

Creating Network Captures with Wireshark

To troubleshoot network problems it sometimes becomes necessary to make a packet capture demonstrating the problem. Follow the directions in this note to create a network capture that you can submit to FacetCorp support for analysis.

Wireshark is a useful utility for capturing network data packets between two or more systems. <u>Wireshark Download</u>

Once you have Wireshark running, select the interface that you will be capturing through if you have multiple interfaces displayed.

Filter:						
WI	RESHARK	The World's Most Popular				
Capture						
Interface List Live list of the capture interfaces (counts incoming packets)						
Start c	apture on interface: Microsoft MS Tunnel Interface Driver Realtek RTL8102E PCI-E Fast	Ethernet NIC				
i	Capture Options Start a capture with detailed opt	ions				

Once the interface is selected, Wireshark will begin to capture data packets via that interface. At this point re-create your network problem so that the event can be captured. Watch the packet count at the bottom of the Wireshark display page. The count should increase as data packets are displayed and captured:

Realtek RTL8102E PCI	-E Fast Ethernet NIC -	Wireshark		
<u>File E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>Analyze</u>	Statistics 7	Felephon <u>y T</u> ools	<u>H</u> elp
Image: Second	 Interfaces Options Start 	Ctrl+I Ctrl+K Ctrl+E	Þ 🗢 သ 孩 50	Expression
No Time	💕 Stop	Ctrl+E		Destination
121 25.65366 122 25.65396 123 25.65447	 <u>R</u>estart Capture <u>Filters</u> 	Ctrl +R	9.166.50 9.166.50 68.44.101	192.168. 192.168. 199.29.1
124 25.682793 125 25.684809	E Ə	199. 199.	29.166.50 29.166.50	192.168. 192.168.
126 25.68568 127 25.714699 128 25.716964	9 1	192. 199. 199.	29.166.50 29.166.50	199.29. 192.168. 192.168.
129 25.717662 130 25.749452 131 25.749689	192. 199. 199.	168.44.101 29.166.50 29.166.50	199.29.1 192.168. 192.168.	
132 25.751091 133 25.777610 134 25.777892	192. 199. 199.	168.44.101 29.166.50 29.166.50	199.29.1 192.168. 192.168.	

When the problem has been captured you can save the capture session to a file that can be emailed to FacetCorp.

Use the Capture menu option dropdown box to select Stop capture. When you exit the program you will be asked if you want to save the captured data. Save it to a file on your system and give it an extension of "cap". You can also use the File menu option and select Save As.

Along with the capture, send us the following information:

- 1. The partnumber of the FacetCorp product being captured
- 2. Your server OS information (uname -a, uname -X or oslevel)
- 3. Entries generated in "syslog" or "messages" during the capture
- 4. The IP addresses that should be examined in the capture (client and server)
- 5. A brief description of the problem being reported.
- 6. Send us all these items via email to: support@facetcorp.com

Your capture file will be submitted to the FacetCorp development team for review. A technical support agent will contactyou with information regarding your reported problem after it has been analyzed.