OONI Glossary

This document summarizes key terms used in OONI documentation, applications, reports and presentations which might be difficult to translate or interpret. Please use this glossary if you are an interpreter and you need to prepare for the translation of an OONI workshop. The full list of terms (with longer explanations) can be found here: https://ooni.org/support/glossary/

ASN

An Autonomous System Number (ASN) is a unique identifier of an autonomous system (AS) responsible for delivering IP packets to a set of IP addresses that it manages. This number allows the respective autonomous system to exchange routing information with other systems.

Blocklist

A blocklist is a list of internet resources (such as websites and IP addresses) which are blocked from user access. Some governments occasionally publish official blocklists (or they get leaked) which contain lists of websites that are legally prohibited in a country.

Block page

A block page (or “Access Denied Page”) is a web page that is displayed when a user attempts to access a website they are not permitted to view.

Circumvention tools

Circumvention tools are technologies that enable their users to bypass internet censorship, such as the blocking of websites and social media apps. VPNs and proxies are common circumvention tools, while Tor also provides its users with online privacy and anonymity (in addition to censorship circumvention).

Client

In the world of computers, a client is a piece of software or hardware that interacts with a service hosted by a server.

Data processing pipeline

A data processing pipeline is a software system designed to process data.

DNS

DNS stands for “Domain Name System” and it maps domain names to IP addresses. A domain is a name that is commonly attributed to websites (when they’re created), so that they can be more easily accessed and remembered. For example, `twitter.com` is the domain of the Twitter website.

DNS query

A DNS query (otherwise known as a “DNS request”) is a request for information sent from a user’s computer to a DNS server. In most cases, a DNS request is sent to ask for the IP address associated with a domain name (such as `ooni.org`).

DNS resolver

A DNS resolver is a server which maps domain names to IP addresses, operating like an “address book”. Internet Service Providers (ISPs), amongst other service providers (such as Google), run DNS resolvers that can be queried to receive the IP address of a given website.

DNS tampering

DNS tampering is an umbrella term used to describe various forms of DNS interference, including DNS hijacking and DNS spoofing.

DNS tampering can happen in various ways, including:

- DNS hijacking: Where the DNS resolver ‘lies’ and returns the wrong IP address.
- DNS spoofing: Where your DNS request is intercepted and you receive the wrong IP address.

Domain name and URL structure

A domain is a name that is commonly attributed to websites (when they’re created), so that they can be more easily accessed and remembered.

For example, **facebook.com** is the domain of the Twitter website. A **subdomain** is an optional part of an internet domain name that appears before the root domain. For example, 'www' is a common subdomain, **www**.facebook.com. A **subfolder** is a page contained within the domain, for example, in www.facebook.com/**profile**, ‘profile’ is a subfolder.

A **URL** is the address of a World Wide Web page. URL always include a protocol (HTTP or HTTPS) and domain name, sometimes it also includes subdomain. For example, `https://twitter.com/` is a URL, while twitter.com is a domain.

DPI

Deep packet inspection (DPI) is a method of examining and managing network traffic. This technology is used for a detailed inspection of data being sent over a computer network.

HTTP

The Hypertext Transfer Protocol (HTTP) is the underlying protocol used by the World Wide Web to transfer or exchange data across the internet. The HTTP protocol allows communication between a client and a server.

HTTPS

The Hypertext Transfer Protocol Secure (HTTPS) – also known as HTTP over TLS, or HTTP over SSL – is the HTTP protocol over an encrypted channel.

HTTP transparent proxy

An HTTP transparent proxy is a type of middlebox, an intermediary system that sits between a client and a server and performs actions over the HTTP protocol.

IP address

An Internet Protocol (IP) address is a unique numerical address that identifies a device or service on the internet.

ISP

An Internet Service Provider (ISP) is an organization that provides services for accessing and using the internet.

Metadata

Metadata is often described as “data about data” and is used to provide context and description of the data.

Middlebox

A middlebox is a computer networking device that transforms, inspects, filters, or otherwise manipulates traffic for purposes other than packet forwarding.

Mirror website

A mirror website is a replica of another website. Such websites have different URLs, but identical or near-identical content.

Performance

Network performance is a measure to define the quality of a network connection. This can be measured in several ways (e.g. speed, bandwidth, latency, error rate).

Protocol

Protocols are a set of rules or procedures for transmitting data between electronic devices (such as computers) on the internet. These rules determine how information will be structured and how it will be sent and received over the internet.

Proxy

A proxy is a server that acts as an intermediary service through which you can channel some or all of your internet communication. Proxies can therefore be used to bypass internet censorship.

Server

A server is a computer that remains on and connected to the internet in order to provide internet services to other computers.

TCP

The Transmission Control Protocol (TCP) is one of the main protocols on the internet. To connect to a website, your computer needs to establish a TCP connection to the address of that website. TCP works on top of the Internet Protocol (IP), which defines how to address computers on the internet.

TLS

Transport Layer Security (TLS) – also referred to as “SSL” – is a cryptographic protocol that allows you to maintain a secure, encrypted connection between your computer and an internet service.

Traffic manipulation

Traffic manipulation (a form of network interference) describes adversarial access to a network connection with capabilities to modify the data stream.

Vantage point

A network vantage point is a unique network location from which internet measurements are performed. In the context of OONI Probe, we consider a vantage point to be a unique network and country pair, such as the vantage point of “Vodafone in Italy”.

VPN

A Virtual Private Network (VPN) is software that creates an encrypted connection (commonly called “tunnel”) from your device to a server (run by a VPN provider).