Upgrading from Monero payment IDs to subaddresses

Current situation

A receiver will publish either:

1. A Monero wallet address along with a 64-hex-character payment ID.
2. A Monero integrated wallet address, which combines the wallet address with a particular payment ID.

New situation

Payment IDs will be discontinued in most wallets in April 2019 and will be disallowed for all transactions in October 2019. A receiver needs to issue a subaddress per sender to identify incoming payments, just like merchants do with Bitcoin addresses.

How to generate subaddresses

Wallets use a subaddress numbering scheme which consists of a 32 bit "account index" combined with a 32 bit "subaddress index."

There are therefore approximately 4 billion accounts available, where each account can have up to 4 billion subaddresses.

The reason for grouping subaddresses into accounts is purely so that it is easy for a wallet user to see balance sub-totals on a per-account basis.

To generate a new subaddress to give out, either:

1. Run the monero-wallet-cli, and type: `address new`.
2. Connect to your wallet via the RPC interface and use the get_address method https://www.getmonero.org/resources/developer-guides/wallet-rpc.html#get_address
3. Generate a subaddress purely in software, using knowledge of your wallet's public spend key and private view key.

   Javascript implementation: https://www.npmjs.com/package/subaddress

   Python implementation: https://github.com/emesik/monero-python

   Instructions for writing your own implementation: https://monero.stackexchange.com/a/10676/42

Ensuring your wallet detects incoming funds

The Monero wallet needs to "precompute" subaddress tables in advance, in order to detect incoming payments to those subaddresses. Therefore, it's important that you tell your wallet to "look ahead" enough subaddress indices to discover incoming payments. Monero will automatically look ahead 200 subaddresses at a time, where it will decide to look ahead further if it sees payments arrive at those higher numbered subaddress indices. You may need to tune your wallet to look ahead further than this. Using non-incremental indices provides no benefit and adds significant computational cost. Instructions here: https://monero.stackexchange.com/q/10184/42