

Peer-to-Peer

The peer-to-peer layer (P2P) of the Internet Computer realizes the reliable and secure communication of network messages, also called **artifacts**, between the nodes of a subnet. Artifacts are the network messages that are to be broadcast in the subnet, including the input to canister smart contracts submitted by users or protocol-originating messages such as the blocks produced by the consensus layer. P2P guarantees the secure eventual broadcast delivery of an artifact to all nodes which require it to make progress. The P2P layer thereby is the communication fabric for the IC protocol stack and is used by the consensus layer, the next layer in the stack above it, to broadcast artifacts to the nodes in the subnet.

It is important to note that broadcast artifacts reach all necessary subnet nodes eventually, that is, no upper bound on when this happens can be given. This **asynchronous communication network** assumption is used for the ICP's communication and consensus layers as it reflects the properties of real-world networks.

Gossip Protocol

The P2P layer builds upon the basic principle of **gossip**. Gossip in communication networks works along the same basic principle as gossip among people: A node in the subnet is connected with a subset of the other nodes of the subnet – its **peers**. Whenever a node receives an artifact from a peer or creates one itself as part of the IC protocol, it gossips this artifact to all its peers. By every node in the network doing exactly this, every artifact **eventually** propagates through the whole subnet, despite potential connectivity issues or malicious node behavior.

Whenever a subnet node receives or generates an artifact to be broadcast, the node makes the artifact available to all peers. Every node doing so ensures that the artifact will eventually be delivered to all subnet nodes. However, doing so in a naïve way by simply sending the artifact to all peers would result in nodes receiving as many copies of the same artifact as the node has peers, which unnecessarily consumes networking bandwidth for transmitting duplicate messages and reduces the achievable throughput of the subnet.

This duplication of delivered artifacts in the naïve approach is mitigated by nodes sending **adverts** for artifacts to their peers instead of sending the artifacts themselves. An advert specifies its corresponding artifact, but is a small message only containing the hash of the artifact to unambiguously refer to it and some additional metadata. A node only pushes adverts for artifacts to its peers. After receiving an advert, a node may request the corresponding artifact from one or more of its peers who sent it an advert for that artifact.

Prioritization of Artifacts

The P2P layer allows the prioritization of artifacts such that the more crucial artifacts are broadcast throughout the subnet nodes more quickly than the others. Prioritizing some artifacts over others is important to ensure that the protocol can always make progress and not be starved of network bandwidth by "less important" traffic. This principle is well known from traditional networking and applies equally well to a blockchain system.

Security

To prevent Denial of Service (DOS) attacks, nodes will only request and accept connections with nodes in the same subnet. Subnet membership is managed by the [Network Nervous System \(NNS\)](#). Thanks to the information stored in the NNS canisters P2P can guarantee that all the communication between two nodes is encrypted and authenticated, by using TLS.

Go Even Deeper

[P2P on the IC wiki](#)

[Blogpost on P2P](#)

