Peeling Onions

Understanding and using the Tor network

hiro@torproject.org

Know your onions

- What is Tor and what it can do for you.
- How Tor provides privacy and anonymity
- Using Tor at the application layer: the Tor browser.
- Onion services and bidirectional anonymity
- Using Tor within other applications through onion services

Who am I?

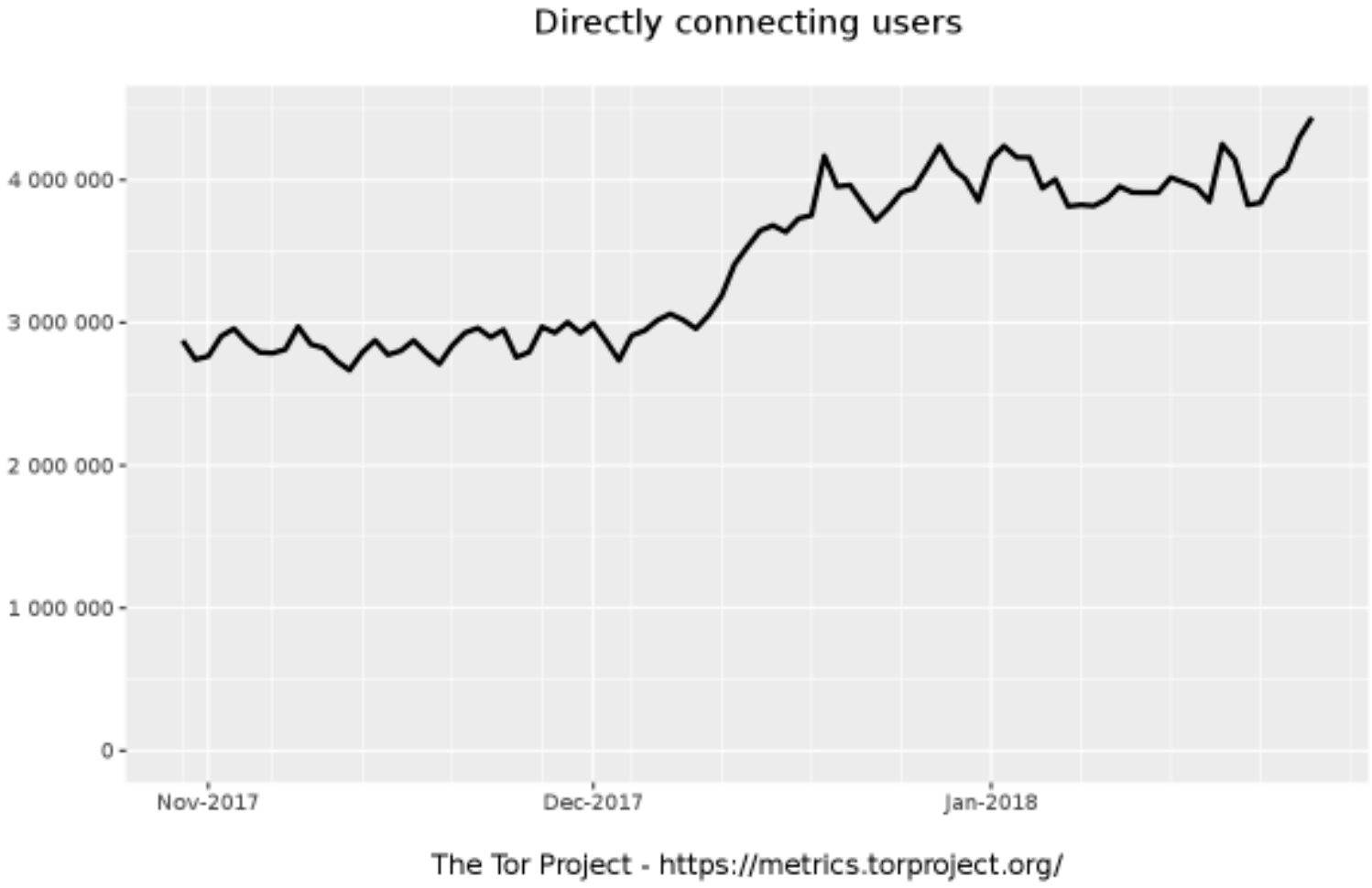
- My name is Silvia Puglisi, some known me as Hiro.
- I work at the Tor Project.
- I am also part of the Information Security Group in the Department of Telematics Engineering at UPC-Barcelona where I got my Ph.D.
- I research topics in the fields of privacy and anonymity of users on the web, in online communities and social networks.

What is Tor and what it can do for you.

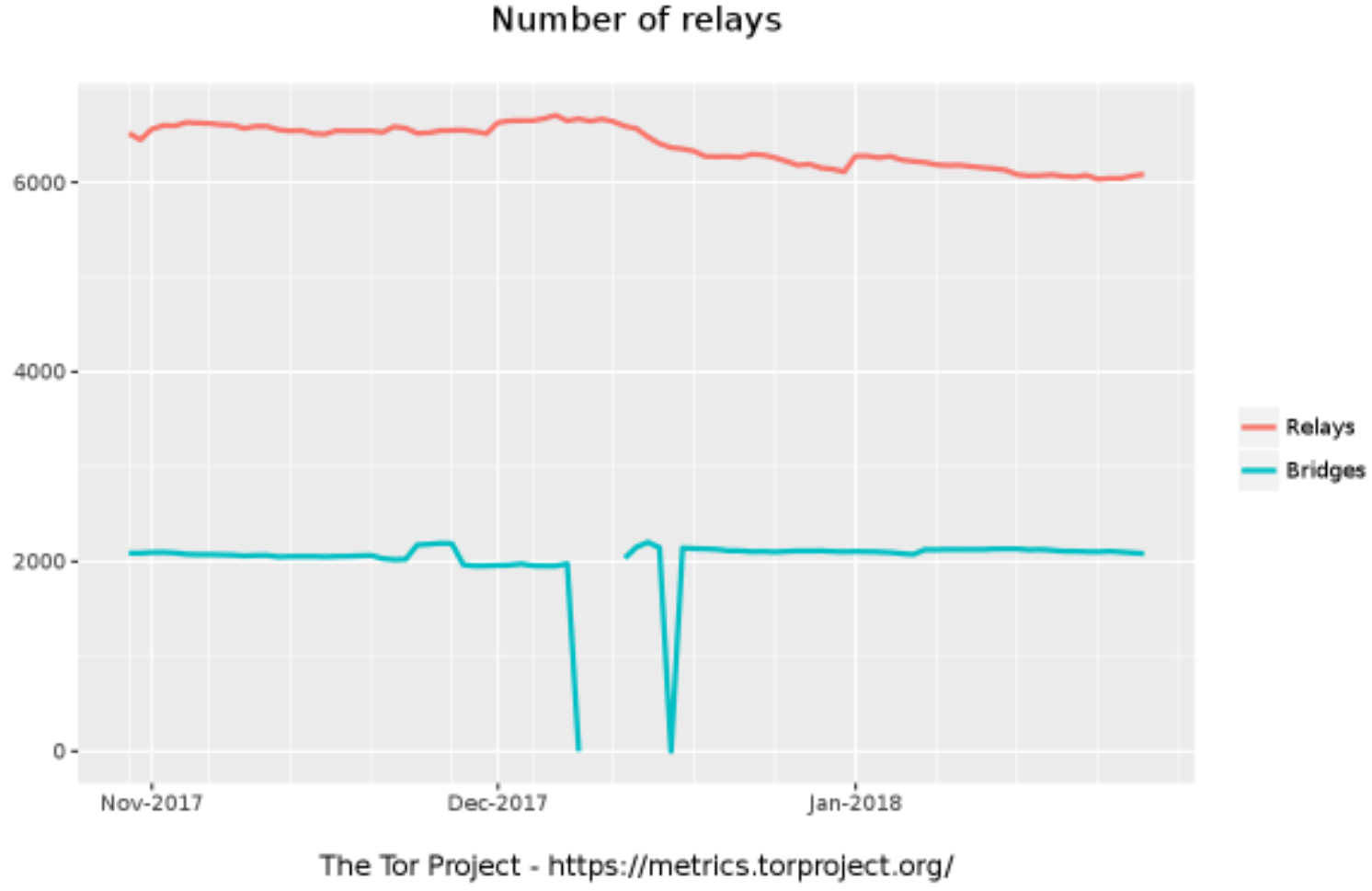
Tor is a privacy tool

- Tor is free software
- Tor is a diverse group of developers, researchers, relay operators, volunteers
- Tor is an open network
- Tor is a non-profit

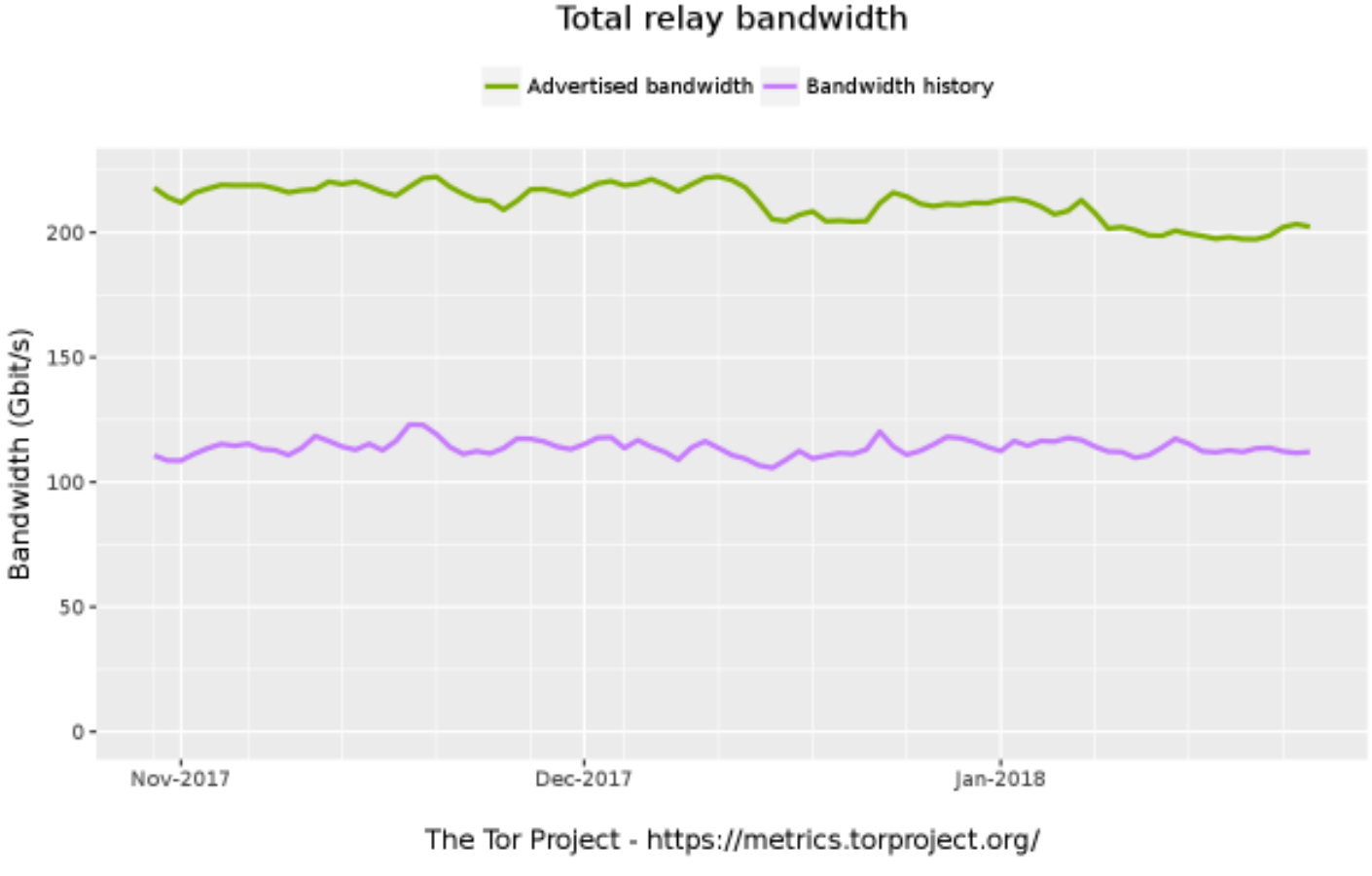
Tor is about 4M daily users using the network!



Tor is about 3K bridges and 7K relays



Tor provides about 200Gbit/s bandwidth



This graph shows the total advertised and consumed bandwidth of all relays in the network.

What does Tor do?

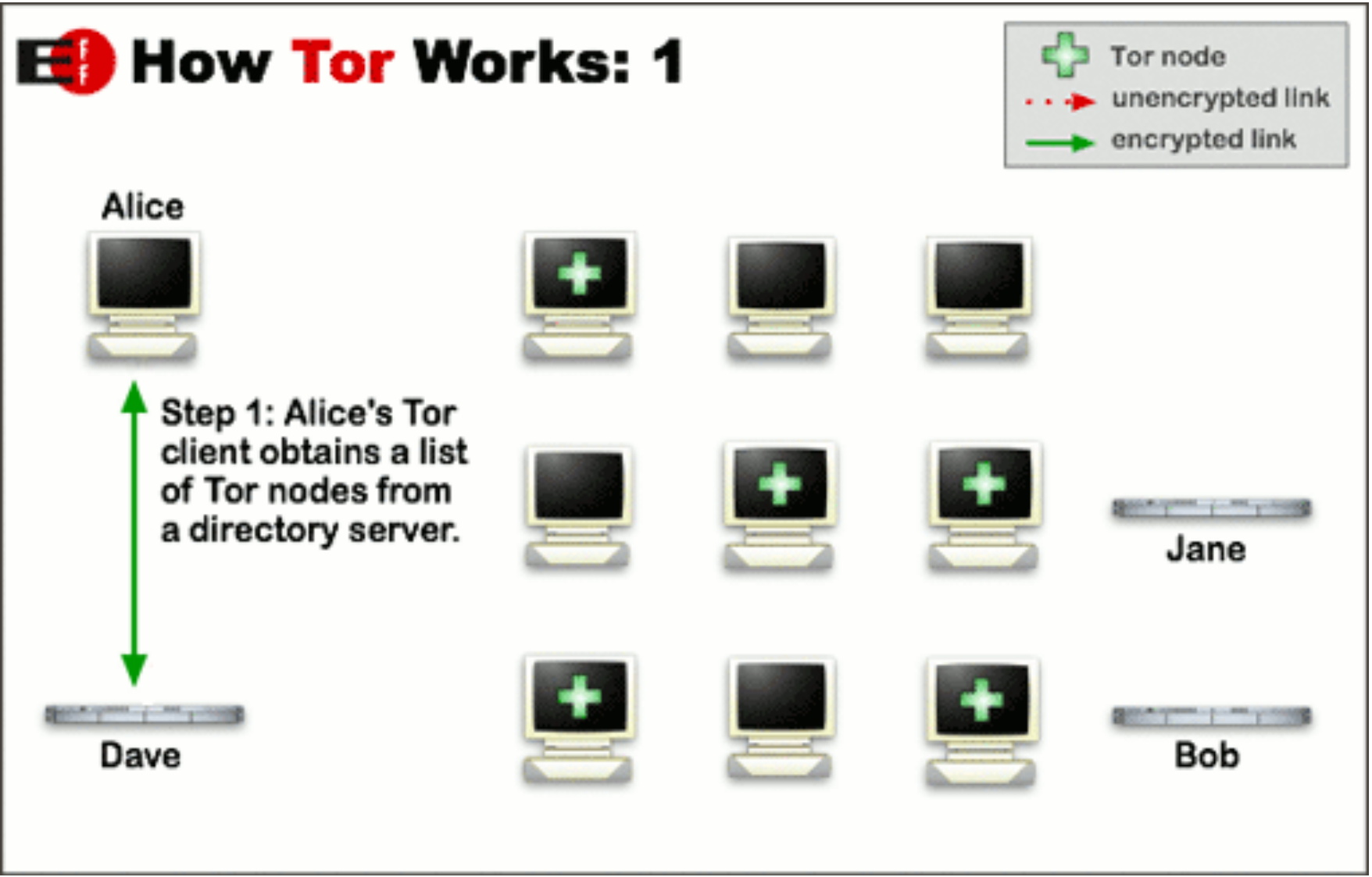
- Tor provides privacy
- Tor provides anonymity
- Tor provides communication security
- Tor provides a traffic analysis resistant communication network
- Tor provides reachability against censorship

How does Tor provides Privacy and Anonymity?

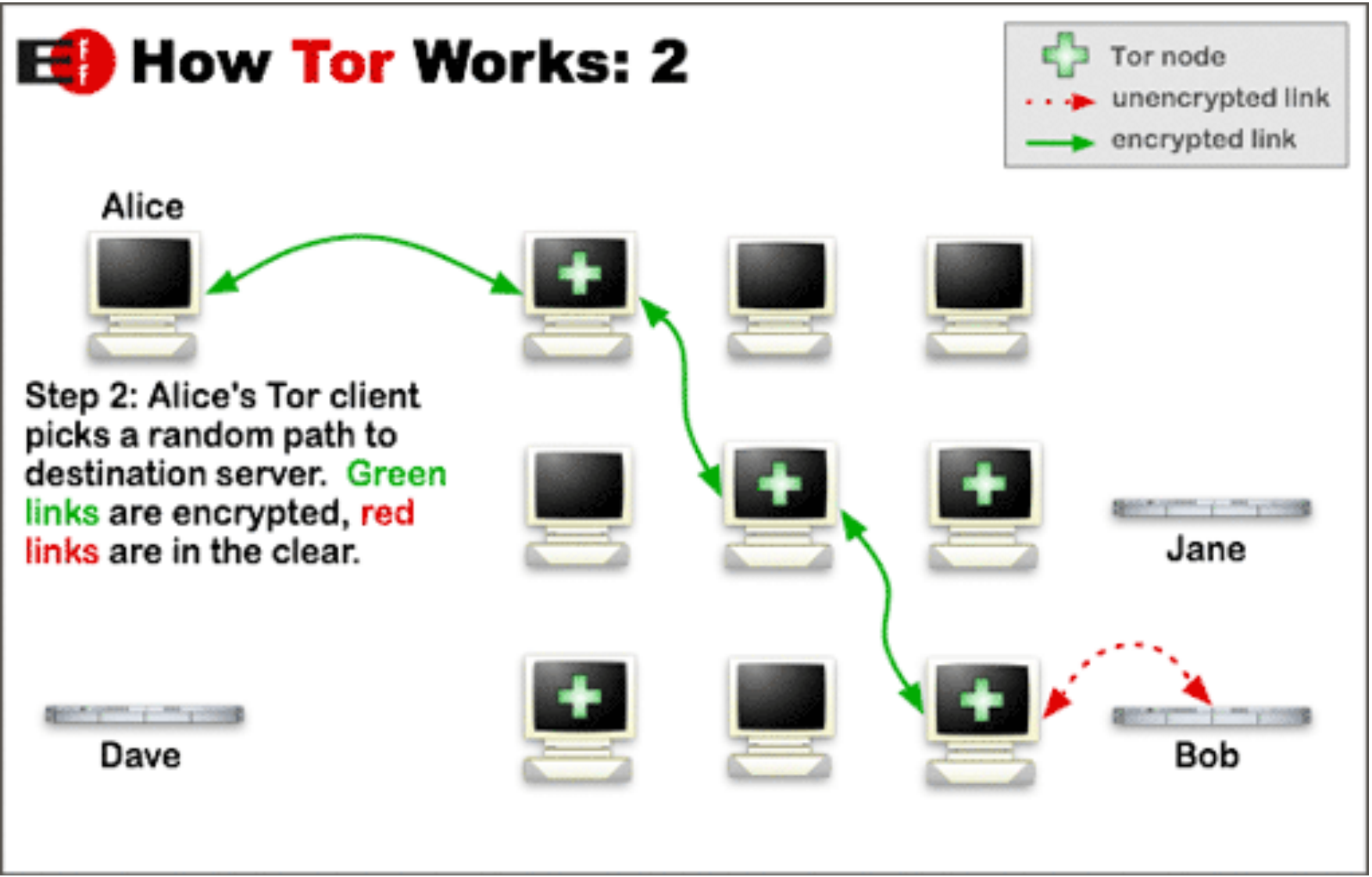
Privacy by design

Tor provides privacy by distributing **TRUST**

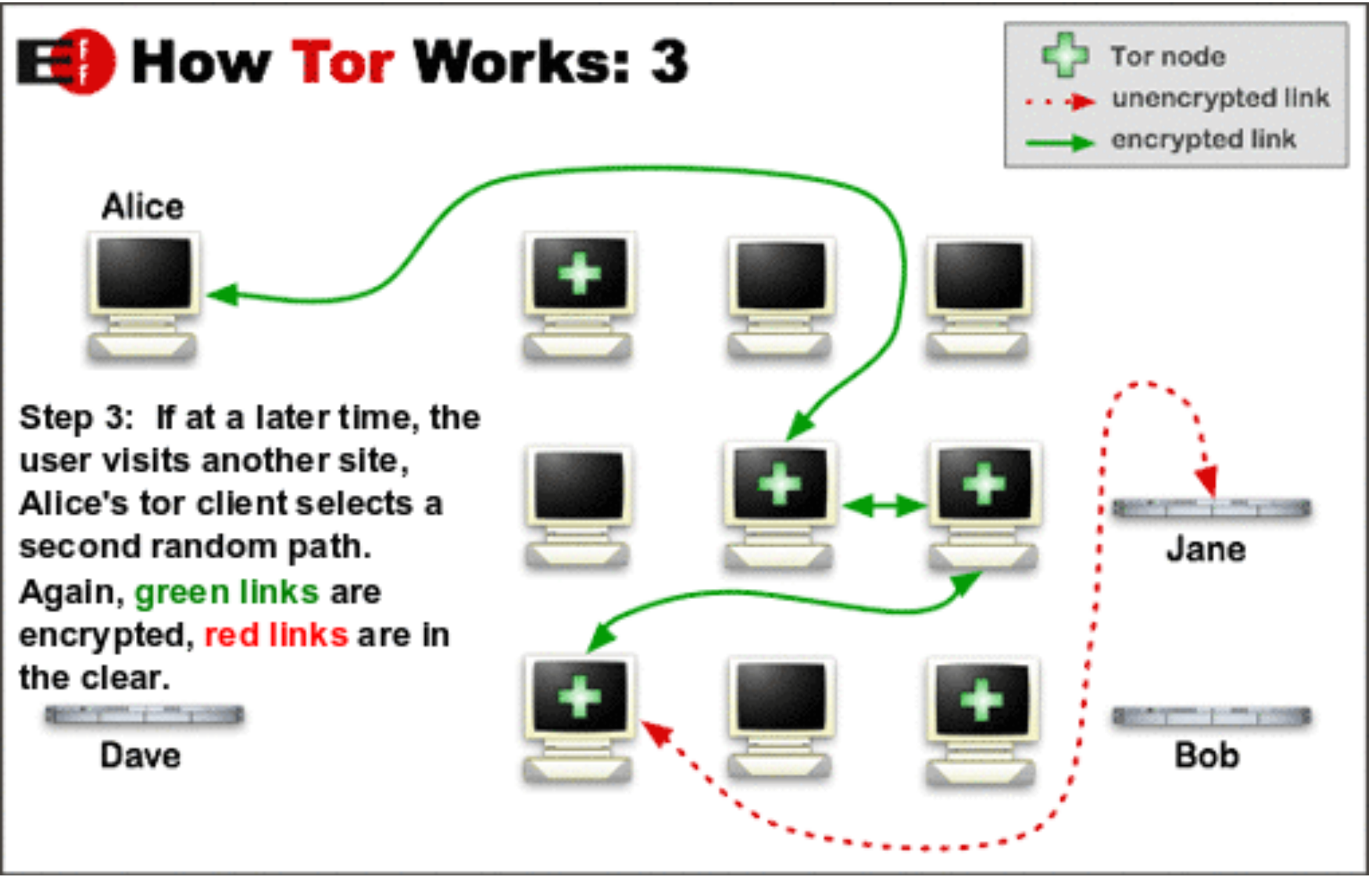
How Tor works



How Tor works



How Tor works



Anonymity > Encryption

- Encryption doesn't hide conversations metadata
- Encryption doesn't hide your social graph
- Encryption doesn't hide network metadata
- Encryption doesn't hide your location

Using Tor at the app layer:

The Tor Browser

What is the Tor Browser

The Tor Browser is a modified Firefox ESR packaging Tor, Torbutton, TorLauncher, NoScript, and HTTPS-Everywhere.

Why Tor has a browser bundle

- The Tor browser is designed to ensure safe use of Tor
- The Tor browser is designed to reduce linkability of user activities on different websites

Onion Services

Providing bidirectional anonymity

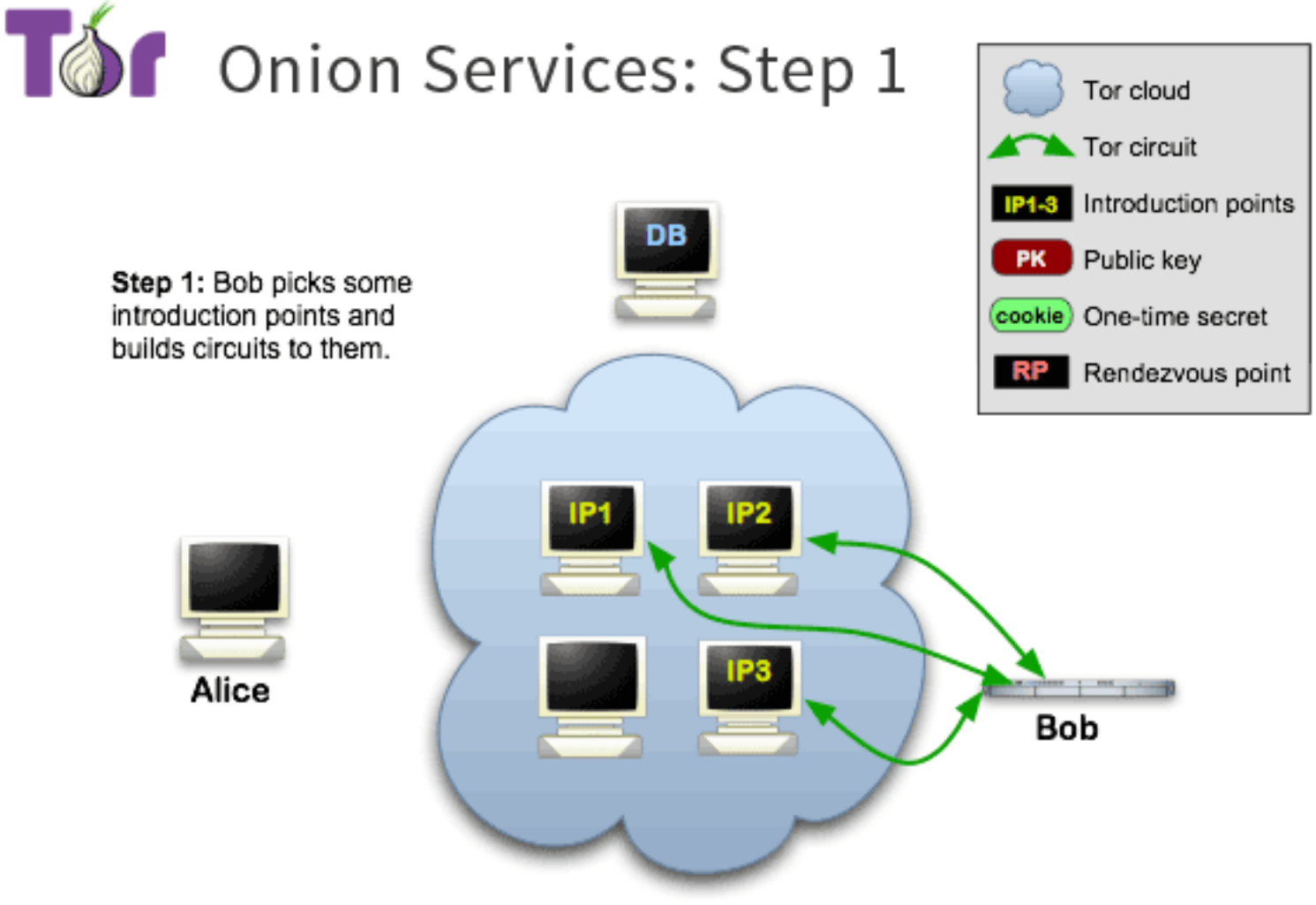
What are onion services?

- Onion services are hidden services
- We also have next gen onion services [more later]
- 16 chars .onion address (base32)
- Both client and server hide their locations (initiator - responder)
- The communicaion stays in the Tor network
- Can be used for all kind of TCP traffic

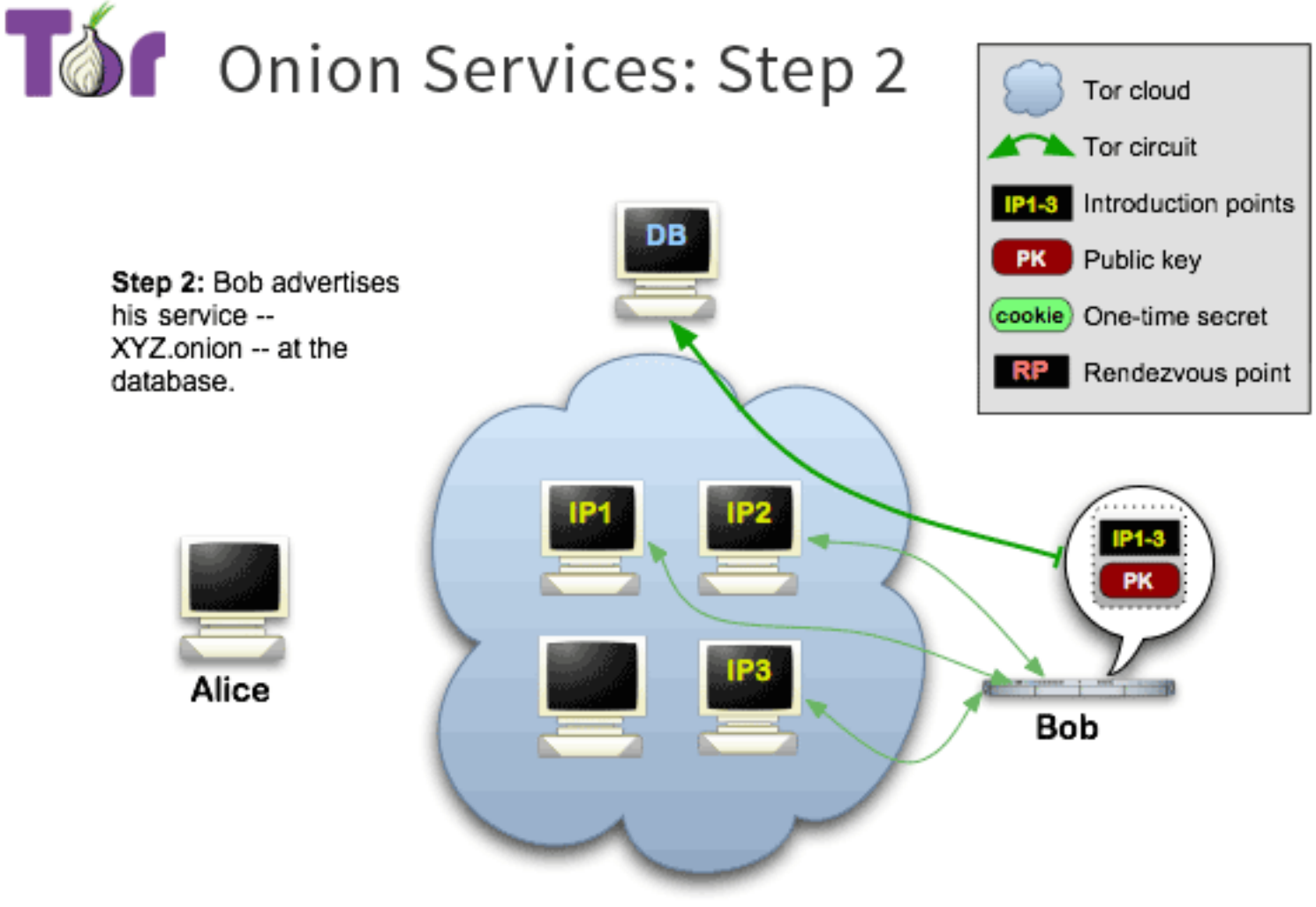
Some interesting properties

- Self authenticated
- End-to-End encrypted
- Isolation and NAT punching
- Limit attack surface
- Censorship resistance
  - No DNS or BGP hijacking/poisoning ...

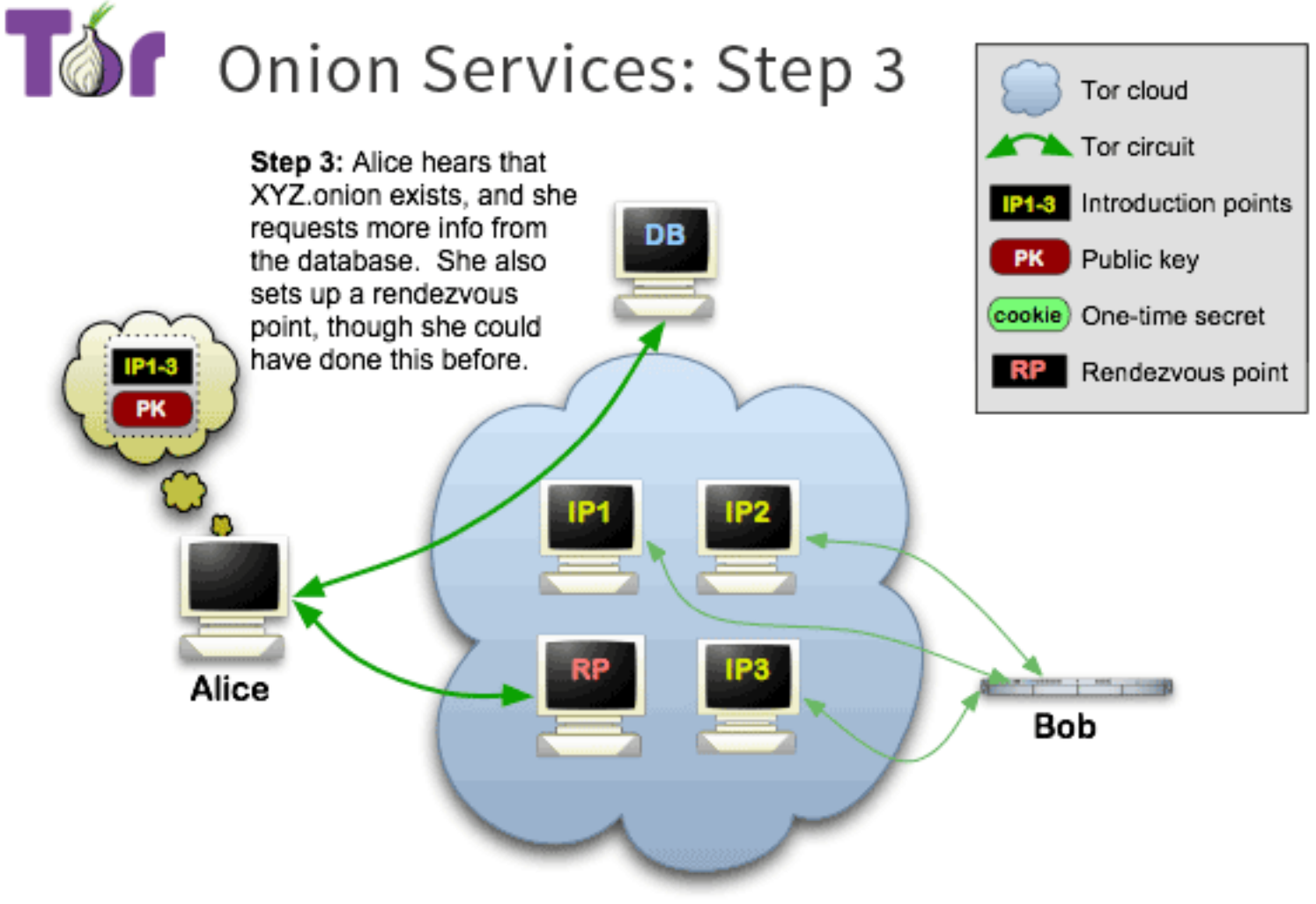
How Onion Services work



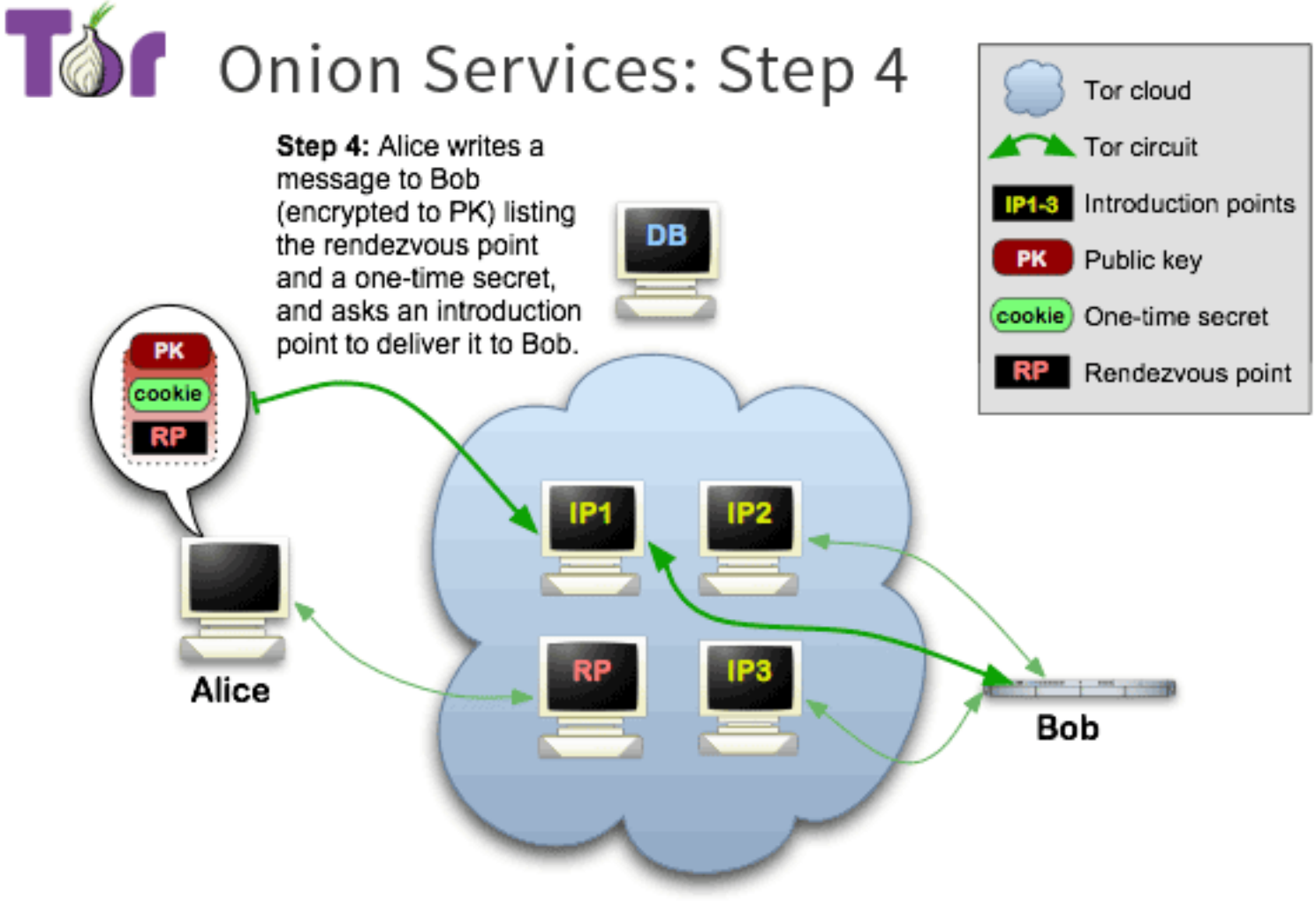
How Onion Services work



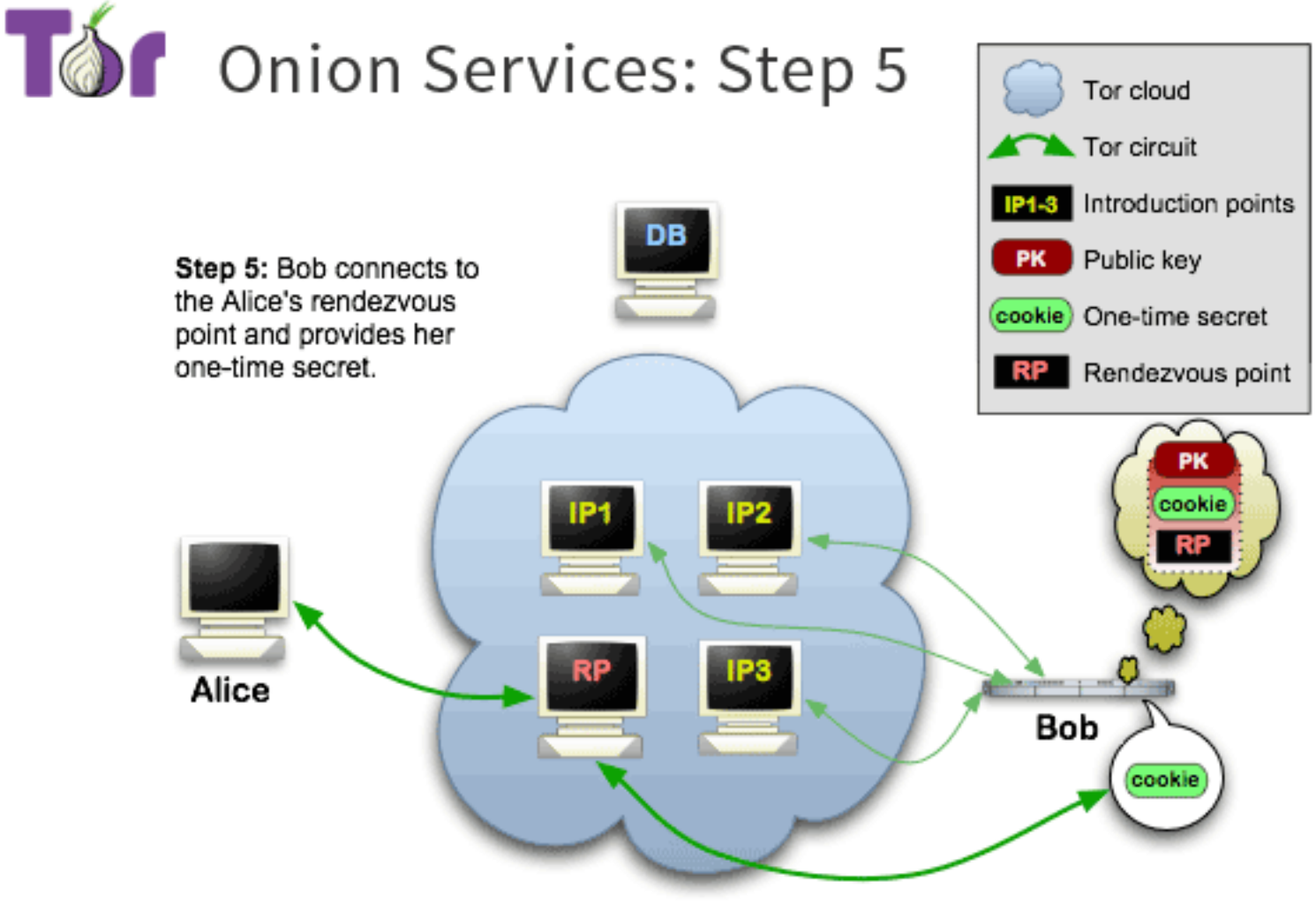
How Onion Services work



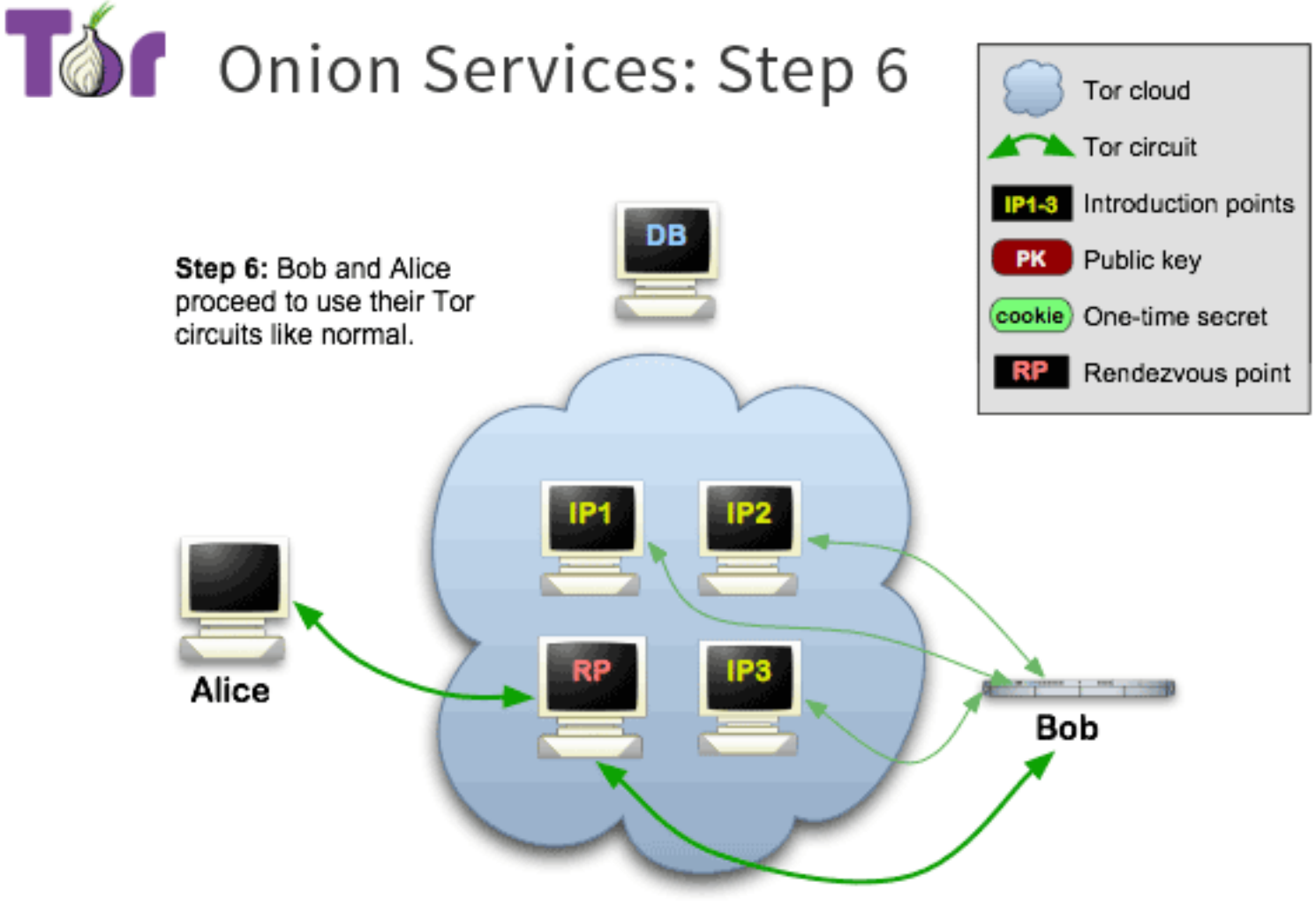
How Onion Services work



How Onion Services work



How Onion Services work



Next gen Onion Services

- Better crypto [edlcurve25519 - Keccak(SHA3)]
- From 16 to 54 chars for onion service.
  - Address the onion service through their public key
  - New key system allows to create subkeys (so the main key stays hidden)
- Rendezvous Single Onion Services
- Vanguards design against the guard discovery attack
- Shared randomness in the desc id

Using Tor within other applications through onion services.

Onion-micro-services ??

- Onion services can be integrated into existing web services, making them more secure.
- This is especially interesting for microservices architectures.

“ Cyberspace.
A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts...

A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding...

William Gibson, Neuromancer

Learn more...

- **www.torproject.org**
- **Tor Browser design doc**
- **Mozilla Firefox Extended Support Release**
- **Tor Projects**
- **Tor Rendezvous Specification - Version 3**
- **Secure Messaging with Onion Services, a How-To**