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!

<table>
<thead>
<tr>
<th>Layer</th>
<th>ISO</th>
<th>TCP/IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application</td>
<td>Application</td>
</tr>
<tr>
<td>6</td>
<td>Presentation</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Session</td>
<td>Transport</td>
</tr>
<tr>
<td>4</td>
<td>Transport</td>
<td>Network</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Data link</td>
<td>Media Access</td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>TCP/IP</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>nslookup</td>
</tr>
<tr>
<td>Transport (TCP)</td>
<td>Ntop (Win32/Linux)</td>
</tr>
<tr>
<td></td>
<td>Visualroute, traceroute</td>
</tr>
<tr>
<td>Network (IP)</td>
<td>Nmap, Ntop (Win32/Linux)</td>
</tr>
<tr>
<td></td>
<td>Ethereal, Etherape</td>
</tr>
<tr>
<td>Media Access Control</td>
<td>Ethereal (Win32/Linux)</td>
</tr>
<tr>
<td></td>
<td>Netstumbler (Win32), Kismet, Wavemon, Wellenreiter</td>
</tr>
<tr>
<td></td>
<td><strong>Vendor Specific Tools</strong></td>
</tr>
</tbody>
</table>
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

![Netstumbler Screen](image)

<table>
<thead>
<tr>
<th>MAC</th>
<th>SSID</th>
<th>Name</th>
<th>Chan</th>
<th>Speed</th>
<th>Vendor</th>
<th>Type</th>
<th>Enc...</th>
<th>SNR</th>
<th>Signal+</th>
<th>Noise-</th>
<th>SNR+</th>
</tr>
</thead>
<tbody>
<tr>
<td>000F3D3B195E</td>
<td>default</td>
<td>2</td>
<td>54 Mbps</td>
<td>AP</td>
<td></td>
<td>18</td>
<td>-82</td>
<td>-100</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>000F669AAE99</td>
<td>linksys</td>
<td>6</td>
<td>11 Mbps</td>
<td>Linksys</td>
<td>AP</td>
<td>19</td>
<td>-80</td>
<td>-100</td>
<td>20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>000F66E1DC43</td>
<td>buss</td>
<td>6*</td>
<td>54 Mbps</td>
<td>Linksys</td>
<td>AP</td>
<td>34</td>
<td>-37</td>
<td>-100</td>
<td>63</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Channels:**
- 2
- 6

**SSID's**
- buss
- default
- linksys

**Filters**
- Encryption Off
- Encryption On
- ESS (AP)
- IBSS (Peer)
- CF Pollable
- Short Preamble
- PBCC
- Short Slot Time (11g)
- Default SSID
Netstumbler

• Retrieve physical/link layer info in ”passive” move
• User our wireless card as a “radio analysiser”
• 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

File: /tmp/etherXXBBsEew
Subtype: application/x-protobuf
Length: 11 KB
Creation time: 00:00:32

P: 102 D: 23 M: 0 Crops: 0

0000 00 12 f0 02 b7 f7 00 02 17 29 b4 00 00 00 04 00 ...b.... ...b.... ...
0010 00 57 32 4e 40 00 00 00 00 a9 32 c2 0d 01 0e 55 62 ...w2@.6...2.m.u. ...
0020 a4 fe 00 0e c7 03 27 47 a4 fe 52 35 d3 46 00 10 ......'...'.m.s.n. ...
0030 a4 fc 00 01 00 01 00 00 00 00 a9 32 c2 0d 01 0e 55 62 ...w2@.6...2.m.u. ...
0040 4b 48 2d 45 52 52 20 5b 41 55 54 48 54 20 22 61 KH-FIR [ AUTH ] = a
0050 65 70 22 3a 20 20 61 69 6e 66 6f 72 20 61 6e 64 ap' acc err dens ...
0060 65 64 2e 0d 0a ed...
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