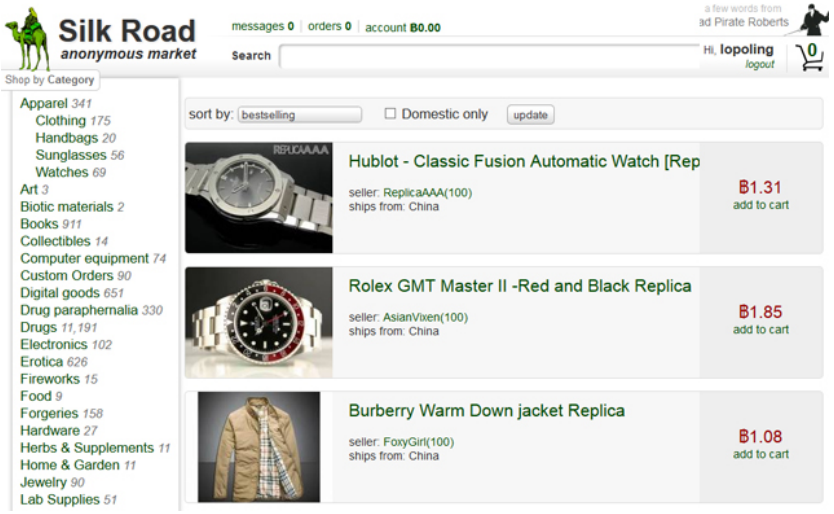
Anonymizing Network Technologies

Based on slides by Chris Zachor

Problem

- Internet surveillance like traffic analysis reveals users privacy.
- 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



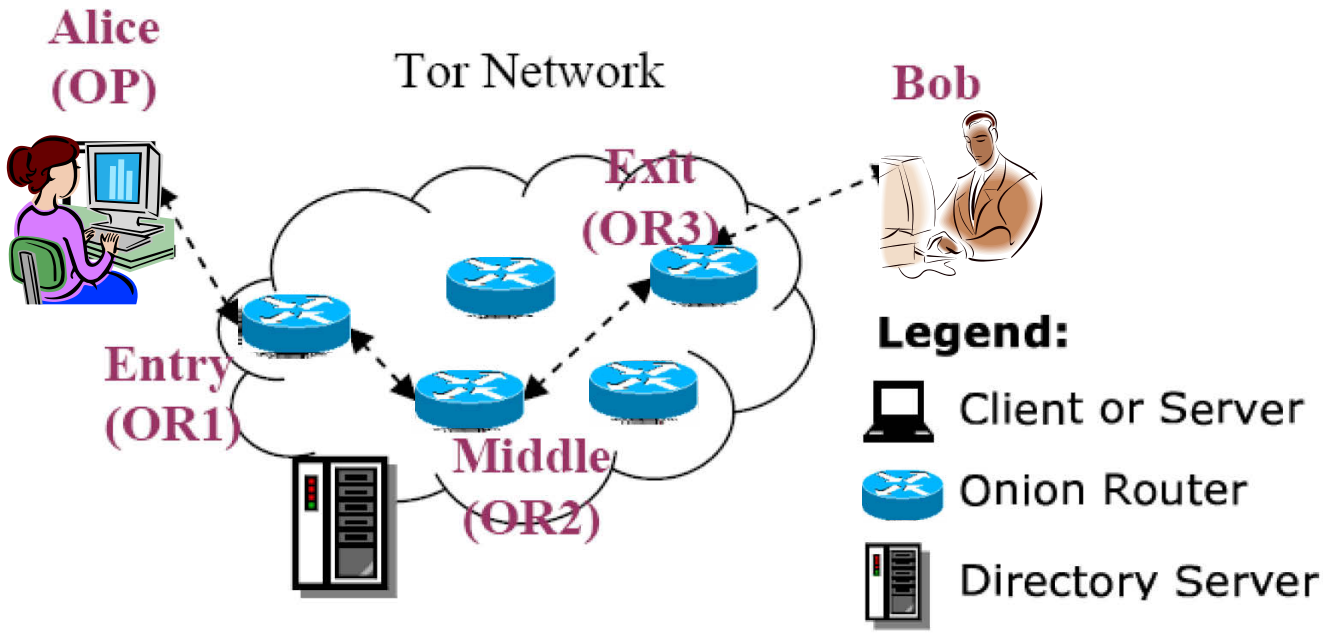
What is Tor

- Tor is a distributed anonymous communication service using an overlay network that allows people and groups 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.

Design

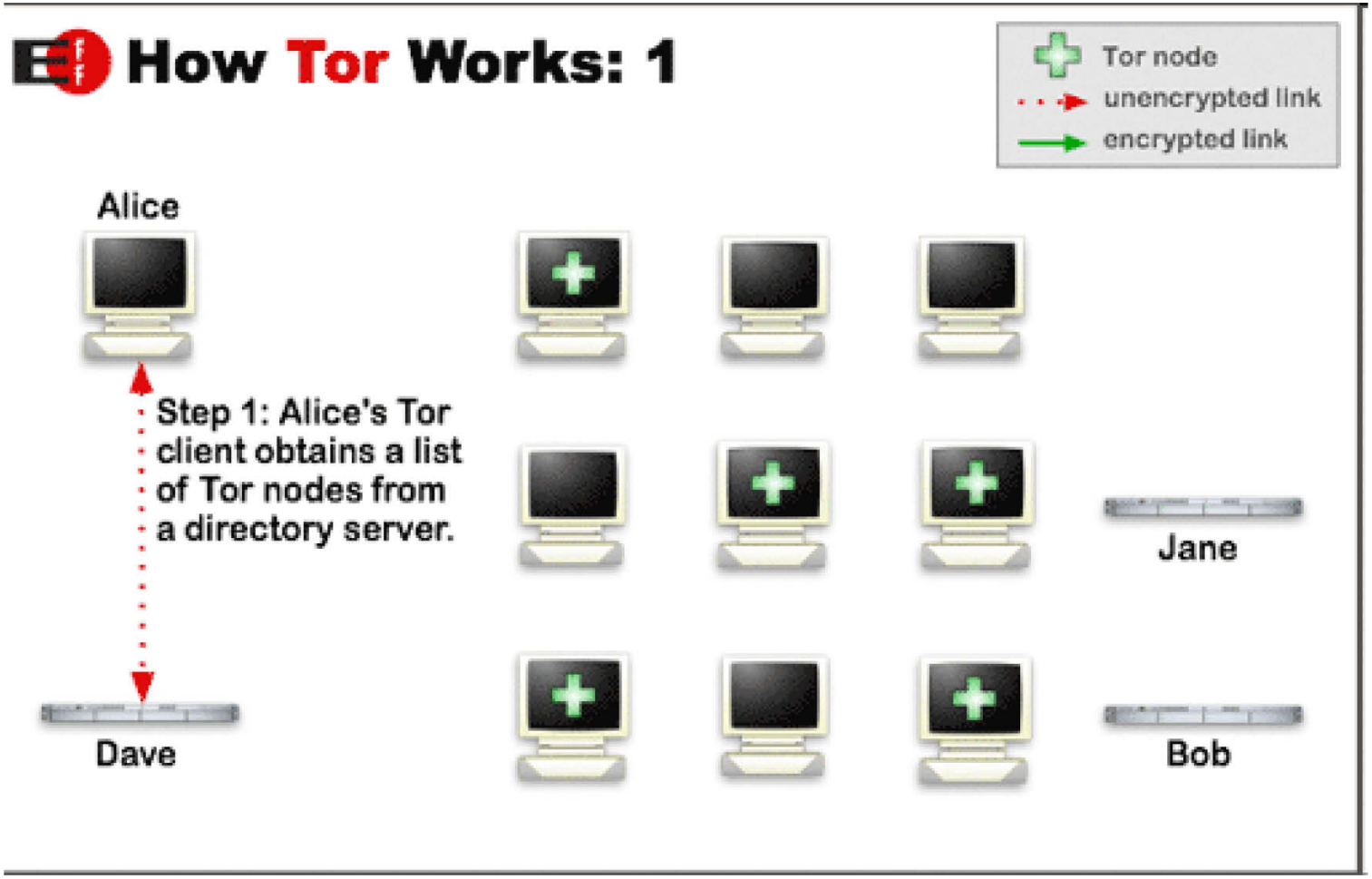
- Overlay network on the user level
- Onion Routers (OR) route traffic
- Onion Proxy (OP) fetches directories and creates virtual circuits on the network on behalf of users.
- Uses TCP with TLS
- All data is sent in fixed size (bytes) cells

Components of Tor

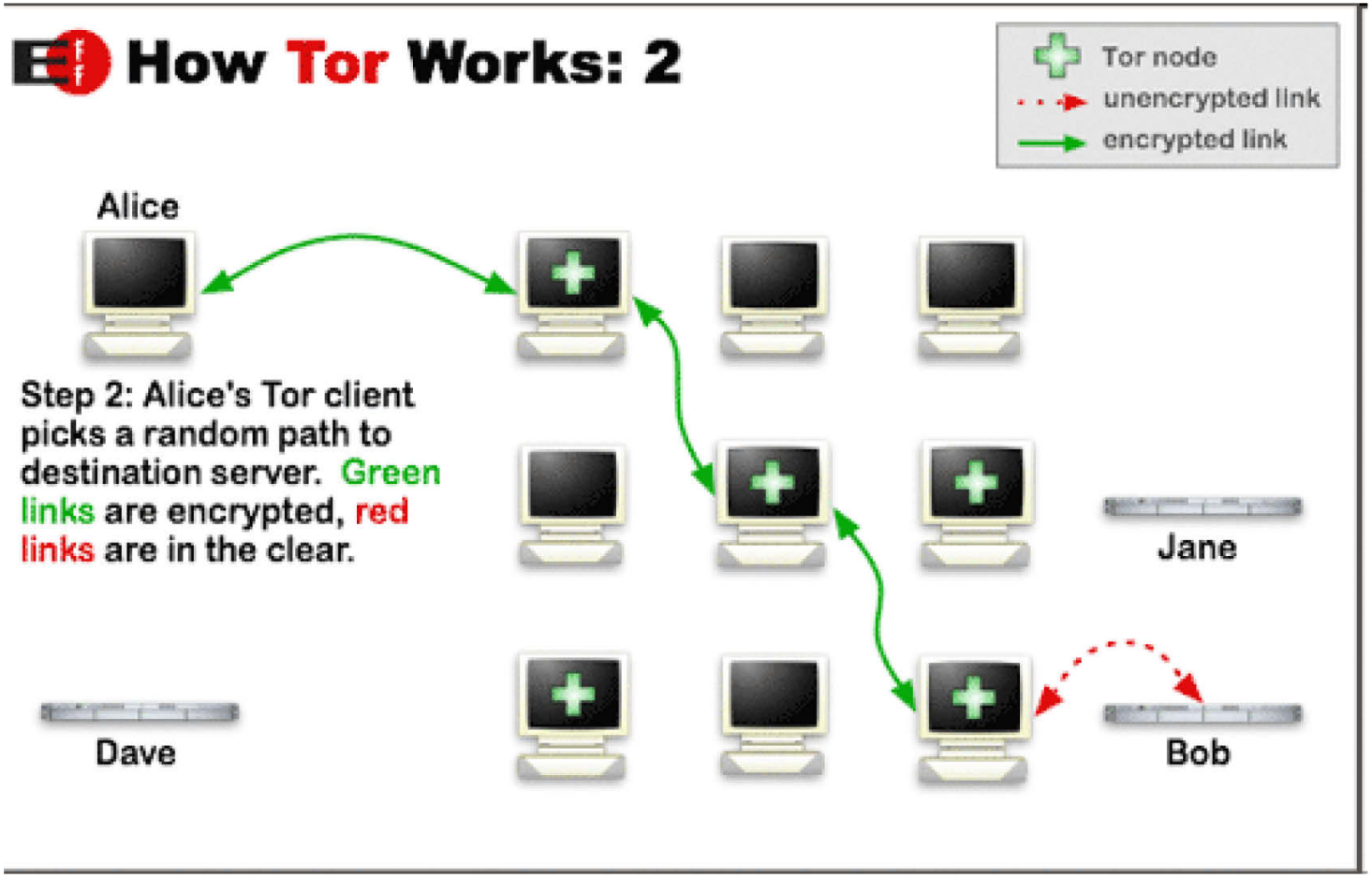


- **Client**: the user of the Tor network
- **Server**: the target TCP applications such as web servers
- **Tor (onion) router**: the special proxy relays the application data
- **Directory server**: servers holding Tor router information

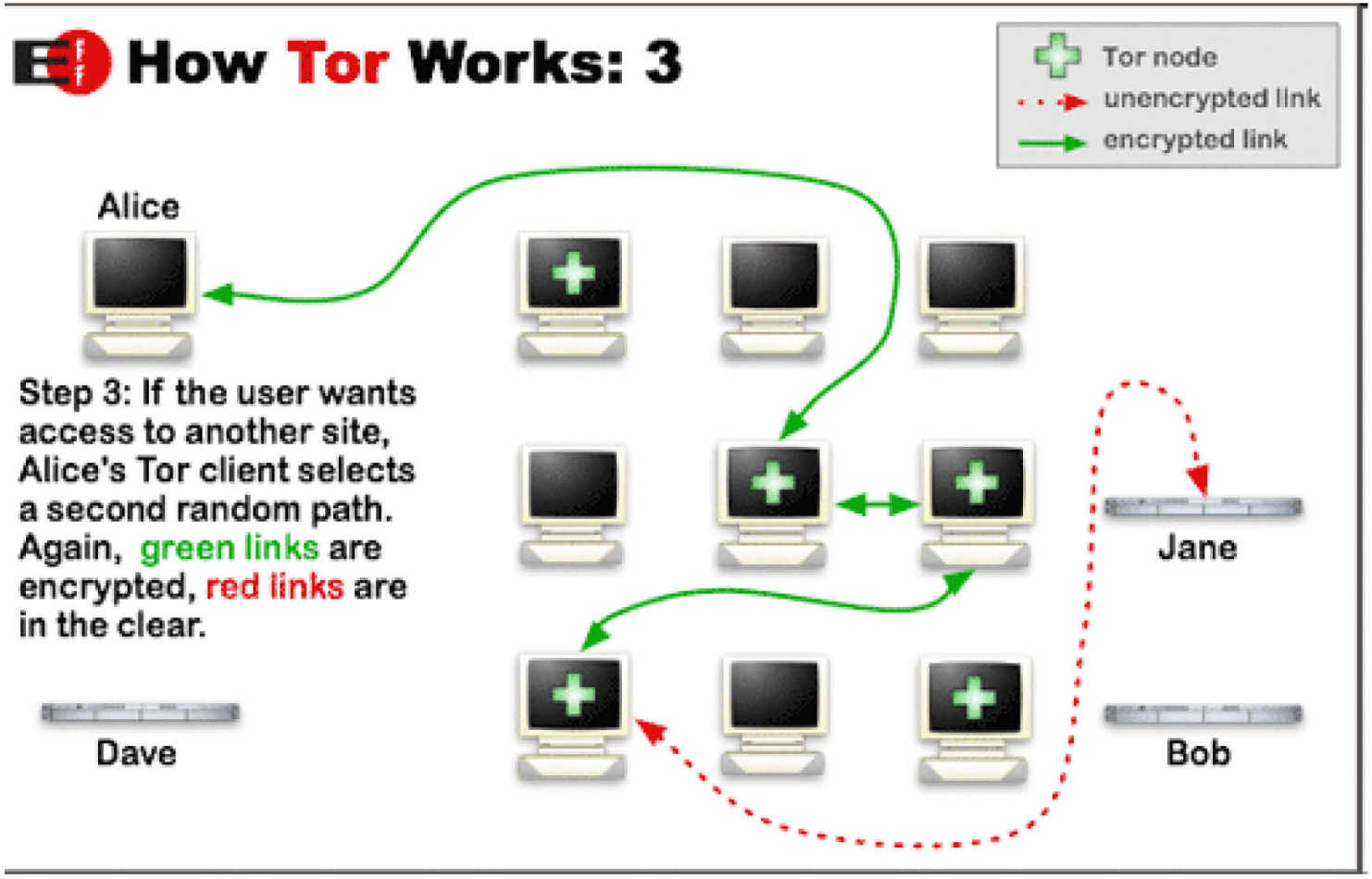
How does Tor work?



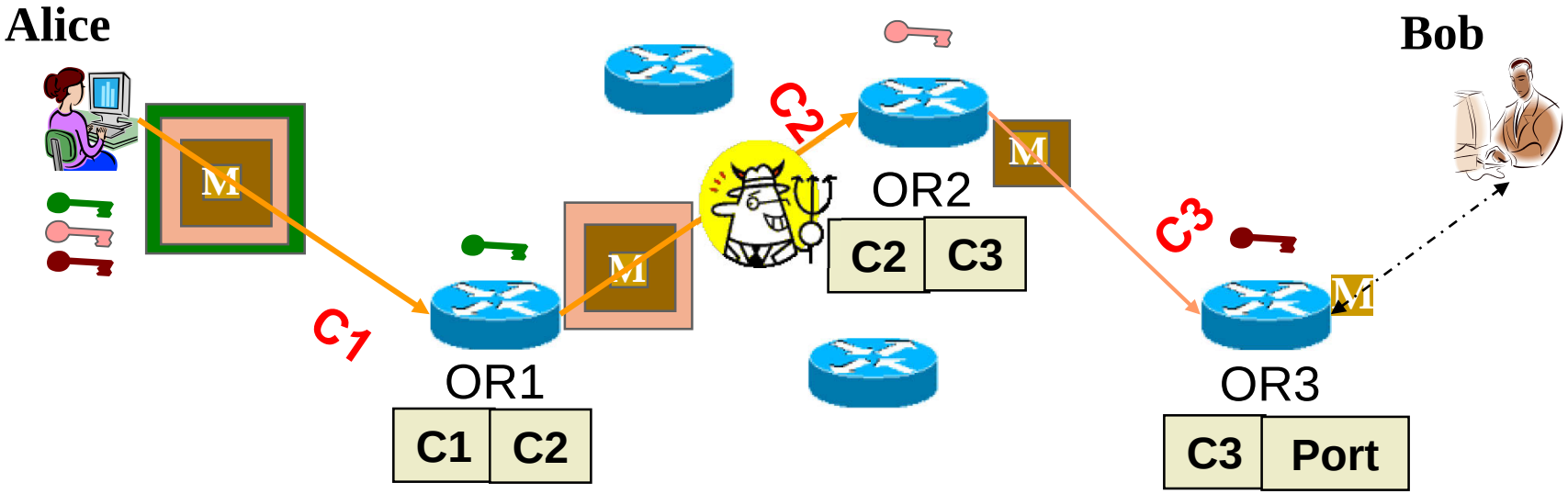
How does Tor work?



How does Tor work?



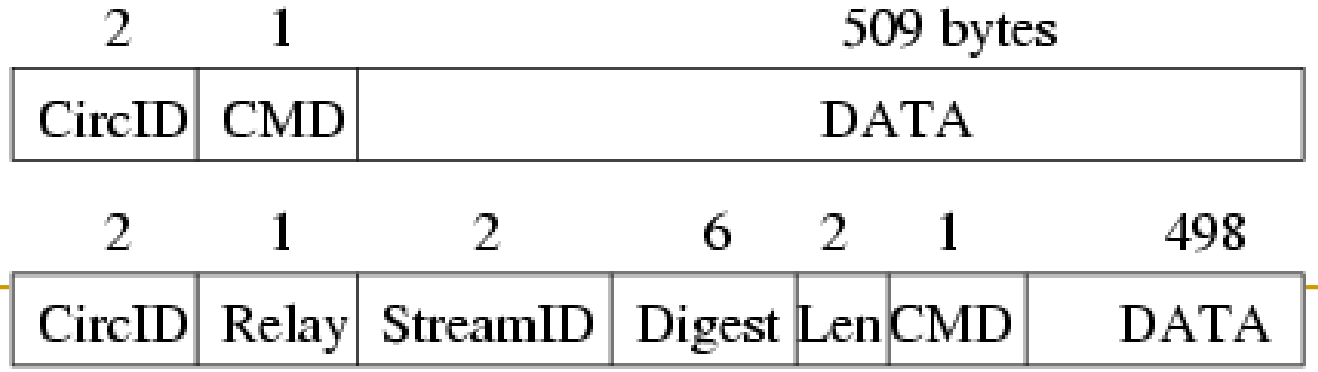
How Tor Works? --- Onion Routing



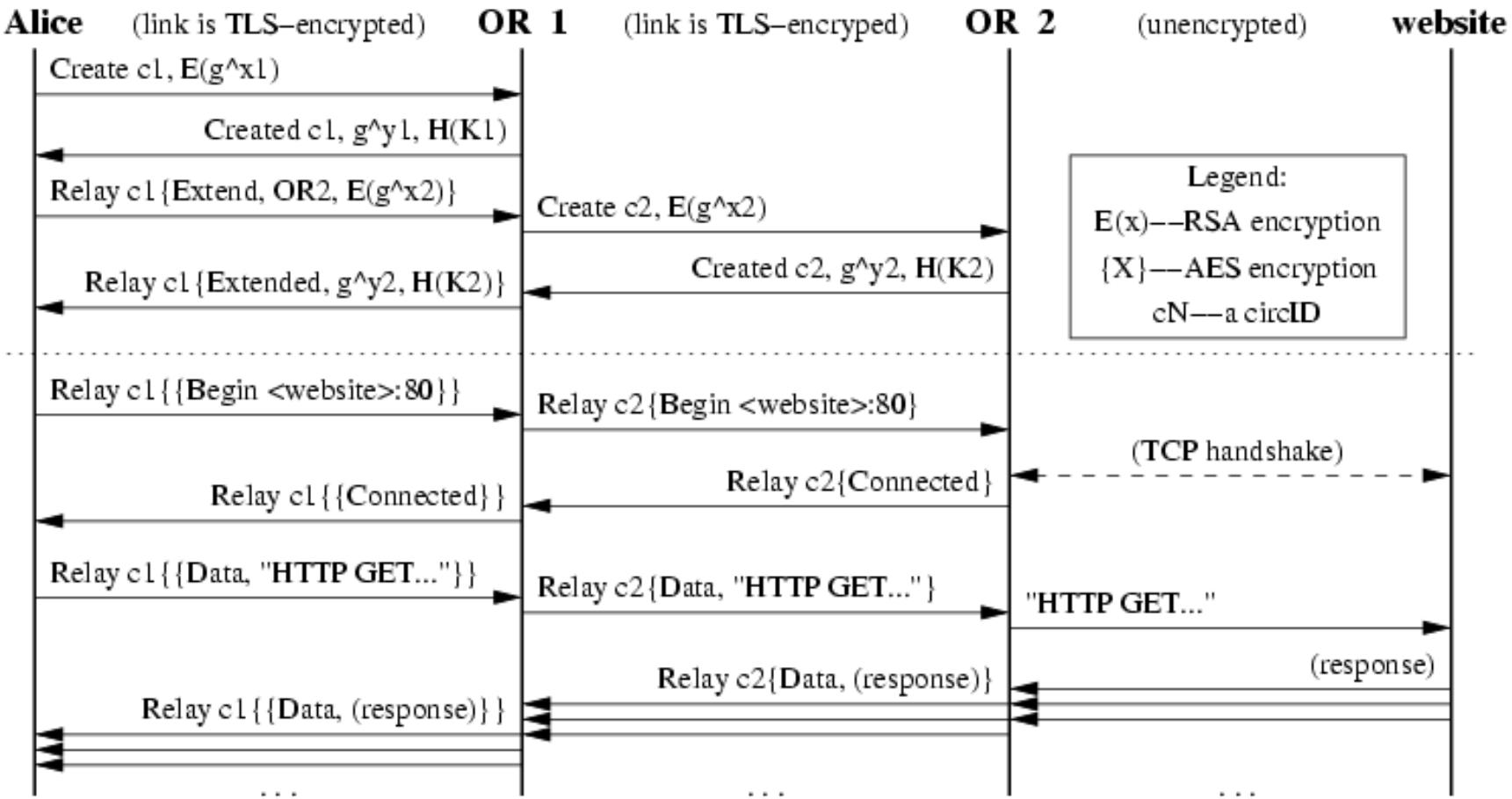
- A circuit is built incrementally one hop by one hop
- Onion-like encryption
  - Alice negotiates an AES key with each router
  - Messages are divided into equal sized cells
  - Each router knows only its predecessor and successor
  - Only the Exit router (OR3) can see the message, however it does not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

Cells

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



Commands in Use



Additional functionality

- Integrity checking
  - Only done at the edges of a stream
  - SHA-1 digest of data sent and received
  - First 4 bytes of digest are sent with each message for verification

Hidden Service and Rendezvous Points

- Location-hidden services allow Bob to offer a TCP service without revealing his IP address.
- Tor accommodates receiver anonymity by allowing location hidden services
- Design goals for location hidden services
  - Access Control: filtering incoming requests
  - Robustness: maintain a long-term pseudonymous identity
  - Smear-resistance: against socially disapproved acts
  - Application transparency
- Location hidden service leverage rendezvous points

Hidden Service and Rendezvous Points

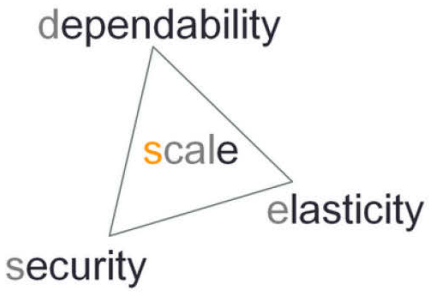
https://senselab.tw

sense lab nctu

Laboratory of SEcurity aNd SystEms

About Member Projects SenseVMs

Welcome !



At SENSE Lab, we are a group of enthusiasts dedicated to research in security and systems. We build systems that will stand firmly in harsh and adversarial environments.

SENSE Lab is located at

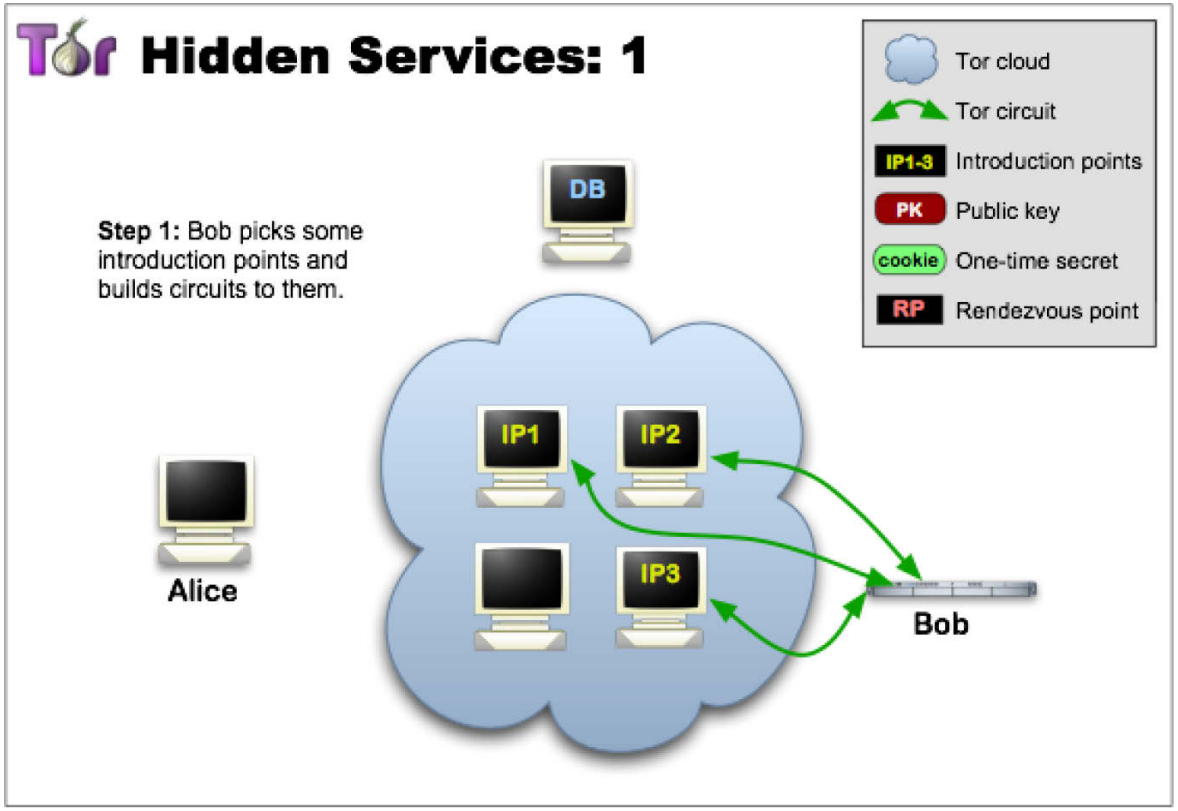
Rm 618, Engineering Bldg III. (24° 47.234', 120° 59.841')

ecp3dytdqf7lzkhf.onion

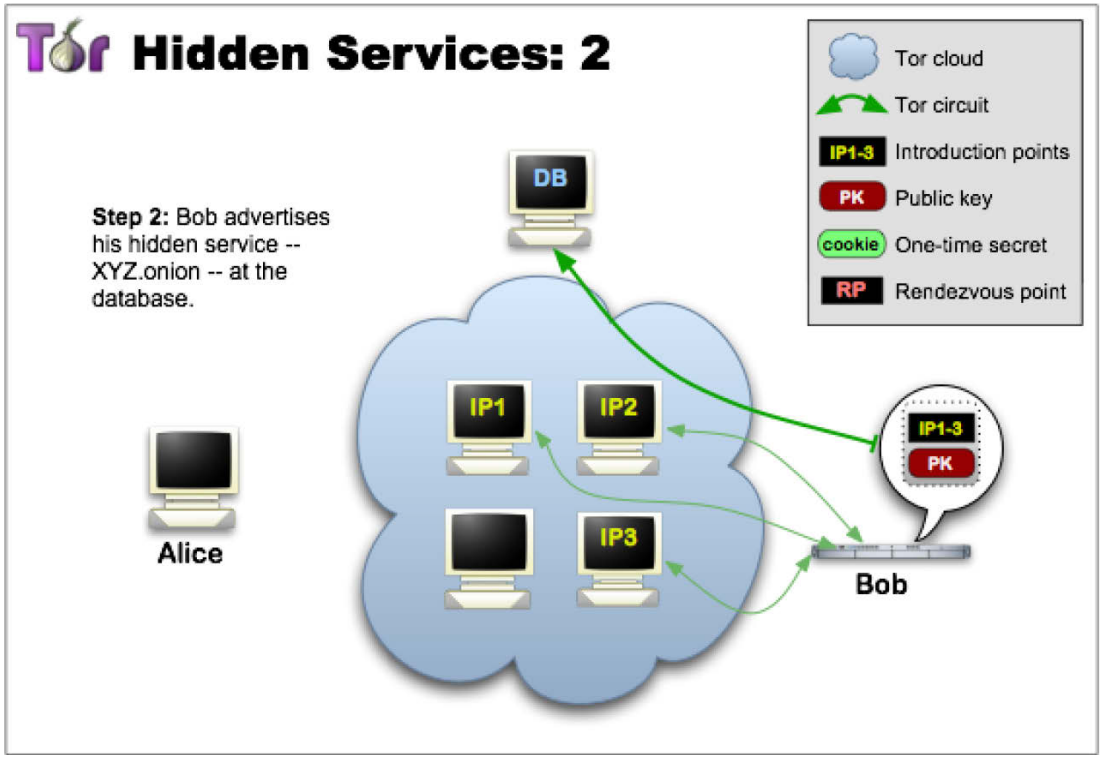
pr4572q7jlddkn4vvk6xovroazezfemmdo34in7p7pf4icfwqmya.b32.i2p

Hidden Service and Rendezvous Points

- https://www.torproject.org/docs/hidden-services.html.en



Hidden Service and Rendezvous Points

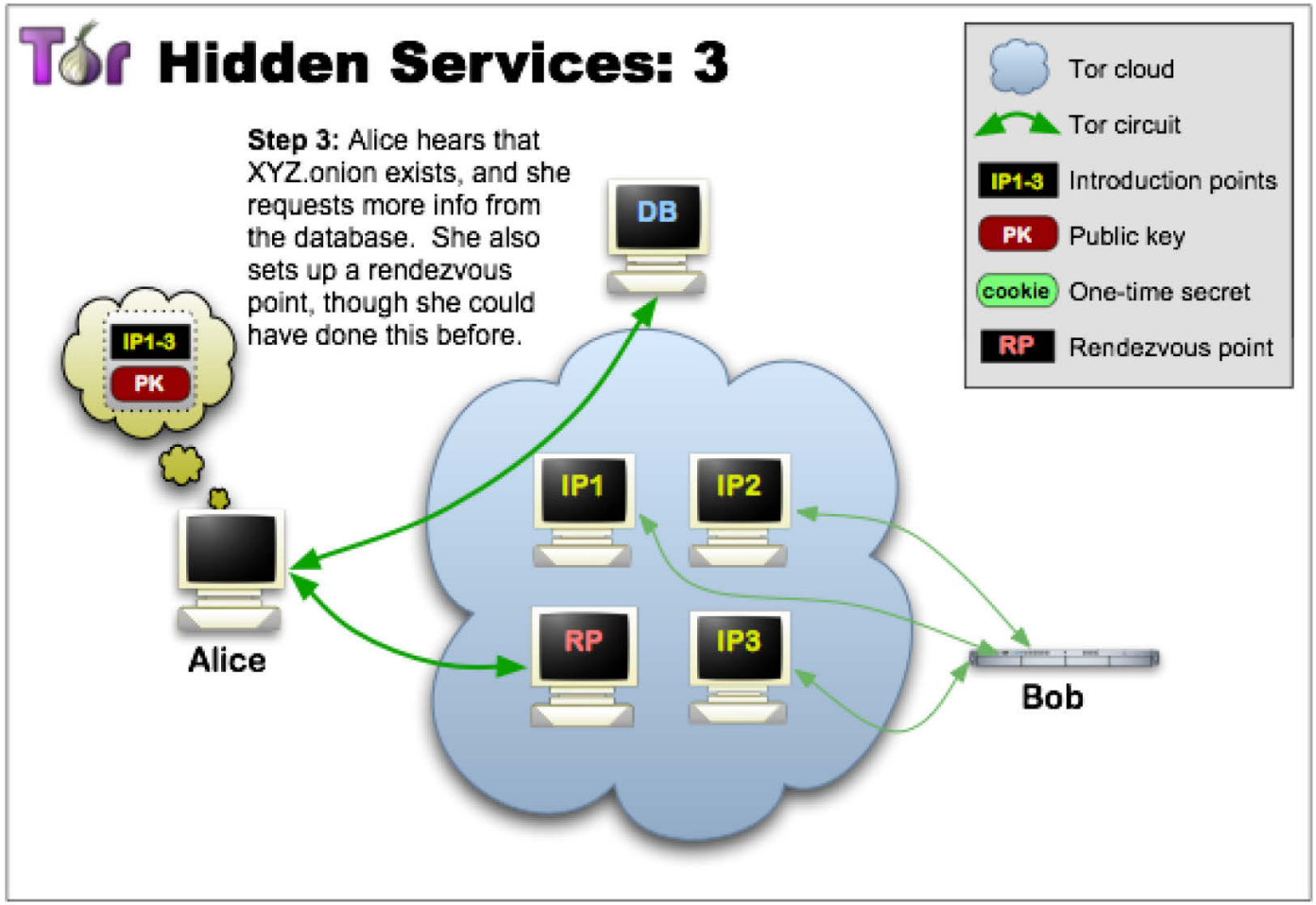


- The hidden service assembles a *hidden service descriptor*, containing its public key and a summary of each introduction point, and signs this descriptor with its private key.
- It uploads that descriptor to a distributed hash table.
- The descriptor will be found by clients requesting XYZ.onion where XYZ is a 16 character name derived from the service's public key.

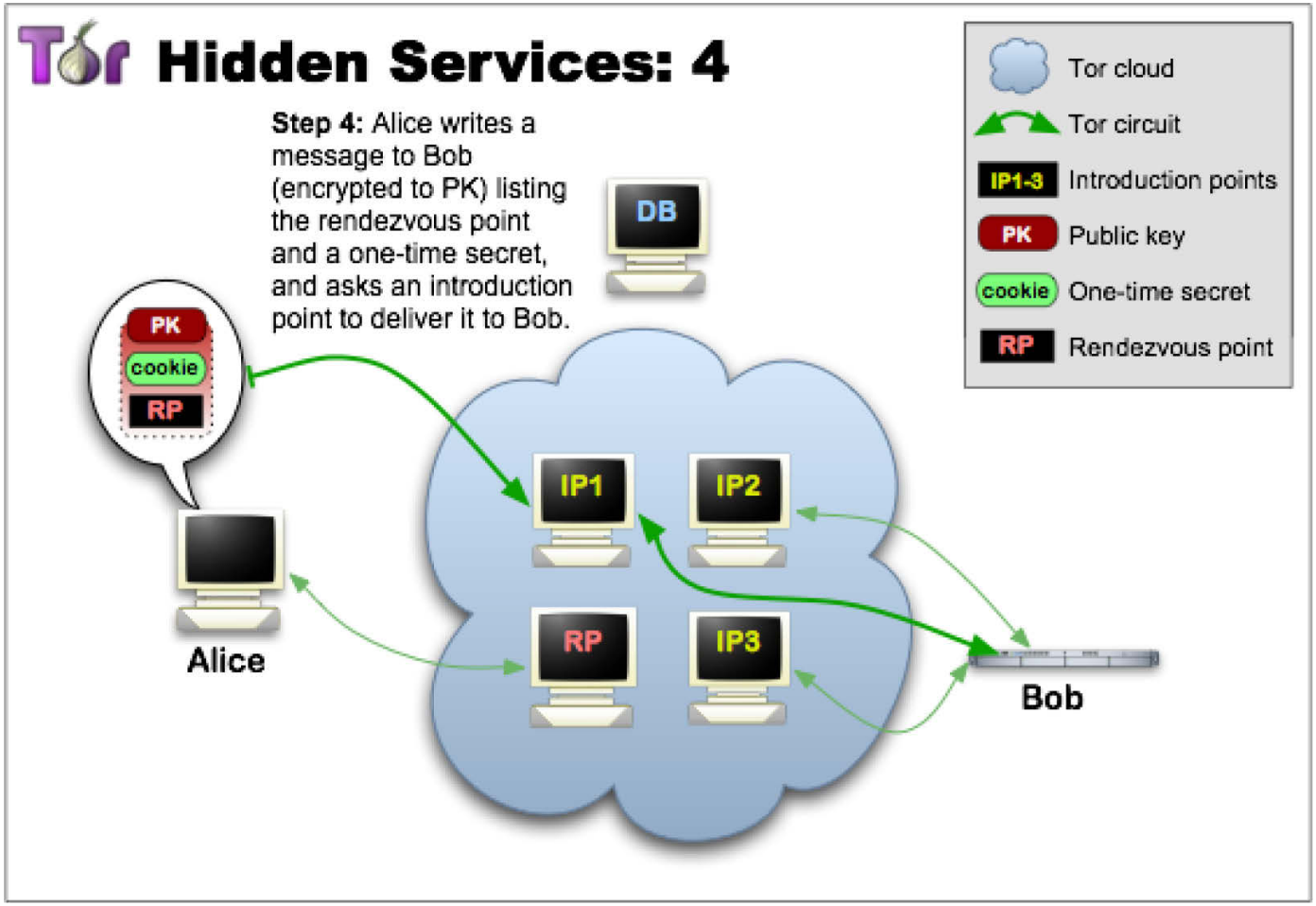
```
rendezvous-service-descriptor yj446zqor4cczgxzl3kgtmdbfgwkj6de
version 2
permanent-key
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAJ/SzzgrXPxTlFrKVhXh3buCWv2QfcNgncUpDpKouLn3AtPH5Ocys0jE
aZSKdvaiQ62md2gOwj4x61cFNdi05tdQjS+2thHKEm/KsB9BGLSLBNJYY356bupg
I5gQozM65ENelfxYlysBjJ52xSDBd8C4f/p9umdzaaaCmzXG/nhzAgMBAAE=
-----END RSA PUBLIC KEY-----
secret-id-part a2pcyuhciqsrah34benwufa54aandwzh
publication-time 2013-10-01 15:59:47
protocol-versions 2,3
introduction-points
-----BEGIN MESSAGE-----
aW50cm9kdWN0aW9uLXBvaW50IGkzdWJoazQzc3RranZlenpmZmlnaXc3ZzRmbmV4
bHI3CmlwLWFkZHJlc3MgNzguNDYuNTEuMjMzCm9uaW9uLXBvcnQgNDQ0Cm9uaW9u
LWtleQotLS0tLUJFR0lOIFJTQSBQVUJMSUMgS0VZLS0tLS0KTUlHSkFvR0JBTWpz
NnZZRmhURWI0U1dTNzd3K3pvMEVrMDFub083cU1aODU0cEtadEt4T2pDSGF1bGhK
V29sTApnYlZwZnpQQVpZeVhoSUJkRW9tK2dabDFyZXhrRE9nTmt2eXNBMHd3cmNS
dk5waklUM3dVYVFhdHlIczIrSnZVCmhzMitzZVY1OXQ2dEZER2VESVdJRHRQVmE0
Q2ZCbUNzSFpiU09aQVFHeUVyNEdHOG9HRjNBZ01CQUFFPQotLS0tLUVORCBSU0Eg
UFVCTElDIEtFWS0tLS0tCnNlcnZpY2Uta2V5Ci0tLS0tQkVHSU4gUlNBIFBVQkxJ
QyBLRVktLS0tLQpNSUdKQW9HQkFOcDM2TlYzeW5GQzd3YTZVbVBaR3psOUI0ejRp
NnpseUVqcXAxZ05vRUIrdmJHbk5yT2x2SDdaCm9pSnVIWlArbTQzNVhNOG1mWGdV
aytxRVp3RFNMUG41QytiNDRjUiszMWNUOEhZSDNSeUZtVk14YStFSXRmT0MKckN1
QTBPYmJKNE45L2YxU0hRdmxHVmpLalZxci9JQU5TK2MzMnZDbGxxSU5CM0VVdXVj
QkFnTUJBQUU9Ci0tLS0tRU5EIFJTQSBQVUJMSUMgS0VZLS0tLS0KaW50cm9kdWN0
aW9uLXBvaW50IHVndW9mcmx5YXI3ZWloemVjbGVycmZoY3BiaXhudGhqCmlwLWFk
ZHJlc3MgMTczLjIxMy43OC4xMjYKb25pb24tcG9ydCA4MApvbmlvbi1rZXkKLS0t
LS1CRUdJTiBSU0EgUFVCTElDIEtFWS0tLS0tCk1JR0pBb0dCQUowa1JMZjNKQ2Fa
KzRodENMenFBNzBKUlFZb1dHWFg1a21zOUoxblI1VmoyUDRyRFc4eEhrVGoKeStK
```

```
Z2NmMFlScmVYZVRMN2pyWmhBUlVjc2hBZDl3a1ZVTXR6N3ZlUGlVbVZFVm44aEN2
SUFnZjFGMkN5STAxQgp1WTJRZ01SUHEzYXZOd2RQUzdSbHVCemdSbXNBQjh6bGw0
QkhObTFNSTJhbHJKY2tXZDRSQWdNQkFBRT0KLS0tLS1FTkQgUlNBIFBVQkxJQyBL
RVktLS0tLQpzZXJ2aWNlLWtleQotLS0tLUJFR0lOIFJTQSBQVUJMSUMgS0VZLS0t
LS0KTUlHSkFvR0JBUDVGNnNQZ25BdHY0VDFKVlRUc3RBcytkUjVjVWpFdmxBS1Z0
d3M5NTVHQUVXUm1CZkp1a3BVKwplV3A4MENsbml1VGVPeW14VG01L0xlZlNBNGdl
YnVNcjgxc3gvYzNMTG1lTmNKZnZsWjl0VitjRnlXdEg2OXRiCkV2RXFhWFl0UGpZ
cnhQUXVzeWNBZVkxRW1NTGJLdXRhZ1ZlSzNnaWFMSTZ2K2VjL0VxekJBZ01CQUFF
PQotLS0tLUVORCBSU0EgUFVCTElDIEtFWS0tLS0tCmludHJvZHVjdGlvbi1wb2lu
dCAycHNoNnpnZWNuYXE2amZuZXdtcWxtZnhqYmN0ejZyNAppdC1hZGRyZXNzIDUu
MTk5LjE0Mi4xOTUKb25pb24tcG9ydCA5MDAxCm9uaW9uLWtleQotLS0tLUJFR0lO
IFJTQSBQVUJMSUMgS0VZLS0tLS0KTUlHSkFvR0JBTjFkNXZqN0xkQkttT0NIaWJ0
VTNyMlBrQVpsenV3L0RDbmRMc2IrMkRnVG90eTRjU1Rjc2E4dAo2TlI0WEN5Tith
N1JURis2Q3dSdnJpUnZ1K0ZwQVEwdUIzV2tkUENCTDVreHJXT1d5V0t6Lzk1blU3
Vlo3cEVMCmNqbktmVVZOMnl0Qng2dWJ3S2lUSktqek51cjA1N0g3MmdoQmRPZlR1
bE9STjhqdWZqb3BBZ01CQUFFPQotLS0tLUVORCBSU0EgUFVCTElDIEtFWS0tLS0t
CnNlcnZpY2Uta2V5Ci0tLS0tQkVHSU4gUlNBIFBVQkxJQyBLRVktLS0tLQpNSUdK
QW9HQkFKNGw5M2pHa1ZoOXp5czZvNkR6aGJudTBoem1jT3dOOFJCUU9JWUU1S2tK
NzNxNjkxaXdTaHkxCnJ6K3pQQXJiOEJ0aHNxZmhhWjNucHBCNHNnYVhuRHJUR2FE
Vjh5bVk1UVVBaGtWSnRkcnRGcmNROFJVTGVsbFcKZFNPZ2VKamNKRnZESkdCdWgz
MzBjcmRIN295Q045Q1BISm1SUWs4VXNHbnpiMzdKbXM3eEFnTUJBQUU9Ci0tLS0t
RU5EIFJTQSBQVUJMSUMgS0VZLS0tLS0KCg==
-----END MESSAGE-----
signature
-----BEGIN SIGNATURE-----
VEToDAxw1X77NwcM6/DG+I3uu8lLlFpI//rUHjLRC0unA7kRp6xY4E6xpcbl4KUX
EUUkJ3hXhmB3gFAjUkk70IDr5HIP86Z/ZTl6WvbTFWYLUPJQtt08XSmY788FG1lA
nTnNbqms5Nt5HKsG5khZf5viIuU3ei+u0SIv3gHy3JY=
-----END SIGNATURE-----
```

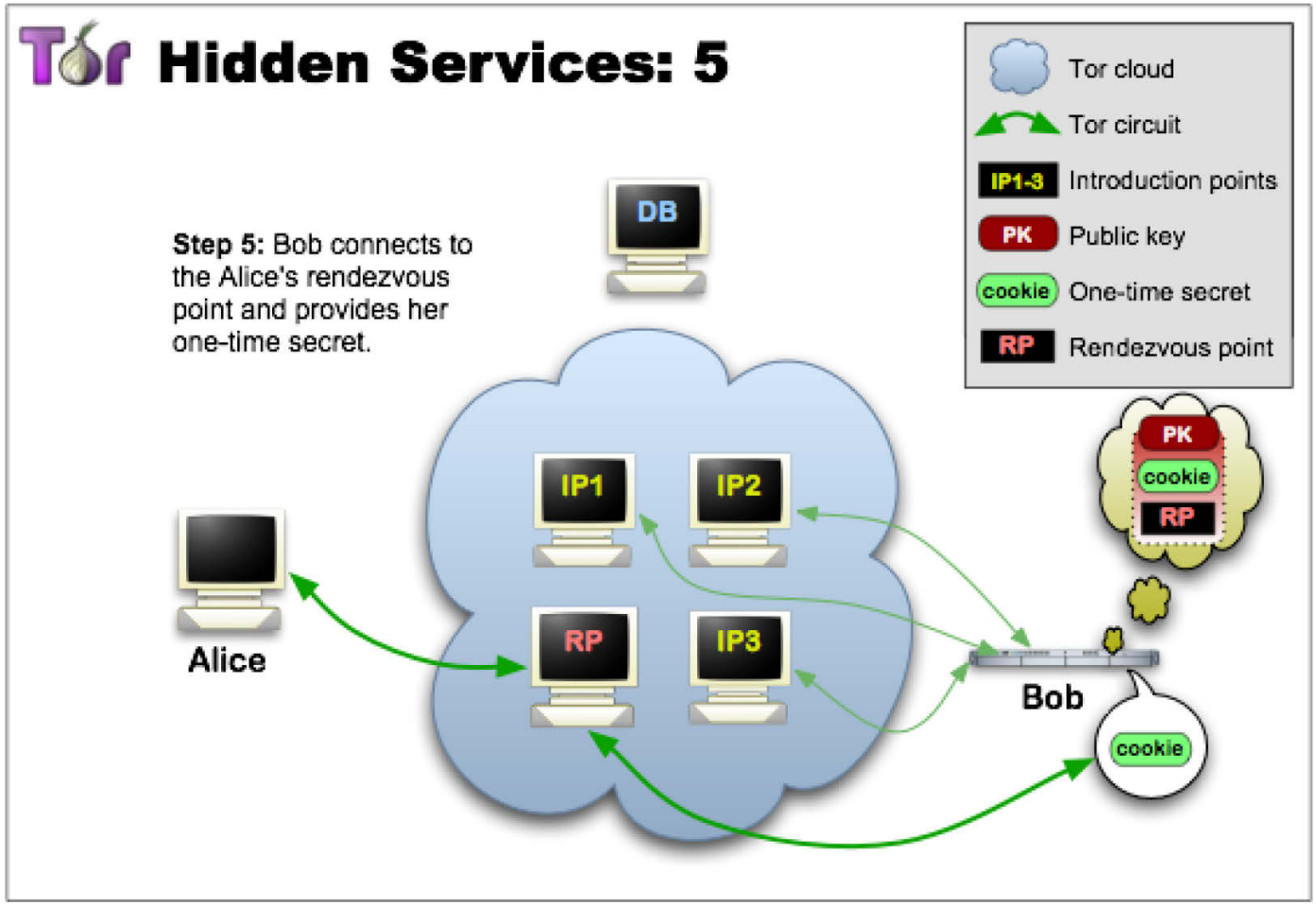
Hidden Service and Rendezvous Points



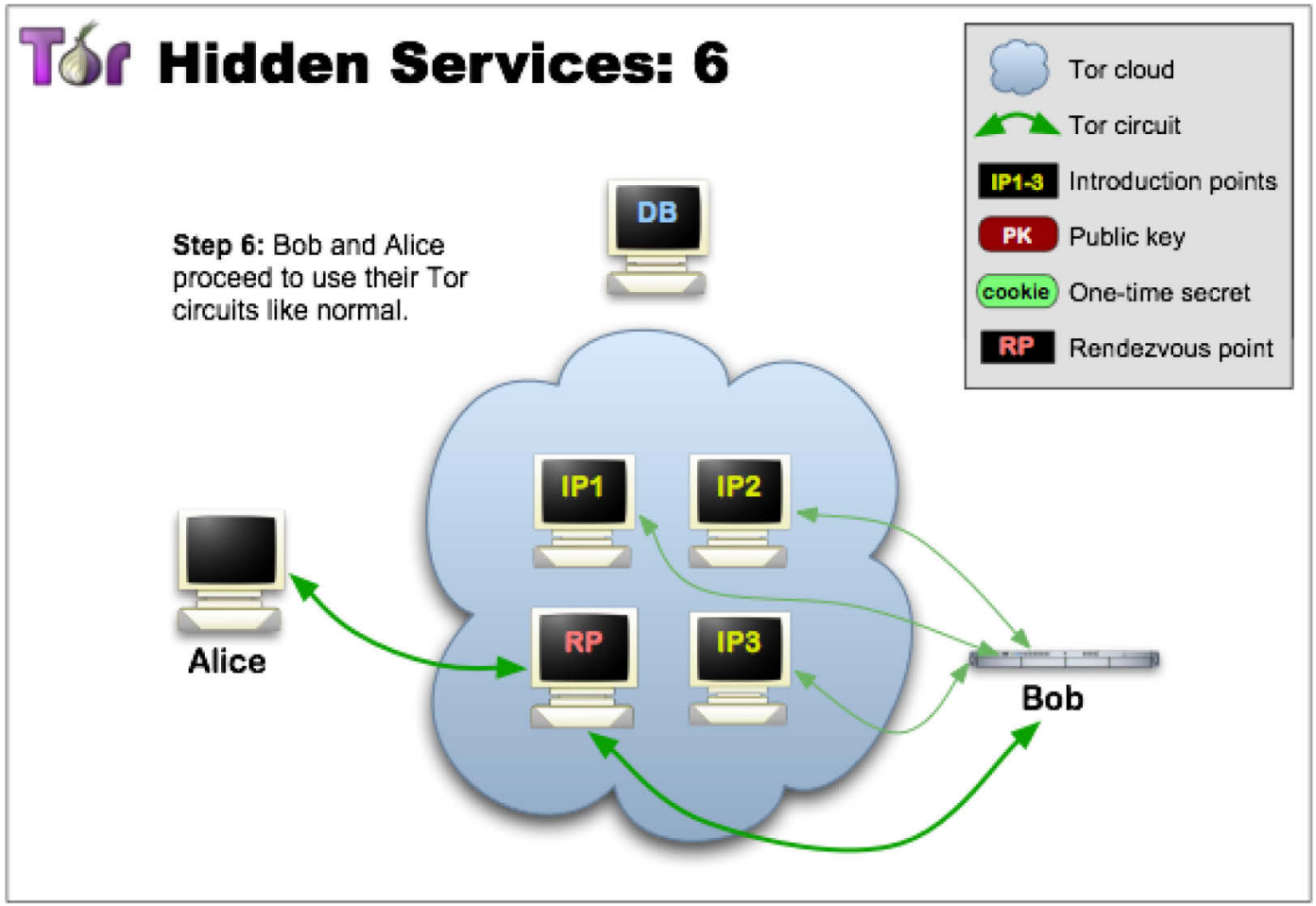
Hidden Service and Rendezvous Points



Hidden Service and Rendezvous Points



Hidden Service and Rendezvous Points



I2P: The Invisible Internet Project

What is I2P?

- An anonymizing P2P network providing end to end encryption*.
- Utilizes decentralized structure to protect the identity of both the sender and receiver.
- It is built for use with multiple applications including email, torrents, web browsing, IM and more.
- UDP based (unlike Tor's TCP streams)

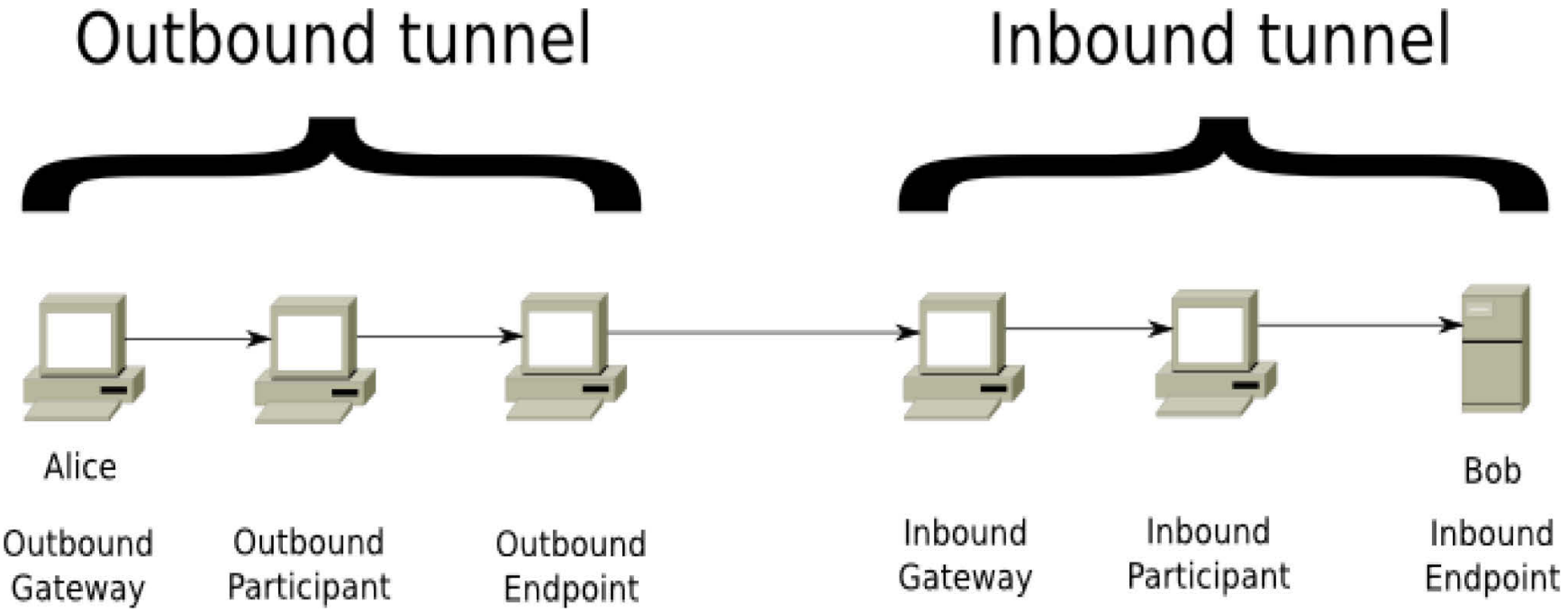
What is I2P Not?

- I2P is not Tor even though they are similar in some ways.
- While you can use it as an anonymizing gateway to the internet, that is not its intended purpose
- I2P was designed primarily to host its own services

I2P Definitions

- Router
- Tunnel
- Gateway
- Endpoint
- NetDB

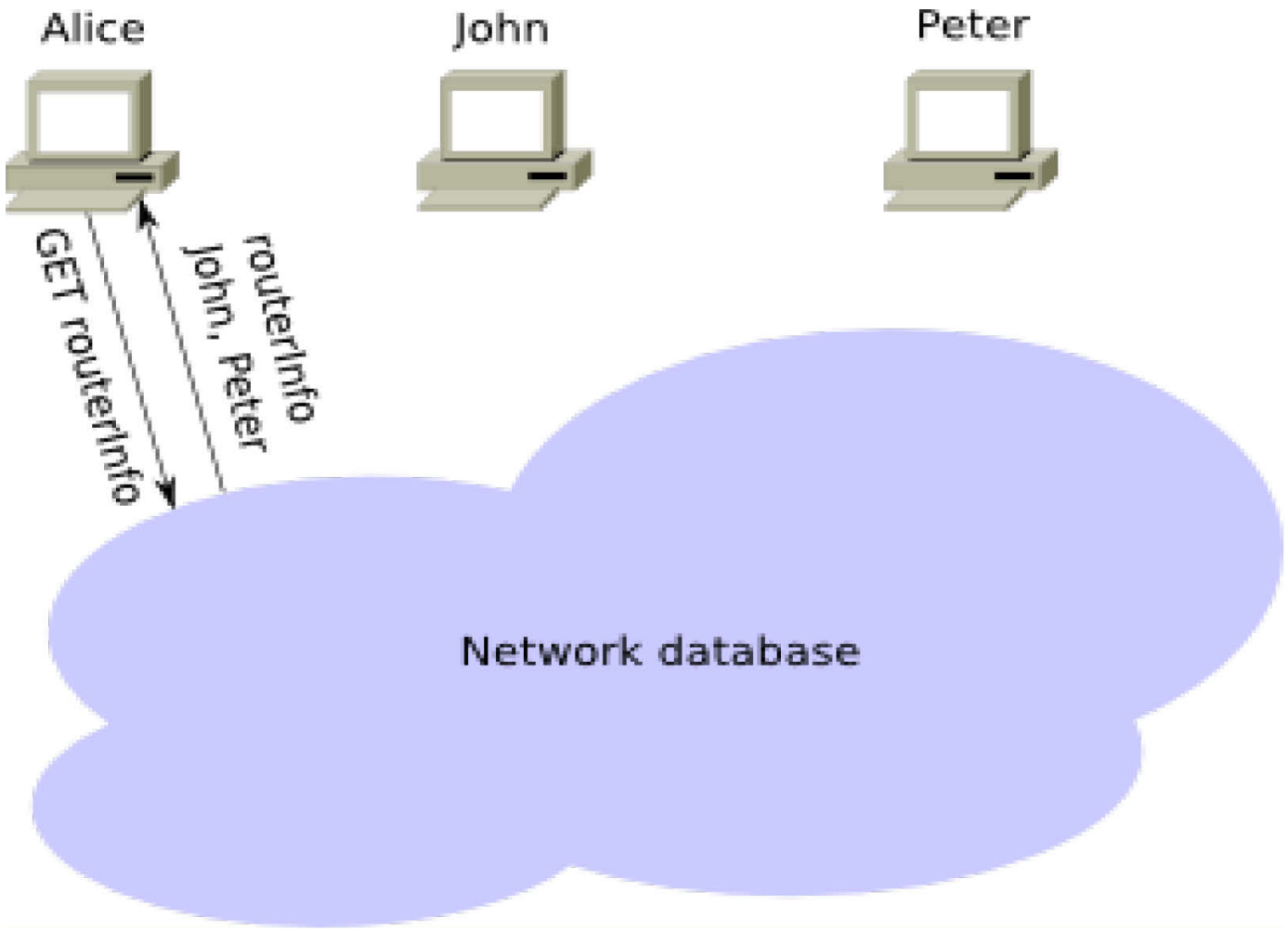
I2P Tunnels


Outbound tunnel
Inbound tunnel
Alice
Bob
Outbound Gateway
Outbound Participant
Outbound Endpoint
Inbound Gateway
Inbound Participant
Inbound Endpoint

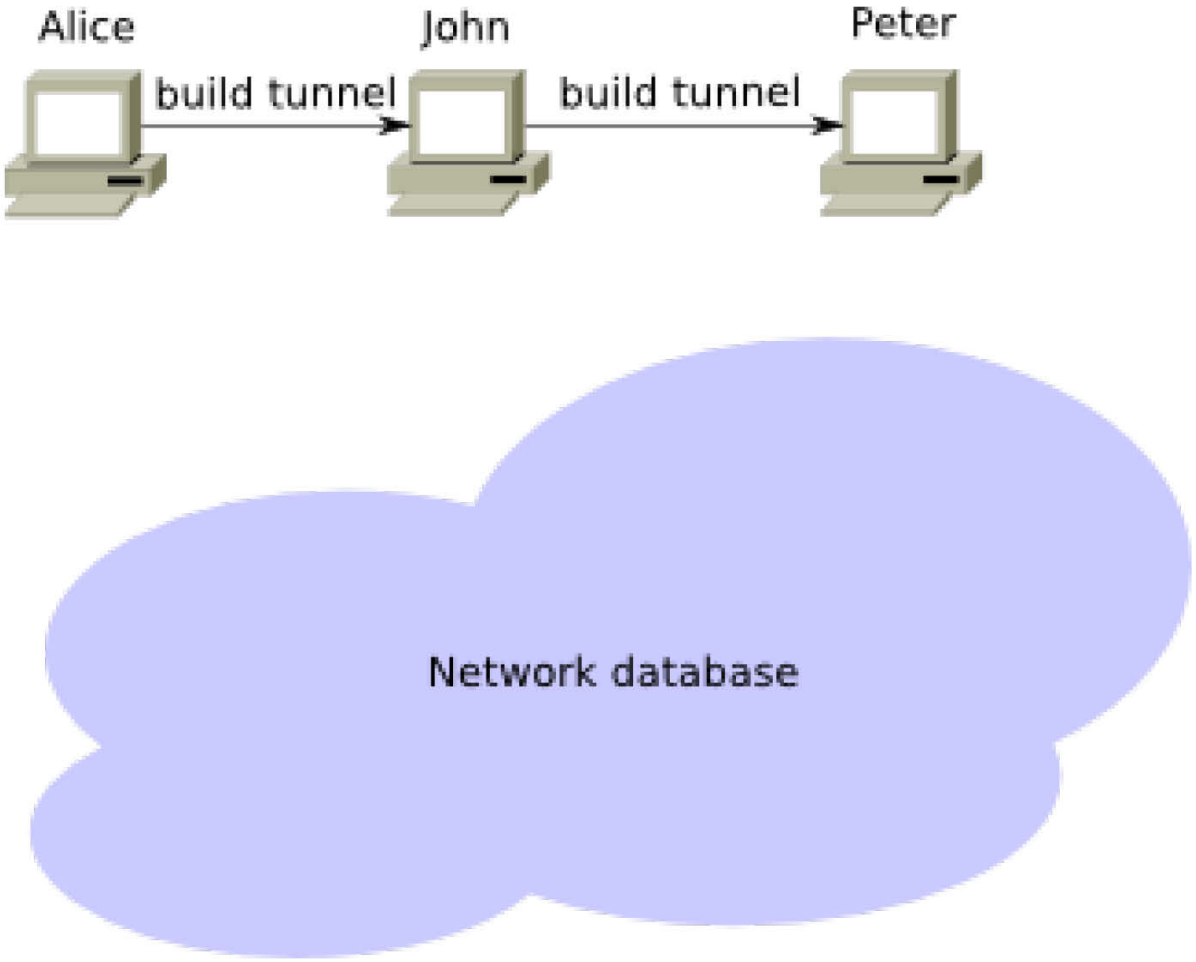
NetDB

- Each router holds a network database
- 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.)

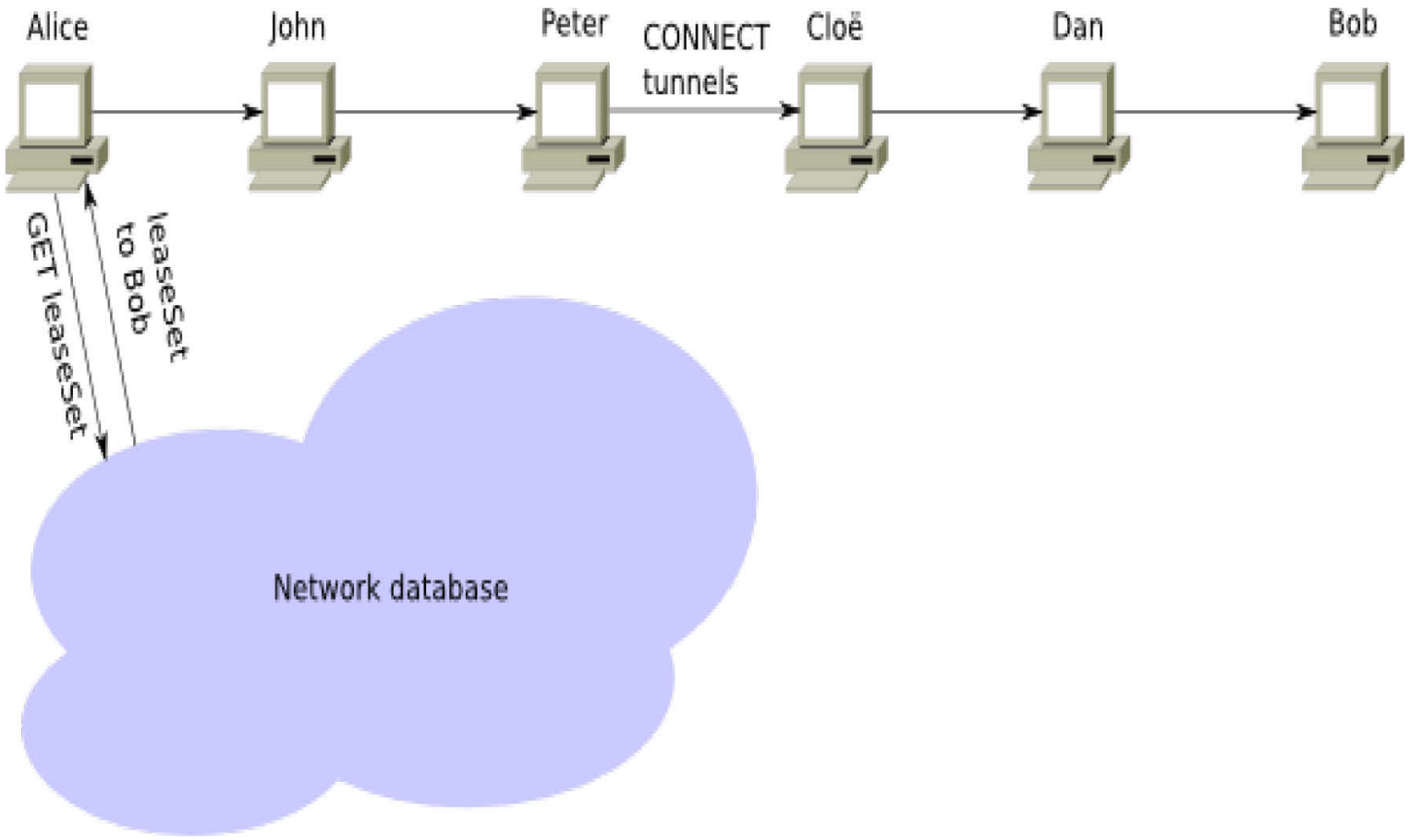
Joining the Network



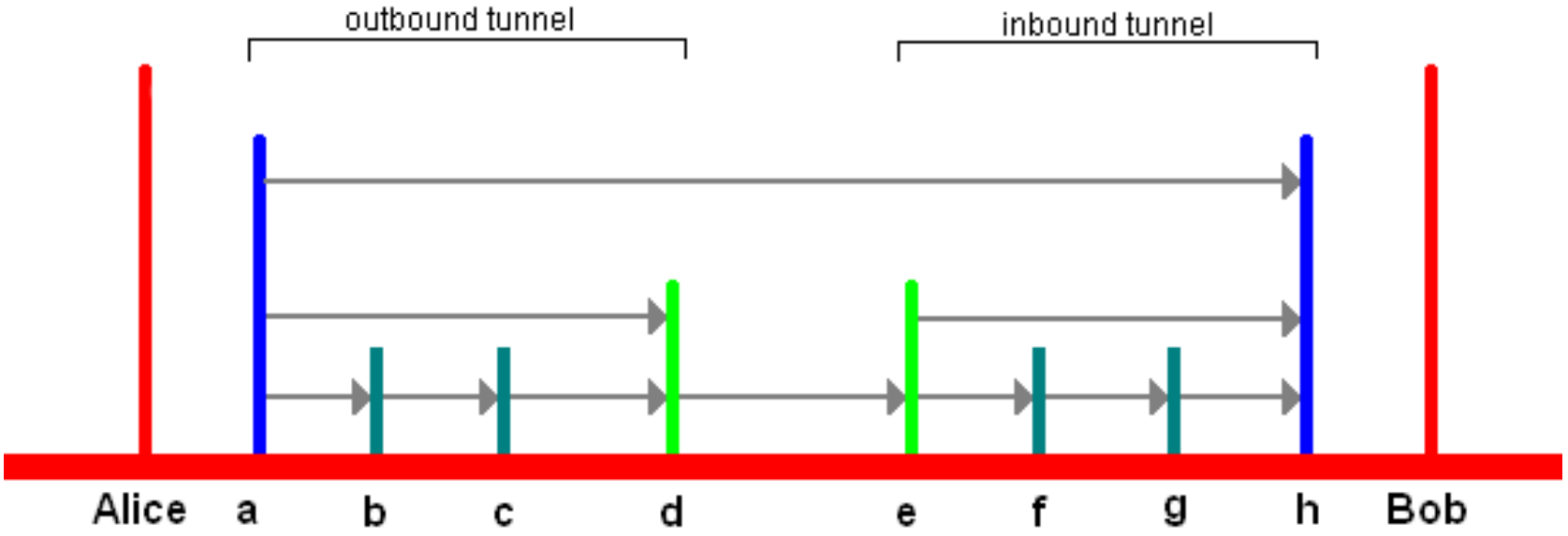
Establishing a Tunnel



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

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