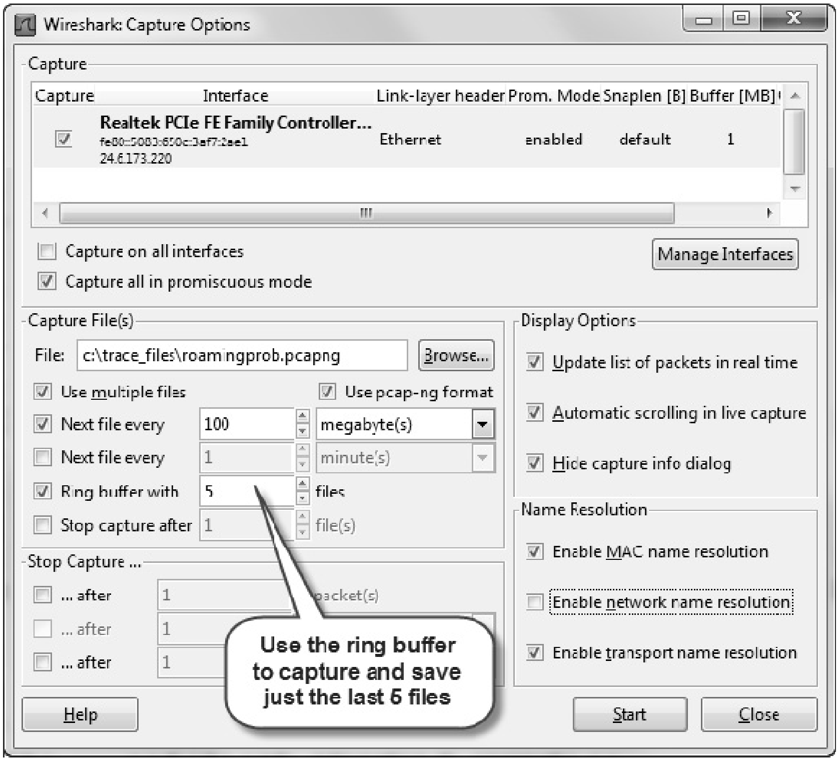
2.6. Use Special Capture Techniques to Spot Sporadic Problems

Sporadic, roaming problems often plague analysts. Using a few key Wireshark functions you can be ready to catch these annoyingly elusive events.

If you have a sporadic problem, one that seems to appear on and off through a network, you will need to be a bit more creative with your capture process. In this case, you should capture traffic continuously until the problem occurs again.

Use File Sets and the Ring Buffer

In this situation, set up Wireshark to capture traffic to file sets, but use the ring buffer option. In Figure 52, we defined a new file name (*roamingprob.pcapng*) and indicated that we want to keep a total of 5 files (ring buffer setting of 5).



Wireshark: Capture Options

Capture

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MB]
☑	Realtek PCIe FE Family Controller... fe80::5083:650c:3ef7:2ae1 24.6.173.220	Ethernet	enabled	default	1

□ Capture on all interfaces
☑ Capture all in promiscuous mode

Capture File(s)

File: c:\trace_files\roamingprob.pcapng

☑ Use multiple files
☑ Use pcap-ng format
☑ Next file every 100 megabyte(s)
□ Next file every 1 minute(s)
☑ Ring buffer with 5 files
□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 1 packet(s)
□ ... after 1
□ ... after 1

Display Options

☑ Update list of packets in real time
☑ Automatic scrolling in live capture
☑ Hide capture info dialog

Name Resolution

☑ Enable MAC name resolution
□ Enable network name resolution
☑ Enable transport name resolution

Use the ring buffer to capture and save just the last 5 files

Figure 52. We are going to examine the last 500 MB of traffic leading up to the problem point in time.

When Wireshark finishes capturing the fifth 100 MB file, it will delete the first 100 MB file and create a sixth 100MB file. Let Wireshark run continuously. The file set feature won't fill up the hard drive and you will have the last 500 MB leading up to the problem.