Solving Network Performance Problems with Wireshark

Laura Chappell
Founder  |  Wireshark University

SHARKFEST '08
Foothill College
March 31 - April 2, 2008
TurboCap

- Full Speed
- Traffic TAP
- 1 Gb
- 2 Copper ports
- Wireshark
- Aggregation
- Capture and Injection
- WinPcap
Capturing Traffic: Analyzer Placement

Considerations:

- Wired vs. Wireless
- Switched Network Issues
- Half-Duplex vs. Full-Duplex
Half-Duplex – Hubbing Out

Hub issues – is it really a hub?
Hub issues – is it really a hub?
Port Spanning

Switch(config)#interface fastethernet 0/1
Switch(config-if)#port monitor fastethernet 0/2
Switch(config-if)#port monitor fastethernet 0/5
Full-Duplex Tap Options

Copper or Fiber
Aggregating or Non-Aggregating
Passive (no power) or Active
Regenerating Taps
Advanced Taps (packet insertion, filtering)
Wireless Traffic Capture

801.11 ABGN
External antennas
Channel scanning (monitor mode)
Multi-channel capture
Aggregating traffic
Transmit capability
Overview of the Onsite Process

The “Primary Directive”
The trace file log (www.wiresharkU.com)
Network diagrams in advance
Trace files in advance (if possible)
Local staff level of knowledge
Tap-in point availability
Bullet list of issues seen during analysis
Recommendations
Report – graphs, notes
Analyzing Network Performance Issues

Key Issues:

- High Latency (Client, Server, Link)
- Packet Loss (Upstream, Downstream)
- Congestion (Network, Receiver)
- Configuration Problems (Service Unavailable, Loops)
- Redirections (Routing, Service)
- Interdependencies (Third Parties)
- Low throughput (Itty-Bitty Stinkin’ Packets)
- Negotiation Faults (Protocol or Application Layer)
Reports

Overview of traffic
Protocol distribution
Conversations
ICMP traffic
… etc.

All with notes included.
What’s Next?

Laura’s Lab Kit v9
In show bags as well as...
ISO image: www.novell.com/connectionmagazine/laurachappell.html
Wireshark University: www.wiresharkU.com
Laura’s Blog: laurachappell.blogspot.com/