



Unidad 11: Guía para Resolución de Problemas de Redes Inalámbricas

Autores: Onno Purbo, Alberto Escudero Pascual /, Louise Berthilson, IT +46

Tabla de contenido

1. Sobre este documento.....	2
1.1 Información sobre propiedad intelectual.....	2
1.2 Grado de dificultad.....	2
1.3 Información sobre los iconos.....	2
2. Introducción.....	2
3. Antes del modelo OSI.....	3
3.1 Fuente de corriente estable.....	3
3.2 Actualización del Firmware.....	4
4. Metodología.....	5
4.1 Resolución de problemas de arriba a abajo.....	5
4.2 Resolución de problemas de la mitad a arriba, de la mitad a abajo.....	5
4.3 Ejemplo práctico.....	5
5. Herramientas para la resolución de problemas.....	7
6. Escenario 1: ¿Interferencias de radio?, ¿Canales ocupados?.....	8
7. Escenario 2: ¿Red congestionada? ¿Inundación?.....	8
8. Escenario 3: ¿Por qué este servicio de red no está trabajando? ¿Conexión rechazada?.....	10
9. Controlando la interferencia.....	11
9.1 Interferencia y ruido.....	11
10.2 Maximizando el nivel de la señal recibida.....	12
10.3 Minimizando los niveles de interferencia y ruido.....	12
10.4 Estrategias para controlar la interferencia.....	12
10. Conclusiones.....	13
11. Declaración de Derechos de Propiedad Intelectual.....	13

1. Sobre este documento

Este material es parte del paquete de materiales del proyecto TRICALCAR. Para información sobre TRICALCAR consulte el módulo de introducción de estos materiales, o www.wilac.net/tricalcar/. Este material fue traducido del inglés de los materiales desarrollados para el proyecto "Capacity Building for Community Wireless Connectivity in Africa" de APC <<http://www.apc.org/wireless/>>. El material fue actualizado y adaptado para el contexto de América Latina.

1.1 Información sobre propiedad intelectual

Esta unidad temática se ha hecho disponible bajo los términos de la licencia **Atribución-No Comercial-Licenciamiento Recíproco 3.0 Genérica**. Para ver los términos completos de esta licencia: http://creativecommons.org/licenses/by-nc-sa/3.0/deed.es_MX






1.2 Grado de dificultad

El grado de dificultad de esta unidad es "medio" con algunas partes adicionales "avanzadas".

Todas las secciones avanzadas están marcadas con un marco rojo para hacer al lector consciente del mayor grado de dificultad.

1.3 Información sobre los iconos

En los contenidos encontraremos 5 tipos de iconos, cuyo significado se describe a continuación:

Concepto teórico clave	Recomendación práctica importante	Ejercicio	Propiedad intelectual	Propiedad intelectual
				

2. Introducción

Esta unidad propone un enfoque metodológico para la resolución de problemas de redes inalámbricas. El principal asunto de la resolución de problemas de cualquier red de comunicación es identificar qué está pasando cuando las cosas "van mal". En lugar de reiniciar todo aquello que sea enchufable a la corriente, o de echarle la culpa a las condiciones climáticas, proponemos seguir el modelo OSI para intentar encontrar la causa del problema.

El modelo de referencia OSI (*Interconexión de sistemas abiertos*), creado por ISO (Organización de Estándares Internacionales), es una descripción abstracta para el diseño de protocolos de redes de computadoras. El modelo divide las diferentes funciones de comunicaciones en siete capas que pueden trabajar independientes unas de otras.

El diseño del protocolo de Internet sigue una estructura similar a la del modelo OSI. Cada *capa* del protocolo sólo usa la funcionalidad de la capa de abajo y provee funcionalidad solamente a las capas de arriba.

Esta estructura es de gran ayuda cuando se trata de resolver un problema pues nos ayuda a aislar donde está localizado el problema. Lo primero que necesitamos hacer cuando las cosas van mal es tratar de identificar en qué “capa” aparece el problema y cuál capa es la causa del problema.

Por ejemplo, los usuarios siempre se quejarán de que una aplicación “x” no está funcionando! (Capa 7 de OSI) pero la causa del problema puede estar en alguna de las capas de abajo. Por ejemplo, esto puede estar relacionado con la falta de señal de radio (Capa 1 de OSI) o a la falta de una dirección IP (Capa 3 de OSI).

Capa	OSI	TCP/IP
7	Aplicación	Aplicación
6	Presentación	
5	Sesión	Transporte (TCP)
4	Transporte	
3	Red	Red (IP)
2	Enlace de datos	Control de Acceso al medio
1	Física	

Tabla 1: Modelo OSI versus la suite de protocolos TCP/IP

3. Antes del modelo OSI

Antes de que el modelo OSI se vuelva una metodología aplicable para la resolución de problemas, debemos asegurarnos de que todas las unidades implicadas estén correctamente iniciadas y estén equipadas con el más reciente firmware.

3.1 Fuente de corriente estable

Cuando un equipamiento inalámbrico aranca, el hardware es extremadamente sensible a fluctuaciones de la tensión eléctrica. Una interrupción o fluctuación de energía , causada ya sea por un corte en el fluido eléctrico, un bajón en la corriente o por alguna accidental desconexión del enchufe, puede causar un daño fatal a las partes del dispositivo inalámbrico.

Ejemplos de hardware que pueden ser afectados por interrupción de la energía son las memorias flash y los controladores Ethernet. Si la memoria flash es dañada durante la secuencia de arranque, la unidad completa debe ser reemplazada. Si un controlador Ethernet falla (suponiendo que sólo uno estaba disponible), el dispositivo se vuelve inusable puesto que, aunque la parte inalámbrica podría funcionar, ni la red local, ni la salida a Internet podría ser conectada al dispositivo.

Tenga siempre esto en mente: use siempre una fuente estable de energía cuando esté trabajando con dispositivos inalámbricos, especialmente en el momento del arrancar. Si sabe que el sistema eléctrico es inestable, use un UPS o un estabilizador para proteger el equipamiento.

Daños similares al hardware pueden también ocurrir cuando al alimentar un dispositivo con muy bajo o muy alto voltaje y/o corriente. Esto puede ocurrir accidentalmente si usa una fuente de alimentación inadecuada. Las fuentes de alimentación tienden a verse muy similares independiente de qué marca o modelo están diseñados y es fácil intercambiar y confundir fuentes de diferentes unidades. Si su implementación inalámbrica incluye dispositivos de diferentes marcas y modelos, marque todas las fuentes (con cinta o similar) con la marca y modelo para la que ha sido diseñado y escriba el voltaje y la corriente que erogan.

Antes de prender una unidad inalámbrica, estudie primero el comportamiento normal de los LEDs en el Manual de Usuario. Haciendo esto, podrá fácilmente seguir la secuencia de arranque y asegurarse de que el dispositivo lo ha hecho apropiadamente.

3.2 Actualización del Firmware

El firmware es una pieza de software que está embebida en un dispositivo de hardware. A menudo viene en una memoria flash de sólo lectura (ROM) o como un archivo de imagen binario que puede ser inscrito sobre el hardware por el usuario.

Cada dispositivo viene con una versión de firmware que ha sido instalado por el fabricante. Sin embargo, el firmware de un dispositivo es constantemente actualizado y siempre habrá disponibles nuevas versiones. Es responsabilidad del cliente mantener actualizado el firmware de estos dispositivos. Comúnmente el más reciente firmware está disponible para descargas en el sitio web del fabricante.

La actualización de firmware puede mejorar las prestaciones y confiabilidad de un dispositivo y corregir defectos (bugs) de funcionamiento. También puede mejorar la funcionalidad básica disponible de un dispositivo introduciéndole nuevas rutinas.

Haga un hábito el comprobar siempre la versión del firmware de una nueva unidad con la que vaya a trabajar. El dispositivo puede haber estado almacenado por varios meses por un vendedor local y contener una versión de firmware no actualizado en el momento en que adquiera la unidad.

Usar una versión no actualizada de firmware puede resultar en un problema inesperado, dependiendo de qué aspectos hayan sido corregidos desde esa versión. Correr un dispositivo con un firmware no

actualizado puede causar muchas horas de frustración aún usando las metodologías presentadas en este documento.

4. Metodología

Dependiendo de la información que tengamos en adelante podemos tomar dos enfoques:

- Resolución de problemas de arriba a abajo y
- Resolución de problemas de la mitad a arriba, o de la mitad a abajo.

4.1 Resolución de problemas de arriba a abajo

Cuando hay un “problema”, la resolución de problemas de arriba a abajo comienza verificando la configuración de la aplicación y termina verificando si hay interferencia en el radio enlace, o si hay un bajo nivel de señal en el radio receptor.

4.2 Resolución de problemas de la mitad a arriba, de la mitad a abajo

Cuando hay un “problema”, este enfoque inicia verificando si hay conectividad IP al servicio solicitado o el enrutador de frontera, y dependiendo del resultado intenta resolver las capas de arriba o de abajo. Este enfoque es el más popular, ping <el servicio>, ping <el enrutador>.

Desafortunadamente, la mayoría de las veces esto solo ayuda a identificar con quién quejarse, en vez de resolver el problema. Si el “ping” al enrutador de frontera falla, entonces podemos quejarnos con el proveedor inalámbrico; si el ping al servicio falla, entonces podemos quejarnos con el proveedor internacional. Si ninguno de estos falla, entonces nos quejamos del usuario o del sistema operativo.

Cualquiera que sea el enfoque que tomemos para resolver un problema es importante que estemos familiarizados con las herramientas que son apropiadas cuando analizamos cada una de las capas funcionales de nuestra red.

El último objetivo de tener una metodología es que le permitirá describir *procedimientos de resolución de problemas* y ser capaz de identificar qué problemas requieren altos niveles de experticia.

4.3 Ejemplo práctico

Tomemos un ejemplo para ilustrar el enfoque. Si alguien le llama y grita “!No puedo leer mi hotmail !”, usted necesita tener un método para identificar la causa sin tener que llamar al mejor de sus ingenieros de red.

Si seguimos el *primero* de los métodos propuestos (de arriba a abajo) haremos las siguientes preguntas tratando de identificar donde está el problema:

- ¿Qué programa usa para chequear su e-mail? (Verificando problemas de aplicación)
- ¿Puede verificar las configuraciones de proxy de su programa?
- ¿Logra entrar a otros sitios de Internet? (Verificando problemas de DNS)
- ¿Tiene su aplicación un tiempo de desconexión (time out)? (Verificando problemas de sesión TCP)
- ¿Se ha autenticado con el servidor de control de acceso? (Verificando problemas de autenticación)
- ¿Logra entrar al sitio web del enrutador/proveedor? (Verificando problemas de enrutamiento)
- ¿Tiene una dirección IP? (Verificando problemas de IP)

Si seguimos el *segundo* método propuesto (de la mitad a abajo/a arriba) haremos las siguientes preguntas:

- ¿Puede hacer ping a hotmail.com?
- ¿Puede hacer ping a <dirección IP del enrutador de frontera del ISP inalámbrico>?

Si las dos respuestas son “no”:

- ¿Tiene una dirección IP?
- ¿Se ha autenticado con el servidor de control de acceso?

Clasificar los problemas no es una tarea fácil; los problemas varían de red a red – pero la *metodología* que usamos para resolverlos siempre es la misma.

Hay una manera fácil de clasificar cualquier problema en una red:

- Las cosas no funcionan nunca (¿Por qué mi computadora no <incluir palabra aquí>?)
- Las cosas no funcionan a veces... (o las cosas funcionan, pero “mal”) (¿Por qué mi computadora esta tan lenta?)

El **primer tipo** de problema es normalmente más fácil de resolver, proviene de problemas relacionados con un mal presupuesto del enlace, pérdida de potencia en el equipo, desalineamiento de antenas, mala configuración, etc.

El **segundo tipo** de problema, especialmente cuando se relaciona con las capas más bajas de la pila TCP/IP, es más difícil de resolver y requerirá que monitoree todos los parámetros inalámbricos durante un periodo de tiempo mientras intenta identificar la causa del problema.

En la tabla 2, incluimos un conjunto de herramientas que pueden ayudarnos a resolver estos problemas.

Capa	Nombre Capa	TCP/IP	Herramientas
7	Aplicación	Aplicación	nslookup
6	Presentación		
5	Sesión	Transporte (TCP)	Ntop (Win32/Linux) Visualroute, traceroute
4	Transporte		
3	Red	Red (IP)	Nmap Ntop (Win32/Linux) Ethereal Etherape
2	Enlace de datos	Control de Acceso al Medio	Ethereal (Win32/Linux) Netstumbler (Win32) Kismet, Wavemon, Wellenreiter Herramientas de administración específicas del fabricante
1	Física		

Tabla 2: Herramientas para la resolución de problemas en cada una de las siete capas de la pila de protocolos TCP/IP

Para identificar problemas en el medio inalámbrico podemos usar dos tipos de herramientas: herramientas que trabajan con cualquier producto IEEE 802.11b, y aquellas que vienen con cada fabricante específico.

Algunos fabricantes (p.e. Proxim con Orinoco Outdoor Solutions) implementan *extensiones* al IEEE 802.11b que requieren herramientas de monitoreo y resolución de problemas muy específicas.

5. Herramientas para la resolución de problemas

1. Nslookup, dig
2. Ntop
3. Visualroute, traceroute
4. Nmap
5. Ethereal (Ver escenario 3)
6. Etherape (Ver escenario 2)
7. Netstumbler (Ver escenario 1)
8. Kismet
9. Herramientas de administración específicas del fabricante.

6. Escenario 1: ¿Interferencias de radio?, ¿Canales ocupados?

No existe una forma fácil de monitorear todos los parámetros involucrados en la “capa física” de nuestra red inalámbrica. Se dispone de herramientas que permiten diagnosticar el funcionamiento de las tarjetas de radio con mayor o menor versatilidad dependiendo del sistema operativo utilizado.

Usando un programa como “Netstumbler”, una tarjeta inalámbrica actúa como un analizador de espectros rudimentario que puede escanear redes existentes, indicando su relación señal/ruido, tasa de transmisión, canal y modo de operación. Netstumbler recoge toda la información y la proporciona en una interfaz fácil de usar.

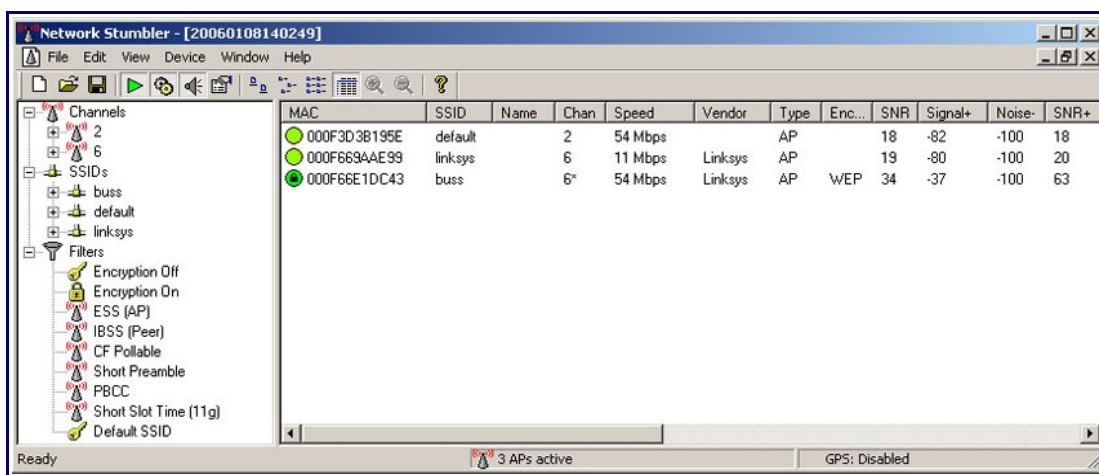


Figura 1: Interfaz de Netstumbler. **Fuente:** <http://upload.wikimedia.org/wikipedia/en/9/95/Netstumbler.jpg>

En el ejemplo (**Figura 1**), podemos ver que hay tres SSID presentes (default, linksys, buss) en “apenas” dos canales (2 y 6). Dos de los access point están operando en el estándar “g” de 54Mbps (default y buss) y el tercero en el estándar “b”.

El cifrado WEP está habilitado en la red con SSID = buss. Todas las redes son escuchadas con buenas S/N (relación señal ruido) SNR>10dB

Netstumbler es un software “pasivo” que escucha el tráfico inalámbrico de una red. No todas las tarjetas inalámbricas van a permitirle “monitorear” la totalidad del tráfico inalámbrico. Antes de instalar Netstumbler, verifique que su tarjeta inalámbrica lo soporte.

7. Escenario 2: ¿Red congestionada? ¿Inundación?

Si quiere tener una “vista general” del tipo de comunicaciones IP que están activas en su red inalámbrica, puede usar un programa de Unix “EtherApe” en su gateway cableado. EtherApe le permite monitorear conexiones *entrantes* y *salientes* enrutadas hacia su red inalámbrica. Puede

ayudarlo no solo a identificar el tipo de tráfico IP presente y la distribución de tráfico entre sus nodos, sino también a saber cuán “dinámica” es su red. Observando las gráficas de tráfico con el software, estará en capacidad de detectar virus provenientes de ciertos clientes, o la presencia de tráfico FTP o peer-to-peer pesado. Hay programas similares y analizadores de protocolo más sofisticados también para MS Windows (AirDefense, Scrutinizer, SolarWinds, etc.), pero pocos de ellos son libres (posiblemente ninguno).

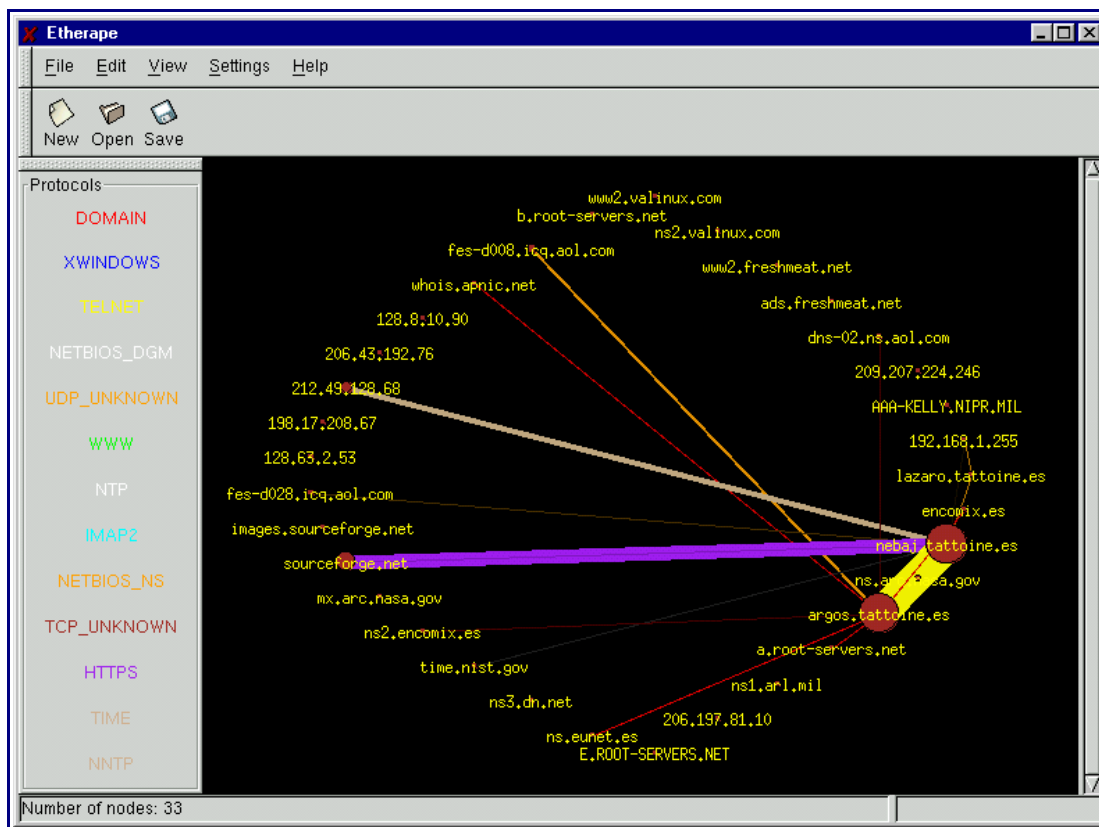


Figura 2: Interfaz gráfica de EtherApe, conexiones IP activas.

En el ejemplo (**Figura 2**) podemos ver que hay una gran cantidad de HTTPS (Tráfico web seguro) entre el nodo “neba1” y “sourceforge” (línea violeta). También podemos ver que hay una conexión “Telnet” entre los nodos “neba1” y “argos” (línea amarilla). El tráfico DNS está trabajando apropiadamente desde “argos” hasta “ns.eunet.es” y “ns2.encomix.es” (líneas rojas) El tráfico UDP desconocido (línea marrón) corresponde al tráfico del ICQ Messenger (conexión a fes-d008.icq.aol.com)

8. Escenario 3: ¿Por qué este servicio de red no está trabajando? ¿Conexión rechazada?

Si necesita tener una visión más cercana de lo que le está pasando a un tipo de tráfico específico, considere la instalación de Ethereal. Ethereal le permitirá capturar todo el tráfico que está pasando por su interfaz y examinar los flujos de tráfico y los bits y bytes de cada transacción.

Ethereal es muy útil para monitorear:

- **Pérdida de paquetes en conexiones TCP:** lo que normalmente es un indicador de una red congestionada, colisiones, etc.
- **Tiempo de retorno:** lo que es una indicación de la latencia (retardo) de su red. Altos tiempos de retorno dentro de su red inalámbrica son una indicación del alto nivel de utilización del canal o de colisiones de paquetes.
- **Errores de protocolo:** errores que normalmente no son visibles al usuario como autenticación inapropiada, direcciones IP duplicadas, red destino inaccesible, inundación ICMP, etc.

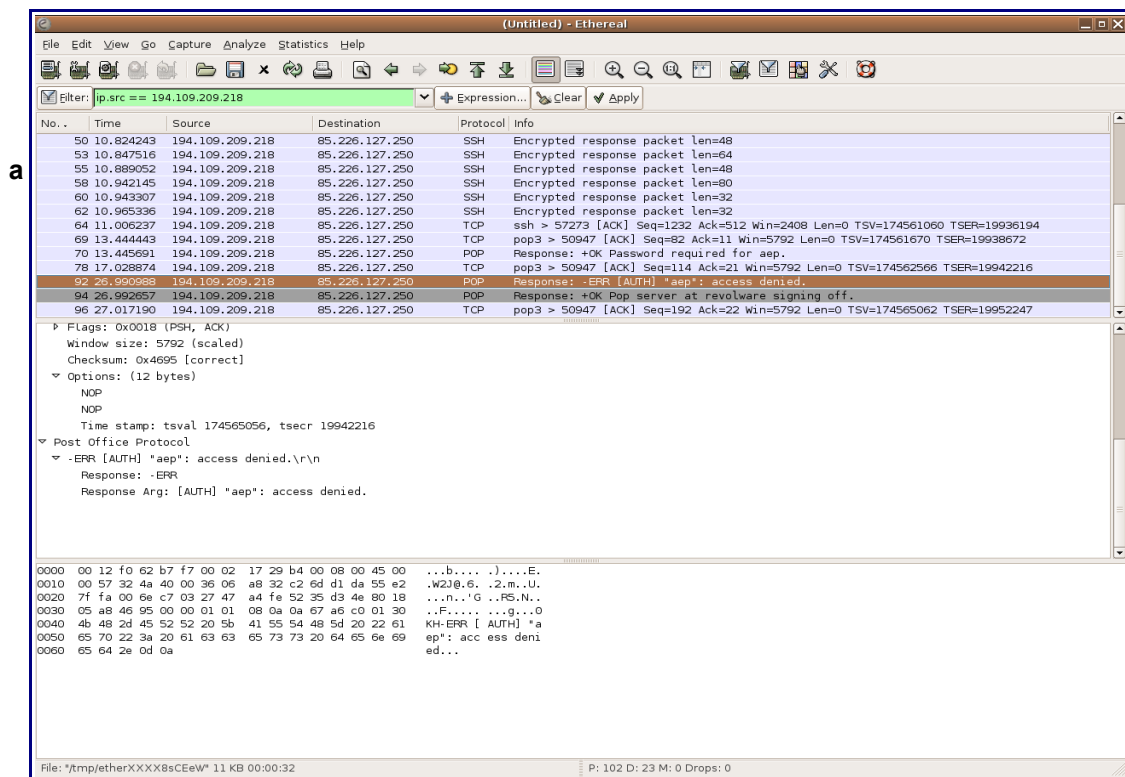


Figura 3:

Resolución de problemas de correo POP3 con Ethereal

Sólo para mostrar cuán potente puede ser Ethereal en la resolución de problemas, en el ejemplo (Figura 3), podemos ver el nivel de detalle que puede alcanzarse con Ethereal.

- Después de capturar tráfico de la red podemos aplicar un filtro (ip.src=194.109.209.218) para filtrar todos los paquetes provenientes del servidor de correo POP. (caja verde)

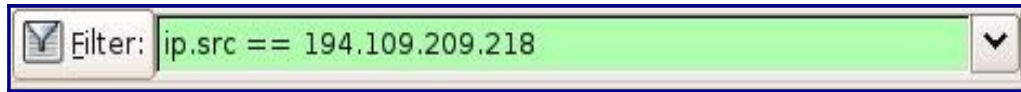


Figura 3 a: Caja verde

- Después de filtrar todos los paquetes podemos ver el intercambio de tráfico entre el servidor de correo (violeta). El tráfico marcado como TCP indica la renegociación de la conexión (conocida como 'handshake' o apretón de manos); el tráfico marcado como POP3 corresponde a la Aplicación "POP3", recuperador de correo.

No. .	Time	Source	Destination	Protocol	Info
50	10.824243	194.109.209.218	85.226.127.250	SSH	Encrypted response packet len=48
53	10.847516	194.109.209.218	85.226.127.250	SSH	Encrypted response packet len=64
55	10.889052	194.109.209.218	85.226.127.250	SSH	Encrypted response packet len=48
58	10.942145	194.109.209.218	85.226.127.250	SSH	Encrypted response packet len=80
60	10.943307	194.109.209.218	85.226.127.250	SSH	Encrypted response packet len=32
62	10.965336	194.109.209.218	85.226.127.250	SSH	Encrypted response packet len=32

Figura 3 b: Caja violeta

- Podemos seleccionar paquetes individuales de la sesión POP3 y ver la presencia de -ERR (AUTH): "aep access denied".

Con esta información podemos determinar que: la conexión desde nuestro cliente hasta el servidor de correo, el servidor POP3 está respondiendo, y que el problema está en la autenticación. Un problema de autenticación puede venir del lado del cliente o del lado del servidor: el cliente ha enviado una contraseña errada o el servidor no la valida correctamente.

9. Controlando la interferencia

9.1 Interferencia y ruido

Un desafío que eventualmente vamos a encarar cuando operamos equipamiento WIFI en exteriores es minimizar la potencia transmitida para reducir los efectos de la interferencia y el ruido.

Una señal fuerte no es suficiente para que un receptor inalámbrico de banda ancha trabaje eficientemente. El nivel de la señal recibida debe ser consistentemente más alto que el ruido recibido. La relación señal/ruido (S/N por sus siglas en inglés) debe ser tan alta como sea posible. Para tener un S/N alta, hay dos condiciones simultáneas a ser satisfechas:

- El receptor debe recibir una señal que está por encima de su sensibilidad.
- El nivel de ruido en la entrada del receptor debe ser más bajo que el nivel de la señal deseada. Ruido es definido como "todo lo que no sea la señal deseada".

La falla de estas dos condiciones resultará en una S/N inaceptable.

10.2 Maximizando el nivel de la señal recibida

Tenemos control directo para maximizar la señal recibida. Algunos de los procedimientos estándar son:

- Presupuesto del enlace – suficiente potencia de transmisión, sensibilidad del receptor, margen de operación y ganancia de la antena para superar la pérdida en el espacio libre y la pérdida de los cables.
- Línea de vista (LOS, por su sigla en inglés) – La ruta de la línea de vista sin obstáculos de principio a fin.
- Zona de Fresnel – lo suficientemente despejada por encima y entre los obstáculos de la ruta.
- Instalación – asegúrese de que la antena esté bien montada, alineada correctamente, y que los conectores están aislados de la humedad, use buenos conectores (no use conectores coaxiales baratos).

10.3 Minimizando los niveles de interferencia y ruido

Normalmente no tenemos mucho control sobre las fuentes de interferencia y ruido. Algunas de las fuentes de ruido son:

- Ruido natural – ruido atmosférico y galáctico.
- Ruido hecho por el hombre – señales RF captadas por nuestra antena. Esto incluye hornos microondas, teléfonos inalámbricos y redes de área local inalámbricas.
- Ruido del receptor – ruido generado al interior de la circuitería del receptor.
- Interferencia de otras redes – interferencia causada por redes inalámbricas cercanas en la misma banda.
- Interferencia desde nuestras propias redes – esto ocurre cuando usamos la misma frecuencia más de una vez, usando canales que no tienen suficiente espacio entre ellos, o seleccionando secuencias de salto de frecuencia incorrectas.
- Interferencia de señales fuera de banda. Proviene de señales muy fuertes, que operan en otras bandas de frecuencia, pero que por su intensidad introducen ruido en bandas adyacentes. Entre estas tenemos transmisores de AM, FM, radios de dos vías, etc.

10.4 Estrategias para controlar la interferencia

Algunas de las típicas estrategias para controlar la interferencia son las siguientes:

1. Uso de antenas sectoriales o direccionales, usualmente antenas de alta ganancia. Esta es la más fácil y efectiva forma de reducir la interferencia en áreas de espectro saturado.
2. Rutas cortas.

3. Selección de frecuencias que no muchas estaciones están usando.
4. Cambiando la polarización de la antena.
5. Ajustando el acimut de la antena.
6. Localización de la antena/equipamiento.

10. Conclusiones

Los cinco principales aspectos que debe recordar de esta unidad pueden sintetizarse en:

1. Cuanto más sepa cómo funcionan las cosas, más fácil será solucionarlas cuando no funcionen.
2. Entender un problema no es lo mismo que resolver un problema.
3. Intente aplicar una metodología lógica cuando las cosas fallen, en lugar de hacer las cosas en orden aleatorio.
4. En cualquier enfoque que tomemos para la resolución de problemas, es importante estar familiarizado con las herramientas apropiadas para analizar cada una de las capas funcionales de la red.
5. Cuando identificamos problemas en el medio inalámbrico, podemos usar dos tipos de herramientas: las que trabajan con cualquier producto compatible al estándar IEEE 802.11 y aquellas que vienen con cada fabricante específico.

11. Declaración de Derechos de Propiedad Intelectual

Los materiales desarrollados en el marco del proyecto TRICALCAR utilizan una versión resumida del formato MMTK – Multimedia Training Kit. Han sido desarrollados para ser utilizados y compartidos libremente por instructores/as vinculados a proyectos de nuevas tecnologías para el desarrollo.

Todos los materiales están disponibles bajo una de las licencias Creative Commons <<http://creativecommons.org/>>. Estas licencias han sido desarrolladas con el propósito de promover y facilitar que se compartan materiales, pero reteniendo algunos de los derechos del autor sobre la propiedad intelectual.

Debido a que las organizaciones del Proyecto TRICALCAR que usan el formato MMTK para el desarrollo de sus materiales tienen diversas necesidades y trabajan en contextos diferentes, no se ha desarrollado una licencia única que cubra a todos los materiales. Para mayor claridad sobre los términos y condiciones en las que usted puede utilizar y redistribuir cada unidad temática, por favor verifique la declaración de derechos de propiedad intelectual incluida en cada una de ellas.

Provisiones de derechos de propiedad intelectual para esta unidad: Esta unidad temática se ha hecho disponible bajo los términos de la licencia **Atribución- No Comercial-Licenciamiento Recíproco**, bajo los siguientes términos:

- **Atribución.** Reconocer la autoría del material en los términos especificados por el propio autor o licenciante.
- **No comercial.** No puede utilizarse este material para fines comerciales.
- **Licenciamiento Recíproco.** Si altera, transforma o crea un material a partir de este, solo podrá distribuir el material resultante bajo una licencia igual a esta.

Documento preparado para el taller de comunicaciones inalámbricas de Tshwane en Sudáfrica (c) 7th September 2005, Creative Commons Deed. Attribution-NonCommercial-ShareAlike 2.0 (c) 21 abril 2007. Cambios en la versión 1.1:Sección 3 adicionada (Antes del modelo OSI). Discusión sobre la importancia de fuentes de corriente estable y la actualización de firmware para los equipamientos.