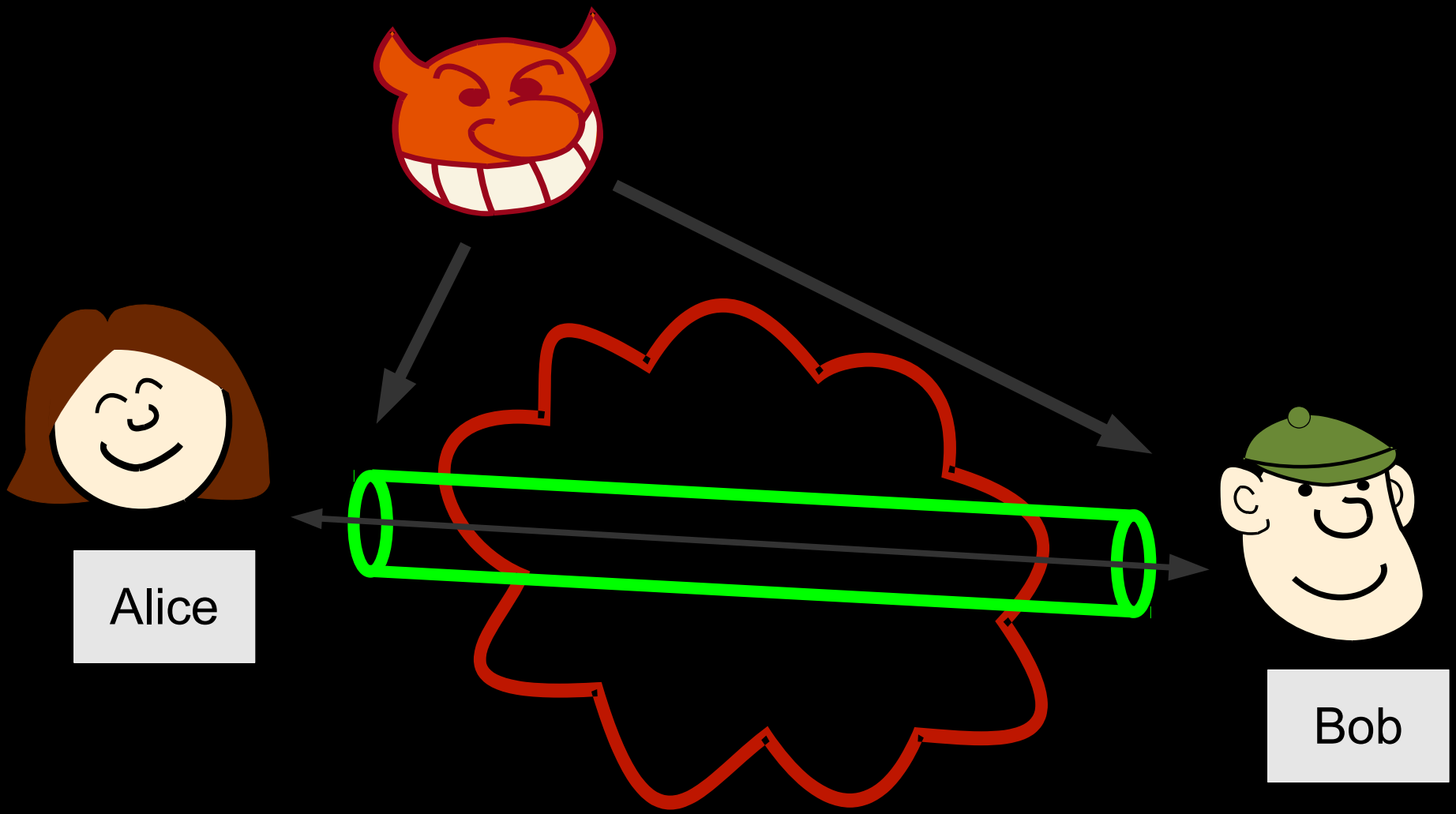
The Tor Project
Anonymity Online

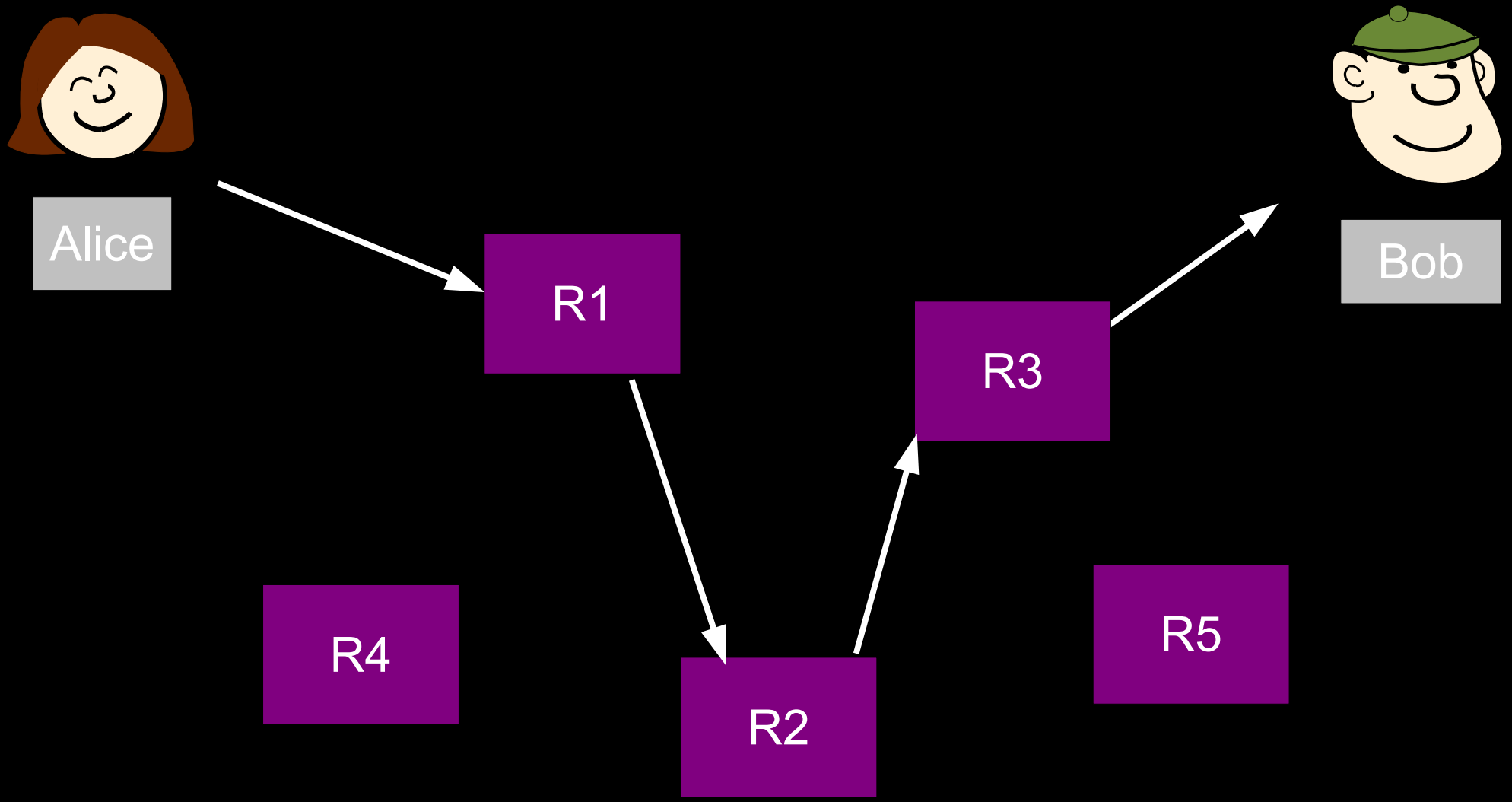
Erinn Clark & Linus Nordberg
erinn@torproject.org
linus@torproject.org

Heard about Tor?

What's the problem?



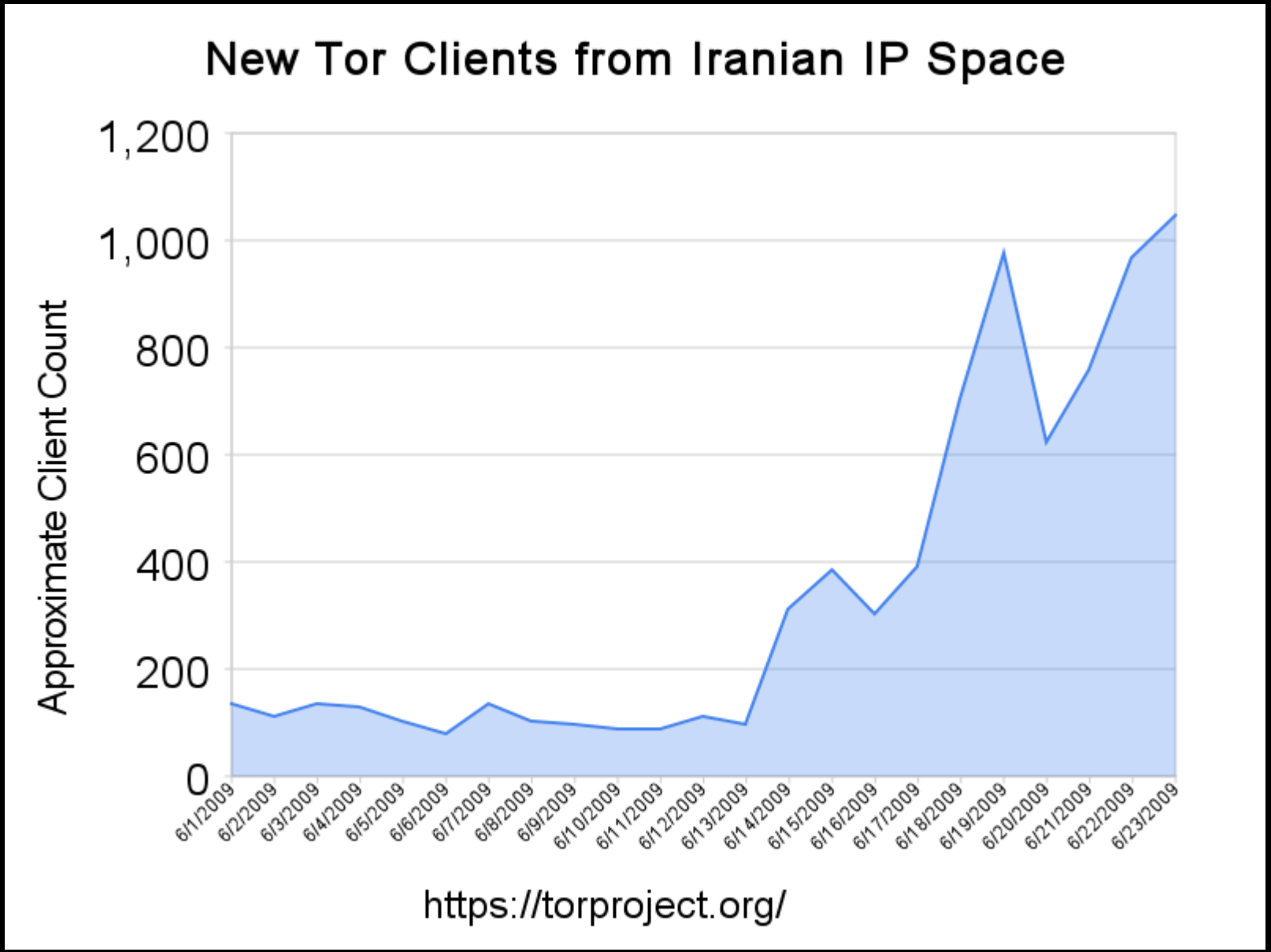
What's the solution?



What's the problem?

What's the solution?

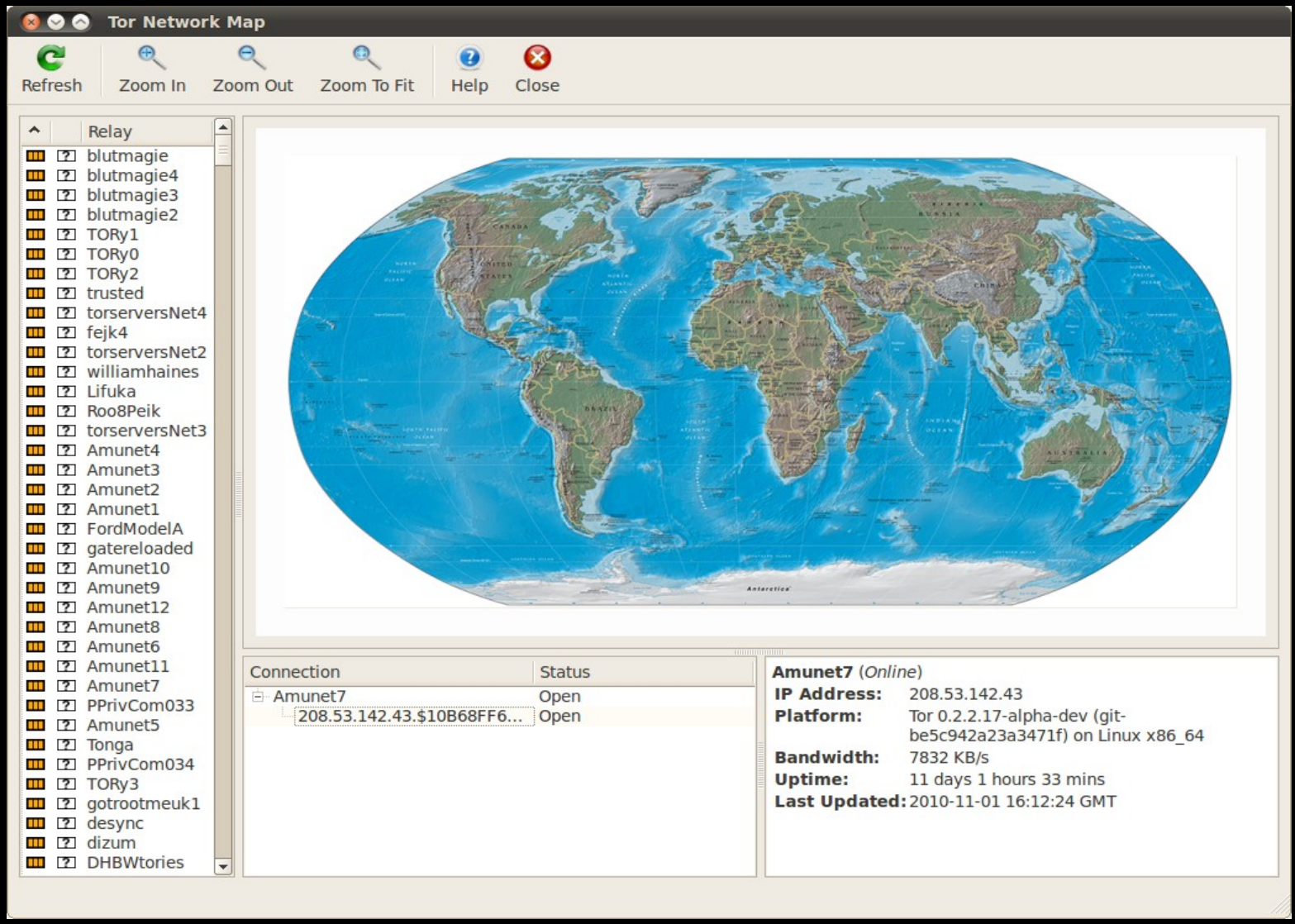
What's the problem?


New Tor Clients from Iranian IP Space
Approximate Client Count
1,200
1,000
800
600
400
200
0
6/1/2009
6/2/2009
6/3/2009
6/4/2009
6/5/2009
6/6/2009
6/7/2009
6/8/2009
6/9/2009
6/10/2009
6/11/2009
6/12/2009
6/13/2009
6/14/2009
6/15/2009
6/16/2009
6/17/2009
6/18/2009
6/19/2009
6/20/2009
6/21/2009
6/22/2009
6/23/2009
https://torproject.org/

What's Tor?

```c
/** Tor main loop. */
/* static */ int
do_main_loop(void)
{
  int loop_result;
  time_t now;

  /* initialize dns resolve map, spawn workers if needed */
  if (dns_init() < 0) {
    if (get_options()->ServerDNSAllowBrokenConfig)
      log_warn(LD_GENERAL, "Couldn't set up any working nameservers. "
               "Network not up yet?  Will try again soon.");
    else {
      log_err(LD_GENERAL,"Error initializing dns subsystem; exiting.  To "
              "retry instead, set the ServerDNSAllowBrokenResolvConf option.");
    }
  }

  handle_signals(1);

  /* load the private keys, if we're supposed to have them, and set up the
   * TLS context. */
  if (! identity_key_is_set()) {
    if (init_keys() < 0) {
      log_err(LD_BUG,"Error initializing keys; exiting");
      return -1;
    }
  }

  /* Set up the packed_cell_t memory pool. */
  init_cell_pool();

  /* Set up our buckets */
  connection_bucket_init();
  stats_prev_global_read_bucket = global_read_bucket;
  stats_prev_global_write_bucket = global_write_bucket;

  /* initialize the bootstrap status events to know we're starting up */
  control_event_bootstrap(BOOTSTRAP_STATUS_STARTING, 0);

  if (trusted_dirs_reload_certs()) {
    log_warn(LD_DIR,
             "Couldn't load all cached v3 certificates. Starting anyway.");
  }
  if (router_reload_v2_networkstatus()) {
    return -1;
```

What's Tor?


Tor Network Map
Refresh
Zoom In
Zoom Out
Zoom To Fit
Help
Close
Relay
blutmagie
blutmagie4
blutmagie3
blutmagie2
TORy1
TORy0
TORy2
trusted
torserversNet4
fejk4
torserversNet2
williamhaines
Lifuka
Roo8Peik
torserversNet3
Amunet4
Amunet3
Amunet2
Amunet1
FordModelA
gatereloaded
Amunet10
Amunet9
Amunet12
Amunet8
Amunet6
Amunet11
Amunet7
PPrivCom033
Amunet5
Tonga
PPrivCom034
TORy3
gotrootmeuk1
desync
dizum
DHBWtories
Connection
Status
Amunet7
Open
208.53.142.43.$10B68FF6...
Open
Amunet7 (Online)
IP Address: 208.53.142.43
Platform: Tor 0.2.2.17-alpha-dev (git-be5c942a23a3471f) on Linux x86_64
Bandwidth: 7832 KB/s
Uptime: 11 days 1 hours 33 mins
Last Updated: 2010-11-01 16:12:24 GMT

What's Tor?

Tor Protocol Specification

Roger Dingledine
Nick Mathewson

0. Preliminaries

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

0.1. Notation and encoding

PK -- a public key.
SK -- a private key.
K -- a key for a symmetric cipher.

a|b -- concatenation of 'a' and 'b'.

[A0 B1 C2] -- a three-byte sequence, containing the bytes with hexadecimal values A0, B1, and C2, in that order.

All numeric values are encoded in network (big-endian) order.

H(m) -- a cryptographic hash of m.

0.2. Security parameters

Tor uses a stream cipher, a public-key cipher, the Diffie-Hellman protocol, and a hash function.

KEY_LEN -- the length of the stream cipher's key, in bytes.

PK_ENC_LEN -- the length of a public-key encrypted message, in bytes.
PK_PAD_LEN -- the number of bytes added in padding for public-key encryption, in bytes. (The largest number of bytes that can be encrypted in a single public-key operation is therefore PK_ENC_LEN-PK_PAD_LEN.)

DH_LEN -- the number of bytes used to represent a member of the Diffie-Hellman group.
DH_SEC_LEN -- the number of bytes used in a Diffie-Hellman private key (x).

HASH_LEN -- the length of the hash function's output, in bytes.

PAYLOAD_LEN -- The longest allowable cell payload, in bytes. (509)

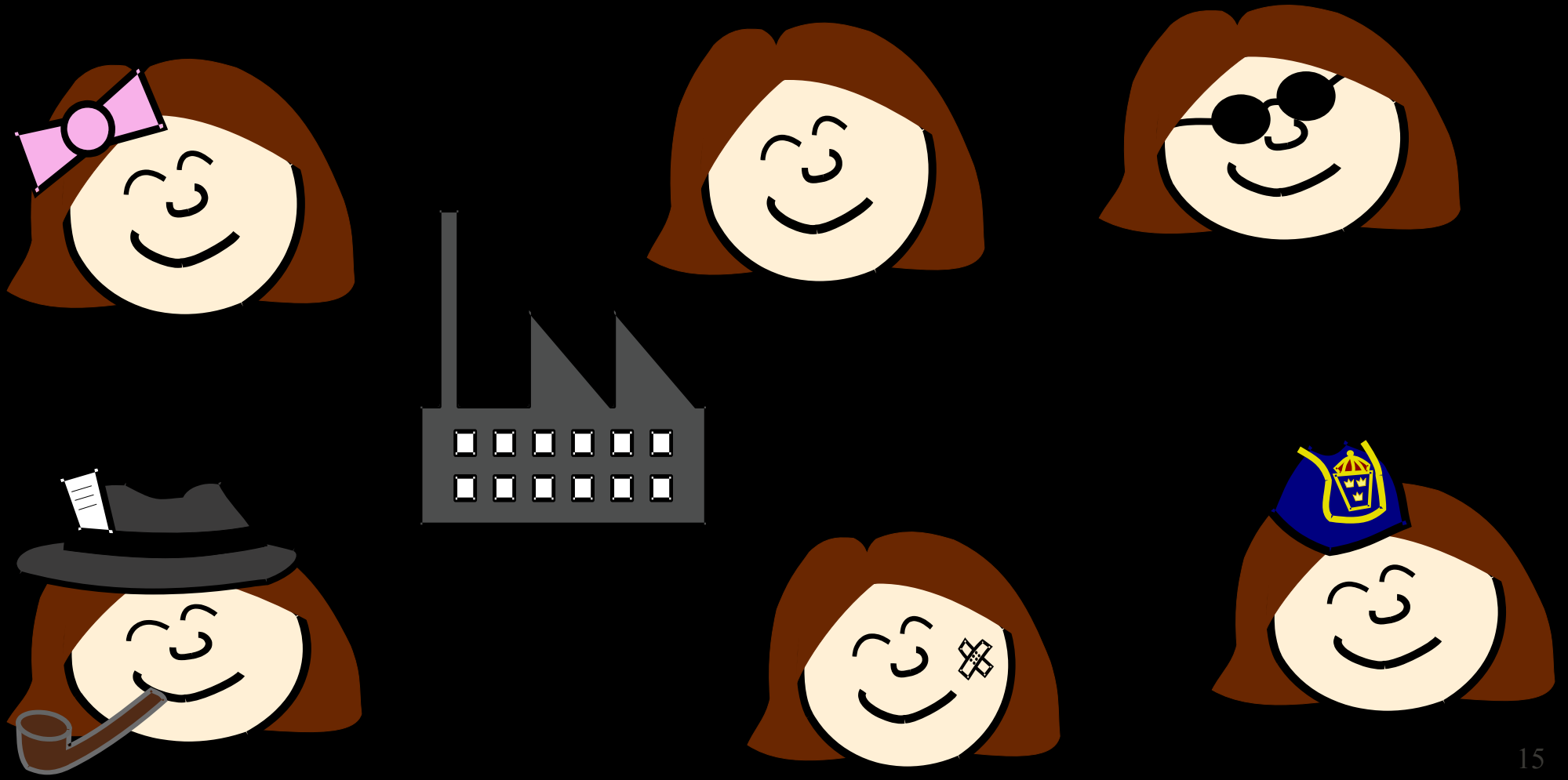
CELL_LEN -- The length of a Tor cell, in bytes.

The Tor Project

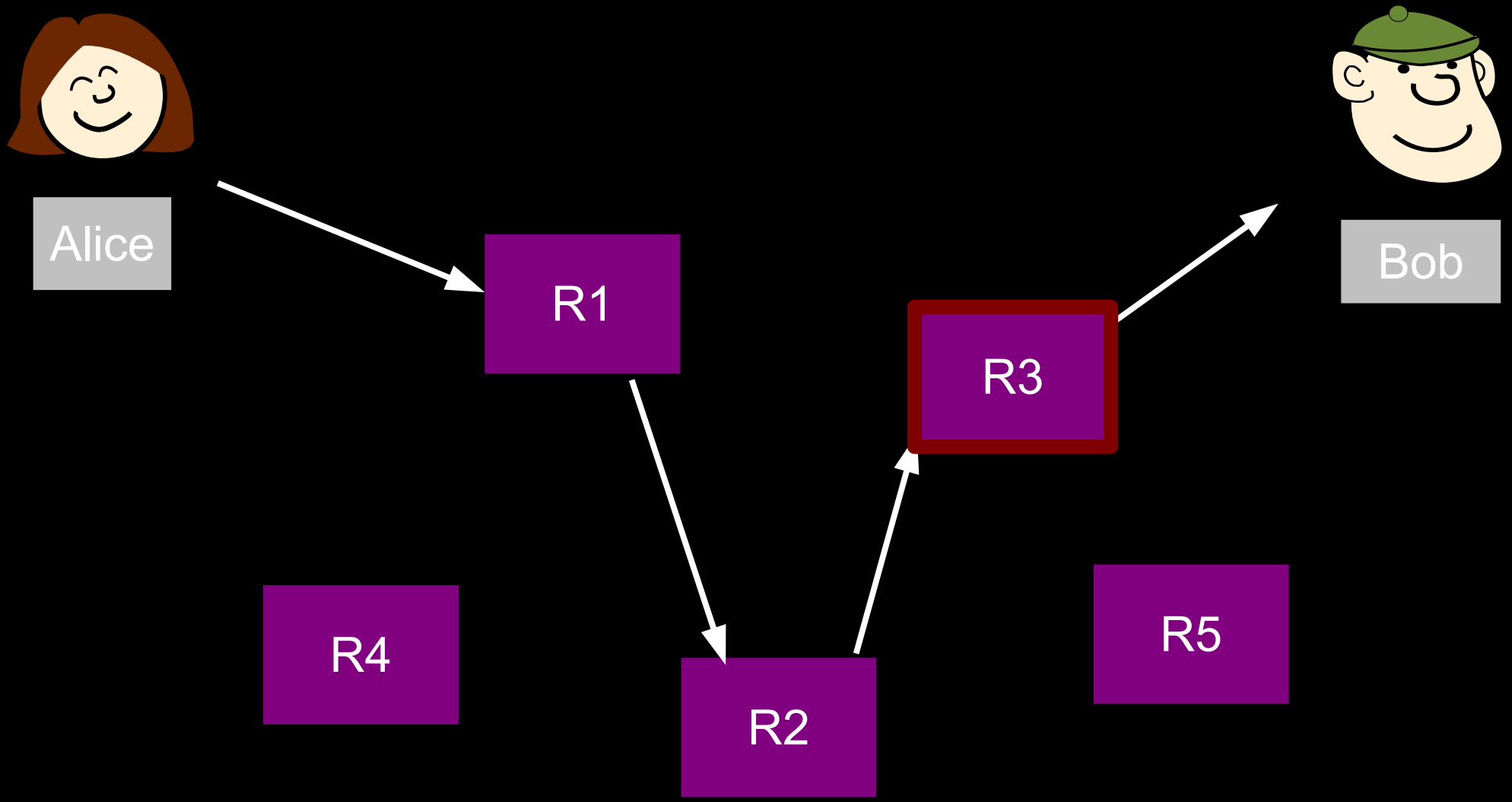
Available software

Available software

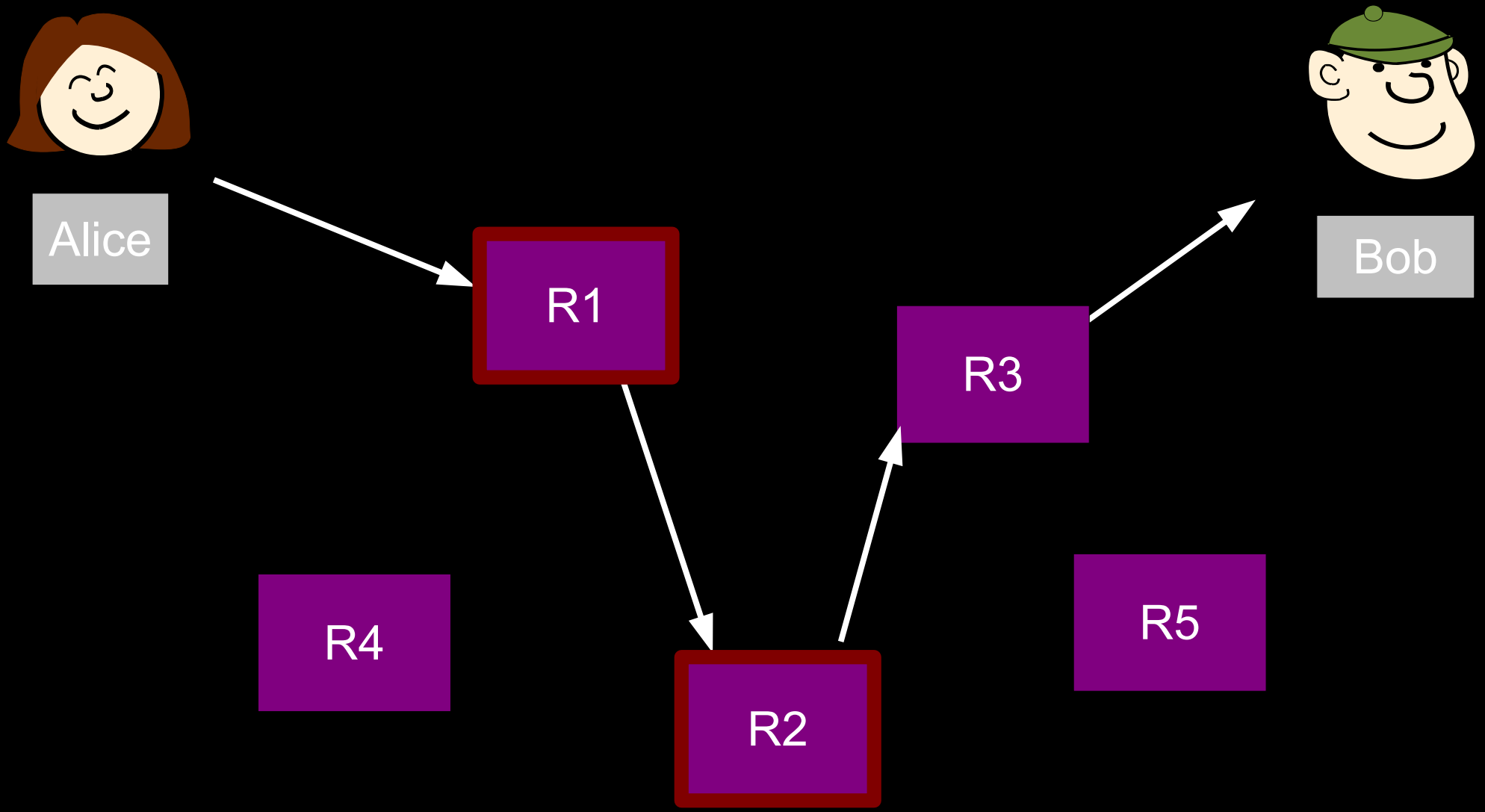
Who uses Tor?



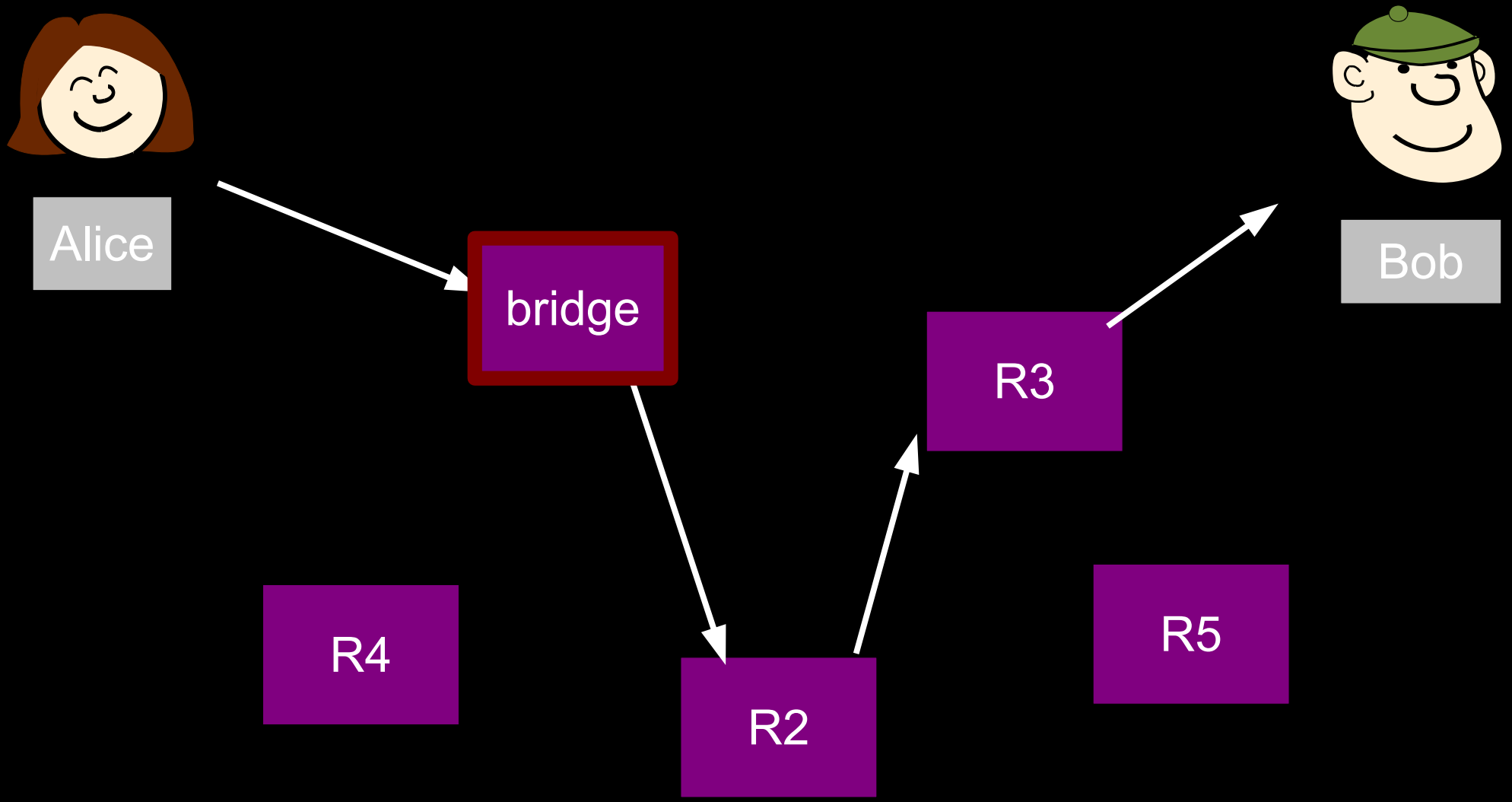
How to help Tor



How to help Tor



How to help Tor



How to help Tor

Where to find us

- IRC: #tor and #tor-dev @ OFTC
- Email: or-talk and or-dev