Internet: Una Breve introducción

Privacy Coffee VI – 2020-02-21

CC BY NC SA

Acerca de Críptica

- Asociación cultural fundada en 2015
- Sin ánimo de lucro
- Eventos, materiales y formaciones de privacidad
  - Herramientas seguras (Seguridad Instrumental)
  - Hábitos seguros (Seguridad Operacional)
- Filosofía (sin orden concreto):
  - Código abierto
  - Usabilidad
  - Descentralización
  - Seguridad por defecto
- El año pasado publicamos el libro *Resistencia Digital*

:~$ whoami

- Ingeniero de Telecos
- Miembro de Críptica
- Coautor del libro *Resistencia Digital*
- Analista de seguridad informática: Equipo rojo
- *Just call me Charlie*

¿Por qué esta charla?

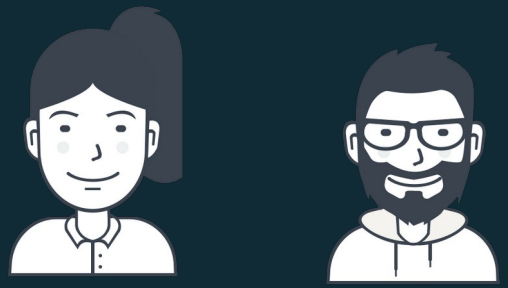
- Todo el mundo usa internet
- No todo el mundo sabe qué es
- Poca gente sabe cómo funciona
- ¡Entender cómo funciona nos ayuda a usarlo mejor!

¿Qué es internet?

- Primera parada: Wikipedia
- *Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen constituyan una red lógica única de alcance mundial.*
- ¿Redes de comunicación?¿Protocolos?¿Redes físicas heterogéneas?¿Conjunto descentralizado?

Empecemos de cero: Comunicación

Comunicar consiste en intercambiar información:
Alice y Bob están uno frente al otro y quieren hablar entre ellos: ¿Qué necesitan?

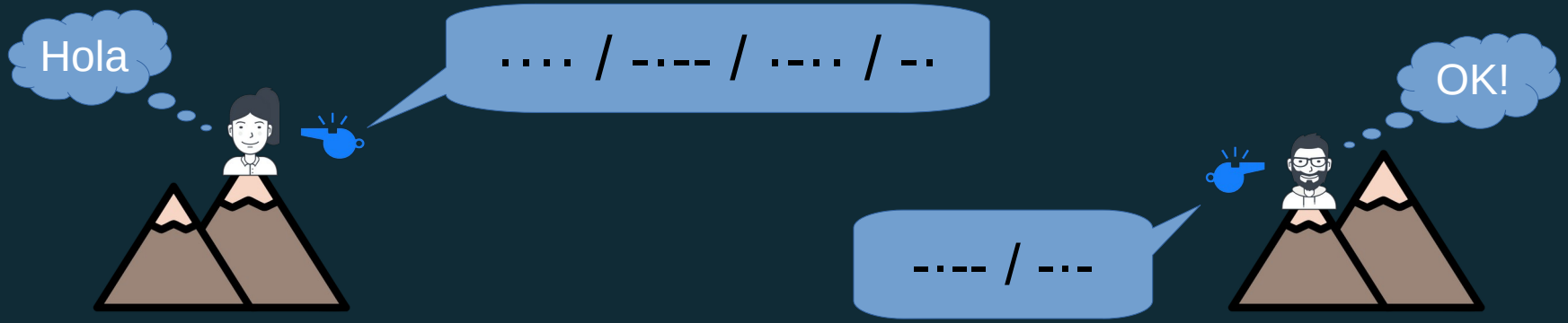


Con hablar el mismo idioma, es suficiente. Ya pueden comunicarse

https://www.iconfinder.com/iconsets/user-avatars-1

Empecemos de cero: Comunicación

Ahora, Alice y Bob están cada uno en una montaña y tienen un silbato cada uno

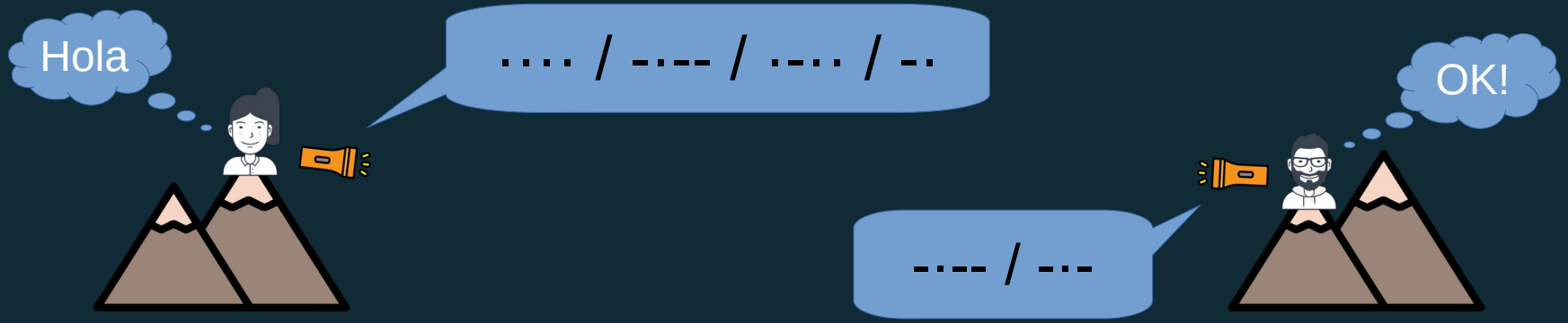


Pueden codificar sus mensajes en código Morse y usar los pitidos para transmitir el morse.
Pitido corto = Punto
Pitido largo = Raya

https://www.iconfinder.com/iconsets/adventure-and-camping-colored-lineal-style
https://www.iconfinder.com/iconsets/hawcons

Empecemos de cero: Comunicación

Cae la noche, hace viento y hay mucho ruido, pero Alice y Bob tienen linternas



¡Usarán el mismo código morse! Pero usarán un medio físico distinto: La luz
Flash corto = Punto
Flash largo = Raya

Empecemos de cero: Comunicación

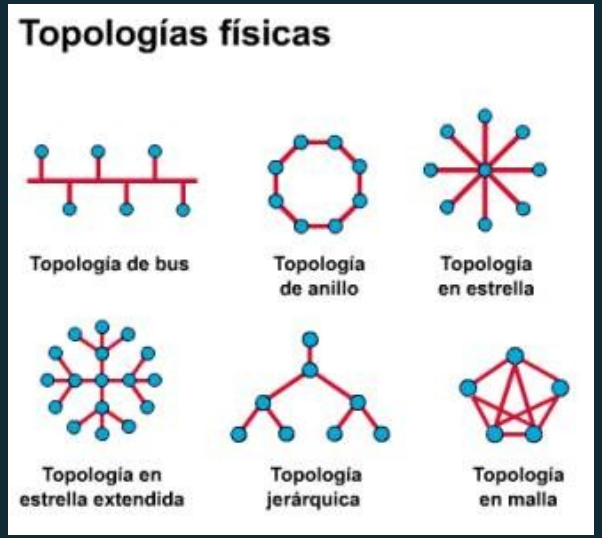
- Alice y Bob tendrán que ponerse de acuerdo en una serie de normas
- ¿Cómo hacen para no hablar a la vez?¿Cuanto rato habla cada uno?
- ¿Cómo confirman que han recibido la información sin errores?
- ¿Cómo le indica Alice a Bob que tiene que reenviarle el mensaje a Charlie, que está en una montaña más lejana?
- En definitiva, Alice y Bob tienen que seguir un protocolo de comunicación

Comunicación entre máquinas

- Las máquinas también han de codificar la información tanto para almacenarla y enviarla.
- En vez de puntos y rayas, utilizan ceros y unos
- Tienen que hablar usando las mismas normas (protocolos)
- Codifican los ceros y unos de muchas maneras:
  - Señales eléctricas en un cable
  - Señales de luz en fibra óptica
  - Ondas electromagnéticas en el aire...

Red de comunicaciones

- Una red de comunicaciones es un conjunto de dispositivos enlazados entre ellos, de forma que pueden comunicarse.
- La distribución de conexiones se conoce como topología



Protocolos: Vamos a echarle imaginación

- Un país imaginario en el que no existe internet, ni teléfono.
- En este país, la gente adora el correo postal y lo utiliza para todo.
- Se puede acceder a muchos servicios a través del correo postal.
- El correo funciona un poco distinto de lo que estamos acostumbrados.
- Vamos a verlo

El correo del país imaginario

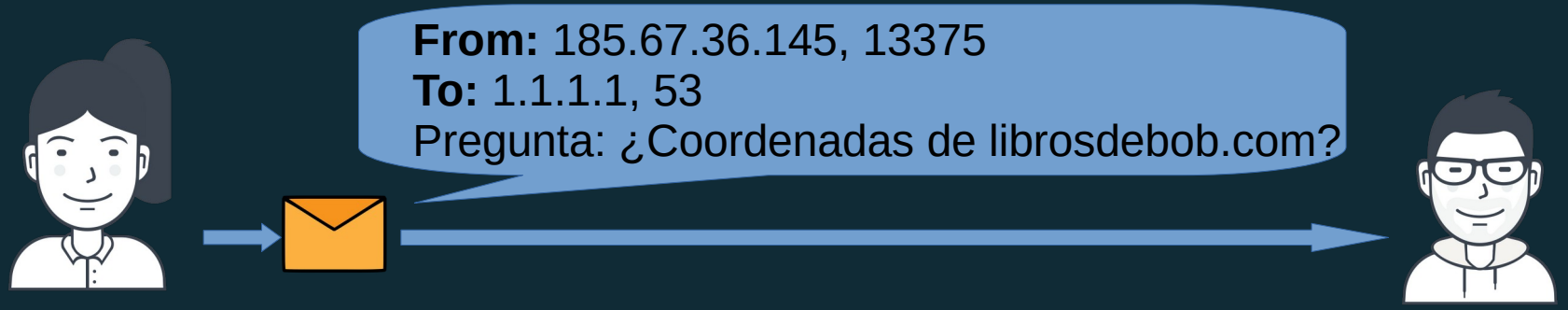
- Cada provincia gestiona el correo de forma independiente, no hay una compañía central
- Destinatario: Coordenada del edificio (159.69.16.135), n.º de puerta (443).
- Remitente: Coordenada del edificio (104.74.140.223), n.º de puerta (13375)
- La gente no se sabe de memoria las coordenadas de los edificios, pero sí que conoce los nombres.
- En este país son muy cuadriculados: Cada servicio se puede usar con una serie de formularios distintos. Hay que usar los formularios adecuados para cada servicio.

Círculo de lectores en el país imaginario

- Bob tiene un servicio de entrega de libros por correo
- Alice quiere pedirle la lista de libros.
- Viven en provincias distintas, pero con el correo, todo es posible.

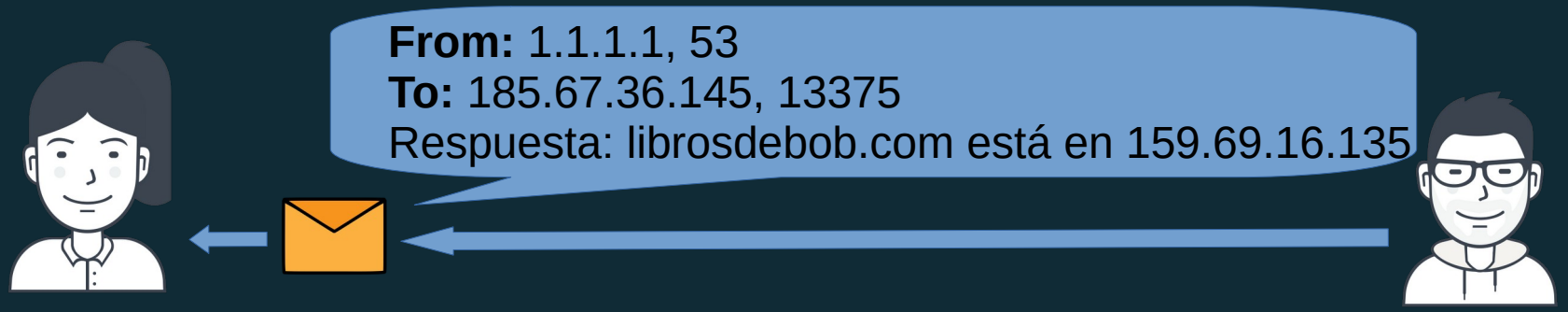
Círculo de lectores en el país imaginario

- Alice le tiene que mandar una carta a Bob, conoce el nombre de su edificio (librosdebob.com) pero no conoce sus coordenadas.
- Dani ofrece un servicio que se encarga de solucionar este problema, Alice solo necesita conocer las coordenadas de Dani y utilizar un formulario para preguntar cuales son las de Bob.



Círculo de lectores en el país imaginario

- Dani responde rápidamente a la carta de Alice
- Ahora Alice ya puede mandar la carta a Bob y consultar la lista de libros.



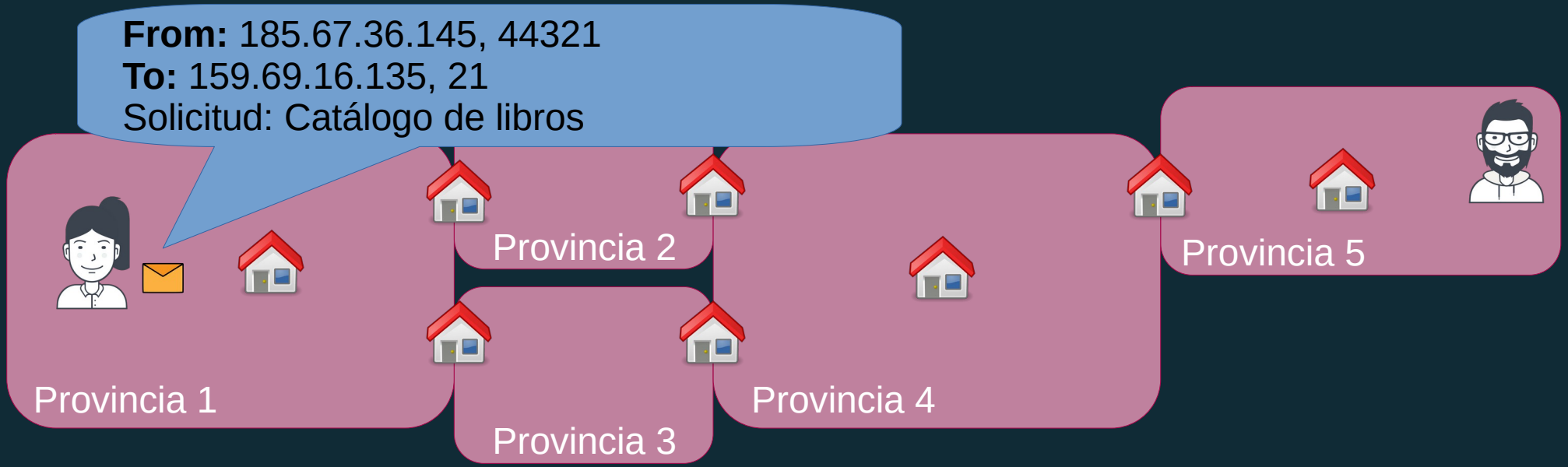
Círculo de lectores en el país imaginario

- Alice ya puede hacerle la petición a Bob.
- Rellena el formulario del servicio de Bob y lo manda por correo a las coordenadas 159.69.16.135
- Indica la puerta 21, que es la estándar para el servicio de Bob.

https://www.iconfinder.com/iconsets/tango-icon-library

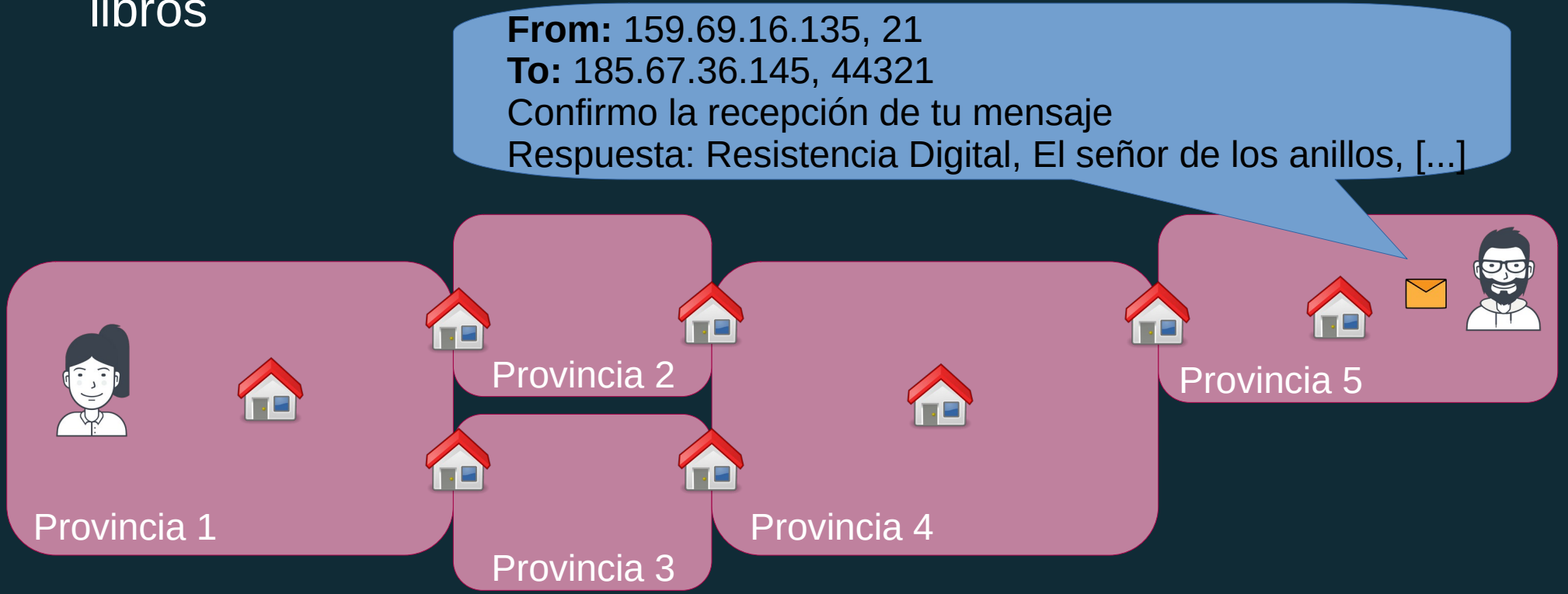
Círculo de lectores en el país imaginario

- Cada provincia tiene varias oficinas de correos.
- Aunque no sepan donde están las coordenadas exactas, saben en qué dirección tienen que mandarlo, para que llegue



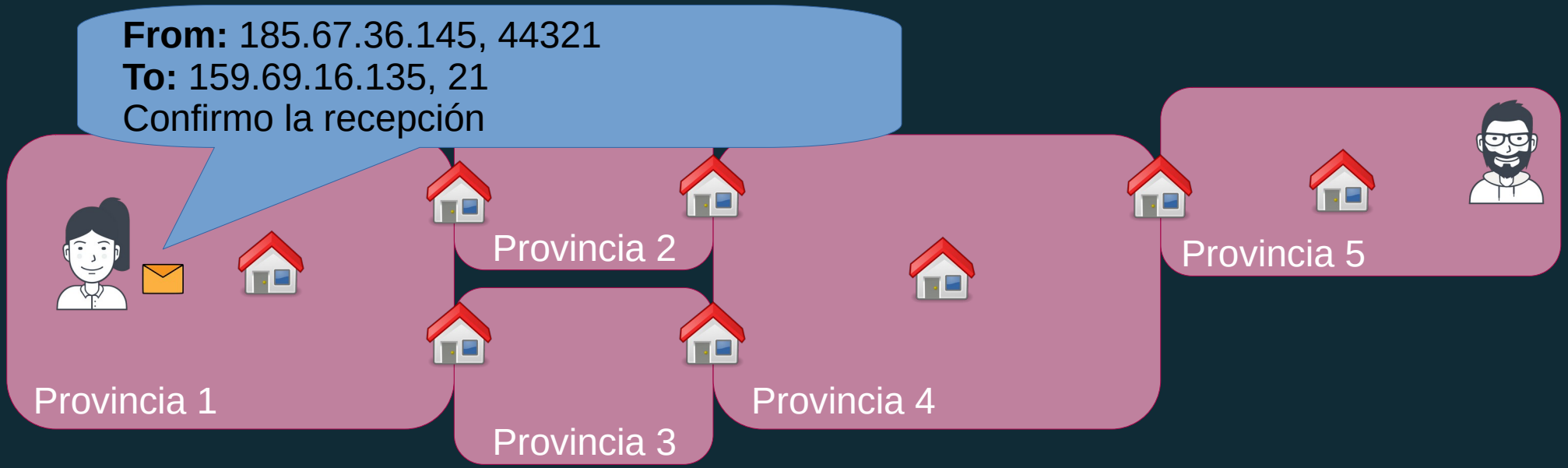
Círculo de lectores en el país imaginario

- Bob procesa la solicitud de Alice y le contesta con la lista de libros



Círculo de lectores en el país imaginario

- Alice contesta con una carta confirmando la recepción correcta (Acuse de recibo)



Círculo de lectores en el país imaginario

- Usando este sistema, Alice puede ir solicitando libros a Bob y Bob se los puede ir enviando.

Círculo de lectores en el país imaginario

- Si el libro no cabe en una carta no pasa nada! Bob lo trocea, lo manda en varias cartas y Alice ya lo reconstruirá
- Alice confirma la recepción de cada carta, si alguna no es confirmada, Bob la reenvía.

TCP/IP

- Internet funciona de forma parecida
- El protocolo IP es el encargado de hacer llegar los mensajes a las máquinas
- El protocolo TCP es el encargado de garantizar la entrega al servicio correcto

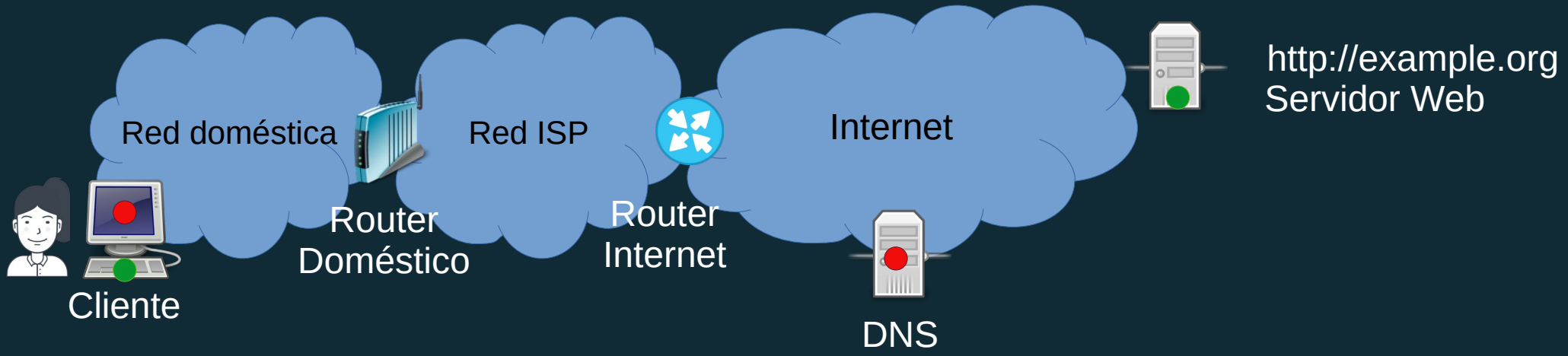
TCP/IP: Metáforas

- Las oficinas de correo son los *routers* de internet
- Las coordenadas son direcciones IP
- Las puertas de cada servicio son puertos TCP
- Los formularios que intercambian Alice, Bob y Dani son protocolos de aplicación
- Dani es un servidor de DNS: traduce los nombres de dominio a direcciones IP
- Hay infinidad de protocolos que se pueden usar sobre TCP/IP:
  - Web: HTTP, HTTPS
  - Correo: SMTP, IMAP, POP3
  - Transferencia de ficheros: FTP, FTPS
  - Administración remota: SSH, RDP….

Usuarios y usuarias

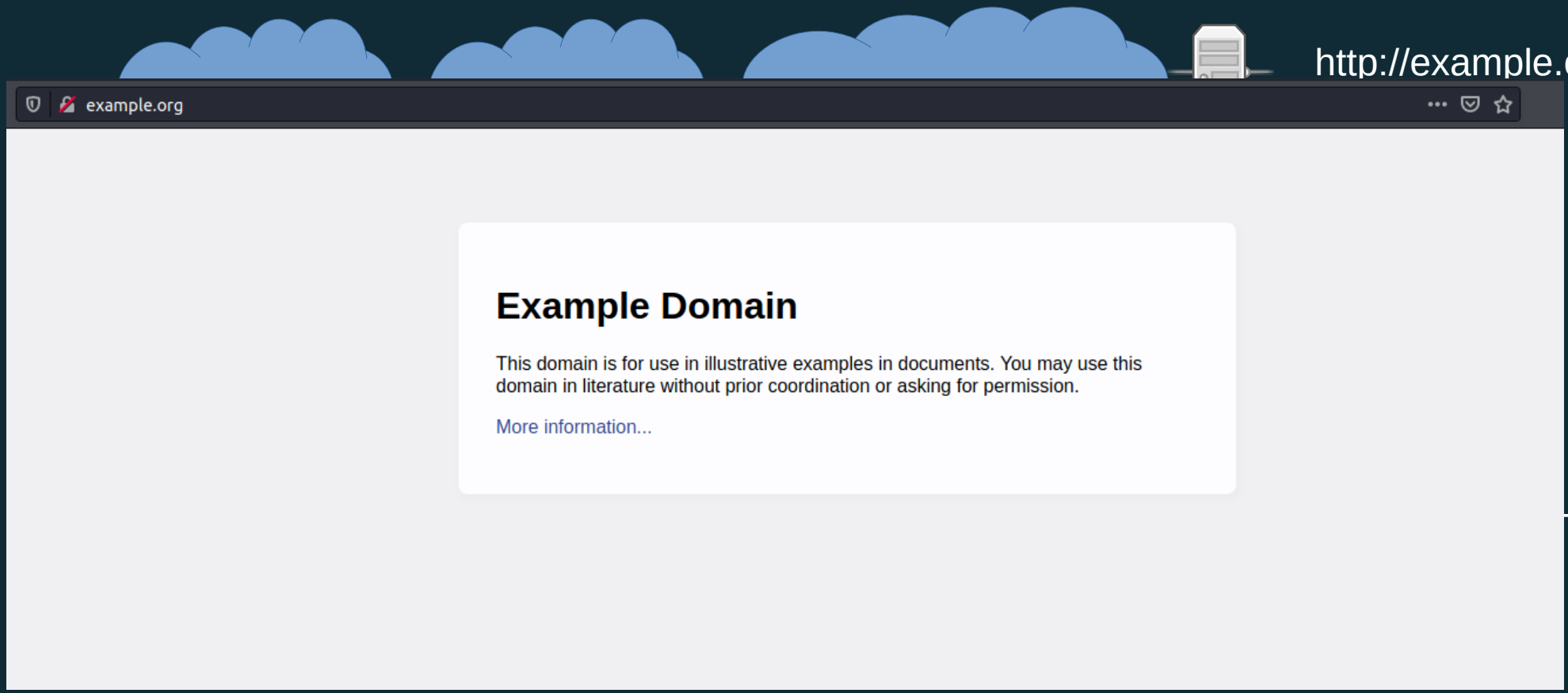
- Accedemos a internet a través de un proveedor (AKA compañía telefónica)
- El proveedor asigna una dirección IP pública a nuestro *router* doméstico, que nos hace de intermediario con internet.
- Los dispositivos de nuestra red doméstica también tienen direcciones IP, pero son privadas.
- Esto significa que nadie puede mandarnos paquetes a nuestros dispositivos desde internet usando esas direcciones.

¿Qué pasa cuando visitamos una web?



1. El navegador web consulta al servidor DNS para saber cual es la IP de example.org
2. El DNS contesta diciendo que example.org tiene la dirección 93.184.216.34
3. El navegador envía una petición al puerto 80 de 93.184.216.34 usando el protocolo HTTP
4. El servidor contesta usando el protocolo HTTP con el contenido de la página
5. El navegador interpreta la información recibida (HTML, CSS, JavaScript) y nos la muestra

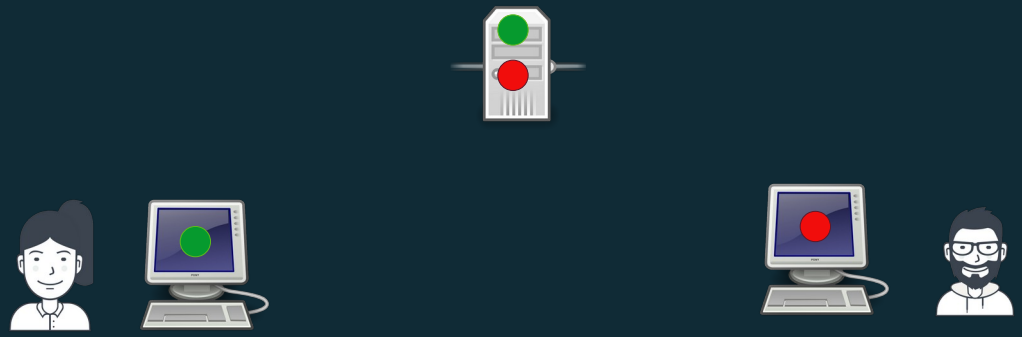
¿Qué pasa cuando visitamos una web?



Comentarios

- Al usar DNS y HTTP los paquetes viajan en claro: Todas las máquinas que esten en el camino pueden ver su contenido
- Si usamos HTTPS protegemos criptográficamente el contenido de las peticiones y las respuestas del servidor
- Al visitar una página, realmente no la estamos visitando, nos la estamos descargando!
- El servidor web conocerá nuestra IP pública y otros datos que le envía el navegador con la petición.
- Muchas veces las páginas contienen recursos de otros servidores, y nuestro navegador solicita estos recursos de forma transparente.

¿Qué pasa cuando enviamos un mensaje instantáneo?



- Los mensajes son enviados a un servidor central
- Para recibirlos, la aplicación de mensajería consulta el servidor y descarga los mensajes
- Si no usamos un chat seguro (e2e) el servidor tiene una copia en claro de nuestros mensajes!
- Además tiene una copia de nuestros contactos, sabe cuando hablamos con quién, con qué frecuencia, en qué grupos estamos…
- Centralizado y no interoperable (generalmente): No se puede mandar un Whatsapp a Telegram

¿Qué pasa cuando enviamos un e-mail?

gmail.com

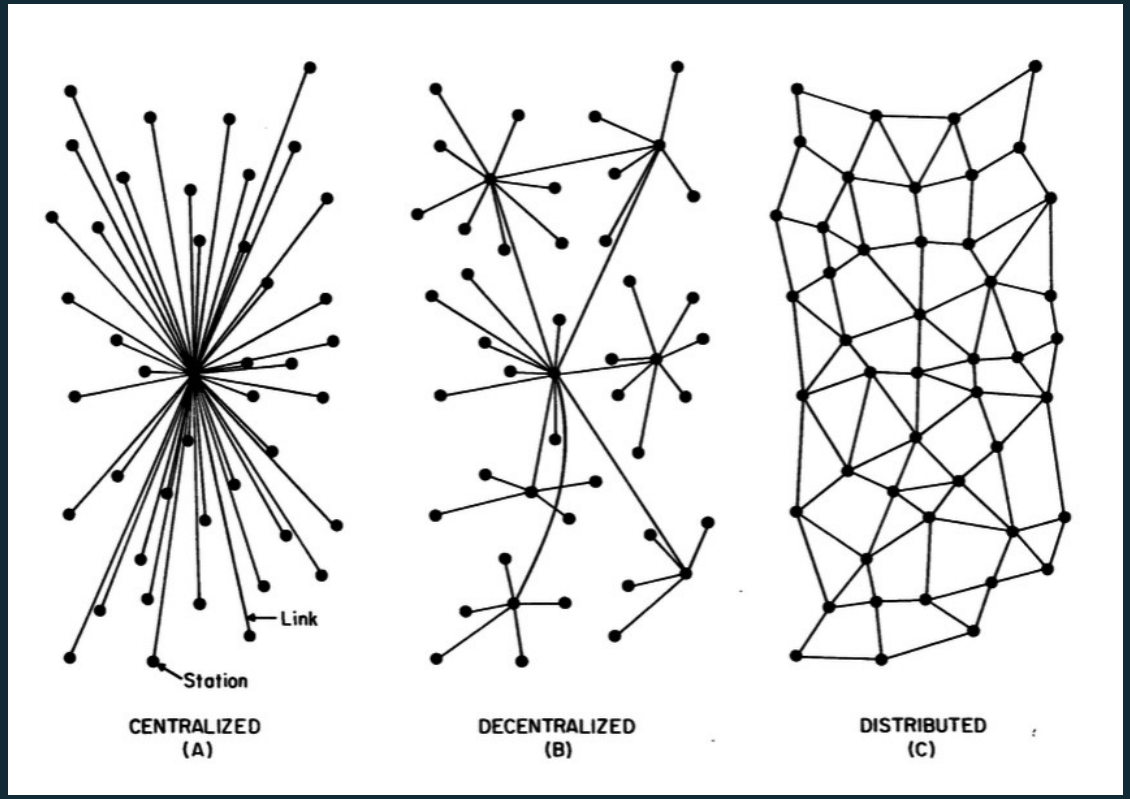
posteo.net

alice@gmail.com

bob@posteo.net

- Los correos son enviados a nuestro proveedor de correo
- Nuestro proveedor envia el correo al proveedor de nuestro destinatario
- El destinatario se descarga el correo de su proveedor
- Los proveedores pueden ver el contenido del correo y guardan una copia
- Federado e interoperable: Podemos escoger el proveedor que deseemos y enviar mensajes a otros proveedores.
- Incluso podemos ser nuestro propio proveedor

Niveles de centralización



Sistemas centralizados

- Pese a que internet es una infraestructura descentralizada, la mayoría de servicios que utilizamos están centralizados en unos pocos proveedores.
- Son aquellos servicios proporcionados por un solo proveedor.
- Ejemplos de servicios centralizados:
  - Tienda online: Amazon
  - Redes sociales: Twitter, Facebook, Instagram
  - Mensajería: Whastapp, Telegram, Signal

Sistemas federados

- Son aquellos servicios en los que podemos escoger un proveedor y comunicarnos con los usuarios de otros proveedores. No dependen de un único proveedor central
- Ejemplos de servicios federados:
  - Redes sociales: Mastodon, GNU Social, Diaspora
  - Mensajería: e-mail*, matrix, XMPP
- *El e-mail es federado, pero una inmensa mayoría de usuarios se concentra en un único proveedor: Google.

Sistemas distribuidos o P2P

- Son aquellos servicios en los que somos cliente y servidor a la vez, no dependemos de servidores centrales o federados.
- Ejemplos de servicios P2P:
  - Redes sociales: Retroshare
  - Web descentralizada: ZeroNet
  - Mensajería: Briar, Ricochet, Tox
  - Otros: Torrent, Syncthing

¿Que es internet?

- Revisitamos la definición de Wikipedia
- *Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen constituyan una red lógica única de alcance mundial.*
- Esperamos que con la ayuda de estas diapositivas, se entienda un poquito mejor :)

Gracias por vuestra atención

- Web: https://criptica.org
- Twitter: @CripticaOrg
- Canal de Telegram : t.me/cripticaorg
- Matrix: #criptica:matrix.org

CC BY NC SA