

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.

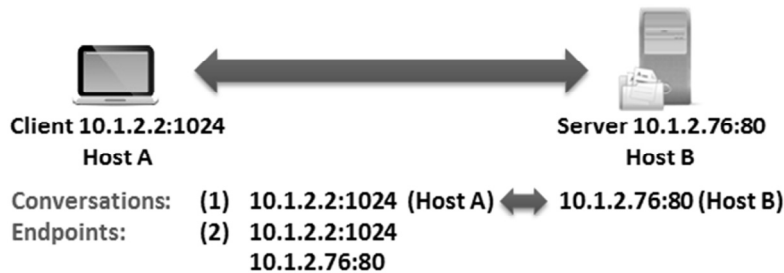


Figure 126. Comparing conversations with endpoints

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.

Conversations: sec-clientdying.pcapng

Ethernet: 1 | Fibre Channel | FDDI | IPv4: 13 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 29 | Token Ring | UDP: 4 | USB | WLAN

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets B→A
69.64.34.124	6667	172.16.1.10	td-postman	48	8 429	24	5 983	24
68.164.173.62	etebac5	172.16.1.10	epmap	17	3 986	9	3 486	8
172.16.1.10	trim	216.127.33.119	http	9	3 593	5	499	4
172.16.1.10	encrypted-admin	216.127.33.119	http	9	3 593			
172.16.1.10	fuscript	216.127.33.119	http	9	3 593			
68.164.194.35	2026	172.16.1.10	epmap	12	2 278			
68.164.173.62	iims	172.16.1.10	epmap	16	1 490			
172.16.1.10	obrpd	216.127.33.119	http	11	1 380			
68.164.194.35	2006	172.16.1.10	epmap	11	1 088	6	446	5
172.16.1.10	proofd	216.127.33.119	http	9	893	5	407	4
68.164.173.62	remcap	172.16.1.10	epmap	13	748	6	362	7
68.164.194.35	tr-rsrb-port	172.16.1.10	epmap	7	412	4	242	3

Sort on the Bytes column to find the most active connection (in bytes transferred)

Name resolution Limit to display filter

Help Copy Follow Stream Close

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