

Wireless Troubleshooting

Developed by: Alberto Escudero-Pascual, IT +46

Goals

- Troubleshooting is the “art” of knowing what to do next
- Troubleshooting is the “art” of discovering who/what to blame

Table of Contents

- Methodology
 - Where do we start?
- Classification of problem
 - What is going wrong?
- General troubleshooting tools
 - What can help?

Friendly reminder... who to blame!

Layer	ISO	TCP/IP
7	Application	Application
6	Presentation	
5	Session	Transport
4	Transport	
3	Network	Network
2	Data link	Media Access
1	Physical	

Methodology

- **Top-down**
 - Start with: application configurations
 - Finish with: wireless interface, SNR
- **Middle-top** or **Middle-down**
 - Start with: Internet connectivity <ping>
 - Continue up/down depending on result
- **Down-Top**
 - Start with: wireless interface, SNR ...
 - Finish with: application layer

I can't read my Hotmail!

(equiv: the printer is not working!)

Top-down

- What e-mail application are you using?
 - Application settings, proxies
- Can you reach other sites?
 - DNS problems?
- Does your application time out?
 - TCP session problems?
- Are you authenticated to the access-control server?
- Can you reach your provider?
 - Routability problems?
- Do you have an IP address?

Middle-top/middle-down

- Can you ping hotmail.com?
- Can you ping the border router of your WISP?

For example, if both answers are “no”:

- Do you have an IP address?
- Are you authenticated with the access-control server?

Classification of problem

- Typical X-files type classifications:
 - Interference for various reasons
 - Network is not “fast”
 - Packets get lost
 - Lots of people
 - Weather conditions

Troubleshooting tools – link layer



- Tools that work with any IEEE 802.11b compliant product
(Listen - troubleshoot)
- Tools that come with every specific vendor
(Accessing/SNMP the boxes!)

Troubleshooting tools

TCP/IP	Tools
Application	nslookup
Transport (TCP)	Ntop (Win32/Linux) Visualroute, traceroute
Network (IP)	Nmap, Ntop (Win32/Linux) Ethereal, Etherape
Media Access Control	Ethereal (Win32/Linux) Netstumbler (Win32), Kismet, Wavemon, Wellenreiter Vendor Specific Tools

Three scenarios for troubleshooting

- Link level problems (Netstumbler)
 - Problems in the radio channel?
- IP level problems (Etherape)
 - Congested network? Slow
- Application problems (Ethereal)
 - Can not check my mail.

Netstumbler

The screenshot displays the Netstumbler application window. The title bar reads "Network Stumbler - [20060108140249]". The menu bar includes "File", "Edit", "View", "Device", "Window", and "Help". The toolbar contains various icons for file operations and scanning. The left sidebar shows a tree view with categories: Channels (2, 6), SSIDs (buss, default, linksys), and Filters (Encryption Off, Encryption On, ESS (AP), IBSS (Peer), CF Pollable, Short Preamble, PBCC, Short Slot Time (11g), Default SSID). The main pane shows a table of detected networks:

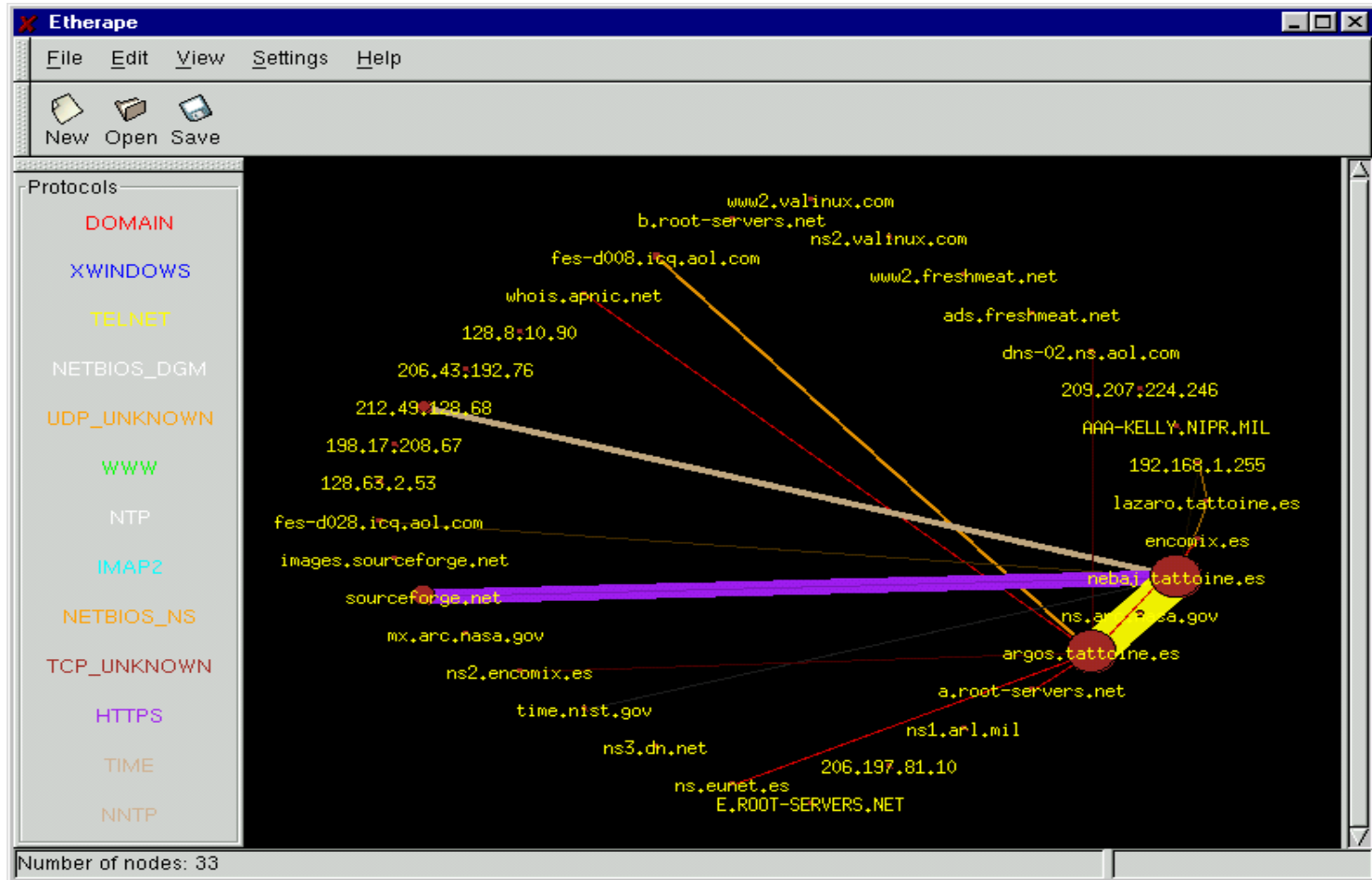
MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise-	SNR+
000F3D3B195E	default		2	54 Mbps		AP		18	-82	-100	18
000F669AAE99	linksys		6	11 Mbps	Linksys	AP		19	-80	-100	20
000F66E1DC43	buss		6*	54 Mbps	Linksys	AP	WEP	34	-37	-100	63

The status bar at the bottom indicates "Ready", "3 APs active", and "GPS: Disabled".

Netstumbler

- Retrieve physical/link layer info in "passive" mode
- Use our wireless card as a "radio analyser"
- Which channels, SSID, WEP are present?
- Monitor the SNR of each of them in our position

EtherApe



EtherApe

- Identify traffic flows and their distribution
- Study the “dynamics” of the network
- Detect malicious programs: viruses, port scanning, flooding...
- Verify at high level the IP connectivity: DNS, HTTP and Mail services

Ethereal

The screenshot shows the Ethereal (Wireshark) interface with a filter set to `ip.src == 194.109.209.218`. The packet list pane shows several SSH and POP3 packets. The selected packet (No. 92) is a POP3 response with the message: `-ERR [AUTH] "aep": access denied.`

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	POP3	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	POP3	Response: -ERR [AUTH] "aep": access denied.
94	26.992657	194.109.209.218	85.226.127.250	POP3	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 8d 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..RS.N.
0030  05 a8 46 95 00 00 01 01 08 0a 0a 67 a6 c0 01 30  ..F.....g...o
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

- Very detailed information for a certain traffic flow
- We can filter and examined per-transaction basis
- We can determine if it is:
 - connectivity problem (machine not reachable)
 - service problem (service not available)
 - user/server problem (authentication, application, configuration)

Most common "wireless" related problems are related to...

- PHY: hidden nodes, multipath, noise
- IP: network planning, multiple dhcpd, asymmetric transmission speeds
- Application: viruses, peer-to-peer

Conclusions

- The more you know about how things work... the easier to troubleshoot when they do NOT work!
- Understanding a problem is not the same that solving a problem

Final tips!

Takes less time to rebuild an undocumented system than to troubleshoot it

If you need help, be ready to provide documentation