Universidad Tecnológica Nacional
Facultad Regional Buenos Aires

Actualización en Redes Convergentes

Autores: Horacio René Del Giorgio y Fabián Carino

Índice

Índice de Figuras

Índice de Tablas

1 Resumen

En este breve informe se abordarán temas que habitualmente se tratan en la asignatura “Redes Convergentes” correspondiente a la carrera de Ingeniería en Electrónica, de la Universidad Tecnológica Nacional, Facultad Regional Buenos Aires.

Los temas que se abordarán son: Paquetización de la Voz, Seguridad en Redes Convergentes, Multicast y Redes SDN.

Con todo esto, se pretende contribuir en la generación de conocimiento científico sobre los sistemas de valor agregado que se pueden desarrollar sobre Redes Convergentes.

2 Introducción

Las Comunicaciones, ya sea en los aspectos de Tecnologías de Comunicaciones, Provisión de Servicios, como en los aspectos de Fabricación, Operación, Mantenimiento y Comercialización, constituyen una parte muy importante del mercado laboral de los profesionales de las TIC (Tecnologías de la Información y la Comunicación).

La evolución que ha experimentado este campo en términos de tecnología y de servicios en el último tiempo impacta en la calidad de vida y en los negocios a nivel mundial.

La multiplicidad de recursos existentes y la necesidad de compatibilizarlos para su uso en una red convergente dan fundamento al desarrollo de asignaturas que brinden estos conocimientos a los futuros especialistas, de modo que puedan comprender las redes convergentes, ya que éstas constituyen la migración natural de redes tradicionales TDM a redes IP extremo a extremo distribuyendo en ese formato el tráfico: voz, datos y

video, desde el origen a destino y en una plataforma de telecomunicaciones unificada.

En ese sentido, este breve informe, realizado por la Cátedra de la Asignatura “Redes Convergentes” de la Universidad Tecnológica Nacional (FRBA), pretende enriquecer algunos temas que se dictan en la misma, tales como la Paquetización de la Voz, la Seguridad en Redes Convergentes, una introducción al Multicast y Redes SDN (Software Defined Networks, o en español, Redes Definidas por Software).

3 Paquetización de la Voz

La voz humana utiliza frecuencias entre 100Hz y 10.000Hz, pero la mayor parte de la energía se encuentra entre los 300Hz y 3.400Hz, por lo que para la telefonía generalmente se utilizan filtros de 4.000Hz.

Digitalizar la señal de audio requiere en primera instancia realizar un muestreo de esta, para luego cuantificarla, por el teorema de muestreo de Nyquist se toman muestras a el doble de frecuencia máxima y se implementa una codificación de 8 bits (2^8=256 niveles), lo que brinda un nivel aceptable de ruido de cuantificación para la voz y por último esta información es codificada.
Antes de la cuantificación se realiza companding para mejorar la respuesta de audio. Existen dos métodos companding, el logarítmico de origen norte americano (PMCU o Ley u) y el lineal de origen europeo (PCMA o Ley A).

Ecuación 1 - Composición del Ancho de Banda en PCM

$$4000\ \frac{1}{seg}\ x\ 2\ muestras\ x\ 8\ \frac{bits}{muestra} = 64000\ \frac{bits}{seg} = 64Kbps$$

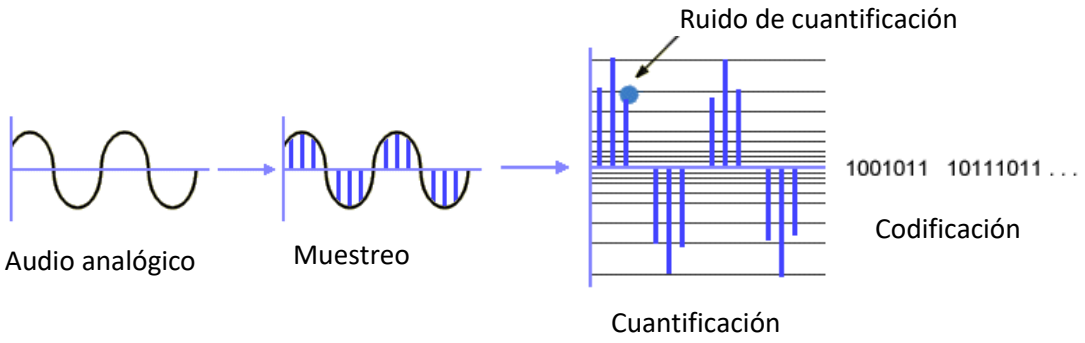

Figura 1 - Muestreo y Cuantificación – Fuente: Elaboración Propia

3.1 Composición del ancho de banda utilizado por una comunicación VoIP

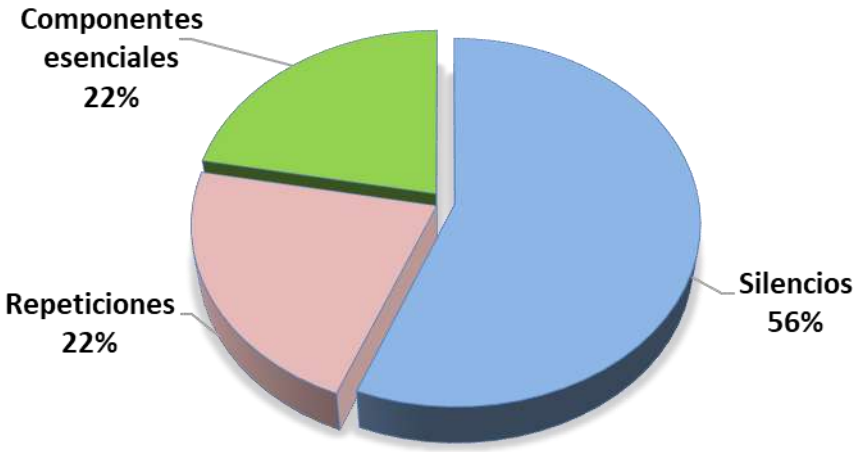

Figura 2 - Distribución del Ancho de Banda en VoIP - Fuente: Elaboración Propia

3.2 Supresión de silencios

Complemento utilizado para reducir el ancho de banda utilizado por una llamada de Voz sobre IP.

3.2.1 VAD (Voice Activity Detection)

El detector de actividad de voz es un algoritmo de detección de períodos de voz, utilizado para eliminar los silencios (ausencia de voz) en una conversación telefónica, puesto que ello permite reducir el flujo de datos entre un 35% y 80%, siendo un valor medio de 56% bastante aceptable.

Durante los períodos de silencio no se envía nada.

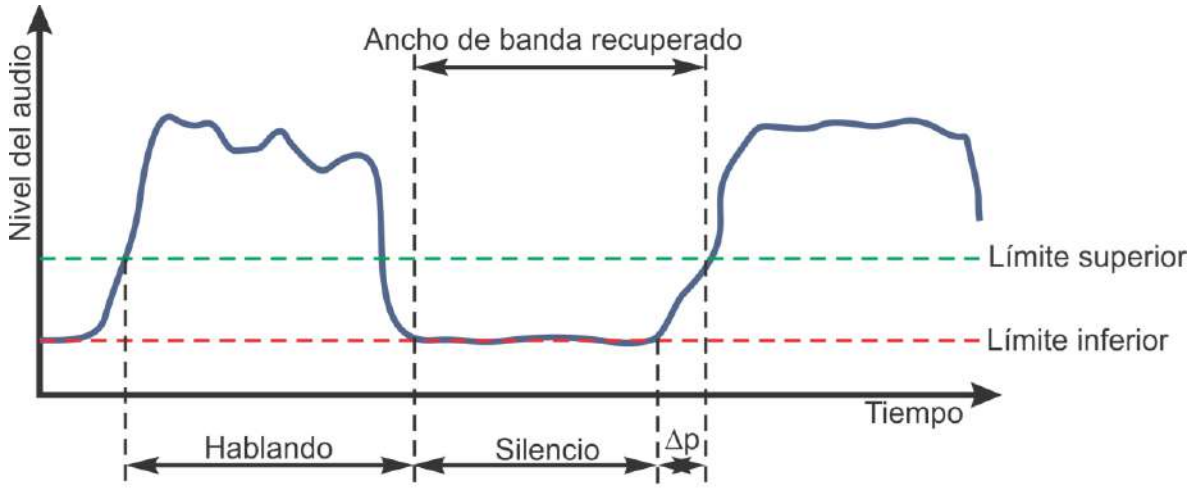

Figura 3 - Umbrales para la VAD - Fuente: Elaboración Propia

3.2.2 SID (Silence Insertion Description)

El paquete de descripción de silencio permite reducir la velocidad de transferencia utilizando un mecanismo de compresión de los instantes de silencio (para ello utiliza un algoritmo VAD).

Durante los silencios, el SID activa un generador de ruido de confort (GNC), para evitar que la ausencia de señal causa la sensación de que se ha cortado la comunicación. Este tipo de comunicaciones posee un módulo DTX (Discontinuous Transmission) para evitar enviar paquetes durante los períodos de silencio.

3.3 Percepción de la calidad de la voz

La voz sufre distorsiones a lo largo de un sistema, las cuales son introducidas por los codec utilizados, por ruidos externos al sistema, demoras (delay), eco y por la pérdida de paquetes de información.

Para evaluar la calidad de la voz percibida se pueden utilizar métodos subjetivos u objetivos.

El método más utilizado de evaluación subjetiva es el **MOS** (Mean Opinion Score) que se encuentra detallada en la recomendación P.800 de la ITU-T, la cual establece valores estadísticos que tiene en cuenta la percepción del usuario donde 5 es excelente y 1 es Mala. Para establecer un valor determinado, un gran número de usuarios deben califican la calidad de la voz (ACR o "Absolute Category Rating") y de ahí que este es un método costoso y lento y es dependiente entre otros factores como el país, idioma y expectativas de los usuarios. Los métodos de evaluación subjetivos requieren ambientes controlados y son complejos de implementar por lo que su aplicación es muy limitada.

La recomendación P.862 de la ITU-T presenta un método objetivo para la evaluación de la voz con codec de banda angosta (300Hz a 3,4kHz), este método se conoce como PESQ ("Perceptual Evaluation of Speech Quality" o "Evaluación de la Calidad Vocal por Percepción") y sus resultados se encuentran en una escala entre -0,5 y 4,5, pero en la mayoría de los casos los resultados varían entre 1 y 4,5, por lo que se compara con el MOS. Este método requiere del envío de una señal conocida para poder ser evaluada (los sistemas generalmente solo requieren de unos pocos segundos para realizar la evaluación). La recomendación P.862.3 de la ITU-T es una guía para la aplicación de la P.862.

En enero del 2011 la ITU-T estandarizó la recomendación P.863 (POLQA o "Perceptual Objetive Listering Quality Assessment") que es la evolución de la P.862 y puede trabajar en la banda super ancha (50Hz a 14kHz) como así también en la banda ancha (50Hz a 7kHz) y en la banda angosta.

El algoritmo P.563 puede predecir la calidad de la voz sin la necesidad de utilizar una señal de referencia conocida, por lo que puede utilizarse con el sistema en funcionamiento normal.

R-Factor ("Transmission Rating Factor") es otro método para estimar la calidad de VoIP, se halla descripto en la recomendación G.107 de la ITU-T y se lo llama E-Model, donde el Anexo II adapta el modelo para ser utilizado en banda ancha. El R-Factor es un valor calculado por el sistema que va desde 0 (Mala / no recomendado) a 100 (excelente) para banda angosta y de 0 a 129 para banda ancha.
El modelo tiene en cuenta varios factores para calcular el valor como compresión, retardos de la red (delay), pérdida de paquetes, ruido externo y eco.

Tabla 1 - Cuadro de comparativo de MOS vs R-Factor para banda angosta – Fuente: Elaboración Propia

Calidad	MOS	R-Factor
Excelente	5	90 – 100
Buena	4	80 – 90
Regular	3	70 – 80
Pobre	2	60 – 70
Mala	1	< 60

La calidad de la voz sobre IP depende principalmente de cinco factores:

- **Codec**: Algoritmo que convierte la señal de voz análoga en datos digitales para la transmisión de una llamada.
- **Delay**: Demora fija sufrida en la transmisión entre usuarios.
- **Jitter**: Variaciones del delay, es decir, demora dinámica sufrida en la transmisión entre usuarios.

- **Eco**: Fenómeno acústico que se produce cuando una onda de audio audible retorna al emisor.
- **Packet Loss**: Paquetes perdidos en la transmisión.

3.3.1 Codec

Son los que realizan la codificación y decodificación de la voz y de ahí su nombre. Se los caracteriza por tasa útil (bit rate), banda (ver cuadro), complejidad y retardo (tiempo de empaquetado). Una mayor complejidad del codec se traduce en mayor consumo de memoria (ROM y RAM), consumo de energía y del número de instrucciones por segundo necesarias.

Los primeros Codecs fueron diseñados para reproducir la voz humana y heredaron de la telefonía tradicional las frecuencias de corte que van de 300Hz a 3,4kHz, actualmente este tipo de Codecs se los denomina de banda angosta, narrowband o banda telefónica.

Actualmente la ITU ha estandarizado los siguientes tipos de Codecs:

Tabla 2 - Frecuencias según la Banda - Fuente: Elaboración Propia

Banda	Frecuencias de audio	Frecuencia de Muestreo
Banda angosta (narrowband)	300Hz - 3,4kHz	8kHz
Banda ancha (wideband)	50Hz - 7kHz	12kHz o 16kHz
Banda súper ancha (superwideband)	50Hz - 14kHz	24kHz o 32kHz
Banda completa (fullband)	20Hz - 20kHz	48kHz

Diferentes Codecs utilizan diferentes esquemas de compresión, en la siguiente tabla pueden verse algunos ejemplos de los más utilizados en banda angosta:

Tabla 3 - Tasas reales según los CODECs - Fuente: Elaboración Propia

Codec	MOS	Tasa útil (Audio)	Bytes por paquete	Tiempo de empaquetado	Tasa real (Ethernet)
G.711 A-LAW / µ-LAW	4,4	64,0 Kbps	160	20 ms	90,4 Kbps
			240	30 ms	81,6 Kbps
			320	40 ms	77,2 Kbps
G.729a	3,7	8,0 Kbps	10	10 ms	60,8 Kbps
			20	20 ms	34,4 Kbps
			40	40 ms	21,2 Kbps
G.723.1 (6.3)	3,9	6,3 Kbps	24	30 ms	24,0 Kbps
G.723.1 (5.3)	3,8	5,3 Kbps	20	30 ms	22,9 Kbps
iLBC	4,1	15,2 Kbps	38	20 ms	41,6 Kbps
	4,0	13,3 Kbps	50	30 ms	30,9 Kbps

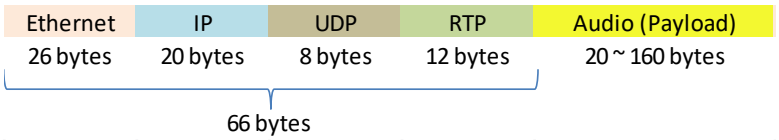

Figura 4 - Composición del overhead para la transmisión de audio - Fuente: Elaboración Propia

Ecuación 2 - Cálculo de la Tasa Real

$$Tasa\ real = \frac{(Bytes\ por\ paquete + Bytes\ de\ cabeceras) * 8\ \frac{bits}{byte}}{Tiempo\ de\ empaquetado}$$

La capa 2 agrega una cola de 4 bytes que, si bien no se incluye en el dibujo, sí se incluyen en las cuentas para calcular el tamaño adicionado por esta capa.

En caso de utilizar una VLAN, 802.1q o 802.1ad se agregan 4 bytes y 6 bytes respectivamente al tamaño del encabezado de la capa 2 (Ethernet). En ningún caso de este documento se incluyen estos bytes adicionales en las cuentas.

3.3.1.1Rendimientos de los Codecs de G.729 y G.711

En el gráfico se muestran los Kbps (kilo bits por segundo) de los paquetes de voz en G.729 y G.711 a una tasa de 50 pps (1 paquete cada 20ms), por lo tanto, puede verse que si bien el Payload (o Datos) puede reducirse de 64 kbps a 8 kbps la tasa total no se reduce en la misma proporción debido a que el Header (o Cabecera) es constante.

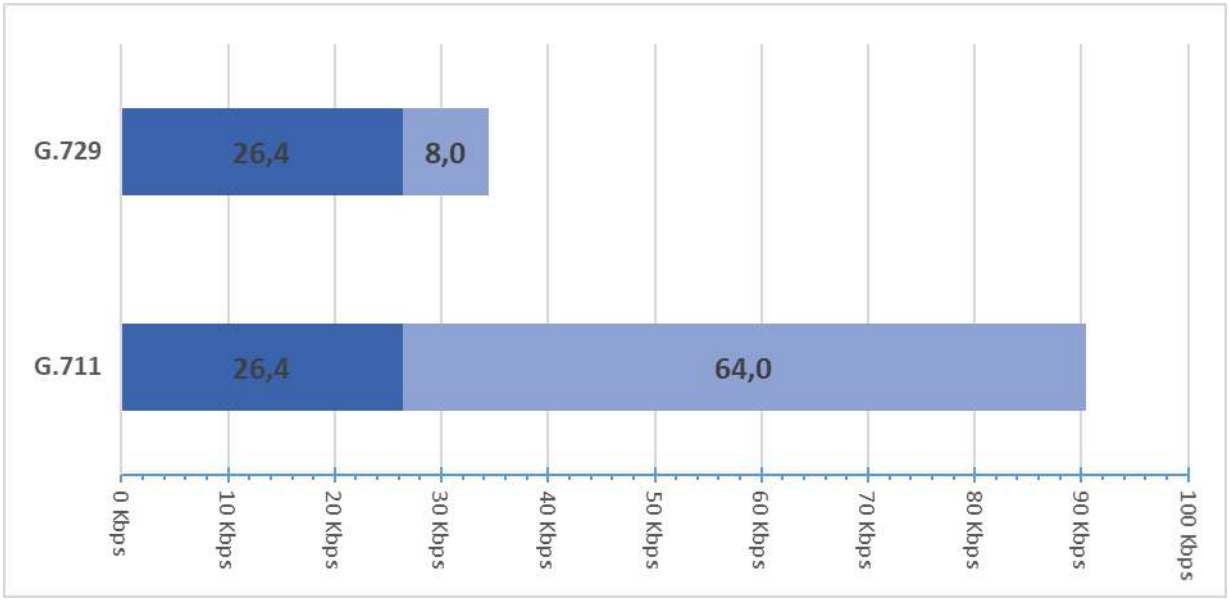

Figura 5 - Influencia del overhead en la transmisión de audio - Fuente: Elaboración Propia

3.3.1.2 Codecs de Banda angosta (narrowband)

G.711 A-law: El algoritmo ley A ("Pulse Code modulation A-Law" o PCMA) recomendado por la ITU es un sistema de cuantificación lineal de señales de audio, utilizado habitualmente en aplicaciones de voz humana. Este sistema de codificación europeo es utilizado en gran parte del mundo y es el mismo codec utilizado por las tramas E1.
Debido a que no utiliza compresión, posee la menor latencia y requiere menor capacidad de procesamiento. Lo malo es que utiliza más ancho de banda que otros codec, no obstante, aumentando el ancho de banda, esto no debería ser un problema.

G.711 U-law: El algoritmo ley Mu ("Pulse Code modulation u-Law" o PCMU) recomendado por la ITU es similar al G.711 A-Law, utiliza cuantificación logarítmica y se utiliza en las tramas T1 y J1, las cuales son el estándar en EEUU, Canadá y Japón.

G.729: Algoritmo de compresión de audio de voz recomendado por la ITU ("Conjugate Structure Algebraic Codebook Excited Linear Prediction" o CS-ACELP) que comprime en bloques a una tasa de 10bytes cada 10ms. Tonos tales como DTMF o fax no pueden ser transportados de forma confiable por este codec, con lo cual, para ser trasportados se debe utilizar G.711 o métodos de señalización fuera banda.
Se utiliza mayoritariamente en aplicaciones de VoIP por sus bajos requerimientos en ancho de banda.
Este codec está cubierto por una variedad de patentes, lo que significa que se debe pagar una patente antes de poder ser utilizado comercialmente. Tonos tales como DTMF o fax no pueden ser transportados de forma confiable por este codec, con lo cual, para ser trasportados se debe utilizar G.711 o métodos de señalización fuera banda. El anexo B de G.729 es un esquema de compresión del silencio, el cual tiene un módulo de VAD que se usa para detectar la actividad de la voz.

Ecuación 3 - Cálculo de la Tasa en G-729

$$\frac{10\ bytes}{10\ mseg} = \frac{80\ bits}{0{,}01\ seg} = 8000\ \frac{bits}{seg} = 8Kbps$$

G.723.1: Algoritmo de compresión de audio de voz recomendado por la ITU que comprime cada 30ms (240 muestras en total). Cada bloque puede ser de 24 ó 20 bytes de longitud, lo que hace a la cadena de datos tanto de 6.3kbps (MP-MLQ - Multipulse LPC with Maximum Likelihood Quantization) o 5.3kbps (ACELP - Algebraic Codebook Excited Linear Prediction).

Este codec está cubierto por una variedad de patentes, lo que significa que se debe pagar una patente antes de poder ser utilizado comercialmente. Tonos tales como DTMF o fax no pueden ser transportados de forma confiable por este codec, con lo cual, para ser trasportados se debe utilizar G.711 o métodos de señalización fuera banda. Utiliza compresión de silencios.
Este codec fue desarrollado originalmente para video conferencias sobre la PSTN.

iLBC: Definido en el RFC 3951 ("Internet Low Bit rate Codec" o BI-LPC). Algoritmo de compresión de voz que utiliza una codificación de predicción-lineal, pues está diseñado para ahorrar ancho de banda y enfrentar perdida de paquetes eventuales, pero consume muchos recursos del procesador.

Tonos tales como DTMF o fax no pueden ser transportados de forma confiable por este codec, con lo cual, para ser trasportados se debe utilizar G.711 o métodos de señalización fuera banda. Es el codec utilizado originalmente por GoogleTalk y Skype, hoy reemplazado por Codecs más modernos, con mayores anchos de banda y mejores valores de MOS.

3.3.1.3 Codecs de Banda ancha (wideband)

G.722: Algoritmo de compresión de audio de alta definición (Sub-band ADPCM) para voz recomendado por la ITU. Realiza un muestreo de la voz a 16kHz en vez de los 8kHz estándar, con una tasa de bits levemente inferior a la del G.711. Es útil en aplicaciones VoIP empresariales donde el ancho de banda no suele ser prohibitivo, ofrece una mejora significativa en la calidad de la conversación sobre los Codecs de banda angosta.
Trabaja con tamaños de paquete variable de 48, 56 o 64kbps.

G.722.1: Algoritmo de compresión de audio de alta definición (Transform Codec) utilizado en audio y video conferencias.
Trabaja con tamaños de paquete variable de 24 o 32kbps.

G.722.2: Algoritmo de compresión de audio de alta definición (AMR-WB) utilizado principalmente en redes celulares 3G. Los bits rates más altos poseen una gran inmunidad al ruido de fondo, lo cual es esencial para ambientes adversos, tales como pueden aparecer en la utilización de teléfonos celulares.
Trabaja con nueve tamaños de paquete distintos (variable) entre 6,6kbps y 23,85kbps.

G.711.1: Aprobado por la ITU-T en el año 2008, extiende el Codec G.711 a un ancho de banda de 7KHz, optimizado para VoIP. Las muestras codificadas en este Codec pueden ser convertidas al G.711 original mediante un simple truncado. Realiza un muestreo de la voz a 16KHz (banda ancha), pero también soporta hacerlo a 8KHz (banda angosta).
Trabaja con tamaños de paquete variable de 64, 80 o 96kbps.

G.729.1: Aprobado por la ITU-T (Wideband G.729) es compatible con el G.729 original.
Trabaja con tamaños de paquete variable entre 8 y 32 kbps.

RtAudio: Codec propietario de Microsoft que utiliza técnicas de LPC (Linear Prediction Coefficients) y codificación VBR (Variable Bit Rate), por lo que no todos los cuadros de voz se codifican con la misma cantidad de bytes.
Este Codec es utilizado en el sistema Lync (evolución del Office Communicator)
Trabaja con tamaños de paquete variable entre 8,8 y 18 kbps.

3.3.1.4Codecs de Banda Super ancha (superwideband)

SILK: Algoritmo de compresión de audio desarrollado y utilizado por Skype, el cual puede trabajar desde banda angosta con muestreos de 8kHz a banda super ancha con muestreos de 24kHz, pasando por muestreos de 12kHz y 16kHz. En el año 2010 se envió un borrador del Codec al IETF (Internet Engineering Task Force) para que el mismo sea convertido en un nuevo RFC.
Si bien el Codec es de código abierto, no es libre, por lo que si se desea realizar un software comercial con dicho Codec, se debe solicitar un permiso especial a Skype.
Trabaja con tamaños de paquete variable entre 6 y 40 kbps.

3.3.1.5Codecs de Banda completa (fullband)

G.719: Es el primer Codec de la ITU-T (Low-complexity, full band) desarrollado para Banda completa (fullband) con muestreos a 48kHz y se encuentra optimizado tanto para voz, como para la música.

Este Codec se encuentra licenciado por Policom y Ericsson.
Trabaja con tamaños de paquete variable entre 32 y 128 kbps.

3.3.2 Delay

Para una buena calidad de voz, el retardo "End-to-end" (extremo a extremo), debe ser menor a 150ms (ITU G.114). Valores mayores a 50ms producen eco (tiempo transcurrido desde que se habla hasta que se percibe el retorno de la propia voz).

El Delay se mide desde el primer bit enviado hasta en último bit recibido.

El delay end-to-end está formado principalmente por 5 factores:

- Delay de propagación: Demora debida a la propagación extremo a extremo por el medio (UTP, FO, etc.).
- Delay de transporte: Demora al pasar a través de los dispositivos de red a lo largo de la ruta de acceso (Switches, routers, firewalls, bridges, etc.).
- Delay de codificación: Demora del codec al digitalizar la señal analógica, construir los paquetes y descodificarlos en el otro extremo. Generalmente a mayor compresión, mayor demora.
- Delay del buffer de Jitter: Demora producida por el receptor en la toma de varios datagramas, para amortiguar las variaciones de los tiempos de arribo (jitter).
- Delay de serialización: Demora al serializar la información por el medio, depende de la velocidad del medio. Por ejemplo, para transmitir un paquete de 226 bytes (G.711 en 20ms con todas las cabeceras) por un medio de 256kbps se requiere un tiempo de 7ms.

Ecuación 4 - Cálculo de la Demora por la Serialización

$$Demora\ debida\ a\ la\ serialización = \frac{226\ bytes * 8\ \frac{bits}{byte}}{256.000\ \frac{bits}{seg}} = 7\ ms$$

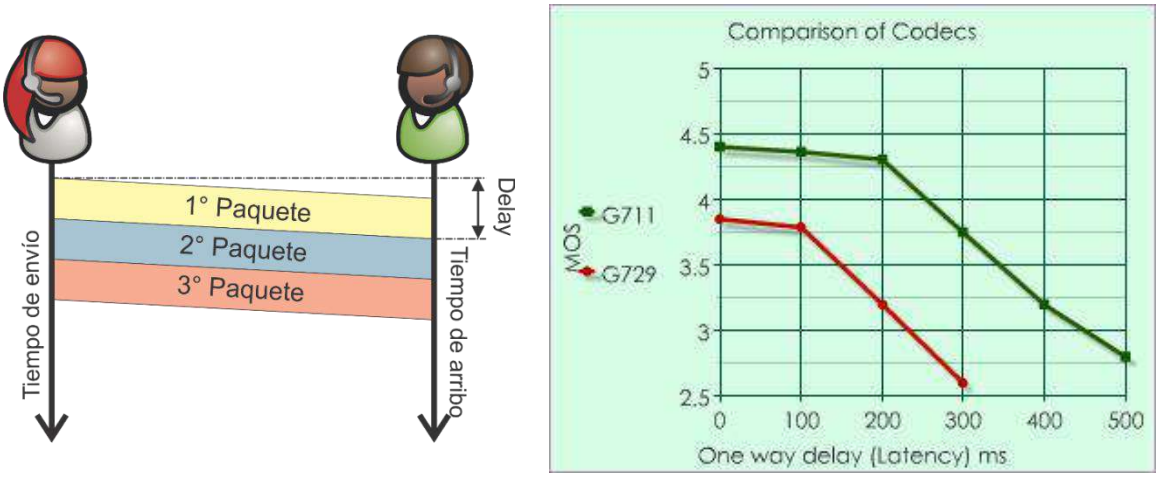

Figura 6 - Comparativa entre el delay y el MOS – Fuente: www.voipmechanic.com

3.3.3 Jitter

Se define técnicamente como la variación en el tiempo en la llegada de los paquetes, causada principalmente por congestiones en la red, perdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino.

El Jitter debe ser inferior a 50ms.

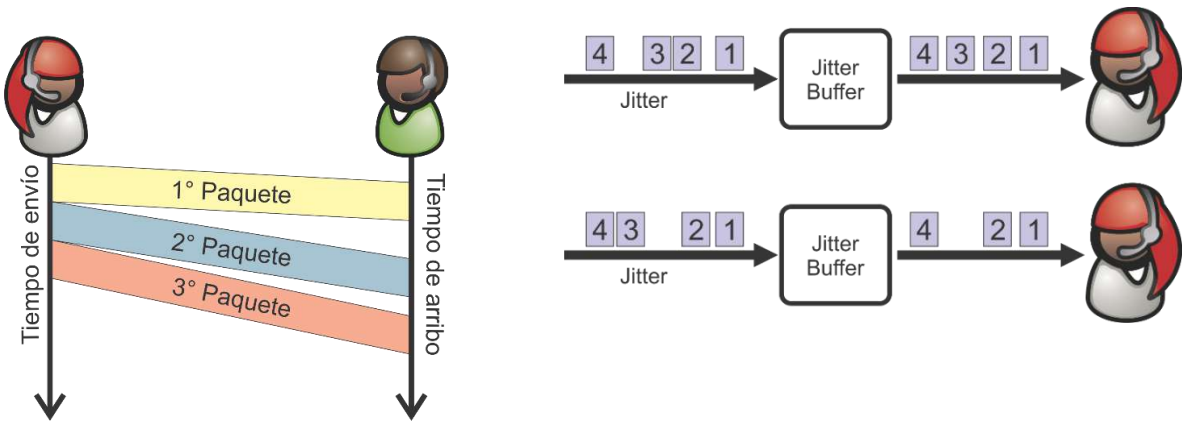

Figura 7 - Influencia del Jitter - Fuente: Elaboración Propia

Para eliminar el efector del Jitter se utiliza un buffer denominado **De-Jitter Buffer**, que consiste básicamente en asignar una pequeña cola o almacén para ir recibiendo los paquetes y sirviéndolos con una demora fija. Si algún paquete que se necesita retransmitir no se encuentra en el buffer (se perdió o aún no ha arribado al buffer) se considera que el mismo es un paquete perdido, descartándolo en caso de que el mismo arribe más tarde.
Un aumento del buffer implica reducir la pérdida de paquetes, pero aumentar la demora introducida por el buffer.

La distribución de la demora de arribo de los paquetes al receptor describe una curva gaussiana donde el nivel medio de la misma se lo denomina Delay propiamente dicho y su a distribución, Jitter.
El tamaño del De-Jitter Buffer puede ser fijo o dinámico y se lo puede determinar utilizando esta curva para contener al menos el 99% de los paquetes, lo que supondría una pérdida de paquetes del 1%.

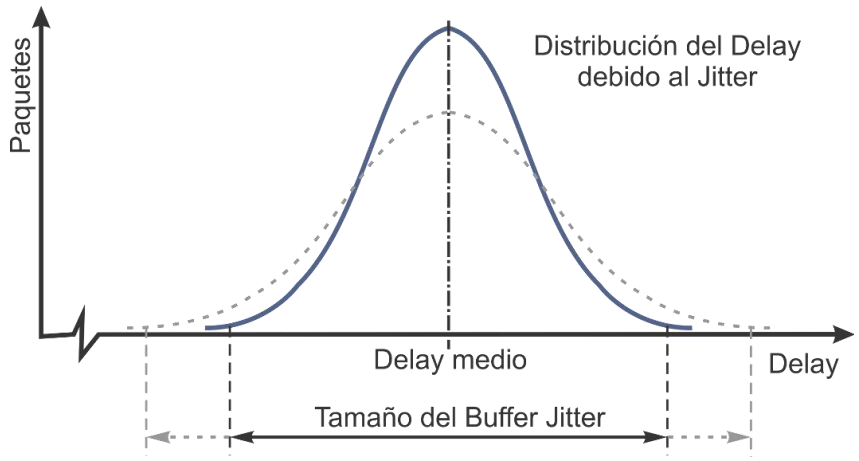

Figura 8 - Distribución del Delay respecto del Jitter - Fuente: Elaboración Propia

3.3.4 Eco

El retorno del audio hacia el emisor de origen se produce entre el micrófono y el parlante que utiliza el usuario para poder comunicarse con el otro extremo, o sea, en la parte analógica de la comunicación.

Todos los retornos acústicos producidos con los teléfonos IP o softphones pueden ser percibidos como Eco, por lo que deben emplearse mecanismos para evitarlos o cancelarlos. La recomendación G.168 de la ITU-T, describe las características que deben tener los compensadores de eco en redes digitales.

Para que un retorno acústico sea percibido como eco, la señal debe poseer un tiempo de demora de retorno (al emisor) mayor o igual a 30ms y un nivel mayor a -25db.

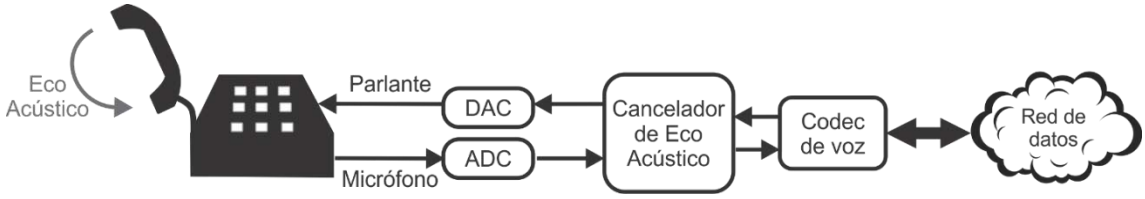

Figura 9 - Componentes para la cancelación del Eco - Fuente: Elaboración Propia

3.3.5 Packet Loss

Las comunicaciones en tiempo real están basadas en el protocolo UDP. Este protocolo no está orientado a la conexión, por lo que, si se produce una pérdida de paquetes, estos no se renvían. La pérdida de paquetes también se produce por descartes de paquetes que no llegan a tiempo al receptor.

Sin embargo, la voz es bastante predictiva y si se pierden paquetes aislados se puede recomponer de una manera bastante óptima. El problema es mayor cuando se producen pérdidas de paquetes en ráfagas (consecutivos).

La pérdida de paquetes máxima admitida para que no se degrade la comunicación deber ser inferior al 1%. Pero es bastante dependiente del códec utilizado. Cuanto mayor sea la compresión del códec, más pernicioso es el efecto de la pérdida de paquetes. Una pérdida del 1% degrada más la comunicación si se usa el códec G.729 en vez del G.711.
Comparativa entre la pérdida de paquetes aleatoria (no en ráfaga) y el MOS realizada por la ITU-T (ITU, 2003). Si bien la comparativa se realizó para un MOS estimado matemáticamente, este es muy similar al MOS "real".

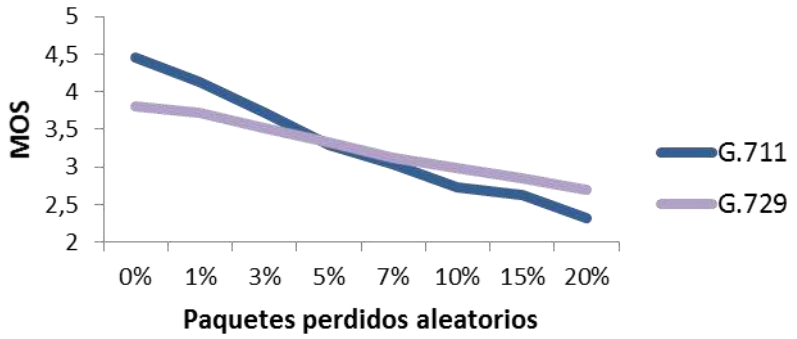

Figura 10 - Caída del MOS con pérdidas consecutivas de Paquetes - Fuente: Elaboración Propia

Existen métodos para mitigar el efecto de la pérdida de paquetes, como por ejemplo el Anexo I de la recomendación G.711 de la ITU-T, donde describe un algoritmo de regeneración en base a la información contenida en los paquetes previos al paquete perdido (PLC o Packet Loss Concealment).

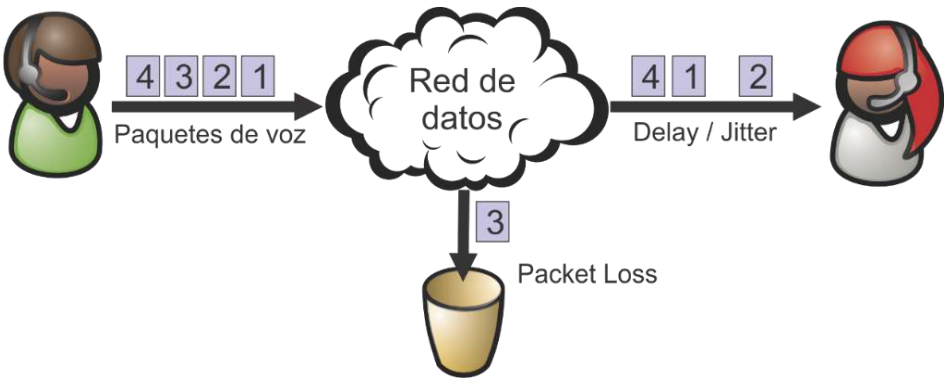

Figura 11 - Delay, Jitter y Packet Loss - Fuente: Elaboración Propia

Tabla 4 - Parámetros para Delay, Jitter y Packet Loss

Parámetro	Excelente	Bueno	Aceptable	Pobre
Delay	< 50 ms	50 ms ~ 150 ms	150 ms ~ 300 ms	> 300 ms
Jitter	< 10 ms	10 ms ~ 20 ms	20 ms ~ 50 ms	> 50 ms
Packet Loss	< 0,1 %	0,1 % ~ 0,5 %	0,5 % ~ 1,5 %	> 1,5 %

4 Seguridad en Redes Convergentes

Las nuevas soluciones convergentes de comunicaciones denominadas UCS (Unified Communication Systems) basadas en voz sobre IP (VoIP), son una tendencia en el mundo empresarial actual, no solamente por lo accesibles, sino porque además ofrecen una amplia variedad de funciones para mejorar la productividad y acercar la tecnología a las nuevas generaciones de trabajadores que acarrean un paradigma muy distinto en cuanto a sus métodos de comunicación y, por lo tanto, demandan nuevas necesidades.

Otro dato importante para tener en consideración es la tendencia actual a la utilización de soluciones basadas en la nube, donde los grandes jugadores de comunicaciones unificadas, a los que inclusive se les sumó Microsoft con Skype for Business, ofrecen este tipo de soluciones. Otras soluciones similares son Micloud de Mitel, HCS (Hosted Collaboration Solution) de Cisco y Denwa Cloud de Denwa, entre otras.

Estos hechos representan nuevas y numerosas ventajas, tales como la movilidad, ubicuidad, reducción de costos en las llamadas, incorporación de video, chat e indicación de presencia, entre otras; aunque ello también acarrea nuevos desafíos como la necesidad de aplicar calidad de servicio dentro de las nuevas redes convergentes y el hecho de poder establecer ciertos parámetros de seguridad para reducir los riesgos y mitigar las posibles consecuencias del accionar de cibercriminales.

Gracias a este tipo de conexiones, cualquier individuo que posea una conexión convencional de Internet puede acceder a este tipo de servicios, pero al mismo tiempo se abre la posibilidad de que cualquier cibercriminal, desde cualquier lugar del mundo, pueda intentar apoderarse de estos sistemas, lo cual podría implicar consecuencias económicas o indisponibilidad de recursos. Por tal motivo, se torna esencial conocer las vulnerabilidades de estos sistemas y los riesgos que implican.

En este contexto, la investigación que se expone en el presente artículo, se propone analizar los distintos vectores de ataque actuales para las nuevas plataformas convergentes, las tecnologías de defensa digital y el rol de los usuarios en la aplicación, configuración y utilización de las distintas soluciones a fin de detectar y analizar las vulnerabilidades de las implementaciones de redes convergentes y en especial, de Voz sobre IP, junto con los riesgos que pueden derivarse, y proponer alternativas para su mitigación.

4.1 Vectores de ataque

En cuanto a los Vectores de Ataque, algunos de ellos se enfocan en un ataque directo a las plataformas convergentes, mientras que otros lo hacen en forma indirecta. La siguiente es una lista no excluyente de los vectores más destacados que afectan la confidencialidad, la integridad o la disponibilidad de los sistemas.

4.1.1 Físico

Acceso físico a dispositivos sensibles, tales como servidores, equipos de red o endpoints (PCs, smartphones, videoteléfonos IP, entre otros) que pueden incurrir en DoS (Denial of Service) por medio de manipulación deliberada o involuntaria de los mismos, ya sea por reinicio, daño físico o modificación en el conexionado.

4.1.2 Phishing

Se trata de un ataque en el que los ciberdelincuentes suplantan una empresa o ente gubernamental mediante una comunicación fraudulenta, de manera tal que parezca una forma legítima de ponerse en contacto con ellos con el objetivo aparente de solucionar algún inconveniente de seguridad o con la cuenta de E.Mail, entre otras variantes. El objetivo del ataque es adquirir información personal o sensible de los usuarios

(cuentas, contraseñas, datos bancarios, entre otros). Este tipo de ataque cobra relevancia en la presente investigación con la utilización de plataformas unificadas de comunicaciones con voz, mensajería e E.Mail, ya que al atacante, el hecho de obtener la contraseña le permite acceder a todos los servicios.

Según el reporte de Bitglass (Bitglass, 2017) sobre la ciberseguridad en el entorno empresarial del 19 de septiembre de 2017, donde encuestó a 129 hackers que habían asistido a la conferencia Black Hat 2017 celebrada en Las Vegas, el 59% de ellos afirmó que el phising es el mejor método para filtrar datos, y la principal razón de ello es que los ciberdelincuentes siempre serán capaces de poder explotar los errores cometidos por los humanos y su ignorancia o inocencia.

4.1.3 Hijacking

Se trata de una técnica ilegal que consiste en adueñarse de algo del usuario, generalmente para obtener información confidencial. Algunas de las diferentes manifestaciones de este vector de ataque son el Call Hijacking, por medio de la redirección de la llamada a un sitio diferente, pudiendo participar en la conversación, y pretendiendo ser una llamada legítima. También existe el Enpoint Hijacking, aprovechando la oportunidad de que los endpoints actuales suelen hacer uso de sistemas operativos convencionales, tales como Windows, Linux, IOS o Android. Esta masificación permite a los ciberdelincuentes rentabilizar esfuerzos en hallar nuevas vulnerabilidades, o simplemente hacer uso de vulnerabilidades conocidas en los diversos endpoints donde no se han aplicado los parches o actualizaciones correspondientes.

4.1.4 ID Spoofing

En este caso, los ciberdelincuentes se presentan como otra persona, al falsificar el número que aparece en la pantalla de identificación de

llamadas del destinatario. Esta suplantación permite que una llamada parezca provenir de algún número de teléfono que el atacante desee, sentando bases para un ataque de ingeniería social.

4.1.5 Telephony Denial of Service (TDoS)

Ataque de denegación de servicio telefónico. Si bien el término es bastante general, en este caso refiere cuando usuarios no autorizados inundan el sistema con demasiadas solicitudes de acceso degradando seriamente el rendimiento de la red o sistema, incluso llegando al punto de impedir la utilización del mismo por parte de usuarios legítimos. Algunas técnicas se basan en la explotación de vulnerabilidades conocidas en algún software o hardware del sistema por medio de paquetes especialmente construidos.

Llegan a ser especialmente dañinos en los ataques provenientes de varias fuentes, también llamadas ataques de denegación de servicio distribuido o simplemente DDoS. Si bien en VoIP esta técnica no se encuentra muy difundida podrían ser más dañinas, mayormente por la necesidad de garantías en la calidad de servicio (QoS), lo que permite que las redes convergentes puedan mantener la comunicaciones en tiempo real de manera aceptable, ya que estas poseen una tolerancia mucho menor a los problemas de rendimiento, por ello poseen un perfil más elevado dentro de los equipos de red, lo que un ataque a este nivel podría repercutir en distintos sistemas.

Las aplicaciones y dispositivos de comunicaciones sobre redes IP suelen trabajar sobre determinados puertos específicos, el bombardear dichos puertos con tráfico falso, fabricado con apariencia de ser legítimo (“real”), puede causar una denegación de servicio y que los usuarios legítimos no puedan hacer uso de la solución.

4.1.6 Call Tempering

Consiste en la interferencia de la calidad de la llamada por inyección de paquetes de ruido directamente en la secuencia de datos. Es una variante de TDoS, mencionada anteriormente

4.1.7 Malware

Se trata de un software malicioso que engloba a todo tipo de programas o códigos informáticos cuya función es dañar un sistema, causar un mal funcionamiento o bien adquirir información confidencial.

4.1.8 Man-in-the-middle (MITM)

Intercepción de una comunicación en progreso. La misma se puede realizar por proximidad al objetivo o por la utilización de malware. En el primer método los atacantes necesitan acceso a una red poco segura, como ser los accesos WiFi gratuitos (Kaspersky Lab, 2013).

4.1.9 Eavesdropping

Intercepción o escuchas secretas no autorizadas de comunicaciones privadas en tiempo real. Las mismas pueden ser llamadas telefónicas, mensajería, videollamadas o envíos de fax.

4.1.10 Password attack

Se trata de un intento de obtención de contraseña de administrador o de un usuario con altos privilegios para acceder al servicio u obtener el control de éste. Estos ataques pueden ser pasivos o activos. En los primeros, también denominados sniffing, la contraseña es capturada durante un proceso de autenticación por medio de algún malware instalado en el endpoint o por una técnica de MITM, lo que lo hace indetectable para el usuario. El método activo generalmente se beneficia

del “factor humano” involucrado en la creación de contraseñas poco robustas y comprueba un listado de contraseñas típicas creando un listado personalizado con información privada del objetivo (nombres, fechas, direcciones, entre otros) y combinándolas mediante softwares específicos (“Cain y Abel”, “THC-Hydra”, entre otros).

4.1.11 Social engineering

Refiere a un arte que se compone de diversos métodos para convencer a las personas de revelar información confidencial, basándose en comportamientos vulnerables de las personas, tales como la tendencia a la confianza, la obligación moral, entre otras. Esto también se ve reflejado como consecuencia de las falencias de las empresas en entrenamiento insuficiente sobre ciberseguridad, fallas en las políticas del manejo de la información o exceso de unidades organizativas. Los intentos de ingeniería social son difíciles de detectar y no existe contramedida que sea completamente efectiva.

4.2 Defensa digital

La Defensa Digital refiere a un conjunto de tecnologías y métodos que serían la contramedida de los distintos ataques de los ciberdelincuentes, con el fin de evitar o mitigar las consecuencias de sus actos. La siguiente es una lista no excluyente de las diferentes contramedidas.

4.2.1 Firewall

Es un Sistema que permite proteger una PC o una red LAN (Local Area Network) de intrusiones provenientes de una red externa, generalmente Internet. Este sistema puede ser basado en software y/o hardware y permite inhabilitar la utilización de determinados puertos de datos según varios criterios configurables; es decir, funciona como una barrera de protección para el ingreso a la LAN desde otras redes externas. Es uno de

los aspectos fundamentales para la ciberseguridad, por lo que su utilización es siempre necesaria. En general se recomienda la utilización de algún Firewall robusto para el acceso a la red interna (LAN) y otro, basado en software, para ser instalado en cada endpoint inteligente (PC, smartphone, entre otros). Los modelos actuales permiten examinar la capa 7 del modelo OSI (Open Systems Interconnection), analizando comportamientos de ataques típicos y bloqueando puertos o paquetes de ciertas direcciones IP origen de manera automática, brindándoles una inteligencia superior a los antiguos Firewalls, que sólo analizaban hasta la capa 4.

4.2.2 Virtual LAN (VLAN)

Se trata de una subdivisión virtual de una red de datos, lo cual genera la posibilidad de utilizar la misma red física en diferentes redes virtuales. Esta separación permite que la propagación de los incidentes de seguridad quede restringida al entorno en donde ocurren, y separar así la gestión de los equipos de red con el objetivo de mitigar configuraciones malintencionadas y crear redes con menores protecciones (DMZ) para los servidores que brindan servicios de extranet. Los puertos de los equipos de red envían y reciben información únicamente hacia y desde la VLAN en la que están configurados, razón por la cual sólo sería posible para los ciberdelincuentes capturar la información transmitida en esa VLAN específica a la cual pudieron tener acceso. Las VLANs también se pueden configurar para conceder o restringir privilegios de seguridad de manera dinámica, según el perfil del usuario.

4.2.3 Encryption

Se trata de una práctica que consiste en cifrar los datos con el fin de que la información no sea inteligible ni manipulada por terceros. Hoy en día, cifrar no es una tarea complicada, y el costo es asequible. Desde ya, se debe asegurar que el sistema de cifrado a emplear no se encuentre

comprometido; es decir, que no se conozca forma de romperlo y que se cuente con un sistema de gestión de claves, en particular, y con un procedimiento de administración de material criptográfico, en general (Teijeira, 2009). Cifrar siempre es conveniente, y en algunos casos puede tratarse de una obligación, debido a las necesidades que pueda haber en materia de confidencialidad. En el resto de los casos, cifrar es de gran utilidad, ya que refuerza la seguridad y genera confianza.

4.2.4 Intrusion Prevention System (IPS)

Este sistema está conformado por una tecnología que examina los flujos de tráfico de red de datos para detectar y prevenir vulnerabilidades. Generalmente se ubica detrás del Firewall con el fin de proporcionar una capa de análisis complementario, analizando activamente los flujos de datos y tomando acciones automáticas. El IPS posee varios métodos de detección de exploits (malware que busca forzar deficiencias o vulnerabilidades del sistema) donde la detección basada en patrones de comportamiento y la detección de anomalías estadísticas son las predominantes. El último de los métodos toma muestras de tráfico de red al azar y los compara con un determinado rendimiento de referencia, generando medidas posteriores cuando éstas se hallan fuera de dichos parámetros (Paloalto Networks, 2018). Un ejemplo de este tipo de sistemas es “Snort”, un sistema libre y gratuito que puede correr en Linux y Windows, y que permite la detección de intrusos en la red. Ofrece la capacidad de almacenamiento de bitácoras en archivos de texto y en bases de datos abiertas, como MySQL

4.2.5 Virtual Private Networks (VPN)

Consisten en la creación de vínculos que poseen la capacidad de conectar dispositivos lejanos como si se encontrasen físicamente en la misma red LAN, utilizando una suerte de túnel en donde los datos son cifrados de extremo a extremo mediante distintos protocolos. En el mundo

corporativo, las VPN constituyen un recurso habitual para empresas que permiten a sus empleados teletrabajar y acceder a una única red privada de forma segura. Para asegurar el correcto funcionamiento del cifrado y resguardo de datos sensibles se deben utilizar soluciones en donde se posea el control de los servidores de VPN, ya que recientes estudios demostraron que aproximadamente 1 de cada 4 servicios de VPN en la nube almacenan datos de sus clientes (Mason, 2018).

4.2.6 Session Border Controllers (SBC)

Solución de Firewall especializado diseñado para proveer de seguridad en las comunicaciones salientes y entrantes, conectándose en el borde de la red, con una interfaz hacia la WAN (generalmente Internet) y otra hacia la red LAN (o DMZ). El factor diferenciador es que se hallan específicamente diseñados para brindar soluciones de seguridad a las comunicaciones convergentes (voz, video, audio, entre otros) entrantes y salientes de una red de datos, las cuales generalmente hacen uso de los protocolos SIP (Session Initiation Protocol) y RTP (Real Time Protocol) y sus homónimos seguros TLS (Transport Layer Security) y SRTP (Secure RTP). Las funcionalidades de los SBC dependen de cada fabricante, aunque generalmente cuentan con, al menos, mitigación ante ataques de DoS, DDoS, TDoS, ocultación de la topología, cifrado extremo a extremo, NAT transversal, conectividad VPN, mitigación ante manipulación del protocolo SIP, priorización del tráfico y limitación de la tasa de transferencia.

Actualmente, luego de la Pandemia, el concepto de “Perímetro” está dando lugar a las Redes ZTNA (Zero Trust Network Access).

4.2.7 Redes ZTNA

Una Red ZTNA (Zero Trust Network Access o, en Español, Acceso de Confianza Cero a la Red) es una solución de seguridad que proporciona un acceso remoto seguro a las aplicaciones, los datos y los servicios de una

organización según una serie de políticas de control de acceso claramente definidas.

Las Redes ZTNA se diferencian de las VPN (Virtual Private Networks o, en Español, Redes Privadas Virtuales) en que otorgan acceso sólo a ciertos recursos específicos, y requiere autenticarse con frecuencia.

Una vez que se accede a través de una VPN, el usuario obtiene acceso a todo el sistema. Las Redes ZTNA adoptan el enfoque opuesto: no otorgan acceso alguno, a menos que un activo (aplicación, datos o servicio) se haya autorizado expresamente para ese usuario. A diferencia de las VPN, los ZTNA brindan una verificación continua de la identificación basada en la autenticación de la identidad. Cada usuario y cada dispositivo se verifican y autentican antes de otorgarles acceso a aplicaciones, sistemas u otros activos específicos

Cada vez son más los usuarios que acceden a los recursos desde sus hogares u otras ubicaciones, por lo que las soluciones ZTNA pueden ayudar a salvar las carencias de estas tecnologías tales como VPN, u otros métodos de acceso remoto seguro (VMWARE, 2023).

4.2.8 User identification

La identidad digital presenta un desafío técnico porque a menudo implica la prueba y autenticación de individuos a través de una red abierta, y por lo tanto insegura. Esto presenta múltiples oportunidades para la suplantación y otros ataques que pueden llevar a reclamos fraudulentos de la identidad digital de un sujeto (Grassi et al, 2017). El reporte de Bitglass mencionado anteriormente (Bitglass, 2017) reveló que el reconocimiento facial resulta hasta 6 veces menos seguro que la utilización del lector de huella dactilar. Sin embargo, sigue siendo muy utilizado. De todos modos, los nuevos softwares de reconocimiento facial se han vuelto más precisos y si bien no llegan a la seguridad de un lector de huella dactilar, seguramente esté decreciendo esa relación de 6 a 1,

aunque seguramente dependerá de la tecnología que se esté utilizando. Además, según el informe de Okta (Okta, 2018), las preguntas de seguridad siguen siendo el método de verificación más utilizado, aunque sus respuestas podrían estar disponibles en línea o ser averiguadas a través de ingeniería social.

4.2.9 Strong password

Uno de los aspectos más importantes que se deben tener en cuenta para proteger las cuentas es la contraseña. A pesar de ello, muchos usuarios no toman las medidas necesarias. El informe de Okta (Okta, 2018) determinó que cerca del 95% de los usuarios utiliza contraseñas de longitud menor a 12 caracteres, lo cual es un valor debajo de lo recomendado por el NIST 2017. Actualmente, muchas empresas continúan siguiendo las recomendaciones del "Best practices 2003" del NIST (García, 2017), en donde se indicaba la necesidad de incrementar la complejidad añadiendo a las contraseñas números y caracteres especiales y exigiendo renovarlas cada 90 días. El problema que se observó fue que esta complejidad llevó a los usuarios a cometer errores tales como olvidarlas, anotarlas o bien realizar combinaciones muy predecibles y comunes, y la renovación forzada cada 90 días (o menos) hacía que los usuarios eligieran rápidamente contraseñas débiles para salir del apuro donde, en la mayoría los casos, sólo se alteraba un número, letra o símbolo. El NIST 2017 (García, 2017) recomienda la utilización de contrafrases (passphrases) en vez de las típicas contraseñas, donde se debe crear una secuencia de al menos 12 caracteres de palabras fáciles de recordar y no es necesario incluir números o símbolos especiales (aunque igualmente se lo recomienda). Estas contrafrases no deben utilizarse en múltiples plataformas, no deben ser anotadas y no deben ser renovadas, salvo sospecha de que hayan sido vulneradas. Para poder recordar una contrafrase se debe armar una imagen mental que referencie a ésta.

Más allá de todo, el concepto de la utilización de contrafrases no terminó de imponerse porque los usuarios malinterpretaron las reglas y siguieron utilizando patrones sencillos. Por ello, en la actualidad se están buscando alternativas para eliminar el uso de contraseñas. Esto se hace por medio de la biometría, o bien a través de algún acceso a cierto dispositivo del usuario; por lo general, una APP del celular.

4.2.10 Two-Factor Authentication (2FA)

Es una capa adicional de seguridad múltiple de autenticación que no sólo requiere un nombre de usuario y una contraseña, sino que además solicita algo que sólo el usuario posea, como un token físico, su smartphone personal, o algún otro dispositivo. Estos dispositivos generan un código de uso único basado en una semilla asociada al usuario para el cálculo y una base de tiempo. Es el estándar más utilizado en sistemas cloud de infraestructura (AWS, Google Cloud, Azure) como así también en los sistemas en la nube que manejan información personal sensible como Gmail, GitHub, Dropbox, entre otros.

4.2.11 Monitoring

Consiste en el monitoreo o gestión del "estado de salud" de la solución de comunicaciones mediante la incorporación de ciertas alertas. El monitoreo en tiempo real permite encontrar posibles inconvenientes con el hardware, software o configuración, como así también intentos de sabotaje o ciberataques, y así brindar un tiempo de reacción suficiente para poder mitigarlos.

4.2.12 Logging Centralizado

Consiste en el registro de eventos que permite, una vez ocurrido el mismo, poder analizar el vector de ataque y modificar la defensa digital para su adaptación. Para el logging centralizado se necesita de un

servidor, o cluster, que reciba los logs de los distintos dispositivos de la red que se envían en tiempo real y lo guarde en su base de datos. Este sistema sirve no sólo para tener un punto central de control, sino que también agrega una capa adicional de seguridad ya que, si un atacante puede acceder a controlar un dispositivo, también puede fácilmente manipular el log para borrar los rastros. Teniendo una copia en el servidor central, el atacante también debería vulnerar el mismo para poder modificarlo.

4.2.13 Upgrades

Se refiere a actualizaciones o parches de softwares en los servidores y/o endpoints. En general, los servidores son los equipos más atacados de Internet. Por eso es extremadamente importante que estén actualizados con todos los parches que los fabricantes vayan liberando, poniendo especial atención en los de seguridad. De igual forma, también es muy importante que los mismos tengan instalada la última versión de los programas que actúan como servicios. Para estar al día de todas estas mejoras, los propios fabricantes de las aplicaciones servidoras las publican a través de listas de correo, a las que es conveniente estar inscriptos. Un ejemplo es la lista US-CERT del Homeland Security de Estados Unidos, la cual recopila y categoriza, de manera semanal y según el peligro, las últimas vulnerabilidades de los softwares más importantes.

4.2.14 Hardening implementation

Se refiere a las técnicas para mejorar la seguridad de las implementaciones. El reporte de Bitglass (Bitglass, 2017) reveló que el mayor punto ciego en la ciberseguridad de las empresas se encuentra en los dispositivos no administrados, las aplicaciones y programas obsoletos, dispositivos móviles, datos almacenados en la nube y en una incorrecta gestión de servicios, por lo que se debe prestar suma atención a estos puntos en el momento de una implementación de un servicio.

Uno de los métodos para el mejoramiento de la seguridad en las implementaciones es visualizar la implementación en un diseño por capas y analizarlas por separado:

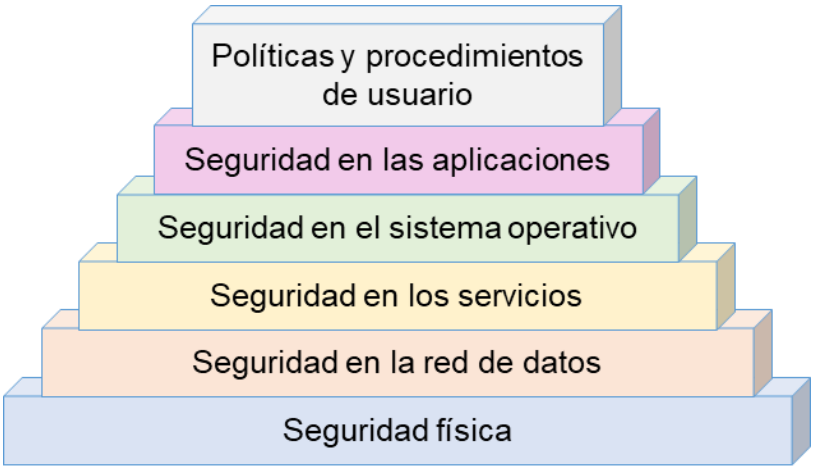

Figura 12 - Diseño por capas para la seguridad – Fuente: Elaboración Propia

Este método favorece el análisis de los distintos vectores de ataque y facilita el trabajo interdisciplinario:

Tabla 5 - Ejemplos de vulnerabilidades en cada capa – Fuente: Elaboración Propia

Capa	**Vectores de ataque / vulnerabilidades**
Física	**Acceso físico a equipos sensibles** **Sabotajes** **Reinicios malintencionados** **Denegación de servicios**
Red	**DDoS** **Floods**
Servicios	**DoS**

	Denegación en DCHP **Falta de gestión de las VPN**
Sistema Operativo	**Malas configuraciones** **Bugs** **Gusanos y Virus**
Aplicaciones	**TDoS** **Hijacking (secuestro de sesiones)** **Eavesdroping (intercepción de llamadas)** **Redirección de llamadas**
Usuario	**Contraseñas débiles** **Malas políticas de privilegios** **Phishing** **Social Engineering** **Malas políticas de reportes de incidentes**

4.3 Rol de los usuarios

El elemento humano es el eslabón más débil de cualquier sistema de seguridad, ya que el mejor sistema de seguridad que exista no podrá evitar que algún empleado haga "clic" dónde no debe (Gophich, 2018). Algunos ejemplos relacionados con el factor humano son los siguientes.

4.3.1 Phishing

Los usuarios deben ser entrenados constantemente con ayuda de soluciones de aplicaciones de simulación de ataques de phishing tipo GOPHISH (getgophish.com), donde poder generar informes para luego reforzar el entrenamiento.

4.3.2 User reporting

Los usuarios deben estar capacitados para detectar amenazas y sentirse libres de reportarlas inmediatamente, antes de que las mismas se propaguen, sin miedo de obtener una sanción devenida de una posible mala utilización. Se debe generar un método de generación y gestión de los reportes, identificando el sector responsable para acelerar la respuesta al incidente y evitar pasos intermedios innecesarios que limitarían o anularían una posible mitigación.

5 Conceptos básicos de Multicast

Una de las definiciones más utilizadas de Multicast refiere al envío de mensajes a un grupo selecto de receptores potencialmente esparcidos por toda la Internet.

En esta definición hay dos frases para analizar más pormenorizadamente:

- "**Grupo selecto de receptores**": A diferencia de Unicast o Broadcast, una conexión Multicast permite el acceso a un Grupo de usuarios que hay que definir, contrariamente a las otras dos alternativas, que sólo le envían datos, o bien a un usuario o bien a todos, respectivamente.

- "**Potencialmente esparcidos por toda la Internet**": Quizás lo de esparcirlos en toda la Internet es algo muy ambicioso porque en realidad la Internet que conocemos hoy día no soporta Multicast (McConnaughy, 2020). Las Redes Multicast que normalmente se utilizan son Privadas. Sin embargo, la clave de esta frase es que una Red Multicast no se define solamente en el entorno de LAN. Una Red Multicast puede estar formada por varias Redes LAN interconectadas entre sí a través de Routers; es decir, emulando a la Internet, pero en forma privada. Esto significa que, al armar una Red Multicast, los Routers deben soportar Multicast, lo cual no es nada trivial. Soportar Multicast significa comprender el direccionamiento de Multicast, soportar Protocolos de Ruteo Multicast (que obviamente no son los mismos a los que se utilizan habitualmente para enlaces Unicast), soportar otros Protocolos accesorios de Multicast (como el IGMP – Internet Group Management Protocol), entre otras opciones.

5.1 Multicast versus Unicast y Broadcast

Al compararlo con Unicast, la ventaja de Multicast parece bastante obvia, porque ahora no es necesario enviar “N” múltiples copias de mensajes a los “N” receptores. Por otra parte (y esto no es un detalle menor), el equipo que envía puede enviar un solo mensaje a la vez. Si se enviara un mismo mensaje a cada uno de los receptores, no sólo se generaría un aumento desmedido e irracional del tráfico, sino que, además, una gran cantidad de receptores podrían experimentar algunos inconvenientes debido a las demoras. Utilizando Multicast, la cantidad de Tráfico disminuye notablemente, especialmente más cerca de las fuentes, tal como se observa en la figura siguiente:

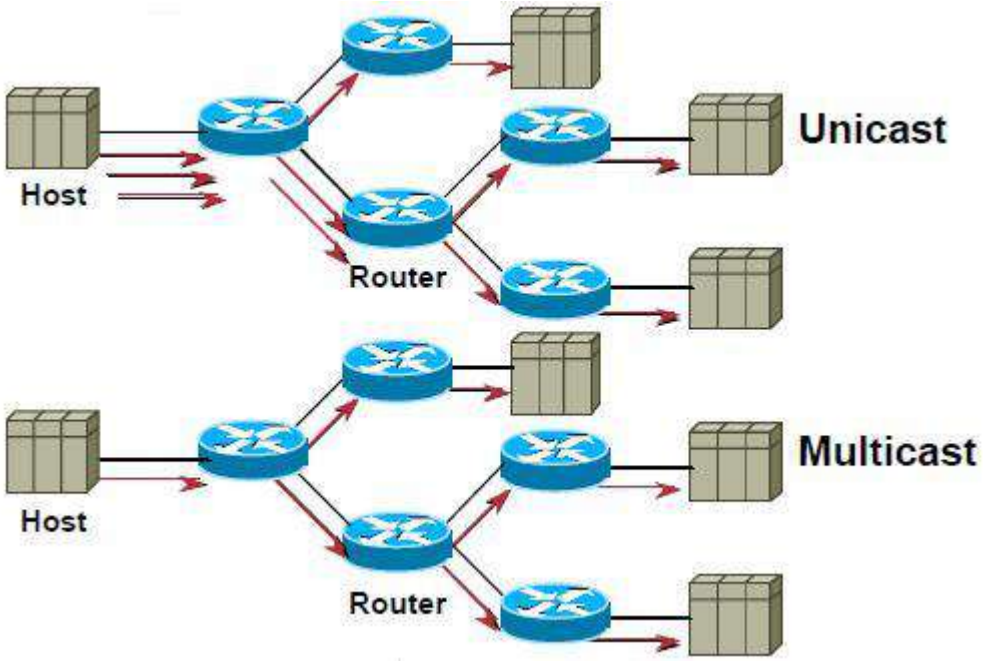

Figura 13 - Multicast versus Unicast - Fuente: Elaboración Propia

Sin embargo, una manera más hábil de desestimar al Multicast es comparándolo con Broadcast. En una primera aproximación, parecería razonable el uso de Broadcast porque se podría enviar el mensaje a

"todos", y que sólo los verdaderos receptores se den por aludidos. En todo caso, el resto lo desestimará. El primer problema que aparece al enviar un mensaje Broadcast es que se está obligando a todos los receptores a que almacenen y lean el mensaje (y, en todo caso, después lo desestimen), lo cual es una pérdida de tiempo innecesaria para los equipos que no son los verdaderos destinatarios de estos mensajes. Por otro lado, es importante tener en cuenta que los mensajes Broadcast no atraviesan los Routers (Doyle, 2017).

5.2 Ventajas del uso de Multicast

- **Mejor eficiencia**: El Ancho de Banda de la Red se utiliza de una manera mucho más eficiente por el hecho de que, comparando con Unicast, múltiples streams de datos pueden ser reemplazados por una transmisión única.

- **Mejor rendimiento**: Hay menos copias de datos que requieren almacenamiento y re-envío.

- **Aplicaciones distribuidas**: Debido a que, en Multicast, el Tráfico no crece proporcionalmente con la cantidad de Usuarios, no es irracional pensar en trabajar con Aplicaciones Multipunto.

5.3 Desventajas del uso de Multicast

Una de las desventajas del uso de Multicast es que indudablemente todas las aplicaciones deberán correr sobre el Protocolo de transporte UDP (User Datagram Protocol) (McConnaughy, 2020); por lo tanto:

- **No hay validaciones**: Aquí se trabaja con el concepto de Mejor Esfuerzo (Best Effort), con lo cual se pierde confiabilidad porque no existe retransmisión ante la pérdida de datos. Es decir, las

aplicaciones Multicast son Sin Conexión y Sin Validación (Connectionless).

- **No hay control de congestión**: Al no haber mecanismos de Control de Flujo o Ventana, en determinados momentos se puede producir una importante degradación en el rendimiento de la Red.

- **Mensajes duplicados o fuera de secuencia**: Al no haber un TCP que ordene o valide, los mensajes pueden llegar fuera de secuencia, o inclusive duplicados.

De todos modos, la buena noticia es que las Aplicaciones Multicast se utilizan habitualmente para envío de Audio y/o Video (un uso que se está popularizando mucho es el de IPTV), y estas aplicaciones ya corren (en forma nativa) sobre UDP. Estas aplicaciones suelen trabajar con un par de Protocolos accesorios que corren sobre UDP y que son el RTP y RTCP (Real Time Protocol y Real Time Control Protocol). Con estos dos Protocolos se puede resolver de una manera bastante aceptable el problema de las duplicaciones, secuenciamientos y hasta temas relacionados con manejo de congestión. Respecto de la pérdida de paquetes, al tratarse de aplicaciones que trabajan en Tiempo Real, nunca se retransmite lo perdido. De todos modos, el RTCP permite detectar pérdidas importantes y así poder hacer un empaquetamiento de los datos en el mismo momento más acorde a las circunstancias.

5.4 Algunas definiciones

Aunque parezca algo trivial, existen algunas definiciones básicas que sería bueno remarcar, y que son las siguientes:

- Para recibir datos enviados a un Grupo Multicast hay que ser miembro (member) de ese Grupo Multicast.

- Cuando se envía un mensaje a un Grupo Multicast, todos los miembros del Grupo lo deben recibir.

- Un equipo puede ser miembro de varios Grupos Multicast.
- No se necesita ser miembro del Grupo Multicast para enviar un mensaje a dicho Grupo.

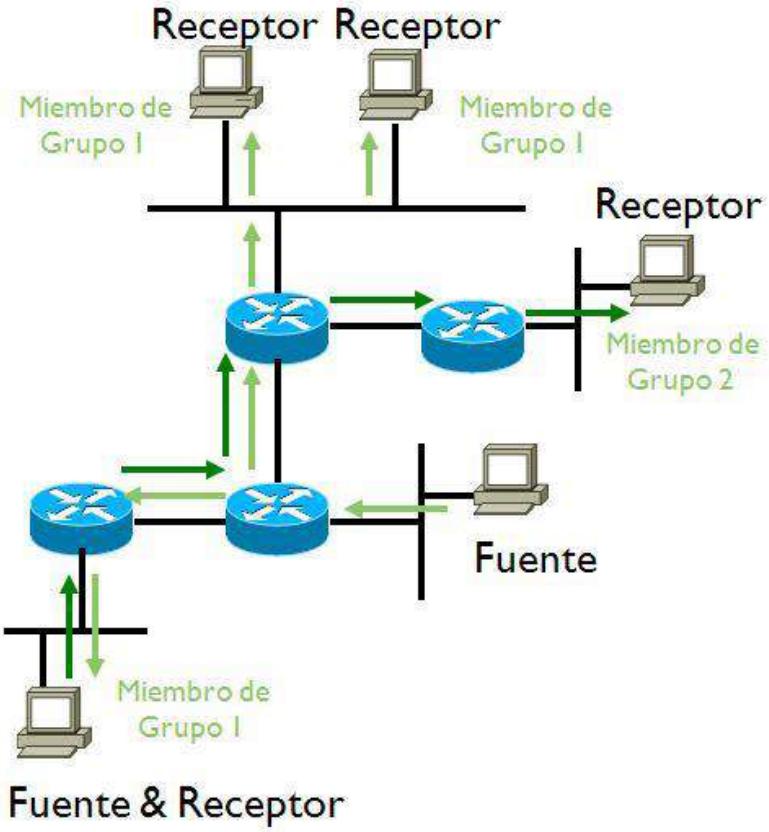

Figura 14 – Ejemplo gráfico de Multicast – Fuente: Elaboración Propia

5.5 Direcciones Multicast

El espacio típico de direccionamiento IP se distribuye en tres Grupos o clases de direcciones, que son las direcciones Clase A, B y C. La clase D es la reservada para las direcciones Multicast. La clase D tiene reservado el rango de direcciones IPv4 entre la 224.0.0.0 y la 239.255.255.255.

En realidad, se trata de Direcciones IP que comienzan con los primeros 4 bits en “1110”, con lo cual el primer Byte puede tomar valores entre el 224 y el 239. Los 28 bits restantes de menor peso están reservados para el

identificador del Grupo Multicast, tal y como se presenta en el siguiente gráfico:

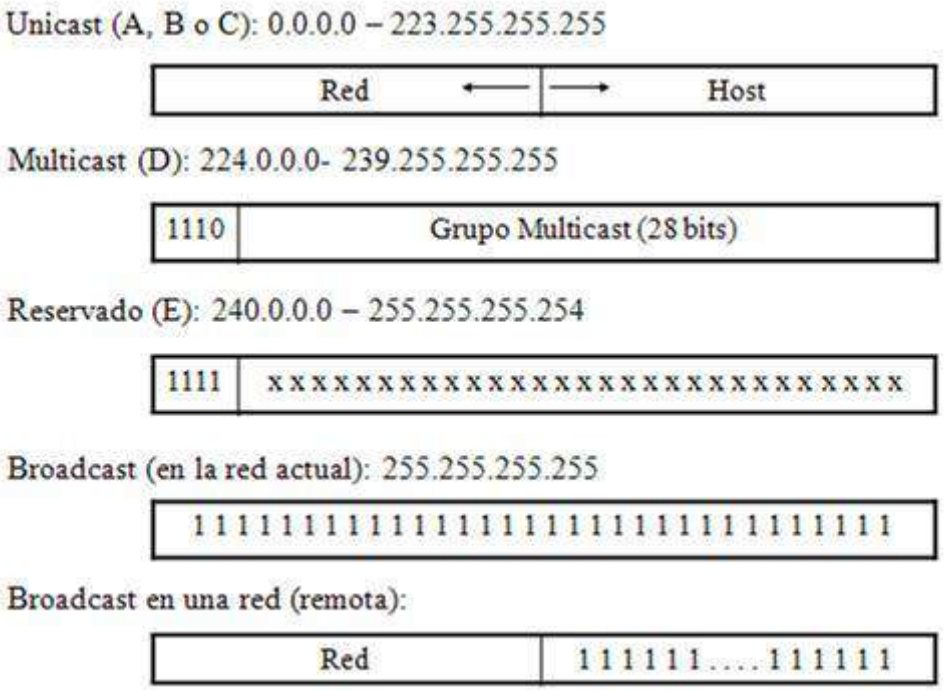

Figura 15 – Direcciones Multicast – Fuente: Elaboración Propia

Hay algunas direcciones Multicast IPv4 especiales (Doyle, 2017):

- La dirección 224.0.0.1 identifica a “todos los Hosts de una Subred que soportan Multicast”. Cualquier Host con capacidades Multicast que se encuentre en una Subred deberá unirse a este Grupo.
- La dirección 224.0.0.2 identifica a “todos los Routers con capacidades Multicast de una Subred”.
- El rango de direcciones 224.0.0.0 - 224.0.0.255 está reservado para “Protocolos de bajo nivel”. Los datagramas destinados a direcciones

dentro de este rango nunca serán encaminados por Routers Multicast. Algunos ejemplos son los siguientes:

- 224.0.0.5: Todos los Routers que soportan OSPF (Open Shortest Path First).
- 224.0.0.6: Todos los Routers DR (Designated Routers) de OSPF.
- 224.0.0.9: Todos los Routers que soportan RIPv2 (Ruteo Information Protocol versión 2).
- 224.0.0.10: Todos los Routers que soportan EIGRP (Enhanced Interior Gateway Ruting Protocol).
- 224.0.1.141: Todos los Gatekeepers que existen en un Entorno H.323

- El rango de direcciones 239.0.0.0 - 239.255.255.255 está reservado para usos administrativos. Las direcciones en este rango se asignan de forma local por cada organización, pero no se asegura que no existan otras direcciones como esas fuera de la Red de la organización. Los Routers de la organización no deberán encaminar los datagramas destinados a direcciones dentro de este rango fuera de la Red corporativa.

5.6 Asociación entre las Direcciones IP Multicast y las Direcciones de Capa II

Las direcciones Multicast IPv4 a nivel de Red, deben asociarse con las direcciones físicas, generalmente llamadas *Direcciones de Capa II*, correspondientes al tipo de Red con el que se esté trabajando.

Si se estuviese trabajando con direcciones a nivel de Red Unicast, se obtendría la dirección física asociada haciendo uso del Protocolo ARP

(Address Resolution Protocol). En el caso de direcciones de Red Multicast, el procedimiento utilizado es diferente.

En las Redes Ethernet, que son las Redes que más se utilizan, el mapeo se realiza colocando en los 24 bits de mayor peso de la dirección Ethernet los valores 01:00:5E. El siguiente bit siempre tiene un valor de 0 y los 23 bits de menor peso restantes contienen el valor de los 23 bits de menor peso de la dirección Multicast IPv4. Este proceso se muestra en el siguiente gráfico:

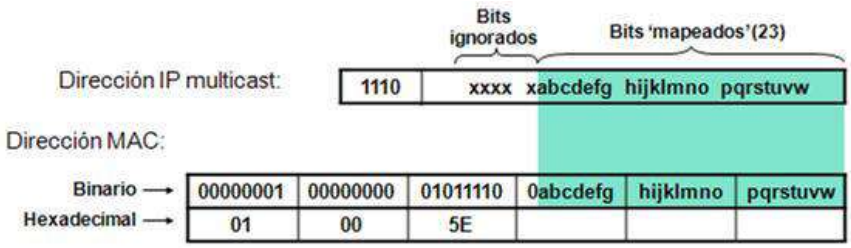

Figura 16 – Asociación IPv4 Multicast y Ethernet – Fuente: Elaboración Propia

Por ejemplo, la dirección Multicast IPv4 224.0.0.5 se correspondería con la dirección física Ethernet 01:00:5E:00:00:05.

5.7 Funcionamiento del Multicast

En una LAN, la interface de Red de un Host subirá a niveles superiores todas aquellas tramas que considere que van destinadas a ella. Estas tramas serán aquellas que tengan como dirección de destino la dirección física asociada a la interface, o aquellas tramas cuya dirección de destino sea la dirección de Broadcast.

Si el Host se ha unido a un Grupo Multicast, la interface de Red deberá reconocer también como tramas destinadas a ella, todas aquellas cuya

dirección de destino sea la correspondiente al Grupo Multicast al cual se haya unido el Host.

A título de ejemplo, si un Host de una Red tiene una interface cuya dirección física es 80:C0:F6:A0:4A:B1 y además se ha unido al Grupo 224.0.1.10, las tramas que reconocerá como destinadas a ella serán aquéllas cuya dirección de destino sea alguna de las siguientes:

- La dirección de la Interface: 80:C0:F6:A0:4A:B1
- La dirección de Broadcast: FF:FF:FF:FF:FF:FF
- La dirección Multicast asociada al Grupo: 01:00:5E:00:01:0A
- La dirección Multicast 01:00:5E:00:00:01 que se corresponde con la 224.0.0.1, por pasar a formar parte de "todos los Hosts de una Subred que soportan Multicast".

Aquí, la gran ventaja es el hecho de no necesitar el ARP para la asociación IP – MAC. Esto constituye una gran ventaja, y por varios motivos, entre los cuales están los siguientes:

- El ARP es un procedimiento que necesita del envío de mensajes en Broadcast para las solicitudes. Aquí se está evitando, con lo cual se está evitando Tráfico Broadcast innecesario, y del cual ya se sabe todos los problemas que trae consigo.
- Al no necesitar ARP, los equipos tampoco necesitan tener Tablas ARP con asociaciones que en un tiempo se pierden o que hay que refrescar.
- Si se daña la interface de LAN, y hay que cambiarla (o hay que cambiar el equipo) y, por lo tanto, cambia la dirección MAC, ello no representa ningún inconveniente para la Red Multicast, porque la asociación sigue siendo siempre la misma (siempre que no cambie la IP).

5.8 Problemas potenciales con la superposición de Direcciones

Siguiendo la metodología empleada en el apartado anterior, si se cuenta con la Dirección Multicast 224.1.1.1; esto permitirá una asociación IP – MAC hacia una MAC Address 01:00:5e:01:01:01.

El problema es que, si en el mismo contexto, se trabaja también con la Dirección IP 224.129.1.1; ó 225.1.1.1; ó 225.129.1.1; ó 226.1.1.1; y así hasta 239.129.1.1; la Dirección MAC va a ser la misma en todos los casos (McConnaughy, 2020). En la figura de abajo se observa un ejemplo similar.

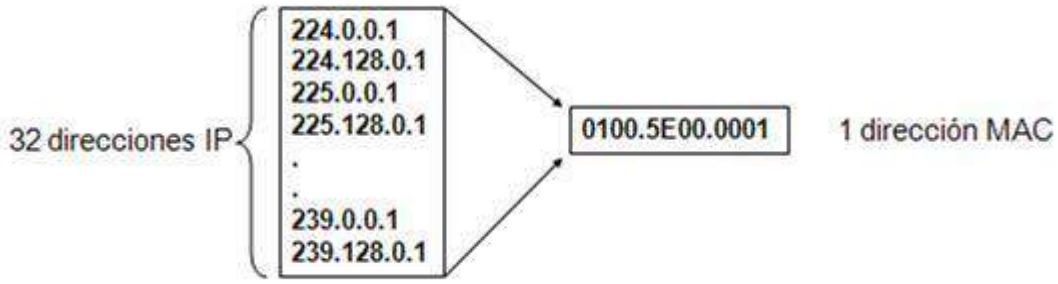

Figura 17 – Solapamiento de Direcciones Multicast – Fuente: Elaboración Propia

Este es un problema potencial, pero claramente evitable, porque si se desea tener más de un Grupo Multicast en una misma Subred, el único detalle que hay que tener en cuenta es que no exista este solapamiento y, en todo caso, elegir otras Direcciones Multicast que no se solapen.

5.9 Sobre el TTL

Es sabido que el TTL (Time To Live) es la máxima cantidad de Routers que puede atravesar un Datagrama IP antes de ser destruido, y que

fundamentalmente se utiliza para evitar Loops y el deambular erráticamente por la Red.

En Multicast, el uso que se le da al TTL es el de *establecer el ámbito* (en Inglés, limit the scope) *de la Aplicación*.

Al estar trabajando en Redes Privadas, quien diseña la Red conoce su Topología y tiene muy clara la cantidad máxima de Routers que el Datagrama va a tener que atravesar en condiciones normales. Entonces, ése valor (más uno) es el valor que se le podría configurar al TTL con el fin de asegurarse de que ese Paquete no va a estar deambulando más allá del ámbito en el que debería estar.

Inclusive, en condiciones habituales (trabajando con Direcciones IP Unicast), cuando un Router recibe un Datagrama IP con el TTL = 1, lo destruye e inmediatamente envía un mensaje ICMP (Internet Control Message Protocol) al Host que originó el Datagrama indicándole que el Datagrama ha sido destruido porque venció el TTL.

En el caso de Multicast, el Router Multicast que recibe el Datagrama IP Multicast (es decir, un Datagrama que tiene una Dirección IP Multicast como Dirección Destino) con TTL = 1, lo destruye, *pero no envía el mensaje ICMP al origen* porque, en este caso, se pretendía que justamente *ESE* Router destruyera ese Datagrama.

Es decir, el mensaje ICMP se envía habitualmente cuando, para el Origen, un aviso de destrucción de Datagrama es algo inesperado y en tal caso está proveyendo información importante. Como se mencionó antes, en este caso no tiene sentido avisar, porque el Host origen insertó ese valor de TTL al Datagrama con toda la intención de que el Router en cuestión lo destruyera.

Generalmente se habla de Umbrales de TTL (en Inglés, TTL Thresholds), y eso es lo que se configura en los Routers, y se pueden configurar valores distintos para cada interface.

5.10 IGMP (Internet Group Management Protocol)

El Protocolo IGMP es un Protocolo accesorio de Capa III que permite que los Routers puedan detectar cuáles son los Grupos Multicast de los Hosts que tienen conectados en sus interfaces.

Gracias a la información recopilada mediante IGMP, los Routers mantienen una lista de los Grupos Multicast a los que están asociados los Hosts que están conectados en sus interfaces. Dado que generalmente los Hosts se conectan a redes locales, todos los mensajes IGMP se envían con un valor de TTL igual a 1, por lo que los mensajes IGMP solo pueden ser intercambiados entre equipos directamente conectados entre sí (normalmente entre Hosts y Routers conectados en una misma LAN) (Loveless et al, 2016).

Existen tres versiones de IGMP: 1, 2 y 3. Dado que cada versión es una ampliación de la anterior, es más sencillo comentar sus funcionalidades por orden cronológico.

El Protocolo IGMPv1 fue definido en el apéndice I del RFC 1112 (Host Extensions for IP Multicasting) aprobado en 1989. Además del IGMP, dicho RFC especifica todos los aspectos fundamentales de la transmisión Multicast y se le considera un documento esencial sobre IP Multicast.

IGMPv1 es un Protocolo sencillo, puesto que sólo implementa dos tipos de mensajes.

Por un lado, existen los mensajes “Membership Query”, que son emitidos por los Routers y enviados a la dirección Multicast 224.0.0.1 (todos los Hosts Multicast de la red). Su objetivo es consultar a los Hosts en qué Grupos Multicast están asociados.

Los Hosts responden a un “Membership Query” con un mensaje “Membership Report”, en el cual informan a los Routers de los Grupos a

los que están asociados. El mensaje “Membership Report” es enviado a la dirección Multicast en la que está asociado el Host.

Cuando un proceso en un Host de una Subred se asocia a un Grupo Multicast, este Host envía un mensaje IGMP a todos los Routers Multicast de su Subred informándoles que, cuando reciban un mensaje Multicast destinado al Grupo al cual él se ha asociado, lo envíen a la Subred para que pueda recibirlo. Estos Routers le comunicarán esta información al resto de Routers Multicast de tal forma que todos los Routers aprendan adónde deberán encaminar los mensajes Multicast que le lleguen.

Los Routers, además envían de forma periódica mensajes IGMP al Grupo 224.0.0.1 solicitando información a los Hosts sobre los Grupos a los cuales están asociados. Un Host, al recibir este mensaje, inicializa un temporizador con un valor aleatorio, y no contestará hasta que este temporizador llegue a cero. Con esto se evita que todos los Hosts contesten a la vez, produciendo una sobrecarga innecesaria en la Red. Cuando el temporizador de alguno de los Hosts llegue a cero, dicho Host enviará su respuesta a la dirección del Grupo Multicast del cual esté informando, por lo que el resto de Hosts asociado a ese Grupo también la verán y anularán su temporizador, cancelando, por lo tanto, su respuesta.

Este procedimiento se realiza de este modo porque, con que un solo Host conteste es suficiente. Al Router únicamente le hace falta saber que hay al menos un Host interesado en determinado Grupo en esa Subred, y entonces, con esa información ya le basta para redirigir los mensajes Multicast destinados al Grupo.

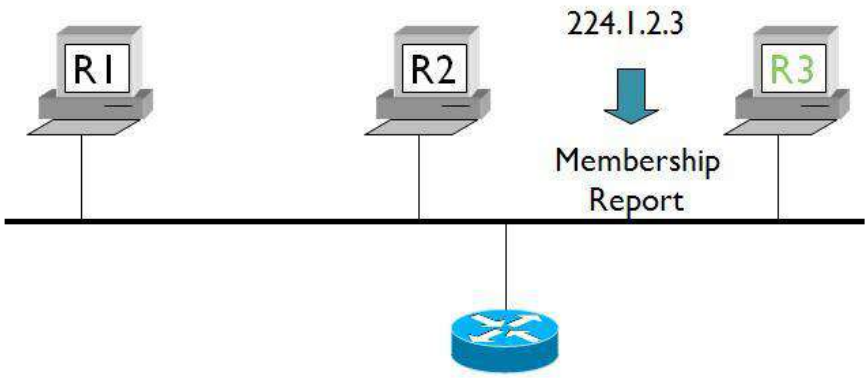

Figura 18 – El Router 3 se presenta y envía un mensaje "Membership Report" – Fuente: Elaboración Propia

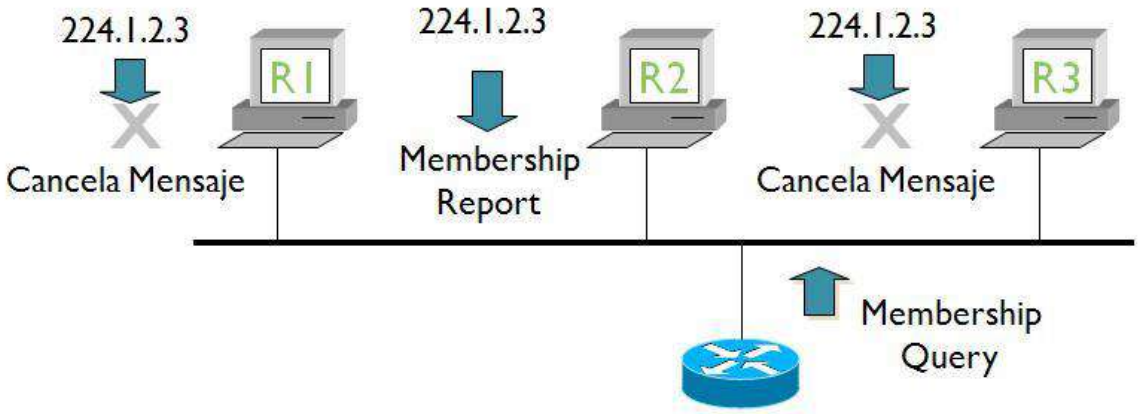

Figura 19 – El Router consulta sobre los Grupos Multicast y sólo R2 responde – Fuente: Elaboración Propia

Si todos los Hosts que estaban en un determinado Grupo se retiran del mismo, entonces ninguno contestará a los mensajes del Router. En ese caso, al detectar que ya no hay equipos interesados en un determinado Grupo en una Subred, dejará de encaminar a la misma los mensajes destinados a ese Grupo.

Otra opción, implementada en IGMPv2, es que el propio Host indique a los Routers que ha abandonado un determinado Grupo, enviando para ello un mensaje de "Membership Leave" a la dirección 224.0.0.2.

5.11 Análisis de una Captura de IGMP

A continuación tenemos 2 (dos) Capturas realizadas con el Analizador de Protocolo Wireshark (http://www.wireshark.org) en el que podemos observar una Solicitud (Membership Query) y una Respuesta (Membership Report) de IGMP.

```
Ethernet II
    Destination: 01:00:5e:00:00:01 (01:00:5e:00:00:01)
    Source: 00:01:f4:8d:2c:e0 (Enterasy_8d:2c:e0)
    Type: IP (0x0800)
Internet Protocol
    Version: 4 ; Header length: 20 bytes
    Differentiated Services Field: 0x00
    Total Length: 28
    Identification: 0x169e (5790)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 1
    Protocol: IGMP (0x02)
    Header checksum: 0xb865 (correct)
    Source: 10.11.0.209 (10.11.0.209)
    Destination: 224.0.0.1 (224.0.0.1)
Internet Group Management Protocol
    IGMP Version: 2
    Type: Membership Query (0x11)
    Max Response Time: 10,0 sec (0x64)
    Header checksum: 0xee9b (correct)
    Multicast Address: 0.0.0.0 (0.0.0.0)

0000  01 00 5e 00 00 01 00 01 f4 8d 2c e0 08 00 45 00   ..^.......,...E.
0010  00 1c 16 9e 00 00 01 02 b8 65 0a 0b 00 d1 e0 00   .........e......
0020  00 01 11 64 ee 9b 00 00 00 00 80 18 00 00 14 00   ...d............
0030  02 00 0f 00 00 00 00 00 00 00 00 00               ............
```

Figura 20 – Captura de Mensaje IGMP "Membership Query" – Fuente: Elaboración Propia

```
Ethernet II
    Destination: 01:00:5e:50:44:53 (01:00:5e:50:44:53)
    Source: 00:50:8b:a3:76:58 (10.11.0.100)
    Type: IP (0x0800)
Internet Protocol
    Version: 4 ; Header length: 24 bytes
    Differentiated Services Field: 0x00
    Total Length: 32
    Identification: 0xb767 (46951)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 1
    Protocol: IGMP (0x02)
    Header checksum: 0x335e (correct)
    Source: 10.11.0.100 (10.11.0.100)
    Destination: 235.80.68.83 (235.80.68.83)
```

```
    Options: (4 bytes) [Router Alert: Every Router examines packet]
Internet Group Management Protocol
    IGMP Version: 2
    Type: Membership Report (0x16)
    Max Response Time: 0,0 sec (0x00)
    Header checksum: 0xba5b (correct)
    Multicast Address: 235.80.68.83 (235.80.68.83)

0000  01 00 5e 50 44 53 00 50 8b a3 76 58 08 00 46 00   ..^PDS.P..vX..F.
0010  00 20 b7 67 00 00 01 02 33 5e 0a 0b 00 64 eb 50   . .g....3^...d.P
0020  44 53 94 04 00 00 16 00 ba 5b eb 50 44 53 00 01   DS.......[.PDS..
0030  00 00 00 01 00 00 03 62 69 73 0c 31               .......bis.1
```

Figura 21 – Captura de Mensaje IGMP "Membership Report" – Fuente: Elaboración Propia

Las dos capturas se corresponden con dos mensajes IGMP, un mensaje de Membership Query y un mensaje de Membership Report.

En el mensaje de Query, que va dirigido desde el Router a los Hosts Multicast, se puede observar que la Dirección IP Destino es 224.0.0.1 (que se corresponde con la Ethernet 01 :00 :5e:00 :00 :01 y que referenciaba a "todos los Hosts de una Subred que soportan Multicast". Otro detalle por observar en la primera captura es el valor del TTL (Time To Live) en 1, lo cual es lógico porque, como ya se mencionó, este tipo de mensajes nunca va a atravesar una LAN (Local Area Network).

A continuación de la indicación del TTL aparece el campo de Protocolo del mensaje IP, el cual vale "02", lo cual implica IGMP.

El Formato del mensaje IGMP es muy sencillo. El primer Parámetro indica el Tipo de Mensaje (Type) y en este caso el número 0x11 indica Membership Query. El segundo Parámetro es el tiempo máximo que el Router va a esperar una respuesta (Maximum Response Time) por parte de los Hosts. En este caso, el tiempo que se va a esperar será de 10 segundos, y se indica con el número 0x64, que en el Sistema Decimal es el 100 porque el valor que hay que configurar aquí es el tiempo, pero medido en décimas de segundo.

Algo importante a destacar es que, al igual que en muchos otros Protocolos de TCP/IP, tales como el ARP (Address Resolution Protocol), sin

ir más lejos, en el IGMP se utiliza el mismo formato de mensaje para todos los casos. Esto es importante aclararlo, porque en la respuesta a este mensaje; es decir, en el mensaje Membership Report, también estará "Maximum Response Time" como segundo parámetro, pero aquí tendrá valor "0" porque simplemente no se utiliza en este caso.

El tercer Parámetro del Mensaje IGMP es un Checksum, que no merece mayores comentarios. El cuarto Parámetro, contrariamente al caso del "Maximum Response Time", sólo tiene valor en la respuesta; es decir, en el mensaje Membership Report, porque aquí es en donde el Host en cuestión va a escribir cuál es la Dirección IP del Grupo Multicast al que pertenece. Aquí, al igual que antes, el valor que tiene es "0".

En la Respuesta (Membership Report), nuevamente el primer Parámetro es el Tipo de Mensaje (en este caso el calor es 0x16 indicando "Membership Report"), como se mencionó antes, el segundo Parámetro, que es el "Maximum Response Time", aquí vale "0", el tercer Parámetro es el Checksum y el cuarto Parámetro, aquí sí tiene un valor y es la Dirección IP del Grupo Multicast (o al menos, de uno de los Grupos Multicast a los que pudiera pertenecer) del Host que está enviando este Mensaje. También aquí, el TTL es igual a "1".

Algo importante a destacar en esta Respuesta es que, además de informar (mediante el mensaje IGMP) al Router que este Host pertenece al Grupo 235.80.68.83, también está enviando este mensaje a la Dirección IP Destino 235.80.68.83 (cuya MAC sería 01:00:5e:50:44:53). Con esto último se cumpliría lo de informar mediante este Mensaje a los otros miembros del Grupo, de tal forma que ya no sea necesario que algún otro miembro conteste en nombre del mismo.

El único detalle de todo esto es que, si bien los miembros del Grupo van a leer este mensaje, y por lo tanto se va a cumplir el objetivo mencionado en el párrafo anterior, el que no va a leer el mensaje va a ser el principal interesado, que es el Router (*porque el Router no pertenece a ese Grupo, o no tiene por qué pertenecer*). Entonces, para que el mensaje pueda ser

leído por los miembros del Grupo y también por el Router, lo que se termina haciendo es, por un lado, enviar dicho mensaje al Grupo (como ya se mencionó), y en el campo de Opciones de IP, se agrega una opción que se llama Router Alert (especificada en el RFC 2113). Con esta Opción agregada en un Mensaje IP, cada Router, por más que ese mensaje no sea para él, igualmente debe examinar al mismo.

6 Redes SDN (Software Defined Networks)

Las Redes SDN (Software Defined Networkd, en Español, Redes Definidas por Software) son una nueva forma de diseñar y gestionar redes de computadoras, que permite una mayor flexibilidad y adaptabilidad a los cambios en la demanda y las necesidades de los usuarios.

La idea principal detrás de SDN es separar la lógica de control de la red de los dispositivos de red, tales como routers y switches, y llevarla a un software centralizado. Esto permite una mayor flexibilidad y agilidad en la gestión, lo que es particularmente importante en entornos de red dinámicos y de rápido cambio.

La ONF (Open Networking Foundation[1]) define SDN de la siguiente manera:

> Una arquitectura emergente que es dinámica, manejable, rentable y adaptable, lo que la hace ideal para la naturaleza dinámica y de alto ancho de banda de las aplicaciones. Esta arquitectura desacopla el control de la red (Switching/Routing) y las funciones de reenvío (Forwarding), lo que permite que el control de la red se vuelva directamente programable y que la infraestructura subyacente se abstraiga para aplicaciones y servicios de red.

6.1 Introducción

Las SDN son una nueva arquitectura de red que separa la capa de control de la capa de datos en una red. En lugar de tener un router o switch que tenga tanto la lógica de control como los datos, en una red SDN, el control se maneja por separado en un controlador de red centralizado.

[1] https://opennetworking.org/sdn-definition/

El controlador recibe información de los dispositivos en la red (por ejemplo, switches y routers, entre otras opciones) y toma decisiones de enrutamiento basadas en esa información. El principal beneficio de las SDN es su capacidad para permitir la programación de la red. Esto significa que la red se puede ajustar para adaptarse a los requisitos específicos de los usuarios y aplicaciones, permitiendo, a su vez, la posibilidad de automatizar tareas, logrando la reducción de costos operativos.

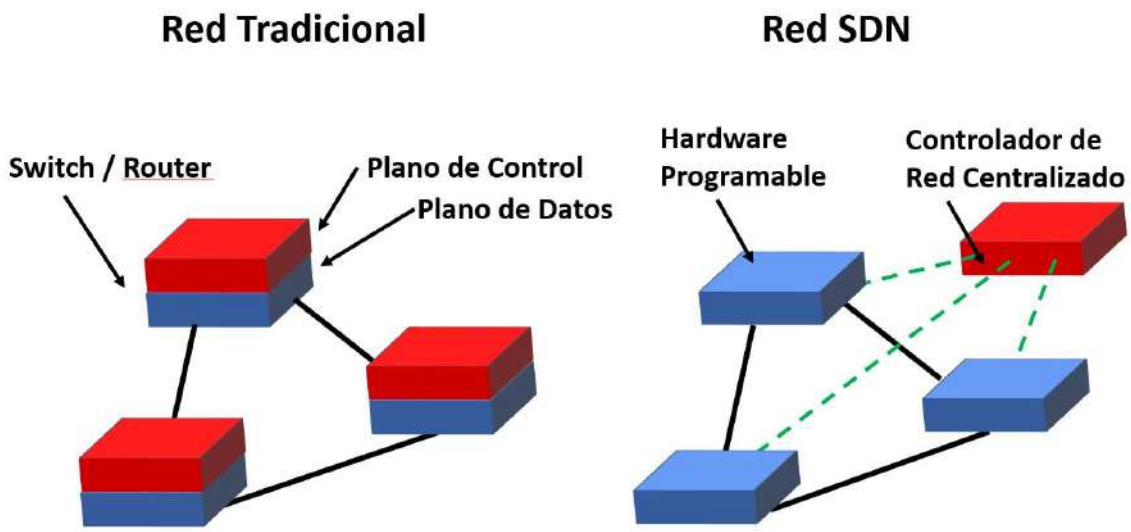

Figura 22 – Red Tradicional versus Red SDN – Fuente: (Prajapati et al, 2018)

El **Plano de Control** incluye un conjunto de protocolos y características que implementa un dispositivo de red para que pueda determinar la ruta más adecuada para reenviar el tráfico de datos (en Inglés, Routing/Switching). Los protocolos de Spanning Tree y los protocolos de ruteo, tales como OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Routing Protocol) y BGP (Border Gateway Protocol) son algunos de los protocolos que conforman el plano de control en los dispositivos de red. Estos protocolos ayudan a construir las tablas de conmutación o enrutamiento en estos dispositivos para permitirles determinar cómo reenviar el tráfico de red.

El **Plano de Datos** incluye los protocolos y funciones que implementa un dispositivo de red para reenviar el tráfico (en Inglés, Forwarding) a su destino lo más rápido posible. El objetivo principal del plano de datos es determinar cómo se debe reenviar el paquete entrante en un puerto a un puerto saliente, en función de valores específicos en los encabezados del paquete.

En las Redes Tradicionales, el Plano de Control y el Plano de Datos formaban parte de la arquitectura del dispositivo de red y trabajaban juntos para determinar la ruta que debía seguir el tráfico de datos a través de la red y cómo mover este tráfico lo más rápido posible desde su origen hasta su destino. Como se mencionó anteriormente, las Redes SDN sugieren un enfoque diferente (Jackson et al, 2021).

6.2 Beneficios de las SDN

Como ya se mencionó, el concepto SDN separa la funcionalidad del plano de control y el plano de datos en diferentes dispositivos, y se obtienen varios beneficios. A continuación, se detallan los más representativos:

- El costo de la red resultante es menor, ya que no todos los dispositivos de red tienen que implementar costosas funciones de software y hardware para acomodar un plano de control y un plano de datos. Ahora, la inteligencia del plano de control se limita a unos pocos dispositivos que se convierten en el cerebro de la red, y el plano de datos se construye con dispositivos más económicos que implementan solo la función de Forwarding.

- La convergencia de esta nueva red, que es la cantidad de tiempo que tardan todos los dispositivos en tener una vista actualizada de la red, debería ser mucho menor que en el caso de las arquitecturas

tradicionales. En redes de tamaños similares, las construidas con dispositivos de red que implementan tanto el plano de control como el plano de datos en su arquitectura tardan mucho más en intercambiar toda la información necesaria para reenviar el tráfico de datos que las redes que implementan funciones separadas de control y plano de datos. en su arquitectura. Dependiendo del tamaño de una red, esto podría significar esperar a que decenas, cientos o miles de dispositivos intercambien información a través de sus protocolos de plano de control y establezcan una determinada vista de la red. En este sentido, las mejoras en el tiempo de convergencia son enormes.

- Por otra parte, la gestión de los dispositivos de red se simplifica notablemente. El siguiente ejemplo desarrolla con más detalle este concepto.

La Figura 23 presenta tres elementos de red: un Router, un Switch y un Access Point inalámbrico. Para cada uno de ellos, se puede observar el Plano de Control y el Plano de Datos.

La gestión de estos dispositivos incluye las funciones para controlar y monitorear estos dispositivos. Como la función de control y monitoreo debe realizarse en cada dispositivo, se llama a esta arquitectura una "arquitectura de plano de control distribuido".

El inconveniente que tiene esta forma de gestión es que los administradores de red tienen que gestionar cada dispositivo de forma independiente, iniciando sesión en cada uno de ellos y configurándolo.

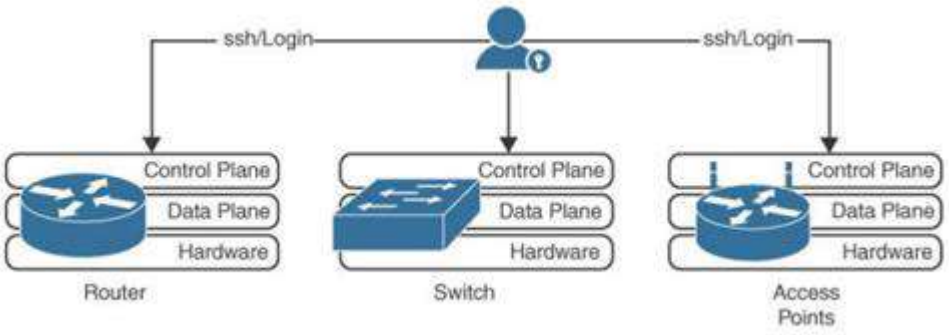

Figura 23 – Planos de Control y de Datos en una Red Tradicional – Fuente: (Jackson et al, 2021)

Para evitar la ineficiencia de administrar manualmente los dispositivos de red, se puede utilizar un controlador único de red. Cuando se utiliza un controlador de estas características, se mueven los planos de control de cada dispositivo de red y se los consolida todos en este controlador único de red.

Dicho controlador puede comunicarse con los elementos de red y éstos pueden enviar datos de gestión al controlador. Debido a que ahora existe un único controlador, esta arquitectura se denomina “plano de control centralizado”.

La Figura 24 muestra cómo se puede utilizar un controlador de red para administrar y controlar mediante programación varios elementos de red usando las API hacia el Norte/Arriba (Northbound) y hacia el Sur/Abajo (Southbound) (Jackson et al, 2021).

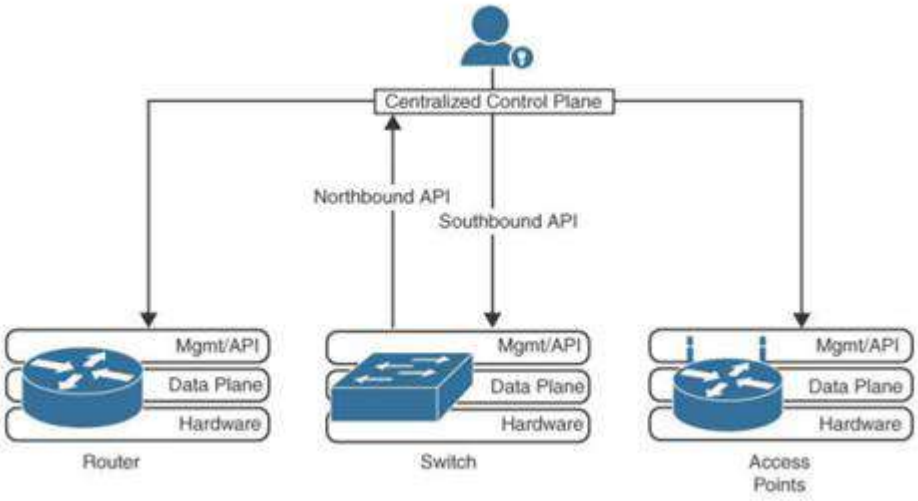

Figura 24 – Planos de Control centralizado en una Red SDN – Fuente: (Jackson et al, 2021)

6.3 Arquitectura de SDN

La arquitectura de una red SDN se divide en tres capas: la capa de Infraestructura, la capa de Control y la capa de Aplicación.

- La capa de **Infraestructura** se compone de equipos de red y elementos que forman la red real y elementos que ayudan a reenviar (Forwarding) el tráfico de red. Podría ser un conjunto de Switches y Routers en la red o centros de datos. La capa de infraestructura es la capa física sobre la que se encuentran las funciones de virtualización de red a través de la capa de control.

- La capa de **Control** es donde residen los controladores SDN para controlar la infraestructura de la red. La capa de control tiene la lógica comercial para obtener y mantener diferentes tipos de información de red, detalles de estado, detalles de topología y detalles de estadísticas. El controlador SDN tiene que ver con la gestión de redes y tiene toda la lógica de control para los casos de uso de la red, como conmutación, ruteo, VPN de capa 2, VPN de

capa 3, reglas de seguridad de firewall, DNS y DHCP, entre otras opciones. Además, provee de información a la capa de Aplicación.

- La capa de **Aplicación** es un área de desarrollo en donde se están produciendo muchas innovaciones. Las aplicaciones de esta capa aprovechan la información sobre la topología de la red, el estado de la red, las estadísticas de la red, entre otras opciones. Se pueden desarrollar varios tipos de aplicaciones, como las relacionadas con la automatización de redes, la configuración de redes, el monitoreo de redes, la solución de problemas de redes, las políticas de redes y la seguridad. Estas aplicaciones SDN pueden proporcionar varias soluciones de extremo a extremo para redes empresariales y de centros de datos del mundo real.

La capa de Control es el núcleo de la arquitectura SDN, ya que es aquí donde se toman las decisiones sobre el tráfico de la red. En SDN, la capa de control está centralizada, lo que significa que todas las decisiones de red se toman desde una ubicación central. Como ya se mencionó, esto permite una mayor flexibilidad y agilidad en la gestión de redes, lo que es particularmente importante en entornos de red dinámicos y de rápido cambio (Jackson et al, 2021).

Los siguientes son los protocolos más populares con los que el controlador se comunica con los dispositivos de red.

- **OpenFlow**: la ONF gestiona este estándar utilizado para la comunicación entre el controlador SDN y los dispositivos de red gestionados.

- **OpenDayLight**: The Linux Foundation[2] administra este estándar, que utiliza OpenFlow para administrar dispositivos de red.

[2] https://www.linuxfoundation.org/

Las siguientes figuras representan las tres capas de una arquitectura de SDN. La primera (Figura 25), muy genérica (pero muy didáctica) propuesta por la ONF (Open Networking Foundation) mientras que la siguiente (Figura 26) ofrece un esquema mucho más pormenorizado.

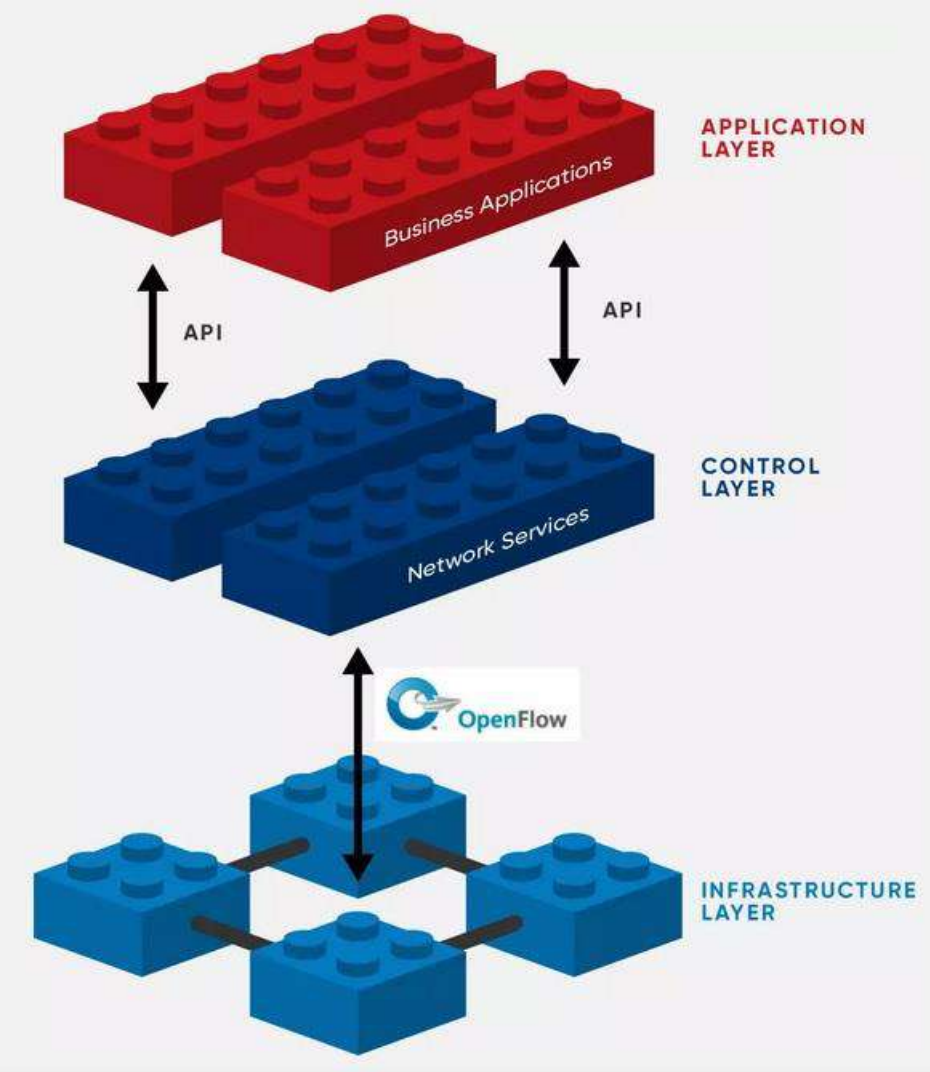

Figura 25 – Arquitectura de una Red SDN – Fuente: https://opennetworking.org/sdn-definition/

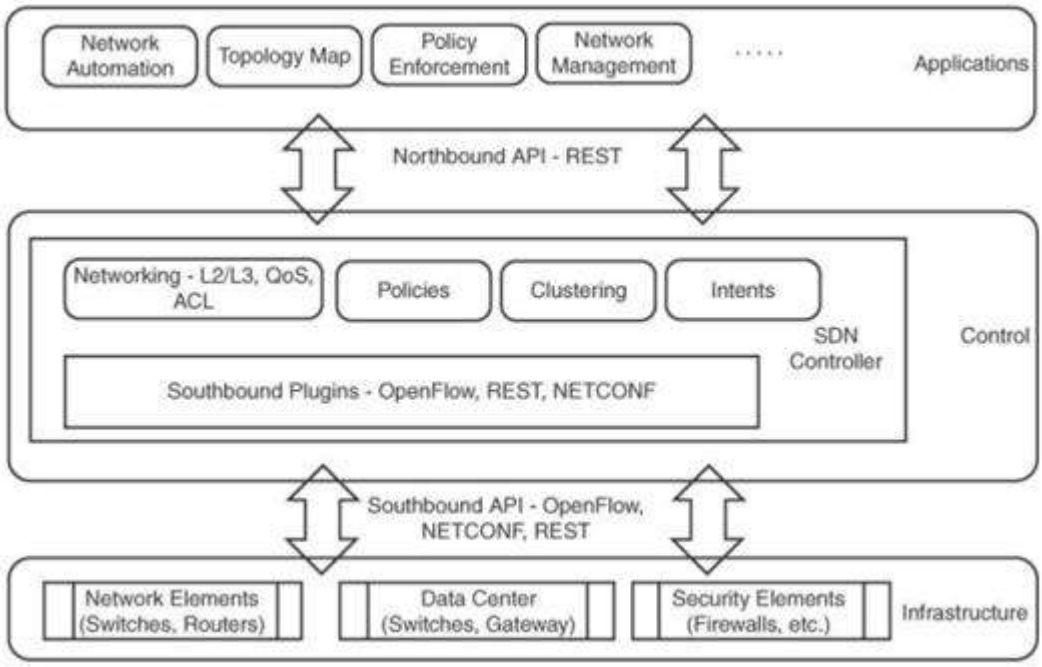

Figura 26 – Arquitectura pormenorizada de una Red SDN – Fuente: (Jackson et al, 2021)

6.4 Ventajas de SDN

Si bien, directa o indirectamente, ya se hizo mención de gran parte de lo que sigue a continuación, aquí se presenta a modo de resumen. Algunas de estas ventajas son:

- **Mayor flexibilidad**: las redes SDN son más flexibles que las redes tradicionales. Esto significa que la red puede adaptarse a las necesidades del usuario y las aplicaciones. Este concepto es muy similar al de las Máquinas Virtuales comparándolas con un Hardware (Server) Dedicado.

- **Mayor eficiencia**: las redes SDN pueden ser más eficientes en términos de costos y recursos. Esto se debe a que el controlador de red centralizado puede tomar decisiones basadas en una visión completa de la red, en lugar de decisiones tomadas individualmente por cada dispositivo.

- **Automatización**: la tecnología SDN permite la automatización de muchas áreas en la administración de la red, lo que a su vez puede reducir los costos operativos.
- **Mejora del rendimiento**: las redes SDN pueden mejorar el rendimiento de la red al permitir un enrutamiento más eficiente del tráfico y una mejor utilización de los recursos de la red.
- **Mayor seguridad**: las redes SDN pueden mejorar la seguridad de la red mediante la aplicación de políticas de seguridad centralizadas y la capacidad de detectar y responder a amenazas de seguridad de manera más eficiente.

6.5 Desafíos y oportunidades de SDN

Uno de los mayores desafíos asociados con la implementación de SDN es la necesidad de una mayor integración con los dispositivos de red existentes. Muchas organizaciones ya tienen dispositivos de red instalados, lo cual significa que es necesario encontrar una manera de integrar SDN con estos dispositivos.

Por otro lado, SDN también ofrece muchas oportunidades, tales como la capacidad de utilizar técnicas avanzadas de análisis de datos y aprendizaje automático para mejorar la gestión de la red, tema que se verá con más detalle en el próximo apartado en relación con el uso de la Inteligencia Artificial.

Además, como ya se mencionó, una Red SDN también puede mejorar la capacidad de las organizaciones para adaptarse a los cambios en el entorno de la red, lo que puede ser particularmente importante en entornos de red dinámicos y en evolución.

6.6 Uso de la inteligencia artificial en las redes SDN

Las redes SDN también plantean nuevos desafíos y oportunidades para la inteligencia artificial (IA), que es la disciplina que estudia cómo crear sistemas capaces de realizar tareas que normalmente requieren inteligencia humana, tales como el aprendizaje, el razonamiento, la percepción o la toma de decisiones.

La IA puede aportar soluciones para mejorar el rendimiento, la seguridad, la fiabilidad y la adaptabilidad de las redes SDN, así como para optimizar el uso de los recursos y reducir los costes operativos.

El controlador SDN ofrece una representación simplificada y unificada de la red a las aplicaciones externas, ocultando los detalles específicos de cada dispositivo o tecnología. Esto facilita el desarrollo e integración de servicios y aplicaciones sobre la red, así como su portabilidad entre diferentes entornos.

Por otro lado, la Inteligencia Artificial (IA) es un campo que engloba diversas ramas, tales como el aprendizaje automático (Machine Learning), el procesamiento del lenguaje natural (Natural Language Processing), la visión artificial (Computer Vision), los sistemas expertos (Expert Systems) o la robótica (Robotics), entre otras. La IA puede aplicarse a diversos dominios y problemas y también puede clasificarse según diferentes criterios, tales como el tipo de aprendizaje o el tipo de razonamiento.

A continuación, se presentan algunas categorías relevantes para las redes SDN.

6.6.1 Aprendizaje supervisado

Es un tipo de aprendizaje en el que se dispone de un conjunto de datos etiquetados con la salida deseada para cada entrada. El objetivo es encontrar una función que relacione las entradas con las salidas, y que pueda generalizar a nuevos datos no vistos. Algunos ejemplos son la

regresión lineal, la clasificación binaria o multiclase, o las redes neuronales artificiales.

El algoritmo utiliza estos datos etiquetados para crear un modelo que pueda clasificar nuevos datos. En el contexto de las redes SDN, los enfoques supervisados se pueden utilizar para predecir los flujos de red y detectar anomalías en el tráfico de red.

Por ejemplo, como se mencionó anteriormente, se puede utilizar un modelo de aprendizaje automático supervisado para predecir el flujo de red en función de las características del tráfico de red, como el puerto de origen y destino, el protocolo utilizado y el tamaño del paquete. Si el modelo predice que un flujo de red es anómalo, se puede tomar una acción para bloquear el flujo de red y prevenir un ataque de seguridad.

6.6.2 Aprendizaje no supervisado

Es un tipo de aprendizaje en el que no se dispone de etiquetas para los datos, y el objetivo es encontrar patrones, estructuras o relaciones ocultas en los mismos. Algunos ejemplos son el análisis de componentes principales, el clustering o la detección de anomalías.

Por ejemplo, se puede utilizar un algoritmo de clustering no supervisado para agrupar el tráfico de red en diferentes categorías. Si un nuevo flujo de red no se ajusta a ninguna de estas categorías, se puede tomar una acción para investigar el flujo de red y prevenir un ataque de seguridad.

6.6.3 Aprendizaje por refuerzo

Es un tipo de aprendizaje en el que un agente interactúa con un entorno y recibe una recompensa (positiva o negativa) por cada acción que realiza. El objetivo es aprender una política que maximice la recompensa acumulada a largo plazo. Algunos ejemplos son los algoritmos Q-learning, SARSA (State–action–reward–state–action) o DQN (Deep Q-Networks).

En el contexto de las redes SDN, un agente de aprendizaje por refuerzo podría aprender a detectar y prevenir ataques de seguridad mediante la retroalimentación de recompensa proporcionada por el controlador de red.

6.6.4 Razonamiento deductivo

Es un tipo de razonamiento en el que se parte de unas premisas generales y se infieren conclusiones específicas mediante la aplicación de reglas lógicas. Algunos ejemplos son los sistemas expertos basados en reglas, los sistemas de lógica difusa o los sistemas de inferencia bayesiana.

Un ejemplo de este tipo de razonamiento en las redes SDN podría ser para optimizar la ruta de los datos. La IA puede analizar el tráfico de red y determinar la mejor ruta para enviar los datos en función de una variedad de factores, como la congestión de la red, la latencia y el ancho de banda disponible. De este modo, se puede mejorar el rendimiento de la red y reducir los tiempos de respuesta.

También podría ayudar en la detección de fallas en la red. La IA puede analizar los patrones de tráfico de la red y detectar cuando hay un problema en la red. Una vez que se detecta un problema, la IA puede tomar medidas para solucionar el problema y restaurar la normalidad en la red.

6.6.5 Razonamiento inductivo

Es un tipo de razonamiento en el que se parte de unos casos particulares y se generalizan a unas reglas o principios universales mediante la búsqueda de regularidades o similitudes. Algunos ejemplos son los algoritmos genéticos, las redes neuronales artificiales o los árboles de decisión.

Por medio del uso de redes neuronales artificiales se podría modelar datos complejos y ser utilizados para predecir el tráfico de red, detectar ataques de seguridad y optimizar el uso de ancho de banda en una red SDN.

6.6.6 Razonamiento abductivo

Es un tipo de razonamiento en el que se parte de unos hechos observados y se infieren unas hipótesis o causas posibles que los expliquen, seleccionando la más plausible o probable.

En síntesis, la IA se está convirtiendo rápidamente en una herramienta importante para las redes SDN, ya que permite una gestión de red más inteligente y automatizada. Y, tal como se ha mencionado, fundamentalmente se puede utilizar para predecir la demanda de tráfico y ajustar la capacidad y el consumo energético de los dispositivos, o para detectar fallos y repararlos automáticamente, como así también colaborar en aspectos relacionados con la seguridad de la Red. (Fortinet, 2023) (García, 2019) (IBM, 2021).

6.7 Ejemplo de Aplicación de Aprendizaje por Refuerzo en una SD-WAN

El Aprendizaje por Refuerzo (o bien, en Inglés, RL o Reinforcement Learning) es una rama del aprendizaje automático que estudia cómo un agente aprende a tomar decisiones siguiendo una estrategia de ensayo y error.

A continuación, se presenta un ejemplo experimentando el aprendizaje por refuerzo para resolver un problema muy pertinente en las redes SD-WAN, que es el de la selección de enlaces (Chakravarty, 2018).

La selección de enlaces es un componente crucial en una solución SD-WAN, ya que es el núcleo de su solución.

La Figura 27 presenta los elementos principales de los modelos del Aprendizaje por Refuerzo. El **agente** es el sujeto del entrenamiento y el que tiene que aprender a tomar decisiones. El **entorno**, en cambio, representa el mundo con el que interactúa el agente. En cada interacción t, el agente recibe una **observación** total o parcial (O) del estado del entorno (S). En base a la observación decide qué **acción** (A) tomar. Una vez ejecutada la acción, el agente recibe una recompensa numérica (R) y una nueva observación del entorno, permitiéndole evaluar la acción realizada y dar un nuevo paso (Sutton et al, 2021).

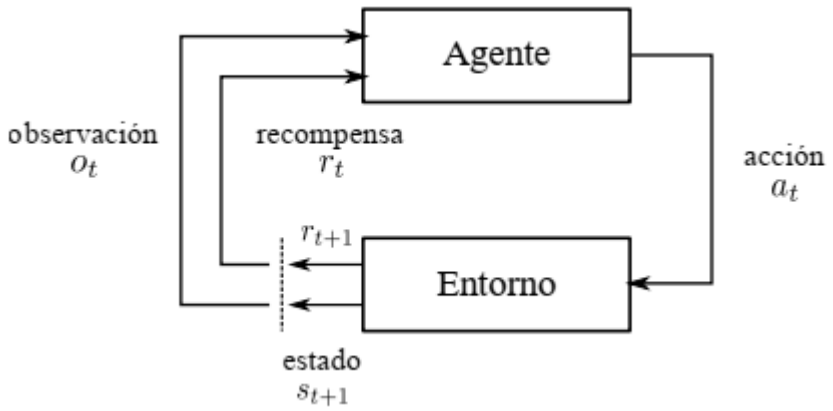

Figura 27 – Elementos principales del Aprendizaje por Refuerzo – Fuente: (Sutton et al, 2021)

La relevancia de este aprendizaje de refuerzo para una SD-WAN se puede pensar a través de un experimento en el que un agente cambia los enlaces WAN y trata de maximizar la utilización del ancho de banda.

Esto se hace cambiando a la nube de Internet siempre que haya suficiente ancho de banda disponible y luego volviendo a MPLS cuando los valores de QOS comienzan a decrecer. El objetivo es cómo hacer dicho conmutador de enlace para lograr un ancho de banda óptimo con una utilización mínima del enlace MPLS.

6.7.1 Entorno para SD-WAN

En este caso se trata de una red WAN entre la llamada "Sucursal" y la "Casa Matriz u Oficina Central". En esta red simplificada existen dos caminos alternativos, uno a través de un circuito MPLS dedicado y otro a través de la Red Pública de Internet.

En la Figura 28, tenemos dos Routers (R1 y R2) que representan el Router del borde de la Sucursal y el borde del lado de la Casa Matriz, respectivamente.

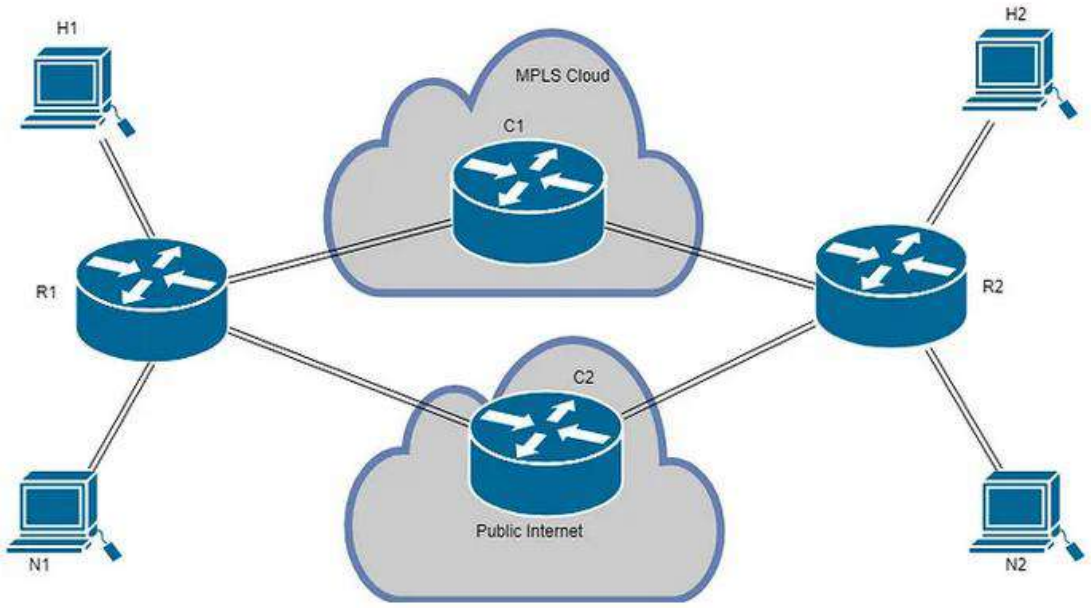

Figura 28 – Ejemplo de Aplicación de Aprendizaje por Refuerzo – Fuente: (Chakravarty, 2018)

6.7.2 Observación (o estado) del entorno

Los siguientes parámetros se observan para obtener información del Estado del Entorno

- Ancho de banda actual: la cantidad de ancho de banda obtenido por cualquier ruta, por ejemplo, MPLS o Internet pública
- Ancho de banda disponible: este es el ancho de banda disponible en la nube de Internet. Se supone que la ruta MPLS tiene suficiente ancho de banda para satisfacer cualquier demanda.
- ID de enlace: el enlace que transporta el tráfico en cualquier momento.
- Parámetros de Calidad de Servicio, tales como Delay y Jitter.

6.7.3 Acción

La acción para este agente sería elegir entre MPLS e Internet.

6.7.4 Diseño de recompensa

La recompensa es una pieza fundamental del diseño y el rendimiento de los algoritmos de aprendizaje por refuerzo depende en gran medida de la forma en que se diseña la recompensa.

La recompensa debe diseñarse teniendo en cuenta el objetivo del sistema. Aquí, para SD-WAN, el objetivo es maximizar la utilización del ancho de banda de la ruta de Internet, que es una opción más económica.

Estos son algunos de los principios que se tienen en cuenta al diseñar la recompensa:

- El SLA (Service Level Agreement o, en Español, Acuerdo de Calidad de Servicio) debe mantenerse a toda costa, por lo que el ancho de banda actual alcanzado siempre debe exceder el límite prescrito del

SLA. La recompensa debe diseñarse para castigar en gran medida tales lapsos cuando el ancho de banda cae por debajo del límite de SLA.

- El circuito MPLS no es rentable, por lo que la recompensa debería desalentar su uso
- La otra cara de lo anterior es que el circuito de Internet debe utilizarse con más frecuencia.
- Independientemente de la elección que se haga, el objetivo es mantener el flujo de tráfico.
- Los valores de Calidad de Servicio deben mantenerse dentro de ciertos límites.

7 Conclusiones

En este documento se han abordado algunos temas de actualización sobre Redes Convergentes, tales como la Paquetización de la Voz, aspectos de Seguridad en Redes Convergentes, Multicast y Redes SDN, incluyendo el uso de la Inteligencia Artificial en la gestión de estas últimas.

Si bien se ha intentado proveer una serie de conocimientos con un nivel académico acorde, el campo de investigación de estos temas es vastísimo y va actualizándose día a día.

Es el deseo de los autores que la información encontrada en este informe sirva como excusa para brindarles, a quienes se especialicen en esta disciplina, un panorama sólido, integral y actualizado sobre el tema y que logren integrar estos conocimientos más los aprendidos en asignaturas afines de manera que los puedan aplicar en soluciones de ingeniería y diseño de Redes Convergentes.

8 Bibliografía

- Bitglass (2017). Bitglass Report: Black Hat and White Hat Hackers Identify Phishing as the Most Effective Data Exfiltration Method. Recuperado de www.bitglass.com/press-releases/bitglass-report-datagames el 21 de Junio de 2023.
- Chakravarty, A. (2018). Open-AI gym for SD-WAN Link Selection. Recuperado de https://towardsdatascience.com/open-ai-gym-for-sd-wan-link-selection-fe7dac671172 el 21 de Junio de 2023
- Doyle, J. (2017). Routing TCO/IP - Volume II, Second Edition, Cisco Press
- Fortinet (2023). Orquestación de seguridad, automatización y respuesta (SOAR). Recuperado de https://www.fortinet.com/lat/products/fortisoar el 21 de Junio de 2023
- Fortinet (2023). Administración y análisis de seguridad. Recuperado de https://www.fortinet.com/lat/products/management el 21 de Junio de 2023
- García, J. (2019). Redes con Inteligencia Artificial y definidas por software (SDN) para mejorar la experiencia de cliente. Recuperado de https://es.linkedin.com/pulse/redes-con-inteligencia-artificial-y-definidas-por-software-garcia el 21 de Junio de 2023
- Garcia, M. (2017). Easy Ways to Build a Better P@$5w0rd. Recuperado de https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd el 21 de Junio de 2023.

- Gophich (2018). Gophish, la herramienta para entrenar usuarios contra el phising. Recuperado de https://derechodelared.com/gophish/ el 21 de Junio de 2023.
- Grassi, P. A.; Fenton, J. L.; Perlner, R.A.; Regenscheid, A. R.; Burr, W. E.; Richer, J. P. (2017). NIST Special Publication 800-63B - Authentication and Lifecycle Management. Recuperado de https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf el 21 de Junio de 2023.
- IBM (2021). Soluciones de orquestación de seguridad, automatización y respuesta (SOAR). Recuperado de https://www.ibm.com/es-es/security/intelligent-orchestration el 21 de Junio de 2023
- ITU (2003). [106] Estimates of Ie and Bpl parameters for a range of CODEC types. Recuperado de https://www.itu.int/md/T01-SG12-030127-D-0106 el 21 de Junio de 2023
- Jackson, C.; Gooley, J.; Iliesiu, A.; Malegaonkar, A. (2021). Cisco Certified DevNet Associate DEVASC - 200-901 Official Cert Guide, Cisco Press
- Kaspersky Lab (2013). ¿QUÉ ES UN ATAQUE MAN-IN-THEMIDDLE?. Recuperado de https://latam.kaspersky.com/blog/que-esun-ataque-man-in-the-middle/469/ el 21 de Junio de 2023.
- Loveless, J.; Blair, R.; Durai, A. (2016). IP Multicast, Volume I: Cisco IP Multicast Networking, Cisco Press
- Mason, J. (2018) 100+ VPN Logging Policies. Recuperado de www.thebestvpn.com/118-vpns-logging-policy el 21 de Junio de 2023.
- McConnaughy, T. (2020). Introduction to IP Multicast. Cisco Live. Recuperado de

https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKIPM-1261.pdf el 21 de Junio de 2023

- Okta (2018). Businesses @ Work Report. Recuperado de www.okta.com/sites/default/files/Okta-Businesses-at-Work-2018.pdf?1516770633 el 21 de Junio de 2023.

- Prajapati, A; Sakadasariya, A; Patel, J (2018). Software defined network: Future of networking. 2nd International Conference on Inventive Systems and Control (ICISC). 1351-1354. Recuperado de https://ieeexplore.ieee.org/document/8399028 el 21 de Junio de 2023.

- Paloalto Networks (2018). What is an intrusion prevention system?. Recuperado de https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips el 21 de Junio de 2023.

- Sutton, R. S.; Barto, A. G. (2018), Reinforcement learning: An introduction. MIT Press

- Teijeira, P. (2009). La importancia del cifrado de datos para las empresas. Recuperado de https://www.redseguridad.com/especialidades-tic/proteccion-de-datos/la-importancia-del-cifrado-de-datos-para-las-empresas_20141204.html el 21 de Junio de 2023.

- VMWARE (2023). ¿Qué es el ZTNA?. Recuperado de https://www.vmware.com/es/topics/glossary/content/zero-trust-network-access-ztna.html el 21 de Junio de 2023.