Alejandro Corletti Estrada

https://darFe.es

paso a paso

Volumen 1

(Charlas 1 a 50)

PRÓLOGO

Desde sus inicios, la cultura hacker siempre ha estado vinculada con la difusión del conocimiento. Tiene sus raíces en los primeros días de la informática, cuando los programadores y entusiastas de la tecnología se reunían en universidades, laboratorios de investigación y clubes de computación para explorar y experimentar con las nuevas tecnologías emergentes. Los primeros hackers compartían un profundo interés por comprender el funcionamiento interno de los sistemas informáticos y por desafiar los límites establecidos. Algunos de sus grandes referentes, como Richard Stallman o Linus Torvalds fueron los promotores del movimiento de código abierto, del licenciamiento libre (Copyleft) y en general de la democratización de la informática.

Ya nadie duda de que compartir conocimiento es, además de una virtud, un principio fundamental que impulsa el avance y la innovación en el mundo de la ciencia y de la tecnología. En el ámbito de la ciberseguridad, esta filosofía colaborativa se ha convertido en un pilar esencial para abordar los desafíos cada vez más complejos / sofisticados a los que nos enfrentamos en el mundo digital.

Mi amistad con Alejandro Corletti (Ale) se remonta a hace más de dos décadas, cuando ambos coincidimos en la Gerencia de Seguridad de Redes de Telefónica Móviles en Madrid. Recuerdo con cariño nuestras "charlas de café" (o mate en su caso) donde conversábamos acerca del software libre y de la importancia de compartir el conocimiento en beneficio de todos. Ha pasado mucho tiempo desde entonces, pero tanto nuestra amistad, como nuestra pasión por la seguridad informática se mantienen firmes, al igual que nuestras convicciones.

Con su último libro 'Aprendiendo Ciberseguridad Paso a Paso', Alejandro demuestra una vez más de su compromiso con la difusión libre del conocimiento en ciberseguridad (se puede descargar de forma gratuita bajo licencia Copyleft). Se trata de una recopilación de cincuenta charlas divulgativas de ciberseguridad online publicadas a lo largo de los dos últimos años como complemento a su colección de títulos 'Seguridad por Niveles', 'Seguridad en Redes', 'Ciberseguridad, una estrategia Informático/Militar' y 'Manual de Resiliencia'.

Sus libros han sido durante años una referencia indispensable en el campo de la ciberseguridad, especialmente dentro de la comunidad de habla hispana. Han servido de base para la formación de numerosos especialistas y son fuente de inspiración y consulta tanto para profesionales como para estudiantes. Su temática abarca desde conceptos básicos hasta técnicas avanzadas, ofreciendo una visión completa y actualizada de los desafíos y soluciones en este campo en constante evolución.

No me cabe duda de que 'Aprendiendo Ciberseguridad Paso a Paso' será una valiosa adición a la ya extensa bibliografía de Alejandro Corletti y un recurso imprescindible para cualquier interesado en adentrarse en el fascinante mundo de la ciberseguridad informática. Su contribución al desarrollo de este campo es digna de admiración y reconocimiento.

José Ignacio Bravo Vicente
Especialista en Ciberseguridad
Madrid, 2024

Indice

www.darFe.es

Charla 01

Presentación

Enlace al Video:

Resumen:

Se trata del video inicial de este ciclo, en el que presentamos el objetivo de todas estas charlas, el público al que va dirigido, y la metodología que emplearemos en todas ellas.

Descripción detallada

En este ciclo iremos desarrollando, nivel a nivel (paso a paso) una serie de conceptos que son fundamentales a la hora de trabajar en Ciberseguridad. Estamos convencidos que el punto de partida, es una base sólida de conocimientos, para que el día de mañana puedas profundizar en cada medida que adoptes para proteger tus infraestructuras.

Estamos cansados de ver empresas cuya seguridad está sustentada por una serie de personas y herramientas buenas, pero a la hora de sufrir incidentes de ciberseguridad, su capacidad de respuesta es limitada, por falta de base para comprender técnicamente qué es lo que les está sucediendo.

Intentaremos en todo el ciclo, poder llegar a las causas o raíces del problema, por eso avanzaremos "**paso a paso**".

CHARLA 01: Presentación

Aprendiendo Ciberseguridad:
Se trata de una serie de videos que nos prepararán de forma muy (pero muy, muy, muy...) didáctica a enfrentar este importante desafío.

Objetivo de esta serie de videos:
Presentar de forma didáctica y paso a paso, el conjunto de conocimientos, medidas técnicas, herramientas y metodologías necesarias para poder administrar la Ciberseguridad de mi empresa u organización

Público al que va dirigido:
Personas con interés técnico que necesiten desde CERO capacitación en Ciberseguridad.

Metodología de la serie:
Secuencia de charlas, de no más de diez minutos cada una, apoyadas en nuestras publicaciones y videos gratuitos que nos guiarán sobre las bases fundamentales de este tema.

Qué vamos a ver en esta serie de videos:

- Modelo de capas TCP/IP.
- Desarrollo de cada capa (nivel), profundizando en la seguridad de cada protocolo.
- Tecnologías de redes.
- Análisis de tráfico.
- Protocolos seguros e inseguros.
- Comandos más empleados.
- Gestión de Switches, Routers y Firewalls.
- Sistemas de detección de intrusiones.
- Herramientas que podemos emplear.
- Empleo de Linux (*en su distribución: "Kali"*)

Como ya hemos mencionado, **DarFe.es**, es la empresa de habla hispana que mayor cantidad de Know How sobre redes y Ciberseguridad comparte en Internet.

En nuestra Web: **https://darFe.es,** encontrarás todos estos contenidos, a los cuáles hemos de sumarle también la creación de nuestra propia **Ciberwiki**.

Por lo tanto durante todo este ciclo, haremos permanentemente referencia a nuestras principales fuentes de información, las cuáles son.

Referencias:

Nuestros **cuatro libros**.

- Seguridad por Niveles.
- Seguridad en Redes.
- Ciberseguridad, una estrategia Informático/Militar.
- Manual de la Resiliencia.

Descarga gratuita en:

https://darFe.es

Nuestra página **Web**.

www.darFe.es

Nuestra **Plataforma de formación**.

https://moodle.darFe.es

Nuestro canal **Youtube**

https://www.youtube.com/c/empresaDarFe

Nuestra Ciberwiki

www.darFe.es/ciberwiki

Volver al índice

www.darFe.es

Charla 02

El modelo de capas

Enlace al Video:

Resumen:

El modelo de capas, es una de las bases de las Telecomunicaciones, nos permite dividir adecuadamente este gran problema en “Funciones y/o Servicios” que se corresponden específicamente a cada nivel de este modelo, facilitando tratar un tema tan complejo, en varias partes, cada una de ellas centrada específicamente en su tarea.

El detalle de esta charla puedes verlo en nuestro libro gratuito “**Seguridad por Niveles**” en el capítulo 1, que puedes descargar en nuestra Web.

Descripción detallada

Presentación de modelo de capas.

Son varios los protocolos que cooperan para gestionar las comunicaciones, cada uno de ellos cubre una o varias capas del modelo **OSI** (Open System interconnection), la realidad, es que para establecer la comunicación entre dos **Equipos Terminales de Datos** (ETD) se emplea más de un protocolo, es por esta razón que se suele hablar no de protocolos aislados, sino que al hacer mención de alguno de ellos, se sobre entiende que se está hablando de una PILA de protocolos, la cual abarca más de un nivel OSI, son ejemplo de ello X.25, TCP/IP, IPX/SPX, ISDN, etc.

Una forma de agruparlos es, como se encuentran cotidianamente los siete niveles del modelo OSI, en tres grupos que tienen cierta semejanza en sus funciones y/o servicios:

OSI	Generalizado
Aplicación	APLICACION
Presentación	
Sesión	
Transporte	TRANSPORTE
Red	RED
Enlace	
Físico	

La **ISO** (International Standard Organization), estableció hace 30 años este modelo OSI que hoy lleva la denominación **ISO 7498** o más conocida como **X.200** de **ITU** (International Telecommunication Union).

Modelo OSI y DARPA (TCP/IP)

El modelo OSI es, sin lugar a dudas el estándar mundial por excelencia, pero como todo esquema tan amplio presenta una gran desventaja, el enorme aparato burocrático que lo sustenta. Toda determinación, protocolo, definición o referencia que este proponga debe pasar por una serie de pasos, en algunos casos reuniendo personal de muchos países, que demoran excesivo tiempo para la alta exigencia que hoy impone Internet. Hoy al aparecer un nuevo dispositivo, protocolo, servicio, facilidad, etc. en Internet, el mercado si es útil, automáticamente lo demanda, como ejemplo de esto hay miles de casos (chat, IRC, SMS, Whatsapp, etc.). Si para estandarizar cualquiera de estos se tardara más de lo necesario, los fabricantes, se verían en la obligación de ofrecer sus productos al mercado, arriesgando que luego los estándares se ajusten a ello, o en caso contrario, los clientes finales sufrirían el haber adquirido productos que luego son

incompatibles con otros. Hoy, no se puede dar el lujo de demorar en una red cuyas exigencias son cada vez más aceleradas e imprevisibles.

Para dar respuesta a esta nueva REVOLUCION TECNOLOGICA (Internet), aparecen una serie de recomendaciones ágiles, con diferentes estados de madurez, que inicialmente no son un estándar, pero rápidamente ofrecen una guía o recomendación de cómo se cree que es la forma más conveniente (según un pequeño grupo de especialistas) de llevar a cabo cualquier novedad de la red.

Se trata aquí de las **RFC** (Request For Commentaries), que proponen una mecánica veloz para que el usuario final no sufra de los inconvenientes anteriormente planteados, dando respuesta a las necesidades del mercado eficientemente.

Se produce aquí un punto de inflexión importante entre el estándar mundial y lo que se va proponiendo poco a poco a través de estas RFC, las cuales en muchos casos hacen referencia al modelo OSI y en muchos otros no, apareciendo un nuevo modelo de referencia que no ajusta exactamente con lo propuesto por OSI. Este modelo se lo conoce como pila, stack, o familia **TCP/IP** o también como modelo **DARPA** por la Agencia de Investigación de proyectos avanzados del **DoD** (Departamento de Defensa) de EEUU, que es quien inicialmente promueve este proyecto.

Este modelo que trata de simplificar el trabajo de las capas, y por no ser un estándar, se ve reflejado en la interpretación de los distintos autores como un modelo de cuatro o cinco capas, es más, existen filosóficos debates acerca de cómo debe ser interpretado.

En todo este texto, se va a tratar el mismo como un modelo de cinco capas, solamente por una cuestión práctica de cómo ajustan las mismas a los cuatro primeros niveles del modelo OSI, tratando de no entrar en la discusión Bizantina del mismo, y dejando en libertad al lector de formar su libre opinión sobre el mejor planteo que encuentre.

Si se representan ambos modelos, sin entrar en detalles de si las distintas capas coinciden exactamente o no (pues este es otro gran tema de discusión, que no será tratado en este texto), se pueden presentar más o menos como se presenta a continuación:

<table>
<tr><th>OSI</th><th>DARPA o TCP/IP</th></tr>
<tr><td>Aplicación</td><td rowspan="3">Aplicación</td></tr>
<tr><td>Presentación</td></tr>
<tr><td>Sesión</td></tr>
<tr><td>Transporte</td><td>Transporte</td></tr>
<tr><td>Red</td><td>Red</td></tr>
<tr><td>Enlace</td><td>Acceso al medio</td></tr>
<tr><td>Físico</td><td>Físico</td></tr>
</table>

Antes de continuar avanzando sobre el concepto de capas vamos a presentar una idea que sería fundamental no olvidarla y mantener siempre presente. Cada capa regula, o es encargada de una serie de funciones que deberían ser “autónomas” (cosa que a veces no se cumple), es decir no tendría por qué depender de lo que se haga en otro nivel. Dentro de este conjunto de tareas, es necesario destacar la razón de ser de cada una de ellas, su objetivo principal, el cual lo podríamos resumir en el cuadro siguiente:

Aplicación	Usuario	Desde aquí hacia arriba mira hacia el usuario
Transporte	Es el primer nivel que ve la conexión "de Extremo a Extremo"	Desde aquí hacia abajo mira hacia la Red
Red	Rutas	
Enlace	Nodo inmediatamente Adyacente	
Físico	Aspectos Mecánicos, físicos y eléctricos (u ópticos)	

Sobre el cuadro anterior insistiremos durante todo el texto, pues será la base del entendimiento de cada uno de los protocolos que abordemos, por ahora tenlo presente!

Si quieres profundizar más sobre los niveles o capas, consulta el capítulo 1 del libro "**Seguridad por Niveles**".

Volver al índice

www.darFe.es

Charla 03

Servicios y/o funciones

Enlace al Video: 

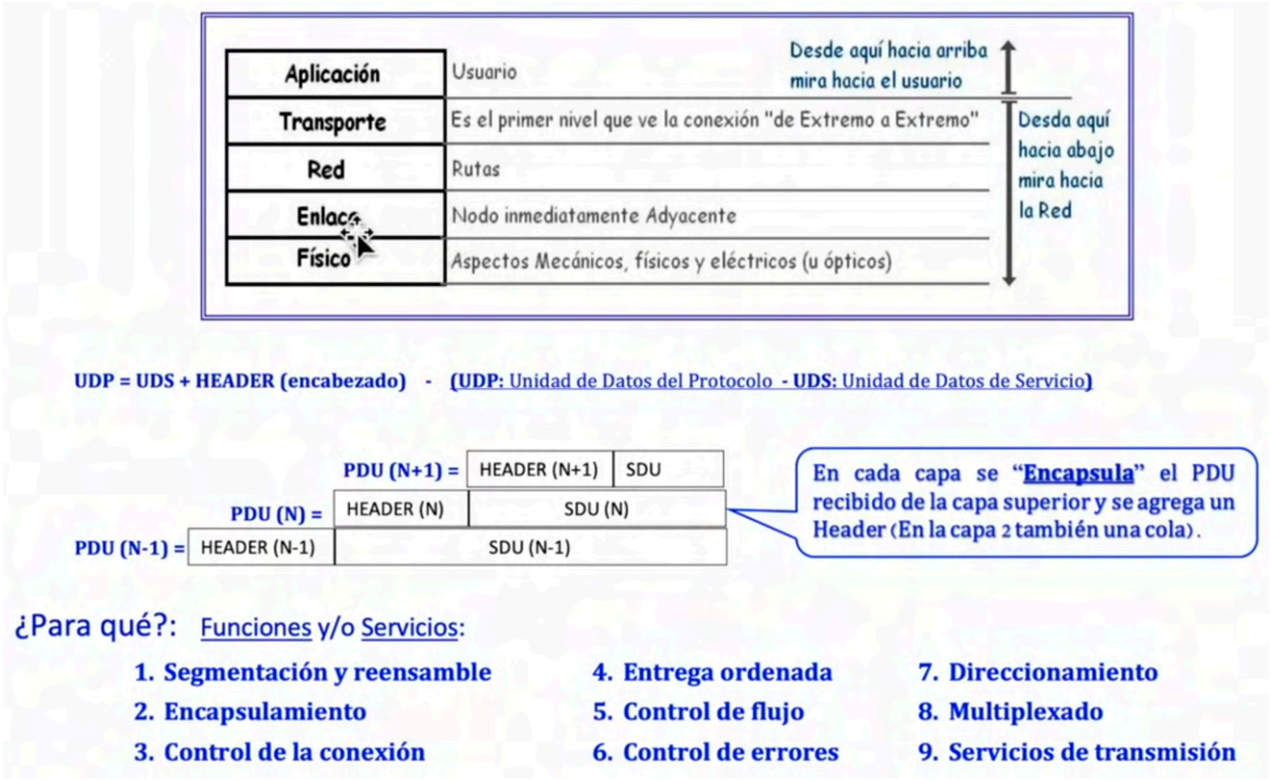
Resumen:

En esta charla comenzaremos a trabajar con la herramienta "**Wireshark**" (https://www.wireshark.org), pues justamente nos permite capturar y desarmar cada uno de los bits que circulan por nuestras redes y analizarlos en detalle. Las funciones y/o servicios que cumple cada nivel del modelo de capas, las veremos de forma práctica por medio de esta herramienta.

Descripción detallada

En el modelo de capas que presentamos la charla anterior, operan cada uno de los protocolos de esa capa concreta. Como se puede ver en la imagen de abajo, en realidad lo que "hace, o deja de hacer" cada protocolo, está definido en su **encabezado** (Header), por eso es muy importante poder visualizarlo de forma real y práctica con

En la imagen de abajo, se presenta como cada uno de ellos baja "**encapsulado**" al nivel inferior, el cual lo recibe como si fuera una caja negra, no debería analizar o ver qué es lo que se hace en cada encabezado de los niveles superiores. Es decir, cada nivel opera con su propio encabezado, y lo entrega al nivel inferior de forma "encapsulada".



El desarrollo de cada una de estas nueve funciones o servicios, podéis seguir estudiándolo en detalle en el capítulo 1 del libro "**Seguridad por Niveles**".

Para aprender el empleo de **Wireshark**, recomendamos el ciclo de "**Análisis de tráfico**" de nuestro canal Youtube:

Volver al índice

www.darFe.es

Charla 04

Señales

Enlace al Video:

Resumen:

En esta charla, desarrollamos el tema “**Señales**” pues es el punto de partida para la transmisión de información. El concepto de “**Modulación**” es lo que nos permite poder transmitir información en todo el mundo.

Desde el punto de vista de Ciberseguridad, las señales son, tal vez, lo más importante del “nivel Físico”, y a lo largo del ciclo veremos la cantidad de vulnerabilidades y ataques que se generan a través de ellas.

Descripción detallada

Para desarrollar y comprender en detalle esta charla, recomendamos que os descarguéis los siguientes ficheros desde:

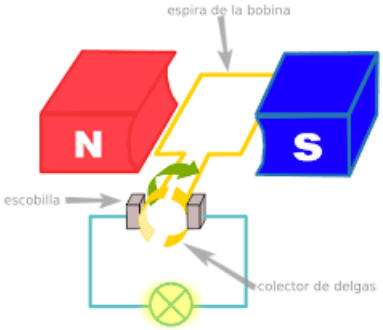
https://darfe.es —> DESCARGAS —> Artículos :

- Modulación.pdf
- Medios de Comunicaciones.pdf
- Técnicas de transmisión de la información.pdf

Estos tres artículos os serán de mucha utilidad para avanzar en detalle sobre esta charla de hoy.

Primero, definamos con sencillez la idea de Señal, como: **todo conjunto de información que nos permite comprender algo**.

Desde el punto de vista de telecomunicaciones, en la vida real del siglo XXI, nos centraremos en las "Señales electromagnéticas y ópticas", que son las que hoy en día se emplean para la transmisión de información.



Comenzando con la señal electromagnética, esta se genera por medio del concepto de "espira", que no es más, ni menos, que un alambre que gira entre dos imanes o campos magnéticos, cada uno de estos giros, producirá un ciclo de señal electromagnética.

Toda señal debe desplazarse por un "**medio**" de comunicaciones, que es el tema que desarrollaremos en las próximas charlas.

Las señales electromagnéticas para que puedan transportar información deben ser "**moduladas**" debidamente.

La técnica de modulación es la combinación de dos señales:

- Portadora
- Moduladora

Se denomina modulación a la operación mediante la cual ciertas características de una onda, denominada portadora, se modifican en función de otra denominada moduladora, que contiene la información a transmitir. La señal resultante se denominará modulada.

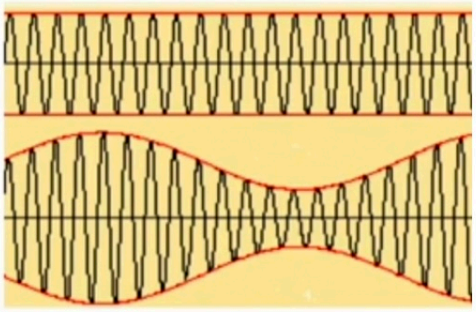
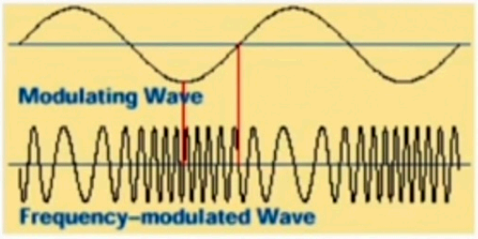
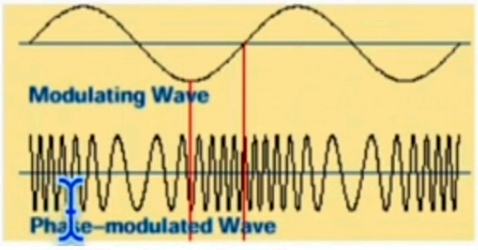
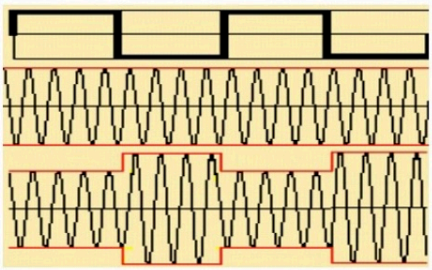
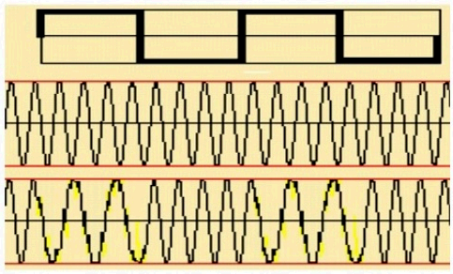
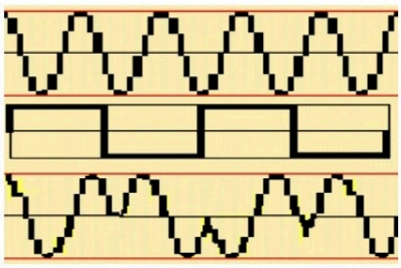
El resultado de esta combinación es sencillamente la sumatoria de ambas, que se denomina "**señal modulada**", y será la que se envía al medio de comunicaciones. En el otro extremo, el receptor ejecuta el proceso inverso para obtener nuevamente la "**señal moduladora"** que es la que contiene la información propiamente dicha.

Como iremos desarrollando más adelante, las señales pueden ser:

- Analógicas
- Digitales

Una señal es "**Analógica**" cuando entre dos puntos de la misma (con independencia de la mínima distancia que pueda haber entre ellos) existen infinitos puntos.

Una señal es "**Digital**" cuando entre dos puntos de la misma (con independencia de la mínima distancia que pueda haber entre ellos) existen acotados puntos.

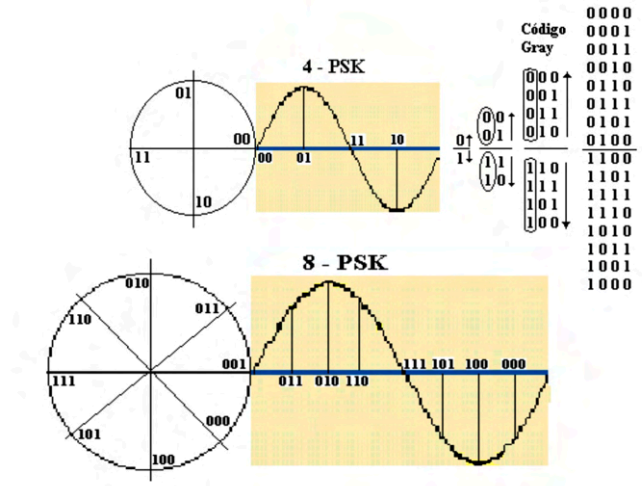
Modulación analógica	Modulación digital
a. Amplitud:  b. Frecuencia:  c. Fase:  	a. Amplitud (ASK: Amplitud Shift Key):  b. Frecuencia (FSK: Frecuency Shift Key)::  c. Fase (PSK: Phase Shift Key): 

A continuación presentamos los principios básicos de modulación, tanto analógica, como digital.

Si deseamos más detalle sobre todas las combinaciones de modulación, en el cuadro que sigue se presentan todas ellas. El detalle y explicación e cada una, podéis verlo en el apunte que mencionamos al principio "**Modulación.pdf"**.

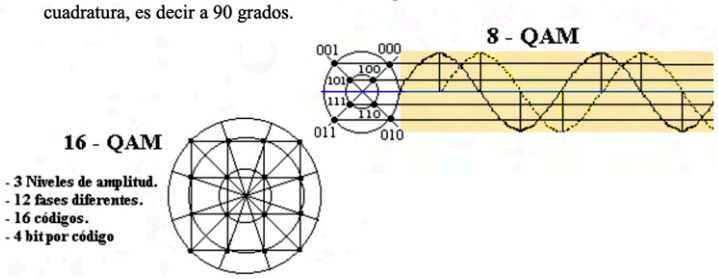
	PARAMETRO VARIABLE DE LA PORTADORA	SEÑAL MODULADORA	
		ANALOGICA	DIGITAL
PORTADORA ANALOGICA (SINUSOIDAL O COSINUSOIDAL)	AMPLITUD	AM	ASK
	FRECUENCIA	FM	FSK
	FASE	PM	PSK
	COMBINACIÓN FASE/AMPLITUD		CUADRATURA
PORTADORA DIGITAL	AMPLITUD	PAM /MIA	*Casos particulares*
	POSICION	PPM	
	DURACION	PDM/PWM	
PORTADORA DIGITAL MODULACION POR CODIGO		PCM / MIC	
PORTADORA DIGITAL MODULACION POR INCREMENTOS		DELTA y DELTA ADAPTATIVA	

A su vez, el cuadro anterior, también da lugar a diferentes combinaciones entre ellas, dando origen a las vertiginosas velocidades de modulación actuales, de las cuales a la derecha se presenta un breve esquema de la técnica **QAM**.



d. QAM (Quadrature Amplitud Modulation):

Este método se basa en modular en amplitud distintas señales desfasadas en cuadratura, es decir a 90 grados.



Volver al índice

www.darFe.es

Charla 05

Espectro

Enlace al Video: 

Resumen:

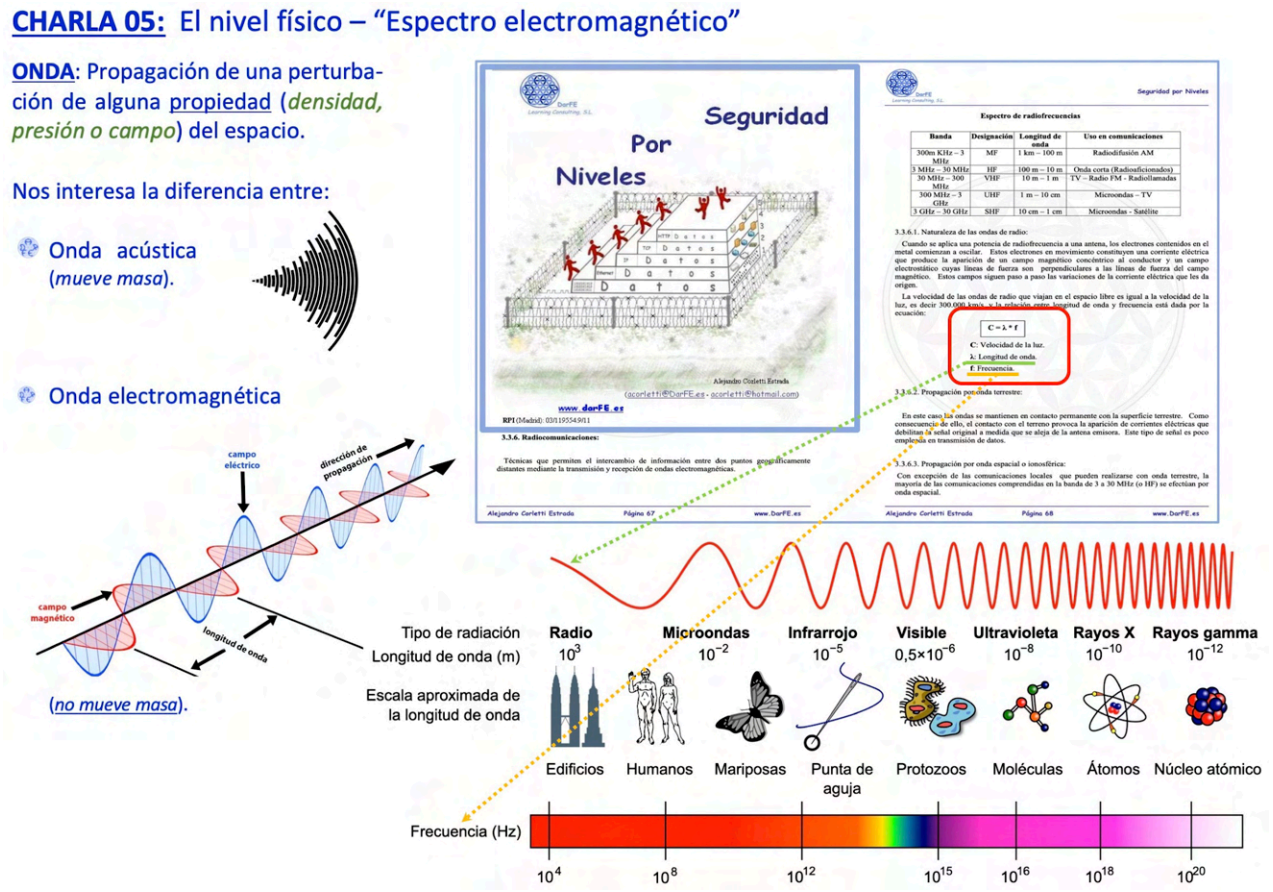
Seguimos avanzando en el concepto de "**Señales**" que vimos en la charla anterior, diferenciando la idea de "**Onda acústica**" y "**Onda electromagnética**". Presentamos los conceptos de Frecuencia y Longitud de onda, que veremos guardan una estrecha relación.

En todos los países está regulado el empleo de las frecuencias, sino nuestro "**Ether**" sería un verdadero caos. Desarrollaremos cómo se regula este espectro.

Descripción detallada

Como se puede ver en las imágenes que se presentan a continuación, para comprender el tema de hoy, es necesario, en primer lugar desarrollar el concepto de "**Onda**". Luego diferenciar bien entre onda acústica y electromagnética.

Estos conceptos, nos permiten entrar en la idea de "**espectro electromagnético**", que no es otra cosa que el conjunto de estas señales que se propagan a través de cualquier medio.



Cada país regula su propio uso del espectro, basado en las directivas internacionales establecidas por **ITU** (International Telecommunication Union). Este referente internacional, justamente sirve para facilitar comunicaciones que no dependen de un país en concreto (aviación, navegación, satélites, radioaficionados, etc.), como también para evitar solapamientos en zonas fronterizas.

Si analizamos la situación del espectro en España, proponemos tomar como punto de partida el **Real Decreto 123/2017**, de 24 de febrero, por el que se aprueba el Reglamento sobre el uso del dominio público radioeléctrico.

Lo podemos descargar en: https://www.boe.es/buscar/act.php?id=BOE-A-2017-2460

Nos centraremos solo en algunos puntos del mismo para comprender su funcionamiento y lógica.

Artículo 3. Concepto de dominio público radioeléctrico.

A los efectos del presente reglamento, se considera dominio público radioeléctrico el espacio por el que pueden propagarse las ondas radioeléctricas. Se entiende por

espectro radioeléctrico las ondas electromagnéticas cuya frecuencia se fija convencionalmente por debajo de 3.000 gigahertzios que se propagan por el espacio sin guía artificial.

La utilización de ondas electromagnéticas en frecuencias superiores a 3.000 gigahertzios y propagadas por el espacio sin guía artificial se somete al mismo régimen que la utilización de las ondas radioeléctricas, siendo de aplicación lo dispuesto en la Ley General de Telecomunicaciones y en el presente reglamento.

El término frecuencia utilizado en el presente reglamento debe entenderse referido tanto a un valor concreto como a la identificación de la porción de espectro necesario para efectuar una determinada comunicación radioeléctrica (ancho de banda en un canal radioeléctrico).

Otro documento base del espectro Español es la **Orden ETD/1449/2021**, de 16 de diciembre, por la que se aprueba el **Cuadro Nacional de Atribución de Frecuencias** (CNAF).

Lo podemos descargar en: https://www.boe.es/buscar/doc.php?id=BOE-A-2021-21346

Nos centraremos en su ANEXO

Cuadro Nacional de Atribución de Frecuencias (CNAF)

El cuadro que se inserta a continuación comprende en primer lugar las notas del Artículo 5 del Reglamento de Radiocomunicaciones (**RR**) que complementa la Constitución y el Convenio de la Unión Internacional de Telecomunicaciones (**UIT**), seguidas de las tablas de atribución de bandas de frecuencias según dicho artículo, esta atribución se indica para las tres regiones en las que la UIT ha dividido el mundo a efectos de atribución de bandas de frecuencias según la nota 5.2 del RR.

A estos fines se han empleado los códigos siguientes para clasificar las modalidades de uso:

C: Uso común

E: Uso especial.

P: Uso privativo.

R: Uso reservado al Estado.

M: Uso mixto que comprende los usos P y R.

Artículo 5 del Reglamento de Radiocomunicaciones

Atribuciones de frecuencia

Introducción

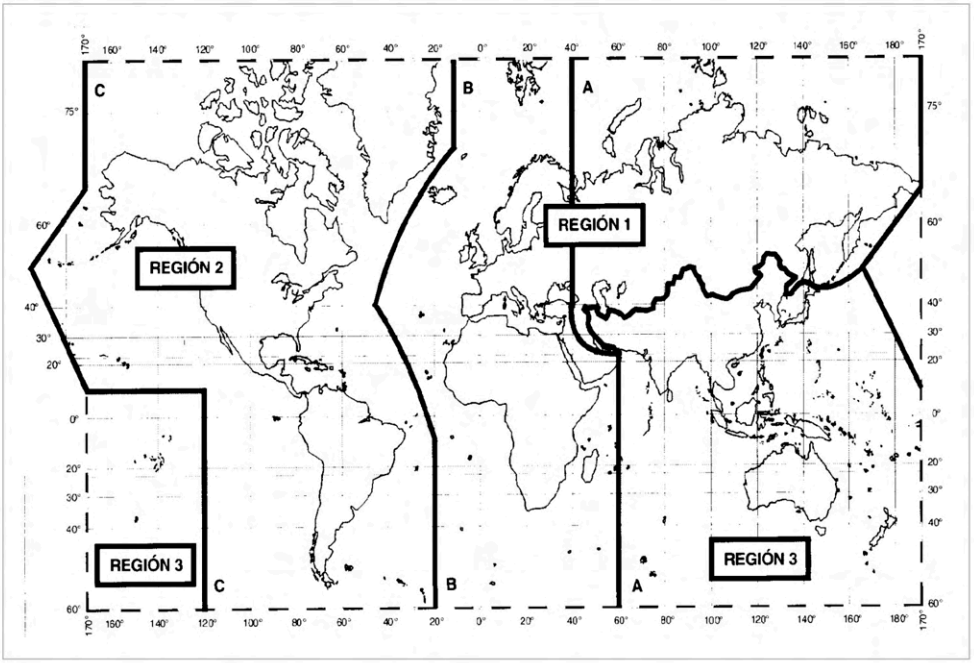
Sección I. Regiones y Zonas

5.2 Desde el punto de vista de la atribución de las bandas de frecuencias, se ha dividido el mundo en tres Regiones indicadas en el siguiente mapa y descritas en los números 5.3 a 5.9:

Luego pasa a definir de forma detallada cada una de las frecuencias. A continuación, solo presentaremos la de inicio y fin de estos cuadros.

Sección I. Regiones y Zonas

5.2 Desde el punto de vista de la atribución de las bandas de frecuencias, se ha dividido el mundo en tres Regiones indicadas en el siguiente mapa y descritas en los números 5.3 a 5.9:



Y finalmente describe las Notas de utilización Nacional (**UN**) que, en el caso de España, van de la UN-0 a la UN-168

ATRIBUCIÓN A LOS SERVICIOS según el RR de la UIT		
8,3 - 110 kHz		
Región 1	**Región 2**	**Región 3**
70 - 72 RADIONAVEGA-CIÓN 5.60	**70 - 90** FIJO MÓVIL MARÍTIMO 5.57 RADIONAVEGACIÓN MARÍTIMA 5.60 Radiolocalización	**70 - 72** RADIONAVEGACIÓN 5.60 Fijo Móvil marítimo 5.57 5.59
72 - 84 FIJO MÓVIL MARÍTIMO 5.57 RADIONAVEGA-CIÓN 5.60 5.56		**72 - 84** FIJO MÓVIL MARÍTIMO 5.57 RADIONAVEGACIÓN 5.60
84 - 86 RADIONAVEGA-CIÓN 5.60		**84 - 86** RADIONAVEGACIÓN 5.60 Fijo Móvil marítimo 5.57 5.59
86 - 90 FIJO MÓVIL MARÍTIMO 5.57 RADIONAVEGA-CIÓN 5.56	5.61	**86 - 90** FIJO MÓVIL MARÍTIMO 5.57 RADIONAVEGACIÓN 5.60
90 - 110	RADIONAVEGACIÓN 5.62 Fijo 5.64	

ATRIBUCIÓN NACIONAL	USOS	OBSERVACIONES
8,3 - 110 kHz		
70 - 72 RADIONAVEGACIÓN	R	5.60 UN-114, UN-117
72 - 84 FIJO MÓVIL MARÍTIMO RADIONAVEGACIÓN	M M R	5.56 5.57 5.60 UN-114, UN-117
84 - 86 RADIONAVEGACIÓN	R	5.60 UN-114, UN-117
86 - 90 FIJO MÓVIL MARÍTIMO RADIONAVEGACIÓN	M M R	5.56 5.57 UN-114, UN-117
90 - 110 RADIONAVEGACIÓN Fijo	R M	5.62 5.64 UN-114, UN-117

ATRIBUCIÓN A LOS SERVICIOS según el RR de la UIT		
248 - 3000 GHz		
Región 1	Región 2	Región 3
248 - 250 AFICIONADOS AFICIONADOS POR SATÉLITE Radioastronomía 5.149		
250 - 252 EXPLORACIÓN DE LA TIERRA POR SATÉLITE (pasivo) RADIOASTRONOMÍA INVESTIGACIÓN ESPACIAL (pasivo) 5.340 5.563A		
252 - 265 FIJO MÓVIL MÓVIL POR SATÉLITE (Tierra-espacio) RADIOASTRONOMÍA RADIONAVEGACIÓN RADIONAVEGACIÓN POR SATÉLITE 5.149 5.554		
265 - 275 FIJO FIJO POR SATÉLITE (Tierra-espacio) MÓVIL RADIOASTRONOMÍA 5.149 5.563A		
275 - 3000 (No atribuida) 5.564A 5.565		

ATRIBUCIÓN NACIONAL	USOS	OBSERVACIONES
248 - 3000 GHz		
248 - 250 AFICIONADOS AFICIONADOS POR SATÉLITE Radioastronomía	E E P	5.149
250 - 252 EXPLORACIÓN DE LA TIERRA POR SATÉLITE (pasivo) RADIOASTRONOMÍA INVESTIGACIÓN ESPACIAL (pasivo)	M P M	5.340 5.563A
252 - 265 FIJO MÓVIL MÓVIL POR SATÉLITE (Tierra-espacio) RADIOASTRONOMÍA RADIONAVEGACIÓN RADIONAVEGACIÓN POR SATÉLITE	P P P P R R	5.149 5.554
265 - 275 FIJO FIJO POR SATÉLITE (Tierra-espacio) MÓVIL RADIOASTRONOMÍA	P P P P	5.149 5.563A
275 - 3000 (No atribuida)		5.564A 5.565

CNAF 2021

Notas de utilización Nacional (**UN**)

UN-0 Usos del Estado por debajo de 27 MHz.

Las bandas que se citan a continuación se destinan a uso preferente del Ministerio de Defensa.

14-19,95 kHz 5.730-5.900 kHz

20,05-70 kHz 9.040-9.400 kHz

126-130 kHz 9.900-9.995 kHz

140-148,5 kHz 12.100-12.230 kHz

283,5-315 kHz 15.800-16.360 kHz

2.300-2.498 kHz 24.000-24.890 kHz

Continúa.....

...

.

UN-168 Límites de cantidad de espectro en bandas armonizadas a nivel europeo.

Hemos presentado este BOE de 2021, pues es el más detallado de los años recientes, pero el mismo tiene su actualización en el año 2023, que solo trata los aspectos que se modifican. Esta actualización es: **Orden ETD/625/2023**, de 12 de junio, por la que se modifica la Orden ETD/1449/2021, de 16 de diciembre, por la que se aprueba el Cuadro Nacional de Atribución de Frecuencias.

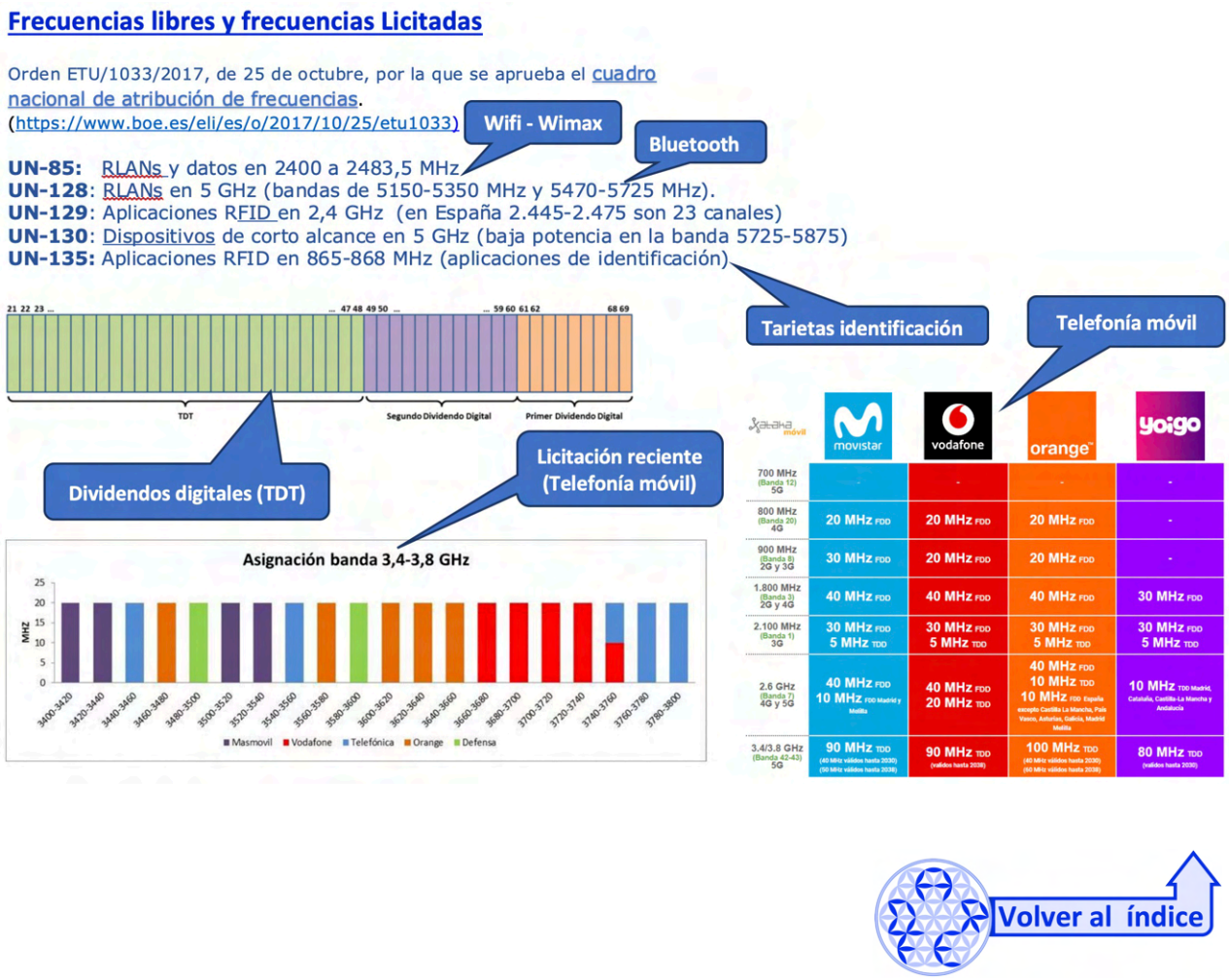
La podemos descargar en:

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2023-14422

Tienes bastante más detalle en **Wikipedia**, buscando: Cuadro Nacional de Atribución de Frecuencias (España).

Un buen ejemplo reciente, sobre regulaciones del espectro lo podemos encontrar en el "**Dividendo digital**". Este llamado "dividendo", justamente se debe a que al digitalizarse la televisión: **TDT** (Televisión Digital Terrestre), en el ancho de banda donde anteriormente la televisión analógica transmitía un canal de televisión, ahora la TDT puede meter seis de ellos, con lo que el espectro de TDT desperdiciaba mucho ancho de banda. Debido a este fenómeno, es que en España, se "dividió" el espectro de Televisión, cediendo dos bandas a la **telefonía móvil**: la banda de 800MHz y posteriormente la de 700MHz, las cuáles se licitaron hace muy pocos años.

En la imagen de abajo puede apreciarse esta situación.



Volver al índice

www.darFe.es

Charla 06

Digitalización

Enlace al Video:

Resumen:

En este video, se describen las señales analógicas y luego cómo se realiza la "**digitalización**" de las mismas.

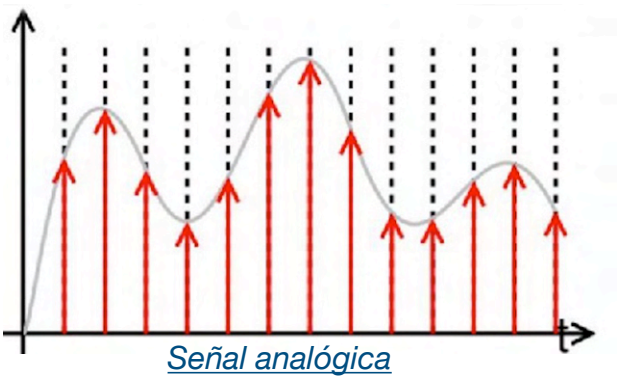
Una vez comprendida la metodología de digitalización, seguimos avanzando en los conceptos de ruido y distorsión, que son la clave por la que hoy en día nos encontramos en un mundo totalmente digital.

Por último se presenta, nuevamente, el empleo de **Wireshark**, para comprender la voz digitalizada.

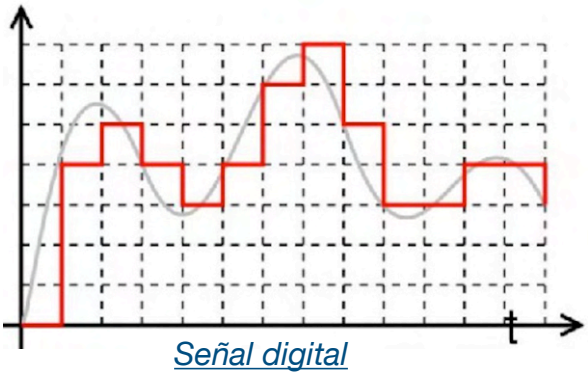
Descripción detallada

Basado en las técnicas de **modulación** (que vimos en la charla 04), es que nace el concepto de "**transmisión**" y de esta forma, pudimos comenzar a enviar información de un sitio a otro.

Inicialmente, nace con señales analógicas por ser la clara representación de las ondas acústicas o, por ejemplo, las generadas por la vibración de una cuerda. Pero, como veremos a continuación, en el siglo XX se descubre la forma de poder transformarlas en digitales (y viceversa).



Señal analógica

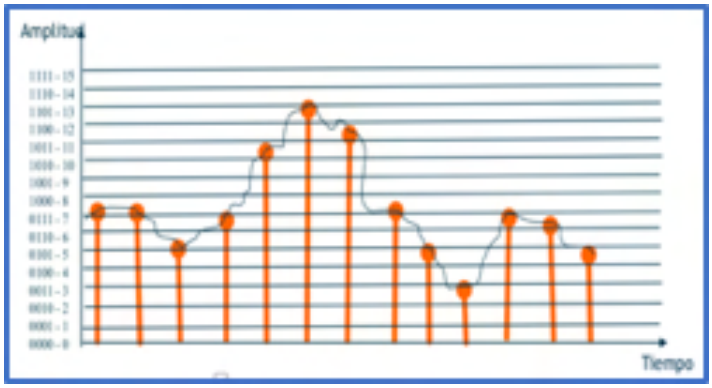


Señal digital

En el mencionado siglo se descubre que es posible convertirlas en un formato digital, es decir "digitalizarlas" por medio de tres pasos:

- **Muestreo**
- **Cuantificación**
- **Codificación**

El muestreo, es tomar "fotos" en puntos concretos de la señal.



El teorema del muestreo (o **Ley de Niquist**) y los tres pasos de la digitalización (*Muestreo – Cuantificación – Codificación*) permiten convertir cualquier señal analógica a digital y viceversa.

Esta **Ley de Niquist**, indica que: tomando muestras de dos veces el ancho de banda de una señal, la misma puede digitalizarse sin perder absolutamente nada de información.

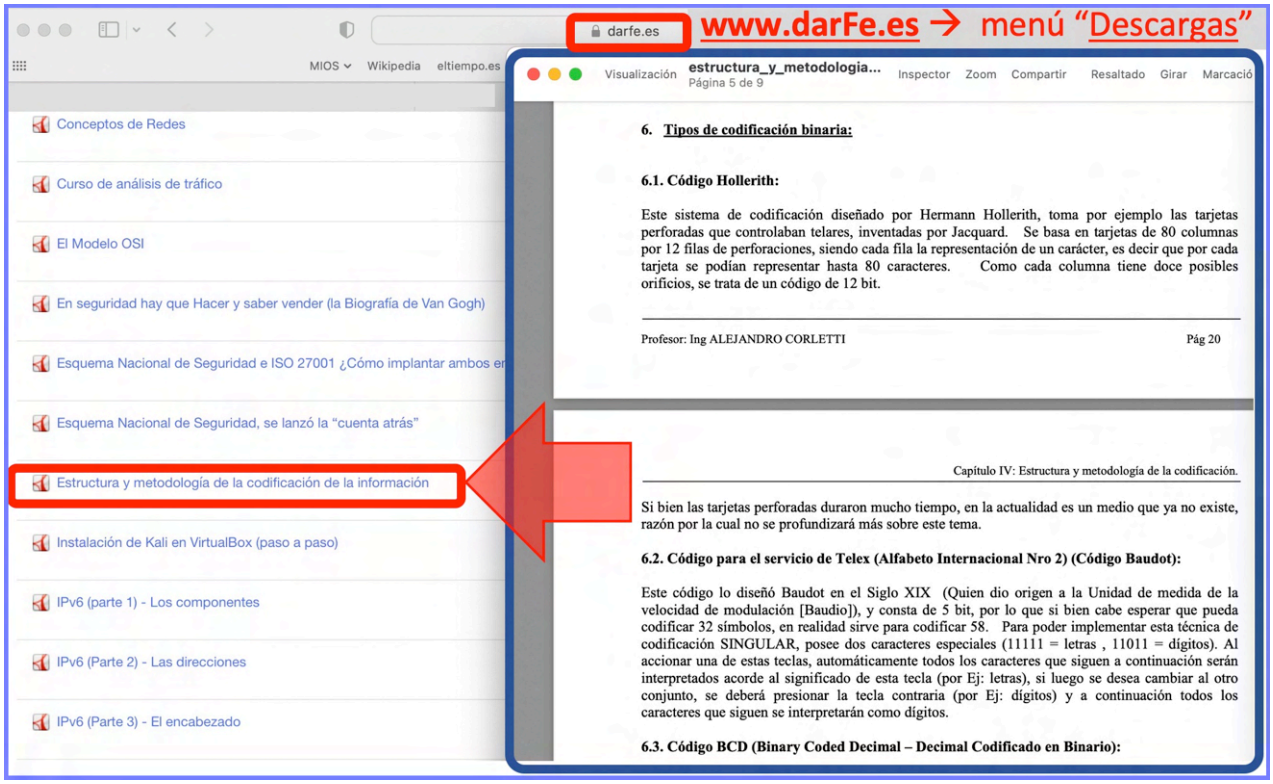
La cuantificación, es la cantidad de bits que se emplean para representar cada punto capturado. Tengamos en cuenta que cuanto mayor cantidad de bits se empleen, mayor será la definición. Siempre ponemos como ejemplo, los primeros monitores que tenían una resolución de 16 colores (opciones), es decir la cuantificación de cada punto

del color era con 4 bits, así se pasaba del amarillo al naranja, de allí al rojo, al violeta, al azul, etc. Hoy en día los monitores de 4k, cuantifican con 12 bits, es decir con 4096 opciones de color, por lo que su definición es abismalmente mayor a los primeros de 4 bits.

Cabe mencionar que en este paso sí se pierde información. Cuanta mayor cantidad de bits empleemos, menor información se perderá.

Por último la codificación es el "código" que se empleará para representar esa señal. Existen innumerables tipos de códigos, desde el conocido código morse, pasando por el ASCII que comúnmente se emplea en informática, hasta códigos más complejos que ofrecen alta capacidad para la compresión, criptografía, etc. como pueden ser los códigos: Diferencial, Manchester, Miller, HDB-3, etc.

Para profundizar en este tema, recomendamos descargar de nuestra Web, el artículo "**estructura_y_metodologia_de_la_codificacion_de_informacion.pdf"**, a continuación puedes ver una imagen de cómo descargarlo.

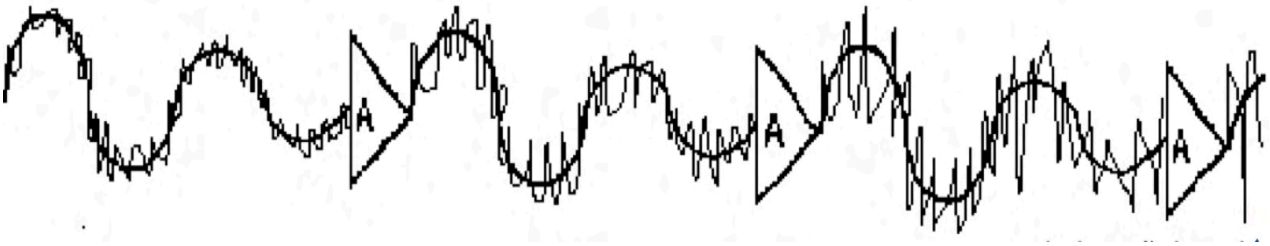


Toda señal electromagnética que se desplace a través de un medio, será afectada por **ruido** y **distorsión**. Estos factores causan fundamentalmente, la atenuación y la deformación. Este fenómeno impacta de manera muy diferente la señal analógica y la digital.

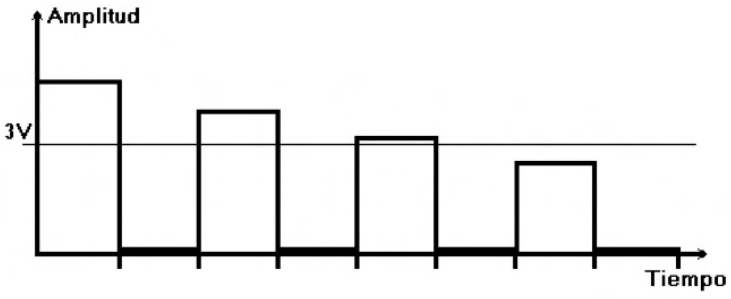
Si se la toma a una distancia tal (Ej: distancia Z) que pueda interpretarse la

información que transporta, se puede colocar un dispositivo llamado **AMPLIFICADOR** cuya tarea consiste en llevar la señal a una potencia mayor, de forma tal que pueda ser nuevamente insertada en el canal de comunicaciones y recorrer una nueva distancia.

Como se mencionó en el primer párrafo, esta señal que se desplaza sufrirá de atenuación, es decir pérdida de la potencia de la señal (como puede apreciarse en los gráficos), por esta causa se implementan los amplificadores, y a su vez también se irá deformando por las distintas interferencias que reciba, sumando **RUIDO**. Estas interferencias se irán sumando o acoplando inexorablemente a la señal que interesa transmitir.



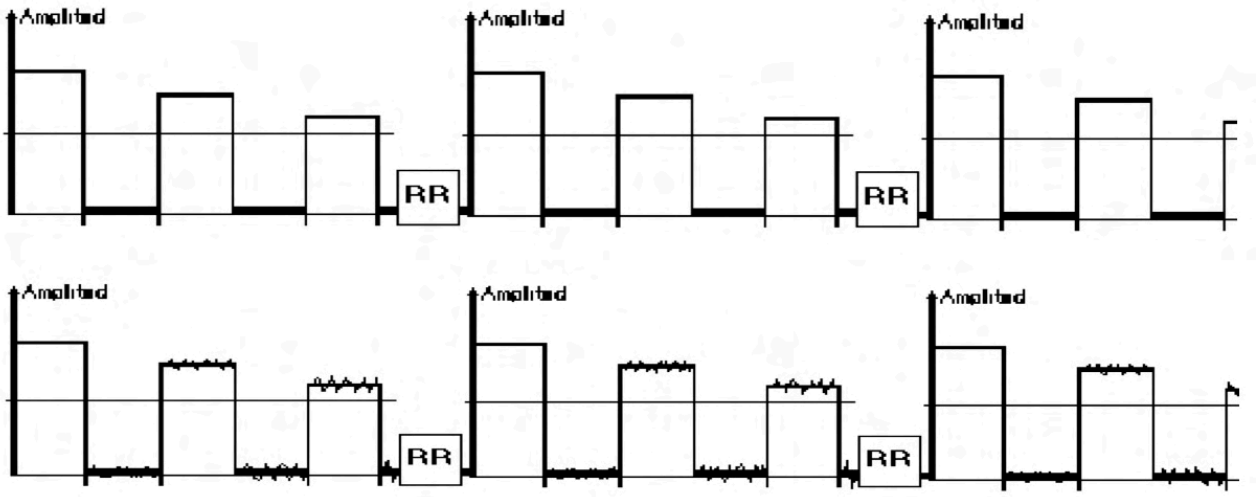
Cuando la señal analógica se **amplifica:** **El ruido TAMBIÉN.**



En el caso de la transmisión digital, este fenómeno es totalmente diferente.

El concepto ya mencionado de este tipo de señal, es que para emitir una transmisión digital, se generará o no un determinado nivel de tensión, el cual si supera el umbral de detección se interpretará como un uno, y al no superarlo se lo interpretará como un cero (o viceversa). (Cabe aclarar que en este ejemplo se está representando una transmisión digital que posee sólo dos niveles, pues se verá después que puede tener más).

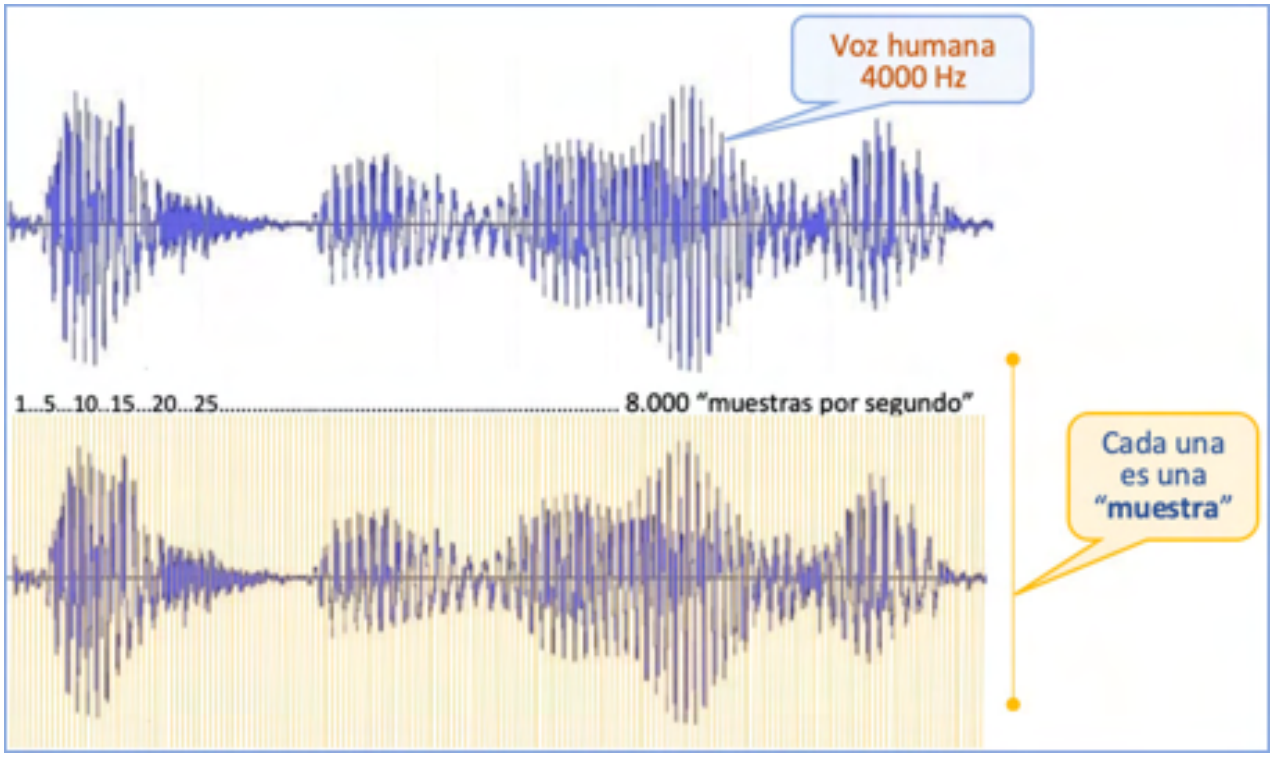
Esta señal al igual que la analógica si alcanza una distancia tal que no supera el umbral de detección, no podrá realizarse ninguna operación, pero si se la toma en distancia adecuada, se podrá colocar un dispositivo llamado REPETIDOR REGENERATIVO cuya función es generar un estado de tensión mayor que el recibido en el caso de superar el umbral de detección, como se grafica a continuación.



La señal digital se **REGENERA** (no se AMPLIFICA) **el ruido NO**

Hoy el mundo es DIGITAL

El oido humano tiene un rango de audición que oscila entre los 200Hz y los 20.000Hz (o 20 KHz), es decir desde una frecuencia muy grave de 300Hz, hasta los máximos agudos audibles de 20KHz, los cuáles por supuesto, dependen de la edad, la capacidad auditiva, etc. Dentro de este rango, la voz humana normal está en los primeros 4.000Hz. Por lo que si aplicamos la Ley de Niquist, tomando 8.000 muestras por segundo, estaríamos cumpliendo con la misma.

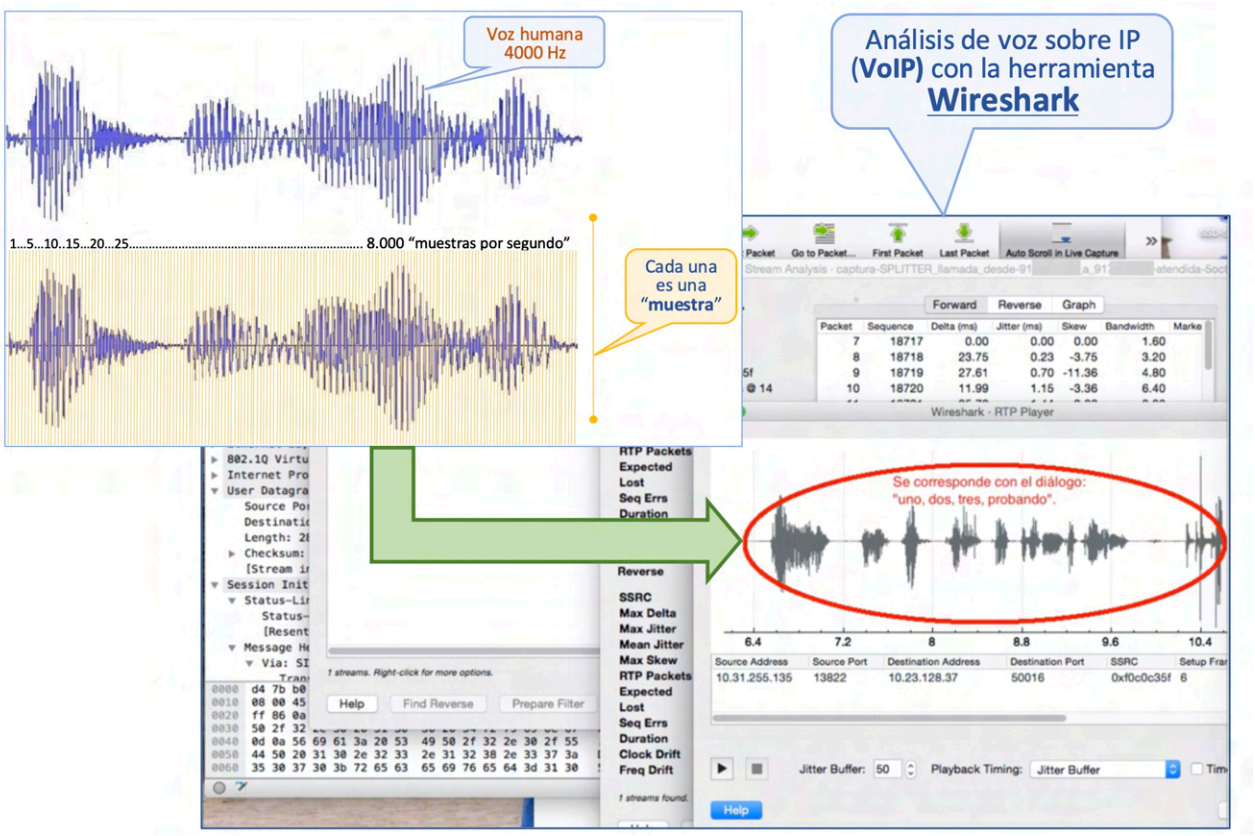


Este es el primer paso en la digitalización de voz en los sistemas telefónicos mundiales. Luego, se los cuantifica con 7 bits en EEUU y Japón, y con 8 bits prácticamente en el

resto del mundo. Si tomamos esta cuantificación de 8 bits, por 8.000 muestras por segundo, tenemos una voz digitalizada de 64.000 bits por segundo (o 64Kbps)

Este canal de 64Kbps, es lo que se denomina "**canal de telefonía básico digital**".

En el video de nuestra charla 06, presentamos cómo se puede capturar y ver de forma concreta la voz digitalizada por medio de "**Wireshark**".



Si quieres avanzar más aún con el tema de digitalización de voz y/o VoIP (Voz sobre IP) puedes adelantarte un poco en este libro e ir a:

VoIP (Voz sobre IP) Seguridad - Charla 62 - Aprendiendo Ciberseguridad paso a paso

Enlace al video:

También tienes bastante más desarrollado el tema en el capítulo 1. "Historia y evolución de redes", punto: 1.5. "Voz sobre IP y VoLTE (Voice Over LTE)" de nuestro libro "**Seguridad en Redes**"

Volver al índice

www.darFe.es

Charla 07

Medios - Cables

Enlace al Video:

Resumen:

Toda señal electromagnética para propagarse, necesita de un medio físico. En el ámbito de telecomunicaciones, los medios físicos que se emplean son cables, fibras ópticas y el “Ether”.

Desarrollaremos todos ellos, pero para darle un cierto orden, comenzaremos en la charla de hoy con los cables.

Descripción detallada

CHARLA 07: El nivel físico – Medios de comunicaciones

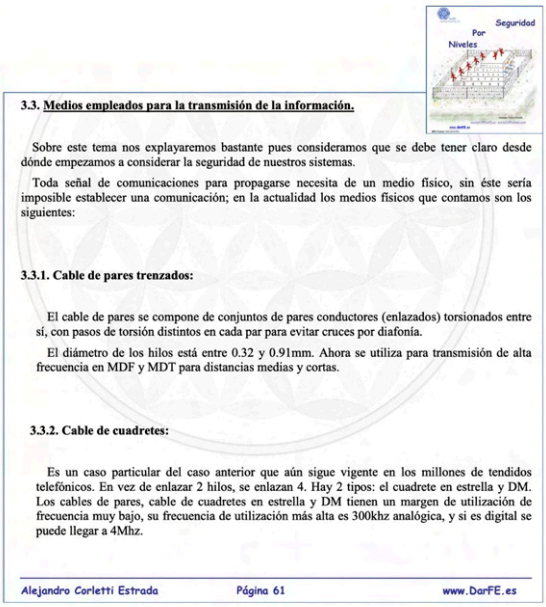
Nos centraremos en el "**medio físico**", es decir:
objeto/materia por la que se desplaza la información o señal.

Funciones y servicios:

- Activar/desactivar la conexión física.
- Transmitir las Unidades de datos.
- Gestión de la capa física.
- Identificación de puntos extremos (Punto a punto y multipunto).
- Secuenciamiento de bit (Entregar bit en el mismo orden que los recibe).
- Control de fallos físicos del canal.

Medios físicos empleados para la transmisión de la información.

- Cable coaxial
- Cable de pares trenzados
- Fibra Óptica
- Ondas electromagnéticas (éter o aire)
- Guías de onda



Toda señal de comunicaciones para propagarse necesita de un medio físico, sin este sería imposible establecer una comunicación, en la actualidad, dentro de los medios físicos que contamos, los cables de telecomunicaciones que podemos presentar son los siguientes.

1. cable de pares trenzados:

   El cable de pares se compone de conjuntos de pares conductores (enlazados) torsionados entre si, con pasos de torsión distintos en cada par para evitar cruces por diafonía.

   El diámetro de los hilos está entre 0.32 y 0.91mm. Ahora se utiliza para transmisión de alta frecuencia en MDF y MDT para distancias medias y cortas

2. Cable de cuadretes:

   Es un caso particular del caso anterior que aún se sigue vigente en los millones de tendidos telefónicos. En vez de enlazar 2 hilos se enlazan 4. Hay 2 tipos: el cuadrete en estrella y DM. Los cables de pares, cable de cuadretes en estrella y DM tienen un margen de utilización de frecuencia muy bajo, su frecuencia de utilización más alta es 300khz analógica, y si es digital se puede llegar a 4Mhz.

3. Cable coaxial:

   Este cable ya prácticamente se está dejando de emplear pues se reemplazó por fibra óptica, pero lo mencionamos aquí pues aún está instalado en varias redes. El cable coaxial consiste en un conductor recubierto en primer lugar por material aislante, luego por una malla conductora y finalmente por una cubierta de material plástico aislante flexible.

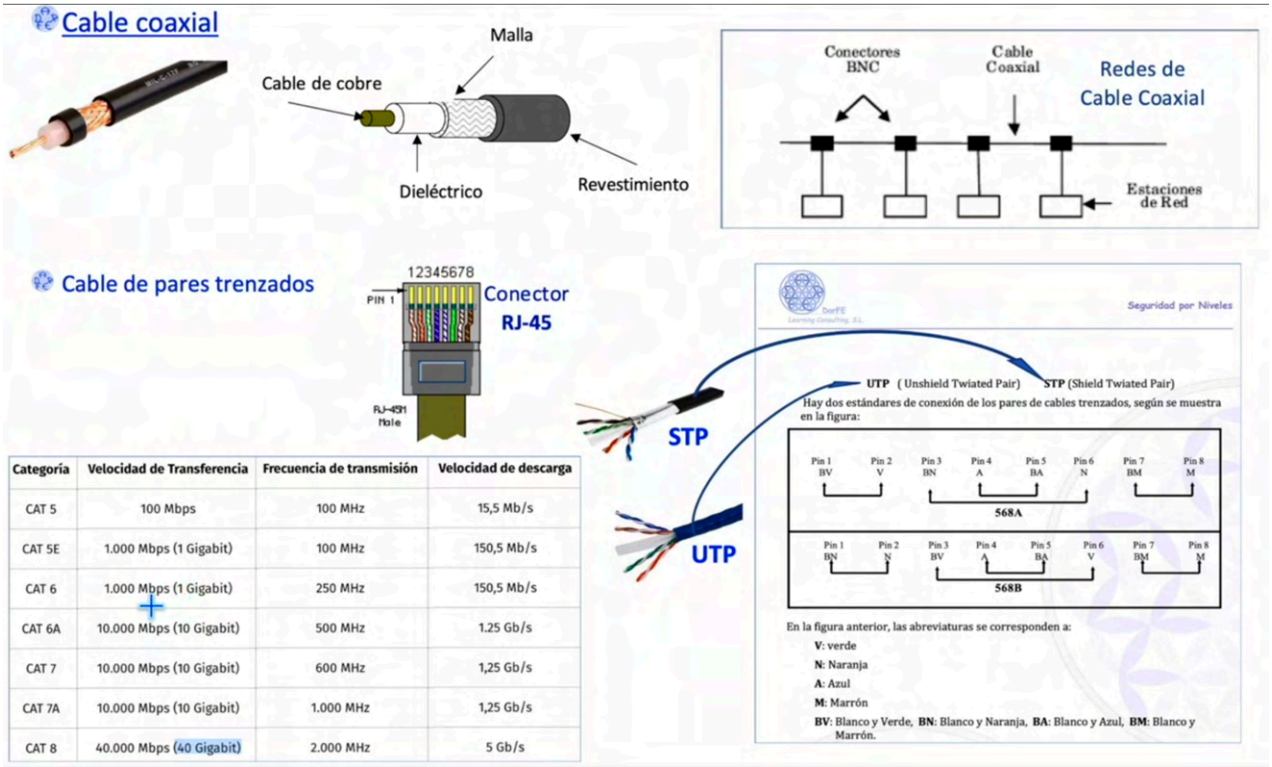
En las aplicaciones LAN, la malla es eléctricamente neutra, y sirve como una malla de protección interna de aislamiento de los ruidos del conductor. La malla también contribuye a eliminar las pérdidas de señal confinando la señal transmitida al cable.

El cable coaxial puede trabajar en un mismo rango de frecuencias, a mayor distancia que el cable par trenzado, pero en contraposición, es más caro.

El cable coaxial de 50 Ohms está "reconocido" por la norma, pero "no se recomienda", y la puesta a tierra se convierte en obligatoria de acuerdo a las prescripciones de la norma **ANSI / TIA / EIA 607**, como parte integral del cableado de telecomunicaciones.

El cable coaxial fino se conecta formando redes "linea" o "bus" por medio de conectores "**T**" denominados British Naval Connector (**BNC**)

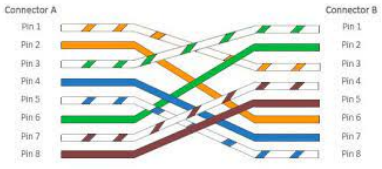
Cada extremo de estas "T", se unan por medio de latiguillos, que en sus extremos llevan este tipo de conectores simples, también denominado BNC.



Categoría	Velocidad de Transferencia	Frecuencia de transmisión	Velocidad de descarga
CAT 5	100 Mbps	100 MHz	15,5 Mb/s
CAT 5E	1.000 Mbps (1 Gigabit)	100 MHz	150,5 Mb/s
CAT 6	1.000 Mbps (1 Gigabit)	250 MHz	150,5 Mb/s
CAT 6A	10.000 Mbps (10 Gigabit)	500 MHz	1.25 Gb/s
CAT 7	10.000 Mbps (10 Gigabit)	600 MHz	1,25 Gb/s
CAT 7A	10.000 Mbps (10 Gigabit)	1.000 MHz	1,25 Gb/s
CAT 8	40.000 Mbps (40 Gigabit)	2.000 MHz	5 Gb/s

4. Cables trenzados de 4 pares:

Un par de cables trenzados, es un par de alambres que se cruzan o trenzan entre sí para minimizar la interferencia electromagnética entre los pares de cables.



Cada par de cables conforma un enlace para transmisión de señales de datos completo. El flujo entre ambos cables es igual, pero de sentido contrario. Este flujo de corrientes produce campos electromagnéticos que pueden introducir ruidos a los pares vecinos. De todos modos, los campos correspondientes a cada par de cables tienen polaridades opuestas. Trenzando los cables entre sí, los campos magnéticos de cada uno se cancelan mutuamente, lo cual minimiza el ruido y/o la interferencia generada por cada par de cables.

Mediante 2 boletines técnicos (**TSB 36**: Especificaciones de cables y **TSB 40**: Equipos de interconexión, jacks, patcheras, etc), dividen al tipo de cable **UTP** (Unshield Twisted Pair) en varias categorías diferentes, según su ancho de banda:

- Cat 3: Hasta 16 Mhz
- Cat 4: Hasta 20 Mhz
- Cat 5: (Cable sólido de pares trenzados), 22 o 24 AWG (0,643mm o 0,511mm), 100 Mhz.
- Cat 5e: (Categoría 5 mejorada), 26 AWG (0,409mm), 100 Mhz, UTP
- Cat 6: (Cable sólido de pares trenzados), 24 AWG (0,511mm), 300 Mhz, FTP
- Cat 7: (Cable sólido de pares trenzados apantallados por par),23 AWG (~0,600mm), 600 Mhz, STP

El **UTP** Cat 6 es el que aún domina el mercado. Es un cable diseñado específicamente para la transmisión de datos y se basa en pares de alambres de cobre retorcidos mediante una hélice en sentido anti horario y una vuelta de 5 a 15 cm. (A mayor cantidad de vueltas por cm es de mayor calidad, pero también más difícil de manipular).

Este giro sobre sí mismo le permite eliminar tanto las componentes internas como externas de inducción y modulación cruzada, agrupando en el mismo cuatro pares diferentes. En un cable dado, cada par tiene un paso diferente del resto de los pares, y esto hace que un cable sea una unidad fabricada bajo estrictas especificaciones y no un simple conjunto de pares.

Esto mismo hace que su instalación deba ser más cuidadosa y considerar que no se puede tirar violentamente del mismo ya que variaría el paso de la hélice del roscado y por lo tanto la respuesta física del cable.

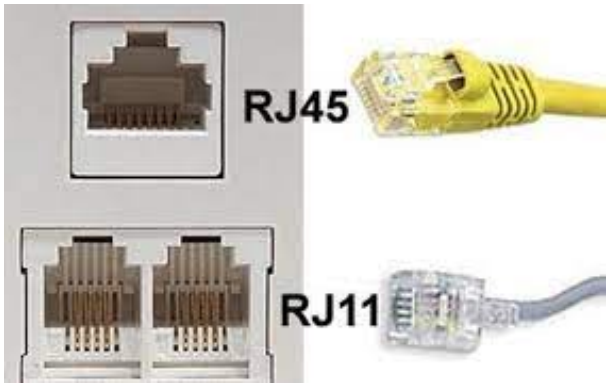
La impedancia característica del mismo es de **100 Ohms** y la longitud máxima de cada segmento de 100 mts.

Para el caso de datos hasta categoría 5e, de los cuatro pares posibles se usan 2, uno para transmisión y otro para recepción, quedando dos libres. Este concepto ya no aplica a categoría 6 y 7.

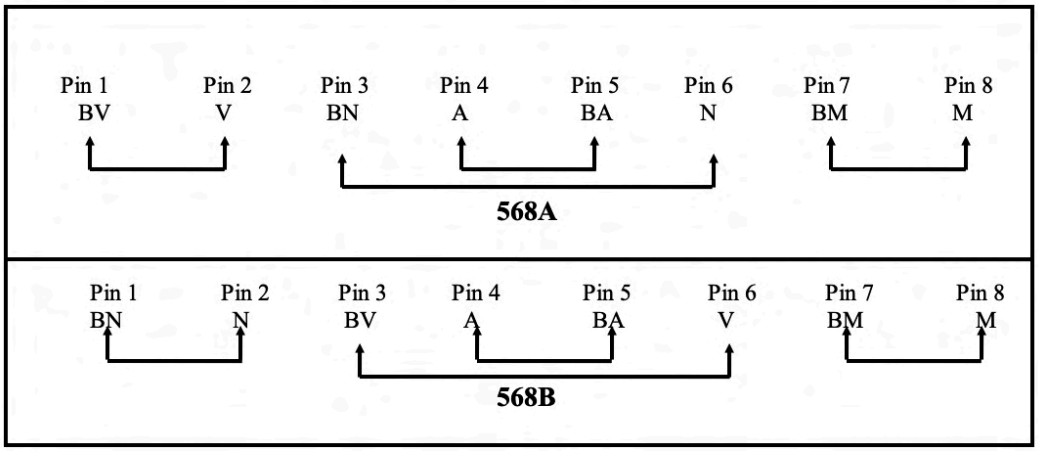
Una variación de este cable es el que se conoce como **STP** (Shield Twisted Pair), que es el mismo cable anterior con un blindaje externo, generalmente un papel de aluminio. Si bien puede disminuir aun más la interferencia obliga a tener un sistema de masas donde en ningún caso existan más de 3 ohms entre los conectores y la masa del sistema.

Este tipo de cables emplean los conectores **RJ-45** para datos y **RJ-11** para telefonía.

Conector RJ-45 hembra



Hay dos estándares de conexión de los pares de cables trenzados ,**TIA/EIA 568 A y B**, y su conexión respecto a los pines de los conectores RJ-45 se colocan según se muestra en la figura siguiente.



En la figura anterior, las abreviaturas se corresponden a:

V: verde

N: Naranja

A: Azul

M: Marrón

BV: Blanco y Verde,

BN: Blanco y Naranja,

BA: Blanco y Azul,

BM: Blanco y Marrón.

El desarrollo completo sobre, podéis seguir estudiándolo en detalle en el capítulo 3 del libro "**Seguridad por Niveles**".

Volver al índice

www.darFe.es

Charla 08

Medios - Fibra óptica

Enlace al Video:

Resumen:

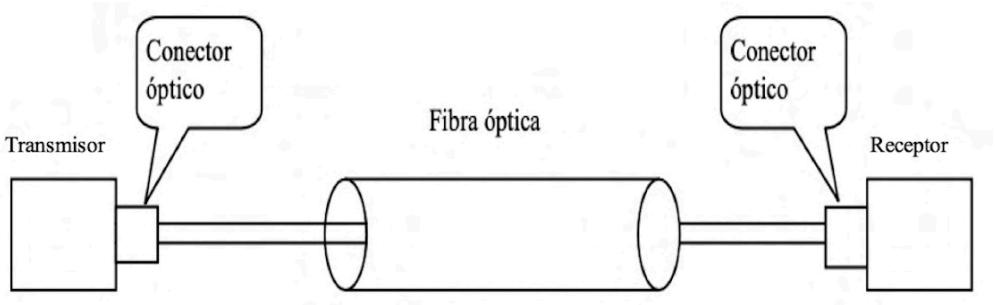
En esta charla, se presenta con todo detalle, los diferentes tipos de fibras ópticas, su funcionamiento, propiedades, características y como se compone un sistema óptico.

Descripción detallada

1. Sistemas de transmisión de fibra óptica.

Para poder implementar la tecnología de transmisión por medio de luz, es necesario contar con todo un sistema diseñado para este uso, los componentes básicos del mismo son:

- Fuente óptica: Convierte la señal eléctrica en luz.
- El cable de fibra óptica que transporta la señal.
- El detector óptico que convierte la señal nuevamente a electrones.



Como fuentes ópticas se emplean comúnmente el diodo **LED** o **LD** de modulación directa, mientras que como detector óptico se emplean el **ADP** o el **PIN – PD** de alta sensibilidad y de respuesta veloz.

2. Características de la luz.

La luz se puede definir como el agente físico que ilumina objetos y los hace visibles, siendo emitida por cuerpos en combustión, ignición, incandescencia, etc. Desde el punto de vista físico, la luz es una radiación u onda electromagnética. El espectro electromagnético se extiende desde las ondas de radio hasta los rayos gamma. De todo este espectro, sólo una zona muy pequeña es detectable por el ojo humano, y es lo que se llama el espectro visible o luz visible.

Toda onda está caracterizada por dos parámetros fundamentales:

- La velocidad de propagación.
- La frecuencia.

La velocidad de propagación es la distancia recorrida por una señal en una unidad de tiempo. Toda onda electromagnética se desplaza en el vacío a **300.000 km/s**. La frecuencia es el número de veces que la onda repite su período en un segundo; en el caso de la luz es del orden de varios cientos de billones de ciclos por segundo.

Otro parámetro a considerar es el de longitud de onda, que se refiere a la distancia que la señal viaja durante un período, es por esta razón que se mide en metros.

$$\lambda = C / f$$

λ: Longitud de onda.

C: Velocidad de propagación.

f: Frecuencia.

La idea de longitud de onda o de frecuencia dentro del espectro visible, se asocia a la idea de un determinado color de una determinada luz. Una luz de un color puro se llama monocromática. Si está compuesta por todos los colores, se llama luz blanca.

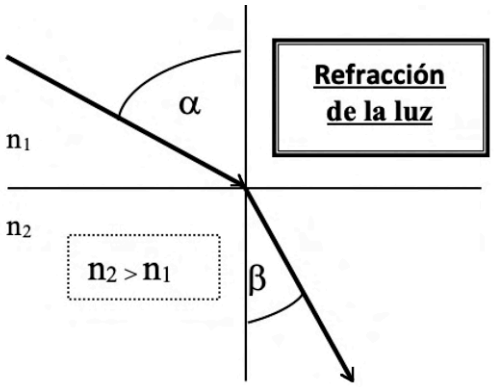
3. Propagación de la luz:

La luz se propaga en el vacío en forma rectilínea de acuerdo con lo que se denomina rayo o **haz lumínico**, en cualquier medio transparente cumple esta propiedad, siempre que la composición de ese material sea la misma en todo su recorrido. Todo medio físico opondrá resistencia al pasaje de una señal electromagnética, produciendo el efecto de disminuir su velocidad respecto al vacío. La relación entre la velocidad de la luz en el vacío y en un medio real se denomina índice de refracción.

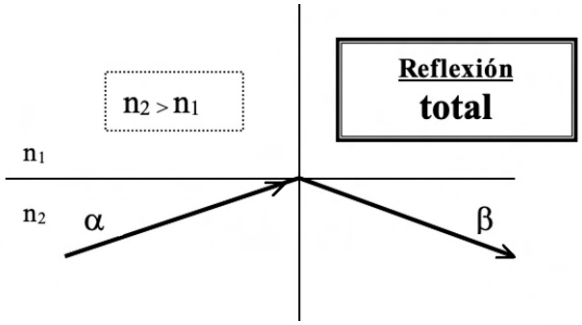
4. Reflexión y refracción de la luz.

Al incidir una onda luminosa sobre una superficie plana divisoria de dos medios de índice de **refracción** diferente, su trayectoria se desviará acorde a la siguiente relación:

$$\textbf{Sen } \alpha \textbf{ / sen } \beta = n_2 \textbf{ / } n_1$$

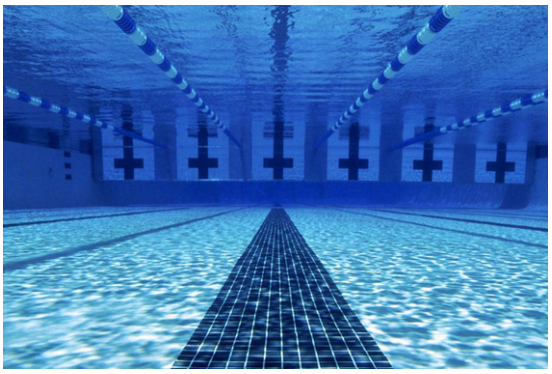


Como se puede apreciar, si se va incrementando el ángulo de incidencia desde n2 a n1, llegará un momento en el cual, el ángulo α llegará a ser de 90 grados, siendo siempre **β** menor a este valor (si: **n2** > **n1**). Superado este umbral, el haz de luz deja de pasar a la superficie n1, para producir el fenómeno denominado reflexión total, en el cual la luz se propaga dentro del medio n2, con un ángulo igual al de incidencia.

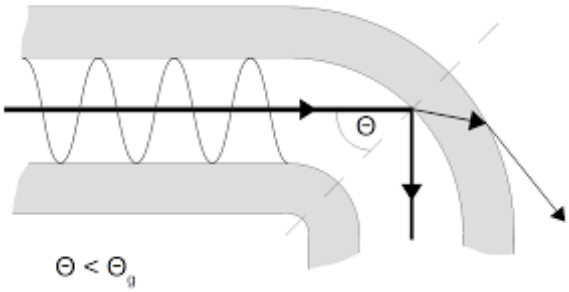


Si el ángulo de incidencia del haz de luz se mantiene inferior al valor descrito, la luz se **reflejará** dentro de la superficie n2. Al ángulo dentro del cual se produce la

reflexión total se lo denomina Angulo de acepción o aceptación.



La mejor analogía con la reflexión total, la solemos ver en cualquier piscina, al sumergirnos en la misma, si miramos desde dentro del agua la superficie y nos vamos acercando a ella, llegará un momento en que la superficie la veremos como un espejo en el que se refleja el fondo de la piscina. Este es un claro ejemplo del fenómeno de "**reflexión total**".



Un detalle de interés, es el de las micro curvaturas, pues, tengamos en cuenta que a medida que se dobla una fibra óptica, el ángulo de incidencia dentro del núcleo varia. Si este ángulo supera la tolerancia de esta fibra, deja de producirse el fenómeno de "**reflexión total**" y la luz, se escapa del núcleo, pues se produce la "**refracción de la luz**". Por esta razón es que hay que ser extremadamente cauteloso al realizar cableados de fibra óptica, para que la misma se encuentre holgada dentro del ducto o canal por el que se la va pasando, para evitar este tipo de anomalías que pueden llegar hasta dejar fuera de servicio este medio.

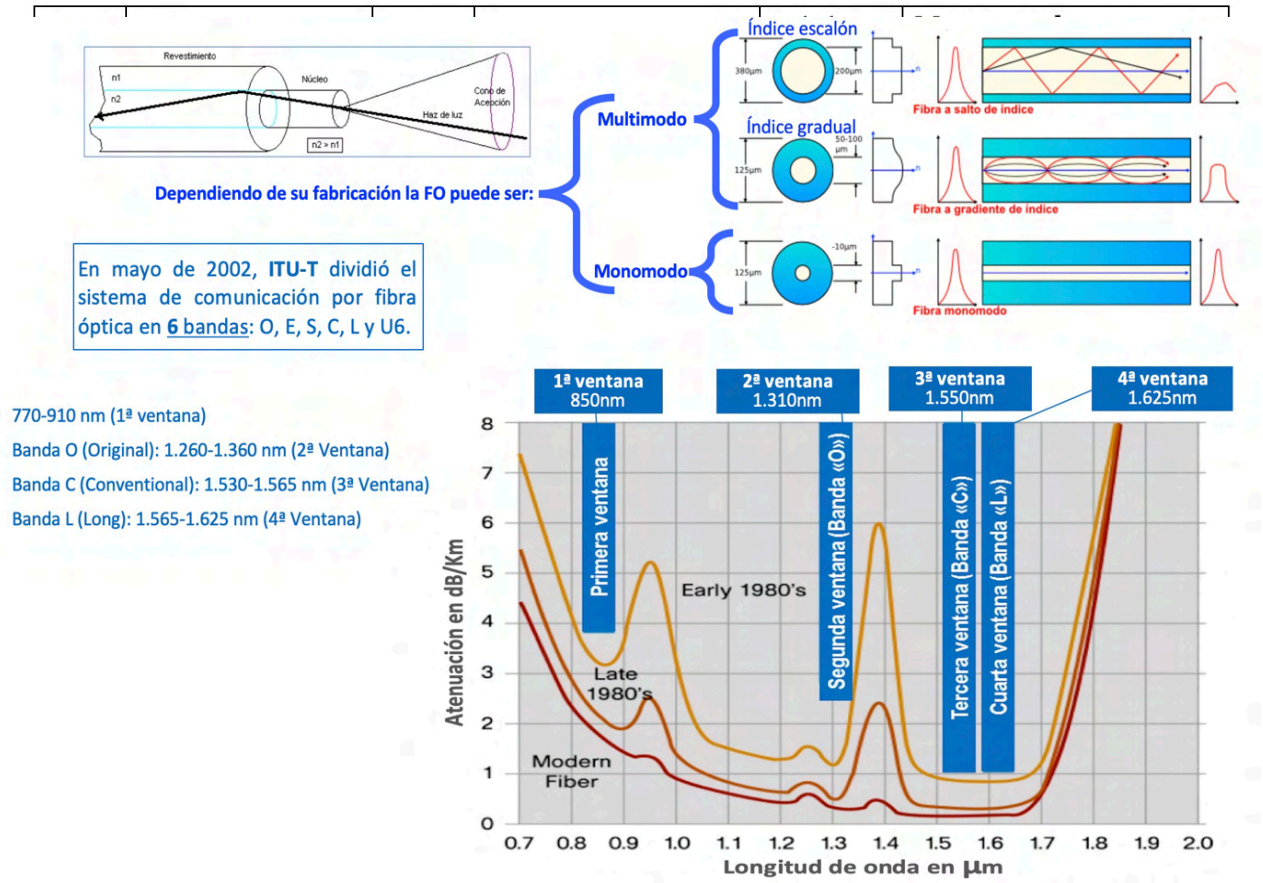
5. Fibra óptica (**FO**) (Descripción general).

La FO es un dispositivo de material dieléctrico (no conductor de corriente eléctrica) que es capaz de confinar y guiar la luz.

Las FFOO usadas en telecomunicaciones están formadas por dos cilindros concéntricos llamados núcleo y revestimiento con diferentes índices de refracción (n1 en el revestimiento y n2 en el núcleo), por medio de los cuales, si se ingresa un haz de luz dentro del cono de acepción, se producirá una y otra vez el fenómeno de reflexión total, transportando de esta forma la señal. Los diámetros que se suelen emplear son 125 µm para el revestimiento y desde los 9 a 62,5 µm para el núcleo acorde al modo (a tratar más adelante).

Como se puede apreciar en las imágenes que siguen, dependiendo de su fabricación, las fibras pueden ser básicamente:

- Multimodo: Su núcleo es de 62,5 µm y la luz dentro del mismo se refleja por diferentes caminos, o "modos". Es la más empleada en redes LAN y/o cortas distancias.
- Monomodo: Su núcleo es de 9 µm y la luz dentro de la misma se desplaza como si se tratara de un único haz o "modo". Este tipo de fibra alcanza mucha mayor distancia, y por esa razón es la más empleada por los cableados de telefonía urbana o los cables submarinos.



Otro aspecto de interés que se aprecia en la imagen anterior, es el hecho de las "ventanas" de la fibra óptica. Por características físicas del silicio, cuestión que también sucede con otros materiales, el paso de la luz por el mismo, sufre diferentes grados de atenuación dependiendo de las longitudes de onda que se le apliquen. En la imagen anterior y a la derecha podemos ver claramente que existen cuatro ventanas en las que la atenuación es menor al resto de la imagen. Estas son las ventanas más comunes y estandarizadas que se emplean para transmitir sobre fibras ópticas.

La primer ventana (850nm) es la que menor requerimientos tecnológicos requiere. Todos sus componentes (emisores y receptores) son más económicos, pero tiene como contrapartida que es la que menor distancia puede alcanzar, pues tal cual se ve en la imagen, de las cuatro, es la que más atenuación tiene. La cuarta ventana (1.625nm) por el contrario, llega a mucha más distancia, pero requiere mayor calidad de componentes y costes.

6. Propiedades de la F.O.

Basados en los diferentes parámetros del material, es que se puede clasificar las FO en cuatro grupos acorde a diferentes propiedades:

7. Los cables de fibra óptica.

Por último, las fibras ópticas, se suelen presentar formando “**cables de FO**”.

Estos, se componen de varias FO, protegidas y recubiertas específicamente para la función que vayan a desempeñar: aéreas, submarinas, colgantes, bajo el asfalto, por ductos subterráneos, etc. Otro aspecto de interés, es que al ser dieléctricas, no sufren ningún tipo de interferencia por el pasaje de la corréate eléctrica, existiendo algunos cables de fibra óptica, por ejemplo, que están dentro de los tendidos de cables eléctricos de alta tensión, pues son huecos, debido al desplazamiento periférico de la corriente eléctrica y el centro de los mismos (hueco) se aprovecha para tendidos de FO.

Volver al índice

www.darFe.es

Charla 09

Nivel Físico - Resumen

Enlace al Video:

Resumen:

Para cerrar el nivel físico, en esta charla se presenta un resumen que destaca los aspectos fundamentales que han sido desarrollados sobre el nivel Físico.

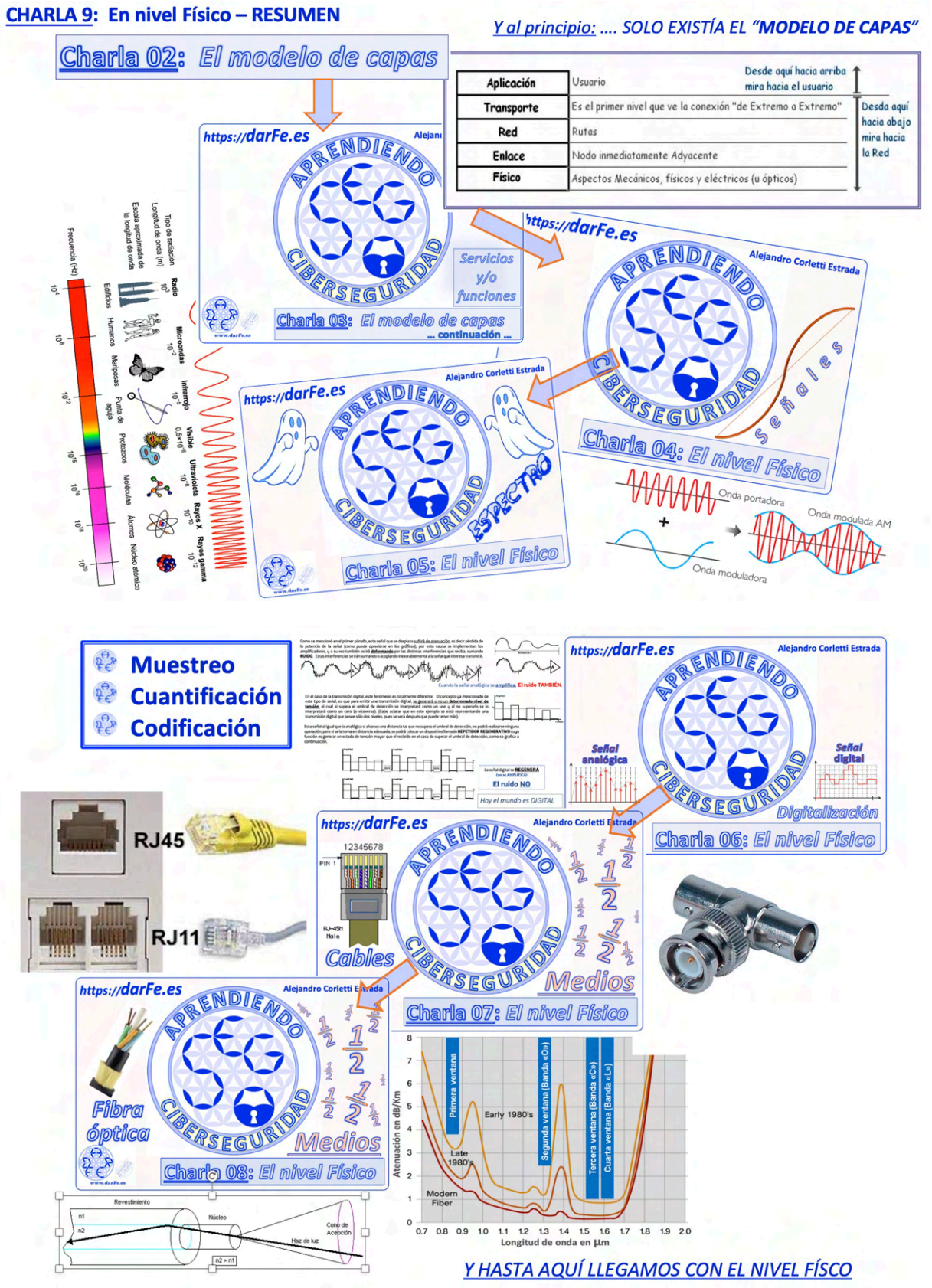
Ocurren muchísimos ataques de nivel físico, tanto con cables, wifi, telefonía, televisión satelital, etc.

El nivel físico es uno de los pilares más fuertes de la ciberseguridad.

Os aconsejamos que le dediquéis unos minutos al mismo pasa afianzar los conocimientos adquiridos hasta aquí.

Descripción detallada

Primero presentamos brevemente la secuencia de lo que hemos ido desarrollando en este nivel.

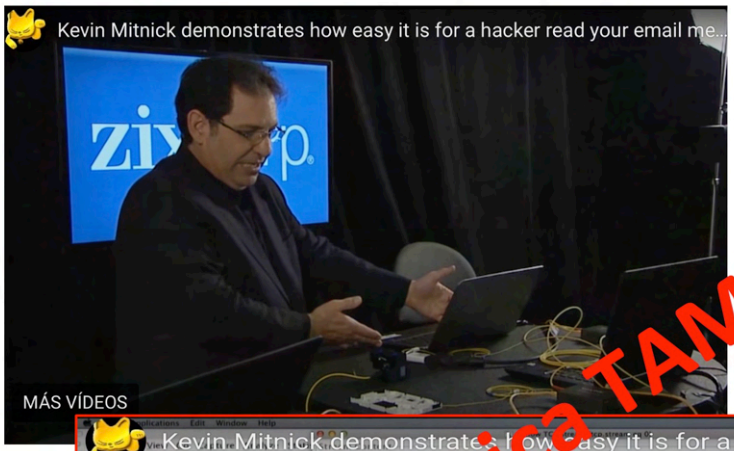


¿Por qué tanto rollo con el nivel físico?

Porque ocurren muchísimos ataques de nivel físico, tanto con cables, wifi, telefonía, televisión satelital. Corriente eléctrica.

Hasta la fibra óptica se puede "pinchar" y hasta por aproximación, lo veremos por medio de lo que ha hecho hace muy poco "**Kevin Mitnick**". Se presentan algunos artículos y publicaciones al respecto

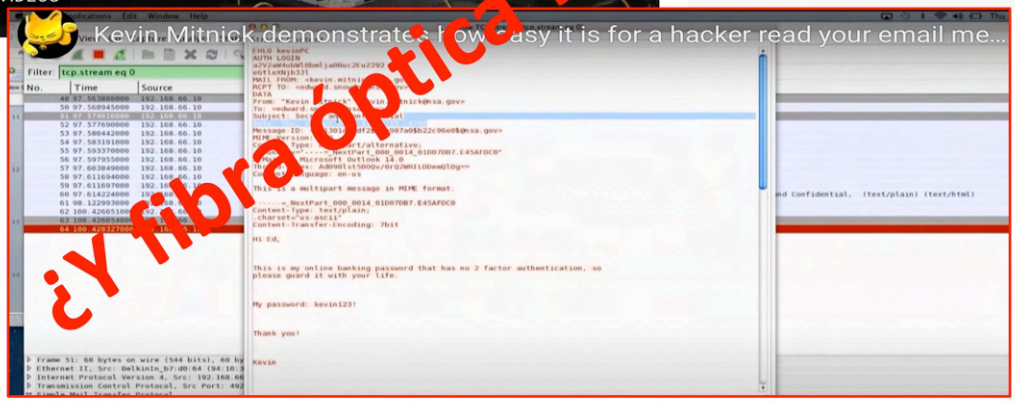
El nivel físico es uno de los pilares más fuertes de la ciberseguridad.



El FOD 5503 utilizado para interceptar las comunicaciones es uno de los muchos acopladores de esta naturaleza que prometen **acoplamiento no invasivo y bidireccional en cables de fibra óptica**, como por ejemplo el OPT130 de Kingfisher, y obviamente no es un *hardware* diseñado para realizar esta clase de *hackeos*, sino simplemente para tareas de mantenimiento e identificación de cables donde no se tiene acceso a los extremos.

El FOD 5503 usado para la demostración

¿Y fibra óptica TAMBIÉNNN...?



Volver al índice

www.darFe.es

Charla 10

Desenchufando - En E de PC

Enlace al Video: 

Resumen:

Durante Todo el ciclo, y también en el presente libro, cada diez videos hacemos un "**Desenchufe**".

La vida no es solo estudio y trabajo, hay que dedicarle su tiempo al ocio y tiempo libre, a los amigos, familia…

Te invitamos a que lo hagas, que pises el freno estos minutos y te "desenchufes".

Descripción detallada

El desenchufe de hoy se llama: “**En e de PC**”

Presentación del tema:

En E de PeCe, debe entenderse que empleé “E”
Pensé que el emprender este deber de entretener
el excelente set de gente que lee y ve este célebre server Web
en vez de ser mequetrefes y peleles que ven tele,
debe ser el deber que excede el presente ser
y perennemente genere el efervescente deber de encender el PeCe

Letra Original:

El que desee verme que emplee el PC,
que entre en red,
teclee <net send> PEPE HELP <enter>.
Que en el CD esté el ftp en Perl,
ese que les entregué el tres de este mes.
Esperen que entre en web,
dejen que el server eject el CD,
se debe encender el red led del TV.
Estremece el set que entremezclé
Se debe leer en peltre el msg: PEPE ´S WEB. (presente)

Este célebre shell en “C” que creé,
es el que ves en el server (Es GPL).
En vez de text, entregué en MS Excel,
se ve entre “B” tres y “S” trece
(□□que célebre el nest que empleé!!!).
dejé el Help en C:\temp\help.exe. (Se debe leer, eh),
El que testee el stress en el server “DELL”
debe tener que encender este en red,
que extreme y pelee el telnet,
este ente, que es TCP,
se teme que chequee el CRC
y degenere en redes Ethernet.

Que espere, que mezcle el relé
que vende este mes Nextel,
se prevé que es el “Best Seller”
que emerge, que vende y emprenden resellers
El tener DSL es excelente, pese que es PPP.

Propuestas futuras de Estribillo:

Este mes empecé en el Deep Web
Me venden cheques que deben ser de Ley
Entré en Skype
Y en el BGP de Nestlé
Reventé el server SMTP del PP
Es que este retrete de server
¿creen que merece verse presente en Red?

www.darFe.es

Charla 11

Nivel de Enlace - Introducción

Enlace al Video: 

Resumen:

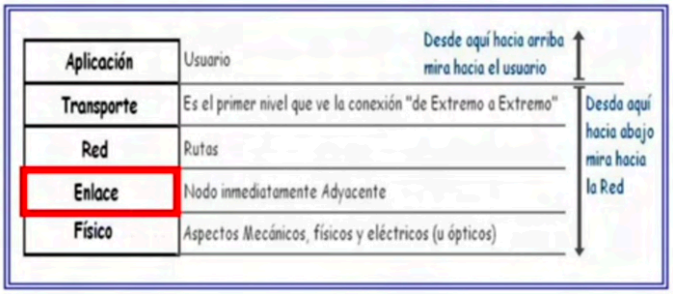
En este video comenzamos a desarrollar el **nivel de Enlace**, o nivel 2 de la pila **TCP/IP**.

Este es el nivel lógico más bajo de toda la pila, con lo que “ve pasar” todos los protocolos superiores. Su mayor aplicación está en los entornos **LAN** (Local Area Network), y dentro de la misma, iremos viendo que existen muchas medidas de Ciberseguridad que debemos implementar para robustecer este nivel.

Descripción detallada

El año 1980 (**80**'), y el mes de febrero (**2**), **IEEE** (Institute of Electrical and Electronics Engineers creó el subcomité "**802**", cuyo objetivo fue el de analizar y estandarizar todo lo referente al nivel de enlace.

Por esa razón cada vez que nos encontremos con estándares IEEE-802.x sabemos que se refiere pura y exclusivamente al nivel de "enlace"



Dentro de este comité se conforman diferentes grupos de trabajo, los cuales en la actualidad son denominados de la siguiente forma:

IEEE 802.1 – Normalización de interfaz.

IEEE 802.2 – Control de enlace lógico.

IEEE 802.3 – CSMA / CD (ETHERNET)

IEEE 802.4 – Token bus.

IEEE 802.5 – Token ring.

IEEE 802.6 – MAN (ciudad) (fibra óptica)

IEEE 802.7 – Grupo Asesor en Banda ancha.

IEEE 802.8 – Grupo Asesor en Fibras Ópticas.

IEEE 802.9 – Voz y datos en LAN.

IEEE 802.10 – Seguridad.

IEEE 802.11 – Redes inalámbricas WLAN.

IEEE 802.12 – Prioridad por demanda

IEEE 802.13 – Se ha evitado su uso por superstición

IEEE 802.14 – Modems de cable.

IEEE 802.15 – WPAN (Bluetooth)

IEEE 802.16 - Redes de acceso metropolitanas sin hilos de banda ancha (WIMAX)

IEEE 802.17 – Anillo de paquete elástico.

IEEE 802.18 – Grupo de Asesoría Técnica sobre Normativas de Radio.

IEEE 802.19 – Grupo de Asesoría Técnica sobre Coexistencia.

IEEE 802.20 – Mobile Broadband Wireless Access.

IEEE 802.21 – Media Independent Handoff.

IEEE 802.22 – Wireless Regional Area Network.

Primero desarrollaremos el funcionamiento de este nivel, comenzando por "**Ethernet**" o **IEEE-802.3**, y luego seguiremos desarrollando varias normas más de la familia 802.x, relacionadas específicamente a los temas de Ciberseguridad que son de interés para

este libro, en particular los relacionados a **IEEE-802.1x** donde encontraremos temas de sumo interés.

Comenzaremos presentando el primer diseño de este tipo de redes Ethernet que creó **Robert Metalfe** en el año 1976, basado en el protocolo "**Aloha**" de la Universidad de Hawai.

CHARLA 11: El nivel de enlace – Introducción

IEEE 802 del **Institute of Electrical and Electronics Engineers** (IEEE).
Se identifica también como LMSC (LAN/MAN Standards Committee)
Referencias: https://www.ieee802.org

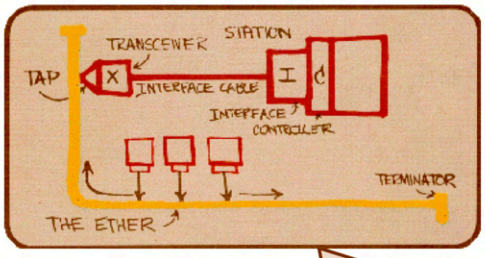
802.1 Higher Layer LAN Protocols Working Group
https://1.ieee802.org/

El Grupo de Trabajo IEEE 802.1 divide su trabajo en los siguientes Grupos de Tareas :

- *Maintenance*
- **Security**
  https://1.ieee802.org/security/
- *Time-Sensitive Networking (TSN)* (**802.1Q – 802.1aq**)

802.1 Lo desarrollaremos al final de las charlas del nivel de Enlace

El Grupo de Trabajo de Seguridad especifica la funcionalidad para soportar la comunicación segura entre dispositivos (estaciones finales y puentes) conectados a las LAN IEEE 802.



Este diagrama fue dibujado a mano por **Robert M. Metcalfe** y fotografiado por **Dave R. Boggs** en 1976 para producir una diapositiva de 35mm utilizada para presentar Ethernet a la Conferencia Nacional de Computación en junio de ese año. En el dibujo están los términos originales para describir Ethernet.

- El IEEE Std **802.1X** Port-Based Network Access Control. Especifica el uso de protocolos de autenticación y autorización estándar del sector para soportar el control de acceso a la red y la creación de infraestructuras seguras. Especifica el protocolo MACsec Key Agreement (**MKA**) utilizado por IEEE Std 802.1AE. https://1.ieee802.org/security/802-1x/
- IEEE Std **802.1AE** MAC Security (MACsec) especifica el uso de suites de cifrado criptográficas para garantizar la autenticidad, la integridad (y opcionalmente la confidencialidad) de los datos (y otros parámetros) del servicio MAC y del servicio de la subcapa interna (como se especifica en IEEE Std 802.1AC y se utiliza dentro de las arquitecturas de puente especificadas en IEEE Std **802.1Q**). https://1.ieee802.org/security/802-1ae/
- IEEE Std **802.1AR** Secure Device Identity especifica las credenciales de autenticación (**DevIDs**) diseñadas para ser utilizadas por los dispositivos conectados a la red LAN IEEE 802 junto con los protocolos de autenticación, aprovisionamiento e inscripción estándar del sector, incluidos los identificados por IEEE Std 802.1X. https://1.ieee802.org/security/802-1ar/
- IEEE Std **802E** Recommended Practice for Privacy Considerations for IEEE 802 Technologies. Especifica un modelo de amenazas a la privacidad para las tecnologías IEEE 802, proporciona recomendaciones sobre cómo protegerse contra las mismas y promueve un enfoque coherente para la mitigación de amenazas por parte de los desarrolladores de protocolos IEEE 802. https://1.ieee802.org/security/802e/

En cuanto al funcionamiento del nivel de enlace, nos interesa en particular centrarnos en tres de estos estándares que son los más empleados hoy en día en el mercado.

Estos tres son los que se presentan a continuación.

Estándares que desarrollaremos a nivel de enlace:

IEEE 802.3 Ethernet Working Group
https://www.ieee802.org/3/

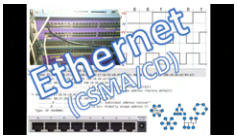
IEEE 802.11 Wireless Local Area Networks (WLAN)
https://www.ieee802.org/11/

IEEE 802.15 Working Group for Wireless Specialty Networks (WSN)
https://www.ieee802.org/15/

En nuestro **canal Youtube**, tenemos también un par de videos para que vayas profundizando en el tema.

Ethernet - CSMA/CD

Este es el enlace es:



ARP protocol - Protocolo ARP (Address Resolution Protocol)

Este es el enlace es:

Si quieres ir avanzando sobre este tema, se desarrolla en detalle en el capítulo 4 del libro "**Seguridad por Niveles**".

Volver al índice

www.darFe.es

Charla 12

Tiempo de Ranura

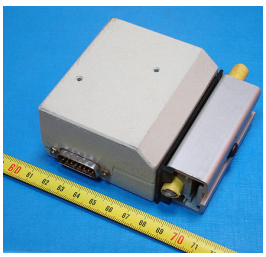
Enlace al Video:

Resumen:

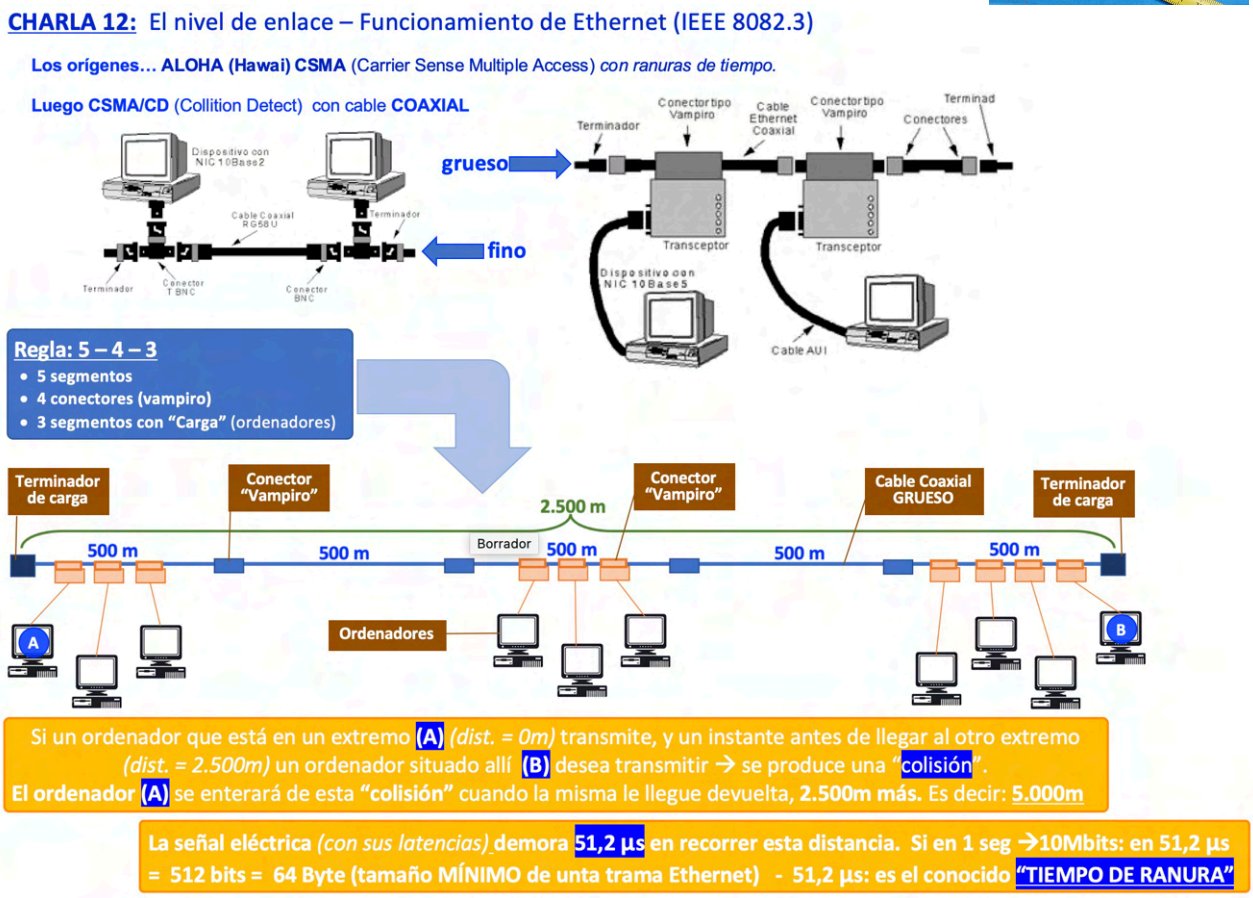
Este conceptos e “**Tiempo de ranura**”, como hemos desarrollado en este video, es uno de los puntos de partida de las redes Ethernet, pues debido al mismo: **51,2 µs**, es que se define el tamaño mínimo de una trama y, a su vez es el tiempo que se emplea para regular las “**colisiones**”, concepto que como veréis en las sucesivas charlas, es la metodología que emplea Ethernet para acceder al medio.

Descripción detallada

En las charlas del **nivel Físico**, presentamos el cable coaxial, fino y grueso. Este cable fue el primero que se empleo en las redes LAN, y como dijimos, se conectaba un ordenador a continuación de otro, formando las redes de topología "**bus**". El coaxial fino, se conectaba a través de esas "T" que se llamaban **BNC** (British Naval Connector), y el coaxial grueso, lo hacía por medio de un conector que, en la jerga de redes era definido como "**vampiro**".



En la imagen que sigue se puede apreciar ambos conectores.



Concepto de Tiempo de ranura (51,2 µs).

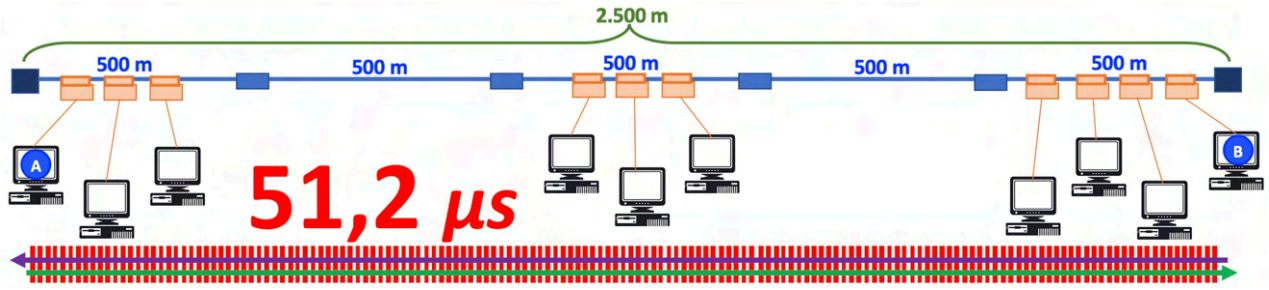
Este valor nace de la definición misma de Ethernet, y aparece en los inicios del este protocolo, cuando este tipo de redes se implementaban, como acabamos de comentar, en topología Bus. Sobre cable coaxial grueso, se podían unir hasta cinco segmentos de 500 m cada uno, a través de cuatro repetidores regenerativos y con solo tres de ellos cargados (con ordenadores conectados). Se la conocía como **norma 5-4-3** (como se aprecia en la imagen anterior). La distancia máxima que alcanzaba esta red era de **2.500 m**.

Teniendo en cuenta el tiempo de latencia de los repetidores, una señal eléctrica tardaba en recorrer esta distancia ida y vuelta, aproximadamente este tiempo: 51,2 µs. El tema de fondo aquí radica en que si se tiene en cuenta dos **ETD** (Equipos Terminales de Datos) separados a esta distancia (el peor de los casos), suponiendo que uno de ellos comienza la transmisión, y un instante antes de llegar al segundo, este escucha el canal

y por estar desocupado, comienza a transmitir; entonces se producirá una colisión muy próxima al segundo ETD.

El que inició la transmisión tomará consciencia de la colisión, cuando este estado anormal de tensión regrese a él, es decir, cuando haya recorrido los 2500m de ida y los 2500m de vuelta, que coincide con estos **51,2 µs**. Si se supone que el segundo ETD no inició ninguna transmisión, al cabo de estos 51,2 µs ningún ETD de esta red podría transmitir, pues al escuchar el medio, lo encontraría ocupado. Esto se llama Apropiarse del canal.

Basado en estos conceptos es que se define que el tamaño mínimo de una trama Ethernet no puede ser menor de 64 Byte, pues 64 Byte = 512 bit y 512 bit transmitidos a 10.000.000 bit por segundo (10 Mbps) = **51,2 µs**. También se define que no podrá tener más de 1.518 Byte, para evitar que el apropiado del canal sea eterno, evitando así monopolios del medio.

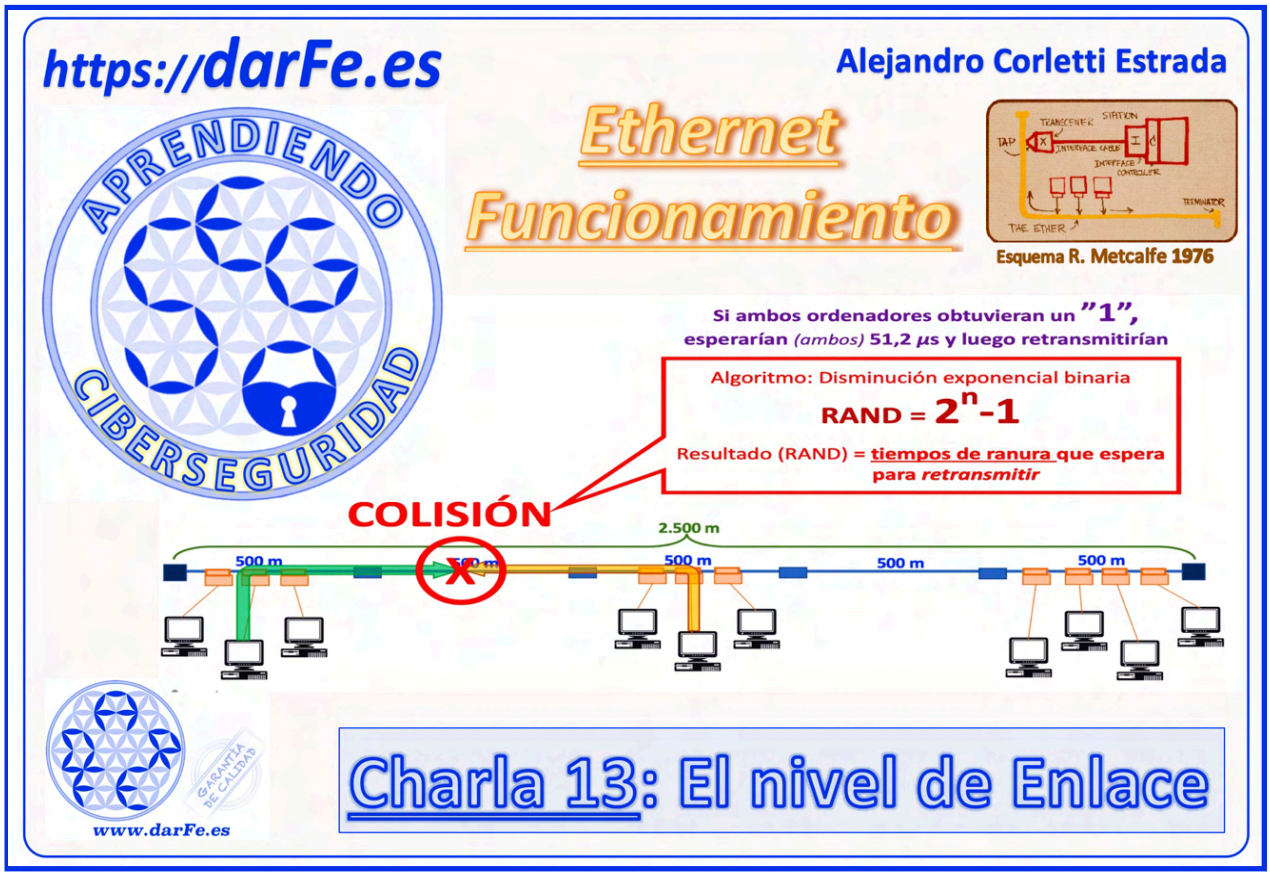


Volver al índice

www.darFe.es

Charla 13

Funcionamiento de Ethernet



Enlace al Video:

Resumen:

En este video presentamos brevemente el nacimiento de **Ethernet**, una diferencias a tener en cuenta respecto a **IEEE-802.3**, pasando luego a desarrollar cómo es la lógica de **CSMA/CD** (Carrier Sence Multiple Access/Colition Detect), pues es la base de este protocolo. Justamente esta idea de "CSMA/CD", se sustenta en la idea de **tiempo de ranura** y el **algoritmo de disminución exponencial binaria**, que no puede ser dejado de lado, por lo que también le dedicamos unos párrafos.

Descripción detallada

Este protocolo, como ya hemos mencionado, tiene sus orígenes en otro conocido como **ALOHA** (saludo de los Hawaianos, que es donde nació), al principio se creyó muy poco probable que está lógica de compulsa por un medio de comunicaciones fuera eficiente, pero en el muy corto plazo se descubrió que sí lo era. **Digital**, **Intel** y **Xerox**, se unen para ponerlo en funcionamiento sobre cable coaxial a 10 Mbps, y como inicialmente se lo empleó en enlaces satelitales que transmitían al "**Ether**", se lo llamó Ethernet, y se lo conocía como **Ethernet DIX**. En el año 1980 (**80**) y en el mes de febrero (**2**), **IEEE** toma cartas en el tema y crea este subcomité, del que también hemos hablado, que estudiaría el tema de **LAN** y **MAN** (Metropolitan Area Network), y por la fecha en que entra en funcionamiento se lo llamó **802.x** (x=distintas áreas), quien será el responsable hasta la actualidad de regular el funcionamiento de estas redes.

Este grupo define todos los aspectos hoy conocidos como familia 802.x, de los cuales como mencionamos solamente en este texto se desea dejar claro algún aspecto de 802.3 y 802.11.

Lo más relevante aquí es que, si se recuerda el aspecto del nivel de enlace (nivel 2) del modelo OSI, este "establece la comunicación con el nodo inmediatamente adyacente". En una topología LAN ¿Cuál es el nodo inmediatamente adyacente? Ante esta cuestión IEEE, propone subdividir el nivel de enlace del modelo OSI en dos sub niveles:

- **MAC** (Medium Acces Control): Responsable de todo lo referente al Hardware de red.
- **LLC** (Logical Link Control), **802.2** : Responsable de la comunicación con los protocolos superiores.

Modelo OSI (Ethernet)	IEEE (802.x)
Enlace (nivel 2)	LLC
	MAC

La propuesta es muy coherente, pues facilita esta compleja actividad característica de las LAN. Pero desde ya, que esta propuesta no es reconocida por OSI, marcando una diferencia entre estos dos protocolos. Aparecen aquí estos dos estándares de mercado, que se recalca "NO SON IGUALES", si bien son muy parecidos. En el caso de CSMA/CD, que es el que interesa en este texto, todo hardware y software de red soporta ambos protocolos y acorde a la trama que se trate, aplica uno u otro.

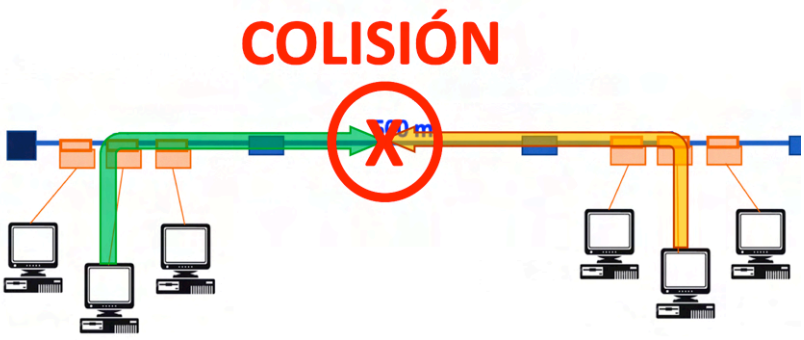
La diferencia más importante se encuentra en dos octetos del encabezado (que se tratarán a continuación). Cuando se trata de tramas **IEEE 802.3**, el encabezado MAC tendrá siempre encima de él el subnivel **LLC**, por esta razón no necesita definir a quién le debe entregar los datos, pues solo existe una opción (LLC); en esta situación los dos octetos referidos establecen la longitud del campo de datos y se llaman "**Length**". Cuando la trama es **Ethernet** (el nivel de enlace de OSI, no se encuentra subdividido) se debe aclarar a qué protocolo entregará los datos en el nivel 3 (Red), por ejemplo IPX, IP, etc. En este caso estos dos octetos se denominan "**Ethertype**", y se emplean justamente para definir qué tipo de protocolo se encuentra por arriba de Ethernet.

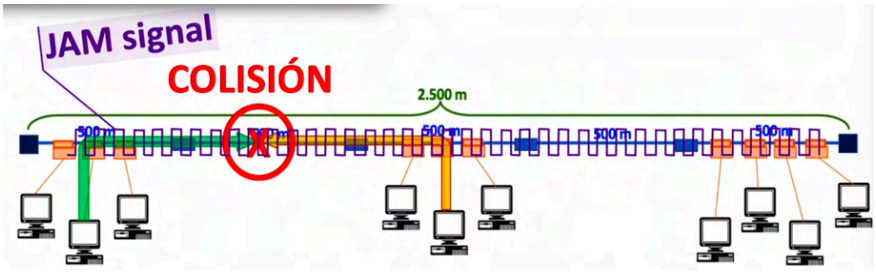
La forma de distinguir de qué trama se trata es mediante el valor en hexadecimal de estos dos octetos: todo valor inferior a **0550**h se corresponde a una trama IEEE-802.3; por encima de este se trata de una trama Ethernet.

¿Qué es **CSMA/CD** (Carrier sence multiple access/colition detect)?

El funcionamiento de una red LAN a nivel dos (enlace) que opere por medio de CSMA/CD, se implementa por medio del protocolo **Ethernet** u **802.3**. Su lógica es básicamente simple, si el canal está libre entonces se puede transmitir, caso contrario no. Como existe la posibilidad que un ETD escuche el canal y, al estar este libre comience la transmisión, antes de llegar esta señal a cualquiera de los otros ETD de la LAN alguno de estos haga lo mismo, es que se analizan las colisiones.

Una colisión se produce cuando dos ETD, por tener el canal libre, inician su transmisión, la cual no es otra cosa (en las primeras redes coaxial) que un estado de tensión que oscila entre +0,85Volt y -0,85 Volt (o ausencia de ella) que se propaga por canal físico. Al encontrarse dos señales dentro del mismo medio físico se produce una alteración en los niveles de tensión, la cual al llegar a cualquier ETD de la red se determina como una **colisión**.





Al producirse una colisión, el ETD que lo detecta, comienza a emitir una señal llamada "**JAM**" (o señal de atasco) para que todos se enteren que esto es sencillamente "ruido", y ninguno intente transmitir.

Los ETD que transmitieron pasan a un algoritmo de espera aleatorio (llamado disminución exponencial binaria), e intentan transmitir nuevamente al cumplirse el plazo determinado por el algoritmo (son múltiplos de este valor muy especial que se llama tiempo de ranura, del que hablamos la charla anterior), si durante 51,2 microsegundos (Tiempo de ranura) no se detecta ninguna colisión, este se ha APROPIADO del canal y se asegura que ningún otro ETD pueda transmitir, por lo cual continuará con el resto de su trama (tamaño máximo **1518 Byte**) y luego entrará nuevamente en compulsa por el medio físico.

Algoritmo de disminución exponencial binaria.

Como acabamos de ver, al producirse una colisión, los ETD responsables de la misma dejan de transmitir (y se envía la señal de atasco: JAM). Automáticamente estos dos equipos generan un número aleatorio entre 0 y 1. Este número es motivado por el algoritmo de disminución exponencial binaria que propone generar un número aleatorio acorde a la siguiente fórmula:

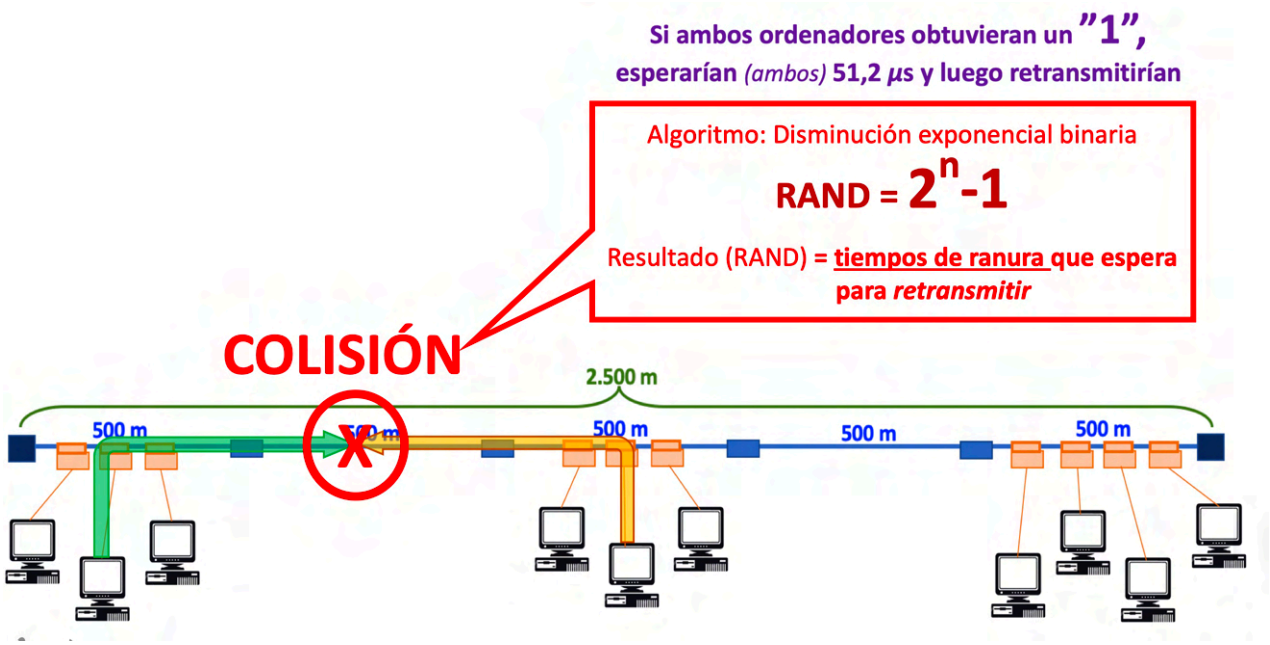
$$\text{Nº Rand} = 2^n - 1$$

n = cantidad de colisiones detectadas en esta compulsa.

Al tratarse de la primera colisión: Nº Rand=2^1-1 = 1 => (*Nro. Random entre 0 y 1*).

Este valor (0 ó 1) establece la cantidad de tiempos de ranura que esperará el ETD para volver a transmitir la trama que ocasionó la colisión, siendo el tiempo de ranura 51,2 µs.

Si los dos ETD generan el mismo valor, colisionarán nuevamente, pero si obtienen valores diferentes, uno de los dos emitirá primero, y cuando pasen los 51,2 µs del segundo ETD y este desee transmitir, encontrará el canal ocupado y no podrá hacerlo (es decir que el primero ganó la compulsa).



Si hubiesen generado el mismo valor, es decir: los 2 ETD =1, ó los 2 ETD = 0, se producirá la segunda colisión, por lo tanto:

Nro Rand = 2^2 -1 = 3 => (*Nro Random entre 0, 1, 2 ó 3*)

Si ambos equipos obtuvieran el mismo valor, colisionarían nuevamente y entonces sería:

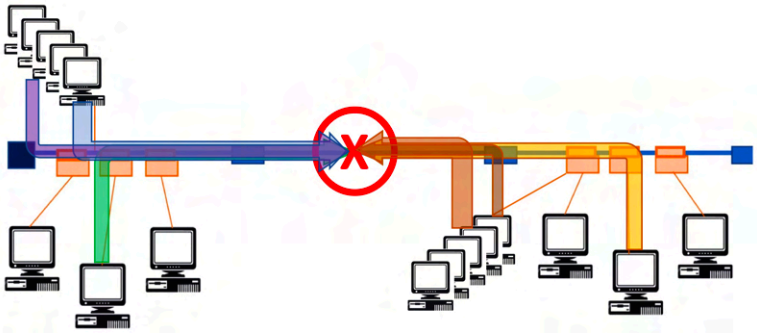
Nro Rand = 2^3 -1 = 8 => (*Nro Random entre 0, 1, 2, 3 ,4, 5, 6, 7 u 8*).

Si siguieran generando iguales números, esta situación se mantendría hasta:

Nro Rand = 2^{10} -1 = 1023 => (*Nro Random entre 0 y 1023*).

Si aún así esto continuara, se ejecutaría el mismo algoritmo con exponente = 10, durante seis veces más, y luego se comienza nuevamente.

Esto que parece muy poco probable, si bien es poco frecuente, no es tan así, pues se debe tener en cuenta que en una red donde existen varios ETD conectados a un mismo dominio de colisión, en cualquier momento de esta secuencia, puede entrar en juego otro ETD, caso en el cual, este último comenzaría a tratar el algoritmo como su primera colisión, y los anteriores seguirían con su rutina de disminución de probabilidades, y así también puede ingresar un cuarto, quinto, etc.



Un tema que os dejamos para la reflexión, pues es totalmente lógico de pensar es que, como acabamos de ver, en este cálculo de disminución exponencial binaria, cuando entran en colisión dos ETD, si ambos obtienen un valor idéntico, supongamos de 1 tiempo de ranura, y tienen que esperar ambos 51,2 µs, puede suceder que un tercer ETD en este lapso, escuche el canal vacío e inserte su trama en el canal. Si esto sucediera, se generaría una nueva colisión, o hasta inclusive se podría apropiar del canal este tercer ETD “colándose” ante los dos anteriores. O puede suceder, que estos tres colisionen, y supongamos que obtengan valores de 1 tiempo de ranura, y en ese lapso se cuele un cuarto ETD. Todo esto es real y se produce.

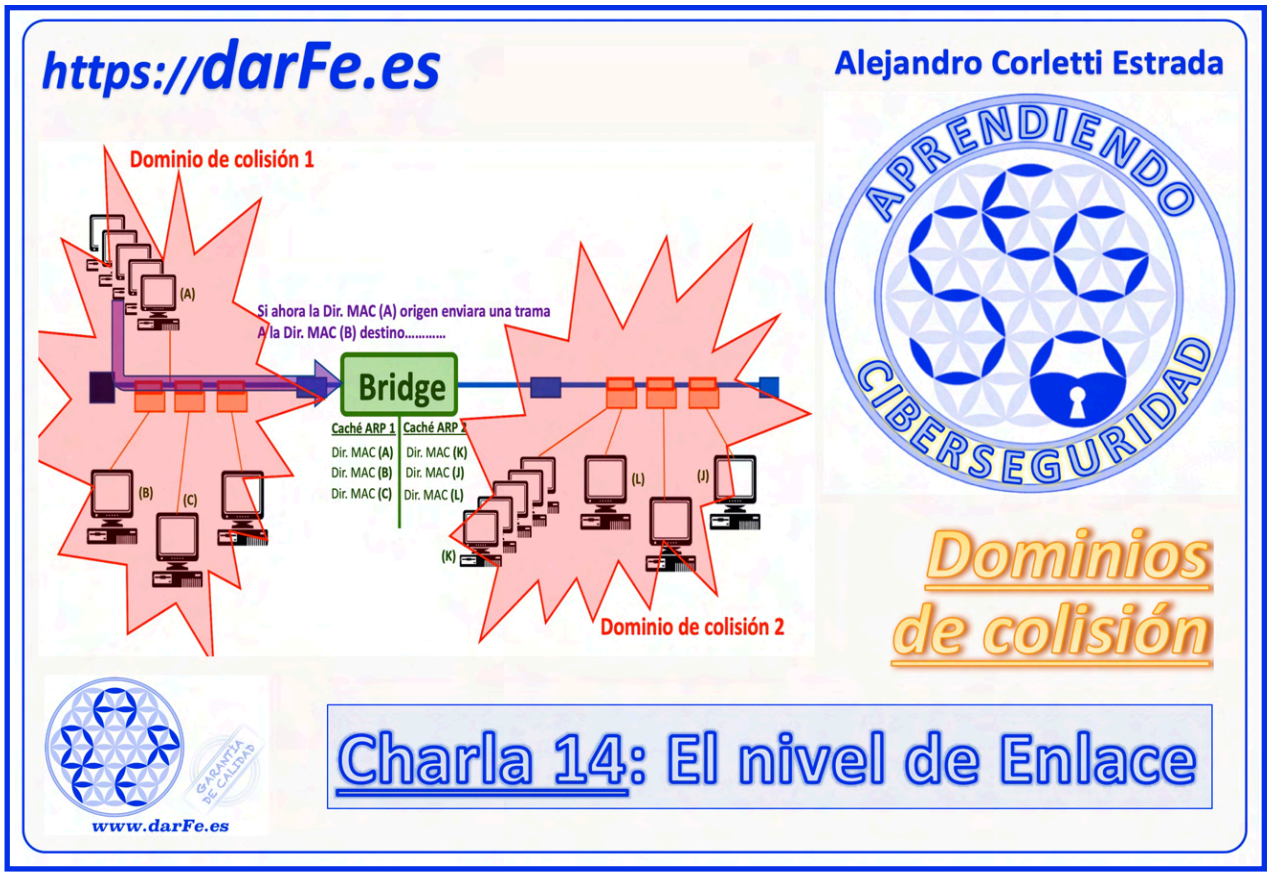
En estos casos cada ETD llevará su propio contador de colisiones (“n”), e irá generando sus propios números aleatorios de espera, peleando con dos, tres, cuatro o “x” cantidad de hosts que se le cuelen.

Volver al índice

www.darFe.es

Charla 14

Dominios de colisión



Enlace al Video:

Resumen:

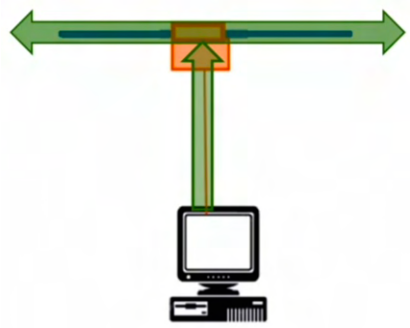
Ya hemos presentado el funcionamiento de CSMA/CD. Si hemos comprendido bien el mismo, no nos cabe duda que las colisiones son algo básico en este tipo de redes.

Si dos personas desean subir a un automóvil no hay ningún inconveniente, si son cinco, ya comienzan a estar apretados, si son más, pues: tenemos un problema.

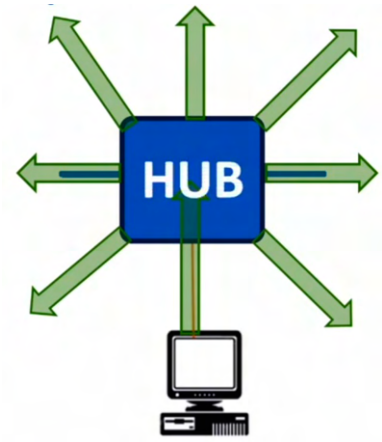
Las redes CSMA/CD, a medida que aumenta el número de ETD, las colisiones también empiezan a ser un problema. En este video desarrollaremos cómo se ha ido mejorando y solucionando el mismo por medio de lograd entender los "**dominios de colisión**".

Descripción detallada

Empezamos repitiendo esto de las colisiones, pues, como nos pudimos imaginar de la reflexión que planteamos al final de charla anterior, cuanto más crezca la red, naturalmente ira habiendo cada vez más colisiones, pues son más los ETD que están peleando por el mismo medio físico.



Hagamos un breve alto en el camino, para explicar en detalle, esto de los conectores "T" o BNC. Si un ETD genera tráfico desde el extremo de esta "T", al llegar la corriente eléctrica al centro de la "T", la señal sigue su camino hacia ambos extremos de la “T", de igual forma que cuando en mi casa empleo un enchufe triple y conecto dos lámparas al mismo, cuando lo enchufo se encienden ambas lámparas, pues la señal eléctrica cuando llegó a a esa "T" se propagó en todas las direcciones.



En algún momento de la historia de estas redes, a alguien se le ocurrió preguntarse entonces: ¿por qué en vez de "T" no empleo un dispositivo que en vez de bifurcar la señal por dos bocas, lo pueda hacer por 8, 16, 24, 48, etc?... y así nacieron los dispositivos denominados **Hub.**

El Hub, que duró pocos años, por lo que seguiremos explicando a continuación, fue un dispositivo fundamental, pues dio origen a las arquitecturas de redes **Estrella** y/o **jerárquica** para las redes Ethernet, que hasta el momento solo podían ser del tipo **Bus**. Es decir, marca un hito importante en el concepto de arquitectura de redes.

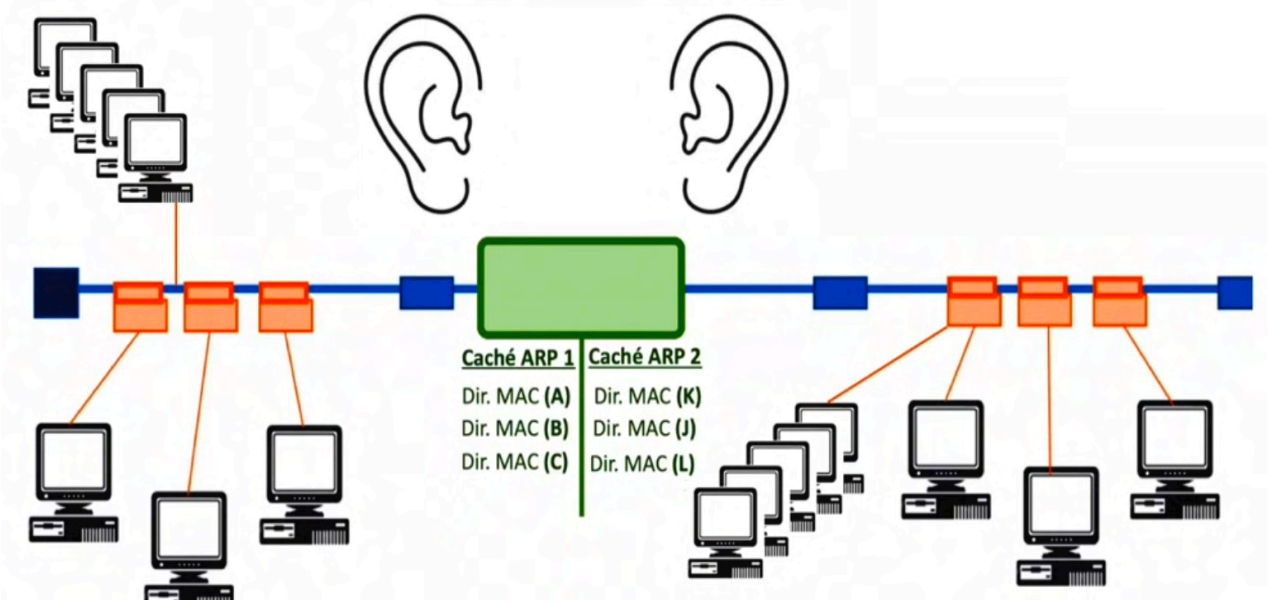
Historia de los Switch.

Como acabamos de comentar, la vida de los Hubs, fue muy breve, pues el problema de las colisiones, en las cada vez más populares redes Ethernet, hacía que estas redes pierdan muchísima eficiencia al sumar, por ejemplo, más de cien ETD en la misma, pues cada vez había más equipos peleando por el medio.

La primera solución, llegó de la mano de lo que se llamó “**Bridge**” (o puente). Este dispositivo, se pensó con el concepto de “**memoria caché ARP**” (por Address Resolution Protocol). Este protocolo que se trata en detalle en la charla 17, por ahora nos basta con mencionar, que sirve para asociar una dirección “**MAC**” con una dirección “**IP**” (ambos temas que también se desarrollarán en las siguientes charlas).

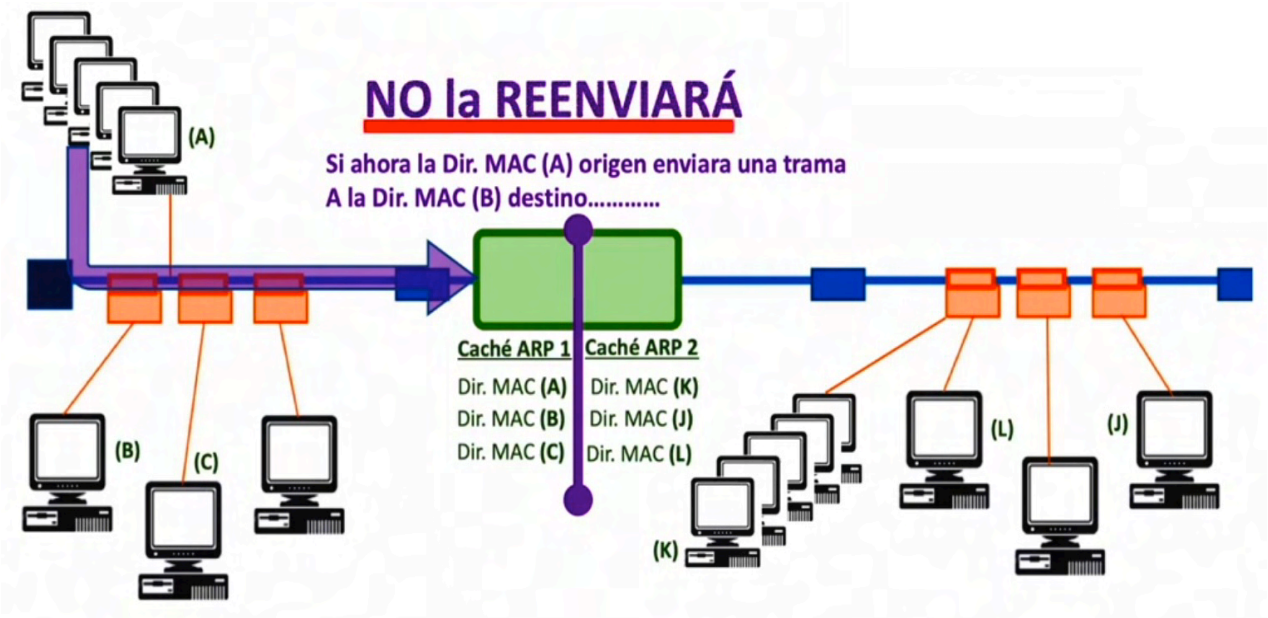
Al querer transmitir un ETD y meter información en la red, uno de los campos que inyecta en la misma, es su propia dirección de este nivel de enlace, que como veremos más adelante, se suele llamar dirección MAC. La gran idea de un Bridge, es colocarlo entre medio de cualquiera de estos cables coaxiales, e imaginemos que tiene una oreja en cada extremo del mismo, es decir por un lado, excucha el tráfico que le llega de la izquierda, y por el otro, el de la derecha. A medida que va escuchando las direcciones MAC que le llegan de cada lado, las va almacenando en su respectiva “**caché ARP**” (una para la interfaz derecha y otra para la interfaz izquierda). Al principio, cuando aún

no tiene almacenada suficiente información en sus caché ARP, al recibir cualquier trama Ethernet, pues no le queda otra opción que reenviarla por la otra interfaz.



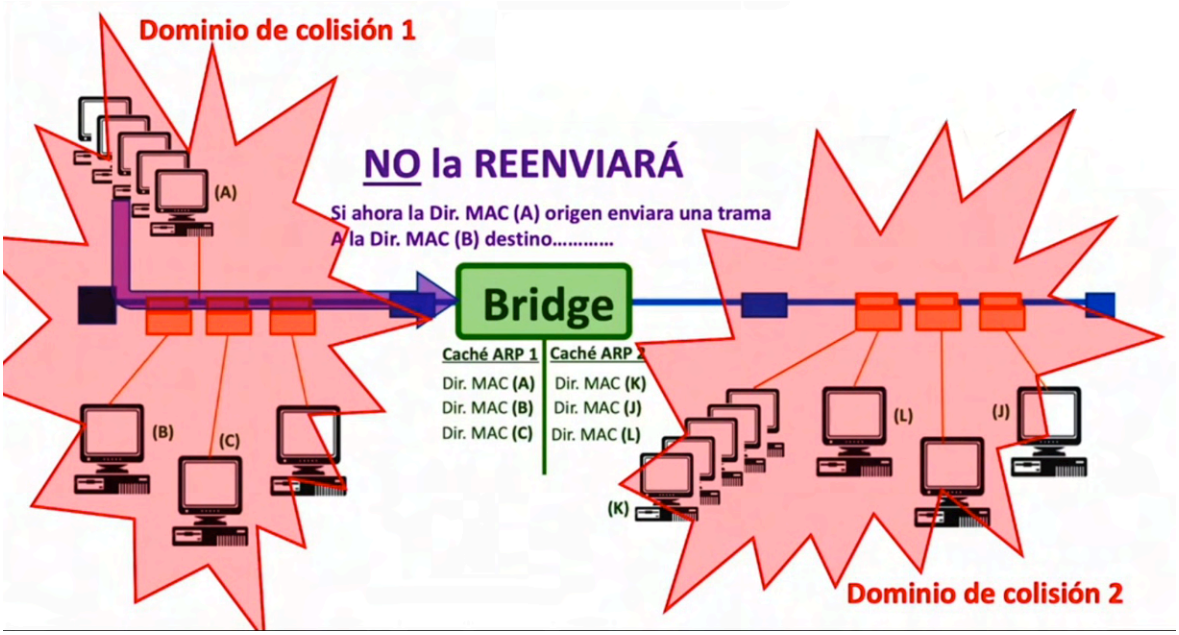
Pero a medida que va almacenando en sus memorias ARP las debidas "tablas de direcciones MAC" (esta etapa se llama aprendizaje), llegará un momento que si le llega por la izquierda una trama que va dirigida a otra MAC que justamente, también está a la izquierda, entonces ¿para qué la va a reenviar por la derecha?, si ambas están en el lado izquierdo. Lo mismo si recibe una trama por la derecha que va dirigida a otra MAC que también está en la derecha, entonces ¿para qué la va a reenviar por la izquierda?

Fijaros que cada vez que un ETD de la derecha desee comunicarse con otro de la derecha, simultáneamente, uno de la izquierda podría estar comunicándose con otro de la izquierda, con ello hemos optimizado el tráfico al doble de su capacidad, separando nuestra red LAN en **dos dominios de colisión.**



El nacimiento de los Bridges, permite por primera vez optimizar el tráfico de las redes LAN, mejorando su rendimiento substancialmente, por medio de separarlas en

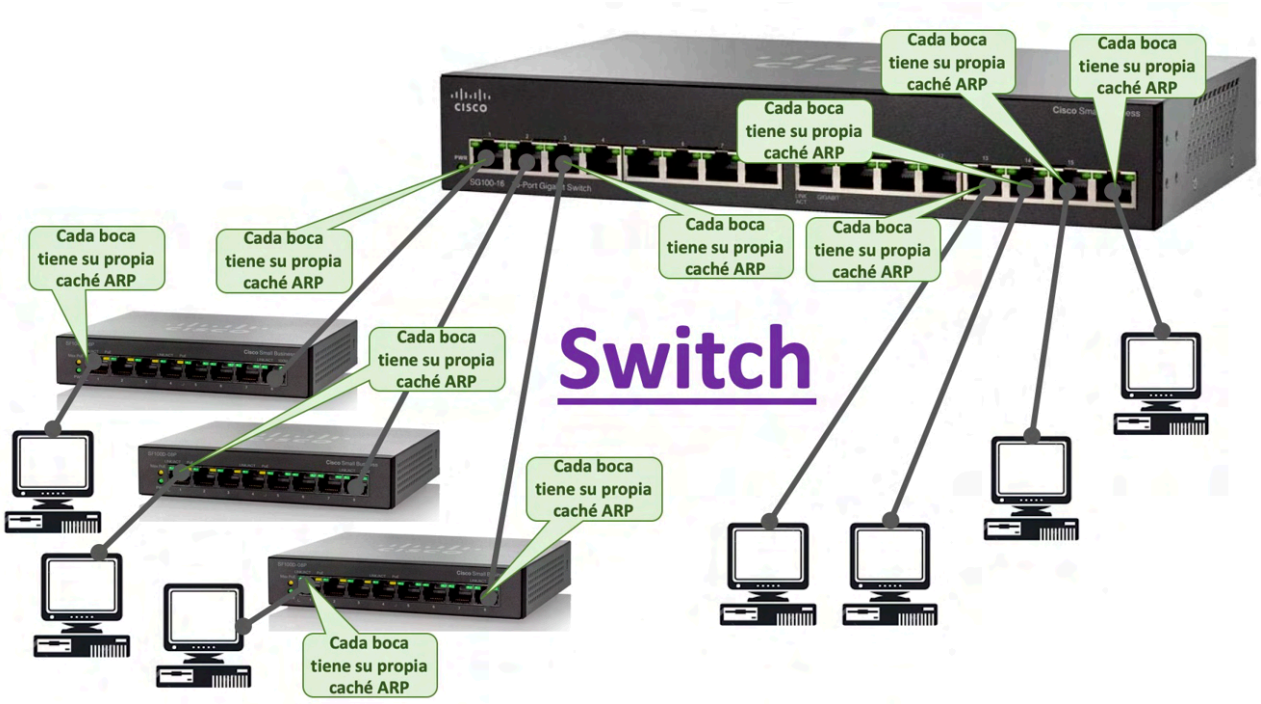
diferentes dominios de colisión. Es decir, cada lado del mismo se peleará entre sí, de forma independiente.



Por supuesto, que cuando un ETD de un lado, desea comunicarse con uno del otro lado, entonces el problema continua. Pero ahora que la idea ya estaba sembrada, fijaros que es natural plantearse:

¿Qué sucedería si en vez de tener dos bocas y dos memorias caché ARP, tuviera "x" bocas y "x" memorias ARP?

Si hemos seguido esta lógica hasta aquí, comprenderemos perfectamente como funciona un "**Switch**".



Un **switch**, es un dispositivo que tiene varias bocas y en cada una de ellas su propia memoria caché ARP, por lo tanto a medida que va aprendiendo qué direcciones MAC

tiene en cada una de ellas, puede establecer comunicaciones "**punto a punto**" entre las mismas, y con ello, tener tantos dominios de colisión, como bocas posea.

Con los switchs, que son los dispositivos por excelencia hoy en día en el nivel de enlace, se pueden armar verdaderas arquitecturas de red de miles de ETD, con unos niveles de segregación y eficiencia óptimos, llegando a velocidades de cientos de gigabits por segundo, y reduciendo las colisiones al mínimo.

www.darFe.es

Charla 15

Formato de la trama Ethernet

Enlace al Video:

Resumen:

A nivel 2, se suele emplear la palabra “**trama**” para definir el encabezado y datos que viajan en el mismo. El **encabezado** (o Header) de un protocolo, define todo lo que hace o no hace el mismo, por esa razón es fundamental comprender los campos que lo componen y para qué sirve cada uno de ellos.

En esta charla, desarrollamos lo que indica la norma **IEEE-802.3**, y la comparamos con la realidad, por medio del análisis de una captura de tráfico real de tramas **Ethernet**.

Descripción detallada

Esta charla, toma como referencia el capítulo 4 de nuestro libro "**Seguridad por Niveles**". Que, como se puede apreciar en la imagen que sigue, en la página 78 del mismo, se presenta con todo detalle el formato de este encabezado.

CHARLA 12: El nivel de enlace – Funcionamiento de Ethernet (IEEE 8082.3)

DarFE Learning Consulting, S.L.

Seguridad por Niveles

4.1. Análisis de tramas Ethernet (IEEE 802.3):

El funcionamiento de una red LAN a nivel dos (enlace) que opere por medio de CSMA/CD (Carrier Sence Multiple Access/Colition Detect) se implementa por medio del protocolo Ethernet u 802.3 (la mínima diferencia entre ellas se verá en breve). Su funcionamiento es básicamente simple, si el canal está libre entonces se puede transmitir, caso contrario no. Como existe la posibilidad que un ETD escuche el canal, al estar éste libre comience la transmisión, y antes de llegar esta señal a cualquiera de los otros ETD de la LAN alguno de estos haga lo mismo, es que se analizan las colisiones. Una colisión se produce cuando dos ETD por tener el canal libre inician su transmisión, la cual no es otra cosa que un estado de tensión que oscila entre + 0,85Volt y - 0,85 Volt (o ausencia de ella) que se propaga por canal físico, al encontrarse dos señales dentro del mismo medio físico se produce una alteración en los niveles de tensión, la cual al llegar a cualquier ETD de la red se determina como una colisión. Los ETD que transmitieron pasan a un algoritmo de espera aleatorio (llamado disminución exponencial binaria) e intentan transmitir nuevamente al cumplirse el plazo determinado por el algoritmo (son múltiplos de un valor muy especial que se llama tiempo de ranura), si durante 51,2 microsegundos (tiempo de ranura) no se detecta ninguna colisión, éste se ha APROPIADO del canal y se asegura que ningún otro ETD pueda transmitir, por lo cual continuará con el resto de su trama (tamaño máximo 1518 Byte) y luego entrará nuevamente en compulsa por el medio físico.

4.1.1. Formato de las direcciones MAC (Medium Access Control).

Las Direcciones MAC son reguladas por IEEE y están formadas por 6 octetos, representados como pares de números hexadecimales (hh-hh-hh-hh-hh-hh).

Los primeros tres octetos identifican al fabricante de la tarjeta. Estos tres octetos son asignados por un grupo de IEEE llamado **RAC** (Registration Authority Commitee) y pueden ser consultados en http://www.ieee.org/index.html. Existe una metodología para solicitarlos y por ser 24 bit, se pueden asignar en el orden de 16.000.000 de valores. Estos tres primeros octetos se les denomina **"OUI"** (Organizationally Unique Identifier) o **"company_id"**, de estos 3 Byte, los dos primeros bit tienen un significado especial:

- **bit 0**: Individual (valor = 0), establece que este valor pertenece a una sola dirección MAC. Grupal (Valor = 1), forma parte de un conjunto de direcciones MAC.
- **bit 1**: Universal (valor = 0), define que esta dirección es única en el mundo. Local (valor = 1) tiene significado solamente en el ámbito local.

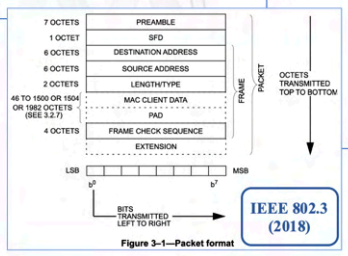
Estos primeros 3 octetos, una vez asignados a una determinada empresa, se deja a criterio de la misma cómo asignará los valores de los 3 octetos siguientes denominados **"Extension identifier"**, para que no puedan repetirse, pero IEEE-RAC no se responsabiliza ni establece ninguna pauta sobre los mismos. Es lógico pensar que un gran fabricante de tarjetas, complete la totalidad de los posibles números a emitir; IEEE-RAC establece que recién al haber completado el 90 % de las asignaciones, podrá solicitar otro OUI para continuar fabricando (en la actualidad ya existen varias empresas en esta situación).

Alejandro Corletti Estrada Página 78 www.DarFE.es

La concatenación de **"OUI" + Extension identifier = "EUI" (Extended Unique Identifier,** conocido como **"EUI-48"**, que es la verdadera denominación teórica de una dirección MAC.

Ejemplo de Representación gráfica de una EUI-48

OUI (company_id)			Extension Identifier		
Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5
AC	DE	48	23	45	67
10101100	11011110	01001000	00100011	01000101	01100111
▲ bit más significativo					▲ bit menos significativo



Como ya hemos mencionado, quien estandariza todo este nivel es **IEEE**, a través de su subcomité **802.x.** Por ello, para descargar cualquiera de estas normas, podemos hacerlo desde:

https://ieee802.org/

IEEE 802.3

Las tramas Ethernet son armadas en el subnivel MAC y responden a **14 octetos de encabezado** y a **4 octetos de cola** que es donde se realiza el **CRC** (Control de Redundancia Cíclica), y entre estos campos van los datos.

Se debe tener en cuenta que para que todos los ETD de la red se sincronicen y sepan que se está por recibir una trama, antes de la misma se envían 7 octetos de **preámbulo** (**10101010**) y luego un octeto de **inicio** (**10101011**). Algunos autores lo consideran parte del encabezado Ethernet y otros no, en este texto no se considerarán parte del mismo.

El formato de una trama Ethernet, es el que se puede apreciar en la imagen inicial, y está compuesto por:

- Dirección destino: Especifica la dirección del host a alcanzar a nivel MAC.
- Dirección origen: Especifica la propia dirección a nivel MAC.

  Las direcciones origen y destino están reguladas en la norma IEEE-802.3 y compuestas por seis octetos, que habitualmente se representan en formato hexadecimal (numeración que explicaremos en detalle unas charlas más adelante) y se las denominó **OUI-48**, como se aprecia en la imagen que sigue.

La concatenación de **"OUI" + Extension identifier = "EUI" (Extended Unique Identifier,** conocido como "**EUI-48**", que es la verdadera denominación teórica de una dirección MAC.

Ejemplo de Representación gráfica de una EUI-48					
OUI (company_id)			**Extension Identifier**		
Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5
AC	DE	48	23	45	67
10101100	11011110	01001000	00100011	01000101	01100111
▲ bit más significativo					▲ bit menos significativo

- Tipo o longitud: Si se trata del protocolo Ethernet, el tipo de protocolo de nivel superior (Ethertype). Si es protocolo 802.3, especifica la longitud del campo de datos (Length)
- CRC: Control de redundancia cíclica, emplea el concepto de polinomio generador como divisor de la totalidad de la trama, el resto de esta operación se enmascara con una secuencia determinada de bit y se envía en este campo. Se trata entonces de una división binaria, en la cual se emplea como polinomio generador justamente el CRC-32, que figura abajo, por lo tanto el resto de esta división SIEMPRE será una secuencia de bit de longitud inferior a 32 bits, que será lo que se incluye en este campo. Los formatos estandarizados de estos CRCs son los que se presentan a continuación:

  CRC-12: $X^{12} + X^{11} + X^3 + X^2 + X + 1$

  CRC-16: $X^{16} + X^{15} + X^2 + 1$

  CRC CCITT V41: $X^{16} + X^{12} + X^5 + 1$

  CRC-32 (Ethernet): = $X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$

  CRC ARPA: $X^{24} + X^{23} + X^{17} + X^{16} + X^{15} + X^{13} + X^{11} + X^{10} + X^9 + X^8 + X^5 + X^3 + 1$

  El tema de CRC, lo desarrollamos en detalle en la charla siguiente.
- Preámbulo: No está representado en la gráfica anterior, pues no es considerado como parte de la trama, pero se trata de 7 byte que indican que comienza una trama y permite sincronizar relojes y 1 Byte de inicio.

Como también se aprecia en la primera imagen, a continuación del campo Tipo o longitud, y antes del CRC, va insertado el campo de datos. Un detalle a considerar sobre este campo, es que NO puede ser menor a 46 Bytes, ni mayor a 1.500 bytes. No puede ser menor a 46 bytes, pues si le sumamos los 15 del encabezado y los 4 de

CRC, veremos que son 64 bytes, y si recordamos lo tratado sobre el tiempo de ranura, recordad que es el la duración mínima de una trama Ethernet, pues a partir de esta cantidad de Bytes, que en las primeras redes eran exactamente **51,2 µs** y es el tiempo en el que un ETD se apropió del canal, cualquier otro ETD, si hiciera **Carrier Sense**, encontraría el canal ocupado y no podría iniciar su transmisión.

El valor máximo de 1.500 bytes, también tiene su explicación para evitar "**monopolios**" del canal, es decir, para que un ETD que tenga que transmitir mucha más información, al finalizar estos 1.500 bytes, deba competir nuevamente por el mismo.

Otro tema que nos interesa detenernos es el "**preámbulo**", que acabamos de mencionar. Recordemos que estas redes, nacieron en los años 70, y aunque parezca mentira luego de más de cincuenta años, siguen siendo la mejor solución en entornos LAN. Hoy en día, es muy frecuente, encontrarnos en cualquier empresa, ordenadores, nuevos, conviviendo con otros que pueden llegar a tener veinte años, o más.

Como es fácil de imaginar, no es lo mismo el procesador de un ordenador de este año, que el de hace veinte. En particular, una de las mayores diferencias está en su velocidad de procesamiento, la cual está regulada por su "**clock**" (o reloj). Cuánta mayor velocidad tenga este clock, mayor cantidad de ciclos por segundos genera.

Una tarjeta de red, también se rige por su clock, y los ciclos por segundo que genere, son los que darán como resultado la duración de ese pulso que inyecta en la red LAN.

Lo que intentamos explicar aquí, es que un ordenador de hace 20 años, posiblemente emplee 2, 4 u 8 ciclos de reloj para generar un pulso (que para nosotros será un 1 o un 0 si lo capturamos en la red). Sin embargo un ordenador 20 años más moderno, posiblemente ese mismo pulso le ocupe miles de ciclos de reloj, pues su velocidad es inmensamente mayor.

En resumen y para no extendernos más, cada ordenador de esa red LAN que está escuchando, sea del año que fuere, necesita determinar con la mayor precisión posible, dónde inicia y finaliza cada pulso que generó el ETD que está emitiendo.

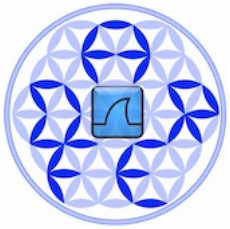
Para esta función, es que justamente se genera el preámbulo siempre, antes del encabezado Ethernet, y justamente como podéis ver abajo, en el punto 4.2.5 de esta norma IEEE-802.3, lo define claramente:

10101010 10101010 10101010 10101010 10101010 10101010 10101010 (7 octetos)

Como podéis apreciar, justamente son unos y ceros alternados, para que cada ETD que escuche tenga este referencia para saber cuantos ciclos de su propio reloj comprende cada pulso.

Para finalizar este tema, debemos aclarar que al final de este preámbulo, como se puede ver en el punto 4.2.8 de esta norma, sigue un último octeto o Byte de inicio, que sencillamente es 10101010**11**, para que con el "**11**" final, deje indicado que a partir de ese "11" comienza el verdadero encabezado Ethernet.

En nuestra web, seleccionando el menú "**Descargas**", tenéis un apartado específico para las "**capturas de Tráfico**"



Para comprender con más detalle, el formato de Ethernet, te recomendamos que descargues la siguiente capturas de tráfico:

Captura_Ejemplo_Ethernet.pcap

Empezaremos a trabajar con la misma desde nuestra herramienta “**Wireshark**”.

Para profundizar en el empleo de **Wireshark**, recomendamos el ciclo de “**Análisis de tráfico**” de nuestro canal Youtube:

En la presente charla (en el video), se explica brevemente el empleo de Wireshark, en este caso, concretamente aplicado al nivel de enlace para comprender de forma práctica cómo es este encabezado de Ethernet. Para ello, a continuación trabajaremos con la captura de tráfico: “**Captura_Ejemplo_Ethernet.pcap**” que acabamos de referenciar.

Para poder verificar la teoría con la práctica, nos interesa ser capaces de detectar tráfico **Unicast**, **Multicast** y **Broadcast** a nivel dos, es decir poder analizar el esquema de direccionamiento MAC y comprender bien sus 6 octetos presentados en forma hexadecimal, teniendo en cuenta los dos bits menos significativos del primer octeto, tal cual se explicará a continuación. Para ello lanzaremos el analizador de protocolos **Wireshark** y abrimos la "**Captura_Ejemplo_Ethernet.pcap**". El ejercicio que haremos, consiste en evaluar lo que se explica en cada trama y compararlo con esta captura.

Vamos a presentar de forma práctica los tipos de comunicación, que pueden ser:

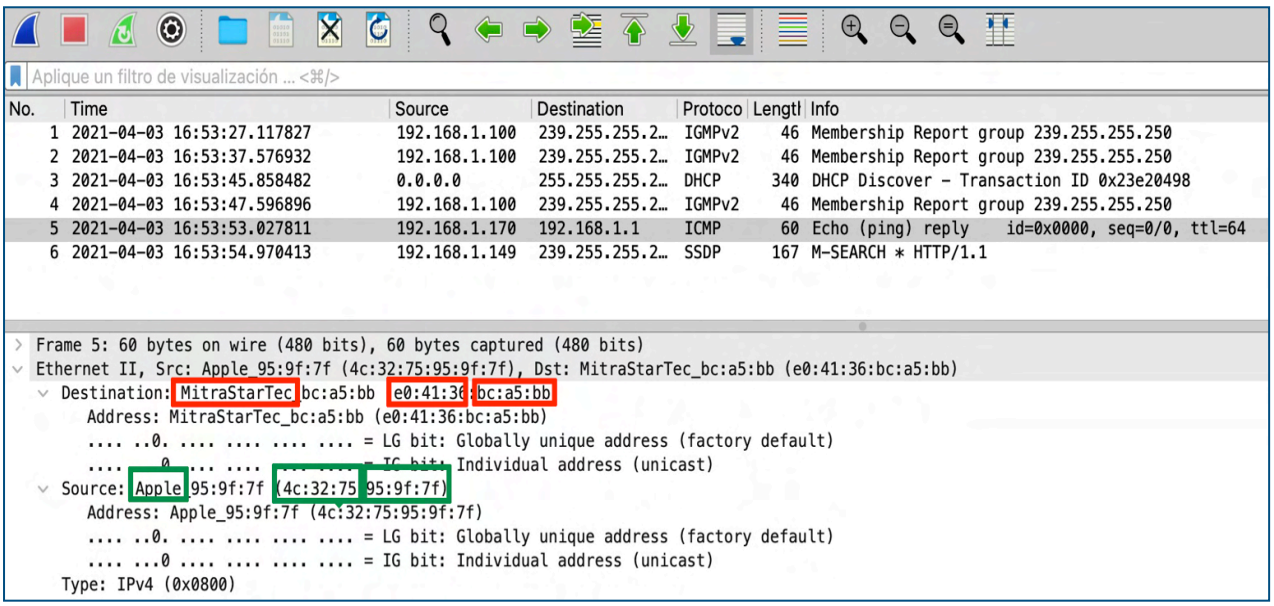
Las comunicaciones en una red pueden ser:

- **Unicast:** de uno a uno.
- **Multicast:** de uno a varios.
- **Broadcast:** de uno a todos.

A continuación desarrollamos los tres tipos de “**tramas Ethernet**” según su tipo de comunicación.

Trama Unicast: Analicemos la trama seis de esta captura de tráfico. En la imagen siguiente a este párrafo (o en la captura que os habéis descargado: **Captura_Ejemplo_Ethernet.pcap**), prestad atención a los bits menos significativos del primer octeto de la dirección destino, los mismos se encuentran con **valor** “**0**” por ser **Unicast**. Se puede ver claramente que los 6 octetos de la dirección origen y destino son pares de valores “hexadecimales” y se corresponden a lo mencionado en la teoría como el formato “**EUI-48**”. Fijaros que, como el analizador de protocolos tiene dentro de sus librerías el listado de todos los fabricantes en esa fecha, inmediatamente pudo

identificar los 3 primeros octetos de la dirección destino (**e0:41:36**) y nos la presenta como "**MitraStarTec**", luego esta sería la tarjeta número: **bc:a5:bb** que fabricó esta empresa. Estos tres primeros octetos los vimos como: "**OUI**" (Organizationally Unique Identifier) o "company_id" en la imagen de la norma, unos párrafos antes. Sucede lo mismo con la dirección origen (Source Address), que esta imagen se corresponde a: **4c:32:75:95:9f:7f** que Wireshark las reconoce como "Apple: **4c:32:75**" y esta es la tarjeta número **95:9f:7f**, que ha impreso este fabricante.



Trama Multicast: Vamos a analizar la trama número uno de esta captura. En esta trama, prestad atención al empleo del primer bit menos significativo del primer octeto con valor ".... ...1". Esto como podemos ver en la Figura 3-3 de la norma IEEE-802.3 (a nuestra derecha) lo describe como: **Grupal** (I/G = 1 GTRPUO ADDRESS). En este caso, el conjunto de direcciones es un mensaje dirigido a un "grupo de dispositivos". Lo primero que deseamos remarcar, es que Wireshark al detectar que este bit que acabamos de mencionar está en "1", automáticamente nos presenta que se trata de una trama "**IPv4mcast**". Luego, y como detalle interesante para observar, es que la **dirección IP destino** (nivel de red) es **239.255.255.250** lo que identifica un Multicast también a nivel de red (nivel 3), y fijaros cómo este mismo valor se "copia" en los tres últimos octetos de la dirección MAC destino pero en formato hexadecimal (**7f:ff:fa**:)…….. ¿Qué raro no?... ¿por qué será?…, es un tema que lo trataremos con detalle al llegar al nivel 3, pero nos pareció importante que prestéis atención a estos pequeños detalles desde el principio.

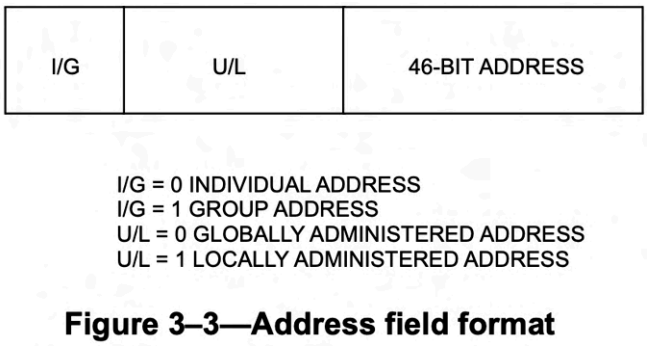
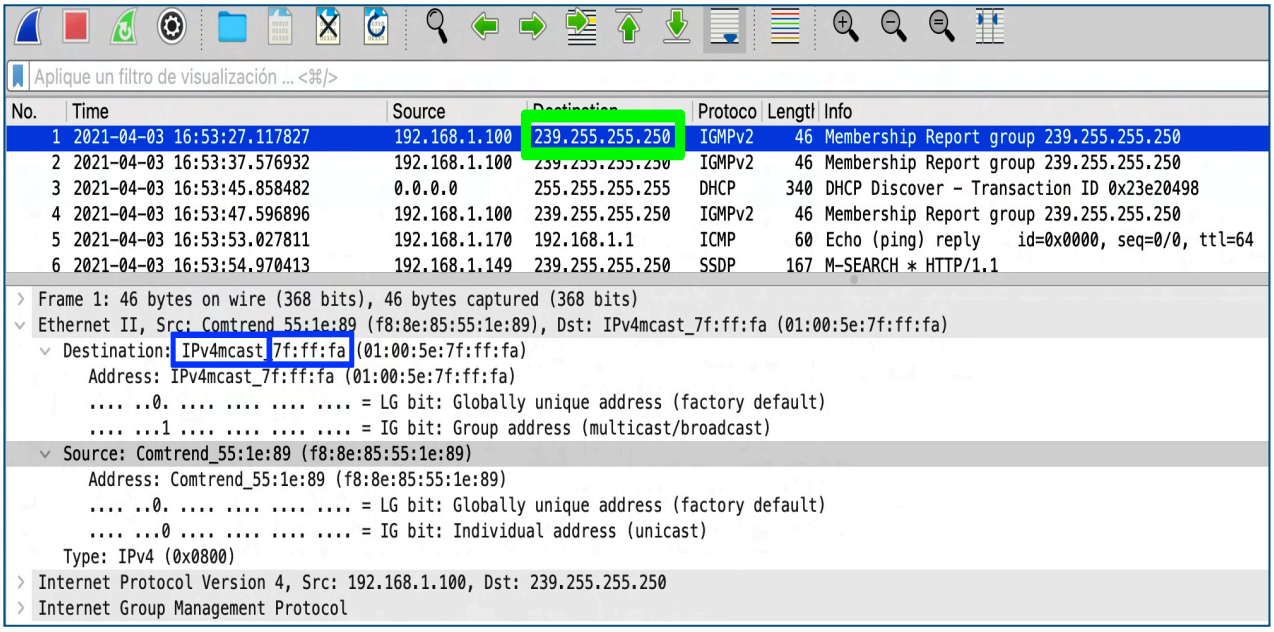


Figure 3–3—Address field format

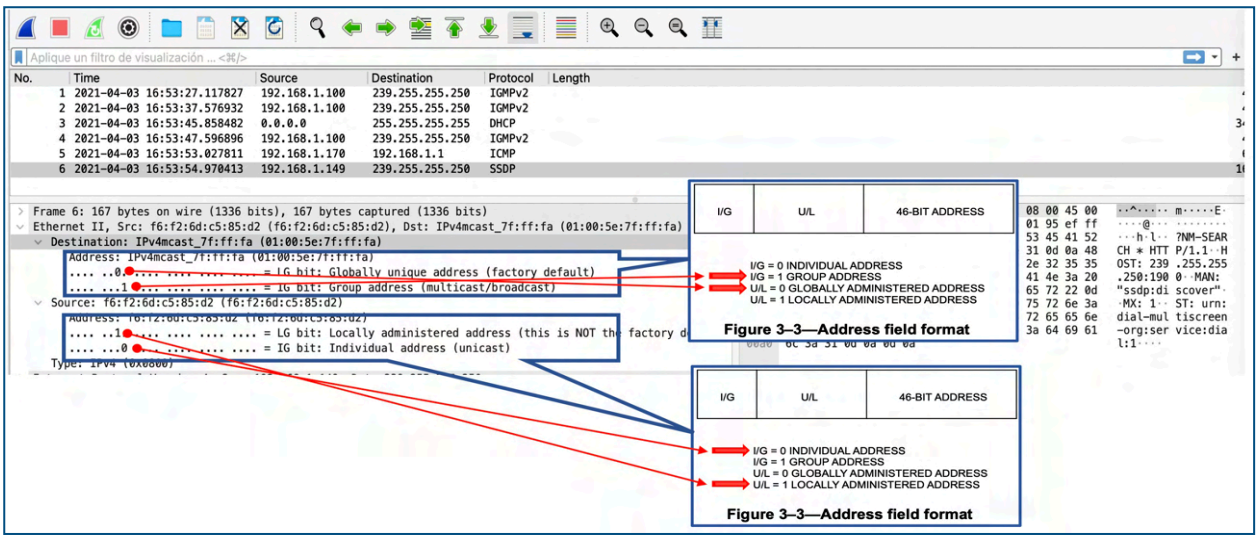


Trama Broadcast: Estas tramas se identifican claramente por su dirección destino: **ff:ff:ff:ff:ff:ff**. El valor "**ff**" en hexadecimal, se corresponde con: "**1111 1111**" en binario y con: "**255**" en decimal, y será una constante en los esquemas de direccionamiento Broadcast. En esta trama, lo que debéis notar es cómo ahora los dos bits menos significativos del primer octeto están puestos en "**1**", pues ahora, continuando con nuestra teoría: el primero de ellos identifica: **Grupal** (Valor = 1), forma parte de un conjunto de direcciones MAC, y el segundo: **Local** (valor = 1), tiene significado solamente en el ámbito local.

Sobre este tipo de trama Broadcast, lo tenéis también en la trama número 3 de esta captura que venimos analizando, pero os invitamos que intentéis lanzar capturas de tráfico con **Wireshark**, buscando justamente este patrón en las direcciones destino Ethernet, veréis que es muy sencillo de encontrar.

Os reiteramos que para comprender Wireshark y ejercitar con las capturas de tráfico, sigáis el ciclo de "**Análisis de tráfico**" de nuestro canal Youtube:

A continuación, presentamos finalmente la captura, describiendo cada uno de estos bits, de acuerdo a lo que nos indica la norma IEEE-802.3.



En el punto 4.1.1 del capítulo 4 de nuestro libro "**Seguridad por Niveles**". Que, como se puede apreciar en la imagen que sigue, en la página 78 del mismo se presenta con todo detalle el formato de este encabezado

4.1.1. Formato de las direcciones MAC (Medium Access Control).

Las Direcciones MAC son reguladas por IEEE y están formadas por 6 octetos, representados como pares de números hexadecimales (hh-hh-hh-hh-hh-hh).

Los primeros tres octetos identifican al fabricante de la tarjeta. Estos tres octetos son asignados por un grupo de IEEE llamado **RAC** (Registration Authority Commitee) y pueden ser consultados en http://www.ieee.org/index.html. Existe una metodología para solicitarlos y por ser 24 bit, se pueden asignar en el orden de 16.000.000 de valores. Estos tres primeros octetos se les denomina "**OUI**" (Organizationally Unique Identifier) o "**company_id**", de estos 3 Byte, los dos primeros bit tienen un significado especial:

- **bit 0**: Individual (valor = 0), establece que este valor pertenece a una sola dirección MAC. Grupal (Valor = 1), forma parte de un conjunto de direcciones MAC.
- **bit 1**: Universal (valor = 0), define que esta dirección es única en el mundo. Local (valor = 1) tiene significado solamente en el ámbito local.

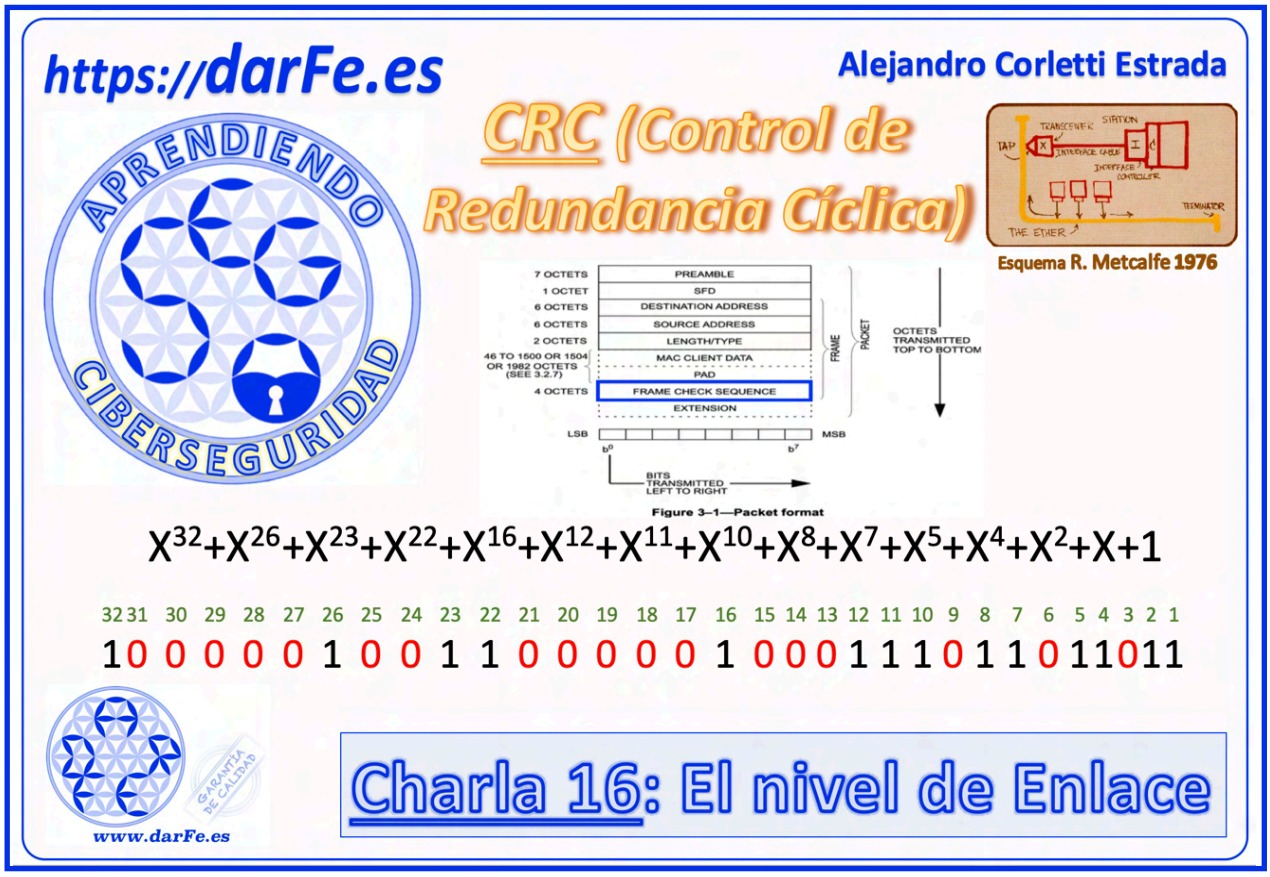
Estos primeros 3 octetos, una vez asignados a una determinada empresa, se deja a criterio de la misma cómo asignará los valores de los 3 octetos siguientes denominados "**Extension identifier**", para que no puedan repetirse, pero IEEE-RAC no se responsabiliza ni establece ninguna pauta sobre los mismos. Es lógico pensar que un gran fabricante de tarjetas, complete la totalidad de los posibles números a emitir; IEEE-RAC establece que recién al haber completado el 90 % de las asignaciones, podrá solicitar otro OUI para continuar fabricando (en la actualidad ya existen varias empresas en esta situación).

Volver al índice

www.darFe.es

Charla 16

Control de redundancia Cíclica



Enlace al Video:

Resumen:

Esta charla, desarrolla con todo detalle este tema de **CRC** (Control de Redundancia Cíclica). Comenzamos explicando el concepto de "**polinomio generador**", que no es otro que el que establece IEEE-802.3 como **CRC-32**. Describimos con todo detalle su funcionamiento y el por qué de elegir este y no otro (**Distancia Hamming**). Presentamos luego los conceptos de división binaria con ejemplos muy claros, y para cerrar, desarrollamos las técnicas **BEC** (Backward Error Control) y **FEC** (Forward Error Control).

Descripción detallada

En esta charla de hoy, seguimos con el estándar **IEEE-802.3**, que recordad lo podéis descargar en:

https://ieee802.org/

Ya hemos presentado brevemente el tema en la charla anterior, cuando vimos el formato de la trama Ethernet, ahora profundaremos con más detalle sobre el funcionamiento de este campo.

En la norma I**EEE-802.3** se denomina a estos cuatro octetos como "**Frame Check Sequence**", como podemos verlo en la imagen de la derecha, pero su función se denomina "**Control de Redundancia Cíclica**" (CRC).

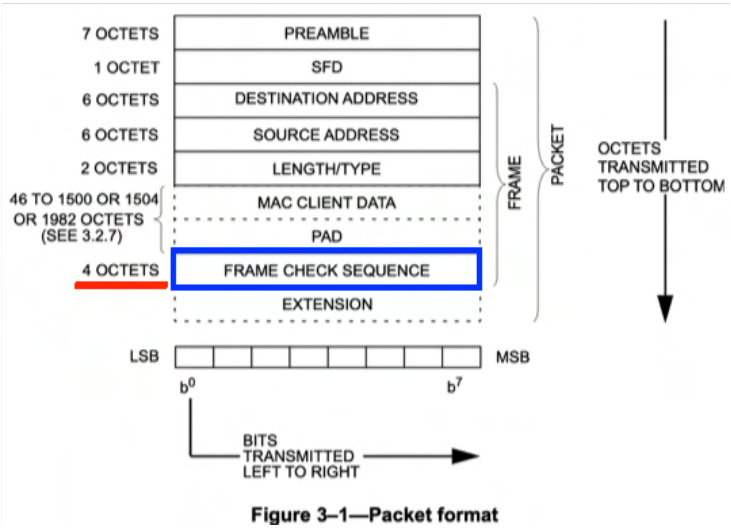
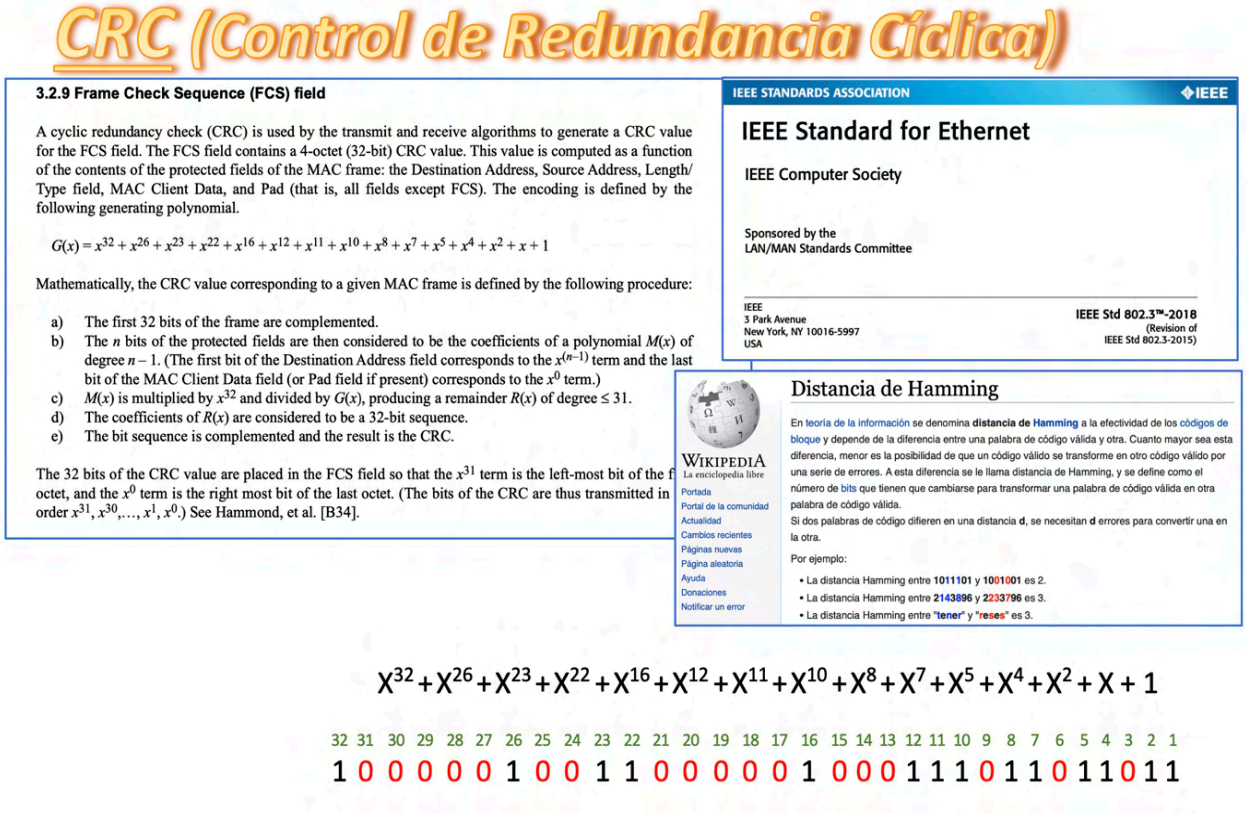


Figure 3–1—Packet format

En la primera imagen que se presenta en el video de esta **Charla 16.** (abajo), el punto 3.2.9 de la mencionada norma, es el que desarrolla este campo, y lo iremos desarrollando a lo largo de este capítulo.



Al final de la imagen anterior, podemos apreciar cómo es el formato de este "**polinomio generador**" de grado 32; esto quiere decir que está compuesto por 32 términos, los cuáles vamos a ampliarlos para mejor comprensión y estudio:

$$X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^{8}+X^{7}+X^{5}+X^{4}+X^{2}+X+1$$

32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
1	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	1	0	0	0	1	1	1	0	1	1	0	1	1	0	1	1

Básicamente, un polinomio binario de grado 32, indica que si el término existe, pues vale 1, y caso contrario vale cero, como podemos ver en **rojo** y **negro** en la imagen anterior.

El primer concepto que debemos considerar, es que se trata de un "grado 32" porque, como acabamos de ver, este campo tiene 4 octetos, lo que implica que 4 x8 = 32 bits.

La segunda idea que no podemos dejar pasar es ¿por que exactamente este polinomio CRC-32, y no cualquier otra combinación de treinta y dos unos y ceros. Para que entendamos la respuesta, tenemos que presentar el concepto de "**Distancia Hamming**".

Tal cual podemos ver en la imagen de abajo, "**Wikipedia**" nos la define como:

"la diferencia entre una palabra de código válida, y otra".

En la parte inferior de la imagen, podemos ver tres ejemplos en **azul**, **rojo** y **negro**, de cuál es la distancia en tres tipos de ellos, un código binario, una decimal y uno de carácter, donde claramente podemos apreciar la distancia Hamming de cada uno de ellos: 2, 3 y 3 respectivamente.

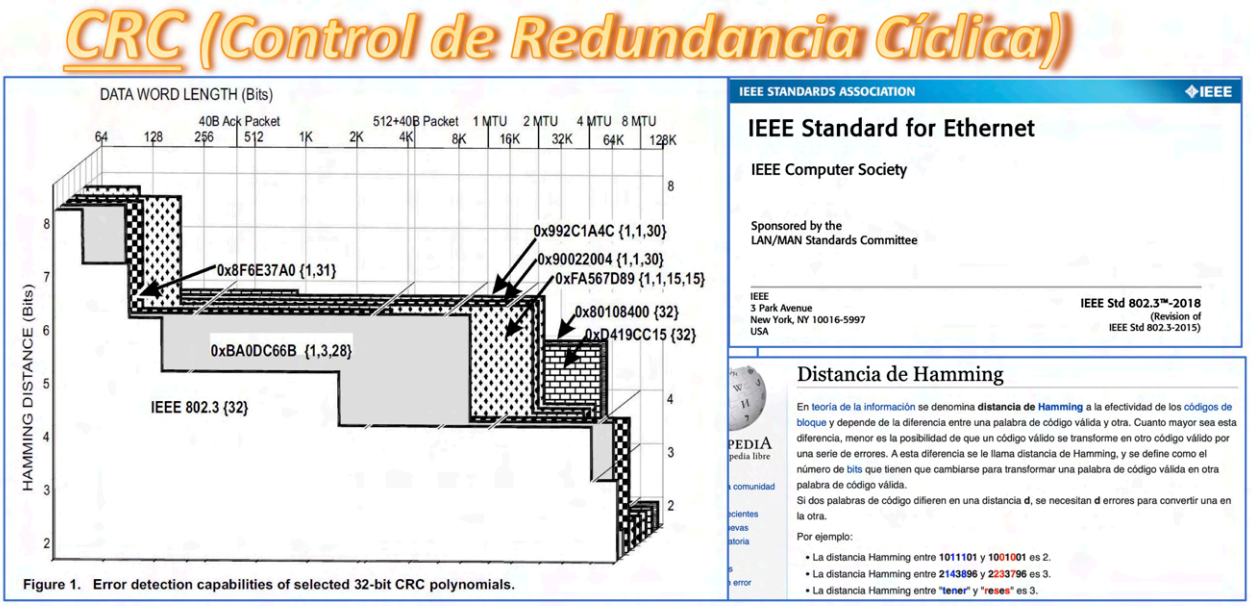
En la figura que sigue a continuación, que es parte de lo que se presenta en el video de esta charla, podemos ver un cuadro que también forma parte del norma IEEE-802.3, en el cual, se evalúan diferentes posibilidades en virtud de la longitud de los bits que viajan (eje de las X). En la parte inferior de ese cuadro y en color blanco de relleno, justamente está el IEEE-802.3. Si miramos los valores del eje de la "X" que figuran en la

parte superior del cuadro, veremos que entre 1K y 2K, se encuentra un "escalón" que coincide exactamente con 5 bits de la **distancia Hamming** (eje de las Y).

Como hemos visto en el nivel Físico de nuestras charlas, en las redes Ethernet, se emplean cables UTP y fibras ópticas. Ambos medios tienen una calidad óptima, lo que provoca que los errores en este tipo de redes LAN; estén en el orden de 10^{-8}. Es decir, un error cada 100.000.000 bits, cosa que podemos apreciar, es una tasa de errores bajísima.

Por otro lado, en telecomunicaciones, los errores no se suelen producir "aislados", es decir de un solo bits, sino que lo más frecuente es el fenómeno de "**burst**" (**ráfagas**). En este tipo de redes Ethernet actuales, la ocurrencia más frecuente de ráfagas es la de 5 bits, por eso es que el **CRC-32 de IEEE-802.3 es el más eficiente**.

Tomémonos un tiempo para entender bien este punto, analizando estos párrafos con la imagen de abajo, hasta que no nos quede ninguna duda.



$$X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^{8}+X^{7}+X^{5}+X^{4}+X^{2}+X+1$$

32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
1	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	1	0	0	0	1	1	1	0	1	1	0	1	1	0	1	1

Y: ¿**Por qué empleamos un polinomio generador de 32 bits**, y no otro tamaño?

Si prestáis atención a la primera imagen de este capítulo, podéis verificar que este campo (**FCS**) viaja luego del "encabezado" y luego de la totalidad de los datos y relleno (**PAD**). Esta ubicación se debe a que todo este contenido (encabezado, datos y PAD) se divide binariamente por exactamente este CRC-32, y lo que viaja en este campo es **el resto de esta división**. Como es un "resto", jamás podrá ser mayor a 32 bits, por esta razón, nos aseguramos que siembre cabrá en esta ubicación.

Analicemos cómo es esto de la división binaria.

Si realizamos una división decimal, por ejemplo: 14 /3:

14	3
2	4

Si hiciéramos lo mismo en binario sería:

8 4 2 1 d	
1 1 1 0	1 1
-1 1	1 0 0
0 0 1 0	

Lo que hace Ethernet es:

Encabezado + datos + PAD	10000010011000001000111011011011
x x x x x …	**Resultado** (no interesa)
Resto —> (Es lo que viaja como FCS)	

El ETD que recibe este FCS o CRC, realiza exactamente la misma operación, obtiene su propio resto, y si este es igual al que ha recibido en el campo FCS o CRC (como prefiráis llamarlo), entonces está **OK**. Si existe alguna diferencia, descarta esa trama, sin generar ningún tipo de aviso.

Técnicas **BEC** y **FEC**.

Por último, si bien no es parte específica de “Ethernet”, merece la pena de presentar las dos grandes familias de control de errores que suelen emplearse en Telecomunicaciones.

Cada una de ellas dependerá del tipo de transmisión. Cuando puedo volver a **reenviar** un error, y solo necesito **detectarlo**, las técnicas más empleadas se denominan Backward o **BEC** (Backward Error Control), como es el caso de IEEE-802.3 con su CRC-32 que acabamos de explicar. Consideremos que es tan, tan, tan, tan baja la tasa de errores (recordad: 10^{-8}) que no se justifica emplear más esfuerzo en este tema.

Cuando la red no es tan confiable, o hasta inclusive, el caso más típico son las comunicaciones de guerra, en las cuáles no pueden darse el lujo de estar dialogando un determinado tiempo, o quedarse esperando que le confirmen, o no, si llegó bien o deben reenviar, etc. (en la guerra la triangulación de radio frecuencias, es la mejor forma de ubicar con máxima certeza una posición enemiga, así que un transmisor es el mayor atractor de bombas. En general, se transmite y se cambia inmediatamente de ubicación con la radio apagada).

En estos tipos de casos, se emplean técnicas redundantes, en las que se envía mayor cantidad de información adicional con el objetivo que el receptor pueda “**detectar** y **corregir** errores” con la única información que contiene el mensaje y sin reenvío. Estas son las técnicas **FEC** (Forward Error Control).

A continuación se presentan los conceptos básicos de ambas técnicas. Son solo ejemplos para que se comprenda el tema, pues, luego cada una de ellas posee algoritmos mucho más complejos, como es el caso de CRC-32 para BEC.

Control de errores

BEC (Backward Error Correction) Bit de Paridad PAR

0	0	0	0	0	0	0	**0**
1	0	1	1	0	1	1	**1**

Bit de Paridad IMPAR

0	0	0	0	0	0	0	**1**
1	0	0	1	1	1	1	**0**

FEC (Forward Error Correction) Matriz cruzada (PAR)

1	1	1	1	0	0	0	0
1	0	0	0	1	1	1	0
0	1	1	0	0	0	0	0
1	0	0	1	1	1	1	1
0	0	0	1	1	1	0	0
1	1	1	0	0	0	1	0
0	0	0	0	1	1	1	1
0	**1**	**1**	**1**	**0**	**0**	**0**	**0**

← Cada 7 tramas, envío una exclusivamente de “paridad”

Volver al índice

www.darFe.es

Charla 17

Address Resolution Protocol

Enlace al Video:

Resumen:

En esta charla sobre el protocolo **ARP**, vemos su funcionamiento, primero de forma teórica, y luego técnicamente, analizando una captura de tráfico realizada con **Wireshark**.

Finalmente, presentaremos la teoría del ataque ARP, que lo desarrollaremos de forma técnica y detallada en la charla siguiente.

Descripción detallada

Para que se pueda establecer la transferencia de datos entre dos ETD en la familia TCP/IP, estos deberán conocer obligatoriamente las direcciones IP y las de Hardware (MAC), del emisor y receptor; hasta que estas cuatro no se encuentren perfectamente identificadas, no se podrá iniciar ninguna transferencia de información.

Bajo este esquema, es fácil pensar que si un ETD A desea envía información, conozca su propia dirección MAC e IP, también es razonable que pueda conocer la dirección IP destino; el responsable de descubrir la dirección MAC faltante es el protocolo **ARP** (Address Resolution Protocolo)

El mecanismo que emplea es el de mantener una tabla dinámica en memoria en cada ETD llamada **caché ARP** (la cual se puede analizar por medio del comando "**arp**"), en la misma se van guardando todas las asociaciones de MAC-IP que escucha el ETD en la red. Al intentar transmitir información, analizará primero en su caché ARP si esta asociación existe, de no encontrarla generará un mensaje ARP.

A continuación presentamos un ejemplo de una consulta por medio del comando "**arp -a**"

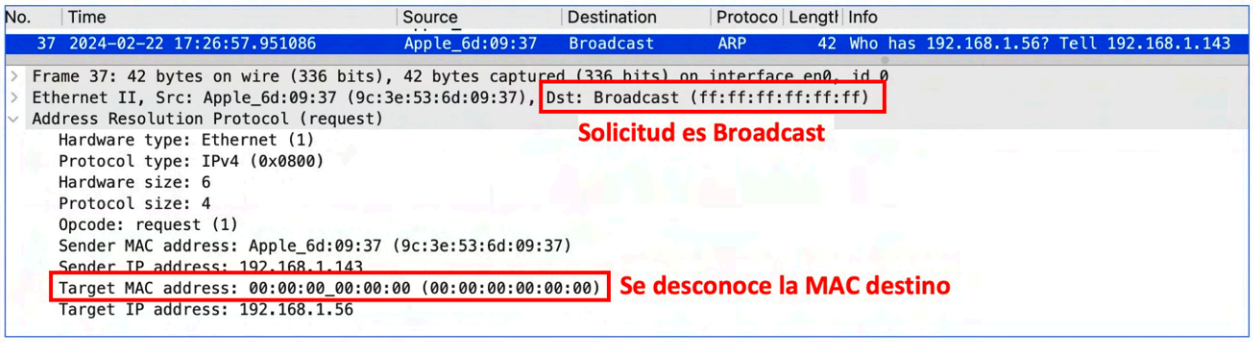
```
# arp -a
    (192.168.1.1) at 98:97:d1:b7:f1:ed on en0 ifscope [ethernet]
    (192.168.1.100) at f8:8e:85:55:1e:89 on en0 ifscope [ethernet]
    (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
```

Tipos de mensajes

ARP trabaja por medio de una **solicitud** y una **respuesta**. La Solicitud es un broadcast de nivel 2 (FF.FF.FF.FF.FF.FF), el cual será escuchado por todos los ETD de la red. Por ser Broadcast, todos los niveles 2 de todos los ETD de la red lo reconocerán como propio, entregando la toda la información correspondiente al nivel 3 en todos los ETD. El único nivel 3 que lo tomará como suyo será el que identifique su propia dirección IP en esta cabecera quien responderá (respuesta ARP), colocando en la dirección MAC faltante la propia, pero ya no por medio de broadcast sino dirigida al ETD que generó la solicitud ARP, pues poseerá todos los datos necesarios. Al llegar a destino se completa toda la información necesaria para iniciar la transferencia de información, y se incluirá esta nueva asociación MAC-IP en la caché ARP.

A continuación se presenta una imagen tomada por medio de una captura con Wireshark, en la que podemos apreciar una solicitud ARP y la respuesta ARP correspondiente.

Solicitud ARP



Respuesta ARP

Si repetimos nuestra consulta a la caché ARP, ahora podremos verificar que se ha recibido la respuesta y ya tenemos la asociación de MAC e IP.

```
# arp -a
    (192.168.1.1) at 98:97:d1:b7:f1:ed on en0 ifscope [ethernet]
    (192.168.1.100) at f8:8e:85:55:1e:89 on en0 ifscope [ethernet]
    (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
    (192.168.1.55) at 30:56:84:8:b8:a0 on en0 ifscope [ethernet]
    (192.168.1.56) at 4:a2:22:1b:42:ac on en0 ifscope [ethernet]
```

La última de las posibilidades existentes ocurre cuando un ETD no conoce su propia dirección IP, circunstancia que puede presentarse cuando bootea (arranca) un ETD y solicita una asignación dinámica de dirección IP o también al inicializar un ETD que no poseen disco duro. Ante este tipo de sucesos existe el Protocolo **R_ARP** (Reverse) (**RFC 903**), el cual genera un mensaje con formato semejante al ARP pero sin contener tampoco su propia dirección IP, la condición imprescindible para este protocolo es la existencia de un servidor R_ARP el cual recibirá este mensaje, resolviendo el direccionamiento IP del ETD que lo requiera. Los pasos de este protocolo son análogos a los del ARP. En el encabezado Ethernet, el campo identificador de protocolo de capa superior, llevará el valor **8035h** que identifica R_ARP.

En nuestra web: **https://darfe.es** en la sección “Descargas” —> “Capturas de tráfico”

Tenéis las siguientes capturas para que, si lo deseáis, puedas analizar este comportamiento:

- **rarp_request.cap**
- **rarp_request_response.pcap**
- **rarp_req_reply.pcap**
- **Protocolo_ARP-Request-Reply 10.28.54.pcap**

Ataque ARP

Este ataque tiene sentido únicamente en redes **LAN** (no debe olvidarse que el 80% de los ataques suceden en este entorno), se trata de una actividad verdaderamente peligrosa, pues redirecciona el tráfico hacia el equipo deseado. La lógica de su implementación es la siguiente:

- Se debe escuchar el tráfico ARP.
- Al detectar una solicitud ARP, se espera la respuesta correspondiente.
- Se capturan ambas.
- Se modifica el campo dirección MAC de la respuesta, colocando la dirección MAC de la máquina que desea recibir el tráfico IP, falsificando la verdadera MAC de la respuesta.
- Se emite la respuesta ARP falsa y ya está.

¿Qué se logra con esto?

Si se supone que la solicitud ARP la emitió el host A y la respuesta ARP la emitió el host B, el resultado de estos mensajes es que el host A, al recibir la respuesta de B, almacena en su memoria caché ARP la dupla IP(B)-MAC(B). Si a continuación de este diálogo, el host A recibe otra respuesta ARP que le asocia la IP(B) con una nueva MAC, supóngase MAC (X), el host A, automáticamente sobre escribirá su memoria caché ARP con la nueva información recibida: IP(B)-MAC(X).

A partir de este momento cada vez que emita información hacia la dirección IP del host A, la dirección MAC que colocará será la MAC(X), ante lo cual, el nivel Ethernet del host A descartará esa información, la cual sí será procesada por el protocolo Ethernet del host X, el cual por ser el intruso sabrá cómo procesarlo.

La totalidad de este ataque es conocido com “**man in the middle**” (ataque del hombre del medio), pues en definitiva el objetivo de máxima es poder “**reencaminar**” todo este flujo de información a través del host que fraguó la MAC para poder operar sobre las tramas que pasan por él.

Pero no nos adelantemos pues este tema lo veremos de forma real concreta en las siguientes charlas.

El comando “**arp**”

Muestra y modifica las tablas de conversión de direcciones IP en direcciones físicas que utiliza el protocolo ARP.

Volver al índice

www.darFe.es

Charla 18

Envenenamiento de caché ARP

Enlace al Video:

Resumen:

Esta charla la iniciamos con la instalación de "**Kali**" como máquina virtual, pues será una herramienta necesaria para la práctica de hoy, y también para el resto del ciclo. Continuaremos con otro video previo donde se explica el empleo de la herramienta "**Ettercap**", que forma parte de Kali. Cerraremos con el desarrollo técnico de este ataque y la presentación también del **ataque del hombre del medio (**MitM**),** y el **secuestro de puertos de nivel de enlace**.

Como podéis ver, se trata de una charla muy productiva.

Descripción detallada

En esta charla, antes de desarrollar el tema de ARP, vamos a comenzar a trabajar con "**Kali**", que nos acompañará el resto del libro.

Como ya hemos dejado traslucir en todas nuestras charlas, y también a lo largo de este texto, tenemos mucha afinidad con los entornos "**Open Source**", es decir de código abierto.

Tal cual podemos ver en **Wikipedia**. (Os recomendamos ir a este enlace para evaluar con todo detalle la importancia que esto tiene).

> "*El **código abierto** (en inglés: open source) es un modelo de desarrollo de software basado en la colaboración abierta. Se enfoca en los beneficios prácticos (acceso al código fuente) y en cuestiones éticas o de libertad que tanto se destacan en el software libre. Para muchos el término «libre» hace referencia al hecho de adquirir un software de manera gratuita. Sin embargo, de lo que se trata es de abaratar los costos y ampliar la participación; que sea libre no necesariamente implica que sea gratuito, lo importante sigue siendo ampliar la participación y extender libertades*".

Dentro de esta filosofía Open source, los sistemas operativos, son quizás el corazón de este proyecto. El sistemas operativo por excelencia de este entorno es, sin lugar a dudas "**Linux**". Para profundizar sobre Linux, os recomendamos que os dirijáis a nuestra "**Ciberwiki**".

Los sistemas operativos de la familia Linux, poseen muchas distribuciones (Red Hat, CentOS, Debian, Fedora, OpenSUSE, etc.). Es difícil poder recomendar una en particular, pues "para gustos, los colores", pero en nuestro caso, por una cuestión: del destino tal vez, hemos trabajado mucho con la distribución **Debian**.

No podemos dejar pasar por alto, nuestro consejo de siempre:

Si os vais a dedicar a Ciberseguridad "sí o sí" debéis familiarizaros con Linux.

(y cuanto más expertos seáis, pues, mucho mejor)

Para nuestro día a día en Ciberseguridad, hay una distribución en particular que no podéis dejar de emplear. Se llama "**Kali**" y se trata de una distribución **Ubuntu/Debian**, en la cuál, se encuentran preinstaladas más de seiscientas herramientas específicas para estos temas, con lo que es imprescindible si queremos seguir avanzando.

Para poder comenzar técnicamente a desarrollar estos temas, más específicos de Ciberseguridad, es que nos parece necesario que antes de continuar con este texto, instaléis una versión de esta distribución.

Para ello, tenemos dos videos publicados en el canal Youtube, y un documento ".PDF" en nuestra Web donde se explica como instalarlo en una máquina virtual.

Los enlaces son:

- **Video 1**: Instalación de "Kali" en VirtualBox (desde un fichero ISO).

- **Video 2**: Instalación de "Kali" en VirtualBox (desde una imagen OVA)

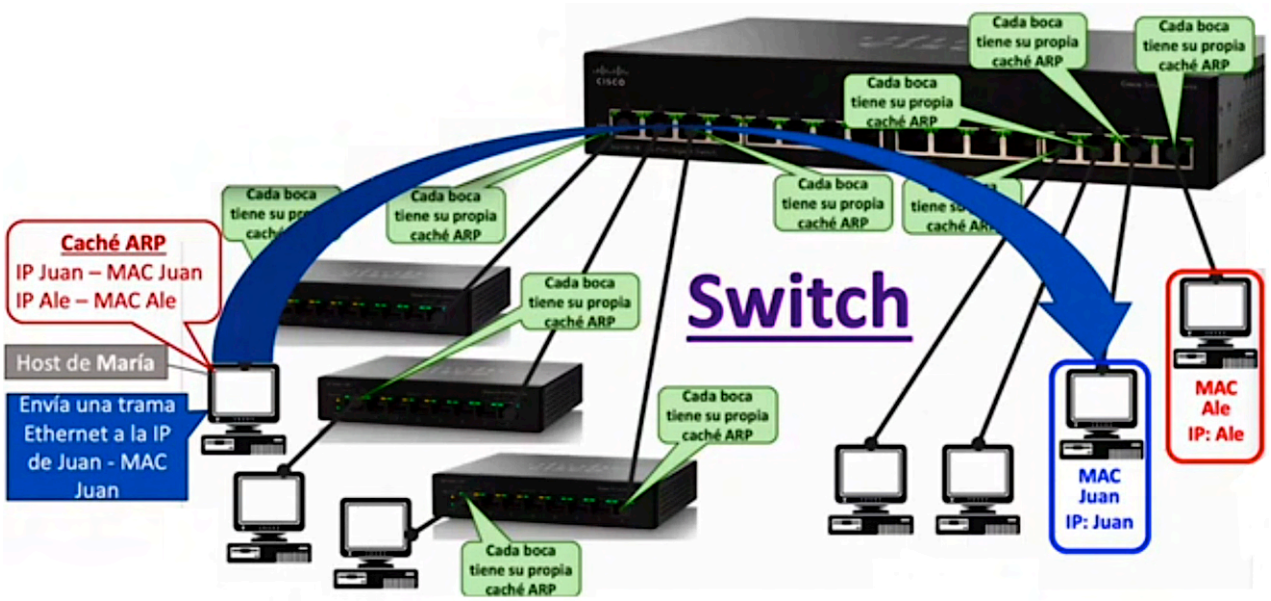
- Documento **PDF**: **Instalación de Kali en VirtualBox (paso a paso)**

Una vez que tengas instalado Kali, te recomendamos que, poco a poco, vayas buscando tutoriales y ejercicios del mismo para ir acostumbrándote a su empleo. Por nuestra parte, durante todo el ciclo, iremos utilizándolo.

Entrando de lleno al tema de hoy, en primer lugar os recomendamos otro video que también está en nuestro canal Youtube, donde explicamos el "**envenenamiento caché ARP empleando Ettercap sobre Kali**".

Lo importante de la charla de hoy, es que entendamos la lógica del envenenamiento de caché ARP, pues es uno de los ataques más peligrosos en entornos LAN.

Para ello, volveremos a la imagen del switch que presentamos en la charla 14, y sobre el mismo, definiremos tres hosts (o ETD), el de **María, Juan** y **Ale**. Supongamos que estos tres ETD, se encuentran conectados como se presentan en la imagen siguiente.



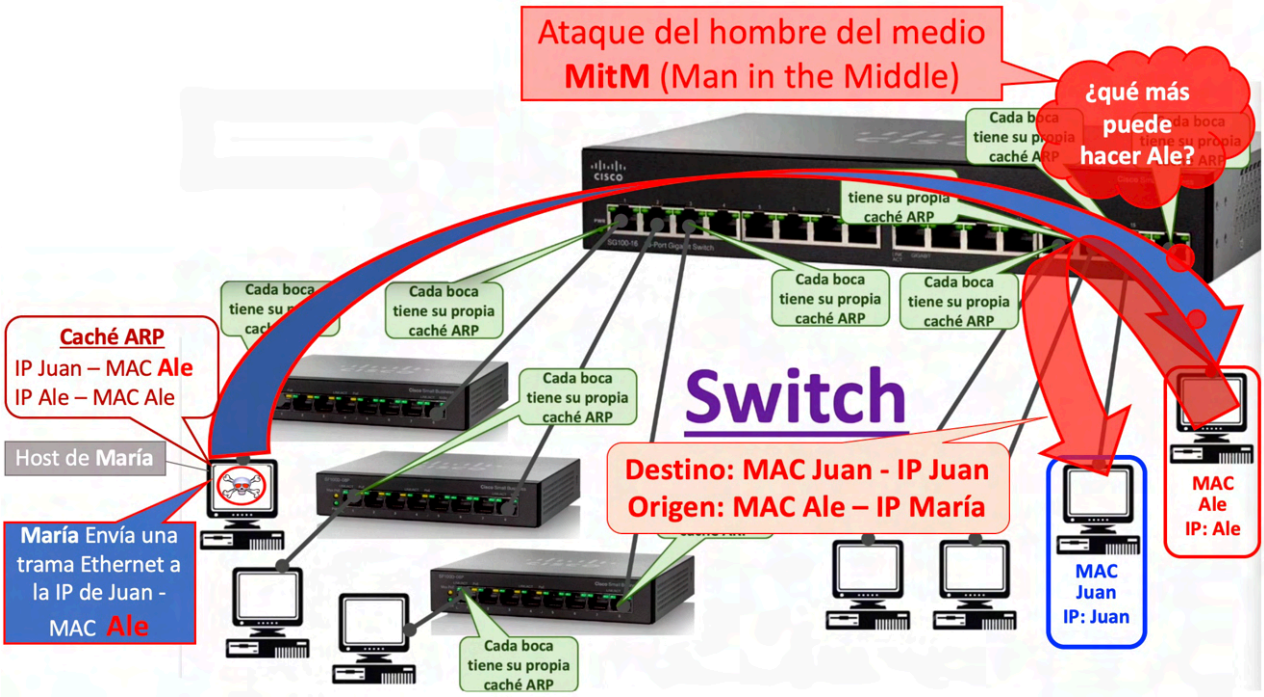
Cada host, tiene su propia dirección **MAC** y su propia dirección **IP,** como se representa en cada cuadro con su nombre. Si María, estuvo dialogando con los otros dos, ya tiene en su propia caché ARP las asociaciones de Ale y de Juan (Como se aprecia en el cuadro rojo de María). Si en esta situación, María le quisiera enviar cualquier información a Juan, podría hacerlo, y le enviaría un mensaje Ethernet con la destination MAC Address de Juan, y a nivel de red, con la dirección IP de juan, pues posee ambos datos en su caché ARP. Esto se representa con la **flecha azul**. Este sería el tráfico normal de esta red LAN entre María y Juan.

Pero supongamos ahora que logramos "**envenenar**" la caché ARP de María, ¿Cómo sería esto?.

El ETD de Ale, comenzaría a generar tráfico ARP (por ejemplo con la herramienta **Ettercap** del video que mencionamos antes), diciéndole a Maria:

—> Mira María: La **IP de Juan**, se corresponde con la **MAC de Ale**.

Al recibir este tipo de mensajes (si se reiteran, mejor aún), la tabla caché ARP de María va a sobre escribir lo que tenía almacenado con la última información que haya recibido. Por lo tanto su caché ARP quedaría como se presenta en la siguiente imagen.



Concretamente, acabamos de "**envenenar**" la caché ARP de María. Si ahora María quisiera comunicarse nuevamente con Juan, lo que enviaría es un mensaje "Ethernet" con la destination MAC Address de **Ale**, y a nivel de red, con la dirección IP de juan, pues posee ambos datos en su caché ARP. La máquina de Juan, descartaría este mensaje, directamente a nivel de enlace pues NO es para su dirección MAC. Quien lo recibiría es el ETD de Ale. El switch, de todo esto ni se entera, pues a su nivel (enlace), está todo OK. Fijaros que ahora Ale, puede perfectamente reenviar esta información a la dirección MAC de Juan, con la dirección IP también de Juan, el cual, al recibirlo lo verá perfectamente normal y su respuesta será para Ale (creyendo que es María). Ale, nuevamente puede reenviar esta respuesta a María, con la dirección MAC y la dirección IP de María, la que lo recibirá, sin enterarse absolutamente de nada.

Acabamos de realizar un ataque del hombre del medio (**MitM**).

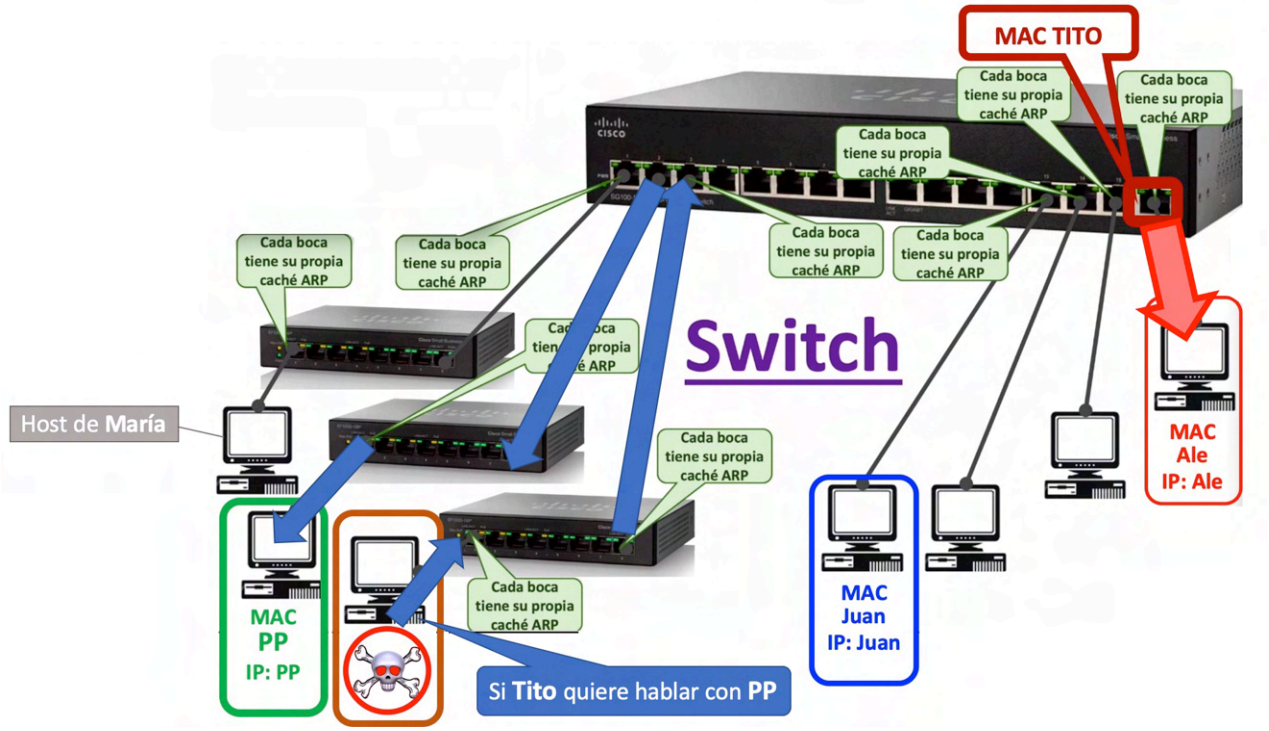
Esto no acaba aquí, pues en las imágenes que estamos tratando, podemos ver una jerarquía de switchs. Cada uno de ellos, tiene su propia caché ARP por cada una de sus bocas.

Supongamos que en uno de los switchs de abajo, existen otro dos ETD, por ejemplo" **PP**" (sin alusiones políticas, por favor…) y "**Tito**". Si, en este caso, yo "Ale", quisiera escuchar el diálogo ente ellos ¿podría?

Si hemos estado atentos, de verdad, verdadera…, en todas las charlas anteriores, tendría toda la lógica si pensareis: esto es imposible, pues cada uno de los switchs de Tito y PP, conmutarán la comunicación entre ellos, y jamás (de los jamases), se la enviarían por la boca de "Ale"… hummm, muy buena reflexión, se ve que habéis estado atentos de verdad, verdadera… peeeeeeeeero… ¿**Y si lograra envenenar la caché ARP de esos switchs**?, ¿entonces qué sucedería?

Esta actividad se llama "**Secuestro de puertos** a nivel enlace". Lo que debería intentar, es, decirle a los switchs de abajo que la MAC de Tito está en el puerto físico del switch donde está conectado "Ale", y si lo logro, pues, el switch en el que está PP, cuando le envíe un mensaje a Tito lo enviará hacia la boca en la que está Ale, pues hemos logrado sobre escribir en su caché ARP.

Mucho cuidado con esto último, pues sabiendo hacerlo adecuadamente, podemos escuchar el tráfico que se nos ocurra en cualquier "dominio de colisión" que deseemos, por supuesto si esos switchs no están debidamente configurados, cosa que es lo más habitual en este mundo, aunque parezca mentira. Por esta razón es que durante todo nuestro ciclo, estamos haciendo muchísimo hincapié en el nivel de enlace, y así seguiremos hasta la charla 40, con todo lo que nos queda de la familia **IEEE-802.x**.



Volver al índice

www.darFe.es

Charla 19

Interceptación de llamadas de VoIP

Enlace al Video:

Resumen:

En esta charla de hoy, continuando con el envenenamiento de caché ARP, lo veremos de forma práctica, a través de **VoIP** (Voice over IP), tema que trataremos en detalle más adelante (charlas 61 y 62), pero que como ataque en sí, se lleva a cabo en el nivel de enlace.

Emplearemos la herramienta "**Caín y Abel**" para realizar de forma concreta y real esta interceptación y os dejamos varios videos, capturas de tráfico y documentos para que podáis profundizar al máximo esta interceptación.

Descripción detallada

El tema de **Voz sobre IP**, generalmente abreviado **VoIP** (Voice Over IP), debe ser presentado marcando bien la diferencia entre cualquier servicio de VoIP y la tecnología de 4G que emplea Voz sobre LTE, que se denomina **VoLTE** (Voice Over LTE).

Para ofrecer VoIP sólo hace falta poder digitalizar los 4 KHz del canal vocal de nuestro dispositivo de entrada (micrófono, teléfono, etc..) en un canal básico de **64 kbps** (que luego podrá o no ser comprimido) e inyectarlo como cualquier otro fichero en una red IP. La calidad que se pueda ofrecer sobre esta red es el punto clave.

Este tema de la digitalización, ya lo hemos visto en la **Charla 06** El nivel Físico (Digitalización - Señal analógica, señal digital).

Hoy en día, cualquier ordenador puede realizar esta digitalización y existen cientos de programas que permiten instalar servicios de VoIP. Si se tiene en cuenta que cualquier red LAN ofrece en la actualidad un ancho de banda mínimo de 100 Mbps y relacionamos esta velocidad con los 64 kbps de nuestro canal de voz digitalizado, estamos hablando de una relación de 1562,5 veces superior (es decir 100.000 % 64 = 1562,5), esto quiere decir que el mismo paquete de voz, podríamos inyectarlo 1.500 veces en la red, y así y todo, viajar cada uno de ellos más rápido que en un canal telefónico clásico de conmutación de circuitos de 4.000 Hz.

Si bien una red de paquetes no nos garantiza la entrega ordenada, y luchará con colisiones para ingresar a esta red LAN, así y todo es tan inmensamente superior la velocidad, que nos podemos dar el lujo de reenviarlo cientos de veces hasta que garanticemos la entrega en el tiempo necesario. Es difícil de comprender estas diferencias de velocidad, pues se llega al caso de poder plantear que si hablo a viva voz, mis mensajes viajarán a 300 m/s (velocidad de la onda acústica), pero si el mismo mensaje lo envío por un cable UTP (pares trenzados) o por una fibra óptica, estaría viajando a velocidades que superan los 200.000.000 m/s…, esto implica que si el mismo mensaje que envío a viva voz, a su vez lo ingreso a esta fibra óptica, el mismo podría enviarlo, prácticamente 1.000.000 de veces antes que llegue a la onda acústica a su destino, aunque esté a pocos metros de distancia.

El problema nuevamente será el de calidad de la red, pues si la red LAN está saturada de hosts, o tiene un insatisfactorio número de colisiones, esta relación comienza a degradarse.

El caso más real es cuando escalamos el entorno de esta red LAN e intentamos transmitir VoIP a través de Internet. En este último caso, nuestros paquetes de voz circularán por los routers, dependiendo de cómo, cada uno de ellos haya decidido enrutar, cada uno de estos poseerá su propio vínculo, con un ancho de banda diferente y procesarán nuestros paquetes junto a varios millones de millones de paquetes más, de los cuáles algunos poseerán un nivel de calidad o prioridad de servicio mejor o peor, serán descartados, o retransmitidos, etc. Y allí la calidad ya empieza a ser un problema más importante, llegando al extremo que la comunicación vocal sea insostenible.

Algunas empresas han desarrollado sus servicios específicamente para mejorar esta calidad, montando verdaderas infraestructuras propietarias de comunicaciones a través del mundo que hacen un alto esfuerzo para mejorar esta calidad (Skype, WhatsApp, etc.), pero así y todo siempre existirán segmentos de red que quedan fuera de su

jurisdicción y la calidad no llega a ser la óptima, aunque en la actualidad hay que reconocer que están ofreciendo un servicio muy bueno.

Todo esto, sin entrar en los detalles de routing, es resumidamente de lo que se trata VoIP, pero iniciamos esta sección justamente con la idea de marcar la diferencia entre VoIP y VoLTE pues es aquí donde la "Calidad del Servicio" es el punto clave.

Si deseáis profundizar más en este tema, os recomendamos que leáis el punto 1.5. Voz sobre IP y VoLTE del libro "**Seguridad en Redes**" (que podéis descargar gratuitamente en nuestra Web https://darFe.es).

También os invitamos a que tengáis un poco de paciencia para poder seguir avanzando "paso a paso", pues el detalle sobre VoIP, se desarrolla en las charlas del nivel de red o nivel 3. Cuando lleguemos a este nivel, veréis con todo detalle este tema.

Si os atrevéis a ir investigando un poco sobre el mismo, os damos permiso para que vayáis viendo nuestros videos.

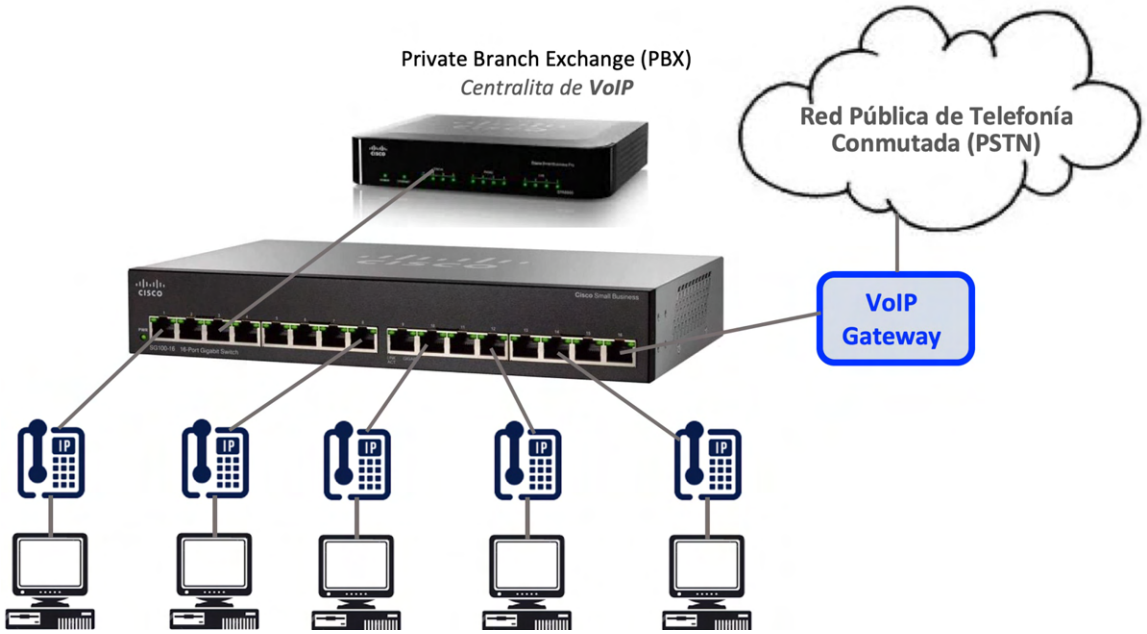
- **VoIP (Voz sobre IP) Presentación - Charla 61** - Aprendiendo Ciberseguridad paso a paso

- **VoIP (Voz sobre IP) Seguridad - Charla 62** - Aprendiendo Ciberseguridad paso a paso

Yendo a la charla de hoy, avanzaremos un poco más sobre el tema de "envenenamiento de caché ARP" que iniciamos en el capítulo anterior, pero ahora orientado a VoIP pues justamente, hoy en día cualquier empresa está en capacidad de montar una infraestructura para ofrecer este servicio en entornos LAN, e inclusive ampliar estas comunicaciones de voz en todo su entorno.

Para implementar una infraestructura de VoIP, solo hace falta apoyarnos en nuestros switchs, conectar nuestros teléfonos IP a ellos como si fuera un ETD más, e integrar una "**centralita de VoIP**" que puede ser por medio de software, como por ejemplo el proyecto Open Source "**Asterix**"

También podemos hacerlo con una centralita de hardware, como se presenta en la imagen que sigue, en este caso presentamos una **PBX** (Private Branch Exchange) del fabricante Cisco.

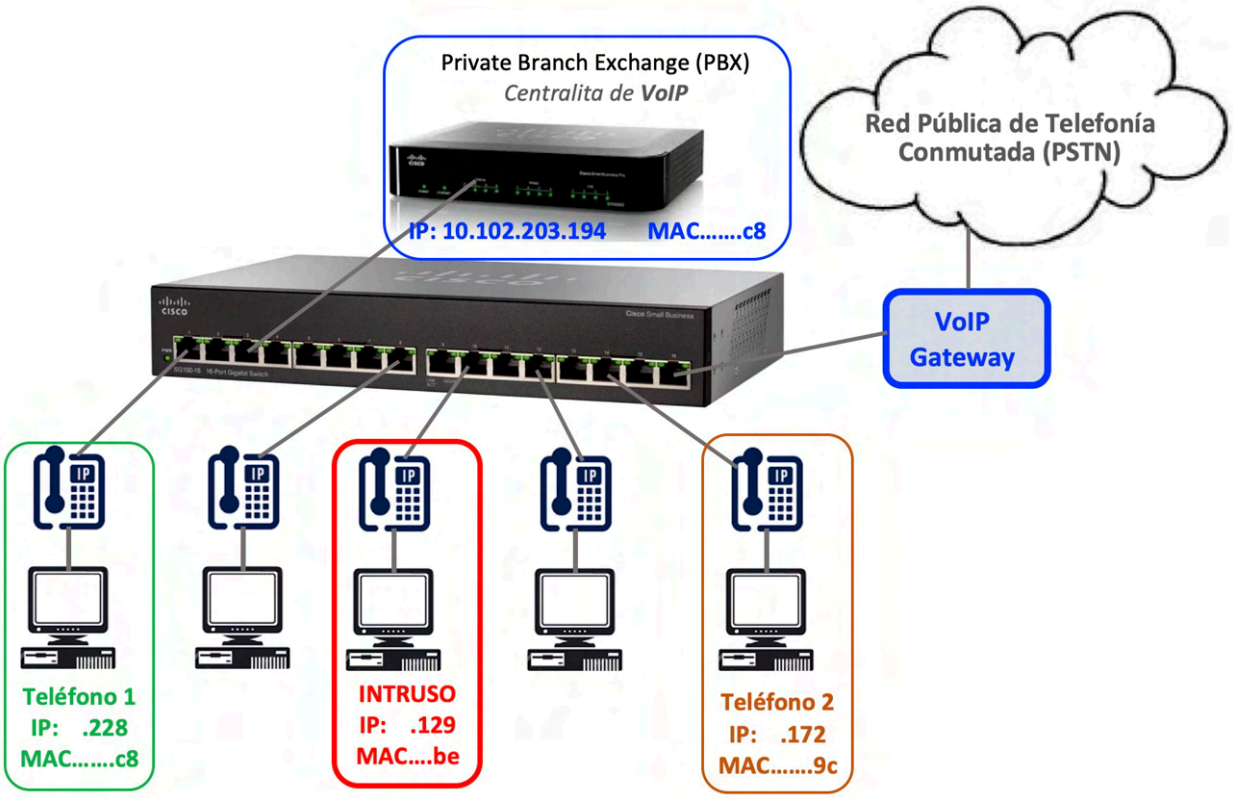


El servicio que ofrecen este tipo de centralitas (o PBX) es el de digitalizar la voz por medio de cada uno de los teléfonos de VoIP, e inyectarlos en la red LAN como tramas Ethernet, enrulándolos por medio del protocolo IP de nivel de red (nivel 3), que lo veremos en detalle más adelante, por ahora seguiremos centrados en el nivel de enlace.

Es importante destacar, tal cual se presenta en la imagen inicial, y con más detalle en la imagen de la derecha, que estos teléfonos IP, vienen con dos conectores **RJ-45**. Uno de ellos es el que se conecta al Switch (generalmente en la boca de conexión del puesto de trabajo, la cual está conectada al switch) y la otra es en la que se conecta el ordenador. Es el mismo teléfono el que separa el tráfico de voz y el de datos.

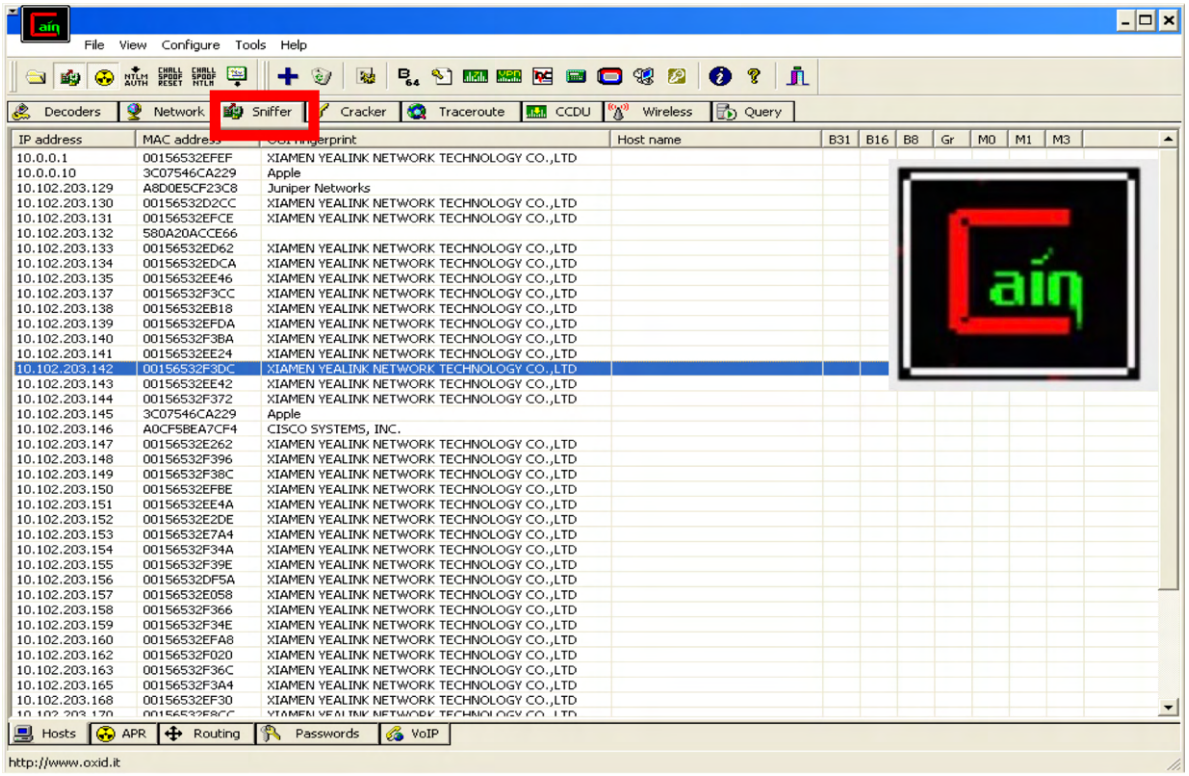
Para lograr comunicaciones hacia cualquier lugar del mundo, como lo hace la telefonía convencional, se instala un **gateway** (o pasarela) que reconvierte la VoIP en telefonía clásica (analógica) y lo inyecta en la red de telefonía conmutada (**PSTN**: Public Switched Telephone Network). Como se presenta en el recuadro **azul** de la primera imagen.

Este ataque de **interceptación de llamadas de VoIP**, como hemos dicho, se basa nuevamente en el envenenamiento de caché ARP. Para comenzar a explicarlo, nos basaremos en la imagen que sigue, en la que podemos ver diferentes teléfonos, donde, cada uno de los cuáles posee su propia dirección MAC y dirección IP (también la PBX).



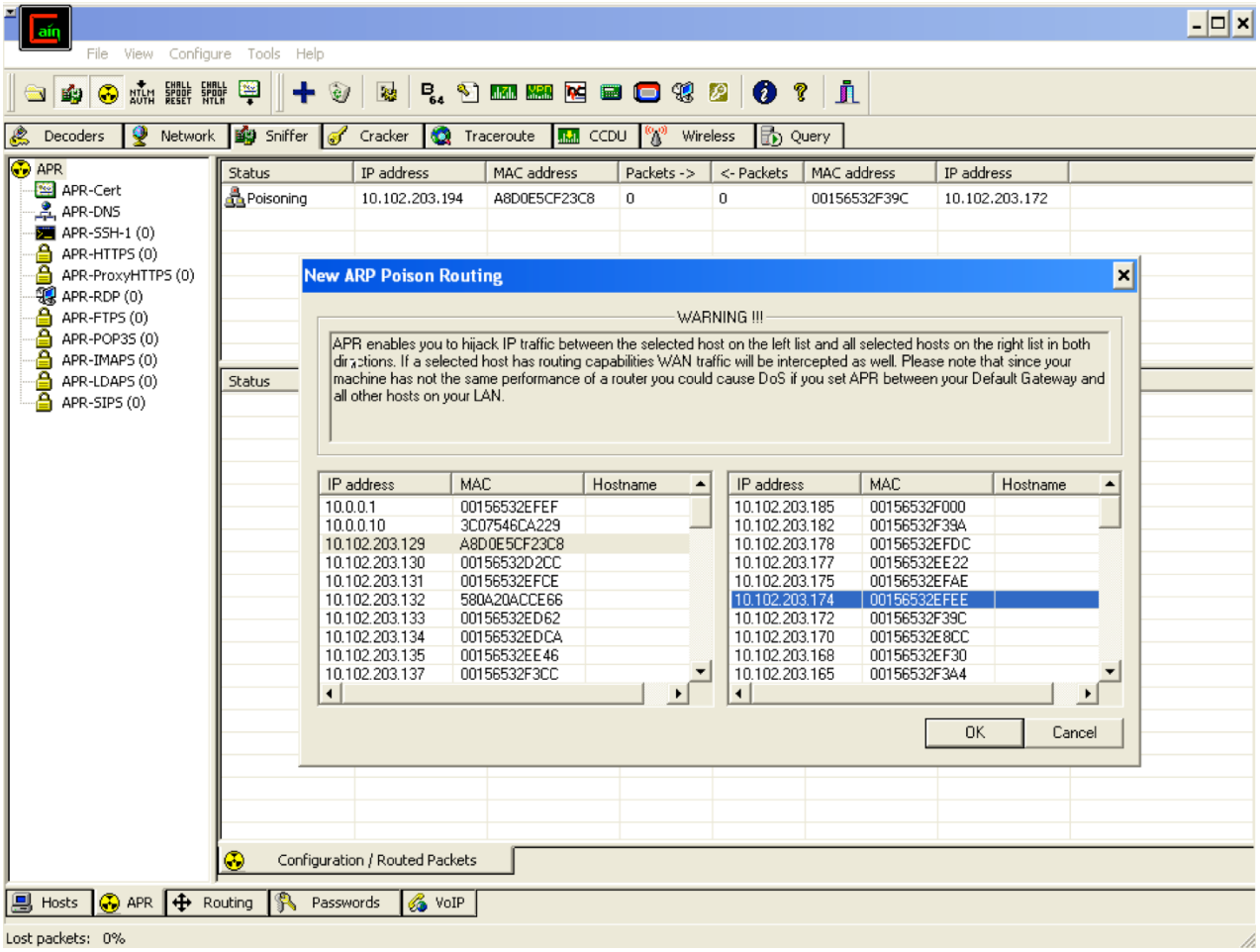
En **rojo**, incluimos también un teléfono más, que será el "**Intruso**", cuyo objetivo será participar entre medio de la comunicación entre el Teléfono 1 y el 2, es decir interceptar esta comunicación.

En esta charla 19, durante el video, presentamos una herramienta que se llama "**Caín y Abel**" (comúnmente, llamada solo **Caín**) que, si bien es antigua, sigue ofreciendo de forma muy sencilla el mecanismo necesario para la realización de este ataque. A continuación se presenta una imagen de la misma.



Lo primero que debemos hacer con Caín, es escuchar (Sniffer) el tráfico de esta red LAN. A medida que los diferentes teléfonos y ordenadores, generen broadcast (que, recordad, es el primer paso de ARP), Caín irá armando su propia tabla "caché ARP", con alguna información adicional, como podemos ver también en la imagen anterior.

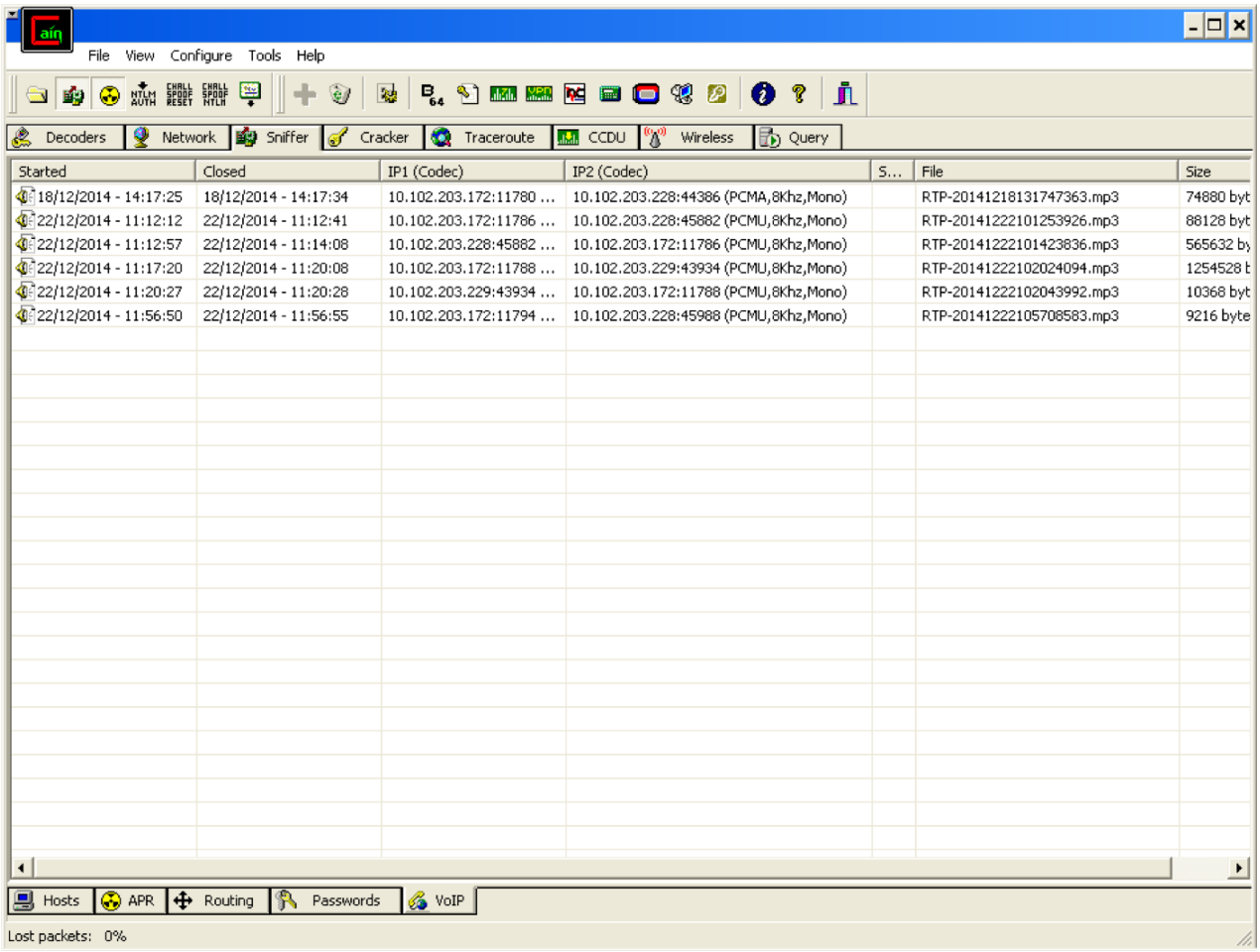
Una vez que hemos identificado el teléfono que se desea interceptar, se selecciona el mismo y se selecciona el botón de abajo que indica "**APR**" (con el icono que comúnmente se emplea para identificar venenos) y al presionar el mismo, se abre la ventana que vemos a continuación, donde solamente basta presionar "OK" y la interceptación ya está realizada.



Una vez envenenada la caché ARP de estos dos teléfonos, Caín automáticamente convierte los paquetes de VoIP en ficheros de audio. En realidad, lo que ha interceptado es el tráfico de voz que viaja en un protocolo que se llama **RTP** (Real Time Protocol), que es el estándar para VoIP. Por ahora no entraremos más en el mismo, pues, tal cual presentamos al inicio de este capítulo, todo esto llegará a su debido tiempo y "paso a paso" en el nivel de red con las charlas 61 y 62.

Por ahora solo presentamos este ataque pues opera exactamente en el nivel de enlace, con la técnica de envenenamiento de caché ARP que hemos visto en la charla anterior.

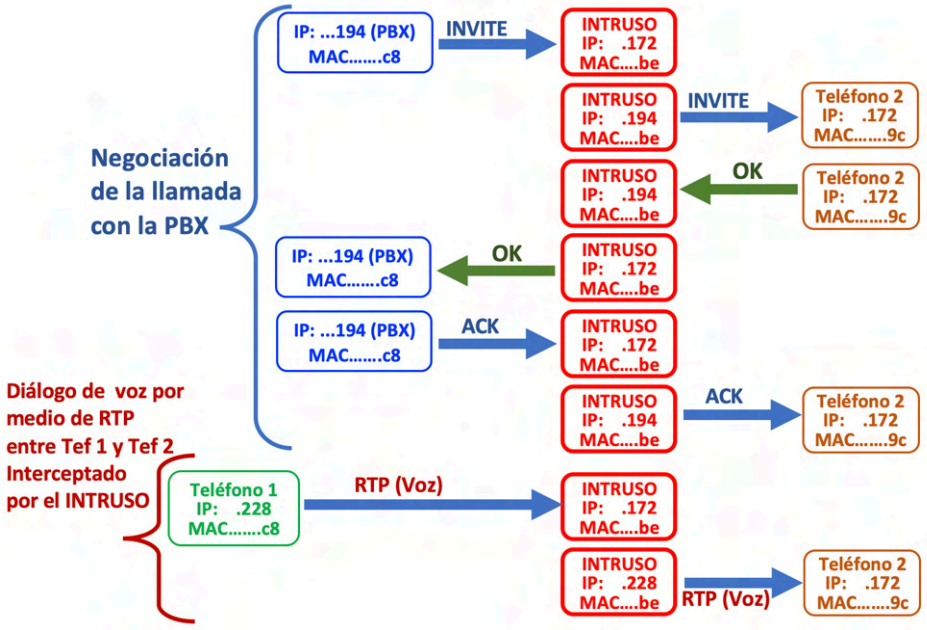
Como se puede ver a continuación, Caín nos ofrece esta voz ya convertida directamente a mp3.



Para los que queráis seguir todo este diálogo completo y analizarlo, hemos dejado la captura de tráfico ·"**VoIP_02_SIP-SDP-RTP_solo.cap**" correspondiente a la imagen anterior, subido a nuestra Web, en el menú:

"**Descargas**" —> "**Capturas de tráfico**"

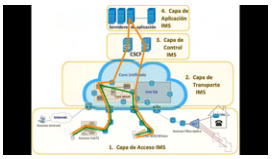
Si habéis juntado el coraje necesario para analizar esta captura, en realidad lo que estáis viendo es la siguiente secuencia.



Os desafiamos a que descarguéis la captura de tráfico **VoIP_02_SIP-SDP-RTP_solo.cap**, la abráis con **Wireshark,** y la vayáis siguiendo trama a trama, con la secuencia de la imagen anterior: INVITE, OK, ACK y RTP, para que comprendáis con detalle este ataque. Si aún os quedan dudas, abrid el video de esta charla de hoy, que está explicado esto mismo con toda la profundidad necesaria.

Para los muy curiosos, si queréis avanzar más aún sobre este ataque, tenemos un video que os puede interesar:

Seguridad en IMS (Internet Multimedia Subsystem)



El PDF de este video, se llama "**seguridad en IMS**" y podéis descargarlo en **este enlace**.

Por último para los más audaces, también tenéis desarrollado algo que os interesará, en el punto 1.8.4. "Ataques a SIP". del libro "**Seguridad en Redes**" (que podéis descargar gratuitamente en nuestra Web https://darFe.es).

Volver al índice

www.darFe.es

Charla 20

¿Móvil en aviones?

Enlace al Video:

Resumen:

¿Seremos capaces de estar "Desenchufados" 5 minutos?... parece ser que hay gente que tiene esta dependencia absoluta del móvil, que no les permite cumplir ni las normas que nos piden. ¿será importante cumplirlas?, hay gente que considera que esto no es necesario. ¿Y tú que opinas?

Descripción detallada

Este desenchufe de hoy, tiene su origen en un viaje de avión que realicé estos días.

Los que me conocen saben que me gusta y disfruto mucho de los viajes en avión.

Fui paracaidista muchos años, con mi querido "**Para Foil**" que era un lujo de paracaídas. Lo compré en EEUU en el año 1981, y cuando lo estrené en Argentina, fue el mejor paracaídas de mi país durante bastante tiempo, es el de la foto… ¡*qué épocas*!

En uno de estos viajes, en el año 1983, hasta nos estrellamos con un avión Fokker F-27 de la Fuerza aérea Argentina, como el de la foto de abajo.

Este accidente, fue debido a que el piloto no cumplió con las normas establecidas.

Por estas razones, fue que en el último viaje, cuando por megafonía, minutos antes del despegue, se indicó que debían apagarse los teléfonos móviles, me desagradó mucho, que una persona sentada en mi misma fila y del otro lado del pasillo, pasó olímpicamente del mensaje y siguió conectado como si nada. Lo peor de todo, es que no se debía a una razón de necesidad imperiosa, causa que podía comprenderse, sino a que seguía, como si nada, mirando, uno tras otro, estos cortos videos de Tik Tok…

Vosotros pensaréis que hoy en día, no es necesario apagar los móviles en ninguna etapa de un vuelo, y quizás tengáis cierto grado de razón, pero os aseguro que, tal vez no del todo, y cuando el piloto dice literalmente que debemos aparcar estos dispositivos, su razón tiene.

Si aún no lo creéis, pues os invito a desenchufar un rato viendo este video.

Volver al índice

www.darFe.es

Charla 21

VLANS - IEEE 802.1Q

Enlace al Video:

Resumen:

Este video presenta la norma **IEEE-802.1Q** "**Bridges and Bridge Networks**", que es la que nos permite, crear **VLANs** (Virtual LAN) dentro de mi red local, para poder optimizar el empleo de los switchs.

Veremos que este estándar nos ofrece también la posibilidad de establecer **prioridades de tráfico**.

Todo esto, primero basándonos en lo que establece la norma y luego analizándolo por medio de capturas de tráfico real con **Wireshark**.

Descripción detallada

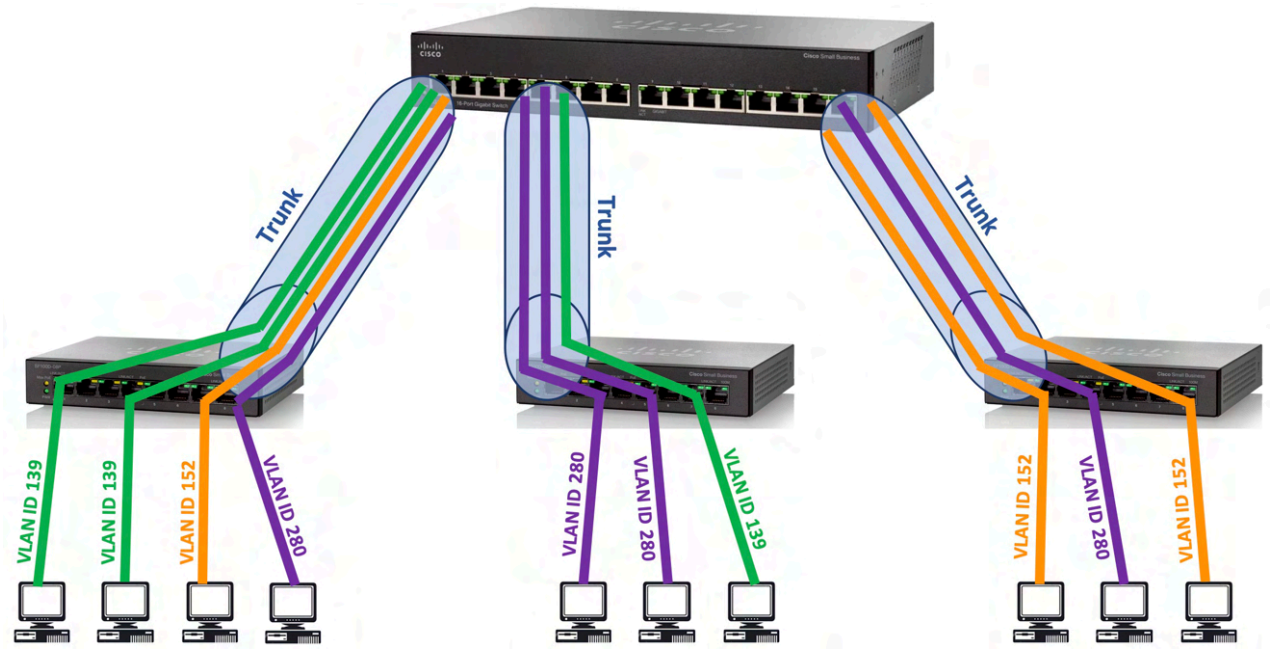
Este protocolo es el empleado justamente para la creación de **VLAN**s (Virtual LAN) dentro de un mismo switch y poder separar diferentes "dominios de colisión" bajo el concepto de "**Trunking**", lo veremos con mucha frecuencia y desde el punto de vista de la seguridad merece la pena prestarle atención pues es un foco importante de problemas.

IEEE-802.1Q como veremos a continuación, permite la creación de VLANs, agregando un encabezado de 4 bytes dentro de la misma trama Ethernet. Para que un switch "encapsule 802.1q" debe tener configurada sus interfaces y sus VLAN para ello. Las buenas prácticas, nos indican que si tenemos más de un switch, es mejor hacerlo bajo la idea de Interfaces "**Trunk**" (o troncal), que no son otra cosa que enlaces físicos entre los dispositivos (generalmente switchs, aunque no exclusivo de estos) por los cuales "entroncaremos" (aunque suene feo…) varias VLAN, transportando el tráfico de varias de estas a la vez, creando una especie de jerarquía entre ellos.

Existe una VLAN por defecto que es la VLAN 1 (o VLAN nativa), la cual ante cualquier error, omisión o ausencia de configuración, será por la que el switch envíe toda trama y sin agregar ningún encabezado 802.1Q, por esta razón es que esta VLAN 1 SIEMRE debe estar deshabilitada como medida de seguridad, debiendo tener precaución (en cuanto a switching) de cómo opero o creo esta ruta por defecto o nativa en mis switch.

Cada VLAN que es configurada en un extremo de cada Trunk, debe ser idéntica en el otro, pues en definitiva se trata de una conexión punto a punto, para operar en modo Trunk una interfaz debe ser puesta en "trunk On", sino por defecto no es trunk.

En la imagen que sigue, podemos ver una representación de diferentes VLANs y trunks.



A continuación presentamos cómo se vería básicamente esta configuración, en un switch tipo Cisco, (primero se crean las VLAN y luego se asignan):

```
vlan 2
 name Empresa-A
```

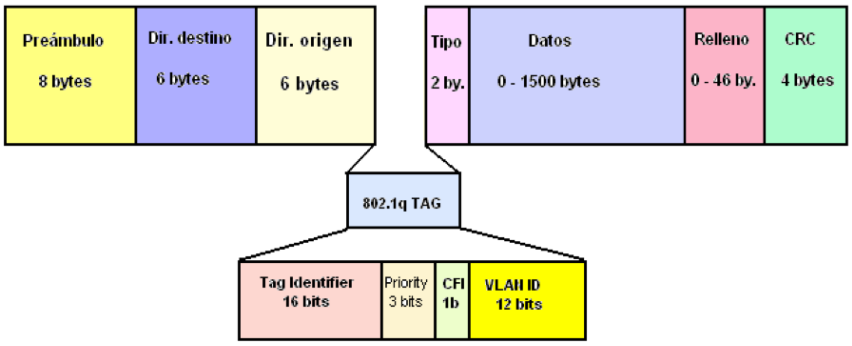
```
!
vlan 3
 name Empresa-B
!
vlan 4
 name Empresa-C
!
vlan 10
 name Zona_X
!
vlan 20
 name Zona_Empleados
!
vlan 100
 name Telefonia_IP
........
....
.

interface Port-channel1
 description conexion con Zona_X
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,10,18,35,92-105
 switchport mode trunk
!
interface Port-channel2
 description conexion con Zona_Empleados
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,10,67,94,95
 switchport mode trunk
!
interface Port-channel3
 description conexion con Empresa_A
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,10,21,61-67,70
 switchport mode trunk
......
...
.
```

Para distinguir el tráfico de las diferentes VLANs, a las tramas Ethernet se le añade un campo de **4 octetos** (trama Ethernet extendida), que contiene:

- Tag Protocol Identifier: 16 bits, contiene el valor **0x8100** , para que se identifique la trama como una trama etiquetada.
- Priority: 3 bits, indica la prioridad de la trama, 0 es el más bajo (best effort), 7 el mayor.
- CFI (Canonical Format Indicator): 1 bit, siempre 0 para switches Ethernet.

- VLAN ID: 12 bits que especifican la VLAN a la que pertenece la trama, es posible tener 4096 VLANs.

A todo el tráfico que entra por un puerto de acceso configurado para el empleo de 802.1Q (o **dot q**), el switch añade el campo relativo a la VLAN. Cuando la trama viaja por el trunk, queda intacta, y cuando sale por el puerto destino, el switch quita el campo.



En la imagen anterior, se presenta este formato especial de trama de nivel 2, pues lo que deseamos resaltar es que en la parte superior de la imagen, lo que vemos es una trama Ethernet pura y completa. Antes del campo "**Ethertype**" de la misma (de dos octetos), vemos que aparece un nuevo "**Tag**", es lo que acabamos de presentar como **Tag Protocol Identifier** de 16 bits, el cual cuando contiene el valor **8100**, a partir de allí cualquier dispositivo de nivel 2 sabe que en este caso particular deberá procesar cuatro octetos "adicionales" que son los que sí, sin lugar a dudas, identifican al protocolo 802.1Q con su VLAN correspondiente. Esta es la metodología empleada en casi todas las grandes redes para la gestión de VLANs.

Antes de seguir adelante con el desarrollo de VLAN, detengámonos un poco a analizar el concepto de "**Virtualización**" centrado en redes.

El concepto de "**redes virtuales**" es un término genérico que se emplea para diferentes tecnologías de virtualización. En el caso de redes, nos interesa particularmente centrarnos en el empleo del nivel de hardware y la conectividad física para a través del mismo poder "escalar" a los niveles de enlace y red en relaciones de "n" a "n", es decir poder relacionar un nivel físico a varios de enlace o red, o viceversa: varios niveles físicos hacia uno de enlace, varios o uno de red, etc.

El concepto que sí debemos tener claro es que:

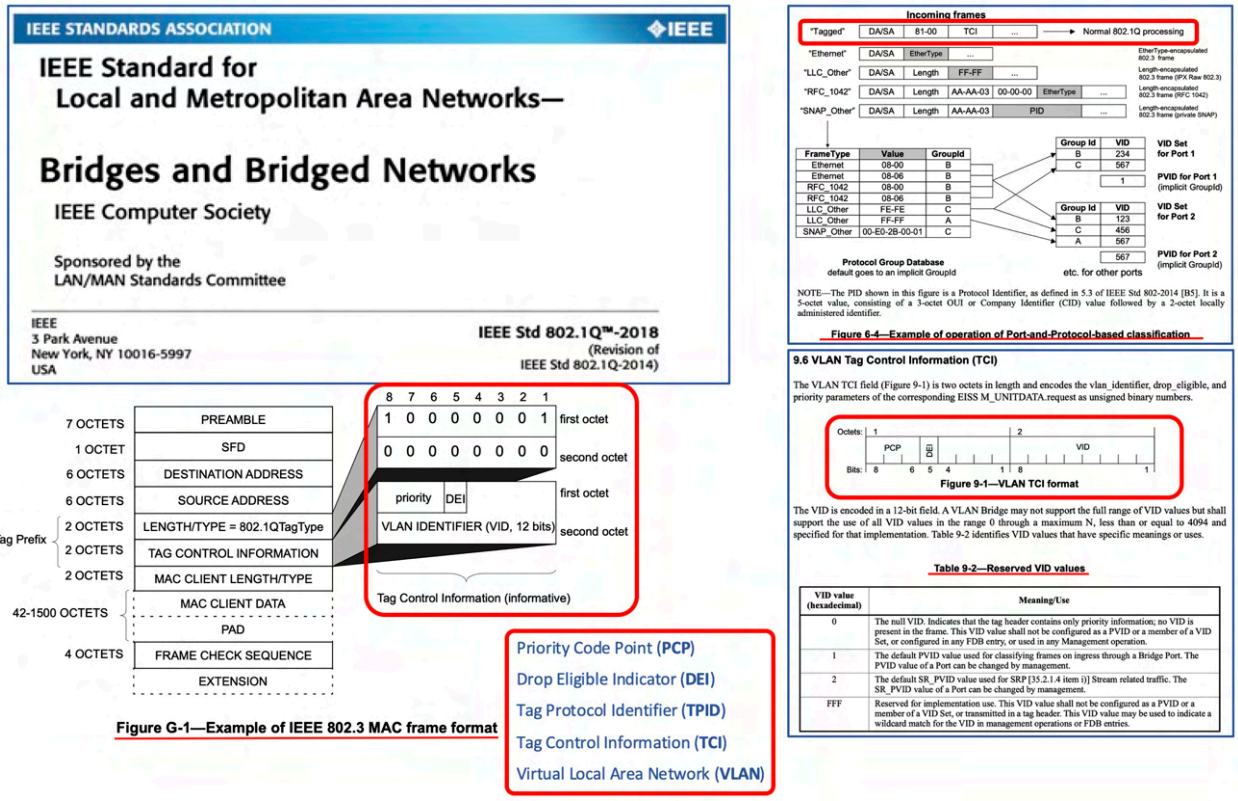
- a nivel físico (nivel 1): Las técnicas de "multiplexación" permiten que una misma interfaz física se pueda ver como varios "canales" diferentes y separados entre sí.
- a nivel de enlace (nivel 2): Protocolos como ATM (Asynchronous Transfer Mode) o Frame Relay ofrecen circuitos y rutas virtuales en este nivel (VCI y VPI), y en Ethernet metodologías de VLAN a nivel de enlace.
- a nivel de red (nivel 3): Toda la lógica de rutas a nivel IP, permite el empleo de múltiples sesiones a través de una sola interfaz, por medio de la cual pasa un sinnúmero de tráfico de diferente tipo.

Basado en los conceptos anteriores, es que cuando se habla de "redes virtuales" hay que tener claro de qué nivel, o niveles, se está hablando y cuál es la intención de las mismas pues, dependiendo de la elección, pueden verse o no entre sí, capturar o no su

tráfico, cifrar, autenticar, etc. Y eso sí es lo que nos interesa desde el punto de vista de seguridad.

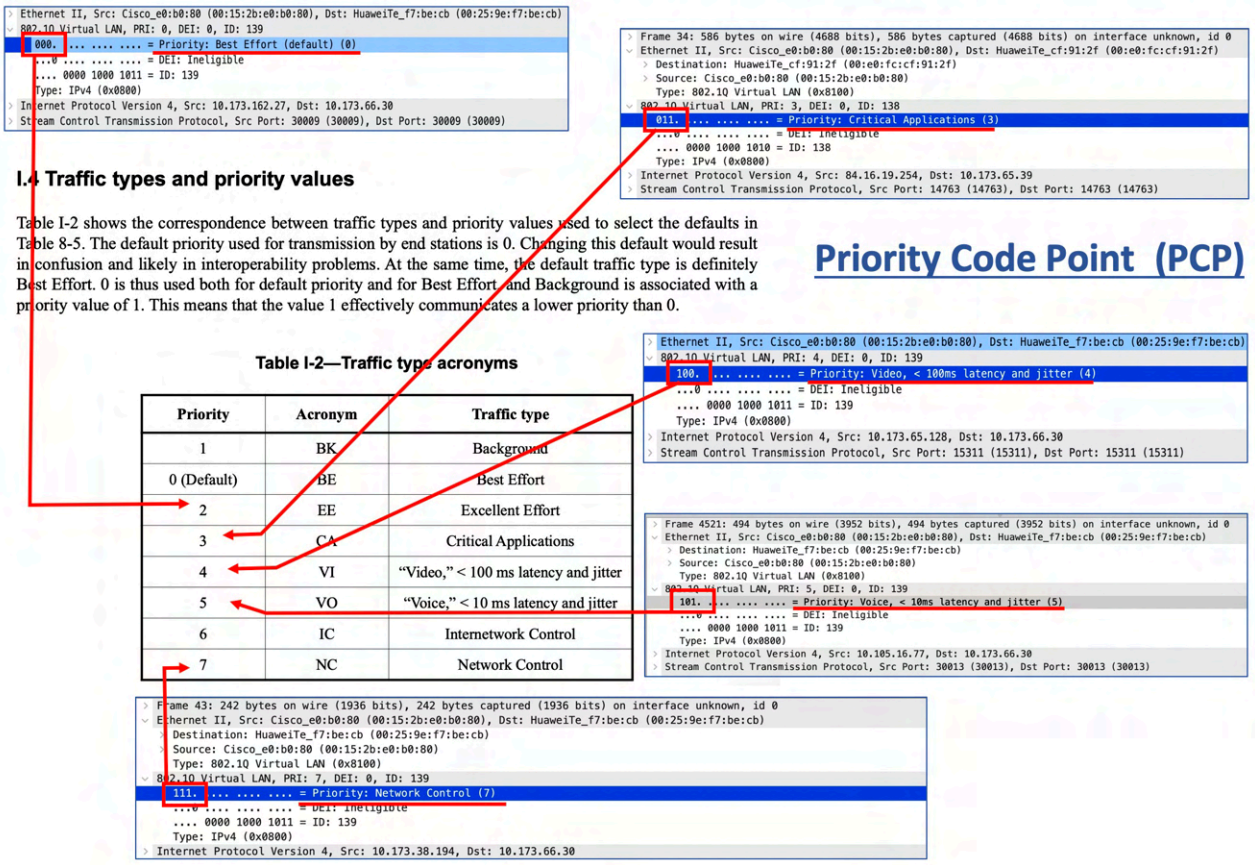
El video de esta charla, comienza con la imagen que sigue, que es justamente el estándar IEEE-802.1Q cuyo nombre real es "**Bridges and Bridge Networks**", pues recordad que el punto de partida de los actuales switchs fueron estos dispositivos denominados "Bridges" (presentados en la charla 14), por esta razón es que se habla de "redes puenteadas". Se ha recuadrado en **rojo**, los campos de especial interés, el primero de ellos es el formato de la cabecera, descripta anteriormente.

El segundo campo que nos interesa es el recuadro de arriba a la derecha, en el cual, la norma ofrece diferentes tipos de operación. De todos ellos, en este texto, nos centraremos en el primero de ellos, el que está recuadrado que es la operación "tagged" (etiquetado) , que si prestáis atención veréis que es la tiene el valor 81-00 sobre el que hablamos antes, esta es la más frecuente en nuestras redes LAN.



Una vez reconocido el valor 81-00 en una trama Ethernet, sigue analizando los valores de **TCI** (Tag Control Information) que se presentan, en la imagen anterior, con los últimos dos recuadros rojos. Para comprender bien estos campos, os recomendamos ver el video de la charla.

Otra de las grandes capacidades, y en general desconocida, que nos ofrece IEEE-802.1Q, es la de proporcionar **prioridades** al tráfico LAN. En la imagen que sigue, presentamos varios ejemplos concretos de algunas de ellas, por medio de capturas de tráfico. Estas son capturas reales, sobre las que hemos destacado su relación con lo que la norma establece en el punto **I.4** "Traffic types and priority values", a través del campo **PCP** (Priority Point Code), que también figura en la imagen anterior dentro del VLAN TCI.



Las capturas de tráfico presentadas en la imagen anterior, si queréis analizarlas en detalle, podéis descargarlas en nuestra Web, en el menú:

"**Descargas**" —> "**Capturas de tráfico**"

Las mismas son:

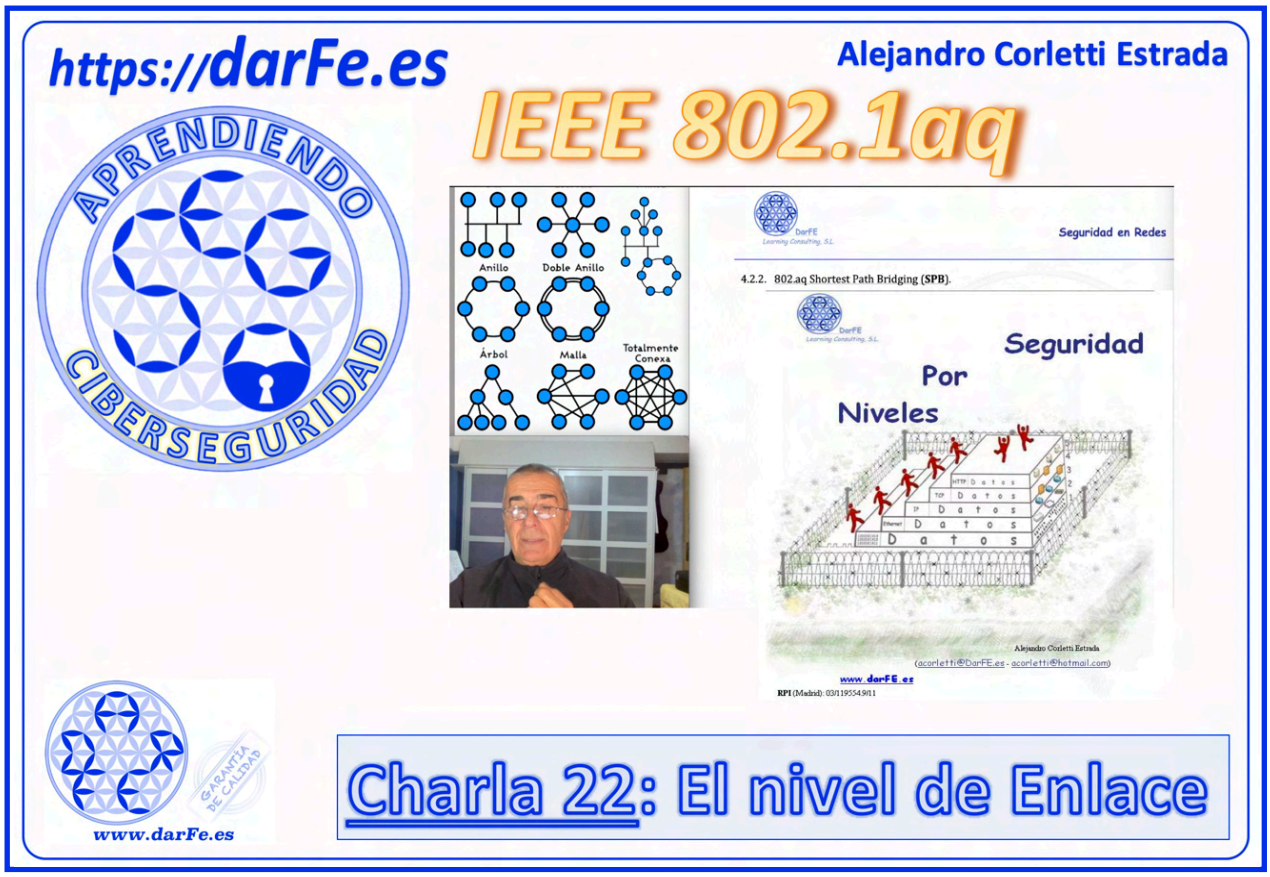
- **802-1q_01.cap**
- **802-1q_02.cap**

Volver al índice

www.darFe.es

Charla 22

Protocolo IEEE 802.1aq



Enlace al Video:

Resumen:

El peor problema de una red jerárquica es que, por error o fallo, se cierre un bucle físico.

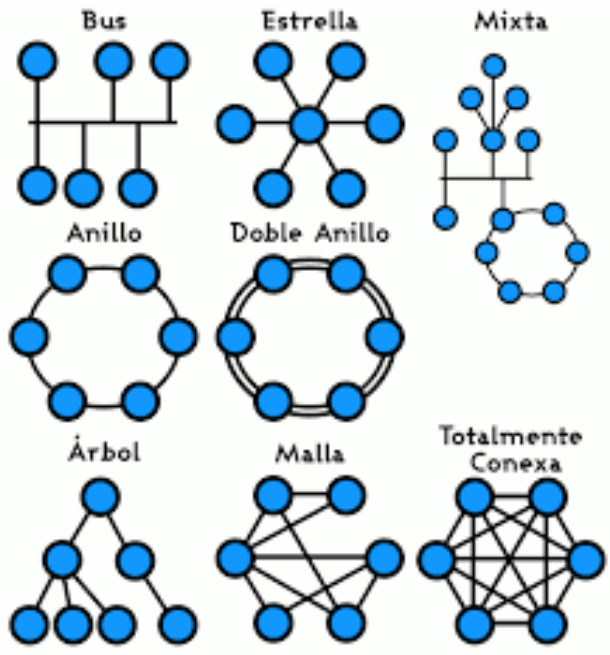
De producirse este fallo, los switchs comenzarán a recibir una misma dirección MAC por diferentes puertos físicos, lo cual es un conflicto difícil de resolver.

La solución inicial nació con el protocolo **IEEE-802.1D** y fue evolucionando hasta llegar a **IEEE-802.1aq**.

En esta charla describimos toda su historia y funcionamiento.

Descripción detallada

El protocolo **IEEE-802.1aq** y su antecesor **IEEE-802.1D**, son protocolos eminentemente orientados a las redes **jerárquicas**.

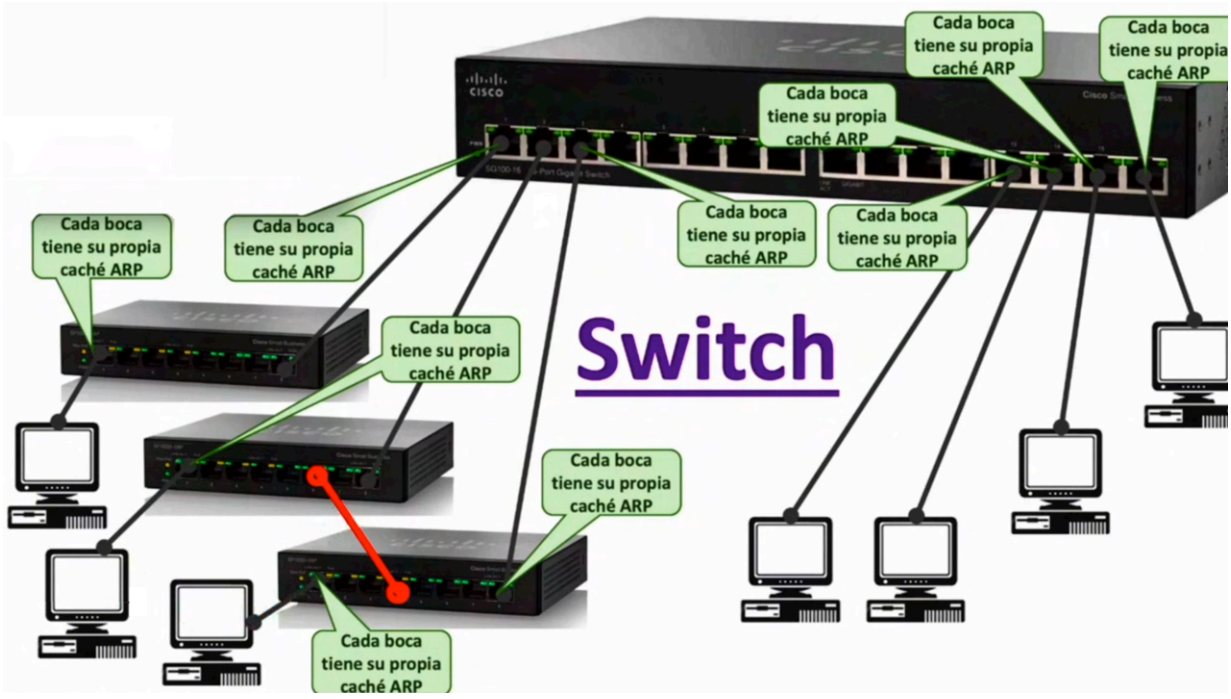


Hasta ahora hemos comenzado presentando, en charlas anteriores, las redes **bus**, que fueron con las que nació el protocolo Ethernet, luego con la aparición de los hubs y los switchs hablamos de las redes **estrella**, y tened siempre presente que, justamente una red estrella si la "cuelgo" de su centro, lo que queda suspendido por debajo pareciera ser una cierta jerarquía o árbol, si a esos nodos "hoja", a su vez les conectamos otras "estrellas colgadas" de ellos, lo que se va formando es una red **jerárquica**.

A nuestra derecha podemos ver de forma gráfica las diferentes **topologías de redes** en una gráfica que nos ofrece Wikipedia..

El peor peligro de una red jerárquica es que se cierre un bucle. Esto que parece algo imposible, en la práctica, cuando tenemos miles de nodos, decenas de switchs, no es tan anormal que suceda. Es tan sencillo como colocar mal un latiguillo dentro de un rack de comunicaciones (armario donde se alojan los dispositivos de red y TI). Los que hemos visitado varios de estos **CPDs** (Centro de Procesamiento de Datos), sabemos que esta situación es mucho más frecuente de lo deseado.

Si volvemos a nuestra imagen de los swichs, esto sería así.



Si recordamos lo hablado en la **charla 18** sobre el envenenamiento de caché ARP, el comentario que hicimos al respecto, es que si un switch, está debidamente bastionado, este ataque no es posible de realizar. En esta charla de hoy, comenzamos a ver la primera de las medidas para bastionar nuestros switchs.

El problema de cerrar un bucle en una red jerárquica, para un Switch es que escucha la misma dirección **MAC** (Medium Access Control) por dos interfaces físicas diferentes, este es un bucle que en principio, no sabría como resolver.

Cuando físicamente se cierra un bucle, la topología pura de red jerárquica, deja de serlo, y se convierte en una red "**Malla**". Para tratar este problema el primer protocolo que lo resolvió fue el protocolo **Spanning Tree** (IEEE-802.1D - STP), creando una red "**Jerárquica lógica**" (o árbol Lógico) sobre esta red "Malla Física". Este protocolo crea "Puentes" (bridges) de unión sobre estos enlaces y define a través de diferentes algoritmos que se pueden configurar, cuál es el que tiene mayor prioridad, este puente de máxima prioridad lo denomina "**Root Bridge**" (o Puente Raíz) y será el que manda jerárquicamente las interfaces por las cuáles se separarán los diferentes dominios de colisión. Todo el control de STP se realiza mediante tramas llamadas **BPDU** (Bridge Protocol Data Unit) que son las que regulan los diferentes dominios de colisión. El parámetro que define esta jerarquía es el **BID** (Bridge Identifier) que está compuesto por el Bridge Priority **+** dirección MAC. El Bridge Priority es un valor configurable que por defecto está asignado en 32768.

En general este protocolo se configura de forma automática, y se basa en el orden de encendido de los diferentes switchs de la red, siendo el primero que se pone en funcionamiento el que se auto designa "**Root Bridge**", pero por supuesto se puede realizar de forma manual.

Cada switch reemplaza los BID de raíz más alta por BID de raíz más baja en las BPDU. Todos los switchs que reciben las BPDU determinan en sus tablas que el switch que cuyo valor de BID es el más bajo será "su" puente raíz, y a su vez envían nuevas BPDU hacia sus otras interfaces con un ID más alto, incrementando el parámetro "**Root Path Cost**" informando con esta nueva BPDU a todo dispositivo que esté conectado físicamente a él cómo debe ir armándose este árbol. Si se desea configurar de forma manual, el administrador de red puede establecer jerarquía que desee configurando la prioridad de switch que sea "Root Bridge" en un valor más pequeño que el del valor por defecto (32768, todo valor debe ser múltiplo de 4096), lo que hace que este BID sea más pequeño y a partir de este "root" puede configurar la jerarquía o árbol si lo desea, o también al reconocer los demás switch a este "root", de forma automática pueden generar el resto del árbol.

Un tema que debemos mencionar, ya que acabamos de desarrollar en la charla anterior el protocolo IEEE-802.1Q (VLAN), es el protocolo Spanning Tree múltiple o **MSTP** (Multiple Spanning Tree Protocol). En el mismo, la extensión ID del sistema puente lleva el número de instancia MSTP. Esta definición tiene lugar pues algunos vendedores propusieron emplear la extensión ID sistema para llevar un ID de VLAN permitiendo un árbol de expansión por cada VLAN que se haya definido en la red.

MSTP es una evolución del protocolo Spanning Tree. Fue introducido en **IEEE-802.1s** como una enmienda a 802.1Q en su edición de 1998, más tarde fusionado con IEEE 802.1Q-2005. Se define esta extensión para poder desarrollar aún más la utilidad de las redes de área local virtuales (VLAN). Si sólo hay una LAN Virtual (VLAN) en la red no se emplea. Si la red contiene más de una VLAN, la red lógica configurada por una sola

STP funcionaría perfectamente, pero es posible hacer un mejor uso de la red (y asegurar su “visibilidad” y “Segmentación”) mediante el uso de un árbol de expansión alternativo para cada VLAN o grupos de VLAN.

Qué puede suceder hasta el estándar IEEE-802.1D. Justamente, este protocolo, como acabamos de describir, a medida que detecta potenciales bucles, va a ir cortando los mismos para evitarlos y volver a su topología jerárquica. Si una persona mal intencionada, comienza a generar ataques de este tipo (envenenamientos de caché ARP reiterados), es posible que el mismo protocolo STP, deje fuera de servicio la misma red, pues llegaría a cerrar los enlaces reales, por interpretarlos como bucles.

Es aquí donde aparece la solución como **IEEE-802.aq** Shortest Path Bridging (**SPB**).

Este protocolo aparece en al año 2006, si bien es alrededor del año 2012 cuando se difunde todo su desarrollo completo. La principal característica que ofrece SPB es que permite mantener “activos” todos los enlaces redundantes, sin necesidad de deshabilitar los bucles físicos (como hace STP), manteniendo una real topología de “Malla”, con ello mejora la eficiencia y los tiempos de convergencia de la red.

La base de SPB es el protocolo de control denominado **IS-IS** (Intermediate System to Intermediate System), regulado por la **RFC-6329** “IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging” de la cual haremos un resumen a continuación.

SPB puede operar de formas:

- Shortest Path Bridging - VID (**SPBV**) Virtual ID: múltiples VLAN se pueden usar para distribuir la carga en diferentes árboles del camino más corto.
- Shortest Path Bridging - MAC (**SPBM**): sus decisiones están basadas en el concepto de “I-SID” (Ethernet Services Instance), se emplea para agrupar “E-LAN” que son enlaces lógicos entre dos interfaces físicas Ethernet, aunque también las VLAN se pueden utilizar para distribuir la carga en diferentes árboles del camino más corto.

En la teoría la gran diferencia para el empleo de uno u otro es que SPBV se pensó para redes de hasta 100 nodos y SPBM hasta 1.000.

Hoy en día a nivel 2 hay que sumar un nuevo problema muy frecuente en grandes redes y es la necesidad de separar lógicamente varias zonas de la mismo switch (o conjunto de switches), lo que se suele llamar **Multitenancy** (Multiple tenencia) y el caso más frecuente, es la necesidad de dar servicio a varios clientes completamente independientes y cuyos flujos de información deben estar debidamente securizados el uno respecto al otro.

Sobre este tema es que surge otra diferencia entre ambos: SPBV utiliza el encapsulamiento Q-in-Q (regulado por **IEEE-802.1ad**), mientras que SPBM utiliza MAC-in-MAC (regulado por **IEEE-802.1ah**).

En grandes líneas:

Q-in-Q no es más que utilizar dos etiquetas para las VLANs, una para el segmento del cliente y otra para el del proveedor. Cuando el tráfico de las VLANs de un cliente entra en la red del proveedor, el mismo se re-encapsula dentro de una nueva VLAN, y así circula por la LAN del proveedor “encapsulando” las VLAN de cada cliente. Esta técnica proporciona 16 millones de posibles "VLANs" (4096 del cliente x 4096 del proveedor).

La técnica de MAC-in-MAC, es similar a la anterior, pero encapsula las tramas del cliente dentro de una nueva trama Ethernet con una MAC del propio proveedor, por lo tanto dentro de la red del proveedor, un cliente enviará y recibirá tráfico identificado por otra MAC diferente. Esta técnica separa completamente los dominios de colisión del cliente y del proveedor, esto optimiza también el tráfico por una cuestión de tablas de aprendizaje diferentes entre cliente y proveedor, por esta razón es que su diseño fue pensado para más dispositivos.

Cabe mencionar que ya existen técnicas más eficientes aún por parte de los diferentes fabricantes (TRILL, MLAG, Qfabric, FabricPath, etc.), y también metodologías de encapsulamiento, pero en la actualidad aún no se encuentran estandarizadas al 100% por lo que no las desarrollaremos en este texto. Es cierto que a la hora de tomar alguna decisión sobre escalar STP es muy probable que hoy por hoy debamos caer en alguna de estas soluciones propietarias pues parece ser que aún no existe un acuerdo unánime por su parte para encarar protocolos estandarizados.

www.darFe.es

Charla 23

PBNAC - IEEE 802.1x

Enlace al Video:

Resumen:

El protocolo **IEEE-802.1x,** es uno de los más importantes de seguridad, en el nivel 2, de nuestras redes LAN. Nos permite regular el acceso a la misma, dejando fuera a quien quiera ingresar hasta que sea debidamente autenticado, y recién ahí se "abre" el puerto físico de entrada, por esta razón es que se llama **PBNAC** (Port Based Network Access Control), trabajando a nivel puerto físico. En esta charla desarrollamos los aspectos fundamentales de la norma, y los compararemos con una captura de tráfico real sobre este protocolo.

Descripción detallada

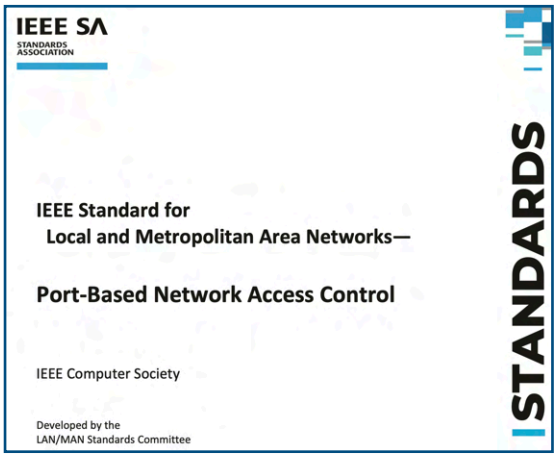
La charla de hoy, la comenzamos con un video anterior, que te invitamos a que veas para comprender bien la idea de "**segregación de entornos**", pues es un concepto clave a la hora de aplicar **IEEE-802.1x** que es el tema del presente capítulo.

El enlace al video es el siguiente:

10 Reglas de Fortificación de Redes:

Del mencionado video, presta especial atención al punto 5. Segregación de entornos.

Ahora sí, entrando en el tema que nos toca, lo haremos teniendo como referencia la norma. **IEEE-802.1x**, que como podéis ver en la imagen de la derecha, su nombre es "**Port Based Network Access Control**" (PBNAC).



Este nombre se debe a que, justamente, este estándar, regula cómo podemos gestionar los accesos a nuestra infraestructura, desde el puerto mismo de nivel de enlace.

En pocas palabras, lo que veremos aquí, es que, si un usuario o dirección MAC, no está debidamente autorizado para ingresar a nuestra red LAN, directamente no tendrá conectividad sobre ese puerto físico del switch, o aéreo si es por WiFi.

De esta norma, comenzaremos presentando el punto 5.3.

5.3 Conformant systems and system components

This clause (Clause 5) specifies requirements and options for implementation of the following components:

a) Port Access Entity (PAE, see 6.3, Clause 12) (5.4, 5.5, 5.6–5.15, 5.18, 5.19)
b) Port Access Controller (PAC, see 6.4) (5.20)

A port for which conformance to this standard is claimed shall implement the mandatory functions of the PAE (5.4) and the mandatory functionality for at least one of the following PAE functions:

— Supplicant (5.6, 5.7)
— Authenticator (5.8, 5.9)
— MACsec Key Agreement (MKA) (5.10, 5.11)

Como se aprecia en la imagen anterior, hay dos componentes clave: **PAE** y **PAC**. De estos dos, el **PAE** puede desempeñar las siguientes funciones: **Supplicant**, **Authenticator** y **MKA**. Sobre la combinación de estas piezas, será lo que desarrollemos en este capítulo.

Avancemos un poco más sobre estos conceptos. A continuación presentamos otra imagen de esta norma, que a primera vista puede parecer complicada, pero es otra de las partes clave.

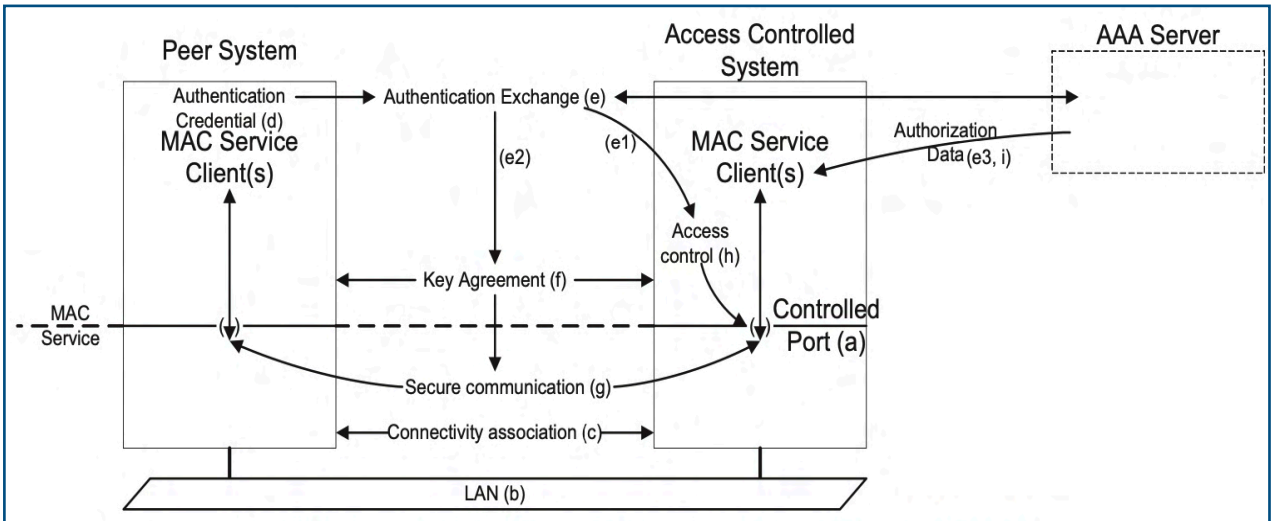


Figure 6-1—Port-based network access control processes

La figura 6.1 de la imagen superior, nos muestra las tres partes intervinientes en el control de este proceso: **Peer System**, **Access Controlled System** y **AAA Server** (Authentication - Authorization - Accounting)

Visto de otra forma, y para que vayamos siendo más concretos sobre estas partes, el estándar IEEE-802.1x, también nos presenta la siguiente imagen que va aclarando su funcionamiento.

En la figura 7.1 podemos apreciar un **host** (a la izquierda de la misma) que está "fuera" de la red asegurada (**Secured Network**), y entre medio de ambos, el **Network Access Point**. Esta figura, tal vez sea la clave para comprender 802.1x: Un host, hasta que **no** sea autorizado, permanecerá fuera de la LAN.

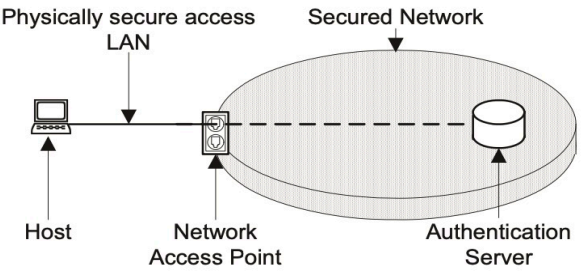


Figure 7-1—Network access control with a physically secure point-to-point LAN

Finalmente presentamos cómo es este diálogo, a través de la figura 8.2 que nos presenta el caso más típico de aplicación de esta norma (no os asustéis que la iremos desarrollando de forma práctica y veréis que hasta parece humanamente comprensible y todo…).

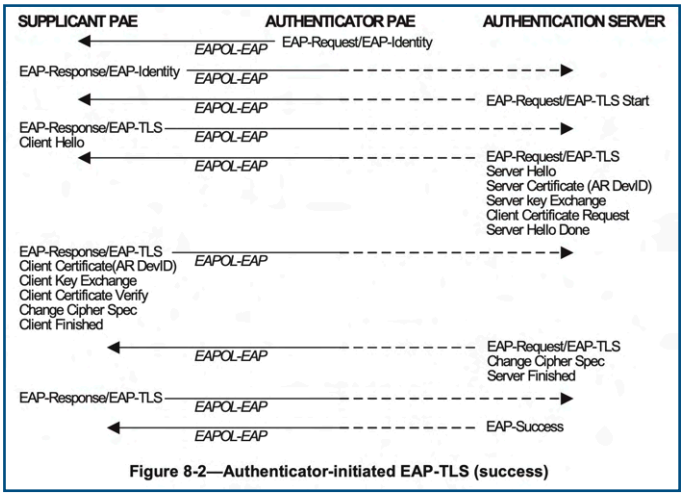


Figure 8-2—Authenticator-initiated EAP-TLS (success)

Lo primero que deseamos destacar es lo de **EAPOL** (Extensible Authentication Protocol Over LAN). Fijaros que las

dos primeras líneas son una solicitud de autenticación/identidad (EAP_Request/EAP-Identity) y una Respuesta a la misma (EAP Response/EAP-Identity).

Una vez que el Authentication Server recibe esta respuesta, comienza EAP-TLS Start. **TLS** quiere decir (Transport Layer Security) que, visto de otra forma, es exactamente lo mismo que "**HTTPS**" (Hiper Text Transport Protocolo Secure) que no es ni más, ni menos que lo que hacemos a diario cuando nos conectamos a casi todos los servidores actuales de Internet. Es el protocolo seguro para navegación Web.

NOTA: Para navegar por Internet, tenemos dos protocolos estandarizados:

a. **HTTP**: Hiper Text Transport Protocol, que emplea el puerto TCP 80 y es inseguro.

b. **HTTPS**: HTTP Secure, que emplea el puerto TCP 443 y es seguro

Este último está estandarizado como **TLS**.

Estos temas los desarrollaremos en detalle más adelante.

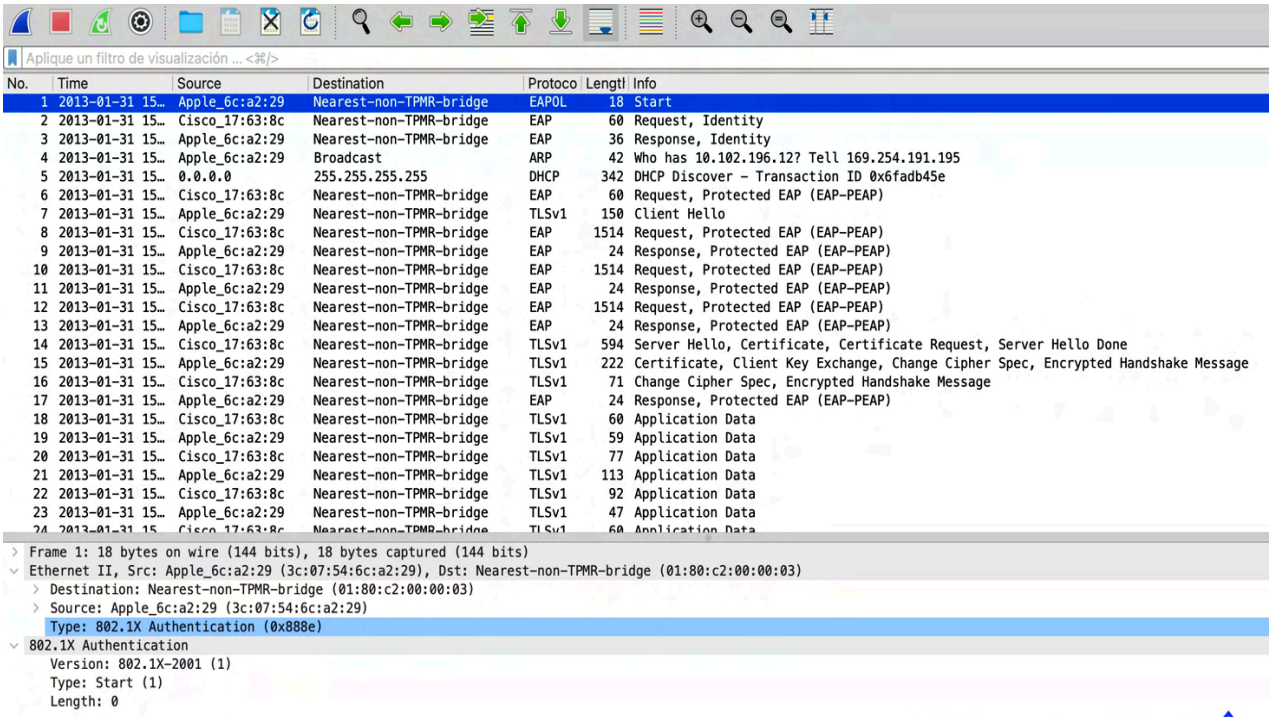
En el video de esta charla, se propone descargar de nuestra Web, en el menú:

"**Descargas**" —> "**Capturas de tráfico**"

La siguiente captura: **Protocolo_802.1x-Autenticacion-EAP.pcap**

En la misma se puede estudiar con todo detalle, la secuencia **EAPOL** que nos presenta la **Figura 8.2** de la norma (Imagen anterior).

A continuación, se presenta una imagen de esta captura de tráfico, la explicación de la misma, es mejor verla directamente desde el video de esta charla 23.



Volver al índice

www.darFe.es

Charla 24

MacSec - IEEE 802.1ae

Enlace al Video:

Resumen:

El protocolo **IEEE-802.1ae,** o también conocido como **MACSec**, nos ofrece la posibilidad de aplicar Autenticación, Confidencialidad e Integridad a nivel de enlace. Esto nos abre un mundo muy interesante para asegurar nuestras comunicaciones LAN, e inclusive, como veremos al final, también para entornos **Cloud**.

Como forma parte de la familia **IEEE-802.x**, veremos que también es compatible con **IEEE-802.1X** e **IEEE-802.1Q**, que los vimos en charlas anteriores.

Descripción detallada

Comenzamos presentando el tema a través de un documento del **CCN** (Centro Criptológico Nacional, de España), que se denomina "**Recomendaciones de Seguridad para MACSec**" y podéis descargarlo desde este mismo título, pues tiene el híper vínculo al artículo.

En este documento, destacamos la imagen que sigue, pues en ella podemos ver cómo luego de los campos dirección origen y destino (en verde) de la trama Ethernet, se inserta este nuevo encabezado de MACSec para poder justamente introducir parámetros de seguridad a nivel enlace, cosa que, antes de MACSec era imposible.

En realidad lo que estamos viendo es que el valor del campo Ethertype, al contener "**88e5**", a partir de este, ya queda establecido que estamos empleando MACSec.

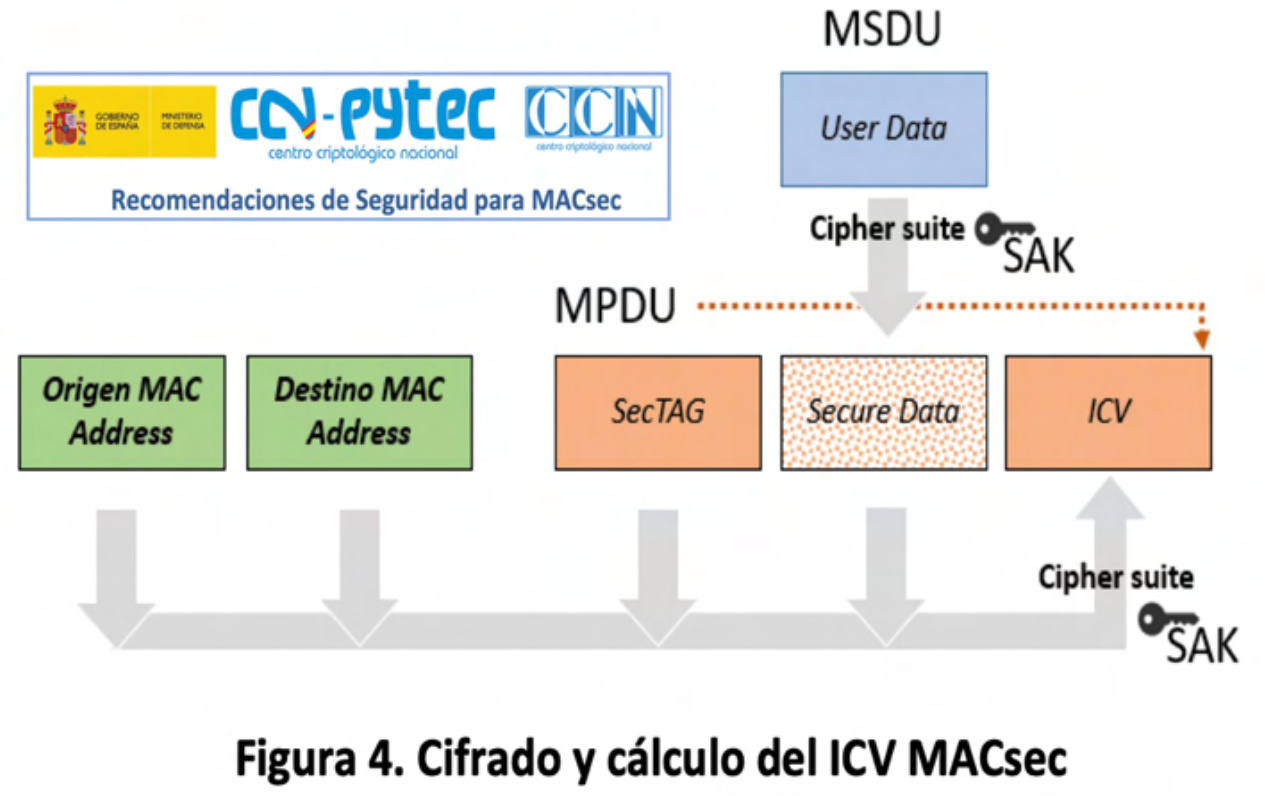
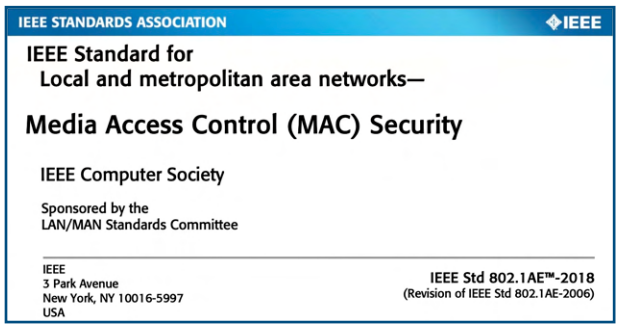


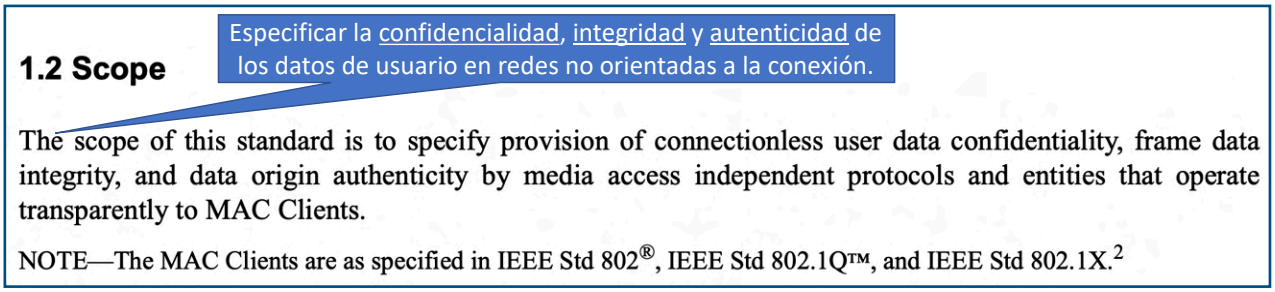
Figura 4. Cifrado y cálculo del ICV MACsec

Continuemos el tema apoyándonos en el estándar **IEEE-802.1ae** que es su referente.

Como podemos ver en la imagen de la derecha, MACSec viene de Media Access Control (MAC) Security y su última versión fue publicada en el año 2018.



El punto 1.2 Scope de esta norma, nos indica que su función es especificar la confidencialidad, integridad y autenticación de los datos en redes no orientadas a la conexión.



Prestad atención a la última línea de la imagen de arriba, pues nos dice claramente que los clientes están especificados en **IEEE-8021Q** e **IEEE-802.1X**, que son los temas que acabamos de ver en las charlas 21 y 23. Esto es importante, pues ratifica la capacidad que posee toda la familia 802.x para trabajar de forma sincronizada.

Hagamos un alto, para aclarar los conceptos mencionados (confidencialidad, integridad y autenticación), pues hay una palabra que siempre ponemos de manifiesto en Ciberseguridad: **ACIDA**. El significado es el siguiente.

- Autenticación: Garantizar que "es quien dice ser"
- Confidencialidad: Garantizar que a los datos y a los sistemas solo accedan personas debidamente autorizadas.
- Integridad: Garantizar la exactitud de la información y de los sistemas contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
- Disponibilidad: Garantizar que la información y los sistemas pueden ser utilizados en la forma y tiempo requeridos
- Auditabilidad: (También llamado "Trazabilidad"). Garantizar que cualquier acción o transacción pueda ser relacionada unívocamente, asegurando el cumplimiento de controles claves establecidos en las correspondientes normativas.

En la imagen que sigue, podemos ver varias figuras de la norma IEEE-802.1ae, que a través de diferentes colores, iremos relacionando paso a paso.

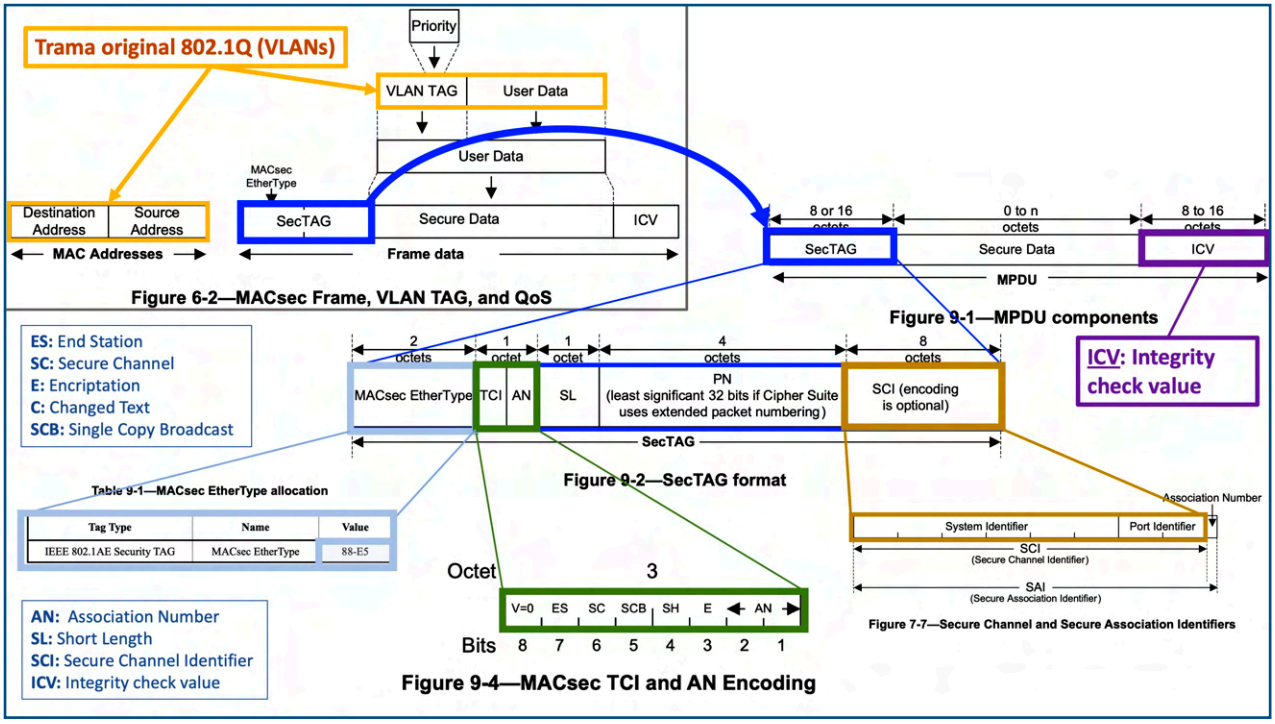
La figura **6-2** (arriba a la izquierda) nos presenta una primera relación que hemos **resaltado en amarillo**, con el estándar **IEEE-802.1Q**, y esto se debe a que podemos perfectamente aplicar MACSec dentro de cualquier VLAN, pues fijaros que aparece una **VLAN TAG** que ya está dentro del contenido de los "**User Data**" que serán securizados. En esta Tag, como podemos ver, nos permite a su vez respetar las prioridades (Priority) de cada VLAN.

Lo segundo a desarrollar, es lo que hemos **remarcado en azul,** que nos relaciona la figura **6-2** con la **9-1** y nos servirá para comprender el formato del **SecTAG** (TAG, quiere decir etiqueta).

El tercer campo, que hemos **remarcado en violeta**, es el **ICV** (Integrity Check Value), que será el que nos ofrezca el control de Integridad.

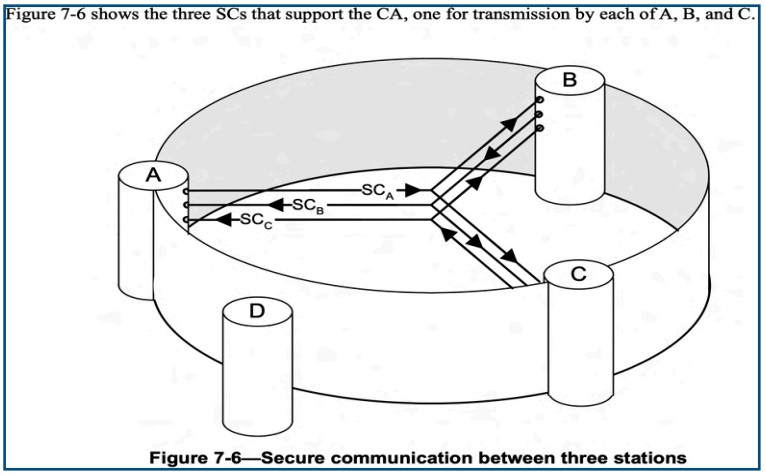
En **verde hemos resaltado** el octeto correspondiente a **TCI-AN** (Tag Control Information- Association Number) pues, como desarrollaremos a continuación, es muy importante, y **finalmente en dorado**, el **SCI** (Secure Channel Identifier) que también lo

veremos al final. Los cuadros remarcados en azul claro (o celeste como decimos en Hispanoamérica), son descriptivos de las diferentes abreviaturas.



Otra Figura del estándar que es muy ilustrativa, es la **7-6**, pues en ella podemos ver claramente que MACSec crea canales seguros (**SC**: Secure Channel) de forma dirigida, es decir punto a punto.

En esta imagen podemos ver que hay cuatro nodos (A, B, C y D) y que existen tres canales seguros SC_A, SC_B y SC_C. Es decir, esta red LAN, el nodo "D" no aplica MACSec.



Volvamos al documento del **CCN** de España, con la imagen que sigue abajo. En la parte superior vemos que es posible aplicar **IEEE-802.1x** (PBNAC) para poder generar una autenticación robusta y generar una clave de sesión (**MSK**: Master Swift Key). En el siguiente recuadro, vemos que a través de esa MSK se pueden derivar dos nuevas claves, una clave de Encriptación y otra de Integridad (**KEK** e **ICK).** En el tercer recuadro, vemos también que de esta primer clave se deriva la clave para esa asociación **SAK** (Secure Association Key). Tengamos en cuenta que todas estas claves son para cada **SC** (Secure Channel) como acabamos de ver en el párrafo anterior (SC_A, SC_B y SC_C). Una vez seleccionadas las suites de cifrado que soportan esos hosts, recién allí entraría en juego IEEE-802.1ae (recuadro final de la imagen).

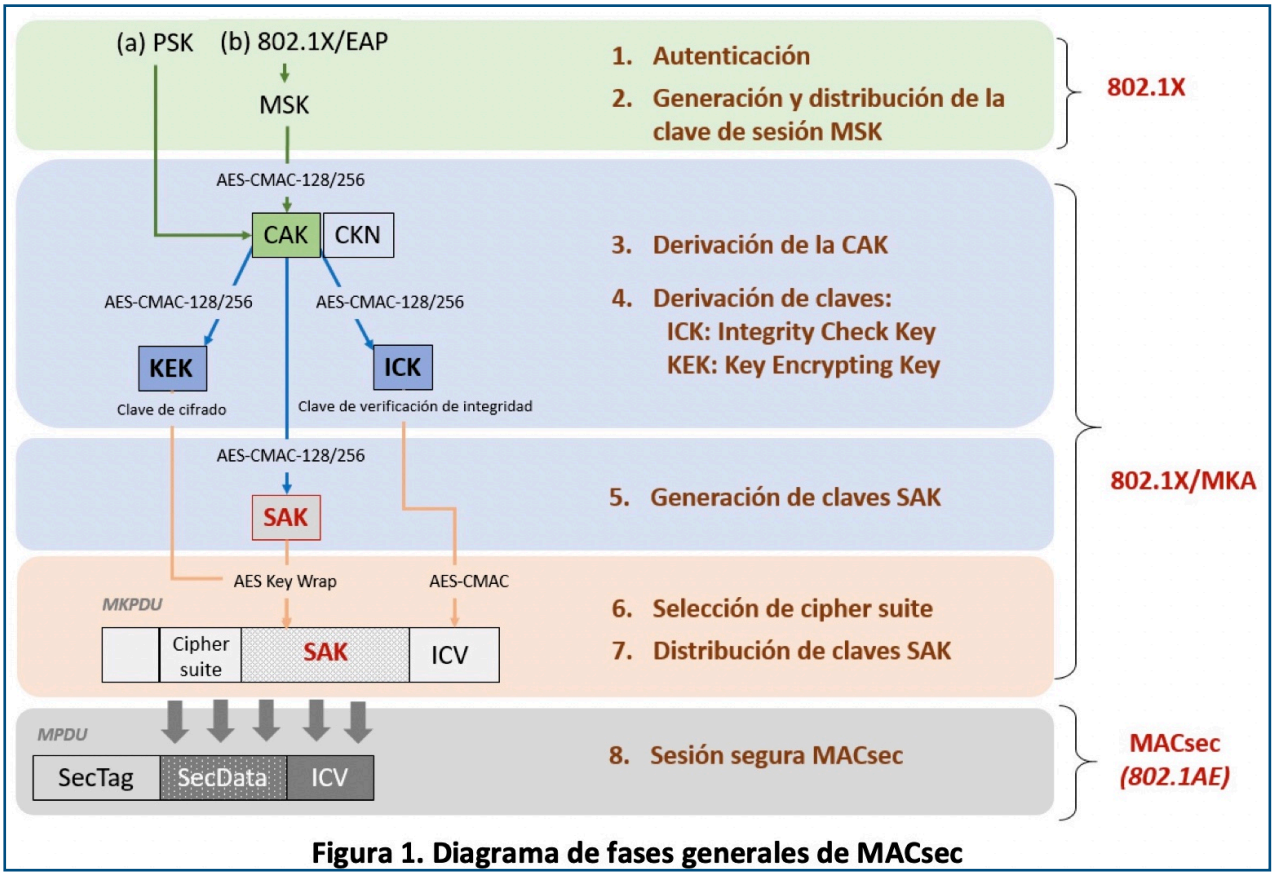
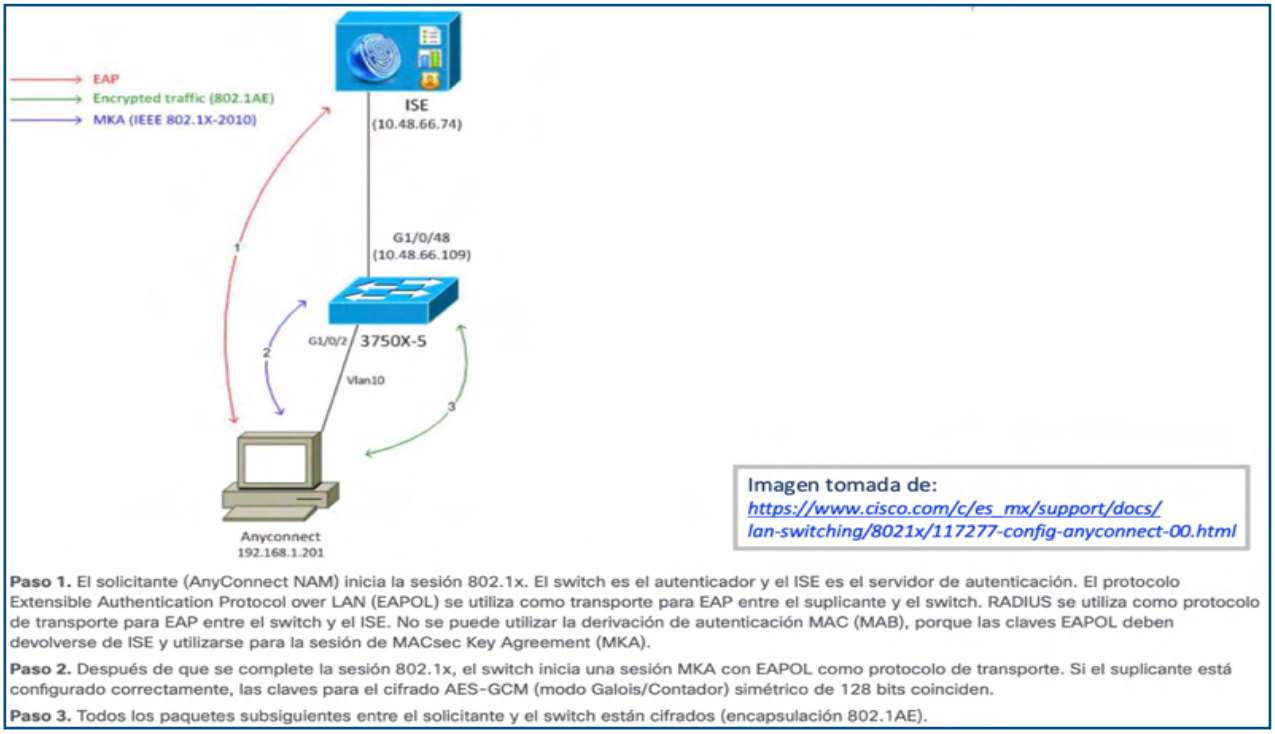


Figura 1. Diagrama de fases generales de MACsec

Por último veamos una configuración real de estos protocolos, en este caso, sobre un dispositivo **Cisco ISE** (Internet Security Engine), en la cual, a través del software (también de Cisco) **AnyConnect**, un usuario puede insertarse en esta infraestructura de seguridad, empleando cada uno de los protocolos que acabamos de presentar.



Paso 1. El solicitante (AnyConnect NAM) inicia la sesión 802.1x. El switch es el autenticador y el ISE es el servidor de autenticación. El protocolo Extensible Authentication Protocol over LAN (EAPOL) se utiliza como transporte para EAP entre el suplicante y el switch. RADIUS se utiliza como protocolo de transporte para EAP entre el switch y el ISE. No se puede utilizar la derivación de autenticación MAC (MAB), porque las claves EAPOL deben devolverse de ISE y utilizarse para la sesión de MACsec Key Agreement (MKA).

Paso 2. Después de que se complete la sesión 802.1x, el switch inicia una sesión MKA con EAPOL como protocolo de transporte. Si el suplicante está configurado correctamente, las claves para el cifrado AES-GCM (modo Galois/Contador) simétrico de 128 bits coinciden.

Paso 3. Todos los paquetes subsiguientes entre el solicitante y el switch están cifrados (encapsulación 802.1AE).

Como se aprecia en la imagen anterior, en el paso 1 inicia IEEE-802.1x, en el paso 2 inicia una sesión MKA con EAPOL y en el paso 3 aplica encapsulamiento IEEE-802.1ae.

Pasemos a ver toda esta teoría, pero ahora a través de una captura de tráfico.

Las capturas de tráfico que presentaremos, si queréis analizarlas en detalle, podéis descargarlas en nuestra Web, en el menú:

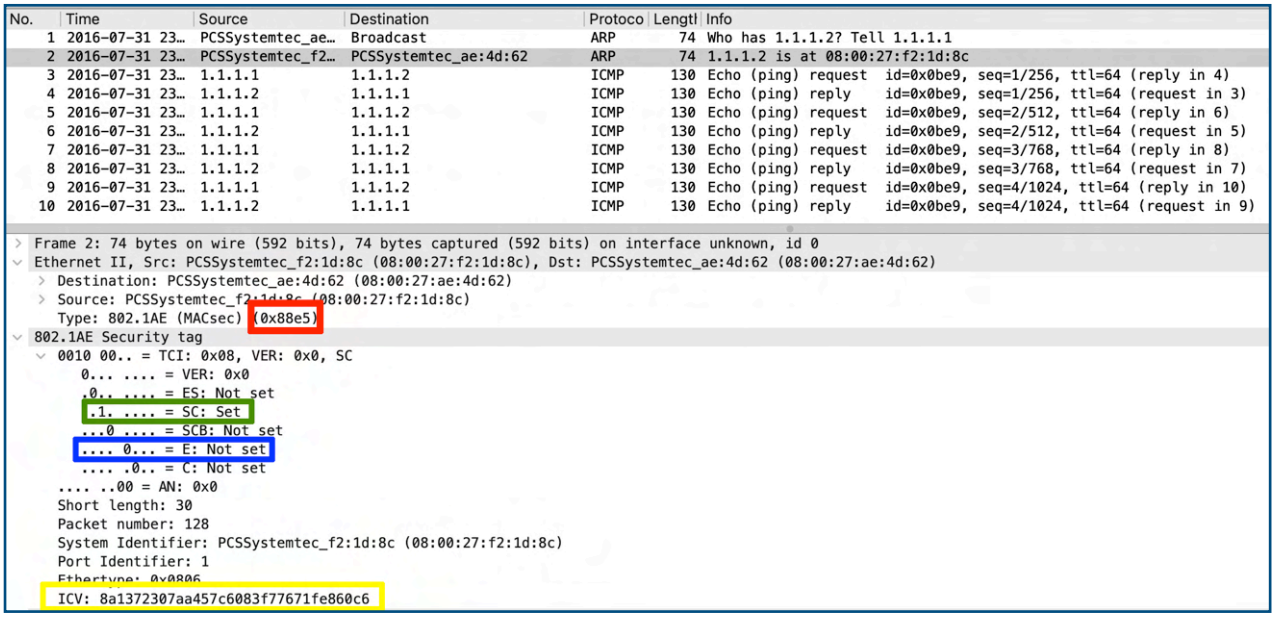
"**Descargas**" —> "**Capturas de tráfico**"

Las mismas son:

Protocolo_802.1ae_MacSec_Sin-Encriptar.pcap

Protocolo_802.1ae_MacSec_trunc-Encriptado.pcap

A continuación vamos a estudiar este tema presentando una imagen de la captura **Protocolo_802.1ae_MacSec_Sin-Encriptar.pcap**, que como su nombre lo indica NO está aplicando criptografía (Encriptación) de los datos.

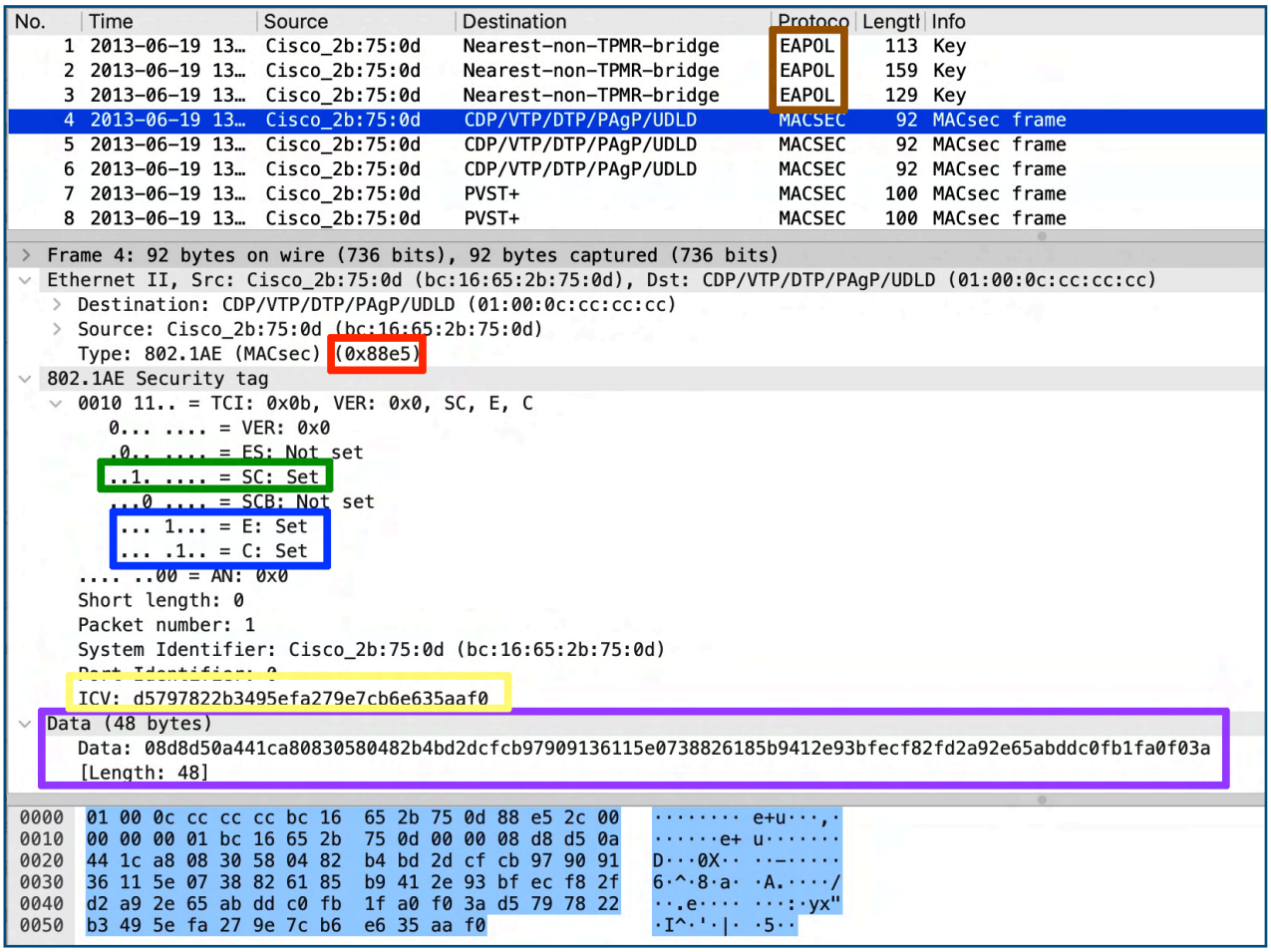


Nuevamente, hemos resaltado en diferentes colores los campos que nos interesa analizar. El primero de ellos, que hemos remarcado en **rojo**, nos presenta el valor que ya mencionamos **88e5**, con lo que Wireshark inmediatamente nos indica que se trata de 802.1AE (MACSec). El otro campo que nos interesa es el que remarcamos en **verde**, que al encontrarse a "**1**" este bit, nos indica que nos encontramos en un canal seguro (**SC Set**). Sin embargo, podemos ver, remarcado en **azul**, que el bit de encriptation "**E**" está puesto a "0" con lo que nos indica que en este canal seguro NO se está empleando criptografía, o confidencialidad de los datos, por esa razón es que Wireshark en toda esta captura nos indica, por ejemplo que a nivel superior, se trata de protocolo ICMP pues todo lo que sigue a esta encabezado está en texto plano. Si estuviera empleando este bit "**E = 1**", Wireshark no podría saberlo, pues todo lo demás estaría criptografiado. Por último, remarcamos en **amarillo**, el campo **ICV**, que nos

muestra que este ese control de Integridad de esta trama, que nos demuestra que esto sí que se está implementando.

A continuación presentamos un pantallazo de la otra captura de tráfico que os invitamos a descargar: **Protocolo_802.1ae_MacSec_trunc-Encriptado.pcap** para que podáis ver otro ejemplo, en el que los datos sí viajan aplicando criptografía.

Al principio de la misma, hemos remarcado en **marrón**, el diálogo **EAPOL**, que recordad que era una formas de negociar las claves que ofrecía **IEEE-802.1x**, tal cual acabamos de presentar en la última imagen del documento del CCN, y que fue un tema que tratamos también en charlas anteriores. En estas tres primeras tramas EAPOL, se genera la **MSK** (Máster Swift Key) que será el punto de partida de todas las demás claves para esta sesión en concreto (volver a la imagen última del CCN).



Hemos remarcado en **rojo**, al igual que en la captura anterior, cómo nos presenta el valor que ya mencionamos **88e5**, indicándonos que se trata de **MACSec**.

El otro campo que nos interesa es nuevamente el que remarcamos en **verde**, que al encontrarse a "**1**" este bit, nos indica que nos encontramos en un canal seguro (**SC Set**).

A continuación, podemos ver una nueva combinación, diferente a la anterior, en esta captura que sigue, hemos remarcado en **azul** estos dos campos, que ahora sí están a "**1**" y nos indican que ahora se está empleando criptografía, el primero de ellos es el bit "**E**" de Encriptation, y el segundo es el bit "**C**" de Change text, que aclara que ahora el texto que sigue ha sido cambiado, justamente por texto criptografiado. Por esta razón

es que el campo data que hemos remarcado en **violeta**, ahora Wireshark no lo sabe interpretar (Como sí lo hizo con ICMP en la imagen anterior), pues todos esos "**Data**" son caracteres criptografiados.

Finalmente, al igual que la imagen anterior, remarcamos en **amarillo**, el campo **ICV**, que nos muestra que este ese control de Integridad de esta trama, que nos demuestra que esto sí que se está implementando.

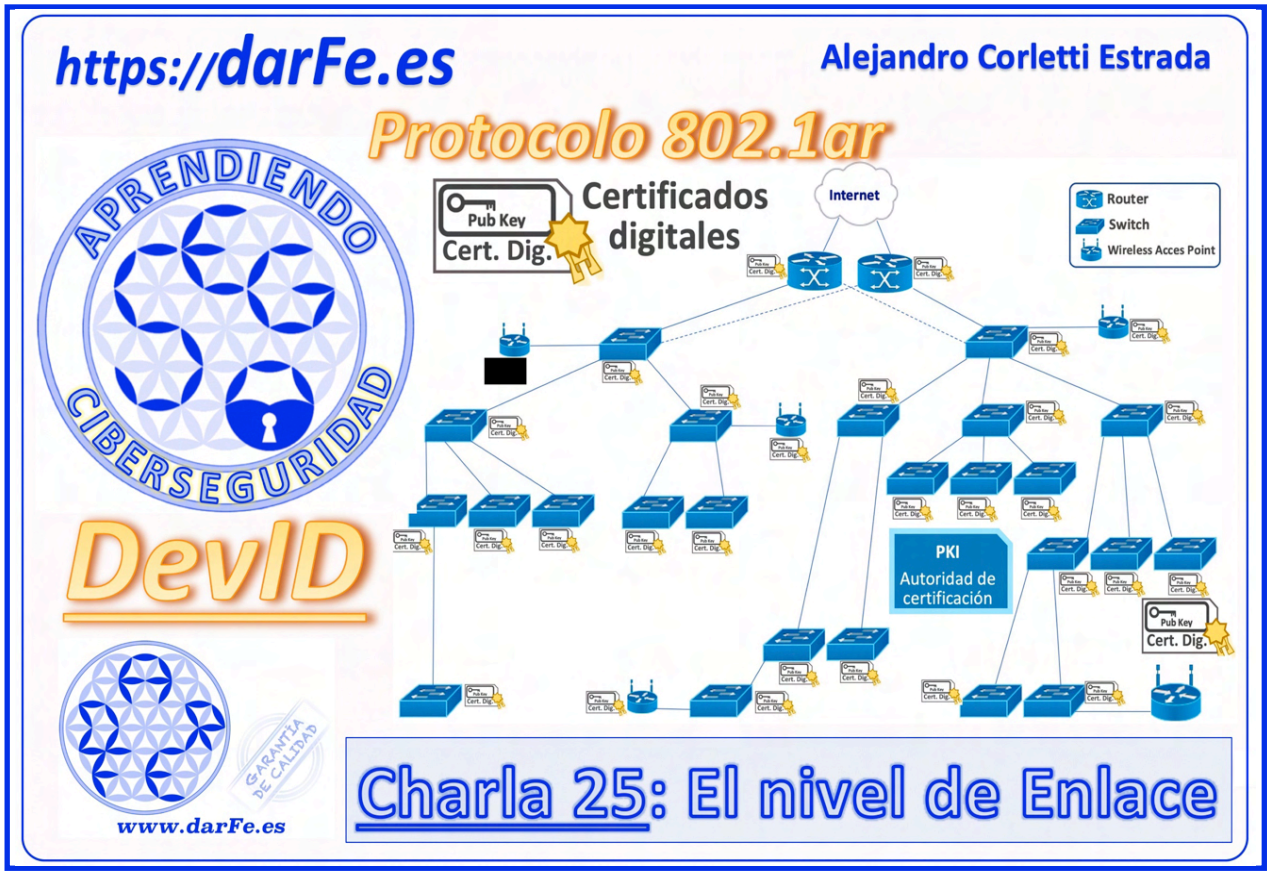
Un aspecto interesante de este protocolo, es que ya se está empleando en entornos **Cloud** para que los diferentes clientes se comuniquen entre sí empleándolo. Por ello tenedlo en cuenta si operáis en estos entornos, pues ya está disponible. Lo ofrecen, por ejemplo, AWS, Azure, etc.

Volver al índice

www.darFe.es

Charla 25

DevID - IEEE 802.1ar



Enlace al Video:

Resumen:

Esta charla, presenta el protocolo **IEEE-802.1ar**, también conocido como **DevID**.

Se trata de una pieza fundamental a la hora de garantizar la entrada en producción de los dispositivos de red, pues como veremos, los fuerza a superar un desafío de autenticación, empleando lo que hemos visto en el capítulo anterior sobre **IEEE-802.1X** y por medio de **certificados digitales**.

Descripción detallada

La charla de este capítulo se basa en el estándar **IEEE-802.1ar**, también conocido como **DevID**. Veremos que es otro de los estándares muy importantes en nuestros entornos LAN, pues nos ofrece una metodología segura para lo que se denomina "**Enrollment**" (inscripción, matriculación).

Esto del enrollment, en nuestro ámbito se suele denominar **entrada en producción**. De hecho, en nuestro libro "**Seguridad en Redes**" (que reiteramos, podéis descargar gratuitamente de nuestra Web: **https://darFe.es**), tenéis desarrollado en el punto 3.1 Entrada en producción, con los aspectos clave a considerar.

La idea del procedimiento de entrada en producción, es el conjunto de pasos a seguir desde que un dispositivo, plataforma o servicio es "imaginado", pensado o planificado, hasta que el mismo entra en producción.

Desde el punto de vista de la Ciberseguridad, un administrador de redes y/o TI, debe prestar especial atención a que los dispositivos que se conectan a la red, cumplan con las medidas de seguridad adecuadas, caso contrario, aparecerán eslabones débiles que serán puertas de entrada casi con certeza a intrusos, o malware.

El caso más frecuente que se suele encontrar es, por ejemplo, con los puntos de acceso WiFi. Hoy en día con la movilidad, es muy frecuente, que si no se considera esta opción de forma seria y regulada en la empresa, los empleados, conecten a la boca de red de su puesto de trabajo, cualquier router WiFi, y si la red no está suficientemente bastonada, los administradores ni se enterarán, y ese empleado tiene la facilidad de trabajar desde el office, o desde la terraza tomando sol. Estos casos, y mucho otros más, son sumamente peligrosos, pues así como se conecta ese empleado, cualquier otra persona puede también hacerlo, y se ha abierto una puerta trasera, con las medidas de seguridad que ese empleado haya decidido poner, o no, a su libre albedrío.

La implantación del protocolo **DevID** es una excelente medida para evitar este tipo de debilidades.

La forma óptima de implantar este protocolo, es haciendo uso de **certificados digitales**.

Un certificado digital, es una metodología que, basada en **criptografía asimétrica** (tema que veremos en detalle bastante más adelante), permite que una **autoridad de certificación**, que puede ser pública, privada o inclusive interna de mi empresa u organización (que es lo que nos propondría básicamente DevID) genere un par de claves **pública** y **privada** y las "firme" como si fuera un notario virtual, y con ello genere un certificado digital que permite al propietario del mismo validar que es quien dice ser (autenticación), también emplear criptografía y firmar información.

Hoy en día, es muy frecuente su uso, para validarnos ante delegaciones oficiales, realizar trámites on Line, etc. En España, por ejemplo, existe la **Fábrica Nacional De Moneda y Timbre** (FNMT) que emite este tipo de certificados digitales de forma gratuita a los ciudadanos,

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

es justamente una **autoridad de certificación** que tiene validez a nivel Nacional, y una vez descargado este certificado en nuestros dispositivos, podemos operar con cualquier organismo oficial de forma segura.

De hecho, los diplomas de finalización de nuestro curso gratuito de "**Técnico en Ciberseguridad**", los firma personalmente Alejandro Corletti Estrada, a través de su propio certificado digital emitido por la **FNMT**, con lo que garantiza que es diploma firmado digitalmente tiene validez a la hora de presentarse en cualquier sitio, pues puede ser verificada su **autenticidad** e **integridad**.

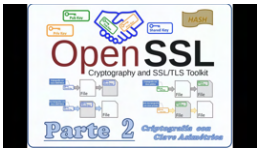
(*Es una orgullo para nosotros informar que este curso ha superado los* **16.000** alumnos).

Para seguir adelante con el tema de hoy, preferimos no entrar en más detalles sobre certificados digitales, pues es un tema demasiado importante como para resumirlo en pocas páginas, por esa razón, más adelante os aseguramos que lo explicaremos con todo el lujo de detalle que hace falta.

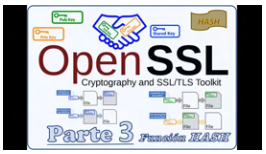
Por ahora, para los más curiosos e inquietos, podéis ir avanzando sobre este tema, viendo nuestro ciclo de videos sobre **OpenSSL**, en los siguientes enlaces:

- **OpenSSL (Parte 1) - Criptografía con clave simétrica:**

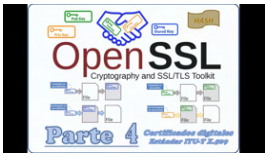
- **OpenSSL (Parte 2) - Criptografía con clave asimétrica:**

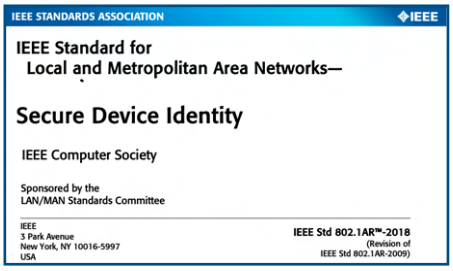


- **OpenSSL (Parte 3) - Función Hash:**



- **OpenSSL (Parte 4) - Certificados digitales (Estándar ITU-T X.509):**





Volviendo a nuestro estándar **IEEE-802.1ar**, tomaremos como referencia la última versión de 2018, que como podéis ver en la imagen de la izquierda, su nombre es **Secure Device Identity**.

Como siempre, presentaremos los aspectos más relevantes de esta norma. En su introducción, una vez

más podemos ver la compatibilidad de toda esta familia IEEE-802.x pues, fijaros que hace mención a su uso con IEEE-802.1X (MACSec) que acabamos de ver en el capítulo anterior.

A continuación, en el punto 1.2 Purpose, nos indica claramente que su propósito es establecer enlaces criptográficos en los dispositivos para **autenticarlos** y facilitar el **servicio de provisión**.

Introduction.

This standard specifies Secure Device Identifiers (DevIDs) for use with IEEE **Std 802.1X** and other industry standards and protocols that authenticate, provision, and authorize communicating devices.

1.1 Scope

This standard specifies unique per-device identifiers (DevID) and the management and cryptographic binding of a device to its identifiers, the relationship between an initially installed identity and subsequent locally significant identities, and interfaces and methods for use of DevIDs with existing and new provisioning and authentication protocols.

1.2 Purpose

This standard defines a standard identifier for IEEE 802 devices that is cryptographically bound to that device, and defines a standard mechanism to authenticate a device's identity. This facilitates secure device provisioning.

Texto

6. Secure Device Identifiers (DevIDs) and their use

This clause describes DevIDs and their use. It provides the context necessary for understanding the DevID module and its operation, as specified in Clause 7.

A DevID comprises:

a) A DevID secret (6.1) that is the private key portion of a public-private key pair;

b) A DevID certificate (6.2) containing the corresponding public key and a subject name that identifies the device; and

c) The certificate chain (6.3) from the DevID certificate up to a trust anchor contained in the DevID trust anchor store (see 6.4) available to potential authenticators.

NOTE—If the DevID trust anchor store includes the certi
there need not be an explicit certificate chain on the device.

1 recordatorio

FIF

Finalmente, de la imagen anterior, deseamos destacar el punto 6. Secure Devices Identifiers, el cual nos indice que DevID está compuesto por:

a) Un Secreto (clave privada)

b) Un certificado (que contiene la clave pública)

c) Una cadena de certificación

Quedémonos con estos tres conceptos.

La figura **6-1,** nos muestra este proceso. Cuando se adquiere un nuevo dispositivo, es muy común que para poder hacer su provisión de forma segura, el fabricante ya nos lo envíe con su propio certificado, firmado, justamente por él (Cisco, Juniper, Huawei, Ericsson, etc.). Esta es la columna de la izquierda de la Figura. Manufacturing CA: Autoridad de certificación del fabricante. Este puede sernos de utilidad como primer paso de su entrada en producción, luego, lo recomendable, sería lo que nos indica también este figura 6-1, de cambiar el mismo por una credencial generaron por una CA Local.

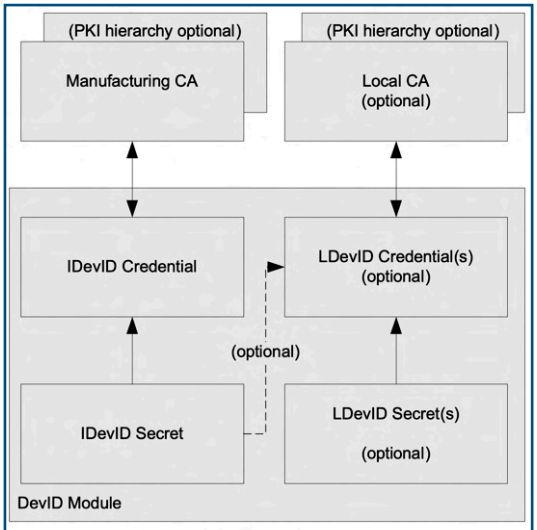


Figure 6-1—DevID trust hierarchy

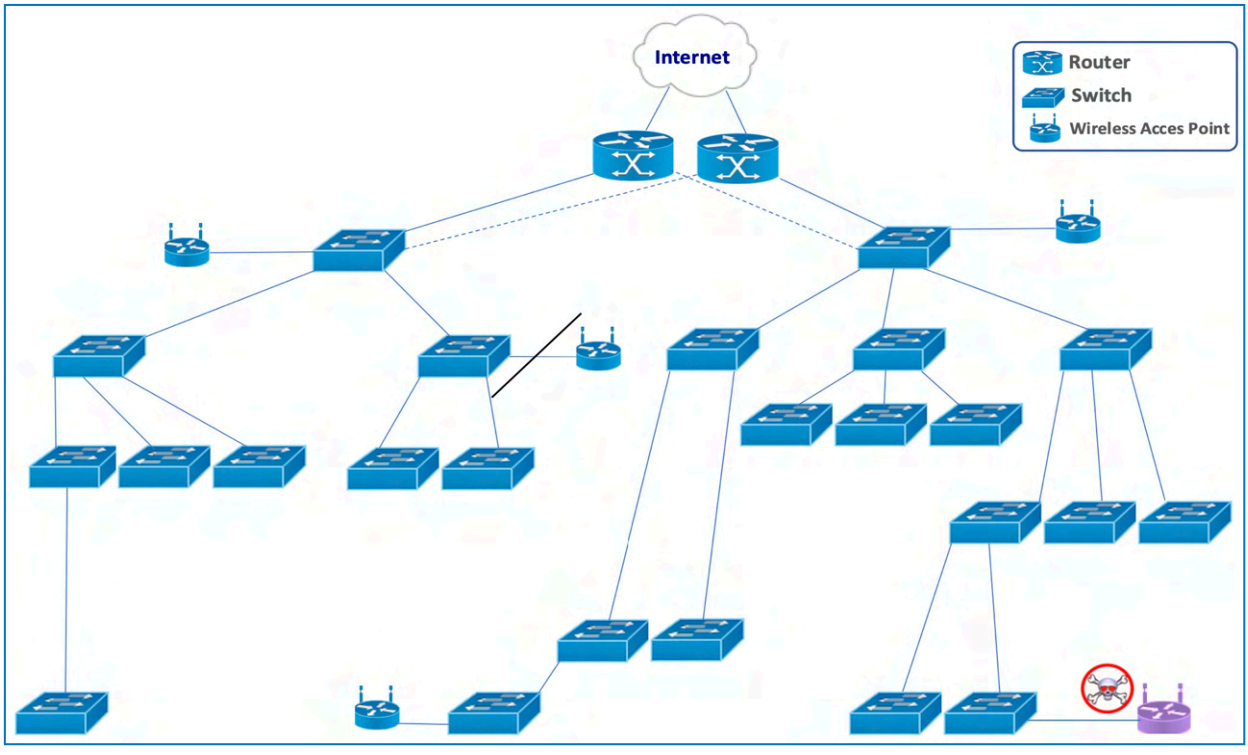
Otro concepto de este estándar que nos interesa es la de la tabla 8-1 que se presenta a continuación.

Table 8-1—DevID certificate and intermediate certificate fields

Field name	RFC 5280 type	Value	Reference
version	INTEGER	3	8.1
serialNumber	INTEGER	Positive integer	8.2
signature	AlgorithmIdentifier	See Clause 9	8.3
issuer	Name	Name of issuing CA	8.4
validity	UTCTime or GeneralizedTime	notBefore (earliest) and notAfter (latest) use	8.5
subject	Name	Name of the DevID device	8.6
subjectPublicKeyInfo	SubjectPublicKeyInfo	The DevID public key	8.7
signatureAlgorithm	AlgorithmIdentifier	See Clause 9	8.8
signatureValue	See Clause 9	See Clause 9	8.9
extensions	Extensions	See Table 8-2	8.10

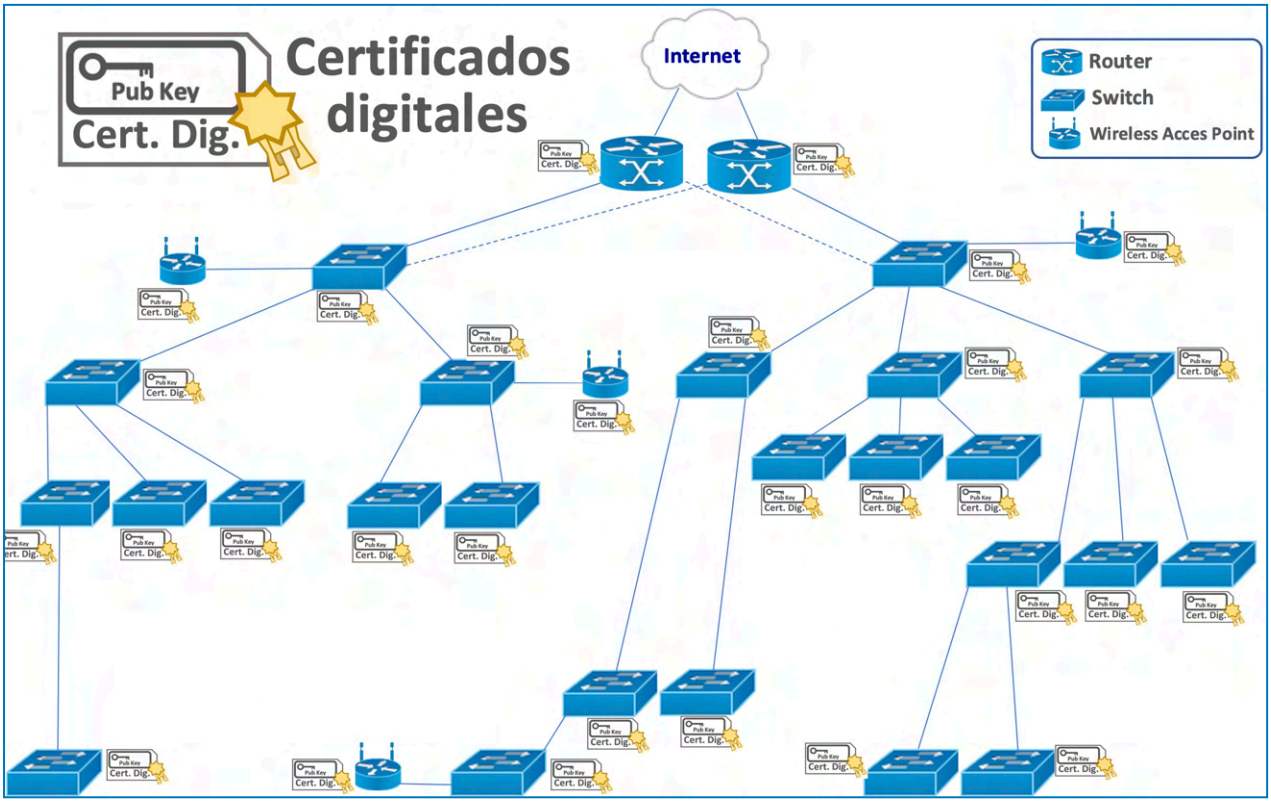
Esta tabla, nos indica los campos básicos que debemos tener en cuenta en estos certificados digitales. Esta tabla se basa (tal cual se indica en la segunda columna) en la **RFC 5280** "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (**CRL**)" que es la que se suele tomar como referencia de certificados digitales, a su vez fijaros que presenta el formato "**X.509**" que son los que más se suelen emplear, digamos que es el tipo de certificado por excelencia.

Avancemos ahora de forma práctica. A continuación se presenta una representación de una red LAN típica.

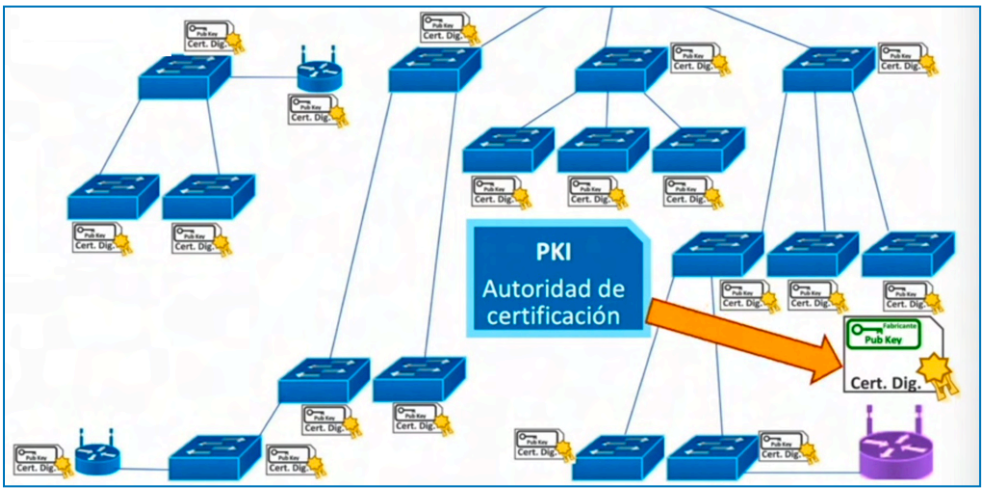


En la imagen anterior, se destaca (abajo y a la derecha) lo que justamente no deseamos que suceda. Es decir, DevID lo que debe asegurar, es que no quepa la posibilidad de que se conecte a nuestra infraestructura un dispositivo que no haya pasado por toda la secuencia que se establezca para la entrada en producción (enrollment).

La metodología que nos propone DevID, es la que presentamos en la imagen que sigue, en la cual, todo el proceso de enrollment, se basa en certificados digitales (del fabricante y/o local), y cualquier dispositivo que no cuente con uno de ellos, no tendrá acceso a la red, directamente a nivel LAN. Para ello, es que se apoya en **IEEE-802.1X**, pues cuando cualquier dispositivo, se enciende y conecta a la LAN; será un "**supplicant**" tal cual vimos en el capítulo anterior, y el punto de acceso (802.1X) le solicitará que se valide con su certificado digital, si no lo tiene, directamente a nivel puerto físico (**PBNAC**) no le habilitará el mismo, con lo que no tendrá conectividad alguna.



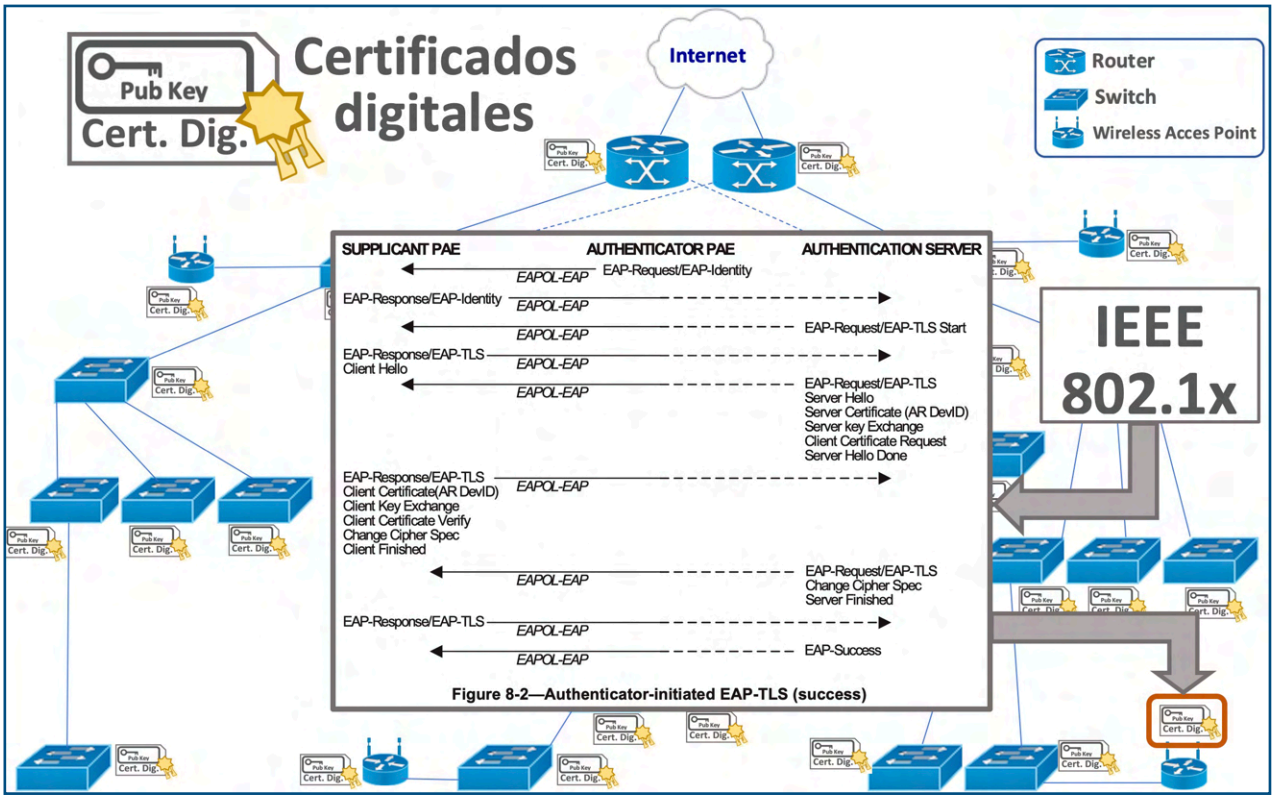
En una infraestructura como la imagen anterior, si un dispositivo quisiera ingresar a la misma, sino poseyera su certificado, no podría.



El proceso del enrollment debería ser como se presenta en la imagen que figura a la derecha, en nuestro caso, empleando una Autoridad de certificación

interna de nuestra empresa.

Finalmente, para que este nuevo dispositivo logre ser integrado a toda nuestra infraestructura, cumpliendo con todos los pasos necesarios, que hemos ido describiendo en el presente capítulo, debería seguir con la secuencia natural ya expuesta que respondería a lo que se representa en la imagen final que sigue.

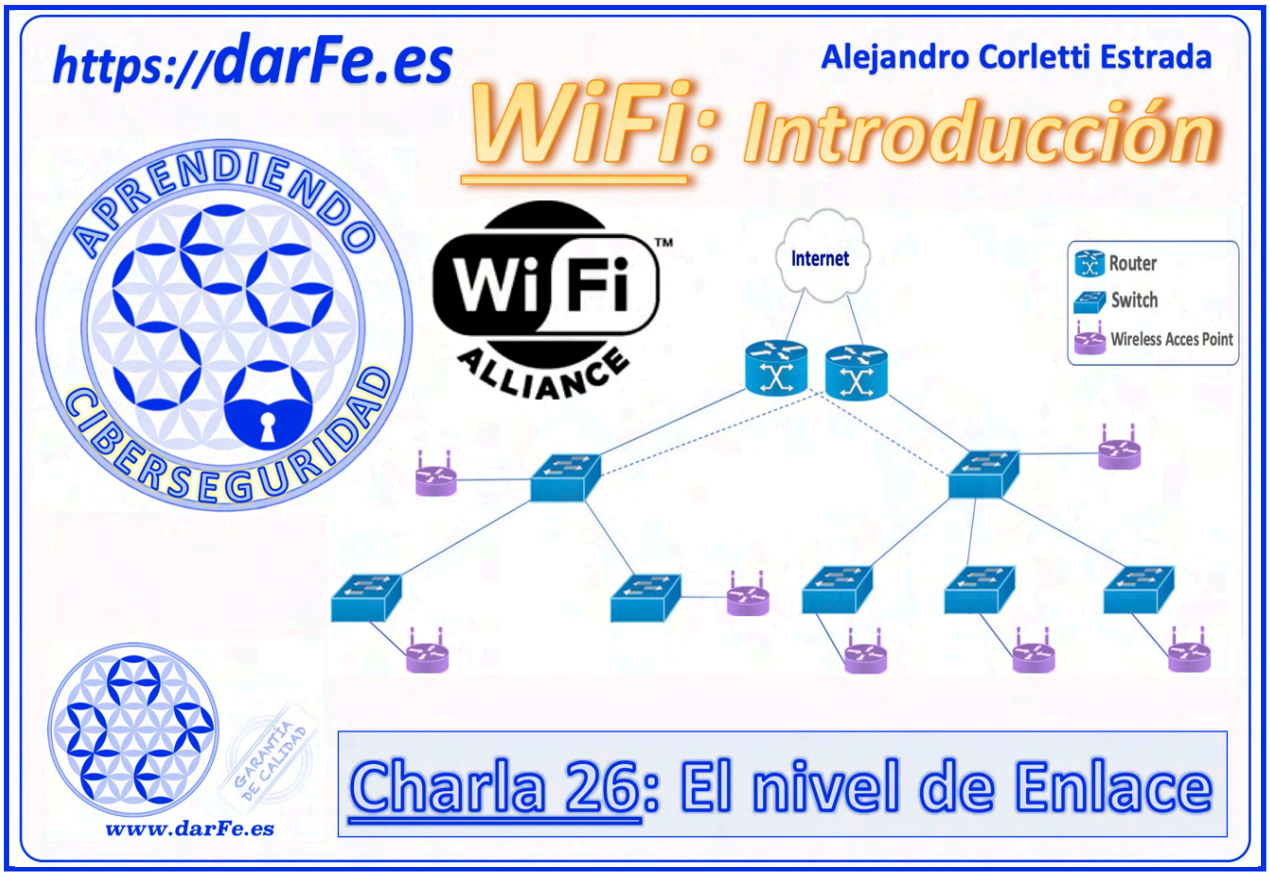


Volver al índice

www.darFe.es

Charla 26

WiFi - Introducción



Enlace al Video:

Resumen:

En este primer capítulo sobre las redes **WiFi**, presentaremos el estándar **IEEE-802.11**, que como veremos, se trata de otra familia, compuesto por varias versiones del mismo.

Desarrollaremos los conceptos básicos para ser considerados como un punto de partida o introducción a estas redes y que nos acompañarán durante varias charlas más.

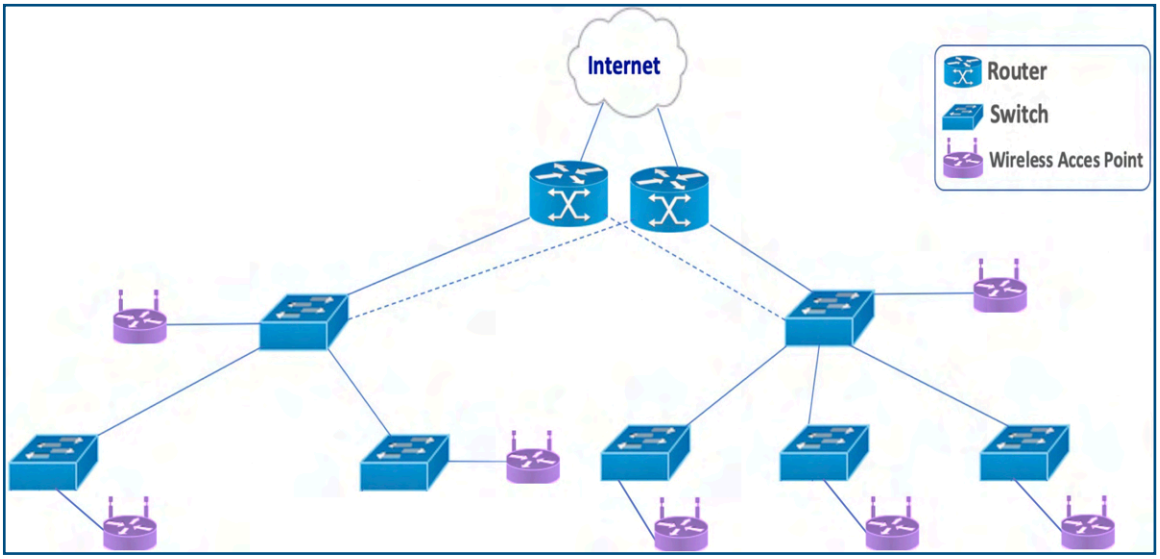
Para cerrar la charla de hoy, hablaremos de su evolución, topología, velocidades y algún detalle histórico desde que nació esta tecnología allá por los años 1999.

Descripción detallada

Es importante, para el tema de hoy, que tengáis presente lo que desarrollamos en la charla 04 sobre "Señales" pues nos apoyaremos mucho en las mismas, así que si no os quedó claro, no dudéis en darle una repasada.

Nos basaremos en la norma **IEEE-802.11** en su versión del año 2020, que es la más importante para desarrollar con buena base las redes "**WiFi**".

La idea que iremos presentando, en cuanto a las redes "WiFi", conociendo ya nuestras estructuras de redes LAN con su jerarquía de switchs y supongamos que a su vez nuestra empresa tiene su propia salida a Internet. Esta salida, será por medio de unos dispositivos llamados **routers**, que no os preocupéis que veremos en detalle cuando iniciemos con el nivel de red. La intención, es incorporar ahora un dispositivo adicional, que se llama **punto de acceso WiFi** (Wireless Access Point), y será el responsable de gestionar justamente este tecnología. A continuación, manteniendo el esquema inicial, se presenta cómo se irían conectando físicamente estos nuevos elementos de red.



El mapa anterior, es importante que desde ya nos quede claro, pues las redes WiFi son una realidad en toda organización, y es casi seguro que en toda empresa nos encontremos con ellas. El mensaje fundamental a transmitir, es la importancia de configurarlas debidamente, pues veremos que una red WiFi bien asegurada es tan robusta como una cableada, así que dediquemos una cuantas líneas para analizar, cómo, ese mapa que acabamos de ver debe protegerse para que podemos confiar en él.

Como se presenta en la imagen que sigue, la abreviatura **WiFi** procede de **Wireless Fidelity**. Tiene su origen en la alianza **WECA** (Wireless Ethernet Compatibility Alliance), que luego cambia su nombre al actual: **Wi-Fi-Alliance**, cuya URL es:

https://www.wi-fi.org

Lo que todos conocemos como "**WiFi**" son las siglas de Wireless Fidelity.

Hasta el año 2002 existía una alianza llamada **WECA** (*Wireless Ethernet Compatibility Alliance*), que en ese año cambia su nombre por **Wi-Fi Alliance**.

Es interesante destacar que tanto su nombre "**WiFi**" como su novedoso logo, fue la acertada decisión de contratar a la agencia **Interbrand**. El logo se inspiró en el "*yin y yang*" y su abreviatura en el fuerte impacto de marketing que había tenido Hi-Fi: High Fidelity.

https://www.wi-fi.org

En el año 1999 se publicó el prime estándar: **802.11b** (*aún era WECA*), no hablaremos de versiones previas pues no merece la pena.

La familia 802.11 tiene el objetivo de reemplazar la capa física y MAC de 802.3 (Ethernet) por una interfaz aire.

Esta nueva lógica de forma similar a **CSMA/CD**, se define como:

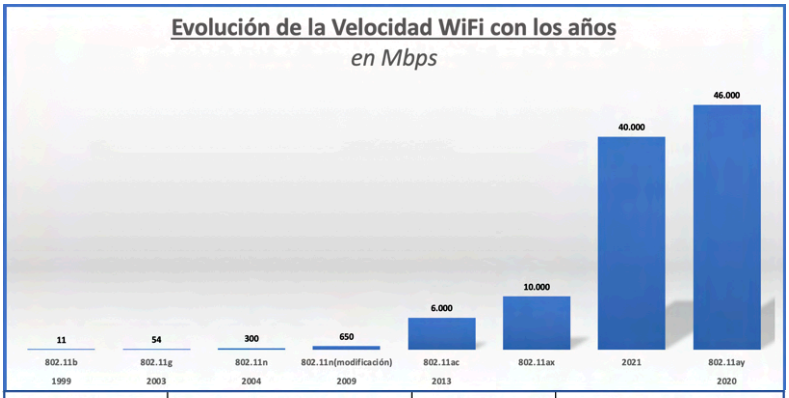
CSMA/CA: *carrier sense multiple access with collision avoidance*

Como figura al final de la imagen anterior, la lógica que emplea es **CSMA/CA**. CSMA ya lo hemos desarrollado entre las charlas 11 y 16, así que no lo repetiremos, pero lo que sí nos interesa es esta nueva idea **CA**: Collision Avoidance.

La tecnología WiFi ha ido evolucionando a lo largo de los años, ofreciendo cada vez mejores prestaciones, no solo en velocidad, como se aprecia a la derecha, sino también en modulación, empleo de los canales, alcance, seguridad, etc.

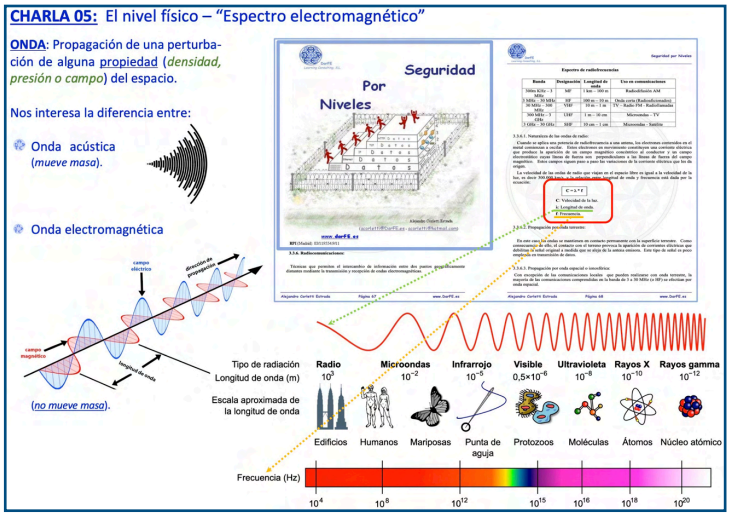
Por esa razón es que la norma IEEE-802.11 ha tenido muchas recomendaciones al original.

Como podemos ver en el cuadro de la derecha, nace en 1999 como 802.11b, hasta llegar a las versiones actuales y las previstas: 30-46 Gbps (para un técnico esto parecía inalcanzable e inimaginable hace diez años).



Año	Estándar IEEE	Velocidad	Frecuencia
1999	802.11b	11Mbps	2,4GHz
2003	802.11g	54Mbps	2,4GHz
2004	802.11n	300Mbps	2,4GHz
2009	802.11n(modificación)	650Mbps	2,4GHz
2013	802.11ac	6Gbps	5GHz
2020	802.11ax	10Gbps	2,4GHz
2021	(WiFi 6E)		6GHz
2021	802.11ay	20-40Gbps	60GHz
2024(previsto)	802.11be	30-46Gbps	2,4GHz, 5GHz, 6GHz
2024(previsto)	802.11bf		2.4GHz,

La tecnología WiFi se basa en el empleo de ciertos rangos de frecuencias que se denominan **ISM** (Industrial Scientific and Medical), se trata de frecuencias que NO están reguladas en ningún país del mundo y han sido dejadas para el libre uso, justamente para este tipo de tecnologías, por esa razón es que se emplean para WiFi, Bluetooth, microondas, aeromodelismo, etc. En la última columna de la tabla anterior, podemos ver claramente cuatro de ellas: 2,4 GHz, 5 GHz, 6 GHz y hasta 60 GHz.



Un detalle que debemos tener en cuenta, tal cual presentamos en la charla 05, es que cuanto más alta sea la frecuencia, mayor ancho de banda tendremos, pero a su vez, menor alcance. Por esa razón, es que, debemos comprender bien estos conceptos y su modulación correspondiente a la hora de decidir qué tipo de tecnología Wifi emplearemos.

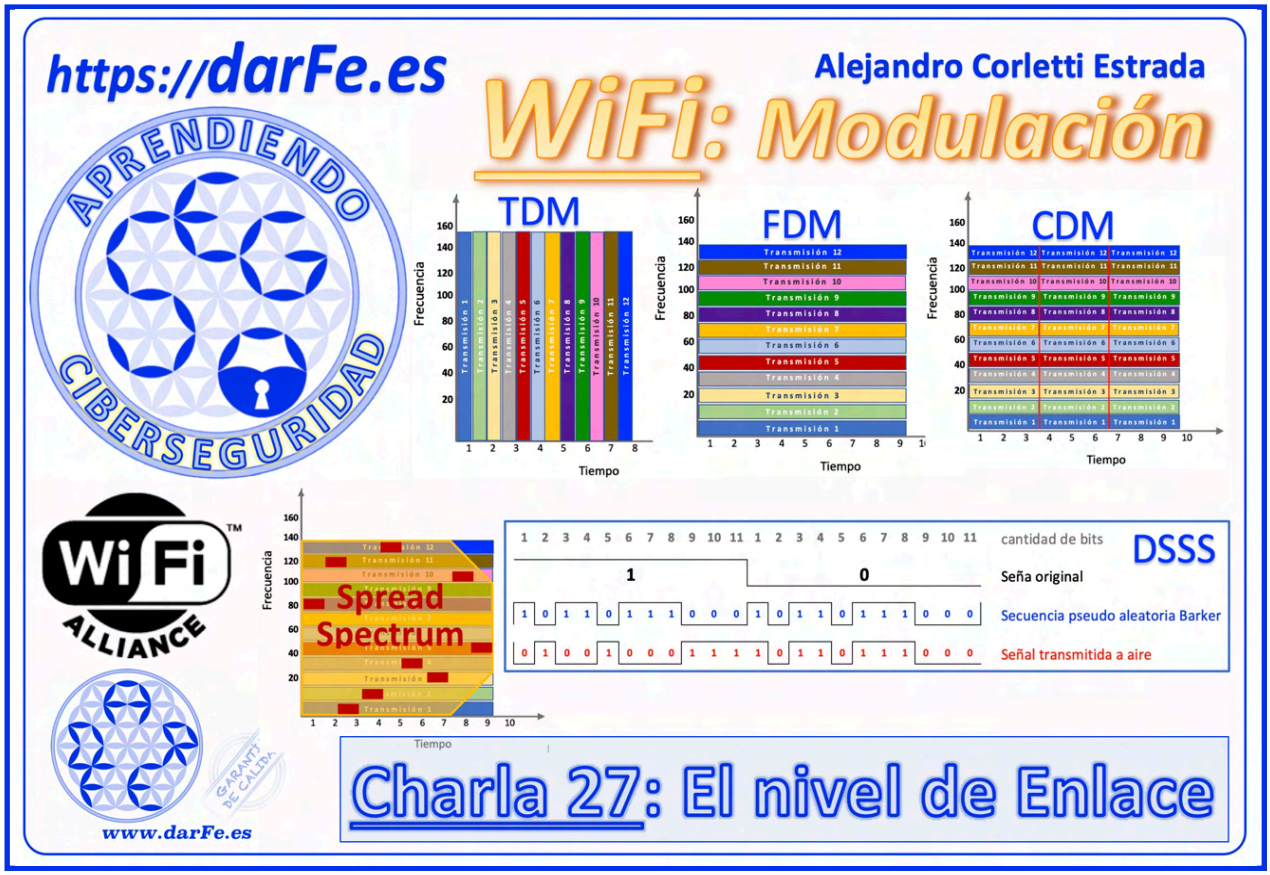
También en virtud del amplísimo uso de estas frecuencias, es que se deben emplear técnicas de modulación y seguridad muy robustas, justamente para poder separarlas del microondas de mi casa, del bluetooth, de la nevera, del móvil de mi abuelo y de las WiFis de todos mis vecinos. Si todo esto no se realiza de forma muy robusta, nuestra red WiFi será un verdadero caos.

Volver al índice

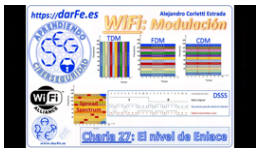
www.darFe.es

Charla 27

WiFi - Modulación



Enlace al Video:



Resumen:

En esta charla, presentamos las diferentes técnicas que aplican las redes WiFi para modular las señales que emite y recibe.

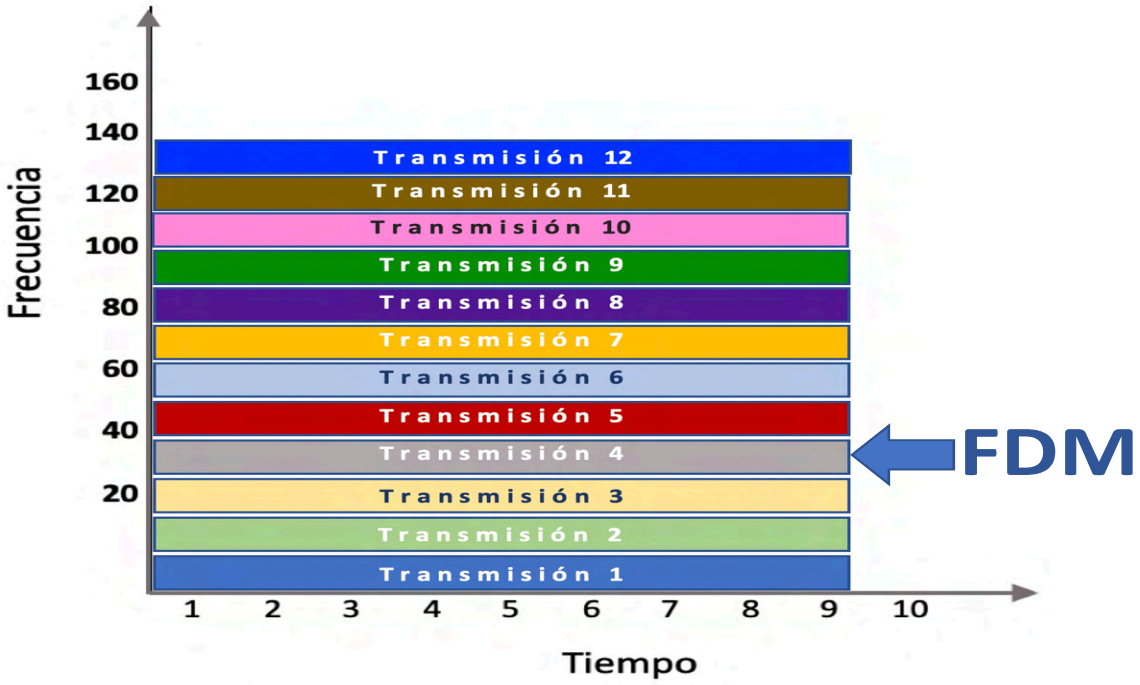
Ya hemos hablado en el nivel físico de las señales, su digitalización, y algo de transmisión de información, con lo que tenemos las bases para comprender estas novedosas técnicas que se emplean en la actualidad.

Descripción detallada

En la charla anterior, pusimos de manifiesto la evolución de las frecuencias que emplea WiFi. Hoy seguiremos avanzando para analizar como hace uso de las mismas para emitir y recibir la información. Este proceso, como no podía ser de otra forma lo ejecuta por medio de la **modulación**, tema que si aún lo recordáis, comenzamos a verlo desde la Charla 04: El nivel Físico (**Señales**).

En el caso de WiFi, para poder comprender bien la complejidad de estas señales, nos detendremos con bastante detalle en las mismas.

Para comenzar a presentar el tema, vamos a analizar la imagen siguiente, donde podemos ver un sistema cartesiano de dos ejes. En el eje horizontal (eje X) se representa el tiempo, y en el vertical (eje Y) vemos las frecuencias.



Cuando escuchamos radio **FM** (Frecuencia Modulada), estamos sintonizando la emisora que deseamos, **filtrando** las frecuencias que emiten las restantes.

Esto se logra por medio de una combinación de dos filtros:

- pasa bajo: deja pasar las frecuencias más bajas desde el punto que se aplica el filtro y atenúa todas las superiores.
- pasa alto: deja pasar las frecuencias más altas desde el punto que se aplica el filtro y atenúa todas las inferiores.

La combinación de ambos, se denomina filtro pasa banda, pues filtra todas las superiores y las inferiores de la sintonía que deseo, y solo dejo pasar las frecuencias que se corresponden, por ejemplo, con “Cadena 100” *(y escucho el programa de Javi y Mar de la mañana, que está buenísimo*).

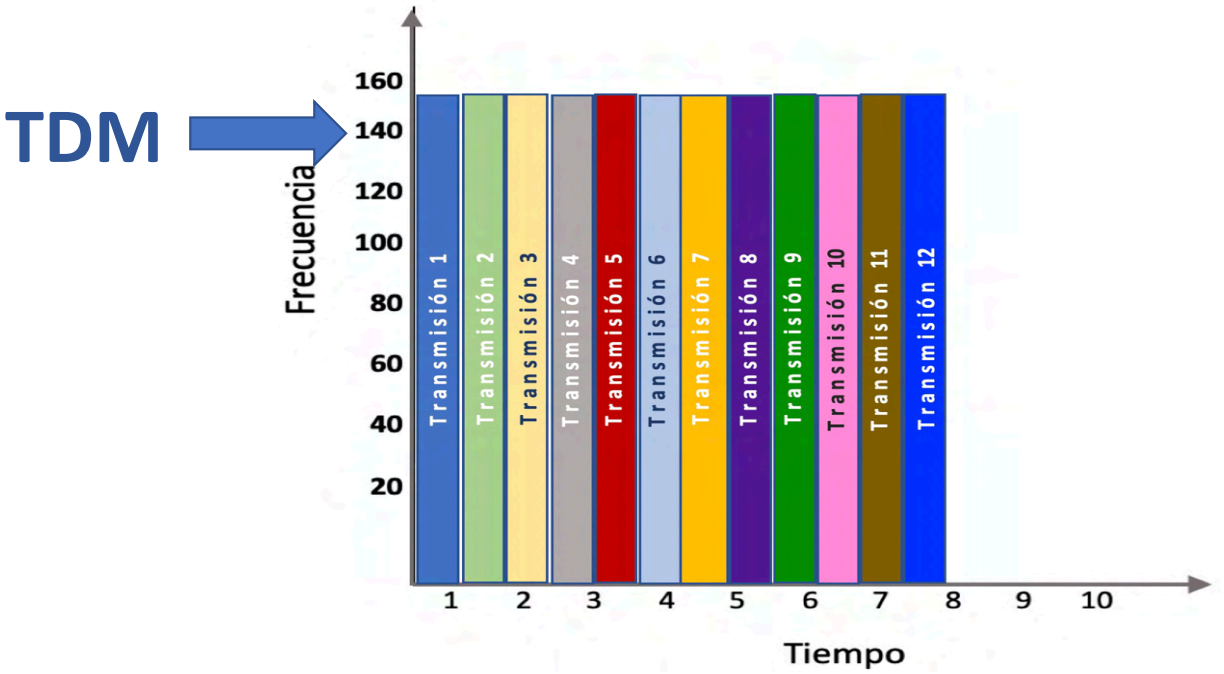
Esta técnica de modulación se denomina **FDM** (Frequency-Division Multiplexing), que en español sería Multiplexación por División de Frecuencias.

Para desarrollar y comprender en detalle este tema, recomendamos que os descarguéis el artículo "**Modulación.pdf**" desde:

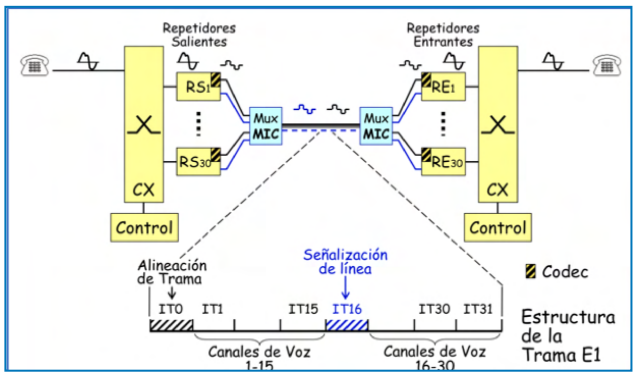
https://darfe.es —> DESCARGAS —> Artículos :

Modulación.pdf

La otra técnica que presentamos a continuación es **TDM** (Time-Division Multiplexing) o Multiplicación por División de Tiempo; en la cual, mantenemos los mismos ejes X e Y, pero esta vez, lo que nos interesa es dividir el eje X en "**ranuras de tiempo**" en cada una de las cuáles, se emite un canal en concreto. Esta técnica, mantiene estas ranuras de tiempo con una duración constante y tanto el emisor, como el receptor, sincronizan sus relojes. Supongamos que nos interesa escuchar la transmisión 5 que figura en **rojo** en la imagen siguiente, entonces únicamente se centra la atención en ese "slot" o ranura, y se descartan las demás.

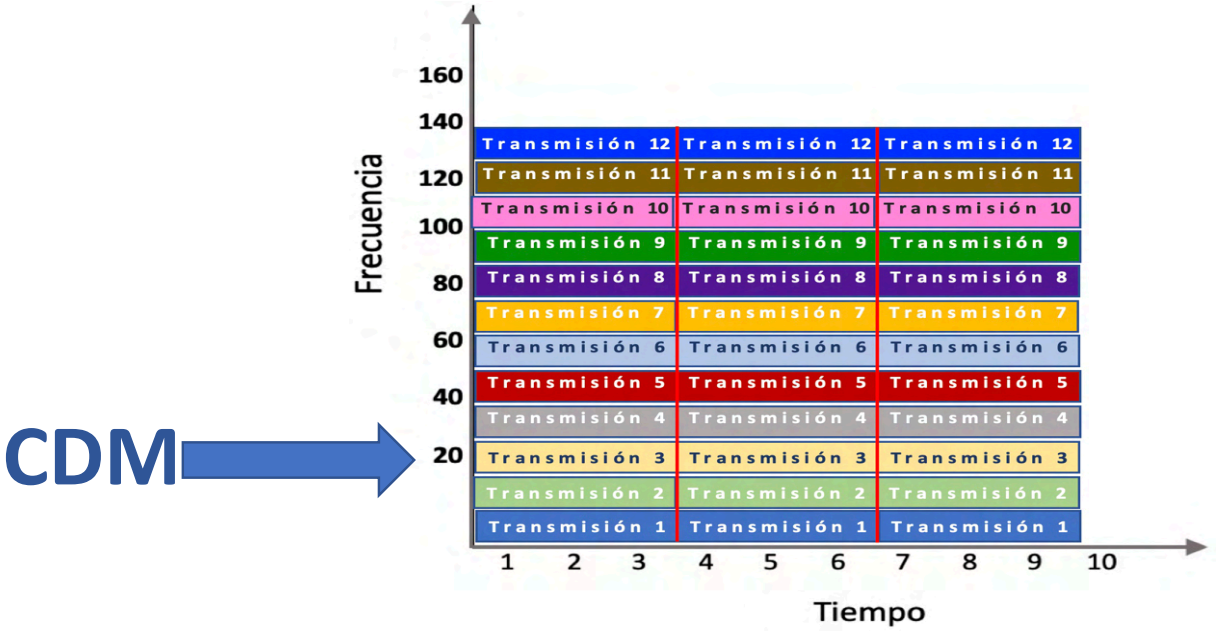


Esta es la técnica que emplea la Televisión Digital Terrestre (**TDT**). También es la técnica que emplea todo el sistema telefónico mundial, o red de telefonía conmutada, cuyas troncales son digitales, y la voz viaja en canales de 64Kbs (esto lo vimos en la Charla 06 - Digitalización), formando lo que se denomina tramas, cuya trama básica es la trama **E1** compuesta por 32 canales de 64 Kbps lo que suman 2.048 Kbps o 2,048 Mbps, como se presenta en la imagen de la derecha. Cuando se establece una comunicación, la voz viaja en uno de esos canales de la mencionada trama E1, y el teléfono, solo escucha ese canal en concreto, pasando por alto cualquier otra ranura de tiempo (o canal).



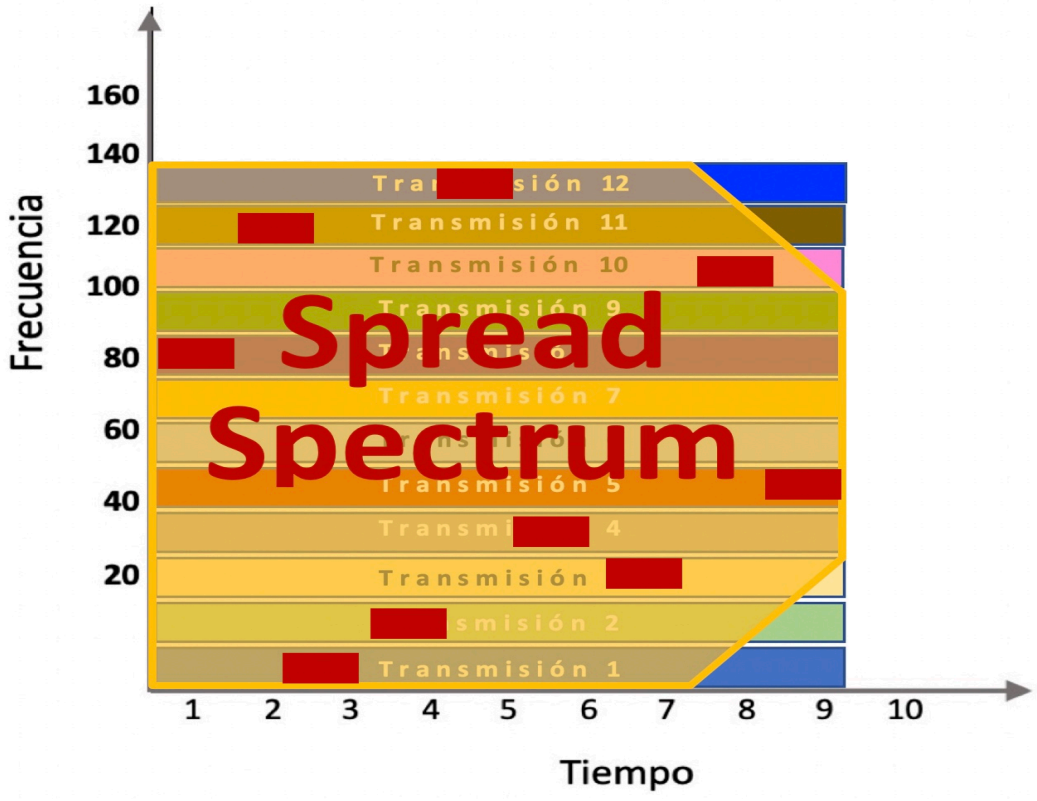
Por último, como una combinación de las dos técnicas anteriores, surge la **CDM** (Code-Division Multiplexing) o Multiplicación por División de Código. En la imagen que sigue,

se puede ver cómo, empleando diferentes frecuencias, sumadas a ranuras de tiempo, podemos optimizar aún más la eficiencia de estas comunicaciones.



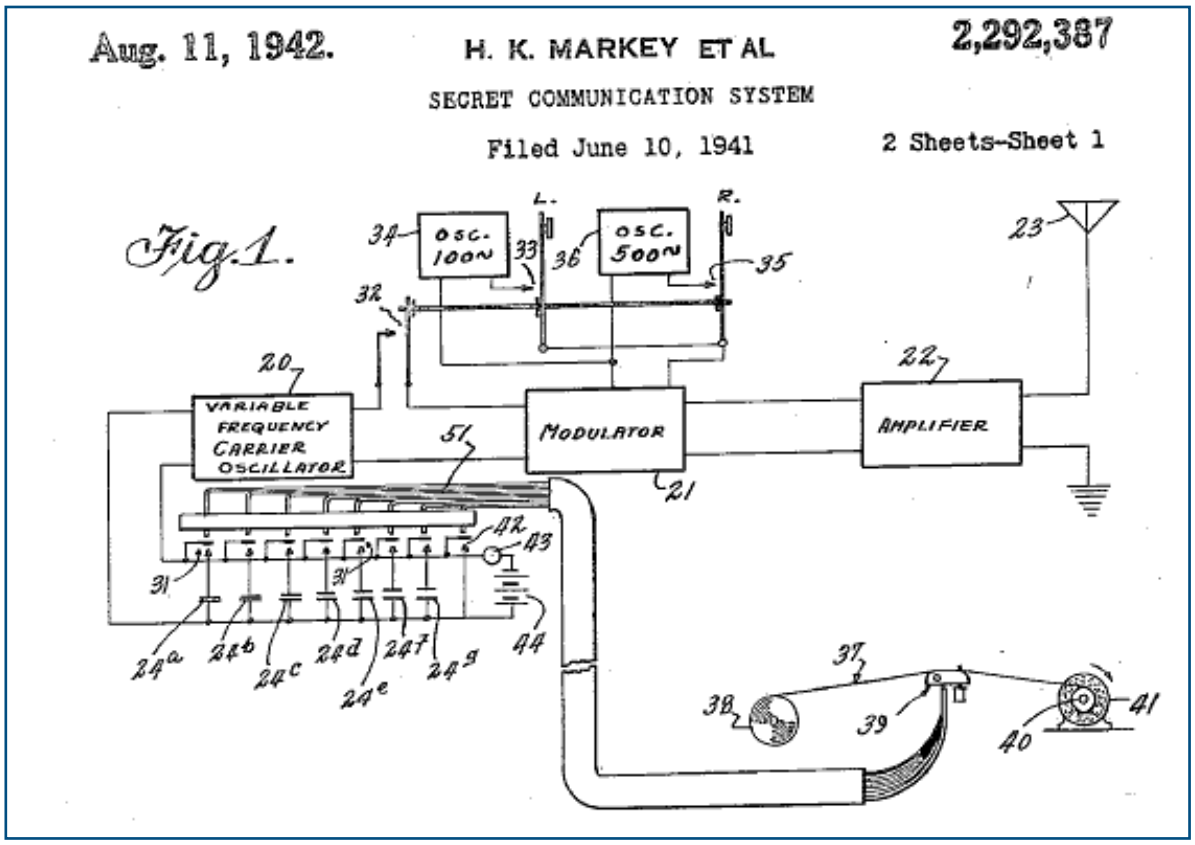
En los años 40`, y debido a la segunda guerra mundial, aparece una técnica muy novedosa diseñada para evitar las escuchas radiofónicas enemigas. Este técnica que se llamó **Spread Spectrum** o Espectro expandido, lo que buscaba era emplear todo el espectro, por ejemplo de las gráficas anteriores e ir realizando saltos en el mismo que respondieran a un patrón preestablecido entre el emisor y el receptor. Si este patrón no se conoce, resulta sumamente complejo poder interceptar o interferir la comunicación.

En la imagen que sigue se presenta esta técnica. Se destaca en **rojo**, un ejemplo de los diferentes paquetes de información que van saltando de una banda de frecuencias a otra.



La primera patente pública fue el 11 de agosto de 1942, en plena guerra, y quien lo hizo fue la actriz hollywoodiense **Hedy Lamarr** (Hedwig Eva Maria Kiesler) y el pianista **George Antheil**.

La lógica de estos saltos, se basaba en la idea de una caja de música o pianola, donde diferentes puntos ubicados en un cilindro, accionan las notas musicales.

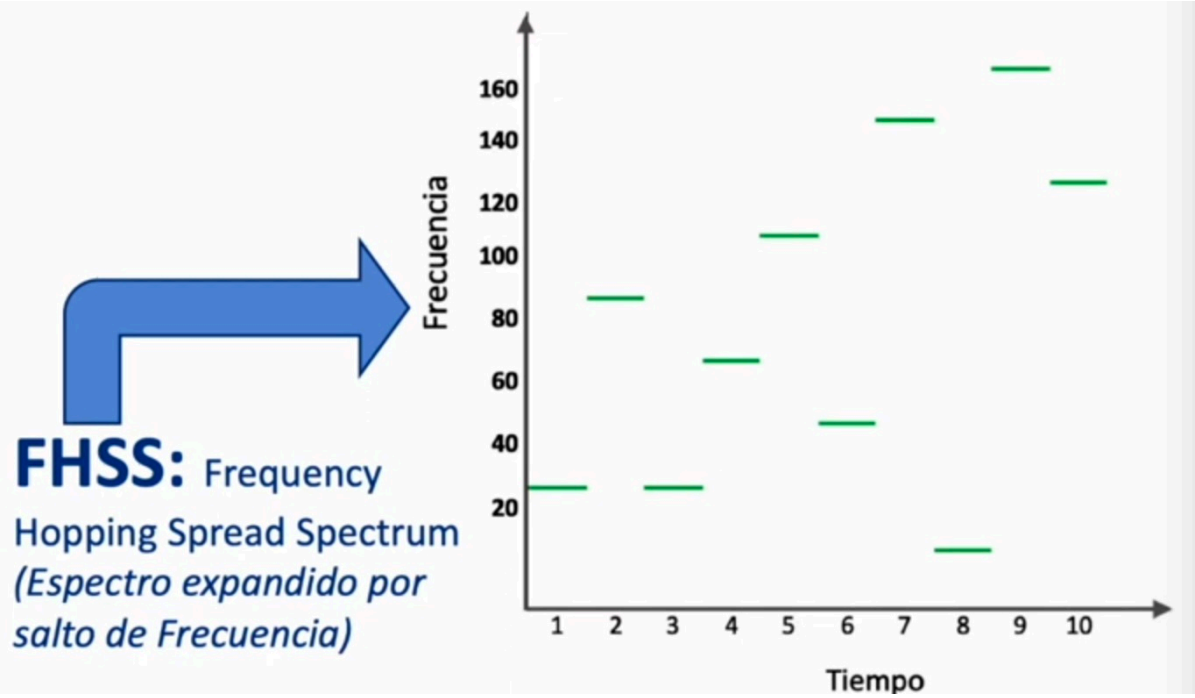


Si prestáis atención a la patente anterior, está a nombre de "H.K. Markey et al". Las iniciales H.K. son de Hedwig Kiesler (Hedy Lamarr) y Markey era su apellido de casada en ese momento.

¿Por qué razón nos hemos extendido en los conceptos anteriores?, pues justamente porque las redes WiFi emplean esta técnica.

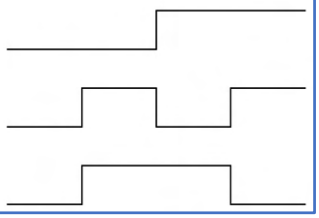
La implementación tiene dos variantes distintas, la primera de ellas se denomina **FHSS** (Frequency Hopking Spread Specturm), es decir, Espectro Expandido por Salto de Frecuencias. El funcionamiento, es prácticamente el que acabamos de presentar en Spread Spectrum, se diferencia en que, el empleo de esta técnica por parte del estándar IEEE-802.11 está pensado para aprovechar al máximo las diferentes bandas que tiene disponibles, evitando transmitir por las que tienen mayor interferencia. Tengamos en cuenta que una red WiFi, comúnmente trabajará cercana a muchas otras más. Dependiendo del país, emplea 13 o 14 canales, los cuales se subdividen en bandas y al establecerse una conexión con un punto de acceso en concreto, el mismo determina cuáles son los canales que menor interferencia tienen y, sobre ellos negocia con el cliente cómo será su técnica de saltos de frecuencia.

A continuación se presenta una imagen de esta técnica.



La segunda variante, es más complicada de comprender. Iniciemos presentando la operación binaria conocida como **XOR**. Esta operación es definida como desigualdad pues solo da como resultado "**1**", cuando los dos términos son diferentes.

XOR			
0	0	1	1
0	1	0	1
0	**1**	**1**	**0**



Sobre esta operación, se plantea la técnica de **DSSS** (Direct Sequence Spread Spectrum, o Espectro Expandido por Secuencia Directa, que es lo que utiliza concretamente la norma **IEEE-802.11b**.

Esta transmisión, se basa en una secuencia, o código pseudo aleatorio, o código **PN** (Pseudorandom Noise), llamado Barker. En el caso del estándar **IEEE-802.11b**, concretamente se define en el punto **18.4.8.4** y es el que vemos a continuación.

18.4.6.4 Spreading sequence and modulation for 1 and 2 Mbit/s

The following 11-chip Barker sequence shall be used as the PN code sequence for the 1 and 2 Mbit/s modulation:

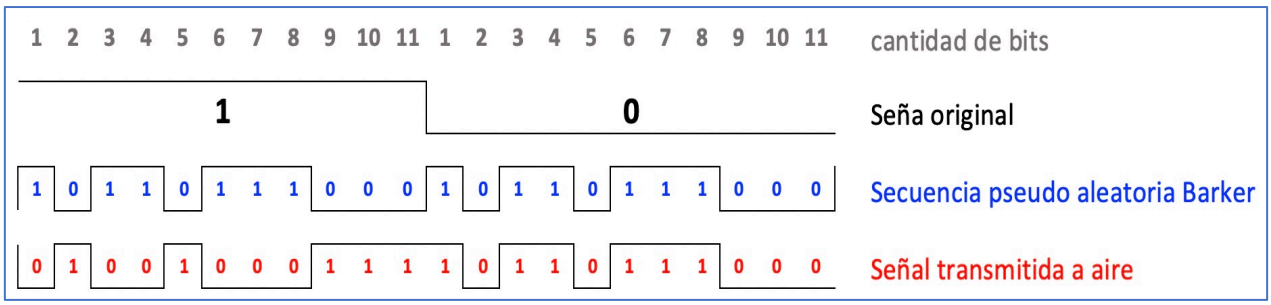
+1, –1, +1, +1, –1, +1, +1, +1, –1, –1, –1

The leftmost chip shall be output first in time. The first chip shall be aligned at the start of a transmitted symbol. The symbol duration shall be exactly 11 chips long.

Estos once bits de la imagen anterior también se conocen como señal de chips. En realidad, lo que se está haciendo es expandir cada bit que se desea transmitir, en este caso once veces, y solapar con el bit original de la señal. Con esto se logra una

importante redundancia que permite reconstruir una señal ante interferencia, normal en este tipo de redes.

A continuación, se presenta una imagen en la que se puede apreciar una señal original, de dos bits: 1 0, debajo de la misma, se secuencia Barker. Entre ambas, se aplica bit a bit la operación XOR, dando como resultado las señal transmitida al aire, que se presenta en **rojo**.



Cualquiera que preste atención a la imagen anterior pensaría que es un total desperdicio de canal, tener que emplear 11 bits para transmitir un único 1 ó 0, pero justamente en esto consisten los código **FEC** (Forward Error Control) que ya hemos visto en la **charla 16 - CRC.**

A través de esta redundancia, si en alguno de esos 11 bits, se produjera una interferencia, el receptor estaría en capacidad de detectar ese error y corregirlo, sin necesidad de solicitar una retransmisión, que es el objetivo final de esta técnica.

Todos los estudios sobre el código Barker, determinan que lo óptimo es el empleo de 100 bits (no sólo 11), pero en el caso de las redes WiFi, por la relación coste/beneficio de la transmisión, se determinó que con 11 bits era suficiente.

Volver al índice

www.darFe.es

Charla 28

WiFi - CDMA/CA

Enlace al Video:

Resumen:

En esta charla, presentaremos por medio capturas de tráfico, cómo se establece una conexión WiFi, se envían y se reciben datos. Todo ello analizado desde la "**interfaz aire**" que, como veremos, es algo que está fuera de la pila **TCP/IP** que venimos desarrollando hasta ahora.

Lo más importante de la charla de hoy, es que veremos un diálogo real y aprenderemos a emplear **Wireshark** en modo "**monitor**", aspecto que nos será de sumo interés y aprovechamiento pare seguir avanzando en la seguridad de las redes WiFi.

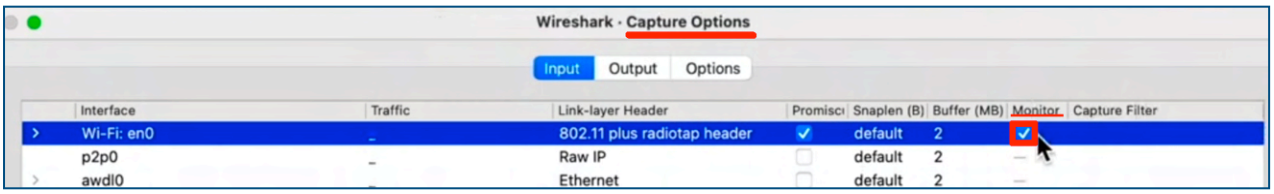
Descripción detallada

La charla de hoy, la comenzamos de forma eminentemente práctica por medio de una maqueta entre dos portátiles, conectadas a un mismo punto de acceso WiFi, como podemos ver en la imagen siguiente.

Para poder analizar el tráfico de toda esta conexión, emplearemos una vez más la herramienta **Wireshark.**

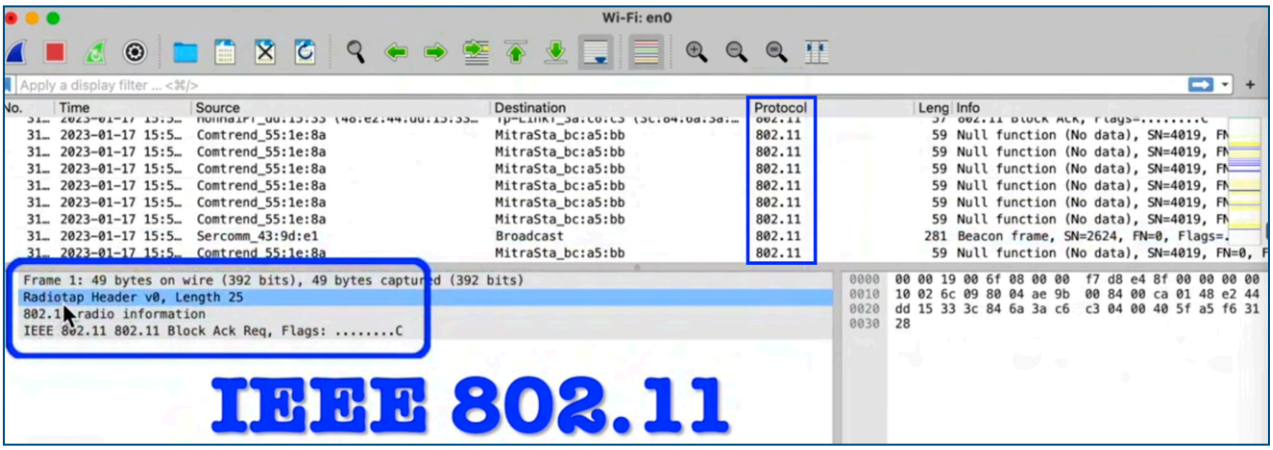
NOTA: recordamos que, para comprender en detalle el empleo de Wireshark, tienes disponible nuestro ciclo sobre "**Análisis de Tráfico**".

Para las capturas de tráfico WiFi, hay que tener en cuenta un detalle importante en la configuración de Wireshark. Dentro del menú "Capture" hay que ir a "Options" y seleccionar modo "**Monitor**" como se presenta en la imagen de abajo.



El modo **Monitor**, no es lo mismo que el modo "**Promisc**", que como vemos, también está seleccionado. Recordad que el modo Promisc (o promiscuo) lo empleábamos para que, al realizar las capturas de tráfico, el nivel de enlace, deje pasar todo el tráfico, sin descartar las "destination MAC Address" que no sean la propia, que sería el funcionamiento normal de Ethernet. Por lo tanto, cuando selecciono "promisc" mi tarjeta Ethernet dejará pasar todo, y no descartará absolutamente nada de tráfico. Es decir ,puedo capturar el 100% del tráfico que está circulando por este medio físico.

El modo **Monitor** es diferente. Cuando lo seleccionamos, le indicamos a la tarjeta WiFi de nuestro ordenador que NO escuche la pila TCP/IP, sino que se centre en la **interfaz aire**. Es decir, lo que capturaremos será la modulación que acabamos de explicar en la charla anterior, según el tipo de protocolo IEEE-802.11**x** que se esté empleando. Por esta razón, iremos viendo en la charla de hoy que las capturas de tráfico nos presentarán una "pila" diferente a la que estamos acostumbrados a ver hasta ahora. En la imagen que sigue, presentamos un ejemplo.



Para que puedas trabajar con todo detalle sobre este charla de hoy, hemos subido a nuestra Web: **https://darFe.es**, en el Menú "DESCARGAS" **—>** "Capturas de Tráfico", las siguientes capturas:

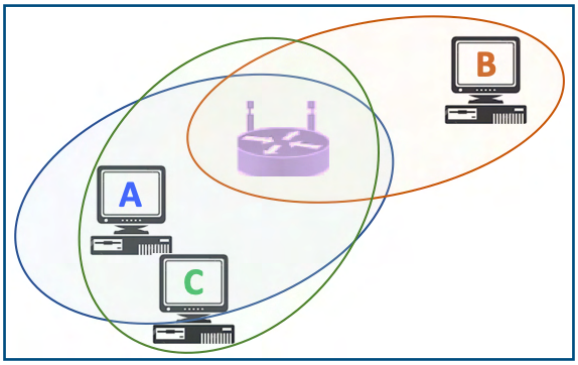
- **WiFi_2.4GHz_hogar.pcap**
- **wifi_casa_5GHz.pcap**
- **wiFi_802.11_BEACON.pcap**
- **WiFi_CTS_RTS_03.pcap**

Para el ejercicio de esta charla de hoy, si volvemos a nuestra imagen inicial de las dos portátiles, podemos ver que la portátil 1 tiene la dirección MAC finalizada en "**.37**", la portátil 2 en "**.7f**" y el punto de acceso WiFi en "**.ed**".

¿Por qué nos interesan estas direcciones MAC?, justamente porque seguimos en el nivel de enlace, lo cual implica que el esquema de direccionamiento de este nivel es el que ya describimos como **OUI-48**, más conocido como **dirección MAC**, tal cual presentamos en la **Charla 15**.

Un tema que debemos tener en cuenta es que en este tipo de redes, encontraremos dos tipos de **nodos**.

- Nodos ocultos: Una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo al que no escucha.
- Nodos expuestos: Una estación cree que el canal está ocupado, pero en realidad está libre pues el nodo al que escucha no le interferiría.

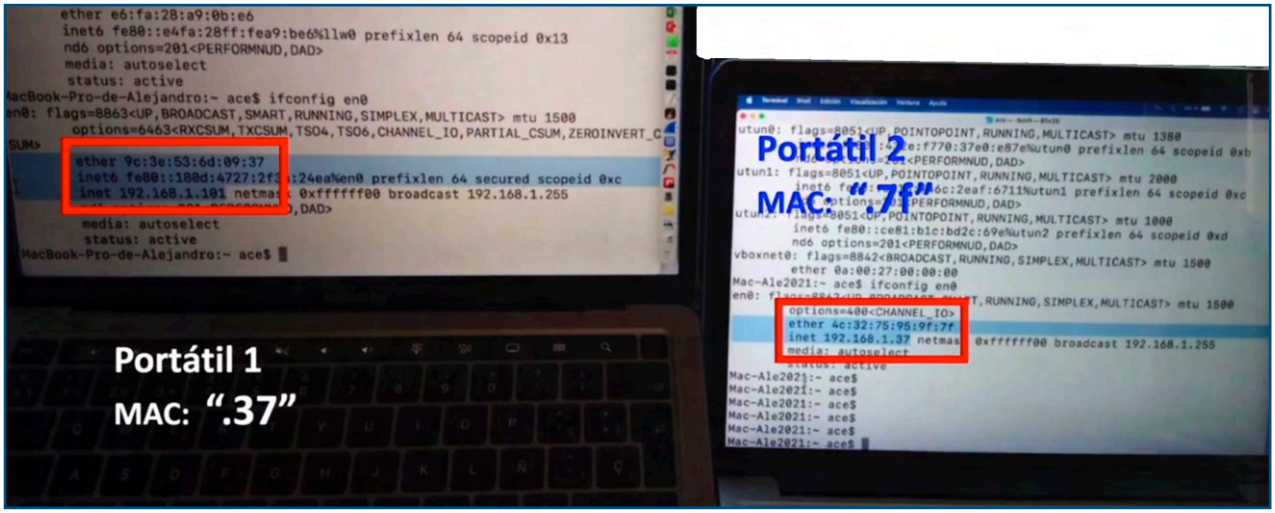


Analicemos la imagen anterior de los nodos "**A, B** y **C**". Cada uno de ellos, tiene una cobertura determinada, la que hemos representado con el óvalo del color correspondiente a cada letra. Está claro que la cobertura (o potencia de emisión) de los nodos **A** y **C** se solapan, es decir cada uno de ellos "escucha" al otro, sin embargo, ninguno de los dos, recibe seña del nodo **B** pues como podemos apreciar, el óvalo naranja no llega hasta ellos. Sin embargo, el punto de acceso WiFi, recibe la señal de los tres, por lo tanto, si los tres están conectados al mismo, podrán establecerse las comunicaciones entre todos, pasando a través del punto de acceso. Lo que queremos destacar aquí, es que el nodo **B** está oculto para **A** y **C**. Este sería el ejemplo de un nodo oculto.

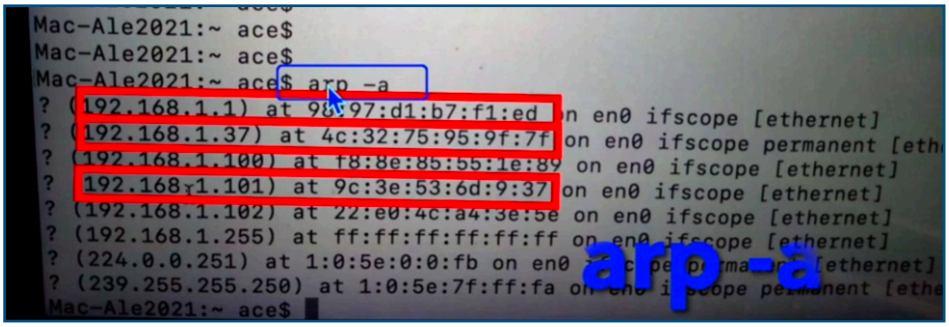
El caso de nodos expuestos lo tenemos entre los nodos **A** y **C**, pues si cualquiera de ellos deseara transmitir, escucharía que hay otro nodo que puede interferirlo (solapamiento de los óvalos verde y azul), pero como existen varios canales o frecuencias para que pueda transmitir, en realidad no lo hará.

Una vez comprendidos estos conceptos, ahora sí podemos pasar a analizar la lógica del protocolo **CSMA/CA** (Carrier Sense Multiple Access/Collision Avoidance), que hasta ahora solamente lo habíamos presentado en la **Charla 26**.

Volvamos a nuestros dos ordenadores portátiles. En la imagen siguiente hemos resaltado ambas direcciones MAC.



Para analizar las conexiones que hay en este momento, podemos hacerlo por medio del comando "**arp -a**" que ya hemos mencionado. En la siguiente imagen podemos verlo en la portátil 1 (MAC "**.37**"). Hemos resaltado en **rojo** las tres direcciones MAC que ya están en caché ARP (y son las de los tres dispositivos presentados en la primera imagen ("**.ed** , **.7f** y **.37**").



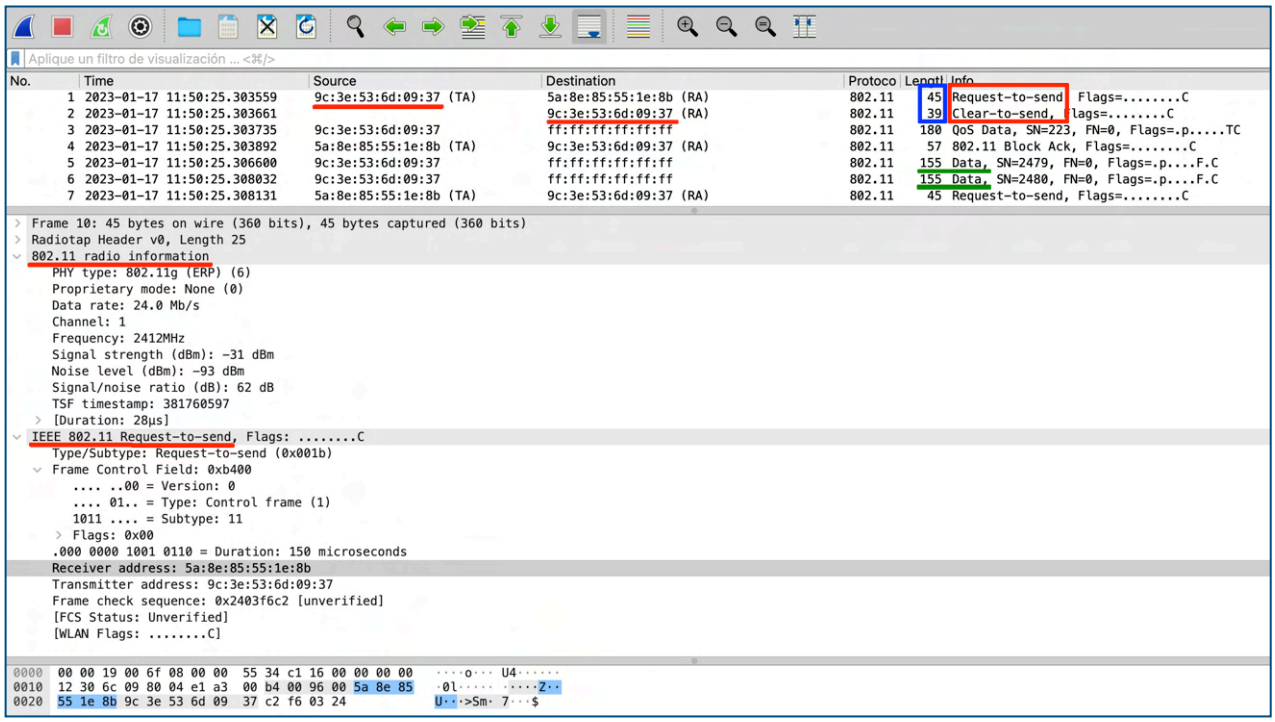
Durante el desarrollo del video, se ha realizado un "**ping**" (Packet Internet Groper) desde la Dirección IP 192.168.1.101 a la 192.168.1.37, este es un comando que ejecuta el tipo 0 y 8 del protocolo **ICMP** (Internet Control Message Protocol) que lo veremos más adelante, pero básicamente es una solicitud y respuesta de eco. Este ping, se realizó para capturarlo con Wireshark.

En la imagen de la derecha podemos ver este ping.

```
MacBook-Pro-de-Alejandro:~ ace$  ping 192.168.1.37
PING 192.168.1.37 (192.168.1.37): 56 data bytes
64 bytes from 192.168.1.37: icmp_seq=122 ttl=116 time=4.849 ms
64 bytes from 192.168.1.37: icmp_seq=123 ttl=116 time=4.861 ms
64 bytes from 192.168.1.37: icmp_seq=124 ttl=116 time=4.895 ms
```

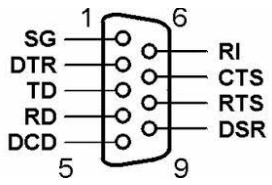
A continuación analizaremos qué ha sucedido a nivel WiFi (aire), al ejecutar este ping.

La imagen que sigue, se corresponde a la captura de tráfico: WiFi_CTS_RTS_03.pcap que, como dijimos al principio, la podéis descargar de nuestra Web.

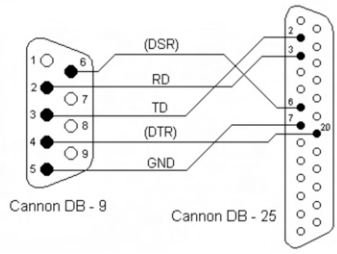


El inicio de toda comunicación WiFi a nivel aire, se desarrolla por medio de dos tramas IEEE-802.11, Request to send (**RTS**) y Clear to send (**CTS**), recuadradas en **rojo** en la imagen anterior.

RTS, es la solicitud para poder transmitir, que si os fijáis bien, la está pidiendo la portátil 1 (MAC "**.37**") al punto de acceso WiFi (MAC "**.8b**"). La segunda trama **CTS**, es en la que el punto de acceso, le responde a la portátil 1 informándole que tiene permitido transmitir.



Este tipo de diálogo inicial, tiene su origen en las primeras comunicaciones cableadas, donde a través de los diferentes "**pines**" de conexión, se activaban, o no, **RTS** y **CTS**. Los que ya peináis canas, recordaréis esos viejos conectores llamados "Cannon DB-9 y Cannon DB-25" que se empleaban para conectar los ordenadores con el ratón, teclado, impresora, etc. En los mismos, justamente existían pines que llevaban estos nombres RTS y



CTS, y a través de estos contactos, cuando se enviaban las señales hacia los dispositivos y viceversa, se iban habilitando las transmisiones por los pies “TX y RX” que era por donde se enviaba y recibía la información.

El inicio de las tramas de una conexión WiFi, se basó en estos mismos conceptos, por esta razón es que podemos apreciar en la captura de tráfico estas dos tramas al principio. Se trata de un diálogo de muy poco volumen, como podemos ver en la captura su tamaño es de 45 y 39 bytes respectivamente (recuadrados en **azul** en la captura anterior), justamente para que sea veloz y no una sobrecarga para la red.

Por último en la misma captura anterior, las tramas 5 y 6 que, como podemos ver, se tratan de “Data” (subrayadas en **verde**), ya es por donde está viajando el “**ping**” que hemos enviado con un tamaño de 155 bytes.

Si seguís analizando esta captura de tráfico, podréis ver que en la trama 18, el punto de acceso le envía un “**Aknowledgement**” confirmándole la recepción.

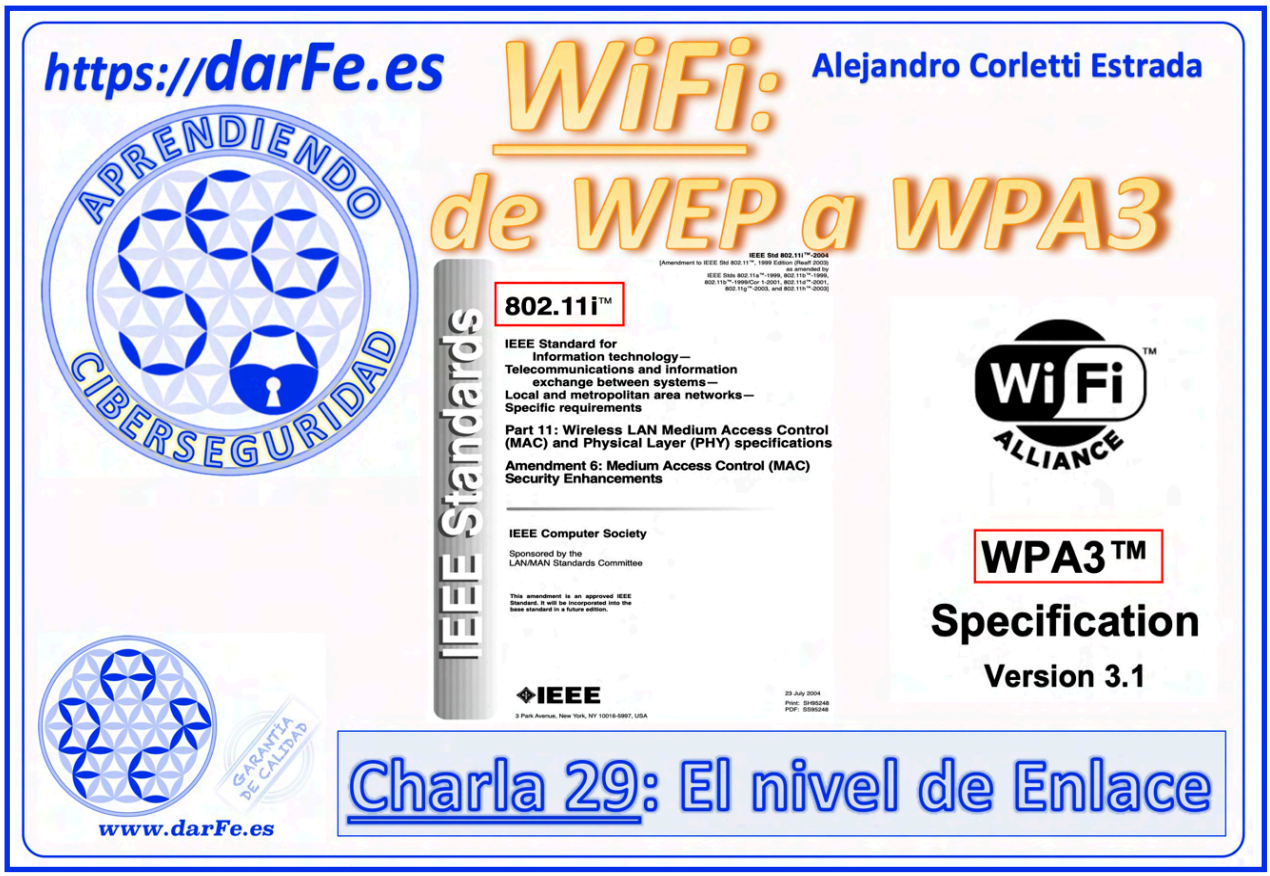
En resumen, lo que hemos visto es que la portátil 1, le solicita transmitir al punto de acceso (RTS), éste la autoriza (CTS), la portátil 1 envía el/los ping (Data); y finalmente el punto de acceso le da el OK (Aknowledgement).

Volver al índice

www.darFe.es

Charla 29

WiFi - de WEP a WPA3



Enlace al Video:

Resumen:

En esta nueva charla sobre WiFi, presentamos la familia de estándares **IEEE-802.11** que son su base de referencia, y en particular nos centraremos en el **IEEE-802.11i,** que es el que más nos interesa desde el punto de vista de Ciberseguridad.

Este tema de hoy, se dividirá en dos charlas, la de hoy, que presentaremos brevemente su historia y evolución desde el protocolo **WEP**, y la siguiente charla, en la que avanzaremos a su versión más actual, que es **WPA3**.

Descripción detallada

En esta charla, comenzamos a desarrollar los primeros aspectos de seguridad en redes WiFi. Como podéis ver a la derecha, nos basaremos en el estándar **IEEE-802.11i**.

En particular, nos centraremos en los protocolos de cifrado que ofrece esta tecnología, y lo haremos siguiendo la historia de los mismos que, como sucede siempre en temas de Ciberseguridad, la vorágine de los avances, transforma en inseguras las técnicas que años antes eran lo más robusto del planeta.

Tomaremos también en cuenta dos artículos que hemos publicado hace unos años, pero que seguramente os servirán para profundizar aún más en este tema. Como siempre los encontraréis para su gratuita descarga en nuestra Web: **https://darFe.es**, en el menú "**DESCARGAS**" —> "**Tecnología**" —> "**Artículos**", y son los siguientes:

- Seguridad WiFi (parte técnica): **seguridad_wifi_tecnico_v02.pdf**
- Seguridad WiFi (resumen ejecutivo): **seguridad_wifi_resumen_ejecutivo_v02.pdf**

Como se trata de dos artículos del año 2005, hay aspectos que aún no existían, pero sí encontraréis bastante desarrollado los primeros protocolos de WiFi que nos servirán de base para avanzar sobre los más recientes.

Así y todo, como podéis ver en este artículo, la familia IEEE-802.11, ya se encontraba compuesta por los siguientes estándares:

- **802.11a**: (5,1-5,2 GHz, 5,2-5,3 GHz, 5,7-5,8 GHz), 54 Mbps. **OFDM**: (Multiplexación por división de frecuencias ortogonal)
- **802.11b**: (2,4-2,485 GHz), 11 Mbps.
- 802.11c: Define características de **AP** (Access Point), como Bridges.
- 802.11d: Múltiples dominios reguladores (restricciones de países al uso de determinadas frecuencias).
- 802.11e: Calidad de servicio (**QoS**).
- 802.11f: Protocolo de conexión entre puntos de acceso (AP), protocolo **IAPP** (Inter Access Point Protocol).
- **802.11g**: (2,4-2,485 GHz), 36 o 54 Mbps. **OFDM**: Multiplexación por división de frecuencias ortogonal. Aprobado en 2003 para dar mayor velocidad con cierto grado de compatibilidad a equipamiento 802.11b.
- 802.11h: **DFS** (Dynamic Frequency Selection), habilita una cierta coexistencia con HiperLAN y regula también la potencia de difusión.
- **802.11i**: Seguridad (aprobada en Julio de 2004).

- 802.11j: Permitiría armonización entre IEEE (802.11), ETSI (HiperLAN2) y ARIB (HISWANa).
- 802.11m: Mantenimiento redes wireless.

Para acotar únicamente el tema de seguridad, en este artículo solo se trataban **802.11a, b g** y **802.11i.**

Lo fundamental que debemos comprender, es que, cuando me conecto a un punto de acceso WiFi, primero debo realizar una autenticación robusta, y luego, una vez validado, se debe crear un canal seguro de forma individual para mí, que debe ser diferente al del resto de los clientes de ese punto de acceso, pues caso contrario, cualquier otra persona, conocida o no, podría analizar mi tráfico en esa red. Esta es una diferencia importante, respecto a una red LAN cableada, pues en estas redes, todos los usuarios conectados, se encuentran dentro de esa LAN. En un punto de acceso WiFi, por ejemplo el de un aeropuerto, la casi totalidad de las personas que se encuentran conectadas al mismo, probablemente sean desconocidas para mí.

Por esta razón, es que, en las redes WiFi, la criptografía cobra mayor importancia.

La forma más amplia de entender las tecnologías inalámbricas es bajo el concepto de **WLAN** (Wireless LAN). En este texto consideramos tres estándares de WLAN:

- **HomeRF**: Es una iniciativa lanzada por Promix, principalmente en EEUU y orientada exclusivamente al mercado residencial. Tiene sus bases en los estándares de teléfono digital inalámbrico mejorado (**DECT**).
- **BlueTooth:** Lo inició IBM, orientado al mercado comercial/ventas, y a la interconectividad de elementos de hardware. En realidad no compite con 802.11, pues tiene la intención de ser una estándar con alcance nominal de 1 a 3 metros y a su vez no supera los 1,5 Mbps.
- **IEEE-802.11**: Cubre todo el espectro empresarial.

Definiciones a tener en cuenta en este texto:

- Access control: es la prevención del uso no autorizado de recursos.
- Access Point (**AP**): cualquier entidad que tiene funcionalidad de estación y provee acceso a servicios de distribución vía wireless medium (**WM**) para estaciones asociadas.
- Ad Hoc network: red wireless compuesta únicamente por estaciones con iguales derechos.
- Portal: punto lógico desde el cual se conecta una red wireless con una no wireless.
- Station (**STA**): cualquier dispositivo que cumple con un nivel MAC conforme a 802.11 y un nivel físico que posee una interfaz wireless.
- Portable station: estación que puede ser movida de ubicación, pero que solo puede Tx o Rx en estado fijo.
- Mobile station: estación que permite Tx o Rx en movimiento.

IEEE-802.11 presenta dos topologías:

- Ad Hoc (o peer to peer): Dos o más clientes que son iguales entre ellos.
- Infraestructura: Red centralizada a través de uno o más Access Point (AP).

Descripción general de componentes de las mismas:

- **BSS** (Basic Service Set): es el bloque básico de construcción de una LAN 802.11. En el caso de tratarse de únicamente dos estaciones se denomina **IBSS** (Independent BSS), es lo que a menudo se denomina "Ad Hoc Netwok".
- **DS** (Distribution System): es la arquitectura que se propone para interconectar distintos BSS. El AP es el encargado de proveer acceso al DS, todos los datos que se mueven entre BSS y DS se hacen a través de estos AP, como los mismos son también STA son, por lo tanto, entidades direccionables.
- **ESS** (Extended Service Set): tanto BSS como DS permiten crear wireless network de tamaño arbitrario, este tipo de redes se denominan redes ESS.
- La integración entre una red 802.11 y una no 802.11 se realiza mediante un **Portal**. Es posible que un mismo dispositivo cumpla las funciones de AP y Portal.

En la figura **4-26** que sigue que se corresponde al estándar **IEEE-802.11**, podemos ver la arquitectura y el empleo del Portal para su integración con redes no 802.11.

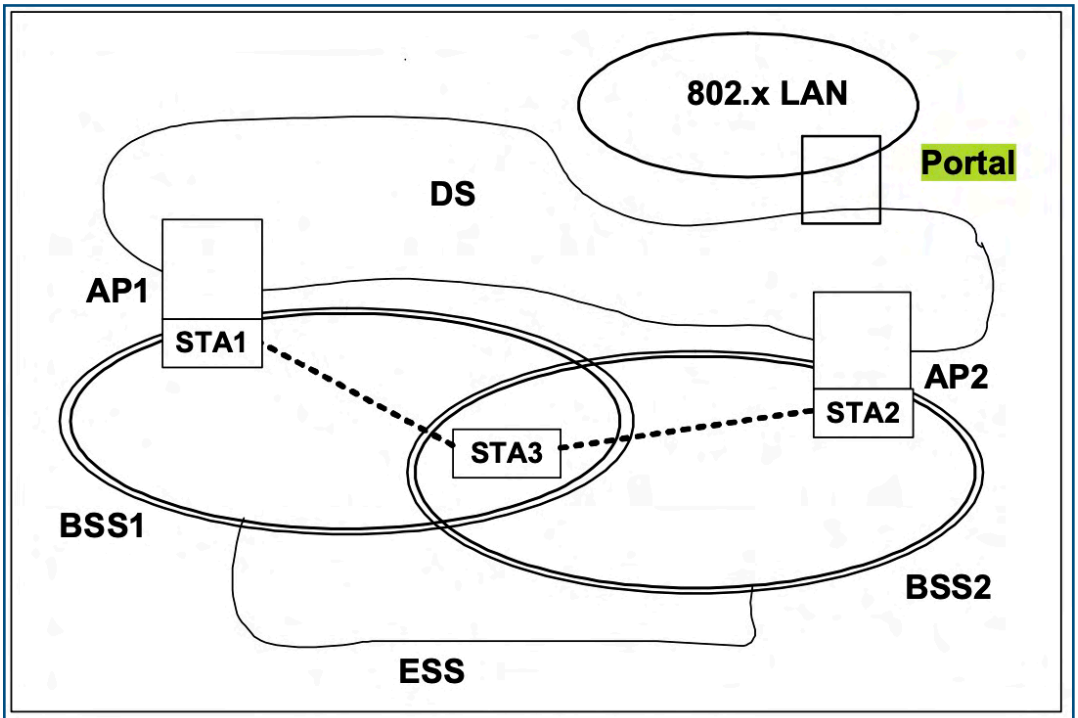


Figure 4-26—ESS link illustration

Los cuatro aspectos fundamentales que se deben tener en cuenta al diferenciar una red WiFi de una cableada, son:

- Autenticación
- Control de acceso
- Integridad

Autenticación y control de acceso

En cuanto a este tema, si consideramos nuevamente el apunte mencionado al principio (**seguridad_wifi_tecnico_v02.pdf**), en el mismo se describe un poco la historia de los métodos que emplea IEEE-802.11. El primero de ellos fue **WEP** (Wireless Equivalent Privacy). No lo desarrollaremos en este texto, pues si bien, no descartamos que alguna vez lo encuentres (y de hecho cuando desarrollemos "crack" para estas redes, lo explicaremos y lo practicaremos en detalle), en la realidad, tuvo muy poca duración, pues se demostró su fragilidad, en particular con el empleo de **RC4** (Rivest Cipher 4) que no posee una longitud de claves adecuada, y aparecieron muchas herramientas para explotarlo. Un par de años después de la aparición de WEP, se intenta solucionar el tema de RC4, reemplazándolo por **TKIP** (Temporal Key Integrity Protocol), pero como veremos más adelante, hoy en día también se desaconseja su uso.

Si deseas ampliar este tema, en el "ANEXO 2: *Teoría y funcionamiento de WEP*" del mencionado artículo lo encontrarás desarrollado en detalle.

Un aspecto de especial interés es el empleo de **IEEE-802.1x.** Este estándar no fue presentado para WiFi, tal cual ya lo hemos tratado en la **Charla 23**, sino para el acceso seguro **PPP** (Point to Point Protocol, en tecnologías de cable).

Una de las grandes características de WiFi es la de "no reinventar la rueda" y emplear todas las herramientas que ya existen y pueden prestar utilidad al mismo. IEEE-802.1x es uno de los mejores ejemplos de esto. Recordad que esta norma permite trabajar con **EAP** (Extensible Authentication Protocol: **RFC 2284**), y este último proporciona una gran flexibilidad (sobre todo a los fabricantes) en la metodología de autenticación.

Otra de las grandes ventajas de emplear IEEE-802.1x, es que el servidor de autenticación, permite también generar claves de cifrado **OTP** (One Time Password) muy robustas, tema en particular que ya lo posiciona como imprescindible en una red WiFi que se precie de segura.

Microsoft ofreció otra alternativa de mejora que inicialmente se denominó **SSN** (Simple Security Network), el cual es un subconjunto de **IEEE-802.11i,** y al mismo tiempo una implementación de **TKIP** (al estilo Microsoft). SSN lo adoptó IEEE-802.11i renombrándolo como **WPA** (WiFi Protected Access), en el año 2004 aparece **WPA2** que es la segunda generación del WPA. Este ya proporciona encriptación con **AES** (Advanced Encryptation Standard), que se menciona a continuación, y ofrece un alto nivel de seguridad en la autenticación de usuarios, hoy está basado en la norma **IEEE-802.11i** y forma parte de ella.

Aunque la WPA impulsa la seguridad WLAN, también fue inicialmente una solución temporal pues se orienta más hacia el Modo Conteo con el Protocolo del Código de Autenticación de Mensajes en cadena para el bloqueo de cifrado (Counter-Mode/CBC-Mac Protocol, que se abrevia: **CCMP**). Se trataba de un nuevo modo de operación para cifrado de bloques, que habilitaba a una sola clave para ser empleada tanto en autenticación como para criptografía (confidencialidad). Era un verdadero "Mix" de funciones, y su nombre completo proviene el "Counter mode" (**CTR**) que habilita la

encriptación de datos y el Cipher Block Chaining Message Authentication Code (**CBC-MAC**) para proveer integridad, y de ahí su extraña sigla CCMP.

El protocolo CCMP usa la Norma de Encriptación Avanzada (**AES**) para proporcionar encriptación más fuerte. Sin embargo, AES no estaba diseñada para ser compatible con versiones anteriores de software.

A pesar de todos los esfuerzos realizados, hoy en día se considera a TKIP y WPA como métodos insuficientes de seguridad, el mayor exponente de esta posición es **FIPS** (Federal Information Process Standard), que excluye a RC4 en las comunicaciones confidenciales. Su publicación **FIPS-197** de finales del 2001, define al estándar **AES** que se mencionó en el punto anterior, con clave mínima de 128 bits, como el aplicable a niveles altos de seguridad, aunque veremos más adelante, que hoy se emplean claves más grandes aún.

Este cifrado fue desarrollado por dos criptólogos belgas, "**Joan Daemen** y **Vincent Rijmen**" (se presentó como algoritmo "Rijndael") y surgió como ganador de un concurso mundial que se celebró en el año 2000, para definir la ultima generación de estos algoritmos.

El tema de AES tampoco es tan sencillo como parece, pues las implementaciones por software imponen una dura carga de trabajo al sistema, ocasionando demoras de rendimiento que pueden llegar al 50% de la tasa efectiva de transmisión de información, por lo tanto, se debe optimizar este aspecto para que sea asumido por el mercado.

La **WiFi Alliance** propone inicialmente dos tipos de certificación para los productos, cuyas características se presentan a continuación:

a. Modelo Empresas:
   - WPA:
     Autentication: IEEE 802.1x/EAP
     Encryptation: TKIP/MIC
   - WPA2:
     Autentication: IEEE 802.1x/EAP
     Encryptation: AES-CCMP

b. Modelo personal (SOHO/personal):
   - WPA:
     Autentication: PSK
     Encryptation: TKIP/MIC
   - WPA2:
     Autentication: PSK
     Encryptation: AES-CCMP

En enero de 2018, la Wi-Fi Alliance anunció **WPA3** como reemplazo de WPA2, con las siguientes opciones:

- WPA3 Personal 128 bits
- WPA3 empresarial 192 bits

El cifrado WPA3 está cubierto por el protocolo Galois/Counter Mode Protocol (**GCMP-256**). La seguridad WPA3 WiFi utiliza el modo de autenticación de mensajes hash de hasta 384 bits.

WPA3 mejorará la seguridad en redes abiertas con Opportunistic Wireless Encryption (**OWE**), que ofrece:

- PFS: Perfect Forward Secrecy
- Wi-Fi Easy Connect

WPA3 registra nuevos dispositivos a través de procesos que no requieren el uso de una contraseña compartida. Este nuevo sistema, es llamado Wi-Fi Device Provisioning Protocol (**DPP**). Con DPP, los usuarios utilizan códigos **QR** o etiquetas **NFC** para permitir que los dispositivos entren en la red… pero no nos adelantemos más que todo esto será desarrollado en detalle en la **Charla 31**.

www.darFe.es

Charla 30

Desenchufando - Jornada micológica.

Enlace al Video:

Resumen:

Este desenchufe de hoy, responde a nuestra filosofía de conectarnos con la naturaleza y cumplir con el viejo proverbio de "*mente sana en cuerpo sano*", así que saldremos a buscar setas.

Descripción detallada

Esto de la búsqueda de setas, tiene sus complicaciones, no es cuestión de salir alegremente por el bosque y juntar las que más nos gustan, sobre todo porque, como todo el mundo comenta, hay alguno que otro que se ha quedado en el camino, y no en el del bosque, sino en el de la vida.

En todo el mundo, existen asociaciones que dominan el tema, son referentes y poseen la experiencia necesaria para poder transmitírnosla de forma directa y en algunos paseos conjuntos. Casi todas ellas ofrecen cursos muy buenos, y sobre todo, eminentemente prácticos, que se realizan con paseos de recolección, donde aprendemos de primera mano cómo se realiza esta actividad.

Nuestra recomendación, es que, si deseáis introduciros en este fascinante mundo "**sí o sí**" lo hagáis de la mano de asociaciones, o de expertos en el tema, que nos sepan guiar y enseñar, no solo las setas comestibles, sino, un sinnúmero de vivencias que son importantes a tener en cuenta para mantener y cuidar nuestro entorno.

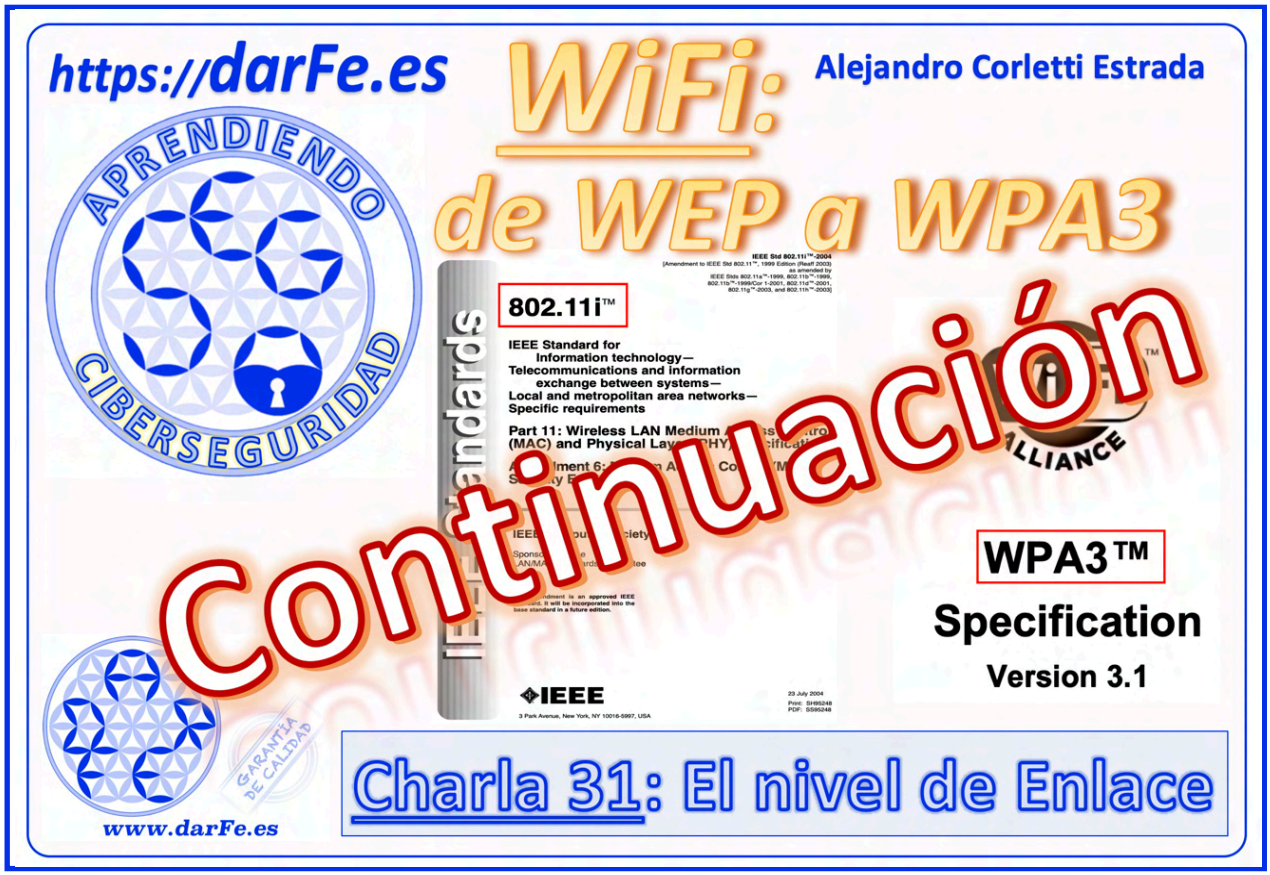
El resultado final es una excusa excelente para salir a caminar por el campo, monte o bosque, con la excusa e ilusión futura de disfrutar de verdaderos manjares gastronómicos, que como los hemos conseguido con sudor y esfuerzo, como todo en la vida logrado así, saben mucho más ricas.

No os perdáis esta oportunidad, y al menos probad algún día esta experiencia.

www.darFe.es

Charla 31

WiFi - de WEP a WPA3 (continuación)



Enlace al Video:

Resumen:

En esta charla, seguimos avanzando con la seguridad de las redes WiFi, y en particular con las mejoras que ofrece **WPA3**. Nos basaremos en el estándar **IEEE-802.11i**, y también en la última versión de **IEEE-802.11** del año 2020 que ya incorpora todos estos avances.

Finalizaremos con una captura de tráfico que nos permite verlo de forma técnica.

Descripción detallada

Para comenzar a desarrollar **WPA3**, nos basaremos en una especificación técnica **versión 3.1** "WPA3" de la **WiFi Alliance** que es la que estamos viendo en estas imágenes.

Este documento, nace en el año 2018, pero la fecha de la última versión, como hemos recuadrado abajo en **rojo**, es de noviembre del año 2022.

WPA3™ Specification v3.1

Document revision history

Version	Date YYYY-MM-DD	Remarks
1.0	2018-04-09	Initial release.
2.0	2019-12-20	Updated to include Fast BSS Transition, Server Certificate Validation, WPA3-Personal only and transition mode definition, WPA3-Enterprise only and transition mode definition
3.0	2020-12-14	Update to include SAE-PK, WIFI URI, Transition Disable indication, and Privacy Extension mechanisms
3.1	2022-11-23	Update to Transition Disable indication section to clarify the use of the mechanism and to add a requirement prohibiting an AP from enabling Transition Disable indication by default.

Sobre este documento, nos basaremos en los aspectos, que según nuestro criterio, son claves. El primero de ellos es, tal cual hablamos en la charla anterior, que existe un "modo personal" y un "modo empresa" -

El punto **2.4** de la especificación, nos presenta el modo personal, en el cual destacamos, que su recomendación es no habilitar en el Access Point **WPA versión 1**, como tampoco **WEP** y **TKIP** en el mismo **BSS** (Basic Service Set). Por último que comencemos a considerar el empleo de **SAE** (Simultáneos Authentication of Equals), que es la arquitectura más robusta, y la iremos desarrollando en esta charla.

2.4 Additional Requirements on WPA3-Personal modes

The following additional requirements apply to all WPA3-Personal modes:

1. An AP shall not enable WPA version 1 on the same BSS with WPA3-Personal
2. An AP shall not enable WEP and TKIP on the same BSS as WPA3-Personal
3. When connecting to an AP that supports both SAE and PSK, a STA shall connect using SAE.
4. On an AP, whenever any PSK AKM (00-0F-AC:2 or 00-0F-AC:6) is enabled, the WPA3-Personal transition mode shall be enabled by default, unless explicitly overridden by the administrator to operate in WPA2-Personal only mode

TKIP: temporal key integrity protocol

SAE: simultaneous authentication of equals

Si analizamos el modo empresa, como podemos ver en la imagen 3.4 de la derecha, nuevamente nos reitera el tema de WPA versión 1 y TKIP.

3.4 Additional Requirements on WPA3-Enterprise modes

The following additional requirements apply to all WPA3-Enterprise modes:

1. An AP shall not enable WPA version 1 on the same BSS with WPA3-Enterprise.
2. An AP shall not enable WEP and TKIP on the same BSS as WPA3-Enterprise.

4.1.2 Enterprise modes

1. FT Authentication using IEEE Std 802.1X (SHA 256) 00-0F-AC:3
2. Authentication using IEEE Std 802.1X (SHA256) 00-0F-AC:5
3. Authentication using IEEE Std 802.1X 00-0F-AC:1

El otro tema que también nos interesa, es el que nos presenta en el punto **4.1.2** (imagen de la izquierda), en el cual, nuevamente habla del modo empresa, y nos reitera, una vez más, su recomendación de emplear **IEEE-802.1x**. En este punto, a su vez, aparece por

primera vez el empleo de **SHA-256** (Secure Hash Algorithm), es decir con una longitud de 256 bits, recordad que el tema de autenticación había comenzado inicialmente con RC4 de 64 bits, con lo que ya estamos multiplicando por cuatro la longitud de este algoritmo.

Solo a título informativo, pues, más adelante lo desarrollaremos con mucho más detalle, definimos este concepto de "**Hash**" como una función resumen. En concreto, se trata de algoritmos matemáticos, que toman como entrada un fichero de cualquier longitud y nos entregan como resultado un nuevo fichero de longitud siempre fija, como por ejemplo estamos viendo en SHA-256, de esta longitud de bits, y a su vez generan fortaleza para el control de integridad; es decir, nos garantizan que el fichero de entrada original no ha sido alterado. Por esta razón, en el proceso de autenticación es de vital importancia. La función "hash", es tan vital, que más adelante le dedicaremos un buen tiempo para que la entendáis con todo lujo de detalle, por ahora, sed pacientes y quedémonos con estas breves ideas.

El último punto que deseamos presentar es el **6.2**, en el cual el aspecto de interés, tal cual subrayamos en rojo, es que ya nos habilita el empleo de clave pública.

6.2 SAE-PK overview

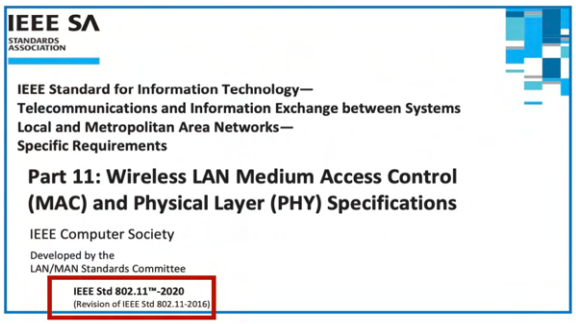
SAE-PK is an extension to SAE authentication. The additional signaling required for SAE-PK is carried in the same IEEE 802.11 Authentication frames that carry SAE Commit and Confirm messages.

When an AP sends an SAE Confirm message to a STA, the frame contains the AP's public key, a Modifier value (wrapped using a Key Encryption Key derived from the SAE keyseed), and a digital signature where the input data comprises the SAE public values used by both AP and STA, the AP's public key and Modifier, and the MAC addresses of both AP and STA signed with the private key analog of the AP's public key.

La clave pública, tal cual desarrollamos en el **Charla 25**, forma parte de la criptografía asimétrica y, recordad que nos incrementa sensiblemente el nivel de seguridad. El tema de criptografía asimétrica, también será otro de los puntos que desarrollaremos con mucho más detalle en charlas posteriores.

En la actualidad, la mayoría de los dispositivos ya soportan el empleo de WPA3, como podéis ver en la imagen izquierda, que se trata de la configuración WiFi, que en este caso se corresponde a un portátil Macintosh.

A continuación volveremos a hablar de la norma **IEEE-802.11** (sin la "**i**") y centrándonos en la versión del año 2020, pues en la misma, hay aspectos de seguridad que van relacionados con la confidencialidad y autenticación.



4.5.4.2 Authentication
IEEE Std 802.11 defines five IEEE 802.11 authentication methods:
- Open System authentication (is a null authentication algorithm).
- Shared Key authentication
- FT authentication (FT: fast BSS transition)
- Simultaneous authentication of equals (SAE)
- FILS authentication (fast initial link setup).

En cuanto a autenticación, como podemos ver en el punto **4.5.4.2**, nos ofrece cuatro opciones. La primera de ellas Open System authentication, es el algoritmo nulo, es decir es cuando no hay autenticación, este es el caso de las redes abiertas a las que podemos conectarnos, sin ningún tipo de negociación de usuario, ni contraseña. La segundo es nuestro conocido secreto compartido. FT aplica cuando se produce un cambio de un BSS a otro, y para el usuario es transparente. SAE es una variante de "Dragonfly Key Exchange" que como su nombre lo indica, se emplea para el intercambio de claves, está definido en la **RFC 7664**, y se basa en el intercambio de claves "**Diffie–Hellman**" que explicaremos con todo detalle más adelante y, reemplaza el método de secreto compartido. Finalmente FILS es la configuración inicial para un enlace rápido, se suele emplear ante un corte inesperado o un re enlace.

4.5.4.4 Data confidentiality
IEEE Std 802.11 proporciona los siguientes protocolos de seguridad para la protección de tramas de gestión
CCMP (CCMP CTR with CBC-MAC Protocol)
GCMP (Galois/Counter Mode Protocol)

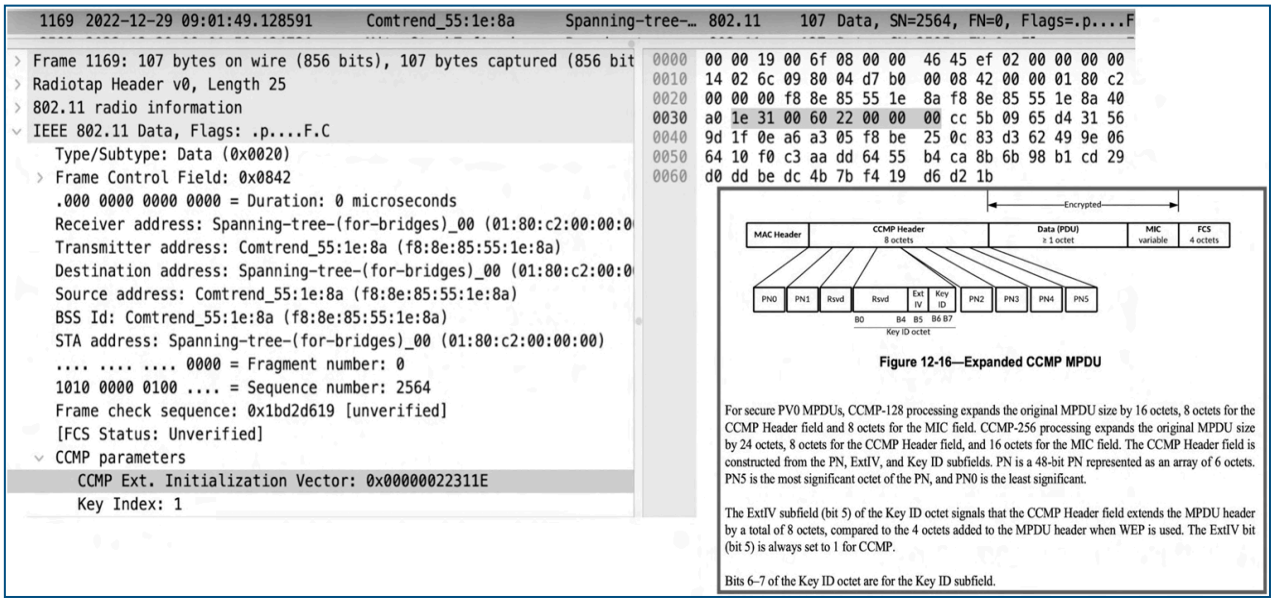
En el punto **4.5.4.4** Nos presenta dos nuevos algoritmos que mejoran la confidencialidad, en particular, como podemos ver, para mejorar las tramas de gestión. Como desarrollaremos en las charlas siguientes, en WiFi existen diferentes tipos de trama, y justamente las de gestión, son tal vez las más importantes, pues son las que se emplean para administrar la comunicación. Debido a ello, en casi todas las comunicaciones inalámbricas se las trata con especial atención, en la telefonía móvil, por ejemplo, mucho más aún.

El punto **5.1.2** nos presenta los nuevos servicios de seguridad que ofrece. De este punto debemos destacar que ya considera todos los nuevos protocolos y en particular que declara obsoletos WEP y TKIP. Por esta razón es que hoy en día no debemos permitirlos en nuestras redes.

5.1.2 Security services
Los servicios de seguridad en IEEE Std 802.11 son proporcionados por el servicio de autenticación y el CCMP (CCMP CTR with CBC-MAC Protocol) , GCMP (GCMP Galois/Counter Mode Protocol) y BIP (broadcast/multicast integrity protocol).
Los servicios de seguridad proporcionados por CCMP y GCMP en IEEE Std 802.11 son los siguientes:
a) Confidencialidad de datos
b) Autenticación
c) Control de acceso junto con la gestión de capas.
WEP está obsoleto.
El uso de TKIP está obsoleto.

Para ir cerrando el tema, vamos a presentar a continuación la **figura 12-16** de esta norma, y la describiremos de forma técnica y real por medio de una captura de tráfico.

En esta captura se despliega, justamente el encabezado de IEEE-802.11, de una trama de datos. En la misma, se encuentran coloreados en gris los ocho octetos del campo CCMP. Os invitamos a que comparéis estos ocho octetos, con lo que expande la figura 12-16 del CCMP Header para que saquéis vuestras propias conclusiones y si queréis verificar si son ciertas, pues mirad el video de esta charla.



Volver al índice

www.darFe.es

Charla 32

WiFi - Frecuencias, canales, logaritmos…

Enlace al Video: 

Resumen:

En esta charla desarrollaremos conceptos muy importantes sobre las frecuencias que emplea WiFi, los tipos de canales que tiene asignados, sus limitaciones y alcances.

Para comprender el detalle de estas técnicas, es importante, ser capaz de medir su potencia, y determinar las interferencias que se reciben, por lo que hablaremos también de cómo se mide y calculan los **decibelios**, como magnitud de medición de potencia.

Descripción detallada

Esta charla de hoy, si bien es “aburridísima…”, haremos todo lo posible para que la disfrutéis, pues no podemos dejar pasar por alto estos temas matemáticos y logarítmicos si queréis comprender el detalle de las señales.

Comenzaremos a tratar el tema de las señales desde un punto de vista de las que nos afectan en Europa y Latinoamérica (**Latam**), pues hay otros rangos y clasificaciones en el mundo, pero no los tendremos en cuenta.

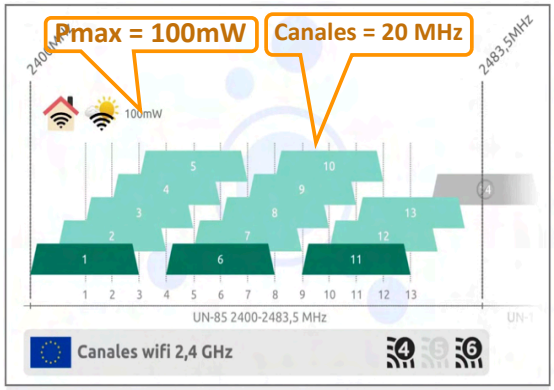
Canal	Frecuencia central	Ancho de banda
1	2.412 GHz	2.401 GHz - 2.423 GHz
2	2.417 GHz	2.406 GHz - 2.428 GHz
3	2.422 GHz	2.411 GHz - 2.433 GHz
4	2.427 GHz	2.416 GHz - 2.438 GHz
5	2.432 GHz	2.421 GHz - 2.443 GHz
6	2.437 GHz	2.426 GHz - 2.448 GHz
7	2.442 GHz	2.431 GHz - 2.453 GHz
8	2.447 GHz	2.436 GHz - 2.458 GHz
9	2.452 GHz	2.441 GHz - 2.463 GHz
10	2.457 GHz	2.446 GHz -2.468 GHz
11	2.462 GHz	2.451 GHz - 2.473 GHz
12	2.467 GHz	2.456 GHz - 2.478 GHz
13	2.472 GHz	2.461 GHz - 2.483 GHz
14	2.484 GHz	2.473 GHz - 2.495 GHz

Como podéis ver en la tabla de la derecha, en estas regiones mencionadas, para el caso de la frecuencia de **2,4 GHz**, que fue la primera que se empleó en WiFi, existen definidos 14 canales. Este rango de frecuencias, comienza en 2,412 GHz y finaliza en 2,495 GHz, es decir ocupa una ancho de bada total de **83 MHz**.

Sin ser Einstein, podemos darnos cuenta que en 85 MHz, no entran 14 canales de 20 MHz, pues si fueran secuenciales (cada uno siguiendo al anterior), serían 14 x 20 = 280 MHz. Inclusive, si miramos la tabla, por ejemplo entre el canal uno, dos y tres, veríamos que:

- Canal 1: 2.401 GHz - 2.423 GHz
- Canal 2: 2.406 GHz - 2.428 GHz
- Canal 3: 2.411 GHz - 2.433 GHz

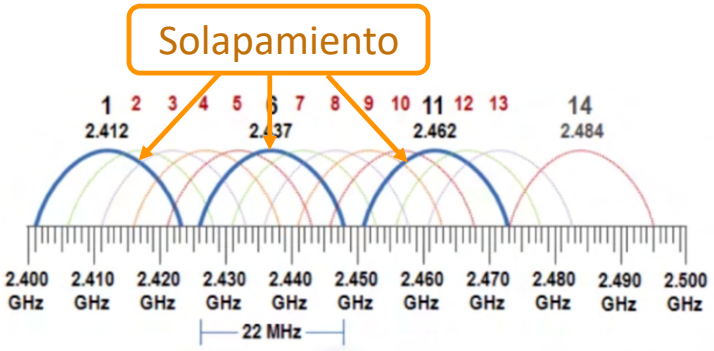
Es decir, se solapan todos ellos.



Canales wifi 2,4 GHz en España junto al canal ilegal 14

Cada uno de ellos, como podemos ver en la imagen de la izquierda, ocupa un ancho de banda de **20 MHz** y se solapan entre sí. Otro dato que por ahora solamente presentamos, pero que iremos viendo en detalle, es que esta frecuencia está restringida a **100mW** (mili Watts) de potencia de emisión.

Este solapamiento, si lo analizamos desde una gráfica de frecuencias, podemos representarlo como la imagen de abajo.



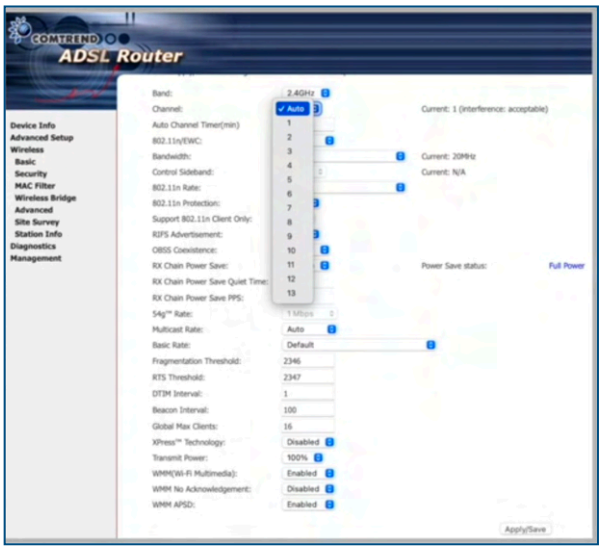
¿Por qué razón se diseña este solapamiento?

Recordemos que las frecuencias más bajas, son las que mayor alcance tienen. Una potencia de 100mW es suficiente para alcanzar varios cientos de metros de distancia, por lo que, en este rango de frecuencias, es muy probable que nos encontremos situaciones en las cuáles, al encender nuestra tarjeta WiFi del

ordenador, estemos recibiendo señales de más de un punto de acceso WiFi (de mi vecino, de la otra empresa, del cibercafé, del móvil, etc.).

Esta frecuencia de 2,4GHz, es la que mayor alcance tiene dentro de la familia IEEE-802.11. Por esta razón, tal cual muestra la imagen anterior (con flechas **color naranja**), están definidas tres bandas principales para estos canales, la banda 1, 6 y 11, que como se aprecia también en la imagen previa, están resaltadas en **azul**. Si prestáis atención, estos tres canales, no se solapan entre sí. Es decir el canal 1 finaliza con 2,423 GHz, el canal 6 comienza con 2,437 GHz y finaliza con 2,448 GHz, y el canal 11 comienza con 2,456 GHz (verificadlo en la tabla inicial de frecuencias).

Ahora que vamos entendiendo estas frecuencias, si administramos una arquitectura de red en nuestra empresa, cuando comencemos a implantar puntos de acceso WiFi, una tarea que debemos realizar, es analizar qué frecuencias están generándome interferencia, y configurar nuestros puntos de acceso, justamente en las bandas en las cuáles menor ruido encuentre.



Como podemos ver en la imagen de la derecha, todos los puntos de accesos WiFi, ofrecen la posibilidad de configurar los canales, o bandas, con los que deseamos que operen. También este concepto nos sirve, si dentro mi empresa tengo más de un punto de acceso WiFi, entonces a cada uno de ellos, es conveniente asignarle bandas bien diferenciadas para que tampoco se solapen ellos entre sí.

> **IMPORTANTE**: Siempre que haya solapamientos, el rendimiento de la red WiFi se degrada y tendremos menor velocidad de transferencia

Por esta razón, es que la charla de hoy (aburridísima…) es fundamental, pues en la medida que sepamos medir y analizar potencias y frecuencias, mejor será el rendimiento de nuestras redes WiFi, y optimizaremos su empleo. Así que sigamos adelante con nuestra aburrida charla de hoy.

Otra reflexión importante que debemos considerar, es que el empleo de esa potencia de 100mW, también debo medirla y estudiarla, pues si no necesito que mi red WiFi llegue hasta las instalaciones de mi vecino, o hasta la calle, donde pasa todo el mundo, es imprescindible que ajuste la potencia de emisión de cada punto de acceso WiFi para que llegue exclusivamente a donde deba llegar, y no más allá. En Ciberseguridad, esto se llama "**reducir la superficie de ataque**". En el video de esta charla, contamos una experiencia real de un CPD de Ciudad de México, en el cual durante una auditoría que realizamos allí, se detectó que el mismo, emitía hasta 200 metros fuera de sus instalaciones, es decir alcanzaba a todos sus vecinos y competencia, a su vez como no estaba debidamente configurado, presentaba brechas de seguridad que se podían explotar con bastante facilidad. Así que fijaros, como al sumar errores, se pueden producir importantes brechas de seguridad.

La segunda potencia que presentamos en las charlas anteriores es la de **5GHz**.

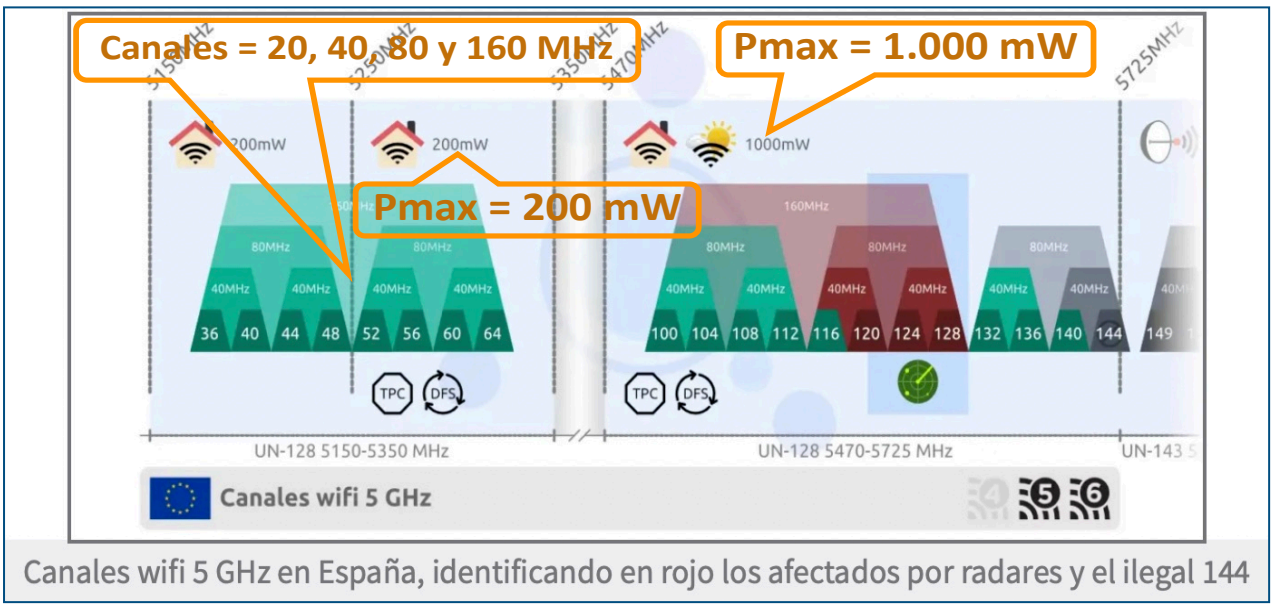
Este espectro va desde los 5,150GHz a 5,725 GHz, aquí ya tenemos una ancho de banda muy superior al anterior, estamos hablando de **575 MHz** (frente a los 83 MHz de la frecuencia anterior), pero no olvidemos que una señal de 5GHz, no va a tener el alcance, ni la penetración que teníamos con la de 2,4GHz.

CHANNEL NUMBER	FREQUENCY MHZ	EUROPE (ETSI)
36	5180	Indoors
40	5200	Indoors
44	5220	Indoors
48	5240	Indoors
52	5260	Indoors / DFS / TPC
56	5280	Indoors / DFS / TPC
60	5300	Indoors / DFS / TPC
64	5320	Indoors / DFS / TPC
100	5500	DFS / TPC
104	5520	DFS / TPC
108	5540	DFS / TPC
112	5560	DFS / TPC
116	5580	DFS / TPC
120	5600	DFS / TPC
124	5620	DFS / TPC
128	5640	DFS / TPC
132	5660	DFS / TPC
136	5680	DFS / TPC
140	5700	DFS / TPC
149	5745	SRD
153	5765	SRD
157	5785	SRD
161	5805	SRD
165	5825	SRD

Como podemos apreciar en al imagen de abajo, esta nueva banda de frecuencias, nos permite ahora, agrupar o configurar canales con un ancho de banda desde los 20MHz, 40MHz, 80MHz o 160MHz.

Si analizamos más en detalle la imagen de abajo, veremos también que hay una brecha en el medio de estas bandas, entre los 5,350GHz y los 5,470GHz que no se puede utilizar. Esta banda, se denomina **U-NII 2B** (Infraestructura Nacional de Información No Licenciada, por sus siglas en inglés) y no ha sido asignada aún para este uso.

También vemos una zona que, exactamente en la frecuencia de 5,250GHz se define con una línea punteada vertical y a partir de esta, aparecen abajo dos mensajes, "**TPC**" (Transmit Power Control) y luego "**DFS**" (Dynamic Frequency Selection o Selección Dinámica de Frecuencias). En 2014, la **FCC** (Federal Communications Commission, de EEUU) emitió reglas nuevas para todos los dispositivos debido a interferencia con sistemas de radar meteorológico del gobierno.

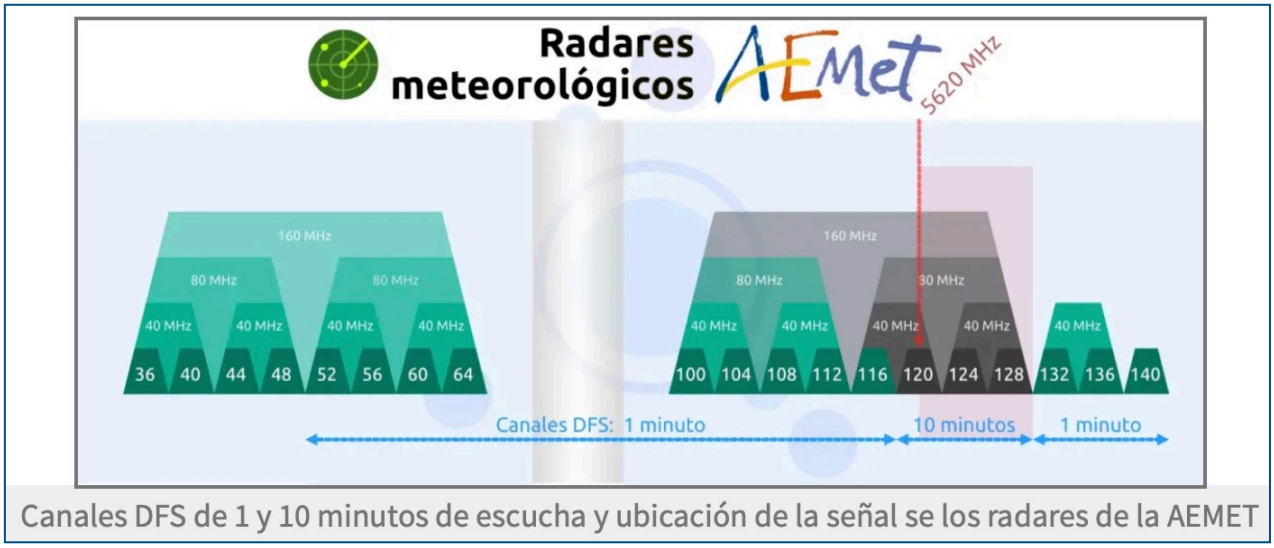


Canales wifi 5 GHz en España, identificando en rojo los afectados por radares y el ilegal 144

Estos sistemas emiten justamente dentro de estas bandas. Aquí es donde aplican DFS y TPC, y funcionan del siguiente modo. Cada vez que se intenta realizar una conexión con un punto de acceso que emplea la banda de 5GHz, el mismo, antes de asignar alguno de estos canales, tiene la obligación de hacer una escucha de estas frecuencias.

Si prestamos atención en la imagen que sigue abajo, vemos que las bandas 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136 y 140, el punto de acceso debe escuchar durante 1 minuto, si en ese tiempo, no detecta señales externas puede asignarlas. Sin

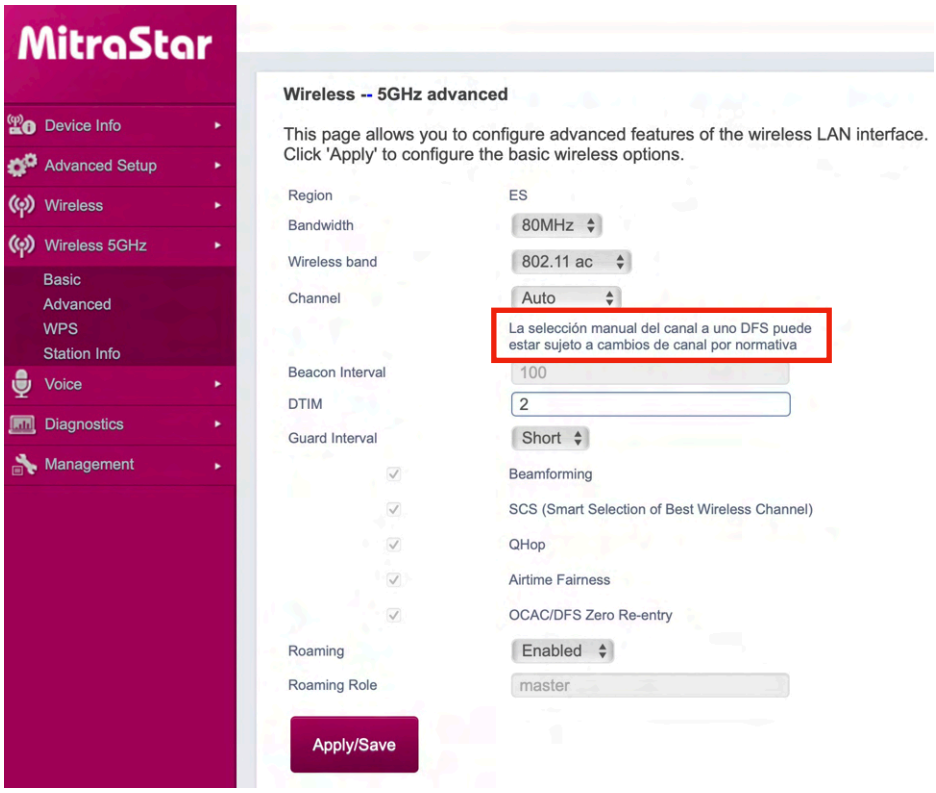
embargo, si nos fijamos en las bandas 120 124 y 128, sombreadas en **rojo**; estos rangos son más delicados en cuanto al empleo de radares, por esta razón, antes de asignarlos, el punto de acceso debe esperar, en algunos casos, hasta 10 minutos. Dentro de esos rangos, a su vez si escuchara algún tipo de señal débil, pueden ser empleados, pero reduciendo su potencia (TPC) para no interferirlos.



Canales DFS de 1 y 10 minutos de escucha y ubicación de la señal se los radares de la AEMET

Estas medidas han sido impuestas para preservar el empleo de radares, frente a las redes WiFi, y podemos verificarlo muy fácilmente, si nos conectamos a este tipo de puntos de acceso, veremos que desde el momento que activamos nuestra tarjeta WiFi en el ordenador, hasta que nos aparezcan los puntos de acceso 5GHz, suelen demorarse un tiempo más que los de 2,4GHz.

Como podemos ver en la imagen de la derecha, al configurar este tipo de frecuencias, los puntos de acceso nos lo informan. Hemos recuadrado en **rojo** el tema de DFS.

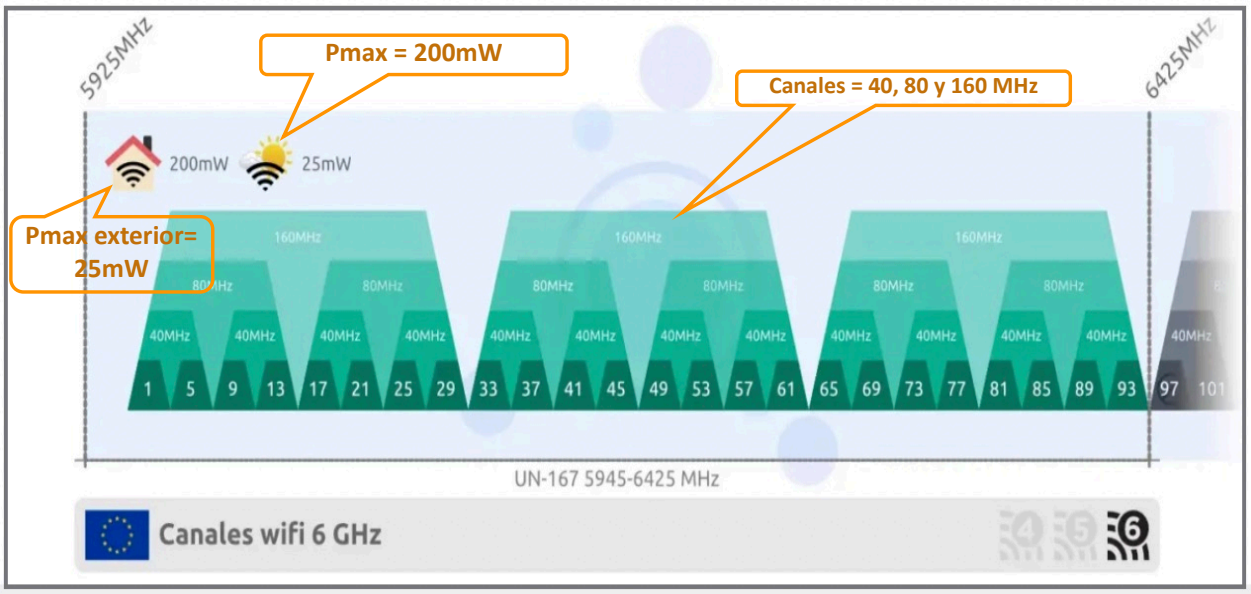


Como idea final de las dos imágenes anteriores de las bandas de 5GHz, solo deciros que, si prestamos atención, al final de estas imágenes veremos las bandas 132, 136 y 140; estas tres bandas, son las menos empleadas generalmente, así que si queremos tener una red 5G libre de interferencias, y nuestro punto de acceso nos permite configurarlas, no dejéis de usarlas, pues son sobre las que obtendremos mejor rendimiento.

Un detalle adicional en 5GHz son las limitaciones de potencia entre el uso interior y exterior. En la primera de las imágenes de bandas, hemos resaltado con dos llamadas en color **naranja** potencias máximas tanto interiores como exteriores. Las mismas, como podéis comparar con la banda de 2,4GHz (100mW) son superiores. La exterior nos permite 1000mW con la idea de sensores exteriores, e interiores 200mW, ambas potencias sujetas al TPC que ya hemos comentado.

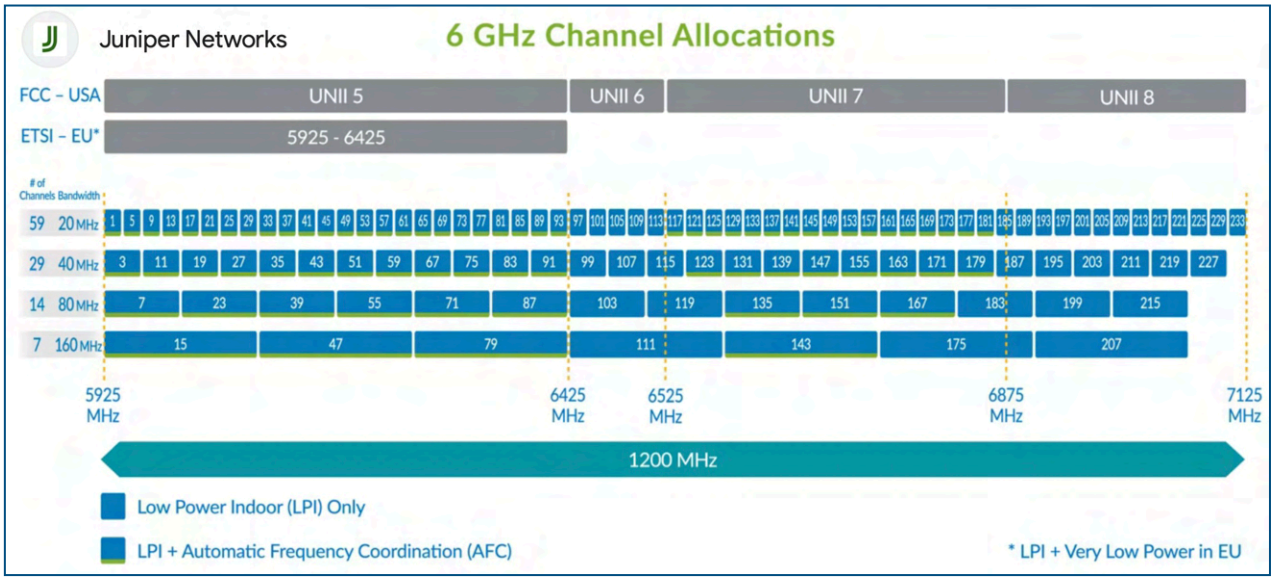
El último espectro que desarrollaremos es el de **6GHz**, que como podemos ver en la imagen que sigue, define un rango de frecuencias que va desde los 5,925GHz hasta los 6,425GHz, con lo cual tenemos un ancho de banda total de 500MHz (*6.425MHz - 5.925 MHz = 500MHz*). Nos permite agrupar canales de 40MHz, 80MHz y 160MHz, y su potencia máxima de emisión es de 200mW en exterior y 25mW en interiores. Fijaros que, a diferencia de la banda de 5GHz cuya potencia exterior es de 1000mW, en esta caso la limit a 25mW, con lo que nos pone de manifiesto que no está diseñada para usos exteriores de cierto alcance en distancia. Por último, como podemos ver en la imagen de abajo, no es un rango de frecuencias que se encuentre con solapamientos de otros usos, es una frecuencia muy limpia.

Una consideración que podemos hacer sobre el párrafo anterior, es comparar esta frecuencia con las restricciones de las bandas anteriores, por ejemplo en la de 2,4GHz, el canal 14 en Europa está restringido, en la banda de 5GHz, el canal 144 también, pues casi, casi, empieza a solaparse con el uso en aviación (ver Charla 20), y en esa misma banda, recordad los temas de DFS y TPC. Sin embargo, como hemos mencionado esta nueva banda de 6GHz, no encuentra otras asignaciones, solo a partir del canal 97 en adelante es donde sí empieza a haber restricciones.

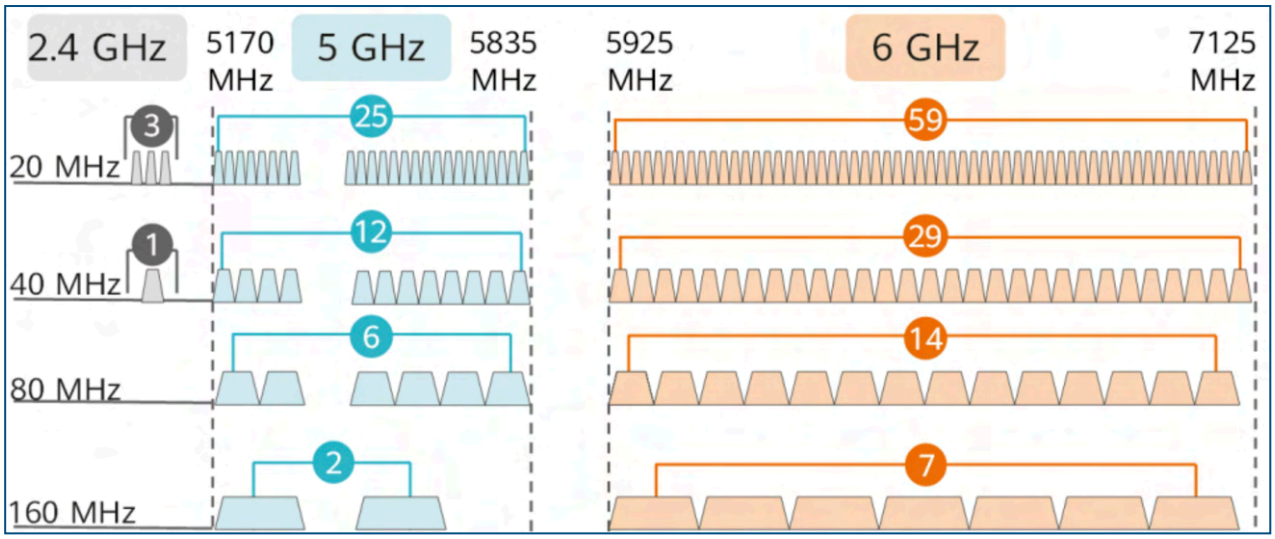


Canales WiFi 6E en 6 GHz en España, con los canales ilegales en Europa a partir del 97

Presentamos a continuación una imagen de la empresa Juniper en la que se presentan las diferentes agrupaciones que ofrece la banda de 6GHz, y también los rangos permitidos en al Unión Europea.



En la imagen que sigue, podemos ver un resumen gráfico de todas las frecuencias que hemos desarrollado en este capítulo.



Logaritmos

Ahora sí que empezamos con lo “aburridísimo…”, pero verás la importancia que tendrá para que seas un verdadero experto en WiFi.

Logaritmo en base a de b, es igual a c, “sí y solo sí” a elevado a la c es igual a b.

Esta especie da trabalenguas, se representa de la siguiente forma:

$$\mathbf{Log_a\ b = C \Leftrightarrow a^C = b}$$

Vamos a meternos con logaritmos, pues, como iremos viendo, es el tipo de respuesta que tiene el oído humano.

Matemáticamente, se dice que el oído humano tiene una respuesta logarítmica, pues si tuviera una respuesta directa, nuestro tímpano sería incapaz de soportar los millones de Watts de potencia de sonido de cualquier recital de rock actual.

El sonido más tenue que puede detectar un oído humano tiene una amplitud de: 20 millonésimas de pascal (**20 µPa**)

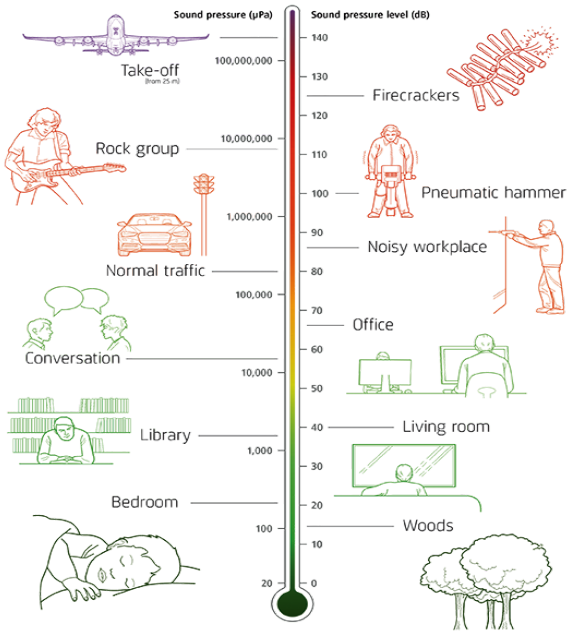
- *5000 millones de veces menos que la presión atmosférica (1 atm ≈ 105 Pa).*

Asombrosamente, nuestro oído tolera presiones sonoras más de **un millón de veces** superiores a ese umbral mínimo.

El umbral de audición de 20 µPa, que se define como **0 dB**.

Si multiplicamos la presión sonora en pascales por 10, el nivel en dB aumenta en 20 dB.

En la figura se muestran los niveles de presión sonora (**SPL**) en **dB** y Pa de distintos sonidos familiares.



En la imagen de la izquierda, podemos ver claramente la relación entre **potencia** y **decibelios**.

Del recuadro siguiente, tenemos que destacar la relación entre **dB** y **dBm** pues suele confundirse. Tal cual se expresa en el cuadro, el **dB** es siempre una magnitud relativa entre dos valores, sin embargo el **dBm**, sí es una magnitud absoluta, pues tendrá como denominador 1mW. Remarcamos este concepto, pues es muy habitual que se expresen valores de sonido o audio como dB, cuando en realidad la referencia de estas mediciones son dBm.

dB y dBm *(decibelios-mW)*

La unidad de medida "**bel**" recibe su nombre en honor a **Alexander Graham Bell.**

Expresa la relación de dos valores de potencia en una escala logarítmica.

El **dBm** (*o dBmW*) es una unidad de potencia absoluta se expresa con referencia a 1mW.

Desarrollemos estas fórmulas.

Potencia [W]

$$\text{Decibelio [dB]} = 10*\text{Log}_{10}(P/P_0)$$

P *(potencia medida),* P_0 *(potencia de referencia)*

El **decibelio**, como podemos ver en la fórmula anterior, es igual a 10, multiplicado por un logaritmo en base 10 de una potencia medida, sobre una cierta potencia de referencia, esto es justamente lo relativo, pues entran en juego estas dos potencias.

$$\textbf{dBm} = 10*\text{Log}_{10}(P/1\text{mW})$$

En cambio, cuando hablamos de **dBm**, como podemos ver a la izquierda, la potencia de referencia es **1mW**.

Volvamos a nuestras fórmulas logarítmicas.

Como podemos ver a nuestra derecha, el logaritmo se puede expresar en diferentes bases. En este ejemplo, lo vemos con base 10 y luego con base 2.

$$\text{Log}_a\ b = C \Leftrightarrow a^C = b$$

$$\text{Log}_{10}\ 1000 = 3 \Leftrightarrow 10^3 = 1000$$

$$\text{Log}_2\ 16 = 4 \Leftrightarrow 2^4 = 16$$

El logaritmo en base 2, es la base de la informática y transmisión de información, es el método para transformar los bits que posee un código, respecto a la cantidad de posibilidades que nos ofrece el mismo.

En la imagen que sigue, se presentan varios ejemplos de aplicación de la fórmula logarítmica para calcular los dBm de diferentes potencias. En estos cálculos podemos ver claramente como un aumento importante de potencia, no lo es tanto en la escala logarítmica. Matemáticamente, se dice que la escala de potencia crece en forma exponencial, y la logarítmica de forma lineal, es decir es una respuesta mucho más suave que la de potencia.

-40 dBm = $10*\text{Log}_{10}(0{,}0001/1\text{mW})$

-20 dBm = $10*\text{Log}_{10}(0{,}01/1\text{mW})$

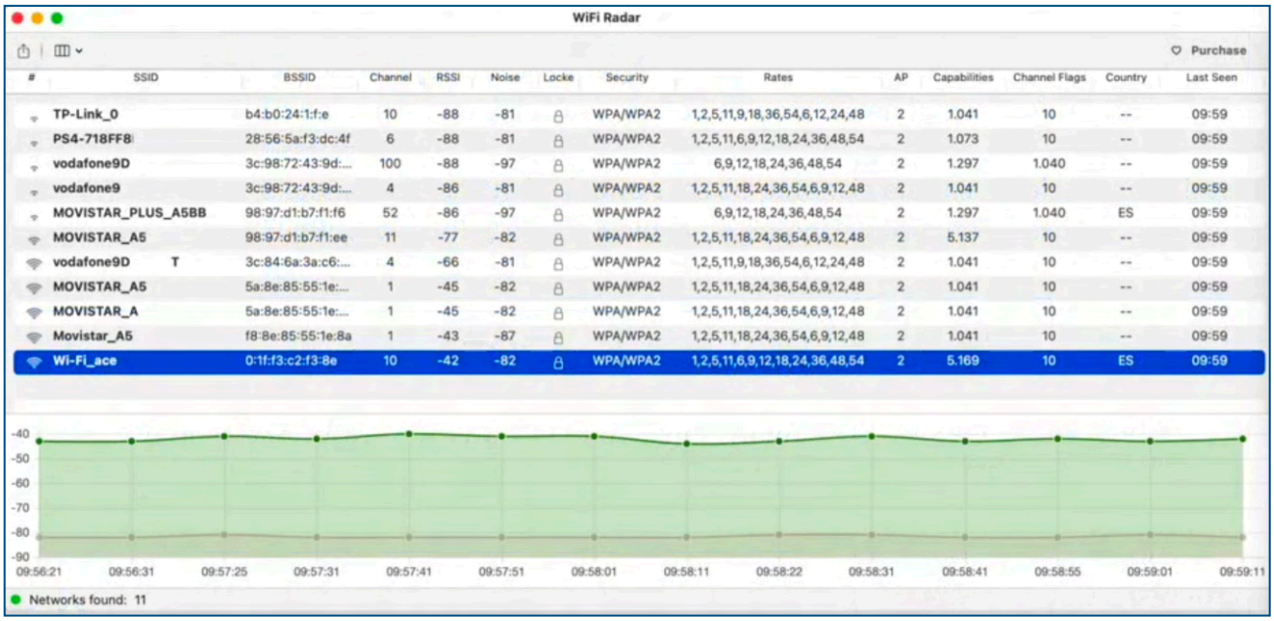
0 dBm = $10*\text{Log}_{10}(1/1\text{mW})$

10 dBm = $10*\text{Log}_{10}(10\text{mW}/1\text{mW})$

Potencia (dBm)	Potencia (W)
-40 dBm	0,0001 mW
-30 dBm	0,001 mW
-20 dBm	0,01 mW
-10 dBm	0,1 mW
0 dBm	1 mW
1 dBm	1,2589 mW
2 dBm	1,5849 mW
3 dBm	1.9953 mW
4 dBm	2,5119 mW
5 dBm	3,1628 mW
6 dBm	3.9811 mW
7 dBm	5,0119 mW
8 dBm	6.3096 mW
9 dBm	7,9433 mW
10 dBm	10 mW
20 dBm	100 mW
30 dBm	1000 mW
40 dBm	10000 mW
50 dBm	100000 mW

Estos cálculos nos interesan mucho en las redes WiFi, pues cuando medimos la intensidad de diferentes puntos de acceso, cuanto más negativo sea el valor de dBm, implicará que peor intensidad de la señal tendré, con lo cual ese punto de acceso WiFi, nos ofrecerá un servicio bastante malo de transferencia.

En la imagen que sigue, se aprecia la captura de varios puntos de acceso, a través de la herramienta **WiFi Radar**, sobre la que avanzaremos en otros capítulos, y en la misma se aprecia en la cuarta columna el valor de **RSSI**, que no es más ni menos que la potencia recibida, medida en dBm.



#	SSID	BSSID	Channel	RSSI	Noise	Locke	Security	Rates	AP	Capabilities	Channel Flags	Country	Last Seen
	TP-Link_0	b4:b0:24:1:f:e	10	-88	-81		WPA/WPA2	1,2,5,11,9,18,36,54,6,12,24,48	2	1.041	10	--	09:59
	PS4-718FF8	28:56:5a:f3:dc:4f	6	-88	-81		WPA/WPA2	1,2,5,11,6,9,12,18,24,36,48,54	2	1.073	10	--	09:59
	vodafone9D	3c:98:72:43:9d:...	100	-88	-97		WPA/WPA2	6,9,12,18,24,36,48,54	2	1.297	1.040	--	09:59
	vodafone9	3c:98:72:43:9d:...	4	-86	-81		WPA/WPA2	1,2,5,11,18,24,36,54,6,9,12,48	2	1.041	10	--	09:59
	MOVISTAR_PLUS_A5BB	98:97:d1:b7:f1:f6	52	-86	-97		WPA/WPA2	6,9,12,18,24,36,48,54	2	1.297	1.040	ES	09:59
	MOVISTAR_A5	98:97:d1:b7:f1:ee	11	-77	-82		WPA/WPA2	1,2,5,11,18,24,36,54,6,9,12,48	2	5.137	10	--	09:59
	vodafone9D T	3c:84:6a:3a:c6:...	4	-66	-81		WPA/WPA2	1,2,5,11,9,18,36,54,6,12,24,48	2	1.041	10	--	09:59
	MOVISTAR_A5	5a:8e:85:55:1e:...	1	-45	-82		WPA/WPA2	1,2,5,11,18,24,36,54,6,9,12,48	2	1.041	10	--	09:59
	MOVISTAR_A	5a:8e:85:55:1e:...	1	-45	-82		WPA/WPA2	1,2,5,11,18,24,36,54,6,9,12,48	2	1.041	10	--	09:59
	Movistar_A5	f8:8e:85:55:1e:8a	1	-43	-87		WPA/WPA2	1,2,5,11,18,24,36,54,6,9,12,48	2	1.041	10	--	09:59
	Wi-Fi_ace	0:1f:f3:c2:f3:8e	10	-42	-82		WPA/WPA2	1,2,5,11,6,9,12,18,24,36,48,54	2	5.169	10	ES	09:59

Como otro ejemplo práctico, presentamos a continuación una imagen de la web: **https://www.xataka.com**. Esta tabla, nos muestra el resultado de una prueba de laboratorio que han realizado los responsables de esta Web, en la cual se aislaron diferentes teléfonos móviles y se los forzó para que emitieran en su máxima potencia. Los teléfonos móviles, tienen obligatoriamente instalado un módulo que se llama **SAR** (Specific Absorption Rate) que regula su potencia de emisión cuanto más cerca esté del cuerpo humano, es una función de protección (que algunas marcas orientales NO cumplen…). Si queréis profundizar en este tema, tenemos un **ciclo de 5G** que os puede resultar de mucho interés.

En la tabla que sigue podéis apreciar la potencia de emisión de cada móvil, tanto en Watts como en dBm, y el **PIRE** (Potencia Isotrópica Radiada Equivalente) que es la potencia irradiada en todas las direcciones.

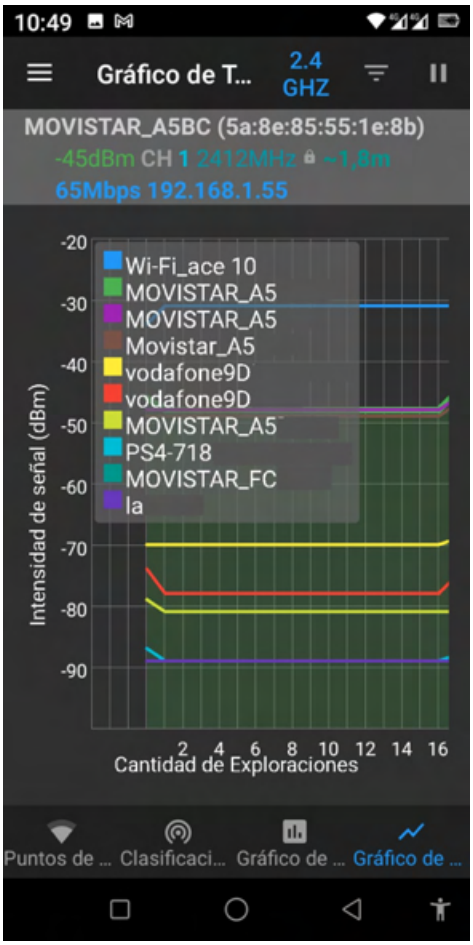
MENÚ xataka NUEVO

MEDIDAS TOMADAS CON LLAMADA ENTRANTE SIN DESCOLGAR	ZTE KIS II MAX (SMARTPHONE DE CONTROL)	APPLE IPHONE XS MAX	BQ AQUARIS C	HUAWEI MATE 20 PRO	LG G7 THINQ	MOTOROLA MOTO Z3	ONEPLUS 6T	OPPO R15 PRO	SAMSUNG GALAXY NOTE 9	SONY XPERIA XZ3	XIAOMI MI 8 (VERSIÓN EUROPEA)	XIAOMI MI 8 (VERSIÓN GLOBAL)
FRECUENCIA (MHz)	895,10	903,70	895	895,10	895,10	895,10	895,10	895	903,60	891,14	895,10	891,10
MEDIDA DIRECTA ANALIZADOR (dBm)	-30,42	-35,91	-37,05	-35,17	-33,45	-30,98	-30,54	-40,05	-35,40	-47,68	-37,11	-34,43
PIRE EMITIDA POR EL SMARTPHONE (dBm)	31,68	26,19	25,05	26,93	28,65	31,12	31,56	22,05	26,70	14,42	24,99	27,67
PIRE EMITIDA POR EL SMARTPHONE (W)	1,47	0,42	0,32	0,49	0,73	1,29	1,43	0,16	0,47	0,03	0,32	0,58

Un móvil tiene permitido emitir hasta 2 Watts, lo cual es para pensárselo, en aquellas personas que lo llevan permanentemente juntos a su oído.

La tabla anterior os puede ser de utilidad para calcular y verificar estas fórmulas logarítmicas. Si tenemos en cuenta la potencia de emisión (PIRE emitido) en dBm y la comparamos con la primera tabla de conversión entre potencias y dBm, veremos que este PIRE emitido, cuyos valores oscilan alrededor de los 30 dBm, se corresponden a potencias cercanas a los 1000 mW, es decir 1W. Y sin embargo la segunda fila (medida directa del analizador (dBm), nos da valores negativos, pues en esa distancia, la potencia se atenúa a valores que oscilan alrededor de los -30 dBm.

Finalmente, como un anticipo de la charla que sigue, se presenta a la derecha una aplicación para teléfonos móviles, que emplearemos bastante en el libro, en la cual podemos ver cómo se mide.



Si prestáis atención, la red que mejor señal nos envía es la que está arriba de todo “Wi-Fi_ace” cuya señal está llegando en unos -3 0 dBm, pues se trata de una maqueta que tenemos montada al lado de nuestro escritorio y que emplearemos en las charlas que siguen.

Luego le siguen las dos redes de MOVISTAR que son las WiFi que me ofrecen el servicio de Internet en mi domicilio, y a medida que bajamos en la imagen, siguen apareciendo otras redes que hemos ocultado parte de sus nombres, pues pertenecen a nuestros vecinos.

En esta charla “aburridísima” hemos presentado una serie de conceptos de las frecuencias que emplean las diferentes tecnologías WiFi, y los conceptos clave de medición de su potencia. Todo esto con la intención que podamos calcular debidamente los despliegues inalámbricos que realicemos bajo nuestra responsabilidad, pues como acabamos de ver, hay varias medidas que nos pueden permitir asegurar debidamente este tipo e conexiones.

Volver al índice

www.darFe.es

Charla 33

WiFi - Mapa de calor

Enlace al Video:

Resumen:

Como su nombre lo indica, esta charla nos sirve para medir la temperatura de nuestras redes. Desarrollaremos una serie de medidas y herramientas que nos permitirán determinar, frecuencias, potencias, canales y solapamientos.

El conjunto de estas acciones, nos dará como resultado redes WiFi, mucho mejor gestionadas y optimizadas. Desde el punto de vista de la Ciberseguridad, conocer este tema es fundamental a la hora de saber qué tengo y qué me rodea.

Descripción detallada

En este capítulo desarrollaremos como medir la “temperatura”, el calor de nuestras redes WiFi. El concepto de mapa de calor, nos servirá para aprender a determinar hasta dónde están irradiando nuestras rede WiFi, donde se solapan o no, y poder tomar las medidas adecuadas para optimizarlas y a su vez para ajustar sus potencias a los rangos de cobertura que deseemos, con lo que estaremos mejorando el nivel de seguridad de las mismas.

Para comenzar a trabajar de forma práctica, en esta ocasión, emplearemos la herramienta “**Netspotapp**” que podéis descargar desde:

https://www.netspotapp.com

Esta aplicación, la podéis instalar en cualquier sistema operativos.

Una vez que la ejecutáis, comienza a detectar y medir las diferentes señales que va recibiendo y nos las muestra como podemos ver en la imagen que sigue.

SSID	BSSID	Canal	Banda	Seguridad	Vendedor	Modo	Nivel...	Señal	Señal...	Med	Máx	Mín	Ruido	Rui...	Último visto
WiFiace	00:1F:F3:C2:F3:8E	6	2.4GHz	WPA/WPA2 Pe...	Apple	b/g/n		-41	59%	-44	-41	-48	-	0%	now
Movistar_A5BC	F8:8E:85:55:1E:8A	5	2.4GHz	WPA/WPA2 Pe...	Comtrend	n		-37	63%	-42	-32	-45	-90	10%	now
MOVISTAR_A5BB	5A:8E:85:55:1E:88	5	2.4GHz	WPA/WPA2 Pe...	5A:8E:85	n		-38	62%	-43	-32	-48	-90	10%	now
MOVISTAR_A5BC	5A:8E:85:55:1E:8B	5	2.4GHz	WPA/WPA2 Pe...	5A:8E:85	n		-38	62%	-42	-32	-46	-90	10%	now
vodafone9DE0_EXT	3C:84:6A:3A:C6:C3	4	2.4GHz	WPA/WPA2 Pe...	TP-LINK	b/g/n		-71	29%	-75	-71	-87	-94	6%	now
MOVISTAR_PLUS_A5BB	98:97:D1:B7:F1:F6	104	5GHz	WPA2 Personal	MitraStar	ac		-82	18%	-80	-76	-83	-97	3%	now
MOVISTAR_A5BC	98:97:D1:B7:F1:EE	11	2.4GHz	WPA2 Personal	MitraStar	n		-77	23%	-80	-73	-86	-90	10%	now
vodafone9DE0	3C:98:72:43:9D:E5	100	5GHz	WPA2 Personal	Sercomm	ac		-84	16%	-84	-82	-89	-97	3%	now
vodafone9DE0	3C:98:72:43:9D:E1	1	2.4GHz	WPA2 Personal	Sercomm	n		-82	18%	-82	-69	-89	-94	6%	now
IQePHlvMgHOsQHv7LO5Tohm...	58:B5:68:10:3B:C8	13	2.4GHz	WPA2 Enterpri...	SECURITAS	b/g		-87	13%	-88	-86	-89	-94	6%	now
PS4-718FF8BC49A5	28:56:5A:F3:DC:4F	6	2.4GHz	WPA2 Personal	Hon	b/g/n		-85	15%	-87	-75	-88	-90	10%	now
Orange-5142	74:DA:88:91:32:97	36	5GHz	WPA/WPA2 Pe...	TP-LINK	ac		-92	8%	-92	-91	-94	-97	3%	now
Livebox6-E199	D4:86:60:E7:E1:98	1	2.4GHz	WPA2 Personal	Arcadyan	ax		-93	7%	-91	-86	-95	-94	6%	now
Orange-5142	74:DA:88:91:32:98	2,+1	2.4GHz	WPA/WPA2 Pe...	TP-LINK	b/g/n		-91	9%	-90	-84	-94	-90	10%	now
MIWIFI_2G_3zE9	7C:39:53:AC:CA:AC	6	2.4GHz	WPA/WPA2 Pe...	zte	b/g/n		-95	5%	-95	-95	-95	-94	6%	now
TP-Link_0F0E	B4:B0:24:01:0F:0E	10	2.4GHz	WPA/WPA2 Pe...	TP-Link	b/g/n		-94	6%	-91	-90	-94	-90	10%	now
ACCTUA	C0:06:C3:47:5A:81	8	2.4GHz	WPA/WPA2 Pe...	TP-Link	b/g/n		-95	5%	-94	-93	-95	-90	10%	now
Hachazuelas12	C0:C9:E3:F7:E8:8E	12	2.4GHz	WPA2 Personal	TP-LINK	ax		-96	4%	-94	-92	-96	-90	10%	now

En esta práctica, iremos viendo varias redes WiFi, pero en particular, trabajaremos con una maqueta que hemos desarrollado sobre un Time Capsule (imagen de la derecha), que es un servidor de ficheros de Macintosh, el que a su vez ofrece la función de punto de acceso WiFi, como se encuentra a medio metro de distancia, podemos verlo en la primera fila de la imagen de arriba, en color **naranja** y lo hemos llamado “**WiFiace**”.

Luego de esta primera línea, podemos ver en segundo lugar la red “**Movistar_A5BC**” que es un punto de acceso repetidor de la marca **Comtrend**, que también se encuentra muy cercano al lugar desde donde estamos ejecutando Netspotapp. La tercer línea es el router de fibra óptica de Telefónica que nos da acceso a Internet y su red es “**MOVISTAR_A5BC**”.

Si prestamos atención a la imagen inicial de Netspotapp, en la octava columna, podemos ver la potencia de las señales que estamos recibiendo, medidas en **dBm**. Tal cual desarrollamos en el capítulo anterior, los valores negativos que mejor se posicionan, están en el orden de los -40 bBm, que se corresponderían a unos 0,0001

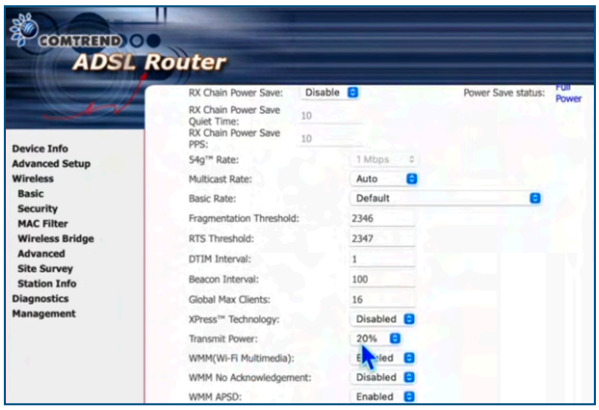
mW, El resto de las señales están por debajo de los -70 dBm, lo que las sitúa como muy mala señal, en las barras de esta columna, están en color naranja o rojo.

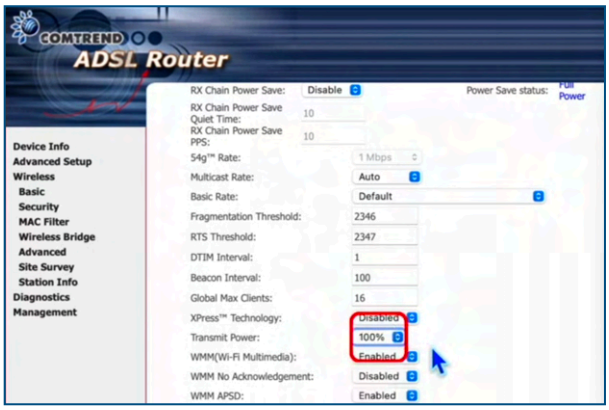
Otro detalle que deseamos remarcar de la misma imagen es la tercer columna, en la que vemos que las tres primeras redes WiFi, operan en los canales 5 y 6.

Para ir viendo de forma práctica el mapa de calor, vamos a modificar el canal de nuestro WiFi de maqueta "**WiFiace**" y lo configuraremos en el canal 3. En la imagen que sigue podemos ver cómo poco a poco van a bajar los dBm en Netspotapp, pues en ese canal, recibirá mayor interferencia, en estos momentos se encuentra a-48 dBm.

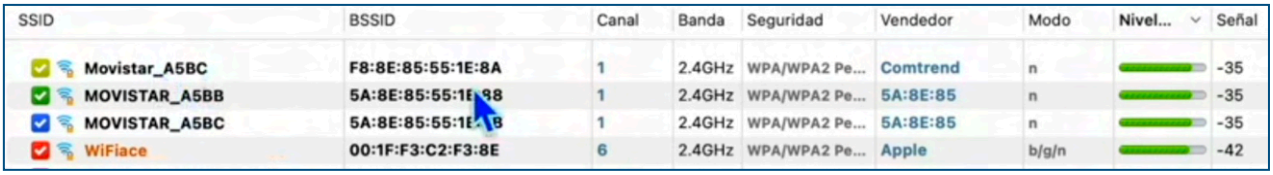
Para seguir experimentando, vamos a modificar los canales y la potencia de los puntos de acceso.

A continuación podemos ver el punto de acceso Comtrend, que se corresponde a la WiFi: "**Movistar_A5BC**", en el cual configuraremos el canal 1 y la potencia, que como podemos ver en la imagen de abajo a la izquierda, estaba en **20%**, la cambiaremos para que irradie al **100%** (imagen de abajo a la derecha).

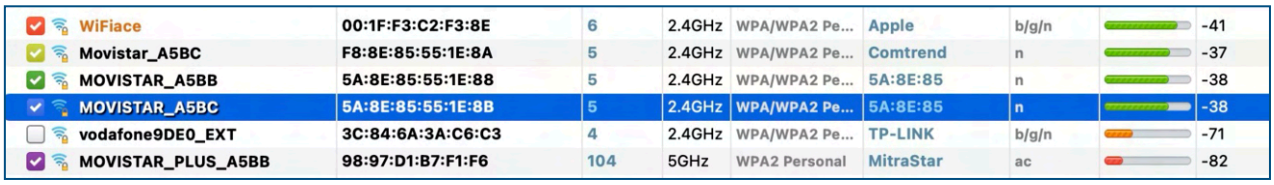




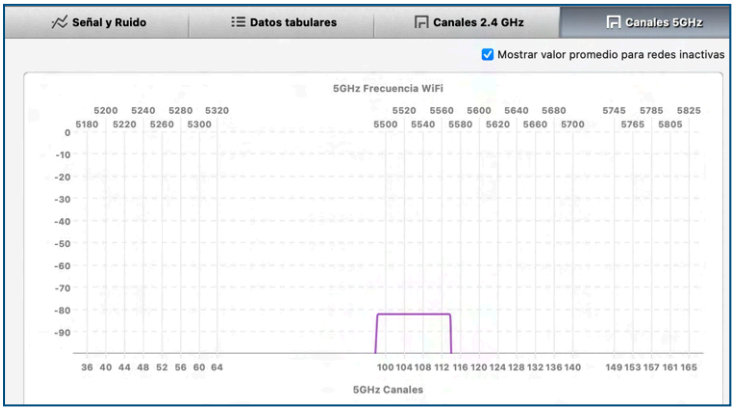
El resultado de haber separado los canales y aumentar su potencia, como podemos ver en la imagen de la medición que sigue abajo, es que se ha posicionado en primer lugar y llega con una potencia de -35 dBm. Los otros dos "MOVISTAR" que le siguen, lo han igualado, porque son repetidores.



Volvamos abajo, a parte de nuestra imagen inicial para seguir avanzando con las funcionalidades de Netspotapp.



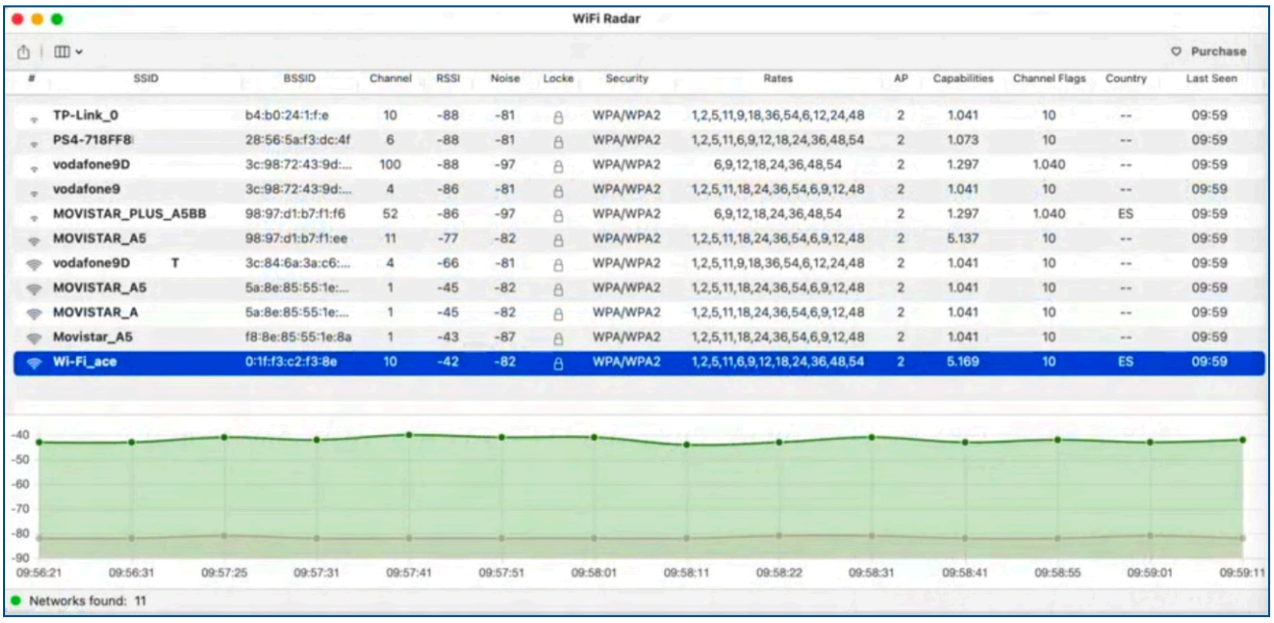
Netspotapp, nos presenta también las gráficas de empleo y potencia de cada uno de los canales de las WiFi que detecta. A la derecha vemos que los canales 5 y 6 se están solapando en la frecuencia de 2,4GHz, que se corresponden a las cuatro primeras líneas de la imagen de arriba.



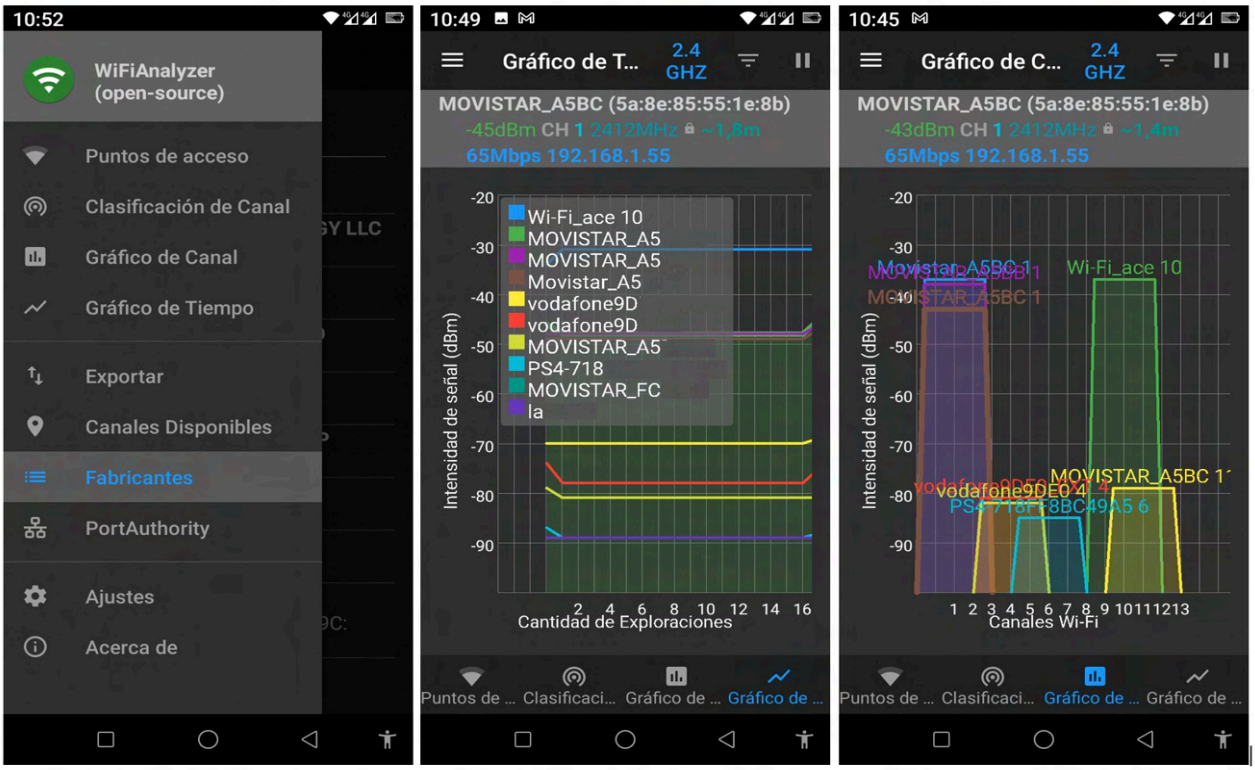
Sin embargo, si miramos la gráfica que se corresponde a la frecuencias de 5GHz (a la izquierda), podemos ver que no hay solapamientos.

Esta frecuencia se corresponde al canal 104, se trata del punto de acceso "MOVISTAR_PLUS_A5BB" y es el mismo punto de acceso de Telefónica que ofrece operar en ambas frecuencias. La señal llega muy débil, si la comparamos con la WiFi "MOVISTAR_ A5BC" justamente por la menor penetración que tiene esta frecuencia (5GHz), aunque ambas emisiones surgen exactamente del mismo dispositivo (router de Telefónica).

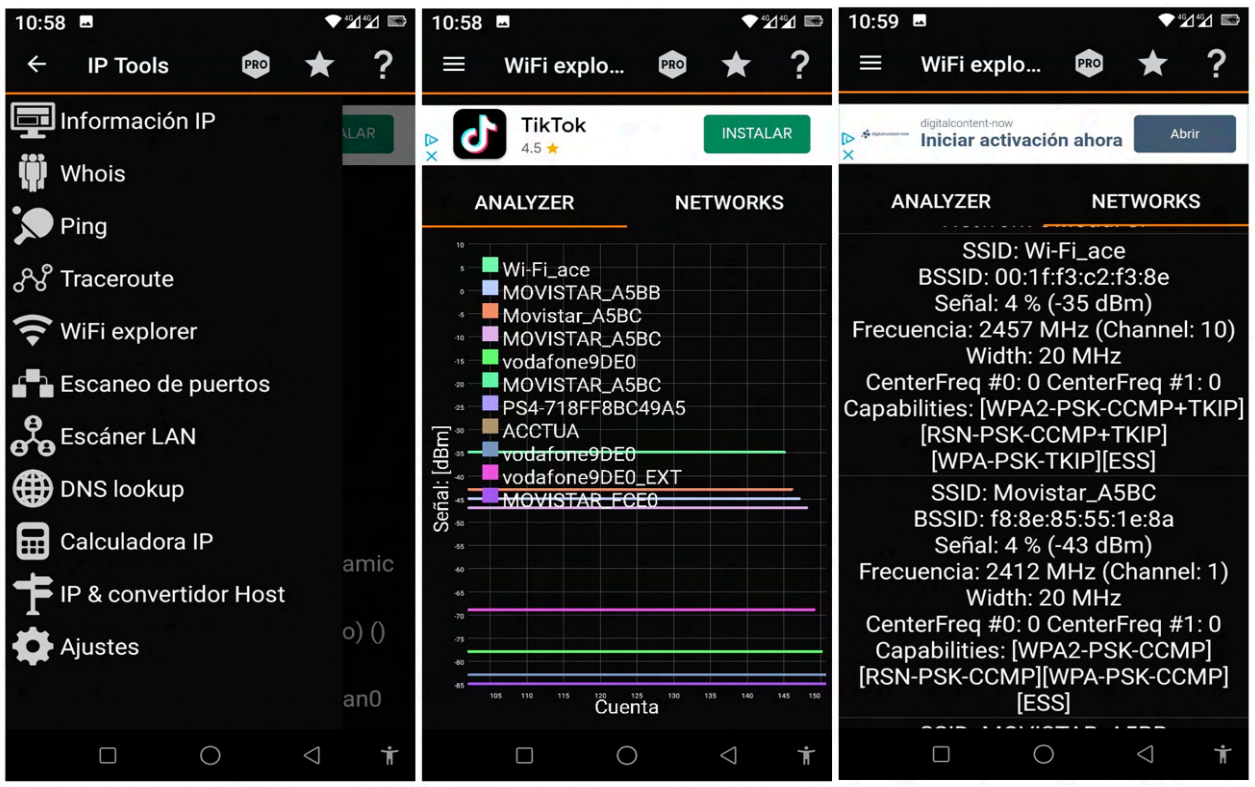
En cuanto al trabajo de mapa de calor, tened en cuenta también, la otra herramienta que hemos presentado en el capítulo anterior "**WiFI Radar**" que nos puede ser de mucha ayuda y repetimos abajo la imagen que presentamos en dicho capítulo.



Si trabajas más con teléfonos móviles, también tenemos varias herramientas que nos pueden ser de utilidad. La primera que deseamos presentar, es "**WiFi Analyzer**", cuyas mediciones presentamos aquí abajo. Como se puede ver, en el gráfico del medio, presenta las diferentes redes WiFi, cada una de ellas con su potencias de emisión, y a la derecha, hemos puesto también, como nos representa el empleo de los diferentes canales, en este caso de la banda de 2,4 GHz.



La última herramienta que presentamos, también para teléfonos móviles es "**IP Tools**".



Esta última herramienta, es muy útil, pues no solo posee la capacidad de explorar redes WiFi, sino que también, como podemos ver dentro de la imagen de arriba, la que está más a la izquierda, nos permite realizar, escaneaos de puertos, traceroute, whois, ping, etcétera, que siempre es bueno tener a mano.

Este capítulo, es un resumen de lo que contiene el video de esta charla, en el cuál se realizan más prácticas con estas herramientas, que pueden seros útiles, y creemos que lo mejor es que veáis el mismo para ampliar el detalle y profundizar más en la parte práctica.

www.darFe.es

Charla 34

WiFi empleando “Wireshark”

Enlace al Video:

Resumen:

En esta charla comenzamos a emplear nuestra herramienta **Wireshark**, pero para capturar tráfico en la interfaz aire, que como iremos desarrollando, tiene sus particularidades.

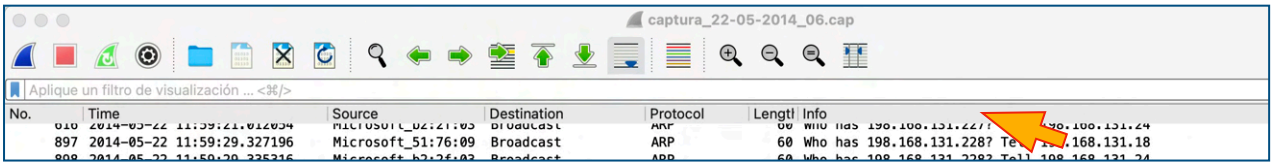
El empleo de Wireshark como herramienta WiFi, veremos más adelante que nos facilita mucho el trabajo de análisis de estas redes, como así también las primeras etapas para el cracking de contraseñas WiFi.

Descripción detallada

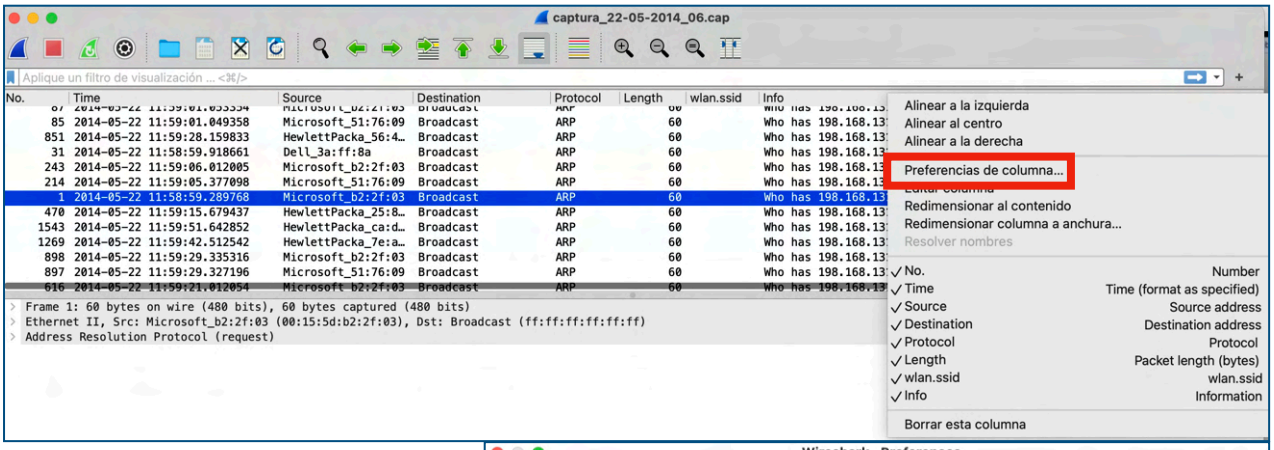
En esta charla de hoy, comenzamos a desarrollar el empleo de "**Wireshark**" sobre las redes WiFi, pues tiene ciertas características especiales que lo diferencian del empleo en redes cableadas.

Sobre "Análisis de tráfico" empleando justamente esta herramienta, tenemos un ciclo de cinco videos que es bastante completo y detallado, así que sería una muy buena opción, que antes de avanzar desde el enfoque WiFi, le deis una mirada a este ciclo.

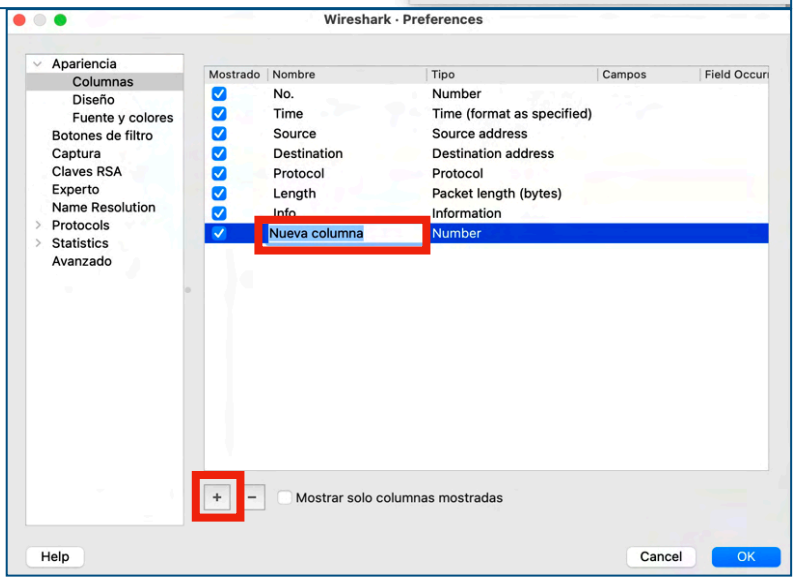
En primer lugar, vamos a configurar Wireshark para que nos muestre los nombres de las redes WiFi que se denominan **SSID** (Service Set Identifier), para ello, nos vamos a cualquier posición de la barra de nombres de las columnas (de color gris), tal cual se indica con la flecha color **naranja**, y presionamos el botón derecho del mouse.



Una vez que presionamos este botón derecho, se desplegará la ventana que sigue, en la que podemos ver varias opciones, de todas ellas, seleccionamos "**Preferencias de columna**", tal cual hemos remarcado en **rojo**.



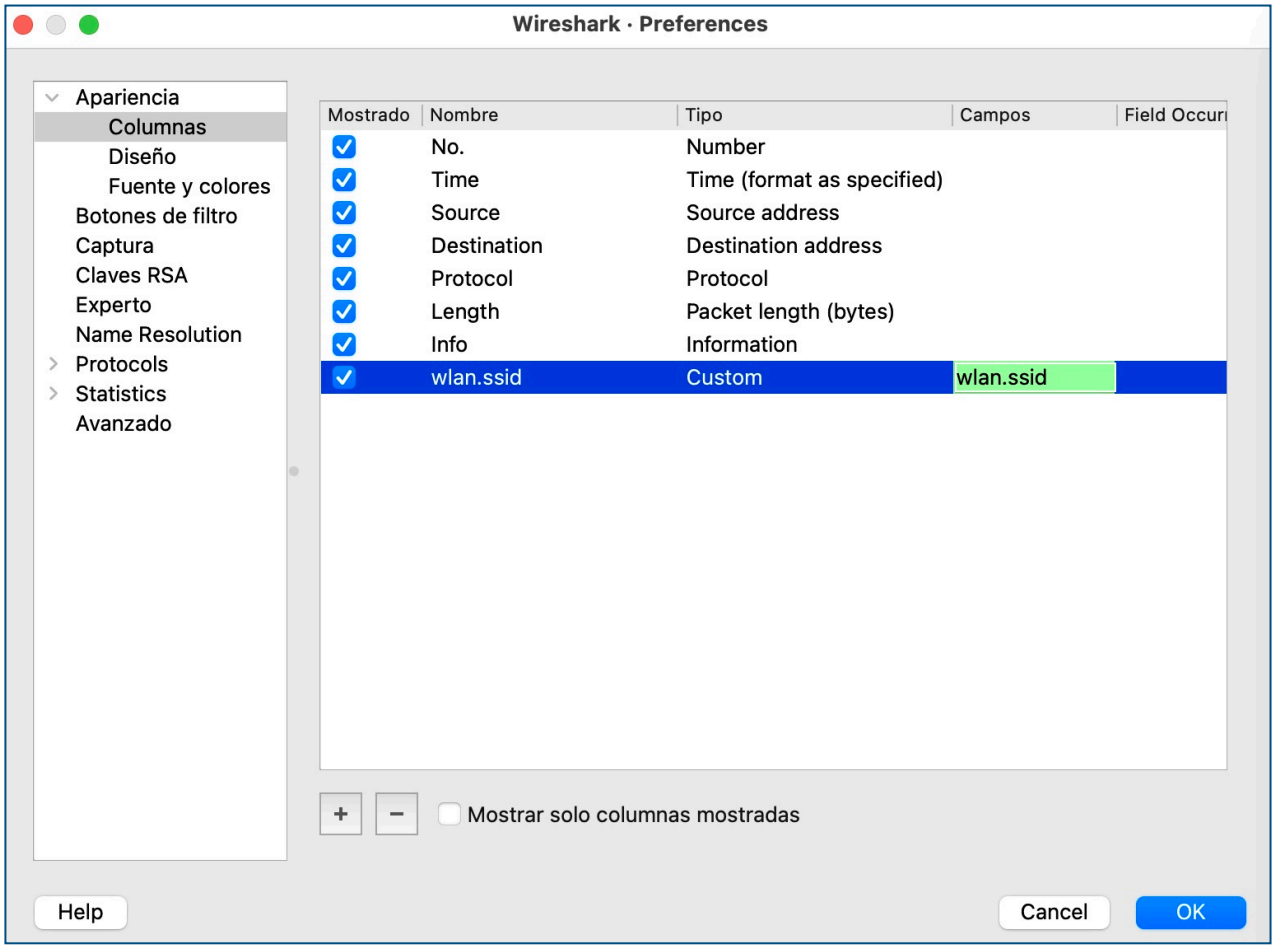
Presionamos en el botón "**+**" que figura recuadrado en **rojo**, para crear una nueva columna, como se muestra en la imagen de la derecha.



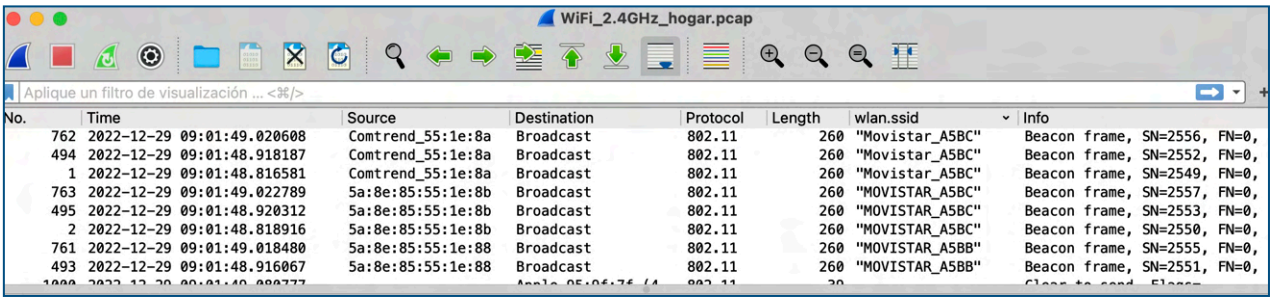
Ahora, sobre esta nueva columna que acabamos de crear, le indicamos qué es lo que deseamos que nos muestre. Para ello, reemplazamos el término que nos muestra por defecto (Nueva columna) por el nombre que le vamos a poner, que será

el que luego nos muestre en la ventana principal de Wireshark. Para nuestro ejemplo, lo llamaremos "**wlan.ssid**", el segundo campo que configuraremos es el que por defecto llama Nombre, y en este caso, es importante que despleguemos este campo y busquemos el Tipo "**Custom**", pues esto es justamente lo que queremos: "personalizarlo". Y por último debemos indicarle cuál será el parámetro o "Campo" que debe presentarnos Wireshark, que en nuestro caso también se trata del campo "**wlan.ssid**".

La configuración de esta nueva columna, es la que se presenta en la imagen de abajo y está resaltada en **azul**.



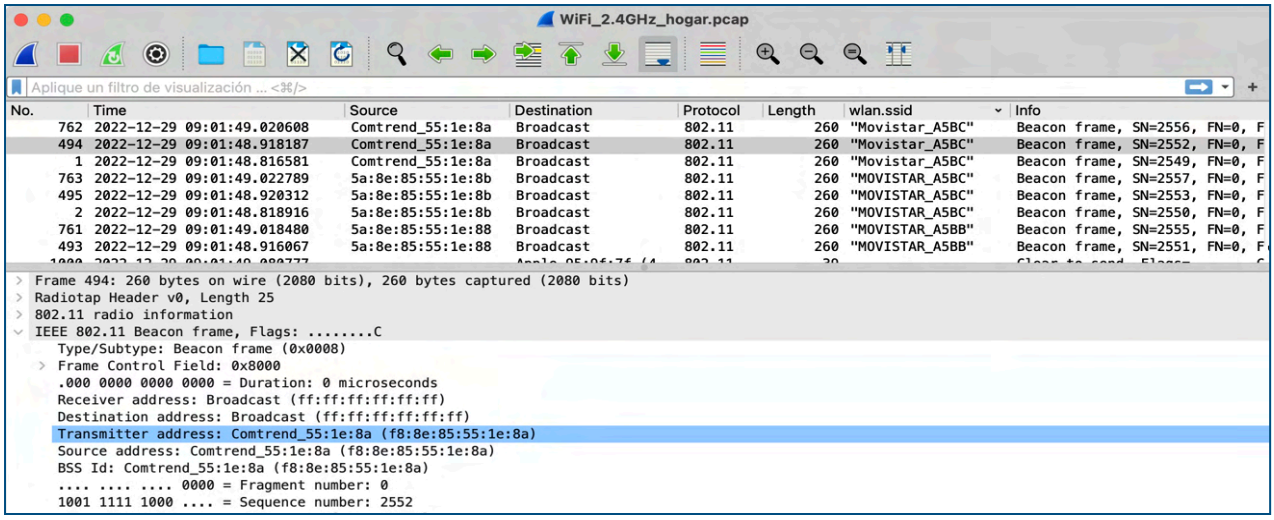
Una vez incorporada esta nueva columna, en la ventana principal de Wireshark, nos aparecerán los nombres de las redes WiFi, denominados "wlan.ssid", tal cual se presentan en la imagen de abajo.



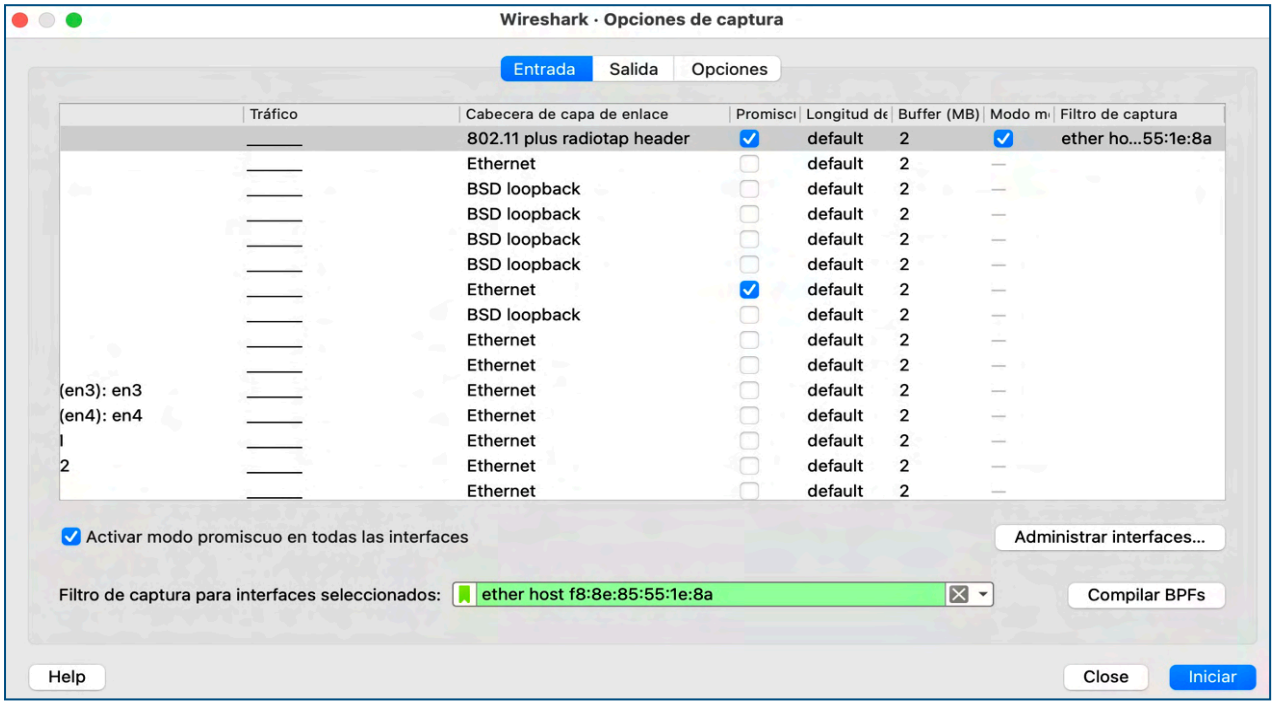
El objetivo de ir avanzando con Wireshark sobre las capturas de redes WiFi, es que poco a poco, seamos capaces de poder profundizar sobre los diferentes puntos de

acceso. En nuestro caso, por ejemplo, estamos viendo los dos puntos de acceso WiFi "Movistar_A5BC", uno con minúsculas la palabra Movistar y el otro con mayúsculas.

Supongamos que queremos centrar nuestra atención en uno de ellos: "Movistar_A5BC". En la imagen que sigue, podemos ver que, en la ventana central de Wireshark, hemos desplegado el protocolo **IEEE 802.11**, que en este caso se trata de una trama "**Beacon**" (baliza). Si prestamos atención, hemos resaltado en azul claro el campo "**Transmitter Address**", el cual no es, ni más, ni menos, que nuestra conocida dirección MAC, en este caso la del punto de acceso WiFi que está transmitiendo, que es "Movistar_A5BC", se trata del router **Comtrend** que ya hemos visto en charlas anteriores, y como podemos ver esta dirección MAC es: **f8:8e:85:55:1e:8a**.



Si solo quisiéramos capturar el tráfico de este punto de acceso, configuraríamos la próxima captura de tráfico para que solo deje entrar a este punto en concreto y descarte todos los temas. Esto se hace por medio de los llamados "**filtros de captura**" de Wireshark, los cuales los encontraremos en el menú "**Options**" y una vez seleccionado el mismo, definimos que solo capture el "**ether host f8:8e:85:55:1e:8a**", como podéis ver en verde en la imagen que sigue.



Una vez configurado este filtro de captura, en el video correspondiente a este capítulo, se realizan una serie de ejercicios y explicaciones, que por ser muy dinámicos, es difícil de desarrollar en texto, así que os aconsejamos que le deis una mirada al video de la charla 34 para que veáis de forma práctica esto que hemos explicado.

www.darFe.es

Charla 35

Kali

Enlace al Video:

Resumen:

En esta charla, hacemos un alto en el camino para dedicarnos a la instalación de una máquina virtual con el sistema operativo "**Kali**" Linux.

Creemos que es una herramienta fundamental e infaltable para cualquiera que se dedique a Ciberseguridad.

Descripción detallada

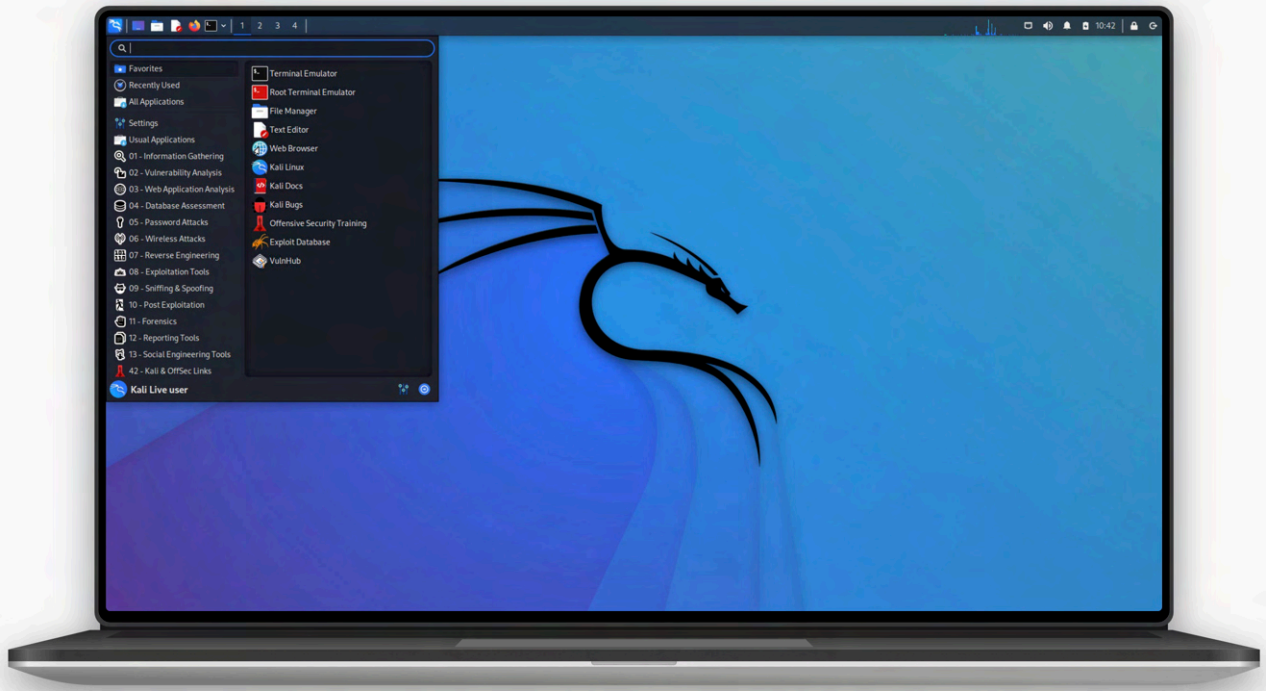
“No estamos lokos”, que sabemos lo que queremos…

Esta charla puede pareceros fuera de contexto, pensaréis:

> “*Pero, tan bien que veníamos con las redes WiFi y ahora nos cambian el rumbo*”

En esta charla, no es que se nos fue la pinza, hacemos sencillamente un “break”, y luego, seguiremos en el nivel de enlace y seguiremos con WiFi.

Pero en esta charla de hoy, nos centraremos en la instalación de **“Kali”**.



Como veremos, es una herramienta fundamental que necesitamos presentar ya mismo para poder seguir avanzando paso a paso en Ciberseguridad.

Kali, se trata de un sistema operativo completo, basado en la distribución “**Debian**” de **Linux**, y nadie que se vaya a dedicar a Ciberseguridad puede desconocer Linux. Es más, según nuestra opinión, es casi, casi, casi, casi IMPRESCINDIBLE saber sacarle el jugo a Linux o Unix, si quieres ser un experto en Ciberseguridad. Debemos reconocer que somos bastante fanáticos de este tipo de sistemas operativos, frente a otros Micro sistemas operativos, pero de verdad, en toda nuestra trayectoria, jamás nos hemos cruzado con un especialista y/o experto en temas de ciberseguridad que sea ajeno al mismo.

Cuando hablamos de sistemas operativos Linux, existen muchas distribuciones (sabores) de los mismos, algunos de ellos son:

- **Debian** (https://www.debian.orgl)

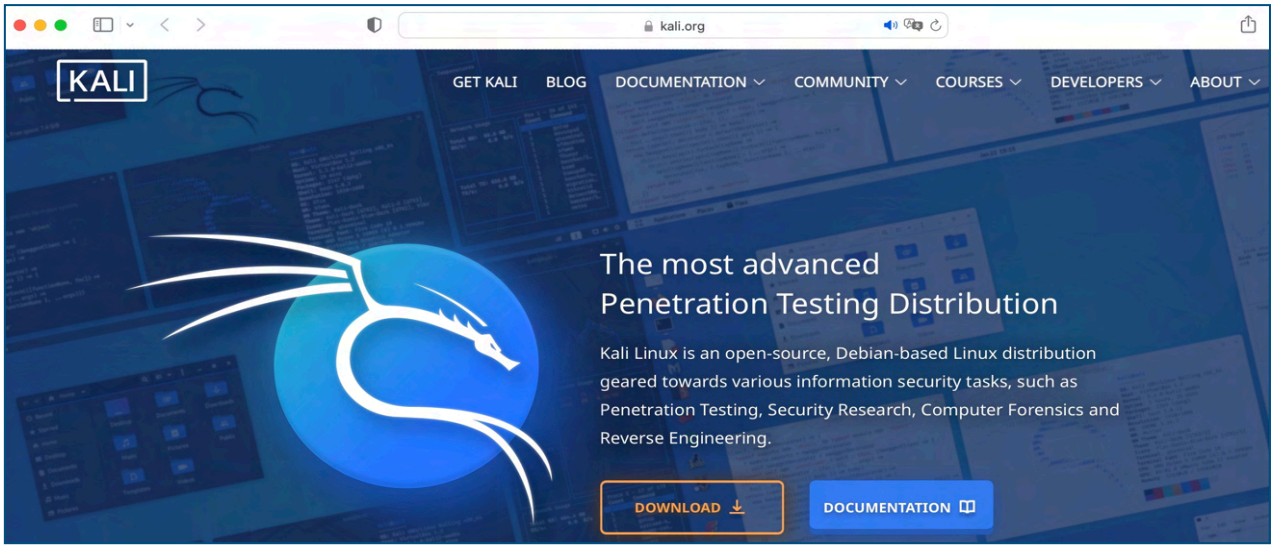
- **Red Hat** (https://www.redhat.com)
- **SUSE** (https://www.suse.com)
- CentOS (https://www.centos.org/)
- Ubuntu (https://ubuntu.com/)

Las anteriores son solo algunos ejemplos, pero existen cientos de distribuciones más.

Dentro de todas estas distribuciones, "**Kali**" es una distribución basada en "**Debian**" pero que a su vez, a lo largo del tiempo fue incorporando cientos de herramientas de ciberseguridad que ya están embebidas en Kali, con lo que al instalarla contamos con una batería importantísima de comandos, funciones, aplicaciones y herramientas específicamente orientadas a tareas de ciberseguridad.

La página oficial de Kali es: **https://www.kali.org/**

Una vez que os conectáis a su Web, la página inicial es esta.



Como podéis ver en la imagen anterior, tenéis un botón (recuadrado en **naranja**) desde donde se pueden descargar sus diferentes versiones.

En el caso nuestro, ya hemos impartido algunas charlas sobre la instalación de Kali, las mismas son:

- **Instalación de "Kali" en VirtualBox**
  (desde un fichero ISO)

- **Instalación de "Kali" en VirtualBox** (desde una imagen OVA)

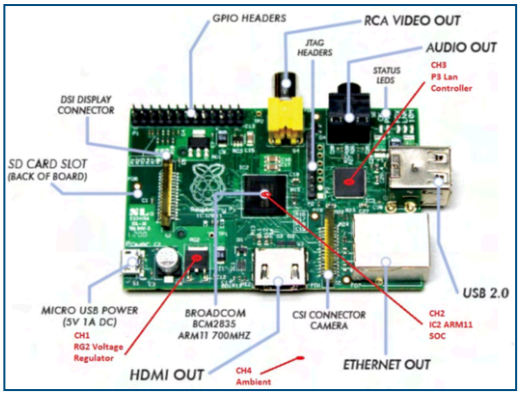
- **Seguridad informática empleando Rasberry Pi y Kali**

Los dos primeros videos, nos presentan la instalación de Kali en "**máquinas virtuales**". Una máquina virtual, es un ordenador que se ejecuta dentro de otro, empleando los recursos físicos de este, pero (si la configuramos bien) en un entorno totalmente aislado del primero, lo que nos permite poder ejecutar sistemas operativos totalmente dispares en un mismo ordenador.

Para la instalación de una máquina virtual, independientemente del ordenador físico que es imprescindible, al que llamaremos "**Anfitrión**", debemos instalar en el mismo una plataforma o gestora de máquinas virtuales, que será el software encargado de crear el entorno de virtualización. Los tres más conocidos y empleados son: **VirtualBox**, **VMWare** y **UTM**. Una vez que hemos instalado cualquiera de ellos, sobre el mismo, es donde se crean o instalan las máquinas virtuales que necesitemos.

Por supuesto que cada máquina virtual, en realidad estará consumiendo los recursos de hardware del anfitrión, así que siempre hay que tener en cuenta la capacidad del ordenador físico, pues el mismo, cuando arranquemos nuestra máquina virtual, estará ejecutando simultáneamente, el sistema operativo origen, las aplicaciones del anfitrión y también el sistema operativo y las aplicaciones de la máquina virtual.

El último video que presentamos arriba, emplea un entorno diferente, pues emplearemos un hardware "**Raspberry Pi**". Esta maravilla de la ciencia, se trata de un hardware de muy pocos euros y del tamaño de un paquete de cigarrillos, que nos ofrece una importante potencia informática. Lo emplearemos muchísimo en futuras charlas para hacer "A**uditorías remotas**"



Solo un agregado a estos conceptos.

Al nacer la informático, se desató una histórica batalla entre dos tecnologías de procesadores:

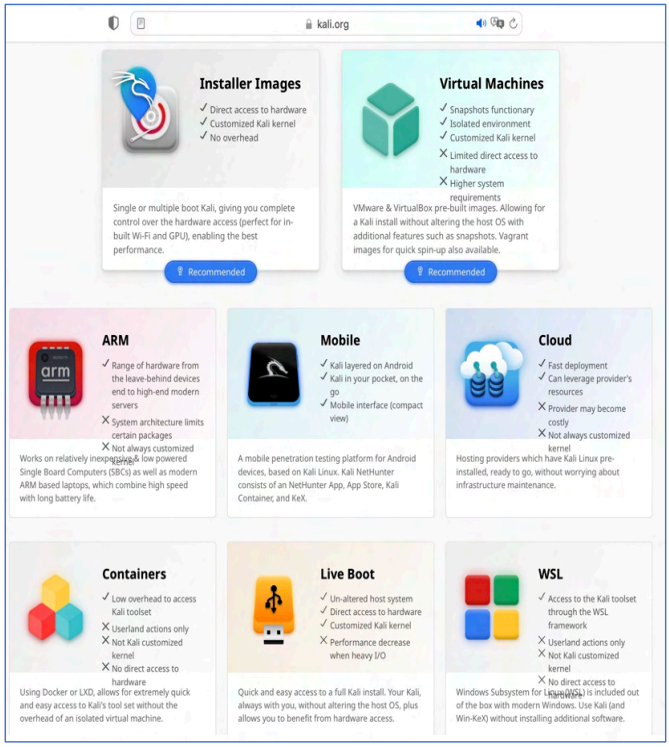
- **CISC**: Complex Instruction Set Computing
- **RISC**: Reduced Instruction Set Computing

Los primeros, son una tecnología, en la que el microprocesador trae incorporada un importante cúmulo de funciones y comandos, son los que dieron origen a los actuales Intel, AMD, etc.

Los segundos, en cambio, como su nombre lo indica, se minimizaba la cantidad de instrucciones para hacerlo ágiles y de bajo consumo eléctrico. Estos fueron ampliamente empleados en microprocesadores de ascensores, sensores, escaleras, y hoy en día son el corazón de todo teléfono móvil. También los procesadores RISC, dieron origen a los llamados **ARM** (Advanced RISC Machine). Esta arquitectura ARM; es la que emplea esta Raspberry, pero cuidado que no es algo trivial, los nuevos

ordenadores **Macintosh M1** y **M2** ya salen con procesadores ARM y os podemos asegurar que son una maravilla que superan bastante a los MAC anteriores con tecnología Intel.

En resumen, el último de los tres videos, no emplea máquinas virtuales, sino que se instala de forma nativa Kali, sobre una Raspberry Pi, que es ARM, e insistimos se pueden hacer verdaderas maravillas con las mismas. Como anticipo, desde la **charla 77** hasta la **87** las dedicaremos plenamente a desarrollar cómo hacer Auditorías Remotas, empleando Kali sobre Raspberry Pi, y os aseguramos que quedaréis totalmente sorprendidos.



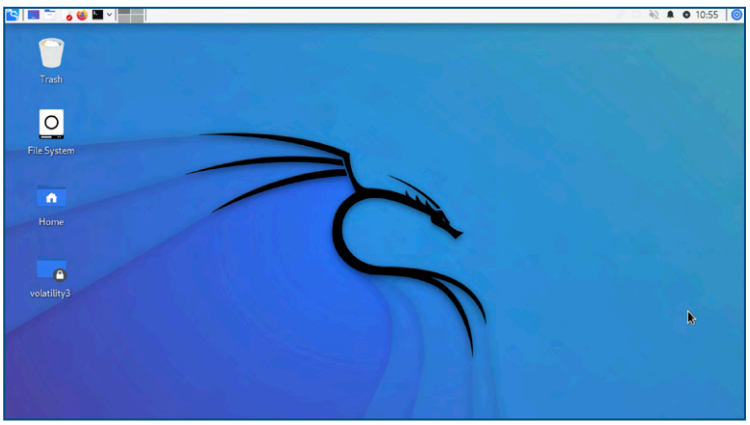
Volviendo a nuestra página de www.Kali.org, si presionamos el botón "**Download**", nos aparecerá la imagen de la derecha.

En la misma nos ofrece las diferentes opciones de instalación. Tenemos la imagen competa, que es la extensión "**.ISO**" de nuestro primer video de instalación. Al lado de la misma, tenemos la opción de "Virtual Machine", esta es la del segundo video, antes era extensión "**.OVA**", ahora la han cambiado y es "**.IMG**", pero la técnica de instalación es la misma que explicamos en el video.

En la segunda fila podemos ver "**ARM**" que es justamente la que acabamos de presentar para la Raspberry Pi. También es la que deberíamos usar en ordenadores MAC M1 y M2 con el software de virtualización "**UTM**".

Sobre el proceso de instalación, no seguiremos adelante en este texto, pues lo tenéis con todo detalle en los tres videos que hemos mencionado.

A continuación, solamente haremos una breve introducción a algunas funcionalidades de Kali, y seguiremos profundizando mucho más durante todo el libro.



Una vez que instalamos nuestra máquina virtual **Kali**, podemos **iniciar** la misma, y veremos una pantalla como la de la derecha. El tema del primer acceso, va cambiando en las diferentes versiones de Kali. Pero en general, nos suele presentar dos opciones.

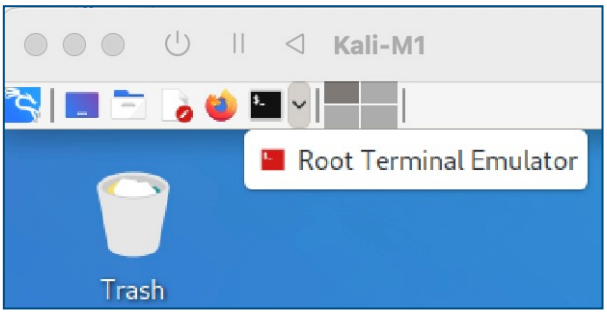
La primera de ellas es que por defecto ya traiga configurado el usuario "kali" y la contraseña "kali".

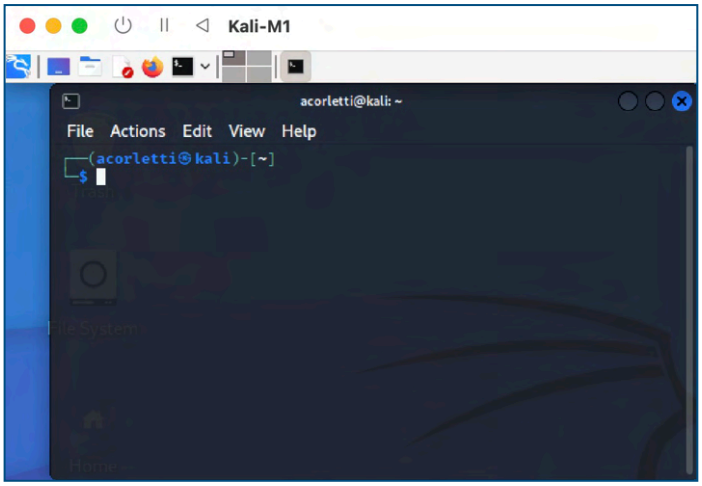
La segunda opción (que es la actual) es que durante la instalación nos pida la creación de un usuario y que ingresemos su contraseña. En este caso, por favor, NO la olvidéis, pues caso contrario no podrás acceder a Kali. En nuestro caso, hemos creado el usuario "acorletti" que será el que empleemos para acceder a Kali.

Una vez validado con un usuario personalizado, lo primero que deseamos presentar es la interfaz de comandos.

Como podemos ver en la imagen de abajo, si hacemos "click" en la pequeña ventana "negra", se despliega otra ventana muy similar pero en color rojo que nos indica que es "**Root Terminal Emulador**", dependiendo de cuál seleccionemos (negra o roja), ingresaremos como nuestro usuario (en nuestro caso "acorletti", si seleccionamos la negra), o seremos "root" si seleccionamos la roja, cosa que reiteramos, no es una buena práctica y deberías evitarlo.

NOTA: En los sistemas Linux, es una muy (*pero muy, muy, muy*) mala práctica, permitir el acceso como usuario "**root**", pues como veremos más adelante, se pierde toda trazabilidad y a su vez tiene los máximos privilegios, cosa que es muy peligrosa.

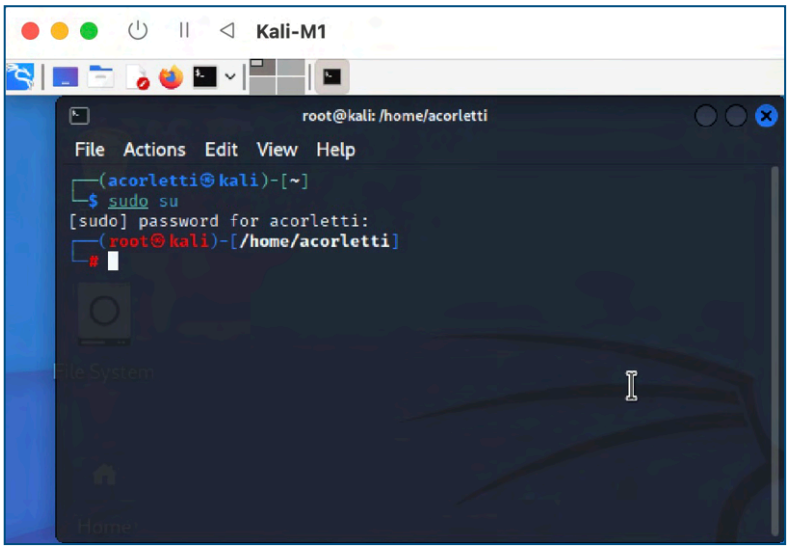




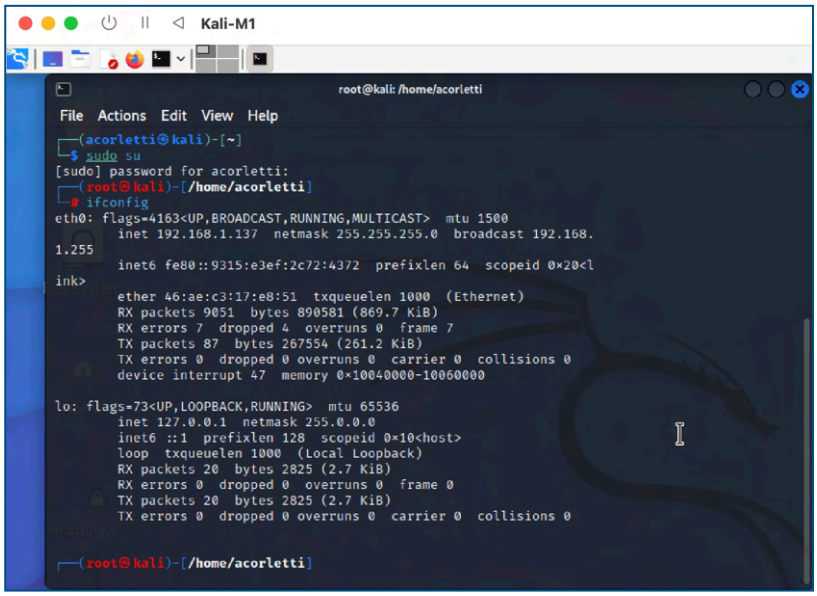
El proceder correcto, entonces, es seleccionar la ventana negra, ante lo cual, se desplegará una ventana como la que vemos a la izquierda.

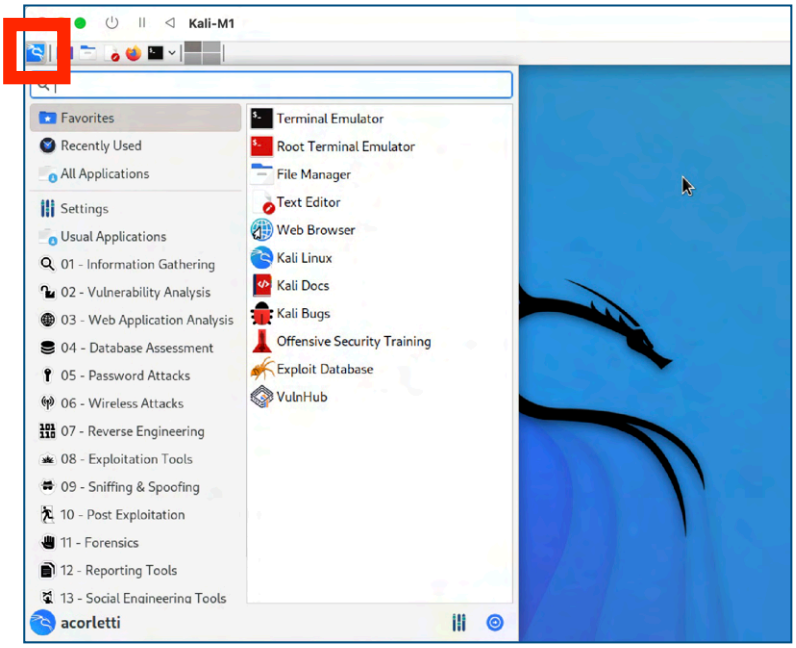
Qué detalle nos interesa prestar atención: el "**prompt**" es el signo dólar "**$**" y en color **azul**. Esto nos indica que somos un usuario "no privilegiado", cosa que reiteramos, es como deberíamos trabajar habitualmente.

En el caso que, por alguna razón, necesitáramos escalar privilegios, tenemos a nuestra disposición el comando "**sudo su**", que nos pedirá la contraseña de ese usuario (en nuestro caso la de acorletti), y nos presentará esta misma ventana, pero ahora, con el prompt "**#**" (almohadilla, o numeral), y en color **rojo**, que nos indica que hemos escalado a "**root**", como podremos apreciar en la ventana de la derecha.



Otro comando que es importante es el comando "**ifconfig**", que nos permite trabajar con las interfaces que posea nuestro Kali. En este caso, como podemos ver an la imagen de la derecha, nos presenta la interfaz **eth0** que tiene la dirección IP **192.168.1.137** y su respectiva dirección MAC. Y más abajo la interfaz "**lo**" que es el "local loop" o lazo local, esta interfaz está presente siempre en la pila TCP/IP y es la que le indica que procese cualquier petición como local.

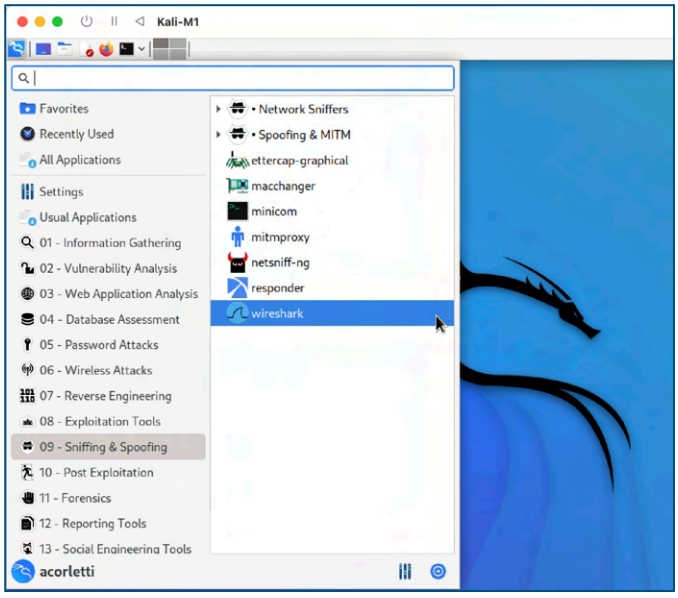




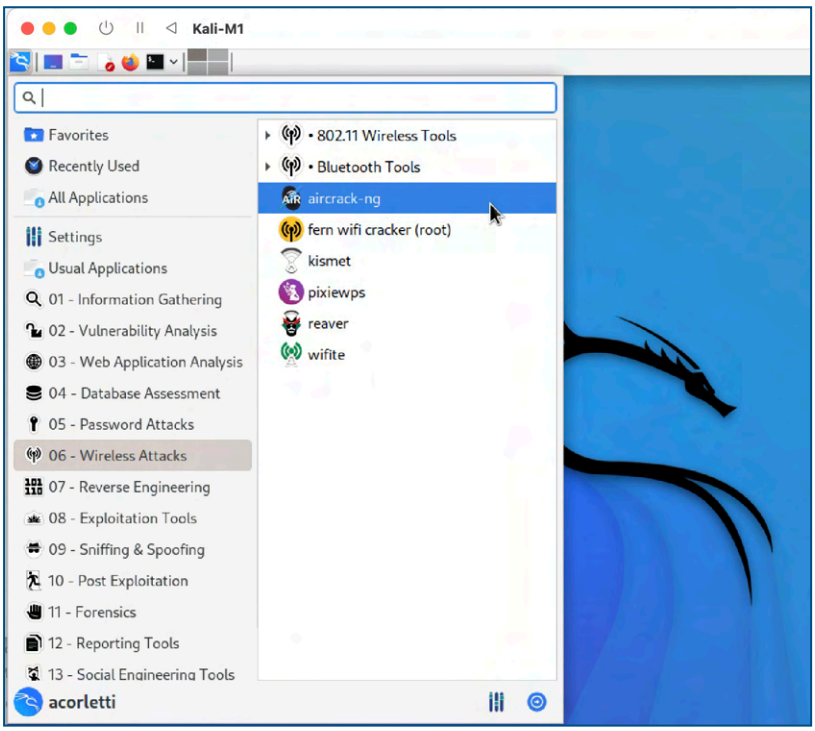
Si presionamos el botón que tiene el icono de Kali (recuadrado en **rojo** en la imagen de la izquierda), se nos desplegarán los grupos de todas las herramientas que tiene embebidas. Como podemos ver, los grupos están ordenados, 01, 02, etc.

Durante todo el desarrollo del libro, iremos empleando herramientas de Kali, que se encuentran en estos grupos o familias.

Fijaros, por ejemplo, que en el grupo 09 - Sniffing & Spoofing se encuentra nuestra herramienta **Wireshark**, sobre la que ya hemos trabajado varias veces. Podemos verlo en la imagen de la derecha.



Por último, en el grupo 06 - Wireless Atacks, hemos resaltado en **azul** la "**Suite aircrack-ng**" que será la que continuaremos empleando en las charlas siguientes.



Volver al índice

www.darFe.es

Charla 36

WiFi - WEP con “aircrack-ng”

Enlace al Video:

Resumen:

Esta charla, más que nada es didáctica, pues hoy en día, es poco probable que sigáis encontrando redes WiFi que empleen el protocolo **WEP**, pero lo importante de la misma, está en la metodología a seguir, para comprender bien y de forma técnica cómo es el empleo de la suite “**aircrack-ng**”, para que en las charlas siguientes, podamos seguir avanzando sobre una base base más robusta.

Descripción detallada

En esta capítulo, desarrollaremos algo que tal vez para muchos sea histórico, pues hoy en día es poco probable que lo encontréis, pero nunca se sabe, siempre hay gente que deja vulnerabilidades expuestas.

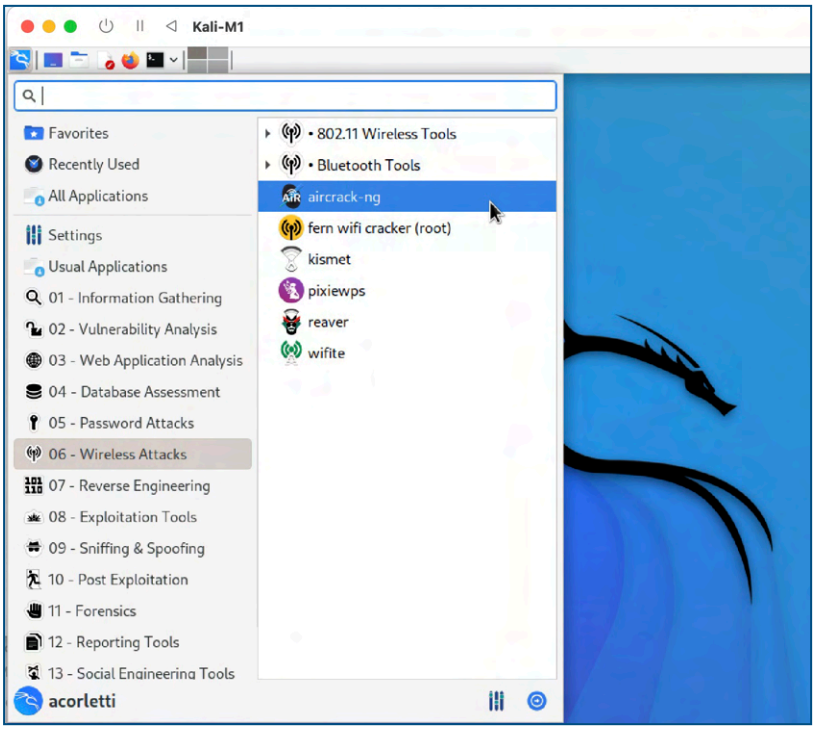
Más que nada nos interesa comprender el protocolo **WEP** (Wired Equivalent Protocol) por dos razones, la primera de ellas es debido a poder comprender la evolución de los algoritmos de autenticación y cifrado, y la segunda, es que nos permitirá familiarizarnos con la suite "**aircrack-ng**" que, como vimos en el capítulo anterior, es una de las herramientas que ya tiene preinstalada **Kali**.

En concreto, desarrollaremos de forma práctica cómo se "crackea" (rompe) una contraseña WEP, empleando esta herramienta.

Para acceder a aircrack-ng, desde nuestro Kali, desplegamos el menú de herramientas (icono de Kali) y desde allí nos vamos al punto 06 - Wireless Attacks y en él encontraremos la suite aricrack-ng, tal cual se muestra en la imagen de la derecha.

La página Web de esta herramienta es:

http://aircrack-ng.org



Dentro de la misma Web, tenéis también un tutorial muy claro en Español

https://www.aircrack-ng.org/doku.php?id=es:aircrack-ng

Para el tema más específico del protocolo WEP, tenéis también este otro "Tutorial: Simple crackeo de clave WEP"

https://www.aircrack-ng.org/doku.php?id=es:simple_wep_crack

Para la parte práctica, trabajaremos con la captura de tráfico "**ptw.cap**" que podéis descargar desde el menú "**Descargas**" —> "**Capturas de tráfico**" de nuestra Web: **https://darfe.es.**

La suite "**aircrack-ng**" está compuesta por tres programas:

- **airodump-ng**: sirve para capturar tráfico.

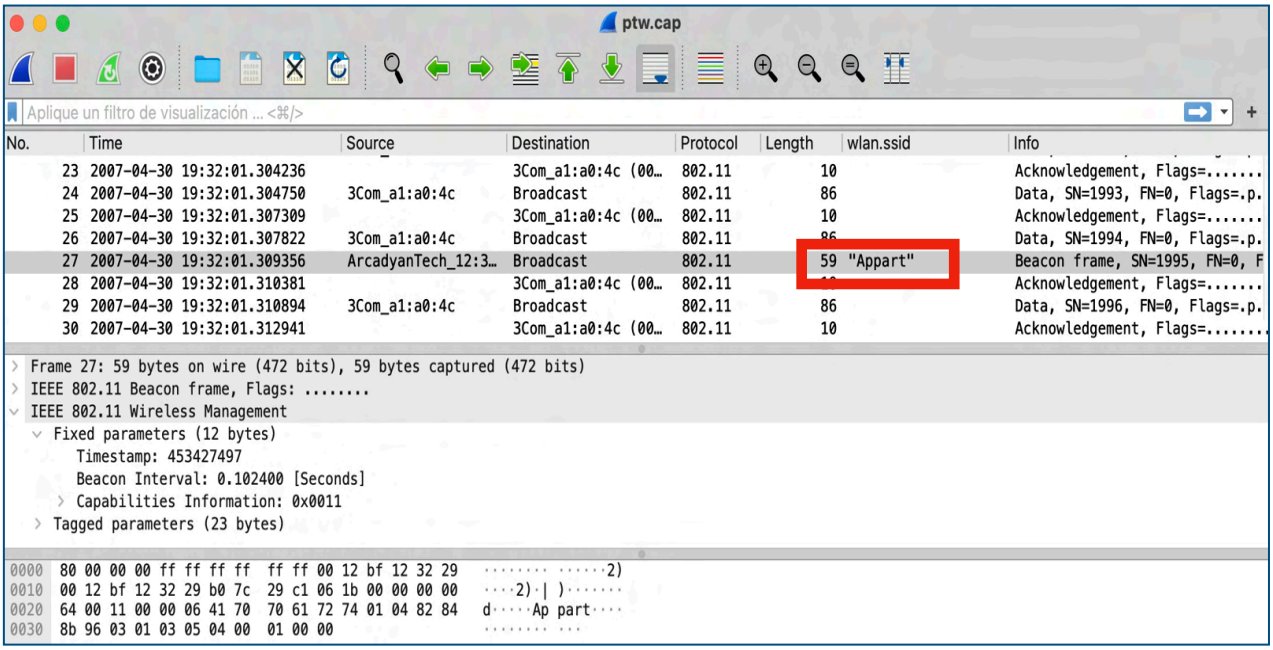
- **aireplay-ng**: sirve para generar tráfico
- **aircrack-ng**: sirve para el criptoanálisis de contraseñas

En nuestro caso, como ya hemos avanzado bastante en el empleo de **Wireshark,** la parte de capturas de tráfico, proponemos hacerla con "Wireshark" que nos ofrece exactamente las mismas capacidades que airodump-ng (y mucho más aún).

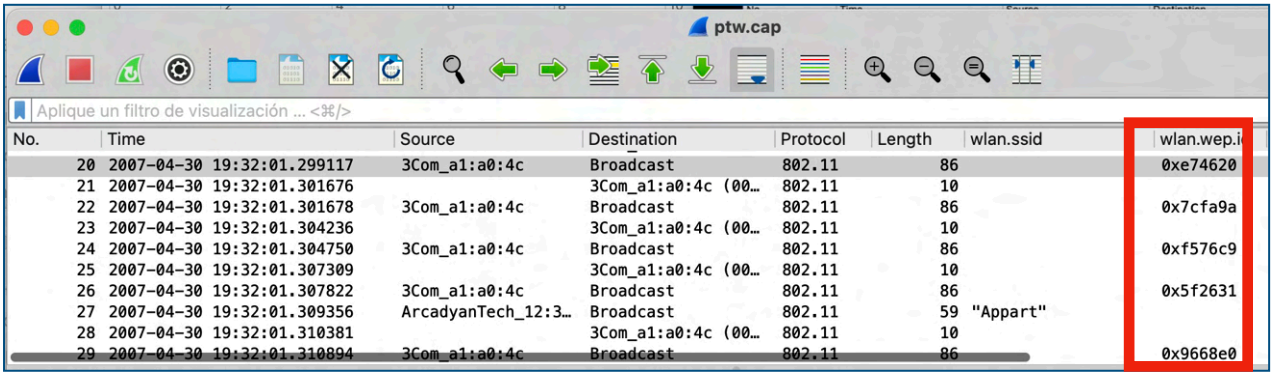
En el caso real de detectar una red WiFi que emplee WEP, lanzaríamos una captura de tráfico inicial, recordad que para redes WiFi, siempre colocarlo en modo "monitor". La idea es que hagamos una breve captura hasta que detectemos en nombre de la WiFi (**SSID**) que emplea WEP. Una vez que lo encontremos, tal cual hemos visto en el capítulo anterior, configuraremos un filtro de captura con el campo "**ether host MAC_del_SSID**" y lo dejaremos capturando hasta que obtenga un número considerable de tramas de este punto de acceso.

En nuestro caso, como trabajaremos con la captura **ptw.cap** que ya hemos descargado, obviaremos esta fase de captura de tráfico, y sencillamente abriremos ptw.cap con Wireshark.

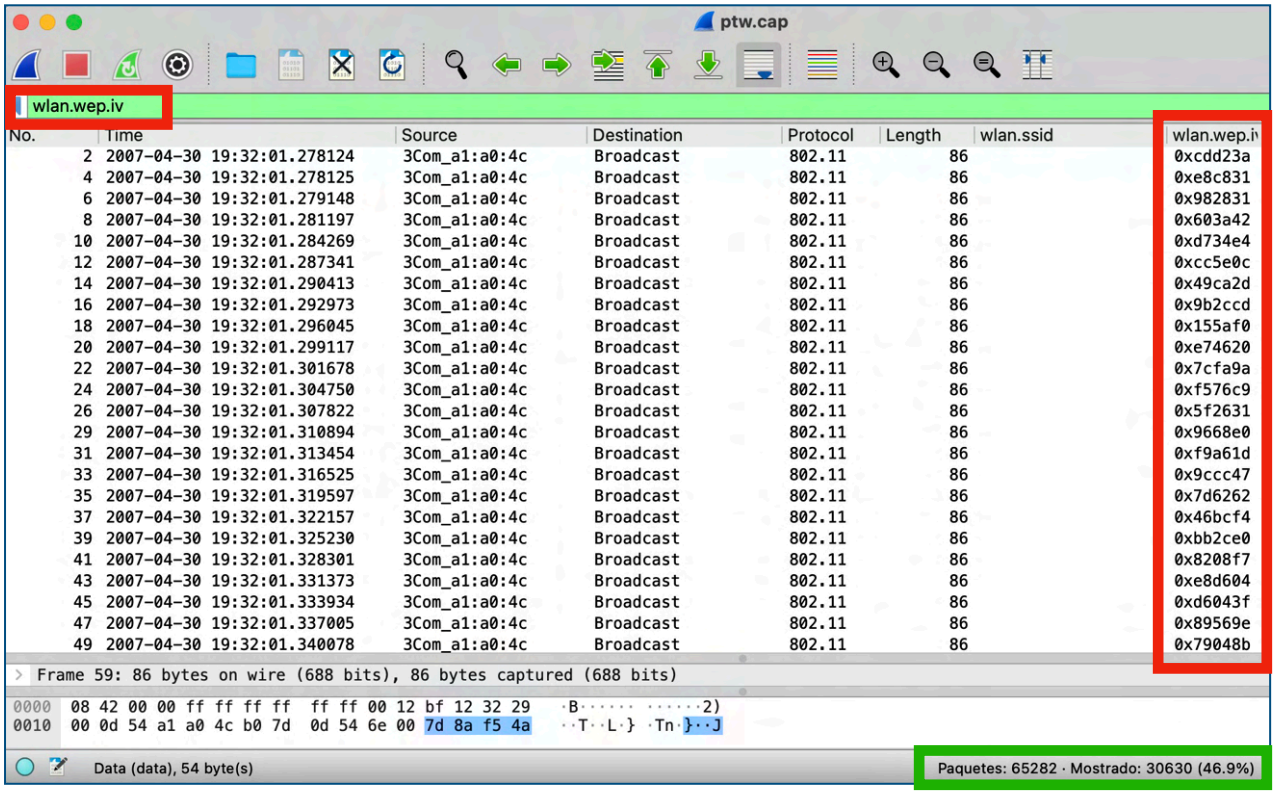
Lo primero que debemos prestar atención es que, en la trama 27, ya no aparece el nombre de este punto de acceso: "**appart**".



Lo segundo a tener en cuenta, es que, recordemos que el cifrado de WEP, se basaba en el "**vector de inicialización**". Para poder analizar este campo, una vez más configuraremos una nueva columna "Custom" en nuestro Wireshark. Recordad que lo hacemos, con el botón derecho del ratón en cualquier posición del menú gris que nos aparece con el nombre de las columnas, allí seleccionamos: "Preferencia de las columnas" y con el signo "**+**" de abajo, creamos una nueva tipo "Custom" y el "Campo" a buscar será "**wlan.wep.iv**", si lo deseáis como nombre, podéis poner también el mismo. Una vez creada esta columna, el valor que allí os aparecerá, es concretamente cada uno de los vectores de inicialización, como podéis verlo en la imagen siguiente.



Si solamente nos interesara visualizar las tramas que contienen vectores de inicialización, en Wireshark, en la ventana de "filtros de visualización" podemos escribir **wlan.wep.iv**, veremos que se ilumina de color verde y si presionamos **[Enter]**, solo nos presentará las tramas que contienen este valor, como podemos verlo en la imagen que sigue.



Otro aspecto de interés de la imagen anterior, es el que hemos remarcado en **verde** abajo, en el que podemos apreciar que, de un total de **65.282** tramas que contiene este captura, ahora nos está mostrando **30.630** (**46,9%**). Es decir, que este es el total de tramas que poseen el campo **wlan.wep.iv** (vector de inicialización).

Hasta aquí hemos podido averiguar que existe una WiFi cuyo SSID es "**appart**", que posee una dirección MAC que es: **00:12:bf:12:32:29**.

Con esta información pasaremos a emplear la segunda herramienta que posee la suite aircrack-ng. Esta herramienta es **aireplay-ng**.

Si solamente escribimos “aireplay-ng” en nuestra línea de comandos, nos presentará las opciones que posee, tal cual vemos a continuación

```
sh-3.2# aireplay-ng
Aireplay-ng 1.7  - (C) 2006-2022 Thomas d'Otreppe
https://www.aircrack-ng.org
usage: aireplay-ng <options> <replay interface>
Filter options:
      -b bssid  : MAC address, Access Point
      -d dmac   : MAC address, Destination
      -s smac   : MAC address, Source
      -m len    : minimum packet length
      -n len    : maximum packet length
      -u type   : frame control, type    field
      -v subt   : frame control, subtype field
      -t tods   : frame control, To      DS bit
      -f fromds : frame control, From    DS bit
      -w iswep  : frame control, WEP     bit
      -D        : disable AP detection

Attack modes (numbers can still be used):
      --deauth      count : deauthenticate 1 or all stations (-0)
      --fakeauth    delay : fake authentication with AP (-1)
      --interactive       : interactive frame selection (-2)
      --arpreplay         : standard ARP-request replay (-3)
      --chopchop          : decrypt/chopchop WEP packet (-4)
      --fragment          : generates valid keystream   (-5)
      --caffe-latte       : query a client for new IVs  (-6)
      --cfrag             : fragments against a client  (-7)
      --migmode           : attacks WPA migration mode  (-8)
      --test              : tests injection and quality (-9)
      --help              : Displays this usage screen
```

De estas opciones, nos interesa considerar las tres que hemos resaltado en negrita, es decir la dirección **MAC origen**, que será la nuestra, la del **Access Point**, y el **modo** de ataque, por lo tanto lanzaría el siguiente comando:

#aireplay-ng -3 -b 00:12:bf:12:32:29. -s 9c:3e:53:6d:09:37 en0

Le estamos diciendo con la opción **“-3”** que-ejecute **arpreplay** que es un “standard ARP-request replay”, esto lo hemos visto en nuestra charla 17, y sencillamente se trata de ejecutar solicitudes “ARP”, para forzar al punto de acceso a que genere muchos vectores de inicialización, los cuáles los estaríamos capturando con Wireshark o con airodump (el que prefiráis). La finalidad es obtener un alto volumen de estos vectores, pues se calcula que en el orden de unos 50.000 vectores de inicialización, son suficientes para que aircrack-ng pueda descifrar (crackear) la contraseña de acceso.

Si os atrevéis a hacer algo interesante, os invitamos a que empleéis la programación "**bash**", que es una de las mejores herramientas que posee todo sistema operativo Linux, y es un método de programación, muy sencillo que nos ofrece una potencia importantísima. Por ahora, no nos detendremos en desarrollar este lenguaje de programación, lo iremos desarrollando a lo largo del libro, pero si de verdad tenéis interés en el mismo, en todo Internet está plagado de tutoriales muy fáciles.

En el video, se presenta un ejemplo de cómo podemos aprovechar este lenguaje para poder generar la cantidad de "arprelay" que deseemos. Aquí abajo, os dejamos un ejemplo de como podéis generar este tipo de scripts.

```
#!/bin/bash
for i in 'seq 1 5000';
    do
        echo "ciclo nro: " $i
        aireplay-ng -3 -b 00:12:bf:12:32:29 -s 9c:3e:53:6d:09:37
en0
```

Una vez que hemos capturado suficientes vectores de inicialización, podemos pasar a la fase final de la suite, que es el comentar "**aircrack-ng**".

Una vez más, si lo ejecutamos sin ningún argumento nos mostrará todas las opciones.

```
sh-3.2# aircrack-ng

 Aircrack-ng 1.7  - (C) 2006-2022 Thomas d'Otreppe
 https://www.aircrack-ng.org
 usage: aircrack-ng [options] <input file(s)>
 Common options:
    -a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
        … (continúa)…
```

Como se puede ver en las opciones anteriores, la opción **"-a"** nos permite identificar si queremos crackear WEP o WPA, en la charla de hoy, nos centraremos en WEP. Como estamos sobre la captura "**ptw.cap**", lo ejecutaremos sobre esta misma. Para lo cual el comando a ejecutar será:

```
#aircrack-ng -a 1 ptw.cap
        Reading packets, please wait...
        Opening ptw.cap
        Read 65282 packets.
          #  BSSID              ESSID                     Encryption
          1  00:12:BF:12:32:29  Appart                    WEP (30566 IVs)
        Choosing first network as target.
        Reading packets, please wait...
        Opening ptw.cap
        Read 65282 packets.
```

1 potential targets

Attack will be restarted every 5000 captured ivs.

Aircrack-ng 1.7

[00:00:00] Tested 1514 keys (got 30566 IVs)

KB	depth	byte(vote)
0	0/ 9	1F(39680) 4E(38400) 14(37376) 9D(37376) 5C(37376) 00(37120) C3(37120) 36(36864) 3F(36864)
1	5/ 9	08(36864) A1(36608) A3(36608) 3E(36352) 34(36096) BA(36096) 46(36096) 20(35584) B5(35584)
2	0/ 1	1F(46592) 6E(38400) 81(37376) AD(36864) 79(36864) 38(36608) EC(36352) 42(36352) 2A(36352)
3	0/ 3	1F(40960) 15(38656) 7B(38400) BB(37888) 5C(37632) 4F(36608) 66(35840) 1B(35584) DE(35584)
4	0/ 7	1F(39168) 23(38144) 97(37120) 59(36608) 1E(36352) 3B(36352) AB(36352) 2E(36096) FD(36096)

KEY FOUND! [1F:1F:1F:1F:1F]

Decrypted correctly: 100%

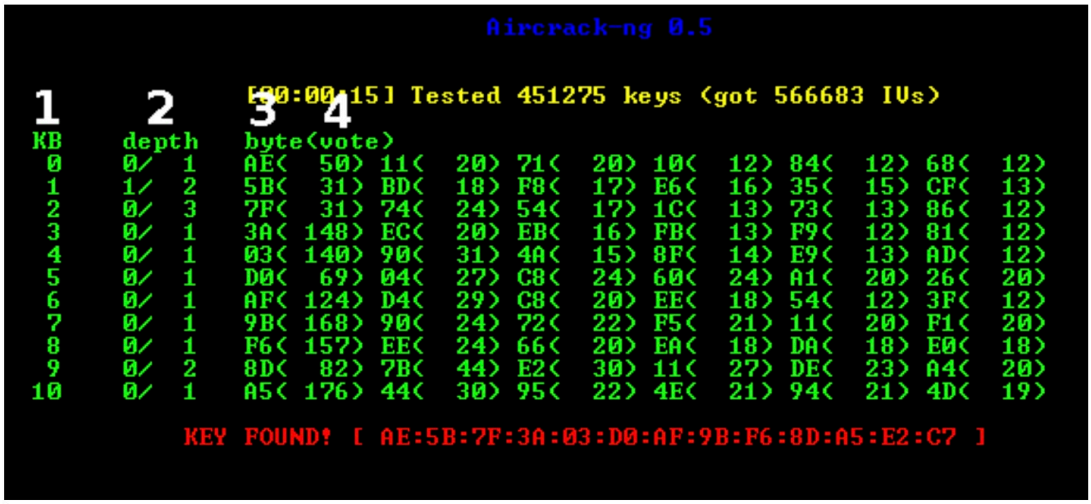
En las líneas de respuesta (presentadas arriba en color **gris**), henos remarcado en **negrita**, la información que nos interesa que tengáis en cuenta. Como podemos ver ha logrado desencriptar la clave de este red WiFi, y la misma es: "**1F:1F:1F:1F:1F**"

Si queréis profundizar sobre el contenido de la respuesta de aircrack-ng, nuevamente os recomendamos el documento citado al principio de esta charla:

https://www.aircrack-ng.org/doku.php?id=es:aircrack-ng

Donde, como podéis ver abajo, os explica cada una de estas columnas.

Captura de pantalla



LEYENDA

1 = Keybyte, es decir el número de cada uno de los bytes o caracteres de la clave.

2 = Profundidad de la actual búsqueda de la clave

3 = Byte o caracter que se está probando

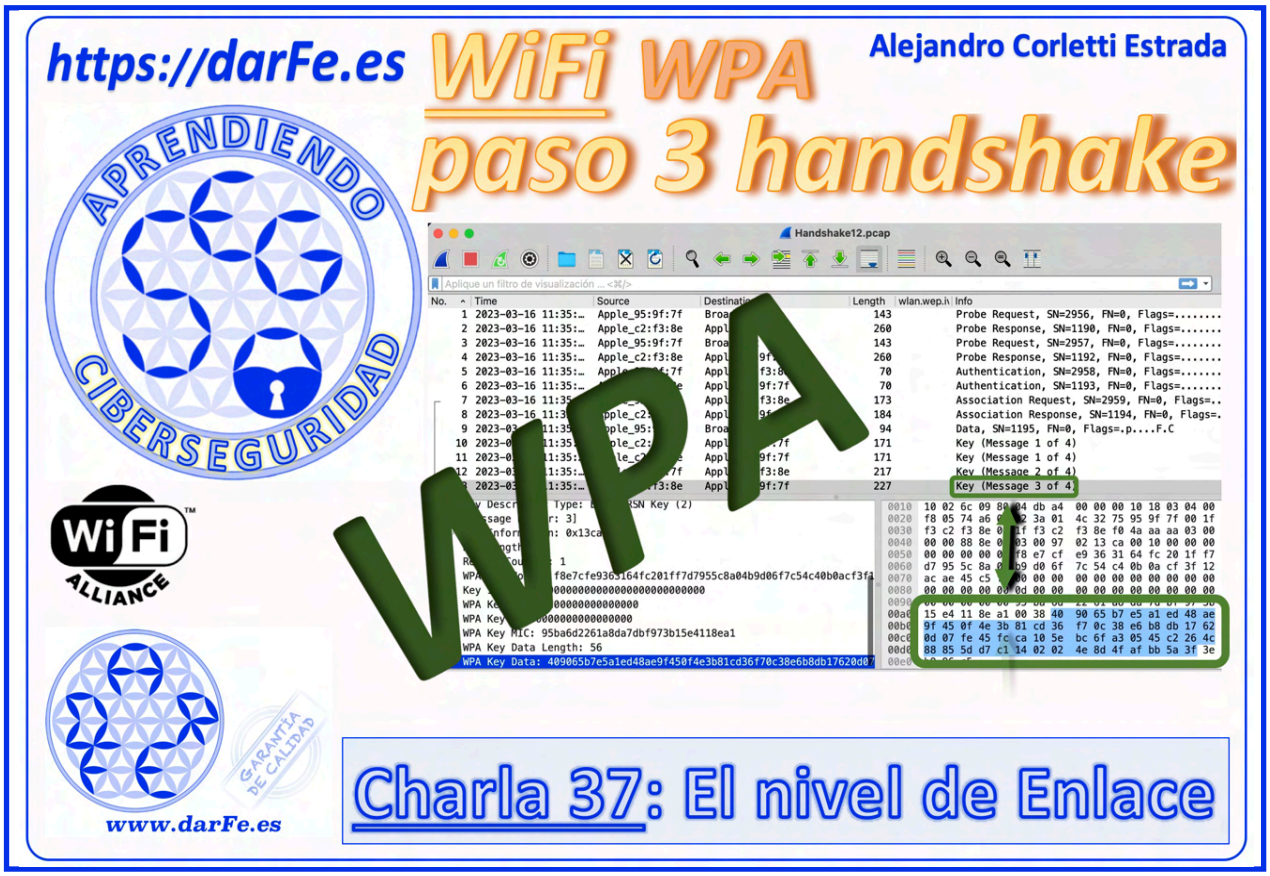
4 = Votos o número de probabilidades de que sea correcto ese byte

Volver al índice

www.darFe.es

Charla 37

WiFi - WPA paso 3: handshake



Enlace al Video:

Resumen:

En el capítulo anterior, comenzamos con el protocolo **WEP**, profundizando en las debilidades que presenta el empleo del mismo.

En este de hoy, continuaremos avanzando sobre la familia **WPA**, hasta llegar a **WPA3**, y sobre todo profundizando en la vulnerabilidad encontrada en 2017 sobre **WPA2**. La presentaremos por medio de una captura de tráfico, explicando brevemente su problema.

Descripción detallada

El experto en seguridad **Mathy Vanhoef,** en el año 2017 publicó en ataque conocido como **KRACK**, que son las siglas de "Key Reinstallation Attack" (Ataque de reinstalación de clave).

En WPA2, la autenticación se realiza a través de un cuádruple "handshake", es decir un intercambio de información de cuatro tramas. En este proceso de negociación se genera una nueva clave con la que se cifrará todo el tráfico de esa sesión.

KRACK afecta al tercer paso del handshake, lo que permite que el atacante manipule y reproduzca la clave de cifrado WPA2 e instalar una clave que ya estuvo en uso.

Una vez que se ha puesto en riesgo la encriptación WPA2, el atacante puede utilizar un software para capturar todos los datos transmitidos por la víctima a través de la red.

Es importante destacar es que con este ataque no se consigue la contraseña de nuestra red WiFi. Un atacante no podrá robar nuestra conexión, pero sí podrá espiar todo lo que hacemos a través de ella.

Para dar solución a este problema, en enero de 2018, la Wi-Fi Alliance anunció **WPA3** como reemplazo de WPA2, con las siguientes opciones:

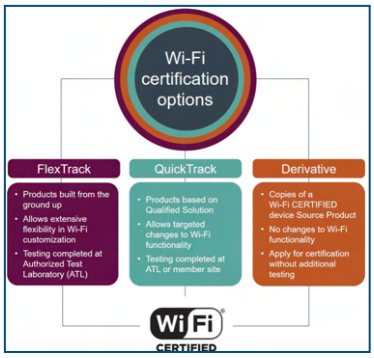
- WPA3 Personal - 128 bits
- WPA3 empresarial - 192 bits

Este algoritmo lo hemos desarrollado en las Charlas 29 y 31, por lo que no seremos redundantes con el mismo, pero sí remarcaremos condiciones que no puedes olvidar sobre configuración de redes WiFi:

1. JAMÁS usar redes abiertas (sin criptografía, ni autenticación)
2. NO usar WEP
3. Evitemos el uso de WPA +TKIP
4. Una opción de mejora es WPA +TKIP/AES (opcional)
5. Un poco mejor: WPA + AES
6. Mejor opción (hasta aquí) WPA2 + AES
7. Óptimo: WPA3 + AES 192 bits

Esta última opción es la que deberíamos intentar configurar. WP3 nos ofrece también, durante el proceso de autenticación, el empleo de **HMAC-SHA256** (Hashed Message Authentication Code - Secure Hash Algorithm), con lo que si alguien intentara colarse en esta autenticación, debería romper esos Hash cuya longitud (256), podríamos afirmar que en el corto tiempo de este intercambio, hoy por hoy es irrompible. Otra pieza clave el la protección de "**Management frames**" o tramas de gestión, esto se denomina **MFP** (Management Frame Protection). Este tema en telecomunicaciones es una batalla antiquísima, pues este tipo de tramas, que son diferentes a las "**Data frames**" o tramas de datos, son las más importantes de toda comunicación, pues son ellas, justamente, las que se emplean para la configuración y administración de la conexión, por lo que si podemos manipularlas se corrompe todo el diálogo.

Otra novedad de WPA3 es "**WiFi Easy Connect**" que nos habilita que el punto de acceso WiFi, ya tenga impreso un **código QR**, que al escanearlo, emplea "clave pública" y nos permite realizar una conexión mucho más segura aún. Sobre esto de la criptografía asimétrica, recordad que lo tratamos en la **charla 25**:

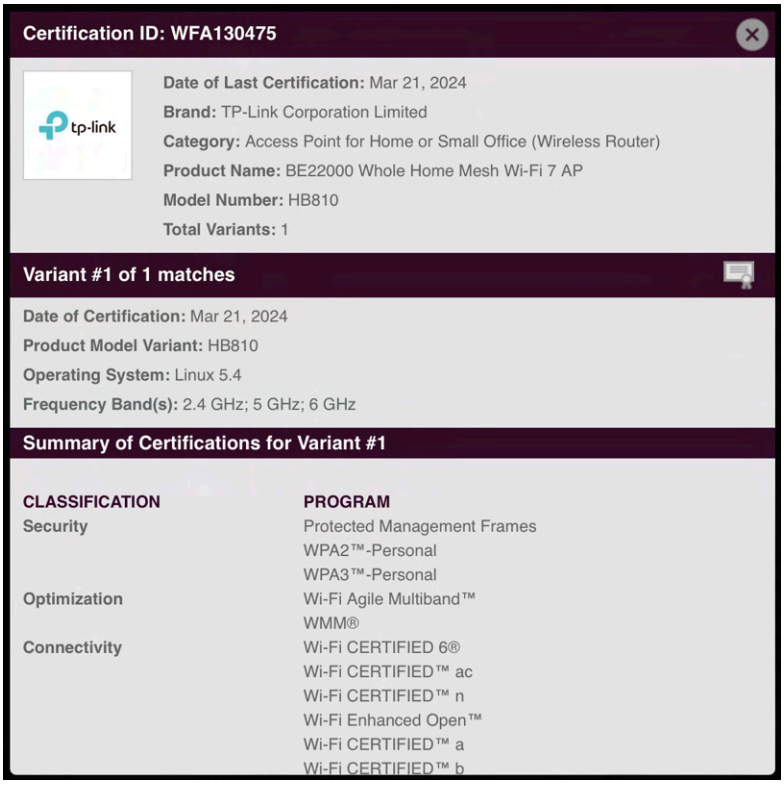


Por estas razones, es importante verificar que nuestros puntos de acceso posean la certificación de WPA3, antes de adquirirlos o implementarlos en nuestra redes WiFi.

Podemos consultar estas certificaciones en:

https://www.wi-fi.org/certification

En esta Web, podemos buscar cualquier producto y verificar si está o no certificado por la **WiFi Alliance**.



Vamos a trabajar con una captura de tráfico de **WPA2** sobre **EAPOL** (Extensible Authentication Protocol Over LAN), tema que ya lo hemos tratado en al **Charla 23**.

En WPA2, lo importante es que puedo trabajar "off-line", es decir, lanzar una captura de tráfico sobre el access point destino, y luego desde cualquier otro sitio, analizar esa captura y aplicarle la suite "aircrack-ng" para intentar desencriptar la contraseña. Cosa que no sería posible de realizar sobre **WPA3**.

En el video correspondiente a esta Charla 37, se puede ver que este trabajo lo estamos realizando con dos portátiles. La primera de ellas, es la que realiza toda la conexión al punto de acceso "**WiFiace**" que es la maqueta que tenemos implementada desde la charla anterior. La segunda portátil, es la que capturará todo este tráfico.

Inicialmente capturamos el establecimiento de la sesión con el punto de acceso "WiFiace", que son las doce tramas que podemos ver en la imagen que sigue.

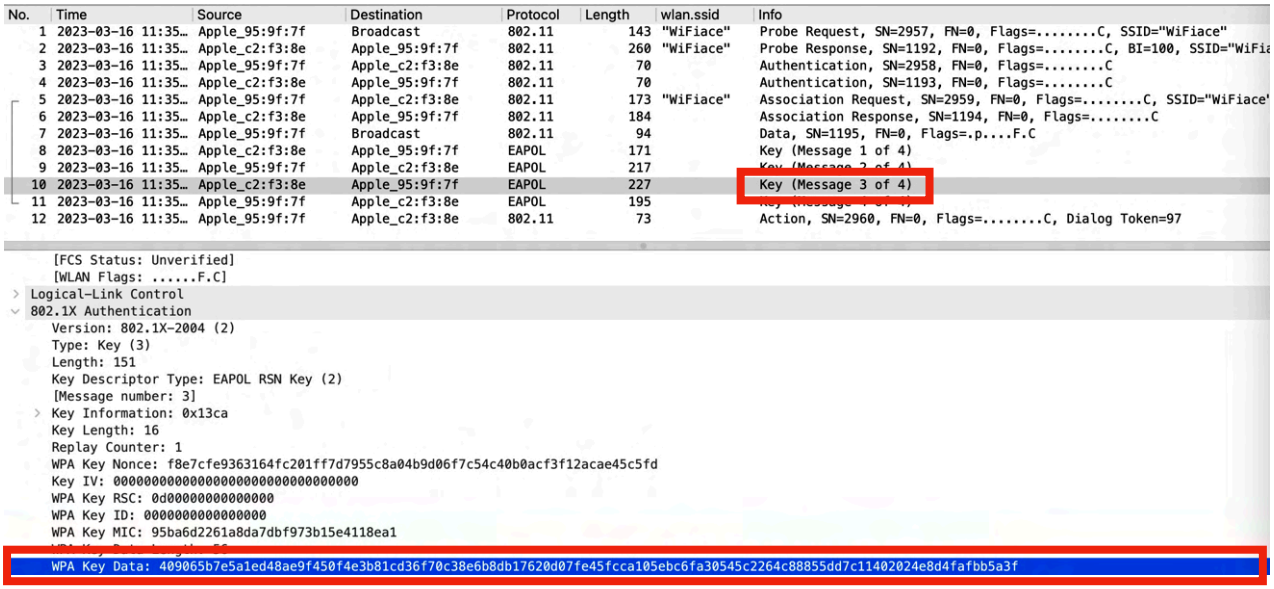
No.	Time	Source	Destination	Protocol	Length	wlan.ssid	Info
1	2023-03-16 11:35…	Apple_95:9f:7f	Broadcast	802.11	143	"WiFiace"	Probe Request, SN=2957, FN=0, Flags=........C, SSID="WiFiace"
2	2023-03-16 11:35…	Apple_c2:f3:8e	Apple_95:9f:7f	802.11	260	"WiFiace"	Probe Response, SN=1192, FN=0, Flags=........C, BI=100, SSID="WiFia
3	2023-03-16 11:35…	Apple_95:9f:7f	Apple_c2:f3:8e	802.11	70		Authentication, SN=2958, FN=0, Flags=........C
4	2023-03-16 11:35…	Apple_c2:f3:8e	Apple_95:9f:7f	802.11	70		Authentication, SN=1193, FN=0, Flags=........C
5	2023-03-16 11:35…	Apple_95:9f:7f	Apple_c2:f3:8e	802.11	173	"WiFiace"	Association Request, SN=2959, FN=0, Flags=........C, SSID="WiFiace"
6	2023-03-16 11:35…	Apple_c2:f3:8e	Apple_95:9f:7f	802.11	184		Association Response, SN=1194, FN=0, Flags=........C
7	2023-03-16 11:35…	Apple_95:9f:7f	Broadcast	802.11	94		Data, SN=1195, FN=0, Flags=.p....F.C
8	2023-03-16 11:35…	Apple_c2:f3:8e	Apple_95:9f:7f	EAPOL	171		Key (Message 1 of 4)
9	2023-03-16 11:35…	Apple_95:9f:7f	Apple_c2:f3:8e	EAPOL	217		Key (Message 2 of 4)
10	2023-03-16 11:35…	Apple_c2:f3:8e	Apple_95:9f:7f	EAPOL	227		Key (Message 3 of 4)
11	2023-03-16 11:35…	Apple_95:9f:7f	Apple_c2:f3:8e	EAPOL	195		Key (Message 4 of 4)
12	2023-03-16 11:35…	Apple_95:9f:7f	Apple_c2:f3:8e	802.11	73		Action, SN=2960, FN=0, Flags=........C, Dialog Token=97

Las tramas 1 y 2 son la solicitud y respuesta, la primera de ellas, como podemos ver, es un “Broadcast” en la cual mi portátil Macintosh, cuya dirección MAC termina en “**:7f**”, está buscando cuál es el punto de acceso “WiFiace” del cual no conoce su dirección MAC, por esta razón, en la trama 2, recibe esta respuesta en la cual le indica cuál es su dirección MAC, la que termina en “**:8e**”.

En las cuatro tramas que siguen: 3, 4, 5 y 6, podemos ver en la 3 y 4, una solicitud de autenticación, su respuesta y luego en las tramas 5 y 6 una solicitud y respuesta de asociación.

Lo que nos interesa ahora son los cuatro pasos de la fama 8 a la 11, en los cuáles podemos claramente este cuádruple handshake EAPOL con los mensajes del 1 al 4.

De estas últimas cuarto tramas, como ya hemos mencionado, la que nos interesa es el mensaje número 3 (trama 10), en el cual, como podemos ver en la imagen que sigue, viaja el campo “**Key Data**”.



Volver al índice

www.darFe.es

Charla 38

WiFi - Crack WPA y WPA2

Enlace al Video:

Resumen:

Este capítulo, es como un alto de marcha en el tema WiFi, pues nos interesa aquí presentar un par de herramientas “**cupp**” y “**pydictor**” que instalaremos en nuestro **Kali**, para trabajar con ataques de diccionario y personalizando los mismos.

Lo iremos viendo “paso a paso”, incorporando también algunos comandos de consola básicos de Linux que nos serán de mucha utilidad.

Descripción detallada

Para seguir avanzando en el criptoanálisis de contraseñas de WPA y WPA2, en esta charla de hoy, haremos una especie de alto en el camino, para profundizar en la "**generación de diccionarios**".

Los diccionarios de usuarios y contraseñas, serán un pilar fundamental en nuestras arquitecturas de Ciberseguridad, pues nos permitirán verificar si realmente los usuarios de mi organización se toman en serio la importancia que tiene el empleo de contraseñas robustas, los usuarios personalizados y no genéricos, los cambios de contraseñas, etc.

Mantener una política de gestión de usuarios y contraseñas robusta, es una actividad tediosa y que suele ser molesta desde los administradores, hasta los usuarios finales. Recordemos que es importante que no sean triviales, que incorporen caracteres especiales, que no se relacionen fácilmente con los datos del usuario, que se cambien periódicamente… Todo esto es una carga adicional de trabajo que, aunque nos cueste, hay que generar y cumplir por el bien de la fortaleza de nuestras redes y sistemas.

Para la verificación de su cumplimiento, nada mejor que contar con herramientas que puedan auditarlas, en este caso, lo haremos con las redes WiFi, pero estos principios aplicarán a todo tipo de redes y sistemas.

A medida, que vamos conociendo nuestras infraestructuras, poco a poco, podemos detectar ciertas tendencias y usos de palabras, contenidos, nombres, fechas, números, usuarios, etc., que nos permiten medir mucho más eficientemente, el nivel de madurez.

En esta charla de hoy, avanzaremos con la creación y mantenimiento de listados de usuarios y contraseñas, que debemos ir mejorando de forma continua, a medida que detectamos rutinas, costumbres y repeticiones, las solucionamos y posteriormente evaluamos que no vuelvan a ocurrir.

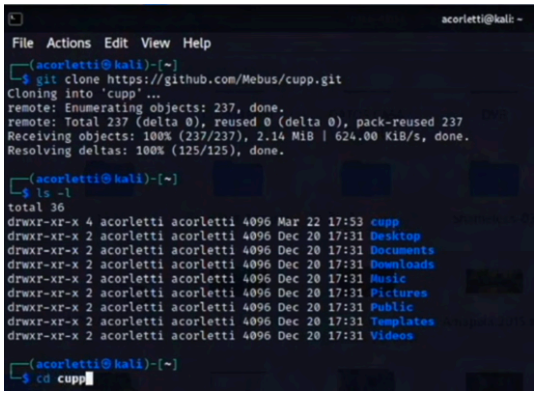
Estos diccionarios, en realidad pueden iniciarse con búsquedas en Internet, pues encontraremos miles de ellos que contienen listados de millones y millones de palabras.

Pero, con independencia que empleemos los que encontremos por Internet, la mejor mecánica de trabajo, es saber ajustarlos a nuestra organización, pues como cabe imaginar, hay nombres, siglas, equipos, fabricantes, grupos, roles y perfiles, nomenclaturas y terminologías, que son particulares de mi empresa, por esa razón, cuanto más lo ajustemos a "lo nuestro", mejor será. Para ello, en este capítulo presentaremos algunas alternativas muy útiles.

Volvemos a trabajar con nuestro "**Kali**" e instalaremos una nueva herramienta que será "**cupp**". Lo haremos desde una consola de línea de comandos de Kali, ejecutando el comando:

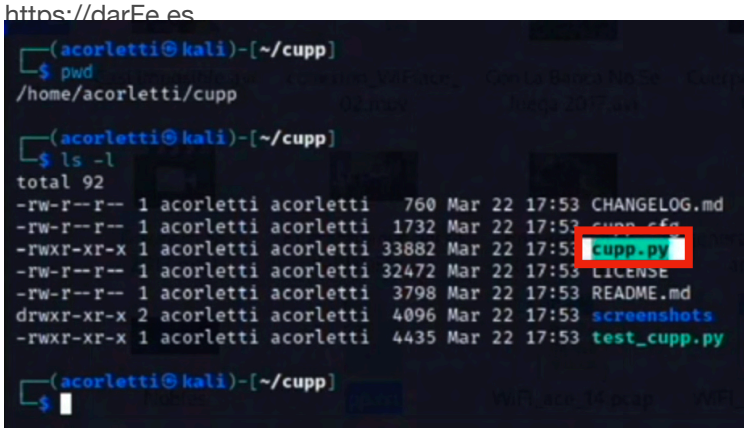
#git clone https://github.com/Mebus/cupp.git

Una vez ejecutado, veremos que se ha creado un nuevo directorio "**cupp**", tal cual se presenta en la imagen de la derecha.



Ejecutamos: **#cd cupp**

E ingresamos en el mismo. Si queremos verificar cuál es la ruta en la que nos encontramos, podemos ejecutar: "**#pwd**" y nos mostrará la ruta completa.



Si deseamos ver todos los ficheros y directorios, podemos ejecutar: "**ls -l**" y nos presentará lodo el listado, tal cual podemos ver en la imagen de la izquierda.

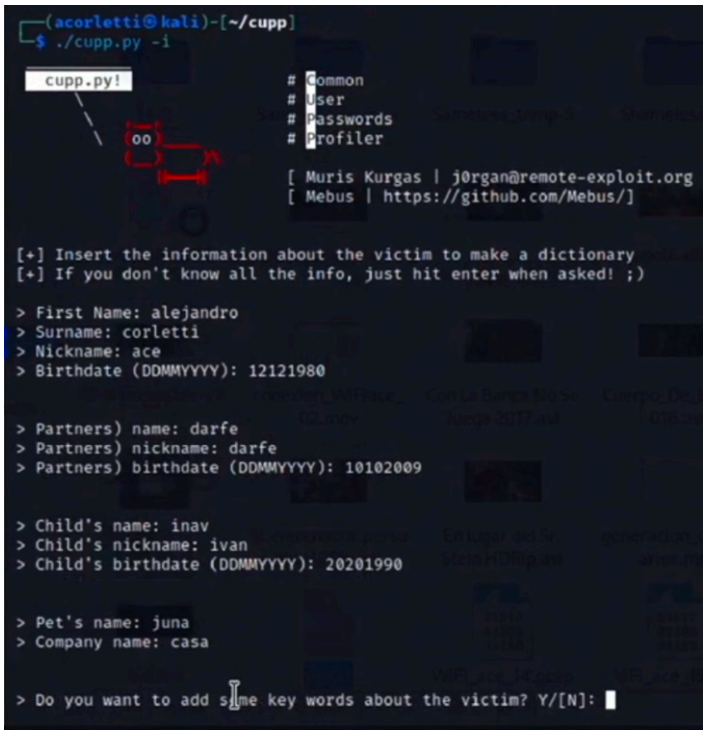
Como podemos ver recuadrado en **rojo,** en este directorio, tenemos en fichero "**cupp.py**".

La extensión "**.py**" nos está indicando que se trata de un programa desarrollado en el lenguaje de programación "**Python**". Si prestamos atención a la línea completa, podemos ver que en este caso el propietario de ese fichero es el usuario "acorletti" y al principio de la línea veremos que nos indica "**rwx**", esto quiere decir que el usuario "acorletti" tiene permisos de: **r** (read - lectura), **w** (write - escritura) y **x** (execute - ejecución). Todo esto está relacionado al usuario "acorletti" pues es el que hemos empleado para acceder a la máquina virtual Kali y con el que instalamos **cupp**.

Para ejecutar un programa "Python", normalmente se lo hace con el comando: **# python cupp.py**, pero Linux nos ofrece también la posibilidad de hacer con "**./**" , por lo que también podemos hacerlo con: **# ./cupp.py**.

Como podéis ver "**cupp**" significa "*Common User Passwords Profiler*"

En la imagen de la derecha, podemos ver también que hemos recuadrado en **verde** la opción **[-i]** que significa"**interactive**".



Esta opción, es la más sencilla para comenzar a emplear esta herramienta.

En la imagen de la izquierda, podemos ver como nos va preguntando diferentes opciones: primer nombre, apellido, nickname, empresa, fechas, etc.

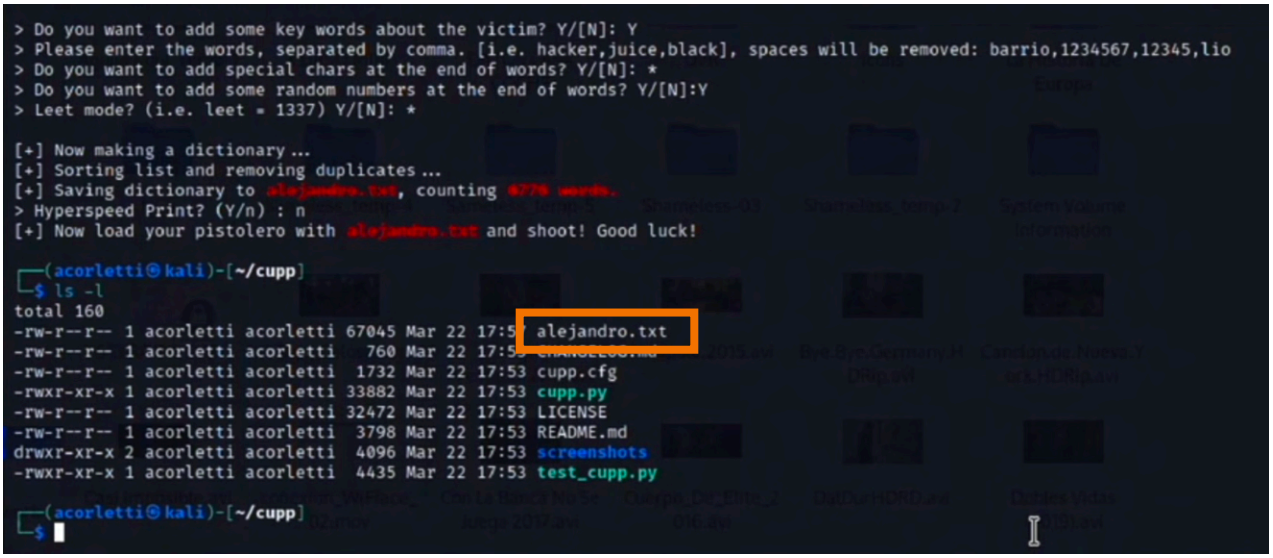
Al finalizar todas estas preguntas por defecto, nos pregunta si deseamos adicionar alguna palabra más. Podemos hacerlo **[Y]**, o seguir sin ninguna más **[N]**.

En nuestro caso, seleccionaremos [Y], e incorporaremos algunas palabras más.

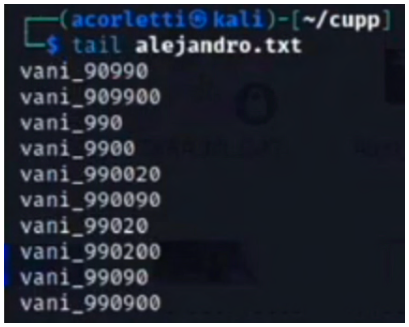
En la imagen de la página siguiente, podemos ver que nos informa que

para ingresa varias palabras, podemos hacerlo separándolas por “coma”. En nuestro agregamos: **barrio,1234567,12345,lio**.

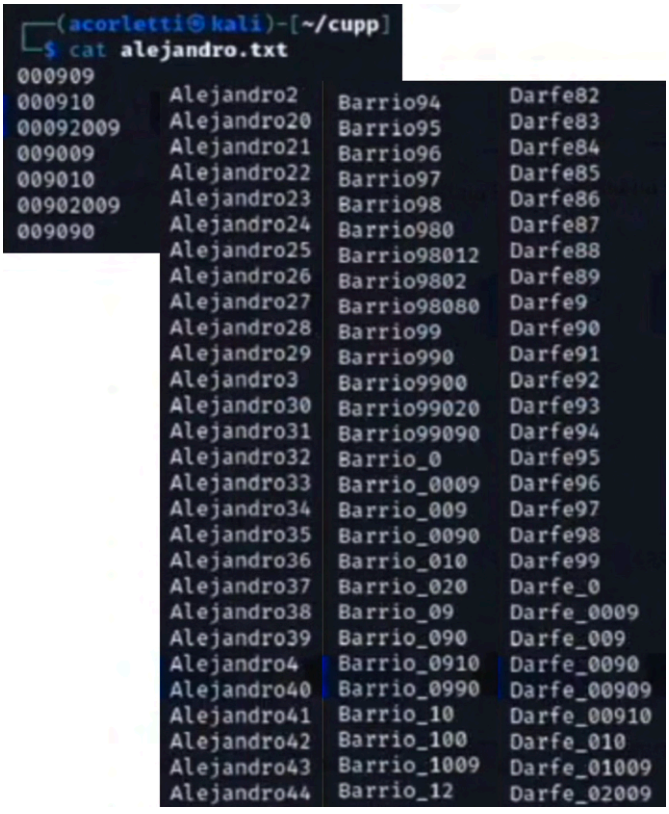
Luego nos permite también incorporar caracteres especiales, los cuáles, recordad que son muy importantes en al fortaleza de contraseñas. En nuestro caso, incorporamos el carácter “*”.



Una vez finalizado, podemos ver que ha sido creado un nuevo fichero “**alejandro.txt**” que lo hemos resaltado en color **naranja**.



Si quisiéramos ver el contenido de un fichero, Linux nos ofrece muchos comandos, uno de ellos es “**tail**” que nos muestra las últimas líneas. Por defecto, nos mostrará las diez últimas.



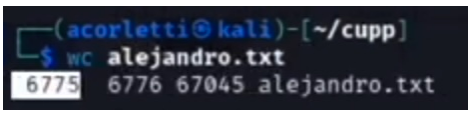
Si quisiéramos ver las últimas veinte filas podríamos poner “**#tail -20 alejandro.txt**”, y así la cantidad de líneas que deseemos del final del fichero.

Si por el contrario, deseamos comenzar a ver la lista desde el principio, el comando es “**head**” y aplica la misma lógica.

Si se desea visualizar el fichero al completo, el comando más conocido es “**cat**”. A la izquierda presentamos solo algunas líneas de la ejecución de “cat”.

El comando en Linux para saber la cantidad de palabras que contiene un fichero es “**wc**” (word count), que si lo

ejecutamos sobre el fichero alejandro.txt, nos informa que se contiene **6.775** palabras, como podemos ven remarcado en "blanco" en la imagen de la derecha.

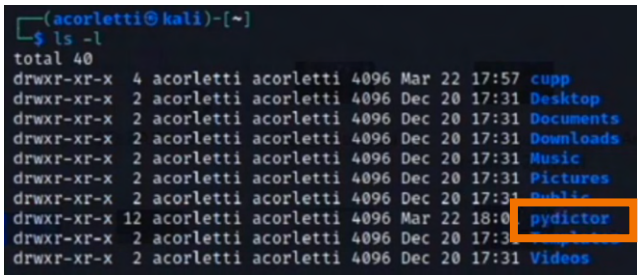


Es decir, en unos pocos segundos, acabamos de generar un diccionario de palabras clave, sobre la base de cierta información que conocíamos (ace, alejandro, barrio, etc.) de 6.775 palabras.

Sigamos avanzando aún más con esto de los diccionarios. Nuevamente por línea de comandos, vamos a instalar otra herramienta, manteniendo la misma mecánica de instalación, esta vez será:

```
git clone https://github.com/LandGrey/pydictor.git
```

Al igual que en la instalación anterior, una vez más podemos ver que se ha creado otro directorio, esta vez con el nombre "**pydictor**"



Nuevamente, si nos desplazamos dentro de este directorio, nos encontraremos con otro fichero "Python" muy similar al anterior, este se llama "**pydictor.py**".

Un detalle que también podemos prestar atención, es que en esta línea NO tenemos permiso de ejecución, pues nos indica que es solamente "**rw**".

Para permitirnos ejecutar este fichero debemos modificar sus permisos. Lo haremos mediante el comando:

```
# chmod 755 pydictor.py
```

Una vez ejecutado este comando, como podemos ver en la imagen de arriba, ya nos aparece "**rwx**", a su vez, si prestamos atención, también ha cambiado de color el nombre del fichero "pydictor.py" que antes era blanco y ahora es "**verde**", lo que también nos indica que es un fichero ejecutable.

En cuanto a la gestión de permisos y grupos en Linux, os recomendamos que veáis el video de esta charla, pues allí hemos explicado con más detalle el tema. También en el video se desarrolla en detalle cómo crear este segundo diccionario con la nueva herramienta. No lo desarrollaremos por escrito pues es muy similar al anterior, y como es más interactivo, es mejor que lo veáis desde el video mismo.

Con esa última herramienta, finaliza el capítulo, pues la continuación y final de este tema, se desarrolla en el capítulo siguiente.

Volver al índice

www.darFe.es

Charla 39

WiFi - Crack WPA y WPA2 (Continuación)

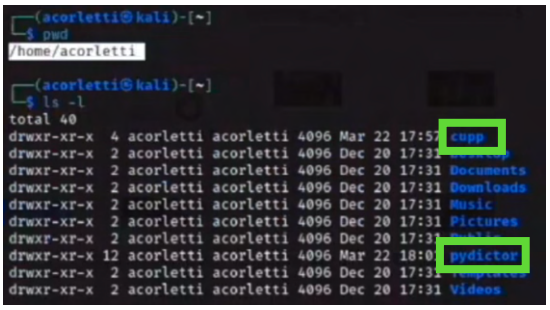
Enlace al Video:

Resumen:

En este último capítulo sobre la suite “**aircrack-ng**”, ampliaremos la potencia de nuestros diccionarios recientemente generados, y luego desarrollaremos cómo se aplican los mismos para crackear una contraseña de **WPA2**, que a diferencia de **WEP**, que recordemos se realizaba por medio de capturas de sus vectores de inicialización, en el caso de WPA2, solo puede hacerse por medio de ataques de “**diccionario**” y/o “**fuerza bruta**”.

Descripción detallada

En la charla anterior, hemos logrado crear dos diccionarios personalizados con palabras que nos interesan o guardan relación con nuestra empresa o infraestructura. Por supuesto que, como todo "ciclo de vida de la seguridad", estos diccionarios se irán mejorando y ampliando mes a mes, sobre la base de nuestra experiencia y mayor conocimiento. Veréis que al cabo de unos años de experiencia, cada vez será más sólido, y no solo sobre vuestras organizaciones, sino también a la hora de hacer una auditoría de seguridad o penetration test sobre cualquier otra empresa.



Ya tenemos instaladas las dos herramientas en nuestro Kali. En la imagen de la derecha, podemos ver, en nuestro caso, dentro del directorio "**/home/acorletti**", los directorios correspondientes a las mismas: "**cupp**" y "**pydictor**".

Con cada una de ellas, logramos generar un diccionario relacionado a nuestras palabras clave, números y signos especiales. Por supuesto, que estos son solo ejemplos, cuando trabajamos en la vida real con ellas, debemos esforzarnos más para lograr diccionarios mucho más grandes y detallados.

Vamos a mejorar nuestros diccionarios "**concatenándolos**" para formar uno solo.

El primer paso, será colocar ambos diccionarios en un mismo directorio. En nuestro caso, lo haremos directamente en "/**home/acorletti**". El primer paso, será posicionarnos en cualquiera de los directorios de las herramientas, por ejemplo, "# **cd /home/acorletti/cupp**" y desde allí copiar el diccionario al directorio indicado.

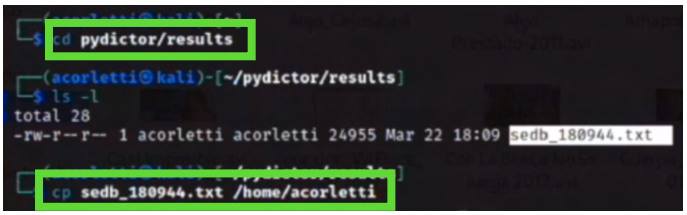
Desde "/home/acorletti/cupp", ejecutaremos:

 # cp alejandro.txt /home/acorletti"

Si ahora nos posicionamos nuevamente en el directorio "/home/acorletti" con el comando "**#cd ..**" (sube un nivel en el árbol de directorios), veremos que en el mismo, ya está el fichero "**alejandro.txt.**"

Ahora, repetimos el mismo paso anterior pero sobre el otro diccionario. Es decir, nos posicionamos en el directorio "**/home/acorletti/pydictor**" con el comando:

#cd /home/acorletti/pydictor/results



Una vez posicionado en el mismo, copiamos el diccionario "**sedb_180944.txt**" en el directorio "**/home/acorletti/**" con el comando:

 # cp sedb_180944.txt /home/acorletti

Ya tenemos copiados los dos diccionarios. Como hemos visto Linux nos ofrece una enorme cantidad de comandos, estuvimos viendo el comando "**cat**" cuyo significado viene de la palabra inglesa. "**concatenate**", es decir, concatenar. Vamos ahora, justamente hacer uso de este comando para concatenar ambos diccionarios y crear uno solo. Lo haremos con la siguiente instrucción:

#cat sedb_180944.txt >> alejandro.txt

Con esta instrucción, hemos logrado unir ambos diccionarios en uno solo cuyo nombre es "alejandro.txt". Si queréis seguir avanzando más aún, tenéis el comando "**sort**" para ordenarlo, dejar registros únicos, etc. que no lo desarrollaremos aquí.

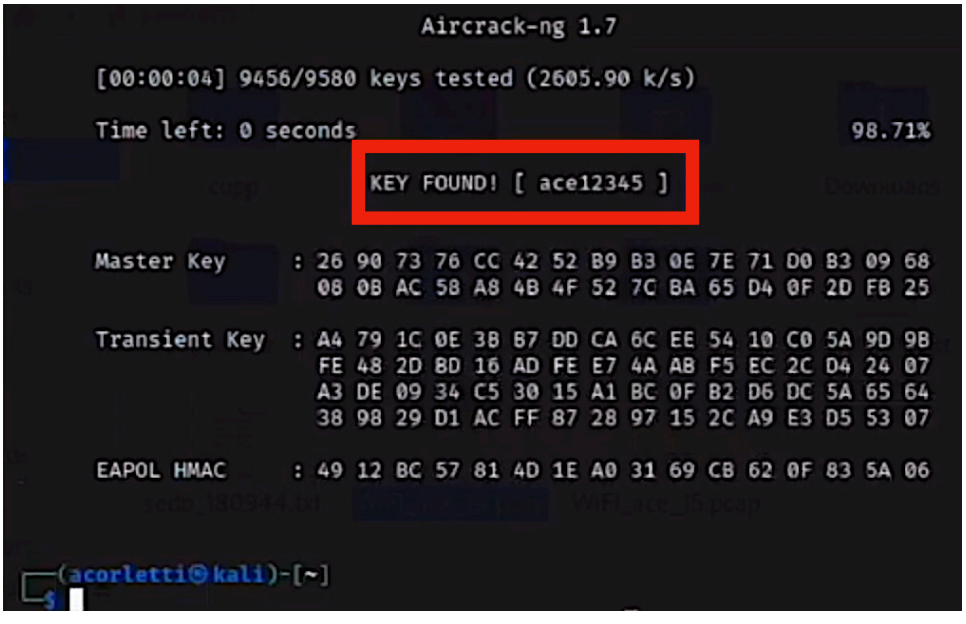
> **CUIDADO**: Hemos ejecutado el comando "**cat**" con el **doble redirector**, es decir "**>>**" justamente para "concatenar" (*sumar ambos ficheros*), pero CUIDADO, si empleamos UN SOLO redirector, lo que hará será sobre sobre escribir (*machacar*) el segundo fichero con el contenido del primero, así que analizadlo, probadlo y aseguraros la diferencia entre concatenar (**>>**) y sobre escribir (**>**), si no queréis arrepentiros de perder un fichero al completo de forma *irrecuperable*.

Vamos ahora a volver an nuestra suite "**aircrack-ng**", operaremos sobre esa captura "**WPA2**" que teníamos desde la charla anterior, y ejecutamos:

#aircrack-ng -e WiFiace WiFiace_14.pcap - w alejandro.txt

Le acabamos de decir, con la opción "**-e**", que trabaje sobre el punto de acceso "**WiFiace**", que utilice la captura de tráfico "**WiFiace_14.cap**" y con la opción "**-w**", que emplee el diccionario "**alejandro.txt**".

Al ejecutarlo, si el diccionario ha dado resultado, se nos presentará una pantalla como la que vemos a continuación, en la cual hemos recuadrado en **rojo**, que ha logrado encontrar encontrar la clave, que en nuestro caso es "**ace12345**".



Por supuesto que es una clave muy trivial y relacionada directamente con el punto de acceso, sin caracteres especiales, etc. Pero, se trata solamente de un ejemplo didáctico sobre una maqueta WiFi, para que podáis analizar y probar el funcionamiento de la suite "**aircrack.ng**" empleando y creando diccionarios.

Si bien parece trivial el ejemplo, cuidado que no lo es tanto, pues si la clave hubiese sido en vez de ocho, de nueve caracteres, tal vez también la hubiese descubierto, si hubiese tenido un asterisco como carácter especial, pues también. Este es solo el punto de partida para que os pongáis las pilas y dediquéis el tiempo necesario para incrementar la fortaleza y experiencia en este tema.

Seguramente en la vida real, sea más complicado, pero "no imposible" y todo dependerá del esfuerzo que pongamos y el ajuste del, o los, diccionarios que queramos emplear.

Volver al índice

Charla 40

Desenchufando: El Camino de Santiago

Enlace al Video:

Resumen:

Por favor, permitidme incorporar este “Desenchufe”, sin mayores críticas, pues es para mí, es el capítulo más importante de este libro.

Es tan, pero tan, pero tan, tan, tan hermoso este Camino, que no puedo dejar de transmitir todas las vivencias que suponen para aquel, que alguna vez en su vida lo emprende. Si en vuestras noches soñáis con hacer un viaje inolvidable, no dejéis de considerar esta opción, pues os aseguro que así será: INOLVIDABLE.

Descripción detallada

Este desenchufe de hoy, es el más bonito de todo este ciclo. Nos presenta "**El Camino de Santiago**", una de las más preciosas maravillas que tiene España.

Durante el video se describe bastante el tema, y sinceramente, lo hago con todo ese "Cariño verdadero" que le tengo al Camino, pues he recorrido casi todos sus itinerarios.

Este camino tiene magia, encanto, sencillez, amistad, paisajes, comidas, playas, montañas, bosques, historia, lenguas, desenchufe, y sobre todo "**deja huella**", y de las buenas, de esas que te hacen ser mejor persona de la que fuiste el día del primer paso.

Dejamos dos enlaces que hace referencia el video:

El libro:

Kayrós (de escalas, tiempos, ciclos y sobre todo "Momentos trascendentes")

https://www.google.es/books/edition/Kayrós_De_escalas_tiempos_espacios_y_so/t5P5v4Kg7WEC?hl=es&gbpv=1&dq=alejandro+corletti&printsec=frontcover

KAYRÓS

Según Wikipedia Kayros o Kayrós es "*el momento justo*", en la filosofía Griega y Romana la *experiencia del momento oportuno*, los pitagóricos le llamaban *Oportunidad*; Kayrós es el tiempo en potencia, tiempo atemporal o eterno, y el tiempo es la duración de un movimiento, una creación. No es el tiempo cuantitativo sino el tiempo cualitativo de la ocasión, la experiencia del momento oportuno. Todos experimentamos en nuestras vidas la sensación de que llegó el momento adecuado para hacer algo, que estamos maduros, que podemos tomar una decisión determinada. Para los mayas era el Zubuya. En general, es un "Momento de claridad" y, en el espacio temporal, es el momentum de la epifanía (según la etimología 'momento milagroso') y de la iluminación; el momento literario de la introspección, y el momento cinematográfico de los instantes antes de la muerte donde todo pasa, como una película ante los propios ojos.

Kayrós: En nuestro aprendizaje de la verdad humana, poco a poco, vamos asumiendo el concepto "cronológico" de la vida (de chornos), es decir todo se mide en segundos, minutos, horas, días... en antes y después. Pero hay otro concepto del tiempo que se consideraba a lo largo de muchos milenios "**Kayrós**", este concepto no guarda relación con el cronológico. Aquí no hay antes ni después. Para no irnos a la definición filosófica ni religiosa, sino a lo que nos importa a cada uno de nosotros, **kayrós es el tiempo de nuestros momentos trascendentes, de los hechos que marcan fuerte el camino personal de cada uno de nosotros, eso que algunos denominan destino, y que en determinados momentos nos hizo tomar decisiones importantes.** No nos importa el antes ni el después, sólo el kayrós, solo esos momentos clave de nuestra historia personal.

El otro enlace, es la Canción:

"**Peregrino Buen Camino**"

https://youtu.be/2WoIZpqFHpo

La letra de esta canción (o su título), se debe a que la primer noche que hice en un albergue (el de León) llegué bastante tarde, casi no quedaba sitio así que desplegué mi saco de dormir en el suelo (en esa época aún te dejaban), y su hospitalero pocos minutos después apagaba las luces despidiéndose con un "Peregrino buenas noches, peregrinos buen Camino", y así nació la letra que sigue:

Peregrino, buenas noches, buen camino
(ACE).

Sin saber bien porqué
O si es verdad, no lo sé
Hay un sitio en que la fe
Atrae millones a ver
Unos van sin razón
Otros buscan un porqué
Aventura, soledad, reflexión
Paisajes, silencios, dolor.
Peregrino, buenas noches, buen camino.

No lo hagas por religión
No solo es cuestión de fe
Este no es un paseo más
Es una meta a lograr
No busques explicación,
Solo camina y verás
Que al entrar por el portal

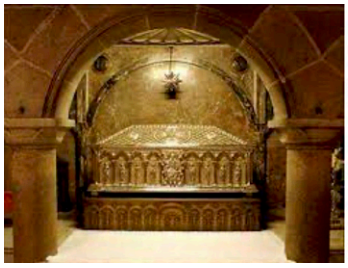
Algo en tu vida cambió
Peregrino, buenas noches, buen camino.

La simpleza es el común
El albergue es comunión
De lenguas, de religión
De sonrisas, de canción.
En ese camino hay algo
Que nos invita a llegar
Desencadena el milagro
De dejar cosas atrás.
Peregrino, buenas noches, buen camino.

Avanzas en tu interior
Subes y bajas tu ser
Pierde sentido tu honor
No tienen precio tus pies
El agua, el sol valen más
Amanece la amistad
Anochece el egoismo
asoma ese nuevo ser
Peregrino, buenas noches, buen camino.

Y al llegar a la ciudad
Te sentirás raro, ya verás
El camino quedó atrás
Y vuelve la realidad
La compostela en la mano
Los recuerdos imborrables
La misa del peregrino
Una marca inolvidable
Peregrino este fue, peregrino este es tu camino.

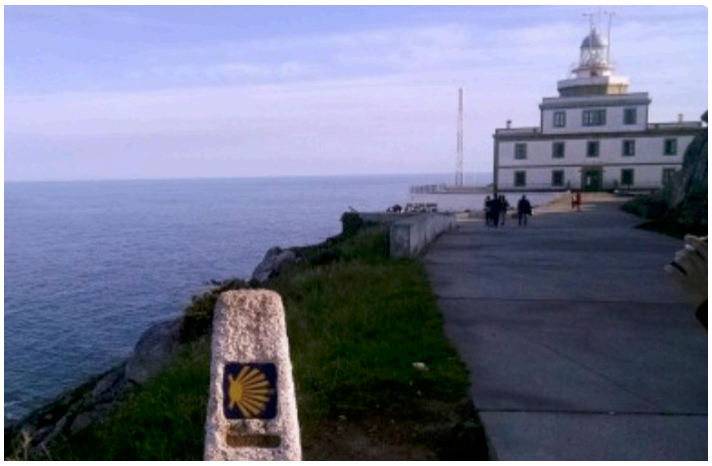
Santiago, Jacobo, Iago, Yago, Tiago, Diego, Santiago, Xacobe, Jaime…



Según el estudio de los escritos de los primeros siglos de la Iglesia, existen hipótesis que mencionan que tres Apóstoles pueden haber estado predicando por la provincia romana de "**Hispania**": **Pedro**, **Pablo** y **Santiago**.

Del primero de ellos, es el que menos constancia se tiene, y se considera bastante improbable. Del segundo se tienen dudas razonables, y al menos, hay suficiente constancia de sus planes de viaje hacia Tarragona,

De Santiago casi podemos afirmar que estuvo, tanto es así que nombró obispos de la zona, y dos de ellos quedan en la península, **Atanasio** y **Teodoro**.



La tradición cuenta que cuando matan a Santiago por orden de Herodes Agripa en el año 44 de nuestra era, sus discípulos para que su cuerpo no sea profanado, lo traen a Hispania, llegando en barca y entrando por **Finisterre**, cuyo nombre implica textualmente "Fin de la Tierra"

Al penetrar tierra adentro llegan al lugar donde se encuentra la actual ciudad de "**Santiago de Compostela**" y lo entierran allí. Años más tarde al fallecer sus dos discípulos que lo acompañaron desde el principio, son enterrados a su lado por seguidores suyos y aquí se pierden varios siglos de historia. El lugar queda oculto,

hasta que en el siglo VIII un ermitaño llamado **Pelayo**, por las noches ve luces como de estrellas en ese campus (de ahí lo de Campo de Estrellas o Compostela), le informa a **Teodosio** Obispo de Iria Flavia, que concurre al lugar y descubren el arca marmórea, donde supuestamente descansa el Apóstol, acompañado a ambos lados por sus dos discípulos. Teodosio lo notifica al rey **Alfonso II** El Casto, que viaja para investigar personalmente lo sucedido, ordenando la construcción en ese mismo lugar de la primera iglesia de "**Santiago de Compostela**" a finales de ese siglo (VIII).

Desde ese momento la noticia viaja por el mundo y comienzan las primeras peregrinaciones. Es cierto que la vía láctea se empleaba como referencia para llegar desde Europa hasta el sepulcro, lo cual sumado a que era el "fin del mundo", significaba un encanto especial, que invitó a millones de peregrinos.

Los siglos IX y X representan la consolidación del reino asturleonés en condiciones muy difíciles desde el punto de vista político, religioso y militar. **Al-Andalus** se había fortalecido políticamente desde la creación del Emirato primero y después el Califato de Córdoba. Este nuevo poder peninsular quedó reflejado en numerosas incursiones militares durante estos siglos, llegando a su máxima expresión, en los tiempos de devastación de **Almanzor**.

En el año 997, **Almanzor** destruyó la ciudad de **Santiago de Compostela** y su catedral.

Solo respetó la tumba del Apóstol.

Es por ello por lo que el enorme prestigio que proporciona la presencia de las reliquias de Santiago, fue hábil y rápidamente aprovechado por los monarcas asturianos y leoneses para consolidar su reino en oposición a Al-Andalus y para darse a conocer al resto de la Cristiandad Europea. Se hace de Santiago el abanderado de los ejércitos del cristianismo y se construyen varios monasterios de órdenes religioso/militares a lo largo del camino para proteger a los peregrinos y a su vez detener al avance Musulmán.

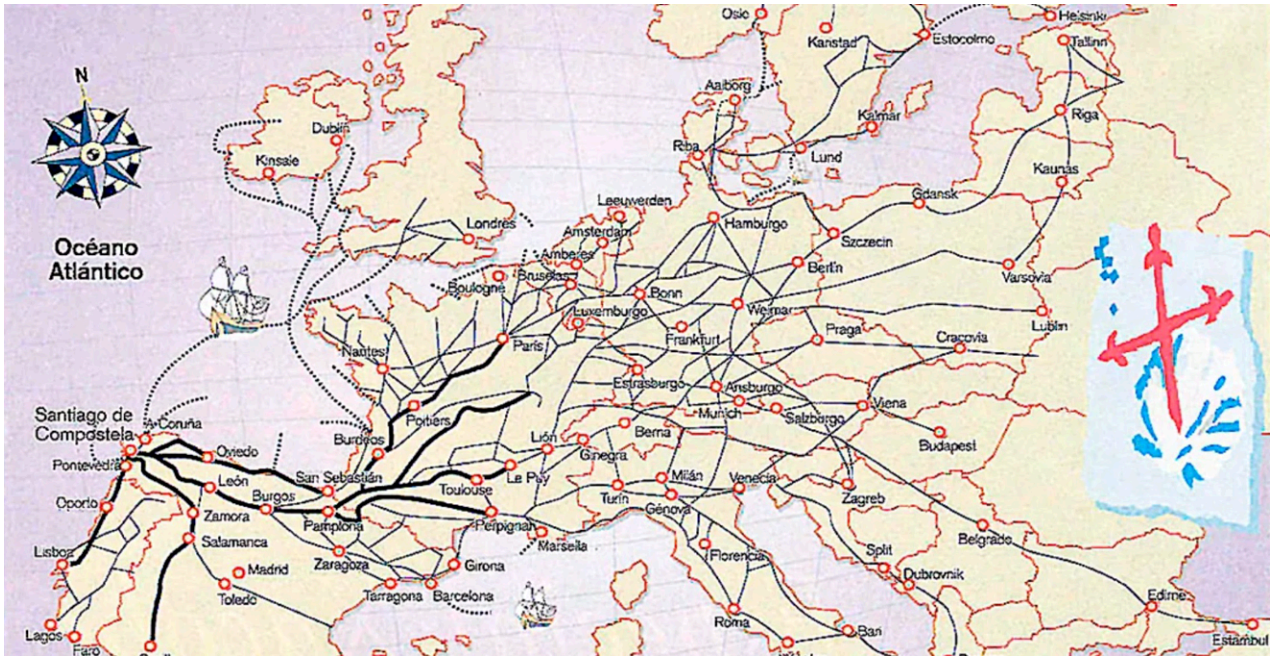
En el siglo X, ya se conoce por toda Europa el sitio de la sepultura del Apóstol, por lo tanto se empieza a generar la devoción de visitar este sitio como un lugar Santo, lo cual si lo analizamos fríamente, es lógico que pueda ser considerado así pues se trata de uno de los más importantes seguidores de Cristo y precursores de esta milenaria iglesia. Cabe destacar que este sitio genera uno de los mayores intercambios

culturales de España, pues el peregrinaje lo realiza todo tipo de gente, muchas de ellas conocidas, escritores, artistas, nobles, reyes y santos. La ciudad pasa a ser una de las más renombradas e importantes del continente, solo basta poder caminar hoy por sus calles para admirar los siglos de historia y esplendor que alberga. Un hecho importante es que en este siglo, se tienen antecedentes de los primeros documentos de la lengua castellana escritos en uno de los monasterios del Camino lo cual sin duda, sirvió, para la propagación de esta lengua por el mundo.

Durante la edad media decae sensiblemente esta devoción de peregrinar allí, pero a finales del siglo XIX resurge este merecido homenaje al Apóstol, que hasta el día de hoy continúa incansablemente.

Durante estos más de mil años de historia del Camino, la gente iba concurriendo desde los diferentes puntos cardinales, es por eso que no hay un solo Camino de Santiago, sino varios, lo que sí es cierto que el más popular y conocido es el denominado "Camino Francés", que entra en España por la localidad de "Roncesvalles" en los Pirineos. Luego del Francés en otros órdenes de concurrencia, pero no menos hermosos, existen también el de Norte (Cantabria - Asturias), otro desde el Sur o vía de la Plata, desde Madrid, también desde Portugal, etc.

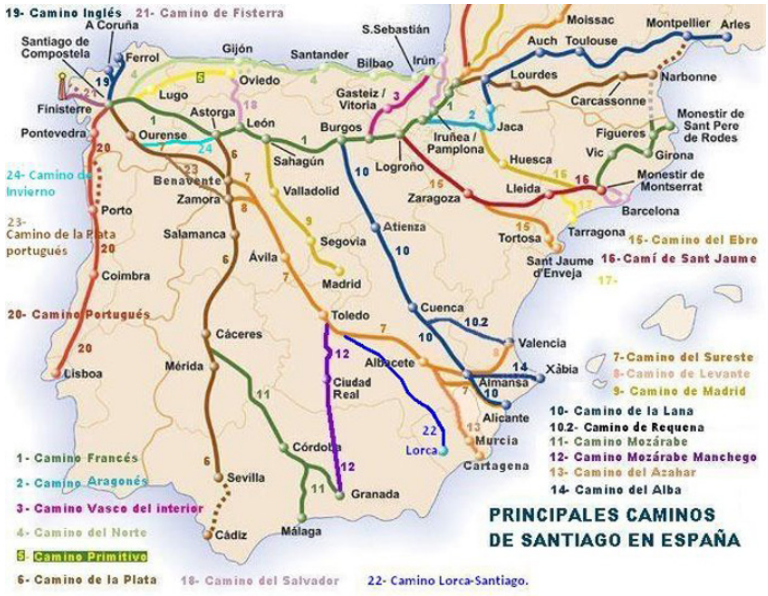
Hay rutas señalizadas y con mapas y guías de todos los países de Europa.



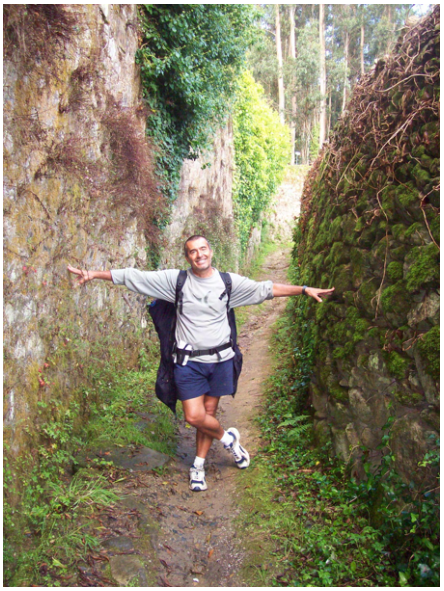
Cada uno de ellos guarda su encanto y los "**Amigos de Camino**", con mayor o menor apoyo de los gobiernos de cada Provincia o Comunidad Autónoma por los que pasa, se encargan de su mantenimiento, señalización, albergues, y difusión.

Independientemente del sentido religioso del Camino, tiene también mucha espiritualidad de fondo. Tal vez sea por los siglos que arrastra, por la tradición, por los

personajes que transitaron por él, o por esa magia que tiene llegar a Santiago de Compostela, pero lo cierto es que todo aquel que lo hace, cambia en algún aspecto de su vida, por supuesto para bien. El recuerdo del Camino lo acompañará por el resto de su vida, la fiebre que despierta en muchos, hasta lo transformará en un fiel asiduo a sus diversas rutas.



Otro aspecto de interés, es que tal vez sea una de las mejores formas de conocer España, pues a pie, en bicicleta o a caballo (que son las tres formas de peregrinación que acepta el otorgamiento de la "**Compostela**"), se puede recorrer prácticamente toda la geografía de este País, contando con la señalización necesaria para no perderse, con las mejores rutas de la historia de la península, el apoyo de muchos organismos, personas, albergues, generalmente siendo muy bien recibido y apoyado por toda la gente que lo reconoce con la característica mochila, concha de peregrino "**Viera**" o "**venera**", y sobre todo con esa cara especial entre agotado y feliz.



Si está en tus manos: **no dejes pasar la oportunidad de hacerlo**.

Y de verdad, si en algo puedo serte de utilidad en tu peregrinaje, cuenta conmigo:

acorletti@darfe.es

Campus stellae, "campo de estrellas", Compostelle o Compostella (también se asocia a: composita tella, "tierras hermosas").

Volver al índice

www.darFe.es

Charla 41

El nivel de Red - Presentación

Enlace al Video:

Resumen:

En este capítulo iniciamos con el **nivel de red**, o nivel tres del modelo **TCP/IP.**

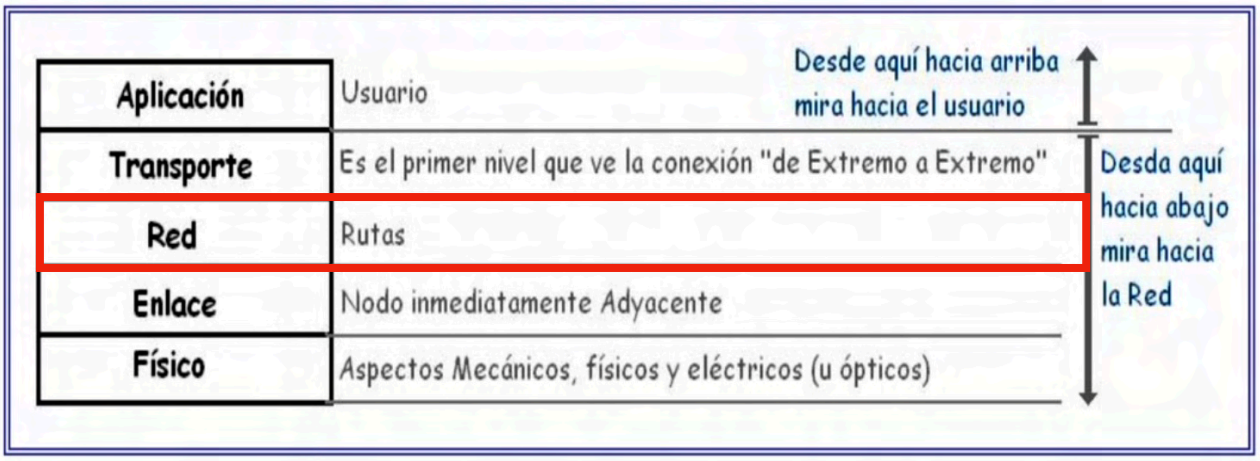
Para llegan a entender las dos grandes tecnologías que se emplean hoy a nivel mundial: red de conmutación de circuitos y red de conmutación de paquetes, haremos una introducción de este nivel describiendo sus tecnologías y dispositivos, con una breve historia de cómo hemos llegado al día de hoy.

Descripción detallada

Comenzamos con el **nivel de red**, o nivel 3 del modelo **TCP/IP**.

Inicialmente desarrollaremos bastante teoría del tema, basado en el capítulo 1 del libro "**Seguridad en Redes**", que como ya sabéis, se puede descargar gratuitamente de nuestra Web: **www.darfe.es**

Como ya hemos mencionado en la presentación del modelo de capas, el nivel de red es el encargado de gestionar las rutas por las que viajará nuestra información

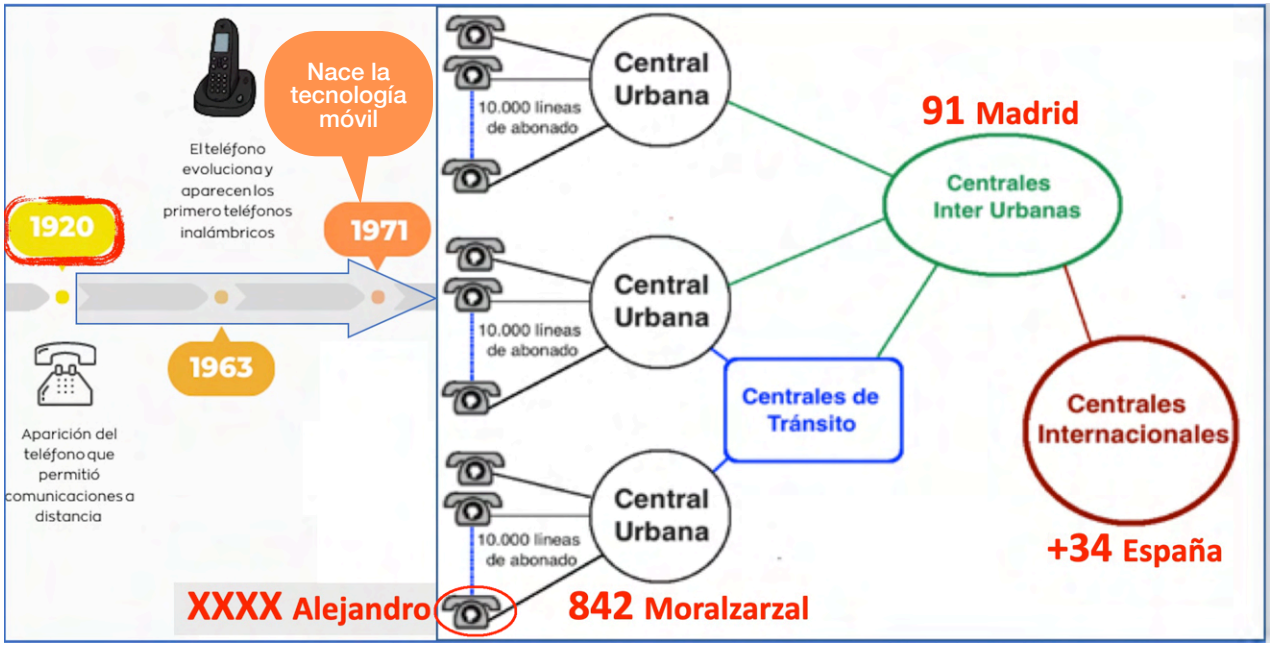


1. La red de telefonía fija

El comienzo de esta historia de las telecomunicaciones está en la red de telefonía fija, y en virtud de su antigüedad, es casi una norma en toda operadora de telecomunicaciones la "Omnipresencia" de elementos y ubicaciones de red heredadas que, con la evolución vertiginosa actual, presentan gran parte de los problemas de seguridad que iremos viendo a lo largo de este texto.

¿Cómo nace esta red?

La red de telefonía conmutada (**RTC**), o también llamada "Public Switching Telephone Network" (**PSTN**), comienza a principios del siglo XX, cerca de los años 20'. Pueden discutirse las fechas exactas y los países, pero a efectos de este texto consideraremos el despliegue domiciliario a nivel internacional con presencia en gran parte del mundo a principios/mediados de ese siglo. Nace como red analógica únicamente para voz, en la cual se comenzaban a interconectar zonas geográficas con una arquitectura estrictamente jerárquica. Esta arquitectura, nacía en las centrales urbanas (**CU**) desde la que partían los 10.000 "pares de abonado". Es decir, diez mil pares de cobre trenzados hacia cada uno de los domicilios de los clientes (abonados). Estas centrales urbanas se conectaban a centrales de tránsito, cuya misión era o sigue siendo, optimizar los enlaces y ofrecer cierta redundancia de caminos. El nivel siguiente en esta jerarquía eran/son, las centrales Inter urbanas, que unen estados, provincias o regiones y por último las centrales internacionales, que son las puertas de entrada de cada país. Podemos ver este detalle en la imagen que se presenta a continuación.

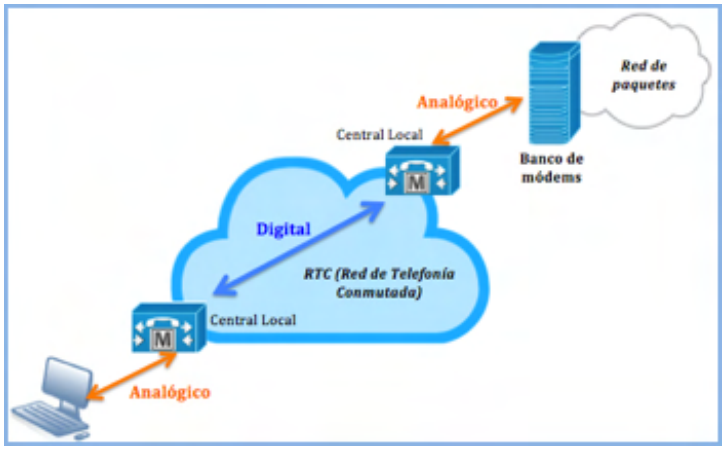


Se destaca en **rojo,** el ejemplo de España, donde podemos ver que su central internacional, se identifica con el prefijo **+34**, dentro de ella, por ejemplo Madrid, se identifica con el prefijo **91**, y dentro de la Comunidad de Madrid, cada área, pueblo o zona, tendrá su propio número de Central urbana. En la imagen, se aprecia la central urbana del pueblo de Moralzarzal, que es la **842** (en realidad en este pueblo existen dos centrales urbanas, las 842 y la 857). Por último, como de ella nacen 10.000 pares de cobre, que en la actualidad son en realidad fibras ópticas, cada uno de los abonados de esa central urbana se identifican con los cuatro últimos dígitos concretos de cada línea fija. En la imagen, se aprecia con un círculo rojo, el de Alejandro, que es **XXXX** (pues no está muy por la labor de que lo llaméis desde todo el mundo y a cualquier hora).

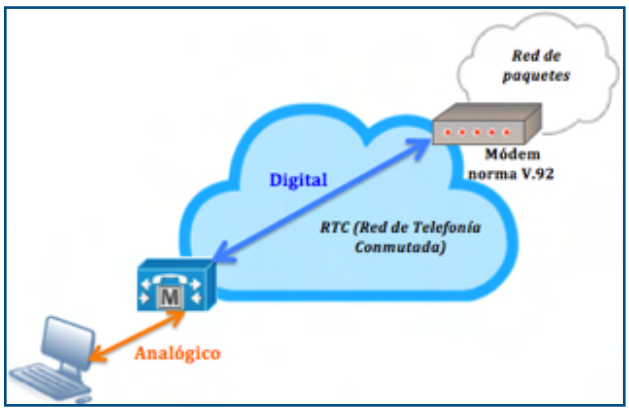
Esta red que nació siendo analógica, poco a poco se fue digitalizando.

Recordad la Charla 06: **Digitalización**.

Inicialmente, se digitalizaron sus troncales, como vemos en la imagen de la derecha.



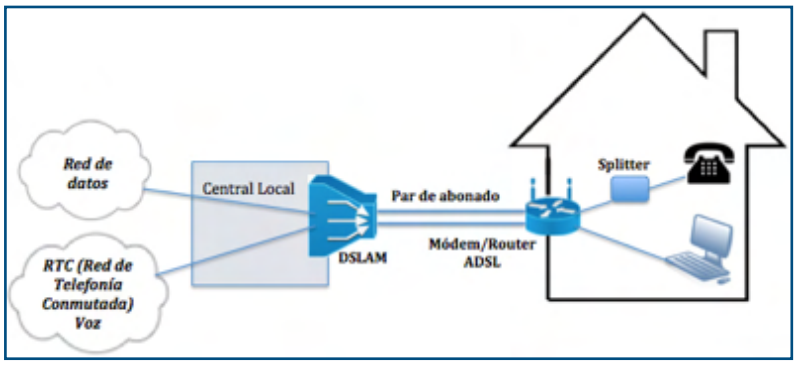
Más adelante apareció la necesidad de poder conectar ordenadores a estas troncales digitales. En general, este requerimiento surge de las universidades y centros de investigación. Para ello, se debía de alguna forma poder convertir esta señal digital nativa que hablaban estos dispositivos (ordenadores) a una señal analógica que era lo que funcionaba en la red, y así nacen los primeros "**modem**" (**mod**ulador-**dem**odulador).



En muy poco tiempo comienzan a implantarse en determinados extremos, las primeras redes de conmutación de paquetes (universitarias, investigación, militares), con ello se gana muchísimo en la relación señal ruido y se evita una segunda conversión analógica digital, la norma **V.92** fue su máximo exponente superando los 64 kbps.

Aparece la tecnología **RDSI** (Red Digital de Servicios Integrados) que rápidamente es superada por **xDSL** (x Digital Subscriber Line), sobre la que nos detendremos aquí.

Estos servicios xDSL se basan, sobre todo, en nuevas formas de modulación (combinando sobre todo fase y amplitud) a través de "constelaciones" de bits, basados en la capacidad de varias portadoras asociadas a la relación señal ruido de esta "**última milla**" que hemos mencionado anteriormente (par de cobre o par de abonado); por esta razón es que xDSL es muy dependiente de la distancia y la calidad del par de cobre que llega hasta el domicilio, cuanto mejor sea la relación señal/ruido, mayor cantidad de bits podrá transmitirse por ese par de cobre y, por lo tanto, mayor ancho de banda se podrá ofrecer.

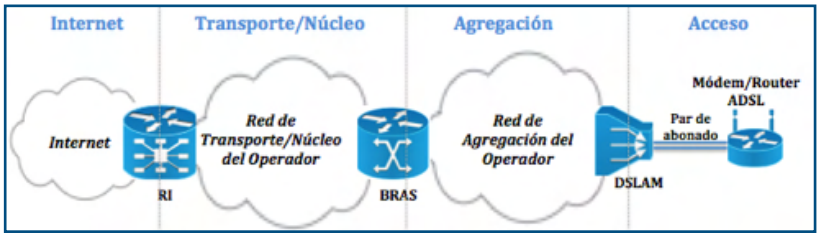


Estas tecnologías xDSL son una familia (HDSL, VDSL, ADSL, etc.), de ellas, la que más empleo se hace en las redes de Telefonía a nivel domiciliario (hogar), es **ADSL** (asynchronous DSL). El concepto de "asíncrono o asimétrico" viene dado en virtud de emplearse dos canales para datos de diferente velocidad (subida y bajada), y un tercero más, independiente para la voz. De los dos canales de datos uno se emplea para bajada de información que suele ser de mayor capacidad y otro para subida de información que suele ser sensiblemente menor. Las especificaciones técnicas de esta tecnología se encuentran en la recomendación **G.992.1** (G.dmt) y **G992.2** (G.lite) de la **ITU-T** y en el estándar **T1.413-1998** de la **ANSI**.

En la imagen anterior, hemos hecho especial hincapié en describir el dispositivo del lado cliente como "**Modem/Router ADSL**", esto se debe a que en realidad estos dispositivos cubren una doble función, por un lado realizan toda la labor de modulación y demodulación específica de cada extremo de ese par de cobre (modem), y por otro lado también trabajan a nivel tres del modelo de capas, es decir, desempeñan actividades de "**Routing**" (router) gestionando y enrutando direcciones y encabezados del protocolo IP del lado **LAN** (dentro del domicilio) y del lado **WAN** (hacia la central telefónica a través del par de cobre). Cabe mencionar que en la jerga telefónica la "acometida" en cada hogar, es decir, el punto de entrada de cada domicilio (o edificio) se denomina **PTR** (Punto Terminal de Red) pues es allí donde se encuentra el eslabón final de cualquier operador.

Como es natural, desde el lado de la central, no se pueden colocar 10.000 modem diferentes, sino que se diseña un nuevo hardware que centraliza esas líneas y así nace el **DSLAM** (Digital Subscriber Line Access Multiplexer (Multiplexor de línea de acceso de abonado digital).

A continuación se presenta una visión más amplia de los componentes fundamentales de toda esta red que permite la navegación por Internet a cualquier abonado que tenga ADSL en su domicilio. En la misma solamente se aprecian los elementos base de esta arquitectura pero, como es de suponer, en cada "nube" del esquema se encuentra una cadena/jerarquía de dispositivos que permiten al interconexión y el routing de cada paquete que circula por ella, como así también una serie de dispositivos y plataformas que forman parte de los procesos de facturación, autenticación, monitorización, supervisión, etc.



En la imagen anterior, podemos ver también otro dispositivo que es el **BRAS** (Broadband Remote Access Server) este es un elemento de agregación de dos o más DSLAM hacia la red IP de la operadora telefónica. Este dispositivo no deja de ser un router más, sobre el cual se pueden configurar determinados parámetros de administración de banda ancha y protocolo IP. En la actualidad, con la difusión y reducción de precio de la fibra óptica (**FO**), en las nuevas instalaciones, se está llegando hasta el domicilio del cliente con la misma, se denomina **FTTH** (Fiber To The Home), siempre y cuando hasta ese barrio ya existe FO (denominado **FTTN**: Fiber To The Neighborhood). Es importante tener en cuenta que la relación que existe entre la red fija y la móvil se está haciendo cada vez más competitiva, pues hoy en día, con 4G y 5G, se está ofreciendo velocidades por aire de la misma magnitud que las de cable de cobre (cuestión inimaginable hace una década). A esta realidad se suma la aparición de teleoperadoras locales y operadores móviles virtuales que lanzan al mercado planes muy tentadores. Para mantener a sus clientes, las empresas que poseen un alto número accesos a la red fija, en las zonas donde su cableado es antiguo o en nuevos barrios, están desplegando fibra óptica de forma masiva. A través de la misma se pueden alcanzar velocidades que dejan fuera de competencia a cualquier otro medio o tecnología. Con ello, una vez acometido todo un barrio, es muy poco probable que estos abonados desistan de su uso en virtud, justamente, de todos los servicios de calidad que le llegarán a su hogar: Voz, datos y video de alta definición.

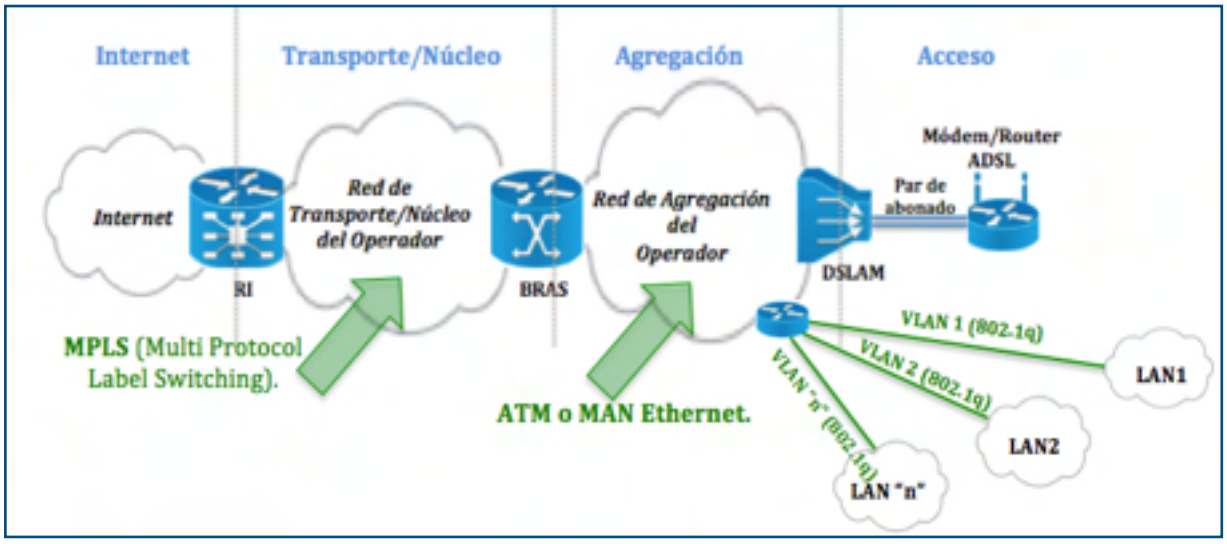
Si se logra llegar con la FO hasta el domicilio del cliente toda la infraestructura es más eficiente, esto impacta también en una reducción de costes para la operadora.

Como hemos mencionado el problema del par de cobre es el denominado "última milla" pues se trata justamente del promedio de las distancias de acometida domiciliaria, es decir los tramos de pares de cobre que van desde la última central hasta los domicilio, oscila en "una milla" (1,6 u 1,8 km dependiendo si es milla náutica o terrestre).

En el caso de las fibras ópticas, estas distancias medias son de diez kilómetros, por lo tanto donde antes debía colocar unas 20 o 30 centrales telefónicas, esto mismo se logra con una sola central de fibra óptica, también otra razón de máxima importancia es que los tendidos de cobre son "auto-alimentados" pues a través del par de abonado viaja también tensión eléctrica que alimenta los teléfonos, este abastecimiento de tensión hace que en cada central se necesite instalar una infraestructura de alimentación importante: Redundancia de acometida, sistemas de cableado

adicionales, Power Bank (Baterías), grupos electrógenos, reguladores, transformadores, combustible, etc. Todo esto es innecesario en fibra óptica.

Estos avances de calidad del medio, sumado a la digitalización masiva de la red fija, comienza a permitir que se acceda a la misma con diferentes tecnologías, cada vez más eficientes y de mayor velocidad. Las empresas y organizaciones, ingresan a esta red, directamente desde sus redes de área local, como podemos ver en la imagen que sigue.



Esta capacidad, en realidad se comienza a reflejar en un cambio muy importante de esta red, pues se migra de la vieja red de "**conmutación de circuitos**" hacia las nuevas redes que emplean la "**conmutación de paquetes**".

2. La red de conmutación de circuitos y la red de conmutación de paquetes

La red de telefonía conmutada (**RTC**) que venimos presentando desde el principio de este capítulo, nace como una red de "conmutación de circuitos". Es decir, en el momento que se levanta el teléfono, y vamos marcando, se va "**estableciendo**" la comunicación desde nuestra centra urbana, pasando por las de tránsito, interurbanas, si sale del país por nuestra central internacional, y esta lo encaminará hacia su homóloga internacional, que realizará el mismo recorrido hasta llegar a la central urbana destino, la que sacará la comunicación por uno de sus diez mil pares (o fibras ópticas) hasta llegar al domicilio físico que acabo de marcar. Este paso es el establecimiento de la comunicación, con el que se reservó un circuito completo que no se modificará hasta que se cuelguen ambos teléfonos.

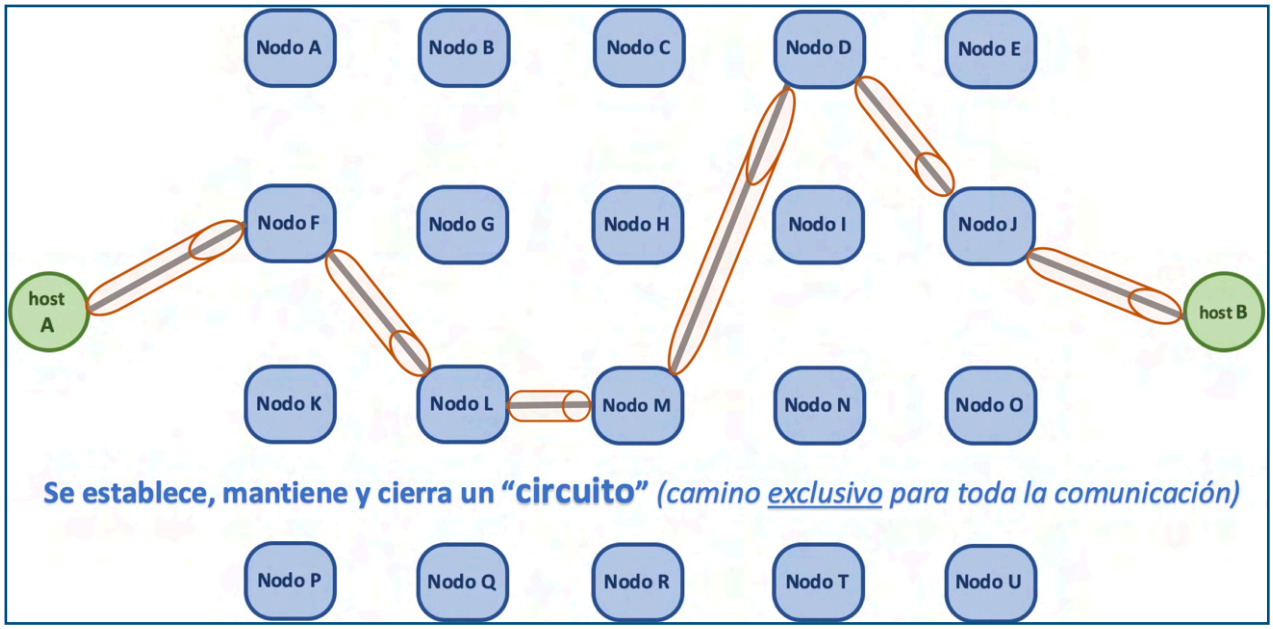
Una vez que el destinatario, levanta (atiende) su teléfono, se pasa al "**mantenimiento**" de la comunicación, que aunque para ambos usuarios sea transparente, tiene por detrás una importante carga de trabajo. Finalmente cuando ambos cortan la comunicación se genera el "**cierre**" de la misma, y el circuito queda liberado para cualquier otro uso futuro.

En resumen, una red de conmutación de circuitos siempre tiene tres pasos:

- Establecimiento

- Mantenimiento
- Cierre de la comunicación

En la imagen siguiente podemos ver representado el esquema de una red de conmutación de circuitos. En esta imagen, cada una de las centrales intervinieres se denominan "nodos" para simplificar la gráfica.



Como mencionamos anteriormente, esta red, a medida que la digitalización avanza, se va transformando en una red de conmutación de paquetes, pues la característica fundamental de la digitalización, es que esos unos y ceros, pueden ser organizados sin la necesidad de viajar exclusivamente por el mismo camino.

De hecho esta fue una de las mayores razones que dio origen a estas redes. Durante los años de la guerra fría entre EEUU y la URSS, el primero de ellos, comenzó a implementar una red que pudiera soportar cualquier tipo de ataque nuclear, mediante la redundancia de enlaces. A través de esta red, si uno de los nodos quedaba indisponible (fuera de combate), la red inmediatamente cambiaba las rutas y la información podía seguir circulando por ella.

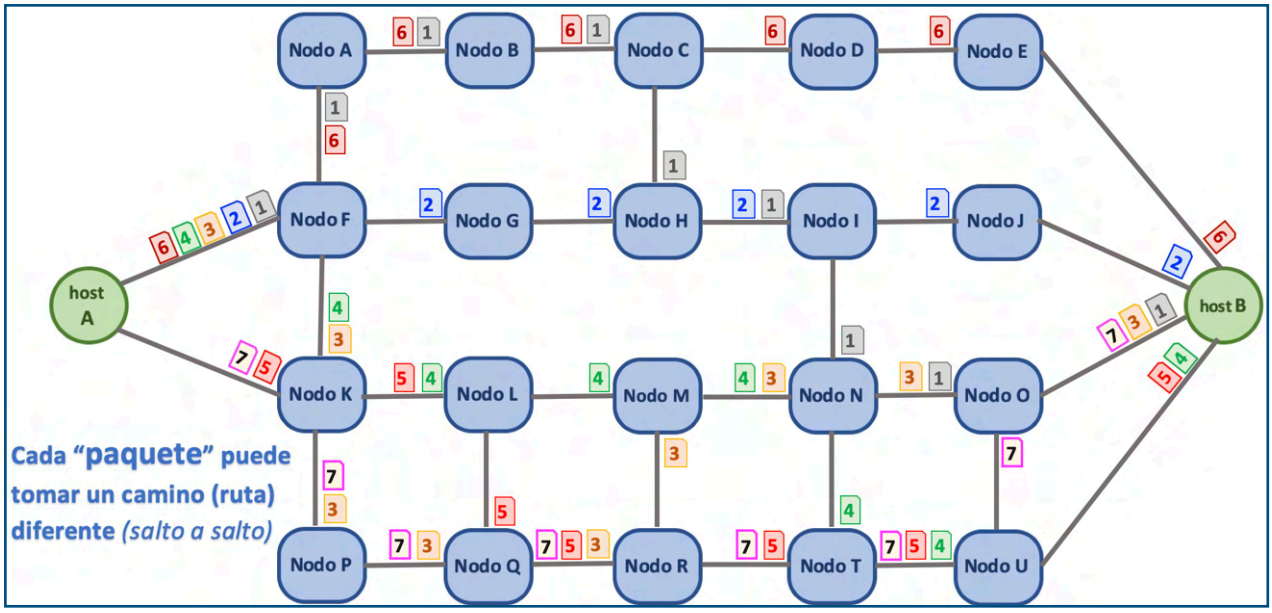
Esta red fue el origen e Internet y se llamo **ARPANET** (Advanced Research Projects Agency Network) o Red de Agencias de Proyectos de Investigación Avanzada.

Inicialmente fue solo para uso militar, pero pocos años después, se hizo claro su crecimiento a nivel universitario sobre todo, y se dividió en: "**Milnet**" e "**Internet**".

Así nació, sobre la base de la red telefónica conmutada, esta gran red mundial, que hoy en día, sigue sustentándose en la red de telefonía, pero ya no de "circuitos", pues ahora está soportada por una nueva clase de nodos, que si bien se relacionan directamente con las centrales (urbanas, interurbanas e internacionales), estos nuevos nodos enrutan paquetes de datos, y poseen varias "**rutas**", algunas principales y otras secundarias, con plena capacidad para "conmutar paquetes", que hoy en día son casi exclusivamente bajo el protocolo "**IP**" (Internet Protocolo).

En esta red de paquetes, cada nodo analiza paquete a paquete, lo que más adelante desarrollaremos como el encabezado del protocolo IP, y sobre la base de la información

de la dirección destino de cada paquete, decide por que camino lo va a enviar al siguiente nodo, y no necesariamente una misma comunicación viajará por la misma ruta, pues puede suceder, y de hecho sucede con muchísima frecuencia, que desde un origen hacia un destino, y viceversa, los paquetes vayan cambiando de ruta en varias oportunidades.



En concreto entonces, una red de conmutación de paquetes, es aquella en la que cada nodo, paquete a paquete, va tomando la decisión del camino seguir, tal cual podemos ver en la imagen que sigue.

Finalizamos el capítulo de hoy con estas dos grandes redes, pues sobre las mismas iremos avanzando, paso a paso, en los capítulos siguientes.

Volver al índice

www.darFe.es

Charla 42

La gran red mundial

Enlace al Video:

Resumen:

En esta charla, desarrollaremos cómo son las entrañas de esta gran red mundial, como se clasifican los diferentes niveles o "**Tier**" de esta verdadera jerarquía. Qué tipo de direccionamiento y protocolos emplea.

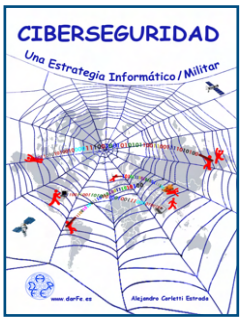
Presentaremos también el gran pilar que la sustenta, que son los cables submarinos de fibra óptica, y por último, sus enlaces secundarios por medio de satélites.

Descripción detallada

Ya hemos presentado la red de conmutación de paquetes, y como la misma conforma hoy el núcleo de las telecomunicaciones mundiales que interconectan todo el planeta.

La charla de hoy, está basada en el capítulo 8 del libro "**Ciberseguridad, una estrategia Informático/Militar**", que como siempre podéis descargar gratuitamente de nuestra Web:

www. darFe.es



Si comenzamos a analizar esta red de forma jerárquica desde arriba hacia abajo, lo primero que nos encontramos son los grandes "**Carriers**" del mundo, es decir los que interconectan continentes y países de forma bastante piramidal. Existen tres niveles de ellos, conocidos como **Tier 1**, **Tier 2** y **Tier 3**.

Profundicemos un poco sobre estos niveles superiores de Internet que son los que transportan los grandes volúmenes de datos y su ancho de banda son inimaginables. El conocimiento de sus entrañas es lo que posiciona a cualquier atacante en un nivel superior en cuanto a volúmenes de tráfico y conectividad de extremo a extremo, por lo tanto, si lo que deseamos desde el punto de vista de "Ciberdefensa" es poder adoptar medidas contra estas acciones delictivas, necesitamos también conocer en detalle el fondo de esta red.

Como cualquier sistema de entrega y recepción, es necesario basarse en algún tipo de "**Direccionamiento**", el cual para el caso de Internet es el protocolo **IP**, en la actualidad sigue siendo la versión 4 del mismo la más difundida. Aunque ya está desplegándose en muchos segmentos la versión 6 que está instalada y funcionando en gran parte de esta arquitectura mundial, aún no podemos pensarla como que está en "producción" al 100%.

Todo este esquema de direccionamiento IP se encuentra asignado y regulado a lo largo de nuestro planeta por **IANA** (Internet Assigned Numbers Authority).

REGISTRY	AREA COVERED
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	Canada, USA, and some Caribbean Islands
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

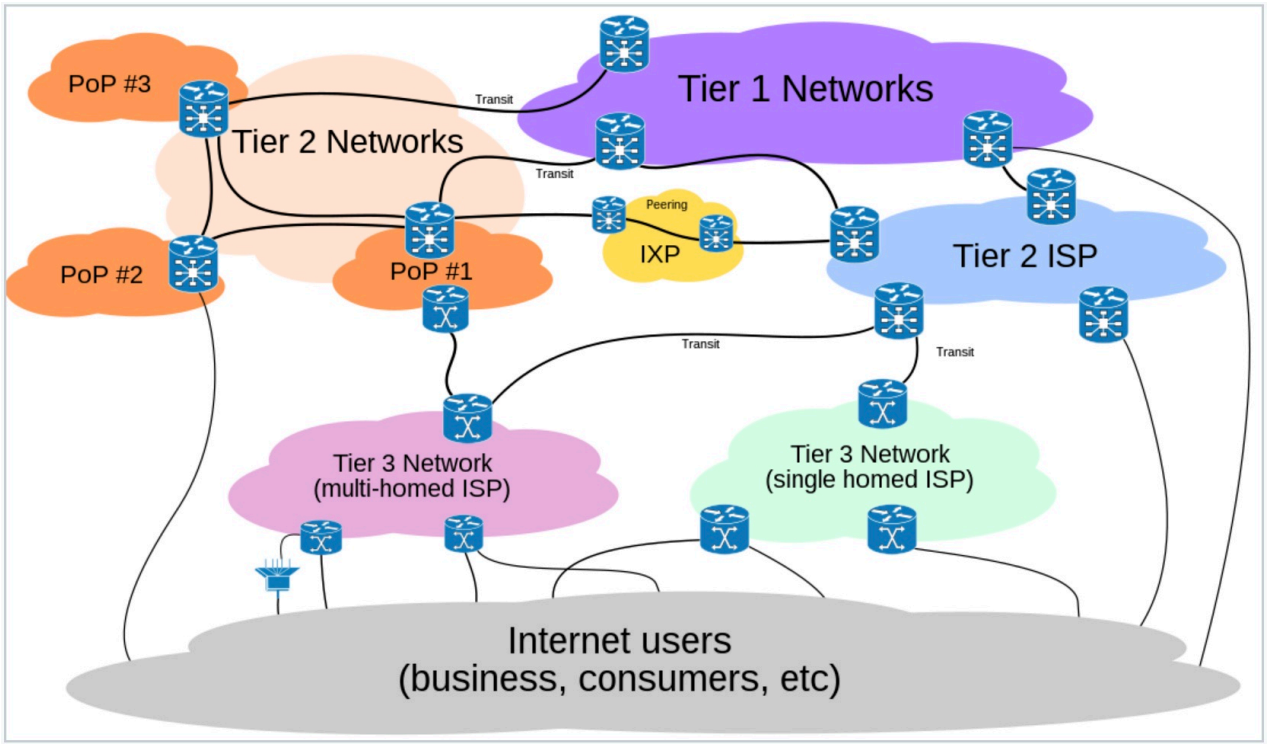
IANA tiene delegado sus rangos de asignación IP por regiones geográficas, tal cual podemos ver en la imagen anterior.

Estas regiones son denominadas **RIR** (Regional Internet Registry).

Otra de las responsabilidades de asignación de IANA es la que respecta a los Sistemas Autónomos (**AS**: Autonomous Systems), los cuáles se tratan de conjuntos de redes IP y routers que se encuentran bajo el control de una misma entidad (en ocasiones varias) y que poseen una política de encaminamiento similar a Internet.

El concepto de Sistema Autónomo es fundamental para el control de Internet, pues los grandes routers de esta red, sólo conocen de AS y van enrutando con este esquema de direccionamiento (no a través de la dirección IP). En la imagen de la derecha, podemos ver algunos de estos sistemas autónomos.

Los grandes puntos de interconexión que tratamos en los párrafos anteriores, son gobernados por lo que podemos llamar "**carriers**". Se trata de grandes corporaciones, que unen el corazón de esta gran red. Estos Carrier son los que se catalogan como "Tier", tal cual mencionamos al principio.



Los **Tier 1** son los grandes operadores globales que tienen tendidos de fibra óptica al menos a nivel continental. Desde la red de un Tier 1 se accede a cualquier punto de Internet, pues todas las redes de Tier 1 deben estar conectadas entre sí. Son backbone, core, núcleo ó troncal de Internet.

Si bien se puede llegar a discutir la frontera entre algún Tier 1 específico, los que podemos considerar sin lugar a dudas como Tier 1, al menos, son los que presentamos en la tabla de la derecha.

Nº	Nº AS	Organización	Cant. ASs
1	3356	Level 3 Parent, LLC	49212
2	1299	Arelion	41512
3	174	Cogent Communications	36870
4	6939	Hurricane Electric LLC	23822
5	6762	Telecom Italia Sparkle S.p.A.	21151
6	2914	NTT America, Inc.	19815
7	3257	GTT Communications Inc.	18336
8	6461	Zayo Bandwidth	17522
9	6453	TATA COMMUNICATIONS INC	16785
10	3491	PCCW Global, Inc.	11409
11	9002	RETN Limited	8260
12	1273	Vodafone Group PLC	7553
13	5511	Orange S.A.	6932
14	4637	Telstra International Limited	6542
15	12956	TELEFONICA GLOBAL SOLUTIONS	5263

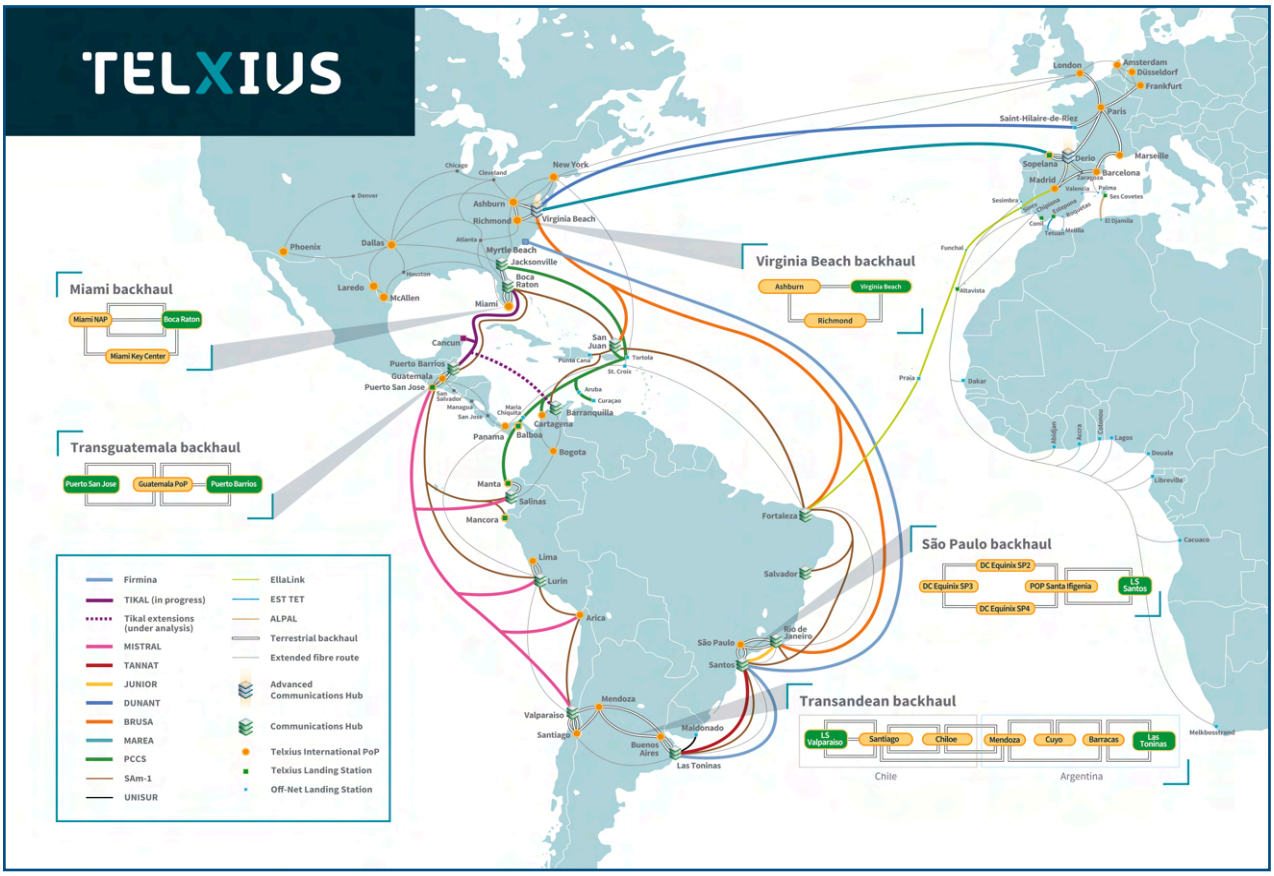
Independientemente de su magnitud, también deben reunir algunas características como son:

- Deben tener acceso a las tablas completas de routing a través de las relaciones que poseen con sus peering (otros Tiers).
- Deben ser propietarios de fibras ópticas transoceánicas y enlaces internacionales.
- Deben poseer redundancia de rutas.

El dato más representativo y actualizado del peso y actividad de cada uno de ellos se puede obtener a través de **CAIDA** (Center for Applied Internet Data Analysis) en:

http://as-rank.caida.org

Un ejemplo cercano de Tier 1 lo tenemos con **Telefónica**, a través de su empresa **TELXIUS** (o **Telefónica Global Solutions** que es el quien la opera), desde su página Web podemos apreciar el mapa que se presenta a continuación donde se presentan todos los vínculos físicos que es propietario este Tier 1.



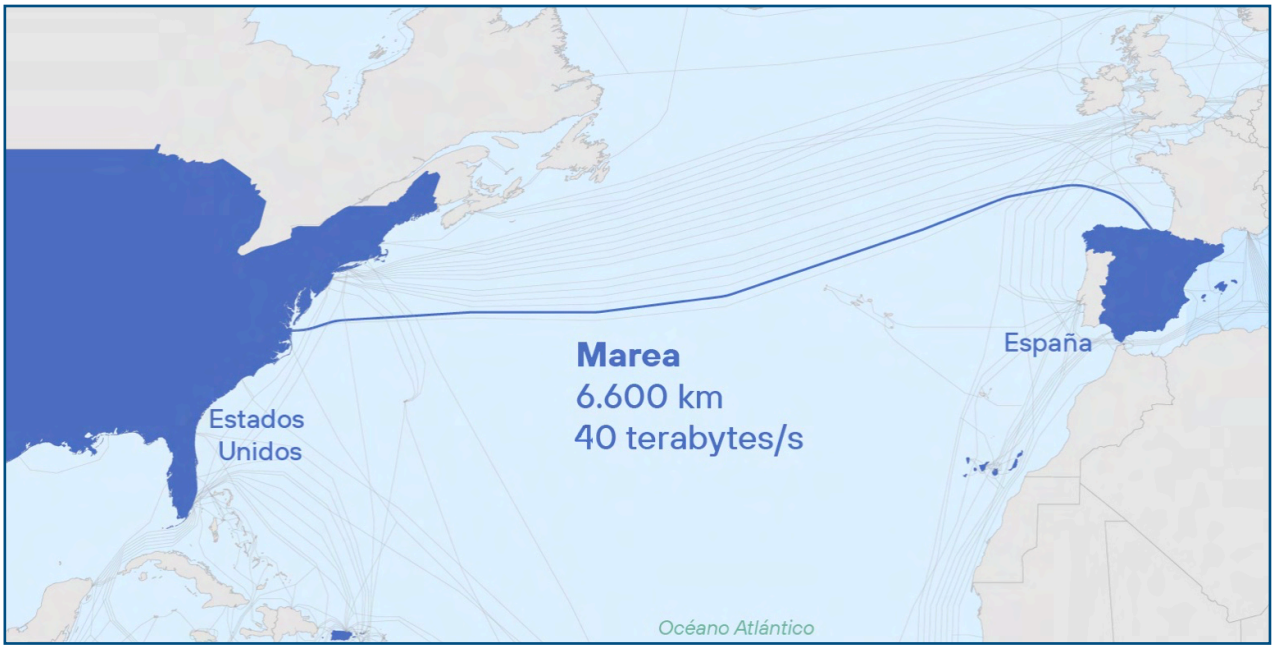
Red Internacional del Grupo Telefónica

(Imagen tomada de la web: https://telxius.com/network/Telxius_map.pdf)

Un video interesante que hemos publicado y os recomendamos que miéis por su interés histórico, es:

"**Primer Cable submarino intercontinental de telefonía**."

Otro dato histórico, al menos para nosotros, es el cable submarino "**Marea**" que se instaló en 2020 y que une EEUU con Europa. Se trata de un cable que posee únicamente 8 hilos de fibra óptica, y que es propiedad de tres grandes empresas mundiales. Lo que nos ha llamado la atención del mismo, es que tiene una velocidad de 40 Tbps (terabits por segundo). Allá por los años 90, en las facultades de informática o telecomunicaciones, para poder llegar a dimensionar, o que en nuestra mente cupiera lo que era un "terabit", es decir: 1.000.000.000.000 de bits, se hacía referencia a que en una sola unidad, es decir "**1T**", cabría la totalidad de los libros de una biblioteca nacional digitalizados en texto plano. Por esta razón queríamos poner de manifiesto "Marea", pues mueve 40 bibliotecas nacionales… en un segundo (guauuu…).



Las diferentes operadoras de telefonía e Internet de cada país, enrutan su tráfico de clientes hacia el resto del mundo a través de estos carriers. Para esta tarea tenemos básicamente dos escenarios:

- Interconexión con su "Carrier" (Salida Internacional): En este caso se trata de routers del ISP, que físicamente están conectados a routers de un "Tier 1 o Tier2" y entregan su tráfico para que ellos lo enruten a través de Internet. Este tipo de enlaces suelen ser redundantes y en general hacia al menos dos Carriers diferentes para garantizar su disponibilidad.
- Punto de Intercambio (**IXP**: Internet eXchange Point) o también denominado o Punto Neutro: Se debe considerar que el tráfico de Internet, tiene un alto porcentaje que se mantiene dentro de las fronteras de cada país (consultas a Web nacionales, correos locales, etc..), este tipo de tráfico no tiene sentido que sea enrutado fuera de estas fronteras pues sobrecargaría las troncales de la red. Para estos casos en muchos países (no todos) se han creado estos IXP, que en definitiva son salas con "**Racks**" de comunicaciones (básicamente switchs de alta capacidad) donde se interconectan los grandes carriers de ese país. Al organizarse las rutas **BGP**, es natural que este tipo de enlaces ofrezcan mayor ancho de banda que si siguieran otros caminos, por lo tanto, a la hora de generarse las tablas de ruteo, el "peso" que tienen estos caminos

supera cualquier otro, debido a ello se generan rutas locales preferenciales que encaminan el tráfico nacional, sin la necesidad de salir de ese país.

El propósito principal de un punto neutro es permitir que las redes se interconecten directamente, a través de la infraestructura, en lugar de hacerlo a través de una o más redes de terceros. Las ventajas de la interconexión directa son numerosas, pero las razones principales son el coste, la latencia y el ancho de banda.

El tráfico que pasa a través de la infraestructura no suele ser facturado por cualquiera de las partes, a diferencia del tráfico hacia el proveedor de conectividad de un Internet Service Provider (**ISP**).

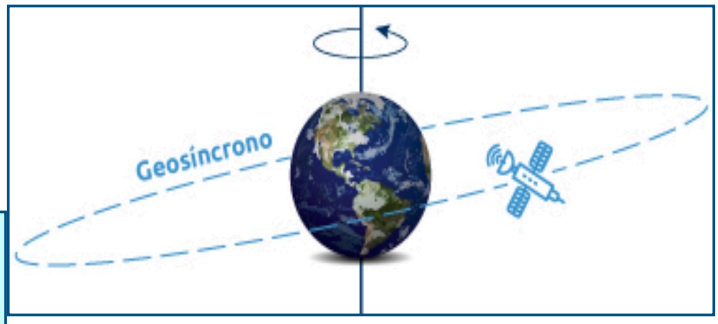
La técnica y la logística de negocios de intercambio de tráfico entre los Internet Service Provider se rige por los acuerdos de interconexión mutua (peering). En virtud de dichos acuerdos, el tráfico a menudo se intercambia sin compensación. Cuando un punto neutro incurre en costos de operación, por lo general éstos son compartidos entre todos sus participantes.

Comunicaciones satelitales

Otro tipo de medios que interconectan todo el planeta son los satélites.

La comunicación satelital, se conforma por sistemas de comunicaciones que emplean uno o más satélites para reflejar las ondas electromagnéticas generadas por una estación transmisora con el objeto de hacerla llegar a otra estación receptora. Generalmente ambas están situadas en puntos geográficamente distantes, sin alcance visual.

Los satélites empleados en telecomunicaciones intercontinentales son los llamados **geoestacionarios** o **geosíncronos**, es decir que se encuentran situados



en un punto fijo respeto a la Tierra, pero en la actualidad se están empleando también otros tipos de órbitas para telecomunicaciones, en especial las de baja altura para evitar las enormes distancias que actualmente recorren las señales.

Los satélites se clasifican en:

- **LEO** (Low Earth Orbit): Poseen órbitas elípticas que oscilan entre los 400 y 2.500 km de altura.
- **MEO** (Medium Earth Orbit): Poseen órbitas elípticas que oscilan entre los 4.000 y los 15.000 km de altura.

- **GEO** (Geostationary Earth Orbit): Poseen órbitas circulares que giran en un punto fijo respecto a la Tierra, se encuentran a 36.000 km de altura.

Un satélite posee dos antenas, una receptora (Uplink) que recibe la información de la Tierra y una transmisora (Downlink) que refleja la señal cambiada de frecuencia par no interferirse mutuamente.

Según su uso pueden ser de cobertura global, hemisférica o direccional (spot).

Los **transponder** son los sistemas encargados de recibir la señal, cambiar la frecuencia, amplificarla y retransmitirla (también suelen incluir funciones de multiplexado/ demultiplexado); cada transponder abarca un número fijo de canales. Los transponder manejan varios anchos de banda, siendo los más usuales 36, 70 y 140 MHz. El número de transponder varía según el tipo de satélite.

En la actualidad, para las conexiones de voz y datos, se están empleando las transmisiones satelitales como un medio secundario. Los medios prioritarios o primarios son las fibras ópticas, pues si comparamos sus distancias son muy inferiores. Debemos considerar que una comunicación GEO, sobre 36.000 km y baja la misma distancia, con lo que si lo sumamos, esta señal viaja 72.000 km. Si redocrdamos que la velocidad de la luz en el vacío es 300.000 km/s (cosa que en la realidad no es así, pues no hay vacío absoluto), en 72.000 km ha demorado al menos 250ms, si a esto le sumamos la latencia que imponen los dispositivos electrónicos por los que pasa, estamos llegando a los 400ms de demora, o más. La transmisión telefónica, tiene justamente este límite de tolerancia (400ms) pues a partir de este tiempo, una comunicación de voz, se entrecorta y se hace muy incómoda para el diálogo.

El Protocolo BGP

Siguiendo con la secuencia de estos párrafos, corresponde ahora ampliar un poco más el tema de Sistemas Autónomos. Siguiendo con más detalle los conceptos anteriores, un sistema autónomo se define como “un grupo de redes IP que poseen una política de rutas propia e independiente”. Esta definición hace referencia a la característica fundamental de un Sistema Autónomo: realiza su propia gestión del tráfico que fluye entre él y los restantes Sistemas Autónomos que forman Internet.

Hasta el año 2007 los números de sistemas autónomos estaban definidos por un número entero de 16 bits lo que permitía un número máximo de 65536 asignaciones de sistemas autónomos. Debido a la demanda, se hizo necesario aumentar la posibilidad La **RFC 4893** introduce los sistemas autónomos de 32 bits, que IANA ha comenzado a asignar. Estos números de 32 bits se escriben como un par de enteros en el formato x.y, donde x e y son números de 16 bits. La representación textual de Números de sistemas autónomos está definido en la **RFC 5396**.

Los números de Sistemas Autónomos son asignados en bloques por la Internet Assigned Numbers Authority (**IANA**) a Registros Regionales de Internet (**RIRs**).

Los números de sistemas autónomos asignados por IANA pueden se encontrados en el sitio web de IANA: **http://iana.org**

El protocolo **BGP** (Border Gateway Protocol), es el responsable de enrutar todos los paquetes de Internet a lo largo del mundo. Este protocolo responde a un esquema de direccionamiento dinámico, es decir que sus rutas se van modificando frecuentemente sobre la base de diferentes métricas, que en definitiva son parámetros lógicos que

permiten decidir por cuál interfaz debe sacar un determinado router cada uno de los paquetes que le llegan a él. Estas rutas se van creando sobre la base de la información que comparten los dispositivos vecinos (**neighbor**) que conforman esa comunidad BGP. A continuación, presentamos una imagen que representa este funcionamiento.

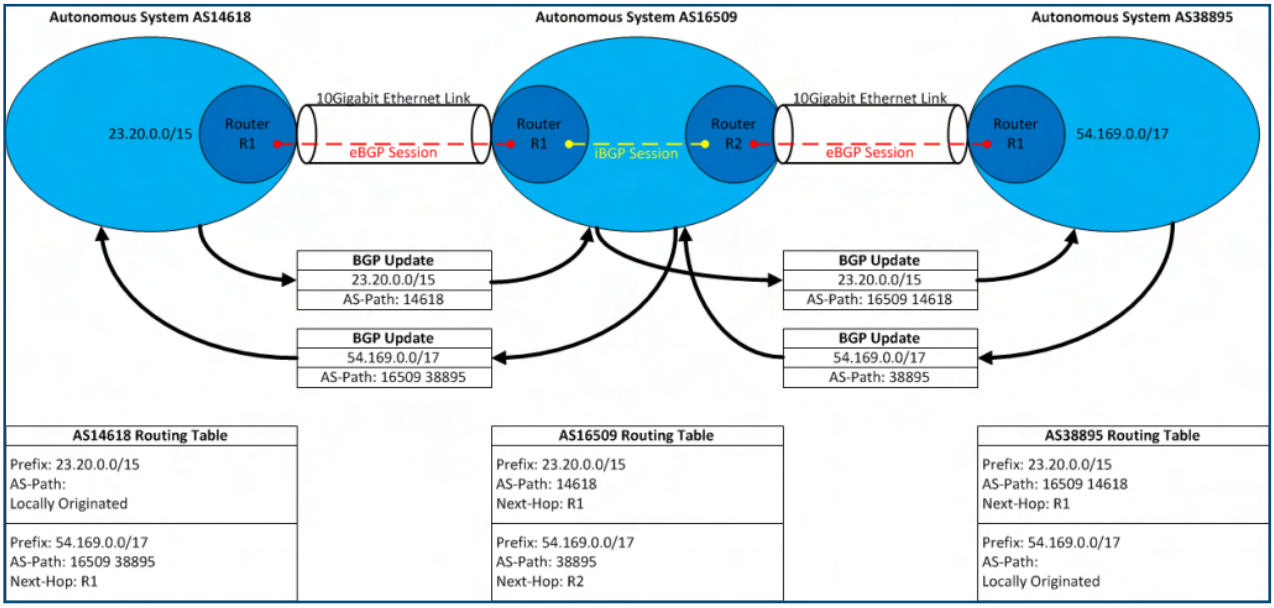


Imagen tomada de: https://www.awsarchitectureblog.com/2014/12/internet-routing.html

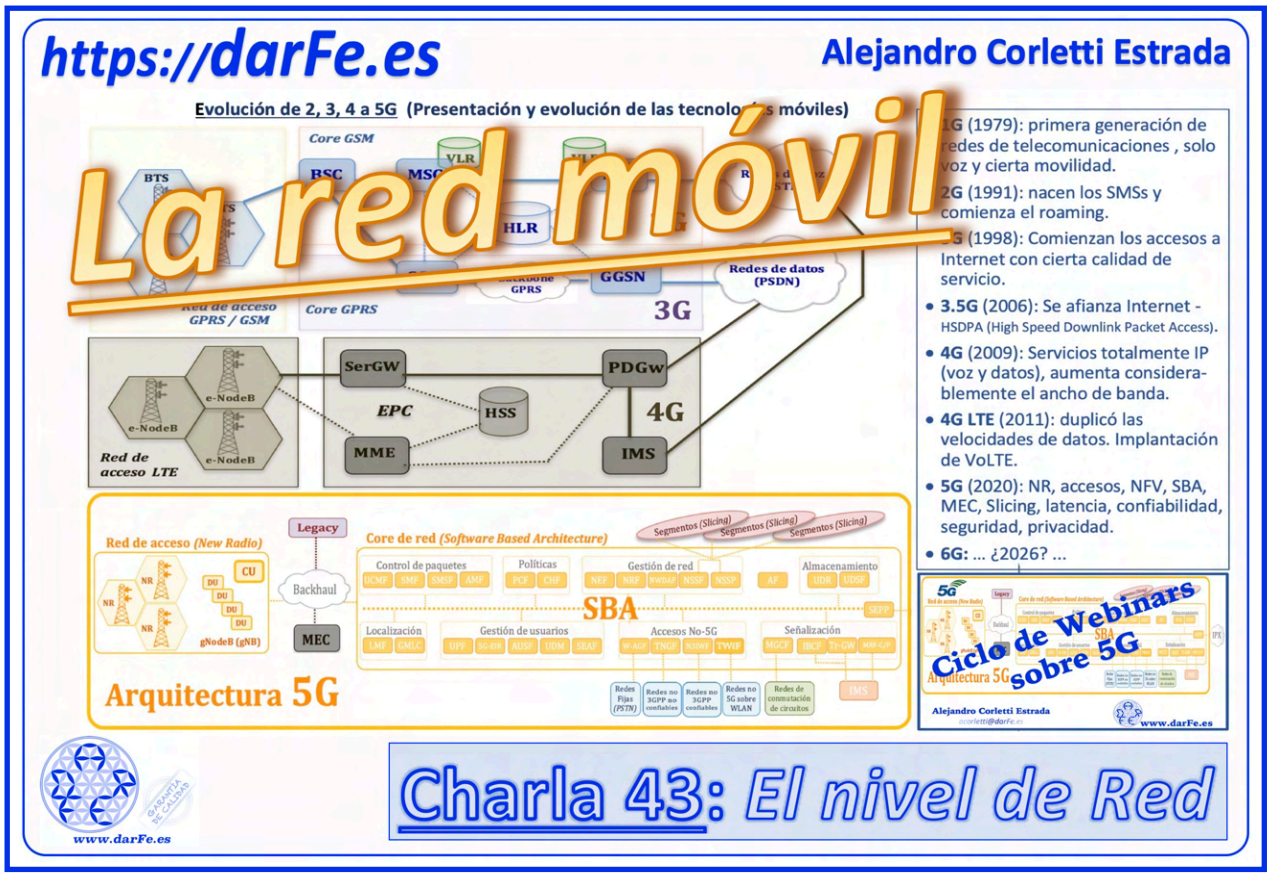
Desde el punto de vista de Ciberseguridad, este protocolo es clave, pues cualquier tipo de alteración de sus rutas originales, nos permitiría "ver pasar" y/o "modificar" los flujos de tráfico de todo el planeta. Por esa razón es que hoy en día, se establecen varias medidas de seguridad sobre el control de los "neighbor" (vecinos) que comparten las rutas, para robustecer su autenticación e integridad.

Volver al índice

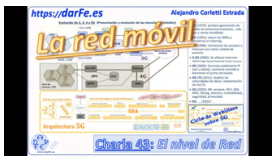
www.darFe.es

Charla 43

La red móvil



Enlace al Video:



Resumen:

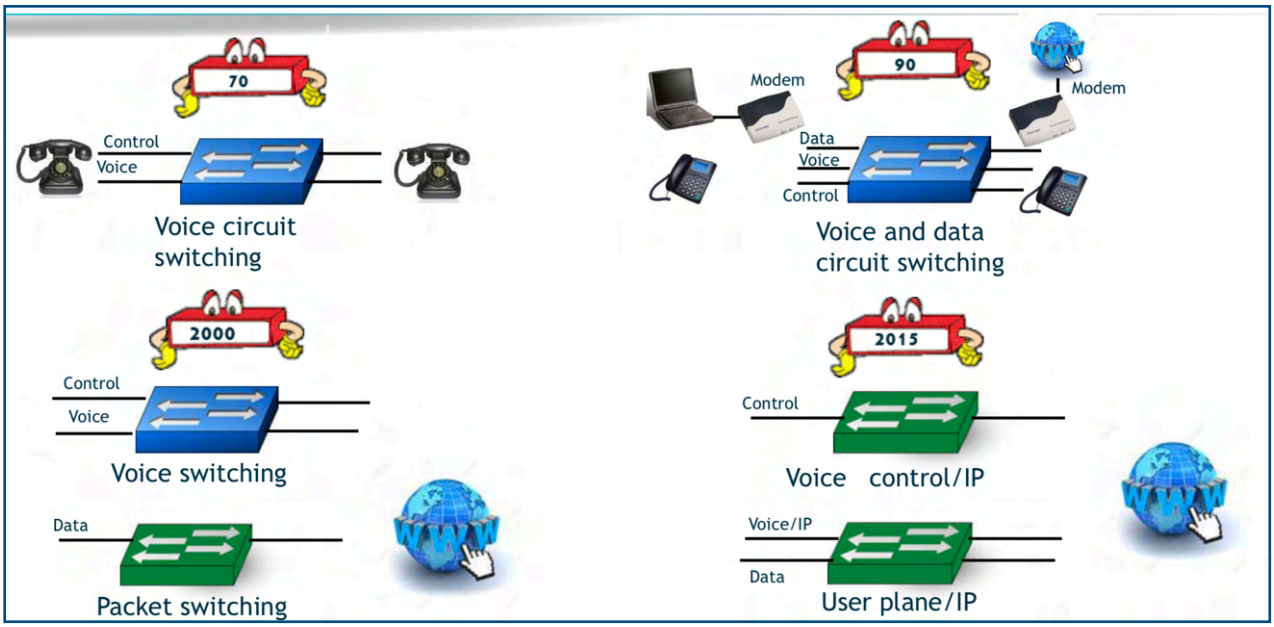
Este es un capítulo complicado para desarrollar en texto, por la cantidad e imágenes que lo sustentan, y los otros videos que ya hemos ido desarrollando sobre este tema, así que en las líneas que siguen, verás que intentaremos resumir todo lo posible el tema, y te invitaremos a que recurras a otros varios videos, documentos PDF y como siempre, también nuestros libros. Creemos que es la mejor forma, para que puedas profundizar con todo el detalle que merece este tema.

Descripción detallada

En esta charla de hoy nos centraremos en la **red móvil.** En la imagen de abajo, podemos ver con un poco más de detalle, lo que hemos visto en la charla anterior, ahora presentado por décadas y arriba a la izquierda podemos ver que los años 70 solo existía la red de conmutación de circuitos, a la derecha ya vemos aparecer en los años 90, la red de voz y datos todavía un poco mezclada dentro de la red de conmutación de datos y conmutación de circuitos, con la aparición de los primeros **modem**.

Más abajo vemos que en el año 2000 ya son dos redes perfectamente separadas e Internet comienza a ser una red totalmente asentada.

En la última imagen abajo y a la derecha, vemos que en el año 2015 aproximadamente ya tenemos dos redes totalmente IP una para el plano de usuario de voz y datos, y otra para el plano de control exclusivamente.



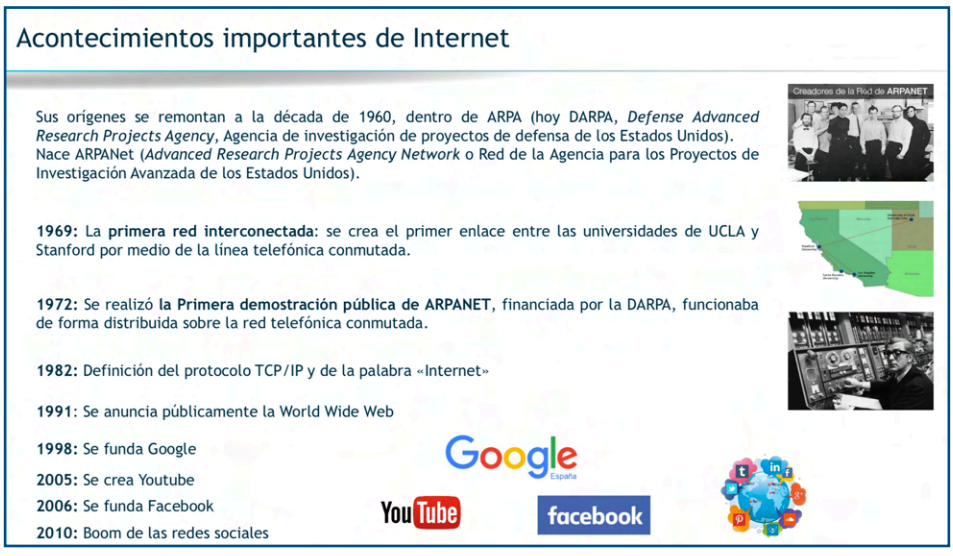
Otra forma de ver la evolución de la red telefónica es con la imagen que sigue, en la que partimos con el Telégrafo, hasta llegar a la actualidad con las redes **5G**.

El actual despliegue de las redes 5G en particular, es un tema que siempre ponemos de manifiesto con con cierta preocupación, pues está ampliando de forma acelerada la brecha entre los países del primer mundo y el resto.

En la imagen que sigue podemos ver perfectamente el volumen de los despliegues de 5G en Europa y Estados Unidos, frente al escasez de los mismos en África y Hispanoamérica.

La tecnología 5G, sin lugar a dudas, es la puerta de acceso a los grandes desafíos tecnológicos, como son: vehículos autónomos, periodismo en vivo, telemedicina, operaciones, quirúrgicas remotas, etc. A medida que los despliegues de 5G incorporen cada vez más estas tecnologías, quien no cuente con ella, quedará fuera del mercado. Este es un hecho de particular interés, pues justamente esta brecha marcará significativamente los desarrollos tecnológicos como un factor clave.

Si ampliamos un poco más aún la historia de esta actual gran red mundial, en la imagen de la derecha podemos ver varios hitos que han sido revolucionarios, desde la primera red, hasta el actual boom de las redes sociales, pasando por Google, Youtube y la WWW.



La red de telefonía móvil

Como podemos ver en la imagen de abajo, en el año 1979 nace la primera generación de telefonía móvil (**1G**). Sobre esta generación ni nos detendremos, pues no merece la pena.

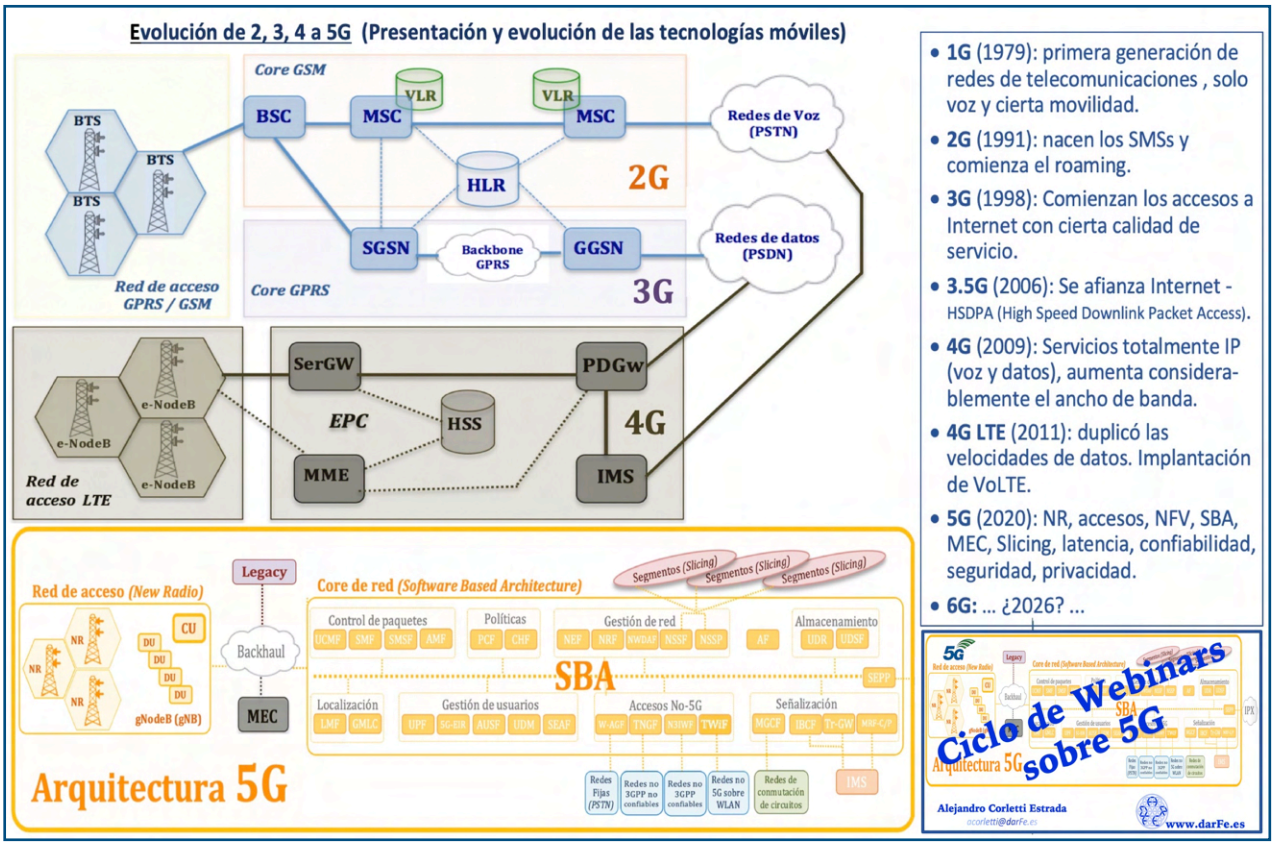
Sí nos interesa comenzar con el desarrollo de **2G**, pues esta si ha sido pionera y aún se sigue usando.

La red **2G** como todas las redes móviles sucesivas, se divide en dos grandes partes, la red de acceso y el Core. La red de acceso se inicia desde las antenas de telefonía cuya electrónica, la gestionan las **BTS** (Base Transceiver Station), el Core de **GSM** (Global System for Mobile Communications, u originariamente: Groupe Special Mobile), que es como se llamó esta segunda generación, como podemos ver, se conecta con la red de acceso por medio de la **BSC** (Base Station Controller). La BSC continúa su trayecto con el **MSC** (Mobile Switching Center), y estos son los que establecen la comunicación únicamente de voz con la red Public switching Telephone Network (**PSTN**).

Reconocemos que esta suma de abreviaturas no te dice absolutamente nada, pero para no ser redundantes, no explicaremos aquí cada una de sus funciones, si deseas profundizar con todo detalle en las mismas, puedes hacerlo en el Capítulo 1. "Historia y evolución de redes" del libro "**Seguridad en Redes**". Luego de la parte de red fija, encontrarás toda la descripción de cada uno de estos elementos.

Lo que debemos destacar de 2G, es que fue una red diseñada únicamente para su empleo en la telefonía, es decir para voz.

Cómo podemos seguir apreciando en la imagen de abajo, en el año 1998 nace la tercera generación o tres también conocida como **GPRS** (General Packet Radio System).



Si prestamos atención, el Core de GPRS ahora es diferente. Nacen dos nuevos dispositivos que son el **SGSN** (Serving GPRS Support Node), y el **GGSN** (Gateway GPRS Support Node). Estos nuevos dispositivos son los responsables de la red de conmutación de paquetes. Al incorporarlos a la vieja tecnología 2G, ahora la BSC asume una nueva funcionalidad; al detectar que se trata de una comunicación de voz, mantiene su ruta original, pero cuando detecta que se trata de un paquete de datos (un usuario que abre un navegador, o envía un e-mail, por ejemplo) lo deriva hacia el **SGSN** el cual seguirá la ruta hacia la red de paquetes o **PSDN** (Packet Switching Data Network). Como puede apreciarse en la mencionada imagen, ahora aparece por primera vez esta red (PSDN).

Si seguimos analizando la imagen anterior, vemos que entre los años 2009 y 2011 aparece la tecnología **4G**, la hemos representado en color marrón, también llamada **LTE** (Long Term Evolution). Esta nueva tecnología introduce una nueva red de acceso y también también un nuevo Core de red, **EPC** (Evolved Packet Core). una vez más, no nos detendremos en la función y significado de cada uno de sus nodos, pues como hemos dicho, puedes verlo con todo detalle en el libro "**Seguridad en Redes**".

Las características fundamentales de esta red es que, la red de acceso, que ahora se compone de los **e-nodeB,** incorpora una cierta inteligencia en estos nodos y desde la misma ya está en capacidad de decidir si se trata de una comunicación de voz, la cual la dirige hacia el **SerGW** (Serving Gateway), o se trata de una comunicación de datos, la cual la envía al **MME** (Mobility Management Entity).

Un detalle final sobre 4G, es la incorporación de **VoLTE** (Voice over LTE). Aquí sí, por primera vez en la historia, se unifica la red de voz y datos de forma paquetizada y digital, generando una comunicación total de extremo a extremo con paquetes de datos (con el teléfono móvil incluido).

Finalmente en el año 2020 comienza a entrar en producción la red **5G**, que revoluciona absolutamente la tecnología móvil en todo su diseño y arquitectura.

Una vez más, para no ser redundante en estos desarrollos, os invitamos a que veáis un **ciclo de videos sobre 5G** que tratan el tema con máximo detalle, estos son:

Ciclo Webinar sobre Ciberseguridad en 5G - 1. Presentación e introducción a 5G

- **Ciclo Webinar sobre Ciberseguridad en 5G - 2. New Radio y gNodeB**

- **Ciclo Webinar sobre Ciberseguridad en 5G - 3. SBA, MEC y Slicing**

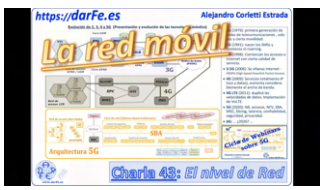
- **Ciclo Webinar sobre Ciberseguridad en 5G - 4. Accesos y Autenticación**

- **Ciclo Webinar sobre Ciberseguridad en 5G - 5. Seguridad en 5G**

También podéis descargar la documentación de estos videos en formato "PDF" desde la sección "Descargas" de nuestra web: **www.darFe.es**

Finalmente, ya se están elaborando los estándares para la tecnología **6G**, que se estima podría comenzar sus despliegues en 2026.

En el video de este capítulo, se desarrollan una serie de conceptos sobre la situación actual de la red móvil, que sumado al ciclo de 5G, creemos que contienen toda la información que necesitas. Hay muchos aspectos gráficos que harían interminable esto si lo quisiéramos expresar en texto, así que os reiteramos la invitación a que veáis el vido completo.



Si deseas ir avanzando en tema de hacking, te recomendamos que no te pierdas el video:

“**Hacking móvil**”

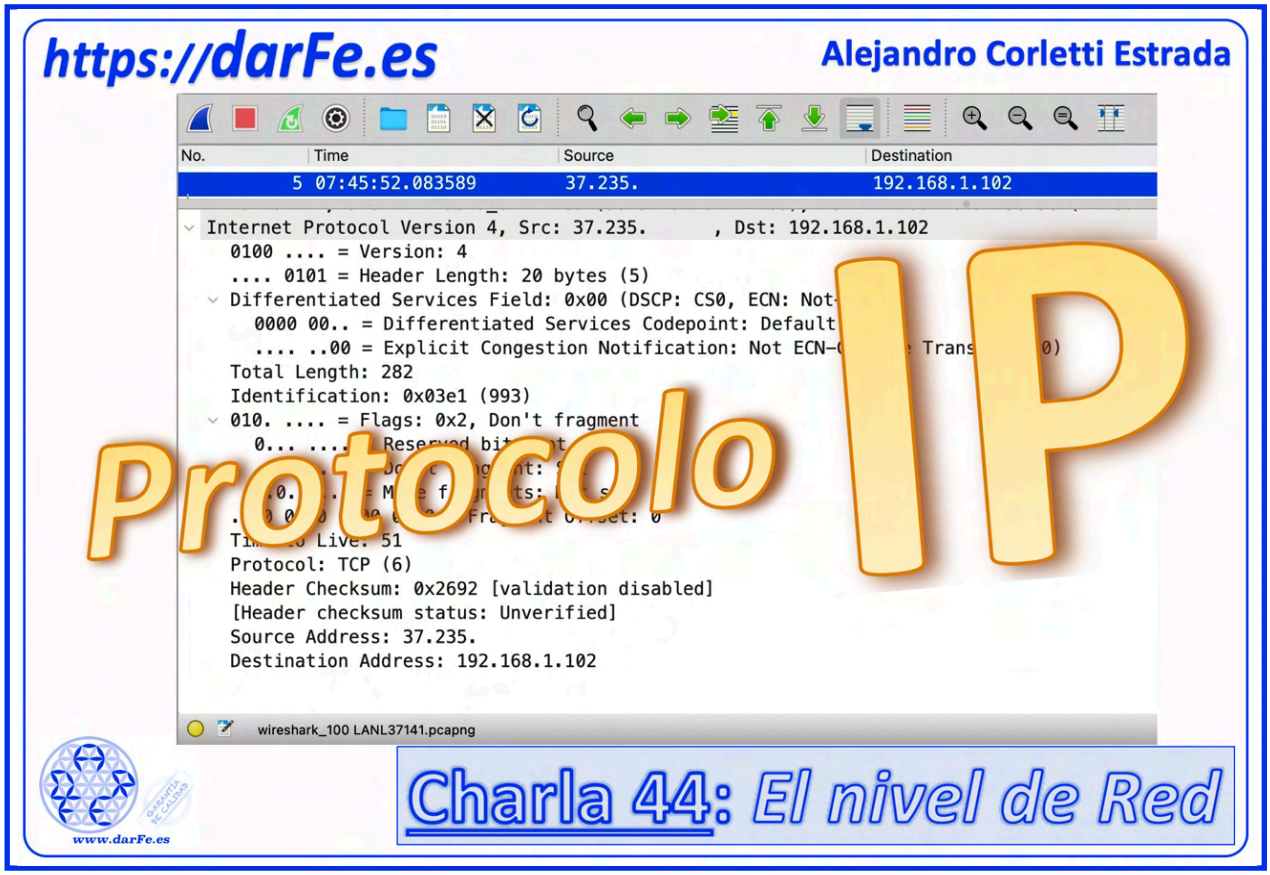
Por último, si lo que te interesa es la historia, puedes ver también el punto 4.4. "Telefonía Móvil" del libro "**Seguridad por Niveles**"

Volver al índice

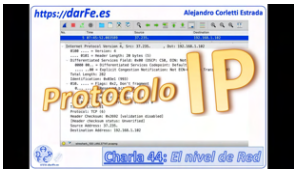
www.darFe.es

Charla 44

Protocolo IP



Enlace al Video:



Resumen:

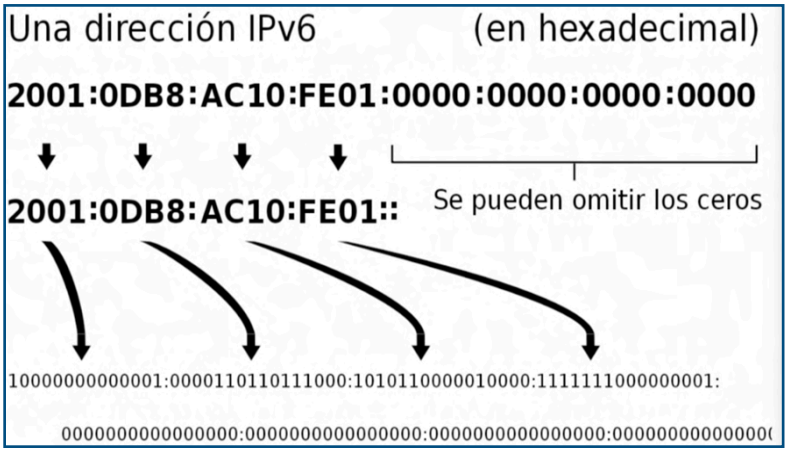
En esta charla desarrollaremos el encabezado del **protocolo IP**. Comenzaremos por las dos versiones que hoy en día están vigentes, la **versión 4** y la **6**. Nos centraremos luego con más detalle en la versión 4 que es la que más presente sigue estando en la mayoría de las redes. Presentaremos los campos de este encabezado, desde el punto de vista teórico para sentar las bases y posteriormente lo verificaremos con una captura de tráfico real, en la que analizaremos cada uno de sus campos.

Descripción detallada

En esta charla de hoy, comenzamos a desarrollar el protocolo **IP** (Internet Protocol). Este es el protocolo por excelencia del nivel de red, por lo que nos centraremos casi con exclusividad en el mismo.

La versión de este protocolo que ha sido la estrella del siglo pasado y aún se mantiene en la masa de las redes es la versión 4. Por una serie de problemas que iremos desarrollando en este nivel, a finales del siglo pasado, nació las versión 6. Esta versión (v6) se viene asegurando que reemplazará a la versión 4 desde hace 25 años, pero como el mejor ejemplo del ave Fenix, la v4 resucita y se sigue manteniendo en vigor hasta estos días. Es cierto que, podríamos decir que en los últimos cinco años, muchas operadoras y empresas han comenzado a implementar la última versión, pero insistimos, la masa de las redes, e Internet inclusive, siguen manteniendo la IPv4 en la mayoría de sus enlaces y hosts.

Tal vez lo más significativo de la versión 6, es su inimaginable capacidad de direccionamiento, pues emplea **128 bits** como estructura del campo de direcciones, frente a los 32 de la versión 4.



A simple vista pareciera que se ha multiplicado por cuatro la cantidad de direcciones, pero hay que tener en cuenta que se trata de una magnitud exponencial, con lo que:

Si $2^{32} = 4.294.967.296$

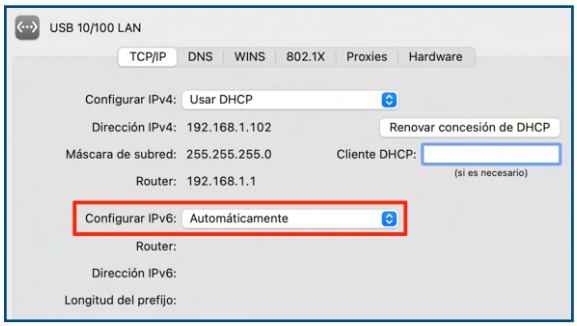
$2^{128} = 3,4 \times 10^{38}$ (en decimal)

Que es algo así como:

340.000.000.000.000.000.000.000.000.000.000.000.000

Lo cual como podéis apreciar es una cantidad inimaginablemente grande. Se dice que podría contener un número similar a $6,6 \times 10^{23}$ direcciones IP por cada metro cuadrado sobre la superficie de la Tierra… como que es mucho ¿no?

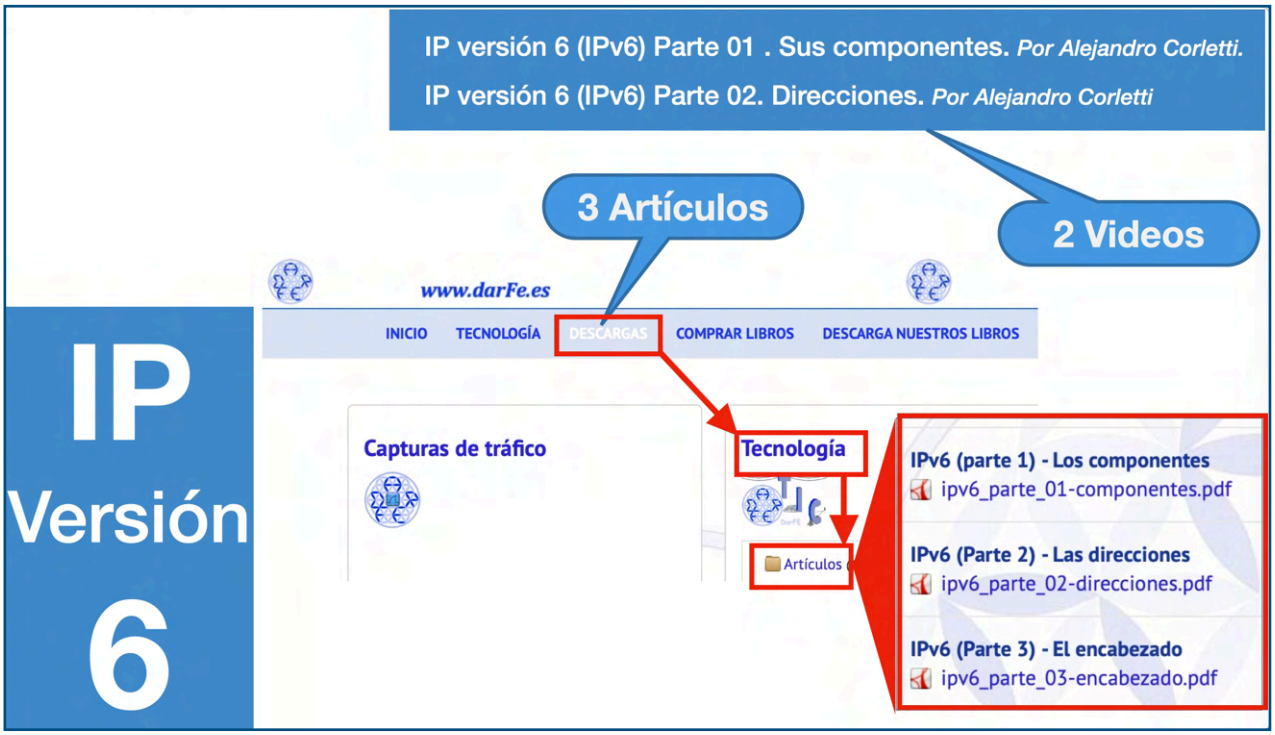
En la actualidad, si prestamos atención, la casi totalidad de los ordenadores, ya poseen la capacidad de operar con IP versión 6, e inclusive generalmente nos asignan una por defecto, como podemos ver en la imagen de la derecha.



En este capítulo, no nos detendremos en IP versión 6, pues, como hemos comentado, la versión 4, es la que sigue siendo la más difundida y, sobre todo, porque para comprender el funcionamiento del nivel de red, es necesario abordar el tema “paso a

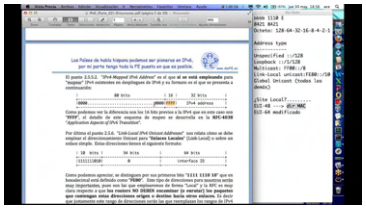
paso", con lo que para poder avanzar a la nueva versión, creemos necesario conocer en detalle la anterior.

Si deseas profundizar en **IPv6**, abajo en la imagen que sigue, puedes ver que contamos con vídeos y documentos PDF, que entran en mucho más detalles sobre este tema.



Los videos son los siguientes:

- **IP versión 6 (IPv6) (Parte 01). Sus componentes.**



- **IP versión 6 . (IPv6) (Parte 02). Direcciones**

También hay algo más de descripción en el punto

5.5.4. "Direccionamiento de IPv6" del libro "**Seguridad por Niveles**"

En cuanto a la versión 4 del protocolo IP, también os recomendamos que recurráis al capítulo 5 de este libro pues está desarrollado con todo detalle.

Lo primero que debemos entender sobre la versión cuatro del protocolo IP es su esquema de direccionamiento. Tenemos un video previo a las charlas de este ciclo que te puede ser de mucha utilidad.

Direccionamiento IP versión 4 (RFC-791)

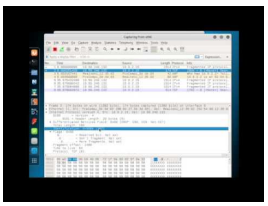
Otro video que te será de máxima utilidad es el que también tenemos publicado en relación a una herramienta muy sencilla que es Open Source y se llama "**ipcalc**". En este video explicamos como instalarla en nuestro "Kali" Linux, verás que es muy fácil, y luego desde la línea de comandos nos ofrece una enorme facilidad para el cálculo de redes, subredes, hosts de inicio y fin, broadcast de red, etc.

Este video es (de verdad, no te lo pierdas):

Ejercicios de direccionamiento IP con la herramienta "ipcalc" sobre Kali

Una función muy importante que nos ofrece el protocolo IP, es la de "fragmentación y de-fragmentación". Esta opción nos permite que, al recibir la Unidad de Datos de Servicio (**UDS**) recibida del protocolo de nivel superior al de red, "romperla" en fragmentos más pequeños e insertarlos en la red. Del otro extremo, al recibirlos, el destino podrá "de-fragmentarlo" y entregarlo a su vez el nivel superior, exactamente igual que como se generó en origen. Esta funcionalidad, es muy común cuando se están enviando ficheros grandes que no entran en la red. Recordemos, por ejemplo, que el protocolo Ethernet (de nivel de enlace) no soporta más que 1514 bytes, con lo que si deseamos transferir un fichero de 2 megabytes, una opción es hacer uso de la fragmentación IP. En el nivel de Transporte (nivel 4) veremos también que se puede realizar una tarea muy similar que se llama "segmentación y re-ensamble", pero no nos adelantemos a ella, cuando lleguemos al nivel cuatro, explicaremos en que caso se emplea una u otra.

El detalle de la fragmentación y re-ensamble puedes verlo en el siguiente video.



Ejercicio de fragmentación IP empleando HPING3 y Wireshark

El **ruteo** es la actividad fundamental del protocolo IP, el cual implementa por medio de un esquema de direccionamiento que se trata a continuación.

Direcciones IP (**RFC-791**)

Toda red que emplee la pila TCP/IP, identifica el origen y destino por medio del empleo del campo de direcciones de los paquetes IP que, para ser correctos, se denominan "**datagramas**". Todo dispositivo que necesite trabajar con estas direcciones sólo puede identificar en cada uno de los bit de ese campo, dos elementos:

- **HOST (h).**
- **NET (n).**

Este campo de direcciones, está constituido por cuatro octetos, los cuales se pueden presentar en binario (**bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb**), en hexadecimal (**hh.hh.hh.hh**) o en decimal (**d.d.d.d**). Es importante habituarse a la correspondencia entre binario y decimal para un ágil manejo de estas direcciones que, como ya puede apreciarse, oscilarán entre **0/255.0/255.0/255.0/255** en sistema decimal. Dentro de este espectro en los cuatro octetos, existen varias direcciones RESERVADAS, las dos más comunes (si bien profundizaremos más en ellas) por ahora son:

00000000 (en binario), o **0** (en decimal): que especifica "La red donde me encuentro".

11111111 (en binario), o **255** (en decimal): que especifica un mensaje de "Broadcast".

Tal vez lo más importante para lograr entender plenamente este esquema de direccionamiento, es no olvidarse que a pesar que las direcciones IP se presentan en forma decimal, ningún dispositivo de red tiene diez dedos, por lo tanto todo (absolutamente TODO) dispositivo que tenga que trabajar sobre una dirección IP, la analizará como una secuencia de 32 bits (pues tiene sólo dos dedos). Lo arraigado que tenemos en nuestra mente el sistema decimal, nos lleva indefectiblemente a razonamientos no adecuados sobre estas direcciones, así que os invitamos a que hagáis un gran esfuerzo por tratar de no usar ocho dedos de vuestras manos y SIEMPRE tratar de razonar el esquema de direccionamiento IP, como secuencias binarias, hasta os permitiremos hacer un poco de trampa y "colar" algún pasaje a decimal, pero insistimos, haced el esfuerzo de familiarizaros con el pasaje de decimal a binario en cada octeto, y veréis que es la mejor forma de ser un experto en redes IP.

Acorde al valor de **primer** octeto, se pueden clasificar distintos tipo de redes:

0xxxxxxx Tipo A: Como el primer bit es 0, este tipo de redes solo podrán abarcar el rango de direcciones entre 0 y 127.

10xxxxxx Tipo B: Como el primer bit es 1 (ya pesa 128) y el segundo obligatoriamente 0, este tipo de redes solo podrán abarcar el rango de direcciones entre 128 + (0 a 63) a 192.

110xxxxx Tipo C: Como los dos primeros bit son 11 (ya pesa 192) y el tercero obligatoriamente 0, este tipo de redes solo podrán abarcar el rango de direcciones entre 192 + (0 a 31) a 223.

1110xxxx Tipo D: Como los tres primeros bit son 111 (ya pesa 224) y el cuarto obligatoriamente 0, este tipo de redes solo podrán abarcar el rango de direcciones entre 224 + (0 a 15) a 239. Este tipo de direcciones están reservadas para empleo de multicast.

11110xxx Tipo E: Como los cuatro primeros bit son 1111 (ya pesa 240) y el quinto obligatoriamente 0, este tipo de redes solo podrán abarcar el rango de direcciones entre 240 + (0 a 7) a 247. Este tipo de direcciones están reservadas para uso experimental por parte de los organismos de Internet.

Al diferenciar estos tipos de redes, a su vez por medio de un concepto denominado **MASCARA DE RED** que se tratará más adelante, en particular las tipo A, B y C determinan ciertos límites entre Host y Net que se detallan a continuación:

Tipo A: (0 a 127), el primer octeto identifica a Net y los otros tres a Host. Por lo tanto existirán 127 posibles redes A y cada una de ellas podrá contener tres octetos de Host lo que equivale a 2 24 = 16.777.214 Host, (N.H.H.H).

Tipo B: (128 a 191) Los dos primeros octetos identifican a Net y los otros dos a Host. Por lo tanto existirán 2 14 Net = 16.384 posibles redes B y cada una de ellas podrá contener dos octetos de Host lo que equivale a 2 16 = 65.534 Host, (N.N.H.H).

Tipo C: (192 a 223) Los tres primeros octetos identifican a Net y el último a Host. Por lo tanto existirán 2 21 Net = 2.097.152 posibles redes C y cada una de ellas podrá contener un octeto de Host lo que equivale a 2 8 = 254 Host, (N.N.N.H).

Las cantidades mencionadas numéricamente son las reales, si bien pueden no coincidir con algunas potencias pues dentro de los rangos establecidos, también existen determinadas direcciones reservadas.

Classless Interdomain Routing (**CIDR**) (**RFC: 1518/1519)**

Ante el inesperado crecimiento de Internet, se produce una saturación del rango de direcciones clase B, dejando libres algunas direcciones clase A y C, y presentando la particular característica que muy pocas empresas (o casi ninguna), puede cubrir una clase A completa, y muchas necesitan más de una clase C. Ante este hecho, se fueron tomando una serie de medidas por medio de las cuales se ajusta la distribución, se restringe la asignación de direcciones a empresas que lo justifiquen con mucho grado de detalle, se distribuyen direcciones en cinco zonas mundiales (**RIPE**, **ARIN**, **APNIC**, **AfriNIC** y **LACNIC**), tal cual lo vimos dos capítulos antes.

REGISTRY	AREA COVERED
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	Canada, USA, and some Caribbean Islands
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

Esto comienza a provocar cada vez mayores tablas en los router con el consiguiente cuello de botella. Para presentar una solución a este problema (momentánea, pues la definitiva recién aparece con IPv6), nace **CIDR** o también llamado "Supernetting". Este concepto permite combinar subredes que comparten más de una clase C, o subdividir redes clase A o B.

Otro tema que surge con motivo de la escasez de direcciones IP, es la **RFC-1918** (Address Allocation for Private Internet) que se publica en febrero de 1996, en la cual se excluye de los rangos de direccionamiento público, es decir de carácter "**Universal**" un cierto rango de direcciones IP que pasan a denominarse "**Privadas**". Resumidamente lo que se hace es verificar que rangos quedan aún disponibles y seleccionar los siguientes de cada clase:

- **Clase A**: 10.0.0.0/8

- **Clase B**: 172. 16 a 31.0.0/12
- **Clase C**: 192.168.0.0/24

Concretamente esta RFC los define en el punto 3. **Private Address Space**

> *The Internet Assigned Numbers Authority (IANA) has reserved the blocks of the IP address space for private internets: following three*
>
> *10.0.0.0 - 10.255.255.255 (10/8 prefix)*
>
> *172.16.0.0 - 172.31.255.255 (172.16/12 prefix)*
>
> *192.168.0.0 - 192.168.255.255 (192.168/16 prefix)*

Aclarando a su vez que:

> *Routers in networks not using private address space, especially those of Internet service providers, are expected to be configured to reject (filter out) routing information about private networks.*

Es decir, todo Internet Service Provider (**ISP**) está obligado a rechazar y/o filtrar cualquier IP dentro de estos rangos.

Continuando con el libro "**Seguridad por Niveles**", como podéis ver en la imagen de abajo, en la página 145, nos describe el formato del encabezado de este protocolo.

Iremos presentando los campos más importantes del mismo. Que como podemos ver, comienza con el campo "Versión" que ocupar 4 bits, y es allí donde nos identificará si se trata de la versión 4 o la 6.

El otro campo que nos interesa es "Longitud de cabecera", que se trata de otros 4 bits que expresa el tamaño de cabecera en palabras de 4 bytes. La longitud mínima que posee la cabecera del protocolo IP, son 20 bytes, por esa razón es que habitualmente encontremos en este campo el número 5, pues 5 x 4 = 20.

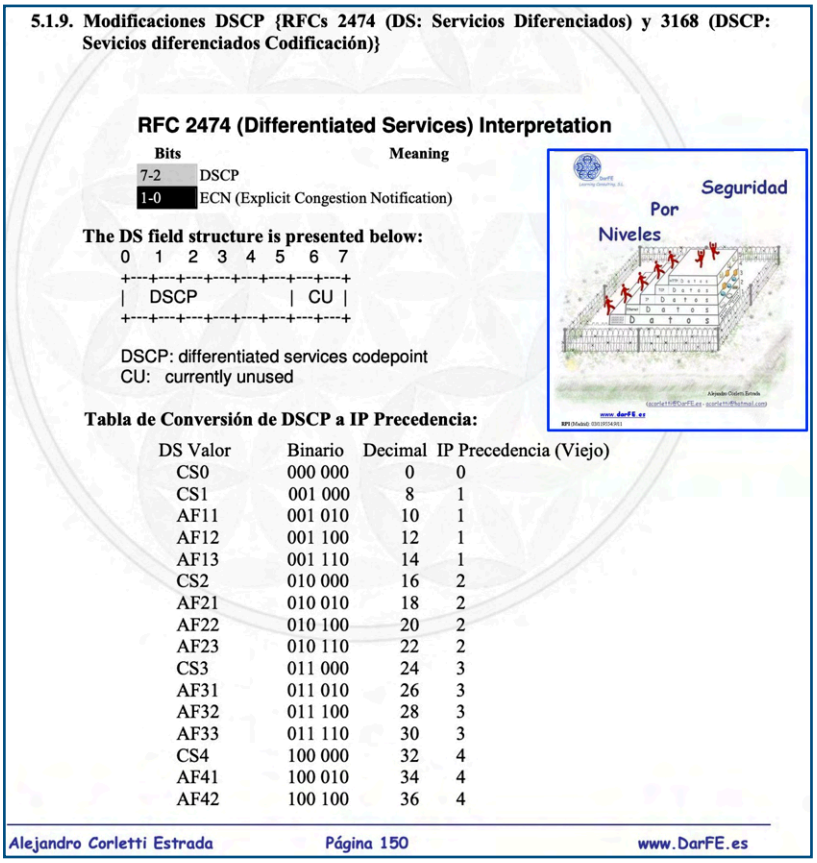
La línea completa que sigue (precedencia - DTR - Reservado), es el octeto que se denomina "Servicios diferenciados". Este es un campo muy importante, pues justamente es lo que hoy en día nos permite generar prioridades y calidad de servicio.

5.1.8. Formato del encabezado (datagrama) IP (Según RFC 791):

Versión			Longitud de cabecera	
precedencia	D	T	R	Reservado
Longitud total				
Identificador				
Identificadores	Desplazamiento de fragmentación			
Tiempo de vida (TTL)				
Protocolo				
Checksum de cabecera				
Dirección Fuente				
Dirección Destino				
Opciones y Relleno (Variable)				
Datos (Variable)				

Versión: 4 bits **Página 145**

Siempre vale lo mismo (0100). Este campo describe el formato



5.1.9. Modificaciones DSCP {RFCs 2474 (DS: Servicios Diferenciados) y 3168 (DSCP: Sevicios diferenciados Codificación)}

RFC 2474 (Differentiated Services) Interpretation

Bits	Meaning
7-2	DSCP
1-0	ECN (Explicit Congestion Notification)

The DS field structure is presented below:

```
 0  1  2  3  4  5  6  7
+--+--+--+--+--+--+--+--+
|   DSCP            | CU |
+--+--+--+--+--+--+--+--+
```

DSCP: differentiated services codepoint
CU: currently unused

Tabla de Conversión de DSCP a IP Precedencia:

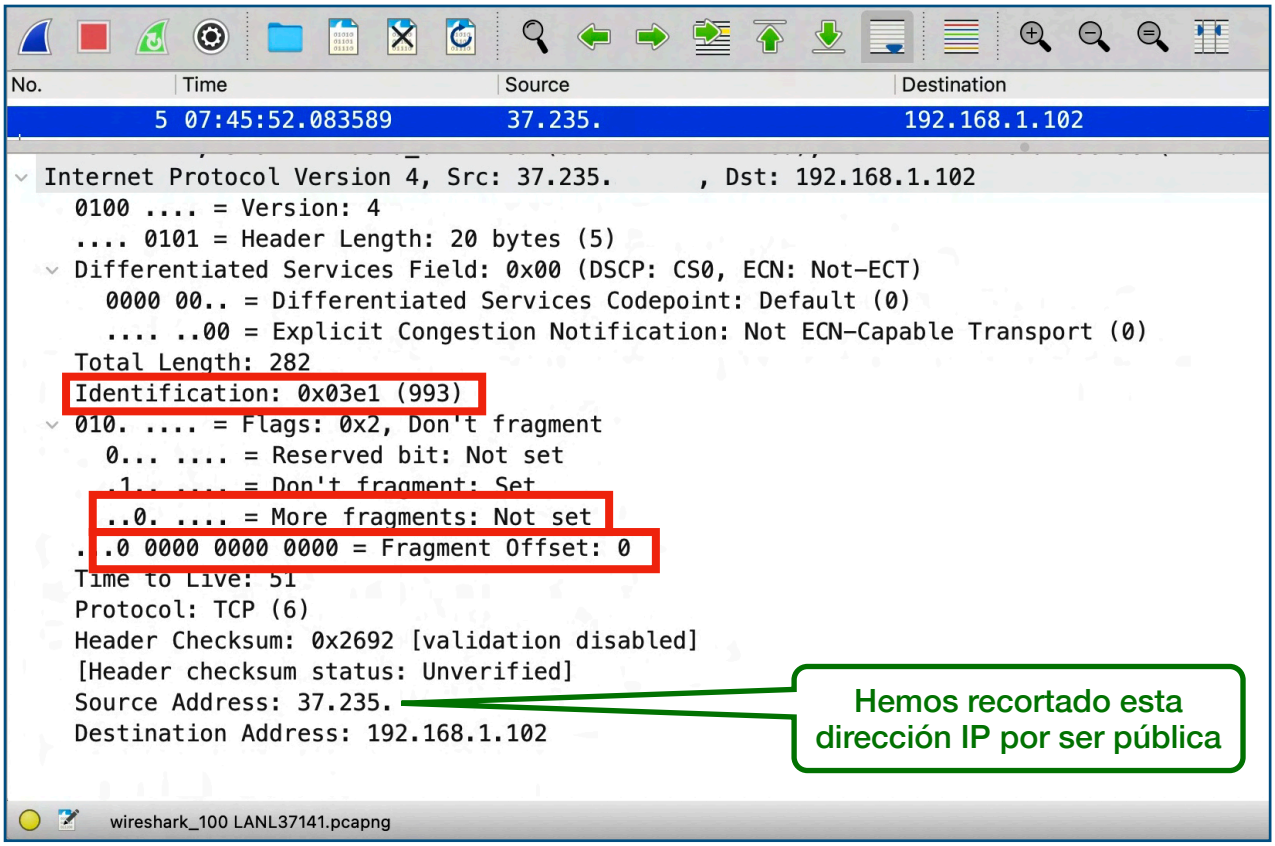
DS Valor	Binario	Decimal	IP Precedencia (Viejo)
CS0	000 000	0	0
CS1	001 000	8	1
AF11	001 010	10	1
AF12	001 100	12	1
AF13	001 110	14	1
CS2	010 000	16	2
AF21	010 010	18	2
AF22	010 100	20	2
AF23	010 110	22	2
CS3	011 000	24	3
AF31	011 010	26	3
AF32	011 100	28	3
AF33	011 110	30	3
CS4	100 000	32	4
AF41	100 010	34	4
AF42	100 100	36	4

Alejandro Corletti Estrada Página 150 www.DarFE.es

En la imagen de la izquierda, podemos ver el punto 5.1.9 de nuestro libro, en el que se desarrolla con más detalle este tema. Lo iremos desarrollando con más profundidad en las charlas siguientes.

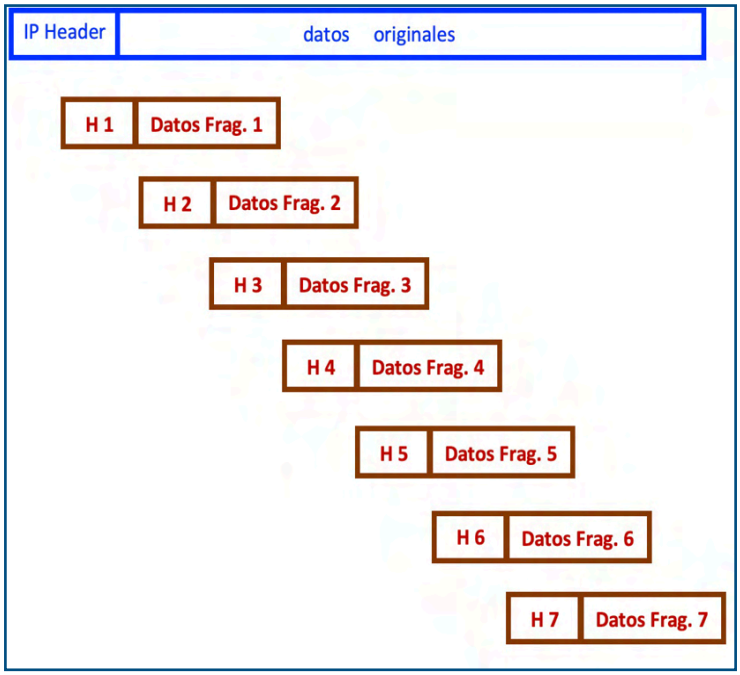
Luego viene el campo Longitud total, que sencillamente, se trata de la suma total de la cabecera más la totalidad de su campo de datos.

Para los campos que siguen, vamos a emplear un caso real de captura de tráfico, pues merece la pena que nos detengamos en ellos.



Los tres campos que hemos resaltado en **rojo** en la captura de tráfico anterior, son los que nos permiten realizar la operación de fragmentación y de-fragmentación.

Tal cual hemos mencionado, cuando el protocolo IP recibe del nivel superior un campo de datos mayor al que puede entregar al nivel e enlace, puede romperlo en fragmentos menores.

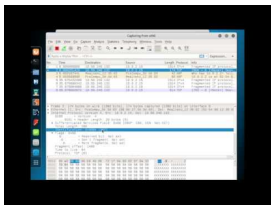


Para este operación, genera aleatoriamente un valor de "Identification" que será el mismo valor para todos los fragmentos que envíe. El segundo campo que empleará será el de "More fragments", que valdrá "**1**" para cada uno de los fragmentos, hasta que envíe el último de ellos, en el cual sí lo volverá a poner a "**0**" para indicar que allí finaliza la fragmentación.

El último de los campos será el de "Fragment Offset" que indicará la posición que ocupará cada uno de los fragmentos, respecto de la unidad de datos completa que ha recibido del nivel superior, para que el nivel IP del receptor sepa dónde va a ir ubicando cada fragmento en el momento de volver a entregarlos al nivel 4 de ese destinatario.

Si queréis ejercitar con estos tres campos, te recomendamos el siguiente video:

ejercicio de fragmentación IP empleando HPING3 y Wireshark



Otro campo que es importante en el encabezado del protocolo IP, es **TTL** (Time To Live), o tiempo de vida. Este campo es el que se emplea para evitar el "bucle infinito". Este campo es tan importante que lo desarrollaremos con todo detalle en otra charla posterior.

El campo "Protocol" indica cuál será el protocolo de nivel superior. En la captura de tráfico de la página anterior, podemos ver claramente que con el valor "6", Wireshark inmediatamente lo identificó como protocolo TCP.

El campo "Header Checksum", es el control de cabecera (únicamente de cabecera, no del resto de los datos), y funciona de forma similar a lo que desarrollamos como CRC en la **charla 16**.

Finalmente podemos ver los cuatro octetos de la dirección fuente y los de la dirección destino, en el formato establecido para la versión del protocolo IP que estemos trabajando. En la captura de tráfico anterior, podemos ver las dos direcciones IPv4, de las cuáles, como hemos remarcado en la imagen, la dirección fuente, tal cual hemos destacado en **verde**, la hemos recortado pues se trata de una dirección pública.

Volver al índice

www.darFe.es

Charla 45

Máscaras de red y subred

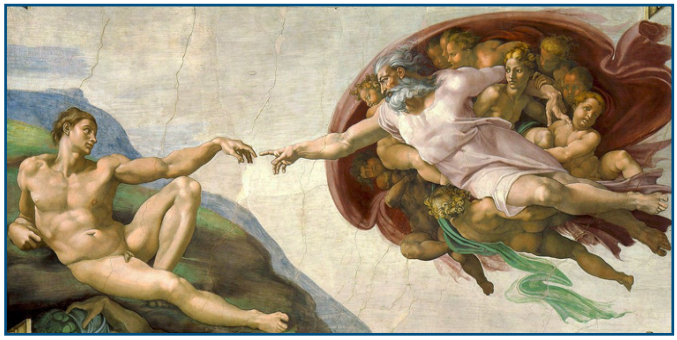
Enlace al Video:

Resumen:

En esta charla, desarrollaremos el tema de **máscaras de red y subred**, pues es uno de los pilares sobre los que construir arquitecturas de red robustas, aprovechando al máximo las opciones que nos ofrece el direccionamiento privado que vimos en el capítulo anterior.

Si sabemos ajustar y dimensionar adecuadamente nuestras redes, lograremos diseñar arquitecturas seguras y que perdurarán muchos años, por su facilidad de expansión y crecimiento. Al final del capítulo presentamos la herramienta "**ipcalc**" (fundamental).

Descripción detallada



Dios creó al mundo en 7 días.

Para Él fue muy sencillo, en primer lugar porque es Dios, pero la clave verdadera fue porque lo comenzó a hacer desde cero. Si hubiese tenido ya alguna base sobre la que continuar, mejorando y/o emparchando, tal vez todavía estuviera trabajando.

Si ya has tenido alguna experiencia en redes y TI, compartirás plenamente este concepto, pues es mucho más sencillo y económico hacer las cosas bien desde el principio, y no tener que re-comenzar a parchear, o solucionar errores que no se consideraron en su origen, este tipo de re-encauces puede ser carísimo, y requerir un esfuerzo, a veces inalcanzable.

¿A que viene todo esto?

Viene a que, si, llegado el momento, tenemos la suerte de poder diseñar desde cero nuestra arquitectura de red y TI, y lo hacemos bien, sentaremos las bases de una infraestructura **muy duradera**, **flexible**, **expansible** y **segura**.

Por el contrario, si no nos tomamos el tiempo y la dimensión necesaria para abordar este problema, dejaremos una herencia muy complicada a nuestros sucesores y equipo de trabajo.

En el capítulo anterior, presentamos los diferentes esquemas de direccionamiento privado. Estas direcciones, nos ofrecen un abanico de posibilidades casi inagotable, si sabemos aprovecharlas debidamente.

En este video, se presenta, justamente el tema, bajo la experiencia de haber diseñado una red real y concreta (la del Ejército Argentino), casi cuando estaba naciendo el despliegue del protocolo IP versión 4. Más allá de volver a describirlo aquí, la mejor forma de entender este despliegue, es viendo el video.

Lo que sí nos detendremos en este texto, es sobre el empleo de las máscaras de red y subred, pues el entendimiento del tema, es la base sobre la que se sustenta un correcto diseño.

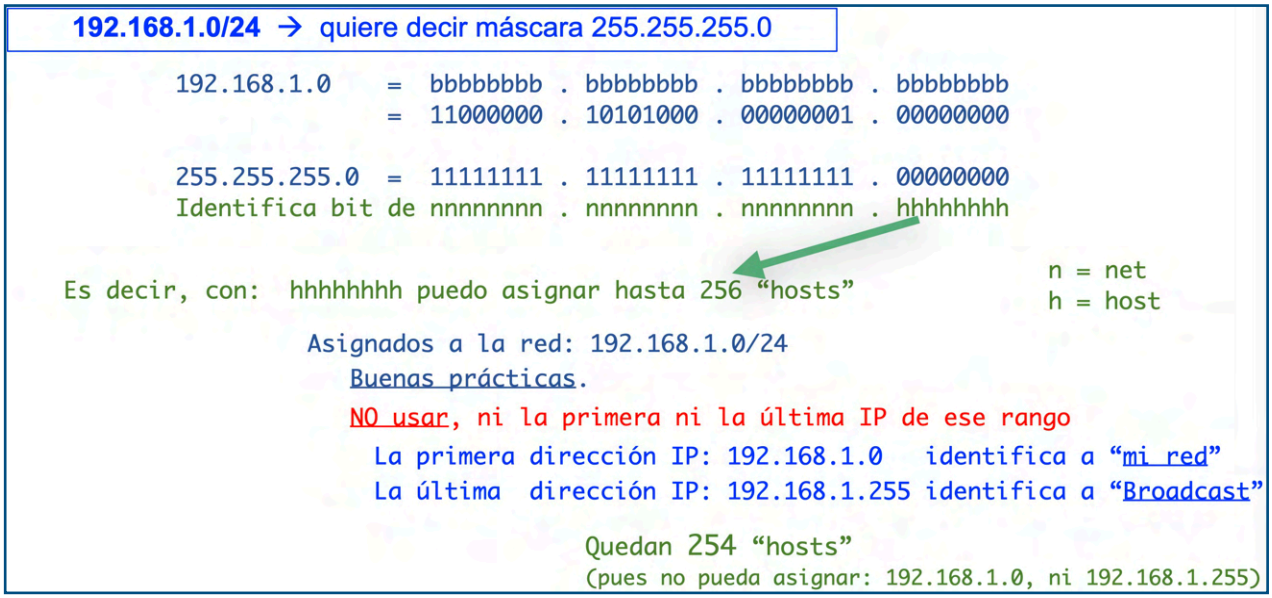
A continuación, comenzaremos a desarrollar el tema, desde un ejemplo de red tipo C.

Tomemos como punto de partida la más frecuente de estas redes, por ejemplo la red **192.168.1.0/24**. Este tipo de nomenclatura de máscara de red, es decir "**/24**" lo que nos está indicando es que la máscara de red es: 255.255.255.0, esto implica que tenemos los tres primeros octetos con todos sus bits puestos a uno y el último octeto a cero: 11111111.11111111.11111111.00000000.

Esto que estamos viendo en formato decimal y binario, recordemos que un dispositivo informático, por ejemplo un router (que no tiene diez dedos, sino solamente dos), lo procesará siempre en formato binario.

En la imagen que sigue, podemos ver con más detalle, la representación de esta red y su máscara, en formato binario. Lo que queremos destacar de esta imagen, inicialmente es que, si recordamos lo que hemos dicho la charla anterior, los unos y ceros de la máscara, identifican unívocamente que cada uno de los bits de la dirección

IP, se corresponderán con un "**host**", o una "**net**", tal cual se puede apreciar en **verde** "**identifica bit de** ".

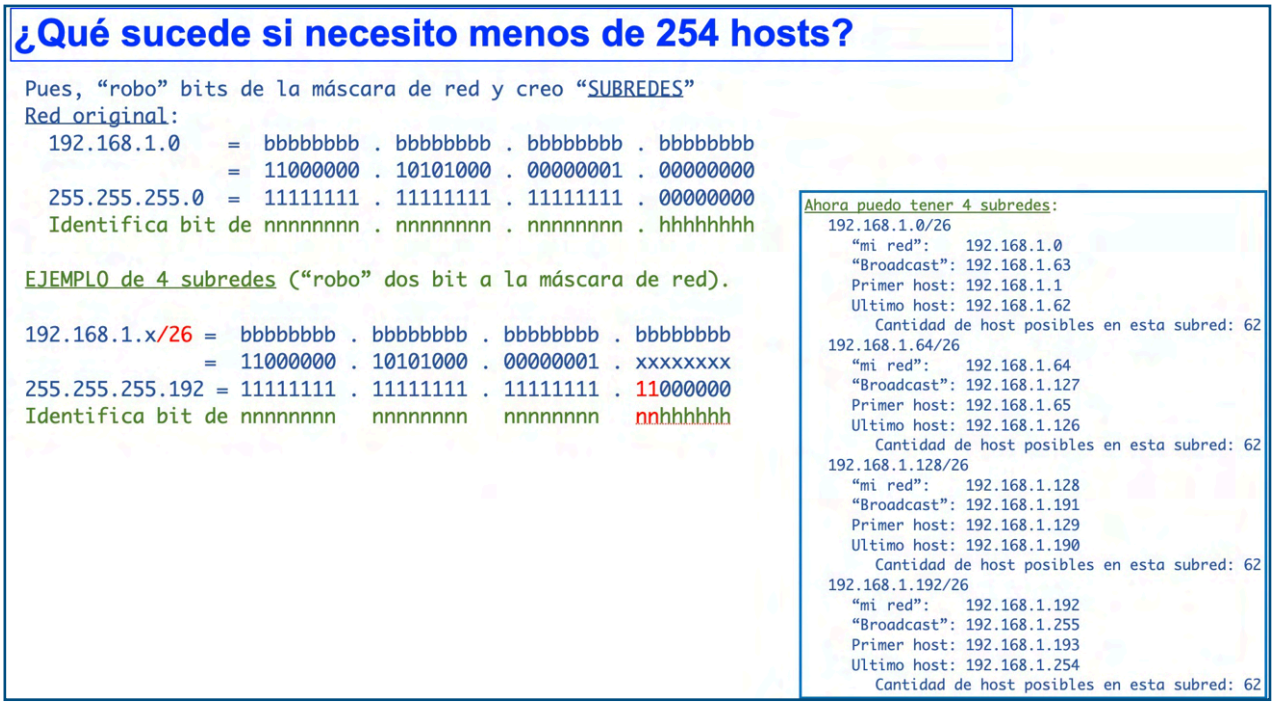


Lo segundo a destacar de la imagen anterior, es, tal cual nos señala la **fecha verde**, con ocho bits correspondientes a hosts (hhhhhhhh), se pueden asignar 256 direcciones IP a los hosts de esta red.

Siguiendo con el análisis de la imagen, es importante destacar las "buenas prácticas" a seguir cuando asignemos direcciones a nuestras redes.

Tal cual se presenta en la imagen, la primera dirección IP (192.168.1.0), en general siempre se interpreta como "**mi red**" y la última (192.168.1.255) como el "**Broadcast**" de esa red. Por lo que siempre es recomendable, dejar libres a ambos y no asignarlos a ningún host.

En el ejemplo que estamos presentando, entonces, de las 256 potenciales direcciones IP que podría asignar a hosts, me estarían quedando disponibles solo **254** de ellas.



En la imagen anterior, presentamos el tema de “Máscara de **sub**red”.

Este concepto de “Subred”, aparece cuando uno “**roba**” bits de la máscara de red original, que en el caso de las redes tipo C, como vimos en la primer imagen es “**/24**” (repasad la charla anterior, sobre la máscaras tipo A = **/8**, y las tipo B = **/12**).

La imagen anterior, nos pone como ejemplo, un caso concreto en el cual no necesitamos 254 hosts en esa red, sino solamente algunos, en el orden de 50 hosts.

Ante este planteo, podemos “romper” la red 192.168.1.0/24, por ejemplo, en **4 subredes**.

Dos bits, me presentan cuatro opciones: 00. 01, 10 y 11. Por lo tanto, le “robamos” los dos primeros bits a este último octeto de la "máscara de red **/24**”, pasando a crear una “máscara de **sub**red **/26**”. Prestad especial atención a los bits que hemos resaltado en **rojo**, en dicha imagen, pues son la clave de este proceso.

Si hacemos esta nueva re-configuración de subredes, nos quedarían las cuatro subredes que se presentan al final de la imagen. Como podemos ver, ahora tenemos cuatro redes y en cada una de las cuáles podemos asignar hasta 62 hosts, dejando libres los dos extremos de cada una de ellas, tal cual hemos presentado como “buenas prácticas” en el trabajo de red y subred.

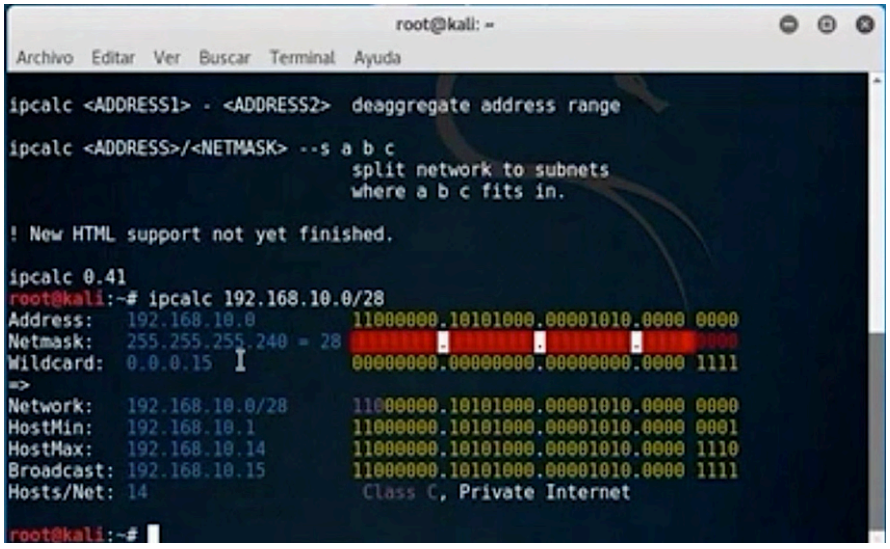
Para cerrar el tema de hoy, os recomendamos una herramienta espectacular que cumple con una de las mejores cualidades que se puede pedir a un desarrollo informático, la **sencillez**.

Se trata de una herramienta que se ejecuta a través de línea de comandos, y es muy sencilla de instalar, solamente desde nuestro “**Kali Linux**” debemos ejecutar el siguiente comando:

```
#apt-get install ipcalc
```

Como podéis imaginar la herramienta, justamente, se llama “**ipcalc**”

Esta sencilla herramienta, en fracciones de segundo, nos permitirá diseñar cualquier tipo de red y subred, ofreciéndonos toda la información necesaria de sus máscaras, la cantidad de host que puedo asignar en cada una de ellas, su dirección de inicio y fin, etc.



Recomendamos especialmente su empleo, y que le dediquéis algunos minutos para familiares con ella, pues de verdad, es de esas maravillas de sencillez que nos ofrece Linux, sobre las que descubriremos una potencia muy buena.

Sobre esta herramienta tenemos otro video que os puede ser de gran ayuda para su instalación y manejo de la misma, este es:

Ejercicios de direccionamiento IP con la herramienta "ipcalc" sobre Kali

Volver al índice

www.darFe.es

Charla 46

Uso de IPs privadas (zonas y enlaces)

Enlace al Video:

Resumen:

En esta charla os presentamos una propuesta de diseño para la arquitectura de las redes de vuestra organización, empleando los conceptos ya aprendidos de **direcciones privadas** y **máscaras de red y subred**.

Se trata de una metodología eminentemente lógica, que es fundamental para asegurar la supervisión y monitorización de la misma.

Descripción detallada

Continuando con el tema de direccionamiento IP y máscaras de red y subred que desarrollamos en los **capítulos 44** y **45**, hoy organizaremos las diferentes sedes de una empresa, teniendo en cuenta una distribución coherente y que nos permita crecer a futuro varios años más.

Ya hemos explicado la diferencia entre direccionamiento IP público y privado. Desde el punto de vista de Ciberseguridad, el empleo de direccionamiento privado, nos ofrece un nivel de seguridad adicional, pues como hemos mencionado, este tipo de direcciones IP, no son visibles, ni pueden ser alcanzadas desde Internet, con lo que si sabemos configurar adecuadamente nuestras redes y sistemas, ya estamos poniendo más difícil la situación a cualquier malintencionado que desee atacarnos.

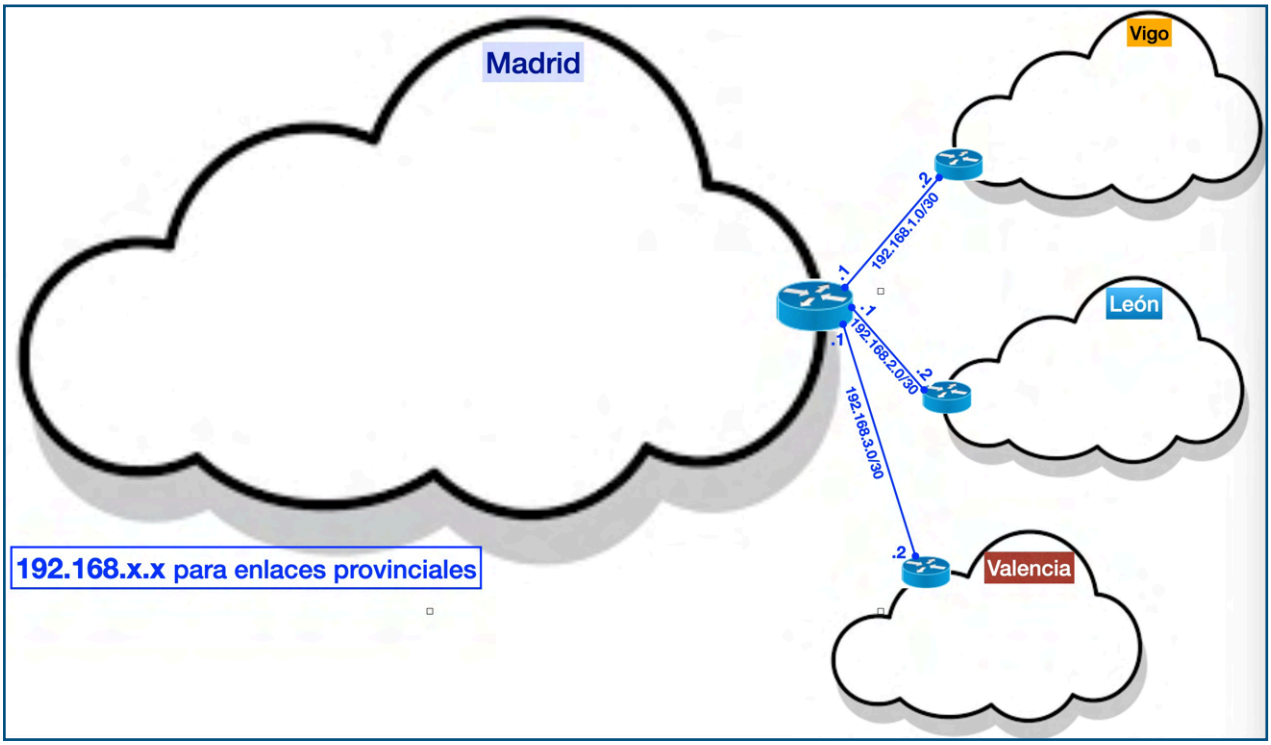
Hoy vamos a comenzar a proponer un diseño de los diferentes vínculos que pueden ser asignados a nuestra organización, considerando que la misma puede tener una distribución territorial amplia. Por supuesto si nuestra red es más pequeña que lo que plantearemos aquí, podemos quedarnos con la idea y aplicarla a los segmentos que se ajusten a nuestra empresa.

Nuestro planteo inicial es un ejemplo de empresa que, por ejemplo, tuviera presencia en cuatro ciudades españolas, en esta caso: Madrid, Vigo, León y Valencia.

En este planteo, proponemos asignar el rango **192.168.x.x** para los enlaces ínter provinciales.

En la imagen que sigue, podemos ver que se han configurado enlaces "**punto a punto**" con cabecera en Madrid y extremos en las otras tres ciudades.

Cuando se trata con enlaces punto a punto, siempre es aconsejable el empleo de subredes con máscara "**/30**", pues esta máscara deja libre solamente dos bits para "hosts", con lo que tenemos cuatro opciones: 00, 01, 10 y 11, de los cuáles, como ya hemos explicado los dos extremos es una buena práctica no emplearlos, con lo que nos quedan solo dos hosts disponibles, será uno para cada extremo.



Como acabamos de presentar en la imagen anterior, tendríamos entonces los siguientes enlaces:

Madrid-Vigo: 192.168.1.1 <—> 192.168.1.2

Madrid-León: 192.168.2.1 <—> 192.168.2.2

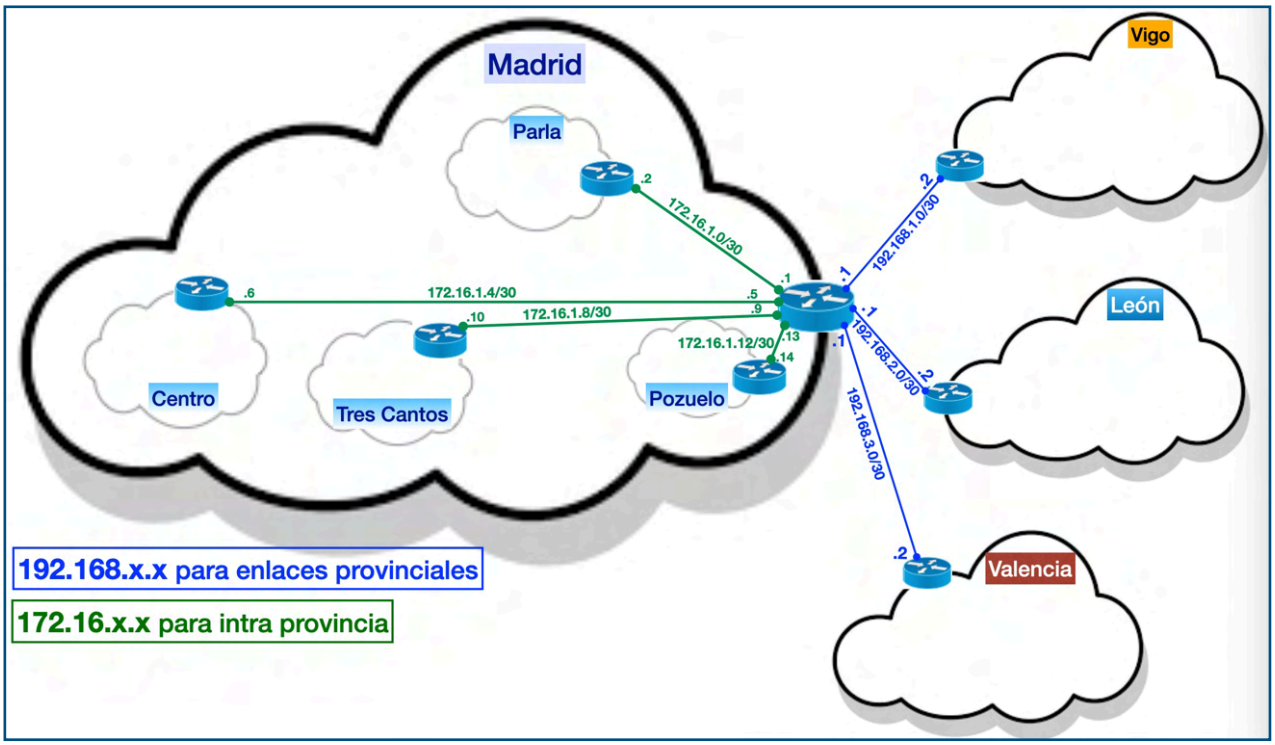
Madrid-Valencia: 192.168.3.1 <—> 192.168.3.2

Esta arquitectura, se trata de un ejemplo didáctico, para que podamos comprender un diseño coherente de asignación de direccionamiento privado. En la realidad, este tipo de enlaces punto a punto puede ser mejorado por medio de enlaces redundantes o topologías tipo "**malla**" o "**anillo**" para que, ante el fallo de cualquiera de estos enlaces, existan caminos o rutas alternativas que mantengan la comunicación.

Sigamos avanzando en el diseño de nuestra organización.

Supongamos que cada ciudad (o provincia), tiene diferentes sucursales dentro de ella. En este caso, por ejemplo podemos tomar otro tipo de redes privadas, por ejemplo la **172.16.x.x**, y con este rango, definir cada uno de los enlaces de estas sucursales.

Esta nueva asignación de enlaces podría ser tal cual se presenta en la imagen que sigue. Solo desarrollaremos el de Madrid, para simplificar la explicación, pero por supuesto, la misma lógica aplicaría en cada ciudad o provincia.



Con color verde, en la imagen anterior podemos ver como hemos asignado estos enlaces entre

El router de entrada a Madrid y Parla: 172.16.1.1 <—> 172.16.1.2

El router de entrada a Madrid y Centro: 172.16.1.5 <—> 172.16.1.6

El router de entrada a Madrid y Tres Cantos: 172.16.1.9 <—> 172.16.1.10

El router de entrada a Madrid y Pozuelo: 172.16.1.13 <—> 172.16.1.14

Si tuviéramos que hacer lo mismo internamente en Vigo, León y Valencia, podríamos perfectamente emplear cualquiera del resto de los rangos 172.16.x.x, por ejemplo, para Vigo 172.16.2.x, para León 172.16.3.x y para Valencia 172.16.3.x. O cualquiera que se nos ocurra dentro de esta red tipo B.

Finalmente, nos quedaría diseñar los esquemas de direccionamiento de cada una de las redes LAN de la totalidad de las ubicaciones.

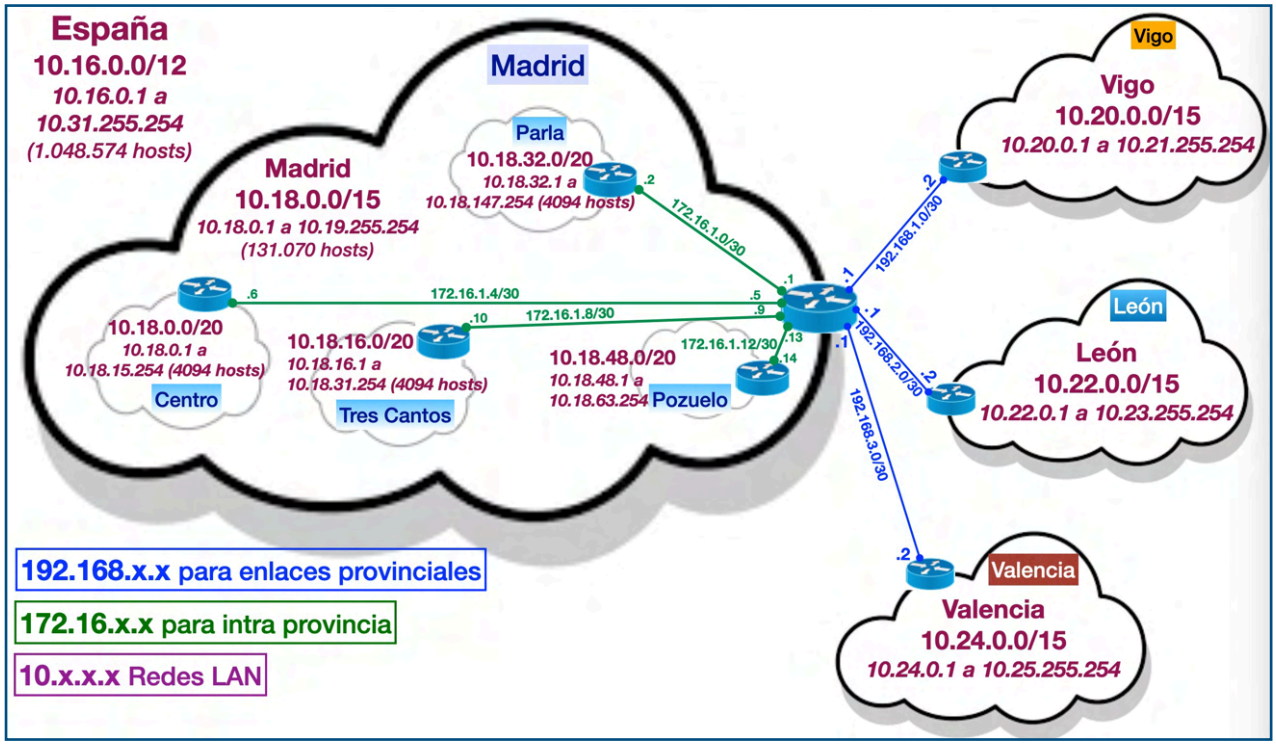
En nuestro diseño, por ejemplo, proponemos emplear la red Tipo A: **10.x.x.x**, para lo cual podría ser:

Madrid: red 10.20.0.0/12

Vigo: red 10.22.0.0/12

León: red 10.16.0.0/12

Valencia: red 10.24.0.0/12



Cada ciudad o provincia a su vez, puede "robarle" bits a la máscara de subred de la misma, para armar subredes más pequeñas para cada sucursal. Ampliemos y pongamos como ejemplo de ello a Madrid, por supuesto, al igual que el punto anterior, esto mismo puede, o debe, reflejarse también en el resto de las ciudades o provincias.

En Madrid podríamos, definir las siguientes redes LAN.

centro: 10.18.0.0/20

Tres Cantos: 10.18.16.0/20

Parla: 10.18.32.0/20

Pozuelo: 10.18.48.0/20

Fijaros que hemos diseñado redes LAN en cada sucursal que soportarían hasta 4094 hosts, lo que es una propuesta bastante ambiciosa y flexible como para que pueda ir creciendo lo suficiente para los próximos años.

El último detalle importante a considerar en nuestra arquitectura, está representado en el extremo superior izquierdo de la última imagen, en el que podemos ver:

España: **10.16.0.0/12**, es decir que a la totalidad de nuestro país podemos asignarle **1.048.574** hosts, siendo el primero de ellos dirección IP 10.16.0.1 y el último el 10.31.255.254. En nuestra opinión, es una cantidad más que suficiente de hosts. A su vez, si prestáis atención, podéis ver que están comprendidas en este rango, todas las provincias y sus sucursales.

La última posibilidad, que ya no graficamos, pues sería exactamente igual al diseño de España, es que, si nuestra empresa tiene sedes en diferentes países, podemos seguir escalando nuestra arquitectura de forma totalmente flexible respetando esta misma lógica. Por ejemplo, podría ser, **Francia: 10 32.0.0/12**, **Alemania: 10.48.0.0/12**, **Italia: 10:64.0.0/12**, y así sucesivamente.

Lo más importante desde el punto de vista de Ciberseguridad.

El hecho de diseñar una arquitectura de red que respete estrictamente una lógica como la de nuestro ejemplo, o cualquier que tenga en cuenta este tipo de detalles en su coherencia, nos facilita enormemente la supervisión y monitorización de la misma.

Es decir, tanto los **SOC** (Scurity Operation Center), como los **NOC** (Network Operation Center), que los desarrollaremos con todo detalle más adelante, ante cualquier anomalía o incidente de seguridad, de forma inmediata al ver pasar cualquier dirección IP, en cuestión de segundos sabrán que se trata de un vínculo provincial, ínter provincial, de una LAN concreta, etc.

Esta velocidad en la identificación de un dirección IP, nos da la capacidad de reacción necesaria para tratar estos problemas en un tiempo adecuado y poder minimizar el impacto que nos pueden producir.

En nuestra experiencia, este hecho es fundamental en la capacidad de reacción, pues hemos visto un sinnúmero de situaciones, en las que la demora en identificar dónde estaba focalizado el problema, desencadenó en daños sumamente importantes, que podrían haberse minimizado o inclusive evitado, si se contara con una metodología como la que estamos presentando. De verdad, aunque tal vez aún no lo valoréis en toda su magnitud, os aseguramos que este tipo de diseño, es vital para el ciclo de vida de la Ciberseguridad de nuestra redes.

Si deseáis ir avanzando en los conceptos de SOC y NOC, tenéis a vuestra disposición los siguientes videos:

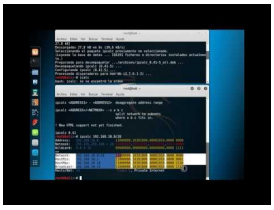
- **NOC y SOC (Network y Security Operation Center)**

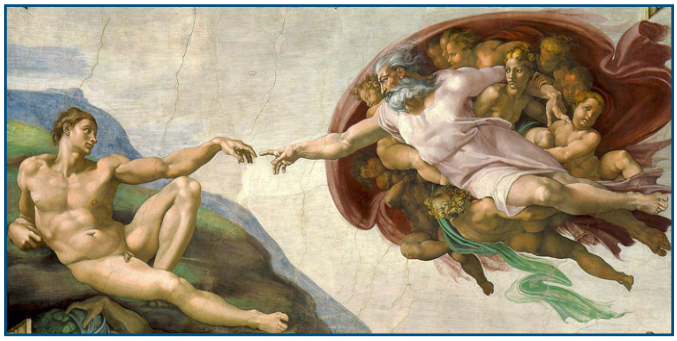
- **Ciberseguridad: empleo de SOC y NOC**

Nuevamente os recomendamos que para este tipo de diseño, no dejéis de lado el empleo de la herramienta "**ipcalc**" que os será de muchísima utilidad.

Recordad el video:

Ejercicios de direccionamiento IP con la herramienta "ipcalc" sobre Kali





Para remarcar una vez más lo importante que es poder diseñar este tipo de arquitecturas. Si alguna vez os sentís como Dios, y tenéis la dicha de crear esto desde cero, como hablamos en la charla anterior, tomaros el tiempo que haga falta, pero pensad bien cada uno de los potenciales y futuros emplazamientos, para poder crear una estructura que, por muchos, y muchos años más, pueda seguir prestando servicio, de forma sólida y coherente, y sobre todo minimizando los riesgos y generando plataformas sencillas de monitorizar, en las cuáles cada vez que tenga que incorporar nuevas funcionalidades, como **firewalls** e **IDSs** (Intrusion Detection System), la gestión de sus reglas sean fácilmente entendibles pues, será coherente, desde, y hacia donde, se dirigen nuestros flujos de tráfico y control.

Volver al índice

www.darFe.es

Charla 47

Routers (parte I)

Enlace al Video:

Resumen:

Este tema, por su importancia, lo dividiremos en dos capítulos, este y el siguiente.

Los **routers**, son los dispositivos por excelencia del nivel de red. Son los que nos permiten llegar a todos los lugares del planeta, "enrutando" nuestros **datagramas IP**.

En este capítulo, describiremos su funcionamiento, presentaremos las marcas más conocidas, sus modelos y finalmente, desarrollaremos puntos clave a tener en cuenta para una gestión segura de los mismos.

Descripción detallada

Esta charla, se basa en el Capítulo 5. Routing, de nuestro libro "**Seguridad en Redes**".

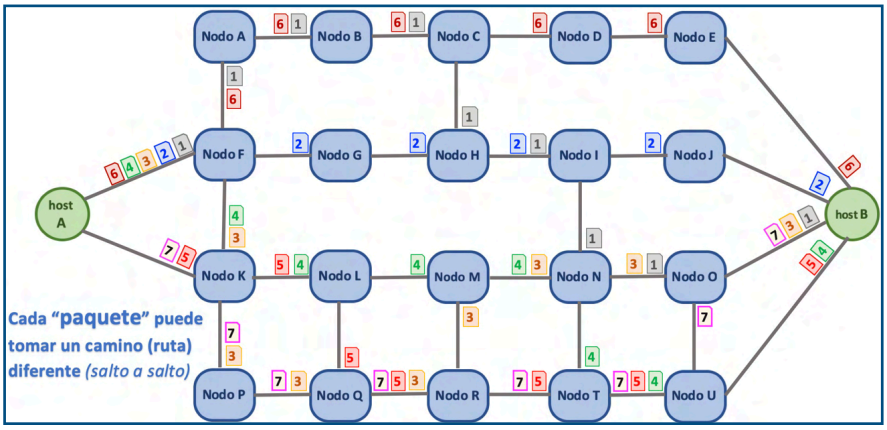
En las charlas anteriores y también en el Capítulo 5 del libro "**Seguridad por Niveles**" hemos desarrollado todos los conceptos relacionados al protocolo IP que es el núcleo del nivel de red. Ahora ya podemos abordar esta capa desde el punto de vista de las medidas de seguridad que debemos considerar para fortalecer los dispositivos encargados de gestionar el nivel 3.

El dispositivo por excelencia en la pila TCP/IP de este capítulo es el "**Router**", cuya misión fundamental es el manejo de las "rutas" IP y su capacidad de conmutación de paquetes a través de la red, siempre basado en el encabezado del protocolo IP, toda esta tarea es la que denominaremos **routing**. Como ya nos ha sucedido varias veces, esta vez tampoco es la excepción, y veremos que los routers actuales tiene capacidad de abordar también funciones de otras capas de la pila TCP/IP que superan la actividad de routing, en estos casos también nos detendremos aunque exceda este concepto.

Definición de Routers

Si aún recordamos la **charla 41,** cuando presentamos el protocolo IP, uno de los puntos de mayor importancia era las redes de:

- Conmutación de circuitos
- Conmutación de paquetes



Para ejecutar la técnica de "**Conmutación de paquetes**" el único elemento de juicio que se tiene para ello, es el campo "Destination Address" del encabezado IP de cada paquete que le llega (no existe otro). En la configuración de cualquier dispositivo de red se poseen más datos, como son las máscaras de red, las interfaces, los protocolos de enrutado (estáticos o dinámicos) las rutas que conoce y las que no, el o los Gateway, las prioridades o no que debe darle a un paquete, etc. Toda esta serie de parámetros serán los que un router es capaz de controlar de forma nativa

Con lo descripto, acaban las funciones nativas de un router. A partir de esto, comienzan a aparecer funcionalidades o servicios adicionales, pero lo importante es

tener claro que esto son un "valor agregado" en un router, su función básica y primordial es la de: **enrutar**.

Un router opera siempre en el nivel 3 (red) del modelo de capas:

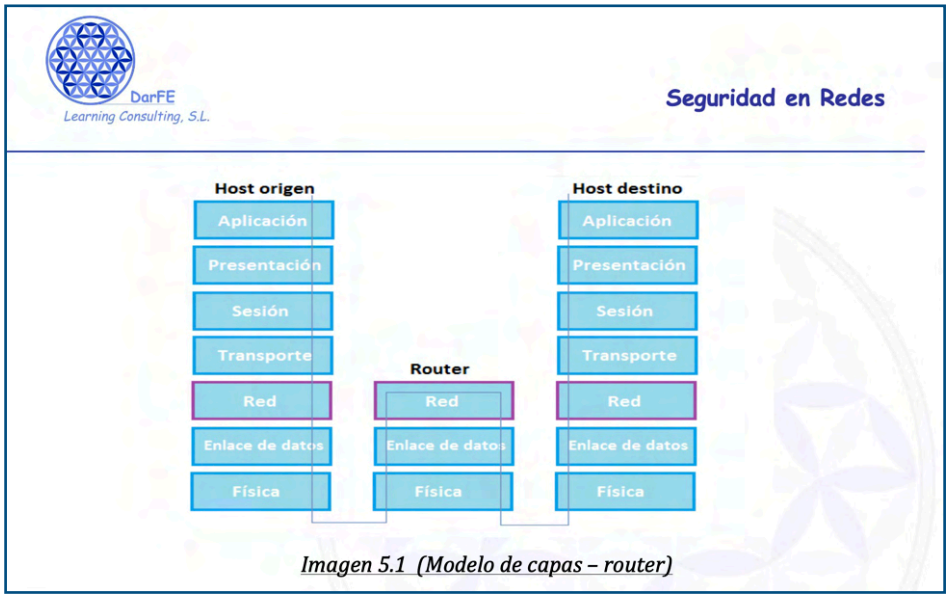


Imagen 5.1 (Modelo de capas – router)

Como podemos ver en la imagen de la derecha, cuando una aplicación de un host origen desea comunicarse con un host destino, el nivel de red, genera el encabezado del protocolo IP, que convinimos en llamarlo "**datagrama**".

Al pasar por cualquier router de la red que comunica a ambos hosts, este dispositivo, únicamente analiza el nivel de red, es decir no tiene por qué seguir subiendo en la pila TCP/IP, solo "**desencapsula**" en encabezado IP.

Siguiendo con el libro "**Seguridad en Redes**", en el mismo, se propone clasificar los router de la siguiente forma, la cual seguramente en otras bibliografías podéis encontrarlo diferente, pues esta es una visión estrictamente nuestra.

a. Router crítico: aquel que sostiene un porcentaje muy alto del tráfico de la red.

   En esta categoría de forma sencilla podemos pensar en tres tipos:

   - Core (voz, datos y señalización)
   - Router Reflector
   - Frontera de Banda Ancha (Internet)

b. Router de criticidad Media: aquel que sostiene un porcentaje inferior al 20%.

   Podemos pensar en (PE, interconexión sedes, Anillos Metro Ethernet).

c. Router de baja criticidad: en general los internos o de acceso (Accesos ADSL, MacroLAN, pequeños clientes o partners (CPEs), zonas de servicio no críticas).

El detalle de cada uno de ellos, podéis encontrarlo en el mencionado libro. Lo que deseamos poner de manifiesto aquí, es que cuando se comienza a diseñar una estrategia de Ciberseguridad sobre estos dispositivos, como es lógico, el punto de partido deben ser los **router críticos**, a medida que voy mejorando mi ciclo de vida de Ciberseguridad, podré continuar con los de menor criticidad. Por esta razón es que consideramos que esta clasificación, es provechosa con nuestra temática de Ciberseguridad.

A nivel redes IP, hay dos grandes marcas que son líderes de mercado en esta gama (**Juniper** y **Cisco**), aunque ahora está entrando de forma muy agresiva **Huawei**.

A título de referencia mencionamos los modelos más frecuentes que encontraremos hoy en grandes redes:

- Familia Cisco: Se puede profundizar en cada uno de ellos en la página Web de Cisco (http://www.cisco.com/c/en/us/products/index.html):

  a) Serie Cisco CRS (Carrier Routing System).

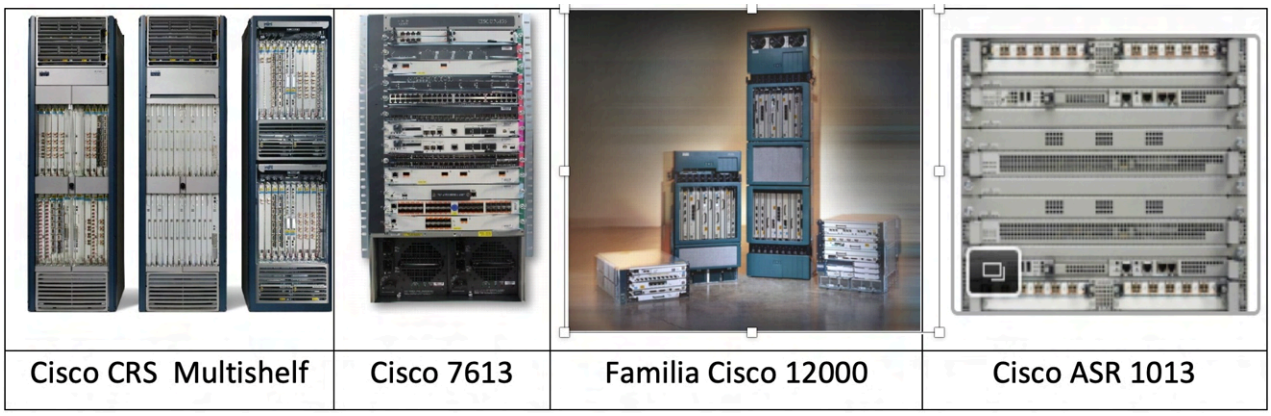
  b) Serie Cisco 7600.

  c) Serie Cisco 12000 XR.

  d) Serie Cisco ASR 1000 y 9000 (ASR: Aggregation Services Routers).

  e) Para redes de menor tamaño están los llamados “Small Business Routers” de las familias 800, 1900 y 2900.

  f) Familia Catalyst (series 6500) y Nexus (serie 7000): En realidad estas dos familias son eminentemente Switchs, pero en la actualidad ofrecen un sinnúmero de posibilidades para configuraciones de niveles superiores.



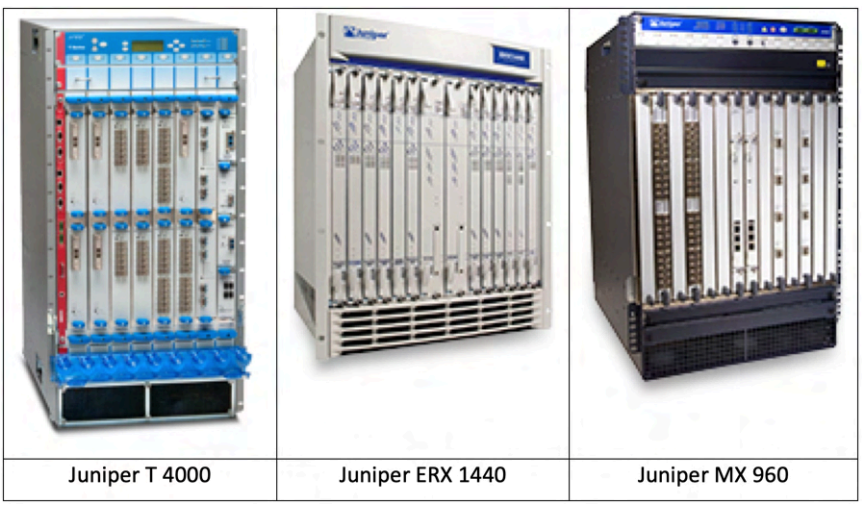
Cisco CRS Multishelf	Cisco 7613	Familia Cisco 12000	Cisco ASR 1013

- Familia Juniper: Se puede profundizar en cada uno de ellos en la página Web de Juniper (http://www.juniper.net/us/en/products-services/routing/):

  a) Series Juniper T.

  b) Series Juniper ERX.

  c) Serie Juniper MX.



Juniper T 4000	Juniper ERX 1440	Juniper MX 960

Un caso especial que debemos mencionar son los **Router Reflector** (RR).

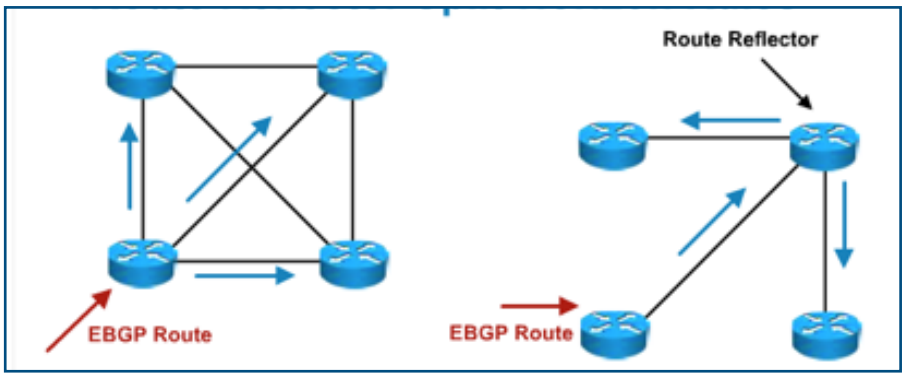
El concepto de router reflector podríamos pensar que nace con el protocolo **BGP** (Border Gateway Protocol) que como ya hemos mencionado, se trata de un protocolo de enrutamiento dinámico para sistemas autónomos (**AS**) y, en definitiva, debe ser el protocolo más importante que comunica las troncales de Internet, de hecho a cada **ISP** (Internet Service Provider), **IANA** (Internet Authority Numbers Asign) le asigna grandes rangos de direcciones IP agrupados dentro de un AS, y este valor será el más importante que se considerará para las rutas que controlan todo Internet.

Este protocolo dinámico debe mantener actualizadas las tablas de ruta de estos grandes routers con bastante frecuencia, para poder hacerlo cada uno de ellos necesitaría conocer el estado que posee de las mismas cada uno de sus "vecinos" (Neighbor). Si no existieran los Router Reflector, esta comunicación debería ser una **malla** "todos con todos", lo cual evidentemente desgastaría en exceso todo los vínculos de comunicación. Justamente para resolverlo es que todos los router BGP miran o dirigen su mirada (peer) hacia estos RR que son los encargados de recibir los cambios de estas rutas y responder ante cualquier consulta de esta "comunidad de vecinos" o vecindario (neighborhood) a lo que podríamos llamar como "**routers clientes**" de este RR. Cabe mencionar que el concepto de "peer" también se suele entender como "par", es decir un router que está conectado a este sistema, o que es cliente del mismo, o que es el otro extremo de esta comunicación (a nivel internacional el tráfico de "peering" son los convenios que firman entre carriers para transportar información de otros carriers a través de sus propios vínculos con condiciones económicas especiales y/o gratuito).

El concepto de AS puede ser dividido en áreas o conjuntos de clientes que se denominan "**cluster**", donde cada cluster debe tener al menos un RR.

En la actualidad estos RR también se integran o emplean con otras familias de protocolos dinámicos (iBGP y eBGP, IS-IS, OSPF, MPLS) trabajando de la misma forma.

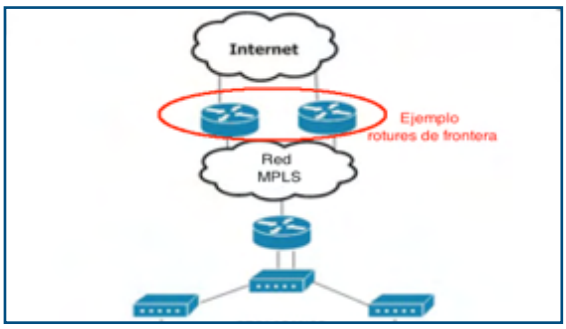
En la imagen de la derecha, podemos apreciar, justamente, cómo se simplifican los enlaces empleando estos RR. Tened en cuenta que en este caso sólo se trata de cuatro nodos, si la red contara con decenas, centenas o miles de routers, como es el caso de algunos AS, una red malla es inaplicable.



Otro caso particular son los "**Routers de frontera**".

Se trata de cualquier router que posea interfaces conectadas a otro dispositivo que no es de responsabilidad de la propia red, o que finaliza túneles de cualquier tipo con dispositivos también externos a la misma.

Un aspecto que también puede considerarse es que el mismo intercambie tráfico hacia estas redes externas a la organización.



Cómo analizar la configuración y seguridad de un Router.

Esta actividad por ser una de las más importantes de nuestro trabajo de Ciberseguridad en redes, presentaremos la parte teórica y conceptual y en la charla siguiente veremos varios ejemplos y ejercicios prácticos.

En una gran red, el trabajo, área o responsable de seguridad en general no es el mismo que el que administra la red, de hecho debería estar claramente separado para no ser "**juez y parte**". Se evidencia mucho esta separación en grandes redes, cuando la actividad la cumple el mismo área y la rutina del día a día va llevando a los responsables de red a crear o modificar, rutas, listas de control de acceso, reglas de firewall, etc.. y la seguridad se va degradando cada vez más.

En estos párrafos, trataremos este tema como si fuera abordado por una persona responsable de seguridad o auditoría, y que justamente no es quien diseña, planifica y opera la red, por lo tanto su labor es totalmente independiente a la gestión de red, de esta forma nos permitirá hacer un trabajo mucho más detallado. Si no es este el caso del lector, y desempeña varios de estos roles a la vez, es un my buen ejercicio, abordar este tema, intentando enfocarlo desde los diferentes perfiles que se tratarán aquí para poner de manifiesto todas las actividades que no debería dejar de lado, independientemente que su responsabilidad sea sobre todas ellas.

En la práctica el trabajo comienza por comenzar metódicamente a comprender la arquitectura y funcionamiento de la red, realizando lo siguiente:

- Solicitar y recolectar información previa sobre estos dispositivos al área responsable.
- Analizar, con todo el detalle posible, la arquitectura de la red en cuestión.
- Solicitar una presentación (si se desea) por parte de los responsables de "Planificación" y/o "Ingeniería" de la red.
- Planificar y organizar entrevistas con los administradores de, al menos, uno de cada uno de los tipos mencionados, o los que consideremos clave en esta revisión de seguridad. Cada una de estas entrevistas deberán ser eminentemente técnicas y con conexión al dispositivo, o plataforma, que se va a analizar.
- Sentarnos al lado de cada administrador, en su puesto de trabajo, o desde el lugar que el prefiera, pero con acceso al dispositivo.
- Solicitarle que "loguee" la sesión (para que posteriormente nos entregue toda la actividad realizada, donde como veremos más adelante, figurarán todos los comandos ejecutados y los parámetros de configuración).

- Avanzar con nuestro análisis de su configuración (y "subliminalmente", nuestra evaluación acerca del conocimiento que este administrador "posee" y "comparte" de ese dispositivo).

El detalle de cada uno de estos puntos, puedes verlo en el libro "**Seguridad en Redes**"

Como norma general en la revisión de seguridad de cualquier tipo de redes (y sus dispositivos), nuestro trabajo, podríamos resumirlo de forma práctica en los siguientes pasos:

1) Recolección y análisis previo de su documentación (planos, arquitecturas, nodos, dispositivos, fabricantes, responsables, funciones, obligaciones, etc.
2) Entrevista con responsables del área de "Planificación/ingeniería" y "Operación/gestión/administración / mantenimiento".
3) Sentarnos en un puesto de trabajo de uno, dos o tres administradores de sus nodos principales, para centrar la atención en lo siguiente:
   - ¿Conoce al detalle la infraestructura/plataforma/red?
   - ¿Posee a mano o tiene acceso a los mapas/planos?
   - Se encuentra claramente documentado su trabajo o actividad..... Este tema es fundamental para evitar la "**Imprescindibilidad**": No puede existir PERSONAL IMPRESCINDIBLE en estas tareas. Nuestra experiencia al respecto es que esta es una problemática muy frecuente, deberíamos hacer un esfuerzo en minimizarlo y erradicarlo lo antes posible, pues es un foco de problemas GRAVE.

     Todo esto se soluciona, cuando su tarea se comparte con otros, se documenta al detalle, y se trabaja de forma transparente (*y no egoísta*) dentro del equipo de trabajo. Insistimos en poner como centro de atención este tema y lo penalicemos rigurosamente cuando no se esté cumpliendo.

     NOTA: Antes de su conexión al, o los dispositivos, deberíamos pedirle que "**Loguee**" esta sesión para que luego nos la pueda pasar para analizarla a posteriori. De no ser posible, le pediríamos que luego nos pase los archivos de configuración de ese elemento.
   - ¿Cómo es su metodología de conexión?, ¿Qué protocolos emplea?, ¿Responde a lo que está documentado, o tiene sus propios mecanismos / rutas / herramientas?.
   - ¿Con qué usuario se conecta?, ¿Local, corporativo, el de un Tacacs o Radius, LDAP, etc?
   - ¿Conoce las configuraciones, comandos, significado de los mismos?
   - ¿Se desenvuelve con soltura una vez conectado al dispositivo?
   - ¿Conoce cómo hacer una copia de respaldo y dónde hacerla?
   - ¿Qué haría si debiera recuperar un dispositivo?
   - ¿Es consciente de las medidas de seguridad que deben aplicarse a ese dispositivo?, ¿recibió formación en seguridad?
   - ¿Cuál es el flujo que sigue en la práctica para cualquier tipo de modificación en las configuraciones?, ¿tiene registros de ello?
   - ¿Guarda archivos de configuración o Logs en su ordenador local, o en otros dispositivos? (en particular que no estén documentados).
   - ¿Cómo procede en la práctica ante cualquier tipo de incidencia?
   - ¿Cómo es su administración de Logs?, ¿los conoce?, ¿los controla o mira frecuentemente?, ¿los envía hacia algún otro sitio?
4) A posteriori de la entrevista, deberíamos analizar los archivos de configuración que nos han entregado verificando el nivel de seguridad de los mismos. Esta actividad es la que iremos desarrollando a continuación y con más detalle para cada tipo en particular.

Volver al índice

www.darFe.es

Charla 48

Routers (parte II) - Crack de usuarios locales

Enlace al Video:

Resumen:

En la charla de hoy, presentamos dos errores muy frecuentes en los routers, que hemos podido detectar en nuestras auditorías de Ciberseguridad. **Usuarios locales** y **algoritmos débiles** en sus contraseñas.

Desarrollaremos técnicamente cómo analizar estos desde **Kali**, a través de comandos sencillos y el empleo de dos importantes herramientas para descifrar estas contraseñas: "**ciscocrack**" y "**John the Ripper**"

Descripción detallada

Esta charla, nuevamente se basa en el Capítulo 5. Routing, de nuestro libro "**Seguridad en Redes**".

Vamos a ver un tema muy interesante que es cómo "**crackear**" (descifrar) las contraseñas de un router cuando en el mismo se comete el **grave error** de emplear usuarios locales, y a su vez no se emplean contraseñas robustas.

Este error, que puede pareceros que no se comente, está presente en una altísimo porcentaje de los routers que hemos auditado en estos años. Como iremos viendo, hay administradores que no son conscientes del empleo de algoritmos robustos, como tampoco valoran la necesidad de validar estos dispositivos contra un servidor de autenticación y acceso externo, como puede ser un servidor TACACS, RADIUS o LDAP (estos temas los desarrollaremos más adelante).

El crackeo de contraseñas de dispositivos de red, sin lugar a dudas, lo empleará cualquier intruso o mal intencionado para avanzar en su proceso de "**fingerprinting**" y "**footprinting**", temas que veremos más adelante pues son fundamentales. En nuestro caso, trabajaremos para "el lado del bien" y justamente, auditaremos esos dispositivos como medida preventiva para anticiparnos a que pueda aprovecharlo "el lado del mal". Por esta razón, las auditorías de Ciberseguridad son actividades periódicas que jamás debemos dejar de lado.

En el trabajo práctico de este capítulo, trabajaremos sobre routers Cisco, pero la misma metodología aplica a Juniper, Huawei, ZTE, etc.

A continuación presentamos un fichero de configuración real de un router que está en producción, que presenta varios aspectos de mejora y que tomaremos como ejemplo para todo este trabajo. Este archivo de configuración podéis encontrarlo en la página 192 del libro "**Seguridad en Redes**".

```
2960_ace#show run

Building configuration...
Current configuration : 858 bytes
!
! Last configuration change at 16:12:07 America Wed Jun 17 2016 by ace
! NVRAM config last updated at 16:12:08 America Wed Jun 17 2016 by ace
!
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
no service password-encryption
!
hostname 2960_ace
!
logging buffered 163846
no logging console
```

```
no logging monitor
enable secret 5 $120h/S3d//2w*wQ08NrFk9O
!
username alejandro secret 5 $1$qJO4B8A5$Yl.S6q227itWNzpanEU6S.
username  ace privilege 7 password 7 13061E010803
aaa new-model
!
aaa authentication login default  group tacacs+ enable
aaa authorization config-commands
aaa authorization exec default  group tacacs+ local
aaa authorization commands 5 default group tacacs+
aaa authorization commands 12 default group tacacs+
aaa authorization commands 15 default group tacacs+
!
!
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
!
ip ssh time-out 60
ip ssh authentication-retries 2
!
interface FastEthernet0/1
 description PISO-1
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/2
 description PISO-2
 switchport access vlan 200
 switchport mode access
 
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan100
 ip address 10.1.1.1 255.255.0.0
 no ip route-cache
!
interface Vlan200
 ip address 10.1.2.1 255.255.0.0
 no ip route-cache
!
ip default-gateway 10.1.1.252
no ip http server
no ip http secure-server
logging trap debugging
```

```
logging facility syslog
logging source-interface Vlan49
logging 10.1.2.10
logging 10.1.2.12
access-list 2 permit 10.1.2.24
access-list 2 permit 10.1.2.21
snmp-server community private RW
snmp-server community public RO
snmp-server community prueba RW 2
snmp-server trap-source Vlan200
snmp-server packetsize 1024
snmp-server location sede_central
snmp-server enable traps tty
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps power-ethernet police
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
snmp-server host 10.1.2.21 version 3
snmp-server host 10.1.2.24 version 3
tacacs-server host 10.1.2.34 key 123456789
tacacs-server host 10.1.2.35 key 123456789
tacacs-server directed-request
!
control-plane
!
banner motd ^C#####################################
#   AVISO: para acceder a este sistema
#   necesita la autorización correspondiente
#   El acceso no autorizado o el uso indebido
#   esta prohibido y es contrario a la
#   legislacion vigente. Toda actividad
#   sobre este sistema sera monitorizada.
#####################################
^C
!
line con 0
 password qwerty
line vty 0 4
 session-timeout 5
 privilege level 15
```

```
 authorization commands 5 default
 authorization commands 12 default
 authorization commands 15 default
 login authentication default
 transport input ssh
line vty 5 15
!
ntp clock-period 36029500
ntp server 10.1.2.46
end
2960_ace#
```

Esta configuración, que como dijimos, se corresponde a un caso real en producción, es un router **Cisco** modelo 2960. Se trata de una familia de routers de tipo pequeño, pero configurable, y que se emplea muchísimo como router de acceso o router de frontera hacia Internet, en los servicios ofrecidos a empresas.

Sobre esta configuración trabajaremos desde nuestro "**Kali Linux**", para lo cual, os recomendamos que abráis una interfaz de comandos (consola). **—>** 

Una vez en ella, que peguéis esta configuración en vuestra máquina virtual y lo llaméis, por ejemplo, "**2960_ace.txt**", con el editor "**vi**", o con el prefiráis.

Cuando realizamos auditorías de seguridad sobre este tipo de dispositivos, lo primero que debemos hacer, es solicitarle al responsable de los mismos, que nos envíe los ficheros de configuración, o los backups de los mismos, para poder analizarlos con todo el detalle. Como estamos realizando una auditoría de seguridad, no pueden negarse a este tipo de requerimientos.

También otro tipo de método de obtención de estas configuraciones, suele ser realizando "**análisis de tráfico**" de las redes, por medio de capturas de tráfico (con Wireshark, tcpdump, o tshark), y al detectar transferencias inseguras, por ejemplo por medio del protocolo **FTP** (File Transfer Protocol), por medio de **SNMP** (Single Network Monitor Protocol) en versiones previas a la 3, o si los gestionan por medio de "**telnet**", todos estos protocolos los veremos más adelante con todo detalle. Cuando se emplean este tipo de protocolos, al capturarlos, veremos pasar perfectamente todo lo que esté circulando como datos en texto plano, con lo que, es tan sencillo con realizar el seguimiento de esta sesión (que es una de las opciones más simples de Wireshark), y allí veremos pasar la totalidad de estos ficheros de configuración, exactamente iguales que el que estamos mostrando como ejemplo.

Volviendo a nuestro **Kali Linux**, una vez que tengamos esta configuración, como un fichero de texto, lo siguiente sería buscar la existencia de usuarios, lo podemos hacer, por ejemplo con un sencillo comando "**grep**", tal cual se muestra a continuación.

$grep "user" 2960_ace.txt

Con esta sencilla instrucción en "**bash**", le estamos diciendo a Kali, que busque la ocurrencia de la palabra "**user**" dentro del fichero "**2960_ace.txt**".

Si ejecutamos este comando, sobre la configuración sobre la que estamos trabajando (2960_ace.txt), la interfaz de comandos nos devolverá:

username alejandro secret 5 1qJO4B8A5$Yl.S6q227itWNzpanEU6S.
username ace privilege 7 password 7 13061E010803

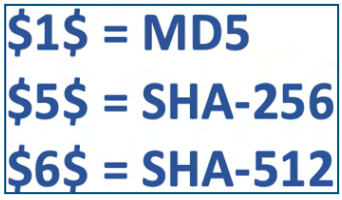
En nuestra interfaz de comandos, lo veríamos tal cual se presenta en la imagen de abajo.

```
┌──(acorletti㉿kali)-[~]
└─$ grep "user" 2960_ace.txt
username alejandro secret 5 $1$qJO4B8A5$Yl.S6q227itWNzpanEU6S.
username  ace privilege 7 password 7 13061E010803
```

Si prestamos atención, nos presenta dos usuarios: "**alejandro**" y "**ace**".

El primero de ellos (alejandro), nos indica que es "**secret 5**" y su contraseña comienza con "**$1**". Este **$1**, nos está indicando que emplea el algoritmo de resumen "**MD5**" para almacenar la contraseña.

Como podemos ver en la imagen de la derecha, podremos encontrar, al menos estos tres algoritmos: **MD5** (Message Digest 5), **SHA-256** (Secure Hash Algorithm) y **SHA-512**.

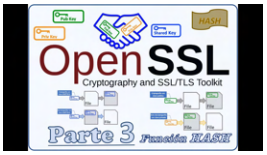


Estos algoritmos, son los que emplean muchos sistemas operativos para almacenar las contraseñas de forma segura. Se tata, nuevamente, de la función "**Hash**", o resumen.

En la charla 31, cuando desarrollábamos el tema de WiFi, ya presentamos algo sobre **Hash**. En concreto, se trata de algoritmos matemáticos, que toman como entrada un fichero de cualquier longitud y nos entregan como resultado un nuevo fichero de longitud siempre fija, generan fortaleza para el control de integridad; es decir, nos garantizan que el fichero de entrada original no ha sido alterado. Por esta razón, en el proceso de autenticación es de vital importancia. La función "**Hash**", es tan importante, que más adelante le dedicaremos un buen tiempo para que la entendáis con todo lujo de detalle, por ahora, sed pacientes y quedaros con estas breves ideas.

Si queréis ir adelantando algo más sobre el tema, en la Charla 3 de nuestro "**Ciclo OpenSSL**", lo desarrollamos con mucho detalle.

OpenSSL (Parte 3) - Función Hash:

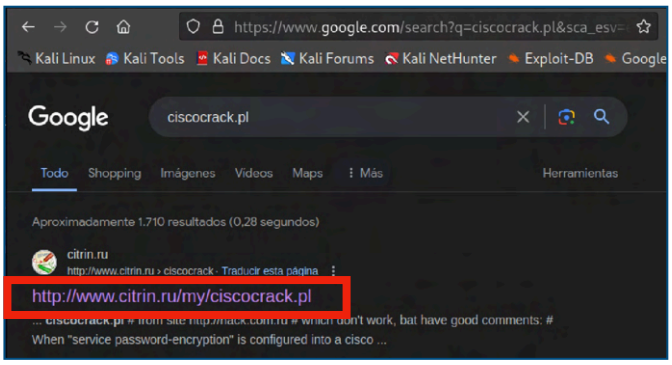


En el caso que estamos viendo del usuario "alejandro", nos indica que emplea **MD5**, esta función Hash tiene una longitud fija de **128** bits, lo que hoy en día no es recomendable emplear pues es muy fácil de atacar, como veremos a continuación. Todas las recomendaciones y buenas prácticas descartan su uso. Cuando configuremos cualquiera de estos dispositivos de red, y también en sistemas Linux, lo que se recomienda es el empleo de **SHA-512** (**$6**) que como su nombre lo indica tiene una longitud fija de **512** bits.

Yendo más al detalle de los dos usuarios encontrados, el otro es "ace", que como podemos ver, nos indica que emplea "**password 7**", esto ya es un pecado mortal imperdonable. Hace más de 20 años que Cisco viene indicando que no debe usarse. Sin embargo, reiteramos nuevamente, os sorprenderéis cuando empecéis a auditar este tipo de elementos, por la cantidad de fallos de este estilo que sin lugar a dudas vais a encontrar.

Para comenzar, analizaremos, justamente esta password 7 de Cisco.

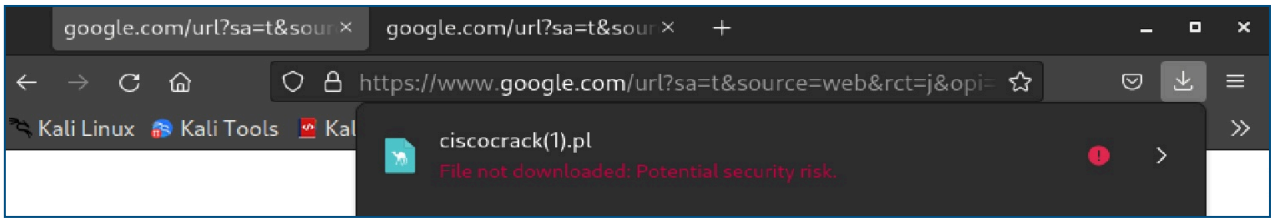
En nuestro ejemplo de Kali Linux, vamos a trabajar con una herramienta, nuevamente muy sencilla que se ejecuta también por línea de comandos que se llama "**ciscocrack**", aunque podéis encontrar cientos de ellas, e inclusive páginas Web de crackeo de password 7, en las que online, tu pegas esa contraseña y te la descifrará en menos de un segundo.



Para instalar "**ciscocrack.pl**", abrimos nuestro navegados de Kali y desde Google, buscamos este nombre.

Elegimos cualquiera de las opciones, en nuestro caso, por ejemplo la primera de ellas que hemos remarcado en **rojo**.

Si hacemos doble "click" en ese enlace, directamente se nos abrirá la ventana para descargarlo.



En nuestro caso, por defecto, el navegador de nuestro Kali, lo descargó en el directorio **/home/ace/Downloads**, como lo podemos ver en la imagen de abajo. Recordad que las extensiones "**.pl**", se tratan de archivos realizados con el lenguaje de programación "**Python**". Este tipo de ficheros, no necesita ser instalados, y Linux por defecto, ya trae un intérprete para que podamos ejecutarlo directamente.

El único detalle que debemos tener en cuenta es que, tal cual podemos ver en la imagen que sigue, este fichero NO tiene aún permiso de ejecución, sus atributos son "**-rw-r—r—**". Recordad que Linux identifica estos atributos como "**r**": read, "**w**": write, y ""**x**": execute, donde los tres primeros **"rxw"** pertenecen al usuario de ese fichero, los segundos **"rxw"** al grupo, y los últimos **"rxw"** a los demás o al resto.

```
┌──(acorletti㉿kali)-[~/Downloads]
└─$ ls -l
total 74572
-rw-r--r-- 1 acorletti acorletti        0 Apr 19 10:55 'ciscocrack(1).pl'
-rw-r--r-- 1 acorletti acorletti     2373 Apr 19 10:53  ciscocrack.pl
```

Para poder transformar en ejecutable debemos modificar estos permisos. Lo haremos con el siguiente comando:

$ chmod 744 ciscocrack.pl

Una vez ejecutado, podemos verificar que sus permisos han sido modificados para que pueda ser ejecutado por el usuario “acorletti” en nuestro caso, por supuesto que para vosotros será otro. En la imagen que sigue, podemos ver esta secuencia de pasos, y a su vez, si prestamos atención, también veremos que el fichero “**ciscocrack.pl**" ahora se nos presenta en color **verde**, lo que nos indica que nos permite su ejecución. Por supuesto, también nos lo demuestran sus atributos que ahora son “**-rwxr—r—**”

```
┌──(acorletti㉿kali)-[~/Downloads]
└─$ chmod 744 ciscocrack.pl

┌──(acorletti㉿kali)-[~/Downloads]
└─$ ls -l
total 74572
-rw-r--r-- 1 acorletti acorletti        0 Apr 19 10:55 'ciscocrack(1).pl'
-rwxr--r-- 1 acorletti acorletti     2373 Apr 19 10:53  ciscocrack.pl
-rw-r--r-- 1 acorletti acorletti    39520 Aug 27  2023  hans-1.1.tar.gz
drwxr-xr-x 2 acorletti acorletti     4096 Nov 29 11:45  volatility_2.5.linux.s
tandalone
-rw-r--r-- 1 acorletti acorletti 32808756 Nov 29 11:41  volatility_2.5.linux.s
tandalone.zip
-rw-r--r-- 1 acorletti acorletti 43502788 Nov 29 16:04  zeus.vmem.zip
```

Ahora que ya tiene los permisos correspondientes, solo nos queda copiar la password 7 de ace (13061E010803), y ejecutar el siguiente comando:

./ciscocrack.pl 13061E010803

En menos de un segundo, nos resolverá cuál es esta contraseña. En este caso es tan trivial como “cisco” pero aunque hubiese sido la más complicada del planeta, también la habría resuelto en menos de un segundo, pues el fallo, está en el algoritmo mismo, es decir, aquí no se trata de un proceso de fuerza bruta, sino de debilidad matemática.

```
┌──(acorletti㉿kali)-[~/Downloads]
└─$ ./ciscocrack.pl 13061E010803

cisco
```

Estamos seguros, que si os empezáis a dedicar a realizar este tipo de auditorías, alguna vez os cruzaréis con “password 7” y hasta con la contraseña “cisco”… aunque en estos momentos, os cueste creerlo.

Avancemos ahora sobre el otro usuario que hemos encontrado, es decir sobre:

username alejandro secret 5 1qJO4B8A5$YI.S6q227itWNzpanEU6S.

Como ya hemos mencionado, en este caso, se trata de un “**Hash**” que responde al algoritmo “**MD5**” de **128** bits de longitud.

Para descifrar este tipo de Hash, emplearemos ahora una de las mejores herramientas del mundo para crackeo de contraseñas. Esta es “**John the Ripper**”, conocida sencillamente como “**John**”.

Es otra de las maravillas que ya trae incorporado nuestro **Kali**.

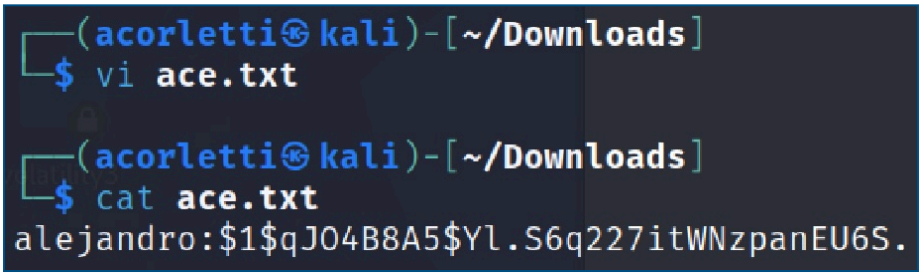
Para poder ejecutarla, debemos, en primer lugar, generar un fichero en el formato que emplea John.

Lo haremos de la siguiente forma. Copiaremos la línea completa: username alejandro secret 5 1qJO4B8A5$Yl.S6q227itWNzpanEU6S.

Una vez más, la pegaremos en un fichero de texto, por ejemplo, "**ace.txt**". Una vez creado este fichero, modificaremos esta línea, borrando los siguientes caracteres: "**username"** y también: "**secret 5"**. Luego separamos con **":"** las dos partes que nos quedaron, para que de una única línea con el siguiente formato:

alejandro:1qJO4B8A5$Yl.S6q227itWNzpanEU6S.

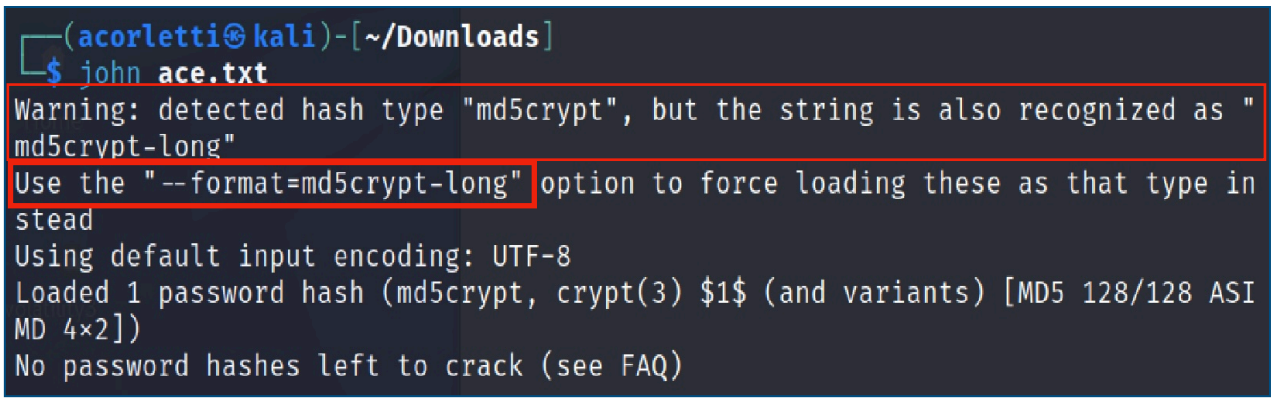
Una vez que la línea nos quede como la que figura arriba, guardaremos este fichero y nos quedará como se muestra en la imagen de la derecha.



La ejecución de "**John**" es muy sencilla, solo debemos insertar por línea de comandos la siguiente instrucción:

$john ace.txt

Intencionadamente, hemos querido ejecutarla sin ninguna opción adicional, para que podáis ver cómo John inmediatamente detecta que se trata de una variante de MD5 y nos presenta el mensaje que pegamos aquí abajo.



Nos está indicando que detecta "**md5crypt**" pero que esta cadena es también reconocida como "**md5crypt-long**", por ello nos recomienda que usemos la opción "**—format=md5crypt-long".**

Cumpliendo entonces con lo que John nos está recomendando en este mensaje, ahora sí ejecutaremos:

$john ace.txt --format=md5crypt-long

Con este comando nos responderá lo que se presenta en la siguiente imagen.

```
┌──(acorletti㉿kali)-[~/Downloads]
└─$ john ace.txt --format=md5crypt-long
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64]
)
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for
 performance.
ale              (alejandro)
1g 0:00:00:00 DONE 1/3 (2024-04-19 12:16) 100.0g/s 2100p/s 2100c/s 2100C/s ale
j..lej
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Como se aprecia en la imagen superior, pudo descifrar la contraseña del usuario "**alejandro**", que es "**ale**". También hemos resaltado en rojo que lo hizo (DONE) en menos de un segundo.

Una vez más, se trata de un ejemplo trivial, solamente para que podáis seguir la secuencia de este tipo de trabajos, pero tened en cuenta que una contraseña de una longitud cercana a los ocho caracteres alfanuméricos, empleando uno o dos caracteres especiales, en pocas horas también la descifraría si se emplea MD5.

John, va almacenando las contraseñas que descifra en el fichero "**john.pot**", que suele encontrarse dentro del directorio "**home**" de ese usuario, y en la ruta "**.john**" dentro del mismo, como podemos verlo a continuación.

```
┌──(acorletti㉿kali)-[~/.john]
└─$ pwd
/home/acorletti/.john

┌──(acorletti㉿kali)-[~/.john]
└─$ ls -l
total 24
-rw------- 1 acorletti acorletti 16962 Apr 19 12:16 john.log
-rw------- 1 acorletti acorletti    39 Apr 19 12:16 john.pot
```

Si se desean ver las contraseñas que ha ido almacenando, podemos hacerlo a través de la ejecución del comando.

```
┌──(acorletti㉿kali)-[~]
└─$ john --show ace.txt
alejandro:ale
```

En resumen, hemos visto dos ejemplos claros del empleo de usuarios locales y contraseñas débiles. En ambos, empleamos herramientas ejecutadas desde nuestro **Kali**, para verificar el nivel de fortaleza de las mismas, que no es, ni más ni menos, que una de las actividades cotidianas que debemos realizar cuando hagamos auditorías de nuestras infraestructuras de red y TI.

En nuestros ejemplos, desde ya que utilizamos usuarios y contraseñas triviales, pero en todo caso, el fallo está en que este tipo configuraciones que emplean algoritmos

inseguros y usuarios locales, tarde o temprano ofrecerán brechas de seguridad, las cuales, demorarán más o menos tiempo, pero terminarán por generarnos problemas.

Debemos mencionar, que John puede trabajar perfectamente con todo un listado de **"user:passw"**. En este ejemplo, hemos puesto solo una línea, pero pueden llegar a ser "n" líneas y las irá tratando todas a la vez, a medida que las va descifrando nos las presenta y las almacena en el mismo fichero "john.pot" que mencionamos

Si queremos reforzar el trabajo de John, podemos perfectamente sumarle diccionarios de contraseñas, que nuevamente, podemos descargarlos de Internet y personalizarlos, tal cual hemos desarrollado en la charla 38.

Reiteramos, que los routers son dispositivos importantes de nuestras redes, por lo que no podemos cometer errores tan sencillos de solucionar en sus configuraciones.

En el ejemplo de configuración de nuestro router **ace_2960** hemos visto que continuación de estos dos usuarios que acabamos de analizar, nos presenta las líneas que figuran aquí abajo.

```
aaa authentication login default  group tacacs+ enable
aaa authorization config-commands
aaa authorization exec default  group tacacs+ local
aaa authorization commands 5 default group tacacs+
aaa authorization commands 12 default group tacacs+
aaa authorization commands 15 default group tacacs+
```

En estas líneas la mención de "aaa", se corresponde con "**Autentication, Authorization** y **Accounting**", que es una de las funcionalidades que nos ofrecen hoy en día casi todos los dispositivos. Podemos ver que en estas líneas las asocia con "**tacacs+**", este es justamente el protocolo que permite la realización de estas tres funciones por medio de un "servidor tacacs", que será un dispositivo independiente que centralice estas funciones para toda la organización.

Concretamente, lo que buscamos en una auditoría de este tipo, es que los routers, y también los switchs de la empresa auditadla, SIEMPRE empleen esta "**AAA**" hacia un dispositivo externo.

En cuanto a las cuentas locales, es una práctica común y aceptable que cuente con una, o a lo sumo dos cuentas de usuarios locales, pues puede ocurrir una incidencia que nos impida llegar hasta el servidor tacacs. En estos casos, si hiciera falta alguna tarea de configuración de este router o switch, a través de esta cuenta podríamos hacerlo. No vamos a entrar aquí en como se configura este tipo de cuentas remotas y locales, pues sería excesivamente largo y en las guías de configuración de cualquiera de estos dispositivos se describe claramente cómo hacerlo. Lo que sí debemos dejar claro, es que estas cuentas de usuarios locales, deben ser lo suficientemente robustas, como para evitar ataques de contraseña como los presentados aquí. Es decir, emplear SHA-512 con contraseñas de más de ocho dígitos, preferiblemente más de diez, y que empleen obligatoriamente mayúsculas, minúsculas y caracteres especiales.

Volver al índice

www.darFe.es

Charla 49

Routers (parte II) - Auditoría con bash

Enlace al Video: 

Resumen:

En esta charla, seguiremos adelante con nuestra auditoría de routers, y desarrollaremos cómo podemos crear nuestras propias consultas a sus configuraciones, empleando el lenguaje nativo de Linux que se llama "**bash**".

Como punto de partida, tomaremos la herramienta "**ccat**" de Cisco, que, como iremos viendo, nos será de suma utilidad.

Descripción detallada

En esta charla, siguiendo con nuestra auditoría de routers, profundizaremos, a través de sencillos comandos "**bash**" el análisis de las configuraciones de estos dispositivos que, tal cual mencionamos en la charla anterior, es la misma lógica que también podemos aplicar a nuestros switchs, y seguramente a otros elementos cuyas configuraciones se realicen por medio de ficheros de texto.

Los desarrollos teóricos de esta charla, nuevamente se basan en el Capítulo 5. Routing, de nuestro libro "**Seguridad en Redes**".

Aspectos básicos de configuración de seguridad de un Router

Al igual que indicamos para los switchs, en este caso nuevamente la mejor referencia la tendremos en las "**Guías CIS**" que publica el "Center for Internet Security" (**https://www.cisecurity.org**).

CIS® Center for Internet Security®

En general las configuraciones de un router se realizan por medio de ficheros de texto plano. Si bien existen un sinnúmero de soluciones gráficas para optimizar este actividad, como así también para la gestión, supervisión y monitorización de este tipo de dispositivos, en definitiva, todas ellas terminan operando finalmente sobre este fichero de texto. Cada fabricante tiene sus propias "reglas" de configuración, pero lo importante de esto es que una vez conocida esta metodología, la misma es "**unívoca**". ¿Qué es lo que queremos transmitir con esto?, pues, que toda configuración de un mismo fabricante responde a un esquema básico de parámetros que se deberán escribir en forma y fondo exactamente igual, independientemente del modelo (es cierto que pueden existir pequeñas diferencias basadas en el número de versión del sistema operativo del router, pero esto no impacta en lo que presentaremos a continuación).

Cualquier responsable de seguridad de una red que deba evaluar el nivel de bastionado de un router, no debe realizar tareas de "Hacking ético" de caja negra, pues no tiene que demostrar nada, lo que debe hacer es analizar justamente los parámetros que tiene en su configuración cada router de su empresa, por lo tanto su actividad es comprender y analizar sus configuraciones.

Esta actividad no debe ser puntual, pues, como bien sabemos, la seguridad se degrada con el tiempo, por lo tanto la mejor forma de realizar este tipo de análisis es de forma periódica y de acuerdo a un "**Plan de revisión de seguridad**" o "**Plan de auditoría**". La forma de llevar a cabo este plan, es reuniéndose con las configuraciones, evaluarlas y compararlas con su análisis anterior, es decir trabajar como un ciclo de mejora continua, o ciclo de Demming, o ciclo **PDCA** (Plan - Do - Check - Act). Este tema lo abordaremos más adelante, pero es bueno que ya empiece a sonar en nuestros oídos.

Para realizar este trabajo lo primero es comprender las configuraciones, y luego, poder realizar las evaluaciones de la forma más eficiente que esté a nuestro alcance.

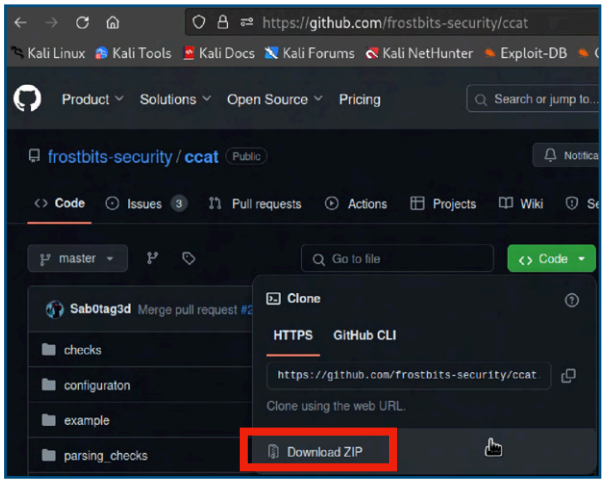
Manteniendo nuestra línea orientada hacia el **software libre**, a continuación vamos a trabajar con una herramienta que para los routers Cisco es de gran utilidad "**ccat**".

En nuestro trabajo cotidiano, hemos desarrollado varios scripts que empleamos también para otros vendors como son "Juniper", "Alcatel Lucent" (Hoy Nokia)" y "Huawei" basadas en la misma lógica que propone **ccat**, por esa razón es que nos pareció importante presentar la lógica que esta herramienta emplea pues, comprendiendo esta base, nos resultará extremadamente fácil aplicarla para el análisis de cualquier tipo de dispositivo.

Esta herramienta es "**ccat**" y podemos descargarla en:

https://github.com/frostbits-security/ccat

Si abrimos nuestro navegador desde Kali sobre este enlace, nos permitirá descargar un fichero "**.zip**"



Al descargarlo, podemos verlo en el directorio "/Downloads" de nuestro home de usuario.

```
┌──(acorletti㉿kali)-[~/Downloads]
└─$ ls -l
total 75136
-rw-r--r-- 1 acorletti acorletti       46 Apr 19 12:08  ace.txt
-rw-r--r-- 1 acorletti acorletti   569946 Apr 20 10:15  ccat-master.zip
```

Recomendamos copiar este fichero "**ccat-master.zip**" al home de nuestro usuario, situándonos en el directorio "Downloads" y desde allí ejecutar (en nuestro caso):

$cp ccat-master.zip /home/acorletti

Nos desplazamos a nuestro directorio home, en nuestro caso "/home/acorletti" y desde allí descomprimimos el fichero con la siguiente instrucción:

$unzip ccat-master.zip

Al ejecutar la misma, veremos que se ha creado un nuevo directorio "**ccat-master**".

```
┌──(acorletti㉿kali)-[~]
└─$ ls -l
total 28292
-rw-r--r--  1 acorletti acorletti     3213 Jun  1  2023 2960_ace.txt
-rw-r--r--  1 acorletti acorletti       45 Apr 19 12:38 ace.txt
drwxr-xr-x  6 acorletti acorletti     4096 Apr 23  2023 ccat-master
-rw-r--r--  1 acorletti acorletti   569946 Apr 20 10:15 ccat-master.zip
```

```
┌──(acorletti㉿kali)-[~/ccat-master]
└─$ ls -l
total 676
-rw-r--r-- 1 acorletti acorletti   3325 Apr 23  2023 args.py
-rw-r--r-- 1 acorletti acorletti 562233 Apr 23  2023 ccat.png
-rwxr-xr-x 1 acorletti acorletti  11622 Apr 23  2023 ccat.py
```

Si nos desplazamos dentro de este directorio, podemos ver que el fichero ejecutable es "**ccat.py**". Esta es la última versión de este software, la cual, como podemos apreciar en su extensión "**.py**" se trata de un desarrollo en "**Python**". Si vais a realizar auditorías de seguridad sobre este tipo de routers, podéis emplear directamente esta versión.

Para el trabajo que nos interesa en este capítulo, iremos "personalizando" diferentes opciones de análisis por medio de programación, "Bash" por lo descargaremos la versión anterior que la hemos dejado disponible en nuestro servidor: **https://darFe.es**

Como puedes ver en la imagen de la derecha, desde el menú “**DESCARGAS**” —> “**Tecnología**” —> “**herramientas bash (scripts)**”

Allí encontrarás el fichero: “**cat.sh**” para su descarga.

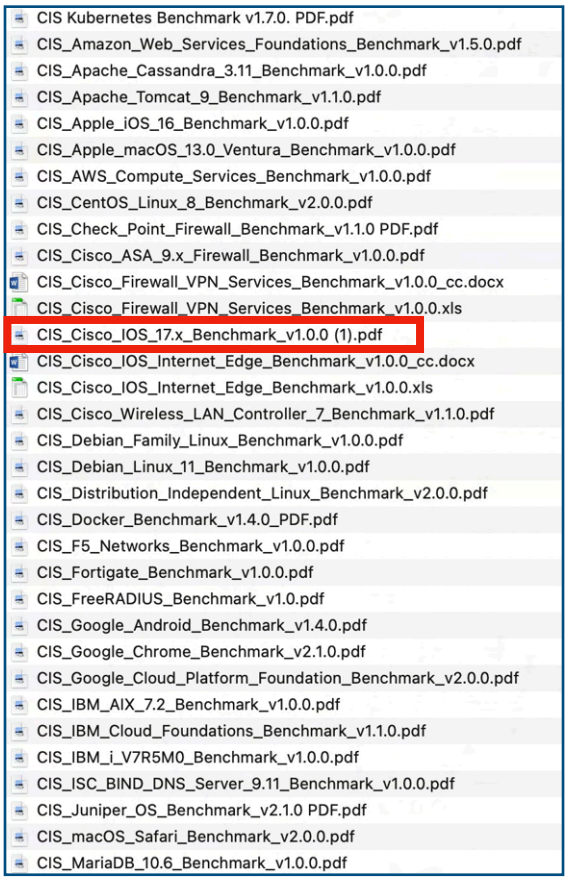
Este archivo es el desarrollado en lenguaje “Bash” y será el que empleemos en nuestro ejemplo.

Te recomendamos que lo descargues en tu Kali, para iniciar el trabajo.

A partir de la página 190 de nuestro libro “**Seguridad en Redes**”, tenéis todo el detalle del formato, configuración y contenido de esta herramienta **ccat**.

Lo que intentaremos presentar a continuación, es una metodología de trabajo que pueda ser comprendida a través de esta herramienta, pero que luego nos permita desarrollar y emplear sencillos “**sripts**” realizados en programación “**bash**” para evaluar el nivel de bastionado de cualquier configuración de router.

Volviendo a nuestras guías **CIS**, siempre es recomendable tenerlas a mano. En nuestro caso, por ejemplo, creamos un directorio “CIS” en nuestros ordenadores, donde las descargamos y las vamos actualizando periódicamente, tal cual podéis ver en el listado de la derecha.



Para la práctica que proponemos hoy, emplearemos lo que nos indica la que hemos resaltado en **rojo**.

CIS_Cisco_IOS_17.x_Benchmark_V1.0.0

Seguramente cuando leáis este texto ya habrá versiones nuevas de esta guía.

Sobre la base de esta guía CIS y aprovechando las líneas de código de “ccat” empezaremos a desarrollar sencillos scripts en “**bash**” para analizar los routers.

Qué es la programación en Bash

Bash es la abreviatura de Bourne again Shell (Otro Shell Bourne), se trata de un intérprete de comandos basado en la **shell** (coraza/corazón) de Linux, su nombre indica

que la base es el Shell de Bourne (cuyo nombre viene por su creador **Stephen Bourne**) que fue tal vez el primer y más importante interprete de las primeras versiones de Linux a finales de los 70' (pero más limitado que el actual).

Stephen Bourne
Imagen de Wikipedia

Brian Fox
Imagen de Wikipedia

Bash fue escrito por **Brian Fox** a finales de los 80' y Chet Ramey fue su principal sucesor.

Es el intérprete por defecto de la mayoría de las distribuciones **GNU/Linux**. Cabe mencionar que hay otros intérpretes como Korn Shell (**ksh**) y el C Shell (**csh**). Durante este texto intentaremos emplear las sintaxis que son comunes a los tres.

A continuación vamos a desarrollar los comandos principales que emplearemos en nuestra labor de auditoría de configuraciones de routers, con estos tendremos la mayor parte del trabajo realizado, pero por supuesto, bash posee muchos más que pueden ser reemplazados, o ampliados por parte del lector para ajustar y desarrollar sus propios scripts.

En particular, yo: *Alejandro Corletti Estrada*, no puedo, ni debo, continuar con estas líneas, sin agradecer especialmente a "**José Ignacio Bravo Vicente**" (*Autor del prólogo de este libro*), gran amigo desde hace más de dos décadas, y una de las mentes más brillantes que he conocido en mi vida (de verdad). Yo sembré la semilla de **ccat**, e hice los primeros análisis con bash con mis limitadas capacidades al respecto, y luego se sumó Nacho, revolucionando la historia de las auditorías de routers. Con su genialidad, comenzó a desarrollar recursividades, llamadas, librerías… ya ni siquiera sé que más incorporó, pero con un 10% mío y un 90% de su parte, logramos desarrollar una herramienta y metodología de análisis que actualmente, estimo, debe ser difícil de superar.

Comencemos con nuestro trabajo de análisis con bash.

Iniciaremos, por ejemplo, analizando la configuración de **SNMP** (Single Network Monitor Protocol). Se trata del protocolo más importante para supervisión y monitorización de dispositivos.

En la página 250 de nuestro libro "**Seguridad por Niveles**", se desarrolla con todo detalle este protocolo.

7.8. SNMP (Single Network Monitor Protocol).

Este es el protocolo que habilita las funciones que permiten administrar redes no uniformes. Esta regulado por la **RFC 1155, 1156** y **1157**, y básicamente separa dos grupos: Administradores y Agentes. Los Administradores (**NMS**: Network Managment Station) son los responsables de la administración del dominio ejecutando un determinado Software de monitorización. Los agentes tienen a su vez un Software residente que responde a las solicitudes del administrador con la información guardada en sus bases de datos locales (MIB: Managment Information Base). Estas consultas en realidad pueden ejecutarse por dos métodos:

- **Poll** (Sondeo): La estación administradora sondea uno por uno a los agentes cada un determinado período de tiempo, y estos van informando si apareciera alguna novedad en su MIB desde el último sondeo.
- **Interrupción**: Los Agentes al aparecer alguna novedad en su MIB, envían un mensaje interrumpiendo los procesos del Administrador para notificar sus cambios.

Como puede deducirse cada uno de ellos tiene sus ventajas y desventajas; si una novedad apareciera inmediatamente después que un sondeo fue realizado a un agente, el Administrador tomaría conocimiento de este suceso recién en el próximo sondeo, lo cual por ejemplo en una red de Terapia Intensiva de un Hospital no sería muy saludable. Por el contrario, si se produjera alguna anomalía en el canal de comunicaciones en un sistema por interrupción, el Administrador nunca volvería a detectar novedades en un Agente que se encuentre sobre ese vínculo. Estos son algunos ejemplos, pero en virtud de la cantidad de posibilidades que existen es que se suelen implementar estrategias mixtas de monitoreo de red, que permitan superar estas contingencias.

Alejandro Corletti Estrada Página 250 www.DarFE.es

Este protocolo, ofrece la posibilidad de monitorizar el estado de los dispositivos y también de escribir sus configuraciones, para ello cuenta con **dos comunidades**, una de lectura y otra escritura. Por defecto estas comunidades ya vienen disponibles bajo el nombre de "**public**" y "**private**" respectivamente.

Para nuestro análisis, tomaremos este parámetro, según nos lo indica la **guía CIS** que hemos mencionado.

1.5 SNMP Rules

Simple Network Management Protocol (SNMP) provides a standards-based interface to manage and monitor network devices. This section provides guidance on the secure configuration of SNMP parameters.

The recommendations in this Section apply to Organizations using SNMP. Organizations using SNMP should review and implement the recommendations in this section.

1.5.1 Set 'no snmp-server' to disable SNMP when unused (Automated)

Como podemos ver en la imagen de la derecha, el punto **1.5** de esta guía desarrolla este protocolo. Lo primero que nos indica en el punto 1.5.1, es que si no se emplea el protocolo **SNMP**, deberíamos deshabilitarlo en el dispositivo, para ello deberíamos incorporar en el fichero de configuración, la línea "**no snmp-server**" con lo que estaría deshabilitado el mismo.

1.5.2 Unset 'private' for 'snmp-server community' (Automated)

Profile Applicability:

- Level 1

Description:

An SNMP community string permits read-only access to all objects.

Audit:

Perform the following to determine if the public community string is enabled:
Ensure `private` does not show as a result

```
hostname# show snmp community
```

Remediation:

Disable the default SNMP community string `private`

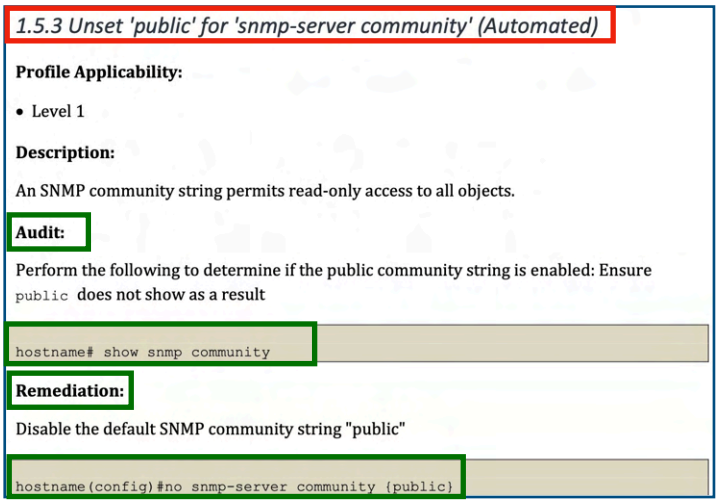
```
hostname(config)#no snmp-server community {private}
```

El punto que sigue, justamente, nos presenta el tema de las comunidades que presentamos en los párrafos anteriores, comienza con la comunidad "**private**", la cual debe ser desactivada (*unset*). Lo remarcamos en **rojo**.

Otro aspecto importante de esta guía es que nos indica como auditarla y como deshabilitarla, tal cual hemos remarcado en **verde**.

En el punto 1.5.3 de esta misma guía aborda el tema de la comunidad "**public**" a la que aplican los mismos conceptos que con "private".

Hemos resaltado estos campos con los mismos colores que la anterior



1.5.3 Unset 'public' for 'snmp-server community' (Automated)

Profile Applicability:

- Level 1

Description:

An SNMP community string permits read-only access to all objects.

Audit:

Perform the following to determine if the public community string is enabled: Ensure `public` does not show as a result

```
hostname# show snmp community
```

Remediation:

Disable the default SNMP community string "public"

```
hostname(config)#no snmp-server community {public}
```

De la guía CIS, para estos puntos nos quedaremos en tres ideas:

- Si no emplea SNMP, debe estar **deshabilitado** el protocolo.
- NO debería encontrarse la comunidad "**private**".
- NO debería encontrarse la comunidad "**public**".

Estos tres conceptos implican que:

1) Si apareciera la frase "**snmp community**", esto implica que **SÍ** se está usando, caso contrario deberíamos encontrar la frase "**no snmp-server**".
2) Si apareciera la frase "**snmp community**", debo buscar la frase : "**show snmp community**" y luego de ella **NO** debe aparecer la palabra "**public**" ni tampoco "**private**".

Veamos cómo podemos aplicar esta lógica por medio de programación **bash**.

Como primer paso, vamos a dar una mirada al fichero"**ccat.sh**" que acabamos de descargar de **www.darFe.es**, el cual como mencionamos emplea programación en "**bash**". Podemos editarlo con "**vi**", "**cat**", o cualquier editor de texto de Linux.

Las primeras líneas que nos presenta son las siguientes.

```
#!/bin/sh -
#########################################################################
# CCSAT                                 Version 2.2                     #
# Copyright (C) 2003-10 BGK Bill Zeng bgk@hotunix.com                   #
#                                       alphan3@yahoo.com               #
# Created: May 9, 2003                  Last Modified: Jan 10, 2010     #
# Script Available at:                  http://ccsat.sourceforge.net    #
#                                       http://hotunix.com/tools        #
#########################################################################
# COPYRIGHT NOTICE                                                      #
# Copyright (C) 2003-10  BGK   All Rights Reserved                      #
#                                                                       #
# CCSAT (Cisco Configuration Security Auditing Tool) is a script to     #
# allow automated audit of configuration security of large numbers      #
# of Cisco routers and switches.  The tool is based upon industry       #
# best practices including Cisco, NSA and SANS security guides and      #
# recommendations.  CCSAT is flexible and can report details down to    #
# individual device interfaces, lines, ACL's, AS's, etc.                #
#                                                                       #
# Special thanks go to T. Dafoe and J. Reid for sharing knowledge       #
```

```
# and resources with the author.  CCSAT has been used on FreeBSD for  #
# real audits (20 seconds of runtime for 75 device configurations of  #
# 620KB on HP Proliant DL380 with 2.8GHz CPU and 1GB RAM).  It was    #
# also tested on Linux and Solaris-8, and should run on all major     #
# UNIX platforms (POSIX.2-compliant).                                 #
#                                                                     #
# CCSAT is freeware, and may be used, modified or redistributed so    #
# long as this copyright & credits notice and the header remain       #
# intact, and be included in documentation.  You agree to indemnify   #
# the author from any liability that might arise from using the code. #
#######################################################################
# CCSAT                               Version 2.2                     #
# Copyright (C) 2003-10 BGK Bill Zeng bgk@hotunix.com                 #
#                                     alphan3@yahoo.com               #
# Created: May 9, 2003                Last Modified: Jan 10, 2010     #
# Script Available at:                http://ccsat.sourceforge.net    #
#                                     http://hotunix.com/tools        #
#######################################################################
# COPYRIGHT NOTICE                                                    #
# Copyright (C) 2003-10  BGK   All Rights Reserved                    #
#                                                                     #
# CCSAT (Cisco Configuration Security Auditing Tool) is a script to   #
# allow automated audit of configuration security of large numbers    #
# of Cisco routers and switches.  The tool is based upon industry     #
# best practices including Cisco, NSA and SANS security guides and    #
# recommendations.  CCSAT is flexible and can report details down to  #
# individual device interfaces, lines, ACL's, AS's, etc.              #
#                                                                     #
# Special thanks go to T. Dafoe and J. Reid for sharing knowledge     #
# and resources with the author.  CCSAT has been used on FreeBSD for  #
# real audits (20 seconds of runtime for 75 device configurations of  #
# 620KB on HP Proliant DL380 with 2.8GHz CPU and 1GB RAM).  It was    #
# also tested on Linux and Solaris-8, and should run on all major     #
# UNIX platforms (POSIX.2-compliant).                                 #
#                                                                     #
# CCSAT is freeware, and may be used, modified or redistributed so    #
# long as this copyright & credits notice and the header remain       #
# intact, and be included in documentation.  You agree to indemnify   #
# the author from any liability that might arise from using the code. #
#######################################################################
```

De las líneas anteriores, solo nos detenemos, en que nos indica que emplea “bash” con su primera línea: “#!/bin/sh -”, que fue creado: “May 9, 2003, Last Modified: Jan 10, 2010”, que si bien el fichero se llama “ccat” su nombre real es: “CCSAT (Cisco Configuration Security Auditing Tool)”.

Que es de uso libre y puede ser usado, modificado, o redistribuido, cumpliendo las siguientes condiciones:

```
#CCSAT is freeware, and may be used, modified or redistributed so    #
# long as this copyright & credits notice and the header remain      #
# intact, and be included in documentation.
```

Luego define las variables que empleará:

```
### working, configuration, and reporting directories

workdir=`pwd`
configdir=$workdir/config
reportdir=$workdir/report
```

De estas variables, nos interesan particularmente los dos directorios que menciona “**config**” y “**report**”, pues en el primero de ellos es donde debemos subir las configuraciones que deseamos analizar, y en el segundo es donde se almacenarán los resultados de los reportes.

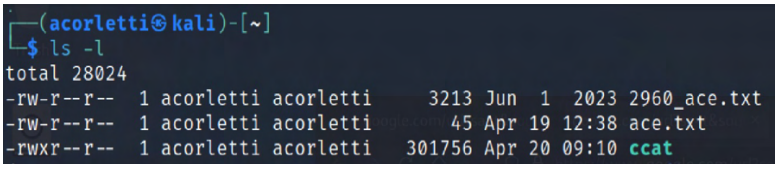
Un poco más adelante, nos indica los pasos a seguir para el uso de la herramienta. No lo traduciremos, haced un pequeño esfuerzo, es sencillo.

```
# instructions and directory preparation:

echo "
HOW-TO:

1) To start, have this script (ccsat) in your working directory $workdir;
2) Within that directory, create subdirectories $configdir and $reportdir;
3) Put config text files in $configdir and ensure same file extension
(default .txt);
4) If none, then add file extension (commands provided here);
5) Run './ccsat 12.4' (assuming 12.4 is the latest IOS);
6) The main report will be $report.
```

Un detalle que aún no hemos hecho, al igual que en el capítulo anterior con “**ciscocrack.pl**" es modificar sus permisos para que pueda ser ejecutable. Para ello repetiremos el comando “chmod”.

$chmod 744 ccat.sh

Podemos verificar ahora, que el fichero “ccat” está en color **verde** y que posee “**rwx**” para el usuario y grupo “**acorletti**”.



En el video, se explican los pasos para la ejecución de “ccat” sobre el mismo router “**2960_ace.txt**” que trabajamos la charla anterior. No repetiremos aquí los mismos pues sería muy extenso, por favor dadle una mirada a esta parte del **video de la charla 49**. Básicamente, he creado los dos directorios “**config** y **report**” y luego copié dentro de “**config**” el fichero e configuración “**2960_ace.txt**”. El paso final es la ejecución del comando:

$./ccat.sh 12.4

El resultado será el siguiente:

$cat audit-results

Cisco Device Configuration Security Audit: CCSAT Report

(Script created by BGK, bgk@hotunix.com)
(Script start time: Sat Apr 20 10:21:25 AM CEST 2024)

The latest IOS version was entered as 12.4

Total number of audited devices = 1
Total number of interfaces = 5
Total number of shutdown interfaces = 0
Total number of open interfaces = 5
Total number of lines (con/vty/aux) = 2

Total number of console lines = 1
Total number of terminal lines = 1
Total number of auxiliary lines = 0
Total number of access lists = 1
Total number of snmp ro/rw rules = 3 (ro=1 + rw=2)

NOTE: IGNORE ANY REPORTED ZERO (OR NEGATIVE) DEVICE OR INTERFACE, ETC!! ONLY POSITIVE NUMBERS BELOW INDICATE VULNERABILITIES!!

I. General Configuration

IOS version (latest 12.4) not up-to-date on:
0 of 1 devices

(12.0 or later supports all 3 snmp versions: SNMPv1, SNMPv2c and SNMPv3.)

banner not configured on...
0 of 1 devices

II. Passwords and Authentation

'service password-encryption' not configured on...
0 of 1 devices

'enable secret' not configured on...
0 of 1 devices

'enable password' (weak) still configured on...
0 of 1 devices

I of II: password not explicitly configured on the following router lines:
2 of 2 lines

II of II: local login authentication not configured on the following router lines:
2 of 2 lines

(Any line appears in both list I & II above uses no authentication!)

SNMP community default strings still configured on...
1 (ro) and 1 (rw) of 1 devices

SNMP-server host v3 not configured on...
-1 of 1 devices
2960_ace.txt

SNMP-server group v3 not configured on...
1 of 1 devices

'AAA new-model' not configured on...
0 of 1 devices

AAA authentication (TACACS+/Radius/Kerberos) not configured on...
0 of 1 devices (tacacs+)
or
1 of 1 devices (radius)
or
1 of 1 devices (kerberos)

user privilege not configured on...
-1 of 1 devices

III. Network Services

'no service tcp-small-servers' not configured on...
1 of 1 devices

'no service udp-small-servers' not configured on...
1 of 1 devices

'no ip bootp server' not configured on...
1 of 1 devices

'no ip finger' not configured on...
1 of 1 devices

'no ip http server' not configured on...
0 of 1 devices

'no cdp run' not configured on...
1 of 1 devices

'no service config' not configured on...
1 of 1 devices

'ip ssh' not configured on...
-1 of 1 devices

IV. IP Routing and Security

'no ip source-route' not configured on...
1 of 1 devices

'ip cef' not configured on...
1 of 1 devices

'no ip directed-broadcast' not configured on the following router interfaces:
5 of 5 interfaces

'no ip mask-reply' not configured on the following router interfaces:
5 of 5 interfaces

'no ip proxy-arp' not configured on the following router interfaces:
5 of 5 interfaces

RIP configured on... (informational)
0 of 1 devices

RIP MD5 authentication not configured on...
0 of 0 devices

OSPF configured for... (informational)
0 networks on 0 devices

MD5 authentication not configured for...
0 of 0 OSPF networks

EIGRP configured for... (informational)
0 AS networks on 0 devices

MD5 authentication not configured for...
0 of 0 EIGRP AS networks

BGP configured for... (informational)
0 AS networks on 0 devices

BGP neighbor passwords not configured for...
0 of 0 BGP AS networks

Only the following remote ASs are password-authenticated:

V. Access Control and ACLs

exec-timeout not configured on the following router lines:
2 of 2 lines

'transport input telnet' not configured on the following router vty lines:
1 of 1 vty lines

'transport input ssh' not configured on the following router vty lines:
1 of 1 vty lines

'access-class <ACL> in' not configured on the following router vty lines:
1 of 1 vty lines

'access-group <ACL> in/out' not configured on the following router interfaces:
5 of 5 interfaces (in & out on same I/F counted twice)

SNMP community (readonly/readwrite) not access-controlled on...
2 of 3 RO/RW rules
snmp-server community private RW
snmp-server community public RO

VI. Logging

'service timestamps log...' not configured on...
1 of 1 devices

'logging <server_IP>' not configured on...
-1 of 1 devices
2960_ace.txt

NOTE: This will be false positive if IPs are stripped off for external audit

NTP server not configured on...
0 of 1 devices

(Script finish time: Sat Apr 20 10:21:25 AM CEST 2024)

Todo lo anterior fue la respuesta que me entregó **ccat** sobre el router que auditamos, únicamente sobre el **router 2960_ace.txt**, pues es el único que existía en el directorio “**config**”, si hubiese habido más configuraciones en este directorio, entonces el reporte

sería sobre todos los que en el mismo se encuentren. En el directorio "**report**", es justamente donde estará el reporte que hemos pegado arriba.

Si queréis profundizar un poco más sobre este reporte, dad una mirada al video de la charla, en que se explica brevemente, pero el foco de este capítulo, es avanzar sobre cómo podemos nosotros mismos ir generando scripts que nos permitan ajustar estas auditorías a lo que necesitamos buscar.

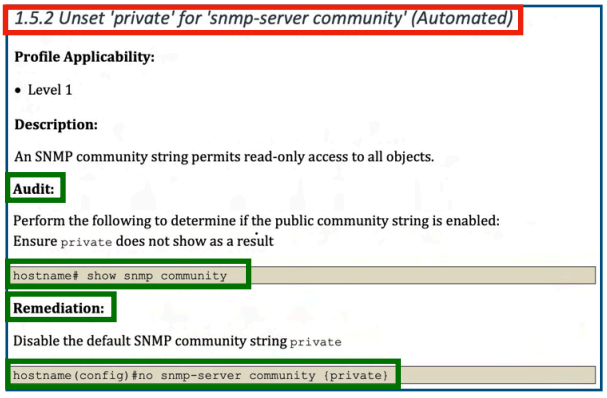
Si queremos ir haciendo este tipo de consultas, situados en el directorio en el que está nuestro router podemos ejecutar, por ejemplo el comando:

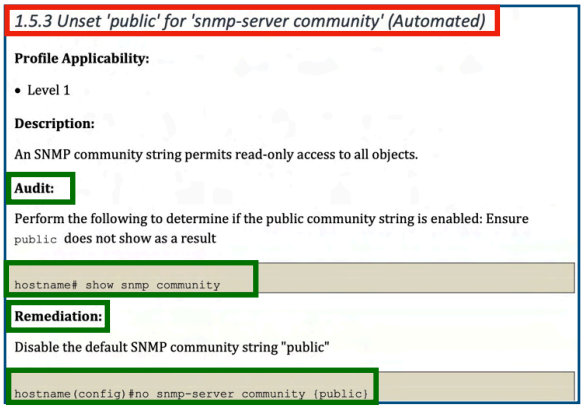
$grep "snmp" 2960_ace.txt

Nos responderá lo siguiente:

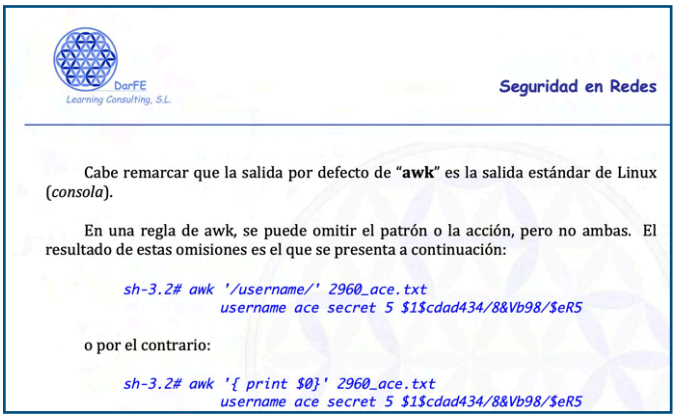
snmp-server community private RW
snmp-server community **public RO**
snmp-server community **prueba RW** 2
snmp-server trap-source Vlan200
snmp-server packetsize 1024
snmp-server location sede_central
snmp-server enable traps tty
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps auth-framework sec-violation snmp-server enable traps power-ethernet police snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps bridge newroot topologychange snmp-server enable traps syslog
snmp-server enable traps vlan-membership
snmp-server host 10.1.2.21 version 3
snmp-server host 10.1.2.24 version 3

Hemos resaltado en negrita, justamente la presencia de las dos comunidades por defecto que la guía CIS nos indicó, unas páginas más arriba, que debían ser desactivadas.





Sigamos avanzando. Volvamos ahora a nuestro libro "**Seguridad en Redes**". A partir de la página 189 está desarrollado con todo detalle los aspectos que estamos resumiendo aquí.



DarFE
Learning Consulting, S.L.

Seguridad en Redes

Cabe remarcar que la salida por defecto de "**awk**" es la salida estándar de Linux (*consola*).

En una regla de awk, se puede omitir el patrón o la acción, pero no ambas. El resultado de estas omisiones es el que se presenta a continuación:

```
sh-3.2# awk '/username/' 2960_ace.txt
        username ace secret 5 $1$cdad434/8&Vb98/$eR5
```

o por el contrario:

```
sh-3.2# awk '{ print $0}' 2960_ace.txt
        username ace secret 5 $1$cdad434/8&Vb98/$eR5
```

Detengámonos en la página 196, para hacer un análisis más, con el comando:

$ awk '/username/ { print $0}' 2960_ace.txt

username alejandro secret 5 1qJO4B8A5$YI.S6q227itWNzpanEU6S.
username ace privilege 7 password 7 13061E010803

Este comando, se basa en <patrón - acción>, es muy similar a **grep** en cuanto búsqueda, pero me permite "partir" la búsqueda. Por esta razón es que en la línea anterior, le estamos diciendo, **patrón** = username y **acción** ={ print$0 }, ese decir que busque 'username' y con el **$0** que me presenta la línea completa. Podéis hacer todas las pruebas que os guste, con las combinaciones que se os ocurran.

Por supuesto que estos son solo dos ejemplos básicos de la infinita potencia que nos ofrece "**bash**". Os recomendamos que vayáis al las páginas mencionadas del libro "**Seguridad en Redes**" y profundicéis mucho más sobre estos comandos, pues os aseguramos que se os abrirán muchas posibilidades.

Volver al índice

www.darFe.es

Charla 50

Desenchufando - Dedicado a los “Moteros”

Enlace al Video:

Resumen:

Qué se puede decir, yo voy en moto.

Descripción detallada

Con este desenchufe, festejo mis 50 años con esta gran compañera de vida que ha sido mi moto. Desde mi primer Siambretta 125, hasta mis actuales scooter. Ya sé que muchos de vosotros pensaréis que estos últimos no pueden considerarse “motos”, pero luego de 50 años subido a ellas, se agradece bastante la protección al frío y la lluvia. Que se va a hacer, los años llegan…

Yo voy en moto (video original): **https://youtu.be/MUQC8tZtFwc**

Letra:

Yo voy en moto por la vida, no soy convencional,
Mis treinta y trece llevo encima y no paro de cantar, (*43 fueron cuando la escribí*)
Un rock and roll o una balada, cualquiera me da igual,
El ritmo fluye por mis venas no paro de tocar...

Yo voy en moto por la vida y hoy conduzco normal,
Ya no hago willies ni carreras, pero disfruto igual,
Cuando hay atasco, algún agujero siempre logro encontrar,
Estaciono donde quiero y no tengo que buscar (ni pagar, ni esperar, ni andar)...

Yo voy en moto por la vida, es mi forma de viajar
Disfruto el aire, paso frío y me suelo mojar,
Pero esos días de verano, cuando empieza el calor,
Donde no hay guardias, dejo el casco, monto en cuero bajo el sol...

Yo voy en moto por la vida y llego siempre puntual,
Si alguien me apura o se me arrima, hoy lo dejo pasar,
Y cuando vuelvo para casa, temprano voy a llegar,
Miro esas caras en los coches con su stress y malestar...

Yo voy en moto por la vida, es mi cierta libertad,
Puede que no sea seguro, tampoco lo es volar,
Hay cosas raras que a la gente le gusta disfrutar
Dios quiera que esta me acompañe por mucho tiempo más...

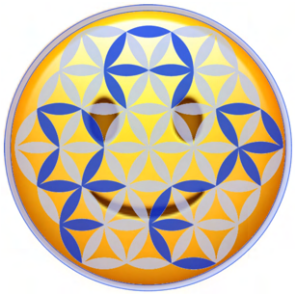
Volver al índice

Epílogo

Llegar al final de un libro, siempre tiene una doble cara, entre la alegría y la tristeza.

Esta vez, me tira más la alegría, pues este no es un final en sí mismo, es como un alto en el camino para ir preparando el **Volumen 2**, que como bien sabéis los que estáis siguiendo este ciclo de "**Aprendiendo Ciberseguridad paso a paso**", sus contenidos ya están prácticamente listos. Lo que seguramente no sepáis, son la cantidad de horas y horas, días y días, meses y meses, que requiere plasmar todos los videos, textos, enlaces e imágenes de forma consolidada en un libro que tenga calidad, se entienda y minimice los infaltables y omnipresentes errores. Esto, aunque parezca trivial, es de verdad agotador, es un esfuerzo considerable.

Justamente en estos momentos, estoy preparando la charla 100 de nuestro ciclo "**Aprendiendo Ciberseguridad paso a paso**".



Este charla, o desenchufe, va de "**Gratitud**".

Aquí sí que estoy en el medio de la alegría y la tristeza.

En estos momentos, no sé cuál de las dos pesa más.

¿Estamos comprendiendo la "**Filosofía Hacker**"?

Esta "**Cultura hacker**" que menciona Nacho en el prólogo de este libro:

> *"La cultura hacker siempre ha estado vinculada con la difusión del conocimiento. Tiene sus raíces en los primeros días de la informática, cuando los programadores y entusiastas de la tecnología se reunían en universidades, laboratorios de investigación y clubes de computación para explorar y experimentar con las nuevas tecnologías emergentes."*

Luego de 30 años compartiendo todo lo que he podido, entre esta alegría y tristeza, de verdad me estoy preguntando ¿valió la pena?

He recibido miles de satisfacciones, se me han abierto cientos de puertas. Como siempre expreso, me ha permitido vivir más que bien, y sobre todo, a gusto con lo que hago, peeeeero…

Sé que los libros, videos y artículos, han llegado a cientos de miles de personas en todo el mundo. Miles me lo han agradecido. Sé que han sido de utilidad, que se usan en universidades, centros de formación, seminarios, bootcamps, peeeero…

Hace años que estoy intentando llevar a cabo mi sueño de poder ofrecer GRATUITAMENTE un "**Máster en Ciberseguridad**". La base del mismo, serían nuestros tres cursos:

- “Técnico en Ciberseguridad”

- “Especialista en Ciberseguridad”

- “Experto en Ciberseguridad”

El primero de ellos, ya lo lanzamos de forma totalmente gratuita. En estos momentos, hemos alcanzado los **16.000** alumnos.

Al finalizar el curso, **emitimos un certificado** firmado digitalmente para que quede una constancia sólida y difícil de falsificar.

Para cumplir este sueño, he recurrido a todos los ámbitos que están a mi alcance.

Es un batalla de David contra Goliat, pues por supuesto, hay importantísimos intereses de por medio, desde las Universidades que cobran en el orden de 5.000 euros por estos máster, pasando por los organismos oficiales y hasta por INCIBE que solo apoya a empresas que facturan millones de euros (si no es así, quedas fuera).

Hay fundaciones que también se suponen que podrían aceptar este desafío.

Hay grandes empresas que también soportan este tipo de iniciativas.

El poder llegar a decenas de miles de personas con formación gratuita en Ciberseguridad, sin lugar a dudas, nos permitiría tener más gente para luchar contra los ciberdelitos, protegernos mejor, minimizar los daños de la red, tener más salidas laborales, mejorar Internet, y miles de efectos más que todos conocemos perfectamente.

Peeeero, mi sueño sigue sin poder tener el menor grado de avance.

Aquí está mi tristeza.

No va tanto con las universidades, empresas, gobierno, INCIBE, etc.

Mi tristeza va contigo.

Ya sé que la gratitud, no está bien que se la espere como una “retribución”.

Pero es que la cosa no es para mí, **es para ti**.

Uno de los caminos que llevo explorando desde hace más de tres años, son las redes sociales e Internet, como estrategia para mover el fenómeno “**crowd**” (multitudes).

Si las moviéramos, como bien sabéis, lograríamos el efecto “Influencias” y esto podría generar las bases y los ingresos para que la “formación gratuita” de calidad, sea una realidad, y lo mejor de todo: SIN NINGUNA DEPENDENCIA de gobiernos, universidades y/o empresas.

Peeeero…

Aquí está mi tristeza: cada paso que he dado, cada nueva propuesta, cada expectativa para seguir un paso más con este sueño… han sido solo centenas de “click”, “likes”. **Con esto no basta**. Si no te mojas tu, y tu, y tu, no puedo, no me da el pulmón para poder llevarlo a cabo. Y aquí está mi tristeza, pues veo que **sí** haces “click” ante la foto de un famoso que no te aporta absolutamente nada de nada, pero a esto que sí ha colaborado con tu formación y capacitación, tú (sí tú que estás leyendo), ¿no lo apoyas?… me da mucha tristeza. Luego de estos tres años, no deja de sorprenderme que menos de un 1%: **sí un 1%** (uno por ciento), es la que agradece, participa y colabora… **el otro 99%**, no es capaz ni de mover un dedo para hacer “**click**”…

Para cerrar el libro, os pido disculpas por hacerlo de esta forma, pero, ya me conocéis, no suelo ocultar lo que pienso. Tal vez esté equivocado, y no deba esperar este tipo de apoyos, pero bueno, la verdad es que sí, me gustaría poder llevar a cabo este sueño.

Por último: 🤔 **¿Conoces el concepto SOCIEDAD de la ROTONDA?** 🤔