Anonymizing Network Technologies

Dr Nadeem Ahmed
Senior Research Fellow
Cyber Security Cooperative Research Centre (CSCRC)

Some slides modified from Dingledine, Mathewson, Syverson, Xinwen and Savchenko

Outline

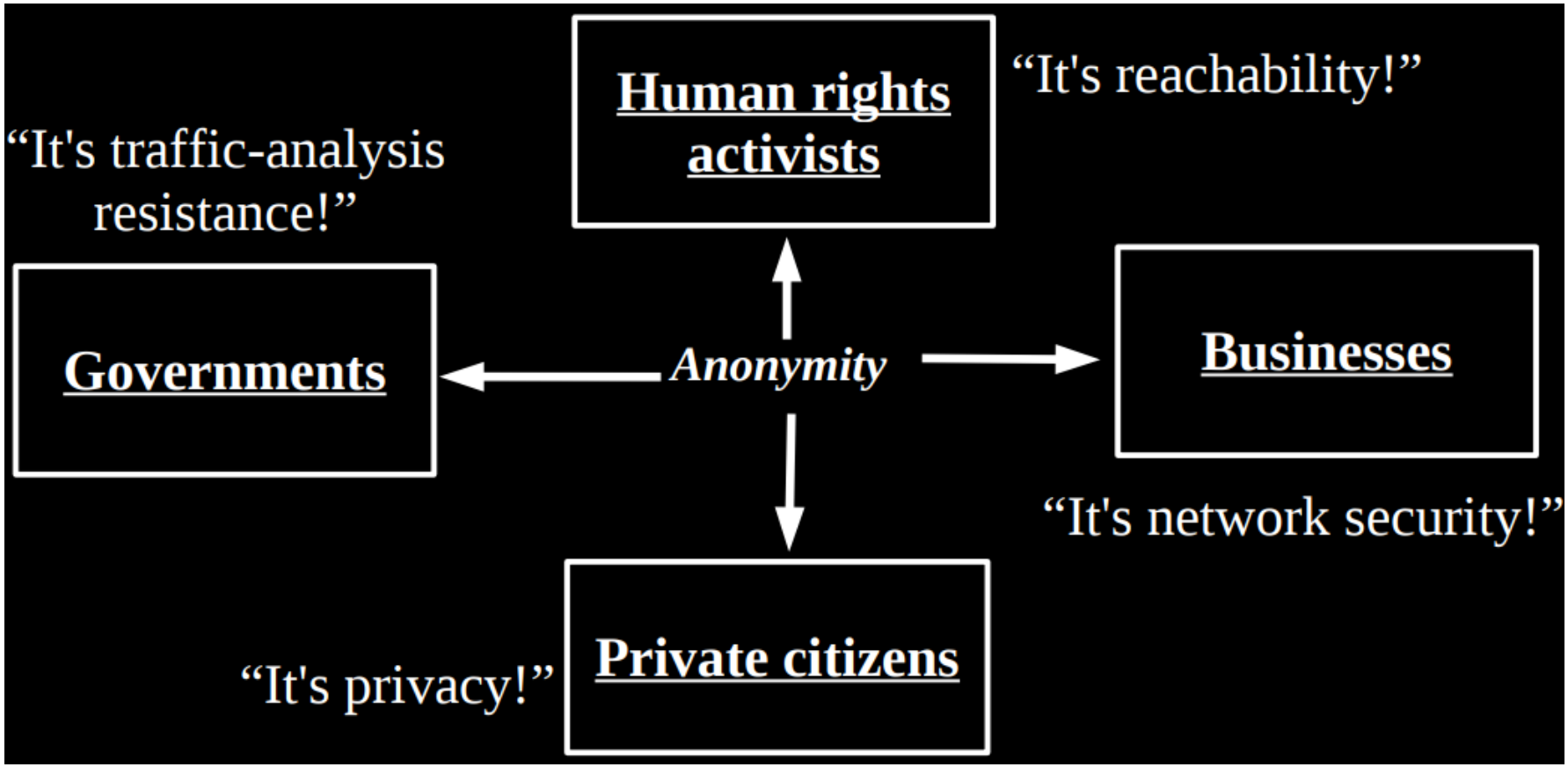
- What is anonymity?
- Tor
- I2P
- Questions/Comments

Anonymity

Anonymity describes situations where the acting person's name is unknown. Some writers have argued that namelessness, though technically correct, does not capture what is more centrally at stake in contexts of anonymity. The important idea here is that a person be non-identifiable, unreachable, or untraceable.

Anonymity is seen as a technique, or a way of realizing, certain other values, such as privacy, or liberty.
~Wikipedia~

Anonymity serves different interests for different user groups



Anonymity serves different interests for different user groups

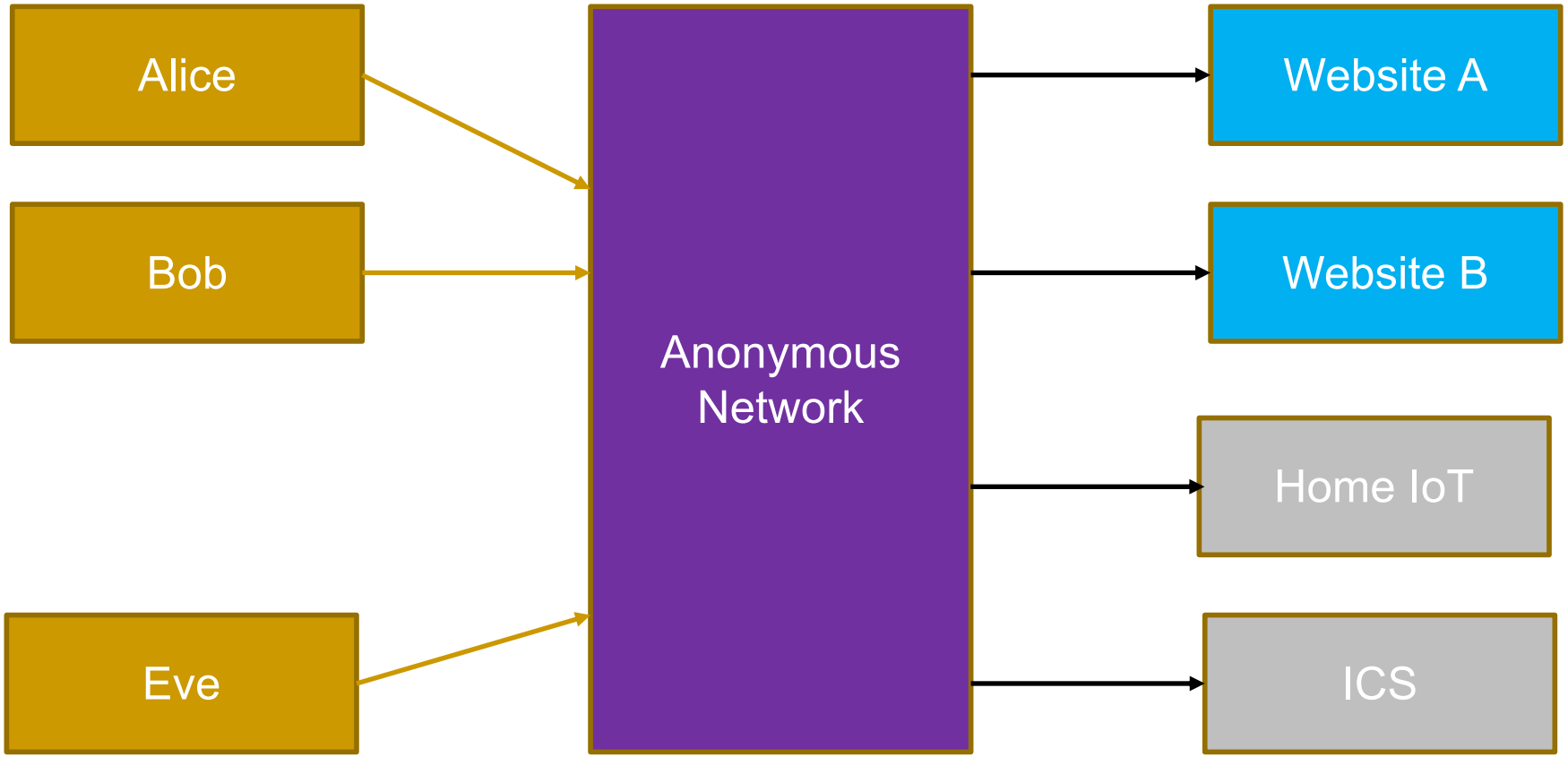
- Don't want to be watched and tracked
  - Browsing history, medical records, unpopular or illegal opinions
  - Hostile, Incompetent and Indifferent Service Providers

- Trade secrets and competitors analysis
  - Engineering / R&D search history

How to achieve Anonymity?

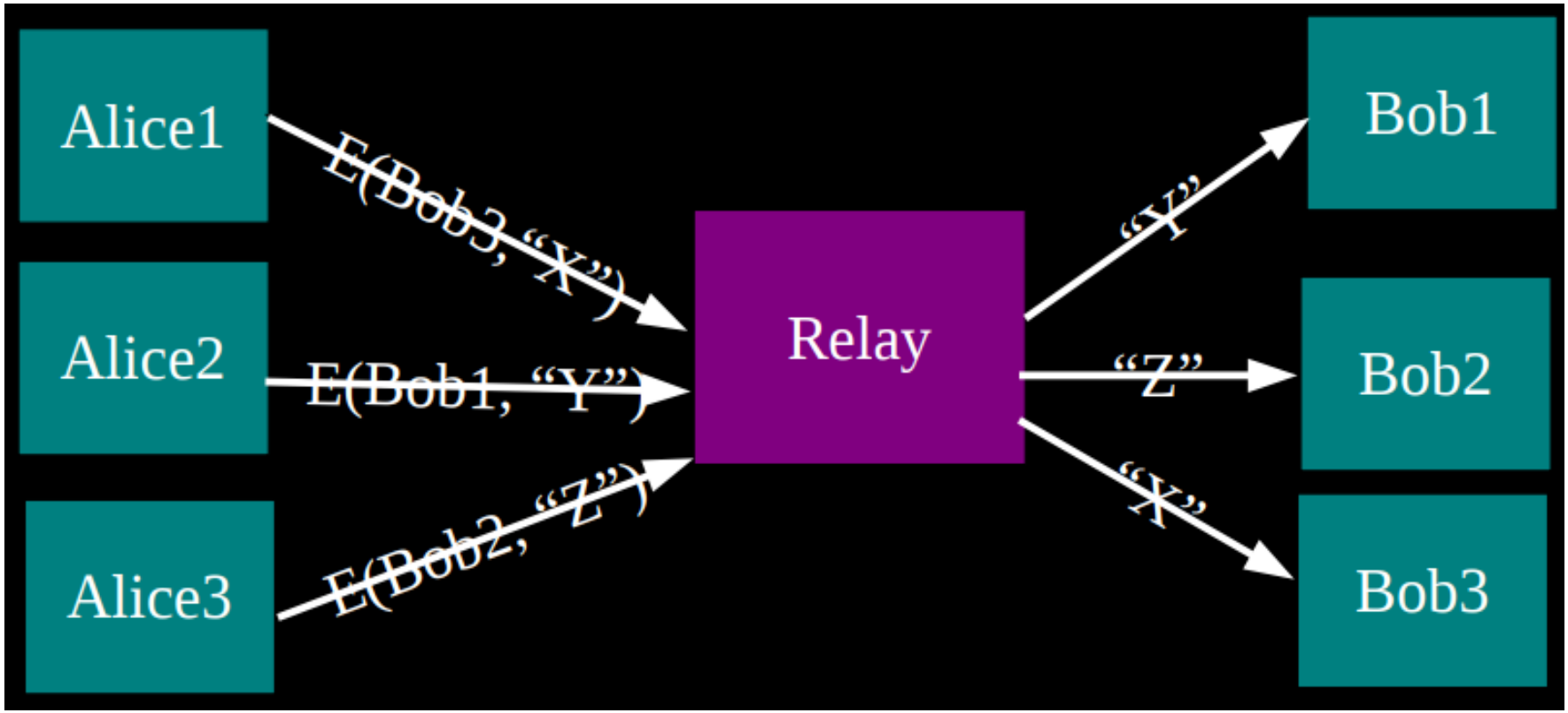
- Indistinguishability within an anonymity net
- You are only anonymous within a group if your actions cannot be distinguished from the actions of anyone else within the group
- The larger the group, the better

Anonymity loves company!

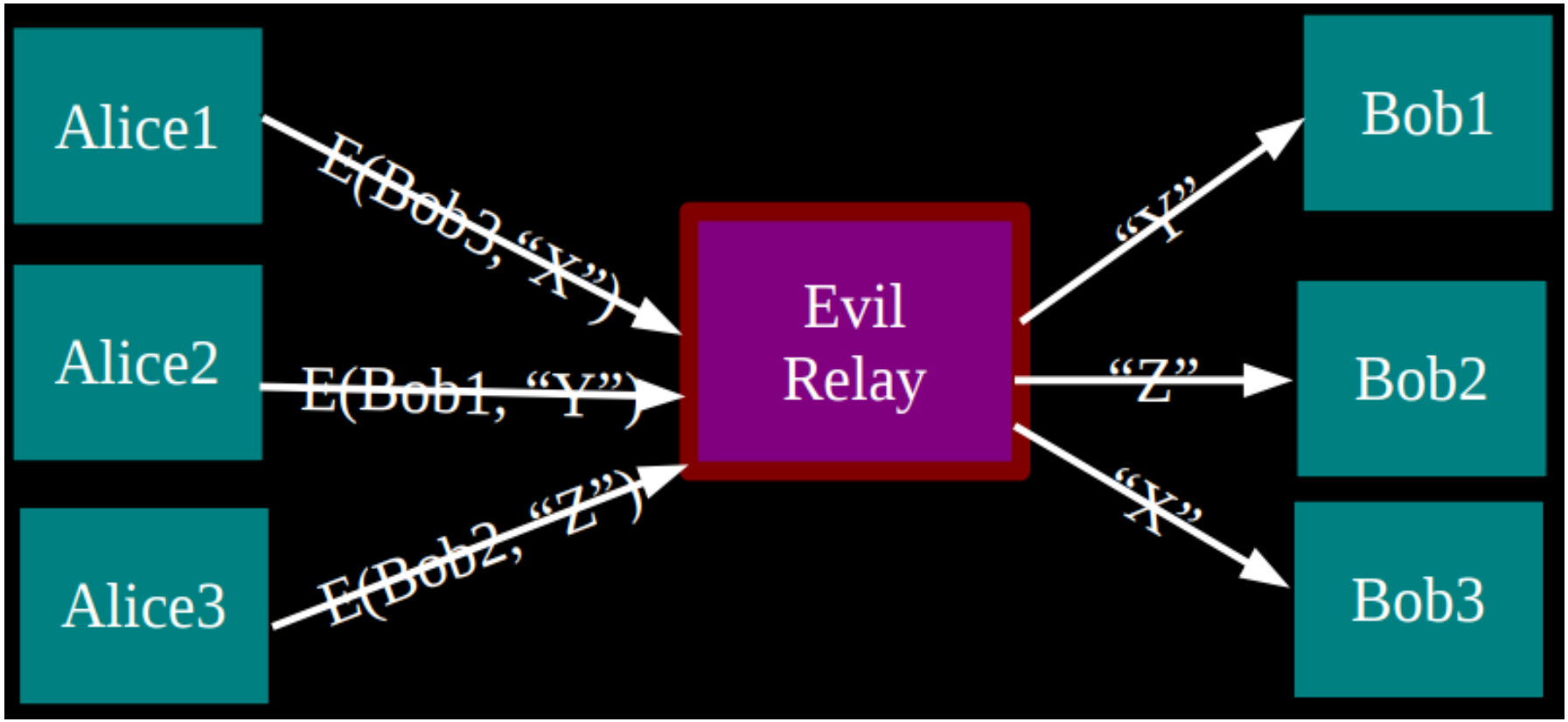


Anonymity

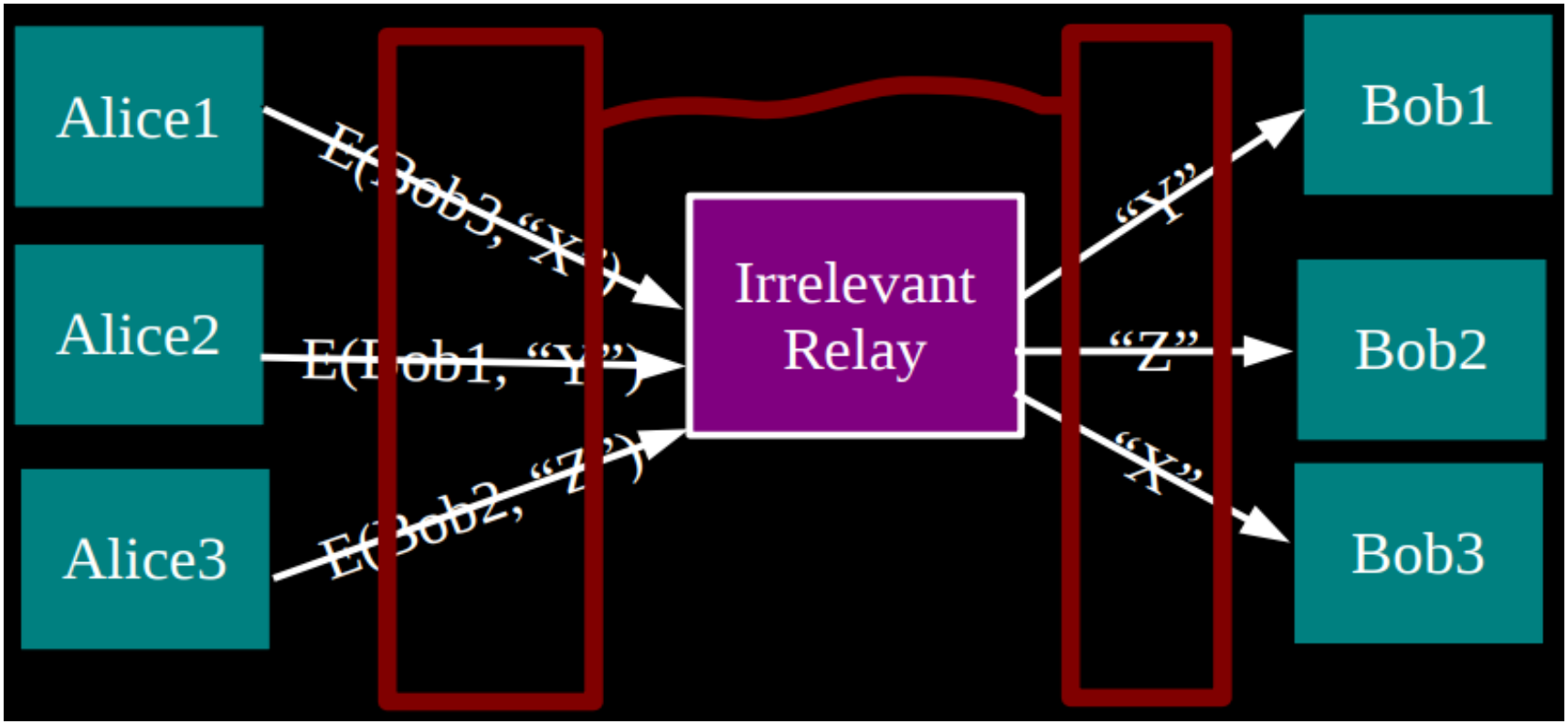
Simplest design:
Single relay (Commercial proxy providers)



Single Relay => Single point of failure



Single Relay => Single point of bypass



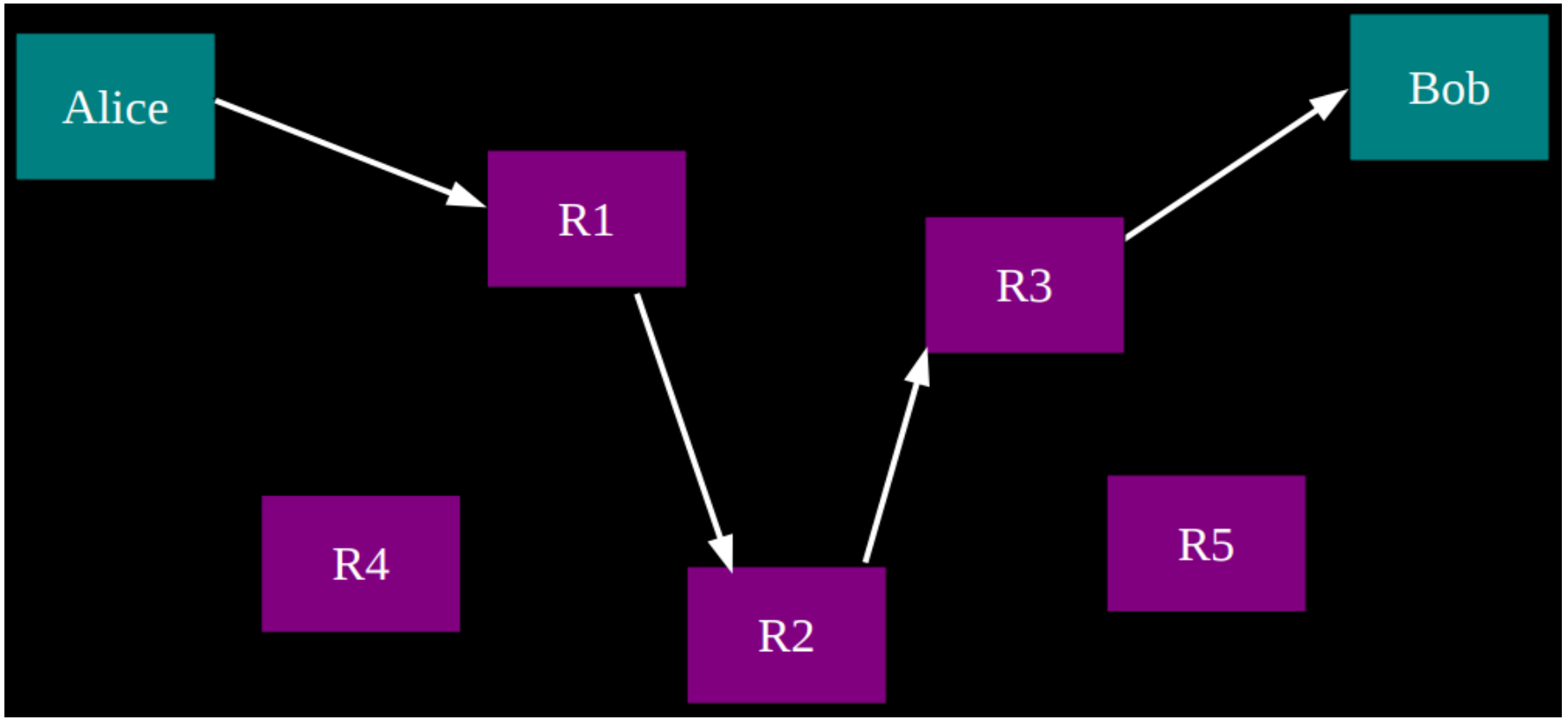
Timing analysis bridges all connections through relay ⇒ An attractive fat target

Problem

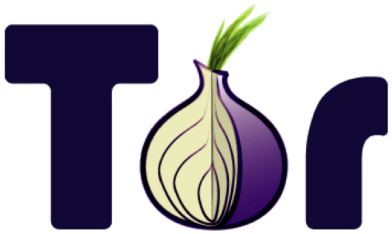
- Internet surveillance like traffic analysis reveals users privacy (Read a bit about X-Keyscore)
- Encryption does not work, since packet headers still reveal a great deal about users
- End-to-end anonymity is needed

- Solution: a distributed, anonymous network

A solution is to add multiple relays



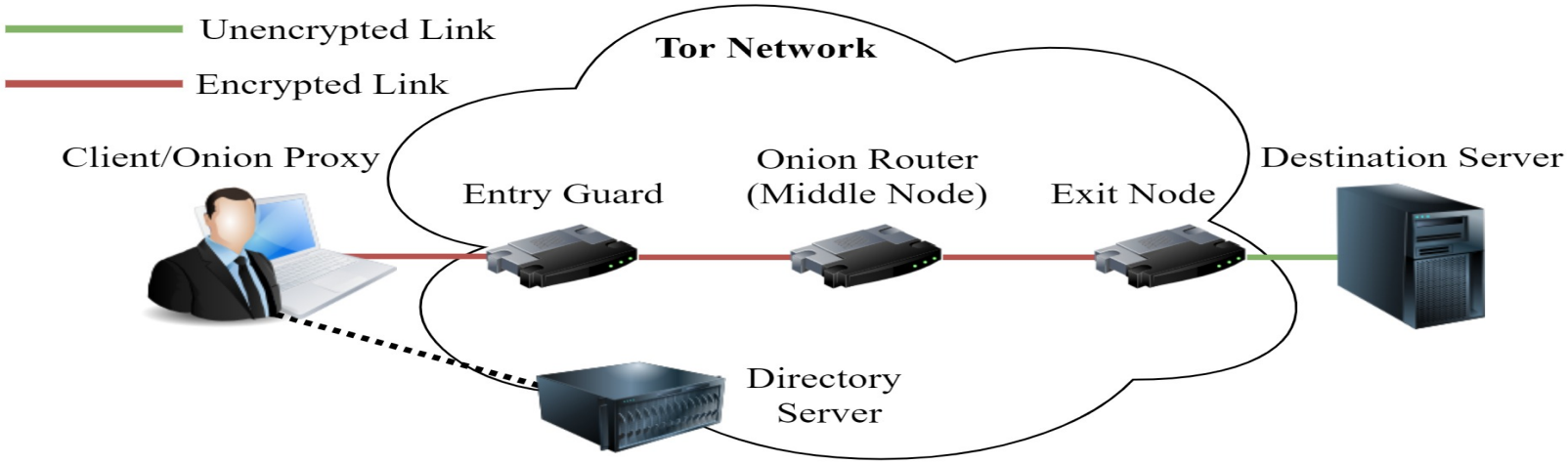
What is Tor?



- Tor is a distributed anonymous communication service using an *overlay* network that allows people to improve their privacy and security on the Internet
- Individuals use Tor to keep websites from tracking them, or to connect to those internet services blocked by their local Internet providers
- Tor's hidden services let users publish web sites and other services without needing to reveal the location of the site

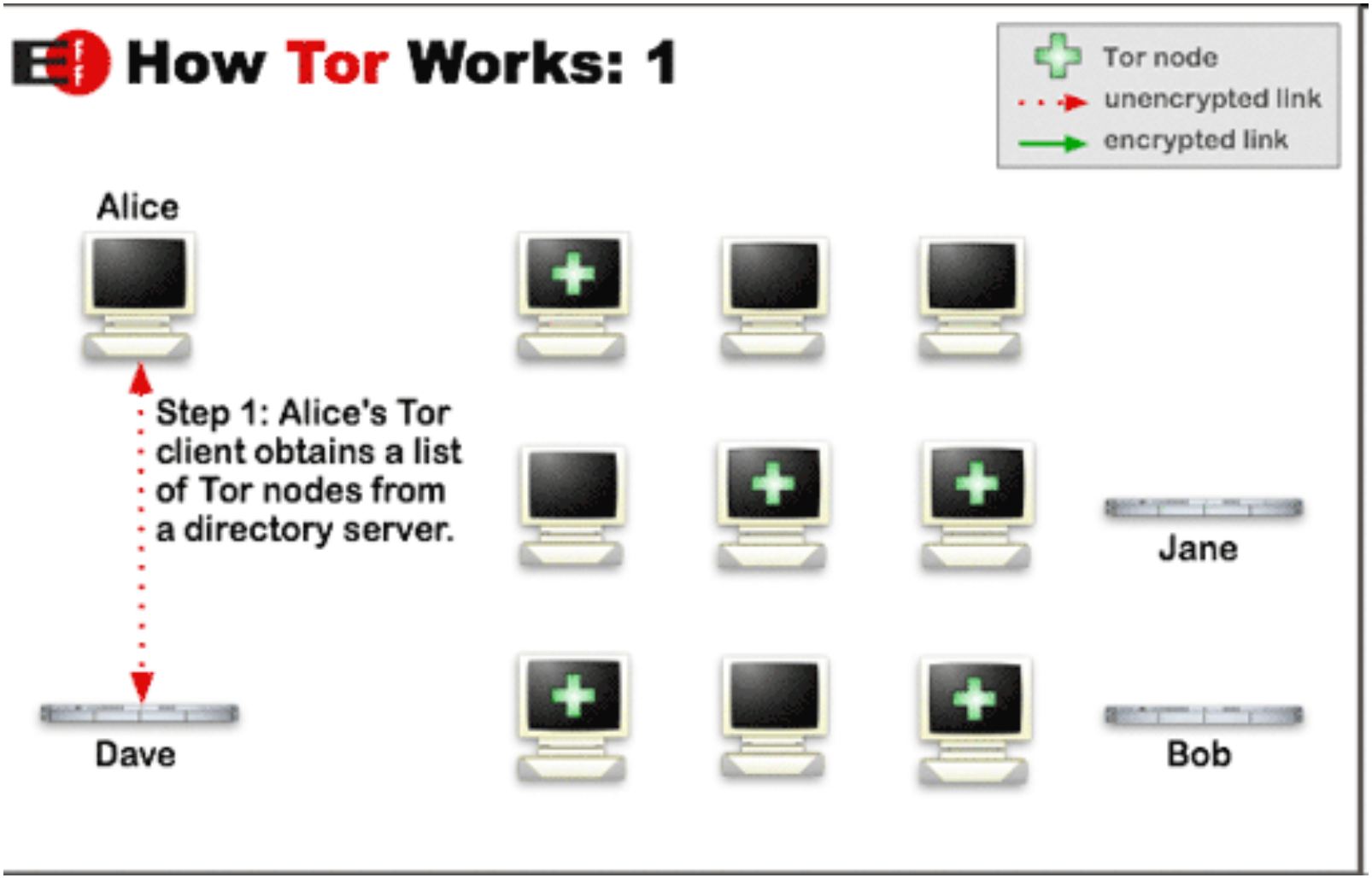
https://www.torproject.org

Components of Tor

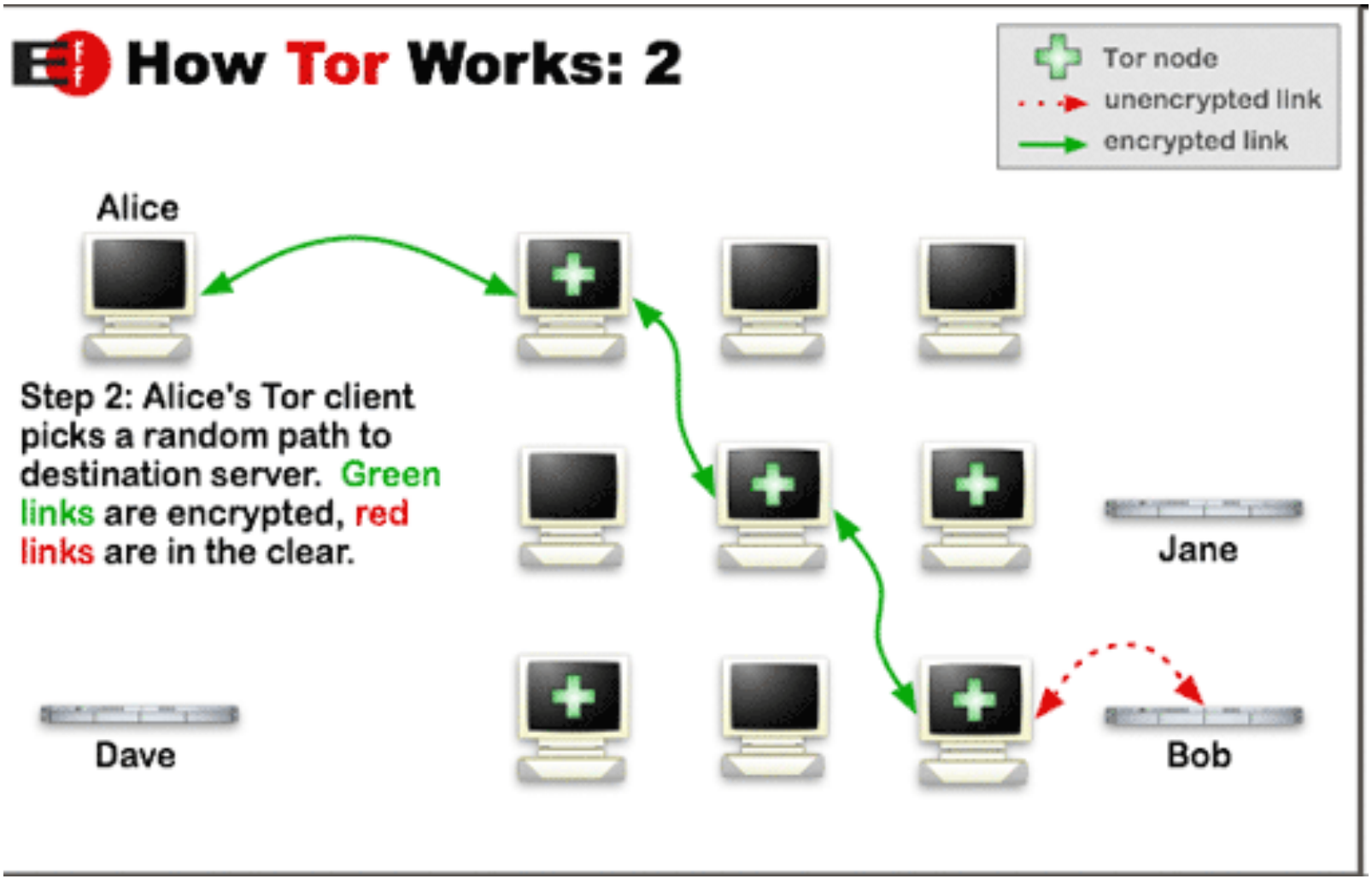


- **Client/OP**: the user of the Tor network, Onion Proxy (OP) fetches directories and creates virtual circuits on the network on behalf of users.
- **Destination Server**: the target TCP applications such as web servers
- **Tor router (Onion Router)**: OR relays the application data
- **Directory server**: Servers holding database of current active ORs

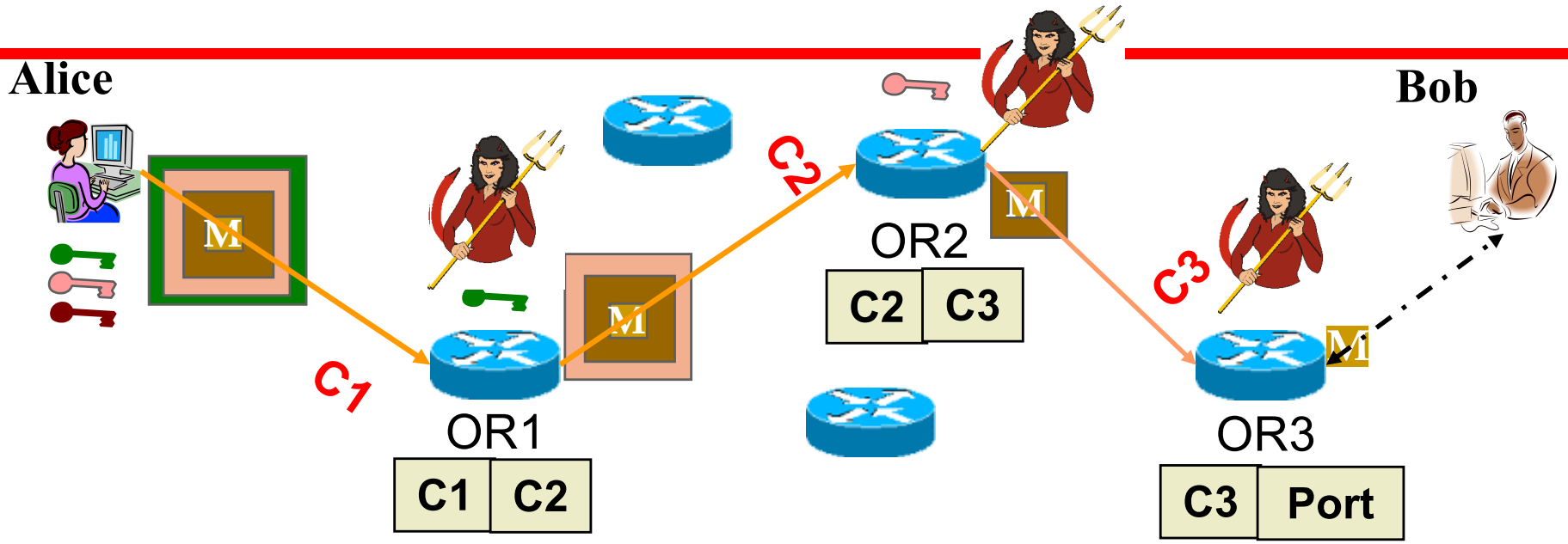
How does Tor work?



How does Tor work?

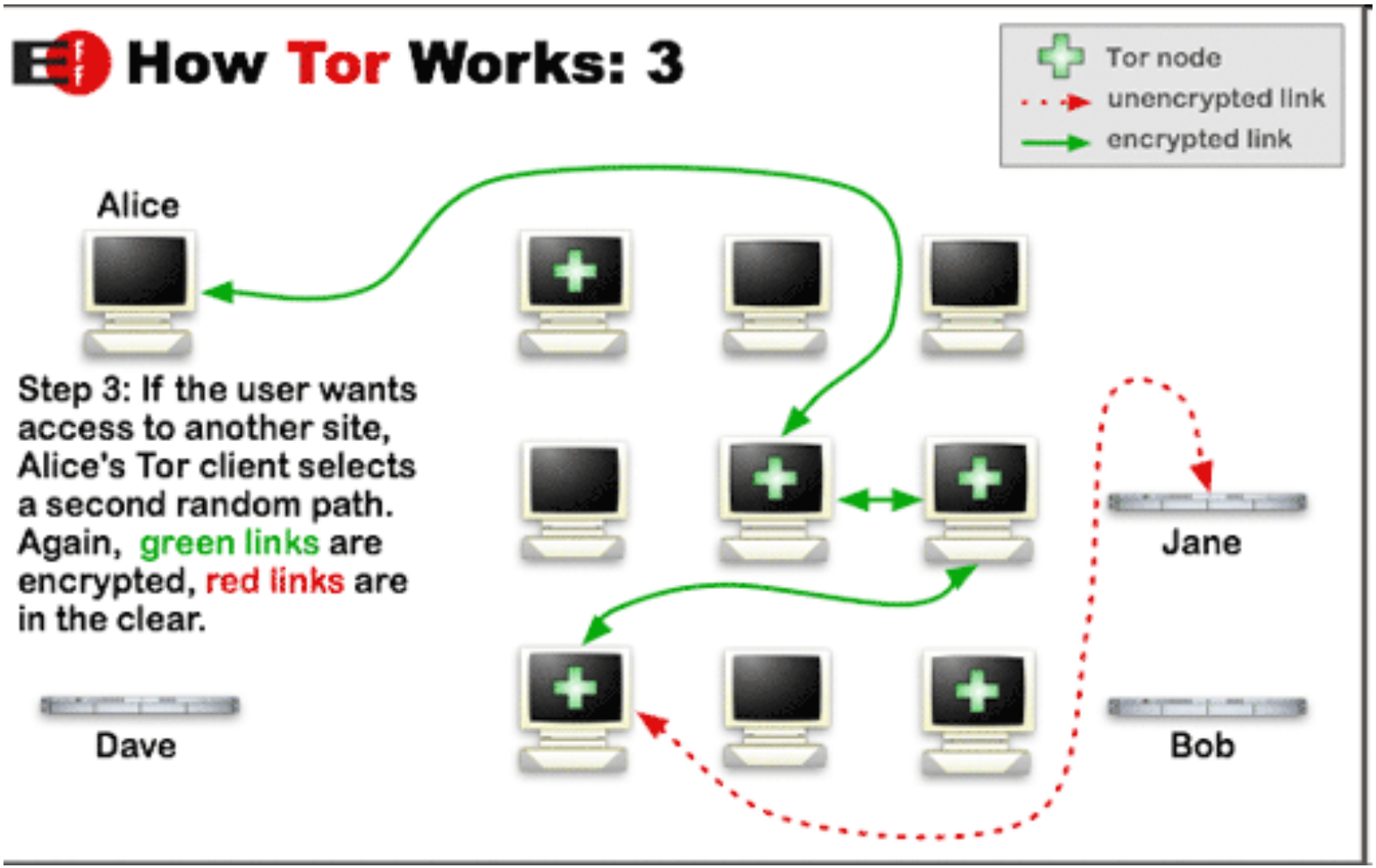


How Tor Works? --- Onion Routing



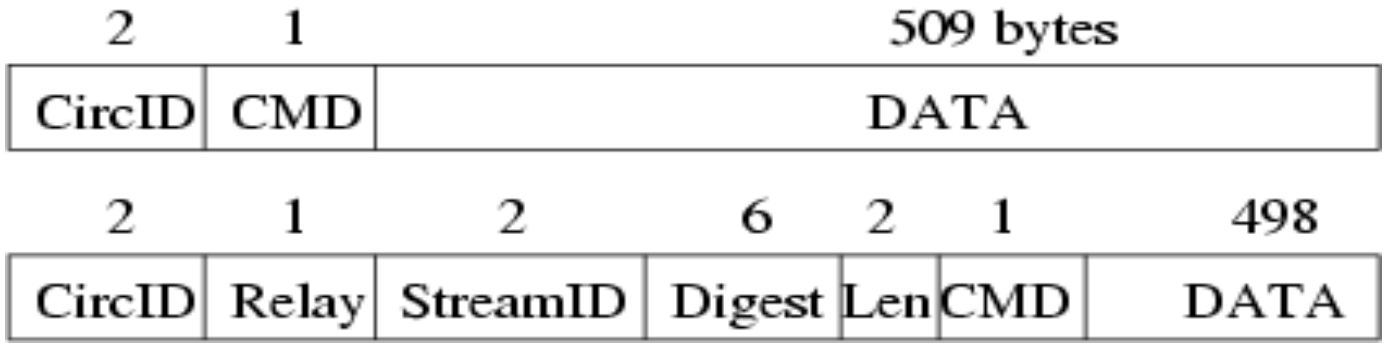
- A circuit is built incrementally hop by hop
- Onion-like encryption
  - Alice negotiates an AES key with each router
  - Messages are divided into equal sized cells
  - Each router knows only its predecessor and successor
  - Only the Exit router (OR3) can see the message, however it does not know where the message is from

How does Tor work?

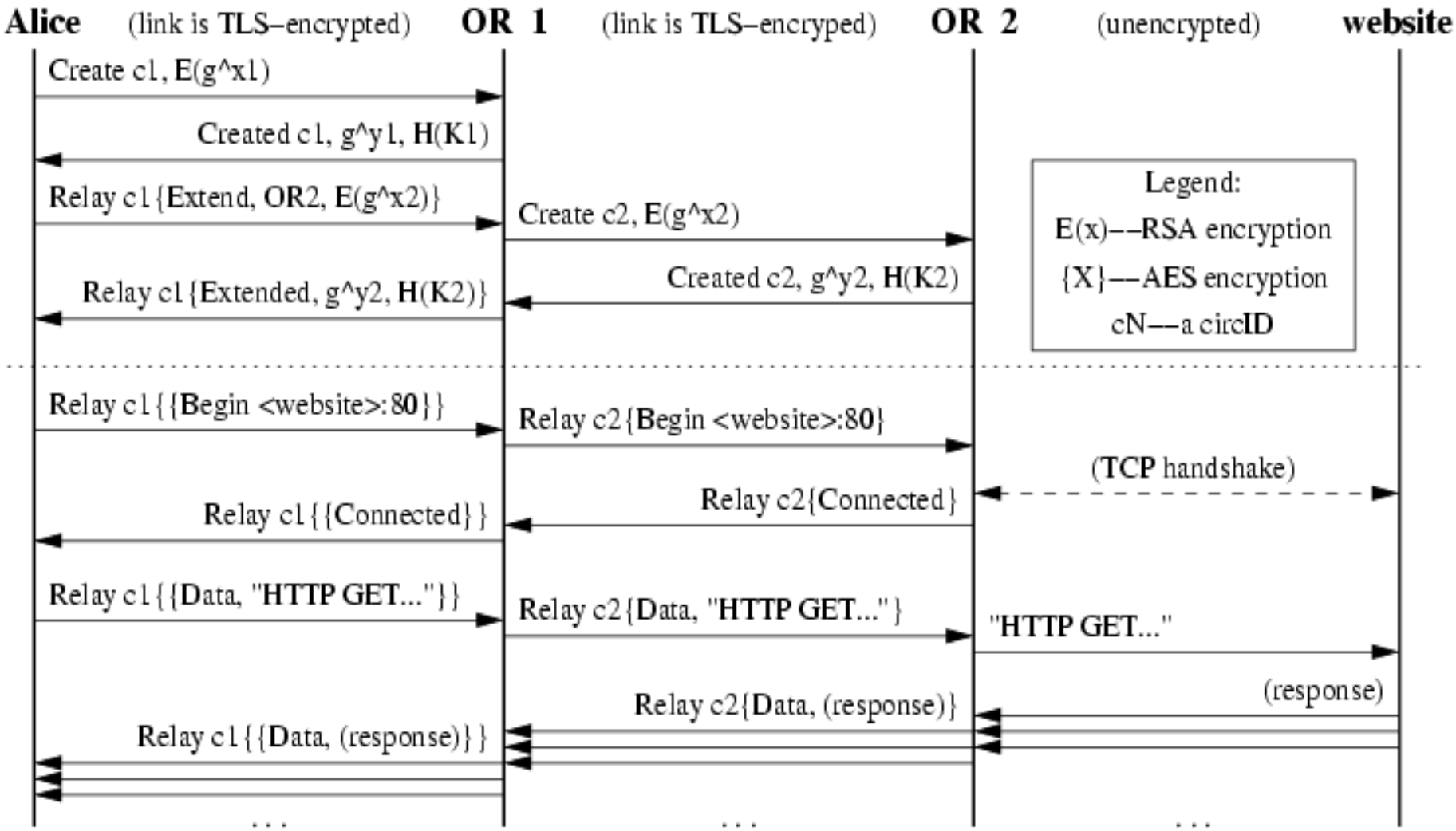


Cells

- All data is sent in fixed size (bytes) cells
  - Similar to cells in ATM
- Control cell commands:
  - Padding, create, destroy
- Relay cell commands:
  - Begin, data, connected, teardown, ...



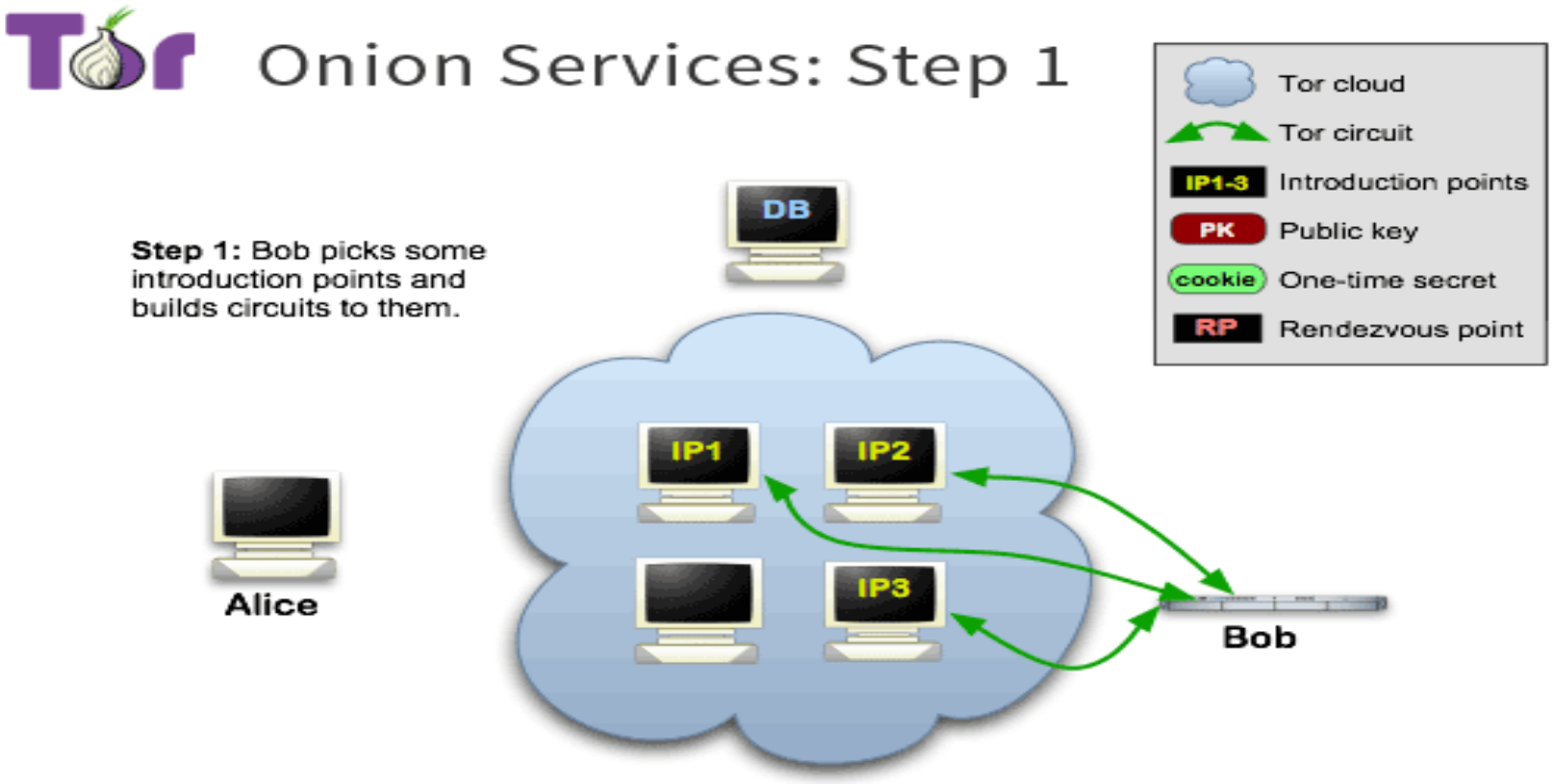
Commands in Use



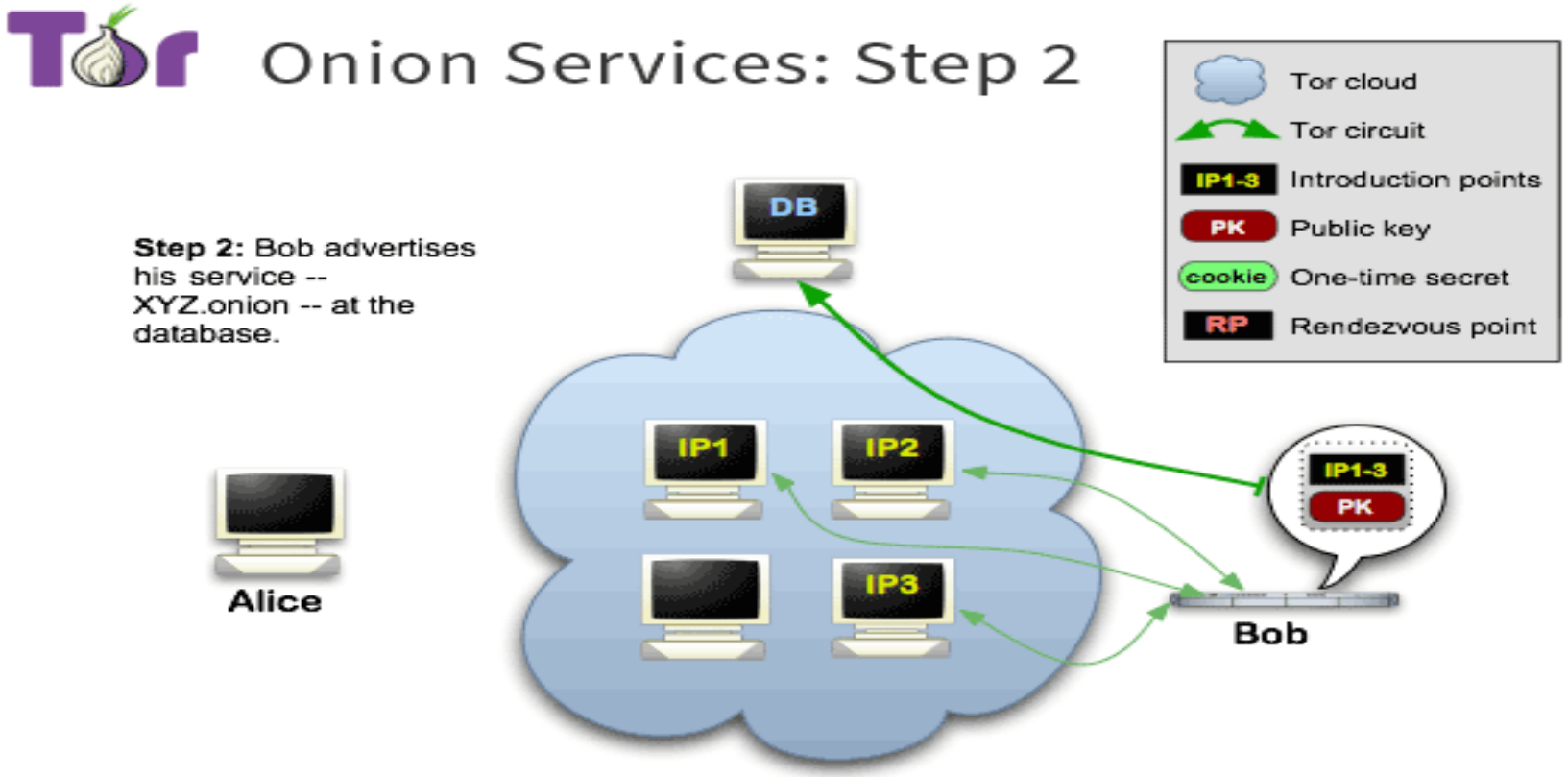
Hidden Service (HS or Onion Service)

- Tor accommodates receiver anonymity by allowing location hidden services
  - Bob can offer anonymous TCP services
- Design goals for location hidden services
  - Access Control:
    - Filtering incoming requests
    - Protection against DDoS attacks
  - Robustness:
    - Maintain a long-term pseudonymous identity
    - Can switch ORs
- facebookcorewwwi.onion
- Dns4torpnlfs2ifuz2s2yf3fc7rdmsbhm6rw75euj35pac6ap25zqqad.onion

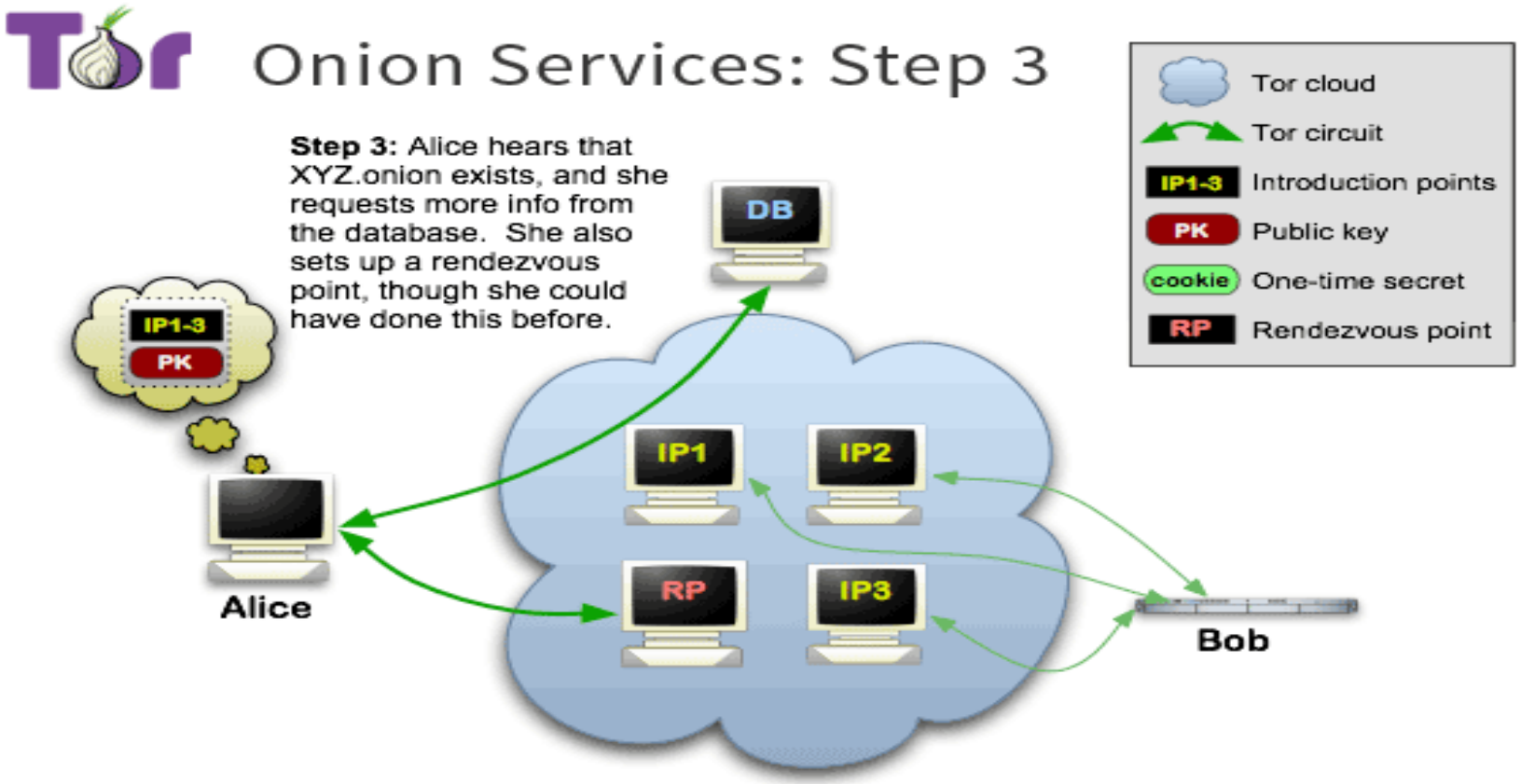
Hidden Services



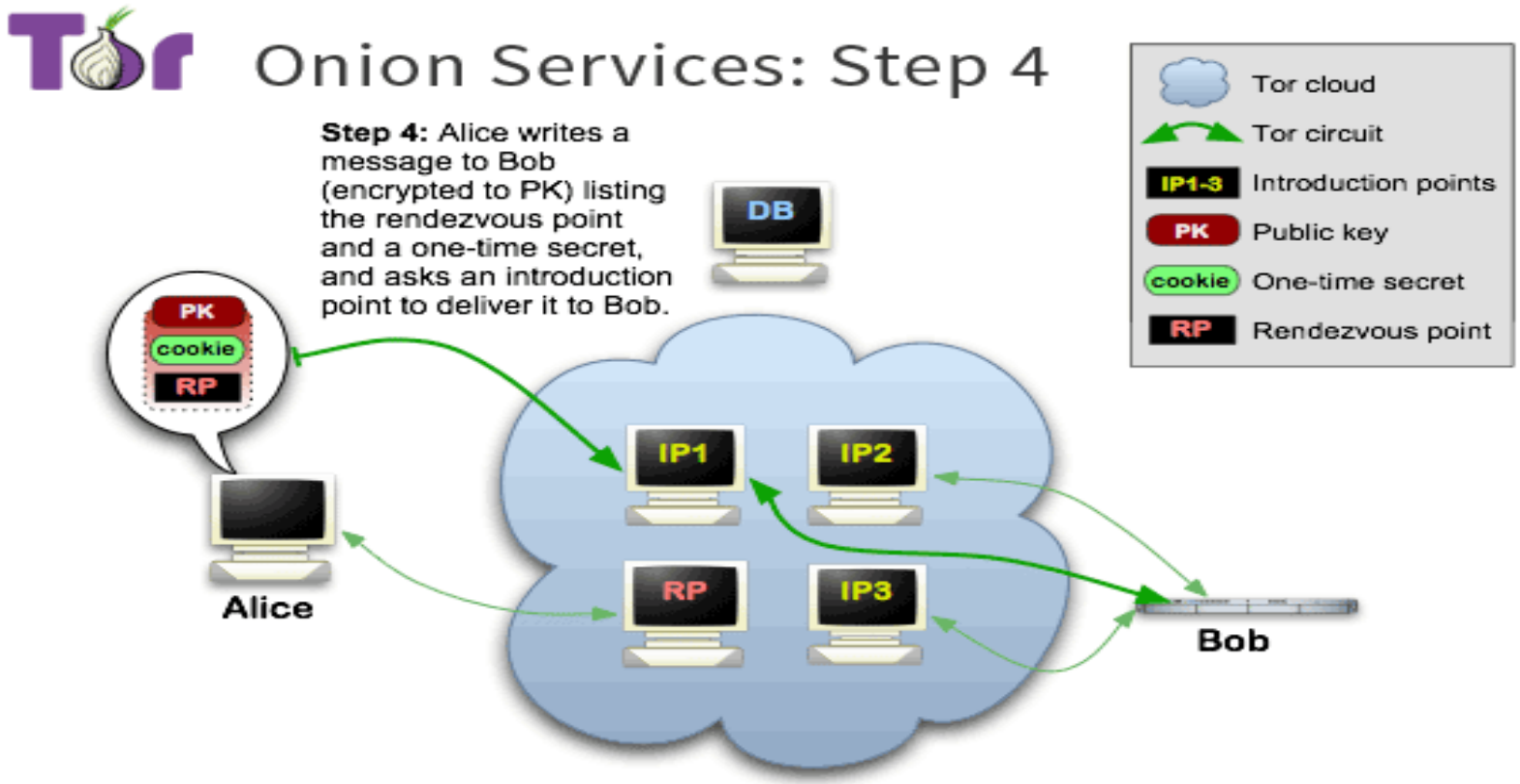
Hidden Services



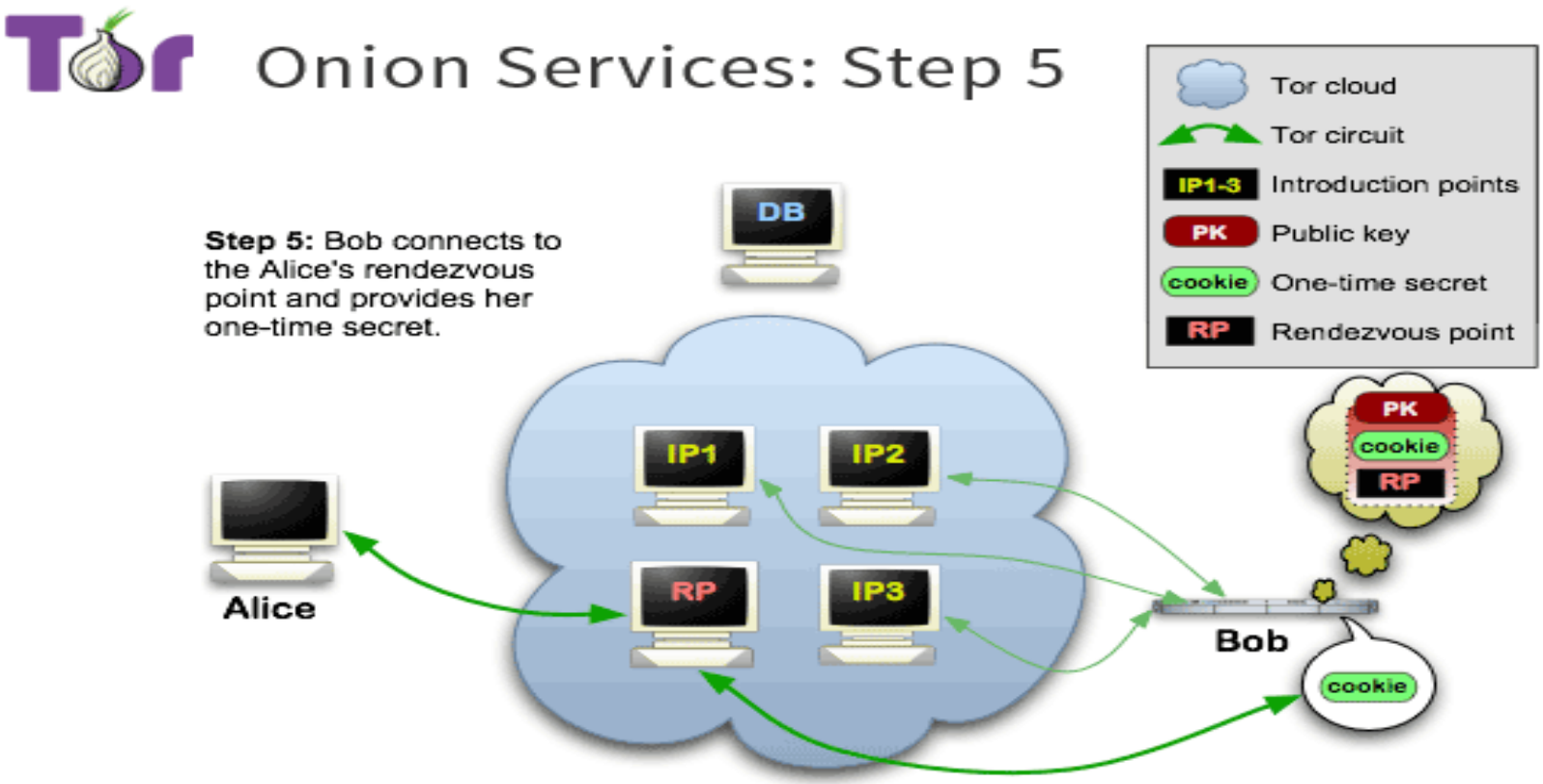
Hidden Services



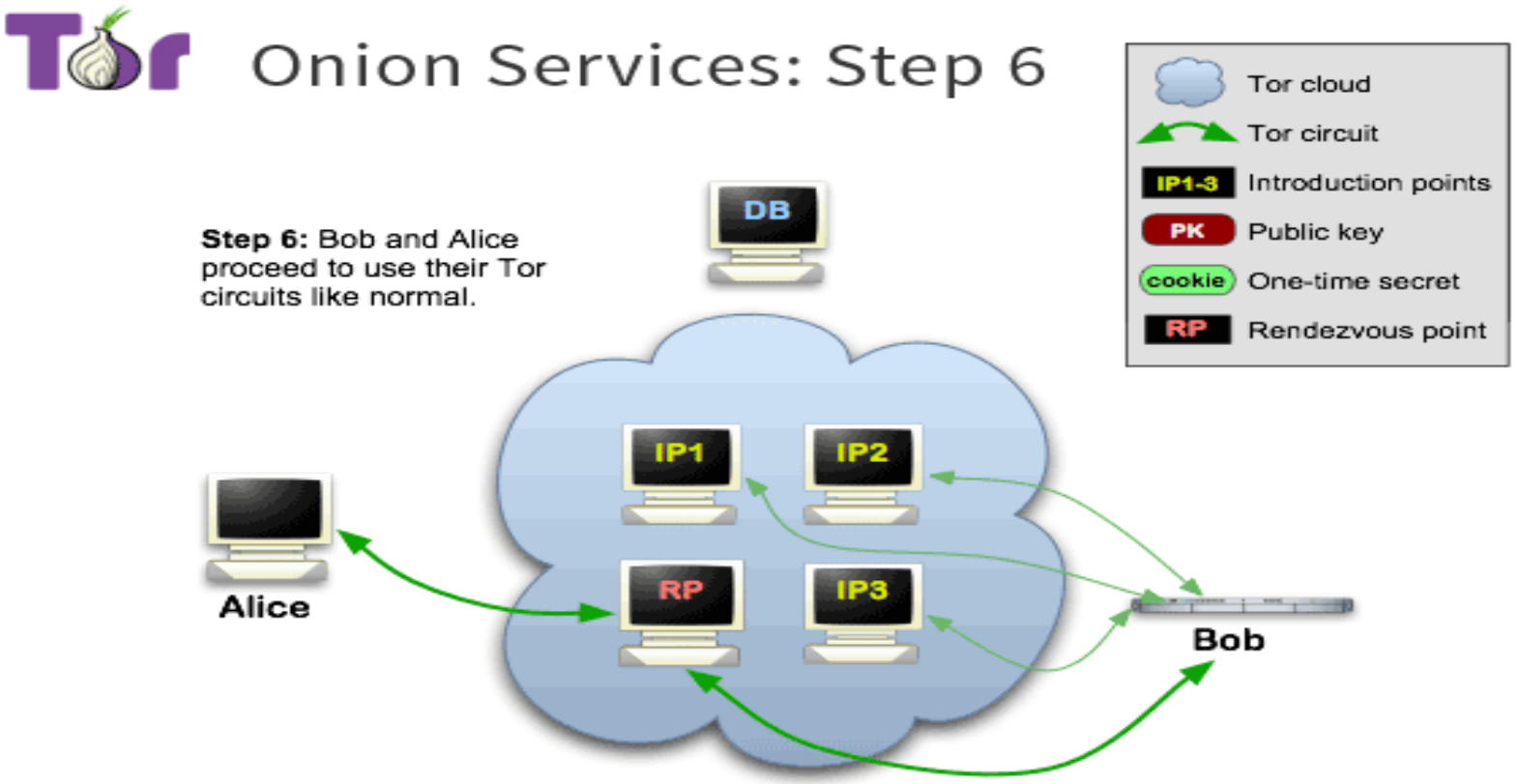
Hidden Services



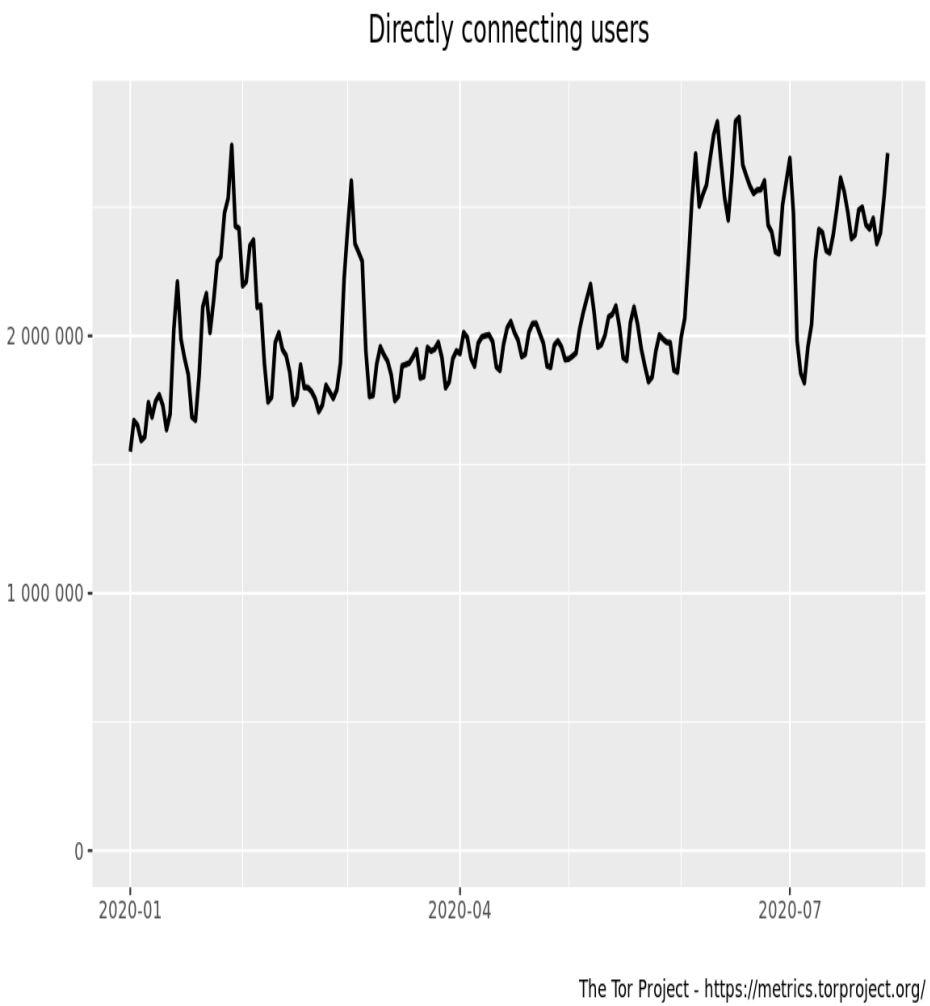
Hidden Services

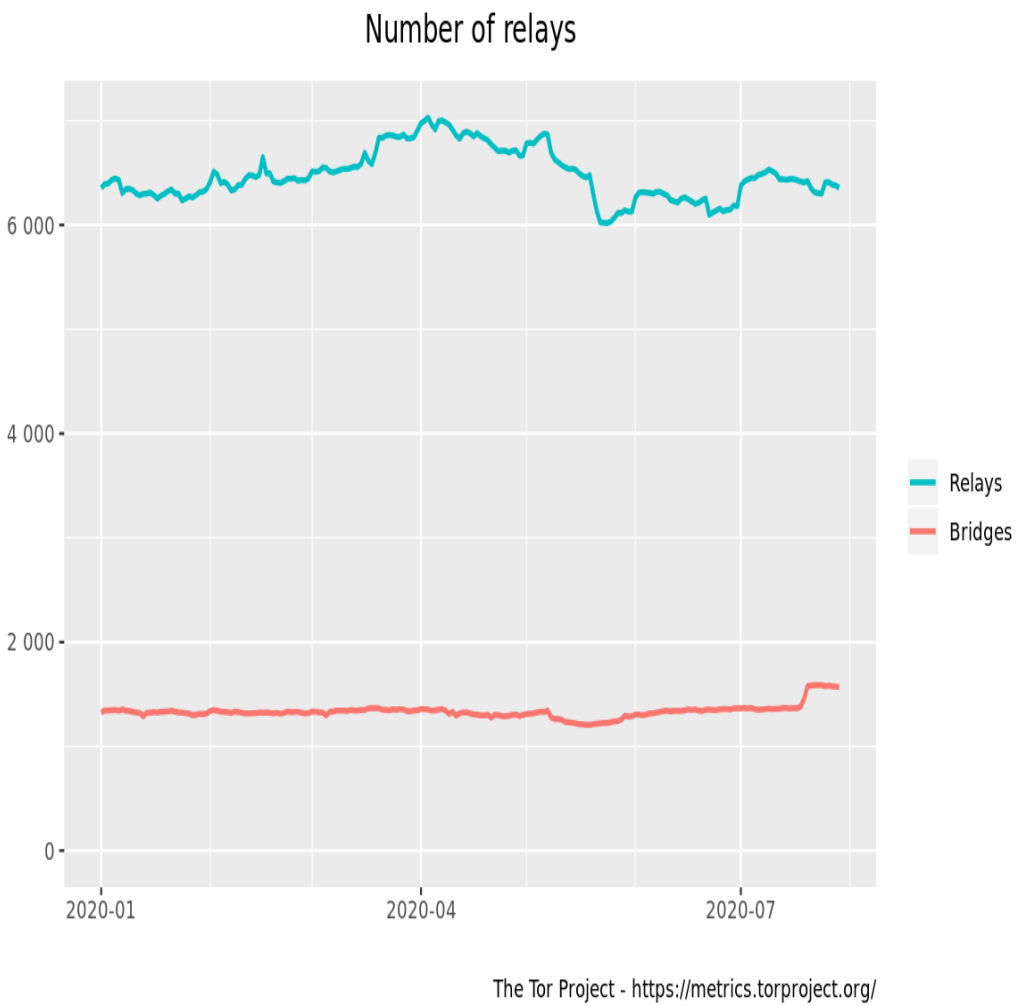


Hidden Services



Some current stats





One more thing …

"A hard-to-use system has fewer users — and because anonymity systems hide users among users, a system with fewer users provides less anonymity. Usability is thus not only a convenience: it is a security requirement"

-Tor Design Document

Questions about Tor?

Problems with ToR?

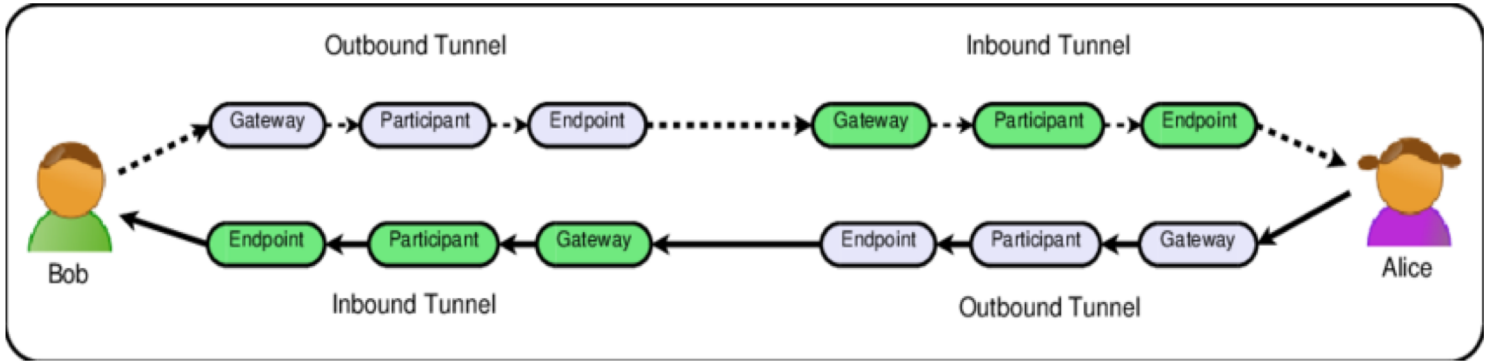
- Entry and Exit OR
  - Most users avoid running Exit OR
- Asymmetric
  - About 8000 OR and millions of users/OP
- Highly centralized
  - Only 10 DS
- Relay/path selection algorithm
- Circuit based
  - Only supports TCP

I2P: The Invisible Internet Project

- An anonymizing message oriented P2P network
- No entry and exit nodes
  - All nodes are Routers
  - Currently around 50,000 nodes
- Utilizes fully decentralized structure (no DS)
- Protects the identity of both the sender and receiver
- Supports multiple applications
- UDP based (unlike Tor's TCP streams)
- Out-proxies used for normal Internet for web browsing

http://www.i2p2.de/en/

I2P Tunnels

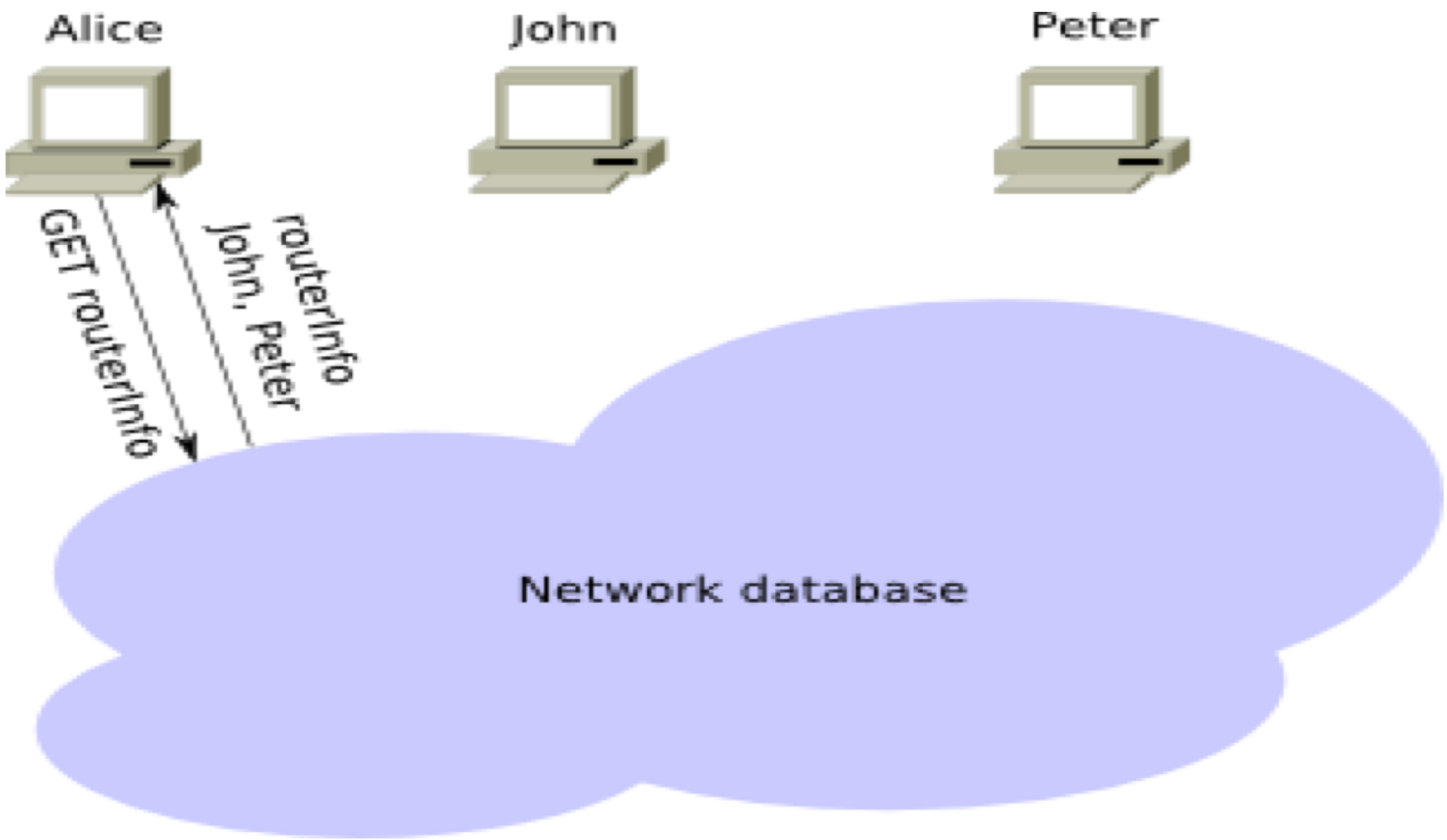


- An application in I2P is not reachable by IP but through a location independent identifier
- Message routed through several intermediate devices using layered encryption (Garlic routing)
- Sender only knows about the inbound Gateway of the receiver
- Tunnels are maintained for 10 minutes only

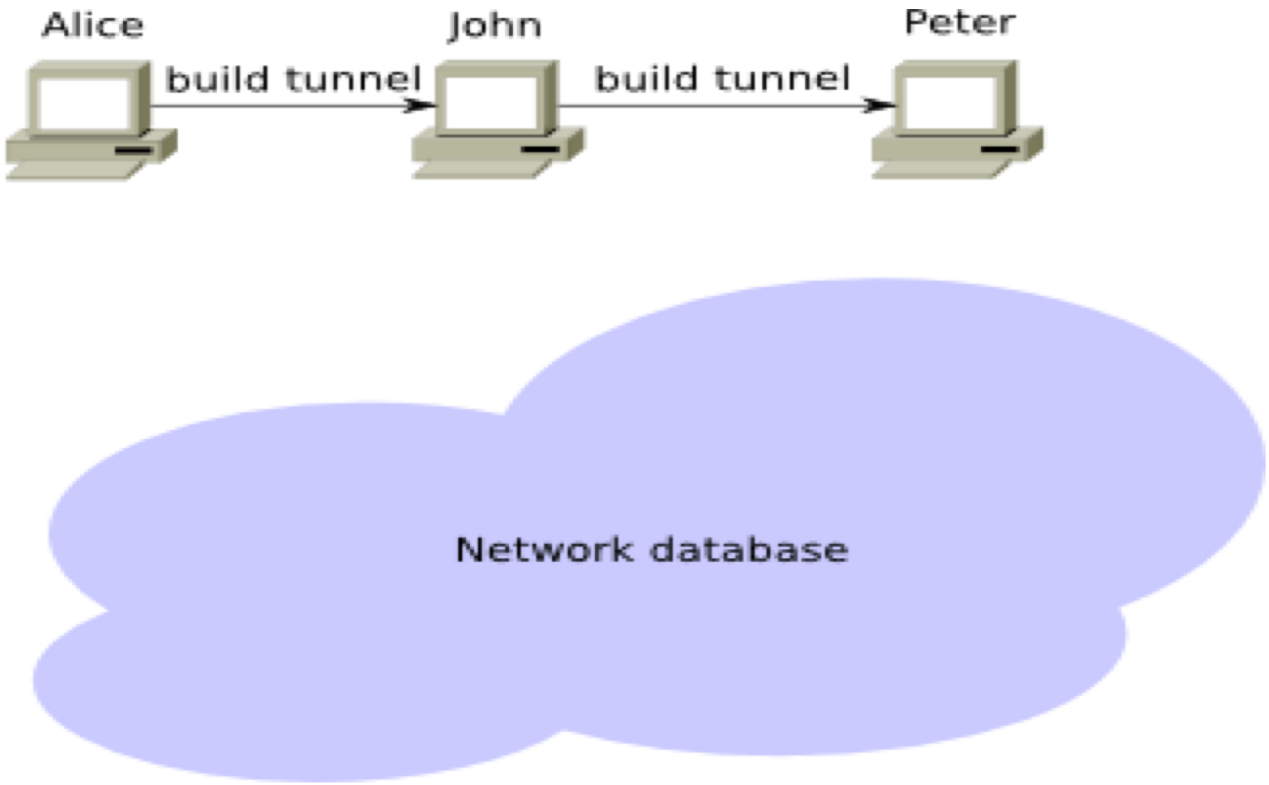
NetDB

- A network database based on DHT hosted at *Floodfill* routers (about 20,000)
- This contains both “routerInfo” and “leaseSets”
- rotuerInfo – stores information on specific I2P routers and how to contact them
- leaseSets – stores information on a specific destinations (i.e. I2P websites, email servers, etc.)

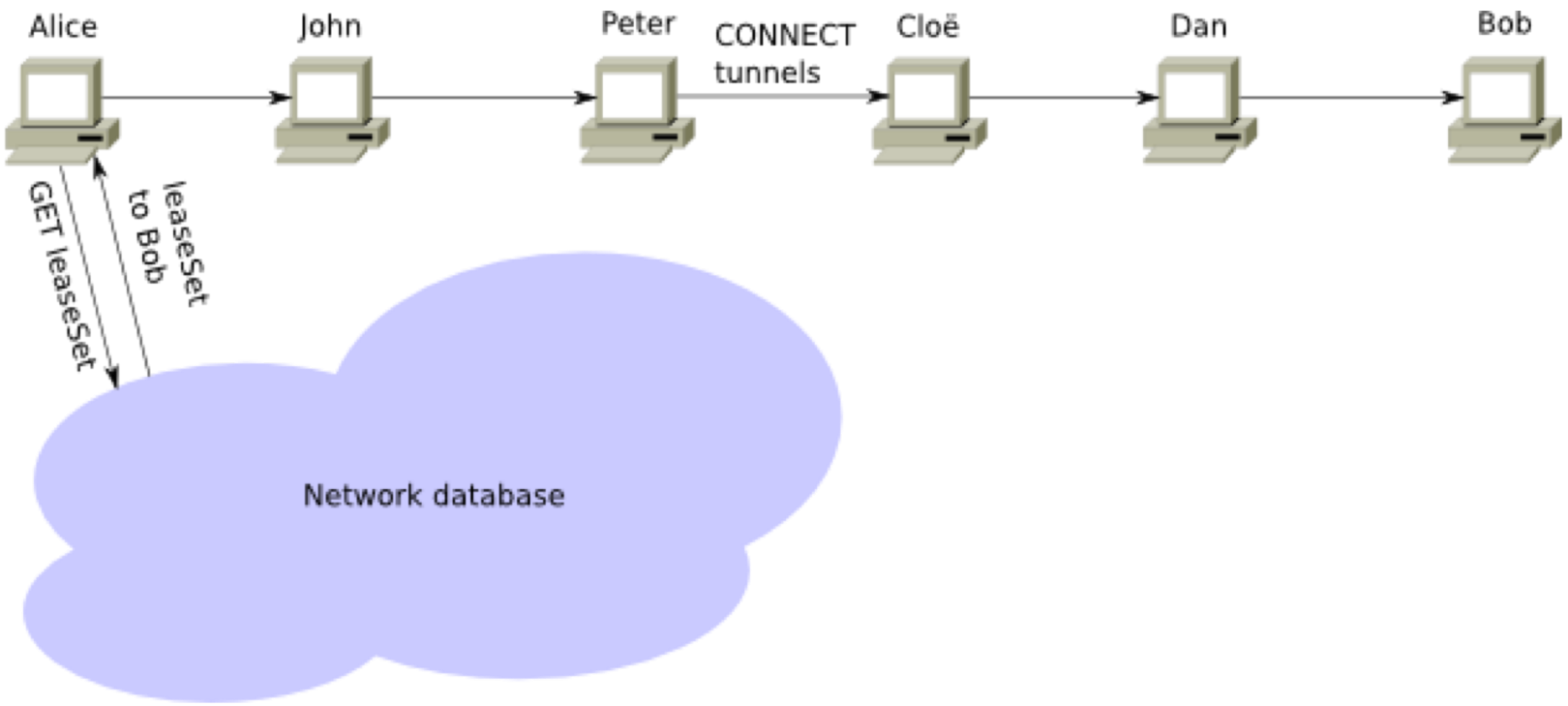
Joining the Network



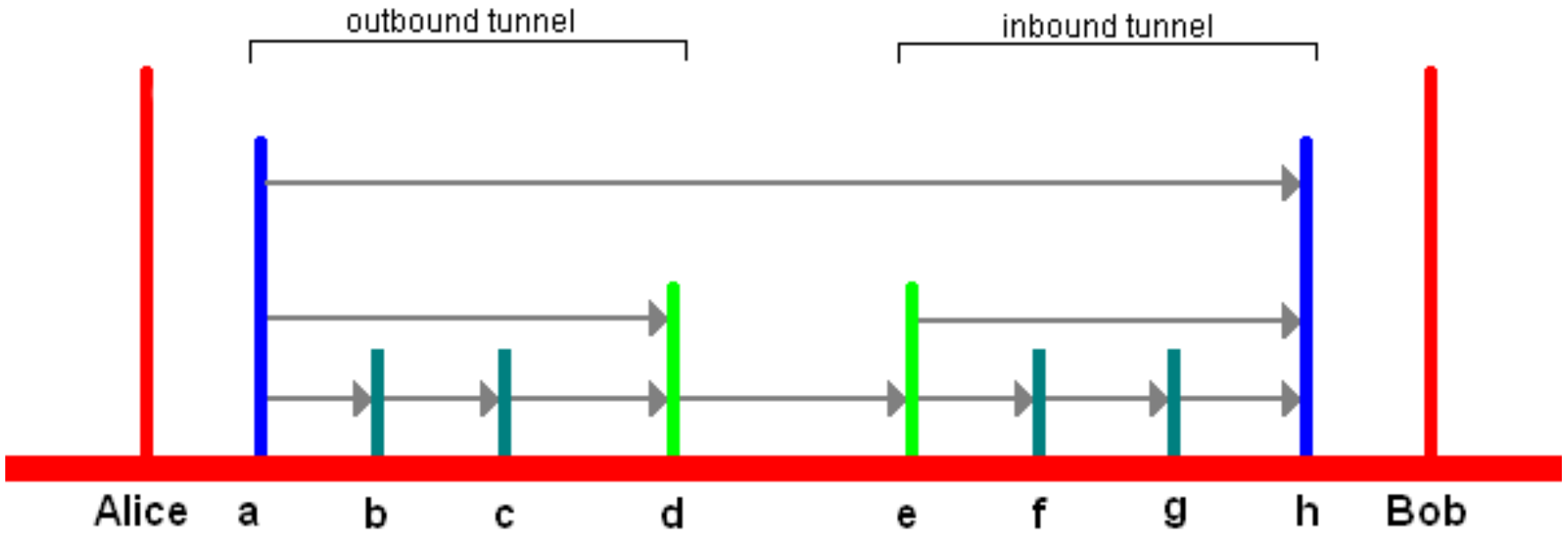
Establishing a Tunnel



Establishing a Connection



Encryption View

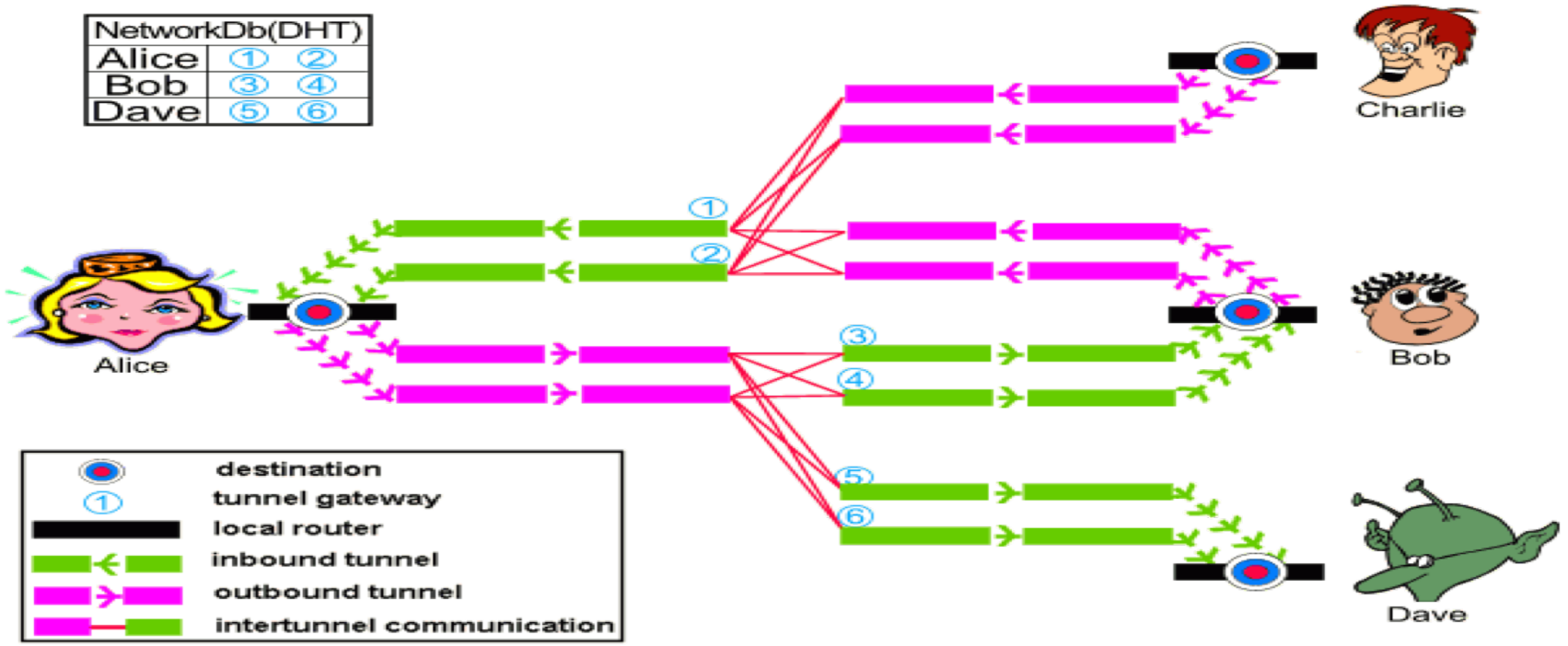


		tunnel encryption (private key AES)	a to d, e to h
garlic encryption (ElGamal/SessionTag+AES)	a to h	transport encryption (DH/STS+AES, etc)	a to b, b to c, c to d, d to e, e to f, f to g, g to h

http://www.i2p2.de/en/docs/how/intro

I2P Tunnels and Garlic routing

- Message routed through several intermediate devices using layered encryption (Garlic routing)



Comparison: Tor vs. I2P

- TCP vs. UDP
- Directory Server vs. NetDB (P2P)
- Separation of Nodes and Clients vs. Everyone routes traffic
- Exit Nodes vs. Outproxies
- Circuits vs. Tunnels

Questions?