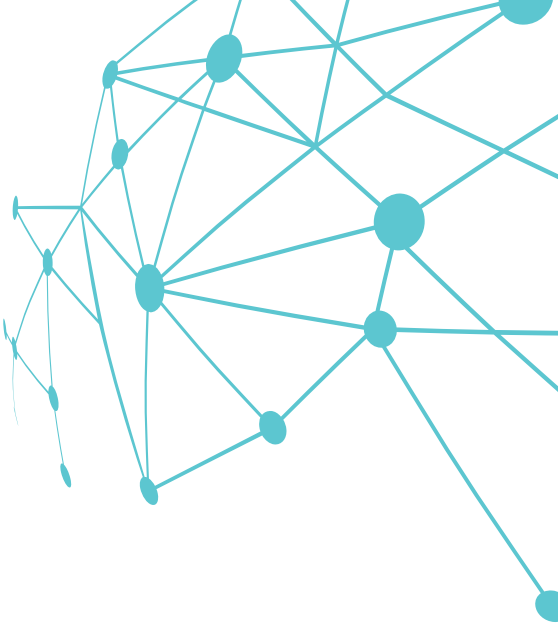
9.5 Research and Innovation

- Measurement provides the ground truth for testing new protocols and architectures.
- Innovations like advanced congestion control, secure DNS extensions, or routing security (RPKI, BGPsec) are validated through real-world measurements.

9.6 Example for Students:

If a student in Chennai tries to access a website hosted in the U.S., measurements can reveal the end-to-end latency, which networks are in path, whether the ISP routes traffic efficiently, and how CDNs reduce delay by caching content locally.

Without measurement, the Internet is a “black box.” Measuring it transforms it into a “glass box,” allowing engineers to see inside and improve its performance, security, and resilience.



2. AIORI-IMN Architecture

1. Introduction

Measuring the Internet has become increasingly critical to guide its continued growth and evolution. The Internet is not controlled by a single entity; instead, it functions through the combined efforts of multiple stakeholders such as ISPs, governments, academic institutions, and content providers. While many of these stakeholders operate their own measurement systems to manage their infrastructure or services, India has lacked a community Internet measurement platform that could serve all stakeholders collectively. Such a platform would provide a holistic view of the "network of networks", enabling better troubleshooting, optimization, analytics, and planning for the Internet's future.

During our research into current and future requirements, we found that protocol data (the structured information exchanged between devices following specific standards) and protocol metadata (the additional descriptive details that provide context about communication) are becoming increasingly encrypted. Encryption converts readable information into an unreadable form to protect it from unauthorized access, but it also makes it harder to measure and analyze network behavior. To overcome this challenge, it was essential to design a measurement system where both ends of communication (client and server) are part of the AIORI Internet Measurement Network (AIORI-IMN). This allows us to dig deeper into how the Internet behaves under different conditions.

Another key insight was the rise of edge devices — such as smartphones, IoT sensors, and autonomous systems — which are becoming powerful compute engines. This means that measurements must happen at different levels of deployment, from home networks to ISP backbones and cloud infrastructures. At every stage, privacy and security were made a top priority in the design of AIORI-IMN, ensuring that while the Internet is studied in depth, user data and trust remain protected.

With these foundations, the AIORI-IMN can serve not only today's Internet but also emerging applications like smart homes, autonomous vehicles, robotics, and other next-generation deployments.

2. Background: Internet Measurement Projects

The Internet has grown and evolved because of the combined efforts of many people and organizations worldwide. One important way this happens is through Internet measurement projects. These projects continuously study different aspects of how the Internet works — such as speed, reliability, routing, security, and traffic patterns. The information they provide helps researchers, operators, and policymakers make the Internet faster, safer, and more resilient.

In 2015, researchers Vaibhav Bajpai and Jürgen Schönwälder published a well-known survey paper titled "A Survey on Internet Performance Measurement Platforms and Related Standardisation Efforts", which reviewed the major Internet measurement platforms of that time. Since then, many new projects have been launched around the world, each focusing on different aspects of Internet performance and security. These projects have become catalysts for innovation, providing data that helps engineers and researchers shape the future Internet.
Some of the important Internet measurement projects across the world are shown in the table below:

Project	Region	Started	URL
AIORI-IMN	India	2022	aiori.in
Internet Society Pulse	Global	2020	pulse.internetsociety.org
MANRS Observatory	Global	2019	observatory.manrs.org
CAIDA MANIC	USA	2014	caida.org/projects/manic
RIPE Atlas	Europe	2010	atlas.ripe.net
ITZ (Internet Topology Zoo)	Asia-Pacific	2010	topology-zoo.org
Science DMZ	USA	2010	fasterdata.es.net/science-dmz
BGPmon	USA	2008	bgpmon.netsec.colostate.edu
Ark (CAIDA)	USA	2007	caida.org/projects/ark
Arbor ATLAS	USA	2007	atlas.arbor.net
iPlane	USA	2006	iplane.cs.washington.edu
PeeringDB	USA	2004	peeringdb.com
DIMES	Asia-Pacific	2004	NetDimes GitHub
RIPE DNSmon	Europe	2003	atlas.ripe.net/dnsmon
APJ MAWI	Asia-Pacific	2002	mawi.wide.ad.jp
US Network Telescope	USA	2002	caida.org/projects

Table 1: Internet Measurement Projects

3. Measuring the Internet: Tools and Tasks

There are many ways to measure how the Internet works and how well it performs. Two of the most basic tools are:

- Ping: This sends a small packet of data to a server and measures how long it takes for the reply to come back. It's like shouting "hello" and waiting to hear "hello" back — the time taken is the latency. You can try this yourself on any computer using the ping command in the terminal or command prompt.
- Traceroute: This traces the exact path that data takes from your computer to the destination, showing all the routers (called "hops") it passes through. It also measures the delay at each hop. This can be run using the traceroute (Linux/macOS) or tracert (Windows) command.

The AIORI Internet Measurement Network (AIORI-IMN) makes it possible to run these kinds of measurement tasks from Remote Endpoints (REs) deployed at different user locations. Students and researchers can schedule these tasks to run once or over a period of time. The collected raw data is processed by an Analytics and Visualization engine, which helps study the Internet's performance, stability, and security over the long term.

- Categories of Measurement Tasks in AIORI-IMN
- Command-based tasks – like ping and traceroute
- Protocol-based tasks – using ICMP, DNS, DNSSEC, HTTP, TLS, etc.
- Standards-based tasks – testing new Internet protocols from recently published IETF RFCs

Each type of task requires different levels of computing power and memory. A detailed analysis of these requirements is part of ongoing and future research.

The reference implementation of AIORI-IMN is available at https://v2.aiori.in, and the platform's capabilities have been explained in detail with real-world results in the IEEE paper "The Internet Measurement Network (AIORI-IMN)".

4. Goal and Architecture of AIORI-IMN

The main goal of AIORI-IMN was to design and develop a distributed Internet measurement network with edge-based Remote Endpoints (REs). These endpoints can run measurement tasks, while a central platform coordinates them and provides tools for analytics and visualization of protocol metrics.
When designing the architecture, we considered two sets of attributes:

Qualitative Attributes (how the system should behave):

- Optimized bandwidth usage – so measurements do not overload the network
- Interoperability – able to work with other systems and platforms
- Secure by design – ensuring privacy and protection from the start
- Resilience (always available) – the platform should continue functioning even if some nodes fail

Functional Attributes (what the system should be able to do):

- Perform active measurements such as ping, traceroute, or DNS tests
- Measure from both edge devices (clients) and servers
- Support easy deployment of new protocols to collect data and metadata
- Allow scheduling tasks across multiple REs for defined time periods

After studying different possibilities, we finalized a Distributed Edge Computing Architecture. This design allows easy integration with other systems, flexibility for testing new protocols, scalability, and measurement at different levels (edge, ISP, core). These features make AIORI-IMN more flexible than many existing platforms.

5. High-Level Architecture

Remote Endpoints (REs): These are edge nodes that can be deployed on Virtual Machines (VMs) or Single Board Computers (SBCs) like Raspberry Pi. They can act as both clients and servers.
Central Servers: Deployed using Anycast routing and Content Delivery Network (CDN) principles, ensuring resilience and global reachability.
User Participation: Anyone can host an RE in their network. Tasks can be run once or repeatedly across one or many REs, all managed through a central web interface.
Layered Design: The architecture follows a layered model, with each component fitting into a structured framework explained in Section 4.1.
Continuous Development: The platform uses a CI/CD (Continuous Integration and Continuous Delivery) pipeline, allowing rapid updates, testing, and deployment of new features.

AIORI-IMN is like a distributed laboratory for the Internet. Small devices (like Raspberry Pi) placed at homes, universities, or ISPs act as measurement probes, while central servers coordinate and visualize results. This setup makes it possible to study the Internet's health, security, and performance in real-time, while also allowing researchers to test new protocols.

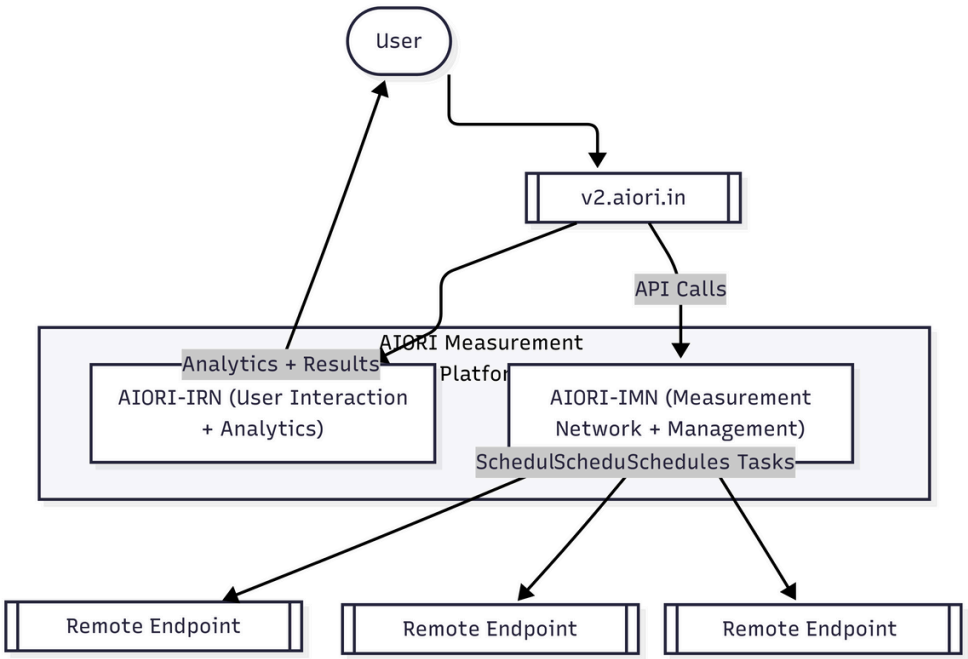


Figure 9: The IRN IMN Flow

6. Layers of the AIORI-IMN Architecture

The AIORI-IMN has been designed in a layered architecture, where each layer has a clear role. The layers talk to each other using standard interfaces (APIs), which makes the system interoperable and easy to extend.

6.1. UI, Management, and Analytics

This layer is what the user interacts with. It provides the interface for:

- Managing the measurement nodes,
- Running analytics,
- Visualizing results.

It works by calling APIs that pass instructions down to the controller layer.

6.2. Controller

This is the brain of the system, coordinating all activities, ensuring performance, and managing communication between layers. It can be accessed through APIs (from above) and message-passing mechanisms (to the workers below).
The main components of the controller are:

- NATS Cluster: Provides a distributed communication system using a Publish–Subscribe messaging model. This ensures that the system is always available and scalable.
- Scheduler: Distributes tasks among remote endpoints (REs) in an efficient way so resources are used optimally.
- Load Balancer: Balances the workload across multiple services to prevent bottlenecks.
- Security Handler: Manages authentication (who you are) and authorization (what you can do) between services.
- Data Collector: Collects the results of measurement tasks and stores them in different data stores for later analysis.

7. Layers of the AIORI-IMN Architecture

7.1. Worker (Remote Endpoints)

The workers are distributed measurement nodes, also called Remote Endpoints (REs). They can run on Single Board Computers (SBCs) like a Raspberry Pi or on Virtual Machines (VMs).

- These nodes receive measurement tasks from the controller,
- Execute the tasks (e.g., ping, traceroute, DNS tests),
- Send the results back to the controller for analysis.

Think of AIORI-IMN like a team project:

- The UI & Analytics layer is the project manager, giving instructions and checking results.
- The Controller layer is the coordinator, making sure tasks are assigned, resources are managed, and rules are followed.
- The Worker layer (REs) is the team on the ground, carrying out the actual tasks and reporting back.

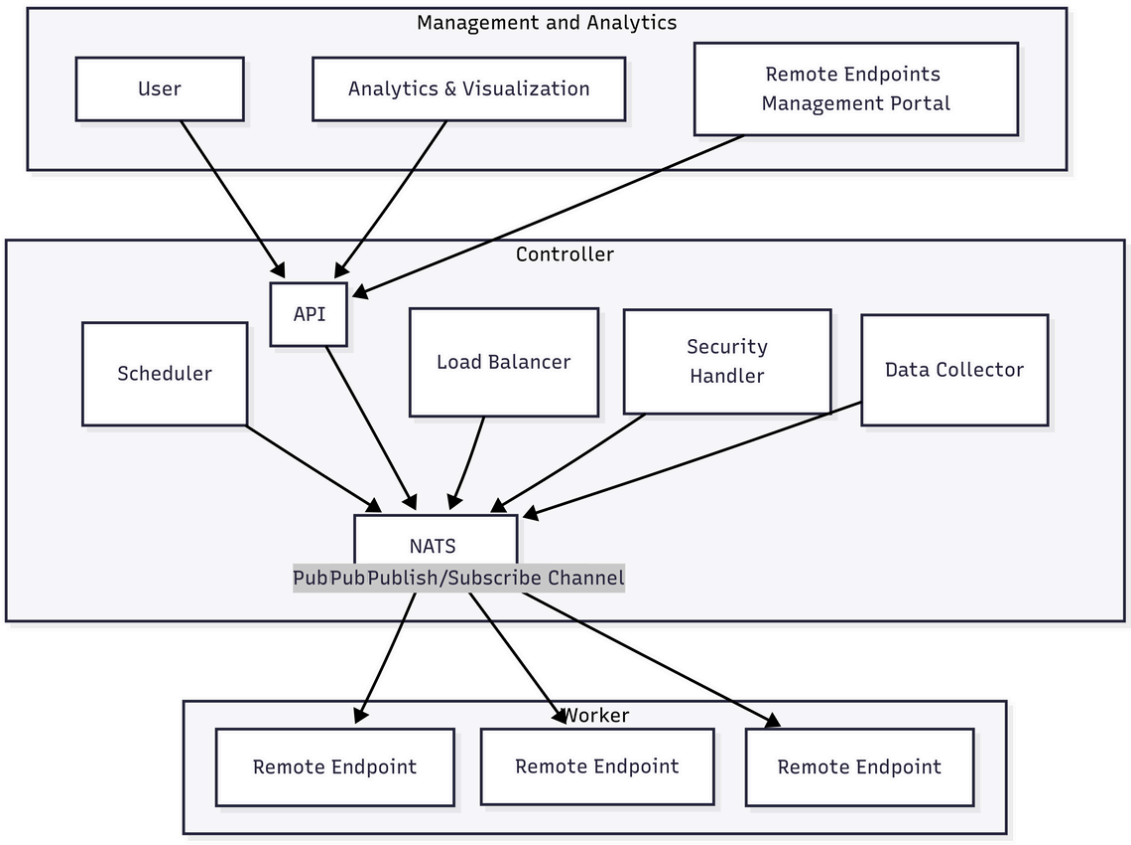


Figure 10: The Architecture

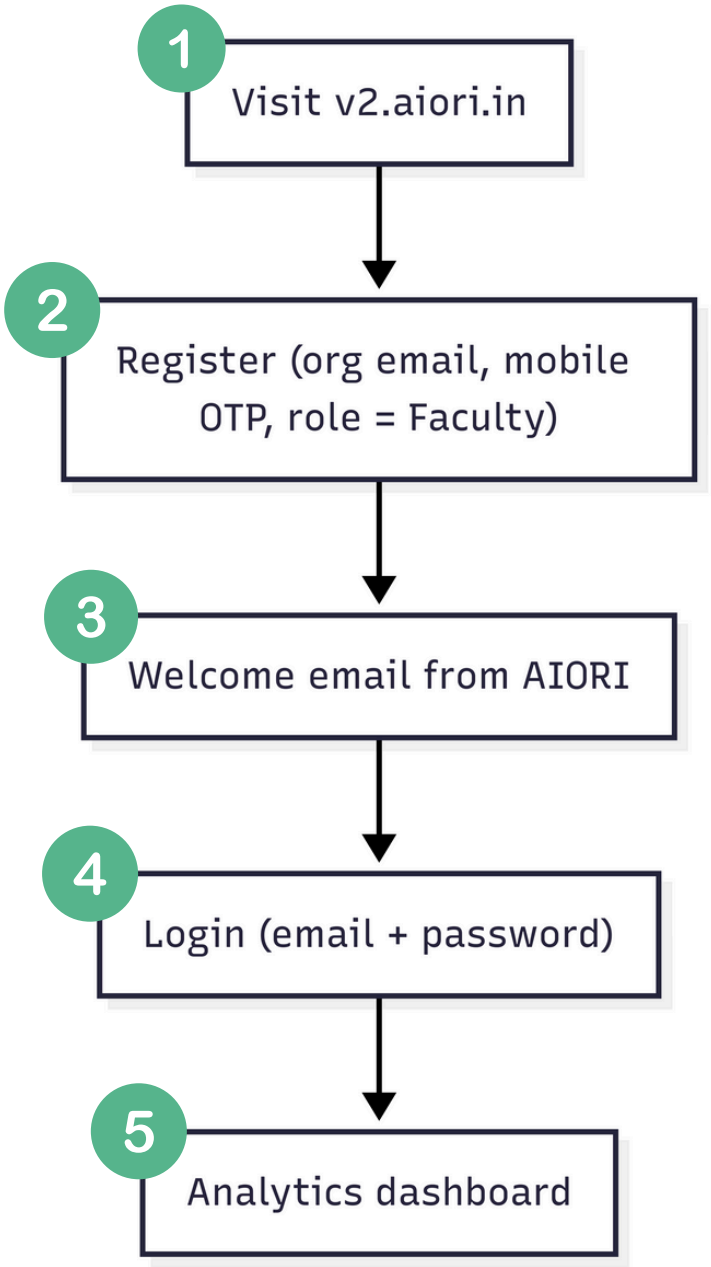
3. About AIORI Internet Measurement Portal

The AIORI Internet Measurement Portal is a national platform designed to help faculties, students, researchers, ISPs, and policymakers examine and evolve the Internet by providing real-world data, tools, and analytics using active measurement techniques.
Key Features:

1. Measurement Tools
    a. Supports basic and advanced tests like ping, traceroute, DNS lookups, latency, packet loss, throughput.
    b. Allows distributed testing through AIORI's Internet Measurement anchors.
2. Research & Education
    a. Faculty can design experiments and assign tasks to students.
    b. Students can run tests, gather data, and generate structured reports (CSV, JSON, PNG, PDF).
3. Standards Engagement
    a. Develop and integrate new measurements and protocols
    b. Helps students see how their measurements relate to global Internet health and protocol development.
4. Capacity Building
    a. Academic institutions can host measurement anchors.
    b. Faculty can join the AIORI Ambassador Program and contribute to national Internet research and skilling the young brains.
5. User-Friendly Access
    a. Web-based portal with dashboards. (v2.aiori.in)
    b. Visual graphs and analytics for quick interpretation.
    c. Multi-format exports for research, presentations, and policymaking.

4. Registration and Login

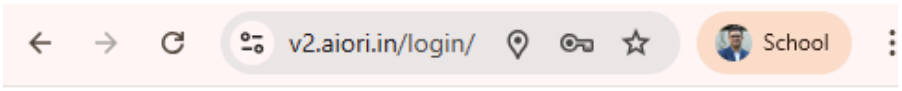
Flow Chart



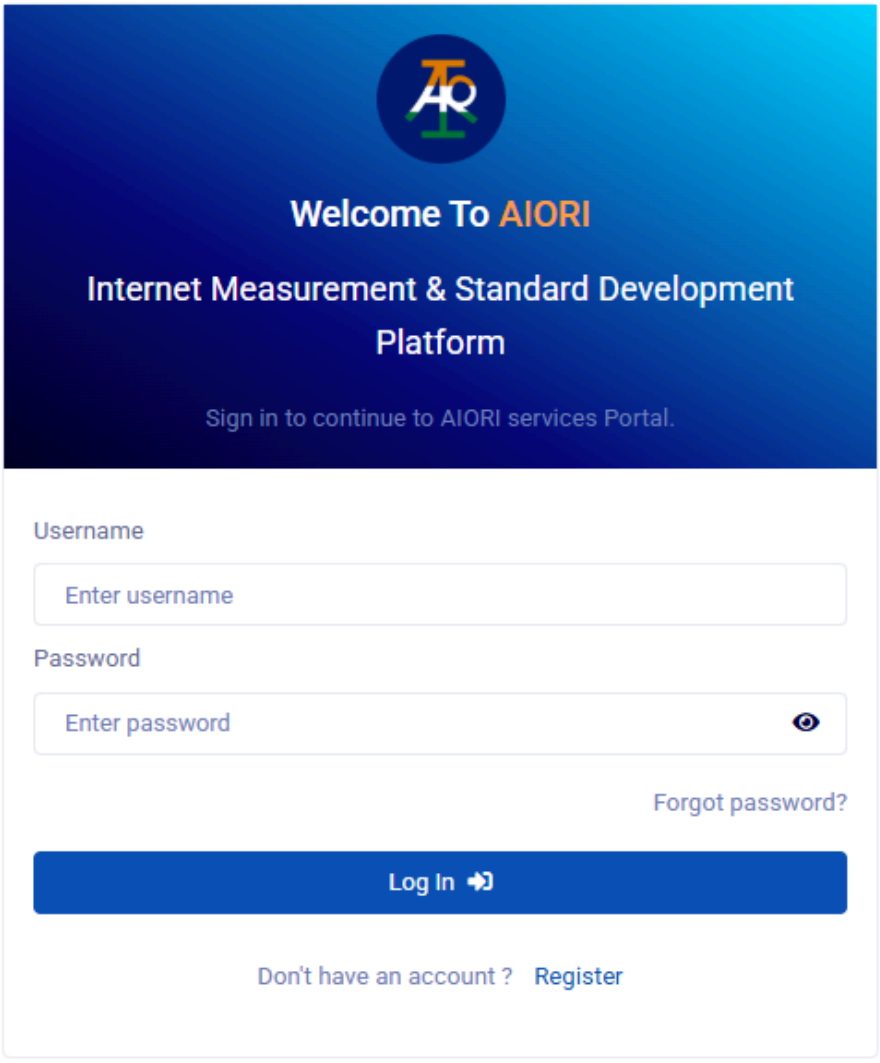
Registration and Login

The Portal - Login and Registration Option

1



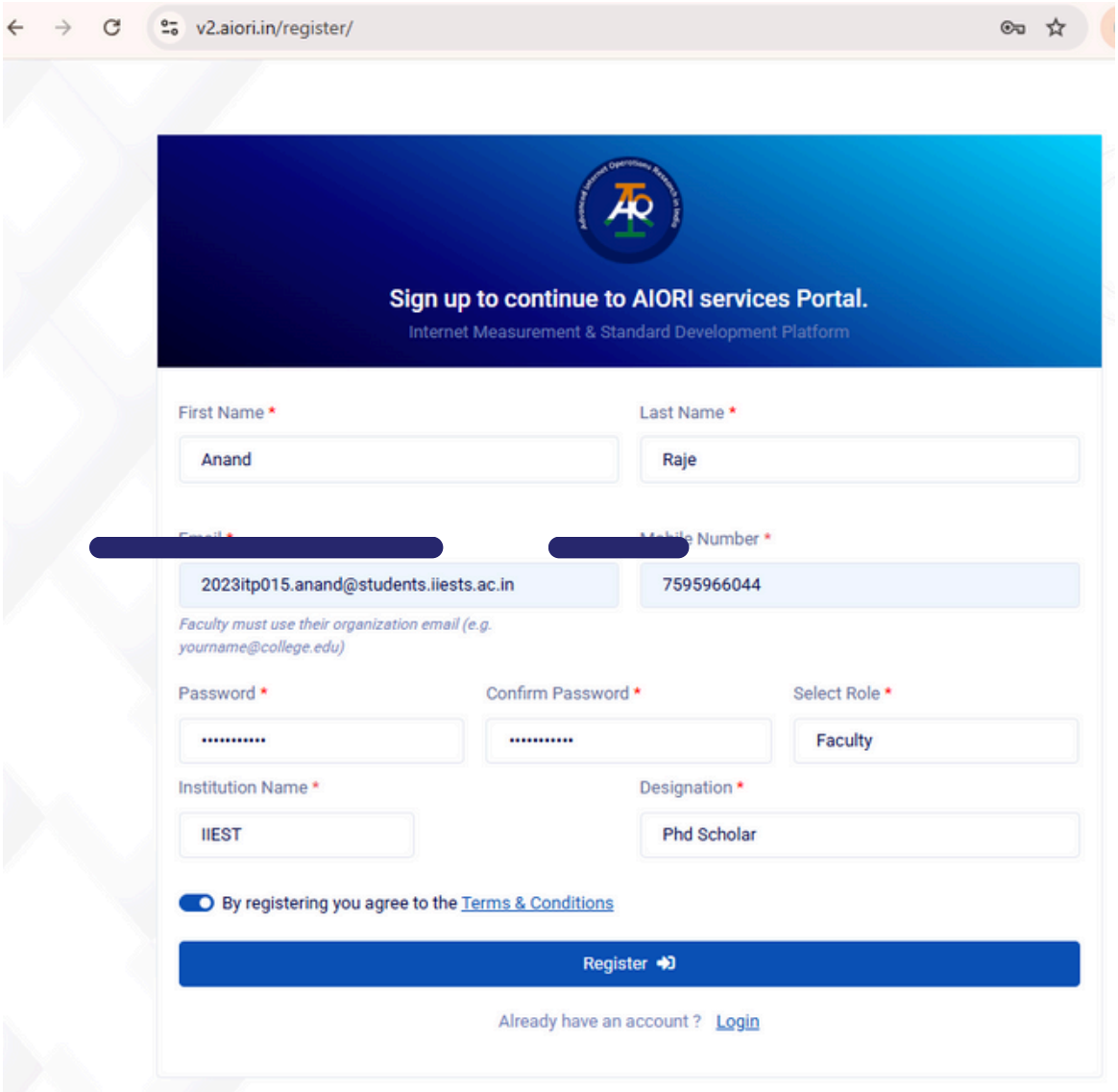
4



Registration and Login

New User Registration

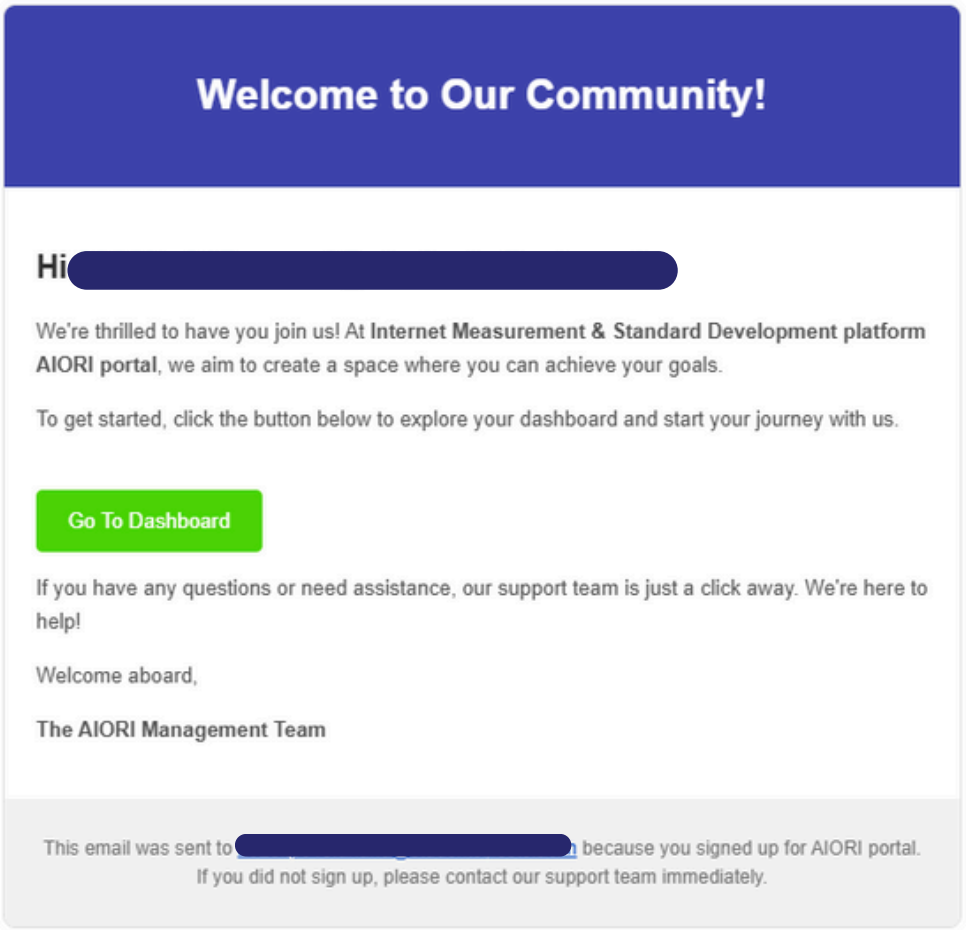
2



Registration and Login

Welcome Mail

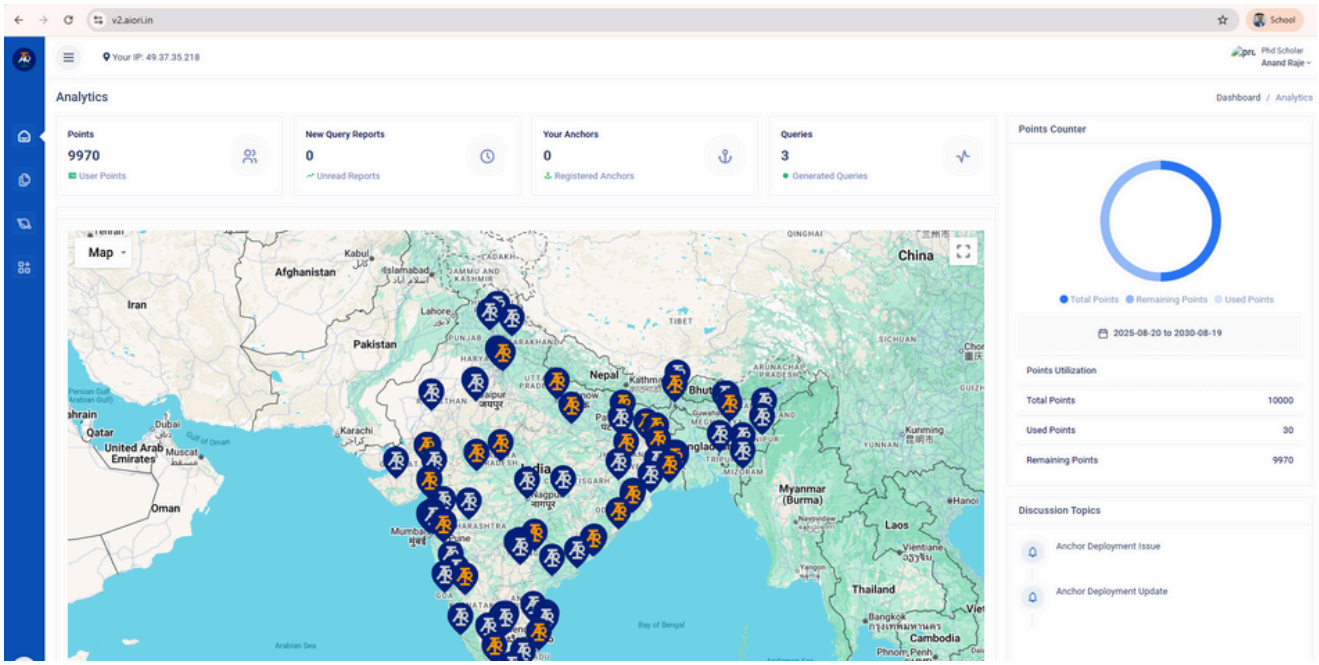
3



Registration and Login

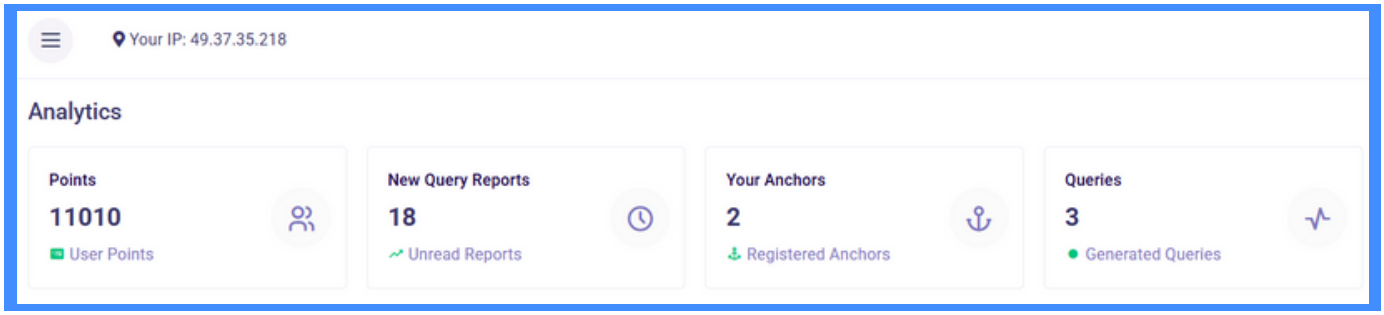
The Dashboard

5



5. Dashboard Widgets

Widgets



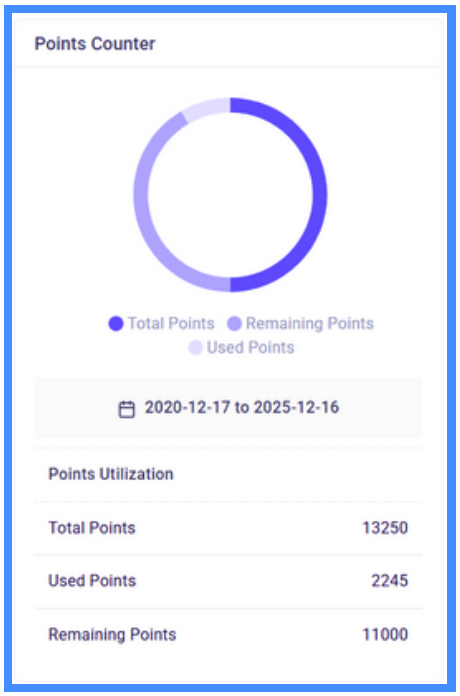
- **Your IP** — It's your Public IP Address
- **Points** — Each measurement costs 5 points. Host an anchor to earn points when others run tests on your device.
- **New Query Reports** — View reports for your recent measurements.
- **Your Anchors** — Anchors currently hosted under your account.
- **Queries** — List of available measurement queries you can run.

Your current public IP address is 49.37.35.218. You appear to be accessing the portal from Kolkata, West Bengal, India, and your connection is served by Reliance Jio Infocomm Limited (AS55836). We use this information to choose nearby anchors, interpret latency and routing results, and attribute measurements to your network. Location is an approximation based on IP geolocation (not GPS).

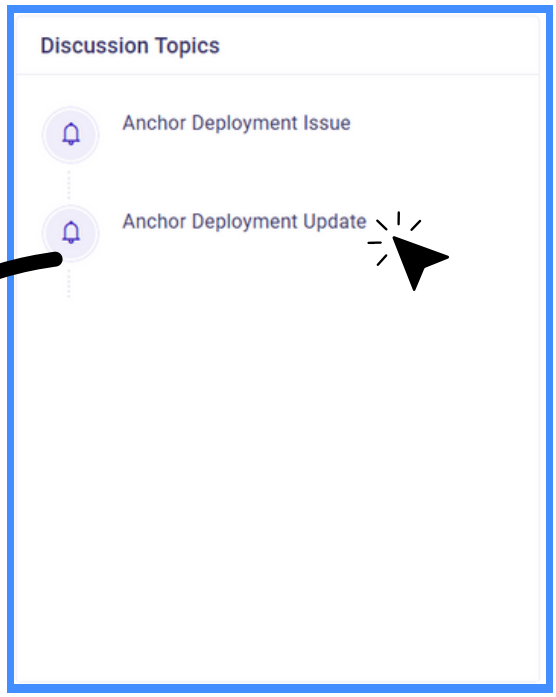
Dashboard Widgets

Points Counter, Discussion Forum

Widgets



The widget shows points history



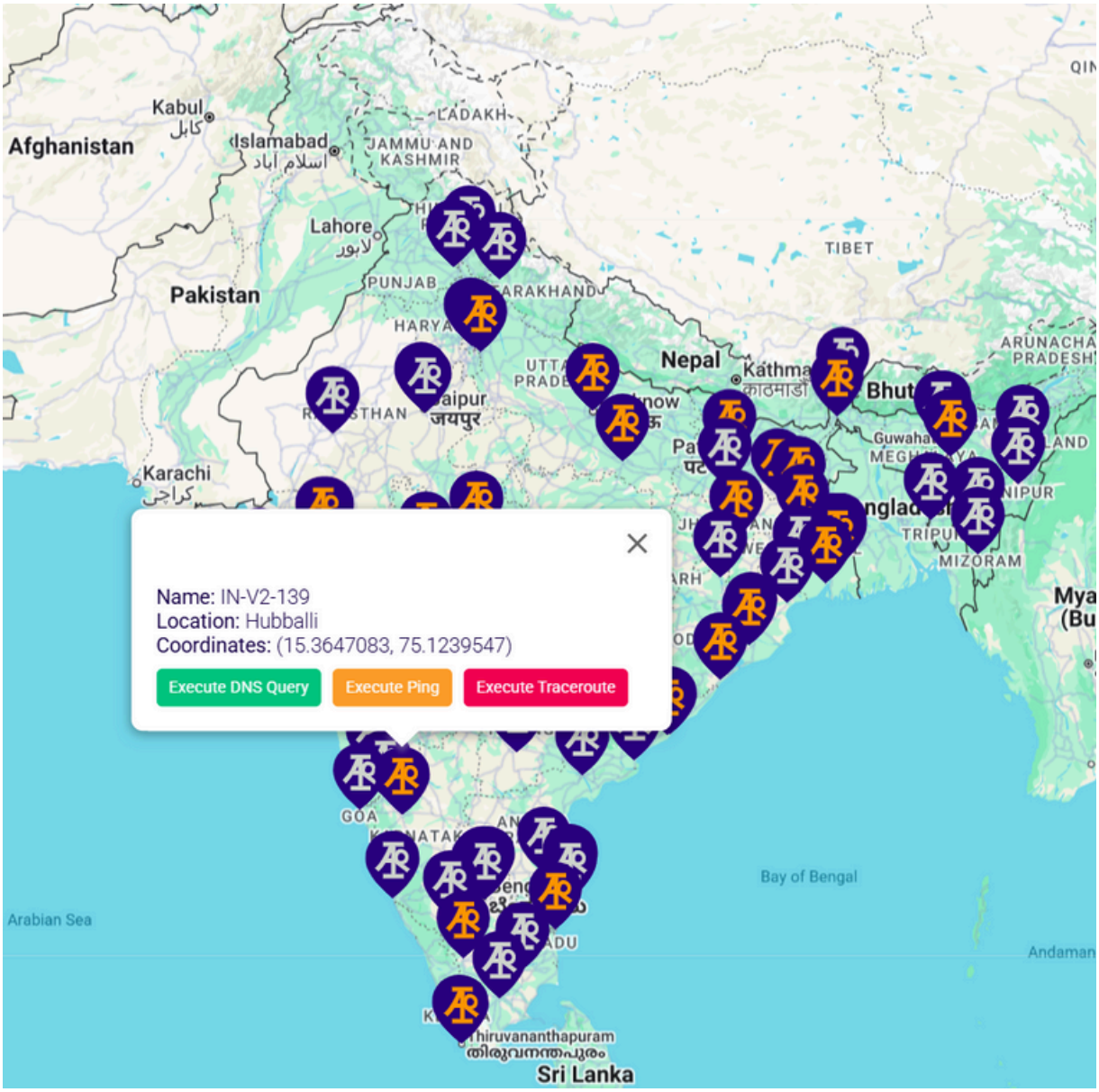
Widget to Access Discussion Forum

Discussion Forum Page

Dashboard Widgets

Measurement Map

Map Widget



Use the interactive map to run tests from any anchor:

- Click a pin to open its card (shows name, city, and coordinates).
- Choose the test you want: Execute DNS Query, Execute Ping, or Execute Traceroute.
- The query runs from that anchor's location, so you can compare results across regions by testing multiple pins.
- This makes it easy to study latency, routing paths, and DNS behavior geographically without changing any settings.

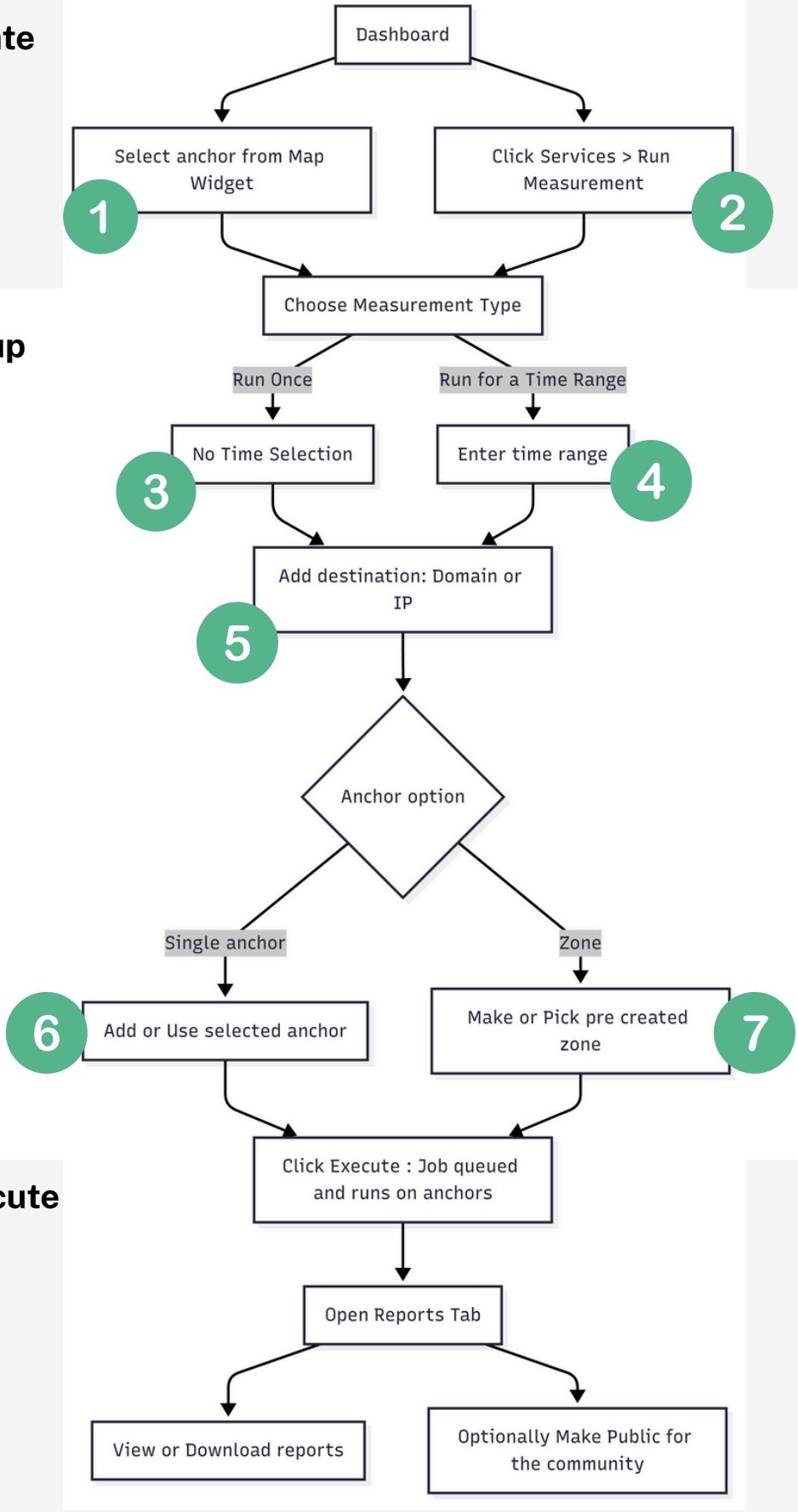
6. Running a measurement

Flow Chart

Initiate

Setup

Execute

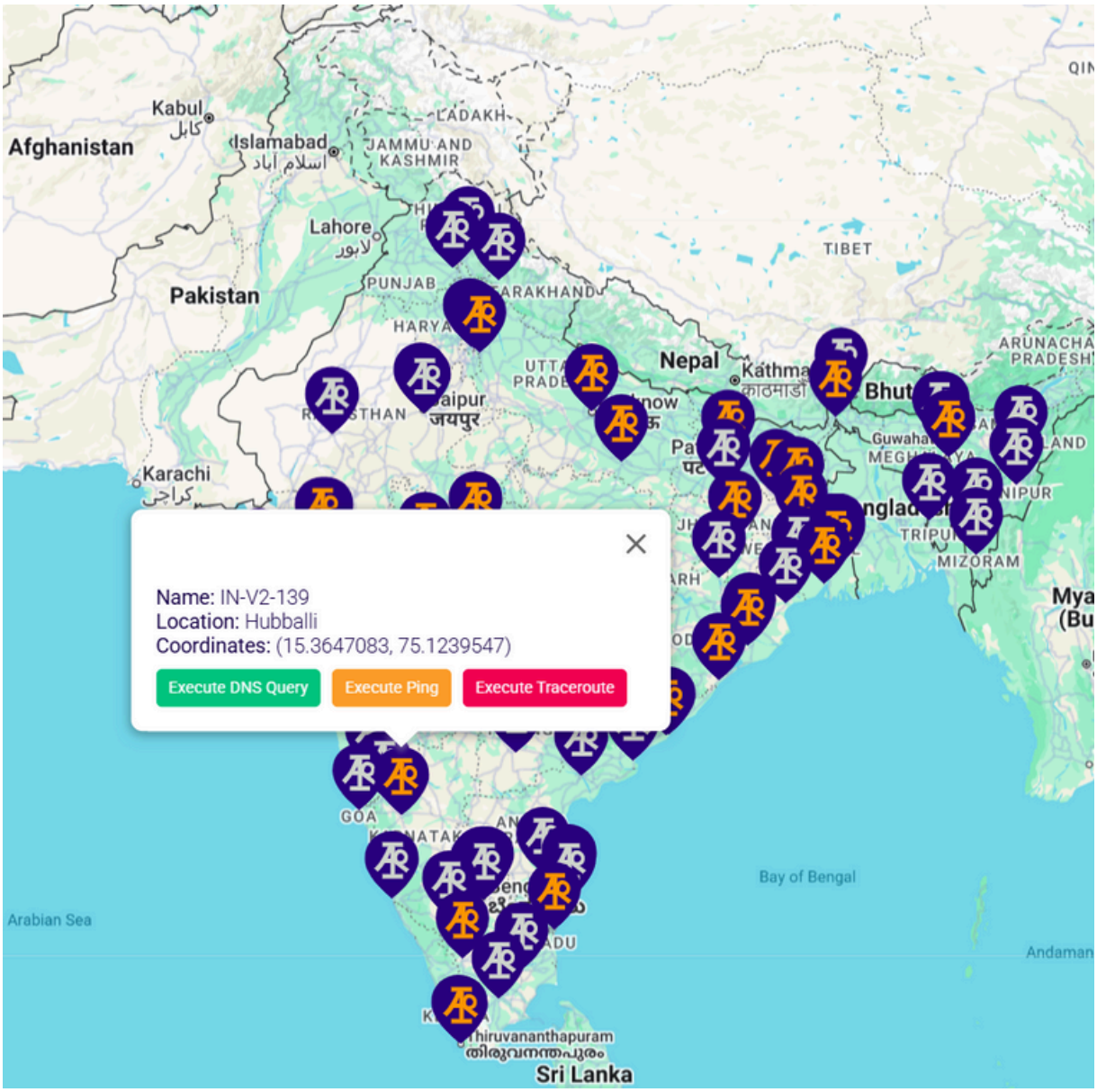


Running Measurements

Initiate - Selecting Anchor to run measurements from Map Widget

Map Widget

1



Use the interactive map to run tests from any anchor:

- Click a pin to open its card (shows name, city, and coordinates).
- Choose the test you want: Execute DNS Query, Execute Ping, or Execute Traceroute.
- The query runs from that anchor's location, so you can compare results across regions by testing multiple pins.
- This makes it easy to study latency, routing paths, and DNS behavior geographically without changing any settings.

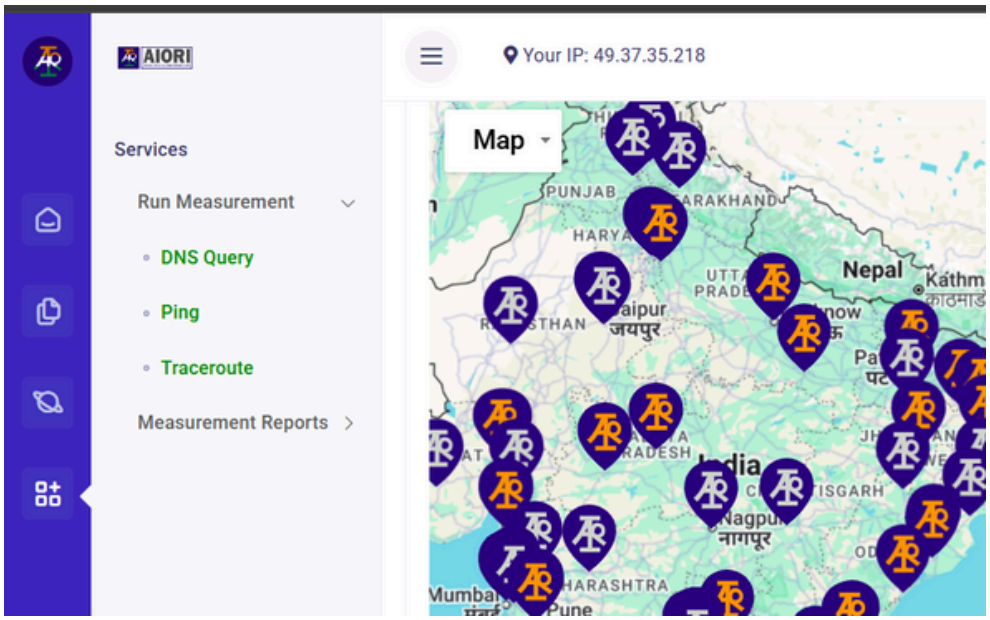
Running a measurement

Initiate - Running measurements from Dashboard menu

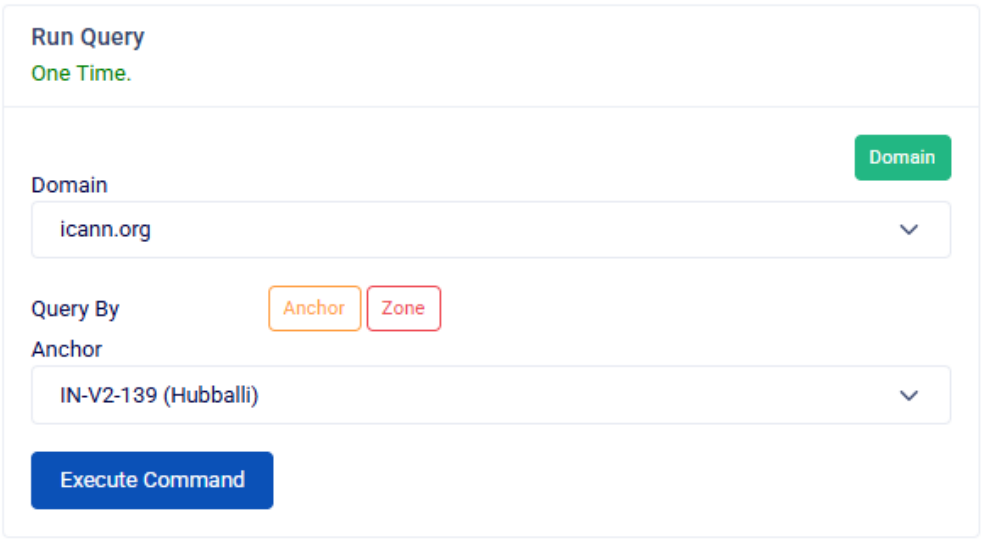
2

The measurement tests can be run from menu as well:

- Click on services or icon in the left PAN
- Select Run Measurement Menu item
- Choose the test you want: DNS Query, Ping, or Traceroute.



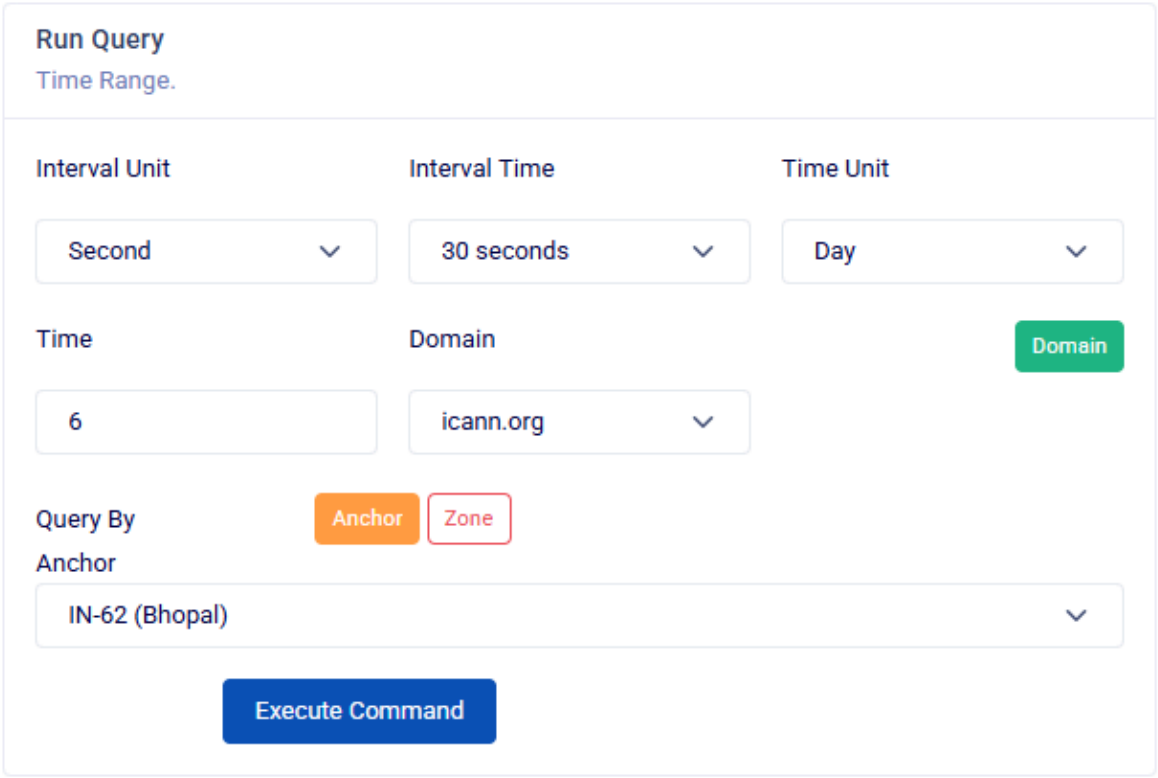
3



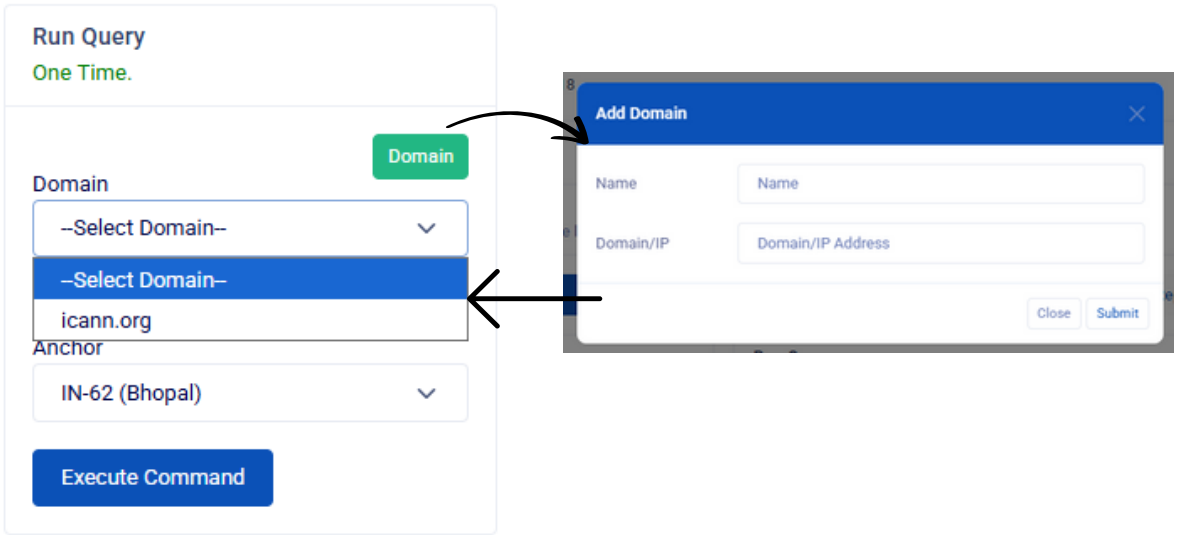
Running a measurement

Setup - Time Range Measurement and Domain Selection or Addition

4



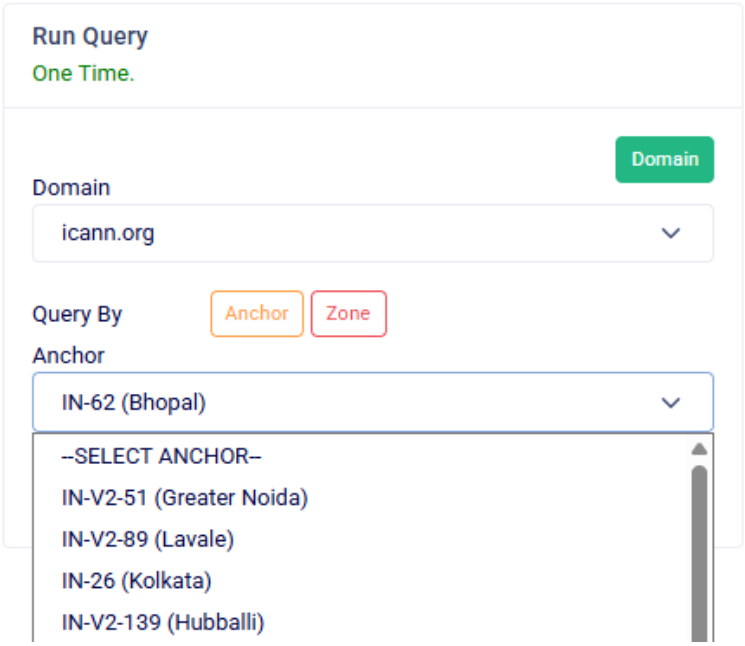
5



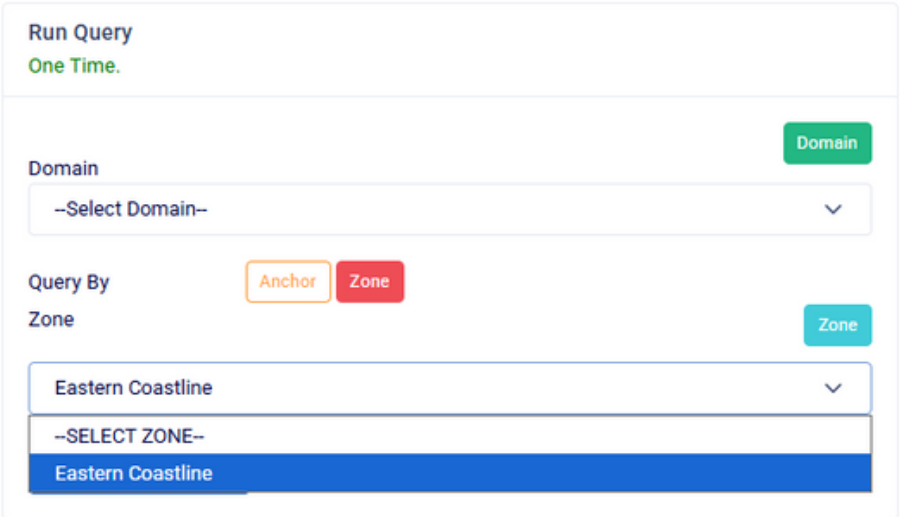
Running a measurement

Setup - Selecting an anchor or zone to run measurements

6



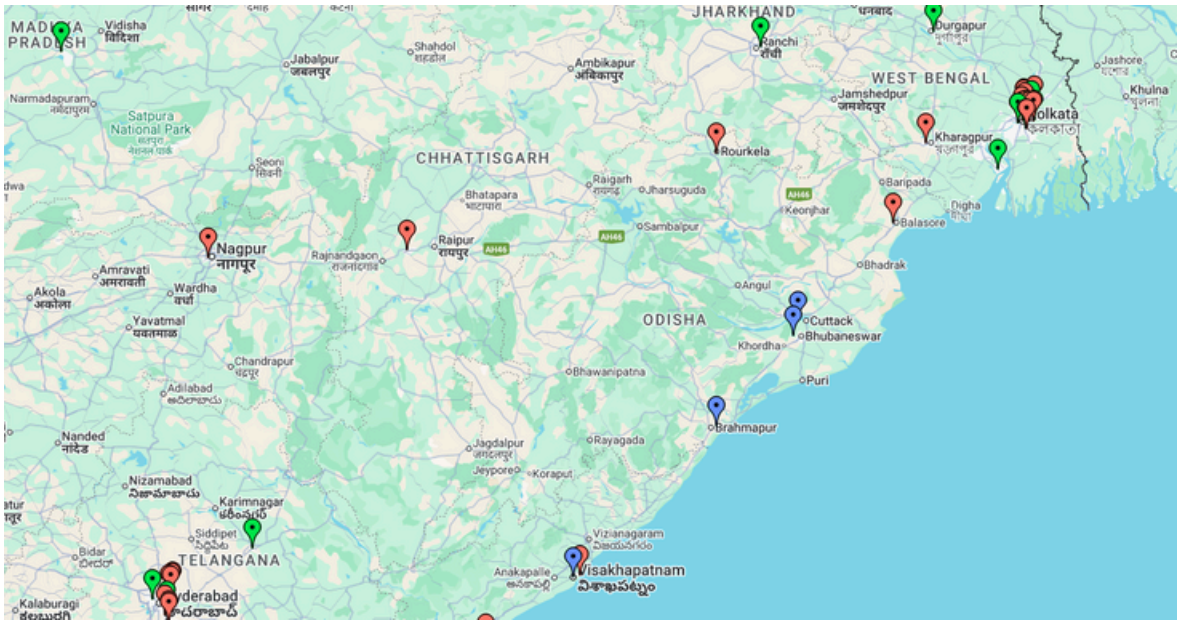
7



Running a measurement

Setup - Create Zone

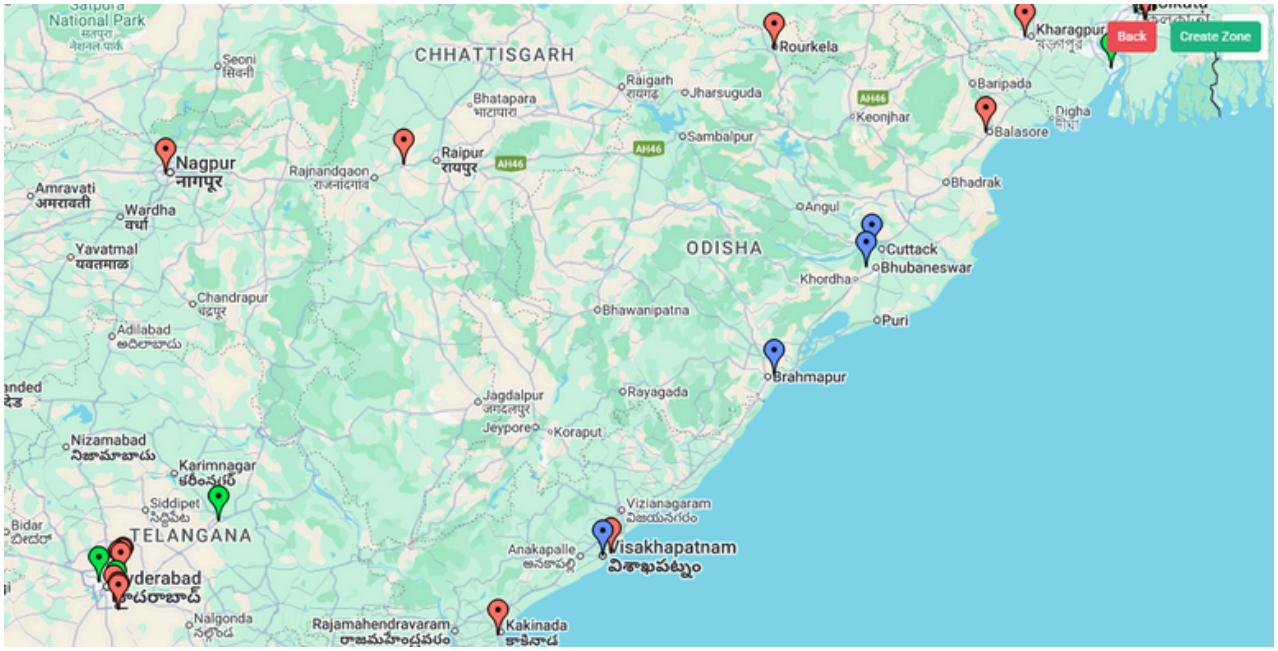
7

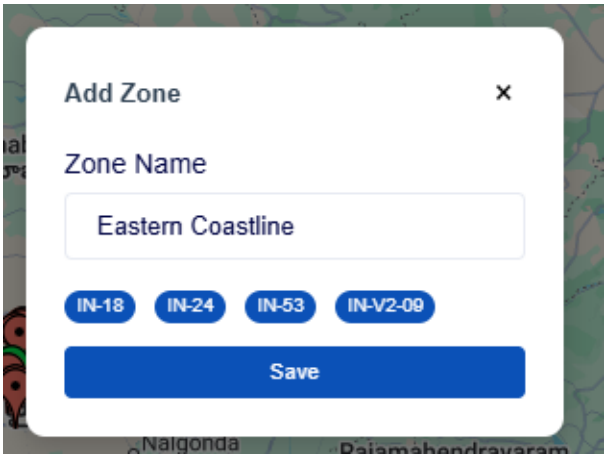


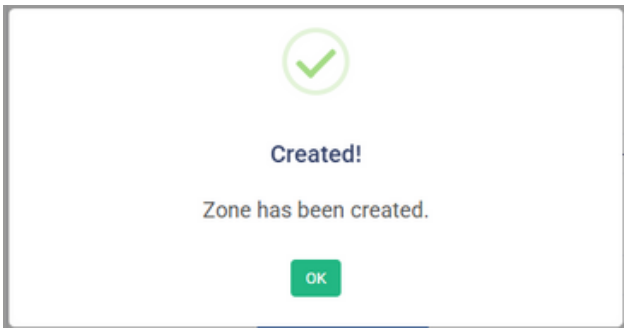
Running a measurement

Setup - Create Zone

7

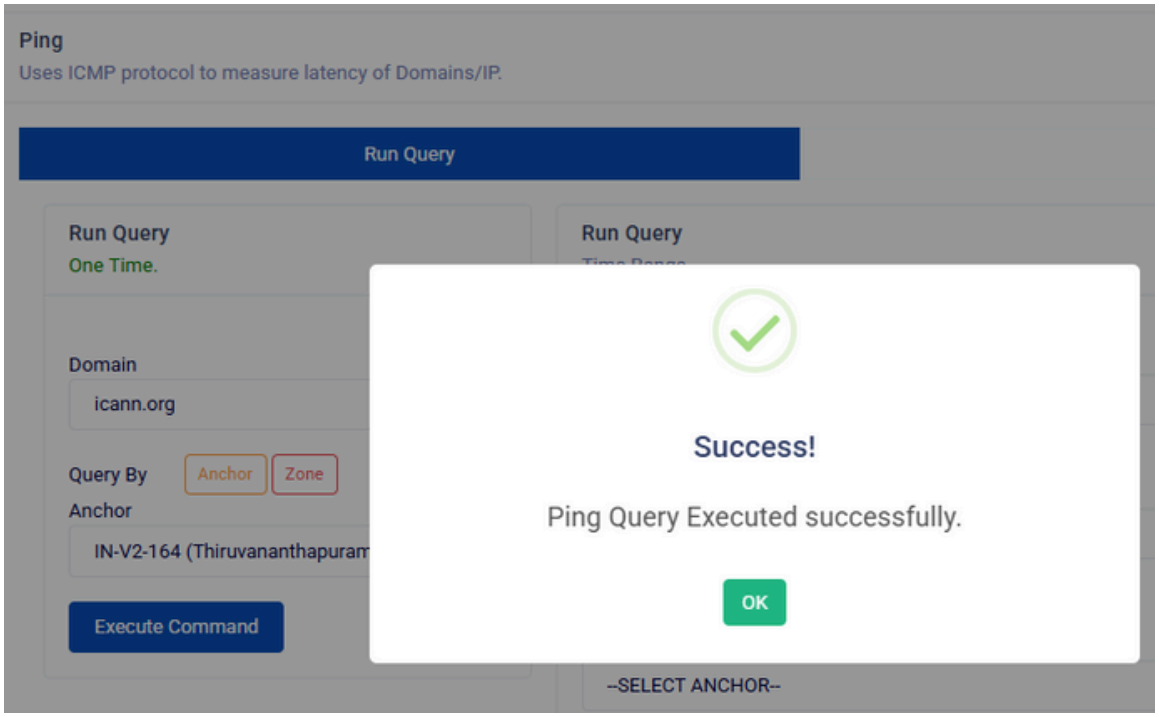


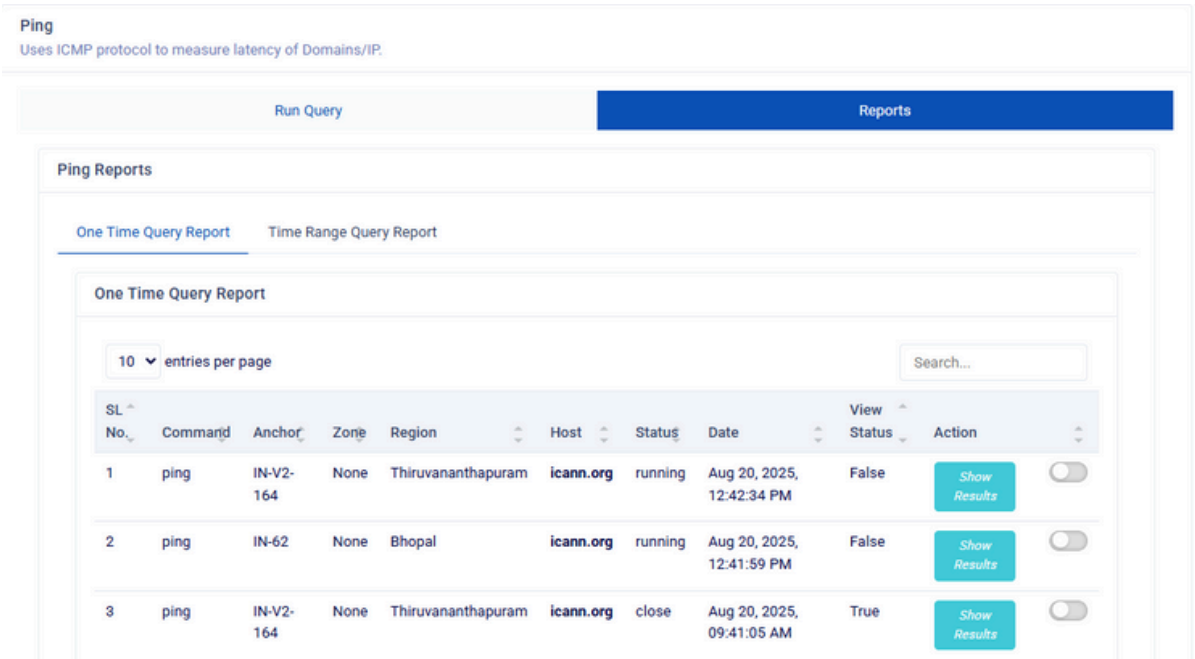




7. PING

Execute to rune once in a single Anchor





PING

Execute to rune once in a single Anchor - Reports

10

PING

Execute to rune once in a single Anchor - Analyzing Report


```
{
  "status": 1,
  "message": "Data set is ready.",
  "data": [
    {
      "time": "2025-08-20T04:11:10.93659855Z",
      "address": "icann.org",
      "avg_rtt": null,
      "destination": "icann.org",
      "id": "dde5d128-27a3-4125-9499-a653972f0ea3",
      "is_alive": true,
      "jitter": 0.1,
      "max_rtt": null,
      "min_rtt": null,
      "packet_duplicate_count": null,
      "packet_duplicate_rate": null,
      "packet_loss": 0,
      "packet_loss_count": null,
      "packet_loss_rate": null,
      "packet_receive": null,
      "packet_transmit": null,
      "packets_received": 3,
      "packets_sent": 3,
      "port": null,
      "protocol": "ICMP",
      "protocol_1": "ICMP",
      "rd3": "29471e5e38518cb414381c411347a476",
      "rtt_avg": 255.584,
      "rtt_max": 255.68,
      "rtt_mdev": null,
      "rtt_min": 255.481
    }
  ]
}
```

PING

Execute to rune once in a Zone of Anchors - Reports

AIORI Ping Reports

Back

Query Visibility

Export Result

One Time Regular (Zone) Ping

Anchor Name: IN-18

Generated On Aug 20, 2025, 02:03:08 PM

Destination: icann.org

RTT (MAX.): 298.826 - RTT (AVG.): 298.631 - RTT (MIN.): 298.431

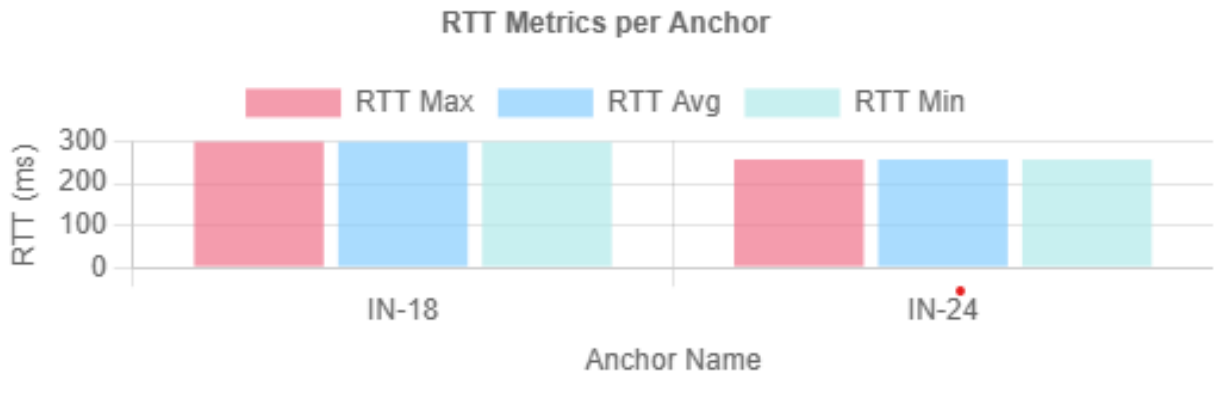
Anchor Name: IN-24

Generated On Aug 20, 2025, 02:03:08 PM

Destination: icann.org

RTT (MAX.): 256.677 - RTT (AVG.): 256.59 - RTT (MIN.): 256.418

Export as PNG

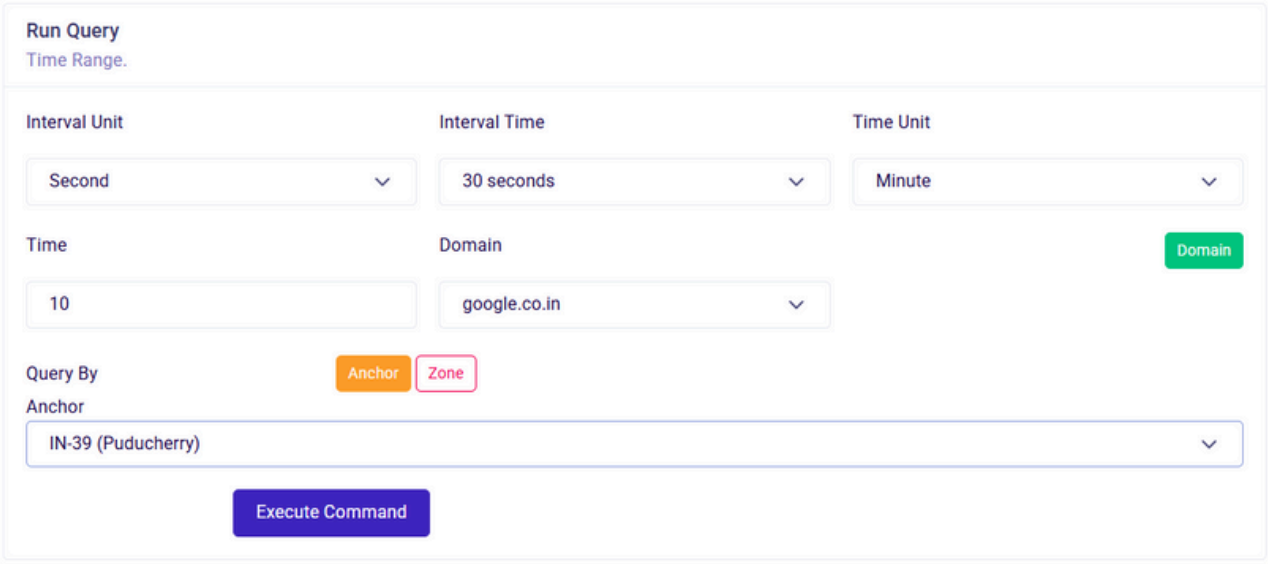


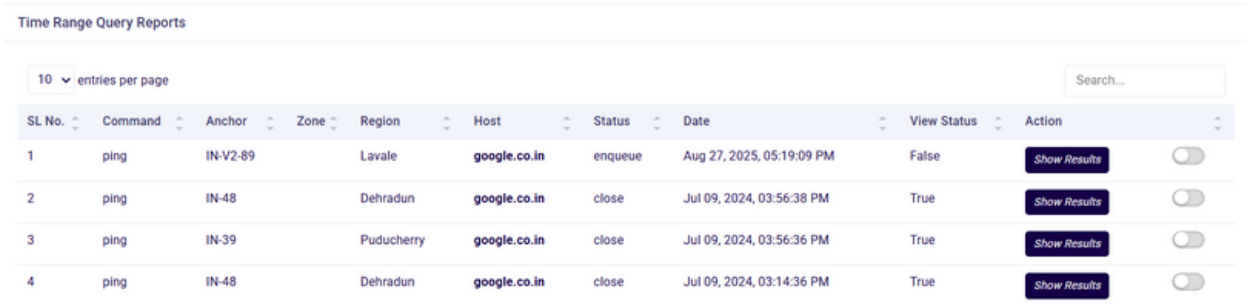
PING

Execute to rune once in a Zone of Anchors - Reports - Analyzing Reports

PING

Execute to rune for a time range from an Anchors





PING

Report : Run for a time range from an Anchor IN-39

AIORI Ping Reports

Back

Query Visibility | Export Result

Time Range Query

Command: ping | **Host:** google.co.in

Generated On Jul 09, 2024, 03:43:35 PM

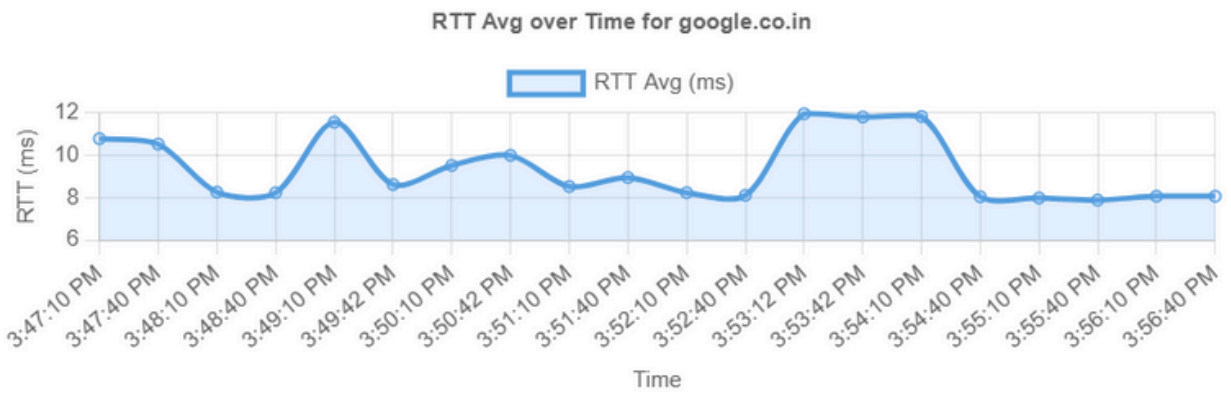
Anchor: IN-39 | **Region:** Puducherry

From Date: Jul 09, 2024, 03:43:35 PM | **To Date:** Jul 09, 2024, 03:56:36 PM

Execution Interval Time: 30 second | **Execution Status:** close

All Date Graphical View

Export as PNG



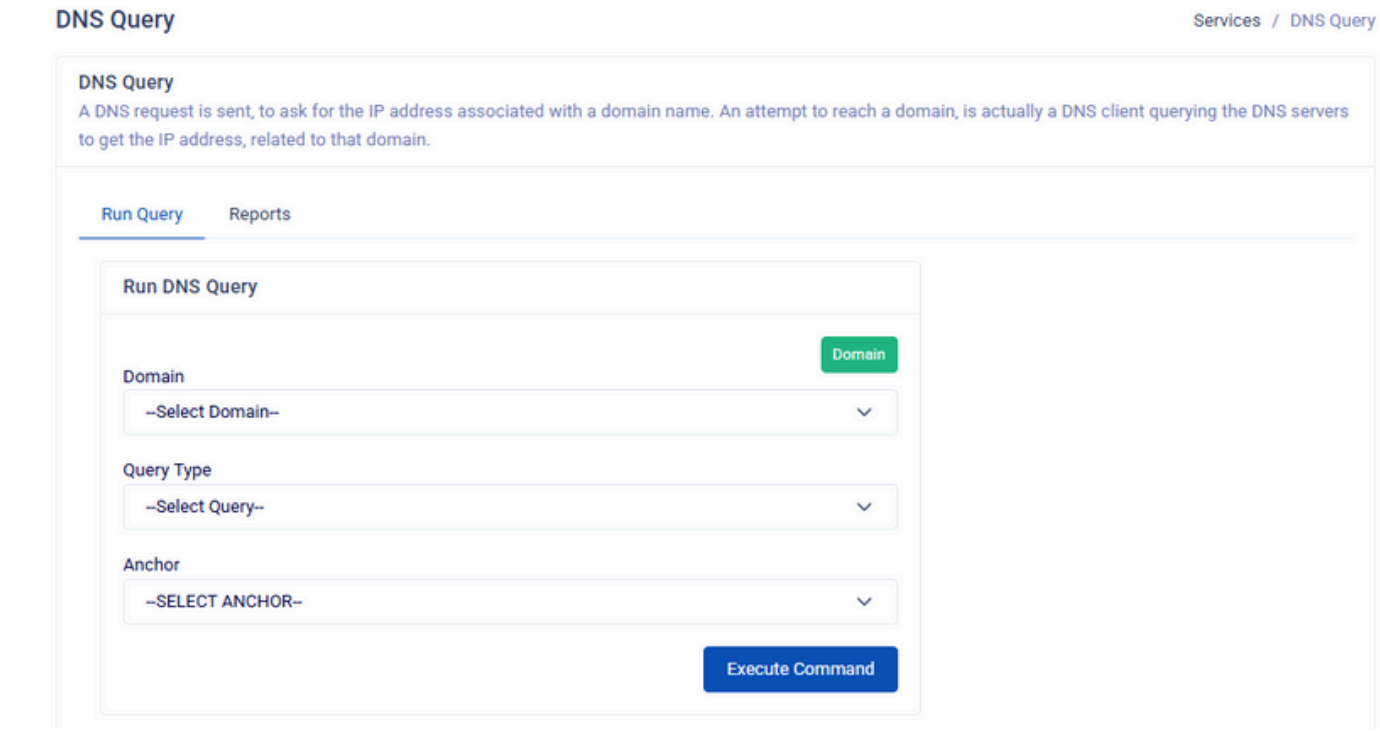
PING

Report : Run for a time range from an Anchor IN-39 - JSON


```
{
  "status": 1,
  "message": "Data set is ready.",
  "data": {
    "google.co.in": [
      {
        "time": "2024-07-09T10:17:12.923032114Z",
        "destination": "google.co.in",
        "rtt_avg": 44.715
      },
      {
        "time": "2024-07-09T10:17:40.925883607Z",
        "destination": "google.co.in",
        "rtt_avg": 44.771
      },
      {
        "time": "2024-07-09T10:18:10.919782288Z",
        "destination": "google.co.in",
        "rtt_avg": 44.409
      },
      {
        "time": "2024-07-09T10:18:40.921045014Z",
        "destination": "google.co.in",
        "rtt_avg": 44.569
      },
      {
        "time": "2024-07-09T10:19:12.950959596Z",
        "destination": "google.co.in",
        "rtt_avg": 44.42
      },
      {
        "time": "2024-07-09T10:19:42.924471772Z",
        "destination": "google.co.in",
        "rtt_avg": 44.442
      },
      {
        "time": "2024-07-09T10:20:10.921709559Z",
        "destination": "google.co.in",
        "rtt_avg": 44.426
      },
      {
        "time": "2024-07-09T10:20:40.914565264Z",
        "destination": "google.co.in",
        "rtt_avg": 44.503
      },
      {
        "time": "2024-07-09T10:21:10.925103384Z",
        "destination": "google.co.in",
        "rtt_avg": 44.403
      },
      {
        "time": "2024-07-09T10:21:40.921415668Z",
        "destination": "google.co.in",
        "rtt_avg": 44.453
      },
      {
        "time": "2024-07-09T10:22:10.919614929Z",
        "destination": "google.co.in",
        "rtt_avg": 44.474
      },
      {
        "time": "2024-07-09T10:22:40.912389689Z",
        "destination": "google.co.in",
        "rtt_avg": 44.408
      },
      {
        "time": "2024-07-09T10:23:10.965490502Z",
        "destination": "google.co.in",
        "rtt_avg": 45.225
      },
      {
        "time": "2024-07-09T10:23:40.91806209Z",
        "destination": "google.co.in",
        "rtt_avg": 45.241
      },
      {
        "time": "2024-07-09T10:24:10.920260884Z",
        "destination": "google.co.in",
        "rtt_avg": 45.181
      },
      {
        "time": "2024-07-09T10:24:40.93332459Z",
        "destination": "google.co.in",
        "rtt_avg": 47.79
      },
      {
        "time": "2024-07-09T10:25:12.936920361Z",
        "destination": "google.co.in",
        "rtt_avg": 47.685
      },
      {
        "time": "2024-07-09T10:25:40.9301526562",
        "destination": "google.co.in",
        "rtt_avg": 47.683
      },
      {
        "time": "2024-07-09T10:26:12.941756107Z",
        "destination": "google.co.in",
        "rtt_avg": 47.708
      },
      {
        "time": "2024-07-09T10:26:40.929114403Z",
        "destination": "google.co.in",
        "rtt_avg": 47.784
      }
    ]
  }
}
```

8. DNS

Execute (aiori.in A on IN-V2-198)



DNS

Reports (aiori.in A on IN-V2-198)

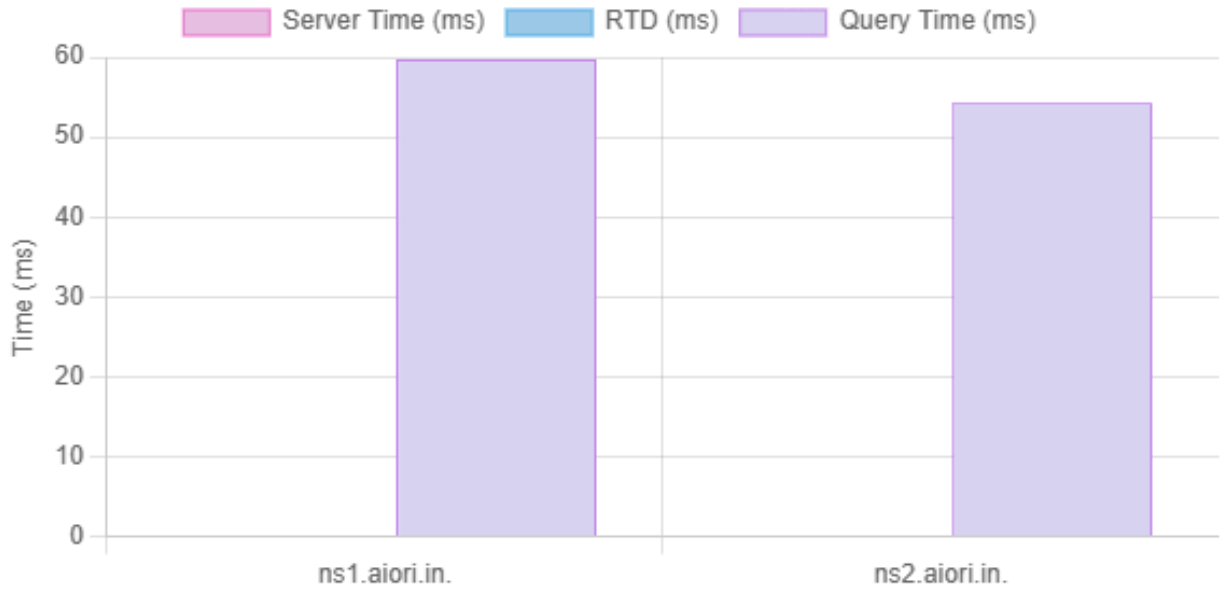
DNS Query Reports

Export Result | Query Visibility

Domain	Anchor	Query Type	Answer
Aiori	IN-V2-198	A	103.149.148.151

Authoritative Zone

Resource Record	Value	Answered	Time(ms)
ns1.aiori.in.	103.149.148.148	True	59.71
ns2.aiori.in.	103.149.148.149	False	54.28

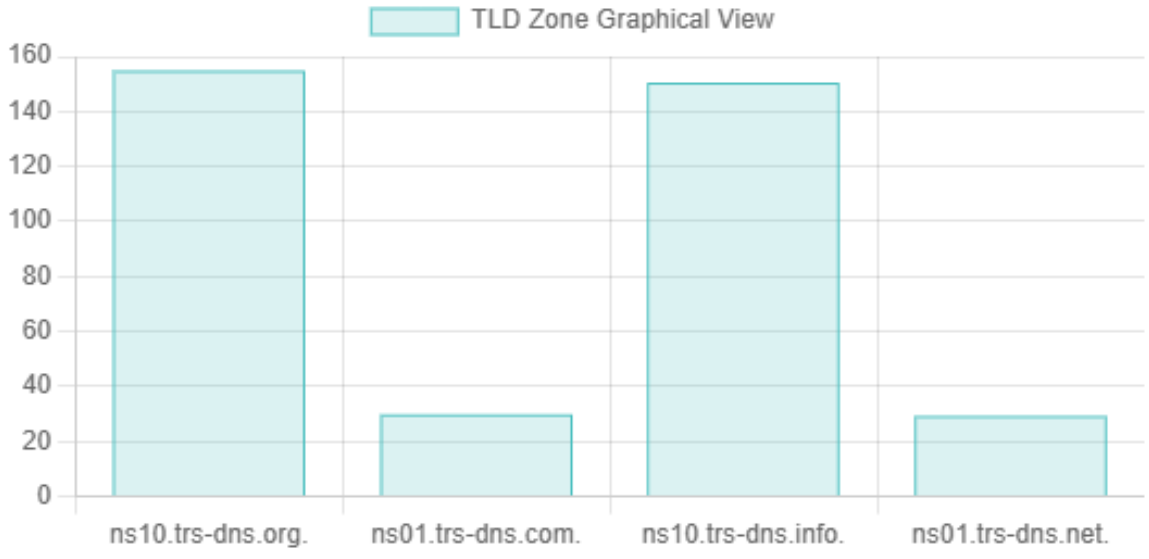


DNS

Reports (aiori.in A on IN-V2-198)

TLD Zone

Resource Record	Value	Time(ms)
ns10.trs-dns.org.	64.78.205.1	154.93
ns01.trs-dns.com.	64.96.1.1	29.87
ns10.trs-dns.info.	64.78.204.1	150.55
ns01.trs-dns.net.	64.96.2.1	29.25

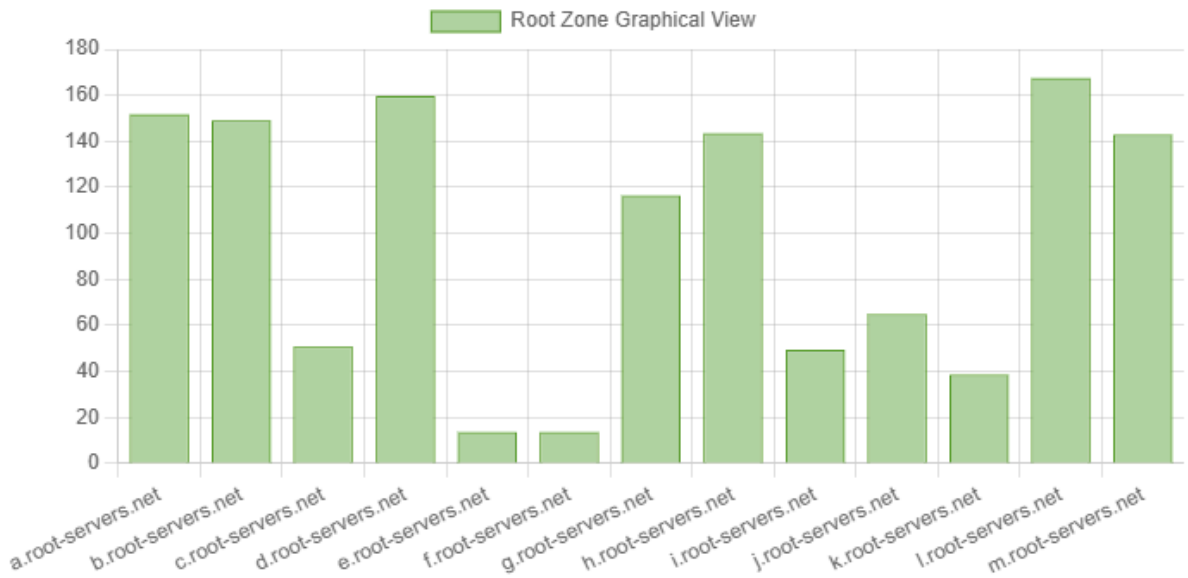


DNS

Reports (aiori.in A on IN-V2-198)

Root Zone

Resource Record	Value	Time(ms)
a.root-servers.net	198.41.0.4	151.58
b.root-servers.net	199.9.14.201	149.10
c.root-servers.net	192.33.4.12	50.79
d.root-servers.net	199.7.91.13	159.68
e.root-servers.net	192.203.230.10	13.64
f.root-servers.net	192.5.5.241	13.66
g.root-servers.net	192.112.36.4	116.46
h.root-servers.net	198.97.190.53	143.46
i.root-servers.net	192.36.148.17	49.38
j.root-servers.net	192.58.128.30	64.83
k.root-servers.net	193.0.14.129	38.46
l.root-servers.net	199.7.83.42	167.36
m.root-servers.net	202.12.27.33	142.87



DNS

Reports (aiori.in A on IN-V2-198) - JSON for Analysis


```
{
  "dnsq_id": "1fcb0eac-043e-4a69-89d3-c88702d5a99b",
  "timestamp": "2025-08-21T07:46:59",
  "query_type": "A",
  "root_data": {
    "error": {},
    "servers": [
      {
        "a.root-servers.net": {
          "ip": "198.41.0.4",
          "query_time": 0.15158390998840332,
          "is_authority": true
        }
      },
      {
        "b.root-servers.net": {
          "ip": "199.9.14.201",
          "query_time": 0.14910483360290527,
          "is_authority": true
        }
      },
      {
        "c.root-servers.net": {
          "ip": "192.33.4.12",
          "query_time": 0.050787925720214844,
          "is_authority": true
        }
      },
      {
        "d.root-servers.net": {
          "ip": "199.7.91.13",
          "query_time": 0.1596822738647461,
          "is_authority": true
        }
      },
      {
        "e.root-servers.net": {
          "ip": "192.203.230.10",
          "query_time": 0.013643264770507812,
          "is_authority": true
        }
      },
      {
        "f.root-servers.net": {
          "ip": "192.5.5.241",
          "query_time": 0.013660192489624023,
          "is_authority": true
        }
      },
      {
        "g.root-servers.net": {
          "ip": "192.112.36.4",
          "query_time": 0.11646342277526855,
          "is_authority": true
        }
      },
      {
        "h.root-servers.net": {
          "ip": "198.97.190.53",
          "query_time": 0.14346051216125488,
          "is_authority": true
        }
      },
      {
        "i.root-servers.net": {
          "ip": "192.36.148.17",
          "query_time": 0.049379825592041016,
          "is_authority": true
        }
      },
      {
        "j.root-servers.net": {
          "ip": "192.58.128.30",
          "query_time": 0.06482720375061035,
          "is_authority": true
        }
      },
      {
        "k.root-servers.net": {
          "ip": "193.0.14.129",
          "query_time": 0.03846025466918945,
          "is_authority": true
        }
      },
      {
        "l.root-servers.net": {
          "ip": "199.7.83.42",
          "query_time": 0.16735601425170898,
          "is_authority": true
        }
      },
      {
        "m.root-servers.net": {
          "ip": "202.12.27.33",
          "query_time": 0.14287114143371582,
          "is_authority": true
        }
      }
    ],
    "authority": [
      "ns01.trs-dns.com.",
      "ns01.trs-dns.net.",
      "ns10.trs-dns.info.",
      "ns10.trs-dns.org."
    ]
  },
```

DNS

Reports (aiori.in A on IN-V2-198)- JSON for Analysis


```
"domain_data": {
  "error": {
    "ns1.aiori.in.": {
      "error": "No response.: Unknown Exception for Nameserver
ns1.aiori.in. 2001:ded:8000::148. "
    },
    "ns2.aiori.in.": {
      "error": "No response.: Unknown Exception for Nameserver
ns2.aiori.in. 2001:ded:8000::149. "
    }
  },
  "answer": [
    "103.149.148.151"
  ],
  "servers": [
    {
      "ns1.aiori.in.": {
        "ip": "103.149.148.148",
        "rtd": null,
        "rtt": 0.05971407890319824,
        "type": "v4",
        "rtd_ms": null,
        "rtt_ms": 59.71407890319824,
        "server": null,
        "is_answer": true,
        "server_ms": null,
        "query_time": 0.05971407890319824
      }
    },
    {
      "ns2.aiori.in.": {
        "ip": "103.149.148.149",
        "rtd": null,
        "rtt": 0.05428481101989746,
        "type": "v4",
        "answer": [
          "103.149.148.151"
        ],
        "rtd_ms": null,
        "rtt_ms": 54.28481101989746,
        "server": null,
        "is_answer": false,
        "server_ms": null,
        "query_time": 0.05428481101989746
      }
    }
  ]
},
"target_name": "aiori.in",
  "tld_data": {
    "error": {},
    "servers": [
      {
        "ns10.trs-dns.org.": {
          "ip": "64.78.205.1",
          "query_time": 0.15492606163024902,
          "is_authority": true
        }
      },
      {
        "ns01.trs-dns.com.": {
          "ip": "64.96.1.1",
          "query_time": 0.029873371124267578,
          "is_authority": true
        }
      },
      {
        "ns10.trs-dns.info.": {
          "ip": "64.78.204.1",
          "query_time": 0.15055179595947266,
          "is_authority": true
        }
      },
      {
        "ns01.trs-dns.net.": {
          "ip": "64.96.2.1",
          "query_time": 0.029248476028442383,
          "is_authority": true
        }
      }
    ],
    "authority": [
      "ns1.aiori.in.",
      "ns2.aiori.in."
    ]
  }
}
```

DNS with PDM (RFC 8250)

Execute (aiori.in A on IN-V2-198)

DNS with PDM (RFC 8250)

Report (testprotocol.in A on IN-V2-7)

DNS Query Reports

Export Result | Query Visibility

Domain	Anchor	Query Type	Answer
Test Protocol	IN-V2-07	A	146.190.62.39

Authoritative Zone

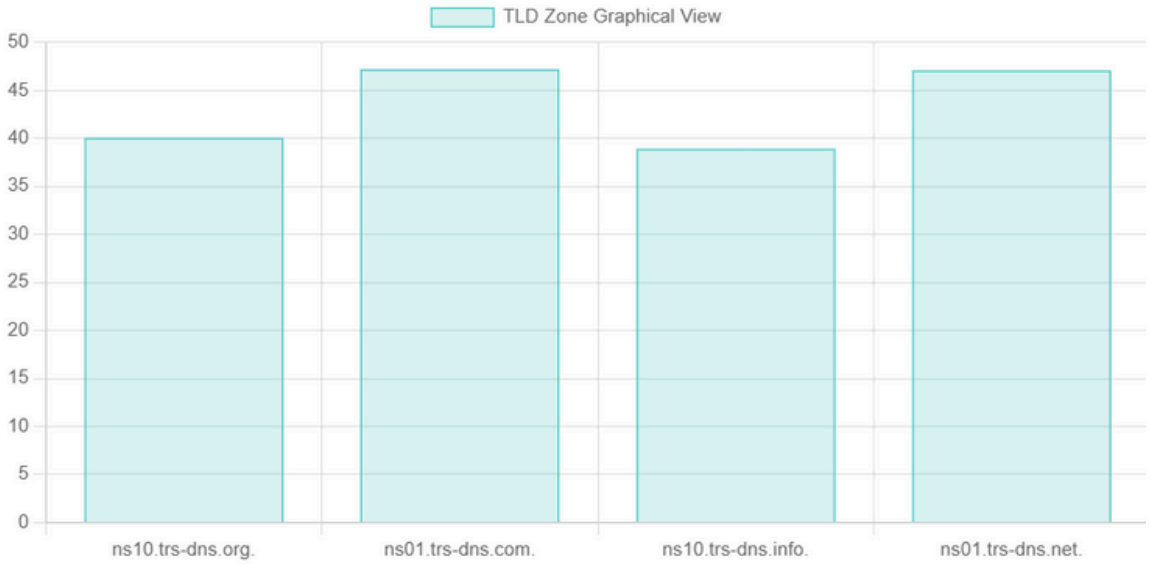
Resource Record	Value	Answered	RTD(ms)	Server Time(ms)	RTT(ms)
ns1.testprotocol.in.	13.127.175.92	True			42.62
ns1.testprotocol.in.	2406:da1a:8e8:e863:ab7a:cb7e:2cf9:dc78	True			91.83
ns2.testprotocol.in.	65.0.92.216	False			35.30
ns2.testprotocol.in.	2406:da1a:8e8:e8cb:97fe:3833:8668:54ad	False	91.695957	0.087424	91.79

DNS with PDM (RFC 8250)

Report (testprotocol.in A on IN-V2-7)

TLD Zone

Resource Record	Value	Time(ms)
ns10.trs-dns.org.	64.78.205.1	40.04
ns01.trs-dns.com.	64.96.1.1	47.22
ns10.trs-dns.info.	64.78.204.1	38.92
ns01.trs-dns.net.	64.96.2.1	47.08

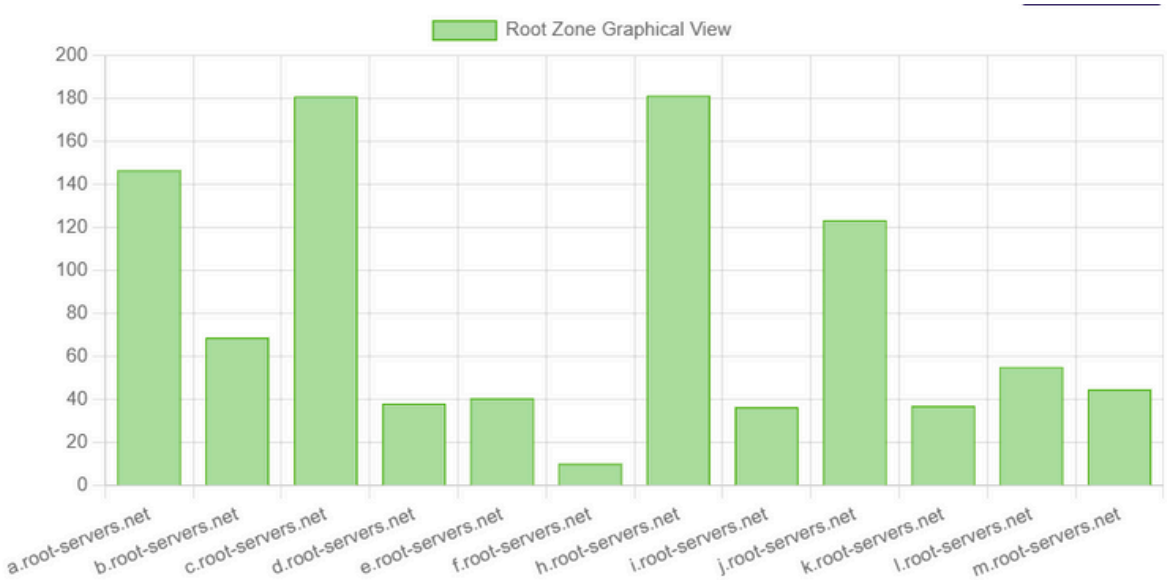


DNS with PDM (RFC 8250)

Report (testprotocol.in A on IN-V2-7)

Root Zone

Resource Record	Value	Time(ms)
a.root-servers.net	198.41.0.4	146.74
b.root-servers.net	199.9.14.201	68.90
c.root-servers.net	192.33.4.12	180.99
d.root-servers.net	199.7.91.13	38.12
e.root-servers.net	192.203.230.10	40.74
f.root-servers.net	192.5.5.241	10.15
h.root-servers.net	198.97.190.53	181.51
i.root-servers.net	192.36.148.17	36.52
j.root-servers.net	192.58.128.30	123.49
k.root-servers.net	193.0.14.129	37.18
l.root-servers.net	199.7.83.42	55.10
m.root-servers.net	202.12.27.33	44.73



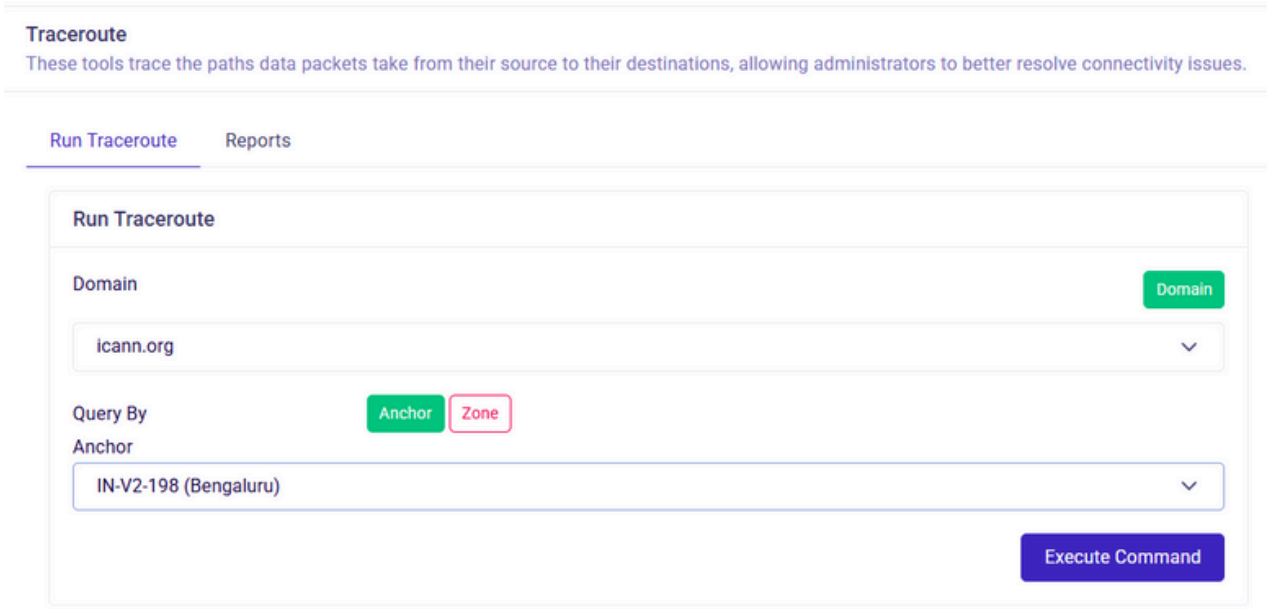
DNS with PDM (RFC 8250)

Report (testprotocol.in A on IN-V2-7) JSON (PDM)


```
"domain_data": {
  "error": {
    "ns3.testprotocol.in.": {
      "error": "No response.: Unknown Exception for Nameserver
ns3.testprotocol.in. 2406:da18:c78:2b8:a93c:708c:4fc7:f75d. "
    },
    "ns4.testprotocol.in.": {
      "error": "No response.: Unknown Exception for Nameserver
ns4.testprotocol.in. 2406:da18:c78:219:22a5:8271:5f0d:780b. "
    }
  },
  "answer": [
    "146.190.62.39"
  ],
  "servers": [
    {
      "ns1.testprotocol.in.": {
        "ip": "13.127.175.92",
        "rtd": null,
        "rtt": 0.042619943618774414,
        "type": "v4",
        "rtd_ms": null,
        "rtt_ms": 42.619943618774414,
        "server": null,
        "is_answer": true,
        "server_ms": null,
        "query_time": 0.042619943618774414
      }
    },
    {
      "ns1.testprotocol.in.": {
        "ip": "2406:da1a:8e8:e863:ab7a:cb7e:2cf9:dc78",
        "rtd": null,
        "rtt": 0.091824417,
        "type": "v6",
        "rtd_ms": null,
        "rtt_ms": 91.824417,
        "server": null,
        "is_answer": true,
        "server_ms": null,
        "query_time": 0.09182977676391602
      }
    },
    {
      "ns2.testprotocol.in.": {
        "ip": "65.0.92.216",
        "rtd": null,
        "rtt": 0.03529644012451172,
        "type": "v4",
        "answer": [
          "146.190.62.39"
        ],
        "rtd_ms": null,
        "rtt_ms": 35.29644012451172,
        "server": null,
        "is_answer": false,
        "server_ms": null,
        "query_time": 0.03529644012451172
      }
    },
    {
      "ns2.testprotocol.in.": {
        "ip": "2406:da1a:8e8:e8cb:97fe:3833:8668:54ad",
        "rtd": 0.091695957,
        "rtt": 0.091783381,
        "type": "v6",
        "answer": [
          "146.190.62.39"
        ],
        "rtd_ms": 91.695957,
        "rtt_ms": 91.783381,
        "server": 0.000087424,
        "is_answer": false,
        "server_ms": 0.087424,
        "query_time": 0.09178876876831055
      }
    }
  ]
},
```

9. Traceroute

Execute icann.org on IN-V2-198



Traceroute

Reports for icann.org on IN-V2-198

Trace Route For Icann.Org

Trace Route For Icann.Org IN-V2-198:-(Bengaluru)

No	Distance	Node	Rtt Max	Rtt Avg	Rtt Min	Latitude	Longitude	Location
1	1	192.168.1.1	0.64	0.529	0.419	13.021368035555746	77.7594387089844	Bengaluru
2	2	10.240.9.208	3.852	3.34	2.829	null	null	null
3	4	125.18.215.57	5.304	5.025	4.747	12.97160	77.59456	Bangalore
4	5	116.119.112.88	118.647	118.113	117.579	48.85717	2.34140	Paris
5	6	62.115.42.118	118.473	117.978	117.483	43.29337	5.37132	Marseille
6	7	212.221.88.253	121.217	120.327	119.436	43.29337	5.37133	Marseille
7	8	213.254.214.158	206.375	205.851	205.328	39.05232	-77.48270	Ashburn
8	9	207.162.206.66	213.395	212.511	211.627	38.92965	-77.19695	McLean
9	10	192.0.43.7	210.764	210.456	210.149	33.98269	-118.40539	Los Angeles

Traceroute

Reports for icann.org on IN-V2-198 - (Download - JSON)


```
{
      "avg_rtt": 120.327,
      "distance": "7",
      "latitude": "43.29337",
      "location": "Marseille",
      "longitude": "5.37133",
      "max_rtt": 121.217,
      "min_rtt": 119.436,
      "node": "212.221.88.253"
    },
    {
      "avg_rtt": 205.851,
      "distance": "8",
      "latitude": "39.05232",
      "location": "Ashburn",
      "longitude": "-77.48270",
      "max_rtt": 206.375,
      "min_rtt": 205.328,
      "node": "213.254.214.158"
    },
    {
      "avg_rtt": 212.511,
      "distance": "9",
      "latitude": "38.92965",
      "location": "McLean",
      "longitude": "-77.19695",
      "max_rtt": 213.395,
      "min_rtt": 211.627,
      "node": "207.162.206.66"
    },
    {
      "avg_rtt": 210.456,
      "distance": "10",
      "latitude": "33.98269",
      "location": "Los Angeles",
      "longitude": "-118.40539",
      "max_rtt": 210.764,
      "min_rtt": 210.149,
      "node": "192.0.43.7"
    }
  ],
```

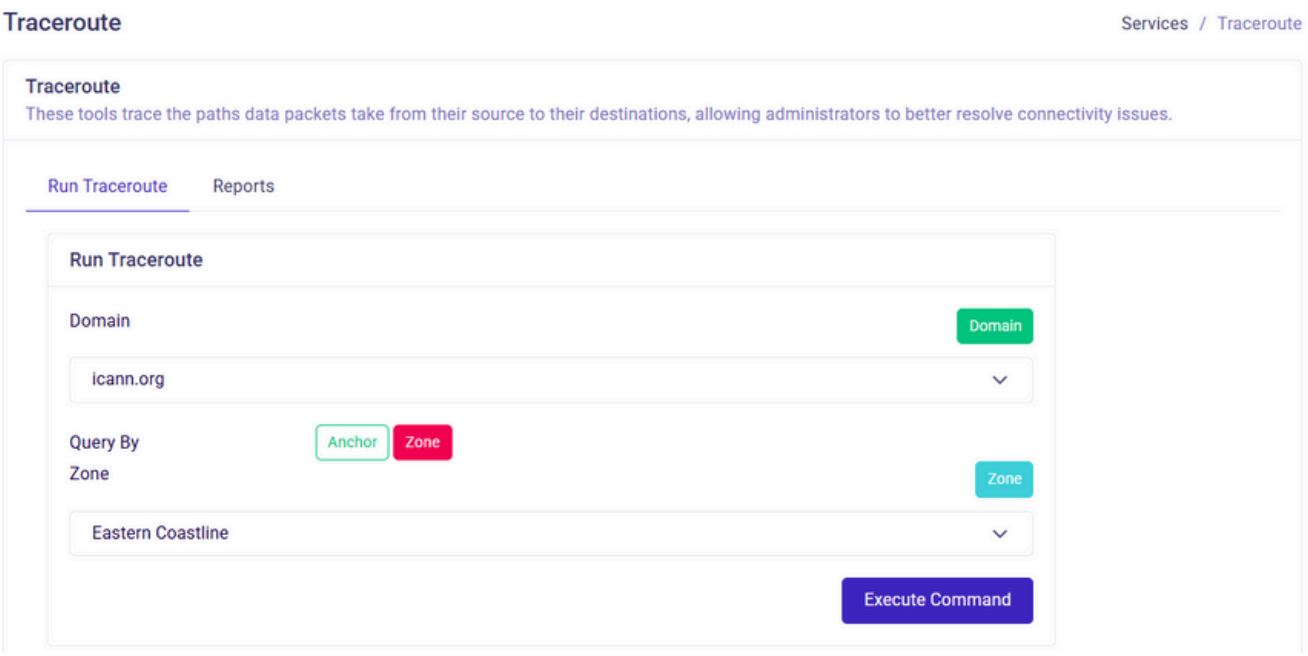
Traceroute

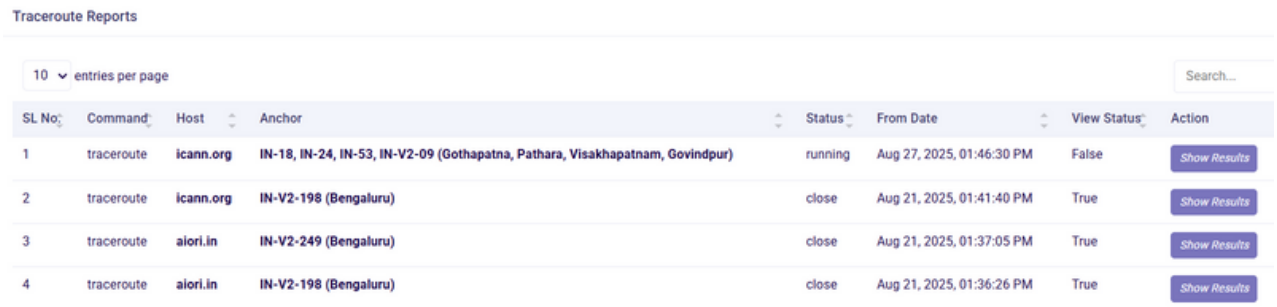
Reports for icann.org on IN-V2-198 - (Download - JSON)

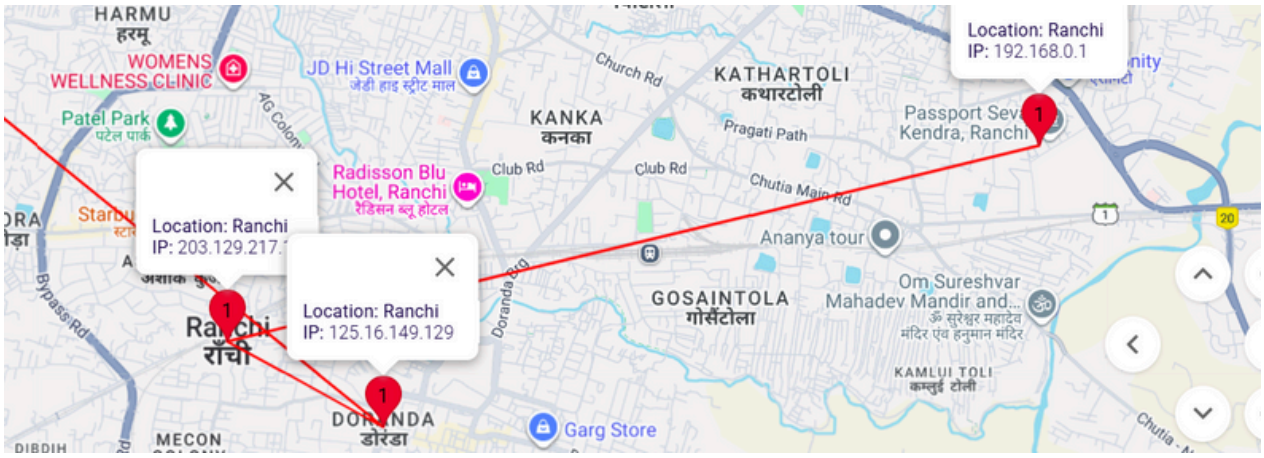

```
"map_data": [
      {
        "ip": "192.168.1.1",
        "latitude": "13.021368035555746",
        "longitude": "77.7594387089844",
        "location": "Bengaluru",
        "distance": 1
      },
      {
        "ip": "125.18.215.57",
        "latitude": "12.97160",
        "longitude": "77.59456",
        "location": "Bangalore",
        "distance": 2
      },
      {
        "ip": "116.119.112.88",
        "latitude": "48.85717",
        "longitude": "2.34140",
        "location": "Paris",
        "distance": 3
      },
      {
        "ip": "62.115.42.118",
        "latitude": "43.29337",
        "longitude": "5.37132",
        "location": "Marseille",
        "distance": 4
      },
      {
        "ip": "212.221.88.253",
        "latitude": "43.29337",
        "longitude": "5.37133",
        "location": "Marseille",
        "distance": 5
      },
      {
        "ip": "213.254.214.158",
        "latitude": "39.05232",
        "longitude": "-77.48270",
        "location": "Ashburn",
        "distance": 6
      },
      {
        "ip": "207.162.206.66",
        "latitude": "38.92965",
        "longitude": "-77.19695",
        "location": "McLean",
        "distance": 7
      },
      {
        "ip": "192.0.43.7",
        "latitude": "33.98269",
        "longitude": "-118.40539",
        "location": "Los Angeles",
        "distance": 8
      }
    ]
  }
 ]
}
```

Traceroute

Execute in Eastern Zone anchors - icann.org



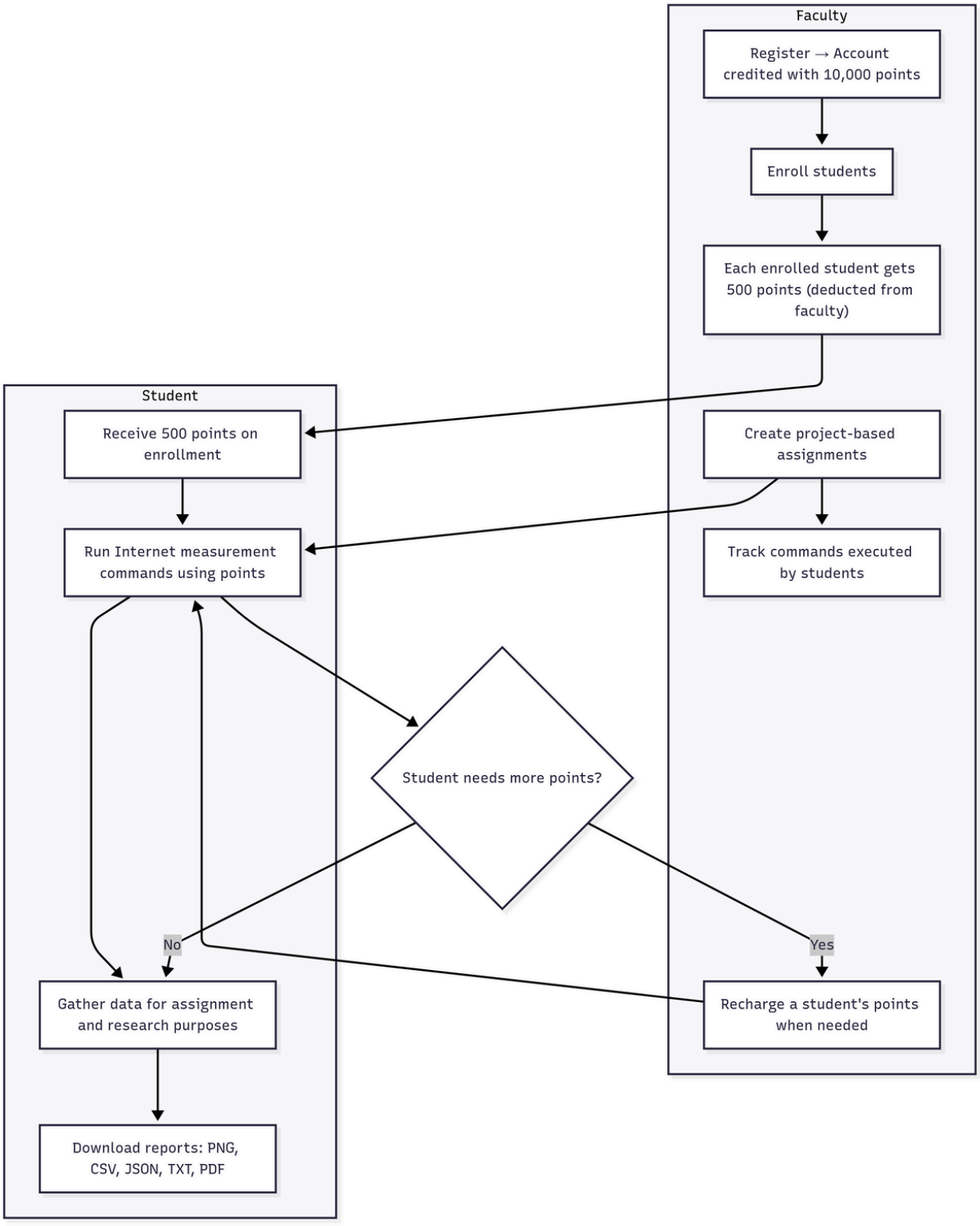




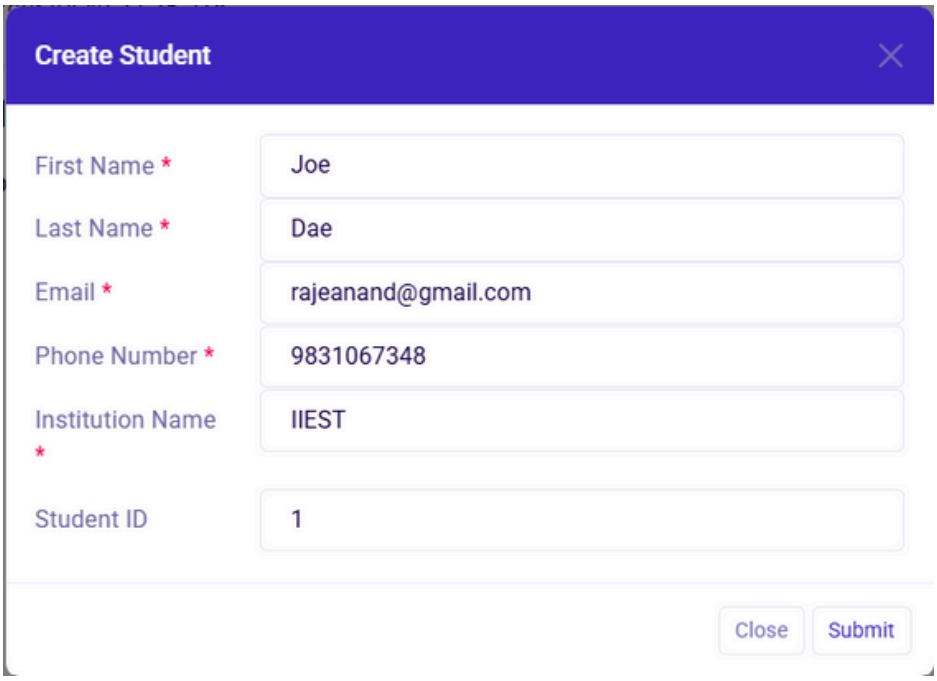
10. How Academic Feature Works?

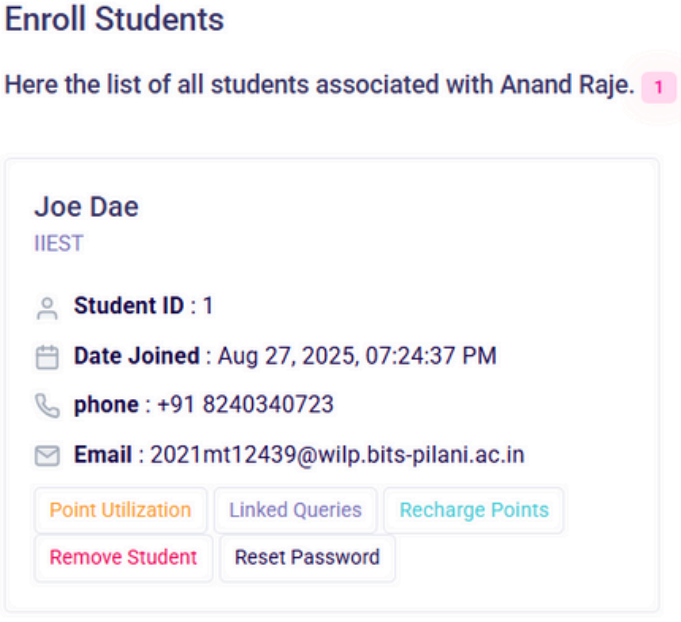
This system introduces a points-based learning model for Internet measurement assignments. When a faculty member registers, their account is credited with points that can be used to enroll students. Each enrolled student receives an initial balance of points, which they use to run Internet measurement commands as part of their coursework. Faculty members can design project-based assignments, monitor the commands executed by students, and recharge points whenever students need more. Students, on the other hand, use these points to conduct real measurements, collect data for assignments and research, and finally download reports in formats like PNG, CSV, JSON, TXT, or PDF. This approach ensures that learning is interactive, measurable, and resource-driven, while also giving both faculty and students a structured way to engage with real Internet data.

The Flowchart



Enroll Students





Enroll Students

Welcome to Our AIORI Platform!

Dear 2021mt12439@wilp.bits-pilani.ac.in,

We're excited to welcome you as a student under: **Anand Raje**. Your account has been successfully created!

Username: 2021mt12439@wilp.bits-pilani.ac.in

Email: 2021mt12439@wilp.bits-pilani.ac.in

To get started, please click the button below to set your password and access your dashboard:

Reset Your Password

Once you've set your password, you can log into your student dashboard using the link below:

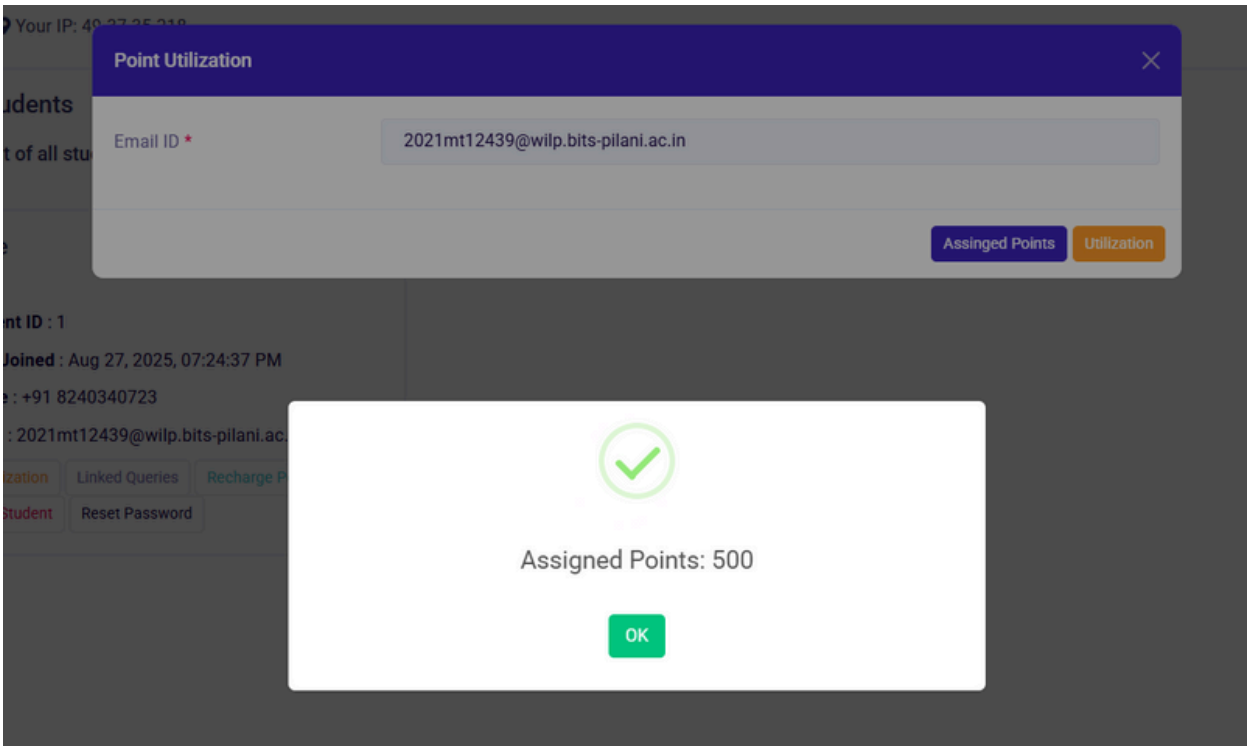
Go to Dashboard

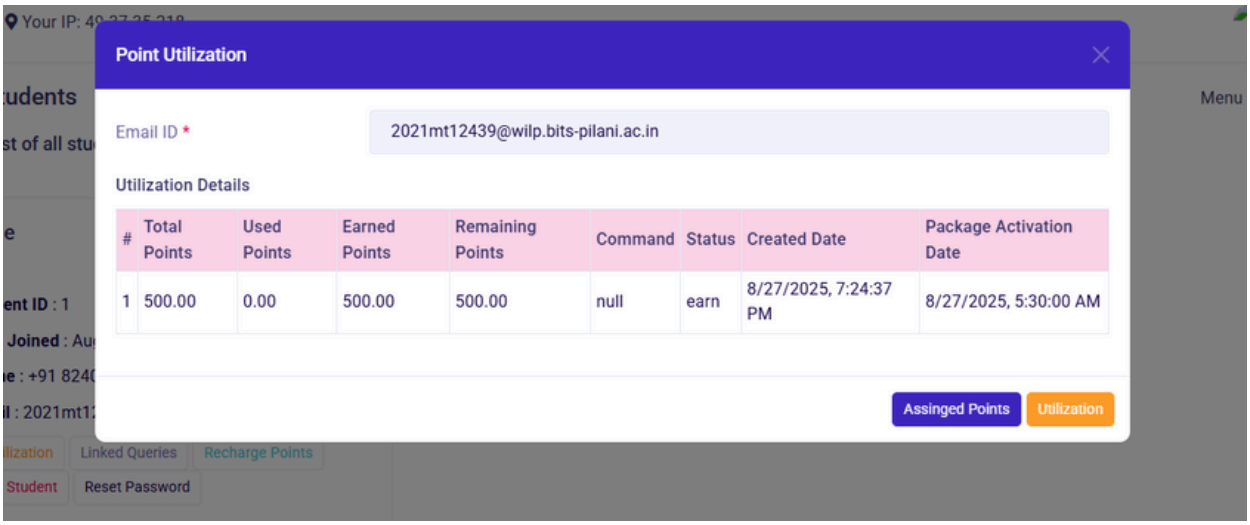
If you face any issues, feel free to contact our support team.

Wishing you a wonderful academic journey!
The AIORI Management Team

Students Management

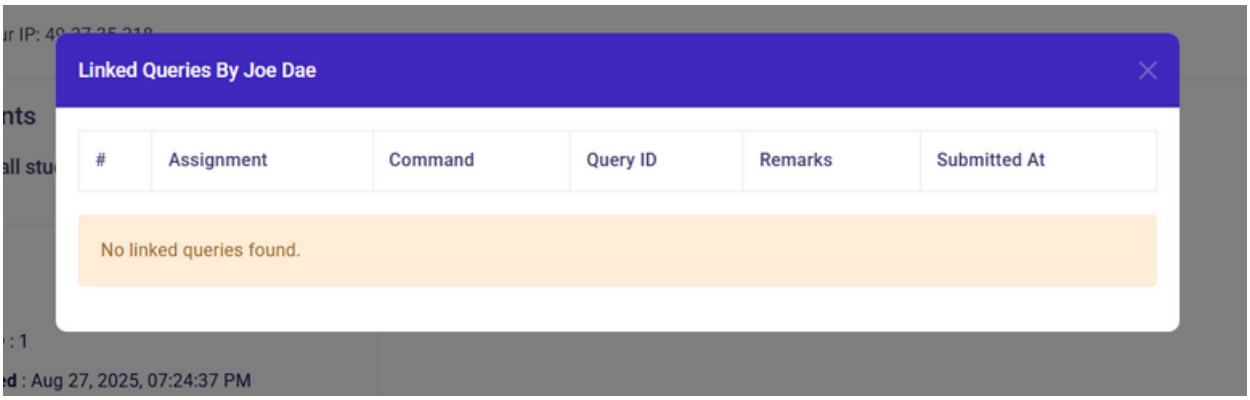
Student Features - Point Utilization





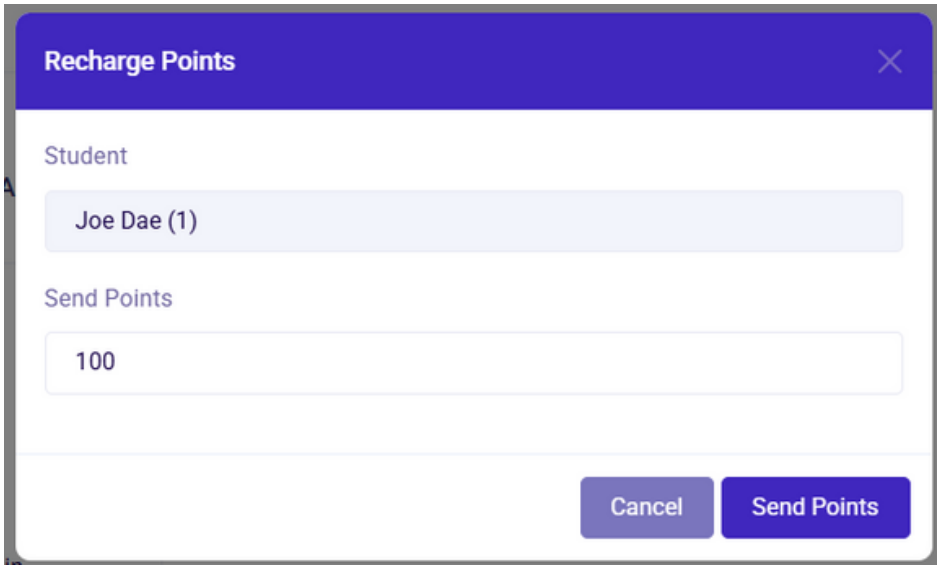
Students Management

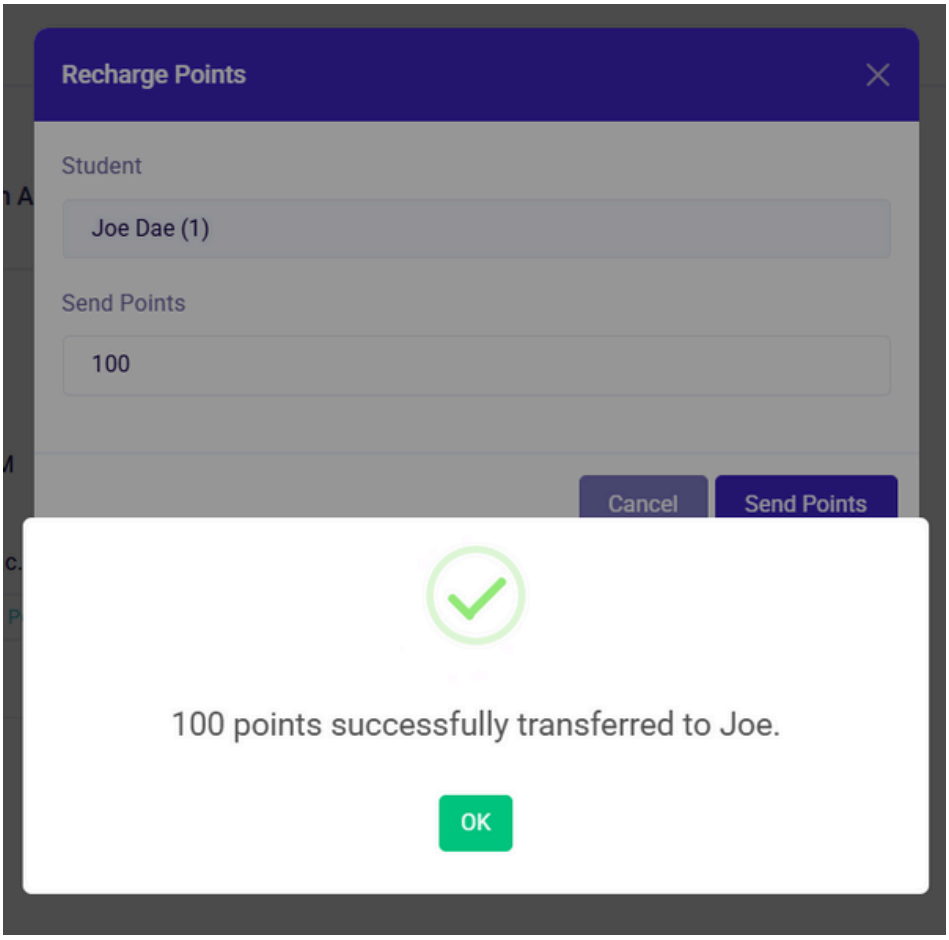
Student Features - Linked Queries



Students Management

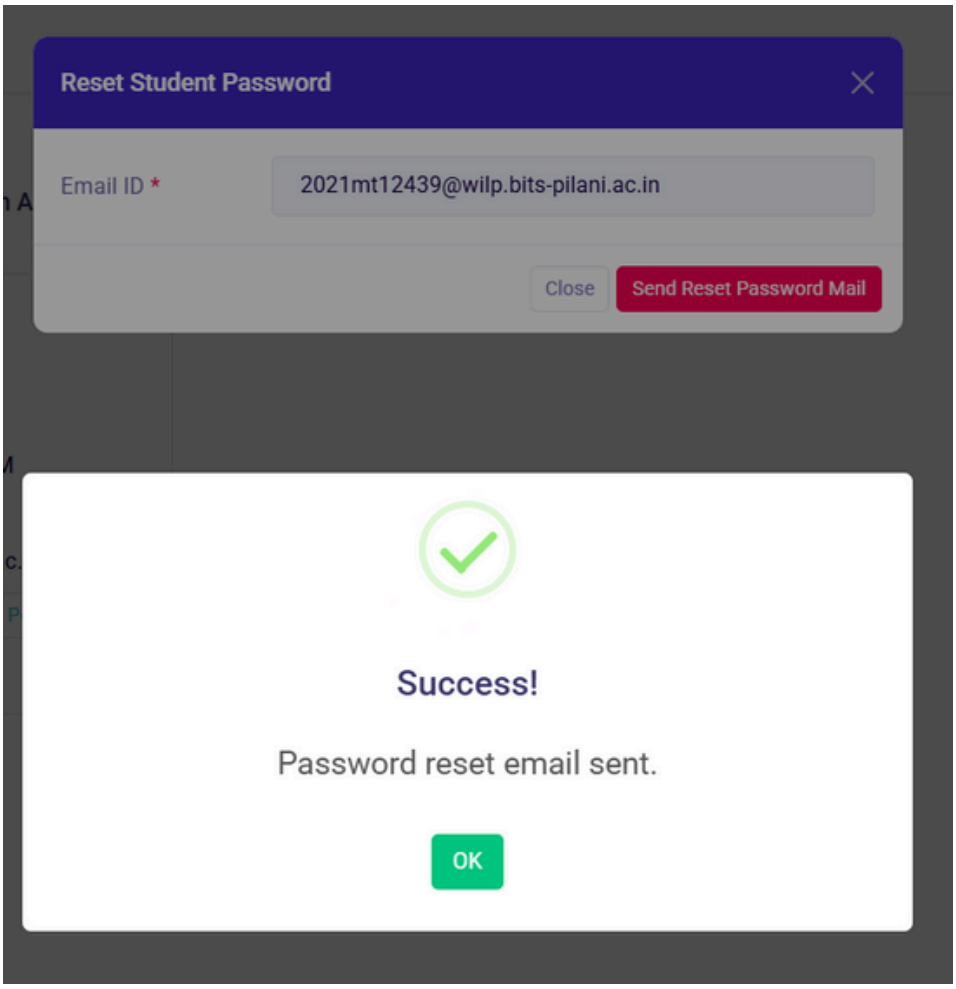
Student Features - Recharge Points

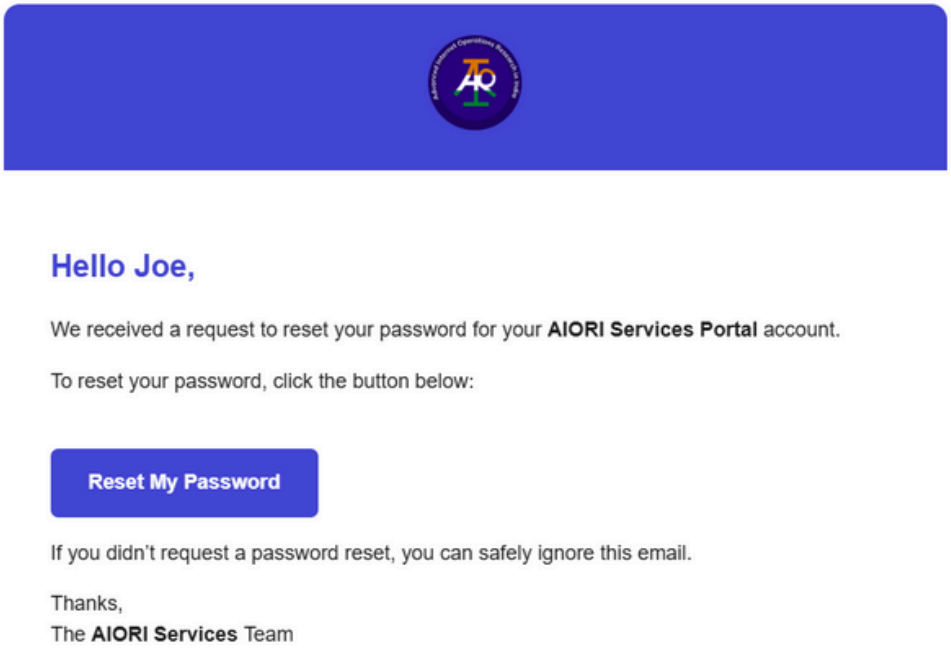




Students Management

Reset Password and Remove Student





Students Management

Reset Password and Remove Student

Assignments

Create Assignment

assignment001.pdf

Assignment: Understanding DNS Resolution (Case Study: aiori.in)

Instructions:
Read the DNS query trace provided (json). Then answer the following questions in your own words. Each answer should explain how DNS hierarchy works and how the resolver reached the final answer.

Part A: Root Level

1. Which root servers were contacted in this query (a.root-servers.net, b.root-servers.net, ...)?
2. What role do root servers play in the DNS hierarchy?
3. Did the root servers return the final IP of aiori.in? If not, what did they provide instead?

Part B: TLD Level (.in)

1. After the root, which TLD servers for .in were queried? Name at least two from the trace.
2. What information did the .in TLD servers return about aiori.in?
3. How do TLD servers help the resolver move one step closer to the answer?

Part C: Authoritative Zone (aiori.in)

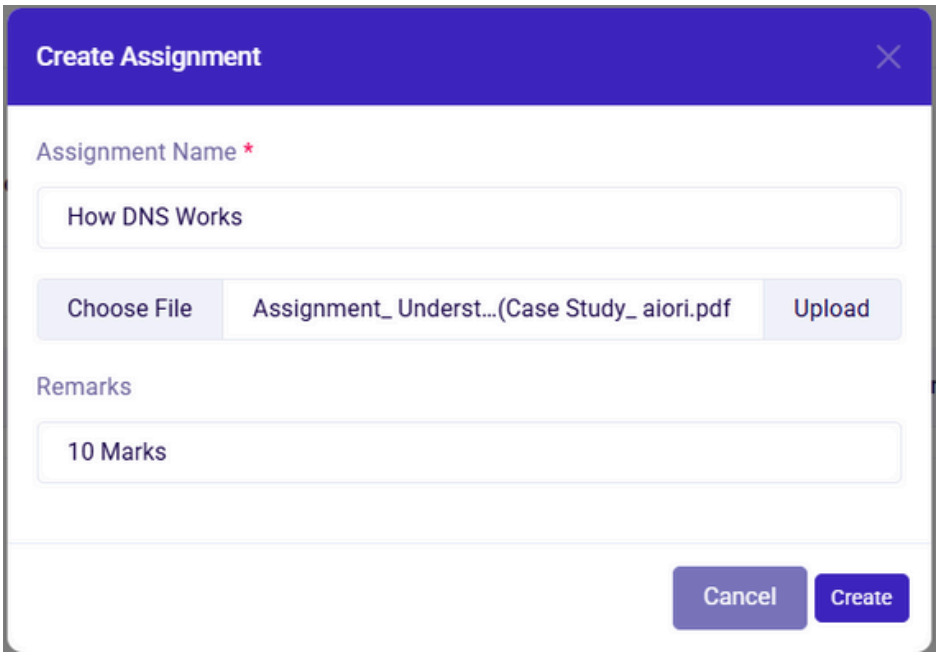
1. Which authoritative nameservers were listed for aiori.in?
2. What was the final A record IP address returned for aiori.in?
3. Did both ns1.aiori.in and ns2.aiori.in respond? If not, explain what errors or differences are visible in the trace.

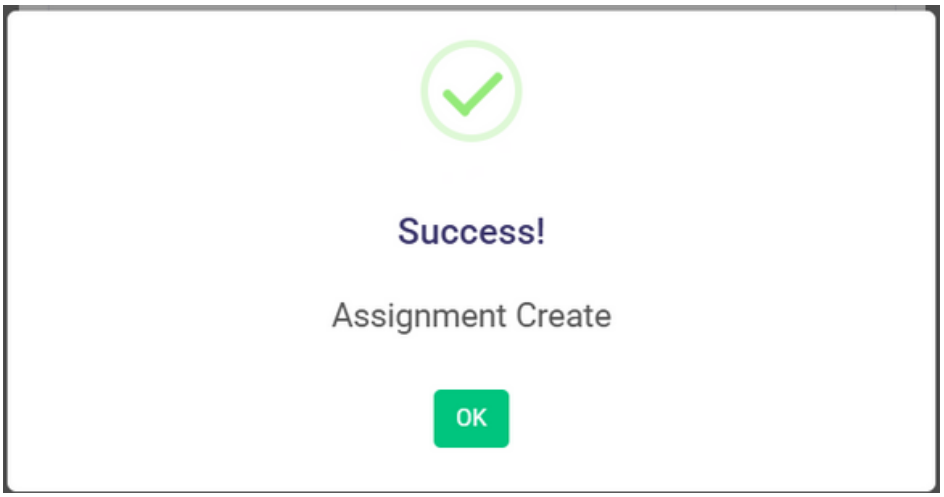
Part D: Putting It All Together

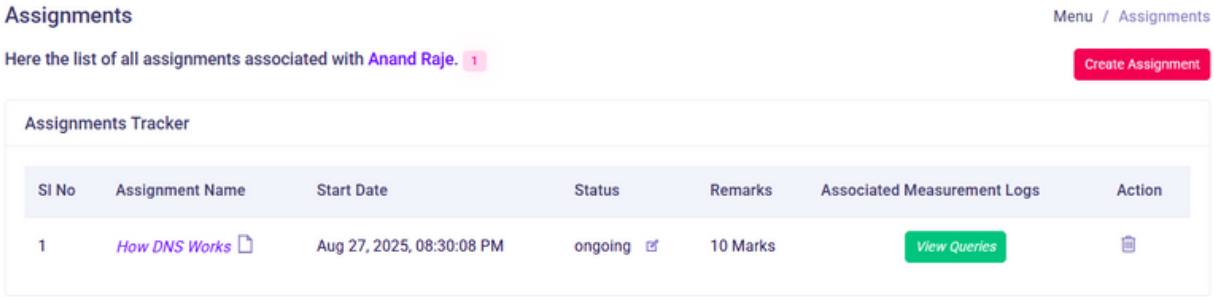
1. Draw or describe the path of resolution from root → TLD → authoritative → final answer.
2. In your own words, explain why DNS is described as a hierarchical, distributed system.
3. Suppose the resolver had cached the .in TLD response — which steps would have been skipped in a repeated query?

Assignments

Create Assignments by Faculty



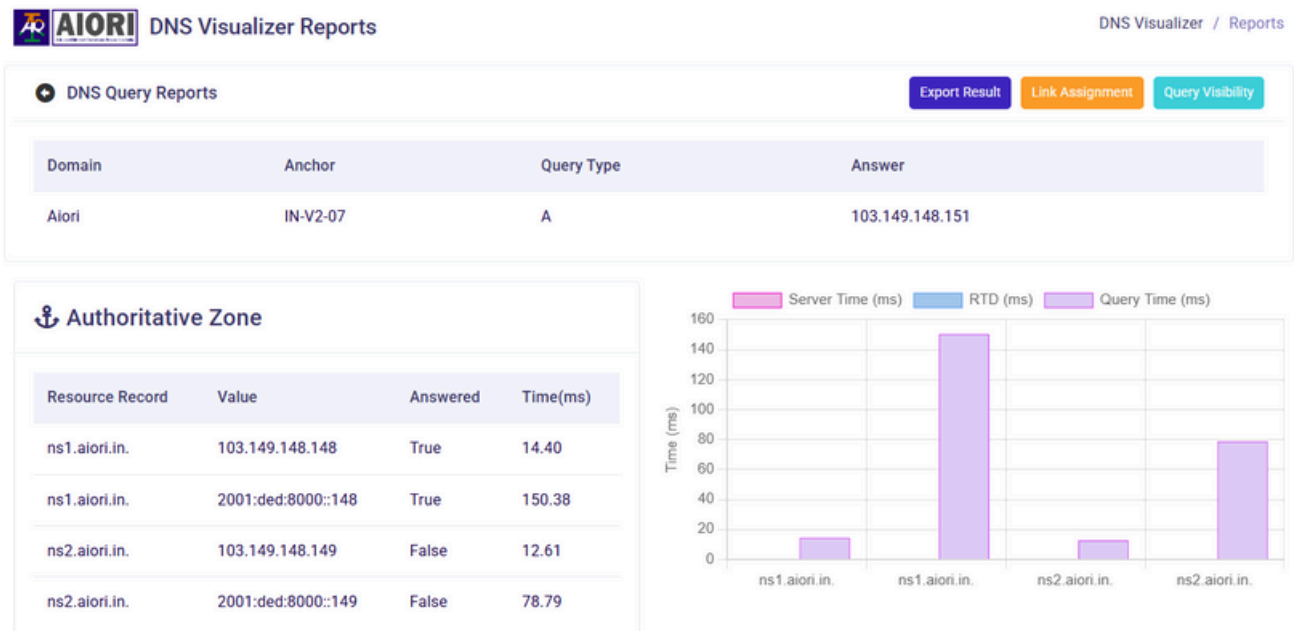




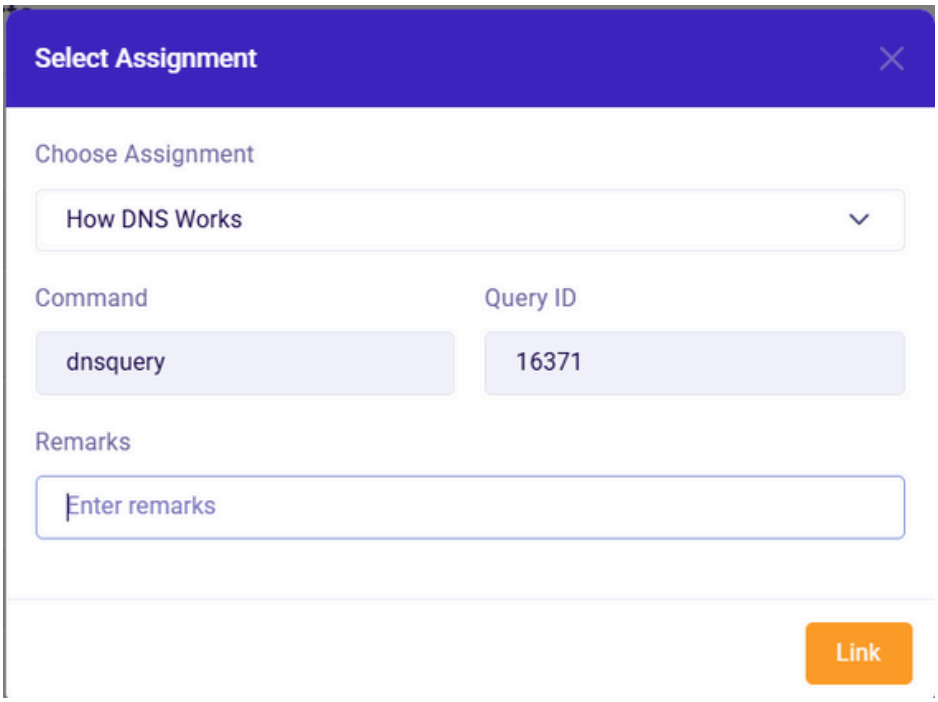
Assignments

Run Query By Students

Login in the Portal



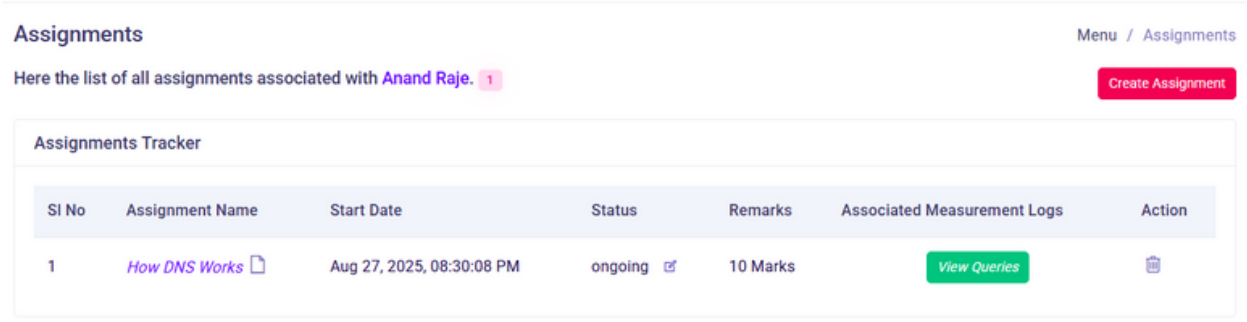
Link Query with an assignment

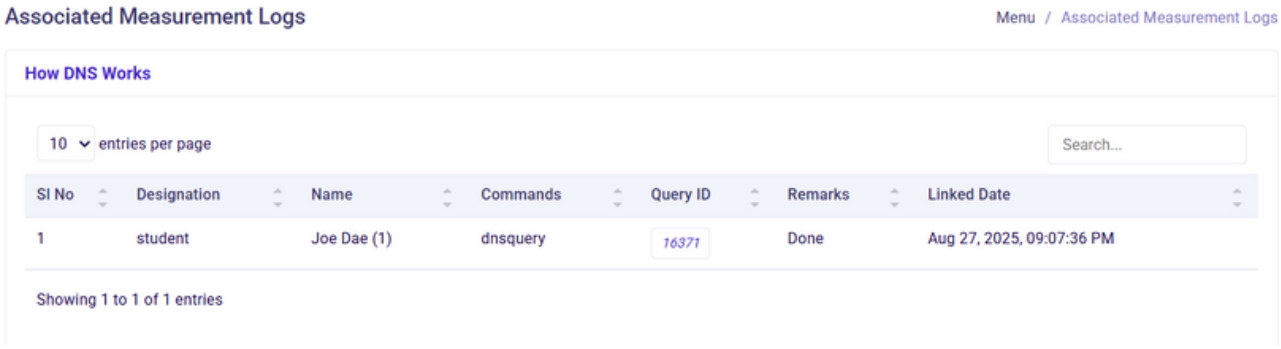


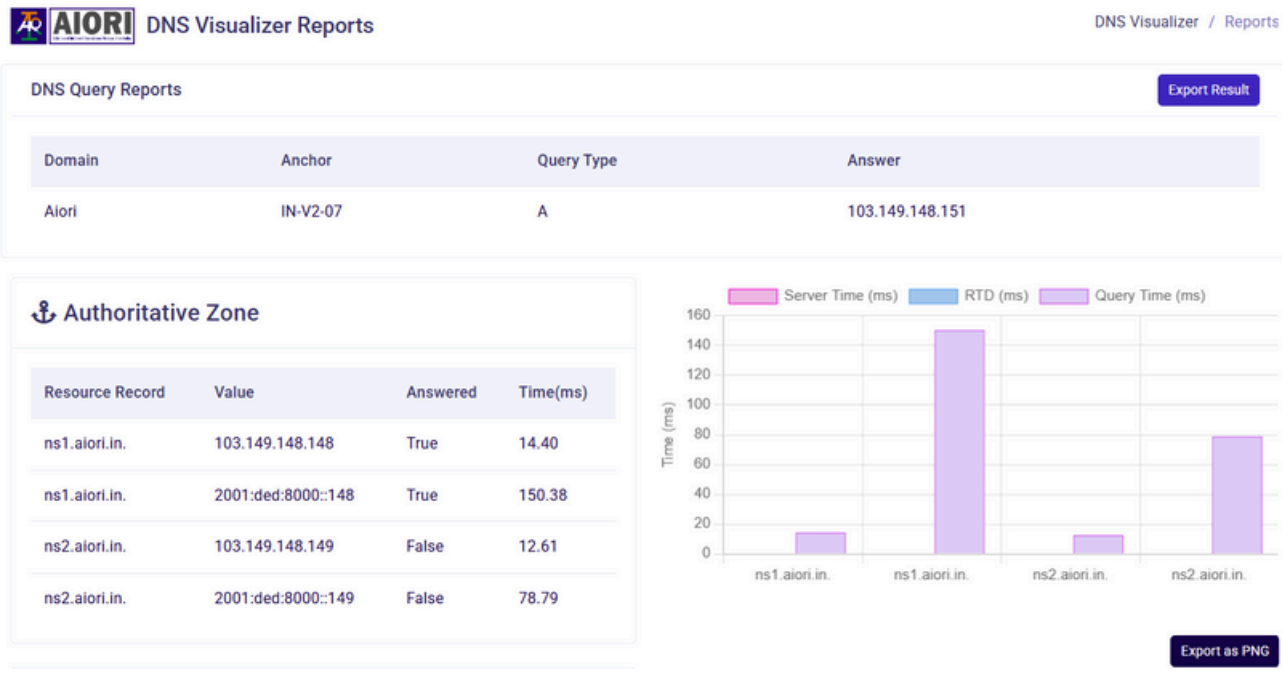
Assignments

Evaluation

Login in the Portal



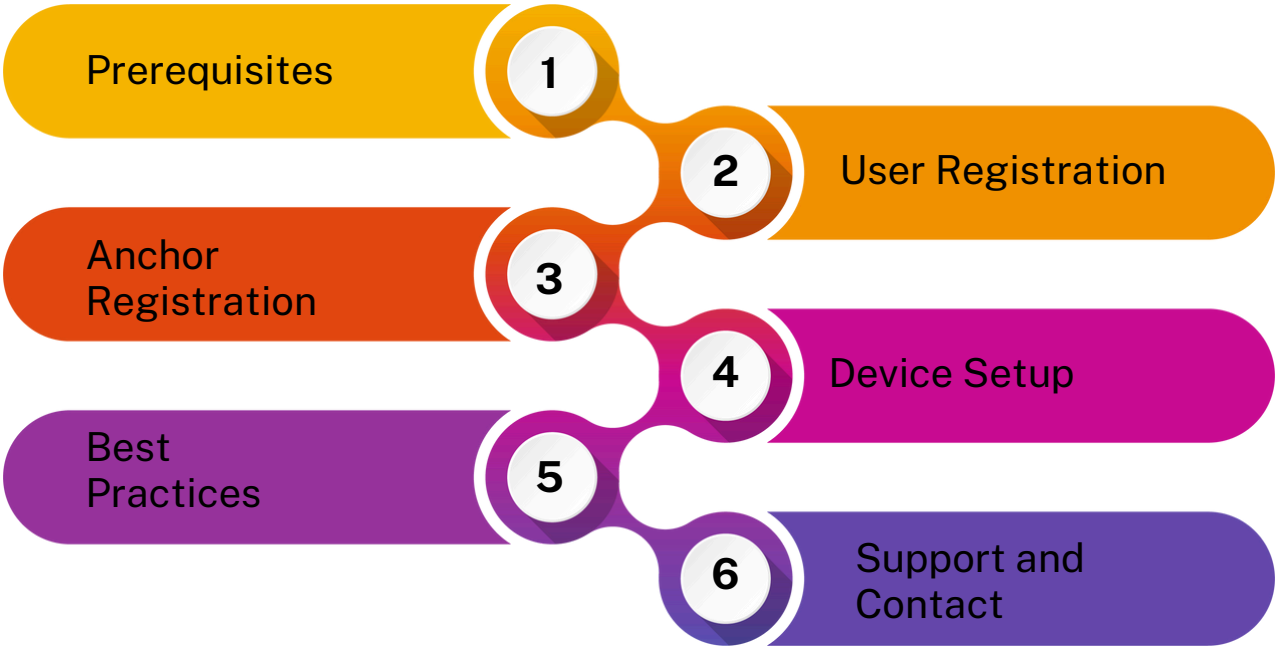




11. Host an Anchor

This handbook provides a comprehensive guide to deploy anchors as part of the Advanced Internet Operations Research in India (AIORI) project. It covers essential steps including equipment preparation, portal registration, device setup, and verification to ensure successful deployment.

The AIORI anchor devices are used for measuring and conducting research related to Internet operations.



Follow these instructions carefully to avoid common deployment issues.

Estimated completion time: 15 - 20 minutes.

1 Prerequisites

Prerequisites

- Stable Internet connection, DHCP enabled
- Web Browser in a connected Laptop/PC/Mobile
- Ensure all items are available before starting.

Items

Measurement Anchor

Provided in the box

Power Adapter

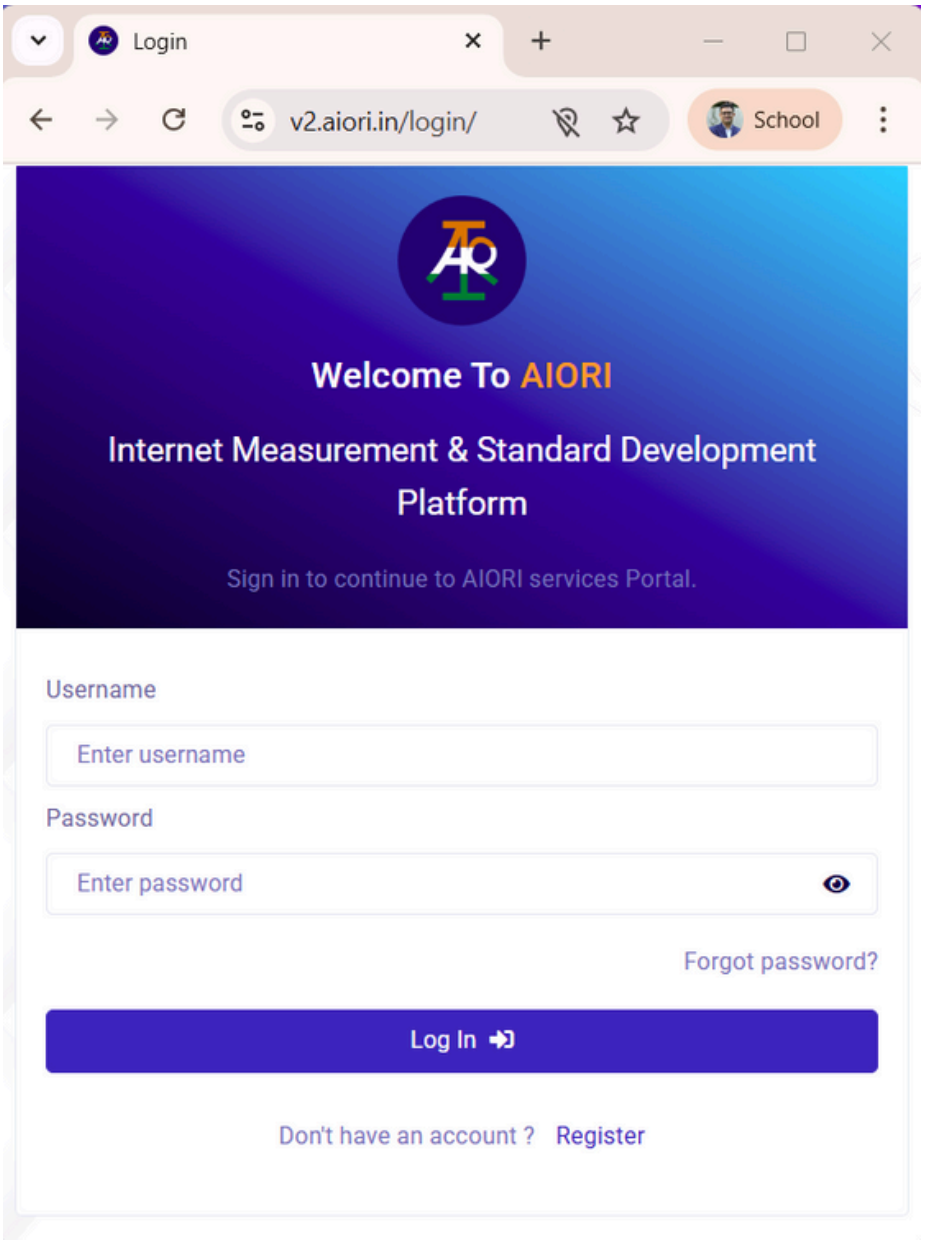
Provided in the box

Ethernet Cable

Provided Separately

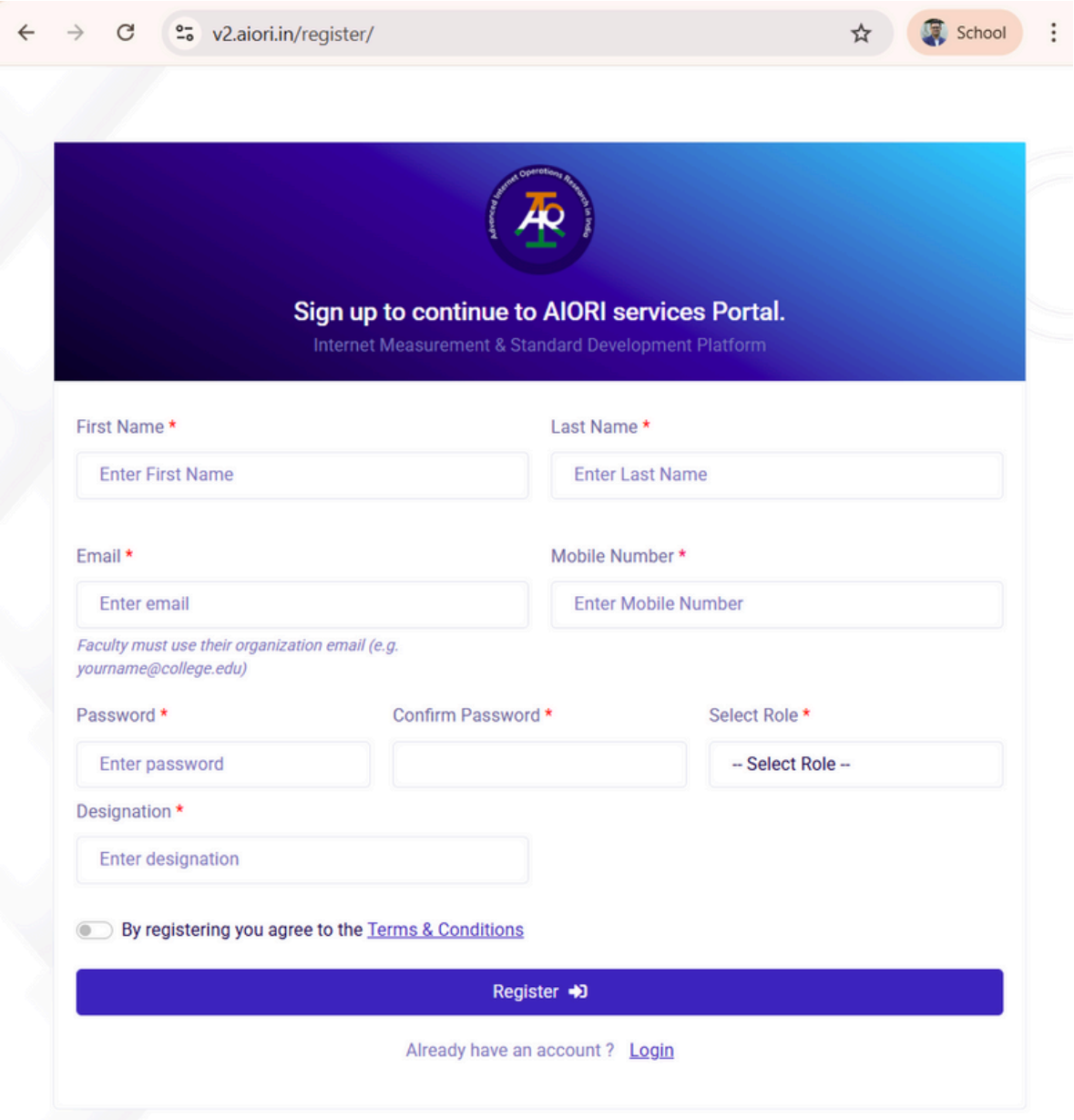
2 User Registration

Visit the AIORI Portal : Access the portal at https://v2.aiori.in for registration.



2 User Registration

If you have not yet registered, go to: https://v2.aiori.in/register/ and fill details



Note while Selecting Role: Use your Official institutional Email ID if you are registering as faculty. Faculties can register students under the role.

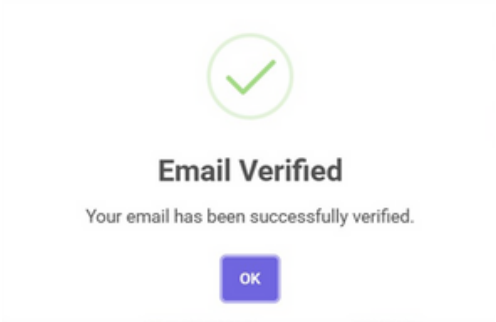
2 User Registration

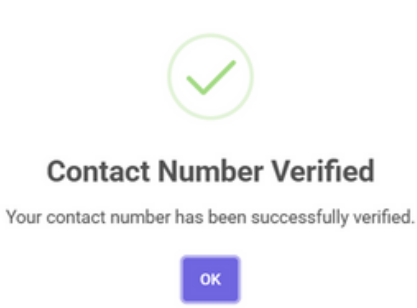
OTP Verification for E Mail and Mobile Phone

Click “**Send OTP**” to receive a One-Time Password on both your email and mobile number.

- Enter the respective OTPs and click “**Verify OTP**” for each.
- Both email and phone number verification are mandatory to complete the registration process.

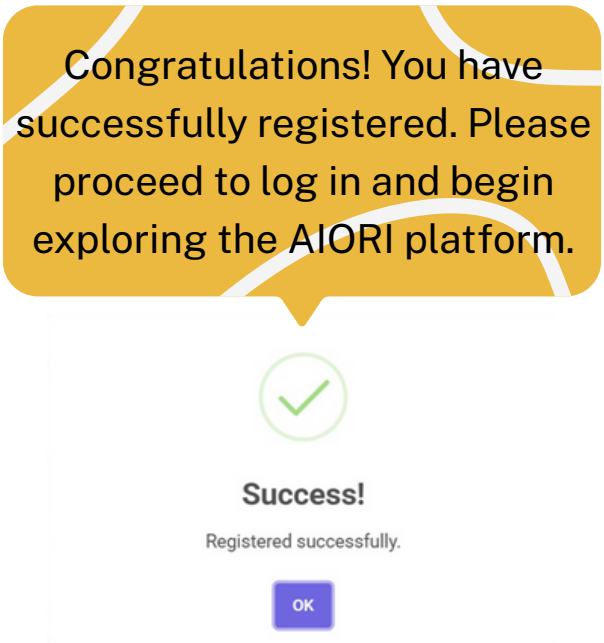
Upon successful verification, a confirmation message will appear





Finalize Your Registration

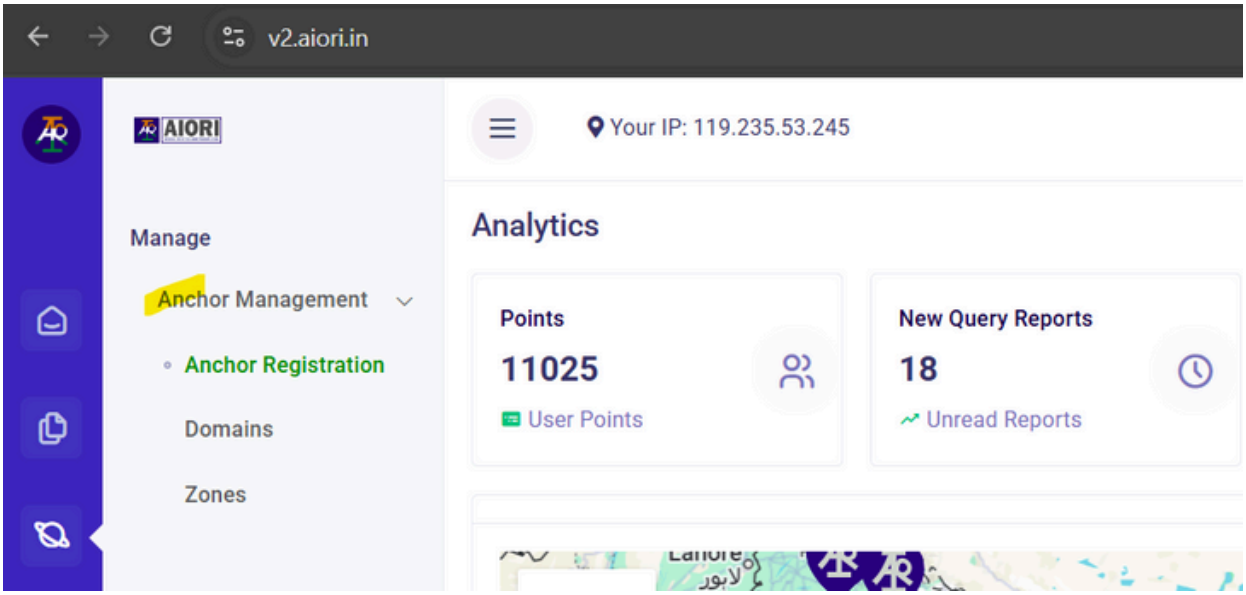
- Enter your Institution Name and Designation.
- Review and accept the Terms of Use.
- Click on “Register” to complete the process.



3 Anchor Registration

Log in to the AIORI Portal
Visit https://v2.aiori.in/login
Log in using your registered credentials.

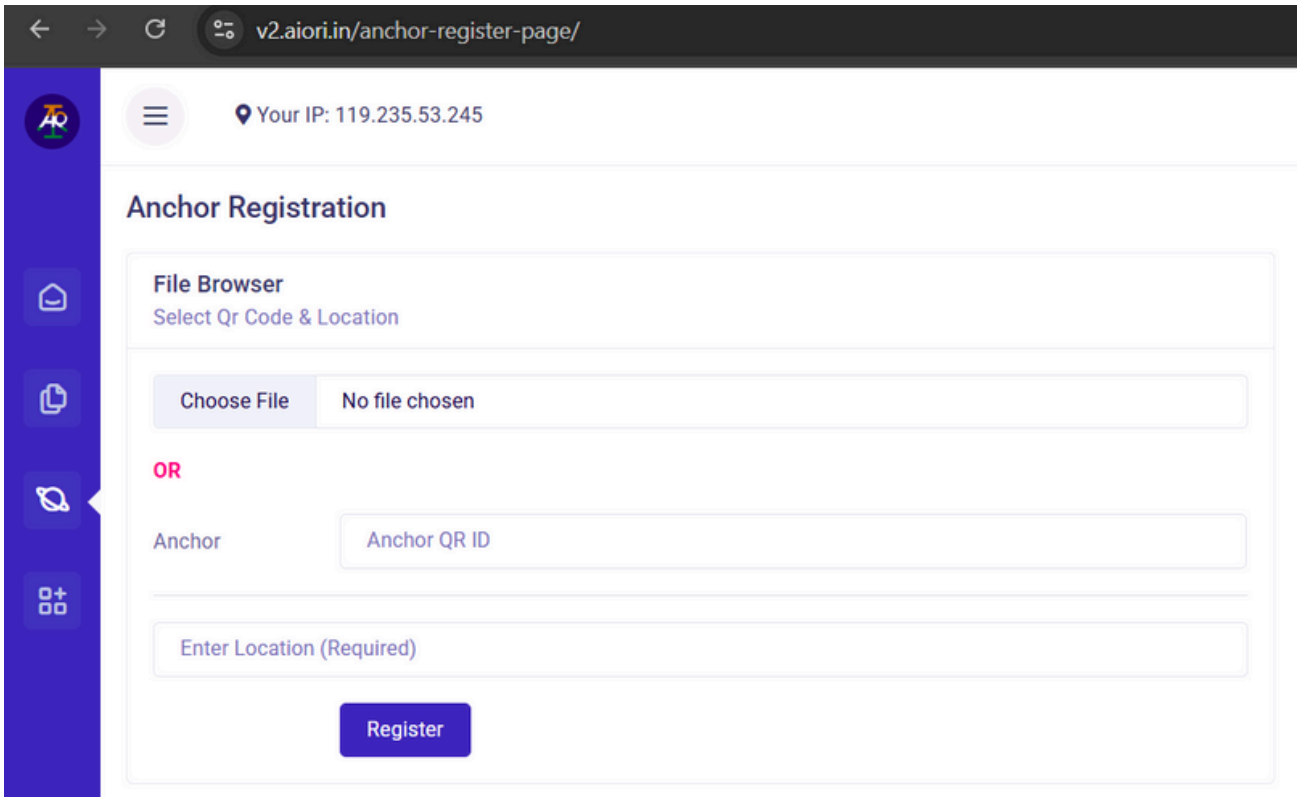
Access the Anchor Registration Section
From the homepage, navigate to the left side panel.
Click on Manage > Anchor Management > Anchor Registration.



3 Anchor Registration

Register the Anchor

- **Preferred Method:** Upload a clear image of the QR code attached to the anchor device.
- **Alternate Method:** Manually scan the QR code and paste the Anchor QR ID in the provided field.



Specify Deployment Location

Enter the location where the anchor is deployed. It can be updated later using “Update Status” option.

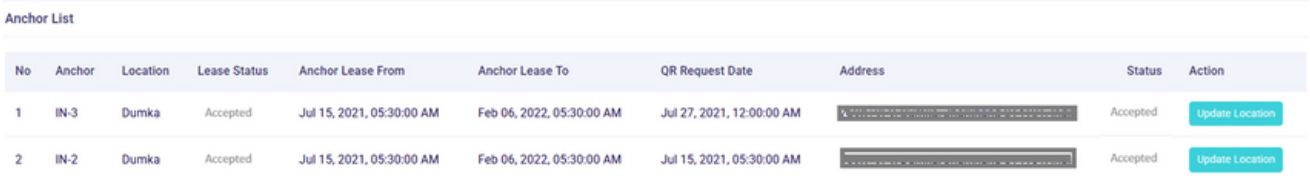
3 Anchor Registration

Complete Registration

Click Register to finalize the anchor addition.

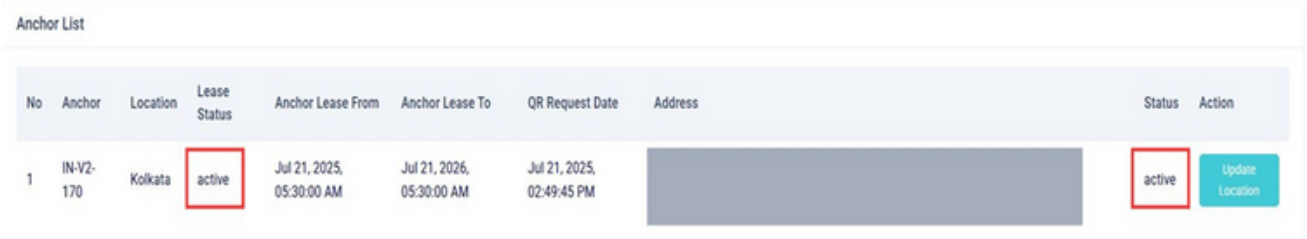
Confirmation

Once registered, the anchor will appear in the Anchor List section for monitoring and management and will have Lease Status and Status “Accepted”



Activating Anchor

Go to step 4 for activating the anchor. Once the anchor is activated the Lease Status and Status will be turned to “Active” and the anchor will be ready to use.



4 Device Setup

A Connect to network

Plug an Ethernet cable into the anchor device and connect it to the local network (router/switch). The anchor supports plug-and-play functionality. It will automatically obtain an IP address via DHCP from the local network.

B Connect to power

Attach the provided power adapter to the anchor and plug it into a reliable power source.

C Power on the device

Switch on the device (if applicable). Allow approximately 3 minutes for the device to fully boot. Once powered on, the anchor will attempt to connect to the network automatically

D Verify device status

Check the LED indicators on the device.

- Power LED should be solid or blinking, indicating the device is receiving power.
- Network LED should show connectivity status (refer to the device manual for LED patterns).

5 Best Practices

To ensure reliable and uninterrupted anchor operation, please follow these best practices

1 **Physical Security**

Secure the anchor device in a safe and stable location to prevent unauthorized access or tampering.

2 **Environmental Care**

- Place the device in a clean, dust-free environment.
- Avoid exposure to extreme temperatures or moisture.

3 **Continuous Monitoring**

- Regularly monitor the device status and performance through the AIORI portal.
- Check for any alerts or anomalies and take prompt action if required.

aiori@iifon.net

portal.aiori.in

https://v2.aiori.in/discussion/

@aiori-vid

+919051624466