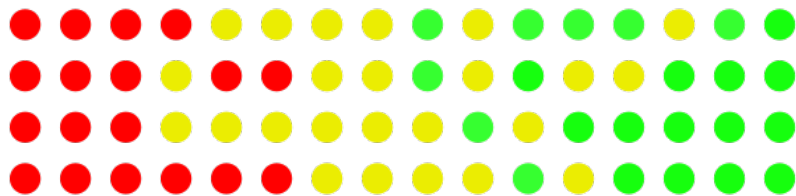


I2P



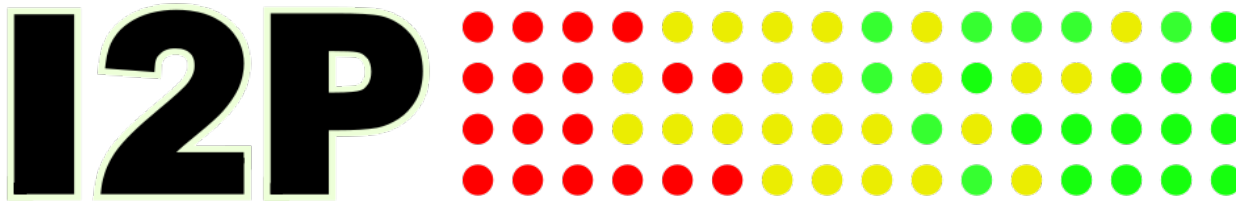
**Arturo Cortés Sánchez
y
Adrián Pérez Ortega**

Índice

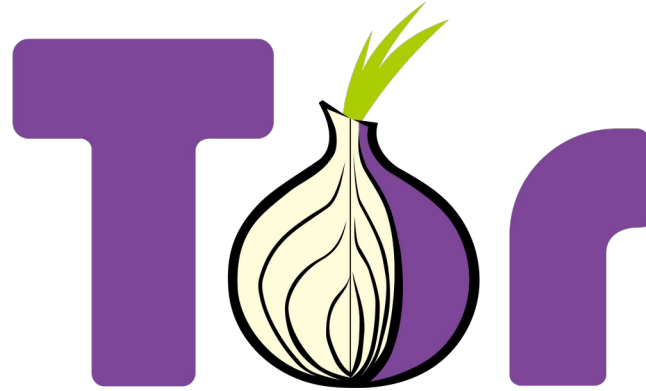
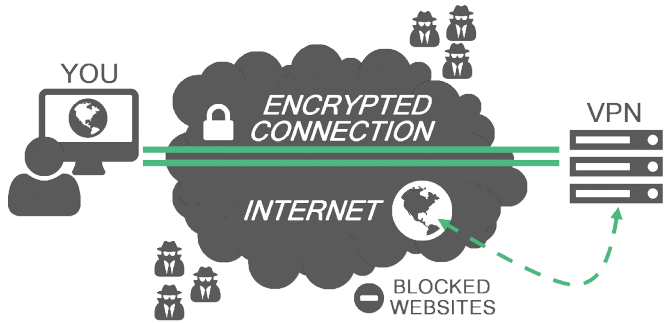
1. ¿Qué es I2P?
2. Diferencias con VPN y TOR
3. ¿Donde se usa?
4. Requisitos de instalación
5. Funcionamiento básico
6. Túneles
7. Base de datos de red
8. Garlic routing
9. Proceso de envío de un mensaje a través de I2P
10. Tutorial de instalación y uso básico

¿Qué es I2P?

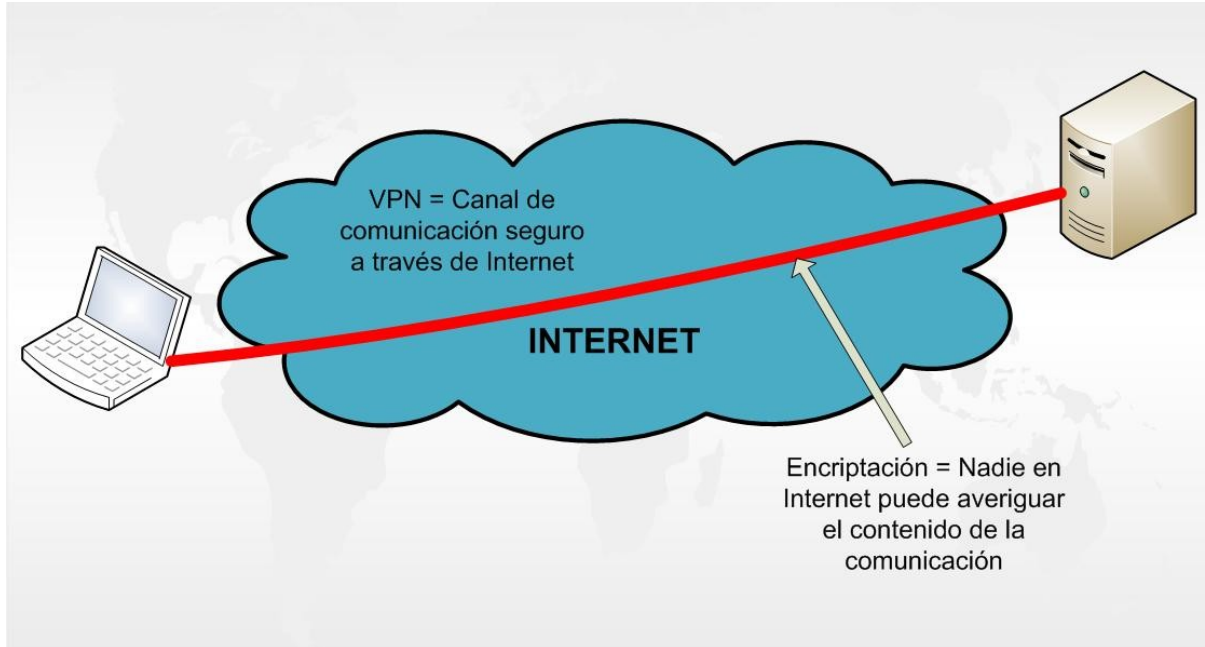
- I2P: Invisible Internet Project
- Software que ofrece una capa de abstracción para comunicaciones anónimas entre ordenadores



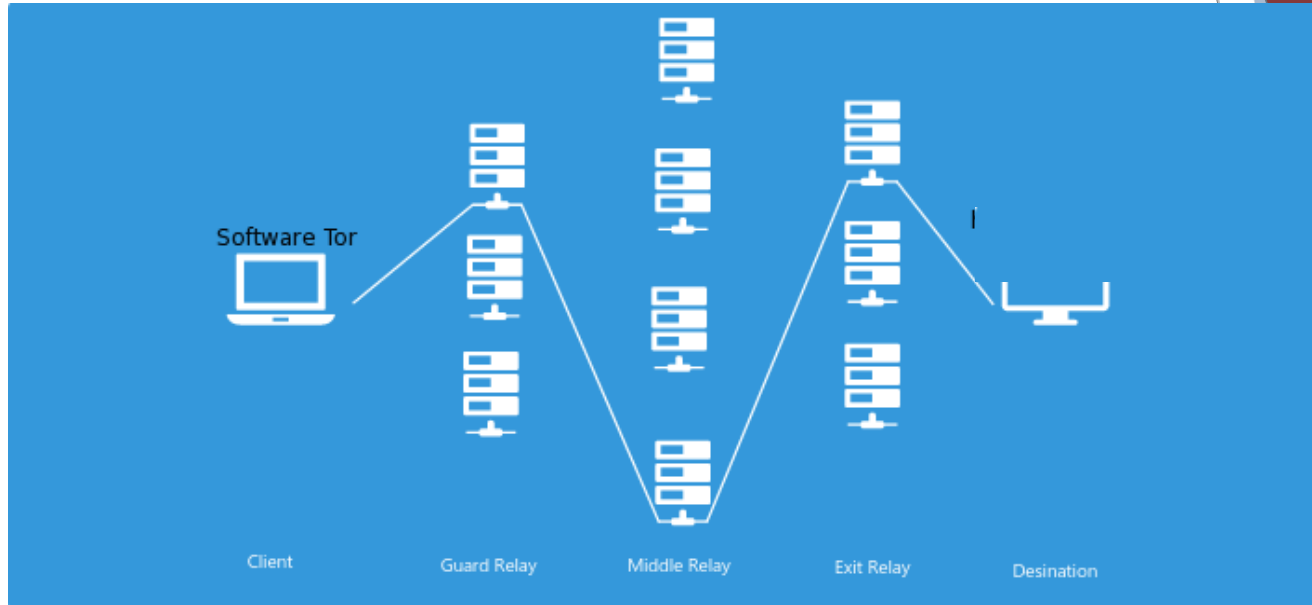
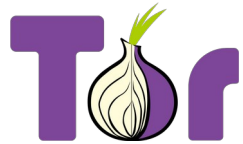
Diferencias con VPN y la red TOR



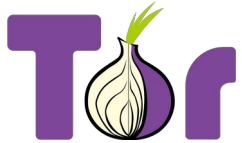
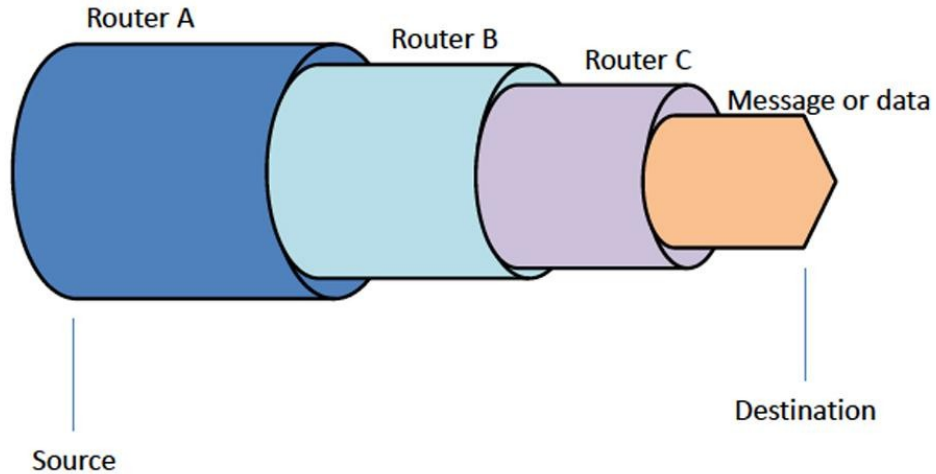
Diferencias con VPN y la red TOR



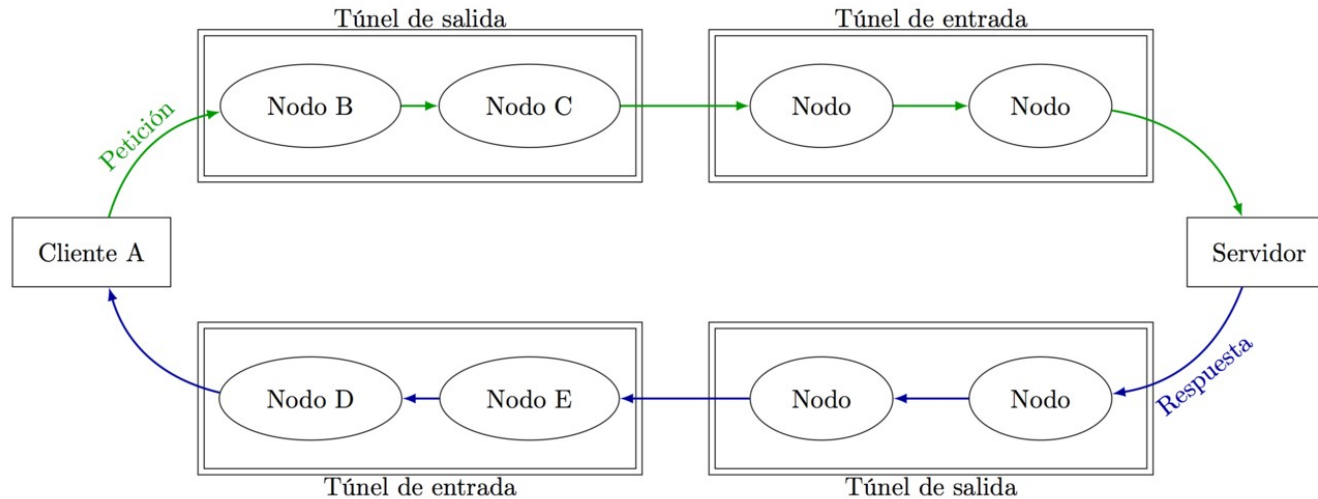
Diferencias con VPN y la red TOR



Diferencias con VPN y la red TOR



Diferencias con VPN y la red TOR



Beneficios frente a TOR



- Servicios ocultos más rápidos que Tor
- Conmutado por paquete en vez de por circuito
- Túneles unidireccionales en vez de bidireccionales
- Los túneles de I2P tienen una vida corta
- TCP y UDP
- Actualizaciones automáticas
- Java, en vez de C (?)

¿Dónde se usa?

- Email



- Compartir archivos



- Chat



- Mensajería instantánea

- Publicación de contenidos



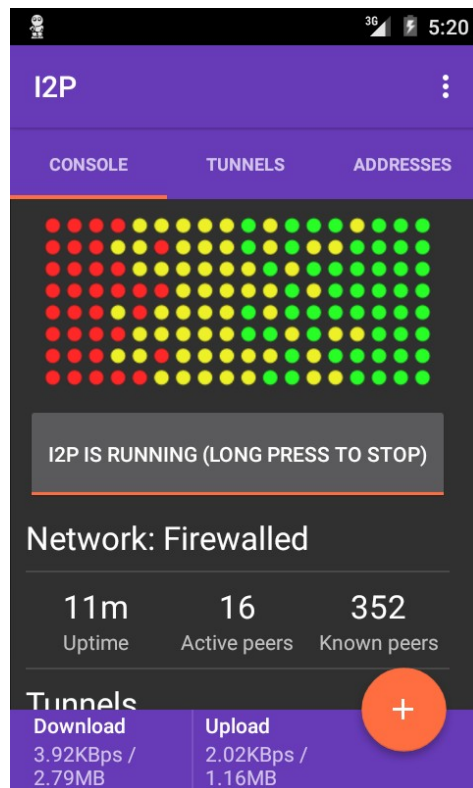
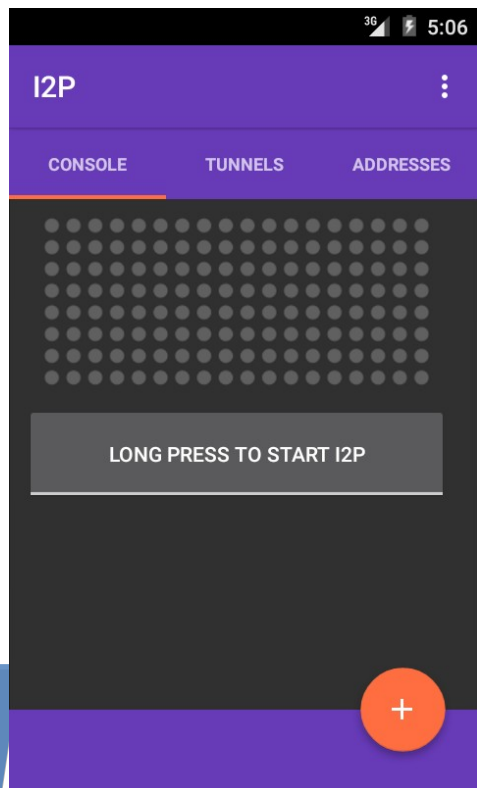
- Routers



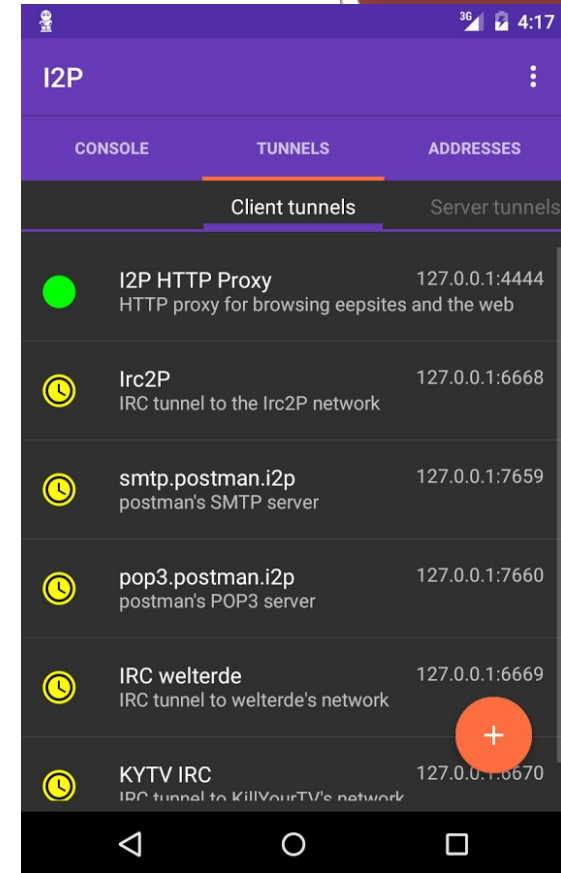
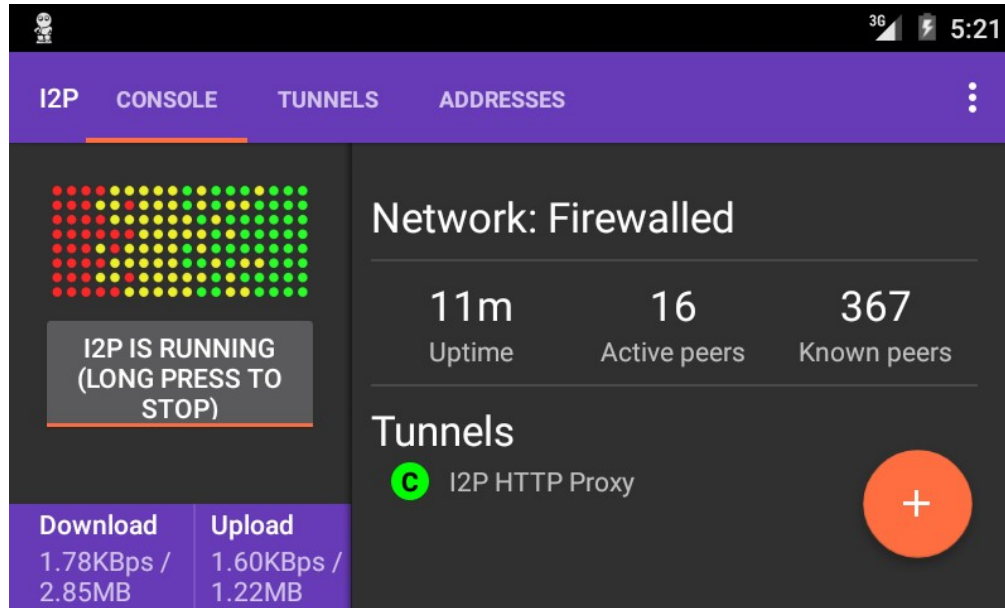
- Android



Aplicación Android



Aplicación Android

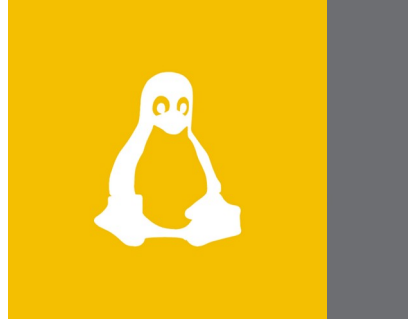


Requisitos de instalación

Java Runtime Version 7 or higher.

(Oracle, OpenJDK, or IcedTea Java Version 7 or 8 recommended, except
Raspberry Pi: Oracle JDK 8 for ARM, PowerPC: IBM Java SE 7 or 8)

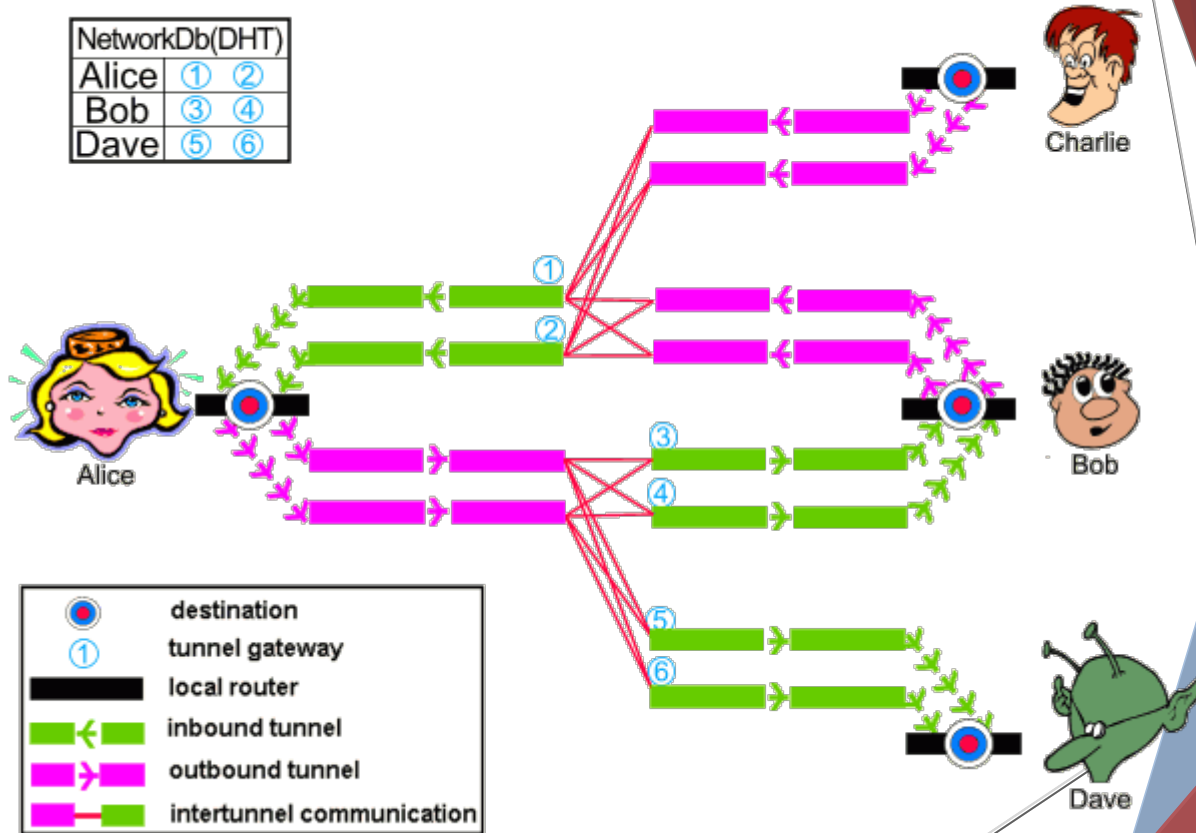
¿Dónde se puede instalar?



Funcionamiento básico

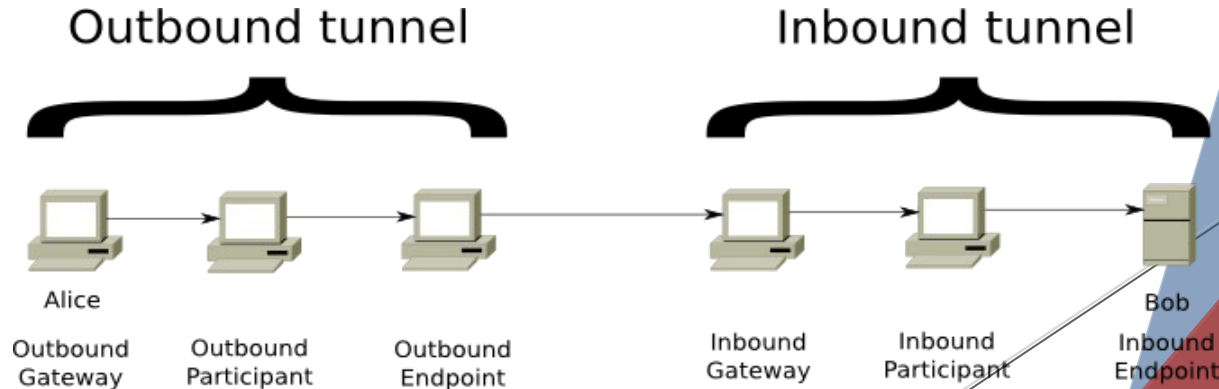
- Red P2P formada por routers y destinos.
- Un router es cualquier aplicación que haga uso de la red, ya sean de usuario o de servidor.
- Los routers se conectan entre sí mediante túneles unidireccionales (entrada o salida) y acaban en un destino.
- Los usuarios normalmente tienen varios destinos, como webs anónimas, torrents etc.

NetworkDb(DHT)		
Alice	①	②
Bob	③	④
Dave	⑤	⑥



Túneles

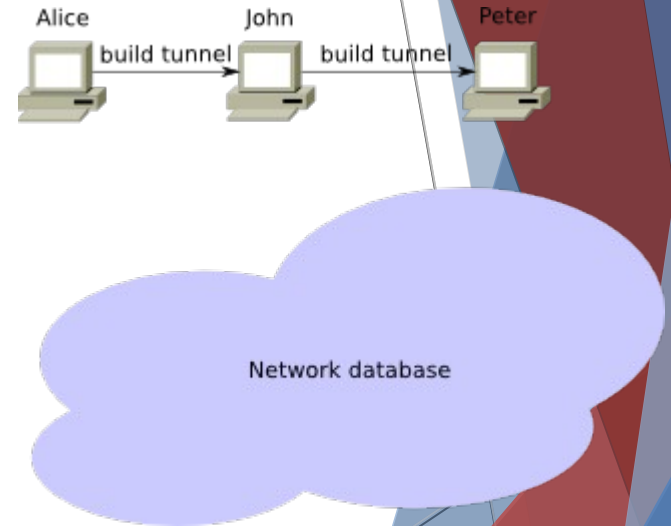
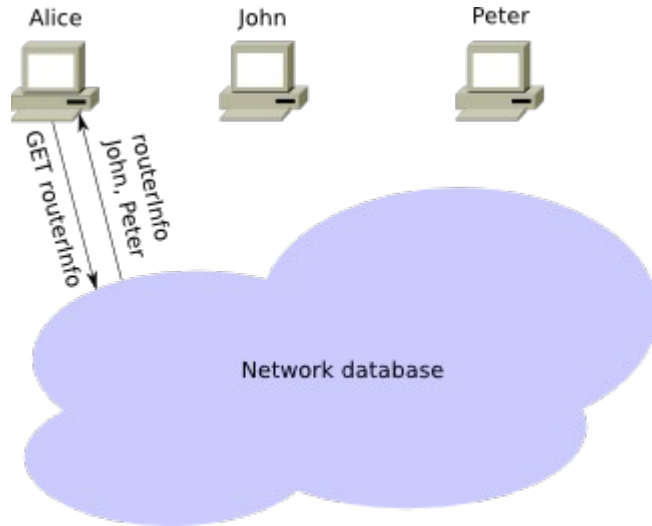
- Camino entre un grupo de routers.
- Cada túnel tiene un punto de inicio o gateway y punto final.
- Dos tipos, entrada y salida.
- Cifrado por capas, cada “paquete” contiene la ip del siguiente router y la información cifrada.



Base de datos de la red

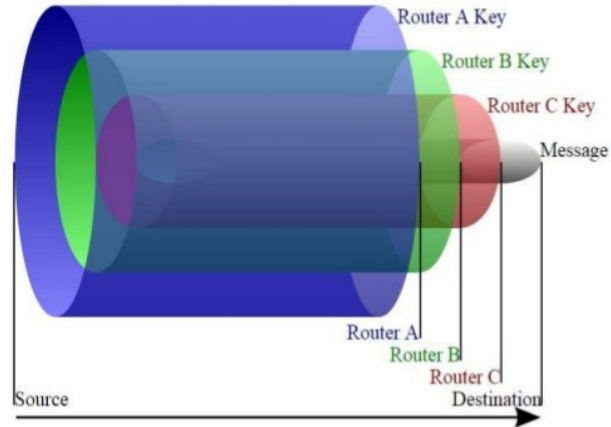
- Base de datos distribuida cuyo objetivo es compartir los metadatos de la red.
- Almacena dos tipos de datos:
 1. routerInfo: Claves públicas, dirección de transporte
 2. leaseSets: Gateway, Tiempo de caducidad del túnel, Par de claves públicas para poder cifrar el mensaje

Base de datos de la red

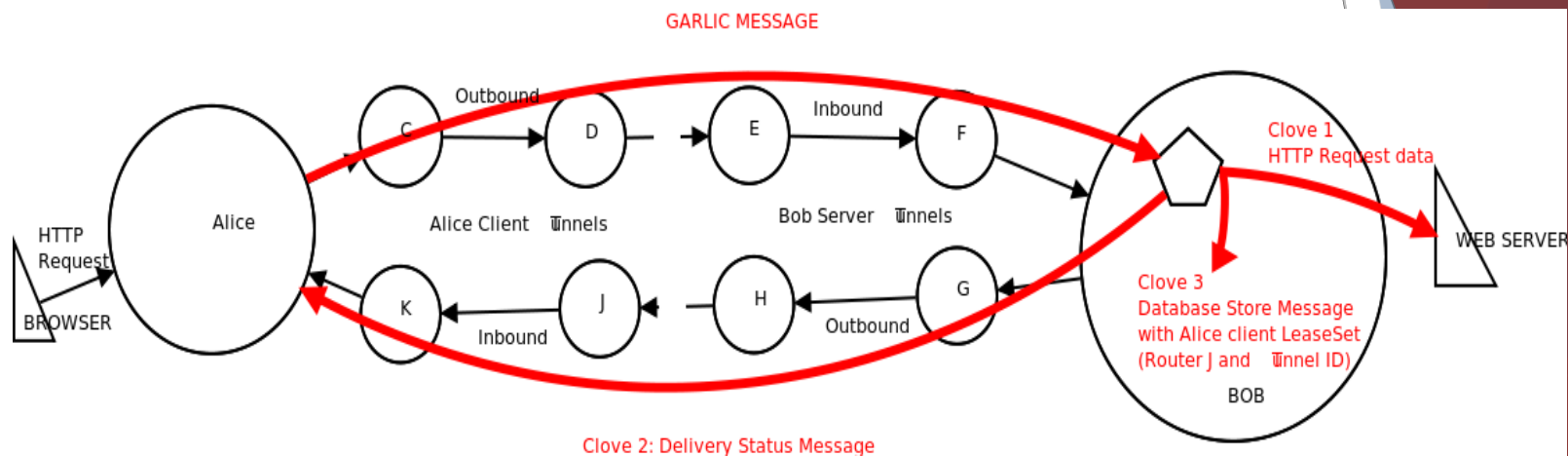


Garlic routing

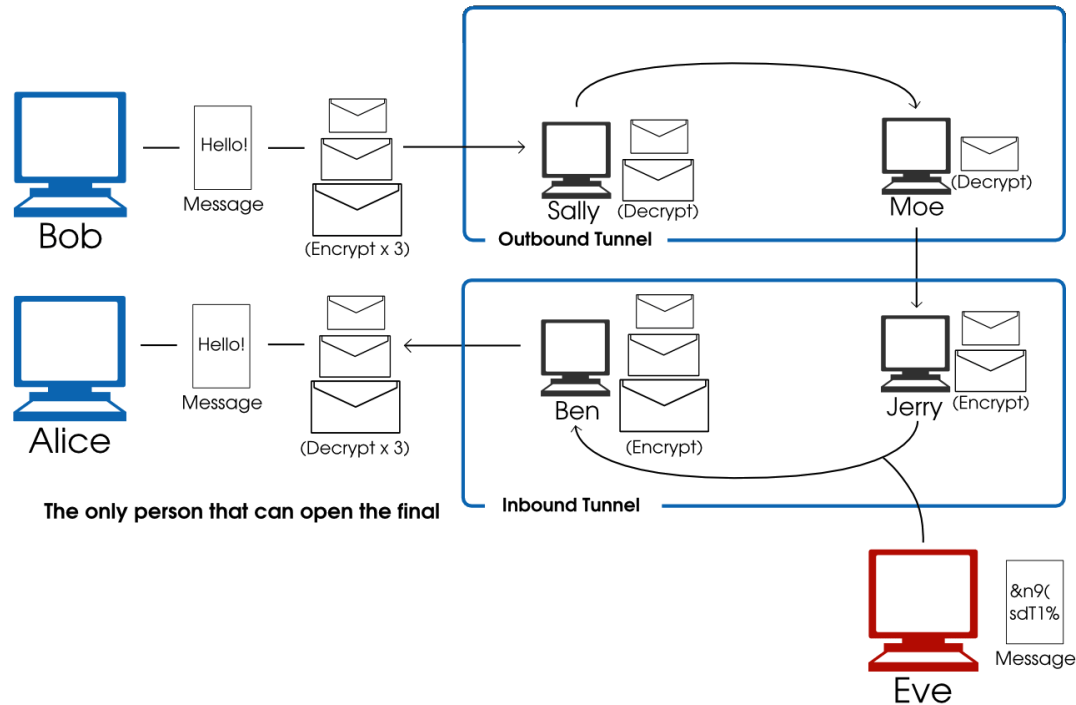
- Variación del Onion routing de tor
- Encripta grupos de mensajes para dificultar ataques e incrementar la velocidad



Garlic routing



Envío de un mensaje a través de I2P



Tutorial

- Descargar desde:
<https://geti2p.net/es/download>
- Ejecutar e instalar.
- Iniciar con:
`~/i2p/i2prouter start`

Tutorial

The image shows a web browser window displaying the I2P router console interface and a terminal window showing the command to start the I2P service.

Consola del router I2P - página principal - Mozilla Firefox

Consola del router I2P - p X Consola del router I2P - p X +

127.0.0.1:7657/home

I2P

Versión: 0.9.32-0
Duración De La Conexión: 5 s

ANCHO DE BANDA ENTRANTE/SALIENTE

3 S: 0.99 / 3.25 KBps
Usados: 2.99 KB / 9.50 KB

Red: Probando

TÚNELES LOCALES

ninguno

CONSOLA DEL ROUTER I2P

7/11/17 **VERSIÓN 0.9.32** 222

La 0.9.32 contiene varias correcciones en la consola del router I2P y las aplicaciones web asociadas (addressbook, i2psnark, y susimail). También hemos cambiado la forma en la que manejamos los nombres de servidor configurados para las 'router infos' publicadas, para eliminar algunos ataques de enumeración de red vía DNS. Hemos añadido algunas comprobaciones en la consola para resistir ataques de reasociación (rebinding).

Como es habitual, recomendamos que actualice a esta versión. La mejor manera de mantener la seguridad y ayudar a la red, es ejecutar la última versión.

Última actualización de noticias hace 9 días. Última búsqueda de noticias hace 27 horas.

Ocultar noticias Mostrar todas las noticias

BIENVENIDO A I2P

APLICACIONES Y CONFIGURACIÓN



Administrar complementos	Ayuda	Configurar ancho de banda	Configurar interfaz de usuario
Consola del router I2P	Correo electrónico	Libreta de direcciones	Personalizar Barra lateral
Personalizar página principal	Servidor web	Torrents	

Terminal - arturo@arturo-VirtualBox: ~/i2p



```
arturo@arturo-VirtualBox:~/i2p$ ./i2prouter start
Starting I2P Service...
Waiting for I2P Service...
running: PID:1851
arturo@arturo-VirtualBox:~/i2p$
```




Tutorial

Aceptando túneles



TÚNELES LOCALES


 clientes compartidos 

 clientes diferentes (DSA) 

☒ Preferir IPv6 sobre IPv4

☐ Sólo usar IPv6 (deshabilitar IPv4) *(Experimental)*

Configuración UDP

 No desvele sus números de puerto a nadie, ya que se pueden usar para revelar su dirección IP.

Puerto UDP:

☐ Deshabilitar por completo *(seleccionar sólo si se encuentra tras un cortafuegos (firewall) que bloquea el UDP saliente)*

Configuración de TCP

Nombre del equipo (host) o dirección IP accesible desde el exterior:

☒ Utilizar dirección IP detectada automáticamente *(en la actualidad 92.56.127.61) si no está bloqueado por cortafuegos (firewall)*

☐ Utilizar siempre la dirección IP detectada automáticamente (no bloqueado por cortafuegos)

☐ Especificar nombre de equipo (host) o IP:


☐ Deshabilitar entrantes (bloqueado por cortafuegos)


☐ Deshabilitar por completo *(seleccionar sólo si está detrás de un cortafuegos (firewall) que regula o bloquea el TCP saliente)*

Puerto TCP accesible desde el exterior

☒ Usar el mismo puerto configurado para UDP *(en la actualidad 15937)*

☐ Especificar puerto:

 Cancelar

 Guardar cambios

Tutorial

Consola del router I2P - con X Nueva pestaña X +

127.0.0.1:7657/confignet#udpconfig

resolver problemas

PARES (PEERS)

Activo:	20 / 85
Rápido:	12
Alta Capacidad:	90
Integrado:	254
Conocidos:	327

TÚNELES

Exploratorios:	8
Cliente:	7
Participando:	0
Tasa De Compartición:	0,00

Rechazando túneles: Inicializando

TÚNELES LOCALES

clientes compartidos

☐ Deshabilitar entrantes (Bloqueado por firewall con NAT de grado proveedor-de-transporte o pasarela DS-Lite)

Configuración de IPV6

☐ Deshabilitar entrantes (Bloqueado por firewall con NAT de grado proveedor-de-transporte o pasarela DS-Lite)

☐ Deshabilitar IPV6


☐ Habilitar IPV6

☐ Preferir IPv4 sobre IPv6

☒ Preferir IPv6 sobre IPv4

☐ Sólo usar IPv6 (deshabilitar IPv4) (*Experimental*)

Configuración UDP

 No desvele sus números de puerto a nadie, ya que se pueden usar para revelar su dirección IP.

Puerto UDP:

☐ Deshabilitar por completo (*seleccionar sólo si se encuentra tras un cortafuegos (firewall) que bloquea el UDP saliente*)

Configuración de TCP

Nombre del equipo (host) o dirección IP accesible desde el exterior:

☒ Utilizar dirección IP detectada automáticamente (*en la actualidad 92.56.127.61*) si no está bloqueado por cortafuegos (firewall)

☐ Utilizar siempre la dirección IP detectada automáticamente (no bloqueado por cortafuegos)

☐ Especificar nombre de equipo (host) o IP:

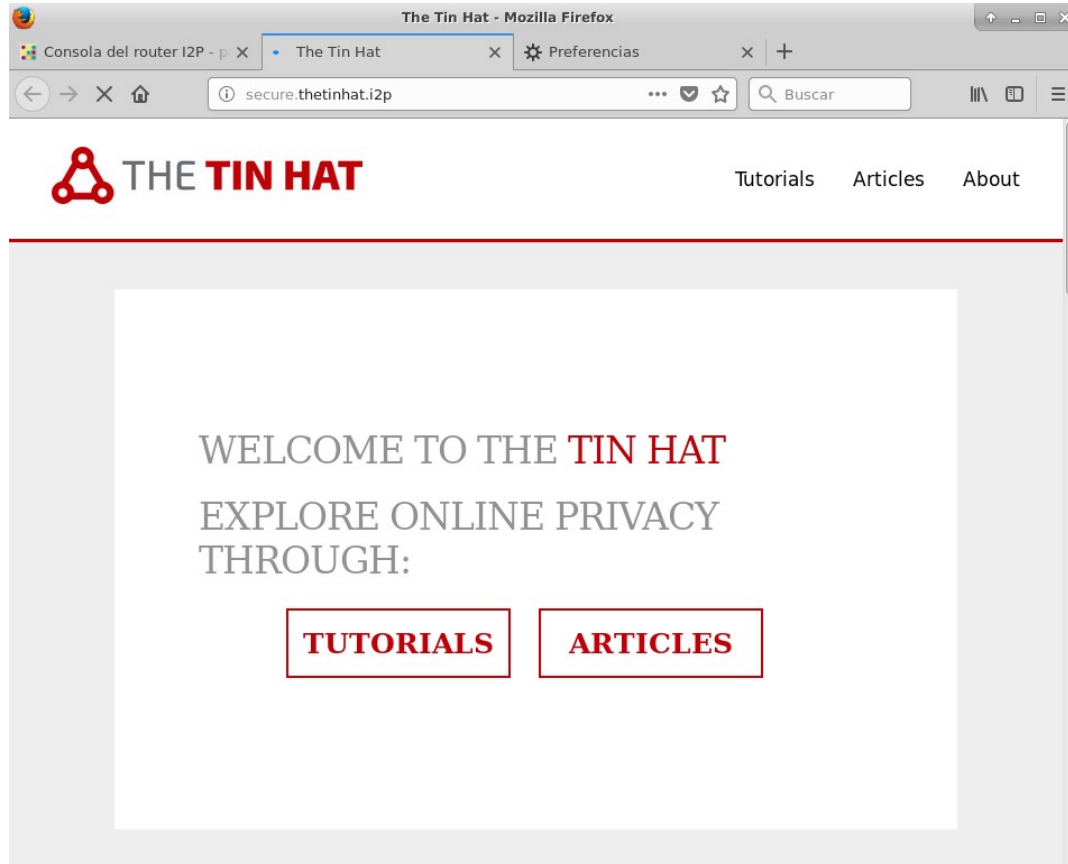
☐ Deshabilitar entrantes (bloqueado por cortafuegos)

☐ Deshabilitar por completo (*seleccionar sólo si está detrás de un cortafuegos (firewall) que regula o bloquea el TCP saliente*)

Tutorial



Tutorial



prueba3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
954	117.251901890	24.98.138.77	10.0.2.15	UDP	1136	33783 → 17428 Len=1094
955	117.265939628	24.98.138.77	10.0.2.15	UDP	1135	33783 → 17428 Len=1093
956	117.267492308	24.98.138.77	10.0.2.15	UDP	1135	33783 → 17428 Len=1093
957	117.268828446	24.98.138.77	10.0.2.15	UDP	1131	33783 → 17428 Len=1089
958	117.316829312	10.0.2.15	37.192.101.248	UDP	105	17428 → 45381 Len=63
959	117.319305799	10.0.2.15	93.27.234.30	UDP	1131	17428 → 13508 Len=1089
960	117.666790340	93.27.234.30	10.0.2.15	UDP	141	13508 → 17428 Len=99
961	117.867506366	10.0.2.15	24.98.138.77	UDP	214	17428 → 33783 Len=172
962	117.913046876	10.0.2.15	89.255.94.161	TCP	1110	41310 → 15155 [PSH, ACK] Seq=41905 Ack=1169 W...
963	117.913156195	89.255.94.161	10.0.2.15	TCP	60	15155 → 41310 [ACK] Seq=1169 Ack=42961 Win=65...
964	118.015983307	10.0.2.15	89.255.94.161	TCP	1110	41310 → 15155 [PSH, ACK] Seq=42961 Ack=1169 W...
965	118.016166471	89.255.94.161	10.0.2.15	TCP	60	15155 → 41310 [ACK] Seq=1169 Ack=44017 Win=65...
966	118.073778071	10.0.2.15	93.27.234.30	UDP	1143	17428 → 13508 Len=1101
967	118.304761581	10.0.2.15	93.27.234.30	UDP	1140	17428 → 13508 Len=1098
968	118.657241918	34.231.150.157	10.0.2.15	TCP	1110	19621 → 57148 [PSH, ACK] Seq=21121 Ack=1 Win=...
969	118.657261682	10.0.2.15	34.231.150.157	TCP	54	57148 → 19621 [ACK] Seq=1 Ack=22177 Win=65535...
970	118.657296522	24.98.138.77	10.0.2.15	UDP	1138	33783 → 17428 Len=1096

▼ Ethernet II, Src: PcsCompu 43:34:4b (08:00:27:43:34:4b), Dst: RealtekU 12:35:02 (52:54:00:12:35:02)

- Destination: RealtekU 12:35:02 (52:54:00:12:35:02)
- Source: PcsCompu 43:34:4b (08:00:27:43:34:4b)
- Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 24.98.138.77

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 200
- Identification: 0x0c81 (3201)
- Flags: 0x02 (Don't Fragment)
- Fragment offset: 0
- Time to live: 64
- Protocol: UDP (17)
- Header checksum: 0x7ee6 [validation disabled]
- [Header checksum status: Unverified]
- Source: 10.0.2.15
- Destination: 24.98.138.77
- [Source GeoIP: Unknown]
- [Destination GeoIP: United States, Cartersville, GA, AS7922 Comcast Cable Communications, Inc., 34.218700, -84.853996]

▼ User Datagram Protocol, Src Port: 17428, Dst Port: 33783

- Source Port: 17428
- Destination Port: 33783
- Length: 180
- Checksum: 0xaf83 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 3]

▼ Data (172 bytes)

- Data: 46fdef31585b86b1790e1ac98b75dada878702a30a12b86c...
- [Length: 172]

```
0000 52 54 00 12 35 02 08 00 27 43 34 4b 08 00 45 00 RT..5... 'C4K..E.
0010 00 c8 0c 81 40 00 40 11 7e e6 0a 00 02 0f 18 62 ....0.0. ....b
0020 8a 4d 44 14 83 f7 00 b4 af 83 46 fd ef 31 58 5b .MD.....F.1X[
0030 86 b1 79 0e 1a c9 8b 75 da da 87 87 02 a3 0a 12 .Y..U.....)
0040 b8 6c 78 ca 4d b4 43 00 42 80 23 40 cf 29 c9 76 .lv.M.C. B.#0..v
0050 85 d7 e2 69 44 b5 43 be 76 54 83 7e 9b 60 82 02 ....l.C. VT...
0060 e9 80 ab d6 90 0a 49 f5 db 83 4a 4a 8d a6 f6 4c ....l. ...J...L
```

prueba3 Packets: 4210 · Displayed: 4210 (100.0%) · Load time: 0:0.28 Profile: Default