Wireshark Developer and User Conference

Network Mysteries & How to Solve Them
Mystery 1 - Case of the Slow Network

Wednesday June 15, 2011 - 10:15am - 11:30am

Betty DuBois
Principal Consultant | DuBois Training & Consultant, LLC
Betty@DTCpackets.com

SHARKFEST '11
Stanford University
June 13-16, 2011

Agenda

- You've just been called to solve a mystery. Where do you start?
  - What questions to ask
  - What tools do you need
  - Once you have the traces - what then?

Client Interview

- This is the most critical step - more data is better
- Think like a reporter and ask the 5 W's
  - **Who** is complaining?
    - Are they in different physical locations?
    - If same location, different subnets?
  - **What** are they complaining about?
    - Which specific applications?
    - Do they have other applications they rely on? AD for example?
  - **Where** are the clients and servers involved physically?
  - **When** did it start?
    - Is it constant or intermittent?
  - **Why** did you call?
    - Are they short on time, expertise, or both?

Tools

- Wireshark - duh…. ☺
- Taps - sure makes life easier
- Mirror switches - not everyone can afford taps
- Cable tester - don't forget layer 1 in the OSI
- 802.11 rfmon capable interfaces - AirPcap
- Long term capture device

- Disclosure - I cheat and use Pilot

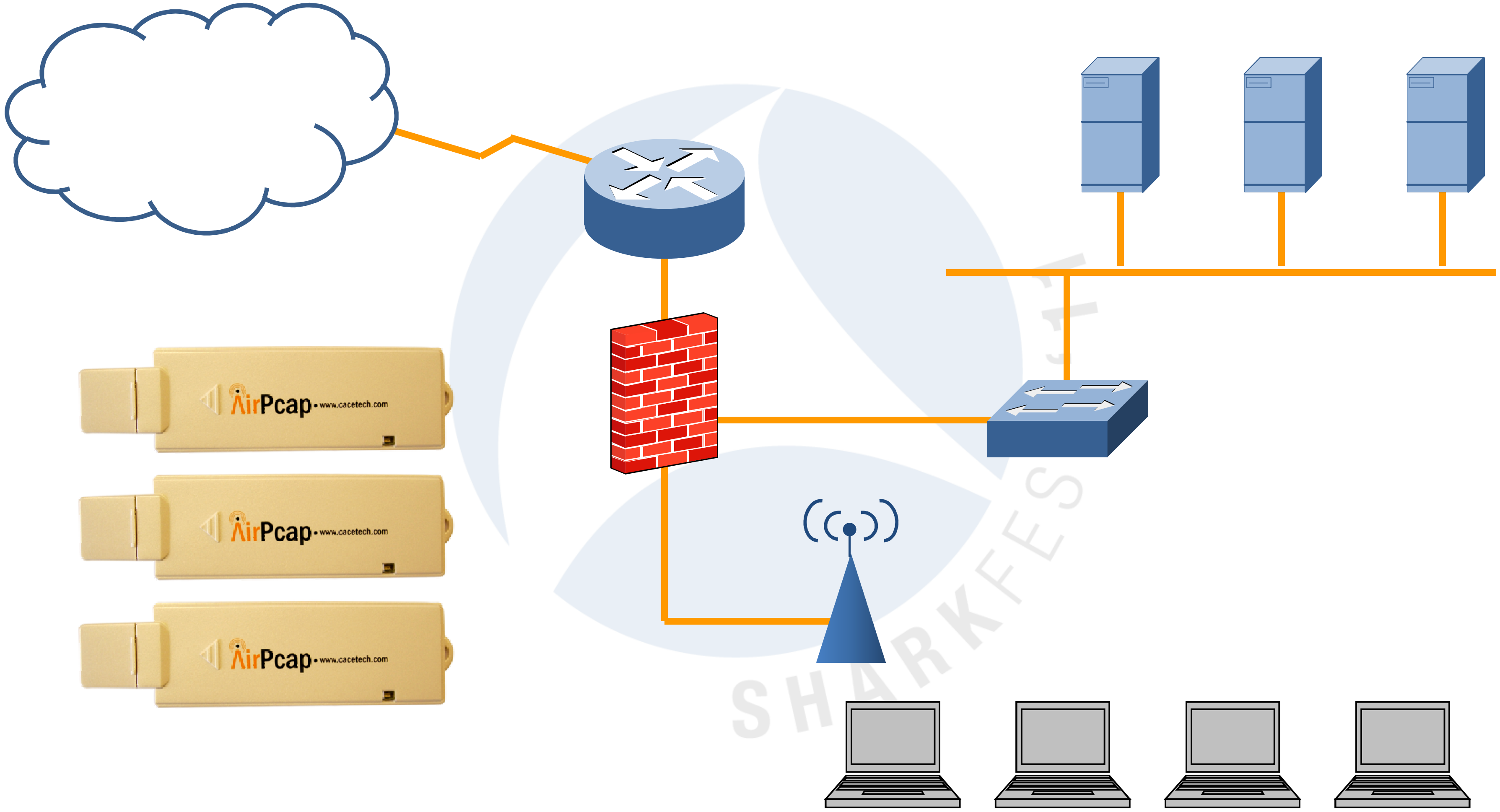
Mystery 1

Case of the Slow Network

- Users were complaining access to the Internet was slow on the guest wireless network. It just started happening yesterday
- Possible suspects?
  1. ______________________________
  2. ______________________________
  3. ______________________________
- Possible accomplices? Are there any interdependent protocols involved?

Crime Scene

- Never start without a network diagram



Tracefile Time

- Case of the Slow Network.pcap

Q & A

- Questions?????

Thanks For Coming!

Enjoy the rest of the conference.