Private Tor Network

Title -> Setting up a private tor network.

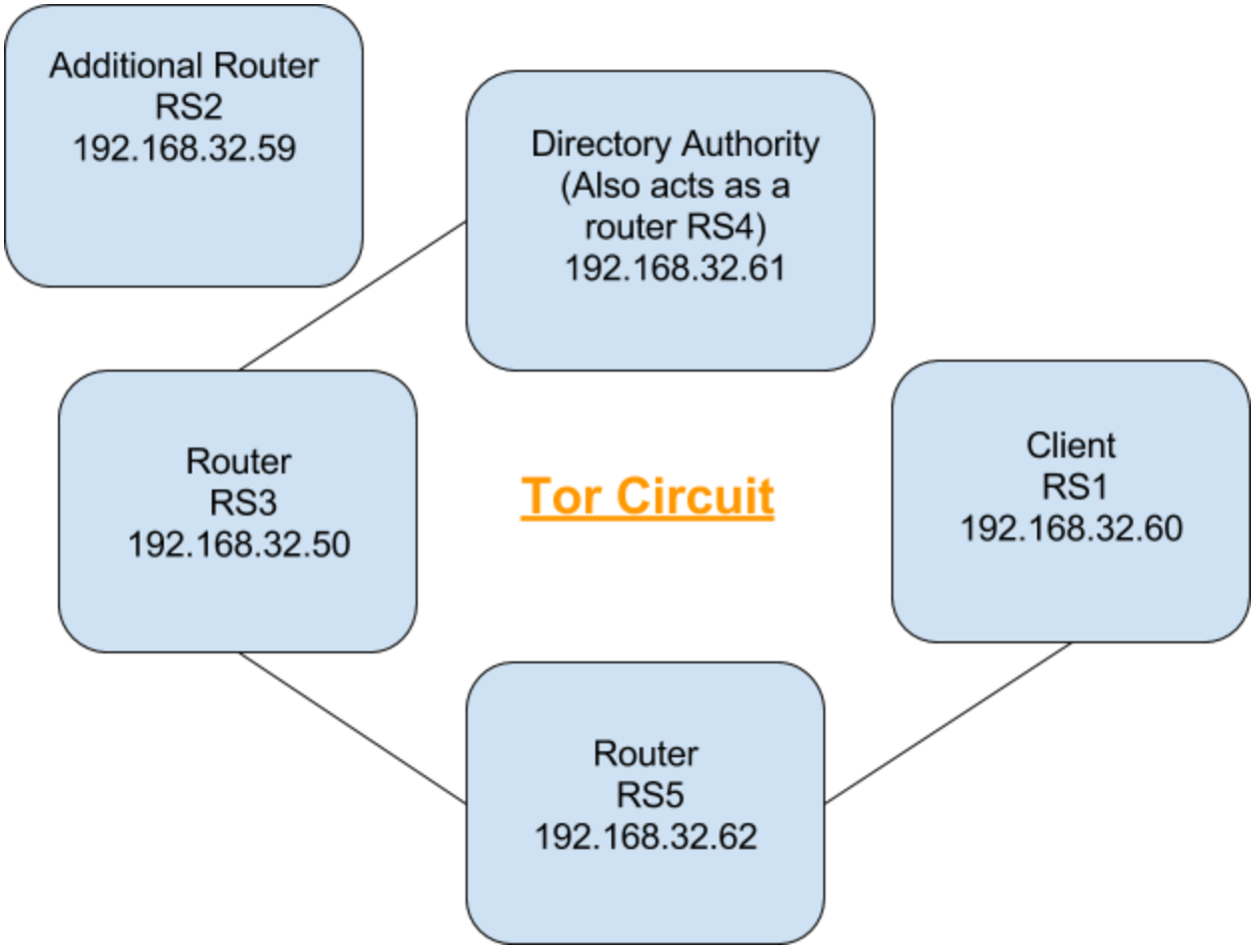
Project ID -> 4

Team -> Ramya Y S - 2015117 - yellapragada15117@iiitd.ac.in
Viraj Parimi - 2015068 - parimi15068@iiitd.ac.in

Objective ->

1. Setting up a private tor network.
2. Server address accessible by the client when circuit is set up i.e tor running on all nodes.

Architecture Diagram ->



Hardware and Software Prerequisites ->

1. Minimum 4 computers to set up different nodes on the tor network
2. Tor installed on all the computers.
3. Wireshark to monitor the network.
4. Set SOCKS proxy in Firefox browser to listen to SOCKS port 9011.

Links to packages/Libraries Used ->

1. https://www.torproject.org/
2. Sudo apt-get install tor would suffice for linux systems.
3. Sudo apt-get install wireshark.

Source Code ->

1. Config Files -> Corresponding torrc files for all nodes can be found here.
2. Server status and Consensus status can be found here.

Use Cases ->

1. Helps users understand how a tor network actually works.
2. Better understanding of tor relay and Directory Authority parameters.
3. Helps one to use a torrc config according to the need of the user.
4. Can see the network in action thereby see that the client does not actually directly talk to the server.

Unfinished Tasks ->

1. Did not set up the network on docker because it is not feasible.

References ->

1. http://fengy.me/prog/2015/01/09/private-tor-network/
2. https://www.torproject.org/docs/tor-relay-debian.html.en
3. https://sourceforge.net/p/silvertunnel-ng/wiki/Tor%20Directory%20Server%20URLs/