1 Definitions

For clarity's sake, when I use the name ZeroTier, unless otherwise specified, I am referring to the V1 ZeroTier protocol.

Definition 1 (Node)**.** A *node* in zerotier is a client machine running the zerotier protocol. A node is capable of making peer-to-peer, end-to-end encrypted connections with any other node, so long as it knows the address of the other node, and the other node chooses to respond to its connection.

Definition 2 (Address)**.** The *address* of a node in zerotier is a uniquely identifying 40-bit number derived from the hash of the node's public key.

Definition 3 (Identity)**.** The *identity* of a node in zerotier consists of that node's public key and matching address.

Definition 4 (Path)**.** A *path* is the physical link that is used for one node to send network packets to another. Generally this is a direct link over UDP, in which case the path is fully specified by the IP address and open port of the other node. Paths are automatically found and established using DNS-like name resolution and NAT hole punching.

Definition 5 (Network Identifier)**.** A *network identifier* is a 64-bit number consisting of an address followed by a 16-bit "network number".

Definition 6 (Network Controller)**.** A *network controller* is simply a node that has had it's address distributed as part of a network identifier. Network controllers are able to define a sub-network of the zerotier global virtual network. Nodes are members of this sub-network if and only if they have been given permission to join it by the network controller. The network controller is also able to distribute certificates, credentials and network rules to members of its network, giving it fine control over all interactions between nodes. It is not however able to decrypt or modify traffic over its network that was not directly sent to it.

Definition 7 (Root Servers)**.** *Root servers* are machines operated by the ZeroTier organization that centrally handle the job of memorizing the mapping between addresses and identities, and the mapping between addresses and possible paths to contact the owner of that address. Within the protocol, they are responsible for public key distribution and for coordinating initial contact between newly connecting machines.

Once keys are distributed and contact is established nodes will no longer contact root servers. The only exception being if the path connecting two nodes goes down, and a new path needs to be established, or if for whatever reason a direct path between two nodes cannot be established, so the nodes decide to route their traffic through their shared connection to the root servers.

Network traffic in zerotier is peer-to-peer and end-to-end-encrypted. Once a secure session is established between two nodes, it is cryptographically infeasible for the ZeroTier organization to read or modify any node's network traffic. However, it is possible for ZeroTier to perform a man-in-the-middle attack on newly connecting nodes that have not yet established a session. When a root server is asked to map an address to its node's identity, the root can instead brute-force the 40-bits of the address to generate an identity that matches it. It can then respond with this identity it controls instead of the correct one. The root server must then sabotage the zerotier pathfinding protocol so that network traffic between these two nodes is either routed through it, or a server controlled by it. Once all this is done a classical man-in-the-middle attack can follow. Any out-of-band confirmation that the identity of the node being contacted is the same as the identity returned by the root will render this attack impossible.

Due to security and reliability concerns it is not yet possible for independent administrators to operate their own root servers. However it is possible to operate mirrors of the root servers. These mirrors, referred to as "moons" create a local copy of some subset of the root server database, and will defer to the root servers if a request is made of them for an address not present in their database.

Upon installation, zerotier generates a random public and private key. The private key is saved to the host machine. The public key is used to generate an address and identity. This identity is submitted to a random root server, and if the root server confirms that the node's address is not in use, it is saved to both the host machine and the root server. If it is in use the host machine will generate a new keypair and try again.

Next zerotier will ask for a network identifier from the user. When this is given the host machine will ask a random root server for the identity of the node