Trabajo Practico Redes

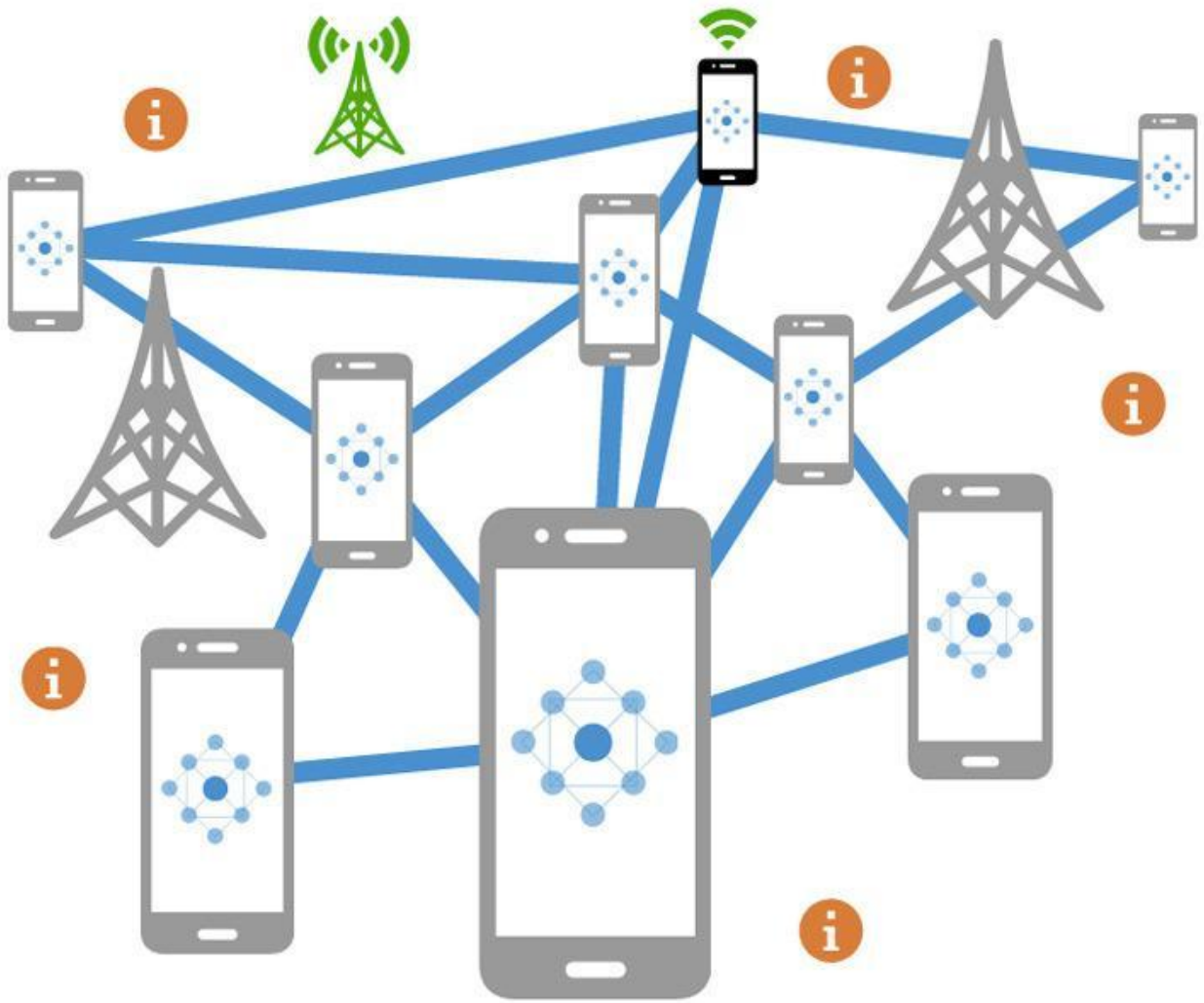
WhatsApp

Paiva Joaquin

Paiva Joaquin 6°T

¿Qué es una red?

Primero definamos que es una red; Una red son, mínimamente, 2 dispositivos conectados por medios físicos o inalámbricos que comparten datos.



¿Qué tipo de red es?

WhatsApp es una red de **mensajería instantáneo**, que es una forma de comunicación en tiempo real entre dos o más personas basada en texto. El texto es enviado a través de dispositivos conectados ya sea a una red como Internet, o datos móviles sin importar la distancia que exista entre los dos dispositivos conectados.

Introducción a WhatsApp

WhatsApp es una aplicación de chat para celulares, Sirve para enviar mensajes de texto y multimedia entre sus usuarios, cada usuario se identifica con su número de teléfono. Basta con saber el número de alguien para tenerlo en la lista de contactos de WhatsApp. Y Para hablar obviamente las 2 personas(emisor y receptor) tienen que tener instalada la app. Los mensajes se envían a través de la red hasta el teléfono de destino.

Ahora WhatsApp Técnicamente

Primero hablemos del registro que es particular, solo se necesita un numero de teléfono y un teléfono compatible.

Su funcionamiento se basa en el protocolo **FunXMPP**, una variante de XMPP que la propia compañía de WhatsApp desarrolló.

Antes de seguir escribiendo, expliquemos que es el protocolo XMPP.

XMPP (Protocolo extensible de mensajería y comunicación de presencia) es un protocolo abierto y extensible basado en XML, ideado para mensajería instantánea. Tiene ciertas ventajas y desventajas

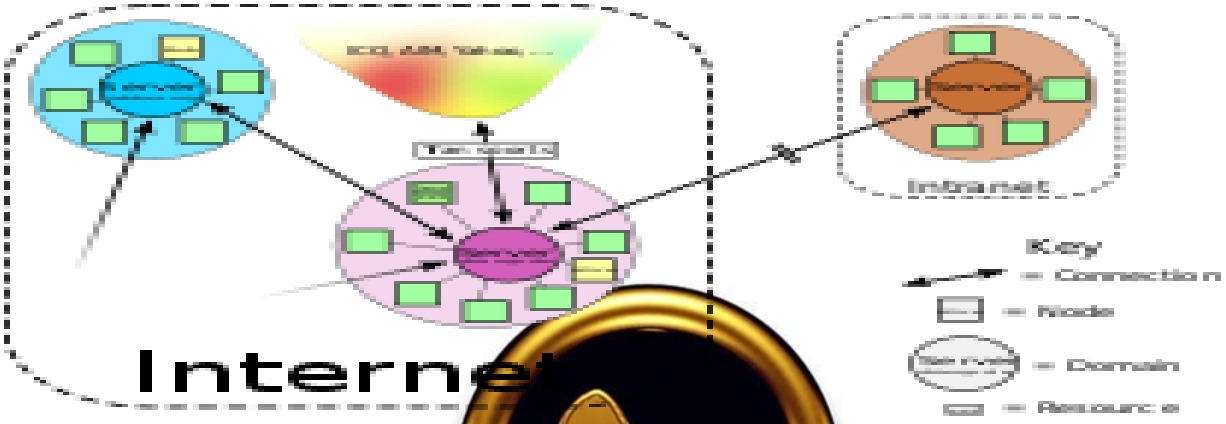
Ventajas

- **Descentralización:** La arquitectura de las redes XMPP es similar a la del correo electrónico; cualquiera puede poner en marcha su propio servidor XMPP, sin que haya ningún servidor central.
- **Estándares abiertos**
- **Seguridad:** Los servidores XMPP pueden estar aislados de la red pública XMPP, y poseen robustos sistemas de seguridad (como SASL y TLS).
- **Flexibilidad**

Desventajas

- **Sobrecarga de datos de presencia**
- **Escalabilidad**
- **Sin datos binarios**

La red XMPP está basada en servidores, pero descentralizada; por diseño, no hay ningún servidor central



Bueno, la compañía desarrollo una variante para hacer que los mensajes que viajan entre los móviles de los usuarios tengan un peso menor. Gracias a esto el proceso de envío y recepción necesita menos recursos, tanto por parte de los usuarios, como por parte de la empresa que cada día debe gestionar miles de millones de mensajes.

El protocolo FunXMPP utiliza como sintaxis el lenguaje XML, *es un lenguaje de marcado que define un conjunto de reglas para la codificación de documentos, además simplifica el intercambio de datos, simplifica el cambio de plataforma, aumenta la disponibilidad de datos y se puede utilizar para crear nuevos idiomas de Internet.*

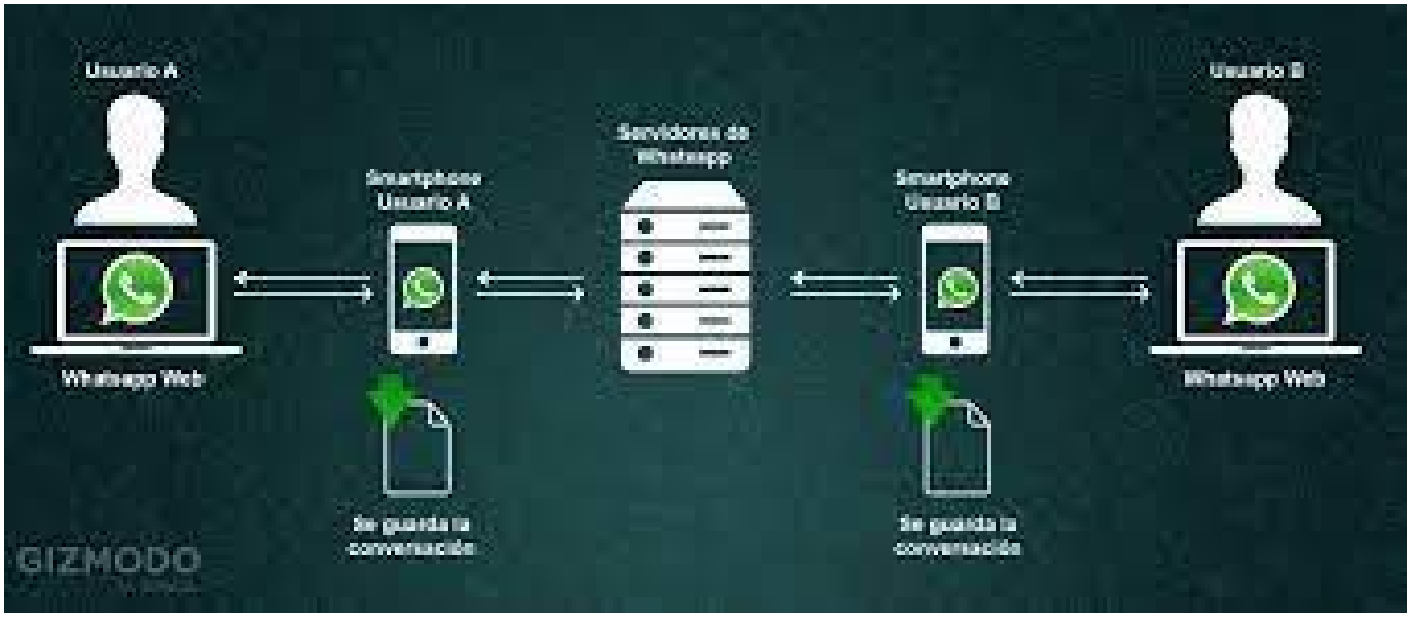
Este tipo de sintaxis genera un determinado formato con una serie de datos para cada mensaje que se envía desde el celular del usuario para que los servidores del servicio sepan en todo momento de qué dispositivo ha salido, a cuál se dirige, la fecha y hora de envío y también el mensaje en sí. Además, cada mensaje tiene un identificar único para que trabajar con él sea más sencillo.

```
<message from="01234567890@s.whatsapp.net"
         id="1339831077-7"
         type="chat"
         timestamp="1339848755">
    <notify xmlns="urn:xmpp:whatsapp"
            name="NcN" />
    <request xmlns="urn:xmpp:receipts" />
    <body>Hello</body>
</message>
```

```
<\x5d \x38="01234567890@\x8a"
      \x43="1339831077-7"
      \xa2="\x1b"
      \x9d="1339848755">
   <\x65 \xbd="\xae"
         \x61="NcN" />
   <\x83 \xbd="\xad" />
   <\x16>Hello</\x16>
</\x5d>
```

En estos archivos XML, es donde WhatsApp ha metido mano para reducir su peso y que todo el proceso de envío/recepción sea mucho más rápido; además de permitirles descongestionar sus servicios. A diferencia del protocolo original, **FunXMPP** no pone un nombre completo e identificable a cada variable que envía. En su lugar utiliza variables con formato xnn, donde las n son sustituidas por números.

Este tipo de archivos viajan encriptados desde el celular que envía hasta el que recibe acompañados de una serie de datos que le permitirá a WhastApp gestionarlos correctamente. Estos datos comienzan con la identificación de la versión del protocolo que utiliza y también con una solicitud de conexión a los servidores del servicio de mensajería. En este punto también se identifica el dispositivo desde el que fue enviado y la versión de la app instalada.



Una vez hecho esto, entra en juego el mecanismo de autenticación. Este proceso identifica al usuario y lo autoriza a enviar el mensaje al celular del receptor. Cuando este lo recibe, es desencriptado utilizando la clave que guarda el dispositivo y gracias al formato XML la app puede interpretar el mensaje y mostrarlo en la conversación correspondiente.

Cuando se envía una foto, un vídeo o cualquier otro tipo de contenido son cifrados con los sistemas Whisper y subidos al servidor HTTP de la herramienta y después son enviados al destinatario.

Seguridad

Cuando activas una cuenta en WhatsApp el servicio te asigna un nombre de usuario de forma automática, también asigna una contraseña de forma interna con la que reconoce el dispositivo. Inicialmente utilizaba el IMEI de los dispositivos y debido a la popularidad de los terminales Dual-SIM empezaron a utilizar la dirección MAC del chip WiFi. En la actualidad esto ha vuelto a cambiar y ahora utilizando un identificador único que generan los sistemas operativos de los celulares basados en el terminal sobre el que corra la app y el nombre del paquete de la misma.

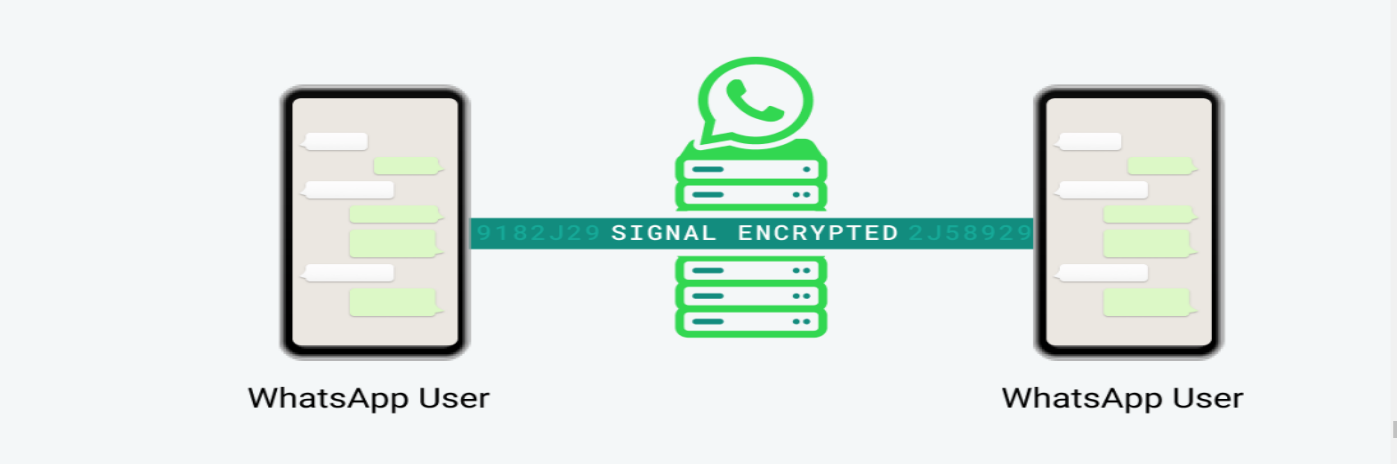
También esta el **proceso de activación,** nadie podrá activar una cuenta con tu número de teléfono sin acceso físico a tu dispositivo. Siempre necesitará conocer el código que WhatsApp envía por SMS o por llamada y éste siempre llegará a tu número de teléfono.

Conversaciones cifradas punto a punto

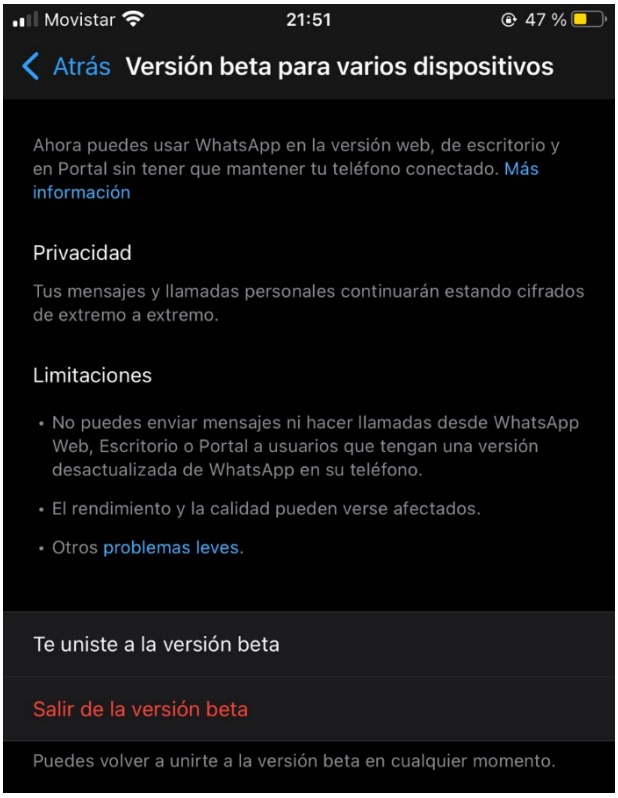
Gracias a esta medida, los mensajes, los archivos adjuntos, las llamadas de audio y las videollamadas son encriptados en el dispositivo emisor utilizando una clave de cifrado que cambia con cada uso, pasan por los servidores de WhatsApp y no son desencriptados hasta llegar al móvil de destino donde está la clave de desencriptado de los mensajes.

La compañía ha optado por no almacenar datos de forma prolongada salvo los referidos a las cuentas de usuarios y los estados de WhatsApp que están visibles durante 24 horas tras su publicación. El resto de los mensajes y archivos adjuntos se guardan en los servidores el tiempo mínimo necesario para ser entregados al usuario de destino y una vez entregados son borrados de los servidores.

Los servidores funcionan únicamente de intermediarios para realizar la transferencia de los datos y también para facilitar el contacto entre la cuenta del emisor y del receptor. Además, también intervienen para enviar notificaciones y las señales de confirmación necesarias para el check , doble check y check azul en caso necesario.



Ahora recientemente sacaron una versión beta de WhatsApp Web, donde por fin podés usar el escritorio sin tener que tener el celu cerca, basta con ir a conectar dispositivos y te sale para unirse al programa beta.



Bibliografia:

https://www.adslzone.net/esenciales/whatsapp/como-funciona/
https://www.fotonostra.com/digital/whatsapp.htm
https://www.fotonostra.com/digital/comunica.htm
https://www.altaruru.com/que-es-xmpp/
https://rockcontent.com/es/blog/que-es-xml/
https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-5&_nc_sid=2fbf2a&_nc_ohc=9A9qsWqU28YAX9N96Rc&_nc_ht=scontent.whatsapp.net&oh=6ac702a563d35d6ec79c476252e1de49&oe=61240A19