Identify the Most Active Conversations

A conversation is a pair of physical or logical entities communicating. Conversations can include just MAC layer addresses (ARP conversations for example), network layer addresses (ICMP ping conversations for example), port numbers (FTP conversations for example), etc.

Conversations are pairs of hosts communicating while an endpoint is a single side of a conversation. Note that communications from a host to the broadcast address are listed as a conversation. Broadcast and multicast addresses are listed as endpoints in the endpoint window, even though there is no such host as a "broadcast" host or a "multicast" host.

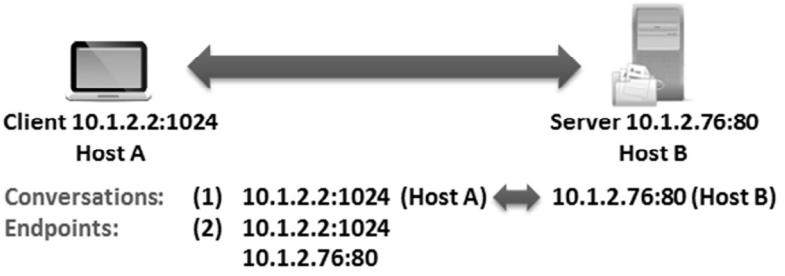

Figure 126. Comparing conversations with endpoints

Select **Statistics | Conversations** to view the Conversations window. When working with a large trace file, sorting on the bytes transferred between hosts enables you to detect the most active connections based on packets, bytes, bits per second or total duration of conversation. Figure 127 shows a conversation list for TCP connections. Notice that there is only one Ethernet conversation, but numerous IP, TCP and UDP conversations that travel over that one Ethernet conversation.

In this example we have sorted on the bytes column to identify the most active conversation based on bytes transferred between TCP hosts.

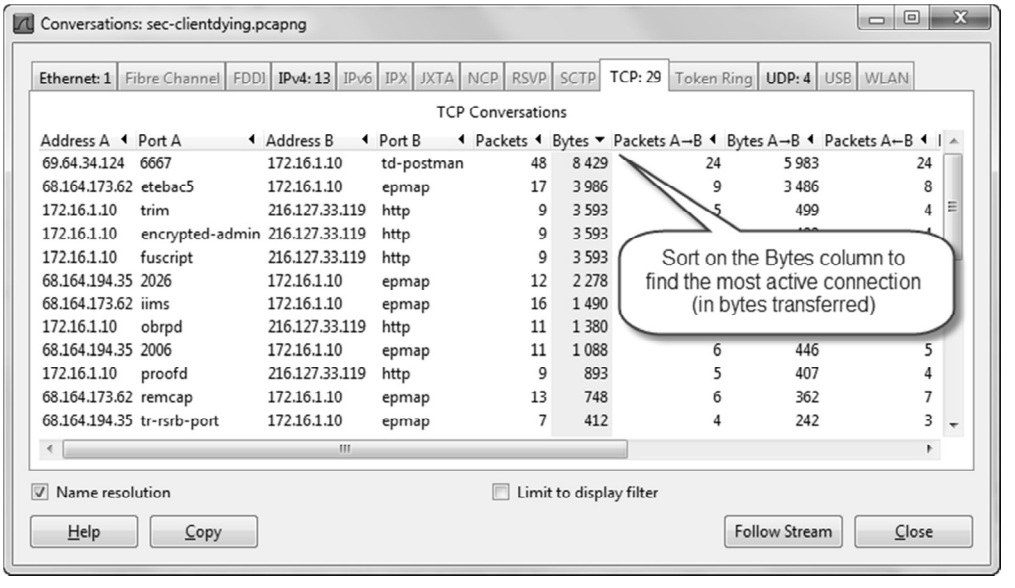

Figure 127. Conversations define pairs of hosts that communicate with each other [sec-clientdying.pcapng]