Table of Contents

About WHOIS 1

What is WHOIS? 1

History of WHOIS 2

What's on the Horizon? 5

Technical Overview 6

Current Technical Specification 6

DNS and WHOIS – How it Works 7

DNS and WHOIS – How it Works 7

The Domain Name Registration Process 9

The Domain Name Registration Process 9

Using WHOIS 11

Basics of WHOIS 11

Starting Point for a WHOIS Query 11

Accessing WHOIS 11

Uses of WHOIS 12

Keeping WHOIS accurate 12

Privacy Issues 13

Glossary of WHOIS Terms 13

# About WHOIS

WHOIS isn’t an acronym, though it may look like one. In fact, it is the Internet protocol that asks the question, *who is* responsible for a domain name or an IP address?

## What is WHOIS?

Every year, millions of individuals, businesses, organizations and governments register domain names. Each one must provide identifying contact information which may include: name, address, email, phone number, and administrative and technical contacts. This information is often referred to as “WHOIS data.” But the WHOIS service is not a single, centrally-operated database. Instead, the data is managed by independent entities known as “registrars” and “registries.” Any entity that wants to become a registrar must earn ICANN accreditation. Similarly, registries are under contract with ICANN to operate a generic top-level domain, such as .COM, .ORG, or one of the new ones that may soon be under operation.

ICANN’s Affirmation of Commitments requires it to “implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information....” To do that, registrars and registries provide public access to data on registered names. Anyone can use the WHOIS protocol to search their databases and identify the registered name holder or “registrant” of a domain name.

WHOIS data also allows network administrators to find and fix system problems, determine the availability of domain names, combat spam or fraud, identify trademark infringement and enhance accountability of domain name registrants. It is also sometimes used to track down and identify registrants who may be posting illegal content or engaging in phishing scams.

Because information can change, ICANN requires registrars to provide registrants with an annual opportunity to review and correct their WHOIS data. Conversely, Internet users who find that their WHOIS data is incomplete or incorrect can file a complaint with ICANN.

Some registrars offer privacy or proxy services to shield registrants who don’t want their personal information to appear in the database. Likewise, registrars in countries where privacy laws restrict the collection and publishing of personal data may be eligible to apply to ICANN for a WHOIS waiver.

## History of WHOIS

WHOIS traces its roots to 1982, when the Internet Engineering Task Force published a protocol for a directory service for ARPANET users. Initially, the directory simply listed the contact information that was requested of anyone transmitting data across the ARPANET. As the Internet grew, WHOIS began to serve the needs of different stakeholders such as registrants, law enforcement agents, intellectual property and trademark owners, businesses and individual users. But the protocol remained fundamentally based on those original IETF standards. This is the WHOIS protocol that ICANN inherited when it was established in 1998. On 30 September 2009, ICANN and the U.S. signed an Affirmation of Commitments (AOC) that recognizes ICANN as an independent, private and non-profit organization.

A key provision in the AOC stated that ICANN “commits to enforcing its existing policy relating to WHOIS, subject to applicable laws. Such existing policy requires that ICANN implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information.” The AOC also set up specific provisions for periodic reviews of WHOIS policy.

In 1999, ICANN began allowing other entities to offer domain name registration services. Registries are responsible for maintaining registries of top-level domain names.

Over the years, ICANN has used its agreements with registrars and registries to modify the WHOIS service requirements. These agreements set up the basic framework that dictates how the WHOIS service is operated. In addition, ICANN adopted several consensus policies aimed at improving the WHOIS service. The policies are:

* [WHOIS Data Reminder Policy](file://localhost/en/whois-data-reminder-policy-wdrp) (2003): at least once a year, registrars must email all registrants and remind them to review and update their WHOIS data; for example, in case of a new cell phone number or changed business address.
* [The Restored Name Accuracy Policy](file://localhost/en/restored-name-accuracy-policy-rnap) (2004): If a domain name is deleted because it contained incorrect contact data, or there was no response to requests for information, the name must remain on hold until the registrant provides updated and accurate WHOIS data.
* [WHOIS Marketing Restriction Policy](file://localhost/en/whois-marketing-restriction-policy-wmrp) (2004): This policy creates two changes to the Registrar Accreditation Agreement to try to bar use of the WHOIS data for marketing and re-use. Registrars must require third parties to “to agree not to use the [WHOIS] data to allow, enable, or otherwise support any marketing activities,” and “not to sell or redistribute the [WHOIS] data” (with some exceptions).
* [WHOIS Data Problem Reporting System](file://localhost/en/whois-data-reminder-policy-wdrp): a mechanism for reporting allegedly inaccurate WHOIS data. Complaints submitted through this system are forwarded to Registrars. Registrars must take reasonable steps to investigate reported inaccuracies. Under ICANN’s WHOIS system, the registrant is responsible for providing correct information. Failure to do so can result in cancellation of the domain name.

ICANN’s WHOIS protocol remains largely unchanged since 1999---in spite of over a decade of task forces, working groups and studies, and changes in privacy laws. As a result, WHOIS is at the center of long-running debate and study at ICANN, among other Internet governance institutions, and in the global Internet community.

The evolution of the Internet ecosystem has created challenges for WHOIS in every area: accuracy, access, compliance, privacy, abuse and fraud, cost and policing. Questions have arisen about the fundamental design of WHOIS, which many believe is inadequate to meet the needs of today’s Internet, much less the Internet of the future. Concerns about WHOIS obsolescence are equaled by concerns about the costs involved in changing or replacing WHOIS.

WHOIS faces these challenges because its use has expanded beyond what was envisaged when its founding protocol was designed. Many more stakeholders make use of it in legitimate ways not foreseen by its creators. So ICANN has had to modify WHOIS over the years; the consensus policies on accuracy are a prime example, as well as the introduction of validation and verification requirements in the new form of Registrar Accreditation Agreement (2013 RAA).

There are other challenges to WHOIS, as well. As domain names have become an important weapon to combat fraud and abuse, ICANN’s Security and Stability Advisory Committee recommended in [SAC 38: Registrar Abuse Point of Contact](http://www.icann.org/en/groups/ssac/documents) that registrars and registries publish abuse point of contact information. This abuse contact would be responsible for addressing and providing timely response to abuse complaints received from recognized parties, such as other registries, registrars, law enforcement organizations and recognized members of the anti-abuse community. Beginning in 2014, registrars under the 2013 RAA will be required to publish WHOIS data that includes registrar abuse contacts.

Even with these modifications, there are calls in the community for improvements to the current WHOIS model. ICANN’s Generic Names Supporting Organization (GNSO) explores these areas and works to develop new policies to address each issue, as appropriate. Over the last decade, the GNSO has undertaken a series of activities to reevaluate the current WHOIS system, and has sought to collect data examining the importance of WHOIS to stakeholders. At the request of the Council, ICANN has initiated a series of WHOIS studies:

WHOIS Misuse -- This study examines the extent to which public WHOIS data is misused to address harmful communications such a phishing or identity theft. The Carnegie Mellon University Cylab in Pittsburgh, PA, USA is performing this study and expects to have initial results in late 2013.

WHOIS Registrant Identification – This study uses WHOIS data and content associated with domain names to classify entities that register gTLD domain names, including natural persons, legal persons, and Privacy and Proxy service providers. Using associated Internet content, it then classifies entities using those domains and potentially commercial activities. NORC at the University of Chicago is performing this study and [initial results have been posted for public comment](http://www.icann.org/en/news/public-comment/whois-regid-15feb13-en.htm).

WHOIS Privacy and Proxy Services Abuse – This study examines the extent to which gTLD domain names used to conduct alleged illegal or harmful Internet activities are registered via Privacy or Proxy services to obscure the perpetrator's identity. The National Physical Laboratory of the United Kingdom is performing this study, with results expected in late 2013.

WHOIS Privacy and Proxy Relay and Reveal – A survey is underway to assess the feasibility of conducting an in-depth study into communication Relay and identity Reveal requests sent for gTLD domain names registered using Proxy and Privacy services. The Interisle Consulting Group in Boston, MA, USA performed this survey and [posted final results following public comment](http://www.icann.org/en/news/public-comment/whois-pp-survey-04jun12-en.htm).

WHOIS Service Requirements Survey – This study will survey community members to estimate the level of agreement with the conclusions and assumptions in the Inventory of WHOIS Service Requirements – Final Report. A GNSO Working Group was assembled to create a survey and this work is underway.

SSAC in its Report on WHOIS Terminology and Structure – To clear up the confusion regarding the various meanings of WHOIS, ICANN has accepted the recommendations of this report, recommending that ICANN transition to adopting new terminology to designate the different aspects of WHOIS. As a result, ICANN also uses this new terminology to refer to the WHOIS system, which includes:

* **Domain Name Registration Data** – refers to the information that registrants provide when registering a domain name and that registrars or registries collect.
* **Domain Name Registration Data Access Protocol** – refers to the elements of a communications exchange—queries and responses—that make access to registration data possible. For example, the WHOIS protocol (RFC 3912) and Hypertext Transfer Protocol (HTTP) (RFC 2616 and its updates) are commonly used to provide public access.
* **Domain Name Registration Data Directory Service** – refers to the service offered by registries and registrars to provide access to the domain name registration data.

## What's on the Horizon?

It’s very likely that WHOIS will change dramatically in the future. The process of re-inventing WHOIS began in November 2012, when ICANN’s Board approved a two-pronged strategy to embrace the recommendations made by the WHOIS Review Team (RT) to improve the manner in which the current WHOIS system was being overseen by ICANN, and at the same time, to accept SAC’s recommendations to redefine the purpose and scope of data directory services, in an attempt to identify a replacement system better suited for the needs of tomorrow’s Internet.

Following the WHOIS RT’s recommendations, ICANN is working on a series of improvements to the WHOIS system to enhance its usefulness to Internet users. This WHOIS portal is intended to be a one-stop shop for WHOIS related inquiries, to include WHOIS look-ups for both “thin” and “thick” registries, as well as educational materials where the WHOIS policy is summarized and readily accessible from one location. ICANN is currently building online capability to proactively identify inaccurate WHOIS records and forward them to registrars for follow-up, as part of a new effort to increase data accuracy and create accuracy metrics, as recommended by the WHOIS RT. Research and planning are currently under way for both of these key initiatives.

The second project launched in response to the Board’s 2012 resolution directed CEO Fadi Chehadé to form an independent Expert Working Group on gTLD Directory Services. The group was charged with finding ways to break the deadlock in the ICANN community over the usefulness and fate of the WHOIS system. The EWG had straightforward objectives:

* Define the purpose of collecting and maintaining gTLD registration data and consider how to safeguard it.
* Propose a model for managing gTLD directory services that addresses accuracy and access issues, while accounting for safeguards for protecting data.
* Identifying what system might better serve the future needs of the global Internet community.

After examining a broad array of actual user cases and the many issues they raised, the EWG concluded that today’s WHOIS model—giving every user the same anonymous public access to (too often inaccurate) gTLD registration data—should be abandoned. The Group determined that WHOIS hasn’t kept pace with the real world, citing the introduction of Internationalized Domain Names and the emergence of privacy and proxy services.

The EWG recommended a paradigm shift in gTLD registration. In its Initial Report, it advised ICANN to contract with an international, third party provider to set up an aggregated registration data service (ARDS). The ARDS would gather copies of registration data from registries, validate them and manage the dissemination of the information for permissible purposes only. Only authenticated parties would be allowed access to the data, and they would be responsible for how it was used.

The EWG is in the consultation phase, and sought public input through 6 September 2013 on its draft recommendations. Itwill use comments received online, at the ICANN Durban Meeting, and through other public consultation to continue refining its recommendations.

# Technical Overview

The WHOIS protocol is a Transmission Control Protocol or TCP-based transaction-oriented query/response protocol that is widely used to provide information services to Internet users. While originally used to provide "white pages" services and information about registered domain names, its current uses offer a broad range of information services. The protocol delivers its content in a human-readable format.

## Current Technical Specification

ICANN requires ICANN accredited registrars and registries to comply with technical specifications for the WHOIS services offered by them, as described in ICANN’s contracts with registrars and registries. These specifications include service level agreements, formatting requirements, and access protocols.

You can find the technical specification of the WHOIS protocol described in detail within a document called “Request for Comment 3912.” When published in September 2004, RFC 3912 made its predecessor, RFC 954, obsolete. For historic reasons, the WHOIS protocol lacks many of the protocol design attributes, for example internationalization and strong security, that would be expected from any recently designed IETF protocol. RFC 3912 does not attempt to rectify any of those shortcomings. Work is currently underway in a separate IETF activity (WEIRDS) to identify a new technical protocol that attempts to address some of the shortcomings recognized with the current protocol. Once published by the IETF as a proposed standard, ICANN’s contracts allow for a transition to the new protocol.

## DNS and WHOIS – How it Works

The Domain Name System (DNS) is a hierarchical distributed database to lookup information from unique names, i.e. to help people connect to resources like websites and email servers on the Internet. To explain it in simple terms, every computer has a unique number called an Internet Protocol (IP) address, e.g. 2620:0:2d0:200::7, which is like a phone number. One computer can contact another as long as it knows its IP address. Because these numbers are difficult to remember, we tend to use domain names, e.g. www.icann.org, instead. DNS is used to translate between domain names and IP addresses.

WHOIS provides information sufficient to contact a responsible party for a particular Internet resource who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name or the DNS name servers. Unfortunately the term “WHOIS” is overloaded with meanings, referring to protocols, services, and data types associated various resources, i.e., domain names, IP addresses, and Autonomous System Numbers (ASNs). This WHOIS Portal is devoted to describing the WHOIS system for generic top-level domain names only, and does not attempt to describe how WHOIS applies to country code top-level domain names (ccTLDs), IP addresses or ASNs.

The service offered by registrars and registries to provide WHOIS data is referred to as a “WHOIS Service” or alternatively, a “Registration Data Directory Service.” Read More about DNS and WHOIS How it works.

### DNS and WHOIS – How it Works

WHOIS databases are mainly run by registrars and registries; for example Public Interest Registry (PIR) maintains the .ORG registry. ICANN’s IANA department runs the central registry for all kinds of Internet resources, pointing to the WHOIS server of the responsible (sub)-registry as well as the contact details of this registry.

DNS Registry operators also maintain another vital system, the authoritative name servers, which hold the key to where a website is located. For example, if you type www.icann.org into a browser, your ISP will query the name servers starting from the hard coded root servers (in this case, PIR’s servers) to find out which name servers are associated to that domain name. One of those name servers is then contacted and will return the IP address for that domain name. Your computer can now connect to the computer that will serve up the ICANN homepage. This process is illustrated below.



As can be seen in the diagram, the selection of which registry operator is to be queried each time depends on an ever increasing trailing part of the domain (e.g. .COM, .NET, .UK, CO.UK, IP6.ARPA), also known as the top-level domain (TLD). If the ISP doesn’t already know, it can determine which name server need to be asked for a given part of the domain name, beginning with asking a root server. There are various root servers located all over the world that point to the appropriate downstream name servers.

WHOIS is designed to work in the same way: Starting at WHOIS.IANA.ORG, follow the references to the downstream WHOIS servers unless the required information is obtained. This process is illustrated below for a “thick” registry. If the registry is a “thin,” an additional process query at the registrar’s database is required to obtain the WHOIS data for the domain name..



## The Domain Name Registration Process

Like IP addresses, domain names also need to be unique so there has to be a way of associating them with a particular person or organization. This is done through the domain name registration process. Learn more about the Domain Name Registration Process and how it relates to WHOIS.

### The Domain Name Registration Process

In order to reserve a domain, a registrant must register it with one of almost a thousand ICANN-accredited registrars. The registrar will check if the domain is available and create a WHOIS record with the registrant’s information. It is also possible to register domains through a registrar’s resellers.

The diagram below illustrates the main functions of the parties that are usually involved in the process.



A **registrant** is the person or organization who has registered the domain name. In order to do so, the registrant will usually apply online to a domain registrar or one of their resellers. The registrant is bound by the terms and conditions of the registrar with which it registers, for instance adhering to a certain code of conduct or indemnifying the registrar and registry against any legal or civil action taken as a result of use of the domain name. Registrants have certain responsibilities that should be incorporated into these terms and conditions like payment of registration fees and submission and timely update of accurate data.

In addition to registering the name, they also need to have their domains listed on name servers in order to have that domain reachable on the Internet. If the registrar does not offer this service or registrants opt out, then they are responsible for procuring or hosting their own name servers.

**Registrars** are organizations accredited by ICANN and certified by the registry operators to sell domains. They are bound by the Registrar Accreditation Agreement (RAA) with ICANN - and by their agreements with the registry operators. The RAA sets out responsibilities for the registrar including maintenance of WHOIS data, submission of data to domain registries, facilitating public WHOIS queries, ensuring registrants details are escrowed, and complying with RAA conditions relating to the conclusion of the registration period.

Some registrants may opt to register through a **reseller**. These are affiliated or under contract with registrars, and usually offer other services such as web hosting, email mailboxes etc. Resellers are bound by their agreements with the registrar(s) whose services they sell; they are not accredited by ICANN. However, the registrar for whom they are re-selling will still be the sponsor for the domain name registration and accountable for the domains sold by the reseller.

 While registrars are contracted to conduct the day-to-day business of selling domain name registrations, **registry operators** are responsible for maintaining the registry for each TLD. The responsibilities of the registry operator include accepting registration requests (whether from registrars or directly from registrants), maintaining a database of the necessary registration data and providing name servers to publish the zone file data (i.e. information about the location of a domain) throughout the Internet.

The Internet Corporation for Assigned Names and Numbers (ICANN) is the international non-profit corporation that oversees the assignment of both IP addresses and domain names. It has responsibility for managing root server and TLD name system management and has contractual agreements with both registries and registrars that provide the foundation for the WHOIS system.

# Using WHOIS

In addition to the WHOIS services offered by registrars and registries, ICANN is currently developing a new WHOIS service that simplifies WHOIS look-ups. ICANN’s WHOIS service will be a publicly searchable database that details domain owner contact details across all contracted gTLDs. The following topics detail how to make use of the WHOIS search service:

## Basics of WHOIS

As many consumers use search engines to find information on the Internet, they may not be aware of the term “WHOIS” to use in a search engine. Even when “WHOIS” is applied to a search engine, all sorts of responses appear. Learn more about the Starting Point for a WHOIS Query.

### Starting Point for a WHOIS Query

Most of the search engine results, particularly those at the top of the search result hierarchy, link to webpage of registrars attempting to sell domain names and related services. It is not at all intuitive how to access WHOIS in order to find the domain registrant information. In order to become proficient with WHOIS, it’s important to start in the right place. ICANN’s WHOIS service, once it is operational, may make it easier for consumers to conduct WHOIS searches.

#### Accessing WHOIS

WHOIS services are provided by registrars and registries for the domain names that they sponsor. Access to this distributed network of independent databases is provided in two ways – through a free web page and through a free Port 43 service. The web page allows real-time access to WHOIS data in individual searches; the Port 43 access allows automated queries by machine. Searches for the full WHOIS contact data for the registrant and the designated administrator and technician, as well as the registration creation and expiration dates can be performed at the registrar’s systems (either through its web page and Port 43 service) or through the systems of certain registries that are obligated to provide “thick” or full contact data. A “thin” registry provides minimal information, namely, the registrar, name servers and registration dates. All of the new gTLDs will have “thick” records. ICANN’s WHOIS service, once it is operational, will provide an additional means of accessing WHOIS, in addition to the access provided by registrars and registries.

#### Uses of WHOIS

WHOIS is used for many legitimate purposes. Under ICANN’s agreements, WHOIS may be used for any lawful purposes except to enable marketing or spam, or to enable high volume, automated processes to query a registrar or registry’s systems, except to manage domain names. In addition to identifying domain name holders, WHOIS data also allows network administrators and others to find and fix system problems and to maintain Internet stability. With it, they can determine the availability of domain names, combat spam or fraud, identify trademark infringement and enhance accountability of domain name registrants. WHOIS data is sometimes used to track down and identify registrants who may be posting illegal content or engaging in phishing scams. These are just a few examples of how WHOIS helps maintain a healthy Internet ecosystem.

#### Keeping WHOIS accurate

ICANN requires WHOIS information to be accurate throughout the registration period of a domain name. Until recently, registrars were not required to proactively verify or validate the information provided by domain name holders. Beginning in 2014, ICANN requires registrars who have signed its new 2013 Registrar Accreditation Agreement (RAA) to validate and verify certain WHOIS entries.

Domain name holders, or “registrants,” as they are referred to, need to carefully follow the instructions of their registrar or risk losing their domain names at the time of registration. A registrar may require a response to an e-mail sent to the email listed in WHOIS or a response from the phone number listed in WHOIS.

Because information can change over time, ICANN requires registrars to provide each registrant with an annual opportunity to review and correct their domain name WHOIS data. They also get a reminder that providing false data can be grounds for registration cancellation. Anyone who submits false data or fails to respond to registrar inquiries related to the accuracy of their data risks having their domain name be cancelled or suspended. Registrants need to respond quickly to inquiries from their registrar related to the accuracy of their contact data to avoid cancellation or suspension.

Conversely, Internet users who find that WHOIS data is incomplete or incorrect can file a complaint with ICANN, which will forward it to the sponsoring registrar. The registrar will investigate and correct inaccurate data in response to the complaint. Beginning in 2014, registrars under the new 2013 RAA are also required to reverify and revalidate certain WHOIS fields in response to a WHOIS inaccuracy claim.

#### Privacy Issues

Sometimes results may not show any contact information for the actual operator of a domain name and instead display information from a privacy and proxy service. Some registries and registrars offer privacy or proxy services that show only the contact information of the service, to shield registrants who don’t want their personal information to appear in the database. Their anonymity is not guaranteed since registrars may abide by any legal requirements to share the true identity of the registrant. Likewise, registries or registrars in countries where privacy laws prohibit the collection and publishing of personal data are not required to break those laws to satisfy WHOIS. Instead, they are eligible to apply to ICANN for a WHOIS waiver.

# Glossary of WHOIS Terms

Adjacency attestation (AAO)

An AAO is a digitally signed object that verifies that an AS has made an attestation that it has an inter-domain adjacency with one or more other ASes.

Advertisements

See Routing advertisement.

Advisory Committee

An Advisory Committee is a formal advisory body made up of representatives from the Internet community to advise ICANN on a particular issue or policy area. Several are mandated by the ICANN Bylaws and others may be created as needed. Advisory committees have no legal authority to act for ICANN, but report their findings and make recommendations to the ICANN Board.

AfriNIC

African Network Information Centre (AfriNIC) is the Regional Internet Registry for the African Region.

ALAC - At-Large Advisory Committee

ICANN's At-Large Advisory Committee (ALAC) is responsible for considering and providing advice on the activities of the ICANN, as they relate to the interests of individual Internet users (the "At-Large" community). ICANN, as a private sector, non-profit corporation with technical management responsibilities for the Internet's domain name and address system, will rely on the ALAC and its supporting infrastructure to involve and represent in ICANN a broad set of individual user interests.

Allocation

Address space allocated by APNIC or NIRs to LIRs for the purpose of subsequent distribution by LIRs to their customers.

APNIC

Asia Pacific Network Information Centre (APNIC) is the Regional Internet Registry for the Asia Pacific Region.

Application Service Provider

Entity who provides specific application(s) direct to the End User.

ARIN - American Registry for Internet Numbers

ARIN is a Regional Internet Registry (RIR), and is a non-profit membership organization established for the purpose of the administration and registration of Internet Protocol (IP) addresses in North America, parts of the Caribbean, and sub-Saharan Africa.

ARPA (or ".ARPA")

The Address and Routing Parameters Area top level domain, used for network infrastructure.

ASO - Address Supporting Organization

The ASO advises the ICANN Board of Directors on policy issues relating to the allocation and management of Internet Protocol (IP) addresses. The ASO selects two Directors for the ICANN Board.

Assignment

Address space assigned for specific use within the Internet infrastructure of a network. Assignments can be made by LIRs to their customer's network infrastructure or to the LIR's own infrastructure.

Assignment of a number

The process for providing an international numbering resource to an eligible applicant (when used in the formal sense as defined in Section 5.4 of ITU-T Rec. E.190 (05/97)).

Assignment window

Refers to the amount of IP address space that you can assign or sub-allocate to your customers without the need to send in a second opinion request form for APNIC's approval.

AUNIC

Australian Network Information Centre.

Autonomous System (AS)

An AS is a group of IP networks run by one or more network operators with a single clearly defined routing policy.

Autonomous System Number (ASN or AS number)

ASNs are globally unique identifiers for Autonomous Systems and are used as identifiers to allow the ASes to exchange dynamic routing information. An Autonomous system (AS) is a group of IP networks having a single clearly defined routing policy run by one or more network operators.

ccNSO - Country-Code Names Supporting Organization

A Supporting Organization responsible for developing and recommending to ICANN’s Board global policies relating to country code top-level domains. It provides a forum for country code top-level domain managers to meet and discuss issues of concern from a global perspective. ￼The ccNSO selects one person to serve on the board.

ccTLD - Country Code Top Level Domain

Two letter domains, such as .UK (United Kingdom), .DE (Germany) and .JP (Japan) (for example), are called country code top level domains (ccTLDs) and correspond to a country, territory, or other geographic location. The rules and policies for registering domain names in the ccTLDs vary significantly and ccTLD registries limit use of the ccTLD to citizens of the corresponding country.

Some ICANN-accredited registrars provide registration services in the ccTLDs in addition to registering names in .BIZ, .COM, .INFO, .NAME, .NET and .ORG, however, ICANN does not specifically accredit registrars to provide ccTLD registration services.

For more information regarding registering names in ccTLDs, including a complete database of designated ccTLDs and managers, please refer to http://www.iana.org/cctld/cctld.htm.

Domain

A set of host names consisting of a single domain name and all the domain names below it

Domain name

As part of the Domain Name System, domain names identify IP resources, such as an Internet website.

DNS - Domain Name System

The Domain Name System (DNS) helps users to find their way around the Internet. Every computer on the Internet has a unique address - just like a telephone number - which is a rather complicated string of numbers. It is called its "IP address" (IP stands for "Internet Protocol"). IP Addresses are hard to remember. The DNS makes using the Internet easier by allowing a familiar string of letters (the "domain name") to be used instead of the arcane IP address. So instead of typing 207.151.159.3, you can type www.internic.net. It is a "mnemonic" device that makes addresses easier to remember.

Domain Name Registration Data (DNRD)

Refers to the information that registrants provide when registering a domain name and that registrars or registries collect. Some of this information is made available to the public. For interactions between ICANN Accredited Generic Top-Level Domain (gTLD) registrars and registrants, the data elements are specified in the current RAA. For country code Top-Level Domains (ccTLDs), the operators of these TLDs set their own or follow their government’s policy regarding the request and display of registration information.

Domain Name Registration Data Access Protocol (DNRD-AP)

Refers to the elements of a (standard) communications exchange—queries and responses—that make access to registration data possible. For example, the WHOIS protocol (RFC 3912) and Hypertext Transfer Protocol (HTTP) (RFC 2616 and its updates) are commonly used to provide public access to DNRD.

Domain Name Registration Data Directory Service (DNRD-DS)

Refers to the service(s) offered by registries and registrars to provide access to (potentially a subset of) the DNRD.

GAC - Governmental Advisory Committee

The GAC is an advisory committee comprising appointed representatives of national governments, multi-national governmental organizations and treaty organizations, and distinct economies. Its function is to advise the ICANN Board on matters of concern to governments. The GAC will operate as a forum for the discussion of government interests and concerns, including consumer interests. As an advisory committee, the GAC has no legal authority to act for ICANN, but will report its findings and recommendations to the ICANN Board.

GNSO - Generic Names Supporting Organization

The supporting organization responsible for developing and recommending to the ICANN Board substantive policies relating to generic top-level domains. Its members include representatives from gTLD registries, gTLD registrars, intellectual property interests, Internet service providers, businesses and non-commercial interests.

gTLD - Generic Top Level Domain

Most TLDs with three or more characters are referred to as "generic" TLDs, or "gTLDs", such as com, .net, and .org.

http

Hypertext transfer protocol

IANA - Internet Assigned Numbers Authority

The authority originally responsible for the oversight of IP address allocation, the coordination of the assignment of protocol parameters provided for within Internet technical standards, and the management of the domain name system, including the delegation of top-level domains and oversight of the root name server system. Under ICANN, the IANA continues to distribute addresses to the Regional Internet Registries, coordinate with the IETF and others to assign protocol parameters, and oversee the operation of the DNS.

ICANN - The Internet Corporation for Assigned Names and Numbers

ICANN is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. Originally, the Internet Assigned Numbers Authority (IANA) and other entities performed these services under U.S. Government contract. ICANN now performs the IANA function. As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes.

IETF - Internet Engineering Task Force

The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

in-addr.arpa

In the .ARPA domain, the subdomain for IP addresses (as names) for host names

Injection

Refers to the method of inserting routing information into the routing table. In context, it can also imply the injection of false routing information

Inspection and alteration

Where false routing advertisements cause traffic to an intended destination to be forwarded to a compromised network segment. Here the traffic may be inspected, or even altered before being passed onward to the actual destination

IDNs - Internationalized Domain Names

IDNs are domain names that include characters used in the local representation of languages that are not written with the twenty-six letters of the basic Latin alphabet "a-z". An IDN can contain Latin letters with diacritical marks, as required by many European languages, or may consist of characters from non-Latin scripts such as Arabic or Chinese. Many languages also use other types of digits than the European "0-9". The basic Latin alphabet, together with the European-Arabic digits, is for the purpose of domain names, termed "ASCII characters" (ASCII = American Standard Code for Information Interchange). These are also included in the broader range of "Unicode characters" that provides the basis for IDNs.

The "hostname rule" requires that all domain names of the type under consideration here are stored in the DNS using only the ASCII characters listed above, with the one further addition of the hyphen "-". The Unicode form of an IDN therefore requires special encoding before it is entered into the DNS.

The following terminology is used when distinguishing between these forms:

A domain name consists of a series of "labels" (separated by "dots"). The ASCII form of an IDN label is termed an "A-label". All operations defined in the DNS protocol use A-labels exclusively. The Unicode form, which a user expects to be displayed, is termed a "U-label". The difference may be illustrated with the Hindi word for "test" -- -- appearing here as a U-label would (in the Devanagari script). A special form of "ASCII compatible encoding" (abbreviated ACE) is applied to this to produce the corresponding A-label: xn-- 11b5bs1di.

A domain name that only includes ASCII letters, digits, and hyphens is termed an "LDH label". Although the definitions of A-labels and LDH-labels overlap, a name consisting exclusively of LDH labels, such as"icann.org" is not an IDN.

Internet Exchange Point

Also known as IX or IXP. It is a layer 1 and layer 2 network structure that interconnects three or more Autonomous Systems 9AS) for the purpose of Internet traffic interchange

Internet Exchange Point (IX or IXP)

An Internet Exchange Point is a layer 1 and layer 2 network structure that interconnects three or more Autonomous Systems (AS) for the purpose of Internet traffic interchange.

Internet Registry

An Internet Registry (IR) is an organization that is responsible for distributing IP address space to its members or customers and for registering those distributions. IRs include: (i) APNIC and other Regional Internet Registries (RIRs); (ii) National Internet Registries (NIRs); (iii) Local Internet Registries (LIRs)

Internet resources

APNIC's refers to IPv4 and IPv6 address blocks and AS numbers as numeric Internet resources.

IP - Internet Protocol

The communications protocol underlying the Internet, IP allows large, geographically diverse networks of computers to communicate with each other quickly and economically over a variety of physical links. An Internet Protocol Address is the numerical address by which a location in the Internet is identified. Computers on the Internet use IP addresses to route traffic and establish connections among themselves; people generally use the human- friendly names made possible by the Domain Name System.

IPv4 address

An IPv4 address is a binary number consisting of 32 bits that are organized into four bytes. The four bytes are usually portrayed using a dotted decimal notation such as 1.2.3.4. Each decimal number is equivalent of a byte; the dots used between the decimals are used to separate the bytes. For example, 205.150.58.7

IPv4-Mapped

These addresses are used to embed IPv4 addresses in an IPv6 address. One use for this is in a dual stack transition scenario where IPv4 addresses can be mapped into an IPV6 address.

IPv6

The next generation Internet layer protocol for the Internet. It has a much larger address space than IPv4 with a 128-bit address. This supports 2 128 addresses. They are conventionally expressed using hexadecimal strings, for example, 2001:0db8:582:ae33::29.

ISOC

Internet Society

ISP - Internet Service Provider

An ISP is a company, which provides access to the Internet to organizations and/or individuals. Access services provided by ISPs may include web hosting, email, VoIP (voice over IP), and support for many other applications.

ITU

International Telecommunication Union

ITU-T

The Telecommunications standardization sector of the International Telecommunication Union

LACNIC

Latin American & Caribbean Network Information Centre (LACNIC) is the Regional Internet Registry for Latin America and some Caribbean Islands.

LAN

Local Area Network

Link-Local Addresses

These addresses are used on a single link or a non-routed common access network, such as an Ethernet LAN. They do not need to be unique outside of that link. Link-local addresses may appear as the source or destination of an IPv6.

Local Internet Registry (LIR)

A LIR is an Internet Registry (IR) that primarily assigns address space to the users of the network services that it provides. LIRs are generally ISPs, whose customers are primarily end users and possibly other ISPs.

Loopback

This address is used when a host talks to itself over IPv6. This often happens when one program sends data to another.

MoU

Memorandum of Understanding

Multicast

These addresses are used to identify multicast groups. They should only be used as destination addresses, never as source addresses.

Multihomed

Describes a computer host that has multiple IP addresses to connected networks. A multihomed host is physically connected to multiple data links that can be on the same or different networks.

Name Server

A DNS component that stores information about one zone (or more) of the DNS name space.

Name Space

The structure of the DNS database.

Name vs Address vs Route

A name identifies an endpoint, an address tells where it is, and a route tells how to get there.

NAPTR

Number Authority Pointer (as used within IETF RFC 2916 to identify possible URLs and numbers that can be returned).

NAT

Network Address Translation (NAT) is the process of modifying a network address while in transit for the purpose of remapping a given address space into another.

National Internet Registry (NIR)

A NIR primarily allocates address space to its members or constituents which are generally LIRs organized at a national level. NIRs mostly exist in the Asia Pacific region.

Network

An international network providing public correspondence services (when used in the formal sense as defined in Section 4.17 of ITU-T Rec. E.164 (05/97).

Nibble boundary

A bit is the smallest unit of data on a binary computer. A nibble is a collection of bits on a four-bit boundary (half-byte), that is, it takes four bits to represent a single binary code decimal (BCD) or hexadecimal digit (0-9, A, B, C, D, E, F in ASCII). When IPv6 addresses are represented in the DNS, the entire binary sequence is listed as hexidecimal characters. When listed in reverse, each hexadecimal character becomes a "nibble boundary".

Non-portable

Non-portable addresses must be returned if the network changes upstream provider.

NP

Number Portability

NRO

Number Resource Organization

Orchid

These IPv6 addresses are used for a fixed-term experiment. They should only be visible on an end-to-end basis and routers should not see packets using them as source or destination addresses.

Ownership vs. use of a number

Numbering resources ... are not to be considered "owned" by the assignee. Assignment of the numbering resource ... confers use of the resources ... (in the formal sense of Principle 5 in ITU-T Rec. E.190.)

PDP - Policy Development Process

A set of formal steps, as defined in the ICANN bylaws, to guide the initiation, internal and external review, timing and approval of policies needed to coordinate the global Internet’s system of unique identifiers.

Phishing

Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social engineering schemes use spoofed emails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers.

Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using Trojan keylogger spyware. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.

PKI

Public Key Infrastructure is a combination of technologies that allow the verification and secure exchange of data through the use of encryption, digitally signed certificates, and public and private keys.

Portable

Portable addresses can be retained by the network if the network changes upstream provider.

Portable allocation

APNIC makes portable allocations to organizations. That is, it distributes address space to IRs for the purpose of subsequent distribution by them.

PSTN

Public Switched Telephone Network

QoS

Quality of Service

Query/Response

A protocol interaction between a client and a server.

Registrar

Domain names can be registered through many different companies (known as "registrars") that compete with one another. A listing of these companies appears in the Accredited Registrar Directory.

The registrar you choose will ask you to provide various contact and technical information that makes up the registration. The registrar will then keep records of the contact information and submit the technical information to a central directory known as the "registry." This registry provides other computers on the Internet the information necessary to send you e-mail or to find your web site. You will also be required to enter a registration contract with the registrar, which sets forth the terms under which your registration is accepted and will be maintained.

Registry

The "Registry" is the authoritative, master database of all domain names registered in each Top Level Domain. The registry operator keeps the master database and also generates the "zone file" which allows computers to route Internet traffic to and from top-level domains anywhere in the world. Internet users don't interact directly with the registry operator; users can register names in TLDs including .BIZ, .COM, .INFO, .NET, .NAME, .ORG by using an ICANN-Accredited Registrar.

Resolver

The client-based software that queries a DNS name server and receives the response

Reverse DNS delegation

Reverse DNS delegations allow applications to map to a domain name from an IP address. Reverse delegation is achieved by use of the pseudo-domain names in-addr.arpa (IPv4) and ip6.arpa (IPv6).

RFC

Request For Comments - the name for an Internet standards-related specification.

RIPE and RIPE NCC - Réseaux IP Européens

Réseaux IP Européens Network Co-ordination Centre (RIPE NCC) is the Regional Internet Registry for Europe, the Middle East and parts of Central Asia. RIPE is an open and voluntary organization, which consists of European Internet service providers. The RIPE NCC acts as the Regional Internet Registry (RIR) for Europe and surrounding areas, performs coordination activities for the organizations participating in RIPE, and allocates blocks of IP address space to its Local Internet Registries (LIRs), which then assign the addresses to end-users.

RIR

Regional Internet Registries (RIRs) are established and authorized by respective regional communities and recognized by the IANA to serve and represent large geographical regions. The primary role of RIRs is to manage and distribute public Internet address space within their respective regions.

Root

The root level is the top level of the Domain Name System, a hierarchical tree-like structure that maps domain names to IP addresses. Top level domains include .COM, .ORG, and country-level names such as .CA and .AU.

Root Servers

The root servers contain the IP addresses of all the TLD registries - both the global registries such as .com, .org, etc. and the 244 country-specific registries such as .FR (France), .CN (China), etc. This is critical information. If the information is not 100 percent correct or if it is ambiguous, it might not be possible to locate a key registry on the Internet. In DNS parlance, the information must be unique and authentic.

Route Origin Attestation (ROA)

A ROA is a digitally signed object that provides a means of verifying that an IP address block holder has authorized an Autonomous System (AS) to originate routes to one or more prefixes within the address block.

Routing advertisements

Each router announces or advertises a list of routes it can process, expressed as ranges of IP addresses for which it can provide routing service. Put simply, a router tells its peers, "If you have traffic intended for IP addresses in the range between 192.0.0.1 and 192.5.255.255 (for example), pass me those packets.”

RPKI

Resource Public Key Infrastructure (see also PKI) is a structure of digitally signed certificates which contain attestations regarding the right to use numeric Internet resources.

RRs

DNS Resource Records

Second opinion request

The process that is used to seek APNIC's approval of assignments or sub-allocation that exceed your assignment window.

Service Registrar (for ENUM)

Entity which provides direct services to ENUM registrants and hosts NAPTR records that contain (service-specific) URIs.

SG2

ITU-T Study Group 2

SIP

Session Initiation Protocol

SMTP

Simple Mail Transfer Protocol

SO - Supporting Organizations

The SOs are the three specialized advisory bodies that advise the ICANN Board of Directors on issues relating to domain names (GNSO and CCNSO) and, IP addresses (ASO).

SSAC - Security and Stability Advisory Committee

An advisory committee to the ICANN Board comprised of technical experts from industry and academia as well as operators of Internet root servers, registrars and TLD registries.

Sub-allocation

IP addresses are sub-allocated when they are distributed to an organization that will further assign them to their own end users.

Subnet mask

The routing prefix of a designated IP address.

Teredo

This is a mapped address allowing IPv6 tunneling through IPv4 NATs. The address is formed using the Teredo prefix, the server's unique IPv4 address, flags describing the type of NAT, the obfuscated client port and the client IPv4 address, which is probably a private address. It is possible to reverse the process and identify the IPv4 address of the relay server, which can then be booked up in the relevant RIR's WHOIS database. You can do this on the following webpage: http://www.potaroo.net/cgi-bin/ipv6addr

Time to Live (TTL)

One of the fields in the DNS records is the TTL (Time-To-Live) field. This is the number of milliseconds corresponding to the amount of time that the Recursive Resolver should keep the answer in its memory.

TN

Telephone Number

TLD - Top-level Domain

TLDs are the names at the top of the DNS naming hierarchy. They appear in domain names as the string of letters following the last (rightmost) ".", such as "net" in "www.example.net". The administrator for a TLD controls what second-level names are recognized in that TLD. The administrators of the "root domain" or "root zone" control what TLDs are recognized by the DNS. Commonly used TLDs include .com, .net, .edu, .jp, .de, etc.

Top-Level Domain (TLD) Server

A Top-Level Domain (TLD) Server is known to the root servers. It is authoritative for TLDs (for example .com, .org, .net).

TTM

Test Traffic Measurement- comprehensively measures key parameters regarding the connectivity of the host's site to other parts of the Internet.

UDP Port

The Recursive Resolver is expecting the answer packet on the same UDP port from where the query was sent.

UDRP - Uniform Dispute Resolution Policy

￼All ICANN-accredited registrars follow a uniform dispute resolution policy. Under that policy, disputes over entitlement to a domain-name registration are ordinarily resolved by court litigation between the parties claiming rights to the registration. Once the courts rule who is entitled to the registration, the registrar will implement that ruling. In disputes arising from registrations allegedly made abusively (such as "cybersquatting" and cyberpiracy"), the uniform policy provides an expedited administrative procedure to allow the dispute to be resolved without the cost and delays often encountered in court litigation. In these cases, you can invoke the administrative procedure by filing a complaint with one of the dispute- resolution service providers.

For more details on the UDRP, see the ICANN UDRP page and the FAQs.

Unique Local Addresses (ULAs)

These addresses are reserved for local use in home and enterprise environments and are not public address space. These addresses might not be unique and there is no formal address registration. Packets with these addresses in the source or destination fields are not intended to be routed on the public Internet but are intended to be routed within the enterprise or organization.

URI

Uniform Resource Identifier - a URL is a URI

URL

Uniform Resource Locator

VLSM

A Variable Length Subnet Mask (VLSM) is a method of allocating IP addresses and other Internet number resources to subnets, according to their individual needs. This serves as an alternative to using a general, network-wide rule.

VoIP

Voice over IP

WG

Working Group

WHOIS

WHOIS protocol (pronounced "who is"; not an acronym) An Internet protocol that is used to query databases to obtain information about the registration of a domain name (or IP address). The WHOIS protocol was originally specified in RFC 954, published in 1985. The current specification is documented in RFC 3912. ICANN's gTLD agreements require registries and registrars to offer an interactive web page and a port 43 WHOIS service providing free public access to data on registered names. Such data is commonly referred to as "WHOIS data," and includes elements such as the domain registration creation and expiration dates, nameservers, and contact information for the registrant and designated administrative and technical contacts.

WHOIS services are typically used to identify domain holders for business purposes and to identify parties who are able to correct technical problems associated with the registered domain.

WP1/2

Working Party 1 of SG 2

Zone

In DNS, a contiguous portion of a domain consisting of names or delegations. Formally, a domain name belongs to exactly one (authoritative) zone.

zone (or "zone")

A segment of an ENUM domain name (used in the Berlin Liaison Statement (now RFC 3026) solely for convenience).