```
BIP: 111
Layer: Peer Services
Title: NODE_BLOOM service bit
Author: Matt Corallo <bip111@bluematt.me>
        Peter Todd <pete@petertodd.org>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0111
Status: Proposed
Type: Standards Track
Created: 2015-08-20
License: PD
```

Abstract

This BIP extends BIP 37, Connection Bloom filtering, by defining a service bit to allow peers to advertise that they support bloom filters explicitly. It also bumps the protocol version to allow peers to identify old nodes which allow bloom filtering of the connection despite lacking the new service bit.

Motivation

BIP 37 did not specify a service bit for the bloom filter service, thus implicitly assuming that all nodes that serve peers data support it. However, the connection filtering algorithm proposed in BIP 37, and implemented in several clients today, has been shown to provide little to no privacy[1], as well as being a large DoS risk on some nodes[2]. Thus, allowing node operators to disable connection bloom filtering is a much-needed feature.

Specification

The following protocol bit is added:

```
NODE_BLOOM = (1 << 2)
```

Nodes which support bloom filters should set that protocol bit. Otherwise it should remain unset. In addition the protocol version is increased from 70002 to 70011 in the reference implementation. It is often the case that nodes which have a protocol version smaller than 70011, but larger than 70000 support bloom filtered connections without the NODE_BLOOM bit set, however clients which require bloom filtered connections should avoid making this assumption.

NODE_BLOOM is distinct from NODE_NETWORK, and it is legal to advertise NODE_BLOOM but not NODE_NETWORK (though there is little reason to do so now, some proposals may make this more useful in the future)

[1] http://eprint.iacr.org/2014/763

[2] 1 is one example where the issues were found, though others independently discovered issues as well. Sample DoS exploit code available at https://github.com/petertodd/bloom-io-attack.

If a node does not support bloom filters but receives a "filterload", "filteradd", or "filterclear" message from a peer the node should disconnect that peer immediately. For backwards compatibility, in initial implementations, nodes may choose to only disconnect nodes which have the new protocol version set and attempt to send a filter command.

While outside the scope of this BIP it is suggested that DNS seeds and other peer discovery mechanisms support the ability to specify the services required; current implementations simply check only that NODE_NETWORK is set.

Design rational

A service bit was chosen as applying a bloom filter is a service.

The increase in protocol version is for backwards compatibility. In initial implementations, old nodes which are not yet aware of NODE_BLOOM and use a protocol version < 70011 may still send filter messages to a node without NODE_BLOOM. This feature may be removed after there are sufficient NODE_BLOOM nodes available and SPV clients have upgraded, allowing node operators to fully close the bloom-related DoS vectors.

Reference Implementation

https://github.com/bitcoin/bitcoin/pull/6579

Copyright

References