Unidad 11

Resolución de Problemas en Redes Inalámbricas

Desarrollado por:
Alberto Escudero-Pascual
Louise Berthilson
IT +46

Objetivos

- La resolución de problemas es el ”arte” de saber qué hacer después
- La resolución de problemas es el ”arte” de encontrar a quién/de qué quejarse

Tabla de Contenidos

Un pequeño recordatorio...

Layer	ISO	TCP/IP
7	Aplicación	Aplicación
6	Presentación	
5	Sesión	Transporte
4	Transporte	
3	Red	Red
2	Enlace de datos	Acceso al medio
1	Física	

Consideraciones previas

- Arranque del dispositivo
- Actualización del firmware

Proceso de arranque

- Fuente de corriente estable
  - UPS o estabilizador si el sistema es inestable
  - Cuidado con el cable de potencia!
- Fluctuaciones de corriente
  - Falla en el hardware (memoria flash, circuito Ethernet)
- Fuente de potencia correcta!
  - Marcar con la marca y modelo

Firmware

- Pieza de software embebida en el hardware
- Instalado por el fabricante
- Actualizado frecuentemente
- Los clientes son responsables de actualizar el firmware

Actualización de firmware

- Mejora el performance y fiabilidad
  - adicionando parches y corrigiendo bugs
- Adiciona o mejora la funcionalidad básica disponible
  - introduciendo nuevas rutinas

Actualización del firmware

- Siempre verifique la versión del firmware y actualícelo si es necesario
- Los equipamientos pueden haber estado almacenados largo tiempo
- Firmware antiguo puede resultar en cuaquier forma de problema inesperado
- Imposible de resolver usemos la herramienta que usemos

Metodología

- **Arriba-Abajo**
  - Empezar con: configuraciones de la aplicación
  - Terminar con: interferencia inalámbrica, SNR
- **Mitad-arriba** o **Mitad-abajo**
  - Empezar con: Conectividad Internet <ping>
  - Continuar arriba/abajo dependiendo del resultado
- **Abajo-Arriba**
  - Empezar con: interferencia inalámbrica,SNR..
  - Terminar con: capa de aplicación

No puedo leer mi Hotmail!

(equiv: la impresora no está funcionando)

Arriba-Abajo

- ¿Qué aplicación de correo está usando?
  - Configuraciones de la aplicación, proxys
- ¿Logra entrar a otros sitios de Internet?
  - ¿Problemas de DNS?
- ¿Tiene su aplicación un tiempo de desconexión(time out)?
  - ¿Problemas de sesión de TCP?

Arriba-Abajo

- ¿Se ha autenticado con el servidor de control de acceso?
- ¿Logra llegar hasta su proveedor de servicio?
- ¿Problemas de enrutamiento?
- ¿Tiene una dirección IP?

Mitad-arriba/Mitad-abajo

- ¿Puede hacer ping a hotmail.com?
- ¿Puede hacer ping al enrutador de frontera de su ISP inalámbrico?
- Por ejemplo, si ambas respuestas son ”no”:
- ¿Tiene una dirección IP?
- ¿Se ha autenticado con el servidor de control de acceso?

Clasificación del problema

- Justificaciones típicas de los problemas ”Los expedientes X”
  - Interferencia por varias razones
  - La red no es muy ”rápida”
  - Los paquetes se pierden
  - Mucha gente
  - Condiciones climáticas

Herramientas de resolución de problemas – capa de enlace

- Herramientas que trabajan con cualquier producto IEE802.11b (trabajan en modo promiscuo)
- Herramientas que vienen con cada fabricante específico

(Accesando a los equipos por SNMP!)

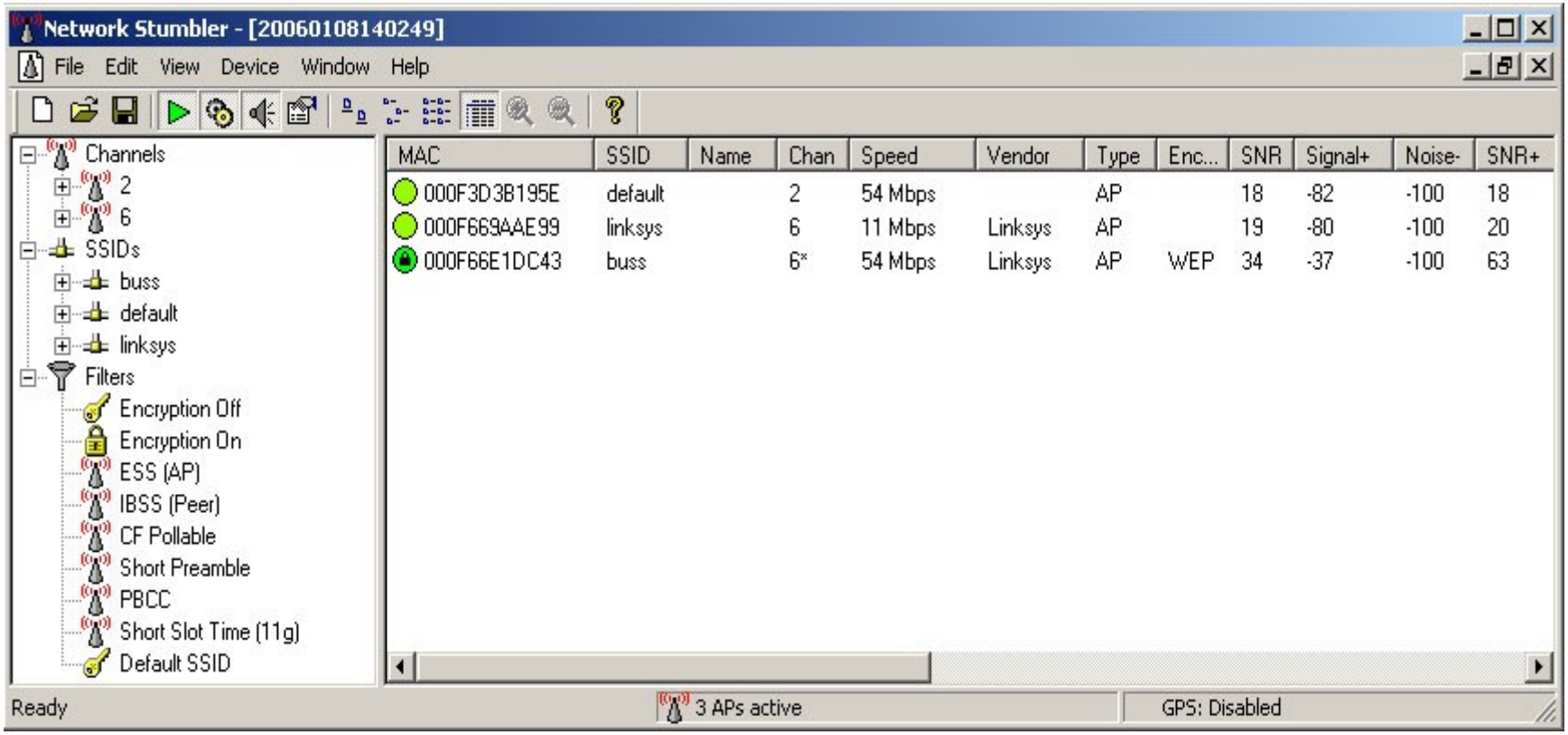
Herramientas de resolución de problemas

TCP/IP	***Herramientas***
Aplicación	nslookup
Transporte (TCP)	Ntop (Win32/Linux) Visualroute, traceroute
Red (IP)	Nmap, Ntop (Win32/Linux) Ethereal, Etherape
Control de Acceso al Medio	Ethereal (Win32/Linux) Netstumbler (Win32), Kismet, Wavemon, Wellenreiter **Herramientas específicas del fabricante**

Tres escenarios para la resolución de problemas

- Problemas a nivel de enlace (Netstumbler)
  - Problemas en el canal de inalámbrico?
- Problemas a nivel de IP (Etherape)
  - ¿Red congestionada? Lenta
- Problemas con aplicación (Ethereal)
  - No puedo chequear mi correo

Netstumbler

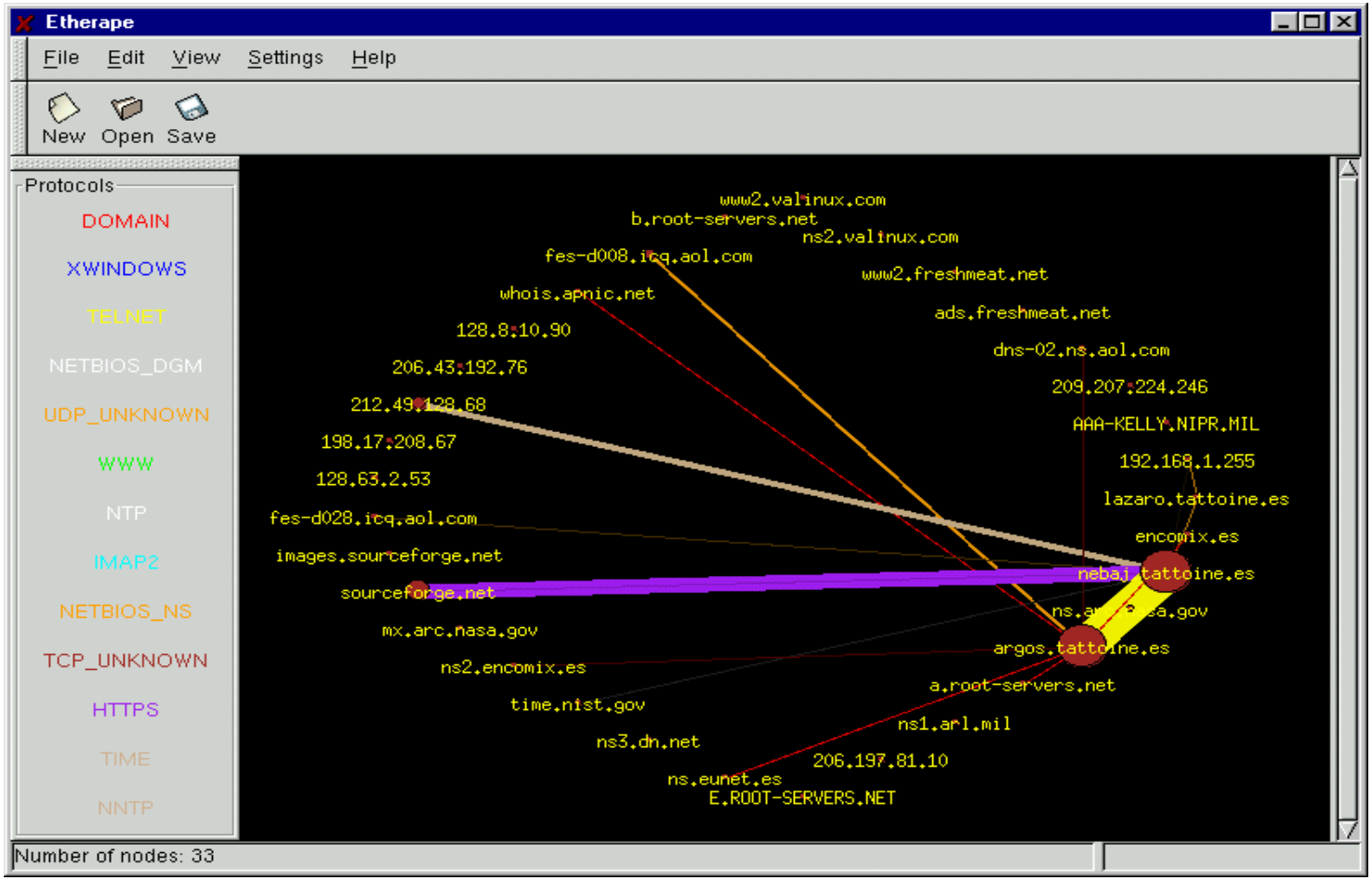


Netstumbler

- Recupera información de la capa física y de enlace en modo ”pasivo”
- ¿Qué canales, SSID, WEP se encuentran?
- Monitorea el ratio SNR de cada enlace en nuestra posición

WiSpy

EtherApe


Etherape
File Edit View Settings Help
New Open Save
Protocols
DOMAIN
XWINDOWS
TELNET
NETBIOS_DGM
UDP_UNKNOWN
WWW
NTP
IMAP2
NETBIOS_NS
TCP_UNKNOWN
HTTPS
TIME
NNTP
www2.valinux.com
b.root-servers.net
ns2.valinux.com
fes-d008.icq.aol.com
www2.freshmeat.net
whois.apnic.net
ads.freshmeat.net
128.8.10.90
dns-02.ns.aol.com
206.43.192.76
209.207.224.246
212.49.128.68
AAA-KELLY.NIPR.MIL
198.17.208.67
192.168.1.255
128.63.2.53
lazaro.tattoine.es
fes-d028.icq.aol.com
encomix.es
images.sourceforge.net
sourceforge.net
mx.arc.nasa.gov
argos.tattoine.es
ns2.encomix.es
a.root-servers.net
time.nist.gov
ns1.arl.mil
ns3.dn.net
206.197.81.10
ns.eunet.es
E.ROOT-SERVERS.NET
Number of nodes: 33

EtherApe

- Identifica los flujos de tráfico y sus distribución
- Estudia las ”dinámicas” de la red
- Detecta programas maliciosos: virus, escaneadores de puertos, inundación...
- Verifica en alto nivel la conectividad IP: DNS, HTTP y servicios de correo

Ethereal

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: ip.src == 194.109.209.218 Expression... Clear Apply

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
64	11.006237	194.109.209.218	85.226.127.250	TCP	ssh > 57273 [ACK] Seq=1232 Ack=512 Win=2408 Len=0 TSV=174561060 TSER=19936194
69	13.444443	194.109.209.218	85.226.127.250	TCP	pop3 > 50947 [ACK] Seq=82 Ack=11 Win=5792 Len=0 TSV=174561670 TSER=19938672
70	13.445691	194.109.209.218	85.226.127.250	POP	Response: +OK Password required for aep.
78	17.028874	194.109.209.218	85.226.127.250	TCP	pop3 > 50947 [ACK] Seq=114 Ack=21 Win=5792 Len=0 TSV=174562566 TSER=19942216
92	26.990988	194.109.209.218	85.226.127.250	POP	Response: -ERR [AUTH] "aep": access denied.
94	26.992657	194.109.209.218	85.226.127.250	POP	Response: +OK Pop server at revolware signing off.
96	27.017190	194.109.209.218	85.226.127.250	TCP	pop3 > 50947 [ACK] Seq=192 Ack=22 Win=5792 Len=0 TSV=174565062 TSER=19952247

```
▷ Flags: 0x0018 (PSH, ACK)
  Window size: 5792 (scaled)
  Checksum: 0x4695 [correct]
▽ Options: (12 bytes)
    NOP
    NOP
    Time stamp: tsval 174565056, tsecr 19942216
▽ Post Office Protocol
▽ -ERR [AUTH] "aep": access denied.\r\n
    Response: -ERR
    Response Arg: [AUTH] "aep": access denied.
```

```
0000  00 12 f0 62 b7 f7 00 02  17 29 b4 00 08 00 45 00   ...b.... .)....E.
0010  00 57 32 4a 40 00 36 06  a8 32 c2 6d d1 da 55 e2   .W2J@.6. .2.m..U.
0020  7f fa 00 6e c7 03 27 47  a4 fe 52 35 d3 4e 80 18   ...n..'G ..R5.N..
0030  05 a8 46 95 00 00 01 01  08 0a 0a 67 a6 c0 01 30   ..F..... ...g...0
0040  4b 48 2d 45 52 52 20 5b  41 55 54 48 5d 20 22 61   KH-ERR [ AUTH] "a
0050  65 70 22 3a 20 61 63 63  65 73 73 20 64 65 6e 69   ep": acc ess deni
0060  65 64 2e 0d 0a                                    ed...
```

File: "/tmp/etherXXXX8sCEeW" 11 KB 00:00:32 P: 102 D: 23 M: 0 Drops: 0

Ethereal

- Información detallada sobre cierto flujo de tráfico
- Puede filtrar y examinar basandose en transacciones
- Puede determinar si es:
  - Problema de conectividad (host inaccesible)
  - Problema de servicio (servicio no disponible)
  - Problema de servidor/usuario (autenticación, aplicación, configuración)

Problemas con ”redes inalámbricas”

Los problemas con ”redes inalámbricas” están relacionados con....

- Física: nodos ocultos, multitrayecto, ruido
- IP: diseño de la red, dhcpd multiple, velocidades de transmisión asimétricas
- Aplicación: virus, peer-to-peer

Conclusiones

- Cuanto más sepa como funcionan las cosas...más fácil será solucionarlas cuando no funcionen!
- Entender un problema no es lo mismo que resolver un problema.

Tips finales!

- Toma menos tiempo reconstruir un sistema sin documentación que tratar de resolverlo
- Si necesita ayuda, esté preparado para aportar información y documentación