GNUnet

GNUnet is a [software framework](#) for [decentralized](#), peer-to-peer [networking](#) and an official [GNU](#) package. The framework offers [link encryption](#), [peer discovery](#), [resource allocation](#), communication over many transports (such as [TCP](#), [UDP](#), [HTTP](#), [HTTPS](#), [WLAN](#) and [Bluetooth](#)) and various basic [peer-to-peer](#) algorithms for [routing](#), [multicast](#) and network size estimation.[5][6]

Christian Grothoff, maintainer of GNUnet, in [Berlin](#) on August 1, 2013, at the "[#youbroketheinternet. We'll make ourselves a GNU one. (http://youbroketheinternet.org/#august2013)](#)" event.

GNUnet's basic network topology is that of a [mesh network](#). GNUnet includes a [distributed hash table](#) (DHT) which is a [randomized](#) variant of [Kademlia](#) that can still efficiently route in [small-world networks](#). GNUnet offers a "[F2F topology](#)" option for restricting connections to only the users' trusted friends. The users' friends' own friends (and so on) can then indirectly exchange files with the users' computer, never using its IP address directly.

GNUnet uses [Uniform resource identifiers](#) (not approved by [IANA](#), although an application has been made). GNUnet URIs consist of two major parts: the module and the module specific identifier. A GNUnet URI is of form `gnunet://module/identifier` where *module* is the module name and *identifier* is a module specific string.

The primary codebase is written in [C](#), but there are [bindings](#) in other languages to produce an API for developing extensions in those languages. GNUnet is part of the [GNU Project](#). It has gained interest in the [hacker community](#) after the [PRISM](#) revelations.[7]

GNUnet consists of several subsystems, of which essential ones are Transport and Core subsystems.[8] Transport subsystem provides insecure link-layer communications, while Core provides peer discovery and encryption.[9] On top of the core subsystem various applications are built.

GNUnet includes various P2P applications in the main distribution of the framework, including filesharing, chat and VPN; additionally, a few external projects (such as secushare) are also extending the GNUnet infrastructure.

GNUnet is unrelated to the older Gnutella P2P protocol. Gnutella is not an official GNU project, while GNUnet is.[10]

Transport

Originally, GNUnet used UDP for underlying transport.[11] The GNUnet transport subsystem were expanded to included additional options, such as TCP and SMTP.[12] Support for the latter was later dropped due to a lack of maintenance.[13]

The communication port, officially registered at IANA, is 2086 (tcp + udp).[14]

Trust system

GNUnet provides trust system based on an excess-based economic model.[15] The idea of employing an economic system is taken from the MojoNation network.[16]

GNUnet network has no trusted entities so it is impossible to maintain a global *reputation*. Instead, each peer maintains its own *trust* for each of its local links.

When resources, such as bandwidth and CPU time, are in excess, the peer provides them to all requesting neighbors without reducing trust or otherwise charging them. When a node is under

GNUnet	
GNUnet with the GTK+ user interface	
Developer	GNUnet e.V.[1]
Initial release	November 5, 2001
Stable release	0.24.1 (April 11, 2025[2]) [±] (https://en.wikipedia.org/w/index.php?title=Template:Latest_stable_software_release/GNUnet&action=edit)
Repository	git.gnunet.org/gnunet.git/ (https://git.gnunet.org/gnunet.git/)
Written in	C[3]
Operating system	official: Free software operating systems (Linux, FreeBSD, NetBSD, OpenBSD);

stress, it denies requests of those neighbors that it trusts less and charges others by reducing their trust.

File sharing

The primary application at this point is [anonymous](), [censorship]()-resistant file-sharing, allowing users to anonymously publish or retrieve information of all kinds. The GNUnet protocol which provides anonymity is called GAP (GNUnet anonymity protocol).[17] GNUnet FS can additionally make use of GNU libextractor to automatically annotate shared files with metadata.

	unofficial: Other operating systems (OS X, Windows)
Available in	Spanish, English, Russian, German, French
Type	Anonymous P2P, Friend-to-friend
License	2018: AGPL-3.0-or-later[a][4] 2007: GPL-3.0-or-later[b] 2001: GPL-2.0-or-later[c]
Website	gnunet.org (https://gnunet.org)

File encoding

Files shared with GNUnet are ECRS (Encoding for Censorship-Resistant Sharing) coded.[18]

All content is represented as GBlocks. Each GBlock contains 1024 bytes. There are several types of GBlocks, each of them serves a particular purpose. Any GBlock B is uniquely identified by its RIPEMD-160 hash $H(B)$.

DBlocks store actual file contents and nothing else. File is split at 1024 byte boundaries and resulting chunks are stored in DBlocks. DBlocks are linked together into Merkle tree by means of IBlocks that store DBlock identifiers.

Blocks are encrypted with a symmetric key derived from $H(B)$ when they are stored in the network.

Queries and replies

GNUnet Anonymity Protocol consists of queries and replies. Depending on load of the forwarding node, messages are forwarded to zero or more nodes.

Queries are used to search for content and request data blocks.

Query contains resource identifier, reply address, priority and TTL (Time-to-Live).

Resource identifier of datum Q is a triple-hash $H(H(H(Q)))$.[19] Peer that replies to query provides $H(H(Q))$ to prove that it indeed has the requested resource without providing $H(Q)$ to intermediate nodes, so intermediate nodes can't decrypt Q.

Reply address is the major difference compared to Freenet protocol. While in Freenet reply always propagates back using the same path as the query, in GNUnet the path may be shorter. Peer receiving a query may drop it, *forward* it without rewriting reply address or *indirect* it by replacing reply address with its own address. By indirecting queries peer provides cover traffic for its own queries, while by forwarding them peer avoids being a link in reply propagation and preserves its bandwidth. This feature allows the user to trade anonymity for efficiency. User can specify an anonymity level for each publish, search and download operation. An anonymity level of *zero* can be used to select non-anonymous file-sharing. GNUnet's DHT infrastructure is only used if non-anonymous file-sharing is specified. The anonymity level determines how much cover traffic a peer must have to hide the user's own actions.

Priority specifies how much of its trust user wants to spend in case of a resource shortage.

TTL is used to prevent queries from staying in the network for too long.

File sharing URIs

The *fs* module *identifier* consists of either *chk*, *sks*, *ksk* or *loc* followed by a slash and a category specific value. Most URIs contain hashes, which are encoded in base32hex.[20]

- *chk* identifies files, typically: `gnunet://fs/chk/[file hash].[query hash].[file size in bytes]`
  File hash is the hash of the plaintext file, which allows decrypting it once it is downloaded. Query hash is the hash of topmost GBlock which allows downloading the whole tree of GBlocks that contain encrypted file. File size is required to determine the shape of the tree.
- *sks* identifies files within namespaces, typically:
  `gnunet://fs/sks/NAMESPACE/IDENTIFIER`
- *ksk* identifies search queries, typically: `gnunet://fs/ksk/KEYWORD[+KEYWORD]*`
- *loc* identifies a datum on a specific machine, typically:
  `gnunet://fs/loc/PEER/QUERY.TYPE.KEY.SIZE`

Examples

A type of GNUnet filesharing URI pointing to a specific copy of GNU GPL license text:

```
gnunet://fs/chk/9E4MDN4VULE8KJG6U1C8FKH5HA8C5CHSJTILRTTPGK8MJ6VHORERHE68J
U8Q0FDTOH1DGLUJ3NLE99N0ML0N9PIBAGKG7MNPBTT6UKG.1I823C58O3LKS24LLI9KB384LH
82LGF9GUQRJHACCUINSCQH36SI4NF88CMAET3T3BHI93D4S0M5CC6MVDL1K8GFKVBN69Q6T30
7U6O.17992
```

Another type of GNUnet filesharing URI, pointing to the search results of a search with keyword "gpl":

```
gnunet://fs/ksk/gpl
```

GNU Name System

GNUnet includes an implementation of the GNU Name System (GNS), a decentralized and censorship-resistant replacement for DNS. In GNS, each user manages their own zones and can delegate subdomains to zones managed by other users. Lookups of records defined by other users are performed using GNUnet's DHT.[21] GNS has been standardized in RFC 9498 (https://www.rfc-editor.org/rfc/rfc9498) . The GANA registry manages the ".alt" top-level domain in GNS.[22]

Protocol translation

GNUnet can tunnel IP traffic over the peer-to-peer network. If necessary, GNUnet can perform IPv4-IPv6 protocol translation in the process. GNUnet provides a DNS Application-level gateway to proxy DNS requests and map addresses to the desired address family as necessary. This way, GNUnet offers a possible technology to facilitate IPv6 transition. Furthermore, in combination with GNS, GNUnet's protocol translation system can be used to access hidden services — IP-based services that run locally at some peer in the network and which can only be accessed by resolving a GNS name.

Social API

Gabor X Toth published in early September 2013 a thesis[23] to present the design of a social messaging service for the GNUnet peer-to-peer framework that offers scalability, extensibility, and end-to-end encrypted communication. The scalability property is achieved through multicast message delivery, while extensibility is made possible by using PSYC (Protocol for SYnchronous Conferencing), which provides an extensible RPC (Remote Procedure Call) syntax that can evolve over time without having to upgrade the software on all nodes in the network. Another key feature

provided by the PSYC layer are stateful multicast channels, which are used to store e.g. user profiles. End-to-end encrypted communication is provided by the mesh service of GNUnet, upon which the multicast channels are built. Pseudonymous users and social places in the system have cryptographical identities — identified by their public key — these are mapped to human memorable names using GNS (GNU Name System), where each pseudonym has a zone pointing to its places.

That is the required building block for turning the GNUnet framework into a fully peer-to-peer social networking platform.
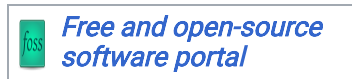
Chat

A chat has been implemented in the CADET module,[24] for which a GTK interface for GNOME exists,[25] specifically designed for the emerging Linux phones (such as the Librem 5 or the PinePhone).[26]

See also

- InterPlanetary File System
- Comparison of file-sharing applications
- Synchronous conferencing

| foss Free and open-source software portal |

Notes

a. AGPL-3.0-or-later since 2018-06-05.

b. GPL-3.0-or-later from 2007-07-02 until 2018-06-05.

c. GPL-2.0-or-later from 2001 until 2007-07-02.

References

1. GNUnet.org – About GNUnet e.V. (https://gnunet.org/en/ev.html)

2. Schanzenbach, Martin (2025-04-11). "GNUnet 0.24.1" (https://lists.gnu.org/archive/html/gnunet-developers/2025-04/msg00000.html) . gnunet.org. Retrieved 2025-05-08.

3. GNUnet Source Code (https://git.gnunet.org/gnunet.git/tree)

4. "license notice placed at the top in one of the source files of the project's repository, probably in each of its source files" (https://gnunet.org/git/gnunet.git/tree/src/core/core.h?id=4e2504a96 7ba09643c6dd7e3b9ce400e30adcb3d) . Retrieved June 8, 2018. "GNUnet is free software: you can redistribute it and/or modify it under the terms of the GNU Affero General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version."

5. EvansPolotGrothoff 2012.

6. Grothoff, Christian (2017-10-10). *The GNUnet System* (https://hal.inria.fr/tel-01654244) (habilitation thesis). Université de Rennes 1.

7. Grothoff 2013.

8. FerreiraGrothoffRuth 2003, Figure 1.

9. FerreiraGrothoffRuth 2003, II. GNUNET AND THE TRANSPORT LAYER: "The core is responsible for link-to-link encryption, binding of node identities to routable addresses, and peer discovery."

10. "GNU Software" (https://www.gnu.org/software/) . *Software - GNU Project - Free Software Foundation*. Free Software Foundation, Inc. Retrieved 25 January 2020.

11. GrothoffPatrascuBennettStef 2002, 3.1.1 UDP.

12. FerreiraGrothoffRuth 2003.

13. "About GNUnet — GNUnet documentation" (https://docs.gnunet.org/latest/about.html) . *docs.gnunet.org*. Retrieved 2025-08-13.

14. Service Name and Transport Protocol Port Number Registry, p. 38 (https://www.iana.org/assig nments/service-names-port-numbers/service-names-port-numbers.xhtml?&page=38)

15. Grothoff 2003.

16. GrothoffPatrascuBennettStef 2002, 2.4 Mojo Nation.

17. BennettGrothoff 2003.

18. BennettGrothoffHorozovPatrascu 2002.

19. GrothoffPatrascuBennettStef 2002, 5.5 More on queries.

20. Grothoff, Christian. "File-Sharing URIs" (https://web.archive.org/web/20160817025026/https:// www.gnunet.org/fs-urisyntax) . *www.gnunet.org*. Archived from the original (https://www.gnu net.org/fs-urisyntax) on 17 August 2016. Retrieved 15 July 2016.

21. Wachs, Schanzenbach & Grothoff 2014.

22. "RFC 9498: The GNU Name System [LWN.net]" (https://lwn.net/Articles/952122/) . *lwn.net*.

23. Toth, Gabor X (2013-09-05), Design of a Social Messaging System Using Stateful Multicast (https://gnunet.org/design-social-messaging-system) Archived (https://web.archive.org/web/20140222032558/https://gnunet.org/design-social-messaging-system) 2014-02-22 at the Wayback Machine - Retrieved 2013-09-28

24. GNUnet.org documentation (2019-11-14) Chatting with a (simple) client (https://gnunet.org/en/use.html#groupchat) - Retrieved 2019-11-14

25. cadet-gtk (https://gitlab.com/TheJackiMonster/cadet-gtk) on GitLab

26. GNUnet CADET for mobile Linux – Reddit (https://www.reddit.com/r/Purism/comments/g22al7/gnunet_cadet_for_mobile_linux/)

Further references

- Grothoff, Christian; Patrascu, Ioana; Bennett, Krista; Stef, Tiberiu; Horozov, Tzvetan (2002-06-13). *The GNet whitepaper* (https://git.gnunet.org/bibliography.git/plain/docs/main.pdf) (PDF) (Technical report). Purdue University.

- Bennett, Krista; Grothoff, Christian; Horozov, Tzvetan; Patrascu, Ioana (2002-07-03). Batten, Lynn; Seberry, Jennifer (eds.). *Efficient Sharing of Encrypted Data*. Lecture Notes in Computer Science. Springer Berlin Heidelberg. pp. 107–120. CiteSeerX 10.1.1.19.9837 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.19.9837) . doi:10.1007/3-540-45450-0_8 (https://doi.org/10.1007%2F3-540-45450-0_8) . ISBN 9783540438618.

- Ferreira, Ronaldo; Grothoff, Christian; Ruth, Paul (2003-05-01). "A transport layer abstraction for peer-to-peer networks" (https://grothoff.org/christian/transport.pdf) (PDF). *CCGrid 2003. 3rd IEEE/ACM International Symposium on Cluster Computing and the Grid, 2003. Proceedings*. IEEE. pp. 398–405. CiteSeerX 10.1.1.13.5086 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.13.5086) . doi:10.1109/CCGRID.2003.1199393 (https://doi.org/10.1109%2FCCGRID.2003.1199393) . ISBN 978-0-7695-1919-7. S2CID 1928711 (https://api.semanticscholar.org/CorpusID:1928711) .

- Grothoff, Dipl-Math Christian (2003-06-01). "Resource allocation in peer-to-peer networks". *Wirtschaftsinformatik*. **45** (3): 285–292. doi:10.1007/BF03254946 (https://doi.org/10.1007%2FBF03254946) . ISSN 0937-6429 (https://search.worldcat.org/issn/0937-6429) . S2CID 4479637 (https://api.semanticscholar.org/CorpusID:4479637) .

- Wachs, Matthias; Schanzenbach, Martin; Grothoff, Christian (2014). "A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System" (https://git.gnunet.org/bibliography.git/

plain/docs/gns2014wachs.pdf) (PDF). *Cryptology and Network Security*. Lecture Notes in Computer Science. Vol. 8813. pp. 127–142. doi:10.1007/978-3-319-12280-9_9 (https://doi.org/10.1007%2F978-3-319-12280-9_9) . ISBN 978-3-319-12279-3.

- Bennett, Krista; Grothoff, Christian (2003-03-26). "Gap – Practical Anonymous Networking". In Dingledine, Roger (ed.). *Privacy Enhancing Technologies*. Lecture Notes in Computer Science. Vol. 2760. Springer Berlin Heidelberg. pp. 141–160. CiteSeerX 10.1.1.125.9673 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.125.9673) . doi:10.1007/978-3-540-40956-4_10 (https://doi.org/10.1007%2F978-3-540-40956-4_10) . ISBN 9783540206101.

- Evans, Nathan; Polot, Bartlomiej; Grothoff, Christian (2012-05-21). "Efficient and Secure Decentralized Network Size Estimation". In Bestak, Robert; Kencl, Lukas; Li, Li Erran; Widmer, Joerg; Yin, Hao (eds.). *Networking 2012*. Lecture Notes in Computer Science. Vol. 7289. Springer Berlin Heidelberg. pp. 304–317. doi:10.1007/978-3-642-30045-5_23 (https://doi.org/10.1007%2F978-3-642-30045-5_23) . ISBN 9783642300448.

- Grothoff, Christian (2013-08-01). "Video: You broke the Internet. We're making ourselves a GNU one" (https://git.gnunet.org/gnunet-videos-2013.git/plain/you%20broke%20the%20internet/internetistschuld.webm) . *gnunet.org*. Pirate Party Germany, Berlin. Retrieved 4 October 2013.

- Grothoff, Christian (2015). "The Architecture of the GNUnet: 45 Subsystems in 45 Minutes" (https://grothoff.org/christian/psc2015.pdf) (PDF). Retrieved 2016-07-14.

External links

- Official website (https://gnunet.org/) ✏️