Problem statement

- RP and shared trees may be the bottleneck in network, with in-optimal forwarding and not always reliable.
  - draft-ietf-pim-source-discovery-bsr-04 provides more details on this and proposes using a new PIM message type for distributing active source information allowing.

- This draft proposes using the IGP for distributing active source information. This has some benefits over the PIM based solution.
  - One concern is security. A forged router can inject a huge amount of fake active sources. It may lead to using a lot of memory for storing and forwarding messages, as well as routers joining towards sources that are not really active.
  - PIM with IPsec can be an option, but complex to configure compared to IGP security mechanisms.
For Example, Router E is attacked, and Re sends forged info into the network. Router C sends join message towards Re for non-active sources.
Problem solution

• IGP has the flooding function.

• IGP has the authentication function to insure the advertisement reliability.

• Use IGP to flood multicast information is a feasible way.
TLV is used to carry the multicast source and group information.
• Any comments are welcome ^_^
Thanks!