Assignment Prerequisites

Operating system: LND runs on Windows or Mac OS X, but Unix operating systems are recommended, while Debian/Ubuntu is used for the examples below. A 64-bit architecture is required due to files growing larger than 2GB.

Machine: LND requires at minimum 2GB RAM and a 1 GHz quad core with at least 5GB of storage. LND makes frequent reads and writes, meaning you should not use a SD card, but instead a SSD of good quality.

Bitcoin: LND does not require a Bitcoin backend as you may run your node in Neutrino mode. For performance reasons it is recommended to run either Bitcoin Core or btcd on the same machine or on a machine on the same network. You may prune your Bitcoin node, though doing so aggressively may impact performance. To make use of LND's taproot functionalities you must run at least bitcoind v0.21 or btcd v0.23.1.

Make sure Lightning Client is configured with the Bitcoin Testnet

Tasks

Creating a Lightning Channel

1. Initialize a Lightning Node A
2. Connect A to Another Lightning Node B and open the channel
3. Initialize a Lightning Node C
4. Connect Node B to Node C and open the channel
5. Connect A to Another Lightning Node D and open the channel
6. Connect Node D to Node C and open the channel

Setting Up Multihop Payment Routing

1. Create a Multihop Payment Route between A and C (Single path)
2. Generate Payment Invoice on the Destination Node
3. Pay the Invoice via Multihop Route

Perform Multipath Payment (MPP vs AMP)

1. Try to initiate a payment from A to C where a single apth capacity is too low to carry the full amount. Observe whether the Lightning Network finds an alternate route or splits the payment across multiple path i.e. multipath payment (MPP).
2. Perform an AMP from A to C (considering payment value exceeds capacity of a single route) and compare it with MPP - To be able to make and send Atomic Multi-path Payments (AMP), you will need to upgrade your node to LND 0.13 or above. Atomic Multi-path Payments are a new type of Lightning payments implemented by LND in version v0.13.0-beta. As the new payment type is an end-to-end upgrade, it doesn't require the internal of the network to update before it can be used widely. Instead, only the sender and receiver need to understand the new payment type.

   Atomic Multi-path payments differ from existing Multi-path Payments (MPP) in that they are atomic, meaning despite being routed through separate paths. In MPPs, all shards use the same payment hash, making the individual routes easily correlatable and prone to only partial settlement. By contrast AMPs are either settled in full or not settled at all. Using AMP, it is possible to make payments safely by only knowing the public key of the recipient. It is also possible to create invoices that can be used repeatedly, which can be used to implement traditional subscriptions. Such invoices can also be published without security implications, allowing for use cases such as static donation invoices.

Closing the Channel

Close Channel AB and DC - Close a Lightning channel and return funds to the Bitcoin testnet wallet.