

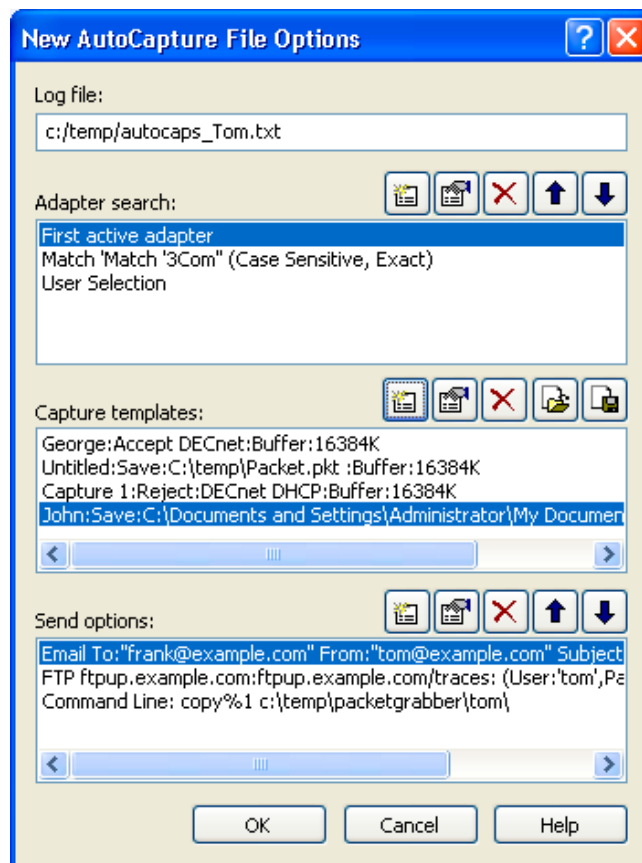
Essential PacketGrabber

Ten Use Scenarios for WildPackets' Distributed Packet Capture Engine

PacketGrabber extends your ability to troubleshoot enterprise networks by easily gathering trace files across the network, from the network core to the most isolated segments and everything in between. Once collected, these trace files can be automatically forwarded for expert analysis by WildPackets' EtherPeek NX. PacketGrabber's robust capture engine can be fully automated to capture only the packets needed for Expert Analysis with EtherPeek NX. The resulting trace file is then automatically forwarded via email, ftp, or file server.

1. Baselining AutoCapture

Use the Windows Task Scheduler with PacketGrabber to periodically run baselining captures. Set the Task Scheduler to run PacketGrabber at the top of every hour, every six hours, once a day, or whatever your baselining needs require. Create an AutoCapture template that captures one full buffer of data and then sends the data back to a central location via FTP, email, or command line.



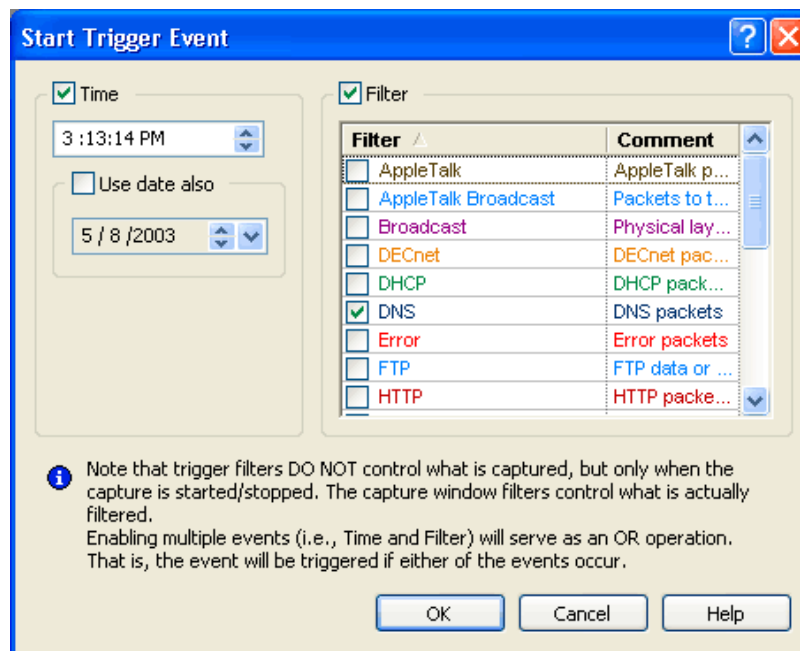
AutoCapture File Options Window

2. Visibility into the Desktop

PacketGrabber's affordable licensing makes it feasible to include it as a part of a standard workstation image. The administrator can put a shortcut to PacketGrabber (including a command line option containing a pre-configured autocapture template) on the desktop. The users could be instructed to click the icon, creating a capture of traffic on their segment, as part of a problem report.

3. Advanced Customizable Triggers

Construct a trigger on a specially chosen, unique packet, and then use the packet as a way to remotely control individual PacketGrabbers running on the network. For example, you could configure each PacketGrabber to start capture when it sees an ARP request for X.X.X.240 (assuming that there are no stations with that IP address). You could then ping the .240 address on a subnet, causing the subnet's edge router to send an ARP request for that address, and triggering the capture remotely. Since PacketGrabber supports "repeat trigger" mode, when it finishes capturing, it will go back to listening for the "trigger packet," allowing you to start another capture at a later date without the need to explicitly reset PacketGrabber.



Start Trigger Event Window

4. Multiple Simultaneous Captures

PacketGrabber is a great way to see multiple perspectives on traffic at the same time. For example, capture with EtherPeek on one end of a WAN link and simultaneously capture with PacketGrabber at the other end. Then, compare the captures side by side to see what differences (e.g. in packet latency, etc...) the WAN link introduced.

5. Minimize Packet Loss

Because PacketGrabber doesn't process the packets that it captures, it may actually be preferable to EtherPeek in high-speed environments where it is important to avoid dropping packets. Since EtherPeek must process each packet it captures in real-time, it may drop packets at very high traffic volumes, especially on machines with slower processors. PacketGrabber is less susceptible to packet loss under the same circumstances. Some

customers actually use multiple copies of PacketGrabber running on different machines, capturing simultaneously and streaming to disk, to further minimize the possibility of packet loss.

6. Automatic File Forwarding

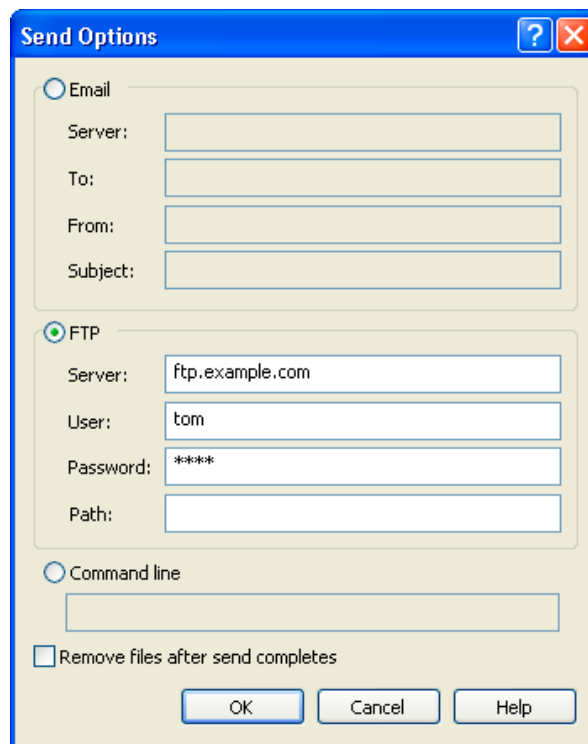
PacketGrabber is great for remote troubleshooting. Instead of sending an engineer to a remote site, send PacketGrabber with an auto-capture template. Double-clicking on the auto-capture template will start capture with the pre-configured parameters. If the template is configured properly, PacketGrabber can automatically send the captured packets back to you.

7. Troubleshoot Problems at the Edge of the Network

Use PacketGrabber as your "eyes and ears in the field." Sometimes, EtherPeek is installed on a machine in the server room. This makes it easy to mirror core switch ports over to EtherPeek for monitoring. But this might also make it difficult to troubleshoot problems at the edge of the network. Since each copy of EtherPeek comes with a single license of PacketGrabber, you can install PacketGrabber on your laptop, take it to the edge, capture, and then bring the files back to the server room for analysis. This method can be used any time that EtherPeek is installed on a machine that can't be moved around easily. Better yet, take advantage of our special PacketGrabber site license pricing, and extend the expert analysis capabilities of EtherPeek across the network, from the network core to the most isolated segments and everything in between.

8. Send Capture Files Across Network

PacketGrabber can send capture files via FTP or SMTP. If you need to send files via some other method, PacketGrabber allows you to specify a command line option. One common use for this is to copy files to a network share. Alternatively, you could run a batch file that first copies the files and then sends an email to you notifying you of the capture.



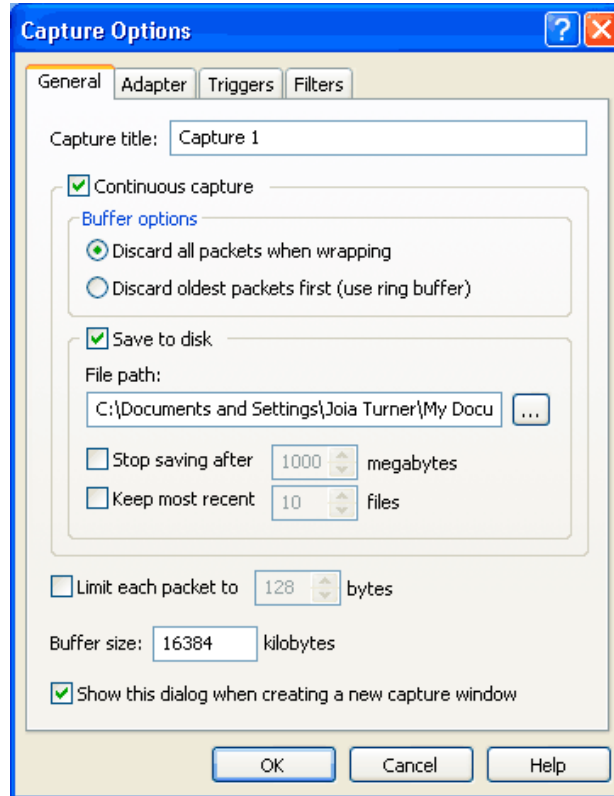
Send Options Window

9. Save Capture Files to Local Directory

Under some circumstances, you might not want PacketGrabber to push files across the network as soon as they are captured. For example, if the network is slow, then PacketGrabber sending captures might slow it down even more. Under these circumstances, create a shared directory on the user's machine and have PacketGrabber save to that directory. Then, browse to the shared directory at your leisure and pull the files down.

10. Continuous Capture for Troubleshooting

Sometimes, network problems are sporadic and unpredictable. In these cases, set PacketGrabber up on one or more machines that have had the problem. Configure PacketGrabber to capture continuously with Save to Disk active. Then, start capture and walk away! PacketGrabber consumes very little system resources, so the user will probably not notice any difference. You could even put PacketGrabber (with appropriate reference to an autocapture template, of course) in their startup folder! When the problem occurs, you know that you'll have captured it. In order to prevent PacketGrabber from filling up the machine's disk, configure the buffer size and "keep last N files" options. With these options, PacketGrabber will keep only the most recent files.



Capture Options Window, showing continuous capture options

WildPackets Professional Services

WildPackets offers a full spectrum of unique professional support services, available on-site, online or through remote dial-in service.

WildPackets Academy

WildPackets Academy provides the most effective and comprehensive network and protocol analysis training available, meeting the professional development and training requirements of corporate, educational, government, and private network managers. Our instructional methodology and course design centers around practical applications of protocol analysis techniques for Ethernet and 802.11 wireless LANs.

In addition to classroom-taught Network Analysis Courses, WildPackets Academy also offers:

- Web-Delivered Training
- On-site and Custom Courseware Delivery
- The (T.E.N.) Technology, Engineering, and Networking Video Workshop Series
- On-site and Remote Consulting Services
- Instruction and testing for the Network Analysis Expert (NAX™) Certification

For more information about consulting and educational services, including complete course catalog, pricing and scheduling, please visit www.wildpackets.com/services. NAX examination and certification details are available at www.nax2000.com.

Live Online Quick Start Program

WildPackets now offers one-hour online Quick Start Programs on using EtherPeek NX/ EtherPeek and AiroPeek NX/AiroPeek, led by a WildPackets Academy Instructor. Please visit www.wildpackets.com for complete details and scheduling information.

About WildPackets, Inc.

Since 1990, WildPackets has built affordable and easy to use network analysis tools. Our customers rely on WildPackets tools to help them design, maintain, troubleshoot, and optimize their networks. For information about our company, its products and partners, please see our website at www.wildpackets.com. See the WildPackets Academy site, www.wildpackets.com/services, for information on courses and Professional Services offerings. WildPackets' Network Analysis Expert (NAX) Certification Program details can be found at www.nax2000.com.

WildPackets, Inc.
1340 Treat Blvd., Suite 500
Walnut Creek, CA 94597
925-937-3200
www.wildpackets.com

20030703-M-TCT002

